SonicWall® SonicOS 6.5 システム設定

管理

SONICWALL®

目次

SonicOS システムのセットアップについて **16**
管理インターフェース SonicOS について 16

基本設定の構成 **18**
「装置 | 基本設定」について 19
ワンクリック無線および非無線制御モード 19
装置を設定する 21
「装置 | 基本設定」ページへのアクセス 21
ファイアウォール名の設定 22
管理者名とパスワードの変更 22
無線 LAN と IPv6 の有効化 23
ログイン セキュリティの設定 24
複数管理者アクセスの設定 29
拡張監査ログのサポートの有効化 33
無線 LAN 制御の設定 34
管理インターフェースの設定 35
フロントパネル管理インターフェースの設定 (SuperMassive ファイアウォールのみ) . . . 41
クライアント証明書の確認の設定 42
証明書の期限切れの確認 46
SSH 管理の設定 46
SonicOS API の有効化 47
より高度な管理オプションの設定 47
SonicPoint イメージの手動ダウンロード 50
言語の選択 51

SNMP の管理 **53**
「**装置 > SNMP**」について 53
SNMP について 53
SNMP アクセスの設定 54
SNMP のサービスとしての設定およびルールの追加 64
SNMP ログについて 64

証明書の管理 **65**
証明書について 65
デジタル証明書について 65
「証明書と証明書署名リクエスト」テーブルについて 66
証明書のインポート 68
証明書の削除 70
証明書署名リクエストの生成 71
単純証明書登録プロトコルの設定 75

時間の設定 77
「**装置 > 時間**」について 77
システム時間の設定 78
NTP の設定 79

スケジュールの設定 82
スケジュールについて 82
「**装置 > スケジュール**」について 83
個別スケジュールの追加 84
スケジュールの変更 85
個別スケジュールの削除 86

ユーザの管理について 89
ユーザ管理について 89
ローカル ユーザおよびローカル グループを使った認証 91
RADIUS を使った認証 93
LDAP/アクティブ ディレクトリ/イーディレクトリ認証の使用 94
TACACS+ の使用 99
シングル サインオンについて 99
シングル サインオン エージェント/ターミナル サーバ エージェントの
インストール 112
複数管理者サポートについて 123
複数管理者サポートの設定 125

ユーザの管理のための設定 128
ユーザ > 設定 128
ユーザ認証とログインの設定 129
ユーザ セッションの設定 140
カスタマイズ 144
アカウント 151
RADIUS 認証の設定 154
LDAP を使用するための SonicWall の設定 162
拡張 LDAP テストについて 178
認証用の TACACS + の設定 179
SonicOS で SonicWall SSO エージェントを使用するための設定 180

認証パーティションの管理 205
認証パーティション処理について 205
ユーザ認証パーティション処理について 206
サブパーティションについて 207
パーティション間ユーザ ローミングについて 210
認証パーティションの選択について 211
複数 LDAP サーバの拡張サポートについて 213
パーティション毎の DNS サーバと分割 DNS 214
RADIUS 認証について 214

パーティション処理以外の設定からのアップグレード 214
認証パーティションおよびポリシーの設定 215
ユーザ/パーティションの表示とフィルタ 215
パーティションの設定と管理 217
パーティション選択ポリシーの設定 230
認証パーティション用のサーバ、エージェント、クライアントの設定 235

ローカル ユーザおよびグループの設定 237
認証とパスワードについて 237
二段階認証の使用 237
初回ログイン パスワードの変更の強制 238
ローカル ユーザの設定 238
すべてのユーザのクォータ制御 239
ローカル ユーザの表示 239
ローカル ユーザの追加 240
ローカル ユーザの編集 247
グローバル設定の構成 248
ローカル ユーザを LDAP からインポートする 249
ゲスト管理者の設定 249
ローカル グループの設定 250
ローカル グループの作成または編集 251
LDAP からのローカル グループのインポート 259
LDAP 位置によるユーザ メンバーシップの設定 259

ゲスト サービスとゲスト アカウント 260
ユーザ > ゲスト サービス 260
グローバル ゲスト設定 261
ゲスト プロファイル 261

ゲスト アカウントの管理 265
ユーザ > ゲスト アカウント 265
ゲスト アカウント統計の表示 266
ゲスト アカウントの追加 268
ゲスト アカウントの有効化 274
ゲスト アカウントの自動削除の有効化 274
ゲスト アカウントの編集 274
ゲスト アカウントの削除 274
アカウント詳細の印刷 275

インターフェースの設定 278
インターフェースについて 279
物理インターフェースと仮想インターフェース 279
SonicOS のセキュリティ保護されるオブジェクト 283
トランスペアレント モード 283
IPS スニッファ モード 283

Firewall Sandwich 286
HTTP/HTTPS リダイレクト 286
インターフェースでの DNS プロキシの有効化 287
LTE モデムのサポート 287
LAN バイパス 287
ネットワーク > インターフェース 287
PortShield インターフェースの表示/非表示 (IPv4 のみ) 289
インターフェース設定 290
インターフェース トラフィック統計 291
インターフェースの設定 292
静的インターフェースの設定 293
ルート モードの設定 300
インターフェースでの帯域幅管理の有効化 301
インターフェースのトランスペアレント IP モード (L3 サブネットを結合) の設定 303
無線インターフェースの設定 307
WAN インターフェースの設定 313
トンネル インターフェースの設定 318
リンク統合化とポート冗長化の設定 323
仮想インターフェース (VLAN サブインターフェース) 327
IPS スニッファ モードの設定 328
セキュリティ サービス (統合脅威管理) の設定 332
ワイヤ モードとタップ モードの設定 333
ワイヤ モードでのリンク統合 337
レイヤ 2 ブリッジ モード 339
レイヤ 2 ブリッジ モードの設定 360
非対称ルーティング 368
インターフェースの IPv6 設定 369
31 ビット ネットワーク 369
PPPoE アンナンバード インターフェースのサポート 371

PortShield インターフェースの設定 373
ネットワーク > PortShield グループ 373
PortShield について 373
SonicOS がサポートする X シリーズ スイッチ 374
SonicOS がサポートする N シリーズ スイッチ 384
ポートの管理 389
PortShield グループの設定 398

PoE の設定 404
ネットワーク > PoE 設定 404
PoE の有効化 405
標準 PoE 設定を構成する 407
ポートの電力設定の構成 407

フェイルオーバーと負荷分散の セットアップ 409

ネットワーク > フェイルオーバーと負荷分散 409
フェイルオーバーと負荷分散について 409
フェイルオーバーと負荷分散のしくみ 410
複数 WAN (MWAN) 411
ネットワーク > フェイルオーバーと負荷分散 412
フェイルオーバーと LB グループの設定 415
グループ メンバーの監視設定の構成 420

ネットワーク ゾーンの設定 422
ゾーンについて 422
ゾーンの動作 423
事前定義ゾーン 424
セキュリティ種別 424
インターフェース間通信を許可する 425
ゾーンで SonicWall セキュリティ サービスを有効にする 425
無線および非無線制御モードの効果 426
ネットワーク > ゾーン 428
ゾーンの設定テーブル 429
新しいゾーンの追加 430
ゲスト アクセス用ゾーンの設定 433
オープン認証およびソーシャル ログイン用ゾーンの設定 436
Radius によるキャプティブ ポータル認証用のゾーンの設定 437
ユーザ定義ポリシー メッセージ用のゾーンの設定 439
ユーザ定義ログイン ページ用のゾーンの設定 441
WLAN ゾーンの設定 442
RADIUS サーバの設定 444
DPI-SSL をゾーン単位できめ細かく制御する設定 446
ユーザポリシー ページへの自動リダイレクトを有効にする 446
ゾーンの削除 447

ワイヤ モード VLAN 変換の設定 449
ネットワーク > VLAN 変換 449
VLAN 変換について 449
VLAN 割付の作成と管理 451

DNS の設定 457
ネットワーク > DNS 457
分割 DNS について 457
DNS サーバの管理 459
DNS と IPv4 467

DNS プロキシの設定 470
ネットワーク > DNS プロキシ 471
DNS プロキシについて 472
DNS プロキシの有効化 475

DNS プロキシの設定 476
DNS サーバ状況の監視 477
分割 DNS サーバの状況の監視 477
静的 DNS キャッシュ エントリの表示と管理 478
DNS プロキシ キャッシュ エントリの表示 479

DNS セキュリティの設定 481
シンクホールについて 481
ネットワーク > DNS セキュリティ 481
DNS セキュリティの設定を構成する 482
リスト内のエントリの削除 483
DNS トンネリング検知について 483

ルート通知とルート ポリシーの設定 486
ルーティングについて 487
メトリックと管理距離 487
ルート通知 489
ECMP ルーティング 489
ポリシーベース ルーティング 489
ポリシーベース TOS ルーティング 490
PBR のメトリックベースの優先順位 491
ポリシー ベースのルーティングと IPv6 491
OSPF および RIP の高度なルーティング サービス 492
ドロップ トンネル インターフェース 500
アプリベースのルーティング 501
ネットワーク > ルーティング 501
ネットワーク > ルーティング > 設定 501
ネットワーク > ルーティング > ルート ポリシー 502
ネットワーク > ルーティング > ルート通知 503
ネットワーク > ルーティング > OSPFv2 504
ネットワーク > ルーティング > RIP 505
ネットワーク > ルーティング > OSPFv3 506
ネットワーク > ルーティング > RIPng 508
ルーティングの設定 508
メトリックによるルートの優先順位付け 509
ルータ広告によって学習されたデフォルト ルートに対するメトリックの設定 509
ルート通知の設定 510
静的およびポリシーベースのルートの設定 511
ドロップ トンネル インターフェースに対応する静的ルートの設定 516
OSPF および RIP の高度なルーティング サービスの設定 517
BGP の高度なルーティングの設定 528
アプリベースのルートの設定 529

ARP トラフィックの管理 530

ネットワーク > ARP 530
静的 ARP エントリ 531
ARP 設定 535
ARP キャッシュ 535

近隣者発見プロトコルの設定 537
ネットワーク > 近隣者発見 (IPv6 のみ) 537
静的 NDP 登録 538
NDP 設定 539
NDP キャッシュ 539
静的 NDP 登録の設定 540
静的 NDP 登録の編集 541
NDP キャッシュの消去 541

MAC-IP アンチスプーフの設定 542
MAC-IP アンチスプーフ保護について 542
IP ヘルパーへの拡張 543
ネットワーク > MAC-IP アンチスプーフ 544
インターフェースに対する設定 545
アンチスプーフ キャッシュ 546
スプーフ検知リスト 547
MAC-IP アンチスプーフ保護の設定 548
トラフィック統計の表示 548
IPv6 インターフェースの MAC-IP アンチスプーフ設定の編集 549
IPv4 インターフェースの MAC-IP アンチスプーフ設定の編集 550
アンチスプーフ キャッシュへの機器の追加 552
アンチスプーフ キャッシュ エントリの削除 553
表示対象のフィルタ 553
スプーフ検知リストからの静的エントリの追加 554

DHCP サーバのセットアップ 555
ネットワーク > DHCP サーバ 555
DHCP サーバ オプション機能 557
インターフェースごとの複数 DHCP スコープ 558
DHCP サーバ恒久性について 560
DHCP サーバの設定 561
DHCP サーバ リース範囲 562
現在の DHCPリース 563
DHCPv6 リレー 564
詳細オプションの設定 565
DHCP サーバの動的範囲の設定 571
静的 DHCP 登録の設定 577
DHCP リース範囲の DHCP 汎用オプションの設定 579
RFC で定義された DHCP オプション番号 580

DHCP と IPv6 587

IP ヘルパーの使用 588
IP ヘルパーについて 588
VPN トンネル インターフェースによる IP ヘルパーのサポート 589
DHCPv6 リレー 590
ネットワーク > IP ヘルパー 592
リレー プロトコル 593
ポリシー 594
DHCP/DHCPv6 リレー リース 594
IP ヘルパーの設定 595
IP ヘルパーの有効化 595
リレー プロトコルの管理 595
IP ヘルパー ポリシーの管理 597
表示される DHCP リレー リースのフィルタ 599
TSR による IP ヘルパー キャッシュの表示 600

ウェブ プロキシ転送のセットアップ 602
ネットワーク > ウェブ プロキシ 602
自動プロキシ転送の設定 (ウェブのみ) 603
ユーザ プロキシ サーバの設定 604

動的 DNS の設定 607
ネットワーク > 動的 DNS 607
動的 DNS について 607
サポートしている動的 DNS プロバイダ 608
動的 DNS プロファイル テーブル 609
動的 DNS プロファイルの設定 610
動的 DNS プロファイルの編集 613
動的 DNS プロファイルの削除 614

AWS 資格情報の設定 615
ネットワーク > AWS 設定 615
AWS について 616
AWSの設定 616
接続のトラブルシューティング 617

SD-WAN について 620

SD-WAN グループの設定 621
SD-WAN グループ 621
SD-WAN グループの作成 622
SD-WAN グループの編集 623
SD-WAN グループの削除 623

性能監視の設定 625

性能監視について 625
性能監視の設定 627
SD-WAN 性能監視の編集 629
SD-WAN 性能監視の削除 629
特定の性能監視の削除 629
複数の性能監視の削除 629
すべての性能監視の削除 630

性能クラス オブジェクトの設定 631
性能クラス オブジェクトについて 631
性能クラス オブジェクトの設定 632
性能クラス オブジェクトの編集 633
SD-WAN 性能クラス オブジェクトの削除 634
特定の性能クラス オブジェクトの削除 634
複数の性能クラス オブジェクトの削除 634
すべての性能クラス オブジェクトの削除 635

パス選択プロファイルの設定 636
パス選択プロファイルについて 636
パス選択プロファイルの設定 638
パス選択プロファイルの編集 639
SD-WAN パス選択プロファイルの削除 639
パス選択プロファイルの削除 639
複数のパス選択プロファイルの削除 640
すべてのパス選択プロファイルの削除 640

SD-WAN ルート ポリシーの設定 641
SD-WAN ルート ポリシーについて 641
SD-WAN ルート ポリシーの設定 642
SD-WAN ルート ポリシーの編集 644
SD-WAN ルート ポリシーの削除 645
SD-WAN ルート ポリシーの削除 645
複数の SD-WAN ルート ポリシーの削除 645
すべての SD-WAN ルート ポリシーの削除 646

SD-WAN の監視 647
SD-WAN > SD-WAN 監視 647

SD-WAN ルート ポリシー接続の表示 649
SD-WAN > SD-WAN 接続ログ 649

スイッチングについて 652
スイッチングについて 652
スイッチングとは 652
スイッチングの利点 653

スイッチングの動作 654
用語集 654

VLAN トランクの設定 656
スイッチング > VLAN トランク 657
トランクについて 658
VLAN の表示 659
VLAN の編集 660
VLAN トランク ポートの追加 661
トランク ポートでの VLAN の有効化 661
VLAN トランク ポートの削除 661

レイヤ 2 発見および LLDP/LLTD の管理 663
スイッチング > ポート ミラーリング 663
L2 発見と LLDP について 664
L2 発見および LLDP/LLTD インターフェースの表示 668
LLDP プロファイルと L2 発見インターフェースの関連付け 671
ページの更新 671
LLDP のグローバルな有効化/無効化 671
近隣者の発見 672
スイッチング > ポート ミラーリング > LLDP プロファイル 673
LLDP プロファイルの表示 674
LLDP ユーザ定義プロファイルの追加 676
ユーザ定義 LLDP プロファイルの編集 677
ユーザ定義プロファイルの削除 678

リンク統合の設定 679
スイッチング > リンク統合 679
リンク統合化について 679
リンク統合の表示 682
論理リンク (LAG) の作成 683
LAG の削除 684

ポート ミラーリングの設定 685
スイッチング > ポート ミラーリング 685
ポート ミラーリングについて 686
ミラーされているポートの表示 686
ポート ミラーリング グループの設定 687
ミラーリング対象グループの有効化 688
ポート ミラーリング グループの編集 688
ポート ミラーリング グループの削除 689

シールド切り替えの設定 691
スイッチング > シールド切り替え 691

アクティブ/アクティブ クラスタリングでの高可用性について 693
高可用性 693
高可用性機能について 694
アクティブ/スタンバイ HA について 700
ステートフル同期について 701
アクティブ/アクティブ DPI HA について 703
アクティブ/スタンバイおよびアクティブ/アクティブ DPI 機能の前提条件 704
メンテナンス 707
アクティブ/アクティブ クラスタリング 709
アクティブ/アクティブ クラスタリングについて 709

高可用性の設定 726
高可用性 > 基本設定 726
アクティブ/スタンバイ高可用性機能の設定 727
動的 WAN インターフェースでの高可用性 (HA) の設定 729
アクティブ/アクティブ DPI 高可用性機能の設定 731
アクティブ/アクティブ クラスタリングの設定 733
アクティブ/アクティブ クラスタリング設定の確認 738
ネットワーク DHCP とインターフェースの設定 740
アクティブ/アクティブ クラスタリング フルメッシュ 742

高可用性の微調整 750
高可用性 > 詳細設定 750
高可用性の詳細設定 751

高可用性の監視 753
高可用性 > 監視設定 753
アクティブ/スタンバイ高可用性監視の設定 754
IPv6 高可用性監視 755

WAN 高速化の使用 758
WAN 高速化について 758
サポート対象プラットフォーム 759
伝送制御プロトコル高速化 759
Windows ファイル共有高速化 760
ウェブ キャッシュ 760
WAN 高速化サービスの配備の前提条件 761
WXA クラスタリングについて 762
WXA クラスタリングの仕組み 763
ルート ポリシーの高速化の許可 764
システム セットアップ > WAN 高速化 765
WAN 高速化の有効化 765
グループの管理 766
WXA テーブルによる WXA の管理 771
VPN ポリシーでの WXA の設定 787

SSL VPN トラフィックの高速化の設定 788
WXA のルート ポリシーの表示と編集 789
グループ接続の監視 789

VoIP について 792
VoIP について 792
VoIP とは 792
VoIP のセキュリティ 792
VoIP プロトコル 794
SonicWall の VoIP 機能 795

SonicWall VoIP 機能の設定 803
設定タスク 803
VoIP の設定 803
VoIP ログ採取の設定 810

仮想アシストの設定 812
仮想アシストについて 812
仮想アシストの柔軟性の最大化 813
仮想アシストの設定 814

オープン認証、ソーシャル ログイン、LHM の設定 820
OAuth とソーシャル ログインについて 820
OAuth およびソーシャル ログインとは 821
OAuth とソーシャル ログインのメリット 821
OAuth とソーシャル ログインの仕組み 822
サポート対象プラットフォーム 823
開発と実稼働の要件 824
ライトウェイト ホットスポット メッセージング (LHM) について 824
ソーシャル ログインのためのフェイスブックの設定 826
フェイスブック設定 827
クライアント OAuth 設定 828
ゲスト状況 (デモ) 828
オープン認証とソーシャル ログインの設定 828
ゲスト サービスの設定について 828
ソーシャル ログインの設定について 829
SonicOS でのソーシャル ログインの設定 829
ソーシャル ログイン設定の確認 836
ソーシャル ログイン、LHM、ABE の使用 837
ABE について 837
セッション ライフ サイクル 838
セッション更新 845
メッセージ形式 846
LHM RESTful API 852
よくある質問と回答 (FAQ) 853

LHM スクリプト ライブラリ 860

IPv6 979
IPv6 979
IPv6 について 979
IPv6 の設定 985
IPv6 可視化 1011
IPv6 高可用性監視 1012
IPv6 の診断と監視 1013

BGP の高度なルーティング 1014
BGP の高度なルーティング 1014
BGP について 1014
注意 1022
BGP の設定 1023
BGP 設定の確認 1033
Ipv6 BGP 1036

SonicWall サポート 1058
このドキュメントについて 1059

第 1 部

システム セットアップ | システム セットアップについて

- SonicOS システムのセットアップ について

1

SonicOS システムのセットアップについて

- 管理インターフェース SonicOS について (16 ページ)

管理インターフェース SonicOS について

ウェブ ベースの SonicOS 管理インターフェースを使用すると、SonicWall 6.5 以降が動作している SonicOS セキュリティ装置 (ファイアウォール) を設定することができます。SonicOS でサポートされる装置の詳細なリストについては、『*SonicOS 6.5 SonicOS について*』を参照してください。

SonicOS は、SonicWall セキュリティ装置を設定するために、使いやすいグラフィック形式の管理インターフェースを提供しています。動的管理インターフェースとその機能 (ツールチップや動的テーブルなど) については、『*SonicOS 6.5 SonicOS について*』を参照してください。

このガイドでは、以下の項目の設定方法について説明します。

- パスワード、ログイン セキュリティ、ウェブ管理、証明書、スケジュール
- ユーザ認証、グループ、ゲスト サービスとゲスト アカウント、パーティション
- ネットワーク設定 (インターフェース、ゾーン、ルーティングなど)
- SD-WAN
- スイッチング設定 (VLAN トランク、L2 発見、リンク統合、ポートミラーリング)
- 高可用性
- WAN 高速化
- VOIP
- 仮想アシスト

設定対象	参照
接続性: VPN、SSL VPN、SonicPoint/SonicWave、無線	*SonicOS 6.5 接続*
ポリシー: アクセス ルール、NAT ポリシー、各種オブジェクト (アドレス、動作、一致、サービス、帯域幅など)	*SonicOS 6.5 ポリシー*
ライセンス、ファームウェアの更新、システムのバックアップ/再起動	*SonicOS 6.5 更新*
監視: ダッシュボード、脅威防御、トラフィック、キャプチャ ATP	*SonicOS 6.5 監視*
セキュリティ: セキュリティ装置設定、セキュリティ サービス、アンチスパム、精密パケット検査 (DPI)	*SonicOS 6.5 セキュリティ設定*
ログとレポート: AppFlow 設定、ログ、法的設定	*SonicOS 6.5 ログとレポート*
クイック設定	*SonicOS 簡易設定*
SonicOS API	*SonicOS 6.5 SonicOS について*

第 2 部

システム セットアップ | 装置

- 基本設定の構成
- SNMP の管理
- 証明書の管理
- 時間の設定
- スケジュールの設定

2

基本設定の構成

- 「装置 | 基本設定」について (19 ページ)
  - ワンクリック無線および非無線制御モード (19 ページ)
- 装置を設定する (21 ページ)
  - ファイアウォール名の設定 (22 ページ)
  - 管理者名とパスワードの変更 (22 ページ)
  - 無線 LAN と IPv6 の有効化 (23 ページ)
  - ログイン セキュリティの設定 (24 ページ)
  - 複数管理者アクセスの設定 (29 ページ)
  - 拡張監査ログのサポートの有効化 (33 ページ)
  - 無線 LAN 制御の設定 (34 ページ)
  - 管理インターフェースの設定 (35 ページ)
  - フロントパネル管理インターフェースの設定 (SuperMassive ファイアウォールのみ) (41 ページ)
  - クライアント証明書の確認の設定 (42 ページ)
  - 証明書の期限切れの確認 (46 ページ)
  - SSH 管理の設定 (46 ページ)
  - SonicOS API の有効化 (47 ページ)
  - より高度な管理オプションの設定 (47 ページ)
  - SonicPoint イメージの手動ダウンロード (50 ページ)
  - 言語の選択 (51 ページ)

「装置 | 基本設定」について

「**管理 | システム セットアップ > 装置 | 基本設定**」には、安全なリモート管理が実現されるようにSonicWall セキュリティ装置を構成する設定があります。

ファイアウォールは、HTTPS、SNMP、SonicWall グローバル管理システム (SonicWall GMS) など、さまざまな方法を使用して管理できます。

メモ：SonicWall 装置に対する変更を適用するには、「**適用**」を選択します。更新を確認するメッセージがブラウザ ウィンドウの一番下に表示されます。

ワンクリック無線および非無線制御モード

重要：無線制御モードを変更するときは、「**管理 | システム セットアップ > 装置 > 基本設定**」ページで「**承諾**」を選択した後にファイアウォールを再起動する必要があります。

SonicOS 6.5 は、ファイアウォールが安全な無線アクセスを提供するためだけに使用されている展開のために無線制御モードを導入します。あるいは、ファイアウォールが無線アクセスを提供しないような展開には、非無線制御モードを選択できます。無線および無線以外の機能をすべて許可する通常の全機能ゲートウェイ モードが既定です。

この機能により、次のいずれかが可能になります。

- 無線制御モードを有効にします。これは次を無効にして編集不可にします:
  - SSL VPN および VPN ゾーン。
  - グループ VPN および SSL VPN ポリシー、およびこれらのポリシーを使用したすべてのゾーンの更新。
  - VPN。
  - WAN 高速化 (WXA)。
  - SIP および H.323 変換。
- 非無線制御モードを有効にします。これは次を無効にして編集不可にします:
  - 既定の WLAN ゾーンを含む無線ゾーン (無線ゾーンの作成も無効にする)。
  - 内部無線機能。
  - L2 および L3 を含むアクセス ポイント。

新しいセクション (「**無線制御**」) が「**管理 | システム セットアップ > 装置 | 基本設定**」ページに追加されました。

トピック:

- 非無線制御モードを有効にした場合の影響
- 無線制御モードを有効にした場合の影響
- 無線制御モードを有効にする
- 非無線制御モードを有効にする
- 通常のファイアウォール モードを有効にする

非無線制御モードを有効にした場合の影響

非無線モードを有効にすると、いくつかの管理インターフェース ページに影響します。

- 無線ゾーンの「**編集**」および「**削除**」アイコンが、「**管理 | システム セットアップ > ネットワーク > ゾーン**」ページで淡色表示になります。
- アクセス ポイント オブジェクトの状況が、「**管理 | 接続性 > アクセス ポイント > 基本設定**」ページで**無効**になります。
- 内部無線ゾーンは無効になっています。
- アクセス ポイントまたは内部無線を有効にする試みは拒否されます。

無線制御モードを有効にした場合の影響

無線制御モードを有効にすると、いくつかの管理インターフェース ページが影響を受けます。これらのページで機能を有効にしたり設定したりする試みは拒否されます。

- VPN および SSL VPN ゾーンの「**編集**」および「**削除**」アイコンが、「**管理 | システム セットアップ > ネットワーク > ゾーン**」ページで淡色表示になります。
- 「**管理 | 接続性 > VPN > 基本設定**」ページに示すように、VPN は無効になっています。

- SSL VPN へのすべてのインターフェースは、「**管理 | 接続性 > SSL VPN > サーバ設定**」ページで無効になっています。
- 「**管理 | システム セットアップ > VOIP**」で SIP または H.323 オプションを有効にしようとすると、ブラウザ ウィンドウの右下隅にエラー メッセージが表示されます。

  「**リストの表示**」リンクをクリックすると、エラー ログが表示されます。
- WXA は無効として表示されます。
- VPN または SSL VPN、あるいはその両方でゾーンを有効にしようとすると、エラーになります。

装置を設定する

トピック:

- 「装置 | 基本設定」ページへのアクセス (21 ページ)
- ファイアウォール名の設定 (22 ページ)
- 管理者名とパスワードの変更 (22 ページ)
- 無線 LAN と IPv6 の有効化 (23 ページ)
- ログイン セキュリティの設定 (24 ページ)
- 複数管理者アクセスの設定 (29 ページ)
- 拡張監査ログのサポートの有効化 (33 ページ)
- 無線 LAN 制御の設定 (34 ページ)
- 管理インターフェースの設定 (35 ページ)
- フロントパネル管理インターフェースの設定 (SuperMassive ファイアウォールのみ) (41 ページ)
- クライアント証明書の確認の設定 (42 ページ)
- 証明書の期限切れの確認 (46 ページ)
- SSH 管理の設定 (46 ページ)
- SonicOS API の有効化 (47 ページ)
- より高度な管理オプションの設定 (47 ページ)
- SonicPoint イメージの手動ダウンロード (50 ページ)
- 言語の選択 (51 ページ)

「装置 | 基本設定」ページへのアクセス

「装置 | 基本設定」ページへのアクセス

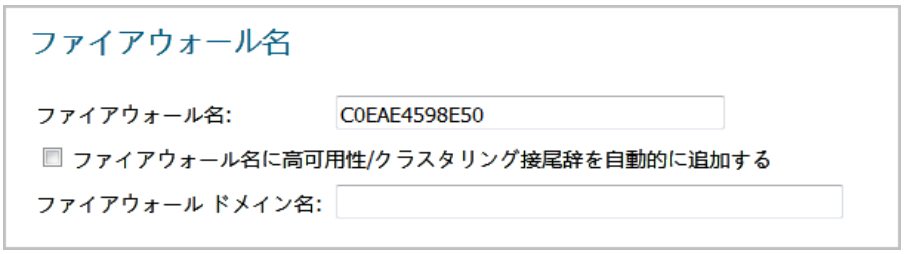
1. 「**管理 | システム セットアップ > 装置**」に移動して、ナビゲーション ペインを展開します。
2. 「**基本設定**」を選択します。

ファイアウォール名の設定

ファイアウォール名を設定するには:

1 「**管理 | システム セットアップ > 装置 > 基本設定**」に移動します。

2 「**ファイアウォール名**」セクションまでスクロールします。



3 「**ファイアウォール名**」フィールドに、ファイアウォールの 16 進数のシリアル番号を入力します。この番号は SonicWall セキュリティ装置を一意に識別します。既定の番号はファイアウォールのシリアル番号です。シリアル番号は SonicWall セキュリティ装置の MAC アドレスでもあります。**ファイアウォール名**を変更するには、「**ファイアウォール名**」フィールドに英数字で一意の名前を入力します。名前は 8 文字以上の長さにする必要があり、最大 63 文字まで使用できます。

4 イベント ログでプライマリ/セカンダリ ファイアウォールを識別しやすくするには、「**ファイアウォール名に高可用性/クラスタリング接尾辞を自動的に追加する**」をオンにします。このオプションをオンにすると、「**管理 | 調査 > ログ > イベント ログ**」でファイアウォール名の後に適切な接尾辞が自動的に追加されます。

- **プライマリ**
- **セカンダリ**
- **プライマリ ノード** <*ノード番号*>
- **セカンダリ ノード** <*ノード番号*>

このオプションは、既定では選択されていません。イベント ログの詳細については、『*SonicOS 6.5 調査*』を参照してください。

5 「**ファイアウォール ドメイン名**」フィールドにわかりやすい名前を入力します。この名前には、プライベートな名前 (内部ユーザ向け) を指定することも、外部登録されたドメイン名を指定することもできます。このドメイン名を「**システム セットアップ > ユーザ > 設定**」ビューの「**ユーザ ウェブ ログインの設定**」と共に用いてユーザ認証のリダイレクトが行われます。ユーザ ウェブ ログインの設定の詳細については、「ユーザ ウェブ ログインの設定 (133 ページ)」を参照してください。

管理者名とパスワードの変更

各 SonicWall セキュリティ装置には、初期段階で既定の管理者名 `admin` とパスワード `password` が設定されています。「**初期セットアップ ガイド**」、「**スタートアップ ガイド**」、または「**セットアップ簡易設定ガイド**」でパスワードを変更しなかった場合は、今すぐパスワードを変更することを強くお勧めします。

管理者の名前やパスワードを変更するには:

1 「**管理 | システム セットアップ > 装置 > 基本設定**」に移動します。

2 「**管理者名とパスワード**」までスクロールします。

3 「**管理者名**」フィールドに新しい名前を入力します。**管理者名**は、既定で「**admin**」に設定されますが、32 文字までの英数字を使用して変更できます。1 文字以上の長さにする必要があります。

4 「**適用**」を選択します。

SonicWall 管理インターフェースにアクセスするための新しいパスワードを設定するには:

1 「**古いパスワード**」フィールドに古いパスワードを入力します。以前のパスワードは「**古いパスワード**」フィールドに暗号化されて表示されます。

2 「**新しいパスワード**」フィールドに新しいパスワードを入力します。新しいパスワードは最大 32 文字の英数字および特殊文字にします。

> **重要**：既定のパスワード (**password**) は、独自の個別パスワードに変更することを推奨します。他人が簡単に推測できない強力なパスワードを入力してください。強力なパスワードは、英字の大文字、小文字、数字、特殊文字をそれぞれ少なくとも 1 文字含めて作成してください。例えば、`MyP@ssw0rd` と入力します。

3 「**パスワードの確認**」フィールドにもう一度新しいパスワードを入力します。

4 ワンタイム パスワード方式の使用を強制するには、ドロップダウンから TOTP を選択します。古いパスワードを再利用できるようにするには、この機能を無効のままにします。

5 「**適用**」を選択します。

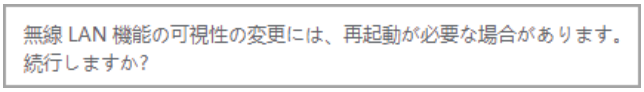
無線 LAN と IPv6 の有効化

無線 LAN や IPv6 の可視性を有効にするには:

1 「**管理 | システム セットアップ > 装置 > 基本設定**」に移動します。

2 「**機能可視性**」までスクロールします。

3 「**無線 LAN を有効にする**」および/または「**IPv6 を有効にする**」を選択します。これらのオプションは、既定ではオンになっています。確認メッセージが表示されます。



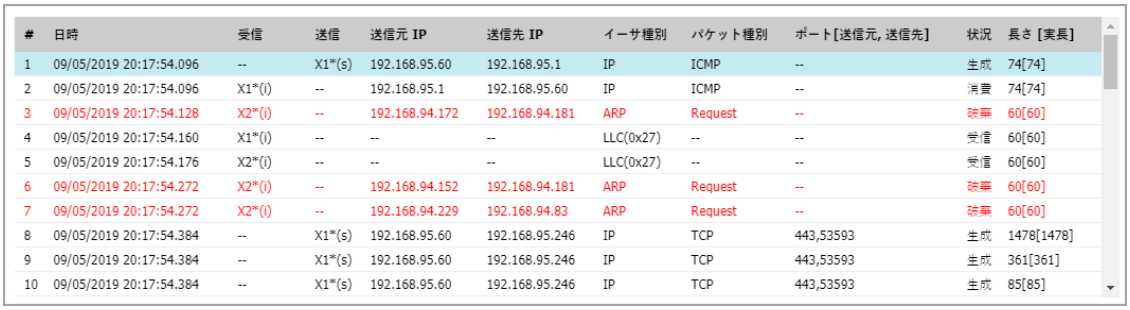
重要：無線 LAN 機能を有効または無効にするには、ファイアウォールを再起動する必要があります。

これらのオプションのいずれか、または両方を選択すると、それらの機能が使用できるようになり、「**監視 | 現在の状況 > システム状況**」ページに表示されます。オプションを選択しなかった場合は、「**システム状況**」ページにはそれらが無効化されていると表示されます。

WLAN が無効である場合:

- アクセス ポイントおよび無線に関連する管理インターフェースのすべてのページは表示されません。
- WLAN はゾーン種別として表示されません。
- 既存の WLAN ゾーンまたはオブジェクトは編集できなくなります。

IPv6 が無効である場合は、すべての IPv6 パケットがファイアウォールによって破棄され、「**調査 | ツール > パケット監視**」ページにログ メッセージが表示されます。



#	日時	受信	送信	送信元 IP	送信先 IP	イーサ種別	パケット種別	ポート[送信元, 送信先]	状況	長さ [実長]
1	09/05/2019 20:17:54.096	--	X1*(s)	192.168.95.60	192.168.95.1	IP	ICMP	--	生成	74[74]
2	09/05/2019 20:17:54.096	X1*(i)	--	192.168.95.1	192.168.95.60	IP	ICMP	--	消費	74[74]
3	09/05/2019 20:17:54.128	X2*(i)	--	192.168.94.172	192.168.94.181	ARP	Request	--	破棄	60[60]
4	09/05/2019 20:17:54.160	X1*(i)	--	--	--	LLC(0x27)	--	--	受信	60[60]
5	09/05/2019 20:17:54.176	X2*(i)	--	--	--	LLC(0x27)	--	--	受信	60[60]
6	09/05/2019 20:17:54.272	X2*(i)	--	192.168.94.152	192.168.94.181	ARP	Request	--	破棄	60[60]
7	09/05/2019 20:17:54.272	X2*(i)	--	192.168.94.229	192.168.94.83	ARP	Request	--	破棄	60[60]
8	09/05/2019 20:17:54.384	--	X1*(s)	192.168.95.60	192.168.95.246	IP	TCP	443,53593	生成	1478[1478]
9	09/05/2019 20:17:54.384	--	X1*(s)	192.168.95.60	192.168.95.246	IP	TCP	443,53593	生成	361[361]
10	09/05/2019 20:17:54.384	--	X1*(s)	192.168.95.60	192.168.95.246	IP	TCP	443,53593	生成	85[85]

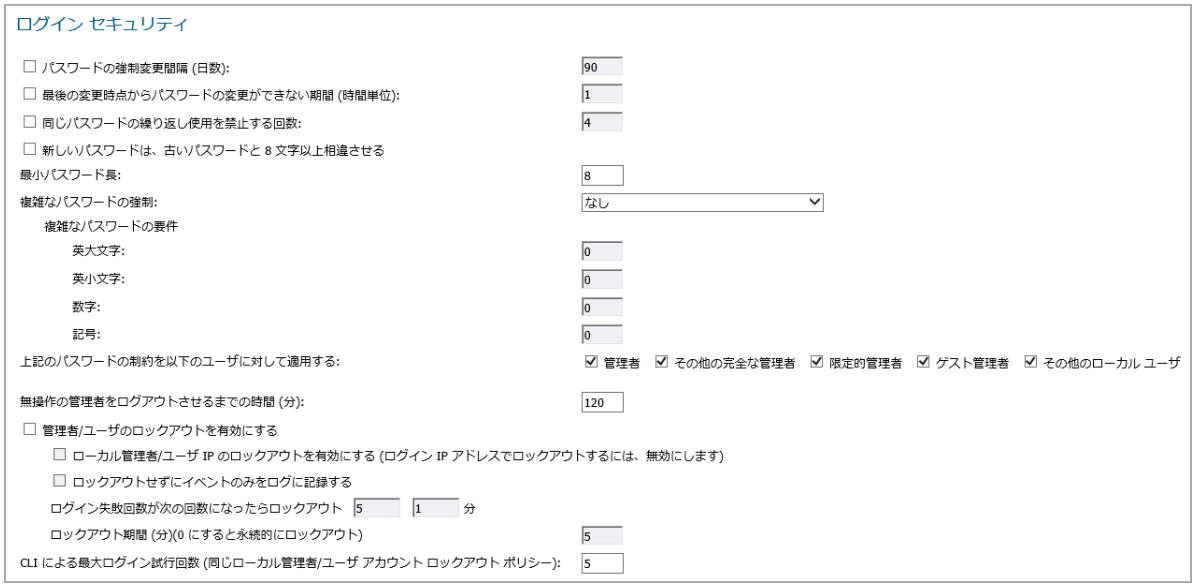
4 「**OK**」を選択します。

ログイン セキュリティの設定

内部 SonicOS ウェブ サーバでは、HTTPS 管理セッションとネゴシエートする場合に、TLS 1.1 以降を強力な暗号 (128 ビット以上) と組み合わせて使うことができます。SSL の実装はサポートされていません。この強化された HTTPS セキュリティにより、潜在的な SSLv2 ロールバックの脆弱性を防御し、PCI (Payment Card Industry) をはじめとするセキュリティおよびリスク管理の標準規格に確実に準拠します。

ヒント：SonicOS は、最新のブラウザがサポートする HTML5 などの先端のブラウザ技術を利用しています。SonicOS の管理には、最新バージョンの Chrome、Firefox、Internet Explorer、または Safari (Windows プラットフォームは対象外) の各ブラウザを使用してください。SonicWall システムの管理には、モバイル機器のブラウザは推奨されません。

SonicOS では、パスワードの制約の強制を設定できます。これによって、管理者およびユーザが必ず安全性の高いパスワードを使用するように設定できます。このパスワードの制約の強制により、現在の情報セキュリティ管理システムで定義されている機密保持の要件、および情報セキュリティ国際評価基準や PCI (Payment Card Industry) などの標準に準拠するための要件を満たすことができます。



トピック:

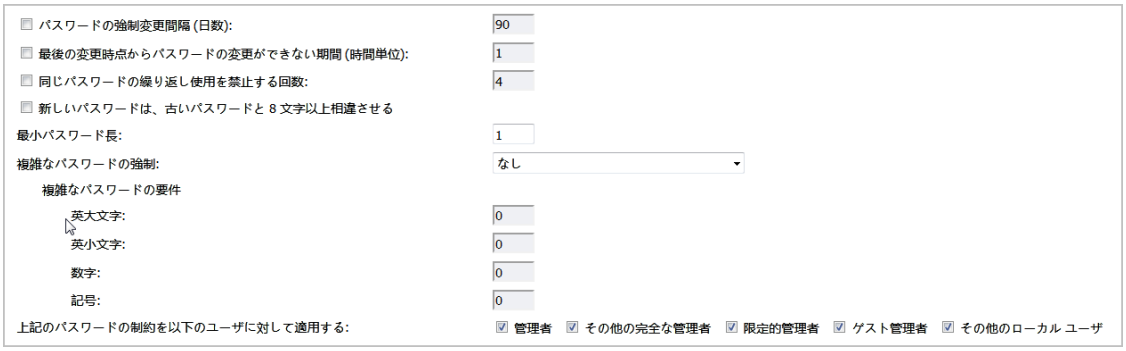
- パスワードの準拠の設定 (25 ページ)
- ログイン制約の設定 (27 ページ)

パスワードの準拠の設定

パスワードの準拠を設定するには:

1 「**管理 | システム セットアップ > 装置 > 基本設定**」に移動します。

2 「**ログイン セキュリティ**」までスクロールします。



3 指定した日数が経過するたびにパスワードを変更するようユーザに義務付けるには:

a 「**パスワードの強制変更間隔 (日数)**」をオンにします。フィールドが有効になります。このオプションは、既定では選択されていません。

b フィールドに日数を入力します。既定の日数は **90**、最小値は 1 日、最大値は 9999 です。

有効期限の切れたパスワードでログインしようとすると、新しいパスワードの入力を求めるポップアップ ウィンドウが表示されます。「**ユーザ ログイン状況**」ウィンドウには、ユーザがいつでもパスワードを変更できるように「**パスワードの変更**」が用意されています。

4 パスワードを変更してから次に変更するまでの最短の期間を時間単位で指定するには:

a 「**最後の変更時点からパスワードの変更ができない期間 (時間単位)**」をオンにします。フィールドが有効になります。このオプションは、既定では選択されていません。

b 時間数を入力します。最小 (既定値) は **1** 時間、最大は 9999 時間です。

5 指定したパスワード変更回数の範囲で重複しないパスワードを使用するようユーザに義務付けるには:

a 「**同じパスワードの繰り返し使用を禁止する回数**」をオンにします。フィールドが有効になります。このオプションは、既定では選択されていません。

b 変更回数を入力します。既定は **4** 回、最小は 1 回、最大は 32 回です。

6 新しいパスワードを作成するときに、古いパスワードで使用していたアルファベット、数字、記号の 8 文字以上を変えるようユーザに義務付けるには、「**新しいパスワードは、古いパスワードと 8 文字以上相違させる**」をオンにします。使用できる文字を指定する方法については、「ステップ 8」を参照してください。

7 パスワードに使用できる最小の長さを指定するには、「**最小パスワード長**」フィールドに最小文字数を指定します。既定値は **8**、最小値は 1、最大値は 99 です。

8 「**複雑なパスワードの強制**」ドロップダウン メニューから、ユーザのパスワードに要求される複雑さの度合いを選択します。

- **なし** (既定)
- **アルファベットと数字を必ず併用**
- **アルファベット、数字、記号を必ず併用** - 記号は **!**、**@**、**#**、**$**、**%**、**^**、**&**、*****、**(**、および **)** のみを使用できます。それ以外は使用できません。

9 複雑なパスワードの強制オプションとして「**なし**」以外を選択すると、「**複雑なパスワードの要件**」の下のオプションが選択可能になります。パスワードで使用する必要があるアルファベット、数字、記号の最小文字数を入力します。既定の文字数はそれぞれ **0** です。すべてのオプションの文字数の合計は 99 文字以内にする必要があります。

- **英大文字**
- **英小文字**
- **数字**
- **記号**

> **メモ**:「**記号**」フィールドは、「**アルファベット、数字、記号を必ず併用**」を選択した場合のみ有効になります。

10 「**上記のパスワードの制約を以下のユーザに対して適用する**」で、パスワードの制約を適用するユーザのクラスを選択します。既定では、すべてのオプションが選択されています。

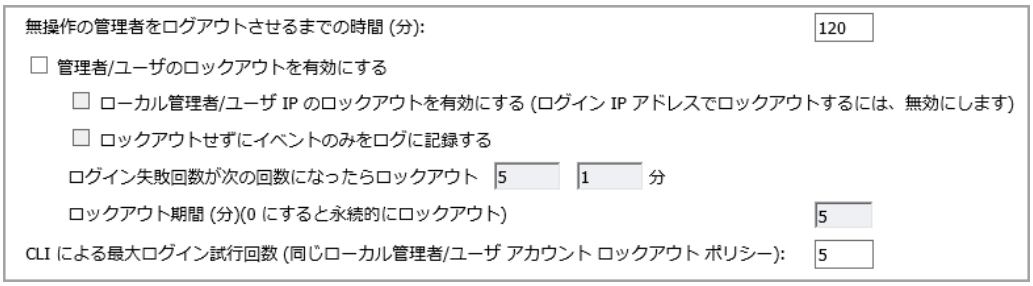
- **管理者** - **admin** というユーザ名の既定の管理者です。
- **その他の完全な管理者**
- **限定的管理者**
- **ゲスト管理者**
- **その他のローカル ユーザ**

ログイン制約の設定

ログイン制約を設定するには:

1 「**管理 | システム セットアップ > 装置 > 基本設定**」に移動します。

2 「**ログイン セキュリティ**」までスクロールします。



3 無操作時に管理者が管理インターフェースから自動的にログアウトさせられるまでの時間を指定するには、「**無操作の管理者をログアウトさせるまでの時間 (分)**」フィールドに分単位で時間を入力します。既定では、無動作時間が **5** 分経過すると管理者はログアウトさせられます。タイムアウトは 1～9999 分の範囲に指定できます。

> **ヒント：**「無操作の管理者をログアウトさせるまでの時間 (分)」に 5 分を超える時間を設定した場合、ファイアウォールの管理インターフェースへの不正アクセスを防ぐため、各管理セッションを終了するときに必ずビューの右上の「**ログアウト**」を選択してください。

4 ログイン資格情報が正しくない場合に管理者またはユーザをロックアウトするよう SonicWall セキュリティ装置を設定するには、「**管理者/ユーザのロックアウトを有効にする**」を選択します。指定した回数の不正なログイン試行が行われた場合、管理者とユーザの両方がロックアウトされ、ファイアウォールにアクセスできなくなります。このオプションは、既定では無効になっています。このオプションを有効にすると、以下のフィールドが有効になります。

> **注意：管理者とユーザが同じ送信元 IP アドレスを使用してファイアウォールにログインしようとすると、管理者もファイアウォールからロックアウトされます。ロックアウトは、ユーザまたは管理者の送信元 IP アドレスに基づいています。**

a 「**ローカル管理者/ユーザ IP のロックアウトを有効にする (ログイン IP アドレスでロックアウトするには、無効にします)**」を選択します。このオプションは、所定の回数を超える不正なログイン試行を受けた場合に、ユーザ アカウントと IP アドレスをロックアウトします。このオプションは、「**管理者/ユーザのロックアウトを有効にする**」が選択されている場合にのみ使用できます。

b SonicOS の「**ロックアウトせずにイベントのみをログに記録する**」を選択します。この場合、失敗したユーザ ログイン試行で一定のしきい値に達したものが記録されますが、ユーザまたは IP アドレスはロックアウトされません。このオプションは、「**管理者/ユーザのロックアウトを有効にする**」が選択されている場合にのみ使用できます。

ユーザまたは IP アドレスがロックアウトされると、「ユーザ ログインが拒否されました - ユーザはロックアウトされています」というメッセージがログイン画面に表示され、ログインが拒否されます。

メモ：「ローカル管理者/ユーザ IP のロックアウトを有効にする (ログイン IP アドレスでロックアウトするには、無効にします)」チェックボックスがオンのときは、**「監視 | 現在の状況 | ユーザ セッション > 使用中のユーザ」**ページで、ロックアウトされたすべてのユーザ アカウントを確認し、編集することができます。

c **「ログイン失敗回数が次の回数になったらロックアウト」**の 1 つ目のフィールドに、ユーザをロックアウトするまでの指定時間内のログイン失敗回数を入力します。既定値は **5**、最小値は 1、最大値は 99 です。

d 失敗回数の最大時間を入力します。既定値は **5** 分、最小値は 1 分、最大値は 240 分 (4 時間) です。

e **「ロックアウト期間 (分)」**フィールドに、ロックアウトされたユーザがファイアウォールに再度ログインできるようになるまでの時間を入力します。既定値は **5** 分、最小値は 0 分 (無期限のロックアウト)、最大値は 60 分です。

5 **「CLI による最大ログイン試行回数」**フィールドに、コマンド ライン インターフェース (CLI) からのログインが何回失敗したらロックアウトするかを指定します。既定値は **5**、最小値は 3、最大値は 15 です。

6 **「適用」**を選択します。

ロックアウトされたユーザ アカウント

SonicOS は、「未認証ユーザ」レコードを保持しています。これは未認証のユーザ アカウントまたは IP アドレスがこれまでにどれだけロックアウトされたかを示します。**「ローカル管理者/ユーザ IP のロックアウトを有効にする (ログイン IP アドレスでロックアウトするには、無効にします)」**機能は、ユーザまたは管理者の認証/ログインが失敗したときに、認証されていないユーザと IP アドレスをロックアウトすることを目的としています。**「監視 | 現在の状況 | ユーザ セッション > 使用中のユーザ」**ページで、そのレコードを確認してください。

未認証ユーザ アカウントのロック解除

ロックされたユーザ アカウントのロックを解除するには、次の 3 つの方法があります。

- **ロックアウト タイマー** - この方法は、所定の待機期間が経過したとき、未認証アカウントを自動的にロック解除します。

- **GUI ロック解除** - この方法では、管理者が「**監視 | 現在の状況 | ユーザ セッション > 使用中のユーザ**」ページの「**ロック解除**」アイコンを選択して未認証ユーザを手動でロック解除する必要があります。
- **チェックボックスで無効化** -「**ローカル管理者/ユーザ IP のロックアウトを有効にする (ログイン IP アドレスでロックアウトするには、無効にします)**」チェックボックスをオフにすると、すべての未認証ユーザがロック解除されます (ただし、「永久」とマークされた特定のユーザは除く)。その特定の未認証ユーザのロックアウト期間が有限な時間 (分) である場合、このオプションをオフにしてもそのユーザはロック解除されません。

複数管理者アクセスの設定

SonicOS は、完全な管理者権限、読み取り専用権限、制限付きの権限を持つ複数の管理者による同時アクセスをサポートします。

トピック:

- 複数管理者サポートについて (29 ページ)
- 複数管理者アクセスの設定 (32 ページ)

複数管理者サポートについて

トピック:

- 複数管理者サポートとは (29 ページ)
- メリット (29 ページ)
- 複数管理者サポートの動作 (30 ページ)

複数管理者サポートとは

これまでのバージョンの SonicOS は、完全な管理者権限でファイアウォールにログオンできる管理者は 1 人だけでした。他のユーザに "制限付き管理者" のアクセス権を付与することはできますが、SonicOS GUI のあらゆる領域を変更できる完全なアクセス権を複数の管理者が同時に持つことはできません。

SonicOS では、複数管理者の同時アクセスがサポートされています。この機能により、複数のユーザが完全な管理者権限でログインできるようになりました。既定の **admin** ユーザ名に加え、他の管理者ユーザ名を作成できます。

複数の管理者が同時に設定を変更することによって競合が生じる可能性もあるため、設定の変更は 1 人の管理者にのみ許可されています。その他の管理者には GUI に対する完全なアクセス権が付与されますが、設定を変更することはできません。

メリット

複数管理者サポートには、次のようなメリットがあります。

生産性の向上	ファイアウォールに対して複数の管理者が同時にアクセスできるため、装置に対して 2 人の管理者が同時にアクセスした場合に一方の管理者が自動的にシステムからログアウトされる "自動ログアウト" が不要になります。
設定リスクの軽減	新たに読み取り専用モードが追加されたため、意図しない設定変更を誤って実行してしまうリスクなしに、ファイアウォールの現在の設定と状況を確認することができます。

複数管理者サポートの動作

トピック:

- 設定モード (30 ページ)
- ユーザ グループ (31 ページ)
- 管理者の先制時に適用される優先順位 (32 ページ)
- GMS と複数管理者サポート (32 ページ)

設定モード

複数の管理者による同時アクセスを許可しつつ、複数の管理者が同時に設定を変更することによって競合が生じることがないように、次の設定モードが定義されています。

「設定」モード	管理者に設定を編集するための完全な権限が割り当てられます。装置にログインしている管理者がいない場合、完全な管理者権限および制限付き管理者権限を持った (読み取り専用管理者以外の) 管理者には自動的に設定モードが適用されます。 **メモ：** 完全な設定権限を持つ管理者は、コマンド ライン インターフェース (CLI、『*SonicOS 6.5 CLI リファレンス ガイド*』を参照) を使ってログインすることもできます。
読み取り専用モード	管理者は設定に変更を加えることは一切できませんが、管理 UI 全体を表示することや、監視操作を実行することはできます。 **SonicWall 読取専用管理者**ユーザ グループに属する管理者には読み取り専用アクセス権が付与され、他の設定モードにはアクセスできません。
非設定モード	管理者は、読み取り専用グループと同じ情報を閲覧できるほか、設定の競合を引き起こすおそれのない管理操作を実行できます。 非設定モードにアクセスできるのは、**SonicWall 管理者**ユーザ グループに属する管理者だけです。既に設定モードを利用している管理者が存在するとき、新しい管理者が既存の管理者を先制しなかった場合は、このモードになります。既定では、設定モードを先制された管理者は、非設定モードに切り替わります。「**システム設定 > 管理**」ページでこの動作を変更して、元の管理者がログアウトされるようにすることもできます。

「各種設定モードにおいて利用可能なアクセス権」テーブルは、各設定モードで利用できるアクセス権をまとめたものです。なお、この表には制限付き管理者のアクセス権も記載されていますが、制限付き管理者が利用できる機能の一部が含まれていません。

各種設定モードにおいて利用可能なアクセス権

機能	設定モードでの完全な管理者権限	非設定モードでの完全な管理者権限	読み取り専用管理者	制限付き管理者
証明書のインポート	X			
証明書署名リクエストの生成	X			
証明書のエクスポート	X			
装置の設定のエクスポート	X	X	X	
TSR のダウンロード	X	X	X	
その他の診断の使用	X	X		X
ネットワーク設定	X			X
ARP キャッシュの消去	X	X		X
DHCP サーバの設定	X			
VPN トンネルの再ネゴシエート	X	X		
ユーザのログオフ	X	X		X ゲスト ユーザのみ
ロックアウトされたユーザのロック解除	X	X		
ログの消去	X	X		X
ログのフィルタ	X	X	X	X
ログのエクスポート	X	X	X	X
ログの電子メール送信	X	X		X
ログ種別の設定	X	X		X
ログ設定	X			X
ログ レポートの生成	X	X		X
完全な UI の参照	X	X	X	
ログ レポートの生成	X	X		X

ユーザ グループ

複数管理者サポート機能では、次の 2 つの既定ユーザ グループをサポートしています。

SonicWall 管理者	このグループのメンバーには、設定を編集するための完全な管理者アクセス権が付与されます。
SonicWall 読み取り専用管理者	このグループのメンバーには、完全な管理インターフェースを閲覧できる読み取り専用アクセス権が付与されます。設定を編集したり、完全な設定モードに切り替えることはできません。

これらの複数のユーザ グループにユーザを追加することはお勧めできません。ただし、そのようにした場合は、次の動作が適用されます。

所属ユーザ グループ	自身の一部
SonicWall管理者	**制限付き管理者**ユーザ グループまたは **SonicWall 読み取り専用管理者**ユーザ グループにも追加した場合、メンバーには完全な管理者権限が付与されます。
制限付き管理者	**SonicWall 読み取り専用管理者**ユーザ グループに追加した場合、メンバーには制限付き管理者権限が付与されます。
読み取り専用管理者	その後、別の管理グループに所属させた場合、**SonicWall 読み取り専用管理者**グループ設定の「**この読み取り専用管理者が他の管理グループと共に使用された場合**」のオプション次第で、メンバーのアクセスが前と同じく読み取り専用に制限されるか、もう一方のグループで設定された完全な管理者権限が付与されます。

管理者の先制時に適用される優先順位

既に装置にログインしている管理者を先制する場合、各種の管理者区分には、次の規則に従って優先順位が適用されます。

1. **admin** ユーザおよび SonicWall グローバル管理システム (GMS) には、どちらも最も高い優先順位が適用され、すべてのユーザを先制できます。
2. **SonicWall 管理者** ユーザ グループに所属するユーザは、**admin**、SonicWall GMS を除くすべてのユーザを先制できます。
3. **制限付き管理者**ユーザ グループに所属するユーザは、**制限付き管理者**グループの他のメンバーのみを先制できます。

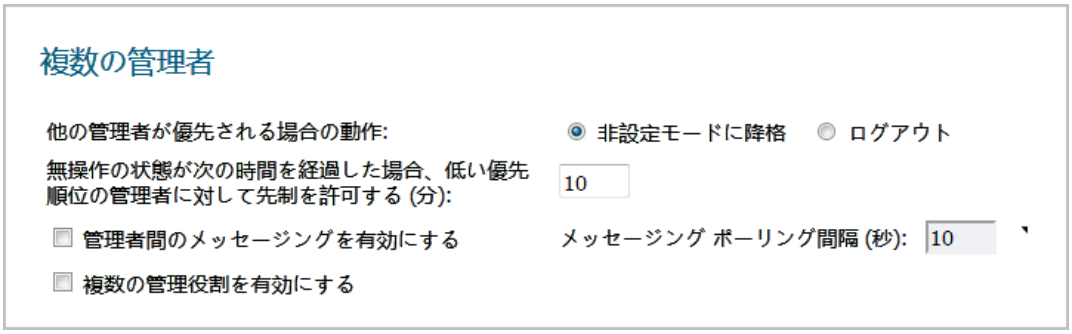
GMS と複数管理者サポート

SonicWall GMS を使用してファイアウォールを管理している場合、GMS は各種のアクティビティ (GMS 管理の IPSec トンネルが正しく作成されたかどうかを確認するなど) を行う関係上、装置にログインする機会が多くなります。GMS はローカル管理者を先制できるため、このような GMS ログインが頻繁に生じることで、装置のローカル管理が困難になる場合があります。

複数管理者アクセスの設定

複数管理者アクセスを設定するには:

1. 「**管理 | システム セットアップ > 装置 > 基本設定**」に移動します。
2. 「**複数の管理者**」までスクロールします。



3 ある管理者が他の管理者を先制した場合の対応を設定するには、「**他の管理者が優先される場合の動作**」オプションで、先制された管理者を非設定モードに変換するか、ログアウトさせるかを選択します。

動作	選択
他の管理者によるアクセスを遮断することなく、複数の管理者が非設定モードで装置にアクセスできるようにします。このオプションは、既定では選択されていません。	**非設定モードに降格**
新しい管理者が他のセッションを先制します。 **メモ：**「**ログアウト**」を選択すると非設定モードは無効になり、非設定モードに手動で入ることはできなくなります。	**ログアウト**

4 指定した時間の経過後に、優先順位の低い管理者が現在の管理者を先制できるようにするには、「**無操作の状態が次の時間を経過した場合、低い優先順位の管理者に対して先制を許可する (分)**」フィールドに時間を分で入力します。既定値は **10** 分、最小値は 1 分、最大値は 9999 分です。

5 SonicOS 管理インターフェースは、管理者が管理インターフェースを通じて、同じ装置にログインしている他の管理者にテキスト メッセージを送信できるようにします。メッセージはブラウザのステータス バーに表示されます。このオプションは、既定では選択されていません。このオプションを有効にするには、以下の手順に従います。

   a 「**管理者間のメッセージングを有効にする**」を選択します。「**メッセージング ポーリング間隔 (秒)**」フィールドが有効になります。

   b 「**メッセージング ポーリング間隔 (秒)**」フィールドに、管理者間で送られるメッセージをブラウザがチェックする頻度を指定します。この間隔を適度に短く設定してメッセージの受け渡しがタイミングよく行われるようにしてください。特に、多数の管理者が装置にアクセスする必要があると考えられる場合は、この設定に注意してください。既定値は **10** 秒、最小値は 1 秒、最大値は 99 秒です。

6 システム管理者、暗号化管理者、監査管理者によるアクセスを有効にするには、「**複数の管理役割を有効にする**」を選択します。このオプションが無効なとき、これらの管理者はシステムおよび関連するどのユーザ グループにもアクセスできず、それらに関する情報が非表示とされます。このオプションは、既定では選択されていません。

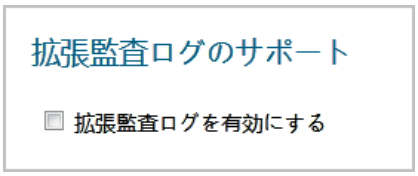
拡張監査ログのサポートの有効化

拡張ログ エントリには、「**調査 | ログ > イベント ログ**」ページの変更されたパラメータとユーザ名が含まれます。ログの詳細については、『*SonicOS 6.5 調査*』を参照してください。

「調査 | ログ> イベント ログ」ページのすべての設定変更がログに記録されるようにするには:

1 「**管理 | システム セットアップ > 装置 | 基本設定**」に移動します。

2 「**拡張監査ログのサポート**」までスクロールします。



3 「**拡張監査ログを有効にする**」を選択します。このオプションは、既定では選択されていません。

4 「**適用**」を選択します。

無線 LAN 制御の設定

無線 LAN 制御は、次のいずれかの方法で設定できます。

- 全機能ゲートウェイ (既定)
- 無線なし
- 無線制御専用

これらのモードの詳細については、「ワンクリック無線および非無線制御モード (19 ページ)」を参照してください。

トピック:

- 通常のファイアウォール モードを有効にする (34 ページ)
- 無線制御モードを有効にする (34 ページ)
- 無線制御モードを有効にする (34 ページ)

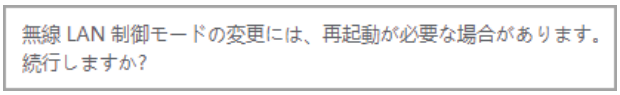
通常のファイアウォール モードを有効にする

通常のファイアウォール モードを有効にするには:

ⓘ **重要**：無線制御のモードを変更した後、ファイアウォールを再起動する必要があります。

1. 「**管理 | システム セットアップ > 装置 > 基本設定**」に移動します。
2. 「**無線 LAN 制御**」までスクロールします。

3. 「**無線制御モード**」から、「**全機能ゲートウェイ**」を選択します。次の警告メッセージが表示されます。



4. 「**OK**」を選択します。
5. 「**適用**」を選択します。

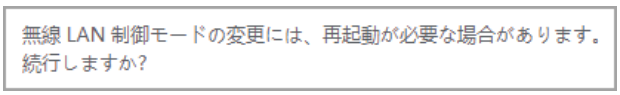
無線制御モードを有効にする

無線制御モードを有効にするには:

ⓘ **重要**：無線制御のモードを変更した後、ファイアウォールを再起動する必要があります。

1. 「**管理 | システム セットアップ > 装置 > 基本設定**」に移動します。
2. 「**無線 LAN 制御**」までスクロールします。

3 「**無線制御モード**」から、「**無線制御専用**」を選択します。次の警告メッセージが表示されます。



4 「**OK**」を選択します。

5 「**適用**」を選択します。

非無線制御モードを有効にする

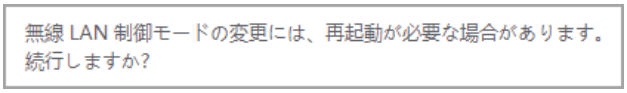
非無線制御モードを有効にするには:

重要：無線制御のモードを変更した後、ファイアウォールを再起動する必要があります。

1 「**管理 | システム セットアップ > 装置 > 基本設定**」に移動します。

2 「**無線 LAN 制御**」までスクロールします。

3 「**無線制御モード**」から、「**無線なし**」を選択します。次の警告メッセージが表示されます。



4 「**OK**」を選択します。

5 「**適用**」を選択します。

メモ：無線ゾーンの「**編集**」および「**削除**」アイコンが、「**管理 | システム セットアップ > ネットワーク > ゾーン**」および「**管理 | 接続性 > アクセス ポイント > 基本設定**」ページで淡色表示になります。

管理インターフェースの設定

このセクションでは、以下を設定します。

- 管理インターフェースのテーブルを表示する方法。
- 証明書の使用方法。
- 開始ページとして表示するページ。
- 設定モードと非設定モードのどちらで操作するか。

- ツールチップの動作。
- その他の管理オプション。

トピック:

- HTTP/HTTPS を介した管理 (36 ページ)
- ブラウザ Cookie の削除 (37 ページ)
- 設定モードの切り替え (38 ページ)
- 設定モードの切り替え (38 ページ)
- 管理インターフェースのテーブルの制御 (39 ページ)
- 開始ページの指定 (40 ページ)
- ツールチップの管理 (40 ページ)
- TLS のバージョンの強制 (41 ページ)

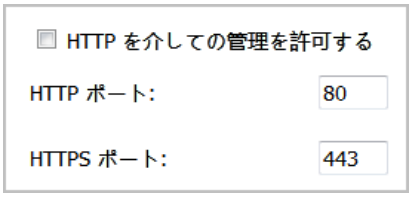
HTTP/HTTPS を介した管理

SonicWall セキュリティ装置は HTTP または HTTPS とウェブ ブラウザを使用して管理できます。既定では、HTTP のウェブ ベースの管理は無効です。工場出荷時の設定の SonicOS 管理インターフェースへのログインには HTTPS を使います。

HTTP または HTTPS を介して管理するには:

1 「**管理 | システム セットアップ > 装置 > 基本設定**」に移動します。

2 「**ウェブ管理設定**」までスクロールします。



3 HTTP 管理をグローバルに有効にするには、「**HTTP を介しての管理を許可する**」を選択します。このオプションは、既定では選択されていません。

4 HTTP の既定ポートはポート **80** ですが、他のポートからアクセスするように設定することもできます。「**HTTP ポート**」フィールドに、使用するポート番号を入力します。

> **重要**：HTTP 管理用に80 番以外のポートを設定した場合、IP アドレスを使用して SonicWall セキュリティ装置にログインするときにポート番号も入力する必要があります。例えば、ポートを 76 番に設定した場合は、ウェブ ブラウザに "*LAN IP アドレス*:76" (http://192.18.16.1:76 など) と入力しなければなりません。

5 HTTPS 管理の既定ポートは **443** です。この既定ポートを変更することによって、SonicWall セキュリティ装置へのログインにセキュリティ層をもう 1 つ追加するには、「**HTTPS ポート**」フィールドに別のポート番号を入力します。

> **重要**：ただし、HTTPS 管理ポートとして別のポートを設定した場合は、IP アドレスを使用して SonicWall セキュリティ装置にログインするときにポート番号も入力する必要があります。例えば、このポートに 700 番を使用する場合、https://192.18.16.1:700 のようにポート番号と IP アドレスを使用して SonicWall にログインする必要があります。

ブラウザ Cookie の削除

> **重要**：Cookie を削除すると、管理インターフェースで行った未保存のすべての変更が失われます。

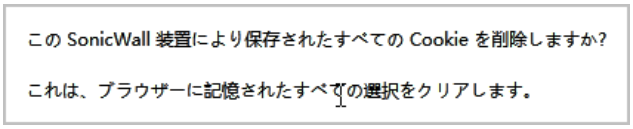
セキュリティ装置で保存されたすべてのブラウザ Cookie を削除するには:

1 「**管理 | システム セットアップ > 装置 > 基本設定**」に移動します。

2 「**ウェブ管理設定**」までスクロールします。

3 「**Cookie の削除**」を選択します。

確認メッセージが表示されます。



4 「**OK**」を選択します。最後に Cookie を削除した後に保存されたすべての Cookie が削除されます。

設定モードの切り替え

各装置には、管理インターフェースの設定モードを切り替える「**モード**」オプションがあります。現在は設定モードの場合、いつでも非設定モードに切り替えることができます。現在は非設定モードの場合、設定モードに切り替えることができます。

ヒント：この方法以外に、各ビューの「**モード**」設定からもモードを切り替えることができます。モードの詳細については、『*SonicOS について*』ガイドを参照してください。

モードを切り替えるには:

1 「**管理 | システム セットアップ > 装置 > 基本設定**」に移動します。

2 「**ウェブ管理設定**」までスクロールします。

3 次の手順を実行します。

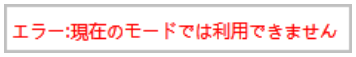
- 現在は設定モードの場合、「**設定モード の終了**」を選択します。ボタンが次のように変わります。

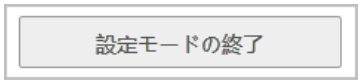
  ページの右上にある「**モード**」インジケータに「**非設定**」と表示されます。

  いずれかのビューで変更内容を保存しようとした場合は、次のエラー メッセージが表示されます。

- 現在は非設定モードの場合、「**設定モード** 」を選択します。ボタンが次のように変わります。

  ページの右上にある「**モード**」インジケータに「**設定**」と表示されます。

「**適用**」を選択する必要はありません。

4 元のモードに戻すには、次の手順を実行します。

- 設定モードに戻すには、「**設定モード** 」を選択します。
- 非設定モードに戻すには、「**設定モード の終了**」を選択します。

セキュリティ証明書の選択

セキュリティ証明書は、データ暗号化とセキュア ウェブ サイトを提供します。

セキュリティ証明書の種別を指定するには:

1 「**管理 | システム セットアップ | 装置 > 基本設定**」に移動します。

2 「**ウェブ管理設定**」までスクロールします。

3 「**証明書の選択**」から、ウェブ サイトで使用する証明書の種別を選択します。

- 「**自己署名証明書を使用**」を選択した場合、SonicWall セキュリティ装置にログインするごとに新しい証明書をダウンロードすることなく、1 つの証明書を続けて使用できます。このオプションは、既定では選択されています。「ステップ 4」に移動します。
- 「**証明書のインポート**」を選択した場合は、管理インターフェースに対する認証のために「**装置 > 証明書**」ページからインポートした証明書を選択します。確認メッセージが表示されます。

a) 「**OK**」を選択します。「**装置 > 証明書**」ページが表示されます。

b) 「証明書の管理 (65 ページ)」に移動します。

4 「**証明書コモンネーム**」フィールドに、ファイアウォールの IP アドレスまたはコモンネームを入力します。「**自己署名証明書を使用**」を選択した場合、SonicOS によってファイアウォールの IP アドレスがフィールドに入力されます。

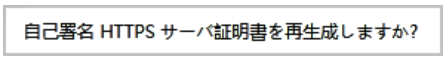
5 「**適用**」を選択します。

自己署名証明書を再生成するには:

1 「**管理 | システム セットアップ > 装置 > 基本設定**」に移動します。

2 「**ウェブ管理設定**」までスクロールします。

3 「**証明書の再生成**」を選択します。確認メッセージが表示されます。



4 「**OK**」を選択します。

管理インターフェースのテーブルの制御

SonicWall 管理インターフェースでは、管理インターフェースのすべてのテーブルにわたるような大きなテーブル情報の表示を次の点で制御できます。

- 1 ページに表示するテーブル エントリの数。
- テーブルをバックグラウンドで自動更新する頻度。

一部のテーブルでは、1 ページあたりの項目数をテーブルごとに個別に設定できます。その個別の設定はログイン時に初期化されて、ここで設定した値になります。これらのページの表示後に項目数を変更しても個別の設定はその場では変化しません。ここで行った変更は次回のログイン時にページの表示に初めて反映されます。

テーブルの表示と更新頻度を変更するには:

1 「**管理 | システム セットアップ > 装置 > 基本設定**」に移動します。

2 「**ウェブ管理設定**」までスクロールします。

3 「**既定のテーブル サイズ**」フィールドに、表示させる数 (「**1 ページの項目数**」) を入力します。最小値は 1、最大値は 5000、既定値は **50** です。

4 「**自動更新テーブルの更新間隔**」フィールドに、更新間隔を秒数で入力します。最小値は 1 秒、最大値は 300 秒、既定値は **10** 秒です。

5 「**適用**」を選択します。

開始ページの指定

管理インターフェースにログインすると、前回管理インターフェースからログアウトしたときに表示していたビューが表示されます。代わりにシステム ダッシュボードの表示で開始されるようにすることができます。

ログイン時に最初に「監視 | ダッシュボード」ページを表示するには:

1 「**管理 | システム セットアップ > 装置 > 基本設定**」に移動します。

2 「**ウェブ管理設定**」までスクロールします。

3 「「**脅威防御表示」を開始ページに使用する。**」を選択します。

4 「**適用**」を選択します。次回ログインするとき、ログアウト時にどのビューを表示していたかに関係なく、監視ダッシュボード ページが表示されます。

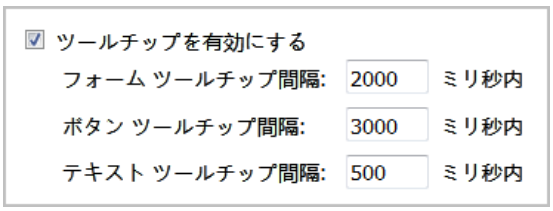
ツールチップの管理

SonicOS 管理インターフェースの多くの要素には組み込みのツールチップがあります。ツールチップの詳細については、『*SonicOS 6.5 SonicOS について*』を参照してください。

ツールチップの動作を設定するには:

1 「**管理 | システム セットアップ > 装置 > 基本設定**」に移動します。

2 「**ウェブ管理設定**」までスクロールします。



3 ツールチップを有効にするには、「**ツールチップを有効にする**」を選択します。

> **ヒント**：ツール チップは既定で有効になっています。ツール チップを無効にするには、「**ツールチップを有効にする**」をクリアします。

4 ツールチップが表示されるまでの時間を設定するには、ミリ秒単位で時間を入力します。

フィールド	時間間隔を入力する対象
フォーム ツールチップ間隔	フィールド。既定値は **2000** ミリ秒、最小値は 500 ミリ秒、最大値は 5000 ミリ秒です。
ボタン ツールチップ間隔	ラジオ ボタンとチェックボックス。既定値は **3000** ミリ秒、最小値は 500 ミリ秒、最大値は 5000 ミリ秒です。
テキスト ツールチップ間隔	管理インターフェース テキスト。既定値と最小値は **500** ミリ秒、最大値は 5000 ミリ秒です。

5 「**適用**」を選択します。

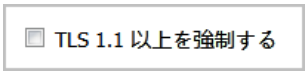
TLS のバージョンの強制

SonicOS は、バージョン 1.0、1.1、および 1.2 の Transport Layer Security (TLS) プロトコルをサポートしています。安全性の高いバージョン 1.1 以上が確実に使用されるようにすることができます。

TLS バージョン 1.1 以上の使用を強制するには:

1 「**管理 | システム セットアップ > 装置 > 基本設定**」に移動します。

2 「**ウェブ管理設定**」までスクロールします。



3 「**TLS 1.1 以上を強制する**」を選択します。このオプションは、既定では選択されていません。

4 「**適用**」を選択します。

フロントパネル管理インターフェースの設定 (SuperMassive ファイアウォールのみ)

メモ：このセクションは、前面に LCD パネルがある SuperMassive セキュリティ装置の場合にのみ表示されます。

フロントパネル管理インターフェースの設定メニューへのアクセスを有効または無効にできます。

ヒント：この機能は、SuperMassive セキュリティ装置を最初に設置したときに自動的に有効になります。

フロントパネル管理インターフェースの設定メニューへのアクセスを許可にするには:

1 「**管理 | システム セットアップ > 装置 > 基本設定**」に移動します。

2 「**フロントパネル管理インターフェース**」までスクロールします。

3 「**フロントパネル管理インターフェースを有効にする**」を選択します。このオプションは、既定では選択されています。

4 「**設定メニュー アクセスに対して PIN を要求する**」で、設定メニューへのアクセスに PIN を使用する必要があるかどうかを選択します。このオプションは、既定では選択されています。

   a 「**PIN**」フィールドに PIN 番号を入力します。既定値は **76642** (SONIC と同等の番号ダイヤル) です。

   ヒント：フロントパネルの設定メニューを設定するには、PIN 番号を入力する必要があります。

   b 「**PIN の確認**」フィールドに同じ PIN 番号を入力します。

5 「**PIN を隠す**」で、「**PIN**」フィールドと「**PIN の確認**」フィールドの入力時に PIN を隠すどうかを選択します。PIN を隠す場合、PIN は黒丸の列で表示されます。このオプションをオフにした場合 (選択しない場合) は、PIN が表示されます。このオプションは、既定では選択されています。

6 「**適用**」を選択します。

クライアント証明書の確認の設定

コモン アクセス カード (CAC) を使う場合と使わない場合について、証明書の確認を設定できます。

メモ：既定では、どのオプションも選択されていません。

トピック:

- コモン アクセス カードについて (43 ページ)
- クライアント証明書の確認の設定 (43 ページ)
- 「クライアント証明書の確認」の使用 (45 ページ)
- ユーザ ロックアウトの解決 (45 ページ)

コモン アクセス カードについて

コモン アクセス カード (CAC) は、米国国防総省 (DoD) のスマート カードです。インターネット上でセキュリティ性の高いアクセスを必要とする軍人その他の政府、非政府機関の職員が使用します。CAC では PKI 認証および暗号化を使用します。

メモ：CAC を使うには、外付けのカード リーダーを USB ポートに接続する必要があります。

「クライアント証明書の確認」は、一応 CAC を使うことを想定していますが、HTTPS/SSL 接続でクライアント証明書を必要とするどのようなシナリオにも対応しています。クライアント証明書に対する CAC サポートは HTTPS 接続でのみ有効です。

メモ：CAC は、Microsoft Internet Explorer 以外のブラウザでは機能しない可能性があります。

クライアント証明書の確認の設定

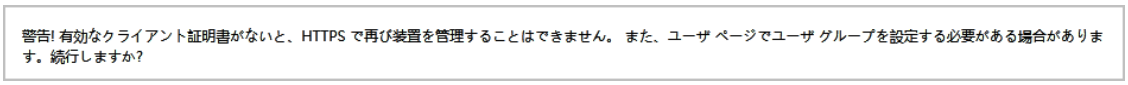
メモ：既定では、どのオプションも選択されていません。

クライアント証明書の確認を設定するには:

1 「**管理 | システム セットアップ > 装置 > 基本設定**」に移動します。

2 「**クライアント証明書の確認**」までスクロールします。

3 SonicWall セキュリティ装置でのクライアント証明書の確認と CAC サポートを有効にするには、「**クライアント証明書の確認を有効にする**」を選択します。このオプションを有効にすると、他のオプションが使用できるようになります。次のような確認の警告メッセージが表示されます。



4 「**OK**」を選択します。

5 クライアント証明書キャッシュを有効にするには、「**クライアント証明書キャッシュを有効にする**」を選択します。

メモ：キャッシュの有効期限は有効化後 24 時間です。

6 証明書のどのフィールドからユーザ名を取得するかを指定するには、「**ユーザ名フィールド**」からオプションを選択します。

- **件名：コモンネーム** (既定)
- **サブジェクト代替名: 電子メール**
- **サブジェクト代替名: Microsoft ユニバーサル プリンシパル名**

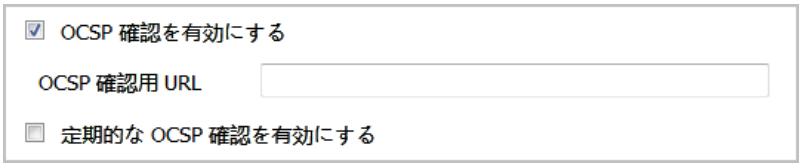
7 証明機関 (CA) 証明書の発行者を選択するには、「**クライアント証明書の発行者**」ドロップダウンメニューから 1 つを選択します。既定は **ComSign CA** です。

メモ：この一覧に目的とする CA がなければ、その CA を SonicWall セキュリティ装置にインポートする必要があります。「証明書の管理 (65 ページ)」を参照してください。

8 CAC ユーザ グループのメンバーシップを取得する方法を選択するには、「**CAC ユーザ グループ メンバーシップの取得方法**」ドロップダウン メニューで選択します。これで適切なユーザ権限が決まります。

- **ローカルで設定済み** (既定) - これを選択した場合は、適切なメンバーシップを持つローカル ユーザ グループを作成してください。
- **LDAP から** - これを選択した場合は、「**管理 | ユーザ > 設定**」で LDAP サーバを設定する必要があります「(LDAP を使用するための SonicWall の設定 (162 ページ)」を参照してください)。

9 クライアント証明書がまだ有効で失効していないことを確認するための OCSP (Online Certificate Status Protocol) 確認を有効にするには、「**OCSP 確認を有効にする**」を選択します。このオプションを有効にすると、「**OCSP 確認用 URL**」フィールドが表示され、「**定期的な OCSP 確認を有効にする**」オプションが表示されます。



a 「**OSCP 確認用 URL**」フィールドに、クライアント証明書の状況を確認する OCSP サーバの URL を入力します。

OCSP 確認用 URL は、通常はクライアント証明書内に埋め込まれているため、入力する必要はありません。クライアント証明書に OCSP リンクが含まれていない場合は、URL リンクを入力できます。このリンクは、OCSP による確認を行うサーバ側の CGI (Common Gateway Interface) を参照している必要があります。以下に例を示します。
`http://10.103.63.251/ocsp`

10 クライアント証明書がまだ有効で失効していないことを確認するための定期的な OCSP 確認を有効にするには:

a 「**定期的な OCSP 確認を有効にする**」を選択します。「OCSP 確認の間隔」フィールドが有効になります。

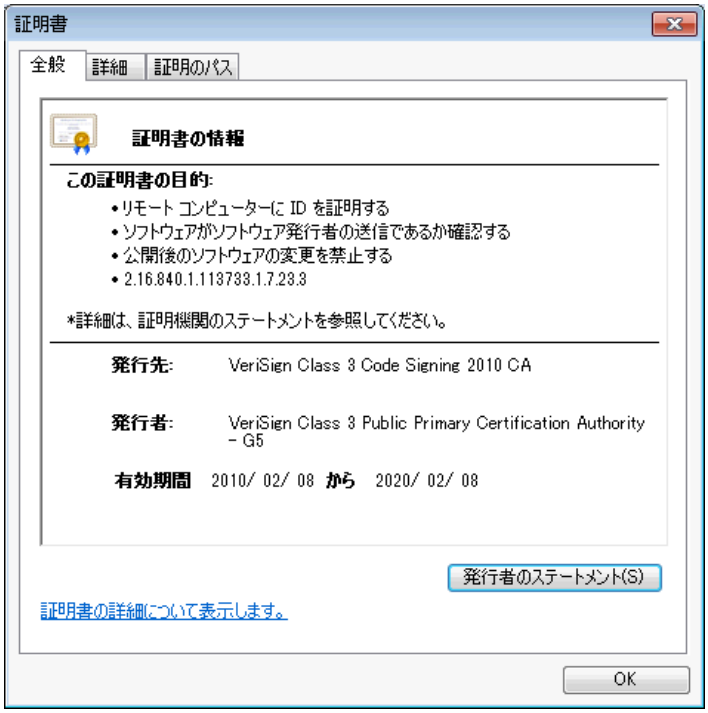
b 「**OCSP 確認の間隔: 1 ～ 72 (時間)**」フィールドに、OCSP による確認の間隔 (時間) を入力します。最小の間隔は 1 時間、最大の間隔は 72 時間、既定値は **24** 時間です。

11 「**適用**」を選択します。

「クライアント証明書の確認」の使用

クライアント証明書の確認で CAC を使用しない場合は、ブラウザにクライアント証明書を手動でインポートする必要があります。

クライアント証明書の確認で CAC を使用する場合は、クライアント証明書はミドルウェアによってブラウザに自動的にインストールされます。HTTPS を介して管理セッションを開始すると、証明書の確認を求める証明書選択ウィンドウが表示されます。



ドロップダウン メニューからクライアント証明書を選択した後で、HTTPS/SSL 接続が再開され、SonicWall セキュリティ装置はクライアント証明書が CA によって署名されているかを確認**するために**クライアント証明書の発行者 を検証します。一致が検出されると、管理者ログイン ページが表示されます。一致が検出されない場合は、ブラウザの接続が失敗したことを示す次のようなメッセージが表示されます。

ウェブ ページを表示できません。

OCSP が有効な場合、管理者ログイン ページが表示される前に、ブラウザによって OCSP 確認が行われ、確認中、次のメッセージが表示されます。

クライアント証明書 OCSP の確認中...

一致が確認されると、管理者ログイン ページが表示され、管理者の資格情報を使って SonicWall セキュリティ装置の管理を開始できます。

一致が検出されない場合は、ブラウザに次のメッセージが表示されます。

OCSP 確認が失敗しました。システム管理者に問い合わせてください。

ユーザ ロックアウトの解決

クライアント証明書機能を使う場合、以下の状況で SonicWall セキュリティ装置からユーザがロックアウトされる可能性があります。

- 「**クライアント証明書の確認を有効にする**」が選択されているが、ブラウザにクライアント証明書がインストールされていない。
- 「**クライアント証明書の確認を有効にする**」が選択され、ブラウザにクライアント証明書がインストールされているが、「**クライアント証明書の発行者**」が選択されていない、または誤った**クライアント証明書の発行者**が選択されている。
- 「**OCSP 確認を有効にする**」が有効だが、OCSP サーバが利用できないか、ネットワークの問題で SonicWall セキュリティ装置が OCSP サーバにアクセスできない。

ロックアウトされたユーザへのアクセスを回復するために、次の CLI コマンドが用意されています。

- `web-management client-cert disable`
- `web-management ocsp disable`

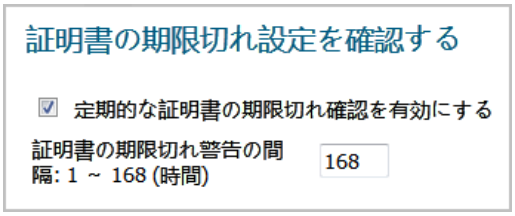
メモ：CLI コマンドの完全なリストと説明については、『*SonicOS 6.2 CLI リファレンス ガイド*』を参照してください。

証明書の期限切れの確認

証明書の期限切れの定期的な確認を有効にするには:

1 「**管理 | システム セットアップ > 装置 > 基本設定**」に移動します。

2 「**証明書の期限切れ設定を確認する**」までスクロールします。



3 「**定期的な証明書の期限切れ確認を有効にする**」を選択します。このオプションは、既定では選択されています。これを有効にすると、「**証明書の期限切れ警告の間隔：1～ 168 (時間)**」フィールドが使用可能になります。

4 証明書を確認する間隔 (時間) を設定するには、「**証明書の期限切れ警告の間隔:1 ～ 168 (時間)**」フィールドに間隔を入力します。最小の間隔は 1 時間、最大の間隔は 168 時間、既定値は **168** 時間です。

5 「**適用**」を選択します。

SSH 管理の設定

SSH を使用してファイアウォールを管理する場合、セキュリティを強化するために SSH ポートを変更できます。

SSH ポートを変更するには:

1 「**管理 | システム セットアップ > 装置 > 基本設定**」に移動します。

2 「**SSH 管理設定**」までスクロールします。

3 「**SSH ポート**」フィールドにポートを入力します。既定のSSH ポートは**22**です。

4 「**適用**」を選択します。

SonicOS API の有効化

選択した機能を設定する SonicOS コマンド ライン インターフェース (CLI) の代わりに SonicOS API を使用することができます。これを行うには、最初に SonicOS API を有効にする必要があります。SonicOS API の詳細については、『*SonicOS API リファレンス*』を参照してください。

SonicOS API を有効にするには、以下の手順に従います。

1 「**管理 | システム セットアップ | 装置 > 基本設定**」に移動します。

2 「**SonicOS API**」までスクロールします。

3 「**SonicOS API を有効にする**」を選択します。このオプションは、既定では選択されていません。

4 「**適用**」を選択します。

より高度な管理オプションの設定

より高度な管理オプションでは、次の項目を指定できます。

- SonicWall セキュリティ装置を SNMP (既定) と SonicWall グローバル管理システム (GMS) のどちらで管理するか。GMS の詳細については、『*GMS 管理者ガイド*』および『*クラウド GMS 管理者ガイド*』を参照してください。
- MGMT インターフェース用の管理インターフェース アドレス オブジェクトの作成。

  この管理インターフェースは、管理装置の保護インターフェースとなります。このインターフェースへのネットワーク接続は非常に制限されます。NTP、DNS、および SYSLOG サーバが MGMT サブネット内に設定されている場合、装置は MGMT IP を送信元 IP として使用し、MGMT アドレス オブジェクトとルート ポリシーの作成を自動的に行います。管理インターフェースからのトラフィックは、すべてこのポリシーによってルーティングされます。作成されたルートは、「**システム セットアップ > ネットワーク > ルーティング**」ページに表示されます (ルーティングの詳細については、「ルート通知とルート ポリシーの設定 (486 ページ)」を参照してください)。

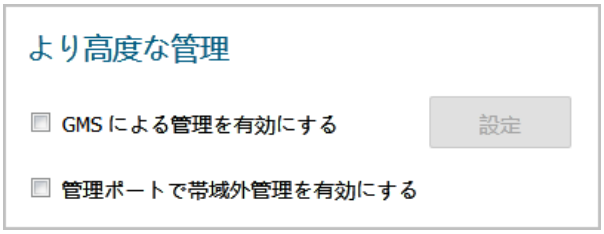
  この MGMT アドレス オブジェクトとルート ポリシーの作成/更新には IPv4 の管理 IP が使われます。既定で作成されるのは IPv6 の管理 IP アドレス オブジェクトなので、この機能は IPv6 の管理 IP アドレス オブジェクトの作成には効果を持ちません。

メモ：既定では、どのオプションも有効になっていません。

より高度な管理オプションを設定するには:

1 「**管理 | システム セットアップ > 装置 > 基本設定**」に移動します。

2 「**より高度な管理**」までスクロールします。



3 SonicWall GMS でファイアウォールを管理できるようにするには、「**GMS を使用する管理を有効にする**」を選択します。「**設定**」が使用可能になります。GMS を使用する管理の設定方法は、「GMS 管理を有効にする (48 ページ)」を参照してください。

4 MGMT インターフェース用の管理インターフェース アドレス オブジェクトの自動的作成を有効にするには、「**管理ポートで帯域外管理を有効にする**」を選択します。これは帯域外管理インターフェースとして機能し、そこで作成された新しいアドレス オブジェクトのルート ポリシーを設定します。「**適用**」を選択します。

重要：削除/作成ルート ポリシーの競合を回避するため、このオプションを更新することによって管理インターフェース アドレス オブジェクトの作成とルート ポリシーの設定が行われると、システムが再起動されます。

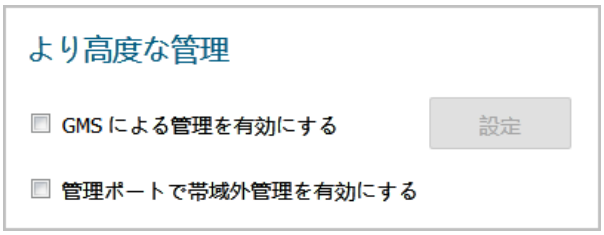
GMS 管理を有効にする

メモ：SonicWall グローバル管理システムの詳細については、http://www.SonicWall.com または『*GMS 管理者ガイド*』を参照してください。

GMS で管理できるように セキュリティ装置を設定するには:

1 「**管理 | システム セットアップ > 装置 > 基本設定**」に移動します。

2 「**より高度な管理**」までスクロールします。



3 「**GMS による管理を有効にする**」を選択します。「**設定**」が使用可能になります。

4 「**設定**」を選択します。「**GMS の設定**」ダイアログが表示されます。

5 「**GMS ホスト名または IP アドレス**」フィールドに GMS コンソールのホスト名または IP アドレスを入力します。

6 「**GMS Syslog サーバ ポート**」フィールドにポートを入力します。既定値は **514** です。

7 ログ メッセージの代わりにハートビート状況のみを送信するには、「**ハートビート状況メッセージのみ送信する**」を選択します。このオプションは、既定では無効になっています。

8 ネットワークで NAT を実行しているデバイスの背後に GMS コンソールが配置されている場合、「**NAT デバイス背後の GMS**」を選択します。このオプションは、既定では無効になっています。

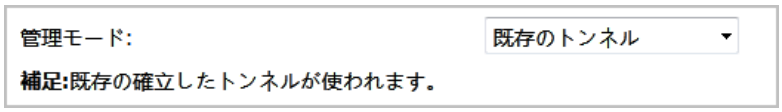
このオプションを選択すると、「**NAT デバイス IP アドレス**」フィールドが有効になります。

a 「**NAT デバイス IP アドレス**」フィールドに NAT デバイスの IP アドレスを入力します。

9 「**管理モード**」から以下の GMS モードのいずれか 1 つを選択します。

管理用 IPSEC トンネル IPsec VPN トンネルを越えた先の GMS 管理コンソールからファイアウォールを管理できます。「ステップ 10」へ進みます。

既存のトンネル GMS 管理サーバとファイアウォールの接続に既存の VPN トンネルを使用します。メッセージが表示されます。



「ステップ 12」へ進みます。

HTTPS 2 つの IP アドレス (GMS プライマリ エージェントとスタンバイ エージェントの IP アドレス) から HTTPS 管理が可能になります。また、SonicWall ファイアウォールは、3DES とファイアウォール管理者のパスワードを使用して暗号化された Syslog パケットと SNMP トラップも送信します。GMS レポーティング サーバを設定するオプションが表示されます。「ステップ 11」へ進みます。

10 SonicOS によって値が入力済みの既定の IPsec VPN 設定が表示されます。設定内容を確認します。

a 「**暗号化/認証の方式**」から、適切なアルゴリズムを選択します。

b (オプション)「**暗号化鍵**」フィールドに新しい暗号化鍵を入力します。

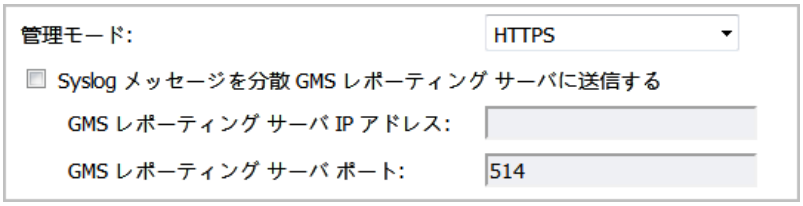
方式	鍵
DES	16 進数 16 文字
3DES	16 進数 48 文字

c (オプション)「**認証鍵**」フィールドに新しい認証鍵を入力します。

方式	鍵
MD5	16 進数 32 文字
SHA1	16 進数 40 文字

d 「ステップ 12」へ進みます。

11 SonicOS は GMS レポーティング サーバを認識する必要があります。



a 「**Syslog メッセージを分散 GMS レポーティング サーバに送信する**」を選択します。このオプションは、既定では選択されていません。以下のオプションが利用可能になります。

b 「**GMS レポーティング サーバ IP アドレス**」フィールドに、GMS サーバの IP アドレスを入力します。

c 「**GMS レポーティング サーバ ポート**」フィールドに、GMS サーバのポートを入力します。既定のポートは **514** です。

12 「**OK**」を選択します。

13 「**適用**」を選択します。

SonicPoint イメージの手動ダウンロード

「**ダウンロード URL**」セクションには、SonicPoint イメージをダウンロードするサイトの URL アドレスを指定するためのフィールドがあります。

使用中のファイアウォールが:

- インターネットに接続できる場合は、SonicPoint 機器を接続したときに SonicWall サーバから適切なバージョンの SonicPoint イメージが自動的にダウンロードされます。
- インターネットにアクセスできない場合、またはプロキシ サーバ経由のアクセスのみが可能な場合は、SonicPoint ファームウェアの URL を手動で指定する必要があります。開始文字列 **http://** は不要ですが、URL の末尾にファイル名を含める必要があります。ファイル名には .bin 拡張子が必要です。IP アドレスとドメイン名の例を次に示します。

```
192.168.168.10/imagepath/sonicpoint.bin
software.SonicWall.com/applications/sonicpoint/sonicpoint.bin
```

詳細については、『*SonicOS 6.5 更新*』を参照してください。

注意：SonicWall セキュリティ装置上で動作している SonicOS ファームウェア バージョンに対応する SonicPoint イメージをダウンロードしなければなりません。MySonicWall ウェブ サイトには、対応するバージョンに関する情報があります。SonicOS ファームウェアをアップグレードするときは、正しい SonicPoint イメージにアップグレードするように注意してください。

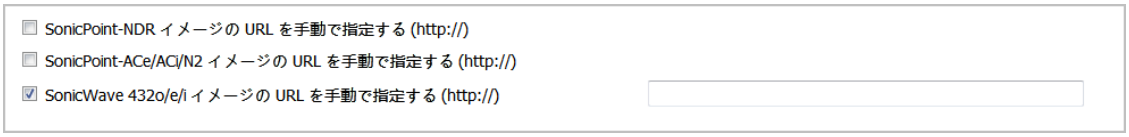
ダウンロードする SonicPoint イメージの種別を選択するには:

1 「**管理 | システム セットアップ > 装置 > 基本設定**」に移動します。

2 「**ダウンロード URL**」までスクロールします。

- **SonicPoint-N イメージの URL を手動で指定する (http://)**
- **SonicPoint-Ni/Ne イメージの URL を手動で指定する (http://)**
- **SonicPoint-NDR イメージの URL を手動で指定する (http://)**
- **SonicPoint-ACe/ACi/N2 イメージの URL を手動で指定する (http://)**
- **SonicPoint-AC Wave2 イメージの URL を手動で指定する (http://)**

3 適切な SonicPoint イメージ URL を選択します。その URL を入力するためのフィールドが表示されます。



4 対象のフィールドにイメージのダウンロードの場所を入力します。

5 「**適用**」を選択します。

言語の選択

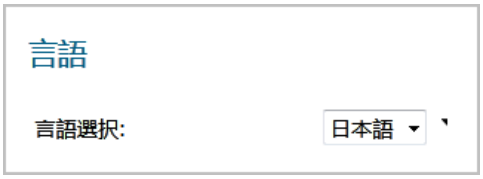
ファームウェアに英語以外の言語が含まれている場合は、「**言語選択**」から言語を選択できます。

メモ：SonicOS 管理インターフェースの言語を変更するには、SonicWall セキュリティ装置を再起動する必要があります。

管理インターフェースの言語を選択するには:

1 「**管理 | システム セットアップ > 装置 > 基本設定**」に移動します。

2 「**言語**」までスクロールします。



3 「**言語選択**」から言語を選択します。

4 「**適用**」を選択します。

3

SNMP の管理

- 「装置 > SNMP」について (53 ページ)
  - SNMP について (53 ページ)
  - SNMP アクセスの設定 (54 ページ)
  - SNMP のサービスとしての設定およびルールの追加 (64 ページ)
  - SNMP ログについて (64 ページ)

「装置 > SNMP」について

SonicWall セキュリティ装置を、SNMP または SonicWall グローバル管理システム (GMS) を用いて管理することができます。このセクションでは、SNMP を使って SonicWall を管理するように設定する方法を説明します。GMS を使用して SonicWall を管理する方法については、『*SonicOS GMS ガイド*』を参照してください。

トピック:

- SNMP について (53 ページ)
- SNMP アクセスの設定 (54 ページ)
- SNMP のサービスとしての設定およびルールの追加 (64 ページ)
- SNMP ログについて (64 ページ)

SNMP について

SNMP (Simple Network Management Protocol) は UDP (User Datagram Protocol) 上で使用されるネットワーク プロトコルです。ネットワーク管理者は SNMP を利用して SonicWall セキュリティ装置の状態を監視したり、ネットワーク上で重大なイベントが発生した際に通知を受信したりできます。SonicWall セキュリティ装置は、SNMP v1/v2c/v3 および関連するすべての Management Information Base II (MIB-II) グループ (**egp**、**at** 以外) をサポートしています。

SNMPv3 は、以前のバージョンの SNMP を拡張で、パケットの認証と暗号化の組み合わせによってネットワーク機器への保護されたアクセスを提供します。

パケット セキュリティは以下で提供されます。

- **メッセージの完全性** - 通信中にパケットが改ざんされていないことを保証します。
- **認証** - メッセージが正しい送信元からのものであることを確認します。
- **暗号化** - パケットの内容を難読化して、権限の無い送信元によって参照されることを防ぎます。

SNMPv3 はセキュリティ モデルとセキュリティ レベルの両方を提供します。セキュリティ モデルはユーザとユーザが所属するグループ間で設定される認証方式です。セキュリティ レベルは与えられたセキュリティ モデルで許可されるセキュリティのレベルです。セキュリティ モデルとそれに関連したセキュリティ レベルによって、SNMP パケットの処理方法が決定されます。SNMPv3 は追加レベルの認証と秘匿に加え、追加の承認とアクセス制御を提供します。

「SNMP のバージョンに基づくセキュリティ レベル、認証、および暗号化」テーブルは、異なるバージョンの SNMP によってどのようにセキュリティ レベル、認証、および暗号化が処理されるかを示しています。

SNMP のバージョンに基づくセキュリティ レベル、認証、および暗号化

バージョン	レベル	認証種別	暗号化	認証方式
v1	noAuthNoPriv	コミュニティ文字列	いいえ	コミュニティ文字列照合
v2c	noAuthNoPriv	コミュニティ文字列	いいえ	コミュニティ文字列照合
v3	noAuthNoPriv	ユーザ名	いいえ	ユーザ名照合
	authNoPriv	MD5 または SHA	いいえ	HMAC-MD5 または HMSC-SRA アルゴリズムに基づいた認証。
	authPriv	MD5 または SHA	DES または AES	HMAC-MD5 または HMSC-SRA アルゴリズムに基づいた認証。CBC-DES (DES-56) 規格に基づく認証に加えた DES 56 ビット暗号化、および AES 128 ビット暗号化も提供。

SonicWall セキュリティ装置は任意のインターフェースを使って MIB-II 用の SNMP `Get` コマンドに応答し、トラップ メッセージ生成のための個別 SonicWall MIB をサポートします。個別 SonicWall MIB は SonicWall のウェブ サイトからダウンロードでき、HP Openview、Tivoli、SNMPC などのサードパーティ製 SNMP 管理ソフトウェアにロードできます。

管理者は SNMP の設定を表示および設定できます。ユーザは設定の参照や編集ができません。SNMPv3 はユーザまたはグループ レベルで編集可能です。アクセス ビューは読取り、書込み、またその両方にすることが可能で、ユーザやグループに割り当て可能です。単一のビューがそれに関連する複数のオブジェクト ID (OID) を持つことが可能です。

SNMPv3 エンジン ID に対する SNMPv3 設定は、「**SNMP の設定**」ダイアログの「**一般設定**」メニュー内で設定できます。このエンジン ID は、受信した SNMP パケットの承認に使われます。一致したパケット エンジン ID だけが処理されます。

SNMP アクセスの設定

SNMP の設定は以下の作業で構成されます。

- SNMP アクセスの有効化と設定 (55 ページ)
- SNMPv3 グループとアクセスの設定 (58 ページ)

SNMP アクセスの有効化と設定

SNMPv1/v2 両方の基本的な機能を使うことも、より高機能な SNMPv3 オプションを使うようにセキュリティ装置を設定することも可能です。

SNMP を使用するには、まず SNMP を有効にします。

トピック:

- 基本的な機能の設定 (55 ページ)
- SNMPv3 エンジン ID の設定 (57 ページ)
- SNMPv3 ビューに対するオブジェクト ID の設定 (59 ページ)
- グループの作成とユーザの追加 (61 ページ)
- アクセスの追加 (63 ページ)

基本的な機能の設定

SNMP を有効にするには、以下の手順に従います。

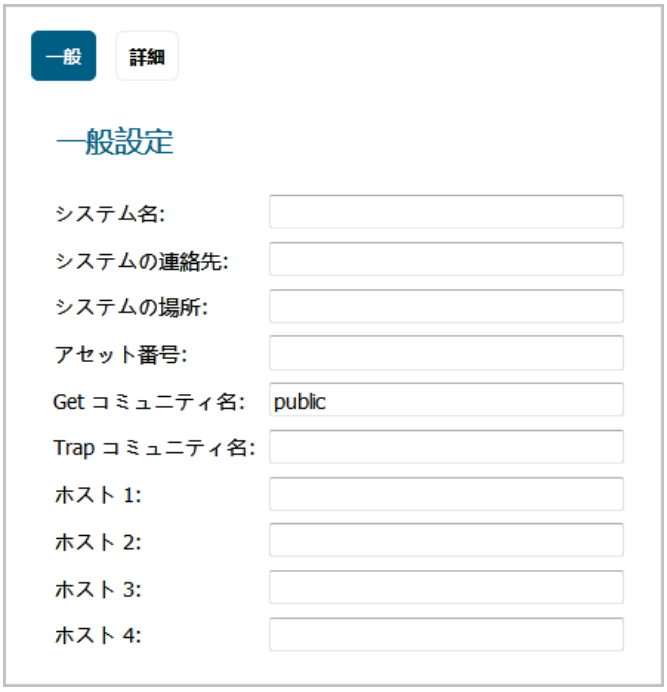
1 「**管理 | システム セットアップ > 装置 > SNMP**」ページに移動します。

2 「**SNMP を有効にする**」を選択します。既定では、SNMP は無効になっています。

3 「**適用**」を選択します。SNMP 情報が SNMP ページに設定され、「**設定**」が使用可能になります。


設定
SNMP を有効にする
設定
表示
名前
OID
設定
root
1.3
system
1.3.6.1.2.1.1
interfaces
1.3.6.1.2.1.2
IP
1.3.6.1.2.1.4
ICMP
1.3.6.1.2.1.5
TCP
1.3.6.1.2.1.6
UDP
1.3.6.1.2.1.7
ifMIB
1.3.6.1.2.1.31
追加
選択の削除
ユーザ/グループ
名前
セキュリティ レベル
認証
プライバシー
設定
* グループなし * (0 件)
グループの追加
ユーザの追加
選択の削除
アクセス
名前
ビュー表示
マスター グループ
セキュリティ レベル
設定
登録がありません。
追加
選択の削除

4 SNMP インターフェースを設定するには、「**設定**」を選択します。「**SNMP の設定**」ダイアログが表示されます。



5 「**一般**」ページで、「**システム名**」フィールドに SonicWall セキュリティ装置のホスト名を入力します。

6 (オプション)「**システムの連絡先**」フィールドにネットワーク管理者の名前を入力します。

7 (オプション)「**システムの場所**」フィールドに電子メール アドレス、電話番号、またはポケットベル番号を入力します。

8 SNMPv3 設定オプションを使用する場合は、「**アセット番号**」フィールドにアセット番号を入力します。それ以外の場合、このフィールドはオプションです。

9 「**Get コミュニティ名**」フィールドに SNMP データを参照できる管理者のグループまたはコミュニティの名前を入力します。既定の名前は、**public** です。

10 (オプション)「**Trap コミュニティ名**」フィールドに SNMP トラップを参照できる管理者のグループまたはコミュニティの名前を入力します。

11 「**ホスト 1**」から「**ホスト *n***」のフィールドに SNMP トラップを受信する SNMP 管理システムの IP アドレスまたはホスト名を入力します。少なくとも 1 つの IP アドレスまたはホスト名を設定する必要があります。ただし、設定できる数は、システムでのアドレス数またはホスト名の最大数が上限になります。

12 次のようにします。

- SNMPV3 を設定するには、「SNMPv3 エンジン ID の設定 (57 ページ)」に進みます。
- 現時点での SNMP の設定が完了した場合は、「**OK**」を選択します。

SNMPv3 エンジン ID の設定

SNMPv3 を使用する場合は、SNMPv3 エンジン ID と SNMP 優先順位を設定できます。SNMPv3 エンジン ID を設定すると、SNMP 管理のセキュリティが最大限に強化されます。

SNMPv3 エンジン ID を設定するには:

1 「**管理 | システム セットアップ > 装置 > SNMP**」に移動します。

2 システムの SNMP をまだ設定していない場合は、「基本的な機能の設定 (55 ページ)」の「ステップ 1」～「ステップ 11」の手順に従います。

3 「**詳細設定**」を選択します。「**詳細**」ページが表示されます。

4 「**SNMPv3 を必須にする**」を選択します。これによって SNMPv1/v2 が無効になり、SNMPv3 アクセスのみが可能になるため、SNMP 管理のセキュリティが最大限に強化されます。

> **重要**：このオプションを選択する場合、「**OK**」を選択する前に、「**一般**」ページでアセット番号を指定する必要があります。

5 「**エンジン ID**」フィールドに 16 進のエンジン ID 番号を入力します。このフィールドは SonicOS によって自動で入力されますが、変更できます。この番号は受信した SNMP パケットと照合されて、パケット処理の承認に使われます。エンジン ID がこの番号と一致したパケットのみが処理されます。

6 必要に応じて、「**SNMP サブシステムの優先順位を上げる**」チェックボックスをオンにします。

システムの処理を効率化するために、特定の処理が SNMP クエリへの応答よりも優先されることがあります。このオプションを有効にすると、SNMP サブシステムの応答と処理が常に高いシステム優先順位で行われるようになります。

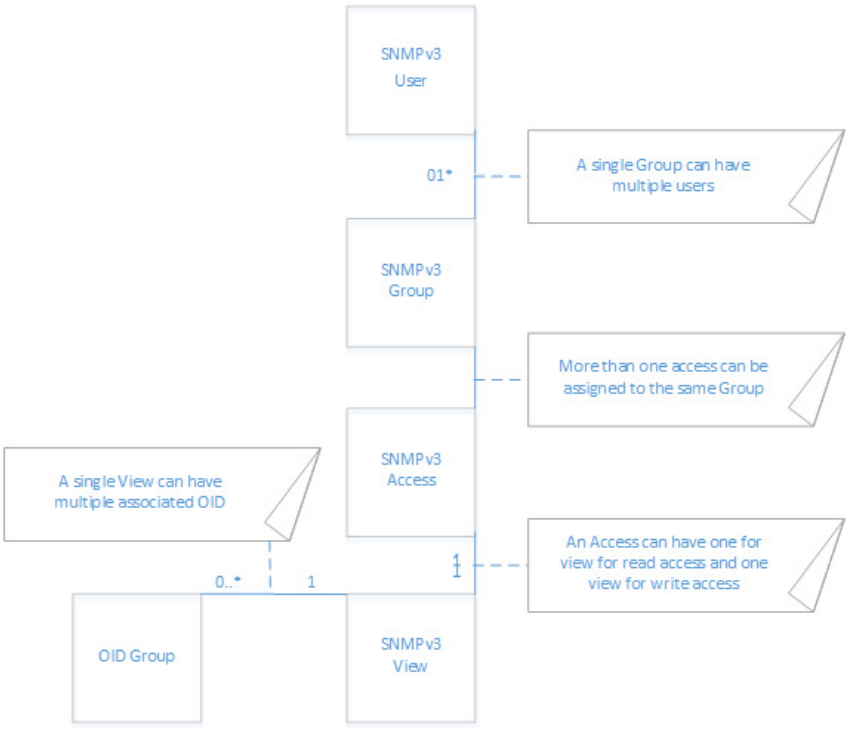
> **重要**：このオプションを有効にすると、システム全体のパフォーマンスに影響が生じることがあります。

7 「**OK**」を選択します。パケット処理で SNMPv3 セキュリティ オプションが使用されるようになります。

SNMPv3 グループとアクセスの設定

SNMPv3 では、グループとアクセスを設定し、異なるレベルのセキュリティを割り当てることが可能です。オブジェクト ID を種々の許可レベルに関連付け、単一のビューを複数のオブジェクトに割り当てることが可能です。「SNMPv3 グループとユーザのアクセス」は、グループとユーザのアクセスが、これらのさまざまな許可レベルにどのように関連付けられるかを示しています。

SNMPv3 グループとユーザのアクセス



SNMPv3 ビューに対するオブジェクト ID の設定

SNMPv3 **ビュー**はユーザまたはグループに対するアクセス設定を示します。ユーザとグループの設定は管理者が作成します。これらのセキュリティ設定はユーザには変更できません。SNMPv3 ビューはオブジェクト ID (OID) とオブジェクト ID グループを定義し、SNMPv3 アクセス オブジェクトと呼ばれることもあります。

この SNMP **ビューは**、OID と OID グループの集合を定義します。最初の既定ビューのセットは、変更または削除できません。既定ビューはルート ビュー、システム ビュー、IP、インターフェース、その他最もよく使われるビューを提供します。これらのビューの OID は事前割り当て済みです。

さらに、特定のユーザやグループに対して個別のビューを作成できます。

管理者は自分が作成したビューを変更できます。システムが作成したビューは変更できません。

SNMPv3 ビューの OID を設定するには:

1 「**管理 | システム セットアップ > 装置 > SNMP**」に移動します。

2 ビューを追加するには、「**ビュー**」セクションで、「**追加**」を選択します。「**SNMP ビューの追加**」ダイアログが表示されます。

3 「**ビュー名**」フィールドにわかりやすい名前を入力します。既定の名前は「**新規 SNMP ビュー**」です。

メモ：既存のビューを編集するときは、名前は編集できません。

4 「**ビューに関連付けされた OID**」フィールドに、未定義の OID を入力します。

5 「**OID の追加**」を選択します。

「**OID 一覧**」に新しいビューが表示されます。「OID 一覧」から OID を削除するには、OID を選択して「**削除**」を選択します。

6 さらに必要な新しいビューを関連する OID とともに追加します。

7 「**OK**」を選択します。新しいビューが「**表示**」テーブルに追加されます。

グループの作成とユーザの追加

既定では、「*** グループなし ***」という 1 つのグループがあります。このグループを設定したり削除したりすることはできません。ただし、この既定のグループにユーザを追加することはできます。

トピック:

- グループの作成 (61 ページ)
- ユーザの追加 (61 ページ)

グループの作成

グループを作成するには、以下の手順に従います。

1 「**管理 | システム セットアップ > 装置 > SNMP**」に移動します。

2 「**ユーザ/グループ**」テーブルの「**グループの追加**」を選択します。「**SNMP グループの追加**」ダイアログが表示されます。

3 「**グループ名**」フィールドにわかりやすい名前を入力します。グループ名は英数字 32 文字までで指定します。

4 「**OK**」を選択します。「**ユーザ/グループ**」テーブルが更新され、「**設定**」列にある**編集**アイコンと**削除**アイコンが使用可能になります。

ユーザの追加

ユーザを追加するには、以下の手順に従います。

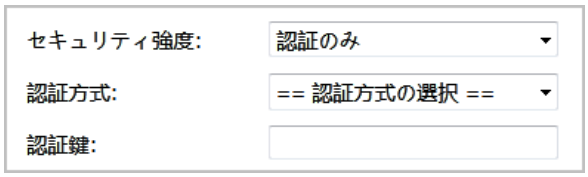
1 「**管理 | システム セットアップ > 装置 > SNMP**」に移動します。

2 「**ユーザ/グループ**」テーブルの「**ユーザの追加**」を選択します。「**SNMP ユーザの追加**」ダイアログが表示されます。

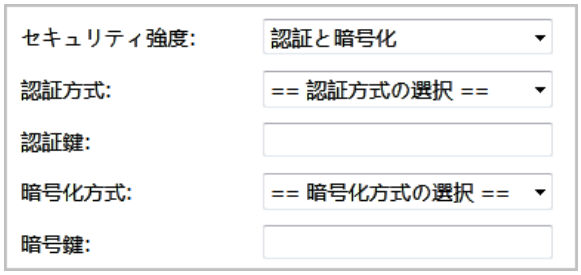
3 「**ユーザ名**」フィールドにユーザ名を入力します。

4 「**セキュリティ強度**」から次のいずれかのセキュリティ レベルを選択します。

- **なし** (既定)
- **認証のみ** - 次の 2 つの新しいオプションが表示されます。



  - **認証方式** - 認証方式として「**MD5**」または「**SHA1**」を選択します。
  - **認証鍵** - フィールドに認証鍵を入力します。この鍵には、印字可能な 8 ～ 32 文字の任意の文字列を指定できます。
- **認証と暗号化** - 次のようにさらに多くのオプションが表示されます。



  - **認証方式** - 上記を参照してください。
  - **認証鍵** - 上記を参照してください。
  - 「**暗号化方式**」ドロップダウン メニューで、暗号化方式として「**AES**」または「**DES**」を選択します。
  - 「**暗号鍵**」フィールドに暗号化鍵を入力します。この鍵には、印字可能な 8 ～ 32 文字の任意の文字列を指定できます。

5 「**グループ**」からグループを選択します。既定では「*** グループなし ***」になります。

6 作業が完了したら「**OK**」を選択します。ユーザが「**ユーザ/グループ**」テーブルに追加され、適切なグループ (「*** グループなし ***」も含む) に追加されます。

アクセスの追加

SNMPv3 アクセスは以下のようなオブジェクトです。

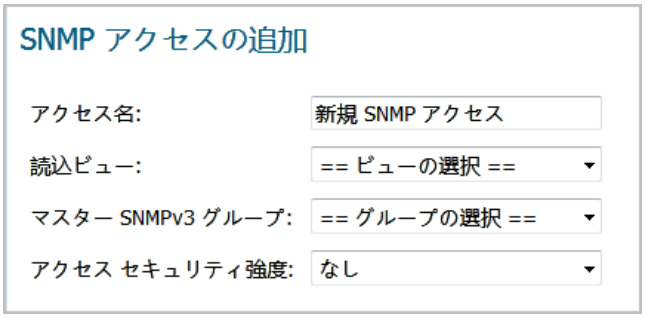
- SNMPv3 ビューの読み/書きアクセス権を定義します。
- SNMPv3 グループに割り当てることができます。

複数のグループを同一のアクセス オブジェクトに割り当てることが可能です。アクセス オブジェクトはまた、割り当てられた複数のビューを持つことが可能です。

アクセス オブジェクトを作成するには、以下の手順に従います。

1 「**管理 | システム セットアップ > 装置 > SNMP**」に移動します。

2 「**アクセス**」テーブルで、「**追加**」を選択します。「**SNMP アクセスの追加**」ダイアログが表示されます。



3 「**アクセス名**」フィールドにわかりやすい名前を入力します。

> **メモ**：既存の項目の名前は編集できません。

4 「**読込ビュー**」で、利用可能なビューのリストからビューを選択します。

5 「**マスター SNMPv3 グループ**」で、利用可能なグループのリストからグループを選択します。

> **メモ**：アクセスは、1 つの SNMPv3 グループにのみ割り当てることができます。ただし、グループを複数のアクセス オブジェクトに関連付けることはできます。
>
> 「*** グループなし ***」にアクセスを割り当てることはできません。

6 「**アクセス セキュリティ強度**」から次のいずれかのセキュリティ レベルを選択します。

- **なし**
- **認証のみ**
- **認証と暗号化**

7 「**OK**」を選択します。「**アクセス**」テーブルにアクセス オブジェクトが追加されます。

SNMP のサービスとしての設定およびルールの追加

既定で、SNMP は SonicWall セキュリティ装置上で無効になっています。SNMP を有効にするには、最初に「**管理 | システム セットアップ > 装置 > SNMP**」ページで SNMP を有効にし、次に個々のインターフェースに対して有効にします。それには、「**管理 | システム セットアップ > ネットワーク > インターフェース**」ページに移動し、SNMP を有効にするインターフェース用の「**設定**」を選択します。SNMP のサービスとしての設定およびルールの追加の詳細については、「インターフェースの設定 (278 ページ)」を参照してください。

SNMP 管理システムが自動検出をサポートしている場合は、SonicWall セキュリティ装置エージェントがネットワーク上の SonicWall セキュリティ装置を自動検出します。サポートしていない場合、SNMP 管理システム上の SNMP 管理機器のリストに SonicWall セキュリティ装置を追加する必要があります。

SNMP ログについて

SNMP ログは、「**調査 | ログ > イベント ログ**」ページで表示できます。イベント ログの詳細については、『*SonicOS 6.5 調査*』を参照してください。

トラップ メッセージは、通常 SonicWall セキュリティ装置が送信する警告メッセージ種別に対してのみ生成されます。例えば、攻撃、システム エラー、ウェブ サイトの遮断に対してトラップ メッセージが生成されます。「**調査 | ログ > イベント ログ**」ページでこれらの種別を選択しなかった場合、トラップ メッセージは生成されません。

4

証明書の管理

トピック:

- 証明書について (65 ページ)
  - デジタル証明書について (65 ページ)
  - 「証明書と証明書署名リクエスト」テーブルについて (66 ページ)
  - 証明書のインポート (68 ページ)
  - 証明書の削除 (70 ページ)
  - 証明書署名リクエストの生成 (71 ページ)
  - 単純証明書登録プロトコルの設定 (75 ページ)

証明書について

VPN ポリシーでの証明書の使用を実装するには、有効な CA 証明書をサードパーティの CA サービスから取得する必要があります。有効な CA 証明書を取得したら、ローカル証明書を有効にするために CA 証明書をファイアウォールにインポートします。有効な CA 証明書をファイアウォールにインポートするには、「**管理 | システム セットアップ > 装置 > 証明書**」ページを使用します。有効な CA 証明書をインポートしたら、それを使用してローカル証明書を有効にします。

SonicOS は、SonicWall セキュリティ装置に多数の証明書を提供します。これらはビルトイン証明書であり、削除したり設定したりできません。

SonicOS は、ローカルの証明書失効リスト (CRL) をサポートします。これは、発行元の認証局 (CA) によって、有効期限が切れる前に失効され、信頼されなくなったデジタル証明書のリストです。ローカル CRL の詳細については、テクニカル サポートにお問い合わせください。

デジタル証明書について

デジタル証明書は、認証局 (CA) として知られる信頼されるサードパーティによって身元を確認するための電子的な手段です。X.509 v3 証明書規格は暗号化証明書で使用される仕様で、証明書に含める拡張領域を定義できます。SonicWall では、サードパーティ証明書のサポートの一環としてこの規格を実装しています。

サードパーティの CA によって署名され確認された証明書は、IKE (インターネット鍵交換) VPN ポリシーで使用できます。IKE は IPsec VPN ソリューションの重要な部分であり、SA (Security Association) を設定する前にデジタル証明書を使用して相手の機器を認証できます。デジタル証明書を使用しない場合、VPN ユーザは共有鍵または対称鍵を手動で交換して認証する必要があります。デジタル署名を使用する機器またはクライアントは、新しい機器またはクライアントがネットワークに追加されるたびに設定を変更する必要はありません。

一般的な証明書は、データ セクションと署名セクションの 2 つのセクションで構成されます。データ セクションには通常、証明書がサポートする X.509 のバージョン、証明書のシリアル番号、ユーザの公開鍵に関する情報、識別名 (DN)、証明書の有効期間、証明書の利用目的のようなオプション情報などの情報が含まれます。署名セクションには、発行元 CA が使用した暗号化アルゴリズムおよび CA のデジタル署名が含まれます。

SonicWall セキュリティ装置は、X.509 v3 準拠のすべての証明書発行者と相互運用性があります。SonicWall セキュリティ装置は、以下の CA 証明書ベンダーについてテスト済みです。

- Entrust
- Microsoft
- OpenCA
- OpenSSL と TLS
- VeriSign

トピック:

- 「証明書と証明書署名リクエスト」テーブルについて (66 ページ)
- 証明書のインポート (68 ページ)
- 証明書の削除 (70 ページ)
- 証明書署名リクエストの生成 (71 ページ)
- 単純証明書登録プロトコルの設定 (75 ページ)

「証明書と証明書署名リクエスト」テーブルについて

「**証明書と証明書署名リクエスト**」テーブルには、CA 証明書およびローカル証明書を管理するためのすべての設定があります。

「**表示形式**」メニューを使用すると、以下の条件に基づいて証明書を表示できます。

条件	表示内容
すべての証明書	すべてのビルトイン証明書およびインポートした証明書と証明書署名リクエスト。このオプションは既定の設定です。
インポートした証明書とリクエスト	インポートした証明書および生成した証明書署名リクエストのみ。このオプションは、既定では選択されていません。
ビルトイン証明書	ビルトイン証明書のみ。このオプションは、既定では選択されていません。
期限切れのビルトイン証明書を含む	すべての期限切れ証明書およびビルトイン証明書。このオプションは、既定では選択されていません。

「**証明書と証明書署名リクエスト**」テーブルには、証明書に関する以下の情報が表示されます。

列	表示内容
証明書	証明書の名前
種別	証明書の種別: • **CA 証明書** • **ローカル証明書** • **要求の保留中**
認証	認証情報: • 空白 • **自己署名** • **失効まであと *n* 日** • **期限切れ**
有効期限	証明書の期限が切れる日時
詳細	証明書の詳細情報。**コメント** アイコンの上にポインタを移動すると、証明書の詳細情報が表示されます。証明書の詳細情報については、「証明書の詳細について (67 ページ)」を参照してください。
設定	以下が含まれます。 • 証明書のエントリを削除する**削除**アイコン • CA 証明書に対する証明書失効リストまたは未処理リクエストに対する署名済み証明書をインポートするための**インポート** アイコン **メモ：** ビルトイン証明書を削除またはインポートすることはできません。

証明書の詳細について

「**詳細**」列で**コメント** アイコンを選択すると、証明書に関する情報が表示されます。証明書の種別によって異なりますが、以下の情報が含まれます。

- 「署名アルゴリズム」
- 「証明書発行者」
- 「サブジェクト識別名」
- 「公開鍵アルゴリズム」
- 「証明書シリアル番号」
- 「有効期間の開始」
- 「有効期間の終了」
- 「状況」 (未処理リクエストまたはローカル証明書の場合)

詳細情報は、証明書の種別によって異なります。「証明書発行者」、「**証明書シリアル番号**」、「**有効期間の開始**」、および「**有効期間の終了**」は、証明書の発行者によって生成される情報であるため、未処理リクエストの場合には表示されません。

証明書のインポート

CA サービスによって未処理リクエストの証明書が発行されるか、またはローカル証明書が提供されたら、それをインポートして VPN またはウェブ管理認証で使用できます。CA 証明書をインポートして、IKE ネゴシエーションで使用されるローカル証明書および相手の証明書を確認することもできます。

トピック:

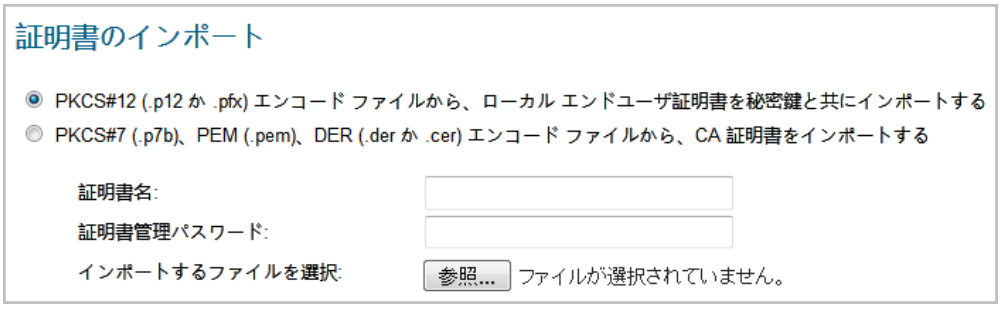
- ローカル証明書のインポート (68 ページ)
- 認証局の証明書のインポート (69 ページ)
- PKCS-12 形式の証明書ファイルの作成 (Linux システムのみ) (70 ページ)

ローカル証明書のインポート

ローカル証明書をインポートするには、以下の手順に従います。

1 「**管理 | システム セットアップ > 装置 > 証明書**」に移動します。

2 「**インポート** 」を選択します。「 **証明書のインポート** 」ダイアログが表示されます。



3 「**証明書名**」フィールドに証明書の名前を入力します。

4 「**証明書管理パスワード**」フィールドに、認証局が PKCS#12 ファイルの暗号化に使用したパスワードを入力します。

5 「**参照**」を選択して証明書ファイルを見つけます。

6 「**開く**」を選択して証明書へのディレクトリ パスを設定します。

7 「**インポート**」を選択してファイアウォールに証明書をインポートします。インポートが完了すると、「**証明書と証明書署名リクエスト**」テーブルに証明書のエントリが表示されます。

8 「**詳細**」列の**コメント** アイコンの上にポインタを移動すると、証明書の詳細情報が表示されます。

> **メモ：**証明書が正常にアップロードされると、マウスを移動したときに表示される「**状況**」は「**確認済**」になります。

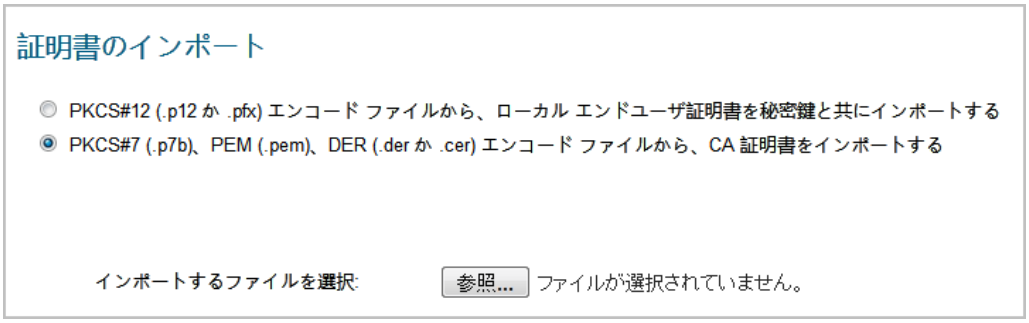
認証局の証明書のインポート

認証局の証明書をインポートするには、以下の手順に従います。

1 「**管理 | システム セットアップ > 装置 > 証明書**」に移動します。

2 「**インポート** 」を選択します。「**証明書のインポート**」ダイアログが表示されます。

3 「**PKCS#7 (.p7b)、PEM (.pem)、DER (.der か .cer) エンコード ファイルから、CA 証明書をインポートする**」を選択します。「**証明書のインポート**」ダイアログの設定が変わります。



4 「**参照**」を選択して証明書ファイルを見つけます。

5 「**開く**」を選択して証明書へのディレクトリ パスを設定します。

6 「**インポート**」を選択してファイアウォールに証明書をインポートします。インポートが完了すると、「**証明書と証明書署名リクエスト**」テーブルに証明書のエントリが表示されます。

7 「**詳細**」列の**コメント** アイコンの上にポインタを移動すると、証明書の詳細情報が表示されます。

PKCS-12 形式の証明書ファイルの作成 (Linux システムのみ)

PKCS-12 形式の証明書ファイルは Linux システムで OpenSSL により作成できます。PKCS-12 形式の証明書ファイルを作成するには、証明書の次の 2 つの構成要素が必要です。

- 秘密鍵 (通常、拡張子 `.key` を持つファイル、またはファイル名に単語 "key" を含むファイル)
- 公開鍵を含む証明書 (通常、拡張子 `.crt` を持つファイル、またはファイル名に単語 "cert" を含むファイル)

例えば、Linux 上の HTTP サーバ Apache では、秘密鍵と証明書は次の場所にあります。

- `/etc/httpd/conf/ssl.key/server.key`
- `/etc/httpd/conf/ssl.crt/server.crt`

これら 2 つのファイルがある状態で、次のコマンドを実行します。

```
openssl pkcs12 -export -out out.p12 -inkey server.key -in server.crt
```

この例では、**`out.p12`** が PKCS-12 形式の証明書ファイルになり、**`server.key`** と **`server.crt`** が PEM 形式の秘密鍵および証明書ファイルです。

`openssl` コマンドを実行した後で、ファイルを保護/暗号化するためのパスワードの入力を求められます。パスワードを選択すると、PKCS-12 形式の証明書ファイルの作成が完了し、装置にインポートできるようになります。

証明書の削除

メモ：ビルトイン証明書は削除できません。

インポートした証明書は、証明書の期限が切れた場合、または VPN 認証にサードパーティの証明書を使用しない場合に削除できます。作成した証明書はいつでも削除できます。

削除するには:

- 1 つの証明書を削除するには、その証明書の**削除**アイコンを選択します。
- 1 つまたは複数の証明書を削除するには:
  a それらの証明書のチェックボックスをオンにします。「**削除**」および「**すべて削除**」が使用可能になります。
  b 「**削除**」または「**すべて削除**」を選択します。
- ビルトイン証明書以外の証明書をすべて削除するには:
  a テーブル見出しにある該当するチェックボックスをオンにします。「**削除**」および「**すべて削除**」が使用可能になります。
  b 「**削除**」または「**すべて削除**」を選択します。

証明書署名リクエストの生成

ヒント：ローカル証明書とともに使用する証明書ポリシーを作成する必要があります。証明書ポリシーは、証明書を検証するために必要な認証要件および認証制限を定めます。

証明書署名リクエストを生成するには:

1 「**管理 | システム セットアップ > 装置 > 証明書**」に移動します。

2 「**新しい署名リクエスト**」を選択します。「**証明書署名リクエストの生成**」ダイアログが表示されます。

3 「**証明書名**」フィールドに証明書のエイリアス名を入力します。

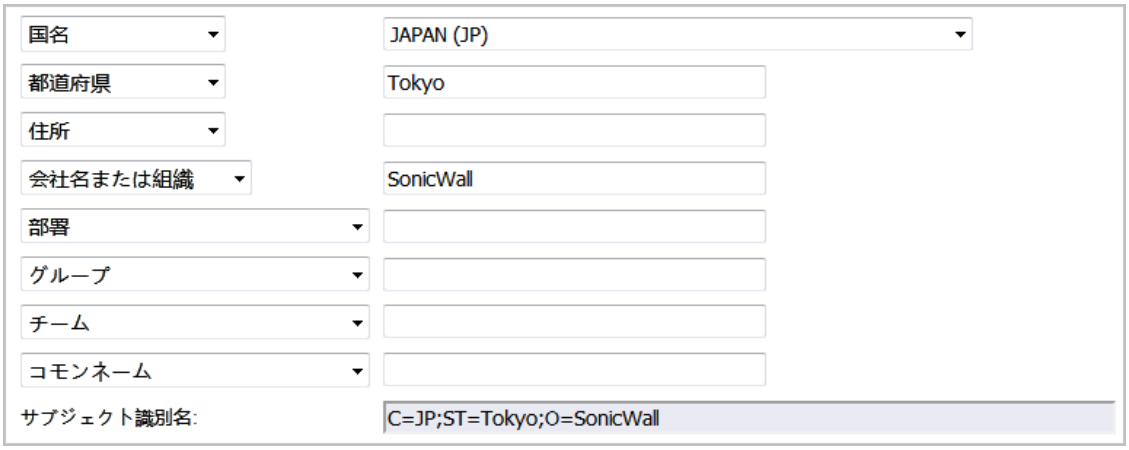
4 「識別名の構成要素」テーブルに示すドロップダウン メニューを使用して識別名 (DN) を作成し、関連フィールドに証明書の情報を入力します。

メモ：DN ごとに、関連ドロップダウン メニューから国を選択できます。他のすべての構成要素については、関連フィールドに情報を入力します。

識別名の構成要素

ドロップダウン メニュー	該当する情報を選択/入力
国名	国名 (既定) 状態 住所 会社名または組織
都道府県	国 都道府県 (既定) 住所 会社名または組織 部署
住所	住所 (既定) 会社名または組織 部署 グループ チーム
会社名または組織	会社名または組織 (既定) 部署 グループ チーム 一般名 シリアル番号 電子メール アドレス
部署	部署 (既定) グループ チーム 一般名 シリアル番号 電子メール アドレス
グループ	グループ (既定) チーム 一般名 シリアル番号 電子メール アドレス
チーム	チーム (既定) 一般名 シリアル番号 電子メール アドレス
コモンネーム	コモンネーム (既定) シリアル番号 電子メール アドレス

構成要素の情報を入力すると、「**サブジェクト識別名**」フィールドに識別名 (DN) が生成されます。



5 必要に応じて、ドロップダウン メニューから種別を選択した後で、証明書に以下の**サブジェクト代替名**を付けることもできます。

- **ドメイン名**
- **電子メール アドレス**
- **IPv4 アドレス**

6 「**署名アルゴリズム**」ドロップダウン メニューで、次のいずれかの署名アルゴリズムを選択します。

- **MD5**
- **SHA1** (既定)
- **SHA256**
- **SHA384**
- **SHA512**

7 「**サブジェクト鍵種別**」ドロップダウン メニューで、次のいずれかのサブジェクト鍵種別を選択します。

RSA (既定)	データを暗号化するために使用される公開鍵暗号化アルゴリズム。
ECDSA	高強度鍵ビット単位セキュリティを確保する Elliptic Curve Digital Signature Algorithm (楕円曲線デジタル署名アルゴリズム) を使用してデータを暗号化します。

8 「**サブジェクト鍵サイズ/曲線**」ドロップダウン メニューで、サブジェクト鍵サイズまたは曲線を選択します。

メモ：認証局はすべての鍵サイズまたは曲線をサポートするわけではないので、認証局がサポートする鍵サイズや曲線を確認する必要があります。

選択した鍵種別が	
RSA の場合は鍵サイズを選択	ECDSA の場合は曲線を選択
1024 ビット (既定)	prime256vi: 256 ビット素体を超える X9.62/SECG 曲線 (既定)
1536 ビット	secp384r1: 384 ビット素体を超える NIST/SECG 曲線
2048 ビット	secp521r1: 521 ビット素体を超える NIST/SECG 曲線
4096 ビット	

9 「**生成**」を選択して証明書署名リクエスト ファイルを生成します。

証明書署名リクエストが生成されると、結果を示すメッセージがブラウザ ウィンドウの下部の「状況」エリアに表示され、新しいエントリが「**証明書と証明書署名リクエスト**」テーブルに「**未処理の要求**」という種別で表示されます。

10 **エクスポート** アイコンを選択します。「**証明書署名リクエストのエクスポート**」ダイアログが表示されます。

11 **エクスポート** アイコンを選択して、コンピュータにファイルをダウンロードします。「***<証明書>*を開く**」ダイアログが表示されます。

12 「**OK**」を選択して、コンピュータ上のディレクトリにファイルを保存します。

これで、検証のために認証局に送信できる「**証明書署名リクエスト**」が生成されました。

13 署名リクエストに対する署名済み証明書をアップロードするために、**アップロード** アイコンを選択します。「**署名リクエストに対する署名済み証明書のアップロード**」ダイアログが表示されます。

14 ファイルを選択するために、「**参照**」を選択します。「ファイルを開く」ダイアログが表示されます。

15 ファイルを選択します。

16 「**開く**」を選択します。

17 「**アップロード**」 を選択します。

単純証明書登録プロトコルの設定

単純証明書登録プロトコル (SCEP) は、拡張性に優れた手法でネットワーク機器への証明書の保護された発行をサポートするように設計されています。SCEP に対して、 2 つの登録シナリオがあります。

- SCEP サーバ CA が自動的に証明書を発行する。
- SCEP 要求が PENDING に設定されて、CA 管理者が手動で証明書を発行する

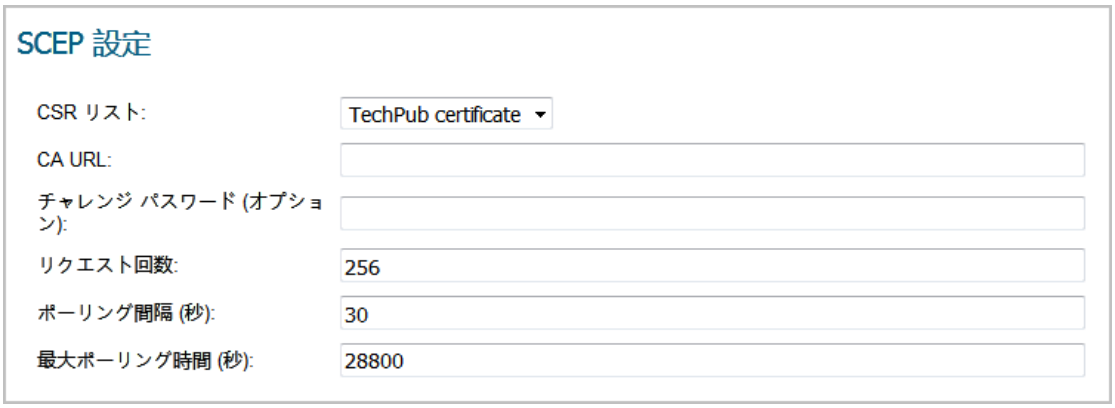
以下のサイトで、SCEP に関する更なる情報を入手できます。http://tools.ietf.org/html/draft-nourse-scep-18 (*Cisco Systems の単純証明書登録プロトコル draft-nourse-scep-18*)

証明書の発行に SCEP を使うには、以下の手順に従います。

1 前述の「証明書署名リクエストの生成 (71 ページ)」で説明したように、署名リクエストを生成します。

2 「**装置 > 証明書**」ページの一番下までスクロールします。

3 「**SCEP**」を選択します。「**SCEP 設定**」ダイアログが表示されます。



4 「**CSR リスト**」では、既定の CSR リストが SonicOS によって自動的に選択されます。複数の CSR リストが設定されている場合は、これを変更できます。

5 「**CA URL**」 フィールドに、認証局の URL を入力します。

6 「**チャレンジ パスワード (オプション)**」フィールドに、要求されている場合は CA のパスワードを入力します。

7 「**リクエスト回数**」フィールドに、リクエストの回数を入力します。既定値は **256** です。

8 「**ポーリング間隔 (秒)**」 フィールドで、ポーリング メッセージの送信間隔の既定値 (秒単位) を変更できます。既定値は **30** 秒です。

9 「**最大ポーリング時間 (秒)**」フィールドで、ファイアウォールがポーリング メッセージへの応答をタイムアウトまで待つ間隔の秒数を既定値から変更できます。既定値は **28800** 秒 (8 時間) です。

10 「**SCEP**」を選択して、SCEP 登録を提出します。

ファイアウォールは証明書をリクエストするために CA に接触します。これにかかる時間は、CA が証明書を自動または手動のどちらで発行するかに依存します。発行された証明書は、「**装置 > 証明書**」ページの「**インポートした証明書とリクエスト**」または「**すべての証明書**」種別の利用可能な証明書リスト内に表示されます。

5

時間の設定

- 「装置 > 時間」について (77 ページ)
  - システム時間の設定 (78 ページ)
  - NTP の設定 (79 ページ)

「装置 > 時間」について

「**管理 | システム セットアップ > 装置 > 時間**」では、ログ イベントのタイム スタンプ、SonicWall セキュリティ サービスの自動更新、およびその他の内部の目的で使用する時刻と日付の設定を定義します。

既定では、SonicWall セキュリティ装置は公開 NTP サーバの内部リストを使用して時刻を自動的に更新します。ネットワーク タイム プロトコル (NPT) は、コンピュータのネットワーク内でコンピュータの時刻を同期するために使用されるプロトコルです。NTP は協定世界時 (UTC) を使用してコンピュータの時計をミリ秒の分解能 (場合によってはさらに小さな単位) で同期します。

トピック:

- システム時間の設定 (78 ページ)
- NTP の設定 (79 ページ)

システム時間の設定

システム時間は、「**装置 > 時間**」の「**システム時間**」セクションで設定します。

システム時間を設定するには:

1 「**管理 | システム セットアップ > 装置 > 時間**」に移動します。

2 「**タイム ゾーン**」で、タイム ゾーンを選択します。

3 時刻を設定するには:

- 自動的に設定するには、内部リストの NTP (ネットワーク タイム プロトコル) サーバを使用することを設定する「**NTP を使用して自動的に時刻を調整する**」をオンにします。このオプションは、既定では選択されています。
- 手動で設定するには、「**NTP を使用して自動的に時刻を調整する**」をオフにします。「**時刻**」と「**日付**」のオプションが使用可能になります。

1) 「**時刻 (hh:mm:ss)**」ドロップダウン メニューを使用して 24 時間形式で時刻を選択します。

2) 「**日付**」ドロップダウン メニューで日付を選択します。

4 サマータイムの自動調整を有効にするには、「**自動的にサマータイムを調整する**」を選択します。サマータイムを使用する地域では、このオプションは既定で選択されています。

5 ログ イベントにローカル タイムではなく、協定世界時 (UTC) を使用するには、「**ログに UTC (協定世界時) を使用する**」を選択します。このオプションは、既定では選択されていません。

6 日が月より前に示される国際形式で日付を表示するには、「**国際形式で時刻を表示する**」を選択します。

このオプションは、既定では選択されていません。

7 内部リストの NTP サーバではなく、手動で入力されたリストの NTP サーバを使用してファイアウォールの時計を設定するには、「**個別 NTP サーバのみ使用する**」を選択します。

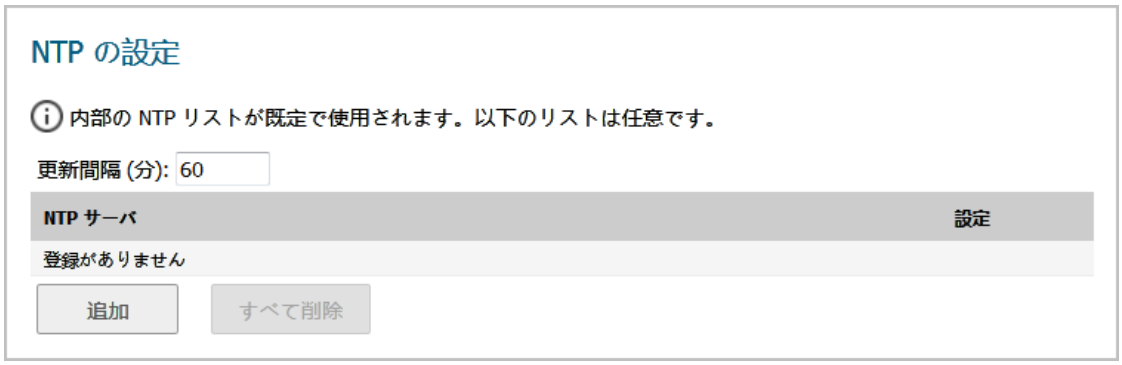
重要：1 つ以上の NTP サーバを設定済みである場合に限り、このオプションを選択してください。NTP サーバの詳細については、「NTP の設定 (79 ページ)」を参照してください。

8 「**適用**」を選択します。

NTP の設定

ネットワーク タイム プロトコル (NPT) は、コンピュータのネットワーク内でコンピュータの時刻を同期するために使用されるプロトコルです。NTP は協定世界時 (UTC) を使用してコンピュータの時計をミリ秒の分解能 (場合によってはさらに小さな単位) で同期します。

ヒント：SonicWall セキュリティ装置は NTP サーバの内部リストを使用します。このため、手動による NTP サーバの入力はオプションです。



トピック:

- NTP サーバを使用したファイアウォールの時計の更新 (79 ページ)
- NTP サーバの追加 (80 ページ)
- NTP サーバ エントリの編集 (80 ページ)
- NTP サーバ エントリの削除 (81 ページ)

NTP サーバを使用したファイアウォールの時計の更新

ローカル サーバを使用してファイアウォールの時計を設定するには:

1 「**管理 | システム セットアップ > 装置 > 時間**」に移動します。

2 「NTP の設定 (79 ページ)」の説明に従って 1 つ以上の NTP サーバを追加します。

3 「**時刻設定に NTP を自動的に使用する**」を選択します(「システム時間の設定 (78 ページ)」を参照してください)。このオプションは、既定では選択されていません。

4 NTP サーバがファイアウォールを更新する頻度を設定するには、「**更新間隔 (分)**」に時間間隔を入力します。既定値は **60** 分です。

5 「**適用**」を選択します。

NTP サーバの追加

ファイアウォールの設定に NTP サーバを追加するには、次の手順に従います。

1 「**管理 | システム セットアップ > 装置 > 時間**」に移動します。

2 「**NTP の設定**」セクションで、「**追加**」を選択します。「**NTP サーバの追加**」ダイアログが表示されます。

3 「**NTP サーバ**」フィールドに、リモート NTP サーバの IP アドレスを入力します。

4 「**NTP 認証種別**」ドロップダウン メニューで、認証種別を選択します。

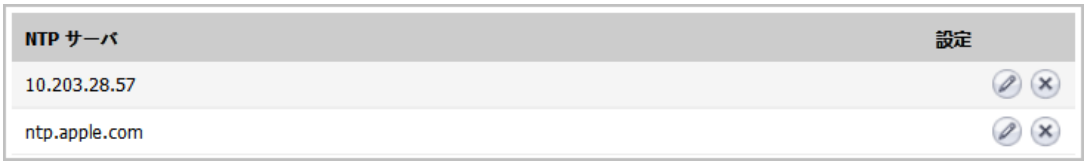
- **認証なし** - 認証は不要であり、以下の 3 つのオプションが淡色表示になります。「ステップ 8」へ進みます。
- **MD5** - 認証は必須であり、以下の 3 つのオプションはアクティブになります。

5 「**信頼鍵番号**」フィールドに信頼鍵番号を入力します。最小値は 1 で、最大値は 99999 です。

6 「**鍵番号**」フィールドに鍵番号を入力します。最小値は 1 で、最大値は 99999 です。

7 「**パスワード**」フィールドにパスワードを入力します。

8 「**OK**」を選択します。「**NTP サーバ**」セクションにサーバが表示されます。



NTP サーバ エントリの編集

NTP サーバ エントリを編集するには、以下の手順に従います。

1 「**管理 | システム セットアップ > 装置 > 時間**」に移動します。

2 「**NTP サーバ**」テーブルで、エントリの**編集**アイコンを選択します。「**NTP サーバの編集**」ダイアログが表示されます。このダイアログの内容は「**NTP サーバの追加**」ダイアログと同様です。「NTP サーバの追加 (80 ページ)」を参照してください。

3 変更を加えます。

4 「**OK**」を選択します。

NTP サーバ エントリの削除

NTP サーバ エントリを削除するには、以下の手順に従います。

1 「**管理 | システム セットアップ > 装置 > 時間**」に移動します。

2 「**NTP サーバ**」テーブルで、エントリの**削除**アイコンを選択します。

すべてのサーバを削除するには、以下の手順に従います。

3 「**管理 | システム セットアップ > 装置 > 時間**」に移動します。

4 「**NTP サーバ**」テーブルの下にある「**すべて削除**」を選択します。

6

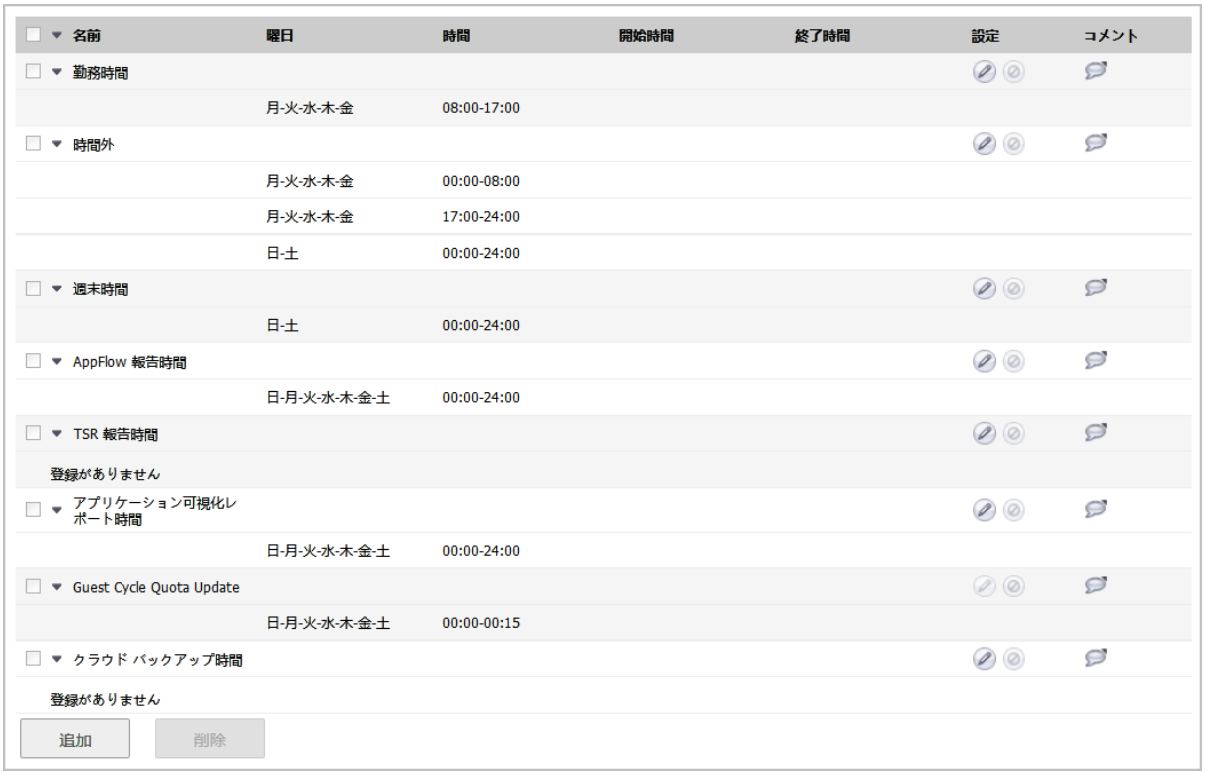
スケジュールの設定

- スケジュールについて (82 ページ)
- 「装置 > スケジュール」について (83 ページ)
  - 個別スケジュールの追加 (84 ページ)
  - スケジュールの変更 (85 ページ)
  - 個別スケジュールの削除 (86 ページ)

スケジュールについて

SonicOS では、セキュリティ機能やポリシーと組み合わせてスケジュール オブジェクトを使用します。スケジュール オブジェクトは、「**管理 | システム セットアップ > 装置 > スケジュール**」で作成します。特定のセキュリティ機能やポリシー (ルール) にスケジュール オブジェクトを適用できます。例えば、「**管理 | ポリシー > ルール > アクセス ルール**」ページでアクセス ルールを追加すると、「**ルールの追加**」ダイアログに、すべての使用可能な定義済みスケジュール オブジェクトおよび「**管理 | システム セットアップ > 装置 > スケジュール**」ページで作成したスケジュール オブジェクトが表示されます。1 つのスケジュールでのルール適用に複数の日付および時刻の追加を含めることができます。

「装置 > スケジュール」について



「管理 | システム セットアップ > 装置 > スケジュール」では、SonicWall セキュリティ装置のさまざまな機能のスケジュール時刻を設定する既定および個別のスケジュール オブジェクトを作成および管理できます。

メモ：既定のスケジュールは編集できますが、削除することはできません。

「スケジュール」テーブルには、定義済みのスケジュールと個別スケジュールがすべて表示されます。既定のスケジュールとして以下のものがあります。

勤務時間	**AppFlow 報告時間**	**クラウド バックアップ (時間単位)**
時間外	**アプリケーション可視化レポート (時間単位)**	**ゲスト サイクル クォータの更新**
週末時間	**TSR 報告時間**	

トピック:

- 個別スケジュールの追加 (84 ページ)
- スケジュールの変更 (85 ページ)
- 個別スケジュールの削除 (86 ページ)

個別スケジュールの追加

個別スケジュールを作成するには:

1 「**管理 | システム セットアップ > 装置 > スケジュール**」に移動します。

2 「**追加**」を選択します。「**スケジュールの追加**」ダイアログが表示されます。

3 「**スケジュール名**」フィールドにスケジュールの名前を入力します。

4 「**スケジュール種別**」に次のいずれかのラジオ ボタンを選択します。

1 回 「**開始**」と「**終了**」の時刻および日付を設定し、その間に一度発生するスケジュールです。これを選択すると「**1 回**」の各フィールドが使用可能になり、「**繰り返し**」の各フィールドが淡色表示になります。

繰り返し 開始と終了の日時は設定せず、時刻と曜日を設定し、その同じタイミングで繰り返し発生するスケジュールです。これを選択すると「**繰り返し**」の各フィールドが使用可能になり、「**1 回**」の各フィールドが淡色表示になります。

混在 開始と終了の日時を設定し、時刻と曜日も設定して、その期間に同じタイミングで繰り返し発生するスケジュールです。これを選択すると、ページ内のすべてのフィールドが有効になります。

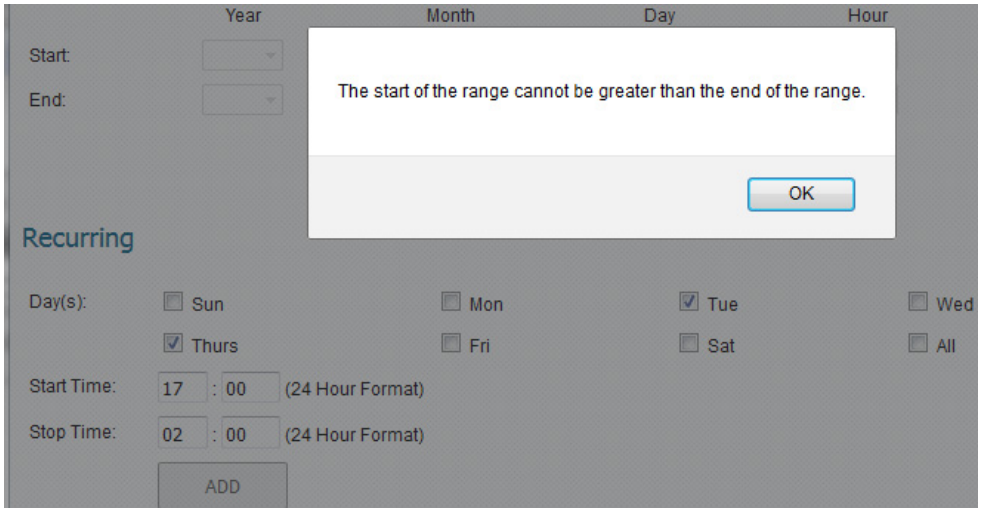
重要: 時刻は 24 時間形式 (5 p.m の場合は 17:00) にする必要があります。

5 「**1 回**」の各フィールドが使用可能な場合:

- 「**開始**」行のドロップダウン メニューから「**年**」、「**月**」、「**日**」、「**時**」、「**分**」を選択して開始日時を設定します。時間は 24 時間形式で入力してください。
- 「**終了**」行のドロップダウン メニューから「**年**」、「**月**」、「**日**」、「**時**」、「**分**」を選択して終了日時を設定します。時間は 24 時間形式で入力してください。

6 「**繰り返し**」の各フィールドが使用可能な場合:

- スケジュールに適用する曜日をチェックボックスで選択するか、「**すべて**」を選択します。
- スケジュールを開始する時刻を「**開始時刻**」フィールドに入力します。
- スケジュールを終了する時刻を「**終了時刻**」フィールドに入力します。



7 「**追加**」を選択して、スケジュールを「**スケジュール リスト**」に追加します。

8 削除するには:

- 1 つの既存のスケジュールを削除するには、「**スケジュール リスト**」から:
  1) スケジュールを選択します。
  2) 「**削除**」を選択します。
- すべての既存のスケジュールを削除するには、「**すべて削除**」を選択します。

9 「**OK**」を選択します。「**スケジュール**」テーブルの情報が更新されます。

スケジュールの変更

既定と個別の両方のスケジュールを変更するには:

1 「**管理 | システム セットアップ > 装置 > スケジュール**」に移動します。

2 変更するスケジュールの**編集**アイコンを選択します。「**スケジュールの編集**」ダイアログが表示されます。

3 スケジュールの各種構成要素 (時刻、種別、日など) を変更できます。ただし、既定のスケジュールの名前を変更することはできません。このフィールドは淡色表示になっています。変更を行うには、「個別スケジュールの追加 (84 ページ)」の手順に従います。

4 「**OK**」を選択します。

個別スケジュールの削除

個別スケジュールは削除できますが、既定のスケジュールを削除することはできません。

個々のスケジュールの削除

作成した個々のスケジュール オブジェクトを削除するには、以下の手順に従います。

1 「**管理 | システム セットアップ > 装置 > スケジュール**」に移動します。

2 「**スケジュール**」テーブルで以下の手順を実行します。

- 1 つの個別スケジュールを削除するには、そのスケジュールの**削除**アイコンを選択します。
- 複数の個別スケジュールを削除するには:
  1) 削除する個別スケジュールの横にあるチェックボックスをオンにします。「**削除**」が使用可能になります。

2) 「**削除**」を選択します。

すべてのスケジュールの削除

作成したすべてのスケジュール オブジェクトを削除するには、

1 「**管理 | システム セットアップ > 装置 > スケジュール**」に移動します。

2 「**スケジュール**」テーブルで、「**名前**」列見出しの隣にあるチェックボックスをオンにしてすべての個別スケジュールを選択します。「**削除**」が使用可能になります。

3 「**削除**」を選択します。

第 3 部

システム セットアップ | ユーザ管理

- ユーザの管理について
- ユーザの管理のための設定
- 認証パーティションの管理
- ローカル ユーザおよびグループの設定
- ゲスト サービスとゲスト アカウント
- ゲスト アカウントの管理

7

ユーザの管理について

- ユーザ管理について (89 ページ)
  - ローカル ユーザおよびローカル グループを使った認証 (91 ページ)
  - RADIUS を使った認証 (93 ページ)
  - LDAP/アクティブ ディレクトリ/イーディレクトリ認証の使用 (94 ページ)
  - TACACS+ の使用 (99 ページ)
  - シングル サインオンについて (99 ページ)
  - シングル サインオン エージェント/ターミナル サーバ エージェントのインストール (112 ページ)
  - 複数管理者サポートについて (123 ページ)
  - 複数管理者サポートの設定 (125 ページ)

ユーザ管理について

メモ：このトピックでは、SonicWall セキュリティ装置の管理機能の概要を示します。

詳細な情報と手順	参照先トピック
ユーザ認証、ウェブ ログイン、セッション管理、RADIUS アカウント、およびポリシーのセットアップ	ユーザの管理のための設定 (128 ページ)
相互接続されていない複数のドメインがある環境でのユーザ認証のためのパーティションの作成	認証パーティションの管理 (205 ページ)
ローカル ユーザおよびローカル グループの作成と管理	ローカル ユーザおよびグループの設定 (237 ページ).
ゲストサービスおよびアカウントのセットアップ	ゲスト サービスとゲスト アカウント (260 ページ)およびゲスト アカウントの管理 (265 ページ)

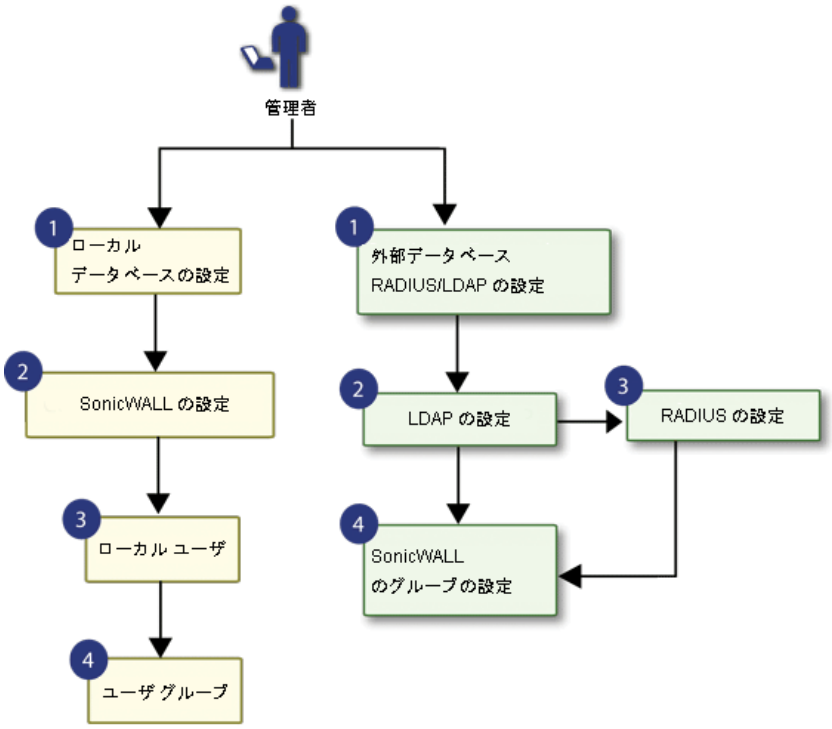
SonicWall セキュリティ装置 (ファイアウォール) は、ローカルおよびリモートで認証されるユーザを管理するためのメカニズムを備えています。ユーザ レベルの認証により、ユーザがインターネット上の離れた場所から LAN にアクセスできるようにしたり、インターネットへのアクセスを試みる LAN ユーザに対して、コンテンツ フィルタ ポリシーを適用またはバイパスしたりすることが可能になります。また、認証されたユーザだけに、VPN トンネルにアクセスし、暗号化された接続を通してデータを送信することを許可することもできます。

ユーザが異なるゾーン (WAN、VPN、WLAN など) のネットワーク リソースにアクセスしようとすると、そのユーザは直ちにファイアウォールによって認証され、ネットワーク トラフィックはそこで初めてファイアウォールを通過することになります。ユーザが LAN 上のコンピュータにログインした

としても、ローカル タスクしか実行しなければ、ファイアウォールによる認証は行われません。ユーザ レベル認証は、ローカル ユーザ データベース、LDAP、RADIUS を使って実行できるほか、ローカル データベースに LDAP または RADIUS を組み合わせて実行することもできます。ユーザ数が多いネットワークでは、LDAP サーバまたは RADIUS サーバを使った認証のほうが効率的です。

SonicOS は、さらに、シングル サイン オン (SSO) 機能を備えています。SSO を LDAP と組み合わせて使用できます。「ユーザ管理の構成」を参照してください。

ユーザ管理の構成



トピック:

- ローカル ユーザおよびローカル グループを使った認証 (91 ページ)
- RADIUS を使った認証 (93 ページ)
- LDAP/アクティブ ディレクトリ/イーディレクトリ認証の使用 (94 ページ)
- シングル サインオンについて (99 ページ)
- シングル サインオン エージェント/ターミナル サーバ エージェントのインストール (112 ページ)
- 複数管理者サポートについて (123 ページ)
- 複数管理者サポートの設定 (125 ページ)

ローカル ユーザおよびローカル グループを使った認証

トピック:

- ユーザ データベースについて (91 ページ)
- ユーザ グループについて (92 ページ)

ユーザ データベースについて

このファイアウォールは、ユーザやグループの情報を格納するためのローカル データベースを備えています。このローカル データベースを使ってユーザを認証したり、ネットワークへのアクセスを制御したりするようにファイアウォールを設定できます。ネットワークにアクセスするユーザ数が比較的少ない場合は、LDAP または RADIUS ではなく、ローカル データベースの使用をお勧めします。一度作成してしまえば管理はさほど難しくありませんが、多数のユーザやグループのエントリを作成するには時間がかかります。

ファイアウォール上のローカル データベースでサポートされるユーザ数は、プラットフォームによって異なります。「プラットフォームごとのサポートされる最大ユーザ数」テーブルにこれを示します。ユーザ総数の最大上限は SSO ユーザの最大数と同じで、ネイティブ ユーザの最大数は SSO ユーザの最大数と同じです。ウェブ ユーザの最大数は、ウェブからのユーザ ログインと、GVC、SSL-VP、および L2TP クライアントからのユーザ ログインの最大合計数です。

プラットフォームごとのサポートされる最大ユーザ数

プラットフォーム	SSO ユーザ数	ウェブ ユーザ数	ウェブ サーバ スレッド数	プラットフォーム	SSO ユーザ数	ウェブ ユーザ数	ウェブ サーバ スレッド数
NS*a* 6650	70,000	5,000	20	NS*a* 9650	100,000	5,000	30
NS*a* 5650	60,000	3,000	16	NS*a* 9450	90,000	5,000	30
NS*a* 4650	50,000	2,000	10	NS*a* 9250	80,000	5,000	20
NS*a* 3650	40,000	1,500	8				
NS*a* 2650	30,000	1,000	8	Super Massive 9600	100,000	5,000	30
				Super Massive 9400	90,000	5,000	30
NSA 6600	70,000	5,000	20	Super Massive 9200	80,000	5,000	20
NSA 5600	60,000	3,000	16				
NSA 4600	50,000	2,000	10	TZ600/TZ600P	500	500	8
NSA 3600	40,000	1,500	8	TZ500/TZ500W	500	500	8
NSA 2600	30,000	1,000	8	TZ400/TZ400W	500	150	8
				TZ350/TZ350W	500	150	8
				TZ300/TZ300W/TZ300P	500	150	8
				SOHO 250/250W	350	150	8
				SOHO W	250	150	8

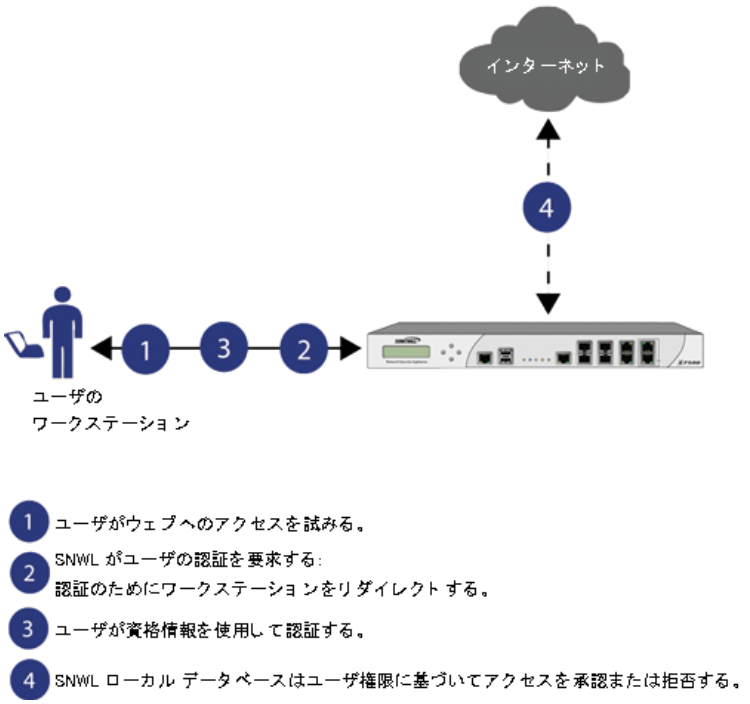
重要：これらの数を処理する際の効率を最大にするための、SonicWall の推奨事項は以下のとおりです。

- 無線ユーザに対しては、可能な限り RADIUS アカウントを使用します。
- SSO エージェント バージョン 4 以上を使用します。バージョン 3.6.10 よりも古い SSO エージェントを使用しないでください。
- 可能であれば、SSO エージェントを LogWatcher 付きの DC ログ モードで使用します。
- 非ドメイン ユーザの識別に NetAPI または WMI が必要な場合は、個別のエージェントでそれを行ってください。
- 可能ならば、SSO によって識別できないものが SSO を開始することがないように、除外を設定します。

ユーザ グループについて

コンテンツ フィルタ サービス (CFS) のポリシーをユーザに適用するには、そのユーザがローカル グループのメンバーであることが必要です。そうすれば、CFS ポリシーがそのグループに適用されます。CFS を使用する場合、LDAP または RADIUS を単独で使用することはできません。LDAP または RADIUS に、ローカル認証を組み合わせて使用する必要があります。CFS ポリシーを使用するために認証方式を組み合わせる場合、ローカルのグループ名と LDAP または RADIUS のグループ名とを完全に一致させる必要があります。「**LDAP + ローカル ユーザ**」の認証方式を使用する場合、LDAP サーバからファイアウォール上のローカル データベースにグループをインポートできます。こうすることで、対応するグループを簡単に作成できます。 対応するグループを作成すれば、CFS ポリシーを適用できるようになります。「ユーザ管理: ローカル ユーザおよびローカル グループを使った認証」を参照してください。

ユーザ管理: ローカル ユーザおよびローカル グループを使った認証



ローカル ユーザおよびグループのアカウントは、SonicOS 管理インターフェースから作成できます。ユーザを追加できるほか、任意のユーザの設定を編集することも可能です。例えば、次のような設定を編集できます。

グループ メンバーシップ	ユーザは 1 つまたは複数のローカル グループに所属できます。既定では、すべてのユーザが **Everyone** グループおよび **Trusted Users** グループに所属します。ユーザからこれらのグループ メンバーシップを削除したり、他のグループのメンバーシップを追加したりできます。
VPN アクセス	ユーザによって開始された VPN クライアントがアクセス可能なネットワークを設定できます。VPN アクセスを設定する際は、ネットワークのリストから選択できます。ネットワークは、対応するアドレス グループまたはアドレス オブジェクトの名前で指定します。 **メモ：**ユーザとグループに対する VPN アクセス設定は、GVC、NetExtender および SSL VPN 仮想オフィス ブックマークを使ってネットワーク リソースにアクセスするリモート クライアントの能力に影響します。GVC、NetExtender、または、仮想オフィスのユーザがネットワーク リソースへアクセスすることを許可するには、ネットワーク アドレス オブジェクトかグループを、「VPN アクセス」タブの "許可" リストに追加する必要があります。

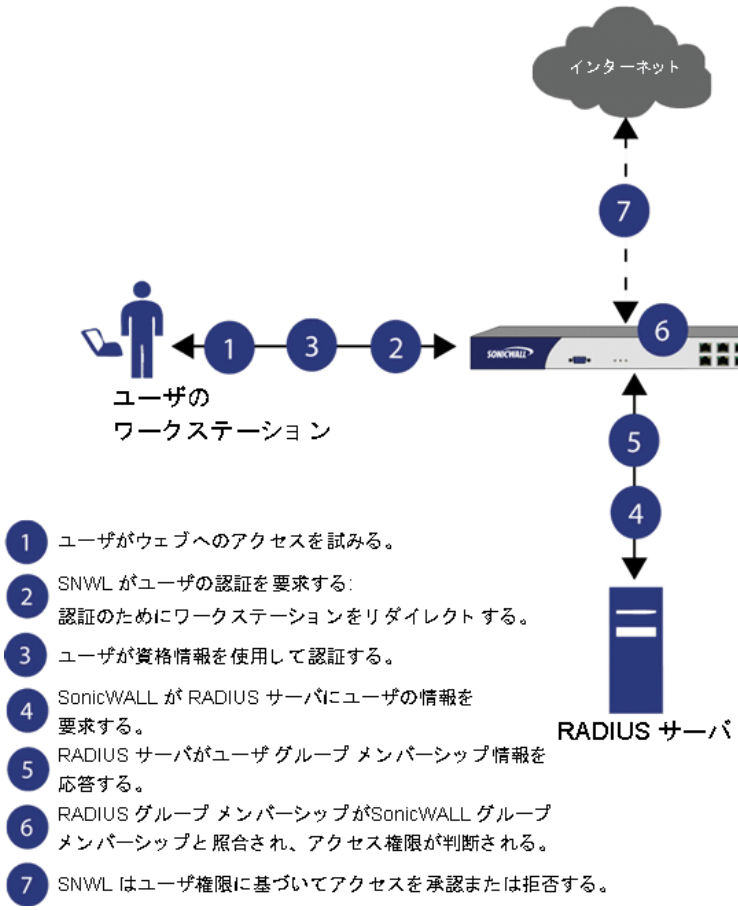
ローカル グループを追加したり編集したりすることもできます。グループでは、次のような設定を編集できます。

グループ設定	管理者グループに対して、ログイン状況ポップアップ ウィンドウをアクティブにすることなく管理インターフェースへのログインを許可するよう、SonicOS を設定することができます。
グループ メンバー	グループのメンバーとして、ローカル ユーザまたは他のローカル グループを追加できます。
VPN アクセス	グループの VPN アクセスは、ユーザの VPN アクセスと同じ方法で設定できます。このグループのメンバーによって開始された VPN クライアントがアクセス可能なネットワークを設定できます。VPN アクセスを設定する際は、ネットワークのリストから選択できます。ネットワークは、対応する**アドレス グループ**または**アドレス オブジェクト**の名前で指定します。
CFS ポリシー	グループのメンバーに対して、コンテンツ フィルタ (CFS) ポリシーを適用できます。CFS ポリシー設定を利用するには、ファイアウォールでプレミアム コンテンツのフィルタ サービスを利用するためのライセンスが必要です。

RADIUS を使った認証

RADIUS (リモート認証ダイヤルイン ユーザ サービス) は、ネットワークへのアクセスを試みるユーザを SonicWall セキュリティ装置および SonicWave 装置が認証するための一元化された認証、承認、アカウンティングの機能を提供するネットワーク プロトコルです。RADIUSサーバには、ユーザ情報を格納したデータベースが存在します。RADIUS サーバは、PAP (パスワード認証プロトコル)、CHAP (チャレンジ ハンドシェーク認証プロトコル)、MSCHAP (Microsoft CHAP)、MSCHAPv2 などの認証スキームを使ってユーザの資格情報をチェックします。「ユーザ管理: RADIUS を使った認証」を参照してください。RADIUS 認証を提供する SonicWave 装置については、『*SonicOS 6.5 接続*』を参照してください。

ユーザ管理: RADIUS を使った認証



RADIUS は LDAP とは大きく異なり、主として安全な認証機能を実現するものですが、ユーザ グループのメンバーシップを渡すのに使用できるさまざまな属性など、エントリごとに非常に多くの属性が用意されています。RADIUS では、数千人規模のユーザ情報を格納できるため、ネットワーク アクセスを必要とするユーザ数が多い場合のユーザ認証として最適です。

LDAP/アクティブ ディレクトリ/イーディレクトリ認証の使用

LDAP (Lightweight Directory Access Protocol) は、例えばユーザ アカウント、ユーザ グループ、ホスト、サーバといったネットワーク上の要素についての情報を格納および管理するためのディレクトリ サービス構造を定義します。ユーザ アカウント、グループ、権限などを管理するために LDAP を使用する標準はいくつか存在します。一部は独自システムで、LDAP による管理が可能な Microsoft アクティブ ディレクトリ (AD) や、ユーザ リポジトリ情報を管理するための LDAP API を提供するノベル イーディレクトリなどがあります。また一部はオープン規格で、LDAP 標準の実装である SAMBA などがあります。

SonicOS は、RADIUS やローカル ユーザ データベースに加えて、ユーザ認証用に LDAP をサポートします。マイクロソフト アクティブ ディレクトリやノベル イーディレクトリのディレクトリ サービスを含む多数のスキーマをサポートするほか、完全に設定可能なユーザ定義のオプションによって、SonicOS があらゆるスキーマとやり取りできるようにします。

Microsoft アクティブ ディレクトリは、SonicWall シングル サインオンおよび SonicWall SSO エージェントとも連携して動作します。詳細については、「シングル サインオンについて (99 ページ)」を参照してください。

トピック:

- LDAP 用語 (95 ページ)
- SonicOS でサポートされる LDAP ディレクトリ サービス (96 ページ)
- LDAP ユーザ グループ ミラーリング (96 ページ)

LDAP 用語

LDAP およびその変種に関連して使用される用語を以下に示します。

アクティブ ディレクトリ (AD)	Microsoft のディレクトリ サービスで、一般的に Windows ベースのネットワークで使用されます。Microsoft アクティブ ディレクトリは LDAP 互換です。
項目	LDAP ディレクトリ内のオブジェクトに格納されるデータ アイテム。オブジェクトは、必須の属性、または、任意の属性を持つことができます。例えば、dc 属性は、dcObject (ドメイン構成要素) オブジェクトの必須の属性です。
cn	コモンネーム (common name) 属性。LDAP 全体にわたって多くのオブジェクト クラスの必須構成要素です。
dc	ドメイン構成要素 (domain component) 属性。識別名のルートによく見られ、多くの場合は必須の属性です。
dn	識別名 (distinguised name) であり、ユーザまたはその他のオブジェクトのグローバルに一意な名前。複数の構成要素から成り、通常は、コモンネーム (cn: common name) 構成要素で開始し、2 つ以上のドメイン構成要素 (dc: domain component) として指定されたドメインで終了します。例えば、cn=john,cn=users,dc=domain,dc=com となります。
eDirectory	ノベルのディレクトリ サービスで、ノベル ネットウェアベースのネットワークで使用されます。ノベル イーディレクトリは、管理用に使用できる LDAP ゲートウェイを持っています。
エントリ	LDAP ディレクトリに格納されているデータ。エントリは、属性/値 (または名前/値) の組で格納されます (属性はオブジェクト クラスにより定義されます)。例えば、cn=john の場合、cn (コモンネーム) が属性、john が値となります。
オブジェクト	LDAP 用語では、ディレクトリ内のエントリをオブジェクトと呼びます。LDAP クライアントの SonicOS 実装の目的上、重要なオブジェクトは、ユーザ オブジェクトとグループ オブジェクトです。LDAP の実装によって、これらのオブジェクト クラスは異なる名前で呼ばれる場合があります。例えば、アクティブ ディレクトリでは、ユーザ オブジェクトは user、グループ オブジェクトは group と呼ばれるのに対し、RFC2798 では、ユーザ オブジェクトは inetOrgPerson、グループ オブジェクトは groupOfNames と呼ばれます。
オブジェクト クラス	LDAP ディレクトリに格納できるエントリの種別を定義します。例えば、AD で使用されるオブジェクト クラスとして、user や group があります。 Microsoft アクティブ ディレクトリのクラスは、http://msdn.microsoft.com/library/ で参照することができます。
ou	組織単位 (organization unit) 属性。ほとんどの LDAP スキーマ実装の必須構成要素です。

スキーマ	ディレクトリに格納できるデータの種別やデータの格納方法を定義するルールのセットまたは構造です。データは、エントリの形式で格納されます。
TLS	トランスポート層セキュリティ (Transport Layer Security)。SSL (Secure Sockets Layer) の IETF で標準化されたバージョンです。TLS 1.1 と 1.2 がサポートされています。

SonicOS でサポートされる LDAP ディレクトリ サービス

企業のネットワークで使用される最も一般的なディレクトリ サービスと統合するために、SonicOS では、以下の LDAP スキーマとの統合をサポートしています。

Microsoft アクティブ ディレクトリ	サンバ SMB
RFC2798 InetOrgPerson	ノベル イーディレクトリ
RFC2307 ネットワーク インフォメーション サービス	ユーザ定義スキーマ

SonicOS は、以下のプロトコルが実行されるディレクトリ サービスのサポートを提供します。

LDAPv3 (RFC2251～2256、RFC3377)	LDAPv2 (RFC3494)
LDAPv3 over TLS (RFC2830)	LDAP Referrals (RFC2251)
LDAPv3 with STARTTLS (RFC2830)	

LDAP ユーザ グループ ミラーリング

LDAP ユーザ グループ ミラーリングは、LDAP ユーザ グループの設定を LDAP サーバから SonicWall セキュリティ装置に自動的に複製する機能です。LDAP ユーザ グループを LDAP サーバ上でだけ管理すればよく、設定をファイアウォールに手動で複製する必要はありません。ユーザ グループの設定は、LDAP サーバから定期的に読み取られてファイアウォールにコピーされます。

ファイアウォールにコピーされる LDAP ユーザ グループ名には、ドメイン名が名前@ドメイン.com の形式で含まれます。したがって、どのドメインからのユーザ グループ名もすべて一意に識別されます。

ミラーされた LDAP ユーザ グループには、以下の機能と制限が適用されます。

- LDAP ユーザ グループの削除は、LDAP サーバ上でのみ行えます。SonicWall セキュリティ装置上のミラーされた LDAP ユーザ グループを削除することはできません。LDAP サーバ上でユーザ グループを削除すると、ファイアウォール上のミラーされたグループも自動的に削除されます。
- LDAP ユーザ グループ名 (およびそのコメント フィールド) の編集は、LDAP サーバ上でのみ行えます。ファイアウォール上のミラーされた LDAP ユーザ グループ名またはそのコメント フィールドを編集することはできません。ファイアウォール上のコメント フィールドには「LDAP より転写」と表示されます。
- SonicWall セキュリティ装置上の LDAP ユーザ グループのメンバーとしてユーザを追加できます。
- SonicWall セキュリティ装置上の他のグループにグループを追加することはできません。既定のユーザ グループの設定は、LDAP サーバ上でのみ行えます。

- SonicWall セキュリティ装置上の LDAP ユーザ グループに対して、VPN、SSL VPN、CFS ポリシー、ISP ポリシーなどを設定できます (ポリシーの詳細については、『*SonicOS 6.5 ポリシー*』を参照してください)。

  メモ：LDAP ユーザ グループは、アクセス ルール、アプリケーション制御ルール、または他のポリシー内で設定されている場合には削除されません。

- 「LDAP ユーザ グループ ミラーリング」を無効にすると、SonicWall セキュリティ装置上のミラーされたユーザ グループは削除されません。これらのグループは変更されているため、手動で削除できます。手動で削除されていない、ユーザ グループのローカルの複製は、再度有効にできます。
- SonicWall セキュリティ装置上に作成するグループの複製の名前と、ユーザの作成した (非複製の) 既存のローカル グループの名前が同じでも、ローカル グループは置き換えられません。ローカル グループのメンバーシップは、LDAP サーバ上で設定されているグループの設定を反映するように更新されます。
- LDAP サーバ上のユーザ グループの名前と、SonicWall セキュリティ装置上の既定のユーザ グループの名前が同じ場合、SonicWall セキュリティ装置上にユーザ グループのミラーは作成されません。既定のユーザ グループのメンバーシップは、LDAP サーバ上で設定されているグループの設定を反映するように更新されます。
- SonicOS 6.2 以前に作成されたグループについては、SonicWall セキュリティ装置上にシンプルな名前のみを持つ (ドメインなし) ローカル ユーザ グループが存在し、その名前が LDAP サーバ上のユーザ グループの名前 (ドメインを含む) と同じ場合、SonicWall セキュリティ装置上に新しいローカル ユーザ グループが作成され、LDAP サーバ上の対応するユーザ グループと同じドメインが割り当てられます。元のローカル ユーザ グループはドメインが無いまま保持されます。元のグループ内のユーザには、その LDAP グループ、新しくローカルにミラーされたグループ、そして元のローカル グループ (ドメイン名なし) のメンバーシップが与えられます。

SonicWall セキュリティ装置への LDAP の統合

ファイアウォールを LDAP ディレクトリ サービスと統合するには、証明書管理のための設定が LDAP サーバに必要となります。さらに、ファイアウォールに正しい証明書をインストールし、LDAP サーバからの情報を使用できるように設定する必要があります。LDAP の概要については、「LDAP/アクティブ ディレクトリ/イーディレクトリ認証の使用 (94 ページ)」を参照してください。

トピック:

- 統合に向けての LDAP サーバの準備 (97 ページ)
- アクティブ ディレクトリ サーバでの CA の設定 (98 ページ)

統合に向けての LDAP サーバの準備

LDAP の設定を行う前に、LDAP over TLS をサポートするように LDAP サーバと SonicWall を準備する必要があります。これには次の操作が必要です。

- LDAP サーバにサーバ証明書をインストールする。
- ファイアウォールに発行元 CA の CA (Certificate Authority) 証明書をインストールする。

次の手順は、これらのタスクをアクティブ ディレクトリ環境で行う方法を示しています。

アクティブ ディレクトリ サーバでの CA の設定

アクティブ ディレクトリ サーバで CA を設定するには、以下の手順に従います。

ヒント：証明書サービスが既にインストールされている場合、最初の 5 つの手順はスキップしてください。

1 「**スタート > 設定 > コントロール パネル > プログラムの追加と削除**」を選択します。

2 「**Windows コンポーネントの追加と削除**」を選択します。

3 「**証明書サービス**」を選択します。

4 要求されたら「**エンタープライズのルート CA**」を選択します。

5 必要な情報を入力します。Windows システムでの証明書については、http://support.microsoft.com/kb/931125 を参照してください。

6 「**ドメイン セキュリティ ポリシー**」アプリケーションを起動します。「**スタート> ファイル名を指定して実行**」を選択し、**dompol.msc** コマンドを実行します。

7 「**セキュリティの設定 > 公開キーのポリシー**」を選択します。

8 「**自動証明書要求の設定**」を右クリックします。

9 「**新規作成 > 自動証明書要求**」を選択します。

10 ウィザードの指示に従い、リストから「**ドメイン コントローラ**」を選択します。

アクティブ ディレクトリ サーバからの CA 証明書のエクスポート

AD サーバから CA 証明書をエクスポートするには、次の手順に従います。

1 「**証明機関**」アプリケーションを起動します。「**スタート > ファイル名を指定して実行 > certsrv.msc**」を選択します。

2 作成した CA 上で右クリックし、「**プロパティ**」を選択します。

3 「**一般**」タブで、「**証明書の表示**」を選択します。

4 「**詳細設定**」タブで、「**ファイルにコピー**」を選択します。

5 ウィザードの指示に従い、「**Base 64 encoded X.509 (CER)**」形式を選択します。

6 証明書を保存するパスとファイル名を指定します。

SonicOS への CA 証明書のインポート

SonicOS に CA 証明書をインポートするには、次の手順に従います。

1 「**システム > CA 証明書**」を選択します。

2 「**新規 CA 証明書の追加**」を選択します。エクスポートした証明書を参照して選択します。

3 「**証明書のインポート**」を選択します。

組織単位別 LDAP グループ メンバーシップ

組織単位ごとの LDAP グループ メンバーシップ機能は、LDAP サーバ上の組織単位 (OU) 内に配置されたユーザに対して LDAP ルールとポリシーを設定する機能を提供します。

ユーザがログインするときに、ユーザ グループが LDAP 位置によるメンバーシップを許可するように設定されている場合、そのユーザは LDAP 位置に一致するすべてのグループのメンバーになります。

既定のローカル グループ (**Everyone** グループと **Trusted Users** グループを除く) を含むどのローカル グループも、LDAP ディレクトリ ツリー内の位置によって設定されるメンバーを持つグループとして設定可能です。

ユーザが、LDAP 位置に対して設定されているいずれかのローカル グループのメンバーである場合は:

- LDAP ツリー内のそれらのローカル グループの位置が取得されます。
- そのユーザのローカル グループの位置が、他のすべてのローカル グループに対してチェックされます。ユーザのメンバーシップ グループと同じ LDAP 位置を持つ他のグループが存在する場合、ユーザはそのログイン セッションにおいて、自動的にそれらのグループのメンバーとして設定されます。

ユーザがログインを試行するとき、成功失敗にかかわらずユーザの識別名がイベント ログに記録されます。このイベント ログは、ユーザが期待されるグループのメンバーシップを取得できなかった場合のトラブルシューティングに役立ちます。

TACACS+ の使用

SonicOS は、TACACS+ (Terminal Access Controller Access-Control System の最新世代) をユーザの認証に使用します。TACACS+ の主な特徴は次のとおりです。

- 認証、承認、およびアカウント (AAA) サービスを個別に提供。
- その転送に TCP を使用。
- TACACS+ 本体全体を暗号化によって保護可能。

シングル サインオンについて

トピック:

- シングル サイン オンとは (99 ページ)
- SonicWall SSO のメリット (100 ページ)
- プラットフォームおよびサポートされている標準 (101 ページ)
- シングル サイン オンの動作 (102 ページ)
- SSO エージェントの動作 (104 ページ)
- ターミナル サービス エージェントの動作 (106 ページ)
- ブラウザ NTLM 認証の動作 (108 ページ)
- RADIUS アカウント シングル サインオンの動作 (109 ページ)

シングル サイン オンとは

シングル サインオン (SSO) とは、ワークステーションへのシングル ドメイン ログインか、あるいは Windows ターミナル サービスまたは Citrix サーバを通じて、複数のネットワーク リソースに特権的にアクセスできるようにする透過的なユーザ認証メカニズムです。

SonicWall セキュリティ装置は、シングル サインオン エージェント (SSO エージェント) と SonicWall ターミナル サービス エージェント (TSA) を使用して SSO 機能を提供し、ユーザのアクティビティを識別します。SSO エージェントは、ワークステーションの IP アドレスに基づいてユーザを識別します。TSA は、サーバの IP アドレスとユーザ名とドメインの組み合わせによってユーザを識別します。

SonicWall SSO は、Samba と共に使用する場合は Mac および Linux ユーザに対しても利用可能です。さらに、ブラウザ NTLM 認証により SonicWall SSO は、SSO エージェントや Samba を必要とせずに、HTTP トラフィックを送信するユーザを認証できます。

SonicWall SSO の設定は、SonicOS 管理インターフェースの「**管理 | システム セットアップ > ユーザ > 設定**」ページで行います。SSO は、**ログイン認証方式設定**とは独立しており、両者を同時に使用して VPN/L2TP クライアント ユーザまたは管理者ユーザの認証を行うことができます。

SonicWall セキュリティ装置は、 SSO エージェントまたは TSA からのデータに基づき、LDAP またはローカル データベースに対してグループのメンバーシップを問い合わせます。必要に応じて、メンバーシップをファイアウォール ポリシーと照合し、アクセス権を持つユーザを制御します。 また、コンテンツ フィルタおよびアプリケーション制御用のポリシーの選択に使用して、アクセスを許可する対象を制御することができます。UNIX SSO で取得したユーザ名は、ユーザからのトラフィックやイベントに関するログで報告され、さらに AppFlow 監視でも報告されます。

無動作タイムアウトは SSO にも適用されますが、セッション時間の制限は適用されません。 ログアウトしたユーザから再びトラフィックが送信されると、そのユーザが自動的かつ透過的に再度ログインされます。

ドメインにログインせずに、ワークステーションまたはターミナル サービス/Citrix サーバに直接ログインしたユーザは、ブラウザ NTLM 認証が有効で HTTP トラフィックを送信しない限り認証されません (必要に応じて、限定的なアクセスを認証することはできます)。SonicWall SSO で認証されていない場合、以降の認証には手動でのセキュリティ装置へのログインが必要であるという内容のメッセージが表示されます。

ユーザとして識別されたとしても、設定されているポリシー ルールに必要なグループ メンバーシップが不足している場合、アクセスが拒否されたことを示すページにリダイレクトされます。

SonicWall SSO のメリット

SonicWall SSO は、管理者によって設定されたグループ メンバーシップとポリシー照合に基づき、ユーザが 1 回のログインで複数のネットワーク リソースにアクセスできるようにする信頼性に優れた機能です。何度もログインする手間が省けるため、時間の節約にもつながります。エンド ユーザが SonicWall SSO の存在を意識する必要はなく、また、管理者に要求される設定も最小限で済みます。

SonicWall SSO では、ユーザがいつログインし、いつログアウトしたかが、ワークステーション IPアドレスのトラフィック (ターミナル サービスまたは Citrix の場合は、サーバ IP アドレスの特定のユーザからのトラフィック) に基づいて自動的に判別されるため、セキュリティに優れ、手間もかかりません。SSO 認証は、SonicWall ディレクトリ コネクタ互換のプロトコルを使用することで、ワークステーションまたはターミナル サービス/Citrix サーバの IP アドレスを持ったユーザの ID を返すことができるエージェントであれば、どのような外部エージェントとでも連携できるように設計されています。

SonicWall SSO は、コンテンツ フィルタ サービス (CFS)、アクセス ルール、グループのメンバーシップと継承、セキュリティ サービス (IPS、GAV、アンチスパイウェア) の包含/除外リストを含め、ユーザ レベル認証が使用されるファイアウォール上のあらゆるサービスに使用できます。

SonicWall SSO エージェントは LAN 上の任意の Windows サーバにインストールでき、TSA は任意のターミナル サーバにインストールできます。SonicWall SSO のその他のメリット:

使いやすさ	ユーザは 1 回サインインするだけで複数のリソースに自動的にアクセスできます。
ユーザ エクスペリエンスの向上	どのような種類のトラフィックを使用するユーザでも、Windows ドメインの資格情報を使用して認証が可能であるため、ウェブ ブラウザを使って装置にログインする必要がありません。
透過性	ユーザが認証のためにユーザ名やパスワードを何度も再入力する必要がなくなります。
セキュアな通信	共有鍵暗号化によってデータ伝送を保護します。
複数の SSO エージェント	最大 8 つのエージェントをサポートして、大規模インストールに適した容量を提供します。
複数の TSA	複数のターミナル サービス エージェント (ターミナル サーバ毎に 1 つ) がサポートされます。サポートされる数は 8 ～ 512 で、SonicWall セキュリティ装置のモデルによって異なります。
ログイン メカニズム	HTTP だけでなくあらゆるプロトコルに対応しています。
ブラウザ NTLM 認証	SonicWall SSO は、SSO エージェントを使わずに HTTP トラフィックを送信するユーザを認証できます。
Mac および Linux サポート	Samba 3.5 以降で、SonicWall SSO は Mac および Linux ユーザに対してサポートされます。
ゾーン単位の執行	SonicWall SSO は、ファイアウォール アクセス ルールかセキュリティー サービス ポリシーによって自動的に開始されない場合でも、任意のゾーンからのトラフィックに対して開始でき、イベントのログ記録や AppFlow 監視用にユーザを識別します。

プラットフォームおよびサポートされている標準

SSO エージェントは、SonicOS SSO をサポートしている SonicWall の全バージョンと互換性があります。SonicWall TSA もサポートされています。

SSO 機能は、LDAP およびローカル データベース プロトコルをサポートします。SonicWall SSO は、SonicWall ディレクトリ コネクタをサポートしています。SonicWall SSO の全機能を正しく動作させるには、SonicOS とディレクトリ コネクタ 3.1.7 以降を使用してください。

SonicWall SSO を Windows ターミナル サービスまたは Citrix で使用するには、SonicOS 6.0 以降が必要であり、SonicWall TSA をサーバにインストールする必要があります。

SonicWall SSO をブラウザ NTLM 認証で使用するには、SonicOS6.0 以降が必要です。ブラウザ NTLM 認証に対しては、SSO エージェントは不要です。

ブラウザ NTLM 認証のみを使うときを除いて、SonicWall SSO を使用するには、SSO エージェントが Windows ドメイン内のサーバ (そのサーバからクライアントに、そして装置からそのサーバに、直接または VPN パス経由で到達できなければならない) にインストールされているか、TSA がドメイン内のターミナル サーバにインストールされているか、あるいはその両方が必要です。

SSO エージェントを実行するには、次の要件が満たされている必要があります。

- UDP ポート 2258 (既定) が開放されていること。 既定では、ファイアウォールと SonicWall SSO エージェントとの通信に UDP ポート 2258 が使用されます。 2258 に代わって別のポートが設定されている場合は、そのポートにこの要件が適用されます。
- Windows Server (最新のサービス パック)
- .NET Framework 2.0

- Net API または WMI

メモ：Mac および Linux の PC は、SSO エージェントが使用する Windows のネットワーク要求をサポートしていないので、SonicWall SSO と動作するには Samba 3.5 以降が必要です。Samba がなくても、Mac および Linux ユーザはまだアクセス可能ですが、ログインしてそうする必要があります。認証を要求するようポリシー ルールが設定されている場合は、ログイン プロンプトにリダイレクトされることがあります。詳細については、「Mac ユーザおよび Linux ユーザへの対応 (118 ページ)」を参照してください。

TSA を実行するには、次の要件が満たされている必要があります。

- TSA がインストールされているすべてのターミナル サーバで UDP ポート 2259 (既定) が開放されていること。 既定では、ファイアウォールと SonicWall TSA との通信に UDP ポート 2259 が使用されます。 2259 に代わって別のポートが設定されている場合は、そのポートにこの要件が適用されます。
- Windows Server (最新のサービス パック)
- Windows ターミナル サービスまたは Citrix が Windows ターミナル サーバ システムにインストールされていること

シングル サイン オンの動作

エンド ユーザが SonicWall SSO の存在を意識する必要はなく、また、管理者に要求される設定も最小限で済みます。

SSO は、以下の状況で開始されます。

- ユーザ認証を要求するファイアウォール アクセス ルールが、WAN ゾーンから着信するのではないトラフィックに適用される場合。
- アクセス ルールにユーザ グループが指定されていなくても、以下のいずれかの条件が成立すると、これらの条件に従うトラフィックだけでなく、ゾーン上のすべてのトラフィックで SSO が開始されます。
    - ゾーン上で CFS が有効で、CFS ポリシーが設定されている
    - ゾーン上で IPS が有効で、認証が必要な IPS ポリシーがある
    - ゾーン上でアンチスパイウェアが有効で、認証が必要なアンチスパイウェア ポリシーがある
    - 送信元ゾーンに対して、認証が必要なアプリケーション制御ポリシーが適用されている
    - ゾーンに対して SSO のゾーン単位の執行が設定されている

SSO ユーザ テーブルはまた、コンテンツ フィルタ、侵入防御、アンチスパイウェア、およびアプリケーション制御を含むセキュリティ サービスが必要とするユーザとグループの識別のために使用されます。

SSO エージェントを使用した SonicWall SSO 認証

個々の Windows ワークステーションのユーザについては、SSO ワークステーション上の SSO エージェントがファイアウォールからの認証要求を処理します。SSO エージェントを使用した SonicWall SSO 認証は 6 つのステップで行われます。

SSO 認証プロセスは、ユーザ トラフィックがファイアウォールを通過した時点 (ユーザがインターネットにアクセスしたときなど) で開始されます。例えば、ユーザがインターネットにアクセスした場合などです。送信されたパケットは一時的に遮断され、ファイアウォールが、SSO エージェント

(SSO ワークステーション) を実行する認証エージェントに "ユーザ名" 要求とワークステーションの IP アドレスを送信する間保存されます。

SSO エージェントを実行している認証エージェントは、ファイアウォールに対し、現在ワークステーションにログインしているユーザ名を提供します。RADIUS や LDAP と同様、ユーザ IPテーブルには、ログインしたユーザのエントリが作成されます。

ターミナル サービス エージェントを使用した SonicWall SSO 認証

ターミナル サービスまたは Citrix サーバからログインするユーザについては、認証プロセスで TSA が SSO エージェントの代わりをします。このプロセスは以下の点が異なります。

- TSA はユーザのログイン先のサーバで実行され、ファイアウォールへの初期通知にユーザ名とドメインとサーバ IP アドレスを含めます。
- ユーザはユーザ番号と IP アドレスによって識別されます (ただし、非ターミナル サービス ユーザの場合は、どの IP アドレスにもユーザが 1 つしか存在しないので、ユーザ番号は使用されません)。ゼロ以外のユーザ番号は、SonicOS 管理インターフェースに「*x.x.x.x user n*」という形式で表示されます (*x.x.x.x* はサーバ IP アドレスで、*n* はユーザ番号です)。
- ユーザがログアウトすると、TSA は SonicOS に通知を送信します。したがって、ポーリングは行われません。

ユーザが識別されると、セキュリティ装置が LDAP またはローカル データベース (管理者の設定による) に対して問い合わせを行い、ユーザ グループのメンバーシップを検索して、そのメンバーシップとポリシーとを照合し、その結果に基づいて、ユーザにアクセスを許可または拒否します。ログイン シーケンスが正常に完了した場合、保存されていたパケットが送信されます。ログイン シーケンスが完了する前に、同じ送信元アドレスからパケットを受信した場合は、最新のパケットだけが保存されます。

SSO エージェントを実行する認証エージェントからは、ユーザ名が<domain>/<user-name>の形式で返されます。ローカルで設定したユーザ グループについては、ユーザ名を以下のどちらかに設定できます。

- SSO エージェントを実行する認証エージェントから返されるフル ネーム (この場合は、ファイアウォールのローカル ユーザ データベース内の名前も一致するように設定します)。
- ドメイン要素を除去した簡易ユーザ名 (既定)。

LDAP プロトコルの場合、ドメイン名と一致する dc (ドメイン構成要素) 属性を持った“ドメイン"クラスのオブジェクトを探すための LDAP 検索を作成して、<domain>/<user-name> 形式をLDAP 識別名に変換します。目的のオブジェクトが見つかった場合、その識別名をディレクトリのサブツリーとして使用し、ユーザのオブジェクトを検索します。例えば、ユーザ名が SV/bob と返された場合、objectClass=domain かつ dc=SV というオブジェクトが検索されます。ここで、“dc=sv,dc=us,dc=sonicwall,dc=com"という識別名を持つオブジェクトが返された場合は、そのディレクトリ サブツリー下から、“objectClass=user"および“sAMAccountName=bob" (アクティブ ディレクトリの場合) というオブジェクトを探すための検索が作成されます。ドメイン オブジェクトが見つからなかった場合は、ディレクトリ ツリーの最上位からユーザ オブジェクトが検索されます。

ドメイン オブジェクトが見つかると、同じオブジェクトを検索しなくても済むように、その情報が保存されます。保存されていたドメインでユーザを特定できなかった場合、保存されていたドメインの情報が削除され、ドメイン オブジェクトが再度検索されます。

SSO エージェントを使用した SonicWall SSO でのユーザ ログアウトの処理は、TSA を伴う SSO とは少し異なります。セキュリティ装置は、SSO エージェントを実行している認証エージェントをポーリングすることによって、ユーザがログアウトしたタイミングを判別します。ユーザがログアウトすると、

SSO エージェントを実行する認証エージェントからファイアウォールに User Logged Out 応答が送信され、ユーザが既にログアウトしていることが確認されて、SSO セッションが終了します。TSA は、セキュリティ装置によるポーリングではなく、TSA 自体でターミナル サービス/Citrix サーバを監視することでログアウト イベントを調べ、ログアウト イベントが発生するとセキュリティ装置に通知し、それによって SSO セッションが終了します。どちらのエージェントについても、無動作タイマーを設定できます。 SSO エージェントについては、ユーザ名要求ポーリング間隔を設定できます (ログアウトをすばやく検知するには、設定するポーリング時間を短くし、システムのオーバーヘッドを少なくするには、ポーリング時間を長くします)。

ブラウザ NTLM 認証を使用した SonicWall SSO 認証

Mozilla ベースのブラウザ (Internet Explorer、Firefox、Chrome、Safari を含む) を使って閲覧するユーザのために、ファイアウォールは NTLM (NT LAN Maanager) 認証によるユーザの識別をサポートします。NTLM は、“統合 Windows セキュリティ" として知られるブラウザ認証スイートで、すべての Mozilla ベースのブラウザでサポートされます。NTLM により、SSO エージェントを利用することなく、装置からブラウザに対して直接認証が要求できます。NTLM は、ユーザがウェブ上でリモートに認証されるような、ドメイン コントローラが利用できない場合にたびたび使用されます。

NTLM 認証は現在 HTTP に対して利用可能で、HTTPS では利用できません。

ブラウザ NTLM 認証は、SSO エージェントがユーザ情報の入手を試みる前または後に試行できます。例えば、SSO エージェントを最初に試行してユーザの識別に失敗してから、トラフィックが HTTP の場合に NTLM が試行されます。

この方式を Linux または Mac クライアントで Windows クライアントと同じように使うために、SSO を **NetAPI** または **WMI** (SSO エージェントがどちらに対して設定されているかに応じて) のどちらかに対してクライアントを調査するように有効にできます。これにより、ファイアウォールが、SSO エージェントに対してユーザを識別するように要求するのに先立って、NetAPI/WMI ポートで応答を監視するようになります。応答がない場合、これらの機器は即時に SSO を失敗します。クライアントによって、以下のように動作します。

- Windows PC では、プローブがほとんどの場合機能 (パーソナル ファイアウォールで遮断されない限り) して、SSO エージェントが使用されます。
- Linux/Mac PC (Samba サーバを実行するように設定されていない場合) では、プローブは失敗して、SSO エージェントはバイパスされ、HTTP トラフィックが送信される際に NTLM 認証が使用されます。

NTLM は、ユーザが HTTP でブラウズするまではユーザを識別できないため、その前に送信されたどんなトラフィックも未確認として扱われます。既定の CFS ポリシーが適用され、ユーザの認証を要求するルールがあれば、トラフィックの通過は許可されません。

NTLM が SSO エージェントの前に使われるように設定されている場合は、最初に HTTP トラフィックを受信すれば、ユーザは NTLM で認証されます。最初に非 HTTP トラフィックを受信すれば、SSO エージェントが認証に使われます。

SSO エージェントの動作

SSO エージェントは、直接 IP アドレスを使って、または、VPN などのパスを使ってクライアントおよびファイアウォールと通信できれば、Windows ドメインに参加している任意のワークステーションまたはサーバにインストールできます。ただし、SSO エージェントは別のスタンドアロン ワークステーションまたはサーバにインストールすることが推奨されます。SSO エージェントのインストール手順については、「SonicWall SSO エージェントのインストール (113 ページ)」を参照してください。

数千ユーザから成る大規模インストールに対応するため、複数の SSO エージェントがサポートされています。最大 8 つの SSO エージェントを設定して、それぞれをネットワーク内にある専用の高性能 PC 上で動作させることができます。

メモ：NetAPI または WMI の使用時には、SSO エージェントを実行するハードウェアのパフォーマンス レベルや、ファイアウォールでの SSO エージェントの設定方法、ネットワークに依存するその他の要因にもよりますが、1 つの SSO エージェントで最大約 2,500 ユーザをサポートできます。類似の要因次第では、ドメイン コントローラ セキュリティ ログからの読み込みを行うように設定されている場合、1 つの SSO エージェントでサポートできるユーザ数を大幅に (潜在的には 50,000 ユーザ以上にまで) 増やすことができます。

SSO エージェントは、クライアントおよびファイアウォールとのみ通信します。SSO エージェントとファイアウォールとの間で交わされるメッセージは、共有鍵を使って暗号化されます。

メモ：共有鍵は SSO エージェントで生成されます。SSO の設定時、ファイアウォールに入力する鍵は、SSO エージェントによって生成された鍵と完全に一致している必要があります。

ファイアウォールは、SSO エージェントに対し、既定のポート 2258 を使って問い合わせを行います。次に、SSO エージェントがクライアントとファイアウォールの間に入って通信し、クライアントのユーザ ID を調べます。ファイアウォールは、SSO エージェントを定期的に (管理者によって設定された頻度で) ポーリングして、絶えずユーザのログイン状況が確認されます。

ログ

SSO エージェントは、管理者によって選択されたログ レベルに基づいて、Windows イベント ログにログ イベント メッセージを送信します。

また、ファイアウォールも、そのイベント ログに SSO エージェント固有のイベントを記録します。

メモ：SSO エージェントに固有のログ メッセージの**補足**フィールドには、<ドメイン/ユーザ名>、認証元： SSO エージェントというテキストが表示されます。ログ メッセージの詳細については、『*SonicOS 6.5 調査*』を参照してください。

ユーザ ログインが拒否されました - ポリシー ルールで許可されていません	ユーザは識別されましたが、ポリシーによって許可されているいずれのユーザ グループにも属していないため、ユーザのトラフィックが遮断されました。
ユーザ ログインが拒否されました - ローカルで見つかりません	ユーザがローカルに見つかりませんでした。ファイアウォールでは、「**ローカルに登録されたユーザのみ許可する**」が選択されています。
ユーザ ログインが拒否されました - SSO エージェントがタイムアウトしました	SSO エージェントへの接続を試みているときにタイムアウトが発生しました。
ユーザ ログインが拒否されました - SSO エージェントの設定エラー	このユーザのアクセスを許可するための適切な設定が SSO エージェントに対してなされていません。
ユーザ ログインが拒否されました - SSO エージェントの通信の問題	SSO エージェントを実行しているワークステーションとの通信に問題があります。
ユーザ ログインが拒否されました - SSO エージェントの名前解決に失敗しました	SSO エージェントがユーザ名を解決できません。
SSO エージェントが返したユーザ名が長すぎます	ユーザ名が長すぎます。
SSO エージェントが返したドメイン名が長すぎます	ドメイン名が長すぎます。

ターミナル サービス エージェントの動作

TSA は、ターミナル サービスまたは Citrix がインストールされている任意の Windows Server マシンにインストールできます。このサーバは、直接 IP アドレスを使用するか VPN などのパスを使用してファイアウォールと通信できる Windows ドメインに属していなければなりません。

TSA のインストール手順については、「SonicWall ターミナル サービス エージェントのインストール (113 ページ)」を参照してください。

トピック:

- 複数の TSA のサポート (106 ページ)
- TSA メッセージの暗号化とセッション ID の使用 (107 ページ)
- ローカル サブネットへの接続 (107 ページ)
- ターミナル サーバからの非ドメイン ユーザ トラフィック (107 ページ)
- ターミナル サーバからの非ユーザ トラフィック (107 ページ)

複数の TSA のサポート

数千のユーザから成る大規模インストールに対応するため、ファイアウォールは、複数のターミナル サービス エージェント (ターミナル サーバごとに 1 つ) と共に動作するように設定できます。サポートされるエージェントの数は、「モデル別のサポートされるターミナル サービス エージェント」テーブルに示すように、モデルによって異なります。

モデル別のサポートされるターミナル サービス エージェント

SonicWall ネットワーク セキュリティ装置	サポートされる TSA の数	SonicWall ネットワーク セキュリティ装置	サポートされる TSA の数	SonicWall ネットワーク セキュリティ装置	サポートされる TSA の数
NS*a* 9650	512	NS*a* 6650	256	TZ600/TZ600 P	4
NS*a* 9450	512	NS*a* 5650	128	TZ500/TZ500 W	4
NS*a* 9250	512	NS*a* 4650	64	TZ400/TZ400 W	4
NSA 9600	512	NS*a* 3650	16	TZ350/350 W	4
NSA 9400	512	NS*a* 2650	8	TZ300/TZ300 W/TZ300 P	4
NSA 9200	512	NSA 6600	256		
SM 9600	512	NSA 5600	128	SOHO 250/250W	4
SM 9400	512	NSA 4600	64	SOHO W	4
SM 9200	512	NSA 3600	16		
		NSA 2600	8		

すべての SonicWall セキュリティ装置において、ターミナル サーバあたり最大 32 個の IP アドレスがサポートされます。サーバは、複数の NIC (ネットワーク インターフェース コントローラ) を装備している場合があります。ターミナル サーバあたりのユーザ数に制限はありません。

TSA メッセージの暗号化とセッション ID の使用

TSA は、TSA とファイアウォールとの間でやり取りされるメッセージにユーザ名とドメインが含まれていると、そのメッセージの暗号化に共有鍵を使用します。ユーザに対する最初のオープン通知は常に暗号化されます。 TSA がユーザ名とドメインを含めるからです。

メモ：共有鍵は TSA で作成され、SSO 設定時にファイアウォールに入力される鍵と TSA の鍵は完全に一致していなくてはなりません。

TSA はユーザ セッション ID をすべての通知に含めます。 ユーザ名とドメインを毎回含めることはしません。これは効率的で安全であり、TSA が再起動後にターミナル サービス ユーザと再同期することを可能にします。

ローカル サブネットへの接続

TSA は装置から返された情報に基づいてネットワーク トポロジを動的に学習し、いったん学習すると、装置を通らないサブネット ユーザ接続に関して通知を装置に送信しません。TSA がこれらのローカル送信先を“記憶から消し去る"メカニズムはないので、装置のインターフェース間でサブネットが移動された場合は、TSA を再起動する必要があります。

ターミナル サーバからの非ドメイン ユーザ トラフィック

ファイアウォールには、必要に応じて非ドメイン ユーザ (ドメインではなく、ローカル マシンにログインしたユーザ) に制限付きアクセスを許可するための「**非ドメイン ユーザには限定的なアクセスのみ許可する**」という設定があります。これはターミナル サービス ユーザに対して、他の SSO ユーザに対する場合と同様に作用します。

ネットワーク内に非 Windows 機器やパーソナル ファイアウォールが動作している Windows コンピュータがある場合は、「**ユーザの監視を右記で行う**」を選択し、SSO エージェントがどちらで設定されているかに応じて、「**NetAPI**」または「**WMI**」ラジオ ボタンを選択します。これにより、ファイアウォールが、SSO エージェントに対してユーザを識別するように要求するのに先立って、NetAPI/WMI ポートで応答を監視するようになります。応答がない場合、これらの機器は即時に SSO を失敗します。そのような機器は、SSO エージェントがユーザを識別するために使用する Windows ネットワーキング メッセージに応答しない、またはそれを遮断します。

ターミナル サーバからの非ユーザ トラフィック

非ユーザ接続は、Windows の更新とアンチウイルスの更新のためにターミナル サーバから開かれます。TSA はログイン サービスからの接続を非ユーザ接続であると認識することができ、装置への通知の中でこれを示します。

これらの非ユーザ接続の処理を制御するため、装置の TSA 設定で「**ターミナル サーバの非ユーザ トラフィックにはアクセス ルールでのユーザ認証を免除する**」チェックボックスが用意されています。このチェックボックスを選択すると、これらの接続が許可されます。このチェックボックスを選択しないと、これらのサービスはローカル ユーザとして扱われます。その場合、「**非ドメイン ユーザには限定的なアクセスのみを許可**」設定を選択し、対応するサービス名を使用して装置上でユーザ アカウントを作成することにより、アクセスを許可することができます。

メモ：TSA からの Ping (ICMP) トラフィックは、非ユーザ トラフィックとして認識されますが、システム サービス トラフィックとしては認識されません。そのため、ユーザ認証のバイパスは許可されず、エージェントのタイムアウト後は破棄されます。ICMP トラフィックが破棄されないようにするには、「**ポリシー | ルール > アクセス ルール**」ページで、ユーザ認証を必要とせずにターミナル サーバからの ICMP を許可するアクセス ルールを追加します。アクセス ルールの詳細については、『*SonicOS 6.5 ポリシー*』を参照してください。

ブラウザ NTLM 認証の動作

トピック:

- ドメイン ユーザの NTLM 認証 (108 ページ)
- 非ドメイン ユーザの NTLM 認証 (108 ページ)
- ブラウザでの NTLM 認証の資格情報 (108 ページ)

ドメイン ユーザの NTLM 認証

ドメイン ユーザに対しては、NTLM 応答は MSCHAP メカニズムを介して RADIUS で認証されます。装置で RADIUS を有効にする必要があります。NTLM 認証の詳細については、「ユーザの管理のための設定 (128 ページ)」を参照してください。

非ドメイン ユーザの NTLM 認証

NTLM を使うと、非ドメインユーザはドメインではなく PC にログインするユーザになることができ、または、ユーザ名とパスワードを要求されて、ドメインの資格情報ではない情報を入力するユーザになることができます。どちらの場合も、NTML は、そうしたユーザとドメイン ユーザを区別します。

ユーザ名がファイアウォール上のローカル ユーザ アカウントと一致すると、NTLM 応答はそのアカウントのパスワードに対してローカルで確認されます。成功した場合は、ユーザはログインしてアカウントに基づいた権限が与えられます。ユーザ グループ メンバーシップは、LDAP からではなく、ローカル アカウントから設定され、そして (パスワードがローカルで確認されたため) Trusted Users グループのメンバーシップを含みます。

ユーザ名がローカル ユーザ アカウントと一致しないと、ユーザはログインされません。NTLM を介して認証されたユーザに対しては、「**非ドメイン ユーザには限定的なアクセスのみ許可する**」オプションは適用されません。

ブラウザでの NTLM 認証の資格情報

NTLM 認証では、ブラウザはドメインの資格情報も使う (ユーザがドメインにログインする場合) ため、完全なシングルサインオン機能を提供する、または、アクセスするウェブサイト (この場合はファイアウォール) のユーザ名とパスワードを入力するようユーザに要求します。ユーザがドメインにログインする場合は、種々の要因がドメインの資格情報を使うためのブラウザの機能に影響します。これらの要因は、使用するブラウザの種別に依存します。

Internet Explorer 9.0 以上	ファイアウォール (SonicWall セキュリティ装置) にログインするときのウェブサイトがローカル イントラネットに存在する場合、インターネット オプションの「セキュリティ」タブに従って、ユーザのドメイン資格情報を使用して透過的に認証を行います。これには、インターネット オプションのローカル イントラネット ゾーンのウェブサイトのリストに、ファイアウォールを追加する必要があります。 これは、ドメイン グループ ポリシーのコンピュータの構成、管理用テンプレート、Windows コンポーネント、Internet Explorer、インターネット コントロール パネル、セキュリティ ページの下の、サイトとゾーンの割り当て一覧から実行できます。
Google Chrome	インターネット オプションのローカル イントラネット ゾーンのウェブサイトのリストに、ファイアウォールを追加することが必要であることを含めて、Internet Explorer と同じように振る舞います。

Firefox	ファイアウォールにログインするウェブサイトが、設定 (Firefox の アドレス バーに **about:config** を入力することによりアクセスする) 内の **network.automatic-ntlm-auth.trusted-uris** エントリにリストされている場合は、ユーザのドメイン資格情報を使用して透過的に認証します。
Safari	Safari は NTLM をサポートしていますが、現状ユーザのドメイン資格情報を使った完全な透過的ログオンはサポートしていません。 **メモ**：Safari は、Windows プラットフォーム上では動作しません。
非 PC プラットフォーム上のブラウザ	Linux や Mac などの非 PC プラットフォームは、Samba を通して Windows ドメイン内のリソースにアクセスできますが、Windows PC が行うような "PC がドメイン内にログインする" という概念がありません。したがって、そのようなプラットフォーム上のブラウザは、ユーザのドメイン資格情報にアクセスできず、それらを NTLM に使用できません。

ユーザがドメインにログインしていない、または、ブラウザがユーザのドメイン資格情報を使えない場合は、名前とパスワードを入力するように求められるか、事前にユーザが保存するように設定している場合は、キャッシュされた資格情報が使われます。

いかなる場合も、ユーザのドメイン資格情報を用いた認証が失敗すると (アクセスに必要な権限がユーザになければ失敗することがあり得る)、ブラウザはユーザに名前とパスワードの入力を求めてきます。これにより、ユーザはドメイン資格情報とは別の資格情報を入力してアクセスを得ることが可能になります。

メモ：シングル サインオンを適用するために NTLM が有効である場合は、「**包含ユーザ**」として **Trusted Users** が設定されている HTTP/HTTPS アクセス ルールを「**管理 | ポリシー > ルール > アクセス ルール**」ページの「**LAN から WAN**」のルールに追加しておく必要があります (詳細については、『*SonicOS 6.5 ポリシー*』を参照してください)。このルールによって、ユーザに対する NTLM 認証要求が開始されます。このアクセス ルールがない場合、アクセスを制限するコンテンツ フィルタ ポリシーなどの他の設定によって、ユーザはインターネット アクセスを遮断され、認証要求ができない可能性があります。

RADIUS アカウント シングル サインオンの動作

RADIUS アカウントは、ネットワーク アクセス サーバ (NAS) がアカウント サーバにユーザ ログイン セッション アカウント メッセージを送信するためのメカニズムとして、RFC 2866 によって規定されています。このメッセージは、ユーザのログイン時およびログオフ時に送信されます。オプションで、ユーザのセッション中に定期的に送信することもできます。

利用者が (通常、リモート アクセスや無線アクセスのために) 外部またはサードパーティ製のネットワーク アクセス装置を使用してユーザ認証を行う場合、その装置が RADIUS アカウントをサポートしていれば、別の SonicWall 装置が RADIUS アカウント サーバの役割を果たし、利用者のネットワーク アクセス サーバから送られてきた RADIUS アカウント メッセージをネットワークのシングル サインオン (SSO) に使用できます。

メモ：SMA 11.4 以降が動作している SonicWall SMA 1000 シリーズ装置を外部の RADIUS アカウント クライアントとして設定し、SonicWall ファイアウォールを RADIUS アカウント サーバとして使うことができます。

リモート ユーザが SonicWall SMA またはサードパーティ装置経由で接続する際、SMA またはサードパーティ装置は (RADIUS アカウント サーバとして設定されている) SonicWall 装置にアカウント メッセージを送信します。SonicWall 装置は、アカウント メッセージの情報に基づいて、そのユーザをログイン ユーザの内部データベースに追加します。

ユーザがログアウトすると、SonicWall SMA またはサードパーティ装置は SonicWall セキュリティ装置に別のアカウント メッセージを送信します。その後、このセキュリティ装置によってユーザのログアウトが行われます。

メモ：ネットワーク アクセス サーバ (NAS) が RADIUS アカウント メッセージを送信するとき、ユーザが RADIUS で認証されている必要はありません。サードパーティ装置がユーザの認証に LDAP、ローカル データベース、またはその他のメカニズムを使用していても、NAS は RADIUS アカウント メッセージを送信できます。

RADIUS アカウント メッセージは暗号化されません。RADIUS アカウントは要求認証子と共有鍵を使用するので、本質的にスプーフィングから保護されます。RADIUS アカウントを使用するには、RADIUS アカウント メッセージを送信できるネットワーク アクセス サーバ (NAS) のリストが装置に設定されている必要があります。この設定では、各 NAS の IP アドレスと共有鍵を指定します。

トピック:

- RADIUS アカウント メッセージ (110 ページ)
- SonicWall とサードパーティ ネットワーク装置の互換性 (111 ページ)
- プロキシ転送 (111 ページ)
- 非ドメイン ユーザ (111 ページ)
- IPv6 に関する考慮事項 (112 ページ)
- RADIUS アカウント サーバ ポート (112 ページ)

RADIUS アカウント メッセージ

RADIUS アカウントには、以下の2 種類のアカウント メッセージが使用されます。

- **アカウント要求**
- **アカウント応答**

Accounting-Request では、**Status-Type** 属性で指定される以下の 3 種類の要求種別の 1 つを送信できます。

要求	送信されるタイミング
Start	ユーザのログイン時に送信されます。
Stop	ユーザのログアウト時に送信されます。
Interim-Update	ユーザのログイン セッション中、定期的に送信されます。

アカウント メッセージは、RFC 2866 で規定されている RADIUS 標準に準じます。各メッセージには、一連の属性と、共有鍵で確認される 1 個の認証子が含まれます。

アカウント要求では、以下の SSO 関連属性が設定されます。

Status-Type	アカウント要求の種別 (**Start**、**Stop**、または **Interim-Update**)。
User-Name	ユーザのログイン名。形式は RFC で指定されていないので、単純なログイン名だけにすることも、ログイン名、ドメイン、識別名 (DN) など各種値の文字列にすることもできます。
Framed-IP-Address	ユーザの IP アドレス。NAT が使用される場合は、ユーザの内部 IP アドレスにする必要があります。

Calling-Station-Id	SMA など一部の装置で使用される、ユーザの IP アドレスの文字列表現。
Proxy-State	要求を別の RADIUS アカウント サーバへ転送するために使用されるパススルー状態。

SonicWall とサードパーティ ネットワーク装置の互換性

RADIUS アカウントによる SSO を使用するにあたり、SonicWall セキュリティ装置とサードパーティ ネットワーク装置の互換性を確保するには、そのサードパーティ装置で次のことが可能である必要があります。

- RADIUS アカウントをサポートする。
- **Start** および **Stop** メッセージの両方を送信する。**Interim-Update** メッセージの送信は必須ではありません。
- ユーザの IP アドレスを **Start** および **Stop** メッセージの **Framed-IP-Address** 属性または **Calling-Station-Id** 属性のいずれかで送信する。

メモ：NAT を使用してユーザの外部パブリック IP アドレスを変換するリモート アクセス サーバの場合、内部ネットワークで使用される内部 IP アドレスがこの属性に指定され、その IP アドレスがユーザの一意の IP アドレスである必要があります。これらの属性の両方を使用する場合、**Framed-IP-Address** 属性は内部 IP アドレスを使用し、**Calling-Station-Id** 属性は外部 IP アドレスを使用する必要があります。

Start メッセージと **Interim-Update** メッセージの **User-Name** 属性でユーザのログイン名を送信する必要があります。**Stop** メッセージの **User-Name** 属性でもユーザのログイン名を送信できますが、これは必須ではありません。**User-Name** 属性には、ユーザのアカウント名を含める必要があり、同時にドメイン名も含めることができます。または、ユーザの識別名 (DN) を含める必要があります。

プロキシ転送

RADIUS アカウント サーバとして使用する SonicWall セキュリティ装置は、ネットワーク アクセス サーバ (NAS) ごとに最大 4 つの他の RADIUS アカウント サーバへ要求をプロキシ転送できます。各 RADIUS アカウント サーバは、NAS ごとに個別に設定できます。

NAS ごとに設定の詳細を再入力する手間を省くには、SonicOS を使用して、設定されているサーバのリストから各 NAS の転送を選択できます。

各 NAS クライアントのプロキシ転送設定には、タイムアウトと再試行回数が含まれます。2 つ以上のサーバへ要求を転送する方法は、以下のオプションを選択して設定できます。

- **タイムアウト時に次のサーバを試行する**
- **すべてのサーバに転送する**

非ドメイン ユーザ

RADIUS アカウント サーバに報告されたユーザは、以下の場合にローカル (非ドメイン) ユーザと認識されます。

- ユーザ名がドメイン名なしで送信されており、LDAP でサーバのドメインを検索するように設定されていない。
- ユーザ名がドメイン名なしで送信されており、LDAP でサーバのドメインを検索するように設定されているが、そのユーザ名が見つからなかった。
- ユーザ名はドメイン名と一緒に送信されたが、LDAP データベース内でそのドメインが見つからなかった。

- ユーザ名はドメイン名と一緒に送信されたが、LDAP データベース内でそのユーザ名が見つからなかった。

RADIUS アカウントで認証される非ドメイン ユーザは、他の SSO メカニズムで認証されるユーザと同じ制約を受け、さらに以下の制限が適用されます。

- ユーザがログインするのは「**非ドメイン ユーザには限定的なアクセスのみ許可する**」がオンになっている場合に限られます。
- ユーザは Trusted Users グループのメンバーにはなりません。

IPv6 に関する考慮事項

RADIUS アカウントでは、ユーザの IPv6 アドレスを含めるために以下の属性が使用されます。

- Framed-Interface-Id / Framed-IPv6-Prefix
- Framed-IPv6-Address

現時点では、これらの IPv6 属性はすべて無視されます。

機器によっては、IPv6 アドレスを **Calling-Station-ID** 属性にテキストとして渡してくるものもあります。

有効な IPv4 アドレスが含まれていないと、**Calling-Station-ID** も無視されます。

IPv6 アドレス属性が含まれていて、IPv4 アドレス属性が含まれていない RADIUS アカウント メッセージは、プロキシ サーバへ転送されます。プロキシ サーバが設定されていない場合は、IPv6 属性は破棄されます。

RADIUS アカウント サーバ ポート

RADIUS アカウントは通常、次の UDP ポートを使用します。

1813	IANA によって指定されたポート。SonicWall セキュリティ装置は、既定ではポート 1813 でリッスンします。
1646	以前の非公式標準ポートです。

RADIUS アカウント ポートとして別のポート番号を設定することもできますが、SonicWall セキュリティ装置がリッスンできるのは 1 つのポートのみです。したがって、複数のネットワーク アクセス サーバ (NAS) を使用する場合は、同じポート番号で通信するようにすべての NAS を設定する必要があります。

シングル サインオン エージェント/ターミナル サーバ エージェントのインストール

SSO を設定するには、SonicWall SSO エージェントおよび/または、SonicWall ターミナル サービス エージェント (TSA) のインストールと設定、さらに、SonicOS を実行するファイアウォールでこの SSO エージェントまたは TSA を使用するための設定が必要になります。SonicWall SSO の概要については、「シングル サインオンについて (99 ページ)」を参照してください。

トピック:

- SonicWall SSO エージェントのインストール (113 ページ)
- SonicWall ターミナル サービス エージェントのインストール (113 ページ)

SonicWall SSO エージェントのインストール

SonicWall SSO エージェントは、SonicWall ディレクトリ コネクタの一部です。SonicWall SSO エージェントは、VPN または IP を使ってアクセスできるアクティブ ディレクトリ サーバへのアクセスがある Windows ドメイン内のワークステーションまたはサーバに、最低 1 台から最大 8 台にインストールされている必要があります。これらのワークステーションやサーバは分離されたスタンドアロンのワークステーションまたはサーバであることが推奨されます。SonicWall SSO エージェントには、ファイアウォールへのアクセス権が必要です。

SonicWall SSO エージェントのインストール手順については、『*SonicWall Directory Services Connector 管理ガイド*』を参照してください。このガイドは、SonicWall Support からダウンロードできます。

SonicWall ターミナル サービス エージェントのインストール

Windows ドメイン内のネットワークの 1 つ以上のターミナル サーバに SonicWall TSA をインストールします。SonicWall TSA は SonicWall セキュリティ装置へのアクセスが必要で、セキュリティ装置は TSA へのアクセスが必要です。ターミナル サーバでソフトウェア ファイアウォールが動作している場合には、セキュリティ装置からの受信メッセージ用の UDP ポート番号を開くことが必要な場合があります。

SonicWall TSA は MySonicWall から無償でダウンロードできます。

SonicWall TSA のインストール手順については、『*SonicWall Directory Services Connector 管理ガイド*』を参照してください。

トピック:

- SonicWall ターミナル サービス エージェントのアクセス (113 ページ)
- SonicWall TSA トラブル シューティング レポートの作成 (113 ページ)

SonicWall ターミナル サービス エージェントのアクセス

SonicWall TSA をインストールして Windows Server システムを再起動した後で、インストーラによってデスクトップ上に作成された SonicWall TSA のアイコンをダブルクリックすると、SonicWall TSA の起動と設定、トラブル シューティング レポート (TSR) の生成、状態とバージョン情報の確認を行うことができます。

詳細については、『*SonicWall Directory Services Connector 管理ガイド*』を参照してください。

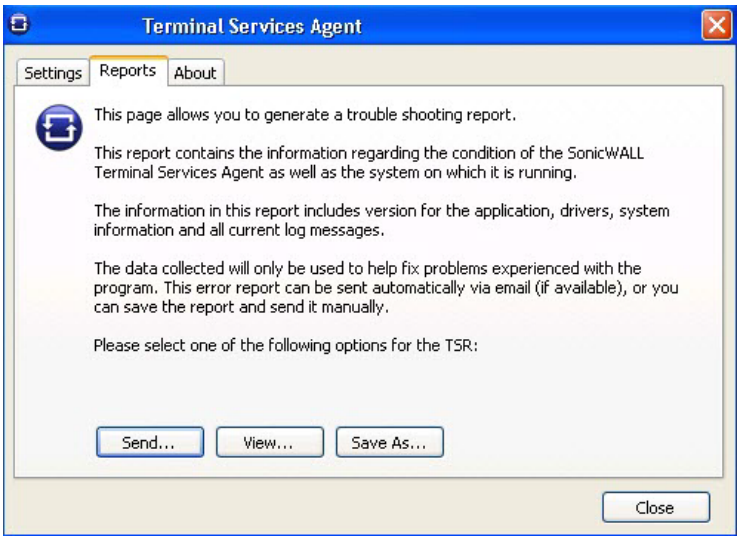
SonicWall TSA トラブル シューティング レポートの作成

現在のログ メッセージおよびエージェント、ドライバ、システム設定についての情報をすべて含んだトラブル シューティング レポート (TSR) を作成できます。 これを使用して、内容を調べたり、SonicWall テクニカル サポートに送信して問い合わせたりできます。

SonicWall TSA の TSR を作成するには、以下の手順に従います。

1 **SonicWall TSA** のデスクトップ アイコンをダブルクリックします。「**SonicWall ターミナル サービス エージェント**」ウィンドウが表示されます。

2 「**レポート**」タブを選択します。



3 TSR を作成した後の処理によって、次の操作を行います。

- TSR を SonicWall テクニカル サポートに電子メールで自動送信するには、「**送信**」を選択します。
- TSR の内容を既定のテキスト エディタで確認するには、「**表示**」を選択します。
- TSR をテキストファイルとして保存するには、「**名前を付けて保存**」を選択します。

4 終了したら、「**閉じる**」を選択します。

シングル サインオンの高度な機能

トピック:

- シングル サインオンについて (114 ページ)
- 詳細設定について (115 ページ)
- マウスを置いたときに表示される SSO の統計 (115 ページ)
- TSR のシングル サイン オン統計の利用 (116 ページ)
- エージェントの検査 (117 ページ)
- 改善措置 (117 ページ)

シングル サインオンについて

SSO を使用している SonicWall セキュリティ装置を介して、ユーザが初めてトラフィックを送信しようとすると、セキュリティ装置は SonicWall SSO エージェントに"who is this" 要求を送信します。エージェントは、Windows ネットワークを介してユーザの PC に問い合わせを行い、ファイアウォールにユーザ名を返します。ユーザ名がポリシーに設定されているいずれかの条件に一致した場合、SonicWall

はユーザが“ログオンしている"と見なします。ユーザが SSO を使用して SonicWall にログインしている場合、SSO 機能によってログアウトも検出されます。ログアウトを検出するため、セキュリティ装置はエージェントに繰り返しポーリングを行い、各ユーザがまだログインしているかどうか確認します。特に、非常に数多くのユーザが接続している場合、このポーリングと内部の識別要求によって、SonicWall SSO エージェント アプリケーション、およびこのアプリケーションが動作している PC に大きな負荷がかかることがあります。

SonicWall SSO 機能は、速度制限メカニズムを利用して、SonicWall 装置がこのようなユーザ要求を SSO エージェントに大量に送信しないようにします。自動計算と装置に設定できる項目の両方で、この速度制限の動作を制御します。SonicWall SSO 機能は、最新のポーリング応答時間に基づいて、エージェントへの各メッセージに格納され、ポーリング期間中に処理できるユーザ要求の最大数を自動的に計算します。また、複数ユーザ要求時のタイムアウトは、ポーリング中にたまにタイムアウトが長くなる可能性を低減できるだけの値に自動的に設定されます。設定可能な項目で、一度にエージェントに送信する要求数を制御します。 また、この項目を調整して、SSO のパフォーマンスを最適化し、潜在的な問題を防ぐことができます。このセクションは、適切な設定値を選択するための指針となります。

エージェントの過負荷によって問題が生じる可能性は、エージェントを専用の高性能 PC 上で動作させたり、複数エージェントを別個の PC 上で使用して PC 間で負荷を共有することによって、低減することができます。後者の方法では、エージェント PC のいずれかが故障した場合の冗長性も実現されます。エージェントは Windows Server PC 上で実行する必要があります。

詳細設定について

SSO エージェントの設定時には、「**一度に送信する最大リクエスト数**」の設定を使用できます (SSO エージェントの設定の詳細については、「SonicOS で SonicWall SSO エージェントを使用するための設定 (180 ページ)」を参照してください)。

この項目は、SonicWall からエージェントに一度に送信できる要求の最大数を制御します。エージェントは、各要求を処理する別個のスレッドを PC 内に生成し、複数の要求を同時に処理します。一度に送信する要求が多すぎると、エージェントが動作している PC が過負荷になることがあります。送信する要求数が最大値を超えた場合、一部の要求は内部の "リング バッファ" キューに配置されます (「TSR のシングル サイン オン統計の利用 (116 ページ)」および「マウスを置いたときに表示される SSO の統計 (115 ページ)」を参照してください)。リング バッファでの要求の待機が長くなりすぎると、SSO 認証の応答時間が遅くなることがあります。

この項目は、ログインしているユーザの状況を確認するためのポーリング時に自動計算される、エージェントへのメッセージごとのユーザ要求数とともに機能します。メッセージごとのユーザ要求数は、最新のポーリング応答時間に基づいて計算されます。送信する必要があるメッセージ数が最小になるよう、SonicWall はこのユーザ要求数をできる限り大きく調整して、エージェントにかかる負荷を低減し、SonicOS 装置とエージェント間のネットワーク トラフィックを減らせるようにします。ただし、ユーザ要求数は、エージェントがメッセージに含まれる全ユーザ要求をポーリング期間内に処理できる値に保たれます。これによって、タイムアウトや、ログアウトしたユーザを迅速に検出できないなどの潜在的な問題を回避します。

マウスを置いたときに表示される SSO の統計

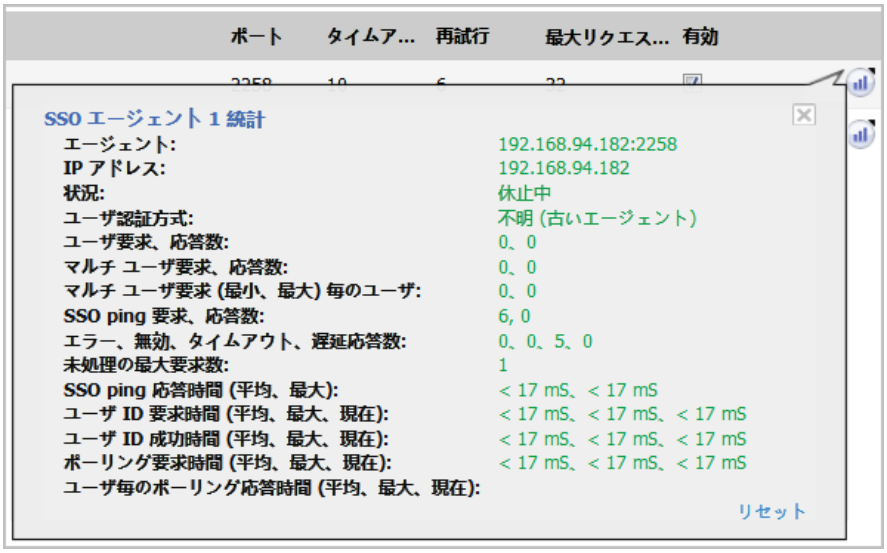
「**SSO 認証の設定**」ダイアログでは、各エージェントおよびすべての SSO エージェントについての統計がマウスオーバー時に表示されます。「**SSO エージェント**」ページでは、エージェントの横にある緑色の LED 形式のアイコンによってそのエージェントが稼働していることが示されます。赤色の LED アイコンは、エージェントが休止中であることを示します。

統計を表示するには、以下の手順に従います。

- 特定のエージェントの場合は、その SSO エージェントの**統計**アイコンの上にマウス ポインタを置きます。

- すべての SSO エージェントの場合は、テーブルの下にある**統計**アイコンの上にマウス ポインタを置きます。

  ヒント：これは、**ターミナル サービス**上の個々の TSA に対しても動作します。



統計の表示を閉じるには、「**閉じる**」アイコンを選択します。

表示されている値をすべてクリアするには、「**リセット**」を選択します。

TSR のシングル サイン オン統計の利用

テクニカル サポート レポート (TSR) には、SSO のパフォーマンスとエラーに関する豊富な統計が含まれています。これらを利用して、インストールされている SSO のパフォーマンスを測定することができます。「**調査 | ツール > システム診断**」ページで TSR をダウンロードして、"SSO operation statistics" (SSO 操作の統計) というタイトルを検索してください。特に注意すべきカウンタは次のとおりです。

1 「**SSO ring buffer statistics**」の「**Ring buffer overflows**」と「**Maximum time spent on ring**」を調べます。後者がポーリング間隔に接近、または越えている場合、あるいはいずれかのリング バッファのオーバーフローが示されている場合、要求は十分な速さでエージェントに送信されていません。「**Current requests waiting on ring**」が絶えず増加している場合も、同じ状況を示しています。これは、要求の送信速度を速めるには、「**一度に送信できる最大要求数**」の値を大きくしなければならないということを意味します。ただし、それによってエージェントにかかる負荷も増加します。 また、増加した負荷をエージェントが処理できない場合は、結果として問題が生じます。 このような場合、エージェントをより強力な PC に移動したり、エージェントの追加を検討する必要があるかもしれません。

2 「**SSO operation statistics**」の「**Failed user id attempts with time outs**」と「**Failed user id attempts with other errors**」を調べます。これらの値は、ゼロかそれに近い値でなければなりません。 ここに多数の失敗が表示される場合は、エージェントに問題があることを示します。 その原因としては、試みられているユーザ認証の数にエージェントが対応できないことが考えられます。

3 「**SSO operation statistics**」の「**Total users polled in periodic polling**」、「**User polling failures with time outs**」、および「**User polling failures with other errors**」を調べます。いくつかのタイムアウトとエラーは許容範囲であり、予想されています。 また、たまにポーリングが失敗しても問題は発生しません。ただし、エラー率は低くなければなりません (許容できるエラー率は約 0.1%未満です)。繰り返しになりますが、ここでの失敗率が高い場合は、前述のとおり、エージェントに問題があることを示しています。

4 「**SSO agent statistics**」の「**Avg user ID request time**」と「**Avg poll per-user resp time**」を調べます。これらの値は数秒未満の範囲になければなりません。 それより長い場合は、ネットワークに問題がある可能性を示しています。ただし、非 Windows PC からの SSO を介したトラフィック認証 (非常に長い時間がかかることがあります) が原因のエラーによって、「**Avg user ID request time**」の値に誤差が生じる可能性があるので、この値が高くても「**Avg poll per-user resp time**」が正しいと思われる場合は、おそらく非 Windows 機器の認証によって、エージェントに非常に多くのエラーが発生していることを示しているということに注意します。「ステップ 6」を参照してください。

5 複数のエージェントを使用している場合は、「**SSO agent statistics**」のさまざまなエージェントに対して報告されたエラー率とタイムアウト率、およびその応答時間も調べます。エージェント間で大きな差がある場合は、あるエージェントに固有の問題を示していることがあります。このような問題は、その特定のエージェントの設定をアップグレードまたは変更することによって対処できます。

6 PC 以外の機器からのトラフィックによって、SSO 識別が開始されることがあります。また、これらの統計にエラーやタイムアウトが報告されることもあります。そのような機器の IP アドレスをアドレス オブジェクト グループに設定し、以下のいずれか、または両方を実行することによって、このような動作を回避することができます。

- コンテンツ フィルタを使用している場合は、SSO 設定ダイアログの「**強制**」タブで、「**次からのトラフィックに対してシングル サイン オン処理をバイパスする**」設定にそのアドレス オブジェクトを選択します。
- 認証済みのユーザのみを許可するようアクセス ルールが設定されている場合は、「**包含ユーザ**」を「**すべて**」にして、そのアドレス オブジェクト用の別個のルールを設定します。

関係する IP アドレスを識別するには、TSR を調べて、“SSO によって保持される IP アドレス"を検索します。すると、「**失敗後の保留時間**」項目で設定された、前の期間中の SSO の失敗が一覧表示されます。

メモ：Mac/Linux PC の IP アドレスが表示されている場合は、「Mac ユーザおよび Linux ユーザへの対応 (118 ページ)」を参照してください。

「ユーザ」タブの「**失敗後の保留時間**」項目の値を大きくすることによっても、この原因によるエラー率を制限できます。

エージェントの検査

TSR 内の統計が、エージェントに関して問題がある可能性を示している場合、次の手順としては、エージェントが動作している PC 上で Windows タスク マネージャを実行し、「**パフォーマンス**」タブの CPU 使用率と、「プロセス」タブの CIAService.exe プロセスの CPU 使用率を調べることをお勧めします。後者は CPU 時間の大部分を消費しており、CPU 使用率はほぼ 100%に急増しています。 これは、エージェントが過負荷になっていることを示すものです。「**一度に送信できる最大要求数**」の値を小さくすることで、負荷を減らすことができます。前述の「TSR のシングル サイン オン統計の利用」の「ステップ 1」を参照してください。

改善措置

設定でバランスを取ってエージェントの PC が過負荷にならないようにすることはできないが、まだ十分な速さでエージェントに要求を送信できている場合は、以下のアクションのいずれかを実行してください。

- ポーリング時間を増やすことによって、「**SSO 認証**」ダイアログの「**ユーザ**」セクションで設定されているポーリング間隔を低下させることを検討する。これを実行すると、エージェントにかかる負荷は減少しますが、ログアウトの検出は遅くなります。

  メモ：共有 PC 環境では、ポーリング間隔をできる限り短く保ち、異なるユーザが同じ PC を使用する場合にログアウトを検出できないことから生じる可能性のある問題 (ある PC の2 番目のユーザからの最初のトラフィックが、前のユーザが送信したものと記録される可能性があるなど) を回避することがおそらく最善の策となります。

- エージェントをより高性能な専用 PC に移動する。
- 1 つまたは複数のエージェントを追加して設定する。

アクセス ルールの設定

SonicWall SSO を有効にすると、SonicOS 管理インターフェースの「**ルール > アクセス ルール**」ページのポリシーに影響を与えます。「**ルール > アクセス ルール**」に指定されたルールは、SSO LDAP 問い合わせで返されたユーザ グループ メンバーシップに照らしてチェックされ、自動的に適用されます。

トピック:

- SonicWall SSO の自動生成ルール (118 ページ)
- Mac ユーザおよび Linux ユーザへの対応 (118 ページ)
- ターミナル サーバからの ICMP Ping を許可する (120 ページ)
- アクセス ルールについて (120 ページ)

SonicWall SSO の自動生成ルール

SonicOS 管理インターフェースで SonicWall SSO エージェントまたは TSA を設定すると、エージェントから LAN への応答を許可するためのアクセス ルールと、対応する NAT ポリシーが作成されます。これらのルールは、**SonicWall SSO Agents** または **SonicWall Terminal Services Agents** アドレス グループ オブジェクトのどちらかを使用します。このアドレス グループ オブジェクトは、設定されたエージェントごとにメンバー アドレス オブジェクトを持ちます。エージェントが追加または削除されると、メンバー アドレス オブジェクトも自動的にグループ オブジェクトに追加、またはグループ オブジェクトから削除されます。IP アドレスが DNS によって解決された (エージェントが DNS 名で指定されている場合) ときなど、エージェントの IP アドレスが変更されると、メンバー アドレス オブジェクトも自動的に更新されます。

SonicWall SSO エージェントまたは TSA をさまざまなゾーンで設定すると、アクセス ルールと NAT ポリシーが該当する各ゾーンに追加されます。各ゾーンで、同じ **SonicWall SSO Agents** または **SonicWall Terminal Services Agents** アドレス グループが使用されます。

メモ：SonicWall SSO が使用されているゾーンではゲスト サービスを有効にしないでください。ゲスト サービスを有効にすると、そのゾーンでの SSO が無効化され、それにより SSO を介して認証されるユーザがアクセスを失うことになります。ゲスト サービスには個別のゾーンを作成してください。

Mac ユーザおよび Linux ユーザへの対応

Mac および Linux のシステムは、SonicWall SSO エージェントが使用する Windows のネットワーク要求をサポートしませんが、Samba 3.5 以降を使用すれば SonicWall SSO を利用できます。

Mac および Linux 上で Samba を用いて SSO を使用する

Windows ユーザに対しては、SonicWall SSO はセキュリティ装置によって Windows ドメイン内のユーザを自動的に認証するために使用されます。これによりユーザは、Windows ドメインへのログイン後に追加のログイン処理をして自身を識別する必要なしに、適切なフィルタとポリシー承諾を使ってセキュリティ装置を通したアクセスを得ることが可能になります。

Samba は、Linux/UNIX または Mac マシンで、ユーザに (Samba の `smbclient` ユーティリティを介して) Windows ドメイン内のリソースへのアクセスを与えたり、Windows ドメイン ユーザに (Samba サーバを介して) Linux や Mac マシン上のリソースへのアクセスを与えたりするために使われる、ソフトウェア パッケージです。

Windows ドメイン内で Samba を用いて Linux PC または Mac 上で動作するユーザは、SonicWall SSO によって識別可能ですが、それには、Linux/Mac マシンと SSO エージェントの適切な設定と、おそらく装置のいくつかの再設定が必要です。例えば、以下の設定が必要です。

- Linux/Mac ユーザで SonicWall SSO を使うには、SonicWall SSO エージェントがユーザのマシンからユーザのログイン情報を得るために、**WMI** ではなく **NetAPI** を使うように設定されている必要があります。
- Samba が SonicWall SSO エージェントからの要求を受信して応答するためには、ドメインのメンバーとして設定され、Samba サーバが動作してドメイン認証を使うように正しく設定されている必要があります。

SonicWall SSO は、Samba 3.5 以降でサポートされます。

メモ：Linux PC に複数のユーザがログインする場合は、その PC からのトラフィックへのアクセスは、最新のログインに基づいて与えられます。

Mac および Linux 上で Samba を用いずに SSO を使用する

Samba がなくても、Mac および Linux ユーザはまだアクセス可能ですが、ファイアウォールにログインしてそうする必要があります。これにより、以下の問題が発生することがあります。

- ユーザがログインするまで、Mac または Linux のシステムからのトラフィックによって、SSO 識別が試行され続けることがあります。そのようなシステムが多数ある場合は、これが SSO システムに対するパフォーマンスのオーバーヘッドとなる可能性がありますが、“失敗後の保留" タイムアウトによって影響は幾分緩和されます。
- ユーザ レベル認証を要求するポリシー ルールがない状態で、ユーザごとのコンテンツ フィルタ (CFS) ポリシーを使用する場合、最初に手動でログインするまで、Mac および Linux のシステムのユーザには既定の CFS ポリシーが適用されます。
- ユーザ レベル認証を要求するようポリシー ルールが設定されている場合、Mac および Linux のシステムのユーザからのウェブ ブラウザ接続は、SSO の失敗後にログイン ページにリダイレクトされますが、失敗によってタイムアウトが発生し、ユーザに対して遅延が生じることがあります。

これらの問題を回避するために、「**管理 | ポリシー > ルール > アクセス ルール**」ページでアクセス ルールを設定する際には、「**ユーザを認証するためにシングル サイン オンを起動しない**」オプションが使用可能になります (アクセス ルールの設定の詳細については、『*SonicOS 6.5 ポリシー*』を参照してください)。このオプションは、SonicWall SSO が有効な場合にのみ表示されます。このオプションがオンになっている場合、ルールに一致するトラフィックについては SSO の試行が行われず、ルールに一致する未認証の HTTP 接続は、ログイン ページに直接誘導されます。通常、「**送信元**」ドロップダウン メニューには、Mac および Linux のシステムの IP アドレスを含むアドレス オブジェクトが設定されます。

CFS の場合は、Mac および Linux のシステムからの HTTP セッションがログイン ページに自動的にリダイレクトされ、これらのシステムのユーザが手動でログインする必要がなくなるよう、CFS の "前" にこのオプションをオンにしたルールを追加することができます。

メモ：ユーザ認証プロセス全体のバイパスが許可されている機器に対しては、「**ユーザを認証するためにシングル サイン オンを起動しない**」オプションを選択しないでください。このオプションが有効になっているとき、アクセス ルールによって影響を受ける可能性がある機器は、手動ログイン可能でなければなりません。そのような機器に対しては、「**包含ユーザ**」を「**すべて**」に設定して、別個のアクセス ルールを追加してください。

ターミナル サーバからの ICMP Ping を許可する

Windows では、ターミナル サーバ上のユーザからの発信 ICMP Ping はソケットを介して送信されないために TSA から見えず、それゆえにセキュリティ装置はそれらに対しての通知を受け取りません。その結果、ファイアウォール ルールがユーザレベルの認証を使用していて、Ping の通過を許可したい場合、すべてからの Ping を許可するための個別のアクセスルールを作成する必要があります。

アクセス ルールについて

アクセス ルールを使用すると、ユーザ アクセスを制御できます。「**管理 | ポリシー > ルール > アクセス ルール**」ページで設定したルールは、SSO LDAP 問い合わせで返されたユーザ グループ メンバーシップに照らしてチェックされ、自動的に適用されます。アクセス ルールは、着信および発信アクセス ポリシーの定義、ユーザ認証の設定、および セキュリティ装置 のリモート管理を可能にするネットワーク管理ツールです。「**ルール > アクセス ルール**」ページには、並べ替え可能なアクセス ルール管理インターフェースが用意されています。

メモ：限定的なポリシー規則には、汎用的なポリシー規則よりも高い優先順位を割り当てる必要があります。特性階層としては、一般に送信元、送信先、サービスが使用されます。ポリシー規則の特性定義に、ユーザ名や対応するグループ権限などのユーザ ID 要素は含まれません。

既定では、ファイアウォールのステートフル パケット検査によって、LAN からインターネットへの通信はすべて許可され、インターネットから LAN へのトラフィックはすべて遮断されます。

既定のアクセス ルールを拡張または指定変更する、追加のネットワーク アクセス ルールを定義することもできます。例えば、アクセス ルールを作成することによって、特定の種類のトラフィック (LAN から WAN への IRC など) を遮断したり、特定の種類のトラフィック (インターネット上の特定のホストから LAN 上の特定のホストへの Lotus Notes データベースの同期など) を許可したり、特定のプロトコル (Telnet など) の使用を LAN 上の承認されたユーザのみに制限したりすることができます。

注意：ネットワーク アクセス ルールを定義する機能は強力なツールです。個別アクセス ルールを使用して、ファイアウォールの保護を無効にしたり、インターネットへのアクセスをすべて遮断したりすることができます。ネットワーク アクセス ルールを作成または削除するときには注意が必要です。

アクセス ルールの詳細については、『*SonicOS 6.5 ポリシー*』を参照してください。

ターミナル サーバからの HTTP ログインによる SonicOS の管理

通常、SonicWall セキュリティ装置は、HTTP ログインで指定された認証資格情報に基づくポリシーにより、1 つの IP アドレスの 1 人のユーザに対してアクセス権を付与します。ターミナル サーバを使用するユーザについては、IP アドレスごとに 1 人のユーザというこの方法による認証は不可能です。しかし、装置を管理する目的に限り、ターミナル サーバからの HTTP ログインが認められています。 このとき、以下の制限および要件が適用されます。

- ターミナル サーバからのインターネット アクセスは TSA から制御され、HTTP ログインによるオーバーライドは行われません。 ターミナル サーバのユーザには、HTTP ログインで指定された資格情報に基づくセキュリティ装置へのアクセス権は付与されません。
- ターミナル サーバからの HTTP ログインは、組み込みの **admin** アカウントおよび管理者権限を持つその他のユーザ アカウントに対してのみ許可されます。管理者以外のアカウントからログインしようとすると、"この場所からは不許可" のエラーにより失敗します。
- 管理者ユーザが HTTP ログインに成功すると、直ちに管理インターフェースが表示されます。小さな「**ユーザ ログイン状況**」ページは表示されません。
- ターミナル サーバからの HTTP ログインに使用する管理者ユーザ アカウントは、ターミナル サーバへのログインに使用したユーザ アカウントと同じである必要はありません。セキュリティ装置上には、完全に別個のログイン セッションとして表示されます。
- 1 つのターミナル サーバでセキュリティ装置を管理できるのは、1 度に 1 人のユーザのみです。2 人のユーザが同時に管理しようとすると、最後にログインしたユーザが優先され、もう 1 人のユーザには、最後のログインに使用されたブラウザではありませんというエラーが表示されます。
- TSA との通信の問題によりユーザを識別できなかった場合、SSO の場合とは異なり、HTTP ブラウザ セッションはウェブ ログイン ページにリダイレクトされません。代わりに、ネットワーク問題により目的のページは一時的に利用不可になっていますというメッセージを示す新規ページが表示されます。

SSO ユーザ セッションの表示および管理

トピック:

- SSO ユーザのログアウト (121 ページ)
- 追加の SSO ユーザ設定の構成 (121 ページ)
- パケット監視を使用した SSO メッセージおよび LDAP メッセージの表示 (122 ページ)
- SSO メッセージのキャプチャ (122 ページ)
- LDAP over TSL メッセージのキャプチャ (122 ページ)

SSO ユーザのログアウト

「**監視 | 現在の状況 > ユーザ セッション > 使用中のユーザ**」ページには、セキュリティ装置上のユーザ セッションが表示されます。ユーザの設定の表示やユーザのログアウト方法については、『*SonicOS 6.5 監視*』を参照してください。

メモ：「**管理 | システム セットアップ > ユーザ > 設定**」で行ったユーザ設定の変更は、そのユーザの現在のセッション中には反映されません。変更を反映するには、ユーザを手動でログアウトさせる必要があります。その後、変更が反映された状態で、ユーザが透過的に再度ログインされます。

追加の SSO ユーザ設定の構成

「**管理 | システム設定 > ユーザ > 設定**」ページには、SSO などのユーザ ログイン設定に加えて、ユーザ セッション設定、グローバル ユーザ設定、規約の承諾設定に対する設定オプションがあります。

「**ユーザ セッション**」にある、ユーザ セッションを制限するオプションは、SSO を使ってログインしたユーザに適用されます。SSO ユーザはセッション時間の制限設定に従ってログアウトされますが、その後、トラフィックを送信すれば自動的かつ透過的に再びログイン状態に戻ります。

メモ：ログイン セッション時間の制限の設定を小さくしすぎないように注意してください。特にユーザ数が多い環境では、パフォーマンス上の問題を引き起こす可能性があります。

SSO セッションがアクティブのときに「**ユーザ > 設定**」ページで適用した変更は、そのセッション中は反映されません。

ヒント：変更を反映するには、ユーザをログ アウトさせる必要があります。その直後、変更が反映された状態で、ユーザが自動的に再度ログインされます。

パケット監視を使用した SSO メッセージおよび LDAP メッセージの表示

「**調査 | ツール > パケット監視**」で利用できるパケット監視機能によって、SSO エージェントとの間の復号化されたメッセージと、復号化された LDAP over TLS (LDAPS) メッセージのキャプチャを有効にするためのオプションが提供されています。詳細については、『*SonicOS 6.5 調査*』を参照してください。

SSO メッセージのキャプチャ

パケット監視の使用の詳細については、『*SonicOS 6.5 調査*』を参照してください。

SSO 認証エージェントとの間の復号化されたメッセージをキャプチャするには、以下の手順に従います。

1. 「**調査 | ツール > パケット監視**」に移動します。
2. 「**16 進ダンプ**」セクションの「**設定**」を選択します。「**パケット監視の設定**」ダイアログが表示されます。
3. 「**詳細監視フィルタ**」を選択します。
4. 「**中間パケットを監視する**」を選択します。
5. 「**中間復号化されたシングル サインオン エージェント メッセージを監視する**」を選択します。
6. 「**OK**」を選択します。

パケットには、「受信」と「送信」のインターフェース フィールドに **(SSO)** というマークが付きます。これらのパケットのイーサネット、TCP、および IP ヘッダーはダミーであるため、これらのフィールドの値は正しくないことがあります。

これによって、復号化された SSO パケットをパケット監視にフィードできますが、監視フィルタは引き続き適用されます。

キャプチャされた SSO メッセージは、完全に復号化されて「**ツール > パケット監視**」ページに表示されます。

LDAP over TSL メッセージのキャプチャ

復号化された LDAP over TLS (LDAPS) パケットを監視するには、以下の手順に従います。

1. 「**調査 | ツール > パケット監視**」に移動します。
2. 「**16 進ダンプ**」セクションの「**設定**」を選択します。「**パケット監視の設定**」ダイアログが表示されます。

3 「**詳細監視フィルタ**」を選択します。

4 「**中間パケットを監視する**」を選択します。

5 「**中間復号化された TLS 上 LDAP パケットを監視する**」を選択します。

6 「**OK**」を選択します。

パケットには、「受信」と「送信」のインターフェース フィールドにマーク (**ldp**) が付きます。これらのパケットのイーサネット、TCP、および IP ヘッダーはダミーであるため、これらのフィールドの値は正しくないことがあります。外部のキャプチャ解析プログラム (Wireshark など) がこれらのパケットを LDAP として復号化することを認識できるよう、LDAP サーバ ポートは 389 に設定されています。キャプチャされた LDAP バインド要求内のパスワードは難読化されます。LDAP メッセージは、「パケット監視」画面では復号化されませんが、監視を Wireshark にエクスポートして、復号化された状態で表示することができます。

これによって、復号化された LDAPS パケットをパケット監視にフィード できますが、監視フィルタは引き続き適用されます。

メモ：LDAPS キャプチャは、ファイアウォールの LDAP クライアントからの接続に対してのみ機能します。ファイアウォールを通過した外部 LDAP クライアントからの LDAP over TLS 接続は表示されません。

複数管理者サポートについて

「ローカル ユーザおよびグループの設定 (237 ページ)」に記されているように、複数の管理者プロファイルを設定できます。

RADIUS または LDAP 認証を使用しているとき、RADIUS または LDAP サーバが到達不能であっても管理者ユーザの一部または全員が常に装置を管理できるようにしたい場合は、「**RADIUS + ローカル ユーザ**」または「**LDAP + ローカル ユーザ**」オプションを選択し、これらの特定のユーザのアカウントをローカルで設定します。

RADIUS または LDAP によって認証されるユーザについて、「**SonicWall 管理者**」または「**SonicWall 読取専用管理者**」という名前のユーザ グループを RADIUS サーバまたは LDAP サーバ (またはそのバックエンド) 上に作成し、これらのグループに適切なユーザを割り当てます。

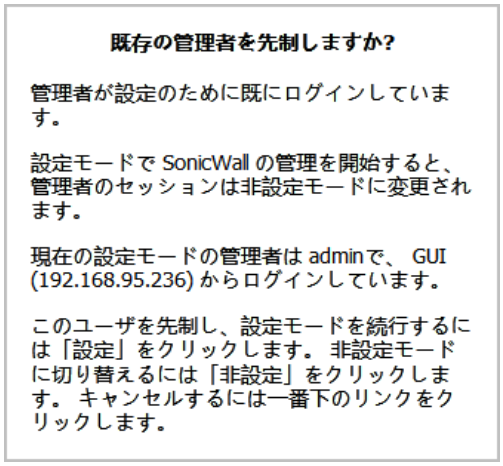
メモ：RADIUS の場合、ユーザ グループ情報を返すための特別な設定が RADIUS サーバに必要となります。

トピック:

- 管理者の先制 (124 ページ)
- 管理者権限によるログイン (124 ページ)

管理者の先制

ある管理者が既にログインしているときに、別の管理者がログインを試みると、次のメッセージが表示されます。



このメッセージでは次の 3 つのオプションが提示されます。

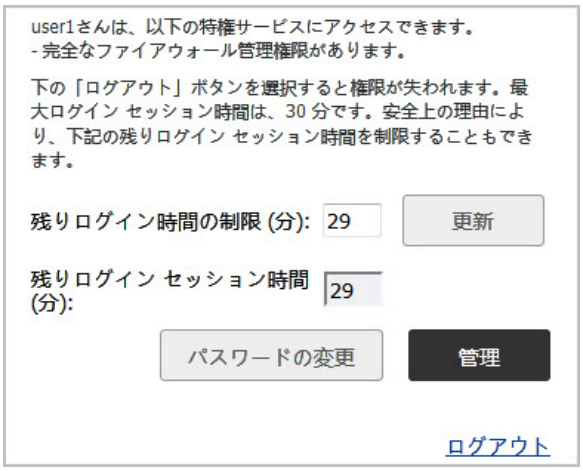
設定	現在の管理者を先制します。現在の管理者は非設定モードに降格され、新しい管理者に完全な管理者アクセス権が付与されます。
非設定	SonicWall セキュリティ装置に非設定モードでログインします。現在の管理者のセッションはそのまま維持されます。
管理を開始しない	ログイン画面に戻ります。

管理者権限によるログイン

管理者以外のユーザ (つまり、**admin** ユーザではない) が、管理者権限を持つユーザとしてログインできます。

管理者権限でログインするには:

1 管理者の資格情報でログインします。「**ユーザ ログイン状況**」メッセージが表示されます。



2 送信先

- SonicWall 管理インターフェースに移動し、「**管理**」を選択します。パスワードの再入力を求められます。これは、管理者がセッションをログアウトせずに自分のコンピュータから離れている隙に不正アクセスされるのを防ぐための措置です。
- パスワードを変更するには、「**パスワードの変更**」を選択します。パスワードを変更するためのダイアログが表示されます。

ユーザ ログイン状況ポップアップの無効化

SonicWall セキュリティ装置への特権的なアクセスのためではなく、セキュリティ装置の管理のためだけに特定のユーザにログインを許可する場合は、「**ユーザ ログイン状況**」ポップアップを無効にすることができます。このポップアップを無効にするには、ローカル グループの追加または編集の際に「**メンバーはウェブ ログインで管理 UI にすぐにアクセスします**」オプションを選択します。

一部のユーザ アカウントを管理専用にして、他のユーザが装置への特権的なアクセスとその管理を行う場合にはログインを要求する (つまり、一部のユーザにはログイン時に管理インターフェースを直接表示し、他のユーザには「**管理**」ボタンが付いた「**ユーザ ログイン状況**」ポップアップ ダイアログを表示する) には、次の手順に従います。

1 ローカル グループを作成し、「**メンバーはウェブ ログインで管理 UI にすぐにアクセスします**」オプションを選択します。
2 このグループを適切な管理グループに追加します。ただし、その管理グループでは上記のオプションを選択しないでください。
3 管理専用にするユーザ アカウントをこの新しいユーザ グループに追加します。これらのユーザについては、「**ユーザ ログイン状況**」ポップアップが無効になります。
4 特権的な管理アクセス権を持たせるユーザ アカウントは、トップレベルの管理グループに直接追加します。

複数管理者サポートの設定

トピック:

- 管理者ユーザ プロファイルの追加設定 (125 ページ)
- LDAP または RADIUS 使用時の管理者のローカル設定 (126 ページ)
- 管理者の先制 (124 ページ)
- 管理者権限によるログイン (124 ページ)
- 複数管理者サポートの設定の確認 (126 ページ)
- 複数管理者関連のログ メッセージの表示 (127 ページ)

管理者ユーザ プロファイルの追加設定

追加の管理者の設定方法は、追加のローカル ユーザを設定したうえで適切なローカル グループに追加する場合と同じです。

グループ	ユーザに付与される権限
制限付き管理者	制限付きの管理者設定権限。
SonicWall 管理者	完全な管理者設定権限。
SonicWall 読み取り専用管理者	管理インターフェース全体に対する表示権限のみ。

ローカル ユーザとローカル グループの設定方法については、「ローカル ユーザおよびグループの設定 (237 ページ)」を参照してください。

LDAP または RADIUS 使用時の管理者のローカル設定

RADIUS または LDAP 認証を使用しているとき、RADIUS または LDAP サーバが到達不能であっても管理者ユーザの一部または全員が常に SonicWall セキュリティ装置を管理できるようにしたい場合は、「**RADIUS + ローカル ユーザ**」または「**LDAP + ローカル ユーザ**」オプションを選択し、これらの特定のユーザのアカウントをローカルで設定します。

RADIUS または LDAP によって認証されるユーザについて、「**SonicWall 管理者**」または「**SonicWall 読取専用管理者**」という名前のユーザ グループを RADIUS サーバまたは LDAP サーバ (またはそのバックエンド) 上に作成し、これらのグループに適切なユーザを割り当てます。

メモ：RADIUS の場合、ユーザ グループ情報を返すための特別な設定が RADIUS サーバに必要となります。

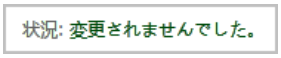
LDAP または RADIUS 使用時の管理者の設定方法については、「ローカル ユーザおよびグループの設定 (237 ページ)」を参照してください。

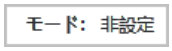
複数管理者サポートの設定の確認

管理者および読み取り専用管理者のユーザ アカウントは、「**管理 | システム セットアップ > ユーザ > ローカル ユーザとグループ > ローカル グループ**」ページで確認できます。

現在の設定モードは、管理インターフェースの右上隅にある「**モード**」で確認できます。

変更を行うと、状況バーに次のように表示されます。





変更を試みると、状況バーに次のように表示されます。

複数管理者関連のログ メッセージの表示

次のイベントが発生した場合、ログ メッセージが生成されます。

- GUI または CLI ユーザが設定モードを開始した (admin ログイン時など)。
- GUI または CLI ユーザが設定モードを終了した (admin ログアウト時など)。
- GUI ユーザが非設定モードでの管理を開始した (admin ログイン時や、設定モードのユーザが先制されて読み取り専用モードに降格された時など)。
- GUI ユーザが読み取り専用モードで管理を開始した。

GUI ユーザは上記のいずれかの管理セッションを終了します (admin ログアウト時など)。

8

ユーザの管理のための設定

トピック:

- ユーザ > 設定 (128 ページ)
  - ユーザ認証とログインの設定 (129 ページ)
  - カスタマイズ (144 ページ)
  - アカウント (151 ページ)
  - RADIUS 認証の設定 (154 ページ)
  - LDAP を使用するための SonicWall の設定 (162 ページ)
  - 拡張 LDAP テストについて (178 ページ)
  - 認証用の TACACS + の設定 (179 ページ)
  - SonicOS で SonicWall SSO エージェントを使用するための設定 (180 ページ)

ユーザ > 設定

「管理 | システム セットアップ > ユーザ > 設定」では、必要な認証方式、グローバル ユーザ設定、ユーザがネットワークにログインしたときに表示される規約の承諾画面を設定できます。

トピック:

- ユーザ認証とログインの設定 (129 ページ)
- ユーザ セッションの設定 (140 ページ)
- RADIUS 認証の設定 (154 ページ)
- LDAP を使用するための SonicWall の設定 (162 ページ)
- 認証用の TACACS + の設定 (179 ページ)
- SonicOS で SonicWall SSO エージェントを使用するための設定 (180 ページ)

ユーザ認証とログインの設定

重要：「**ユーザ > 設定**」ページの設定が完了したら、「**適用**」を選択してください。

トピック:

- ユーザ認証の設定 (130 ページ)
- ユーザ ウェブ ログインの設定 (133 ページ)
- キャプティブ ポータル認証 (136 ページ)
- 認証バイパスの設定 (136 ページ)
- ユーザ セッション設定 (141 ページ)
- SSO で認証されたユーザのユーザ セッションの設定 (142 ページ)
- ウェブ ログイン用ユーザ セッションの設定 (143 ページ)
- ログイン後の規約の承諾 (146 ページ)
- ユーザ定義ログイン ページ (148 ページ)

ユーザ認証の設定

ユーザ認証の設定を行うには、次の手順に従います。

1 「**管理 | システム セットアップ > ユーザ > 設定**」に移動します。

2 パーティション処理が有効かそうでないかによって手順が異なります。

- 有効でない場合は、「ステップ 4」に進みます。
- 有効である場合は、「**認証パーティションごとの個別の設定 (特定の設定に関するもののみ)**」オプションが表示されています。このオプションを選択します。「**パーティションの設定**」のオプションが表示されます。

3 パーティションごとに、以下の「ステップ 4」を行います。

4 「**ユーザ認証方式**」で、ネットワークで使用するユーザ アカウント管理の種別を選択します。

ローカル ユーザ

「**管理 | システム セットアップ > ユーザ > ローカル ユーザとグループ**」ページを使用してセキュリティ装置のローカル データベース内のユーザを設定します。

認証にローカル データベースを使用する方法および詳細な設定手順については、「ローカル ユーザおよびローカル グループを使った認証 (91 ページ)」を参照してください。

RADIUS

ユーザ数が 1,000 人を超える場合、またはセキュリティ装置のユーザ認証にさらなるセキュリティを付加したい場合に選択します。ユーザ認証のために RADIUS を選択した場合、ユーザはセキュリティ装置に送るパスワードを暗号化するために HTTPS を使用してセキュリティ装置にログインする必要があります。ユーザが HTTP を使用してセキュリティ装置へのログインを試みた場合、ブラウザは自動的に HTTPS にリダイレクトされます。

LDAP に加えて RADIUS が必要とされることがあります。

- LDAP は通常 CHAP/MS-CHAP 認証をサポートしないため (Microsoft アクティブ ディレクトリと Novell eDirectory で不可)、 RADIUS が設定されている場合、SonicWall は RADIUS を介して CHAP/MS-CHAP を認証します。
- SSO に NTLM が使用されている場合は、RADIUS を介した MS-CHAP モードでのみ認証できます。

RADIUS が必要と考えられるのは、L2TP サーバや VPN/SSL VPN クライアント (NetExtender とポータルを含む) で CHAP/MS-CHAP を使用する場合、または NTLM を使用する場合です。

メモ：RADIUS を CHAP 認証に使用するとき、CHAP 以外の認証には一般に LDAP がまだ使われます。

認証に RADIUS データベースを使用する方法の詳細については、「RADIUS を使った認証 (93 ページ)」を参照してください。

詳細な設定手順については、「RADIUS 認証の設定 (154 ページ)」を参照してください。

RADIUS + ローカル ユーザ

RADIUS とセキュリティ装置の両方のローカル ユーザ データベースを認証に使用します。

LDAP

Lightweight Directory Access Protocol (LDAP) サーバ、Microsoft アクティブ ディレクトリ (AD) サーバ、または Novell eDirectory を使用してユーザ アカウント データを管理する場合に選択します。

認証に LDAP データベースを使用する方法の詳細については、「LDAP/アクティブ ディレクトリ/イーディレクトリ認証の使用 (94 ページ)」を参照してください。

詳細な設定手順については、「SonicWall セキュリティ装置への LDAP の統合 (97 ページ)」を参照してください。

LDAP + ローカル ユーザ

LDAP とセキュリティ装置の両方のローカル ユーザ データベースを認証に使用します。

TACACS +

TACACS + (Terminal Access Controller Access-Control System の最新世代) をユーザの認証に使用します。

TACACS + ローカル ユーザ	TACACS + とセキュリティ装置の両方のローカル ユーザ データベースを認証に使用します。

5 「**シングルサインオン方式**」は、以下から 1 つを選択します。

メモ：ユーザ認証にシングル サインオンを使用していない場合、以上のオプションをいずれも選択しないでください。

SSO エージェント	認証にアクティブ ディレクトリを使用していて、SSO エージェントが同じドメイン内のコンピュータにインストールされている場合に選択します。SSO の詳細な設定手順については、「シングル サインオンについて (114 ページ)」を参照してください。
ターミナル サービス エージェント	ターミナル サービスを使用していて、ターミナル サービス エージェント (TSA) が同じドメイン内のターミナル サーバにインストールされている場合に選択します。
RADIUS アカウント	ネットワーク アクセス サーバ (NAS) からアカウント サーバにユーザ ログイン セッション アカウント メッセージを送信する場合に選択します。
サードパーティ API	サードパーティの API を使用します。
ブラウザ NTLM 認証のみ	SSO エージェントまたは TSA を使わずにウェブ ユーザを認証したい場合に選択します。ユーザは HTTP トラフィックを送信すると即時に識別されます。NTLM は MSCHAP 認証にアクセスするために RADIUS (LDAP を使う場合は LDAP) が設定されている必要があります。上で LDAP が選択されている場合は、NTLM を選択した際に RADIUS のための独立した「**設定**」が現れます。

6 ユーザ アカウント名を照合する際に大文字と小文字を区別する場合は、「**ユーザ名の大文字と小文字を区別する**」を選択します。

7 複数の場所から同じユーザ名でネットワークにログインできないようにするには、「**多重ログインを禁止する**」を選択します。このオプションは、ローカル ユーザと RADIUS/LDAP ユーザの両方に適用されますが、ユーザ名 **admin** の既定の管理者には適用されません。このオプションは、既定では選択されていません。

8 パスワードの変更後にユーザをログインさせるには、「**パスワードが変更された後に再ログインを強制する**」をオンにします。このオプションは、既定では選択されていません。

9 前回のログイン以降に生じたユーザ ログイン情報を表示するには、「**監視 | 現在の状況 > システム状況**」ページで「**最終ログイン以降のユーザ ログイン情報を表示する**」を選択します。このオプションは、既定では選択されていません。

このオプションを有効にすると、ユーザ ログイン情報 (最後にログインが成功した日時、すべてのユーザのログイン試行成功数、ログイン試行失敗数、管理者権限の変更回数) が「**調査 | ログ > イベント ログ**」に表示されます。ログの詳細については、『*SonicOS 6.5 調査*』を参照してください。

10 以下の「**ワンタイム パスワード**」のオプションを設定します。

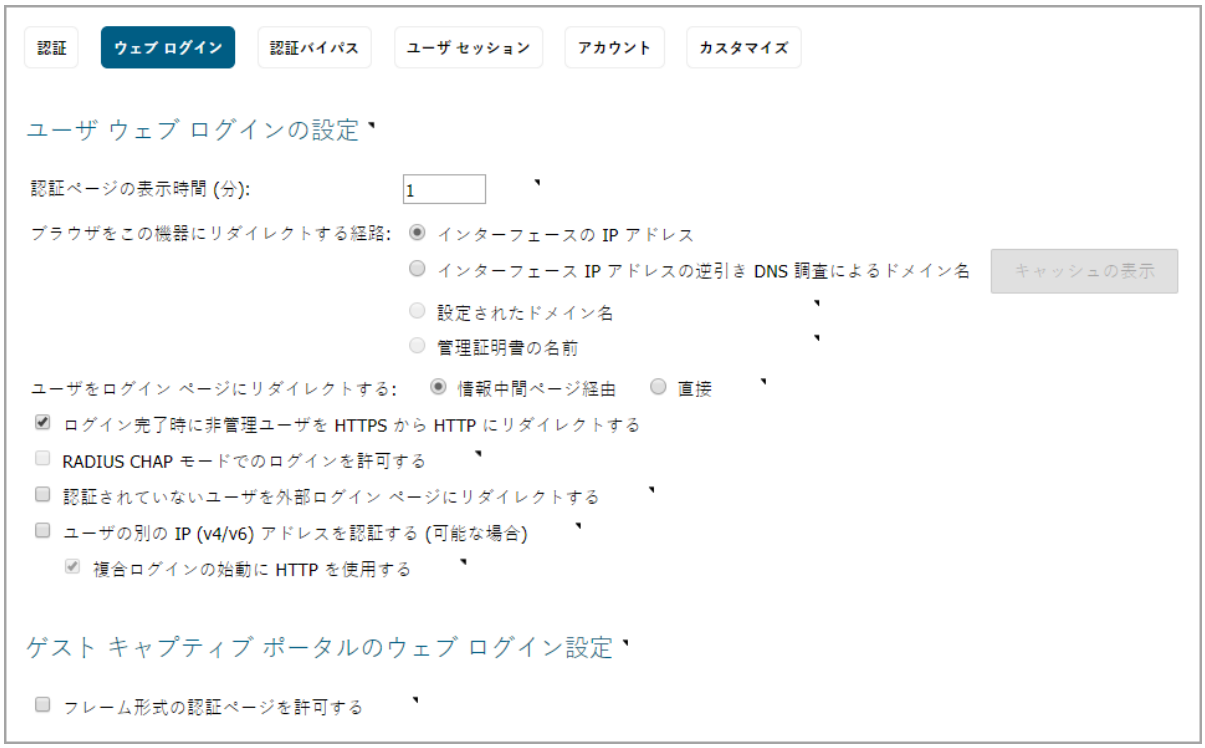
- **ワンタイム パスワードの電子メール形式** -「**プレーン テキスト**」または「**HTML**」を選択します。

- **ワンタイム パスワード形式** -「**英字**」 (既定値)、「**英数字**」、または「**数字**」をドロップダウン メニューから選択します。

  ヒント：パスワードの 2 つの値と共に形式を選択することで、パスワードの強度は「脆弱」、「良」、または「優秀」とされます。特に強力なパスワードは、「**英字**」または「**英数字**」を用いた長いパスワードです。特に脆弱なパスワードは、長さに関係なく「**数字**」を用いたパスワードです。

- 「**ワンタイム パスワード長**」では、最初のフィールドに最小の長さを、次のフィールドに最大の長さを入力します。最小と最大の長さは 4 ～ 14 文字の範囲で指定し、各フィールドの既定値は **10** です。最小の長さを最大の長さより大きくすることはできません。

ユーザ ウェブ ログインの設定



ユーザ ウェブ ログインの設定を行うには、次の手順に従います。

1 「**管理 | システム セットアップ | ユーザ > 設定**」に移動します。

2 「**ウェブ ログイン**」を選択します。

3 「**認証ページの表示時間 (分)**」フィールドには、ユーザがユーザ名とパスワードを使ってログインするまでの制限時間、つまりログイン ページがタイム アウトするまでの分数を入力します。ログイン ページがタイム アウトすると、再度ログインを試みる前に行うべきことを知らせるメッセージが表示されます。既定値は **1** 分です。

   ログイン認証ページが表示されている間はシステム リソースが消費されます。時間制限を設けてその間にログインしなければログイン ページを閉じるようにすることで、それらのリソースを解放します。

4 ユーザのブラウザを SonicWall 装置のウェブ サーバに最初にリダイレクトする方法を指定するために、「**ブラウザをこの機器にリダイレクトする経路**」でオプションを選択します。

- **インターフェースの IP アドレス** - ブラウザを装置のウェブ サーバ インターフェースの IP アドレスにリダイレクトする場合に選択します。このオプションは、既定では選択されています。
- **インターフェース IP アドレスの逆引き DNS 調査によるドメイン名** - 「**キャッシュの表示**」が有効になります。このボタンを選択すると、装置のウェブ サーバのインターフェース、IP アドレス、DNS 名、および TTL (秒) が表示されます。このオプションは、既定では選択されていません。

  「**キャッシュの表示**」を選択して、ユーザのブラウザをリダイレクトするために使われているドメイン名 (DNS 名) を確認します。

- **設定されたドメイン名** - これを選択すると、「**システム セットアップ | 装置 > 基本設定**」で設定したドメイン名へのリダイレクトが有効化されます。管理証明書の名前へのリダイレクトが許可されるのは、インポートした証明書がそのページで HTTPS ウェブ管理用として選択してある場合です。

  メモ：このオプションは、「**システム セットアップ | 装置 > 基本設定**」でドメイン名を指定した場合にのみ使用できます。指定していない場合、このオプションはグレーアウトされます。

- **管理証明書の名前** - これを選択すると、適切な署名済み証明書のあるドメイン名へのリダイレクトが有効化されます。この管理証明書の名前へのリダイレクトが許可されるのは、インポートした証明書がそのページで HTTPS ウェブ管理用として選択してある場合です。「**システム セットアップ | 装置 > 基本設定**」でドメイン名を設定します。

  メモ：このオプションは、「**システム セットアップ | 装置 > 基本設定**」の「**ウェブ管理設定**」セクションで証明書を HTTPS 管理用としてインポートした場合にのみ使用できます。「基本設定の構成 (18 ページ)」を参照してください。

  ヒント：インポートした管理証明書を使用する場合は、このオプションを使います。管理証明書を使用するつもりがなければ、「**設定されたドメイン名**」オプションを選択します。

  HTTPS 管理を行うときブラウザで無効な証明書の警告が表示されないようにするには、証明機関によって適切に署名された証明書 (管理証明書) をインポートする必要があります。内部的に生成された自己署名証明書はこの目的に合いません。この証明書は、当該装置およびそのホスト ドメイン名を対象として生成されたものでなければなりません。適切に署名された証明書は、装置のドメイン名を取得する最善の方法です。

  管理証明書を使用する場合、証明書に関する警告が表示されないようにするには、ブラウザを IP アドレスではなく、そのドメイン名へリダイレクトする必要があります。例えば、インターネットをブラウズしていて `https://gateway.sonicwall.com/auth.html` のログインにリダイレクトされた場合、装置上の管理証明書によって装置が実際に `gateway.sonicall.com` だとわかるので、ブラウザはそのログイン ページを表示します。しかし、リダイレクト先が `https://10.0.02/auth.html` の場合は、証明書の示す装置が `gateway.sonicall.com` であってもブラウザはそれが正しいか判断できないので、代わりに証明書に関する警告を表示します。

5 HTTPS でログインしたユーザをセキュリティ装置からネットワーク接続させるとき HTTP を使いたい場合は、「**ログイン完了時にユーザを HTTPS から HTTP にリダイレクトする**」を選択します。HTTPS は HTTP よりも多くのシステム リソースを消費するので、HTTPS でのログイン ユーザ数が多い場合には、HTTP へのリダイレクトを使用したほうがよいでしょう。このオプションは、既定では選択されています。このオプションをオフにすると、警告ダイアログが表示されます。

6 RADIUS ユーザが HTTP でログインする際に CHAP チャレンジを発行する場合は、「**RADIUS CHAP モードでのログインを許可する**」を選択します。これは、HTTPS を使わずに保護された接続を可能にします。RADIUS サーバがこのオプションをサポートしていることを確認してください。このオプションは、既定では選択されていません。

ⓘ **メモ**：この方式を使用してログインする場合は、実行できる管理操作が制限されます。一部の操作で、装置が管理者のパスワードを知る必要があるからです。リモート認証サーバによる CHAP 認証では、装置がパスワードを知る必要はありません。

したがって、この設定が有効になっていると、管理ユーザ グループに所属するユーザは管理目的でログインする場合に HTTPS を通して手動でログインしなければならないことがあります。この制限は組み込みの **admin** アカウントには適用されません。

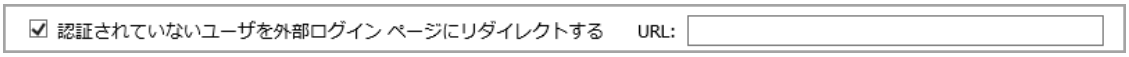
ⓘ **メモ**：LDAP を使用するとき、このメカニズムを標準的に利用するには、「**ログインのための認証方法**」を **RADIUS** に設定し、RADIUS に関する設定を行う際にユーザ グループ メンバーシップの設定メカニズムとして LDAP を選択します。

7 認証されていないユーザからの HTTP/HTTPS トラフィックを SonicWall 固有のログイン ページではなく所定の URL にリダイレクトするには、「**認証されていないユーザを外部ログイン ページにリダイレクトする**」を選択します。このオプションを使用すると、ユーザを外部の認証システムで認証できるようになります。このオプションは、既定では選択されていません。

ⓘ **ヒント**：認証されていないユーザだけをリダイレクトできるようにするには、この状況に対応する 1 つ以上のアクセス ルールを作成する必要があります。

ⓘ **メモ**：その後、外部システムは SSO 用のサードパーティ API や RADIUS アカウントを使用してユーザの名前と資格情報をファイアウォールに渡すことができるので、アクセス制御やログ記録といったアクティビティでユーザが特定されるようになります。

このオプションを選択すると、「**URL**」フィールドが表示されます。



このフィールドにリダイレクト先の URL を入力します。

8 特定のゾーンのゲスト設定に基づいて構成されたキャプティブ ポータルを満足するようにオプションの設定を構成するには、「**ゲスト キャプティブ ポータルのウェブ ログイン設定**」までスクロールします。

9 キャプティブ ポータルでのゲスト認証で、認証ページをフレームとしてポータル ホスト ページに表示できるようにするには、「**フレーム形式の認証ページを許可する**」を選択します。このオプションは、既定では選択されていません。

10 「**適用**」を選択します。

キャプティブ ポータル認証

キャプティブ ポータル認証は、認証され承認されたユーザによるアクセスを支援します。ネットワークへのウェブ アクセスを求めるユーザは、RADIUS サーバと統合されたキャプティブ ポータル サーバでホストされている認証ウェブ ログイン ページにリダイレクトされます。

この認証方法は、SonicWall の既存の LHM (Lightweight Hotspot Messaging) の拡張です。LHM 展開では、すべての認証を外部 LHM サーバで処理する必要があります。キャプティブ ポータル認証では、ファイアウォール自体をさらに活用してRADIUS サーバと通信し、認証プロセスを完了します。

キャプティブ ポータル認証を設定するには:

1 RADIUS ポータル サーバを設定します。

   a ユーザ情報とユーザ グループ情報を設定します。ユーザ グループ名は次の条件を満たす必要があります。

      - ACCEPT メッセージとともにファイアウォールに戻ってください。
      - ファイアウォールのグループ名と一致させてください。
      - ファイアウォールでゲスト特権を持っています。

   b ACCEPT メッセージで返すことをファイアウォールが要請している場合は、「**アイドル タイムアウト**」および「**セッション タイムアウト**」属性を設定します。

   c ウェルカム URL を**ベンダー固有属性**として定義します。SonicWall のベンダー コードは 8741 です。

   d RADIUS アカウントがサポートされている場合は、暫定間隔を設定します。

2 「**管理 | システム セットアップ > ユーザ > 設定**」に移動します。

3 「**認証**」を選択します。

4 「**ユーザ認証の設定**」で、「**ユーザ認証方式**」から「**RADIUS + ローカル ユーザ**」を選択します。

5 「**RADIUS の設定**」を選択します。「**RADIUS の設定**」ダイアログが表示されます。

6 「**RADIUS ユーザ**」を選択します。

7 「**RADIUS ユーザに対するグループ メンバーシップの検索方式:**」では、「**Filter-Id 属性を RADIUS サーバで使用する**」を選択します。

8 「**OK**」を選択します。

9 「**管理 | システム セットアップ > ネットワーク > ゾーン**」に移動します。

10 無線ゾーンの場合は、**追加**アイコンまたは**編集**アイコンを選択します。「**ゾーンの追加 / ゾーンの編集**」ダイアログが表示されます。

11 「**セキュリティ種別**」が**無線**であることを確認してください。

12 RADIUS によるキャプティブ ポータル認証用にゾーンを設定する手順に従います。

認証バイパスの設定

SonicOS ゲスト サービスは、保護されたネットワークに対するアクセスをゲスト ユーザに与えることなく、ゲスト ユーザがネットワークを通じて直接インターネットに接続できるようにします。これを行うために、SonicOS はユーザのコンピュータの IP アドレスを使用します。

IP アドレスを識別子として使用することは、ゲスト ユーザ トラフィックがネットワーク ルータを通過する場合に役立ちます。この場合、送信元 MAC アドレスはルータの MAC アドレスに変わるからです。これに対し、ユーザの IP アドレスは変わらずに通過します。

MAC アドレスのみを使って識別を行う場合、同じルータを通る 2 つのクライアントは同じ MAC アドレスでセキュリティ装置に到達します。その結果、一方のクライアントが認証されると、もう一方のクライアントからのトラフィックも認証済みとして処理され、ゲスト サービス認証をバイパスすることになります。

クライアントの IP アドレスを使って識別することによって、ルーティング機器を通るすべてのゲスト クライアントを個別に認証することが必要となります。

トピック:

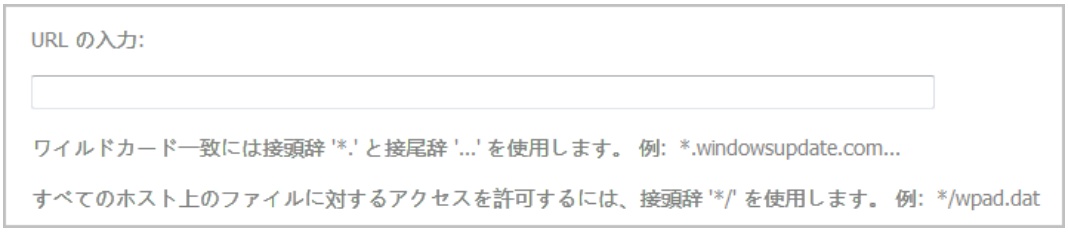
- 認証バイパスへの URL の追加 (137 ページ)
- 自動設定の設定 (138 ページ)
- ワイルドカード一致への URL の変換 (140 ページ)
- ネットワークへの変換 (140 ページ)

認証バイパスへの URL の追加

アクセス ルールに HTTP URL ユーザ認証バイパスを追加するには:

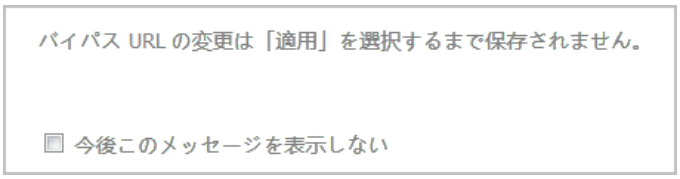
1 「**システム セットアップ | ユーザ > 設定 > 認証バイパス**」に移動します。

2 「**追加**」を選択します。「**URL の追加**」ポップアップが表示されます。



3 「**URL の入力**」フィールドに URL を入力します。

4 「**OK**」を選択します。確認メッセージがポップアップで表示されます。



5 「**OK**」を選択します。

6 URL の追加が完了したら、「**適用**」を選択します。

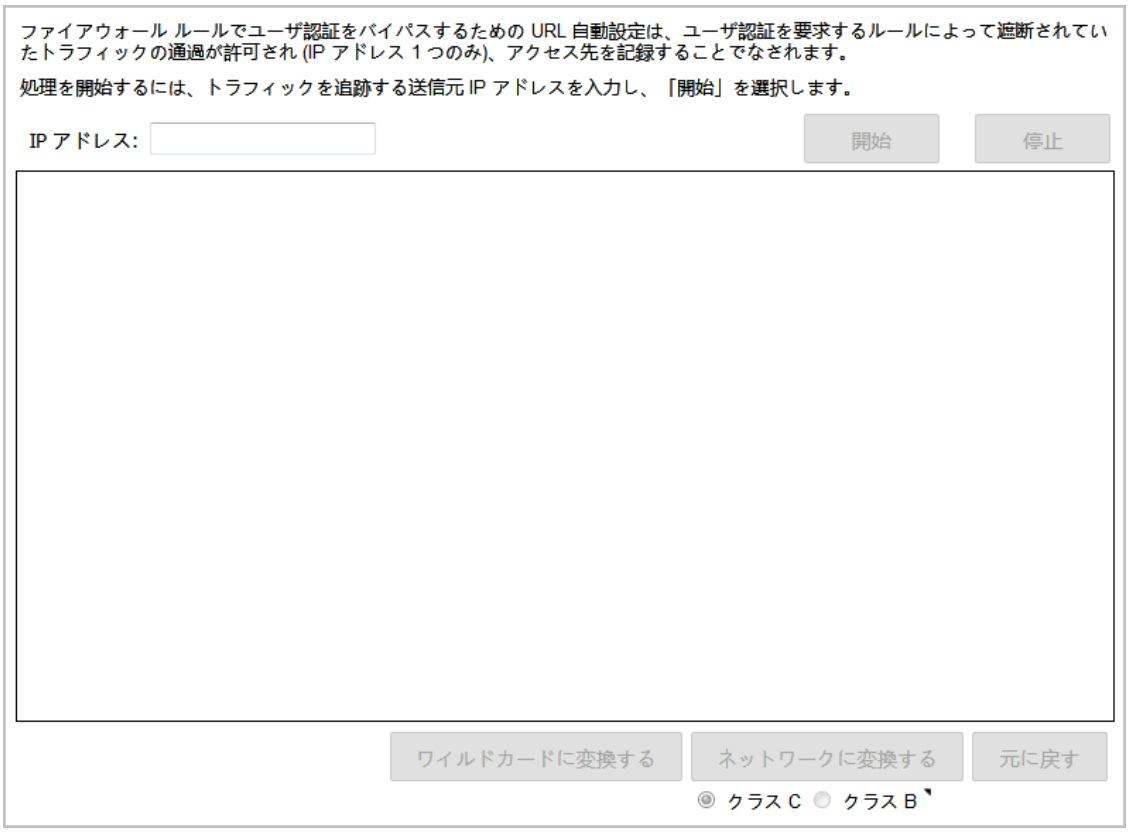
自動設定の設定

ファイアウォール ルールでユーザ認証をバイパスするための URL 自動設定は、ユーザ認証を要求するルールによって遮断されていたトラフィックの通過が許可され (IP アドレス 1 つのみ)、アクセス先を記録することでなされます。

自動設定を設定するには:

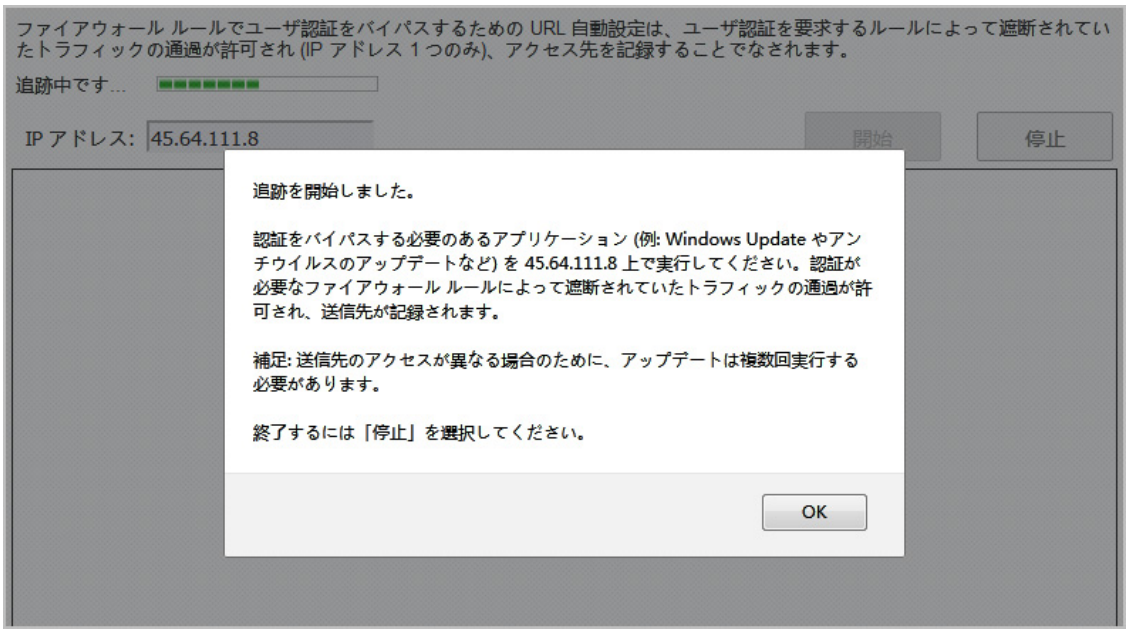
1 「**システム セットアップ | ユーザ > 設定 > 認証バイパス**」に移動します。

2 「**自動設定**」を選択します。「**ユーザ認証バイパス自動設定のポリシー**」ダイアログが表示されます。



3 「**IP アドレス**」フィールドに送信元 IP アドレスを入力します。「**開始**」が使用可能になります。

4 「**開始**」を選択します。「**追跡中です**」というインジケータと「**追跡を開始しました**」というメッセージが表示されます。



5 「**OK**」を選択します。

ワイルドカード一致への URL の変換

バイパス認証ではワイルドカード一致がサポートされます。これによって、追跡する 1 つ以上の URL を、現在選択している すべての URL に一致する単一のワイルドカードに変換することができます。

メモ：選択している URL のドメインが同じである必要があります。

ネットワークへの変換

Windows Update には HTTPS でアクセスする送信先があり、これらの送信先は IP アドレスでのみ追跡できます。ただし、実際にアクセスする IP アドレスは毎回異なるので、この場合は IP アドレスごとにバイパスを設定する代わりに、そのネットワーク上のすべての IP アドレスへの HTTPS のバイパスを許可することができます。

ネットワーク バイパスへの変換では、追跡する HTTPS 送信先 IP アドレスを以下のいずれかに変換できます。

- クラス B (16 ビット) ネットワーク (既定)
- クラス C (24 ビット) ネットワーク

ユーザ セッションの設定

トピック:

- ユーザ セッション設定 (141 ページ)
- SSO で認証されたユーザのユーザ セッションの設定 (142 ページ)
- ウェブ ログイン用ユーザ セッションの設定 (143 ページ)

ユーザ セッション設定

セキュリティ装置を通して認証されるすべてのユーザに適用される設定を構成するには、次の手順に従います。

1 無動作状態が一定期間続いたらユーザをセキュリティ装置からログアウトさせる時間の長さを「**無動作時タイムアウト (分)**」フィールドで指定します。既定値は **15** 分です。

2 「**無動作時のユーザ ログアウトを防ぐために次のサービスからのトラフィックを許可しない**」ドロップダウン メニューから、無動作ユーザのログアウトを阻止するサービスまたはサービス グループ オプションを選択します。このオプションを有効化すると、ユーザはログアウトではなく非アクティブ化されるので、システムのオーバーヘッドが減り、寿命が超過した認証済みユーザを再度識別する場合に生じる遅延が回避されます。無動作ユーザはシステム リソースを消費しませんが、「**ユーザ > 状況**」ページには表示されます。既定は「**なし**」です。

3 以下の「**ユーザが識別されていない接続のログ記録**」オプションで、 実行するログ記録の種類 (「**ユーザ名をログに記録しない**」または「**ユーザ名をログに記録する**」) を選択し、必要に応じてログ ユーザ名も選択します。

- **SSO がユーザの識別に失敗した場合:ユーザ名をログに記録する - 不明 SSO 失敗** (既定値)
- **SSO をバイパスする接続の場合:ユーザ名をログに記録する - SSO バイパス** (既定値)

  メモ：このオプションは、「**シングル サイン オン認証設定**」ダイアログの「強制」タブの「**SSO バイパス**」セクションで設定できます。

- **発信元が外部である接続の場合: ユーザ名をログに記録しない** (既定値); 「**ユーザ名をログに記録する**」を選択した場合、既定のユーザ名は**不明 (外部)**
- **その他の識別できない接続の場合: ユーザ名をログに記録しない** (既定値); 「**ユーザ名をログに記録する**」を選択した場合、既定のユーザ名は**不明**

4 ユーザが SonicWall 装置からログアウトした後も残るユーザの接続をどう処置するかを「**ログアウト時の残りのユーザ接続に対する動作**」オプションで指定します。

ログアウトの種類	動作	
	ユーザ認証を必要とする接続の場合 [a]	その他の接続の場合 [b]
無動作によるログアウト時の動作	接続を維持 (既定値) 接続を終了 次の時間経過後に終了: ... 分	接続を維持 (既定値) 接続を終了 次の時間経過後に終了: ... 分
能動的/報告対象ログアウト時の動作	接続を維持 接続を終了 (既定値) 次の時間経過後に終了: ... 分	接続を維持 接続を終了 次の時間経過後に終了: 15 分 (既定値)

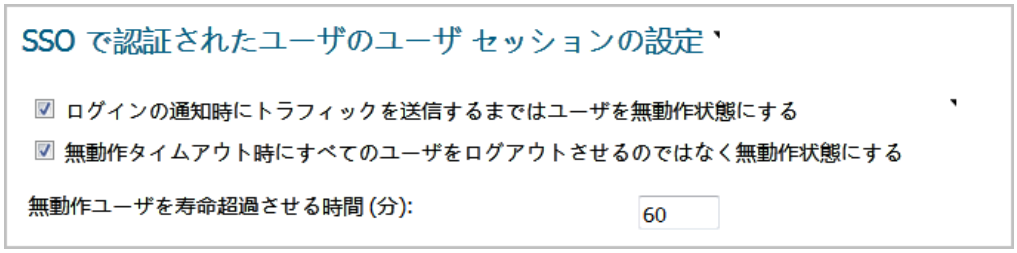
a. 特定のユーザのみを許可するアクセス ルールによる接続に対して適用されます。

b. 特定のユーザ認証要件を備えていないその他の接続に対して適用されます。

以下に対しては、別の動作を設定できます。

- 無動作によるログアウト (ユーザがドメイン/コンピュータにログインしたままのこともあれば、そうでないこともある)
- ユーザによる能動的なログアウト、または SonicWall 装置へのユーザ ログアウトの報告 (後者は通常、ユーザがドメイン/コンピュータからログアウトしたことを意味する)

SSO で認証されたユーザのユーザ セッションの設定



SSO で認証された無動作ユーザの処置を指定するには、次の手順に従います。

1 SonicWall 装置から SSO メカニズムを通して識別されたユーザを、そのユーザからのトラフィックをまだ受け入れていない段階で、無動作状態にしてリソースが消費されないようにするには、「**ログインの通知時にトラフィックを送信するまではユーザを無動作状態にする**」チェックボックスをオンにします。ユーザの無動作状態はトラフィックを受け取るまで続きます。このオプションは、既定では選択されています。

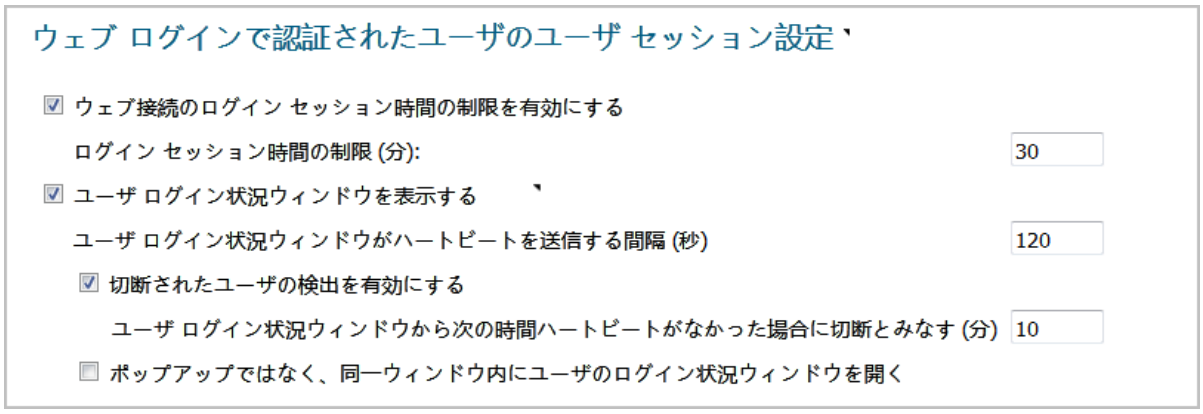
SSO メカニズムによっては、SonicWall 装置がユーザを能動的に再識別する仕組みを提供していない場合があり、そのようなメカニズムで識別されたユーザからトラフィックが送られてこないと、装置が最終的にユーザのログアウト通知を受け取るまで、ユーザは無動作状態のままになります。それ以外の再識別可能なユーザは、無動作状態のままトラフィックを送信しないと、「ステップ 3」で設定できる期間を超過したときに寿命超過で削除されます。

2 能動的にログインして SSO で識別されたユーザが無動作によりタイムアウトした場合、再識別されなければユーザは無動作状態に戻ります。何も処置しなければ無動作によりログアウトするところのユーザを無動作状態に戻すには、「**無動作タイムアウト時にすべてのユーザをログアウトさせるのではなく無動作状態にする**」チェックボックスをオンにします。これを行うと、オーバーヘッドが減り、動作状態に復帰するユーザを再識別する場合に生じる遅延が回避されます。このオプションは、既定で選択されています。

3 無動作ユーザが寿命超過処置の対象となる場合、無動作状態のままトラフィックを送信しなかったとき寿命超過で削除されるまでのタイムアウト時間 (分) を設定できます。具体的には、「**無動作ユーザを寿命超過させる時間 (分)**」チェックボックスをオンにし、フィールドにタイムアウト時間を入力します。この設定は既定で選択されています。最小タイムアウト値は 10 分、最大値は 10000 分、デフォルト値は **60** 分です。

メモ：無動作ユーザと動作中のユーザを区別する理由はユーザの管理に使われるリソースの消費を抑えるためであり、寿命超過タイマーは 10 分間隔で更新されます。そのため、無動作ユーザが実際に削除されるまでの時間は、ここで設定した時間よりも最大で 10 分長くなる可能性があります。

ウェブ ログイン用ユーザ セッションの設定



ウェブ ログインのユーザ セッションの設定を行うには、次の手順に従います。

1 **ウェブ接続のログイン セッション時間の制限を有効にする**: ウェブ ログインからセキュリティ装置にログインするユーザのログイン時間を制限するには、このチェック ボックスをオンにし、「**ログイン セッション時間の制限 (分)**」フィールドに時間を分単位で入力します。この設定は既定で選択されています。既定値は **30** 分です。

2 **ユーザ ログイン状況ウィンドウを表示する** - ウェブ ログインからログインするユーザについて、ユーザのセッション中に「**ログアウト**」ボタン付きの状況ウィンドウが表示されます。「**ログアウト**」を選択することにより、セッションからログアウトすることができます。

メモ：ユーザのセッション中は、このウィンドウをずっと開いておかなければなりません。ウィンドウを閉じると、ユーザはログアウトします。

重要：このオプションを有効化しないと、状況ウィンドウは表示されず、ユーザがログアウトできないことがあります。その場合は、ログイン セッション時間の制限を設けてユーザを最終的にログアウトさせなければなりません。

「**ユーザ ログイン状況**」ウィンドウには、ログイン セッションの残りの分数が表示されます。ユーザは、数値を入力して「**更新**」を選択することで、残りの分数を短く設定し直すこともできます。

このオプションを有効化すると、そのウィンドウから送られてくるハートビートを監視するメカニズムも有効化し、ログアウトせずに切断されたユーザを検知してログアウトさせることができます。

ユーザが SonicWall Administrators グループまたは Limited Administrators グループのメンバーである場合、「**ユーザ ログイン状況**」ウィンドウには「**管理**」ボタンが表示されます。このボタンを選択すると、セキュリティ装置の管理インターフェースに自動的にログインできます。管理ユーザの「**ユーザ ログイン状況**」ウィンドウを無効にする方法の詳細については、「ユーザ

ログイン状況ポップアップの無効化 (125 ページ)」を参照してください。グループの設定手順については、「ローカル ユーザおよびグループの設定 (237 ページ)」を参照してください。

- **ユーザ ログイン状況ウィンドウがハートビートを送信する間隔 (秒)** - ユーザが有効な接続を保持しているかどうかを確認するために使用されるハートビート信号の周期を設定します。ハートビート信号の周期は、最小 10 秒、最大 65530 秒で、既定値は **120** 秒です。

3 **切断されたユーザの検出を有効にする** - 接続が有効でなくなったユーザを検出すると、セキュリティ装置はそのセッションを終了させます。このオプションは、既定で選択されています。

- **ユーザ ログイン状況ウィンドウから次の時間ハートビートがなかった場合に切断とみなす (分)**: ハートビートからの応答がなかった場合に、ユーザ セッションを終了するまでの時間を設定します。ユーザ セッションを終了するまでの遅延時間は、最小 1 分、最大 65535 分で、既定値は **10** 分です。

4 ユーザのログイン状況ウィンドウを、ポップアップ ウィンドウではなく、同じウィンドウ内に表示する場合は、「**ポップアップではなく、同一ウィンドウ内にユーザのログイン状況ウィンドウを開く**」チェックボックスをオンにします。

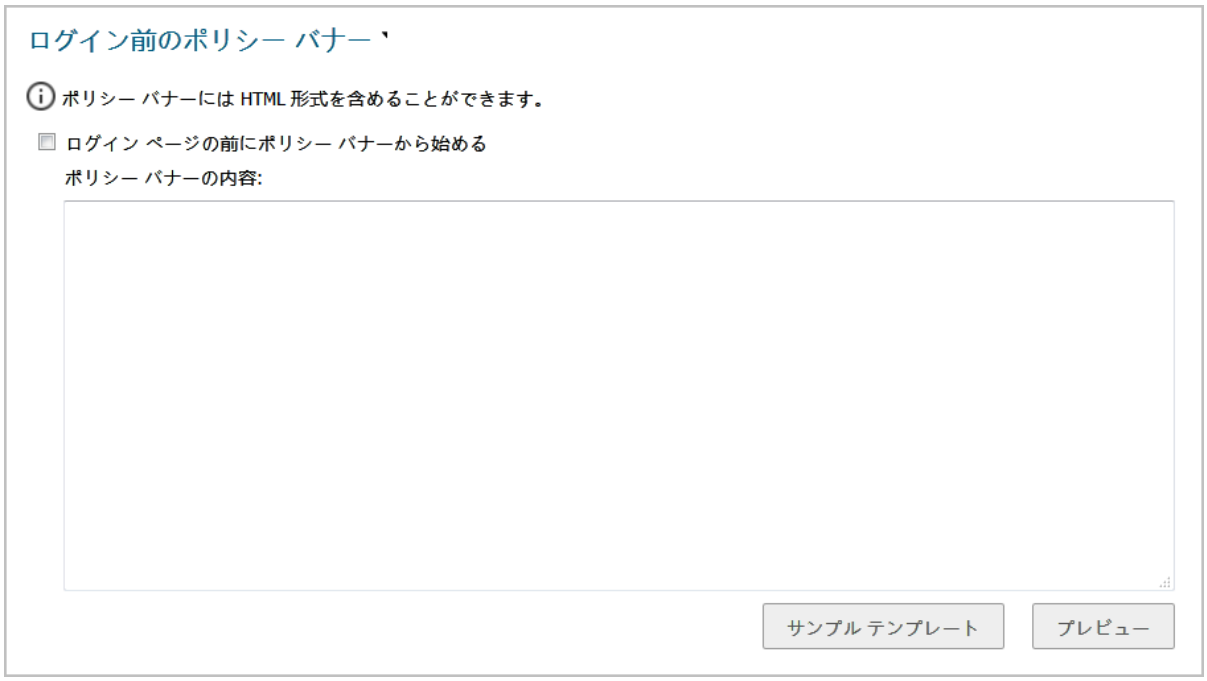
カスタマイズ

トピック:

- ログイン前のポリシー バナー (144 ページ)
- ログイン後の規約の承諾 (146 ページ)
- ユーザ定義ログイン ページ (148 ページ)

ログイン前のポリシー バナー

このセクションでは、ウェブ ログインの前にすべてのユーザにウィンドウ内のバナーとして提示されるポリシー ステートメントを作成します。ポリシー バナーに HTML フォーマットを含めてもかまいません。



ログイン前のポリシー バナーを作成するには:

1 「**管理 | システム セットアップ | ユーザ > 設定**」に移動します。

2 「**カスタマイズ**」を選択します。

3 「**ログイン前のポリシー バナー**」セクションまでスクロールします。

4 「**ログイン前のポリシー バナー**」セクションで、「**ログイン ページの前にポリシー バナーから始める**」を選択します。このオプションは、既定では選択されていません。

5 「**ポリシー バナーの内容**」フィールドにポリシー テキストを入力します。HTML フォーマットを含めることができます。ユーザに表示されるこのページには、ユーザの確認操作用の「**承諾する**」と「**キャンセル**」があります。

> **ヒント：**「**サンプル テンプレート**」を選択すると、ポリシー バナー ウィンドウ用に書式設定済みの HTML テンプレートが挿入されます (「サンプル テンプレート (145 ページ)」を参照)。

6 「**適用**」を選択します。

トピック:

- サンプル テンプレート (147 ページ)
- プレビュー メッセージ (145 ページ)

サンプル テンプレート

「**サンプル テンプレート**」を選択すると、既定の AUP テンプレートの内容が表示されます。この内容は自由に変更することができます。

```
<font face=arial size=3>
<center><b><i>ようこそ</center></b></i>
<font size=2>

<table width="100%" border="1">
<tr><td>
<font size=2>
<br><br><br>
<center>ここに規約を記述します。
<br><br><br>
</td></tr>
</table>
```

これらの規約を承諾して続行するには「承諾する」を選択してください。そうでない場合は「キャンセル」を選択してください。

プレビュー メッセージ

「**プレビュー**」を選択すると、作成した AUP メッセージがどのようにユーザに表示されるかを確認できます。

ログイン後の規約の承諾

規約承諾 (AUP) は、ネットワークやインターネットにアクセスするためにユーザが従う必要のあるポリシーです。多くの企業や教育施設では、社員や学生が セキュリティ装置 を使用してネットワークやインターネットにアクセスする前に、規約の承諾に同意するよう求めるのが一般的です。

「**ログイン後の規約の承諾**」セクションでは、ユーザのために表示する AUP メッセージ ウィンドウを作成できます。メッセージの本文には HTML フォーマットを使用できます。「**サンプル テンプレート**」を選択すると、AUP ウィンドウ用に書式設定済みの HTML テンプレートが挿入されます (「サンプル テンプレート (147 ページ)」を参照)。

ログイン後の AUP メッセージ ウィンドウを作成するには:

1 「**管理 | システム セットアップ | ユーザ > 設定**」に移動します。

2 「**カスタマイズ**」を選択します。

3 「**ログイン後の規約の承諾**」セクションまでスクロールします。

4 以下の設定を行います。

- **規約の承諾を要求する** - ユーザがログインしたときに規約承諾画面を表示するネットワーク インターフェースを選択します。「**保護ゾーン**」(既定値)、「**WAN ゾーン**」、「**公開ゾーン**」(既定値)、「**無線ゾーン**」、「**VPN ゾーン**」を任意に組み合わせて選択できます。
- **ウィンドウ サイズ (ピクセル)** - AUP ウィンドウのサイズをピクセル単位で指定できます。
  - 幅: 最小 400 ピクセル、最大 1280 ピクセルで、既定値は **460** ピクセルです。
  - 高さ: 最小 200 ピクセル、最大 1024 ピクセルで、既定値は **310** ピクセルです。
- **ウィンドウでスクロール バーを有効にする** - ウィンドウの表示サイズに内容が収まりきらない場合、スクロール バーが表示されます。このオプションは、既定では選択されています。

- **規約承諾画面の内容** - 規約承諾のテキストを、このフィールドに入力します。HTML フォーマットを含めることができます。ユーザに表示されるこのページには、ユーザの確認操作用の「**承諾する**」と「**キャンセル**」があります。

5 「**適用**」を選択します。

トピック:

- サンプル テンプレート (147 ページ)
- プレビュー メッセージ (147 ページ)

サンプル テンプレート

「**サンプル テンプレート**」を選択すると、既定の AUP テンプレートの内容が表示されます。この内容は自由に変更することができます。

```
<font face=arial size=3>
<center><b><i>SonicWall へようこそ</center></b></i>
<font size=2>

<table width="100%" border="1">
<tr><td>
<font size=2>
<br><br><br>
<center>ここに規約を記述します。
<br><br><br>
</td></tr>
</table>
```

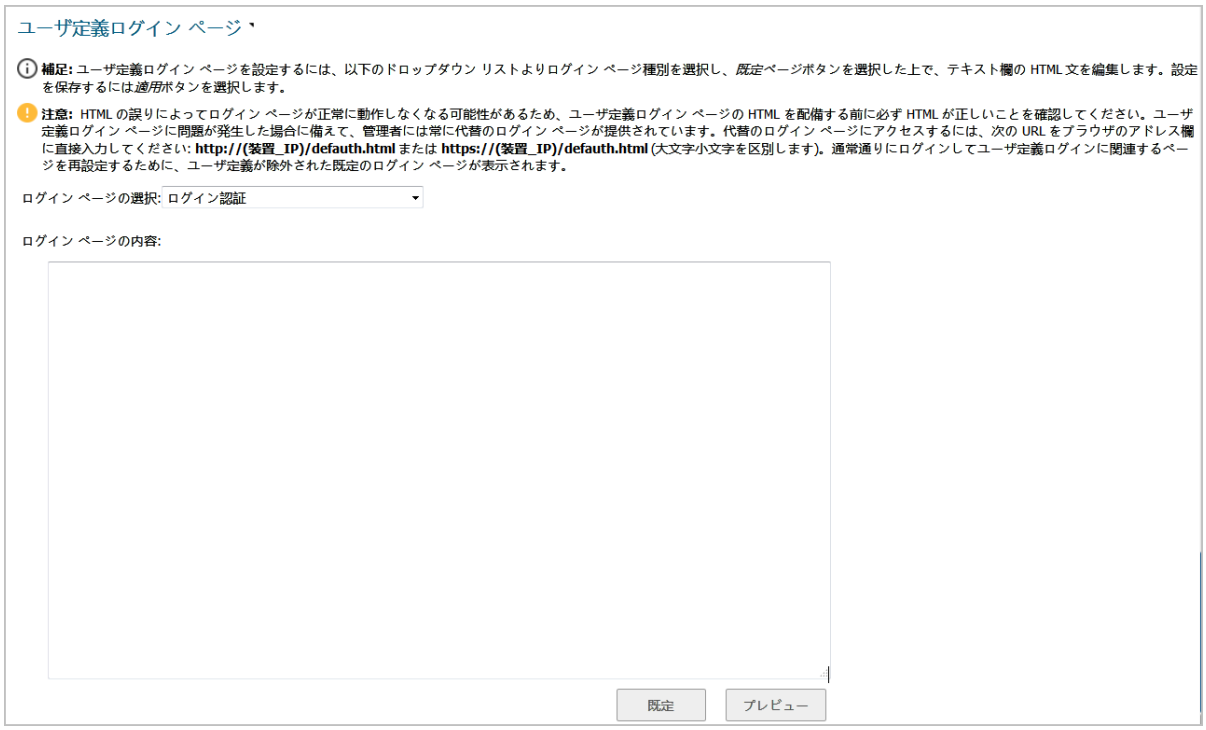
これらの規約を承諾して続行するには「承諾する」を選択してください。

そうでない場合は「キャンセル」を選択してください。

プレビュー メッセージ

「**プレビュー**」を選択すると、作成した AUP メッセージがどのようにユーザに表示されるかを確認できます。

ユーザ定義ログイン ページ



SonicOS では、ユーザに表示されるログイン認証ページのテキストをユーザ定義する機能を提供します。ログイン関連のページは、独自の表現を用いて翻訳できます。その変更を適用すると、再起動しなくても結果が反映されます。

SonicOS 管理インターフェース全体はさまざまな言語で利用可能ですが、ユーザ インターフェース全体の言語を特定の地域の言語に変更したくない場合があります。

しかし、セキュリティ装置でユーザの認証を要求してから他のネットワークへのアクセスを許可する場合や、外部アクセス サービス (VPN、SSL VPN など) を有効にする場合については、通常、それらのログイン関連ページを一般的なユーザから見てより使いやすくなるようにローカライズしてください。

「**ユーザ定義ログインページ**」には次の機能があります。

- 既定では元のログインのスタイルを維持する
- ログイン関連ページをカスタマイズする
- 既定のログイン関連ページをテンプレートして使用する
- カスタマイズしたページをシステム プリファレンスに保存する
- 変更内容をプリファレンスに保存する前に確認する
- カスタマイズしたログイン関連ページを一般的なユーザに提示する

以下のログイン関連ページをユーザ定義できます。

- 管理の先制
- ログイン認証
- ログアウト
- ログイン数超過
- ログイン拒否

- ログイン ロックアウト
- ログイン状況
- ゲスト ログイン状況
- ポリシー アクセス遮断
- ポリシー アクセス ダウン
- ポリシー アクセス利用不可
- ポリシー ログイン リダイレクト
- ポリシー シングル サイン オン監視失敗
- ユーザ パスワード更新
- ユーザ ログイン メッセージ

これらのページのいずれかをカスタマイズするには、以下の手順を実行します。

1 「**管理 | システム セットアップ > ユーザ > 設定**」に移動します。

2 「**カスタマイズ**」を選択します。

3 「**ログイン ページのユーザ定義**」セクションまでスクロールします。

4 カスタマイズするページを「**ログイン ページの選択**」から選択します。

5 「**既定**」を選択して既定のページ内容をロードします。

6 ページ内容を編集します。

メモ：テンプレート ページにある `var strXXX =` という行は、ユーザ定義の JavaScript 文字列です。これらは好きな語句に変更できます。変更する場合は、JavaScript の構文に従ってください。HTML セクションの語句も編集できます。

7 「**プレビュー**」を選択して、カスタマイズ後のページがどのように見えるかを確認します。メッセージが表示されます。

8 「**OK**」を選択します。ユーザ定義したページが表示されます。

9 ウィンドウを閉じます。

10 変更を加えます。

11 ページの編集が完了したら、「**適用**」を選択します。

注意：ユーザ定義ログイン ページを配備する前にそのページの HTML をよく確認してください。HTML エラーがあると、ログイン ページが正しく機能しなくなる場合があります。ユーザ定義ログイン ページに問題が発生した場合に備えて、管理者は常に代替ログイン ページを使用できます。代替ログイン ページにアクセスするには、*https://(device_ip)/defauth.html* という URL をブラウザのアドレス行に直接手動で入力します (大文字と小文字は区別されます)。これによって、ユーザ定義の加えられていない既定のログイン ページが表示されるので、ここから通常どおりにログインし、ユーザ定義のログイン関連ページをリセットできます。

ヒント：表示するページを既定のページに戻すには、「**ログイン ページの内容**」フィールドを空白のまま変更を適用します。

アカウント

SonicOS は、RADIUS アカウントと TACACS+ アカウントの両方をサポートしています。RADIUS サーバと TACACS+ サーバの両方が設定されている場合、ユーザのアカウント メッセージは両方のサーバに送信されます。

トピック:

- TACACS+ アカウントの設定 (151 ページ)

TACACS+ アカウントの設定

SonicOS 6.5 は TACACS+ アカウントの Start、Watchdog、および Stop メッセージをサポートしますが、TACACS+ アカウント プロキシはサポートしません。つまり、SonicOS はアカウント要求をアカウント サーバに転送しません。

TACACS+ アカウントを設定するには:

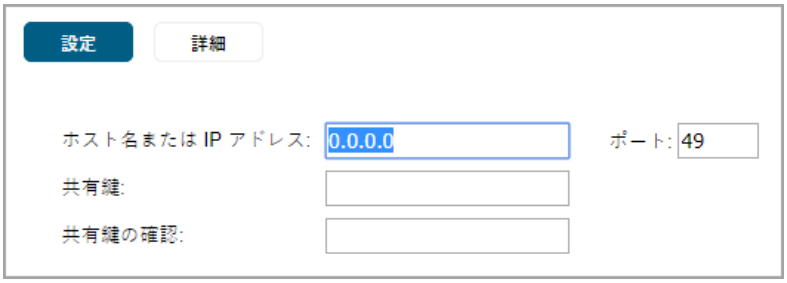
1 「**管理 | システム セットアップ > ユーザ > 設定**」に移動します。

2 「**アカウント**」をクリックします。

3 「**TACACS+ アカウント**」を選択します。「**TACACS+ アカウント サーバ設定**」ダイアログが表示されます。

4 TACACS+ サーバを追加するには、「**TACACS+ サーバ**」を選択します。

5 「**追加**」を選択します。「**TACACS+ アカウント サーバの追加**」ダイアログが表示されます。



6 「**ホスト名または IP アドレス**」フィールドに TACACS+ サーバのホスト名または IP アドレスを入力します。

7 「**ポート**」 フィールドに、サーバのポート番号を入力します。既定値は **49** です。

8 「**共有鍵**」フィールドと「**共有鍵の確認**」フィールドに、共有鍵を入力します。

9 「**詳細**」を選択します。

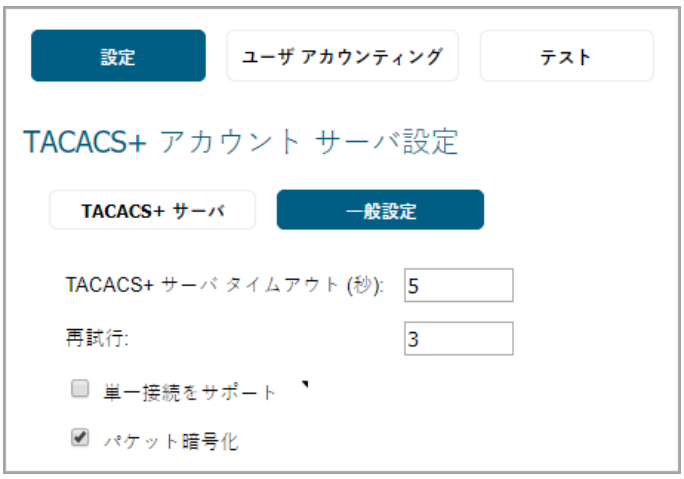
10 「**ユーザ名の形式**」から、ユーザ名の形式を選択します。

- **簡易名**
- **名前@ドメイン** (既定)
- **ドメイン\名前**

- **名前.ドメイン**

11 「**保存**」を選択します。

12 「**設定**」を選択します。



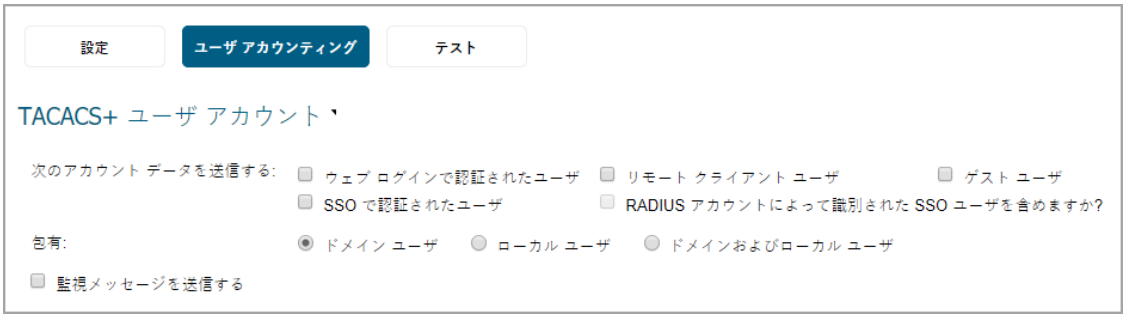
13 サーバ タイムアウトを「**TACACS+ サーバ タイムアウト (秒)**」フィールドに入力します。既定値は **5** 秒です。

14 「**再試行**」フィールドに再試行の最大数を入力します。既定値は **3** です。

15 単一接続をサポートするには、「**単一接続をサポート**」を選択します。このオプションは、既定では選択されていません。

16 暗号化パケットを許可するには、「**パケット暗号化**」を選択します。このオプションは、既定では選択されています。

17 「**ユーザ アカウンティング**」を選択します。



18 「**次のアカウント データを送信する:**」から、1 つまたは複数の種類のユーザを選択します。「**RADIUS アカウントによって識別された SSO ユーザを含める**」は、既定では選択できません。これを選択できるようにするには、まず「**SSO で認証されたユーザ**」フィールドを選択します。

19 「**包有**」からドメイン ユーザまたはローカル ユーザ、あるいはその両方を追跡するかどうかを選択します。**ドメイン ユーザ**が既定で選択されています。

20 監視メッセージを受信するには、「**監視メッセージを送信する**」を選択します。このオプションは、既定では選択されていません。このオプションを選択すると、「**毎:.... 分**」オプションが表示されます。**監視メッセージ**を受信する頻度を指定します。

21 「**テスト**」を選択します。

22 「**テストするサーバを選択**」から、TACACS+ サーバの IP アドレスを選択します。

23 「**テスト**」から、テストの種類を選択します。既定では「**接続性**」が選択されます。

24 「**テスト**」を選択します。テストの結果は「**返されたユーザ属性**」に表示されます。

25 「**適用**」を選択します。

26 サーバごとに上記の手順を繰り返します。

27 「**OK**」を選択します。

RADIUS 認証の設定

メモ：SonicPoint または SonicWave に対する RADIUS の設定については、『*SonicOS 6.5 接続*』を参照してください。

SonicOS での RADIUS 認証の概要は、「RADIUS を使った認証 (93 ページ)」を参照してください。「**管理 | システム セットアップ > ユーザ > 設定**」ページの「**ログインの認証方法**」ドロップダウン メニューから「**RADIUS**」または「**RADIUS + ローカル ユーザ**」を選択すると、「**RADIUS の設定**」が選択可能な状態になります。

トピック:

- RADIUS 設定の構成 (155 ページ)
- 「RADIUS ユーザ」ページ (158 ページ)

- ユーザ グループに LDAP を使用する RADIUS (159 ページ)
- RADIUS クライアントのテスト (160 ページ)

RADIUS 設定の構成

RADIUS の設定を行うには、次の手順に従います。

1 「**管理 | システム セットアップ | ユーザ > 設定**」に移動します。

2 「**認証**」を選択します。

3 「**RADIUS の設定**」を選択します。「**RADIUS サーバ設定**」ダイアログが表示されます。

4 「**設定 > RADIUS サーバ 設定**」で、「**追加**」を選択します。「**サーバの追加**」ダイアログが表示されます。

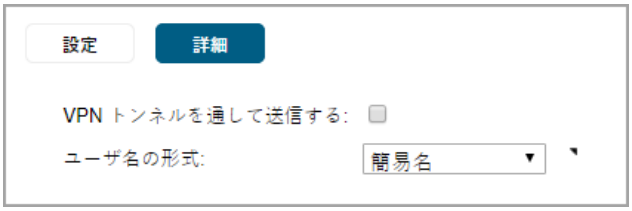
5 パーティション処理が有効になっている場合、「**パーティションの選択**」ポップアップが「**サーバの追加**」ダイアログに表示されます。パーティションを選択し、「**OK**」を選択します。

6 「**設定**」で、「**ホスト名または IP アドレス**」フィールドに IP アドレスまたはホスト名を入力します。既定値は `0.0.0.0` です。

7 「**ポート**」フィールドに、SonicOS との通信に使用する RADIUS サーバのポートを入力します。既定値は **1812** です。

8 「**共有鍵**」および「**共有鍵の確認**」フィールドに、RADIUS サーバの管理者パスワードまたは共有鍵を入力します。**事前共有鍵**は大文字と小文字が区別され、1 ～ 31 文字の範囲の英数字です。

9 「**詳細**」を選択します。



10 必要に応じて、「**VPN トンネルを通して送信する**」を選選択します。このオプションは、既定では選択されていません。

11 「**ユーザ名の形式**」で、ユーザ名の形式を選択します。

- **簡易名** (既定)
- **名前@ドメイン**
- **ドメイン\名前**
- **名前.ドメイン**

RADIUS サーバで送信するユーザ名にドメイン コンポーネントを含める必要がある場合は、ここでその形式を選択します。

メモ：サーバがドメイン コンポーネントのない単純名とドメインを含む修飾名のどちらも受け入れる場合、サーバに送信される名前にドメインを強制的に含めることが特に必要でない限り、ここで選択する内容は既定の単純名のままでかまいません。

メモ：Windows ドメインにおいて、ここで設定するのとは異なる修飾されたユーザ名の形式でもユーザがログインできるようにする (例えば、`name@domain` が選択されたら `domain\name` を含むファイアウォールへのログインを許可する、または *その逆*) 場合は、ドメイン名マッピングの検索のために LDAP を有効にする必要があります。そうしないと、ユーザは、RADIUS サーバで受け入れられる正しい形式の名前を入力しなければなりません。

12 「**保存**」を選択します。

13 「**OK**」を選択します。「**RADIUS アカウント サーバ**」テーブルにサーバが追加されます。

14 「**一般設定**」を選択します。

15 「**RADIUS サーバ タイムアウト (秒)**」フィールドにタイムアウト値を入力します。許容範囲は 1～60 秒で、既定値は **5** です。

16 SonicOS が RADIUS サーバに接続を試行する回数を「**再試行**」フィールドに入力します。RADIUS サーバが指定された試行回数内に応答しない場合、接続が破棄されます。このフィールドで指定できる値は 0 ～ 10 で、RADIUS サーバの既定の試行回数は **3** 回です。

17 RADIUS サーバの状況を定期的に確認するには、「**休止中の RADIUS サーバを定期的に確認する**」を選択します。このオプションは、既定では選択されています。

プライマリ RADIUS サーバが要求への応答に失敗すると、その状況はダウンに変更されます (「**RADIUS の設定**」ダイアログの「**RADIUS サーバ**」テーブルで赤色が表示され、その後の認証要求はプライマリが復旧するまでセカンダリ サーバに送信されます)。この設定をオンにすると、サーバがダウンしている間、ダミーの認証要求が定期的に送信されてチェックされます。サーバが要求に応答すると、その状況は稼働中に戻ります。お使いの RADIUS サーバでは、たまに生じる認証要求の失敗がユーザ名 `status check`でログに記録されることがあります。

このオプションを無効にしても、通常はユーザ認証に悪影響を及ぼすことはありません。ただし、プライマリ サーバが一時的にダウンしたときに無効にした場合、ファイアウォールはそれがいつ稼働状態になったかわからないので、引き続きサーバがダウンしているものと見なし、セカンダリ サーバに認証要求を送信します。この状態は、セカンダリが要求への応答に失敗するか、プライマリの状況が手動でチェックされるまで続きます。これは、「**RADIUS の設定**」ダイアログの「**テスト**」で RADIUS テストを実行することによりチェックできます。

メモ：プライマリ サーバがダウンしているときにセカンダリ サーバがダウンすると、ファイアウォールはプライマリ サーバへの要求の送信に戻るため、ファイアウォールはこの設定に関係なくプライマリ サーバが応答するかどうかを検出します。

18 必要に応じて、MS-CHAPv2 RADIUS 認証を強制するために「**MSCHAPv2 を強制する**」を選択します。このオプションは、既定では選択されていません。

19 「**適用**」を選択します。

20 「**OK**」を選択します。

21 RADIUS ユーザを設定するには、「「RADIUS ユーザ」ページ (158 ページ)」に進みます。

「RADIUS ユーザ」ページ

「**RADIUS の設定**」ダイアログの「**RADIUS ユーザ**」ページでは、RADIUS 認証と組み合わせて使用するローカルまたは LDAP 情報の種類を指定できます。RADIUS ユーザの既定のユーザ グループを定義することもできます。

RADIUS ユーザの設定を行うには、次の手順に従います。

1 「**RADIUS ユーザ**」を選択します。

2 SonicOS データベースに登録されているユーザだけが RADIUS で認証されるようにするには、「**ローカルに登録されたユーザのみ許可する**」を選択します。

3 「**RADIUS ユーザに対する グループ メンバーシップの検索方式**」のオプションを以下から選択します。

> **メモ：「ベンダー固有の属性を RADIUS サーバで使用する」または「Filter-Id 属性を RADIUS サーバで使用する」**オプションを選択した場合は、RADIUS サーバを適切に設定して、ユーザの認証時にこれらの属性が SonicWall 装置に返されるようにしなければなりません。RADIUS サーバは、選択された属性の 0 個以上のインスタンスを返します。各インスタンスにより、ユーザの所属するユーザ グループの名前が与えられます。
>
> ベンダー固有の属性設定の詳細については、テクニカル ノートの『*SonicOS Enhanced: ユーザ レベル認証*』と SonicOS Enhanced RADIUS 辞書ファイル `SonicWall.dct` を参照してください。どちらも https://www.sonicwall.com/ja-jp/support から入手できます。

- **ベンダー固有の属性を RADIUS サーバで使用する** - RADIUS サーバから設定済みのベンダー固有の属性を適用する場合に選択します。この属性には、ユーザが所属するユーザ グループが指定されている必要があります。推奨されるベンダー固有の RADIUS 属性は

SonicWall-User-Group です。一部のユーザ グループでは SonicWall-User-Privilege も使用できますが、主として後方互換性のためにサポートされているものであり、「**RAIDUS ユーザのユーザ グループ メンバーシップを設定するためのメカニズム**」による管理は及びません。つまり、「**ベンダー固有の属性を RADIUS サーバで使用する**」以外を選択してもまだ有効になります。

- **Filter-Id 属性を RADIUS サーバで使用する** - RADIUS サーバから設定済みの Filter-ID 属性を適用する場合に選択します。この属性には、ユーザが所属するユーザ グループが指定されている必要があります。
- **ユーザ グループ情報の検索に LDAP を使用する** (既定値) - LDAP サーバからユーザ グループを取得する場合に選択します。まだ LDAP を設定していない場合、または、変更を加える必要がある場合は、「**設定**」を選択すると、LDAP の設定を行うことができます。LDAP の設定については、「LDAP を使用するための SonicWall の設定 (162 ページ)」を参照してください。
- **ローカル設定のみ** - ユーザ グループ情報を RADIUS からも LDAP からも取得しない場合に選択します。
- **重複した RADIUS ユーザ名によるメンバーシップ設定可能です** - RADIUS ユーザ グループを簡単に管理できるようにします。セキュリティ装置上に同じ名前のユーザをローカルに作成し、そのグループ メンバーシップを管理すると、その内容が RADIUS データベース内のメンバーシップの設定に自動的に反映されます。

4 既に SonicOS 上でユーザ グループを設定している場合は、「**すべての RADIUS ユーザが初期状態で所属するグループ**」ドロップダウン メニューからグループを選択します。新規のユーザ グループを作成するには、「RADIUS ユーザ用の新しいユーザ グループの作成 (159 ページ)」を参照してください。

5 次のどちらかを選択します。

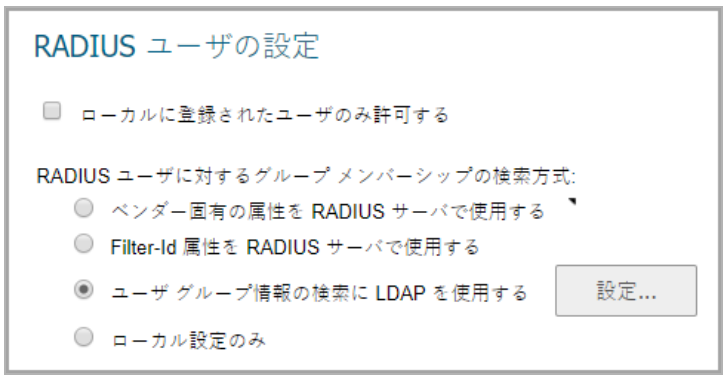
- 「**OK**」- RADIUS サーバの設定が完了した場合
- 「**適用**」- RADIUS ユーザの設定や設定内容のテストを引き続き行う場合

RADIUS ユーザ用の新しいユーザ グループの作成

新規のグループを作成するには、「**RADIUS ユーザ設定**」ダイアログの「**すべての RADIUS ユーザが初期状態で所属するグループ**」ドロップダウン メニューから「**ユーザ グループの作成...**」を選択します。「**グループの追加**」ダイアログが表示されます。新規のユーザ グループを作成する手順については、「ローカル グループの作成または編集 (251 ページ)」を参照してください。

ユーザ グループに LDAP を使用する RADIUS

RADIUS をユーザ認証に使用している場合、RAIDUS ユーザのユーザ グループ メンバーシップを設定するためのメカニズムとして LDAP を選択できるようにするオプションが、「**RADIUS の設定**」ダイアログの「**RADIUS ユーザ**」ページにあります。



「**ユーザ グループ情報の検索に LDAP を使用する**」が選択されている場合、RADIUS を介してユーザ認証が行われた後、ユーザ グループ メンバーシップ情報が、LDAP を介して LDAP/AD サーバ上のディレクトリ内で参照されます。

メモ：このメカニズムを**選択しない**で、ワンタイム パスワードを有効化すると、RADIUS ユーザは SSL VPN を通してログインを試行するとき、ワンタイム パスワードの失敗メッセージを受け取ります。

「**設定**」を選択すると、「**LDAP 設定**」ダイアログが表示されます。LDAP 設定の方法については、「統合に向けての LDAP サーバの準備 (97 ページ)」を参照してください。

メモ：この場合、LDAP はユーザ パスワードを扱わず、ディレクトリから読み込まれる情報も通常は制限されるので、TLS を使用しない操作を選択することもできます。TLS が利用できない場合 (証明書サービスがアクティブ ディレクトリにインストールされていない場合など) は警告を無視してください。その際、SonicOS は平文テキストを使用して LDAP サーバにログインするので、セキュリティが侵されないような措置が必要です。例えば、SonicOS でのみ利用するディレクトリを読み取り専用でアクセスするユーザ アカウントを作成します。この場合は管理者アカウントを使用しないでください。

RADIUS クライアントのテスト

「**RADIUS の設定**」ダイアログでは、有効なユーザ名とパスワードを入力し、「テスト」でいずれかの認証方式を選択することによって、RADIUS クライアントのユーザ名やパスワードなどの設定を**テスト**できます。テストを実行すると、それまでに行ったすべての変更が適用されます。

RADIUS の設定をテストするには、次の手順に従います。

1 「**テスト**」を選択します。

2 「**ユーザ名**」フィールドに、有効な RADIUS ログイン名を入力します。

3 「**パスワード**」フィールドにパスワードを入力します。

4 「**テスト**」で、次のいずれかを選択します。

- **接続性**: これを選択して、RADIUS 接続をテストします。
- **パスワード認証**: 認証にパスワードを使用する場合に選択します。
- **CHAP**: チャレンジ ハンドシェーク認証プロトコルを使用する場合に選択します。CHAP では、初回検証後、3 ウェイ ハンドシェークを使ってクライアントの ID が定期的に検証されます。
- **MSCHAP**: Microsoft の実装による CHAP を使用する場合に選択します。MSCHAP は、Windows Vista より前のすべてのバージョンの Windows に対応しています。
- **MSCHAPv2**: Microsoft による実装の CHAP バージョン 2 を使用する場合に選択します。MSCHAPv2 は、Windows 2000 以降のバージョンの Windows に対応しています。

5 「**テスト**」を選択します。検証に成功した場合は、「**状況**」メッセージが「**成功**」に変わります。検証に失敗した場合は、「**状況**」メッセージが「**失敗**」に変わります。

6 RADIUS の設定を完了するには、「**OK**」を選択します。

SonicOS が設定されると、RADIUS 認証を必要とする VPN Security Association から、着信VPN クライアントがユーザ名とパスワードをダイアログに入力するよう求められます。

LDAP を使用するための SonicWall の設定

トピック:

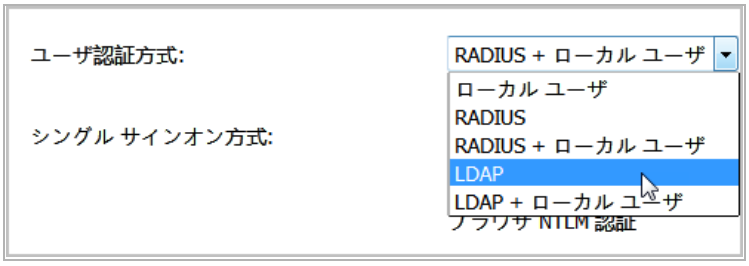
- LDAP 統合の管理 (162 ページ)
- 複数 LDAP サーバの拡張サポートについて (174 ページ)
- LDAP からのインポートとミラーリングについて (176 ページ)

LDAP 統合の管理

LDAP 統合を管理するには、次の手順に従います。

1 「**管理 | システム セットアップ > ユーザ > 設定**」に移動します。

2 「**ユーザ認証方式**」で、「**LDAP**」または「**LDAP + ローカル ユーザ**」のどちらかを選択します。



3 「**LDAP の設定**」を選択します。

4 現在 HTTPS ではなく HTTP でセキュリティ装置に接続している場合は、ディレクトリ サービスに格納された情報の機密性について警告し、接続を HTTPS に変更するように促すメッセージが表示されます。接続しているインターフェースで HTTPS 管理を有効にしている場合 (推奨) は、「**はい**」を選択します。「**LDAP 設定**」ダイアログが表示されます。

メモ：動的に学習されたセカンダリ サーバは、設定されているサーバと区別しやすいように青色で表示されます。

トピック:

- 設定 (163 ページ)
- スキーマ ページ (165 ページ)
- 「ディレクトリ」ページ (167 ページ)
- 「紹介」ページ (169 ページ)

- 「ユーザとグループ」ページ (170 ページ)
- 「LDAP リレー」ページ (172 ページ)
- 「テスト」ページ (173 ページ)

設定

LDAP サーバの設定を行うには、次の手順に従います。

1 以下のフィールドを設定します。

- **名前または IP アドレス** - 認証に使用する LDAP サーバの FQDN または IP アドレスを入力します。名前を使用する場合は、DNS サーバで名前が解決できることを確認してください。また、「サーバからの有効な証明書を要求する」オプションとともに TLS を使用している場合、ここで指定した名前は、サーバ証明書の発行先の名前 (すなわち CN) と一致する必要があります。 一致しない場合、TLS 交換は失敗します。
- **ポート番号** - 既定の LDAP over TLS ポート番号は TCP 636 です。既定の LDAP (非暗号化) ポート番号は、TCP 389 です。LDAP サーバで個別のリッスン ポートを使用している場合は、ここでポート番号を指定します。
- **サーバ タイムアウト (秒)** - SonicOS が LDAP サーバからの応答を待つ秒数を入力します。この秒数が経過すると、タイム アウトが発生します。指定できる範囲は 1 ～ 99999 で、既定値は **10** 秒です。
- **総合操作のタイムアウト (分)** - 自動動作に費やす時間を分単位で指定します。複数の LDAP サーバを使用している場合は特に、ディレクトリの設定やユーザ グループのインポートなど、数分かかる動作もあります。
- 次のいずれかのラジオ ボタンを選択します。
  - **匿名ログイン** - LDAP サーバによっては、匿名でツリーにアクセスできます。利用するサーバでこの機能がサポートされている場合 (通常、アクティブ ディレクトリではサポートされない)、このオプションを選択することもできます。
  - **ログイン名/ツリー内位置を渡す** - LDAP サーバへのバインドに使う識別名 (dn) を以下の規則に従って「ログイン　ユーザ名」フィールドと「サーバにログインするためのユーザ　ツリー」フィールドから作成するには、このオプションを選択します。
    - 最初の名前構成要素は "cn=" で開始する
    - 「ツリー内位置」構成要素はすべて "ou=" を使用する ("cn="で始まる特定のアクティブ ディレクトリのビルトインとは別に)
    - ドメイン構成要素はすべて "dc="を使用する
    - 「サーバにログインするためのユーザ ツリー」フィールドが dn として指定されている場合は、バインド dn が上記の 1 番目の規則に従うなら 2 番目と 3 番目の規則に従わなくても、このオプションを選択できる
  - **識別名のバインドを渡す** - バインド dn が上記の 1 番目の項目に一致していない場合 (最初の名前構成要素が "cn=" で始まらない場合) は、このオプションを選択します。dn がわかっている場合は、常にこのオプションを選択することができます。バインド dn が上記の 1 番目の項目に一致しない場合は、バインド dn を明示的に指定する必要があります。

- **ログイン ユーザ名** - LDAP ディレクトリにログインする権限のあるユーザ名を指定します。ログイン名は、完全な 'dn' 表記で LDAP サーバに自動的に提示されます。これには LDAP の読み取り権限がある任意のアカウント (実質的にすべてのユーザ) を指定でき、管理者権限は必要ありません。

  メモ：これはユーザの名前であって、ログイン ID ではありません (例えば、jsmith ではなく、John Smith)。

- **ログイン パスワード** - 上記で指定したユーザ アカウントのパスワードを指定します。
- **プロトコル バージョン** - LDAP バージョン 3 か LDAP バージョン 2 を選択します。現在の LDAP のほとんど (アクティブ ディレクトリを含む) の実装では、LDAP バージョン 3 が採用されています。
- **TLS (SSL) を使用する** - LDAP サーバへのログインに Transport Layer Security (SSL) を使用します。ネットワーク上に送信されるユーザ名とパスワード情報を保護するために TLS を使用することを強くお勧めします。現在の LDAP のほとんど (アクティブ ディレクトリを含む) の実装では、TLS がサポートされています。この既定の設定を変更して選択を解除した場合は、警告が表示されます。この警告を承諾しないと先に進めません。
- **LDAP'Start TLS'要求を送信する** - 一部の LDAP サーバの実装では、ネイティブな LDAP over TLS を使用しないで、Start TLS 指示をサポートしています。これにより、LDAP サーバが、LDAP 接続を 1 つのポート (通常 389) でリッスンすること、および、クライアントによる指示で TLS へ切り替えることが可能になります。アクティブ ディレクトリではこのオプションはサポートされません。 このオプションは、LDAP サーバによって要求された場合にのみ選択すべきです。
- **サーバからの有効な証明書を要求する** - TLS 交換時に、サーバによって提示された証明書の名前が上記で指定した名前と一致するかどうかを確認します。この既定のオプションを非選択にした場合、警告が表示されますが、SonicOS と LDAP サーバ間の交換には引き続き TLS が使われます (発行の妥当性が確認されなくなるだけです)。
- **TLS に用いるローカル証明書** - オプション。LDAP サーバが接続のためにクライアント証明書を要求する場合にのみ使用されます。LDAP クライアントの識別を確実にするためにパスワードを返すLDAP サーバの実装では有用です (アクティブ ディレクトリではパスワードは返されません)。この設定はアクティブ ディレクトリでは必要ありません。

  ネットワークで参照機能を使用して複数の LDAP/AD サーバを利用している場合は、1 つのサーバ (通常、大量のユーザを保持しているサーバ) をプライマリ サーバとして選択し、そのサーバに上記の設定を行う必要があります。プライマリ サーバは、自分以外のドメインのユーザが他のサーバに向かうよう SonicOS に仕向けます。このような別のサーバに SonicOS がログインするためには、それぞれのサーバにおいて、プライマリ サーバへのログインと同じ資格情報 (ユーザ名、パスワード、ディレクトリ内の場所) を使用してユーザを設定する必要があります。そのために、SonicOS ログイン用に、ディレクトリ内に特別なユーザを作成することが必要になるかもしれません。ディレクトリへの読み取りアクセスのみが必要とされていることに注意してください。

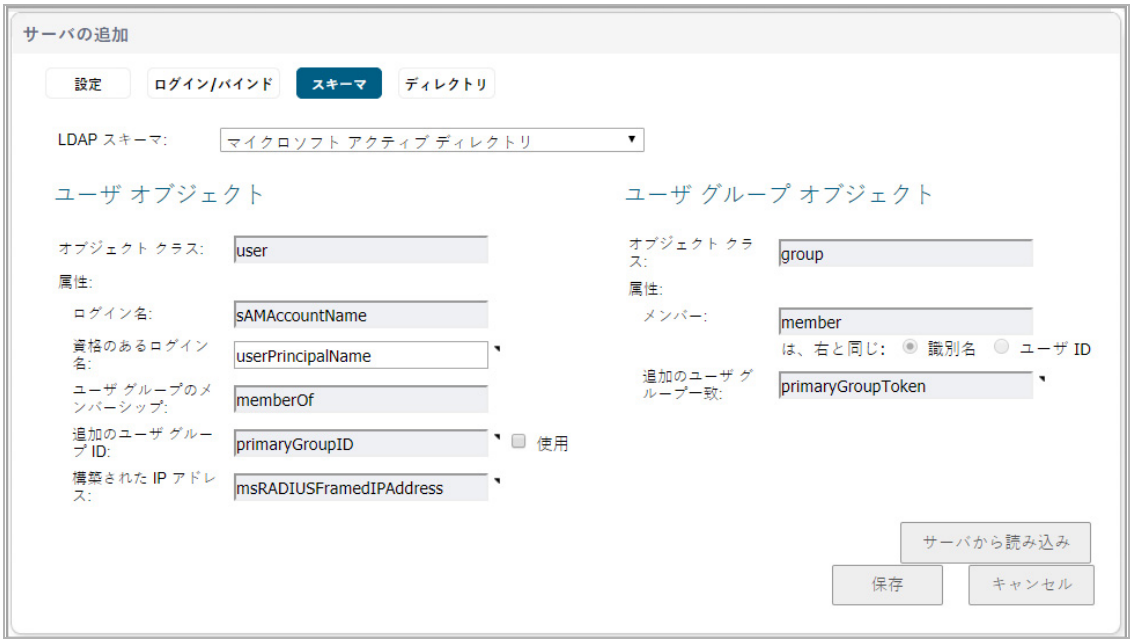
- **PAP を MSCHAPv2 に強制する** - 必要に応じて、MS-CHAPv2 LDAP 認証を強制するには、このオプションを選択します。RADIUS サーバも設定してあれば、LDAP 認証が失敗したとき、それで認証が行われます。このオプションは、既定では選択されていません。

2 「**適用**」を選択します。

スキーマ ページ

LDAP サーバのスキーマの設定を行うには、次の手順に従います。

1 「**スキーマ**」を選択します。



2 **LDAP スキーマ** - 「**LDAP スキーマ**」ドロップダウン メニューから次のいずれかを選択します。

> **メモ**：定義済みのいずれかのスキーマを選択した場合、そのスキーマによって使用されるフィールドに適切な値が自動的に入力されます。これらの値は変更できません。フィールドが淡色表示になっています。

- **マイクロソフトアクティブ ディレクトリ** (既定値)
- **RFC2798 InetOrgPerson**
- **RFC2307 ネットワーク インフォメーション サービス**
- **サンバ SMB**
- ***ノベル イーディレクトリ***
- **ユーザ定義** - 独自の値を指定できます。これを指定するのは、使用する LDAP スキーマ設定が決まっている場合やメーカー固有のスキーマ設定を使用する場合に限ってください。

3 **オブジェクト クラス** - 次の 2 つのフィールドが適用される個々のユーザ アカウントを表す属性を選択します。

4 **ログイン名** - 次のいずれかを選択して、ログイン認証に使用する属性を定義します。

- **sAMAccountName**: Microsoft アクティブ ディレクトリ用
- **inetOrgPerson**: RFC 2798 inetOrgPerson 用
- **posixAccount**: RFC2307 ネットワーク インフォメーション サービス用
- **sambaSAMAccount**: サンバ SMB 用
- **inetOrgPerson**: ノベル イーディレクトリ用

5 **資格のあるログイン名** - 必要に応じて、ユーザ オブジェクトから 1 つの属性を選択し、それで「名前@ドメイン」という形式の代替ログイン名を設定します。これは、特に、多数のドメインがあって単純なログイン名ではドメイン間で一意性を保てないような場合に必要となる可能性があります。

> **メモ：Microsoft アクティブ ディレクトリ**の場合は、通常、ここで「**userPrinicpalName**」を選択して「名前@ドメイン」形式のログイン名を使いますが、「**mail**」を選択すればメール アドレス別のログを有効にすることもできます。**RFC2798 inetOrgPerson** の場合は、「**mail**」を選択します。

6 **ユーザ グループ メンバーシップ** - ユーザ オブジェクトの所属先グループについての情報を表す属性を選択します。これに該当するのは、Microsoft アクティブ ディレクトリの **memberOf** 属性です。他の定義済みのスキーマでは、グループ メンバーシップ情報がユーザ オブジェクトではなくグループ オブジェクト内に格納されるので、このフィールドは使用されません。

7 **構築された IP アドレス** - ディレクトリ内でユーザに割り当てられた静的 IP アドレスを取得するための属性を選択します。現在は、L2TP を介して SonicOS の L2TP サーバと接続するユーザに対してのみ使用されます。将来的には、グローバル VPN クライアントでもサポートされる可能性があります。アクティブ ディレクトリでは、ユーザ プロパティの「ダイヤルイン」タブで静的 IP アドレスを設定します。

8 **ユーザ グループ オブジェクト** - このセクションは自動的に設定されます。ただし、「**LDAP スキーマ**」で「**ユーザ定義**」を選択した場合はその限りでありません。

- **オブジェクト クラス** - 属性のグループに関連付けられる名前を指定します。
- **メンバー** - メンバーに関連付けられる属性を指定します。
  - **識別名**または**ユーザ ID** のどちらかを選択します。
- **サーバから読み込み** - 選択すると、LDAP サーバからユーザ グループ オブジェクトの情報を読み込みます。

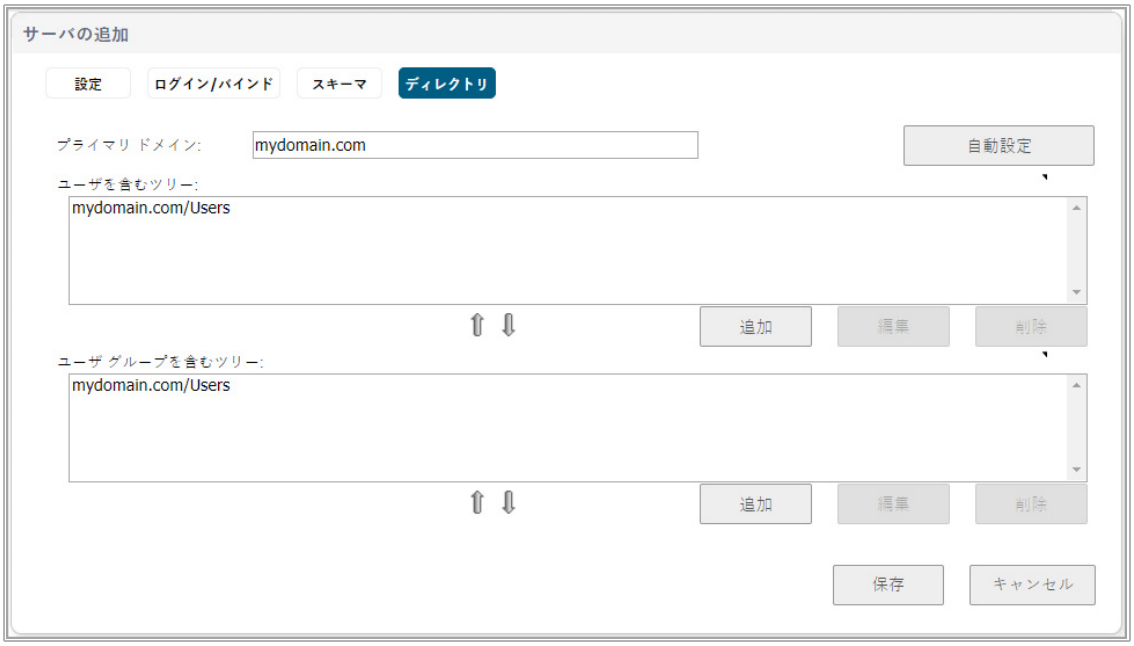
  > **メモ：**最初に「**ディレクトリ**」タブでプライマリ ドメインを入力する必要があります。

  - **スキーマ設定を自動的に更新**または**スキーマの詳細をエクスポート**のどちらかを選択します。

「ディレクトリ」ページ

LDAP サーバのディレクトリの設定を行うには、以下の手順に従います。

1 「**ディレクトリ**」ページで、以下のフィールドを設定します。



- **プライマリ ドメイン** - LDAP 実装により使用されているユーザ ドメイン。AD の場合は、これがアクティブ ディレクトリのドメイン名になります (例えば、*yourADdomain.com*)。オプションで、このフィールドを変更したときにページ内の残りのツリー情報を自動的に更新することもできます。既定では、ノベル イーディレクトリを除くすべてのスキーマで **mydomain.com** に設定されます (ノベル イーディレクトリの既定値は **o=mydomain**) です。
- **ユーザを含むツリー** - LDAP ディレクトリ内でユーザが一般に含まれるツリー。編集可能な 1 つの既定値が提供されます。 合計 64 個の DN 値を登録することができます。SonicOS は、これらすべてを使用して、一致するかリストの最後になるまで、ディレクトリを検索します。LDAP または AD ディレクトリ内に他のユーザ コンテナを作成している場合は、ここにユーザ コンテナを指定する必要があります。
- **ユーザ グループを含むツリー** - ユーザ グループ コンテナに関連し、DN 値の最大数が 32 であること以外は、「ユーザを含むツリー」と同じです。スキーマのユーザ オブジェクト内にユーザ グループ メンバーシップ属性がない場合にのみ適用できます。 AD では使用されません。
- 上記のすべてのツリーは、通常 URL 形式で指定しますが、識別名で指定することもできます (例えば、`myDom.com/Sales/Users` の代わりに `ou=Users,ou=Sales,dc=myDom,dc=com` という識別名を使ってもかまいません)。後者の形式は、DN がサンプルに示すような通常の書式ルールに従っていない場合に必要になります。アクティブ ディレクトリでは、ツリーの識別名に対応する URL が、ツリーの最上部にあるコンテナのプロパティの「オブジェクト」タブに表示されます。

  メモ：AD の一部のビルトイン コンテナは通常の書式ルールに従っていません (例えば、最上位のユーザ コンテナの DN では `cn=Users,dc=…` というように、`ou` ではなく `cn` が使われます)。しかし、SonicOS がこれを認識して適切に処理するので、より簡単な URL 形式で入力できます。

順序は重要ではありませんが、検索が特定の順序で行われることから、最も効率的な検索を行うためには頻繁に使用されるツリーを各リストの先頭に配置します。複数の LDAP サーバにわたった参照をする場合は、プライマリ サーバのツリーを最初に配置し、残りのツリーはサーバを参照する順に並べるようにすると、ツリーを最適に並べ替えることができます。

メモ：AD を使用しているとき、「**サーバにログインするためのユーザ ツリー**」フィールドで指定したディレクトリ内で特定のユーザの場所を調べるには、サーバのコントロール パネルの「Active Directory ユーザとコンピュータ」アプレットからディレクトリを手動で検索するか、ドメイン内の任意の PC から Windows NT/2000/XP リソース キットに含まれる queryad.vbs のようなディレクトリ検索ユーティリティを実行します。

- **自動設定** - ディレクトリをスキャンしてユーザ オブジェクトが含まれるすべてのツリーを検出することにより、「**ユーザを含むツリー**」フィールドと「**ユーザ グループを含むツリー**」フィールドを自動的に設定します。自動設定を使用するには、最初に「**サーバにログインするためのユーザ ツリー**」フィールドに値を入力し (匿名ログインが設定されていない場合)、「**自動設定**」を選択して、「**ユーザ/グループ ツリー自動設定**」ダイアログを表示します。

a) 「**検索するドメイン**」フィールドに目的のドメインを入力します。

b) 次のいずれかを選択します。

- **現在のツリーに追加する** - 新たに検出されたツリーを現在の設定に追加します。このオプションは既定の設定です。
- **現在のツリーを置き換える** - 現在設定されているすべてのツリーを削除してから新規に作り直します。

c) 「**ここでセカンダリ LDAP サーバとして構成されている他のサーバへの参照の取得時**」で、次のいずれかを選択します。

- **そのサーバで見つかったツリーをそのサーバ自体の設定に追加する** - この選択は、サーバで見つかった新しく配置されたツリーを独自の構成に追加します。このオプションは既定の設定です。
- **そのサーバで見つかったツリーを無視する** - この選択は、指定されたサーバ上のツリーを無視します。

2 「**OK**」を選択します。

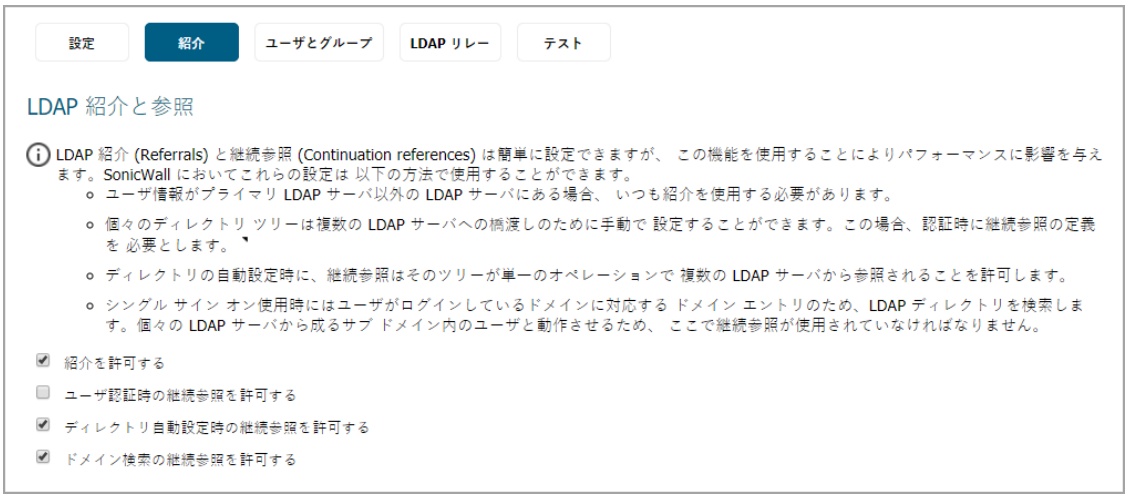
自動設定プロセスでは、ユーザ ログインに不要なツリーも検出される可能性があります。これらのエントリは手動で削除できます。

参照機能を使用して複数の LDAP/AD サーバを利用している場合は、「**検索するドメイン**」の値を適切な情報で置き換え、「**現在のツリーに追加する**」オプションを選択して、それぞれのサーバに対してこの処理を繰り返します。

「紹介」ページ

LDAP サーバの紹介の設定を行うには、次の手順に従います。

1 「**紹介**」を選択します。



2 以下のフィールドを設定します。

- **紹介を許可する** - 設定されたプライマリ LDAP サーバ以外の LDAP サーバ上にユーザ情報がある場合は常にこのオプションを選択します。このオプションは、既定では選択されています。
- **ユーザ認証時の継続参照を許可する** - 個々のディレクトリ ツリーを複数の LDAP サーバにわたって手動で設定した場合は常にこのオプションを選択します。このオプションは、既定では選択されていません。
- **ディレクトリ自動設定時の継続参照を許可する** - 1 回の動作で複数の LDAP サーバからツリーを読み出せるようにするにはこのオプションを選択します。このオプションは、既定では選択されています。
- **ドメイン検索の継続参照を許可する** - 別個の LDAP サーバを持つ複数サブドメイン内のユーザに対してシングル サインオンを使用する場合はこのオプションを選択します。このオプションは、既定では選択されています。

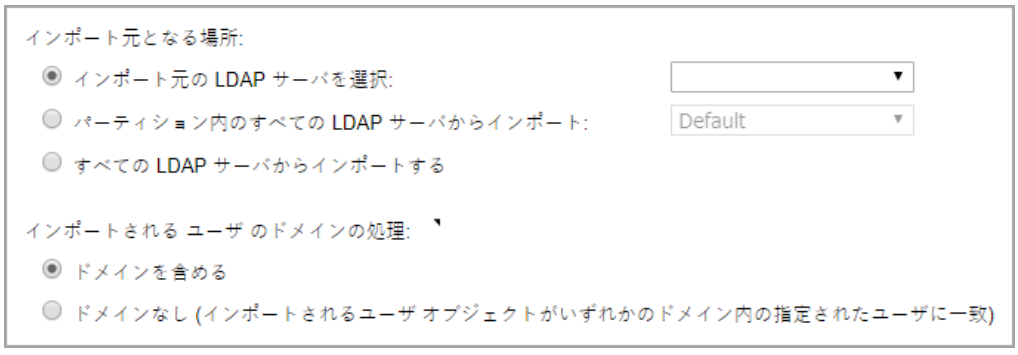
「ユーザとグループ」ページ

LDAP のユーザとグループの設定を行うには、次の手順に従います。

1 「**ユーザとグループ**」を選択します。

2 以下のフィールドを設定します。

- **ローカルに登録されたユーザのみ許可する** - LDAP ユーザが SonicOS ローカル ユーザ データベースにも登録されている場合にのみ、そのユーザのログインを許可するようにします。
- **既定の LDAP ユーザ グループ** - LDAP サーバ上で設定されたグループ メンバーシップに加えて、LDAP ユーザが所属する SonicOS の既定のグループ。
- **ユーザのインポート** - このボタンを選択すると、LDAP サーバからユーザ名を取得して、SonicOS のローカル ユーザを設定できます。「**ユーザのインポート** 」を選択すると、「**サーバの選択 - ユーザ**」ダイアログが表示されます。



a) どのサーバからユーザをインポートするかを選択します。

- 「**インポート元の LDAP サーバを選択**」から LDAP サーバを選択します。
- 「**パーティション内のすべての LDAP サーバからインポート**」から、サーバが含まれているパーティションを選択します。

- すべてのLDAPサーバからユーザをインポートするには、「**すべてのLDAPサーバからインポートする**」を選択します。

b) インポートされたユーザ オブジェクトにドメインを含めるかどうかを選択します。

- **ドメインを含める**
- **ドメインなし (インポートされるユーザ オブジェクトがいずれかのドメイン内の指定されたユーザに一致)**

ユーザをインポートするときにドメインを含めると、ユーザ名が同じでもドメインの異なるユーザを区別できます。特に多数のドメインがある場合は、ドメインを含めることをお勧めします。ドメインを含むインポートされたユーザ オブジェクトに対して行われるローカル ユーザ グループのメンバーシップやアカウントの有効期限などの設定は、指定されたユーザがそのドメインから認証されたときに初めて適用されます。

ドメインが含まれていない場合、インポートされた各ユーザ オブジェクトは任意のドメインの同じ名前を持つユーザと一致し、インポートされたユーザ オブジェクトに対して行われる設定は、ドメインに関係なく一致するすべてのユーザに適用されます。

c) 「**OK**」を選択します。

既存の LDAP/AD ユーザ グループと同じ名前のユーザが SonicOS にあれば、LDAP認証に成功したときに SonicWall のユーザ権限が与えられます。

- **ユーザ グループのインポート** - このボタンを選択すると、LDAP サーバからユーザ グループ名を取得することにより、SonicOS でユーザ グループを設定できます。「**ユーザ グループのインポート** 」を選択すると、「**サーバの選択 - ユーザ グループ**」ダイアログが表示されます。

a) ユーザのインポート方法を選択します。

- **LDAP ディレクトリからユーザ グループをインポートする**
- **LDAP位置(OU)別にメンバーシップを設定するためにグループを自動作成する**

既存の LDAP/AD ユーザ グループと同じ名前のユーザ グループが SonicOS にあれば、LDAP 認証に成功したときに SonicWall のグループ メンバーシップおよび権限が与えられます。

代わりに、SonicWall のビルトイン グループ (「ゲスト サービス」、「Content Filtering Bypass」、「制限付き管理者」など) と同じ名前で、LDAP/AD サーバ上にユーザ グループを手動で作成し、ディレクトリ内のこれらのグループにユーザを割り当てることもできます。この場合も、LDAP 認証が成功したときに SonicWall のグループ メンバーシップが与えられます。

b) どのサーバからユーザをインポートするかを選択します。

- 「**インポート元の LDAP サーバを選択**」から LDAP サーバを選択します。
- 「**パーティション内のすべての LDAP サーバからインポート**」から、サーバが含まれているパーティションを選択します。
- すべての LDAP サーバからユーザをインポートするには、「**すべての LDAP サーバからインポートする**」を選択します。

c) インポートされたユーザ オブジェクトにドメインを含めるかどうかを選択します。

- **ドメインを含める**
- **ドメインなし (インポートされるユーザ オブジェクトがいずれかのドメイン内の指定されたユーザに一致)**

アクティブ ディレクトリの場合、セキュリティ装置は、独自仕様である戻り値 "memberOf" ユーザ属性を利用することにより、より効率的にグループ メンバーシップを取得できます。

「LDAP リレー」ページ

LDAP サーバのリレーの設定を行うには、次の手順に従います。

1 「**LDAP リレー**」を選択します。

RADIUS からLDAP へのリレー機能は、LDAP/AD サーバおよびセントラル SonicWall を備えたセントラル サイトと、LDAP をサポートしていないローエンド セキュリティ装置を経由して接続されたリモート サテライト サイトが存在するトポロジで使用するために設計されました。この場合、セントラル SonicWall は、リモート SonicWall 用の RADIUS サーバとして動作し、RADIUS と LDAP の間のゲートウェイとして、リモート サイトからの認証要求を LDAPサーバへ転送します。

2 以下のフィールドを設定します。

- **RADIUS から LDAP へのリレーを有効にする** - この機能を有効にします。このオプションは、既定では選択されていません。
- **以下の RADIUS クライアントからの接続を許可する** - 適切なチェックボックスを選択します。着信 RADIUS 要求を許可するためのポリシー ルールが追加されます。既定では、「**WAN ゾーン**」と「**VPN ゾーン**」が選択されています。
- **RADIUS 共有鍵** - すべてのリモート SonicWall に共通の事前共有鍵です。
- **レガシー VPN ユーザに対するユーザ グループ** - 従来の 'VPN へのアクセスを許可する' 権限に対応するユーザ グループを定義します。このユーザ グループに所属するユーザが認証された場合、リモートの SonicWall に通知が送られ、そのユーザに適切な権限が与えられます。
- **レガシー VPN クライアント ユーザに対するユーザ グループ** - 従来の 'XAUTH による VPN クライアントからのアクセスを許可する' 権限に対応するユーザ グループを定義します。このユーザ グループに所属するユーザが認証された場合、リモートの SonicWall に通知が送られ、そのユーザに適切な権限が与えられます。
- **レガシー L2TP ユーザに対するユーザ グループ** - 従来の 'L2TP による VPN クライアントからのアクセスを許可する' 権限に対応するユーザ グループを定義します。このユーザ グループに所属するユーザが認証された場合、リモートの SonicWall に通知が送られ、そのユーザに適切な権限が与えられます。
- **インターネット アクセスのあるレガシー ユーザに対するユーザ グループ** - 従来の 'インターネット アクセスを許可する (アクセス制限時)' 権限に対応するユーザ グループを定義します。このユーザ グループに所属するユーザが認証された場合、リモートの SonicWall に通知が送られ、そのユーザに適切な権限が与えられます。

メモ：「フィルタのバイパス」と「制限された管理機能へのアクセスを許可する」権限は、「Content Filtering Bypass」と「制限付き管理者」のユーザ グループのメンバーシップに基づいて返されます。 これらを設定することはできません。

「テスト」ページ

重要：LDAP 設定をテストすると、それまでに行ったすべての変更が適用されます。

LDAP サーバのテストの設定を行うには、次の手順に従います。

1 「**テスト**」を選択して、構成された LDAP 設定をテストします。

「**LDAP 設定のテスト**」ページでは、指定したユーザとパスワード資格情報を使用して認証を試みることにより、設定された LDAP 設定をテストすることができます。ユーザに対して LDAP/AD サーバ上で設定されたユーザ グループ メンバーシップや構築された IP アドレスが表示されます。

複数 LDAP サーバの拡張サポートについて

複数のプライマリ LDAP サーバを設定できます (各認証パーティションに 1 つずつ)。また、それぞれに対する追加サーバのリストも設定できます。各プライマリ LDAP サーバは、現在の LDAP サーバと同様に設定します。追加サーバの場合、設定は最小限ですが (プライマリ サーバの共通設定を適用)、ログイン (バインド) 資格情報とそのサーバが制御するサブドメインを含めます。

メモ：アクティブ ディレクトリには LDAP サーバとドメインの 1 対 1 の割付がありますが、他の LDAP サーバではそうとは限りません。1 対 1 の割付がある場合、LDAP サーバごとに 1 つのドメインを設定するとサーバの選択が効率的になりますが、そうでない場合の選択の効率は下がります。

サーバごとに個別に設定できる設定項目は、管理インターフェースの「**システム セットアップ | ユーザ > 設定 > LDAP の設定**」ダイアログに現在含まれている項目です。LDAP の設定の詳細については、「LDAP を使用するための SonicWall の設定 (162 ページ)」を参照してください。

重要：適切な動作を実現するには、同じパーティション内の LDAP サーバはすべて同じスキーマに設定する必要があります。そうしないと、警告が発生します。

「**紹介**」の設定はグローバルに設定され、すべての認証パーティションのすべての LDAP サーバで共通になります。

メモ：セカンダリ サーバの明示的な設定は任意で行います。各プライマリ サーバとセカンダリ サーバを個別に設定するか、紹介を介してアクセスできるすべてのユーザ/グループ ツリーでプライマリを設定することができます。

トピック:

- セカンダリ サーバの設定について (175 ページ)
- 動的に学習されたセカンダリ サーバについて (175 ページ)
- バックアップ サーバについて (175 ページ)

セカンダリ サーバの設定について

永続的セカンダリ サーバの作成や設定は、プライマリ/セカンダリの設定以外はプライマリ サーバの場合と同じです。両者の機能における唯一の相違点は、検索を実行するときにその場所が設定済みユーザ/グループ ツリーから未知である場合、その検索はプライマリ サーバに送信され、プライマリ サーバは必要に応じて検索をセカンダリ サーバに渡すときに参照/紹介を送信することです。

動的に学習されたセカンダリ サーバについて

セカンダリ サーバが紹介または参照によって初めてアクセスされたとき、セキュリティ装置は設定されているさまざまなユーザ ツリーに基づいて複数のバインド ドメイン名 (DN) を試行した後、そのセカンダリ サーバにバインドします。セキュリティ装置は、セカンダリ サーバのレコードを内部的に作成し、今後の試行のためのバインド情報をそこに保存します。このプロセスには、設定されていないセカンダリ サーバも含まれます。そのようなサーバについて作成される動的なサーバ オブジェクトは、設定されているサーバのサーバ オブジェクトとともに内部的に保持されます。

このような動的に学習されたサーバ オブジェクトには、設定されているサーバと同様に、現在のバインド情報や追加情報を保存できます。この情報には、サーバによって学習されたユーザ/グループ ツリーや、オブジェクトの統計情報も含まれます。

メモ：この情報は再起動すると持続せず、必要に応じて再学習されます。ただし、動的セカンダリ サーバのユーザ/グループ ツリーの設定は、プライマリ サーバとともに保存されます。

バックアップ サーバについて

バックアップ サーバのサポートはアクティブ ディレクトリによって提供され、DNS ネーム システムを使用してバックアップを実現します。アクティブ ディレクトリ ドメイン コントローラには、機器またはドメインの DNS 名を使用してアクセスします。後者の場合、ドメイン名はドメインのすべてのコントローラ レプリカの IP アドレスのリストに解決されます。LDAP サーバ DNS 名が IP アドレスのリストに解決された場合、SonicWall セキュリティ装置はその 1 つが応答するまでそれぞれを試行します。したがって、プライマリ ドメイン名としてドメイン コントローラ機器名ではなく LDAP サーバ DNS 名を設定すると冗長性が加わり、プライマリが応答しない場合はバックアップ サーバが使用されます。

このメカニズムはアクティブ ディレクトリの紹介と参照でも機能し、ドメインへの紹介でセカンダリ ドメインの DNS 名が返されます。

メモ：アクティブ ディレクトリにおいては、バックアップ サーバは通常、レプリカ サーバと呼ばれます。

設定されているプライマリまたはセカンダリ LDAP サーバごとに、1 つまたは複数のバックアップを設定することができます。この設定によって、個々のサーバごとに状況と統計を記録することができ、上記の DNS 名メカニズムで冗長性サポートが提供されない非アクティブ ディレクトリ環境に、バックアップ サーバによる冗長性サポートを提供できます。

バックアップ サーバの大部分の設定はバックアップ元のサーバと同じなので、バックアップ サーバには他のサーバの設定のサブセットのみが指定されます。既定では、バックアップ サーバのホスト名と IP アドレスのみが必要とされます。

LDAP からのインポートとミラーリングについて

LDAP ユーザ グループ ミラーリングが有効である場合、LDAP ディレクトリ内でミラー関係にあるユーザ グループをローカルに作成するため、SonicWall セキュリティ装置は、LDAP サーバからユーザ グループおよびユーザ グループのネスト (グループを他のグループのメンバーにしたもの) を定期的に自動インポートします。

ミラー ユーザ グループは、アクセス ルールや CFS ポリシーなど、通常のユーザ グループを選択できるすべての部分で選択できます。ただし、ミラー ユーザ グループには一部の制限があります。例えば、ミラー ユーザ グループに他のユーザ グループをSonicWall セキュリティ装置上でローカルに追加することはできません。一方、ミラー ユーザ グループを他のローカル ユーザ グループのメンバーにしたり、ローカル ユーザをミラー ユーザ グループのメンバーにしたりすることはできます。ユーザは、LDAP サーバ上にあるユーザ グループのメンバーになると、そのローカルなミラー グループを介して設定されたアクセス権を自動的に受け取ります。

トピック:

- ユーザのインポート (176 ページ)
- ユーザ グループのインポートとミラーリング (177 ページ)

ユーザのインポート

「**LDAP 設定**」ダイアログまたは「**システム セットアップ | ユーザ > ローカル ユーザとグループ**」ページで LDAP からユーザのインポートを行う場合、インポート元の LDAP サーバを指定するオプションがあります。

- 特定の 1 つの LDAP サーバ
- 認証パーティション (有効な場合) 内のすべてのサーバ
- すべての LDAP サーバ

同じユーザ名が含まれる異なるドメインの異なる LDAP サーバからインポートしたユーザを区別するために、ドメインが含まれるいずれかの修飾ユーザ名形式を持つローカル ユーザ オブジェクトを作成するオプションもあります。このオプションは、シンプルなユーザ名とともに付加的に使用します。

いずれかの修飾ユーザ名形式でユーザ アカウントをインポートする場合、以下の点に留意してください。

- そのアカウントを使用してウェブ ログインまたはクライアント ログインを行うには、インポートしたとおりの完全修飾ユーザ名を正確に入力する必要があります。
- SSO を介してユーザを識別する場合、SSO 送信元に応じて名前形式が異なるため、ユーザ オブジェクトのユーザ名とドメイン構成要素は別個に照合されます。例えば、LDAP からインポートされたユーザ名が `jdoe@mydomain.com` で、SSO エージェントからレポートされたユーザ名が `MYDOMAIN/jdoe` である場合、両者は一致すると見なされ、そのユーザ アカウントはユーザの追加グループ メンバーシップの設定に使用されます。このように、SSO に関してどの修飾名前形式が選択されるかは問題ではなく、主として表示上の違いにすぎません。

  > ⓘ **メモ**：これは、「**システム セットアップ | ユーザ > 設定**」で「**ユーザ グループ情報の検索に LDAP を使用する**」または「**ローカルに登録されたユーザのみ許可する**」オプションが設定されている場合にのみ適用されます。詳細については、「LDAP を使用するための SonicWall の設定 (162 ページ)」および「SonicOS で SonicWall SSO エージェントを使用するための設定 (180 ページ)」を参照してください。

ユーザ グループのインポートとミラーリング

認証パーティショニングを使用する場合、パーティション内のユーザには、そのパーティションからインポートするユーザ グループへのアクセス権限を付与し、他のパーティションからインポートする同じ名前のユーザ グループへのアクセス権限を付与しないようにする必要があります。

例えば、インポートまたはミラーリングしたユーザ グループをポリシー内で使用して対象ユーザ グループを選択する場合、ポリシー内のグループ名と、ユーザのログイン時に LDAP から読み込んだグループ名を照合します。インポートしたユーザ グループとミラーリングしたユーザ グループの動作は少し異なります (主に歴史的理由によるものです)。

- ユーザ グループを手動でインポートすると、ドメイン構成要素のないシンプルなグループ名のローカル ユーザ グループ オブジェクトが作成されます。この場合、ユーザのグループ メンバーシップがローカル グループ名と照合されるとき、シンプルなグループ名のみが比較され、ドメイン構成要素は無視されます。したがって、複数の異なるドメインに同じ名前のユーザ グループが存在する場合は、どのドメインのユーザもそのローカル グループのメンバーシップを取得することになります。
- LDAP ユーザ グループ ミラーリングでグループをミラーリングする場合は、`group-name@domain.com` という名前のローカル ユーザ グループ オブジェクトが作成されるので、異なるドメインからミラーリングされたグループは区別されます。この場合、ユーザのグループ メンバーシップが LDAP から読み込まれるときも同じ形式が使用され、ドメイン構成要素も含む完全なグループ名が比較されます。複数の異なるドメインに同じ名前のユーザ グループが存在する場合は、ミラーリング元のドメインと同じドメインのユーザのみにそのグループのメンバーシップが設定されます。

手動でインポートしたユーザ グループの場合も、上記のミラーリングしたグループの場合と同様に、修飾グループ名をインポートしてドメイン別にユーザのメンバーシップを設定するオプションがあります。「**システム セットアップ | ユーザ > 設定 > LDAP の設定**」ダイアログまたは「**ユーザ > ローカル ユーザとグループ**」ページでグループのインポートを行う場合、ユーザについて同様のオプションがあります。ただし、選択できるのは「**シンプルな名前**」または「**名前@ドメイン**」 (既定) のいずれかの形式のみです。

メモ：インポートまたはミラーリングするユーザ グループには、認証パーティションの明示的な記録や確認は必要ありません。ドメイン構成要素を照合することによって、暗黙的にユーザのパーティション内のドメインのグループのみが選択されるからです。

下位互換性の目的と、異なるパーティションの標準グループのメンバーの共通アクセスを容易に設定できるようにするため、ユーザ グループをシンプルな名前で LDAP からインポート (または手動で作成) した場合は照合時にドメインが無視され、どのドメインやパーティションのユーザにもシンプルな名前を使用してアクセス権限を設定できます。

例えば、以下の状況があるとします。

- パーティション A: ドメイン `dom_a.com`
- パーティション B: ドメイン `dom_b.com`

この場合に両方から Administrators グループを **名前@ドメイン.com** としてインポートすると、`Administrators@dom_a.com` と `Administrators@dom_b.com` というローカル ユーザ グループがインポートされます。それぞれのパーティション内のユーザには、該当するグループへのアクセス権限のみが付与されます。

- パーティション A の管理者ユーザがログインし、LDAP 検索によって `dom_a.com` のAdministrators グループのメンバーであることが確認されると、そのユーザに `Administrators@dom_a.com` のメンバーシップが付与されます。

- 同様に、パーティション B の管理者ユーザがログインした場合には、Administrators@dom_b.com のメンバーシップが付与されます。

一方、いずれかのドメインからシンプルな名前として Administrators グループをインポートした場合は、Administrators という名前のローカル ユーザ グループが作成され、どちらのパーティションの管理者ユーザもそのグループへのアクセス権限を取得します。

ミラーリングの有効化はグローバルです。ミラーリングを有効にすると、設定されている LDAP サーバと学習された LDAP サーバのすべてからユーザ グループがミラーリングされます。

メモ：除外機能とワイルドカードを使用して、特定のサーバの全グループを除外することができます。

拡張 LDAP テストについて

LDAP テストでは、テストする LDAP サーバを選択でき、現在のユーザ認証のテストの他、接続性と検索のテストも追加できます。「LDAP テスト」テーブルを参照してください。

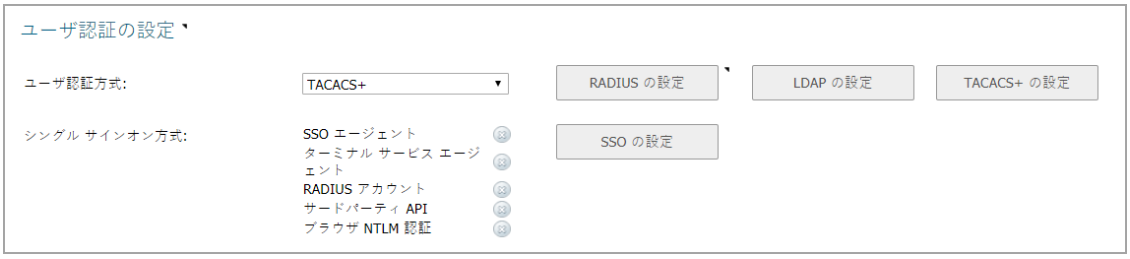
LDAP テスト

テスト	機能
接続性/バインド	設定されているバインド資格情報で LDAP サーバへのバインドを単純に試行します。
ユーザ認証	特定のユーザ名とパスワードが LDAP サーバに送信され、認証されることをテストします。
LDAP 検索	基本モードと詳細モードがあります。 **基本モード**は以下を検索します。 • 特定のログイン名、資格のあるログイン名、またはコモンネームでユーザを検索します。 • 特定の名前またはメンバーでユーザ グループを検索します。 **詳細モード**では以下が可能です。 • 明示的な検索フィルタ • 必要に応じた検索ベースと検索範囲の変更 (既定では、ドメイン サブツリーの最上位から、そのサブツリー全体を範囲として検索) • 複数オブジェクトの検索 • 返される情報の制限

認証用の TACACS + の設定

TACACS+ を設定するには:

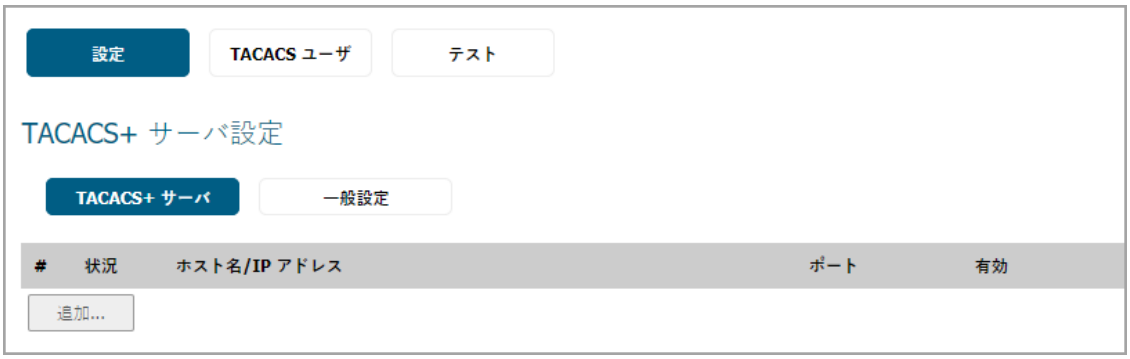
1 「**管理 | システム セットアップ > ユーザ > 設定**」に移動します。



2 「**ユーザ認証方式**」から、次のいずれかを選択します。

- **TACACS+**
- **TACACS+ + ローカル ユーザ**

3 「**TACACS+ の設定**」を選択します。「**TACACS+ 設定**」ダイアログが表示されます。



4 「**TACACS+ サーバ**」テーブルで、「**追加**」を選択します。「**サーバの追加**」ダイアログが表示されます。

5 「**ホスト名または IP アドレス**」フィールドにサーバの ID を入力します。

6 「**ポート**」フィールドにポート番号を入力します。既定値は **49** です。

7 「**共有鍵**」フィールドに共有鍵を入力します。

8 「**共有鍵の確認**」フィールドに共有鍵をもう一度入力します。

9 「**保存**」を選択します。サーバが TACACS に追加されます。

10 「**OK**」を選択します。

SonicOS で SonicWall SSO エージェントを使用するための設定

SonicWall SSO エージェントを使うようにセキュリティ装置を設定するには、以下の手順に従います。

1 「**管理 | システム セットアップ > ユーザ > 設定**」に移動します。

2 「**ユーザ認証の設定**」セクションの「**シングル サインオン方式**」で、「**SSO エージェント**」を選択します。TSA を追加して設定する場合も、SSO 方式としての SSO エージェントと同様に、この選択を使用します。

3 「**SSO の設定**」をクリックします。「**シングル サイン オン認証設定**」ダイアログが表示されます。

トピック:

- 「SSO エージェント」ページ (180 ページ)
- 「ユーザ」ページ (183 ページ)
- 「強制」ページ (187 ページ)
- ターミナル サービス エージェント (189 ページ)
- NTLM ページ (192 ページ)
- 「RADIUS アカウンティング」ページ (194 ページ)
- 「サードパーティ API」ページ (202 ページ)
- 「テスト」ページ (203 ページ)

「SSO エージェント」ページ

「**SSO エージェント**」ページの「**認証エージェント設定**」で、設定済みの SSO エージェントを確認できます。

- エージェントの IP アドレスの横の緑色の LED は、エージェントが現在稼働していることを示します。
- 赤色の LED は、エージェントが停止していることを示します。
- 灰色のLED は、エージェントが無効になっていることを示します。

LED は、AJAX を使用して動的に更新されます。

SSO エージェントを設定するには:

ヒント：フィールドに値を入力すると、ページ上部の行が赤色に更新され、新しい情報が強調表示されます。

1 「**追加**」を選択してエージェントを作成します。「**エージェントの追加**」ダイアログが表示されます。

2 パーティションがある場合は、エージェントを追加するパーティションを選択します。

3 「**OK**」を選択します。

4 SSO 設定オプションを構成します。

- 「**ホスト名または IP アドレス**」に、SonicWall SSO エージェントがインストールされているワークステーションのホスト名または IP アドレスを入力します。既定では、**0.0.0.0** が入力されます。
- 「**ポート**」には、SonicWall SSO エージェントが装置との通信に使用しているポート番号を入力します。既定のポートは **2258** です。

  メモ：エージェントは IP アドレスが異なれば、同じポート番号を使用できます。

- 「**共有鍵**」に、作成した共有鍵または SonicWall SSO エージェントで生成した共有鍵を入力します。共有鍵は完全に一致している必要があります。「**共有鍵の確認**」フィールドにもう一度共有鍵を入力します。
- 「**タイムアウト (秒)**」に、認証の試行がタイムアウトするまでの秒数を入力します。このフィールドには、既定の **10** 秒が自動的に設定されます。
- 「**再試行**」に、認証の試行回数を入力します。既定値は **6** です。

5 「**詳細設定**」を選択します。

6 「**一度に送信する最大リクエスト数**」に、装置からエージェントに一度に送信できる最大リクエスト数を入力します。既定値は **32** です。

エージェントは、各要求を処理する別個のスレッドをエージェント PC 内に生成し、複数の要求を同時に処理します。認証エージェントが扱える同時要求の数は、ネットワーク上またはネットワーク自身の機器の性能レベルに依存します。この設定を増やすと、シングル サイン オンのユーザ認証効率は上がりますが、エージェントを圧倒するまでに増やすと、一度に多数の要求が送信された場合に PC に過大な負荷がかかり、タイムアウトや認証失敗の原因になります。

その一方、装置から送信される要求数が少なすぎると、一部の要求は待たなければならなくなり、リング バッファ オーバーフローが発生する可能性があります。待機している要求が多すぎると、シングル サイン オン認証の応答時間が遅くなることがあります。リング バッファの警告を抑えるためにこの値を増やそうとしても、著しい数のタイムアウトが生じて十分に大きな値を設定できない場合は、エージェントを高性能の専用機器に移動させるか、エージェントの追加を検討してください。リング バッファ オーバーフローおよび SonicOS TSR 内の関連する統計情報の確認方法については、「シングル サインオンの高度な機能 (114 ページ)」を参照してください。

ヒント：テクニカル サポート レポートの「**シングル サイン オン認証**」セクションの統計を参照してください。著しい数のタイムアウトがある場合は、この値を減らすことで解決する可能性があります。「**リングに使用される最大時間**」がポーリング率 (「**ユーザ**」タブで設定) に近づくか超えている場合、またはリング バッファ オーバーフローが見られる場合は、この値を増やすことをお勧めします。

ページが更新され、ページ上部のテーブルに新しい行が表示されます。

ヒント：これらのエントリを編集するには、エントリを選択します。エントリが、編集可能なフィールドになります。

7 「**認証エージェント設定**」の下にある「**一般設定**」を選択します。

8 以下のオプションを設定します。

- ユーザ認証に SSO エージェントを使用するには、「**SSO エージェント認証を有効にする**」チェックボックスを選択します。このオプションは、既定で選択されています。
- 最初のエージェントから応答がない場合やエラーが返されたときに別の SSO エージェントによる認証を試行させるには、「**NetAPI/WMI から名前を受け取らなかった場合は次のエージェントを試行する**」チェックボックスを選択します。このオプションは、既定では選択されていません。

  メモ：この設定は NetAPI/WMI を使用するエージェントにのみ適用され、ドメインコントローラのセキュリティ ログ調査メカニズムだけを使用するエージェントには適用されません。

  重要：「**ユーザ**」タブの「**ユーザを認証したエージェントにポーリングする**」も参照してください。この設定を有効化する場合は、これを設定する必要があります。

  ユーザ識別のために SSO エージェントによって使用される NetAPI/WMI プロトコルは Windows が提供しており、これらのプロトコルの実際の動作内容に対しては、エージェントと装置のどちらの制御も及びません。NetAPI または WMI を使用しているとき、Windows がエージェントからの要求に対してユーザ名もなくエラーもない応答を返した場合、装置は既定で、他のエージェントも同じ応答を取得し、(エラー応答を受け取った場合に行うような) 別のエージェントによる要求の再試行を行わないものと想定します。

  本来ならばユーザが認識されているはずなのに「SSO エージェントがユーザ名を返しません」という認証エラーがログに記録されている場合は、試しにこの設定を有効化してみてください。この設定が有効な場合にユーザ名がないという応答をエージェントから受け取ると、装置はその応答をエラーと見なし、別のエージェントを使って要求を再試行します。

  一般的に言って、この設定を有効化しなければならないのは、一部のエージェントだけが特定のユーザに到達できるような状況が生じているときです。例えば、中央サイトのエージェントから簡単に到達できないユーザを識別するために別のエージェントをリモート サイトにどうしても配置する必要がある場合です。

- 「**シングル サイン オンの待機中にユーザのトラフィックを遮断しない**」チェックボックスを選択すると、ユーザの識別時に既定のポリシーを使用します。これによって参照の遅延を回避できます。このオプションは、既定では選択されていません。

  ユーザが SSO を通して識別されているとき、そのユーザからのトラフィックは通常、ユーザの識別が完了して適切なポリシーが必要に応じて適用されるまでは遮断されます。しかし、SSO エージェントによるユーザの識別にはかなり時間がかかることがあり、その結果、ユーザのウェブ閲覧体験に遅延が生じる場合があります。

  この設定を有効にすると、シングル サイン オンの待機中に、ユーザの識別が完了するまでの間は既定のポリシーを適用して遅延をやり過ごし、ユーザ トラフィックを通過させることができます。

  ユーザ認証を必要とするアクセス ルールでユーザを識別しなければならないとき (つまり、適切に識別されなければ、ユーザのアクセスを許可しないような状況では)、ユーザのトラフィックの通過を許可するかどうかを選択することもできます。

注意：この処置には、識別されたとき、本来であれば許可しないユーザを一時的に通過させてしまうことがあるので注意が必要です。選択した特定のアクセス ルールに対してこの処置を行うと、それに関係する設定は、ユーザ認証を必要とするルールの詳細設定に現れます。

- 「**含まれる対象**」チェックボックスを選択し、さらに「**すべてのアクセス ルール**」(既定値) と「**選択したアクセス ルール**」ラジオ ボタンのどちらかを選択すると、ユーザ識別の待機中も、ユーザ認証を必要とするアクセス ルールに影響されるトラフィックが許可されます。

△ **注意：このオプションを使用すると、ユーザが識別されていれば許可されないアクセスも一時的に許可されます。**

- すべての SSO エージェントをユーザ データベースと同期させるには、次のどちらかを選択します。
  - **すべてのエージェントを同期する** - 使用する識別メカニズムとは無関係に全体を同期させることで、すべてのエージェント上に単一の同質なユーザ データベースを作成します。
  - **同じユーザ識別メカニズムを持つエージェントを同期する** - 同じ識別メカニズムを使用するデータベースだけを同期させます (既定値)。

  各 SSO エージェントは、識別したユーザを登録するデータベースをそれぞれ独自に維持しており、必要に応じてエージェントを設定してデータベースが同期されるようにすることで、各エージェント上に複製された共通のユーザ データベースを作成できます。共通の同期されたユーザ データベースは、ユーザ調査をより効率化し、冗長性を高めます。ここで同期を指定すると、装置から同期対象の他のすべてのエージェントに情報を伝えることができるので、エージェントごとに設定を行わなくてすみ、無用な混乱を回避できます。

  既定で、装置のエージェントは同じユーザ識別メカニズムを用いて互いに同期するように設定されます。例えば、一群のエージェントがドメイン コントローラのログを読み、他の一群のエージェントが NetAPI を使用する場合、この 2 つのエージェント グループには、それぞれ独立した外部データベースが含まれることになります。1 つは、ドメイン コントローラのログで発見されたユーザを登録するデータベースで、もう 1 つは NetAPI で識別されるユーザ登録するデータベースです。

  ⓘ **メモ：**この設定は、互いに同期するその他のエージェントのリストを各 SSO エージェント内に設定することで、オーバーライドできます。

- 「**Windows サービスにより使用されるユーザ名**」テーブル内で、Windows サービス ユーザ名のリストを設定します。エンドユーザの PC 上のサービスから使用できるユーザ名は最大 64 個です。それらの名前を用いたログインはサービスのログインであると見なされ、SSO エージェントからは無視されます。

  a) 「**追加**」を選択します。「**サービス ユーザ名**」ダイアログが表示されます。

  b) サービス ユーザ名を入力します。

  c) 「**OK**」を選択します。

  d) ユーザ アカウントごとに「ステップ a」～「ステップ c」を繰り返します。

  Windows サービスは、マシンまたはドメインにログオンするとき、現実のユーザと同じようにユーザ アカウントを使います。SSO エージェントで使われる Windows の一部の API は、サービスのログインと現実ユーザのログインを区別する仕組みを提供していません。そのため、サービスで使われたユーザ名が SSO エージェントから誤って伝えられ、それが現実のユーザのユーザ名と一致しないことがあります。

「ユーザ」ページ

1 「**ユーザ**」を選択して、以下の「**ユーザ設定**」オプションを指定します。

- 「**ローカルに登録されたユーザのみ許可する**」チェックボックスをオンにすると、装置上でローカルに登録されたユーザだけが認証されるようになります。この設定はデフォルトで無効になっています。
- ドメインではなくコンピュータにログインしたユーザに対して限定的なアクセスを許可する場合は、「**非ドメイン ユーザには限定的なアクセスのみ許可する**」チェックボックスを選択します。ローカルで設定されている場合でも、これらのユーザには、Trusted Users ユーザ グループのメンバーシップは付与されません。 また、Trusted Users に設定されているアクセス権も与えられません。これらには、ポリシーを通してアクセス権が与えられます。例えば、Everyone に適用されるものや、許可されたユーザとして明示的にリストされたものなどです。この設定はデフォルトで無効になっています。

  ログ内では、これらのユーザは 「*コンピュータ名/ユーザ名*」という形式で識別されます。ユーザの認証にローカル ユーザ データベースを使用しているとき「**ローカル データベースでシンプルなユーザ名を使用する**」オプションが無効になっている場合は、ローカル データベースでのユーザ名の設定に「*コンピュータ名/ユーザ*」という形式の完全な識別名を使用しなければなりません。

  メモ：これは NTLM を通して認証されたユーザには適用されません。NTLM 認証では、名前/パスワードが装置上のローカル ユーザ アカウントと一致する場合に限って非ドメイン ユーザにアクセス権が与えられます。

- ネットワークに Windows 以外の機器や、パーソナル セキュリティ装置が稼働している Windows コンピュータが存在する場合は、次の手順に従います。

  a) 「**ユーザの監視を右記で行う**」チェックボックスをオンにします。

  b) 次のいずれかを選択します。これは SSO エージェントのためにどれを設定するかによります。

  - **NetBIOS を超えた NetAPI**
  - **TCP を超えた NetAPI**
  - **WMI**

  ヒント：これらのオプションの上にマウスを移動すると、小さなツールチップで TCP ポート番号が表示されます。

  SSO エージェントは、Windows ドメイン内のユーザの識別を試みるとき、NetAPI または WMI を使用している場合、トラフィックの送信元であるユーザのコンピュータと直接通信を試みます。これは次の問題を起こす可能性があります。

  - つまり、トラフィックの発信源が Windows 以外の機器のとき、それらは SSO エージェントがユーザを識別するために使用する Windows ネットワーキング メッセージに応答せず、それらのメッセージを遮断することもあります。
  - Windows コンピュータに、それらを遮断するパーソナル セキュリティ装置が設定されている場合もあります。

  その結果、多数のスレッドが応答待ちの要求で待機状態となり、エージェントに過大な負荷がかかります。

  この問題を回避するには、このオプション (既定で無効) を有効化し、SSO エージェント側で使うように設定されている適切な NetAPI/WMI プロトコルを選択します。エージェントに要求を送信する前に SonicWall 装置は NetAPI または WMI を通してユーザを識別するために、トラフィックの送信元のマシンをプローブして、NetAPI または WMA プロト

コルのポートに応答が返されるか確認します。応答がない場合、装置は SSO を直ちに失敗させるので、エージェントの関与は起こりません。

メモ：この設定は、ユーザ ログイン情報をドメイン コントローラから読むエージェントには影響しません。

- 「**ユーザの監視を右記で行う**」を有効化すると、セキュリティ装置は SSO エージェントにユーザを識別するよう要求する前に、NetAPI/WMI ポートで応答をプローブするようになります。「**監視タイムアウト (秒)**」フィールドは、既定で **5** 秒に設定されています。
- シングル サイン オン中にユーザ認証を中断しないで SSO プローブが正常に機能していることをテストするには、「**監視テスト モード**」チェックボックスをオンにします。監視は、SSO エージェントを介してユーザ認証を開始した後に送信されます。この設定はデフォルトで無効になっています。

  このオプションを有効化すると、SSO エージェントを通してユーザ認証を初期化した後にプローブが送信されます (通常、プローブが成功すれば、初期化は完了しています)。プローブの統計は、いつもどおりに更新されます。プローブに失敗したユーザがエージェントによって正しく認証された場合は、その旨がコンソール ポートにメッセージで報告されます。
- 「**ユーザ グループのメンバーシップの設定方法**」で、どちらかを選択します。
  - **ユーザ グループ情報の検索に LDAP を使用する** - ユーザ情報の検索に LDAP を使用します。このオプションは、既定では選択されています。
    - LDAP 設定を構成するには、「**設定...**」を選択します。「**LDAP 設定**」ダイアログが表示されます。このダイアログの設定情報については、「LDAP の詳細設定 (204 ページ)」を参照してください。
  - **ローカル設定** - ローカルで設定したユーザ グループを使用します。
- 「**ポーリング間隔 (分)**」フィールドに、ポーリング間隔 (分)を入力します。既定値は **5** 分です。識別されてログインしたユーザに対して、SonicWall はこの間隔で認証エージェントをポーリングすることで、ユーザがまだログオンしているか確認します。

  NTLM 認証を使用している場合は、NTLM の設定で、装置にユーザのポーリングを選択的に行わせることが可能で、具体的にはエージェントを通してポーリングする代わりに NTLM を通してユーザを強制的に再認証することができます。
- ユーザがまだログイン中かどうかを判断する際に任意のエージェントにポーリングするのではなく、ネットワーク トポロジーの都合によって、ユーザの場所に応じて特定のエージェントを使用する必要がある場合は、「**ユーザを認証したエージェントにポーリングする**」チェックボックスをオンにします。このオプションは既定で無効になっています。

  重要：これを設定する場合は、「**SSO エージェント - 一般設定**」タブの「**NetAPI/WMI から名前を受け取らなかった場合は次のエージェントを試行する**」も設定する必要があります。

  既定で、装置は任意の SSO エージェントが NetAPI または WMI 要求を任意のユーザに送信できると仮定し、ユーザの現在のログイン状態を確認するためにポーリンスを行うとき、現在のローディング状況に基づいていずれかのエージェントを選択できます。これに該当しない場合、ネットワーク トポロジの関係から、ユーザの位置に基づいて特定のエージェントを使う必要があるときは、このオプションを有効化します。これを有効化すると、ユーザがエージェントによって正常に識別された後、同じユーザに関するそれ以降のポーリングは同じエージェントを通して行われます。

  メモ：この設定は NetAPI/WMI を使用するエージェントにのみ適用され、ドメイン コントローラのセキュリティ ログ調査メカニズムだけを使用するエージェントには適用されません。

- トラフィックの識別時、セキュリティ装置は最初の試行に失敗した場合、一定時間待ってから再度トラフィックの識別を試みます。このときの待機時間 (分単位) を「**失敗後の保留時間 (分)**」フィールドに入力します。SSO が繰り返し失敗すると送信元からいっそう多くのトラフィックが送られてくるようになり、未処理の要求が溢れかえります。この機能はエージェントに対して要求を送る頻度を制限することで、こうした状況が発生を回避します。既定値は **1** 分です。

  メモ：保留時間は、SSO エージェントのエラーを契機とするものとログイン ユーザなしの報告を契機とするものがあり、それぞれ別々に設定されます。

- 「**...ユーザが見つからなかった後の保留時間 (分)**」フィールドには、SSO エージェントからエラーが返された場合やエージェントからログイン済のユーザがいないと報告された場合に再試行するまでの待機時間を分単位で入力します。既定値は **1** 分です。

- 「**増加**」が有効になっている場合、SSO 障害後の最初の再試行は迅速であり、設定されたレートに達するまで、後続の障害でホールドオフ期間が指数関数的に増加します。これは、一時的な障害 (例えば、起動中の PC でトラフィックが生じているとき起こる障害) の後にユーザを識別することが大幅に遅れるような事態を回避するのに有効です。このオプションは、既定では選択されています。

  ヒント：増加が役に立たない問題が発生した場合は、増加のタイミングが早すぎて問題がまだ解決していない可能性があるので、増加速度を遅くしてみてください。

- 増加速度を選択します。
  - **4 (高速増加)** (既定)
  - **3**
  - **2**
  - **1 (低速増加)**

2 ログに記録されるドメインの名前に一貫性を持たせるため、「**異なる SSO ソースがユーザのドメインに対して異なる名前を報告した場合:**」で以下のいずれかのラジオ ボタンを選択します。

- **受け取ったドメイン名をそのまま使用する** (既定値)
- **一貫性のあるドメイン名を常に使用する** (「ステップ a」に進んでください)

既定で、SSO を通して識別されたユーザは SonicWall 装置上のログに記録されます。そこには、ユーザを識別した外部ソースからドメイン名が報告されます。しかし、ドメインは、通常、2 つまたは 3 つの異なるドメイン名を持ちます (例えば、Windows ドメインには DNS 名、NetBIOS 名、Kerberos 領域名があります)。そのため、同じドメイン内の特定のユーザに対して、異なる複数の SSO ソースからそれらの異なる名前が報告されることがあります。

こうした名前の変化によって、ログ内でユーザをドメイン別に追跡するのが困難になるおそれがあります。これに対処するため、同じドメインのすべてのユーザで同じドメイン名のバリアントを使うことにより、SonicWall 装置にどのバリアントが報告されても、名前に一貫性を持たせることができます。

a 「**一貫性のあるドメイン名を常に使用する**」を選択した場合は、「**選択**」を選択します。「**各ドメインで使用する名前の選択**」ポップアップ ダイアログに、既知のドメインがリストされます。このリストから表示に使う名前を選択することができます。

b 使用するバリアントを選択します。各ドメインの初期の既定値は「**なし**」です。これは SSO を通して装置に報告されるどのドメイン名についても、「**一貫性のあるドメイン名**

を常に使用する」を有効にして、使用するドメイン名をここで選択するまでは、名前の使用動作に変化が起こらないことを意味します。

メモ：このリストにドメインが表示されない場合は、ドメイン内のユーザが SSO によって識別されるのを待ってから、この手順を再度実行してください。

c 「**OK**」を選択します。

シングル サイン オンを使用しているとき、「**管理 | システム セットアップ > ユーザ > 状況**」ページで予期せぬユーザ名を見つけ場合や、ログで予期せぬユーザ名によるユーザ ログインまたはユーザ ログインの失敗を見つけた場合は、Windows サービスのログインに起因するものと考えられるので、それらのユーザ名をここで設定して SSO エージェントに無視すべき名前と認識されるようにしてください。

複数のセキュリティ装置が 1 つの SSO エージェントと通信している場合、サービス アカウント名のリストはいずれか 1 台の装置上でのみ設定してください。異なる装置上で複数のリストを設定した場合の影響は不明確です。

「強制」ページ

1 特定のゾーンからのトラフィックでも SSO を開始したい、また、内部プロキシ ウェブ サーバや IP 電話のような、非ユーザ機器からのトラフィックは SSO をバイパスさせたい場合は、「**強制**」を選択します。

2 「**ゾーン毎に SSO を強制する**」の下で、トラフィックが送られてきたときどのゾーンで SSO を開始してユーザを識別するかを指定するために、ゾーンに対応する各チェックボックスを選択します。

- **LAN**
- **DMZ**
- **VPN**

- **MGMT**
- **WLAN**

アプリケーション制御やその他のポリシーによって SSO がゾーン上で既に必要な場合は、これらのチェックボックスは選択済みで、解除できません。ゾーン上でゲスト サービスが有効な場合は、SSO は強制できず、チェックボックスは選択できません。SSO が開始されていないそれ以外のゾーンについて、このオプションで SSO の強制を有効化できます。

メモ：ユーザ認証を要求するセキュリティ サービス ポリシーやアクセス ルールが設定されたゾーンでは、影響のあるトラフィックに対して常に SSO が開始されるので、ここでさらに SSO の強制を有効にする必要はありません。

これらのゾーンごとの SSO 強制設定は、SSO が別の方法で、コンテンツ フィルタ、IPS、またはアプリケーション制御ポリシーによって、またはユーザ認証が必要なアクセス ルールによって開始されない場合でも、イベント ログ取得と AppFlow 監視の視覚化の際にユーザの識別と追跡に役立ちます。

3 特定のサービスまたは位置からのトラフィックをバイパスし、既定のコンテンツ フィルタ ポリシーをトラフィックに適用するには、「**SSO バイパス**」テーブル内のリストから適切なサービスまたは位置を選択するか、新規のサービスまたは位置をテーブルに追加します。このテーブルには、SSO をバイパスする組み込みサービスが表示されます。これらのサービスは削除できません。

ヒント：この目的で SSO バイパス アドレスやサービス グループ オブジェクトを作成すれば、同じオブジェクトをここだけでなく該当するアクセス ルールでも参照することができます。

メモ：SSO のバイパス設定は、ユーザ認証を要求するアクセス ルールによって SSO が開始された場合には適用されません。この種の SSO バイパスを設定するには、影響を受けるトラフィックに対してユーザ認証を要求しない別のアクセス ルールを追加します。アクセス ルール設定の詳細については、『*SonicOS 6.5 ポリシー*』を参照してください。

既定では、SSO によって認証されない Linux および Mac ユーザには、既定のコンテンツ フィルタ ポリシーが割り当てられます。そのような、SSO により認証されないすべてのユーザを資格情報を手動で入力させるようリダイレクトするには、「**HTTP**」サービスに対して、「**WAN**」ゾーンから「**LAN**」ゾーンへのアクセス ルールを「**包含ユーザ**」を「**すべて**」に設定して作成します。そして、ユーザまたはユーザ グループに対して適切な CFS ポリシーを設定します。アクセス ルール設定の詳細については、『*SonicOS 6.5 ポリシー*』を参照してください。

SSO バイパスが必要とされるのは、次のような場合です。

- 非ユーザ機器 (内部メール サーバや IP 電話) からのトラフィック
- 認証が不要で SSO 待ちの遅延が悪影響を及ぼす可能性のあるユーザ トラフィック

SSO をバイパスするトラフィックには、既定のコンテンツ フィルタリング ポリシーが適用されます。ユーザを包含/除外するために何らかのアプリケーション ルールや侵入防御/アンチスパイウェア ポリシーが設定されていても、それらのルールやポリシーによってそのトラフィックが包含/除外されることはなくなります。

2 つ目の設定は、認証される必要のないユーザ トラフィックに対して適切で、SSO を開始することにより、サービスに対して望ましくない遅延を引き起こす可能性があります。

4 必要に応じて、サーバまたは位置を追加します。

a 「**追加**」を選択します。「**SSO バイパス ルールの追加**」ダイアログが表示されます。

b 「**次の場合に SSO をバイパスする:**」で、「**サービス**」または「**アドレス**」を選択します。

c ドロップダウン メニューからサービスまたはドレスを選択します。

d 「**バイパス種別**」を選択します。

- **完全なバイパス (SSO を開始しない)**
- **SSO を開始するが SSO 待機中に保有パケットをバイパスする** (既定)

e 「**追加**」を選択します。テーブルにエントリが追加されます。

5 ログのための SSO バイパス ユーザ名を選択します。

a 「**SSO バイパス用のユーザ名 <*バイパス名*> をログに記録する**」をオンにします。

b SSO をバイパスするユーザのための名前を指定します。既定値は **不明 (SSO バイパス)** です。

この設定は既定で選択されており、既定の名前 **SSO バイパス**が指定されています。この設定が有効な場合は、(ここで設定したように) SSO をバイパスしたトラフィックがログ内や AppFlow 監視で表示されるとき不明ユーザではなく所定のユーザ名を付けて表示されるので、SSO が識別できなかったユーザから送られてきたトラフィックとは区別できます。

ヒント：ログオンの設定は、「**ユーザ > 設定**」ページの「**ユーザ セッション設定**」でも行うことができます。

6 必要に応じて、「**ダミー ユーザを作成する**」をオンにします。このオプションは、既定では選択されていません。

このオプションとともに「**SSO バイパス用のユーザ名 <*バイパス名*> をログに記録する**」をオンにすると、SSO バイパス トラフィックの受信時にダミー ユーザ エントリが作成され、発信元 IP アドレスに対応する所定のユーザ名が付与されます。そのため、ログ内や AppFlow 監視で表示される名前の他に、ダミー ユーザ エントリが「**管理 | システム セットアップ > ユーザ > 状況**」ページに表示されます。このダミー エントリの名前はそのまま表示されます。その表示は、対応する IP アドレスからのトラフィックが所定の無動作時間にわたって停止するか、(バイパス サービスの場合) 同じ IP アドレスから非バイパス トラフィックが送られてくるまで持続します。

メモ：このダミーのユーザ名は、完全な SSO バイパス用に設定されたバイパス ルールに対してのみ適用されます。SSO を開始するものの SSO の待機中に保有パケットをバイパスするように設定されたユーザは、開始された SSO 識別の結果に従って設定されることになります。

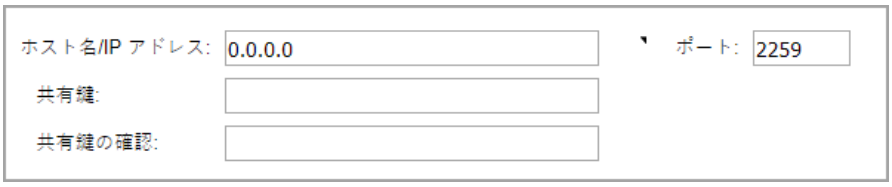
メモ：このオプションのログ記録に関する部分は、「**ユーザ > 設定**」ページの「**ユーザ セッション設定**」セクションの「**ユーザが識別されていない接続のログ記録**」オプションでも設定できます。

a 必要に応じて、「**無動作時タイムアウト (分)**」フィールドに無動作タイムアウトの時間 (分) を指定します。既定値は **15** 分です。

ターミナル サービス エージェント

1 「**ターミナル サービス**」を選択して、以下の「**ターミナル サービス エージェント設定**」オプションを指定します。

2 エージェントを追加には、「**追加**」を選択します。「**ターミナル サービス エージェントの追加**」ダイアログが表示されます。



ヒント：パーティション処理が有効になっている場合、「**パーティションの選択**」ダイアログが「**ターミナル サービス エージェントの追加**」ダイアログの上に表示されます。

1 新しいエージェントをどのパーティションに追加するかを指定します。

2 「**OK**」を選択します。

- 「**ホスト名/IP アドレス**」フィールドに、SonicWall TSA がインストールされているターミナル サーバのホスト名または IP アドレスを入力します。ターミナル サーバがマルチホーム (複数の IP アドレスを持つ) で、ホストを DNS 名ではなく IP アドレスで識別している場合には、すべての IP アドレスをカンマ区切りのリストとして入力します。
- 「**ポート**」には、SonicWall TSA が装置との通信に使用しているポート番号を入力します。既定のポートは **2259** です。

  メモ：エージェントは IP アドレスが異なれば、同じポート番号を使用できます。

- 「**共有鍵**」フィールドに、作成した共有鍵または SonicWall TSA で生成した共有鍵を入力します。共有鍵は完全に一致している必要があります。「**共有鍵の確認**」フィールドにもう一度共有鍵を入力します。

  ヒント：共有鍵は、偶数文字でなければなりません。

ページが更新され、ページ上部のテーブルに新しい行が表示されます。また、ページの下半分に新しい入力フィールドが表示されます。既存のエージェントに関する表示は次のとおりです。

- 緑色の LED アイコンは、エージェントが稼働していることを示します。

- 赤色の LED アイコンは、エージェントが停止していることを示します。
- 黄色の LED アイコンは、TSA が無動作状態で、TSA からファイアウォールへの通知が 5 分以上途絶えていることを示します。

装置がエージェントに要求を送信するのではなく、TSA が装置に通知を送信する形であることから、通知がないときには問題が生じている可能性もあり得ますが、それより考えられるのは、単にターミナル サーバで現在どのユーザもアクティブではないという可能性です。

3 「**ターミナル サービス エージェント設定**」の「**一般設定**」を選択すると、次のオプションを設定できます。

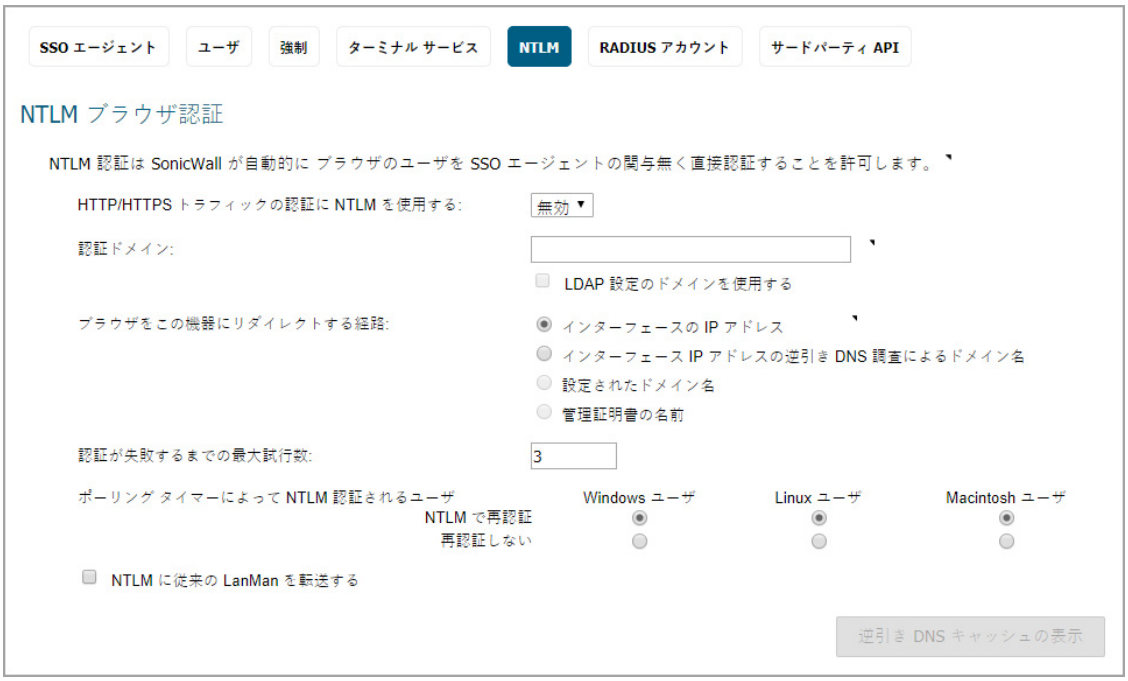
- ユーザ認証に TSA を使用するには、「**ターミナル サービス エージェント認証を有効にする**」を選択します。このオプションは、既定では選択されていません。
- 「**ターミナル サーバのサービスからのトラフィックが、アクセス ルールのユーザ認証をバイパスすることを許可する**」は既定でオンになっています。この設定の場合は、Windows アップデートやアンチウイルスの更新など、ユーザ ログイン セッションと関連付けられていないサービス トラフィックは認証なしで通過できます。そのトラフィックは、認証を要求するアクセス ルールが適切に設定されていれば本来遮断されるはずのものです。

  このオプションを選択解除した場合、アクセス ルールでユーザ認証が必要なときには、サービスからのトラフィックが遮断されることがあります。この場合、サービスのトラフィックの宛先に**すべて**へのアクセスを許可するルールを追加するか、その宛先をアクセス ルールでユーザ認証がバイパス可能な HTTP URL として設定することで対応できます。

NTLM ページ

重要：RADIUS を設定する必要があります。

1 「**NTLM**」を選択します。



NTLM 認証は Mozilla ベースのブラウザでサポートされ、SSO エージェントを介して、またはエージェントを使わずに自身でいくつかの制限付きで、ユーザを識別する補足として使うことができます。セキュリティ装置はユーザを認証するためにブラウザと直接情報交換します。ドメインの資格情報を使ってログインしたユーザは透過的に認証されます。その他の場合、ユーザは装置にログインするために資格情報を入力する必要があります。しかし、資格情報を保存すれば 1 度だけそうすれば済むはずです。

NTLM の詳細については、「ブラウザ NTLM 認証の動作 (108 ページ)」を参照してください。

2 以下の設定を行います。

- 以下の選択肢のうちの 1 つを、「**HTTP トラフィックの認証に NTLM を使用する**」から選択します。
  - **無効** - NTML 認証を使用しません。
  - **有効** - SonicWall SSO エージェントを使う前に NTLM を使ってユーザの認証を試行します。
- 以下のうちの 1 つを、「**認証ドメイン**」に対して行います。
  - 次のいずれかを入力します。
    - ドメインの完全な DNS 名。形式は `www.somedomain.com`。
    - LDAP を使用している場合、LDAP 設定に入力したのと同じドメイン。

NTLM プロトコルでは、サーバ (現在のファイアウォール) は自分のドメインをブラウザに知らせる必要があるので、ユーザに対する認証が完全に透過的に行われるのは、ブラウザがそれをローカル ドメインとして認識する場合に限られます。

ヒント：NTLM プロトコルにおけるドメインは、名前/パスワードを実際に認証するために必要ですが、ブラウザから要求されたり、ブラウザで必要とされたりする可能性もあります。ドメインが認証の結果に影響を与えるかどうかは、ブラウザによって異なります。

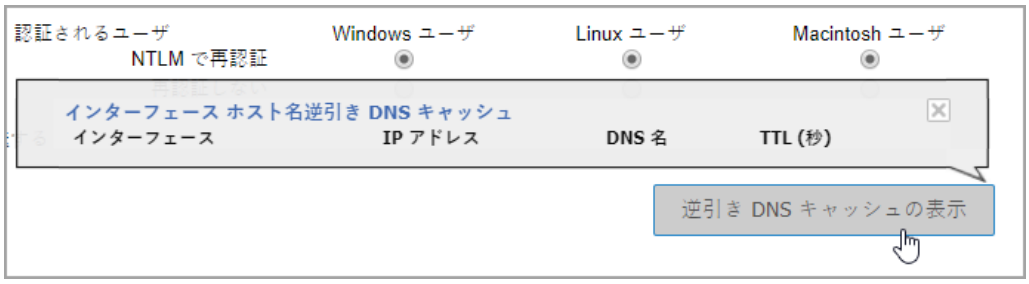
- LDAP 設定内で使っているものと同じドメインを使うために、「**LDAP 設定のドメインを使用する**」を選択します。

ブラウザが装置のドメインをローカル ドメインと見た場合にのみ、完全に透過的な認証が行われます。

- ユーザのブラウザを最初にセキュリティ装置自身のウェブ サーバにどのようにリダイレクトするを決めるために、「**ブラウザをこの機器にリダイレクトする経路**」に対して、以下のオプションのうちの 1 つを選択します。
  - **インターフェースの IP アドレス** - ブラウザを装置のウェブ サーバ インターフェースの IP アドレスにリダイレクトする場合に選択します。このオプションは、既定では選択されています。
  - **インターフェース IP アドレスの逆引き DNS 調査によるドメイン名** - ウィンドウ下部の「**逆引き DNS キャッシュの表示**」を有効にします。このボタンを選択すると、ポップアップが装置のウェブ サーバのインターフェース、IP アドレス、DNS 名、TTL の秒数を表示します。ユーザのブラウザをリダイレクトするために使われているドメイン名 (DNS 名) を確認する場合にこのボタンを選択します。
  - **設定されたドメイン名** -「**システム > 管理**」ページで設定したセキュリティ装置のドメイン名を使用します。
  - **管理証明書の名前** -「**装置 > 基本設定**」ページで HTTPS ウェブ管理用として選択した、インポートした証明書を使用します。
- 「**認証が失敗するまでの最大試行数**」に再試行回数を入力します。既定値は **3**、最小値は 1、最大値は 99 です。
- ユーザのログオフを検出するには、Windows、Linux、および マッキントッシュ ユーザに対して装置で使用されるポーリング方式を、「**ポーリング タイマーによって NTLM 認証されるユーザ**」オプション内で選択します。それぞれの種別のコンピュータのユーザ (**Windows ユーザ**、**Linux ユーザ**、**Macintosh ユーザ**) のオプションを選択します。
  - **NTLM で再認証** - ブラウザがドメインの資格情報を保存するように設定されている、またはユーザがブラウザに資格情報を保存するように指示した場合は、この方式はユーザに透過的です。
  - **再認証しない** - このオプションを選択した場合は、無動作タイムアウト以外ではログアウトは検出されません。

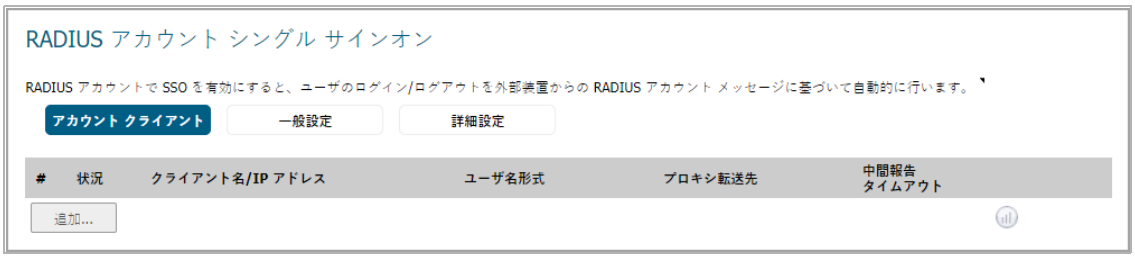
メモ：複数のコンテンツ フィルタ ポリシーが設定されているとき、NTLM を有効にしてシングル サインオンを強制する場合は、Trusted Users を「包含ユーザ」として設定した HTTP/HTTPS アクセス ルールを「**管理 | ポリシー > ルール > アクセス ルール**」ページの「LAN から WAN」ルールのリストに追加する必要があります。このルールによって、ユーザに対する NTLM 認証要求が開始されます。このアクセス ルールがないと、制限の厳しい CFS ポリシーによってユーザのインターネット アクセスが遮断されて認証が行われない場合があります。

- 旧形式の LAN Manager 構成要素が NTLM メッセージ内に含まれることを必要とする古い旧形式のサーバを使っている場合は、「**NTLM に従来の LanMan を転送する**」チェックボックスを選択します。これにより、安全でないために既定では NTLM 内 LanMan を許可しない、新しい Windows サーバでは認証が失敗します。
- インターフェース IP アドレスの逆引き DNS 調査によるドメイン名を選択した場合は、「**逆引き DNS キャッシュの表示**」を選択します。ポップアップが表示されます。



「RADIUS アカウンティング」ページ

1 「**RADIUS アカウント**」を選択して、「**RADIUS アカウント シングル サインオン**」を表示します。



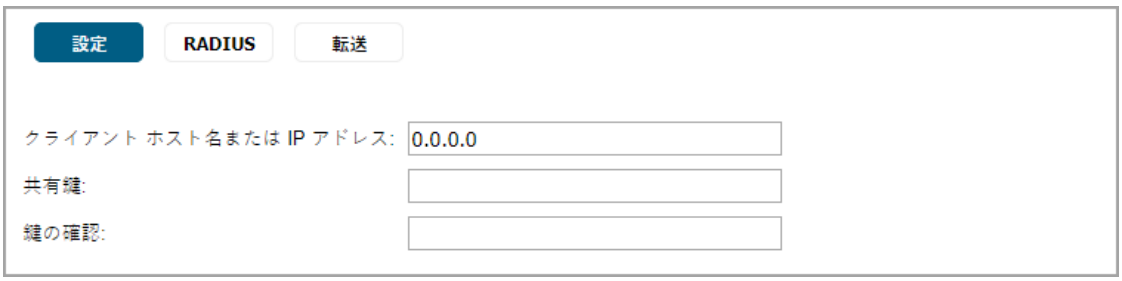
RADIUS アカウントによるシングル サインオンでは、装置を外部のサードパーティ装置の RADIUS アカウント サーバとして利用し、サードパーティ装置からのアカウント メッセージに基づいてユーザをログイン、ログアウトすることができます。サードパーティ装置がその他の目的で RADIUS アカウントを使用している場合、SonicOS は RADIUS アカウント メッセージを別の RADIUS アカウント サーバに転送することもできます。

リスト上の各 RADIUS アカウント クライアントの現在の状況が、パネルの「**状況**」列に次のように表示されます。

- 緑色 - クライアントはアクティブ状態
- 黄色 - クライアントはアイドル状態
- 灰色 - クライアントが検出されない

2 新しい RADIUS クライアントを追加するには、「**追加**」を選択します。「**RADIUS アカウント クライアントの追加**」ダイアログが表示されます。

メモ：このダイアログで変更を行うと、「**アカウント クライアント**」テーブル内で強調表示されているエントリに変更内容がそのまま反映されます。編集を完了しペインを閉じるには、ペインの外側を選択します。「**アカウント クライアント**」テーブル内のエントリを直接選択することにより、個々のフィールドを更新することもできます。



ヒント：パーティション処理が有効になっている場合、「**パーティションの選択**」ダイアログが「**RADIUS アカウント クライアントの追加**」ダイアログの上に表示されます。

1 新しいエージェントをどのパーティションに追加するかを指定します。
2 「**OK**」を選択します。

3 「**クライアント ホスト名または IP アドレス**」フィールドに、RADIUS クライアント ホストの名前または IP アドレスを入力します。

4 「**共有鍵**」フィールドと「**鍵の確認**」フィールドにクライアントの事前共有鍵を入力します。

5 「**RADIUS**」を選択します。

6 「**ユーザ名 (User-Name) 属性の形式**」から、ユーザ名ログインの形式を選択します。

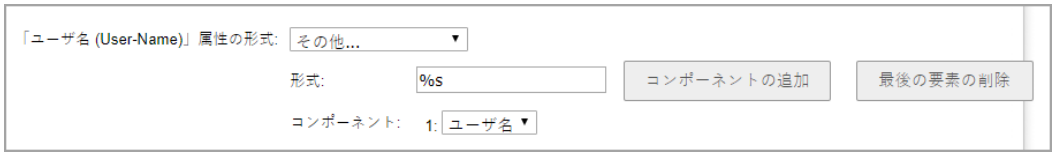
RADIUS アカウント メッセージで渡される "ユーザ名 (User-Name)" というコンテンツの形式は RADIUS アカウントで規定されたものではりません。そのため、クライアントから送信される形式を入力する必要があります。以下の標準的な形式の中から選択できます。

- **ユーザ名**
- **ドメイン\ユーザ名**
- **ドメイン/ユーザ名**
- **ユーザ名@ドメイン**
- **SonicWall Aventail (SonicWall SMA)**
- **その他** - 標準以外の形式

重要：上記の定義済みの形式は一般的な用途を想定しています。しかし、ネットワーク アクセス サーバから送信される形式と一致しない場合は、「**ユーザ名 (User-Name)**」属性の形式として「**その他**」を選択し、ユーザ定義の形式を入力してください。

7 選択した内容によって次の手順が異なります。

- 標準形式の場合は、「ステップ 8」へ進みます。
- 「**その他**」を選択した場合は、さらにオプションが表示され、属性に含まれるコンポーネントを設定できます。



  - **形式**
  - **コンポーネント**
  - **コンポーネントの追加**
  - **最後の要素の削除**

a 「**形式**」フィールドに、制限された scanf 形式の文字列を入力します。ここでは、`%s` または `%[...]` 命令で個々のコンポーネントを指定します。この命令は、ネットワーク アクセス機器 (NAS) が「**ユーザ名 (User-Name)**」属性で何を送信するかを装置に伝える働きをします。この形式は、RADIUS アカウント RFC では規定されていません。機器がこの属性で送信する内容に制約はないので、その内容は非常に多様なものとなる可能性があります。ここで設定する形式は、装置側で「**ユーザ名 (User-Name)**」属性をどのように解読してユーザ名、ドメイン、および DN あるいはそのいずれかを抽出するかを指定します。

> **ヒント**：「**その他**」を選択すると、これらのフィールドは、その前に選択されていた形式の文字列とコンポーネントに設定されます。そこで、まず、ネットワーク アクセス サーバから送信される内容に最も近い定義済み形式を選択してください。これを出発点として、ユーザ定義の形式を入力するとよいでしょう。次に、「**その他**」に変更してください。

b 「**コンポーネント**」から、以下のいずれかを選択します。

- **未使用**
- **ユーザ名** (既定値)
- **ドメイン**
- **DN**

「**形式**」フィールドに、制限された scanf 形式の文字列として入力するコンポーネントは、以下の 1 つ以上の項目で構成します。

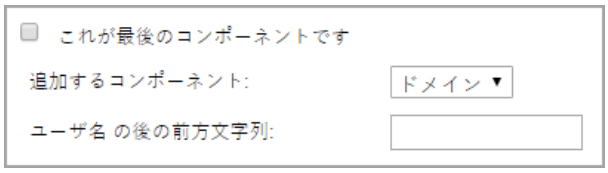
- ユーザ名
- ドメイン
- 完全修飾識別名 (DN)

> **メモ**：「**コンポーネント**」をダブルクリックすると、scanf 形式の文字列を入力する手順がツールチップで表示されます。

c 「**コンポーネント の追加**」を選択します。「**ユーザ名形式に対するコンポーネントの追加**」ダイアログが表示されます。

メモ：scanf 形式の意味がわかっていれば、「**コンポーネントの追加**」を使う代わりに「**形式**」フィールドを直接編集してもかまいません。

ヒント：%s は、空白が続くコンポーネントまたは最後のコンポーネントに使います。他の文字が続くコンポーネントには、%[^x]x を使います。例えば、「名前@ドメイン」という形式に対応する**形式**文字列は `%[^@]@%s` で表され、「**ユーザ-名前**」、「**ドメイン**」、「**未使用**」の 3 つのコンポーネントに対応します。



d 「**追加するコンポーネント:**」からコンポーネントの種類を選択します。

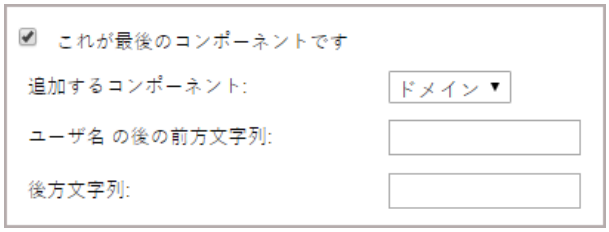
- **ユーザ名**
- **ドメイン** (既定)
- **DN**

e 「**ユーザ名の後の前方文字列**」フィールドに、エントリを区切るテキストを入力します。

f 各コンポーネントについて、「ステップ c」～「ステップ e」を繰り返します。

追加した最後のコンポーネントを削除するには、「**最後の要素の削除**」を選択します。

g これが最後のユーザ名コンポーネントの場合は、「**これが最後のコンポーネントです**」を選択します。別のオプションが表示されます。



h 「**追加**」を選択します。「**ユーザ名 (User-Name) 属性の形式に対するコンポーネントの追加**」ダイアログで、さらにオプションが表示されます。

i 「**ドメイン コンポーネントが無い場合**」から、次を選択します。

- **非ドメイン ユーザと想定する** - このオプションは、既定で選択されています。
- **LDAP でユーザ名を検索する**。

8 RADIUS アカウント クライアントは、ユーザのログイン中に、必要に応じて、中間報告メッセージを定期的に送信できます。クライアントがそれらのメッセージをだいたい定期的に送信している場合、SonicWall 装置はそれらのメッセージを監視することで、メッセージが送られてこなくなったときにユーザがログアウトしたものと見なすことができます。これは、ユーザのログアウト時に送信される RADIUS アカウント停止メッセージの見逃しを防ぐフォールバック メカニズムを提供します。

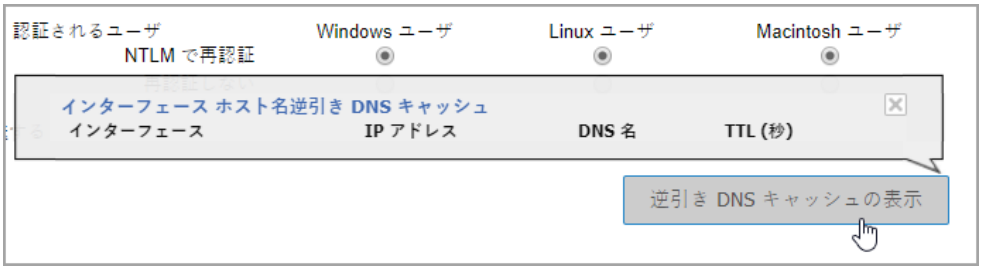
「**次の時間内に中間報告を受信しなかった場合、ユーザをログアウトする**」オプションをオンにします。

- **無効** - メッセージを送信させません。無効 - メッセージを送信させません。
- **有効** - 手動で**タイムアウト**時間を指定します。この**タイムアウト**は、RADIUS アカウント クライアントが中間報告メッセージを送信する間隔よりも大きな値に設定する必要があり、中間報告メッセージの破棄または見逃しに備えて、少なくとも 2 倍または 3 倍以上の値に設定してください。
- **自動** (このオプションは、既定で選択されています)。- Interim-Update メッセージが定期的に送信されているかどうかをファイアウォールに自動的に検知させ、定期的に送信されている場合は、「有効」時の指定に基づいてタイムアウトを自動的に設定します。

メモ：時間が経過してページの再読み込みが行われてもタイムアウトがゼロのままになっている場合は、送信中のメッセージが検出されず、タイムアウトが発生しないことを意味します。

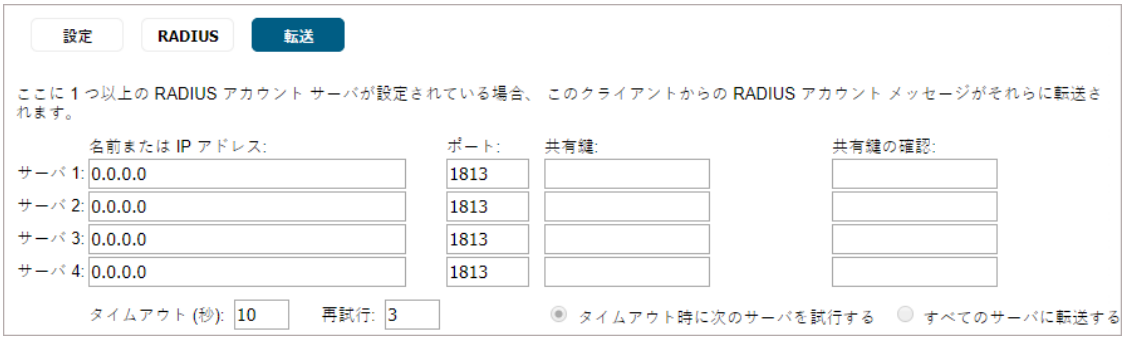
クライアントによるメッセージの送信頻度によっては、自動検出の完了までに相当な時間がかかる可能性があります。例えば、クライアントがメッセージの送信を 10 分毎に行っている場合、測定されたタイムアウトがここに表示されるまでに 30 分以上かかる可能性があります。

ヒント：「**情報の表示**」リンクを選択すると、ポップアップ ダイアログに進行状況が表示されます。



ヒント：自動検出を再実行するには、設定をいったん「**無効**」に変更してから「**自動**」に戻します。変更のたびに「**保存**」を選択してください。

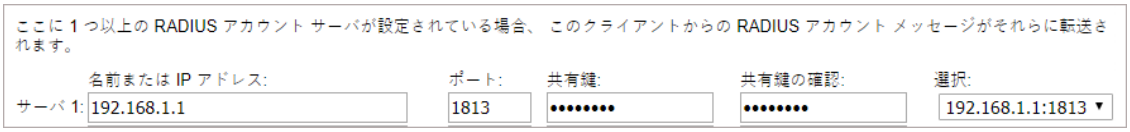
9 「**転送**」を選択します。



10 これらのフィールドで、最大 4 つの RADIUS アカウント サーバを入力できます。

- **名前または IP アドレス**
- **ポート** (既定値 **1813**)
- **共有鍵** (クライアントからのメッセージ転送先である RADIUS アカウント サーバで使用する)
- **共有鍵の確認**

この情報をサーバに対して入力すると、サーバごとに「**選択**」ドロップダウン メニューが表示されます。



11 サーバごとに、「**選択**」で次のどちらかを選択します。

- **転送なし**
- アカウント サーバの IP アドレス

複数のクライアントからの要求が同じアカウント サーバに転送される場合、そのサーバはいずれかのクライアントで 1 度設定されると、他のクライアントの「**選択**」からも選択できるようになります。選択したアカウント サーバの情報は、事前共有鍵を含め、このクライアントにすべてコピーされ、適用されます。

12 「**タイムアウト (秒)**」フィールドにタイムアウトする時間を秒単位で入力し、「**再試行**」フィールドに再試行回数を入力します。「**タイムアウト (秒)**」の既定値は **10** 秒で、「**再試行**」の既定値は **3** 回です。

どのユーザがログアウト済みであるかを確認するために、SonicWall セキュリティ装置は、複数のログイン中ユーザへの要求を SSO エージェントへの 1 つの要求メッセージで送信することによって、SSO エージェントをポーリングします。セキュリティ装置が「テスト」タブへの 1 つの要求メッセージで送信できるユーザ要求の数を設定するには、以下の手順を実行します。

13 このクライアントから RADIUS アカウント メッセージを転送する方法とし、次のどちらかを選択します。

- **タイムアウト時に次のサーバを試行する**
- **すべてのサーバに転送する**

14 「**保存**」を選択します。「**アカウント クライアント**」テーブルが更新されます。

15 「**一般設定**」を選択します。

16 「**RADIUS アカウントで SSO を有効にする**」 チェックボックスで、SSO または RADIUS アカウントを有効化します。このオプションは、既定では選択されています。

17 「ポート番号」フィールドでポートを指定します。既定のポートは **1813** です。

18 RADIUS アカウント ユーザに対するユーザ グループ メンバーシップを検索するメカニズムについては、次を選択します。

- **「SSO ユーザ」タブで選択されている方式を使用する。**(既定)
- **RADIUS アカウント要求の Filter-Id 属性を使用する。**

19 「**詳細設定**」を選択します。

20 装置に RADIUS アカウント メッセージを追跡させて開始/停止メッセージを見つける場合は、「**無線ローミングにより発生する開始/停止メッセージを予期します**」チェックボックスをオンにします。このオプションは、既定では選択されていません。

RADIUS アカウント クライアントは、開始/停止メッセージを送信してセキュリティ装置にユーザの接続/切断を通知します。それらのクライアントが無線アクセス ポイントであるか無線アクセス ポイントを使用している場合は、無線ユーザがアクセス ポイント間を移動する可能性があり、ユーザが新しいアクセス ポイントに接続して以前のアクセス ポイントから切断されるのに伴って、不要な開始/停止メッセージが発生することがあります。こうした移動に伴う開始/停止メッセージによって SSO 認証プロセスが妨害される可能性があります。本来であれば、停止メッセージはユーザ ログアウトの通知として処理されます。

このオプションを有効にすると、セキュリティ装置は RADIUS アカウント メッセージを追跡して開始/停止のシーケンスを探します。そしてそのシーケンスが見つかった場合、セキュリティ装置はそれらの停止メッセージがユーザ ログアウトの通知ではなく、ユーザの移動を示しているものと解釈します。

つまり、セキュリティ装置は、メッセージが次の条件を満たす場合に、開始/停止メッセージをアクセス ポイント間のローミングの切り替えによって発生したメッセージと見なします。

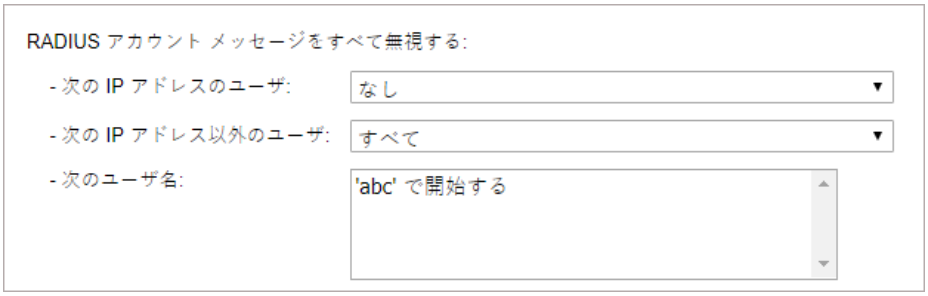
- 現在接続中のユーザが別のアクセス ポイントにいることを示す開始メッセージと共に以前のアクセス ポイントから停止メッセージを受信した (順番は問わない)。
- これらのメッセージは所定の時間内に一緒に発生した。

メモ：RADIUS アカウント メッセージが破棄されてから再送信されるまでの時間を見越して最大切り替え時間を決定してください。タイムアウトまでの時間に RADIUS アカウント クライアントの最大再試行回数を乗じた値を設定することをお勧めします。

21 セキュリティ装置にユーザの RADIUS アカウント メッセージを無視させるには、「**RADIUS アカウント メッセージをすべて無視する**」で次のようにします。

- 特定の IP アドレスにあるユーザのメッセージを無視する場合は、アドレス オブジェクトまたはアドレス グループを「**次の IP アドレスのユーザ**」から選択するか、新規のアドレス オブジェクトまたはアドレス グループを作成します。既定は「**なし**」です。
- 特定の IP アドレスにないユーザのメッセージを無視する場合は、アドレス オブジェクトまたはアドレス グループを「**次の IP アドレス以外のユーザ**」から選択するか、新規のアドレス オブジェクトまたはアドレス グループを作成します。既定は「**すべて**」です。
- 「次のユーザ名」で特定の名前を指定して、
  1) 「**追加**」を選択します。「**RADIUS アカウント ユーザ名除外の追加**」ダイアログが表示されます。

  2) 「次のユーザ名を無視する」ドロップダウン メニューから、次のどちらかを選択します。
     - **開始**
     - **終了**
  3) 「**次の文字列**」フィールドにユーザ名を入力します。
  4) 「**適用**」を選択します。リストにエントリが追加されます。



特定のエントリを編集するには、エントリを選択して「**編集**」を選択します。

特定のエントリを削除するには、エントリを選択して「**削除**」を選択します。す。

「サードパーティ API」ページ

SSO API は、ユーザ ログイン/ログアウト通知をファイアウォールに渡すためのサードパーティ デバイスまたはスクリプト用の XML/JSON ベースの REST API です。

サードパーティ API を設定するには:

1 「**サードパーティ API**」を選択します。

2 「**API クライアント**」テーブルで、「**追加**」を選択します。「**API クライアントの追加**」ダイアログが表示されます。

ヒント：パーティション処理が有効になっている場合、「**パーティションの選択**」ダイアログが「**RADIUS アカウント クライアントの追加**」ダイアログの上に表示されます。

1 新しいエージェントをどのパーティションに追加するかを指定します。
2 「**OK**」を選択します。

3 以下のオプションを設定します。

4 「**保存**」を選択します。クライアントは、「**API クライアント**」テーブルに追加されます。

5 「**一般設定**」を選択します。

6 「**SSO サードパーティ API を有効にする**」を選択します。このオプションは、既定では選択されていません。

7 API のユーザ ログイン/ログアウト通知の送信先を:

- HTTPS ウェブ管理に使用される TCP ポート番号と同じにする場合は、「**HTTPS 管理ポートを使用する**」を選択します。このオプションは、既定では選択されています。
- 専用の TCP ポート番号を個別に指定する場合は、「HTTPS 管理ポートを使用する」をオフにします。ポート番号を入力するフィールドが表示されます。

> **重要**：API クライアントの認証にクライアント証明書を使用する場合は、ポート番号を個別に指定する必要があります。

> **ヒント**：大量の API 要求がウェブ管理に悪影響を及ぼす可能性を防ぐため、大規模な導入環境では、専用の TCP ポート番号を個別に指定することを推奨します。

8 「**適用**」を選択します。

「テスト」ページ

1 設定したエージェントの設定をテストするには、「**テスト**」を選択します。

> **重要**：このページでテストを実行すると、それまでに行ったすべての変更が適用されます。

装置と SSO エージェントまたは TSA との接続をテストできます。また、ワークステーションにログインしたユーザを識別するための設定が SSO エージェントに対して適切に行われているかどうかもテストできます。

2 複数のエージェントを設定した場合は、テストする SSO エージェントまたは TSA を「**テストするエージェントの選択**」ドロップダウン メニューから選択します。このドロップダウン メニューでは、最初に SSOエージェントが示され、TSA は「**--ターミナル サーバ エージェント--**」の見出しの下で最後に示されます。

3 実行するテストの種別を選択します。

- **エージェントとの接続を確認**ラジオ ボタン - 認証エージェントとの通信をテストします。セキュリティ装置が SSO エージェントに接続できた場合、「**エージェントが利用可能**」というメッセージが表示されます。TSA のテスト時には、「**テスト状況**」フィールドにメッセージが表示され、「**エージェントから戻ってきた情報**」フィールドにバージョンおよびサーバの IP アドレスが表示されます。
- SSO エージェントのみの場合は、「**ユーザの確認**」を選択し、ワークステーションの IP アドレスを「**ワークステーションの IP アドレス**」フィールドに入力します。これで、ワー

クステーションにログインしているユーザを識別するための設定が、SSO エージェントに対して適切に行われているかどうかがテストされます。

ヒント：「**エージェントが応答しません**」または「**設定エラー**」というメッセージが表示された場合は、設定内容を確認してから、これらのテストをもう一度実行します。

4 「**テスト**」を選択します。

5 認証エージェントの設定がすべて完了したら、「**OK**」を選択します。

SSO 用の RADIUS アカウントの設定

シングル サインオン用の RADIUS アカウントは、「**ユーザ > 設定**」ページで設定します。

SSO 用の RADIUS アカウントを設定するには、以下の手順を実行します。

1 「**管理 | システム セットアップ > ユーザ > 設定**」ページが表示されます。

2 「**SSO の設定**」をクリックします。「**シングル サイン オン認証設定**」ダイアログが表示されます。

3 「**RADIUS アカウント**」タブを選択します。RADIUS アカウントを設定する手順については、「「RADIUS アカウンティング」ページ (194 ページ)」を参照してください。

4 「**適用**」を選択します。

LDAP の詳細設定

「**ユーザ**」ページの「**ユーザ グループ情報の検索に LDAP を使用する**」(「SonicOS で SonicWall SSO エージェントを使用するための設定 (180 ページ)」を参照) を選択した場合は、LDAP の設定を行う必要があります。

ユーザ グループ情報の検索に LDAP を使用するには、次の手順に従います。

1 「**管理 | システム セットアップ > ユーザ > 設定**」に移動します。

2 「**SSO の設定**」をクリックします。「**SSO 設定時の認証**」ダイアログが表示されます。

3 「**ユーザ**」を選択します。

4 「**ユーザ グループ情報の検索に LDAP を使用する**」オプションの横にある「**設定**」を選択します。「**LDAP 設定**」ダイアログが表示されます。

5 LDAP の設定については、「LDAP を使用するための SonicWall の設定 (162 ページ)」を参照してください。

9

認証パーティションの管理

トピック:

- 認証パーティション処理について (205 ページ)
  - ユーザ認証パーティション処理について (206 ページ)
  - サブパーティションについて (207 ページ)
  - パーティション間ユーザ ローミングについて (210 ページ)
  - 認証パーティションの選択について (211 ページ)
  - 複数 LDAP サーバの拡張サポートについて (213 ページ)
  - パーティション毎の DNS サーバと分割 DNS (214 ページ)
  - RADIUS 認証について (214 ページ)
  - パーティション処理以外の設定からのアップグレード (214 ページ)
- 認証パーティションおよびポリシーの設定 (215 ページ)
  - ユーザ/パーティションの表示とフィルタ (215 ページ)
  - パーティションの設定と管理 (217 ページ)
  - パーティション選択ポリシーの設定 (230 ページ)
  - 認証パーティション用のサーバ、エージェント、クライアントの設定 (235 ページ)

認証パーティション処理について

トピック:

- ユーザ認証パーティション処理について (206 ページ)
- サブパーティションについて (207 ページ)
- パーティション間ユーザ ローミングについて (210 ページ)
- 認証パーティションの選択について (211 ページ)
- 複数 LDAP サーバの拡張サポートについて (213 ページ)
- パーティション毎の DNS サーバと分割 DNS (214 ページ)
- パーティション処理以外の設定からのアップグレード (214 ページ)

ユーザ認証パーティション処理について

メモ：このセクションで使用されている用語の定義については、「用語と頭字語」テーブルを参照してください。

SonicWall セキュリティ装置は、相互接続されていない複数のドメインを管理する環境での LDAP、RADIUS、およびシングル サイン オン (SSO) 認証のメカニズムを備えています。このような環境では、特定のドメインのユーザを以下に示す特定の手段を用いて認証する必要があります。

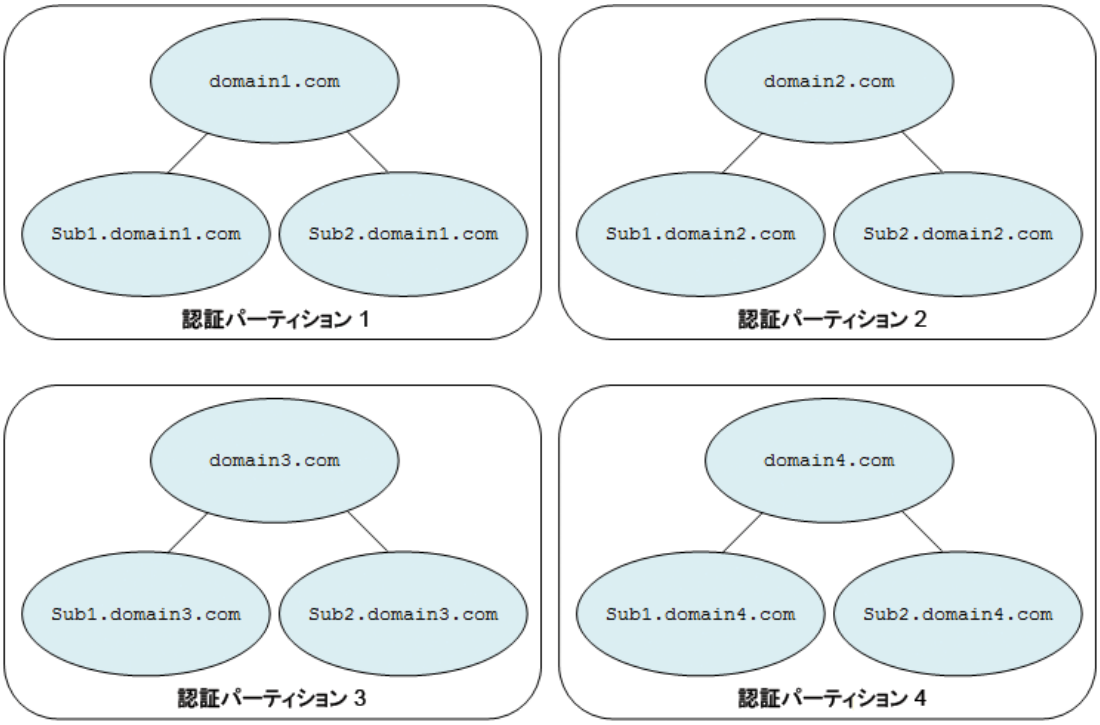
- そのドメインの LDAP/RADIUS サーバ
- そのドメインに置かれている SSO エージェント

こうした環境向けのメカニズムがユーザ認証パーティション処理です。これは次のことを意味します。

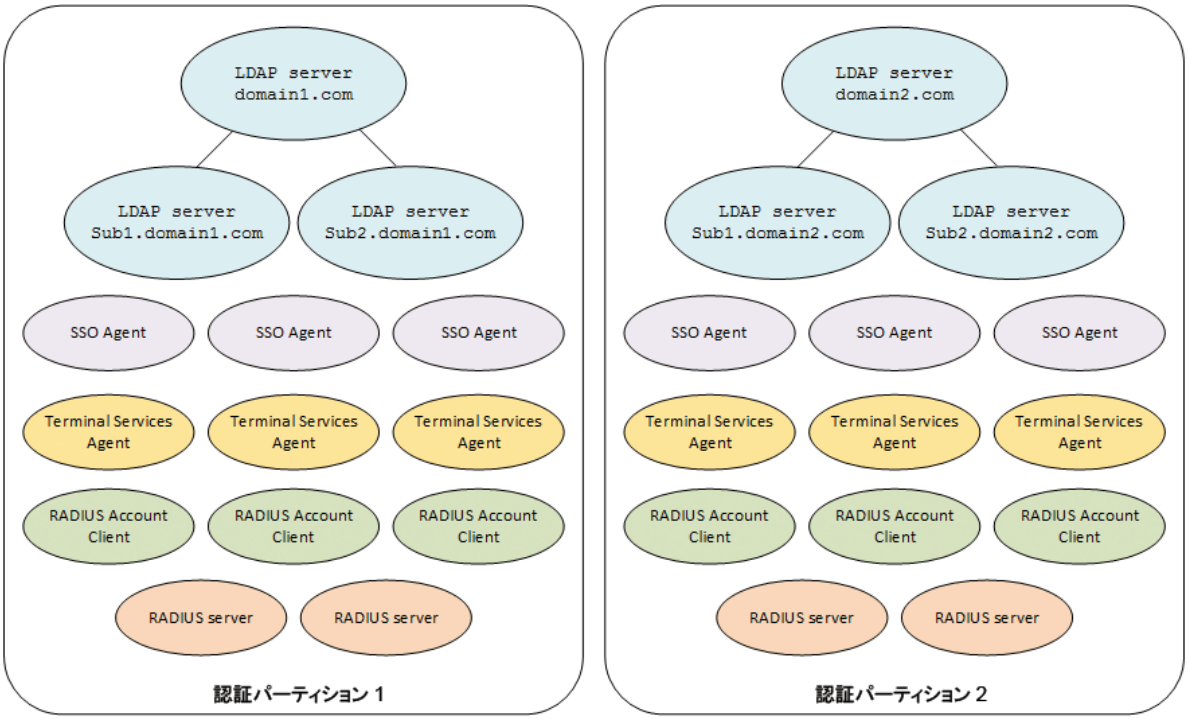
- まず、ネットワークをそれぞれ独自の認証サーバ/エージェント/クライアントを持つ別々のパーティションに分割すること。
- 次に、ユーザのいる認証パーティションに従って、各ユーザを関連する認証機器 (サーバ/エージェント/クライアント) に照らして認証すること。ユーザのパーティションは、次のいずれかの方法によって選択されます。
    - ユーザのドメイン名と、そのドメインに設定されているドメイン名との照合。
    - ユーザのドメイン名が使用できない場合は、パーティション選択ポリシーで設定されている物理的な場所に基づいた選択。

通常、認証パーティションは 1 つ以上のドメインに対応しています。例えば、Windows ドメインでは 1 つのパーティションが 1 つの Active Directory フォレストに対応しています。各パーティションは、個別の LDAP サーバ、RADIUS サーバ、SSO エージェント、ターミナル サービス エージェント (TSA) を持ちます。「認証パーティション」および「中央サイトとリモート サイトがあるインストール」を参照してください。

認証パーティション



パーティションの内容



用語と頭字語

認証パーティション	独自の認証サーバ/エージェント/クライアント (これらはネットワークの他の部分のものとは分離されています) を持つ、ネットワークの一部
DC	ドメイン コントローラ
LDAP	Lightweight Directory Access Protocol (LDAP) の使用
RADIUS	リモート認証ダイヤルイン ユーザ サービス
SSO	シングル サイン オン
TSA	ターミナル サービス エージェント

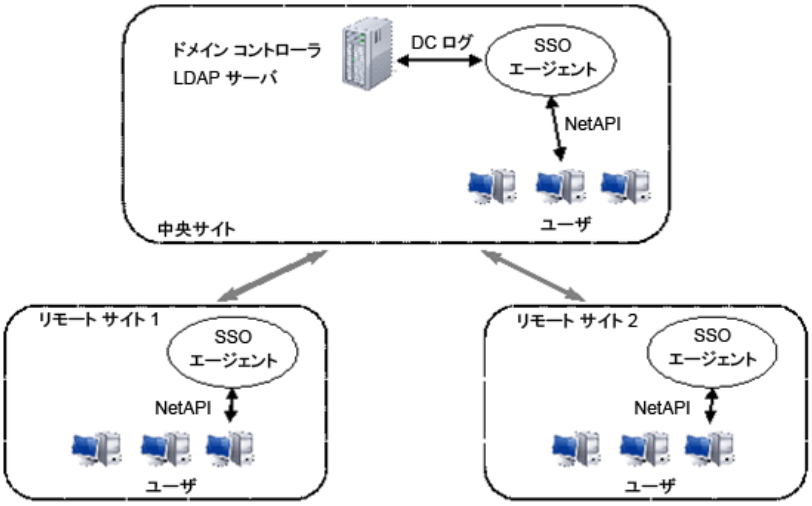
サブパーティションについて

認証パーティションでは、特定のユーザの認証に使用する LDAP サーバ、RADIUS サーバ、SSO エージェント、および TSA が選択されます。パーティションにこうしたサーバやエージェントを割り当てるだけでなく、インスタンスを用意することもできます。インスタンスでは、それらの一部をパーティション内の異なるサブセットのユーザにさらに割り当てる必要があります。サブパーティションを使用すると、パーティションの一部のユーザで特定のエージェントを使用する必要がある場合に、そうしたサブセットのユーザに特定のエージェントを割り当てることができます。認証パーティションが別のパーティションのサブパーティションとして設定されている場合は、最上位または親の認証パーティションのユーザ特有のエージェントを、サブパーティションに割り当てることができます。該当する場合にはサブパーティションのエージェントが使用されますが、親パーティションのサーバやエージェントも適宜使用できます。

例えば、中央サイトとリモート サイトを持つインストールで、ドメイン コントローラ (DC)/LDAP サーバが中央サイトに置かれているとします。ただし、アクセス ポリシーにより、中央サイトに置かれている SSO エージェントはリモート ユーザのコンピュータにアクセスできません。NetAPI または WMI に対応した SSO をこのトポロジで機能させるには、中央サイトに置かれているものに加えて、

リモートサイト毎に 1 つ以上の SSO エージェントを配置しておく必要があります (「中央サイトとリモート サイトがあるインストール」を参照してください)。NetAPI/WMI では、SSO エージェントがユーザのコンピュータと直接通信し、DC セキュリティ ログでのユーザ識別にはドメイン コントローラの SSO エージェントが使用されます。

中央サイトとリモート サイトがあるインストール



最上位パーティションのサブパーティション処理により、次の問題が解決されます。

- 個々の各サイトにある SSO エージェントがそのサイトにいるユーザの NetAPI または WMI 識別で使用されることを装置に知らせる。
- 全サイトにわたるすべてのユーザを対象とした DC ログ識別およびユーザ グループ検索で中央サイトにある SSO エージェントおよび LDAP サーバを使用する。

リモート サイトのそれぞれを中央サイトのサブパーティションとして設定し、各リモート サイトの SSO エージェントをサブパーティションに割り当てることができます。1 つ以上のパーティションを親パーティションのサブパーティションとして設定し、ユーザ サブセットの場所を定義している選択ポリシーをそれぞれで異なるものにすることができます。「中央サイトとリモート サイトがあるインストール」では、インストール全体が 1 つのパーティションであり、各リモート サイトはこのパーティション内のサブパーティションになっています。リモート サイトのユーザを識別するために該当するエージェントをサブパーティションから選択した後は、親パーティションの LDAP サーバによってユーザのグループ メンバーシップが検索されます。

以下に、サブパーティションの特別なケースを示します。

- LDAP サーバをサブパーティションに割り当てることができません。サブパーティションが、独自の LDAP サーバを持つサブドメインに対応している場合、それらのサーバを親パーティションに割り当てる必要があります。LDAP サーバはサブドメインに対する参照要求を管理します。
- RADIUS サーバの場合、サブパーティションは、そのサブパーティションに割り当てられているサーバと、親パーティションのサーバの両方ではなく、それらのどちらかを使用します。RADIUS サーバがサブパーティションに割り当てられている場合、RADIUS サーバはそのサブパーティション内に配置されているユーザのために使用されます。それ以外の場合は、親パーティションのサーバが使用されます。
- ドメイン コントローラのログからの読み取りではなく、NetAPI または WMI を使用している SSO エージェントでは、サブパーティションとその親の両方にエージェントが存在する場合は、サブパーティションの SSO エージェントのみがそのサブパーティションにいるユーザの NetAPI/WMI 識別で使用されます。サブパーティションの SSO エージェントは、ユーザのコンピュータへの

直接アクセスを必要とします。ドメイン コントローラ ログの読み取りは、親およびサブ パーティションの SSO エージェントによって行われます (サブパーティションの SSO エージェントがそのように設定されている場合)。

サブパーティションによるサーバ、エージェント、クライアントの操作

一般に、サブパーティションにいるユーザについては、そのサブパーティションに割り当てられているサーバ、エージェント、クライアントが使用されますが、親パーティションの特定のサーバ、エージェント、クライアントが使用されることもあります (「サブパーティションによるサーバ、エージェント、クライアントの使用」テーブルを参照してください)。

サブパーティションによるサーバ、エージェント、クライアントの使用

サーバ、エージェント、クライアント	説明
LDAP サーバ	サブパーティションではなく、最上位レベルのパーティションにのみ割り当て可能。 独自の LDAP サーバを持つサブドメインにサブパーティションが対応している場合、それらのサーバは親パーティションに割り当てる必要があり、LDAP の照会/参照メカニズムは要求をサブドメインのサーバに差し向けます。 ただし、独自の LDAP サーバを持つサブドメインにサブパーティションが対応している状況では、それらのサーバをサブパーティションに割り当てるほうが理にかなっていると思われるかもしれません。また、そうすることも可能です。サブパーティションに割り当てられているサーバは内部で親パーティションにリンクされています。
RADIUS サーバ	サブパーティションは、そのパーティションに割り当てられている RADIUS サーバと、親パーティションの RADIUS サーバの両方ではなく、それらのどちらかを使用します。RADIUS サーバがサブパーティションに割り当てられている場合、RADIUS サーバはそのサブパーティション内に配置されているユーザのために使用されます。それ以外の場合は、親パーティションのサーバが使用されます。
SSO エージェント	NetAPI または WMI の使用時には、ユーザ PC に直接アクセスできる場所にエージェントを配置する必要があり、DC (ドメイン コントローラ) からの読み取り時には、エージェントが DC にアクセスする必要があります。SSO エージェントは双方の作業を行うように設定することができます。 DC ログと NetAPI/WMI の両方を使用する場合は、どちらをどんな順序で使用するかが SonicWall セキュリティ装置によって制御されます。セキュリティ装置: 1 各 DC から読み取られた DC ログでのユーザの検索をエージェントに行わせます。 2 ユーザがログに見つかった場合は、NetAPI/WMI を試すために別のフォローアップ要求を行います。 サブパーティションを使用している場合、このメカニズムはサブパーティションにいるユーザを識別するために次のように動作します。 1 サブパーティションに割り当てられている SSO エージェントに DC ログが有効になっているものがある場合は、それらの SSO エージェントの DC ログでユーザを検索するためにそうしたエージェントに要求が送信されます。

サブパーティションによるサーバ、エージェント、クライアントの使用

サーバ、エージェント、クライアント	説明
	2 「ステップ 1」でユーザが識別されなかった場合、サブパーティションに割り当てられている SSO エージェントに DC ログが有効になっているものがあれば、それらの SSO エージェントの DC ログでユーザを検索するためにそうしたエージェントに要求が送信されます。 3 「ステップ 2」でユーザが識別されなかった場合、サブパーティションに割り当てられている SSO エージェントに NetAPI または WMI が有効になっているものがあれば、ユーザ識別するためにそうしたエージェントのいずれかに要求が送信されます。 **メモ**：親パーティションの SSO エージェントを介した NetAPI/WMI がサブパーティションにいるユーザに対して試行されることはありません。サブパーティションに割り当てられているエージェントに NetAPI または WMI が有効になっているものがない場合、認証は試行されません。
TSA と RADIUS アカウント クライアント	これらのエージェント/クライアントによる送信ユーザが割り当てられているパーティションは、ユーザ グループ検索で使用される LDAP サーバの選択のみに影響します。親パーティションの LDAP サーバはそのサブパーティションのすべてでも使用されるので、TSA および RADIUS アカウント クライアントはどちらにも割り当てることができます。唯一の違いは、それらのユーザにどのパーティションが表示されるかであり、ユーザの割り当てはユーザの物理的な場所に基づいて行われます。 **メモ**：これはドメインが提供されていない場合にのみ適用されます。

パーティション間ユーザ ローミングについて

あるパーティション内のドメインにログインしているユーザは、ネットワーク トポロジがログイン パーティションから自らのパーティションのドメイン サーバへのアクセスを許可するようにセットアップされている場合、異なるパーティションの物理ネットワークからのローミングや接続を行うことができます。SSO エージェントがこうした場合に使用されている場合、装置は、ユーザの物理的な場所に基づいて、ユーザのホーム パーティションのエージェントではなく、ローカル パーティションの SSO エージェントを選択します。

ローカル パーティションの SSO エージェントは、適切なドメイン コントローラからの読み取りを行わないため、ドメイン コントローラ ログからはローミング ユーザを識別できません。これらのエージェントは、適切な権限 (Windows のドメイン間信頼を必要とします) があれば、NetAPI または WMI を介してローミング ユーザを識別できます。そのため、セキュリティ装置がユーザ名を SSO エージェントから取得すると、セキュリティ装置は、指定されたドメインがあるパーティションを確認し、ユーザの物理的な場所に基づいて最初に選択されたパーティションのオーバーライドを許可します。

ローミング ユーザを識別してそのアクセス権限を設定する処理は、次のとおりです。

1 ドメイン 1 (パーティション 1 内にあります) にログインしているユーザがパーティション 2 内のサブネットからの接続を行います。このユーザのパーティションは元々パーティション 2 と記録されています。

2 パーティション 2 のエージェントがドメイン コントローラ ログの読み取りを行っている場合、こうしたログをチェックするための要求が最初に送信されます。これらの要求では、パーティション 2 のドメインにログインしていないユーザの発見に失敗します。

3 NetAPI 試行のための要求がパーティション 2 内の SSO エージェントに送信されます。エージェントはその試行を実施し、このユーザをドメイン 1 からのユーザとして識別します。

4 セキュリティ装置は、ドメイン 1 がパーティション 1 内にあることを確認し、そのユーザのパーティションをパーティション 1 に切り替えます。続いてセキュリティ装置は、パーティション 1 内の LDAP サーバを介してそのユーザのグループ メンバーシップを参照します。

認証パーティションの選択について

トピック:

- 選択ポリシー (211 ページ)
- リモート ユーザ (212 ページ)
- 装置によるユーザ ログインの通知 (212 ページ)
- ウェブ ユーザ ログイン (212 ページ)

選択ポリシー

ネットワーク トポロジは、SonicOS がネットワーク上の認証パーティション ユーザの場所をどのように特定するかに影響を与えることがあります。SonicOS には、ユーザのパーティションを特定および選択するためのオプションがいくつかあります。

選択に関するオプション

選択手段	それぞれの認証パーティション
IP アドレス	設定内のアドレス オブジェクト (ネットワーク、範囲、またはグループ) によって選択された一連の IP アドレスに対応します。
ネットワーク インターフェース	設定で選択されている 1 つ以上のインターフェース経由でアクセスされるネットワークに対応します。
ネットワーク ゾーン	設定で選択されている 1 つ以上のネットワーク ゾーンに対応します。
ユーザ名ドメイン コンポーネント	1 つ以上のドメインのメンバーであり、ログイン時にユーザによって与えられたドメイン名との照合によって選択されます。このオプションでは、ユーザが修飾名 (`domain\user`、`user@domain.com` など) を使ってログインする必要があります。 ドメイン名が与えられた場合、このオプションは上記の場所に基づいたオプションよりも優先されます。 このオプションは、GVC、L2TP、および SSL VPN クライアント ユーザの認証で使用する必要があります (「リモート ユーザ (212 ページ)」を参照してください)。 **メモ**：SSO エージェント認証では、場所に基づいたオプションの 1 つを使用する必要があります。SonicWall セキュリティ装置は、使用する SSO エージェントの選択処理の開始時にパーティションを導き出す必要があり、その時点ではまだユーザのログイン名がセキュリティ装置にはわからないためです (「パーティション間ユーザ ローミングについて (210 ページ)」を参照してください)。

これらのオプションは、別の選択ポリシー セットとして設定されており、そうしたパーティションの選択方法を定義するために、パーティション 1 つにつき 1 つ以上のポリシーが設定されます。ユーザ認証の際、ドメインが与えられない場合、パーティションの選択は、アクセス ルールの照合と非常によく似た形で、ゾーン、インターフェース、および IP アドレスを設定済みポリシーと照合することで行われます。既定のパーティションを指定する既定の選択ポリシーは、明示的に設定されてい

るポリシーに一致しないすべての要素に対応できるものになっています。既定のパーティションの名前は最初「Default」になっていますが、これは変更できます。また、既定の選択ポリシーを別のパーティションに対して設定することもできます。その場合は、自動作成された「Default」を後で削除できます。

リモート ユーザ

GVC/L2TP クライアントおよび SSL VPN ユーザで使用する認証パーティションの選択は、異なる方法で処理されます。こうしたリモート ユーザによる接続は認証パーティションに対して行われ、認証パーティションからのものではないからです。セキュリティ装置は、こうしたユーザのユーザ グループ メンバーシップを参照するための適切な LDAP サーバを選択するために、それらのユーザの認証パーティションを把握し、さらにそのサーバから、そうしたユーザがアクセスできるサブネットを知る必要があります。リモート ユーザを認証するためのオプションとして次の 2 つがあります。

- ユーザ名ドメイン コンポーネントによる選択を使用し、ドメインが含まれている修飾名の提供をリモート ユーザに要求します。
- 複数の WAN インターフェースや WAN ゾーンを用意し、各認証パーティションのユーザに異なるパブリック IP アドレスに接続させます。その後、リモート ユーザが経由する WAN インターフェースまたはゾーンは、認証パーティションを選択するために使用され、リモート ユーザによる修飾ユーザ名の提供は必要ありません。

  メモ：GVC/L2TP ユーザの場合、別の WAN ゾーンがあれば、ゾーン毎に異なるグループ VPN ポリシーを使用できます。これにより、適切な認証ゾーンへのより安全なアクセスを適用できる可能性があります。

複数の WAN インターフェースが存在する場合、各 WAN インターフェース経由でのリモート アクセスに対してパーティションを選択するためのパーティション選択ポリシーを設定できます。WAN インターフェースが 1 つしかない場合は、提供されたユーザ名から導き出せないときにリモート アクセス用の既定のパーティションを選択するための特別な選択ポリシーを設定できます。

メモ：そうした選択ポリシーが設定されていない場合、リモート アクセス ユーザは、それらのユーザを認証するサーバが、既定で選択されているパーティションに割り当てられていない限り、修飾ユーザ名を提供する必要があります。

装置によるユーザ ログインの通知

SonicWall セキュリティ装置がエージェント/クライアントによってユーザ ログインの通知を受けたものの、そうしたユーザの識別要求を送信しない場合 (ターミナル サービス、RADIUS アカウント、DC ログを読み取る SSO エージェントからのログイン通知など)、セキュリティ装置は、SSO エージェントに要求を送信するために行うような、エージェント/クライアントの選択のために認証パーティションを知る必要がありません。ただし、適切な LDAP サーバを選択してユーザのユーザ グループ メンバーシップを参照するために、セキュリティ装置はこうしたユーザの認証パーティションを把握する必要があります。そうした選択は、ユーザ名のドメイン コンポーネント (存在する場合) から行われるか、認証パーティションへのそのような各エージェント/クライアントの手動割り当てによって行われます。

ウェブ ユーザ ログイン

SonicWall セキュリティ装置のウェブ ログイン ポータルを介してログインするユーザは、そのユーザがいる場所に関係なく、任意のアカウント名を使用できると考えられます。通常、認証パーティションはユーザがどこからログインしているかに基づいて選択されますが (「選択ポリシー (211 ページ)」を参照してください)、ユーザがドメインの含まれているユーザ名を提供した場合は、そのパーティ

ションをオーバーライドできます。そのためには、ドメインが含まれている修飾されたユーザ名を使ってログインして認証パーティションを選択します。

CLI ログイン

ユーザがビルトイン管理者アカウントを使用して CLI からログインすると、常にローカルで認証されるため、パーティション処理は重要ではありません。しかし、LDAP または RADIUS によって認証される追加の管理者アカウントが使用されると、その認証を行うサーバを選択するためにパーティションを知る必要があります。この場合は次の 3 つのケースがあります。

コンソール ポートでのログイン	パーティションを導き出すための IP アドレスがないので、そうした IP アドレスが必要な場合、ユーザは修飾ユーザ名を使ってログインする必要があります。
ファイアウォールの内側からのローカル SSH 接続	ユーザが置かれている認証パーティションは、「選択ポリシー (211 ページ)」に記されているように、SSH 接続の送信元 IP アドレスによって選択されます。
ファイアウォールの外側からのリモート SSH 接続	パーティションの選択はユーザの場所には基づいていませんが、必要に応じて、リモート クライアント ユーザのように、接続先の WAN インターフェースに従ってパーティションが選択されるようにすることが可能です。「選択ポリシー (211 ページ)」を参照してください。

ユーザ名ドメイン コンポーネントによる選択が設定されている場合 (「選択ポリシー (211 ページ)」を参照してください)、ユーザはどのケースでも、認証パーティションが選択される基準となるドメインが含まれている修飾ユーザ名を使ってログインすることで、その設定をオーバーライドできます。特別な選択ポリシーを設定して、提供されたユーザ名からパーティションを導き出せないときにはコンソール ポート ログイン用の既定のパーティションを選択することもできます。

メモ：選択ポリシーが設定されていない場合、ユーザを認証するサーバが既定で選択されているパーティションに割り当てられていない限り、ユーザは修飾ユーザ名を提供してコンソール ポート上でのログインを行う必要があります。

パーティション毎のユーザ認証設定

いくつかのケースでは、ユーザ認証をパーティション毎に異なる形で管理するような設定が必要になることがあります。例えば、あるパーティションには RADIUS サーバしかなく、別のパーティションには LDAP サーバしかない場合、ユーザ認証のために、最初のパーティションでは RADIUS を、もう一方のパーティションでは LDAP を選択する必要があります。

既定では、このようなすべての設定は、グローバルに適用されており、ユーザ認証方式とシングル サイン オン方式に限定されています。これらの設定は、最上位レベルのパーティションに対してのみ設定されます。サブパーティションには、その親パーティションの認証設定が適用されます。

複数 LDAP サーバの拡張サポートについて

パーティション処理には複数の LDAP サーバが必要です。複数のプライマリ LDAP サーバを設定できます (各認証パーティションに 1 つずつ)。また、それぞれに対する追加サーバのリストも設定できます。複数 LDAP サーバとその設定方法の詳細については、「複数 LDAP サーバの拡張サポートについて (174 ページ)」を参照してください。

パーティション毎の DNS サーバと分割 DNS

認証パーティションの有無に関係なく、通常はドメイン独自の DNS サーバを使用してそのドメイン内にある機器の名前を解決する必要があります。また、ときには異なる外部 DNS サーバを使用した外部ホスト名の解決が必要になることもあります。ただし、複数の認証パーティションでは通常、異なる DNS サーバを使用して各種パーティション内のホスト名を解決する必要があります。

分割 DNS 機能を持つ DNS プロキシでは、さまざまなドメイン名が関連付けられた各種 DNS サーバの設定が可能です。この機能は、DNS プロキシとは分離されているので、例えば、認証パーティション処理に対応した関連性のない複数のドメインで、DNS プロキシを有効にする必要なしにドメイン内機器の名前を解決するために、セキュリティ装置による直接使用が可能です。分割 DNS の詳細については、「認証パーティションの管理 (205 ページ)」を参照してください。

RADIUS 認証について

RADIUS 認証に関しては、いくつか追加の検討事項があります。LDAP の場合とは異なり、SonicWall セキュリティ装置によってユーザのドメインが導き出されるという保証も、ユーザ グループのドメインが RADIUS 属性で返されるという保証もありません。そのため、セキュリティ装置は適切なドメイン ユーザ オブジェクトやユーザ グループ オブジェクトを選択するためにドメインを見つけることができます。セキュリティ装置は、以下を試すことで RADIUS 認証に関するユーザのドメインを学習します。

1. ユーザのログイン時に、ドメインが含まれている修飾ユーザ名をユーザに提供させます。RADIUS サーバが RADIUS 属性 (Filter-ID または SonicWall ベンダー特有のもの) でユーザ グループを返す場合は、そのドメインが含まれているグループの完全修飾名を提供する形でそれらを返すように設定します。
2. RADIUS によるユーザの認証後は、ユーザ グループ参照のために LDAP を使用します (こちらが優先される方法です)。この場合、ユーザがドメインをユーザ名と共に提供しなくても、ドメインを LDAP 検索から学習してユーザ グループを見つけ出すことができます。
3. これらのどちらかに失敗しても、ドメインは、ユーザがログインする際の認証パーティションから、また物理的に認証パーティションに配置されている IP アドレスから検索できますが、パーティション毎にドメインが 1 つしか存在しない場合は、この方法によってユーザのドメインを確実に提供できます。そのため、この方法を使用するには、すべてのサブドメインに個別のサブパーティションを持たせる必要があります。

   メモ：この方法は、クロスドメインのユーザ グループ メンバーシップでは機能しません。

まとめると、RADIUS 認証での最善のオプションは、ユーザ グループ検索のために LDAP を使用することになります。これが不可能な場合 (LDAP サーバが存在しない場合など)、最善のオプションは、RADIUS サーバに修飾ユーザ グループ名を RADIUS 属性に含めて返させることです。

RADIUS から返されるユーザ グループのドメインを導き出すために、これらのいずれも使用できない場合は、ユーザ/ユーザ グループ オブジェクトをどのドメインでも一致するように設定する必要があります。

パーティション処理以外の設定からのアップグレード

認証パーティション処理がない既存の設定から開始した場合、パーティション処理が有効になっている場合:

- **既定**という名前の単一認証パーティションが、そのパーティション内にある既存のすべてのサーバ、エージェント、クライアントに対して作成されています。
- **既定**パーティションをすべてに対する既定パーティションとして選択するために、既定パーティション選択ポリシーが 1 つだけ設定されています。

これをもとにして、新しいパーティションを追加できます。また、関連するサーバ、エージェントおよびクライアントを容易に既定のパーティションから新しいパーティションに移したり、新しいものを追加したりできます。

認証パーティションおよびポリシーの設定

「**ユーザ > パーティション**」ページでは、認証パーティションのリストや、そうしたパーティションを選択するポリシーのリストを作成できます。各パーティションで、以下の設定を行うことができます。

- 認証パーティションの名前 (例えば、認証パーティションに相当するドメインまたはフォレストの名前)。
- パーティションに含まれるドメイン。
- ユーザに対する認証パーティションの選択方法 (例えば、個別のパーティション選択ポリシーとして設定されているもの)。

認証パーティションとパーティション選択ポリシーを設定する前に、「**監視 > 現在の状況 > ユーザ セッション > 使用中のユーザ**」ページからパーティション内でのユーザの場所を決定できます。

認証パーティションが設定されている場合は、サーバ、エージェント、またはクライアントの追加/編集時に認証パーティションを選択できるように、さまざまなサーバ/エージェント/クライアント設定に選択対象が追加されます。サーバ、エージェント、およびクライアントは、「**管理 | システム セットアップ > ユーザ > 設定**」ページで設定します。

トピック:

- ユーザ/パーティションの表示とフィルタ (215 ページ)
- パーティションの設定と管理 (217 ページ)
- パーティション選択ポリシーの設定 (230 ページ)
- 認証パーティション用のサーバ、エージェント、クライアントの設定 (235 ページ)

ユーザ/パーティションの表示とフィルタ

「**監視 | ユーザ セッション > 使用中のユーザ**」ページには、各ユーザのいるパーティションが表示されます。

メモ：このページの詳細については、ご利用の SonicWall セキュリティ装置の『*SonicOS 6.5 監視*』を参照してください。

トピック:

- ユーザ情報の表示 (216 ページ)
- ユーザのフィルタ (216 ページ)

ユーザ情報の表示

多様なカテゴリ別のユーザ数を表示できます。

- アクティブ/非アクティブ
- 識別方法別の SSO ユーザ数
- クライアント種別毎のクライアント ユーザ数
- ウェブ ユーザ数
- SSL VPN ポータル ユーザ数

この情報を表示するには、「**現在のユーザ**」テーブルのすぐ下にある**統計**アイコンを選択します。「**ユーザ数**」ポップアップ ダイアログが表示されます。

ユーザのフィルタ

「**フィルタ**」フィールドを使用すると、パーティションのフィルタ処理が可能になり、選択したパーティション内のユーザのみを表示できます。1 つ以上のユーザ名、ドメイン、IP アドレス、ユーザ種別の全体または一部を指定して、ユーザを検索します。ユーザを除外するには、エントリの先頭に感嘆符 (!) を付けます。文字列を組み合わせると、次のようなマッチングが行われます。

- リストされているエントリのいずれかと一致させるには、エントリをカンマで区切ります。"a,b" には a と b のどちらかに一致するユーザが含まれます。
- リストされているエントリのすべてと一致させるには、エントリをセミコロン (;) で区切ります。"a;b" には a と b の両方に一致するユーザが含まれます。

ターミナル サーバ ユーザを検索するには、`user-num=<`*ユーザ番号*`>` と入力します。`type` フィルタは「**種別/モード**」列のテキスト (マウス ポインタをその列に重ねたときに表示されるすべてのものが含まれます) に一致します。IPv6 アドレスはサポートされていますが、完全一致検索のみが可能です。例えば、`ip=2012::1`、`!ip=2012::1`、または「フィルタの例」テーブルに示されているその他のエントリの組み合わせにあるようなものです。

フィルタの例

```
name=bob                    name=bob,john,sue          domain=mydomain
ip=192.1.1.1                ip=192.1.1.1,192.1.1.2     ip=192.1.1.0/24
type=config mode            type=sso,web               type=sso;netapi
type=sso;from logs on domain controller 192.1.1.10
partition=somePartition     group=Trusted Users
name=bob;ip=192.1.1.1(名前とIP アドレスの両方を照合する場合)
!name=bob !ip=192.1.1.1 (ユーザを除外する場合)
```

単純な文字列を使用することもできます。以下に例を示します。`bob 192.1.1.1 mydomain`

パーティションの設定と管理

トピック:

- 「ユーザ > パーティション」ページ (217 ページ)
- 認証パーティションの有効化/無効化 (222 ページ)
- パーティションとサブパーティションの追加 (222 ページ)
- パーティションとサブパーティションの削除 (224 ページ)
- サーバ、エージェント、クライアントの割り当て (226 ページ)
- パーティションの編集 (228 ページ)

「ユーザ > パーティション」ページ

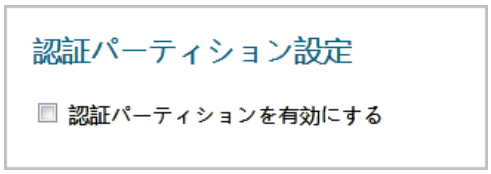
「管理 | システム セットアップ > ユーザ > パーティション」ページには次の 3 つのセクションがあります。

- 「認証パーティション設定」セクション (218 ページ)

- 「認証パーティション」セクション (218 ページ)
- 「パーティション選択ポリシー」セクション (221 ページ)

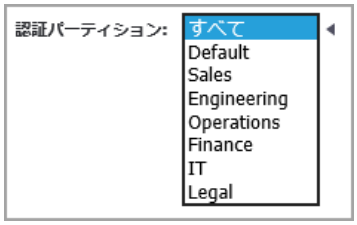
「認証パーティション設定」セクション

このセクションは認証パーティション処理を有効または無効にします。認証パーティション処理が無効になっている場合、その他のセクションは表示されません。



認証パーティション処理が有効になっている場合、2 つのセクション、「**認証パーティション**」および「**認証選択ポリシー**」も表示されます。

また、パーティション処理が有効になっていると、「**認証パーティション**」ドロップダウン メニューがページの上部に表示されます。このメニューでは、「**管理 | システム セットアップ > ユーザ > 設定**」および「**管理 | システム セットアップ > ユーザ > ローカル ユーザとグループ**」ページの設定も適用されるパーティションを選択できます。既定は「**すべて**」です。つまり、設定がすべてのパーティションに適用されます。

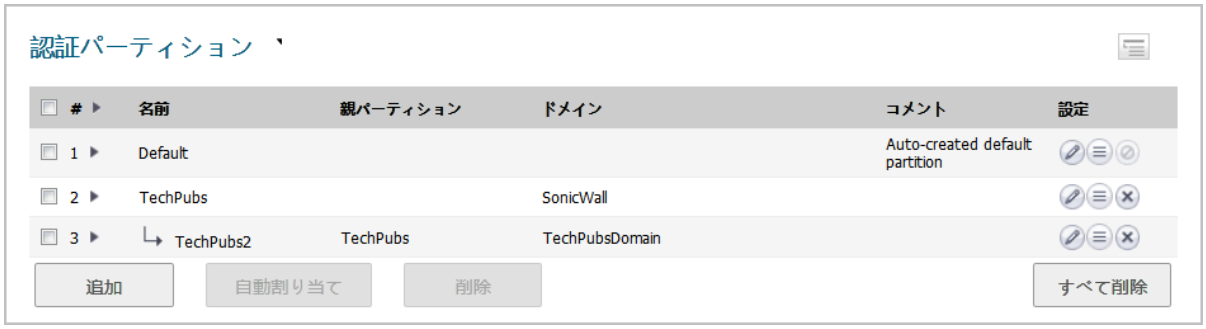


「認証パーティション」セクション

メモ：このセクションは、認証パーティション処理が有効になっている場合にのみ表示されます。

このセクションには、認証パーティションのテーブルが表示され、パーティションの作成、編集、削除、管理を行うことができます。ここで設定するパーティションにより、どのユーザでどの認証サーバが使用されるかが制御されます。

パーティションのツリーを展開すると、そのパーティションに割り当てられているサーバ、エージェント、クライアントを表示できます。



サブパーティションのグループ化 アイコン	親の認証パーティションによるサブパーティションのグループ化、またはサブパーティションのグループ化解除と、最上位レベルのパーティションによるサブパーティションの並べ替えとの切り替えを行います。 **メモ**：グループ化されたサブパーティションは、親パーティションのすぐ後に表示され、**リンク** ↳ アイコンによってサブパーティションであることがわかります。
選択用チェックボックス	テーブルにある 1 つ以上のパーティションやサブパーティションを選択できます。テーブル見出しにあるチェックボックスをオンにすると、「**Default**」パーティションを除くすべてのエントリが選択されます。
名前	認証パーティションの名前を指定します。サブパーティションは、名前の前に**リンク** ↳ アイコンが表示されます。
親パーティション	サブパーティションに対する親の認証パーティションを指定します。親パーティションの場合、この列は空欄になります。
ドメイン	パーティションまたはサブパーティションが属するドメインを指定します。「**Default**」パーティションの場合、この列は空欄になります。
コメント	パーティションの追加時に入力したコメントが表示されます。「**Default**」パーティションに対するコメントは、「**自動作成された既定パーティション**」です。
設定	パーティションの**編集**アイコン、**選択** アイコン、**削除**アイコンが表示されます。 **メモ**：「**Default**」パーティションでは、**編集**アイコンと**削除**アイコンがグレーアウトされています。
追加	認証パーティションまたはサブパーティションを追加するための「**認証パーティションの追加**」ポップアップ ダイアログを表示します。
自動割り当て	まだ割り当てられていないすべての LDAP サーバ、RADIUS サーバ、SSO エージェント、TSA、および RADIUS アカウント クライアントをその IP アドレスまたはホスト名に基づいて、関連するパーティションに自動的に割り当てます。 **メモ**：「**自動割り当て**」および「**削除**」は、パーティションまたはサブパーティションが少なくとも 1 つは選択されていないと、グレーアウトされます。
削除	選択されている認証パーティションまたはサブパーティションを削除します。 **メモ**：「**Default**」パーティションは削除できません。
すべて削除	「**Default**」パーティションを除くすべてのパーティションおよびサブパーティションをテーブルから削除します。

このテーブルには、認証パーティションが必ず 1 つは存在します。それは自動生成された「**Default**」パーティションです。このパーティションは削除できません。ただし、既定パーティションを編集して、サーバ、エージェント、クライアントや、サブパーティションを選択することは可能です。認証パーティションを無効にした場合、すべての LDAP サーバ、SSO エージェント、TSA、および RADIUS アカウント クライアントは「**Default**」パーティションに割り当て直されます。これらは、認証パーティションを再び有効化する際に割り当て直す必要があります。なお、RADIUS サーバは影響を受けないので、割り当てられたパーティションにとどまります。

ツリーの展開

認証パーティションのツリーを展開すると、そのパーティションに割り当てられているサーバ、クライアント、エージェントが表示されます。

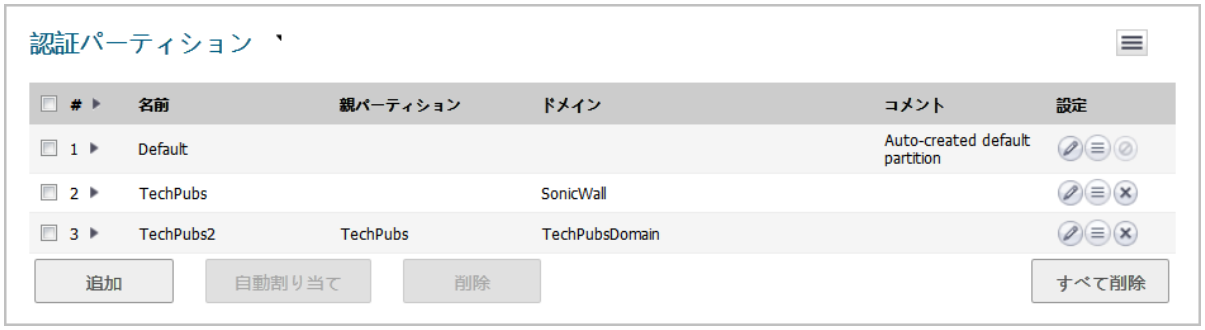
以下のツリーを展開できます。

- すべてのテーブル エントリ - 見出しのチェックボックスの横にある三角形をクリックします。
- 1 つ以上のテーブルエントリ - それぞれの**展開**アイコンをクリックします。

階層の表示

既定では、サブパーティションが親パーティションの下に表示され、サブパーティションの名前の前には**リンク** アイコンが付いています。

グループ アイコンを選択すると、親パーティションと同じレベルにあるサブパーティションを表示できます。



「パーティション選択ポリシー」セクション

メモ：このセクションは、認証パーティション処理が有効になっている場合にのみ表示されます。

このセクションには、認証パーティションの選択に影響を与えるポリシーのテーブルが表示され、ポリシーの作成、削除、編集を行ったり、作成した任意のポリシーの優先順位を変更したりできます。こうしたポリシーにより、認証されるユーザの物理的な場所に基づいて「**認証パーティション**」テーブル内のパーティションが選択されます。選択パーティション内のドメインとの照合が利用できないドメイン名を持つユーザを認証する際、そのユーザのパーティションはこうしたポリシーによって設定されたユーザの物理的な場所に基づいて選択されます。こうした選択ポリシーは、認証機器をその物理的な場所に基づいてパーティションに自動的に割り当てるためにも使用されます。

既定パーティションに対する既定の選択ポリシーは、削除することも、優先度を変更することもできません。このポリシーは常に最低の優先順位となります。

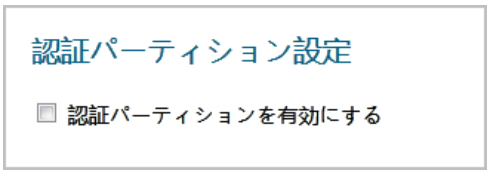
選択用チェックボックス	テーブル内の 1 つ以上のエントリを選択できます。テーブル見出しにあるチェックボックスをオンにすると、「**既定**」選択ポリシーのエントリを除くすべてのエントリが選択されます。
優先順位	割り当てた優先順位に従ってパーティション選択ポリシーに順序を付けます。**優先順位の矢印** をクリックすると、「**選択ポリシー優先順位の変更**」ポップアップ ダイアログが表示されます。「**既定**」選択ポリシーの優先順位は変更できません。このポリシーは常に最低の優先順位となります。
ゾーン	パーティション選択ポリシーに割り当てられているゾーンが表示されます。
インターフェース	認証パーティション選択ポリシーに割り当てられているインターフェースが表示されます。
パーティション	選択ポリシーが適用される認証パーティションが表示されます。
コメント	選択ポリシーの作成または編集時に入力したコメントがあれば表示されます。「Default」パーティションの選択ポリシーには、「**自動作成された既定ポリシー**」というコメントが付いています。
設定	**編集**アイコンと**削除**アイコンが表示されます。既定のポリシーではグレーアウトされています。
追加	認証パーティションまたはサブパーティション用の選択ポリシーを追加するための「**パーティション選択ポリシーを追加する**」ポップアップ ダイアログを表示します。
削除	選択されているポリシーを削除します。 **メモ**：「Default」パーティション用のポリシーは削除できません。ポリシーが 1 つも選択されていない場合、「**削除**」はグレーアウトされています。
すべて削除	「Default」パーティション用のポリシーを除くすべてのポリシーをテーブルから削除します。

このテーブルには、選択ポリシーが必ず 1 つは存在します。「Default」パーティション用の自動生成された既定のポリシーです。このポリシーは、削除、優先順位の変更、編集ができません。ただし、適用されるパーティションの選択は可能です。

認証パーティションの有効化/無効化

パーティション処理を有効にするには、以下の手順に従います。

1 「**ユーザ > パーティション**」ページに移動します。



2 「**認証パーティション設定**」セクションで、「**認証パーティションを有効にする**」を選択します。「**認証パーティション**」および「**パーティション選択ポリシー**」セクションが表示されます。

パーティション処理を無効にするには、以下の手順に従います。

1 「**ユーザ > パーティション**」ページに移動します。

2 「**認証パーティション設定**」セクションで、「**認証パーティションを有効にする**」チェックボックスをオフにします。「**認証パーティション**」および「**パーティション選択ポリシー**」セクションが表示されなくなります。

重要：認証パーティション処理を無効にした場合、パーティション処理されているすべての LDAP サーバ、SSO エージェント、TSA、および RADIUS アカウント クライアントは「**Default**」認証パーティションに移されます。RADIUS サーバは影響を受けず、設定されている認証パーティション内にとどまります。その後、認証パーティション処理を有効にする場合は、他のすべてのサーバ、エージェント、クライアントを設定し直す必要があります。

パーティションとサブパーティションの追加

パーティションを追加するには、以下の手順に従います。

1 「**ユーザ > パーティション**」ページに移動します。

2 「**認証パーティション**」セクションで、「**追加**」を選択します。「**認証パーティションの追加**」ポップアップ ダイアログが表示されます。

3 「**パーティション名**」フィールドに、意味のあるわかいやすい名前を入力します。名前は 1 ～ 32 文字の英数字で指定します。

4 「**パーティション種別**」で、認証パーティションを次のどれにするかを選択します。

- **最上位レベルのパーティション**。「ステップ 6」に進みます。
- **サブパーティション**にする場合は、「**親パーティション**」ドロップダウン メニューが表示されます。

5 このドロップダウン メニューから親パーティションを選択します。既定のパーティションは「**Default**」です。

> **ヒント**：インストールに複数のパーティションが存在しない場合は、サブパーティションを「**Default**」パーティションのサブパーティションとして作成します。

6 「**ドメイン**」リストで、「**追加**」を選択します。「**ドメインの追加**」ポップアップ ダイアログが表示されます。

7 ドメイン名を入力します。

8 「**OK**」を選択します。

9 追加するドメイン毎に「ステップ 6」～「ステップ 8」を繰り返します。

10 必要に応じて、「**コメント**」フィールドにコメントを入力します。

11 「**保存**」を選択します。パーティションやサブパーティションは「**認証パーティション**」テーブルに追加されます。サブパーティションは、その親パーティションのすぐ後に配置され、**リンク** アイコンによってサブパーティションであることがわかります。

パーティションとサブパーティションの削除

メモ：このセクションでは、パーティションという語がパーティションとサブパーティションの両方を指します。

1 つのパーティション、複数のパーティション、またはすべてのパーティションを削除できます。1 つのパーティションを削除した場合、そのサーバ、エージェント、クライアントは「**Default**」パーティションへの再割り当てが行われます。

メモ：「**Default**」パーティションは削除できません。

トピック:

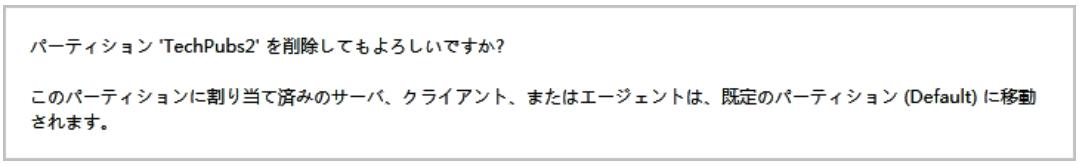
- 単一パーティションの削除 (224 ページ)
- 複数パーティションの削除 (225 ページ)
- すべてのパーティションの削除 (既定を除く) (225 ページ)

単一パーティションの削除

パーティションを 1 つ削除するには、以下の手順に従います。

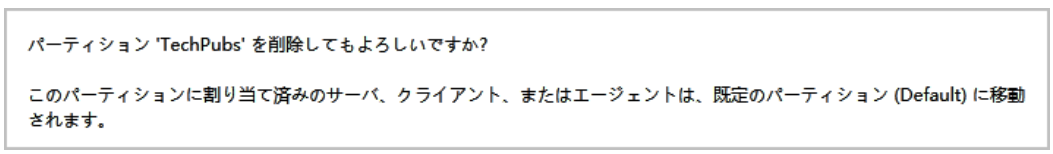
1 「**ユーザ > パーティション**」に移動します。

2 「**認証パーティション**」テーブルで、削除するパーティションの「**設定**」列にある**削除**アイコンを選択します。確認メッセージが表示されます。



3 「**OK**」を選択します。このパーティションにサブパーティションがあるかないかによって操作は異なります。

- サブパーティションがない場合、パーティションは削除され、そのサーバ/エージェント/クライアントは「**Default**」パーティションへの再割り当てが行われます。
- サブパーティションがある場合、次のメッセージが表示されます。



a) 次のいずれかを行います。

- 親パーティションと共にサブパーティションも削除する場合は、「**はい**」を選択します。すべてのサーバ/エージェント/クライアントは「**Default**」パーティションへの再割り当てが行われます。

- サブパーティションを最上位レベルのパーティションに変換して親パーティションを削除するには、「**いいえ**」を選択します。すべてのサーバ/エージェント/クライアントは「**Default**」パーティションへの再割り当てが行われます。
- 親パーティションを削除しない場合は、「**キャンセル**」を選択します。

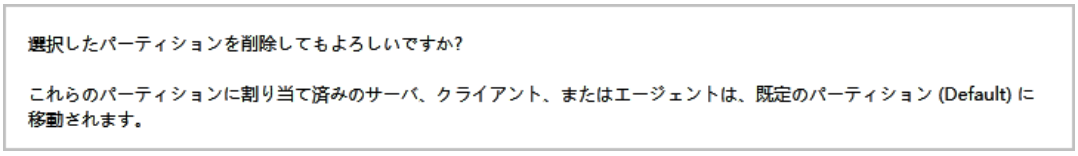
複数パーティションの削除

複数のパーティションを削除するには、以下の手順に従います。

1 「**ユーザ > パーティション**」に移動します。

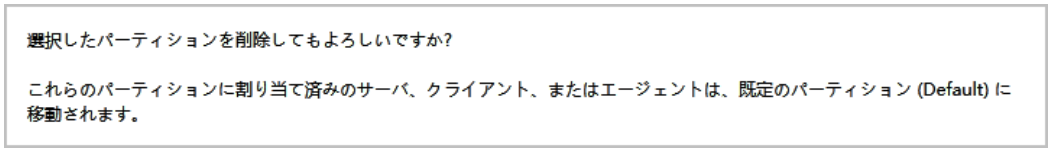
2 「**認証パーティション**」テーブルで、削除する認証パーティションのチェックボックスを選択します。複数のパーティションを選択できます。

3 「**削除**」を選択します。確認メッセージが表示されます。



4 「**OK**」を選択します。サブパーティションの有無によって操作は異なります。

- サブパーティションがない場合、パーティションは削除され、そのサーバ/エージェント/クライアントは「**Default**」パーティションへの再割り当てが行われます。
- サブパーティションがある場合、次のメッセージが表示されます。



a 次のいずれかを行います。

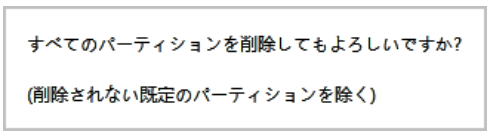
- 親パーティションと共にサブパーティションも削除する場合は、「**はい**」を選択します。すべてのサーバ/エージェント/クライアントは「**Default**」パーティションへの再割り当てが行われます。
- サブパーティションを最上位レベルのパーティションに変換して親パーティションを削除するには、「**いいえ**」を選択します。すべてのサーバ/エージェント/クライアントは「**Default**」パーティションへの再割り当てが行われます。
- 親パーティションを削除しない場合は、「**キャンセル**」を選択します。

すべてのパーティションの削除 (既定を除く)

すべてのパーティション (既定を除く) を削除するには、以下の手順に従います。

1 「**ユーザ > パーティション**」に移動します。

2 「**認証パーティション**」テーブルで、「**すべて削除**」を選択します。確認メッセージが表示されます。



3 「**OK**」を選択します。すべてのサーバ/エージェント/クライアントは「**Default**」パーティションへの再割り当てが行われます。

サーバ、エージェント、クライアントの割り当て

認証パーティションを追加した後は、サーバ、エージェント、クライアントをパーティションに割り当てます。同じ手順に従うことで、いつでも認証パーティションへの割り当てを行うこともできます。

割り当てられていないサーバ、エージェント、クライアントをパーティションに自動的に割り当てることができます。

トピック:

- 手動割り当て (226 ページ)
- 自動割り当て (227 ページ)

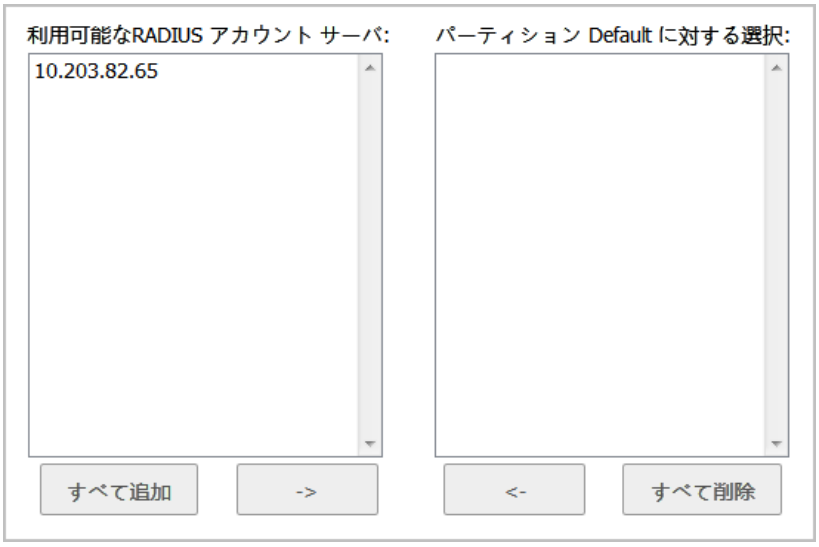
手動割り当て

サーバ、エージェント、クライアントを割り当てるには、以下の手順に従います。

1 「**ユーザ > パーティション**」に移動します。

2 「**認証パーティション**」テーブルで、「**設定**」列にある該当するパーティションの**設定**アイコンを選択します。「**何を選択しますか?**」ポップアップ ダイアログが表示されます。

3 割り当てるサーバ、エージェント、またはクライアントの種別を選択します。***<パーティション名> パーティション用の サーバ/エージェント/クライアントを選択***するための適切なポップアップ メニューが、使用可能なサーバ、エージェント、またはクライアントのリストと共に表示されます。



4 以下のいずれかを実行します。

- 「**利用可能な RADIUS アカウントサーバ**」リストからサーバ/エージェント/クライアントを選択し、**右矢印**を選択します。
- **Ctrl** キーを押しながら各項目を選択して、「**利用可能な RADIUS アカウントサーバ**」リストから複数の項目を選択したうえで、**右矢印**を選択します。
- 「**すべて追加**」を選択して、すべての項目を選択します。

5 「**保存**」を選択します。

自動割り当て

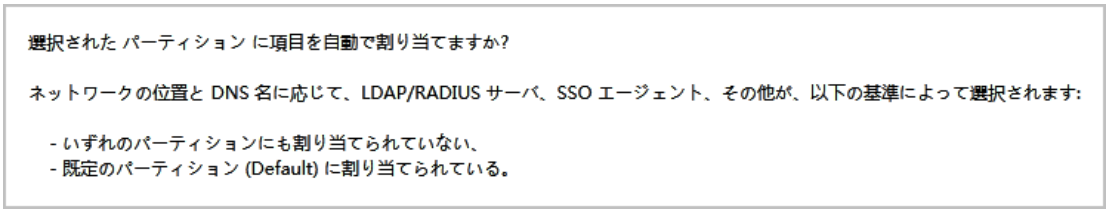
まだ割り当てられていないすべてのサーバ、エージェント、クライアントをその IP アドレスまたはホスト名に基づいて適切なパーティションに割り当てるための「**自動割り当て**」が存在します。

サーバ、エージェント、クライアントの自動割り当てを行うには、以下の手順に従います。

1 「**ユーザ > パーティション**」に移動します。

2 「**認証パーティション**」テーブルで、未割り当てのサーバ、エージェント、クライアントを割り当てる認証パーティションのチェックボックスを選択します。複数のパーティションを選択できます。「**自動割り当て**」が使用可能になります。

3 「**自動割り当て**」を選択ます。自動割り当てメッセージが表示されます。



4 「**OK**」を選択します。

パーティションの編集

「**Default**」パーティションを含むすべてのパーティションを編集できます。

パーティションを編集するには、以下の手順に従います。

1 「**管理 | システム セットアップ > ユーザ > パーティション**」に移動します。

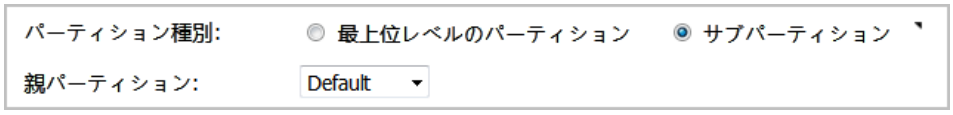
2 「**認証パーティション**」テーブルで、変更する認証パーティションの「**設定**」列にある**編集**アイコンを選択します。「**認証パーティションの編集**」ポップアップが表示されます。

3 「**パーティション名**」フィールドでは、パーティションの名前を変更できます。名前は 1 ～ 32 文字の英数字で指定します。

4 パーティションは、「**パーティション種別**」を変更することで、最上位レベルのパーティションからサブパーティションに、またはサブパーティションから最上位レベルのパーティションに変更できます。また、認証パーティションを以下のどちらにするか選択します。

> **メモ**：サブパーティションを持つ最上位レベルのパーティションは、そのサブパーティションをまず削除するか、別の最上位レベル パーティションに割り当て直すか、最上位レベルのパーティションにするかしないと、サブパーティションに変更することができません。

- **最上位レベルのパーティション**にする場合は、「ステップ 6」に進みます。
- **サブパーティション**にする場合は、「**親パーティション**」ドロップダウン メニューが表示されます。



5 「**親パーティション**」ドロップダウン メニューから親パーティションを選択します。既定のパーティションは「**Default**」です。

6 適宜、以下の操作を行います。

- ドメインを編集する場合は、「ステップ 10」に進みます。
- ドメインを削除する場合は、「ステップ 15」に進みます。
- ドメインを追加するには、「**ドメイン**」リストで「**追加**」を選択します。「**ドメインの追加**」ポップアップ ダイアログが表示されます。

7 ドメイン名を 1 ～ 32 文字の英数字で入力します。

8 「**OK**」を選択します。

9 「ステップ 17」へ進みます。

10 編集するドメインを選択します。

11 「**編集**」を選択します。「**ドメインの編集**」ダイアログが表示されます。

12 ドメイン名を変更します。

13 「**OK**」を選択します。

14 「ステップ 17」に進んでください。

15 削除するドメインを選択します。

16 「**削除**」を選択します。

17 追加、編集、または削除するドメイン毎に「ステップ 6」を繰り返します。

18 パーティションで名前を検索するために使用するサーバを変更するには、「**パーティションで名前を検索する**」で、次のいずれかを選択します。

- 「**既定の DNS サーバを使用する**」。「ステップ 20」に進みます。
- 「**パーティションの DNS サーバを使用する**」。「**DNS サーバ 1/-2/-3**」フィールドが使用可能になります。

19 「**DNS サーバ 1/-2/-3**」フィールドに最大 3 つの DNS サーバを入力します。

20 必要に応じて、「**コメント**」フィールドにコメントを入力します。

21 「**保存**」を選択します。

パーティション選択ポリシーの設定

パーティション選択ポリシーにより、ユーザに対する認証パーティションの選択方法が指定されます。認証パーティション選択ポリシーの追加、編集、管理は、「**管理 | システム セットアップ > ユーザ > パーティション**」ページの「**パーティション選択ポリシー**」セクションで行います。パーティション選択ポリシーの詳細な説明については、「認証パーティションの選択について (211 ページ)」を参照してください。

トピック:

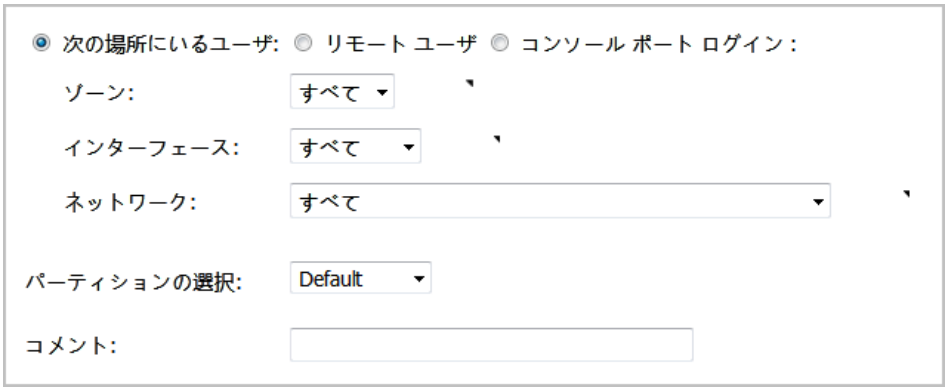
- 認証パーティション選択ポリシーの追加 (231 ページ)
- 選択ポリシーの優先順位の変更 (233 ページ)
- 選択ポリシーの変更 (233 ページ)
- パーティション選択ポリシーの削除 (234 ページ)

認証パーティション選択ポリシーの追加

パーティション選択ポリシーを追加するには、以下の手順に従います。

1 「**管理 | システム セットアップ > ユーザ > パーティション**」ページに移動します。

2 「**パーティション選択ポリシー**」セクションで、「**追加**」を選択します。「**パーティション選択ポリシーを追加する**」ポップアップ ダイアログが表示されます。



3 ユーザのログイン場所を選択します。表示される内容は次の選択によって異なります。

選択対象	参照先
次の場所にいるユーザ:	「ステップ 4」に進みます。 これは既定の設定です。

選択対象	参照先
リモート ユーザ	ステップ 7
コンソール ポート ログイン	ステップ 9

4 「**次の場所にいるユーザ**」を選択した場合は、パーティションが配置されている場所を「**ゾーン**」、「**インターフェース**」、および「**ネットワーク**」ドロップダウン メニューから選択します。

> **メモ**：通常、パーティションを選択するために、ゾーン、インターフェース、およびネットワークのすべてを選択する必要はありません。最適な効率性のためには、必要最小限に抑えるのが最善です。
>
> 例えば、パーティションが特定のインターフェースを介して配置されている場合は、そのインターフェースだけを選択し、「**ゾーン**」は既定値である「**すべて**」のままにしておきます。パーティションが特定のサブネット内に配置されている場合は、そのサブネットを「**ネットワーク**」で選択するだけにして、「**ゾーン**」と「**インターフェース**」はどちらも既定の設定である「**すべて**」のままにしておきます。

> **メモ**：各ドロップダウン メニューで提示される選択肢は、サイトによって異なります。

- **ゾーン** - 既定は「**すべて**」です。
- **インターフェース** - 既定は「**すべて**」です。
- **ネットワーク** - 既定は「**すべて**」です。新しいアドレス オブジェクトやアドレス グループを作成するためのオプションがあります。

5 「**パーティションの選択**」ドロップダウン メニューから、パーティションまたはサブパーティションを選択します。既定のパーティションは「**Default**」です。

6 「ステップ 10」へ進みます。

7 リモート ユーザを選択した場合はオプションが変化します。「**パーティションの選択**」ドロップダウン メニューから、パーティションまたはサブパーティションを選択します。既定のパーティションは「**Default**」です。

8 「ステップ 10」へ進みます。

9 コンソール ポート ログインを選択した場合はオプションが変化します。「**パーティションの選択**」ドロップダウン メニューから、パーティションまたはサブパーティションを選択します。既定のパーティションは「**Default**」です。

10 必要に応じて、「**コメント**」フィールドにコメントを入力します。

11 「**保存**」を選択します。

選択ポリシーの優先順位の変更

使用する認証パーティションを決定すると、SonicOS によって「**パーティション選択ポリシー**」テーブルが最上位 (1) から最下位 (*n*) まで順に検索されます。作成した選択ポリシーは、次のように優先順位付けされます。

1 ゾーン (グループの最後には「**すべて**」がリストされています)

2 インターフェース (グループの最後には「**すべて**」がリストされています)

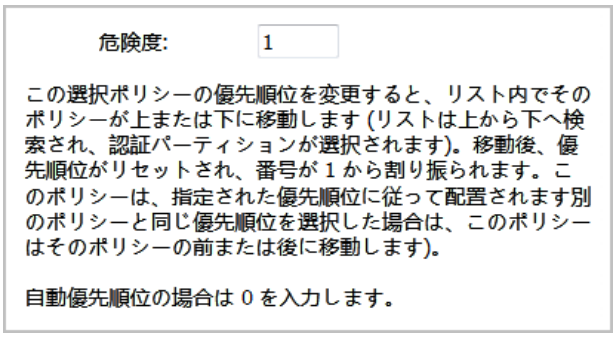
3 ネットワーク (グループの最後には「**すべて**」がリストされています)

任意のポリシーの優先順位 (常に最低の優先順位となる「**Default**」パーティション選択ポリシーを除きます) を変更できます。

選択ポリシーの優先順位を変更すると、優先順位リストでのそのポリシーの位置が上下に移動します。移動後は、新しい順序付けに合わせて優先順位が再設定されます。

ポリシーの優先順位を変更するには、以下の手順に従います。

1 「**パーティション選択ポリシー**」テーブルで、選択ポリシーの**優先順位**アイコン 1 を選択します。「**選択ポリシーの優先順位の変更**」ポップアップ ダイアログが表示されます。



2 「**優先順位**」フィールドに適切な優先順位を入力します。

> **メモ**：0 を入力すると自動で優先順位付けされます。

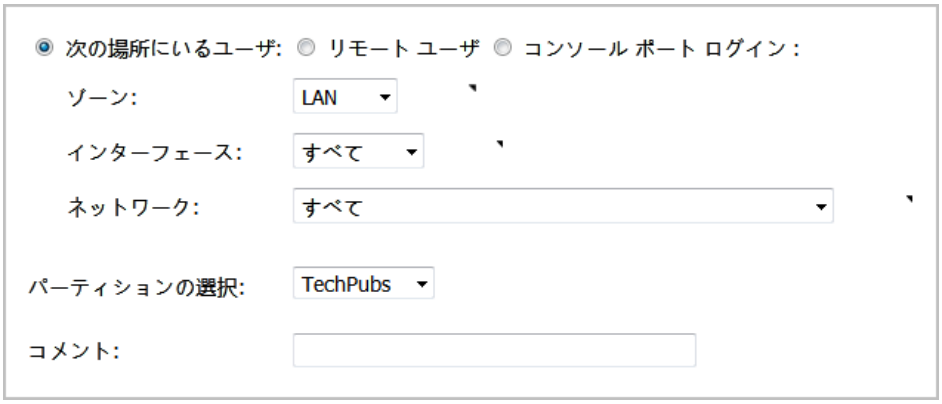
3 「**OK**」を選択します。「**パーティション選択ポリシー**」テーブルが更新され、他のポリシーの順序付けの再設定を含む、新しい順序付けが反映されます。

選択ポリシーの変更

自動生成された「**既定**」ポリシーを除き、任意のパーティション選択ポリシーを変更できます。「既定」ポリシーについては、**選択されているパーティション**の変更のみが可能です。

パーティション選択ポリシーを変更するには、以下の手順に従います。

1 「**パーティション選択ポリシー**」テーブルで、その選択ポリシーの「**設定**」列にある**編集**アイコンを選択します。「**パーティション選択ポリシーを編集する**」ポップアップ ダイアログが表示されます。



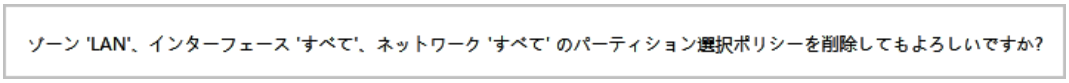
2 これは「パーティション選択ポリシーを追加する」ダイアログと同じものです。このダイアログについては、「認証パーティション選択ポリシーの追加 (231 ページ)」を参照してください。

パーティション選択ポリシーの削除

「**Default**」認証パーティション用の自動生成された「**既定**」ポリシーを除き、任意のパーティション選択ポリシーを削除できます。単一のポリシー、複数のポリシー、または作成したすべてのポリシーを削除できます。

ポリシーを削除するには、以下の手順に従います。

1 「**ユーザ > パーティション**」ページの「**パーティション選択ポリシー**」セクションで、削除するポリシーの「**設定**」列にある**削除**アイコンを選択します。確認メッセージが表示されます。



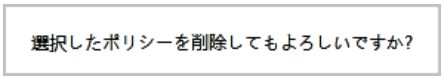
2 「**OK**」を選択します。

複数のポリシーを削除するには、以下の手順に従います。

メモ：既定のパーティション選択ポリシーは削除できません

1 「**ユーザ > パーティション**」ページの「**パーティション選択ポリシー**」セクションで、チェックボックスの選択により、削除するポリシーを 1 つ以上選択します。「**削除**」が使用可能になります。

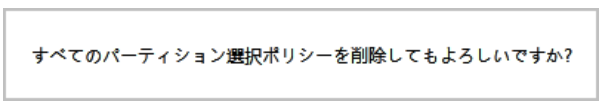
2 「**削除**」を選択します。確認メッセージが表示されます。



3 「**OK**」を選択します。

すべてのポリシーを削除するには、以下の手順に従います。

1 「**ユーザ > パーティション**」ページの「**パーティション選択ポリシー**」セクションで、「**すべて削除**」を選択します。確認メッセージが表示されます。



2 「**OK**」を選択します。

認証パーティション用のサーバ、エージェント、クライアントの設定

各パーティションで、以下の設定を行うことができます。

ユーザ認証方式	ローカル ユーザ
	RADIUS
	RADIUS + ローカル ユーザ
	LDAP
	LDAP + ローカル ユーザ
シングル サインオン方式	SSO エージェント
	ターミナル サービス エージェント (TSA)
	RADIUS アカウント
	ブラウザ NTLM 認証

サーバ、エージェント、クライアントのすべての認証パーティション処理の設定は、「**ユーザ > 設定**」ページで行います。これらのエンティティの設定方法と「**ユーザ > 設定**」ページの詳細な説明については、「ユーザの管理のための設定 (128 ページ)」を参照してください。パーティションがどのようにサーバやエージェントの設定に影響するかの説明については、「サーバとエージェントの設定」テーブルを参照してください。

メモ：サーバ、エージェント、クライアントの操作の詳細については、「サブパーティションによるサーバ、エージェント、クライアントの操作 (209 ページ)」を参照してください。

サーバとエージェントの設定

サーバ/エージェント	パーティション処理の設定
RADIUS サーバ	最大で 2 つの RADIUS サーバをプライマリ/セカンダリ冗長化ペアとして設定されます。認証パーティション毎に 1 つのプライマリ/セカンダリ ペアを用意する形で、複数の RADIUS サーバ ペアを設定できます。
LDAP サーバ	複数のプライマリ LDAP サーバ (認証パーティション毎に 1 つ) を設定できます。さらに、それぞれに対するセカンダリ サーバのリストも設定できます (「複数 LDAP サーバの拡張サポートについて (174 ページ)」を参照してください)。通常、ドメイン用または相互接続されているドメインのグループ (Active Directory の用語ではフォレスト) 用の LDAP サーバは、各認証パーティションに割り当てられています。
SSO エージェント	負荷分散と冗長化の両方のサポートに加えて、複数の SSO エージェントでも認証パーティションに対するエージェントの割り当てがサポートされています。1 つ以上のエージェントのグループがそれぞれの認証パーティションに割り当てられ、負荷分散と冗長化が各グループ内で行われます。
TS エージェント	TSA のパーティション処理は、ユーザ グループ メンバーシップ検索用の LDAP サーバ選択のためだけに必要となります。TSA では常に完全な Windows NetBIOS ドメイン名がユーザ名と共に提供されるので、設定は省略可能です。そのため、ほとんどの場合は、ユーザ名から認証パーティションを導き出すことが可能です。

サーバとエージェントの設定

サーバ/エージェント	パーティション処理の設定
RADIUS アカウント クライアント	SSO RADIUS アカウント クライアントのパーティション処理は、ユーザ グループ メンバーシップ検索用の LDAP サーバ選択のためだけに必要です。一部の RADIUS アカウント クライアント (すべてではありません) は、ドメイン名をユーザ名と共にアカウント メッセージ内に提示するので、設定は省略可能です。そのため、場合によっては、ユーザ名から認証パーティションを導き出すことが可能です。

10

ローカル ユーザおよびグループの設定

トピック:

- 認証とパスワードについて (237 ページ)
  - 二段階認証の使用 (237 ページ)
  - 初回ログイン パスワードの変更の強制 (238 ページ)
- ローカル ユーザの設定 (238 ページ)
  - すべてのユーザのクォータ制御 (239 ページ)
  - ローカル ユーザの表示 (239 ページ)
  - ローカル ユーザの追加 (240 ページ)
  - ローカル ユーザの編集 (247 ページ)
  - ローカル ユーザを LDAP からインポートする (249 ページ)
  - ゲスト管理者の設定 (249 ページ)
- ローカル グループの設定 (250 ページ)
  - ローカル グループの作成または編集 (251 ページ)
  - LDAP からのローカル グループのインポート (259 ページ)
  - LDAP 位置によるユーザ メンバーシップの設定 (259 ページ)

認証とパスワードについて

トピック:

- 二段階認証の使用 (237 ページ)
- 初回ログイン パスワードの変更の強制 (238 ページ)

二段階認証の使用

多くのユーザ ログイン認証はワンタイム パスワード (OTP) を必要とします。SonicOS 6.5.4 は、電子メールを介した OTP 方式を提供しています: 2 要素認証による時間ベースのワンタイム パスワード (TOTP) 認証。

この機能を使用するには、ユーザは自分のスマートフォンに TOTP クライアント アプリ (Google Authentication、DUO、Microsoft Authentication など) をダウンロードする必要があります。「**ユーザの追加/編集**」ダイアログで TOTP を選択します。

初回ログイン パスワードの変更の強制

以前は、ユーザの作成時に、初回ログイン後にパスワードを変更することをユーザに許可できました。SonicOS 6.5.4 では、ローカル ユーザの作成または編集時に初回ログイン前にユーザにパスワードの変更を強制できます。ユーザまたはグループに対してログイン変更を指定できます。

ローカル ユーザの設定

ローカル ユーザは、SonicWall セキュリティ装置のローカル データベースに格納され、管理されるユーザです。「**管理 | システム セットアップ > ユーザ > ローカル ユーザとグループ**」で、すべてのローカル ユーザの表示と管理、新しいローカル ユーザの追加、既存ローカル ユーザの編集を行うことができます。LDAP サーバからユーザをインポートすることもできます。

チェックボックス	個々のローカル ユーザを選択するために使います。
展開/折りたたみアイコン	既定では、ローカル ユーザのユーザ名のみがリストされます。「展開」アイコンを選択すると、ローカル ユーザが属するグループが表示されます。
名前	ローカル ユーザのユーザ名を一覧表示します。展開すると、ローカル ユーザが属するグループの名前が一覧表示されます。
ゲスト サービス	ローカル ユーザでゲスト サービスが有効になっているかどうかを緑色のチェックマーク アイコンで示します。
管理者	ローカル ユーザで使用可能な管理機能の種別が表示されます。
VPN アクセス	各ローカル ユーザおよびそのローカル ユーザが属する各グループに関する「**コメント**」アイコンが表示されます。このアイコンにマウス カーソルを合わせると、ローカル グループの VPN アクセスの状況が、そのグループの各メンバーの状況と共に表示されます。

コメント	各ローカル ユーザおよびそのローカル ユーザが属する各グループに関する「**コメント**」アイコンが表示されます。このアイコンにマウス カーソルを合わせると、ローカル ユーザ/グループの設定または編集時に入力したコメントが表示されます。
クォータ	各ローカル ユーザの「**統計**」アイコンが表示されます。このアイコンにマウス カーソルを合わせると、ローカル ユーザの使用クォータが表示されます。
設定	各ローカル ユーザの「**編集**」アイコンと「**削除**」アイコンが表示されます。アイコンが淡色表示か無効になっている場合、その機能はそのローカル ユーザまたはローカル グループでは使用できません。

認証と 2 ファクタ パスワードの詳細については、「認証とパスワードについて (237 ページ)」を参照してください。

トピック:

- すべてのユーザのクォータ制御 (239 ページ)
- ローカル ユーザの表示 (239 ページ)
- ローカル ユーザの追加 (240 ページ)
- ローカル ユーザの編集 (247 ページ)
- グローバル設定の構成 (248 ページ)
- ローカル ユーザを LDAP からインポートする (249 ページ)
- ゲスト管理者の設定 (249 ページ)

すべてのユーザのクォータ制御

ユーザのクォータ制御機能は、ユーザのアカウントに基づくクォータ制御を提供します。クォータは、セッション存続期間、または送受信トラフィック制限として指定できます。サイクル クォータでは、ユーザはアカウント クォータを使い切ると、次のサイクル (日、週、または月) が始まるまでインターネットにアクセスできなくなります。クォータ サイクルの設定が「循環しない」である場合、ユーザはクォータを使い切るとインターネットにアクセスできなくなります。

以前は、クォータ制御はゲスト ユーザに対してのみサポートされていました。すべてのローカル ユーザにもクォータ制御が指定されるようになりました。

ローカル ユーザの表示

「**ユーザ > ローカル ユーザとグループ**」で、ユーザが所属するすべてのグループを表示できます。ユーザの横の**展開**アイコンを選択すると、ユーザのグループ メンバーシップが表示されます。

ユーザ名の右側にある列には、ユーザの持つ権限が表示されます。展開表示では、ユーザが各権限を得ている元のグループが表示されます。

適宜、以下の操作を行います。

- 「**VPN アクセス**」列の**コメント** アイコンにマウス ポインタを重ねると、ユーザが VPN アクセス可能なネットワーク リソースが表示されます。
- 「**クォータ**」列の**統計**アイコンにマウス ポインタを重ねると、ユーザのクォータが表示されます。

- 展開表示で、「**設定**」列にある**削除**アイコンを選択して、グループからユーザを削除します。

  メモ：グループから削除できないユーザのアイコンは、グレーアウトされています。

- 「**設定**」列にあるユーザの**編集**アイコンを選択して、ユーザを編集します。「ローカル ユーザの編集 (247 ページ)」を参照してください。
- ユーザの「**設定**」列にある**ごみ箱**アイコンを選択して、その行のユーザまたはグループを削除します。

  メモ：グループから削除できないローカル ユーザのアイコンは、グレーアウトされています。

「**ユーザ > ローカル ユーザとグループ**」ページの下部に、ローカル ユーザの総数が表示されます。

ローカル ユーザの追加

セキュリティ装置の内部データベースにローカル ユーザを追加するには、「**ユーザ > ローカル ユーザ**」ページを使用します。

メモ：SSL VPN クライアントのユーザを作成する手順については、『*SonicOS 6.5 接続*』を参照してください。

データベースにローカル ユーザを追加するには、次の手順に従います。

1. 「**管理 | システム セットアップ > ユーザ > ローカル ユーザとグループ**」に移動します。
2. パーティション処理が有効かそうでないかによって手順が異なります。
   - 有効でない場合は、「ステップ 3」に進みます。
   - 有効になっている場合は、設定を適用するパーティションを「**認証パーティション**」ドロップダウン メニューから選択します。既定は「**すべて**」です。

   ヒント：このメニューは、パーティション処理が有効になっている場合にのみ表示されます。
3. **追加**アイコンを選択します。「**ユーザの追加**」ダイアログが表示されます。

4 「**設定**」では、グループ メンバーシップ、アクセス権、その他の属性が、登録されているドメイン アカウントを使用してログインしているすべてのドメイン ユーザに適用されるかどうかを、「**ドメインユーザに相当する**」の選択によって示します。このオプションは、既定では選択されていません。選択されている場合は、他のオプションが表示されます。

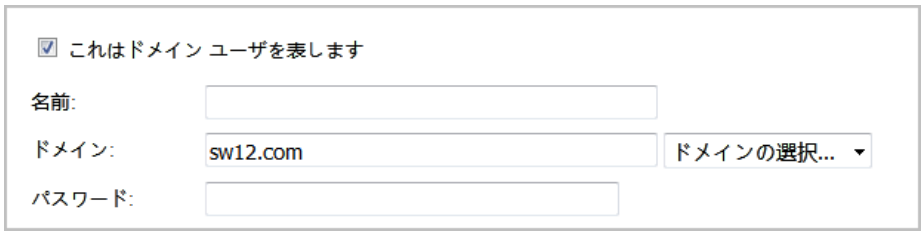
「**ドメインユーザに相当する**」が選択されているかどうかによって、手順が異なります。

- 選択されている場合は、グループ メンバーシップ、アクセス権など、設定されているすべての属性が、指定されたドメイン アカウント (RADIUS または LDAP によって認証されたもの) を使用してログインしているユーザ、または SSO によってそのドメイン ユーザとして識別されているユーザに適用されます。この属性の適用対象は、特定のドメイン内で指定された名前を持つユーザ アカウントにすることも、任意のドメイン内で指定された名前を持つユーザにすることもできます。
- 選択されていない場合、ローカル ユーザはローカル アカウントであり、これが設定されているものはすべて、そのアカウントを使用してログインし、ローカルで認証されたユーザのみに適用されます。この場合は、「ステップ 8」でパスワードを設定しておく必要があります。

5 「**名前**」フィールドにユーザ名を入力します。

6 ローカル ユーザがドメイン ユーザを表すかどうかによって、手順が異なります。

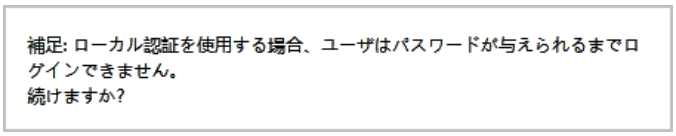
- ドメイン ユーザを表している場合、オプションが変化します。「ステップ 7」に進みます。



- ドメイン ユーザを表していない場合、「ステップ 8」に進みます。

7 「**ドメイン**」フィールドに、ドメイン名を入力します。「**ドメイン**」ドロップダウン メニューからドメインを選択できます。リストにないドメイン名を入力する場合は、完全なドメイン名を入力する必要があります。そうしないと、次のメッセージが表示されます。

ドメインがローカルの場合は、パスワードを入力する必要があります。パスワードを入力しない場合、次のメッセージが表示されます。



8 「**パスワード**」フィールドに、ユーザのパスワードを入力します。パスワードでは大文字と小文字が区別されます。また、家族、友人、ペットなどの名前ではなく、32 文字 の英数字と特殊文字の組み合わせにする必要があります。文字数と文字の種別は「**管理 | システム セットアップ | 装置 > 基本設定 > ログイン セキュリティ**」で設定されます。

メモ：「**これはドメイン ユーザを表します**」が選択されなかった場合は、パスワードを入力する必要があります。

9 確認のため、「**パスワードの確認**」フィールドにパスワードを再入力します。

10 初回ログイン時にユーザにパスワードの変更を求める必要がある場合は、「**ユーザはパスワードを変更する必要があります**」を選択します。このオプションは、既定では選択されていません。「**ユーザはパスワードを変更する必要があります**」を選択した場合、このダイアログは最初のログイン試行時に表示されます。

11 「**ワンタイム パスワード方式**」から、**2 ファクタ認証のために SSL VPN ユーザにシステム生成パスワードを送信するよう要求する**方式を選択します。

ヒント：ローカル ユーザがワンタイム パスワードを有効にしていないのに、そのユーザが所属するグループで有効にしている場合には、そのユーザの電子メール アドレスが設定されていることを確認してください。電子メール アドレスが設定されていない場合、このユーザはログインできません。

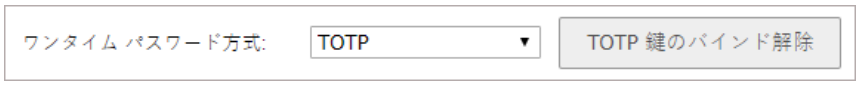
ヒント：このユーザに対する別のパスワード変更要求を回避するために、このオプションは最初のログインにのみ適用されます。

- **無効** (既定) -「**ユーザはパスワードを変更する必要があります**」を選択した場合、このダイアログは最初のログイン試行時に表示されます。

「ステップ 13」に移動します。

- **メール経由の OTP** - ユーザは、自分のユーザ名と最初のパスワードを入力した後に、電子メールで一時パスワードを受け取ります。パスワードを含む電子メールを受信したら、2 番目のパスワードを入力してログイン プロセスを完了できます。「ステップ 12」に移動します。
- **TOTP** - ユーザは自分のユーザ名と最初のパスワードを入力すると電子メールで一時パスワードを受け取りますが、この機能を使用するには、ユーザは自分のスマートフォンに TOTP クライアント アプリ (Google Authentication、DUO、Microsoft Authentication など) をダウンロードする必要があります。

  TOTP 鍵のバインド解除が表示されます。



12 ユーザがワンタイム パスワードを受信できるよう、ユーザの電子メール アドレスを入力します。

13 「**アカウント存続期間**」で、ユーザ アカウントが削除または無効化によって存在しなくなるまでの期間を選択します。選択内容に応じて、さらに次のオプションが表示されます。

- 「**期限なし**」は、アカウントを永続的なものにします。このオプションは既定の設定です。「ステップ 16」へ進みます。
- 「**分間**」、「**時間**」、または「**日間**」では、ユーザ アカウントが削除または無効化されるまでの存続期限を指定します。制限付きの存続期間を選択した場合、オプションは次のように変化します。

14 「**アカウント存続期間**」フィールドに存続期間を入力します。最大で 9999 時間、9999 分間、または 9999 日間を指定できます。

15 適宜、以下の操作を行います。

- 有効期限が切れた後にユーザ アカウントを削除するには、「**有効期間が切れた場合に削除する**」を選択します。このオプションは、既定では選択されています。
- 有効期限が切れた後に単にアカウントを無効にするには、このオプションを無効にします。その後、アカウントの有効期限をリセットすれば、アカウントを再度有効にできます。

16 必要に応じて、「**コメント**」フィールドにコメントを入力します。

17 「**グループ**」を選択します。

グループ

1 「**ユーザ グループ**」で、以下の操作を行います。

a ユーザの所属先のグループを 1 つ以上選択します。

b 次のどちらかを行います。

- 選択したグループ名を「**右矢印 ->**」で「**所属するグループ**」リストに移動します。ユーザが、選択したグループのメンバーになります。
- 「**すべて追加**」を選択します。

メモ：ユーザをグループから削除するには、以下の手順に従います。

1「**所属するグループ**」リストからグループを選択します。

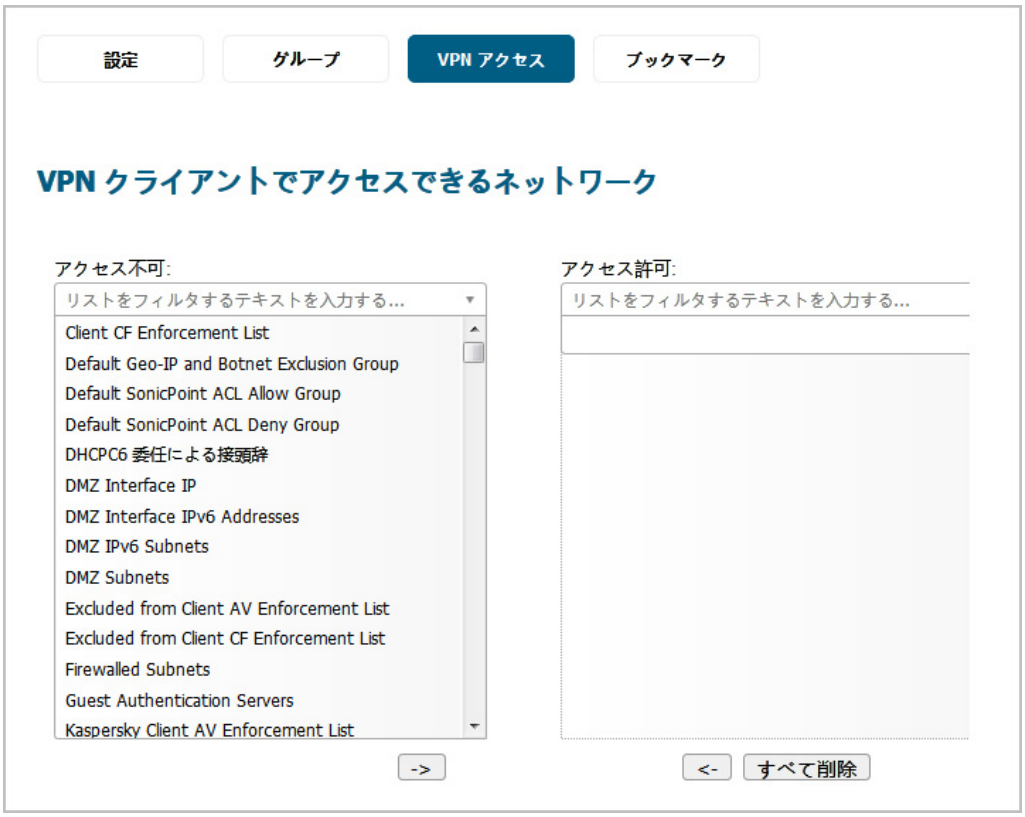
2 次のどちらかを行います。

- **左矢印 <-** を選択します。
- 「**すべて削除**」を選択します。

メモ：「**Everyone**」および「**Trusted Users**」は「**所属するグループ**」から削除できません。

2 VPN ユーザがアクセスできるネットワーク リソース (GVC、NetExtender、または仮想オフィス ブックマーク) を設定するには、「**VPN アクセス**」を選択します。

VPN アクセス



1 「**アクセス不可**」から 1 つ以上のネットワークを選択します。

2 **右矢印**を選択して、それらを「**アクセス許可**」リストに移動します。

メモ：「**VPN アクセス**」は、GVC、NetExtender、および SSL VPN 仮想オフィス ブックマークを使ってネットワーク リソースにアクセスするリモート クライアントの能力に影響します。こうしたユーザにネットワーク リソースへのアクセスを許可するには、ネットワーク アドレス オブジェクトまたはグループを「**アクセス許可**」に追加しておく必要があります。

ネットワークへのユーザ アクセスを削除するには、以下の手順に従います。

- 「**アクセス許可**」リストからネットワークを選択して、**左矢印**を選択します。
- 「**すべて削除**」を選択します。

3 関係するグループに所属する各ユーザについて、仮想オフィス ブックマークを追加、編集、または削除するには、「**ブックマーク**」を選択します。

ブックマーク

4 ブックマークを追加するには、「**ブックマークの追加**」を選択します。SSL VPN ブックマークの設定方法については、『*SonicOS 6.5 ポリシー*』を参照してください。

> **メモ**：ユーザのブックマークを設定するためには、そのユーザが SSL VPN サービス グループのメンバーである必要があります。ユーザがメンバーになっていない場合は、そうしたユーザを SSL VPN サービス グループに追加したうえで変更内容を送信してブックマークを有効にする必要があります。

5 「**ユーザ クォータ**」を選択します。

ユーザ クォータ

1 「**ユーザ クォータ**」を選択します。

2 すべてのオプションを設定します。

3 「**OK**」を選択してユーザ設定を完了します。

ローカル ユーザの編集

「**ユーザ > ローカル ユーザとグループ**」ページで、ローカル ユーザを編集できます。

ローカル ユーザを編集するには、次の手順に従います。

1 「**ローカル ユーザ**」テーブルで、「**設定**」の下にあるユーザの**編集**アイコンを選択します。「**ユーザの編集**」ダイアログが表示されます。

2 新しいユーザを追加する場合と同様に、「**設定**」、「**グループ**」、「**VPN アクセス**」、「**ブックマーク**」、「**ユーザ クォータ**」の各オプションを設定します。「ローカル ユーザの追加 (240 ページ)」を参照してください。

グローバル設定の構成

すべてのユーザ用の設定を行うには、以下の手順に従います。

1 「**管理 | システム セットアップ > ユーザ > ローカル ユーザとグループ**」に移動します。

2 「設定」を選択します。

3 「**すべてのローカルユーザにパスワード制約を適用する**」を選択します。このオプションは、既定では選択されています。

4 「**期限切れユーザ アカウントを削除する**」を選択します。このオプションは、既定では選択されています。

5 管理インターフェースで表示形式を選択するには、「**ドメイン ユーザ/グループ名の優先表示形式**」から形式を選択します。

> **ヒント**：このオプションは、名前の表示方法にのみ影響し、ファイアウォールによる処理方法には影響しません。例えば、Windows 形式を選択すると、`user1@mydomain.com` は `MYDOMAIN\user1` として表示されますが、ユーザ オブジェクトは `user1@mydomain.com` として処理されます。また、表示が変化するのは、明示的なドメイン (つまり、選択されているどのドメインも影響を受けないようなドメイン) を持つユーザおよびユーザ グループ オブジェクトだけです。

- **<名前>@<ドメイン>.com**
- **ドメイン\名前 (Windows)**
- **<名前>.<ドメイン> (Novell)**
- **自動 (LDAP スキーマに従う)** (既定)

> **メモ**：「自動」を選択すると、LDAP サーバのスキーマに基づいて形式が選択されます。したがって、LDAP を有効にする必要があります。それ以外の場合、既定の形式の `name@domain.com` が使用されます。
>
> パーティション化が有効になっている場合、表示形式は、ドメインをホストするパーティションの LDAP スキーマに基づいて選択されます。これにより、異なるドメイン種別を持つパーティションで異なる表示形式を使用できます。

6 「**適用**」を選択します。

ローカル ユーザを LDAP からインポートする

LDAP サーバからユーザ名を取得することでファイアウォール上のローカル ユーザを設定できます。ファイアウォール上に既存の LDAP/AD ユーザと同じ名前を持つユーザがある場合、LDAP 認証の成功によって SonicWall ユーザ権限が与えられます。

LDAP サーバから読み込んだユーザのリストは、非常に長くなる場合があるため、それらのうち少数をインポートしたいことがあります。望まないユーザを選択するいくつかの方法と共に、「**リストより削除**」が提供されます。これらのオプションを使って、リストを管理可能なサイズに縮小してからインポートするユーザを選択できます。LDAP サーバからユーザをインポートする方法については、「LDAP からのインポートとミラーリングについて (176 ページ)」を参照してください。

ゲスト管理者の設定

ゲスト アカウントとセッションを管理することに限定した管理者アクセスを提供する「ゲスト管理者」権限グループを使用できます。

「ゲスト管理者」アカウントを設定するには、以下の手順に従います。

1 「**ユーザ > ローカル ユーザとグループ**」に移動します。

2 「**追加**」を選択します。「**ユーザの追加**」ダイアログが表示されます。

3 ユーザに付ける名前を「**名前**」フィールドで指定します。

4 「**グループ**」を選択します。

5 「**ユーザ グループ**」リストで「**ゲスト管理者**」を選択します。

6 右矢印を選択して、**ゲスト管理者**を「**所属するグループ**」リストに移動します。

7 「**OK**」を選択します。

8 「**ネットワーク > インターフェース**」に移動します。

9 LAN インターフェースの**編集**アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。

10 「ゲスト管理者」アカウントが LAN からセキュリティ装置にログインできるようにするには、「**ユーザ ログイン**」の下で「**HTTP**」と「**HTTPS**」の両方をオンにします。

11 「**OK**」を選択します。

ゲスト管理者としてのログオン

ゲスト管理者としてログオンするには、以下の手順に従います。

1 セキュリティ装置にゲスト管理者としてログオンします。特権サービスへのアクセス権があることを示すダイアログが表示されます。

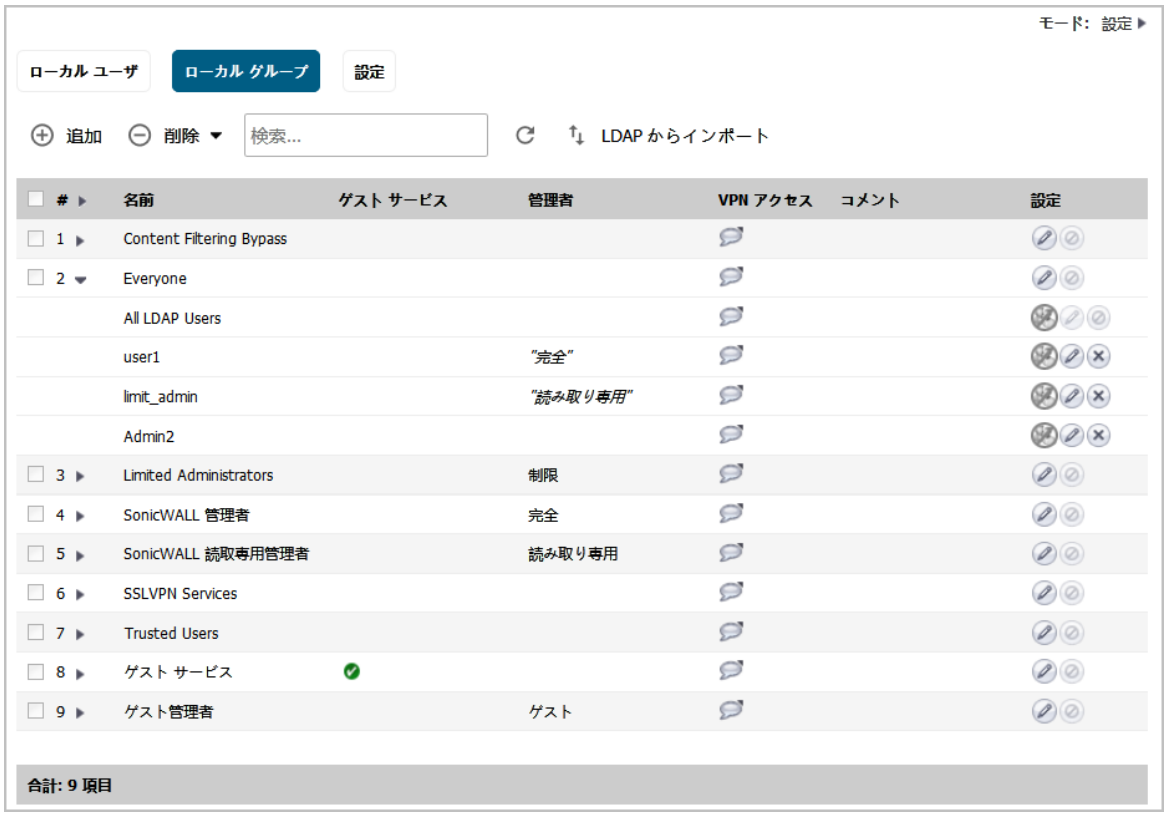
2 「**管理**」を選択します。

ログイン後、ゲスト管理者は次のことができます。

- 「**監視 | ユーザ セッション > 使用中のゲスト ユーザ**」ページで、すべてのゲスト アカウントとセッションを表示する。
- 次の管理インターフェース ページで、ゲスト ユーザを管理 (作成、削除、更新) する。
  - **管理 | システム セットアップ > ユーザ > ゲスト アカウント**
  - **管理 | システム セットアップ > ユーザ > ゲスト サービス**

ローカル グループの設定

ローカル グループは、「**ローカル グループ**」テーブルに表示されます。ローカル グループの中には、変更可能でも削除できない既定のグループがあります。



チェックボックス	個々のローカル グループを選択するために使います。既定のローカル グループは変更できないので、対応するチェックボックスが淡色表示になっています。
展開/折りたたみアイコン	既定では、ローカル グループの名前だけが一覧表示されています。
名前	既定のローカル グループおよび設定されたローカル グループが名前順に一覧表示されます。 「**システム > 管理**」ページの「**複数の管理役割を有効にする**」オプションが有効な場合、「**ユーザ > ローカル グループ**」ページには役割ベースの以下の既定の管理者グループが一覧表示されます。 • システム管理者 • 暗号化管理者 • 監査管理者
ゲスト サービス	ローカル グループでゲスト サービスが有効になっているかどうかを緑色のチェックマーク アイコンで示します。
管理者	ローカル グループで使用可能な管理機能の種別が表示されます。このアイコンにマウス カーソルを合わせると、一覧表示された機能についてのツールチップが表示されます。
VPN アクセス	各グループおよびそのグループの各メンバーに関する「**コメント**」アイコンが表示されます。このアイコンにマウス カーソルを合わせると、ローカル グループの VPN アクセスの状況が、そのグループの各メンバーの状況と共に表示されます。
コメント	ローカル グループのコメントが一覧表示されます。
クォータ	ローカル グループの使用クォータが一覧表示されます。
設定	個々のローカル グループとグループ メンバーごとに「**編集**」アイコンと「**削除**」アイコンが表示されます。また、グループ メンバー全体の「**削除**」アイコンも表示されます。淡色表示のアイコンは、その機能がローカル グループまたはグループ メンバーで使用できないことを意味します。

認証と 2 ファクタ パスワードの詳細については、「認証とパスワードについて (237 ページ)」を参照してください。

トピック:

- ローカル グループの作成または編集 (251 ページ)
- LDAP からのローカル グループのインポート (259 ページ)

ローカル グループの作成または編集

このセクションではローカル グループの作成方法を説明しますが、その内容は既存のローカル グループの編集にも当てはまります。ローカル グループの追加または編集時に、他のローカル グループをグループのメンバーとして追加することができます。

トピック:

- ローカル グループの追加 (252 ページ)
- ローカル グループの編集 (259 ページ)

ローカル グループの追加

ローカル グループを追加するには、次の手順に従います。

1 「**ユーザ > ローカル ユーザとグループ**」に移動します。

2 「**追加**」を選択します。「**グループの追加**」ダイアログが表示されます。

トピック:

- 設定 (252 ページ)
- メンバー (255 ページ)
- VPN アクセス (256 ページ)
- ブックマーク (257 ページ)
- 管理 (258 ページ)

設定

1 ログインしたり SSO によって識別されたりする際にこのユーザ グループに対するメンバーシップがそのユーザにどのように与えられるかを選択します。

メモ：このユーザ グループに対するメンバーシップが与えられるユーザには、そのグループに与えられているすべての権限とアクセス権が与えられます。

ドメイン ユーザ グループを照合する (既定)	これと同じ名前を持つドメイン ユーザ グループのメンバーであるすべてのユーザにこのグループに対するメンバーシップが与えられます。メンバーシップを与えるユーザは次のように選択できます。 • 特定のドメイン内のドメイン ユーザ グループのメンバーに対してのみ。 • 任意のドメイン内の名前付きグループのメンバーであるユーザ。 **メモ**：これが選択されるとオプションは変化します。
ローカルのみでメンバーを設定する	ローカル ユーザのみにグループでのメンバーシップが与えられます。このオプションは、既定では選択されていません。
ユーザのメンバーシップを LDAP ディレクトリのユーザの位置によって決定する	ログインしたユーザまたは SSO 経由で認証されたユーザには、LDAP サーバ上の対応するユーザ オブジェクトが「**LDAP 位置**」で指定した位置 (または、その配下) にあれば、そのセッションの間、当該ユーザ グループへのメンバーシップが与えられます。この設定はデフォルトで無効になっています。 **メモ**：LDAP サーバ上に対応するユーザ グループは存在しません。このグループに対するメンバーシップは、LDAP サーバ上のドメイン ユーザ グループで設定されているどのメンバーシップとも関連付けられません。 **メモ**：これが選択されるとオプションは変化します。

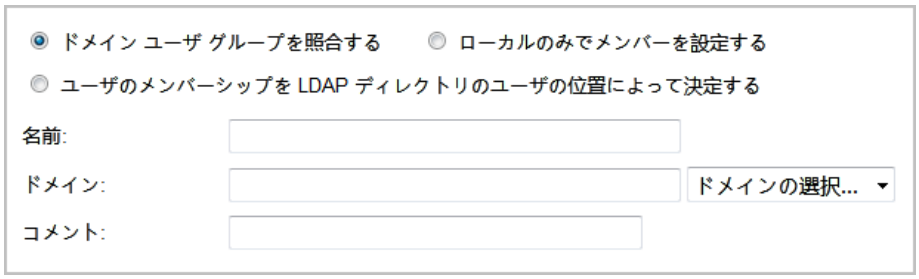
メモ：また、ローカル ユーザ (ドメイン ユーザを表すユーザを含みます) および他のユーザ グループは、どんな場合も、このダイアログの「**メンバー**」ページでグループのメンバーにすることができます。

2 ローカル グループに付ける名前を「**名前**」フィールドに入力します。

メモ：定義済みのユーザまたはグループの名前を編集することはできません。このフィールドはグレーアウトされています。

3 選択した内容によって次の手順が異なります。

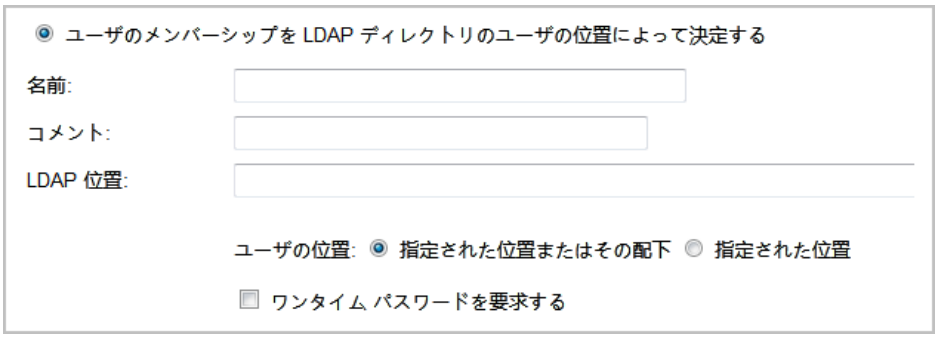
- 「**「ドメイン ユーザ グループを照合する」**」を選択した場合、オプションは変化します。「ステップ 4」に進みます。



- 「**ローカルのみでメンバーを設定する**」を選択した場合は、「ステップ 5」に進みます。

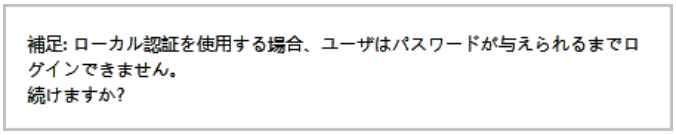
- 「**ユーザのメンバーシップを LDAP ディレクトリのユーザの位置によって決定する**」を選択した場合、オプションは変化します。「ステップ 5」に進みます。

  ヒント：「**メンバー**」タブで、ローカル ユーザや他のグループを、このグループのメンバーにすることもできます。



4 「**ドメイン**」フィールドに、ドメイン名を入力します。「**ドメイン**」ドロップダウン メニューからドメインを選択できます。リストにないドメイン名を入力する場合は、完全なドメイン名を入力する必要があります。そうしないと、次のメッセージが表示されます。

ドメインがローカルの場合は、パスワードを入力する必要があります。パスワードを入力しない場合、次のメッセージが表示されます。



5 必要に応じて、「**コメント**」フィールドに、わかりやすいコメントを入力します。

6 「**ドメイン ユーザ グループを照合する**」または「**ローカルのみでメンバーを設定する**」を選択した場合は、「ステップ 9」に進みます。

7 「**LDAP 位置**」フィールドに、LDAP ディレクトリ ツリー内の位置を入力します。位置の指定にはパス (`domain.com/users` など) または LDAP 識別名を使用できます。

メモ：「LDAP ユーザ グループ ミラーリング」を有効にした場合、ミラー ユーザ グループのこのフィールドは読み取り専用になり、ミラー元グループのLDAP ディレクトリ内の位置を示します。

8 「**ユーザの位置**」オプションからその場所を選択します。

- **指定された位置またはその配下** (既定値)
- **指定された位置**

9 必要に応じて、そのグループでワンタイム パスワードを要求するために、「**ワンタイム パスワードを要求する**」チェックボックスをオンにします。この設定を有効にした場合は、ユーザの電子メール アドレスを設定する必要があります。

10 適宜、以下の操作を行います。

- グループの追加を終了するには、「**OK**」を選択します。
- メンバーを追加するには、「メンバー (255 ページ)」に進みます。

メンバー

1 「**メンバー**」を選択します。

2 「**所属していないユーザとグループ**」リストから、追加したいユーザやグループを選択します。

3 追加の内容によって手順が異なります。

- 「**所属しているユーザとグループ**」リストにユーザやグループを追加する場合:
  a) 「**所属していないユーザとグループ**」リストから、ユーザやグループを選択します。
  b) **右矢印** (->) を選択します。
- すべてのユーザとグループを追加するには、「**すべて追加**」を選択します。

ⓘ **メモ**：任意のグループを「**Everyone**」、「**All LDAP Users**」以外の他のグループのメンバーとして追加できます。グループを他のグループに追加する場合は、メンバーシップに注意してください。

ユーザやグループを削除するには、「**所属しているユーザとグループ**」リストから、ユーザやグループを選択し、**左矢印** <- を選択します。すべてのユーザとグループを削除するには、「**すべて削除**」を選択します。

4 適宜、以下の操作を行います。

- グループの追加を終了するには、「**OK**」を選択します。
- VPN アクセスを指定するには、「VPN アクセス (256 ページ)」に進みます。

VPN アクセス

1 「**VPN アクセス**」を選択します。

2 「**アクセス不可**」リストから、このグループに既定で VPN アクセスを許可するネットワーク リソースを選択します。

> **メモ**：GroupVPN アクセス設定は、リモート クライアントおよび SSL VPN 仮想オフィスブックマークに影響します。

3 **右矢印 ->**を選択して、リソースを「**アクセス許可**」リストに追加します。

リソースを削除するには、「**アクセス許可**」から、リソースを選択し、**左矢印 <-** を選択します。すべてのリソースを削除するには、「**すべて削除**」を選択します。

4 適宜、以下の操作を行います。

- グループの追加を終了するには、「**OK**」を選択します。
- ブックマークを指定するには、「ブックマーク (257 ページ)」に進みます。

ブックマーク

1 「**ブックマーク**」を選択します。

2 関係するグループに所属する各ユーザについて、仮想オフィス ブックマークを追加、編集、削除することができます。SSL VPN ブックマークの設定方法については、*SonicOS 6.5 接続*を参照してください。

> **メモ**：ユーザがブックマークを自ら設定するためには、SSL VPN サービス グループのメンバーである必要があります。

3 適宜、以下の操作を行います。

- グループの追加を終了するには、「**OK**」を選択します。
- グループに管理者権限を持たせるかどうかを指定するには、「管理 (258 ページ)」に進みます。

管理

1 「**管理**」を選択します。

2 別の管理グループへのメンバーシップを与えて新しいグループを管理グループにする場合は、「**メンバーはウェブ ログインで管理 UI に直にアクセスする**」を選択します。このオプションは、既定では選択されていません。

3 「**このグループが読み取り専用管理者権限を付与し、他の管理グループと共に使用された場合**」オプションは、読み取り専用管理者権限を付与するユーザ グループ (つまり、SonicWall Read-Only Admins グループまたはそのメンバーシップを持つグループ) のメンバーシップを取得したユーザがさらに別の管理ユーザ グループのメンバーシップを取得した場合の処理方法を制御します。ユーザに次の権限を与えるには、以下の操作を行います。

- 読み取り専用の制限なしで他の管理グループによって設定された管理者権限を付与する場合は、「**他のグループの管理者権限がこれに優先する (読み取り専用制限なし)**」を選択します。このオプションを使うと、ユーザの既定のグループを読み取り専用管理グループとしておき、その中の特定のユーザだけを他の管理グループのメンバーにして読み取り専用の権限をオーバーライドすれば、それらのユーザが設定を行えるようになります。このオプションは、既定では選択されています。「**ローカル ユーザ**」テーブルのユーザの「**管理**」列に、他のグループを識別する指示語 (*制限*、*"完全"* など) が表示されます。
- 他のグループによって設定された管理者権限レベルをメンバー ユーザに付与し、アクセスを読み取り専用に制限する場合は、「**他のグループの管理者権限が読み取り専用に制限される**」をオンにします。「**ローカル ユーザ**」テーブルのユーザの「**管理**」列に、2 つの他のグループを識別する指示語 (*"読み取り専用の制限された"* など) が表示されます。

  ヒント：両方を混在させるには、SonicWall Read-Only Admins で最初のオプションを選択し、そのメンバーとなる別のグループを作成して 2 番目のオプションを選択します (*逆ではうまくいきません*)。

  メモ：読み取り専用管理グループのメンバーで、かつ他の管理グループに所属していないユーザには、読み取り専用に制限された (SonicWall Administrators の) 完全なアクセス権が付与されます。

4 「**OK**」を選択してユーザ設定を完了します。

ローカル グループの編集

ローカル グループを編集するには、以下の手順を実行します。

1 編集したいグループの「**編集**」アイコンを選択します。「グループの編集」ダイアログが表示されます。このダイアログの内容は「グループの追加」ダイアログと同様です。

2 「ローカル グループの追加 (252 ページ)」の手順を実行します。

LDAP からのローカル グループのインポート

既存の LDAP/AD ユーザ グループと同じ名前のユーザ グループが SonicOS にあれば、LDAP 認証に成功したときに SonicWall のグループ メンバーシップおよび権限が与えられます。LDAP サーバからユーザ グループ名を取得することにより、SonicOS 上でローカル ユーザ グループを設定できます。ローカル グループのインポートの詳細については、「「ユーザとグループ」ページ (170 ページ)」を参照してください。

LDAP 位置によるユーザ メンバーシップの設定

LDAP サーバ上の特定の組織単位 (OU) に配置されているユーザに対して LDAP のルールやポリシーを設定できます。組織単位別 LDAP グループ メンバーシップの詳細については、「組織単位別 LDAP グループ メンバーシップ (98 ページ)」を参照してください。新規のメンバーを作成する詳細な手順については、「RADIUS ユーザ用の新しいユーザ グループの作成 (159 ページ)」を参照してください。

11

ゲスト サービスとゲスト アカウント

トピック:

- ユーザ > ゲスト サービス (260 ページ)
  - グローバル ゲスト設定 (261 ページ)
  - ゲスト プロファイル (261 ページ)

ユーザ > ゲスト サービス

ゲスト アカウントとは、ユーザがネットワークにログインするための一時的なアカウントです。これらのアカウントは、必要に応じて手動で作成するか、バッチで生成できます。SonicOS には、ゲスト アカウントの設定を前もって行うためのプロファイルがあります。プロファイルを使用することで、ゲスト アカウントを生成する際の設定を自動化できます。一般的に、ゲスト アカウントには有効期限が設定されます。既定では、有効期限が切れた後にアカウントは削除されます。

「ゲスト サービス」では、ゲスト アカウントの制限と設定を定義します。「**管理 | システム セットアップ > ユーザ > ゲスト サービス**」ページには、ゲスト プロファイルのリストが表示されます。ゲスト プロファイルは、ゲスト アカウントを生成する際に使用する設定を定義します。「**ユーザ > ゲスト サービス**」では、ゲスト プロファイルを追加、削除、設定できます。また、セキュリティ装置にログインしたすべてのユーザに対して、現在のログイン セッションの残り時間が示されるログイン ウィンドウを表示するかどうかを設定できます。

トピック:

- グローバル ゲスト設定 (261 ページ)
- ゲスト プロファイル (261 ページ)

グローバル ゲスト設定

「グローバル ゲスト設定」セクションには、ログイン状況ウィンドウを表示するオプションがあります。ウィンドウには、現在のセッションの残り時間が表示されます。ユーザは、ログイン セッションの間、このウィンドウを開いたままにしておく必要があります。また、ログイン状況ウィンドウ内の「**ログアウト**」を選択することにより、ログアウトできます。

ゲスト ログイン状況ウィンドウを設定するには、以下の手順に従います。

1 「**ログアウト付きゲスト ログイン状況ウィンドウを表示する**」を選択して、ユーザがログインするたびにユーザのログイン ウィンドウに「**ログアウト**」が表示されるようにします。このオプションは既定で選択されています。

2 「**適用**」を選択します。

ゲスト プロファイル

「**ゲスト プロファイル**」テーブルには、作成済みのプロファイルが表示されます。このテーブルで、こうしたプロファイルの追加、編集、削除を行うことができます。「**既定**」というゲスト プロファイルは常に存在します。このプロファイルは SonicOS によって生成されたもので、編集できますが削除はできません。

トピック:

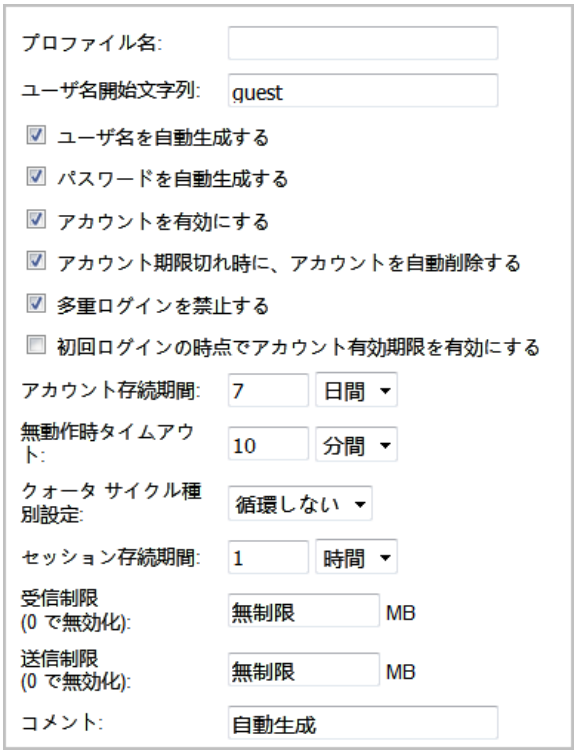
- ゲスト プロファイルの追加 (261 ページ)
- ゲスト プロファイルの編集 (264 ページ)
- ゲスト プロファイルの削除 (264 ページ)

ゲスト プロファイルの追加

プロファイルを追加するには、次の手順に従います。

1 「**管理 | システム セットアップ > ユーザ > ゲスト サービス**」に移動します。

2 「**ゲスト プロファイル**」テーブルの下にある「**追加**」を選択します。「**ゲスト プロファイルの追加**」ダイアログが表示されます。



3 「**プロファイル名**」フィールドに、プロファイルの名前を入力します。

4 「**ユーザ名開始文字列**」フィールドに、このプロファイルから生成される各ユーザ アカウント名の最初の部分を入力します。このプロファイルから生成されるゲスト アカウントのユーザ名を自動生成するには、「**ユーザ名を自動生成する**」を選択します。通常、ユーザ名開始文字列に 2 または 3 桁の数字を付加した文字列がユーザ名となります。このオプションは、既定では選択されています。

5 このプロファイルから生成されるゲスト アカウントのパスワードを自動生成するには、「**パスワードを自動生成する**」を選択します。生成されるパスワードは、一意な 8 文字の英字から構成される文字列です。このオプションは、既定では選択されています。

6 このプロファイルから生成されるすべてのゲスト アカウントを作成時に有効にするには、「**アカウントを有効にする**」を選択します。このオプションは、既定では選択されています。

7 アカウントの有効期限が切れたときに、アカウントをデータベースから削除するには、「**アカウント期限切れ時に、アカウントを自動削除する**」を選択します。このオプションは、既定では選択されています。

8 任意の時点でアカウントの単一のインスタンスのみを使用できるようにするには、「**多重ログインを禁止する**」を選択します。既定では、新しいゲスト アカウントを作成するときに、この機能は有効になっています。単一のアカウントを使用して複数のユーザがログインできるようにする場合は、「**多重ログインを禁止する**」チェックボックスをオフにしてこの無効にします。

9 ユーザがアカウントに初回ログインするまで「アカウント存続期間」タイマーを遅延させるには、「**初回ログインの時点でアカウント有効期限を有効にする**」を選択します。このオプションは、既定では選択されていません。

10 アカウントの有効期限が切れるまで、セキュリティ装置上にアカウントを保持しておく期間を定義するには、「**アカウント存続期間**」にその期間を入力します。1 ～ 9999 の数値を「**アカウント存続期間**」フィールドに指定してドロップダウン メニューから期間の種別を選択できます。

- **分**
- **時間**
- **日**

既定値は **7 日間** です。

11 アクティブ化されたゲスト サービス セッションでトラフィックが受け渡しされない期間の最大時間を定義するには、「**無動作時タイムアウト**」にタイムアウト時間を入力します。この設定で定義した期間を過ぎるとセッションの有効期限が切れますが、アカウント自体は「**アカウント存続期間**」まではアクティブのままです。「**無動作時タイムアウト**」の値は、「**セッション存続期間**」で設定された値よりも大きくすることはできません。

1 ～ 9999 の数値を「**アカウント存続期間**」フィールドに指定してドロップダウン メニューから期間の種別を選択できます。

- **分**
- **時間**
- **日**

既定値は **10 分**です。

12 クォータ サイクル種別設定を指定する場合は、「**クォータ サイクル種別設定**」ドロップダウン メニューから選択します。

- **循環しない** (既定)
- **1 日ごと**
- **1 週間ごと**
- **1 か月ごと**

13 ゲスト ログイン セッションがアクティブになった後、アクティブであり続ける期間を定義するには、「**セッション存続期間**」にその期間を指定します。既定では、アクティブ化はゲスト ユーザが最初にアカウントにログインするときに行われます。「**セッション存続期間**」には、「**アカウント存続期間**」より長い値を設定することはできません。

1 ～ 9999 の数値を「**セッション存続期間**」フィールドに指定してドロップダウン メニューから期間の種別を選択できます。

- **分**
- **時間**
- **日**

既定値は **1 時間** です。

14 ユーザが受信できるデータ量を制限するには、「**受信制限 (0 で無効化)**」フィールドにその量を MB 単位で入力します。範囲は 0 (データを一切受信できない) ～ 999999999 MB および「**無制限**」 (既定) です。

15 ユーザが送信できるデータ量を制限するには、「**送信制限 (0 で無効化)**」フィールドにその量を MB 単位で入力します。範囲は 0 (データを一切受信できない) ～ 999999999 MB および「**無制限**」 (既定) です。

16 必要に応じて、「**コメント**」フィールドに、わかりやすいコメントを入力します。既定は 「**自動生成**」 です。

17 「**OK**」を選択します。

ゲスト プロファイルの編集

ゲスト プロファイルを編集するには、以下の手順に従います。

1 プロファイルの「**設定**」列で**編集**アイコンを選択します。

2 「ゲスト プロファイルの追加 (261 ページ)」の手順を実行します。

> **メモ：**「**既定**」プロファイルを編集する際には、「**プロファイル名**」と「**ユーザ名開始文字列**」(これらのオプションはグレーアウトされています) を除くすべてのオプションを編集できます。

ゲスト プロファイルの削除

「**既定**」プロファイルを除くすべてのゲスト プロファイルを削除できます。

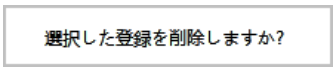
ゲスト プロファイルを削除するには、以下の手順に従います。

1 以下のどちらかを選択してください。

- 削除するゲスト プロファイルのチェックボックス。
- 「**ゲスト プロファイル**」テーブルにある該当するチェックボックス。(「**既定**」プロファイルを除く) すべてのチェックボックスがオンになります。

「**削除**」が使用可能になります。

2 「**削除**」を選択します。確認メッセージが表示されます。



3 「**OK**」を選択します。

12

ゲスト アカウントの管理

トピック:

- ユーザ > ゲスト アカウント (265 ページ)
  - ゲスト アカウント統計の表示 (266 ページ)
  - ゲスト アカウントの追加 (268 ページ)
  - ゲスト アカウントの有効化 (274 ページ)
  - ゲスト アカウントの自動削除の有効化 (274 ページ)
  - アカウント詳細の印刷 (275 ページ)

ユーザ > ゲスト アカウント

「**管理 | システム セットアップ | ユーザ > ゲスト アカウント**」には、SonicWall セキュリティ装置上のゲスト サービス アカウントがリストされます。個々のアカウント、アカウントのグループ、またはすべてのアカウントを有効化/無効化する、アカウントの自動削除機能を設定する、アカウントまたはセッションの失効日時を設定する、またはアカウントの追加、編集、削除、印刷を行うことができます。

トピック:

- ゲスト アカウント統計の表示 (266 ページ)
- ゲスト アカウントの追加 (268 ページ)
- ゲスト アカウントの有効化 (274 ページ)
- ゲスト アカウントの自動削除の有効化 (274 ページ)
- アカウント詳細の印刷 (275 ページ)

ゲスト アカウント統計の表示

「**ゲスト アカウント**」テーブルには、ゲスト アカウントに関する統計が表示されます。

トピック:

- トラフィック統計の表示 (266 ページ)
- アカウント有効期限の表示 (266 ページ)
- セッション有効期限の表示 (267 ページ)
- 受信および送信制限統計の表示 (267 ページ)
- ゲスト アカウントのエクスポート (267 ページ)

トラフィック統計の表示

ゲスト アカウントのトラフィック統計を表示するには、以下の手順に従います。

1 ゲスト アカウントの「**統計**」列にある**統計**アイコンの上にマウス ポインタを置きます。「**トラフィック統計**」ポップアップに、完了したすべてのセッションで送受信された累積バイト数およびパケット数が表示されます。現在アクティブなセッションでの送受信データについては、ゲスト ユーザがログアウトするまでこの統計には加算されません。

アカウント有効期限の表示

アカウントが期限切れになるまでの残り時間を表示するには、以下の手順に従います。

1 ゲスト アカウントの「**アカウント有効期限**」列にある**時計**アイコンの上にマウス ポインタを置きます。「**アカウント有効期限**」ポップアップにゲスト アカウントの残り時間が表示されます。

セッション有効期限の表示

セッションが期限切れになるまでの残り時間を表示するには、以下の手順に従います。

1 ゲスト アカウントの「**アカウント有効期限**」列にある**時計**アイコンの上にマウス ポインタを置きます。「**アカウント有効期限**」ポップアップにゲスト アカウントの残り時間が表示されます。

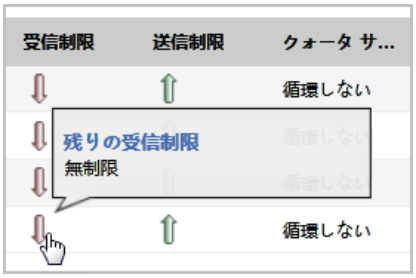
メモ：ユーザのセッションが開始されていない場合、「**セッション有効期限**」ポップアップには「未使用」と表示されます。

受信および送信制限統計の表示

テーブル内のユーザ アカウント毎に、「**受信制限**」列に赤色の下矢印アイコン、「**送信制限**」列に緑色の上矢印アイコンが表示されます。

受信/送信制限の統計を表示するには、以下の手順に従います。

1 ゲスト アカウントの「**受信制限/送信制限**」列にある**矢印**アイコンの上にマウス ポインタを置きます。「**残り受信クォータ/残り送信クォータ**」ポップアップに、ゲスト ユーザがダウンロードまたは送信できる残りデータ量が表示されます。



ゲスト アカウントのエクスポート

「**ゲスト アカウント**」テーブルは .csv ファイルとしてエクスポートできます。このファイルには、表示されるすべてのデータだけでなく、受信および送信データの制限や残りデータ量に関する統計も含まれます。

ゲスト アカウントを .csv ファイルとしてエクスポートするには、以下の手順に従います。

1 「**ゲスト アカウント**」テーブルで、「**エクスポート**」を選択します。「***guestaccounts_nnn*.csv を開く**」ダイアログが表示されます。

2 次の操作が可能です。
   - ファイルを開いて表示します。
   - ファイルを後で使用できるように保存します。
3 「**OK**」を選択します。

ゲスト アカウントの追加

ゲスト アカウントを個別に追加することも、複数のゲスト アカウントを自動的に生成することもできます。

トピック:

- ゲスト アカウントの追加 (268 ページ)
- 複数ゲスト アカウントの生成 (271 ページ)

ゲスト アカウントの追加

アカウントを個別に追加するには、次の手順に従います。

1 「**管理 | システム セットアップ > ユーザ > ゲスト アカウント**」に移動します。
2 「**ゲスト アカウント**」テーブルで、「**ゲストの追加**」を選択します。「**ゲストの追加**」ダイアログが表示されます。

3 「**プロファイル**」で、このアカウントの生成に使用するゲスト プロファイルを選択します。既定のプロファイルは「**既定**」です。

4 以下のいずれかの方法でゲスト アカウントに名前を付けます。

- 「**名前**」フィールドにアカウントの名前を入力します。
- 「**生成**」を選択して SonicOS による名前の生成を行います。生成される名前は、プロファイルの名、"guest" という文字列、ランダムな 2 ～ 5 桁の数字をつなげたものになります。以下に例を示します。
  - guest1235 (既定のプロファイルの場合)
  - TechPubs guest51026 (TechPubs ゲスト プロファイルの場合)

5 「**コメント**」フィールドに、わかりやすいコメントを入力します。既定のコメントは「**自動生成**」です。

6 以下のいずれかの方法でユーザ アカウントのパスワードを作成します。

- 「**パスワード**」フィールドと「確認」フィールドにパスワードを入力します。パスワードは最大 32 文字の英数字です。
- 「**生成**」を選択します。生成されるパスワードは、ランダムな 8 文字の英字から構成される文字列です。

  ヒント：パスワードは記録してください。忘れた場合には、パスワードをリセットする必要があります。

7 「**ゲスト サービス**」を選択します。

8 作成してすぐに有効にするアカウントについては、「**ゲスト サービスの権限を有効にする**」を選択します。このオプションは、既定では選択されています。

9 セキュリティ装置にログインするために同時に使用できるこのアカウントのインスタンスの数を 1 つに制限するには、「**多重ログインを禁止する**」を選択します。選択しないと、同時に複数のユーザがこのアカウントを使用できます。このオプションは、既定では選択されています。

10 アカウントの有効期限が切れたときに、アカウントをデータベースから削除するには、「**アカウント期限切れ時に、アカウントを自動削除する**」を選択します。このオプションは、既定では選択されています。

11 アカウント有効期限のカウントを開始するには、「**初回ログインの時点でアカウント有効期限を有効にする**」を選択します。

12 アカウントがセキュリティ装置上に保持される、期限切れになるまでの期間を定義するには、「**アカウント有効期限**」にその期間を入力します。1 ～ 9999 の数値を「**アカウント有効期限**」フィールドに指定してドロップダウン メニューから期間の種別を選択できます。

- **分**
- **時間**
- **日**

既定値は **7 日間** です。

「**アカウント期限切れ時に、アカウントを自動削除する**」を

- 有効にすると、アカウントは有効期限が切れたときに削除されます。
- 無効にすると、アカウントは、簡単に再びアクティブにできるように「**失効**」状態で「**ゲスト アカウント**」テーブルに残ります。

> **メモ**：この設定は、「ゲスト プロファイル (261 ページ)」でのアカウント有効期限の設定より優先されます。

13 アクティブ化されたゲスト サービス セッションでトラフィックが受け渡しされない期間の最大時間を定義するには、「**無動作時タイムアウト**」にタイムアウト時間を入力します。この設定で定義した期間を過ぎるとセッションの有効期限が切れますが、アカウント自体は「**アカウント存続期間**」まではアクティブのままです。「**無動作時タイムアウト**」の値は、「**セッション存続期間**」で設定された値よりも大きくすることはできません。

> **メモ**：この設定は、プロファイルでの無動作時タイムアウトの設定より優先されます。

1 ～ 9999 の数値を「**アカウント存続期間**」フィールドに指定してドロップダウン メニューから期間の種別を選択できます。

- **分**
- **時間**
- **日**

既定値は **10 分**です。

14 クォータ サイクル種別設定を指定する場合は、「**クォータ サイクル種別設定**」ドロップダウン メニューから選択します。

- **循環しない** (既定)
- **1 日ごと**
- **1 週間ごと**
- **1 か月ごと**

15 ゲスト ログイン セッションがアクティブになった後、アクティブであり続ける期間を定義するには、「**セッション存続期間**」にその期間を指定します。既定では、アクティブ化はゲスト ユーザが最初にアカウントにログインするときに行われます。「**セッション存続期間**」には、「**アカウント存続期間**」より長い値を設定することはできません。

> **メモ**：この設定は、プロファイルでのセッション有効期限の設定より優先されます。

1 ～ 9999 の数値を「**セッション存続期間**」フィールドに指定してドロップダウン メニューから期間の種別を選択できます。

- **分**
- **時間**
- **日**

既定値は **1 時間** です。

16 **受信制限 (0 で無効化)**: ユーザに受信を許可するメガバイト数を入力します。最小値の 0 を指定すると制限が無効化されます。最大は「**無制限**」 (既定値) です。

17 **送信制限 (0 で無効化)**: ユーザに送信を許可するメガバイト数を入力します。最小値の 0 を指定すると制限が無効化されます。最大は「**無制限**」 (既定値) です。

18 ユーザが受信できるデータ量を制限するには、「**受信制限 (0 で無効化)**」フィールドにその量を MB 単位で入力します。範囲は 0 (データを一切受信できない) ～ 999999999 MB および「**無制限**」 (既定) です。

19 ユーザが送信できるデータ量を制限するには、「**送信制限 (0 で無効化)**」フィールドにその量を MB 単位で入力します。範囲は 0 (データを一切受信できない) ～ 999999999 MB および「**無制限**」 (既定) です。

20 「**OK**」を選択して、アカウントを生成します。

複数ゲスト アカウントの生成

複数のアカウントを生成するには、次の手順に従います。

1 「**管理 | システム セットアップ > ユーザ > ゲスト アカウント**」に移動します。

2 「**ゲスト アカウント**」テーブルで、「**生成**」を選択します。「**ゲスト アカウントの生成**」ダイアログが表示されます。

3 「**プロファイル**」で、このアカウントの生成に使用するゲスト プロファイルを選択します。既定は「**既定**」です。

4 「**アカウント数**」フィールドに生成するアカウントの数を入力します。1 ～ 6000 個のアカウントを作成できます。

5 「**ユーザ名開始文字列**」フィールドにアカウント名の生成に使用する開始文字列を入力します。例えば、"**Guest**" と入力した場合、生成されるアカウント名は、`Guest123`、`Guest234` のようになります。既定の開始文字列は **guest** です。

6 「**コメント**」フィールドに、わかりやすいコメントを最大 16 文字の英数字で入力します。

7 「**ゲスト サービス**」を選択します。

8 作成してすぐに有効にするアカウントについては、「**ゲスト サービスの権限を有効にする**」を選択します。このオプションは、既定では選択されています。

9 セキュリティ装置にログインするために同時に使用できるこのアカウントのインスタンスの数を 1 つに制限するには、「**多重ログインを禁止する**」を選択します。選択しないと、同時に複数のユーザがこのアカウントを使用できます。このオプションは、既定では選択されています。

10 アカウントの有効期限が切れたときに、アカウントをデータベースから削除するには、「**アカウント期限切れ時に、アカウントを自動削除する**」を選択します。このオプションは、既定では選択されています。

メモ：この設定は、ゲスト プロファイルでの自動削除の設定が優先されます (2 つの設定が異なる場合)。

11 アカウント有効期限のカウントを開始するには、「**初回ログインの時点でアカウント有効期限を有効にする**」を選択します。

12 アカウントがセキュリティ装置上に保持される、期限切れになるまでの期間を定義するには、「**アカウント有効期限**」にその期間を入力します。1 ～ 9999 の数値を「**アカウント有効期限**」フィールドに指定してドロップダウン メニューから期間の種別を選択できます。

- **分**
- **時間**
- **日**

既定値は **7 日間** です。

「**アカウント期限切れ時に、アカウントを自動削除する**」を

- 有効にすると、アカウントは有効期限が切れたときに削除されます。

- 無効にすると、アカウントは、簡単に再びアクティブにできるように「**失効**」状態で「**ゲスト アカウント**」テーブルに残ります。

  メモ：この設定は、「ゲスト プロファイル (261 ページ)」でのアカウント有効期限の設定より優先されます。

13 アクティブ化されたゲスト サービス セッションでトラフィックが受け渡しされない期間の最大時間を定義するには、「**無動作時タイムアウト**」にタイムアウト時間を入力します。この設定で定義した期間を過ぎるとセッションの有効期限が切れますが、アカウント自体は「**アカウント存続期間**」まではアクティブのままです。「**無動作時タイムアウト**」の値は、「**セッション存続期間**」で設定された値よりも大きくすることはできません。

メモ：この設定は、プロファイルでの無動作時タイムアウトの設定より優先されます。

1 ～ 9999 の数値を「**アカウント存続期間**」フィールドに指定してドロップダウン メニューから期間の種別を選択できます。

- **分**
- **時間**
- **日**

既定値は **10 分**です。

14 クォータ サイクル種別設定を指定する場合は、「**クォータ サイクル種別設定**」ドロップダウン メニューから選択します。

- **循環しない** (既定)
- **1 日ごと**
- **1 週間ごと**
- **1 か月ごと**

15 ゲスト ログイン セッションがアクティブになった後、アクティブであり続ける期間を定義するには、「**セッション存続期間**」にその期間を指定します。既定では、アクティブ化はゲスト ユーザが最初にアカウントにログインするときに行われます。「**セッション存続期間**」には、「**アカウント存続期間**」より長い値を設定することはできません。

メモ：この設定は、プロファイルでのセッション有効期限の設定より優先されます。

1 ～ 9999 の数値を「**セッション存続期間**」フィールドに指定してドロップダウン メニューから期間の種別を選択できます。

- **分**
- **時間**
- **日**

既定値は **1 時間** です。

16 **受信制限 (0 で無効化)**: ユーザに受信を許可するメガバイト数を入力します。最小値の 0 を指定すると制限が無効化されます。最大は「**無制限**」 (既定値) です。

17 **送信制限 (0 で無効化)**: ユーザに送信を許可するメガバイト数を入力します。最小値の 0 を指定すると制限が無効化されます。最大は「**無制限**」 (既定値) です。

18 ユーザが受信できるデータ量を制限するには、「**受信制限 (0 で無効化)**」フィールドにその量を MB 単位で入力します。範囲は 0 (データを一切受信できない) ～ 999999999 MB および「**無制限**」 (既定) です。

19 ユーザが送信できるデータ量を制限するには、「**送信制限 (0 で無効化)**」フィールドにその量を MB 単位で入力します。範囲は 0 (データを一切受信できない) ～ 999999999 MB および「**無制限**」 (既定) です。

20 「**OK**」を選択して、アカウントを生成します。

ゲスト アカウントの有効化

複数のアカウントを一度に有効/無効にすることができます。

1 つまたは複数のゲスト アカウントを有効にするは、以下の手順に従います。

1 有効にするアカウントの名前の横にある「**有効**」列のチェックボックスをオンにします。すべてのアカウントを有効にするには、テーブル見出しの「**有効**」チェックボックスをオンにします。

2 「**適用**」を選択します。

ゲスト アカウントの自動削除の有効化

複数のアカウントの自動削除機能を一度に有効/無効にすることができます。アカウントの自動削除が有効な場合、アカウントは有効期限が切れた後に削除されます。

メモ：これは、ユーザ プロファイルまたはゲスト アカウントの設定時にセットされた自動削除オプションよりも優先されます。

自動削除を有効にするには、以下の手順に従います。

1 アカウントの名前の横にある「**自動削除**」列のチェックボックスをオンにします。すべてのアカウントで有効にするには、テーブル見出しの「**自動削除**」チェックボックスをオンにします。

2 「**適用**」を選択します。

ゲスト アカウントの編集

ゲスト アカウントを編集するには、以下の手順に従います。

1 プロファイルの「**設定**」列で**編集**アイコンを選択します。

2 「ゲスト プロファイルの追加 (261 ページ)」の手順を実行します。

メモ：「**既定**」プロファイルを編集する際には、「**プロファイル名**」と「**ユーザ名開始文字列**」 (これらのオプションはグレーアウトされています) を除くすべてのオプションを編集できます。

ゲスト アカウントの削除

「**既定**」プロファイルを除くすべてのゲスト プロファイルを削除できます。

ゲスト アカウントを削除するには、以下の手順に従います。

1 ゲスト アカウントの**削除**アイコンを選択します。確認メッセージが表示されます。

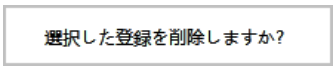
2 「**OK**」を選択します。

1 つまたは複数のゲスト アカウントを削除するには、以下の手順に従います。

1 「**管理 | システム セットアップ | ユーザ > ローカル ユーザとグループ**」に移動します。

2 削除するゲスト プロファイルのチェックボックスをオンにします。「**削除**」が使用可能になります。

3 「**削除**」を選択します。確認メッセージが表示されます。

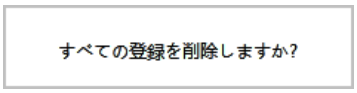


4 「**OK**」を選択します。

すべてのゲスト アカウントを削除するには、以下の手順に従います。

1 「**ゲスト アカウント**」テーブルのヘッダーにあるチェックボックスをオンにします。(「**既定**」プロファイルを除く) すべてのチェックボックスがオンになります。「**すべて削除**」が使用可能になります。

2 「**すべて削除**」を選択します。確認メッセージが表示されます。



3 「**OK**」を選択します。

アカウント詳細の印刷

ゲスト アカウントの概要情報を印刷することができます。

ゲスト アカウントの詳細を印刷するには、以下の手順に従います。

1 **印刷**アイコンを選択すると、アカウントの概要レポートと「**印刷**」ダイアログが表示されます。

ゲスト アカウント詳細

説明	値
アカウント名:	guest37890
パスワード:	freuibos
有効化:	有
コメント:	admin
作成:	FRI OCT 27 17:19:07 2017
アカウント有効期限:	FRI NOV 03 17:19:07 2017
セッション有効期限:	未使用
セッション存続期間:	1 時
無動作時タイムアウト:	10 分
受信制限:	無制限
送信制限:	無制限
クォータ サイクル:	循環しない

2 「**OK**」を選択して、概要レポートをプリンターに送信します。

第 4 部

システム セットアップ | ネットワーク

- インターフェースの設定
- PortShield インターフェースの設定
- PoE の設定
- フェイルオーバーと負荷分散の セットアップ
- ネットワーク ゾーンの設定
- ワイヤ モード VLAN 変換の設定
- DNS の設定
- DNS プロキシの設定
- DNS セキュリティの設定
- ルート通知とルート ポリシーの設定
- ARP トラフィックの管理
- 近隣者発見プロトコルの設定
- MAC-IP アンチスプーフの設定
- DHCP サーバのセットアップ
- IP ヘルパーの使用
- ウェブ プロキシ転送のセットアップ
- 動的 DNS の設定
- AWS 資格情報の設定

13

インターフェースの設定

トピック:

- インターフェースについて (279 ページ)
  - 物理インターフェースと仮想インターフェース (279 ページ)
  - SonicOS のセキュリティ保護されるオブジェクト (283 ページ)
  - トランスペアレント モード (283 ページ)
  - IPS スニッファ モード (283 ページ)
  - Firewall Sandwich (286 ページ)
  - HTTP/HTTPS リダイレクト (286 ページ)
  - インターフェースでの DNS プロキシの有効化 (287 ページ)
- ネットワーク > インターフェース (287 ページ)
  - PortShield インターフェースの表示/非表示 (IPv4 のみ) (289 ページ)
  - インターフェース設定 (290 ページ)
  - インターフェース トラフィック統計 (291 ページ)
- インターフェースの設定 (292 ページ)
  - 静的インターフェースの設定 (293 ページ)
  - ルート モードの設定 (300 ページ)
  - インターフェースでの帯域幅管理の有効化 (301 ページ)
  - インターフェースのトランスペアレント IP モード (L3 サブネットを結合) の設定 (303 ページ)
  - 無線インターフェースの設定 (307 ページ)
  - WAN インターフェースの設定 (313 ページ)
  - トンネル インターフェースの設定 (318 ページ)
  - リンク統合化とポート冗長化の設定 (323 ページ)
  - 仮想インターフェース (VLAN サブインターフェース) (327 ページ)
  - IPS スニッファ モードの設定 (328 ページ)
  - セキュリティ サービス (統合脅威管理) の設定 (332 ページ)
  - ワイヤ モードとタップ モードの設定 (333 ページ)
  - ワイヤ モードでのリンク統合 (337 ページ)
  - レイヤ 2 ブリッジ モード (339 ページ)

- レイヤ 2 ブリッジ モードの設定 (360 ページ)
- 非対称ルーティング (368 ページ)
- インターフェースの IPv6 設定 (369 ページ)
- 31 ビット ネットワーク (369 ページ)
- PPPoE アンナンバード インターフェースのサポート (371 ページ)

インターフェースについて

- 物理インターフェースと仮想インターフェース (279 ページ)
- SonicOS のセキュリティ保護されるオブジェクト (283 ページ)
- トランスペアレント モード (283 ページ)
- IPS スニッファ モード (283 ページ)
- Firewall Sandwich (286 ページ)
- HTTP/HTTPS リダイレクト (286 ページ)
- インターフェースでの DNS プロキシの有効化 (287 ページ)

物理インターフェースと仮想インターフェース

SonicOS のインターフェースは大きく次のように分けられます。

- **物理インターフェース** - 物理インターフェースは、単一のポートにバインドされます。
- **仮想インターフェース** - 仮想インターフェースは、サブインターフェースとして物理インターフェースに割り当てられ、複数のインターフェースに割り当てられたトラフィックを物理インターフェースが搬送できるようにします。

トピック:

- 物理インターフェース (279 ページ)
- 仮想インターフェース (VLAN) (281 ページ)
- サブインターフェース (282 ページ)

物理インターフェース

SonicWall セキュリティ装置のフロント パネルには多くの物理インターフェースがあります。インターフェースの数と種類は装置のモデルとバージョンによって異なります (お使いの装置のインターフェースの詳細は、関連する『*導入ガイド*』を参照してください)。

物理インターフェース (モデル番号別)

インターフェース ポート		コメント
1 GE	高速銅線ギガビット イーサネット ポート	NS*a* 2600 シリーズ以降と SuperMassive シリーズのみ
1 GE SFP	ホットプラグ可能な 1 ギガビット イーサネット SFP インターフェース	NS*a* 3600 シリーズ以降と SuperMassive シリーズのみ
2.5/1	GE 銅線ポート	NS *a* 2650/3650/4650/5650 のみ
2.5/1	GE SFP ポート	NS *a* 2650/3650/4650/5650 のみ
10/5/2.5	GE 銅線ポート	NS *a* 2650/3650/4650/5650 のみ
10 GE SFP+	ホットプラグ可能な 10 ギガビット ポート	NS*a* 3600 シリーズ以降と SuperMassive 9000 シリーズのみ。詳細は、「NSA 6600 および SuperMassive 9000 シリーズの 10 ギガビット イーサネット SFP+ ポート (280 ページ)」を参照してください。
10/5/2.5 GE SFP+	10/5/2.5 ギガビット ホットプラグ対応ポート	NS *a* 2650/3650/4650/5650 のみ
MGMT	1 ギガビット イーサネット管理インターフェース ポート (装置のファームウェアをセーフモードで安全にアップグレードするために使用)。MGMT ポートを用いてファームウェアをセーフモードでアップグレードする方法については、『*SonicOS 6.0 アップグレード ガイド*』を参照してください。MGMT ポートの既定の IP アドレスは `192.168.1.254` です。	

物理インターフェースは、送受信トラフィックを規定するアクセス ルールの設定が可能なゾーンに割り当てる必要があります。セキュリティ ゾーンは、送受信トラフィックの経路として動作する各物理インターフェースにバインドされます。インターフェースがなければ、トラフィックはゾーンにアクセスしたり、ゾーンを出ていくことができません。

ゾーンの詳細については、「ゾーンについて (422 ページ)」を参照してください。

NSA 6600 および SuperMassive 9000 シリーズの 10 ギガビット イーサネット SFP+ ポート

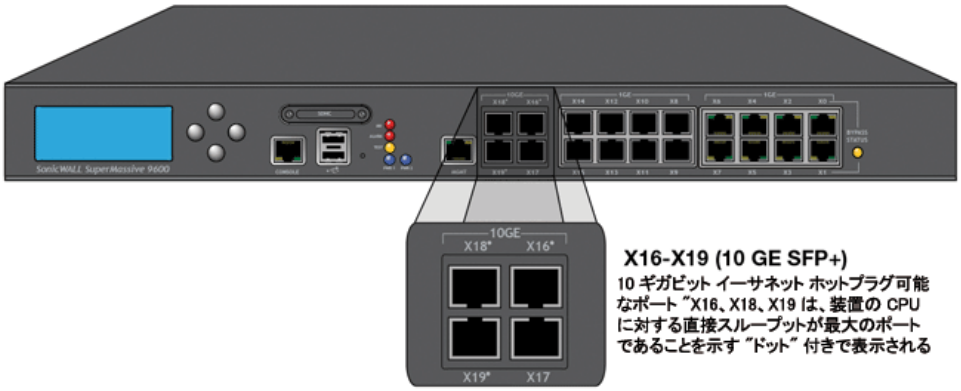
NSA 6600 および SuperMassive 9000 シリーズ装置では、強化された Small Form-Factor Pluggable (SFP+) ポートである X16、X18、および X19 は、CPU に対する直接スループットが最大であることを表すため、ドット付きで示されます。これらのドット付きポートには、CPU への専用 (非共有) アップリンクがあります。

これは、例えば 10Gb の企業ネットワーク バックボーンがあり、部門のゲートウェイ機器として SuperMassive 9200 を使用している場合に有益です。ドット付きポート (X16、X18、または X19) のいずれかをバックボーンに直接接続する必要があります。これらのポートは CPU からポートの接続先までを直接接続するので、最大限のアクセス速度が得られます。バックボーンへの接続で、ネットワーク上のユーザや他の機器と帯域幅を共有することは望ましくありません。最大の速度と効率を得るために、ドット付きポートはバックボーンに直接接続してください。

また、商業的に重要なリンクや、著しく多重化されているリンクもドット付きインターフェースに接続してください。商業的に重要なリンクの使用事例としては、管理部門による 10Gb バックボーン ネットワークへの接続があります。パフォーマンスを最大限に引き出すため、ドット付きインターフェースを介して上流のバックボーン接続を接続してください。これにより、CPU アップリンクを共有する、ドット付きでない他のインターフェース上の一時的な高負荷状況によって、重要なバックボーン トラフィックが失われることはなくなります。

著しく多重化されているリンクの使用事例としては、それぞれが 10Gb のアップリンクを持つ、多数の下流エンタープライズ スイッチがあります。パフォーマンスを最大限に引き出すため、ドット付きインターフェースを介して各スイッチを接続してください。これにより、高レベルの異なるスイッチング ドメインが CPU リソースを互いに奪い合うことはできなくなります。

10 ギガビット イーサネット ホットプラグ可能なポート



X17 インターフェースは、SonicOS 管理インターフェースにアスタリスク (*) マーク付きで表示されます。これは、このインターフェースがポート X0 ～ X15 と共有される共通スイッチング ドメインに接続され、そのため X17 は SonicOS 詳細スイッチング機能に参加できることを意味します。

仮想インターフェース (VLAN)

仮想インターフェースは、物理インターフェースに割り当てられたサブインターフェースであり、SonicWall セキュリティ装置でサポートされます。仮想インターフェースにより、1 つの物理接続で複数のインターフェースを使用できます。

仮想インターフェースは、ゾーンの割り当て、DHCP サーバ、NAT、アクセル ルールの管理など、物理インターフェースと同じ機能を数多く備えています。

仮想ローカル エリア ネットワーク (VLAN) は、IP ヘッダーのタグ付けを使用することで、単一の物理 LAN の中で複数の LAN をシミュレートできるため、“タグベースの LAN 多重テクノロジ"と表現できます。物理的に個別の、接続されていない 2 つの LAN は、互いに完全に分かれています。 2 つの異なる VLAN についても同様ですが、VLAN の場合、2 つの VLAN は、同じ回線上に存在できます。VLAN では、このような仮想化を実現する VLAN 対応のネットワーキング機器が必要です。 これらは、ネットワークの設計とセキュリティ ポリシーに従って VLAN タグ (ID) を認識、処理、削除、および挿入できるスイッチ、ルータ、およびファイアウォールです。

VLAN は多くのさまざまな理由で役立ちますが、その理由の多くは、VLAN が、物理的ではなく論理的なブロードキャスト ドメイン、つまり LAN 境界を提供できる機能に基づいています。これは、大きな物理 LAN を複数の小さな仮想 LAN に分割する場合と、物理的に異なる複数の LAN を論理的に連続する 1 つの仮想 LAN にまとめる場合の、両方に該当します。この利点は、以下のとおりです。

- **パフォーマンスの向上** - 論理的に分割された小さなブロードキャスト ドメインを作成することで、必要な送信先にのみブロードキャストを送信し、アプリケーション トラフィック用に多くの帯域幅を残せるため、ネットワーク全体の使用率が低下します。
- **コストの減少** - ブロードキャストのセグメント化は、かつてはルータで行われていたため、新たなハードウェアと設定が必要でした。VLAN では、ルータの機能的な役割は一変しました。 通信の抑制目的で使用されるのではなく、必要に応じて、異なる VLAN 間の通信を促進するために使用されます。
- **仮想ワークグループ** - ワークグループは、マーケティング部門やエンジニアリング部門など、一般に情報を共有する論理単位です。効率上の理由で、ブロードキャスト ドメイン境界は、このような機能ワークグループに対応するように作成する必要がありますが、それが常に可能であるとはかぎりません。エンジニアリング ユーザとマーケティング ユーザが建物の同じ階 (および同じワークグループ スイッチ) を共有していて、入り混じっていることもあれば、その逆にエンジニアリング チームが、構内全体に分散していることもあります。この状態を複雑な配線を駆使して解決するのはコストがかかり、絶えず行われる追加や移動を保守するのは不可能です。VLAN では、スイッチを簡単に再設定して、論理的なネットワーク配置をワークグループの要求に対応させることができます。
- **セキュリティ** - ある VLAN 上のホストは、別の VLAN 上のホストと、両者間の通信を促進するネットワーク機器がなければ通信できません。

サブインターフェース

SonicOS の VLAN サポートは、物理インターフェースの下にネストされる論理インターフェースである、サブインターフェースを使用して実現されます。一意のタグごとに、独自のサブインターフェースが必要です。セキュリティと管理上の理由で、SonicOS は VLAN トランク プロトコルに対応していません。 代わりに、サポートされる各 VLAN を設定し、適切なセキュリティ機能を割り当てる必要があります。

メモ：VLAN ID の範囲は 0 ～ 4094 です。 ただし、VLAN 0 は QoS 用に予約されており、VLAN 1 はネイティブ VLAN 指定用に一部のスイッチに予約されています。

メモ：ファイアウォールに接続している他の機器からのトランク リンクで、VTP (VLAN Trunking Protocol) や GVRP (Generic VLAN Registration Protocol) などの動的な VLAN トランク プロトコルを使用しないでください。

VLAN ケーブル スイッチからのトランク リンクは、関連する VLAN ID をファイアウォール上のサブインターフェースとして宣言し、それらを、物理インターフェースを設定する方法とほぼ同じ方法で設定することにより、サポートされます。言い換えると、サブインターフェースとして定義された VLAN だけがファイアウォールによって処理され、それ以外は対象外として破棄されます。この方法の場合、トランク リンクの接続先であるファイアウォール上の親物理リンクは従来のインターフェースとして動作し、同じリンク上に存在する可能性があるネイティブの (タグ付きでない) VLAN トラフィックもサポートできます。また、親インターフェースは、“未定義"のままです。

VLAN サブインターフェースは、ゾーンの割り当て、セキュリティ サービス、GroupVPN、DHCPサーバ、IP ヘルパー、ルーティング、NAT ポリシーとアクセス ルールの完全な制御など、物理インターフェースの大部分の機能と特徴を備えています。マルチキャスト サポートは、現時点では VLAN サブインターフェースから除外されています。

SonicOS のセキュリティ保護されるオブジェクト

SonicOS のインターフェース アドレス指定方式は、アドレス オブジェクト、サービス オブジェクト、およびネットワーク ゾーンと連動しています。この構造は、セキュリティが保護されるオブジェクトに基づいており、SonicOS 内のルールとポリシーでこれらのオブジェクトが使用されます。

セキュリティが保護されるオブジェクトには、物理インターフェースに直接リンクされ、「**ネットワーク > インターフェース**」ページで管理されるオブジェクトが含まれます。アドレスとサービス オブジェクトは、それぞれ「**管理 | ポリシー > オブジェクト > アドレス オブジェクト**」、「**管理 | ポリシー > オブジェクト > サービス オブジェクト**」で定義されています。アドレスおよびサービス オブジェクトの詳細については、『*SonicOS 6.5 ポリシー*』を参照してください。

ゾーンは、SonicOS のセキュリティ保護されたオブジェクトの手法の、階層上の頂点にあたります。SonicOS には事前に定義されたゾーンがあり、これとは別に独自のゾーンを定義することもできます。事前定義ゾーンは、LAN、DMZ、WAN、WLAN、および個別です。ゾーンに関する詳細は、「ネットワーク ゾーンの設定 (422 ページ)」を参照してください。

ゾーンには複数のインターフェースを指定できます。ただし、WAN ゾーンは最大でインターフェースの合計数マイナス 1 に制限されています。「**ネットワーク > フェイルオーバーと負荷分散**」での WAN フェイルオーバーと負荷分散の設定に応じて、WAN ゾーン内では、1 つまたは複数の WAN インターフェースがアクティブにトラフィックを搬送できます。SonicWall セキュリティ装置における WAN フェイルオーバーおよび負荷分散の詳細については、「ネットワーク > フェイルオーバーと負荷分散 (409 ページ)」を参照してください。

ゾーン設定レベルでは、ゾーンの「**インターフェース間通信を許可する**」設定により、許可を指示するゾーン内アクセス ルールの作成に関する処理が自動的に行われます。ゾーン全体の総合的なアドレス オブジェクトと、ゾーン アドレスからゾーン アドレスへの許可を包括的に指示するアクセス ルールが作成されます。

トランスペアレント モード

SonicOS のトランスペアレント モードは、インターフェースが管理階層のトップ レベルにあるものと見なすモードです。トランスペアレント モードは、一意のアドレス指定およびインターフェース ルーティングをサポートします。

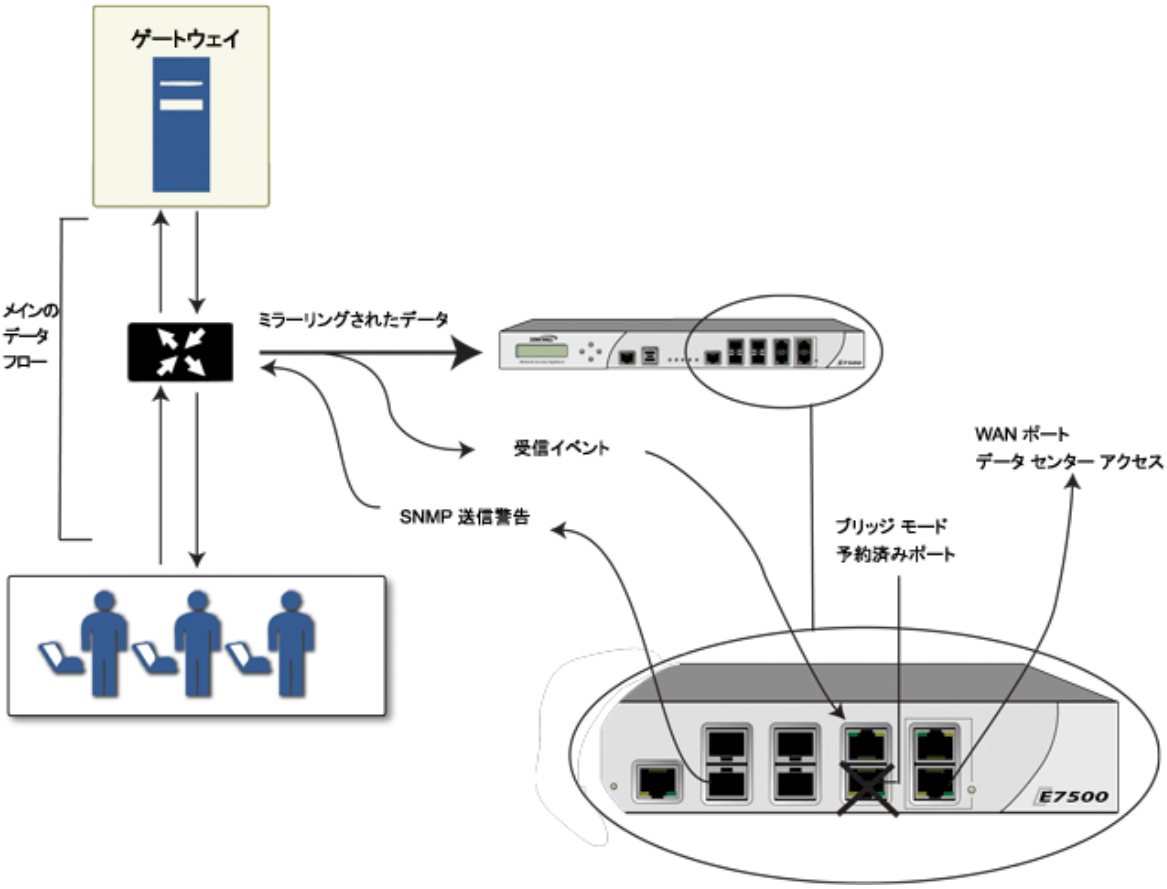
IPS スニッファ モード

IPS スニッファ モードは、SonicWall セキュリティ装置でサポートされており、侵入検知に使用されるレイヤ 2 ブリッジ モードの一種です。IPS スニッファ モードを設定して、セキュリティ装置のインターフェースをスイッチ上のミラーリングされたポートに接続してネットワーク トラフィックを検査できます。一般に、メイン ゲートウェイ内部のスイッチでイントラネットのトラフィックを監視する目的でこのモードを使用します。

「IPS スニッファ モード: ネットワーク図」では、ローカル ネットワーク内のスイッチに流れ込んだトラフィックがスイッチのミラー ポートでミラーリングされ、SonicWall セキュリティ装置の IPS スニッファ モード インターフェースに送られます。セキュリティ装置では、ブリッジ ペアで構成された設定に従ってパケットが検査されます。警告が発行されると、SNMP トラップがセキュリティ装置の別のインターフェースから指定の SNMP マネージャに送信されます。セキュリティ装置で検査されたネットワーク トラフィックは、検査終了後に破棄されます。

セキュリティ装置の WAN インターフェースは、ファイアウォール データ センターに接続してシグネチャ更新やその他のデータを取得するために使用されます。

IPS スニッファ モード: ネットワーク図



IPS スニッファ モードでは、レイヤ 2 ブリッジが、セキュリティ装置上の同じゾーンにある 2 つのインターフェース (LAN-LAN、DMZ-DMZ など) の間に設定されます。個別ゾーンを作成してレイヤ 2 ブリッジに使用することもできます。

WAN ゾーンだけは、IPS スニッファ モードでの使用に**適していません**。その理由は、SonicOS は LAN-LAN トラフィックのような同じゾーン内のトラフィックのすべてのシグネチャを検出しますが、方向固有の (クライアント側対サーバ側) シグネチャの中には一部のLAN-WAN のケースに当てはまらないものがあるからです。

レイヤ 2 ブリッジの一方のインターフェースを、スイッチのミラーリングされたポートに接続できます。ネットワーク トラフィックがスイッチに到達すると、トラフィックはミラーリングされたポートにも送信され、そこからセキュリティ装置に渡されて厳密なパケット検査を受けます。悪意のあるイベントが認められると警告とログ入力が開始され、SNMP が有効な場合は SNMP トラップが SNMP マネージャ システムの設定済み IP アドレスに送信されます。このトラフィックは、実際にはレイヤ 2 ブリッジのもう一方のインターフェースまで進みません。IPS スニッファ モードでは、セキュリティ装置はネットワーク トラフィックに対してインラインに配置されません。トラフィックを検査する手段を提供するだけです。

「**ネットワーク > インターフェース**」ページから表示できる「**インターフェースの編集**」ダイアログには、IPS スニッファ モードを設定するときに使用する「**このブリッジ ペアのトラフィックのみスニフする**」というオプションがあります。このオプションをオンにすると、セキュリティ装置ではミラーリングされたスイッチ ポートから L2 ブリッジに届くすべてのパケットが検査されます。IPS ス

ニッファ モードを使う場合、ミラーリングされたスイッチ ポートからのトラフィックがネットワークに送り返されないように「**このブリッジ ペアにトラフィックをルーティングしない**」オプションも選択する必要があります。

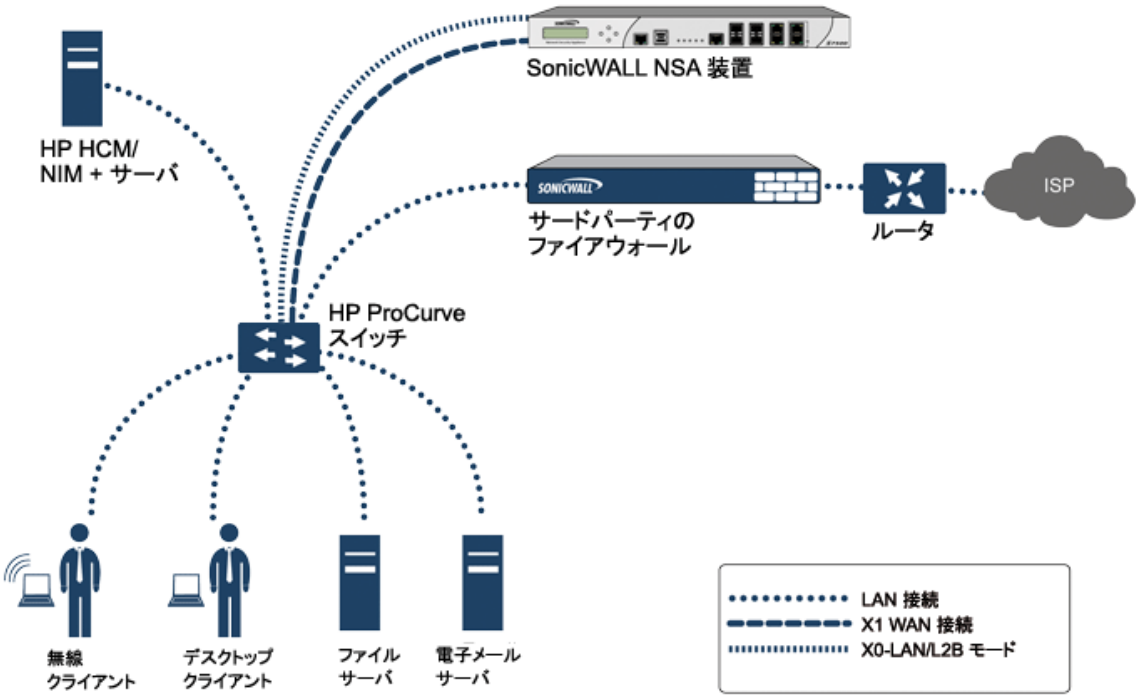
IPS スニッファ モードでインターフェースを設定する詳細な手順については、「IPS スニッファ モードの設定 (328 ページ)」を参照してください。

IPS スニッファ モードのサンプル トポロジ

このサンプル トポロジでは、Hewlett Packard ProCurve スイッチング環境で SonicWall IPS スニッファ モードを使用します。このシナリオは、脅威がやってくるポートを抑制したり閉じたりできる HP の ProCurve Manager Plus (PCM+) および HP Network Immunity Manager (NIM) サーバ ソフトウェア パッケージの機能に依存しています。

この方式は、既にセキュリティ装置が備わっているネットワークで、セキュリティ装置のセキュリティ サービスをセンサーとして利用したい場合に便利です。

IPS スニッファ モード: サンプル トポロジ



この配備では、WAN インターフェースおよびゾーンを*内部*ネットワークのアドレス指定方式用に設定し、内部ネットワークに接続します。X2 ポートは LAN ポートにブリッジされたレイヤ 2 ですが、何にも接続されません。X0 LAN ポートは HP ProCurve スイッチ上の特別にプログラムされた第 2 のポートに設定します。この特別なポートはミラー モード用に設定します。これはすべての内部ユーザおよびサーバのポートをファイアウォールの「スニッフ」ポートに転送します。それにより、ファイアウォールは内部ネットワークの全トラフィックを分析でき、セキュリティ シグネチャをトリガーするトラフィックがあれば、X1 WAN インターフェースを通じて PCM+/NIM サーバにただちにトラップするので、脅威がやってくるポートに対して処置を講じることができます。

Firewall Sandwich

SonicWall Firewall Sandwich を配備、設定して IT インフラストラクチャ全体の可用性、スケーラビリティ、管理性を高めることができます。Firewall Sandwich の配備には、次の特長があります。

- スケーラビリティ - 既存の装置を再利用しつつ、必要に応じてさらなるキャパシティを追加します
- 冗長性と回復力 - プライマリ コンポーネントとセカンダリ コンポーネント
- インライン アップグレード - システムをシャットダウンすることなく、ファイアウォールとスイッチをアップグレードします
- 一元管理 - 複数のファイアウォール クラスタとブレードのポリシーを管理します
- フル セキュリティ サービス - DPI-SSL の機能を含みます

Firewall Sandwich の配備および設定は、サポート対象の以下の装置とサービスによって実装できます。

- Dell Force10 S シリーズ スイッチ (FTOS v9.8+ が稼働する S5000、S4810、S4048、または S6000 など)
- SonicWall NSA 2600 以降の装置または SuperMassive シリーズの装置
- SonicWall サービス (すべてワイヤ モードでシングル サインオンを使用する GAV、IPS、ASPR、DPI-SSL、CFS など)

HTTP/HTTPS リダイレクト

セキュリティ装置の設定でユーザ認証が要求されている場合、認証されていない送信元からの HTTP/HTTPS トラフィックは SonicOS ログイン画面にリダイレクトされ、そこでユーザが資格情報を入力します。送られてくる HTTP および HTTPS トラフィックの送信元でユーザがログインしておらず、そのような 1 つ以上の送信元が新しい接続を繰り返し試みると、このリダイレクトが繰り返しトリガーされるという問題が発生します。これは、正当にアクセスの確立を試行する非ユーザ デバイスかもしれませんし、サービス妨害 (DoS) 攻撃をしかける有害なコードかもしれません。セキュリティ装置でこのような問題が発生すると、データ プレーン タスクでのリダイレクトの実行と、ウェブ サーバのスレッド タスクでのターゲット リダイレクト ページの表示の両方が影響して CP の CPU 負荷が高くなります。

この影響をできるだけ小さくするため、インターフェースを追加または編集するときは「**HTTP から HTTPS へのリダイレクトを有効にするためのルールを追加する**」オプションを選択するようにしてください。このオプションを有効にすると、SonicOS によって HTTP を許可するアクセス ルールがインターフェースに追加され、このルールの二次的な効果として、セキュリティ上の問題がない場合に、SonicOS で HTTPS から HTTP へのリダイレクトも可能になります。認証が必要なトラフィックをリダイレクトするときの最初の手順は、この例の 1 つです。その時点で暗号化して隠さなければならない重要なデータは存在しません。その後、CP ではなくデータ プレーン (DP) で HTTP 処理を行うことができます。

メモ：VPN トンネル インターフェースを追加または編集するとき、または「**モード / IP 割り当て**」で「**ワイヤ モード (2 ポート ワイヤ)**」、「**タップ モード (1 ポート タップ)**」、または「**PortShield スイッチ モード**」を選択したとき、このオプションを使用することはできません。

DP のオフロードによる HTTP/HTTPS リダイレクト

この機能により、セキュリティ装置を通過してアクセスするユーザにユーザ認証が必要な際に発生する HTTP/HTTPS リダイレクト要求を効果的に処理できます。認証されていないユーザの HTTP/HTTPS リクエストはセキュリティ装置のログイン ページにリダイレクトされます。このページは装置自身の

ビルトイン ウェブ サーバによって起動します。こうしたリダイレクトは、シングル サインオン (SSO) によってユーザを識別できない、または SSO が使用されていない場合に発生します。

この機能は、ウェブ サーバと HTTP/HTTPS リダイレクト プロセスの両方の効率を高めます。また、複数のコア全体に処理が分散するデータ プレーン (DP) に対する多くのリダイレクト プロセスの負荷を軽減します。

メモ：この機能の構成要素は、内部の「ユーザ認証の設定」オプションで制御することができます。これには、DP でのリダイレクト処理をグローバルに有効化/無効化するオプション、リダイレクト ファイル キャッシュを消去するオプション、ウェブ サーバ用の NAT の内部ポート番号を指定するオプションなどが含まれます。内部設定の詳細については、SonicWall テクニカル サポートにお問い合わせください。

インターフェースでの DNS プロキシの有効化

DNS プロキシがグローバルで有効になっている場合、DNS プロキシを個々のインターフェースに対して有効にすることができます。これにより、この機能を異なるネットワーク セグメントで個別に有効にすることができます。インターフェースで DNS プロキシを有効にする方法については、「DNS プロキシの有効化 (475 ページ)」を参照してください。

LTE モデムのサポート

LTE USB モデムが SonicWall セキュリティ装置に接続されている場合、SonicOS はそのモデルを検知し、「**管理 | システム セットアップ > ネットワーク > インターフェース**」ページで U0 インターフェースを表示します。このインターフェースは、既定で WAN ゾーンに属し、フェイルオーバーと負荷分散や、LTE 接続、プロファイル、詳細設定のために使用できます。LTE モデムの詳細については、『*SonicOS 6.5 接続*』を参照してください。

LAN バイパス

NS*a* 6650、NS*a* 9250、NS*a* 6450、および NS*a* 9650 プラットフォームにおいて、ハードウェア (LAN) バイパス モードは、ワイヤ モードと L2 ブリッジの両方で有効になります。LAN バイパス モードの主な機能 (有効になっている場合):

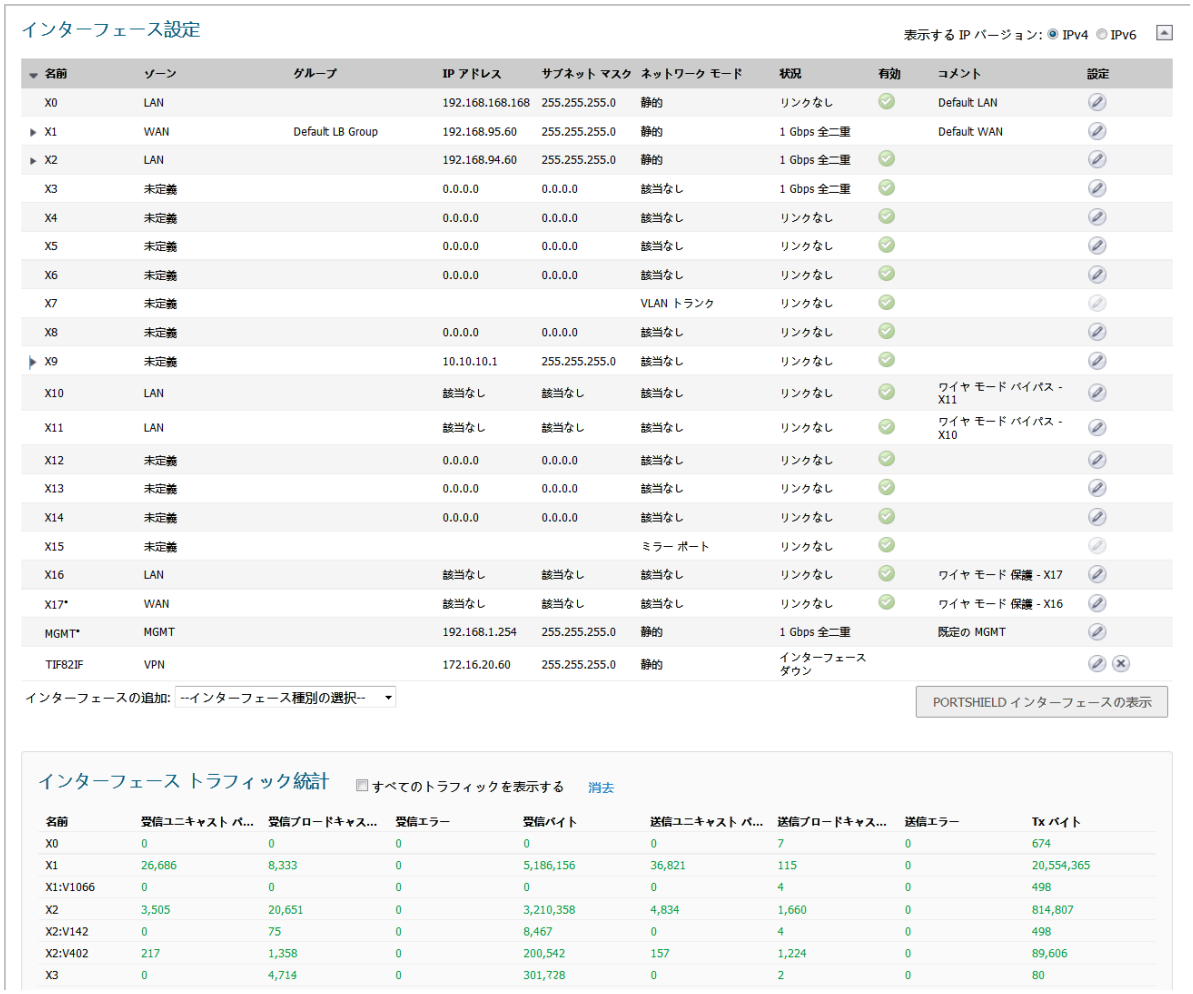
- 再起動中に、LBP 対応インターフェース間でトラフィックを渡します。
- ファイアウォールの電源がオフの場合でも、これらの LBP 対応インターフェース間でトラフィックを渡します。

NS*a* 9250、NS*a* 6450、NS*a* 9650 プラットフォームの場合、LAN バイパス機能はインターフェース X26 と X27 の間で使用できます。NS*a* 6650 の場合、この機能は X0 と X1 の間で使用できます。

ネットワーク > インターフェース

「**ネットワーク > インターフェース**」ページには、物理インターフェースに直接リンクされたインターフェース オブジェクトが含まれます。SonicOS のインターフェース アドレス指定方式は、ネットワーク ゾーンおよびアドレス オブジェクトと連動しています。NSA 2600 以降のセキュリティ装置と TZ および SOHO セキュリティ装置の間には、いくつかの小さな違いがあります。この違いについては、適宜、注意書きを加えます。

NSA 2600 以降のセキュリティ装置



インターフェース設定

表示する IP バージョン: IPv4 IPv6

名前	ゾーン	グループ	IP アドレス	サブネット マスク	ネットワーク モード	状況	有効	コメント	設定
X0	LAN		192.168.168.168	255.255.255.0	静的	リンクなし		Default LAN	
X1	WAN	Default LB Group	192.168.95.60	255.255.255.0	静的	1 Gbps 全二重		Default WAN	
X2	LAN		192.168.94.60	255.255.255.0	静的	1 Gbps 全二重			
X3	未定義		0.0.0.0	0.0.0.0	該当なし	1 Gbps 全二重			
X4	未定義		0.0.0.0	0.0.0.0	該当なし	リンクなし			
X5	未定義		0.0.0.0	0.0.0.0	該当なし	リンクなし			
X6	未定義		0.0.0.0	0.0.0.0	該当なし	リンクなし			
X7	未定義				VLAN トランク	リンクなし			
X8	未定義		0.0.0.0	0.0.0.0	該当なし	リンクなし			
X9	未定義		10.10.10.1	255.255.255.0	該当なし	リンクなし			
X10	LAN		該当なし	該当なし	該当なし	リンクなし		ワイヤ モード バイパス - X11	
X11	LAN		該当なし	該当なし	該当なし	リンクなし		ワイヤ モード バイパス - X10	
X12	未定義		0.0.0.0	0.0.0.0	該当なし	リンクなし			
X13	未定義		0.0.0.0	0.0.0.0	該当なし	リンクなし			
X14	未定義		0.0.0.0	0.0.0.0	該当なし	リンクなし			
X15	未定義				ミラー ポート	リンクなし			
X16	LAN		該当なし	該当なし	該当なし	リンクなし		ワイヤ モード 保護 - X17	
X17*	WAN		該当なし	該当なし	該当なし	リンクなし		ワイヤ モード 保護 - X16	
MGMT*	MGMT		192.168.1.254	255.255.255.0	静的	1 Gbps 全二重		既定の MGMT	
TIF82IF	VPN		172.16.20.60	255.255.255.0	静的	インターフェース ダウン			

インターフェースの追加: --インターフェース種別の選択-- PORTSHIELD インターフェースの表示

インターフェース トラフィック統計 すべてのトラフィックを表示する 消去

名前	受信ユニキャスト パ...	受信ブロードキャス...	受信エラー	受信バイト	送信ユニキャスト パ...	送信ブロードキャス...	送信エラー	Tx バイト
X0	0	0	0	0	0	7	0	674
X1	26,686	8,333	0	5,186,156	36,821	115	0	20,554,365
X1:V1066	0	0	0	0	0	4	0	498
X2	3,505	20,651	0	3,210,358	4,834	1,660	0	814,807
X2:V142	0	75	0	8,467	0	4	0	498
X2:V402	217	1,358	0	200,542	157	1,224	0	89,606
X3	0	4,714	0	301,728	0	2	0	80

TZ シリーズおよび SOHO セキュリティ装置

インターフェース設定

表示する IP バージョン: IPv4 IPv6

名前	ゾーン	グループ	IP アドレス	サブネット マスク	ネットワーク モード	状況	有効	コメント	設定
X0	LAN		192.168.168.168	255.255.255.0	静的	1 Gbps 全二重		Default LAN	
X1*	WAN	Default LB Group	192.168.95.54	255.255.255.0	静的	1 Gbps 全二重		Default WAN	
X2	LAN		192.168.94.54	255.255.255.0	静的	1 Gbps 全二重			
W0	WLAN		172.16.31.1	255.255.255.0	静的	1300 Mbps 半二重		既定 WLAN	
W0:V31	WLAN		10.1.2.5	255.255.255.0	静的	WLAN サブネット		VLAN for WLAN VAP3	

インターフェースの追加: --インターフェース種別の選択-- PORTSHIELD ウィザード PORTSHIELD インターフェースの表示

インターフェース トラフィック統計 すべてのトラフィックを表示する 消去

名前	受信ユニキャスト パ...	受信ブロードキャスト...	受信エラー	受信バイト	送信ユニキャスト パ...	送信ブロードキャスト...	送信エラー	Tx バイト
X0	0	382,990	0	24,511,360	0	6	0	1,062
X1	167,305	703,878	0	102,495,876	240,857	73	0	234,801,938
X2	0	442,838	0	44,019,974	0	14	0	1,742
W0	0	0	0	0	0	22	0	2,312
W0:V31	0	0	0	0	0	11	0	1,156

トピック:

- PortShield インターフェースの表示/非表示 (IPv4 のみ) (289 ページ)

- インターフェース設定 (290 ページ)
- インターフェース トラフィック統計 (291 ページ)
- 物理インターフェースと仮想インターフェース (279 ページ)
- SonicOS のセキュリティ保護されるオブジェクト (283 ページ)
- トランスペアレント モード (283 ページ)
- IPS スニッファ モード (283 ページ)
- インターフェースの設定 (292 ページ)
- IPS スニッファ モードの設定 (328 ページ)
- ワイヤ モードとタップ モードの設定 (333 ページ)
- ワイヤ モードでのリンク統合 (337 ページ)
- レイヤ 2 ブリッジ モード (339 ページ)
- レイヤ 2 ブリッジ モードの設定 (360 ページ)
- インターフェースの IPv6 設定 (369 ページ)
- 31 ビット ネットワーク (369 ページ)
- PPPoE アンナンバード インターフェースのサポート (371 ページ)

PortShield インターフェースの表示/非表示 (IPv4 のみ)

IPv4 モードでは、「**PortShield インターフェースの表示**」を選択して、「**インターフェース設定**」テーブルと「**インターフェース トラフィック統計**」テーブルに PortShield インターフェースを表示できます。PortShield インターフェースが表示されると、ボタンは「**PortShield インターフェースの非表示**」になります。

PortShield インターフェースの表示/非表示

PortShield インターフェースを非表示にするには、「**PortShield インターフェースの非表示**」を選択します。

インターフェース設定

「**インターフェース設定**」テーブルには、各インターフェースに関する次の情報がリストされます。

- **名前** - インターフェースの名前。
- **ゾーン** - 既定で LAN、WAN、および WLAN がリストされ、該当する場合は DMZ と MGMT もリストされます。ゾーンが設定されると、この列に名前がリストされます。設定されていないゾーンは「**未定義**」と示されています。ゾーンの上にマウスを置くと、ゾーンのプロパティが表示されます。

セキュリティ種別	ゾーンの設定時に選択されたセキュリティ種別を表示します。
メンバー インターフェース	このゾーンに割り当てられているインターフェースをリストします。
インターフェース間通信	このゾーンに対して、「**インターフェース間通信を許可する**」が有効になっているかどうかを示します。
アンチウイルス	このゾーンに対して、「**クライアント AV 強制サービスを有効にするe**」および/または「**ゲートウェイ アンチウイルス サービスを有効にする**」が有効になっているかどうかを示します。
秒	
GSC	このゾーンに対して「**グローバル セキュリティ クライアントを強制する**」(GSC) 保護が有効になっているかどうかを示します。詳細については、「ゾーンで SonicWall セキュリティ サービスを有効にする (425 ページ)」を参照してください。

- **グループ** - インターフェースが負荷分散グループに割り当てられた場合は、この列に表示されます。
- **IP アドレス** - インターフェースに割り当てられた IP アドレス。
- **サブネット マスク** - サブネットに割り当てられたネットワーク マスク。
- **ネットワーク モード** - 使用可能な IP 割り当て方法は、インターフェースが割り当てられるゾーンによって異なります。

メモ：ワイヤ モードは、NSA 2600 以降のセキュリティ装置でのみ使用できます。

LAN	**静的 IP モード** (既定)、**トランスペアレント IP モード (L3 サブネットを結合)**、**レイヤ 2 ブリッジ モード (IP ルート オプション)**、**ワイヤ モード (2 ポート ワイヤ)**、**タップ モード (1 ポート タップ)**、**IP アンナンバード**、**PortShield スイッチ モード**、**ネイティブ ブリッジ モード**
WAN	**静的** (既定)、**DHCP**、**PPPoE**、**PPTP**、**L2TP**、**ワイヤ モード (2 ポート ワイヤ)**、**タップ モード (1 ポート タップ)**
DMZ	**静的 IP モード** (既定)、**トランスペアレント IP モード (L3 サブネットを結合)**、**レイヤ 2 ブリッジ モード (IP ルート オプション)**、**ワイヤ モード (2 ポート ワイヤ)**、**タップ モード (1 ポート タップ)**、**IP アンナンバード**、**PortShield スイッチ モード**、**ネイティブ ブリッジ モード**
WLAN	**静的 IPモード** (既定)、**PortShield スイッチ モード**、**レイヤ 2 ブリッジ モード**、**ネイティブ ブリッジ モード**
Xn* への *PortShield (IPv4 表示のみ)	PortShield インターフェースが設定されている場合、PortShield 割り当て

- **状況** - リンクの状況と速度。
- **有効** -「**ネットワーク > インターフェース**」から有効/無効にできるポートを示します。有効になっているポートは**有効** アイコン、無効になっているポートは**無効** アイコンで示されます。アイコンを選択すると、ポートを有効/無効にするかどうかを確認するメッセージが表示されます。「**OK**」を選択します。ポートが有効/無効になり、アイコンが変化します。
- **コメント** - ユーザ定義のコメント。
- **設定** - **編集**アイコンを選択すると、「**インターフェースの編集**」ダイアログが表示され、指定したインターフェースの設定を行うことができます。インターフェースの設定については、「インターフェースの設定 (292 ページ)」を参照してください。

インターフェース トラフィック統計

「**インターフェース トラフィック統計**」テーブルには、VLAN 副インターフェースを含めて、設定されているすべてのインターフェースの送受信情報が、インターフェースごとに一覧表示されます。


インターフェース トラフィック統計 ☑すべてのトラフィックを表示する 消去

名前	受信ユニキャスト パ...	受信ブロードキャス...	受信エラー	受信バイト	送信ユニキャスト パ...	送信ブロードキャス...	送信エラー	Tx バイト
X0	0	0	0	0	37,964	7	0	2,430,370
X1	428,749	532,013	0	141,287,430	583,576	42,674	0	193,189,968
X1:V1066	0	0	0	0	0	4	0	498
X2	19	1,007,056	0	67,336,584	0	135,665	0	8,192,266
X2:V142	0	0	0	0	0	4	0	498
X2:V402	0	285,072	0	20,321,388	0	99,685	0	5,889,126
X3	0	0	0	0	0	0	0	0
X3:V66	0	0	0	0	0	2	0	88
X4	0	0	0	0	0	0	0	0
X5	0	0	0	0	0	0	0	0
X6	0	0	0	0	0	0	0	0
X7	0	0	0	0	0	0	0	0
X8	0	0	0	0	0	0	0	0
X9	0	0	0	0	2	4	0	698

名前	インターフェースの名前。
受信ユニキャスト パケット	インターフェースが受信したポイント ツー ポイント通信の数。
受信ブロードキャスト パケットまたは受信マルチキャストパケット	インターフェースが受信したマルチポイント通信の数。
受信エラー	インターフェースが受信したエラーの数。
受信バイト	インターフェースが受信したデータ量 (バイト数)。
送信ユニキャスト パケット	インターフェースが送信したポイント ツー ポイント通信の数。
送信ブロードキャスト バイト	インターフェースが送信したマルチポイント通信の数。
送信エラー	インターフェースが送信したエラーの数。
送信バイト	インターフェースが送信したデータ量 (バイト数)。

現在の統計を消去するには、「**インターフェース トラフィック統計**」テーブルの上部にある「**クリア**」を選択します。

インターフェースの設定

トピック:

- 静的インターフェースの設定 (293 ページ)
- ルート モードの設定 (300 ページ)
- インターフェースでの帯域幅管理の有効化 (301 ページ)
- インターフェースのトランスペアレント IP モード (L3 サブネットを結合) の設定 (303 ページ)
- 無線インターフェースの設定 (307 ページ)
- WAN インターフェースの設定 (313 ページ)
- トンネル インターフェースの設定 (318 ページ)
- リンク統合化とポート冗長化の設定 (323 ページ)
- 仮想インターフェース (VLAN サブインターフェース) (327 ページ)
- IPS スニッファ モードの設定 (328 ページ)
- セキュリティ サービス (統合脅威管理) の設定 (332 ページ)
- ワイヤ モードとタップ モードの設定 (333 ページ)
- ワイヤ モードでのリンク統合 (337 ページ)
- レイヤ 2 ブリッジ モード (339 ページ)
- レイヤ 2 ブリッジ モードの設定 (360 ページ)
- 非対称ルーティング (368 ページ)

- インターフェースの IPv6 設定 (369 ページ)
- 31 ビット ネットワーク (369 ページ)
- PPPoE アンナンバード インターフェースのサポート (371 ページ)

静的インターフェースの設定

インターフェースの概要については、「物理インターフェースと仮想インターフェース (279 ページ)」を参照してください。

静的とは、固定 IP アドレスがインターフェースに割り当てられていることを意味します。

静的インターフェースを設定するには、以下の手順を実行します。

1 「**管理 | ネットワーク > インターフェース**」に移動します。

2 「**インターフェース設定**」テーブルで、設定するインターフェースの**編集**アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。

3 「**ゾーン**」で、インターフェースに割り当てるゾーンを選択します。

- **LAN**
- **WAN**
- **DMZ**
- **WLAN**
- 作成した個別ゾーン
- 「**ゾーンの作成**」。「**ゾーンの追加**」ダイアログが表示されます。ゾーンの追加の詳細については、「ゾーンについて (422 ページ)」を参照してください。

メモ：表示されるオプションは、選択する**ゾーン**によって変化します。

4 **ネットワーク モード**:で、次のように選択します。

- **静的** (WAN での既定)
- **静的 IP モード** (LAN での既定)

5 「**IP アドレス**」フィールドと「**サブネット マスク**」フィールドに、インターフェースの IP アドレスとサブネット マスクを入力します。

メモ：別のゾーンと同じサブネットにある IP アドレスは入力できません。

6 設定対象によって、次の操作を行います。

- WAN ゾーンのインターフェースまたは管理インターフェースを設定する場合は、ゲートウェイ装置の IP アドレスを「**デフォルト ゲートウェイ**」フィールドに入力します。

  メモ：WAN サブネットの IP アドレス空間に属さない WAN インターフェース経由で送信先に到達する必要がある場合は、WAN サブネット上のピア装置のルーティング プロトコルから既定のルートを動的に受信しているかどうかにかかわらず、WAN インターフェースにデフォルト ゲートウェイの IP アドレスを指定する必要があります。LAN インターフェースではデフォルト ゲートウェイ IP がオプションになっています。

- LAN ゾーンのインターフェースまたは DMZ ゾーンのインターフェースを設定する場合は、ゲートウェイ装置の IP アドレスを「**デフォルト ゲートウェイ (オプション)**」フィールドに入力します。

このインターフェースが内部ネットワークかプライベート ネットワークかにかかわらず、ゲートウェイ装置によって外部ネットワークへのアクセスが可能になります。

7 設定対象によって、次の操作を行います。

- LAN ゾーンのインターフェースを設定する場合は、「ステップ 8」に進みます。
- WAN ゾーンのインターフェースを設定する場合は、DNS サーバの IP アドレスを最大 3 つまで「**DNS サーバ**」フィールドに入力します。DNS サーバはパブリックでもプライベートでもかまいません。詳細については、「WAN インターフェースの設定 (313 ページ)」を参照してください。

8 「**コメント**」フィールドに、必要に応じてコメント テキストを入力します。このテキストは、「**インターフェース設定**」テーブルの「**コメント**」列に表示されます。

9 このインターフェースを介した セキュリティ装置のリモート管理を有効にするには、サポートされている**管理**プロトコルを選択します。**HTTPS、Ping、SNMP、SSH** から 1 つ以上を選択できます。「**HTTPS**」を選択すると、「**HTTP から HTTPS へのリダイレクトを有効にするためのルールを追加する**」が使用可能になり、「**HTTP**」を選択すると、「**HTTP から HTTPS へのリダイレクトを有効にするためのルールを追加する**」が淡色表示 (無効) になります。

メモ：この機能の構成要素は、内部の「ユーザ認証の設定」オプションで制御することができます。詳細については、「DP のオフロードによる HTTP/HTTPS リダイレクト (286 ページ)」を参照してください。

同じセキュリティ装置の別のゾーンからの管理用 WAN インターフェースへのアクセスを許可するには、アクセス ルールを作成する必要があります。LAN ゾーンからの WAN プライマリ IP アクセスの許可の詳細については、『*SonicOS 6.5 ポリシー*』を参照してください。

10 限定的な管理権限を持つ選ばれたユーザがセキュリティ装置にログインすることを許可するには、「**ユーザ ログイン**」で、「**HTTP**」と「**HTTPS**」のいずれかまたは両方を選択します。「**HTTPS**」を選択すると、「**HTTP から HTTPS へのリダイレクトを有効にするためのルールを追加する**」が使用可能になり、「**HTTP**」を選択すると、「**HTTP から HTTPS へのリダイレクトを有効にするためのルールを追加する**」が淡色表示 (無効) になります。

11 次のどちらかを行います。

- 「**詳細設定**」を設定し、「静的インターフェースの詳細設定 (295 ページ)」に進みます。
- 「**OK**」を選択します。

メモ：セキュリティ装置のアドレスを変更した後に暗号キーを再生成するには、管理者パスワードが必要です。

静的インターフェースの詳細設定

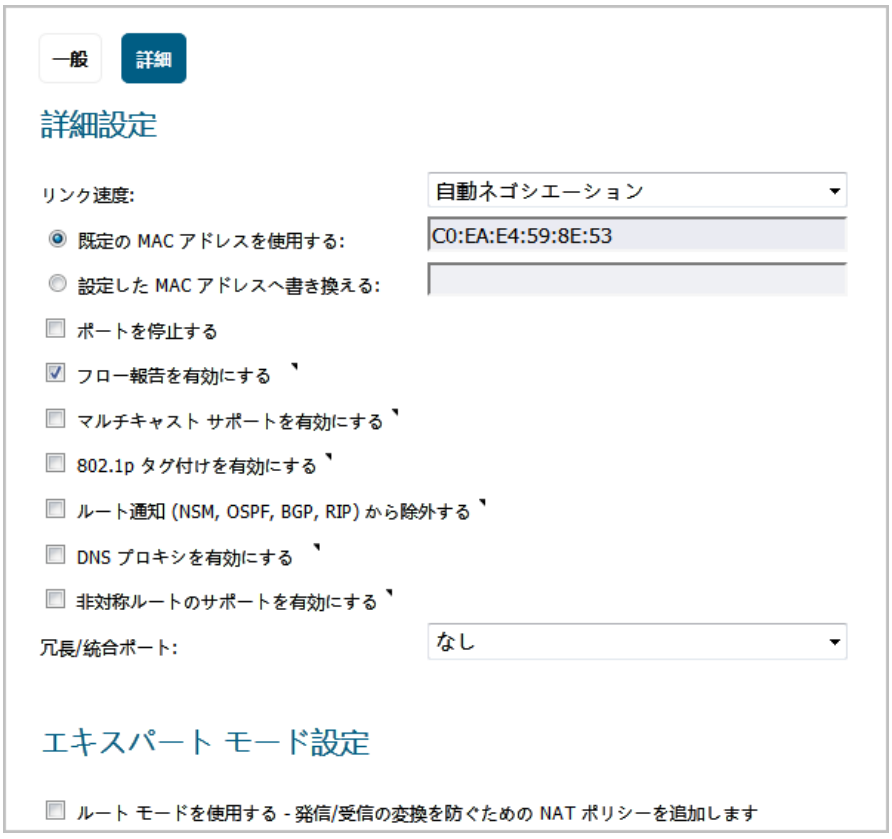
静的インターフェースの詳細設定を行うには、以下の手順に従います。

1 「**インターフェースの編集**」ダイアログで、「**詳細**」を選択します。

メモ：静的インターフェースの「**詳細**」で利用可能なオプションは、選択したゾーンとプラットフォームによって異なります。

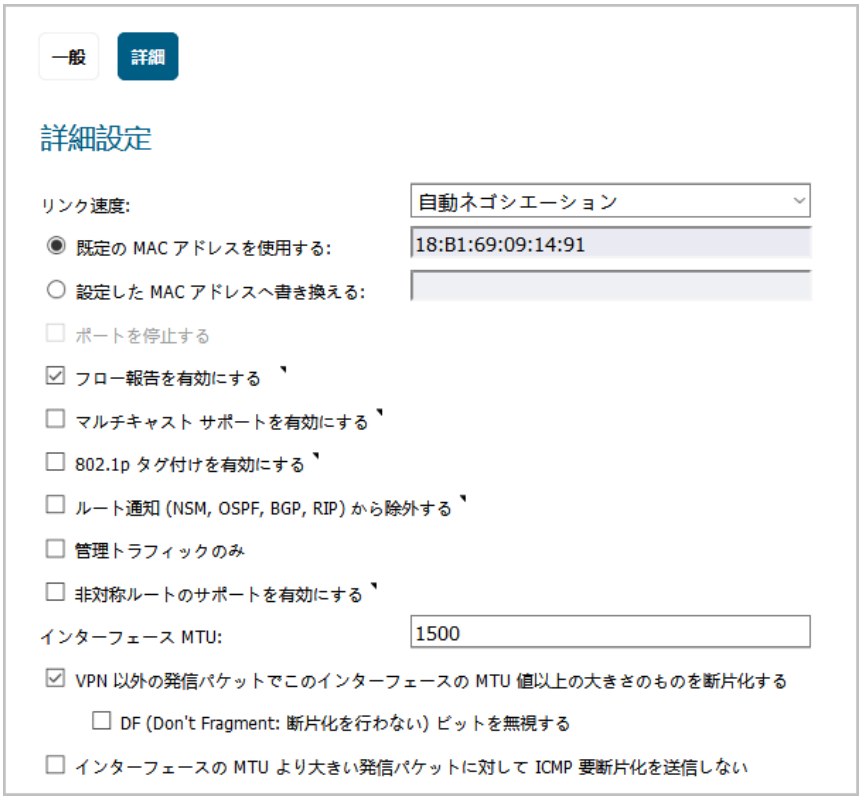
- インターフェースの編集の詳細設定 - LAN/DMZ/WLANTZ シリーズおよび SOHO W セキュリティ装置 (295 ページ)
- インターフェースの編集の詳細設定 - LAN/DMZ/WLANNSA 2600 以降のセキュリティ装置 (296 ページ)
- インターフェースの編集の詳細設定 - WANTZ シリーズおよび SOHO W セキュリティ装置 (296 ページ)
- インターフェースの編集の詳細設定 - WANNSA 2600 以降のセキュリティ装置 (297 ページ)

インターフェースの編集の詳細設定 - LAN/DMZ/WLANTZ シリーズおよび SOHO W セキュリティ装置

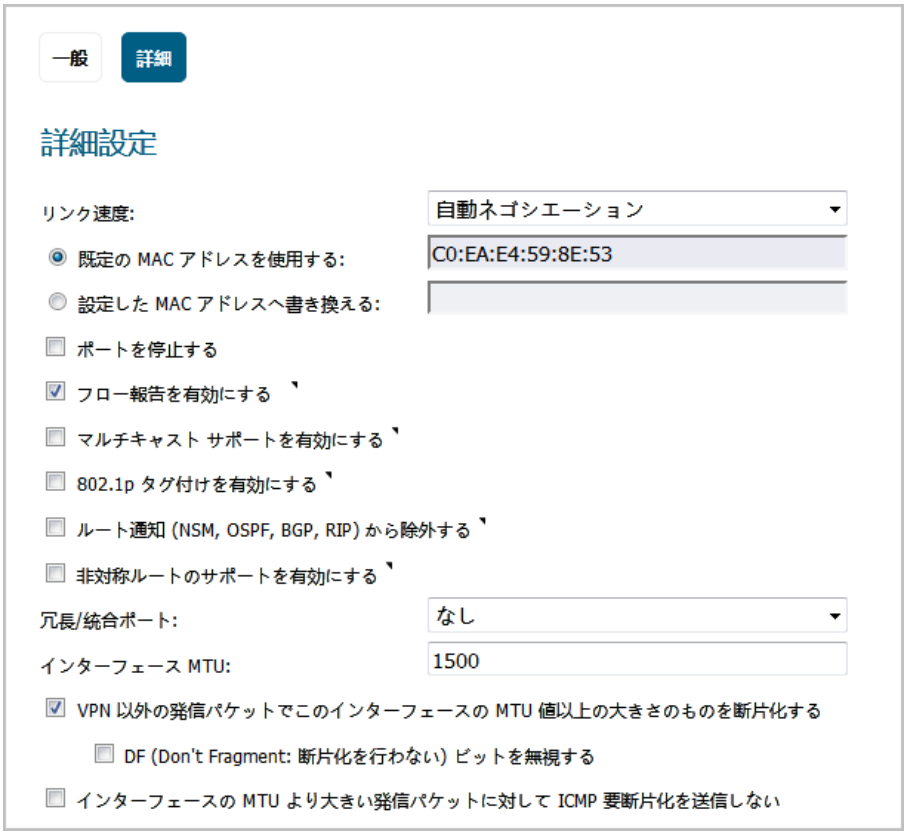


インターフェースの編集の詳細設定 - LAN/DMZ/WLANNSA 2600 以降のセキュリティ装置

インターフェースの編集の詳細設定 - WANTZ シリーズおよび SOHO W セキュリティ装置



インターフェースの編集の詳細設定 - WANNSA 2600 以降のセキュリティ装置



2 「**リンク速度**」では、「**自動ネゴシエーション**」が既定で選択され、接続された機器はイーサネット接続の速度と通信方式を自動的にネゴシエートします。イーサネット速度と通信方式を強制的に設定する場合は、「**リンク速度**」から以下のオプションの 1 つを選択します。

1 Gbps のインターフェースの場合	10 Gbps のインターフェースの場合
1Gbps - 全二重	10 Gbps - 全二重
100Mbps - 全二重	
100Mbps - 半二重	
10Mbps - 全二重	
10Mbps - 半二重	

△ **注意：特定のイーサネット速度と通信方式を選択した場合は、イーサネット カードから セキュリティ装置への接続の速度と通信方式も強制的に変更する必要があります。**

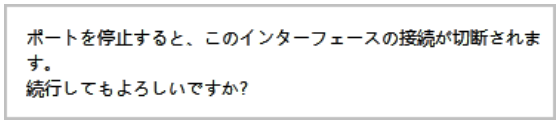
3 「**既定の MAC アドレスを使用する**」が既定で選択されています。インターフェースの「**既定の MAC アドレスを使用する**」をオーバーライドするには、「**設定した MAC アドレスへ書き換える**」を選択し、フィールドに MAC アドレスを入力します。

4 保守またはその他の理由でこのインターフェースを一時的にオフラインにする場合は、「**ポートを停止する**」を選択します。接続していたリンクは切断されます。このオプションは、既定では選択されていません。

このオプションをクリアすると、インターフェースが有効になり、リンクは稼働状態に戻ることができます。

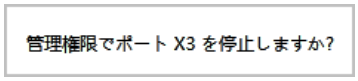
重要：管理インターフェースや現在使用中のインターフェースは停止できません。

このオプションを選択すると、確認メッセージが表示されます。

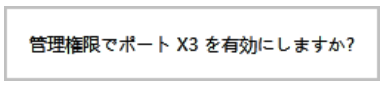


「**OK**」を選択してポートを停止します。

ヒント：インターフェースを停止するには、インターフェースの「**有効**」列の「**有効**」アイコンを選択します。確認メッセージが表示されます。



「**OK**」を選択すると、「**有効**」アイコンが「**無効**」アイコンに変わります。インターフェースを有効にするには、「**無効**」アイコンを選択します。確認メッセージが表示されます。



「**OK**」を選択すると、「**無効**」アイコンが「**有効**」アイコンに変わります。

5 AppFlow 機能については、「**フロー報告を有効にする**」を選択すると、このインターフェースに対して作成されたフローのフロー報告が有効になります。このオプションは、既定では選択されています。

6 必要に応じて、「**マルチキャスト サポートを有効にする**」を選択して、このインターフェースでマルチキャスト受信を許可します。このオプションは、既定では選択されていません。

7 必要に応じて、「**802.1p CoS タグ付けをを有効にする**」を選択して、このインターフェースを通過する情報に QoS (サービス品質) 管理の 802.1p 優先順位情報のタグを付けます。このオプションは、既定では選択されていません。

メモ：このオプションは、VLAN インターフェースでのみ利用できます。

このインターフェースを通じて送信されるパケットは、VLAN id=0 のタグ付けが行われ、802.1p 優先順位情報を搬送します。この優先順位情報を利用するには、このインターフェースに接続されている機器が、優先順位フレームをサポートしている必要があります。QoS 管理は、「**管理 | ポリシー | ルール > アクセス ルール**」にあるアクセス ルールで制御されます。QoS および帯域幅管理については、『*SonicOS ポリシー*』を参照してください。

8 必要に応じて、インターフェースをルート通知から除外するには、「**ルート通知 (NSM, OSPF, BGP, RIP) から除外する**」を選択します。このオプションは、既定では選択されていません。

9 NSA 2600 以降のセキュリティ装置を設定する場合は、「ステップ 11」に進みます。

10 必要に応じて、「**管理トラフィックのみ**」を選択し、トラフィックを SonicWall 管理トラフィックとルーティング プロトコルのみに制限します。このオプションは、既定では選択されていません。

メモ：TZ シリーズおよび SOHO W 装置だけに、このオプションがあります。

11 必要に応じて、DNS プロキシを有効にしている場合は「**DNS プロキシを有効にする**」オプションが LAN、DMZ、または WLAN インターフェースに対して表示されます。インターフェースで DNS プロキシを有効にするには、このオプションを選択します。このオプションは、既定では選択されていません。

12 必要に応じて、「**非対称ルートのサポートを有効にする**」を選択し、インターフェースでの非対称ルートのサポートを有効にします。有効にすると、このインターフェースから初期化されたトラフィックは非対称ルートをサポートします。つまり、初期パケットや応答パケットが他のインターフェースから通過できるようになります。このオプションは、既定では選択されていません。非対称ルーティングの詳細については、「クラスタ設定における非対称ルーティング (722 ページ)」を参照してください。

13 次の各ケースで TZ シリーズまたは SOHO W セキュリティ装置を設定する場合

- LAN/DMZ/WLAN インターフェースでは、「ルート モードの設定 (300 ページ)」に進みます。
- WAN インターフェースでは、「ステップ 16」に進みます。

14 必要に応じて、「**冗長/統合ポート**」から「**リンク統合化**」または「**ポート冗長化**」を選択します。詳細については、「リンク統合化とポート冗長化の設定 (323 ページ)」を参照してください。

メモ：このオプションは、NSA 2600 以上の装置でのみ利用できます。

15 NSA 2600 以降のセキュリティ装置の LAN/DMZ/WLAN インターフェースを設定する場合は、「ルート モードの設定 (300 ページ)」に進みます。

16 WAN インターフェースが断片化せずに転送できる最大パケット サイズ (MTU - 最大転送単位) を指定するには、ポートが送受信するパケットのサイズを「**インターフェース MTU**」フィールドに入力します。

標準パケット (既定)	1500
ジャンボ フレーム パケット	9000

メモ：ポートでジャンボ フレームを処理するには、*SonicOS 6.5 ポリシー*の説明に従って、あらかじめジャンボ フレームのサポートを有効にしておく必要があります。ジャンボ フレーム パケットのバッファ サイズの要件により、ジャンボ フレームをサポートするためのメモリ要件は 4 倍になります。

ジャンボ フレームは、NSA 3600 以降の装置でサポートされています。

17 必要に応じて、このインターフェースの MTU 値よりも大きな VPN 以外の送信パケットを断片化するには、「**VPN 以外の送信パケットでこのインターフェースの MTU 値以上の大きさのものを断片化する**」を選択します。このオプションは、既定では選択されています。選択すると、以下のオプションが利用可能になります。

重要：送信 VPN トラフィックの断片化の指定は、「**管理 | 接続性 | 詳細設定**」で行います。詳細については、『*SonicOS 接続*』を参照してください。

a 必要に応じて、Do-not-fragment packet (パケットの断片化を行わない) ビットをオーバーライドするには、「**DF (Don't Fragment: 断片化を行わない) ビットを無視する**」を選択します。このオプションは、既定では選択されていません。

18 WAN インターフェースが断片化されたパケットを受信できるという通知を遮断するには、「**インターフェースの MTU より大きい送信パケットに対して ICMP 要断片化を送信しない**」を選択します。このオプションは、既定では選択されていません。

19 このインターフェースでの帯域幅管理を設定するには、「インターフェースでの帯域幅管理の有効化 (301 ページ)」に進みます。

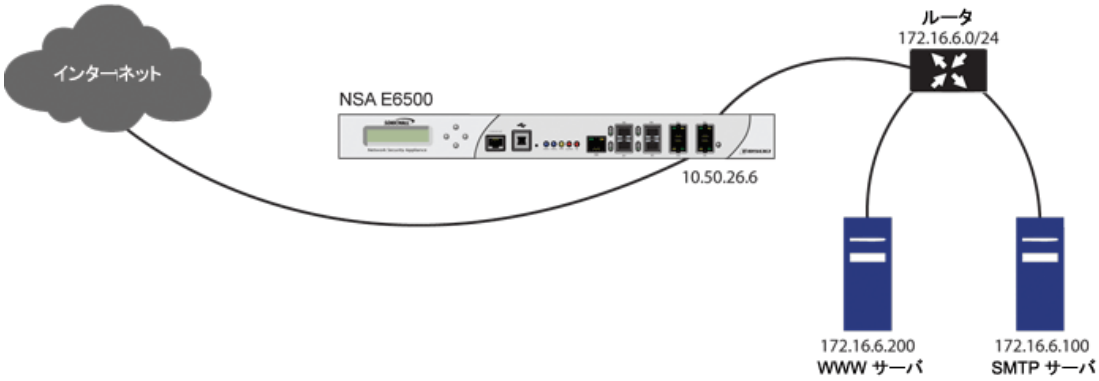
20 「**OK**」を選択します。

ルート モードの設定

ルート モードは、別々のパブリック IP アドレス範囲の間でトラフィックをルーティングするためのNATの代替策を提供します。「ルート モードの設定」のトポロジについて考えます。セキュリティ装置が 2 つのパブリック IP アドレス範囲の間でトラフィックをルーティングしています。

- 10.50.26.0/24
- 172.16.6.0/24

ルート モードの設定



172.16.6.0 用のインターフェースでルート モードを有効にすることにより、そのインターフェースの NAT 変換は自動的に無効になり、10.50.26.0 用に設定された WAN インターフェースにすべての送受信トラフィックがルーティングされるようになります。

メモ：ルート モードは、LAN、DMZ、および WLAN のゾーンのインターフェースに静的 IP モードを使用する場合に利用できます。DMZ の場合は、レイヤ 2 ブリッジ モードを使用する場合も利用できます。ルート モードは WAN モードでは使用できません。

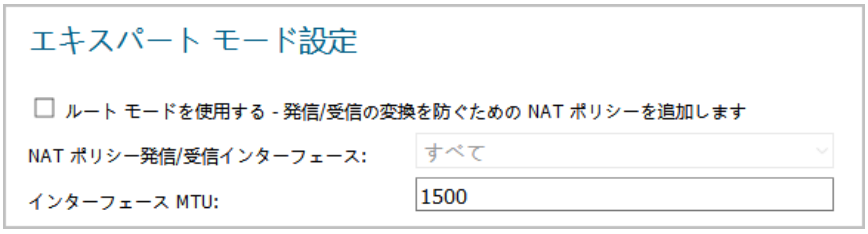
ルート モードを設定するには、以下の手順に従います。

1 「**管理 | システム セットアップ > ネットワーク > インターフェース**」に移動します。

2 適切なインターフェースの「**設定**」アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。

3 「**詳細設定**」を選択します。

4 「**エキスパート モード設定**」セクションまでスクロールします。



5 インターフェースでルート モードが有効にするには、「**ルート モードを使用する - 発信/受信の変換を防ぐための NAT ポリシーを追加します**」を選択します。このオプションは、既定では選択されていません。これを選択すると、次のエキスパート モード設定が使用できるようになります。

6 「**NAT ポリシー発信/受信インターフェース**」から、そのインターフェースのトラフィックをルーティングするために使用する WAN インターフェースを選択します。既定は「**すべて**」です。

7 断片化せずに転送できる最大パケット サイズ (MTU - 最大転送単位) を指定するには、ポートが送受信するパケットのサイズを「**インターフェース MTU**」フィールドに入力します。

標準パケット (既定)	1500
ジャンボ フレーム パケット	9000

メモ：ポートでジャンボ フレームを処理するには、*SonicOS 6.5 ポリシー*の説明に従って、あらかじめジャンボ フレームのサポートを有効にしておく必要があります。ジャンボ フレーム パケットのバッファ サイズの要件により、ジャンボ フレームをサポートするためのメモリ要件は 4 倍になります。

ジャンボ フレームは、NSA 3600 以降の装置でサポートされています。

8 セキュリティ装置で帯域幅管理が有効になっている場合は、「帯域幅管理」セクションが表示されます。このインターフェースで帯域幅管理を設定するには、「インターフェースでの帯域幅管理の有効化 (301 ページ)」に進みます。

9 「**OK**」を選択します。

重要：セキュリティ装置は、設定されたインターフェースと選択された WAN インターフェースの両方について「NAT ではない」ポリシーを作成します。これらのポリシーは、より一般的な多対 1 NAT ポリシーが設定されていても、それらに優先して使用されます。

インターフェースでの帯域幅管理の有効化

帯域幅管理 (BWM) により、最小帯域幅の保証と、トラフィックの優先順位付けが可能になります。「**管理 | セキュリティ設定 | ファイアウォール設定 > 帯域幅管理**」では帯域幅管理が有効になっています。帯域幅管理 (BWM) については、『*SonicOS 6.5 セキュリティ設定*』を参照してください。アプリケーションやユーザの帯域幅の量を制御することにより、利用可能な帯域幅すべてを少数のアプリケーションやユーザが消費することを防げます。異なるネットワーク トラフィックに割り当てられた帯域幅のバランスをとり、そしてトラフィックに優先順位を付けることで、ネットワークのパフォーマンスを向上できます。

さまざまな種別の帯域幅管理を有効にできます。

- **詳細** - 帯域幅オブジェクト、アクセス ルール、そしてアプリケーション ポリシーを設定することにより、インターフェース毎に送信および受信の最大帯域幅制限を設定できます。
- **グローバル** - 帯域幅管理設定をグローバルに有効にして、それらをすべてのインターフェースに適用できます。
- **なし** - (既定) 帯域幅管理は無効です。

帯域幅管理の設定と各種帯域幅管理の効果については、『*SonicOS 6.5 セキュリティ設定*』を参照してください。

SonicOS では、すべてのインターフェース上の送信 (発信) トラフィックと受信 (着信) トラフィックの両方に帯域幅管理を適用できます。送信帯域幅管理は、等級ベース キューイングを使用して行われます。受信帯域幅管理は、TCP 固有の動作を使用してトラフィックを制御する、ACK 遅延アルゴリズムを実装することによって行われます。

等級ベース キューイング (CBQ) により、ファイアウォールの保証された帯域幅と最大帯域幅のサービス品質 (QoS) が提供されます。そのインターフェース宛てのすべてのパケットは、対応する優先順位のキューに登録されます。スケジューラは、パケットのキュー登録を解除して、フローの保証された帯域幅と利用可能なリンクの帯域幅に応じて、パケットをリンク上で送信します。

帯域幅管理の有効化

受信および送信の帯域幅管理を有効または無効にするには、以下の手順を実行します。

1 「**管理 | システム セットアップ > ネットワーク > インターフェース**」に移動します。

2 インターフェースの**編集**アイコンを選択します。「**インターフェースの追加/編集**」ダイアログが表示されます。

3 未定義のインターフェースの場合は、「インターフェースの設定 (292 ページ)」に記載の各セクションに従ってインターフェースを設定します。

4 「**詳細**」タブを選択します。

5 「**帯域幅管理**」までスクロールします。

ⓘ **メモ：**「**詳細設定**」は、セキュリティ装置のモデルや選択したゾーンの種別によって異なる場合があります。

6 このインターフェースでの帯域幅管理を有効にします。帯域幅管理の詳細については、『*SonicOS 6.5 セキュリティ設定*』を参照してください。

   a 送信トラフィックをインターフェースの最大帯域幅に制限するには、「**送信帯域幅制限を有効にする**」を選択します。このオプションは、既定では選択されていません。

      - 最大帯域幅 (kbps) を「**利用可能なインターフェース送信帯域幅**」フィールドに指定します。最小値は 20 Kbps、最大値は 1000000、既定値は **384.000000** です。

   b 受信トラフィックをインターフェースの最大帯域幅に制限するには、「**受信帯域幅制限を有効にする**」を選択します。このオプションは、既定では選択されていません。

      - 最大帯域幅 (kbps) を「**利用可能なインターフェースス受信帯域幅**」フィールドに指定します。最小値は 20 Kbps、最大値は 1000000、既定値は **384.000000** です。

   これらのオプションのどちらかが選択されているかどうかで、次の違いが生じます。

   - 選択されている場合、利用可能な最大送信帯域幅管理は定義されていますが、詳細帯域幅管理はポリシー ベースなので、その制限は対応するアクセス ルールまたはアプリケーション ルールが存在しなければ適用されません。
   - 選択されていない場合は、帯域幅の制限はインターフェース レベルでは設定されませんが、トラフィックはその他のオプションを使用して調整できます。

7 「**OK**」を選択します。

インターフェースのトランスペアレント IP モード (L3 サブネットを結合) の設定

トランスペアレント IP モードを設定すると、SonicWall セキュリティ装置は、WAN サブネットを内部インターフェースにブリッジできるようになります。

インターフェースをトランスペアレント モード用に設定するには、以下の手順に従います。

1 「**管理 | システム セットアップ > ネットワーク > インターフェース**」に移動します。

2 設定する「**未定義**」インターフェースの**設定**アイコンを選択します。「**インターフェースの設定**」ダイアログが表示されます。

3 次のどちらかを行います。

- 「**ゾーン**」で「**LAN**」または「**DMZ**」を選択します。

  メモ：利用可能なオプションは、選択するゾーンの種別によって異なります。

- 設定可能なインターフェース用の新しいゾーンを作成する場合は、「**ゾーンの作成**」を選択します。「**ゾーンの追加**」ダイアログが表示されます。ゾーンの追加の詳細については、「ゾーンについて (422 ページ)」を参照してください。

4 「**モード / IP 割り当て**」から「**トランスペアレント IP モード (L3 サブネットを結合)**」を選択します。オプションが次のように変化します。

5 「**トランスペアレント範囲**」で、このインターフェースを通じてアクセスする IP アドレスの範囲を含むアドレス オブジェクトを選択します。アドレス範囲は、LAN、DMZ、または、内部のトランスペアレント インターフェースに使用されるゾーンに一致するその他の保護ゾーンといった、内部ゾーン内にあることが必要です。

要求を満たすアドレス オブジェクトが設定されていない場合は、「**アドレス オブジェクトの作成**」を選択します。「**アドレス オブジェクトの追加**」ダイアログが表示されます。アドレス オブジェクトの作成については、『*SonicOS 6.5 ポリシー*』を参照してください。

6 「**コメント**」フィールドに、必要に応じてコメント テキストを入力します。このテキストは、「**インターフェース**」テーブルの「**コメント**」列に表示されます。このオプションは、既定では選択されていません。

7 このインターフェースを介した セキュリティ装置のリモート管理を有効にするには、サポートされている管理プロトコルを選択します。**HTTPS**、**Ping**、**SNMP**、**SSH** から 1 つ以上を選択できます。このオプションは、既定では選択されていません。

同じセキュリティ装置の別のゾーンからの管理用 WAN インターフェースへのアクセスを許可するには、アクセス ルールを作成する必要があります。LAN ゾーンから WAN プライマリ IP アクセスを許可する方法については、『*SonicOS 6.5 ポリシー*』を参照してください。

8 制限付き管理権限を持つ選ばれたユーザがこのインターフェースを使ってセキュリティ装置に直接ログインすることを許可するには、「**ユーザ ログイン**」で、「**HTTP**」と「**HTTPS**」のいずれかまたは両方を選択します。

9 「**管理**」や「**ユーザ ログイン**」プロトコルで 「**HTTPS**」を選択すると、「**HTTP から HTTPS へのリダイレクトを有効にするためのルールを追加する**」が使用可能になり、選択されます。HTTP から HTTPS へのリダイレクトを防ぐには、このオプションの選択を解除します。

ヒント：「**ユーザ ログイン**」プロトコルで「**HTTP**」を選択すると、リダイレクトは無効になります。

メモ：この機能の構成要素は、内部の「ユーザ認証の設定」オプションで制御することができます。詳細については、「DP のオフロードによる HTTP/HTTPS リダイレクト (286 ページ)」を参照してください。

10 「**OK**」を選択します。

メモ：セキュリティ装置のアドレスを変更した後に暗号キーを再生成するには、管理者パスワードが必要です。

トランスペアレント IP モード インターフェースの詳細設定

トランスペアレント IP モード インターフェースの詳細設定を行うには、以下の手順に従います。

1 「**インターフェースの編集**」ダイアログで、「**詳細**」を選択します。

2 「**リンク速度**」では、「**自動ネゴシエーション**」が既定で選択され、接続された機器はイーサネット接続の速度と通信方式を自動的にネゴシエートします。イーサネット速度と通信方式を強制的に設定する場合は、「**リンク速度**」から以下のオプションの 1 つを選択します。

1 Gbps のインターフェースの場合	10 Gbps のインターフェースの場合
1Gbps - 全二重	10 Gbps - 全二重
100Mbps - 全二重	
100Mbps - 半二重	
10Mbps - 全二重	
10Mbps - 半二重	

△ **注意：特定のイーサネット速度と通信方式を選択した場合は、イーサネット カードから セキュリティ装置への接続の速度と通信方式も強制的に変更する必要があります。**

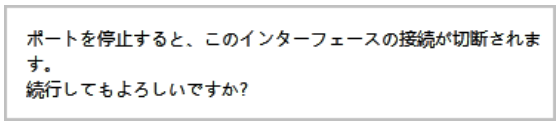
3 「**既定の MAC アドレスを使用する**」が既定で選択されています。インターフェースの「**既定の MAC アドレスを使用する**」をオーバーライドするには、「**設定した MAC アドレスへ書き換える**」を選択し、フィールドに MAC アドレスを入力します。

4 保守またはその他の理由でこのインターフェースを一時的にオフラインにする場合は、「**ポートを停止する**」を選択します。接続していたリンクは切断されます。このオプションは、既定では選択されていません。

このオプションをクリアすると、インターフェースが有効になり、リンクは稼働状態に戻ることができます。このオプションは、既定では選択されていません。

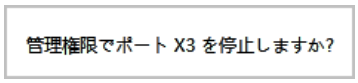
ⓘ **メモ**：管理インターフェースや現在使用中のインターフェースは停止できません。

このオプションを選択すると、確認メッセージが表示されます。

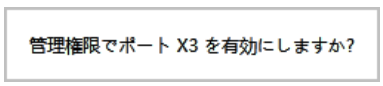


「**OK**」を選択してポートを停止します。

ヒント：インターフェースを停止するには、インターフェースの「**有効**」列の「**有効**」アイコンを選択します。確認メッセージが表示されます。



「**OK**」を選択すると、「**有効**」アイコンが「**無効**」アイコンに変わります。インターフェースを有効にするには、「**無効**」アイコンを選択します。確認メッセージが表示されます。



「**OK**」を選択すると、「**無効**」アイコンが「**有効**」アイコンに変わります。

5 AppFlow 機能については、「**フロー報告を有効にする**」を選択すると、このインターフェースに対して作成されたフローのフロー報告が有効になります。このオプションは、既定では選択されています。

6 必要に応じて、「**マルチキャスト サポートを有効にする**」を選択して、このインターフェースでマルチキャスト受信を許可します。このオプションは、既定では選択されていません。

7 必要に応じて、「**802.1p CoS タグ付けを有効にする**」を選択して、このインターフェースを通過する情報に QoS (サービス品質) 管理の 802.1p 優先順位情報のタグを付けます。このオプションは、既定では選択されていません。

メモ：このオプションは、VLAN インターフェースでのみ利用できます。

このインターフェースを通じて送信されるパケットは、VLAN id=0 のタグ付けが行われ、802.1p 優先順位情報を搬送します。この優先順位情報を利用するには、このインターフェースに接続されている機器が、優先順位フレームをサポートしている必要があります。QoS 管理は、「**管理 | ポリシー > ルール > アクセス ルール**」にあるアクセス ルールで制御されます。QoS および帯域幅管理については、『*SonicOS ポリシー*』を参照してください。

8 必要に応じて、インターフェースをルート通知から除外するには、「**ルート通知 (NSM, OSPF, BGP, RIP) から除外する**」を選択します。このオプションは、既定では選択されていません。

9 必要に応じて、「**管理トラフィックのみ**」を選択し、トラフィックを SonicWall 管理トラフィックとルーティング プロトコルのみに制限します。このオプションは、既定では選択されていません。

メモ：TZ シリーズおよび SOHO W 装置だけに、このオプションがあります。

10 必要に応じて、DNS プロキシを有効にしている場合は「**DNS プロキシを有効にする**」オプションが表示されます。インターフェースで DNS プロキシを有効にするには、このオプションを選択します。このオプションは、既定では選択されていません。

11 必要に応じて、「**非対称ルートのサポートを有効にする**」を選択し、インターフェースでの非対称ルートのサポートを有効にします。有効にすると、このインターフェースから初期化されたトラフィックは非対称ルートをサポートします。つまり、初期パケットや応答パケットが他のインターフェースから通過できるようになります。このオプションは、既定では選択されていません。非対称ルーティングの詳細については、「クラスタ設定における非対称ルーティング (722 ページ)」を参照してください。

12 TZ シリーズおよび SOHO シリーズのセキュリティ装置を設定する場合は、ステップ 14 に進みます。

13 必要に応じて、「**冗長/統合ポート**」から「**リンク統合化**」または「**ポート冗長化**」を選択します。詳細については、「リンク統合化とポート冗長化の設定 (323 ページ)」を参照してください。

メモ：このオプションは、NSA 2600 以上の装置でのみ利用できます。

14 「**WAN に向けての重複回避用 ARP の転送を有効にする**」を選択すると、このインターフェースで受信した重複回避用 ARP パケットは、WAN インターフェースのハードウェア MAC アドレスを送信元 MAC アドレスとして、WAN に転送されます。

15 「**WAN に向けての重複回避用 ARP 自動生成を有効にする**」を選択すると、このインターフェース上の新しいマシンの登録が ARP テーブルに追加されるたびに自動的に重複回避用 ARP パケットが WAN に送信されます。WAN インターフェースのハードウェア MAC アドレスが ARP パケットの送信元 MAC アドレスとして使用されます。

16 断片化せずに転送できる最大パケット サイズ (MTU - 最大転送単位) を指定するには、ポートが送受信するパケットのサイズを「**インターフェース MTU**」フィールドに入力します。

標準パケット (既定)	1500
ジャンボ フレーム パケット	9000

メモ：ポートでジャンボ フレームを処理するには、『*SonicOS ポリシー*』の説明に従って、あらかじめジャンボ フレームのサポートを有効にしておく必要があります。ジャンボ フレーム パケットのバッファ サイズの要件により、ジャンボ フレームをサポートするためのメモリ要件は 4 倍になります。

ジャンボ フレームは、NSA 3600 以降の装置でサポートされています。

17 帯域幅管理が有効になっている場合、このインターフェースで帯域幅管理を設定するには、「インターフェースでの帯域幅管理の有効化 (301 ページ)」に進みます。

18 「**OK**」を選択します。

無線インターフェースの設定

無線インターフェースは無線ゾーンに割り当てられたインターフェースであり、SonicWall SonicPoint および SonicWave の安全なアクセス ポイントをサポートするために使用されます。

メモ：SonicPoint は、セキュリティ種別の無線 (既定では WLAN) のインターフェースでのみプロビジョニングと管理を行うことができます。

無線インターフェースを設定するには、以下の手順に従います。

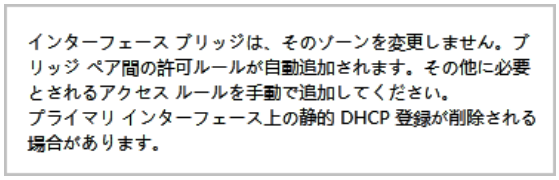
1 「**管理 | システム セットアップ > ネットワーク > インターフェース**」に移動します。

2 設定するインターフェースの「**設定**」列にある**編集**アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。

3 「**ゾーン**」で、「**WLAN**」または定義済みの個別無線ゾーンを選択します。

4 「**モード / IP 割り当て**」で、次のいずれかを選択します。

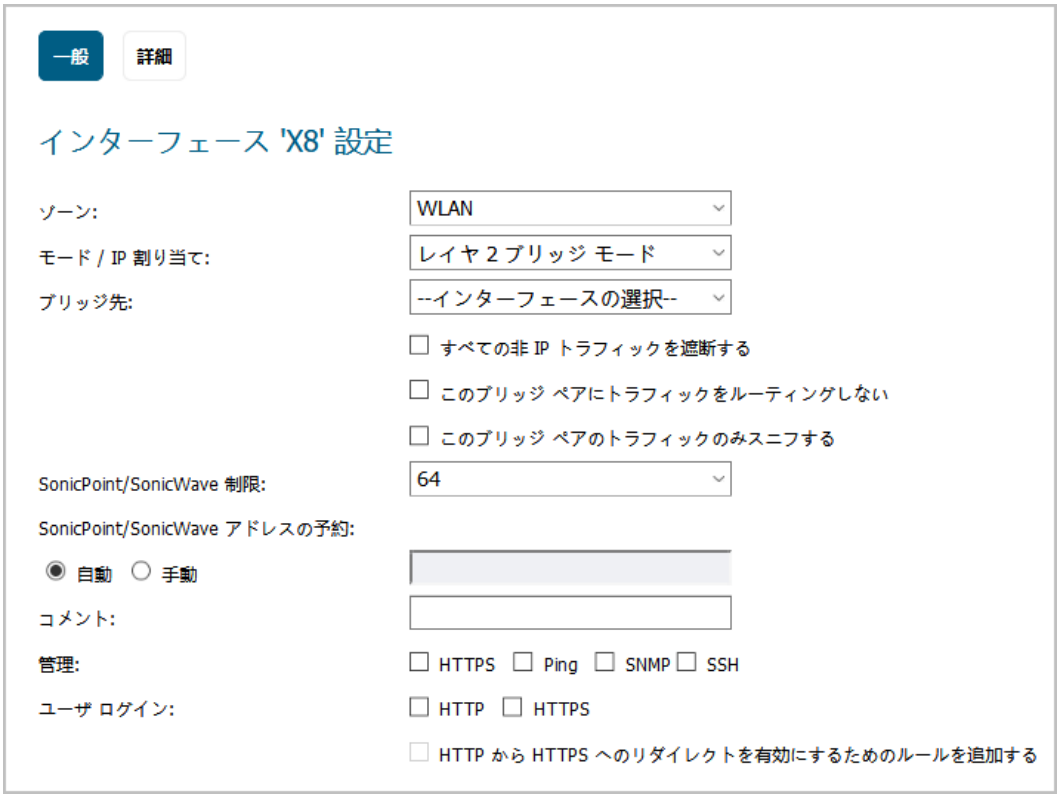
- **静的 IP モード** (既定)。次の箇所に進みます。「ステップ 12」
- **レイヤ 2 ブリッジ モード**。次のメッセージが表示されます。



重要：このモードを選択するには、ブリッジ ペア用のアクセス ルールの設定が必要です。アクセス ルールの設定については、『*SonicOS ポリシー*』を参照してください。

レイヤ 2 ブリッジ モードの詳細については、「レイヤ 2 ブリッジ モード (339 ページ)」を参照してください。

5 「**OK**」を選択します。オプションが次のように変化します。



6 「**ブリッジ先**」から、ブリッジする先のインターフェースを選択します。このインターフェースのブリッジ先として指定できるインターフェースだけが表示されます。

7 すべての非 IP トラフィックを遮断するには、「**すべての非 IP トラフィックを遮断する**」を選択します。

8 ブリッジ ペアでトラフィックをルーティングしないようにするには、「**このブリッジ ペアにトラフィックをルーティングしない**」を選択します。

9 TZ シリーズまたは SOHO W セキュリティ装置の場合は、「ステップ 16」に進みます。

10 ブリッジ ペアでトラフィックのスニッフのみを行う場合は、「**このブリッジ ペアのトラフィックのみスニフする**」を選択します。

11 「ステップ 14」へ進みます。

12 ゾーンの IP アドレスを「**IP アドレス**」フィールドに入力します。

13 ゾーンのサブネット マスクを「**サブネット マスク**」フィールドに入力します。

> **重要**：サブネット マスクの上限は、「**SonicPoint/SonicWave 制限**」で選択する SonicPoint の数で決まります。複数のインターフェースまたはサブインターフェースを無線インターフェースとして設定する場合は、小さなサブネット (上位) を使用することで、インターフェース上で使用可能な DHCP リースの数を制限できます。そうしないと、各無線インターフェースでクラス C サブネット (サブネット マスク `255.255.255.0`) を使用する場合、セキュリティ装置上で使用可能な DHCP リースの制限を越える可能性があります。

14 「**SonicPoint/SonicWave 制限**」フィールドで、このインターフェースで許可される SonicPoint の最大数を選択します。この値によって、「**サブネット マスク**」フィールドに入力できる最大のサブネット マスクが決まります。「使用できるサブネット マスクの最大サイズ」テーブル以下の表は、「**SonicPoint/SonicWave 制限**」の各項目のサブネット マスク制限と、許可される最

大サブネット マスクを入力した場合にインターフェース上で使用可能な DHCP リースの数を示しています。

「使用可能なクライアント IP」は、このインターフェース上で許可される最大数の SonicPoint が存在し、それぞれが 1 つの IP アドレスを使用していることに加えて、ファイアウォール ゲートウェイ インターフェースに対して 1 つの IP を想定しています。

使用できるサブネット マスクの最大サイズ

インターフェースあたりの SonicPoint 数/ SonicWave 数	最大サブネット マスク	使用可能な IPアドレスの総数	利用可能なクライアント IP アドレス
なし	30 ビット - 255.255.255.252	2	2
2	29 ビット - 255.255.255.248	6	3
4	29 ビット - 255.255.255.248	6	1
8	28 ビット - 255.255.255.240	14	5
16	27 ビット - 255.255.255.224	30	13
24	26 ビット - 255.255.255.192	62	29
32	26 ビット - 255.255.255.192	62	29
48	25 ビット - 255.255.255.128	126	77
64	25 ビット - 255.255.255.128	126	61
96	24 ビット - 255.255.255.0	190	93
128	23 ビット - 255.255.254.0	254	125

ヒント：「使用できるサブネット マスクの最大サイズ」テーブルは、使用できるサブネット マスクの最大サイズを示しています。WLAN インターフェースでは、クラスフル サブネット (クラス A、クラス B、またはクラス C) や、可変長のサブネット マスクも使用できます。多数の無線クライアントをサポートする必要がある場合は、小さなサブネット マスク (例: 24 ビット クラス C - 255.255.255.0 - 使用可能 IP の総数が 254) を使用して、より多くの IP アドレス空間をクライアントに割り当てることが推奨されます。

15 「SonicPoint/SonicWaveアドレス」から、SonicOS でのSonicPoint/SonicWave 装置の予約アドレスの決定方法を選択します。

- 自動 - このオプションは、既定で選択されています。「ステップ 16」に移動します。
- 手動 - これを選択すると、「アドレス」フィールドが使用可能になります。予約アドレスを入力します。

16 「**コメント**」フィールドに、必要に応じてコメント テキストを入力します。このテキストは、「**インターフェース**」テーブルの「**コメント**」列に表示されます。

17 このインターフェースを介したファイアウォールのリモート管理を有効にするには、サポートされている**管理**プロトコルを選択します。**HTTPS**、**Ping**、**SNMP**、**SSH** から 1 つ以上を選択できます。

18 限定的な管理権限を持つ選ばれたユーザがセキュリティ装置にログインすることを許可するには、「**ユーザ ログイン**」で、「**HTTP**」と「**HTTPS**」のいずれかまたは両方を選択します。

19 「**管理**」または「**ユーザ ログイン**」プロトコルで 「**HTTPS**」を選択すると、「**HTTP から HTTPS へのリダイレクトを有効にするためのルールを追加する**」が使用可能になり、選択されます。「**ユーザログイン**」に対して「**HTTP**」を選択すると、「**HTTPS**」オプションは選択されていても選択が解除されます。

20 「**OK**」を選択します。

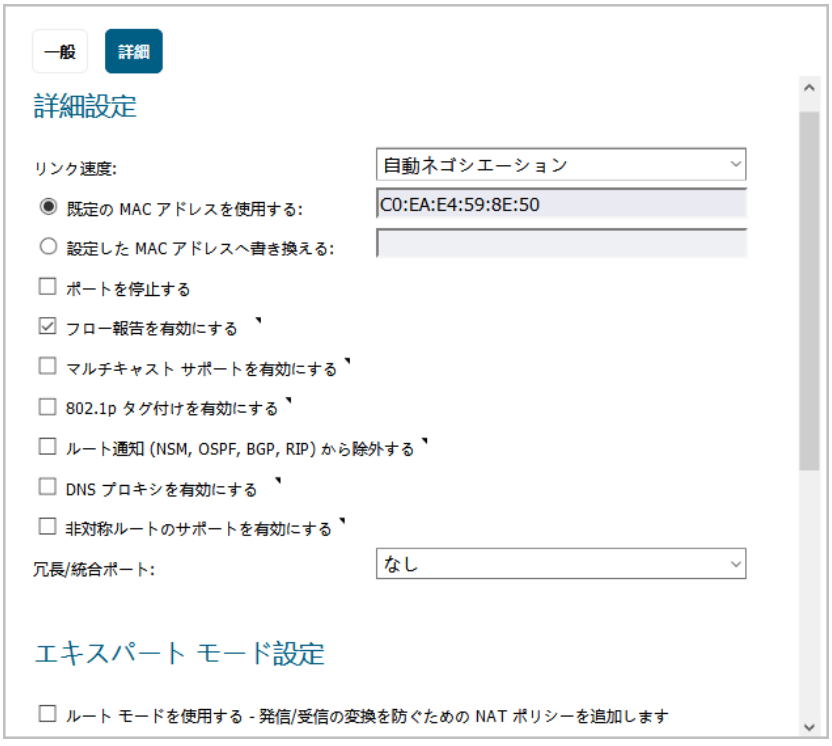
無線インターフェースの詳細設定

無線インターフェースの詳細設定を行うには、以下の手順に従います。

1 「**インターフェースの編集**」ダイアログで、「**詳細**」タブを選択します。これらのオプションは、セキュリティ装置のプラットフォームによって異なります。

「詳細」タブ: TZ シリーズおよび SOHO W セキュリティ装置

「詳細」タブ: NSA 以降のセキュリティ装置



2 TZ シリーズおよび SOHO W 装置を設定する場合は、「ステップ 6」に進みます。

3 「**リンク速度**」では、「**自動ネゴシエーション**」が既定で選択され、接続された機器はイーサネット接続の速度と通信方式を自動的にネゴシエートします。イーサネット速度と通信方式を強制的に設定する場合は、「**リンク速度**」から以下のオプションの 1 つを選択します。

1 Gbps のインターフェースの場合	10 Gbps のインターフェースの場合
1Gbps - 全二重	10 Gbps - 全二重
100Mbps - 全二重	
100Mbps - 半二重	
10Mbps - 全二重	
10Mbps - 半二重	

△ **注意：特定のイーサネット速度と通信方式を選択した場合は、イーサネット カードから セキュリティ装置への接続の速度と通信方式も強制的に変更する必要があります。**

4 既定の MAC アドレスの場合は、次のいずれかを選択します。

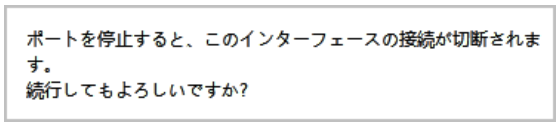
- **既定の MAC アドレスを使用する** - アドレスが自動的に選択されます。アドレスは淡色表示のフィールドに表示され、変更できません。このオプションは、既定では選択されています。
- **設定した MAC アドレスへ書き換える** - インターフェースに別の既定の MAC アドレスを指定します。「アドレス」フィールドが使用可能になります。MAC アドレスをフィールドに入力します。

5 保守またはその他の理由でこのインターフェースを一時的にオフラインにする場合は、「**ポートを停止する**」を選択します。接続していたリンクは切断されます。このオプションは、既定では選択されていません。

このオプションをクリアすると、インターフェースが有効になり、リンクは稼働状態に戻ることができます。このオプションは、既定では選択されていません。

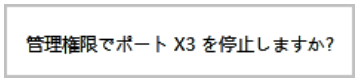
ⓘ **メモ：**管理インターフェースや現在使用中のインターフェースは停止できません。

このオプションを選択すると、確認メッセージが表示されます。

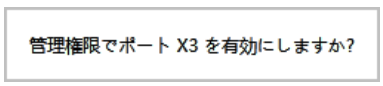


「**OK**」を選択してポートを停止します。

ヒント：インターフェースを停止するには、インターフェースの「**有効**」列の「**有効**」アイコンを選択します。確認メッセージが表示されます。



「**OK**」を選択すると、「**有効**」アイコンが「**無効**」アイコンに変わります。インターフェースを有効にするには、「**無効**」アイコンを選択します。確認メッセージが表示されます。



「**OK**」を選択すると、「**無効**」アイコンが「**有効**」アイコンに変わります。

6 AppFlow 機能については、「**フロー報告を有効にする**」を選択すると、このインターフェースに対して作成されたフローのフロー報告が有効になります。このオプションは、既定では選択されています。

7 必要に応じて、「**マルチキャスト サポートを有効にする**」を選択して、このインターフェースでマルチキャスト受信を許可します。このオプションは、既定では選択されていません。

8 必要に応じて、「**802.1p CoS のタグ付けを有効にする**」を選択して、このインターフェースを通過する情報に QoS (サービス品質) 管理の 802.1p 優先順位情報のタグを付けます。このオプションは、既定では選択されていません。

メモ：このオプションは、VLAN インターフェースでのみ利用できます。

このインターフェースを通じて送信されるパケットは、VLAN id=0 のタグ付けが行われ、802.1p 優先順位情報を搬送します。この優先順位情報を利用するには、このインターフェースに接続されている機器が、優先順位フレームをサポートしている必要があります。QoS 管理は、「**管理 | ポリシー | ルール > アクセス ルール**」にあるアクセス ルールで制御されます。QoS および帯域幅管理については、『*SonicOS ポリシー*』を参照してください。

9 必要に応じて、インターフェースをルート通知から除外するには、「**ルート通知 (NSM, OSPF, BGP, RIP) から除外する**」を選択します。このオプションは、既定では選択されていません。

10 SuperMassive または NSA シリーズ装置を設定する場合は、「ステップ 12」に進みます。

11 必要に応じて、「**管理トラフィックのみ**」を選択し、トラフィックを SonicWall 管理トラフィックとルーティング プロトコルのみに制限します。このオプションは、既定では選択されていません。

メモ：TZ シリーズおよび SOHO シリーズのセキュリティ装置だけに、このオプションがあります。

12 必要に応じて、DNS プロキシを有効にしている場合は「**DNS プロキシを有効にする**」オプションが表示されます。インターフェースで DNS プロキシを有効にするには、このオプションを選択します。このオプションは、既定では選択されていません。

13 必要に応じて、「**非対称ルートのサポートを有効にする**」を選択し、インターフェースでの非対称ルートのサポートを有効にします。有効にすると、このインターフェースから初期化されたトラフィックは非対称ルートをサポートします。つまり、初期パケットや応答パケットが他のインターフェースから通過できるようになります。このオプションは、既定では選択されていません。非対称ルーティングの詳細については、「クラスタ設定における非対称ルーティング (722 ページ)」を参照してください。

14 TZ シリーズおよび SOHO シリーズのセキュリティ装置を設定する場合は、「ステップ 14」に進みます。

15 必要に応じて、「**冗長/統合ポート**」から「**リンク統合化**」または「**ポート冗長化**」を選択します。詳細については、「リンク統合化とポート冗長化の設定 (323 ページ)」を参照してください。

メモ：このオプションは、NSA 2600 以上の装置でのみ利用できます。

16 「**WAN に向けての重複回避用 ARP の転送を有効にする**」を選択すると、このインターフェースで受信した重複回避用 ARP パケットは、WAN インターフェースのハードウェア MAC アドレスを送信元 MAC アドレスとして、WAN に転送されます。

17 「**WAN に向けての重複回避用 ARP 自動生成を有効にする**」を選択すると、このインターフェース上の新しいマシンの登録が ARP テーブルに追加されるたびに自動的に重複回避用 ARP パケットが WAN に送信されます。WAN インターフェースのハードウェア MAC アドレスが ARP パケットの送信元 MAC アドレスとして使用されます。

18 断片化せずに転送できる最大パケット サイズ (MTU - 最大転送単位) を指定するには、ポートが送受信するパケットのサイズを「**インターフェース MTU**」フィールドに入力します。

標準パケット (既定)	1500
ジャンボ フレーム パケット	9000

メモ：ポートでジャンボ フレームを処理するには、『*SonicOS ポリシー*』の説明に従って、あらかじめジャンボ フレームのサポートを有効にしておく必要があります。ジャンボ フレーム パケットのバッファ サイズの要件により、ジャンボ フレームをサポートするためのメモリ要件は 4 倍になります。

ジャンボ フレームは、NSA 3600 以降の装置でサポートされています。

19 このインターフェースでルート モードを設定する場合は、「ルート モードの設定 (300 ページ)」に進みます。

20 帯域幅管理が有効になっている場合、このインターフェースで帯域幅管理を設定するには、「インターフェースでの帯域幅管理の有効化 (301 ページ)」に進みます。

21 「**OK**」を選択します。

WAN インターフェースの設定

メモ：WAN サブネットの IP アドレス空間に属さない WAN インターフェース経由で送信先に到達する必要がある場合は、WAN サブネット上のピア装置のルーティング プロトコルから既定のルートを動的に受信しているかどうかにかかわらず、WAN インターフェースにデフォルト ゲートウェイの IP アドレスを指定する必要があります。

WAN インターフェースを設定することにより、インターネット接続が可能になります。SonicWall セキュリティ装置には、最大で *N - 2* 個の WAN インターフェースを設定できます。ここで、*N* は装置で定義されたインターフェース (物理および VLAN インターフェース) の数です。ただし、X0 および MGMT インターフェースだけは WAN インターフェースとして設定できません。

WAN インターフェースを設定するには、以下の手順に従います。

1 「**管理 | システム セットアップ | ネットワーク > インターフェース**」に移動します。

2 設定するインターフェースの「**設定**」列にある**編集**アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。

3 未定義インターフェースを設定している場合は、「**ゾーン**」メニューから「**WAN**」を選択します。**既定の WAN** インターフェースを選択した場合は、「**ゾーン**」メニューで「**WAN**」が既に選択されています。

4 「**ネットワーク モード**」から、以下のいずれかの WAN ネットワーク アドレッシング モードを選択します。

メモ：「ネットワーク モード」ドロップダウン メニューで選択するオプションによって、利用できるオプションが変わります。オプションを選択すると表示される各フィールドに、必要な情報を入力してください。

- **静的** - 静的 IP アドレスを使うネットワーク用にセキュリティ装置を設定します。
- **DHCP** - インターネット上の DHCP サーバから IP 設定を要求するようにセキュリティ装置を設定します。「DHCP クライアントでの NAT」は、ケーブルおよび DSL ユーザ向けの一般的なネットワーク アドレス指定モードです。

- **PPPoE** - PPPoE (Point to Point over Ethernet) を使用して、インターネットに接続します。ISP への接続にユーザ名とパスワードが必要な場合は、「**ユーザ名**」および「**ユーザ パスワード**」フィールドに入力します。DSL モデムを使用する場合は、このプロトコルが一般的です。
- **PPTP** - PPTP (Point to Point Tunneling Protocol) を使用して、リモート サーバに接続します。トンネル接続が必要な旧式の Microsoft Windows 実装をサポートします。
- **L2TP** - IPsec を使用して L2TP (Layer 2 Tunneling Protocol) サーバに接続し、クライアントからサーバに送信されるすべてのデータを暗号化します。ただし、他の宛先へのネットワーク トラフィックは暗号化しません。
- **ワイヤ モード (2 ポート ワイヤ)** - バイパス、検査、保護の各モードでセキュリティ装置をネットワークに配備できます。詳細については、「ワイヤ モードとタップ モードの設定 (333 ページ)」を参照してください。
- **タップ モード (1 ポート タップ)** - セキュリティ装置をネットワークに配備し、ネットワーク タップ、ポート ミラーリング、SPAN ポートを使用できます。詳細については、「ワイヤ モードとタップ モードの設定 (333 ページ)」を参照してください。

5 **DHCP** を使用する場合は、必要に応じて「**ホスト名**」フィールドにわかりやすい名前を入力し、「**コメント**」フィールドに必要なコメントを入力します。

6 **PPPoE**、**PPTP**、**L2TP** を使用する場合は、次のようなフィールドが追加で表示されます。

- 「**スケジュール**」が表示される場合は、このインターフェースで接続する時間のスケジュールをドロップダウン リストから選択します。
- 「**ユーザ名**」および「**ユーザ パスワード**」には、ISP から受領したアカウント名とパスワードを入力します。
- 「**サーバ IP アドレス**」フィールドが表示される場合は、ISP から受領したサーバ IP アドレスを入力します。
- 「**(クライアント) ホスト名**」フィールドが表示される場合は、装置のホスト名を入力します。これは「**管理 | システム セットアップ | 装置 > 基本設定**」からのファイアウォール名です。
- 「**事前共有鍵**」フィールドが表示される場合は、ISP から受領した値を入力します。

7 このインターフェースを介した セキュリティ装置のリモート管理を有効にするには、サポートされている管理プロトコルを選択します。**HTTPS**、**Ping**、**SNMP**、**SSH** から 1 つ以上を選択できます。

同じセキュリティ装置の別のゾーンからの管理用 WAN インターフェースへのアクセスを許可するには、アクセス ルールを作成する必要があります。アクセス ルールの作成については、『*SonicOS ポリシー*』を参照してください。

8 PPPoE、PPTP、L2TP を使用する場合は、次のようなフィールドが追加で表示されます。

- PPPoE の場合は、以下のいずれかを選択します。
  - PPPoE サーバから IP アドレスを取得するには、「**自動的に IP アドレスを取得する**」を選択します。
  - このインターフェースに静的 IP アドレスを使用する場合は、「**IP アドレスを指定する**」を選択し、IP アドレスをフィールドに入力します。
  - 「**アンナンバード インターフェース**」を選択し、次のいずれかを行います。
    - アンナンバード インターフェースを選択します。

- 「**新規アンナンバード インターフェースの作成**」を選択して、新しいアンナンバード インターフェースを作成します。

  メモ：このインターフェースは未割り当てでなければなりません。

- PPTP または L2TP の場合は、次のオプションを設定します。
  - 「**無動作時に切断**」を選択し、時間 (分) を入力すると、動作がない状態でこの時間が経過すると、接続が切断されます。無動作タイムアウトを無効にするには、このオプションをクリアします。
  - 「**ネットワーク モード**」で、次のいずれかを選択します。
    - 「**DHCP**」の場合、IP アドレス、サブネット マスク、デフォルト ゲートウェイの各フィールドはサーバによって自動的に設定されます。
    - 「**静的**」の場合、これらのフィールドに適切な値を入力します。

9 DHCP を使用する場合は、必要に応じて以下の選択を行います。

- DHCP サーバから前回提供された IP アドレスと同じアドレスを WAN インターフェース用に要求する場合は、「**起動時に前の IP の更新を要求する**」を選択します。
- この WAN インターフェースの切断後の再接続の際に毎回 DHCP サーバにリース再取得の要求を送信する場合は、「**リンク アップ時に DHCP リースを再取得する**」を選択します。

次のオプションの下に表示されるフィールドは、DHCP サーバから割り当てられます。プロビジョニングの後、以下のボタンが使用可能になるので選択を行います。

- 「**再取得**」を選択すると、現在割り当てられている IP アドレスの DHCP リース期間がリセットされます。
- 「**破棄**」を選択すると、現在の IP アドレスの DHCP リースがキャンセルされます。接続は破棄されます。接続を再確立するには、DHCP サーバから新しい IP アドレスを取得する必要があります。
- 「**更新**」を選択すると、DHCP サーバから新しい IP アドレスを取得します。

10 制限付き管理権限を持つ選ばれたユーザがこのインターフェースを使ってセキュリティ装置に直接ログインすることを許可するには、「**ユーザ ログイン**」で、「**HTTP**」と「**HTTPS**」のいずれかまたは両方を選択します。

11 HTTP 接続をセキュリティ装置への安全な HTTPS 接続に自動的にリダイレクトするには、「**HTTP から HTTPS へのリダイレクトを有効にするためのルールを追加する**」をオンにします。このオプションの詳細については、「HTTP/HTTPS リダイレクト (286 ページ)」を参照してください。

12 「WAN インターフェースの詳細設定 (316 ページ)」の説明に従って、「**詳細**」および「**プロトコル**」タブ (表示される場合) で設定を続行します。

13 詳細設定を続行するには、「WAN インターフェースの詳細設定 (316 ページ)」に進みます。

14 「**ネットワーク モード**」で「**PPPoE**」、「**PPTP**」、または「**L2TP**」を選択した場合は、「WAN インターフェースのプロトコルの設定 (317 ページ)」に進みます。

15 **「OK」を選択します。**

WAN インターフェースの詳細設定

WAN インターフェースの詳細設定を行うには、以下の手順に従います。

1 「**インターフェースの編集**」ダイアログで、「**詳細**」タブを選択します。

2 「**リンク速度**」では、「**自動ネゴシエーション**」が既定で選択され、接続された機器はイーサネット接続の速度と通信方式を自動的にネゴシエートします。強制的に変更したイーサネット速度と通信方式を指定する場合は、「**リンク速度**」メニューから以下のいずれかのオプションを選択します。

- 1 Gbps のインターフェースでは、以下の選択肢があります。
  - **1Gbps - 全二重**
  - **100Mbps - 全二重**
  - **100Mbps - 半二重**
  - **10Mbps - 全二重**
  - **10Mbps - 半二重**
- 10 Gbps のインターフェースでは、「**10 Gbps - 全二重**」のみ選択できます。

重要：特定のイーサネット速度と通信方式を選択した場合は、イーサネット カードからファイアウォールへの接続の速度と通信方式も強制的に変更する必要があります。

3 インターフェースの「**既定の MAC アドレスを使用する**」をオーバーライドするには、「**設定した MAC アドレスへ書き換える**」を選択し、フィールドに MAC アドレスを入力します。

4 保守またはその他の理由でこのインターフェースをオフラインにする場合は、「**ポートを停止する**」チェックボックスをオンにします。接続していたリンクは切断されます。チェックボックスをオフにすると、インターフェースが有効になり再びリンクが接続されます。

5 AppFlow 機能については、「**フロー報告を有効にする**」チェックボックスをオンにすると、このインターフェースに対して作成されたフローのフロー報告が有効になります。

6 このインターフェースでマルチキャスト受信を許可するには、「**マルチキャスト サポートを有効にする**」チェックボックスをオンにします。

7 このインターフェースを通過する情報に QoS (Quality of Service) 管理の 802.1p 優先順位情報のタグを付けるには、「**802.1p タグ付けを有効にする**」チェックボックスをオンにします。このインターフェースを通じて送信されるパケットは、VLAN id=0 のタグ付けが行われ、802.1p 優先順位情報を搬送します。この優先順位情報を利用するには、このインターフェースに接続されている機器が、優先順位フレームをサポートしている必要があります。QoS 管理は、「**管理 | セキュリティ設定 | ファイアウォール ルール > QoS 割付**」にあるアクセス ルールによって制御されます。QoS および帯域幅管理については、『*SonicOS セキュリティ設定*』を参照してください。

8 必要に応じて、「**冗長/統合ポート**」ドロップダウン リストから、「**リンク統合**または**ポート冗長化**」を選択します。詳細については、「リンク統合化とポート冗長化の設定 (323 ページ)」を参照してください。

9 **インターフェース MTU** - インターフェースが、パケットを断片化せずに転送できるパケットの最大サイズを指定します。ポートが送受信するパケットのサイズを特定します。

標準パケット (既定)	1500
ジャンボ フレーム パケット	9000

メモ：ポートでジャンボ フレームを処理するには、あらかじめジャンボ フレームのサポートを有効にしておく必要があります。ジャンボ フレームの詳細については、『*SonicOS セキュリティ設定*』を参照してください。ジャンボ フレーム パケットのバッファ サイズの要件により、ジャンボ フレームをサポートするためのメモリ要件は 4 倍になります。

ジャンボ フレームは、NSA 3600 以上の装置でサポートされます。

- **VPN 以外の送信パケットでこのインターフェースの MTU 値以上の大きさのものを断片化する** - VPN 以外の送信パケットでこのインターフェースの MTU 値以上の大きさのものをすべて断片化することを指定します。VPN 送信パケットの断片化の指定は、「**管理 | 接続性 | VPN**」で設定します。VPN トラフィックの詳細については、『*SonicOS 接続*』を参照してください。
- **DF (Don't Fragment: 断片化を行わない) ビットを無視する** - パケットの DF ビットをオーバーライドします。
- **ICMP の「フラグメント必要」メッセージを生成しない** - このインターフェースが断片化されたパケットを受信できるという通知を遮断します。

10 DHCP を使用する場合は、次のオプションが表示されます。

- サーバが変わる可能性がある場合は、「**DHCP の使用時に「発見」を使って更新を開始する**」を選択します。
- DHCP サーバがすぐに応答しない可能性がある場合は、「**リース取得中に _ 秒間隔で「DHCP 発見」を送信する**」を選択し、その間隔の秒数を調節します。

11 必要に応じて、このインターフェースでの帯域幅管理を有効にします。帯域幅管理の詳細については、「インターフェースでの帯域幅管理の有効化 (301 ページ)」を参照してください。

WAN インターフェースのプロトコルの設定

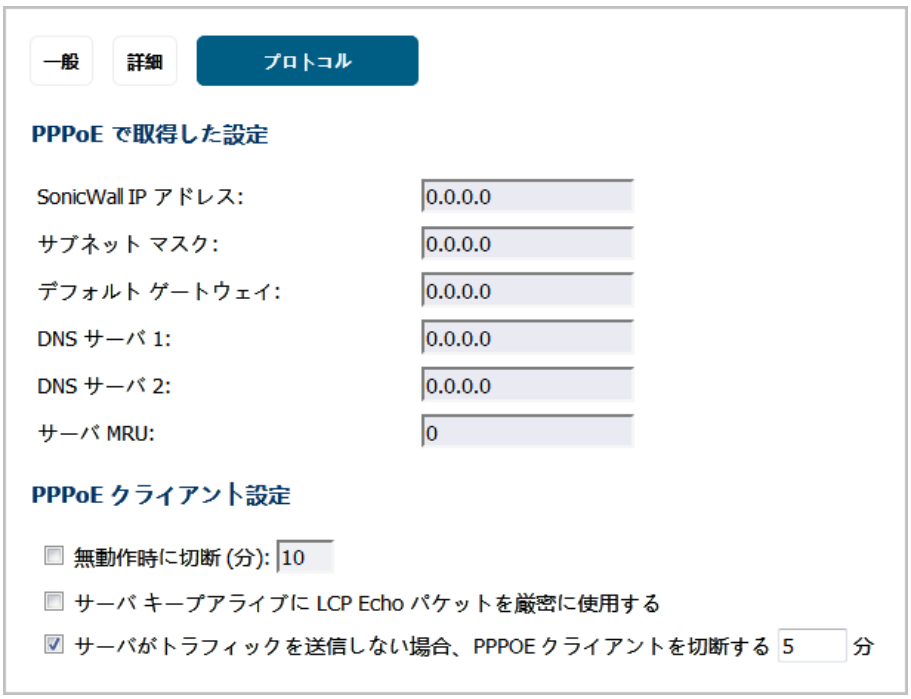
WAN インターフェースの設定時に「**ネットワーク モード**」で「**PPPoE**」、「**PPTP**」、または「**L2TP**」を指定した場合は、「**インターフェースの編集**」ダイアログが「**プロトコル**」タブに表示されます。

「**プロトコル**」タブの「**設定の取得先**」セクションのフィールド (**SonicWall の IP アドレス**、**サブネット マスク**、**デフォルト ゲートウェイ**など) は、インターネット サービス プロバイダ (ISP) から割り当てられます。セキュリティ装置を ISP に接続すると、これらのフィールドに実際の値が表示されます。

また、PPPoE を指定すると、SonicOS によって「**詳細**」タブの「インターフェース MTU」オプションが「**1492**」に設定され、「**プロトコル**」タブのその他の設定も割り当てられます。

PPPoE のその他の設定を行うには、次の手順に従います。

1 「**インターフェースの編集**」ダイアログで、「**プロトコル**」を選択します。



2 「**PPPoE クライアント設定**」セクションの次のオプションを有効にします。

- **無動作時に切断 (分)**: 時間を分で入力します (既定は 10 分)。パケットが送信されない状態でこの時間が経過すると、SonicOS は接続を切断します。このオプションは、既定では選択されていません。
- **サーバ キープアライブに LCP Echo パケットを厳密に使用する**: PPPoE サーバから `ppp LCP echo request` パケットが 1 分間送信されていないことを検知したときに、SonicOS が接続を切断するようにするにはこれを選択します。このオプションは、PPPoE サーバが `send LCP echo` 機能をサポートする場合のみ選択してください。このオプションは、既定では選択されていません。
- **サーバがトラフィックを送信しない場合、PPPOEクライアントを切断する - 分**: PPPoE サーバがパケット (LCP echo request を含む) を一切送信しないままその時間が経過したときに SonicOS によって接続が切断され、その後その再接続が行われることになる時間を分単位 (既定では 5 分) を入力します。このオプションは、既定では選択されています。

トンネル インターフェースの設定

SonicOS では、次のようなさまざまな種別のトンネル インターフェースを設定できます。

- 番号付けされたトンネル インターフェースと番号付けされないトンネル インターフェース、WLAN トンネル インターフェース、IPv6 6to4 トンネル インターフェースは、「**ネットワーク > インターフェース**」で設定します。
- ドロップ トンネル インターフェースと VPN トンネル インターフェースは、「**管理 | ネットワーク > ルーティング**」から設定します。詳細については、「ルート通知とルート ポリシーの設定 (486 ページ)」を参照してください。

- 番号付けされていないトンネル インターフェースは「**管理 | 接続性 > VPN**」から VPN ポリシーの一部として設定します。VPN ポリシーについては、『*SonicOS 接続*』を参照してください。

番号付けされたトンネル インターフェースと番号付けされないトンネル インターフェースは、VPN で使用されます。番号付けされたトンネル インターフェースには固有の IP アドレスが割り当てられますが、番号付けされないトンネル インターフェースは、既存の物理または仮想 (VLAN) インターフェースから IP アドレスを借用します。

どちらの種別のインターフェースも静的ルーティングと RIP および OSPF による動的ルーティングをサポートしますが、番号付けされたトンネル インターフェースは BGP にも対応しています。

また、番号付けされた VPN と番号付けされないトンネル インターフェースの両方が高度なルーティングをサポートでき、番号付けされないしトンネル インターフェースには制限がありません。「プラットフォームごとの VPN ポリシーおよびトンネルの最大数」を参照してください。

プラットフォームごとの VPN ポリシーおよびトンネルの最大数

プラットフォーム	VPN ポリシーの最大数	VPN トンネルの最大数	プラットフォーム	VPN ポリシーの最大数	VPN トンネルの最大数
SM 9200	10000	192	NSA 2600	75	64
SM 9400	10000	192	NSA 3600	1000	96
SM 9600	10000	192	NSA 4600	3000	96
			NSA 5600	4000	128
TZ 600	50	50	NSA 6600	6000	128
TZ 500	25	25			
TZ 500 W	25	25	NS*a* 2650	75	64
TZ 400	20	20	NS*a* 3650	1000	96
TZ 400 W	20	20	NS*a* 4650	3000	96
TZ 300	10	10	NS*a* 5650	4000	128
TZ 300 W	10	10	NS*a* 6650	6000	128
			NS*a* 9250	10000	192
SOHO W	10	10	NS*a* 9450	10000	192
			NS*a* 9650	10000	192

各種トンネル インターフェースの設定については、以下のセクションを参照してください。

- 番号付けされたトンネル インターフェースについては、「VPN トンネル インターフェースの設定 (319 ページ)」を参照してください。
- 番号付けされない (アンナンバード) トンネル インターフェースについては、『*SonicOS 接続*』を参照してください。
- ドロップ トンネル インターフェース。「ドロップ トンネル インターフェース (500 ページ)」を参照してください。
- IPv6 6to4 トンネル インターフェース。「6to4 自動トンネルを設定する (998 ページ)」を参照してください。

VPN トンネル インターフェースの設定

「インターフェースの追加」ドロップダウン リストから「VPN トンネル インターフェース」を選択して、番号付けされたトンネル インターフェースを作成できます。VPN トンネル インターフェース

は、インターフェース 設定テーブルに追加されると、RIP、OSPF、 BGP などの動的ルーティングに使用できるようになります。また、静的ルート ベース VPN の設定において、静的ルート ポリシーのインターフェースとして使用できるようになります。

VPN トンネル インターフェース (TI) は標準インターフェースと同じように設定して、装置管理や HTTP/HTTPS/Ping/SSH によるユーザ ログインを有効にすることができます。また、マルチキャスト、フロー報告、非対称ルーティング、断片化パケットの処理、DF (Don't Fragment: 断片化を行わない) ビットも設定できます。

メモ：同じ VPN ポリシーと番号付けされたトンネル インターフェースをリモート ゲートウェイにも設定する必要があります。これらの番号付けされたトンネル インターフェース (ローカル ゲートウェイとリモート ゲートウェイ) に割り当てる IP アドレスは同じサブネットにある必要があります。

「VPN トンネル インターフェースの配備」テーブルは、VPN トンネル インターフェースを配備できる方法を示しています。

VPN トンネル インターフェースの配備

TI をインターフェースとして設定できる機能	TI を使用できないインターフェース
静的ルート	静的 ARP 登録インターフェース
NAT	HA インターフェース
ACL (仮想アクセス ポイント アクセス制御リスト)	WLB (WAN 負荷分散) インターフェース
	静的 NDP (近隣者発見プロトコル) 登録インターフェース
OSPF	OSPFv3/RIPnG: 現在は IPv6 の高度なルーティングでサポートされていない
RIP	MAC_IP アンチスプーフ インターフェース
BGP	DHCP サーバ インターフェース

すべてのプラットフォームで、サポートされる VPN トンネル インターフェース (番号付けされるトンネル インターフェース) の最大数は 64 です。番号付けされないトンネル インターフェースの最大数はプラットフォームによって異なり、各プラットフォームでサポートされる VPN ポリシーの最大数と一致します。

VPN トンネル インターフェースを設定するには、以下の手順を実行します。

1 「**管理 | システム セットアップ > ネットワーク > インターフェース**」に移動します。

2 「**インターフェース設定**」テーブルの下の「**インターフェースの追加**」で、「**VPN トンネル インターフェース**」を選択します。「**トンネル インターフェースの追加**」ダイアログが表示されます。

ゾーンは VPN として定義されており、変更できません。

3 「**VPN ポリシー**」で、VPN ポリシーを選択します。

4 「**名前**」フィールドに、このインターフェースのわかりやすい名前を入力します。この名前に使用できる文字は英数字、ピリオド (.)、下線 (_) です。空白とハイフン (-) は使用できません。

5 「**IP アドレス**」フィールドに IP アドレスを入力します。既定値は 0.0.0.0 ですが、明示的な IP アドレスを入力する必要があります。そうしないとエラー メッセージが表示されます。

6 「**サブネット マスク**」フィールドに、サブネット マスクを入力します。既定値は 255.255.255.0 です。

7 必要に応じて、「**コメント**」フィールドにコメントを入力します。

8 必要に応じて、このインターフェースで許可される**管理**プロトコルを指定します。**HTTPS**、**Ping**、**SNMP**、**SSH** から 1 つ以上を選択できます。

9 必要に応じて、このインターフェースで許可される**ユーザ ログイン** プロトコルを指定します。**HTTP** と **HTTPS** のどちらかまたは両方を選択できます。

10 「**詳細設定**」を選択します。

11 トンネル インターフェースに対して作成されるフローのフロー報告を有効にするには、「**フロー報告を有効にする**」を選択します。このオプションは、既定では選択されています。

12 必要に応じて、「**マルチキャスト サポートを有効にする**」を選択し、インターフェースでのマルチキャスト受信を有効にします。このオプションは、既定では選択されていません。

13 必要に応じて、「**非対称ルートのサポートを有効にする**」を選択し、トンネル インターフェースでの非対称ルートのサポートを有効にします。このオプションは、既定では選択されていません。非対称ルーティングの詳細については、「クラスタ設定における非対称ルーティング (722 ページ)」を参照してください。

14 ルート モードを使用して発信/受信の変換を防ぐための NAT ポリシーを追加するには、「**ルート モードを使用する - 発信/受信の変換を防ぐための NAT ポリシーを追加します**」を選択します。選択すると、以下のオプションが利用可能になります。このオプションは、既定では選択されていません。

15 ルート モードが選択されている場合、NAT ポリシーのインターフェースを指定するには、「**NAT ポリシー発信/受信インターフェース**」でインターフェースを選択します。使用できるインターフェースはセキュリティ装置によって異なります。既定は「**すべて**」です。

16 このインターフェースで断片化パケットの処理を有効にするには、「**断片化パケットの処理を有効にする**」を選択します。このオプションがオフの場合、断片化パケットは破棄され、VPN ログ レポートにログ メッセージ「`Fragmented IPsec packet dropped`」 (断片化された IPSec パケットが破棄された) が表示されます。このオプションは、既定では選択されています。

このオプションをオンにすると、「**DF (断片化を行わない) ビットを無視する**」オプションが使用できるようになります。

17 パケット ヘッダーの DF ビットを無視するには、「**DF (Don't Fragment: 断片化を行わない) ビットを無視する**」を選択します。一部のアプリケーションでは、パケットの「断片化を行わない」オプションを明示的に設定できます。これにより、すべてのセキュリティ装置にそのパケットを断片化しないよう指示されます。このオプションが有効になっていると、セキュリティ装置は DF ビットを無視し、パケットの断片化を強行します。

18 「**OK**」を選択します。新しい番号付けされた VPN トンネル インターフェースが「**インターフェース設定**」テーブルに追加されます。

リンク統合化とポート冗長化の設定

メモ：リンク統合とポート冗長化は、NSA 2600 以降のセキュリティ装置でサポートされています。

リンク統合化もポート冗長化も、SonicOS 管理インターフェースの「**インターフェースの編集**」ダイアログの「**詳細**」タブで設定します。

- 「リンク統合化 (323 ページ)」- 複数のイーサネット インターフェースをまとめて単一の論理リンクにし、それによって単一の物理インターフェースを上回るスループットをサポートします。そのため、2 つのイーサネット ドメイン間でマルチギガビットのトラフィックが送信できるようになります。

  メモ：リンク統合化は、NSA 2600 以降のセキュリティ装置でサポートされます。NSA 2600 では、ネットワーク インターフェースのリンク統合化はサポートされますが、NSA 2600 がスイッチングをサポートしていないため、スイッチングのリンク統合化はサポートされません。詳細については、「スイッチング > リンク統合 (679 ページ)」を参照してください。

  リンク統合化は、レイヤ 2 ブリッジ モードではサポートされません。

- 「ポート冗長化 (326 ページ)」- 第 2 のスイッチに接続できる任意の物理インターフェースに対して単一の冗長ポートを設定して、プライマリ インターフェースまたはプライマリ スイッチに障害が起きた場合に接続が失われるのを防ぎます。

  メモ：ポート冗長化は、NSA 2600 以降のセキュリティ装置でサポートされます。リンク統合化とポート冗長化は、HA 制御インターフェースではサポートされません。

トピック:

- リンク統合化 (323 ページ)
- リンク統合化の設定 (324 ページ)
- ポート冗長化 (326 ページ)
- ポート冗長化の設定 (326 ページ)

リンク統合化

リンク統合化は、ファイアウォールとスイッチの間で利用可能な帯域幅を増やすために使用され、最高で 4 つのインターフェースをまとめて 1 つの統合リンクにすることで行われます。 これは LAG (Link Aggregation Group) と呼ばれます。統合リンクのすべてのポートは、同じスイッチに接続されていなければなりません。セキュリティ装置は、リンク統合化グループ内のインターフェース間でのトラフィックの負荷分散のためにラウンドロビン アルゴリズムを使用します。リンク統合化は一定の冗長化も提供します。 つまり、LAG 内の 1 つのインターフェースがダウンしても、他のインターフェースの接続は維持されるということです。

リンク統合化は、ベンダーによって呼称が異なり、ポート チャンネル、イーサ チャンネル、トランク、ポート グルーピングなどと呼ばれることもあります。

トピック:

- リンク統合化フェイルオーバー (324 ページ)
- リンク統合化の制限 (324 ページ)

リンク統合化フェイルオーバー

SonicWall は、リンク障害で接続が失われるのを防ぐために、高可用性 (HA)、負荷分散グループ (LB グループ)、リンク統合化といった複数の方法を用意しています。セキュリティ装置上でこれらの機能が 3 つとも設定されている場合、リンク障害の際に次の優先順位が適用されます。

1 高可用性

2 リンク統合化

3 負荷分散グループ

リンク統合化よりも HA が優先されます。LAG 内の各リンクは負荷を平等に分担するので、アクティブ ファイアウォールのリンクが失われると、アイドル ファイアウォールへのフェイルオーバーが強制的に行われます (そのファイアウォールのすべてのリンクの接続が維持されている場合)。物理的な監視を設定する必要があるのは、プライマリ統合ポートについてだけです。

リンク統合化と LB グループを併用すると、リンク統合化が優先されます。LB が作動するのは、統合リンクのすべてのポートがダウンした場合だけです。

リンク統合化の制限

- 現在、リンク統合化では静的アドレッシングのみがサポートされています。PAG (ポート統合化) と呼ばれる静的ポート チャンネルは、イーサネット ポート チャンネルを設定する 1 つの方法です。パートナー機器 (スイッチやサーバなど) とのイーサチャンネルを形成するために送信される LACP パケットや PAGP パケットはありません。
- イーサネット ポート チャンネルを使用して設定される静的 LAG (Link Aggregation Group) は、NSA 3600 以降のセキュリティ装置では手動で設定/バンドルする必要があります。
- 現在、動的 LACP (Link Aggregation Control Protocol) はサポートされていません。IEEE LACP や Cisco の PAGP など、動的な、プロトコルを介したイーサーネット ポートのバンドルは、イーサネット ポート チャンネルを設定するもう 1 つの方法です。この方法では、LACP パケットや PAGP パケットがポートから送信されます。

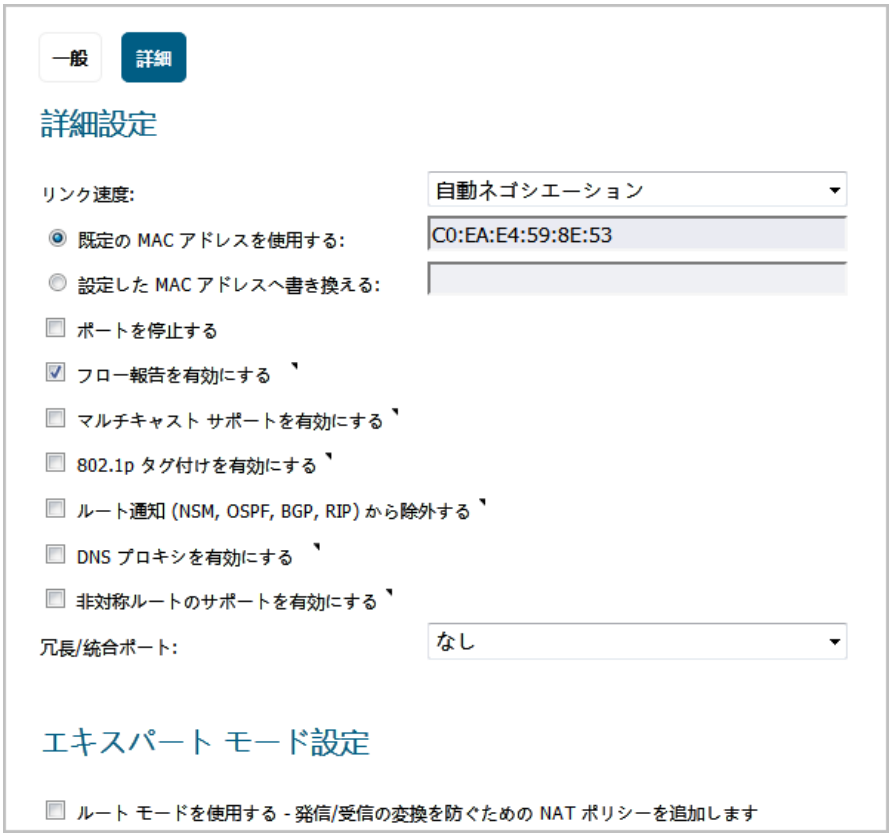
リンク統合化の設定

リンク統合を設定するには、以下の手順に従います。

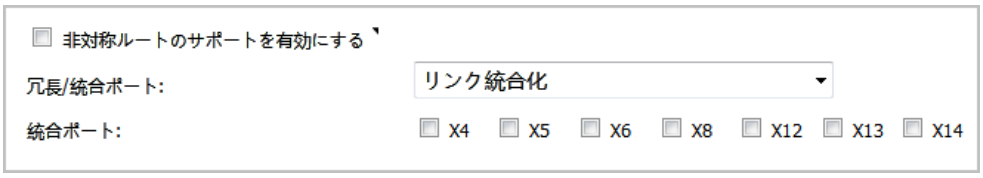
1 「**管理 | システム セットアップ** | **ネットワーク > インターフェース**」に移動します。

2 リンク統合グループのマスターとして指定するインターフェースの**設定**アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。

3 「**詳細設定**」を選択します。



4 「**冗長/統合ポート**」で、「**リンク統合化**」を選択します。その他のオプションが表示されます。

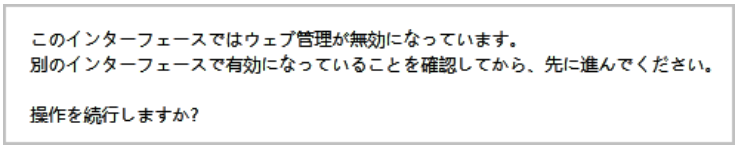


5 セキュリティ装置上の現在割り当てられていないインターフェースごとに「**統合ポート**」オプションが表示されます。ポートはどれも選択されていません。LAG に割り当てる他のインターフェースを最高 3 つまで選択します。

> **メモ**：インターフェースを LAG に割り当てると、そのインターフェースの設定はリンク統合化マスター インターフェースによって管理され、個別に設定することができなくなります。「**インターフェース設定**」テーブルには、そのインターフェースのゾーンが「**統合ポート**」として表示され、**設定**アイコンが表示されなくなります。

6 インターフェースの「**リンク速度**」を「**自動ネゴシエーション**」に設定します。

7 「**OK**」を選択します。インターフェースでウェブ管理が設定されていない場合、メッセージが表示されます。



a 「**OK**」を選択します。

b 別のインターフェースでウェブ管理を有効にします。

重要：リンク統合化には、スイッチ上に対応する設定が必要です。スイッチの負荷分散方法はベンダーによって異なります。リンク統合化の設定については、スイッチのドキュメントを参照してください。リンク統合化は、ポート チャンネル、イーサ チャンネル、トランク、ポート グルーピングなどと呼ばれることもあります。

ポート冗長化

ポート冗長化は、物理イーサネット ポートに対して冗長ポートを設定するための単純な方法です。これは単一障害点としてのスイッチの障害を防ぐのに役立つ機能であり、ハイエンドの配備では特にそうです。

プライマリ インターフェースがアクティブのとき、プライマリ インターフェースはそこを出入りするトラフィックをすべて処理します。プライマリ インターフェースがダウンすると、セカンダリ インターフェースが送受信トラフィックをすべて引き継ぎます。セカンダリ インターフェースはプライマリ インターフェースの MAC アドレスを引き継ぎ、フェイルオーバー イベントでの適切な重複回避用 ARP を送信します。プライマリ インターフェースが回復すると、プライマリ インターフェースはセカンダリ インターフェースからすべてのトラフィック処理の責務を再び引き継ぎます。

典型的なポート冗長化設定では、プライマリ インターフェースとセカンダリ インターフェースを別々のスイッチに接続します。これはプライマリ スイッチがダウンした場合のフェイルオーバー パスを提供します。両方のスイッチは同じイーサネット ドメインになければなりません。両方のインターフェースが同じスイッチに接続されている場合にもポート冗長化を設定することができます。

ポート冗長化フェイルオーバー

SonicWall は、リンク障害で接続が失われるのを防ぐために、高可用性 (HA)、負荷分散グループ (LB グループ)、ポート冗長化といった複数の方法を用意しています。セキュリティ装置上でこれらの機能が 3 つとも設定されている場合、リンク障害の際に次の優先順位が適用されます。

1 ポート冗長化

2 HA

3 LB グループ

ポート冗長化と HA を併用すると、ポート冗長化が優先されます。一般に、インターフェース フェイルオーバーは HA フェイルオーバーを発生させますが、そのインターフェースで冗長ポートが利用可能であれば、インターフェース フェイルオーバーが発生しても HA フェイルオーバーは発生しません。プライマリ ポートとセカンダリの冗長ポートが両方ともダウンした場合は、HA フェイルオーバーが発生します (ただし、セカンダリ セキュリティ装置の対応するポートがアクティブであると仮定します)。

ポート冗長化と LB グループを併用しても、やはりポート冗長化が優先されます。1 つのポート (プライマリまたはセカンダリ) の障害であれば、HA の場合と同様にポート冗長化で処理されます。両方のポートがダウンした場合は、LB が作動し、代替インターフェースを探します。

ポート冗長化の設定

ポート冗長化を設定するには、以下の手順に従います。

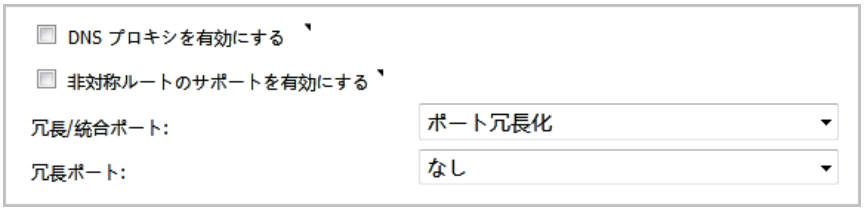
1 「**管理 | システム セットアップ | ネットワーク > インターフェース**」に移動します。

2 リンク統合グループのマスターとして指定するインターフェースの**設定**アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。

3 「**詳細設定**」を選択します。

4 インターフェースの「**リンク速度**」を「**自動ネゴシエーション**」に設定します。

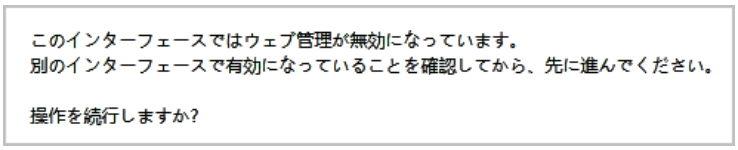
5 「**冗長/統合ポート**」で、「**ポート冗長化**」を選択します。別のオプションが表示されます。



6 この「**冗長ポート**」オプションには、現在割り当てられていない利用可能なインターフェースがすべて表示されます。いずれかのインターフェースを選択します。既定では「**なし**」になっています。

メモ：いずれかのインターフェースを冗長ポートとして選択すると、そのインターフェースの設定はプライマリ インターフェースによって管理され、個別に設定することができなくなります。「**インターフェース設定**」テーブルには、そのインターフェースのゾーンが「**冗長ポート**」として表示され、**設定**アイコンが表示されなくなります。

7 「**OK**」を選択します。インターフェースでウェブ管理が設定されていない場合、メッセージが表示されます。



a 「**OK**」を選択します。

b 別のインターフェースでウェブ管理を有効にします。

仮想インターフェース (VLAN サブインターフェース)

VLAN サブインターフェースを追加する場合は、それをゾーンに割り当て、VLAN タグを割り当てて、さらに物理インターフェースに割り当てる必要があります。ゾーンの割り当てに基づき、同じゾーンの物理インターフェースを設定するときと同じように VLAN サブインターフェースを設定します。

仮想インターフェースを追加するには、次の手順に従います。

1 「**管理 | システム セットアップ | ネットワーク > インターフェース**」に移動します。

2 「**インターフェース設定**」テーブル下部の「**インターフェースの追加**」で「**仮想インターフェース**」を選択します。「**インターフェースの追加**」ダイアログが表示されます。

3 インターフェースに割り当てるゾーンを選択します。LAN、WAN、DMZ、WLAN、または個別ゾーンを選択できます。ゾーンの割り当ては、必ずしも親 (物理) インターフェースと合わせる必要はありません。実際、親インターフェースを**未定義**のままにすることも可能です。

サブインターフェースのネットワーク設定で何を選択するかは、選択したゾーンによって異なります。

- **LAN**、**DMZ**、または保護種別の個別ゾーン -**静的**または**トランスペアレント**
- **WLAN** または個別無線ゾーン - 静的 IP のみ (モードはリストされない)

4 「**VLAN タグ**」フィールドで、VLAN タグ (ID) をサブインターフェースに割り当てます。有効な VLAN ID は **0** (既定値) ～ 4094 です。ただし、一部のスイッチでは、VLAN 1 がネイティブ VLAN 指定用に予約され、VLAN 0 が QoS 用に予約されています。お使いのセキュリティ装置で保護したい VLAN ごとに、対応する VLAN ID を持つ VLAN サブインターフェースを作成する必要があります。

重要：がプロビジョニングされている場合、0 - 35 の VLAN ID は内部 VLAN ID であり、VLAN サブインターフェースには使用できません。

5 このサブインターフェースが属することになる親 (物理) インターフェースを「**親インターフェース**」で選択します。1 つのインターフェースに対して割り当てることのできるサブインターフェース数に制限はありません。 サブインターフェースはシステムの上限に達するまでいくつでも割り当てることができます。

6 選択したゾーンに基づき、サブインターフェースのネットワーク設定を行います。以下のインターフェース設定手順を参照してください。

- 静的インターフェースの設定 (293 ページ)
- 静的インターフェースの詳細設定 (295 ページ)
- インターフェースのトランスペアレント IP モード (L3 サブネットを結合) の設定 (303 ページ)
- 無線インターフェースの設定 (307 ページ)
- WAN インターフェースの設定 (313 ページ)

7 サブインターフェースの管理方法とユーザのログイン方法を選択します。

8 「**OK**」を選択します。

IPS スニッファ モードの設定

セキュリティ装置を設定して IPS スニッファ モードを有効にするには、同じゾーンにある 2 つのインターフェースを L2 ブリッジ ペアに使用します。WAN インターフェース以外のインターフェースであれば、どれでも使用できます。この例では、X2 と X3 がブリッジ ペアに使用され、LAN ゾーン内で設定されています。WAN インターフェース (X1) は、必要に応じて セキュリティ装置データ センターにアクセスするためにセキュリティ装置で使用されます。スイッチ上のミラーリングされたポートは、ブリッジ ペアの一方のインターフェースに接続しています。

トピック:

- IPS スニッファ モード用の設定タスク リスト (328 ページ)
- プライマリ ブリッジ インターフェースの設定 (329 ページ)
- セカンダリ ブリッジ インターフェースの設定 (329 ページ)
- SNMP の有効化と設定 (330 ページ)
- IPS スニッファ モードの設定 (331 ページ)

IPS スニッファ モード用の設定タスク リスト

- プライマリ ブリッジ インターフェースの設定
  - プライマリ ブリッジ インターフェースの LAN ゾーンの選択
  - 静的IP アドレスの割り当て

- セカンダリ ブリッジ インターフェースの設定
  - セカンダリ ブリッジ インターフェースの LAN ゾーンの選択
  - プライマリ ブリッジ インターフェースへの L2 ブリッジの有効化
- SNMP の有効化と SNMP マネージャ システムのトラップ送信先 IP アドレスの設定
- LAN トラフィックのセキュリティ サービスの設定
- “警告"またはそれ以下のレベルのログ警告の設定
- スイッチ上のミラーリングされたポートをブリッジ ペアの 1 インターフェースへ接続
- インターネット経由で動的シグネチャ データを取得するための WAN の接続と設定

プライマリ ブリッジ インターフェースの設定

プライマリ ブリッジ インターフェースを設定するには、以下の手順に従います。

1 「**管理 | システム セットアップ | ネットワーク > インターフェース**」に移動します。

2 X2 インターフェースの右の列にある**設定**アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。

3 「**ゾーン**」ドロップダウン メニューから「**LAN**」を選択します。追加のオプションが表示されます。

> **メモ**：「**詳細設定**」タブまたは「**VLAN フィルタリング**」タブで設定を行う必要はありません。

4 「**ネットワーク モード**」で「**静的 IP モード**」を選択します。

5 インターフェースに静的 IP アドレス (`10.1.2.3` など) を設定します。ここで選択する IP アドレスが、スイッチから見える他のネットワークの IP アドレスと衝突しないように注意してください。

> **メモ**：プライマリ ブリッジ インターフェースには、静的 IP を割り当てる必要があります。

6 **サブネット マスク**を設定します。

7 わかりやすいコメントを入力します。

8 インターフェースに対する「**管理**」オプションを選択します。**HTTPS**、**Ping**、**SNMP**、**SSH** の中から 1 つ以上の管理オプションを選択します。

9 「**ユーザ ログイン**」オプションを選択します。**HTTP** と **HTTPS** のいずれか、または両方のプロトコルを選択します。

10 HTTP から HTTPS へのリダイレクトを有効にするには、「**HTTP から HTTPS へのリダイレクトを有効にするためのルールを追加する**」を選択します。このオプションの詳細については、「HTTP/HTTPS リダイレクト (286 ページ)」を参照してください。

11 「**OK**」を選択します。

セカンダリ ブリッジ インターフェースの設定

ここでは、例として X3 をセカンダリ ブリッジ インターフェースとして使用します。

セカンダリ ブリッジ インターフェースを設定するには、以下の手順に従います。

1 「**管理 | システム セットアップ | ネットワーク > インターフェース**」に移動します。

2 X2 インターフェースの右の列にある**設定**アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。

3 「**ゾーン**」ドロップダウン メニューから「**LAN**」を選択します。追加のオプションが表示されます。

> **メモ：**「詳細設定」タブまたは「VLAN フィルタリング」タブで設定を行う必要はありません。

4 「**ネットワーク モード**」で、「**レイヤ 2 ブリッジ モード**」を選択します。

5 「**ブリッジ先**」で、「**X2**」インターフェースを選択します。

6 IPv4 以外のトラフィックを監視する場合は、「**すべての非 IPv4 トラフィックを遮断する**」設定を有効にしないでください。

7 「**このブリッジ ペアにトラフィックをルーティングしない**」チェックボックスをオンにして、ミラーリングされたスイッチ ポートからのトラフィックがネットワークに送り返されないようにします。

8 「**このブリッジ ペアのトラフィックのみスニフする**」チェック ボックスをオンにして、ミラーリングされたスイッチ ポートから L2 ブリッジに到達したパケットのスニッファ、つまり監視を有効にします。

9 「**このブリッジ ペアでステートフル インスペクションを無効にする**」を選択して、これらのインターフェースをステートフル高可用性検査から除外します。これらのインターフェースに対して精密パケット検査が有効になっている場合、DPI サービスは引き続き適用されます。

10 インターフェースに対する「**管理**」オプションを選択します。**HTTPS**、**Ping**、**SNMP**、**SSH** の中から 1 つ以上の管理オプションを選択します。

11 「**ユーザ ログイン**」オプションを選択します。**HTTP** と **HTTPS** のいずれか、または両方のプロトコルを選択します。

12 HTTP から HTTPS へのリダイレクトを有効にするには、「**HTTP から HTTPS へのリダイレクトを有効にするためのルールを追加する**」を選択します。このオプションの詳細については、「HTTP/HTTPS リダイレクト (286 ページ)」を参照してください。

13 「**OK**」を選択します。

SNMP の有効化と設定

SNMP を有効にすると、SonicWall セキュリティ サービスが生成するゲートウェイ アンチウイルス (GAV)、侵入防御などの多くのイベントに対して自動的に SNMP トラップが発行されます。

現在、50 種類を超える IPS イベントと GAV イベントによって SNMP トラップが発行されます。『*SonicOS ログ イベント リファレンス ガイド*』には SonicOS でログを記録するイベントのリストがあり、各イベントに対応する SNMP トラップ番号も記載されています。このガイドは、https://www.sonicwall.com/ja-jp/support/ でページ上部の検索フィールドに "**Log Event**" と入力するとオンラインで入手できます。

侵入防御サービスを有効にして IPS スニッファ モードを使用する場合にトラップが発行可能かどうかを確認するには、『*SonicOS ログ イベント リファレンス ガイド*』の「ログ イベント メッセージのインデックス」セクションにある表で "**侵入**" を検索します。イベントに対応する SNMP トラップ番号があれば、表の「**SNMP トラップ タイプ**」列に記載されています。

ゲートウェイ アンチウイルス サービスを有効にして IPS スニッファ モードを使用する場合にトラップが発行可能かどうかを確認するには、表で "**セキュリティ サービス**" を検索し、**「SNMP トラップ タイプ」**列の SNMP トラップ番号を確認します。

SNMP を有効にし、設定するには、以下の手順を行います。

1 **「管理 | システム セットアップ | 装置 | SNMP」**に移動します。

2 **「SNMP を有効にする」**を選択します。

3 **「適用」**を選択します。**「設定」**が有効になり、**「表示」**、**「ユーザ/グループ」**、**「アクセス」**の各セクションが表示されます。

4 **「設定」**を選択します。**「SNMP の設定」**ダイアログが表示されます。

5 **「システム名」**フィールドに、セキュリティ装置から送信されるトラップを受け取る SNMP マネージャ システムの名前を入力します。

6 **「システムの連絡先」**フィールドに SNMP 連絡先の担当者の名前または電子メール アドレスを入力します。

7 **「システムの場所」**フィールドに、システムの場所を説明する文 (「3 階研究室」など) を入力します。

8 **「アセット番号」**フィールドに、システムのアセット番号を入力します。

9 **「Get コミュニティ名」**フィールドに、SNMP 情報をファイアウォールから受け取る権限を持つコミュニティ名 (「パブリック」など) を入力します。

10 **「Trap コミュニティ名」**フィールドに、SNMP トラップをファイアウォールから SNMP マネージャに送信する際に使うコミュニティ名 (「パブリック」など) を入力します。

11 **ホスト 1/2/3/4**の各フィールドに、トラップを受け取る SNMP マネージャ システムの IP アドレスを入力します。

12 **「OK」**を選択します。

IPS スニッファ モードの設定

IPS スニッファ モードを設定するには、以下の手順に従います。

1 **「管理 | システム セットアップ | ネットワーク > インターフェース」**に移動します。

2 **X2** インターフェースの**編集**アイコンを選択します。**「インターフェースの編集」**ダイアログが表示されます。

3 **「モード/IP 割り当て」**を**「レイヤ 2 ブリッジ モード」**に設定します。オプションが次のように変化します。

4 **「ブリッジ先:」**インターフェースを**「X0」**に設定します。

5 **「このブリッジ ペアのトラフィックのみスニフする」**を選択します。

6 **「OK」**を選択すると、変更内容が保存されて有効になります。ダイアログが閉じられ、**「ネットワーク > インターフェース」**ページが再び表示されます。

7 **X1 WAN** インターフェースの**編集**アイコンを選択します。**「インターフェースの編集」**ダイアログが表示されます。

8 X1 WAN インターフェースにネットワークの*内部* LAN セグメントの一意の IP アドレスを割り当てます。変に思われるかもしれませんが、実はこれが装置を管理するときに使うインターフェー

スです。また、このインターフェースからセキュリティ装置は SNMP トラップを送信し、セキュリティ サービス シグネチャの更新を取得します。

9 「**OK**」を選択します。

10 また、トラフィックが正常に伝わるように、ファイアウォール ルールを変更して次の方向のトラフィックを許可してください。

- LAN から WAN
- WAN から LAN

11 次のように接続します。

- スパン/ミラー スイッチ ポートをセキュリティ装置の X2 ではなく X0 に接続 (実際、X2 には何も接続されない)
- X1 を内部ネットワークに接続

重要：ポートをスパニング/ミラーリングして X0 に接続するときは慎重にプログラミングしてください。

ビデオ：インターフェースの設定例を紹介するビデオ チュートリアルがオンラインで公開されています。例えば、『How to configure the SonicWall WAN / X1 Interface with PPPoE Connection (SonicWall WAN / X1 インターフェース を PPPoE 接続に設定する方法)』をご覧ください。その他のビデオは、以下でご覧いただけます。
https://www.sonicwall.com/ja-jp/support/videos-product-select。

セキュリティ サービス (統合脅威管理) の設定

このセクションで有効にする設定に基づいて、IPS スニッファ モードで検知する悪意のあるトラフィックの種類が決まります。一般には侵入防御を有効にしますが、ゲートウェイ アンチウイルス、アンチスパイウェアなどの他のセキュリティ サービスを有効にしてもよいでしょう。

セキュリティ サービスを有効にするには、SonicWall セキュリティ装置のライセンスを取得し、シグネチャ情報を SonicWall データ センターからダウンロードする必要があります。IPS、GAV、およびアンチスパイウェアの有効化と設定の完全な手順については、『*SonicOS セキュリティ設定*』を参照してください。

トピック:

- ログの設定 (332 ページ)
- ミラーリングされたスイッチ ポートを IPS スニッファ モード インターフェースへ接続 (333 ページ)
- データ センターに接続する WAN インターフェースの設定 (333 ページ)

ログの設定

「**ログ > 設定**」ページでログを設定して、ファイアウォールで検知された攻撃についての情報を記録することができます。ログを有効にする方法については、『*SonicOS ログとレポート*』を参照してください。

ミラーリングされたスイッチ ポートを IPS スニッファ モード インターフェースへ接続

標準の Cat-5 イーサネット ケーブルを使って、ミラーリングされたスイッチ ポートとブリッジ ペアのいずれかのインターフェースを接続します。ネットワーク トラフィックは、スイッチからセキュリティ装置に自動的に送信されます。セキュリティ装置ではトラフィックを検査できます。

ミラーリングされたポートの設定手順については、スイッチのドキュメントを参照してください。

データ センターに接続する WAN インターフェースの設定

セキュリティ装置の WAN ポート (通常はポート X1) をゲートウェイまたはゲートウェイにアクセスできる機器に接続します。セキュリティ装置は、SonicWall データ センターと自動的に通信します。WAN インターフェースを設定する詳細な手順については、「WAN インターフェースの設定 (313 ページ)」を参照してください。

ワイヤ モードとタップ モードの設定

SonicOS はワイヤ モードとタップ モードをサポートしており、これにより全体的な中断を伴わずにネットワークへの挿入を段階的に増やす形で進めることができます。「ワイヤ モードとタップ モードの設定」テーブルに、ワイヤ モードとタップ モードを示します。

メモ：ワイヤ モードは NSA 2600 以降の装置でサポートされます。

ワイヤ モードとタップ モードの設定

ワイヤ モード設定	説明
バイパス モード	バイパス モードにより、ネットワークへのセキュリティ装置ハードウェアの迅速でどちらかといえば中断のない導入が可能になります。ネットワークへ挿入するポイント (例: コア スイッチと境界セキュリティ装置の間、VM サーバ ファームの前、データ分類ドメイン間の移行ポイント) を選択すると、セキュリティ装置は物理データ パスに挿入され、必要となる整備期間が非常に短くなります。セキュリティ装置上のスイッチ ポートの 1 つ以上のペアが、すべてのパケットをセグメントを越えて完全なライン速度で転送するために使われます。すべてのパケットは、マルチコア検査および強制パスに搬送されるのではなく、セキュリティ装置の 240Gbps スイッチ ファブリック上に残ります。バイパス モードは検査やファイアウォール機能を提供しないので、このモードによって最小のダウンタイムと危険をもってセキュリティ装置をネットワークに物理的に導入して、ネットワークおよびセキュリティ インフラの新しく挿入された構成要素である水準の安心感を得ることができます。その後、再設定を行うための簡素なユーザ インターフェースを通してバイパス モードから検査または保護モードに即座に移行できます。
検査モード	検査モードは、低リスク、遅延の無いパケットパスなどの機能を変えることなくバイパスモードを拡張します。パケットはセキュリティ装置のスイッチ ファブリックを通過し続けますが、それらはまた、パッシブ検査、分類、フロー報告の目的のために、マルチコア RF-DPI エンジンにミラーされます。これは、実際の中間処理なしでのセキュリティセキュリティ装置のアプリケーション情報および脅威検出機能を示します。

ワイヤ モードとタップ モードの設定 (続き)

ワイヤ モード設定	説明
保護モード	保護モードは、検査モードを進化させたもので、セキュリティ装置のマルチコア プロセッサをパケット処理パスに積極的に介入させます。これは、アプリケーション情報と制御、侵入防御サービス、ゲートウェイおよびクラウド ベースのアンチウイルス、アンチスパイウェア、そしてコンテンツ フィルタを含む、検査とポリシー エンジンの完全な機能セットを開放します。保護モードは、通常の NAT や L2 ブリッジ モードの配備と同じレベルの可視性と強制を、L3/L4 変換なしで、そして ARP やルーティング動作の変更なしで提供します。こうして保護モードは、既存のネットワーク設計への最低限の物理的変更だけで論理的変更を必要としない、少しずつ到達可能な NGFW 配備を提供します。 VLAN 変換のためにワイヤ モード ペアを作成するとき保護モードを使用してください。
タップ モード	タップ モードは検査モードと同じ可視性を提供しますが、セキュリティ装置上の単一スイッチ ポートを介してミラーされたパケット ストリームを吸収して、物理的な中間挿入の必要性を除去する点が異なります。タップ モードは、検査や収集用に外部機器にパケットを届けるためにネットワーク タップ、スマート タップ、ポート ミラー、または、SPAN ポートを利用する環境で使用するように設計されています。ワイヤ モードの他のすべての形態と同様に、タップ モードは複数同時ポート インスタンスで動作可能で、複数タップからの不連続ストリームをサポートします。

「ワイヤ モード: 機能の違い」テーブルは、インターフェース設定モード間の主な機能の違いです。

ワイヤ モード: 機能の違い

インターフェース設定	バイパス モード	検査モード	保護モード	タップ モード	L2 ブリッジ、トランスペアレント、NAT、ルート モード
アクティブ/アクティブ クラスタリング [a]	いいえ	いいえ	いいえ	いいえ	はい
アプリケーション制御	いいえ	いいえ	はい	いいえ	はい
アプリケーション可視化	いいえ	はい	はい	はい	はい
ARP/ルーティング/NAT [a]	いいえ	いいえ	いいえ	いいえ	はい
統合アンチスパム サービス [a]	いいえ	いいえ	いいえ	いいえ	はい
コンテンツ フィルタ	いいえ	いいえ	はい	いいえ	はい
DHCP サーバ [a]	いいえ	いいえ	いいえ	いいえ	はい [b]
DPI 検出	いいえ	はい	はい	はい	はい
DPI 防御	いいえ	いいえ	はい	いいえ	はい
DPI-SSL [a]	いいえ	いいえ	はい	いいえ	はい
高可用性	はい	はい	はい	はい	はい
リンク状況伝達 [c]	はい	はい	はい	いいえ	いいえ
ステートフル パケット検査	いいえ	はい	はい	はい	はい
TCP ハンドシェーク強制 [d]	いいえ	いいえ	いいえ	いいえ	はい

ワイヤ モード: 機能の違い

インターフェース設定	バイパス モード	検査モード	保護モード	タップ モード	L2 ブリッジ、トランスペアレント、NAT、ルート モード
仮想グループ[a]	いいえ	いいえ	いいえ	いいえ	はい
VLAN 変換 [e]	いいえ	いいえ	はい	いいえ	いいえ

a. これらの機能とサービスは、ワイヤ モードで設定されたインターフェースでは利用できませんが、システム全体レベルでは、他の互換性のある動作モードで設定されたどのインターフェースでも利用可能です。

b. L2 ブリッジ モードでは利用不可です。

c. **リンク状況伝播**は、ワイヤ モード ペアのインターフェースがパートナーの遷移によってトリガーされたリンク状況をミラー化する機能です。これは、冗長化パスのあるネットワークで正しい動作をするために不可欠です。リンク状況伝播は VLAN インターフェース越しのワイヤ モードではサポートされていません。

d. ワイヤ モードでは、複数のワイヤ モードのパスまたは複数のセキュリティ装置が冗長または非対称パスと共に使用されている場合に、ネットワーク上のどこかで発生するフェイルオーバー イベントがサポートされることを許可するために、設計上無効になっています。

e. VLAN 変換は VLAN インターフェース越しのワイヤ モードではサポートされていません。

メモ：ワイヤ モードで動作しているときは、ファイアウォール専用の管理インターフェースがローカル管理に使われます。リモート管理および動的なセキュリティ サービスとアプリケーション情報の更新を有効にするには、WAN インターフェース(ワイヤ モード インターフェースから独立した) をインターネット接続のために設定する必要があります。これは、SonicOS がほぼすべての組み合わせの混在モードのインターフェースをサポートするので、簡単にできます。

ワイヤ モードでのインターフェースの設定

ワイヤ モードは、WAN、LAN、DMZ、および個別ゾーン (無線ゾーンを除く) に対して設定可能です。ワイヤ モードはレイヤ 2 ブリッジ モードを簡潔にしたもので、インターフェースのペアとして設定されます。ワイヤ モードでは、送信先ゾーンは「**ペア インターフェース ゾーン**」です。送信元の「**ゾーン**」とその「**ペア インターフェース ゾーン**」間のトラフィックの方向に基づいて、アクセス ルールがワイヤ モード ペアに適用されます。例えば、送信元の「**ゾーン**」が「**WAN**」で、「**ペア インターフェース ゾーン**」が「**LAN**」の場合、トラフィックの方向に応じて WAN から LAN へのルールと LAN から WAN へのルールが適用されます。

ワイヤ モードでは、インターフェースのリンク状況をペア インターフェースに伝播する**リンク状況伝達**を有効にすることができます。インターフェースが停止すると、そのインターフェースのリンク状況をミラーリングするために、対応するペア インターフェースが強制的に停止されます。ワイヤ モード ペアのインターフェースは、どちらも常に同じリンク状況になります。

ワイヤ モードでは、**ステートフル検査**を**無効**にできます。「**ステートフル検査を無効にする**」を選択すると、ステートフル パケット検査がオフになります。「**ステートフル検査を無効にする**」が*選択されていない*場合は、3 ウェイ TCP ハンドシェーイクを強制することなく、新しい接続を確立できます。非対称ルートを配備する場合は、「**ステートフル検査を無効にする**」を選択する必要があります。

インターフェースをワイヤ モード用に設定するには、以下の手順に従います

1 「**管理 | システム セットアップ | ネットワーク > インターフェース**」に移動します。

2 ワイヤ モード用に設定するインターフェースの**設定**アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。

3 「**ゾーン**」で、WLAN 以外の任意のゾーン種別を選択します。

4 「**モード / IP 割り当て**」で、次のように選択してインターフェースを設定します。

- タップ モードの場合、「**タップ モード (1 ポート タップ)**」を選択
- ワイヤ モードの場合、「**ワイヤ モード (2 ポート ワイヤ)**」を選択

5 「**ワイヤ モード種別**」で、適切なモードを選択します。

- **バイパス (内部スイッチ/リレーによる)**
- **検査 (ミラー トラフィックのパッシブ DPI)**
- **保護 (直列トラフィックのアクティブ DPI)**

6 「**ペア インターフェース**」で、上流のセキュリティ装置に接続するインターフェースを選択します。このペア インターフェースは同じ種別 (2 つの 1 GB インターフェースまたは 2 つの 10 GB インターフェース) である必要があります。

> **メモ**：未定義のインターフェースのみが、「**ペア インターフェース**」で利用可能です。インターフェースを未定義にするには、そのインターフェースの「**設定**」を選択し、「**ゾーン**」で「**未定義**」を選択します。

7 「**OK**」を選択します。

WAN/LAN ゾーン ペアに対するワイヤ モードの設定

以下の設定は、ワイヤ モードの設定例です。この例は、LAN ゾーンとペアリングされた WAN ゾーン向けです。ワイヤ モードは、DMZ ゾーンおよび個別ゾーンに対しても設定できます。

WAN/LAN ゾーン ペアに対してワイヤ モードを設定するには:

1 「**管理 | システム セットアップ | ネットワーク > インターフェース**」に移動します。

2 次のいずれかを選択します。

- **インターフェースの追加**。
- 設定するインターフェースの**設定**アイコン

「**インターフェースの追加/編集**」ダイアログが表示されます。

3 「**ネットワーク モード**」で、「**ワイヤ モード (2 ポート ワイヤ)**」を選択します。

4 「**ゾーン**」で、「**WAN**」を選択します。

5 「**ペア インターフェース ゾーン**」で、「**LAN**」を選択します。

6 「**ステートフル検査を無効にする**」オプションを選択します。

7 「**リンク状況伝播を有効にする**」オプションを選択します。

8 「**OK**」を選択します。「**インターフェース設定**」テーブルが更新されます。

ワイヤ モードでのリンク統合

メモ：VLAN インターフェース越しのワイヤ モードは、リンク統合化をサポートしていません。

リンク統合 (LAG) は、複数のリンクを単一のインターフェースにバンドルして帯域幅を増やすために使用されます。LAG インターフェース上でトラフィックを検査するため、SonicWall セキュリティ装置をインラインで接続し、1 つのリンクに送信されるパケットを送信先に透過的にブリッジすることができます。リンク状況伝播などの既存のワイヤ モード機能がサポートされています。LAG ごとに最大 8 つのメンバーをサポートします。

ワイヤ モードでのリンク統合は、「**ネットワーク > インターフェース**」で設定します。「**リンク統合化**」が「**インターフェースの編集 > 詳細**」ダイアログで選択されている場合は、未定義のインターフェースもリストに表示されます。ワイヤ モード接続のそれぞれの側に対してメンバー インターフェースを選択できます。それぞれの側のメンバー数は同じでなければなりません。メンバー インターフェースのタイプと帯域幅サイズも一致させることをお勧めします。

ワイヤ モードでの LAG を設定するには;

1 「**管理 | システム セットアップ | ネットワーク > インターフェース**」に移動します。

2 設定するインターフェースの**設定**アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。

3 「**ゾーン**」で、適切なゾーンを選択します。オプションが次のように変化します。

4 「**モード / IP 割り当て**」で、「**ワイヤ モード (2 ポート ワイヤ)**」を選択します。再びオプションが変化します。

5 「**ワイヤ モード種別**」で、「**保護 (直列トラフィックのアクティブ DPI)**」を選択します。

6 「**ペア インターフェース**」から、ペアにするインターフェースを選択します。

7 「**ペア インターフェース ゾーン**」から、ペアにするインターフェースのゾーンを選択します。

8 「**ステートフル検査を無効にする**」オプションを選択します。このオプションは、既定では選択されています。

9 必要に応じて、「**リンク状況伝播を有効にする**」オプションを選択します。このオプションは、既定では選択されていません。

10 「**詳細設定**」を選択します。

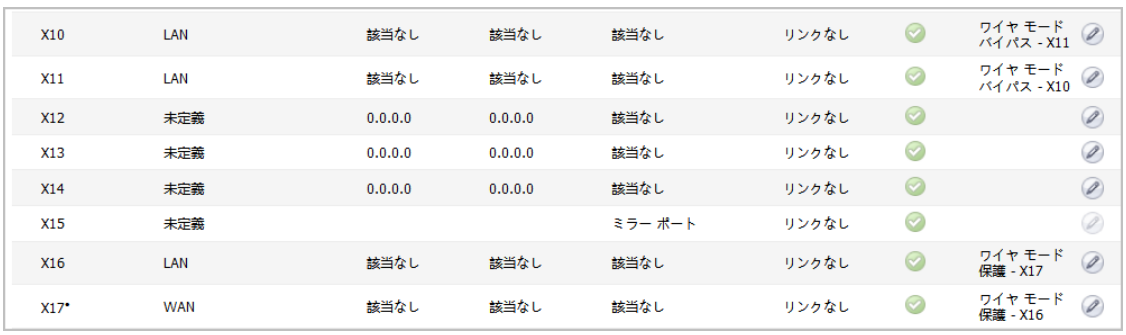
「詳細設定」での設定を続行するには、以下の手順に従います。

1 「**冗長/統合ポート**」で、「**リンク統合化**」を選択します。オプションが次のように変化します。

2 「**統合ポート**」で、統合するポートを選択します。

3 「**ペア インターフェース統合ポート**」から、統合するペア ポートを選択します。

4 「**OK**」を選択します。設定が「**ネットワーク > インターフェース**」の「**インターフェース設定**」テーブルに表示されます。



レイヤ 2 ブリッジ モード

SonicOS には、セキュリティ装置をあらゆるイーサネット ネットワークに透過的に統合するための手法として、**L2 (レイヤ 2) ブリッジ モード**が備わっています。L2 ブリッジ モードは、セキュリティ装置が、2 つのインターフェース間で共通のサブネットを共有し、すべての IP トラフィックに対してステートフルな精密パケット検査を実行できるという点で、見かけ上は SonicOS のトランスペアレント モードに似ていますが、機能的にはより多目的な用途に対応しています。

L2 ブリッジ モードでは、セキュリティで保護された学習ブリッジ手法が採用されているため、他の多くの透過的なセキュリティ装置統合方式では処理できない種類のトラフィックを通過させ、検査することができます。L2 ブリッジ モードを使うと、既存のイーサネット ネットワークに影響を与えずに SonicWall セキュリティ装置を追加して、インラインの精密パケット検査機能をすべての IPv4 TCP と UDP のトラフィックに提供することができます。このシナリオでは、セキュリティ装置がセキュリティを適用するためではなく、両方向のスキャン、ウイルスとスパムの遮断、および侵入の阻止に使用します。

他の透過的なソリューションとは異なり、L2 ブリッジ モードは、IEEE 802.1Q VLAN、Spanning Tree Protocol、マルチキャスト、ブロードキャスト、IPv6 を含む、すべての種類のトラフィックを通過させるため、いずれのネットワーク通信も中断されることはありません。

L2 ブリッジ モードの多目的性を示すもう 1 つの例が、このモードを使用して IPS スニッファ モードを設定できることです。IPS スニッファ モードは、SonicWall セキュリティ装置でサポートされ、ブリッジ ペアの 1 インターフェースを使用してスイッチ上のミラーリングされたポートからのネットワーク トラフィックを監視します。IPS スニッファ モードでは侵入検知が可能ですが、セキュリティ装置がトラフィック フローにインラインで接続されていないため、悪意のあるトラフィックを遮断することはできません。IPS スニッファ モードの詳細については、「IPS スニッファ モード (283 ページ)」を参照してください。

L2 ブリッジ モードは、既存のセキュリティ装置が存在し、既存のセキュリティ装置を変更する計画が当面はなく、一方で SonicWall 精密パケット検査とセキュリティ サービスのセキュリティ機能 (侵入防御サービス、ゲートウェイ アンチウイルス、ゲートウェイ アンチスパイウェアなど) を追加する必要のあるネットワークにとって理想的なソリューションです。SonicWall セキュリティ サービスを購読していない場合は、MySonicWall で無料トライアルに申し込むことができます。

L2 ブリッジ モードは高可用性を備えた配備でも使用できます。このシナリオについては、「高可用性を備えたレイヤ 2 ブリッジ モード (356 ページ)」で説明します。

メモ：リンク統合化は、レイヤ 2 ブリッジ モードではサポートされません。

トピック:

- SonicOS レイヤ 2 ブリッジ モードの主要な機能 (340 ページ)
- L2 ブリッジ モードとトランスペアレント モードの設定に関連した重要な概念 (340 ページ)
- L2 ブリッジ モードとトランスペアレント モードの比較 (342 ページ)
- L2 ブリッジ パスの決定 (350 ページ)
- L2 ブリッジ インターフェース ゾーンの選択 (351 ページ)
- サンプル トポロジ (353 ページ)

SonicOS レイヤ 2 ブリッジ モードの主要な機能

「SonicOS レイヤ 2 ブリッジ モード: 主要な機能と利点」テーブルは、レイヤ 2 ブリッジ モードの主要な機能とその利点をまとめたものです。

SonicOS レイヤ 2 ブリッジ モード: 主要な機能と利点

機能	利点
精密パケット検査を備えた L2 ブリッジング	アドレスの再割り当てや再構成を行うことなく、SonicWall セキュリティ装置をあらゆるネットワークに追加でき、かつ、既存のネットワーク デザインを変更することなく、精密パケット検査のセキュリティ サービスを追加できるトランスペアレントな処理手法です。L2 ブリッジ モードは、セキュリティと同程度に接続性を重視して設計され、あらゆる種類のイーサネット フレームを通過させることができるため、シームレスな統合が可能となります。
セキュリティで保護された学習ブリッジ手法	許可されているすべてのトラフィックが L2 ブリッジを介してネイティブに通過できなければ、真の L2 動作とは言えません。L2 ブリッジ モード以外のトランスペアレント処理手法は、透過性を実現するために ARP やルート操作に依存しており、そのことが原因で問題が生じることも少なくありません。これに対し、L2 ブリッジ モードでは、ネットワークのトポロジを動的に学習することによって最適なトラフィック パスが決定されます。
あらゆるイーサネット フレーム タイプのサポート	すべてのイーサネット トラフィックが L2 ブリッジを通過できます。つまり、どのようなネットワーク通信も中断されることはありません。その他多くのトランスペアレント処理手法が IPv4 トラフィックしかサポートしていないのに対し、L2 ブリッジ モードは、すべての IPv4 トラフィックを検査したうえで、その他すべてのトラフィック (LLC、全 Ethertype、独自フレーム形式など) を通過させるか、必要であれば遮断します。
混在モード処理	L2 ブリッジ モードは、L2 ブリッジに加え、従来のセキュリティ装置のサービス (ルーティング、NAT、VPN、無線動作など) を同時に提供します。したがって、ネットワークの特定のセグメントでは L2 ブリッジとして使用しながら、それ以外のセグメントにはセキュリティ サービス一式をすべて提供するといったことも可能です。SonicWall セキュリティ装置をピュア L2 ブリッジとして導入しておき、将来、必要に応じて完全なセキュリティ サービス動作に移行させることもできます。
無線 レイヤ 2 ブリッジ	LAN、WLAN、DMZ、または個別ゾーンなど、複数のゾーン タイプにわたって単一の IP サブネットを使用します。この機能により、無線クライアントと有線クライアントは、DHCP アドレスなどの同じネットワーク リソースをシームレスに共有できます。レイヤ 2 プロトコルはペアインターフェースの間で動作可能で、ブロードキャスト パケットや非 IP パケットなど、複数のトラフィック種別がブリッジを通過できるようにします。

L2 ブリッジ モードとトランスペアレント モードの設定に関連した重要な概念

L2 ブリッジ モードの運用と設定について言及する際、次のような用語が使用されます。

- **L2 ブリッジ モード** - SonicWall セキュリティ装置の設定手法の 1 つです。ファイアウォールをインラインで既存のネットワークに追加でき、トランスペアレント モードを超える完全な透過性を実現します。レイヤ 2 ブリッジ モードは、*ブリッジ ペアの セカンダリ ブリッジ インターフェース*に対して選択された*ネットワーク モード*設定と言うこともできます。
- **トランスペアレント モード** - SonicWall セキュリティ装置の設定方法の 1 つです。自動的に適用される ARP とルーティング ロジックを使用し、単一の IP サブネットを複数のインターフェースにスパニングすることにより、IP を設定し直すことなく、セキュリティ装置を既存のネットワークに追加できるようにします。
- **ネットワーク モード** - 保護インターフェース (LAN) またはパブリック インターフェース (DMZ) を設定するとき、インターフェースのネットワーク モードとして、次のいずれかを選択できます。
  - **静的** - インターフェースの IP アドレスを手動で入力します。
  - **トランスペアレント モード** - インターフェースの IP アドレスが、WAN プライマリ IP サブネット範囲内のアドレス オブジェクト (ホスト、範囲、またはグループ) を使って割り当てられ、WAN インターフェースから、割り当てられているインターフェースへとサブネットを効果的にスパニングすることができます。
  - **レイヤ 2 ブリッジ モード** - このモードで設定されたインターフェースは、同じブリッジ ペアの *プライマリ ブリッジ インターフェース*に対する *セカンダリ ブリッジ インターフェース*になります。このブリッジ ペアは、完全な L2 透過性を備えた 2 ポートの学習ブリッジのように振る舞い、それを通過するすべての IP トラフィックは完全なステートフル フェイルオーバーと精密パケット検査の対象となります。
- **ブリッジ ペア** - *プライマリ ブリッジ インターフェース*と *セカンダリ ブリッジ インターフェース*の組み合わせから成る論理的なインターフェースです。ここで言うプライマリとセカンダリは、本質的な動作上の優位性や主従関係を表すものではありません。 どちらのインターフェースも絶えずそれぞれのゾーン タイプに従って扱われ、設定されているアクセス ルールに従って IP トラフィックを通過させます。ブリッジ ペアを通過する非 IPv4 トラフィックは、*セカンダリ ブリッジ インターフェース*の「*すべての非 IPv4 トラフィックをブロックする*」の設定によって制御されます。サポートされるブリッジ ペアの数は、利用可能なインターフェースのペアに依存します。つまり、ブリッジ ペアの最大数は、プラットフォーム上の物理インターフェース数を 2 で割った値になります。ブリッジ ペアに属しているからといって、インターフェースの従来の動作が妨げられることはありません。例えば、X1 が、X3 を *セカンダリ ブリッジ インターフェース*とするブリッジ ペアの *プライマリ ブリッジ インターフェース*として設定されている場合、X1 は、同時にプライマリ WAN としての従来の役割を果たし、*自動的に追加される X1 の既定 NAT ポリシー*を介して、インターネット宛てのトラフィックの NAT 変換を実行できます。
- **プライマリ ブリッジ インターフェース** - *セカンダリ ブリッジ インターフェース*と対をなすインターフェースの呼称です。プライマリ ブリッジ インターフェースは、非保護ゾーン (WAN)、保護ゾーン (LAN)、パブリック ゾーン (DMZ) のいずれかに所属することができます。
- **セカンダリ ブリッジ インターフェース** - *ネットワーク モード*が*レイヤ 2 ブリッジ モード*に設定されたインターフェースの呼称です。セカンダリ ブリッジ インターフェースは、保護ゾーン (LAN) またはパブリック ゾーン (DMZ) に所属することができます。
- **ブリッジ管理アドレス** - プライマリ ブリッジ インターフェースのアドレスは、*ブリッジ ペア*の両方のインターフェースによって共有されます。プライマリ ブリッジ インターフェースがプライマリ WAN インターフェースとしても機能する場合、セキュリティ装置の発信通信 (NTP など) やライセンス マネージャの更新には、このアドレスが使用されます。また、*混在モード*の配備において、ブリッジ ペアのいずれかのセグメントに接続されたホストが、そのゲートウェイとしてブリッジ管理アドレスを使用する場合もあります。
- **ブリッジ パートナー** - *ブリッジ ペア*のもう一方のメンバーを指す用語です。

- **非 IPv4 トラフィック** - SonicOS は以下の IP プロトコル種別をサポートします。ICMP (1)、IGMP (2)、TCP (6)、UDP (17)、GRE (47)、ESP (50)、AH (51)、EIGRP (88)、OSPF (89)、PIM-SM (103)、L2TP (115)。Combat Radio Transport Protocol (126) などの特殊な IP 種別や IPX、(現時点では) IPv6 などの非 IPv4 トラフィック種別については、セキュリティ装置でネイティブに処理することはできません。非 IPv4 トラフィックは、L2 ブリッジ モードの設定により通過させるか破棄することができます。
- **キャプティブ ブリッジ モード** - L2 ブリッジ動作のこのオプション モードでは、L2 ブリッジに到着したトラフィックを非ブリッジ ペア インターフェースに転送することができません。既定では、L2 ブリッジのロジックにより、L2 ブリッジに到着したトラフィックは ARP およびルーティング テーブルによって決定される最適なパスに従って送信先に転送されます。場合によっては、こうした最適なパスで非ブリッジ ペア インターフェースへのルーティングや NAT 変換が必要になることがあります。キャプティブ ブリッジ モードを有効にすると、L2 ブリッジに到着するトラフィックは論理的に最適なパスを取ることなく L2 ブリッジを出て行きます。一般に、このモードの動作が必要になるのは、冗長なパスが存在する複雑なネットワークでパスの厳守が求められる場合に限られます。
- **ピュア L2 ブリッジ トポロジ** - ネットワークにインライン セキュリティを提供することを目的とし、セキュリティ装置を厳密な *L2 ブリッジ モード*で使用することをいいます。つまり、*ブリッジ ペア*の一方の側に着信したトラフィックは常にもう一方の側に宛てて送出されます。異なるインターフェースを介してルーティングまたは NAT 変換されることはありません。既に境界セキュリティ装置が存在する場合や、既存のネットワークの特定のパス (部門間または 2 つのスイッチ間のトランク リンクなど) に沿ったインライン セキュリティが求められる場合に用いられる代表的なトポロジです。ピュアL2 ブリッジ トポロジは機能的な制約を意味するものではなく、むしろ混成環境における一般的な配備を表すトポロジ上の概念と言えます。
- **混在モード トポロジ** - セキュリティ装置を介した受信/送信のポイントが*ブリッジ ペア*以外にも存在する配備をいいます。つまり、*ブリッジ ペア*の一方の側に着信したトラフィックは、異なるインターフェースを介してルーティングまたは NAT 変換されることもあります。例えば、次のような環境が既に整っているとき、同時にセキュリティ装置を使用することで、1 つまたは複数のブリッジ ペアにセキュリティを提供できます。
    - ブリッジ ペアまたは他のインターフェース上のホストに対する境界セキュリティ (WAN 接続など)。
    - 保護 (LAN) インターフェースや公開 (DMZ) インターフェースなど、追加のセグメントに対するファイアウォールやセキュリティ サービス。この場合、これらのセグメント上のホストと、ブリッジ ペア上のホストとの間で通信を行うことになります。
    - SonicPoint による無線サービス。この場合、無線クライアントと、ブリッジ ペア上のホストとの間で通信が行われます。

L2 ブリッジ モードとトランスペアレント モードの比較

トランスペアレント モードでは、SonicOS が実行されているセキュリティ装置を、アドレスの再割り当てなしに既存のネットワークに導入できますが、この場合、特に ARP、VLAN サポート、複数サブネット、非 IPv4 トラフィック種別に関して、ある程度の中断を伴います。例えば、統合に伴う中断を最小限に抑えることを優先し、トランスペアレント モードの SonicWall セキュリティ装置をネットワークに追加したとします。この構成の特徴を次に示します。

- 予定外のダウンタイムがまったく発生しないか、発生したとしても無視できるほど小さい。
- ネットワークのどの部分にもアドレスの再割り当てが不要。
- (ルータが ISP によって所有されている場合によく見られるような) ゲートウェイ ルータの再設定や変更が不要。

トピック:

- トランスペアレント モードでの ARP (343 ページ)
- トランスペアレント モードの VLAN サポート (343 ページ)
- トランスペアレント モードでの複数サブネット (344 ページ)
- トランスペアレント モードの非 IPv4 トラフィック (344 ページ)
- L2 ブリッジ モードでの ARP (344 ページ)
- L2 ブリッジ モードでの VLAN サポート (344 ページ)
- L2 ブリッジの IP パケット パス (345 ページ)
- L2 ブリッジ モードでの複数サブネット (346 ページ)
- L2 ブリッジ モードでの非 IPv4 トラフィック (347 ページ)
- L2 ブリッジ モードとトランスペアレント モードの比較 (347 ページ)
- L2 ブリッジ モードにはないトランスペアレント モードのメリット (350 ページ)

トランスペアレント モードでの ARP

トランスペアレント モードでは、ARP (Address Resolution Protocol: ネットワーク インターフェース カードの一意のハードウェア アドレスと IP アドレスとを関連付けるメカニズム) が*プロキシされます*。左側のワークステーションまたはサーバが、過去にルータ (192.168.0.1) の MAC アドレスを 00:99:10:10:10:10 に解決したことがある場合、これらのホストが セキュリティ装置 を介して通信を行うためには、このキャッシュされた ARP 登録がクリアされている必要があります。これは、セキュリティ装置が、トランスペアレント モード動作のインターフェースに接続されているホストに代わって、ゲートウェイの IP (192.168.0.1) をプロキシ (つまり、代理で応答する) するためです。したがって、左側のワークステーションが 192.168.0.1 の解決を試みるために ARP 要求を送信すると、セキュリティ装置が自分の X0 の MAC アドレス (00:06:B1:10:10:10) を返すことによって応答します。

同様に、セキュリティ装置がその X1 (プライマリ WAN) インターフェースで ARP 要求を受信した場合、トランスペアレント モードのインターフェースに割り当てられたトランスペアレント範囲 (192.168.0.100〜192.168.0.250) に指定されている IP アドレスを対象に ARP のプロキシを行います。ルータが過去にサーバ (192.168.0.100) の MAC アドレスを 00:AA:BB:CC:DD:EE に解決したことがある場合、セキュリティ装置 を介してホストと通信するためには、このキャッシュされた ARP 登録がクリアされている必要があります。通常、そのためには、管理インターフェースを使用するか、再起動することによって、ルータの ARP キャッシュを消去する必要があります。ルータの ARP キャッシュがクリアされると、このルータは、192.168.0.100 に対する新しい ARP 要求を送信できます。セキュリティ装置は、それに対する応答として、X1 の MAC アドレスである 00:06:B1:10:10:11 を返します。

トランスペアレント モードの VLAN サポート

上図のネットワークは単純なものですが、VLAN を使ってトラフィックをセグメント化する大規模なネットワークでは決して珍しくありません。スイッチとルータ間のリンクが VLAN トランクであるようなネットワークの場合、リンクのいずれかの側のサブインターフェースへの VLAN を、トランスペアレント モードの SonicWall セキュリティ装置で終端させることはできますが、一意のアドレス割り当てが必要となります。つまり、非トランスペアレント モードの動作となるため、少なくとも一方の側のアドレスを再割り当てする必要があります。これは、トランスペアレント モードのアドレス空間の*送信元*として使用できるのはプライマリ WAN インターフェースだけであるためです。

トランスペアレント モードでの複数サブネット

大規模なネットワークでは、単一の有線上、複数の有線上、別個の VLAN 上、またはそれらを組み合わせた回線上で、複数のサブネットが使用されることも少なくありません。トランスペアレント モードは、静的 ARP エントリとルート エントリを使って複数のサブネットをサポートできます。

トランスペアレント モードの非 IPv4 トラフィック

トランスペアレント モードでは、非 IPv4 トラフィックがすべて破棄 (および通常はログに記録) されるため、他の種類のトラフィック (IPX など、処理されない IP タイプ) が通過することはできません。

L2 ブリッジ モードでは、こうしたトランスペアレント モード配備の一般的な問題を解決できます。この点については、以下のセクションで説明します。

- L2 ブリッジ モードでの ARP (344 ページ)
- L2 ブリッジ モードでの VLAN サポート (344 ページ)
- L2 ブリッジの IP パケット パス (345 ページ)
- L2 ブリッジ モードでの複数サブネット (346 ページ)
- L2 ブリッジ モードでの非 IPv4 トラフィック (347 ページ)
- L2 ブリッジ モードとトランスペアレント モードの比較 (347 ページ)
- L2 ブリッジ モードにはないトランスペアレント モードのメリット (350 ページ)

L2 ブリッジ モードでの ARP

L2 ブリッジ モードには、どのホストが、L2 ブリッジ (ブリッジ ペア) のどのインターフェース上に存在するかを動的に調査する学習ブリッジ設計が採用されています。ARP はネイティブに通過します。つまり、L2 ブリッジを介して通信を行うホストからは、そのピアの実際のホスト MAC アドレスが見えます。例えば、ルータ (192.168.0.1) と通信しているワークステーションは、ルータを 00:99:10:10:10:10 として認識し、ルータはワークステーション (192.168.0.100) を 00:AA:BB:CC:DD:EE として認識します。

この動作により、L2 ブリッジ モードで動作する SonicWall セキュリティ装置は、物理的な挿入に伴う一時的な中断を除けば、ほとんどのネットワーク通信を中断させることなく、既存のネットワークに導入できます。

メモ：L2 ブリッジ モードのセキュリティ装置を挿入した場合は、ストリームベースの TCP プロトコル通信 (クライアントとサーバ間の FTP セッションなど) を再度確立する必要があります。これは、ステートフル パケット検査によりもたらされるセキュリティを維持することを目的としています。ステートフル パケット検査エンジンは、自分より前に存在していた TCP 接続に関する情報を持ちません。そのため、これらの*確立済み*のパケットはログ イベント (*存在しない接続または終了済みの接続で TCP パケットが受信されたために、その TCP パケットは破棄された* など) を伴って破棄されます。

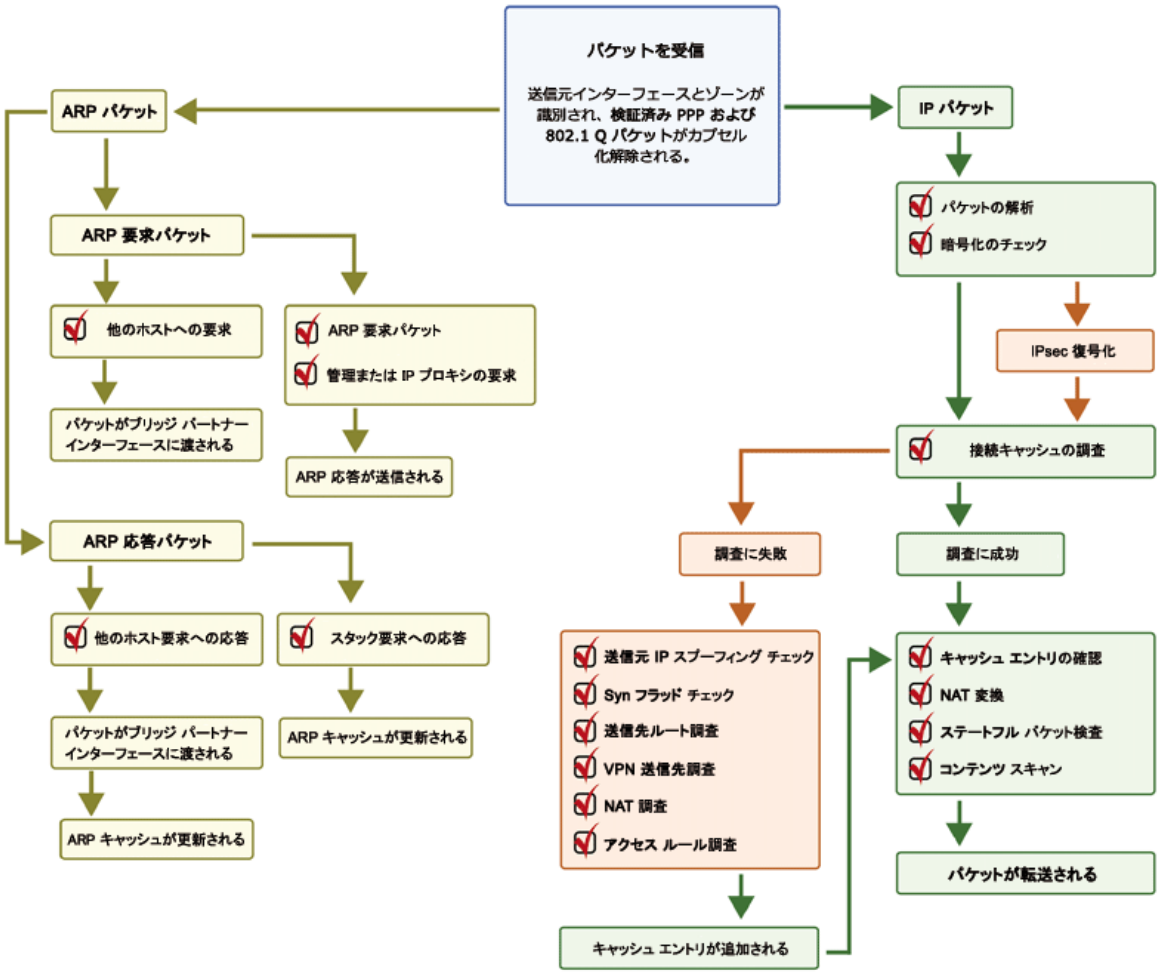
L2 ブリッジ モードでの VLAN サポート

SonicWall セキュリティ装置の L2 ブリッジ モードでは、L2 ブリッジを通過する 802.1Q VLAN トラフィックをきめ細かく制御できます。VLAN の既定の処理では、カプセル化されたトラフィックに、あらゆるファイアウォール ルール、および、ステートフル精密パケット検査を適用しながら、L2 ブリッジを通過するすべての 802.1Q VLAN タグが許可および維持されます。さらに、L2 ブリッジでは、許可/禁止された VLAN ID のホワイト/ブラック リストを指定することも可能です。

例えば、任意の数の VLAN を持つ VLAN トランクに対し、L2 ブリッジ モードで動作するセキュリティ装置をインラインで挿入し、いずれの VLAN ID またはサブネットにも明示的な設定を施すことなく、その VLAN を通過するすべての IPv4 トラフィックに完全なセキュリティ サービスを提供できます。VLAN トラフィックの処理手法により、必要であれば、L2 ブリッジ モード経由で通過するすべての VLAN トラフィックにアクセス ルールを適用することもできます。

L2 ブリッジの IP パケット パス

L2 ブリッジの IP パケット フロー



次のイベント シーケンスは、「L2 ブリッジの IP パケット フロー」のフローを説明するものです。

1 802.1Q カプセル化フレームが L2 ブリッジ インターフェースに到着します (この最初の手順、「ステップ 2」、および「ステップ 12」は、802.1Q VLAN トラフィックにのみ当てはまります)。

2 802.1Q VLAN ID が VLAN ID のホワイト/ブラック リストと照らしてチェックされます。VLAN ID:

- 禁止されていた場合、パケットは破棄されてログに記録されます。
- 許可されていた場合、パケットのカプセル化が解除され、VLAN ID が格納されて、内部パケット (IP ヘッダーを含む) がフル パケット ハンドラを介して渡されます。

3 L2 ブリッジでは任意の数のサブネットがサポートされるため、パケットの送信元 IP に対する送信元 IP スプーフィング チェックは実行されません。アクセス ルールを使って特定のサブネットだけをサポートするように L2 ブリッジを設定することもできます。

4 SYNフラッド チェックが実行されます。

5 適切なアクセス ルールを適用するため、送信先ゾーンに対して送信先ルート調査が実行されます。送信元ゾーンと同じゾーン (LAN から LAN など)、非保護ゾーン (WAN)、暗号化 (VPN)、無線 (WLAN)、マルチキャスト、任意のタイプの個別ゾーンを含め、すべてのゾーンが有効な送信先になります。

6 NAT 調査が実行され、必要に応じて適用されます。

- 一般に、L2 ブリッジに到達したパケットの送信先は*ブリッジ パートナー* インターフェース (つまり、ブリッジのもう一方の側) です。この場合、変換は一切実行されません。
- *混在モードのトポロジ*で多く見られるように、L2 ブリッジ管理アドレスがゲートウェイである場合、NAT が必要に応じて適用されます (詳細については、「L2 ブリッジ パスの決定 (350 ページ)」を参照してください)。

7 パケットにアクセス ルールが適用されます。例えば、SonicWall セキュリティ装置の場合、次のパケット デコードは、VLAN ID 10、送信元 IP アドレス `110.110.110.110`、送信先 IP アドレス `4.2.2.1` の ICMP パケットを示しています。

```
⊞ Frame 219 (102 bytes on wire, 102 bytes captured)
⊞ Ethernet II, Src: 08:00:46:a2:eb:4d (08:00:46:a2:eb:4d), Dst: 99:88:77:66:55:44 (99:88:77:66:55:44)
⊟ 802.1Q Virtual LAN
    000. .... .... .... = Priority: 0
    ...0 .... .... .... = CFI: 0
    .... 0000 0000 1010 = ID: 10
    Type: IP (0x0800)
⊞ Internet Protocol, Src: 110.110.110.110 (110.110.110.110), Dst: 4.2.2.1 (4.2.2.1)
⊞ Internet Control Message Protocol
```

VLAN のメンバーシップに関係なく、どの IP 要素 (送信元 IP、送信先 IP、サービス種別など) でも任意の IP パケットを制御するアクセス ルールを作成できます。禁止されたパケットは破棄されてログに記録されます。許可されたパケットは引き続き処理されます。

8 パケットに対する接続キャッシュ エントリが作成され、必要に応じて NAT 変換が実行されます。

9 TCP、VoIP、FTP、MSN、Oracle、RTSP のほか、メディア ストリーム、PPTP、およびL2TP に対するステートフル パケット検査および変換が実行されます。禁止されたパケットは破棄されてログに記録されます。許可されたパケットは引き続き処理されます。

10 GAV、IPS、アンチスパイウェア、CFS、電子メール フィルタなどの精密パケット検査が実行されます。禁止されたパケットは破棄されてログに記録されます。許可されたパケットは引き続き処理されます。クライアント通知が設定どおりに実行されます。

11 パケットの宛先が暗号化ゾーン (VPN)、非保護ゾーン (WAN)、またはその他の接続インターフェース (非保護ゾーンとその他の接続インターフェースは、通常、混在モード トポロジの場合に該当) であった場合、パケットは適切なパスを介して送信されます。

12 パケットの宛先が VPN/WAN/接続インターフェースではなかった場合、保存されていた VLAN タグが復元され、(再び元の VLAN タグを持った) パケットが*ブリッジ パートナー* インターフェースへと送出されます。

L2 ブリッジ モードでの複数サブネット

「L2 ブリッジの IP パケット パス (345 ページ)」の説明にあるように、L2 ブリッジ モードでは、ブリッジを介して任意の数のサブネットを処理できます。既定では、すべてのサブネットが許可されますが、アクセス ルールを適用してトラフィックを制御することも可能です。

L2 ブリッジ モードでの非 IPv4 トラフィック

サポート対象外のトラフィックは、既定では、L2 ブリッジ インターフェースからブリッジ パートナー インターフェースへと渡されます。これにより、セキュリティ装置は LLC パケット (Spanning Tree など) や他の EtherType (MPLS ラベル スイッチ パケット (EtherType 0x8847)、Appletalk (EtherType 0x809b)、Banyan Vines (EtherType 0xbad)) など、IPv4 以外のトラフィックを通過させることができます。これらの非 IPv4 パケットはブリッジを通過するだけで、パケット ハンドラによって検査されることも、制御されることもありません。これらのトラフィック タイプが不要である場合は、「**セカンダリ ブリッジ インターフェース**」設定ダイアログの「**すべての非 IPv4 トラフィックをブロックする**」オプションを有効にすることで、ブリッジの動作を変更できます。

L2 ブリッジ モードとトランスペアレント モードの比較

L2 ブリッジ モードとトランスペアレント モードの比較

項目	レイヤ 2 ブリッジ モード	トランスペアレント モード
動作のレイヤ	レイヤ 2 (MAC)	レイヤ 3 (IP)
ARP 動作	ARP (Address Resolution Protocol) の情報は変更されません。MAC アドレスはそのままの形で L2 ブリッジを通過します。SonicWall セキュリティ装置の MAC アドレスを宛先とするパケットは処理され、それ以外のパケットは通過します。送信元と送信先が学習されてキャッシュされます。	ARP は、トランスペアレント モードで動作するインターフェースによってプロキシされます。
パスの決定	ブリッジ ペアのいずれかの側のホストが、動的に学習されます。インターフェースの関連付けを宣言する必要はありません。	プライマリ WANインターフェースは、常にトランスペアレント モード トラフィックおよびサブネット空間決定のマスター受信/送信ポイントになります。このサブネット空間を透過的に共有するホストは、アドレス オブジェクトの割り当てを使用して明示的に宣言されている必要があります。
最大インターフェース数	2 つ (プライマリ ブリッジ インターフェースおよびセカンダリ ブリッジ インターフェース)。	複数のインターフェース。マスター インターフェースは常にプライマリ WANになります。利用可能なインターフェースさえあれば、従属トランスペアレント インターフェースの数に制限はありません。
最大ペア数	最大数ブリッジ ペア数は、利用可能な物理インターフェース数に依存します。これは、"複数の 1 対 1 ペアリング" と考えることができます。	トランスペアレント モードでは、複数のインターフェースが同時にプライマリ WANに対するトランスペアレント パートナーとして動作することはできますが、これは単にプライマリWANのサブネットを他のインターフェースにスパニングしているに過ぎません。これは、"単一の 1 対 1 ペアリング" または "単一の 1 対多ペアリング" と考えることができます。

L2 ブリッジ モードとトランスペアレント モードの比較

項目	レイヤ 2 ブリッジ モード	トランスペアレント モード
ゾーンの制限	プライマリ ブリッジ インターフェースは、非保護、保護、パブリックのいずれかになります。セカンダリ ブリッジ インターフェースは、保護またはパブリックのいずれかになります。	トランスペアレント モード ペアのインターフェースは、1 つの非保護インターフェース (ペアのサブネットのマスターとしてのプライマリ WAN) と、1 つ以上の保護/パブリック インターフェース (LAN または DMZ など) で構成されている必要があります。
サポートされるサブネット数	任意の数のサブネットがサポートされます。サブネットへのトラフィックまたはサブネットからのトラフィックは、アクセス ルールを作成することによって制御できます。	既定の設定では、トランスペアレント モードでサポートされるサブネット数は 1 つだけです (つまり、プライマリ WANに割り当てられ、プライマリ WAN からスパニングされるサブネット)。ARP エントリおよびルートを使用して、サブネットを手動で追加することはできます。
非 IPv4 トラフィック	既定では、セカンダリ ブリッジ インターフェースの設定ページで無効にされていない限り、すべての非 IPv4 トラフィックが、ブリッジ ペア インターフェースからそのブリッジ パートナー インターフェースへとブリッジされます。これには、IPv6 トラフィック、STP (Spanning Tree Protocol)、および識別不能の IP タイプも含まれます。	トランスペアレント モードでは非 IPv4 トラフィックは処理されません。 破棄されてログに記録されます。
VLAN トラフィック	VLAN トラフィックは L2 ブリッジを介して渡され、ステートフル精密パケット検査エンジンによって完全に検査されます。	VLAN サブインターフェースを作成し、トランスペアレント モード アドレス オブジェクトを割り当てることはできますが、VLAN はそのまま通過するのではなく、セキュリティ装置で終端されます。
VLAN サブインターフェース	ブリッジ ペア インターフェース上で VLAN サブインターフェースを作成することはできます。ただし、VLAN フレーム内の送信先 IP アドレスが、セキュリティ装置上の VLAN サブインターフェースの IP アドレスと一致しない限り、VLAN サブインターフェースは、ブリッジを介してブリッジ パートナーへと渡されます。両者のアドレスが一致した場合は (例えば、管理トラフィックとして) 処理されます。	トランスペアレント モードで動作する物理インターフェースに VLAN サブインターフェースを割り当てることはできますが、動作モードはその親に依存しません。これらの VLAN サブインターフェースに、トランスペアレント モード アドレス オブジェクトを割り当てることもできますが、VLAN サブインターフェースはそのまま通過するのではなく終端されます。
動的アドレッシング	プライマリ ブリッジ インターフェースを WANゾーンに割り当てることはできますが、プライマリ ブリッジ インターフェースに対しては静的アドレッシングしか行えません。	トランスペアレント モードでは、プライマリWANがマスター インターフェースとして使用されますが、トランスペアレント モードでは静的アドレッシングしか許可されません。

L2 ブリッジ モードとトランスペアレント モードの比較

項目	レイヤ 2 ブリッジ モード	トランスペアレント モード
VPN サポート	ルート設定を 1 つ追加することで VPN 動作がサポートされます。詳細については、「レイヤ 2 ブリッジ モードでの VPN 統合 (367 ページ)」を参照してください。	VPN 動作がサポートされます。 特別な設定要件はありません。
DHCP サポート	DHCP はブリッジ ペアを通過できます。	トランスペアレント モードで動作するインターフェースは、DHCP サービスを提供するか、IP ヘルパーを使って DHCP を通過させることができます。
ルーティングと NAT	L2 ブリッジ ペアと他のパス間のトラフィックはインテリジェントにルーティングされます。既定では、ブリッジ ペア インターフェースからブリッジ パートナーへのトラフィックは NAT 変換されませんが、他のパスへのトラフィックを必要に応じて NAT 変換することもできます。必要に応じて独自のルートおよび NAT ポリシーを追加できます。	他のパスとの間のトラフィックはインテリジェントにルーティングされます。既定では、WAN とトランスペアレント モード インターフェース間のトラフィックは NAT 変換されませんが、他のパスへのトラフィックを必要に応じて NAT 変換することもできます。必要に応じて独自のルートおよび NAT ポリシーを追加できます。
ステートフル パケット検査	ファイアウォールの VLAN トラフィックなど、L2 ブリッジを通過するすべてのサブネットのすべての IPv4 トラフィックには、完全なステートフル パケット検査が適用されます。	トランスペアレント モード アドレス オブジェクトの割り当てによって定義されたサブネットへのトラフィックおよびサブネットからのトラフィックには、完全なステートフル パケット検査が適用されます。
セキュリティ サービス	すべてのセキュリティ サービス (GAV、IPS、アンチスパイ、CFS) が完全にサポートされます。これには、標準的な IP トラフィックと 802.1Q カプセル化 VLAN トラフィックがすべて含まれます。	トランスペアレント モード アドレス オブジェクトの割り当てによって定義されたサブネットとの間で、すべてのセキュリティ サービス (GAV、IPS、アンチスパイ、CFS) が完全にサポートされます。
ブロードキャスト トラフィック	ブロードキャスト トラフィックは、受信したブリッジ ペア インターフェースからブリッジ パートナー インターフェースへと渡されます。	ブロードキャスト トラフィックは破棄されてログに記録されます。 ただし、NetBIOS については、IP ヘルパーによって処理される場合があります。
マルチキャスト トラフィック	**「管理 | セキュリティ設定 | ファイアウォール設定 > マルチキャスト」**でマルチキャストが有効にされている場合、マルチキャスト トラフィックは検査され、L2 ブリッジ ペアを介して渡されます。IGMP メッセージングには依存せず、個々のインターフェースでマルチキャスト サポートを有効にする必要はありません。	**「管理 | セキュリティ設定 | ファイアウォール設定 > マルチキャスト」**ページでマルチキャストが有効にされており、かつ、関連するインターフェースでマルチキャスト サポートが有効になっている場合、マルチキャスト トラフィック (IGMP に依存) は検査され、トランスペアレント モードで渡されます。

L2 ブリッジ モードにはないトランスペアレント モードのメリット

L2 ブリッジ ペアでは最大 2 つのインターフェースしか許容されなません。3 つ以上のインターフェースを同じサブネット上で運用する必要がある場合は、トランスペアレント モードを検討することをお勧めします。

L2 ブリッジ パスの決定

セキュリティ装置がブリッジ ペア インターフェースで受信したパケットは、適切かつ最適なパスに沿って送信先へと転送されなければなりません。そのパスはブリッジ パートナーである場合もあれば、その他の物理インターフェース (またはサブインターフェース) である場合もあります。あるいは VPN トンネルである場合も考えられます。同様に、ブリッジ ペア上の特定のホスト宛てに、他のパス (物理、仮想、または VPN) から到達したパケットは、適切なブリッジ ペア インターフェースを介して送出される必要があります。

以下は、こうした状況下で、パス決定に適用されるロジックを順に説明したものです。

1 送信先に対して、*既定以外*の最も限定的なルートが存在する場合は、そのルートが選択されます。例えば、次のようなケースが該当します。

   a ホスト 15.1.1.100 サブネット宛てのパケットが X3 (非 L2 ブリッジ LAN) に到達した。ここで、15.1.1.0/24 サブネットへのルートが、X0 (セカンダリ ブリッジ インターフェース、LAN) インターフェースを介し、192.168.0.254 を経由したパスに存在する。この場合、パケットは、X0 を介して、送信先IP アドレス 15.1.1.100 を持つ、192.168.0.254 の送信先 MAC アドレスに転送されます。

   b ホスト 10.0.1.100 宛てのパケットが X4 (プライマリ ブリッジ インターフェース、LAN) に到達した。ここで、10.0.1.0/24 へのルートが、X5 (DMZ)インターフェースを介し、192.168.10.50 を経由したパスに存在する。この場合、パケットは、X5 を介して、送信先IP アドレス 10.0.1.100 を持つ、192.168.10.50 の送信先 MAC アドレスに転送されます。

2 送信先への特定のルートが存在しない場合は、送信先 IP アドレスを調べるために、ARP キャッシュ調査が実行されます。キャッシュ エントリと比較した結果、一致が見つかった場合、適切な送信先インターフェースが判明します。例えば、次のようなケースが該当します。

   a ホスト 192.168.0.100 (L2プライマリ ブリッジ インターフェース X2 上に存在) 宛てのパケットが X3 (非 L2 ブリッジ LAN) に到着した。この場合、パケットは X2 を介し、ARP キャッシュから取得された既知の送信先 MAC および IP アドレス (192.168.0.100) に転送されます。

   b X5 (DMZ) 上のホスト 10.0.1.10 宛てのパケットが、X4 (プライマリ ブリッジ インターフェース、LAN) に到着した。この場合、パケットは X5 を介し、ARP キャッシュから取得された既知の送信先 MAC および IP アドレス (10.0.1.10) に転送されます。

3 ARP エントリが見つからない場合は、次の処理が行われます。

   a パケットがブリッジ ペア インターフェースに到着した場合、そのパケットはブリッジ パートナー インターフェースに送信されます。

   b パケットが他のパスから到着する場合、セキュリティ装置が、ブリッジ ペアの両方のインターフェースに ARP 要求を送出して、送信先 IP が存在するセグメントを特定します。

   最後のケースでは、ARP 応答を受信するまでは送信先が不明であるため、それまでは送信先ゾーンも判明しません。したがって、パスが決定するまで、セキュリティ装置は適切なアクセス ルールを適用できません。パスが決定された時点で、後続の関連するトラフィックに対して適切なアクセス ルールが適用されます。

L2 ブリッジ ペア インターフェースに到着したトラフィックのアドレス変換 (NAT) については、確定している送出先に応じて次のように処理されます。

1 ブリッジ パートナー インターフェースの場合、IP 変換 (NAT) は実行されません。

2 異なるパスの場合は、そのパスに応じて適切な NAT ポリシーが適用されます。

   a パスが別の接続 (ローカル) インターフェースである場合、変換が実行される可能性は低くなります。つまり、事実上、*最終的な措置*として、「すべて->元の NAT ポリシー」に従ってルーティングされます。

   b パスが WAN を経由することが確定している場合、既定の「*自動的に追加された[インターフェース]発信 NAT ポリシー - X1 WAN*」が適用され、インターネットへの配信のためにパケットの送信元が変換されます。これは、「内部セキュリティ (355 ページ)」の図にあるような混在モード トポロジの場合によく見られます。

L2 ブリッジ インターフェース ゾーンの選択

ブリッジ ペア インターフェースのゾーンの割り当ては、実際のネットワークのトラフィック フロー要件に従って行う必要があります。トランスペアレント モードでは、送信元インターフェースをプライマリ WAN とし、トランスペアレント インターフェースを保護またはパブリックとすることで "高保護から低保護へと保護レベルが推移していくシステム" をある意味強制的に実現しています。これに対し、L2 ブリッジ モードでは保護の運用レベルをより細かく制御できます。例えば、L2 ブリッジ モードでは、*プライマリ ブリッジ インターフェース*と*セカンダリ ブリッジ インターフェース*を同じゾーンに割り当てることも、異なるゾーンに割り当てることもできます (LAN+LAN、LAN+DMZ、WAN+CustomLAN など)。こうした割り当ては、トラフィックに適用される既定のアクセス ルールだけでなく、ブリッジを通過するトラフィックに対する精密パケット検査セキュリティ サービスの適用方法にも影響します。ブリッジ ペアで使用するインターフェースを選択して構成する際、考慮すべき重要な要素として、セキュリティ サービス、アクセス ルール、および WAN 接続があります。

セキュリティ サービスの方向性

L2 ブリッジ モードを中心とした配備では、ブリッジ ペア インターフェースに対するゾーンを適切に選択するために、セキュリティ サービスの適用性を理解することが大切です。セキュリティ サービスの適用性は、次のような基準に基づいて決定されます。

1 **サービスの方向**:

- GAV は、主にインバウンド サービスです。 HTTP、FTP、IMAP、SMTP、POP3、TCPのインバウンド ストリームが検査されます。SMTP についてはアウトバウンド要素もあります。
- アンチ スパイウェアは、主にインバウンドです。インバウンドの HTTP、FTP、IMAP、SMTP、POP3 が検査され、通常はクラス ID によって識別されたスパイウェア コンポーネントの配信 (取得など) の有無がチェックされます。これとは別にアウトバウンド コンポーネントも存在します。 スパイウェア コンポーネントの認識をトリガーする IPSシグネチャに固有の方向性 (すなわち“送信") と対比して、ここでは“アウトバウンド"という用語を用いています。通常、これらのコンポーネントは、インターネット上のウェブ サーバ (WAN ホスト) から、クライアント (LAN ホストなど) によって HTTP 経由で取得されるため、送信の分類基準 (「IPS: トラフィックの方向」を参照) が使用されます。「IPS: トラフィックの方向」でいうと、これは*送信*接続に該当し、送信方向に分類されるシグネチャが必要となります。
- IPS には、着信、送信、両方向の 3 つの方向があります。受信と送信は「IPS: トラフィックの方向」に記載したとおりです。両方向とは、表において交差するすべてのポイントを指します。

- 精度を高めるため、接続状態 (SYN または確立済みなど) やフローにおけるパケットの送信元 (始動者または応答者など)、他の要素も考慮されます。

2 **トラフィックの方向**: IPS に関連したトラフィックの方向は、主にトラフィック フローの送信元および送信先ゾーンによって決まります。通常、セキュリティ装置がパケットを受信すると、そのパケットの送信元ゾーンが即座に判明し、その送信先ゾーンも、ルート (または VPN) 調査を実行することによってすぐに判別されます。

パケットの方向性は、その送信元と送信先に基づき、*受信*と*送信* (インバウンド/アウトバウンドと混同しないようにしてください) のいずれかに分類されます。この決定には、「IPS: トラフィックの方向」テーブルに示す基準が使用されます。

IPS: トラフィックの方向 [a]

送信先/送信元	非保護	公開	無線	暗号化	信頼済み	マルチキャスト
非保護	受信	受信	受信	受信	受信	受信
公開	送信	送信	送信	受信	受信	受信
無線	送信	送信	信頼	信頼	信頼	受信
暗号化	送信	送信	信頼	信頼	信頼	送信
信頼済み	送信	送信	信頼	信頼	信頼	送信

a. 表のデータは変更される場合があります。

この分類に加えて、あるゾーンから別のゾーンへと、より高い信頼性を持って転送されるパケットは、本質的に高レベルのセキュリティ (LAN | 無線 | 暗号化 <--> LAN | 無線 | 暗号化) が確保されていることを表す、特別な*信頼*という種別に分類されます。信頼として分類されたトラフィックには、すべてのシグネチャが適用されます (着信、送信、および両方向)。

3 **シグネチャの方向**: これは、主に IPS に関連したものです。各シグネチャには、SonicWall のシグネチャ開発チームにより方向が割り当てられます。これは、擬陽性を最小限に抑えるための最適化措置として行われます。シグネチャには、次の方向があります。

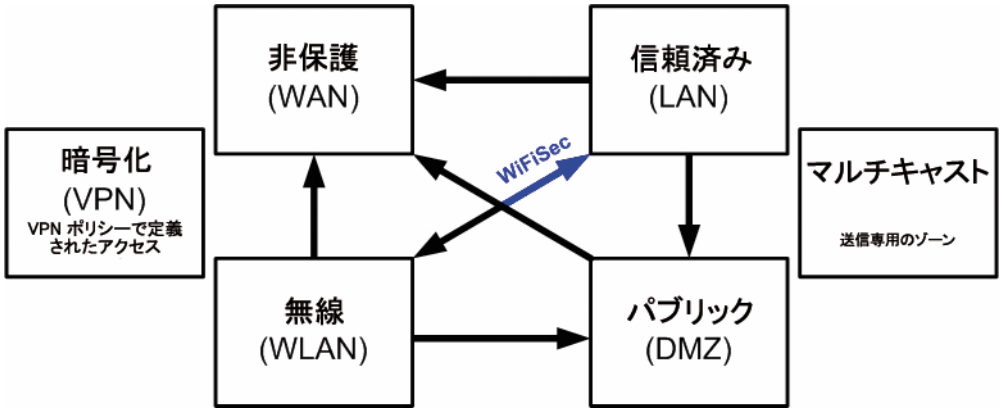
- **着信** - *着信*および*信頼*に適用されます。シグネチャの大半は着信です。 これには、アプリケーションの脆弱性を狙ったあらゆる形態の攻撃のほか、列挙やフットプリンティングといった、あらゆる試みが含まれます。シグネチャの約 85%は着信です。
- **送信** - *送信*および*信頼*に適用されます。送信に分類されるシグネチャの例としては、IM や P2P のログイン試行のほか、悪性の応答 (例: 攻撃の応答) などがあります。シグネチャの約 10%は送信です。
- **両方向** - すべてに適用されます。例えば、両方向のシグネチャには、IM ファイル転送、各種 NetBIOS 攻撃 (例: Sasser の通信)、各種 DoS 攻撃 (例: ポート 0 宛ての UDP/TCP トラフィック) があります。シグネチャの約 5%は両方向です。

4 **ゾーンの適用**: シグネチャがトリガーされるためには、*必要なセキュリティ サービスが、経路上のゾーンの少なくとも 1 つで有効になっている必要があります*。例えば、インターネット (X1、WAN) 上のホストが Microsoft ターミナル サーバ (X3、セカンダリ ブリッジ インターフェース、LAN) にアクセスしている場合、IPS が WAN、LAN、またはその両方で有効になっていれば、*着信*のシグネチャである "IPS 検出警告: MISC MS ターミナル サーバ要求、SID: 436、優先順位: 低" がトリガーされます。

既定のアクセス ルール

既定では、ゾーン対ゾーンのアクセス ルールが使用されます。必要に応じて変更することもできますが、既定のアクセス ルールをお勧めします。既定の設定を「既定のアクセス ルール」に示します。

既定のアクセス ルール



WAN 接続

ライセンス、セキュリティ サービスに使用するシグネチャのダウンロード、NTP (時刻の同期)、CFS (コンテンツ フィルタ サービス) などのスタック通信には、インターネット (WAN) 接続が必要です。現時点では、これらの通信は、プライマリ WANインターフェース経由でしか行うことができません。これらのタイプの通信が必要な場合、プライマリ WANにインターネットへのパスが必要です。プライマリ WAN がブリッジ ペアに属しているかどうかは、これらのスタック通信を提供する機能に影響しません。

メモ：インターネット接続が利用できない場合、ライセンシングやシグネチャの更新を手動で実行することもできます。詳細については、http://www.MySonicWall.com/ を参照してください。

サンプル トポロジ

次の図は、一般的な配備を表すサンプル トポロジです。

- **インライン レイヤ 2 ブリッジ モード**では、SonicWall セキュリティ装置が追加されて、既にセキュリティ装置が備わっているネットワークでセキュリティ サービスを提供します。
- **境界セキュリティ**では、SonicWall セキュリティ装置が*ピュア L2 ブリッジ モード*で既存のネットワークに追加されており、セキュリティ装置はネットワークの境界付近に配置されています。
- **内部セキュリティ**では、SonicWall セキュリティ装置が*混在モード*で完全統合されており、L2 ブリッジ、WLAN サービス、および NAT 変換による WAN アクセスを同時に提供します。
- **高可用性を備えたレイヤ 2 ブリッジ モード**は、セキュリティ装置の HA ペアが L2 ブリッジと共に高可用性を提供する混在モード シナリオを表しています。
- **SSL VPN を備えたレイヤ 2 ブリッジ モード**は、SonicWall SMA SSL VPN または SonicWall SSL VPN シリーズ装置が L2 ブリッジ モードと組み合わせて配備されているシナリオを表しています。

トピック:

- 無線レイヤ 2 ブリッジ (354 ページ)
- インライン レイヤ 2 ブリッジ モード (354 ページ)
- 境界セキュリティ (355 ページ)
- 内部セキュリティ (355 ページ)
- 高可用性を備えたレイヤ 2 ブリッジ モード (356 ページ)
- SSL VPN を備えたレイヤ 2 ブリッジ モード (358 ページ)

無線レイヤ 2 ブリッジ

メモ：無線レイヤ 2 ブリッジは、SuperMassive 9800 には適用されません。

無線モードでは、無線 (WLAN) インターフェースの LAN または DMZ ゾーンへのブリッジ後、WLAN ゾーンがセカンダリ ブリッジ インターフェースになり、無線クライアントが同等の有線クライアントと同じサブネットおよび DHCP プールを共有できるようになります。

WLAN から LAN へのレイヤ2 インターフェース ブリッジを設定するには、次の手順に従います。

1 「**管理 | システム セットアップ | ネットワーク > インターフェース**」に移動します。

2 ブリッジの対象とする無線インターフェースの**設定**アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。

ヒント：設定済みの仮想アクセス ポイントがある場合、既に WLAN ゾーン内の X4 などのインターフェースに VLAN インターフェースがあり、仮想アクセス ポイントはその VLAN ID を使用するように設定されています。

3 「**レイヤ 2 ブリッジ モード**」で、「**モード/IP 割り当て**」を選択します。

メモ：WLAN ゾーンと選択したブリッジ インターフェースとの間のトラフィックを許可する一般的なルールが自動的に作成されますが、WLAN ゾーン タイプのセキュリティ ポリシーが依然として適用されます。限定的なルールがあれば手動で追加する必要があります。

4 WLAN のブリッジ先となるインターフェースを「**ブリッジ先**」から選択します。この例では、X0 (既定の LAN ゾーン) を選択します。

5 残りのオプションは通常どおりに設定します。WLAN インターフェースの設定方法については、「無線インターフェースの設定 (307 ページ)」を参照してください。

インライン レイヤ 2 ブリッジ モード

この方式は、既にセキュリティ装置が備わっているネットワークで、ネットワークに大きな変更を加えずにセキュリティ装置のセキュリティ サービスを利用したいという場合に便利です。セキュリティ装置をレイヤ 2 ブリッジ モードで使用することにより、X0 および X1 インターフェースが同じブロードキャスト ドメイン/ネットワーク (X1 WAN インターフェース) の一部になります。

この例は、Hewlett Packard ProCurve スイッチング環境にインストールされた SonicWall セキュリティ装置を表しています。SonicWall は HP の ProCurve Alliance のメンバーです。
http://www.procurve.com/alliance/members/SonicWall.htm。

HP の ProCurve Manager Plus (PCM+) および HP Network Immunity Manager (NIM) サーバ ソフトウェア パッケージを使用すると、SonicWall セキュリティ装置の諸機能やスイッチを管理できます。

インライン レイヤ2 ブリッジ モードを設定するには、以下の手順に従います。

1 「**管理 | システム セットアップ | ネットワーク > インターフェース**」に移動します。

2 **X0 (LAN)** インターフェースの**設定**アイコンを選択します。

3 「**インターフェースの編集**」ダイアログで、「IP 割り当て」を「**レイヤ 2 ブリッジ モード (IP ルート オプション)**」に設定します。オプションが次のように変化します。

4 「**ブリッジ先:**」インターフェースを「**X1**」に設定します。

5 ブリッジ ペアですべての非 IP トラフィックを遮断するには、「**すべての非 IP トラフィックを遮断する**」を選択します。このオプションは、既定では選択されていません。

6 トラフィックがブリッジ ペアでルーティングされないようにするには、「**このブリッジ ペアにトラフィックをルーティングしない**」を選択します。このオプションは、既定では選択されていません。

7 ブリッジ ペアでトラフィックのスニッフのみを行う場合は、「**このブリッジ ペアのトラフィックのみスニフする**」を選択します。このオプションは、既定では選択されていません。

8 ブリッジ ペアでステートフル検査が行われないようにするには、「**このブリッジ ペアでステートフル インスペクションを無効にする**」を選択します。このオプションは、既定では選択されていません。

9 インターフェースが **HTTPS** および **SNMP** 用に設定されていて、**PCM+/NIM** で DMZ から管理できるようになっていることを確認します。

10 残りのオプションは通常どおりに設定します。

11 「**OK**」を選択すると、変更内容が保存されて有効になります。

LAN から WAN へのトラフィックおよび WAN から LAN へのトラフィックが許可されるようにアクセス ルールを変更することも必要です。そうしないと、トラフィックがうまく通りません。DMZ 上に PCM+/NIM サーバがある場合は、ファイアウォール上でルーティング情報に変更を加える必要もあるかもしれません。

境界セキュリティ

境界セキュリティは、セキュリティ サービス提供のために、セキュリティ装置を境界部分に追加したネットワーク シナリオです (セキュリティ装置とルータ間には既存のセキュリティ装置があってもなくてもかまいません)。通常、このシナリオでは、セキュリティ装置の下にあるものすべて (*プライマリ ブリッジ インターフェース* セグメント) は、セキュリティ装置の左側にあるものすべて (*セカンダリ ブリッジ インターフェース* セグメント) と比べて信頼レベルが低いと考えることができます。そのため、X1 (プライマリ WAN) を *プライマリ ブリッジ インターフェース* として使用するのが適切です。

セカンダリ ブリッジ インターフェース (LAN) に接続されたホストからのアウトバウンド トラフィックは、ファイアウォールを介して (L3 スイッチ上の VLAN インターフェースとルータを順に通過して) ゲートウェイへと出ていくことが許可されます。一方、*プライマリ ブリッジ インターフェース* (WAN) からのインバウンド トラフィックは既定では通過できません。

セカンダリ ブリッジ インターフェース (LAN) セグメントにメール サーバやウェブ サーバなどのパブリック サーバが存在する場合、特定の IP アドレスやサービスについて WAN から LAN へのトラフィックを許可するアクセス ルールを追加すれば、これらのサーバへの受信トラフィックを許可することができます。

内部セキュリティ

セキュリティ装置が境界セキュリティ機器およびセキュア ワイヤレス プラットフォームとして動作するネットワーク シナリオです。同時に、*ワークステーションまたはサーバのアドレスを再割り当てすることなく*、ワークステーション セグメントとサーバ セグメント間の L2 ブリッジ セキュリティが実現されています。

セキュリティ装置は、ブリッジおよびルーティング/NAT を同時に行うことができますが、この配備例は、それを象徴する典型的な部門間混在モード トポロジと言えます。*プライマリ ブリッジ インターフェース* (サーバ) セグメントと *セカンダリ ブリッジ インターフェース* (ワークステーション) セグメントとの間を行き来するトラフィックは、L2 ブリッジを通過します。

ブリッジ ペアの両方のインターフェースが保護 (LAN) ゾーンに割り当てられているため、次の原則が成り立ちます。

- 既定ではすべてのトラフィックが許可されます。ただし、必要に応じてアクセス ルールを作成することも可能です。

  試しに、X2 (プライマリ ブリッジ インターフェース) を公開 (DMZ) ゾーンに割り当てたらどうなるかを考えてみます。この場合、すべてのワークステーションはサーバに到達することができますが、サーバからワークステーションへの通信を開始することはできません。これでトラフィック フローの要件が満たされる (ワークステーションからサーバへのセッションを開始するなど) 場合もありますが、望ましくない影響が 2 点ほど生じます。

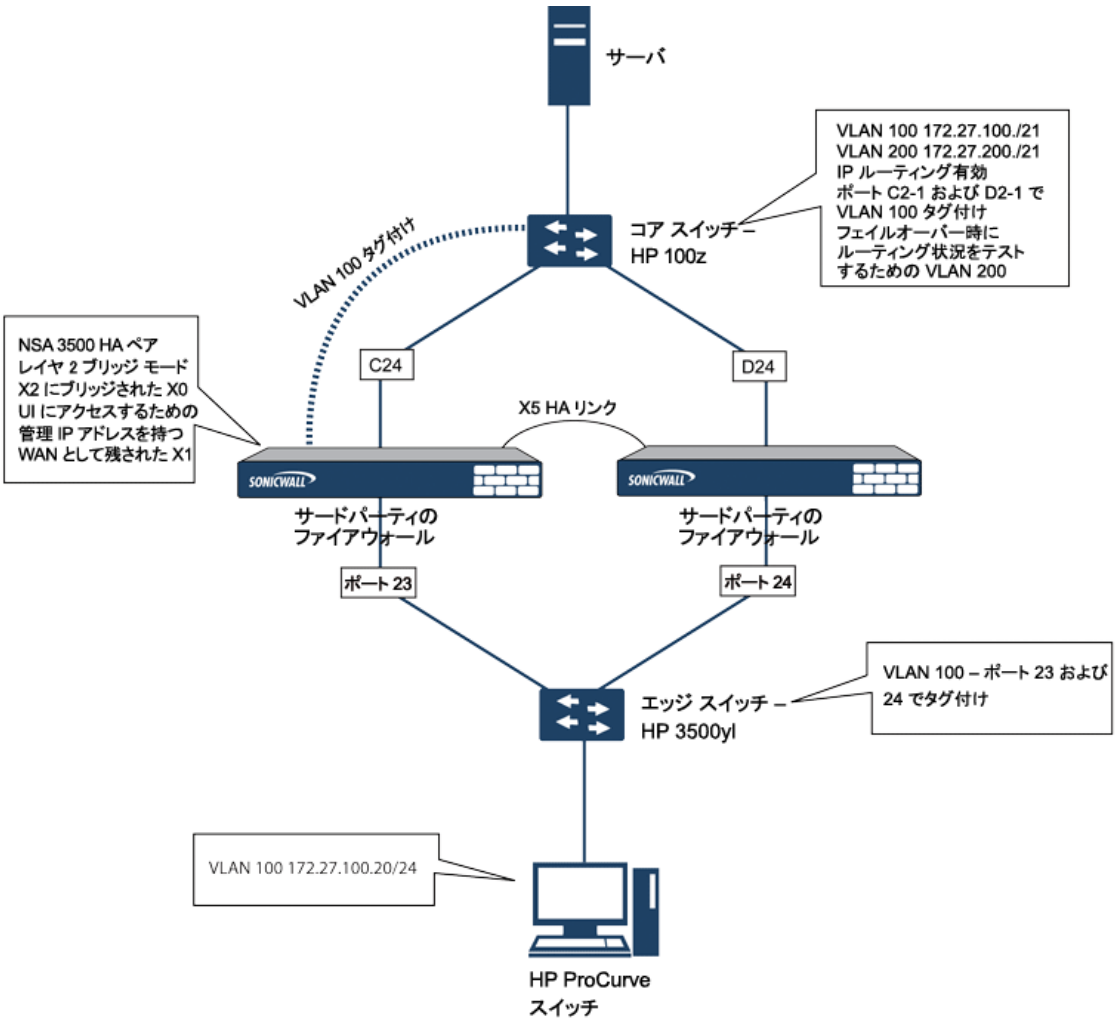
- DHCP サーバが DMZ に入ります。このため、ワークステーションからの DHCP 要求は L2 ブリッジを介して DHCP サーバ (192.168.0.100) に到達できますが、既定では DMZ から LAN へのアクセスがアクセス ルールによって拒否されるため、サーバからの DHCP OFFER は破棄されてしまいます。アクセス ルールを追加するか、既定のアクセス ルールを変更して、DMZ から LAN へのこのトラフィックを許可する必要があります。
- ワークステーションからサーバへのトラフィックは、送信元が保護ゾーンで送信先が公開ゾーンであるため、セキュリティ サービスの方向性は*送信*として分類されます。*着信*または (理想的には) *信頼*の分類に比べると、調査の水準が低くなるという点で、これは次善の選択肢と言えます。
- セキュリティ サービスの方向性は*信頼*として分類されます。また、すべてのシグネチャ (*受信*、*送信*、および*両方向*) が適用され、どちらのセグメントにも最高水準のセキュリティが提供されます。

レイヤ 2 ブリッジ モードでインターフェースを設定する詳細な手順については、「レイヤ 2 ブリッジ モードの設定 (360 ページ)」を参照してください。

高可用性を備えたレイヤ 2 ブリッジ モード

この方式は、高可用性 (HA) とレイヤ 2 ブリッジ モードの両方が望まれるネットワークに適しています。この例は、SonicWall セキュリティ装置の場合であり、VLAN を設定したスイッチの使用を想定しています。「内部セキュリティの例: 高可用性とレイヤ 2 ブリッジ モードの両方が適切な場合」を参照してください。

内部セキュリティの例: 高可用性とレイヤ 2 ブリッジ モードの両方が適切な場合



セキュリティ装置 HA ペアは、ポート X5 (指定の HA ポート) で互いに接続された 2 つのセキュリティ装置から成っています。各装置のポート X1 は、通常の WAN 接続用に設定されており、その機器の管理インターフェースへのアクセスに使用されます。レイヤ 2 ブリッジ モードは、ポート X0 からポート X2 へのブリッジによって実装されています。

このシナリオを設定する際には、セキュリティ装置とスイッチの両方について注意すべき事柄がいくつかあります。

セキュリティ装置に関して留意すべき点:

- 高可用性を設定するときに仮想 MAC オプションを有効にしないでください。レイヤ 2 ブリッジ モード設定では、この機能は有用ではありません。
- このようなインライン環境で先制モードを有効にするのはお勧めできません。先制モードが必要な場合は、スイッチのドキュメントに書かれている推奨事項に従ってください。ここではトリガーとフェイルオーバーの時間値が重要な役割を果たすからです。
- 管理ネットワーク用のインターフェース (この例では X1 を使用) を確保することを検討してください。プローブやその他の理由でブリッジ インターフェースに IP アドレスを割り当てる必要がある場合、SonicWall ではセキュリティと管理のためにスイッチに割り当てた管理 VLAN ネットワークの使用を推奨しています。

  メモ: HA 用に割り当てた IP アドレスが実際のトラフィック フローと直接に相互作用することはありません。

スイッチに関するもの:

- 複数のタグ ポートの使用。「内部セキュリティの例: 高可用性とレイヤ 2 ブリッジ モードの両方が適切な場合」に示してあるように、エッジ スイッチ (ポート 23 および 24) とコア スイッチ (C24 - D24) の両方で VLAN 100 用に 2 つのタグ (802.1q) ポートが作成されています。この 2 つのスイッチの間でセキュリティ装置がインラインで接続されています。高パフォーマンス環境では、リンク集約/ポート トランク、Dynamic LACP、またはこのような配備 (OSPF を使用) のために指定された完全に独立したリンクの使用が通常は推奨され、スイッチごとのフォールト トレランスを考慮する必要があります。詳細については、スイッチのドキュメントを参照してください。
- HP ProCurve スイッチでは、2 つのポートが同じ VLAN でタグ付けされた場合、そのポート グループは自動的にフェイルオーバー設定になります。その場合、一方のポートに障害が起きると、もう一方のポートがすぐに有効になります。

SSL VPN を備えたレイヤ 2 ブリッジ モード

このサンプル トポロジは、既存の SonicWall EX シリーズ SSL VPN または SonicWall SSL VPN ネットワーク環境への SonicWall セキュリティ装置の適切なインストールに適用されます。セキュリティ装置をレイヤ 2 ブリッジ モードにすることにより、SSL VPN 装置への内部のプライベートな接続でウイルス、スパイウェア、および侵入を両方向でスキャンできます。このシナリオでは、セキュリティ装置がセキュリティを適用するためではなく、両方向のスキャン、ウイルスとスパムの遮断、および侵入の阻止に使用します。正しくプログラムすれば、トラフィックの動作や内容が有害であると判断されない限り、セキュリティ装置がネットワーク トラフィックを妨げることはありません。このセクションでは、SonicWall セキュリティ装置の 1 ポート配備と 2 ポート配備の両方を取り扱います。

WAN から LAN へのアクセス ルール

この配備シナリオでは、セキュリティ装置をアンチウイルス、アンチスパイウェア、および侵入防御の実施ポイントとしてのみ使用するので、既存のセキュリティ ポリシーを修正して、WAN と LAN の間で両方向でトラフィックが行き来できるようにする必要があります。WAN と LAN の間でトラフィックがどちらの方向にも行き来できるようにする手順については、『*SonicOS ポリシー*』を参照してください。

ネットワーク インターフェースの設定と L2B モードの有効化

このシナリオでは、WAN インターフェースを次の目的に使用します。

- 管理者用の管理インターフェースへのアクセス
- MySonicWall での購読サービスの更新
- 機器の既定のルートと SSL VPN 装置の内部トラフィックの「次のホップ」(そのため、WAN インターフェースは SSL VPN 装置の内部インターフェースと同じ IP セグメントにある必要があります)

セキュリティ装置の LAN インターフェースは、SSL VPN 装置の外部インターフェースから届く暗号化されていないクライアント トラフィックの監視に使用されます。このことは、(この LAN インターフェースを既定のルートと見なすために SSL VPN 装置の外部インターフェースを再構成する代わりに) レイヤ 2 ブリッジ モードで実行する理由になっています。

インターフェースで L2B モードを有効にするには:

1 「**管理 | システム セットアップ > ネットワーク > インターフェース**」に移動します。

2 **WAN** インターフェースの**設定**アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。

3 セキュリティ装置がシグネチャの更新を取得して NTP と通信できるように、インターネットにアクセスできるアドレスをインターフェースに割り当てます。ゲートウェイと内部/外部 DNS アドレスの設定は SSL VPN 装置の設定と一致している必要があります。

- **IP アドレス**: これは SSL VPN 装置の内部インターフェースのアドレスと一致しなければなりません。
- **サブネット マスク**、**デフォルト ゲートウェイ**、**DNS サーバ**: これらのアドレスを SSL VPN 装置の設定と一致させます。

4 「**管理**」設定で、「**HTTPS**」および「**Ping**」を選択します。

5 「**OK**」を選択すると、変更内容が保存されて有効になります。

LAN インターフェースを設定するには、以下の手順に従います。

1 「**管理 | システム セットアップ | ネットワーク > インターフェース**」に移動します。

2 **LAN** インターフェースの**設定**アイコンを選択します。

3 「ネットワーク モード」設定として、「**レイヤ 2 ブリッジ モード**」を選択します。

4 「**ブリッジ先**」設定として、「**X1**」を選択します。

5 セキュリティ装置でサポートされている、VLAN タグ付きのトラフィックを通過させる必要もある場合は、「**VLAN フィルタリング**」を選択します。

6 通過させる必要のある VLAN をすべて追加します。

7 「**OK**」を選択すると、変更内容が保存されて有効になります。

セキュリティ装置の管理インターフェースから自動的に切断されることもあります。ここでセキュリティ装置の X0 インターフェースから管理用のラップトップまたはデスクトップを切断し、ネットワークに物理的に接続する前にセキュリティ装置の電源を切ることができます。

ネットワークと SSL VPN 装置の間へのセキュリティ装置のインストール

配備方式 (シングルホームまたはデュアルホーム) に関係なく、セキュリティ装置を SSL VPN 装置の X0/LAN インターフェースと内部ネットワークへの接続との間に配置する必要があります。そうすることで、機器が SonicWall のライセンスおよびシグネチャの更新サーバに接続したり、内部ネットワーク リソースへのアクセスを要求する外部クライアントからの復号化されたトラフィックをスキャンしたりすることが可能になります。

SSL VPN 装置がサードパーティのファイアウォールの背後にあって 2 ポート モードの場合、それはデュアルホームです。

デュアルホーム SSL VPN 装置を接続するには、次の手順に従います。

1 セキュリティ装置の X0/LAN ポートを SSL VPN 装置の X0/LAN ポートにケーブルで接続します。

2 セキュリティ装置の X1/WAN ポートを、SSL VPN を前に接続したポートにケーブルで接続します。

3 セキュリティ装置の電源を入れます。

SSL VPN 装置がサードパーティのファイアウォールの DMZ 内にあって 1 ポート モードの場合、それはシングルホームです。

シングルホーム SSL VPN 装置を接続するには、次の手順に従います。

1 セキュリティ装置の X0/LAN ポートを SSL VPN 装置の X0/LAN ポートにケーブルで接続します。

2 セキュリティ装置の X1/WAN ポートを、SSL VPN を前に接続したポートにケーブルで接続します。

3 セキュリティ装置の電源を入れます。

設定の構成または確認

この段階で、ネットワーク内の管理ステーションから セキュリティ装置の管理インターフェースに WAN IP アドレスを使ってアクセスできるようになっているはずです。

設定を構成または確認するには、以下の手順に従います。

1 SonicWall セキュリティ装置のすべてのセキュリティ サービスが有効になっていることを確認します。「サービスのライセンス取得 (361 ページ)」および「ゾーンごとのセキュリティ サービスの有効化 (362 ページ)」を参照してください。

2 機器を SonicWall SMA SSL VPN 装置と共に配備する前に、SonicWall コンテンツ フィルタ サービスを無効にする必要があります。

   a 「**管理 | システム セットアップ | ネットワーク > ゾーン**」ページに移動します。

   b 「**LAN (X0)**」ゾーンの横にある「**設定**」を選択します。

   c 「**コンテンツ フィルタ サービスを強制する**」をクリアします。

   d 「**OK**」を選択します。

3 SonicWall セキュリティ装置での管理者パスワードをまだ変更していなければ、「**管理 | システム セットアップ | 装置 > 基本設定**」で変更することができます。

4 外部クライアントからのネットワークへのアクセスをテストするには、SSL VPN 装置に接続し、ログインします。

5 接続したら、内部ネットワーク リソースへのアクセスを試みます。何か問題があれば、設定を確認し、「レイヤ 2 ブリッジ モード配備における一般的な項目の設定 (361 ページ)」を参照してください。

レイヤ 2 ブリッジ モードの設定

トピック:

- レイヤ 2 ブリッジ モード用の設定タスク リスト (360 ページ)
- レイヤ 2 ブリッジ モード手順の設定 (363 ページ)
- レイヤ 2 ブリッジ モードでの VLAN 統合 (366 ページ)
- レイヤ 2 ブリッジ モードでの VPN 統合 (367 ページ)

レイヤ 2 ブリッジ モード用の設定タスク リスト

- ネットワークに合ったトポロジを選択します。
- レイヤ 2 ブリッジ モード配備における一般的な項目の設定 (361 ページ)
  - セキュリティ サービスをライセンスします。
  - DHCP サーバを無効化します。

    - SNMP および HTTP/HTTPS 管理を設定し有効化します。
    - Syslog を有効化します。
    - 対象ゾーンに関してセキュリティ サービスを有効化します。
    - アクセス ルールの作成
    - ログ設定
    - 無線ゾーンを設定します。
- プライマリ ブリッジ インターフェースの設定 (363 ページ)
    - プライマリ ブリッジ インターフェースのゾーンを選択します。
    - 管理を有効化します。
    - セキュリティ サービスを有効化します。
- セカンダリ ブリッジ インターフェースの設定 (364 ページ)
    - セカンダリ ブリッジ インターフェースのゾーンを選択します。
    - 管理を有効化します。
    - セキュリティ サービスを有効化します。
- 適切なゾーンにセキュリティ サービスを適用します。

レイヤ 2 ブリッジ モード配備における一般的な項目の設定

大部分のレイヤ 2 ブリッジ モード トポロジでは、SonicWall セキュリティ装置の使用に先だって次の設定を行う必要があります。

- サービスのライセンス取得 (361 ページ)
- DHCP サーバの無効化 (362 ページ)
- SNMP の設定 (362 ページ)
- インターフェースの SNMP および HTTPS の有効化 (362 ページ)
- Syslog の有効化 (362 ページ)
- ゾーンごとのセキュリティ サービスの有効化 (362 ページ)
- アクセス ルールの作成 (363 ページ)
- ログの設定 (363 ページ)
- 無線ゾーンの設定 (363 ページ)

サービスのライセンス取得

セキュリティ装置が正しく登録されている場合:

1 「**管理 | 更新 | ライセンス**」に移動します。

2 「**セキュリティ サービスのオンライン管理**」の下にある「**同期**」を選択します。

これにより、セキュリティ装置ライセンス サーバへの接続が行われ、セキュリティ装置が確実にライセンスを受けられるようになります。

ライセンス状況を確認するには、「**監視 | 現在の状況 | システム状況**」ページに移動し、すべてのセキュリティ サービス (ゲートウェイ アンチウイルス、アンチスパイウェア、侵入防御) のライセンス状況を表示します。

DHCP サーバの無効化

別の機器が DHCP サーバとして動作しているネットワーク設定で SonicWall セキュリティ装置をレイヤ 2 ブリッジ モードで使用するときは、まずセキュリティ装置の内部の DHCP エンジンを無効にする必要があります。既定では、このエンジンが設定されて動作しています。

DHCP サーバを無効にするには、以下の手順に従います。

1. 「**管理 | システム セットアップ | ネットワーク > DHCP サーバ**」に移動します。
2. 「**DHCP サーバを有効にする**」をクリアします。
3. 「**適用**」を選択します。

SNMP の設定

SNMP の設定を行うには、以下の手順に従います。

1. 「**管理 | システム セットアップ | 装置 | SNMP**」に移動します。
2. 「**SNMP を有効にする**」を選択します。
3. 「**適用**」を選択します。「**設定**」が使用可能になり、SNMP 情報が設定されます。
4. 「**設定**」を選択します。「**SNMP の設定**」ダイアログが表示されます。SNMP の設定方法については、「SNMP アクセスの設定 (54 ページ)」を参照してください。

インターフェースの SNMP および HTTPS の有効化

インターフェースで SNMP および HTTPS を有効化するには、以下の手順に従います。

1. 「**管理 | システム セットアップ | ネットワーク > インターフェース**」に移動します。
2. 装置の管理に使用するインターフェースの**編集**アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。
3. 「**管理**」オプションとして、**HTTPS** および **SNMP** を有効化します。
4. 「**OK**」を選択します。

Syslog の有効化

「**ログ > Syslog**」ページで Syslog を有効化します。Syslog を有効にする方法については、『*SonicOS ログとレポート*』を参照してください。

ゾーンごとのセキュリティ サービスの有効化

「**管理 | システム セットアップ | ネットワーク > ゾーン**」で、使用するゾーンごとにセキュリティ サービスが有効になっていることを確認します。

次に「**管理 | セキュリティ設定 | セキュリティ サービス**」ページで、サービスごとに、環境に最も適した設定項目を有効にして設定します。セキュリティ サービスの有効化と設定については、『*SonicOS セキュリティ設定*』を参照してください。

アクセス ルールの作成

異なるゾーンのセキュリティ装置を管理したり、あるいはサードパーティのサーバを管理、SNMP、Syslog サービスで使用したりする場合は、ゾーン間のトラフィックに関してアクセス ルールを作成します。「**管理 | ポリシー | ルール > アクセス ルール**」で、そのサーバのゾーンとユーザおよびサーバが含まれるゾーンとの共通部分のアイコンを選択します (環境によっては共通部分が複数存在することもあります)。新しいルールを作成して、サーバがそのゾーンのすべての機器と通信できるようにします。アクセス ルールについては、『*SonicOS ポリシー*』を参照してください。

ログの設定

「**管理 | ログと報告 | ログの設定 | 名前解決**」で、「**名前解決方法**」を「**DNS の後に NetBIOS**」に設定します。ログの設定については、『*SonicOS ログとレポート*』を参照してください。

無線ゾーンの設定

HP PCM+/NIM システムを使用して、WLAN/無線ゾーンに割り当てたインターフェース上の HP ProCurve スイッチを管理するのであれば、2 つの機能を無効にする必要があります。そうしないと、スイッチを管理できません。

無線ゾーンを設定するには、以下の手順に従います。

1. 「**管理 | システム セットアップ | ネットワーク > ゾーン**」に移動します。
2. 無線ゾーンを選択します。
3. 「**無線**」で、「**SonicPoint により生成された通信のみ許可する**」および「**WiFiSec を有効にする**」オプションをクリアします。
4. 「**OK**」を選択します。

レイヤ 2 ブリッジ モード手順の設定

ご使用のネットワークに最適なトポロジの選択については、「L2 ブリッジ インターフェース ゾーンの選択 (351 ページ)」を参照してください。この例では、「単純な L2 ブリッジ トポロジ」に最も近いトポロジを使用します。

プライマリ ブリッジ インターフェースとして使用するインターフェースを選択します。この選択の詳細については、「L2 ブリッジ インターフェース ゾーンの選択 (351 ページ)」を参照してください。この例では、(プライマリ WAN に自動的に割り当てられる) X1 を使用します。

トピック:

- プライマリ ブリッジ インターフェースの設定 (363 ページ)
- セカンダリ ブリッジ インターフェースの設定 (364 ページ)
- ハードウェア障害に備えた L2 バイパスの設定 (365 ページ)

プライマリ ブリッジ インターフェースの設定

プライマリ ブリッジ インターフェースを設定するには、以下の手順に従います。

1. 「**管理 | システム セットアップ | ネットワーク > インターフェース**」に移動します。

2 X1 (WAN) インターフェースの右の列で**設定**アイコンを選択します。

3 インターフェースに静的 IP アドレス (192.168.0.12 など) を設定します。

> **メモ：**プライマリ ブリッジ インターフェースには、静的 IP を割り当てる必要があります。

4 WAN インターフェースの場合のみ:

a デフォルト ゲートウェイを設定します。これは、セキュリティ装置そのものをインターネットに到達させるための必須の設定です。

b DNS サーバを設定します

5 インターフェースに対する「**管理**」オプションを 1 つ以上選択します。**HTTPS**、**Ping** (既定で選択されている)、**SNMP**、**SSH**。

> **メモ：**「**HTTPS**」を選択すると、「**HTTP から HTTPS へのリダイレクトを有効にするためのルールを追加する**」が自動的に選択されます。HTTP/HTTPS リダイレクトの詳細は、「HTTP/HTTPS リダイレクト (286 ページ)」を参照してください。

6 「**ユーザ ログイン**」オプションを選択します。**HTTP** と **HTTPS** のいずれか、または両方のプロトコルを選択します。

7 HTTP から HTTPS へのリダイレクトを有効にするには、「**HTTP から HTTPS へのリダイレクトを有効にするためのルールを追加する**」を選択します。このオプションの詳細については、「HTTP/HTTPS リダイレクト (286 ページ)」を参照してください。

8 「**OK**」を選択します。

セカンダリ ブリッジ インターフェースとして使用するインターフェースを選択します。この選択の詳細については、「L2 ブリッジ インターフェース ゾーンの選択 (351 ページ)」を参照してください。

セカンダリ ブリッジ インターフェースの設定

この例では、(LAN に自動的に割り当てられる) X0 を使用します。

1 「**管理 | システム セットアップ | ネットワーク > インターフェース**」に移動します。

2 X0(LAN) インターフェースの右の列で「**設定**」アイコンを選択します。

3 「**ネットワーク モード**」で、「**レイヤ 2 ブリッジ モード**」を選択します。

4 「**ブリッジ先**」で、「**X1**」インターフェースを選択します。

5 インターフェースに対する「**管理**」オプションを 1 つ以上選択します。**HTTPS**、**Ping** (既定で選択されている)、**SNMP**、**SSH**。

> **メモ：**「**HTTPS**」を選択すると、「**HTTP から HTTPS へのリダイレクトを有効にするためのルールを追加する**」が自動的に選択されます。HTTP/HTTPS リダイレクトの詳細は、「HTTP/HTTPS リダイレクト (286 ページ)」を参照してください。

6 「**ユーザ ログイン**」オプションを選択します。**HTTP** と **HTTPS** のいずれか、または両方のプロトコルを選択します。

7 HTTP から HTTPS へのリダイレクトを有効にするには、「**HTTP から HTTPS へのリダイレクトを有効にするためのルールを追加する**」を選択します。このオプションの詳細については、「HTTP/HTTPS リダイレクト (286 ページ)」を参照してください。

8 必要に応じて、L2 ブリッジが IPv4 以外のトラフィックを通すことを防ぐために「**すべての非 IPv4 トラフィックを遮断する**」を有効にすることもできます。

9 L2 ブリッジを通る VLAN トラフィックを制御するには、「VLAN フィルタ」を選択します。既定では、すべての VLAN が許可されます。

- ドロップダウン リストから「**リストされた VLAN を遮断する (ブラックリスト)**」を選択し、遮断する VLAN を左ペインから選んで右ペインに追加します。右ペインに追加された VLAN はすべて遮断されます。また、左ペインに残っている VLAN はすべて許可されます。
- ドロップダウン リストから「**リストされた VLAN を許可する (ホワイトリスト)**」を選択し、明示的に許可する VLAN を左ペインから選んで右ペインに追加します。右ペインに追加された VLAN はすべて許可されます。また、左ペインに残っている VLAN はすべて遮断されます。

10 「**OK**」を選択します。「**インターフェース設定**」テーブルに更新された設定が表示されます。

これで、必要に応じて、セキュリティ サービスを適切なゾーンに適用できるようになりました。この例では、LAN、WAN、または両方のゾーンにセキュリティ サービスを適用する必要があります。

ハードウェア障害に備えた L2 バイパスの設定

L2 バイパスを使用すると、インターフェースが LAN バイパス機能を持つ別のインターフェースにブリッジされる際に、セキュリティ装置の物理的バイパスを行うことができます。これにより、回復不能なファイアウォールのエラーが発生した場合も、ネットワーク トラフィックが流れ続けることができます。

L2 バイパス リレーが閉じられると、バイパスされたインターフェース (X0 および X1) に接続されたネットワーク ケーブルは、単一の連続的なネットワーク ケーブルのように物理的に接続されます。「**異常時の物理的なバイパスを保証する**」オプションを有効にすると、異常時にファイアウォールをバイパスすることにより、ネットワーク トラフィックの中断を回避できます。

L2 バイパスは、**レイヤ 2 ブリッジ モード**のインターフェースにのみ設定できます。「**異常時の物理的なバイパスを保証する**」オプションは、「**モード / IP 割り当て**」で「**レイヤ 2 ブリッジ モード**」を選択した場合のみ表示されます。ブリッジペアの 2 つのインターフェースの間に物理的なバイパス リレーがないかぎり、このオプションは表示されません。

「**異常時の物理的なバイパスを保証する**」オプションを有効にすると、他の「**レイヤ 2 ブリッジ モード**」オプションも自動的に次のように設定されます。

- **すべての非 IPv4 トラフィックを遮断する** - 無効。このオプションが有効の場合、すべての非 IPv4 イーサネット フレームが遮断されます。そのため、このオプションは無効になります。
- **このブリッジ ペアにトラフィックをルーティングしない** - 有効。このオプションが有効の場合、ブリッジ ペアのピア ネットワーク以外に向けてパケットがルーティングされるのを防ぎます。そのため、このオプションは有効になります。
- **このブリッジ ペアのトラフィックのみスニフする** - 無効。このオプションが有効の場合、ブリッジ ペアのインターフェースで受信したトラフィックは一切転送されません。そのため、このオプションは無効になります。
- **このブリッジ ペアでステートフル インスペクションを無効にする** - 変更しない。このオプションは影響を受けません。

L2 バイパスを設定するには、以下の手順に従います。

1 「**管理 | システム セットアップ | ネットワーク > インターフェース**」に移動します。

2 設定するインターフェースの「**設定**」列にある**編集**アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。

3 「**異常時の物理的なバイパスを保証する**」を選択します。

メモ：「**異常時の物理的なバイパスを保証する**」オプションは、NSA-6600 以降の装置で X0 および X1 インターフェースをブリッジしている場合にのみ利用可能です。

4 「**OK**」を選択します。

レイヤ 2 ブリッジ モードでの VLAN 統合

VLAN は、SonicWall セキュリティ装置でサポートされています。VLAN タグを持ったパケットが物理インターフェースに到着すると、VLAN ID が評価され、それがサポートされているかどうかが判断されます。VLAN タグが除去され、その後は、他のトラフィックと同じようにパケット処理が続行されます。受信および送信パケット パスの単純化された表示には、繰り返しが起こり得る次の手順が含まれます。

- IP 検証と再組み立て
- カプセル化解除 (802.1q、PPP)
- 復号化
- 接続キャッシュの調査と管理
- ルート ポリシー調査
- NAT ポリシー調査
- アクセス ルール (ポリシー) 調査
- 帯域幅管理
- NAT 変換
- 高度なパケット処理 (該当する場合)
    - TCP 検証
    - 管理トラフィック処理
    - コンテンツ フィルタ
    - 変換とフロー分析 (SonicWall セキュリティ装置の場合): H.323、SIP、RTSP、ILS/LDAP、FTP、Oracle、NetBIOS、Real Audio、TFTP
    - IP と GAV

この時点で、許可されたトラフィックであると確認された場合、そのパケットが送信先へと転送されます。パケットの送信パスには次の処理が含まれます。

- 暗号化
- カプセル化
- IP 断片化

送信時には、ルート ポリシーの調査によってゲートウェイ インターフェースが VLAN サブインターフェースであると判断された場合、パケットが適切な VLAN ID ヘッダーでタグ付け (カプセル化) されます。ファイアウォールのルーティング ポリシー テーブルは、VLAN サブインターフェースを作成すると自動的に更新されます。

VLAN サブインターフェースに関連した NAT ポリシーおよびアクセス ルールの自動作成は、物理インターフェースの場合とまったく同じように行われます。VLAN 間のトラフィックを制御するルールおよびポリシーは、SonicOS の使いやすく効率的なインターフェースを使ってカスタマイズできます。

一般的な管理の過程で、またはサブインターフェースの作成手順でゾーンを作成する際、ゾーンの作成ページに、そのゾーンに対する GroupVPN の自動作成を制御するチェックボックスが表示されます。既定では、新たに作成された無線タイプのゾーンについてのみ、「**GroupVPN を生成する**」が有効になっています。なお、このオプションは、他のゾーン タイプでもゾーンの作成時にチェックボックスをオンにすることで有効化できます。

VLAN サブインターフェース間のセキュリティ サービスの管理は、ゾーン レベルで行われます。すべてのセキュリティ サービスは、物理インターフェース、VLAN サブインターフェース、またはその両者の組み合わせから成るゾーンに対して設定および適用できます。

異なるワークグループ間のゲートウェイ アンチウイルスおよび侵入防御サービスは、保護セグメントごとに専用の物理インターフェースを用意しなくても、VLAN のセグメント化によって容易に達成できます。

VLAN サポートにより、組織は、ファイアウォール上で専用の物理インターフェースを使用することなく、各種ワークグループ間やワークグループとサーバ ファーム間に (単純なパケット フィルタと比べて) より効果的な内部セキュリティを導入できます。

本書では、VLAN サブインターフェースを WAN ゾーンに割り当てて、WAN クライアント モードを使用する機能 (WAN ゾーンに割り当てられた VLAN サブインターフェースでは、静的アドレッシングのみサポートされます) のほか、WAN 負荷分散およびフェイルオーバーをサポートする機能を紹介しています。また、SonicPoint をワークグループ スイッチ上のアクセス モードの VLAN ポートに接続することによって、ネットワーク全体に SonicPoint を分散させる方法についても紹介しています。これらのスイッチは、コア スイッチにバックホールされ、その後、すべての VLAN がトランク リンクを介して装置に接続されます。

レイヤ 2 ブリッジ モードでの VPN 統合

レイヤ 2 ブリッジ モード向けにも設定されているインターフェースでの VPN 設定時には、着信 VPN トラフィックが適切に セキュリティ装置を通過するように追加のルートを設定する必要があります。

レイヤ2 ブリッジ モードで VPN 統合を設定するには、以下の手順に従います。

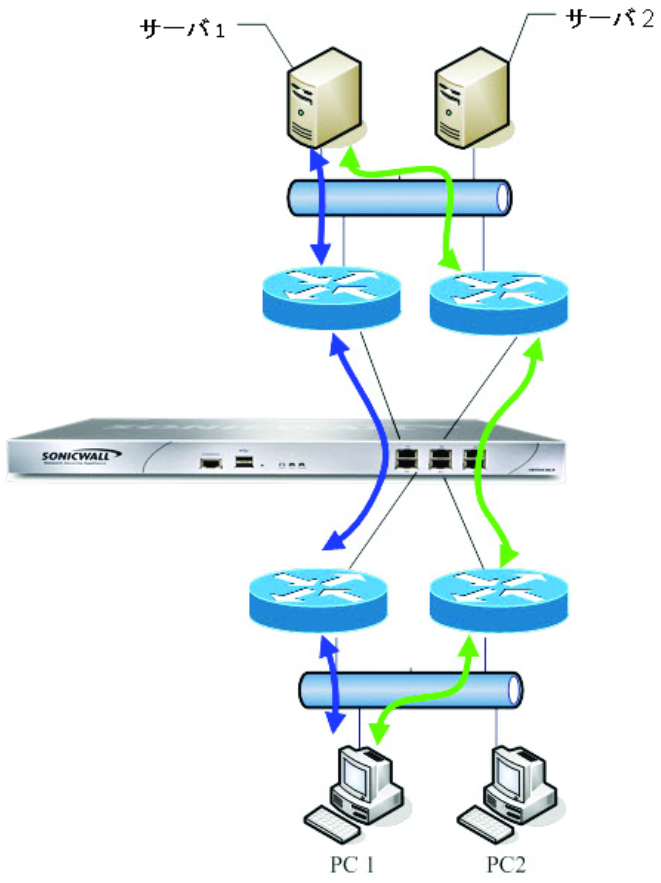
1. 「**管理 | システム セットアップ | ネットワーク > インターフェース**」に移動します。
2. **追加**アイコンを選択します。「**ルート ポリシーの追加**」ダイアログが表示されます。
3. ルートを次のように設定します。
   - 送信元: **すべて**
   - 送信先: *個別の VPN アドレス オブジェクト* (これはローカル VPN トンネルの IP アドレス範囲を表すアドレス オブジェクトです)
   - サービス: **すべて**
   - ゲートウェイ: 0.0.0.0
   - インターフェース: **X0**
4. 「**OK**」を選択します。

非対称ルーティング

SonicOS は非対称ルーティングをサポートしています。非対称ルーティングとは、往路と復路でパケットのフローが別のインターフェースを通るようなルーティングです。これが行われることがあるのは、トラフィックがセキュリティ装置上の異なるレイヤ 2 ブリッジ ペア インターフェースを通るとき、または高可用性クラスタ内の異なるセキュリティ装置を通るときです。

精密パケット検査またはステートフルなファイアウォール アクティビティを実行するすべてのセキュリティ装置は、パケット フローに関連付けられているすべてのパケットを "確認" する必要があります。これは、フロー内の各パケットが、目的の送信先に到達する限り、理論的には異なるパスに沿って転送されてもよい (つまり、介在するルータがパケットをいちいち確認しなくてよい) 従来の IP ルーティングとは対照的です。現在のルータは各パケット フローで一貫したネクストホップによるパケット転送を試みますが、これは一方向へのパケット転送にしか当てはまりません。ルータは、送信側ルータへの戻りのトラフィックの誘導を一切試みません。こうした IP ルーティング動作は、非対称ルーティングをサポートしないセキュリティ装置クラスタにとって問題となります。一連のクラスタ ノードが、すべて同じネットワークへのパスを提供するからです。クラスタを介してネットワークにパケットを転送するルータは、任意のクラスタ ノードをネクストホップとして選択する可能性があります。その結果、ある方向へのパケットのフローに使用されたノードがその戻りのパスで使用されるノードとは異なる非対称なルーティングとなります。フローのこの変化が、一方または両方のクラスタ ノードでトラフィックが破棄される原因となります。どちらのノードもフローのすべてのトラフィックを "確認" していないからです。「非対称ルーティング」を参照してください。

非対称ルーティング



非対称ルーティング トラフィック

「非対称ルーティング」で、PC1 が Server1 と通信するとき、双方向のトラフィックは異なるルータを通ります。つまり、同じ接続のパケットの中に青色のパスを通るものと、緑色のパスを通るものがあります。このような配備では、ルータが冗長ルート プロトコルや負荷分散プロトコル (例えば、Cisco HSRP プロトコル) を実行することがあります。

SonicOS ではステートフル検査が使われます。このセキュリティ装置を通るすべての接続はインターフェースに関連付けられます。しかし、非対称ルーティングがサポートされるようになったので、SonicOS は、フローが異なるインターフェースを通るときも、受信トラフィックと送信トラフィックを追跡し、ステートフルな精密パケット検査を提供します。

メモ：非対称ルーティングは、応答を返さない単方向接続 (すなわち、TCP 状態バイパス) とは別のものです。

インターフェースの IPv6 設定

IPv6 インターフェースの設定の詳細については、「IPv6 インターフェースの設定 (986 ページ)」を参照してください。

31 ビット ネットワーク

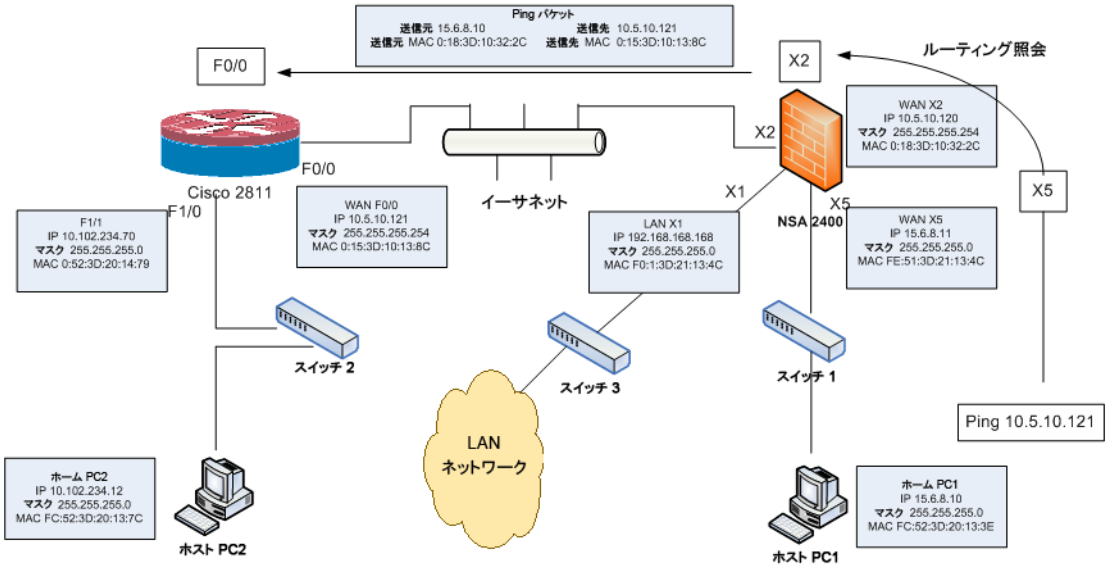
SonicOS 6.2.7 では、31 ビットのサブネット マスクの使用を定義する RFC 3021 がサポートされるようになりました。このマスクでは、サブネット内で 2 つのホスト アドレスしか使用できず、ネットワーク アドレスやゲートウェイ アドレス、ブロードキャスト アドレスはありません。このような設定は、大規模なネットワーク内で 2 つのホストをポイント ツー ポイント リンクで接続するために使用できます。この変更がアドレス空間の節約に結び付くことは明白で、大規模なネットワーク内の各ポイント ツー ポイント リンクが消費するアドレスが 4 つではなく 2 つになります。

ここでいうポイント ツー ポイント リンクは、PPP (Point to Point Protocol) とは異なります。31 ビット マスクを使用するポイント ツー ポイント リンクでは、PPP プロトコルを使用してもしなくてもかまいません。ポイント ツー ポイント リンク上の 31 ビットの接頭辞付き IPv4 アドレスは、イーサネット ネットワークでも使用できます。

トピック:

- ネットワーク環境の例 (370 ページ)
- SonicOSの設定 (370 ページ)

ネットワーク環境の例



このネットワーク環境では、ホスト PC1 とホスト PC2 は相互にアクセスすることができます。一方、LAN ネットワーク内のホストはホスト PC2 にアクセスすることができます。

この環境用の設定を行うには:

1 ホスト PC1 で、次のように 2 つのルート エントリを追加します。

- `Route add 10.5.10.0 mask 255.255.255.0  15.6.8.10`
- `Route add 10.102.234.0 mask 255.255.255.0  15.6.8.10`

2 ホスト PC2 で、次のように 2 つのルート エントリを追加します。

- `Route add 10.5.10.0 mask 255.255.255.0  10.102.234.70`
- `Route add 15.6.8.0 mask 255.255.255.0  10.102.234.70`

3 Cisco ルータ (F0/0) で、次の設定を行います。

- `interface fastEthernet 0/0`
- `ip address 10.5.10.120 255.255.255.254`

4 Cisco 2811 で、次のように 1 つのルート エントリを追加します。

```
!
ip route 15.6.8.0 255.255.255.0 10.5.10.120
!
```

5 ファイアウォールで、次のように 1 つのルート エントリを追加して、WAN ゾーンのデータが X2 から X5、および X5 から X2 に流れるようにします。

```
Any    10.102.234.0    Any    X2 Default Gateway    X2
```

SonicOSの設定

インターフェースを 31 ビット サブネット用に設定するには:

1 **「管理 | システム セットアップ | ネットワーク > インターフェース」**に移動します。

2 目的のインターフェースを編集します。

3 「**サブネット マスク**」を 255.255.255.254 に設定します。

4 「**IP アドレス**」フィールドに一方のホスト IP アドレスを入力します。

5 「**デフォルト ゲートウェイ**」フィールドにもう一方のホスト IP アドレスを入力します。

6 必要に応じて、使用中のネットワークに合わせて他のフィールドを設定します。

7 「**OK**」を選択します。

PPPoE アンナンバード インターフェースのサポート

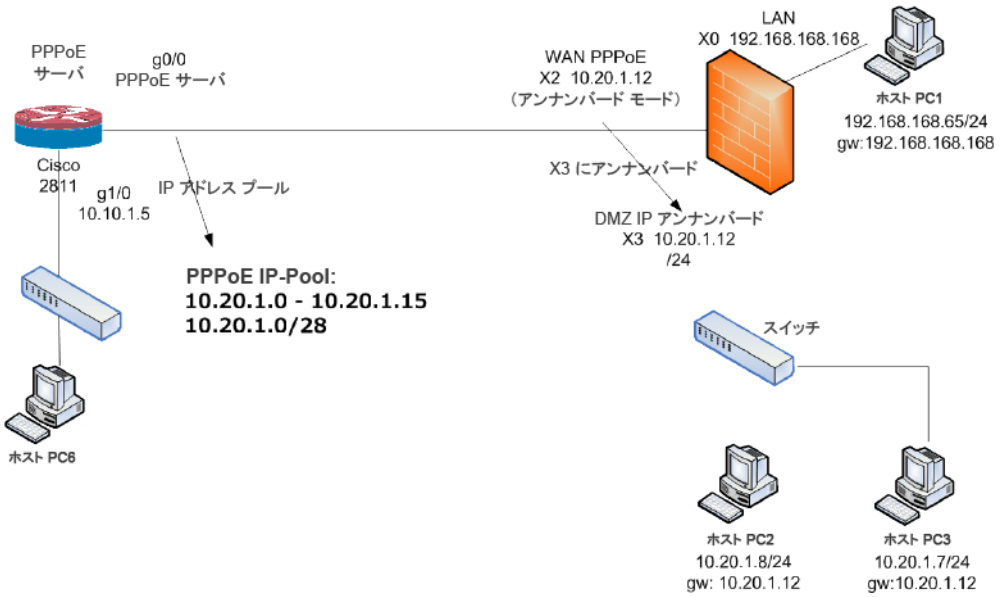
PPPoE アンナンバード インターフェースを使用すると、1 つの PPPoE 接続だけで一連の IP アドレスを管理できます。インターネット サービス プロバイダ (ISP) は、サブネット内で割り当て可能な複数の静的 IP アドレスを提供します。最初のアドレスはネットワーク アドレスとして指定され、最後のアドレスはブロードキャスト アドレスとして指定されます。

PPPoE の既定の MTU は **1492** です。

トピック:

- サンプル ネットワーク トポロジ (371 ページ)
- 注意 (372 ページ)
- PPPoE アンナンバード インターフェースの設定 (372 ページ)
- PPPoE アンナンバードによる HA の設定 (372 ページ)

サンプル ネットワーク トポロジ



このトポロジでは、X2 は PPPoE アンナンバード インターフェースで、X3 はアンナンバード インターフェースです。

SonicOS は、2 つのポリシーを「**ネットワーク > ルーティング > ルート ポリシー**」テーブルに追加します。

SonicOS は 2 つの NAT ポリシーも追加します。

注意

X2 から X3 へのアンナンバードが設定されているときに、X3 を別のモードに変更するには、先に X2 を別のモードに変更して X2 との関係を終了します。そうしないと、インターフェース X3 の IP アドレスまたはマスクを変更した場合に、X3 は PPPoE サーバに再接続します。

X3 がアンナンバード インターフェースとして設定されている場合、他のインターフェースから L2 ブリッジを使用して X3 に接続することはできません。

PPPoE アンナンバード インターフェースの設定

PPPoE アンナンバード インターフェースを設定するには、以下の手順に従います。

1 「**管理 | システム セットアップ | ネットワーク > インターフェース**」に移動します。

2 **編集**アイコンを選択して、WAN インターフェースに対する PPPoE クライアント設定を行います。「**インターフェースの編集**」ダイアログが表示されます。

3 「**アンナンバード インターフェース**」を選択します。ドロップダウン メニューがアクティブになります。

4 「**新規アンナンバード インターフェースの作成**」を選択します。「**アンナンバード インターフェースの追加**」ダイアログが表示されます。

5 「**ゾーン**」で、「**LAN**」または「**DMZ**」を選択するか、新しいゾーンを作成します。

ⓘ **メモ：**「**モード / IP 割り当て**」が「**IP アンナンバード**」に設定され、淡色表示になります。

6 「**IP アドレス**」には、ISP から提供されたアドレスを入力します。通常は、プロバイダから割り当てられた 2 番目の IP アドレスを使用します。

7 「**サブネット マスク**」フィールドに、ISP によって割り当てられたサブネット マスクを入力します。

8 このインターフェースの設定を終了します。

9 「**OK**」を選択します。

10 最初のインターフェースの設定を終了します。

11 「**OK**」を選択します。

PPPoE アンナンバードによる HA の設定

PPPoE アンナンバードによる HA の設定方法については、「アクティブ/スタンバイ高可用性機能の設定 (727 ページ)」を参照してください。

14

PortShield インターフェースの設定

メモ：NSA 2600 セキュリティ装置は PortShield をサポートしておらず、SOHO W セキュリティ装置は X シリーズ ソリューションをサポートしていません。

- ネットワーク > PortShield グループ (373 ページ)
  - PortShield について (373 ページ)
  - SonicOS がサポートする X シリーズ スイッチ (374 ページ)
  - SonicOS がサポートする N シリーズ スイッチ (384 ページ)
  - ポートの管理 (389 ページ)
  - PortShield グループの設定 (398 ページ)

ネットワーク > PortShield グループ

トピック:

- PortShield について (373 ページ)
- SonicOS がサポートする X シリーズ スイッチ (374 ページ)
- SonicOS がサポートする N シリーズ スイッチ (384 ページ)
- ポートの管理 (389 ページ)
- PortShield グループの設定 (398 ページ)

PortShield について

PortShield インターフェースとは、Dell X シリーズ、つまり拡張されたスイッチ上のポートを含む、一連のポートが割り当てられた仮想インターフェースです。PortShield 手法により、LAN ポートの一部または全部を別々のセキュリティ コンテキストに設定し、WAN と DMZ からだけでなく、ネットワーク内の機器間でも保護できるようになります。実際、各コンテキストには、専用の精密パケット検査セキュリティ装置によって保護される独自のワイヤスピード PortShield があります。

ヒント：PortShield グループを使用しなくても、「**管理 | システム セットアップ | ネットワーク > インターフェース**」で複数のインターフェースにいつでもゾーンを適用できます。ただし、PortShield を使用してグループ化しないと、それらのインターフェースで同じネットワーク サブネットは共有されません。

PortShield インターフェースには、さまざまな組み合わせのポートを割り当てることができます。PortShield インターフェースに割り当てられていないポートはすべて、LAN インターフェースに割り当てられます。

静的モードとトランスペアレント モード

PortShield インターフェースの作成に使用できる IP 割り当て方式は 2 種類あります。

- 静的モード
- トランスペアレント モード

静的モードの処理

静的モードで PortShield インターフェースを作成する場合、PortShield インターフェースに適用する明示的アドレスを手動で作成します。そのインターフェースに割り当てるポートはすべて、このアドレスで識別されます。静的モードは、保護ゾーン、公開ゾーン、または無線ゾーンに割り当てられるインターフェースに使用できます。

メモ：静的モードで PortShield インターフェースを作成する場合、そのインターフェースに割り当てる IP アドレスが別の PortShield インターフェースに使用されていないことを確認してください。

トランスペアレント モードの処理

トランスペアレント モードのアドレス指定では、アドレス オブジェクトの割り当てを通じて、現在のインターフェースで WAN サブネットワークを共有できます。インターフェースの IP アドレスは、WAN インターフェースの IP アドレスと同じになります。トランスペアレント モードは、保護ゾーンと公開ゾーンに割り当てられるインターフェースに使用できます。

メモ：PortShield インターフェースに割り当てる IP アドレスが WAN サブネットワーク内にあることを確認してください。

トランスペアレント モードで PortShield インターフェースを作成する場合、PortShield インターフェースに適用するアドレスの範囲を作成します。これらのアドレスは、アドレス オブジェクトという 1 つのエンティティに含めます。アドレス オブジェクトを使用することで、1 度定義したエンティティを SonicOS インターフェース全体の複数の参照インスタンスで再利用することができます。アドレス オブジェクトを使用して PortShield インターフェースを作成する場合、そのインターフェースに割り当てられるポートはすべて、アドレス範囲で指定するアドレスのいずれかによって識別されます。

メモ：静的にアドレス指定する PortShield インターフェースは、それぞれ 1 つのサブネットワークに作成する必要があります。複数のサブネットワークに PortShield インターフェースを分散させることはできません。

SonicOS がサポートする X シリーズ スイッチ

トピック:

- X シリーズ ソリューションについて (375 ページ)
- サポートされているトポロジ (383 ページ)

X シリーズ ソリューションについて

メモ：X シリーズ ソリューションは、NSA 2600 および SOHO W セキュリティ装置ではサポートされていません。

セキュリティ装置、スイッチなどの重要なネットワーク要素は、一般に個別に管理する必要があります。SonicOS により、セキュリティ装置管理インターフェースと GMS を使用して、セキュリティ装置と Dell X シリーズ スイッチの両方を統合管理できます。

SonicWall セキュリティ装置で使用可能なインターフェースの最大数は、「セキュリティ装置あたりのインターフェース数」テーブルに示すように、モデルによって異なります。

セキュリティ装置あたりのインターフェース数

ファイアウォール モデル	物理インターフェース
SM 9600	20 (10 GbE SFP+ x 4、1 GbE SFP x 8、1GE 銅線 x 8)、GbE 管理 x 1、コンソール x 1
SM 9400	20 (10 GbE SFP+ x 4、1 GbE SFP x 8、1GE 銅線 x 8)、GbE 管理 x 1、コンソール x 1
SM 9200	20 (10 GbE SFP+ x 4、1 GbE SFP x 8、1GE 銅線 x 8)、GbE 管理 x 1、コンソール x 1
NSA 6600	20 (10 GbE SFP+ x 4、1 GbE SFP x 8、1GE 銅線 x 8)、GbE 管理 x 1、コンソール x 1
NSA 5600	18 (10 GbE SFP+ x 2、1 GbE SFP x 4、1GE 銅線 x 12)、管理 x 1
NSA 4600	18 (10 GbE SFP+ x 2、1 GbE SFP x 4、1GE 銅線 x 12)、管理 x 1
NSA 3600	18 (10 GbE SFP+ x 2、1 GbE SFP x 4、1GE 銅線 x 12)、管理 x 1
NSA 2650	
TZ600	1 GbE x 10
TZ500 シリーズ	1 GbE x 8
TZ400 シリーズ	1 GbE x 7
TZ300 シリーズ	1 GbE x 5

ある種の配備では、セキュリティ装置上で使用可能なインターフェースの最大数を軽く超えるポート数が必要になる場合があります。X シリーズ ソリューションでは、Dell X シリーズ スイッチ上のポートをセキュリティ装置の拡張インターフェースと見なすことができます。そのため、使用できるインターフェースの数を最大 192 (X シリーズ スイッチによって値は異なる) に増やすことができます。これらの拡張ポートは、Portshield で保護したり、高可用性 (HA) を提供するように設定したり、セキュリティ装置の他のインターフェースとして扱われるようにすることができます。

メモ：X シリーズ スイッチ、X スイッチ、外部スイッチ、および拡張スイッチは、同じものを意味します。

「SonicWall セキュリティ装置 でサポートされている X シリーズ スイッチ」テーブルに示す SonicWall セキュリティ装置は、記載されている X シリーズ スイッチを 4 台までサポートします。

メモ：X シリーズ スイッチの詳細と設定方法については、『*SonicWall X シリーズ ソリューション配備ガイド*』、『*Dell Networking X1000 および X4000 シリーズ スイッチ ユーザ ガイド*』、『*Dell Networking X1000 および X4000 シリーズ スイッチ導入ガイド*』を参照してください。

SonicWall セキュリティ装置 でサポートされている X シリーズ スイッチ

SonicWall セキュリティ装置		
• SuperMassive 9600 • SuperMassive 9400 • SuperMassive 9200	• NSA 6600 • NSA 5600 • NSA 4600 • NSA 3600 • NSA 2650	• TZ600 • TZ500/TZ500W • TZ400/TZ400W • TZ350/TZ350W • TZ300/TZ300W

サポート対象の X シリーズ スイッチ (ポート)

- X1008 (8 10/100/1000Base-T GbE)
- X1008P (8 10/100/1000Base-T GbE、2 1GbE SFP 光ファイバ、 8 PoE/最大合計 123 W)
- X1018 (16 10/100/1000Base-T GbE、2 1GbE SFP 光ファイバ)
- X1018P (16 10/100/1000Base-T GbE、2 1GbE SFP 光ファイバ、16 PoE/最大合計 246 W)
- X1026 (24 10/100/1000Base-T GbE、2 1GbE SFP 光ファイバ)
- X1026P (24 10/100/1000Base-T GbE、2 1GbE SFP 光ファイバ、24 PoE/12 PoE+/最大合計 369 W)
- X1052 (48 10/100/1000Base-T GbE、2 10GbE SFP/SFP+ 光ファイバ)
- X1052P (48 10/100/1000Base-T GbE、24 PoE/12 PoE+/最大合計 369 W)
- X4012 (12 10GbE SFP/SFP+ 光ファイバ)

メモ：X シリーズ ソリューションは、NSA 2600 および SOHO W セキュリティ装置ではサポートされていません。

トピック:

- 用語 (376 ページ)
- パフォーマンスの要件 (377 ページ)
- X シリーズ スイッチでサポートされる主な機能 (377 ページ)
- PortShield 機能と X シリーズ スイッチ (378 ページ)
- Dell X シリーズのデイジーチェーン接続のサポート (379 ページ)
- PoE/PoE+ および SFP/SFP+ のサポート (380 ページ)
- X シリーズ ソリューションと SonicPoint (381 ページ)
- GMS による拡張スイッチの管理 (381 ページ)
- 拡張スイッチのグローバル パラメータ (382 ページ)
- リンクの概要 (382 ページ)
- ログ記録と Syslog サポート (383 ページ)

用語

HA	高可用性
拡張スイッチ	X シリーズスイッチと同じ。
外部スイッチ	X シリーズスイッチと同じ。

IDV	Interface Disambiguation through VLAN - 拡張スイッチ上で、ポートをセキュリティ装置のインターフェースに対して PortShield して再設定し、PortShield VLAN に対応する VLAN アクセス ポートとします。
PoE	Power over Ethernet - イーサネット ケーブルを通じてデータと共に電力を供給するシステム。1 本のケーブルでデータ接続と装置への電力の両方を提供できます。
PoE+	Power over Ethernet Plus - PoE より多くの電力を供給できる、PoEの強化バージョン (標準 802.3at)。
SFP	Small Form-Factor Pluggable - 電気通信アプリケーションとデータ通信アプリケーションの両方に使用されるホットプラグ対応の小型トランシーバ。1Gb ファイバ モジュールをサポートします。
SFP+	Enhanced Small Form-Factor Pluggable - 10 Gb ファイバ モジュールをサポートする、SFP の強化バージョン。
SPM	シングル ポイント管理
STP	スパニング ツリー プロトコル (Spanning Tree Protocol) - イーサネット ネットワークにループフリー トポロジを保証するネットワーク プロトコル。冗長 (予備) リンクを提供し、アクティブなリンクに障害が発生した場合にバックアップ パスを提供します。

パフォーマンスの要件

SonicWall セキュリティ装置は次のことができるようになりました。

- 最大 4 台の X シリーズ スイッチをプロビジョニングする。
- より多くのポートを管理する。

X シリーズ スイッチでサポートされる主な機能

メモ：これらの機能については、『SonicWall 展開計画ガイド』を参照してください。

- X シリーズ スイッチの、拡張スイッチとしてのプロビジョニング
- PortShield 機能
- 拡張スイッチ インターフェース設定の実行
- 基本的な拡張スイッチ グローバル パラメータの管理
- GMS による拡張スイッチの管理
- PortShield 機能による高可用性 (HA)

  HA モードの PortShield 機能が共通アップリンクを使用してサポートされます。この設定では、アクティブ/スタンバイ セキュリティ装置と X シリーズ スイッチの間のリンクが、すべての PortShield トラフィックを伝送する共通アップリンクとして機能します。また、この設定では、PortShield ホストとして機能するセキュリティ装置インターフェースが、アクティブ装置とスタンバイ装置に接続された同じ X シリーズ スイッチではなく、独立したスイッチに接続されている必要があります。これにより、同じ PortShield VLAN でのパケットのループが回避されます。PortShield メンバーは、アクティブ/スタンバイ セキュリティ装置から制御される X シリーズ スイッチのポートに接続できます。
- 拡張スイッチの診断サポート
- SPM による共通アップリンク設定での VLAN のサポート
- 専用アップリンク設定での VLAN のサポート

- VLAN トラフィック用の共通アップリンクを介した一元管理

  VLAN は共通アップリンクでもサポートされます。このため、セキュリティ装置と X シリーズ スイッチを結ぶ単一のリンクで、X シリーズ スイッチを管理するセキュリティ装置の管理トラフィック、セキュリティ装置のインターフェースに対応する IDV (*Interface Disambiguation via VLAN*) VLAN の PortShield トラフィック、および共通アップリンク インターフェースに存在する VLAN サブインターフェースのトラフィックを伝送できます。

  メモ：同じスイッチに対する専用アップリンクまたは共通アップリンクとして設定されたセキュリティ装置インターフェースに、重複する VLAN が存在することはできません。これは、VLAN 空間が X シリーズ スイッチ上でグローバルだからです。

  メモ：アクセス/トランク設定用の VLAN を選択せずに、拡張スイッチ インターフェースから共通アップリンク インターフェースへの PortShield を設定することはできません。

- 特定の Dell X シリーズ スイッチが備えている SonicWall セキュリティ装置向けの PoE/PoE+ 機能および SFP/SFP+ 機能
- 設定メッセージのバッチ化 - X シリーズ スイッチのサポートを容易にするため、設定メッセージをバッチ化してから X シリーズ スイッチに送信できます。

PortShield 機能と X シリーズ スイッチ

PortShield アーキテクチャは、セキュリティ装置のポートを複数の独立したセキュリティ ゾーンに設定することを可能にします。ゾーンをまたいでデバイス間を流れるトラフィックを精密パケット検査セキュリティ装置で保護できます。PortShield 機能の詳細については、「PortShield インターフェースの設定 (373 ページ)」を参照してください。

SonicWall X シリーズ ソリューションでは、拡張スイッチ上でセキュリティ装置インターフェースに対する PortShield 機能を使用できます。X シリーズ スイッチは L2 スイッチで、既定では拡張スイッチのすべてのポートが既定の VLAN 1 のアクセス ポート部として設定されます。拡張スイッチのポートをセキュリティ装置インターフェースに対して PortShield すると、それらのポートは PortShield VLAN に対応する VLAN のアクセス ポートとして再設定されます。このような設定は、PortShield ホスト インターフェースの IDV VLAN とも呼ばれます。

トピック:

- PortShield によるさまざまなトラフィック シナリオ (378 ページ)
- X シリーズ スイッチを PortShield するための前提条件 (379 ページ)

PortShield によるさまざまなトラフィック シナリオ

- ネットワーク装置を同一の PortShield グループに属する、拡張スイッチのポートに接続した場合、それらのネットワーク装置の間を流れるトラフィックは拡張スイッチによって自動的に交換されます。
- ネットワーク装置を拡張スイッチのポートに接続し、さらに同一の PortShield グループに属する、セキュリティ装置のポートに接続した場合、それらのネットワーク装置の間を流れるトラフィックはセキュリティ装置の内部スイッチによって交換されます。
- ネットワーク装置をセキュリティ装置のインターフェースに向けられる、拡張スイッチのポートに接続した場合、それらのネットワーク装置の間を流れるトラフィックはソフトウェア内のデータ パスで処理されます。これらのトラフィックをセキュリティ装置のセキュリティ サービス (アクセス ルール、精密パケット検査、侵入防御など) で処理することもできます。

- ネットワーク装置を拡張スイッチのポートに接続し、さらに異なるゾーンまたは異なる PortShield グループに属する、セキュリティ装置のポートに接続した場合、それらのネットワーク装置の間を流れるトラフィックはソフトウェア内のデータ パスで転送されます。それらのトラフィックはセキュリティ装置のセキュリティ サービスによってソフトウェアで処理されます。

X シリーズ スイッチを PortShield するための前提条件

重要：トポロジに 2 台以上の X シリーズ スイッチがある場合は、それらの X シリーズ スイッチをカスケード接続またはデイジー チェーン接続にすることができます。つまり、1 台の X シリーズ スイッチを、セキュリティ装置に接続されている別の X シリーズ スイッチに接続できます。

- X シリーズ スイッチ (モデル X1052/X1052P 以外) は、スイッチへの不正アクセスを防止するために非管理モードで出荷されます。スイッチを管理モードに切り替えるには、電源プラグ近くの「**モード**」を 7 秒以上押す必要があります。

  出荷時のモデル X1052/X1052P は既定で管理モードになっています。

  スイッチの初期セットアップ段階では、セキュリティ装置のインターフェースで DHCP サーバが有効になっていても X シリーズ スイッチの IP が動的に変化しないようにするために、**動的 IP** ではなく**静的 IP** を選択してください。

  詳細は、『*SonicWall X シリーズ ソリューション配備ガイド*』を参照してください。
- 初期の IP アドレス、ユーザ名/パスワード設定 (スイッチに記載されている) は別として、その他の設定は X シリーズ スイッチの GUI/コンソールから直接行わないようにすることをお勧めします。そのようにすると、セキュリティ装置と X シリーズ スイッチの設定状態との同期がとれなくなります。
- X シリーズのスイッチをセキュリティ装置から管理するには、セキュリティ装置のインターフェースの 1 つが X シリーズのスイッチと同じサブネットに存在する必要があります。例えば、既定の IP `192.168.2.1` を使って X シリーズ スイッチを管理する場合は、セキュリティ装置のインターフェースを `192.168.2.0/24` サブネット内に設定し、X シリーズ スイッチに接続する必要があります。
- セキュリティ装置からスイッチのプロビジョニングや管理を行う前に、セキュリティ装置から X シリーズ スイッチに Ping を実行して X シリーズ スイッチに到達できることを確認します。
- VLAN サポート:
  - VLAN のサポートは共有された共通のアップリンクで利用できます。例えば、X シリーズ スイッチの共有アップリンクとしてプロビジョニングされているのセキュリティ装置インターフェースでは VLAN を設定できません。
  - VLAN サポートの詳細は、『*SonicWall X シリーズ ソリューション配備ガイド*』を参照してください。
  - 専用アップリンクとして設定されたセキュリティ装置インターフェースに重複する VLAN は存在できません。例えば、X3 と X5 が専用アップリンクとして設定されている場合、VLAN 100 は X3 と X5 の両方に存在できません。このような設定は拒否されます。

Dell X シリーズのデイジーチェーン接続のサポート

メモ：この機能は NSA 2600 プラットフォームではサポートされていません。

Dell TZ-X デイジーチェーン接続ソリューションは、デイジーチェーン モードで接続された Dell X シリーズ スイッチと SonicWall セキュリティ装置との統合を可能にします。デイジーチェーン モードでは、すべての Dell X シリーズ スイッチ モデル (X1008/X1008P、X1018/X1018P、X1026/X1026P、X1052/X1052P、X4012 など) との統合がサポートされます。

デイジー チェーン接続により、大規模な設備 (倉庫など) を持つユーザは、敷地内に 2 台の X シリーズ スイッチを 1,000 フィート以上の距離を置いて配備できます。2 台のスイッチは光ファイバーを介して相互に接続し、1 台目のスイッチ (親スイッチ) をセキュリティ装置に接続して、両方のスイッチをセキュリティ装置から管理できるようにします。こうした配備では、セキュリティ装置の単一インターフェースを使用して、X シリーズ スイッチ上のより多くのインターフェースにアクセスすることもできます。親スイッチおよび子スイッチのすべてのインターフェースをセキュリティ装置から管理できます。

トピック:

- 想定条件と依存関係 (380 ページ)
- デイジー チェーン接続のサポート (380 ページ)

想定条件と依存関係

- Dell X シリーズ スイッチのデイジーチェーン接続ソリューションでサポート可能なのは、シングル レベルのチェーン接続のみです。2 台を超えるスイッチを直列に接続する、マルチレベルのチェーン接続はサポートされていません。例えば、親スイッチを子スイッチに接続することはできますが、この子スイッチを別の子スイッチに接続することはできません。
- プロビジョニング可能な拡張スイッチは最大 4 台という上限があります。例えば、1 台の親スイッチは最大 3 台の子スイッチを持つことができます。
- デイジーチェーン接続モードでは、子スイッチでサポートされているトポロジが共通アップリンクのみです。このトポロジでは、子スイッチが単一のアップリンクによって親スイッチに接続されます。専用アップリンクや隔離されたリンクなど、その他のバリエーションは子スイッチではサポートされていません。

デイジー チェーン接続のサポート

デイジーチェーン モードで接続された双方のスイッチは同じサブネット内の IP アドレスを持つ必要があり、セキュリティ装置はこのサブネットに到達可能でなければなりません。デイジーチェーン接続モードにあるこれらのスイッチのプロビジョニングの処理は、2 つのステップで行います。

1 親スイッチをスタンドアロン スイッチとしてプロビジョニングします。

2 子スイッチをデイジーチェーン接続されるスイッチとしてプロビジョニングします。

PoE/PoE+ および SFP/SFP+ のサポート

SonicWall セキュリティ装置は PoE/PoE+ 機能をサポートしませんが、特定の X シリーズ スイッチにこの機能を追加することができます。詳細は、「X シリーズ スイッチの PoE/PoE+ および SFP/SFP+ のサポート」テーブルを参照してください。この機能を追加すると、SonicWall セキュリティ装置で使用できる SonicPoint シリーズ製品が増えます。特に 802.11ac をサポートする新しい SonicPoint シリーズを使えるのは、大きなメリットです (802.11ac は最大 30 W の電力をサポートしますが、802.11a/b/g/h は最大 15.4 W にとどまります)。

一部の X シリーズ スイッチでも、SFP/SFP+ 機能がサポートされています。詳細は 「X シリーズ スイッチの PoE/PoE+ および SFP/SFP+ のサポート」テーブルを参照してください。

メモ：X シリーズ スイッチの PoE/PoE+ ポートの設定は、X シリーズ スイッチの UI から管理できます。SonicWall セキュリティ装置の「**管理 | システム セットアップ | ネットワーク > Portshield グループ**」では管理できません。

X シリーズ スイッチの PoE/PoE+ および SFP/SFP+ のサポート

X シリーズ スイッチのモデル	サポートする機能
X1008	1 PoE PD ポート、既定でポート 8 が PD ポート
X1008P	8 PoE ポート、全体で最大 123 W、既定でポート 1 ～ 8 が PoE をサポート
X1018	2 1GbE SFP ポート、既定でポート 17 と 18 が SFP をサポート
X1018P	16 PoE ポート、全体で最大 246W、既定でポート 1 ～ 16 が PoE をサポート 2 1GbE SFP ポート、既定でポート 17 と 18 が SFP をサポート
X1026	2 1GbE SFP ポート、既定でポート 25 と 26 が SFP をサポート
X1026P	24 PoE/12 PoE+ ポート、全体で最大 369W、既定で: • ポート 1 ～ 12 が PoE+ をサポート • ポート 13 ～ 24 が PoE をサポート 2 1GbE SFP ポート、既定でポート 25 と 26 が SFP をサポート
X1052	4 10GbE SFP ポート、既定でポート 49 ～ 52 が SFP+ をサポート
X1052P	24 PoE/12 PoE+ ポート、全体で最大 369W、既定で: • ポート 1 ～ 12 が PoE+ をサポート • ポート 13 ～ 24 が PoE をサポート • ポート 25 ～ 48 は PoE と PoE+ のどちらにも未対応 4 10GbE SFP ポート、既定でポート 49 ～ 52 が SFP+ をサポート
X4012	12 10GbE SFP ポート、既定でポート 1 ～ 12 が SFP+ をサポート

重要：外部電源のない SonicPoint AC の場合、X1026P または X1052P の でポート 1 ～ 12 が PortShield されている必要があります。

外部電源のない SonicPoint の AC 以外のモデルは、ポート 1 ～ 8 (X1008P)、1 ～ 16 (X1018P)、または 1 ～ 24 (X1026P、X1052P) に PortShield できます。

外部電源のある SonicPoint は、どのイーサネット ポートにも PortShield できます。

X シリーズ ソリューションと SonicPoint

拡張スイッチのポートは、セキュリティ装置の WLAN ゾーンに PortShield でき、それらのポートに SonicPoint を接続できます。

SonicPoint を X シリーズ スイッチに接続するときは SonicPoint の所要電力を考慮することが大切です。SonicPointACe/ACi/N2 には、最低 25.5 W が必要です。お使いの X シリーズ スイッチ モデルが PoE+ をサポートしていない場合は、SonicPoint 電力インジェクタを使用する必要があります。スイッチの PoE+ サポート状況については、「PoE/PoE+ および SFP/SFP+ のサポート (380 ページ)」を参照してください。SonicPoint の管理の詳細については、ナレッジ ベース記事『*SonicWall TZ Series and SonicWall X-Series Solution managing SonicPoint ACe/ACi/N2 access points*』 (SW13970) を参照してください。

GMS による拡張スイッチの管理

X シリーズ スイッチの統合機能により、SonicOS 管理インターフェースと SonicWall GMS バージョン 8.1 SP1 以降を使ってセキュリティ装置とスイッチの両方を一元的に管理できます。GMS は、拡張ス

イッチのプロビジョニング、拡張スイッチ インターフェースの設定、拡張スイッチのグローバル パラメータの管理など、すべての設定操作に対応しています。

GMS を使った拡張スイッチの管理については、最新の『*SonicWall GMS 管理者ガイド*』を参照してください。

拡張スイッチのグローバル パラメータ

「拡張スイッチのグローバル パラメータ」テーブルに、拡張スイッチのグローバル パラメータを示します。これらは SonicOS 管理インターフェースから設定できます。

メモ：これらのパラメータの詳細は、『*SonicWall X シリーズ ソリューション配備ガイド*』を参照してください。

拡張スイッチのグローバル パラメータ

すべてのスイッチ	X1026P および X1052P のみのスイッチ
STP モード	PoE 警告使用量のしきい値
STP 状態	PoE トラップ
	PoE 電力制限モード

リンクの概要

管理トラフィックのみを伝送する管理 (MGMT) リンクは、PortShield の対象とすることはできません。

データ リンクは、すべての PortShield トラフィックを伝送します。そのすべての伝送内容がデータなら共通リンクと呼ばれます。多くはありませんがトポロジによっては管理トラフィックを伝送するケースもあり、その場合、共有リンクと呼ばれます。

共有リンクまたは共通リンクは、PortShield されたすべてのグループを伝送します。

専用リンクは、1 つの PortShield グループのみを伝送できます。このグループは、セキュリティ装置の専用ポートに対して PortShield されている必要があります。

アップリンク インターフェースの概要

アップリンク インターフェースは、タグ付けされた / タグ付けされないトラフィックを伝送するように設定された「トランク」ポートとして表示されます。拡張スイッチを追加する際にセキュリティ装置アップリンクと X スイッチ アップリンクのオプションを使うと、SuperMassive アップリンクとして設定されたセキュリティ装置のポートと、スイッチ アップリンクとして設定された拡張スイッチのポートが、すべての IDV VLAN についてタグ付けされたトラフィックを送受信するように自動的に設定されます。IDV VLAN のトラフィックがタグ付けされると、ファームウェアは PortShield ホスト インターフェースでこのトラフィックを扱うことができます。

アップリンク インターフェースを設定するための条件

- インターフェースは、物理インターフェースでなければなりません。仮想インターフェースは使用できません。
- インターフェースは、スイッチ インターフェースでなければなりません (一部のプラットフォームでは、セキュリティ装置のインターフェースがスイッチに接続されていないケースがあります。このようなインターフェースは使用できません)。

- インターフェースを PortShield ホストにすること (他のセキュリティ装置インターフェースをこのインターフェースから PortShield すること)、または PortShield グループ メンバーにすること (他のセキュリティ装置インターフェースから PortShield されること) はできません。
- インターフェースは、ブリッジ プライマリ インターフェースまたはブリッジ セカンダリ インターフェースであってはなりません。
- インターフェースは、子を持つことができません (他の子インターフェースの親インターフェースになることはできません)。

ログ記録と Syslog サポート

クリティカルな設定イベント (スイッチの追加/削除、拡張スイッチ ポートでの PortShield の設定など) やネットワーク イベント (ポートのアップ/ダウンなど) をログに記録するためのサポートが用意されています。

サポートされているトポロジ

重要：セキュリティ装置と X シリーズ スイッチの間のインターフェースをセットアップする前に、『*SonicWall X シリーズ ソリューション配備ガイド*』の説明に従ってスイッチをセットアップしてください。

メモ：これらのトポロジのプロビジョニングおよび設定の詳細は、『*SonicWall X シリーズ ソリューション配備ガイド*』を参照してください。

PortShield インターフェースと X シリーズ スイッチを設定するための基本的な事項については、「ポートの管理 (389 ページ)」を参照してください。

X シリーズ スイッチ サポートでサポートされている主なトポロジは次のとおりです。

- 共通アップリンク設定
- 専用アップリンク設定

  重要：専用リンクに属するポート経由で SonicPoint を PortShield しなければなりません。

- 共通アップリンクと専用アップリンクによるハイブリッド設定
- 管理トラフィックとデータ トラフィックの両方を伝送する共有リンク設定
- 管理およびデータ用のアップリンクとして隔離されたリンク
- 専用アップリンクによる HA および PortShield 設定
- 共通アップリンクによる HA および PortShield 設定
- SPM 設定による共通アップリンクを持つ VLAN
- 専用アップリンクによる VLAN 設定
- SonicPoint アクセス向けの専用リンク

SonicOS がサポートする N シリーズ スイッチ

トピック:

- N シリーズ スイッチについて
- N シリーズ スイッチの設定
- N シリーズ スイッチの、拡張スイッチとしてのプロビジョニング
- アップリンク インターフェースの重要性
- N シリーズ スイッチのプロビジョニング
- PortShield での拡張スイッチの設定

N シリーズ スイッチについて

NSA 2600 および SOHO W プラットフォームを除くすべてのプラットフォームは、これらの Dell® N シリーズ スイッチと N シリーズ ソリューションをサポートしています。

N1100	• N1108T-ON • N1108P-ON	• N1124T-ON • N1124P-ON	• N1148T-ON • N1148P-ON
N1500	• N1524 • N1524P	• N1548 • N1548P	
N2000	• N2024 • N2024P	• N2048 • N2048P	• N2128PX-ON
N3000	• N3024 • N3024P • N3024F	• N3048 • N3048P	• N3132PX-ON

顧客にとっての大きな問題の 1 つは、セキュリティ装置やスイッチなどの重要なネットワーク要素を個別に管理する必要があることです。Dell N シリーズ スイッチと Dell N シリーズ ソリューションにより、セキュリティ装置の管理インターフェースと GMS を使用して、セキュリティ装置と N シリーズ スイッチの両方を統合管理できます。TZ シリーズ装置で使用できるインターフェースの最大数は、5 (TZ300 の場合) ～ 10 (TZ600 の場合) です。ある種の配備では、TZ シリーズ装置上で使用可能なインターフェースの最大数を軽く超えるポート数が必要になる場合があります。Dell N シリーズ ソリューションでは、N シリーズ スイッチのポートをセキュリティ装置の拡張インターフェースと見なすことができるため、使用可能なインターフェースの数が増えます。

N シリーズ スイッチと N シリーズ ソリューションの基本的な違いの 1 つは、セキュリティ装置がスイッチをプログラムする方法です。

- N シリーズ ソリューションでは、セキュリティ装置がスイッチとの間で設定をプッシュ/取得するメカニズムとして XML API が使用されます。
- N シリーズ ソリューションでは、スイッチを設定し、スイッチから設定を取得するメカニズムとして CLI が使用されます。

TZ シリーズ、NSA シリーズ、および SM シリーズ プラットフォームでサポートされる N シリーズ ソリューションの機能は、これらのプラットフォームでサポートされる N シリーズ ソリューションの機能セットと同等であり、Dell X シリーズ スイッチ ソリューションに類似しています。最大で 4 台の N シリーズ スイッチがサポートされます。N シリーズと N シリーズ スイッチの両方が同じファイアウォールに統合されているシナリオでは、最大 4 つの N シリーズ + N シリーズ スイッチを組み合わせてサポートできます。N シリーズ スイッチのデイジーチェーン接続もサポートされています。

以下は、Dell Switch Integration Solution (Dell スイッチ統合ソリューション) の初期フェーズでサポートされる主要な機能セットです。

- 拡張スイッチとしての N シリーズ スイッチのプロビジョニング
- PortShield 機能
- N シリーズ スイッチのインターフェースの設定
- 基本的な N シリーズ スイッチのグローバル パラメータの管理性
- GMS を使用した拡張スイッチの管理性
- 高可用性と PortShield
- N シリーズ スイッチの診断サポート
- N シリーズ スイッチのデイジーチェーン接続

N シリーズ スイッチの設定

工場出荷時の N シリーズ スイッチには、既定で IP アドレスは設定されておらず、DHCP が有効になっています。例えば、N1524 スイッチを既定の設定で起動した場合:

```
console#show running-config

!Current Configuration:
!System Description "Dell Networking N1524, 6.2.5.3, Linux 3.6.5"
!System Software Version 6.2.5.3
!
configure
stack
member 1 1    ! N1524
exit
interface vlan 1
ip address dhcp
exit
snmp-server engineid local 800002a203f48e3807701e
exit

console#
```

N シリーズ スイッチの再起動後、Easy Setup Wizard を使用して初期セットアップを設定できます。このウィザードに従うと、初期のスイッチの設定を短時間で遂行してスイッチを起動できます。

メモ：`Ctrl Z` を入力すると、いつでもセットアップ ウィザードを終了できます。

ヒント：セットアップ ウィザードをスキップして、CLI モードに入り、スイッチを手動で設定することもできます。

重要：セットアップ ウィザードを実行するには、60 秒以内にこの質問に答える必要があります。

```
Would you like to run the setup wizard (you must answer this question within
60 seconds)? (y/n) y
```

それ以外の場合、システムは既定のシステム設定を使用して通常どおりの動作を続行します。空のスタートアップ設定でスイッチをリセットして、Dell Easy Setup Wizard を再実行します。

Dell Easy Setup Wizard を使用して N シリーズ スイッチを設定する方法については、ご使用のスイッチの『*Dell 導入ガイド*』を参照してください。

N シリーズ スイッチの、拡張スイッチとしてのプロビジョニング

メモ：PoE 関連のフィールドは、N シリーズ スイッチの PoE モデルでのみ設定可能です。

スタンドアロン TZ シリーズ システムでは、拡張スイッチのプロビジョニングは、次の拡張スイッチパラメータを指定します。

必須パラメータ		オプション パラメータ	
• ID	• ユーザ名	• ファイアウォール アップリンク	• PoE 使用量しきい値
• スイッチ モデル	• パスワード	• スイッチ アップリンク	• PoE 管理モード
• IP アドレス	• スイッチ管理	• STP モード	• PoE 検知種別
		• STP 状態	

高可用性が有効な TZ シリーズシ ステムでは、次の拡張スイッチ パラメータを指定することにより、拡張スイッチを追加できます。

必須パラメータ		オプション パラメータ	
• ID	• ユーザ名	• STP モード	• PoE 使用量しきい値
• スイッチ モデル	• パスワード	• STP 状態	• PoE 管理モード
• IP アドレス	• スイッチ管理		• PoE 検知種別

メモ：ファイアウォール アップリンクおよびスイッチ アップリンク パラメータは、高可用性モードで動作しているセキュリティ装置には関係ありません。現在、必須パラメータは設定後に変更できません。

アップリンク インターフェースの重要性

アップリンク インターフェースは、タグ付けされた / タグ付けされないトラフィックを伝送するように設定されたトランク ポートとして表示できます。拡張スイッチを追加する際にファイアウォール アップリンクと X スイッチ アップリンクのパラメータを使うと、ファイアウォール アップリンクとして設定されたセキュリティ装置のポートと、スイッチ アップリンクとして設定された拡張スイッチのポートが、すべての IDV VLAN についてタグ付けされたトラフィックを送受信するように自動的に設定されます。タグ付けされたトラフィックの IDV VLAN は、そのトラフィックに関して SonicOS が受信インターフェース、つまり portshield ホスト インターフェースを導き出すことができるようにします。

ファイアウォール アップリンクとして設定するインターフェースの要件:

- 物理インターフェースでなければなりません。仮想インターフェースは許可されません。
- スイッチ インターフェースである必要があります (一部のプラットフォームでは、セキュリティ装置の一部のインターフェースがスイッチに接続されません。そのようなインターフェースは除外されます)。
- PortShield ホストにすること (他のセキュリティ装置インターフェースをこのインターフェースから PortShield すること)、または PortShield メンバーにすること (他のセキュリティ装置インターフェースから PortShield されること) はできません。

- ブリッジ プライマリ インターフェースまたはブリッジ セカンダリ インターフェースであってはなりません。
- 子を持つことができません (他の子インターフェースの親インターフェースになることはできません)。

N シリーズ スイッチのプロビジョニング

N シリーズ スイッチをプロビジョニングするには:

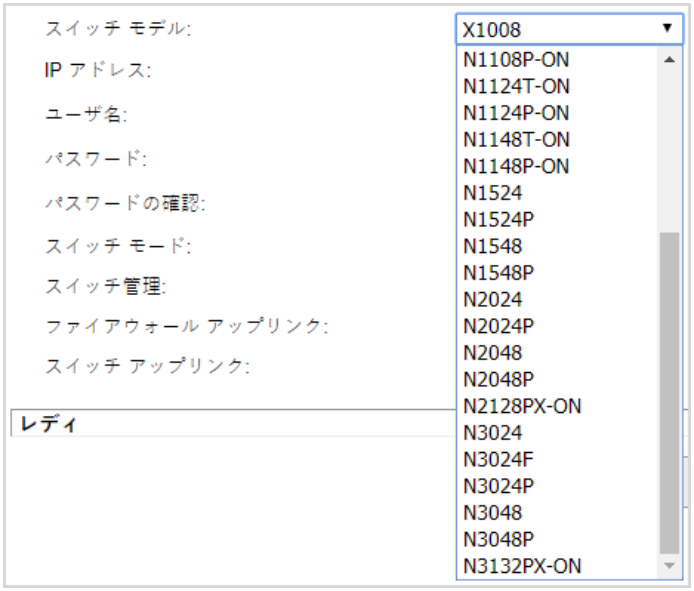
1 「**管理 | システム セットアップ > ネットワーク > PortShield グループ**」に移動します。

2 「**外部スイッチの設定**」を選択します。

3 「**スイッチの追加**」を選択します。「**外部スイッチの追加**」ダイアログが表示されます。

4 このスイッチの ID を「**ID**」から選択します。既定値は **1** です。

5 「スイッチ モデル」からスイッチの種別を選択します。



6 一般オプションの設定を完了します。

7 「**詳細**」を選択します。

8 詳細オプションの設定を完了します。

ⓘ | **メモ：**PoE オプションは、PoE N シリーズ スイッチに対してのみ表示されます。

9 「**追加**」を選択します。スイッチは「**外部スイッチの設定**」テーブルに追加されます。

PortShield での拡張スイッチの設定

拡張スイッチを設定するには:

1 「**管理 | システム セットアップ > ネットワーク > PortShield グループ**」に移動します。

2 「**ポート画像**」を選択します。

3 設定するポートを選択します。

4 「**設定**」を選択します。「**スイッチ ポートの編集**」ダイアログが表示されます。

5 すべてのオプションを設定します。

6 「**OK**」を選択します。

ポートの管理

重要：SOHO W セキュリティ装置は、X シリーズ リューションをサポートしていません。すべてのセキュリティ装置ポートは同様に管理されますが、「**管理 | システム セットアップ | ネットワーク > PortShield グループ**」についてはこれらのセキュリティ装置で違いがあります。「SOHO W ファイアウォールでのポートの管理 (397 ページ)」参照してください。

「**管理 | システム セットアップ | ネットワーク > PortShield グループ**」では、PortShield インターフェースへのポート割り当てを以下の方法で管理できます。

- **ポート画像**
- **ポート設定**
- **外部スイッチ設定**
- **外部スイッチ診断**

トピック:

- ポート画像でのインターフェース (ポート) の表示 (390 ページ)
- 「ポート設定」タブでの PortShield インターフェースの状況表示と編集 (392 ページ)
- 外部スイッチ設定の表示と管理 (394 ページ)
- 監視: 外部スイッチ診断とファームウェアの管理 (395 ページ)
- SOHO W ファイアウォールでのポートの管理 (397 ページ)

ポート画像でのインターフェース (ポート) の表示

「**ポート画像**」は、セキュリティ装置の PortShield インターフェース (ポート) を表示します。大きな図は、セキュリティ装置のインターフェースを表しています。各インターフェースは、その設定状況に応じて色分けされています。

インターフェース設定のカラー コード

色	表しているインターフェースの種別
黒	未定義、つまり PortShield グループに割り当てられていない
黄色	設定対象として選択されている
同じ色 (黒色、黄色、灰色を除く)	同じ PortShield グループに属し、その色が白色の枠線で囲まれているインターフェースがマスター インターフェース
灰色の淡色表示	割り当て不可、つまり PortShield グループに追加済み
灰色のインターフェースで人の形の図が付いているもの	スイッチ MGMT
上矢印が付いているもの (黒色、黄色、灰色を除く)	アップリンク

各ポートのグラフィックには対応するポート名X0 ～ X*n* が付いています。特定のインターフェースまたは複数のインターフェースを選択し、「PortShield グループの設定 (398 ページ)」の説明に従って設定できます。

拡張スイッチが設定されるタイミング

1 つ以上の拡張スイッチがプロビジョニングされると、「**ポート画像**」には、セキュリティ装置とそのスイッチの両方の PortShield インターフェース (ポート) が表示されます。

- 最初のグラフィックには、セキュリティ装置のポートが表示され、ラベルが付いていません。
- 次のグラフィックには、最初の外部スイッチ (外部スイッチ 1) のポートが表示されています。このスイッチは「***SwitchModel* 外部スイッチ 1**」 (例: X1018P 外部スイッチ 1) とラベル付けされています。
- 外部スイッチがさらにプロビジョニングされた場合、以降のグラフィックには、その他の外部スイッチのポートが ID 順に (外部スイッチ 2、外部スイッチ 3、外部スイッチ 4 のように) 表示されます。

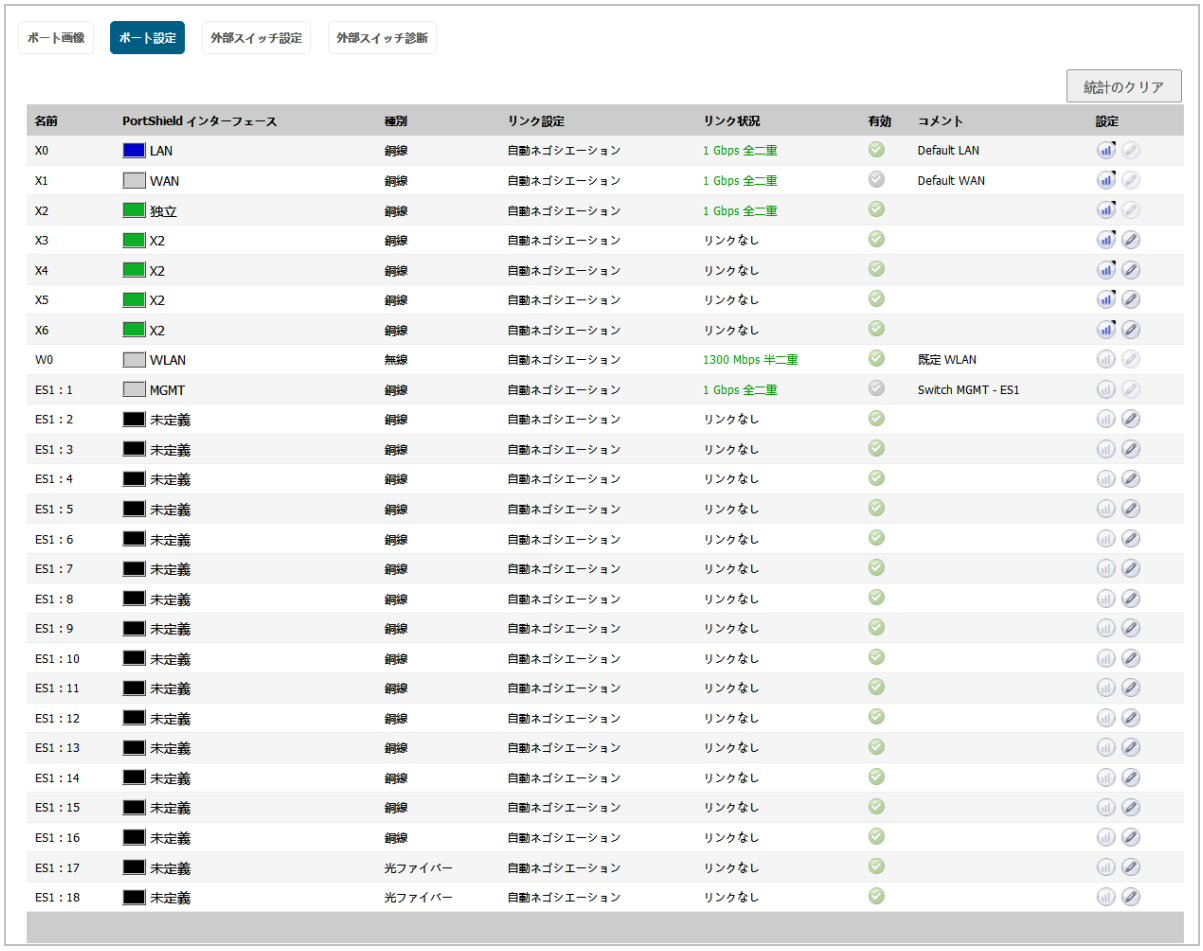
外部インターフェースのカラー コード付けは、セキュリティ装置の場合と同じです。「インターフェース設定のカラー コード」テーブルを参照してください。

「ポート設定」タブでの PortShield インターフェースの状況表示と編集

拡張スイッチなし

名前	PortShield インターフェース	種別	リンク設定	リンク状況	有効	コメント	設定
X0	LAN	銅線	自動ネゴシエーション	リンクなし		Default LAN	
X1	WAN	銅線	自動ネゴシエーション	1 Gbps 全二重		Default WAN	
X2	独立	銅線	自動ネゴシエーション	1 Gbps 全二重			
X3	未定義	銅線	自動ネゴシエーション	1 Gbps 全二重			
X4	未定義	銅線	自動ネゴシエーション	リンクなし			
X5	未定義	銅線	自動ネゴシエーション	リンクなし			
X6	未定義	銅線	自動ネゴシエーション	リンクなし			

拡張スイッチあり



名前	PortShield インターフェース	種別	リンク設定	リンク状況	有効	コメント	設定
X0	LAN	銅線	自動ネゴシエーション	1 Gbps 全二重		Default LAN	
X1	WAN	銅線	自動ネゴシエーション	1 Gbps 全二重		Default WAN	
X2	独立	銅線	自動ネゴシエーション	1 Gbps 全二重			
X3	X2	銅線	自動ネゴシエーション	リンクなし			
X4	X2	銅線	自動ネゴシエーション	リンクなし			
X5	X2	銅線	自動ネゴシエーション	リンクなし			
X6	X2	銅線	自動ネゴシエーション	リンクなし			
W0	WLAN	無線	自動ネゴシエーション	1300 Mbps 半二重		既定 WLAN	
ES1 : 1	MGMT	銅線	自動ネゴシエーション	1 Gbps 全二重		Switch MGMT - ES1	
ES1 : 2	未定義	銅線	自動ネゴシエーション	リンクなし			
ES1 : 3	未定義	銅線	自動ネゴシエーション	リンクなし			
ES1 : 4	未定義	銅線	自動ネゴシエーション	リンクなし			
ES1 : 5	未定義	銅線	自動ネゴシエーション	リンクなし			
ES1 : 6	未定義	銅線	自動ネゴシエーション	リンクなし			
ES1 : 7	未定義	銅線	自動ネゴシエーション	リンクなし			
ES1 : 8	未定義	銅線	自動ネゴシエーション	リンクなし			
ES1 : 9	未定義	銅線	自動ネゴシエーション	リンクなし			
ES1 : 10	未定義	銅線	自動ネゴシエーション	リンクなし			
ES1 : 11	未定義	銅線	自動ネゴシエーション	リンクなし			
ES1 : 12	未定義	銅線	自動ネゴシエーション	リンクなし			
ES1 : 13	未定義	銅線	自動ネゴシエーション	リンクなし			
ES1 : 14	未定義	銅線	自動ネゴシエーション	リンクなし			
ES1 : 15	未定義	銅線	自動ネゴシエーション	リンクなし			
ES1 : 16	未定義	銅線	自動ネゴシエーション	リンクなし			
ES1 : 17	未定義	光ファイバー	自動ネゴシエーション	リンクなし			
ES1 : 18	未定義	光ファイバー	自動ネゴシエーション	リンクなし			

「**ポート設定**」は、PortShield インターフェースに関する情報を一覧表示するテーブルで構成されています。

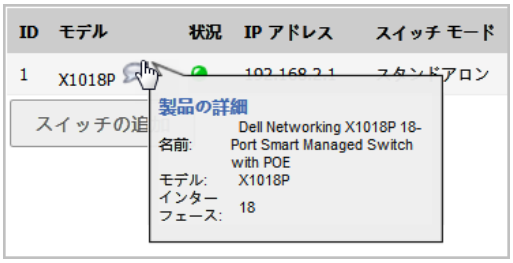
名前	PortShield インターフェースに関連付けられたポート名 (X0、X15 など)。すべての外部スイッチのポートが **ES*s*:*n*** の形式で表示されます。ここで、***s*** はスイッチ ID、***n*** はポート番号をそれぞれ表しています。
PortShield インターフェース	PortShield インターフェースの設定状況と所属 PortShield グループを表す色分けされたグラフィック。このグラフィックは、「**ポート画像**」にある大きな図の縮小版です。
種別	ポートの種別: • **銅線** • **無線**
リンク設定	リンク速度: • **自動ネゴシエート** • **1000Mbps - 全二重** • **100Mbps - 全二重** • **100Mbps - 半二重** • **10Mbps - 全二重** • **10Mbps - 半二重**
リンク状況	次のどちらかが表示されます。 • 現在のリンク速度 (緑色)。例: **1000Mbps - 全二重**。 • **接続されていません**。
有効	**有効**アイコンは色によって状態を示します。 • 緑色 (インターフェースが有効な場合)。 • 淡色表示の灰色 (インターフェースが無効になっている場合)
コメント	インターフェース設定時に入力されたコメント。
設定	次の 2 つのアイコンがあります。 • **統計** - 選択すると、インターフェースに関する統計を示すポップアップサマリが表示されます。  **メモ**：すべての統計を消去するには、「**ネットワーク > PortShield グループ > ポート設定**」の一番上にある「**統計のクリア**」を選択します。 • **編集** - 選択時、「**スイッチ ポートの編集**」ダイアログを表示します。このダイアログの詳細は、「「ネットワーク > PortShield グループ」での PortShield インターフェースの設定 (400 ページ)」の手順を参照してください。

外部スイッチ設定の表示と管理

メモ：外部スイッチがプロビジョニングされていない場合、このテーブルには「**登録がありません**」と表示されます。

ID
外部スイッチの ID 番号: **1**、**2**、**3**、または **4**。

モデル
拡張スイッチのモデル番号。この列には各スイッチの**コメント**アイコンもあります。このアイコンを選択すると、ポップアップ サマリで製品の詳細が表示されます。



状況
スイッチの状況: 緑色の「**有効**」アイコンは、スイッチが稼働していて使用可能であることを示します。

メモ：拡張スイッチの電源をオフにしてからセキュリティ装置を再起動 (リブート) した場合、セキュリティ装置が拡張スイッチを検出し、スイッチの「**状況**」を稼働中で使用可能と報告するまでに最大で 5 分かかります。

IP アドレス
拡張スイッチの IP アドレス。

スイッチ モード
スイッチのモード (**スタンドアロン**など)。

スイッチ管理
管理トラフィック用のスイッチ ポート。

ファイアウォール アップリンク
セキュリティ装置のアップリンクとして設定されたセキュリティ装置のポート。セキュリティ装置のアップリンクとして設定されたセキュリティ装置のポートが存在しない場合は、「**なし**」と表示されます。

スイッチ アップリンク
スイッチ アップリンクとして設定された拡張スイッチのポート。スイッチ アップリンクとして設定されたスイッチ ポートが存在しない場合は "**なし**" と表示されます。

親スイッチ ID
デイジーチェーン接続されたスイッチにとっての親スイッチの ID。親スイッチとして設定されたスイッチ ポートが存在しない場合、この列には "**該当なし**" と表示されます。

親スイッチ アップリンク
スイッチ アップリンクとして設定された、デイジーチェーン接続されている親スイッチのポート。親スイッチのアップリンクとして設定されたスイッチ ポートが存在しない場合は "**該当なし**" と表示されます。

設定
以下が含まれます。

- 「**編集**」アイコン - 選択すると、「**外部スイッチの編集**」ダイアログが表示されます。
- 「**削除**」アイコン - 選択すると、スイッチ エントリが削除されます。

「**外部スイッチ設定**」では、セキュリティ装置上でプロビジョニングされた外部スイッチに関する情報が提供され、そのスイッチを管理できます。拡張スイッチの設定や削除も行えます。拡張スイッチの設定については、「PortShield グループの設定 (398 ページ)」を参照してください。拡張スイッチの削除については、『*SonicWall X シリーズ ソリューション配備ガイド*』を参照してください。

監視: 外部スイッチ診断とファームウェアの管理

メモ：外部スイッチがプロビジョニングされていない場合、テーブルには「**登録がありません**」と表示されます。

「**外部スイッチ診断**」では、以下のことができます。

- 拡張スイッチに関する統計の監視
- ファームウェア イメージ、ブート イメージのアップロード
- 拡張スイッチの再起動

トピック:

- 表示の変更 (395 ページ)
- 統計の監視 (395 ページ)
- 外部スイッチの再起動 (396 ページ)
- 外部スイッチ ファームウェアの管理 (396 ページ)

表示の変更

「**外部スイッチ診断**」は、特定のスイッチに関する統計その他の情報を表示します (一度に表示されるのは 1 つのスイッチに関するもののみ)。既定では、外部スイッチ 1 (**ES1**) のデータが表示されます。2 台以上の外部スイッチがある場合、別の外部スイッチに関するデータを表示するには、「**スイッチ名**」で「**ES2**」、「**ES3**」、または「**ES4**」を選択します。

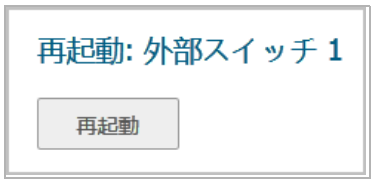
統計の監視

すべての統計の現在までの集計は「**統計**」テーブルに表示されます。統計の収集を最初からやり直す場合は、「**クリア**」を選択してカウンタをリセットします。

名前	ポート名 (1 ～ *n*)。
状況	ポートの状況 (「**稼働中**」または「**休止中**」)。
受信ユニキャスト パケット	ポートで受信したユニキャスト パケット数。
受信マルチキャスト パケット	ポートで受信したマルチキャスト パケット数。
受信ブロードキャスト パケット	ポートで受信したブロードキャスト パケット数。
受信バイト	ポートで受信したバイト数。
受信エラー	ポートで受信したエラー パケット数。
送信ユニキャスト パケット	ポートで送信したユニキャスト パケット数。

送信マルチキャスト パケット	ポートで送信したマルチキャスト パケット数。
送信ブロードキャスト パケット	ポートで送信したブロードキャスト パケット数。
送信バイト	ポートで送信したバイト数。
FCS エラー	ポートで受信した FCS (frame check sequence) エラー パケット数。
単一衝突フレーム	ポートで検出したフレーム衝突回数。
遅れ衝突	ポートで遅延フレーム ビット送信後に検出されたフレーム衝突回数。
過度の衝突	ポートで再試行回数を超えて検出されたフレーム衝突回数。
内部 MAC 送信エラー	ポートで検出された衝突以外の送信エラー数。
オーバーサイズ パケット	ポートで受信した、想定よりも大きなパケット数。
受信停止フレーム	ポートで受信した停止フレーム数。
送信停止フレーム	ポートで送信した停止フレーム数。

外部スイッチの再起動

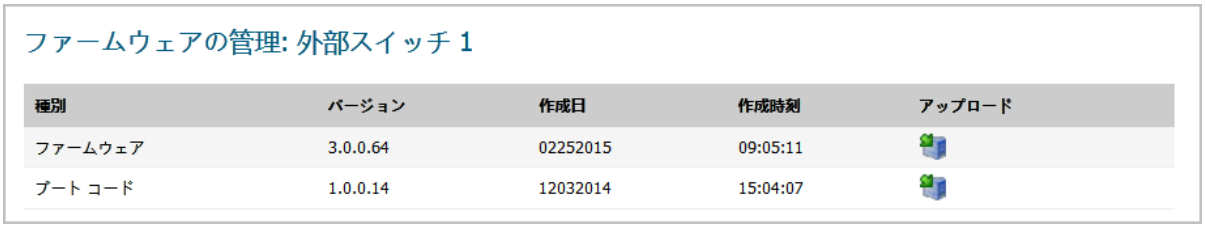


重要：拡張スイッチの電源をオフにしてからセキュリティ装置を再起動 (リブート) した場合、セキュリティ装置が拡張スイッチを検出し、スイッチの「**状況**」を「**接続**」と報告するまでに最大で 5 分かかります。

外部スイッチを再起動するには、以下の手順を実行します。

1. 「**管理 | システム セットアップ | ネットワーク > PortShield グループ**」に移動します。
2. 「**外部スイッチ診断**」を選択します。
3. 「**スイッチ名**」で、再起動する外部スイッチを選択します。
4. 「**再起動: 外部スイッチ 1**」セクションまでスクロールします。
5. 「**再起動**」を選択します。

外部スイッチ ファームウェアの管理

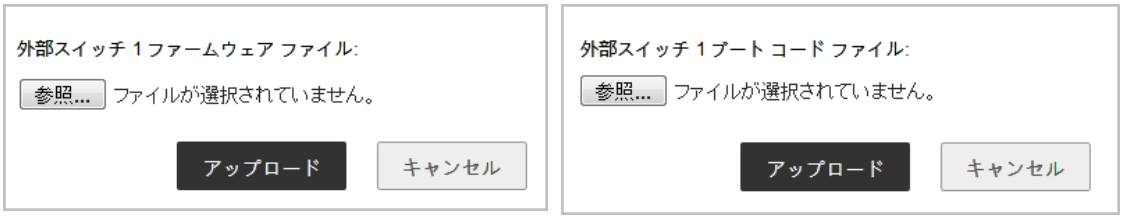


「**ファームウェア管理: 外部スイッチ 1**」テーブルは、外部スイッチのファームウェアおよびブートコードに関する情報を表示します。

種別	**ファームウェア**または**ブート コード**。
バージョン	外部スイッチのファームウェアまたはブート コードのバージョン。
作成日	ファームウェアまたはブート コードが作成された日付。
作成時刻	ファームウェアまたはブート コードが作成された時刻。
アップロード	**アップロード**アイコン。 • 「**ファームウェア**」の場合、「**外部スイッチ ファームウェアのアップロード**」ダイアログが表示されます。 • 「**ブート コード**」の場合、「**外部スイッチ ブート コードのアップロード**」ダイアログが表示されます。

ファームウェアまたはブート コードをアップロードするには、以下の手順を実行します。

1 **ファームウェア**または**ブート コード**の「**アップロード**」を選択します。「**外部スイッチ ファームウェアのアップロード**」または「**外部スイッチ ブート コードのアップロード**」ダイアログが表示されます。



2 「**参照**」を選択します。「**ファイルのアップロード**」ダイアログが表示されます。

3 ファイルを選択します。

4 「**アップロード**」をクリックします。

SOHO W ファイアウォールでのポートの管理

SOHO W セキュリティ装置の「**ネットワーク > PortShield グループ**」ページは外観が異なります。このページ上の情報は、「**ポート画像**」(「ポート画像でのインターフェース (ポート) の表示 (390 ページ)」を参照) および「**ポート設定**」(「「ポート設定」タブでの PortShield インターフェースの状況表示と編集 (392 ページ)」を参照) の情報を組み合わせたものです。

「PortShield グループの設定 (398 ページ)」の説明に従って、セキュリティ装置のインターフェースを設定します。

PortShield グループの設定

PortShield グループは、SonicOS 管理インターフェースのさまざまなページで設定できます。

- 「ネットワーク > インターフェース」での PortShield インターフェースの設定 (398 ページ)
- PortShield インターフェース ガイドによる PortShield インターフェースの設定 (TZ シリーズおよび SOHO W ファイアウォールのみ) (399 ページ)
- 「ネットワーク > PortShield グループ」での PortShield インターフェースの設定 (400 ページ)
- 「ポート画像」からの外部スイッチ PortShield グループの設定 (402 ページ)

「ネットワーク > インターフェース」での PortShield インターフェースの設定

重要：インターフェースとするポートには IP アドレスを設定してください。設定しないと、そのポートは「**PortShield インターフェース**」に表示されません。

PortShield インターフェースを設定するには、以下の手順に従います。

1 「**管理 | システム セットアップ | ネットワーク > インターフェース**」に移動します。

2 「**インターフェース設定**」テーブルで、設定するインターフェースの**設定**アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。

3 「**ゾーン**」で、インターフェースを割り付けるゾーン種別オプションを選択します。追加のオプションが表示されます。

メモ：PortShield インターフェースを追加できるのは、**保護**ゾーン、**公開**ゾーン、および**無線**ゾーンのみです。

4 「**モード/IP 割り当て**」ドロップダウン メニューで、「**PortShield スイッチ モード**」を選択します。再びオプションが変化します。

5 「**PortShield 先**」で、このポートを割り付けるインターフェースを選択します。選択したゾーンと一致するポートのみが表示されます。

6 「**OK**」を選択します。

PortShield インターフェース ガイドによる PortShield インターフェースの設定 (TZ シリーズおよび SOHO W ファイアウォールのみ)

『*SonicOS クイック設定ガイド*』の説明に従って、PortShield インターフェースを PortShield インターフェース ガイドによって設定できます。PortShield インターフェース ガイドには、次のようにしてアクセスできます。

- 管理インターフェースの任意のページで「**クイック設定ガイド**」を選択します。「**設定ガイド**」が表示されるので、「**PortShield インターフェース ガイド**」を選択します。
- TZ シリーズまたは SOHO W セキュリティ装置の「**管理 | システム セットアップ | ネットワーク > インターフェース**」ページで、「**PORTSHIELD ウィ ザード**」を選択して「**PortShield インターフェース ガイド**」を表示します。

「ネットワーク > PortShield グループ」での PortShield インターフェースの設定

「**ポート画像**」には、PortShield インターフェースの現在の設定を視覚的に表したものが表示されます。グラフィック表示の説明については、「ポート画像でのインターフェース (ポート) の表示 (390 ページ)」を参照してください。

この **PortShield グループ**のグラフィック インターフェースを使用すると、グループ化したいポートを選択することにより、ポートを手動でグループ化できます。ポートをグループ化すると、それらのポートで共通のネットワーク サブネットおよび共通のゾーン設定を共有できます。

メモ：インターフェースを PortShield でグループ化するには、その前にインターフェースを設定しておいてください。

PortShield グループを設定するには、以下の手順を実行します。

1 ポート グラフィックで、PortShield グループに含めたいインターフェースを選択します。選択したインターフェースの色が黄色に変わります。

2 「**設定**」を選択します。「**スイッチ ポートの編集**」ダイアログが表示されます。

メモ：このポートのインターフェースの名前は、淡色表示になり、変更できなくなります。

3 「**ポートの有効化**」で、そのインターフェースを有効にするか無効にするかを選択します。既定は「**有効**」です。

4 「**PortShield インターフェース**」で、この PortShield インターフェースのマスター インターフェースとして割り当てるインターフェースを選択します。既定は「**未定義**」です。

メモ：外部スイッチ ポートでは Portshield オプションが無効になることがあります。

5 「**リンク速度**」で、そのインターフェースのリンク速度を選択します。

- **自動ネゴシエーション** (既定)
- **1000Mbps - 全二重**
- **100Mbps - 全二重**
- **100Mbps - 半二重**
- **10Mbps - 全二重**
- **10Mbps - 半二重**

6 「**OK**」を選択します。

「ポート画像」からの外部スイッチ PortShield グループの設定

重要：拡張スイッチの電源をオフにしてからセキュリティ装置を再起動 (リブート) した場合、セキュリティ装置が拡張スイッチを検出し、スイッチの「**状況**」を「**接続**」と報告するまでに最大で 5 分かかります。

拡張スイッチを PortShield グループに設定すると、この設定が「**ネットワーク > PortShield グループ**」に表示されるまで最大で 5 分かかります。

重要：インターフェースを PortShield でグループ化するには、その前にインターフェースを設定しておいてください。

メモ：さまざまなトポロジでの PortShield グループの設定方法については、『*SonicWall X シリーズ ソリューション配備ガイド*』を参照してください。

メモ：拡張スイッチは、SOHO W セキュリティ装置ではサポートされません。

「**ネットワーク > PortShield グループ**」には、セキュリティ装置および拡張 (外部) スイッチの PortShield インターフェースの現在の設定がグラフィック表現で表示されます。外部スイッチが 1 台ならグラフィックは 2 つ、外部スイッチが 2 台ならグラフィックは 3 つ、というように表示されます。各スイッチのグラフィックには、スイッチのモデルと外部スイッチ ID (1、2、3、4) が表示されます。

この PortShield グループのグラフィック インターフェースでは、グループ化したいポートを選択することにより、セキュリティ装置およびスイッチのポートを手動で一緒にグループ化できます。ポートをグループ化すると、それらのポートで共通のネットワーク サブネットおよび共通のゾーン設定を共有できます。

外部スイッチで PortShield グループを設定するには、以下の手順を実行します。

1. 「「ネットワーク > PortShield グループ」での PortShield インターフェースの設定 (400 ページ)」の手順に従って、セキュリティ装置のポートを設定します。
2. 外部スイッチのポート グラフィック内で、PortShield グループに含めたいインターフェースを選択します。選択したインターフェースの色が黄色に変わります。
3. 「**設定**」を選択します。「**複数のスイッチ ポートを編集する**」ダイアログが表示されます。

「**名前**」フィールドは淡色表示で、変更できません。ここには両方のセキュリティ装置の名前と、選択した外部スイッチのポートが表示されます (*n* は選択したポート)。

- ファイアウォールのポートの名前は、**X*n*** となっています。
- 外部スイッチ 1 のポートは、**ES1 : *n*** という名前になります。

- 外部スイッチ 2 のポートは、**ES2 : *n*** という名前になります。
- 外部スイッチ 3 のポートは、**ES3 : *n*** という名前になります。
- 外部スイッチ 4 のポートは、**ES4 : *n*** という名前になります。

4 「**ポートの有効化**」で以下の選択を行います。

- **無効**
- **有効**
- **--現在の設定を保持する--** (既定) - 既定では、拡張スイッチのすべてのポートが有効になります。

5 「**PortShield インターフェース**」で、これらの PortShield インターフェースのマスター インターフェースとして割り当てるインターフェースを選択します。

- **未定義**
- ポート名

  重要：インターフェースとするポートには IP アドレスを設定してください。設定しないと、そのポートは「**PortShield インターフェース**」に表示されません。

- **--現在の設定を保持する--** (既定)

  メモ：外部スイッチ ポートでは Portshield オプションが無効になることがあります。ここで PortShield したポートは、対応する PortShield VLAN の VLAN にアクセスしたとき自動的に設定されます。

6 「**リンク速度**」で、そのインターフェースのリンク速度を選択します。

- **自動ネゴシエート**
- **1000Mbps - 全二重**
- **100Mbps - 全二重**
- **100Mbps - 半二重**
- **10Mbps - 全二重**
- **10Mbps - 半二重**
- **--現在の設定を保持する--** (既定) - 既定では、拡張スイッチのすべてのポートのリンク速度は、**自動ネゴシエーション**に設定されます。

7 「**OK**」を選択します。

15

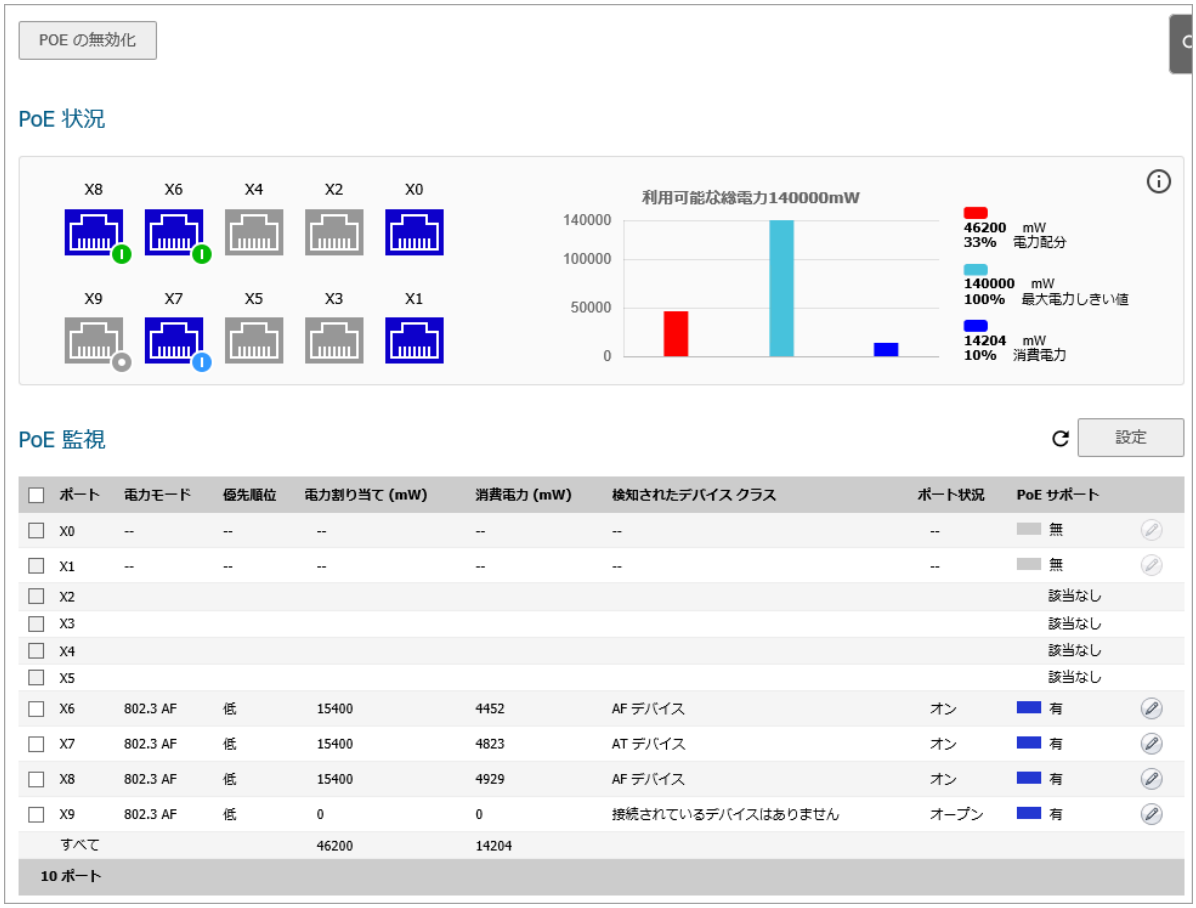
PoE の設定

重要：TZ600P および TZ300P ファイアウォールのみが「**管理 | システム セットアップ** > **ネットワーク** > **PoE 設定**」ページを表示します。

トピック:

- ネットワーク > PoE 設定 (404 ページ)
  - PoE の有効化 (405 ページ)
  - 標準 PoE 設定を構成する (407 ページ)
  - PoE の有効化 (405 ページ)

ネットワーク > PoE 設定



「**管理 | システム セットアップ > ネットワーク > PoE 設定**」ページは、以下の設定や監視を行うための使いやすい一元化されたダッシュボードを提供します。

- 全体の消費電力
- PoE コントローラ全体または個々のポートを有効/無効にする
- 個々のポートの電力しきい値を設定する
- 電力モード (802.3 AT または 802.3 AF) を設定する
- 電源優先度を設定する
- 複数のポートを同時に変更する

トピック:

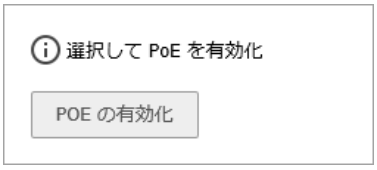
- PoE の有効化 (405 ページ)
- 標準 PoE 設定を構成する (407 ページ)

PoE の有効化

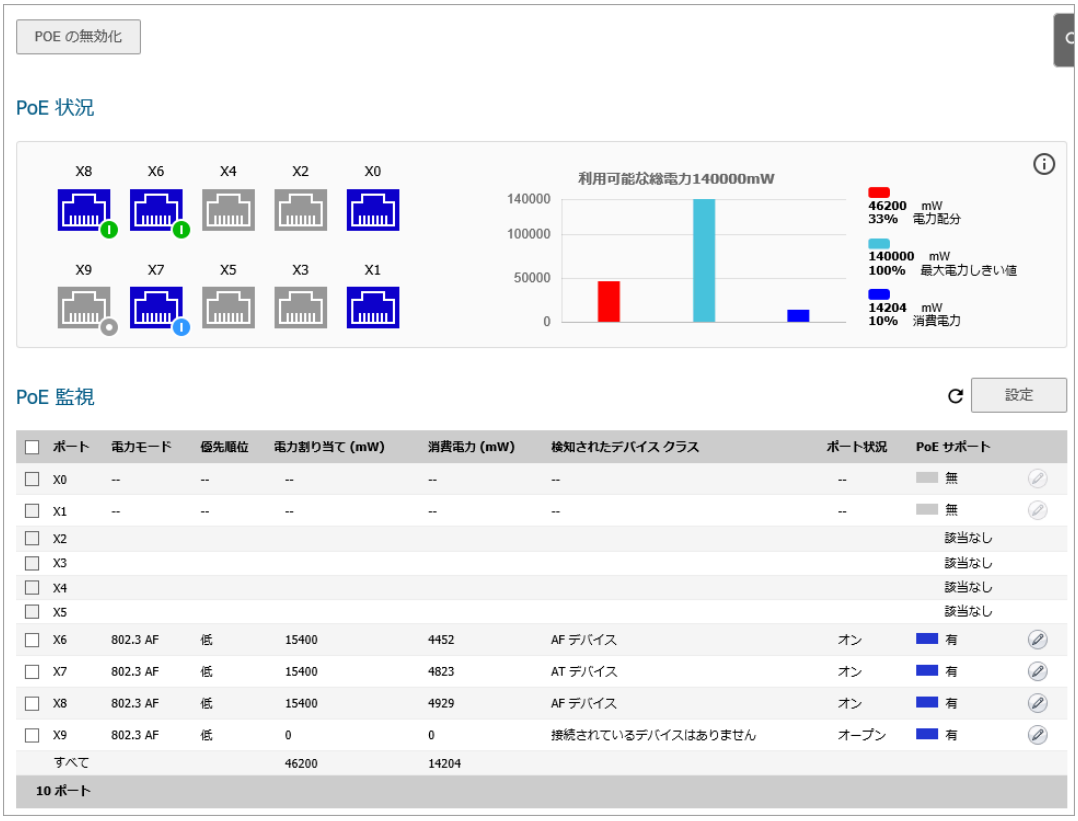
PoE を TZ600P/TZ300P セキュリティ装置で使用する場合は、その前に有効化してください。

セキュリティ装置で PoE を有効にするには:

1 「**管理 | システム セットアップ > ネットワーク > PoE 設定**」に移動します。



2 「**PoE の有効化**」を選択します。ページが展開されます。

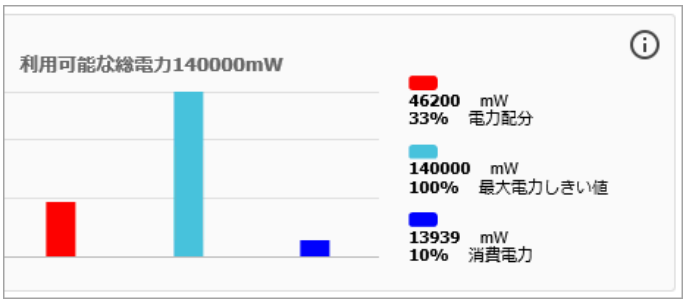


「**ネットワーク > PoE 設定**」ページには 2 つのセクションがあります。

- **PoE 状況** - グラフィックスによる可視化のために以下を表示します。
  - 状況インジケーター。PoE の各インターフェース (ポート) の状況が丸アイコンとさまざまな色で示されます。

これらのポートは、「**PoE 監視**」テーブルにも表示されます。

- リアルタイムの電力消費モニター。使用可能な総電力、最大電力しきい値の割合、および消費電力の割合を示します。



情報アイコンを選択すると、ポートに関する詳細な情報が表示されます。

- **PoE 監視** - ポートを一覧表示し、各ポートについて、電力モード、優先度、電力割り当て(mW)、消費電力、PoE サポートの有無、および PoE ポートの「**編集**」アイコンを示します。

標準 PoE 設定を構成する

ポートの一般 PoE 設定を構成するには:

1 「**管理 | システム セットアップ > ネットワーク > PoE 設定**」に移動します。

2 「**PoE 監視**」セクションまでスクロールします。

3 「**設定**」を選択します。「**PoE システム設定**」ダイアログが表示されます。

4 PoE を有効にするには、「**PoE を有効にする**」を選択します。

5 「**最大電力しきい値**」フィールドに最大電力しきい値の割合を指定します。

6 「**OK**」を選択します。

ポートの電力設定の構成

ポートの電力設定を構成するには:

1 「**管理 | システム セットアップ > ネットワーク > PoE 設定**」に移動します。

2 「**PoE 監視**」セクションまでスクロールします。

3 電源設定を構成するポートを選択します。

4 ポートの「**編集**」アイコンを選択します。「**PoE ポート設定**」ダイアログが表示されます。

5 ポートの電源を有効にするには、「**電源有効**」を選択します。このオプションは、既定では選択されています。

6 「**電力モード**」オプションから電力モードを選択します。

- **802.3 AT** (既定)
- **802.3 AF**

7 「**電力優先順位レベル**」オプションからポートの優先度を選択します。

- **高い**
- **低** (既定)

8 「**OK**」を選択します。

16

フェイルオーバーと負荷分散の セットアップ

トピック:

- ネットワーク > フェイルオーバーと負荷分散 (409 ページ)
  - フェイルオーバーと負荷分散について (409 ページ)
  - フェイルオーバーと負荷分散のしくみ (410 ページ)
  - 複数 WAN (MWAN) (411 ページ)
  - ネットワーク > フェイルオーバーと負荷分散 (412 ページ)
  - フェイルオーバーと LB グループの設定 (415 ページ)
  - グループ メンバーの監視設定の構成 (420 ページ)

ネットワーク > フェイルオーバーと負荷分散

トピック:

- フェイルオーバーと負荷分散について (409 ページ)
- フェイルオーバーと負荷分散のしくみ (410 ページ)
- 複数 WAN (MWAN) (411 ページ)
- ネットワーク > フェイルオーバーと負荷分散 (412 ページ)
- フェイルオーバーと LB グループの設定 (415 ページ)
- グループ メンバーの監視設定の構成 (420 ページ)

フェイルオーバーと負荷分散について

フェイルオーバーと負荷分散 (LB) (この 2 つをまとめて、FLB) は、WAN 接続を能動的に監視し、各 WAN インターフェースで障害が発生したときや障害から復旧したときに適切な動作を保つしくみです。この全体効果により、個々の WAN 接続が故障または復旧してもシステム全体としての対応が可能です。使用する WAN が 1 つだけの場合にもメリットがあります。FLB の通常の処理の中でその 1 つの WAN に対して、より高速な復旧プロシージャが実行されるからです (使用する WAN が 1 だけの場合の FLB の詳細については、ナレッジ ベースの記事「*ファイアウォール上で使用する WAN が 1 つだけの場合にグローバル負荷分散を無効にできるか?*」 (SW13851) を参照してください)。要するに、FLB は可用性の高いシステムを実現します。

FLB では、ハードウェア プラットフォームのインターフェースの総数を *N* とすると、*N*-1 個の WAN メンバーがサポートされます。以下に例を示します。

- プライマリ WANイーサネット インターフェース
- バックアップWAN #1
- バックアップWAN #2
- バックアップ WAN #<*n-1*> ...

重要：使用する WAN が 1 つだけの場合にも負荷分散を常に有効にすることを推奨します。詳細は、「*ファイアウォール上で使用する WAN が 1 つだけの場合にグローバル負荷分散を無効にできるか?*」(SW13851) を参照してください。

プライマリ WAN イーサネット インターフェースは、以前の "プライマリ WAN" という概念と同じものです。これは、LB グループの中で最も順位が高い WAN インターフェースです。**バックアップ WAN #1** は "セカンダリ WAN" に対応します。この階級すなわち順位はプライマリ WAN より下ですが、次の 2 つのバックアップ WAN より上です。**それ以外のバックアップ WAN #2** と**バックアップ WAN #<*n-1*>** は新しく追加されたもので、**バックアップ WAN #<*n-1*>** の順位は LB グループの 4 つの WAN メンバーの中で最も下です。

フェイルオーバーと負荷分散のしくみ

トピック:

- WAN インターフェースの障害 (410 ページ)
- WAN インターフェースの復旧 (411 ページ)

WAN インターフェースの障害

WAN インターフェースの障害 (リンク ダウン、監視失敗、IP 設定なし) が検出されると、以下の処理が行われます。

1. インターフェースの正規シャットダウン (用意されていれば、pppoe-stop、dialup-stop などの stop API を呼び出す)。
2. 故障したインターフェースに関連付けられているルートの無効化を開始する (ただし、「リンクダウン時も無効にしない」と指示されたルートは除く)。
3. 故障したインターフェースを使用していた動的 ARP エントリを消去する。
4. 故障したインターフェースを発信インターフェースとして使用していたキャッシュ エントリを消去する。
5. バックアップ WAN に接続する WAN デフォルト ルートがあれば更新する。状況データを更新する (復旧プロシージャの中で実行)。
    - 他のアプリケーション (CASS など) で使われているアドレス オブジェクトも更新される。
    - セキュリティ サービスのフェイルオーバー機能はこれに依存する。
6. 関係するサービス (VPN、BWM、CASS、DDNS、DNS) に通知する。
7. 故障したインターフェースの状況を能動的に監視し、WAN 接続の再起動などの復旧を試みる (用意されていれば、pppoe-start、dial-start などの start API を呼び出す)。

WAN インターフェースの復旧

WAN インターフェースの復旧 (リンク アップ、監視成功、IP 変更) が検出されると、以下の処理が行われます。

1 リンク アップ時、インターフェース接続をジャンプスタートする (用意されていれば、pppoe-start、dial-startcall などの start API を呼び出す)。ほとんどの場合は既に接続状態となっているが、そうでなければ、FLB が接続開始を試みる。ハング状態を検出すると (タイマをかけて所定の時間内に応答がない場合)、正規シャットダウン後に再起動されることもある。

2 接続確立 (無条件のリンク アップまたは監視成功) が確認されると、インターフェースに関連付けられているルートの有効化を開始する。

3 ARP エントリ (必要とされる場合) を追加する。

- 一方的な (要求に対応したものでない) ARP 応答を送出して近隣のデバイスを更新する。

4 必要なら (先制モードの場合など)、WAN デフォルト ルートを更新して最も可用性の高い WAN を使用する。状況データを更新する。

- 他のアプリケーション (CASS など) で使われているアドレス オブジェクトも更新される。
- セキュリティ サービスのフェイルオーバー機能はこれに依存する。

5 関係するサービス (VPN、BWM、CASS、DDNS、DNS) に通知する。

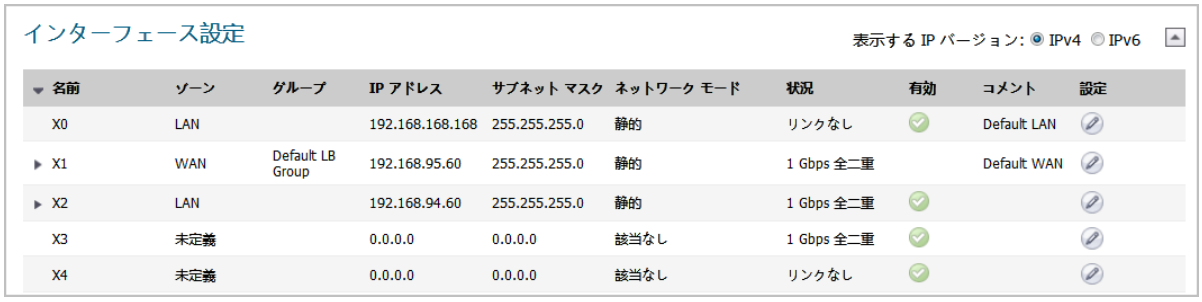
6 インターフェースの状況監視を継続する。

複数 WAN (MWAN)

複数 WAN (MWAN) 機能を使用すると、装置のインターフェースのうち、1 つを除くすべてのインターフェースを WAN ネットワーク ルーティング用に設定できます (LAN ゾーンのローカル管理用に 1 つのインターフェースを残しておく必要があります)。WAN インターフェースはすべて、SNWL グローバル レスポンダ ホストを使用して論理監視することができます。

ネットワーク インターフェース

「**管理 | ネットワーク > インターフェース**」で、3 つ以上の WAN インターフェースのルーティング設定を行うことができます。WAN インターフェースを「**ネットワーク > インターフェース**」で設定しても「**ネットワーク > フェイルオーバーと負荷分散**」に含まれることはありません。LB が有効になっている場合は常に、プライマリ WANイーサネット インターフェースのみを LB グループに含める必要があります。LB グループに属していない WAN インターフェースは LB 機能には含まれませんが、通常の WAN ルーティング機能を実行します。



メモ：仮想 WAN インターフェースは、LB グループに属することができます。ただし、LB グループ内で使用する前に、仮想 WAN ネットワークが物理 WAN のように完全にルーティング可能であることを確認してください。

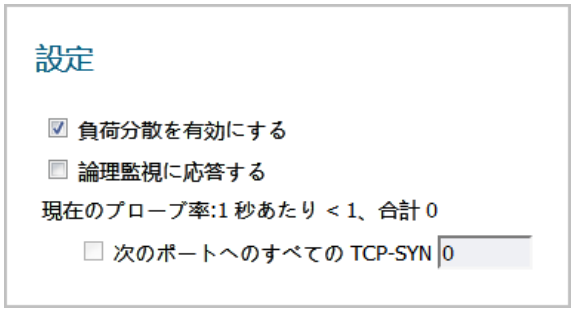
WAN サブネットの IP アドレス空間に属さない WAN インターフェース経由で送信先に到達する必要がある場合は、WAN サブネット上のピア装置のルーティング プロトコルから既定のルートを動的に受信しているかどうかにかかわらず、WAN インターフェースにデフォルト ゲートウェイの IP アドレスを指定する必要があります。

ネットワーク > フェイルオーバーと負荷分散

トピック:

- 設定 (413 ページ)
- グループ (413 ページ)
- 統計 (414 ページ)

設定



- **負荷分散を有効にする** - ユーザがフェイルオーバーと負荷分散設定の LB グループと LB 統計のセクションにアクセスするためには、このオプションを有効にする必要があります。これが無効になっていると、フェイルオーバーと負荷分散に関するオプションを設定することはできません。このオプションは既定で有効です。

  重要：使用する WAN が 1 つだけの場合にも負荷分散を常に有効にすることを推奨します。詳細は、「*ファイアウォール上で使用する WAN が 1 つだけの場合にグローバル負荷分散を無効にできるか?*」(SW13851) を参照してください。

- **論理監視に応答する** - これを有効にすると、装置が自らのインターフェースのいずれかに着信したプローブ要求パケットに応答できます。このオプションは、既定では選択されていません。

  現在のプローブ率とプローブの総数が表示されます。

  - **次のポートへのすべての TCP-SYN** -「**論理監視に応答する**」オプションが有効になっている場合、このオプションを使用できます。このオプションを選択すると、装置は設定値と同じ送信先アドレス TCP ポート番号を持つ TCP プローブ要求パケットにのみ応答します。このオプションは、既定では選択されていません。

グループ

LB グループに追加された LB メンバーは、ある一定の「役割」を果たします。各メンバーは次に示す役割のうちの 1 つだけを果たします。

- **プライマリ** - プライマリにできるメンバーはグループごとに 1 つだけです。このメンバーは常にメンバー リストの先頭に表示されます。

  メモ：グループを設定するときに空のメンバー リストを使用してもかまいませんが、プライマリ メンバーは常に必要です。

- **バックアップ** - 複数のメンバーをバックアップとして設定できますが、バックアップ メンバーだけのグループは存在できません。
- **最後の手段** - 最後の手段として指定できるメンバーは 1 つだけです。最後の手段を設定するときは、グループの他のメンバーと共に設定する必要があります。

グループの各メンバーには順位があります。メンバーは順位の高い順に表示されます。順位は、インターフェースがグループのメンバー リストに表示される順序によって決定されます。この順序は、インターフェースの使用優先度およびグループ内での優先度を決定するときに重要になります。そのため、グループ内で 2 つのインターフェースが同じ順位を持つことはなく、インターフェースごとに異なる順位を持ちます。

「グループ」テーブル

- 「**展開/折りたたみ**」アイコン - 選択すると、メンバーを含むグループが展開または折りたたまれます。
- **名前** - これでグループを選択します。既定のグループは選択できません。
- **種別** - フェイルオーバーの種類。メンバーではなくグループにのみ適用されます。
- **IP アドレス** - グループ メンバーの IP アドレス。
- **リンク状況** - リンクの状況 (リンク アップまたはリンク ダウン) が表示されます。
- **LB 状況** - 負荷分散の状況が表示されます。
- **メイン ターゲット** - メイン ターゲットが監視中かどうかが表示されます。
- **バックアップ ターゲット** - バックアップ ターゲットが監視中かどうかが表示されます。
- **設定** - 「**編集**」アイコンと、さらにグループでは「**削除**」アイコンが表示されます (既定のグループは削除できないので、「**削除**」アイコンは淡色表示になります)。
- **補足** - 「**メモ**」アイコンが表示されます。その上にカーソルを置くと、ポップアップ バルーンにグループの状況が表示されます。

統計

「**次の統計を表示する**」ドロップダウン メニューから、統計情報を表示したい LB グループを選択します。

負荷分散「**統計**」テーブルには、ファイアウォールに関する次の LB グループ統計情報が表示されます。

- インターフェース -
- 接続の総数 -
- 新規接続数 -

- 現在比率 -
- 平均比率 -
- ユニキャスト合計バイト -
- 受信ユニキャスト -
- 受信バイト -
- 送信ユニキャスト -
- 送信バイト -
- スループット (KB/秒) -
- スループット (Kbits/秒) -

統計情報を消去するには、「**統計**」テーブルの右上にある「**クリア**」を選択します。

フェイルオーバーと LB グループの設定

トピック:

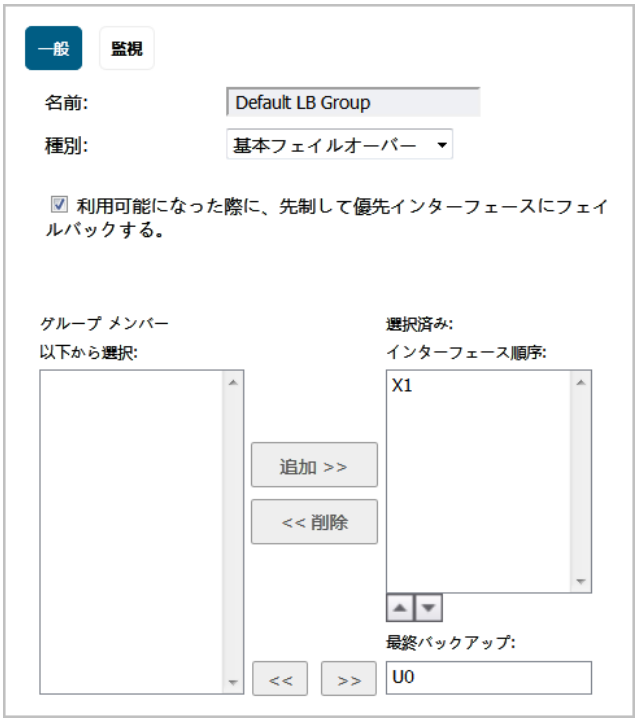
- 一般設定 (415 ページ)
- 監視設定 (418 ページ)

一般設定

グループ設定を構成するには、以下の手順を実行します。

1 「**管理 | ネットワーク > フェイルオーバーと負荷分散**」に移動します。

2 設定するグループの**設定**アイコンを選択します。「**LB グループの修正**」ダイアログが表示されます。



3 「**名前**」フィールドで、グループの表示名を編集します。既定のグループの名前は変更できないので、そのフィールドは淡色表示になっています。

4 「**種別**」ドロップダウン メニューから、LB の種類 (すなわち方式) を選択します。オプションは選択した種別に応じて変化します。

- **基本フェイルオーバー** -「**利用可能になった際に、先制して優先インターフェースにフェイルバックする**」チェックボックスが選択されている場合、4 つの WAN インターフェースが順位を使用して優先順序を決定します。アクティブな WAN インターフェースに優先することができるのは、より高い順位のインターフェースのみです。これは、既定で選択されています。
- **ラウンドロビン** - ラウンド ロビン方式で選択する WAN インターフェースの順序を変更できるようになりました。既定の順序は次のとおりです。
  - プライマリ WAN
  - バックアップWAN #1
  - バックアップWAN #2
  - バックアップWAN #3

  その後、プライマリ WAN に戻ってこの順序が繰り返されます。
- **使用帯域** - 帯域幅のしきい値がプライマリ WAN に適用されます。しきい値を超えると、新しいトラフィック フローはラウンド ロビン方式でバックアップ WAN に割り当てられます。プライマリ WAN の帯域幅が設定済みしきい値を下回ると、ラウンド ロビンは停止し、新しい送信フローは再びプライマリ WAN のみを介して送信されるようになります。

  メモ：現存するフローは (既にキャッシュされているので) 正常にタイムアウトするまではバックアップ WAN に関連付けられたままになります。

- **使用比率** - LB グループの WAN ごとに比率を設定できます。設定エラー関連の問題を回避するために、比率と WAN インターフェースが正しく対応していることを確認してください。

5 「**種別**」ドロップダウン メニューから選択した内容に応じて、以下のオプションのいずれかが表示されます。

選択した種別	オプション
基本フェイルオーバー	**利用可能になった際に、先制して優先インターフェースにフェイルバックする。** このオプションを選択すると、先制の順序を決める階級すなわち順位が有効になります。既定で選択されています。

選択した種別	オプション
スピルオーバー	**帯域幅が *プライマリ インターフェースの帯域幅制限* (Kbits/秒) *を超えると*、新しいフローはラウンド ロビン方式でバックアップ グループ メンバーに向けられる。** このフィールドでプライマリ インターフェースの帯域幅を指定します。この値を超えた場合、新しいフローは「**選択済み**」列の表示順序に従ってバックアップ グループ メンバーに送信されます。 既定値は **0** です。
ラウンド ロビン、使用帯域、使用比率	**送信元と送信先 IP アドレス バインディングを使う。** このオプションは、HTTP/HTTPS リダイレクトを使用している場合などに特に便利です。例えば、接続 A と接続 B が同じ WAN インターフェース上に存在する必要があり、接続 A での送信元および送信先 IP アドレスが接続 B のものと同じであるが、異なるサービスが使用されている場合などです。この場合、トランザクションがエラーにならないように同じ WAN インターフェース上で両方の接続を維持するために、送信元および送信先の IP アドレスのバインドが必要です。 このオプションは、既定では選択されていません。

6 メンバー インターフェースの追加、削除、並べ替えを「**グループ メンバー**」、「**以下から選択**」、「**選択済み**」の各リストで行います。「**選択済み**」リストの選択済みメンバーの用途は、選択した**種別**によって異なります。

- **基本フェイルオーバー: インターフェース順序:**
- **ラウンド ロビン: インターフェース プール:**
- **使用帯域: プライマリ/バックアッププール:**
- **使用比率: インターフェース分配:**

7 メンバーを追加するには、「**グループ メンバー:**」列に表示されるインターフェースを選択し、「**追加>>**」を選択します。

8 「**選択済み**」列のエントリの順序を並べ替えるには、次の操作を行います。

a 特定のエントリを選択する。

b 「**上/下矢印**」を選択します。

9 「**使用比率**」を選択した場合は、エントリを並べ替える代わりに、各インターフェースの比率を指定できます。「使用比率による帯域幅の設定 (418 ページ)」を参照してください。

重要：設定エラー関連の問題を回避するために、比率と WAN インターフェースが正しく対応していることを確認してください。

10 インターフェースに割り当てる帯域幅の比率を「パーセント (%)」フィールドに入力します。すべてのインターフェースの帯域幅の合計が 100% となるようにしてください。割り当てた帯域幅の合計パーセントが表示されます。

11 比率を変更するには、「**比率の変更**」を選択するか、「**自動調整**」を選択して比率を自動調整します。

12 「**選択済み**」列のメンバーを削除するには、次の操作を行います。

a 表示されたインターフェースを選択する。

b 「**<<削除**」を選択します。

メモ：リストの先頭に表示されるインターフェースがプライマリです。

個々のメンバーに対して実行される処理はインターフェースの順位では決まりません。実行される処理は、グループ種別で指定されます。

13 必要に応じて、次の設定を入力します。

- **最終バックアップ** - この設定のエントリは "最終手段" のインターフェースです。つまり、「**選択済み:**」グループの他のインターフェースがすべて利用不可の場合にのみ使用されるインターフェースです。最終バックアップ インターフェースを指定するには、「グループ メンバー」リストでエントリを選択し、二重右矢印を選択します。**最終バックアップ** インターフェースを削除するには、二重左矢印を選択します。

14 「**OK**」を選択します。

使用比率による帯域幅の設定

「**使用比率**」を選択した場合は、「**追加 >>**」の代わりに「パーセント (%)」フィールドと「**二重右矢印**」が表示され、「**上/下矢印**」の代わりに「**自動調整**」が表示されます。

インターフェースに割り当てる帯域幅の比率を入力します。割り当てた帯域幅の合計パーセントが表示されます。

重要：設定エラー関連の問題を回避するために、比率と WAN インターフェースが正しく対応していることを確認してください。

複数のインターフェースを選択した場合は、次のどちらかの操作を行えます。

- 「**自動調整**」を選択して各インターフェースに帯域幅を均等に割り当てる。
- 各インターフェースに割り当てる帯域幅の比率を入力する。

インターフェースの帯域幅の比率を変更するには、次の手順を実行します。

1 「**選択済み**」列でインターフェースを選択します。

2 「**比率の変更**」を選択します。

3 「パーセント (%)」フィールドに新しい比率を入力します。

4 「**比率の変更**」をもう一度選択します。帯域幅の比率と、割り当てた帯域幅の合計が更新されます。

監視設定

論理監視が有効になっている場合、テスト パケットをリモート監視対象に送信して、WAN パスの可用性を確認することができます。追加された WAN インターフェース、バックアップ WAN #3 およびバックアップ WAN #4 から監視を行える、新しいオプションが追加されています。

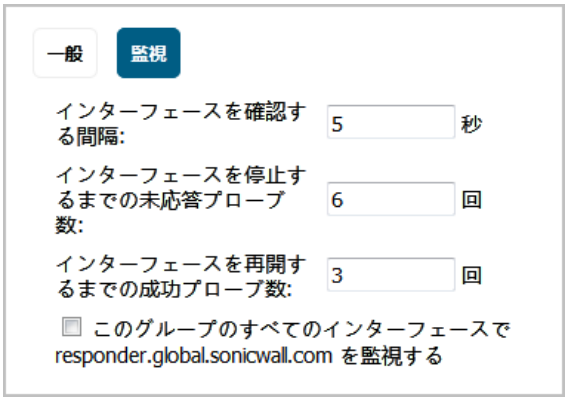
メモ：バックアップ WAN の VLAN は、QoS または VPN 終了をサポートしていません。

特定のグループの監視オプションを設定するには、以下の手順を実行します。

1 「**管理 | ネットワーク > フェイルオーバーと負荷分散**」に移動します。

2 設定するグループの**設定**アイコンを選択します。「**LB グループの修正**」ダイアログが表示されます。

3 「**監視**」を選択します。



4 以下の設定を変更します。

- **インターフェースを確認する間隔:** - *n* **秒** - 健全性チェックの間隔 (秒単位)。既定値は **5** 秒です。
- **インターフェースを停止するまでの未応答プローブ数:** *n* **回** - インターフェースがフェイルオーバーに設定されるまでの健全性チェックの失敗回数。既定値は **6** 回です。
- **インターフェースを再開するまでの成功プローブ数:** *n* **回** - インターフェースが利用可能に設定されるまでの健全性チェックの成功回数。既定値は **3** 回です。
- **このグループのすべてのインターフェースで responder.global.SonicWall.com を監視する** - グループ内のすべてのインターフェースで論理監視を自動的に設定するには、このチェックボックスを有効にします。有効にすると、論理監視対象宛先アドレス `204.212.170.23:50000` を使用して、SNWL TCP パケットに応答するグローバル SNWL ホスト (`responder.global.SonicWall.com`) に TCP プローブ パケットが送信されます。このチェックボックスを選択すると、残りの論理監視設定でビルトイン設定が自動的に有効になります。同じ論理監視が 4 つの WAN イーサネット インターフェースすべてに適用されます。

  メモ：ダイアルアップ WAN 論理監視の設定も、既定でビルトイン設定になります。

5 「**OK**」を選択します。

グループ メンバーの監視設定の構成

監視グループ メンバーの設定を構成するには、以下の手順に従います。

1 「**管理 | ネットワーク > フェイルオーバーと負荷分散**」に移動します。

2 設定するグループ メンバーの**設定**アイコンを選択します。「**監視設定**」ダイアログが表示されます。

3 実行する監視の種別を選択します。

- **物理監視のみ** (既定のオプション。他のオプションはすべて淡色表示)。「ステップ 9」へ進みます。
- **論理/プローブ監視有効** - 他のすべてのオプションが選択できるようになります。

4 「**論理精査監視**」で、プローブが成功する条件を選択します。

- **どちらか一方でも監視対象から応答がある場合に、WAN 利用可能とする。**
- **両方の監視対象から応答がある場合に、WAN 利用可能とする。**
- **監視対象 1 から応答がある場合に、WAN 利用可能とする。**
- **常に WAN 利用可能とする (監視しない)**。- 既定のオプション。他のオプションはすべて淡色表示。「ステップ 9」へ進みます。

5 「**監視対象 1**」で、以下の選択を行います。

- **Ping (ICMP)**
- **TCP** (既定値)
  a 監視対象 1 の「**ホスト**」フィールドにホスト名を入力します。既定は **responder.global.SonicWall.com** です。
  b 監視対象 1 の「**ポート**」フィールドに、適用可能なポート番号を入力します。既定値は **50000** です。

6 「監視対象 1 から応答がある場合に、WAN 利用可能とする」が選択されていた場合は、「ステップ 8」に進みます。

7 「**監視対象 2 (オプション)**」ドロップダウン メニューから、次のいずれかを選択します。

メモ：「監視対象 2 (オプション)」のオプションが選択できるようになるのは、「**論理/プローブ監視有効**」で「**どちらか一方でも監視対象から応答がある場合に、WAN 利用可能とする**」または「**両方の監視対象から応答がある場合に、WAN 利用可能とする**」を選択した場合です。

- **Ping (ICMP)**
- **TCP** (既定値)

a 監視対象 2 の「**ホスト**」フィールドにホスト名を入力します。既定は **responder.global.SonicWall.com** です。

b 監視対象 2 の「**ポート**」フィールドに、適用可能なポート番号を入力します。既定値は **50000** です。

8 「**既定のターゲット IP**」フィールドに既定のターゲットの IP アドレスを入力します。

メモ：このオプションは、「**論理/プローブ監視有効**」で「**常に WAN 利用可能とする (監視しない)**」を選択した場合、淡色表示になります。

IP アドレスが 0.0.0.0 の場合または DNS 解決が失敗した場合に、設定した既定のターゲット IP が使用されます。

9 「**OK**」を選択します。

17

ネットワーク ゾーンの設定

- ゾーンについて (422 ページ)
  - ゾーンの動作 (423 ページ)
  - 事前定義ゾーン (424 ページ)
  - セキュリティ種別 (424 ページ)
  - インターフェース間通信を許可する (425 ページ)
  - ゾーンで SonicWall セキュリティ サービスを有効にする (425 ページ)
  - 無線および非無線制御モードの効果 (426 ページ)
- ネットワーク > ゾーン (428 ページ)
  - ゾーンの設定テーブル (429 ページ)
  - 新しいゾーンの追加 (430 ページ)
  - ゲスト アクセス用ゾーンの設定 (433 ページ)
  - オープン認証およびソーシャル ログイン用ゾーンの設定 (436 ページ)
  - Radius によるキャプティブ ポータル認証用のゾーンの設定 (437 ページ)
  - ユーザ定義ポリシー メッセージ用のゾーンの設定 (439 ページ)
  - ユーザ定義ログイン ページ用のゾーンの設定 (441 ページ)
  - WLAN ゾーンの設定 (442 ページ)
  - RADIUS サーバの設定 (444 ページ)
  - DPI-SSL をゾーン単位できめ細かく制御する設定 (446 ページ)
  - ゾーンの削除 (447 ページ)

ゾーンについて

ゾーンとは、アクセス ルールの定義と適用などの管理作業を行うために、1 つ以上のインターフェースを論理的にグループ化したものです。このグループ化は、物理インターフェースのみによる方法よりも単純でより直感的なプロセスです。ゾーン ベース セキュリティは、内部および外部のネットワーク セグメントを強力かつ柔軟に管理する方法であり、これを利用して未承認アクセスや攻撃から内部の重要ネットワーク リソースを切り離し、保護することができます。

ネットワーク セキュリティ ゾーンは、扱いやすくユーザにも設定可能な名前で 1 つ以上のインターフェースを簡単にグループ化し、ゾーン間をトラフィックが通過する際にセキュリティ規則を適用する論理的な手法です。セキュリティ ゾーンによって、ファイアウォール用により柔軟なセキュリティ層が追加されます。ゾーン ベース セキュリティを使用することで、管理者は類似するインター

フェースをグループ化して同じポリシーを適用できるので、各インターフェースについて同じポリシーを作成する必要がなくなります。インターフェースの設定方法については、「ネットワーク > インターフェース (287 ページ)」を参照してください。

SonicOS のゾーンを利用して、ネットワーク内部にセキュリティ ポリシーを適用できます。これにより、ネットワーク リソースを別々のゾーンに分類し、ゾーン間のトラフィックを許可または制限することができます。この方法によって、給与支払いサーバやエンジニアリング コード サーバなどの重要な内部リソースへのアクセスを厳格に制御することができます。

ゾーンでは NAT テーブルを完全に公開でき、トラフィックがゾーン間で転送されるときに送信元アドレスと送信先アドレスを制御することで、インターフェース全体でトラフィックを制御することができます。つまり、NAT を内部で、つまり VPN トンネル全体で適用できます。 これはユーザが長年要望していた機能です。またファイアウォールでは、VPN が VPN ゾーンに論理的にグループ化されたため、NAT ポリシーおよびゾーン ポリシーを使って VPN トラフィックを管理できるようになりました。

トピック:

- ゾーンの動作 (423 ページ)
- 事前定義ゾーン (424 ページ)
- セキュリティ種別 (424 ページ)
- インターフェース間通信を許可する (425 ページ)
- ゾーンで SonicWall セキュリティ サービスを有効にする (425 ページ)

ゾーンの動作

セキュリティ ゾーンの動作をわかりやすく模式化して説明してみましょう。複数の部屋がある大きな新築ビルと、ビル内の通路を知らない新入社員のグループがいるとします。このビルには 1 つ以上の出口があります。 これは WAN インターフェースと見なすことができます。ビル内の部屋には 1 つ以上のドアがあります。 これはインターフェースと見なすことができます。部屋はゾーンと考えられます。 各部屋にはたくさんの人がいます。人々は分類され、ビル内の別々の部屋に割り当てられます。各部屋にいる人は、別の部屋に行くときやビルを出るときに、各部屋の出口に立っている門番に話しかける必要があります。この門番が、ゾーン間/ゾーン内セキュリティ ポリシーです。 門番の仕事は、リストを参照して、その人物が別の部屋への通行を許可されているか、またはビルを出ることが許可されているかを確かめることです。その人物は許可されていれば (例えば、セキュリティ ポリシーで許可されていれば)、ドア (インターフェース) から部屋の外に出ることができます。

廊下に出ると、目的の部屋がどこにあるのか、またはビルの外に出るドアがどこにあるのかを警備員に確認する必要があります。警備員はすべての部屋の場所と、ビルから出入りする方法を知っているため、経路を教えることができます。また、警備員はすべての支店の住所を知っています。 これは VPN と見なすことができます。ビルに複数の出入口 (WAN インターフェース) がある場合、警備員は指示に応じて (例えば、緊急の場合や、出入口の通行量を分散する目的のために) 第 2 の出入口を使用するように人々を誘導できます。この働きは、WAN 負荷分散と見なすことができます。

ビル内の部屋には複数のドアがあることもあれば、部屋の中にいるグループ同士が親しくないこともあります。例えば、同じ部屋のグループでも、あるグループと別のグループが別々のドアを使用する場合があります。この 2 つのグループは互いを認識しないため、ユーザは門番 (セキュリティ ポリシー) に依頼して、別のグループ内にいる話しかけたい人物を指し示してもらう必要があります。門番は、あるグループの人が同じ部屋の別のグループの人に話しかけられないようにすることもできます。これは、ゾーンに複数のインターフェースが関連付けられており、ゾーン内トラフィックが許可されていない場合の例です。

ときおり、人々は支店に出向くこともあれば、支店からやってきてビル内の特定の部屋にいる人を訪問することもあるでしょう。これは VPN トンネルと見なすことができます。警備員と門番は許可されているかどうかを確認してから、トラフィックの通過を許可します。また門番は、別の部屋に行く人やビルを出る人、また別の支店に行く人に、衣装を着るように強制することもできます。これにより、その人物の本当の身分を隠し、別人に見せかけます。このプロセスは、NAT ポリシーと見なすことができます。

事前定義ゾーン

ファイアウォールには、機器に応じた事前定義ゾーンがあります。SonicWall セキュリティ装置の事前定義セキュリティ ゾーンは変更可能でありません。

ゾーン	機能
DMZ	パブリックにアクセスできるサーバで通常は使用され、ネットワークの設計に応じて 1 ～ 4 個のインターフェースで構成できます。
LAN	ネットワークの設計に応じて複数個のインターフェースで構成されます。各インターフェースには別々のネットワーク サブネットが接続されますが、グループ化することで 1 つのエンティティとして管理することができます。
MGMT	装置管理に使用され、管理インターフェースだけを含みます。他のゾーンのインターフェースも SonicOS 管理用に有効化できますが、MGMT ゾーン/インターフェースを使用すると、管理専用の独立したゾーンによるセキュリティ強化を図ることができます。
マルチキャスト	IP マルチキャストをサポートします。IP マルチキャストとは、1 つの送信元から同時に複数のホストに IN パケットを送信する手法です。
SSLVPN:	SonicWall NetExtender クライアントを使用してリモート アクセスを保護する場合に使用されます。
VPN	安全なリモート接続を簡単に実現するために使用される仮想ゾーンです。
WLAN	SonicWall SonicPoint とSonicWave をサポートします。このゾーンを Opt ポートに割り当てると、SonicPoint の強制が適用され、非 SonicPoint 機器から受信したすべてのパケットが自動的に破棄されます。WLAN ゾーンでは、以下がサポートされます。 • 接続された SonicPoint SonicWave を自動的にポーリングして識別するためのディスカバリ プロトコル (SDP)。 • プロファイルを使用して SonicPoint および SonicWave を設定するための SonicWall シンプル プロビジョニング プロトコル。 • 無線とゲスト サービスの設定。
WAN:	複数のインターフェースで構成できます。セキュリティ装置の WAN フェイルオーバー機能を使用する場合、WAN ゾーンに 2 つ目のインターネット インターフェースを追加する必要があります。

メモ：インターフェースを 1 つのセキュリティ ゾーンにグループ化しても、そのゾーン内に 1 つのインターフェースを割り当てる必要はあります。

セキュリティ種別

各ゾーンには、そのゾーンの信頼レベルを定義するセキュリティ種別があります。

信頼済み	最も高い信頼レベルを提供します。これは、保護ゾーンから送信されたトラフィックには、最小限の調査しか行われないことを意味します。保護セキュリティは、セキュリティ装置の LAN (保護) 側であると考えることができます。LAN ゾーンは常に「保護」です。
管理	管理ゾーンおよび管理インターフェースに固有のものであり、これもまた最高レベルの保護を提供します。
暗号化	VPN および SSL VPN ゾーンのみで使用されます。暗号化ゾーンで送受信されるトラフィックはすべて暗号化されます。
無線	ネットワークへの唯一のインターフェースが SonicWall SonicPoint および SonicWave 機器で構成されている WLAN ゾーンまたはその他のゾーンに適用されます。無線セキュリティ種別は、特に SonicPoint および SonicWave で使用するために設計されています。無線ゾーンにインターフェースを配置すると、そのインターフェースで SDP (SonicWall ディスカバリ プロトコル) および SSPP (SonicWall シンプル プロビジョニング プロトコル) が有効になり、SonicPoint および SonicWave 機器の自動検出とプロビジョニングが実行されます。SonicPoint または SonicWave を通過するトラフィックのみが無線ゾーンの通過を許可されます。それ以外のトラフィックはすべて破棄されます。
公開	「非保護」ゾーンよりも高く、「保護」ゾーンよりは低い信頼レベルを提供します。公開ゾーンは、セキュリティ装置の LAN (保護) 側と WAN (非保護) 側の中間にある安全領域であると考えることができます。例えば、DMZ は公開ゾーンです。 DMZから送信されたトラフィックは LAN と WAN の両方に送られるためです。既定では、DMZ から LAN へのトラフィックは拒否されますが、LAN から ANY (すべて) へのトラフィックは許可されます。つまり、LAN 側から開始された接続のみによって DMZ と LAN の間のトラフィックが生成されます。DMZ から既定でアクセスできるのは LAN ではなく、WAN のみです。
非保護	最も低い信頼レベルを表します。これは WAN および仮想マルチキャスト ゾーンで使用されます。非保護ゾーンは、セキュリティ装置の WAN (非保護) 側と考えることができます。既定では、非保護ゾーンからのトラフィックは明示的なルールがない限り他のゾーン タイプへの入力が許可されませんが、他のゾーン タイプから非保護ゾーンへのトラフィックは入力が許可されます。

インターフェース間通信を許可する

「**ゾーンの追加**」ダイアログの「**インターフェース間通信を許可する**」設定を使用して、ゾーン インスタンスのインターフェース間でトラフィックの通過を許可するアクセス ルールを自動的に作成できます。例えば、LAN ゾーンに **LAN** インターフェースと **X3** インターフェースの両方が割り当てられている場合、LAN ゾーンで「**インターフェース間通信を許可する**」をオンにすることで、これらのインターフェース上のホストに相互通信を許可するために必要なアクセス ルールが作成されます。

ゾーンで SonicWall セキュリティ サービスを有効にする

ゾーン間を通過するトラフィックに対して、SonicWall セキュリティ サービスを有効にすることができます。例えば、WLAN ゾーンで入出力されるトラフィックに対して SonicWall 侵入防御を有効にすることで、内部ネットワーク トラフィックのセキュリティを高めることができます。以下の SonicWall セキュリティ サービスをゾーンで有効にできます。

コンテンツ フィルタ サービスを強制する	WLAN ゾーンの同じ「保護」および「公開」セキュリティ種別の複数のインターフェースにコンテンツ フィルタを適用します。
クライアント アンチウイルス サービスを強制する	WLAN ゾーンの同じ「保護」および「公開」セキュリティ種別の複数のインターフェースにアンチウイルス保護を適用します。
ゲートウェイ アンチウイルス サービスを有効にする	WLAN ゾーンの同じ「保護」および「公開」セキュリティ種別の複数のインターフェースにゲートウェイ アンチウイルス保護を適用します。
IPS を有効にする	WLAN ゾーンの同じ「保護」および「公開」セキュリティ種別の複数のインターフェースに侵入検知と侵入防御を適用します。
アプリケーション制御サービスを有効にする	WLAN ゾーンの同じ「保護」および「公開」セキュリティ種別の複数のインターフェースにアプリケーション制御ポリシー サービスを適用します。
アンチスパイウェア サービスを有効にする	WLAN ゾーンの同じ「保護」および「公開」セキュリティ種別の複数のインターフェースにアンチスパイウェア検出とスパイウェア防御を適用します。
グローバル セキュリティ クライアントを強制する	WLAN ゾーンの同じ「保護」および「公開」セキュリティ種別の複数のインターフェースにグローバル セキュリティ クライアント (GSC) 保護を適用します。
グループ VPN を作成する	ゾーンの GroupVPN ポリシーを作成します。このポリシーは、「**管理 | 接続性 > VPN > 基本設定**」の「VPN ポリシー」テーブルに表示されます。「**VPN > 基本設定**」で、GroupVPN ポリシーをカスタマイズできます。「**グループ VPN を作成する**」をクリアした場合、GroupVPN ポリシーは「**VPN > 基本設定**」から削除されます。VPN ポリシー作成の詳細については、『*SonicOS 6.5 接続*』を参照してください。
SSL 制御を有効にする	このゾーンで SSL 制御を有効にします。これで、このゾーンから開始されるすべての新しい SSL 接続に対して検査が実行されるようになります。SSL 制御はまず「**管理 | ファイアウォール設定 | SSL 制御**」でグローバルに有効化しておく必要があります。SSL 制御の詳細については、『*SonicOS 6.5 セキュリティ設定*』を参照してください。
SSLVPN アクセスを有効にする	このゾーンで SSL VPN セキュア リモート アクセスを有効にします。

無線および非無線制御モードの効果

トピック:

- 非無線制御モードを有効にした場合の影響 (426 ページ)
- 無線制御モードを有効にした場合の影響 (427 ページ)

非無線制御モードを有効にした場合の影響

非無線制御モードを有効にすると、「**ネットワーク > ゾーン**」ページに影響します。影響を受ける機能を有効または削除しようとする試みは拒否されます。

- 無線ゾーンの「**編集**」および「**削除**」アイコンが、「**管理 | システム セットアップ > ネットワーク > ゾーン**」ページで淡色表示になります。

- 内部無線ゾーンは無効になっています。

無線制御モードを有効にした場合の影響

無線制御モードを有効にすると、「**ネットワーク > ゾーン**」ページに影響します。影響を受ける機能を有効または削除しようとする試みは拒否されます。

- VPN および SSL VPN ゾーンの「**編集**」および「**削除**」アイコンが、「**管理 | システム セットアップ > ネットワーク > ゾーン**」ページで淡色表示になります。

- VPN または SSL VPN、あるいはその両方でゾーンを有効にしようとすると、エラーになります。

ネットワーク > ゾーン

- ゾーンの設定テーブル (429 ページ)
- 新しいゾーンの追加 (430 ページ)
- ゾーンの削除 (447 ページ)
- ゲスト アクセス用ゾーンの設定 (433 ページ)

- オープン認証およびソーシャル ログイン用ゾーンの設定 (436 ページ)
- Radius によるキャプティブ ポータル認証用のゾーンの設定 (437 ページ)
- ユーザ定義ポリシー メッセージ用のゾーンの設定 (439 ページ)
- ユーザ定義ログイン ページ用のゾーンの設定 (441 ページ)
- WLAN ゾーンの設定 (442 ページ)

ゾーンの設定テーブル

「**ゾーンの設定**」テーブルには、ユーザが作成したゾーンだけでなく SonicWall の既定の事前定義ゾーンもすべて表示されます。このテーブルには、各ゾーンの設定に関する以下の状況情報が表示されます。

名前 ゾーンの名前。事前定義されているゾーン名である「**LAN**」、「**WAN**」、「**WLAN**」、「**VPN**」、「**SSLVPN**」、「**MGMT**」、「**MULTICAST**」、「**暗号化**」は変更できません。

セキュリティ種別 セキュリティ種別: セキュリティ タイプは、「**保護**」、「**非保護**」、「**公開**」、「**無線**」、または「**暗号化**」です。

メンバー インターフェース ゾーンのメンバーであるインターフェース。

インターフェース間通信 チェック マークがある場合、そのゾーンで「**インターフェース間通信を許可する**」設定が有効になっています。

クライアント AV チェック マークがある場合、そのゾーンに入出力されるトラフィックに対して SonicWall クライアント アンチウイルスが有効になっています。SonicWall クライアント アンチウイルスにより、ゾーン内のすべてのクライアントのアンチウイルス クライアント アプリケーションが管理されます。

クライアント CF チェック マークがある場合、クライアント コンテンツ フィルタ サービスが有効になっています。

ゲートウェイ AV チェック マークがある場合、そのゾーンに入出力されるトラフィックに対して SonicWall ゲートウェイ アンチウイルスが有効になっています。SonicWall ゲートウェイ アンチウイルスにより、ファイアウォールのアンチウイルス サービスが管理されます。

アンチスパイウェア チェック マークがある場合、そのゾーン内のインターフェースを通過するトラフィックに対して SonicWall アンチスパイウェア検出およびスパイウェア防御が有効になっています。

IPS	チェック マークがある場合、そのゾーンに入出力されるトラフィックに対して SonicWall 侵入防御サービスが有効になっています。
アプリケーション制御	チェック マークがある場合、そのゾーンに入出力されるトラフィックに対してアプリケーション制御サービスが有効になっています。
SSL 制御	チェック マークがある場合、そのゾーンに入出力されるトラフィックに対して SSL 制御が有効になっています。これで、このゾーンから開始されるすべての新しい SSL 接続に対して検査が実行されるようになります。
SSL VPN アクセス	チェック マークがある場合、そのゾーンに入出力されるトラフィックに対して SSLVPN セキュア リモート アクセスが有効になっています。
DPI-SSL クライアント	チェック マークがある場合、DPI-SSL クライアントに対して、グローバル ベースではなく、ゾーンごとのきめ細かな DPI-SSL が有効になっています。
DPI-SSL サーバ	チェック マークがある場合、DPI-SSL サーバに対して、グローバル ベースではなく、ゾーンごとのきめ細かな DPI-SSL が有効になっています。
コメント	「**コメント**」アイコンにマウス カーソルを合わせると、ゾーンの設定時に入力したコメントが表示されます。
設定	**編集**アイコンを選択すると、「**ゾーンの編集**」ダイアログが表示されます。**削除**アイコンを選択すると、ゾーンが削除されます。事前定義ゾーンについては、削除アイコンが淡色表示になっています。こうしたゾーンは削除できません。

新しいゾーンの追加

新しいゾーンを追加するには、以下の手順を実行します。

1 「**管理 | システム セットアップ > ネットワーク > ゾーン**」に移動します。

2 **追加**アイコンを選択します。「**ゾーンの追加**」ダイアログが表示されます。

3 新しいゾーンの名前を「**名前**」フィールドに入力します。

4 「**セキュリティ種別**」で、以下の選択を行います。

信頼済み 信頼レベルが最も高いゾーン (内部 LAN セグメントなど)。

公開 要求される信頼レベルがより低いゾーン (DMZ インターフェースなど)。

無線 WLAN インターフェース。

SSLVPN: コンテンツ フィルタ、クライアント AV 強制、およびクライアント CF サービスが有効なインターフェース。

メモ：このセキュリティ種別を選択すると、このダイアログで「**SSLVPN アクセスを有効にする**」および「**グループ VPN を作成する**」オプションが無効になります。

5 ゾーン内通信を許可する場合は、「**インターフェース間通信を許可する**」を選択します。ゾーン インスタンスのインターフェース間のトラフィック フローを許可するアクセス ルールが自動的に作成されます。このオプションは、既定では選択されています。

6 このゾーンと同じ信頼度の他のゾーンとの間のトラフィックを許可するアクセス ルールを SonicOS に自動的に作成させる場合は、「**同じ信頼度のゾーン間のトラフィックを許可するためのアクセス ルールを自動追加する**」を選択します。例えば、CUSTOM_LAN -> CUSTOM _LAN または CUSTOM_LAN -> LAN。このオプションは、既定では選択されています。

メモ：このオプションと以下のアクセス ルール オプションについては、『*SonicOS 6.5 ポリシー*』でアクセス ルールに関する情報を参照してください。

7 このゾーンと信頼度の低い他のゾーンとの間のトラフィックを許可するアクセス ルールを SonicOS に自動的に作成させる場合は、「**低い信頼度のゾーンへのトラフィックを許可するためのアクセス ルールを自動追加する**」を選択します。例えば、CUSTOM_LAN -> WAN または CUSTOM_LAN -> DMZ。このオプションは、既定では選択されています。

8 このゾーンと信頼度の高い他のゾーンとの間のトラフィックを許可するアクセス ルールを SonicOS に自動的に作成させる場合は、「**高い信頼度のゾーンからのトラフィックを許可するためのアクセス ルールを自動追加する**」を選択します。例えば、LAN -> CUSTOM_DMZ または CUSTOM_LAN -> CUSTOM_DMZ。このオプションは、既定では選択されています。

9 このゾーンと信頼度の低いゾーンとの間のトラフィックを禁止するアクセス ルールを SonicOS に自動的に作成させる場合は、「**低い信頼度のゾーンからのトラフィックを拒否するためのアクセス ルールを自動追加する**」を選択します。例えば、WAN -> CUSTOM_LAN または DMZ -> CUSTOM_LAN。このオプションは、既定では選択されています。

10 ネットワーク ホストのクライアント アンチウイルス サービスを使用して、同じ保護ゾーン、公開ゾーン、または WLAN ゾーンの複数のインターフェースに接続されたクライアントに管理されたクライアント アンチウイルス保護を適用する場合は、「**クライアント AV 強制サービスを有効にする**」を選択します。このオプションは、既定では選択されていません。

メモ：このオプションは、「**セキュリティ種別**」からセキュリティ種別を選択するまで、淡色表示で使用できない状態になっています。

メモ：このオプションと以下のセキュリティ サービス オプションについては、『*SonicOS 6.5 セキュリティ設定*』でこれらのサービスに関する情報を参照してください。

11 ネットワーク ホストのクライアント CF サービスを使用して、同じ保護ゾーン、公開ゾーン、または WLAN ゾーンの複数のインターフェースに接続されたクライアントに管理されたクライアント コンテンツ フィルタを適用する場合は、「**クライアント CF サービスを有効にする**」を選択します。このオプションは、既定では選択されていません。

メモ：このオプションは、「**セキュリティ種別**」からセキュリティ種別を選択するまで、淡色表示で使用できない状態になっています。

12 DPI-SSL 強制や SentinelOne AV 強制などの強化された NGAV (Next Generation AV) を実施するには、「DPI-SSL 強制サービスを有効にする」を選択します。このオプションは、既定では選択されていません。NGAV の詳細については、『*SonicOS 6.5 セキュリティ設定*』を参照してください。

13 このゾーンで SSL VPN セキュア リモート アクセスを有効にする場合は、「**SSLVPN アクセスを有効にする**」を選択します。このオプションは、既定では選択されていません。

メモ：「セキュリティ種別」で SSLVPN を選択すると、このオプションは淡色表示になります。

14 このゾーンに対して、SonicWall のグループ VPN ポリシーを自動的に作成する場合は、「**グループ VPN を作成する**」を選択します。グループ VPN ポリシーは、「**管理 | 接続性 > VPN > 設定**」でカスタマイズできます。このオプションは、既定では選択されていません。このオプションは、「**セキュリティ種別**」として **SSLVPN** を選択するまで使用でき、このセキュリティ種別をそれ以外のいずれかの種別に変更した後は単色表示となって使用できない状態になります。

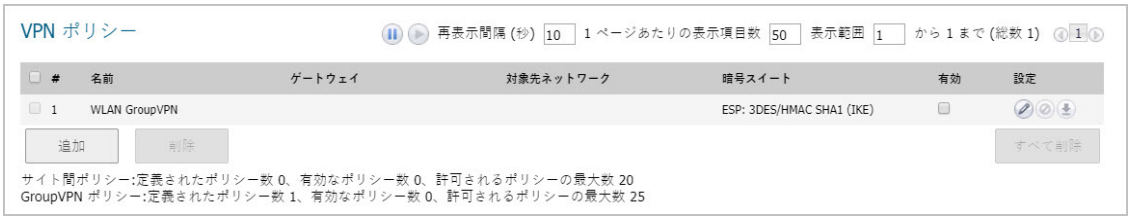
注意：「グループ VPN を作成する」を無効にすると、対応するグループ VPN ポリシーはすべて削除されます。

メモ：「セキュリティ種別」で SSLVPN を選択すると、このオプションは淡色表示になります。

このオプションとその他の接続オプションの詳細については、『*SonicOS 6.5 接続*』を参照してください。

WAN/WLAN VPN ポリシーのグループ VPN を無効にすると、すべての VPN ポリシーが削除されます。「**グループ VPN を作成する**」オプションを再度有効にすると、新しい有効な VPN ポリシーが自動的に作成されます。VPN ポリシーをグローバルに無効にしても、自動ルールは削除されません。VPN ポリシーをまったく使用したくない場合は、VPN をグローバルに無効にしてから、VPN 関連のポリシーをすべて削除します。

GroupVPN ポリシーは、「**管理 | 接続性 | VPN > 基本設定**」にある「**VPN ポリシー**」テーブルに表示されます。ファイアウォールが工場出荷時の既定の設定で起動されたとき、WAN/WLAN GroupVPN ポリシーは既定で無効になっています。



15 このゾーンで SSL 制御を有効にする場合は、「**SSL 制御を有効にする**」を選択します。これで、このゾーンから開始されるすべての新しい SSL 接続に対して検査が実行されるようになります。このオプションは、既定では選択されていません。

メモ：「管理 | セキュリティ設定 > ファイアウォール > SSL 制御」でまず SSL 制御をグローバルに有効化しておく必要があります。

16 このゾーンに接続されたすべてのクライアントに対して、セキュリティ装置上でゲートウェイ アンチウイルス保護を適用する場合は、「**ゲートウェイ アンチウイルス サービスを有効にする**」を選択します。SonicWall ゲートウェイ アンチウイルスにより、セキュリティ装置のアンチウイルス サービスが管理されます。このオプションは、既定では選択されていません。

17 同じ保護ゾーン、公開ゾーン、または WLAN ゾーンの複数のインターフェースに侵入検知と侵入防御を適用する場合は、「**IPS を有効にする**」を選択します。このオプションは、既定では選択されていません。

18 WLAN ゾーンのセキュリティ種別 (保護または公開) が同じ複数のインターフェースにアンチスパイウェア検出とスパイウェア防御を適用する場合は、「**アンチスパイウェア サービスを有効にする**」を選択します。このオプションは、既定では選択されていません。

19 WLAN ゾーンのセキュリティ種別 (保護または公開) が同じ複数のインターフェースにアプリケーション制御ポリシーを適用する場合は、「**アプリケーション制御サービスを有効にする**」を選択します。このオプションは、既定では選択されていません。アプリケーション制御の詳細については、『*SonicOS 6.5 ポリシー*』を参照してください。

20 DPI-SSL クライアントに対してグローバル ベースではなく、ゾーンごとのきめ細かな DPI-SSL を有効にするには、「**SSL クライアント検査を有効にする**」を選択します。このオプションは、既定では選択されていません。

21 DPI-SSL サーバに対してグローバル ベースではなく、ゾーンごとのきめ細かな DPI-SSL を有効にするには、「**SSL サーバ検査を有効にする**」を選択します。このオプションは、既定では選択されていません。

22 「**OK**」を選択します。これで、新しいゾーンが セキュリティ装置 に追加されます。

ゲスト アクセス用ゾーンの設定

重要：非保護、暗号化、SSL VPN または管理のゾーンをゲスト アクセス用に設定することはできません。

SonicWall ユーザ ゲスト サービスは、訪問者や信頼されていないネットワーク ノード用に無線ゲスト パスおよびロックダウンされたインターネット専用のネットワーク アクセスを簡単に作成できるソリューションを提供します。この機能は、WLAN、LAN、DMZ、または任意の公開/半公開ゾーンの無線ユーザまたは有線ユーザにまで拡張できます。

ゲスト サービスを設定するには、以下の手順を実行します。

1 「**管理 | システム セットアップ > ネットワーク > ゾーン**」に移動します。

2 ゲスト サービスを追加したいゾーンの「**編集**」を選択します。「**ゾーンの編集**」ダイアログが表示されます。

3 「**ゲスト サービス**」を選択します。「**ゲスト サービスを有効にする**」のみが使用可能です。

4 「**ゲスト サービスを有効にする**」を選択します。その他すべてのオプションが使用可能になりますが、これらは既定では選択されていません。

5 ゲスト サービスについて、以下の設定オプションを選択します。

ゲスト間の通信を有効にする	ゲストがこのゾーンに接続している他のユーザと直接通信することを許可します。
ゲストに対してアンチウイルスの確認を行わない	ゲスト トラフィックがアンチウイルス保護をバイパスできるようにします。
ゲストに対してクライアント CF の確認を行わない	ゲスト トラフィックがクライアント CF の強制をバイパスできるようにします。
ゲストに対して DPI-SSL 強制の確認を行わない	ゲスト トラフィックが DPI-SSL 強制をバイパスできるようにします。
外部ゲスト認証を有効にする	選択した機器またはネットワークから接続するゲストを、アクセスに先立って認証する必要があります。このオプションを選択すると、「**設定**」が使用可能になります。「**設定**」を選択すると、「**外部ゲスト認証**」ダイアログが表示されます。このオプションの設定については、「SonicOS でのソーシャル ログインの設定 (829 ページ)」を参照してください。 **メモ**：このオプションを選択すると、次の 4 つのオプションが淡色表示になり、使用できなくなります。

キャプティブ ポータル認証を有効にする	RADIUS 認証によってカスタマイズされたログイン ページを作成できます。このオプションを選択すると、「**設定**」が使用可能になります。「**設定**」ボタンを選択すると、「**認証ページの設定**」ダイアログが表示されます。このオプションの設定については、「Radius によるキャプティブ ポータル認証用のゾーンの設定 (437 ページ)」を参照してください。
認証なしにポリシー ページを有効にする	WLAN ゾーンで SonicPoint または SonicWave に初めて接続するユーザに対して、ゲスト サービスの利用に関するポリシー ページが表示されます。ゲスト ユーザは、ユーザ名とパスワードの入力ではなく、ポリシーの承諾によって認証されます。このオプションを選択すると、「**設定**」が使用可能になります。HTML カスタマイズ可能なポリシーの使用に関するページを設定するには、「**設定**」を選択します。「**ポリシー メッセージの設定**」ダイアログが表示されます。このオプションの設定については、「ユーザ定義ポリシー メッセージ用のゾーンの設定 (439 ページ)」を参照してください。
個別認証ページ	ユーザがネットワークに最初に接続するときに、ユーザを個別認証ページにリダイレクトします。このオプションを選択すると、「**設定**」が使用可能になります。個別認証ページを設定するには、「**設定**」を選択して、「**認証ページの設定**」ダイアログを表示します。このオプションの設定については、「ユーザ定義ログイン ページ用のゾーンの設定 (441 ページ)」を参照してください。
認証後に表示するページ	認証が成功した直後にユーザを指定のページに振り向けます。このオプションを選択すると、対応するフィールドが使用可能になります。認証後に表示されるページの URL をフィールドに入力します。
ゲスト認証のバイパス	何らかのユーザレベル認証が既に使用されている環境に、ゲスト サービス機能を統合することを許可します。この機能によって認証プロセスが自動化され、認証を要求することなく無線ユーザに無制限の無線ゲスト サービスを割り当てることができます。選択すると、このオプションのドロップダウン メニューが使用可能になります。以下から選択します。 • **すべての MAC アドレス** (既定) • アドレス オブジェクト • アドレス グループ • 「**MAC オブジェクトの作成**」-「**アドレス オブジェクトの追加**」ダイアログが表示されます。[a] **メモ：**この機能は、無制限のゲスト サービス アクセスが必要な場合、またはアップストリームにある別の機器によって認証が適用される場合にのみ使用してください。
SMTP トラフィックのリダイレクト先	このゾーンに入ってくる SMTP トラフィックを指定の SMTP サーバにリダイレクトします。選択すると、このオプションのドロップダウン メニューが使用可能になります。以下から選択します。 • アドレス オブジェクト • 「**新しいアドレス オブジェクトの作成**」を選択すると、「**アドレス オブジェクトの追加**」ダイアログが表示されます。a

通信を禁止するネットワーク	指定されたネットワークへのトラフィックを遮断します。選択すると、このオプションのドロップダウン メニューが使用可能になります。以下から選択します。 • アドレス オブジェクト • アドレス オブジェクト グループ • **アドレス オブジェクトの作成** a • **アドレス オブジェクト グループの作成** a
通信を許可するネットワーク	選択したネットワークへのトラフィックが、ゲスト サービスが有効になっているゾーンを通過することを自動的に許可します。選択すると、このオプションのドロップダウン メニューが使用可能になります。以下から選択します。 • アドレス オブジェクト • アドレス オブジェクト グループ • **アドレス オブジェクトの作成** a • **アドレス オブジェクト グループの作成** a **メモ：**「**アドレス オブジェクトの追加**」ダイアログが表示されます。
最大同時接続ゲスト数	このゾーンへの接続を許可されるゲスト ユーザの最大数を指定します。最小値は 1、最大値は 4500 で、既定の設定は **10** になっています。
無線ゾーン ゲスト サービス オプション	WLAN ゾーンで、または**セキュリティ種別**が**無線**の個別ゾーンでのみ表示されます。
動的アドレス変換を有効にする	DHCP 以外のゲストに対し、アクセスを許可します。このオプションは、既定では選択されていません。

a. アドレス オブジェクトおよびアドレス オブジェクト グループの作成については、『*SonicOS ポリシー*』を参照してください。

6 「**OK**」を選択すると、設定がこのゾーンに適用されます。

オープン認証およびソーシャル ログイン用ゾーンの設定

SonicOS はオープン認証 (OAuth) とソーシャル ログインをサポートしています。

- OAuth は、ユーザによるアプリケーション間でのデータの共有を支援します。
- ソーシャル ログインは、さまざまなソーシャル メディアでのログイン処理を簡素化します

これらの機能を使用するためには、「オープン認証、ソーシャル ログイン、LHM の設定 (820 ページ)」での説明に従って、ゾーンを作成します。

Radius によるキャプティブ ポータル認証用のゾーンの設定

Radius によるキャプティブ ポータル認証を設定するには:

1 「**ゾーンの追加/編集**」ダイアログで、「**ゲスト サービス**」を選択します。

2 「**ゲスト サービスを有効にする**」を選択します。オプションが使用可能になります。

3 「**キャプティブ ポータル認証を有効にする**」を選択します。「**設定**」が使用可能になります。

4 「**設定**」を選択します。「**認証ページの設定**」ダイアログが表示されます。

5 「**キャプティブ ポータル認証設定**」セクション:

a 内部キャプティブ ポータル ベンダーの URL を「**内部キャプティブ ポータル ベンダー URL**」フィールドに入力します。

b 外部キャプティブ ポータル ベンダーの URL を「**外部キャプティブ ポータル ベンダー URL**」フィールドに入力します。

6 「**RADIUS サーバ属性の設定**」セクション :

a 「**キャプティブ ポータル ウェルカム URL 送信元**」からキャプティブ ポータル ウェルカム URL のソースを選択します。

- **RADIUS から** (既定)。「ステップ c」に進みます。
- **ユーザ定義**。次のオプションが使用可能になります。

b ウェルカム URL を「**ユーザ定義キャプティブ ポータル ウェルカム URL**」フィールドに入力します。

c セッション タイムアウト制限の送信元を「セッション タイムアウト送信元」から選択します。

- **RADIUS から** (既定)。「ステップ f」に進みます。
- **ユーザ定義**。次のオプションが使用可能になります。

d 「**ユーザ定義セッション タイムアウト**」からセッション タイムアウト期間のタイプを選択します。

- **分間**

- **時間**
- **日間** (既定)

e 制限値をフィールドに入力します。

f 無動作時タイムアウトの送信元を「**無動作時タイムアウト送信元**」から選択します。

- **RADIUS から** (既定)。「ステップ 7」に進みます。
- **ユーザ定義**。次のオプションが使用可能になります。

g 「**ユーザ定義無動作時タイムアウト**」から無動作時タイムアウト期間のタイプを選択します。

- **分間**
- **時間**
- **日間** (既定)

h 期間の制限値をフィールドに入力します。

7 「**RADIUS 認証設定**」セクションで、「**RADIUS 認証方式**」から認証方式を選択します。

- **CHAP** (既定)
- **PAP - 暗号化**
- **PAP -平文**

8 「**OK**」を選択します。

ユーザ定義ポリシー メッセージ用のゾーンの設定

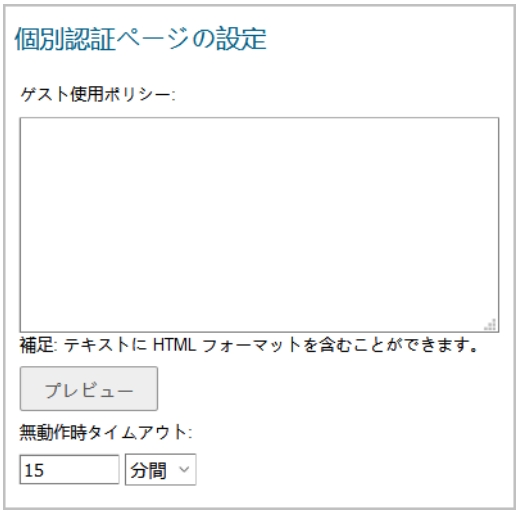
ユーザ定義ポリシー メッセージを設定するには:

1 「**ゾーンの追加/編集**」ダイアログで、「**ゲスト サービス**」を選択します。

2 「**ゲスト サービスを有効にする**」を選択します。オプションが使用可能になります。

3 「**認証なしにポリシー ページを有効にする**」を選択します。「**設定**」が使用可能になります。

4 「**設定**」を選択します。「**認証ページの設定**」ダイアログが表示されます。



5 ゲストが利用する場合のポリシーを「**ゲスト使用ポリシー**」フィールドに入力します。テキストには HTML フォーマットを含めることができます。

6 入力したポリシー メッセージをプレビューするには、「**プレビュー**」を選択します。

7 無動作タイムアウトを指定するには、「**無動作時タイムアウト**」フィールドにタイムアウト値を入力します。

8 タイムアウトのタイプを選択します。

- **秒間**
- **分間** (既定)
- **時間**
- **日間**

9 「**認証なしにポリシー ページを有効にする**」を選択します。このオプションは、既定では選択されていません。

10 「**OK**」を選択します。

ユーザ定義ログイン ページ用のゾーンの設定

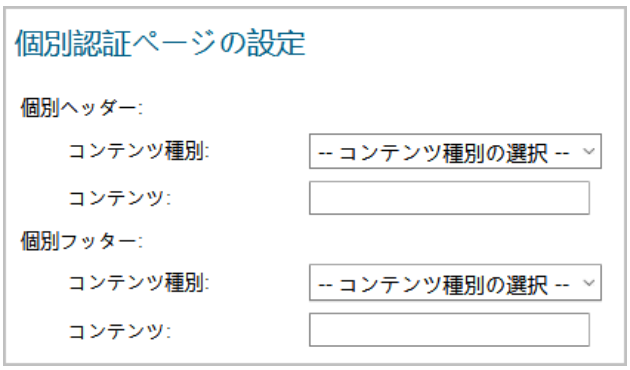
ユーザ定義ログイン ページを設定するには:

1 「**ゾーンの追加/編集**」ダイアログで、「**ゲスト サービス**」を選択します。

2 「**ゲスト サービスを有効にする**」を選択します。オプションが使用可能になります。

3 「**個別認証ページ**」を選択します。「**設定**」が使用可能になります。

4 「**設定**」を選択します。「**認証ページの設定**」ダイアログが表示されます。



5 「**個別ヘッダー**」で、「**コンテンツ種別**」から次を選択します。

- **URL**
- **テキスト**

6 URL またはテキストを「**コンテンツ**」フィールドに入力します。

7 「**個別フッター**」で、「**コンテンツ種別**」から次を選択します。

- **URL**
- **テキスト**

8 URL またはテキストを「**コンテンツ**」フィールドに入力します。

9 「**OK**」を選択します。

WLAN ゾーンの設定

1 「**管理 | システム セットアップ > ネットワーク > ゾーン**」に移動します。

2 次の手順を実行します。

- 新規のゾーンを設定する場合は、「**追加...**」を選択します。
- 既存のゾーンを設定する場合は、WLAN ゾーンの**編集**アイコンを選択します。

「**ゾーンの追加/ゾーンの編集**」ダイアログが表示されます。

> **メモ**：ゾーンによっては、「**ゲスト サービス**」、「**無線**」、および「**RADIUS サーバ**」のビューも表示されます。
>
> 「**一般**」ビューの設定方法については、「新しいゾーンの追加 (430 ページ)」を参照してください。

3 新しいゾーンを作成する場合は、「**セキュリティ種別**」から「**無線**」を選択します。「**ゲスト サービス**」、「**無線**」、および「**RADIUS サーバ**」が表示されます。

4 ゾーン インスタンスのインターフェース間でトラフィックの通過を許可するアクセス ルールの作成を自動化するには、「**インターフェース間通信を許可する**」を選択します。例えば、LAN ゾーンに **LAN** インターフェースと **X3** インターフェースの両方が割り当てられている場合、LAN ゾーンで「**インターフェース間通信を許可する**」をオンにすることで、これらのインターフェース上のホストに相互通信を許可するために必要なアクセス ルールが作成されます。このオプションは、既定では選択されていません。

5 「**無線**」を選択します。

6 WLAN ゾーンに入るすべてのトラフィックに SonicWall SSL VPN 装置による認証を義務付けるには、「**無線**」セクションで「**SSL VPN を強制する**」を選択します。このオプションを選択すると、次の 2 つのオプションが使用可能になります。このオプションは、既定では選択されていません。

7 「**SSLVPN サーバ**」で、トラフィックを SonicWall SSL VPN 装置に振り向けるアドレス オブジェクトを選択するか、新しいアドレス オブジェクトを作成します。アドレス オブジェクトおよびアドレス オブジェクト グループの作成については、『*SonicOS 6.5 ポリシー*』を参照してください。

8 「**SSL VPN サービス**」で、SSL VPN によって認証されたクライアントに許可するサービスまたはサービスのグループを選択します。

9 「**SonicPoint/SonicWave 設定**」セクションで、このゾーンに接続されるすべての SonicPoint/SonicWave に適用する「**SonicPoint/SonicWave プロビジョニング プロファイル**」を選択します。個別に異なる設定を指定していない限り、このゾーンに接続する SonicPoint/SonicWave は、SonicPoint/SonicWave プロビジョニング プロファイルの設定によって自動的にプロビジョニングされます。SonicPoint/SonicWave プロビジョニング プロファイルについては、『*SonicOS 6.5 接続*』を参照してください。

> ⓘ **メモ**：以下の 4 つの設定では、必要に応じて、「**自動プロビジョニング**」を選択すると、プロファイルに関連付けられた SonicPoint/SonicWave が、プロファイルの変更時に自動的にプロビジョニングされるようになります。このオプションは、既定では選択されていません。

10 このゾーンに接続されるすべての SonicPointN/Ni/Ne にプロファイルを適用するには、「**SonicPointN/Ni/Ne プロビジョニング プロファイル**」を選択します。個別に異なる設定を指定していない限り、このゾーンに接続される SonicPointN/Ni/Ne は、SonicPoint プロビジョニング プロファイルの設定によって自動的にプロビジョニングされます。既定のプロビジョニング プロファイルは「**SonicPointN**」です。

11 このゾーンに接続されるすべての SonicPointNDR にプロファイルを適用するには、「**SonicPoint N Dual Radio プロビジョニング プロファイル**」を選択します。個別に異なる設定を指定していない限り、このゾーンに接続される SonicPointNDR は、SonicPointNDR プロビジョニング プロファイルの設定によって自動的にプロビジョニングされます。既定のプロビジョニング プロファイルは「**SonicPointNDR**」です。

12 このゾーンに接続されるすべての SonicPointACe/ACi/N2 にプロファイルを適用するには、「**SonicPointACe/ACi/N2 プロビジョニング プロファイル**」を選択します。個別に異なる設定を指定していない限り、このゾーンに接続される SonicPointACe/ACi/N2 は、SonicPointACe/ACi/N2 プロビジョニング プロファイルの設定によって自動的にプロビジョニングされます。既定のプロビジョニング プロファイルは「**SonicPointACe/ACi/N2**」です。

13 このゾーンに接続されるすべての SonicPointNDR にプロファイルを適用するには、「**SonicWave プロビジョニング プロファイル**」を選択します。個別に異なる設定を指定していない限り、このゾーンに接続される SonicPointNDR は、SonicPointNDR プロビジョニング プロファイルの設定によって自動的にプロビジョニングされます。既定のプロビジョニング プロファイルは「**SonicWave**」です。

14 「**SonicPoint/SonicWave により生成された通信のみ許可する**」を選択すると、SonicWall SonicPoint からのトラフィックのみが WLAN ゾーンのインターフェースを通過できます。これにより、WLAN のセキュリティが最大限に高められます。このオプションは、既定では選択されていま

す。トラフィックの送信元が無線接続かどうかに関係なく、WLAN ゾーンですべてのトラフィックを許可する場合は、このオプションをオフにしてください。

ヒント：送信元が無線接続かどうかに関係なく、WLAN ゾーンですべてのトラフィックを許可するには、「**SonicPoint/SonicPointN により生成された通信のみ許可する**」をオフにします。

メモ：ゲスト サービスの設定については、「ゲスト アクセス用ゾーンの設定 (433 ページ)」を参照してください。

RADIUS サーバの設定情報については、「RADIUS サーバの設定 (444 ページ)」を参照してください。

15 オプションで、「**SonicPoint/SonicWave の 2.4GHz 自動チャンネル選択を 1、6、11 のみの選択にする**」を選択します。このオプションは、既定では選択されていません。

重要：このオプションは、SonicPointN/AC 2.4Hz 自動チャンネル選択として 1、6、および 11 を優先する場合にのみ有効にします。

16 「**安全で信頼できるライセンス マネージャからの SonicWave ライセンス アクティベーションを強制する**」を選択します。

注意：**このオプションは、安全で信頼できるライセンス マネージャからのライセンス アクティベーションを強制します。ライセンス キーセットの手動入力は許可されません。この設定は、テクニカル サポートから指示された場合にのみ変更してください。**

17 「**SonicPoint/SonicWave 管理を無効にする**」を選択して、この WLAN のすべての管理機能を無効にします。

18 これを行うには、次の手順に従います。

- RADIUS サーバを設定する場合は、「RADIUS サーバの設定 (444 ページ)」に進みます。
- これらの設定を WLAN ゾーンに適用する場合は、「**OK**」を選択します。

RADIUS サーバの設定

1 「**管理 | システム セットアップ > ネットワーク > ゾーン**」に移動します。

2 次の手順を実行します。

- 新規のゾーンを設定する場合は、「**追加...**」を選択します。
- 既存のゾーンを設定する場合は、WLAN ゾーンの**編集**アイコンを選択します。

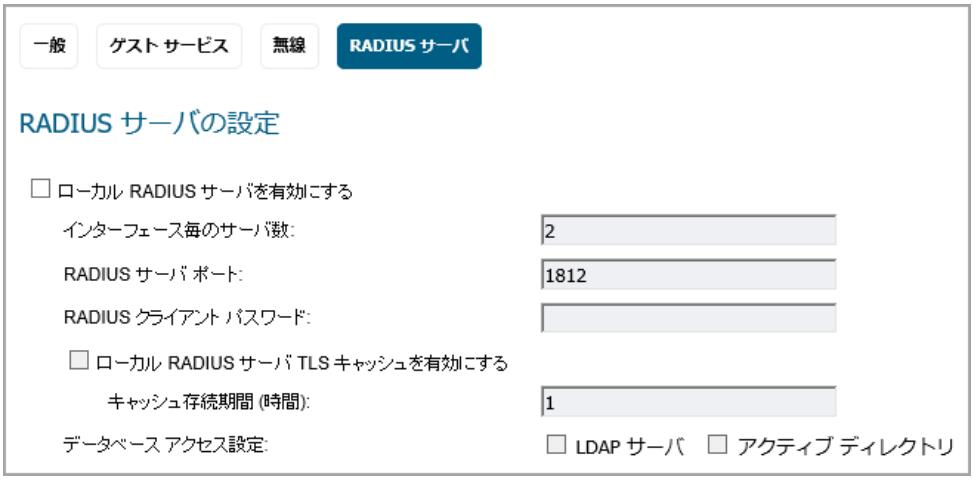
「**ゾーンの追加/ゾーンの編集**」ダイアログが表示されます。

メモ：ゾーンによっては、「**ゲスト サービス**」、「**無線**」、および「**RADIUS サーバ**」のビューも表示されます。

「**一般**」ビューの設定方法については、「新しいゾーンの追加 (430 ページ)」を参照してください。

3 新しいゾーンを作成する場合は、「**セキュリティ種別**」から「**無線**」を選択します。「**ゲスト サービス**」、「**無線**」、および「**RADIUS サーバ**」が表示されます。

4 「**RADIUS サーバ**」を選択します。



5 「**ローカル RADIUS サーバを有効にする**」を選択します。他のオプションが使用可能になります。

6 「**インターフェース毎のサーバ数**」に、インターフェースあたりの RADIUS サーバの数を入力します。最小値は 1、最大値は 512、既定値は **2** です。

7 「**RADIUS サーバ ポート**」フィールドに RADIUS サーバのポートを入力します。既定値は **1812** です。

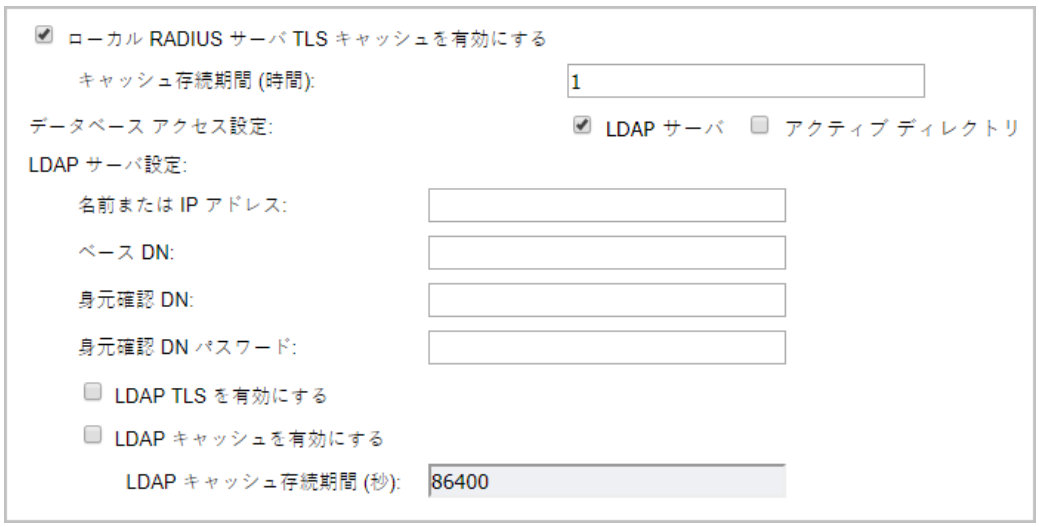
8 「**RADIUS クライアント パスワード**」フィールドに RADIUS クライアントのパスワードを入力します。

9 必要に応じて、「**ローカル RADIUS サーバ TLS キャッシュを有効にする**」を選択します。このオプションは、既定では選択されていません。「**キャッシュ存続期間 (時間)**」フィールドが使用可能になります。

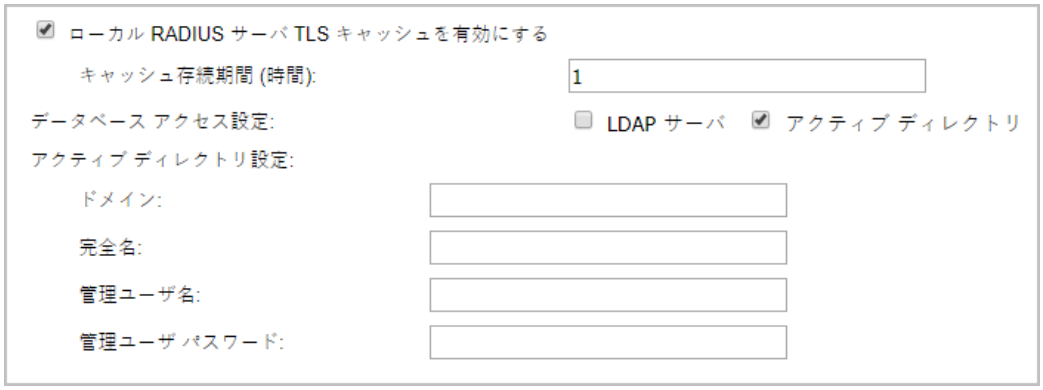
   a 「**キャッシュ存続期間 (時間)**」フィールドに存続期間を時間単位で入力します。最小 (既定値) は **1** 時間、最大は 99999 時間です。

10 「**データベース アクセス設定**」からデータベース アクセス方法を選択します。

- **LDAP サーバ** - さらにオプションが表示されます。「ステップ 11」に進みます。



- **Active Directory** - さらにオプションが表示されます。「ステップ 18」に進みます。



11 「**名前または IP アドレス**」フィールドに LDAP サーバの名前または IP アドレスを入力します。

12 「**ベース DN**」フィールドに基本識別名を入力します。

13 「**身元確認 DN**」フィールドに本人識別名を入力します。

14 「**身元確認 DN パスワード**」フィールドに識別名パスワードを入力します。

15 LDAP Transport Layer Security (TLS) を有効にするには、「**LDAP TLS を有効にする**」を選択します。このオプションは、既定では選択されていません。

16 LDAP キャッシュを有効にするには、「**LDAP キャッシュを有効にする**」を選択します。「LDAP キャッシュ存続期間 (秒)」フィールドが使用可能になります。

   a 「**LDAP キャッシュ存続期間 (秒)**」フィールドに存続期間を秒単位で入力します。最小値は 1、最大値は 99999、既定値は **86400** です

17 「ステップ 22」に移動します。

18 「**ドメイン**」フィールドに、ドメイン名を入力します。

19 「**完全名**」フィールドに Active Directory で使用するフルネーム (氏名) を入力します。

20 「**管理ユーザ名**」フィールドに管理者ユーザのユーザ名を入力します。

21 「**管理ユーザ パスワード**」フィールドに管理者ユーザのパスワードを入力します。

22 「**OK**」を選択します。

DPI-SSL をゾーン単位できめ細かく制御する設定

DPI-SSL をきめ細かく制御する設定では、グローバル ベースではなくゾーン単位で DPI-SSL を有効化することができます。ゾーンごとに DPI-SSL クライアントと DPI-SSL サーバの両方を有効にできます。詳細については、『*SonicOS 6.5 セキュリティ設定*』を参照してください。

ユーザポリシー ページへの自動リダイレクトを有効にする

SonicOS 6.5 を使用すると、ゲストを自動的にゲスト使用ポリシー ページにリダイレクトできます。この機能 (ゼロタッチ ポリシー ページのリダイレクトとも呼ばれる) を有効にすると、ゲスト ユーザは自動的にゲスト使用ポリシー ページにリダイレクトされます。この機能を無効にした場合、ゲストは「**承諾**」を選択する必要があります。

ユーザ ポリシーページへの自動リダイレクトを有効にするには:

1 「**管理 | システム セットアップ > ネットワーク > ゾーン**」に移動します。

2 次のいずれかをクリックします。

- 新しいゾーンを追加する**追加**アイコン。
- 既存ゾーンの**編集**アイコン。

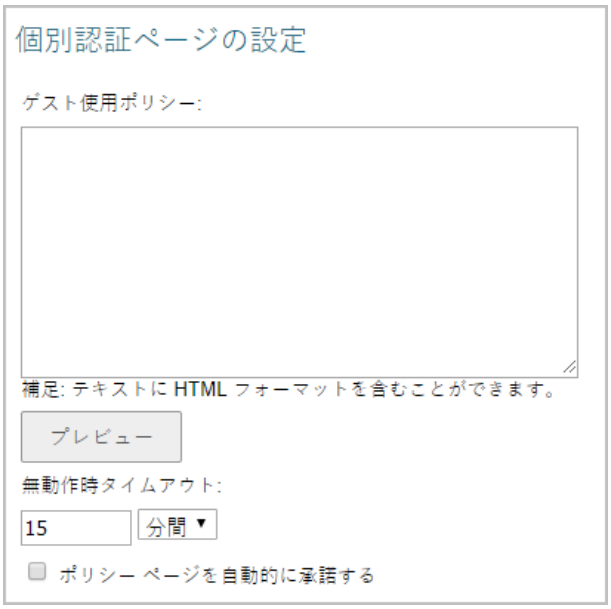
「**ゾーンの追加/ゾーンの編集**」ダイアログが表示されます。

3 「**ゲスト サービス**」を選択します。

4 「**ゲスト サービスを有効にする**」を選択します。

5 「**認証なしにポリシー ページを有効にする**」を選択します。

6 「**設定**」を選択します。「**個別ポリシー メッセージ**」ダイアログが表示されます。



7 「**ポリシー ページを自動的に承諾する**」を選択します。このオプションは、既定では選択されていません。

8 「**OK**」を選択します。

9 ゾーンの設定を終了します。

10 「**OK**」を選択します。

ゾーンの削除

ユーザが作成したゾーンを削除するには、以下の手順に従います。

1 「**管理 | システム セットアップ | ネットワーク > ゾーン**」に移動します。

> ⓘ **メモ**：事前定義ゾーンについては、**削除**アイコンは使用できません。このようなゾーンを削除することはできません。ユーザが作成したゾーンはすべて削除できます。

2 ゾーンの「**設定**」列にある**削除**アイコンを選択します。

ユーザが作成した1 つまたは複数のゾーンを削除するには、以下の手順に従います。

1 「**管理 | システム セットアップ | ネットワーク > ゾーン**」に移動します。

メモ：これらのチェックボックスは事前定義ゾーンでは使用できません。このようなゾーンを削除することはできません。ユーザが作成したゾーンはすべて削除できます。

2 削除するゾーンを選択します。

3 「**削除**」で、削除するゾーンを選択します。

- **選択した項目の削除**
- **すべて削除**

18

ワイヤ モード VLAN 変換の設定

トピック:

- ネットワーク > VLAN 変換 (449 ページ)
  - VLAN 変換について (449 ページ)
  - VLAN 割付の作成と管理 (451 ページ)

ネットワーク > VLAN 変換

メモ：VLAN 変換は、ワイヤ モードをサポートするすべてのプラットフォームで使用できます。

メモ：VLAN 変換と VLAN インターフェース越しのワイヤ モードを同時に有効にすることはできません。

- VLAN 変換について (449 ページ)
- VLAN 割付の作成と管理 (451 ページ)

VLAN 変換について

VLAN 変換 (割付) 機能を使用すると、VLAN に到着したトラフィックを保護モードで動作しているワイヤ モード インターフェースへ送るとき、そのトラフィックをペアになっている送信側インターフェースの別の VLAN に割り付けることができます。SonicWall セキュリティ装置に送られてきたトラフィックのルートを変更して異なる VLAN へ送ることで、詳細な分析や加工、あるいはトラフィックの単なる再割付を行うことができます。この機能は、ワイヤ モード対応のべての機器でサポートされています。

ワイヤ モードの利点は、VLAN 割付を事前にプロビジョニングできることです。これにより、インターフェースがトラフィックを受け取る前に割付を用意できます。アクティブなワイヤ モード インターフェース上で割付を追加または削除することもできます。

トピック:

- 割付のモード (450 ページ)
- 割付の恒久性 (450 ページ)
- 複数のインターフェース ペアの割り付け (450 ページ)

割付のモード

VLAN 割付は以下のモードで作成できます。

- 単方向割付 - 例えば、次のようなケースがあります。
  - 安全性の低いネットワークから安全性の高いネットワークに対して保護された印刷を行う。
  - 安全性の低いネットワークから安全性の高いネットワークに対してアプリケーションやオペレーティング システムのアップデートを転送する。
  - SOC (セキュリティ オペレーション センター) で複数ネットワークを監視する。
  - 安全性の高いネットワークで時間同期機能を提供する。
  - ファイルを転送する。
  - 安全性の低いネットワークから安全性の高いネットワークに対して "メール受信" 通知を行う。
- 双方向割付 - 例えば、セキュリティ装置経由で機器とやり取りする双方向接続 (TCP など) をセットアップする場合に使います。

割付の恒久性

インターフェース ペアに対して作成した VLAN 割付は、設定の一部として格納され、再ロード後も持続します。ワイヤ モード ペア (保護モード) にそれらと関連付けられた割付がある場合、割付ポリシーが削除されない限り、ワイヤ モードを変更できません。

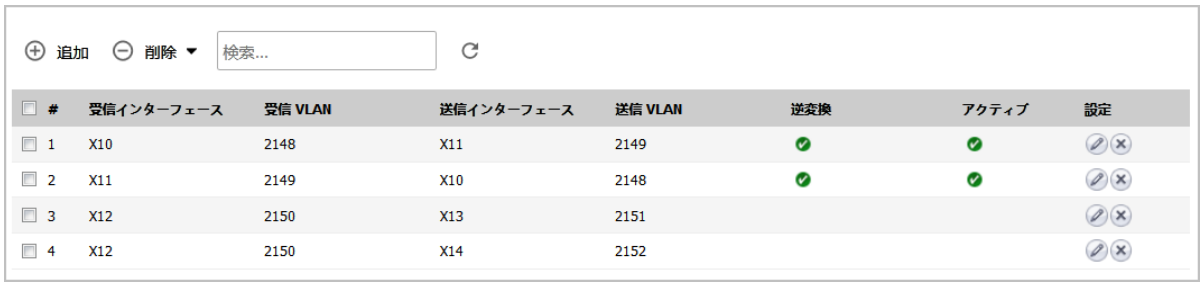
複数のインターフェース ペアの割り付け

複数のインターフェース ペアに対して同時に VLAN 割付を作成できます。これらのインターフェースは、VLAN 割付の作成時に既存の保護ワイヤ モード ペアの一部を形成していなければなりません。複数のインターフェースを持つインターフェースに対して割付を作成することもできます。ただし、どの時点でも現在アクティブなワイヤ モード ペアの割付だけが使われます。

ペアになっているインターフェースが変更された場合、「インターフェースにワイヤモード VLAN 登録がある場合、ワイヤモード ペア インターフェースを変更することはできません」というメッセージが表示されます。

例

複数のインターフェース ペアの割り付け



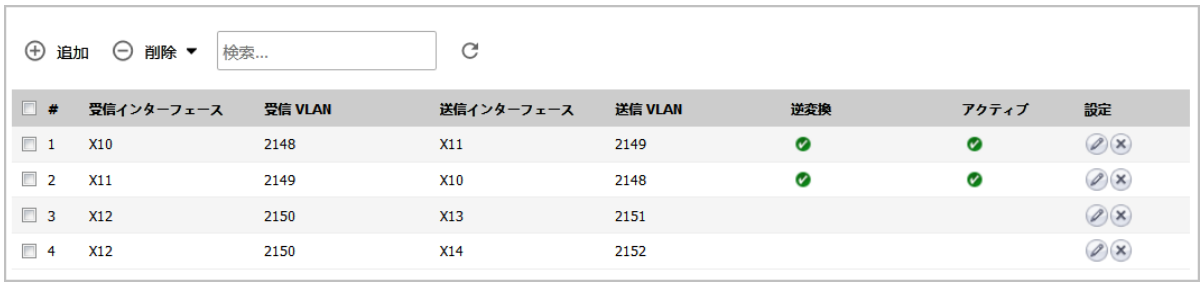
「複数のインターフェース ペアの割り付け」を見ると、X12 から X13 への割付 (ポリシー 1) と X12 から X15 への割付 (ポリシー 2) があります。

現在、X12 と X13 (ポリシー 1 および 3)、X14 と X15 (ポリシー 4 および 6) だけがワイヤ モード ペアを形成しており、「アクティブ」列の緑色のチェックマークが示すように、ポリシー 1、3、4、および 6 だけがアクティブになっています。

メモ：インターフェースにワイヤ モード VLAN 登録が存在する場合は、ワイヤ モード ペア インターフェースを変更できません。

VLAN 割付の作成と管理

「**ネットワーク > VLAN 変換**」で、インターフェースの VLAN 割付を作成、管理することができます。



追加アイコン	「**VLAN 変換の追加**」ダイアログを表示します。
削除	「**削除**」ドロップダウン メニューを表示します。 • **選択した項目の削除** • **すべて削除**
検索フィールド	関心のある VLAN 変換だけを表示できます。
再表示アイコン	「VLAN 変換」テーブルを再表示します。
ポリシー番号とチェックボックス	ポリシーの番号とそれに対応するチェックボックス。
受信インターフェース	受信インターフェースの名前。
受信 VLAN	受信インターフェースの VLAN タグ。
送信インターフェース	トラフィックの割り付け先のインターフェースの名前。
送信 VLAN	トラフィックの割り付け先のインターフェースの VLAN タグ。
逆変換	割付が単方向か双方向かを示します。 • **無効** - 単方向。列は空白です。 • **有効** - 双方向。緑色のチェックマークが表示されます。
アクティブ	割り付けられたペアの状況。 • **アクティブ** - このワイヤ モード ペアは割り付け済みで、アクティブです。緑色のチェックマークが表示されます。 • **非アクティブ** - このワイヤ モード ペアは割り付け済みですが、アクティブでありません (事前プロビジョニング)。列は空白です。
設定	割り付けられたペアの「**編集**」アイコンと「**削除**」アイコンを表示します。

トピック:

- VLAN 割付の作成 (452 ページ)
- VLAN 割付の管理 (455 ページ)

VLAN 割付の作成

単方向 VLAN 割付は、ワイヤ モード ペアの作成前または作成後に作成できます。VLAN 割付の作成は次の 2 ステップで行われます。

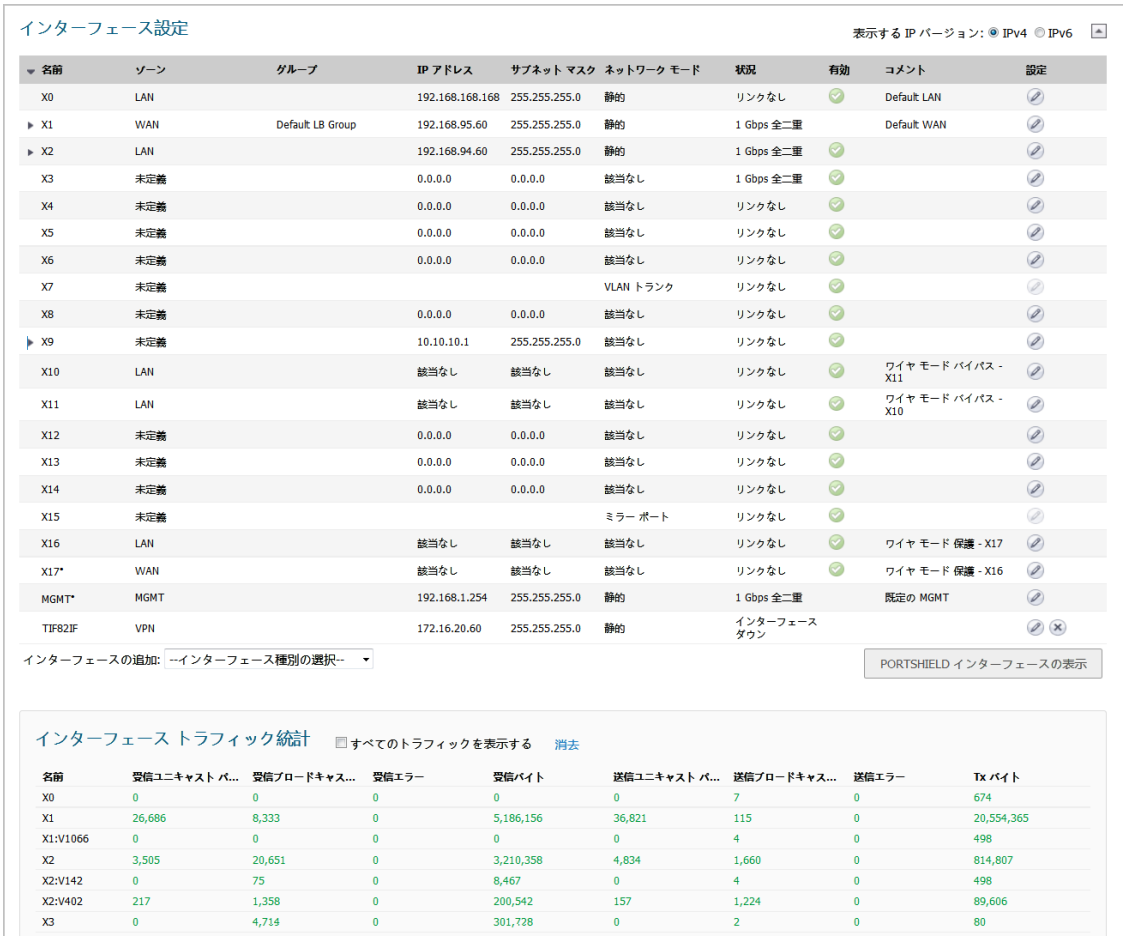
1 ワイヤ モード ペアを保護モードで作成する (452 ページ)

2 VLAN 割付を作成する (454 ページ)

ワイヤ モード ペアを保護モードで作成する

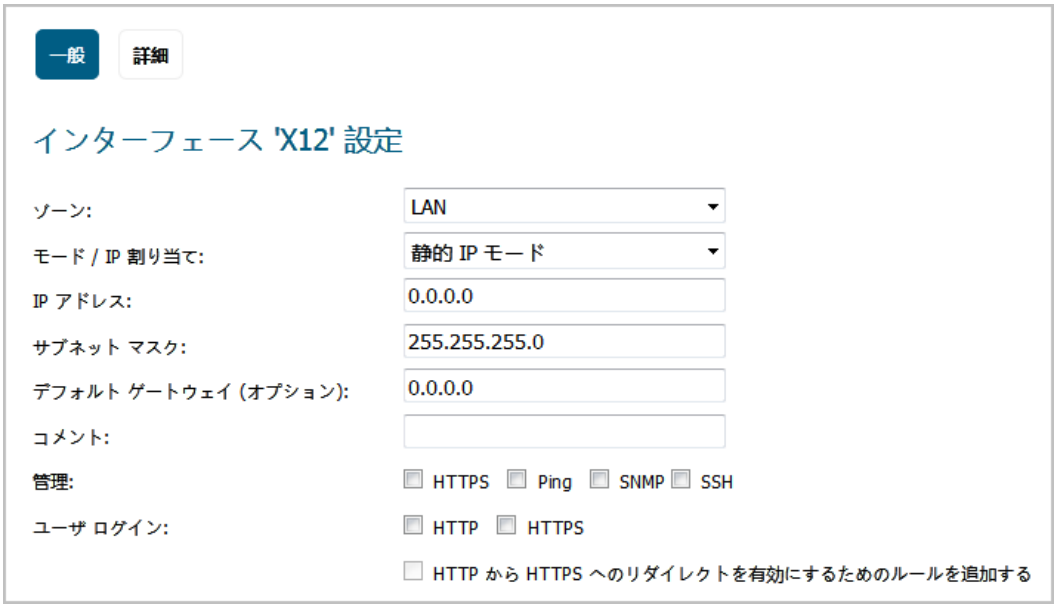
ワイヤ モード ペアを保護モードで作成するには、以下の手順を実行します。

1 「**管理 | システム セットアップ | ネットワーク > インターフェース**」に移動します。



2 ワイヤ モード ペアの一方とするインターフェースの**編集**アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。

3 ワイヤ モード ペアのゾーンを「**ゾーン**」から選択します。オプションが次のように変化します。



4 「**モード / IP 割り当て**」から「**ワイヤ モード (2 ポート ワイヤ)**」を選択します。再びオプションが変化します。

5 「**ワイヤ モード種別**」から「**保護 (直列トラフィックのアクティブ DPI)**」を選択します。

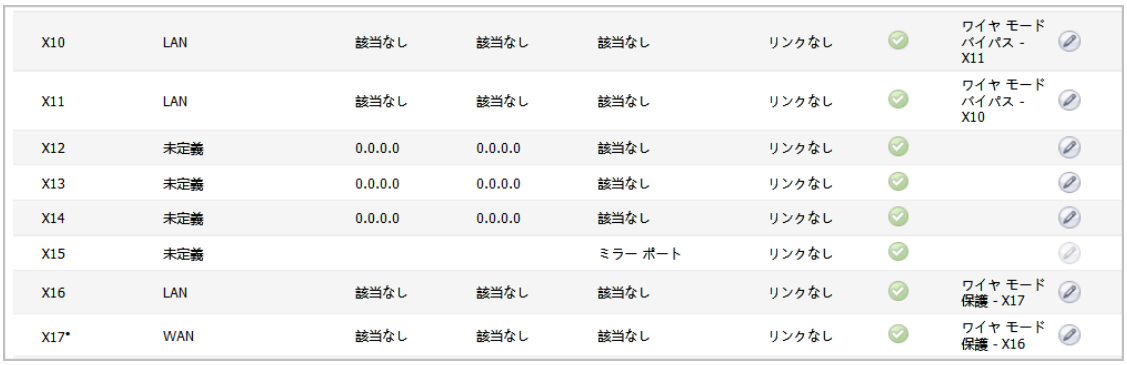
6 現在のインターフェースとペアにするインターフェースを「**ペア インターフェース**」ドロップダウン メニューから選択します。

ヒント：ペアにするインターフェースは未割り当てでなければなりません。

7 ペアにするインターフェースのゾーンを「**ペア インターフェース ゾーン**」から選択します。既定は **LAN** です。

8 通常のワイヤ モード ペアと同じように他のオプションを設定します(「ワイヤ モードとタップ モードの設定 (333 ページ)」および「ワイヤ モードとタップ モードの設定 (333 ページ)」を参照)。

9 「**OK**」を選択します。「**ネットワーク > インターフェース**」ページが更新されます。

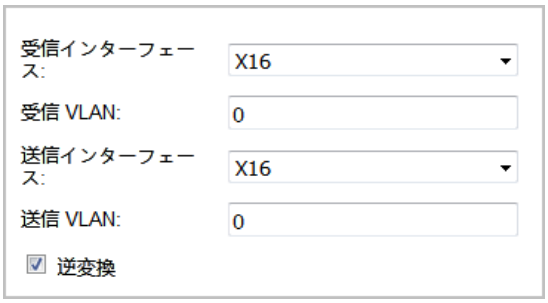


VLAN 割付を作成する

VLAN 割付を作成するには、以下の手順を実行します。

1 「**ネットワーク > VLAN 変換**」に移動します。

2 **追加**アイコンを選択します。「**VLAN 変換の追加**」ダイアログが表示されます。



3 ペアのうち、トラフィックを受け取る側のワイヤ モード インターフェースを「**受信インターフェース**」から選択します。

4 「**受信 VLAN**」に、割り付けるトラフィックを受け取る側の VLAN を設定します。

5 ペアのうち、トラフィックを割り付ける対象となるワイヤ モード インターフェースを「**送信インターフェース**」ドロップダウン メニューから選択します。

6 「**送信 VLAN**」に、トラフィックを割り付ける対象となる VLAN を設定します。

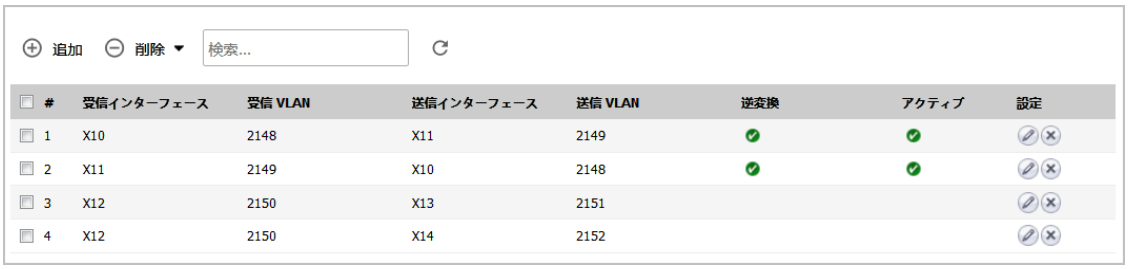
7 作成する割付のモードに応じて、以下の作業を行います。

- 単方向割付を作成する場合は、「**逆変換**」チェックボックスをオフにします。例えば、インターフェース A の VLAN X をインターフェース B の VLAN Y に割り付ける場合がこれに該当します。

  メモ：このオプションは、既定では選択されています。

- 双方向割付を作成する場合は、「**逆変換**」チェックボックスをオンにします。例えば、インターフェース B の VLAN Y をインターフェース A の VLAN X に割り付け、さらにインターフェース A の VLAN X をインターフェース B の VLAN Y に割り付ける場合がこれに該当します。

8 「**追加**」を選択します。「**ワイヤ モード VLAN 変換**」テーブルが更新されます。



VLAN 割付の管理

トピック:

- 割付の編集 (455 ページ)
- 割付のフィルタリング (455 ページ)
- 割付の削除 (456 ページ)

割付の編集

割付を編集するには、「**設定**」列の対応する「**編集**」アイコンを選択します。「**VLAN 変換の編集**」ダイアログが表示されます。割付に関しては「**逆変換**」以外のすべての設定を変更できます。

割付のフィルタリング

多数の VLAN 割付がある場合、次の操作によって、興味のある割付だけを表示できます。

1 「**検索**」フィールドにインターフェース名または VLAN タグを入力します。

2 **Enter** キーを押します。

検索条件を満たす割付だけが表示されます。

すべての割付を再表示するには、次の操作を行います。

1 「**検索フィールド**」の条件を削除します。

2 **Enter** キーを押します。

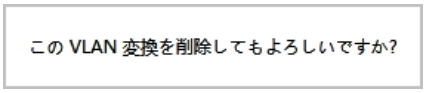
割付の削除

割付を削除するには、以下の手順に従います。

1 削除するには:

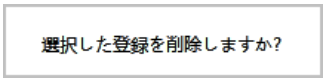
- 単一の割付を削除する場合:
  - 「設定」列の対応する**削除**アイコンを選択します。

    確認メッセージが表示されます。

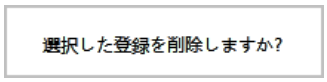
  - **対応する「選択」**チェックボックスを選択したうえで**「削除」**ドロップダウン メニューから**「選択の削除」**を選択します。

    確認メッセージが表示されます。

- 複数の割付を削除する場合は、対応するそれぞれの**「選択」**チェックボックスを選択したうえで**「削除」**ドロップダウン メニューから**「選択の削除」**を選択します。

  確認メッセージが表示されます。

- すべての割付を削除する場合は、**「すべて削除」**ドロップダウン メニューから**「選択の削除」**を選択します。

  確認メッセージが表示されます。

2 **「OK」**を選択します。

双方向のポリシーでは、一方を削除すると両方の方向が削除されます。

19

DNS の設定

トピック:

- ネットワーク > DNS (457 ページ)
  - 分割 DNS について (457 ページ)
  - DNS サーバの管理 (459 ページ)
  - DNS と IPv4 (467 ページ)

ネットワーク > DNS

ドメイン ネーム システム (DNS) は、覚えにくい数値の IP アドレスではなく、完全修飾ドメイン (FQDN) と呼ばれる英数字の名前を使ってインターネット上のホストを識別する、分散型の階層システムです。「**管理 | システム セットアップ | ネットワーク > DNS**」では、必要に応じて DNS 設定を手動で構成できます。

メモ：SonicOS の IPv6 実装の詳細については、「IPv6 (979 ページ)」を参照してください。

トピック:

- 分割 DNS について (457 ページ)
- DNS サーバの管理 (459 ページ)
- DNS と IPv4 (467 ページ)

分割 DNS について

分割 DNS は、一連のサーバを設定してそれらを特定のドメイン名 (ワイルドカードも使用可能) に関連付けられるようにする拡張機能です。SonicOS がドメイン名と一致するクエリを受信すると、指定された DNS サーバにその名前が送信されます。「分割 DNS の例」はこのしくみを示したものです。

分割 DNS の例

- このトポロジでは、2 台のファイアウォールがネットワークに接続されています。
  - 1 台のファイアウォールはインターネットに接続されています。
  - もう 1 台は企業ネットワークに接続された VPN トンネルです。
- 既定の DNS クエリはパブリック ISP の DNS サーバに送信されます。
- *.sonicwall.com に対するすべてのクエリは、VPN トンネルの背後にある DNS サーバに送信されます。

分割 DNS エントリの表示と設定については、「分割 DNS 用のドメイン固有 DNS サーバの設定 (462 ページ)」を参照してください。

分割 DNS エントリを追加すると、sonicwall.com に対するすべてのクエリは特定のサーバに送信されます (「分割 DNS 用のドメイン固有 DNS サーバの設定 (462 ページ)」を参照してください)。

複数の DNS サーバを、sonicwall.com に対するクエリを処理するように設定することもできます。

パーティションごとの DNS サーバと分割 DNS について

認証パーティションの有無に関係なく、通常はドメイン独自の DNS サーバを使用してそのドメイン内にある機器の名前を解決する必要があります。また、ときには異なる外部 DNS サーバを使用した外部ホスト名の解決が必要になることもあります。複数の認証パーティションがある場合はさらに複雑になります。通常、複数のパーティション内のホスト名を解決するには複数の DNS サーバを使用する必要があるからです。

メモ：通常、LDAP 紹介では、LDAP サーバが IP アドレスによって設定されていても DNS 名で参照先サーバを示すため、ドメイン独自の DNS サーバの使用が予期せず必要となる場合があります。

また、異なる外部 DNS サーバを使用した外部ホスト名の解決が必要になる例として、内部ドメインの DNS サーバでは解決できない外部使用クラウド サービスが関係している場合があります。

分割 DNS 機能を SonicWall セキュリティ装置から直接使用するのは、ドメイン内の機器の名前を解決するとき DNS プロキシを有効化する必要がない場合です。例えば、関連性のない複数のドメインで認証パーティション処理を行う場合などが該当します。

分割 DNS で設定された DNS サーバは、次のように、内部ドメイン内のホスト名の DNS 検索に直接使用されます。

- これは、セキュリティ装置のメイン DNS キャッシュ内にエントリのあるすべてに適用されます。
  - SMTP サーバ
  - Syslog サーバ
  - ウェブ プロキシ サーバとユーザ (内部) プロキシ サーバ
  - GMS と GMS スタンバイ
  - POP サーバ
  - RADIUS 認証サーバとアカウント サーバ
  - LDAP サーバ
  - SSO / ターミナル サービス エージェントと RADIUS アカウント クライアント
- パーティション処理が有効になっていて、1 つのパーティションに 1 つのドメインまたは親/サブドメインの 1 つのツリー (1 つの AD フォレスト) が割り当てられている場合、パーティションの最上位ドメインに分割 DNS サーバを設定すると、それらは内部パーティション構造にコピー

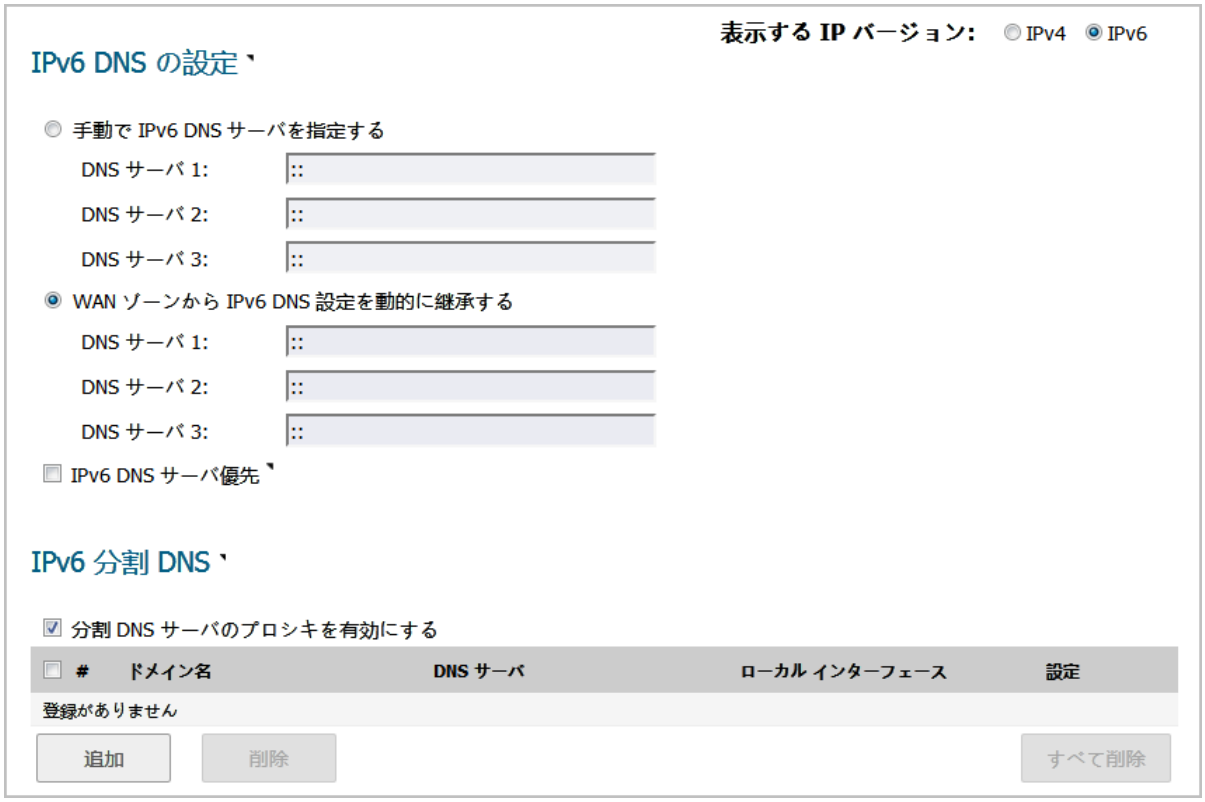
されます。それらの DNS サーバは、パーティション内のエージェント、サーバ、クライアントの名前の解決に使用されます。

- パーティション処理が有効になっていて、1 つのパーティションに複数の別個のドメインが設定されている場合 (これは可能ですが、一般的ではありません)、どの DNS サーバもパーティション構造にコピーされず、以下で説明するメカニズムが適用されます。
- パーティション処理が無効になっているか、パーティションに DNS サーバが設定されていないか、解決する項目がパーティションに関連付けられていない場合、分割 DNS が提供する API によるリクエストごとに、使用する DNS サーバが選択されます。

DNS サーバの管理

「**ネットワーク > DNS**」のオプションは、IPv6 と IPv4 のどちらを指定するかによって異なります。次を参照してください。「IPv6 の「ネットワーク > DNS」」および「IPv4 の「ネットワーク > DNS」」。

IPv6 の「ネットワーク > DNS」



IPv4 の「ネットワーク > DNS」

どちらのバージョンの管理インターフェース ページも「**DNS の設定**」、「**分割 DNS**」、および「**TCP を介した FQDN 用 DNS ホスト名検索**」セクションは共通なので、まとめて説明します。

トピック:

- IP バージョンの選択 (461 ページ)
- 使用する DNS サーバの指定 (461 ページ)
- 分割 DNS 用のドメイン固有 DNS サーバの設定 (462 ページ)
- 「TCP を介した FQDN 用 DNS ホスト名検索」の有効化 (466 ページ)

IP バージョンの選択

IP バージョンを選択するには:

1 「**管理 | システム セットアップ > ネットワーク > DNS**」に移動します。

2 ページの右上にある「**表示する IP バージョン**」で、以下のいずれかを選択します。

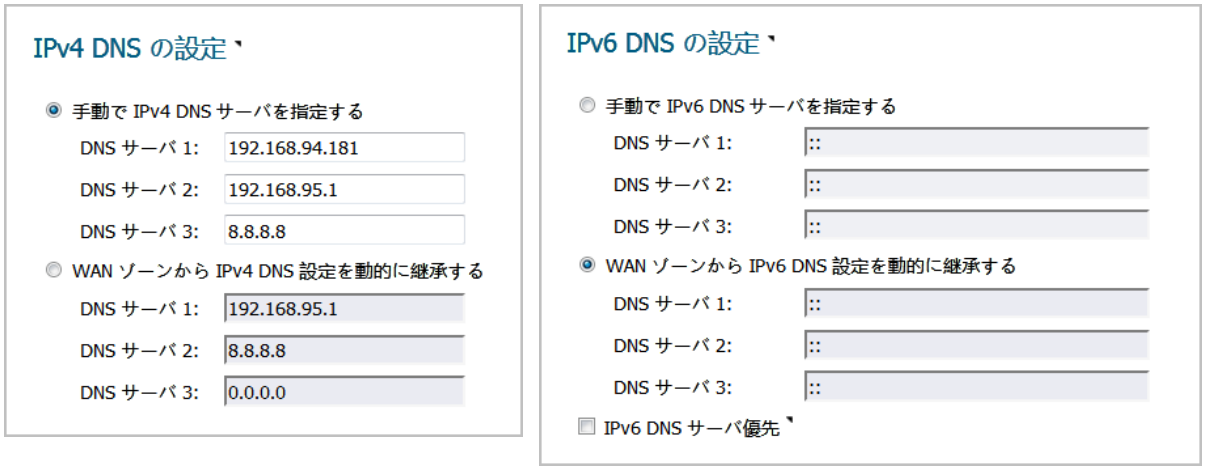
- **IPv4**
- **IPv6**

「**ネットワーク > DNS**」のオプションは、IPv6 と IPv4 のどちらを指定するかによって異なります。「IPv6 の「ネットワーク > DNS」」テーブルと「IPv4 の「ネットワーク > DNS」」テーブルを参照してください。

使用する DNS サーバの指定

IP バージョンに関係なく、SonicOS による DNS サーバの選択方法を指定できます。この方法はどちらの IP バージョンでも同じです。

「IPv4 DNS の設定」/「IPv6 DNS の設定」セクション



使用する DNS サーバを指定するには:

1 「**ネットワーク > DNS**」に移動します。

2 「**IPv4/IPv6 DNS の設定**」セクションで、次のいずれかを選択します。

- 手動で DNS サーバを指定するには:
  a) 「**手動で IPv4/IPv6 DNS サーバを指定する**」を選択します。
  b) 「**DNS サーバ**」フィールドに IP アドレスを最大 3 つ入力します。
  c) 次の手順に従います。
    - IPv4 を使用する場合は、「ステップ 4」に進みます。
    - IPv6 を使用する場合は、「ステップ 3」に進みます。
- WAN ゾーン用に設定された DNS 設定を使用するには:

a) 「**WAN ゾーンから IPv4/IPv6 DNS 設定を動的に継承する**」オプションを選択します。このオプションは既定の設定です。「**DNS サーバ**」フィールドに、IP アドレスが自動的に入力されます。

b) IPv4 を使用する場合は、「ステップ 4」に進みます。

3 IPv6 サーバのみを使用するには、「**IPv6 DNS サーバ優先**」を選択します。このオプションは、既定では選択されていません。

SonicOS DNS は、次の種類のサーバをサポートしています。

- DNS_SYSTEM_BEHAVIOR - システムの既定の動作。このオプションの設定に依存します。
- DNS_PREFER_V4_DNSSERVER - 障害が発生しない限り IPv4 DNS サーバを優先し、障害が発生した場合に IPv6 DNS サーバを要求します。
- DNS_PREFER_V6_DNSSERVER - 障害が発生しない限り IPv6 DNS サーバを優先し、障害が発生した場合に IPv4 DNS サーバを要求します。

注意：IPv6 DNS サーバを適切に設定済みである場合に限り、このオプションを選択してください。

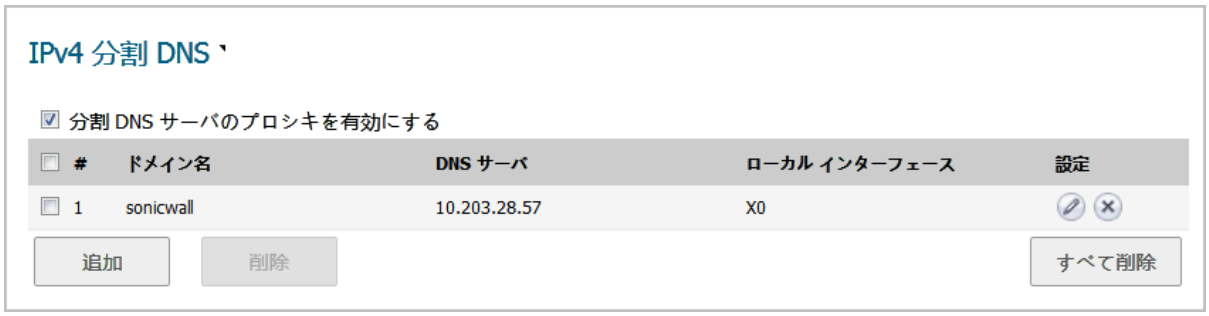
4 「**適用**」を選択して変更を保存します。

分割 DNS 用のドメイン固有 DNS サーバの設定

必要に応じて、IPv6 または IPv4 で使用する個別のドメイン固有 DNS サーバを設定することができます。この方法はどちらの IP バージョンでも同じです。相違点にご注意ください。

「IPv6 分割 DNS」セクション

「IPv4 分割 DNS」セクション



ドメイン名	DNS サーバの名前。
DNS サーバ	DNS サーバの IPv4/IPv6 IP アドレス。 **メモ：** DNS サーバの状況は、「**ネットワーク > DNS プロキシ**」ページに表示されます。
ローカル インターフェース	DNS サーバに割り当てられているインターフェース
設定	各サーバについて**編集**アイコンと**削除**アイコンが表示されます。

トピック:

- DNS サーバの追加 (463 ページ)
- 分割 DNS エントリの編集 (465 ページ)
- 分割 DNS エントリの削除 (466 ページ)

DNS サーバの追加

ドメイン固有 DNS サーバを追加し、そのサーバを所定のドメイン名に関連付けるには:

重要：分割 DNS の最大エントリ数は 32 です。リストがいっぱいになった場合、新しいエントリは追加できません。

1 「**管理 | システム セットアップ > ネットワーク > DNS**」に移動します。

2 「**表示する IP バージョン**」で IP バージョンを選択します。

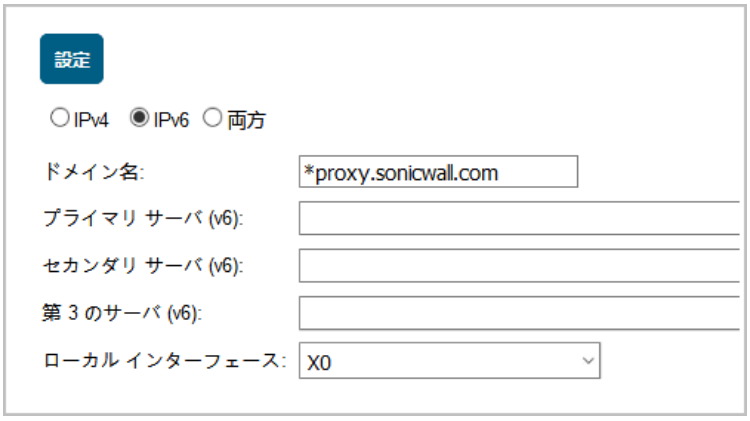
3 分割 DNS サーバのプロキシを有効にするには、「**分割 DNS サーバのプロシキを有効にする**」を選択します。このオプションは、既定では選択されています。

4 「**分割 DNS**」テーブルの下にある「**追加**」を選択します。「**分割 DNS 登録の追加**」ダイアログが表示されます。

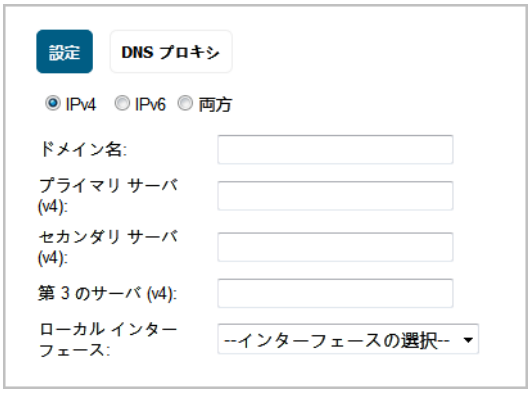
ヒント：DNS プロキシを選択した場合は、そのためのページ「**DNS プロキシ**」も「**分割 DNS 登録の追加**」ダイアログ上に表示されます。

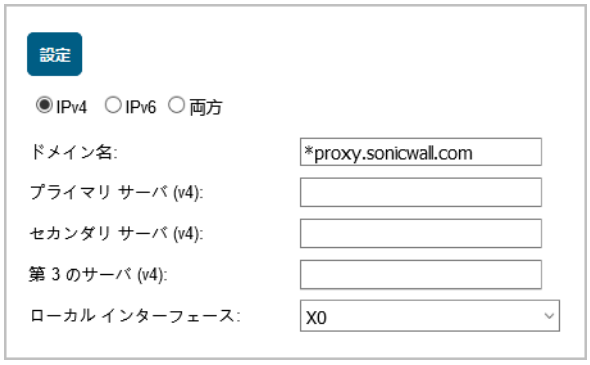
IPv6 の分割 DNS 登録の追加-DNS プロキシ有効

IPv6 の分割 DNS 登録の追加-DNS プロキシ無効



IPv4 の分割 DNS 登録の追加





IPv6 と IPv4 の分割 DNS 登録の追加-DNS プロキシ有効

5 IP バージョンを選択します。

- **IPv4**
- **IPv6**

- **両方**

6 「**ドメイン名**」フィールドにドメイン名を入力します。この名前にはワイルドカード (*) を含めることができます (例: *.SonicWall.com)。

7 このドメインに対して 1 つ以上の IPv4/IPv6 分割 DNS サーバを設定するには、該当するフィールドに IP アドレスを入力します。

- **プライマリ サーバ (v4/v6)**
- **セカンダリ サーバ (v4/v6)** (オプション)
- **第 3 のサーバ (v4/v6)** (オプション)

8 「**ローカル インターフェース**」からインターフェースを選択します。

9 DNS プロキシを有効にしていない場合は、「ステップ 13」に進みます。

10 「**DNS プロキシ**」を選択します。

11 持続時間を指定するには、「**DNS 応答の TTL 値を手動で設定する**」を選択します。このオプションは、既定では選択されていません。このオプションが選択されていない場合、TTL 値はDNS 応答の値と同じです。設定されている場合、TTL 値は設定値と同じです。

メモ：このオプションは、DNS プロキシで分割 DNS が使用される場合にのみ適用されます。

12 キャッシュ エントリの最大持続時間を入力します。最小値は 1 秒、最大値は 9999999999999999 秒です。

13 「**OK**」を選択します。

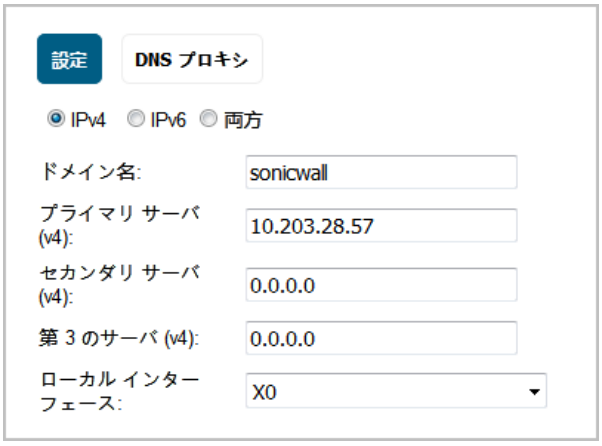
ヒント：DNS サーバの設定時にどの IP バージョンを選択したかに関係なく、両方の IP バージョンの「**分割 DNS**」テーブルに DNS サーバが表示されます。

分割 DNS エントリの編集

分割DNS エントリを編集するには、以下の手順に従います。

1 「**管理 | システム セットアップ > ネットワーク > DNS**」に移動します。

2 「**分割 DNS**」テーブルで、エントリの**編集**アイコンを選択します。「**分割 DNS 登録の編集**」ダイアログが表示されます。



3 変更を加えます。

4 「**OK**」を選択します。

分割 DNS エントリの削除

分割 DNS エントリを削除するには、以下の手順に従います。

1 エントリの**削除**アイコンを選択します。

2 つ以上の分割 DNS エントリを削除するには、以下の手順に従います。

1 削除するエントリのチェックボックスをオンにします。「**削除**」が使用可能になります。

2 「**削除**」を選択します。

すべての分割 DNS エントリを削除するには、以下の手順に従います。

1 「**すべて削除**」を選択します。

「TCP を介した FQDN 用 DNS ホスト名検索」の有効化

既定では、DNS クエリは UDP で送信されます。応答の長さが UDP で許可される最大値を超える場合、DNS の応答に Truncated (切り捨て) フラグが含まれる場合があります。

「**TCP を介した FQDN 用 DNS ホスト名検索を有効にする**」オプションが

- 有効化されていて、DNS の応答に Truncated フラグが設定されている場合、SonicOS は、追加の DNS クエリを TCP で送信し、複数の IP アドレスに対して完全な DNS 応答を決定します。
- このオプションが無効の場合、DNS クエリは UDP で送信され、SonicOS は、応答に Truncated フラグの設定があっても DNS 応答のパケットに含まれる IP アドレスの処理のみを行います。

TCP による DNS 応答を DNS サーバから受信できない場合、DNS クエリは 1 秒後にタイムアウトします。

このオプションは、セキュリティ装置が UDP 経由で DNS 応答を受信している間に、FQDN から TCP を介して DNS クエリを送信するとき、より多くの IP アドレスを取得するために使用されます。

「TCP を介した FQDN 用 DNS ホスト名検索」を有効化するには:

1 「**管理 | システム セットアップ > ネットワーク > DNS**」に移動します。

2 「**TCP を介した FQDN 用 DNS ホスト名検索**」セクションまでスクロールします。

3 「**TCP を介した FQDN 用 DNS ホスト名検索を有効にする**」を選択します。このオプションは、既定では選択されていません。

4 「**適用**」を選択します。

DNS と IPv4

IPv4 の「**ネットワーク > DNS**」ページには、IPv6 の「**ネットワーク > DNS**」ページと共通のセクションの他に、以下のセクションがあります。

- DNS 再割り当て攻撃の防御 (468 ページ)
- FQDN に対する DNS の割り当て (469 ページ)
- DNS キャッシュ (469 ページ)

DNS 再割り当て攻撃の防御

DNS 再割り当ては、ウェブ ページに埋め込まれたコードに対する DNS ベースの攻撃です。通常、ウェブ ページに埋め込まれたコード (JavaScript、Java、および Flash) からの要求は、その発信元のウェブ サイトにバインドされます (「同一発信元ポリシー」を参照)。DNS 再割り当て攻撃によって、プライベート ネットワークに侵入する JavaScript ベースのマルウェアの能力が高められ、ブラウザの同一発信元ポリシーが覆されることがあります。

DNS 再割り当て攻撃者は、自らが制御する DNS サーバに委託されるドメインを登録します。このサーバは、非常に短い持続時間 (TTL) パラメータで応答するように設定されているため、結果がキャッシュされません。最初の応答には、悪意のあるコードをホストしているサーバの IP アドレスが含まれます。その後の要求には、プライベート (RFC 1918) ネットワークからの IP アドレスが含まれます。このネットワークはおそらくファイアウォールの後ろにあり、攻撃者のターゲットになります。どちらも完全に有効な DNS 応答であるため、これによってサンドボックス スクリプトにプライベート ネットワーク内のホストへのアクセスが許可されます。このような短期的ながら有効な DNS 応答でアドレスを繰り返すことによって、スクリプトがネットワーク内をスキャンし、他の悪意ある動作を実行することができます。

DNS 再割り当て攻撃の防御を設定するには、以下の手順を実行します。

1 「**ネットワーク > DNS**」に移動します。

2 「**DNS 再割り当て攻撃の防御**」セクションまでスクロールします。

3 「**DNS 再割り当て攻撃の防御を有効にする**」を選択します。このオプションは、既定では選択されていません。2 つのオプションが使用可能になります。

4 「**動作**」から、DNS 再割り当て攻撃が検知されたときに実行する動作を選択します。

- **攻撃をログする** (既定)
- **攻撃をログし、クエリ拒否応答を返す**
- **攻撃をログし、DNS 応答を破棄する**

5 「**許可ドメイン**」から、許可するドメイン名を含む FQDN アドレス オブジェクトや FQDN アドレス オブジェクト グループ (`*.SonicWall.com` など) を選択します。これらのオブジェクトやオブジェクト グループについては、ローカルに接続/ルーティングされるサブネットを正当な応答と見なします。

「**新しい FQDN アドレス オブジェクトを作成する...**」または「**新しい FQDN アドレス オブジェクト グループを作成する...**」を選択して、新しい FQDN アドレス オブジェクトや FQDN アドレス オブジェクト グループを作成することもできます。

6 「**適用**」を選択します。

FQDN に対する DNS の割り当て

FQDN に対する DNS の割り当てを有効にするには:

1 「**ネットワーク > DNS**」に移動します。

2 「**FQDN に対する DNS の割り当て**」セクションまでスクロールします。

3 「**FQDN オブジェクトは承認済みサーバからの DNS 応答のみをキャッシュする**」をオンにします。このオプションは、既定では選択されていません。

4 「**適用**」を選択します。

DNS キャッシュ

通常 DNS キャッシュの内容を表示するには、「**DNS キャッシュの表示**」を選択します。ポップアップにキャッシュの内容が表示されます。

対象	DNS サーバ名: • 正引き DNSキャッシュ、ホスト名。 • 逆引き DNS キャッシュ、IP アドレスの文字列表現。
DNS 名	ドメイン名 (`www.SonicWall.com` など) または IP アドレス。
IP アドレス	解決結果 IP アドレス
TTL (秒)	持続時間 (TTL)。DNS 応答からの TTL 値。
消去	選択すると、サーバの DNS キャッシュ エントリが消去されます。
すべて消去	選択すると、表示されているすべてのサーバのすべての DNS キャッシュ エントリが消去されます。

20

DNS プロキシの設定

トピック:

- ネットワーク > DNS プロキシ (471 ページ)
  - DNS プロキシについて (472 ページ)
  - DNS プロキシの有効化 (475 ページ)
  - DNS プロキシの設定 (476 ページ)
  - DNS サーバ状況の監視 (477 ページ)
  - 分割 DNS サーバの状況の監視 (477 ページ)
  - 静的 DNS キャッシュ エントリの表示と管理 (478 ページ)
  - DNS プロキシ キャッシュ エントリの表示 (479 ページ)

ネットワーク > DNS プロキシ

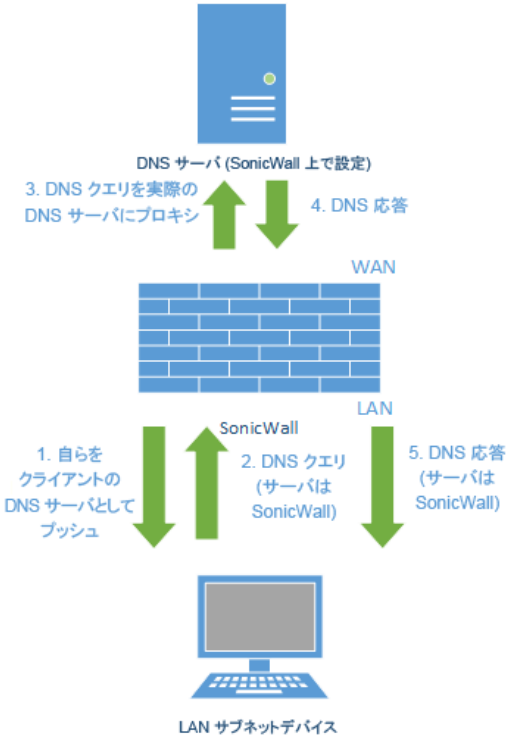
トピック:

- DNS プロキシについて (472 ページ)
- DNS プロキシの有効化 (475 ページ)
- DNS プロキシの設定 (476 ページ)
- DNS サーバ状況の監視 (477 ページ)
- 分割 DNS サーバの状況の監視 (477 ページ)
- DNS プロキシ キャッシュ エントリの表示 (479 ページ)
- 静的 DNS キャッシュ エントリの表示と管理 (478 ページ)

DNS プロキシについて

IPv4 インターフェースは IPv4 インターネット上で名前解決を行うことができます。IPv6 インターフェースは、DNS プロキシを通じてのみ IPv6 インターネット上で名前解決を行うことができます。IPv4 と IPv6 が混在するネットワーク内の DNS サービスに IPv4 クライアントがアクセスできるように、SonicOS は DNS プロキシをサポートしています。「DNS プロキシ」を参照してください。

DNS プロキシ



DNS プロキシ機能は、機器がクライアントに代わってホスト名解決要求をプロキシできる、トランスペアレントなメカニズムを提供します。このプロキシでは、既存の DNS キャッシュを使用できます。このキャッシュは、クエリに対して直接応答するように、管理者によって静的に設定されたものか、動的に学習されたもののどちらかです。

このプロキシは、特定の DNS サーバに対する DNS クエリのリダイレクトを、部分的なドメイン指定または完全なドメイン指定に従って選択的に行うことができます。これは、VPN トンネルまたは PPPoE 仮想リンクが複数のネットワーク接続を提供していて、一部の DNS クエリをあるネットワークに、その他のクエリを別のネットワークに誘導する必要がある場合に便利です。

DNS プロキシを利用している場合、LAN サブネットの機器は SonicWall セキュリティ装置を DNS サーバとして使用し、DNS クエリをこのセキュリティ装置に送信します。セキュリティ装置は、DNS クエリを実際の DNS サーバにプロキシします。このように、セキュリティ装置は、ネットワークの DNS トラフィックにとって中心的な管理ポイントであり、ネットワークの DNS クエリを 1 か所で管理できるようにします。

メモ：セキュリティを維持するために、受信 DNS クエリのプロキシは、アクセス ルールと DPI によるチェック後にのみ行われます。

インターフェースで DNS プロキシを有効にすると、SonicOS によって 1 つの許可ルールが自動的に追加されます。インターフェースに関連付けられているアクセス ルールについては、『*SonicOS ポリシー*』を参照してください。

「**TCP 経由の DNS プロキシ**」が有効になっていると、別の許可ルールが自動的に追加されます。

トピック:

- サポートされているインターフェース (473 ページ)
- DNS サーバのライブネス検知とフェイルオーバー (473 ページ)
- DNS キャッシュ (473 ページ)
- DHCP サーバ (474 ページ)
- ログの設定の有効化 (474 ページ)
- パケットの監視 (474 ページ)

サポートされているインターフェース

DNS プロキシ機能は、物理インターフェース、VLAN インターフェース、または VLAN トランク インターフェースでサポートされています。各インターフェースのゾーンには LAN、DMZ、または WLAN のみを使用できます。

DNS サーバのライブネス検知とフェイルオーバー

複数の DNS サーバが設定されている場合に「最適」なサーバを決定するために、SonicOS は以下の要因を考慮します。

- DNS サーバの優先順位
- DNS サーバの状況 (稼働中、休止中、不明)
- フェイルオーバー後の経過時間

DNS キャッシュ

DNS プロキシでは、よく使用されるドメインやホスト アドレスが DNS キャッシュ メモリに保存されます。DNS キャッシュ内のドメインに一致する DNS クエリを受け取ると、セキュリティ装置は、DNS クエリや応答プロキシの処理を行わずに、キャッシュ レコードを使用してクライアントに直接応答を返します。

DNS キャッシュには次の 2 種類があります。

静的	管理者が手動で設定します。
動的	SonicOS によって自動学習されます。それぞれの DNS クエリについて、SonicOS DNS プロキシは、URI に対する精密検査を行い、有効な応答をキャッシュに記録します。

DNS クエリが既存のキャッシュ エントリに一致した場合、SonicOS DNS プロキシはキャッシュに記録されている URI を用いて直接応答を返します。これにより、通常はネットワーク トラフィックが減少し、結果としてネットワークの全体的なパフォーマンスが向上します。

最大 DNS プロキシ キャッシュ サイズ

静的 DNS プロキシ キャッシュ サイズ

静的 DNS プロキシ キャッシュ エントリのサイズは、プラットフォームに関係なく、常に 256 です。静的 DNS キャッシュは、手動で削除しない限り、決して削除されません。

動的 DNS プロキシ キャッシュ サイズ

動的 DNS プロキシ キャッシュ サイズは、「動的キャッシュ サイズ」テーブルに示すように、プラットフォームによって異なります。

動的キャッシュ サイズ

プラットフォーム	最大キャッシュ サイズ
SM 9600/SM 9400	4096
SM 9200	2048
NSA 6600/NSA 5600/NSA 4600	2048
NSA 3600/NSA 2600/NSA 2650	1024
TZ600	512
TZ500/TZ500 W/TZ400/TZ400 W/TZ350/ TZ350 W/TZ300/TZ300 W	512
SOHO 250/SOHO 250 W/SOHO W	512

セキュリティ装置が DNS プロキシ キャッシュにエントリを追加しようとしたとき、プロキシ キャッシュが最大サイズに達していた場合、セキュリティ装置は次の処理を行います。

1 有効期限が最も近い DNS プロキシ キャッシュ エントリを削除します。

2 新しい DNS プロキシ キャッシュ エントリを追加します。

DNS キャッシュの高可用性ステートフル同期

DNS プロキシは DNS プロキシ キャッシュのステートフル同期をサポートしています。DNS プロキシ キャッシュが追加、削除、または動的に更新された場合、DNS プロキシ キャッシュはアイドル状態のセキュリティ装置との同期をとります。

DHCP サーバ

あるインターフェースで DNS プロキシが有効になっている場合、機器はそのインターフェース IP を DNS サーバ アドレスとしてクライアントにプッシュする必要があるので、DHCP サーバの設定は、「**DNS/WINS**」タブの「**DHCP サーバ**」設定でそのインターフェース アドレスを「**DNS サーバ 1**」のアドレスとして使用して、手動で行う必要があります。「**動的範囲の設定**」ダイアログの「**インターフェースの事前設定**」オプションを使用すると、この設定を簡単に行うことができます。選択したインターフェースで DNS プロキシが有効になっている場合、「DNS/WINS」ページに DNS サーバの IP が自動的に追加されます。DHCP サーバの静的な設定方法については、「静的 DHCP 登録の設定 (577 ページ)」を参照してください。

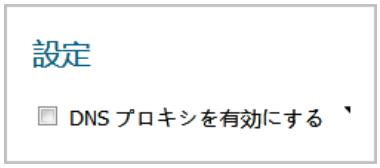
ログの設定の有効化

DNS プロキシには複数のログが関連しています。これらのロ グは *SonicOS 調査*の説明に従って設定する必要があります。

パケットの監視

DNS プロキシの処理は「ダッシュボード > パケット監視」で監視できます。パケット監視については、『*SonicOS 調査*』を参照してください。

DNS プロキシの有効化



DNS プロキシの有効化は、まず「**ネットワーク > DNS プロキシ**」ページで行ってから、各インターフェースに対して行う必要があります。これにより、異なるネットワーク セグメントに対してこの機能を個別に有効化する段階的な制御を実現できます。

DNS プロキシを有効にするには、以下の手順に従います。

1 「**ネットワーク > DNS プロキシ**」に移動します。

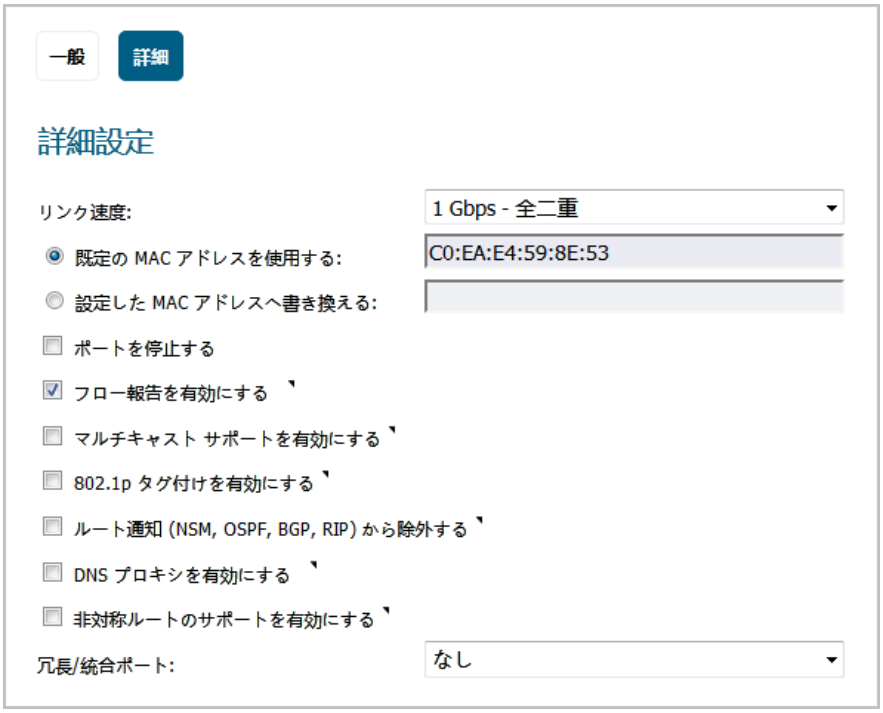
2 「**DNS プロキシを有効にする**」を選択します。このオプションは、既定では選択されていません。

3 「**適用**」を選択します。

4 「**ネットワーク > インターフェース**」に移動します。

5 DNS プロキシを有効にするインターフェースの**編集**アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。

6 「**詳細設定**」を選択します。



7 「**DNS プロキシを有効にする**」を選択します。このオプションは、DNS プロキシがグローバルで有効になっている場合にのみ表示されます。

8 「**OK**」を選択します。

9 DNS プロキシを有効にするインターフェースのそれぞれについて、「ステップ 5」～「ステップ 8」を繰り返します。

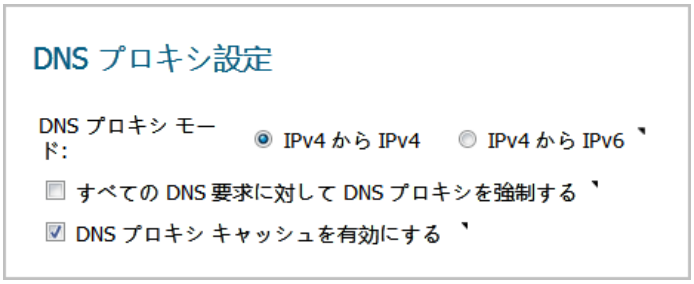
10 「**適用**」を選択します。

インターフェースに関連付けられているアクセス ルールについては、『*SonicOS ポリシー ガイド*』を参照してください。

DNS プロキシの設定

DNS プロキシを設定するには、以下の手順に従います。

1 「**ネットワーク > DNS プロキシ | DNS プロキシ設定**」に移動します。



2 「**DNS プロキシ モード**」で、セキュリティ装置と DNS サーバとの間で DNS プロキシ パケットを送受信するための IP バージョンを選択します。

- **IPv4 から IPv4** (既定)
- **IPv4 から IPv6**

3 SonicOS から送られてきたスタック DNS パケットも含め (送信先アドレスに外部の DNS サーバが設定された DNS クエリを転送する場合など)、あらゆる種別の DNS 要求が DNS プロキシで処理されるようにするには、「**すべての DNS 要求に対して DNS プロキシを強制する**」を選択します。このオプションが無効になっている場合は、SonicWall セキュリティ装置宛ての要求のみが処理されます。このオプションは、既定では選択されていません。

ⓘ **メモ**：このオプションは UDP 経由の DNS にのみ影響します。このオプションを選択しない場合は、SonicWall セキュリティ装置宛ての DNS プロキシ要求のみが有効になります。

4 UDP 経由の DNS 要求のみの場合は、「**DNS プロキシ キャ ッ シュを有効にする**」を選択します。このオプションは、既定では選択されています。

5 「**適用**」を選択します。

ⓘ **メモ**：DNS プロキシ プロトコルなど、いくつかの高度な設定項目を設定できます。これらの設定の詳細については、テクニカル サポートにお問い合わせください。

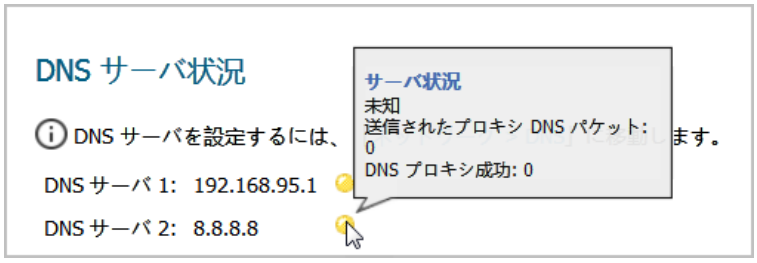
DNS サーバ状況の監視

メモ：設定済みの DNS サーバには IP アドレスが表示されます。設定されていないサーバの IP アドレスは 0.0.0.0 になっています。サーバを設定するには、「**ネットワーク > DNS**」へのリンクを選択します。「DNS の設定 (457 ページ)」を参照してください。

設定済みの各上流 DNS サーバの状況の監視は、「**DNS サーバ状況**」セクションで行います。サーバの状況は、そのサーバからの DNS 応答によって決定されます。

稼働中 (緑色の LED)	応答は成功しました。
不明 (黄色の LED)	DNS 応答がサーバに届いていません。
休止中 (赤色の LED)	エラーのカウント数が上限である 20 を超えました。状況は、DNS 応答が次に成功するまでは休止中のままになります。

マウス ポインタを LED 表示の上に移動すると、プロキシされた DNS パケットの送信数や DNS プロキシ クエリの成功数に関する詳細情報を示すポップアップが表示されます。



分割 DNS サーバの状況の監視

メモ：設定済みの分割 DNS サーバには IP アドレスが表示されます。分割サーバを設定するには、「**ネットワーク > DNS**」へのリンクを選択します。「DNS の設定 (457 ページ)」を参照してください。

設定済みの各上流 DNS サーバの状況の監視は、「**分割 DNS**」セクションで行います。サーバの状況は、そのサーバからの DNS 応答によって決定されます。

稼働中 (緑色の LED)	応答は成功しました。
不明 (黄色の LED)	DNS 応答がサーバに届いていません。
休止中 (赤色の LED)	エラーのカウント数が上限である 20 を超えました。状況は、DNS 応答が次に成功するまでは休止中のままになります。

マウス ポインタを LED 表示の上に移動すると、プロキシされた DNS パケットの送信数や DNS プロキシ クエリの成功数に関する詳細情報を示すポップアップが表示されます。

静的 DNS キャッシュ エントリの表示と管理

ドメイン名	ドメインの名前。
IPv4 アドレス 1	静的 DNA キャッシュのプライマリ IPv4 アドレス。指定されていない場合は 0.0.0.0 となります。
IPv4 アドレス 2	静的 DNA キャッシュのセカンダリ IPv4 アドレス。指定されていない場合は 0.0.0.0 となります。
IPv6 アドレス 1	静的 DNA キャッシュのプライマリ IPv6 アドレス。指定されていない場合は :: となります。
IPv6 アドレス 2	静的 DNA キャッシュのセカンダリ IPv6 アドレス。指定されていない場合は :: となります。
設定	エントリごとに**編集**アイコンと**削除**アイコンがあります。

静的DNS キャッシュ エントリを追加するには、以下の手順に従います。

1 「**ネットワーク > DNS プロキシ**」に移動します。

2 「**静的 DNS プロキシ キャッシュ登録**」までスクロールします。

3 テーブルの上下どちらかにある「**追加**」を選択します。「**静的 DNS キャッシュの追加**」ダイアログが表示されます。

4 「**ドメイン名**」フィールドに名前を入力します。

5 IPv4 静的 DNS キャッシュの場合は、「**IPv4 アドレス 1**」フィールドにプライマリ IPv4 アドレスを入力します。

6 必要に応じて、IPv4 静的 DNS キャッシュでは「**IPv4 アドレス 2**」フィールドにセカンダリ IPv4 アドレスを入力します。

7 IPv6 静的 DNS キャッシュの場合は、「**IPv6 アドレス 1**」フィールドにプライマリ IPv6 アドレスを入力します。

8 必要に応じて、IPv6 静的 DNS キャッシュでは「**IPv6 アドレス 2**」フィールドにセカンダリ IPv6 アドレスを入力します。

9 「**OK**」を選択します。

10 別の静的 DNS キャッシュ エントリを追加する場合は、「ステップ 4」から「ステップ 9」を繰り返します。

11 「**キャンセル**」を選択します。

静的 DNS キャッシュ エントリの削除

静的DNS キャッシュ エントリを削除するには、以下の手順に従います。

1 エントリの**削除**アイコンを選択します。

2 つ以上の静的DNS エントリを削除するには、以下の手順に従います。

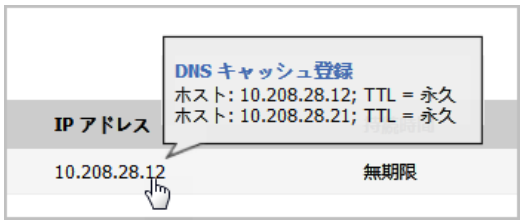
1 削除するエントリのチェックボックスをオンにします。「**削除**」が使用可能になります。

2 「**削除**」を選択します。

すべての静的DNS エントリを削除するには、以下の手順に従います。

1 「**すべて削除**」を選択します。

DNS プロキシ キャッシュ エントリの表示

表示する IP バージョン	**IPv4** または **IPv6** のどちらかを選択します。
ドメイン名	DNS サーバの名前。
種別	**動的** **静的**
IP アドレス	DNS サーバの IPv4 または IPv6 アドレス。マウス ポインタをエントリの上に移動すると、そのエントリの**ホスト**と持続時間 (**TTL**) の情報が表示されます。 
持続時間	次のどちらかを行います。 • ***n 分 x 秒*後に失効** (動的 DNS) • **失効** (動的 DNS) • **無期限** (静的 DNS)
消去	各エントリの**消去**アイコン。

動的 DNS キャッシュは DNS プロキシ処理時に自動的に追加されます。静的 DNS キャッシュは設定時に追加されます。動的 DNS キャッシュは TTL 値を持ち、消去が可能です。静的 DNS キャッシュは削除する必要があります。「静的 DNS キャッシュ エントリの削除 (479 ページ)」を参照してください。

動的 DNS キャッシュ エントリの消去

動的 DNS キャッシュ エントリを消去するには、以下の手順に従います。

1 エントリの**消去**アイコンを選択します。

2 つ以上の動的 DNS エントリを消去するには、以下の手順に従います。

1 削除するエントリのチェックボックスをオンにします。「**消去**」が使用可能になります。

2 「**消去**」を選択します。

すべての動的 DNS キャッシュ エントリを消去するには、以下の手順に従います。

1 「**すべて消去**」を選択します。

21

DNS セキュリティの設定

トピック:

- シンクホールについて (481 ページ)
- ネットワーク > DNS セキュリティ (481 ページ)
  - DNS セキュリティの設定を構成する (482 ページ)
  - リスト内のエントリの削除 (483 ページ)

シンクホールについて

DNS シンクホールは、シンクホール サーバ、インターネット シンクホール、または BlackholeDNS とも呼ばれ、それに対応するドメイン名の使用を防ぐために偽情報を提供する DNS サーバです。DNS シンクホールは、悪意のあるトラフィックを検知して遮断するのに効果的であり、ボットその他の望まれていないトラフィックとの戦いに使用されます。

SonicOS は、シンクホールをブラック リストとホワイト リストで構成できるようになりました。

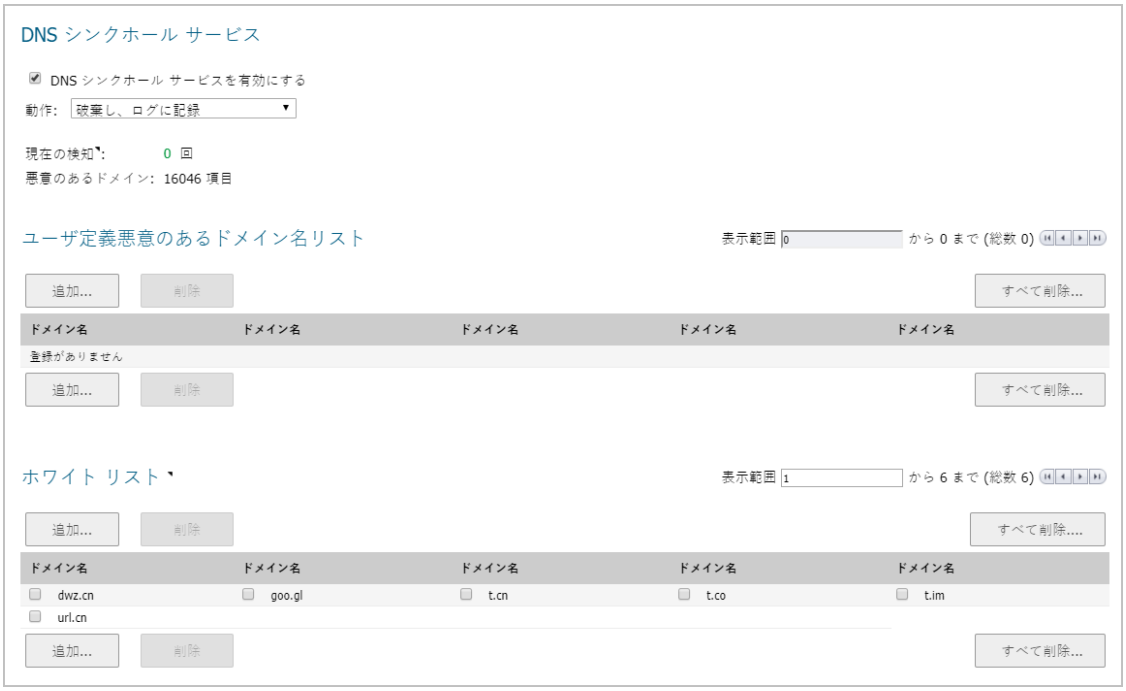
ネットワーク > DNS セキュリティ

「管理 | システム セットアップ > ネットワーク > DNS セキュリティ」では、DNS セキュリティの設定を手動で構成できます。

DNS セキュリティの設定を構成する

DNS セキュリティの設定を構成するには:

1 「**管理 | システム セットアップ > ネットワーク > DNS セキュリティ**」に移動します。



2 「**DNS シンクホール サービスを有効にする**」を選択します。このオプションは、既定では選択されています。

3 「**動作**」から、このサービスで実行する内容を選択します。

- **ログだけを記録します**
- **否定的な返信**
- **偽装 IP による返信** - 2 つのフィールドが表示されます。

a) これらのフィールドに IPv4 アドレスと IPv6 アドレスを入力します。

4 「**ユーザ定義悪意のあるドメイン名リスト**」までスクロールします。

5 「**追加**」を選択します。「**ドメイン名を 1 つ追加する**」ダイアログが表示されます。

6 「**OK**」を選択します。

7 悪意のあるドメインの名前を「**ドメイン名**」フィールドに入力します。

8 ドメイン名ごとに「ステップ 5」-「ステップ 7」を繰り返します。

9 「**ホワイト リスト**」までスクロールします。

10 「**追加**」を選択します。「**ホワイト リスト エントリを 1 つ追加する**」ダイアログが表示されます。

11 ホワイト リストに載せるドメインの名前を「**ドメイン名**」フィールドに入力します。

12 「**OK**」を選択します。

13 ドメイン名ごとに「ステップ 10」-「ステップ 7」を繰り返します。

14 「**適用**」を選択して変更を保存します。

リスト内のエントリの削除

リストのエントリを削除するには:

1 「**管理 | システム セットアップ > ネットワーク > DNS セキュリティ**」に移動します。

2 削除するエントリを選択します。「**削除**」および「**すべて削除**」が使用可能になります。

3 適切なボタンを選択します。

DNS トンネリング検知について

DNS トンネリングとは、セキュリティ制御を迂回して標的の組織からデータをこっそり抜き取る手法です。DNS トンネルは、危険にさらされている内部ホスト用の完全なリモート制御チャンネルとして使用できます。オペレーティング システム (OS) のコマンド、ファイル転送、さらに IP トンネル全体などが抜き取られる可能性があります。

SonicOS は、DNS トンネリング攻撃を検知する機能を提供しており、不審なクライアントを表示したり、DNS トンネル検知用のホワイト リストを作成したりすることができます。

DNS トンネリング検知が有効になっている場合、不審な DNS パケットが破棄されるたびに SonicOS はそれをログに記録します。

トピック:

- DNS トンネリング検知の有効化 (484 ページ)
- 検知された不審なクライアントの表示 (484 ページ)
- DNS トンネル検知用ホワイト リストの作成 (484 ページ)
- DNS トンネル検知用ホワイト リストのエントリの削除 (485 ページ)

DNS トンネリング検知の有効化

DNS トンネリング検知を設定するには:

1 「**管理 | システム セットアップ > ネットワーク > DNS セキュリティ**」に移動します。

2 「**DNS トンネル検知**」セクションまでスクロールします。

3 DNS トンネル検知を有効にするには、「**DNS トンネル検知を有効にする**」を選択します。

4 検知されたすべてのクライアントの DNS トラフィックを遮断するには、「**クライアントの DNS トラフィックをすべて遮断する**」を選択します。

5 「**適用**」を選択します。

検知された不審なクライアントの表示

SonicOS は、「**検知した不審なクライアント情報**」テーブルに DNS トンネルを確立したすべてのホストに関する情報を表示します。

ヒント：このテーブルは、DNS トンネル検知が有効になっている場合にのみデータが入力されます。ホストは、クライアントの DNS トラフィックの遮断が有効になっている場合にのみ破棄されます。「DNS トンネリング検知の有効化 (484 ページ)」を参照してください。

IP アドレス	不審なクライアントの IP アドレス。
MAC アドレス	不審なクライアントの MAC アドレス。
検知方式	不審なクライアントの検知に使用される DNS 種別: • **標準 DNS タイプ**: A、AAAA、CNAME • **特定 DNS 種別**: TXT、NULL、SRV、PRIVATE、MX など
インターフェース	DNS トンネルを確立するホストが検知されたインターフェース
遮断	ホストが遮断されたかどうかを示します

DNS トンネル検知用ホワイト リストの作成

安全と見なすことができる IP アドレスのホワイト リストを作成できます。検知された DNS トンネルの IP アドレスがホワイト リストのアドレスと一致する場合、DNS トンネル検知はバイパスされます。

DNS を作成するには:

1 「**管理 | システム セットアップ > ネットワーク > DNS セキュリティ**」に移動します。

2 「**DNS トンネル検知用ホワイト リスト**」までスクロールします。

3 「**追加**」を選択します。「**ホワイト リスト エントリを 1 つ追加する**」ダイアログが表示されます。

4 「**OK**」を選択します。

5 ホワイト リスト エントリごとに「ステップ 3」と「ステップ 4」を繰り返します。

DNS トンネル検知用ホワイト リストのエントリの削除

DNS トンネル検知用ホワイト リストのすべてのエントリを削除するには:

1 「**管理 | システム セットアップ > ネットワーク > DNS セキュリティ**」に移動します。

2 「**DNS トンネル検知用ホワイト リスト**」までスクロールします。

3 「**すべて削除**」を選択します。

DNS トンネル検知用ホワイト リストの 1 つ以上のエントリを削除するには:

1 「**管理 | システム セットアップ > ネットワーク > DNS セキュリティ**」に移動します。

2 「**DNS トンネル検知用ホワイト リスト**」までスクロールします。

3 DNS トンネル検知用ホワイト リストの 1 つ以上のエントリを選択します。「**削除**」が使用可能になります。

4 「**削除**」を選択します。

22

ルート通知とルート ポリシーの設定

重要：SD-WAN ルーティングおよびルート ポリシーについては、「SD-WAN ルート ポリシーの設定 (641 ページ)」を参照してください。

トピック:

- ルーティングについて (487 ページ)
  - メトリックと管理距離 (487 ページ)
  - ルート通知 (489 ページ)
  - ECMP ルーティング (489 ページ)
  - ポリシーベース ルーティング (489 ページ)
  - ポリシーベース TOS ルーティング (490 ページ)
  - PBR のメトリックベースの優先順位 (491 ページ)
  - ポリシー ベースのルーティングと IPv6 (491 ページ)
  - OSPF および RIP の高度なルーティング サービス (492 ページ)
  - ドロップ トンネル インターフェース (500 ページ)
- ネットワーク > ルーティング (501 ページ)
  - ネットワーク > ルーティング > 設定 (501 ページ)
  - ネットワーク > ルーティング > ルート通知 (503 ページ)
  - ネットワーク > ルーティング > OSPFv2 (504 ページ)
  - ネットワーク > ルーティング > RIP (505 ページ)
  - ネットワーク > ルーティング > OSPFv3 (506 ページ)
  - ネットワーク > ルーティング > RIPng (508 ページ)
- ルーティングの設定 (508 ページ)
  - メトリックによるルートの優先順位付け (509 ページ)
  - ルータ広告によって学習されたデフォルト ルートに対するメトリックの設定 (509 ページ)
  - ルート通知の設定 (510 ページ)
  - 静的およびポリシーベースのルートの設定 (511 ページ)
  - ドロップ トンネル インターフェースに対応する静的ルートの設定 (516 ページ)
  - OSPF および RIP の高度なルーティング サービスの設定 (517 ページ)
  - BGP の高度なルーティングの設定 (528 ページ)

ルーティングについて

SonicWall セキュリティ装置は、以下のルーティング プロトコルをサポートしています。

- RIPv1 (ルーティング情報プロトコル)
- RIPv2
- OSPFv2 (オープン ショーテスト パス ファースト)
- OSPFv3
- PBR (ポリシーベース ルーティング)

トピック:

- メトリックと管理距離 (487 ページ)
- ルート通知 (489 ページ)
- ECMP ルーティング (489 ページ)
- ポリシーベース TOS ルーティング (490 ページ)
- PBR のメトリックベースの優先順位 (491 ページ)
- ポリシー ベースのルーティングと IPv6 (491 ページ)
- OSPF および RIP の高度なルーティング サービス (492 ページ)
- ポリシー ベースのルーティングと IPv6 (491 ページ)

メトリックと管理距離

メトリックと管理距離は、ネットワーク パフォーマンス、可読性、回路選択に影響します。

メトリックについて

メトリックとは、静的ルートおよび動的ルートに割り当てられる重み付けされたコストのことです。メトリックにより、複数のルートのうち最良のもの、通常はメトリックが最小のゲートウェイが決定されます。通常、このゲートウェイがデフォルト ゲートウェイです。

メトリックは 1 から 254 までの値で指定します。「メトリック値の説明」テーブルを参照してください。低い値のほうが適切と見なされ、高い値よりも優先されます。SonicOS は、直接接続されたインターフェース、静的にエンコードされたルート、および動的な IP ルーティング プロトコルに対して Cisco が定義したメトリック値に準拠しています。

メトリック値の説明

メトリック値	説明
1	静的ルート
5	EIGRP Summary
20	External BGP
90	EIGRP
100	IGRP
110	OSPF

メトリック値の説明

メトリック値	説明
115	IS-IS
120	RIP
140	EGP
170	External EIGRP
200	内部 BGP

管理距離について

*管理距離*は、送信元が異なる 2 つの同一ルートがある場合にルートの送信元としてどちらを使用するかに影響を与える値です。管理距離の値が小さいほど、そのルートの信頼度は高くなります。

設定された管理距離は、次のためのルート選択時に ZebOS コンポーネントでのみ使用されます。

- PBR 内への登録
- ある静的ルートが特定のルーティング プロトコルから受け取ったルートと競合した際の、他のルーティング プロトコルへの再配布

管理距離は、PBR 自身内でのルートの優先順位付けには使用されません。そのため、動的ルーティングが使用中でない限り、静的ルートに対して設定されている管理距離には影響力がありません。動的ルーティングが使用されている場合、管理距離は、PBR で定義されている静的ルートと、OSPF、RIP、BGP などのプロトコルから受け取る可能性がある、その他の点では等価な動的ルートとを比較するために使用できるメカニズムを提供します。既定では、ネットワーク サービス モジュール (NSM) 内に挿入された PBR 静的ルートの管理距離は、PBR ルートで定義されているメトリックと等しくなります。必要に応じて、各静的ルートの管理距離は、管理距離に対する個別値の入力時に、異なる値に設定できます。

例えば、単純な (送信先のみの) 静的ルート (例: 送信先 = `14.1.1.0/24`) がメトリック 10 で定義されていて、管理距離が既定値である「**自動**」に設定されている場合、このルートは管理距離とメトリック 10 を用いて NSM 内に登録されます。

ここで、同じ `14.1.1.0/24` へのルートを RIP と OSPF の両方から受け取ったと仮定します。RIP ルートは既定の管理距離 120 を、OSPF ルートは 110 を持つため、既定の管理距離 (= メトリック) が 10 である静的ルートは、どちらのルートよりも優先されます。そのため、NSM は OSPF および RIP ルートのどちらも PBR 内に登録しません。しかし、静的ルートの管理距離が 115 に設定されていたとすると (メトリックは 10 のまま)、OSPF ルート (管理距離 110) は静的ルートよりも優先されますが、RIP ルートが静的ルートよりも優先されることはありません。OSPF ルートが存在しなくなったとした場合、NSM は OSPF ルートを削除しますが、RIP ルートについては、120 の管理距離 (AD) が静的ルートの 115 AD よりも大きいため、登録されることはありません。

上記のどちらのケースでも、静的ルートは依然として PBR で優先されます。NSM から PBR 内に登録された既定以外のすべてのルートはメトリック 110 で追加されており、この値は静的ルートのメトリック 10 よりも大きいからです。

静的ルートで 110 という管理距離と 110 を超えるメトリックが使用されている場合、NSM に渡されたメトリック値は、OSPF がこの静的ルートと競合する任意の OSPF ルートの OSPF メトリック (またはコスト) との比較を行う際に OSPF によって使用されます。

ルート通知

SonicWall セキュリティ装置は、RIPv1 または RIPv2 を使用して、その静的ルートおよび動的ルートをネットワーク上の他のルータに通知します。セキュリティ装置とリモート VPN ゲートウェイとの間で VPN トンネルの状況が変化した場合にも、RIPv2 で通知します。ご利用のルータの機能または設定に基づき、次のいずれかを選択します。

- RIPv1。プロトコルの初期バージョンであり、機能が少なく、マルチキャストではなくブロードキャストを使ってパケット送信を行います。
- RIPv2。プロトコルの後継バージョンであり、近隣ルータへのルーティング テーブルのマルチキャスト時のサブネット情報や、ルート学習のためのルート タグを含めます。RIPv2 パケットは下位互換性があり、マルチキャスト パケットのリッスンするオプションを提供する一部の RIPv1 実装でも受け付けることができます。「RIPv2 有効 (ブロードキャスト)」を選択すると、パケットをマルチキャストする代わりにブロードキャストします。これは RIPv1 ルータと RIPv2 ルータが混合する異機種ネットワークに適しています。

ECMP ルーティング

SonicOS 6.5 はイコールコスト マルチパス (ECMP) ルーティングをサポートしています。これは、パケットのルーティングをコストが等しい複数のパスに沿って行うための手法です。転送エンジンは、ネクストホップによってパスを識別します。パケットの転送時、ルータはどのネクストホップ (パス) を使用するか決定する必要があります。マルチパス ルーティングは、大半のルーティング プロトコルと組み合わせて使用できます。

SonicOS では、ECMP ルーティングを使用して、特定のルートの送信先に対して複数のネクスト ホップを指定できます。大量の要件がある環境では、そうすべき理由がいくつかあります。ルータはほとんどの場合、1 つの ISP しか使用しませんが、何らかの理由で最初の ISP に問題が生じた場合に別の ISP に切り替える可能性があります。マルチパスのもう 1 つの用途は、スタンバイ状態のパスを維持し、帯域幅の要求が事前に定義されたしきい値を上回った場合に限りそのパスを有効にすることです。SonicOS は最大 4 つのネクストホップ パスをサポートします。

オープン ショーテスト パス ファースト (OSPF) や中間システム間連携 (ISIS) など、さまざまなルーティング プロトコルで ECMP ルーティングが明示的に許可されています。一部のルータ実装では、RIP やその他のルーティング プロトコルでのイコールコスト マルチパスの使用も可能です。

ポリシーベース ルーティング

単純な静的ルーティング エントリには、特定の条件に一致するトラフィックの処理方法を指定します。 条件には、送信先アドレス、送信先ネットマスク、トラフィックを転送するゲートウェイ、そのゲートウェイがあるインターフェース、ルート メトリックなどがあります。この静的ルーティングはほとんどの静的要件を満たしますが、送信先アドレスを指定している場合にのみ転送可能となります。

ポリシー ベース ルーティング (PBR) を使用すると、拡張静的ルートを作成して、トラフィックをさらに柔軟かつきめ細かく処理できます。SonicOS PBR では、送信元アドレス、送信元ネットマスク、送信先アドレス、送信先ネットマスク、サービス、インターフェース、およびメトリックに基づいて照合を行うことができます。このルーティングを使用すると、多数のユーザ定義変数に基づいて、転送元から転送先に至るルートを完全に制御できます。

FQDN は PBR エントリの送信元や送信先としては使用できません。

ポリシーベース TOS ルーティング

SonicOS は、ポリシーベースのTOS (サービス種別) ルーティングを、サービス種別 (TOS) および TOS マスク値によるポリシーベース ルーティング (PBR) ポリシーの定義時にサポートしています。TOS およびマスク値が定義されている場合、これらの値は、ルート一致の検索時に、関連付けられている IP パケットの TOS/DSCP フィールド (IP ヘッダー内) と比較されます。

TOS 値は IP パケット ヘッダー内の 8 ビット フィールドと比較されます (このヘッダーの詳細については、*差別化サービスに関する RFC 2474*、および *明示的輻輳通知に関する RFC 2168* を参照してください)。TOS 値は、定量的なパフォーマンス要件 (ピーク帯域幅など) や、相対パフォーマンスに基づく要件 (クラスによる差別化など) に関連するサービスを定義するために使用できます。

TOS ルーティングは既存の SonicOS QoS マーキングとは異なります。後者はパケットのルーティングに影響せず、受信パケットの TOS フィールドに基づいた異なる形でのパケットの転送を行うことができません。TOS ルーティングでは、ポリシー ルートによる TOS 値/TOS マスクのペアの定義を許可して、受信パケットとの比較によって転送を差別化できるようにすることで、この機能を実現しています。TOS ルーティングはパケットがセキュリティ装置に入るときにのみ適用されます。

TOS ルーティングでは、送信元 IP、送信先 IP、およびサービス値がそれぞれ同一で TOS 値/TOS マスク値が異なる、複数のポリシー ルートを定義することができます。これにより、TOS フィールドがマークされたパケットを、受信パケット内の TOS フィールドの値に基づいて異なる形で転送できます。

SonicOS 6.5 よりも前に定義されたどの PBR ポリシー ルートにも、TOS/TOS マスク用に定義された値はありません。同様に、TOS/TOS マスク フィールドの既定値は 0 になっています (値が定義されていません)。

0 以外の TOS 値を持つポリシー ルートの優先順位は、送信先のみの単純なすべてのルートよりも高くなりますが、送信元またはサービスを定義しているどのポリシー ルートよりも低くなります。2 つの TOS ポリシー ルートを比較する場合、送信元、送信先、サービス値が (定義済みであれ未定義であれ) どちらも同じとすると、1 に設定されている TOS マスク ビットの数がより多い TOS ルートのほうが、設定されている TOS マスク ビット数の少ない TOS ルートよりも優先されます。

PBR ルートの一般的な優先順位 (高いものから低いものへの順) は、TOS に対して「**すべて**」でも 0 でもない値が定義されているポリシー フィールドに基づき、次のようになります。

送信先、送信元、サービス、TOS
送信先、送信元、サービス
送信先、送信元、TOS
送信先、送信元
送信先、サービス、TOS
送信先、サービス
送信先、TOS
送信先
送信元、サービス、TOS
送信元、サービス
送信元、TOS
送信元
サービス、TOS
サービス
サービス タイプ

PBR のメトリックベースの優先順位

SonicOS は、ポリシーベース ルーティング (PBR) でルート ポリシーに割り当てられるメトリックによる重み付けコストをサポートしています。これにより、ルートの優先順位付けにおいて既定で使用されるルート限定度よりも設定されたメトリックを優先させることができます。メトリックは 0 から 255 までの値をとります。メトリックは低い値のほうが適切と見なされ、高い値よりも優先されます。

PBR ルートの一般的な優先順位 (高いものから低いものへの順) は、TOS に対して「**すべて**」および 0 以外の値が定義されているポリシー フィールドに基づき、次のようになります。

送信先、送信元、サービス、TOS
送信先、送信元、サービス
送信先、送信元、TOS
送信先、送信元
送信先、サービス、TOS
送信先、サービス
送信先、TOS
送信先
送信元、サービス、TOS
送信元、サービス
送信元、TOS
送信元
サービス、TOS
サービス
サービス タイプ

これら 15 の分類内で、ルートはさらに、定義されたルート登録の累積的な限定度に基づいて優先順位付けされます。送信元と送信先のフィールドでは、アドレス オブジェクトで表される IP アドレスの個数に基づいて限定度が測定されます。例えば、ネットワーク アドレス オブジェクト `10.0.0.0/24` は、256 個の IP アドレスを表し、ネットワーク アドレス オブジェクト `10.0.0.0/20` は 4096 個の IP アドレスを表します。ネットワーク プレフィックスが長い `/24` (24 ビット) のほうが表せるホスト IP アドレス数は少なくなり、限定度が高くなります。

メトリックで重み付けされた新しいオプションにより、ルートの優先順位付けにおいてルート限定度よりも設定されたメトリックを優先させることができます。このオプションが有効になっている場合、優先順位付けには以下の要素が次の表記順で優先的に使用されます。

1. ルート クラス (送信元、送信先、サービス、および、「すべて」および 0 以外の値を持つ TOS のフィールドの組み合わせによって決まります)
2. メトリックの値
3. 送信元、送信先、サービス、および TOS フィールドの累積的限定度

ポリシー ベースのルーティングと IPv6

SonicOS の IPv6 実装の詳細については、「IPv6 (979 ページ)」を参照してください。

IPv6 に対してポリシー ベースのルーティングを完全にサポートするには、「**ネットワーク > ルーティング**」でルート ポリシーに対して IPv6 アドレス オブジェクトとゲートウェイを選択します。「**ルート ポリシー**」テーブル内のエントリは、**IPv4** と **IPv6** との切り替えが可能です。

次世代 RIP (RIPng) は、IPv6 ベースのネットワークを通して、ルート計算のための情報を交換することを可能にする、IPv6 に対するルーティング情報プロトコルです。

ルート通知については、「ルート通知 (489 ページ)」を参照してください。ルート ポリシーの設定については、「ルート通知 (489 ページ)」を参照してください。

OSPF および RIP の高度なルーティング サービス

SonicOS では、ポリシー ベース ルーティングおよび RIP 通知のほかに、高度なルーティング サービス (ARS) を有効にするオプションが用意されています。高度なルーティング サービスは、ルーティング情報プロトコル (RIPv1 - RFC1058 および RIPv2 - RFC2453) および Open Shortest Path First (OSPFv2 - RFC2328) の通知およびリッスンを全面的にサポートしています。高度なルーティング サービスを有効にするのは、この 2 つの動的ルーティング プロトコルの一方または両方をサポートする必要がある環境のみにしてください。

RIP および OSPF は、さまざまな規模のネットワークでルート決定処理を自動化するのに広く使用されている Interior Gateway Protocols (IGP) です。RIP が小規模なネットワークでよく使用されるのに対して、OSPF はそれよりも大きなネットワークで使用されます。ただし、ネットワークの規模のみを見てプロトコルの妥当性を判断するのではなく、ネットワーク速度、相互運用性要件、ネットワーク全体の複雑さなども考慮する必要があります。RIPv1 と RIPv2 のどちらも ARS でサポートされており、両者の最大の違いは RIPv2 が VLSM (可変長サブネット マスク)、認証、およびルーティング更新をサポートしていることです。「ルーティング情報プロトコルの違い」テーブルは、RIPv1、RIPv2、OSPFv2/OSPFv3 の主な違いをまとめたものです。

ルーティング情報プロトコルの違い

	RIPv1	RIPv2	OSPFv2/OSPFv3
プロトコル メトリック	距離ベクトル	距離ベクトル	リンク状態
最大ホップ数	15	15	無制限
ルーティング テーブル更新	定期的にテーブル全体をブロードキャストする、収束が遅い	定期的にテーブル全体をブロードキャストまたはマルチキャストする、収束が遅い	状態が変更されたらリンク状態をマルチキャストで通知する、収束が速い
サブネット サイズのサポート	クラス (a/b/c) によるサブネットのみをサポート	クラス別のみ	VLSM
自律システム トポロジ	分割不可、フラット	分割不可、フラット	エリア ベース、セグメント化および集約が可

トピック:

- ルーティング サービスについて (493 ページ)
- OSPF の条件 (496 ページ)

ルーティング サービスについて

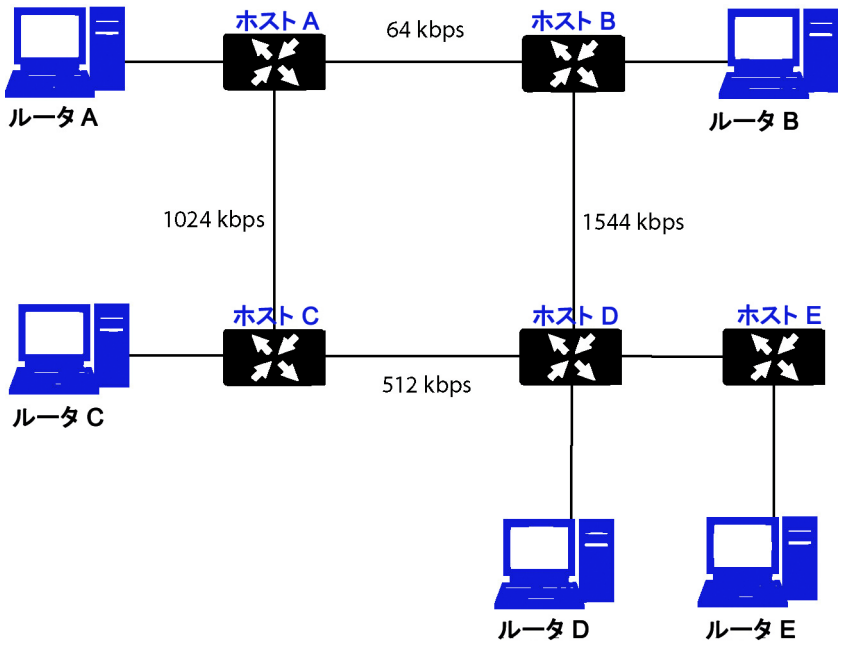
トピック:

- プロトコル種別 (493 ページ)
- 最大ホップ数 (494 ページ)
- スプリット ホライズン (494 ページ)
- ポイズン リバース (494 ページ)
- ルーティング テーブル更新 (494 ページ)
- サブネット サイズのサポート (495 ページ)
- 自律システム トポロジ (496 ページ)

プロトコル種別

RIP などの距離ベクトル プロトコルがホップ数のみに基づいてルーティング メトリックを決めているのに対して、OSPF などのリンク状態プロトコルではメトリックを決めるときにリンクの状態を考慮に入れます。例えば、OSPF では参照帯域幅 (既定では 100Mbit) をインターフェース速度で割ってインターフェース メトリックを決めており、リンクの速度が速くなればなるほど、コストが低くなり、的確なパスが選択される確率が高くなります。一例として「コストが最も低いルートを決めるためのネットワーク例」に示すネットワークを考えてみます。

コストが最も低いルートを決めるためのネットワーク例



「コストが最も低いルートを決めるためのネットワーク例」のサンプル ネットワークでは、ホスト A が RIP を使用してホスト B に到達しようとした場合、コストが最も低いルートはルータ A からルータ B となり、比較的低速の 64kbps リンクを通ることになります。OSPF を使用すると、ルータ A からルータ B へのコストが 1562 になるのに対して、ルータ A からルータ C、ルータ D、ルータ B へのへのコストは 364 で、優先ルートになります。

最大ホップ数

RIP ではホップ数を 15 までとしており、設定が間違っていたり収束が遅かったりしたために不適切なルーティング情報 (例えば、情報が古いなど) がブロードキャストされてネットワークに伝播されても、ルーティング ループが発生しないようにしています。「コストが最も低いルートを決めるためのネットワーク例」の例でルータ D とルータ E 間のリンクで障害が発生し、予防措置が取られていなかった場合を考えてみます。

- ルータ A のルーティング情報には、メトリックが 3 のルータ B またはルータ C を通ってネットワーク E に到達できると記載されています。
- ルータ D とルータ E 間のリンクで障害が発生し、ルータ A がルーティング情報をブロードキャストすると、ルータ B およびルータ C はメトリックが 4 のルータ A を通ってネットワーク E に到達できると判断します。
- ルータ B およびルータ C がこの情報をブロードキャストし、ルータ D に届くため、ルータ D はメトリックが 5 のルータ B またはルータ C を通ってネットワーク E に到達できると判断します。
- このループは、ホップ数が 16 (無限) になるまで続きます。

このような状況になったときによく取られる措置にはこのほか、次のように RIP を使用したものがあります。

- スプリット ホライズン (494 ページ)
- ポイズン リバース (494 ページ)
- ルーティング テーブル更新 (494 ページ)
- サブネット サイズのサポート (495 ページ)
- 自律システム トポロジ (496 ページ)

スプリット ホライズン

あるインターフェースから学習したルーティング情報をそのインターフェースには送り返さないという予防メカニズムです。これは一般に、ブロードキャスト リンクでは正しく機能しますが、フレーム リレーのように、単一のリンクを使用して 2 つの自律システムに到達できる非ブロードキャスト リンクでは正しく機能しません。

ポイズン リバース

ルート ポイズニングとも呼ばれ、スプリット ホライズンを拡張したものです。ネットワークにメトリック 16 (到達不能) を通知して、誤ったバックアップ ルートが伝播されないようにします。

OSPF では、ネットワークの状況が変化すると、ルーティング テーブル全体を通知するのではなく、一般にリンク状態更新を送信するだけにとどまるため、ホップ数を制限する必要はありません。これは、収束速度を高め、更新トラフィックを減らし、ホップ数を無限にできることから、大規模なネットワークでは大きな利点となります。

ルーティング テーブル更新

上記のとおり、ルーティング テーブル全体を送信すると、収束が遅くなり、帯域幅の使用率が増え、ルーティング情報が古くなる確率が高まるという問題を引き起こします。RIPv1 は所定の間隔 (通常 30 秒ごと) でルーティング テーブル全体をブロードキャストし、RIPv2 はブロードキャストまたはマルチキャストが可能であり、OSPF はネットワーク ファブリックの状況が変化したときには常にリンク状態更新のみをマルチキャストします。OSPF にはこのほか、更新をネットワーク全体に送信し

なくてもすむように、マルチ アクセス ネットワーク (その概念については後の説明を参照) で隣接関係を形成するのに指名ルータ (DR) を使用するという利点もあります。

サブネット サイズのサポート

ネットワークがクラス A、クラス B、およびクラス C (後に D および E) に厳密に分類されたときに初めて RIPv1 が実装されました。

クラス A 1.0.0.0 から 126.0.0.0 まで (0.0.0.0 と 127.0.0.0 は予約済み)

- 左端ビット 0；7 個のネットワーク ビット；24 個のホスト ビット
- 0nnnnnnn hhhhhhhh hhhhhhhh hhhhhhhh (8 ビットのクラスフル ネットマスク)
- 126 個のクラス A ネットワーク、それぞれのネットワークに 16,777,214 個のホスト

クラス B 128.0.0.0〜191.255.0.0

- 左端ビット 10；14 個のネットワーク ビット；16 個のホスト ビット
- 10nnnnnn nnnnnnnn hhhhhhhh hhhhhhhh (16 ビットのクラスフル ネットマスク)
- 16,384 個のクラス B ネットワーク、それぞれのネットワークに 65,532 個のホスト

クラス C 192.0.0.0〜223.255.255.0

- 左端ビット 110；21 個のネットワーク ビット；8 個のホスト ビット
- 110nnnnnn nnnnnnnn nnnnnnnn hhhhhhhh (24 ビットのクラスフル ネットマスク)
- 2,097,152 個のクラス C ネットワーク、それぞれのネットワークに 254 個のホスト

クラス D 225.0.0.0 〜 239.255.255.255 (マルチキャスト)

- 左端ビット 1110；28 個のマルチキャスト アドレス ビット
- 1110mmmm mmmmmmmm mmmmmmmm mmmmmmmm

クラス E 240.0.0.0 〜 255.255.255.255 (予約済み)

- 左端ビット 1111；28 個の予約済みアドレス ビット
- 1111rrrr rrrrrrrr rrrrrrrr rrrrrrrr

このアドレス割り当ての方法は、セグメント分割 (サブネット) の方法でも、VLSM (可変長サブネットマスク) の手段による集約 (スーパーネットまたは CIDR (Classless Inter-Domain Routing)) でも柔軟性を提供しないため、極めて非効率的であることがわかっています。

RIPv2 および OSPF でサポートされる VLSM を使用すると、クラスを使用しないネットワーク表現で大きなネットワークをより小さなネットワークに分割することができます。

> 例えば、クラスフル 10.0.0.0/8 ネットワークを取り、/24 ネットマスクを割り当てます。このサブネットでは、ホスト範囲からネットワーク範囲に追加の 16 ビットが割り当てられます (24 - 8=16)。このサブネットで提供される追加のネットワーク数を計算するには、2 の追加のビット数乗を計算します(2^16=65,536)。つまり、1,670 万のホスト (通常ほとんどの LAN が必要な数以上) を含む 1 つのネットワークを持つことなく、それぞれが 254 の使用可能なホストを含む 65,536 のネットワークを持つことができます。

VLSM は、次のようにルート集約 (CIDR) も可能にします。

> 例えば、8 個のクラス C ネットワーク、192.168.0.0/24 〜 192.168.7.0/24 がある場合に、各ネットワークへの別々のルート ステートメントを定義するのではなく、それらすべてを包含する 192.168.0.0/21 への単一のルートを指定できます。

この機能を使用すると、IP アドレス空間のより効率的で柔軟性のある割り当てを実現できるばかりでなく、ルーティング テーブルとルーティング アップデートを小規模に維持することもできます。

自律システム トポロジ

自律システム (AS) は、共通の管理制御下にあり、同じルーティング特性を共有するルータのコレクションです。自律システムのグループがルーティング情報を共有する場合、これらのシステムは一般に自律システムの連合と呼ばれます。(RFC1930 と RFC975は、これらの概念を詳細に扱っています)。簡単に言えば、AS は設定の共通性に基づいて物理ネットワーク要素を包含する論理上の区別です。

RIP と OSPF に関しては、RIP 自律システムをセグメント分割することはできません。 また、すべてのルーティング情報は AS を介して通知 (ブロードキャスト) される必要があります。これは、管理が困難になり、過剰なルーティング情報トラフィックを招く可能性があります。一方 OSPF は、エリアの概念を採用し、論理的に管理可能なセグメント分割で AS 内での情報の共有を制御できるようにします。エリア ID は管理上の識別子です。OSPF エリアは、バックボーン エリア (エリア 0 または 0.0.0.0) で始まり、他のすべてのエリアは、このバックボーン エリアに接続する必要があります (例外あり)。ルーティングAS をセグメント分割するこの機能は、管理するには大きくなりすぎないように、またルータを扱うには計算が多用されすぎないようにするうえで役に立ちます。

OSPF の条件

OSPF の設定やメンテナンスは RIP よりもかなり複雑です。OSPF ルーティング環境を理解するには、次の概念が重要です。

- **リンク状態** - リンク状態は OSPF に関係しています。リンクはルータ上の送信インターフェースであり、状態にはそのコストなどインターフェースの特性が記述されています。リンク状態は、リンク状態通知 (*LSA*) の形式で送信されます。これは、5 種類の OSPF パケットの 1 つであるリンク状態の更新 (*LSU*) パケット内に含まれます。
- **コスト** - 特定のリンクに沿ってパケットを送信するために必要な定量化されたオーバヘッド。コストは、基準帯域 (通常 100Mbit、または 10^8 ビット) をインターフェースの速度で除算して計算されます。コストが低いほど、リンクはより適切になります。一部の一般的なパス コストを「インターフェースごとのコスト計算」テーブルに示します。

  インターフェースごとのコスト計算

インターフェース	10^8 (100Mbit) で除算=OSPF コスト
ファースト イーサネット	1
イーサネット	10
T1 (1.544Mbit)	64
DSL (1Mbit)	100
DSL (512Kbps)	200
64Kbps	1562
56Kbps	1785

- **エリア** - 共通のリンク状態データベースを共有することを目的とする OSPF ルータのグループで構成されるネットワーク。OSPF ネットワークは、バックボーン エリア (エリア 0 または 0.0.0.0) の周辺に構築され、仮想リンクを使用する (通常、推奨されていません) 場合を除き、他のすべてのエリアはバックボーン エリアに接続する必要があります。エリアの割り当ては、OSPF ルータ上のインターフェースに固有です。言い換えると、複数のインターフェースを含むルータは同じエリアや異なるエリア用に設定されたインターフェースを持つことができます。
- **近隣** - 一般的なネットワーク セグメント上の OSPF ルータは、Hello パケットを送信することで近隣ルータになることができます。Hello パケットは通知と ID の形式で機能し、2 つの OSPF ルータが特定の特性の共通する組み合わせを共有している場合、これらのルータがもう一方の

ルータの Hello パケットにあるルータ ID を確認して近隣ルータとなります。Hello パケットは、*DR* (指定ルータ) および *BDR* (バックアップ指定ルータ) の選出プロセスでも使用されます。2 つのルータが近隣ルータになるには、次の共通する特性を持っている必要があります。

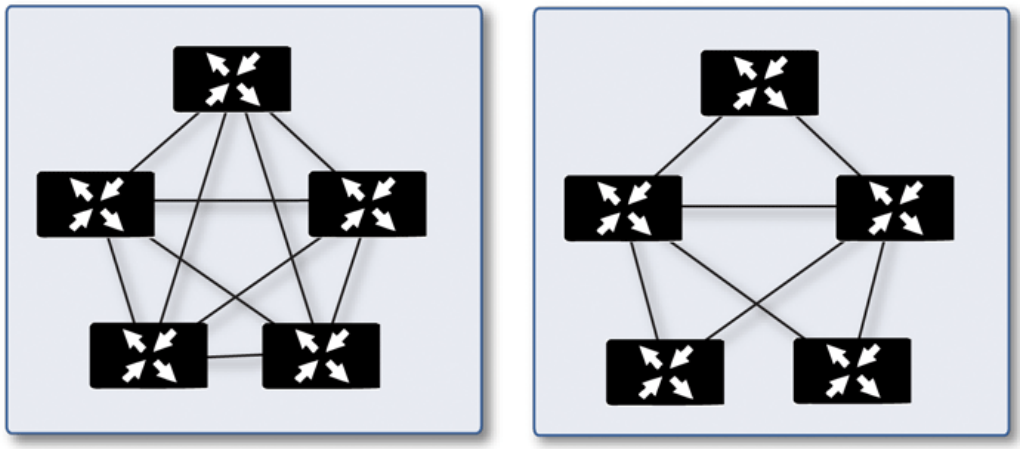
- **エリア ID** - エリア ID は、32 ビット値を使用して OSPF*エリア*を識別します。これは一般に IP アドレス形式で表されます。OSPF は、動作するためにバックボーン エリア、エリア 0 (または 0.0.0.0) を最小限度必要とします。
- **認証** - 認証の種類は、一般に、なし、単純な文字列、または MD5 に設定できます。単純な文字列は保護なしで送信されるので、認証を識別にのみ使用する必要があります。セキュリティを考慮する場合は、MD5 を使用する必要があります。
- **タイマ間隔** - Hello 判断間隔と Dead 判断間隔は同じである必要があります。「Hello 送出間隔」は、Hello パケットから次の Hello パケットが送信されるまでの秒数 (キープアライブ機能として利用される) を指定します。「Dead 判断間隔」は、Hello パケットの受信がなくなった場合にルータを使用不能と見なすまでの秒数を指定します。
- **スタブ エリア フラグ** -「*スタブ エリア*」は、1 つの送出ポイントのみを必要とするため、外部リンク通知の完全なリストを必要としません。2 つの潜在的な近隣ルータ上のスタブ エリア フラグは、不適切なリンク状態の交換を避けるために同じである必要があります。近隣に影響を及ぼすもう 1 つの要因はネットワークの種類です。OSPF は、次に示すネットワークの 3 つの種類を認識します。
  - **ブロードキャスト** - 例えば、イーサネット。ブロードキャスト ネットワークでは、ブロードキャスト ドメインにある他のすべてのルータと近隣を確立できます。
  - **ポイント ツー ポイント** - 例えば、シリアル リンク。ポイント ツー ポイント (またはポイント ツー マルチポイント) ネットワークでは、リンクの一端にあるルータと近隣関係を確立できます。
  - **NBMA** (Non-Broadcast Multiple Access) - 例えば、フレーム リレー。NBMA ネットワークでは、近隣を明示的に宣言する必要があります。

- **リンク状態データベース** - リンク状態データベースは、*エリア*内で*隣接関係*を形成している*近隣* OSPF により送受信される LSA で成り立っています。データベースが作成されると、データベースには所定のエリアのすべてのリンク状態情報が含まれます。この時点で最短パス優先 (SPF) アルゴリズムが適用され、接続されているすべてのネットワークへの最適なルートがコストに基づいて決定されます。SPF アルゴリズムは、すべてのルータをグラフ内の頂点と見なして各頂点間のコストを計算する Dijkstra のパス検索アルゴリズムを採用しています。
- **隣接関係** - OSPF ルータは、隣接するルータと LSA を交換して LSDB を作成します。隣接関係は、ネットワークの種類に応じて種々の方法で形成されます (前述の「*近隣*」を参照)。一般にネットワークの種類は、ブロードキャスト (例えば、イーサネット) です。このため、隣接関係はハンドシェイクのような方法で OSPF パケットを交換することで形成されます (下記の「OSPF パケットの種類」を参照)。隣接するルータ、OSPF ルータを含むセグメント (ブロードキャスト ドメイン) 間で交換される情報の量を最小にするには、Hello パケットを使用して指定ルータ (DR) およびバックアップ指定ルータ (BDR) を選択します。
- **DR** (指定ルータ) - マルチアクセス セグメント上では、OSPF ルータが DR および BDR を選択し、セグメント上の他のすべてのデータは DR と BDR との隣接関係を形成します。DR 検出はルータの OSPF優先順位に基づきます。 この優先順位は 0 (DR には不適格) から 255 までの値に設定できます。高い優先順位を持つルータが DR になります。優先順位が同じ場合、最も高いルータ ID (インターフェース アドレス指定に基づく) を持つルータが採用されます。ルータが DR になると、そのルータが利用不可になるまではその役割をめぐって競争が生じることはありません。

  次に、セグメント上の可能性のある各ペアリングの組み合わせ間ではなく、これらの隣接関係にまたがる LSU 内で LSA が交換されます。「ルーティングの隣接関係: 指定ルータ (DR)」を参照し

てください。リンク状態の更新は、DR 以外のルータによりマルチキャスト アドレス 225.0.0.6 に送信されます。このアドレスは、RFC1583 が割り当てた「OSPFIGP 指定ルータ」アドレスです。これらの更新は、すべてのルータが LSA を受信できるようにマルチキャスト アドレス 225.0.0.5「OSPFIGP 全ルータ」にも行き渡ります。

ルーティングの隣接関係: 指定ルータ (DR)



DR/BDR のない隣接関係　　DR/BDR のある隣接関係

- **OSPF パケットの種別** - OSPF パケットには、次に示す 5 つの種別があります。
  - **Hello** (OSPF 種別 1) - 近隣 OSPF ルータとの関係を確立および維持し、指定ルータを選出するために一定の間隔で送信されます。(*LSDB 同期の初期化および 2 ウェイ フェーズ中に送信*)。
  - **データベース記述** (OSPF 種別 2) - 隣接関係を形成中に OSPF ルータ間で送信されます。*LSDB 同期の EXstart フェーズ中に*、DD パケットは LSA の追跡に使用される ISN (初期シーケンス番号) を確立し、近隣 OSPF ルータ間でマスタ/スレーブ関係を確立します。*LSDB 同期の交換フェーズでは*、これらのパケットはリンク状態通知の短いバージョンを含んでいます。DD 交換は、複数のパケットにわたることができるため、これらのパケットはポール (マスタ) と応答 (スレーブ) の形式で交換され、完全性が確保されます。
  - **リンク状態要求** (OSPF 種別 3) - *LSDB 同期の読み込みフェーズ中に*、近隣ルータからのデータベース更新を要求する LSR パケットが送信されます。これは、隣接関係を確立する最終手順です。
  - **リンク状態更新** (OSPF 種別 4) - リンク状態要求に対する応答で送信されます。LSU パケットはリンク状態通知を使用して隣接関係を行き渡らせて LSDB 同期を実現します。
  - **リンク状態確認応答** (OSPF 種別 5) - LSA フラッドの信頼性を確保するために、すべての更新は確認されます。
- **リンク状態通知 (LSA)** - LSA には、次の 7 つの種別があります。
  - タイプ 1 (ルータ リンク通知) - OSPF ルータにより送信され、このルータが属する各エリアへのリンクを記述します。種別 1 LSA は、ルータのエリアのみに行き渡ります。
  - **種別 2** (ネットワーク リンク通知) - ネットワーク内のルータのセットを記述するためにエリアの DR により送信されます。種別 2 LSA は、ルータのエリアのみに行き渡ります。
  - **種別 3** (概要リンク通知) - ABR (領域境界ルータ) によりエリア全体に送信され、エリア内のネットワークを記述します。種別 3 LSA は、ルート統合のためにも使用され、完全スタブ エリアには送信されません。

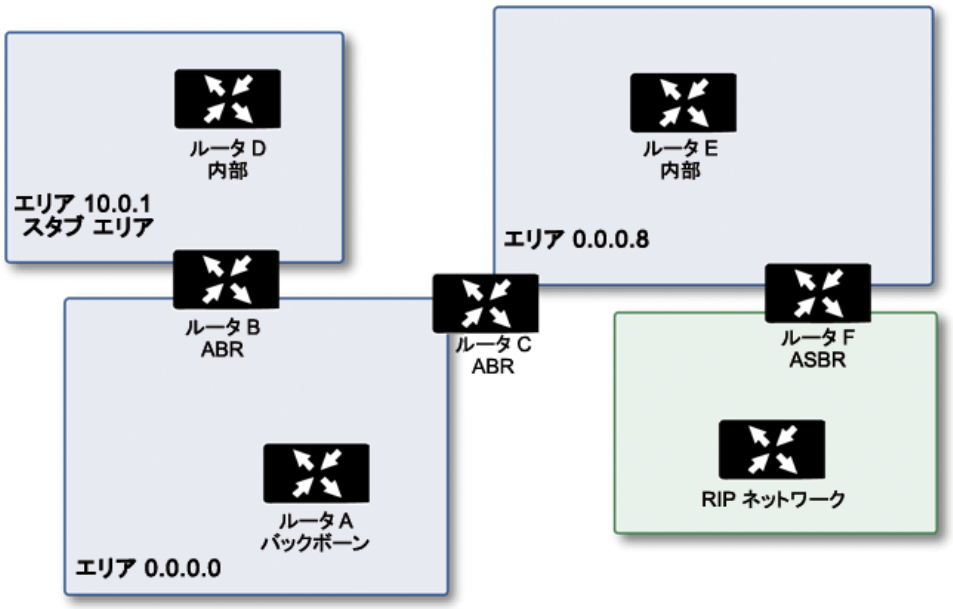
- **種別 4** (AS 概要リンク通知) - ABR (エリア境界ルータ) によりエリア全体に送信され、異なる AS 内のネットワークを記述します。種別 4 LSA はスタブ エリアには送信されません。
- **種別 5** (AS 外部リンク通知) - ASBR (自律システム境界ルータ) により送信され、異なるAS 内のネットワークへのルートを記述します。種別 5 LSA はスタブ エリアには送信されません。外部リンク通知には、次の 2 つの種別があります。
  - **外部種別 1** - 種別 1 のパケットは、リンクの測定基準を計算するときに内部リンク コストを外部リンク コストに追加します。同じ送信先に向かう場合、種別 1 ルートは種別 2 ルートよりも常に優先されます。
  - **外部種別 2** - 種別 2 パケットは測定基準を求めるために外部リンク コストのみに使用されます。通常、種別 2 は外部 AS へのパスが 1 つだけある場合に使用されます。
- **種別 6** (マルチキャスト OSPF または MOSPF) - 送信元/送信先ルーティングと呼ばれます。これは、送信先のみに基づいてルーティングを行う多くのユニキャスト データグラム転送アルゴリズム (OSPF など) とは対照的です。MOSPF の詳細については、「*RFC1584 - Multicast Extensions to OSPF*」を参照してください。
- **種別 7** (NSSA AS 外部リンク通知) - NSSA の一部である ASBR により送信されます (「スタブ エリア」を参照)。

- **スタブ エリア** - スタブ エリアは、最適なルートではなく 1 つのパスのみを必要とするエリアです。これは、1 つの送出ポイントのみを持つエリアであったり、SPF 最適化が必要ではないエリアとすることができます。スタブ エリアのすべてのルータは、完全な状態データベースを受信したり、SPF ツリーを計算したりすることのないスタブ ルータとして構成される必要があり、概要リンク情報のみを受信します。

  スタブ エリアには次の種別があります。

  - **スタブ エリア** - 標準的なスタブ エリアであり、LSA 種別 5 (AS 外部リンク通知) を除くすべての LSA を受信します。これは、LSDB を小規模に維持するうえで役に立ち、ルータ上での計算オーバヘッドを減らします。
  - **完全スタブ エリア** - LSA 種別 3 (概要リンク)、4 (AS 概要リンク)、および 5 が通過しない特殊な種類のスタブ エリアです。エリア内のルートのみおよび既定のルートが完全スタブ エリア内に通知されます。
  - **NSSA** (準スタブ エリア) - RFC3101 で説明されている NSSA は、種別 7 LSA (NSSA AS 外部ルート) を使用して外部ルートを NSSA エリア内に行き渡らせることができるようにするハイブリッド スタブ エリアですが、種別 5 LSA を他のエリアから受け入れません。NSSA は、異なる IGP (RIP など) を実行しているリモート サイトを OSPF サイトに接続するときに役立ちます。ここでは、リモート サイトのルートをメイン OSPF サイトに配布し直す必要はありません。また、NSSA *ABR* (エリア境界ルータ) には、種別 7 LSA を種別 5 LSA に変換する機能もあります (この操作は SonicOS CLI からのみ可能です。『*SonicOS CLI リファレンス ガイド*』を参照してください)。
- **ルータの種別** - OSPF では、ルータの役割を基にルータを次の 4 つの種別に分類しています。「OSPF 認定ルータの種別の例」を参照してください。

OSPF 認定ルータの種別の例



- **IR** (内部ルータ) - インターフェースがすべて同じエリア内に含まれるルータ。内部ルータの LSDB にはそのエリアの情報のみが含まれます。
- **ABR** (エリア ボーダ ルータ) - インターフェースが複数のエリアにあるルータ。ABR は接続先の各エリアの LSDB を維持し、通常その 1 つがバックボーンです。
- **バックボーン ルータ** - エリア 0 のバックボーンに接続されたインターフェースがあるルータ。
- **ASBR** (自律システム境界ルータ) - AS から OSPF AS に外部ルーティング情報を通知する OSPF AS 以外 (RIP ネットワークなど) に接続されたインターフェースがあるルータ。

ドロップ トンネル インターフェース

ドロップ トンネル インターフェースは、設定されたルートがダウンしている場合に、トラフィックが誤ったルートで送信されるのを阻止します。ドロップ トンネル インターフェースに送信されたトラフィックは、セキュリティ装置から外へ出ることはなく、破棄されたように見えます。

ドロップ トンネル インターフェースは、単独でも使用できますが、VPN トンネル インターフェースと組み合わせて使用してください。静的ルートがトンネル インターフェースにバインドされている場合、SonicWall は、ドロップ トンネル インターフェースにバインドされている静的ルートを同じネットワーク トラフィックに対して設定することを推奨します。このようにすると、トンネル インターフェースがダウンしたときに、2 番目の静的ルートが使用され、トラフィックは実質的に破棄されます。これにより、データが平文のまま別のルートに転送されるのを防止できます。

VPN トンネル インターフェースを使用してルートを設定すると、トンネルが一時的にダウンすると、対応するルート登録も無効化されます。SonicOS は、VPN 保護ネットワークに向かう接続のために新しいルート登録を探し出します。リモート VPN ネットワークへのバックアップ リンクがない配備では、それ以外の適切なルート登録が使用できません。そのためトラフィックは誤ったルート登録 (通常、デフォルト ルート) に送信され、そこで内部データが暗号化されずに送信されるというようなセキュリティ上の問題が生じます。

バックアップ リンクのない配備では、次の例のようにルート テーブルを設定することを検討してください。

```
route n:   local VPN network(source), remote VPN network(destination), VPN TI(egress_if)
route n+1: local VPN network(source), remote VPN network(destination), Drop If(egress_if)
```

VPN トンネル インターフェースをこの例のように設定すると、トラフィックはドロップ インターフェースと一致するので、送出されません。VPN トンネル インターフェースが再開すると、トラフィックも再開します。

アプリベースのルーティング

アプリベースのルーティングは、トラフィックがルート テーブルで指定されたネクスト ホップから代替パスを使用できるようにする一種の PBF (ポリシーベース転送) ルールであり、通常、セキュリティまたはパフォーマンス上の理由で送信インターフェースを指定するために使用されます。

アプリベースのルート登録 (ルート エントリ) が作成されると、最初はセキュリティ装置にアプリケーションを識別するのに十分な情報がないため、ルート エントリを強制できません。さらにパケットが到着すると、セキュリティ装置はアプリケーションを判別し、アプリ ID キャッシュに内部エントリを作成します。これはセッションの間保持されます。同じ送信先 IP アドレス、送信先ポート、およびプロトコル ID で新しいセッションが作成されると、セキュリティ装置はアプリケーションを初期セッションから同じものとして識別し、アプリベースのルートを適用できます。したがって、完全に一致せず、同じアプリケーションではないセッションは、アプリベースのルートに基づいて転送できません。

この機能は、ゲートウェイ AV/アンチスパイウェア/侵入防御/アプリケーション制御/アプリケーション可視化がライセンスされ、アプリケーション制御が「**管理 | ポリシー > ルール > アプリケーション制御**」で有効になっている場合にのみ使用可能です。

ネットワーク > ルーティング

インターフェースにルータを配置している場合は、「**管理 | システム セットアップ > ネットワーク > ルーティング**」ページで SonicWall セキュリティ装置に静的ルートを設定できます。送信元アドレス、送信元ネットマスク、送信先アドレス、送信先ネットマスク、サービス、インターフェース、ゲートウェイ、およびメトリックに基づいてルートが決まるように、静的ルーティング ポリシーに静的ルーティング エントリを作成できます。この機能を使用すると、多数のユーザ定義変数に基づいて、転送元から転送先に至るルートを完全に制御できます。

トピック:

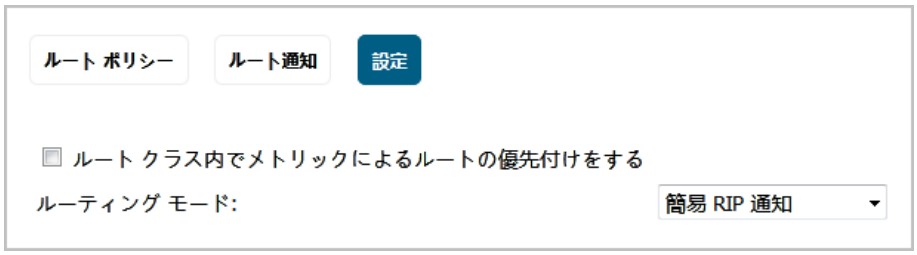
- ネットワーク > ルーティング > 設定 (501 ページ)

ネットワーク > ルーティング > 設定

「**管理 | システム セットアップ > ネットワーク > ルーティング > 設定**」の外観は、選択するルーティング モードによって変わります。

- **Simple RIP Advertisement【簡易 RIP 通知】**
- **Advanced Routing【高度なルーティング】**

簡易 RIP 通知



Advanced Routing 【高度なルーティング】

ネットワーク > ルーティング > ルート ポリシー

「**ネットワーク > ルーティング > ルート ポリシー**」には、IPv4 または IPv6 のどちらかについて、既定およびユーザ定義ルートのすべてが表示されます。表示内容は、IPv6 では IP アドレスの代わりに IPv6 リンクローカル アドレスが表示される点を除き、どちらの IP バージョンについても同じです。

以下のいずれかを選択して、「**ルート ポリシー**」テーブルに表示されるルート ポリシーの表示形式を変更できます。

- **IPv4** または **IPv6**
- 「**表示**」にある次の表示設定のいずれか

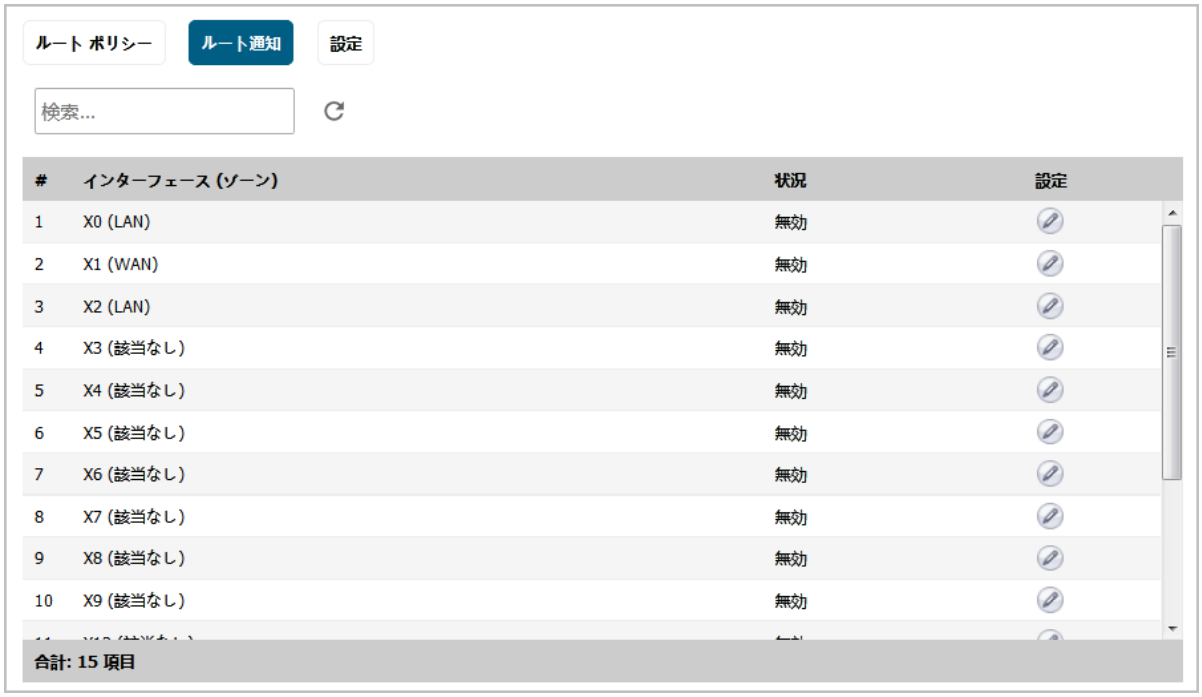
すべての種別	**ユーザ定義ポリシー**および**既定のポリシー**を含むすべてのルーティング ポリシー。最初は、「**すべての種別**」を選択すると、「**ルート ポリシー**」テーブルに「**既定のポリシー**」のみが表示されます。
ユーザ定義ポリシー	管理者が作成したものです。
既定のポリシー	SonicOS によって作成されたもの。

「**検索**」フィールドに送信元、送信先、またはインターフェースを入力すると、表示対象をフィルタできます。

列	ルート ポリシーの設定
送信元	送信元の IP バージョン アイコンと名前。
送信先	送信先の IP アドレス (IPv4) または MAC アドレス (IPv6)。
サービス	ルート ポリシーで設定されているサービス オブジェクト。
TOS/マスク	ルートで設定されている TOS と TOS マスク。
ゲートウェイ	ゲートウェイの IP アドレス (IPv4) または MAC アドレス (IPv6)。
インターフェース	ルート ポリシーで設定されているインターフェース。
メトリック	ルート優先順位のために設定されているメトリック。
優先順位	ルート ポリシーの優先順位。
プローブ	プローブが設定されているかどうか。
コメント	ユーザ定義ルートの設定時に入力されたコメント (既定のポリシーの場合は「**自動追加されたルート ポリシー**」) が含まれているコメント アイコン。
設定	**編集**アイコンと**削除**アイコンがあります。既定のポリシーではアイコンが淡色表示になっています。

ネットワーク > ルーティング > ルート通知

「**ネットワーク > ルーティング > ルート通知**」は、「**ルーティング モード**」で「**簡易 RIP 通知**」が選択されている場合にのみ表示されます。

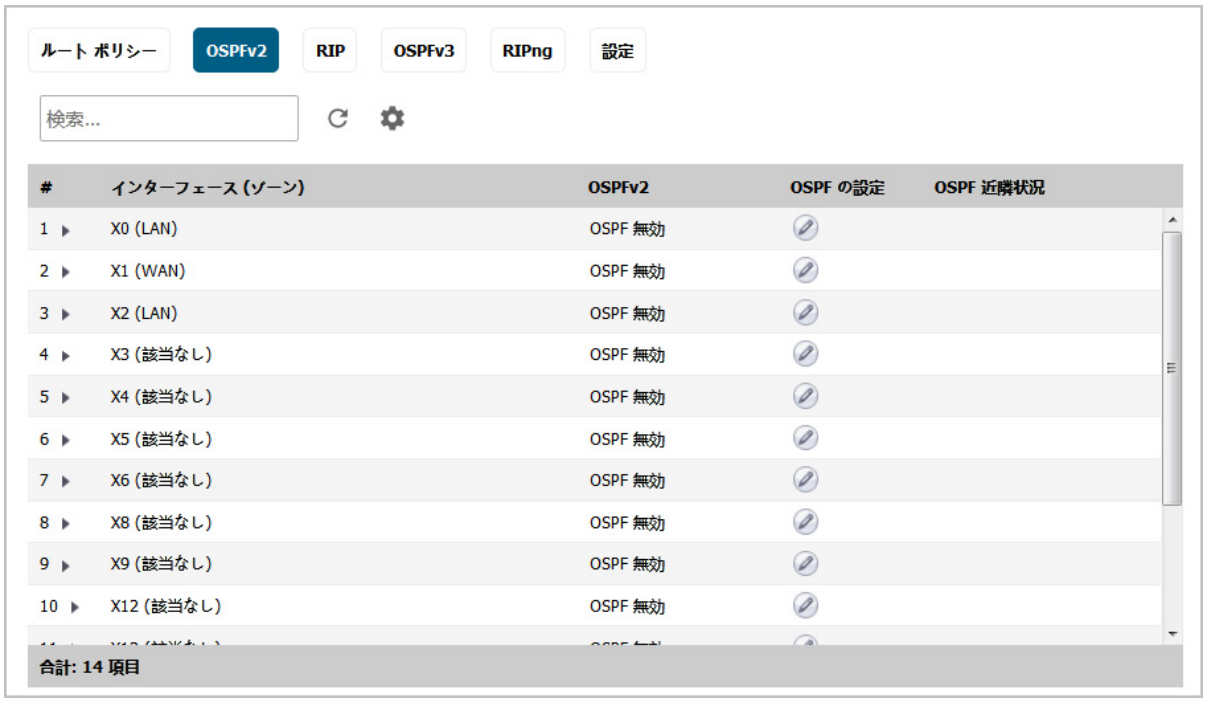


インターフェース (ゾーン)	ルート通知で設定されているインターフェース。インターフェースにゾーンが設定されていない場合、**(ゾーン)** 部分の表示は「**(該当なし)**」となります。

状況	「**有効**」または「**無効**」のどちらかです。
設定	**編集**アイコンが表示されています。

ネットワーク > ルーティング > OSPFv2

「**ネットワーク > ルーティング > OSPFv2**」は、「**ルーティング モード**」で「**高度なルーティング**」が選択されている場合にのみ表示され、OSPFv2 の状況を示すとともにインターフェースに対する OSPFv2 の設定を可能にします。



設定	デフォルト ルートに対するメトリックを設定するための「**設定**」ポップアップを表示するアイコン。
インターフェース (ゾーン)	OSPFv2 で設定されているインターフェースとそのゾーン。インターフェースにゾーンが設定されていない場合、**(ゾーン)** 部分の表示は「**(該当なし)**」となります。
OSPFv2	OSPF がインターフェース上で有効になっているかどうかを示します。 • **OSPF 有効** • **OSPF 有効 (パッシブ)** • **OSPF 無効**
OSPF の設定	インターフェースの**編集**アイコンが表示されます。
OSPF 近隣状況	動作中または停止中の近隣者があるかどうかを示す**状況**アイコンが表示されます。このアイコンを選択すると、インターフェースの近隣者に関する詳細を示す「**インターフェース OSPFv2 近隣**」ポップアップが表示されます。「ネットワーク > ルーティング > OSPFv2 > インターフェース OSPFv2 近隣 (505 ページ)」を参照してください。

ネットワーク > ルーティング > OSPFv2 > インターフェース OSPFv2 近隣

インターフェースの**状況**アイコンを選択すると、このポップアップが表示されます。

ルータ ID 近隣者のルータ ID

現在の状況 確立された OSPFv2 近隣関係の状況

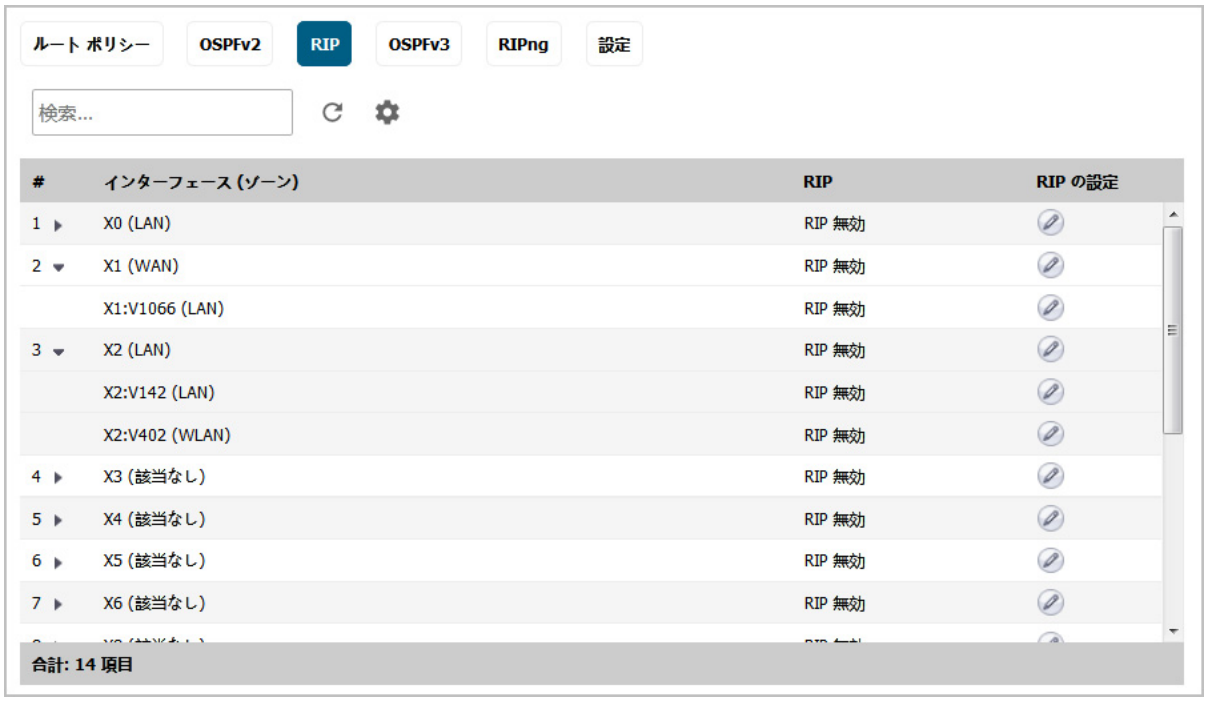
- **Init (始動)**
- **2-way (2 ウェイ)**
- **ExStart (交換開始)**
- **Exchange (交換)**
- **Loading (ロード中)**
- **Full (完全)**

優先順位 近隣者のルータの優先順位

IP アドレス 近隣者のルータの IP アドレス

ネットワーク > ルーティング > RIP

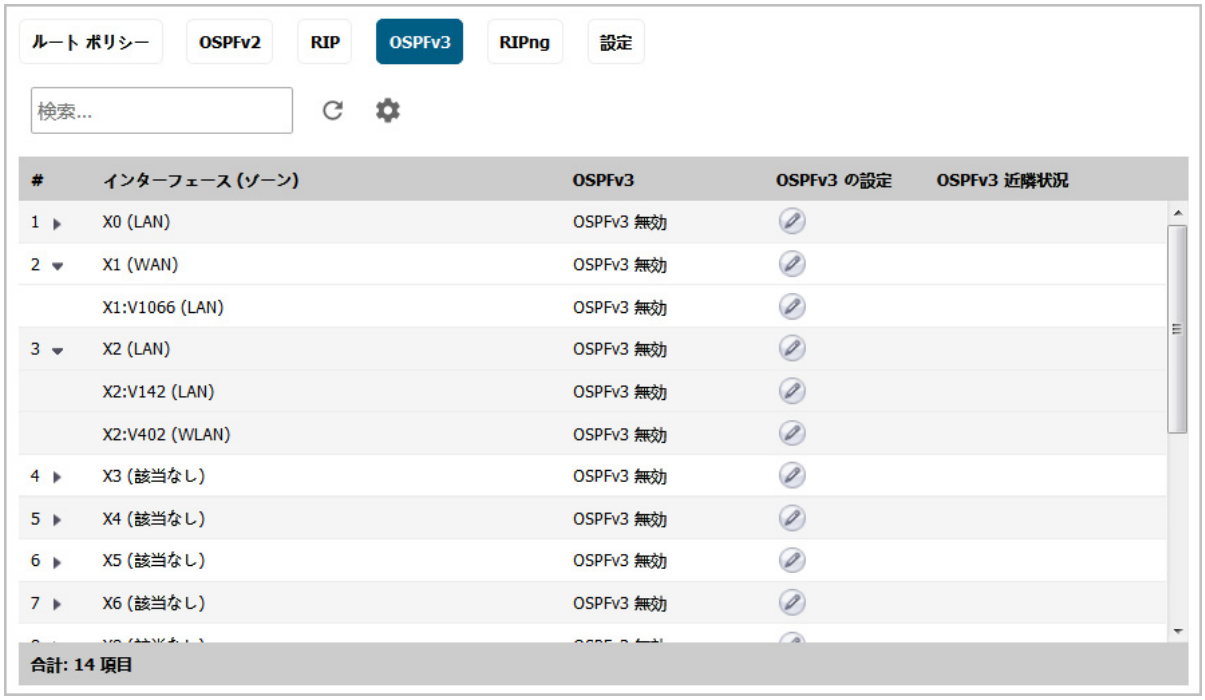
「**ネットワーク > ルーティング > RIP**」は、「**ルーティング モード**」で「**高度なルーティング**」が選択されている場合にのみ表示され、RIP の状況を示すとともにインターフェースに対する RIP の設定を可能にします。



設定	デフォルト ルートに対するメトリックを設定するための「**設定**」ポップアップを表示するアイコン。
インターフェース (ゾーン)	RIP で設定されているインターフェースとそのゾーン。インターフェースにゾーンが設定されていない場合、**(ゾーン)** 部分の表示は「**(該当なし)**」となります。
RIP	RIP がインターフェース上で有効になっているかどうかを示します。 • **RIP 有効** • **RIP 有効 (パッシブ)** • **RIP 無効**
RIP の設定	インターフェースの**編集**アイコンが表示されます。

ネットワーク > ルーティング > OSPFv3

「**ネットワーク > ルーティング > OSPFv3**」は、「**ルーティング モード**」で「**高度なルーティング**」が選択されている場合にのみ表示され、OSPFv3 の状況を示すとともにインターフェースに対する OSPFv3 の設定を可能にします。

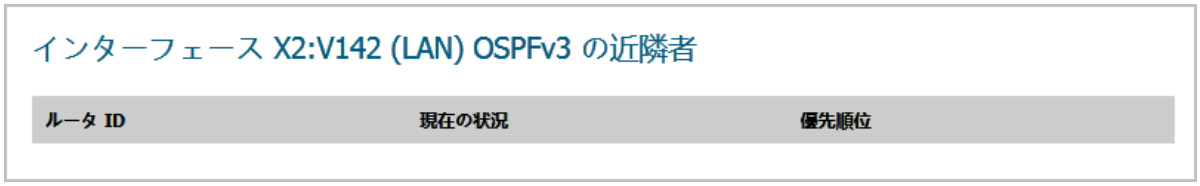


設定	デフォルト ルートに対するメトリックを設定するための「**設定**」ポップアップを表示するアイコン。
インターフェース (ゾーン)	OSPFv3 で設定されているインターフェースとそのゾーン。インターフェースにゾーンが設定されていない場合、**(ゾーン)** 部分の表示は「**(該当なし)**」となります。

OSPFv3	OSPF がインターフェース上で有効になっているかどうかを示します。 • **OSPFv3 有効** • **OSPFv3 有効 (パッシブ)** • **OSPFv3 無効**
OSPFv3 の設定	インターフェースの**編集**アイコンが表示されます。
OSPFv3 近隣状況	動作中または停止中の近隣者があるかどうかを示す**状況**アイコンが表示されます。このアイコンを選択すると、インターフェースの近隣者に関する詳細を示す「**インターフェース OSPFv3 の近隣者**」ポップアップが表示されます。 「ネットワーク > ルーティング > OSPFv3 > インターフェース OSPFv3 近隣者 (507 ページ)」を参照してください。

ネットワーク > ルーティング > OSPFv3 > インターフェース OSPFv3 近隣者

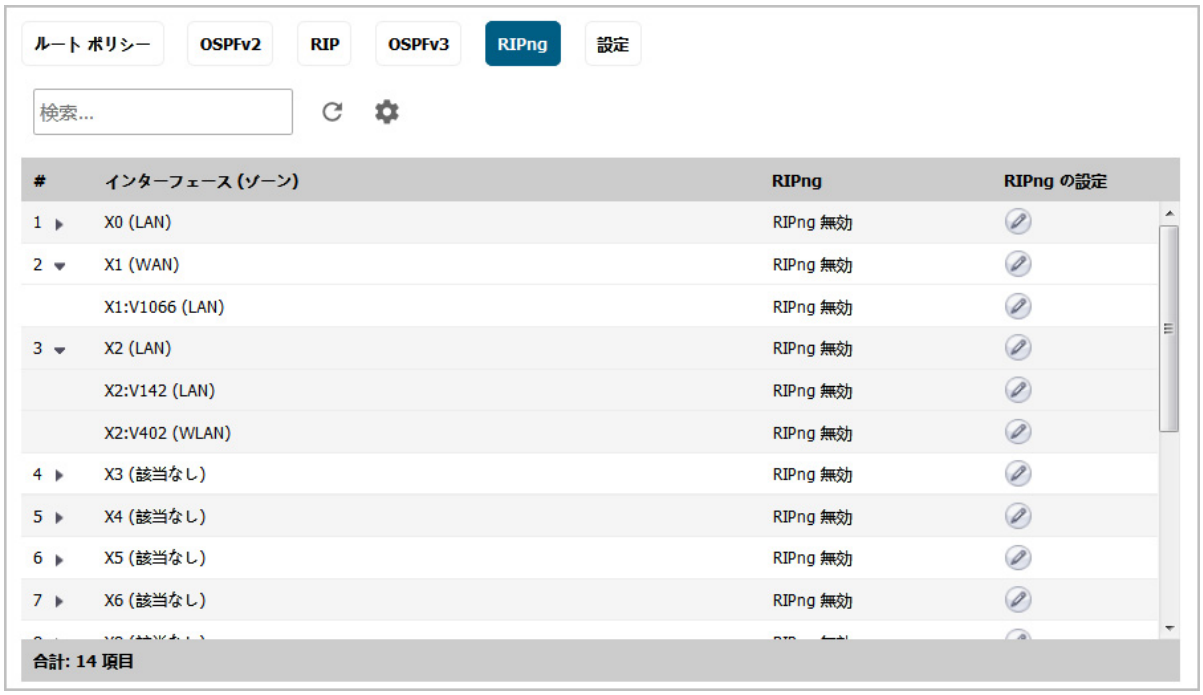
インターフェースの**状況**アイコンを選択すると、このポップアップが表示されます。



ルータ ID	近隣者のルータ ID。
現在の状況	確立された OSPFv3 近隣関係の状況。 • **Init (始動)** • **2-way (2 ウェイ)** • **ExStart (交換開始)** • **Exchange (交換)** • **Loading (ロード中)** • **Full (完全)**
優先順位	近隣者のルータの優先順位。

ネットワーク > ルーティング > RIPng

「**ネットワーク > ルーティング > RIPng**」は、「**ルーティング モード**」で「**高度なルーティング**」が選択されている場合にのみ表示され、RIPng の状況を示すとともにインターフェースに対する RIPng の設定を可能にします。



設定	デフォルト ルートに対するメトリックを設定するための「**設定**」ポップアップを表示するアイコン。
インターフェース (ゾーン)	RIPng で設定されているインターフェースとそのゾーン。インターフェースにゾーンが設定されていない場合、**(ゾーン)** 部分の表示は「**(該当なし)**」となります。
RIPng	RIPng がインターフェース上で有効になっているかどうかを示します。 • **RIP 有効** • **RIP 有効 (パッシブ)** • **RIP 無効**
RIPng の設定	インターフェースの**編集**アイコンが表示されます。

ルーティングの設定

トピック:

- メトリックによるルートの優先順位付け (509 ページ)
- ルータ広告によって学習されたデフォルト ルートに対するメトリックの設定 (509 ページ)
- 静的およびポリシーベースのルートの設定 (511 ページ)
- ドロップ トンネル インターフェースに対応する静的ルートの設定 (516 ページ)

- OSPF および RIP の高度なルーティング サービスの設定 (517 ページ)
- BGP の高度なルーティングの設定 (528 ページ)

メトリックによるルートの優先順位付け

重要：メトリックで重み付けされたルート優先順位に変更するには、SonicWall セキュリティ装置を再起動する必要があります。

メトリックによる重み付けオプションを使用すると、優先順位付けにおいてルート限定度よりもメトリックを優先させることができます。メトリック オプションが選択されているかどうかによって、優先順位付けでの優先度 (高いものか低いものへの順) は次のようになります。

- 選択されていない場合 (既定):
    a ルート クラス (「**すべて**」以外の値を持つ送信元、送信先、サービス、および TOS のフィールドの組み合わせによって決まります)
    b 送信元、送信先、サービス、および TOS の累積的限定度
    c メトリック
- 選択されている場合:
    a ルート クラス
    b メトリック
    c 送信元、送信先、サービス、および TOS フィールドの累積的限定度

メトリックで重み付けされたルート優先順位を変更するには、以下の手順に従います。

1 「**管理 | システム セットアップ > ネットワーク > ルーティング > 設定**」に移動します。
2 「**ルート クラス内でメトリックによるルートの優先付けをする**」を選択します。確認メッセージが表示されます。

> **警告! メトリックで重み付けされたルート優先順位に変更しますか? 再起動が必要です。「OK」をクリックすると続行します。**

3 「**OK**」を選択します。
4 「**管理 | 更新 > 再起動**」に移動して SonicOS を手動で再起動します。

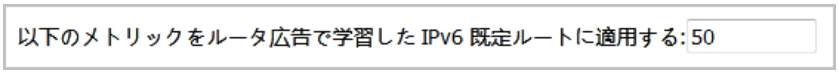
ルータ広告によって学習されたデフォルト ルートに対するメトリックの設定

メモ：この設定は、ルータ広告から学習された IPv6 デフォルト ルートに対してのみ有効です。

ルータ広告によって学習されたデフォルト ルートに対してメトリックを設定するには、以下の手順に従います。

1 「**管理 | ネットワーク > ルーティング**」に移動します。
2 「**ルート ポリシー**」を選択します。

3 **設定**アイコンを選択します。「**設定**」ダイアログが表示されます。



4 このルート メトリックは、ルータ広告によって学習されたデフォルト ルートに適用されます。「**以下のメトリックをルータ広告で学習した IPv6 既定ルートに適用する**」フィールドにメトリックを入力します。最小値は 1、最大値は 255、既定値は **50** です。

ⓘ **ヒント：**メトリックは低い値のほうが適切と見なされ、高い値よりも優先されます。

5 「**適用**」を選択します。

ルート通知の設定

ネットワーク インターフェースのルート通知を有効にするには、以下の手順を実行します。

1 「**管理 | ネットワーク > ルーティング**」に移動します。

2 「**ルート通知**」を選択します。

3 インターフェースの「**設定**」列で**編集**アイコンを選択します。「**インターフェース XO(LAN) ルートの通知設定**」ダイアログが表示されます。

4 「**ルートの通知**」ドロップダウン メニューから次のいずれかの種別を選択します。

- **無効** (既定) - ルートの通知を無効にします。
- **RIPv1 有効** - RIPv1 はルーティング情報プロトコルの最初のバージョンです。
- **RIPv2 有効 (マルチキャスト)** - マルチキャストを使用してルートの通知を送信します (ネットワーク上の特定のノードに単一のデータ パケットを送信します)。
- **RIPv2 有効 (ブロードキャスト)** - ブロードキャストを使用してルートの通知を送信します (ネットワーク上の全ノードに単一のデータ パケットを送信します)。

「**無効**」以外の種別を選択すると、他のオプションが選択できるようになります。

5 「**デフォルト ルートの通知**」**ドロップダウン** メニューから、次のいずれかを選択します。

- **無効** (既定)
- **WAN 動作時** (WAN インターフェースでは選択できない)
- **常に**

6 セキュリティ装置 に静的ルートが設定されている場合、「**静的ルートの通知**」を有効にしてそれらを「ルート通知」から除外します。

7 VPN ネットワークを通知する場合は、「**リモート VPN ネットワークの通知**」を有効にします。

8 「**ルート変更通知までの待ち時間 (秒)**」フィールドに、通知がネットワーク上にブロードキャストされる間隔を秒単位で入力します。既定値は **30** 秒、最小値は 1 秒、最大値は 99 秒です。低い値ほどネットワークにおけるブロードキャスト トラフィック量が多くなります。「**ルート変更通知までの待ち時間 (秒)**」の設定によって、VPN トンネルの状態 (アップまたはダウン) が変化してから、その変化が RIP で通知されるまでの待ち時間が決まります。数秒の遅延を設定することにより、VPN トンネル状態の一時的な変更から不明瞭なルート通知が送信されることを防止します。

9 「**ルート削除時の通知回数 (0 - 99)**」フィールドに、削除されたルートの通知がブロードキャストされる回数を入力します。既定値は **1** です。

10 「**ルート メトリック (1 - 15)**」フィールドに、**1** (既定) から 15 までの値を入力します。これは、送信元 IPアドレスから送信先 IP アドレスまでにパケットがルータに接触する回数です。

> **メモ**：以下のオプションは、「**ルートの通知**」ドロップダウン メニューで RIPv2 通知オプションを選択した場合にのみ、選択できるようになります。「**RIPv1 有効**」を選択した場合は、「ステップ 13」に進みます。

11 ルート タグの値を「**RIPv2 ルート タグ (16 進数 4 文字)**」フィールドに入力できます。この値は実装依存であり、ルータが RIPv2 通知の送信元を分類するメカニズムを提供します。既定値は **0** です。

12 RIPv2 認証を有効にする場合は、「**RIPv2 認証**」ドロップダウン メニューから次のいずれかのオプションを選択します (既定は「**無効**」)。

- **ユーザ定義** - 次の 2 つのフィールドが表示されます。
  - **認証種別 (16 進数 4 文字)** - 16 進数 4 文字をこのフィールドに入力します。既定値は **0** です。
  - **認証データ (16 進数 32 文字)** - 16 進数 32 文字をこのフィールドに入力します。
- **平文パスワード** -「**認証用パスワード**」フィールドが表示されます。最大 16 文字のパスワードをこのフィールドに入力します。
- **MD5 ダイジェスト** -「**認証鍵 Id (0-255)**」フィールドに 0 から 255 までの数値を入力します。「**認証鍵 (16 進数 32 文字)**」フィールドに 16 進数 32 文字を入力するか、生成した鍵を使用します。
  - **認証鍵 Id (0-255)** - 最大 255 文字をこのフィールドに入力します。既定値は **1** です。
  - **認証鍵** - 最大 32 文字をこのフィールドに入力します。

13 「**OK**」を選択します。

静的およびポリシーベースのルートの設定

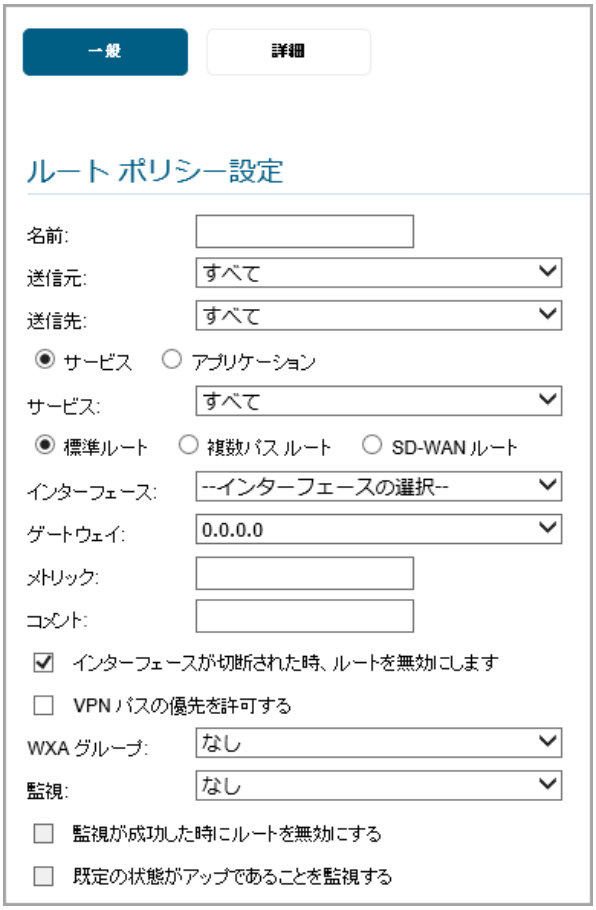
SonicOS では、基本的なルート ポリシーを使用して静的ルートを設定します。セキュリティ装置 1 台あたりのルートの最大数については、『*SonicOS 6.5 ポリシー*』にあるルート ポリシー設定の説明を参照してください。

静的ルートを設定するときに、必要に応じてルートのネットワーク監視ポリシーを設定できます。ネットワーク監視ポリシーを使用すると、ポリシーのプローブの状態に基づいて、静的ルートが動的に無効または有効になります。

静的またはポリシーベースのルートを設定するには:

1 「**管理 | システム セットアップ > ネットワーク > ルーティング > ルート ポリシー**」に移動します。

2 **追加**アイコンを選択します。「**ルート ポリシーの追加**」ダイアログが表示されます。



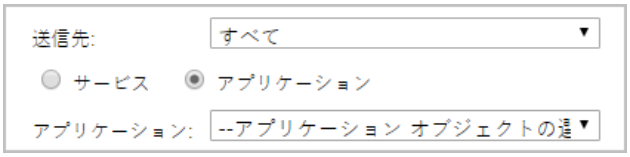
3 「**名前**」フィールドにわかりやすい名前を入力します。

4 「**送信元**」で、静的ルートの送信元アドレス オブジェクトを選択します。または、「**アドレス オブジェクトの作成**」を選択して、新しいアドレス オブジェクトを動的に作成します。既定は「**すべて**」です。

5 「**送信先**」で送信先アドレス オブジェクトを選択するか、「**アドレス オブジェクトの作成**」を選択して新しいアドレス オブジェクトを動的に作成します。既定は「**すべて**」です。

6 ルート ポリシーの種別を選択します。

- **サービス** (既定)
- **アプリケーション** -サービスが「**アプリケーション**」に切り替わります。



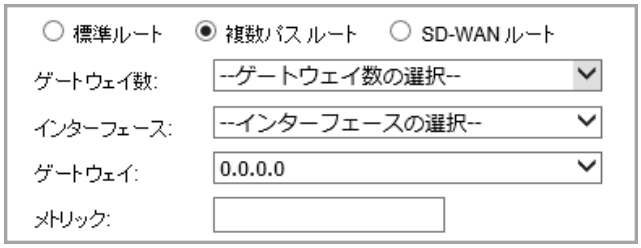
7 「**サービス**」で、サービス オブジェクトを選択します。すべての種類のトラフィックを許可する汎用静的ルートの場合は、単に「**すべて**」 (既定) を選択します。

8 「ステップ 14」に移動します。

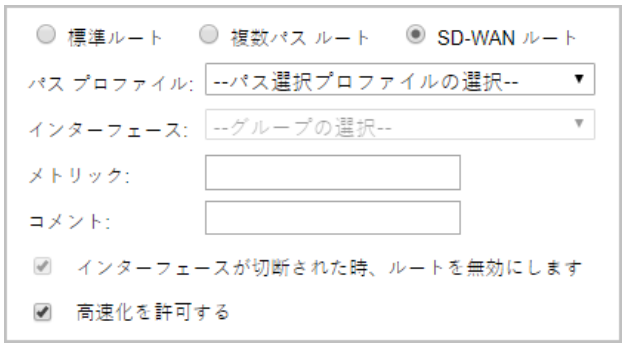
9 「**アプリケーション**」から、アプリケーション オブジェクトを選択します。

10 使用するルートの種別を選択します。

- **標準ルート** (既定) - 「ステップ 14」に進みます。
- **複数パス ルート** - 「**ゲートウェイ数**」オプションが表示されます。



- **SD-WAN ルート** - オプションが次のように変わります。



> **メモ：**「**インターフェース**」および「**インターフェースが切断された時、ルートを無効にします**」オプションは、SD-WAN ポリシーで編集できないため、淡色表示されています。「**インターフェース**」オプションには、関連するパス選択プロファイル (PSP) の SD-WAN グループ名が入力されているため変更できません。SD-WAN ルートのインターフェースは、SD-WAN ルートに関連付けられている PSP の一部である SD-WAN グループから選択されているため、設定できません。

「ステップ 13」に移動します。

11 「**ゲートウェイ数**」で、ゲートウェイの最大数を選択します。

- **2**
- **3**
- **4**

12 「ステップ 16」に移動します。

13 「**パス プロファイル**」から、パス選択プロファイルを選択します。

14 「**インターフェース**」からルートで使用するインターフェースを選択するか、「**VPN トンネル インターフェースの作成**」を選択して新しい VPN ポリシーを動的に作成します。VPN ポリシーの作成については、『*SonicOS 6.5 接続*』を参照してください。

15 「**ゲートウェイ**」で、ルートで使用するゲートウェイ アドレス オブジェクトを選択します。または、「**アドレス オブジェクトの作成**」を選択して、新しいアドレス オブジェクトを動的に作成します。既定値は 0.0.0.0 です。アドレス オブジェクトの作成については、『*SonicOS 6.5 ポリシー*』を参照してください。

16 「**メトリック**」にルートのメトリック (重み付けされたコスト) を入力します。最小値は 1 で、最大値は 254 です。既定のメトリックは次のとおりです。

- 静的ルートの場合: **1**

- 動的ルートの場合 (学習元によって異なります):
  - RIP/RIPng: **120**
  - OSPFv2/OSPFv3: **110**
  - BGP: **20**

メトリックの詳細については、「メトリックと管理距離 (487 ページ)」および「ポリシーベース ルーティング (489 ページ)」を参照してください。

ヒント：メトリックは、低い値のほうが適切と見なされ、高いメトリック (コスト) のものよりも優先されます。SonicOS は、直接接続されたインターフェース、静的にエンコードされたルート、および動的な IP ルーティング プロトコルに対して Cisco が定義したメトリック値に準拠しています。

17 必要に応じて、「**コメント**」にルートのコメントを入力します。このフィールドには、新しい静的ルート ポリシーについて説明するコメントを入力できます。

18 インターフェースが切断されたときにルートを自動的に無効にするには、「**インターフェースが切断されたとき、ルートを無効にします**」を選択します。このオプションは、既定では選択されています。

メモ：SD-WAN ルートを設定している場合、このオプションは選択済みで淡色表示になっており、変更することはできません。

19 SD-WAN ルートを設定している場合は、「ステップ 21」に進みます。

20 必要に応じて、VPN トンネルのバックアップ ルートを作成するには、「**VPN パスの優先を許可する**」を選択します。このオプションは、既定では選択されていません。

既定では、ユーザによって設定された VPN トンネル静的ルートのメトリックは 1 であり、VPN トラフィックよりも優先されます。「**VPN パスの優先を許可する**」オプションは、同じ送信先アドレス オブジェクトに対する VPN トラフィックを静的ルートよりも優先します。その結果、VPN トンネルの状態に基づいて次の動作が適用されます。

- **アクティブな場合**: 「**VPN パスの優先を許可する**」オプションが有効であれば、VPN トンネルと送信先アドレス オブジェクトが一致する静的ルートが自動的に無効になります。すべてのトラフィックが VPN トンネルを通って送信先アドレス オブジェクトへ向かいます。
- **停止した場合**: VPN トンネルと送信先アドレス オブジェクトが一致する静的ルートが自動的に有効になります。送信先アドレス オブジェクトへ向かうすべてのトラフィックが静的ルートを通ります。

21 WXA がライセンスされている場合は、「**WXA グループ**」で WXA グループを選択します。既定は「**なし**」です。

22 SD-WAN ルートを設定している場合は、「ステップ 28」に進みます。

23 これを行うには、次の手順に従います。

- プローブ対応ポリシー ベース ルーティングを使用するには、「ステップ 24」に進みます。
- プローブ対応ルーティングを無視して TOS および管理距離の値を設定するには、「ステップ 28」に進みます。
- 設定を適用するには、「ステップ 32」に進みます。

24 「**プローブ**」で、以下の選択を行います。

- 「**なし**」 (既定)「ステップ 27」に移動します。

- ネットワーク監視オブジェクト。プローブ対応ポリシーベース ルーティングを設定するための次の 2 つのオプションが使用可能になります。
- **新しいネットワーク監視オブジェクトを作成する。**「**ポリシーの追加**」ダイアログが表示されます。ネットワーク監視オブジェクトの作成方法については、『*SonicOS 6.5 調査*』の手順を参照してください。

25 プローブ成功時にルートを無効化するには、「**監視が成功したときにルートを無効にする**」を選択します。このオプションは、既定では選択されていません。

> **重要**：通常の設定では、「**監視が成功したときにルートを無効にする**」チェックボックスをオンにすることはありません。一般に、管理者はルートの送信先へのプローブが失敗したときにルートを無効にしたいと考えるからです。このオプションにより、ルートとプローブをより柔軟に定義できるようになります。

26 連結されたネットワーク監視ポリシーの状態が UNKNOWN のときにプローブが成功した (つまり稼働中の状態にある) とルートで見なすには、「**既定の状態がアップであることを監視する**」を選択します。これは、高可用性ペアの 1 台の装置の状態が IDLE から ACTIVE に移行したときのプローブベースの動作を制御するのに役立ちます。この移行によって、ネットワーク監視ポリシーの状態がすべて UNKNOWN に設定されるからです。

27 既定の TOS および管理距離の値を使用するには、「ステップ 32」に進みます。

28 「**詳細**」を選択します。

29 「**TOS (16 進)**」フィールドに TOS 値を入力します。最大値は FF です。「**TOS (16進)**」および「**TOS マスク (16進)**」フィールドが設定されていない場合、値 0 が使用されます。TOS および TOS マスク値の詳細については、「ポリシーベース TOS ルーティング (490 ページ)」を参照してください。

30 同じ値を「**TOS マスク (16 進)**」フィールドに入力します。

31 管理距離を手動で指定するには、以下の手順に従います。

a 「**自動**」の選択を解除します。「**管理距離**」フィールドが使用可能になります。このオプションは、既定では選択されています。管理距離の詳細については、「メトリックと管理距離 (487 ページ)」を参照してください。

b 「**管理距離**」フィールドに管理距離を入力します。

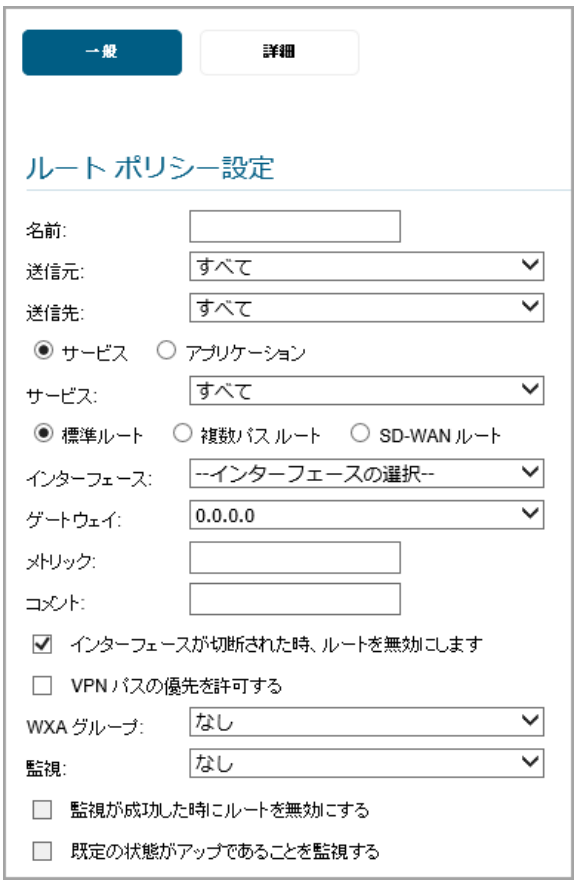
32 「**OK**」を選択します。

ドロップ トンネル インターフェースに対応する静的ルートの設定

ドロップ トンネル インターフェースに対応する静的ルートを追加するには:

1 「**管理 | システム セットアップ | ネットワーク > ルーティング > ルート ポリシー**」に移動します。

2 **追加**アイコンを選択します。「**ルート ポリシーの追加**」ダイアログが表示されます。



3 「静的およびポリシーベースのルートの設定 (511 ページ)」の説明に従って、「**送信元**」、「**送信先**」、「**サービス**」および「**ルート**」オプションの値を設定します。

4 「**インターフェース**」の「**Drop_TunnelIf**」を選択します。オプションが次のように変化します。

5 オプションの設定を「静的およびポリシーベースのルートの設定 (511 ページ)」と同じようにして終了します。

6 「**OK**」を選択します。ルートが有効になり、「**ルート ポリシー**」テーブルに表示されます。

OSPF および RIP の高度なルーティング サービスの設定

メモ：ARS はすべての機能を備えたマルチプロトコル ルーティング スイートです。非常に多くの設定可能オプションとパラメータが用意されている一方、グラフィカル ユーザ インターフェースは簡単なものです。ARS の機能を制限しないでその機能を SonicOS 管理インターフェースに簡潔に表示することで、最も密接な関係があるルーティング機能を制御する一方、CLI で完全なコマンド スイートを使用できます (『*SonicOS CLI リファレンス ガイド*』を参照してください)。ARS CLI には、認証された CLI セッションからアクセスでき、以下の 3 つのモジュールがあります。

- **route ars-nsm** - 高度なルーティング サービス ネットワーク サービス モジュール。このコンポーネントは、インターフェース バインディングおよび再配布可能ルートなど、中核となるルータ機能を制御します。
- **route ars-rip** - RIP モジュール。RIP ルータを制御します。
- **route ars-ospf** - OSPF モジュール。OSPF ルータを制御します。

一般に、セキュリティ装置を大部分の RIP 環境や OSPF 環境に統合するために必要な機能は、すべてウェブ ベースの GUI を通じて利用できます。CLI の追加機能により、より高度な設定が可能になります。

既定では、高度なルーティング サービスは無効となっているため、有効にして使用する必要があります。

RIP および OSPF ルーティング プロトコルの動作は、インターフェース依存です。各インターフェースと仮想サブインターフェースに RIP と OSPF を個別に設定でき、各インターフェースで RIP と OSPF の両方のルータを実行できます。

トピック:

- 高度なルーティング サービスおよび BGP の有効化 (518 ページ)
- OSPF の設定 (518 ページ)

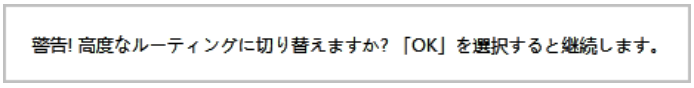
- RIP および RIPng の設定 (524 ページ)
- トンネル インターフェースに対する高度なルーティング設定 (527 ページ)

高度なルーティング サービスおよび BGP の有効化

高度なルーティング サービスを有効にするには、以下の手順に従います。

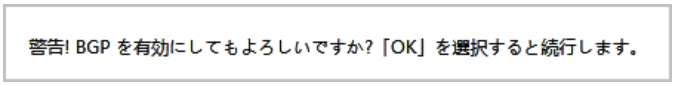
1 「**管理 | システム セットアップ | ネットワーク > ルーティング > 設定**」に移動します。

2 「**ルーティング モード**」で、「**高度なルーティング**」を選択します。確認メッセージが表示されます。



3 「**OK**」を選択します。「**ネットワーク > ルーティング**」のオプションが次のように変化します。

4 BGP を有効にするには、「**BGP**」で「**有効 (CLI での設定)**」を選択します。既定は「**無効**」です。確認メッセージが表示されます。



5 「**OK**」を選択します。「**BGP 状況**」が利用可能になります。

OSPF の設定

メモ：OSPF デザインの概念は、このドキュメントの範囲外です。このセクションでは、既存または新規に実装されたものでデザイン ガイドラインが提供されていない SonicWall セキュリティ装置を設定して OSPF ネットワークに統合する方法を説明します。このセクション全体で使われている用語については、「OSPF の条件 (496 ページ)」を参照してください。

トピック:

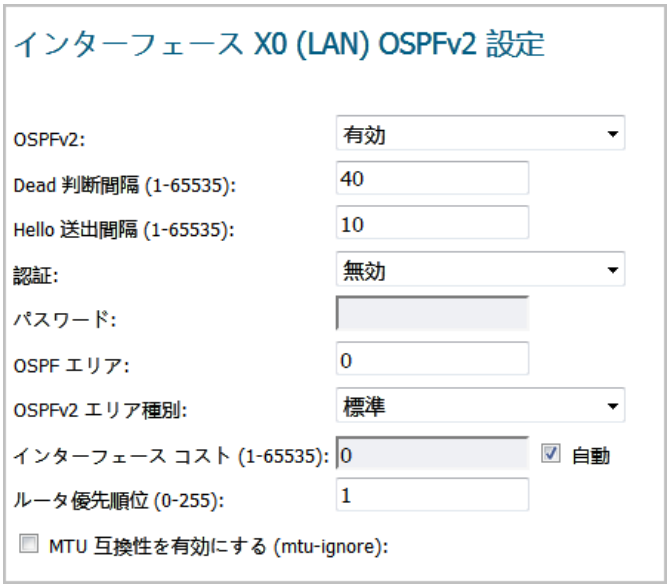
- OSPFv2 の設定 (518 ページ)
- OSPFv3 の設定 (520 ページ)

OSPFv2 の設定

OSPFv2 用のインターフェースを設定するには、以下の手順に従います。

1 「**管理 | システム セットアップ | ネットワーク > ルーティング > OSPFv2**」に移動します。

2 インターフェースの**編集**アイコンを選択します。「**インターフェース OSPFv2 設定**」ダイアログが表示されます。



3 「**OSPFv2**」で、以下を選択します。

無効 (既定)	このインターフェースでは OSPF ルータは無効です。「ステップ 13」へ進みます。
有効	このインターフェースでは OSPF ルータは有効です。
パッシブ	このインターフェースでは OSPF ルータは有効ですが、種別 1 LSA のルータ リンク通知を使用して接続ネットワークのみをローカル エリアに通知します。「**OSPF エリア**」を除くすべてのオプションが淡色表示になります。「ステップ 9」に進みます。

4 Hello の受信がない場合に LSDB のエントリを削除するまでの時間を指定するには、その秒数を「**Dead 判断間隔 (1-65535)**」フィールドに入力します。既定値は **40** 秒で、最小値は 1、最大値は 65,535 です。

> **重要**：近隣関係が正しく確立されるように、この値はセグメント上の他の OSPF ルータと一致させてください。

5 Hello パケットを送信する間隔を指定するには、その秒数を「**Hello 送出間隔 (1-65535)**」フィールドに入力します。既定値は **10** 秒で、最小値は 1、最大値は 65,535 です。

> **重要**：近隣関係が正しく確立されるように、この値はセグメント上の他の OSPF ルータと一致させてください。

6 「**認証**」で、このインターフェースで使用される認証の種別を選択します。

無効	どの認証も使用されていない場合は、「ステップ 8」に進みます。
パスワード	OSPF ルータによる識別用にプレーン テキストのパスワードが使用されます。
メッセージ ダイジェスト	OSPF ルータを確実に識別するために MD5 ハッシュが使用されます。

> **重要**：近隣関係が正しく確立されるように、この設定はセグメント上の他の OSPF ルータと一致させてください。

7 指定したオプションに応じて、次のように入力します。

パスワード	1 ～ 15 文字の英数字によるパスワードを入力します。
メッセージ ダイジェスト	1 ～ 15 文字の英数字によるパスワードを入力します。

8 「**OSPF エリア**」フィールドにエリア ID を入力します。OSPF エリアは IP または 10 進法表記で表すことができます。例えば、`X4:100` に接続されたエリアは、`100.100.100.100` または `1684300900` と表せます。既定値は **0** です。

9 「**OSPFv2 エリア種別**」で、OSPFv2 エリア種別を選択します (設定の詳しい説明は、「OSPF の条件 (496 ページ)」を参照してください)。

標準	既定の設定です。すべての適用可能な LSA 種別を送受信します。
スタブ エリア	種別 5 LSA (AS 外部リンク通知) は受け取りません。
完全スタブ エリア	LSA の種別 3、4、5 は受け取りません。
半スタブ エリア	種別 7 LSA (NSSA AS 外部ルート) を受信します。
完全スタブ NSSA	種別 1 および 2 の LSA を受信します。

10 適宜、以下の手順に従います。

- このインターフェース上でのパケット送信のオーバーヘッドを指定するには、「**インターフェース コスト (1-65535)**」フィールドにそのオーバーヘッドを入力します。既定値は **0** で、通常イーサネット インターフェースを示す場合に使用します。最小値と既定値は 0 (高速イーサネットなど) で、最大値は 65,535 (パディングなど) です。
- コストが自動的に決定されるようにするには、「**自動**」を選択します。すると、「**インターフェース コスト**」フィールドが淡色表示になります。このオプションは、既定では選択されています。

11 セグメントの指定ルータ (DR) を決定するときに使われるルータ優先順位を指定するには、「**ルータ優先順位 (0-255)**」フィールドに値を入力します。値が高いほど、優先順位は高くなります。優先順位が同じ場合は、ルータ ID がタイブレーカとして使われます。値を 0 に設定すると、このインターフェースの OSPF ルータは DR 状況に対して不適格となります。既定値は **1** で、最大値は 255 です。

12 MTU 互換性を有効にするには、「**MTU 互換性を有効にする (mtu-ignore)**」を選択します。このオプションは、既定では選択されていません。

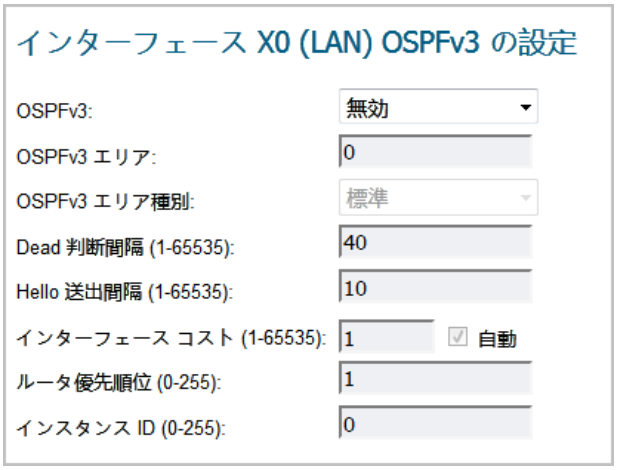
13 「**OK**」を選択します。

OSPFv3 の設定

OSPFv3 用のインターフェースを設定するには、以下の手順に従います。

1 「**管理 | システム セットアップ | ネットワーク > ルーティング > OSPFv3**」に移動します。

2 インターフェースの**編集**アイコンを選択します。「**インターフェース OSPFv3 の設定**」ダイアログが表示されます。



3 「**OSPFv3**」で、以下を選択します。

無効 (既定)	このインターフェースでは OSPF ルータは無効です。「ステップ 12」へ進みます。
有効	このインターフェースでは OSPF ルータは有効です。
パッシブ	このインターフェースでは OSPF ルータは有効ですが、種別 1 LSA のルータ リンク通知を使用して接続ネットワークのみをローカル エリアに通知します。「**OSPFv3 エリア**」を除くすべてのオプションが淡色表示になります。

4 「**OSPF エリア**」フィールドにエリア ID を入力します。OSPF エリアは IP または 10 進法表記で表すことができます。例えば、X4:100 に接続されたエリアは、100.100.100.100 または 1684300900 と表せます。既定値は **0** です。

5 「**OSPFv3**」で「**パッシブ**」を選択した場合は、「ステップ 12」に進みます。

6 Hello の受信がない場合に LSDB のエントリを削除するまでの時間を指定するには、その秒数を「**Dead 判断間隔 (1-65535)**」フィールドに入力します。既定値は **40** 秒で、最小値は 1、最大値は 65,535 です。

> **重要**：近隣関係が正しく確立されるように、この値はセグメント上の他の OSPF ルータと一致させてください。

7 「**OSPFv3 エリア種別**」で、OSPFv3 エリア種別を選択します (設定の詳しい説明は、「OSPF の条件 (496 ページ)」を参照してください)。

標準	既定の設定です。すべての適用可能な LSA 種別を送受信します。
スタブ エリア	種別 5 LSA (AS 外部リンク通知) は受け取りません。
完全スタブ エリア	LSA の種別 3、4、5 は受け取りません。

8 Hello パケットを送信する間隔を指定するには、その秒数を「**Hello 送出間隔 (1-65535)**」フィールドに入力します。既定値は **10** 秒で、最小値は 1、最大値は 65,535 です。

> **重要**：近隣関係が正しく確立されるように、この値はセグメント上の他の OSPF ルータと一致させてください。

9 適宜、以下の手順に従います。

- このインターフェース上でのパケット送信のオーバーヘッドを指定するには、「**インターフェース コスト (1-65535)**」フィールドにそのオーバーヘッドを入力します。既定値

は **0** で、通常イーサネット インターフェースを示す場合に使用します。最小値と既定値は 0 (高速イーサネットなど) で、最大値は 65,535 (パディングなど) です。

- コストが自動的に決定されるようにするには、「**自動**」を選択します。すると、「**インターフェース コスト**」フィールドが淡色表示になります。このオプションは、既定では選択されています。

10 セグメントの指定ルータ (DR) を決定するときに使われるルータ優先順位を指定するには、「**ルータ優先順位 (0-255)**」フィールドに値を入力します。値が高いほど、優先順位は高くなります。優先順位が同じ場合は、ルータ ID がタイブレーカとして使われます。値を 0 に設定すると、このインターフェースの OSPF ルータは DR 状況に対して不適格となります。既定値は **1** で、最大値は 255 です。

11 インターフェースのインスタンス ID を設定するには、「**インスタンス ID (0-255)**」フィールドに値を入力します。最小値および既定値は 0 で、最大値は 255 です。このオプションは、既定では選択されていません。

> **重要**：このオプションは通常淡色表示されているため、SonicOS コマンド ライン インターフェースで設定する必要があります (SonicOS CLI については、『*SonicOS コマンド ライン インターフェース*』を参照してください)。

12 「**OK**」を選択します。

グローバル OSPFv3 の設定

グローバル OSPFv3 を設定するには、以下の手順に従います。

1 「**管理 | システム セットアップ | ネットワーク > ルーティング**」に移動します。

2 「**OSPFv3**」を選択します。

3 **設定**アイコンを選択します。「**設定**」ポップアップ ダイアログが表示されます。

4 以下のオプションを設定します。

- **OSPFv3 ルータ ID (n.n.n.n)** - ルータ ID を IP アドレス表記の任意の値で設定できます。セキュリティ装置上の IP アドレスのいずれとも無関係で、OSPF ネットワーク内の任意の一意の値に設定できます。
- **ABR 種別** - この OSPF ルータを参加させるトポロジを指定できます (互換性維持のため)。以下のオプションがあります。
  - **スタンダード** - RFC2328 に完全に準拠した ABR OSPF 動作です。
  - **Cisco** - ABR フラグを設定する前にバックボーンを設定してアクティブにする、Cisco の ABR 動作との相互運用性用。
  - **IBM** - ABR フラグを設定する前にバックボーンを設定してアクティブにする、IBM の ABR 動作との相互運用性用。
  - **ショートカット** - ショートカット エリアでは、ABR ルータがエリア 0 に接続されているかどうかにかかわらず、バックボーン以外のエリアにトラフィックを低メトリックで送信できます。
- **既定のメトリック (1-16777214)** - 他のルーティング情報元 (既定、静的、接続、RIP、VPN) からルートを再配布する際に使用されるメトリックを指定します。既定値 (**Undefined【未定義】**) は **1** で、最大値は 16,777,214 です。
- **自動コスト基準帯域幅 (Mb/s)**- 既定値は 100 です。
- **静的ルートを再配布する** - OSPF システムへの静的 (ポリシーベース ルーティング) ルートの通知を有効または無効にします。このオプションは、既定では選択されていません。

メモ：以下が、再配布されたすべてのルートに適用されます。

- **メトリック** - この再配布で明示的に設定するか、「**既定のメトリック**」オプションで指定した値 (**既定値**) を使用できます。
- **メトリック種別** - 再配布されたルート通知は LSA 種別 5 で、種別は**外部種別 1** (内部リンク コストを追加) または**外部種別 2** (外部リンク コストのみを使用) として選択できます。

メモ：再配布するルートのオプションを選択しなければ、これらのフィールドは淡色表示になっています。

- **接続されたネットワークを再配布する** - OSPF システムへのローカルに接続されたネットワークの通知を有効または無効にします。このオプションは、既定では選択されていません。
- **RIP ルートを再配布する** - RIP 経由で取得したルートの OSPF システムへの通知を有効または無効にします。このオプションは、既定では選択されていません。

5 「**適用**」を選択します。

「**ルーティング プロトコル**」セクションには、アクティブなすべての OSPF ルータの状況がインターフェース別に表示されます。

「**ルーティング ポリシー**」セクションには、OSPF が **OSPF** または **RIP ルート**として取得したルートが表示されます。

「**状況**」が使用可能になります。

RIP および RIPng の設定

トピック:

- RIP の設定 (524 ページ)

RIP の設定

RIP ルーティングをインターフェースに対して設定するには、以下の手順に従います。

1 「**管理 | ネットワーク > ルーティング**」に移動します。

2 「**RIP**」を選択します。

3 インターフェースの**編集**アイコンを選択します。「**インターフェース RIP 設定**」ダイアログが表示されます。

4 「**RIP**」で、モードを選択します。

無効 (既定)	このインターフェースでは RIP は無効です。「ステップ 12」に進みます。
送受信	このインターフェースの RIP ルータは更新を送信し、受信した更新を処理します。
送信のみ	このインターフェースの RIP ルータは更新を送信するだけで、受信した更新を処理しません。これは基本的なルーティング実装に似ています。
受信のみ	このインターフェースの RIP ルータは受信した更新を処理するだけです。
パッシブ	このインターフェースの RIP ルータは受信した更新を処理せず、CLI コマンド `neighbor` で指定された近隣 RIP ルータに更新を送信するだけです。 **重要**：このモードは、高度な RIP オプションを ARS-RIP CLI から設定する場合にのみ使用する必要があります (『*SonicOS CLI リファレンス ガイド*』を参照してください)。選択すると、他のすべてのオプションが淡色表示になります。

5 指定したオプションに応じて次の手順に従います。

- 「**送信のみ**」を指定した場合は、「ステップ 8」に進みます。
- 「**パッシブ**」を指定した場合は、「ステップ 12」に進みます。

6 「**受信**」で、RIP パケットを受け取るための RIP バージョンを選択します。

RIPv1	*ブロードキャスト* RIPv1 パケットのみ受信します。
RIPv2 (既定)	*マルチキャスト* RIPv2 パケットのみ受信します。RIP ルータの実装の一部 (SonicWall 機器の基本ルーティングなど) にはブロードキャストまたはマルチキャスト形式でRIPv2 を送信する機能がありますが、RIPv2 パケットはマルチキャストで送信されます。 **重要**：RIPv2 の更新を送信する機器ではマルチキャスト モードを使用してください。そうしないと、更新が ars-rip ルータで処理されません。

7 「**RIP**」で「**受信のみ**」を選択した場合は、「ステップ 11」に進みます。

8 ルートの取得元となったルータへの更新情報からそのルートを除外するには、「**スプリット ホライズン**」を選択します。これはルーティング ループを防止する一般的な RIP メカニズムです。「最大ホップ数 (494 ページ)」を参照してください。このオプションは、既定では選択されています。

9 スプリット ホライズン操作のオプション モードを指定するには、「**ポイズン リバース**」を選択します。取得したルートを含めないのではなく、ルートは無限メトリック (16) によって送信され、到達不可であることが示されます。「最大ホップ数 (494 ページ)」を参照してください。このオプションは、既定では選択されています。

10 「**送信**」で、パケットを送信するための RIP バージョンを選択します。

RIPv1	*ブロードキャスト* RIPv1 パケットを送信します。
RIPv2 - v1 互換	RIPv1 と互換性のある *マルチキャスト* RIPv2 パケットを送信します。
RIPv2 (既定)	*マルチキャスト* RIPv2 パケットを送信します。

11 パスワードの使用を強制するには、「**パスワードを使用**」を選択します。「**パスワード**」フィールドが使用可能になります。このオプションは、既定では選択されていません。

- 「**パスワード**」フィールドにパスワードを入力します。

12 「**OK**」を選択します。

RIPng の設定

RIP ルーティングをインターフェースに対して設定するには、以下の手順に従います。

1 「**管理 | システム セットアップ | ネットワーク > ルーティング > RIPng**」に移動します。

2 インターフェースの**編集**アイコンを選択します。「**インターフェース RIPng の設定**」ダイアログが表示されます。

3 「**RIPng**」で、モードを選択します。

無効 (既定)	このインターフェースでは RIPng は無効です。「ステップ 6」に進みます。
有効	このインターフェースの RIPng ルータは更新を送信し、受信した更新を処理します。
パッシブ	このインターフェースの RIP ルータは受信した更新を処理せず、CLI コマンド `neighbor` で指定された近隣 RIPng ルータに更新を送信するだけです。 **重要**：このモードは、高度な RIP オプションを ARS-RIP CLI から設定する場合にのみ使用する必要があります (『*SonicOS CLI リファレンス ガイド*』を参照してください)。

4 ルートの取得元となったルータへの更新情報からそのルートを除外するには、「**スプリット ホライズン**」を選択します。これはルーティング ループを防止する一般的な RIP メカニズムです。「最大ホップ数 (494 ページ)」を参照してください。このオプションは、既定では選択されています。

5 スプリット ホライズン操作のオプション モードを指定するには、「**ポイズン リバース**」を選択します。取得したルートを含めないのではなく、ルートは無限メトリック (16) によって送信され、到達不可であることが示されます。「最大ホップ数 (494 ページ)」を参照してください。このオプションは、既定では選択されています。

6 「**OK**」を選択します。

グローバル RIPng の設定

グローバル OSPFv3 を設定するには、以下の手順に従います。

1 「**管理 | システム セットアップ | ネットワーク > ルーティング**」に移動します。

2 「**OSPFv3**」を選択します。

3 **設定**アイコンを選択します。「**設定**」ポップアップ ダイアログが表示されます。

4 以下のオプションを設定します。

- **メトリック** - 他のルーティング情報元（既定、静的、接続、OSPF、VPN）からルートを再配布する際に使用されるメトリックを指定するために使用します。既定値 (未定義) は **1** で、最大値は 15 です。
- **デフォルト ルートを登録する** - このチェックボックスは、RIP システムへのセキュリティ装置の既定ルートの通知を有効または無効にします。
- **静的ルートを再配布する** - RIP システムへの静的 (ポリシーベース ルーティング) ルートの通知を有効または無効にします。メトリックはこの再配布に明示的に設定できます。または、「**既定のメトリック**」設定で指定した値 (既定値) を使用できます。
- **接続されたネットワークを再配布する** - RIP システムへのローカルに接続されたネットワークの通知を有効または無効にします。メトリックはこの再配布に明示的に設定できます。または、「**既定のメトリック**」設定で指定した値 (既定値) を使用できます。
- **OSPF ルートを再配布する** - OSPF 経由で取得したルートの RIP システムへの通知を有効または無効にします。メトリックはこの再配布に明示的に設定できます。または、「**既定のメトリック**」設定で指定した値 (既定値) を使用できます。

5 「**適用**」を選択します。

トンネル インターフェースに対する高度なルーティング設定

VPN トンネル インターフェースを高度なルーティングのために設定できます。そうするには、トンネル インターフェース設定の「**詳細**」タブで、高度なルーティングを有効にする必要があります。

トンネル インターフェースに対する高度なルーティングを有効にすると、「**ネットワーク > ルーティング**」の各種表示で他のインターフェースと一緒にテーブルに表示されます。

「高度なルーティング」オプションを設定するには、以下の手順に従います。

1 設定するトンネル インターフェースの「**RIP/RIPng 設定**」または「**OSPF/OSPFv3 設定**」列で**編集**アイコンを選択します。トンネル インターフェースの RIP および OSPF 設定は、従来のインターフェースの設定とよく似ています。

グローバル多種設定

番号付けされないトンネル インターフェースは物理インターフェースではなく固有の IP アドレスを持たないため、別のインターフェースの IP アドレスを "借用する" 必要があります。その結果、トンネル インターフェースに対する高度なルーティング設定には、トンネルの送信元と送信先の IP アドレスを指定するための、以下のオプションが含まれます。

- **IP アドレスの借用元** - IP アドレスがトンネル インターフェースに対する送信元 IP アドレスとして使用されているインターフェースです。

  メモ：借用した IP アドレスは静的アドレスである必要があります。

- **リモート IP アドレス** - トンネル インターフェースが接続されるリモート ピアの IP アドレスです。別のトンネル インターフェースを持つ SonicWall 対 SonicWall の設定の場合は、これはリモート ピア上のトンネル インターフェースの借用するインターフェースの IP アドレスになります。

高度なルーティングのためのトンネル インターフェース設定のガイドライン

高度なルーティングのためにトンネル インターフェースを設定する際には、以下のガイドラインが成功の手助けになります。

- 借用元のインターフェースには、静的 IP アドレス割り当てが必要です。
- 借用元のインターフェースでは、RIP または OSPF 有効の設定を持てません。

  ヒント：SonicWall は、単独で借用元のインターフェースとして使うためだけの VLAN インターフェースの作成を推奨します。これにより、有線接続インターフェースの使用時に競合を避けます。

- 借用元のインターフェースの IP アドレスは、プライベート アドレス空間のものである必要があり、すべてのリモート トンネル インターフェースのエンドポイントの中で一意の IP アドレスを持つ必要があります。
- トンネル インターフェースのエンドポイントのリモート IP アドレスは、借用元のインターフェースと同じネットワーク サブネット内にある必要があります。
- トンネル インターフェースがすべて異なるリモート機器に接続されるならば、複数のトンネル インターフェースに対して同じ借用元のインターフェースが使うことができます。
- 1 台の装置の 2 つ以上のトンネル インターフェースが同一のリモート機器に接続される場合は、それぞれのトンネル インターフェースは、別々の借用元のインターフェースを使う必要があります。

ネットワーク設定の特定の状況によっては、トンネル インターフェースが正しく機能することを確実にするために、これらのガイドラインは完全ではないことがあります。しかし、これらのガイドラインは、SonicWall によるベスト プラクティスであり、潜在的なネットワーク接続性の問題を回避するのに役立ちます。

BGP の高度なルーティングの設定

メモ：BGP は次の装置でサポートされています。

- NSA 2600 以降のセキュリティ装置
- SonicOS 拡張のライセンスを購入済みの TZ400 シリーズ、TZ500 シリーズ、および TZ600 セキュリティ装置

TZ300 シリーズと SOHO Wireless セキュリティ装置では BGP はサポートされません。

Border Gateway Protocol (BGP) は、明確に定義され、個別に管理されるネットワーク ドメインである自律システム (AS) 間でルーティング情報を伝達するために使用される、大規模ルーティング プロトコルです。BGP サポートは、セキュリティ装置がネットワークの AS の端点にある従来の BGP ルータの代わりをすることを考慮しています。現在の SonicWall の BGP 実装は、ネットワークが 1 つの ISP をインターネット プロバイダとして使い、そのプロバイダへの接続が 1 つだけのシングルプロバイダ/シングルホーム環境に対して最も適しています。SonicWall BGP はまた、ネットワークが 1 つの ISP を使っているが、そのプロバイダへの少数の異なるルートがあるシングルプロバイダ/マルチホーム環境のサポートも可能です。BGP は、SonicOS 管理インターフェースの「**ネットワーク > ルーティング**」ページで有効にしてから、SonicOS のコマンド ライン インターフェース (CLI、『*SonicOS CLI リファレンス ガイド*』を参照) を通じて完全に設定します。

SonicWall の BGP 実装の詳細については、「BGP の高度なルーティング (1014 ページ)」を参照してください。

BGP セッション用 IPSec トンネルの設定

BGP は、パケットを平文で送信します。したがって、セキュリティを強化するため、SonicWall では BGP セッションに使用する IPSec トンネルを設定することをお勧めします。BGP 用 IPSec トンネルを設

定して BGP を有効にする方法については、「BGP の高度なルーティング (1014 ページ)」を参照してください。

管理インターフェースから BGP が有効になった後、SonicOS のコマンドライン インターフェース (CLI) を使用して、BGP 設定の仕様が実行されます。SonicWall セキュリティ装置の BGP 実装の詳細については、「BGP の高度なルーティング (1014 ページ)」を参照してください。

アプリベースのルートの設定

アプリベースのルート エントリを設定するには:

1 「**管理 | ポリシー > オブジェクト > 一致オブジェクト**」に移動します。

2 「**追加**」から、「**一致オブジェクト**」を選択します。「**一致オブジェクトの作成**」ダイアログが表示されます。

3 「**一致オブジェクト種別**」から、以下を選択します。

- **アプリケーション種別リスト**
- **アプリケーション リスト**

4 一致オブジェクトの設定を完了します。

5 「**OK**」を選択します。

6 「**管理 | システム セットアップ > ネットワーク > ルーティング**」に移動します。

7 ルート ポリシーを作成します。

8 「**OK**」を選択します。

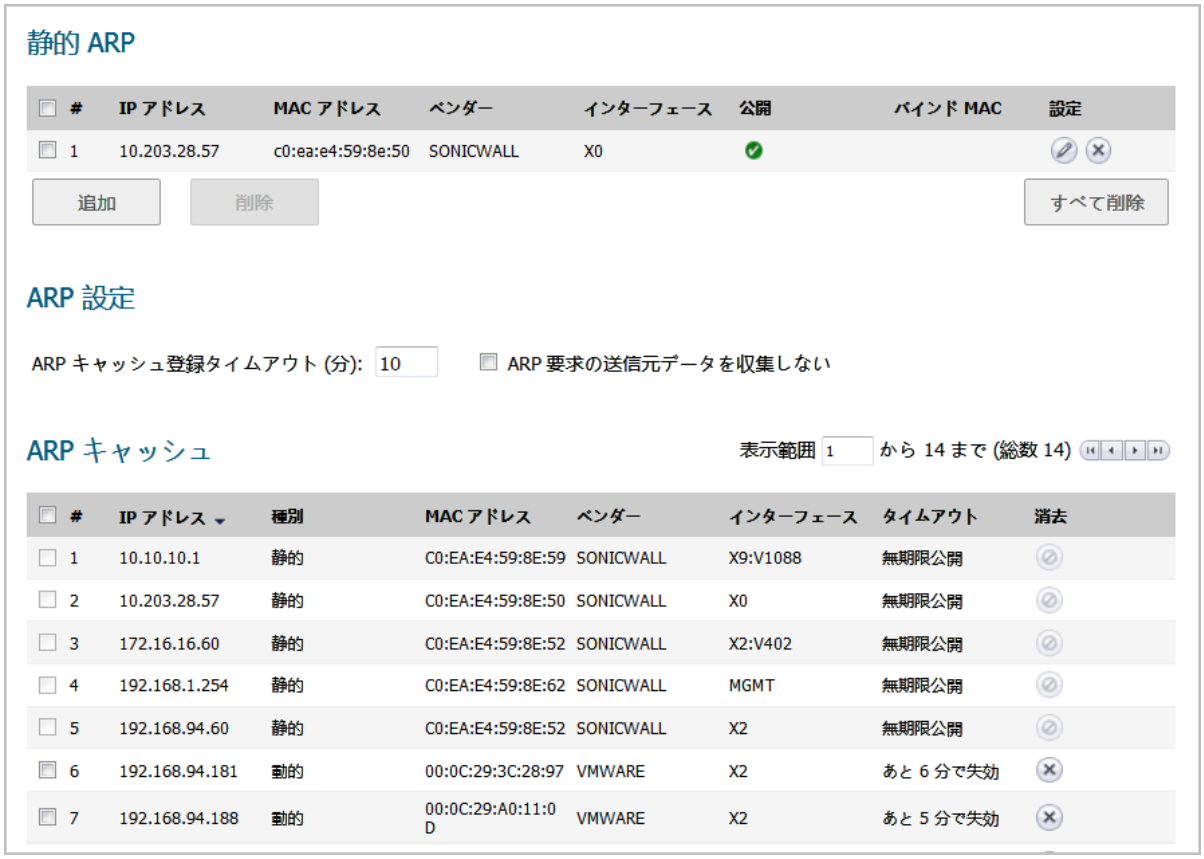
23

ARP トラフィックの管理

トピック:

- ネットワーク > ARP (530 ページ)
  - 静的 ARP エントリ (531 ページ)
  - ARP 設定 (535 ページ)
  - ARP キャッシュ (535 ページ)

ネットワーク > ARP



ARP (Address Resolution Protocol) は、第 3 層 (IP アドレス) を第 2 層 (物理アドレスまたは MAC アドレス) に割り付け、同じサブネットに存在するホスト間の通信を可能にします。ARP は、ネットワークのトラフィックを増大させるブロードキャスト プロトコルです。ブロードキャスト トラフィックを最小限にするため、ARP キャッシュが保持されて、以前に取得された ARP 情報が保管および再使用されます。

トピック:

- 静的 ARP エントリ (531 ページ)
- ARP 設定 (535 ページ)
- ARP キャッシュ (535 ページ)

静的 ARP エントリ

静的 NDP 機能により、レイヤ 2 MAC アドレスとレイヤ 3 IP アドレスとの間に静的割付を作成できます。

トピック:

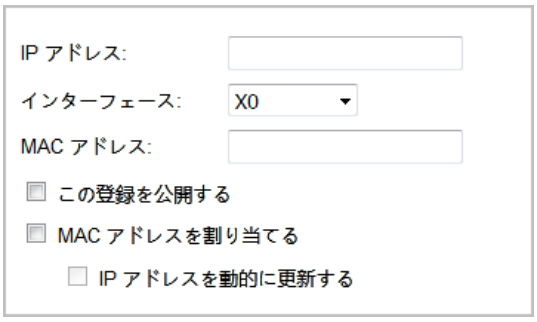
- 静的 ARP の設定 (531 ページ)
- 静的 ARP エントリの編集 (532 ページ)
- 静的 ARP によるセカンダリ サブネット (533 ページ)
- 静的 ARP エントリの表示 (534 ページ)

静的 ARP の設定

静的 ARP を設定するには、以下の手順に従います。

1 「**ネットワーク > ARP**」に移動します。

2 「**静的 ARP**」テーブルで、「**追加**」を選択します。「**静的 ARP の追加**」ダイアログが表示されます。



3 「**IP アドレス**」フィールドに、SonicWall セキュリティ装置の IP アドレスを入力します。

4 「**インターフェース**」で、この静的 ARP エントリと関連付けられるセキュリティ装置上の LAN インターフェースを選択します。

5 「**MAC アドレス**」フィールドに、セキュリティ装置の MAC アドレスを入力します。

6 セキュリティ装置が、指定された IP アドレスに対する ARP クエリに、指定された MAC アドレスで応答するようにするには、「**この登録を公開する**」オプションを選択します。このオプションは、既定では選択されていません。

このオプションを使用すると、例えば、セキュリティ装置の MAC アドレスを追加して、セキュリティ装置で特定のインターフェースのバックアップの IP アドレスに応答できるようになります。「静的 ARP によるセカンダリ サブネット (533 ページ)」を参照してください。このオプションを選択すると、「**MAC アドレス**」フィールドと「**MAC アドレスを割り当てる**」オプションが淡色表示になります。

7 「**この登録を公開する**」を選択した場合は、「ステップ 10」に進みます。

8 指定された MAC アドレスを目的の IP アドレスおよびインターフェースにバインドするには、「**MAC アドレスを割り当てる**」を選択します。このオプションは、既定では選択されていません。

このオプションにより、(ネットワーク カードの一意の MAC アドレスで認識される) 特定のワークステーションを、セキュリティ装置上の指定のインターフェースでのみ使用できるようになります。MAC アドレスが 1 つのインターフェースにバインドされた後、セキュリティ装置は次のように動作します。

- 他のどのインターフェースでもその MAC アドレスに応答しなくなります。
- 存在している可能性がある、その MAC アドレスに対する動的にキャッシュされた参照をすべて削除します。
- その MAC アドレスへの追加的な (一意でない) 静的割付を禁止します。

「MAC アドレスを割り当てる」を選択すると、「**IP アドレスを動的に更新する**」が使用可能になります。

9 DHCP を動的な IP アドレスの割り当てに使用するときに MAC アドレスをインターフェースにバインドできるようにするには、「**IP アドレスを動的に更新する**」を選択します、これは「**MAC アドレスを割り当てる**」オプションのサブ機能です。

このオプションを有効にすると、「**IP アドレス**」フィールドが淡色表示になって 0.0.0.0 に設定され、「**MAC アドレス**」フィールドが使用可能になり、セキュリティ装置の内部 DHCP サーバによって割り当てられた IP アドレス (IP ヘルパーを使用中の場合は外部 DHCP サーバによって割り当てられた IP アドレス) が ARP キャッシュに格納されます。

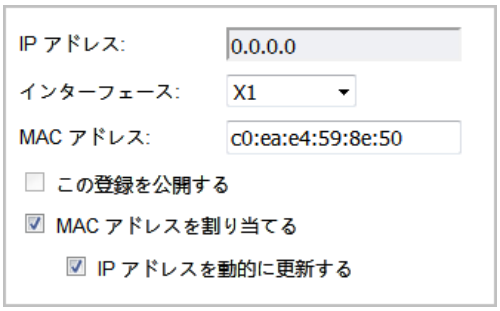
10 「**OK**」を選択します。

静的 ARP エントリの編集

静的 ARP エントリを編集するには、以下の手順に従います。

1 「**ネットワーク > ARP**」に移動します。

2 「**静的 ARP**」テーブルで、そのエントリの「**設定**」列にある**編集**アイコンを選択します。「**静的 ARP の編集**」ダイアログが表示されます。



3 変更を加えます。

4 「**OK**」を選択します。エントリが更新されます。

静的 ARP によるセカンダリ サブネット

静的 ARP 機能により、自動 NAT ルールを追加せずに、セカンダリ サブネットを別のインターフェースに追加できます。

トピック:

- セカンダリ サブネットの追加 (533 ページ)
- 例 (533 ページ)

セカンダリ サブネットの追加

静的ARP 方式を使用してセカンダリ サブネットを追加するには、以下の手順に従います。

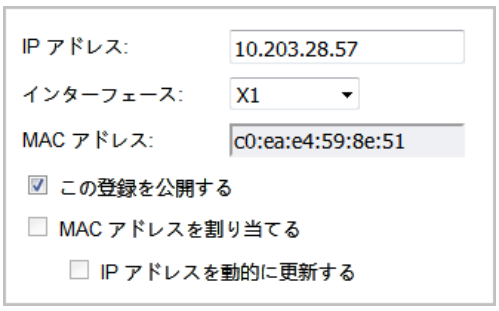
1. セカンダリのサブネットに使用するゲートウェイ アドレスの静的 ARP を、“公開する" オプションを有効に設定して追加し、その ARP に、接続するセキュリティ装置インターフェースの MAC アドレスを割り当てます。
2. セカンダリのサブネットへの静的ルートを追加します。これにより、セキュリティ装置がそれを有効なトラフィックと見なすようになり、そのサブネットのトラフィックをどのインターフェースにルーティングすべきかが認識されます。
3. アクセス ルールを追加して、サブネットへのトラフィックが正しいネットワーク インターフェースを通過できるようにします。
4. 必要に応じて、アップストリームの機器に静的ルートを追加し、どのゲートウェイ IP を使用すればセカンダリのサブネットに到達可能かを識別できるようにします。

例

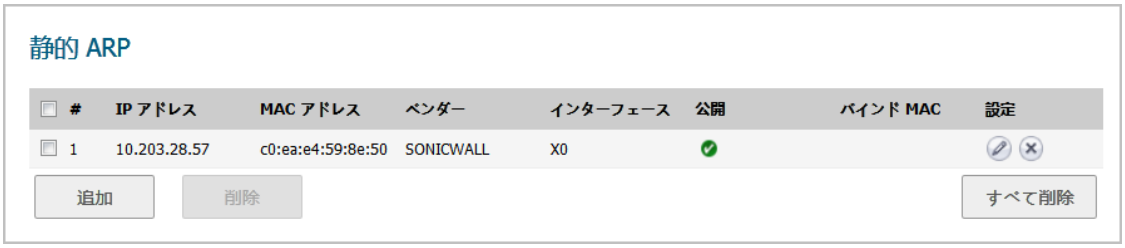
次のネットワークの例について考えます (「セカンダリ サブネットの追加 (533 ページ)」を参照してください)。

追加された設定をサポートするには、以下の手順に従います。

1. セカンダリ サブネットのゲートウェイとなるアドレス、192.168.50.1 について、公開される静的 ARP エントリを作成します。
2. これを適切な LAN インターフェースと関連付けます。「**ネットワーク > ARP**」で、「**静的 ARP**」テーブルの下にある「**追加**」を選択します。
3. 次のエントリを追加します。



4 「**OK**」を選択します。エントリは「**静的 ARP**」テーブルに表示されます。



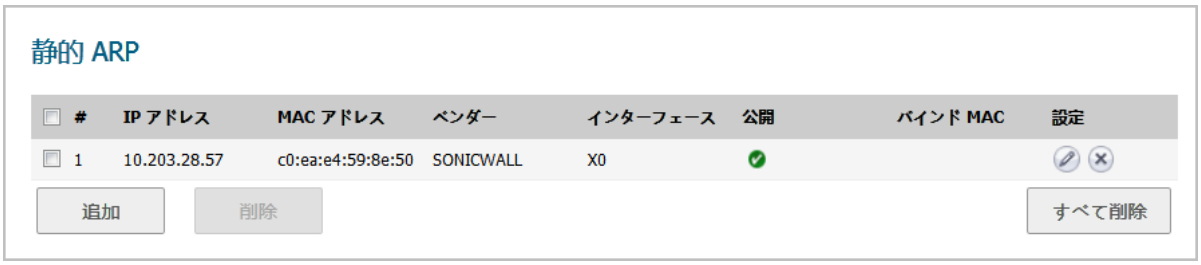
5 「**ネットワーク > ルーティング**」を選択します。

6 サブネット マスク `255.255.255.0` を指定して、ネットワーク `192.168.50.0/24` への静的ルートを X3 インターフェース上に追加します。静的ルートの追加については、「ルート通知とルート ポリシーの設定 (486 ページ)」を参照してください。

7 トラフィックがサブネット `192.168.50.0/24` に到達し、またサブネット `192.168.50.0/24` が LAN 上のホストに到達できるようにするために、「**ポリシー | ルール > アクセス ルール**」ページに移動します。

8 トラフィックの通過を許可するための適切なアクセス ルールを追加します。アクセス ルールの追加については、『*SonicOS ポリシー*』を参照してください。

静的 ARP エントリの表示



IP アドレス	ゲートウェイの役割を果たすセキュリティ装置の IP アドレス。
MAC アドレス	ゲートウェイの役割を果たすセキュリティ装置の MAC アドレス。
ベンダー	セキュリティ装置のメーカーの名前。
インターフェース	このエントリに関連付けられている LAN インターフェース。
公開	緑色のチェックマークにより、セキュリティ装置が、指定された IP アドレスに対する ARP クエリに、指定された MAC アドレスで応答するかどうかを示します。
バインド MAC	緑色のチェックマークにより、指定された IP アドレスおよびインターフェースに MAC アドレスがバインドされているかどうかを示します。
設定	エントリの**編集**アイコンと**削除**アイコンを表示します。

ARP 設定

ARP キャッシュ登録タイムアウト (分)	エントリがタイムアウトしてキャッシュから消去されるまでの時間を指定します。最小値は 2 分、最大値は 600 分 (10 時間) 、既定値は **10** 分です。
ARP 要求の送信元データを収集しない	ARP 要求から送信元データが取得されないようにします。このオプションは、既定では選択されていません。

ARP キャッシュ

IP アドレス	セキュリティ装置の IP アドレス。
種別	ARP が**静的**または**動的**のどちらであるかを示します。
MAC アドレス	IP アドレスと関連付けられている MAC アドレス。
ベンダー	セキュリティ装置のメーカーの名前。
インターフェース	この ARP エントリに関連付けられている LAN インターフェース。
タイムアウト	このエントリについてのキャッシュでの残り時間を示します。設定時にエントリが公開されていた場合、「**タイムアウト**」には「無期限公開」と表示されます。
消去	ARP キャッシュからエントリを消去するための**削除**アイコンを表示します。 **メモ**： **削除**アイコンは**動的**エントリでのみ使用できます。

ARP キャッシュの消去

ネットワーク上の機器の IP アドレスが変更された場合は、ARP キャッシュを消去する必要があります。IP アドレスは物理アドレスにリンクされるので、変更された IP アドレスは ARP キャッシュ内で物理アドレスに関連付けられたままです。ARP キャッシュを消去すると、新しい情報が収集され、ARPキャッシュに保管されます。

ヒント：エントリがタイムアウトするまでの時間を設定するには、「**ARP キャッシュ登録タイムアウト (分)**」フィールドに時間を分単位で入力します。「ARP 設定 (535 ページ)」を参照してください。

「ARP キャッシュ」テーブル内の 1 つの動的エントリを消去するには:

1 「**消去**」列の**削除**アイコンを選択します。

「ARP キャッシュ」テーブル内の 1 つ以上の動的エントリを消去するには:

1 消去する 1 つ以上のエントリのチェックボックスをオンにします。「**消去**」が使用可能になります。

2 「**消去**」を選択します。

「ARP キャッシュ」テーブル内のすべての動的エントリを消去するには:

1 「**ARP キャッシュの消去**」を選択します。

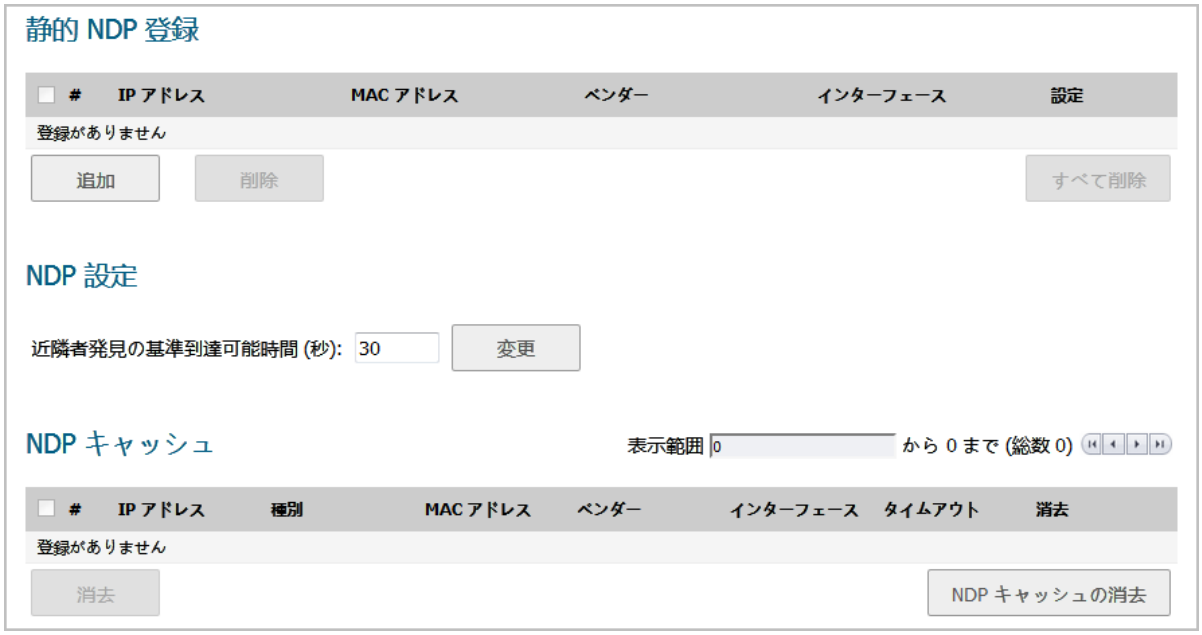
24

近隣者発見プロトコルの設定

トピック:

- ネットワーク > 近隣者発見 (IPv6 のみ) (537 ページ)
  - 静的 NDP 登録 (538 ページ)
  - NDP 設定 (539 ページ)
  - NDP キャッシュ (539 ページ)
  - 静的 NDP 登録の設定 (540 ページ)
  - 静的 NDP 登録の編集 (541 ページ)
  - NDP キャッシュの消去 (541 ページ)

ネットワーク > 近隣者発見 (IPv6 のみ)



近隣者発見プロトコル (NDP) は、IPv4 の ICMP と ARP が実現するいくつかのタスクを実行するために IPv6 の一部として作成された、新しいメッセージング プロトコルです。ARP と同じように、近隣者発見によって動的エントリ (登録) のキャッシュが構築されます。静的な近隣者発見のエントリ (登録) は設定することができます。「IPv4/IPv6 近隣者メッセージと機能」テーブルに、従来の IPv4 近隣者メッセージと類似した IPv6 近隣者メッセージおよび機能を示します。

IPv4/IPv6 近隣者メッセージと機能

IPv4 近隣者メッセージ	IPv6 近隣者メッセージ
ARP 要求メッセージ	近隣者要請メッセージ
ARP 応答メッセージ	近隣者広告メッセージ
ARP キャッシュ	近隣者キャッシュ
重複回避用 ARP	重複アドレス検出
ルータ要請メッセージ (オプション)	ルータ要請 (必須)
ルータ広告メッセージ (オプション)	ルータ広告 (必須)
リダイレクト メッセージ	リダイレクト メッセージ

静的 NDP 機能により、レイヤ 3 IPv6 アドレスとレイヤ 2 MAC アドレスとの間に静的割付を作成できます。

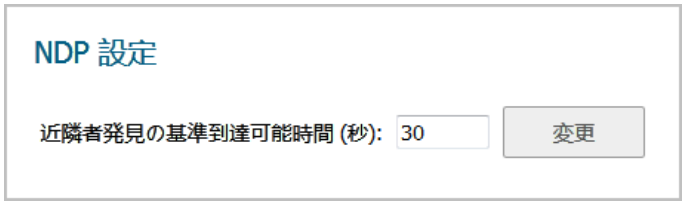
トピック:

- 静的 NDP 登録 (538 ページ)
- NDP 設定 (539 ページ)
- NDP キャッシュ (539 ページ)
- 静的 NDP 登録の設定 (540 ページ)
- 静的 NDP 登録の編集 (541 ページ)
- NDP キャッシュの消去 (541 ページ)

静的 NDP 登録

IP アドレス	リモート機器の IPv6 IP アドレス。
MAC アドレス	リモート機器の MAC アドレス。
ベンダー	リモート機器の製造元の名前。
インターフェース	リモート機器に関連付けられているインターフェース。
設定	エントリの**編集**アイコンと**削除**アイコンがあります。

NDP 設定



近隣者に到達するための最大時間を「**NDP 設定**」に指定します。

メモ：IPv6 では、「**ネットワーク > インターフェース > インターフェースの編集 > 詳細設定**」ダイアログでこの値を各インターフェースに対して設定することもできます。インターフェースでルータ広告が有効になっている場合、あるインターフェースに対して設定されている値はそのインターフェースでのみ使用されます。詳細については、「インターフェースの設定 (292 ページ)」を参照してください。

最大時間を指定するには、以下の手順に従います。

1 「**近隣者発見の基準到達可能時間 (秒)**」フィールドに数値を入力します。最小値は 0 秒、最大値は 3600 秒、既定値は **30** 秒です。

ヒント：このオプションの値が 0 に設定されている場合は、NDP 設定のグローバル値が使用されます。

2 **変更** をクリックします。

NDP キャッシュ

NDP キャッシュ テーブルに、現在のすべての IPv6 近隣者が表示されます。

IP アドレス	近隣者機器の IPv6 IP アドレス。
種別	近隣者の種別: • **REACHABLE** - 近隣者は 30 秒以内で到達可能であると認識されています。 • **STALE** - 近隣者は既に到達可能であると認識されていなく、その近隣者に 1200 秒以内にトラフィックが送信されています。 • **STATIC** - 近隣者は静的近隣者として手動で設定されました。
MAC アドレス	近隣者機器の IPv6 MAC アドレス。
ベンダー	近隣者機器の製造元の名前。
インターフェース	この近隣者機器に関連付けられているインターフェース。

タイムアウト	ユーザがタイムアウトするまでの無動作時間の長さ。
消去	エントリの**削除**アイコンがあります。

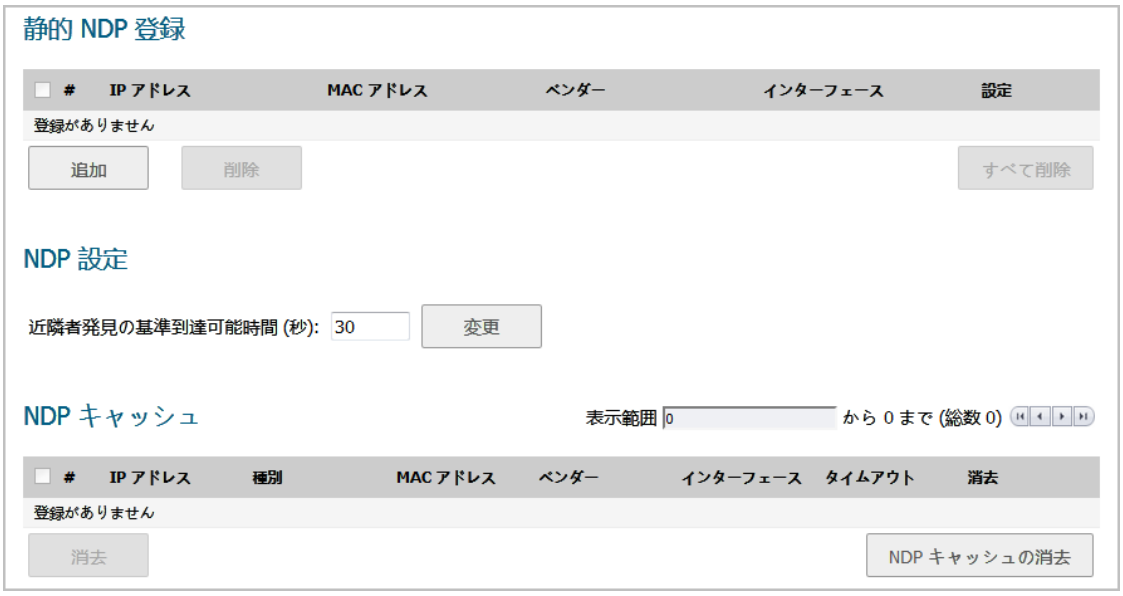
以下の種別の近隣者が表示されます。

- **REACHABLE** - 近隣者は 30 秒以内で到達可能であると認識されています。
- **STALE** - 近隣者は既に到達可能であると認識されていなく、その近隣者に 1200 秒以内にトラフィックが送信されています。
- **STATIC** - 近隣者は静的近隣者として手動で設定されました。

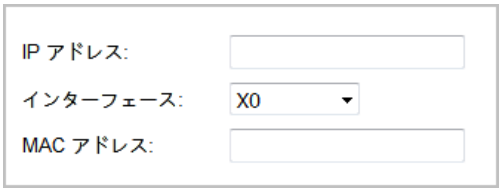
静的 NDP 登録の設定

静的 NDP 登録を設定するには、以下の手順を実行します。

1 「**ネットワーク > 近隣者発見**」ページに移動します。



2 「**静的 NDP 登録**」テーブルで、「**追加**」を選択します。「**静的 NDP の追加**」ダイアログが表示されます。



3 「**IP アドレス**」フィールドに、リモート機器の IPv6 アドレスを入力します。

4 「**インターフェース**」から、このエントリで使用する SonicWall セキュリティ装置上のインターフェースを選択します。

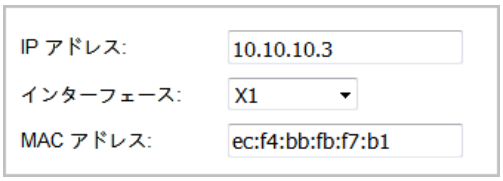
5 「**MAC アドレス**」フィールドに、リモート機器の MAC アドレスを入力します。

6 「**OK**」を選択します。静的 NDP 登録が追加されます。

静的 NDP 登録の編集

静的NDP エントリを編集するには、以下の手順に従います。

1 「**静的 NDP 登録**」テーブルで、エントリの「**設定**」列にある**編集**アイコンを選択します。「**静的 NDP の編集**」ダイアログが表示されます。



2 変更を加えます。

3 「**OK**」を選択します。エントリが更新されます。

NDP キャッシュの消去

ネットワーク上の機器の IP アドレスが変更された場合は、NDP キャッシュの消去が必要になることがあります。IP アドレスは物理アドレスにリンクされるので、変更された IP アドレスは NDP キャッシュ内で物理アドレスに関連付けられたままです。NDP キャッシュを消去すると、新しい情報が収集され、NDP キャッシュに保管されます。

ヒント：エントリがタイムアウトするまでの時間を設定するには、「**NDP キャッシュ エントリ タイムアウト (分)**」フィールドに時間を分単位で入力します。「NDP 設定 (539 ページ)」を参照してください。

「NDP キャッシュ」テーブルのエントリを消去するには、以下の手順に従います。

1 「**消去**」列の**削除**アイコンを選択します。

「NDP キャッシュ」テーブル内の 1 つ以上のエントリを消去するには、以下の手順に従います。

1 消去する 1 つ以上のエントリのチェックボックスをオンにします。2 つの消去ボタンがアクティブになります。

2 「**消去**」ボタンまたは「**NDP キャッシュの消去**」ボタンのどちらかを選択します。

「NDP キャッシュ」テーブル内のすべてのエントリを消去するには、以下の手順に従います。

1 「**NDP キャッシュ**」テーブルのヘッダーにあるチェックボックスをオンにします。2 つの消去ボタンがアクティブになります。

2 「**消去**」ボタンまたは「**NDP キャッシュの消去**」ボタンのどちらかを選択します。

25

MAC-IP アンチスプーフの設定

トピック:

- MAC-IP アンチスプーフ保護について (542 ページ)
  - IP ヘルパーへの拡張 (543 ページ)
- ネットワーク > MAC-IP アンチスプーフ (544 ページ)
  - インターフェースに対する設定 (545 ページ)
  - アンチスプーフ キャッシュ (546 ページ)
  - スプーフ検知リスト (547 ページ)
- MAC-IP アンチスプーフ保護の設定 (548 ページ)
  - トラフィック統計の表示 (548 ページ)
  - IPv6 インターフェースの MAC-IP アンチスプーフ設定の編集 (549 ページ)
  - IPv4 インターフェースの MAC-IP アンチスプーフ設定の編集 (550 ページ)
  - アンチスプーフ キャッシュへの機器の追加 (552 ページ)
  - アンチスプーフ キャッシュ エントリの削除 (553 ページ)
  - 表示対象のフィルタ (553 ページ)
  - スプーフ検知リストからの静的エントリの追加 (554 ページ)

MAC-IP アンチスプーフ保護について

MAC および IP アドレスをベースにした攻撃は、今日のネットワーク セキュリティ環境でますます一般化しています。この種の攻撃は、ローカル エリア ネットワーク (LAN) を標的にすることが多く、ネットワークの外部からも内部からも行われることがあります。実際、オフィスの会議室、学校、図書館など、内部 LAN がある程度公開されている場所ならどこでも、この種の攻撃の緒になる可能性があります。これらの攻撃にはさまざまな異名があり、 man-in-the-middle 攻撃、ARP ポイズニング、SPITS などと呼ばれています。MAC-IP アンチスプーフ機能は、ネットワークへのアクセスを制御する種々の方法を管理者に提供し、OSI レイヤ 2/3 へのスプーフィング攻撃を排除することにより、これらの攻撃のリスクを減じます。

MAC-IP アンチスプーフ機能は 2 つの点に重点的に取り組んでいます。

- 1 つは受付制御で、これはどの機器にネットワークへのアクセスを許すかを選択できるようにするものです。
- もう 1 つは、第 2 層へのサービス拒否攻撃などのスプーフィング攻撃の排除です。

これらの目標を達成するためには、2 つの情報キャッシュを構築する必要があります。 それは MAC-IP アンチスプーフ キャッシュと ARP キャッシュです。

MAC-IP アンチスプーフ キャッシュは、着信パケットを検証し、ネットワーク内に入れてよいかどうかを判定するためのものです。着信パケットの送信元の MAC アドレスと IP アドレスがこのキャッシュ内から検索されます。それらのアドレスが見つかれば、そのパケットの通過が許可されます。MAC-IP アンチスプーフ キャッシュは、次のサブシステムのうちの 1 つ以上のものから構築されます。

- DHCP サーバベースのリース (SonicWall - DHCP サーバ、IPv4 のみ)
- DHCP リレーベースのリース (SonicWall - IP ヘルパー、IPv4 のみ)
- 静的 ARP エントリ、IPv4 のみ
- ユーザが作成した静的エントリ

ARP キャッシュは次のサブシステムから構築されます。

- ARP パケット (ARP 要求と ARP 応答の両方、IPv4 のみ)
- ユーザ作成エントリからの静的 ARP エントリ、IPv4 のみ
- MAC-IP アンチスプーフ キャッシュ

MAC-IP アンチスプーフ サブシステムは、ARP キャッシュをロックすることで送信 (イーグレス) 制御を実現し、不正な機器や望ましくない ARP パケットによって送信パケット (ネットワークから出ていくパケット) がなりすましに利用されないようにします。これにより、マッピングに基づいて SonicWall セキュリティ装置で意図しない機器にパケットがルーティングされるのを防ぎます。また、ARP キャッシュ内のクライアントの MAC アドレスを更新して、man-in-the-middle 攻撃も防ぎます。

IP ヘルパーへの拡張

IP ヘルパーの DHCP リレー サブシステムからのリースをサポートするには、以下の手順に従います (「**ネットワーク > IP ヘルパー**」)。

- DHCP リレー ロジックの一部として、IP ヘルパーはクライアントと DHCP サーバとの間で交換されるリースを学習し、それらをフラッシュ メモリに保存します。
- これらの学習されたリースは、IP ヘルパー状態同期メッセージの一部として、アイドル状態の SonicWall セキュリティ装置に同期されます。

リースからの MAC アドレスと IP アドレスのバインドは、MAC-IP アンチスプーフ キャッシュに変換されます。

IP ヘルパーの詳細については、「IP ヘルパーの使用 (588 ページ)」を参照してください。

ネットワーク > MAC-IP アンチスプーフ

IPv6

IPv4

このセクションでは、SonicWall SonicOS で MAC-IP アンチスプーフ保護を計画、設計、および実装する方法について説明します。

トピック:

- インターフェースに対する設定 (545 ページ)
- アンチスプーフ キャッシュ (546 ページ)
- スプーフ検知リスト (547 ページ)

インターフェースに対する設定

メモ：緑色のチェック マーク アイコンは、その設定が有効になっていることを示します。

IPv6

インターフェースに対する設定	MAC-IP アンチスプーフを適用できるすべてのインターフェースがリストされます。表示用の既定の設定は「**すべて**」です。
インターフェース	「**インターフェースに対する設定**」で選択されているインターフェース。
強制	このインターフェースで受信アンチスプーフが強制されているかどうかを示します。
有効	このインターフェースで MAC-IP アンチスプーフが有効になっているかどうかを示します。
NDP ロック	このインターフェース上のすべての送信パケットに対して MAC-IP アンチスプーフ チェックが有効になっているかどうかを示します。
静的 NDP	対応する MAC-IP アンチスプーフ テーブル エントリがすべての静的 NDP エントリに対して作成されているかどうかを示します。
スプーフ検知	アンチスプーフ キャッシュに一致しないパケットのための MAC-IP アンチスプーフ検知リストが作成されるかどうかを示します。 **メモ**： MAC-IP アンチスプーフ リストから除外されているインターフェースは、 • 非イーサネット インターフェース • Portshield メンバー インターフェース • 高可用性インターフェース • 高可用性データ インターフェース
管理を許可	有効な MAC-IP アンチスプーフ キャッシュがなくてもセキュリティ装置宛てのすべてのトラフィックが許可されるかどうかを示します。
設定	エントリに対する**統計**アイコンと**編集**アイコンがあります。

IPv4

インターフェースに対する設定	MAC-IP アンチスプーフを適用できるすべてのインターフェースがリストされます。表示用の既定の設定は「**すべて**」です。
インターフェース	「**インターフェースに対する設定**」で選択されているインターフェース。

強制	このインターフェースで受信アンチスプーフが強制されているかどうかを示します。
有効	このインターフェースで MAC-IP アンチスプーフが有効になっているかどうかを示します。
ARP ロック	このインターフェース上のすべての送信パケットに対して MAC-IP アンチスプーフ チェックが有効になっているかどうかを示します。
ARP 監視	接続されている機器の ARP ポイズニング防御が有効になっているかどうかを示します。
静的 ARP	対応する MAC-IP アンチスプーフ テーブル エントリがすべての静的 ARP エントリに対して作成されているかどうかを示します。
DHCP サーバ	MAC-IP アンチスプーフ エントリが DHCP リース (SonicWall の DHCP サーバ) から設定されているかどうかを示します。
DHCP リレー	MAC-IP アンチスプーフ エントリが DHCP リース (DHCP リレー - IP ヘルパー) から設定されているかどうかを示します。
スプーフ検知	アンチスプーフ キャッシュに一致しないパケットのための MAC-IP アンチスプーフ検知リストが作成されるかどうかを示します。 **メモ：** 以下のインターフェースは、MAC-IP アンチスプーフ リストから除外されます。 • 非イーサネット インターフェース • Portshield メンバー インターフェース • 高可用性インターフェース • 高可用性データ インターフェース
管理を許可	有効な MAC-IP アンチスプーフ キャッシュがなくてもファイアウォール宛てのすべてのトラフィックが許可されるかどうかを示します。
設定	エントリに対する**統計**アイコンと**編集**アイコンがあります。

アンチスプーフ キャッシュ

MAC-IP アンチスプーフ キャッシュには、MAC アドレスから IP アドレスへのすべてのバインドが登録されます。これには、その時点で次の状態にあるすべての機器を含めることができます。

- ネットワークへのアクセスが "許可" された機器として登録されているもの。
- 背後にネットワークを持つルータのように機能する機器として指定されているもの。
- ネットワークから "排除" された (アクセスを拒否された) 機器として登録されているもの。

MAC-IP アンチスプーフ機能を有効にしていても、次のタイプのパケットはこの機能をバイパスします。

- 非 IP パケット。
- 送信元 IP が 0 である DHCP パケット。
- VPN トンネルからのパケット。
- 送信元 IP が無効なユニキャスト IP であるパケット。
- アンチスプーフの設定で管理の状態が有効になっていないインターフェースからのパケット。

テーブルの下部にアンチスプーフ ルックアップ統計が表示されます。

IP アドレス	機器の IP アドレス
種別	エントリの種別: **静的**または**リース**
インターフェース	受信トラフィックを受け取るインターフェース
MAC アドレス	機器の MAC アドレス
ベンダー	機器の製造元 (既知の場合)
ホスト名	機器のホスト名 (既知の場合)
ルータ	設定時に機器がルータの候補として指定されていたか
ブラックリスト	設定時に機器がブラックリストの対象として指定されていたか
設定	各エントリに対する**統計**アイコン、**編集**アイコン、**削除**アイコンが表示されます。

1 つまたは複数の機器でキャッシュ統計をクリアするには、以下の手順に従います。

1 「**ネットワーク > MAC-IP アンチスプーフ**」に移動します。

2 1 つまたは複数の機器を選択します。

3 「**統計のクリア**」を選択します。

最新のキャッシュ情報を表示するには、以下の手順に従います。

1 「**ネットワーク > MAC-IP アンチスプーフ**」に移動します。

2 「**アンチスプーフ キャッシュ**」テーブルの下部にある「**再表示**」を選択します。

スプーフ検知リスト

スプーフ検知リストには、受信アンチスプーフ キャッシュ チェックをパスできなかった機器が表示されます。このリストのエントリは、「**アンチスプーフ キャッシュ**」テーブルの静的アンチスプーフ エントリとして追加できます。

IP アドレス	機器の IP アドレス。
インターフェース	受信トラフィックを受け取るインターフェース。
MAC アドレス	機器の MAC アドレス。
ベンダー	機器の製造元 (既知の場合)。

名前	機器の名前。
パケット	受信されたパケットの数。
追加	**編集**アイコンが表示されています。

スプーフ検知リストからエントリを消去するには、以下の手順に従います。

1 「**消去**」を選択します。

NetBIOS を使用して各機器の名前を解決するには、以下の手順に従います。

1 「**解決**」を選択します。

最新のキャッシュ情報を表示するには、以下の手順に従います。

1 「**スプーフ検知リスト**」テーブルの下部にある「**再表示**」を選択します。

MAC-IP アンチスプーフ保護の設定

トピック:

- トラフィック統計の表示 (548 ページ)
- IPv6 インターフェースの MAC-IP アンチスプーフ設定の編集 (549 ページ)
- IPv4 インターフェースの MAC-IP アンチスプーフ設定の編集 (550 ページ)
- アンチスプーフ キャッシュへの機器の追加 (552 ページ)
- アンチスプーフ キャッシュ エントリの削除 (553 ページ)
- 表示対象のフィルタ (553 ページ)
- スプーフ検知リストからの静的エントリの追加 (554 ページ)

トラフィック統計の表示

「設定」または「アンチスプーフ キャッシュ」テーブルにインターフェースのトラフィック統計を表示するには、以下の手順に従います。

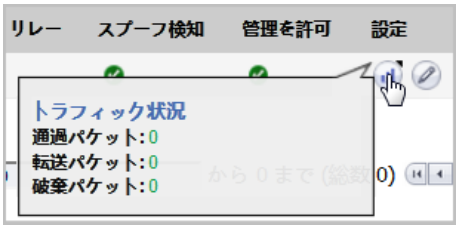
1 「**ネットワーク > MAC-IP アンチスプーフ**」に移動します。

2 「**設定**」テーブルにあるインターフェースのトラフィック統計を表示するには、「**インターフェースに対する設定**」から表示対象のインターフェースを選択します。既定値は「**すべて**」です。

3 インターフェースの**統計**アイコンの上にマウス ポインタを置きます。

4 「**トラフィック統計**」ポップアップに次の情報が表示されます。

「設定」テーブル



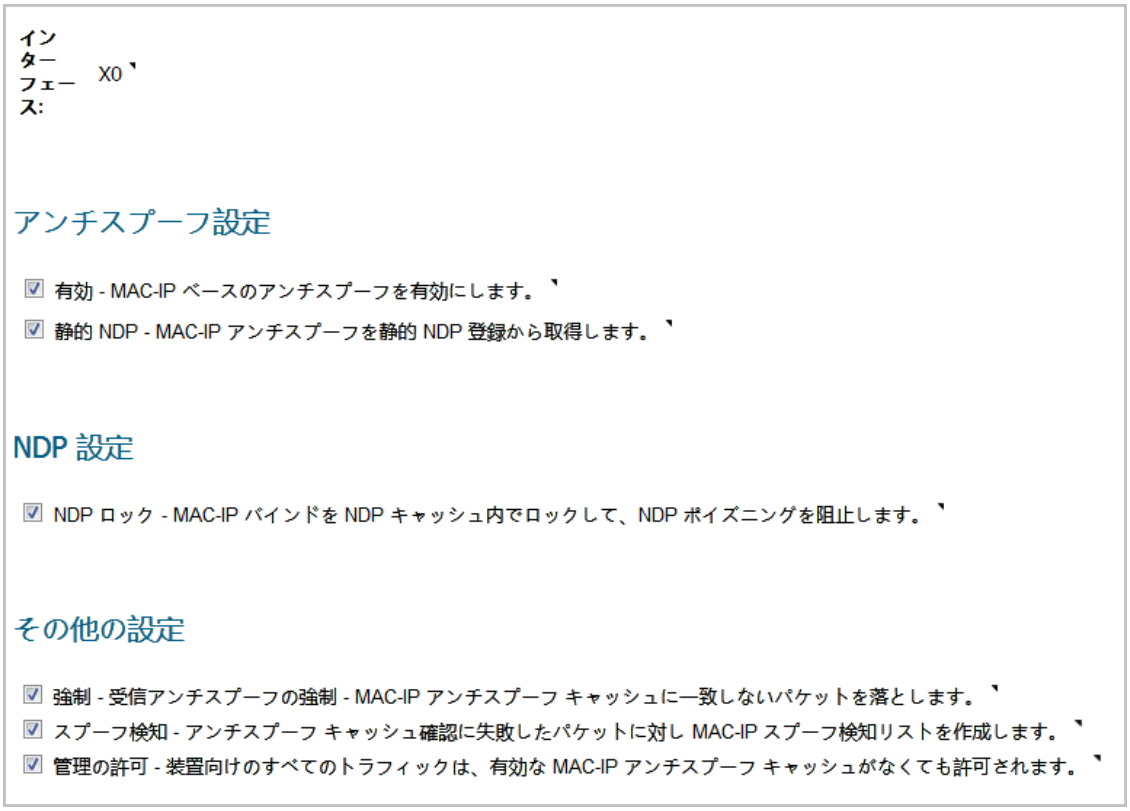
「アンチスプーフ キャッシュ」テーブル

IPv6 インターフェースの MAC-IP アンチスプーフ設定の編集

特定のインターフェースについてMAC-IP アンチスプーフの設定を行うには、以下の手順に従います。

1 「**ネットワーク > MAC-IP アンチスプーフ**」に移動します。

2 「**インターフェースに対する設定**」テーブルで、目的のインターフェースの**設定**アイコンを選択します。「**MAC-IP アンチスプーフ設定の編集**」ダイアログが表示されます。



3 このインターフェースを介したアンチスプーフに基づく MAC アドレスおよび IP アドレス トラフィックを有効にするには、「**アンチスプーフ設定**」セクションで「**有効 - MAC-IP ベースのアンチスプーフを有効にします**」を選択します。このオプションは、既定では選択されていません。

4 MAC-IP アンチスプーフ テーブルですべての静的 NDP エントリについて対応するエントリを作成するには、「**静的 NDP - MAC-IP アンチスプーフを静的 NDP 登録から取得します**」を選択します。このオプションは、既定では選択されていません。

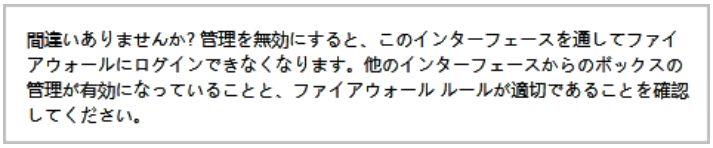
5 アンチスプーフ キャッシュ内のすべての MAC-IP バインドについて NDP キャッシュ エントリを追加するには、「**NDP 設定**」セクションで「**NDP ロック - MAC-IP バインドを NDP キャッシュ内でロックして、NDP ポイズニングを阻止します**」を選択します。このオプションは、既定では選択されていません。

6 すべてのトランジット パケットで MAC-IP アンチスプーフ チェックを有効にするには、「**その他の設定**」セクションで「**強制 - 受信アンチスプーフの強制 - MAC-IP アンチスプーフ キャッシュに一致しないパケットを落とします**」を選択します。このオプションは、既定では選択されていません。

7 MAC-IP アンチスプーフ キャッシュ チェックに失敗するすべてのデバイスについてスプーフ検知リストを作成するには、「**スプーフ検知 - アンチスプーフ キャッシュ確認に失敗したパケットに対し MAC-IP スプーフ検知リストを作成します**」を選択します。このオプションは、既定では選択されていません。

8 有効な MAC-IP アンチスプーフ キャッシュがないものも含めて、セキュリティ装置宛てのすべてのトラフィックを許可するには、「**管理の許可 - 装置向けのすべてのトラフィックは、有効な MAC-IP アンチスプーフ キャッシュがなくても許可されます**」を選択します。このオプションは、既定では選択されています。

注意：このオプションを無効にした場合、このインターフェースを介した SonicWall セキュリティ装置へのログインができなくなる可能性があります。セキュリティ装置の管理のためにその他のインターフェースが使用可能になっていること、適切なルールやポリシーが用意されていることを確認してください。このオプションを無効にした場合、次の警告メッセージが表示されます。



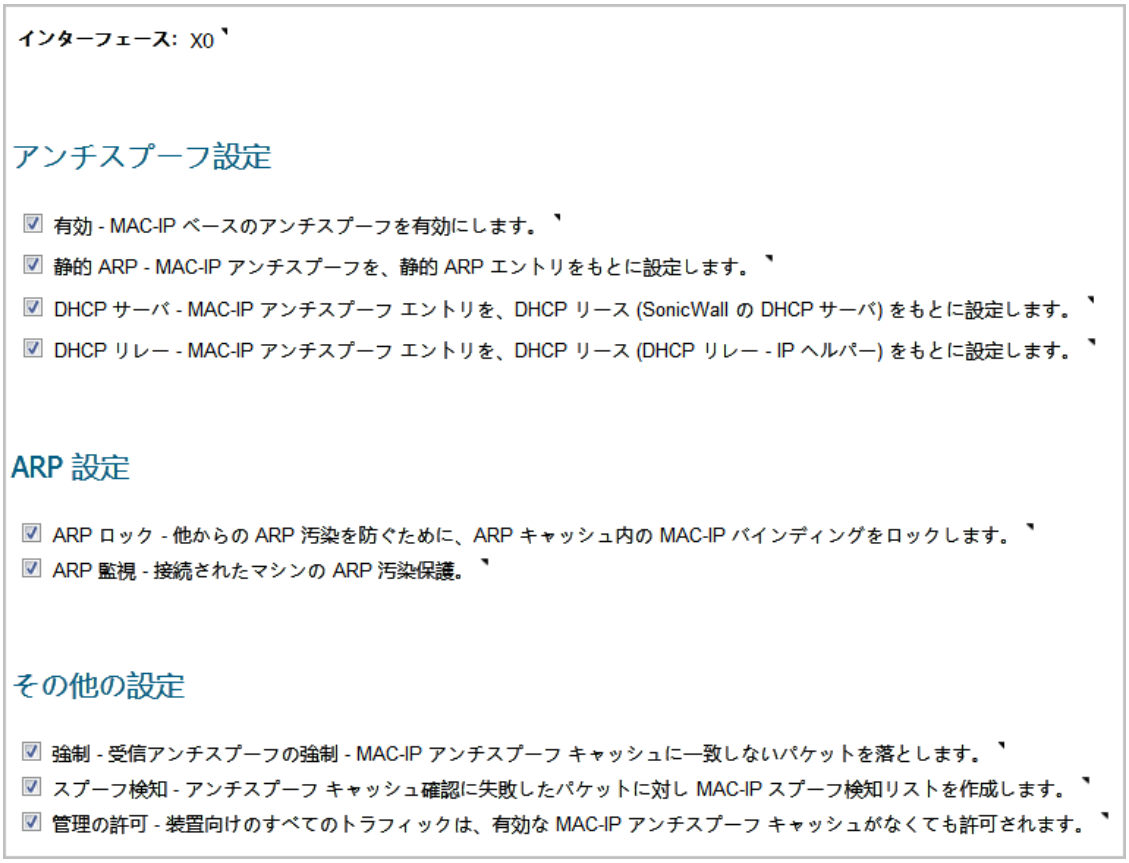
9 「**OK**」を選択します。

IPv4 インターフェースの MAC-IP アンチスプーフ設定の編集

特定のインターフェースについて MAC-IP アンチスプーフの設定を行うには、以下の手順に従います。

1 「**ネットワーク > MAC-IP アンチスプーフ**」に移動します。

2 「**インターフェースに対する設定**」テーブルで、目的のインターフェースの**設定**アイコンを選択します。「**MAC-IP アンチスプーフ設定の編集**」ダイアログが表示されます。



3 このインターフェースを介したアンチスプーフに基づく MAC アドレスおよび IP アドレス トラフィックを有効にするには、「**アンチスプーフ設定**」セクションで「**有効 - MAC-IP ベースのアンチスプーフを有効にします**」を選択します。このオプションは、既定では選択されていません。

4 MAC-IP アンチスプーフ テーブルですべての静的 ARP エントリについて対応するエントリを作成するには、「**静的 ARP - MAC-IP アンチスプーフを、静的 ARP エントリをもとに設定します**」を選択します。このオプションは、既定では選択されていません。

5 MAC-IP アンチスプーフ テーブルで DHCP サーバによって割り当てられているすべての DHCP リースについて対応するエントリを作成するには、「**DHCP サーバ - MAC-IP アンチスプーフ エントリを、DHCP リース (SonicWall の DHCP サーバ) をもとに設定します**」を選択します。このオプションは、既定では選択されていません。

6 DHCP リレー設定に基づいて MAC-IP アンチスプーフ テーブルでリモート DHCP サーバによって割り当てられているすべての DHCP リースについて対応するエントリを作成するには、「**DHCP リレー - MAC-IP アンチスプーフ エントリを、DHCP リース (DHCP リレー - IP ヘルパー) をもとに設定します**」を選択します。このオプションは、既定では選択されていません。

7 アンチスプーフ キャッシュ内のすべての MAC-IP バインドについて ARP キャッシュ エントリを追加するには、「**ARP 設定**」セクションで「**ARP ロック - 他からの ARP 汚染を防ぐために、ARP キャッシュ内の MAC-IP バインディングをロックします**」を選択します。このオプションは、既定では選択されていません。

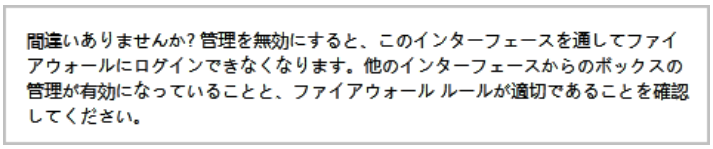
8 接続されている装置の ARP 汚染を防ぎ、すべてのクライアント PC を man-in-the-middle 攻撃から保護するには、「**ARP 監視 - 接続されたマシンの ARP 汚染保護**」を選択します。このオプションは、既定では選択されていません。

9 すべてのトランジット パケットで MAC-IP アンチスプーフ チェックを有効にするには、「**その他の設定**」セクションで「**強制 - 受信アンチスプーフの強制 - MAC-IP アンチスプーフ キャッシュに一致しないパケットを落とします**」を選択します。このオプションは、既定では選択されていません。

10 MAC-IP アンチスプーフ キャッシュ チェックに失敗するすべてのデバイスについてスプーフ検知リストを作成するには、「**スプーフ検知 - アンチスプーフ キャッシュ確認に失敗したパケットに対し MAC-IP スプーフ検知リストを作成します**」を選択します。このオプションは、既定では選択されていません。

11 有効な MAC-IP アンチスプーフ キャッシュがないものも含めて、セキュリティ装置宛てのすべてのトラフィックを許可するには、「**管理の許可 - 装置向けのすべてのトラフィックは、有効な MAC-IP アンチスプーフ キャッシュがなくても許可されます**」を選択します。このオプションは、既定では選択されています。

注意：このオプションを無効にした場合、このインターフェースを介した SonicWall セキュリティ装置へのログインができなくなる可能性があります。セキュリティ装置の管理のためにその他のインターフェースが使用可能になっていること、適切なルールやポリシーが用意されていることを確認してください。このオプションを無効にした場合、次の警告メッセージが表示されます。



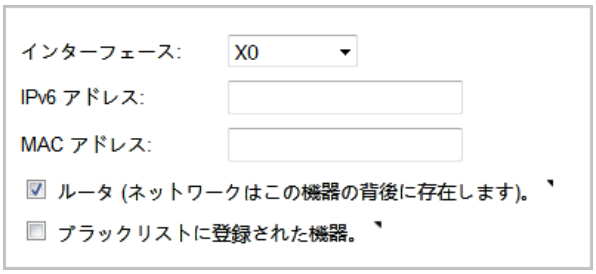
12 「**OK**」を選択します。

アンチスプーフ キャッシュへの機器の追加

アンチスプーフ キャッシュに機器を追加するには、以下の手順に従います。

1 「**ネットワーク > MAC-IP アンチスプーフ**」に移動します。

2 「**アンチスプーフ キャッシュ**」テーブルの下部にある「**追加**」を選択します。「**静的 MAC-IP アンチスプーフを追加する**」ダイアログが表示されます。



3 「**インターフェース**」で、機器からのトラフィックが到着するインターフェースを選択します。

4 「**IPv6 アドレス**」フィールドに、機器の IP アドレスを入力します。

5 「**MAC アドレス**」フィールドに、機器の MAC アドレスを入力します。

6 背後にネットワークがあるルータとして機器を指定するには、「**ルータ**」を選択します。このオプションは、既定では選択されています。

7 この機器をブラックリストに登録し、機器からのトラフィックを遮断するには、「**ブラックリストに登録された機器**」を選択します。このオプションは、既定では選択されていません。

機器をブラックリストに載せると、その IP アドレスに関係なく、その機器からのパケットが遮断されます。

8 「**OK**」を選択します。

アンチスプーフ キャッシュ エントリの削除

静的アンチスプーフ キャッシュ エントリを 1 つ削除するには、以下の手順に従います。

1 「**ネットワーク > MAC-IP アンチスプーフ**」に移動します。

2 そのエントリの**削除**アイコンを選択します。

1 つ以上の静的アンチスプーフ キャッシュ エントリを削除するには、以下の手順に従います。

1 「**ネットワーク > MAC-IP アンチスプーフ**」に移動します。

2 削除するエントリを選択します。「**削除**」が使用可能になります。

3 「**削除**」を選択します。

すべてのアンチスプーフ キャッシュ エントリを削除するには、以下の手順に従います。

1 「**ネットワーク > MAC-IP アンチスプーフ**」に移動します。

2 「アンチスプーフ キャッシュ」テーブルのヘッダーにあるチェックボックスをオンにします。「**削除**」が使用可能になります。

3 「**削除**」を選択します。

表示対象のフィルタ

フィルタ機能を使用すると、「**アンチスプーフ キャッシュ**」テーブルおよび「**スプーフ検知リスト**」テーブルで特定の機器のみを表示できます。

テーブル表示をフィルタするには、以下の手順に従います。

1 「**ネットワーク > MAC-IP アンチスプーフ**」に移動します。

2 フィルタ対象のテーブルの下にある「フィルタ」フィールドで、機器の IP アドレス、インターフェース、MAC アドレス、ホスト名、名前のいずれかを指定します。このフィールドへの入力では、「フィルタ演算子の構文オプション」テーブルに示されている各演算子の適切な構文を使用する必要があります。

フィルタ演算子の構文オプション

演算子	構文オプション
タイプを持つ値	• Ip=1.1.1.1 or ip=1.1.1.0/24 • Mac=00:01:02:03:04:05 • Iface=x1
文字列	• X1 • 00:01 • Tst-mc • 1.1.
AND	• Ip=1.1.1.1;iface=x1 • Ip=1.1.1.0/24;iface=x1;just-string
OR	• Ip=1.1.1.1,2.2.2.2,3.3.3.0/24 • Iface=x1,x2,x3
否定	• !ip=1.1.1.1;!just-string • !iface=x1,x2
混合	• Ip=1.1.1.1,2.2.2.2;mac=00:01:02:03:04:05; just-string;!iface=x1,x2

スプーフ検知リストからの静的エントリの追加

スプーフ検知リストから静的エントリを追加するには、以下の手順に従います。

1 「**ネットワーク > MAC-IP アンチスプーフ**」に移動します。

2 「**スプーフ検知リスト**」テーブルで、目的の機器の「**追加**」列にある**編集**アイコンを選択します。警告メッセージが表示され、この静的エントリを追加するかどうか確認を求められます。

3 「**OK**」を選択します。

26

DHCP サーバのセットアップ

トピック:

- ネットワーク > DHCP サーバ (555 ページ)
  - DHCP サーバ オプション機能 (557 ページ)
  - インターフェースごとの複数 DHCP スコープ (558 ページ)
  - DHCP サーバ恒久性について (560 ページ)
  - DHCP サーバの設定 (561 ページ)
  - DHCP サーバ リース範囲 (562 ページ)
  - 現在の DHCPリース (563 ページ)
  - DHCPv6 リレー (564 ページ)
- 詳細オプションの設定 (565 ページ)
  - 詳細オプションの設定 (565 ページ)
  - DHCP サーバの動的範囲の設定 (571 ページ)
  - 静的 DHCP 登録の設定 (577 ページ)
  - DHCP リース範囲の DHCP 汎用オプションの設定 (579 ページ)
  - RFC で定義された DHCP オプション番号 (580 ページ)
  - DHCP と IPv6 (587 ページ)

ネットワーク > DHCP サーバ

「**ネットワーク > DHCP サーバ**」の IPv6 バージョン (「IPv6 の「ネットワーク > DHCP サーバ」」) と IPv4 バージョン (「IPv4 の「ネットワーク > DHCP サーバ」」) の違いはわずかです。手順には相違点があります。

IPv6 の「ネットワーク > DHCP サーバ」

IPv4 の「ネットワーク > DHCP サーバ」

SonicWall セキュリティ装置には、IP アドレス、サブネット マスク、ゲートウェイ アドレス、および DNS サーバ アドレスをネットワーク クライアントに配布する DHCP (Dynamic Host Configuration Protocol) サーバが搭載されています。セキュリティ装置の DHCP サーバの設定は、「**ネットワーク > DHCP サーバ**」で行います。

重要：セキュリティ装置の DHCP サーバを使用することも、ネットワーク上の既存の DHCPサーバを使用することもできます。ネットワーク独自の DHCP サーバを使用する場合は、「**DHCP サーバを有効にする**」をオフにしてください。

ファイアウォールの DHCP サーバが割り当てることができるアドレス範囲と IP アドレスの数は、ファイアウォールのモデル、オペレーティング システム、およびセキュリティ装置のライセンスによって異なります。「最大 DHCP リース数」テーブルに SonicWall セキュリティ装置の最大許容 DHCP リース数を示します。

最大 DHCP リース数

プラットフォーム	最大 DHCP リース数	プラットフォーム	最大 DHCP リース数	プラットフォーム	最大 DHCP リース数
SM 9600	16384	NSA 6650	16384	TZ600	4096
SM 9400	16384	NSA 6600	16384	TZ500/TZ500 W	4096
SM 9200	16384	NSA 5650	8192	TZ400/TZ400 W	4096
		NSA 5600	8192	TX350/TZ350 W	4096
		NSA 4650	8192	TZ300/TZ300 W	4096
		NSA 4600	8192		
		NSA 3650	4096	SOHO 250/SOHO 250 W	4096
		NSA 3600	4096	SOHO W	4096
		NSA 2650	4096		
		NSA 2600	4096		

トピック:

- DHCP サーバ オプション機能 (557 ページ)
- インターフェースごとの複数 DHCP スコープ (558 ページ)
- DHCP サーバ恒久性について (560 ページ)
- DHCP サーバの設定 (561 ページ)
- DHCP サーバ リース範囲 (562 ページ)
- 現在の DHCPリース (563 ページ)
- 詳細オプションの設定 (565 ページ)
- DHCP サーバの動的範囲の設定 (571 ページ)
- 静的 DHCP 登録の設定 (577 ページ)
- DHCP リース範囲の DHCP 汎用オプションの設定 (579 ページ)
- RFC で定義された DHCP オプション番号 (580 ページ)
- DHCP と IPv6 (587 ページ)

DHCP サーバ オプション機能

SonicWall DHCP サーバ オプション機能は、ベンダー拡張とも呼ばれる DHCP オプションのサポートを提供します。これらのオプションは、主に RFC 2131 および RFC 2132 で定義されている機能です。DHCP オプションを使用すると、あらかじめ定義されたベンダー固有の情報を追加的なDHCP パラメータとして指定することができ、指定した情報は DHCP メッセージのオプション フィールドに格納されます。そのため、DHCP メッセージの送信により、ネットワーク上のクライアントに対してベンダー

固有の設定情報およびサービス情報を提供することができます。各 DHCP オプションの説明は、セクション「RFC で定義された DHCP オプション番号 (580 ページ)」の一覧表 (RFC で割り当てられたオプション番号順) にまとめてあります。

トピック:

- メリット (558 ページ)
- DHCP サーバ オプション機能の仕組み (558 ページ)
- サポートされている標準 (558 ページ)

メリット

SonicWall DHCP サーバ オプション機能では、DHCP オプションを番号または名前で選択できるわかりやすいインターフェースが用意されているため、RFC で定義されている DHCP 標準に準拠した形で DHCP オプションを手早く簡単に設定することができます。

DHCP サーバ オプション機能の仕組み

SonicWall DHCP サーバ オプション機能では、RFC 定義のオプション番号に基づくドロップダウン メニューを使用して DHCP オプションを指定できるため、管理者は DHCP オブジェクトや DHCP オブジェクト グループを簡単に作成できるだけでなく、動的および静的な DHCP リース範囲に関する DHCP 汎用オプションも容易に設定できます。設定後の DHCP オプションは DHCP メッセージのオプション フィールドに格納されてネットワーク上の DHCP クライアントに渡され、クライアントはネットワークの設定や利用可能なサービスに関する情報を取得することができます。

サポートされている標準

SonicWall DHCP サーバ オプション機能では、次の標準がサポートされています。

- RFC 2131 - Dynamic Host Configuration Protocol
- RFC 2132 - DHCP Options and BOOTP Vendor Extensions

インターフェースごとの複数 DHCP スコープ

トピック:

- インターフェースごとの複数 DHCP スコープとは (558 ページ)
- 複数の DHCP スコープの利点 (559 ページ)
- インターフェースごとの複数 DHCP スコープの仕組み (559 ページ)

インターフェースごとの複数 DHCP スコープとは

通常、DHCP サーバとクライアントは同じ IP ネットワークまたはサブネット上に存在しますが、DHCP クライアントとそれに関連付けられている DHCP サーバが同じサブネットに存在しない場合もあります。インターフェースごとの複数 DHCP スコープの機能を使用すると、1 台の DHCP サーバで複数のサブネットに存在するクライアントに対する異なるスコープを管理できます。

複数の DHCP スコープの利点

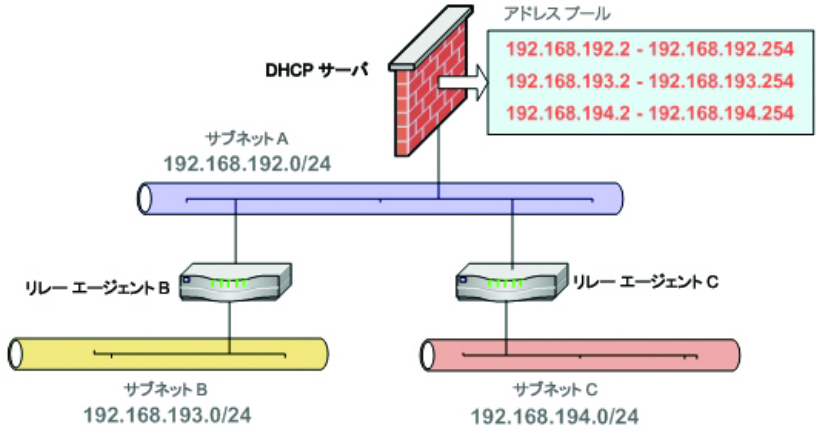
効率的	1 台の DHCP サーバで、複数のサブネットに存在するクライアントに IP アドレスを提供できます。
VPN を越えた DHCP との互換性	リレーされる DHCP メッセージの処理は、メッセージの送信元が VPN トンネルか DHCP リレー エージェントかに関係なく、同じように扱われます。
サイト間 VPN に対する複数のスコープ	内部 DHCP サーバを使うときは、LAN/DMZ サブネットとは異なるスコープ範囲を使用して、リモート サブネットを設定できます。リモート サブネットのスコープ範囲は、リモート ゲートウェイで設定される「リレー IP アドレス」によって決まります。
グループ VPN に対する複数のスコープ	内部 DHCP サーバを使うときは、LAN/DMZ サブネットとは異なるスコープ範囲を使用して、SonicWall GVC クライアントを設定できます。GVC クライアントのスコープ範囲は、セントラル ゲートウェイで設定される「リレー IP アドレス (オプション)」オプションによって決まります。
競合検出との互換性	現在、DHCP サーバは、この機能が有効な場合にサーバ側の競合検出を実施します。サーバが輪の競合検出の優位点は、DHCP クライアントがクライアント側の競合検出を実行しない場合でも競合を検出することにあります。しかしながら、ネットワーク上に多数の DHCP クライアントがある場合は、サーバ側の競合検出では、完全な IP アドレス割り当てを完了するために、より長い待ち時間を要することがあります。競合検出 (およびネットワーク事前検出) は、"リレーされる"サブネット スコープに属する IP アドレスに対しては実行されません。DHCP サーバはインターフェースに結びついているサブネット範囲に対してのみ、競合検出の ICMP 確認を実行します。

インターフェースごとの複数 DHCP スコープの仕組み

通常、DHCP クライアントは、ブロードキャスト DHCP 検出メッセージを送信することで、アドレスの割り当てを開始します。ほとんどのルートはブロードキャスト パケットを転送しないので、この方法では、DHCP クライアントとサーバが同じ IP ネットワークまたはサブネット上に存在している必要があります。

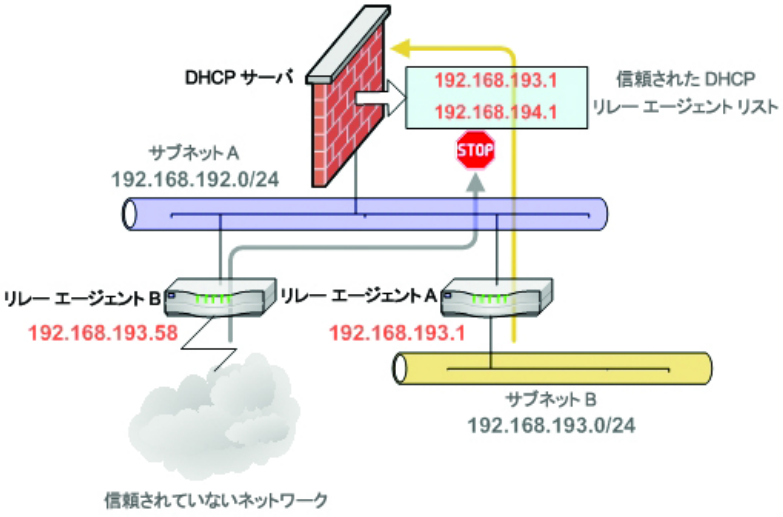
DHCP クライアントとそれに関連付けられた DHCP サーバが同じサブネット上に存在しない場合、クライアントとサーバの間で DHCP メッセージを転送するために、ある種のサードパーティ エージェント (BOOTP リレー エージェント、IP ヘルパーなど) が必要です。「1 つの DHCP サーバを共有する複数のサブネット」を参照してください。DHCP リレー エージェントは、その受信インターフェースの IP アドレスを giaddr フィールドに設定した後、設定されている DHCP サーバに転送します。DHCP サーバはメッセージを受信すると、giaddr フィールドを調べて、クライアントにIP アドレスのリースを提供するために使用できる DHCP スコープかどうかを判断します。

1 つの DHCP サーバを共有する複数のサブネット



インターフェースごとの複数 DHCP スコープの機能は、DHCP サーバへのアクセスを広く許可するとどうしても発生する可能性のある脆弱性を保護するための、セキュリティの拡張を提供します。「**DHCP の詳細設定**」ダイアログには、信頼できる DHCP リレー エージェントを指定するための、信頼できるエージェントに関するタブが用意されています。「信頼できる DHCP リレー エージェント」を参照してください。DHCP サーバは、リストにないエージェントによってリレーされたメッセージをすべて破棄します。

信頼できる DHCP リレー エージェント



DHCP サーバ恒久性について

DHCP サーバの恒久性は、DHCP リースの情報をセキュリティ装置に保存することにより、クライアントが再起動された場合でも、ネットワーク上の他の用途と競合するおそれのない予測可能な IP アドレスをクライアントに提供できるようにする機能です。

DHCP サーバの恒久性は、DHCP リースの情報を定期的にフラッシュ メモリに保存することによって実現されます。これにより、予測可能な IP アドレスを各ユーザに確実に割り当てることが可能となり、再起動後に IP アドレスが競合する危険を最小限に抑えられます。

DHCP サーバの恒久性は、ユーザがワークステーションを再起動しても変化しない安定した使用環境を実現します。DHCP リースの情報が保存されているため、ワークステーションの再起動後も同じ IP アドレスが保持されます。DHCP サーバの恒久性は、保守やアップグレードの作業に伴ってファイアウォールが再起動される場合にも、次の点で有益です。

- IP アドレスの一意性: リース情報はフラッシュ メモリに保存されているので、複数のユーザに同じ IP アドレスが割り当てられる危険はまったくありません。
- 使いやすさ: ユーザの接続は、フラッシュ メモリに保存されているリース情報を使用して、自動的に復元されます。

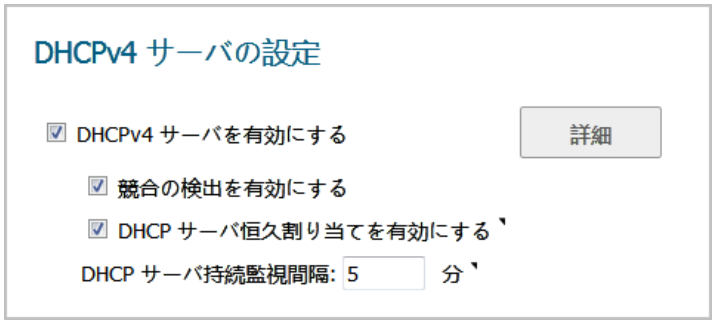
DHCP サーバの設定

SonicWall セキュリティ装置の DHCP サーバを使用するには:

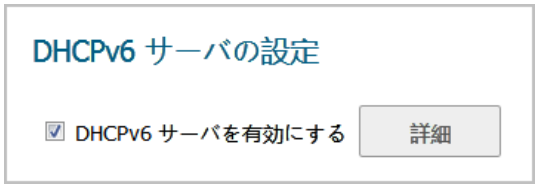
1 「**管理 | システム セットアップ | ネットワーク > DHCP サーバ**」に移動します。

2 「**表示する IP バージョン**」で使用する IP バージョンを選択します。

- **IPv4**



- **IPv6**



3 IP アドレス、サブネット マスク、ゲートウェイ アドレス、および DNS サーバ アドレスをネットワーク クライアントに配布するために、「**DHCPv4/6 サーバを有効にする**」を選択します。このオプションは、既定では選択されています。「**詳細**」が有効になり、IPv4 の場合はサーバ設定オプションが使用可能になります。

4 DHCPv6 を設定する場合は、「ステップ 7」へ進みます。

5 別の DHCP サーバが存在する場合に各ゾーンで自動 DHCP スコープ競合検出を有効にするには、「**競合の検出を有効にする**」を選択します。このオプションは、既定では選択されています。

現在、DHCP サーバは、この機能が有効な場合にサーバ側の競合検出を実施します。サーバが輪の競合検出の優位点は、DHCP クライアントがクライアント側の競合検出を実行しない場合でも競合を検出することにあります。しかしながら、ネットワーク上に多数の DHCP クライアントがある場合は、サーバ側の競合検出では、完全な IP アドレス割り当てを完了するために、より長い待ち時間を要することがあります。

メモ：競合検出は、"リレーされる" サブネット スコープに属する IP アドレスに対しては実行されません。DHCP サーバはインターフェースに結びついているサブネット範囲に対してのみ、競合検出の ICMP 確認を実行します。

6 ネットワーク内の DHCP リースの現在の状況が定期的にフラッシュに書き込まれるようにするには、「**DHCP サーバ恒久割り当てを有効にする**」を選択します。再起動時に、システムはフラッシュに保存された IP リース回数に基づいて、以前の DHCP サーバ ネットワークの DHCP 割り当て情報を復元します。このオプションは、既定では選択されています。このオプションを選択すると、「**DHCP サーバ持続監視間隔**」オプションが使用可能になります。

- ネットワークの変化を調査し、必要に応じてフラッシュに書き込む頻度を制御するには、「**DHCP サーバ持続監視間隔**」に時間間隔を分単位で入力します。既定値は **5** 分、最小値は 5 分、最大値は 1440 分 (24 時間) です。

7 **オプション オブジェクト**、**オプション グループ**、および**信頼されたエージェント**を設定するには、「**詳細**」を選択します。これらの機能を設定するための詳細な情報については、「詳細オプションの設定 (565 ページ)」を参照してください。

8 「**適用**」を選択します。

トピック:

- DNS プロキシのための DHCP サーバの設定 (562 ページ)
- 現在の DHCPv4 リース (564 ページ)

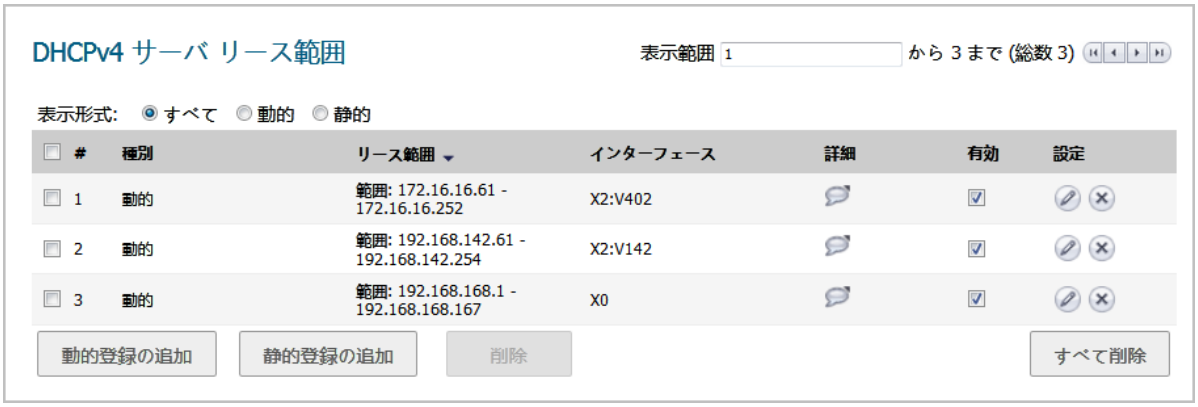
DNS プロキシのための DHCP サーバの設定

インターフェースで DNS プロキシが有効になっている場合、機器はインターフェース IP を DNS サーバ アドレスとしてクライアントにプッシュする必要があるので、DHCP サーバを手動で設定し、「**DNS/WINS**」タブの DHCP サーバの設定でインターフェース アドレスを「**DNS サーバ 1**」のアドレスとして使用する必要があります。DHCP ページの「**インターフェースの事前設定**」チェックボックスを使用すると、この設定を簡単に行うことができます。選択したインターフェースで DNS プロキシが有効になっている場合、「**DNS/WINS**」ページに DNS サーバの IP が自動的に追加されます。

DHCP サーバ リース範囲

DHCPv6 サーバ リース スコープ

DHCPv4 サーバ リース範囲



「**DHCP サーバ リース範囲**」テーブルには、現在設定されている DHCP の IP 範囲が表示されます。

種別	**動的**または**静的**。
接頭辞	IPv6 のみ。
リース範囲	IP アドレスの範囲 (例えば、`172.16.31.2-172.16.31.254`)。
インターフェース	IPv4 のみ。そのアドレス範囲が割り当てられるインターフェース。
詳細	**コメント** アイコンの上にマウス ポインタを置くと、リースに関する詳細情報がツール チップとして表示されます。
有効	DHCP 範囲を有効にするには、このチェックボックスをオンにします。範囲を無効にする場合は、チェックボックスをオフにします。
設定	テーブルの項目に対する**設定**アイコンと**削除**アイコンがあります。

現在の DHCPリース

トピック:

- 現在の DHCPv6 リース (563 ページ)
- 現在の DHCPv4 リース (564 ページ)

現在の DHCPv6 リース

「**現在の DHCP リース**」テーブルには、現在の DHCP リース情報が表示されます。各バインド エントリに表示される情報は以下のとおりです。

- **IPv6 アドレス**
- **リース期間**

- **IAID**
- **DUID**
- **種別 (動的、動的 BOOTP、または静的 BOOTP)**
- **削除**

バインドを削除して DHCP サーバで IP アドレスを解放するには:

1 エントリの横にある**削除**アイコンを選択します。例えば、ネットワークからホストが削除されていて、その IP アドレスを再利用する必要がある場合は、**削除**アイコンを使用します。

2 「**適用**」を選択します。

現在の DHCPv4 リース

「**現在の DHCP リース**」テーブルには、現在の DHCP リース情報が表示されます。各バインド エントリに表示される情報は以下のとおりです。

- **IP アドレス**
- **ホスト名**
- **リース期間**
- **MAC アドレス**
- **ベンダー**
- **種別 (動的、動的 BOOTP、または静的 BOOTP)**
- **削除**

バインドを削除して DHCP サーバで IP アドレスを解放するには:

1 エントリの横にある**削除**アイコンを選択します。例えば、ネットワークからホストが削除されていて、その IP アドレスを再利用する必要がある場合は、**削除**アイコンを使用します。

2 「**適用**」を選択します。

DHCPv6 リレー

SonicOS では、DHCPv6 リレーがサポートされます。SonicOS の DHCPv6 リレーについては、「DHCPv6 リレー (590 ページ)」を参照してください。

詳細オプションの設定

メモ：DHCP サーバのオプションの設定は、IPv4 と IPv6 のどちらでもほぼ同じです。相違点については、手順の中で示します。

トピック:

- DHCP オプション オブジェクトの設定 (565 ページ)
- DHCP オプション グループの設定 (567 ページ)
- 信頼された DHCP リレー エージェント アドレス グループの設定 (IPv4 のみ) (570 ページ)
- 信頼された DHCP リレー エージェントの有効化 (570 ページ)

各 DHCP オプションの説明は、「RFC で定義された DHCP オプション番号 (580 ページ)」の一覧表 (RFC で割り当てられたオプション番号順) にまとめてあります。

DHCP オプション オブジェクトの設定

DHCP オプション オブジェクトを設定するには、以下の手順に従います。

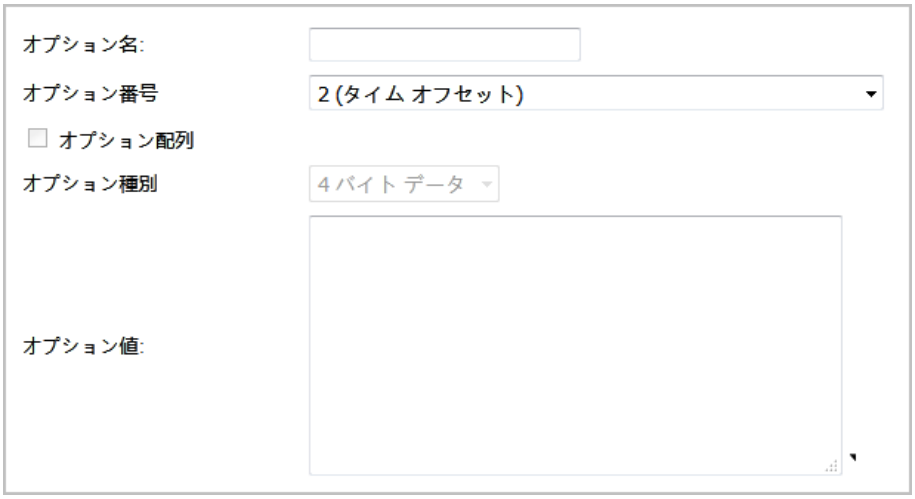
1 「**管理 | システム セットアップ | ネットワーク > DHCP サーバ**」に移動します。

2 「**DHCPv4/6 サーバの設定**」で、「**詳細**」を選択します。「**DHCP 詳細設定**」ダイアログが表示されます。IPv4 と IPv6 のダイアログはわずかに異なります。「IPv6 の「DHCP 詳細設定」」と「IPv4 の「DHCP 詳細設定」」を参照してください。

IPv6 の「DHCP 詳細設定」

IPv4 の「DHCP 詳細設定」

3 「**オプションの追加**」を選択します。「**DHCP オプション オブジェクトの追加**」ダイアログが表示されます。



4 「**オプション名**」フィールドにオプションの名前を入力します。

5 「**オプション番号**」で、目的の DHCP オプションに対応するオプション番号を選択します。オプションの番号、名前、および説明の一覧については、「RFC で定義された DHCP オプション番号 (580 ページ)」を参照してください。

メモ：利用可能なオプションは、IPv4 または IPv6 のどちらのオプションを設定しているかによって異なります。

6 次の場合：

- 「**オプション番号**」で「**2 (タイム オフセット)**」を選択したときなど、該当するオプション種別が 1 つしかない場合は、「**オプション配列**」は淡色表示されます。「ステップ 7」へ進みます。
- 例えば、「**77 (ユーザ クラス情報)**」では、「**オプション種別**」が使用可能になり、このオプションで使用できるタイプとして「**IP アドレス**」、「**2 バイト データ**」、「**文字列**」、「**論理型**」などがリストされます。オプション種別を選択します。

7 オプションの値 (例えば、IP アドレスなど) を「**オプション値**」フィールドに入力します。「**オプション配列**」チェックボックスがオンの場合は、複数の値をセミコロン (;) で区切って入力することができます。

8 「**OK**」を選択します。設定したオブジェクトが「**オプション オブジェクト**」テーブルに表示されます (「DHCPv6 の「オプション オブジェクト」テーブル」と「DHCPv4 の「オプション オブジェクト」テーブル」を参照)。

DHCPv6 の「オプション オブジェクト」テーブル

DHCPv4 の「オプション オブジェクト」テーブル

DHCP オプション グループの設定

DHCP オプション グループを設定するには、以下の手順に従います。

1 「**管理 | システム セットアップ | ネットワーク > DHCP サーバ**」に移動します。

2 「**DHCPv4/6 サーバの設定**」で、「**詳細**」を選択します。「**DHCP 詳細設定**」ダイアログが表示されます。

> **メモ**：利用可能なオプションは、IPv4 オプションまたは IPv6 オプションのどちらを設定するかによって異なります (「IPv6 の「DHCP 詳細設定」」または「IPv4 の「DHCP 詳細設定」」を参照)。

IPv6 の「DHCP 詳細設定」

IPv4 の「DHCP 詳細設定」

3 「**オプション グループ**」を選択します。

4 「**グループの追加**」をクリックします。「**DHCPv6 オプション グループの追加**」ダイアログが表示されます。

5 グループの名前を「**名前**」フィールドに入力します。

6 グループに追加するオプション オブジェクトを左の列から選択して、**右矢印**を選択します。同時に複数のオプション オブジェクトを選択するには、**Ctrl** キーを押しながらオプション オブジェクトを選択します。

7 「**OK**」を選択します。設定したグループが「**オプション グループ**」テーブルに表示されます。

DHCPv6 の「オプション グループ」テーブル

DHCPv4 の「オプション グループ」テーブル

信頼された DHCP リレー エージェント アドレス グループの設定 (IPv4 のみ)

「**既定の信頼されたリレー エージェント リスト**」アドレス グループを設定するには、最初に信頼できる各リレー エージェントに対してアドレス オブジェクトを設定した後、これらのアドレス オブジェクトを「**既定の信頼されたリレー エージェント リスト**」アドレス グループまたはカスタム アドレス グループに追加します。

アドレス オブジェクトとアドレス グループは「**管理 | ポリシー | オブジェクト > アドレス オブジェクト**」で設定します。アドレス オブジェクトとアドレス グループを設定する方法については、『*SonicOS 6.5 ポリシー*』を参照してください。

信頼された DHCP リレー エージェントの有効化

「**DHCP 詳細設定**」ダイアログでは、「**既定の信頼されたリレー エージェント リスト**」アドレス グループを使用して「**信頼されたリレー エージェント リスト**」オプションを有効にするか、または既存のアドレス オブジェクトを使用して別のアドレス グループを作成できます。

メモ：サーバが VPN セントラル ゲートウェイを越えた DHCP で内部 DHCP サーバとして割り当てられている場合、VPN トンネルからの DHCP メッセージは常にバイパスされます。

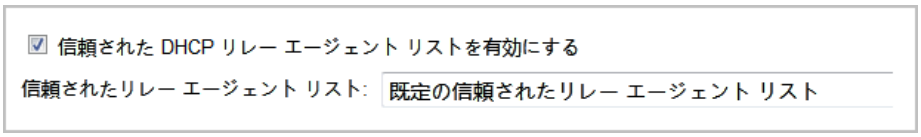
「信頼されたリレー エージェント リスト」オプションを有効にして目的のアドレス グループを選択するには、次の手順を実行します。

1 「**管理 | システム セットアップ | ネットワーク > DHCP サーバ**」に移動します。

2 「**DHCPv4 の設定**」で、「**詳細**」を選択します。「**DHCP 詳細設定**」ダイアログが表示されます。

3 「**信頼されたエージェント**」を選択します。

4 「**信頼された DHCP リレー エージェント リストを有効にする**」を選択します。このオプションは、既定では選択されていません。「**信頼されたリレー エージェント リスト**」が使用できるようになります。



5 「**既定の信頼されたリレー エージェント リスト**」からアドレス グループを選択します。このオプションには、既存のすべてのアドレス グループと共に、「**新しいアドレス オブジェクト グループを作成する**」オプションが含まれます。

> **メモ**：このオプションのカスタム アドレス グループを作成するには、「**新しいアドレス オブジェクト グループを作成する**」を選択します。「**アドレス オブジェクト グループの追加**」ダイアログが表示されます。アドレス グループを設定する方法については、『*SonicOS ポリシー*』を参照してください。

6 「**OK**」を選択し、選択したアドレス グループで「**信頼されたリレー エージェント リスト**」オプションを有効にします。

DHCP サーバの動的範囲の設定

SonicOS ではインターフェースごとに複数の DHCP スコープを設定できるので、DHCP スコープを設定するときにサブネット範囲がインターフェースに接続されている必要はありません。

DHCP サーバの動的 IP アドレス範囲を設定するには、次の手順に従います。

1 「**管理 | システム セットアップ | ネットワーク > DHCP サーバ**」に移動します。

2 「**DHCPv4/6 サーバ リース範囲/スコープ**」テーブルの下にある「**動的登録の追加**」を選択します。対象が

- IPv6 の場合、「**DHCPv6 動的スコープの追加**」ダイアログが表示されます。「DHCPv6 動的スコープの追加 (572 ページ)」に移動します。
- IPv4 の場合、「**動的範囲の設定**」ダイアログが表示されます。「動的範囲の設定 (574 ページ)」に移動します。

DHCPv6 動的スコープの追加

動的スコープを追加するには:

1 この範囲を有効にするには、「**この DHCPv6 スコープを有効にする**」を選択します。このオプションは、既定では選択されています。

2 「**名前**」フィールドに範囲の名前を入力します。

3 「**接頭辞**」フィールドに、この範囲で IPv6 アドレスの配布に使用する接頭辞を入力します。

4 「**開始アドレス**」フィールドと「**終了アドレス**」フィールドに、範囲の開始アドレスと終了アドレスを入力します。両方のアドレスが接頭辞の範囲内である必要があります。

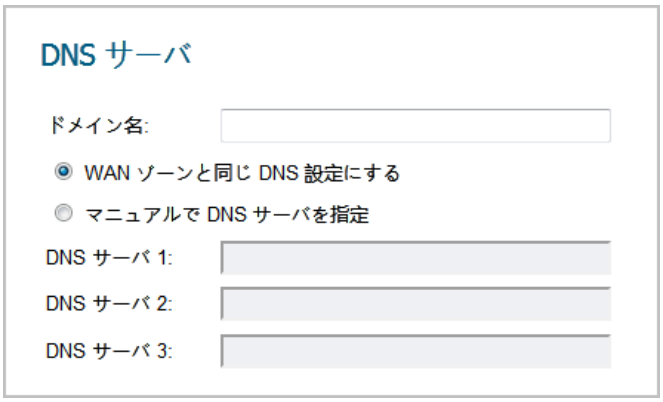
5 「**有効存続期間 (分)**」フィールドに、範囲によってリースされる IPv6 アドレスの有効存続期間を分単位で入力します。最小値は 0、最大値は 71582789、既定値は **2160** です。

6 「**優先存続期間 (分)**」フィールドに、範囲によってリースされる IPv6 アドレスの優先存続期間を分単位で入力します。最小値は 0、最大値は 71582789、既定値は **1440** です。

7 必要に応じて、「**コメント**」フィールドにコメントを入力します。

8 「**DNS**」を選択します。

DNS



DNS サーバを追加するには:

1 「**ドメイン名**」フィールドにドメイン名を入力します。

2 次のどちらかを行います。

- 「**WAN ゾーンと同じ DNS 設定にする**」を選択し、「ステップ 4」へ進みます。
- 「**マニュアルで DNS サーバを指定**」を選択します。「**DNS サーバ 1/2/3**」フィールドが使用可能になります。

3 「**DNS サーバ 1/2/3**」フィールドに、それぞれの DNS サーバの IP アドレスを入力します。

4 「**詳細設定**」を選択します。

詳細

一般的な DHCP オプションを設定するには:

1 「**DHCPv6 汎用オプション**」で、DHCP オプション オブジェクトまたはグループを選択します。既定は「**なし**」です。新しい DHCPv6 オプションまたはグループを設定するには、「DHCP オプション オブジェクトの設定 (565 ページ)」および「DHCP オプション グループの設定 (567 ページ)」を参照してください。

2 DHCPv6 クライアントからのメッセージに含まれるオプション要求オプションに関係なく、この範囲に設定されているすべての DHCPv6 オプションを送信するには、「**DHCPv6 オプションを常に送信する**」を選択します。このオプションは、既定では選択されていません。

3 「**OK**」を選択します。

動的範囲の設定

動的範囲を設定するには:

1 この範囲を有効にするには、「**この DHCP 範囲を有効にする**」を選択します。このオプションは、既定では選択されています。

2 「**開始アドレス**」、「**終了アドレス**」、「**デフォルト ゲートウェイ**」、および「**サブネット マスク**」フィールドを設定するには:

a 特定のインターフェースで既定値を使用するには:

1) ダイアログの下の方にある「**インターフェースの事前設定**」を選択します。選択されているオプションが使用可能になります。このオプションは、既定では選択されていません。

2) インターフェースを選択します。設定される IP アドレスは、選択したインターフェースと同じプライベート サブネットの IP アドレスです。

重要:「**インターフェースの事前設定**」からインターフェースを選択するには、対象のインターフェースをあらかじめ完全に設定しておく必要があります。
- ゾーン タイプの LAN、WLAN、または DMZ。
- VLAN サブインターフェース。

3) 「ステップ 3」へ進みます。

b 手動:

1) 自分の固有の IP アドレス範囲を入力します。

2) 「**リース期間 (分)**」フィールドに、別の IP アドレスが発行されるまで範囲によって IP アドレスがリースされる時間を分単位で入力します。最小値は 0、最大値は 71582789、既定値は **1440** (24 時間) です。

3) ゲートウェイの IP アドレスを「**デフォルト ゲートウェイ**」フィールドに入力します。

4) ゲートウェイのサブネット マスクを「**サブネット マスク**」フィールドに入力します。

3 必要に応じて、「**コメント**」フィールドにコメントを入力します。

4 ネットワークに BOOTP クライアントがある場合、「**BootP クライアントによる DHCP アドレス範囲の利用を許可する**」を選択します。このオプションは、既定では選択されていません。

BOOTP は Bootstrap Protocol の略であり、ディスクを持たないワークステーションが自分の IP アドレス、他の TCP/IP 設定情報、起動イメージ ファイルを BOOTP サーバから取得することを実現する TCP/IP プロトコルおよびサービスです。

5 「**DNS/WINS**」を選択して、DHCP サーバ機能の設定を続けます。

DNS/WINS

DNS/WINS サーバを設定するには:

1 DNS サーバのドメイン名がある場合は、「**ドメイン名**」フィールドに入力します。

2 次のどちらかを行います。

- 「**WAN ゾーンと同じ DNS 設定にする**」を選択し、「ステップ 4」へ進みます。
- 「**マニュアルで DNS サーバを指定**」を選択します。「**DNS サーバ 1/2/3**」フィールドが使用可能になります。

3 「**DNS サーバ 1/2/3**」フィールドに、それぞれの DNS サーバの IP アドレスを入力します。

4 ネットワーク上で WINS が実行されている場合は、「**WINS サーバ 1**」フィールドに WINS サーバの IP アドレスを入力します。さらに別の WINS サーバも追加できます。

5 「**詳細設定**」を選択します。「**詳細**」オプションでは、Cisco コール マネージャ情報をネットワーク上の VoIP クライアントに送信するように、DHCP サーバを設定できます。

詳細

詳細設定を設定するには:

1 「**VoIP コール マネージャ**」で、「**コール マネージャ 1**」フィールドに VoIP コール マネージャの IP アドレスまたは FDQN を入力します。さらに 2 つの VoIP コール マネージャ アドレスを追加できます。

2 「**ネットワーク起動設定**」で、「**次のサーバ**」フィールドに、起動プロセスの次のステージの間に PXEクライアントが使用する PXE 起動サーバ (TFTP サーバ) の IP アドレスを入力します。

> ⓘ **重要**：「**ネットワーク起動設定**」の下のフィールドは Pre-boot Execution Environment (PXE) で使われるものであり、クライアントはネットワーク インターフェースから取得したファイルを使用して起動します。PXE クライアントは、PXE 起動サーバの IP アドレスと名前および起動ファイル名を、DHCPサーバから取得します。
>
> これらのオプションを使用するときは、「**DHCP 汎用オプション**」の「**PXE**」を選択します。

3 「**起動ファイル**」フィールドに、PXE クライアントが PXE 起動サーバから TFTP 経由で取得できる起動ファイルの名前を入力します。

4 「**サーバ名**」フィールドに、PXE 起動サーバ (TFTP サーバ) の DNS ホスト名を入力します。

5 DHCP 汎用オプションの設定の詳細については、「DHCP リース範囲の DHCP 汎用オプションの設定 (579 ページ)」を参照してください。

6 「**OK**」を選択します。

7 「**適用**」を選択してファイアウォールに設定を適用します。

SonicWall セキュリティ装置の VoIP サポート機能の詳細については、「VoIP について (792 ページ)」を参照してください。

静的 DHCP 登録の設定

静的登録は、永続的な IP 設定を要求するサーバに割り当てられる IP アドレスです。SonicOS ではインターフェースごとに複数の DHCP スコープを設定できるので、DHCP スコープを設定するときにサブネット範囲がインターフェースに接続されている必要はありません。

静的エントリ (登録) を設定するには、以下の手順に従います。

1 「**管理 | システム セットアップ | ネットワーク > DHCP サーバ**」に移動します。

2 「**DHCPv4/6 サーバ リース範囲/スコープ**」テーブルの下にある「**静的登録の追加**」を選択します。対象が

- IPv6 の場合、「**DHCPv6 静的スコープの追加**」ダイアログが表示されます。「DHCPv6 静的スコープの追加 (577 ページ)」に移動します。
- IPv4 の場合、「**静的登録の設定**」ダイアログが表示されます。「静的登録の設定 (578 ページ)」に移動します。

DHCPv6 静的スコープの追加

1 この範囲を有効にするには、「**この DHCPv6 スコープを有効にする**」を選択します。このオプションは、既定では選択されています。

2 「**登録名**」フィールドに、静的 DHCPv6 登録の名前を入力します。

3 「**接頭辞**」フィールドに、この範囲で IPv6 アドレスの配布に使用する接頭辞を入力します。

4 「**静的 IPv6 アドレス**」フィールドに IPv6 アドレスを入力します。このアドレスは接頭辞の範囲内である必要があります。

5 「**IAID**」フィールドに、IAID (Interface Association Identifier) を 10 進形式で入力します。最大長は 10 桁、最大値は 4294967295 です。

6 「**DUID**」フィールドに、DUID (Device Unique Identifier) を入力します。最大長は 128 文字です。

7 「**有効存続期間 (分)**」フィールドに、範囲によってリースされる IPv6 アドレスの有効存続期間を分単位で入力します。最小値は 0、最大値は 71582789、既定値は **2160** です。

8 「**優先存続期間 (分)**」フィールドに、範囲によってリースされる IPv6 アドレスの優先存続期間を分単位で入力します。最小値は 0、最大値は 71582789、既定値は **1440** です。

9 必要に応じて、「**コメント**」フィールドにコメントを入力します。

10 DNS 設定と詳細設定の設定方法については、「DNS (572 ページ)」および「詳細 (573 ページ)」を参照してください。

静的登録の設定

1 この範囲を有効にするには、「**この DHCP 範囲を有効にする**」を選択します。このオプションは、既定では選択されています。

2 「**登録名**」フィールドに、静的登録の名前を入力します。

3 「**静的 IP アドレス**」フィールドに、機器の IP アドレスを入力します。

4 「**MAC アドレス**」フィールドに、機器のイーサネット (MAC) アドレスを入力します。

5 「**リース期間 (分)**」、「**デフォルト ゲートウェイ**」、および「**サブネット マスク**」の各フィールドに特定のインターフェースの既定値を設定するには、ダイアログの下の方にある「**インターフェースの事前設定**」をオンにします。ドロップダウン メニューが使用可能になります。このオプションは、既定では選択されていません。

   a ドロップダウン メニューで、インターフェースを選択します。設定される IP アドレスは、選択したインターフェースと同じプライベート サブネットの IP アドレスです。

重要：「インターフェース」メニューからインターフェースを選択するには、対象のインターフェースをあらかじめ完全に設定しておく必要があります。 選択できるのは、LAN、WLAN、DMZ のいずれかのゾーン タイプ、または VLAN サブインターフェースのみです。

6 「**リース期間 (分)**」フィールドに、別の IP アドレスが発行されるまで範囲によって IP アドレスがリースされる時間を分単位で入力します。最小値は 0、最大値は 71582789、既定値は **1440** (24 時間) です。

7 設定されているゲートウェイ アドレスを使用するか、ゲートウェイの IP アドレスを「**デフォルト ゲートウェイ**」フィールドに入力します。

8 設定されているサブネット マスクを使用するか、ゲートウェイのサブネット マスクを「**サブネット マスク**」フィールドに入力します。

9 必要に応じて、「**コメント**」フィールドにコメントを入力します。

10 DNS/WINS 設定と詳細設定の設定方法については、「DNS/WINS (575 ページ)」および「詳細 (576 ページ)」を参照してください。

11 「**OK**」を選択してファイアウォールに設定を追加します。

12 「**適用**」を選択してファイアウォールに設定を適用します。

SonicWall セキュリティ装置の VoIP サポート機能の詳細については、「VoIP について (792 ページ)」を参照してください。

DHCP リース範囲の DHCP 汎用オプションの設定

ここでは、リース範囲の DHCP 汎用オプションの設定作業について説明します。

メモ：DHCP リース範囲の汎用オプションを設定するには、あらかじめ静的または動的な DHCP サーバ リース範囲を作成しておく必要があります。

各 DHCP オプションの説明は、「RFC で定義された DHCP オプション番号 (580 ページ)」の一覧表 (RFC で割り当てられたオプション番号順) にまとめてあります。

DHCP サーバ リース範囲の DHCP 汎用オプションを設定するには、以下の手順を実行します。

1 次の場合：

- 既存の DHCP リース範囲に変更を加える場合:
  1) 「**ネットワーク > DHCP サーバ**」の「DHCP サーバ リース範囲」テーブルを表示し、変更を加えるリース範囲のエントリを確認します。
  2) **設定**アイコンを選択します。
  3) 表示されるダイアログで「**詳細**」を選択します。
- 新しい DHCP リース範囲を作成する場合:
  1) 「**一般**」タブおよび「**DNS/WINS**」タブでオプションを設定した後 (「DHCP サーバの動的範囲の設定 (571 ページ)」または「静的 DHCP 登録の設定 (577 ページ)」を参照してください)、「**詳細**」タブを選択します。

2 「**DHCP 汎用オプション グループ**」ドロップダウン メニューで、DHCP オプションまたはオプション グループを選択します。

「**ネットワーク起動設定**」のフィールドを PXE 用に設定する場合は、ここで「**PXE**」を選択します。

3 この DHCP サーバ リース範囲の DHCP オプションを常に使用する場合は、「**汎用オプションを常に送信**」チェックボックスをオンにします。

4 「**OK**」を選択します。

RFC で定義された DHCP オプション番号

オプション番号	IPv6 √	名前	説明
2		Time Offset 【タイム オフセット】	協定世界時からのオフセット時間
3		Routers 【ルータ】	N/4 ルータのアドレス
4		Time Servers 【タイム サーバ】	N/4 タイム サーバのアドレス
5		Name Servers 【ネーム サーバ】	N/4 IEN-116 ネーム サーバのアドレス
6		DNS Servers 【DNS サーバ】	N/4 DNS サーバのアドレス
7		Log Servers 【ログ サーバ】	N/4 ログ サーバのアドレス
8		Cookie Servers 【Cookie サーバ】	N/4 Cookie サーバのアドレス
9		LPR Servers 【LPR サーバ】	N/4 プリンタ サーバのアドレス
10		Impress Servers 【Impress サーバ】	N/4 Imagen Impress サーバのアドレス
11		RLP Servers 【RLP サーバ】	N/4 リソース ロケーション サーバのアドレス
12	√	Host Name 【ホスト名】	ホスト名の文字列 (**(サーバ ユニキャスト)** など)
13		Boot File Size 【ブート ファイル サイズ】	ブート ファイルのサイズ (512 バイト ブロックの数)
14		Merit Dump File 【メリット ダンプ ファイル】	クライアントのコア イメージがダンプされるファイルの名前
15		Domain Name 【ドメイン名】	クライアントの DNS ドメイン名
16		Swap Server 【Swap サーバ】	スワップ サーバのアドレス
17		Root Path 【ルート パス】	ルート ディスクのパス名
18		Extension File 【拡張ファイル】	追加的な BOOTP 情報が含まれているファイルのパス名
19		IP Layer Forwarding 【IP レイヤ転送】	IP 転送の有効化または無効化
20		Src route enable 【送信元ルート有効】	送信元ルーティングの有効化または無効化
21	√	Policy Filter 【ポリシー フィルタ】(IPv4)	ルーティングに対するポリシー フィルタ (IPv4)
		SIP Servers Domain Name List 【SIP サーバ ドメイン名リスト】(IPv6)	SIP サーバ ドメイン名のリストを有効にする (IPv6)

オプション番号	IPv6 √	名前	説明
22	√	Max DG Reassembly Size 【最大 DG 再編成サイズ】(IPv4) SIP Servers IPv6 Address List 【SIP サーバ IPv6 アドレス リスト】(IPv6)	再編成するデータグラムの最大サイズ (IPv4) SIP サーバ IPv6 アドレスのリストを有効にする (IPv6)
23	√	Default IP TTL 【既定の IP TTL】(IPv4) DNS Recursive Name Server 【DNS 再帰名前サーバ】(IPv6)	既定の IP 存続期間 (IPv4) DNS 再帰名前サーバのリストを有効にする (IPv6)
24	√	Path Mtu Aging Timeout 【Path Mtu Aging タイムアウト】(IPv4) Domain Search List 【ドメイン検索リスト】(IPv6)	Path MTU Aging タイムアウト (IPv4) 検索用ドメイン名のリストを有効にする (IPv6)
25		MTU Plateau	パス MTU 検出の実行時に使用する MTU サイズのテーブル
26		Interface MTU Size 【インターフェース MTU サイズ】	インターフェースの MTU のサイズ
27	√	All Subnets Are Local 【すべてのサブネットはローカル】(IPv4) Network Information Service (NIS) Servers 【ネットワーク情報サービス (NIS) サーバ】(IPv6)	すべてのサブネットはローカル (IPv4) ネットワーク情報サービス (NIS) サーバのリストを有効にする (IPv6)
28	√	Broadcast Address 【ブロードキャスト アドレス】(IPv4) Network Information Service V2 (NIS+) Servers 【ネットワーク情報サービス V2 (NIS+) サーバ】(IPv6)	ブロードキャスト アドレス (IPv4) ネットワーク情報サービス V2 (NIS+) サーバのリストを有効にする (IPv6)
29	√	Perform Mask Discovery 【マスク発見の実行】(IPv4) Network Information Service (NIS) Domain Name 【ネットワーク情報サービス (NIS) ドメイン名】(IPv6)	マスク発見の実行 (IPv4) ネットワーク情報サービス (NIS) ドメイン名のリストを有効にする (IPv6)
30	√	Provide Mask To Others 【マスクを他者に提供】(IPv4) Network Information Service V2 (NIS+) Domain Name 【ネットワーク情報サービス V2 (NIS+) ドメイン名】(IPv6)	マスクを他者に提供 (IPv4) ネットワーク情報サービス V2 (NIS+) ドメイン名のリストを有効にする (IPv6)
31	√	Perform Router Discovery 【ルータ発見の実行】(IPv4) Simple Network Time Protocol (SNTP) Servers 【シンプル ネットワーク タイム プロトコル (SNTP) サーバ】(IPv6)	ルータ発見の実行 (IPv4) シンプル ネットワーク タイム プロトコル (SNTP) サーバのリストを有効にする (IPv6)

オプション番号	IPv6 √	名前	説明
32	√	Router Solicitation Address 【ルータ要請アドレス】(IPv4) Information Refresh Time 【情報更新時間】(IPv6)	ルータ要請アドレス (IPv4) 情報更新時間 (IPv6)
33		Static Routing Table 【静的ルーティング テーブル】	静的ルーティング テーブル
34		Trailer Encapsulation 【Trailer カプセル化】	トレーラの使用を試みるか否かを指定
35		ARP Cache Timeout 【ARP キャッシュ タイムアウト】	ARP キャッシュのタイムアウト時間
36		Ethernet Encapsulation 【イーサネット カプセル化】	イーサネットのカプセル化を使用するか否かを指定
37		Default TCP Time to Live 【既定の TCP 持続時間】	既定の TCP 存続期間
38		TCP Keepalive Interval 【TCP キープアライブ間隔】	TCP キープアライブ メッセージの送信間隔
39		TCP Keepalive Garbage 【TCP キープアライブ ガーベイジ】	TCP キープアライブ メッセージとともに互換性のための無意味なバイトを送信するか否かを指定
40		NIS Domain Name 【NIS ドメイン名】	NIS ドメイン名
41		NIS Server Addresses 【NIS サーバ アドレス】	NIS サーバのアドレス
42		NTP Server Addresses 【NTP サーバ アドレス】	NTP サーバのアドレス
43		Vendor Specific Information 【ベンダー固有情報】	ベンダー固有情報
44		NETBIOS Name Servers 【NETBIOS ネーム サーバ】	NetBIOS ネーム サーバのアドレス
45		NETBIOS Datagram Distribution 【NETBIOS データグラム ディストリビューション】	NetBIOS データグラム配信サーバのアドレス
46		NETBIOS Node Type 【NETBIOS ノード種別】	NetBIOS ノードの種類
47		NETBIOS Scope 【NETBIOS スコープ】	NetBIOS スコープ
48		X Window Font Server 【X Window フォント サーバ】	X ウィンドウ フォント サーバのアドレス
49		X Window Display Manager 【X Window ディスプレイ マネージャ】	X ウィンドウ表示マネージャが実行されているシステムのアドレス
50		Requested IP Address 【要求 IP アドレス】	要求された IP アドレス
51		IP Address Lease Time 【IP アドレス リース時間】	IP アドレスのリース期間

オプション番号	IPv6 √	名前	説明
52		Overload sname or file 【"sname" または "file" の過多】	“sname" または “file" フィールドをオプション用に使用していることを示す
53		DHCP Message Type 【DHCP メッセージ種別】	DHCP メッセージの種類
54		DHCP Server Identification 【DHCP サーバ証明】	DHCP サーバの識別情報
55		Parameter Request List 【パラメータ要求リスト】	要求するパラメータのリスト
56		DHCP Error Message 【DHCP エラー メッセージ】	DHCP エラー メッセージ
57		DHCP Maximum Message Size 【DHCP 最大メッセージ サイズ】	DHCP メッセージの最大サイズ
58		DHCP Renewal T1 Time 【DHCP リニューアル T1 タイム】	DHCP リースの再取得を要求するまでの時間 (T1)
59		DHCP Rebinding T2 Time 【DHCP リバインド T2 タイム】	DHCP 再割り当てを要求するまでの時間 (T2)
60		Class Identifier 【クラス識別子】	クライアント識別子
61		Client Identifier 【クライアント識別子】	クライアント識別子
62		Netware/IP Domain Name 【Netware/IP ドメイン名】	Netware/IP ドメイン名
63		Netware/IP sub Options 【Netware/IP サブ オプション】	Netware/IP サブ オプション
64		NIS+ v3 Client Domain Name 【NIS+ v3 クライアント ドメイン名】	NIS+ V3 クライアントのドメイン名
65		NIS+ v3 Server Addresses 【NIS+ v3 サーバ アドレス】	NIS+ V3 サーバのアドレス
66		TFTP Server Name 【TFTP サーバ名】	TFTP サーバ名
67		Boot File Name 【ブート ファイル名】	ブート ファイル名
68		Home Agent Addresses 【ホーム エージェント アドレス】	モバイル IP ホーム エージェントのアドレス
69		Simple Mail Server Addresses 【Simple Mail サーバ アドレス】	Simple Mail Transfer Protocol (SMTP) サーバのアドレス
70		Post Office Server Addresses 【Post Office サーバ アドレス】	Post Office Protocol (POP3) サーバのアドレス
71		Network News Server Addresses 【Network News サーバ アドレス】	Network News Transfer Protocol (NNTP) サーバのアドレス
72		WWW Server Addresses 【WWW サーバ アドレス】	WWW サーバのアドレス
73		Finger Server Addresses 【Finger サーバ アドレス】	フィンガー サーバのアドレス

オプション番号	IPv6 √	名前	説明
74		Chat Server Addresses 【Chat サーバ アドレス】	Internet Relay Chat (IRC) サーバのアドレス
75		StreetTalk Server Addresses 【StreetTalk サーバ アドレス】	StreetTalk サーバのアドレス
76		StreetTalk Directory Assistance Addresses 【StreetTalk Directory Assistance アドレス】	StreetTalk Directory Assistance (STDA) サーバのアドレス
77		User Class Information 【ユーザ クラス情報】	ユーザ クラス情報
78		SLP Directory Agent 【SLP ディレクトリ エージェント】	Service Location Protocol (SLP) ディレクトリ エージェントのアドレス
79		SLP Service Scope 【SLP サービス スコープ】	Service Location Protocol (SLP) エージェントのスコープ
80		Rapid Commit 【急速コミット】	高速コミットの使用
81		FQDN, Fully Qualified Domain Name 【FQDN、完全修飾ドメイン名】	完全修飾ドメイン名
82		Relay Agent Information 【Relay エージェント情報】	リレー エージェント情報
83		Internet Storage Name Service 【インターネット ストレージ ネーム サービス】	Internet Storage Name Service (iSNS) サーバのアドレス
84		Undefined 【未定義】	N/A
85		Novell Directory Servers 【Novell ディレクトリ サービス】	Novell Directory Services (NDS) サーバのアドレス
86		Novell Directory Server Tree Name 【Novell ディレクトリ サーバ ツリー名】	Novell Directory Services (NDS) サーバ ツリー名
87		Novell Directory Server Context 【Novell ディレクトリ サーバ コンテキスト】	Novell Directory Services (NDS) サーバ コンテキスト
88		BCMCS Controller Domain Name List 【BCMCS コントローラ ドメイン名リスト】	Broadcast/Multicast Services (BCMCS) コントローラのドメイン名リスト
89		BCMCS Controller IPv4 Address List 【BCMCS コントローラ IPv4 アドレス リスト】	BCMCS コントローラの IPv4 アドレス リスト
90		Authentication 【認証】	認証
91 - 92		Undefined 【未定義】	N/A
93		Client System 【クライアント システム】	クライアントのシステム手法の種類
94		Client Network Device Interface 【クライアント ネットワーク装置インターフェース】	クライアントのネットワーク機器インターフェースの種類
95		LDAP Use 【LDAP 利用】	Lightweight Directory Access Protocol (LDAP) の使用

オプション番号	IPv6 √	名前	説明
96		Undefined 【未定義】	N/A
97		UUID/GUID-based Client Identifier 【UUID/GUID に基づくクライアント識別子】	UUID/GUID に基づくクライアント識別子
98		Open Group's User Authentication 【オープン グループのユーザ認証】	オープン グループのユーザ認証サービスの URL
99 - 108		Undefined 【未定義】	N/A
109		Autonomous System Number 【自律システム番号】	自律システム番号
110 - 111		Undefined 【未定義】	N/A
112		NetInfo Parent Server Address 【NetInfo Parent サーバ アドレス】	NetInfo 親サーバのアドレス
113		NetInfo Parent Server Tag 【NetInfo Parent サーバ タグ】	NetInfo 親サーバのタグ
114		URL:	URL
115		Undefined 【未定義】	N/A
116		Auto Configure 【自動設定】	DHCP 自動設定
117		Name Service Search 【ネーム サービス探索】	ネーム サービス検索
118		Subnet Selection 【サブネットの選択】	サブネットの選択
119		DNS Domain Search List 【DNS ドメイン探索リスト】	DNS ドメイン検索リスト
120		SIP Servers DHCP Option 【SIP サーバ DHCP オプション】	Session Initiation Protocol (SIP) サーバのドメイン名またはアドレス
121		Classless Static Route Option 【クラス静的ルート オプション】	クラスレス静的ルート オプション
122		CCC, CableLabs Client Configuration 【CCC, CableLabs クライアント設定】	CableLabs クライアントの設定オプション
123		Geographic location setting information 【地理的位置設定情報】	地理的位置設定情報
124		Vendor-Identifying Vendor Class 【Vendor-Identifying ベンダー クラス】	ベンダー識別のためのベンダー種別情報
125		Vendor Identifying Vendor Specific 【Vendor-Identifying ベンダー固有】	ベンダー識別のためのベンダー固有情報
126 - 127		Undefined 【未定義】	N/A
128		TFTP Server IP Address 【TFTP サーバ IP アドレス】	IP 電話のソフトウェアを読み込むための TFTP サーバの IP アドレス

オプション番号	IPv6 √	名前	説明
129		Call Server IP Address 【Call サーバ IP アドレス】	通話サーバの IP アドレス
130		Discrimination String 【差別文字列】	ベンダーを識別するための判別文字列
131		Remote Statistics Server IP Address 【リモート統計サーバ IP アドレス】	リモート統計サーバの IP アドレス
132		802.1Q VLAN ID	IEEE 802.1Q の VLAN ID
133		802.1Q L2 Priority 【802.1Q L2 優先順位】	IEEE 802.1Q の第 2 層優先順位
134		Diffserv Code Point 【Diffserv コード ポイント】	VoIP シグナルとメディア ストリームのための Diffservコード ポイント
135		HTTP Proxy For Phone Applications 【電話アプリケーションの HTTP プロキシ】	電話固有アプリケーション用の HTTP プロキシ
136 - 149		Undefined 【未定義】	N/A
150		TFTP Server Address, Etherboot, GRUB Config 【TFTP サーバ アドレス、イーサ ブート、GRUB 設定】	TFTP サーバのアドレス、イーサブート、GRUB 設定
151 - 174		Undefined 【未定義】	N/A
175		Ether Boot 【イーサ ブート】	イーサブート
176		IP Telephone 【IP 電話】	IP 電話
177		Ether Boot, PacketCable And Cable Home 【イーサ ブート、PacketCable 及び Cable Home】	イーサブート、PacketCable および CableHome
178 - 207		Undefined 【未定義】	N/A
208		`pxelinux.magic` (string) = `241.0.116.126`	`pxelinux.magic` (string) = `241.0.116.126`
209		`pxelinux.configfile` (text)	`pxelinux.configfile` (text)
210		`pxelinux.pathprefix` (text)	`pxelinux.pathprefix` (text)
211		`pxelinux.reboottime`	`pxelinux.reboottime`
212 - 219		Undefined 【未定義】	N/A
220		Subnet Allocation 【サブネット割り当て】	サブネットの割り当て
221		Virtual Subnet Allocation 【仮想サブネット割り当て】	仮想サブネットの選択
222 - 223		Undefined 【未定義】	N/A
224 - 254		Private Use 【プライベート利用】	私的使用

DHCP と IPv6

SonicOS の IPv6 実装の詳細については、「IPv6 (979 ページ)」を参照してください。

27

IP ヘルパーの使用

トピック:

- IP ヘルパーについて (588 ページ)
  - VPN トンネル インターフェースによる IP ヘルパーのサポート (589 ページ)
  - DHCPv6 リレー (590 ページ)
- ネットワーク > IP ヘルパー (592 ページ)
  - リレー プロトコル (593 ページ)
  - ポリシー (594 ページ)
  - DHCP/DHCPv6 リレー リース (594 ページ)
- IP ヘルパーの設定 (595 ページ)
  - IP ヘルパーの有効化 (595 ページ)
  - トラフィック統計の表示 (595 ページ)
  - リレー プロトコルの管理 (595 ページ)
  - IP ヘルパー ポリシーの管理 (597 ページ)
  - 表示される DHCP リレー リースのフィルタ (599 ページ)

IP ヘルパーについて

重要：WAN インターフェースおよび NAT 向けに構成されたインターフェースについては、IP ヘルパーではサポートしていません。

UDP (ユーザ データグラム プロトコル) の多くは、それぞれのサーバを探し出すためにブロードキャスト/マルチキャストを使用します。この際、通常はサーバが同じブロードキャスト サブネット上に存在する必要があります。サーバがクライアントと異なるサブネット上に存在する状況に対応するためには、UDP ブロードキャスト/マルチキャストをサーバのサブネットに転送するメカニズムが必要になります。このメカニズムを、UDP ブロードキャストの転送と呼びます。IP ヘルパーを使用すると、ブロードキャスト/マルチキャスト パケットが SonicWall セキュリティ装置のインターフェースを通過し、ポリシーに基づいて他のインターフェースに転送されるようになります。IP ヘルパーを使用して、 セキュリティ装置がそのインターフェース上で受信した DHCP 要求を中央の DHCP サーバに転送するように設定できます。

IP ヘルパーは、ユーザ定義のプロトコルと拡張ポリシーをサポートします。また、既存の NetBIOS/DHCP リレー アプリケーションをより細かく制御できるようになりました。拡張された組み込みアプリケーションの一部を以下に示します。

拡張されたビルトイン リレー アプリケーション

プロトコル	UDP ポート番号
DHCP	67/68
DHCPv6	546、547
Net-BIOS NS	137
Net-BIOS データグラム	138
DNS	53
Time サービス	37
Wake on LAN (WOL)	
mDNS	5353 マルチキャスト アドレス: 224.0.0.251

VPN トンネル インターフェースによる IP ヘルパーのサポート

VPN トンネル インターフェースで IP ヘルパーをサポートできます。「トンネル インターフェース サポートを使用した IP ヘルパー内の DHCP リプレイ」は、IP ヘルパー内の DHCP リプレイの簡単な例を示しています。

- PC は、DHCP プロトコルから IPv4 アドレスを取得するために必要な機器です。
- ゲートウェイ A は、ゲートウェイに対応した IP ヘルパーです。
- ゲートウェイ B は、DHCP サーバを備えたゲートウェイです。

トンネル インターフェース サポートを使用した IP ヘルパー内の DHCP リプレイ

VPN トンネル インターフェースを使用して IP ヘルパーを設定するには、以下の手順に従います。

メモ：「トンネル インターフェース サポートを使用した IP ヘルパー内の DHCP リプレイ」の数字は、タスクの番号に対応しています。

1 PC:
   a ゲートウェイ A の LAN (X0) サブネットに接続します。
   b DHCP モード経由で IP アドレスを取得するように設定します。
2 ゲートウェイ A とゲートウェイ B の間の VPN トンネルの設定
   - VPN トンネル インターフェースを追加します。
3 ゲートウェイ B:
   a トンネル インターフェースの IP アドレスからゲートウェイ A の X0 インターフェースへのルート登録を追加します。

b トンネル インターフェースの発信インターフェースを追加します。

c PC の DHCP スコープとして IP アドレス範囲を追加します。

4 ゲートウェイ A:

a IP ヘルパーを有効にします。

b X0 からゲートウェイ B のトンネル インターフェース アドレスへの IP ヘルパー DHCP リレー プロトコルを追加します。プロトコルは DHCP です。

DHCPv6 リレー

トピック:

- DHCPv6 リレーについて (590 ページ)
- DHCPv6 リレーの設定 (591 ページ)

DHCPv6 リレーについて

SonicOS では、DHCPv6 リレーがサポートされます。DHCP リレー エージェントは、クライアントとサーバ間で DHCP メッセージをやりとりするための仲介ノードとして機能し、クライアントと同じリンク上に存在します。クライアントとサーバが同じ IPv6 リンク上にない場合に、DHCPv6 リレー エージェントを使用して、クライアントとサーバ間でメッセージをリレーします。DHCPv6 リレー エージェントの動作をクライアントから意識する必要はありません。

SonicOS では、サポートされる送信先アドレスに、グローバル アドレスまたはリンクローカル アドレスを指定できますが、マルチキャスト アドレスは使用できません。

DHCPv6 リレーは、物理と仮想の両方のインターフェースで有効にすることができます。DHCPv6 は、IP ヘルパーのプロトコルに組み込まれたアプリケーションの一種です。

DHCPv6 リレーの設定

DHCPv6 リレーを設定するには:

1 「**管理 | システム セットアップ > ネットワーク > IP ヘルパー**」ページに移動します。

2 「**ポリシー**」セクションまでスクロールします。

3 「**追加**」を選択します。「**IP ヘルパー ポリシーの追加**」ダイアログが表示されます。

4 「**プロトコル**」から「**DHCPv6**」を選択します。

5 「**送信元**」から目的のインターフェースを選択します。

6 「**送信先**」フィールドに、送信先の IPv6 アドレスを入力します。これには、ユニキャスト アドレス、または選択した他のアドレスなど、送信先アドレスのリストを指定することもできます。このアドレスとしてマルチキャスト アドレスを指定することはできません。

7 「**送信先**」フィールドの送信先が

- グローバル アドレスの場合は、送信インターフェースを選択する必要はありません。「ステップ 8」へ進みます。
- リンクローカルアドレスの場合は、「**送信インターフェース**」から送信インターフェースを選択します。

8 「**OK**」を選択します。

クライアントがサーバから新しい IP アドレスを取得すると、このページの「**DHCPv6 リレー リース**」セクションに新規の DHCP リースが表示されます。

ネットワーク > IP ヘルパー

トピック:

- リレー プロトコル (593 ページ)
- ポリシー (594 ページ)
- DHCP/DHCPv6 リレー リース (594 ページ)

リレー プロトコル

名前 IP ヘルパー アプリケーション名。

ポート IP ヘルパー アプリケーションの最初の UDP ポート番号。

ポート IP ヘルパー アプリケーションの 2 番目の UDP ポート番号 (オプション)。

Raw IP ヘルパー アプリケーションの設定時に Raw モードが選択されたかどうかを示します。このオプションが有効になっている場合、タイムアウトは無視されます。

プロトコル UDP。

タイムアウト (秒) IP ヘルパー キャッシュのタイムアウト時間。「**該当なし**」は Raw モードが選択されていてタイムアウトが無視されることを示します。

モード プロトコルがサポートしているモードを示します。

- **ブロードキャスト**
- **マルチキャスト**
- **両方**

マルチキャスト IP プロトコルが使用するマルチキャスト IP。

IP 変換 IP ヘルパー ポリシーによるパケット転送時に送信元 IP アドレスが変換されるかどうかを示します。

有効 IP ヘルパー ポリシーが有効かどうかを示します。

設定 エントリの**統計**アイコン、**編集**アイコン、**削除**アイコンがあります。

メモ： ユーザによって生成されたリレー プロトコルのみを削除できます。

ポリシー

リレー プロトコル	ポリシーのプロトコル。
送信元	ポリシーのインターフェースまたはゾーン。
送信先	ネットワーク送信先。
コメント	ポリシー設定時に入力されたコメント。
有効	IP ヘルパー ポリシーが有効かどうかを示します。
設定	各エントリの統計アイコン、編集アイコン、削除アイコンがあります。

DHCP/DHCPv6 リレー リース

クライアントの IP アドレス	クライアント機器の IP アドレス。
インターフェース	セキュリティ装置上の受信インターフェース。
DHCP リレー リース:	
クライアントの MAC アドレス	クライアント機器の MAC アドレス。
クライアントのベンダー	クライアント機器の製造元。
DHCPv6 リレー リース	
IAID	インターフェース ID (Interface Association Identifier)。このインターフェースと 1 つ以上の IP アドレスとの間のバインディングです。
DUID	デバイス (ホスト) ID。DHCP 参加者を一意に識別する DHCP UID。
サーバの IP アドレス	DHCP サーバの IP アドレス。
リース期間	リレー リースの期間。
残り時間	リレー リースの残り時間。

DHCP リレー リース テーブルを再表示するには、以下の手順に従います。

1 「**再表示**」を選択します。

IP ヘルパーの設定

トピック:

- IP ヘルパーの有効化 (595 ページ)
- リレー プロトコルの管理 (595 ページ)
- IP ヘルパー ポリシーの管理 (597 ページ)

IP ヘルパーの有効化

IP ヘルパー機能を有効化するには、以下の手順に従います。

1 「**ネットワーク > IP ヘルパー**」に移動します。

2 「**IP ヘルパー設定**」で「**IP ヘルパーを有効にする**」を選択します。

リレー プロトコルの管理

トピック:

- トラフィック統計の表示 (595 ページ)
- ユーザ定義リレー プロトコルの追加 (596 ページ)
- ユーザ定義プロトコルの削除 (597 ページ)

トラフィック統計の表示

トラフィック統計は、リレー プロトコル テーブルとポリシー テーブルのどちらでも表示できます。

トラフィック統計を表示するには、以下の手順に従います。

1 プロトコルまたはポリシーの**統計**アイコンの上にカーソルを置きます。そのエントリのトラフィック状況がポップアップに表示されます。

リレー プロトコル テーブル

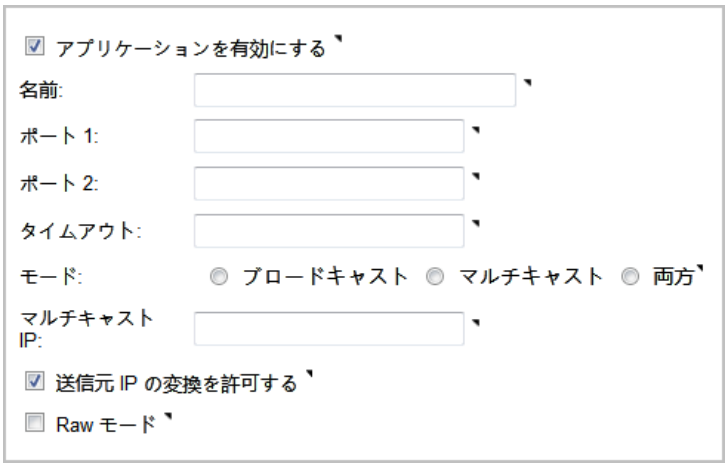
ポリシー テーブル

ユーザ定義リレー プロトコルの追加

リレー プロトコルを追加するには、以下の手順に従います。

1 「**ネットワーク > IP ヘルパー**」に移動します。

2 「**リレー プロトコル**」セクションの「**追加**」を選択します。「**IP ヘルパー アプリケーションの追加**」ダイアログが表示されます。



3 「**アプリケーションを有効にする**」を選択して、IP ヘルパー アプリケーションを有効にします。

> **メモ**：このオプションが無効になっている場合、すべての IP ヘルパー キャッシュが削除されます。

4 「**名前**」フィールドに、IP ヘルパー アプリケーションの一意の名前 (大文字と小文字の区別があります) を入力します。

5 「**ポート 1**」フィールドに、アプリケーションの一意の UDP ポート番号を指定します。

6 オプションで、「**ポート 2**」フィールドに、一意となる第 2 の UDP ポート番号をアプリケーションに対して指定します。

7 オプションで、「**タイムアウト**」フィールドに、IP ヘルパー キャッシュ タイムアウトの秒数を 10 ～ 60 の範囲で 10 秒単位で指定します。タイムアウトを指定しない場合は、既定値の **30** 秒が選択されます。

> **ヒント**：「**Raw モード**」が選択されている場合、このフィールドは無視されます。

8 「**モード**」を選択します。

- **ブロードキャスト**
- **マルチキャスト**
- **両方**

9 「**モード**」で「**マルチキャスト**」または「**両方**」を選択した場合は、「**マルチキャスト IP**」フィールドに、このプロトコルで使用する有効なマルチキャスト IP を指定します。

10 IP ヘルパー ポリシーによるパケット転送時に送信元 IP アドレスの変換を許可するには、「**送信元 IP の変換を許可する**」を選択します。このオプションは、既定では選択されています。

11 IP ヘルパー ポリシーによるパケットの転送時にキャッシュが作成されないようにするには、「**Raw モード**」を選択します。単方向の転送がサポートされています。このオプションは、既定では選択されていません。

ⓘ **メモ：**「**タイムアウト**」フィールドに設定されている時間は無視されます。

12 「**OK**」を選択します。

ユーザ定義プロトコルの削除

ユーザ定義プロトコルを削除するには、以下の手順に従います。

1 「**ネットワーク > IP ヘルパー**」に移動します。

2 そのプロトコルの**削除**アイコンを選択します。

1 つまたは複数のユーザ定義リレー プロトコルを削除するには、以下の手順に従います。

1 「**ネットワーク > IP ヘルパー**」に移動します。

2 目的のプロトコルの (プロトコル名のそばにある) 一番左のチェックボックスをオンにします。「**削除**」が使用可能になります。

3 「**削除**」を選択します。

すべてのユーザ定義リレー プロトコルを削除するには、以下の手順に従います。

1 「**ネットワーク > IP ヘルパー**」に移動します。

2 「**リレー プロトコル**」テーブルのヘッダーにあるチェックボックスをオンにします。「**削除**」が使用可能になります。

3 「**削除**」を選択します。

IP ヘルパー ポリシーの管理

IP ヘルパー ポリシーを使用すると、DHCP ブロードキャストと NetBIOS ブロードキャストをインターフェース間で転送できます。

ⓘ **重要：**WAN インターフェースおよび NAT 向けに構成されたインターフェースについては、IP ヘルパーではサポートしていません。

トピック:

- IP ヘルパー ポリシーの追加 (597 ページ)
- IP ヘルパー ポリシーの編集 (598 ページ)
- IP ヘルパー ポリシーの削除 (599 ページ)
- TSR による IP ヘルパー キャッシュの表示 (600 ページ)

IP ヘルパー ポリシーの追加

追加できるポリシーは最大 256 個です。

IP ヘルパー ポリシーを追加するには、以下の手順に従います。

1 「**ネットワーク > IP ヘルパー**」に移動します。

2 「**IP ヘルパー ポリシー**」テーブルの「**追加**」を選択します。「**IP ヘルパー ポリシーの追加**」ダイアログが表示されます。

3 このポリシーは既定で有効になっています。有効にせずにポリシーを設定するには、「**ポリシーを有効にする**」チェックボックスをオフにします。

4 「**プロトコル**」メニューからプロトコルを選択します。既定は「**DHCP**」です。

5 「**送信元**」で、送信元のインターフェースまたはゾーンを選択します。

6 「**送信先**」で、以下のどちらかを選択します。

- 送信先のアドレス グループまたはアドレス オブジェクト。
- **ネットワークの作成** (新しいアドレス オブジェクトを作成する場合)。「**アドレス オブジェクトの追加**」ダイアログが表示されます。アドレス オブジェクトの作成の詳細については、『*SonicOS ポリシー ガイド*』を参照してください。

7 必要に応じて、「**コメント**」フィールドに任意のコメントを入力します。

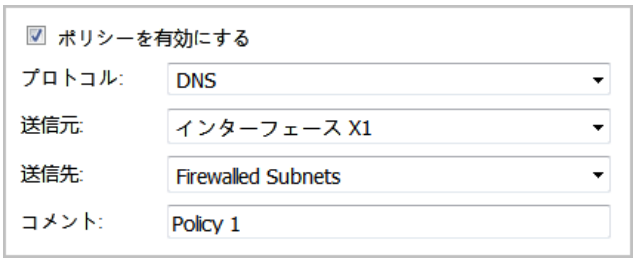
8 「**OK**」を選択します。

IP ヘルパー ポリシーの編集

IP ヘルパー ポリシーを編集するには、以下の手順に従います。

1 「**ネットワーク > IP ヘルパー**」に移動します。

2 「**IP ヘルパー ポリシー**」テーブルで、該当するエントリの「**設定**」列にある**編集**アイコンを選択します。「**IP ヘルパー ポリシーの編集**」ダイアログが表示されます。



3 設定内容は、「**IP ヘルパー ポリシーの追加**」ダイアログと同じです。このダイアログについては、「IP ヘルパー ポリシーの追加 (597 ページ)」を参照してください。

IP ヘルパー ポリシーの削除

ユーザ定義ポリシーを削除するには、以下の手順に従います。

1 「**ネットワーク > IP ヘルパー**」に移動します。

2 そのポリシーの「**ポリシー**」テーブルにある**削除**アイコンを選択します。

1 つまたは複数のユーザ定義ポリシーを削除するには、以下の手順に従います。

1 「**ネットワーク > IP ヘルパー**」に移動します。

2 目的のポリシーの (リレー プロトコルのそばにある) 一番左のチェックボックスをオンにします。「**削除**」が使用可能になります。

3 「**削除**」を選択します。

すべてのユーザ定義ポリシーを削除するには、以下の手順に従います。

1 「**ネットワーク > IP ヘルパー**」に移動します。

2 「**ポリシー**」テーブルのヘッダーにあるチェックボックスをオンにします。「**削除**」が使用可能になります。

3 「**削除**」を選択します。

表示される DHCP リレー リースのフィルタ

フィルタ機能を使用すると、「**アンチスプーフ キャッシュ**」テーブルおよび「**スプーフ検知リスト**」テーブルで特定の機器のみを表示できます。

テーブル表示をフィルタするには、以下の手順に従います。

1 「**ネットワーク > MAC-IP アンチスプーフ**」に移動します。

2 フィルタ対象のテーブルの下にある「**フィルタ**」フィールドで、機器の IP アドレス、インターフェース、MAC アドレス、ホスト名、名前のいずれかを指定します。このフィールドへの入力では、「フィルタ演算子の構文オプション」テーブルに示されている各演算子の適切な構文を使用する必要があります。

フィルタ演算子の構文オプション

演算子	構文オプション
タイプを持つ値	• Ip=1.1.1.1 or ip=1.1.1.0/24 • Mac=00:01:02:03:04:05 • Iface=x1
String	• X1 • 00:01 • Tst-mc • 1.1.
AND	• Ip=1.1.1.1;iface=x1 • Ip=1.1.1.0/24;iface=x1;just-string

フィルタ演算子の構文オプション

演算子	構文オプション
OR	• Ip=1.1.1.1,2.2.2.2,3.3.3.0/24 • Iface=x1,x2,x3
否定	• !ip=1.1.1.1;!just-string • !iface=x1,x2
混合	• Ip=1.1.1.1,2.2.2.2;mac=00:01:02:03:04:05; just-string;!iface=x1,x2

TSR による IP ヘルパー キャッシュの表示

テクニカル サポート レポートでは、IP ヘルパー キャッシュ、現在のポリシーおよびプロトコルのすべてが次のように表示されます。

```
#IP_HELPER_START
IP Helper
-----IP Helper Global Run-time Data-------
 IP Helper is OFF
 IP Helper - DHCP Relay is OFF
 IP Helper - Netbios Relay is OFF
  Total Number Of Fwded Packets           :0
  Total Number Of Dropped Packets         :0
  Total Number Of Passed Packets          :0
  Total Number Of Unknown Packets         :0
  Total Number Of record create failure   :0
  Total Number Of element create failure  :0User-defined
-----IP Helper Applications -------
 Name: DHCP
  Port: 67, 68, Max Record: 4000, Status: OFF
  CanBeDel: NO, ChangeIp: 1, Raw: NO
  Max Element: 8000, Timeout: 3, index: 1, proto: 1,
  Record Count: 0, Element Count: 0,
  Fwded: 0, Dropped: 0, Passed: 0
 Name: NetBIOS:
  Port: 138, 137, Max Record: 4000, Status: OFF
  CanBeDel: NO, ChangeIp: 1, Raw: NO
  Max Element: 8000, Timeout: 4, index: 2, proto: 1,
  Record Count: 0, Element Count: 0,
  Fwded: 0, Dropped: 0, Passed: 0
 Name: DNS
  Port: 53, 0, Max Record: 8000, Status: OFF
  CanBeDel: NO, ChangeIp: 1, Raw: NO
  Max Element: 16000, Timeout: 3, index: 3, proto: 1,
  Record Count: 0, Element Count: 0,
  Fwded: 0, Dropped: 0, Passed: 0
 Name: TIME
  Port: 37, 0, Max Record: 8000, Status: OFF
  CanBeDel: NO, ChangeIp: 1, Raw: NO
  Max Element: 16000, Timeout: 3, index: 4, proto: 1,
  Record Count: 0, Element Count: 0,
  Fwded: 0, Dropped: 0, Passed: 0
 Name: WOL
  Port: 7, 9, Max Record: 8000, Status: OFF
  CanBeDel: NO, ChangeIp: 1, Raw: YES
  Max Element: 16000, Timeout: 3, index: 5, proto: 1,
```

```
  Record Count: 0, Element Count: 0,
  Fwded: 0, Dropped: 0, Passed: 0
 Name: mDNS
  Port: 5353, 0, Max Record: 8000, Status: OFF
  CanBeDel: NO, ChangeIp: 1, Raw: YES
  Max Element: 16000, Timeout: 3, index: 6, proto: 1,
  Record Count: 0, Element Count: 0,
  Fwded: 0, Dropped: 0, Passed: 0
----------GEN APP Relay Policy-----------
---------------------------------Record Table----------------------------
Record(hash)[ClientIP, ClientIf, ClientMac, Proto, Vpn, transId, Age(pkts)]
 Elmnt(hash)[serverIp, serverIf, srcIp, dhcpMac, transId, Vpn, proto(fm,to)]
------------------------------------------------------------------------
----------DHCP Relay Policy-----------
--------NETBIOS Relay Policy-----------#IP_HELPER_END
```

28

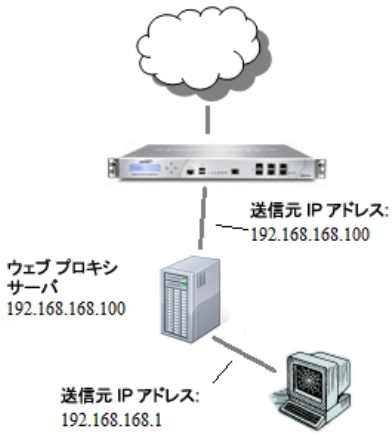
ウェブ プロキシ転送のセットアップ

トピック:

- ネットワーク > ウェブ プロキシ (602 ページ)
  - 自動プロキシ転送の設定 (ウェブのみ) (603 ページ)
  - ユーザ プロキシ サーバの設定 (604 ページ)

ネットワーク > ウェブ プロキシ

内部ネットワーク (ユーザと SonicWall セキュリティ装置の間) にあるプロキシ サーバを通じてユーザがウェブにアクセスすると、セキュリティ装置からはユーザではなくプロキシ サーバから HTTP/HTTPS 接続が行われているように見えます。



ウェブ プロキシ サーバは HTTP 要求をインターセプトし、要求されたウェブ ページのコピーを保管しているかどうかを判別します。保管していない場合、プロキシはインターネット上のサーバへの要求を完了し、要求された情報をユーザに返すとともに将来の要求に備えてローカルに保存します。ネットワーク上の各コンピュータがウェブ要求をサーバに送る設定をする必要があるため、ネットワーク上のウェブ プロキシ サーバのセットアップは手間がかかる場合があります。

プロキシ サーバがネットワーク上にある場合は、各コンピュータのウェブ ブラウザがプロキシ サーバに接続する設定をする代わりに、サーバを WAN または DMZ ゾーンに移動し、「**ネットワーク > ウェブ プロキシ**」ページの設定を使用して、ウェブ プロキシ転送を有効にすることができます。セキュリティ装置によってすべてのウェブ プロキシ要求が自動的にプロキシ サーバに転送され、ネットワーク上のすべてのコンピュータを設定する必要はありません。

トピック:

- 自動プロキシ転送の設定 (ウェブのみ) (603 ページ)
- ユーザ プロキシ サーバの設定 (604 ページ)

自動プロキシ転送の設定 (ウェブのみ)

メモ：ウェブ プロキシを有効にするには、クライアントの送信元となる関連ゾーンで CFS を有効にします (TZ シリーズ装置で WXA のウェブ キャッシュを使用するときは不要です)。

自動プロキシ転送 (ウェブのみ) を設定するには:

1 ウェブ プロキシ サーバをハブに接続します。

2 ハブをファイアウォールの WAN または DMZ ポートに接続します。

メモ：プロキシ サーバは WAN または DMZ ゾーンに配置しなければなりません。LAN に配置することはできません。

3 「**ネットワーク > ウェブ プロキシ**」に移動します。

4 すべてのウェブ プロキシ要求がプロキシ サーバに自動的に転送されるようにするには、「**自動プロキシ転送 (ウェブのみ)**」セクションの「**プロキシ ウェブ サーバ (名前または IP アドレス)**」フィールドにプロキシ サーバの名前または IP アドレスを入力します。長さは最小 0 文字、最大 39 文字です。

5 「**プロキシ ウェブ サーバのポート番号**」フィールドに、プロキシの IP ポートを入力します。既定値は 0 です。

6 ウェブ プロキシ サーバが利用できなくなった場合に、クライアントからインターネットに直接アクセスできるようにするには、「**プロキシ サーバが利用できない場合、プロキシ サーバをバイパスする**」を選択します。このオプションは、既定では無効になっています。

> **メモ：「プロキシ サーバが利用できない場合、プロキシ サーバをバイパスする」**チェックボックスをオンにすることにより、ウェブ プロキシ サーバが利用できなくなったときに、ファイアウォールの背後にあるクライアントがウェブ プロキシ サーバをバイパスできるようになります。代わりに、クライアントのブラウザは、ウェブ プロキシ サーバが指定されていないかのようにインターネットに直接アクセスします。

7 公開ゾーンにあるクライアントにもプロキシ サーバを強制的に使わせるには、「**公開ゾーン クライアント リクエストをプロキシ サーバに転送する**」を選択します。このオプションは、既定では無効になっています。

8 「**適用**」を選択します。

セキュリティ装置が更新された後、ブラウザ ウィンドウの一番下に更新を確認するメッセージが表示されます。

ユーザ プロキシ サーバの設定

ホスト名または IP アドレスを入力して、最大 32 のユーザ プロキシ サーバを設定できます。

ユーザ プロキシ サーバを設定するには:

1 「**ネットワーク > ウェブ プロキシ**」に移動します。

2 「**ユーザ プロキシ サーバ**」セクションに移動します。

3 「**追加**」を選択します。「**プロキシ サーバの追加**」ポップアップ ダイアログが表示されます。

メモ：ユーザのウェブ要求が SonicWall セキュリティ装置に到達する前にプロキシ サーバを経由する場合は、セキュリティ装置によって確認されたウェブ要求がユーザから直接届くのではなく、プロキシ サーバから届きます。そのため、セキュリティ装置は送信元 IP アドレスからユーザを特定することができません。しかし、各ウェブ要求の送信元を特定するプロキシ サーバは通常、この情報を HTTP ヘッダーに含めます。

内部プロキシ サーバがここで設定されている場合、セキュリティ装置はそのサーバからの情報を使用してユーザを特定します。

これは、内部ネットワークのプロキシ サーバ経由でウェブにアクセスするユーザの特定と、WAN 側の外部プロキシ サーバ経由でのセキュリティ装置のリモート HTTP 管理の両方に役立ちます。

4 プロキシ サーバの名前または IP アドレスを入力します。

5 「**OK**」を選択します。

6 プロキシ サーバをさらに追加するには、「ステップ 3」～「ステップ 5」を繰り返します。

7 「**適用**」を選択します。

8 インターフェースを設定した後で、それをホストに接続することができます。「インターフェースの設定 (278 ページ)」を参照してください。

ユーザ プロキシ サーバの編集

プロキシ サーバの名前または IP アドレスを編集するには:

1 「**ネットワーク > ウェブ プロキシ**」に移動します。

2 「**ユーザ プロキシ サーバ**」セクションに移動します。

3 「**ユーザ プロキシ サーバ**」テーブルで、編集するプロキシ サーバを選択します。

4 「**編集**」を選択します。「**プロキシ サーバの編集**」ポップアップ ダイアログが表示されます。

5 プロキシ サーバの名前または IP アドレスを変更します。

6 「**OK**」を選択します。

ユーザ プロキシ サーバの削除

プロキシ サーバを削除するには:

1 「**ネットワーク > ウェブ プロキシ**」に移動します。

2 「**ユーザ プロキシ サーバ**」セクションに移動します。

3 「**ユーザ プロキシ サーバ**」テーブルで、削除するプロキシ サーバを選択します。

4 「**削除**」を選択します。

5 「**適用**」を選択します。

29

動的 DNS の設定

トピック:

- ネットワーク > 動的 DNS (607 ページ)
  - 動的 DNS について (607 ページ)
  - サポートしている動的 DNS プロバイダ (608 ページ)
  - 動的 DNS プロファイル テーブル (609 ページ)
  - 動的 DNS プロファイルの設定 (610 ページ)
  - 動的 DNS プロファイルの編集 (613 ページ)
  - 動的 DNS プロファイルの削除 (614 ページ)

ネットワーク > 動的 DNS

トピック:

- 動的 DNS について (607 ページ)
- サポートしている動的 DNS プロバイダ (608 ページ)
- 動的 DNS プロファイル テーブル (609 ページ)
- 動的 DNS プロファイルの設定 (610 ページ)
- 動的 DNS プロファイルの編集 (613 ページ)
- 動的 DNS プロファイルの削除 (614 ページ)

動的 DNS について

動的 DNS (DDNS) は、IP アドレスを動的に変更する際、DNS レコードを人の手を介さず自動的に更新できるようにするサービスで、さまざまな会社や組織によって提供されています。このサービスは、対象の IP アドレスが変更された場合にも、IP アドレスではなくドメイン名を使用することによって、ネットワーク アクセスを可能にします。例えば、ユーザが IP アドレスを ISP から動的に割り当てられ

るDSL 接続を使用している場合、DDNS を使用して IP アドレスを DDNS サーバに登録し、またその後のアドレス変更もすべて登録することによって、外部のホストは同じドメイン名を使いながら変更後のアドレスにアクセスを継続することができます。

動的 DNS の実装は、サービス プロバイダごとに内容が異なります。通信方式や登録できるレコードの種類、提供可能なサービスの種類に、厳密な標準はありません。また、プレミアム バージョンのサービスを有償で提供するプロバイダもあります。このため、特定の DDNS プロバイダをサポートするには、そのプロバイダ固有の実装との明示的な相互運用性が必要です。

プロバイダのほとんどは、IP アドレスの変更が発生した場合のみ DDNS レコードを更新するほうが望ましいと考えています。頻繁な更新は、特に登録 IP アドレスが変更されていない場合、プロバイダによってサービスの誤用と判断され、その結果 DDNS アカウントがロック アウトされる場合があります。プロバイダのページに掲載されている使用方針を確認し、その方針に準拠してください。SonicWallでは DDNS プロバイダに関するテクニカル サポートは行いませんので、お問い合わせはプロバイダの方にお願いします。

サポートしている動的 DNS プロバイダ

すべてのプロバイダのすべてのサービスや機能をサポートしてはいません。また、サポートしているプロバイダのリストは、予告なく変更されることがあります。SonicOS では現在、「動的 DNSプロバイダ」テーブルに示すプロバイダのサービスをサポートしています。

動的 DNSプロバイダ

dns.org	SonicOSで `DynDNS.org` の DDNS を設定するには、ユーザ名、パスワード、メール エクスチェンジャー、バックアップ MX が必要です。
changeip.com	単一の古くからある動的 DNS サービスです。SonicOS の設定に必要なのは、ユーザ名、パスワード、ドメイン名のみです。
no-ip.com	SonicOS の設定に、ユーザ名、パスワード、ドメイン名のみを必要とする動的 DNS サービスです。ホスト名のグループ化もサポートしています。
Yi.org	SonicOS の設定に、ユーザ名、パスワード、ドメイン名のみを必要とする動的 DNS サービスです。動的更新を正しく行うには、`yi.org` 管理ページ上で RR レコードを作成する必要があります。

動的 DNS プロバイダによる追加サービス

動的 DNS プロバイダによって提供される共通の追加サービスには次のようなものがあります。

ワイルドカード	サブドメインのワイルドカード参照を可能にします。例えば、`yourdomain.dyndns.org` を登録すると、サイトは `*.yourdomain.dyndns.org` (`server.yourdomain.dyndns.org`、`www.yourdomain.dyndyn.org`、`ftp.yourdomain.dyndns.org` など) からアクセスできるようになります。
メール エクスチェンジャー	SMTP サーバが DNS によってアドレスを検索してメールを送信できるように、ドメインの MX レコード エントリを作成します。 **メモ：**受信 SMTP が ISP によって遮断されていることがよくあるので、メール サーバをホストしようとする前にプロバイダへお問い合わせください。

バックアップ MX (dns.org、yi.org が提供)	プライマリ IP アドレスが停止中のときのために、MX レコード用のバックアップ IP アドレスを指定できます。
グループ	ホストをグループ化することによって、更新を個々のメンバーに対して複数回行うのではなく、グループ レベルで一度に実行できます。
オフライン IP アドレス	登録されたプライマリ IP アドレスがオフラインの場合、登録ホスト名用のバックアップ アドレスを指定できます。

DDNS プロファイルの設定については、「動的 DNS プロファイルの設定 (610 ページ)」を参照してください。

動的 DNS プロファイル テーブル

「**動的 DNS プロファイル**」テーブルは、設定された動的 DNS プロファイルに関する情報を提供します。

表示する IP バージョン	IPv4 および IPv6 動的 DNS プロファイル間でのテーブルの切り替えを可能にします。
プロファイル名	動的 DNS エントリを作成したときに割り当てた名前です。任意の値が可能で、識別のためにのみ使用されます。
ドメイン	動的 DNS エントリの完全修飾ドメイン名 (FQDN) です。
プロバイダ	このエントリが登録されている動的 DNS プロバイダです。
状況	最後にレポートされた時点または現在の動的 DNS エントリの状況です。

オンライン	動的 DNS エントリは、管理上オンラインです。このエントリの現在の IP 設定が、タイム スタンプとともに表示されます。
オフライン中	動的 DNS エントリは、管理上オフラインです。エントリが**有効**な場合、「**動的 DNS プロファイルの追加**」の「**詳細設定**」ページにある「**オフライン設定**」セクションで設定された動作を実行します。
誤用	動的 DNS プロバイダが、頻繁な更新を誤用であると見なしました。どのような場合に誤用とされるかを、動的 DNS プロバイダのガイドラインで確認してください。
IP 変更なし	誤用の可能性。IP アドレスを変更しない強制的な更新を行った場合、誤用であると見なす動的 DNS プロバイダがあります。自動更新は、アドレスや状況が変化した場合にのみ発生します。手動の更新や強制更新は、登録情報が間違っているなど、明確に必要な場合にのみ行われます。
無効	設定エラーまたはポリシー違反のため、アカウントを無効にされました。プロファイルの設定と、プロバイダの動的 DNS アカウント状況を確認してください。
無効なアカウント	提供されたアカウント情報が有効ではありません。プロファイルの設定と、プロバイダの動的 DNS アカウント状況を確認してください。

	ネットワーク エラー	動的 DNS プロバイダと通信できません。ネットワーク エラーの疑いがあります。プロバイダがアクセス可能であり、オンラインになっていることを確認してください。時間を置いて再度実行してください。
	プロバイダ エラー	動的 DNS プロバイダは、今回要求された動作を実行することができません。プロファイルの設定と、プロバイダの動的 DNS アカウント状況を確認してください。時間を置いて再度実行してください。
	寄付者のアカウントではありません	プロバイダによって特定の機能 (オフライン アドレス設定など) が有料会員や寄付者にのみ利用可能な場合があります。どのサービスが有料または寄付が必要かの詳細は、プロバイダに確認してください。
有効	選択すると、このプロファイルは管理上有効になり、セキュリティ装置は「**動的 DNS プロファイルの追加**」の「**詳細設定**」ページで設定した「**オンライン設定**」の動作を行います。この設定は、エントリの「**動的 DNS プロファイルの追加**」の「**この動的 DNS プロファイルを有効にする**」オプションを使用して制御することもできます。このオプションを非選択にするとプロファイルは無効になり、再度有効になるまで、このプロファイルのための動的 DNS プロバイダとの通信は発生しません。	
オンライン	選択すると、このプロファイルは管理上オンラインになります。この設定は、エントリの「**動的 DNS プロファイルの追加**」で「**オンライン設定を使用する**」オプションを使用して制御することもできます。プロファイルが有効な間にこのオプションを非選択にした場合、プロファイルはオフラインになり、セキュリティ装置は「**詳細設定**」ページで設定された「**オフライン設定**」の動作を行います。	
設定	動的 DNS プロファイルを設定するための**編集**アイコンと、動的 DNS プロファイル登録を削除するための**削除**アイコンがあります。	

動的 DNS プロファイルの設定

DDNS プロファイルの設定に関する一般的な情報については、「動的 DNS について (607 ページ)」を参照してください。

動的 DNS サービスの使用は、利用する DDNS サービス プロバイダを選び、アカウントを設定することから始めます。同時に複数のプロバイダを利用することも可能です。「動的 DNSプロバイダ」テーブルにある各種プロバイダの一覧を参照してください。通常の登録手続きでは、プロバイダから確認の電子メールを受け取り、そのメールに埋め込まれている固有の URL へのアクセスを実行して最終確認を行います。選択したプロバイダのページにログインした後、管理用のリンク (一般に、「追加」や「管理」) を選択し、ホスト エントリを作成します。この作業は、SonicOS 上で動的 DNS クライアントを使用する前に行う必要があります。「**ネットワーク > 動的 DNS**」ページに、DDNS サービスを使用するように SonicWallセキュリティ装置を設定するための項目があります。

SonicWall セキュリティ装置で動的DNS を設定するには、以下の手順に従います。

1 「**ネットワーク > 動的 DNS**」に移動します。

2 「**追加**」を選択します。「**動的 DNS プロファイルの追加**」ダイアログが表示されます。

3 「**この動的 DNS プロファイルを有効にする**」チェックボックスがオンの場合は、このプロファイルは管理上有効になり、セキュリティ装置によって、「**詳細設定**」ページの「**オンライン設定**」セクションで定義されている動作が実行されます。このオプションは、既定では選択されています。

4 「**オンライン設定を使用する**」チェックボックスがオンの場合は、このプロファイルの管理はオンラインになります。このオプションは、既定では選択されています。

5 「**プロファイル名**」フィールドに、DDNS エントリに割り当てる名前を入力します。これには、「**動的DNS 設定**」テーブルでエントリを識別するのに使用する任意の名前を指定できます。名前は最小 1 文字、最大 63 文字です。

6 「**プロバイダ**」で、動的 DNS プロバイダを選択します。これらのプロバイダについては、「動的 DNSプロバイダ」テーブルを参照してください。既定値は **dyn.com** です。

ⓘ **重要**：選択した DNS プロバイダで動的サービス レコードを作成しておく必要があります。

ⓘ **ヒント**：どの DNS プロバイダでもすべてのオプションを使用できるわけではありません。また、ページ下部の「**補足**」には DNS プロバイダが HTTP または HTTPS プロトコルを使用しているかどうかや、そのプロバイダのウェブサイトへのリンクが表示されます。

7 「**ユーザ名**」フィールドに、DNS プロバイダでのユーザ名を入力します。名前は最小 1 文字、最大 63 文字です。

8 「**パスワード**」フィールドに DNS パスワードを入力します。名前は最小 1 文字、最大 31 文字です。

9 「**ドメイン名**」フィールドに、DNS プロバイダに登録したホスト名の完全修飾ドメイン名 (FQDN) を入力します。ホスト名とドメインが、設定したものと同じであることを確認します。名前は最小 1 文字、最大 63 文字です。

10 オプションで、この動的 DNS プロファイルを特定の WAN インターフェースに割り当てるために、「**関連付け先**」から該当する WAN インターフェースを選択します。複数 WAN 負荷分散を設定している場合は、このオプションにより、予測可能な IP アドレスを動的 DNS サービスに通知

できます。既定では、これは「**すべて**」に設定されていて、プロファイルがセキュリティ装置上でどの WAN インターフェースでも自由に使用できることを意味します。

11 「**プロバイダ**」で「**dyn.com**」を選択した場合は、「ステップ 13」に進みます。

12 dyn.org を使用する際には、「**サービス種別**」で選択したサービスの種類に対応するサービス種別を選択します。

動的	無料の動的 DNS サービスです。このオプションは既定の設定です。
ユーザ定義	管理されたプライマリ DNS ソリューションで、プライマリおよびバックアップの統合 DNSサービスと、ウェブベースのインターフェースを提供します。動的、静的双方の IP アドレスをサポートしています。
静的	静的 IP アドレスを使用する無料の DNS サービスです。

13 「**詳細設定**」を選択します。

ヒント：通常は、このページの既定の設定をそのまま使用できます。

14 「**オンライン設定**」セクションでは、動的 DNS プロバイダにどのアドレスを登録するかを指定します。次のどちらかを行います。

DDNS プロバイダに IP アドレスを検出させる	セキュリティ装置は DNS プロバイダによる IP アドレスの指定を許可します。 **メモ**：IPv4 のみ。このオプションは、既定では選択されています。
自動的に IP アドレスをプライマリ WAN IP アドレスに設定する	セキュリティ装置によって WAN IP アドレスが登録 IP アドレスとして割り付けられ、動的 DNS サーバによる自動検出に優先して使用されます。自動検出が適切に動作しない場合に役に立つ設定です。このオプションは、既定では選択されています。 **メモ**：IPv6 の場合: このオプションは、既定では選択されています。
IP アドレスを手動で指定する	登録する IP アドレスを手動で指定および割り付けできます。

15 「**オフライン設定**」セクションでは、セキュリティ装置で動的 DNS 登録がローカルにオフラインになっている (無効になっている) 場合に、動的 DNS サービス プロバイダにどの IP アドレスを登録するかを指定します。次のどちらかを行います。

何も行わない	前に登録したアドレスを動的 DNS プロバイダでの現在のアドレスにすることができます。このオプションは、既定では選択されています。
プロバイダ サイトで事前に設定したオフライン IP アドレスを使用する	プロバイダでオフライン設定の手動設定をサポートしている場合は、このオプションを選択して、このプロファイルの管理がオフラインのときにこれらの設定を使用できます。

16 「**OK**」を選択します。

動的 DNS プロファイルの編集

動的DNS プロファイルを編集するには、以下の手順に従います。

1 「**ネットワーク > 動的 DNS**」に移動します。

2 動的 DNS プロファイル テーブルで、該当するプロファイルの**編集**アイコンを選択します。「動的 DNS プロファイルの編集」ダイアログが表示されます。

3 変更を行います。各オプションの説明については、「動的 DNS プロファイルの設定 (610 ページ)」の手順を参照してください。

4 「**OK**」を選択します。

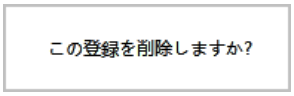
動的 DNS プロファイルの削除

1 つまたはすべての動的 DNS プロファイルを削除できます。

動的 DNS プロファイルを削除するには、以下の手順に従います。

1 「**ネットワーク > 動的 DNS**」に移動します。

2 削除するプロファイルの**削除**アイコンを選択します。確認メッセージが表示されます。

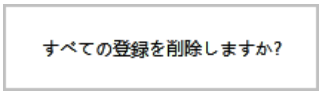


3 「**OK**」を選択します。

すべての動的 DNS エントリを削除するには、以下の手順に従います。

1 「**ネットワーク > 動的 DNS**」に移動します。

2 「**すべて削除**」を選択します。確認メッセージが表示されます。



3 「**OK**」を選択します。

30

AWS 資格情報の設定

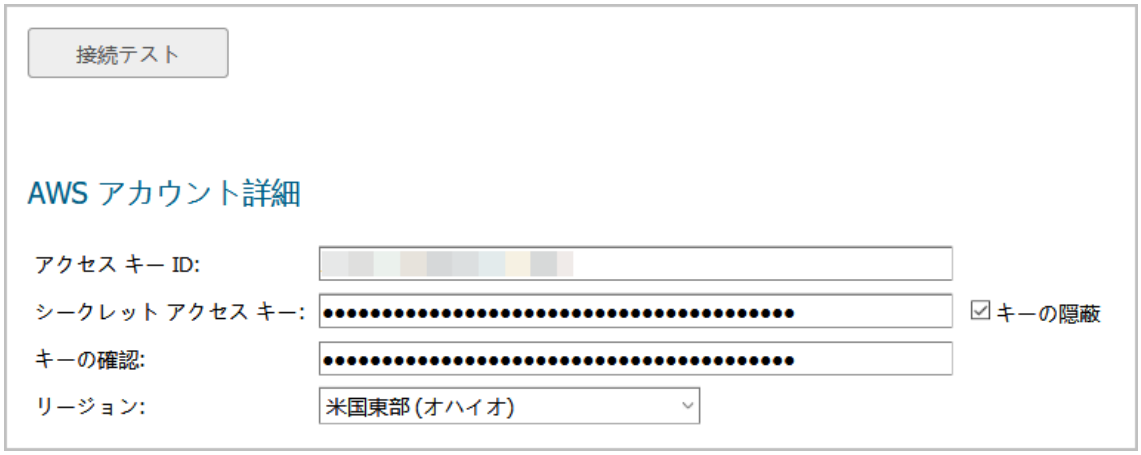
重要：SonicOS-AWS 統合機能を使用するには、以下の作業が必要です。

- アマゾン ウェブ サービス (AWS) に登録する。
- AWS ID とアクセス管理 (IAM) ユーザのアクセス キー ID とアクセス キーを取得する。
- IAM のベスト プラクティスを十分に理解する。

トピック:

- ネットワーク > AWS 設定 (615 ページ)
  - AWS について (616 ページ)
  - AWSの設定 (616 ページ)
  - 接続のトラブルシューティング (617 ページ)

ネットワーク > AWS 設定



トピック:

- AWS について (616 ページ)
- AWSの設定 (616 ページ)
- 接続のトラブルシューティング (617 ページ)

AWS について

SonicOS を アマゾン ウェブ サービス (AWS) と統合すると、次のことが可能になります。

- ログを AWS CloudWatch ログのサービス監視に保存し、システムやアプリケーションのトラブルシューティングを行う。
- AWS でホストされる分析ツール (ElasticSearch、Kibana など) を使用する。

SonicOS を AWS と統合し、セキュリティ装置が AWS のさまざまなアプリケーション プログラミング インターフェース (API) と通信できるようにするには、次の作業が必要です。

1 AWS セキュリティ資格情報を提供します。「AWSの設定 (616 ページ)」を参照してください。

2 AWS EC2 インスタンスに対応する AWS オブジェクト (アドレス オブジェクトやアドレス グループなど) を作成します。AWS オブジェクトの作成の詳細については、『*SonicOS 6.5 のポリシー*』を参照してください。

3 セキュリティ装置から AWS 仮想プライベート クラウド (VPC) に VPN 接続を作成します。VPN 接続の作成の詳細については、『*SonicOS 6.5 接続*』を参照してください。

4 ログ ストリームを作成し、ログ記録を有効にします。Amazon CloudWatch ログへのログ記録の詳細については、『*SonicOS 6.5 ログとレポート*』を参照してください。

AWSの設定

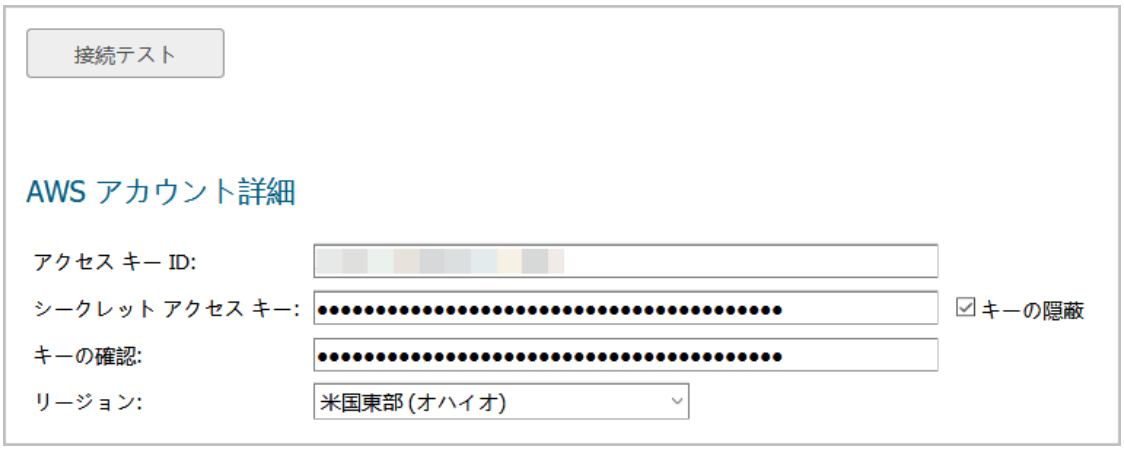
メモ：TLS v1.0 for AWS を使用できるように SonicOS を設定するには、SonicWall サポートに連絡してください。

AWS を設定するには:

1 次の作業を完了します。

- アマゾン ウェブ サービス (AWS) に登録する。
- AWS ID とアクセス管理 (IAM) ユーザのアクセス キー ID とシークレット アクセス キーを取得する。
- IAM のベスト プラクティスを十分に理解する。

2 「**管理 | システム セットアップ > ネットワーク > AWS 設定**」に移動します。



3 AWS アクセス キー ID を「**アクセス キー ID**」フィールドに入力します。AWS アクセス キー ID を使用してセキュリティ装置は AWS の API にアクセスします。このオプションは、既定では選択されていません。

4 安全のため、「**キーの隠蔽**」を選択してキーが見られないようにしてください。このオプションは、既定では選択されています。

5 AWS シークレット アクセス キーを「**シークレット アクセス キー**」フィールドに入力します。シークレット アクセス キーを使用してセキュリティ装置は AWS の API にアクセスします。「**キーの隠蔽**」を選択すると、このフィールドは一連の黒点で表示されます。

6 AWS シークレット アクセス キーを「**キーの確認**」フィールドに入力します。

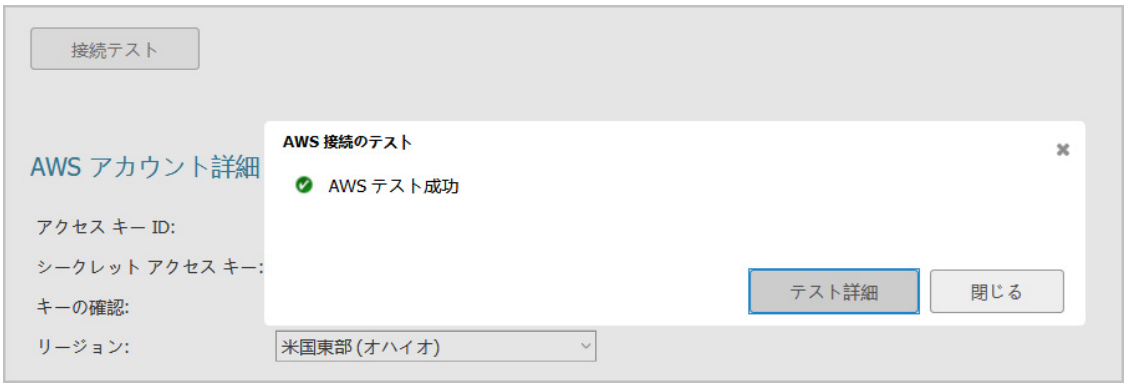
7 「**リージョン**」から、「**管理 | ポリシー > オブジェクト > AWS オブジェクト**」ページと「**管理 | 接続性 > VPN > AWS VPN**」ページを初期化するための既定の地域を選択します。既定値は **米国東部 (バージニア北部)** です。

重要：既定の地域がセキュリティ装置のイベント ログを AWS CloudWatch ログに送信する際に使用される地域である場合、それは「**管理 | ログと報告 > ログ設定 > AWS ログ**」ページで行った変更の影響を受けます。

8 「**適用**」を選択します。「**接続テスト**」が使用可能になります。

注意：この時点でエラーが発生すると、後で問題が発生するため、現時点で接続と設定をテストすることが重要です。

9 資格情報の有効性をテストし、セキュリティ装置が AWS と正常に通信できるようにするには、「**接続テスト**」を選択します。複数のテストを実行して、資格情報と AWS への接続をテストします。結果が表示されます。



ヒント：テストに問題があった場合は、「接続のトラブルシューティング (617 ページ)」を参照してください。

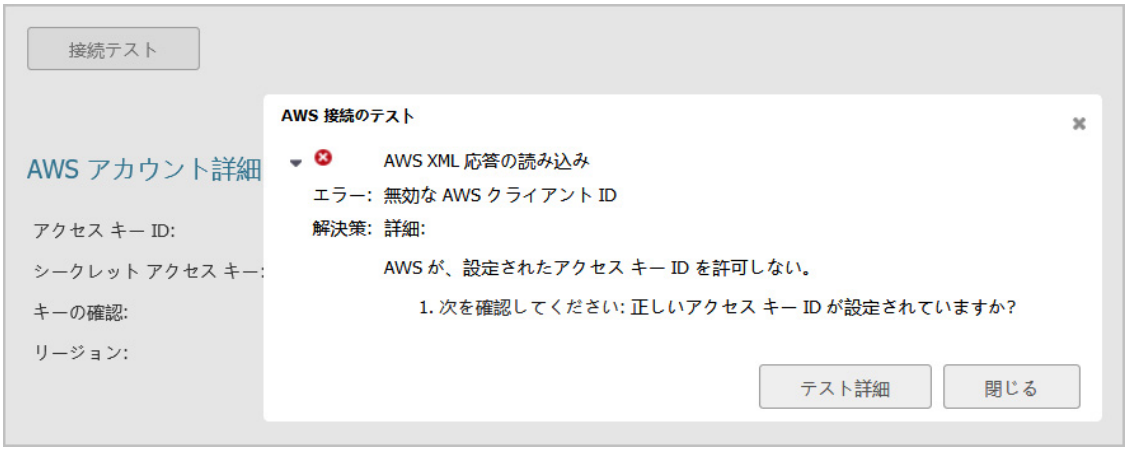
10 「**閉じる**」を選択します。

接続のトラブルシューティング

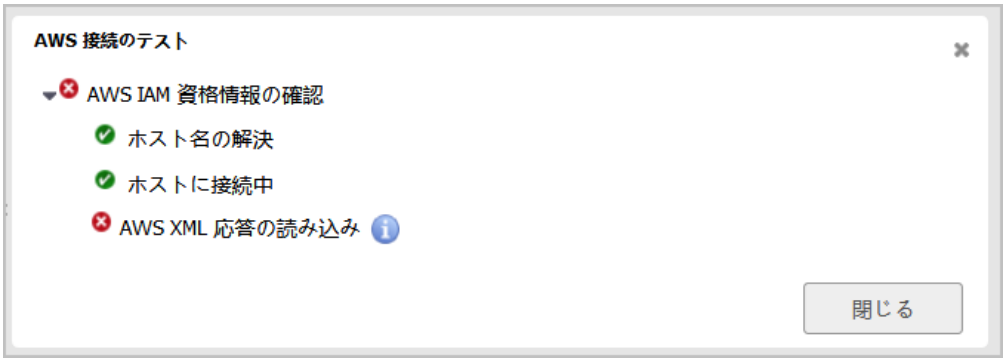
この例では、無効なアクセス キー ID を示しています。

接続のトラブルシューティングを行うには:

1 「**接続テスト**」を選択します。結果が表示されます。



2 「**テスト詳細**」を選択します。詳細な情報が表示されます。



3 さらに情報を表示するには、**情報**アイコンを選択します。別のポップアップが表示されます。

4 診断結果をメモします。

5 「**OK**」を選択します。

6 「**閉じる**」を選択します。

7 「**診断**」で説明されている問題を解決します。

8 「**接続テスト**」を選択します。

9 問題が完全に解決するまで「ステップ 1」から「ステップ 8」を繰り返します。

10 「**閉じる**」を選択します。

第 5 部

システム セットアップ | SD-WAN

- SD-WAN について
- SD-WAN グループの設定
- 性能監視の設定
- 性能クラス オブジェクトの設定
- パス選択プロファイルの設定
- SD-WAN ルート ポリシーの設定
- SD-WAN の監視
- SD-WAN ルート ポリシー接続の表示

31

SD-WAN について

SD-WAN (Software-Defined Wide Area Network) は、ワイド エリア ネットワーク (WAN) 接続をソフトウェア ベースで制御します。SonicOS SD-WAN は以下の機能を提供します。

- SD-WAN インターフェース グループ
  - WAN と VPN
  - 1 ～ N の範囲で拡張可能
- 以下に基づく動的パス選択:
  - 遅延、ジッタ、パケット損失
  - 品質評価のためのユーザ定義閾値
- アプリケーション対応ルーティング
- メトリック用のパス性能監視
- 接続ベースのトラフィック分散
- VPN 経由の自動接続フェイルオーバー
- プロビジョニングと管理 (GMS と Capture Security Center)

SD-WAN は、ネットワーク パスの動作方法に応じて動的に選択される最適な送信先インターフェースを必要とする特定のトラフィック タイプやアプリケーションに最適です。各アプリケーションは、適正に動作するために、ネットワーク パスで決まる一定の要件を持ちます。例えば、VoIP が正常に動作するネットワーク品質では、最適な遅延が 100 ミリ秒以下である必要がありますが、遅延が 150 ミリ秒以上だと通話が途切れます。SD-WAN は、このようなシナリオで役立つように、最初に複数のネットワーク パス上で遅延、ジッタ、パケット損失などのさまざまなネットワーク性能関連のメトリックを動的に測定します。SD-WAN は、これらのメトリックを特定のトラフィック フローの性能しきい値と比較し、それに応じてフローのネットワーク品質を満たす最適なネットワークを決定します。

トピック:

- SD-WAN グループの設定 (621 ページ)
- 性能監視の設定 (625 ページ)
- 性能クラス オブジェクトの設定 (631 ページ)
- パス選択プロファイルの設定 (636 ページ)
- SD-WAN ルート ポリシーの設定 (641 ページ)
- SD-WAN の監視 (647 ページ)
- SD-WAN ルート ポリシー接続の表示 (649 ページ)

32

SD-WAN グループの設定

トピック:

- SD-WAN グループ (621 ページ)
  - SD-WAN グループの作成 (622 ページ)
  - SD-WAN グループの編集 (623 ページ)
  - SD-WAN グループの削除 (623 ページ)

SD-WAN グループ

SD-WAN は、物理および仮想 WAN インターフェース種別と、VPN 番号付き/番号なしのトンネル インターフェース インスタンスをサポートしています。必要な選択肢は、SD-WAN グループの設定時にすべて提供されます。

番号付きトンネル インターフェース グループは、より進化したルートベースの実装であり、これまでよりもずっと直感的に操作できます。ただし、インターフェース テーブル内の他の実際のエントリから借用しているため、スケーリングに不向きです。番号なしトンネル インターフェース設定は、インターフェース テーブルのエントリと関連付けられていないため、必要なスケーラビリティの要件を満たすことができます。

SD-WAN グループは、各インターフェース パスを介した性能基準に基づいて、ロードバランシングや動的パス選択に使用できるインターフェースの論理グループです。個別グループを独自に作成することもできます。SonicOS SD-WAN とその機能の説明については、「SD-WAN について (620 ページ)」を参照してください。

「**SD-WAN グループ**」ページには、最適化された回復力のあるトラフィック フローに使用されるインターフェースの個別プールが表示されます。

名前 SD-WAN グループの名前。

ゾーン インターフェース メンバーのゾーン:

- WAN
- VPN

IP アドレス インターフェースの IP アドレス。

リンク状況 リンクの状態を示します:

- **リンク アップ** (緑)
- **リンク ダウン** (赤)

優先順位 グループ内のインターフェースの優先順位。

設定 グループの「**編集**」アイコンと「**削除**」アイコンがあります。

SD-WAN グループの作成

要件に合わせて複数の SD-WAN グループを作成できます。

SD-WAN グループを追加するには:

1 「**管理 | システム セットアップ > SD-WAN > SD-WAN グループ**」に移動します。SD-WAN グループのインターフェース設定オプションとして含まれている番号なしトンネル インターフェースに注意してください。

2 **追加**アイコンを選択します。「**SD-WAN グループの追加**」ダイアログが表示されます。

3 「**名前**」フィールドにわかりやすい名前を入力します。

4 「**グループ メンバー以下から選択**」リストから、1 つ以上のインターフェースを選択します。メンバー インターフェースとすることができるのは、WAN、番号付き、または番号なしのトンネル インターフェースのみです。

ⓘ **重要**：インターフェースを複数の SD-WAN グループのメンバーにすることはできません。

5 **右矢印**をクリックして、選択したインターフェースを「**選択済みインターフェース順序**」列に移動します。

6 選択したグループ メンバーの優先順位を変更するには、以下の手順に従います。

a インターフェースを選択します。

b **上矢印**または**下矢印**を選択します。

7 優先順位を付けるには、インターフェースごとに「ステップ 6」を繰り返します。

8 「**OK**」を選択します。

SD-WAN グループの編集

SD-WAN グループを編集するには:

1 「**管理 | システム セットアップ > SD-WAN > SD-WAN グループ**」に移動します。

2 編集するグループの「**編集**」アイコンを選択します。「**SD-WAN グループの編集**」ダイアログが表示されます。これは、「**SD-WAN グループの追加**」ダイアログと同じです。

3 「SD-WAN グループの作成 (622 ページ)」の説明に従って変更を加えます。

4 「**OK**」を選択します。

SD-WAN グループの削除

1 つ、複数、またはすべての SD-WAN グループを削除できます。

トピック:

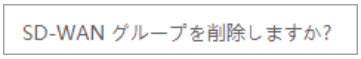
- 特定の SD-WAN グループの削除 (623 ページ)
- 複数の SD-WAN グループの削除 (623 ページ)
- すべての SD-WAN グループの削除 (624 ページ)

特定の SD-WAN グループの削除

特定の SD-WAN グループを削除するには:

1 「**管理 | システム セットアップ > SD-WAN > SD-WAN グループ**」に移動します。

2 削除するグループの「**削除**」アイコンを選択します。確認メッセージが表示されます。



3 「**OK**」を選択します。

複数の SD-WAN グループの削除

複数の SD-WAN グループを削除するには:

1 「**管理 | システム セットアップ > SD-WAN > SD-WAN グループ**」に移動します。

2 削除するグループを選択します。

3 「**SD-WAN グループ**」テーブルの上にある「**削除**」から、「**選択項目の削除**」を選択します。

確認メッセージが表示されます。

4 「**OK**」を選択します。

すべての SD-WAN グループの削除

すべての SD-WAN グループを削除するには:

1 「**管理 | システム セットアップ > SD-WAN > SD-WAN グループ**」に移動します。

2 「**SD-WAN グループ**」テーブルのヘッダーにあるチェックボックスをオンにします。すべてのグループが選択されます。

3 「**SD-WAN グループ**」テーブルの上にある「**削除**」から、「**すべて削除**」を選択します。

確認メッセージが表示されます。

4 「**OK**」を選択します。

33

性能監視の設定

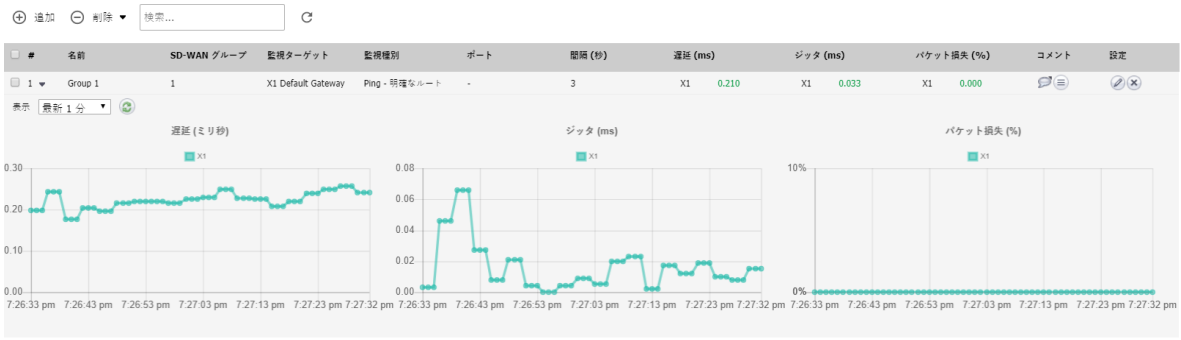
トピック:

- 性能監視について (625 ページ)
- 性能監視の設定 (627 ページ)

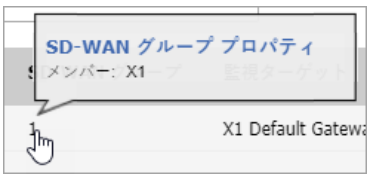
性能監視について

ネットワーク パスの性能メトリックは、SD-WAN 性能監視を使用して決定されます。これは、ネットワーク監視と似ています。SonicOS は ICMP および TCP 監視種別をサポートしています。SD-WAN 性能監視は、複数のパス選択プロファイルで使用できます (詳細については、「パス選択プロファイルの設定 (636 ページ)」を参照してください。SonicOS SD-WAN とその機能の説明については、「SD-WAN について (620 ページ)」を参照してください)。

「**管理 | システム セットアップ > SD-WAN > 性能監視**」ページには、SD-WAN グループ内の各パス (インターフェース) の動的な性能データ (遅延/ジッタ/パケット損失) と監視状況が表とグラフで表示されます。最新 1 分 (既定値)、最新 1 日、最新 1 週、または最新 1 月のデータを表示することができます。



#	監視の番号。「**折りたたみ/展開**」アイコンは、グラフの表示を切り替えます。
名前	SD-WAN 性能監視の名前。
SD-WAN グループ	SD-WAN 性能監視に関連付けられている SD-WAN グループの名前。この項目にマウス カーソルを合わせると、SD-WAN グループに関するプロパティが表示されます。



監視ターゲット SD-WAN 性能監視のターゲット アドレス オブジェクト。この項目にマウス カーソルを合わせると、ホスト アドレスが表示されます。

監視種別 性能監視の種別:

- **Ping - 明示的なルート**
- **TCP - 明示的なルート**

メモ: 「**TCP - 明示的ルート**」を「**RST 応答を未応答としてカウントする**」フィールドとともに選択すると、「**ポート**」フィールドも使用可能になります。

ポート SD-WAN 性能監視のポート。指定できる値は、1 (最小) ～65535 (最大) です。

メモ：ポートは、監視種別として「**TCP - 明示的ルート**」を選択した場合にのみ表示されます。監視種別が「**Ping - 明示的なルート**」の場合は、ハイフン (-) が表示されます。

間隔 (秒) SD-WAN 性能監視の間の時間間隔 (秒単位)。

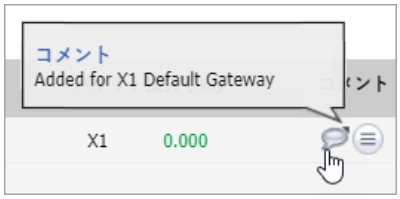
遅延 (ms) 特定のパス/インターフェースを介して送信されたプローブが、監視ターゲットに到達して確認応答が返されるまでの往復の時間 (ミリ秒単位)。これは、「**性能監視**」テーブルの監視項目の下にグラフで表示されます。

ジッタ (ms) 特定のパス/インターフェースを介したプローブに関する遅延測定値の変動 (ミリ秒単位)。これは、「**性能監視**」テーブルの監視項目の下にグラフで表示されます。

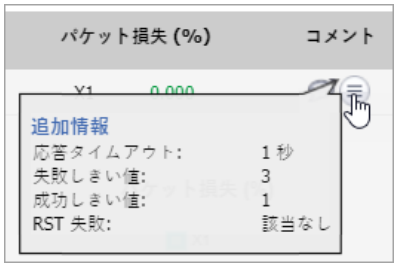
パケット損失 (%) 特定のパス/インターフェースを介して送信されたプローブに対する欠落したプローブの割合。これは、「**性能監視**」テーブルの監視項目の下にグラフで表示されます。

コメント 表示内容:

- 「**コメント**」アイコン。このアイコンにマウス　カーソルを合わせると、性能監視の設定時に入力したコメントが表示されます。



- 「**補足**」アイコン。このアイコンにマウス　カーソルを合わせると、性能監視に関する統計が表示されます。



  - **応答タイムアウト**: 応答に対する最大待ち時間。
  - **失敗しきい値**: 監視状態が「休止中」と設定されるまで無応答回数。
  - **成功しきい値**: 監視状態が「稼働中」と設定されるまでの応答回数。
  - **RST 失敗**: 監視種別が「**TCP - 明示的ルート**」の場合、RST 応答を失敗としてカウントするかどうか。

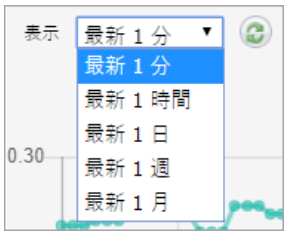
設定

SD-WAN 性能監視の「**編集**」アイコンと「**削除**」アイコンを表示します。

メモ：これらのアイコンは、自動的に追加されるプローブ (番号付けされたトンネル インターフェースが含まれている SD-WAN グループ用のプローブなど) では、グレーアウトされています。これらのプローブは、SD-WAN グループが削除されると自動的に削除されます。

表示

グラフ データの表示間隔を制御します。



既定値は「**最新 1 分**」です。

グラフ

グラフで表現された柱状データ:

- **遅延 (ミリ秒)**
- **ジッタ (ms)**
- **パケット損失 (%)**

ヒント：性能監視ごとにグラフの表示を切り替えるには、プローブ番号の横にある「**折りたたみ/展開**」アイコンを選択します。

ヒント：これらのグラフには、「**表示**」ドロップダウン メニューで指定した期間についての履歴データのスナップショットが表示されます。「**監視 | 装置の健全性 > SD-WAN 監視**」および「**管理 | システム セットアップ > SD-WAN > SD-WAN 監視**」ページのグラフは、動的なリアルタイム データを表示します。**SD-WAN 監視** グラフの詳細については、『*SonicOS 6.5 監視*』または「SD-WAN の監視 (647 ページ)」を参照してください。

SD-WAN 性能監視を設定すると、「ネットワーク監視ポリシー」画面の SD-WAN グループで使用されるインターフェースごとに既定の行が作成されます。

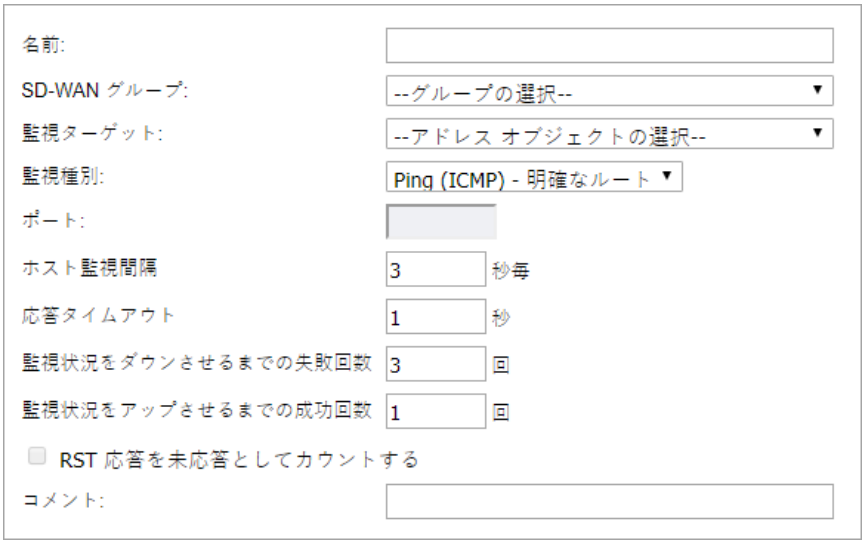
性能監視の設定

重要：SD-WAN グループに VPN 番号付きトンネル インターフェースが含まれている場合は、性能監視が自動的に作成されます。追加の性能監視を作成する必要はありません。

VPN 以外の SD-WAN グループに対して性能監視を追加するには:

1 「**管理 | システム セットアップ > SD-WAN > 性能監視**」に移動します。

2 **追加**アイコンを選択します。「**SD-WAN 性能監視の追加**」ダイアログが表示されます。



3 「**名前**」フィールドにわかりやすい名前を入力します。

4 「**SD-WAN グループ**」から SD-WAN グループを選択します。

5 「**監視ターゲット**」からアドレス オブジェクトを選択します。

6 「**監視種別**」から、以下を選択します。

- **Ping (ICMP) - 明確なルート** (既定)。「ステップ 8」に進みます。
- **TCP - 明確なルート**。「**ポート**」フィールドが利用可能になります。

7 明確なルートのポート番号を「**ポート**」フィールドに入力します。

8 「**ホスト監視間隔**」フィールドに監視の時間間隔を入力します。最小値は 1 秒、最大値は 3600 秒、既定値は **3** 秒です。

ⓘ | **ヒント**：監視間隔は応答タイムアウトより長くなければなりません。

9 「**応答タイムアウト**」フィールドに、応答の最大遅延を入力します。最小値は 1 秒、最大値は 60 秒、既定値は **1** 秒です。

10 「**監視状況をダウンさせるまでの失敗回数**」フィールドに、性能監視が「休止中」と設定されるまでの無応答回数の最大数を入力します。最小値は 1、最大値は 100、既定値は **3** です。

11 「**監視状況をアップさせるまでの成功回数**」フィールドに、性能監視が「稼働中」と設定されるまでの応答回数の最大数を入力します。最小値は 1、最大値は 100、既定値は **1** です。

12 「**監視種別**」で「**TCP - 明確なルート**」を選択した場合は、「**RST 応答を未応答としてカウントする**」オプションが使用可能になります。RST 応答を欠落間隔としてカウントするオプションを選択してください。このオプションは、既定では選択されていません。

13 必要に応じて、「**コメント**」フィールドにコメントを入力します。

14 「**追加**」を選択します。

15 さらにプローブを追加するには、「ステップ 14」から「ステップ 3」を繰り返します。

16 「**閉じる**」を選択します。

SD-WAN 性能監視の編集

SD-WAN 性能監視を編集するには:

1 「**管理 | システム セットアップ > SD-WAN > 性能監視**」に移動します。

2 編集する性能監視の「**編集**」アイコンを選択します。「**SD-WAN 性能監視の編集**」ダイアログが表示されます。これは、「**SD-WAN 性能監視の追加**」ダイアログと同じです。

3 「性能監視の設定 (627 ページ)」の説明に従って変更を加えます。

4 「**OK**」を選択します。

SD-WAN 性能監視の削除

1 つ、複数、またはすべての SD-WAN 性能監視を削除できます。

トピック:

- 特定の性能監視の削除 (629 ページ)
- 複数の性能監視の削除 (629 ページ)
- すべての性能監視の削除 (630 ページ)

特定の性能監視の削除

特定の SD-WAN 性能監視を削除するには:

1 「**管理 | システム セットアップ > SD-WAN > 性能監視**」に移動します。

2 削除する性能監視の「**削除**」アイコンを選択します。確認メッセージが表示されます。

3 「**OK**」を選択します。

複数の性能監視の削除

複数の SD-WAN 性能監視を削除するには:

1 「**管理 | システム セットアップ > SD-WAN > 性能監視**」に移動します。

2 削除する性能監視を選択します。

3 「**SD-WAN 性能監視**」テーブルの上にある「**削除**」から、「**選択項目の削除**」を選択します。

確認メッセージが表示されます。

4 「**OK**」を選択します。

すべての性能監視の削除

すべての SD-WAN 性能監視を削除するには:

1 「**管理 | システム セットアップ > SD-WAN > 性能監視**」に移動します。

2 「**SD-WAN 性能監視**」テーブルのヘッダーにあるチェックボックスをオンにします。すべての性能監視が選択されます。

3 「**SD-WAN 性能監視**」テーブルの上にある「**削除**」から、「**すべて削除**」を選択します。

確認メッセージが表示されます。

4 「**OK**」を選択します。

34

性能クラス オブジェクトの設定

トピック:

- 性能クラス オブジェクトについて (631 ページ)
- 性能クラス オブジェクトの設定 (632 ページ)
- 性能クラス オブジェクトの編集 (633 ページ)
- SD-WAN 性能クラス オブジェクトの削除 (634 ページ)

性能クラス オブジェクトについて

性能クラスは、最適なパスを選択するための性能基準を指定します。以下の指定が可能です。

- 既存のパス間で最小の遅延/ジッタ/パケット損失。
- 遅延、ジッタ、およびパケット損失のメトリックしきい値を定義する性能クラス オブジェクト。

SD-WAN 性能クラス オブジェクトを使用して、アプリケーション/トラフィック カテゴリに必要な性能特性を設定します。これらのオブジェクトは、パス選択プロファイルでこれらのメトリックに基づいてパスの選択を自動化するために使用されます。(SonicOS SD-WAN とその機能の説明については、「SD-WAN について (620 ページ)」を参照してください。)

これらは既定の性能クラス オブジェクトです。

- **最小ジッタ**
- **最小遅延**
- **最小パケット損失**

メモ：これらの既定の性能クラス オブジェクトは、編集も削除もできません。

性能クラス オブジェクトを使用して、アプリケーション/トラフィック カテゴリのニーズに最も適した個別性能しきい値を設定します。

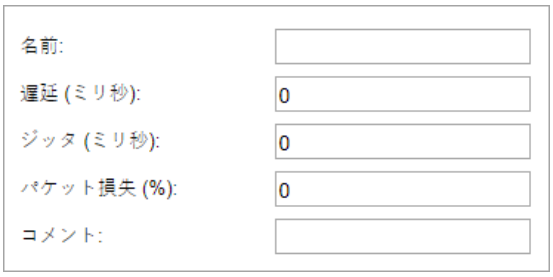
名前	性能クラス オブジェクトの名前
遅延 (ms)	特定のパス/インターフェースを介して送信されたプローブが、監視ターゲットに到達して確認応答が返されるまでの往復の時間のしきい値 (ミリ秒単位)。「**最小遅延**」性能クラス オブジェクトでは、この時間は常に「**最低**」となります。その他の既定の性能クラス オブジェクトでは、ハイフン (-) が表示されます。
ジッタ (ms)	特定のパス/インターフェースを介したプローブに関する遅延測定値の変動しきい値 (ミリ秒単位)。「**最小ジッタ**」性能クラス オブジェクトでは、この時間は常に「**最低**」となります。その他の既定の性能クラス オブジェクトでは、ハイフン (-) が表示されます。
損失 (%)	特定のパス/インターフェースを介して送信されたプローブに対する欠落したプローブの割合を示すしきい値。「**最小パケット損失**」性能クラス オブジェクトでは、この時間は常に「**最低**」となります。その他の既定の性能クラス オブジェクトでは、ハイフン (-) が表示されます。
コメント	「**コメント**」アイコンを表示します。このアイコンにマウス カーソルを合わせると、性能クラス オブジェクトの設定時に入力したコメントが表示されます。 **メモ：** 既定の性能クラス オブジェクトの「**コメント**」アイコンにマウス カーソルを合わせたときのコメントは次と同じです。 
設定	SD-WAN 性能クラス オブジェクトの「**編集**」アイコンと「**削除**」アイコンを表示します。 **メモ：** 既定の性能クラス オブジェクトを編集または削除することはできません。これらのアイコンはグレーアウトされています。
合計	「**性能クラス オブジェクト**」テーブル内の性能クラス オブジェクトの総数を表示します。

性能クラス オブジェクトの設定

性能クラス オブジェクトを追加するには:

1 「**管理 | システム セットアップ > SD-WAN > 性能クラス オブジェクト**」に移動します。

2 **追加**アイコンを選択します。「**性能クラス オブジェクトの追加**」ダイアログが表示されます。



3 「**名前**」フィールドにわかりやすい名前を入力します。

4 「**遅延 (ミリ秒)**」フィールドに許容遅延をミリ秒単位で入力します。最小値は 0 ミリ秒、最大値は 1000、既定値は **0** です。

5 「**ジッタ (ミリ秒)** 」フィールドに許容ジッタをミリ秒単位で入力します。最小値は 0 ミリ秒、最大値は 100 ミリ秒、既定値は **0** ミリ秒です。

6 「**パケット損失 (%)**」フィールドに許容可能なパケット損失率を入力します。最小値は 0、最大値は 100、既定値は **0** です。

7 必要に応じて、「**コメント**」フィールドにコメントを入力します。

8 「**OK**」を選択します。

9 さらに性能クラス オブジェクトを設定するには、性能クラス オブジェクトごとに「ステップ 3」-「ステップ 8」を繰り返します。

10 終了したら、「**キャンセル**」を選択します。

性能クラス オブジェクトの編集

SD-WAN 性能監視を編集するには:

1 「**管理 | システム セットアップ > SD-WAN > 性能クラス オブジェクト**」に移動します。

2 編集する性能監視の「**編集**」アイコンを選択します。「**SD-WAN 性能クラス オブジェクトの編集**」ダイアログが表示されます。これは、「**SD-WAN 性能クラス オブジェクトの追加**」ダイアログと同じです。

3 「性能クラス オブジェクトの設定 (632 ページ)」の説明に従って変更を加えます。

4 「**OK**」を選択します。

SD-WAN 性能クラス オブジェクトの削除

1 つ、複数、またはすべての SD-WAN 性能クラス オブジェクトを削除できますが、既定の性能クラス オブジェクトは削除できません。

トピック:

- 特定の性能クラス オブジェクトの削除 (634 ページ)
- 複数の性能クラス オブジェクトの削除 (634 ページ)
- すべての性能クラス オブジェクトの削除 (635 ページ)

特定の性能クラス オブジェクトの削除

特定の SD-WAN 性能クラス オブジェクトを削除するには:

1 「**管理 | システム セットアップ > SD-WAN > 性能クラス オブジェクト**」に移動します。

2 削除する性能クラス オブジェクトの「**削除**」アイコンを選択します。確認メッセージが表示されます。

3 「**OK**」を選択します。

複数の性能クラス オブジェクトの削除

複数の SD-WAN 性能クラス オブジェクトを削除するには:

1 「**管理 | システム セットアップ > SD-WAN > 性能クラス オブジェクト**」に移動します。

2 削除する性能クラス オブジェクトを選択します。

3 「**SD-WAN 性能クラス オブジェクト**」テーブルの上にある「**削除**」から、「**選択項目の削除**」を選択します。

確認メッセージが表示されます。

4 「**OK**」を選択します。

すべての性能クラス オブジェクトの削除

すべての SD-WAN 性能クラス オブジェクトを削除するには:

1 「**管理 | システム セットアップ > SD-WAN > 性能クラス オブジェクト**」に移動します。

2 「**SD-WAN 性能クラス オブジェクト**」テーブルのヘッダーにあるチェックボックスをオンにします。すべての性能クラス オブジェクトが選択されます。

3 「**SD-WAN 性能クラス オブジェクト**」テーブルの上にある「**削除**」から、「**すべて削除**」を選択します。

確認メッセージが表示されます。

4 「**OK**」を選択します。

35

パス選択プロファイルの設定

トピック:

- パス選択プロファイルについて (636 ページ)

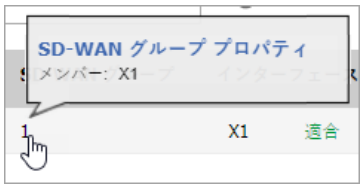
パス選択プロファイルについて

パス選択プロファイル (PSP) は、利用可能なネットワーク パス/インターフェースのプールから、特定のネットワーク性能基準を満たすネットワーク パスまたはインターフェースを決定するのに役立つ設定です。適合パスまたはインターフェースは、性能クラスの基準を満たしています。

動的パス選択メカニズムは、ポリシーベース ルート (PBR) に関連付けられた状態の PSP 設定を使用して実装されます。複数のネットワーク パスが (PSP の性能クラスに従う) 基準を満たしているとき、トラフィックは適合ネットワーク パス/インターフェース間で負荷分散されます。ポリシー ベースのルーティング ポリシーに関連付けられている場合、パス選択プロファイルは SD-WAN インターフェース間でアプリケーション/サービスに最適なパスを選択するのに役立ちます。

名前
パス選択プロファイルの名前。

SD-WAN グループ
プロファイルが適用される SD-WAN インターフェース グループ。SD-WAN グループ名にマウス カーソルを合わせると、グループのメンバーが表示されます。



インターフェース状況

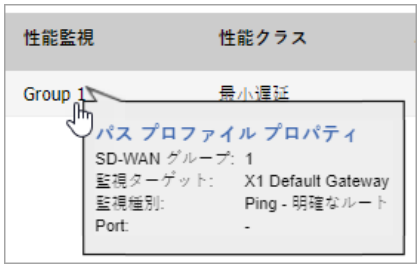
SD-WAN インターフェース グループのメンバーの状況:

- インターフェース メンバー
- メンバーの状況:
  - **適合** (緑)
  - **不適合** (赤)

この状況アイコンにマウス カーソルを合わせると、最終更新時刻のポップアップが表示されます。

性能監視

パス選択プロファイルで使用されている性能監視。性能監視の名前にマウス カーソルを合わせると、性能監視のプロパティを示すポップアップが表示されます。



- **SD-WAN グループ**: グループに関連付けられている SD-WAN インターフェース グループの名前。
- **監視ターゲット**: 監視のアドレス オブジェクト。
- **監視種別**: 監視の種別:
  - **Ping (ICMP) - 明示的なルート**
  - **TCP - 明示的なルート**
- **ポート**: 監視種別に関連付けられたポート。監視種別が「**TCP - 明示的なルート**」の場合にのみ表示されます。

性能クラス

パス選択プロファイルで使用されている性能クラス オブジェクト:

- **最小遅延**
- **最小ジッタ**
- **最小パケット損失**
- 個別性能 クラス オブジェクト

この項目にマウス カーソルを合わせると、性能クラス オブジェクトのプロパティを表示するポップアップが表示されます。

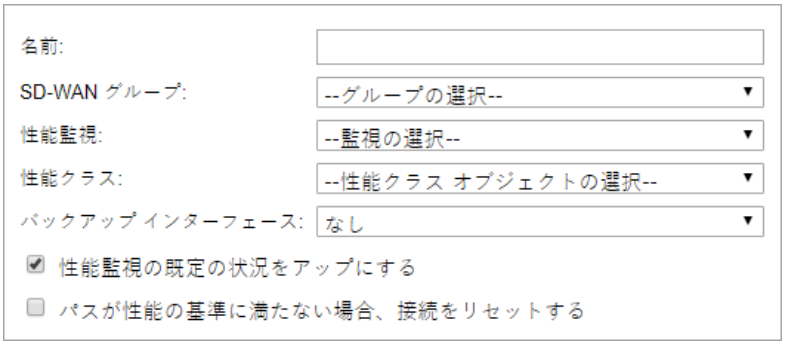
バックアップ インターフェース	SD-WAN グループのインターフェースがいずれも性能基準を満たしていないときに選択されるインターフェースを表します。バックアップ インターフェースが選択されていない場合は、「**なし**」と表示されます。
監視規定アップ	性能監視の既定の状態を表します。以下のいずれかです。 • 稼働中 (緑色のチェックマーク アイコン) • 休止中 (赤い X アイコン)
設定	パス選択プロファイルの「**編集**」アイコンと「**削除**」アイコンを表示します。

パス選択プロファイルの設定

パス選択プロファイルを追加するには:

1 「**管理 | システム セットアップ > SD-WAN > パス選択プロファイル**」に移動します。

2 **追加**アイコンを選択します。「**パス選択プロファイルの追加**」ダイアログが表示されます。



3 「**名前**」フィールドにわかりやすい名前を追加します。

4 「**SD-WAN グループ**」から、プロファイルが適用される SD-WAN インターフェース グループを選択します。

5 「**性能監視**」から、プロファイルで使用するプローブを選択します。

6 「**性能 クラス**」から、最適なネットワーク パスを動的に選択するための性能クラス オブジェクトを選択します。

- **最小遅延**
- **最小ジッタ**
- **最小パケット損失**
- 個別性能 クラス オブジェクト

7 「**バックアップ インターフェース**」から、SD-WAN グループのどのインターフェースも「**性能クラス**」で指定された性能基準を満たしていないか、すべてのインターフェースが休止中である場合に使用するインターフェースを選択します。

- **なし** (既定)
- 個々のインターフェース
- VPN トンネル インターフェース (もしあれば)

8 性能監視の既定の状態を稼働中として扱うかどうかを指定するには、「**性能監視の既定の状況をアップにする**」を選択します。このオプションが選択されていない場合、性能監視は休止中として扱われます。このオプションは、既定では選択されています。

9 VPN 以外の SD-WAN グループを含むパス選択プロファイルで、パスが性能基準を満たさなくなったときにパス上の既存の接続を休止する場合は、「**パスが性能の基準に満たない場合、接続をリセットする**」を選択します。このオプションは、既定では選択されていません。

10 「**追加**」を選択します。

11 さらにパス選択プロファイルを追加するには、追加プロファイルごとに「ステップ 3」から「ステップ 10」を繰り返します。

12 「**閉じる**」を選択します。

パス選択プロファイルの編集

SD-WAN パス選択プロファイルを編集するには:

1 「**管理 | システム セットアップ > SD-WAN > パス選択プロファイル**」に移動します。

2 編集するパス選択プロファイルの「**編集**」アイコンを選択します。「**SD-WAN パス選択プロファイルの編集**」ダイアログが表示されます。これは、「**SD-WAN パス選択プロファイルの追加**」ダイアログと同じです。

3 「パス選択プロファイルの設定 (638 ページ)」の説明に従って変更を加えます。

4 「**OK**」を選択します。

SD-WAN パス選択プロファイルの削除

1 つ、複数、またはすべての SD-WAN パス選択プロファイルを削除できます。

トピック:

- パス選択プロファイルの削除 (639 ページ)
- 複数のパス選択プロファイルの削除 (640 ページ)
- すべてのパス選択プロファイルの削除 (640 ページ)

パス選択プロファイルの削除

SD-WAN パス選択プロファイルを削除するには:

1 「**管理 | システム セットアップ > SD-WAN > パス選択プロファイル**」に移動します。

2 削除する性能クラス オブジェクトの「**削除**」アイコンを選択します。確認メッセージが表示されます。

3 「**OK**」を選択します。

複数のパス選択プロファイルの削除

複数の SD-WAN パス選択プロファイルを削除するには:

1 「**管理 | システム セットアップ > SD-WAN > パス選択プロファイル**」に移動します。

2 削除するパス選択プロファイルを選択します。

3 「**SD-WAN パス選択プロファイル**」テーブルの上にある「**削除**」から、「**選択項目の削除**」を選択します。

確認メッセージが表示されます。

4 「**OK**」を選択します。

すべてのパス選択プロファイルの削除

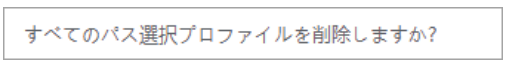
すべての SD-WAN パス選択プロファイルを削除するには:

1 「**管理 | システム セットアップ > SD-WAN > パス選択プロファイル**」に移動します。

2 「**SD-WAN パス選択プロファイル**」テーブルのヘッダーにあるチェックボックスを選択します。すべてのパス選択プロファイルが選択されます。

3 「**SD-WAN パス選択プロファイル**」テーブルの上にある「**削除**」から、「**すべて削除**」を選択します。

確認メッセージが表示されます。



4 「**OK**」を選択します。

36

SD-WAN ルート ポリシーの設定

ヒント：SD-WAN 以外のネットワーク ルーティングおよびポリシーについては、「ルート通知とルート ポリシーの設定 (486 ページ)」を参照してください。

トピック:

- SD-WAN ルート ポリシーについて (641 ページ)
- SD-WAN ルート ポリシーの設定 (642 ページ)
- SD-WAN ルート ポリシーの編集 (644 ページ)
- SD-WAN ルート ポリシーの削除 (645 ページ)

SD-WAN ルート ポリシーについて

特定のトラフィックのフローに対して動的パスを選択する場合には、ポリシーベースのルートが使用されます。SD-WAN ポリシーベースのルートは、特定の送信元/送信先サービス/アプリの組み合わせでルート ポリシーを設定するために使用され、その際に対応するパス選択プロファイルによってパス選択プロファイル ベースの発信パスが動的に決定されます。パス選択プロファイルによって修飾されたパスが複数ある場合、トラフィックは修飾パス間で自動的にロードバランスされます。どのパスもパス選択プロファイルによって修飾されておらず、プロファイル内のバックアップ インターフェースが設定されていないか停止している場合、そのルートは無効になります。SonicOS SD-WAN の詳細については、「SD-WAN について (620 ページ)」を参照してください。

ヒント：SD-WAN ルーティングは、「**管理 | システム セットアップ > ネットワーク > ルーティング**」ページまたは「**管理 | システム セットアップ > SD-WAN > SD-WAN ルート ポリシー**」ページから設定できます。ただし、「**SD-WAN > SD-WAN ルート ポリシー**」ページでは、SD-WAN ルートだけが表示され、SD-WAN タイプのルートを設定することだけができます。

名前	SD-WAN ルート ポリシーの名前。IP バージョンはアイコンで示されます。この列には、ルート ポリシーが IPv4 および/または IPv6 用かどうかを示すアイコンがあります。
送信元	SD-WAN ルートの送信元アドレス オブジェクト。
送信先	SD-WAN ルートの送信先アドレス オブジェクト。
サービス	SD-WAN ルートのサービス オブジェクト。ルート ポリシーの種別として「**サービス**」ではなく「**アプリケーション**」を選択した場合は、**N/A** と表示されます。
アプリケーション	SD-WAN ルートのアプリケーションオブジェクト。ルート ポリシーの種別として「**アプリケーション**」ではなく「**サービス**」を選択した場合は、**N/A** と表示されます。
TOS/マスク	16 進の TOS および TOS マスク。これらのオプションが設定されていない場合は、**Any** と表示されます。
パス プロファイル	SD-WAN ルートのパス選択プロファイル。
インターフェース	SD-WAN ルートに関連付けられた SD-WAN インターフェース グループ。
メトリック	SD-WAN ルートに使用されるメトリック。
優先順位	ルート ポリシーの優先順位。
コメント	情報アイコン。マウス ポインタを合わせると、SD-WAN ルート ポリシーの設定時に入力したコメントが表示されます。「**コメント**」フィールドを空白のままにしておいた場合は、ポップアップで SD-WAN ルート ポリシーの名前が表示されます。
設定	ルート ポリシーの「**統計**」、「**編集**」、「**削除**」アイコンが表示されます。「**統計**」アイコンにマウス ポインタを合わせると、ルートのアクティブな接続数が表示されます。

SD-WAN ルート ポリシーの設定

SD-WAN ルート ポリシーを追加するには:

1 「**管理 | システム セットアップ > SD-WAN > SD-WAN ルート ポリシー**」に移動します。

2 **追加**アイコンを選択します。「**SD-WAN ルート ポリシーの追加**」ダイアログが表示されます。

> **重要**:「**管理 | システム セットアップ > ネットワーク > ルーティング > ルート ポリシー**」ページから SD-WAN ルートを設定するとき、「**ルート ポリシーの追加**」ダイアログで **SD-WAN ルート**を選択すると、「**SD-WAN ルート ポリシーの追加**」ダイアログのオプションと一致するようにオプションが変更されます。

メモ：「**インターフェース**」および「**インターフェースが切断されたとき、ルートを無効にします**」オプションは、SD-WAN ポリシーで編集できないため、淡色表示されています。「**インターフェース**」オプションには、関連するパス選択プロファイル (PSP) の SD-WAN グループ名が入力されているため変更できません。SD-WAN ルートのインターフェースは、SD-WAN ルートに関連付けられている PSP の一部である SD-WAN グループから選択されているため、設定できません。

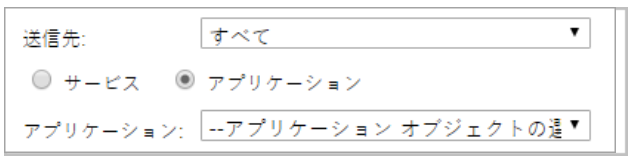
3 「**名前**」フィールドにわかりやすい名前を入力します。

4 「**送信元**」で、静的ルートの送信元アドレス オブジェクトを選択します。または、「**アドレス オブジェクトの作成**」を選択して、新しいアドレス オブジェクトを動的に作成します。既定は「**すべて**」です。

5 「**送信先**」で送信先アドレス オブジェクトを選択するか、「**アドレス オブジェクトの作成**」を選択して新しいアドレス オブジェクトを動的に作成します。既定は「**すべて**」です。

6 ルート ポリシーの種別を選択します。

- **サービス** (既定)
- **アプリケーション** -サービスが「**アプリケーション**」に切り替わります。



重要：アプリケーション ベースのルーティングには、アプリケーション制御ライセンスが必要です。

「ステップ 9」に移動します。

7 「**サービス**」で、サービス オブジェクトを選択します。すべての種類のトラフィックを許可する汎用静的ルートの場合は、単に「**すべて**」 (既定) を選択します。

8 「ステップ 10」に移動します。

9 「**アプリケーション**」から、アプリケーション オブジェクトを選択します。

10 「**パス プロファイル**」から、パス選択プロファイルを選択します。

11 「**メトリック**」にルートのメトリック (重み付けされたコスト) を入力します。最小値は 1 で、最大値は 254 です。

メトリックの詳細については、「メトリックと管理距離 (487 ページ)」および「ポリシーベース ルーティング (489 ページ)」を参照してください。

ヒント：メトリックは、低い値のほうが適切と見なされ、高いメトリック (コスト) のものよりも優先されます。

12 必要に応じて、「**コメント**」にルートのコメントを入力します。このフィールドには、新しい静的ルート ポリシーについて説明するコメントを入力できます。

13 WXA がライセンスされている場合は、「**WXA グループ**」で WXA グループを選択します。既定は「**なし**」です。

14 「**詳細設定**」を選択します。

15 「**TOS (16 進)**」フィールドに TOS 値を入力します。最大値は FF です。「**TOS (16進)**」および「**TOS マスク (16進)**」フィールドが設定されていない場合、値 0 が使用されます。TOS および TOS マスク値の詳細については、「ポリシーベース TOS ルーティング (490 ページ)」を参照してください。

16 同じ値を「**TOS マスク (16 進)**」フィールドに入力します。

17 管理距離を手動で指定するには、以下の手順に従います。

a 「**自動**」の選択を解除します。「**管理距離**」フィールドが使用可能になります。このオプションは、既定では選択されています。管理距離の詳細については、「メトリックと管理距離 (487 ページ)」を参照してください。

b 「**管理距離**」フィールドに管理距離を入力します。

18 「**OK**」を選択します。

SD-WAN ルート ポリシーの編集

SD-WAN ルート ポリシーを編集するには:

1 「**管理 | システム セットアップ > SD-WAN > SD-WAN ルート ポリシー**」に移動します。

2 編集するパス選択プロファイルの「**編集**」アイコンを選択します。「**SD-WAN ルート ポリシーの編集**」ダイアログが表示されます。これは、「**SD-WAN ルート ポリシーの追加**」ダイアログと同じです。

3 「SD-WAN ルート ポリシーの設定 (642 ページ)」の説明に従って変更を加えます。

4 「**OK**」を選択します。

SD-WAN ルート ポリシーの削除

1 つ、複数、またはすべての SD-WAN ルート ポリシーを削除できます。

トピック:

- SD-WAN ルート ポリシーの削除 (645 ページ)
- 複数の SD-WAN ルート ポリシーの削除 (645 ページ)
- すべての SD-WAN ルート ポリシーの削除 (646 ページ)

SD-WAN ルート ポリシーの削除

特定の SD-WAN ルート ポリシーを削除するには:

1 「**管理 | システム セットアップ > SD-WAN > SD-WAN ルート ポリシー**」に移動します。

2 削除する SD-WAN ルート ポリシーの「**削除**」アイコンを選択します。

複数の SD-WAN ルート ポリシーの削除

複数の SD-WAN ルート ポリシーを削除するには:

1 「**管理 | システム セットアップ > SD-WAN > SD-WAN ルート ポリシー**」に移動します。

2 削除するパス選択プロファイルを選択します。

3 「**SD-WAN パス選択プロファイル**」テーブルの上にある「**削除**」から、「**選択項目の削除**」を選択します。

確認メッセージが表示されます。

4 「**OK**」を選択します。

すべての SD-WAN ルート ポリシーの削除

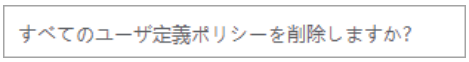
すべての SD-WAN ルート ポリシーを削除するには:

1 「**管理 | システム セットアップ > SD-WAN > SD-WAN ルート ポリシー**」に移動します。

2 「**SD-WAN ルート ポリシー**」テーブルのヘッダーにあるチェックボックスをオンにします。すべてのパス選択プロファイルが選択されます。

3 「**SD-WAN パス選択プロファイル**」テーブルの上にある「**削除**」から、「**すべて削除**」を選択します。

確認メッセージが表示されます。



4 「**OK**」を選択します。

37

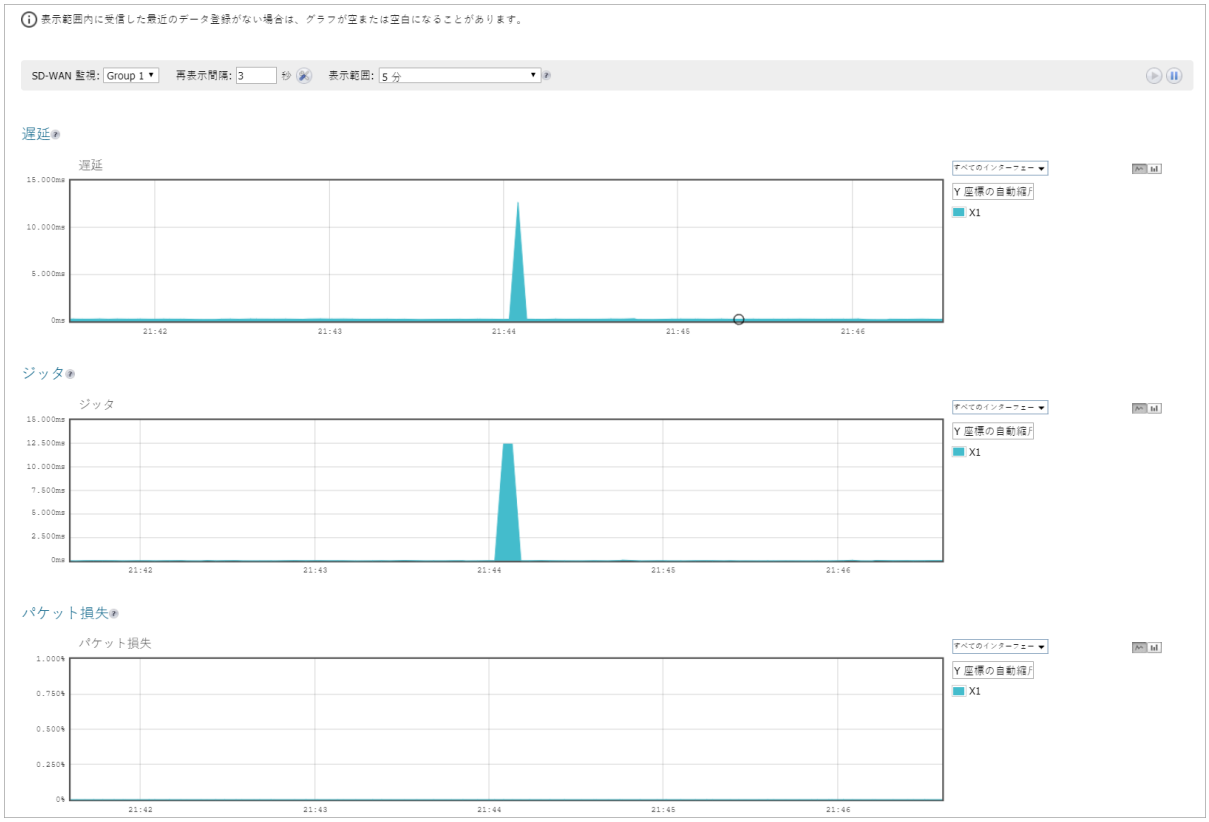
SD-WAN の監視

トピック:

- SD-WAN > SD-WAN 監視 (647 ページ)

SD-WAN > SD-WAN 監視

ヒント：これらのグラフは、「**監視 | 装置の健全性 > SD-WAN 監視**」ページでも表示できます。詳細については、『*SonicOS 6.5 監視*』を参照してください。



メモ：表示範囲内に受信した最近のデータ エントリがない場合は、グラフが空または空白になることがあります。

SD-WAN の性能を監視するには:

1 「**監視 | 装置の健全性 > SD-WAN 監視**」に移動します。

2 「**SD-WAN 監視**」から、監視に使用する性能監視を選択します。

3 「**再表示間隔:**」フィールドに再表示間隔を秒単位で指定します。

4 「**表示範囲**」を選択します。

- **60 秒**
- **2 分**
- **5 分**
- **10 分** (既定)。

5 追跡するインターフェースを選択するか、右側のドロップダウン メニューから「**すべてのインターフェース**」を選択します。

6 縮尺比率には、次のような値を入力できます。

- **自動** - Y 座標の自動縮尺
- **<num>[<unit>]** - *num* は整数です。<unit> はオプションですが、空欄、キロを表す K、メガを表す M、ギガを表す G、またはパーセンテージを表す % を指定することもできます。

  メモ：無効な値が指定された場合は、既定で Y 座標の自動縮尺に設定されます。

7 右側にある 2 つの小さなアイコンで、ライン表示とブロック表示を切り替えることができます。

38

SD-WAN ルート ポリシー接続の表示

トピック:

- SD-WAN > SD-WAN 接続ログ (649 ページ)

SD-WAN > SD-WAN 接続ログ

「**管理 | システム セットアップ > SD-WAN > SD-WAN 接続ログ**」ページでは、SD-WAN ルート ポリシーに関連付けられている接続を表示できます。SonicOS SD-WAN とその機能の詳細については、「SD-WAN について (620 ページ)」を参照してください。

ヒント：この情報は、「**調査 | ログ > SD-WAN 接続ログ**」ページでも確認できます。

送信元 MAC	接続のソースである装置の MAC アドレス。
送信元ベンダー	接続のソースである装置のベンダーの名前。
送信元 IP	接続のソースである装置の IP アドレス。
送信元ポート	接続のソースである装置のポート。
送信先 MAC	接続の宛先である装置の MAC アドレス。
送信先ベンダー	接続の宛先である装置のベンダーの名前。
送信先 IP	接続の宛先である装置の IP アドレス。
送信先ポート	接続の宛先である装置のポート。
プロトコル	接続に使用されるプロトコル。
送信元インターフェース	接続のソースである装置のインターフェース。
送信先インターフェース	接続の宛先である装置のインターフェース。
フロー種別	**FTP 制御**などの、データフロー制御の種別。
IPS 種別	IPS (Internet Provider Security) 種別。この情報が利用できないか該当しない列には、**N/A** と表示されます。
ABR アプリ ID	アプリベースのルーティング アプリケーション ID。
ABR 種別 ID	アプリベースのルーティング種別 ID。

失効 (秒)	接続が失効するまでの秒数。
送信バイト	接続で送信したバイト数。
受信バイト	接続で受信したバイト数。
送信パケット	接続で送信したパケット数。
受信パケット	接続で受信したパケット数。
消去	「**消去**」アイコンを表示します。このアイコンを選択すると、接続が消去されます。
合計	「**SD-WAN > SD-WAN 接続ログ**」ページの項目の総数。

第 5 部

システム セットアップ | スイッチング

メモ：このセクションでは、TZ 装置から Dell X シリーズ スイッチまたは N シリーズ スイッチを管理する手法とは別に、SonicOS の高度なスイッチングについて説明します。X シリーズ スイッチの管理の詳細については、「SonicOS がサポートする X シリーズ スイッチ (374 ページ)」を参照してください。

メモ：スイッチングは NSA 2650 以降およびすべての SuperMassive 装置で利用可能です。

- スイッチングについて
- VLAN トランクの設定
- レイヤ 2 発見および LLDP/LLTD の管理
- リンク統合の設定
- ポートミラーリングの設定
- シールド切り替えの設定

39

スイッチングについて

メモ：スイッチングは NSA 2650 以降およびすべての SuperMassive 装置で利用可能です。

メモ：このセクションでは、SonicWall セキュリティ装置から Dell X シリーズ スイッチまたは N シリーズ スイッチを管理する手法とは別に、SonicOS の高度なスイッチングについて説明します。X シリーズ スイッチまたは N シリーズ スイッチの管理の詳細については、「SonicOS がサポートする X シリーズ スイッチ (374 ページ)」を参照してください。

トピック:

- スイッチングについて (652 ページ)
  - スイッチングとは (652 ページ)
  - スイッチングの利点 (653 ページ)
  - スイッチングの動作 (654 ページ)
  - 用語集 (654 ページ)

スイッチングについて

トピック:

- スイッチングとは (652 ページ)
- スイッチングの利点 (653 ページ)
- スイッチングの動作 (654 ページ)
- 用語集 (654 ページ)

スイッチングとは

SonicOS は、次のスイッチング機能をサポートするレイヤ 2 (データリンク層) スイッチング機能を提供しています。

- **VLAN トランク** - 複数のスイッチ間で異なる VLAN をトランクする機能を提供します。
- **レイヤ 2 ネットワーク発見** - IEEE 802.1AB (LLDP) および Microsoft LLTD プロトコルと、スイッチ転送テーブルを使用して、ポートから見える機器を発見します。

- **リンク統合** - パフォーマンスの向上と冗長性のために、ポートをまとめる機能を提供します。

  メモ：リンク統合化は、NSA 3600 以降のセキュリティ装置でサポートされます。NSA 2600 上では、ネットワーク インターフェース用のリンク統合は、スイッチング用のリンク統合とは別の機能です。NSA 2600 は、ネットワーク インターフェース用のリンク統合はサポートしますが (「リンク統合の設定 (679 ページ)」を参照)、スイッチングをサポートしないため、スイッチング用のリンク統合をサポートしません。

- **ポート ミラーリング** - ポート グループからの受信、送信、または双方向のパケットをミラーするために、ミラーポートを割り当てることが可能になります。
- **ジャンボ フレーム** - ジャンボ フレームのサポートにより、1500～9000 バイトのペイロードを持つイーサネット フレームを処理できます。

  メモ：ジャンボ フレームは、NSA 3600 以降の装置でサポートされています。

スイッチングの利点

SonicOS は、セキュリティとスイッチングを組み合わせたソリューションを提供します。レイヤ 2 スイッチング機能は、レイヤ 2 ネットワーク内での SonicWall 機器の配備と相互運用性を強化します。

メモ：高度なスイッチングは、NSA 3600 以降の装置でサポートされています。

ネットワーク セキュリティ装置の高度なスイッチング機能は、次のような利点を提供します。

- **ポート密度の向上** - 1 つの装置に (最大 24 のスイッチ ポートを含む) 最大 26 のインターフェースが備わっているので、内部ネットワーク上の機器の数を削減できます。
- **複数のスイッチ ポート全体でのセキュリティの強化** - PortShield 手法は、すべての LAN スイッチ ポートを個別のセキュリティ ゾーン (LAN、WLAN、DMZ など) に設定できる柔軟性を備えており、WAN および DMZ からの保護だけでなく、LAN 内側の機器間でも保護を実現します。実際、各セキュリティ ゾーンには、専用の精密パケット検査ファイアウォールによって保護される、独自のワイヤスピード「ミニ スイッチ」があります。
- **VLAN トランク** - スイッチごとに VLAN 情報を設定する必要がなくなるので、VLAN の管理と設定が簡素化されます。複数のスイッチ間で異なる VLAN をトランクする機能を提供します。
- **レイヤ 2 ネットワーク発見** - 装置に接続されているすべての機器のレイヤ 2 ネットワーク情報を提供します。IEEE 802.1AB (LLDP) および Microsoft LLTD プロトコルと、スイッチ転送テーブルを使用して、ポートから見える機器を発見します。
- **リンク統合** - 統合ポートは、統合をサポートしているスイッチへの接続時には、負荷分散によるパフォーマンスの向上を、統合をサポートしているスイッチまたはサーバへの接続時には、冗長化を実現します。
- **ポート ミラーリング** - 1 つ以上のポートでネットワーク トラフィックの監視と検査を容易に行い、ポート グループからの受信、送信、または双方向のパケットをミラーするために、ミラーポートを割り当てることが可能です。
- **ジャンボ フレーム** - SonicOS で 1500～9000 バイトのペイロードを持つイーサネット フレームを処理できるようにすることで、スループットを向上させ、処理するイーサネット フレームの数を減らします。スループットの向上が見られない場合もありますが、パケットのサイズが非常に大きい場合は一定の効果があります。

  メモ：ジャンボ フレームは、NSA 3600 以降の装置でサポートされています。

スイッチングの動作

一部のスイッチング機能は、PortShield グループに対して作用し、「**ネットワーク > PortShield グループ**」ページでの事前設定を必要とします。また、既存の「**ネットワーク > インターフェース**」設定において作用するものもあります。SonicOS におけるこうした関連機能の設定の詳細については、以下を参照してください。

- インターフェースの設定 (278 ページ)
- PortShield インターフェースの設定 (373 ページ)

各スイッチング機能の動作の詳細については、以下を参照してください。

- VLAN トランクの設定 (656 ページ)
- レイヤ 2 発見および LLDP/LLTD の管理 (663 ページ)
- リンク統合の設定 (679 ページ)
- ポート ミラーリングの設定 (685 ページ)

用語集

BPDU Bridge Protocol Data Unit - BPDU は、ブリッジ ID とルート経路コストに関する情報を交換するために、RSTP で使用される、特殊なデータ フレームです。BPDU の交換は、スイッチがネットワーク トポロジを追跡してポート転送を開始または停止できるように、数秒ごとに行われます。

CoS Class of Service (サービス等級) - CoS (IEEE 802.1p) によって 8 種類のサービス等級が定義されています。これらのサービス等級は、802.1 ネットワークでのタグ付きフレームの使用時にイーサネット フレームに付加される IEEE 802.1Q ヘッダー内の 3 ビットの user_priority (ユーザ優先順位) フィールドで示されます。

DSCP Differentiated Services Code Point - DiffServ コード ポイントとも呼ばれる DSCP は、単純で大雑把な等級ベースのメカニズムを定義するネットワーキング手法です。このメカニズムのねらいは、ネットワーク トラフィックを分類および管理すると共に IP ネットワークでのサービス品質 (QoS) の保証を実現することにあります。1998 年に IETF が公開した RFC 2475 によって DSCP は定義されています。DSCP は IP パケットのヘッダー内に 8 ビットのフィールドを設定することで動作します。

IETF Internet Engineering Task Force (インターネット エンジニアリング タスク フォース) - IETF は、インターネット規格を策定および推進するオープンな標準化団体です。

L2 OSI レイヤ 2 (イーサネット) - OSI 7 層モデルのレイヤ 2 はデータ リンク層であり、イーサネット プロトコルはこのレイヤ上で実行されます。レイヤ 2 はネットワーク エンティティ間でのデータの転送に使用されます。

LACP Link Aggregation Control Protocol - LACP は、複数の物理ポートをまとめて 1 つの論理チャンネルを形成するための IEEE 仕様です。LACP では、接続された機器による負荷分散が可能になります。

LLDP Link Layer Discovery Protocol (IEEE 802.1AB) - LLDP は、識別情報、処理能力、相互接続の状況を伝えるためにネットワーク機器によって使用されます。こうした情報は各ホストの MIB データベースに格納され、ネットワーク トポロジを決定するために SNMP によって問い合わせることができます。この情報には、システム名、ポート名、VLAN 名、IP アドレス、システム機能 (スイッチング、ルーティング)、MAC アドレス、リンク統合などが含まれます。

LLTD	Link Layer Topology Discovery (Microsoft 規格) - LLTD は LLDP と同様の機能を備えた Microsoft 独自のプロトコルです。有線または無線ネットワーク (イーサネット 802.3 または無線 802.11) で動作します。LLTD は Windows Vista および Windows 7 に含まれており、Windows XP にもインストールできます。
PDU	Protocol Data Unit - スイッチング機能に関しては、フレームがレイヤ 2 の PDU です。フレームには、リンク レイヤ ヘッダーが含まれ、その後にパケットが続きます。
RSTP	Rapid Spanning Tree Protocol (高速スパニング ツリー プロトコル、IEEE 802.1D-2004) - RSTP は、1998 年にスパニング ツリー プロトコルの改良版として定義されたものです。トポロジ変更後のスパニング ツリーの収束が速くなっています。

40

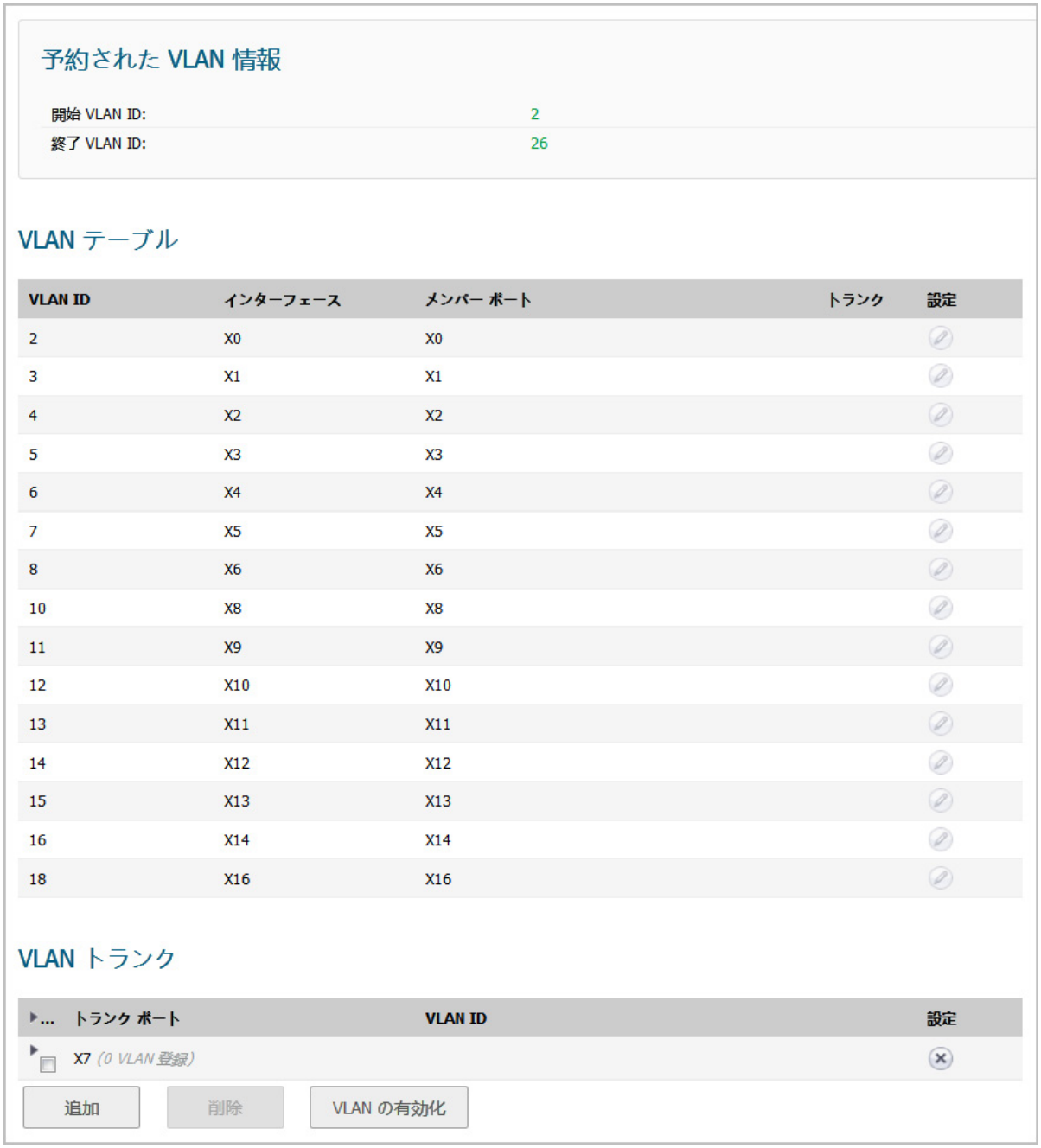
VLAN トランクの設定

メモ：スイッチングは NSA 2650 以降およびすべての SuperMassive 装置で利用可能です。

トピック:

- スイッチング > VLAN トランク (657 ページ)
  - トランクについて (658 ページ)
  - VLAN の表示 (659 ページ)
  - VLAN の編集 (660 ページ)
  - VLAN トランク ポートの追加 (661 ページ)
  - トランク ポートでの VLAN の有効化 (661 ページ)
  - VLAN トランク ポートの削除 (661 ページ)

スイッチング > VLAN トランク



トピック:

- トランクについて (658 ページ)
- VLAN の表示 (659 ページ)
- VLAN の編集 (660 ページ)
- VLAN トランク ポートの追加 (661 ページ)
- VLAN トランク ポートの削除 (661 ページ)
- トランク ポートでの VLAN の有効化 (661 ページ)

トランクについて

SonicOS の未定義のスイッチ ポートは、VLAN トランク ポートの役割を果たすことができます。トランク ポートで VLAN を有効または無効にすると、SonicOS 上の既存の VLAN をトランク ポート経由で接続されている別のスイッチ上の対応する VLAN にブリッジできます。SonicOS は、トランク ポートでの 802.1Q カプセル化をサポートしています。各トランク ポートで最大 32 個の VLAN を有効にできます。

VLAN トランク機能は、以下の機能を提供します。

- 既存の PortShield グループの VLAN ID の変更
- VLAN トランク ポートの追加と削除
- トランク ポートでの カスタム VLAN の有効化と無効化

使用できる VLAN ID の範囲は、1 ～ 4094 です。いくつかの VLAN ID は PortShield 用に予約済みであり、予約済みの範囲は「**管理 | システム セットアップ | スイッチング > VLAN トランク**」に表示されます。

特定の PortShield グループを「トランク」に設定できます。PortShield グループが破棄されている場合、トランク ポートでは関連する VLAN が自動的に無効になります。

VLAN は、PortShield グループの形でローカルに配置することも、完全にリモート VLAN 上にすることもできます。SonicOS では、PortShield グループの VLAN ID を変更できます。これにより、既存の VLAN 番号付けと容易に統合できます。

SonicOS では、アドホックな方法ではポートの VLAN メンバーシップを変更できません。ポートの VLAN メンバーシップは SonicOS 管理インターフェースの PortShield 設定によって設定する必要があります。PortShield グループの設定の詳細については、「PortShield インターフェースの設定 (373 ページ)」を参照してください。

リモート VLAN では (VLAN トランク インターフェースと呼ばれる) 仮想インターフェースが自動的に作成されます。別のトランク ポートで同じリモート VLAN が有効になっている場合、新しいインターフェースは作成されません。受信先のトランク ポートが違っても同じ VLAN タグを持つすべてのパケットは、同じ仮想インターフェースによって処理されます。これは、VLAN サブインターフェースと VLAN トランク インターフェースの主な違いです。

「**管理 | システム セットアップ | ネットワーク > インターフェース**」の「**名前**」列には、VLAN トランクの VLAN トランク インターフェースの VLAN ID が表示されます。

VLAN トランクで、ローカルまたはリモートの任意の VLAN を有効にして、別のスイッチ上の対応する 2 つの VLAN へのブリッジングを行うことができます。例えば、ローカル VLAN 345 を、2 つのリモート VLAN も有効になっているポート X2 の VLAN トランク上で有効にすることができます。

VLAN トランクは、リンク統合およびポート ミラーリングの機能と相互に作用します。VLAN トランク ポートは、ミラーリングできますが、ミラー ポート自体の役割を果たすことはできません。

VLAN トランクとして設定されたポートは、他のいかなる役割で使用することもできず、レイヤ 2 専用として予約されます。例えば、トランク ポートには IP アドレスを設定できません。

特定のトランク ポートでトランク VLAN インターフェースが設定されている場合、そのトランク ポートは、たとえ複数のトランク ポートで VLAN が有効になっていても、VLAN インターフェースが削除されるまでは削除できません。これは実装上の制限です。

VLAN の表示

トピック:

- 予約された VLAN 情報 (659 ページ)
- VLAN テーブル (659 ページ)
- VLAN トランク テーブル (660 ページ)

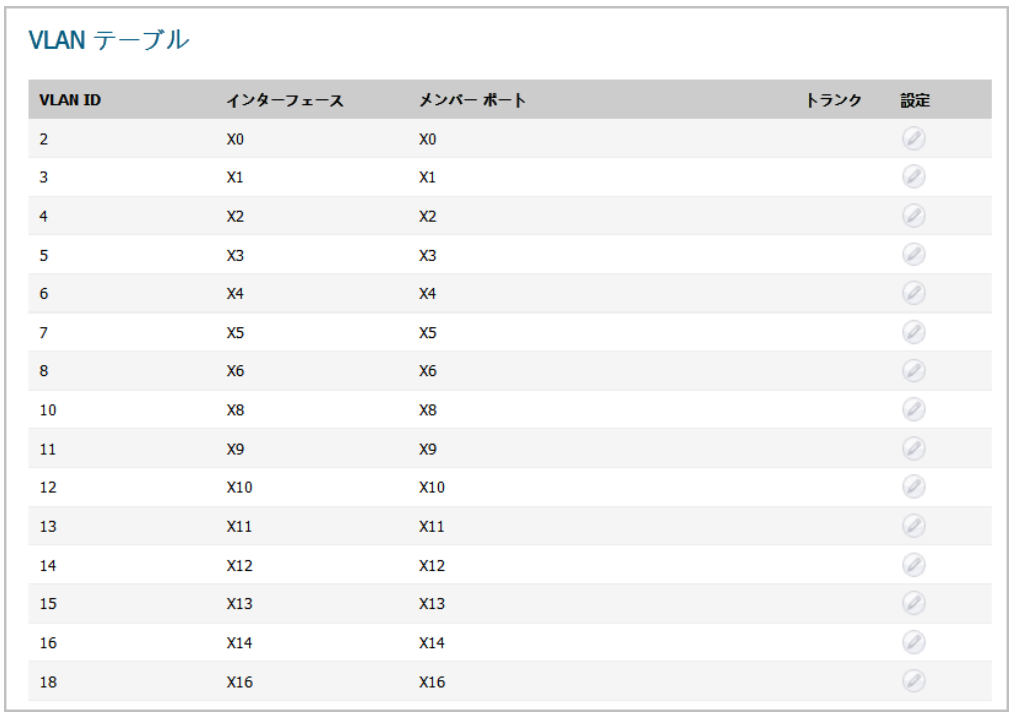
予約された VLAN 情報

「**予約された VLAN 情報**」テーブルには、予約済み VAN ID の範囲がリストされます。

- **開始 VLAN ID**
- **終了 VLAN ID**

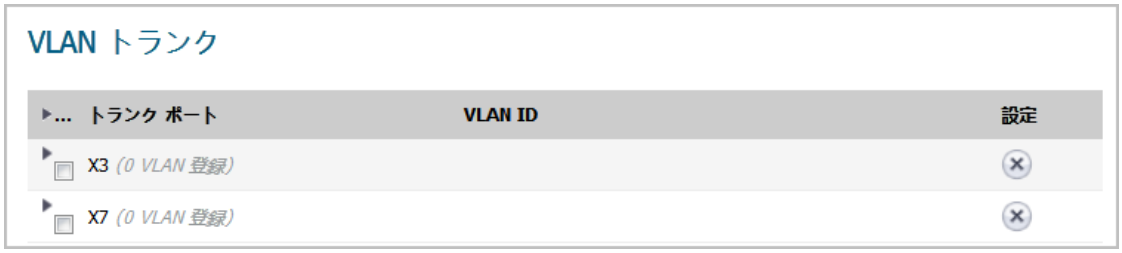
開始 VLAN ID を変更するには、「ここをクリックして設定します...」リンクを選択します。「**管理 | セキュリティ設定 > ファイアウォール設定 > 詳細設定**」ページが表示されます。詳細については、『*SonicOS 6.5 システム設定*』を参照してください。

VLAN テーブル



VLAN ID	VLAN の ID。
インターフェース	VLAN に割り当てられているインターフェース。
メンバー ポート	インターフェースに関連付けられているポート。
トランク	この VLAN がトランクされているかどうかを示します。
設定	VLAN の**編集**アイコンがあります。

VLAN トランク テーブル



トランク ポート	トランク ポートのインターフェースとそのインターフェースに関連付けられている VLAN エントリの数
VLAN ID	VLAN の ID
設定	VLAN の**削除**アイコンがあります。

トランク ポートの VLAN ID を表示するには、トランク ポートの**展開**アイコンを選択します。すべてのトランク ポートの VLAN ID を表示するには、「**VLAN トランク**」テーブルの見出しにある**展開**アイコンを選択します。VLAN ID を非表示にするには、適切な**折りたたみ**アイコンを選択します。

VLAN の編集

VLAN を編集するには、以下の手順に従います。

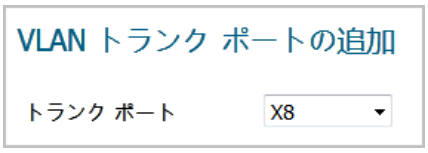
1. 「**スイッチング > VLAN トランク**」に移動します。
2. 編集する VLAN ID の「**VLAN テーブル**」行にある**設定**アイコンを選択します。「**PortShield ホスト X2 の VLAN の編集**」ダイアログが表示されます。
3. 以下のいずれかを実行します。
   - 「**VLAN ID**」フィールドに別の VLAN ID を入力します。システムで指定された元の VLAN ID と「**予約された VLAN 情報**」にある他のすべての VLAN ID を除き、任意の VLAN ID を入力できます。
   - 「**VLAN ID**」フィールドにある VLAN ID 番号を使用します。これは**設定**アイコンを選択した際の VLAN ID に一致します。
4. この VLAN でトランクを有効にするには、「**トランク**」チェックボックスをオンにします。この VLAN でトランクを無効にする場合は、このチェックボックスをオフにします。
5. 「**OK**」を選択します。

VLAN トランク ポートの追加

VLAN トランク ポートを追加するには、以下の手順に従います。

1 「**スイッチング > VLAN トランク**」に移動します。

2 「**VLAN トランク**」で、「**追加**」を選択します。「**VLAN トランク ポートの追加**」ダイアログが表示されます。



3 追加するポートを「**トランク ポート**」ドロップダウン メニューから選択します。

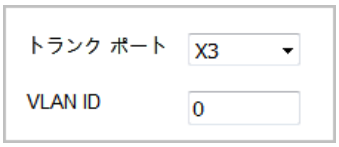
4 「**OK**」を選択します。

トランク ポートでの VLAN の有効化

特定のトランク ポートでカスタム VLAN ID を有効にするには、以下の手順を実行します。

1 「**スイッチング > VLAN トランク**」に移動します。

2 「**VLAN トランク**」テーブルで、「**VLAN の有効化**」を選択します。「**VLAN の有効化**」ダイアログが表示されます。



3 トランクされたポートを「**トランク ポート**」ドロップダウン メニューから選択します。これは「**VLAN ID**」フィールドに示されている VLAN ID のトランクに使用するポートです。

4 「**VLAN ID**」フィールドに、トランクする VLAN ID を入力します。別のスイッチの VLAN ID を入力できます。

5 「**OK**」を選択します。

VLAN トランク ポートの削除

VLAN トランク ポートは 1 つ削除することも、一度に複数のポートを削除することもできます。また、すべてのポートを削除することもできます。

VLAN トランク ポートを削除するには、以下の手順に従います。

1 「**スイッチング > VLAN トランク**」に移動します。

2 削除する VLAN トランク ポートを展開します。

3 削除する VLAN の「**設定**」列で**削除**アイコンを選択します。確認メッセージが表示されます。

4 「**OK**」を選択します。

5 削除するポートの「**設定**」列で**削除**アイコンを選択します。確認メッセージが表示されます。

6 「**OK**」を選択します。

複数の VLAN トランク ポートを削除するには、以下の手順に従います。

1 「**スイッチング > VLAN トランク**」に移動します。

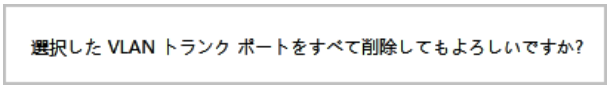
2 「**VLAN トランク**」テーブルで、削除する VLAN トランク ポートを展開します。

3 削除する各 VLAN の「**設定**」列で**削除**アイコンを選択します。確認メッセージが表示されます。

4 それぞれについて「**OK**」を選択します。

5 削除する VLAN トランク ポートの各チェックボックスをオンにします。「**削除**」が使用可能になります。

6 「**削除**」を選択します。確認メッセージが表示されます。



7 「**OK**」を選択します。

すべての VLAN トランク ポートを削除するには、以下の手順に従います。

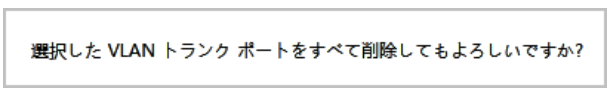
1 「**スイッチング > VLAN トランク**」に移動します。

2 「**VLAN トランク**」テーブルで、「**VLAN トランク**」テーブルの見出しにある**展開**アイコンを選択して、VLAN トランク ポートを展開します。

3 削除する各 VLAN の「**設定**」列で**削除**アイコンを選択します。確認メッセージが表示されます。

4 「**VLAN トランク**」テーブル見出しにあるチェックボックスをオンにします。「**削除**」が使用可能になります。

5 「**削除**」を選択します。確認メッセージが表示されます。



6 「**OK**」を選択します。

41

レイヤ 2 発見および LLDP/LLTD の管理

メモ：スイッチングは NSA 2650 以降およびすべての SuperMassive 装置で利用可能です。LLDP は NSA 3600 以降のセキュリティ装置でサポートされており、高可用性が有効な場合にもサポートされます。

トピック:

- スイッチング > ポート ミラーリング (663 ページ)
  - L2 発見と LLDP について (664 ページ)
  - L2 発見および LLDP/LLTD インターフェースの表示 (668 ページ)
  - LLDP プロファイルと L2 発見インターフェースの関連付け (671 ページ)
  - ページの更新 (671 ページ)
  - LLDP のグローバルな有効化/無効化 (671 ページ)
  - 近隣者の発見 (672 ページ)
- スイッチング > ポート ミラーリング > LLDP プロファイル (673 ページ)
  - LLDP プロファイルの表示 (674 ページ)
  - LLDP ユーザ定義プロファイルの追加 (676 ページ)
  - ユーザ定義 LLDP プロファイルの編集 (677 ページ)
  - ユーザ定義プロファイルの削除 (678 ページ)

スイッチング > ポート ミラーリング

トピック:

- L2 発見と LLDP について (664 ページ)
- L2 発見および LLDP/LLTD インターフェースの表示 (668 ページ)
- LLDP プロファイルと L2 発見インターフェースの関連付け (671 ページ)
- ページの更新 (671 ページ)
- LLDP のグローバルな有効化/無効化 (671 ページ)
- 近隣者の発見 (672 ページ)

L2 発見と LLDP について

近隣のデバイスとその機能を検出するために SonicWall セキュリティ装置は次のものを使用します。

- IEEE 802.1AB (LLDP: Link Layer Discovery Protocol)/Microsoft LLTD (Link Layer Topology Discovery)
- IEEE 802.3-2012 プロトコル
- スイッチ転送テーブル

レイヤ 2 で動作し、タイプ、長さ、値 (TLV) を含む一連の可変長情報の要素を含んだ LLDP プロトコル データ ユニット (LLDPDU) を近隣のデバイスとの間で交換します。情報は SNMP MIB に格納されます。これらのレイヤ 2 プロトコルを使用してネットワーキング デバイスはデバイスの ID および機能をアドバタイズします。また、有線のイーサネット ネットワークでデバイスに直接接続されたレイヤ 2 の近隣者/ピア (ブロードキャスト ドメインを越えることはない) を識別します。

これらのプロトコルの詳細については、以下を参照してください。

- https://en.wikipedia.org/wiki/Link_Layer_Topology_Discovery
- https://en.wikipedia.org/wiki/Link_Layer_Discovery_Protocol

ヒント：SonicOS では、LLDP の Transmit モードと Transmit-Receive モードがサポートされます。

- https://msdn.microsoft.com/en-us/library/windows/desktop/dn594471(v=vs.85).aspx

LLDP は、トラブルシューティングに役立ちます。特に、ping または traceroute コマンドでピアを検出できない場合に便利です。

トピック:

- サポートされている LLDP モード (664 ページ)
- TLV (Type-Length-Values: タイプ、長さ、値) (665 ページ)
- LLDP の機能に対するインターフェース リンクの影響 (667 ページ)

サポートされている LLDP モード

SonicOS では次の LLDP モードがサポートされています。

- LLDP-receive (SonicOS 6.5 の以前のバージョンで既にサポートされています)
- LLDP-transmit
- LLDP-transmit-receive
- LLDP-disabled

個々のインターフェースに対してユーザ定義 LLDP プロファイルを作成できます。

次の種類のインターフェースとモードが LLDP をサポートしています。

L2 インターフェース	物理ポートを L2 モードに設定している場合
L3 インターフェース	物理ポートを L3 モードに設定している場合
ワイヤモード インターフェース	セキュリティ保護および検査モードはワイヤモード インターフェースでサポートされますが、VLAN インターフェースではサポートされません

L2 ブリッジインターフェース	物理インターフェースでサポートされ、VLAN インターフェースではサポートされません
VLAN サブインターフェース	サポートされません
LAG/LACP	学習用に統合ポートでのみサポートされ、メンバーではサポートされません。ただし、送信用には個々のインターフェースでサポートされます。統合ポートでは、そのポート自体とメンバーの両方の近隣情報が示されます。

TLV (Type-Length-Values: タイプ、長さ、値)

個々の LLDP フレームは Chassis ID (シャーシ ID)、Port ID (ポート ID)、TTL の 3 つの必須 TLV で開始し、その後に多くのオプション TLV が続きます。LLDP フレームは、必須の End-of-frame (フレーム終了) TLV で終了します。

トピック:

- 必須 TLV (665 ページ)
- オプション TLV (666 ページ)

必須 TLV

「必須 TLV」テーブルで、送信と受信の両方に対してサポートされる必須 LLDP TLV を説明します。

必須 TLV

TLV の名前	TLV の種別	説明	SonicOS 使用法
Chassis ID (シャーシ ID) TLV	1	ファイアウォールのシャーシを識別します。各ファイアウォールは一意の Chassis ID を持つ必要があります。	SonicOS は、「Chassis ID」フィールドにセキュリティ装置の MAC アドレスを設定して送信します。MAC アドレスはセキュリティ装置のシリアル番号と同じです。
Port ID (ポート ID) TLV	2	LLDPDU がどのポートから送信されるかを識別します。セキュリティ装置は、インターフェースの `ifname` を Port ID として使用します。例えば、X1、X2、X3 といった Port ID になります。	Port ID サブタイプ 5 (インターフェースの名前) が、送信ポートを識別するために使用されます。

必須 TLV (続き)

TLV の名前	TLV の種別	説明	SonicOS 使用法
Time-to-live (生存時間) (TTL) TLV	3	ピアからの LLDPDU 情報をどれくらい長く (秒単位) 受信し、有効と見なしてローカル セキュリティ装置で保持するかを指定します (範囲は 0 ～ 65535)。値は、LLDP の Hold Time Multiplier (ホールド時間の乗数) の倍数になります。TTL 値が 0 になると、そのデバイスに関する情報は有効ではなくなり、SonicOS が、そのエントリをデータベースから削除します。	内部的に計算されます。
End of LLDPDU (LLDPDU の終了) フレームの TLV	0	LLDP イーサネット フレームにおける TLV の終了を示します。	

オプション TLV

「オプション TLV」テーブルで、送信と受信の両方に対してサポートされる、オプションの LLDP TLV を説明します。

オプション TLV

TLV の名前	TLV の種別	説明	SonicOS 使用法
ポートの説明	4	英数字形式のポートの説明。	ネットワーク インターフェース フィールドのコメント セクションに追加された値/文字列を通知 (アドバタイズ) します。
システム名	5	英数字形式のセキュリティ装置名。	「**管理 | システム セットアップ > 装置 > 基本設定**」で設定した**ファイアウォール名**を通知します。
システムの説明	6	システムのハードウェア種別、ソフトウェア オペレーティング システム、ネットワーキング ソフトウェアの完全な名前とバージョン識別子を英数字形式で示します。	このフィールドで「ファイアウォール」として通知されます。

オプション TLV (続き)

TLV の名前	TLV の種別	説明	SonicOS 使用法
システムの機能	7	このフィールドには、システムの主な機能を定義するビット割り当てが含まれます。インターフェースの配備モードが次のように記述されます。 • L3 インターフェースは、ルータ (ビット 6) 機能と「other (その他)」ビット (ビット 1) を使用して通知されます。 • L2 インターフェースは、MAC ブリッジ (ビット 3) 機能と「other (その他)」ビット (ビット 1) を使用して通知されます。 Virtual wire (仮想ワイヤ) インターフェースは、リピータ (ビット 2) 機能と「other (その他)」ビット (ビット 1) を使用して通知されます。	セキュリティ装置でサポートされている機能、および有効になっている機能を通知します。
管理アドレス	8	デバイス管理に使用される IP アドレス: • 管理 (MGT) インターフェースの IP アドレス • `interfaceLoopback` アドレスを示す IPv4 アドレス • 管理アドレス フィールドには、ユーザ定義のアドレスを指定します。管理 IP アドレスを指定しない場合、既定では、送信インターフェースの MAC アドレスが指定されます。また、指定した管理アドレスのインターフェース番号が含まれます。該当する場合、指定した管理アドレスとともにハードウェア インターフェースの OID も含まれます。1 つ以上の管理アドレスを指定すると、リストの先頭から指定した順に送信されます。 1 つの管理アドレスがサポートされています。 これはオプション パラメータのため、無効にしておくこともできます。	設定がある場合、インターフェースの管理 IP アドレスを通知します。 **メモ：** IPv6 はサポートされません。

LLDP の機能に対するインターフェース リンクの影響

LLDP はリンクが確立しているときにのみ機能します。以下のモード変更

- Receive から Transmit
- Transmit-Only から Receive-Only
- 無効化

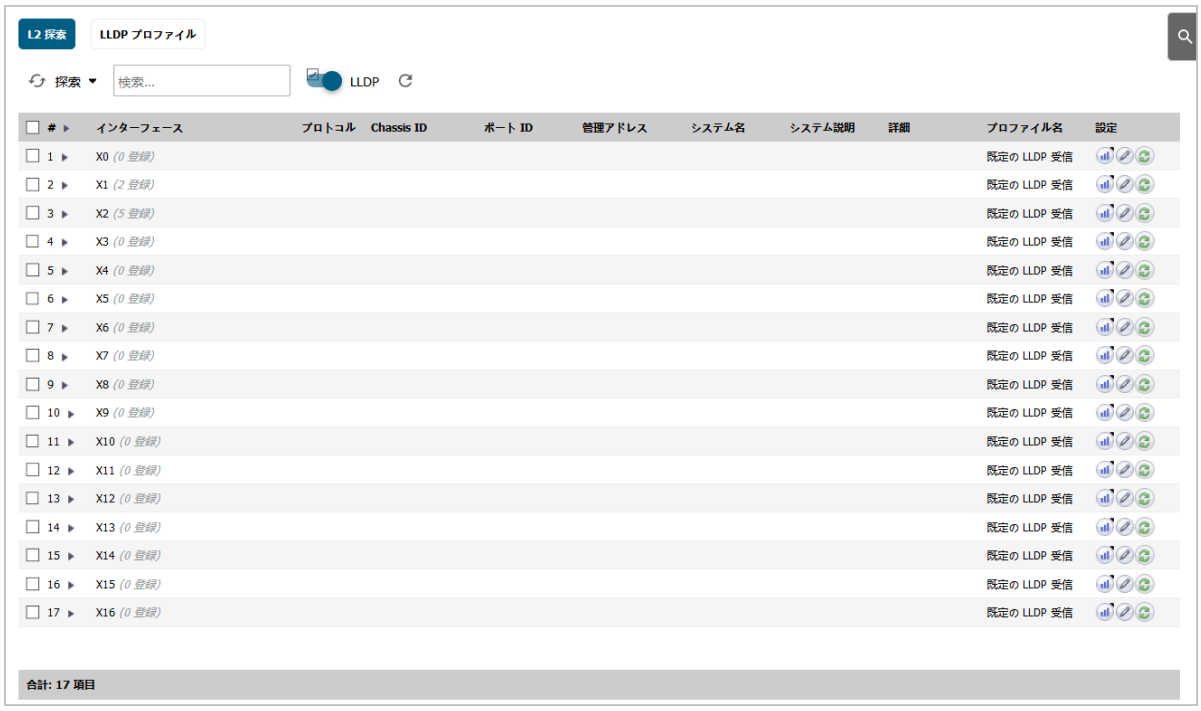
のときに、最終的な LLDP シャットダウン LLDPDU が、次の必須 TLV を指定して送信されます。

- Chassis ID (シャーシ ID) TLV

- Port ID (ポート ID) TLV
- TTL TLV
- End of LLDPDU (LLDPDU の終了) TLV

リンクがダウンすると統計カウンタはリセットされます。

L2 発見および LLDP/LLTD インターフェースの表示



インターフェース	セキュリティ装置のインターフェースを、いずれかのエントリ数とともにリストします。
プロファイル名	既定の、またはユーザ定義のプロファイルの名前。
設定	インターフェースの**統計**、**編集**、および**再表示**アイコンが含まれています。 **メモ：再表示**アイコンは、LLTD 発見のみを再表示し、LLDP 発見は再表示しません。LLDP 発見を再表示するには、「**L2 発見**」テーブルの上部にある**再表示**アイコンを選択します。

メモ：インターフェースに関する情報は「**インターフェース**」および「**プロファイル名**」列にのみ含まれ、「設定」列のアイコンはインターフェースにのみ適用されます。その他の列には、インターフェースの下にあるエントリに関する情報が表示されます。これらの列については、「ピア情報の表示 (669 ページ)」を参照してください。

トピック:

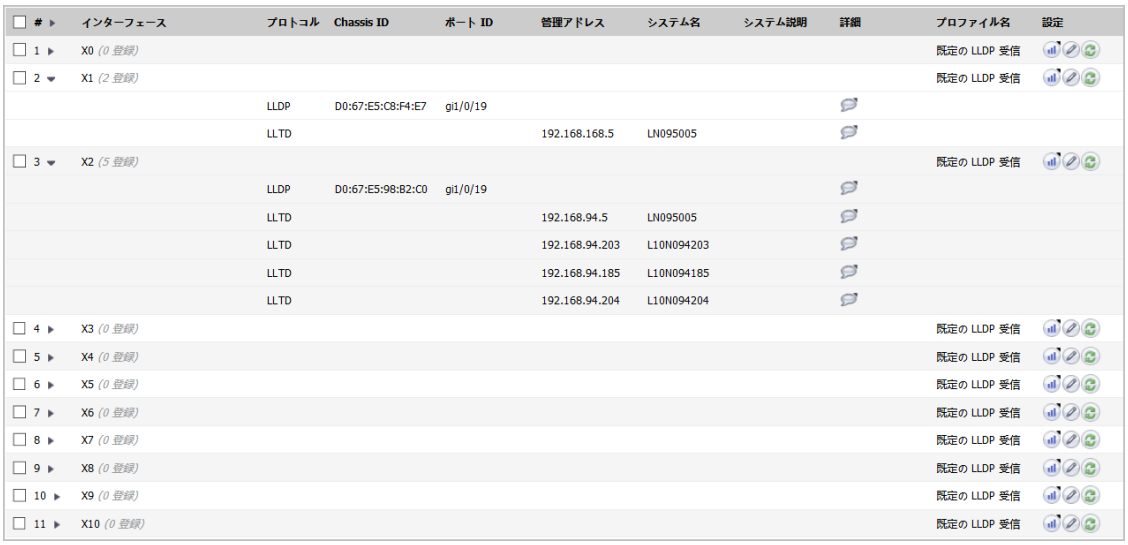
- ピア情報の表示 (669 ページ)
- 統計情報の表示 (670 ページ)
- 「L2 発見」テーブルの検索 (670 ページ)

ピア情報の表示

L2 発見情報を表示するには:

1 「**管理 | システム セットアップ > スイッチング > ポート ミラーリング**」に移動します。

2 「**L2 発見**」テーブルで、目的のインターフェースの**展開**アイコンを選択します。そのインターフェースで発見されたノード (エントリ) に関する情報が表示されます。



#	インターフェース	プロトコル	Chassis ID	ポート ID	管理アドレス	システム名	システム説明	詳細	プロファイル名	設定
1	X0 (0 登録)								既定の LLDP 受信	
2	X1 (2 登録)								既定の LLDP 受信	
		LLDP	D0:67:E5:C8:F4:E7	gi1/0/19						
		LLTD			192.168.168.5	LN095005				
3	X2 (5 登録)								既定の LLDP 受信	
		LLDP	D0:67:E5:98:B2:C0	gi1/0/19						
		LLTD			192.168.94.5	LN095005				
		LLTD			192.168.94.203	L10N094203				
		LLTD			192.168.94.185	L10N094185				
		LLTD			192.168.94.204	L10N094204				
4	X3 (0 登録)								既定の LLDP 受信	
5	X4 (0 登録)								既定の LLDP 受信	
6	X5 (0 登録)								既定の LLDP 受信	
7	X6 (0 登録)								既定の LLDP 受信	
8	X7 (0 登録)								既定の LLDP 受信	
9	X8 (0 登録)								既定の LLDP 受信	
10	X9 (0 登録)								既定の LLDP 受信	
11	X10 (0 登録)								既定の LLDP 受信	

Chassis ID セキュリティ装置のシャーシを識別します。セキュリティ装置ごとに一意の Chassis ID を 1 つだけ指定してください。これは、主にピアの MAC アドレスで構成される文字列値です。

ポート ID LLDPDU がどのポートから送信されるかを識別します。ポート名またはポート番号の文字列値です。セキュリティ装置は、インターフェースの `ifname` を Port ID として使用します。例えば、X1、X2、X3 といった Port ID になります。

管理アドレス デバイスの管理に使用されるピアの IP アドレスまたは MAC アドレスをリストします。複数の管理アドレスが返された場合は、最初のアドレスのみが表示されます。

システム名 セキュリティ装置の名前 (英数字形式)。

システム説明 セキュリティ装置のハードウェア種別、ソフトウェア オペレーティング システム、ネットワーキング ソフトウェアの完全な名前とバージョン識別子を英数字形式で示します。

詳細 追加のピア情報を表示する**情報**アイコンが含まれています。

メモ：その他の列については、「L2 発見および LLDP/LLTD インターフェースの表示 (668 ページ)」を参照してください。

3 ピア エントリの追加ピア情報を表示するには、そのピアの「**詳細**」列にある**情報**アイコンの上にマウス ポインタを置きます。ポップアップが表示されます。

MAC アドレス	ピアの MAC アドレス。
ベンダー	メイン メニューのベンダー名。
ポート説明	SonicWall セキュリティ装置のインターフェースに関する「**コメント**」フィールドにある文字列。
システム処理能力	ピア デバイスでサポートされる機能のリストを表す文字列値。

統計情報の表示

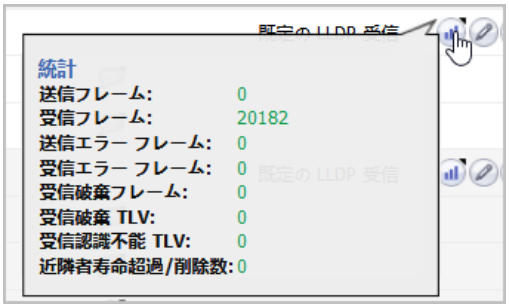
インターフェースごとに、次の値を表示できます。

- 送信フレーム数、受信フレーム数、エラー フレーム数、破棄フレーム数。
- 破棄された TLV と認識されなかった TLV。
- 寿命を越えた、または削除された近隣者。

インターフェースの統計情報を表示するには:

1 「**管理 | システム セットアップ > スイッチング > ポート ミラーリング**」に移動します。

2 「**L2 発見**」テーブルで、インターフェースの**統計**アイコンの上にマウス ポインタを置きます。「**統計**」ポップアップが表示されます。



「L2 発見」テーブルの検索

「L2 発見」テーブルに表示されるインターフェースの数を制限するには:

1 「**管理 | システム セットアップ > スイッチング > ポート ミラーリング**」に移動します。

2 「**検索**」フィールドに検索条件を入力します。表示が変更されます。

3 検索をクリアしてテーブル全体を再表示するには「**検索**」フィールドの赤い**削除**アイコンを選択します。

LLDP プロファイルと L2 発見インターフェースの関連付け

LLDP プロファイルを L2 発見インターフェースに関連付けるには:

1 「**管理 | システム セットアップ > スイッチング > ポート ミラーリング**」に移動します。

2 インターフェースの「**設定**」列で**編集**アイコンを選択します。「**インターフェース上で発見**」ダイアログが表示されます。

3 「**LLDP プロファイル**」から既定の、またはユーザ定義のプロファイルを選択します。

- **既定の LLDP 無効**
- **既定の LLDP 受信** (既定)
- **既定の LLDP 送信**
- **既定の LLDP 送受信**
- ユーザ定義プロファイル

4 「**保存**」を選択します。プロファイルの名前は、「**L2 発見**」テーブルの「**プロファイル名**」列に表示されます。

ページの更新

ページに表示されているデータを再表示するには:

1 「**L2 発見**」テーブルの上部にある**再表示**アイコンを選択します。

LLDP のグローバルな有効化/無効化

既定で、LLDP はグローバルに有効になっています。「LLDP」スイッチを切り替えることで、LLDP の送受信をグローバルで有効化または無効化できます。

LLDP をグローバルに有効化/無効化するには:

1 「**管理 | システム セットアップ > スイッチング > ポート ミラーリング**」に移動します。

2 「**L2 発見**」テーブルの上部にある「**LLDP**」を選択します。確認メッセージが表示されます。

3 「**OK**」を選択します。

近隣者の発見

次の各ケースで近隣者を発見できます。

- 単一のインターフェース。
- 複数のインターフェース。
- すべてのインターフェース。

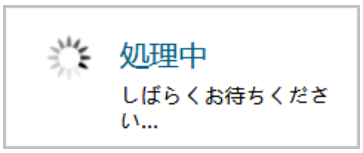
ヒント：LAG がトランク モードの場合は、すべてのポートが近隣者を検出できます。PortShield モードの LAG は、統合ポートの下でのみ近隣者を学習します。

単一のインターフェースの近隣者を検出するには:

1 「**管理 | システム セットアップ > スイッチング > ポート ミラーリング**」に移動します。

2 インターフェースの「**設定**」列にある**再表示**アイコンを選択します。

処理中であることを示すメッセージが表示されます。



インターフェースの情報が更新されます。

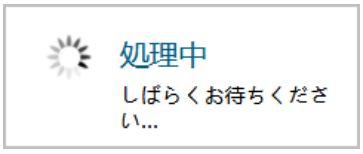
複数のインターフェースの近隣者を検出するには:

1 「**管理 | システム セットアップ > スイッチング > ポート ミラーリング**」に移動します。

2 「**L2 発見**」テーブルで目的の各インターフェースを選択します。

3 テーブルの上部にある「**探索**」から「**探索**」を選択します。このオプションは、インターフェースが選択されていなければ淡色表示になります。

処理中であることを示すメッセージが表示されます。



選択したインターフェースの情報が更新されます。

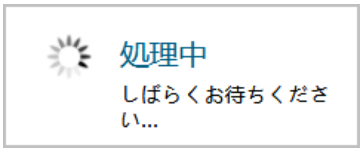
すべてのインターフェースの近隣者を検出するには:

1 「**管理 | システム セットアップ > スイッチング > ポート ミラーリング**」に移動します。

2 「**L2発見**」テーブルでいずれかのインターフェースを選択します。

3 テーブルの上部にある「**探索**」から「**すべて探索**」を選択します。

処理中であることを示すメッセージが表示されます。



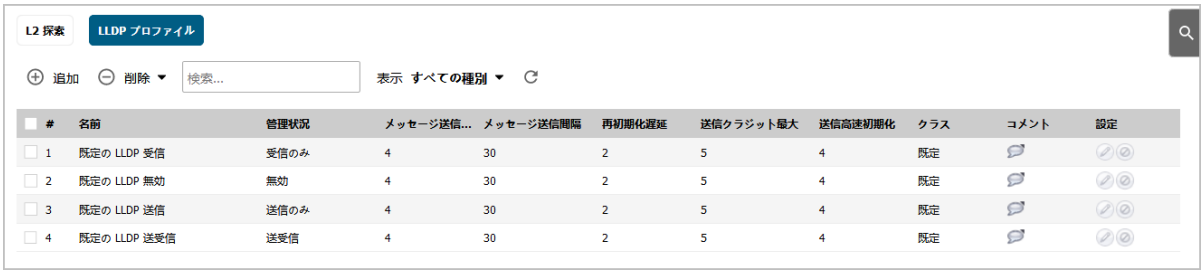
すべてのインターフェースの情報が更新されます。

スイッチング > ポート ミラーリング > LLDP プロファイル

トピック:

- LLDP プロファイルの表示 (674 ページ)
- LLDP ユーザ定義プロファイルの追加 (676 ページ)
- ユーザ定義 LLDP プロファイルの編集 (677 ページ)
- ユーザ定義プロファイルの削除 (678 ページ)

LLDP プロファイルの表示



名前	既定の、またはユーザ定義のプロファイルの名前。
管理状況	LLDP プロファイルの LLDP モード: • **無効** • **受信のみ** • **送受信** • **送信のみ**
メッセージ送信保持	LLDP プロファイルの LLDP フレーム存続時間を通常の送信間隔の何倍にするかを指定する乗数。
メッセージ送信間隔	LLDP プロファイルの通常の送信間隔 (タイマー ティック数)。
再初期化遅延	「**管理状況**」が「**無効**」になってからプロファイルの再初期化が再試行されるまでの時間を示します。
送信クレジット最大	LLDP プロファイルの最大送信クレジット。
送信高速初期化	高速送信期間中に送信される LLDPDU の数を決定します。
クラス	プロファイルの種類: • **既定** • **ユーザ定義**
コメント	この情報アイコンにマウス ポインタを置くと、次のいずれかが表示されます。 • 既定のプロファイルの **自動追加された LLDP プロファイル**。 • ユーザ定義プロファイルを追加または編集するときに指定したコメント。コメントを指定しなかった場合は何も表示されません。
設定	ユーザ定義プロファイルの**編集**アイコンと**削除**アイコンがあります。既定のプロファイルは編集も削除もできないため、アイコンは淡色表示になります。

トピック:

- 「LLDP プロファイル」テーブルの情報の再表示 (675 ページ)
- 「LLDP プロファイル」テーブルの検索 (675 ページ)
- 特定の種類の LLDP プロファイルのみを表示する (675 ページ)

「LLDP プロファイル」テーブルの情報の再表示

LLDP プロファイルの情報を再表示するには:

1 「**管理 | システム セットアップ > スイッチング > ポート ミラーリング**」に移動します。

1 **LLDP プロファイル**を選択します。

2 「**LLDP プロファイル**」テーブルの上部にある**再表示**アイコンを選択します。

「LLDP プロファイル」テーブルの検索

「LLDP プロファイル」テーブルに表示されるプロファイル数を制限するには:

1 「**管理 | システム セットアップ > スイッチング > ポート ミラーリング**」に移動します。

2 **LLDP プロファイル**を選択します。

3 「**検索**」フィールドに検索条件を入力します。表示が変更されます。

4 検索をクリアしてテーブル全体を再表示するには「**検索**」フィールドの赤い**削除**アイコンを選択します。

特定の種類の LLDP プロファイルのみを表示する

特定の種類の LLDP プロファイルのみを表示するには:

1 「**管理 | システム セットアップ > スイッチング > ポート ミラーリング**」に移動します。

2 **LLDP プロファイル**を選択します。

3 「**表示**」から、表示する LLDP プロファイルの種類を選択します。

- 「**すべてのタイプ**」（既定）
- **既定**
- **ユーザ定義**

LLDP ユーザ定義プロファイルの追加

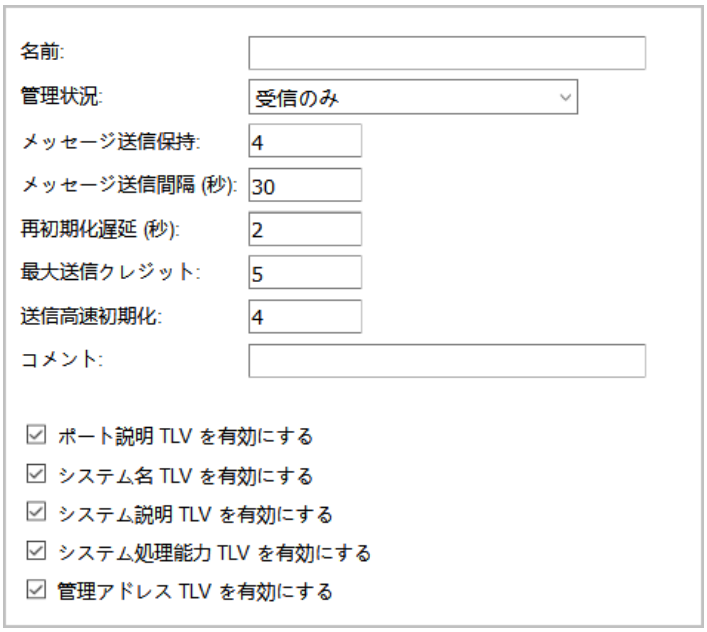
重要：既定値を変更すると、経過時間と、各サイクルの間に送信されるフレーム数が影響を受けます。

LLDP ユーザ定義プロファイルを追加するには:

1 「**管理 | システム セットアップ > スイッチング > ポート ミラーリング**」に移動します。

2 **LLDP プロファイル**を選択します。

3 「**追加**」を選択します。「**LLDP プロファイルの追加**」ダイアログが表示されます。



4 「**名前**」フィールドに、LLDP プロファイルのわかりやすい名前を入力します。

5 「**管理状況**」から、LLDP プロファイルの送信モードを選択します。

- **無効**
- **受信のみ** (既定)
- **送信のみ**
- **送受信**

6 LLDP エージェントによって送信される LLDP フレームの TTL 値をメッセージの送信間隔に基づいて決定するには、「**メッセージ送信保持**」フィールドに乗数を入力します。最小値は 1、最大値は 100、既定値は **4** です。

7 時間間隔 (通常の送信期間中の送信間隔のタイマー ティック数) を定義するには、「**メッセージ送信間隔 (秒)**」フィールドに間隔を秒単位で入力します。最小値は 1 秒、最大値は 3600 秒、既定値は **30** 秒です。

8 「管理状況」が「無効」になってからプロファイルの再初期化が再試行されるまでの時間を指定するには、「**再初期化遅延 (秒)**」フィールドに時間を秒単位で入力します。最小値は 1 秒、最大値は 10 秒、既定値および推奨値は **2** 秒です。

9 LLDP プロファイルの、いつでも送信できる LLDPDU の最大数を指定するには、「**最大送信クレジット**」フィールドに値を入力します。最小値は 1、最大値は 10、既定値は **5** です。

10 高速送信期間中に送信される LLDPDU の初期数を指定するには、「**送信高速初期化**」フィールドに値を入力します。最小値は 1、最大値は 8、既定値は **4** です。

11 必要に応じて、「**コメント**」フィールドに任意のコメントを入力します。「**LLDP プロファイル**」テーブルの「**コメント**」列にある情報アイコンの上にマウス ポインタを置くと、ここに入力する内容が表示されます。

12 LLDPDU メッセージのオプションの TLV にセキュリティ装置のポートの説明を含めるには、「**ポート説明 TLV を有効にする**」を選択します。 このオプションは、既定では選択されています。

13 LLDPDU メッセージの場合にオプションの TLV にセキュリティ装置の設定済みのファイアウォール名を含めるには、「**システム名 TLV を有効にする**」を選択します。このオプションは、既定では選択されています。

14 LLDPDU メッセージの場合にオプションの TLV のセキュリティ装置の ID として **ファイアウォール** を含めるには、「**システム説明 TLV を有効にする**」を選択します。このオプションは、既定では選択されています。

15 LLDPDU メッセージの場合にオプションの TLV のセキュリティ装置のインターフェースを管理するために使用される IPv4 または MAC アドレスを含めるには、「**管理アドレス TLV を有効にする**」を選択します。このオプションは、既定では選択されています。

16 「**OK**」を選択します。

ユーザ定義 LLDP プロファイルの編集

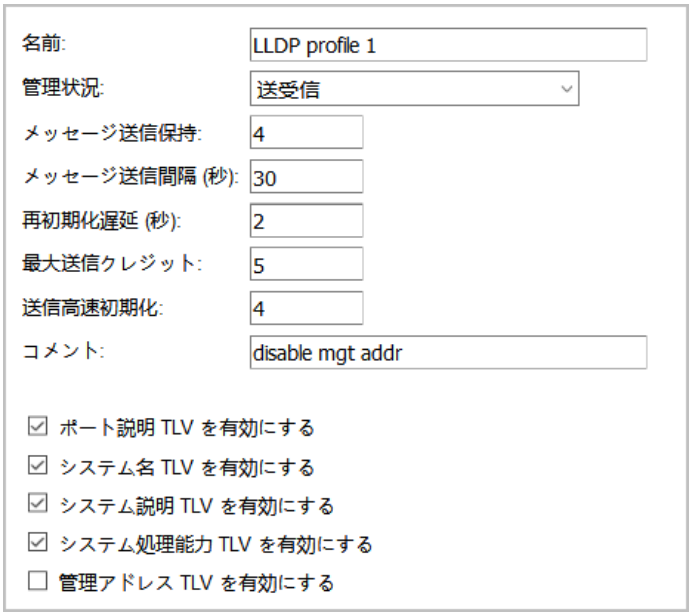
ヒント：既定の LLDP プロファイルは編集できません。

ユーザ定義 LLDP プロファイルを編集するには:

1 「**管理 | システム セットアップ > スイッチング > ポート ミラーリング**」に移動します。

2 **LLDP プロファイル**を選択します。

3 プロファイルの**編集**アイコンを選択します。「**LLDP プロファイルの編集**」ダイアログが表示されます。



4 必要に応じて変更を行います。これらのオプションについては、「LLDP ユーザ定義プロファイルの追加 (676 ページ)」を参照してください。

5 「**OK**」を選択します。

ユーザ定義プロファイルの削除

ヒント：既定のプロファイルは削除できません。

ユーザ定義プロファイルを削除するには:

1 「**管理 | システム セットアップ > スイッチング > ポート ミラーリング**」に移動します。

2 **LLDP プロファイル**を選択します。

3 プロファイルの**削除**アイコンを選択します。確認メッセージが表示されます。

4 「**OK**」を選択します。

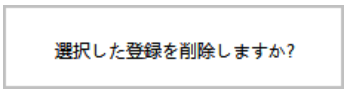
1 つ以上のユーザ定義プロファイルを削除するには:

1 「**管理 | システム セットアップ > スイッチング > ポート ミラーリング**」に移動します。

2 **LLDP プロファイル**を選択します。

3 削除するプロファイルを選択します。

4 「**削除**」から「**選択の削除**」を選択します。確認メッセージが表示されます。



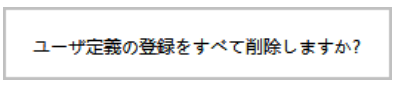
5 「**OK**」を選択します。

すべてのユーザ定義プロファイルを削除するには:

1 「**管理 | システム セットアップ > スイッチング > ポート ミラーリング**」に移動します。

2 **LLDP プロファイル**を選択します。

3 「**削除**」から「**すべて削除**」を選択します。確認メッセージが表示されます。



4 「**OK**」を選択します。

42

リンク統合の設定

メモ：スイッチングは NSA 2650 以降およびすべての SuperMassive 装置で利用可能です。

トピック:

- スイッチング > リンク統合 (679 ページ)
  - リンク統合化について (679 ページ)
  - リンク統合の表示 (682 ページ)
  - 論理リンク (LAG) の作成 (683 ページ)
  - LAG の削除 (684 ページ)

スイッチング > リンク統合

トピック:

- リンク統合化について (679 ページ)
- リンク統合の表示 (682 ページ)
- 論理リンク (LAG) の作成 (683 ページ)

リンク統合化について

メモ：リンク統合化 (LAG) は、NSA 3600 以降のファイアウォールでサポートされています。

リンク統合化は、複数のリンクを結合して、合計帯域幅の拡大が可能な 1 つのより大きな仮想パイプにするという形で、2 つ以上のリンクによる SonicWall セキュリティ装置どうしの相互接続を許可する

ことで、レイヤ 2 ネットワークでのポート冗長化と負荷分散を可能にします。2 つの機器間に複数のリンクが存在するので、あるリンクに障害が発生しても、トラフィックは中断することなく他のリンクを介して転送されます。複数のリンクが存在することで、均等な分配を実現するという方法によるトラフィックの負荷分散も可能になります。負荷分散は、送信元と送信先の MAC アドレスのペアに基づき、SonicWall セキュリティ装置によって制御されます。統合に関する情報や統計が「**スイッチング > リンク統合**」ページに表示され、それに基づいてインターフェースを設定できます。

SonicOS では次 2 つの種別の LAG をサポートしています。

- 静的 LAG (680 ページ)
- 動的 LAG (680 ページ)

静的 LAG

静的リンク統合化では、同じ VLAN (同じ PortShield グループ) 内にあるポート、または VLAN トランクポートであるポートは、リンク統合化が可能です。最大 4 つのポートを 1 つの論理グループに統合でき、4 つの論理リンク (LAG) を設定できます。静的リンク統合化では、すべての設定項目が参加する両方の LAG コンポーネントに対して設定されます。

この機能によって主な 2 つの種別の使用法が有効になります。

ファイアウォールからサーバ	同じ VLAN (同じ PortShield グループ) 内にあるポートどうしでのリンク統合を有効にすることで実現されます。この設定により、ポートの冗長化が可能になりますが、セキュリティ装置 からサーバの方向では、装置のハードウェア上の制限のために負荷分散がサポートされません。
ファイアウォールからスイッチ	VLAN トランク ポートでのリンク統合を有効にすることで可能になります。負荷分散はハードウェアによって自動的に実行されます。セキュリティ装置は、送信元と送信先の MAC アドレスのペアに基づく負荷分散アルゴリズムをサポートしています。

PortShield の設定と同様、統合されたグループを代表しているインターフェースを選択します。このポートを*統合元*と呼びます。統合元ポートには固有の鍵を割り当てる必要があります。オプションで、統合元以外のポートに鍵を設定することもできます。これは、スイッチ接続の配線が正しくない場合に LAG の誤りを回避するのに役立ちます。

メモ：鍵は LAG ID と同じものではありません。LAG ID はインターフェース番号と同じであり、変更できません。鍵は LAG グループの設定時に割り当てられている必要があります。すべての非統合元ポートは、統合元ポートと同じキーを持つ必要があります。

接続先のリンク パートナーが同じで鍵が一致するポートどうしは関連付けられます。静的なリンク統合ではリンク パートナーを発見できません。この場合、ポートは鍵のみに基づいて統合されます。

PortShield ホストと同様、統合元ポートは、システム内の LAG を代表しているので、LAG から削除できません。

メモ：リンク統合化が VLAN トランク ポートで有効になった後、LAG での VLAN の追加や削除はできなくなります。

動的 LAG

SonicOS では、高度なスイッチング機能をサポートしているすべての SonicWall セキュリティ装置で、Link Aggregation Control Protocol (IEEE 802.3ad で定義されている LACP) を使用した動的リンク統合化をサポートしています。

LACP を使用した動的 LAG について

LACP を使用すると、リンク統合化制御 PDU (Protocol Data Unit) と呼ばれるプロトコル パケット内にあるリンク統合化に関連する情報を LAG グループのメンバー間で交換できます。LACP により、設定、ワイヤリングのエラーや、リンク障害を迅速に検出できます。

スループットの向上、リンク冗長化といった LAG の 2 つの大きな利点は、LACP を使用して効率的に実現できます。LACP は LAG 内のメンバー間で使用されるシグナル プロトコルです。リンクどうしが適切に設定および結合されている場合に限り、統合してバンドル化されるようにします。LACP は次の 2 つのモードのいずれかで設定できます。

- **アクティブ モード** - ポートが稼働中になると機器は直ちに LACP PDU を送信します。

  メモ：SonicOS 6.5 は LACP のアクティブ モードのみをサポートしています。

- **パッシブ モード** - ポートはパッシブ ネゴシエート状態に置かれます。この場合、ポートは受け取った LACP PDU に応答するだけで、LACP ネゴシエーションを開始しません。

どちら側もアクティブに設定されている場合、その他のパラメータのネゴシエーションの成功を想定して LAG を形成することができます。一方の側がアクティブ、他方がパッシブに設定されている場合、アクティブ側から受け取った LACP PDU に応答するパッシブ ポートとして LAG を形成することができます。両側ともパッシブの場合、LACP はバンドルのネゴシエーションができません。パッシブ モードが配備で使用されることはまれです。

設定では、同じ LAG のすべてのメンバー ポートが同じ VLAN で統合元ポートとしてセットアップされている必要があります。LAG メンバーで受信されたデータ パケットは、VLAN を使用している親の統合元ポートと関連付けられます。LAG の統合元/メンバー ポートの状態が安定した収集/分配状態に到達すると、それらのポートはデータ トラフィックを送受信する準備が整ったことになります。

次に示す情報や、設定されている統合元ポートなど、LAG に関連するすべての情報は「**スイッチング > リンク統合**」ページに表示されます。

- LAG の一部になっているメンバー ポート。
- LAG を形成する各ポートの状況。
- LACP を介して受信したパートナーの MAC アドレス。

設定では 6 つの負荷分散オプションが使用可能です。統合元ポートを伴う LAG の作成時には、負荷分散オプションを選択しておく必要があります。

重要：LAG の作成後は、負荷分散オプションを変更できません。

LAG に対する VLAN の機能強化点

メモ：この拡張は、NSA 2600、TZ シリーズ、または SOHO W ファイアウォールではサポートされていません。

リンク統合 (LAG) を使用すると、間にある複数のリンクを束ねて 1 つの大きな仮想パイプを作るような方法で機器どうしを相互に接続し、伝送できる帯域幅を拡大することができます。2 つの機器間に複数のリンクが存在するので、あるリンクに障害が発生しても、トラフィックは中断することなく他のリンクを介して続けて転送されます。複数のリンクが存在することで、均等な分配を実現するという方法によるトラフィックの負荷分散も可能になります。

この機能強化により、次のことが達成されます。

- VLAN を追加/削除する前に、LAG を分解または削除する必要はありません。この設定により、LAG (または LAG 上で設定した他の VLAN) に関連する現在のトラフィックを中断することなく、既存の LAG に VLAN を追加したり、既存の LAG から VLAN を削除したりできます。
- VLAN は LAG の任意のメンバーに追加/削除でき、LAG の他のメンバーに明示的に追加/削除しなくても LAG の他のすべてのメンバーに自動的に適用されます。

リンク統合の表示

トピック:

- 状況の表示 (682 ページ)
- リンク統合ポートの表示 (682 ページ)

状況の表示

「**状況**」テーブルには、ファイアウォールの MAC アドレスによるシステム ID が表示されます。

リンク統合ポートの表示

リンク統合ポートを表示するには、「**システム セットアップ | スイッチング > リンク統合**」に移動します。

ポート	統合元ポートまたはメンバー ポートとして使われるインターフェース
LAG ID	システムによって設定されたリンク統合元。統合元でないポートは、それをメンバーとする統合元の LAG ID を持ちます。
鍵	「**LAG ポートの追加**」ダイアログのポート メンバーシップを示します。
統合元	統合元ポートには緑色のチェックマークが表示されます。それ以外は空白になっています。
LACP 有効	LACP が有効かどうかを示します。
状況	ポートの状況 (「**稼働中**」または「**休止中**」) を示します。

相手　物理的に接続された後のリンク パートナーの MAC アドレス。

- 静的 LAG の場合、00:00:00:00:00:00
- 動的 LAG の場合、パートナーの MAC アドレス

ベンダー　機器の製造元の名前が表示されます。

動作　以下のアイコンが表示されます。

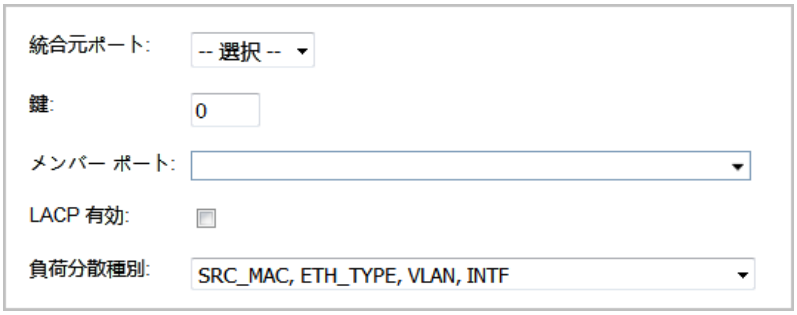
- **統計** - マウス ポインタをこの上に移動すると、**LAG ポート統計**がポップアップ表示されます。

- **編集** (統合元ポートが編集可能な場合のみ)
- **削除**

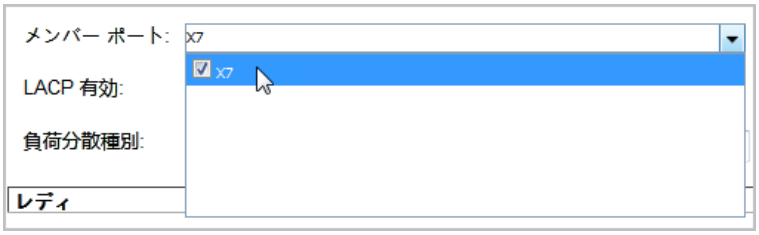
論理リンク (LAG) の作成

論理リンク(LAG) を作成するには、以下の手順に従います。

1. 「**スイッチング > リンク統合**」に移動します。
2. 「**追加**」を選択します。「**LAG ポートの追加**」ダイアログが表示されます。



3. 「**統合元ポート**」からインターフェースを選択します。
4. 適切なキーを「**鍵**」フィールドに入力することにより、LAG グループに対するポート メンバーシップを指定します。最小値は 1 で、最大値は 255 です。このフィールドには既定値の **0** が設定されており、これを必ず置き換えてください。
5. 統合するポートを「**メンバー ポート**」ドロップダウン メニューから選択します。統合する各ポートのチェックボックスをオンにすることで、リスト内の任意の数のポートを選択できます。



メモ：リストされるポートは、「ステップ 3」で選択したインターフェースによって異なります。

6 このポートで LACP (Link Aggregation Control Protocol) を有効にするには、「**LACP 有効**」を選択します。このオプションは、既定では選択されていません。

7 「**負荷分散種別**」で、負荷分散の実行方法を選択します。

重要：LAG の作成後は、負荷分散オプションを変更できません。

- SRC_MAC、ETH_TYPE、VLAN、INTF (既定)
- DST_MAC、ETH_TYPE、VLAN、INTF
- SRC_MAC、DST_MAC、ETH_TYPE、VLAN、INTF
- SRC_IP、SRC_PORT
- DST_IP、DST_PORT
- SRC_IP、SRC_PORT、DST_IP、DST_PORT

8 「**OK**」を選択します。

LAG の削除

LAG のメンバーを削除するには、以下の手順に従います。

1 「**システム セットアップ | スイッチング > リンク統合**」に移動します。

2 LAG のメンバー ポートの**削除**アイコンを選択して、そのメンバー ポートを削除します。

統合元ポートを削除するには、以下の手順に従います。

1 「**システム セットアップ | スイッチング > リンク統合**」に移動します。

2 すべてのメンバー ポートの**削除**アイコンを選択して、メンバー ポートをすべて削除します。

メモ：統合元ポートを削除する前に、すべてのメンバー ポートを LAG から削除しておく必要があります。

3 統合元ポートの**削除**アイコンを選択して、統合元ポートを削除します。

43

ポート ミラーリングの設定

メモ：スイッチングは NSA 2650 以降およびすべての SuperMassive 装置で利用可能です。

トピック:

- スイッチング > ポート ミラーリング (685 ページ)
  - ポート ミラーリングについて (686 ページ)
  - ミラーされているポートの表示 (686 ページ)
  - ポート ミラーリング グループの設定 (687 ページ)
  - ポート ミラーリング グループの編集 (688 ページ)
  - ポート ミラーリング グループの削除 (689 ページ)

スイッチング > ポート ミラーリング

トピック:

- ポート ミラーリングについて (686 ページ)
- ミラーされているポートの表示 (686 ページ)
- ポート ミラーリング グループの設定 (687 ページ)
- ポート ミラーリング グループの編集 (688 ページ)
- ポート ミラーリング グループの削除 (689 ページ)

ポート ミラーリングについて

SonicOS ではポート ミラーリングを設定して、1 つ以上のスイッチ ポート (または 1 つの VLAN) で検出されたネットワーク パケットのコピーを、ミラー ポートと呼ばれる別のスイッチ ポートに送信できます。ミラー ポートに接続することで、ミラーリングされたポートを通過するトラフィックを監視できます。

NSA 2650 では、VLAN トランク ポートをミラー ポートまたはミラーリング対象ポートにすることができます。その他すべてのプラットフォームの場合、VLAN トランク ポートは、ミラーリングできますが、ミラー ポート自体の役割を果たすことはできません。

「**管理 | システム セットアップ | スイッチング > ポート ミラーリング**」では、ポートのグループとの受信、送信、または双方向のパケットをミラーリングするために、ミラー ポートを割り当てることができます。

ミラーされているポートの表示

ミラー ポートに接続することで、ミラーリング対象ポートのトラフィックを監視します。

グループ名 インターフェース グループの名前。

ミラー ポート ミラー ポートとして使用されるインターフェース、つまり、選択されている方向でその他のポートを監視しているポートです。

方向 ミラーリングされるトラフィックの方向:

- **双方向** (両方の方向)
- **受信**
- **送信**

受信 ミラーされているポートに送られてきたパケット数。送信専用ポートでは、常に 0 になります。

送信 ミラーされているポートから送出されたパケット数。受信専用ポートでは、常に 0 になります。

有効 グループのミラーリングが有効 (チェックボックス オン) か無効 (チェックボックス オフ) かを示します。

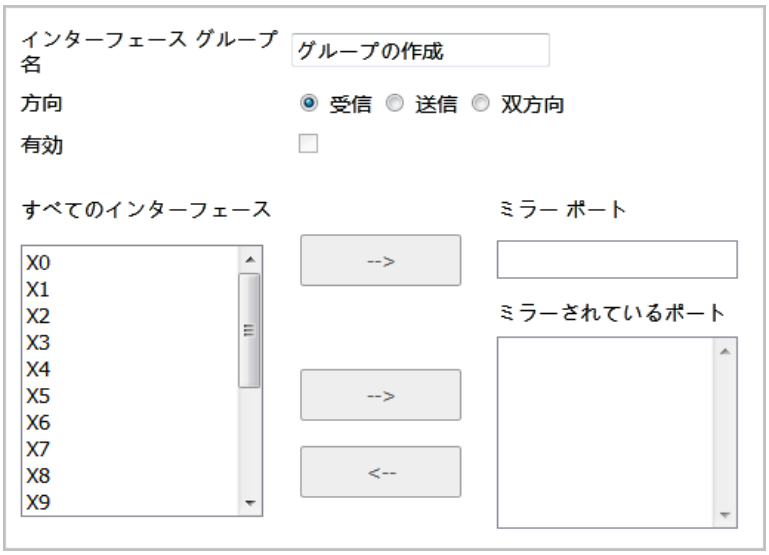
設定 グループ エントリの**編集**アイコンと**削除**アイコン、およびグループ内の各ポートの**削除**アイコンがあります。

ポート ミラーリング グループの設定

新しいポート ミラーリング グループを作成するには、以下の手順に従います。

1 「**スイッチング > ポート ミラーリング**」に移動します。

2 「**グループの作成**」を選択します。「**ミラー グループの編集**」ダイアログが表示されます。



3 「**インターフェース グループ名**」フィールドに、グループのわかりやすい名前を入力します。既定の名前は、**新規グループ**です。

4 「**方向**」では、次のいずれかを選択します。

- **受信** - ミラーされているポートに送られてくるトラフィックを監視します。
- **送信** - ミラーされているポートから送出されるトラフィックを監視します。
- **双方向** - ミラーされているポートで両方向のトラフィックを監視します。

5 「**すべてのインターフェース**」リストで、次の操作を行います。

a トラフィックのミラーリング先ポートを選択します。未定義のポートをミラー ポートとして使用する必要があります。

b 上部にある**右矢印**を選択して、そのポートを「**ミラー ポート**」フィールドに移動します。

6 「**すべてのインターフェース**」リストで、次の操作を行います。

a 監視対象となる 1 つ以上のポートを選択します。ミラー ポートに接続することで、ミラーリング対象ポートのトラフィックを監視します。

b 下部にある**右矢印**を選択して、そのポートを「**ミラーされているポート**」リストに移動します。

7 これらのポートでポート ミラーリングを有効にするには、「**有効**」オンにします。

> **メモ**：一度に有効にできるのは、1 つの受信グループと 1 つの送信グループだけです。双方向のグループが有効になっている場合、個々の受信グループや送信グループ、または双方向の別のグループを有効にすることはできません。個々の受信グループと送信グループを別々に有効にすることができます。
>
> ミラー ポートとそのミラーリング対象ポートが指定されるまで、このオプションはグレーアウトされます。

8 「**OK**」を選択します。

ミラーリング対象グループの有効化

ミラーリング対象グループの作成時にそのグループを有効にしなかった場合は、「**グループ**」テーブルで、そのミラーリング対象グループの「**有効**」を選択してミラーリングを有効にすることができます。

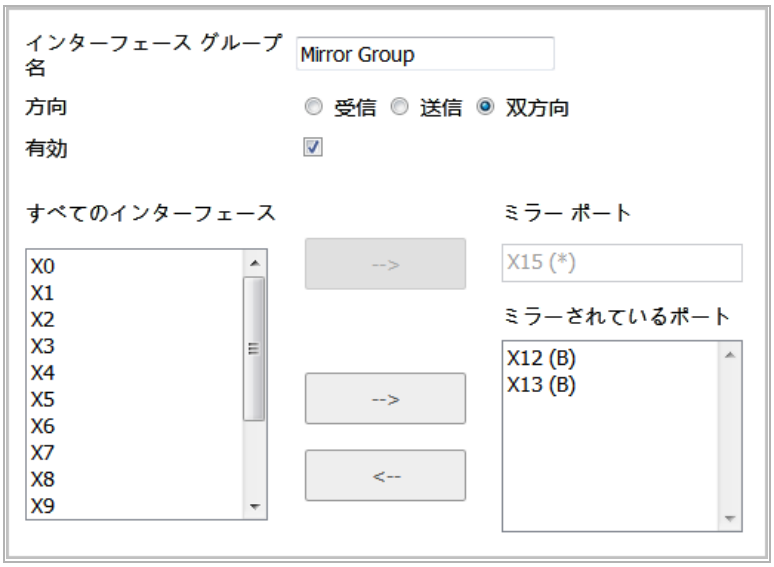
ポート ミラーリング グループの編集

ミラー ポート (グレーアウトされています) を除き、ミラーリング対象グループのすべての属性を編集できます。

ポート ミラーリング グループを編集するには、以下の手順に従います。

1 「**スイッチング > ポート ミラーリング**」に移動します。

2 ミラー ポートの**編集**アイコンを選択します。そのグループの「**ミラー グループの編集**」ダイアログが表示されます。



3 必要なオプションを適宜変更します。

> **メモ**：ミラーリング対象ポートは追加または削除ができますが、ミラー ポートそのものの追加や削除はできません。グループのメンバーを削除する場合、確認メッセージは表示されません。

4 グループでミラーリングが有効な場合は、「**有効**」が選択されています。これらのポートでポート ミラーリングを無効にするには、「**有効**」の選択を解除します。

> **メモ**：一度に有効にできるのは、1 つの受信グループと 1 つの送信グループだけです。双方向のグループが有効になっている場合、個々の受信グループや送信グループ、または双方向の別のグループを有効にすることはできません。個々の受信グループと送信グループを別々に有効にすることができます。

5 「**OK**」を選択します。

ポート ミラーリング グループの削除

ミラー グループのメンバー、特定のミラー グループ、複数のミラー グループ、またはすべてのミラー グループを削除できます。

トピック:

- ポート グループ メンバーの削除 (689 ページ)
- ポート ミラーリング グループの削除 (689 ページ)
- 複数のポート ミラーリング グループの削除 (690 ページ)
- すべてのポート ミラーリング グループの削除 (690 ページ)

ポート グループ メンバーの削除

ポート グループのメンバーの削除は、「ポート ミラーリング グループの編集 (688 ページ)」の説明に従って行うことも、「**グループ**」テーブルで行うこともできます。

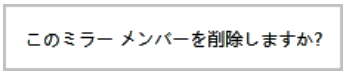
「グループ」テーブルでポート グループのメンバーを削除するには、以下の手順に従います。

1 「**スイッチング > ポート ミラーリング**」に移動します。

2 グループの「**展開**」ボタンを選択して、グループ メンバーを表示します。

3 次のどちらかを行います。

- 削除するメンバーの**削除**アイコンを選択します。確認メッセージが表示されます。

- 削除するメンバーのチェックボックスを 1 つ以上選択し、「**グループの解除**」を選択します。確認メッセージが表示されます。

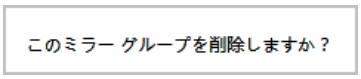
4 「**OK**」を選択します。

ポート ミラーリング グループの削除

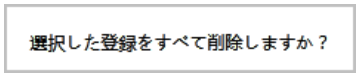
「グループ」テーブルで特定のポート ミラーリング グループを削除するには、以下の手順に従います。

1 次のどちらかを行います。

- 削除するグループの**削除**アイコンを選択します。確認メッセージが表示されます。

- グループのチェックボックスをオンにし、「**グループの解除**」を選択します。確認メッセージが表示されます。



2 「**OK**」を選択します。

複数のポート ミラーリング グループの削除

複数のポート ミラーリング グループを削除するには、以下の手順に従います。

1 「**グループ**」テーブルで、削除したいポート ミラーリング グループの横にあるチェックボックスをオンにします。

2 「**グループの解除**」を選択します。確認ダイアログが表示されます。

3 「**OK**」を選択します。

すべてのポート ミラーリング グループの削除

すべてのポート ミラーリング グループを削除するには、以下の手順に従います。

1 「**グループ**」テーブルで、テーブル見出しにあるチェックボックスをオンにします。

2 「**グループの解除**」を選択します。確認ダイアログが表示されます。

3 確認のダイアログで、「**OK**」を選択します。

44

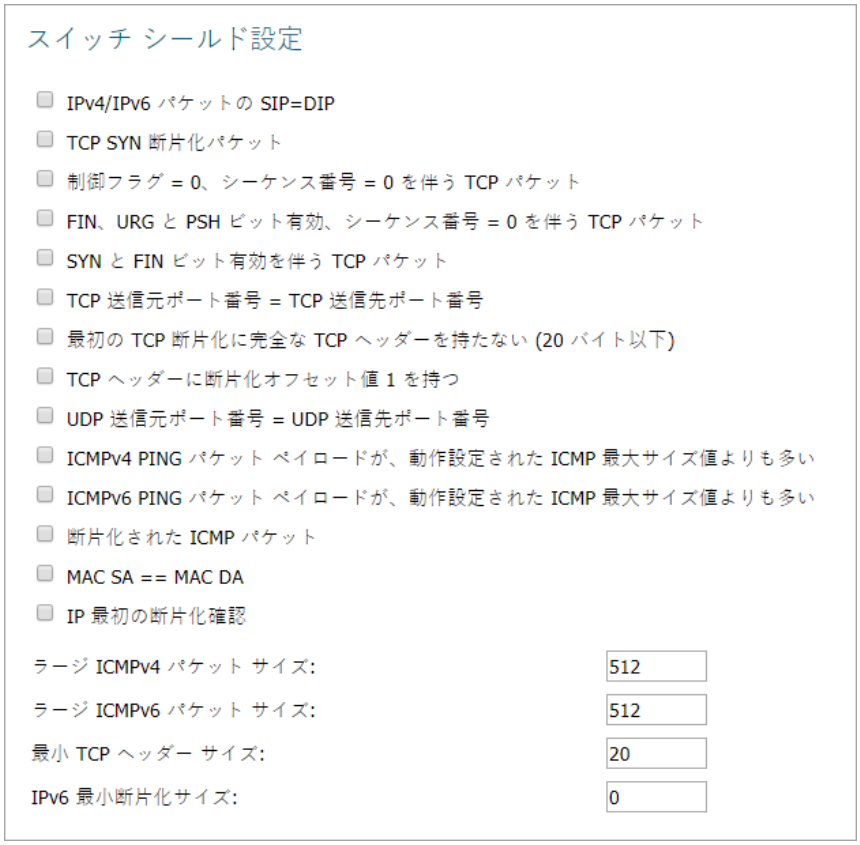
シールド切り替えの設定

メモ：スイッチングは NSA 2650 以降のすべてのファイアウォールで利用可能です。

トピック:

- スイッチング > シールド切り替え (691 ページ)

スイッチング > シールド切り替え



シールド切り替えの設定を構成するには:

1. 「**管理 | システム セットアップ > スイッチング > シールド切り替え**」に移動します。
2. DDOS 保護のためにスイッチ機能を使用するオプションを選択します。既定では、すべてのオプションがオフになっています。
3. 「**適用**」を選択します。

第 6 部

システム セットアップ | 高可用性

- アクティブ/アクティブ クラスタリングでの高可用性について
- 高可用性の設定
- 高可用性の微調整
- 高可用性の監視

45

アクティブ/アクティブ クラスタリングでの高可用性について

メモ：高可用性 (HA) は TZ シリーズ以降のセキュリティ装置でサポートされていますが、無線が有効な TZ シリーズのセキュリティ装置では HA はサポート対象外です。ステートフル HA およびアクティブ/アクティブ DPI は、TZ500 シリーズ以降のセキュリティ装置でサポートされています。「アクティブ/スタンバイおよびアクティブ/アクティブ DPI 機能の前提条件 (704 ページ)」を参照してください。アクティブ/アクティブ クラスタリングは、NSA 3600 以降のセキュリティ装置でサポートされます。「アクティブ/アクティブ クラスタのライセンス要件 (722 ページ)」を参照してください。

NAT64 は高可用性機能をサポートしていません。

トピック:

- 高可用性 (693 ページ)
  - 高可用性機能について (694 ページ)
  - アクティブ/スタンバイ HA について (700 ページ)
  - ステートフル同期について (701 ページ)
  - アクティブ/アクティブ DPI HA について (703 ページ)
  - アクティブ/スタンバイおよびアクティブ/アクティブ DPI 機能の前提条件 (704 ページ)
  - メンテナンス (707 ページ)
- アクティブ/アクティブ クラスタリング (709 ページ)
  - アクティブ/アクティブ クラスタリングについて (709 ページ)

高可用性

このセクションでは、SonicOS の高可用性 (HA) の概念的な情報を示し、HA を利用するためのセキュリティ装置の接続方法を説明します。

トピック:

- 高可用性機能について (694 ページ)
- アクティブ/スタンバイ HA について (700 ページ)
- ステートフル同期について (701 ページ)
- アクティブ/アクティブ DPI HA について (703 ページ)

- アクティブ/スタンバイおよびアクティブ/アクティブ DPI 機能の前提条件 (704 ページ)
- セキュリティ装置の物理的な接続 (706 ページ)

高可用性機能について

トピック:

- 高可用性機能とは (694 ページ)
- 高可用性機能のモード (695 ページ)
- 高可用性暗号化 (697 ページ)
- クラッシュ検出 (697 ページ)
- 仮想 MAC アドレス (697 ページ)
- PPPoE HA での動的 WAN インターフェース (698 ページ)
- DHCP のステートフル同期 (698 ページ)
- 高可用性監視について (699 ページ)

高可用性機能とは

高可用性 (HA) 機能は、SonicOS が動作している同一の SonicWall セキュリティ装置 2 つを設定して、パブリック インターネットへの連続した信頼性の高い接続を提供する冗長デザインです。1 台の SonicWall セキュリティ装置をプライマリ装置として設定し、それと同一のセキュリティ装置をセカンダリ装置として設定します。プライマリ セキュリティ装置に障害が発生した場合、セカンダリ セキュリティ装置が引き継ぎ、保護されたネットワークとインターネット間の信頼性の高い接続を確保します。このようにして設定された2 台のセキュリティ装置は、高可用性ペア (HA ペア) とも呼ばれます。

高可用性機能を使用すると、一方の装置が他方の装置の高可用性システムとして機能しているときに、2 つの SonicWall セキュリティ装置の間で SonicWall ライセンスを共有できます。両方のセキュリティ装置は同一の SonicWall モデルでなければなりません。

この機能を使用するには、MySonicWall で SonicWall セキュリティ装置を関連付けられた製品として登録する必要があります。詳細については、『*SonicOS 6.5 更新*』を参照してください。

高可用性機能の用語

アクティブ	ハードウェア装置の稼働状態を示します。アクティブの識別子は、プライマリ ハードウェア装置またはセカンダリ ハードウェア装置のいずれかが持つことができる論理的な役割です。
フェイルオーバー	アクティブな装置の障害と判断された後に、スタンバイ状態の装置がアクティブの役割を引き継ぐ実際のプロセスを表します。障害かどうかの判断は、「高可用性の設定 (726 ページ)」に記載されている設定可能なさまざまな物理的および論理的な監視機能によって行われます。
HA	高可用性: 非ステートのハードウェア フェイルオーバー機能。
IDV	Interface Disambiguation via VLAN (VLAN を介したインターフェースの曖昧性解消)。
PoE	Power over Ethernet は、ネットワーク ケーブルで電力を供給する技術です。

PPP	ポイント ツー ポイント リンクでマルチプロトコル ダイアグラム伝送を行う標準方式を提供するポイント ツー ポイント プロトコルです。
PPPoE	イーサネット上で PPP 伝送を行う方式です。
PPPoE HA	HA PPPoE はステートなしの機能をサポートします。
先制	プライマリ装置に障害が発生し、セカンダリ装置がアクティブの役割を引き継ぐ、フェイルオーバー後の状態を示します。先制を有効にすると、プライマリ装置が稼働状態に復元されたことが確認された後に、プライマリ装置がセカンダリ装置からアクティブの役割を取り戻します。
プライマリ	プライマリ ハードウェア装置を示します。プライマリの識別子は手動で指定し、条件による変更の対象にはなりません。通常の動作条件下では、プライマリ ハードウェア装置はアクティブな役割で動作します。
セカンダリ (バックアップ)	従属のハードウェア装置を示します。セカンダリの識別子は関連に基づく指定であり、プライマリ装置と組み合わせたときに装置によって想定されます。通常の動作条件下では、セカンダリ装置はスタンバイ モードで動作します。プライマリ装置で障害が発生すると、セカンダリ装置がアクティブな役割を引き継ぎます。
SHF	ステート ハードウェア フェイルオーバーは、プライマリ セキュリティ装置で障害が発生し、バックアップ セキュリティ装置が引き継ぐときに、既存のネットワーク フローをアクティブのままにすることのできる SonicOS の機能です。
スタンバイ (アイドル)	ハードウェア装置のパッシブ状態を示します。スタンバイの識別子は、プライマリ ハードウェア装置またはセカンダリ ハードウェア装置のいずれかが持つことができる論理的な役割です。スタンバイ状態の装置は、アクティブな装置の障害と判断できるイベントが発生したときに、アクティブの役割を引き継ぎます。
STP	Spanning Tree Protocol です。

高可用性機能のモード

高可用性機能には、いくつかの動作モードがあります。これらのモードは「**高可用性 > 基本設定**」で選択できます。

- **なし** -「**なし**」を選択すると、標準の高可用性設定とハードウェア フェイルオーバー機能が、ステートフル HA およびアクティブ/アクティブ DPI を有効化するオプションとともに、有効になります。
- **アクティブ/スタンバイ** - アクティブ/スタンバイ モードでは、2 つの同一のセキュリティ装置を高可用性ペアとして構成することで、基本的な高可用性を実現します。アクティブ装置はすべてのトラフィックを処理します。スタンバイ装置は設定情報を共有し、アクティブ装置が停止した場合に直ちに動作を引き継いでネットワーク接続の持続性を確保します。

  既定では、アクティブ/アクティブ モードはステートレスです。つまり、フェイルオーバー後にネットワーク接続と VPN トンネルを再確立する必要があります。ステートフル同期のライセンスを追加して有効化すると、アクティブ/スタンバイ モードでこれを回避できます。このステートフルな高可用性モードでは、アクティブ装置とスタンバイ装置の間で動的な状態が常時同期されます。アクティブ装置に障害が発生すると、既存のネットワーク接続に中断を発生さ

せることなくスタンバイ セキュリティ装置がアクティブの役割を引き継ぐので、ステートフル フェイルオーバーとなります。

メモ：ステートフル HA:

- NSA 4600 以降の NSA プラットフォームと、SuperMassive シリーズのプラットフォームに含まれています。
- SonicOS 拡張ライセンスまたは高可用性ライセンスがある NSA 2600 および NSA 3600 プラットフォームでサポートされています。
- SonicOS 拡張ライセンスまたは高可用性 (ステートフル) アップグレード ライセンスがある TZ500 以降の TZ プラットフォームでサポートされています。

ライセンス情報については、『*SonicOS 6.5 更新*』を参照してください。

- **アクティブ/アクティブ DPI** - アクティブ/アクティブ DPI (精密パケット検査) モードは、アクティブ/スタンバイ モードと並行して使用できます。アクティブ/アクティブ DPI モードを有効にすると、侵入防御 (IPS)、ゲートウェイ アンチウイルス (GAV)、アンチスパイウェアなどのプロセッサ使用率の高い DPI サービスはスタンバイ セキュリティ装置が処理を実行し、ファイアウォール、NAT、その他のトラフィックなどのサービスはアクティブ セキュリティ装置が同時的に処理を実行します。

  メモ：アクティブ/アクティブ DPI:

  - SM 9000 シリーズ プラットフォームに含まれています。
  - SonicOS 拡張ライセンスまたは高可用性 (ステートフル) ライセンスがある NSA 5600 以降のプラットフォームでサポートされています。

  ライセンス情報については、『*SonicOS 6.5 更新*』を参照してください。

- **アクティブ/アクティブ クラスタリング** - このモードでは、複数のセキュリティ装置がクラスタ ノードとしてグループを形成し、複数のアクティブ装置が DPI の処理やネットワーク負荷を分散しながらトラフィックを処理します (複数のゲートウェイとして動作)。各クラスタ ノードは、ステートフル高可用性ペアとして動作する 2 つの装置から構成されます。アクティブ/アクティブ クラスタリングでは、負荷分散に加えてステートフル フェイルオーバーがサポートされます。各クラスタ ノードを 1 つの装置で構成することもできます。その場合は、ステートフル フェイルオーバーとアクティブ/アクティブ DPI は利用できません。

  メモ：アクティブ/アクティブ クラスタリング:

  - SM 9000 シリーズ プラットフォームに含まれています。
  - SonicOS 拡張ライセンスが購入されている NSA 3600 以降のプラットフォームでのみサポートされています。

  ライセンス情報については、『*SonicOS 6.5 更新*』を参照してください。

- **アクティブ/アクティブ DPI クラスタリング** - このモードでは、フェイルオーバーと負荷分散のために最大 4 つの HA クラスタ ノードを設定できます。負荷分散では、各ノードによってネットワーク トラフィックに対する DPI セキュリティ サービスのアプリケーションの負荷が分散されます。このモードを有効にすると、各クラスタ ノードのスタンバイ装置の利用によりパフォーマンスを向上できます。

  メモ：アクティブ/アクティブ DPI クラスタリング:

  - SM 9000 シリーズ プラットフォームに含まれています。
  - SonicOS 拡張ライセンスが購入されている NSA 3600 以降のプラットフォームでのみサポートされています。

  ライセンス情報については、『*SonicOS 6.5 更新*』を参照してください。

高可用性暗号化

高可用性暗号化は、HA ペアの装置間の通信にセキュリティを追加します。ハートビート、設定の同期、HA 状態情報など、アクティブ ファイアウォールとスタンバイ ファイアウォール間の HA 制御メッセージは、ノード間通信のセキュリティを確保するために暗号化されています。

このオプションはアクティブ - スタンバイ HA モードでのみ使用可能で、アクティブ - スタンバイ モードでもステートフル同期のために交換されるメッセージには適用されません。検出メッセージ (find-peer および found-peer) は暗号化なしで送信されます。ただし、発見段階の後、すべての制御メッセージはファイアウォール間で暗号化されます。

- ハートビート
- 増分構成の更新に使用されるメッセージ
- `prefSync` メッセージ
- ファイアウォール ペア間で HA コマンドを送信するためのさまざまなメッセージ
- ファームウェア同期メッセージ

クラッシュ検出

HA 機能は、アクティブ セキュリティ装置とスタンバイ セキュリティ装置の両方に対する完全な自己診断メカニズムを備えています。スタンバイ装置へのフェイルオーバーが発生するのは、重要なサービスに影響があった場合、監視中のインターフェースで物理 (または論理) リンクの障害が検出された場合、またはセキュリティ装置で停電が発生した場合です。

自己チェック メカニズムはソフトウェア診断によって管理されます。ソフトウェア診断では、セキュリティ装置の完全なシステム整合性がチェックされます。診断では、内部システム状況、システム プロセス状況、および内外部のネットワーク接続がチェックされます。フェイルオーバー ループの発生を避けるため、両側において、どちらの側の接続が優れるかの重み付けをするメカニズムがあります。

NAT、VPN、DHCP などの重要な内部システム プロセスは、リアルタイムでチェックされます。障害の発生したサービスは可能な限り速やかに切り離され、フェイルオーバー メカニズムによって自動的に修復されます。

仮想 MAC アドレス

仮想 MAC アドレスを使用することで高可用性ペアが同じ MAC アドレスを共有できるため、フェイルオーバー後の収束にかかる時間が大幅に減少します。収束にかかる時間は、ネットワーク内の装置のルーティング テーブルを高可用性機能に起因する変更に適合させるためにかかる時間です。

仮想 MAC アドレスが有効でない場合、アクティブ状態のセキュリティ装置とスタンバイ状態のセキュリティ装置はそれぞれ独自の MAC アドレスを持ちます。しかし、セキュリティ装置で同じ IP アドレスを使用しているため、フェイルオーバーが発生した場合には、すべてのクライアントおよびネットワーク リソースの ARP キャッシュにおいて、IP アドレスと MAC アドレスの間のマッピングが壊れてしまいます。セカンダリセキュリティ装置は ARP 要求を発行して、新しい MAC アドレスと IP アドレスのペアを通知する必要があります。この ARP 要求がネットワーク全体に伝播するまで、プライマリセキュリティ装置の MAC アドレス宛てのトラフィックが失われる可能性があります。

仮想 MAC アドレスの導入により、プライマリ セキュリティ装置とセカンダリ セキュリティ装置の両方で同じ MAC アドレスが使用されるため、この処理が大幅に簡素化されました。フェイルオーバーが発生しても、プライマリ セキュリティ装置に到達するルートおよびプライマリ セキュリティ装置から発信するルートのすべてが、セカンダリ セキュリティ装置で有効なままになります。すべての

クライアントおよびリモート サイトは、同じ仮想 MAC アドレスおよび IP アドレスを途切れることなく使用し続けます。

既定では、この仮想 MAC アドレスは SonicWall ファームウェアによって指定されるものであり、プライマリまたはセカンダリ セキュリティ装置のいずれの物理 MAC アドレスとも異なります。これにより、設定エラーの発生を防止し、仮想 MAC アドレスの一意性を確保して競合が起こらないようにしています。必要に応じて、仮想 MAC アドレスの手動設定を「**高可用性 > 監視設定**」で行うことができます。

仮想 MAC の設定は、ステートフル高可用性機能のライセンスがなくても利用できます。仮想 MACが有効になっていると、ステートフル同期が有効になっていなくても、常に仮想 MAC アドレスが使用されます。

PPPoE HA での動的 WAN インターフェース

メモ：PPPoE HA での動的 WAN インターフェースは SuperMassive 9800 ではサポートされていません。DHCP サーバの動的 WAN モードのみがサポートされています。

PPPoE を 非ステートフル モード、HA アクティブ/スタンバイ モードのインターフェースで有効にすることができます。PPPoE HA の提供する HA では、アクティブ セキュリティ装置で障害が発生すると、セカンダリ セキュリティ装置が PPPoE サーバへの接続を引き継ぎます。

メモ：1 つの WAN インターフェースを PPPoE として設定する必要があります。「WAN インターフェースの設定 (313 ページ)」を参照してください。

アクティブ装置が PPPoE サーバに接続した後、セキュリティ装置は PPPoE セッション ID とサーバ名をセカンダリ装置に同期します。

アクティブ セキュリティ装置で障害が発生すると、タイムアウトすることによってクライアント側の PPPoE HA 接続を終了します。セカンダリ セキュリティ装置は PPPoE サーバに接続し、サーバ側の元の接続を終了し、新しい PPPoE 接続を開始します。既存のネットワーク接続はすべて再接続され、PPPoE セッションが再確立されて、PPP プロセスが再ネゴシエートされます。

DHCP のステートフル同期

アクティブ/スタンバイ (非ステートフル) モードとステートフル同期モードの両方のインターフェースで DHCP を有効にできます。

DHCP リースを取得できるのはアクティブ セキュリティ装置のみです。アクティブ セキュリティ装置は、DHCP IP アドレスを DNS アドレスおよびゲートウェイ アドレスと共にセカンダリ セキュリティ装置に同期します。DHCP クライアント ID も同期されるため、仮想 MAC を有効にしなくてもこの機能を利用できます。

フェイルオーバー時に、アクティブ セキュリティ装置は DHCP リースを解放します。セカンダリ セキュリティ装置がアクティブ装置になり、既存の DHCP IP アドレスとクライアント ID を使用して DHCP リースを更新します。IP アドレスは変わらず、VPN トンネル トラフィックを含むネットワーク トラフィックは引き続き送信されます。

フェイルオーバー発生時にアクティブ セキュリティ装置に IP アドレスが設定されていない場合は、セカンダリ セキュリティ装置が新しい DHCP 検出を開始します。

DNS プロキシのステートフル同期

DNS プロキシは DNS キャッシュのステートフル同期をサポートしています。DNS キャッシュが追加、削除、または動的に更新された場合、DNS キャッシュはアイドル状態のセキュリティ装置との同期をとります。

高可用性監視について

「**管理 | システム セットアップ > 高可用性 > 監視設定**」ページで、物理インターフェースと論理インターフェースの監視を設定できます。

- 物理リンク監視を有効にすると、指定された HA インターフェースのリンク検出が可能になります。このリンクの検出は、リンクの動作状態を判断するために物理層で行われます。
- 論理監視とは、SonicWall を設定して接続先ネットワークの 1 つ以上に存在する信頼性の高い機器を監視することです。

HA ペアのアクティブな装置がこの機器との定期的な通信に失敗すると、スタンバイ装置へのフェイルオーバーが実行されます。HA ペアのどちらもこの機器に接続できない場合は、何も処理が行われません。

「**高可用性 > 監視設定**」で設定されるプライマリおよびセカンダリ IP アドレスは、LAN または WAN インターフェース上で設定でき、以下に示す複数の目的に使用されます。

- 各装置の固有の管理アドレス (すべての物理インターフェース上でサポートされている) として使用
- スタンバイ状態の装置と SonicWall ライセンス サーバの間のライセンスの同期用
- 論理監視中に送出されるプローブ Ping の送信元 IP アドレス

HA ペアの両方の装置に一意の管理 IP アドレスを設定すると、各装置に個別にログインして管理タスクを行うことができます。管理 IP アドレス宛てに送信された管理目的ではないトラフィックは無視されます。プライマリおよびセカンダリの セキュリティ装置の一意の LAN IP アドレスは、アクティブ ゲートウェイとしては機能できません。内部 LAN に接続されたすべてのシステムは、ゲートウェイとして仮想 LAN IP アドレスを使用する必要があります。

WAN 監視 IP アドレスを設定する場合、X0 監視 IP アドレスは不要です。WAN 監視 IP アドレスを設定しない場合は、X0 監視 IP アドレスが必要です。このようなシナリオでは、スタンバイ装置は X0 監視 IP アドレスを使用してライセンス サーバに接続し、すべてのトラフィックがアクティブ装置を通過するためです。

セカンダリ/スタンバイ装置の管理 IP アドレスを使用すると、SonicWall ライセンス サーバとライセンスを同期できます。このサーバは、HA ペア単位ではなくセキュリティ装置単位でライセンスを管理します。HA の関連付けを作成する前にセカンダリ装置が MySonicWall で登録されていた場合でも、管理 IP アドレスによってセカンダリ セキュリティ装置にアクセスしているときは、SonicWall サーバに接続するために「**管理 | 更新 > ライセンス**」上のリンクを使用する必要があります (詳細については、『*SonicOS 更新*』を参照してください)。

論理監視の使用時には、指定された論理監視対象 IP アドレスを送信先とした Ping が、HA ペアのプライマリおよびセカンダリの装置から実行されます。「プライマリ IP アドレス」または「セカンダリ IP アドレス」のフィールドに設定された IP アドレスは、Ping の送信元 IP アドレスとして使用されます。両方が送信先への Ping に成功した場合、フェイルオーバーは発生しません。両方が送信先への Ping に失敗した場合は、SonicOS は、セキュリティ装置ではなく送信先に問題があると見なし、フェイルオーバーは発生しません。しかし、一方のセキュリティ装置が送信先への Ping に成功し、もう一方が失敗した場合は、Ping に成功したほうのファイアウォールへのフェイルオーバーが行われます。

「**高可用性 > 監視設定**」での設定タスクは、プライマリ装置で実行された後、セカンダリ装置に対して自動的に同期されます。

アクティブ/スタンバイ HA について

HA 機能を使用すると、SonicOS が動作している同一の 2 台のセキュリティ装置を設定して、パブリック インターネットへの連続した信頼性の高い接続を提供できます。1 台のセキュリティ装置をプライマリ装置として設定し、それと同一のセキュリティ装置をセカンダリ装置として設定します。プライマリ セキュリティ装置に障害が発生した場合、セカンダリ セキュリティ装置が引き継ぎ、保護されたネットワークとインターネット間の信頼性の高い接続を確保します。このようにして設定された2台のセキュリティ装置は、高可用性ペア (HA ペア) とも呼ばれます。

アクティブ/スタンバイ HA は、ステートフル HA およびアクティブ/アクティブ DPI を有効化できる標準の高可用性ハードウェア フェイルオーバー機能です。

HA 機能を使用すると、一方の装置が他方の装置の高可用性システムとして機能するので、2 台のセキュリティ装置の間でライセンスを共有できます。この機能を使用するには、MySonicWall でセキュリティ装置を関連付けられた製品として登録する必要があります。両方のセキュリティ装置は同一の SonicWall モデルでなければなりません。

トピック:

- アクティブ/スタンバイ HA 機能のメリット (700 ページ)
- アクティブ/スタンバイ HA 機能の動作 (700 ページ)

アクティブ/スタンバイ HA 機能のメリット

- **ネットワークの信頼性の向上** - 高可用性構成では、プライマリユニットに障害が発生した場合、セカンダリ セキュリティ装置がすべてのネットワーク責任を引き継ぎ、保護されたネットワークとインターネット間の信頼性の高い接続を確保します。
- **優れたコスト効果** - 高可用性機能は、セキュリティ装置を冗長化して使用することで高可用性を得る、配備にとってコスト効果の高いオプションです。高可用性ペアのセカンダリ装置のためにライセンスをもう 1 セット購入する必要はありません。
- **フェイルオーバー後の収束時間を短縮する仮想 MAC** - 仮想 MAC アドレスを設定することで HA ペアが同じ MAC アドレスを共有できるため、フェイルオーバー後の収束にかかる時間が大幅に減少します。収束にかかる時間は、ネットワーク内の装置のルーティング テーブルを高可用性機能に起因する変更に適合させるためにかかる時間です。既定では、この仮想 MAC アドレスは SonicWall ファームウェアによって指定されるものであり、プライマリまたはセカンダリ セキュリティ装置のいずれの物理 MAC アドレスとも異なります。

アクティブ/スタンバイ HA 機能の動作

メモ：TZ300 シリーズおよび TZ400 シリーズのセキュリティ装置は、ステートフル同期がなくても、アクティブ/スタンバイ HA モードで動作させることができます。SOHO W はステートフル同期の有無にかかわらず、高可用性機能をサポートしていません。

HA 機能を使用するには、プライマリ SonicWall として設定された 1 台の SonicWall セキュリティ装置と、セカンダリ SonicWall として設定された同一モデルのセキュリティ装置が必要です。通常の動作中は、プライマリ SonicWall がアクティブ状態となり、セカンダリ SonicWall がスタンバイ状態となり

ます。プライマリ機器が接続を失った場合、セカンダリ SonicWall 機器がアクティブ モードに移行し、プライマリ機器の設定と役割を代行します。設定されたインターフェースのインターフェース IP アドレスもそのまま使用されます。

基本的なアクティブ/スタンバイ HA 機能では、ステートレス高可用性が提供されます。セカンダリ セキュリティ装置へのフェイルオーバーが行われた後は、既存のすべてのネットワーク接続を再確立する必要があります。VPN トンネルの再ネゴシエートも必要になります。オプションで、ステートフル同期のライセンスを追加して有効化することもできます。詳細については、「ステートフル同期について (701 ページ)」を参照してください。

フェイルオーバーが適用されるのは、プライマリ SonicWall の機能またはネットワーク層接続が失われた場合です。セカンダリ SonicWall へのフェイルオーバーが発生するのは、重要なサービスに影響があった場合、監視中のインターフェースで物理 (または論理) リンクの障害が検出された場合、またはプライマリ SonicWall で停電が発生した場合です。現在、プライマリ SonicWall 機器およびセカンダリ SonicWall 機器では、アクティブ/スタンバイ高可用性機能、またはアクティブ/アクティブ DPI 機能のみを実行できます。完全なアクティブ/アクティブ高可用性機能は、現時点ではサポートされていません。

すべての設定に適用される同期には、次の 2 つの種別があります。

- **増分** - タイムスタンプが同期されており、アクティブな装置で変更が行われた場合、増分同期がスタンバイ状態の装置にプッシュされます。
- **完全** - タイムスタンプが同期されておらず、スタンバイ状態の装置が利用可能な場合、完全同期がスタンバイ状態の装置にプッシュされます。増分同期が失敗した場合、完全同期が自動的に試みられます。

ステートフル同期について

ステートフル同期機能では、フェイルオーバーのパフォーマンスが大幅に改善されています。ステートフル同期が有効な場合、ネットワーク接続と VPN トンネルの情報が 2 つの装置の間で常時同期され、プライマリ セキュリティ装置に障害が発生した場合に、既存のネットワーク接続を中断することなく、ネットワークに関するすべての役割をセカンダリ セキュリティ装置がシームレスに引き継ぐことができます。

メモ：ステートフル HA は、NSA 4600 以降の NSA プラットフォームと、すべての SuperMassive シリーズのプラットフォームに含まれています。ステートフル HA は、TZ500 以降の TZ プラットフォームと、拡張ライセンスまたはステートフル HA アップグレード ライセンスがある NSA 2600 および NSA 3600 プラットフォームでサポートされます。ライセンス情報については、『*SonicOS の更新*』を参照してください。

トピック:

- ステートフル同期のメリット (701 ページ)
- ステートフル同期機能の動作 (702 ページ)

ステートフル同期のメリット

- **信頼性の向上** - ステートフル同期機能により最も重要なネットワーク接続情報が同期されるため、セキュリティ装置に障害が発生した場合にもダウン時間が発生することがなく、接続が切断されることがありません。

- **フェイルオーバーの高速化** - ステートフル同期機能によりプライマリ セキュリティ装置およびセカンダリ セキュリティ装置の間で常時同期がとられるため、障害が発生した場合にも、ダウン時間が発生したりネットワーク接続が失われたりすることが事実上なく、セカンダリ セキュリティ装置が引き継ぐことができます。
- **CPU のパフォーマンスへの影響の最小化** - 通常、使用率は 1% 未満です。
- **帯域幅への影響の最小化** - 同期データの送信は、他のデータの送信に影響しないように調整されます。

ステートフル同期機能の動作

ステートフル同期機能は、負荷分散ではありません。プライマリ セキュリティ装置ですべてのトラフィックが処理されるアクティブ-スタンバイ構成です。ステートフル同期機能が有効にされている場合、プライマリ セキュリティ装置はセカンダリ セキュリティ装置とアクティブに通信して、ほとんどのネットワーク接続情報を更新します。プライマリ セキュリティ装置でネットワーク接続情報 (VPN トンネル、動作中のユーザ数、接続キャッシュ エントリなど) が作成および更新されると、プライマリ セキュリティ装置からセカンダリ セキュリティ装置にすぐに通知されます。これにより、セカンダリセキュリティ装置は常にアクティブ状態に移行する準備が整っているため、接続が切断されることはありません。

同期トラフィックは、通常のネットワーク トラフィックが影響を受けることのないように調整されます。設定の変更はすべてプライマリ セキュリティ装置で実行され、セカンダリ セキュリティ装置へ自動的に伝播されます。どちらのセキュリティ装置がアクティブであるかに関係なく、高可用性ペアでは同じ LAN および WAN IP アドレスが使用されます。

SonicWall グローバル管理システム (GMS) を使用してセキュリティ装置を管理する場合、GMS は共有 WAN IP アドレスにログインします。フェイルオーバーが発生した場合、GMS 管理はシームレスに継続されます。また、その時点でセキュリティ装置にログインしている GMS 管理者がログアウトされることはありません。ただし、**Get** および **Post** コマンドがタイムアウトとなって応答が返されないことがあります。

「同期される情報と同期されない情報」テーブルに、現在のステートフル同期機能で同期される情報と同期されない情報を示します。

同期される情報と同期されない情報

同期される情報	同期されない情報
VPN の情報	動的 WAN クライアント (L2TP、PPPoE、PPTP)
基本接続キャッシュ	精密パケット検査 (GAV、IPS、アンチ スパイウェア)
FTP	IPHelper バインド (NetBIOS や DHCP など)
Oracle SQL*NET	SYNFlood 保護の情報
Real Audio	コンテンツ フィルタ サービスの情報
RTSP	VoIP プロトコル
GVC の情報	動的 ARP エントリおよび ARP キャッシュ タイムアウト
動的アドレス オブジェクト	アクティブなワイヤレス クライアントの情報
DHCP サーバの情報	ワイヤレス クライアント パケットの統計情報

同期される情報と同期されない情報 (続き)

同期される情報	同期されない情報
マルチキャストと IGMP	Rogue AP リスト
動作中のユーザ	
ARP	
SonicPoint の状況	
ワイヤレス ゲストの状況	
ライセンスの情報	
重み付け負荷分散の情報	
RIP および OSPF の情報	

ステートフル同期の例

フェイルオーバーが行われる場合、イベントが発生するシーケンスは次のとおりです。

1 PC ユーザがネットワークに接続し、プライマリ セキュリティ装置でそのユーザのためのセッションが作成されます。

2 プライマリ セキュリティ装置は、セカンダリ セキュリティ装置と同期します。これで、セカンダリ装置にそのユーザのすべてのセッション情報が保存された状態になります。

3 管理者がプライマリ装置を再起動します。

4 セカンダリ装置はプライマリ装置の再起動を検知し、スタンバイからアクティブに切り替わります。

5 セカンダリ セキュリティ装置は、プライマリ セキュリティ装置と同じ仮想 MAC アドレスおよび IP アドレスを使用して、LAN および WAN スイッチへの重複回避用 ARP メッセージの送信を開始します。下流または上流のネットワーク機器でルーティングを更新する必要はありません。

6 PC ユーザがウェブ ページにアクセスしようとした場合、セカンダリ セキュリティ装置にそのユーザのすべてのセッション情報が保存されているため、中断なくユーザのセッションを継続できます。

アクティブ/アクティブ DPI HA について

重要：アクティブ/アクティブ DPI モードではキャプチャ機能はサポートされません。

ステートフル HA ペアでアクティブ/アクティブ DPI 機能を有効にすると、アクティブ セキュリティ装置でのセキュリティ装置、NAT、および他のモジュールの処理と並行して、精密パケット検査 (DPI) サービスが HA ペアのスタンバイ セキュリティ装置で処理されます。影響を受けるのは、次のDPI サービスです。

- 侵入防御サービス (IPS)
- ゲートウェイ アンチウイルス (GAV)
- ゲートウェイ アンチスパイウェア
- アプリケーション制御

アクティブ/アクティブ DPI 機能を使用するには、追加インターフェースを**アクティブ/アクティブ DPI インターフェース**として設定する必要があります。例えば、X5 をアクティブ/アクティブ DPI イン

ターフェースにする場合は、HA ペアのアクティブ装置の X5 を同じペアのスタンバイ装置の X5 に物理的に接続する必要があります。アクティブ/アクティブ DPI インターフェース上で、アクティブ装置の特定のパケット フローを選択し、スタンバイ装置にオフロードします。DPI はスタンバイ装置で実行され、結果は同じインターフェースを介してアクティブ装置に返されます。それ以外の処理は、アクティブ装置で実行されます。

メモ：アクティブ/アクティブ DPI は、SuperMassive 9200、9400、および 9600 プラットフォームに含まれてり、拡張ライセンスがある NSA 5600 および NSA 6600 でのみサポートされます。ライセンス情報については、『*SonicOS の更新*』を参照してください。

アクティブ/アクティブ DPI HA 機能のメリット

アクティブ/アクティブ DPI では、スタンバイ装置で利用可能な未使用の CPU サイクルを活用しますが、トラフィックのやりとりは従来どおりにアクティブ装置で行われます。ネットワーク トラフィックの負荷は、アクティブ装置によって処理され、スタンバイ装置にはかかりません。また、DPI サービス以外のすべてのモジュールの処理はアクティブ装置でのみ行われます。

アクティブ/スタンバイおよびアクティブ/アクティブ DPI 機能の前提条件

このセクションでは、サポート対象プラットフォームの一覧を示し、装置を物理的に接続するための推奨事項と要件を紹介します。さらに、高可用性に必要な装置の登録、関連付け、ライセンス有効化の方法について説明します。

トピック:

- HA のサポート対象プラットフォームとライセンス (704 ページ)
- セキュリティ装置の物理的な接続 (706 ページ)
- アクティブ/アクティブ DPI のためのアクティブ/アクティブ DPI インターフェースの接続 (707 ページ)

HA のサポート対象プラットフォームとライセンス

「SonicWall セキュリティ装置で利用可能な HA ライセンス」テーブルに、SonicWall セキュリティ装置の購入時に付属するライセンスを示します。一部のプラットフォームでは、HA 機能の利用に追加ライセンスが必要です。

メモ：HA ライセンスは、セキュリティ装置ごとに有効にする必要があります。そのためには、MySonicWall で SonicOS 管理インターフェースから装置を登録するか、インターネット アクセスが利用できない場合は各装置にライセンス キーセットを適用します。

「SonicWall セキュリティ装置で利用可能な HA ライセンス」テーブルに、SonicWall セキュリティ装置の購入時に付属する HA ライセンスを示します。一部のプラットフォームでは、ステートフル同期やアクティブ/アクティブ DPI を利用するためには追加ライセンスが必要です。SonicOS 拡張ライセンスまたは高可用性ライセンスは、MySonicWall または SonicWall 再販業者から購入できます。

メモ：ステートフル高可用性ライセンスは、セキュリティ装置ごとに有効にする必要があります。そのためには、MySonicWall で SonicOS 管理インターフェースから装置を登録するか、インターネット アクセスが利用できない場合は各装置にライセンス キーセットを適用します。

SonicWall セキュリティ装置で利用可能な HA ライセンス

プラットフォーム	アクティブ/スタンバイ HA [a]	ステートフル HA	A/A クラスタリング	A/A DPI
SM 9600	付属	付属	付属	付属
SM 9400	付属	付属	付属	付属
SM 9200	付属	付属	付属	付属
NS*a* 9650	付属	付属	付属	付属
NS*a* 9450	付属	付属	付属	付属
NS*a* 9250	付属	付属	付属	付属
NS*a* 6650	付属	付属	拡張ライセンス	拡張ライセンス
NSA 6600	付属	付属	拡張ライセンス	拡張ライセンス
NS*a* 5650	付属	付属	拡張ライセンス	拡張ライセンス
NSA 5600	付属	付属	拡張ライセンス	拡張ライセンス
NS*a* 4650	付属	付属	拡張ライセンス	N/A
NSA 4600	付属	付属	拡張ライセンス	N/A
NS*a* 3650	付属	ステートフル HA ライセンス 拡張ライセンス	拡張ライセンス	N/A
NSA 3600	付属	ステートフル HA ライセンス 拡張ライセンス	拡張ライセンス	N/A
NS*a* 2650	付属	ステートフル HA ライセンス 拡張ライセンス	N/A	N/A
NSA 2600	付属	ステートフル HA ライセンス 拡張ライセンス	N/A	N/A
TZ600/TZ600 P	付属	拡張ライセンス ステートフル HA ライセンス	該当なし	N/A
TZ500/TZ500 W	付属	拡張ライセンス ステートフル HA ライセンス	該当なし	N/A
TZ400/TZ400 W	付属	N/A	N/A	N/A
TZ350/TZ350 W	付属	N/A	N/A	N/A
TZ300/TZ300 W /TZ300 P	付属	N/A	N/A	N/A
SOHO 250/SOHO 250 W	該当なし	N/A	N/A	N/A
SOHO W	N/A	N/A	N/A	N/A

a. N/A = 機能は利用不可

システム ライセンスは、「**管理 | 更新 > ライセンス**」で確認できます。このページには、MySonicWall へのログインやセキュリティ装置へのライセンスの適用を行う方法も用意されています。詳細については、『*SonicOS 6.5 更新*』を参照してください。

また、インターネットにアクセスできないセキュリティ装置がある HA ペアについてもライセンスを同期する方法があります。ネットワーク ポリシーの制約により SonicWall ライセンス サーバとの常時通信が許可されない場合は、ライセンス キーセットを使用してセキュリティ サービス ライセンスを

セキュリティ装置に手動で適用することができます。MySonicWall でセキュリティ装置を登録すると、そのセキュリティ装置用のライセンス キーセットが生成されます。新しいセキュリティ サービス ライセンスを追加する場合、キーセットが更新されます。ただし、このライセンスをセキュリティ装置に登録するまで、その装置でライセンスされたサービスを実行することはできません。

重要：インターネット接続なしで高可用性を提供する配備では、HA ペアの両方のセキュリティ装置にライセンス キーセットを適用する必要があります。

システム ライセンスは、「**管理 | 更新 > ライセンス**」で確認できます。このページには、MySonicWall へのログイン方法も用意されています。ライセンスについては、『*SonicOS 6.5 更新*』を参照してください。

重要：MySonicWall でセキュリティ装置を初めて登録する場合も、プライマリとセカンダリのセキュリティ装置でそれぞれの管理 IP アドレスにログインし、SonicOS 管理インターフェースから個別にセキュリティ装置を登録する必要があります。これにより、セカンダリ装置は SonicWall ライセンス サーバと同期され、関連付けられているプライマリ セキュリティ装置とライセンスを共有できるようになります。インターネットへのアクセスが制限されている場合は、共有するライセンスを手動で両方のセキュリティ装置に適用できます。

セキュリティ装置の物理的な接続

メモ：セキュリティ装置どうしを接続する完全な手順については、使用するセキュリティ装置の『*導入ガイド*』を参照してください。アクティブ/アクティブ クラスタ セキュリティ装置どうしを接続する手順については、「アクティブ/アクティブ クラスタリングでの HA ポートの接続 (723 ページ)」および「冗長ポート インターフェースの接続 (723 ページ)」を参照してください。

スパニング ツリー プロトコルを使用するイーサネット スイッチにプライマリ セキュリティ装置とセカンダリ セキュリティ装置を接続する場合は、SonicWall インターフェースが接続するスイッチ ポートのリンク アクティブ化時間の調整が必要になる場合があることに注意してください。例えば、Cisco Catalyst シリーズ スイッチでは、SonicWall セキュリティ装置のインターフェースに接続する各ポートで、**spanning tree port fast** をアクティブ化する必要があります。

高可用性機能を使用するには、影響を受ける SonicWall セキュリティ装置の間に物理的な接続を追加する必要があります。すべてのモードで、HA 制御および HA データ用の接続が必要です。アクティブ/アクティブ DPI には追加の接続インターフェースが必要です。

どのような高可用性配備でも、すべての装置の LAN および WAN ポートを適切なスイッチに物理的に接続する必要があります。

すべての装置の X0 インターフェースを同じブロードキャスト ドメインに接続することが重要です。そうしないと、トラフィックのフェイルオーバーは動作しません。また、X0 は既定の冗長 HA ポートになります。標準の高可用性制御リンクに障害が発生すると、装置間のハートビート通信には X0 が使用されます。X0 が同じブロードキャスト ドメインにない場合、高可用性制御リンクの障害時に両方の装置がアクティブになります。

ヒント：SonicOS セキュリティ装置では、HA 制御インターフェースに加えて、MGMT インターフェース越しの HA ペア間でハートビートを交換できるようになりました。

インターネットへの WAN 接続は、MySonicWall でセキュリティ装置を登録したり、ライセンス情報を同期したりする場合に役立ちます。ネットワーク ポリシーによって SonicWall ライセンス サーバとの常時通信が許可されていない場合を除き、WAN (X1) インターフェースを接続してから登録やライセンス処理を実行してください。

アクティブ/アクティブ DPI のためのアクティブ/アクティブ DPI インターフェースの接続

アクティブ/アクティブ DPI では、各 HA ペアまたはクラスタ ノード内の 2 台のセキュリティ装置間で少なくとも 1 つの追加インターフェース (**アクティブ/アクティブ DPI インターフェース**と呼ばれます) を物理的に接続する必要があります。接続されるインターフェースは、両方のセキュリティ装置で同じ番号、かつ「**管理 | システム セットアップ | ネットワーク > インターフェース**」で最初は未使用、未定義のインターフェースとして表示されていなければなりません。例えば、X5 が未定義のインターフェースである場合、プライマリ装置の X5 をセカンダリ装置の X5 に接続できます。アクティブ/アクティブ DPI を有効にした後、接続されたインターフェースは「**HA データリンク**」というゾーン割り当てを持ちます。

アクティブ/アクティブ DPI インターフェース上で、アクティブ装置の特定のパケット フローを選択し、スタンバイ装置にオフロードします。DPI はスタンバイ装置で実行され、結果は同じインターフェースを介してアクティブ装置に返されます。

必要に応じて、アクティブ/アクティブ DPI によるポート冗長化のために、各 HA ペアの 2 台のセキュリティ装置間で 2 番目の アクティブ/アクティブ DPI インターフェースを物理的に接続することもできます。このインターフェースは、1 番目のアクティブ/アクティブ DPI インターフェースに障害が発生した場合、アクティブ/アクティブ DPI 処理時の 2 台の装置間でのデータ転送を引き継ぐことになります。

アクティブ/アクティブ DPI のためのアクティブ/アクティブ DPI インターフェースを接続するには:

1. HA ペアのセキュリティ装置間の追加接続に使用するインターフェースを決定します。各セキュリティ装置で同じインターフェースを選択する必要があります。
2. SonicOS 管理インターフェースで、「**管理 | システム セットアップ | ネットワーク > インターフェース**」に移動して、目的のアクティブ/アクティブ DPI インターフェースの「**ゾーン**」が「**未定義**」になっていることを確認します。
3. 標準のイーサネット ケーブルを使用して、2 つのインターフェースを相互に直接接続します。
4. 必要に応じて、アクティブ/アクティブ DPI によるポート冗長化のために、各 HA ペアの 2 台のセキュリティ装置間で 2 番目の アクティブ/アクティブ DPI インターフェースを物理的に接続することもできます。

メンテナンス

トピック:

- HA 関連付けの削除 (707 ページ)
- SonicWall セキュリティ装置の交換 (708 ページ)

HA 関連付けの削除

MySonicWall では、2 台の SonicWall セキュリティ装置間の関連付けをいつでも削除できます。セキュリティ装置を交換する場合、またはネットワークを再設定する場合は、既存の HA 関連付けの削除が必要になる場合があります。例えば、SonicWall セキュリティ装置の 1 台が故障した場合、それを交換する必要があります。または、ネットワークを再設定した後、HA プライマリ装置をセカンダリ (HA

セカンダリ) セキュリティ装置と入れ替えることが必要になる場合があります。このような場合は、最初に既存の HA 関連付けを削除した後、新しいセキュリティ装置を使用する新しい関連付けを作成するか、または 2 台の装置の親子関係を変更する必要があります (「SonicWall セキュリティ装置の交換 (708 ページ)」を参照してください)。

2 台の登録済み SonicWall セキュリティ装置の関連付けを削除するには、以下の手順に従います。

1 MySonicWall にログインします。

2 左側にあるナビゲーション バーで、「**製品管理**」を選択します。

3 「**製品管理**」ページの「**登録されている製品**」で、下にスクロールして関連付けを削除するセカンダリセキュリティ装置を探します。製品の**名前**または**シリアル番号**を選択します。

4 「**サービス管理 - 関連する製品**」ページで、「**関連済み製品**」セクションのすぐ上にある「**親製品**」セクションまで下にスクロールします。

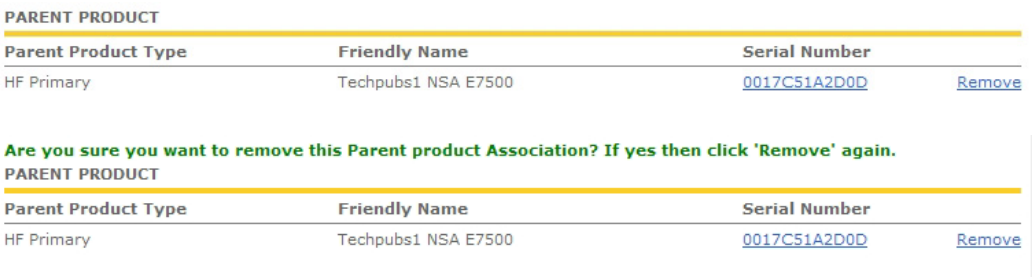
5 「**親製品**」の下で、このセキュリティ装置の関連付けを削除するには、以下の手順に従います。

   a 「**削除**」を選択します。

   b ページが再ロードされるのを待ちます。

   c 下にスクロールします。

   d もう一度「**削除**」を選択します。


PARENT PRODUCT

Parent Product Type	Friendly Name	Serial Number	
HF Primary	Techpubs1 NSA E7500	0017C51A2D0D	Remove

Are you sure you want to remove this Parent product Association? If yes then click 'Remove' again.

PARENT PRODUCT

Parent Product Type	Friendly Name	Serial Number	
HF Primary	Techpubs1 NSA E7500	0017C51A2D0D	Remove

SonicWall セキュリティ装置の交換

保証期間中に SonicWall セキュリティ装置のハードウェアが故障した場合は、SonicWall が装置を交換します。その場合、ユーザは MySonicWall で故障したセキュリティ装置を含む HA 関連付けを削除して、新しい装置を含む新しい HA 関連付けを追加する必要があります。SonicWall テクニカル サポートに連絡して交換を手配すると (RMA と呼ばれます)、通常は、サポートがこの作業を行います。

機器ラックの故障した装置を新しいセキュリティ装置に交換した後、ユーザは MySonicWall および SonicOS の設定を更新できます。

故障した HA プライマリ装置の交換は、HA セカンダリ装置の交換と若干異なります。以降のセクションでは、両方の手順について説明します。

- HA プライマリ装置の交換 (709 ページ)
- HA セカンダリ装置の交換 (709 ページ)

HA プライマリ装置の交換

HA プライマリ装置を交換するには、以下の手順に従います。

1 残っている SonicOS セキュリティ装置 (セカンダリ装置) の SonicWall 管理インターフェースの「高可用性」ページで、「**高可用性を有効にする**」をオフにして機能を無効にします。

2 「**高可用性を有効にする**」をオンにします。

これで、古いセカンダリ装置がプライマリ装置になります。そのシリアル番号が、「プライマリ SonicWall シリアル番号」フィールドに自動的に表示されます。

3 交換装置のシリアル番号を「**セカンダリ SonicWall シリアル番号**」フィールドに入力します。

4 「**設定の同期**」を選択します。

5 MySonicWall で、古い HA 関連付けを削除します。「HA 関連付けの削除 (707 ページ)」を参照してください。

6 MySonicWall で、交換した SonicWall セキュリティ装置を登録します。また、新しいプライマリ (元のセカンダリ) 装置を HA プライマリとし、交換装置を HA セカンダリとして、HA 関連付けを作成します。『*SonicOS の更新*』を参照してください。

7 以前の HA ペアから新しい HA ペアにセキュリティ サービス ライセンスを転送するには、SonicWall テクニカル サポートに問い合わせてください。

ライセンスは HA ペアのプライマリ装置にリンクされているので、HA プライマリ装置が故障したときは、このステップが必要になります。

HA セカンダリ装置の交換

HA セカンダリ装置を交換するには、以下の手順に従います。

1 MySonicWall で、古い HA 関連付けを削除します (「HA 関連付けの削除 (707 ページ)」を参照)。

2 MySonicWall で、交換用の SonicWall セキュリティ装置を登録します。

3 交換装置を HA セカンダリとして使用して、元の HA プライマリとの HA 関連付けを作成します (「HA プライマリ装置の交換 (709 ページ)」を参照)。

アクティブ/アクティブ クラスタリング

メモ： アクティブ/アクティブ クラスタリングは、NSA 3600 以降のセキュリティ装置でサポートされます。「SonicWall セキュリティ装置で利用可能な HA ライセンス」テーブルおよび 「A/A クラスタリングのライセンス要件」テーブルを参照してください。

アクティブ/アクティブ クラスタリングについて

アクティブ/アクティブ クラスタは、最大 4 つのクラスタ ノードのグループとして形成され、複数のアクティブ装置 (複数のゲートウェイとして動作) が DPI の処理やネットワーク負荷を分散しながらトラフィックを処理します。クラスタ ノードは、ステートフル HA ペアか、標準的なフェイルオーバーを設定したステートレス HA ペアか、単一のスタンドアロン装置 (この場合、ステートフル フェイルオーバーおよびアクティブ/アクティブ DPI は利用できない) によって構成できます。動的な状態の同

期は、ステートフル HA ペアのクラスタ ノードでのみ利用できます。従来の SonicWall 高可用性プロトコルまたはステートフル HA プロトコルは、クラスタ ノード内の通信、つまり HA ペアである装置間の通信で使用されます。

クラスタ ノードがステートフル HA ペアである場合、パフォーマンス向上のためにアクティブ/アクティブ DPI をクラスタ ノード内で有効にできます。

アクティブ/アクティブ クラスタリングを使用すると、特定のトラフィック フローをクラスタ内の各ノードに割り当て、負荷分散や冗長性を実現したり、単一障害点のないスループットの大幅向上をサポートしたりできます。

一般的な推奨セットアップには、2 つのクラスタ ノードとして設定された、同一 SonicWall モデルである 4 つのセキュリティ装置が含まれ、各クラスタ ノードは 1 つのステートフル HA ペアを構成します。より大規模な配備では、4 つのクラスタ ノード (または HA ペア) として設定された、8 つのセキュリティ装置をこのクラスタに含めることができます。各クラスタ ノード内では、単一障害点でのデータ損失がゼロとなるシームレスなフェイルオーバーを実現するために、ステートフル HA 機能によって同期された動的な状態が維持されます。ステートフル HA は、必須ではありませんが、フェイルオーバー時に最高のパフォーマンスを得るために強く推奨されます。

負荷分散は、異なるクラスタ ノードをネットワーク内の別々のゲートウェイとして設定することで実現されます。通常、この機能はアクティブ/アクティブ クラスタのダウンストリーム側にある別の機器 (DHCP サーバ、ルータなど) によって処理されます。

1 つのクラスタ ノードを単独のセキュリティ装置とし、2 つのセキュリティ装置を使用してアクティブ/アクティブ クラスタのセットアップを構築することもできます。この配備のセキュリティ装置の 1 つに障害が発生した場合、クラスタ ノード内のどちらのセキュリティ装置にも HA セカンダリが存在しないので、フェイルオーバーはステートフルではありません。

アクティブ/アクティブ クラスタリングでは、冗長性がいくつかのレベルで実現されます。

- クラスタによって冗長なクラスタ ノードが実現され、障害が発生した場合、各クラスタ ノードは他のどのクラスタ ノードのトラフィック フローも処理できます。
- クラスタ ノードはステートフル HA ペアによって構成され、このペアでは障害の発生時にセカンダリ セキュリティ装置がプライマリ装置の役割を引き受けることができます。
- 未使用のポートが別のポートのセカンダリとして割り当てられるポート冗長化では、別のセキュリティ装置またはノードへのフェイルオーバーを必要とせずにインターフェース レベルでの保護が実現されます。
- アクティブ/アクティブ DPI を有効にすると、各クラスタ ノード内のスループットを向上できます。

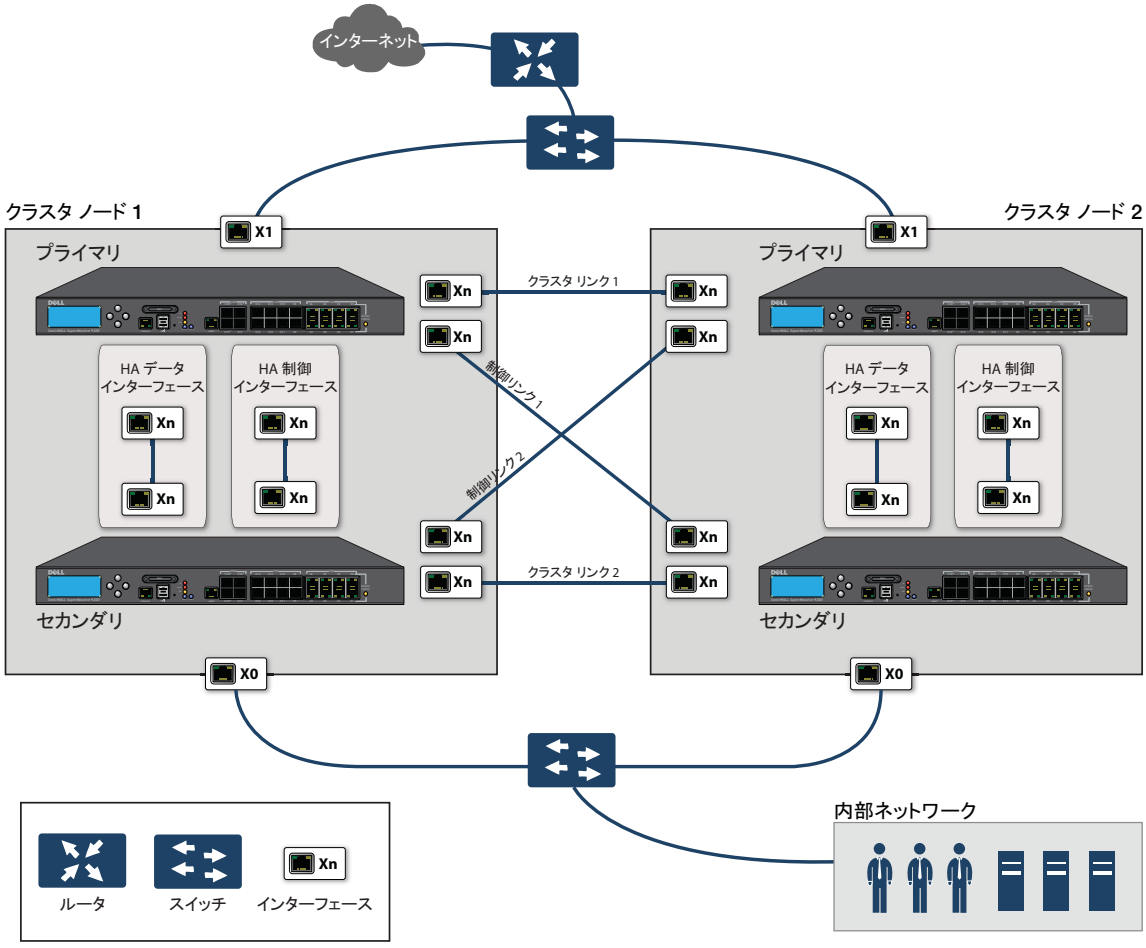
トピック:

- 例: アクティブ/アクティブ クラスタリング - 装置 4 台の配備 (711 ページ)
- 例: アクティブ/アクティブ クラスタリング - 装置 2 台の配備 (712 ページ)
- アクティブ/アクティブ クラスタリングのメリット (712 ページ)
- アクティブ/アクティブ クラスタリングの動作 (713 ページ)
- アクティブ/アクティブ クラスタリングでサポートされる機能 (719 ページ)

例: アクティブ/アクティブ クラスタリング - 装置 4 台の配備

「装置 4 台によるアクティブ/アクティブ クラスタ」に 4 台の装置によるクラスタを示します。各クラスタ ノードには 1 つの HA ペアが含まれています。4 台のセキュリティ装置すべての指定された HA ポートは同じ レイヤ 2 スイッチに接続されています。これらのポートは、SVRRP 経由で送信されるクラスタ ノードの管理と監視に関する状況メッセージや、設定の同期に使用されます。また、各 HA ペア内の 2 台の装置は、別のインターフェース (図中の Xn インターフェース) を使用して相互に接続されています。これは、アクティブ/アクティブ DPI で必要となるアクティブ/アクティブ DPI インターフェースです。アクティブ/アクティブ DPI が有効になっている場合、特定のパケットは DPI 処理のために HA ペアのスタンバイ装置にオフロードされます。

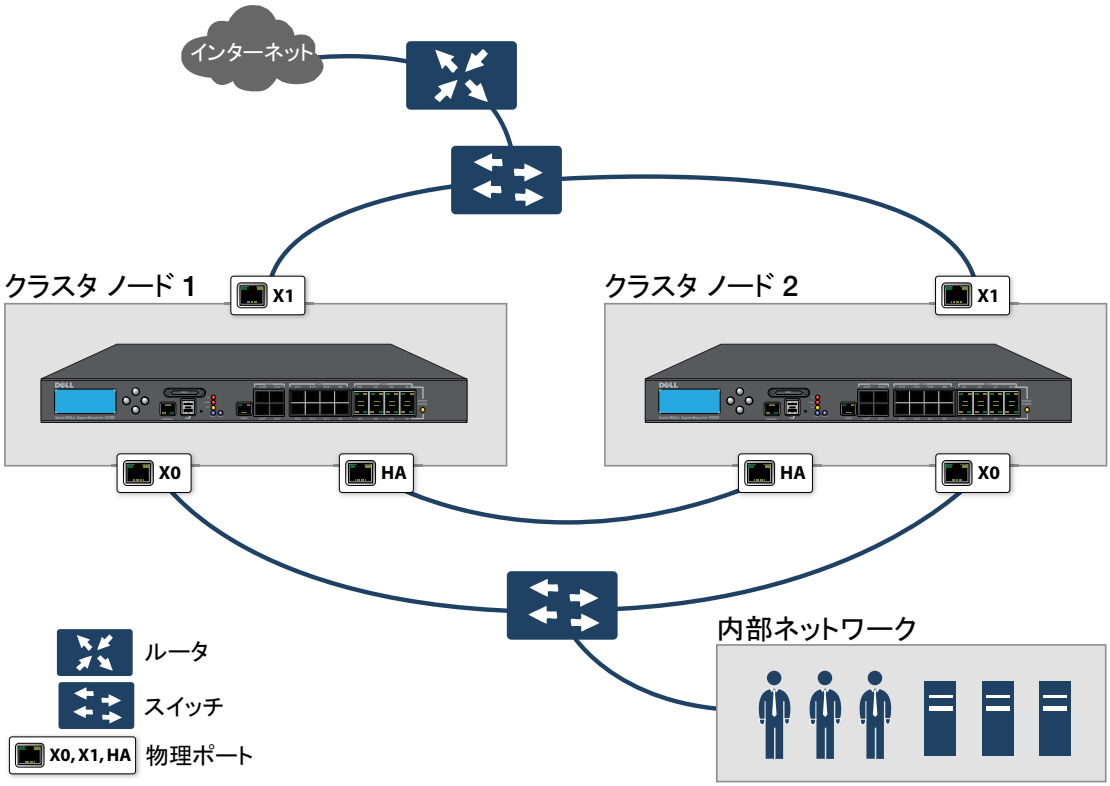
装置 4 台によるアクティブ/アクティブ クラスタ



例: アクティブ/アクティブ クラスタリング - 装置 2 台の配備

「装置 2 台によるアクティブ/アクティブ クラスタ」に 2 台の装置によるクラスタを示します。装置 2 台のクラスタでは、HA ペアは使用されません。代わりに、各クラスタ ノードには 1 台のセキュリティ装置のみが含まれます。2 台のセキュリティ装置の指定された HA ポートは、クロスオーバー ケーブルを使用して相互に直接接続されます。SonicWall Virtual Router Redundancy Protocol (SVRRP) では、この HA ポート接続を使用して、クラスタ ノードの管理と監視に関する状況メッセージを送信します。SVRRP 管理メッセージはマスター ノードから送信され、監視情報はクラスタ内のすべてのセキュリティ装置から送信されます。HA ポート接続は、クラスタ ノード間での設定の同期にも使用されます。

装置 2 台によるアクティブ/アクティブ クラスタ



アクティブ/アクティブ クラスタリングのメリット

アクティブ/アクティブ クラスタリングのメリットは次のとおりです。

- クラスタ内のすべてのセキュリティ装置を利用して、最大のスループットを引き出せる
- アクティブ/アクティブ DPI と併用すると、プロセッサ使用率の高い、IPS、GAV、アンチスパイウェア、およびアプリケーション ルールの各サービスの同時処理を各 HA のスタンバイ セキュリティ装置で実行しつつ、その他の処理をアクティブ セキュリティ装置で実行できる
- 特定のトラフィック フローをクラスタ内の各ノードに割り当てることで、負荷分散がサポートされる
- クラスタ内のすべてのノードで他のノードに対する冗長性を実現し、他のノードがダウンした場合に必要に応じてトラフィックを処理できる

- インターフェースの冗長化により、フェイルオーバーを必要とせずにトラフィック フローに対するセカンダリ要素を実現できる
- フル メッシュと非フル メッシュの両方の配備をサポートできる

アクティブ/アクティブ クラスタリングの動作

アクティブ/アクティブ クラスタリングを説明するために、いくつかの重要な概念を導入します。

トピック:

- クラスタ ノードについて (713 ページ)
- クラスタについて (713 ページ)
- 仮想グループについて (715 ページ)
- SVRRP について (717 ページ)
- フェイルオーバーについて (717 ページ)
- アクティブ/アクティブ クラスタリングによる DPI について (718 ページ)
- アクティブ/クラスタリングでの高可用性監視について (718 ページ)

クラスタ ノードについて

アクティブ/アクティブ クラスタは、クラスタ ノードの集まりによって形成されます。クラスタ ノードは、ステートフル HA ペア、ステートレス HA ペア、または単一のスタンドアロン装置によって構成できます。動的な状態の同期は、ステートフル HA ペアのクラスタ ノードでのみ利用できます。従来の SonicWall 高可用性プロトコルまたはステートフル HA プロトコルは、クラスタ ノード内の通信、つまり HA ペアである装置間の通信で使用されます。

クラスタ ノードがステートフル HA ペアである場合、パフォーマンス向上のためにアクティブ/アクティブ DPI をクラスタ ノード内で有効にできます。

クラスタについて

クラスタ内のすべてのセキュリティ装置は、同じ製品モデルで、同じファームウェア バージョンを実行している必要があります。

クラスタ内では、すべてのセキュリティ装置が相互に接続され、通信を行います。「アクティブ/アクティブ 2 ノード クラスタ」を参照してください。クラスタ ノード間の通信では、SonicWall Virtual Router Redundancy Protocol (SVRRP) という新しいプロトコルが使用されます。クラスタ ノードの管理と監視に関する状況メッセージは、SVRRP を使用して送信されます。

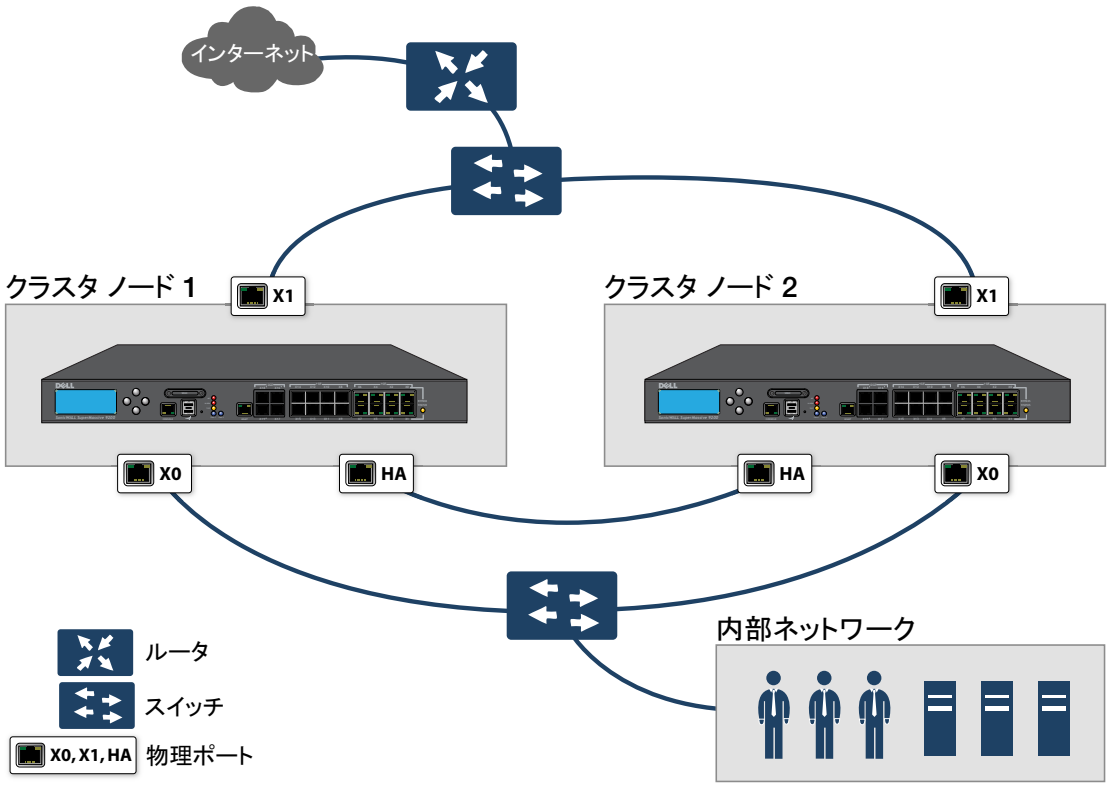
すべてのクラスタ ノードは同じ設定を共有し、その設定はマスター ノードによって同期されます。マスター ノードは、クラスタ内の他のノードに対するファームウェアの同期も担当します。HA ポート接続は、設定およびファームウェアの更新の同期に使用されます。

動的な状態は、クラスタ ノード間では同期されず、クラスタ ノード内でのみ同期されます。クラスタ ノードに HA ペアが含まれる場合、そのクラスタ ノード内でステートフル HA を有効にでき、必要に応じて動的な状態の同期とステートフル フェイルオーバーの利点が得られます。クラスタ ノード全体に障害が発生した場合、フェイルオーバーはステートレスになります。これは、以前から存在するネットワーク接続の再構築が必要になることを意味します。例えば、Telnet および FTP セッションを再確立し、VPN トンネルを再ネゴシエートする必要があります。

フェイルオーバーの仕組みについては、「フェイルオーバーについて (717 ページ)」を参照してください。

現在、1 つのクラスタ内のクラスタ ノードは最大 4 つに制限されています。各クラスタ ノードが HA ペアである場合、各クラスタには 8 つのセキュリティ装置が含まれることになります。

アクティブ/アクティブ 2 ノード クラスタ



クラスタ内で許可される動作

許可される管理動作の種類は、クラスタ内のセキュリティ装置の状態によって異なります。マスター ノードのアクティブ セキュリティ装置上で適切な権限を持つ管理者ユーザは、すべての設定動作など、あらゆる動作を実行できます。非マスター ノードのアクティブ セキュリティ装置では一部の動作が許可されており、スタンバイ状態のセキュリティ装置では許可されている動作がさらに少なくなります。クラスタ内の非マスター ノードのアクティブ セキュリティ装置やスタンバイ セキュリティ装置で許可されている動作の一覧については、「許可される管理動作」テーブルを参照してください。

許可される管理動作

管理動作	アクティブな非マスター	スタンバイ
読み取り専用の動作	許可	許可
MySonicWall での登録	許可	許可
SonicWall ライセンス マネージャとのライセンスの同期	許可	許可
「**調査	ツール	システム診断**」の診断ツール (これらのツールの詳細については、『*SonicOS 調査*』を参照してください)。	許可	許可
パケット監視	許可	許可

許可される管理動作 (続き)

管理動作	アクティブな非マスター	スタンバイ
HA による設定の同期 (ノード内の HA ピアに対して設定を同期)	不許可	不許可
HA によるファームウェアの同期 (ノード内の HA ピアに対してファームウェアを同期)	許可	不許可
ユーザの管理ログアウト	許可	不許可
認証のテスト (LDAP、RADIUS、認証エージェントなどのテスト)	許可	不許可

仮想グループについて

アクティブ/アクティブ クラスタリングでは、仮想グループの概念もサポートしています。同時に最大 4 つの仮想グループがサポートされます。

仮想グループは、クラスタの設定で設定されたすべてのインターフェースに対する仮想 IP アドレスの集まりです (未使用/未割り当てのインターフェースに仮想 IP アドレスはありません)。アクティブ/アクティブ クラスタリングが初めて有効になったときに、そのセキュリティ装置のインターフェースに対して設定された IP アドレスは、仮想グループ 1 の仮想 IP アドレスに変換されます。そのため、仮想グループ 1 には、X0、X1、およびゾーンに対して設定および割り当てが行われているその他のあらゆるインターフェースの仮想 IP アドレスが含まれることになります。

仮想グループは、トラフィック フローの論理グループが障害発生時の状況に応じてあるノードから別のノードへのフェイルオーバーが可能であるという点で、フェイルオーバー コンテキスト内のトラフィック フローの論理的なグループとも見なせます。各仮想グループには、オーナーとして機能するクラスタ ノードが 1 つ、スタンバイとして機能するクラスタ ノードが 1 つ以上存在します。1 つの仮想グループは一度に 1 つのクラスタ ノードによってのみ所有され、そのクラスタ ノードはその仮想グループに関連付けられているすべての仮想 IP アドレスのオーナーになります。仮想グループ 1 のオーナーは、マスター ノードとして指定され、クラスタ内の他のノードに対する設定とファームウェアの同期を担当します。仮想グループのオーナー ノードが障害が発生した場合は、スタンバイ ノードの 1 つがオーナーになります。

アクティブ/アクティブ クラスタリングの設定の一環として、クラスタ内の他のセキュリティ装置のシリアル番号を SonicOS 管理インターフェースに入力し、スタンバイの順序を示す順位付け番号をそれぞれに割り当てます。アクティブ/アクティブ クラスタリングの設定の適用時には、追加のクラスタ ノード数に応じて、最大 3 つ追加仮想グループを作成できますが、これらの仮想グループについては仮想 IP アドレスが作成されません。こうした仮想 IP アドレスは、「**管理 | システム セットアップ | ネットワーク > インターフェース**」で、設定する必要があります。

仮想グループのオーナーシップ (どのクラスタ ノードを仮想グループのオーナーにするか) を決定する際には、次の 2 つの要因を考慮します。

- **クラスタ ノードのランク** - このランクは、仮想グループのオーナーシップを引き継ぐ各ノードの優先順位を指定するために、SonicOS 管理インターフェースで設定します。
- **クラスタ ノードの仮想グループ リンク重み** - これは、起動状態にあって仮想 IP アドレスが設定されている、仮想グループ内のインターフェースの数です。

あるクラスタ内に設定されているクラスタ ノード数が 2 を超えている場合、仮想グループのオーナーシップを取得できる最適なクラスタ ノードがこれらの要因によって決定されます。2 つのクラスタ ノードを持つクラスタでは、一方のノードに障害が発生すると、必然的にもう一方のノードがオーナーシップを取得することになります。

仮想グループのリンクの状態とオーナーシップの状態をクラスタ内のすべてのクラスタ ノードに伝えるために、SVRRP が使用されます。

仮想グループ 1 のオーナーは、マスター ノードに指定されます。設定の変更やファームウェアの更新はマスター ノードでのみ許可され、マスター ノードは SVRRP を使用して、設定とファームウェアの同期をクラスタ内のすべてのノードに対して行います。特定のインターフェースでは、仮想グループ 1 の仮想 IP アドレスを設定しないと、他の仮想グループを設定できません。

負荷分散と複数のゲートウェイのサポート

仮想グループのトラフィックは、オーナー ノードによってのみ処理されます。仮想グループに到着したパケットは、その同じ仮想グループ上のセキュリティ装置から外に出ます。通常の設定では、各クラスタ ノードは、仮想グループを持つので、1 つの仮想グループに対応したトラフィックを処理します。

この仮想グループの機能は、冗長化された複数ゲートウェイのモデルをサポートしています。2 つのクラスタ ノードを持つ配備では、X0 による仮想グループ 1 の IP アドレスをあるゲートウェイに、X0 による仮想グループ 2 の IP アドレスを別のゲートウェイにすることができます。トラフィックを各ゲートウェイにどのように割り当てるかは、ネットワーク管理者に委ねられます。例えば、ゲートウェイの割り当てを直接的に接続されたクライアント ネットワーク上の各 PC に配布する気の利いた DHCP サーバを使用することも、ポリシー ベースのルートをダウンストリームのルータで使用することもできます。

アクティブ/アクティブ クラスタリングが有効になると、SonicOS の内部 DHCP サーバはオフになり、有効にできなくなります。DHCP サーバを必要とするネットワークでは、ゲートウェイの割り当てを配布できるように、複数のゲートウェイを認識する外部 DHCP サーバを使用できます。

メモ：アクティブ/アクティブ クラスタリングが有効になると、SonicOS の内部 DHCP サーバはオフになります。

関連する設定ページへの影響

アクティブ/アクティブ クラスタリングが初めて有効になったときに、すべての設定済みインターフェースの既存 IP アドレスは、仮想グループ 1 の仮想 IP アドレスに自動的に変換されます。仮想グループ 1 または任意の仮想グループが作成されると、既定のインターフェース オブジェクトが、仮想 IP アドレスに対して適切な名前 (仮想グループ 1、仮想グループ 2 など) で作成されます。同じインターフェースに複数の仮想 IP アドレス (設定される仮想グループごとに 1 つ) を持たせることができます。こうした仮想 IP アドレスは、「**管理 | システム セットアップ | ネットワーク > インターフェース**」で確認できます。

メモ：アクティブ/アクティブ クラスタ内のすべてのクラスタ ノードは、同じ設定を共有します。

仮想 MAC アドレスは、インターフェース上の各仮想 IP アドレスと関連付けられ、Sonic OS によって自動的に生成されます。仮想 MAC アドレスは `00-17-c5-6a-XX-YY` という形式で作成されます。ここで、`XX` はインターフェース番号 (ポート X3 の場合は `03`)、`YY` は内部グループ番号 (仮想グループ 1 の場合は `00`、仮想グループ 2 の場合は `01`) です。

メモ：アクティブ/アクティブの仮想 MAC アドレスは、高可用性機能の仮想 MAC アドレスとは異なります。高可用性の仮想 MAC アドレス機能は、アクティブ/アクティブ クラスタリングが有効な場合にはサポート されません。

影響を受ける、各仮想グループのインターフェース オブジェクトに対し、NAT ポリシーが自動的に作成されます。こうした NAT ポリシーは、特定のインターフェースに対する既存の NAT ポリシーを、対応する仮想インターフェースにまで拡大します。これらの NAT ポリシーは、「**管理 | ポリシー | ルール > NAT ポリシー**」で確認できます。追加の NAT ポリシーは、必要に応じて設定したり、それが適切な場合にはある仮想グループに特有のものにしたりできます。NAT ポリシーについては、『*SonicOS ポリシー*』を参照してください。

アクティブ/アクティブ クラスタリングが有効になった後は、VPN ポリシー追加時の設定で仮想グループ番号を選択する必要があります。

SVRRP について

アクティブ/アクティブ クラスタ内のクラスタ ノード間の通信では、SonicWall Virtual Router Redundancy Protocol (SVRRP) という新しいプロトコルが使用されます。クラスタ ノードの管理と監視に関する状況メッセージは、SVRRP を使用してアクティブ/アクティブ クラスタ リンクを介して送信されます。

SVRRP は、設定の変更、ファームウェアの更新、およびシグネチャの更新をマスター ノードからクラスタ内のすべてのノードに対して同期するためにも使用されます。各クラスタ ノードでは、アクティブな装置のみが SVRRP メッセージを処理します。

アクティブ/アクティブ クラスタ リンクに障害が発生した場合には、SVRRP ハートビート メッセージが X0 インターフェースで送信されます。ただし、アクティブ/アクティブ クラスタ リンクがダウンしている間は、設定の同期が行われません。ファームウェアまたはシグネチャの更新、ポリシーの変更、およびその他の設定変更は、アクティブ/アクティブ クラスタ リンクが修復されるまで、他のクラスタ ノードに対して同期できません。

フェイルオーバーについて

アクティブ/アクティブ クラスタリングが有効な場合に発生しうるフェイルオーバーには次の 2 種類があります。

高可用性フェイルオーバー	HA ペア内で、セカンダリ装置がプライマリ装置の処理を引き継ぎます。HA ペアでステートフル HA が有効になっている場合、フェイルオーバーはネットワーク接続の中断なしに行われます。
アクティブ/アクティブ フェイルオーバー	仮想グループのオーナー ノード内にあるすべての装置で障害が発生した場合は、仮想グループのスタンバイ ノードが仮想グループのオーナーシップを引き継ぎます。アクティブ/アクティブ フェイルオーバーは、仮想グループのオーナーシップをあるクラスタ ノードから別のクラスタ ノードに渡します。仮想グループのオーナーになるクラスタ ノードは、その仮想グループと関連付けられているすべての仮想 IP アドレスのオーナーにもなり、対応する仮想 MAC アドレスの使用を開始します。 アクティブ/アクティブ フェイルオーバーはステートレスです。つまり、ネットワーク接続はリセットされ、VPN トンネルの再ネゴシエートが必要になります。レイヤ 2 ブロードキャストによってトポロジの変更がネットワーク機器に通知され、仮想グループの新しいオーナーとなったクラスタ ノードが新たに所有した仮想 IP アドレスに対する仮想 MAC アドレスによって ARP 要求を生成します。これにより、フェイルオーバーの処理は大幅に簡素化されます。接続されているスイッチのみが学習テーブルを更新すれば済むからです。その他すべてのネットワーク機器は、引き続き同じ仮想 MAC アドレスを使用します。仮想 IP アドレスと仮想 MAC アドレスのマッピングは保持されているので、ARP テーブルを更新する必要はありません。

高可用性 (HA) フェイルオーバーとアクティブ/アクティブ フェイルオーバーのどちらも可能な場合には、次の理由により、HA フェイルオーバーがアクティブ/アクティブ フェイルオーバーよりも優先されます。

- HA フェイルオーバーはステートフルにできるのに対し、アクティブ/アクティブ フェイルオーバーはステートレスである。

- HA ペアのスタンバイ セキュリティ装置は、負荷が軽く、必要な処理の引き継ぎに使用できるリソースがあるのに対し、アクティブ/アクティブ DPI が有効な場合はスタンバイ装置が既に DPI トラフィックを処理している可能性がある。代替のクラスタ ノードは、既に相当な量のトラフィックを処理している場合があり、フェイルオーバー後に過負荷状態になる可能性がある。

アクティブ/アクティブ フェイルオーバーは、必ずアクティブ/アクティブの先制モードで行われます。先制モードでは、2 つのクラスタ ノード間でのフェイルオーバー後に、仮想グループの元のオーナー ノードが稼働状態に復元されたことが確認されると、そのノードがスタンバイ ノードからアクティブの役割を取り戻すことになります。すべての仮想 IP インターフェースが起動していて 2 つのクラスタ ノード間でリンクの重みが同じ場合、元のオーナーは、順位が高いため、仮想グループでの優先度が高くなります。

アクティブ/アクティブ クラスタリングによる DPI について

アクティブ/アクティブ DPI は、アクティブ/アクティブ クラスタリングと併用できます。アクティブ/アクティブ DPI が有効になっている場合、DPI 処理には HA ペアのスタンバイ セキュリティ装置が利用されます。

アクティブ/アクティブ クラスタのパフォーマンスを向上するために、アクティブ/アクティブ DPI を有効にすることをお勧めします。アクティブ/アクティブ DPI は、HA ペアのスタンバイ セキュリティ装置を活用して精密パケット検査 (DPI) を処理するからです。

アクティブ/クラスタリングでの高可用性監視について

アクティブ/アクティブ クラスタリングが有効になっている場合、各クラスタ ノードの HA ペアでは HA 監視の設定がサポートされます。HA 監視機能は、以前のバージョンと首尾一貫しています。HA 監視は、物理/リンク監視と論理/プローブ監視の両方で設定できます。マスター ノードにログインした後、「**管理 | システム セットアップ | 高可用性 > 監視設定**」で、監視設定をノードごとに追加する必要があります。

メモ：「**高可用性 > 監視設定**」は、クラスタ全体ではなく、ログインしている HA ペアのみに適用されます。

物理インターフェース監視により、監視対象インターフェースのリンク検出が有効になります。このリンクの検出は、リンクの動作状態を判断するために物理層で行われます。

物理インターフェース監視が有効になっている場合は、論理監視の有効/無効に関係なく、HA フェイルオーバーがアクティブ/アクティブ フェイルオーバーよりも優先されます。アクティブ装置でリンクに障害が発生するかポートが切断されると、その HA ペアのスタンバイ装置がアクティブになります。

メモ：仮想 IP アドレスが設定されているインターフェースの場合、アクティブ/アクティブの物理監視は暗黙的であり、これを使用して仮想グループ リンク重みが計算されます。これらのインターフェースでは、物理監視を無効にできません。この点が HA 監視との違いです。

論理監視とは、SonicOS を設定して接続先ネットワークの 1 つ以上に存在する信頼性の高い機器を監視することです。HA ペアのアクティブな装置がこの機器との定期的な通信に失敗すると、スタンバイ装置へのフェイルオーバーが実行されます。HA ペアのどちらの装置もこの機器に接続できない場合は、この機器に問題があると見なされ、フェイルオーバーは行われません。

物理監視と論理監視のどちらも無効になっている場合は、リンクの障害発生時またはポートの切断時にアクティブ/アクティブ フェイルオーバーが行われます。

「**管理 | システム セットアップ | 高可用性 > 監視設定**」で設定されるプライマリおよびセカンダリ IP アドレスは、LAN または WAN インターフェース上で設定でき、以下に示す複数の目的に使用されます。

- 装置の状態がアクティブかスタンバイかにかかわらず、各装置の固有の管理アドレスとして使用 (すべての物理インターフェース上でサポートされている)
- スタンバイ状態の装置と SonicWall ライセンス サーバの間のライセンスの同期用
- 論理監視中に送出されるプローブ Ping の送信元 IP アドレス

HA ペアの両方の装置に管理 IP アドレスを設定すると、管理のために各装置に個別にログインできます。監視 IP アドレスのいずれかに送信された管理目的ではないトラフィックは無視されます。プライマリおよびセカンダリの セキュリティ装置の一意の LAN IP アドレスは、アクティブ ゲートウェイとしては機能できません。内部 LAN に接続されたすべてのシステムは、ゲートウェイとして仮想 LAN IP アドレスを使用する必要があります。

メモ：HA 監視/管理 IP アドレスを WAN インターフェースのみに設定する場合、仮想 IP アドレスが設定されているすべての WAN インターフェースに設定する必要があります。

セカンダリ装置の管理 IP アドレスを使用すると、SonicWall ライセンス サーバとライセンスを同期できます。このサーバは、HA ペア単位ではなくセキュリティ装置単位でライセンスを管理します。HA 関連付けを作成する前にスタンバイ装置が MySonicWall に登録済みであっても、管理 IP アドレスからセカンダリ セキュリティ装置にアクセスしている間は、「**管理 | 更新 | ライセンス**」上のリンクを使用して SonicWall サーバに接続する必要があります。これにより、スタンバイ装置と SonicWall ライセンス サーバとの間のライセンス (アクティブ/アクティブ クラスタリング、ステートフル HA などのライセンス) の同期が可能になります。

論理監視の使用時には、指定された論理監視対象 IP アドレスを送信先とした Ping が、HA ペアのプライマリおよびセカンダリの SonicWall から実行されます。「プライマリ IP アドレス」または「セカンダリ IP アドレス」のフィールドに設定された IP アドレスは、Ping の送信元 IP アドレスとして使用されます。両方が送信先への Ping に成功した場合、フェイルオーバーは発生しません。両方が送信先への Ping に失敗した場合、SonicWall は、SonicWall ではなく送信先に問題があると見なし、フェイルオーバーは発生しません。しかし、一方の SonicWall が送信先への Ping に成功し、もう一方の SonicWall が失敗した場合は、Ping に成功したほうの SonicWall へのフェイルオーバーが行われます。

「**管理 | システム セットアップ | 高可用性 > 監視設定**」での設定タスクは、プライマリ装置で実行された後、セカンダリ装置に対して自動的に同期されます。

アクティブ/アクティブ クラスタリングでサポートされる機能

トピック:

- 注意 (719 ページ)
- 下位互換性 (720 ページ)
- SonicPoint の互換性 (720 ページ)
- WAN 負荷分散の互換性 (720 ページ)
- ルーティング トポロジとプロトコル互換性 (721 ページ)

注意

アクティブ/アクティブ クラスタリングが有効になっている場合、WAN では静的 IP アドレスしか使用できません。

以下の機能は、アクティブ/アクティブ クラスタリングが有効な場合にはサポートされません。

- DHCP サーバ
- L3 トランスペアレント モード
- L2 ブリッジ / L2 トランスペアレント モード
- 動的 DNS
- ワイヤ モード

以下の機能は、仮想グループ 1 でのみサポートされます。

- SonicWall GVC
- SonicOS の SSL VPN
- IP ヘルパー

下位互換性

アクティブ/アクティブ クラスタリング機能には、下位互換性がありません。アクティブ/アクティブ クラスタリングをサポートしていない以前のリリースから SonicOS をアップグレードする際には、以前のバージョンの SonicOS が動作している HA ペアから設定をエクスポートする前に、高可用性を無効にすることを強くお勧めします。そうすれば、アップグレード後の競合が発生する可能性なしに設定をインポートできます。

SonicPoint の互換性

SonicWall SonicPoint または SonicWave をアクティブ/アクティブ クラスタリングと併用する場合には、次の 2 つの点を考慮します。

- SonicPoint および SonicWave は、ファームウェアのダウンロードや運用のその他の面に関してマスター ノードとの通信しか行いません。
- SonicPoint および SonicWave は個別の DHCP サーバにアクセスする必要があります。SonicPoint および SonicWave は、無線クライアントに IP アドレスを提供するために DHCP サーバを必要としますが、組み込みの SonicOS DHCP サーバは、アクティブ/アクティブ クラスタリングが有効になると自動的に無効になります。

WAN 負荷分散の互換性

アクティブ/アクティブ クラスタ内で WAN 負荷分散 (WLB) が有効になっている場合は、クラスタ内のすべてのノードで同じ WLB インターフェース設定が使用されます。

WAN インターフェースに障害が発生すると、以下の状況に応じて、WLB フェイルオーバー、HA ペア フェイルオーバー、または別のクラスタ ノードへのアクティブ/アクティブ フェイルオーバーのいずれかが行われます。

- WLB プローブの障害によって WAN がダウンした場合 - WLB フェイルオーバー
- 物理監視が有効になっているときに物理 WAN がダウンした場合 - HA ペア フェイルオーバー
- 物理監視が有効になっていないときに物理 WAN がダウンした場合 - アクティブ/アクティブ フェイルオーバー

ルーティング トポロジとプロトコル互換性

このセクションでは、ルーティング トポロジとルーティング プロトコルに関するアクティブ/アクティブ クラスタリング設定の現時点での制限事項と特殊な要件について説明します。

トピック:

- レイヤ 2 ブリッジのサポート (721 ページ)
- OSPF のサポート (721 ページ)
- RIP のサポート (721 ページ)
- BGP のサポート (722 ページ)
- クラスタ設定における非対称ルーティング (722 ページ)

レイヤ 2 ブリッジのサポート

レイヤ 2 でブリッジ接続されたインターフェースは、クラスタ設定ではサポートされません。

OSPF のサポート

OSPF はアクティブ/アクティブ クラスタリングと共にサポートされます。OSPF が有効になっている場合、アクティブなクラスタ ノードのそれぞれの OSPF 対応インターフェースで OSPF が実行されます。ルーティングの観点からは、すべてのクラスタ ノードが並列なルータとなり、そのそれぞれがクラスタ ノードのインターフェースの仮想 IP アドレスを持ちます。一般に、あるノードによってアドバタイズされたネットワークはすべて、他のすべてのノードによってアドバタイズされます。

各クラスタ ノードの OSPF ルータ ID は、一意でなければならず、次のようにマスター ノードで設定されているルータ ID から派生します。

- ユーザが OSPF 設定でルータ ID に **0** または **0.0.0.0** を入力した場合、各ノードのルータ ID にはノードの X0 仮想 IP アドレスが割り当てられます。
- ユーザがルータ ID に **0** または **0.0.0.0** 以外の任意の値を入力した場合、各ノードには、ノードごとに値が 1 ずつ増える連続値を持つルータ ID が割り当てられます。例えば、マスター ノードにルータ ID `10.0.0.1` が設定された 4 ノードのクラスタでは、ルータ ID が次のように割り当てられます。
  - ノード 1: `10.0.0.1`
  - ノード 2: `10.0.0.2`
  - ノード 3: `10.0.0.3`
  - ノード 4: `10.0.0.4`

RIP のサポート

RIP はサポートされており、OSPF と同様、各クラスタ ノードの RIP 対応インターフェースで動作します。ルーティングの観点からは、すべてのクラスタ ノードがクラスタ ノードのインターフェースの仮想 IP アドレスを持つ並列なルータとなります。一般に、あるノードによってアドバタイズされたネットワークはすべて、他のすべてのノードによってアドバタイズされます。

BGP のサポート

BGP はクラスタでサポートされ、またクラスタ ノードのインターフェースの仮想 IP アドレスを使用している並列な BGP ルータとなります。OSPF や RIP と同様、マスター ノードで行われた設定の変更は、他のすべてのクラスタ ノードに適用されます。CLI によってのみ設定を適用できる BGP の場合は、実行中の設定を CLI コマンド **write file** (『*SonicOS 6.2 CLI リファレンス ガイド*』を参照) で保存するときに設定が配信されます。

クラスタ設定における非対称ルーティング

SonicOS では、トラフィックがセキュリティ装置上の異なるレイヤ 2 ブリッジ ペア インターフェースを通るとき、または高可用性クラスタ内の異なるセキュリティ装置を通るときに、非対称ルーティングがサポートされます。

アクティブ/アクティブ クラスタリングの前提条件

メモ：このセクションで説明する要件に加え、「アクティブ/スタンバイおよびアクティブ/アクティブ DPI 機能の前提条件 (704 ページ)」で説明している前提条件を満たしていることを確認してください。

アクティブ/アクティブ クラスタリングでは、以下の追加の物理接続が必要です。

- **アクティブ/アクティブ クラスタ リンク** - 各アクティブ/アクティブ クラスタ リンクは最低 100MB のインターフェースでなければなりませんが、1GB のインターフェースが推奨されます。

アクティブ/アクティブ クラスタリング設定には、仮想グループ ID と冗長ポートの設定を含めることができます。このセクションで説明する手順は、「高可用性 > 基本設定 (726 ページ)」の以下の 2 つのタスクに関係しています。

トピック:

- アクティブ/アクティブ クラスタのライセンス要件 (722 ページ)
- アクティブ/アクティブ クラスタリングでの HA ポートの接続 (723 ページ)
- 冗長ポート インターフェースの接続 (723 ページ)

アクティブ/アクティブ クラスタのライセンス要件

「A/A クラスタリングのライセンス要件」テーブルに、SonicWall セキュリティ装置の購入時に付属するアクティブ/アクティブ クラスタリング ライセンスを示します。一部のプラットフォームでは、ステートフル同期やアクティブ/アクティブ クラスタリング機能の利用に追加ライセンスが必要です。SonicOS 拡張ライセンスは、MySonicWall または SonicWall 再販業者から購入できます。

メモ：アクティブ/アクティブ クラスタリング ライセンスは、セキュリティ装置ごとに有効にする必要があります。そのためには、MySonicWall で SonicOS 管理インターフェースから装置を登録するか、インターネット アクセスが利用できない場合は各装置にライセンス キーセットを適用します。

A/A クラスタリングのライセンス要件

プラットフォーム	ライセンスの要件[a]	プラットフォーム	ライセンスの要件
NSA 6600	拡張ライセンス	SM 9600	付属
NS*a* 5650	拡張ライセンス	SM 9400	付属

A/A クラスタリングのライセンス要件 (続き)

プラットフォーム	ライセンスの要件[a]	プラットフォーム	ライセンスの要件
NSA 5600	拡張ライセンス	SM 9200	付属
NS*a* 4650	拡張ライセンス		
NSA 4600	拡張ライセンス	TZ600/600P	該当なし
NS*a* 3650	拡張ライセンス	TZ500/TZ500 W	該当なし
NSA 3600	拡張ライセンス	TZ400/TZ400 W	該当なし
NS*a* 2650	該当なし	TZ350/TZ350 W	該当なし
NSA 2600	該当なし	TZ300/TZ300P/TZ300 W	該当なし
		SOHO 250/SOHO 250 W	該当なし
		SOHO W	該当なし

a. N/A = 該当なし、付属 = 基本ライセンスに付属

システム ライセンスは、「**管理 | 更新 > ライセンス**」で確認できます。このページには、MySonicWall へのログイン方法も用意されています。ライセンスについては、『*SonicOS の更新*』を参照してください。

アクティブ/アクティブ クラスタ内のセキュリティ装置がインターネットにアクセスできる場合は、各セキュリティ装置の管理 IP アドレスにログインした状態で、SonicOS 管理インターフェースからクラスタ内の各セキュリティ装置を個別に登録する必要があります。これにより、セカンダリ装置は SonicWall ライセンス サーバと同期され、各 HA ペアの関連付けられたプライマリ セキュリティ装置とライセンスを共有できるようになります。

アクティブ/アクティブ クラスタリングでの HA ポートの接続

アクティブ/アクティブ クラスタリングの場合、アクティブ/アクティブ クラスタ内のすべての装置の指定された HA ポートを同じレイヤ 2 ネットワークに物理的に接続する必要があります。

SonicWall では、すべての指定された HA ポートを同じレイヤ 2 スイッチに接続することをお勧めします。専用のスイッチを使用することも、単純に内部ネットワークにある既存のスイッチ上の一部のポートを使用することもできます。これらのスイッチ ポートはすべて、それらの間でトラフィックを自由に流すためにレイヤ 2 トラフィックを許可するように設定する必要があります。

2 つのクラスタ ノードがそれぞれ 1 台のセキュリティ装置しか持たない、2 台の装置によるアクティブ/アクティブ クラスタ配備の場合は、互いの HA ポートどうしをクロスオーバー ケーブルを使用して接続できます。この場合、スイッチは必要ありません。

SonicWall Virtual Router Redundancy Protocol (SVRRP) では、この HA ポート接続を使用して、クラスタ ノードの管理と監視に関する状況メッセージを送信します。SVRRP 管理メッセージはマスター ノードから送信され、監視情報はクラスタ内のすべてのセキュリティ装置から送信されます。

HA ポート接続は、マスター ノードから配備内の他のクラスタ ノードへの設定の同期にも使用されます。こうした設定には、ファームウェアまたはシグネチャのアップグレード、VPN および NAT に関するポリシー、およびその他の設定も含まれます。

冗長ポート インターフェースの接続

未使用の物理インターフェースは、"プライマリ インターフェース" と呼ばれる設定された物理インターフェースへの冗長ポートとして割り当てることができます。各クラスタ ノードでは、プライマ

リ ポートと冗長ポートの各ペアを同じスイッチ、できればネットワーク内の冗長スイッチに物理的に接続する必要があります。

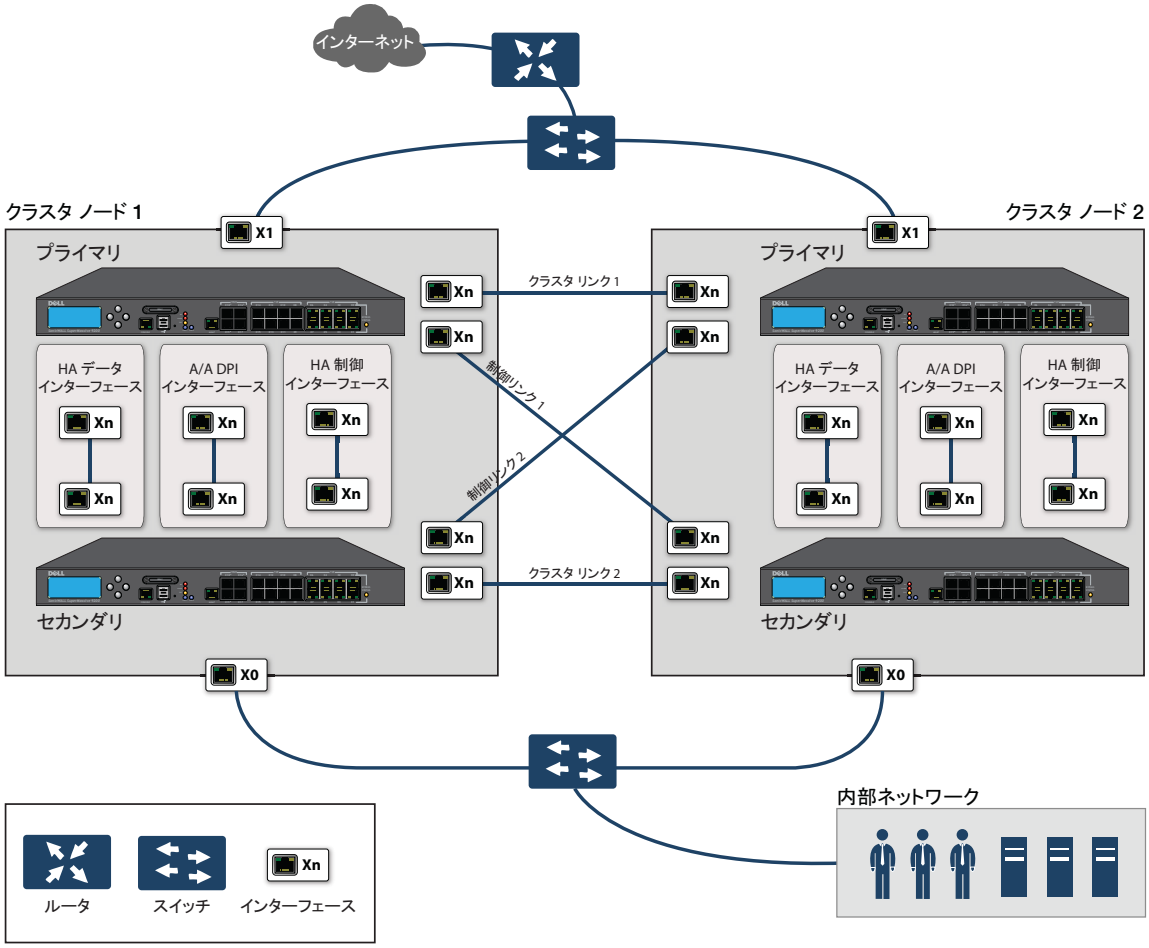
メモ：すべてのクラスタ ノードは同じ設定を共有するので、各ノードは同じ冗長ポートが設定され、同じスイッチに接続されている必要があります。

アクティブ/アクティブ クラスタリングを使用するには、MySonicWall でクラスタ内のすべての SonicWall セキュリティ装置を登録する必要があります。各 HA ペア内の 2 台のセキュリティ装置は、MySonicWall で HA プライマリおよび HA セカンダリとして関連付けられている必要もあります。つまり、クラスタ ノード 1 の HA ペアの 2 台のセキュリティ装置を関連付けたら、次はクラスタ ノード 2 の HA ペアのセキュリティ装置を関連付け、さらに、残りすべてのクラスタ ノードについても同様の関連付けを行います。

アクティブ/アクティブ DPI クラスタリング高可用性

アクティブ/アクティブ DPI クラスタリング高可用性では、フェイルオーバーと負荷分散のために最大 4 つの HA クラスタ ノードを設定できます。負荷分散では、各ノードによってネットワーク トラフィックに対する精密パケット検査 (DPI) セキュリティ サービスのアプリケーションの負荷が分散されます。「アクティブ/アクティブ DPI クラスタリング高可用性機能」を参照してください。

アクティブ/アクティブ DPI クラスタリング高可用性機能



クラスタ リンクと制御リンクについては、クラスタ ノード 1 の各装置は、ピア ノード (クラスタ ノード 2) の各装置に接続します。ベスト プラクティスとしては、各ノードの各装置の同じインターフェースのセットを使用してください(例えば、ある装置の X8 をピア装置の X8 に接続し、X9、X10 などについても使用する場合は同様にします)。ただし、使用するポートに制限はありません。

46

高可用性の設定

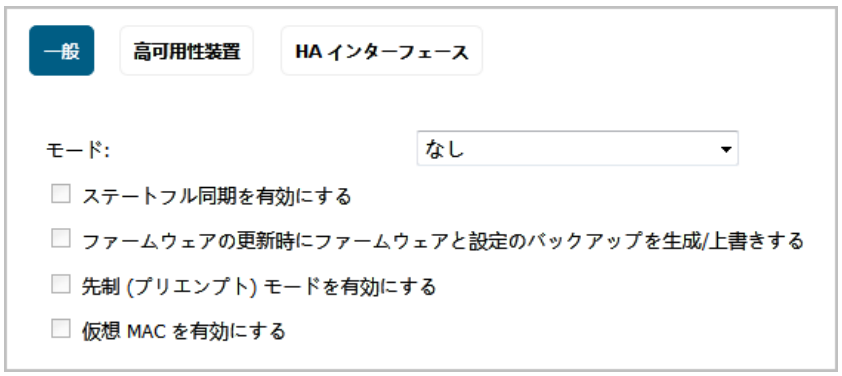
重要：高可用性は、SonicWall X シリーズ ソリューション以外の PortShield と併用できません。HA を設定する前に、既存の PortShield 設定があれば「**管理 | システム セットアップ > ネットワーク > PortShield グループ**」で削除します。HA を PortShield と併用する方法については、「SonicOS がサポートする X シリーズ スイッチ (374 ページ)」および『*SonicWall X シリーズ ソリューション配備ガイド*』を参照してください。

ヒント：SonicOS の高可用性の説明については、「アクティブ/アクティブ クラスタリングでの高可用性について (693 ページ)」を参照してください。

トピック:

- 高可用性 > 基本設定 (726 ページ)
  - アクティブ/スタンバイ高可用性機能の設定 (727 ページ)
  - 動的 WAN インターフェースでの高可用性 (HA) の設定 (729 ページ)
  - アクティブ/アクティブ DPI 高可用性機能の設定 (731 ページ)
  - アクティブ/アクティブ クラスタリングの設定 (733 ページ)
  - アクティブ/アクティブ クラスタリング設定の確認 (738 ページ)
  - ネットワーク DHCP とインターフェースの設定 (740 ページ)
  - アクティブ/アクティブ クラスタリング フルメッシュ (742 ページ)

高可用性 > 基本設定



高可用性 (HA) は、「**管理 | システム セットアップ > 高可用性 > 基本設定**」で設定します。

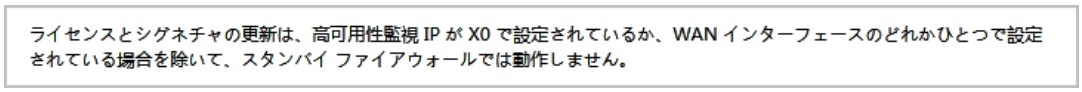
- アクティブ/スタンバイ高可用性機能の設定 (727 ページ)
- 動的 WAN インターフェースでの高可用性 (HA) の設定 (729 ページ)

- アクティブ/アクティブ DPI 高可用性機能の設定 (731 ページ)

メモ：高可用性の詳細については、「高可用性機能について (694 ページ)」および「アクティブ/スタンバイおよびアクティブ/アクティブ DPI 機能の前提条件 (704 ページ)」を参照してください。アクティブ/アクティブ クラスタリング環境で VPN または NAT を使用する場合は、アクティブ/アクティブ設定の完了後に「アクティブ/アクティブ クラスタリングでの VPN と NAT の設定 (738 ページ)」を参照してください。

- アクティブ/アクティブ クラスタリングの設定 (733 ページ)
- アクティブ/アクティブ クラスタリング設定の確認 (738 ページ)
- ネットワーク DHCP とインターフェースの設定 (740 ページ)
- アクティブ/アクティブ クラスタリング フルメッシュ (742 ページ)

ライセンスとシグネチャの更新は、HA 監視用 IP アドレスが X0 またはいずれかの WAN インターフェースで設定されていなければ、スタンバイ セキュリティ装置では機能しません。これらのインターフェースが設定されていない場合、以下のようなメッセージが表示されます。

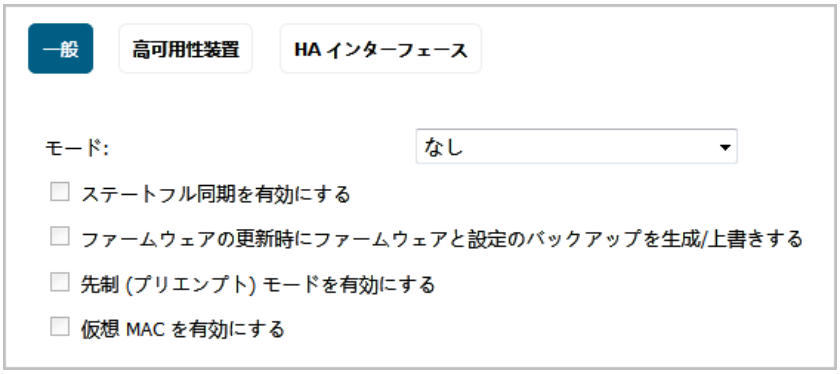


アクティブ/スタンバイ高可用性機能の設定

プライマリ ファイアウォールで行った「**高可用性 > 基本設定**」の設定タスクは、セカンダリ ファイアウォールに自動的に同期されます。

アクティブ/スタンバイを設定するには:

1 「**システムセットアップ | 高可用性 > 基本設定**」に移動します。

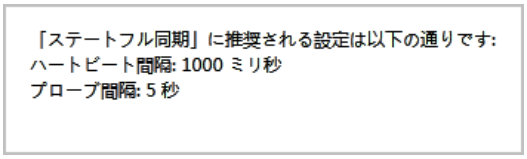


2 「**モード**」で、「**アクティブ / スタンバイ**」を選択します。オプションが使用可能になります。

3 「**ステートフル同期を有効にする**」をオンにします。このオプションは、既定では選択されていません。

ステートフル高可用性機能が有効になっていないと、プライマリ ファイアウォールとセカンダリ ファイアウォールの間でのセッション状態の同期は行われません。フェイルオーバーが発生した場合、フェイルオーバー時にアクティブであったセッションは再ネゴシエートされる必要があります。

推奨メッセージが表示されます。



4 「**OK**」を選択します。

5 ファームウェアのバージョンをアップグレードするときに設定をバックアップするには、「**ファームウェアの更新時にファームウェアと設定のバックアップを生成/上書きする**」を選択します。このオプションは、既定では選択されていません。

6 プライマリ ファイアウォールが障害後の再起動によりプライマリの役割に復帰するように高可用性ペアを設定するには、「**先制 (プリエンプト) モードを有効にする**」を選択します。このオプションは、既定では選択されていません。

> **ヒント**：ステートフル高可用性機能を有効にする場合は、先制モードを無効にすることを推奨します。セカンダリ ファイアウォールへのフェイルオーバーが過度に実行される可能性があるからです。

7 「**仮想 MAC を有効にする**」をオンにすると、プライマリとセカンダリの各ファイアウォールで同じ MAC アドレスを共有できます。これにより、フェイルオーバーが発生したとき、ネットワーク ARP テーブルとキャッシュの更新処理が大幅に簡素化されます。このオプションは、既定では選択されていません。

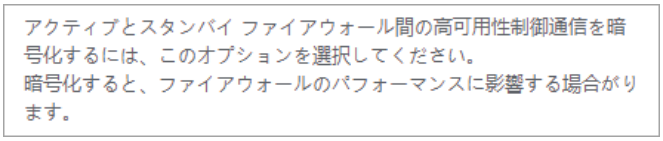
> **重要**：PPPoE アンナンバードを設定している場合、「**仮想 MAC を有効にする**」をオンにします。

2 台のファイアウォールが接続されているスイッチへの通知だけで済みます。外部のすべての機器は、単一の共有 MAC アドレスに引き続きルーティングされます。

8 アクティブ ファイアウォールとスタンバイ ファイアウォール間の HA 制御通信を暗号化するには、「**制御通信の暗号化を有効にする**」を選択します。このオプションは、既定では選択されていません。

> **重要**：暗号化を選択すると、ファイアウォールのパフォーマンスが影響を受ける場合があります。

確認メッセージが表示されます。

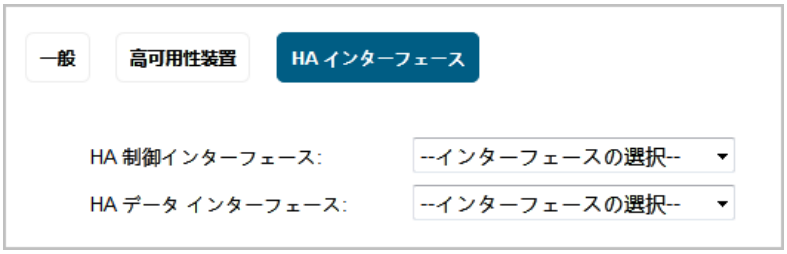


「**OK**」を選択します。

9 セカンダリ ファイアウォールのシリアル番号を設定するには、「**高可用性装置**」を選択します。プライマリ装置のシリアル番号が表示されます。ただし、このフィールドは淡色表示になっており、編集できません。

10 「**セカンダリ装置**」の「**シリアル番号**」を入力します。

11 「**HA インターフェース**」を選択します。



12 「**HA 制御インターフェース**」でインターフェースを選択します。インターフェースが既に設定済みであることがファイアウォールによって検出されている場合、このオプションは淡色表示になり、そのインターフェースが表示されます。

13 「**アクティブ/アクティブ DPI インターフェース**」でインターフェースを選択します。インターフェースが既に設定済みであることがファイアウォールによって検出されている場合、このオプションは淡色表示になり、そのインターフェースが表示されます。

14 すべての高可用性設定が終了したら、「**適用**」を選択します。すべての設定がセカンダリ ファイアウォールに同期され、セカンダリ ファイアウォールが再起動します。

動的 WAN インターフェースでの高可用性 (HA) の設定

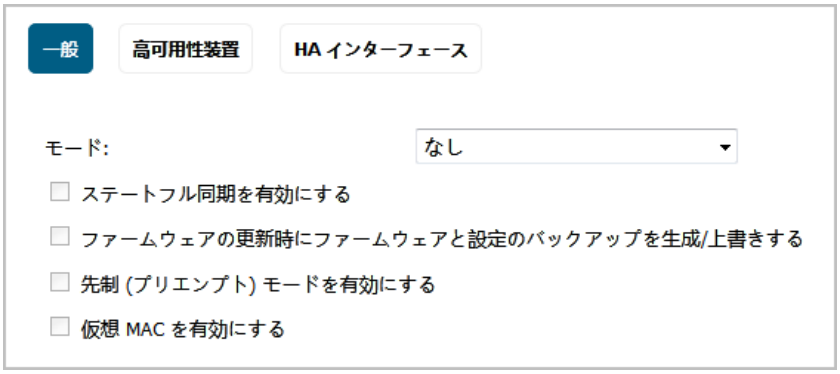
プライマリ ファイアウォールで行った「**高可用性 > 基本設定**」の設定タスクは、セカンダリ ファイアウォールに自動的に同期されます。

動的 WAN インターフェースで HA を設定するには:

1 「**管理 | システム セットアップ > ネットワーク > インターフェース**」に移動します。

2 「WAN インターフェースの設定 (313 ページ)」の説明に従って、WAN インターフェースを PPPoE として設定します。

3 「**高可用性 > 基本設定**」に移動します。



4 「**モード**」で、HA モードを選択します。「**アクティブ/アクティブ DPI**」または「**アクティブ/アクティブ クラスタリング**」を選択した場合は、ライセンスとシグネチャの更新に関するメッセージが表示されます。

ライセンスとシグネチャの更新は、高可用性監視 IP が X0 で設定されているか、WAN インターフェースのどれかひとつで設定されている場合を除いて、スタンバイ ファイアウォールでは動作しません。

5 「**OK**」を選択します。

6 「**ステートフル同期を有効にする**」がオフになっていることを確認します。このオプションは、既定では選択されていません。

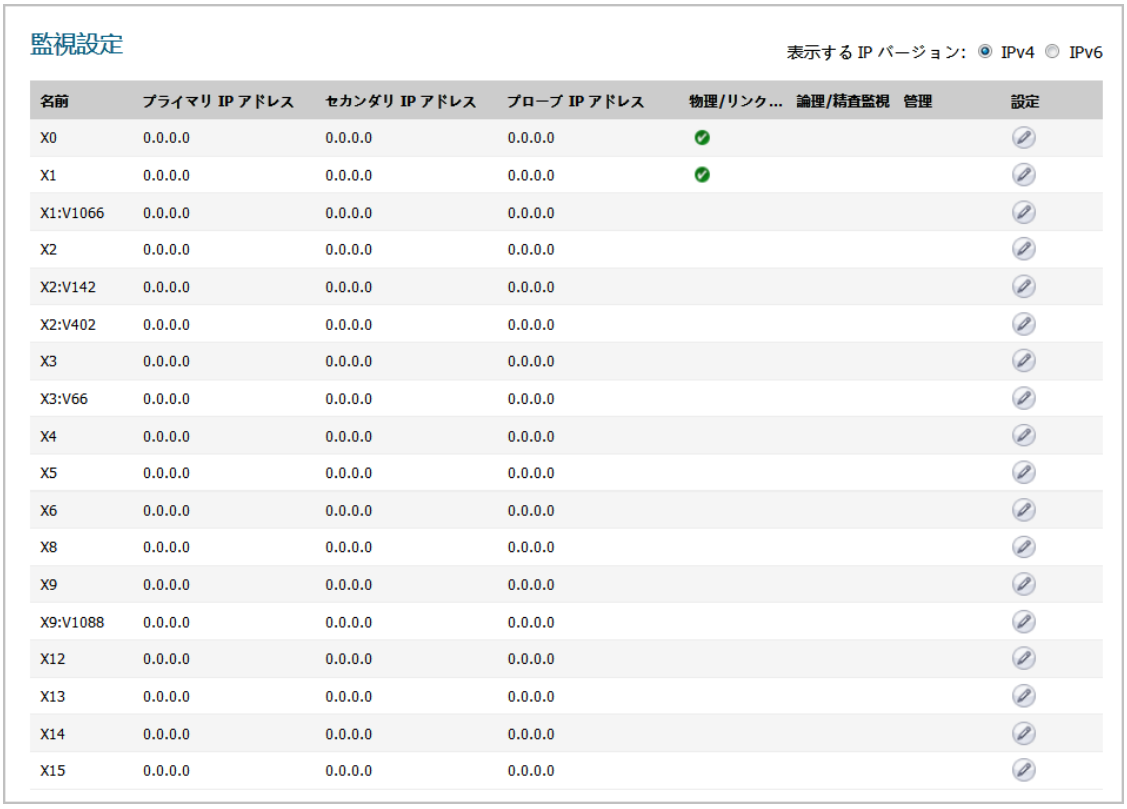
7 「**先制 (プリエンプト) モードを有効にする**」がオフになっていることを確認します。このオプションは、既定では選択されていません。

8 「**仮想 MAC を有効にする**」をオンにします。このオプションは、既定では選択されていません。

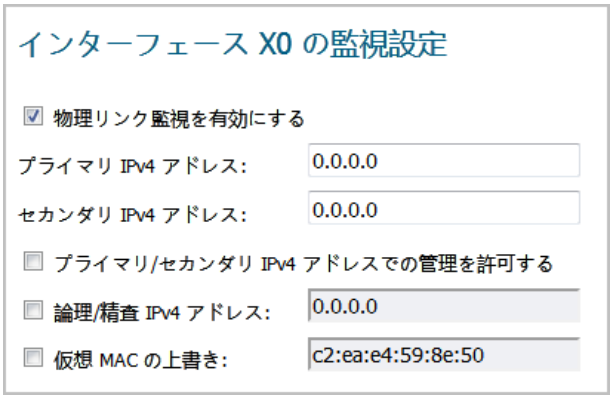
9 「アクティブ/スタンバイ高可用性機能の設定 (727 ページ)」の説明に従って、「**高可用性装置**」と「**HA インターフェース**」のオプションを設定します。

10 「**適用**」を選択します。

11 「**管理 | システム セットアップ > 高可用性 > 監視設定**」に移動します。



12 PPPoE インターフェースの**設定**アイコンを選択します。「**HA 監視の編集**」ダイアログ ボックスが表示されます。



13 「**物理リンク監視を有効にする**」チェックボックスをオンにします。このオプションは、既定では選択されていません。

14 「**プライマリ IPv4 アドレス**」フィールドと「**セカンダリ IPv4 アドレス**」フィールドが「0.0.0.0」に設定されていることを確認します。

15 他のオプションがすべてオフになっていることを確認します。

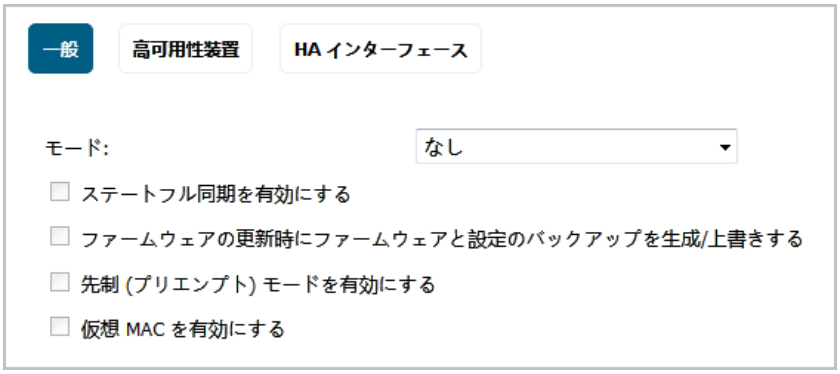
16 「**OK**」を選択します。

アクティブ/アクティブ DPI 高可用性機能の設定

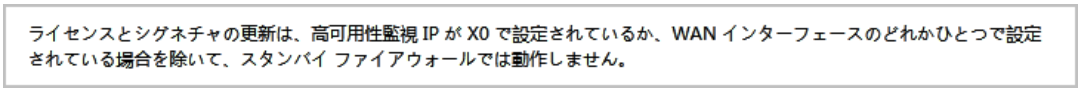
プライマリ ファイアウォールで行った「**管理 | システム セットアップ > 高可用性 > 基本設定**」の設定タスクは、セカンダリ ファイアウォールに自動的に同期されます。

アクティブ/アクティブ DPI を設定するには:

1 「**高可用性 > 基本設定**」に移動します。



2 「**モード**」ドロップダウン メニューで「**アクティブ/アクティブ DPI**」を選択します。ライセンスとシグネチャの更新に関するメッセージが表示されます。



3 「**OK**」を選択します。

アクティブ/アクティブ DPI では「**ステートフル同期を有効にする**」オプションが自動的に有効になるので、このオプションは淡色表示になります。

4 ファームウェアのバージョンをアップグレードするときに設定をバックアップするには、「**ファームウェアの更新時にファームウェアと設定のバックアップを生成/上書きする**」を選択します。このオプションは、既定では選択されていません。

5 通常、アクティブ/アクティブ DPI では先制 (プリエンプト) モードを無効にする必要があります。「**先制 (プリエンプト) モードを有効にする**」がオフになっていることを確認します。このオプションは、既定では選択されていません。

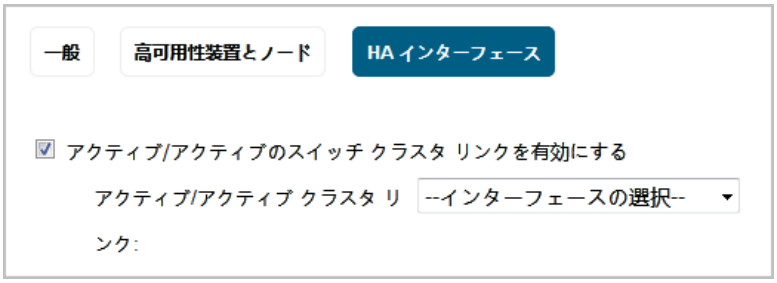
> **メモ**：このオプションは、プライマリ ファイアウォールが障害後の再起動によりプライマリの役割に復帰するように指示するものです。そのため、アクティブ/スタンバイ設定のみに適用されます。

6 HA ペアの両方のセキュリティ装置で同じ MAC アドレスを共有できるようにするには、「**仮想 MAC を有効にする**」をオンにします。このオプションにより、フェイルオーバーが発生したとき、ネットワーク ARP テーブルとキャッシュの更新処理が大幅に簡素化されます。2 台のセキュリティ装置が接続されているスイッチへの通知だけで済みます。外部のすべての機器は、単一の共有 MAC アドレスに引き続きルーティングされます。このオプションは、既定では選択されていません。

7 「**高可用性装置**」タブを選択します。プライマリ装置のシリアル番号が表示されます。このフィールドは淡色表示になっており、編集できません。

8 「**セカンダリ装置**」の「**シリアル番号**」を入力します。

9 「**HA インターフェース**」を選択します。



10 「**HA 制御インターフェース**」で HA 制御インターフェースを選択します。インターフェースが既に設定済みであることがセキュリティ装置によって検出されている場合、このオプションは淡色表示になり、そのインターフェースが表示されます。

11 「**HA データ インターフェース**」でインターフェース番号を選択します。インターフェースが既に設定済みであることがセキュリティ装置によって検出されている場合、このオプションは淡色表示になり、そのインターフェースが表示されます。

12 「**アクティブ/アクティブ DPI インターフェース**」でインターフェース番号を選択します。インターフェースが既に設定済みであることがセキュリティ装置によって検出されている場合、このオプションは淡色表示になり、そのインターフェースが表示されます。

このインターフェースは、アクティブ/アクティブ DPI 処理中に 2 台のセキュリティ装置間でデータを転送するために使用されます。未割り当てかつ利用可能なインターフェースのみがドロップダウン メニューに表示されます。接続されるインターフェースは、両方のセキュリティ装置で同じ番号、かつ「**管理 | ネットワーク > インターフェース**」で最初は未使用、未定義のインターフェースとして表示されていなければなりません。例えば、X5 が未定義のインターフェースである場合、プライマリ装置の X5 をセカンダリ装置の X5 に接続できます。アクティブ/アクティブ DPI を有効にした後、接続されたインターフェースは「**HA データリンク**」という**ゾーン**割り当てを持ちます。

13 すべての高可用性設定が終了したら、「**適用**」を選択します。すべての設定がスタンバイ セキュリティ装置に同期され、スタンバイ セキュリティ装置が再起動します。

アクティブ/アクティブ クラスタリングの設定

トピック:

- アクティブ/アクティブ クラスタリング高可用性機能の設定 (733 ページ)
- アクティブ/アクティブ DPI クラスタリング高可用性機能の設定 (735 ページ)
- アクティブ/アクティブ クラスタリングでの VPN と NAT の設定 (738 ページ)

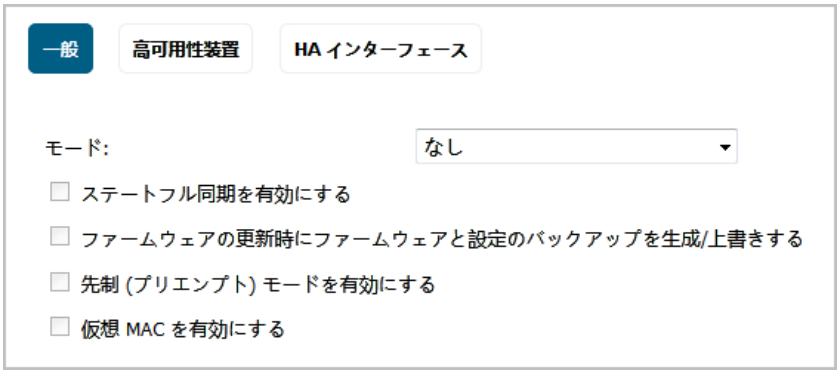
アクティブ/アクティブ クラスタリング高可用性機能の設定

アクティブ/アクティブ クラスタリング高可用性では、フェイルオーバーと負荷分散のために最大 4 つの HA クラスタ ノードを設定できます。各ノードには、1 台のセキュリティ装置または HA ペアのいずれかを含めることができます。

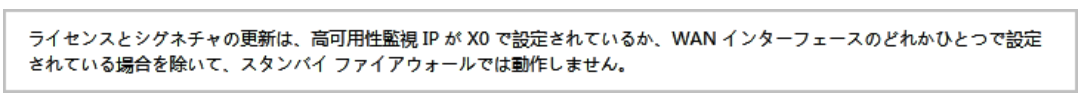
アクティブ/アクティブ クラスタリング高可用性機能を設定するには、以下の手順に従います。

1 マスター クラスタ ノードのプライマリ装置にログインします。

2 「**管理 | システム セットアップ > 高可用性 > 基本設定**」に移動します。



3 「**モード**」ドロップダウン メニューで「**アクティブ/アクティブ クラスタリング**」を選択します。ライセンスとシグネチャの更新に関するメッセージが表示されます。



4 「**OK**」を選択します。「高可用性装置」が「**高可用性装置とノード**」に変わります。

5 「**ステートフル同期を有効にする**」をオンにします。

6 新しいファームウェアをセキュリティ装置にアップロードするときにファームウェアと設定を自動的にバックアップするには、「**ファームウェアの更新時にファームウェアと設定のバックアップを生成/上書きする**」を選択します。マスター ノードによって新しいセキュリティ装置がクラスタ内の他のセキュリティ装置に同期される際に、これらのセキュリティ装置がセカンダリ装置になります。

7 アクティブ/アクティブ クラスタの情報を設定するには、「**高可用性装置とノード**」を選択します。

8 **クラスタ ノード**のテーブルで、それぞれのクラスタ ノード内にあるセキュリティ装置のシリアル番号を、該当する「**プライマリ装置シリアル番号**」および「**セカンダリ装置シリアル番号**」フィールドに入力します。

9 「**仮想グループ *n* 階級**」ドロップダウン メニューで、各仮想グループでクラスタ ノード 1 が保持する階級を選択します。既定では、クラスタ ノード 1 がグループ 1 の**オーナー**となり、また通常は他のグループの**スタンバイ**として位置づけられます。

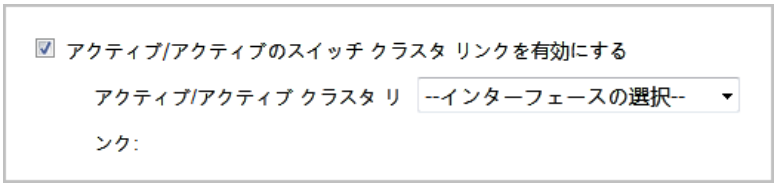
クラスタからセキュリティ装置を除外するには、「**仮想グループ *n* 階級**」で「**なし**」を選択します。

10 2 行目の「**仮想グループ *n* 階級**」ドロップダウン メニューで、各仮想グループでクラスタ ノード 2 が保持する階級を選択します。

11 「**HA インターフェース**」を選択します。

12 「**HA 制御インターフェース**」で HA 制御インターフェースを選択します。インターフェースが既に設定済みであることがセキュリティ装置によって検出されている場合、このオプションは淡色表示になり、そのインターフェースが表示されます。

13 「**アクティブ/アクティブのスイッチ クラスタ リンクを有効にする**」を選択します。オプションが次のように変化します。



14 「**アクティブ/アクティブ クラスタ リンク**」で、アクティブ/アクティブ処理中に 2 台の装置間でデータを転送するために使用するインターフェースを選択します。未定義かつ利用可能なインターフェースのみがリストに表示されます。

15 「**アクティブ/アクティブのスイッチ クラスタ リンクを有効にする**」を選択した場合は、「ステップ 17」に進みます。

16 「**アクティブ/アクティブ クラスタ リンク 2**」で、アクティブ/アクティブ処理中に 2 台の装置間の第 2 のリンクでデータを転送するために使用するインターフェースを選択します。未定義かつ利用可能なインターフェースのみがリストに表示されます。

17 「**適用**」を選択します。すべての設定がスタンバイ装置に同期され、スタンバイ装置が再起動します。

18 「**管理 | システム セットアップ > 高可用性 > 詳細設定**」に移動し、「高可用性 > 詳細設定 (750 ページ)」の手順に従います。

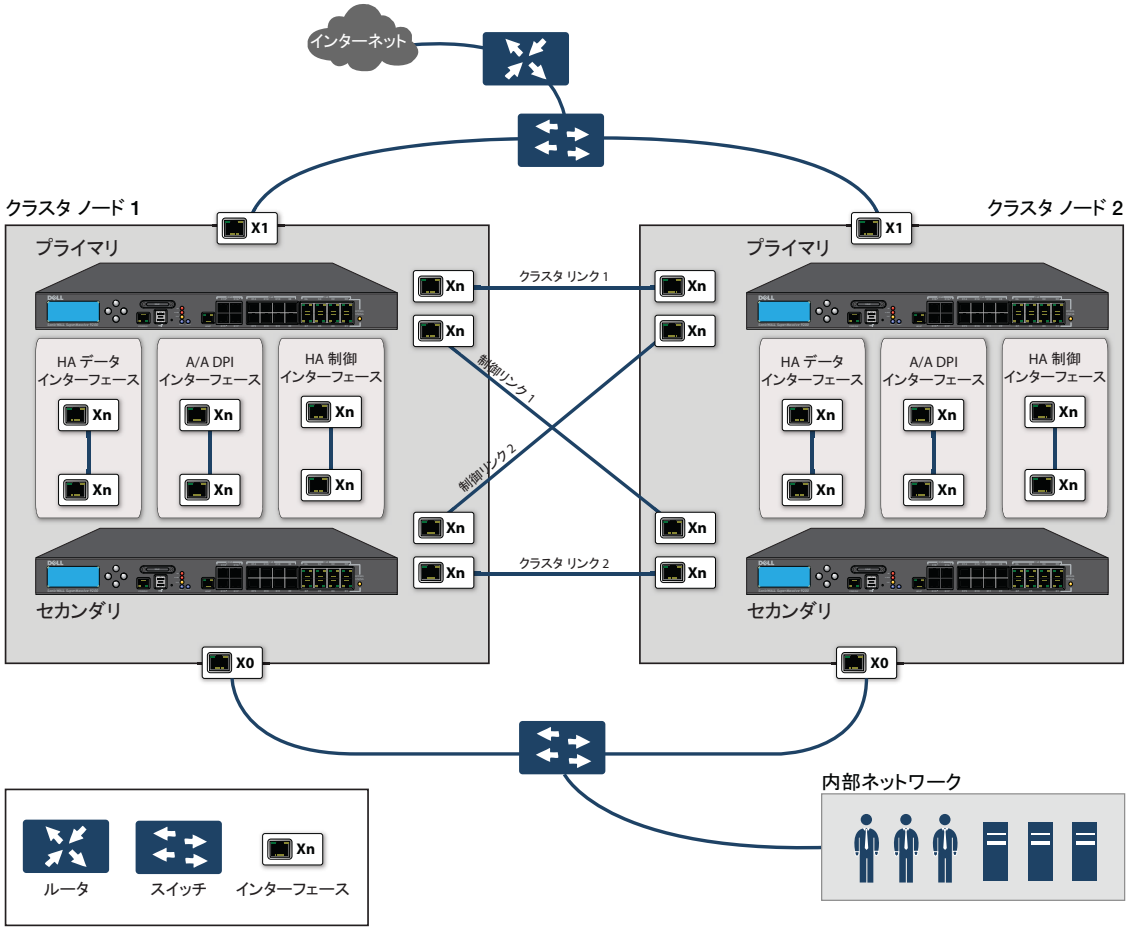
19 「**管理 | システム セットアップ > ネットワーク > インターフェース**」ページに移動して、必要なアクティブ/アクティブ インターフェースが設定できたことを確認します。

20 「**管理 | システム セットアップ > 高可用性 > 監視設定**」に移動して、アクティブ/アクティブ クラスタリングの設定を確認します。

アクティブ/アクティブ DPI クラスタリング高可用性機能の設定

アクティブ/アクティブ DPI クラスタリング高可用性では、フェイルオーバーと負荷分散のために最大 4 つの HA クラスタ ノードを設定できます。負荷分散では、各ノードによってネットワーク トラフィックに対する精密パケット検査 (DPI) セキュリティ サービスのアプリケーションの負荷が分散されます。「アクティブ/アクティブ DPI クラスタリング高可用性機能」を参照してください。

アクティブ/アクティブ DPI クラスタリング高可用性機能



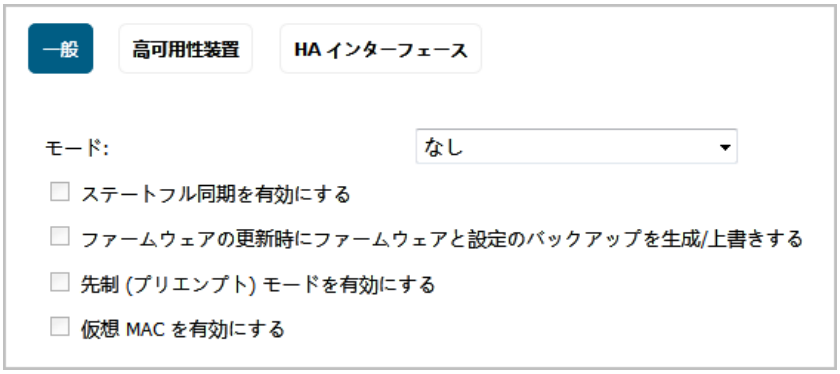
クラスタ リンクと制御リンクについては、クラスタ ノード 1 の各装置は、ピア ノード (クラスタ ノード 2) の各装置に接続します。ベスト プラクティスとしては、各ノードの各装置の同じインターフェースのセットを使用してください(例えば、ある装置の X8 をピア装置の X8 に接続し、X9、X10 などについても使用する場合は同様にします)。ただし、使用するポートに制限はありません。

アクティブ/アクティブ DPI クラスタリング高可用性機能を設定するには、以下の手順に従います。

メモ：「セキュリティ装置の物理的な接続 (706 ページ)」の説明どおりにアクティブ/アクティブ DPI インターフェースに物理的に接続している場合は、SonicOS 管理インターフェースでアクティブ/アクティブ DPI を設定する準備ができています。

1 マスター クラスタ ノードのプライマリ装置にログインします。

2 「**管理 | システム セットアップ > 高可用性 > 基本設定**」に移動します。



3 「**モード**」で、「**アクティブ/アクティブ DPI クラスタリング**」を選択します。

4 アクティブ/アクティブ DPI クラスタリング では「**ステートフル同期を有効にする**」オプションが自動的に有効になります。

5 新しいファームウェアをセキュリティ装置にアップロードするときにセカンダリのファームウェアと設定を自動的に作成するには、「**ファームウェアの更新時にファームウェアと設定のバックアップを生成/上書きする**」を選択します。マスター ノードによって新しいファイアウォールがクラスタ内の他のセキュリティ装置に同期される際に、これらのセキュリティ装置がセカンダリ装置になります。

6 アクティブ/アクティブ クラスタの情報を設定するには、「**高可用性装置**」を選択します。

7 タブの上部にある「**HA セカンダリ**」オプションでは、以下のように選択します。

- 設定されているセカンダリ セキュリティ装置がこのセキュリティ装置のクラスタ ノードの一部である場合は、「**内部**」を選択します。
- 設定されているセカンダリセキュリティ装置が別のクラスタ ノードの一部である場合は、「**外部**」を選択します。

8 各クラスタ ノード内のセキュリティ装置のシリアル番号をテーブルに入力します。

> **ヒント**：プライマリ装置のシリアル番号は、自動的に設定されて淡色表示になっている場合があります。

9 各仮想グループでクラスタ ノード 1 が保持する階級を、シリアル番号の右側にある「**仮想グループ *X* 階級**」フィールドに入力します。既定では、クラスタ ノード 1 がグループ 1 の**オーナー**となり、また通常はグループ 2 の**スタンバイ**として位置づけられます。クラスタからファイアウォールを除外するには、「**仮想グループ *X* 階級**」で「**なし**」を選択します。

10 2 行目には、各仮想グループでクラスタ ノード 2 が保持する階級を、シリアル番号の右側にある「**仮想グループ *X* 階級**」フィールドに入力します。

11 「**HA インターフェース**」タブを選択します。「**HA 制御インターフェース**」でインターフェースを選択します。インターフェースが既に設定済みであることがセキュリティ装置によって検出されている場合、このオプションはグレーアウトされています。

12 「**アクティブ/アクティブ DPI インターフェース**」でインターフェースを選択します。インターフェースが既に設定済みであることがセキュリティ装置によって検出されている場合、このオプションはグレーアウトされています。

13 「**アクティブ/アクティブ DPI インターフェース**」を選択します。このインターフェースは、アクティブ/アクティブ DPI 処理中に 2 台の装置間でデータを転送するために使用されます。未割り当てかつ利用可能なインターフェースのみがドロップダウン メニューに表示されます。

14 「**アクティブ/アクティブ クラスタ リンク**」インターフェースを選択します。

15 すべての高可用性設定が終了したら、「**適用**」を選択します。すべての設定がスタンバイ装置に同期され、スタンバイ装置が再起動します。

16 「**管理 | システム セットアップ > 高可用性 > 詳細設定**」に移動し、「高可用性の微調整 (750 ページ)」の手順に従います。

17 「**管理 | システム セットアップ > ネットワーク > インターフェース**」に移動して、必要なアクティブ/アクティブ インターフェースが設定できたことを確認します。

18 「**監視 | 現在の状況 > 高可用性状況**」に移動して、アクティブ/アクティブ クラスタリングの設定を確認します。**高可用性状況**については、『*SonicOS 6.5 監視*』を参照してください。

アクティブ/アクティブ クラスタリングでの VPN と NAT の設定

アクティブ/アクティブ クラスタリング環境で以下の機能を設定する際には、追加の考慮事項を検討する必要があります。

- アクティブ/アクティブ クラスタリングでの VPN の設定 (738 ページ)
- アクティブ/アクティブ クラスタリングでの NAT ポリシーの設定 (738 ページ)

アクティブ/アクティブ クラスタリングでの VPN の設定

VPN ポリシー設定では、アクティブ/アクティブ クラスタリング モードでの実行時に仮想グループとの関連付けを必要とします。この関連付けの作成に関するオプションは、「**管理 | 接続性 > VPN | 基本設定**」で設定します。VPN ポリシーの設定については『*SonicOS 6.5 接続*』を参照してください。

ローカル ネットワークでは、仮想グループ アドレス オブジェクトを使用できます。これらの仮想グループ アドレス オブジェクトは、仮想 IP アドレスの追加時に SonicOS によって作成され、仮想 IP の削除時に削除されます。リモート ネットワークの VPN ポリシーを作成する場合も、仮想グループ アドレス オブジェクトを使用できます。例えば、**Active-Active-Lan-Host-1** という個別名があります。

アクティブ/アクティブ クラスタリングでの NAT ポリシーの設定

アクティブ/アクティブ クラスタリング モードで動作する場合、NAT ポリシー設定には、仮想グループの設定が含まれます。既定の NAT ポリシーは、仮想 IP アドレスの追加時に SonicOS によって作成され、仮想 IP の削除時に削除されます。個別 NAT ポリシーを作成する際には、仮想グループを指定できます。例えば、インターフェース X1 の仮想グループ 2 に対して NAT ポリシーが自動的に作成されます。NAT ポリシーの作成については、『*SonicOS 6.5 ポリシー*』を参照してください。

アクティブ/アクティブ クラスタリング設定の確認

このセクションでは、アクティブ/アクティブ クラスタリングおよびアクティブ/アクティブ DPI の設定が適切かどうかを確認する方法をいくつか説明します。以下を参照してください。

- クラスタ内のファイアウォール上の CPU アクティビティの比較 (739 ページ)
- 「監視 | 現在の状況 > 高可用性状況」の設定の確認 (739 ページ)
- TSR の追加パラメータ (739 ページ)

- DPI の一致に対する応答 (740 ページ)
- ログ (740 ページ)

クラスタ内のファイアウォール上の CPU アクティビティの比較

ステートフル HA ペアでアクティブ/アクティブ DPI 機能を有効にすると、HA ペアのセキュリティ装置上の CPU 使用率の変化を監視できます。CPU アクティビティはアクティブ装置で低下し、スタンバイ装置で上昇します。

CPU 使用率はマルチコア監視で確認できます。マスター ノードのアクティブ セキュリティ装置で、**「監視 | 装置の健全性 > ライブ監視」**に移動し、「マルチコア監視」までスクロールすると、アクティブ/アクティブ クラスタ内のすべてのセキュリティ装置の動作が表示されます。マルチコア監視の詳細については、『*SonicOS 6.5 監視*』を参照してください。

クラスタ内のアクティブ装置でマルチコア監視を閲覧すると、クラスタ内のすべてのセキュリティ装置が表示されます。ただし、クラスタ内のスタンバイ装置の個別の IP アドレスにログインしている場合は、マルチコア監視ページにその特定の HA ペア内の 2 つのセキュリティ装置のコア使用率のみが表示されます。

メモ：クラスタ内のすべてのセキュリティ装置のコア使用率を確認する場合、SonicWall では、マスター ノードのアクティブ装置で「マルチコア監視」を閲覧することをお勧めします。

「監視 | 現在の状況 > 高可用性状況」の設定の確認

「監視 | 現在の状況 > 高可用性状況」の**「アクティブ/アクティブ クラスタリング ノード状況」**テーブルには、アクティブ/アクティブ クラスタ全体と配備内の各クラスタ ノードの状況が表示されます。高可用性状況の表示については、『*SonicOS 6.5 監視*』を参照してください。

TSR の追加パラメータ

「調査 | ツール > システム診断」でテクニカル サポート レポートを生成することによって、ステートフル HA ペアにアクティブ/アクティブ DPI 機能が正しく設定されているかどうか判断できます。以下の設定パラメータが、テクニカル サポート レポートに正しい値で表示されるはずです。

- アクティブ/アクティブ DPI を有効にする
- アクティブ/アクティブ DPI インターフェース設定

TSR の生成については、『*SonicOS 6.5 調査*』を参照してください。

この場合、TSR を生成するには、以下の手順を実行します。

1 共有 IP アドレスを使用して、ステートフル HA ペアにログインします。

2 **「調査 | ツール > システム診断」**に移動します。

3 **「テクニカル サポート レポート」**の下にある**「レポートのダウンロード」**を選択します。

DPI の一致に対する応答

ネットワーク トラフィック内に DPI の一致が見つかった場合、応答 (アクション) は、常にアクティブ/アクティブ DPI 機能が動作しているステートフル HA ペアのアクティブ装置から送信されます。

メモ：これは、すべての処理がアクティブ装置で実行されたことを示すわけではありません。

精密パケット検査によって、ウイルスの添付ファイル、アプリケーション ルール ポリシー、および他のマルウェアに一致するネットワーク トラフィックが検出されます。一致が検出されると、SonicOS は、パケットの破棄や TCP 接続のリセットなどのアクションを実行します。

DPI 一致アクションの中には、追加の TCP パケットを既存のストリームに注入するものもあります。例えば、SMTP セッションがウイルスの添付ファイルを搬送している場合、SonicOS はその SMTP クライアントに対して 552 エラー応答コードと、"電子メールの添付ファイルにウイルスが含まれています" というメッセージを送信します。このエラー応答コードに続いて TCP がリセットされ、接続が終了されます。

このような追加 TCP パケットは、スタンバイ セキュリティ装置上での DPI 処理の結果として生成されます。生成されたパケットは、アクティブ/アクティブ DPI インターフェースを介してアクティブ セキュリティ装置に送信され、アクティブ セキュリティ装置上で処理が行われたかのように、アクティブ セキュリティ装置から送出されます。これによって、シームレスな動作が保証され、DPI 処理がアクティブ セキュリティ装置上で行われたかのように見えます。

ログ

アクティブ/アクティブ DPI が有効で、スタンバイ セキュリティ装置上で DPI 処理が行われた結果、前述のような DPI 一致アクションが発生した場合、アクションは、一致アクションを検出したスタンバイ装置ではなく、ステートフル HA ペアのアクティブ装置に記録されます。これは、すべての処理がアクティブ装置で実行されたことを示すわけではありません。

高可用性に関連するログ イベントは、「**調査 | ツール | ログ > イベント ログ**」で確認できます。ログについては、『*SonicOS 6.5 調査*』を参照してください。

ネットワーク DHCP とインターフェースの設定

アクティブ/アクティブ クラスタリングが有効になると、SonicOS の内部 DHCP サーバはオフになり、有効にできなくなります。DHCP サーバを必要とするネットワークは、外部の DHCP サーバを使用できます。アクティブ/アクティブ クラスタリング、および削除されたすべての DHCP サーバ リース範囲を有効にする前に、管理インターフェースで SonicOS DHCP サーバを無効にする必要があります。

「**管理 | システム セットアップ >ネットワーク > インターフェース**」では、仮想グループ内のインターフェースに追加の仮想 IP アドレスを設定したり、インターフェースの冗長ポートを設定したりできます。

これらのタスクの実行方法については、以下を参照してください。

- SonicOS DHCP サーバの無効化 (741 ページ)
- 仮想 IP アドレスの設定 (741 ページ)
- 冗長ポートの設定 (742 ページ)

SonicOS DHCP サーバの無効化

SonicOS DHCP サーバを無効にし、すべての DHCP サーバ リース範囲を削除するには:

1 クラスタ ノードのプライマリ装置にログインします。

2 「**管理 | システム セットアップ > ネットワーク > DHCP サーバ**」に移動します。

3 IP バージョンを選択します。(**IPv4** または **IPv6**) を指定できます。

4 「**DHCPv4/6 サーバを有効にする**」をオフにします。

5 「**DHCPv4/6 サーバ リース範囲/スコープ**」で、「**表示形式**」として「**すべて**」を選択してテーブル内のすべてのリース範囲を選択します。

6 テーブルの見出しにある該当するチェックボックスをオンにします。

7 「**削除**」を選択します。

8 確認のダイアログで、「**OK**」を選択します。

9 「**適用**」を選択します。

仮想 IP アドレスの設定

アクティブ/アクティブ クラスタリングが初めて有効になったときに、そのセキュリティ装置のインターフェースに対して設定された IP アドレスは、仮想グループ 1 の仮想 IP アドレスに自動的に変換されます。そのため、仮想グループ 1 には、X0、X1、およびゾーンに対して設定および割り当てが行われているその他のあらゆるインターフェースの仮想 IP アドレスが含まれることになります。

アクティブ/アクティブ クラスタリングでは、仮想グループを追加する場合に仮想 IP アドレスの追加設定が必要になります。複数の仮想 IP アドレス (仮想グループごとに 1 つ) を各インターフェースに割り当てることができます。追加の仮想 IP アドレスのそれぞれは、クラスタ内にある他の仮想グループの 1 つに関連付けられます。各インターフェースは、最大 4 つの仮想 IP アドレスを持つことができます。VLAN インターフェースも、最大 4 つの仮想 IP アドレスを持つことができます。

メモ：トラフィック フローを処理している仮想グループのインターフェース上に仮想 IP アドレスが設定されていない場合、そのインターフェースではパケットを転送できません。

インターフェースに仮想 IP アドレスを設定するには:

1 クラスタ ノードのプライマリ装置にログインします。

2 「**管理 | システム セットアップ > ネットワーク > インターフェース**」に移動します。

3 「**インターフェース設定**」テーブルで、設定するインターフェースの**設定**アイコンを選択します。

4 「**インターフェースの編集**」ダイアログで、「**IP アドレス**」フィールドに仮想 IP アドレスを入力します。ここで、*X* は仮想グループ番号です。

メモ：新しい仮想 IP アドレスは、そのインターフェースの既存の仮想 IP アドレスすべてと同じサブセット内になければなりません。

5 「**OK**」を選択します。設定された仮想 IP アドレスは、「**インターフェース設定**」テーブルに表示されます。

冗長ポートの設定

冗長ポートは、アクティブ/アクティブ クラスタリングと併用できます。未使用の物理インターフェースは、"プライマリ インターフェース" と呼ばれる設定された物理インターフェースへの冗長ポートとして割り当てることができます。プライマリ インターフェースの物理リンクに障害が発生した場合は、冗長インターフェースによって一切の中断なしに処理を続行できます。この機能の利点の 1 つは、物理リンクに障害が発生しても機器のフェイルオーバーを行う必要がないことです。

冗長ポートは、「**管理 | システム セットアップ > ネットワーク > インターフェース > インターフェースの編集 > 詳細**」ダイアログで設定できます。「**冗長ポート**」フィールドは、アクティブ/アクティブ クラスタリングが有効な場合にのみ使用できます。

メモ：すべてのクラスタ ノードは同じ設定を共有するので、各ノードは同じ冗長ポートが設定され、同じスイッチに接続されている必要があります。

インターフェースの冗長ポートを設定するには:

1 クラスタ ノードのプライマリ装置にログインします。

2 「**管理 | システム セットアップ > ネットワーク > インターフェース**」に移動します。

3 「**インターフェース設定**」テーブルで、冗長ポートを作成するプライマリ インターフェースの「**設定**」アイコンを選択します。例例えば、**X2** の「**設定**」アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。

4 「**詳細設定**」を選択します。

5 「**冗長 / 統合ポート**」で、「**ポート冗長化**」を選択します。ダイアログ上のオプションが変化します。

6 「**冗長ポート**」で冗長ポートを選択します。選択肢には未使用のインターフェースのみが表示されます。例えば、**X4** を冗長ポートとして選択します。

7 「**3**」を選択します。

選択したインターフェースは、「**インターフェースの設定**」テーブルで淡色表示されます。冗長ポートであることとそのプライマリ インターフェースを示すメモが表示されます。このインターフェースは、プライマリ ポートの「**インターフェースの編集**」ダイアログの「**冗長ポート**」フィールドにも表示されます。

メモ：プライマリ ポートと冗長ポートは、同じスイッチか、できればネットワーク内の冗長スイッチに物理的に接続されている必要があります。

8 各クラスタ ノードで、プライマリ ポートおよび冗長ポートに同じインターフェース番号を使用して、物理的な接続を複製します。すべてのクラスタ ノードは、マスター ノードと同じ設定を共有します。

アクティブ/アクティブ クラスタリング フルメッシュ

トピック:

- アクティブ/アクティブ クラスタリング フルメッシュの概要 (743 ページ)
- アクティブ/アクティブ クラスタリング フル メッシュの設定 (745 ページ)
- アクティブ/アクティブ フル メッシュのケーブル配線 (746 ページ)

- アクティブ/アクティブ クラスタ セキュリティ装置の設定 (747 ページ)
- 装置 2 台によるアクティブ/アクティブ クラスタ フルメッシュの設定 (749 ページ)

アクティブ/アクティブ クラスタリング フルメッシュの概要

アクティブ/アクティブ クラスタリングのフルメッシュ設定は、アクティブ/アクティブ クラスタリングの設定オプションに対する強化であり、ネットワーク内のあらゆる単一障害点を回避します。ファイアウォールをはじめとするすべてのネットワーク機器は、完全な冗長化のために連携されます。フルメッシュでは、機器 (セキュリティ装置/スイッチ/ルータ) であれリンクであれ、一切の単一障害点が配備に存在しないことが保証されます。すべての機器は、接続先の機器に二重に配線されます。フルメッシュによるアクティブ/アクティブ クラスタリングは、実現可能な最高レベルの可用性と高いパフォーマンスを提供します。

メモ：セキュリティ装置のアップストリーム側ネットワーク内にあるルータは、Virtual Router Redundancy Protocol (VRRP) 向けにあらかじめ設定されている必要があります。

トピック:

- フル メッシュ配備について (743 ページ)
- アクティブ/アクティブ クラスタリング フル メッシュのメリット (743 ページ)
- 冗長ポートと冗長スイッチ (744 ページ)

フル メッシュ配備について

アクティブ/アクティブ クラスタリングのフル メッシュ設定は、アクティブ/アクティブ クラスタリングの設定オプションに対する強化であり、実現可能な最高レベルの可用性と高いパフォーマンスを提供します。フル メッシュ配備では、ネットワークで非常に高いレベルの可用性を実現します。これは、すべての機器 (ルータ、スイッチ、セキュリティ装置など) が 1 つ以上の冗長なパートナーを持つからです。ネットワーク全体に単一障害点がまったく存在しないように、すべての機器が接続対象機器に対して 2 重に配線されています。例えば、すべての SonicWall ファイアウォールは冗長ポートを使用して、各ネットワーキング機器に対して 2 回接続されます。

メモ：フル メッシュ配備では、ポート冗長化が有効かつ実現されている必要があります。

アクティブ/アクティブ クラスタリング フル メッシュのメリット

- **コア ネットワーク内に単一障害点が存在しない**: アクティブ/アクティブ クラスタリング フルメッシュ配備では、セキュリティ装置だけでなく、コア ネットワーク全体にわたって単一障害点が存在しません。パス上のスイッチ、ルータ、セキュリティ装置に同時に障害が発生した場合でも、トラフィック フローの代替パスが必ず利用できるので、最高レベルの可用性を実現できます。
- **ポート冗長化**: アクティブ/アクティブ クラスタリング フルメッシュでは、各クラスタ ノード内の HA 冗長化や、クラスタ内のノード レベルの冗長化に加え、冗長ポートも利用します。ポート冗長化では、プライマリ ポートに障害が発生した場合、バックアップ リンクがトランスペアレントな形で処理を引き継ぎます。この場合、機器レベルのフェイルオーバーは必要ありません。

冗長ポートと冗長スイッチ

冗長ポートは、アクティブ/アクティブ クラスタリングと併用できます。あるポートに障害が発生した場合、そのトラフィックは、HA またはアクティブ/アクティブのフェイルオーバーなしに冗長ポートによってシームレスに処理されます。アクティブ/アクティブ クラスタリングが有効な場合、「**管理 | システム セットアップ > ネットワーク > インターフェース > インターフェースの編集**」ダイアログの「**冗長ポート**」フィールドが利用可能になります。

冗長ポートを設定する場合、インターフェースは未使用、つまり、どのゾーンにも割り当てられていない状態でなければなりません。2 つのポートは、同じスイッチか、できればネットワーク内の冗長スイッチに物理的に接続されている必要があります。

メモ：すべてのクラスタ ノードは同じ設定を共有するので、各ノードは同じ冗長ポートが設定され、同じスイッチに接続されている必要があります。

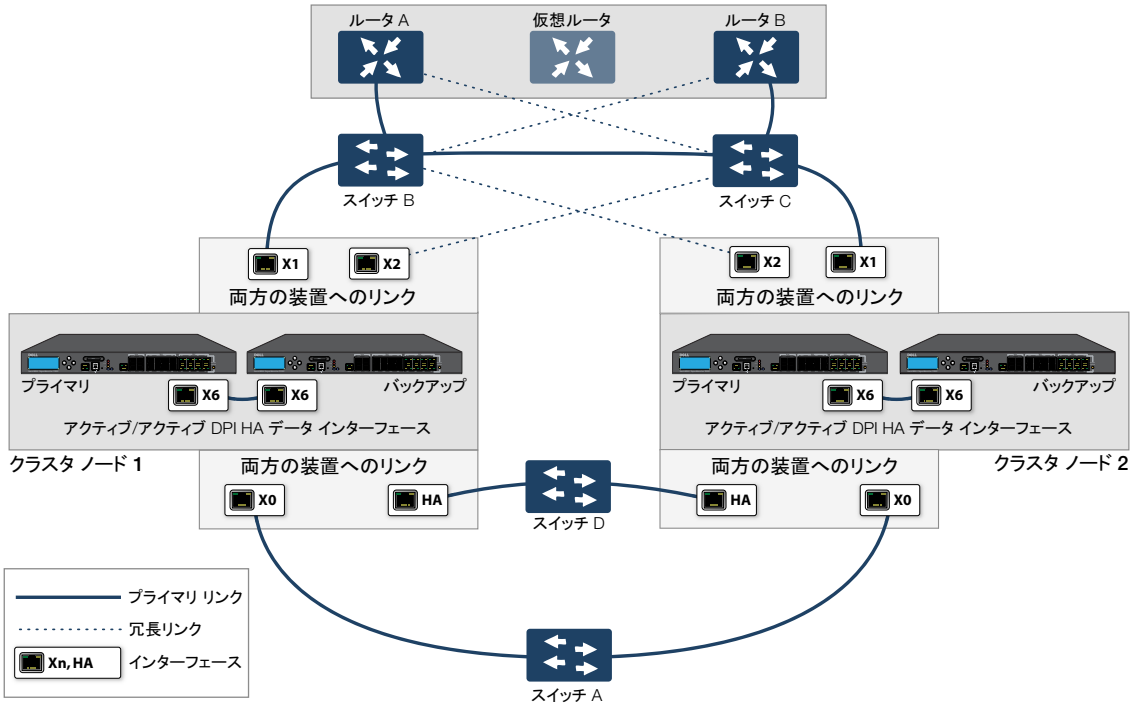
すべてのクラスタ ノードが起動していてトラフィックを通常どおりに処理している間、冗長ポートは、スタンバイ状態のままで、パートナー ポートが何らかの理由でダウンした場合にすぐに使えるように準備されています。あるクラスタ ノードがダウンし、アクティブ/アクティブ フェイルオーバーが発生した場合、残りのクラスタ ノードの冗長ポートは、障害が発生したノードによって所有されていた仮想グループのトラフィックを処理するために直ちに使用されます。これにより、負荷分散が実現されます。

例えば、仮想グループ 1 がクラスタ ノード 1 によって、仮想グループ 2 がクラスタ ノード 2 によって所有されている配備があるとします。各クラスタ ノードには冗長ポート X3 および X4 が設定されています。すべてのノードが適切に機能している場合、X4 ではトラフィックが一切送信されません。クラスタ ノード 2 がダウンした場合は、仮想グループ 2 もクラスタ ノード 1 によって所有されることになります。この時点で、冗長ポート X4 は負荷分散のために使用が開始されます。仮想グループ 1 のトラフィックは X3 で送信され、仮想グループ 2 のトラフィックは X4 で送信されます。より大規模な配備で、クラスタ ノード 1 が 3 つまたは 4 つの仮想グループを所有している場合、トラフィックは冗長ポートの間で分配されます。つまり、仮想グループ 1 および 3 のトラフィックは X3 で、仮想グループ 2 および 4 のトラフィックは X4 で送信されます。

冗長スイッチが設定されている場合、SonicWall では冗長ポートを使用してこのスイッチに接続することを推奨します。冗長ポートを使用せずに冗長スイッチに接続することも可能ですが、その場合はプローブを使用した複雑な設定が必要になります。冗長スイッチは、高可用性機能の必要性に応じて、ネットワーク内の任意の場所に配備できます。例えば、冗長スイッチを通過するトラフィックが事業的に非常に重要な場合は冗長スイッチを WAN 側に配備できます。

「WAN 側の冗長化」は、冗長なルータ、スイッチ、およびポートが WAN 側に含まれていても、LAN 側では冗長化を使用していないのでフル メッシュにはなっていない配備を示しています。

WAN 側の冗長化



冗長ポートや冗長スイッチを配備する場合にフル メッシュは必須ではありませんが、フル メッシュ配備には冗長ポートや冗長スイッチが含まれます。フル メッシュ配備では、メインのトラフィック ポート (LAN、WAN など) のそれぞれで冗長ポートを使用し、冗長スイッチに加えて冗長アップストリーム ルータも使用します。

アクティブ/アクティブ クラスタリング フル メッシュの設定

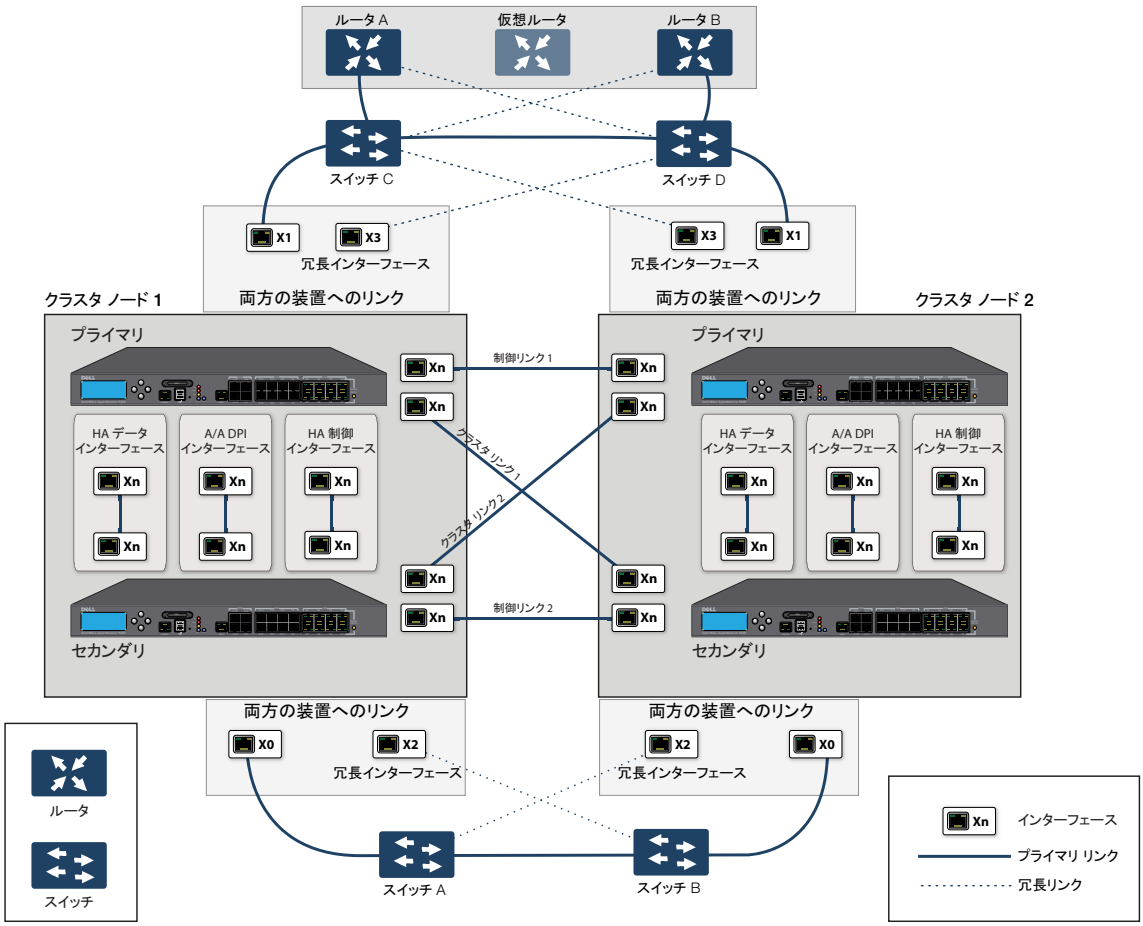
このセクションでは、4 台の装置によるアクティブ/アクティブ クラスタ フルメッシュ配備のセットアップ手順を説明します (「装置 4 台によるアクティブ/アクティブ クラスタ フルメッシュ」を参照)。

- アクティブ/アクティブ フル メッシュのケーブル配線 (746 ページ)
- アクティブ/アクティブ クラスタ セキュリティ装置の設定 (747 ページ)
- 装置 2 台によるアクティブ/アクティブ クラスタ フルメッシュの設定 (749 ページ)

ここで説明する配備は例です。実際の配備は、以下の点で異なる場合があります。

- ネットワークのトポロジ/設計や使用するネットワーク機器の種類 (スイッチ、ルータ、負荷分散機器など)
- 適切な可用性のレベル
- リソースの制約

装置 4 台によるアクティブ/アクティブ クラスタ フルメッシュ



アクティブ/アクティブ フル メッシュのケーブル配線

ここでは、「装置 4 台によるアクティブ/アクティブ クラスタ フルメッシュ」に示した配備のケーブル配線の手順を説明します。

フルメッシュ配備でネットワーク機器を物理的に接続するには:

1 すべてのファイアウォールのすべての HA リンクをスイッチ E のポートベース VLAN に接続します。

2 このセットアップでは、X2 が X0 の冗長ポートになります。X0、X2 の各ポートについてケーブルを次のように接続します。

   a CN2 プライマリ ファイアウォールの X0 をスイッチ A に、X2 をスイッチ B に接続します。

   b CN2 バックアップ ファイアウォールの X0 をスイッチ A に、X2 をスイッチ B に接続します。

   c CN2 プライマリ ファイアウォールの X0 をスイッチ B に、X2 をスイッチ A に接続します。

   d CN2 バックアップ ファイアウォールの X0 をスイッチ B に、X2 をスイッチ A に接続します。

3 スイッチ A とスイッチ B で、以下の作業を行います。

   a X0、X2 インターフェースに接続されているすべてのスイッチ ポートを、同じポートベース VLAN に属するように設定します。

b ファイアウォールに接続されているポートで、スパニング ツリーを有効にし、ポートの高速化 (または等価なコマンド) も有効にします。

4 X3 が X1 の冗長ポートになります。X1、X3 の各ポートについてケーブルを次のように接続します。

a CN2 プライマリ ファイアウォールの X1 をスイッチ C に、X3 をスイッチ D に接続します。

b CN2 バックアップ ファイアウォールの X1 をスイッチ C に、X3 をスイッチ D に接続します。

c CN2 プライマリ ファイアウォールの X1 をスイッチ D に、X3 をスイッチ C に接続します。

d CN2 バックアップ ファイアウォールの X1 をスイッチ D に、X3 をスイッチ C に接続します。

5 スイッチ C とスイッチ D で、以下の作業を行います。

a X1、X3 インターフェースに接続されているすべてのスイッチ ポートを、同じポートベース VLAN に属するように設定します。

b ファイアウォールに接続されているポートで、スパニング ツリーを有効にし、ポートの高速化 (または等価なコマンド) も有効にします。

6 スイッチ A とスイッチ B を互いにケーブルで接続します。

7 スイッチ C とスイッチ D を互いにケーブルで接続します。

8 ルータ A とルータ B が冗長ポートをサポートしている場合は、ファイアウォール ポートをスイッチに接続したときと同じように、これらのルータをスイッチに接続します。つまり、ルータ A のプライマリ ポートをスイッチ C に、ルータ A のバックアップ ポートをスイッチ D に接続します。ルータ B についても同様にポートを接続します。

9 ルータが冗長ポートをサポートしておらず、スイッチングをサポートしている場合は、ルータ A の同じ VLAN 内に 2 つのポートを作成し、ポートではなく VLAN に IP アドレスを割り当てます。その後、一方のポートをスイッチ C に、他方のポートをスイッチ D に接続します。ルータ B についても同じように設定します (「装置 4 台によるアクティブ/アクティブ クラスタ フルメッシュ」のセットアップを参照)。

10 アクティブ/アクティブ DPI は、アクティブ/アクティブ クラスタリングと併用できます。ポート X6 および X7 は、冗長化と、アクティブ セキュリティ装置からスタンバイ セキュリティ装置にオフロードされたトラフィックの負荷分散のための 2 つの HA データ ポートです。以下のケーブル配線を実行します (「装置 4 台によるアクティブ/アクティブ クラスタ フルメッシュ」では、簡略化のために X6、X7 ポートとケーブル配線は省略されています)。

a CN1 プライマリの X6 を CN1 バックアップの X6 にクロスオーバー ケーブルで接続します。

b CN1 プライマリの X7 を CN1 バックアップの X7 にクロスオーバー ケーブルで接続します。

c CN2 プライマリの X6 を CN2 バックアップの X6 にクロスオーバー ケーブルで接続します。

d CN2 プライマリの X7 を CN2 バックアップの X7 にクロスオーバー ケーブルで接続します。

アクティブ/アクティブ クラスタ セキュリティ装置の設定

トピック:

- 設定手順 (748 ページ)
- 障害点が存在しないことのテスト (748 ページ)

設定手順

アクティブ/アクティブ クラスタ セキュリティ装置を設定するには、以下の手順に従います。

1 CN1 プライマリ装置を除くすべてのファイアウォールをシャットダウンします。

2 「**管理 | システム セットアップ > 高可用性 > 基本設定**」ページで以下の手順を実行します。

   a 「**モード**」で、「**アクティブ/アクティブ クラスタリング**」を選択します。

   b 「**ステートフル同期を有効にする**」をオンにします。

   c 「**高可用性装置とノード**」を選択します。

   d クラスタ ノードのプライマリおよびセカンダリ装置のシリアル番号を、該当する「**プライマリ装置のシリアル番号**」および「**セカンダリ装置のシリアル番号**」フィールドに入力します。

   e CN1 については、「**仮想グループ 1 階級**」から「**オーナー**」を、「**仮想グループ 2 階級**」から「**スタンバイ**」をそれぞれ選択します。

   f CN2 については、「**仮想グループ 1 階級**」ドロップダウン メニューから「**オーナー**」を、「**仮想グループ 2 階級**」ドロップダウン メニューから「**スタンバイ**」をそれぞれ選択します。

   g X6、X7 を 2 つの HA データ ポートとしてアクティブ/アクティブ DPI を有効にします。

   h 「**適用**」を選択します。

3 「**管理 | システム セットアップ > ネットワーク > インターフェース**」で以下の手順を実行します。

   a X0 インターフェースと X1 インターフェースの両方に対して仮想グループ (VG) IP アドレスを追加します。

   b 冗長ポートの設定を追加します (X2 を X0 の冗長ポートに、X3 を X1 の冗長ポートにします)。

4 「**管理 | システム セットアップ > 高可用性 > 監視設定**」ページで、クラスタ内の各装置の X0 または X1 のどちらかに監視/管理 IP アドレスを追加します。

5 その他すべてのセキュリティ装置を起動します。CN1 プライマリから他のすべてのセキュリティ装置に対して設定の完全な同期が行われます。

6 専用の監視/管理アドレスを使用して各セキュリティ装置にログインし、以下の操作を行います。

   a MySonicWall でセキュリティ装置を登録します。

   b MySonicWall によってライセンスの同期を行います。

障害点が存在しないことのテスト

上記の配備の接続と設定が終了すると、CN1 は仮想グループ 1 (VG1) の、CN2 は仮想グループ 2 (VG2) のオーナーになります。

X0 の VG1 IP アドレスを特定のトラフィック フローのゲートウェイとして、X0 の VG2 IP アドレスを別のトラフィック フローのゲートウェイとして設定します。以下のように、別の方法でこの設定を行うこともできます。

- ゲートウェイの割り当てを直接的に接続されたクライアント ネットワーク上の各 PC に分散させるスマート DHCP サーバを使用します。
- ポリシー ベースのルートをダウンストリームのルータで使用します。

トラフィックのセットアップが完了すると、両方のクラスタ ノードによってネットワーク トラフィックがアクティブに処理されます。

どの機器やリンクにも単一障害点が存在しないことをテストするには:

1 **機器の障害**: 以下に示すような機器の障害のいずれかが発生しても、トラフィックは両方のクラスタ ノードを流れ続けるはずです。

   a スイッチ B が起動および準備完了の状態でスイッチ A の電源をオフにします。

   b スイッチ A が起動および準備完了の状態でスイッチ B の電源をオフにします。

   c CN1 のスタンバイ装置が起動および準備完了の状態で CN1 のアクティブ装置を SonicOS 管理インターフェースから再起動します (このシナリオは、CN1 のアクティブ装置でソフトウェアの障害が発生した場合に類似しています)。

   メモ：この場合はステートフル HA フェイルオーバーが行われます。

   d CN1 のスタンバイ装置が起動および準備完了の状態で CN1 のアクティブ装置をシャットダウンします (このシナリオは、CN1 のアクティブ装置でハードウェアの障害が発生した場合に類似しています)。

   メモ：この場合はステートフル HA フェイルオーバーが行われます。

   e CN2 についても「ステップ c」および「ステップ d」を繰り返します。

   f ルータ B が起動および準備完了の状態でルータ A をシャットダウンします。

   g ルータ A が起動および準備完了の状態でルータ B をシャットダウンします。

2 **リンクの障害**: 以下に示すようなリンクの障害のいずれかが発生しても、トラフィックは流れ続けるはずです。

   a クラスタ ノード内のアクティブ セキュリティ装置のそれぞれで、X2 が接続された状態で X0 のケーブルを取り外します。

   b クラスタ ノード内のアクティブ セキュリティ装置のそれぞれで、X3 が接続された状態で X1 のケーブルを取り外します。

   c アップストリームのスイッチからアクティブな仮想ルータであるルータへのプライマリリンクを切断します。

   d アクティブ/アクティブ DPI HA データ インターフェースである X6 の接続を切断します。

装置 2 台によるアクティブ/アクティブ クラスタ フルメッシュの設定

各 CN が 1 台のセキュリティ装置だけで構成される (HA バックアップがない)、セキュリティ装置 2 台によるアクティブ/アクティブ クラスタ フルメッシュを配備できます。ただし、そのようなセットアップには以下の制限があります。

- フェイルオーバーがステートフルではないので、既存の接続の再構築が必要になります。
- フェイルオーバー時に各装置のトラフィックがセキュリティ装置 1 台の容量の 50% を超えていた場合、フェイルオーバー後はトラフィックの 50% 超過分が破棄されます。

装置 2 台によるフルメッシュ向けの手順は、装置 4 台によるフルメッシュの手順と似ていますが、以下の点が異なります。

- 各ノードのバックアップ装置に関する手順は適用されません。
- ステートフル同期およびアクティブ-アクティブ DPI の設定に関する手順は適用されません。
- HA ポートの接続に必要なスイッチが存在しません (装置は 2 台だけなので、両装置はクロスオーバー ケーブルで直接接続されます)。

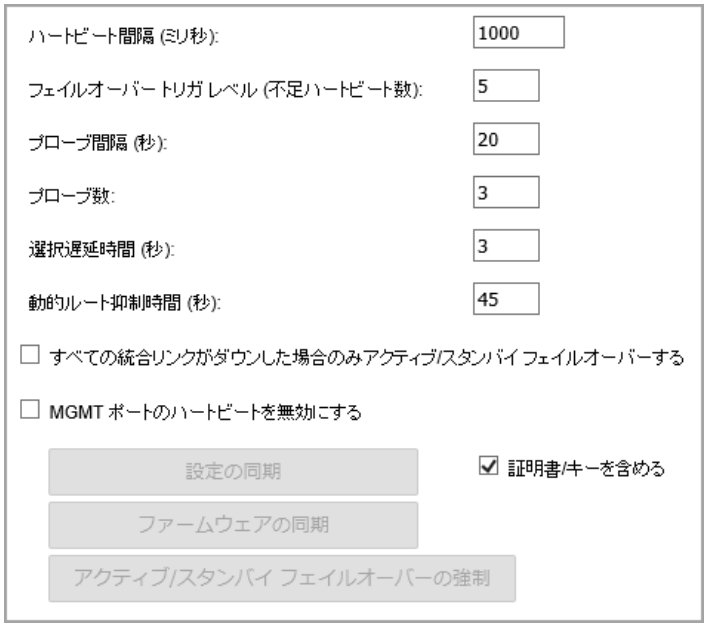
47

高可用性の微調整

トピック:

- 高可用性 > 詳細設定 (750 ページ)
  - 高可用性の詳細設定 (751 ページ)

高可用性 > 詳細設定



「**管理 | システム セットアップ > 高可用性 > 詳細設定**」では、高可用性設定を微調整したり、高可用性セキュリティ装置の間で設定やファームウェアを同期したりできます。「**高可用性 > 詳細設定**」の内容は、アクティブ/スタンバイとアクティブ/アクティブのどちらの設定でも同じです。

「**ハートビート間隔 (ミリ秒)**」および「**フェイルオーバー トリガ レベル (不足ハートビート数)**」の設定は、SVRRP ハートビート (アクティブ/アクティブ クラスタリング ハートビート) と HA ハートビートの両方に適用されます。「**高可用性 > 詳細設定**」のその他の設定は、クラスタ ノード内の HA ペアのみに適用されます。

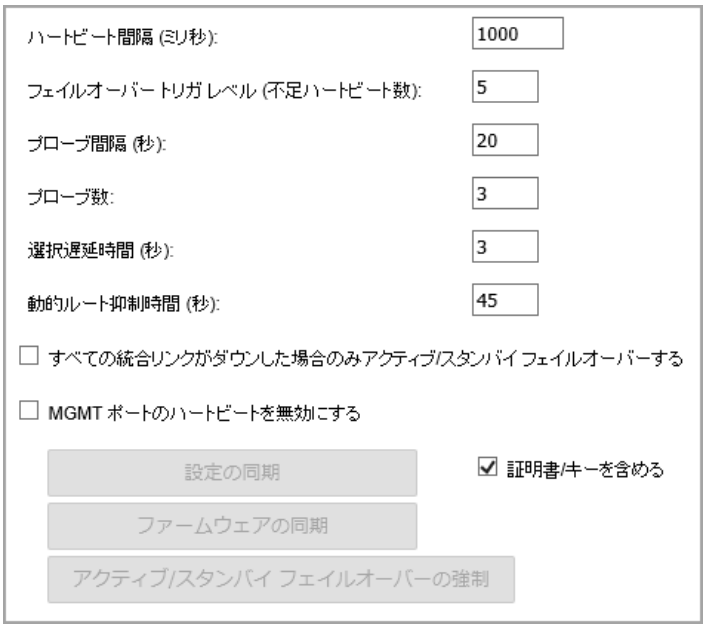
メモ：高可用性の詳細については、「高可用性機能について (694 ページ)」および「アクティブ/スタンバイおよびアクティブ/アクティブ DPI 機能の前提条件 (704 ページ)」を参照してください。

高可用性の詳細設定

詳細設定を設定するには:

1 マスター ノードの SonicOS 管理インターフェース、つまり、仮想グループ 1 の (X0 または HTTP 管理が有効になっている別のインターフェースの) IP アドレスに管理者としてログインします。

2 「**管理 | システム セットアップ > 高可用性 > 詳細設定**」に移動します。



3 必要に応じて「**ハートビート間隔 (ミリ秒)**」を調節して、アクティブ/アクティブ クラスタ内の各セキュリティ装置が通信する頻度を制御します。この設定は、アクティブ/アクティブ クラスタ内のすべての装置に適用されます。既定値は **1,000** ミリ秒 (1 秒)、最小値は 1,000 ミリ秒、最大値は 300000 です。

メモ：SonicWall は、少なくとも 1000 のハートビート間隔に設定することをお勧めします。

大量のネットワーク トラフィックを処理する配備の場合は、高い値を設定してください。値が低すぎると、特にセキュリティ装置の負荷が高い場合に不必要なフェイルオーバーが発生する可能性があります。

このタイマーは、「**フェイルオーバー トリガ レベル (不足ハートビート数)**」タイマーとリンクしています。

4 「**フェイルオーバー トリガ レベル (不足ハートビート数)**」には、フェイルオーバーの実行前に許容されるハートビート欠落回数を設定します。この設定は、アクティブ/アクティブ クラスタ内のすべての装置に適用されます。既定値は **5**、最小値は 4、最大値は 99 です。

このタイマーは、「ハートビート間隔 (ミリ秒)」タイマーとリンクしています。「**フェイルオーバー トリガ レベル (不足ハートビート数)**」が 5 に、「**ハートビート間隔 (ミリ秒)**」が 10,000 ミリ秒 (10 秒) に設定されている場合は、ハートビートがないまま 50 秒が経過するとフェイルオーバーが行われます。

5 「**プローブ間隔 (秒)**」には、ネットワークのクリティカル パスがまだ到達可能であることを監視するために指定された IP アドレスにプローブを送信する間隔を設定します。この間隔は、ローカル HA ペアの論理監視に使用されます。既定値は **20** 秒で、設定可能な範囲は 5 ～ 255 秒です。

ヒント： SonicWall は、少なくとも 5 秒の間隔に設定することをお勧めします。

監視対象 IP アドレスは、「**管理 | システム セットアップ > 高可用性 > 詳細設定**」で設定できます。「高可用性 > 監視設定 (753 ページ)」を参照してください。

6 「**プローブ数**」には、ネットワークのクリティカル パスが使用可能ではない、またはプローブ対象が到達可能ではないと判断するまでに連続して実行するプローブの回数を設定します。この回数は、ローカル HA ペアの論理監視に使用されます。既定値は **3** 回で、設定可能な範囲は 3 ～ 10 回です。

7 「**選択遅延時間 (秒)**」には、インターフェースが起動して安定していると見なされるまでプライマリ セキュリティ装置が待機する秒数を設定します。既定値は **3** 秒、最小値は 3 秒、最大値は 255 秒です。

ヒント：このタイマーは、スパニング ツリー遅延が設定されているスイッチ ポートに役立ちます。

8 「**動的ルート抑制時間 (秒)**」には、新たにアクティブになったセキュリティ装置が以前にルーティング テーブルで学習した動的ルートを保持する秒数を設定します。既定値は **45** 秒、最小値は 0 秒、最大値は 1,200 秒 (20 分) です

メモ：「**動的ルート抑制時間**」の設定は、「**管理 | システム セットアップ > ネットワーク > ルーティング**」で「**高度なルーティング**」オプションを選択した場合にのみ表示されます。

ヒント：大規模または複雑なネットワークでは、この値を大きくすることでフェイルオーバー時のネットワークの安定性を向上できます

この設定は、RIP または OSPF の動的ルーティングを使用している高可用性ペアでフェイルオーバーが発生した場合に使用されます。この間に、新たにアクティブになった装置はネットワーク内の動的ルートを学習します。「**動的ルート抑制時間 (秒)**」の秒数を過ぎると、SonicOS によって古いルートは削除され、RIP または OSPF から学習した新しいルートが実装されます。

9 すべての統合リンクがダウンした場合にのみフェイルオーバーを行うには、「**すべての統合リンクがダウンした場合のみアクティブ/スタンバイ フェイルオーバーする**」をオンにします。このオプションは、既定では選択されていません。

10 HA ペア内ですべての証明書および鍵を装置間で同期させるには、「**証明書/キーを含める**」をオンにします。このオプションは、既定では選択されています。

11 (オプション) プライマリ HA ファイアウォールとセカンダリ HA ファイアウォールの間で SonicOS 設定を同期させるには、「**設定の同期**」を選択します。

12 (オプション) プライマリ HA ファイアウォールとセカンダリ HA ファイアウォールの間でファームウェアのバージョンを同期させるには、「**ファームウェアの同期**」を選択します。

13 (オプション) セカンダリ セキュリティ装置へのアクティブ/スタンバイ HA フェイルオーバーを試みて HA フェイルオーバー機能の適切な動作をテストするには、「**アクティブ/スタンバイ フェイルオーバーの強制**」を選択します。

14 すべての高可用性設定が終了したら、「**適用**」を選択します。すべての設定は、セカンダリ セキュリティ装置またはクラスタ内の他の装置に同期されます。

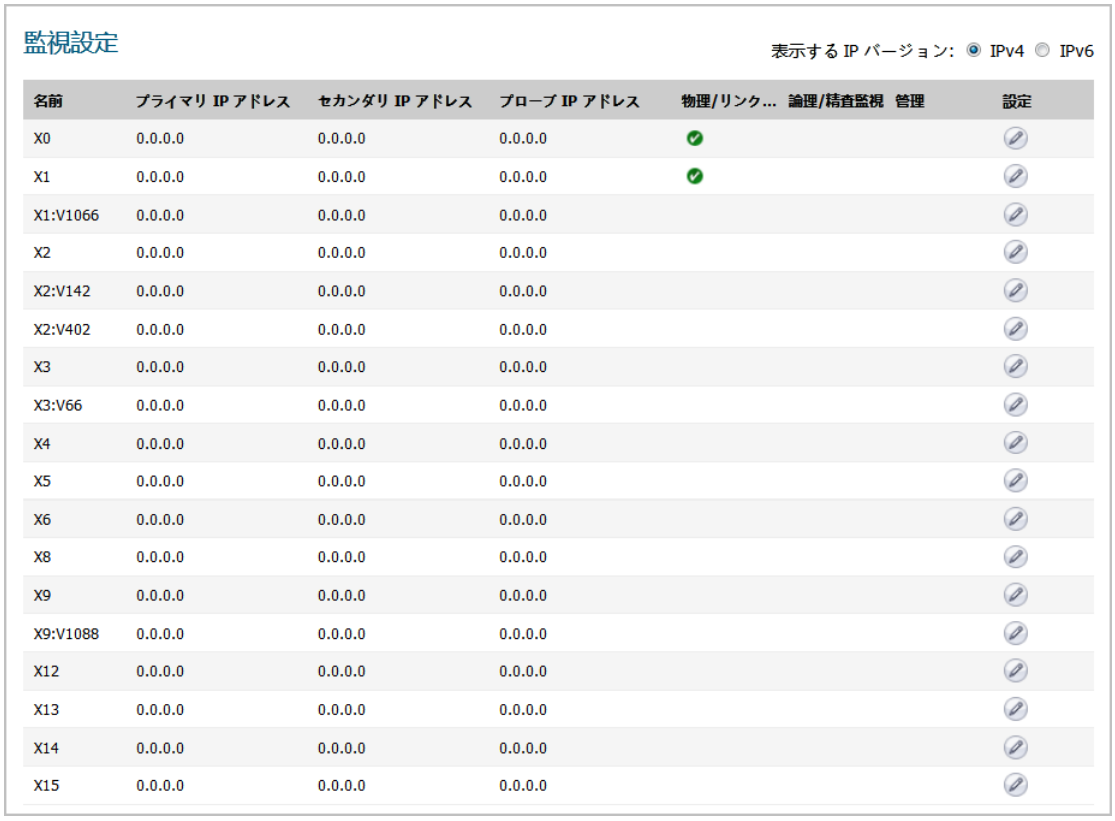
48

高可用性の監視

トピック:

- 高可用性 > 監視設定 (753 ページ)
  - アクティブ/スタンバイ高可用性監視の設定 (754 ページ)
  - IPv6 高可用性監視 (755 ページ)

高可用性 > 監視設定



名前	プライマリ IP アドレス	セカンダリ IP アドレス	プローブ IP アドレス	物理/リンク...	論理/精査監視	管理	設定
X0	0.0.0.0	0.0.0.0	0.0.0.0	✔			
X1	0.0.0.0	0.0.0.0	0.0.0.0	✔			
X1:V1066	0.0.0.0	0.0.0.0	0.0.0.0				
X2	0.0.0.0	0.0.0.0	0.0.0.0				
X2:V142	0.0.0.0	0.0.0.0	0.0.0.0				
X2:V402	0.0.0.0	0.0.0.0	0.0.0.0				
X3	0.0.0.0	0.0.0.0	0.0.0.0				
X3:V66	0.0.0.0	0.0.0.0	0.0.0.0				
X4	0.0.0.0	0.0.0.0	0.0.0.0				
X5	0.0.0.0	0.0.0.0	0.0.0.0				
X6	0.0.0.0	0.0.0.0	0.0.0.0				
X8	0.0.0.0	0.0.0.0	0.0.0.0				
X9	0.0.0.0	0.0.0.0	0.0.0.0				
X9:V1088	0.0.0.0	0.0.0.0	0.0.0.0				
X12	0.0.0.0	0.0.0.0	0.0.0.0				
X13	0.0.0.0	0.0.0.0	0.0.0.0				
X14	0.0.0.0	0.0.0.0	0.0.0.0				
X15	0.0.0.0	0.0.0.0	0.0.0.0				

「**管理 | システム セットアップ > 高可用性 > 監視設定**」では、LAN または WAN インターフェースを使用して、HA ペアの各装置に独立した管理 IP アドレスを設定できます。物理リンク監視と論理精査監視も設定できます。HA 監視設定の詳細については、「アクティブ/アクティブ クラスタリングでの高可用性について (693 ページ)」を参照してください。

トピック:

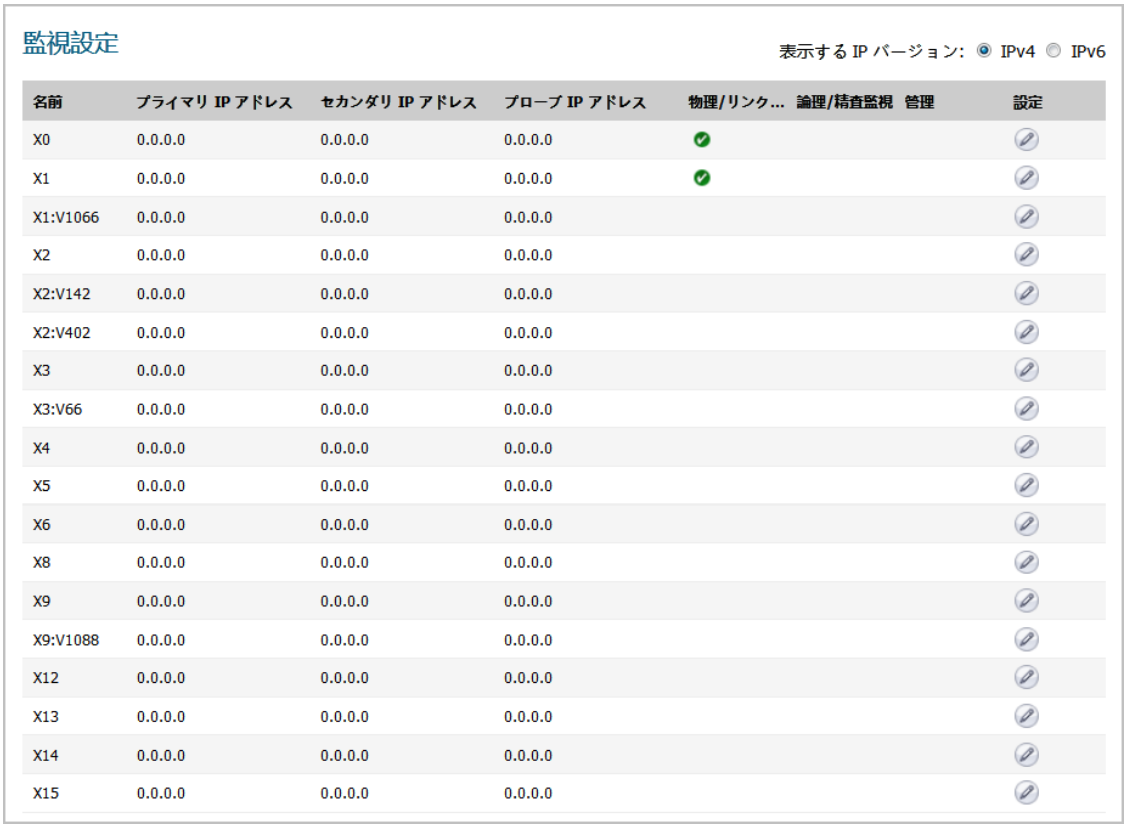
- アクティブ/スタンバイ高可用性監視の設定 (754 ページ)
- IPv6 高可用性監視 (755 ページ)

アクティブ/スタンバイ高可用性監視の設定

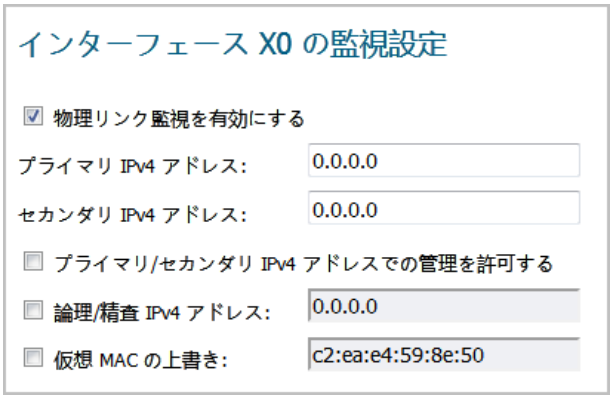
固有の LAN 管理 IP アドレスを設定し、物理/論理インターフェース監視を設定するには:

1 プライマリ SonicWall セキュリティ装置の SonicOS 管理インターフェースに管理者としてログインします。

2 「**管理 | システム セットアップ > 高可用性 > 監視設定**」に移動します。



3 **X0** など、LAN 上のインターフェースの「**設定**」アイコンを選択します。「**HA 監視の編集**」ダイアログ ボックスが表示されます。



4 プライマリ装置およびセカンダリ装置で指定の HA インターフェース間のリンク検出を有効にするには、「**物理リンク監視を有効にする**」を選択したままにします。このオプションは、既定では選択されています。

5 「**プライマリ IPv4/v6 アドレス**」フィールドにプライマリ装置の一意の LAN 管理 IP アドレスを入力します。既定値は 0.0.0.0 です。

6 「**セカンダリ IPv4/v6 アドレス**」フィールドにセカンダリ装置の一意の LAN 管理 IP アドレスを入力します。既定値は 0.0.0.0 です。

7 「**プライマリ/セカンダリ IP アドレスでの管理を許可する**」をオンにします。あるインターフェースに対してこのオプションを有効にすると、「**監視設定**」テーブルにある、そのインターフェースの「**管理**」列に、緑色のアイコンが表示されます。このオプションが有効な場合、1 つのインターフェースに対してのみ管理が許可されます。このオプションは、既定では選択されていません。

8 「**論理/精査 IPv4/v6 アドレス**」フィールドに、接続を監視する LAN ネットワーク上のダウンストリーム機器の IP アドレスを入力します。通常、これはダウンストリームのルータまたはサーバになります(WAN 側でのプローブ処理が望ましい場合は、アップストリームの機器を使用してください)。このオプションは、既定では選択されていません。

プライマリおよびセカンダリ セキュリティ装置から、この監視対象 IP アドレスに対して定期的に Ping が実行されます。両方が送信先への Ping に成功した場合は、フェイルオーバーは発生しません。両方が送信先への Ping に失敗した場合は、セキュリティ装置ではなく送信先に問題があると見なされ、フェイルオーバーは発生しません。しかし、一方のセキュリティ装置が送信先への Ping に成功し、もう一方のセキュリティ装置が失敗した場合は、送信先への Ping に成功したセキュリティ装置へのフェイルオーバーが実行されます。

論理監視が正しく機能できるように、「**プライマリ IPv4/v6 アドレス**」および「**セカンダリ IPv4/v6 アドレス**」のフィールドに、X0 などの LAN インターフェース (WAN でのプローブ処理の場合は X1 などの WAN インターフェース) 上の個別の IP アドレスを設定する必要があります。

9 必要に応じて、インターフェースの仮想 MAC アドレスを手動で指定することもできます。その場合は、「**仮想 MAC の上書き**」を選択し、MAC アドレスをフィールドに入力します。MAC アドレスは、A1:B2:C3:d4:e5:f6 のように、6 つの 16 進数をコロンで区切った形式になっています。このオプションは、既定では選択されていません。

ⓘ **重要**：仮想 MAC アドレスの選択時には、設定エラーが起こらないように注意が必要です。

「**管理 | システム セットアップ | 高可用性 > 詳細設定**」で「**仮想 MAC を有効にする**」をオンにすると、SonicOS ファームウェアによってすべてのインターフェースの仮想 MAC アドレスが自動的に生成されます。SonicOS ファームウェアによって仮想 MAC アドレスが生成されるため、設定エラーは発生しなくなり、仮想 MAC アドレスの一意性が確保され、競合が防止されます。

10 「**OK**」を選択します。

11 他のインターフェースにも監視を設定するには、インターフェースごとに「ステップ 3」から「ステップ 10」を繰り返します。

12 すべての高可用性設定が終了したら、「**適用**」を選択します。すべての設定が自動的にセカンダリ装置に同期されます。

IPv6 高可用性監視

SonicOS の IPv6 実装の詳細については、「IPv6 (979 ページ)」を参照してください。

IPv6 の高可用性 (HA) 監視は、IPv4 での HA 監視の拡張版として実装されています。IPv6 に対する HA 監視を設定した後は、プライマリとバックアップの両方のセキュリティ装置を IPv6 監視アドレスから管理でき、IPv6 監視によって HA ペアのネットワーク状況を検出できます。

「**管理 | システム セットアップ > 高可用性 > 監視設定**」で IPv6 と IPv4 の表示を切り替えて、双方の IP バージョンを容易に設定できます。

IPv6 HA 監視の設定ページは、IPv4 のものを継承しているので、設定手順はほとんど同じです。IPv6 を選択するだけです。その後の設定の詳細については、「高可用性機能について (694 ページ)」および「IPv6 HA 監視に関する考慮事項 (756 ページ)」を参照してください。

IPv6 HA 監視に関する考慮事項

IPv6 HA 監視の設定時には、次の点を考慮します。

- 「**HA 監視の編集**」ダイアログの「**物理リンク監視を有効にする**」と「**仮想 MAC の上書き**」は、レイヤ 2 のプロパティなので淡色表示されています。つまり、これらのプロパティは IPv4 と IPv6 の両方で使用されるので、IPv4 監視のページで設定する必要があります。
- プライマリ/バックアップの IPv6 アドレスはインターフェースの同じサブネット内に存在する必要があり、プライマリ/バックアップ セキュリティ装置のグローバル IP およびリンクローカル IP と同じにすることはできません。
- プライマリ/バックアップの監視 IP が ("::"以外に) 設定されている場合、それらは同じにはできません。
- 「**プライマリ/セカンダリ IPv6 アドレスに対する管理を許可する**」が有効になっている場合は、プライマリ/バックアップの監視 IPv6 アドレスを未指定 (::) にはできません。
- 「**論理/精査 IPv6 アドレス**」が有効になっている場合は、精査 IP を未指定にすることはできません。

第 7 部

システム セットアップ | WAN 高速化

- WAN 高速化の使用

49

WAN 高速化の使用

トピック:

- WAN 高速化について (758 ページ)
  - サポート対象プラットフォーム (759 ページ)
  - 伝送制御プロトコル高速化 (759 ページ)
  - Windows ファイル共有高速化 (760 ページ)
  - ウェブ キャッシュ (760 ページ)
  - WAN 高速化サービスの配備の前提条件 (761 ページ)
  - WXA クラスタリングについて (762 ページ)
  - WXA クラスタリングの仕組み (763 ページ)
  - ルート ポリシーの高速化の許可 (764 ページ)
- システム セットアップ > WAN 高速化 (765 ページ)
  - WAN 高速化の有効化 (765 ページ)
  - グループの管理 (766 ページ)
  - WXA テーブルによる WXA の管理 (771 ページ)
  - VPN ポリシーでの WXA の設定 (787 ページ)
  - SSL VPN トラフィックの高速化の設定 (788 ページ)

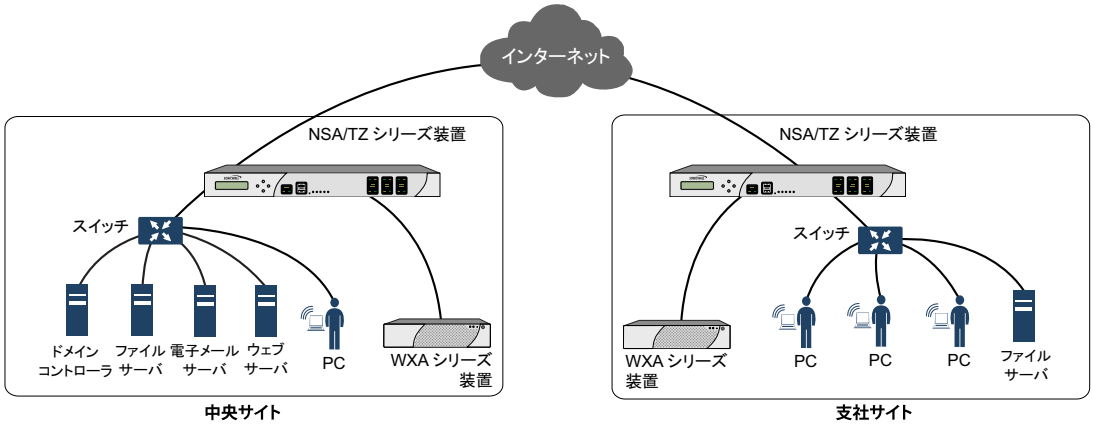
WAN 高速化について

WAN 高速化 (WXA) サービスでは、転送制御プロトコル (TCP) を使う中央サイトとブランチ サイト間の WAN トラフィック、および Windows ファイル共有 (WFS) を高速化することができます。SonicWall WXA シリーズ装置は、SonicWall NSA シリーズ装置と共に配備されます。この種類の配備では、NSA シリーズ装置は攻撃防御といった動的なセキュリティ サービス、仮想プライベート ネットワーク (VPN)、ルーティング、およびウェブ コンテンツ フィルタを提供します。WAN 高速化サービスで、NSA シリーズ装置のパフォーマンスを高めることができます。

重要：「**無線 LAN 制御**」で「**無線制御専用**」モードが選択されている場合、WXA は無効になり、次のメッセージが表示されます。

「SonicWall WXA シリーズ装置のトポロジ」に、SonicWall WXA シリーズ装置と SonicWall セキュリティ装置の基本ネットワーク トポロジを示します。

SonicWall WXA シリーズ装置のトポロジ



トピック:

- サポート対象プラットフォーム (759 ページ)
- 伝送制御プロトコル高速化 (759 ページ)
- Windows ファイル共有高速化 (760 ページ)
- ウェブ キャッシュ (760 ページ)

サポート対象プラットフォーム

WAN 高速化は、次のプラットフォームの SonicOS で利用可能です。

- SuperMassive 9200、9400、および 9600
- TZ600、TZ500/500 W、TZ400/400 W、TZ350/350 W、TZ300/300 W
- NSA 6600/5600/4600/3600/2650/2600
- SOHO 250/250 W、SOHO W

WXA クラスタリングは、現時点では NSA および SuperMassive シリーズのセキュリティ装置でのみ利用できます。

伝送制御プロトコル高速化

TCP 高速化サービスは、WAN 経由で伝送されるデータの量を圧縮を使用して減少させるプロセスです。これにより、中央サイトと支社サイトの間の選択されたトラフィックの伝送が高速化されます。選択されたトラフィックは、データ ブロックとして SonicWall WXA シリーズ装置の共有データベースに保存され、参照インデックスでタグ付けされます。これにより、WXA シリーズ装置は、実際のデータの代わりに (サイズがデータより小さい) 参照インデックスのみを WAN 経由で送信することができます。

Windows ファイル共有高速化

WAN 高速化とは、アプリケーションの高速化、スループットの改善、および遅延の短縮を目的とした幅広い技術のことです。Windows ファイル共有 (WFS) 高速化は、WAN 高速化のサブセットです。

ネットワーク内で WFS 高速化を使用すると、遅延が長く、帯域幅が狭いリンクの影響を少なくすることができます。これは、先読み機能および後書き機能と、変更されていないファイル部分の再転送を回避するための差分ファイルを使用して、ストリーミング動作に近づけることによって実現されます。WFS 高速化により、ブランチ ユーザは、WAN 上で LAN に近い速度で、よく使用されるファイルにアクセスして共有できます。

WFS 高速化ソリューションを配備する分散企業は、ストレージを会社の中央サイトに統合することにより、以前は支社サイトに置かれていたデータをバックアップおよび管理することが不要になります。

ストレージが統合されていない場合、ローカルおよび支社ストレージデータに他のサイトからアクセスするコストと遅延も削減されます。

WXA シリーズ装置は次の WFS 高速化があります。

- 署名なし SMB トラフィック - 署名なし SMB トラフィックをサポートするネットワークでは、WFS 高速化の設定が大幅に簡素化されます。これは、署名なし SMB トラフィックにはセキュリティ レイヤがないためです。このため、WXA シリーズはドメインに参加せずにトラフィックを受信できます。これによって、カスタム DNS ゾーン、逆引き検索、およびファイル共有を設定する必要がなくなります。
- 署名あり SMB トラフィック - SMB 署名が必要なネットワークでは、署名あり SMB トラフィックにセキュリティ レイヤがあるため、セキュリティ装置はドメインに参加する必要があります。署名あり SMB 設定は、署名なし SMB 設定よりも複雑で、粒度が高くなります。署名あり SMB 設定には、その他のオプションがある詳細設定モードもあります。

署名あり SMB 用の拡張サポート

署名あり SMB トラフィック用の拡張サポートは、単一の WXA で処理され、その設定は、その他の WXA クラスタリングで使用されるグループ設定とは別の箇所で行われます。Windows ドメイン上で設定を行うことで、ユーザは、署名あり SMB をサポートするネットワーク上で WFS 高速化モジュールの拡張機能を最大限に活用できます。WXA シリーズ装置が参加しているドメインで、リモート サーバ上のどの共有を WFS 高速化プロセスに含めるかを設定できます。

重要：共有へのリモート アクセスが必要なブランチ サイトで WXA シリーズ装置を設定する前に、ファイル サーバが配置されているサイトで WXA シリーズ装置を設定することを、強くお勧めします。

ウェブ キャッシュ

ウェブ キャッシュ機能は、頻繁および直近に要求されてネットワークを通過したウェブ ページと Youtube 動画のコピーを保存します。したがって、そのようなウェブ ページは、ユーザから要求されるとインターネットからではなくローカル ウェブ キャッシュから取得されるので、帯域幅や応答時間を節約できます。「最小限」、「中程度」、および「アグレッシブ」のキャッシュ方針を利用できます。キャッシュ方針によって、ウェブ キャッシュに入るオブジェクトと、オブジェクトがキャッシュ内にとどまる期間が決まります。

WAN 高速化サービスの配備の前提条件

SonicWall WXA シリーズ装置を配備するには、SonicWall セキュリティ装置が必要です。

SonicWall WXA シリーズ装置を通過するトラフィックでは、インターネット プロトコル バージョン 4 (IPv4) が必要です。WAN 高速化サービスは、IPv6 との互換性はありません。

配備に関して考慮すべき事項

SonicWall WXA シリーズ装置を配備する際は、以下を考慮してください。

- WXA クラスタリングは、NSA および SuperMassive シリーズのセキュリティ装置でサポートされます。こうしたセキュリティ装置には複数の WXA を接続できます。
- WXA クラスタリングでは、WXA シリーズ装置は SonicWall 6.2.2 以降のファームウェアを実行する SonicOS NSA 2600 以降および SuperMassive シリーズのセキュリティ装置との組み合わせで動作します。
- WXA 500 をメモリ モードで実行するには、CD を挿入して PC を起動します。あるいは、ハードディスクにインストールできます。後者の場合、より多くの機能を使用できます。
- 通常、WXA シリーズ装置は、それぞれの SonicWall セキュリティ装置によってサイト間 VPN 設定に配備されます。ただし、ルーティング モードまたは L2 ブリッジ モードも使用できます。
- WXA シリーズ装置を高可用性設定で使用する場合、両方の高可用性ペアへの切り替え接続が必要です。
- WXA シリーズ装置の最初の設定は、WXA セットアップ ウィザードを使用して実行する必要があります。このウィザードを使用するには、SonicWall セキュリティ装置の管理インターフェースにある「**簡易設定**」を選択します。WXA セットアップ ウィザードの詳細については、『*SonicOS 簡易設定*』を参照してください。
- 暗号化トラフィックは高度に乱数化されているため、WXA シリーズ装置の WAN 高速化サービスからは実質的な利益を得られません。したがって、SSL および TLS トラフィック タイプは高速化されません。
- 署名あり SMB を使用した WFS 高速化では、認証および許可に Active Directory、Kerberos、および NTLM を使用する Windows ファイル サービスがサポートされます。
- NTLM クライアントとの署名あり SMB を使用する WFS 高速化では、ドメイン内で有効な認証情報を SonicWall WXA シリーズ装置に提供します。SonicWall WXA シリーズ装置は、ドメイン コントローラによって Kerberos 資格情報を取得します。これにより、ドメインに参加していないクライアント装置をユーザが使用できるようになり、ユーザは有効なドメイン資格情報を得ます。
- WXA シリーズ装置を物理的に接続する前に、管理中の SonicWall セキュリティ装置上で DHCP スコープを作成してください。
- 支社にドメイン コントローラと DNS サーバがある場合、DHCP スコープには、その DNS サーバアドレスおよびドメイン DNS 名を使用することをお勧めします。設定済みの DHCP スコープで、ドメイン名およびドメイン DNS サーバ IP アドレスのみを設定します。WXA シリーズ装置は、装置のドメインへの参加を支援するために、この種の情報に基づいて、Kerberos、LDAP、および NTP サーバを自動検出します。
- LDAP、Kerberos、および NTP サービスを確認します。サイトおよびサービスが明示的に設定されていない複数サイト ドメインでは、WXA シリーズ装置が最も近いサーバを選択しない可能性があります。

- SonicWall は、 WXA シリーズ装置がドメイン コントローラから NTP 更新を取得することをお勧めします。NTP サーバが設定されていない場合、これは自動的に行われます。
- SonicWall は、WXA 名または IP アドレスを保持する Active Directory DNS ゾーンを、セキュリティ更新のみを許可するように設定することをお勧めします。
- WXA シリーズ装置が LAN ゾーンとして接続されているインターフェースのゾーン プロパティを設定します。

WXA クラスタリングについて

メモ：WXA クラスタリングは、NSA 2600 以降の装置でサポートされます。

SonicOS は、2 台以上の NSA シリーズ装置または SuperMassive 装置から成る WXA クラスタリングをサポートします。最大規模の SonicWall WXA シリーズ装置で対応できる接続数は最大 1200 接続で、これは凡そ 240 人の同時ユーザをサポートすることに相当します。このサポート ユーザ数が WXA クラスタリングにより、さらに拡大します。

- SonicOS は、複数の WXA シリーズ装置を対象に同時に監視やプローブを実行し、各 WXA をわかりやすい名前で記録できます。
- SonicOS が実装する負荷共有は、TCP 高速化、署名なし SMB 高速化、WXA ウェブ キャッシュの 3 形態です。
- VPN ポリシーを割り当てれば、常に同じ WXA グループを使用できます。
- 接続数は同じグループ内のすべての WXA シリーズ装置に均等に分散されます。
- いずれかの WXA の接続能力が限界に達すると、グループ内の次の WXA が使われます。

トピック:

- クラスタリングでサポートされるプラットフォーム (762 ページ)
- WXA クラスタリングとは (763 ページ)
- WXA クラスタリングの仕組み (763 ページ)

クラスタリングでサポートされるプラットフォーム

WXA クラスタリングがサポートされる条件は次のとおりです。

- WXA ファームウェア バージョン 1.3.2 以上
- 以下の SonicWall セキュリティ装置:

SM 9600	NSA 6600
SM 9400	NSA 5600
SM 9200	NSA 4600
	NSA 2600
	NSA 3600

WXA クラスタリングとは

WXA クラスタリングは、スループットと耐障害性を高めるために連携して動作する複数の WXA シリーズ装置と定義されています。

メリット

WXA シリーズ装置をクラスタリングすることで、同時に高速化できる接続の数が大幅に増加します。WXA 装置の台数を増やすだけで、その能力を何倍にも高めることができます。「WXA モデルによる最大のユーザ数と接続数」テーブルは、各 WXA プラットフォームで対応できる最大ユーザ数と最大接続数を示しています。

WXA モデルによる最大のユーザ数と接続数

	WXA シリーズ装置				
	WXA 6000	WXA 4000	WXA 2000	WXA 5000	WXA 500 Live
プラットフォーム	ソフトウェア	ハードウェア			
装置	ハードウェア				
装置	仮想				
装置	ソフトウェア				
最大ユーザ数	2000	240	120	360	20
最大接続	10,000	1,200	600	1,800	100

WXA 装置のクラスタリングには、以下の利点があります。

- ユーザと WAN インフラストラクチャの両方に対する高速化ソリューションのスケーラビリティの向上
- 企業とアプリケーションの要件に合わせてスケーリングできる弾力性のあるソリューション
- 1 台または複数の専用 WXA を特定のタスクやネットワーク セグメントに割り当てることができる柔軟性のあるソリューション
- WAN 高速化に対応する耐障害性のあるインフラストラクチャ

WXA クラスタリングの仕組み

WXA クラスタリングでは、複数の WXA シリーズ装置を連結し、負荷分散と接続分散を使用して、処理できる同時接続数を増やします。リモート ロケーションとローカル ロケーションの両方で WXA クラスタリングを実装する必要はありませんが、各ロケーションに少なくとも 1 台の WXA が必要です。

複数の WXA を接続して連携させると、WAN を介して高速化できるデータの量が大幅に増加します。

WXA クラスタリング設定では、WXA はグループのメンバーになり、グループは複数作成することができます。各グループ内の WXA の設定は同じですが、別々のグループの WXA の設定は異なっていても構いません。

WXA の設定は、SonicWall セキュリティ装置の SonicOS から配布されます。

トピック:

- 制限 (764 ページ)

- WXA クラスタリングのライセンス (764 ページ)

制限

WXA クラスタリングでは、署名あり SMB の WFS 高速化はサポートされません。署名あり SMB を高速化する単一の専用 WXA を使用すれば、署名あり SMB の WFS 高速化がサポートされます。その WXA はグループに属していても、属していなくても構いません。とはいえ、クラスタリング グループから除外することで、WXA は署名あり SMB トラフィックの高速化に専念できるようになります。

WXA クラスタリングのライセンス

WXA クラスタリングのライセンスは、高速化をサポートする同時接続の最大数に基づいて購入します。高速化される接続の数に合わせて WXA クラスタリング ライセンスを購入できます。

WXA 500、WXA 5000、および WXA 6000 では、必要な接続数に基づいて WXA クラスタリング ライセンスを購入します。各ライセンスは、許可される最大接続数を表します。高速化されるのは、ライセンスされている最大接続数のみです。最大接続数を超える接続が SonicWall セキュリティ装置を通過した場合、超過分の接続も確立されますが、高速化はされません。

WXA 2000 と WXA 4000 では、追加のライセンスは不要です。これらのモデルでは、装置に組み込まれている最大接続数が、そのまま高速化される最大接続数になります。

WXA 500、WXA 5000、または WXA 6000 が含まれるクラスタに WXA 2000 または WXA 4000 を追加すると、接続数はその分だけ増加します。例えば、クラスタに WXA 2000 に追加すると、許可される接続数に 600 の同時接続が追加されます。

SonicWall セキュリティ装置には仮想 WXA 500、WXA 5000、および WXA 6000 を何台でも追加できますが、高速化される接続の数は、購入されたライセンスによって異なります。

許可された高速化される接続数を超えた場合、クラスタ内に何台の WXA があるかにかかわらず、超過分の接続はすべてクラスタをバイパスします。ライセンスされた接続数をサポートするのに十分な数の WXA をセキュリティ装置に接続することは、管理者の責任です。

ルート ポリシーの高速化の許可

WXA を設定した後、ルート ポリシーの高速化を許可することができます。ルート ポリシーの高速化の許可は、「**システム セットアップ > WAN 高速化**」ページ、または「**ネットワーク > ルーティング**」ページで行います (「ルート通知とルート ポリシーの設定 (486 ページ)」を参照してください)。

ネットワークで VPN をまだ設定していない場合で、ユーザ定義ルート ポリシーを使用している場合は、各サイトに 2 つのルート ポリシーを追加する必要があります。つまり、送信トラフィック用のルーティング ポリシーと、受信トラフィック用のルーティング ポリシーです。

システム セットアップ > WAN 高速化

トピック:

- WAN 高速化の有効化 (765 ページ)
- グループの管理 (766 ページ)
- WXA テーブルによる WXA の管理 (771 ページ)
- VPN ポリシーでの WXA の設定 (787 ページ)
- SSL VPN トラフィックの高速化の設定 (788 ページ)

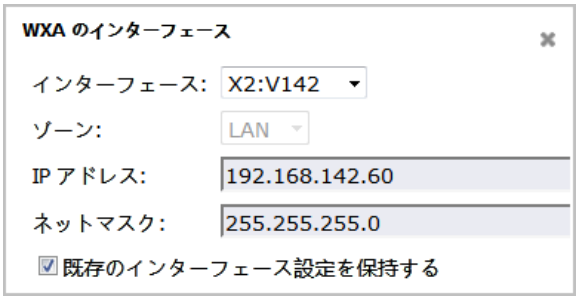
WAN 高速化の有効化

WAN 高速化を有効にするには、以下の手順に従います。

1 「**システム セットアップ > WAN 高速化**」に移動します。

2 「**WAN 高速化**」セクションで、「**WAN 高速化を有効にする**」を選択します。

3 「**インターフェース**」の**編集**アイコンを選択して、WXA の接続先インターフェースを選択します。「**WXA のインターフェース**」ポップアップが表示されます。



4 「**インターフェース**」で、WXA の接続先インターフェースを選択します。

5 「**ゾーン**」で、インターフェースのゾーンを選択します。

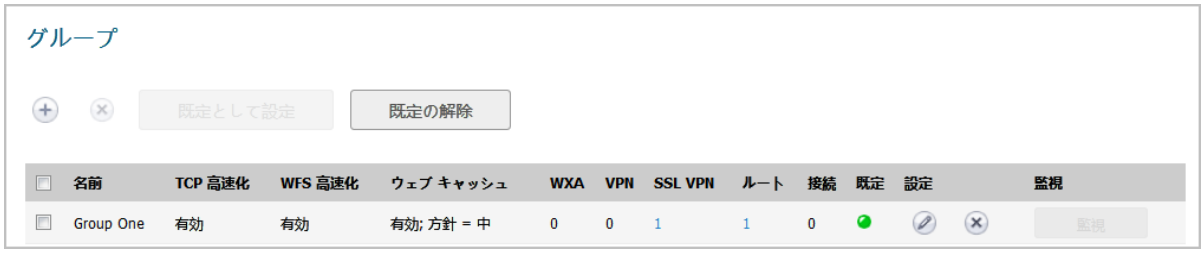
6 「**IP アドレス**」フィールドに、選択したインターフェースの IP アドレスを入力します。

> **重要**：WXA にアドレスを割り当てるために使用される DHCP の範囲は、インターフェースの IP アドレスとネットマスクによって決定されます。

7 「**ネットマスク**」フィールドに、選択したインターフェースのネットマスクを入力します。

8 「**OK**」を選択します。

グループの管理



列	表示対象
名前	グループの名前
TCP 高速化	TCP 高速化が**有効**か**無効**か
WFS 高速化	WFS 高速化が**有効**か**無効**か
ウェブ キャッシュ	• ウェブ キャッシュが**有効**か**無効**か • キャッシュ方針: **弱**、**中**、または**強**
WXA	見つかった使用可能な WXA (オンラインおよびクラスタ レディ) の数と、グループに対して設定されている数: *見つかった数/設定されている数*。
VPN	グループによって高速化が管理されている VPN の数:
SSL VPN	グループによって高速化が管理されている SSL VPN の数。
ルート	グループによって高速化が管理されているルートの数。
接続	グループ内で現在 WXA を経由している接続の数。数値にマウス ポインタを重ねると、次の情報を示すポップアップが表示されます。 • グループ内で WXA モデルごとにサポートされる接続の総数: • 高速化できる同時接続のライセンスされている総数:
既定	緑色のアイコンは既定のグループを示します。

列	表示対象
設定	グループの**編集**アイコンと**削除**アイコンがあります。
監視	「**WXA 接続**」監視を表示するための「**監視**」ボタンがあります。

トピック:

- グループの追加 (767 ページ)
- 既定グループの設定 (769 ページ)
- グループの編集 (769 ページ)
- グループの削除 (770 ページ)

グループの追加

グループを追加するには、以下の手順に従います。

1 「**システム セットアップ > WAN 高速化**」に移動します。

2 「**グループ**」セクションの**追加**アイコンを選択します。「**グループの作成**」ダイアログが表示されます。

3 グループに対する意味のある名前を「**名前**」フィールドに入力します。

4 グループを既定のグループとして指定するには、「**既定グループとして使用する**」を選択します。このオプションは、既定では選択されていません。

5 以下、状況に応じて、

- TCP 高速化を使用しない場合は、「ステップ 10」に進みます。
- TCP 高速化を使用する場合は、「**TCP 高速化**」を選択します。

6 「**TCP 高速化を有効にする**」を選択します。

7 「**TCP 高速化モード**」でモードを選択します。

- **既定で除外されているものを除くすべての TCP サービス** (既定の設定。「サービス オブジェクト」ドロップダウンはグレーアウトされています)。「ステップ 9」に進みます。

- **サービス オブジェクトで指定されているものを除くすべての TCP サービス**
- **サービス オブジェクトで指定されているものと既定で除外されているものを除くすべての TCP サービス**
- **サービス オブジェクトで指定されている TCP サービスのみ** (TCP 高速化をそのサービス オブジェクトに対してのみ有効にする場合)

  ヒント：除外されている TCP サービスを確認するには、「**TCP 高速化モード**」にマウス ポインタを重ねて、除外サービスの一覧を示すポップアップを表示します。

8 「**サービス オブジェクト**」で、除外または包含の対象となるサービス オブジェクトを選択します。

9 アドレス オブジェクトを TCP 高速化から除外するには、「**常に除外されるアドレス オブジェクト**」でそのアドレス オブジェクトを選択します。既定の設定は「**なし**」です。

10 以下、状況に応じて、

- WFS 高速化を使用しない場合は、「ステップ 12」に進みます。
- WFS 高速化を使用する場合は、「**WFS 高速化**」を選択します。

11 「**WFS 高速化を有効にする**」を選択します。

12 以下、状況に応じて、

- ウェブ キャッシュを使用しない場合は、「ステップ 19」に進みます。
- ウェブ キャッシュを使用する場合は、「**ウェブ キャッシュ**」を選択します。

13 「**ウェブ キャッシュを有効にする**」を選択します。

14 「**ウェブ サーバ ポート**」で、トラフィックをインターセプトして WXA ウェブ キャッシュに送信するウェブ サーバ ポートを表すサービス オブジェクトを選択します。既定の設定は「**HTTP**」です。

15 「**クライアント包含アドレス オブジェクト**」で、ウェブ トラフィックが WXA ウェブ キャッシュを経由するように転送されるローカル サブネットを表す、アドレス オブジェクトまたはアドレス グループを選択します。既定の設定は「**LAN Subnets**」です。

16 「**サーバ除外アドレス オブジェクト**」で、WXA ウェブ キャッシュを通したトラフィック転送の対象外となるウェブ サーバ送信先アドレスが含まれたアドレス オブジェクトまたはアドレス グループを選択します。既定の設定は「**なし**」です。この場合、どのウェブ サーバも除外されず、すべての適切なトラフィックが WXA を通して送信されます。

17 「**キャッシュ方針**」で、キャッシュされるオブジェクトの種別を決定するキャッシュ方針と、オブジェクトがキャッシュに保存される期間を指定するプロパティを選択します。

弱	基本的なキャッシュを提供します。この場合、ウェブ キャッシュは、HTTP ヘッダーで明示的にキャッシュしないように指定 (no cache、または expire の時刻が過ぎているなど) されていない限り、オブジェクトをキャッシュします。
中	それよりも制約が緩く、より長期間オブジェクトをキャッシュに保存します。このオプションは既定の設定です。
アグレッシブ	no store、reload などのヘッダー オプションを無視し、expire の時刻よりも優先されます。 **注意：この方針は HTTP の標準規格に違反しており、望ましくない結果となる可能性があるため、使用する際には注意が必要です。**

メモ：「**中**」および「**強**」のモードには、YouTube 動画のキャッシュが含まれます。

18 必要に応じて、「**管理者の電子メール**」フィールドに、管理者の電子メール アドレスを入力します。

19 「**OK**」を選択します。

既定グループの設定

通常、既定グループは、グループの設定時に指定されますが (「グループの追加 (767 ページ)」を参照してください)、既定グループはいつでも変更することができます。

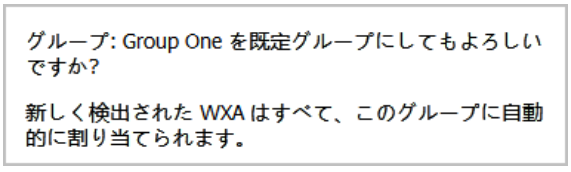
既定グループを変更するには、以下の手順に従います。

1 「**システム セットアップ > WAN 高速化**」に移動します。

2 「**グループ**」テーブルで、既定グループの選択を解除します。

3 既定になるグループを選択します。「**既定として設定**」が使用可能になります。

4 「**既定として設定**」を選択します。確認メッセージが表示されます。



5 「**はい**」を選択します。すると、緑色のインジケータが既定グループの「**既定**」列に表示されます。

グループの編集

グループを編集するには:

1 「**システム セットアップ > WAN 高速化**」に移動します。

2 「**グループ**」テーブルで、編集するグループの**編集**アイコンを選択します。「**グループの編集**」ダイアログが表示されます。

3 「グループの追加 (767 ページ)」の「ステップ 3」から「ステップ 19」を実行します。

グループの削除

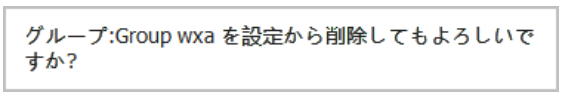
1 つ以上のグループを削除できます。WXA が関連付けられているグループ、または 1 つ以上の VPN、SSL VPN、またはルートの高速化の管理に使用されているグループは削除できません。

グループを削除するには、以下の手順に従います。

1 「**システム セットアップ > WAN 高速化**」に移動します。

2 「**グループ**」テーブルで、削除するグループを選択します。

3 グループの**削除**アイコンを選択します。確認メッセージが表示されます。



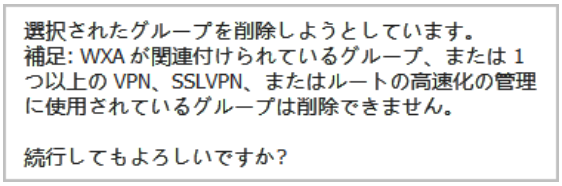
4 「**はい**」を選択します。

複数のグループを削除するには、以下の手順に従います。

1 「**システム セットアップ > WAN 高速化**」に移動します。

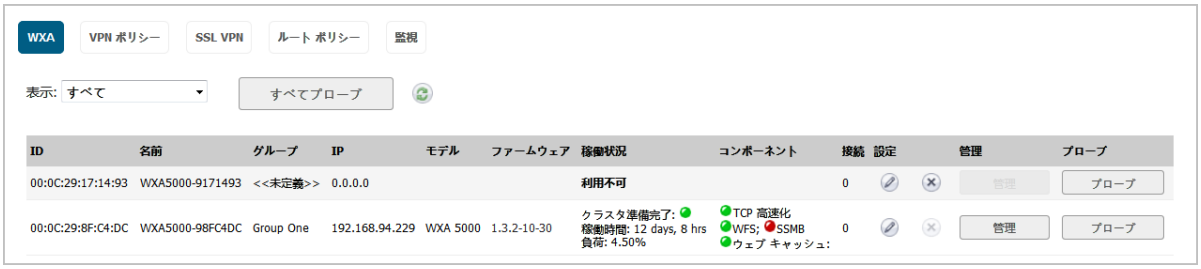
2 「**グループ**」テーブルで、削除するグループを選択します。テーブルの上にある削除アイコンが使用可能になります。

3 「**削除**」アイコンを選択します。確認メッセージが表示されます。



4 「**はい**」を選択します。

WXA テーブルによる WXA の管理



ID WXA シリーズ装置の MAC アドレス。

名前 WXA シリーズ装置の名前。

グループ WXA シリーズ装置が属するグループ。

IP WXA シリーズ装置の IP アドレス。

モデル WXA シリーズ装置のモデル。

ファームウェア WXA シリーズ装置にインストールされているファームウェアのバージョン。

メモ： WXA シリーズ装置のファームウェア バージョンを選択すると、「**管理 | 更新 | WXA ファームウェア**」に移動します。WXA ファームウェアおよびその更新方法については、『*SonicOS 更新*』を参照してください。

稼働状況 WXA シリーズ装置の稼働状況を表示します。

- **クラスタ準備完了** - 緑色のドットは、WXA がクラスタリングで使用可能であることを示します。
- **稼働時間** - WXA が稼働している日数および時間です。
- **負荷** - WXA 上の移動平均負荷のパーセント表示です。

コンポーネント

- **TCP 高速化**
- **WFS 高速化**
- **署名あり SMB 用の WFS 拡張サポート**
- **ウェブ キャッシュ**

高速化コンポーネントの状況を表示します。

- 緑色のドットは、サービスが WXA 上で稼働していることを示します。
- 白いドットは、サービスが WXA 上で稼働しており、トラフィックの高速化に利用可能ですが、コンポーネントは現在、WXA のグループ設定で無効になっていることを示します。

接続 現在 WXA を経由している接続の数。このツール チップには、以下の情報も表示されます。

- この特定の WXA モデルによってサポートされる接続の最大数。
- 高速化できる同時接続のライセンスされている総数。

設定 **編集**アイコンと**削除**アイコンがあります。

メモ： アクティブな WXA シリーズ装置は削除できません。

管理 「**管理**」ボタンを押すと、「**WXA を管理する**」ダイアログが表示されます。

プローブ 「**プローブ**」ボタンを押すと、WXA のプローブが行われ、テーブル内の統計が更新されます。

トピック:

- WXA テーブルのフィルタ処理 (772 ページ)
- プローブ (772 ページ)
- WXA テーブルの再表示 (772 ページ)
- 署名あり SMB 用の拡張サポートを有効にしています (773 ページ)

WXA テーブルのフィルタ処理

既定では、すべての WXA がテーブルに表示されます。表示対象を制限して、選択されているグループまたは未割り当ての WXA のみを表示できます。

WXA テーブルの表示をフィルタするには、以下の手順に従います。

1 「**システム セットアップ > WAN 高速化**」に移動します。

2 「**表示**」で、表示対象を選択します。

すべて (既定)	すべての WXA を表示します。
選択されたグループ	選択されているグループに属する WXA のみを表示します。
未定義	どのグループにも割り当てられていない WXA のみを表示します。

3 「**選択されたグループ**」を選択した場合は、「**グループ**」テーブルで、表示する WXA が含まれているグループを選択します。

プローブ

プローブ (監視) は、WXA シリーズ装置の存在と状況を確認します。また、最新グループ設定を WXA シリーズ装置にプッシュします。個々の WXA またはすべての WXA をプローブできます。

すべての WXA をプローブするには、以下の手順に従います。

1 「**システム セットアップ > WAN 高速化**」に移動します。

2 「**すべてプローブ**」を選択します。WXA テーブルが更新されます。

個々の WXA をプローブするには、以下の手順に従います。

1 「**システム セットアップ > WAN 高速化**」に移動します。

2 WXA テーブルで、該当する WXA の「**プローブ**」列にある「**プローブ**」を選択します。その WXA の表示が更新されます。

WXA テーブルの再表示

WXA テーブルの再表示を行うと、WXA のリストの表示が、各 WXA 上の異なる高速化コンポーネントの状況と共に更新されます。

WXA テーブルを再表示するには、以下の手順に従います。

1 「**システム セットアップ > WAN 高速化**」に移動します。

2 **再表示**アイコンを選択します。

署名あり SMB 用の拡張サポートを有効にしています

ヒント：署名あり SMB 用の拡張サポートをすばやく設定するには、署名あり SMB セットアップ ガイドを使用します。署名あり SMB セットアップ ガイドの WFS にアクセスするには、SonicOS 管理インターフェースの「**簡易設定**」を選択します。このガイドの詳細については、『*SonicOS 簡易設定*』を参照してください。

メモ：署名あり SMB 用の WFS 拡張サポートの設定は、グループ設定とは別の箇所で行われます。

署名あり SMB 用の WFS 拡張サポートを設定する際には、署名あり SMB トラフィックの高速化のための専用の WXA シリーズ装置を選択します。

トピック:

- 拡張サポート署名あり SMB (773 ページ)
- 詳細モード (777 ページ)
- ドメインの詳細 (779 ページ)
- ローカル/リモート サーバ テーブル (781 ページ)

拡張サポート署名あり SMB

署名あり SMB 高速化用の拡張サポートを設定するには、以下の手順に従います。

1 「**システム セットアップ > WAN 高速化**」に移動します。

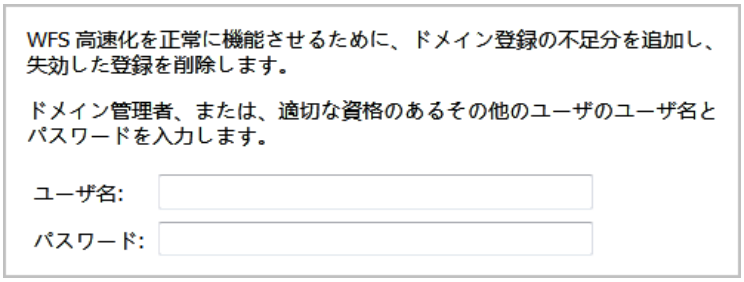
2 「**拡張サポート署名あり SMB**」を選択します。「**署名あり SMB 高速化用の拡張サポート**」ダイアログが表示されます。

3 「**署名あり SMB 用の拡張サポートを有効にする**」を選択します。このオプションは、既定では選択されています。

4 **編集**アイコンを選択して、拡張サポート専用にする WXA を選択します。

> **重要**：既に署名あり SMB 高速化用の拡張サポートの専用になっている WXA を変更すると、すべてのアクティブなセッションとファイル転送が停止するため、データが紛失する可能性があります。
>
> 新しい WXA はドメインに参加し、関連するサーバおよび共有が設定されている必要があります。新しい WXA の設定を反映してエンド ユーザの機器上のパスを変更する必要があります。これを行わない場合、同じパスを維持するには、同じホスト名と同一設定の新しい WXA を設定する前に、最初の WXA のドメイン参加を解除して、すべてのドメイン登録を削除する必要があります

5 「**ドメイン登録の更新**」を選択して、SPN エイリアスと "委任に対する信頼" のための、ドメイン登録の不足分を追加し、失効した登録を削除します。「**ドメイン登録の更新**」ポップアップが表示されます。

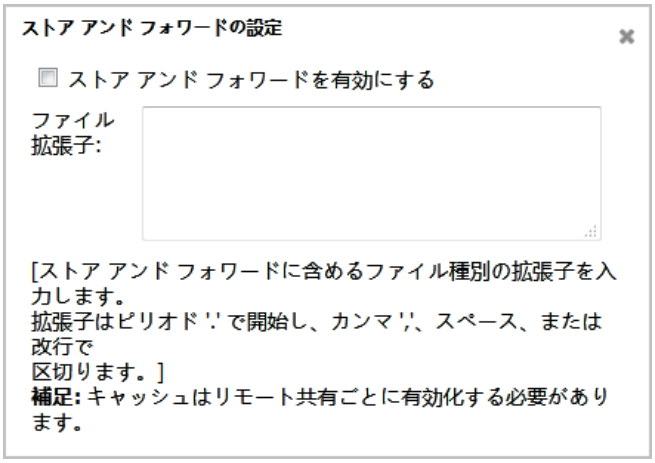


6 ドメイン管理者のユーザ名とパスワードを「**ユーザ名**」と「**パスワード**」のフィールドにそれぞれ入力します。

7 「**登録の更新**」を選択します。

8 ストア アンド フォワードを使用しない場合は、「ステップ 17」に進みます。

9 ストア アンド フォワードの設定を行うには、「**設定**」を選択します。「**ストア アンド フォワードの設定**」ダイアログが表示されます。



10 「**ストア アンド フォワードを有効にする**」を選択します。このオプションは、既定では選択されていません。

11 「**ファイル拡張子**」フィールドに、ストア アンド フォワードに含めるファイル種別の拡張子を入力します。拡張子はピリオド (.) で開始し、カンマ、スペース、または改行で区切ります。

> **メモ**：キャッシュはリモート共有ごとに有効化する必要があります。

12 「**OK**」を選択します。

13 ストア アンド フォワードの現在のファイル操作を表示するには、「**表示**」を選択します。「**ストア アンド フォワード**」ダイアログが表示されます。

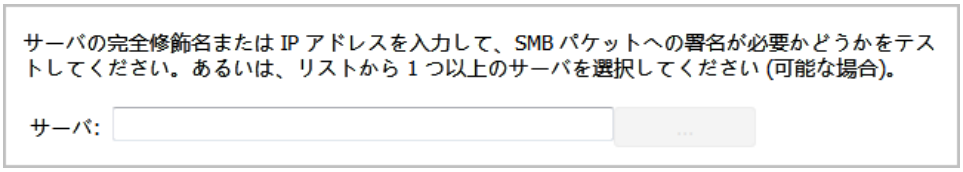
14 適宜、以下の操作を行います。

- 表示を更新するには、**再表示**アイコンを選択します。
- 表示を停止するには、**停止**アイコンを選択します。

15 再表示間隔を変更する場合は、「**再表示**」フィールドにその間隔を入力します。最小値は 1 秒、最大値は 999 秒、既定値は **600** 秒です。

16 署名のテストを行わない場合は、「ステップ 24」に進みます。

17 指定されたサーバへのトラフィックに署名が必要かどうかをテストするには、「**署名テスト**」を選択します。「**署名テスト**」ダイアログが表示されます。



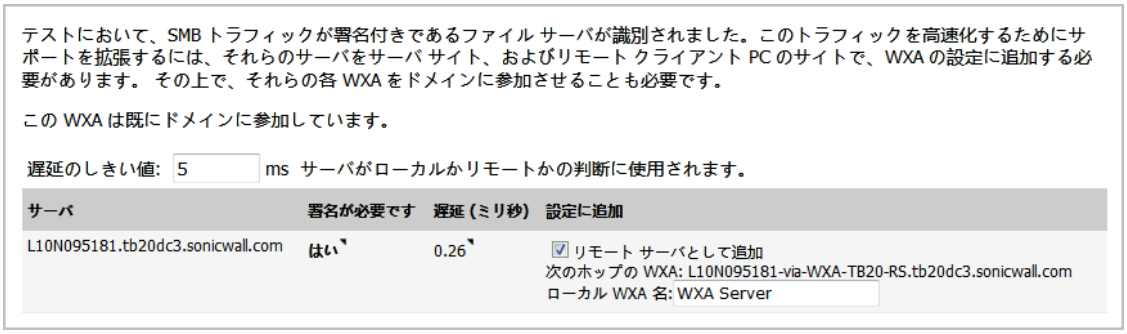
18 次のどちらかを行います。

- テストするサーバの完全修飾名または IP アドレスを入力します。
- **リスト** (...) を選択してサーバのリストを表示します。「**テストするサーバを選択**」ポップアップが表示されます。

19 1 つ以上のサーバを選択します。

20 「**OK**」を選択します。ポップアップが閉じられます。

21 「**OK**」を選択します。テスト結果が表示されるまでに数分かかることがあるので、そのままお待ちください。



重要：SMB 署名が必要な場合は、WXA シリーズ装置がドメインに参加する必要があります。テスト結果には、WXA シリーズ装置がドメインに参加しているかどうかが示されます。

ヒント：署名が必要な場合は、次の表示の近くにあるツールチップにマウス ポインタを置くと情報が表示されます。

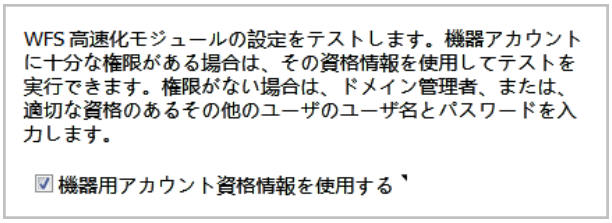
- 「**はい**」のツールチップにより、署名に必要なアドレスが表示されます。
- 遅延時間のツールチップにより、「**遅延のしきい値**」に設定されている時間に対してのサーバの超過時間が表示されます。

22 サーバがローカルかリモートかを判断するためのしきい値を指定するには、「**遅延のしきい値**」に、そのミリ秒数を入力します。最小値は 1 ミリ秒、最大値は 99999999 ミリ秒、既定値は **5** 秒です。

23 「**OK**」を選択します。

24 WFS 高速化のテストを行わない場合は、「ステップ 29」に進みます。

25 WFS 高速化モジュールのテストを行うには、「**設定のテスト**」を選択します。「**設定のテスト**」ポップアップが表示されます。



26 WXA シリーズ装置が適切な権限を持つそれ自体の機器アカウントを所有している場合は、「**機器用アカウント資格情報を使用する**」を選択します。このオプションは、既定では選択されています。

メモ：WXA に適切な権限がない場合は、ドメイン管理者の管理者用ユーザ名とパスワードの入力が必要になります。

27 「**テストの実行**」を選択します。テスト結果が表示されるまでに数分かかることがあるので、そのままお待ちください。

サーバ	テストするサーバのサービス プリンシパル名 (SPN)
解決結果	IP アドレス。緑色のチェックマークは正しく解決されたことを示します。
共有設定に使用	SPN が装置識別用の名前としてどのように使用されるかを示します。
短い SPN	短い SPN が機器アカウント上に存在するかどうかを示します。
長い SPN	長い SPN が機器アカウント上に存在するかどうかを示します。
委任に対する信頼	緑色のチェックマークは、サーバが委任に対して信頼されているかどうかを示します。 • 全般的 - サーバは委任に対して全般的に信頼されています。 • 特定のホスト - ツールチップの上にマウス ポインタを置くと、サーバが委任に対して信頼されているホストが表示されます。
委任の適用	緑色のチェックマークは、サーバが委任を受け入れていることを示します。ツールチップの上にマウス ポインタを置くと、サーバの短い名前または長い名前を使用した資格情報を提示できるホストが表示されます。
許可された接続	緑色のチェックマークは、サーバが認証接続を受け入れたことを示します。ツールチップの上にマウス ポインタを置くと、接続が表示されます。
伝搬された接続	緑色のチェックマークは、サーバが認証接続を伝搬したことを示します。ツールチップの上にマウス ポインタを置くと、接続が表示されます。
逆引き DNS	逆引き DNS の解決方法を示します。

28 「**閉じる**」を選択します。

29 詳細モードを使用するには、「**詳細モード**」を選択します。このオプションは、既定では選択されていません。

詳細モード

「**詳細モード**」が選択されている場合、「署名あり SMB 高速化用の拡張サポート」ダイアログ上のオプションは変化します。

詳細モードを設定するには、以下の手順に従います。

1 「**システム セットアップ > WAN 高速化**」に移動します。

2 「**拡張サポート署名あり SMB**」を選択します。「**署名あり SMB 高速化用の拡張サポート**」ダイアログが表示されます。

3 「**詳細モード**」を選択します。オプションが次のように変化します。

4 「**詳細オプション**」を選択します。「**詳細オプション**」ダイアログが表示されます。

5 「**クライアント署名**」で、クライアントが使用する必要がある署名オプションを選択します。

- **自動** (既定)
- **必須**
- **無効**

6 「**サーバ署名**」で、サーバが使用する必要がある署名オプションを選択します。

- **自動** (既定)
- **必須**
- **無効**

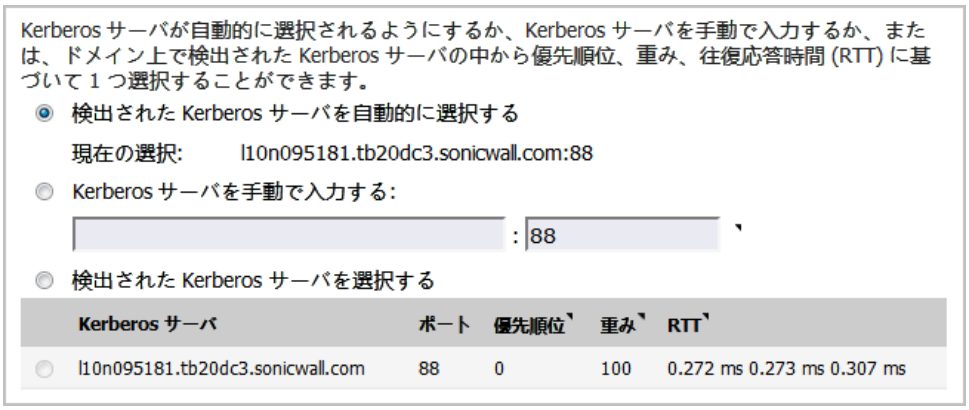
7 「**最大伝送量**」フィールドに、クライアントが送信できる最大データ量をバイト単位で入力します。既定値は **4096** です。

8 「**OK**」を選択します。

9 署名あり SMB 用の WFS 拡張サポート サービスを再起動するには、「**再起動**」を選択します。

10 キャッシュを消去するには、「**キャッシュの消去**」を選択します。

11 「**ドメイン詳細**」セクションで、「**ドメイン コントローラ**」の**編集**アイコンを選択して、Kerberos サーバを設定します。「**Kerberos サーバの設定**」ダイアログが表示されます。

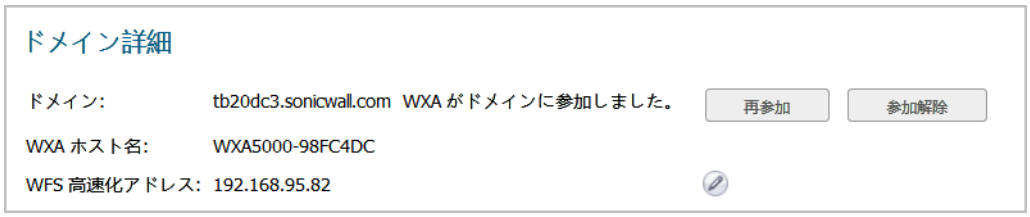


12 Kerberos サーバの選択方法を指定します。

- **検出された Kerberos サーバを自動的に選択する** - 現在の選択内容とそのポートが表示されます。
- **Kerberos サーバを手動で入力する** - 名前とポートのフィールドが使用可能になります。
  - ドメイン認証に使用する Kerberos サーバ名とポートを入力します。
- **検出された Kerberos サーバを選択する** -「**Kerberos サーバ**」テーブル内の検出されたエントリが使用可能になります。
  - そうしたエントリのいずれかを選択します。

13 「**OK**」を選択します。

ドメインの詳細



ドメイン	ドメインの名前と WXA がそのドメインに参加しているかどうか。
WXA ホスト名	WXA の名前
WFS 高速化アドレス	WFS 高速化モジュールの IP アドレス

トピック:

- ドメインへの再参加 (779 ページ)
- ドメインの参加解除 (779 ページ)
- ドメインへの参加 (780 ページ)
- ドメインの削除 (781 ページ)

ドメインへの再参加

ドメインに再参加するには、以下の手順に従います。

1 「**システム セットアップ > WAN 高速化**」に移動します。

2 「**拡張サポート署名あり SMB**」を選択します。「**署名あり SMB 高速化用の拡張サポート**」ダイアログが表示されます。

3 「**再参加**」をクリックします。

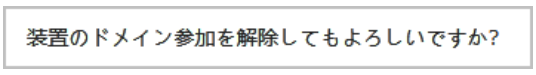
ドメインの参加解除

ドメインへの参加を解除するには、以下の手順に従います。

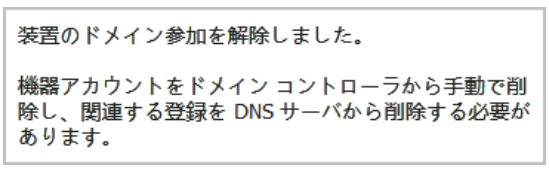
1 「**システム セットアップ > WAN 高速化**」に移動します。

2 「**拡張サポート署名あり SMB**」を選択します。「**署名あり SMB 高速化用の拡張サポート**」ダイアログが表示されます。

3 「**参加解除**」を選択します。確認メッセージが表示されます。



4 「**はい**」を選択します。確認メッセージが表示されます。



5 「**OK**」を選択します。「**再参加**」が**削除**アイコンになります。

6 機器アカウントをドメイン コントローラから手動で削除します。

7 関連するエントリをすべて DNS サーバから削除します。

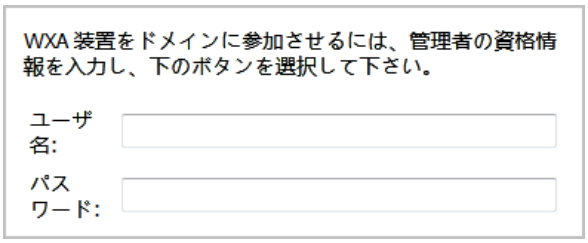
ドメインへの参加

ドメインに参加するには、以下の手順に従います。

1 「**システム セットアップ > WAN 高速化**」に移動します。

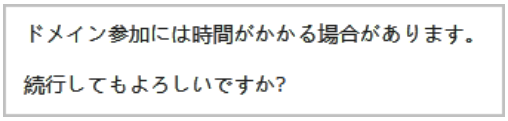
2 「**拡張サポート署名あり SMB**」を選択します。「**署名あり SMB 高速化用の拡張サポート**」ダイアログが表示されます。

3 「**参加**」を選択します。「**ドメインに参加**」ダイアログが表示されます。

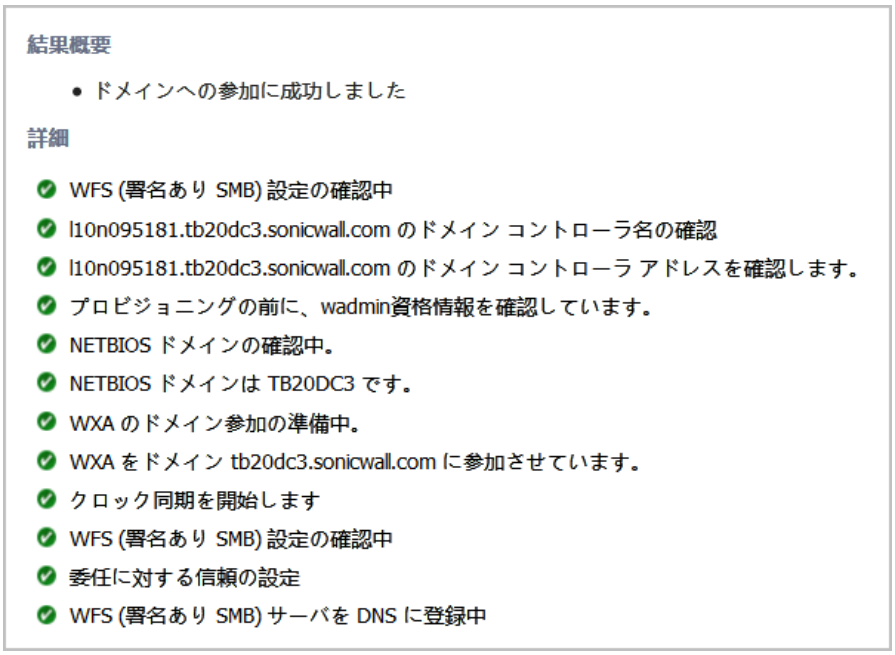


4 管理者のユーザ名とパスワードを「**ユーザ名**」と「**パスワード**」のフィールドにそれぞれ入力します。

5 **ドメインに参加**をクリックします。



6 「**はい**」を選択します。「**ドメイン参加結果**」ポップアップに、参加に成功したかどうか、またその処理の詳細が表示されます。



7 「**閉じる**」を選択します。

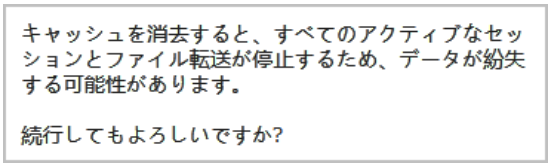
ドメインの削除

ドメインを削除するには:

1 「**システム セットアップ > WAN 高速化**」に移動します。

2 「**拡張サポート署名あり SMB**」を選択します。「**署名あり SMB 高速化用の拡張サポート**」ダイアログが表示されます。

3 「**削除**」アイコンを選択します。



4 「**はい**」を選択します。

ローカル/リモート サーバ テーブル

ファイル サーバ ファイル サーバの名前。

ローカル WXA 名 ローカル WXA サーバの名前。

共有

ドメイン登録 緑色のチェックマークは、ドメイン登録が現行のものであることを示し、X はその登録の更新が必要なことを示します。更新するには、「**ドメイン登録の更新**」を選択します。

設定 **削除**アイコンが表示されます。

トピック:

- サーバの削除 (781 ページ)
- ローカル ファイル サーバの追加 (782 ページ)

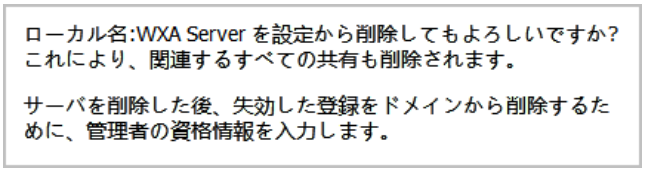
サーバの削除

サーバを削除するには、以下の手順に従います。

1 「**システム セットアップ > WAN 高速化**」に移動します。

2 「**拡張サポート署名あり SMB**」を選択します。「**署名あり SMB 高速化用の拡張サポート**」ダイアログが表示されます。

3 「**サーバ**」テーブルで、削除するサーバの**削除**アイコンを選択します。確認メッセージが表示されます。



4 「**削除**」を選択します。ダイアログが表示されます。

5 管理者のユーザ名とパスワードを「**ユーザ名**」と「**パスワード**」のフィールドにそれぞれ入力します。

6 「**OK**」を選択します。

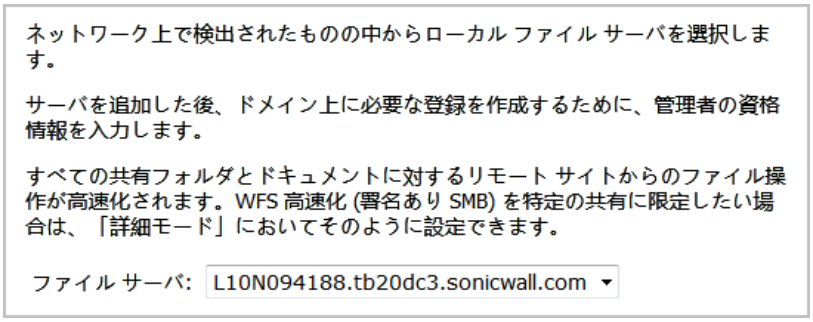
ローカル ファイル サーバの追加

ローカル ファイル サーバを追加するには、以下の手順に従います。

1 「**システム セットアップ > WAN 高速化**」に移動します。

2 「**拡張サポート署名あり SMB**」を選択します。「**署名あり SMB 高速化用の拡張サポート**」ダイアログが表示されます。

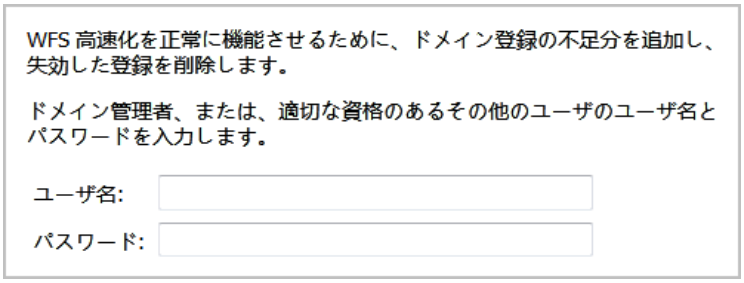
3 「**ローカル サーバ**」で、**追加**アイコンを選択します。「**ローカル ファイル サーバの追加**」ダイアログが表示されます。



4 「**ファイル サーバ**」でファイル サーバを選択します。

5 「**OK**」を選択します。

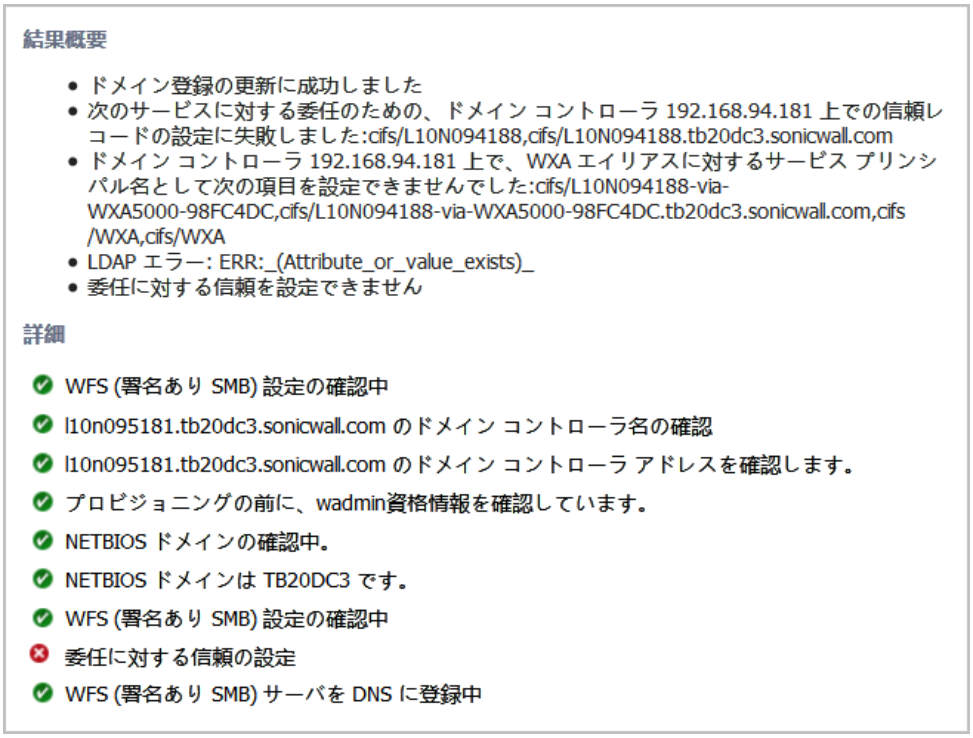
6 「**ドメイン登録の更新**」ダイアログが表示されます。



7 管理者のユーザ名とパスワードを「**ユーザ名**」と「**パスワード**」のフィールドにそれぞれ入力します。

8 「**登録の更新**」を選択します。

9 「**はい**」を選択します。「**ドメイン更新結果**」ポップアップに、参加に成功したかどうか、またその処理の詳細が表示されます。



10 「**閉じる**」を選択します。

リモート サーバの表示

「サーバ」テーブルにリモート サーバを表示するには、以下の手順に従います。

1 「**システム セットアップ > WAN 高速化**」に移動します。

2 「**拡張サポート署名あり SMB**」を選択します。「**署名あり SMB 高速化用の拡張サポート**」ダイアログが表示されます。

3 「**ドメイン詳細**」で、「リモート サーバ」を選択します。「**サーバ**」テーブルに、設定されているすべてのリモート サーバが表示されます。

リモート サーバの追加

リモート サーバを追加するには、以下の手順に従います。

1 「**システム セットアップ > WAN 高速化**」に移動します。

2 「**拡張サポート署名あり SMB**」を選択します。「**署名あり SMB 高速化用の拡張サポート**」ダイアログが表示されます。

3 「**リモート サーバ**」を選択します。「**リモート サーバ**」テーブルが表示されます。

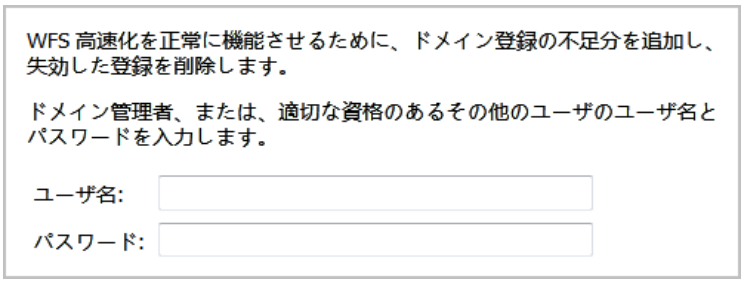
4 「**リモート サーバ**」で、**追加**アイコンを選択します。「**リモート ファイル サーバの追加**」ダイアログが表示されます。

5 「**ファイル サーバ**」でファイル サーバを選択します。

6 「**ローカル WXA 名**」フィールドに、WXA サーバの一意の名前またはエイリアスを入力します。

7 「**OK**」を選択します。

8 「**ドメイン登録の更新**」ダイアログが表示されます。



9 管理者のユーザ名とパスワードを「**ユーザ名**」と「**パスワード**」のフィールドにそれぞれ入力します。

10 「**登録の更新**」を選択します。

11 「**はい**」を選択します。「**ドメイン更新結果**」ポップアップに、参加に成功したかどうか、またその処理の詳細が表示されます。

署名あり SMB ツールの使用

トピック:

- DNS 名調査 (785 ページ)
- 利用可能な共有 (785 ページ)

DNS 名調査

DNS 名を検索するには、以下の手順に従います。

1 「**システム セットアップ > WAN 高速化**」に移動します。

2 「**拡張サポート署名あり SMB**」を選択します。「**署名あり SMB 高速化用の拡張サポート**」ダイアログが表示されます。

3 「**署名あり SMB ツール**」を選択します。

4 「**検索する名前または IP**」フィールドに検索するサーバの名前または IP アドレスを入力します。「**実行**」が使用可能になります。

5 「**実行**」を選択します。結果が表示されます。

利用可能な共有

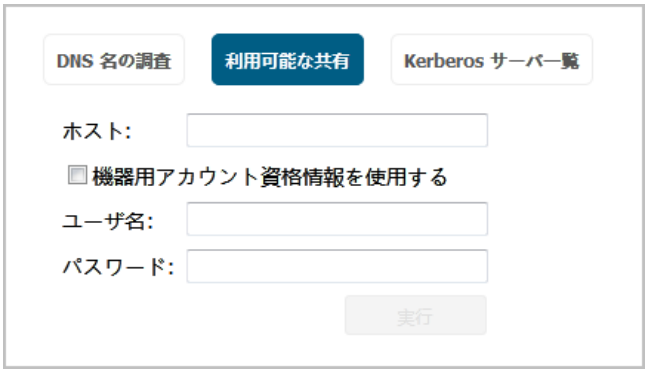
使用可能な共有を検索するには、以下の手順に従います。

1 「**システム セットアップ > WAN 高速化**」に移動します。

2 「**拡張サポート署名あり SMB**」を選択します。「**署名あり SMB 高速化用の拡張サポート**」ダイアログが表示されます。

3 「**署名あり SMB ツール**」を選択します。

4 「**利用可能な共有**」を選択します。



5 「**ホスト**」フィールドに、検索するサーバを入力します。

6 管理者のユーザ名とパスワードをそれぞれ「ユーザ名」と「パスワード」のフィールドに入力します。「**実行**」が使用可能になります。

7 「**実行**」を選択します。「利用可能な共有」ポップアップが表示されます。

8 「**OK**」を選択します。

Kerberos サーバー覧の表示

Kerberos サーバの一覧を表示するには、以下の手順に従います。

1 「**システム セットアップ > WAN 高速化**」に移動します。

2 「**拡張サポート署名あり SMB**」を選択します。「**署名あり SMB 高速化用の拡張サポート**」ダイアログが表示されます。

3 「**署名あり SMB ツール**」を選択します。

4 「**Kerberos サーバー覧**」を選択します。

5 サーバー覧の表示方法を選択します。

- 「**基本一覧**」- Kerberos サーバのポートと解決結果 IP のみが表示されます。
- 「**接続テストを含める**」 (既定) - サーバの優先順位、重み、RTT を含めます。

6 「**実行**」を選択します。結果が表示されます。

- **基本一覧**:

- **接続テストを含める**:

Kerberos サーバ	Kerberos サーバの名前。
ポート	Kerberos サーバのポート。
解決結果 IP	サーバの名前解決によって得られた IP アドレス。
優先順位	Kerberos サーバの優先順位。値が低い方が優先されます。
重み	同じ優先順位の Kerberos サーバの相対的な重み。値が高い方が優先されます。
RTT	Kerberos サーバをプローブする際の往復時間 (RTT) です。

VPN ポリシーでの WXA の設定

「VPN ポリシー」テーブルには、WXA 高速化が設定されたすべての VPN ポリシーが表示されます。

VPN ポリシーの WXA 高速化設定を編集するには、以下の手順に従います。

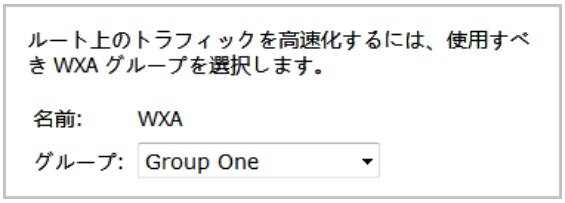
1 「**システム セットアップ > WAN 高速化**」に移動します。

2 「**VPN ポリシー**」を選択します。

3 ポリシーをフィルタするには、「**グループ**」テーブルから WXA グループを選択します。

4 「**表示**」で「**選択されたグループ**」を選択します。既定は「**すべて**」です。

5 ポリシーの**編集**アイコンを選択します。「**VPN の編集**」ダイアログが表示されます。



6 「**グループ**」で、VPN ポリシーに適用される WXA グループを選択します。

7 「**OK**」を選択します。

SSL VPN トラフィックの高速化の設定

WXAC クライアントからの NetExtender SSL VPN トラフィックの高速化は、有効または無効にすることができます。

メモ：NetExtender WAN 高速化クライアント (WXAC) をサポートするには、WXA がライセンスされている必要があります。

WXAC を有効にするには:

1 「**システム セットアップ > WAN 高速化**」に移動します。

2 「**SSL VPN**」を選択します。

3 WXAC を有効にするグループを「**グループ**」から選択します (既定の設定は「**なし**」です)。「**適用**」が使用可能になります。

4 「**適用**」を選択します。

5 現在使用中のアクティブなライセンスの数が「**グループ**」ドロップダウン メニューの下に表示されます。

WXA のルート ポリシーの表示と編集

送信元　VPN トラフィックの送信元となったゲートウェイ。

送信先　VPN トラフィックの送信先。

コメント　ルートの設定時に入力されたオプションのコメント。

グループ　ルートに適用されるグループ。

編集　**編集**アイコンが表示されています。

「ルート」テーブルに表示されるルートをフィルタするには、以下の手順に従います。

1 「**システム セットアップ > WAN 高速化**」に移動します。

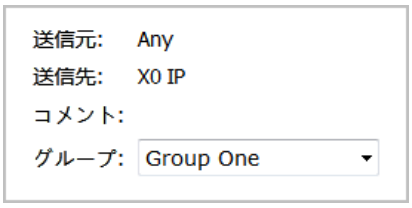
2 「**グループ**」テーブルの「**表示**」で、特定のグループのルートを選択します。既定は「**すべて**」です。

ルート ポリシーを編集するには、以下の手順に従います。

1 「**システム セットアップ > WAN 高速化**」に移動します。

2 「**グループ**」テーブルで、「**ルート ポリシー**」を選択します。

3 該当するルートの**編集**アイコンを選択します。「**ルートの編集**」ポップアップが表示されます。



4 「**グループ**」で、ルートの適用対象を選択します。

5 「**OK**」を選択します。

グループ接続の監視

WXA を通過する接続の総数は、折れ線グラフまたは (積み上げ) 棒グラフのどちらかで表示できます。特定のグループの合計接続数を表示することもできます。

接続数を表示するには、以下の手順に従います。

1 「**システム セットアップ > WAN 高速化**」に移動します。

2 「**グループ**」テーブルで、「**監視**」を選択します。

> ⓘ **ヒント：**「**グループ**」テーブルで適切なグループの「**監視**」を選択して、接続数を表示することもできます。

3 「**グループ**」で、接続を表示するグループを選択します。既定は「**すべて**」です。

4 「**グラフの種類**」で、データの表示方法を選択します。

- **ライン** (既定)
- **スタック** (棒グラフ)

5 グラフの選択領域の表示を拡大するには、該当する領域上でマウスをドラッグします。

6 グラフのズームを既定の状態に戻すには、「**拡大のリセット**」を選択します。

第 8 部

システム セットアップ | VOIP

- VoIP について
- SonicWall VoIP 機能の設定

50

VoIP について

トピック:

- VoIP について (792 ページ)
  - VoIP とは (792 ページ)
  - VoIP のセキュリティ (792 ページ)
  - VoIP プロトコル (794 ページ)
  - SonicWall の VoIP 機能 (795 ページ)

VoIP について

トピック:

- VoIP とは (792 ページ)
- VoIP のセキュリティ (792 ページ)
- VoIP プロトコル (794 ページ)
- SonicWall の VoIP 機能 (795 ページ)

VoIP とは

Voice over IP (VoIP) は、ボイス トラフィックをインターネット プロトコル (IP) ネットワーク経由で搬送できるようにする一連の技術を意味する、包括的な用語です。VoIP は、パケット交換電話網 (PSTN) で使用された従来のアナログ回線交換式のボイス通信とは対照的に、音声通話のボイス ストリームをデータ パケットに転送します。

ボイス テレフォニーとデータを 1 つの統合 IP ネットワーク システムに一体化する VoIP は、ネットワークと電気通信の収束を促す大きな原動力となっています。VoIP は、冗長なインフラストラクチャと通信回線による高価な使用料金を削減することで企業コストを切り詰めるとともに、拡張管理機能や通話サービス機能を提供します。

VoIP のセキュリティ

通信コストを削減しつつ、さまざまな場所の従業員に企業ボイス サービスを展開するために VoIP 技術を実装している企業は、ボイス/データ ネットワークの収束に関連したセキュリティ リスクに直面しています。VoIP セキュリティおよびネットワークの保全は、あらゆる VoIP 配備に欠くことのできない部分です。

今日のデータ ネットワークで問題化しているセキュリティ脅威は VoIP にも共通していますが、VoIP をネットワーク上のアプリケーションとして追加した場合、そうした脅威がさらに危険性を増します。ネットワークに VoIP コンポーネントを追加すると、新たなセキュリティ要件が加わってしまうことになります。

VoIP に包含されている複雑な規格のなかには、ソフトウェア実装のバグおよび脆弱性が放置されているものもあります。今日利用可能なあらゆるオペレーティング システムおよびアプリケーションに障害を及ぼしているものと同じ種類のバグおよび脆弱性が、VoIP 装置にも障害を及ぼします。今日の VoIP 通話サーバおよびゲートウェイ機器の多くが、脆弱な Windows/Linux オペレーティング システム上に構築されています。

VoIP のセキュリティ装置要件

VoIP は、標準の TCP/UDP ベースのアプリケーションよりも複雑です。VoIP シグナルおよびプロトコルが複雑であることや、セキュリティ装置で送信元アドレスおよび送信元ポート情報をネットワーク アドレス変換 (NAT) によって変換する際に不整合が生じることなどから、標準セキュリティ装置を VoIP が効率的に通過するのは困難になっています。そうした理由のいくつかを次に挙げます。

- **VoIP の動作には、2 つの異なるプロトコルが使用される** - クライアントと VoIP サーバ間にはシグナル プロトコルが使用され、クライアント間にはメディア プロトコルが使用されます。各セッションのメディア プロトコル (RTP/RTCP) で使用されるポート/IP アドレスのペアは、シグナル プロトコルによって動的にネゴシエートされます。ファイアウォールは、この情報を動的に追跡し保守し、セッションに対して選択されたポートを確実に開放して、適時に閉じる必要があります。
- **マルチ メディア ポートは、シグナル セッションによって動的にネゴシエートされる** - メディア ポートのネゴシエーションは、シグナル プロトコル (IP アドレスおよびポート情報) のペイロードに含まれています。ファイアウォールは、各パケットに対して精密パケット検査を実行し、情報を取得してセッションを動的に維持する必要があるため、別途セキュリティ装置処理を要求します。
- **送信元/送信先 IP アドレスは、VoIP のシグナル パケット内に埋め込まれている** - NAT をサポートしているセキュリティ装置では、パケットの IP アドレスおよびポートが IP ヘッダー レベルで変換されます。完全対称型 NAT セキュリティ装置では、NAT のバインドを頻繁に調整し、各セキュリティ装置で防御されているネットワークに着信パケットが入り込む可能性のあるピンホールを任意に閉じて、サービス プロバイダから顧客に送出される着信通話を遮断します。VoIP を効果的にサポートするには、セキュリティ装置をパケットが通過するたびに、NAT セキュリティ装置で精密パケット検査を実行して埋め込み IP アドレスおよびポート情報を変換する必要があります。
- **さまざまな VoIP システムで使用される各種メッセージ フォーマットから成るシグナル プロトコル スイートを、ファイアウォールで処理する必要がある** - ベンダー 2 社が同じプロトコル スイートを使用しているからといって、それらのプロトコル スイートに相互運用性があるとは限りません。

VoIP および NAT の複雑さに起因する多くの障害を克服するためにベンダー各社が提供しているのが、セッション ボーダー コントローラ (SBC) です。SBC はセキュリティ装置のインターネット側に配置され、VoIP メディア トラフィックおよびシグナル トラフィックをすべて終了してから再開することによって、VoIP ネットワーク境界を制御します。SBC は本質的に、VoIP 非対応のセキュリティ装置に対する VoIP トラフィック用プロキシとして機能します。SonicWall セキュリティ装置は VoIP 対応のセキュリティ装置であるため、ネットワーク上に SBC を配置する必要がありません。

メモ： VoIP は、SonicWall 6.2を稼働できるすべての SonicOS 装置でサポートされています。ただし、VoIP アプリケーションは RFC に準拠する必要があります。

VoIP プロトコル

VoIP は、次の 2 つのプライマリ プロトコルを基盤とする技術です。H.323 および SIP。これらのプロトコルは、グローバルまたはファイアウォール ルールごとに適用できます。

トピック:

- H.323 (794 ページ)
- SIP (794 ページ)

H.323

H.323 は、国際通信連合 (ITU) が策定した規格であり、コンピュータ、ターミナル、ネットワーク機器およびネットワーク サービス間のボイス/映像/データ通信用のプロトコルの包括的スイートです。コンピュータ、ターミナル、ネットワーク機器およびネットワーク サービス間のボイス/映像/データ通信用のプロトコルの包括的スイートです。H.323 は、コネクションレス パケット交換ネットワーク (プライベート IP ネットワークやインターネットなど) 経由でユーザがポイントツーポイント型マルチメディア電話を架電できるように設計されています。H.323 は、ビデオ カンファレンス機器、VoIP 機器、およびインターネット テレフォニー ソフトウェア/機器のメーカー各社によって広範にサポートされています。

H.323 では、シグナル送信の際は TCP と UDP を組み合わせて使用し、メッセージ エンコードの際は ASN.1 を使用します。1996 年に H.323v1 がリリースされ、2003 年に H.323v5 がリリースされました。古い規格である H.323 は、初期 VoIP 事業者の多くで採用されています。

H.323 ネットワークを構成するエンティティには、次の 4 種類があります。

- **ターミナル** - マルチメディア通信に対応したクライアント エンド ポイントです。例えば、H.323 対応のインターネット電話や PC などがあります。
- **ゲートキーパー** - 通信用 H.323 ターミナルを登録し、通話セットアップ/切断用のサービスを実行します。次の機能があります。
  - アドレス変換
  - 登録、受付制御、および状況 (RAS)
  - インターネット ロケータ サービス (ILS) も、この種別に分類されます (ただし、H.323 の一部ではありません)。ILS で使用されるのは、H.323 メッセージではなく、ライトウェイト ディレクトリ アクセス プロトコル (LDAP) です。
- **多地点制御装置 (MCU)** - 各ターミナル間の多地点通信向けのカンファレンス制御およびデータ配信を行う装置です。
- **ゲートウェイ** - H.323 ネットワークと、回線交換式のパケット交換電話網 (PSTN) をはじめとする情報提供サービスとの間の相互運用。

SIP

セッション開始プロトコル (SIP) 規格は、インターネット エンジニアリング タスク フォース (IETF) によって策定されました。1999 年 3 月に RFC2543 がリリースされ、2002 年 6 月に RFC3261がリリースされました。SIP は、セッション開始、管理および停止のためのシグナル プロトコルです。SIP は“プレゼンス"とモビリティをサポートしているため、ユーザ データグラム プロトコル (UDP) と転送制御プロトコル (TCP) を利用して実行することができます。

VoIP クライアントは SIP を使用することによって、通話セッションを開始/停止し、カンファレンス セッションにメンバーを招待するなどの、テレフォニー タスクを実行することができます。また、SIP を導入すると、構内交換機 (PBX) や VoIP ゲートウェイなどの通信機器が連携して通信できるようになります。また、SIP は H.323 の重いオーバヘッドを回避する設計になっています。

SIP ネットワークを構成する論理エンティティには、次のものがあります。

- **ユーザ エージェント (UA)** - 通話を開始し、受け付け、停止します。
- **プロキシ サーバ** - UA に代わって要求の転送、または要求への応答を行います。プロキシ サーバで、複数のサーバに要求を割り振ることができます。Back-to-Back ユーザ エージェント (B2BUA) は一種のプロキシ サーバであり、その B2BUA を通行する通話の各行程を、2 つの別個の SIP 通話セッションとして扱います。1 つはその B2BUA と発呼側電話間のセッション、もう 1 つはその B2BUA と着呼側電話との間のセッションです。 その他のプロキシ サーバでは、同じ通話の全行程を 1 つの SIP 通話セッションとして扱います。
- **リダイレクト サーバ** - 要求に応答します。 ただし、要求の転送は行いません。
- **登録サーバ** - UA の認証および登録を扱います。

SonicWall の VoIP 機能

重要：「**無線 LAN 制御**」で「**無線制御専用**」モードが選択されている場合、VOIP は無効になります。

トピック:

- VoIP のセキュリティ (795 ページ)
- VoIP ネットワーク (796 ページ)
- VoIP ネットワークの相互運用性 (797 ページ)
- サポートされているインターフェース (798 ページ)
- サポートされている VoIP プロトコル (798 ページ)
- BWM と QoS (800 ページ)
- SonicOS での VoIP 通話処理方法 (800 ページ)

VoIP のセキュリティ

- **トラフィックの正当性** - セキュリティ装置を通過する VoIP シグナルおよびメディア パケットすべてに対してステートフル検査を実行することによって、すべてのトラフィックの正当性が保証されます。実装上の不備を突いたパケットにより、対象機器にバッファ オーバフローなどを引き起こすことができるため、よく攻撃手段として使用されます。SonicWall セキュリティ機器は、不正な形式のパケットおよび無効なパケットが目的の宛先に達する前に未然に検出して破棄します。
- **アプリケーション層での VoIP プロトコルの保護** - SonicWall 侵入防御サービス (IPS) は、アプリケーションレベルの VoIP の悪用から完全に防御します。構成可能な高性能スキャン エンジンを、攻撃および脆弱性に関するシグネチャ データベース (動的な更新/配布が可能) と統合したIPS は、巧妙なトロイの木馬や多相型の脅威に対してネットワークを保護します。SonicWallは、保護 VoIP 電話およびサーバに不当なトラフィックが到達するのを防ぐように設計された VoIP固有のシグネチャ群を取り入れて、IPS シグネチャ データベースを拡張しています。

- **DoS および DDoS シグネチャの防御** - ネットワークやサービスの無効化をねらった DoS 攻撃および DDoS 攻撃 (例えば、SYN フラッド、Ping of Death、LAND (IP) 攻撃など) を防ぎます。
    - TCP を使用して VoIP シグナル パケットのパケット シーケンスを検証し、シーケンスの不正なパケットや時間枠を超えて再転送されたパケットを否認します。
    - 無作為化された TCP シーケンス番号 (接続セットアップ時に暗号乱数ジェネレータによって生成された番号) を使って各 TCP セッション内のデータ フローを検証して、リプレイ攻撃およびデータ挿入攻撃を防ぎます。
    - SYN フラッド防御により、攻撃者が (通常は送信元アドレスのなりすましのために完全には確立されることのない) TCP/IP 接続を多数開いてサーバを制圧できないようにします。
- **ステートフル監視** - ステートフル監視は、パケットが (そのパケット自体の形式が有効な場合でも) 関連する VoIP 接続の現状態に適合することを保証します。
- **暗号化 VoIP 機器のサポート** - SonicWall では、暗号化を利用できる VoIP 機器がサポートされているため、VoIP 対話におけるメディア交換を保護することができます。 また、暗号化メディアをサポートしていない VoIP 機器を IPsec VPN でセキュリティ保護することによって、VoIP 通話を保護することもできます。
- **アプリケーション層の保護** - SonicWall では、SonicWall 侵入防御サービス (IPS) によってアプリケーションレベルの VoIP 悪用から完全に防御できます。SonicWall IPS は、構成可能で高性能な精密パケットパケット検査エンジンに基づいて構築されており、VoIP、Windows のサービス、DNS などの主要ネットワーク サービスに対する拡張保護を実現します。また、SonicWall の精密パケット検査エンジンで使用されている広範なシグネチャ言語により、アプリケーションおよびプロトコルで新たに見つかった脆弱性に対する事前対処的な防御を実現します。SonicWall IPS の詳細なシグネチャ情報によって攻撃をグローバル、攻撃グループ別、またはシグネチャごとに検出して防止することで、柔軟性を絶大源に高めるとともに、偽陽性による誤検出を抑制できます。

VoIP ネットワーク

- **無線 LAN (WLAN) を介した VoIP** - SonicWall は、分散型無線ソリューションを備えた完全な VoIP セキュリティを接続先無線ネットワークに展開します。SonicWall 背後の有線ネットワークに接続された VoIP 機器に提供されているセキュリティ機能はすべて、無線ネットワークを使用する VoIP 機器にも提供されます。

    メモ：SonicWall のセキュア ワイヤレス ソリューションには、セキュリティ保護された VoIP 通信を無線ネットワーク経由で展開するための、ネットワーク イネーブラが含まれています。詳細については、SonicWall のウェブ サイト http://www.SonicWall.com で提供されている『*SonicWall Secure Wireless Network Integrated Solutions Guide*』を参照してください。

- **帯域幅管理 (BWM) とサービス品質 (QoS)** - 帯域幅管理 (送受信の両方) を使用することによって、時間検知型 VoIP トラフィック用の帯域幅を確保し続けることができます。BWM は、SonicWall サービス品質 (QoS) 機能に統合されています。 これにより、特定タイプのアプリケーションで重要となる予測可能性が得られます。
- **WAN の冗長性と負荷分散** - WAN では冗長性と負荷分散によって、インターフェースがセカンダリ WAN ポートとして機能できます。その場合、プライマリ WAN ポートが機能停止または利用不可能になったときに限り、トラフィックがバックアップ WAN ポートを介して転送されます。トラフィックのルーティングを送信先に基づいて分割することによって、負荷分散の実行が可能になります。
- **高可用性** - SonicOS 高可用性により、システム障害が発生した場合に信頼できる継続的な接続を確実に確保することで、高可用性を実現しています。

VoIP ネットワークの相互運用性

- **VoIP 機器に対するプラグ アンド プロテクトのサポート** - SonicOS では、VoIP 機器の追加、変更および取り外しが自動処理されるため、VoIP 機器が無防御な状態のまま放置されるのを確実に回避できます。先進的な監視および追跡技術の採用によって、セキュリティ装置の背後にあるネットワークに VoIP 機器を接続すると直ちに VoIP 機器が自動保護されます。
- **すべての VoIP シグナル パケットに対する完全な構文検証** - 受信されたシグナル パケットは、SonicOS の内部で完全に解析されるため、関連する規格において定義された構文に準拠することが保証されています。セキュリティ装置での構文検証により、不正な形式のパケットがファイアウォールをすり抜けたり、目的の宛先に悪影響を及ぼしたりすることを確実に防止できます。
- **メディア ストリームの動的セットアップ/追跡記録のサポート** - SonicOS では、通話セットアップを最初に要求したシグナル パケットから通話の終了ポイントまでの各 VoIP 通話が記録されます。発呼側と着呼側の間に追加ポート (追加のシグナルおよびメディア交換用) が開くのは、通話状況が“成功"の場合のみです。

  通話セットアップの際にネゴシエートされたメディア ポートは、セキュリティ装置によって動的に割り当てられます。以降の通話では、同じ通話相手との通話にも別のポートが使用されるため、特定のポートが攻撃者に監視されるのを回避できます。必要なメディア ポートは、通話が完全に接続されたときにのみ開き、通話が終了するとシャットダウンされます。通話外でポートを使おうとしたトラフィックを切り離すことによって、セキュリティ装置の背後にある VoIP 機器に対する保護を強化しています。
- **すべてのメディア パケットのヘッダーの検証** - SonicOS ではメディア パケット内のヘッダーを調べて監視し、シーケンスの不正なパケットや (時間枠を超えて) 再転送されたパケットを検出して破棄できます。また、有効なヘッダーが付いているかどうかを確認することにより、無効なメディア パケットを検出して破棄します。SonicWall では、メディア ストリームとシグナルを追跡することで、VoIP セッション全体の保護を実現しています。
- **シグナルおよびメディア用に構成可能な、無動作時のタイムアウト** - 切断された VoIP 接続が無期限に開いたまま放置されることのないよう、SonicOS では VoIP セッションに関連付けられているシグナルおよびメディア ストリームの使用状況が監視されます。アイドル状態のストリームは、設定済みタイムアウトの経過後にシャットダウンされます。 これにより、潜在的セキュリティ ホールを防ぐことができます。
- **SonicOS における管理者の着信通話制御権限** - SonicOS では、H.323 ゲートキーパーまたはSIP プロキシですべての着信通話を許可し認証することを要求することで、未許可通話およびスパム通話を遮断できます。これにより、管理者は VoIP ネットワークの使用を企業で認可された通話のみに限定できます。
- **包括的監視とレポーティング** - SonicOS では、サポートされているすべての VoIP プロトコル用の拡張監視/トラブルシューティング ツールとして、次のものが提供されています。
  - アクティブな VoIP 通話の、発呼側、着呼側、および使用帯域幅を示す動的ライブ レポーティング
  - すべての VoIP 通話の、発呼側、着呼側、通話持続時間、および帯域幅合計使用量を示したオーディット ログ: 確認された異常パケット (不正な応答など) のログ採取と、関与した通話相手および確認された条件に関する詳細
  - VoIP シグナルおよびメディア ストリームに関する、詳細な Syslog レポートと ViewPoint レポート: SonicWall ViewPoint は、ウェブベースのグラフィカル レポーティング ツールです。SonicWall ViewPoint は、ウェブベースのグラフィカル レポーティング ツールであり、セキュリティ装置から受信する Syslog データ ストリームに基づいて、セキュリティとネットワークのアクティビティに関する詳細レポートおよび包括的レポートを出力できます。セキュリティ装置アクティビティのほぼ全般 (特定のセキュリティ装置またはセキュリティ

装置グループ上での個別ユーザまたはグループの使用パターンとイベント、攻撃の種類と時刻、リソース消費量と制約など) に関するレポートを生成できます。

サポートされているインターフェース

VoIP 機器は、次の SonicOS ゾーンでサポートされます。

- 保護ゾーン (LAN、VPN)
- 非保護ゾーン (WAN)
- パブリック ゾーン (DMZ)
- 無線ゾーン (WAN)

サポートされている VoIP プロトコル

トピック:

- H.323 (798 ページ)
- SIP (798 ページ)
- SonicWall VoIP ベンダー間の相互運用性 (799 ページ)
- CODEC (799 ページ)
- SonicOS での精密パケット検査が実行されない VoIP プロトコル (800 ページ)

H.323

H.323 に関しては、次のサポートが SonicOS により提供されます。

- H.323 のすべてのバージョン (現行では 1～5) を実行する VoIP 機器のサポート
- Microsoft の LDAP ベースのインターネット ロケータ サービス (ILS)
- LAN H.323 ターミナルでマルチキャストを使用してゲートキーパーを検出できる
- ゲートキーパーの登録、受付制御、および状況 (RAS) メッセージのステートフル監視/処理
- メディア ストリームに暗号化を使用する H.323 ターミナルに対するサポート
- DHCP のオプション 150: DHCP サーバは、VoIP 固有の TFTP サーバのアドレスを DHCP クライアントに返すように設定できます。
- SonicOS がサポートしている VoIP 機器のなかには、H.323 サポート以外に、次に挙げる ITU 規格を採用しているものもあります。
  - T.120: アプリケーション共有、電子ホワイトボード、ファイル交換、およびチャットに関する規格
  - H.239:音声、映像、およびデータ配信用に複数チャンネルの使用を許可する規格
  - H.281:遠端カメラ制御 (FECC) に関する規格

SIP

SIP に関しては、次のサポートが SonicOS により提供されます。

- ベース SIP 規格 (RFC 2543 および RFC 3261)

- SIP INFO メソッド (RFC 2976)
- SIP の暫定応答の信頼性 (RFC 3262)
- SIP 固有のイベント通知 (RFC 3265)
- SIP UPDATE メソッド (RFC 3311)
- SIP サーバ用の DHCP オプション (RFC 3361)
- インスタント メッセージングの SIP 拡張 (RFC 3428)
- SIP REFER メソッド (RFC 3515)
- 対称応答ルーティングのための SIP 拡張 (RFC 3581)

SonicWall VoIP ベンダー間の相互運用性

「SonicWall VoIP と相互運用性のある機器の部分的なリスト」テーブルに、SonicWall VoIP との相互運用性がある多数の主要メーカー製機器のリストを示します。

SonicWall VoIP と相互運用性のある機器の部分的なリスト

H.323	SIP
ソフトフォン: Avaya Microsoft ネットミーティング OpenPhone PolyCom SJLabs SJ フォン 電話/ビデオ電話: Avaya Cisco D-Link PolyCom ソニー ゲートキーパー: Cisco OpenH323 ゲートキーパー ゲートウェイ: Cisco	ソフトフォン: Apple iChat Avaya Microsoft MSN メッセンジャー Nortel マルチメディア PC クライアント PingTel Instant Xpressa PolyCom Siemens SCS Client SJLabs SJPhone XTen X-Lite Ubiquity SIP ユーザ エージェント 電話/アナログ電話アダプタ (ATA): Avaya Cisco Grandstream BudgetOne Mitel Packet8 ATA PingTel Xpressa PolyCom PolyCom Pulver Innovations WiSIP SoundPoint SIP プロキシ/サービス: Cisco SIP プロキシ サーバ Brekeke Software OnDo SIP プロキシ Packet8 Siemens SCS SIP プロキシ Vonage

CODEC

- **SonicOS は、あらゆる種類の CODEC のメディア ストリームもサポートする** - VoIP 機器内のハードウェア/ソフトウェア CODEC (コーダ/デコーダ) で処理された音声信号および映像信号は、メディア ストリームによって搬送されます。CODEC は、コーディング技術および圧縮技術を使用して、音声/映像信号の表現に必要なデータの量を低減します。次に、CODEC の例をいくつか挙げます。

- H.264、H.263 および H.261:映像用
- MPEG4、G.711、G.722、G.723、G.728、G.729:音声用

SonicOS での精密パケット検査が実行されない VoIP プロトコル

現行バージョンの SonicWall ネットワーク セキュリティ装置は、次のプロトコルに対しては精密パケット検査をサポートしていません。したがって、次のプロトコルは非 NAT 環境でのみ使用する必要があります。

- H.323 または SIP に対するベンダー独自の拡張
- MGCP
- Megaco/H.248
- Cisco スキニー クライアント コントロール プロトコル (SCCP)
- IP-QSIG
- 独自仕様プロトコル (Mitel MiNET、3Com NBX など)

BWM と QoS

VoIP の最大の課題の 1 つは、IP ネットワーク上で高度な通話品質を保証することです。IP は遅延を許容する非同期データ トラフィックを主な処理対象として設計されていますが、VoIP は遅延とパケット損失に非常に敏感です。高品質なリアルタイム VoIP 通信を保証するには、アクセスの管理およびトラフィックの優先順位設定が重要な要件となります。

SonicWall の統合帯域幅管理 (BWM) およびサービス品質 (QoS) 機能には、VoIP 通信の信頼性および品質を管理するためのツール群が提供されています。

サービス品質

QoS に包括されているメソッドには、予測可能なネットワーク動作およびパフォーマンスの実現を意図したものが多数あります。ネットワーク予測可能性は、VoIP と他のミッション クリティカル アプリケーションにとって不可欠です。この種類の予測可能性は、帯域幅量の調整では実現されません。なぜなら、ネットワークにおいては帯域幅をどんなに増やしても任意の時点でその容量まで使い果たされる結果になるためです。QoS を正しく設定し実装することによってのみ、トラフィックを適切に管理し、望ましいレベルのネットワーク サービスを保証することが可能になります。

SonicOS には、業界標準の 802.1p および DiffServe コード ポイント (DSCP) クラス オブ サービス (CoS) 指示子の識別、マップ、変更および生成を可能にする QoS 機能が組み込まれています。

SonicOS での VoIP 通話処理方法

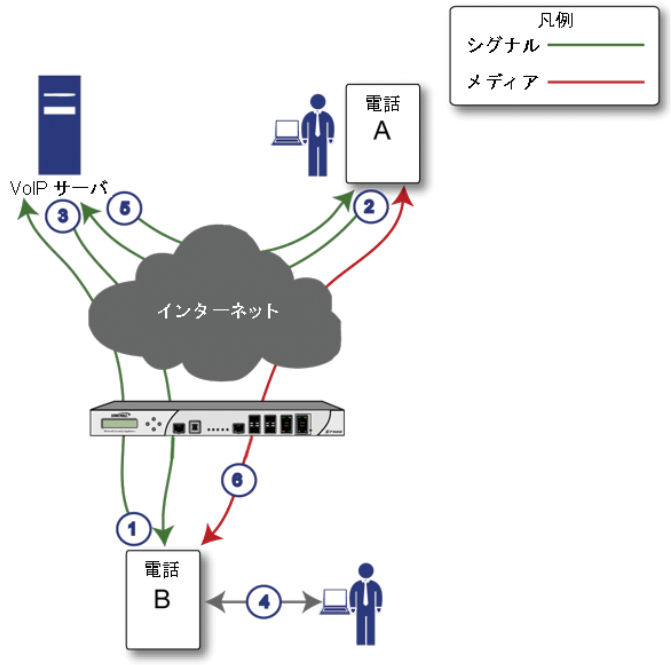
SonicOS では、あらゆる VoIP 通話シナリオに対応した、効率的かつセキュアなソリューションを提供しています。SonicOS における VoIP 通話フロー処理の仕組みを、次の例に示します。

- 着信通話 (800 ページ)
- ローカル通話 (802 ページ)

着信通話

着信通話中に発生するイベントのシーケンスを、「着信通話のイベント シーケンス」に示します。

着信通話のイベント シーケンス



「着信通話のイベント シーケンス」で示したイベントのシーケンスについて説明します。

1 **電話 B を VoIP サーバに登録する** - セキュリティ装置は、送信 VoIP 登録要求を監視して、背後にあるアクセス可能 IP 電話のデータベースを構築します。SonicOS は、電話 B のプライベート IP アドレスと、登録メッセージで使用されるセキュリティ装置のパブリック IP アドレスとの間で変換を実行します。VoIP サーバは、電話 B がセキュリティ装置の背後にあることも、電話 B にプライベート IP アドレスが割り当てられていることも認識しません。電話 B はセキュリティ装置のパブリック IP アドレスに関連付けられます。

2 **電話 A が電話 B への通話を開始する** - 電話 A は電話番号または別名を使用して、電話 B への通話を開始します。電話 A はこの情報を VoIP サーバに送信するときに、サポート可能なメディア種別とフォーマット、および対応する IP アドレスとポートに関する詳細も提供します。

3 **VoIP サーバが通話要求を検証して、その要求を電話 B に送信する** - VoIP サーバがセキュリティ装置のパブリック IP アドレス宛てに通話要求を送信します。その通話要求がセキュリティ装置に到着すると、SonicOS は要求の送信元およびコンテンツを検証します。その後、セキュリティ装置で電話 B のプライベート IP アドレスを判別します。

4 **電話 B が鳴り、応答される** - 電話 B はその接続が応答した後で、サポート可能なメディア種別とフォーマット、および対応する IP アドレスとポートに関する情報を VoIP サーバに返します。SonicOS は、このプライベート IP 情報を変換して、セキュリティ装置のパブリック IP アドレスを VoIP サーバ宛てメッセージに使用します。

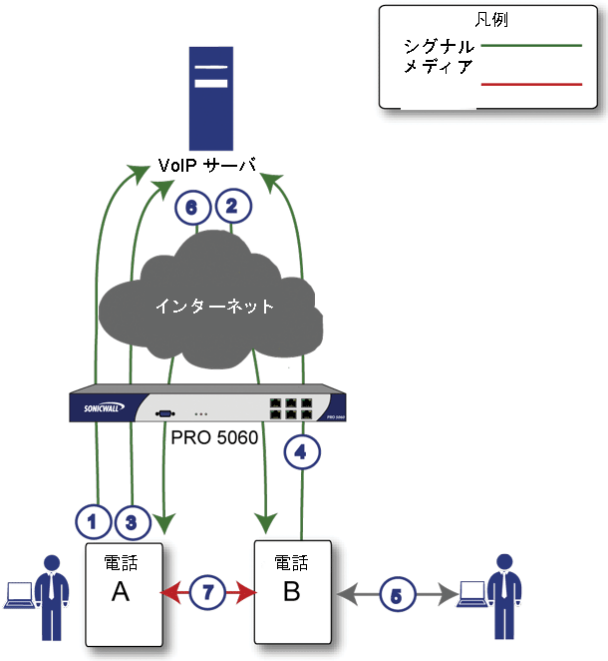
5 **VoIP サーバが電話 B のメディア IP 情報を電話 A に返す** - この時点で、電話 A は電話 B とメディア交換を開始するための十分な情報を確保しています。VoIP サーバによってセキュリティ装置のパブリック アドレスが電話 B に割り当てられましたが、電話 B がセキュリティ装置の背後にあることは電話 A に認識されません。

6 **電話 A と電話 B が VoIP サーバ経由で音声/映像/データを交換する** - SonicOS は内部データベースを使用して、メディアの発信元を電話 A だけに限定し、電話 B が許可した特定のメディア ストリームだけが使われるようにします。

ローカル通話

ローカル VoIP 通話中に発生するイベントのシーケンスを、「ローカル VoIP 通話のイベント シーケンス」 に示します。

ローカル VoIP 通話のイベント シーケンス



「ローカル VoIP 通話のイベント シーケンス」で示したイベントのシーケンスについて説明します。

1 **電話 A と電話 B を VoIP サーバに登録する** - セキュリティ装置は、送信 VoIP 登録要求を監視して、背後にあるアクセス可能 IP 電話のデータベースを構築します。SonicOS により、各電話のプライベート IP アドレスと、セキュリティ装置のパブリック IP アドレスの間で変換が実行されます。VoIP サーバは、各電話がセキュリティ装置の背後にあることを認識しません。VoIP サーバは、両方の電話に同じ IP アドレスと別々のポート番号を関連付けます。

2 **電話 A は要求を VoIP サーバに送信して、電話 B への通話を開始する** - 両方の電話は同じセキュリティ装置の背後にありますが、電話 B の IP アドレスは電話 A に認識されません。電話 Aは、電話番号または別名を使用して、電話 B への通話を開始します。

3 **VoIP サーバが通話要求を検証して、その要求を電話 B に送信する** - VoIP サーバがセキュリティ装置のパブリック IP アドレス宛てに通話要求を送信します。その後、セキュリティ装置で電話 B のプライベート IP アドレスを判別します。

4 **電話 B が鳴り、応答される** - 電話 B が応答すると、セキュリティ装置はプライベート IP 情報を変換して、セキュリティ装置のパブリック IP アドレスを VoIP サーバ宛てメッセージに使用します。

5 **VoIP サーバが電話 B のメディア IP 情報を電話 A に返す** - SonicOS により、メッセージ内の発呼側/着呼側の両方の情報が、電話 A および電話 B のプライベート IP アドレスおよびポート宛てとなるように再度変換されます。

6 **電話 A と電話 B が音声/映像/データを直接に交換する** - セキュリティ装置は、2 つの電話間のトラフィックを LAN 経由で直接転送します。2 つの電話を直接つなげることによって、VoIP サーバへのデータ転送に必要とされる帯域幅要件を減らし、セキュリティ装置でアドレス変換を実行する必要性をなくします。

51

SonicWall VoIP 機能の設定

トピック:

- 設定タスク (803 ページ)
  - VoIP の設定 (803 ページ)
  - VoIP ログ採取の設定 (810 ページ)

設定タスク

SonicWall セキュリティ装置を VoIP 配置用に設定した場合、SonicWall 管理インターフェース内の基本ネットワーク設定がその基盤となります。このセクションは、ご利用のネットワーク環境に合わせてセキュリティ装置が設定されていることを前提としています。

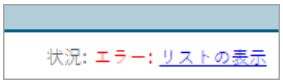
メモ：VoIP の概要については、「VoIP について (792 ページ)」を参照してください。

トピック:

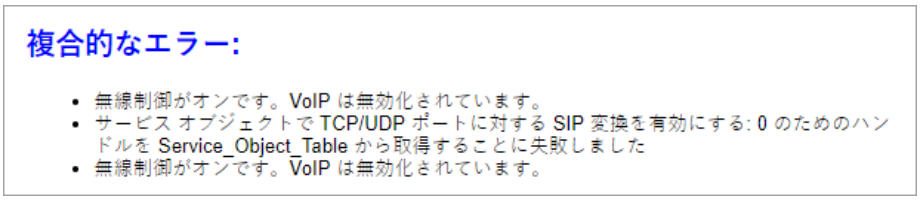
- VoIP の設定 (803 ページ)
- VoIP ログ採取の設定 (810 ページ)

VoIP の設定

重要：「**無線 LAN 制御**」で「**無線制御専用**」モードが選択されている場合、SIP または H.323 オプションを有効にしようとすると、ブラウザ ウィンドウの右下隅にエラー メッセージが表示されます。



「リストの表示」リンクをクリックすると、エラー ログが表示されます。



VoIP 通過設定は、「**管理 | システム セットアップ > VOIP**」で設定します。このページは次の 3 つのセクションに分かれています。

- **一般設定**

- SIP の設定
- H.323 の設定

トピック:

- 一般設定 (804 ページ)
- SIP の設定 (806 ページ)
- H.323 の設定 (808 ページ)

一般設定

「**一般設定**」の下に「**継続性 NAT を有効にする**」というオプションがあります。

継続性 NAT では、標準 NAT ポリシーが強化され、接続するために VoIP のような継続性 IP アドレスを要求するピアツーピア アプリケーションとの高い互換性が提供されます。継続性 NAT は、MD5 ハッシュ方式を使用して、割り当て済みの同じパブリック IP アドレスと UDP ポートのペアを、それぞれの内部プライベート IP アドレスとポートのペアに持続的に割り当てます。

例えば、NAT では、プライベート (LAN) IP アドレスとポートのペア 192.116.168.10/50650 および 192.116.168.20/50655 は、「IP アドレスとポートのペア」テーブルのようにパブリック (WAN) IP とポートのペアに変換されます。

IP アドレスとポートのペア

プライベート IP/ポート	変換後のパブリック IP/ポート
192.116.168.10/50650	64.41.140.167/40004
192.116.168.20/50655	64.41.140.167/40745

継続性 NAT を有効にすると、それ以降にホスト 192.116.168.10 または 192.116.168.20 から「IP アドレスとポートのペア」テーブルの同じポートを使用して送信されるすべての要求は、変換先の同じアドレスとポートのペアを使用します。継続性 NAT を使用しないと、要求ごとにポートや IP アドレスが変わる可能性があります。

メモ：継続性 NAT を有効にすると、アドレスとポートのペアの予測可能性が高くなるので、全体的なセキュリティはやや低下します。大多数の UDP ベース アプリケーションは従来の NAT に対応しています。したがって、継続性 NAT を必要とするアプリケーションをネットワークで使用する場合を除き、継続性 NAT は有効にしないでください。

重要：「継続性 NAT」が正しく機能するためには、コール間の最小時間間隔を少なくとも 200 ミリ秒とする必要があります。

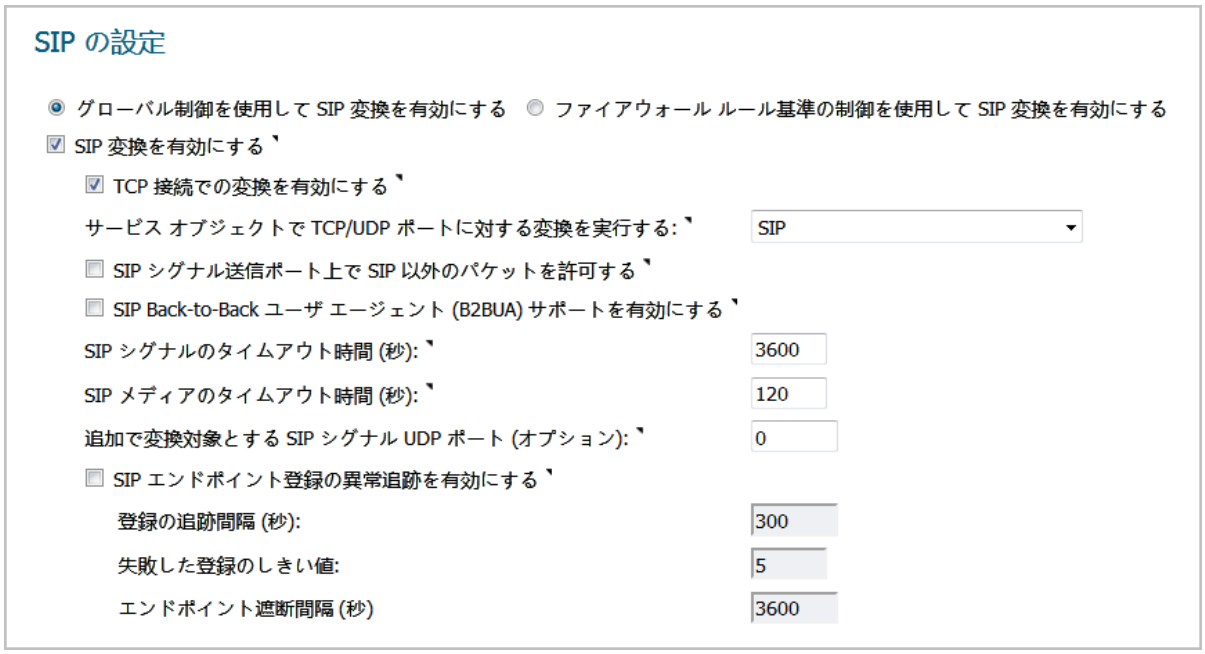
継続性 NAT の有効化

継続性 NAT を有効にするには、以下の手順に従います。

1 「**継続性 NAT を有効にする**」オプションを選択します。このオプションは、既定では選択されていません。

2 「**適用**」を選択します。

SIP の設定



既定では、SIP クライアントは自身のプライベート IP アドレスを、SIP プロキシ宛てに送信される SIP (セッション開始プロトコル) セッション定義プロトコル (SDP) メッセージに使用します。SIP プロキシがファイアウォールのパブリック (WAN) 側に配置されていて、SIP クライアントがファイアウォールのプライベート (LAN) 側に配置されている場合、SDP メッセージは変換されないため、SIP プロキシは SIP クライアントに到達できません。

SIP の有効化

SIP を有効にするには、以下の手順に従います。

1 「**管理 | システム セットアップ > VOIP**」に移動します。

2 「**SIP の設定**」セクションで、SIP 変換をグローバルに有効にするか、ファイアウォール ルールごとに有効にするかを選択します。

- 「**グローバル制御を使用して SIP 変換を有効にする**」。このオプションは、既定では選択されています。
- 「**ファイアウォール ルール基準の制御を使用して SIP 変換を有効にする**」。『*SonicOS ポリシー*』の説明に従って、SIP 変換を制御するファイアウォール ルールを設定してください。

3 SIP 変換を設定しない場合は、「ステップ 12」に進みます。

4 「**SIP 変換を有効にする**」は既定ではオンになっていません。このオプションをオンにすると、次の効果がもたらされます。

- LAN (保護) と WAN/DMZ (非保護) の間で SIP メッセージの変換が行われます。

  セキュリティ装置で SIP 変換を実行したい場合、「SIP 変換を有効にする」設定のチェックボックスをオンにする必要があります。SIP プロキシがセキュリティ装置のパブリック (WAN) 側にあって SIP クライアントが LAN 側にある場合、既定では SIP クライアントは自身のプライベート IP アドレスを、SIP プロキシ宛てに送信される SIP/セッション定義

プロトコル (SDP) メッセージの中に埋め込み/使用します。つまり、これらの SIP メッセージおよび SDP メッセージは未変更のままになるため、セキュリティ装置背後のクライアントにメッセージを返信する方法を SIP プロキシは認識できません。

- セキュリティ装置が各 SIP メッセージを検査してプライベート IP アドレスおよび割り当て済みポートを変更できるようになります。
- SIP セッション コールを実行するために開く必要のある RTP (リアルタイム転送プロトコル) ポートや RTCP (RTP 制御プロトコル) ポートを制御して開くことができます。

NAT で第 3 層のアドレスは変換されますが、第 7 層の SIP/SDP アドレスは変換されません。このため、SIP メッセージを変換するには「**SIP 変換を有効にする**」を選択する必要があります。

ヒント：一般的には「**SIP 変換を有効にする**」をオンにする必要があります (ただし、この機能を無効にする必要のある NAT トラバーサル ソリューションが他に存在している場合を除きます)。SIP 変換は双方向モードで機能します。 つまり、LAN から WAN に送出されたメッセージに対しても、その逆に WAN から LAN に送出されたメッセージに対しても変換が実行されます。

「**SIP 変換を有効にする**」チェックボックスをオンにすると、他のすべてのオプションが使用できるようになります。

5 TCP ベースの SIP セッションで SIP 変換を実行するには、「**TCP 接続での SIP 変換を有効にする**」を選択します。このオプションは、既定では選択されています。

6 「**サービス オブジェクトで TCP/UDP ポートに対する変換を実行する**」で、サービス オブジェクトを選択します。既定値は「**SIP**」です。

7 「**SIP シグナル送信ポート上で SIP 以外のパケットを許可する**」を選択すると、追加の独自メッセージで SIP シグナル送信ポートを用いるアプリケーション (例えば、Apple iChat や MSN Messengerなど) を使用できるようになります。このオプションは、既定では選択されていません。

重要：このチェックボックスがオンの場合、不適切または無効な SIP トラフィックを濫用した悪意のある攻撃に対してネットワークが開放されてしまうおそれがあります。

8 SIP プロキシ サーバを B2BUA として使用している場合は、「**SIP Back-to-Back ユーザ エージェント (B2BUA) サポートを有効にする**」設定を有効にします。このオプションは既定で無効になっています。これを有効にするのは、セキュリティ装置がボイス通話の両行程を確認できる場合 (例えば、LAN 上の電話が同じ LAN 上の別の電話と通話する場合) だけにしてください。

ヒント：ファイアウォールがボイス通話の両行程を確認できない場合 (例えば、通話先および通話受信元が WAN 上の各電話だけに限られる場合) は、「**SIP Back-to-Back ユーザ エージェント (B2BUA) サポートを有効にする**」設定を無効にして不要な CPU の使用を回避する必要があります。

9 「**SIP シグナルのタイムアウト時間 (秒)**」オプションと「**SIP メディアのタイムアウト時間 (秒)**」オプションを使用して、通話のアイドル状態 (トラフィック交換のない状態) の許容時間を定義します。この時間の経過後は、ファイアウォールにより以降のトラフィックがブロックされます。通話は保留にされた場合、アイドル状態になります。最大アイドル時間を以下のように指定します。

- 「**SIP シグナルのタイムアウト時間 (秒)**」に、交換されるシグナル (制御) メッセージがない場合の最大アイドル時間を指定します。最小値は 30 秒、最大値は 1000000 秒 (約 1.2 日)、既定値は **3600** 秒 (60 分) です。
- 「**SIP メディアのタイムアウト時間 (秒)**」に、交換されるメディア (オーディオ、ビデオなど) パケットがない場合の最大アイドル時間を指定します。最小値は 30 秒、最大値は 3600 秒 (1 時間)、既定値は **120** 秒 (2 分) です。

10 「**追加で変換対象とする SIP シグナル UDP ポート (オプション)**」設定を使用して、非標準 UDP ポートを SIP シグナル トラフィックの搬送に使用するように指定します。SIP シグナル トラフィックは UDP ポート 5060 で搬送されるのが一般的ですが、市販 VOIP サービスによっては別のポート (例えば 1560) を使用するものもあります。この設定が 0 以外のとき (既定値は **0**、最大値は 65535)、セキュリティ装置はこれらの非標準ポートで SIP 変換を行います。

ヒント：Vonage の VoIP サービスには、UDP ポート 5061 が使用されます。

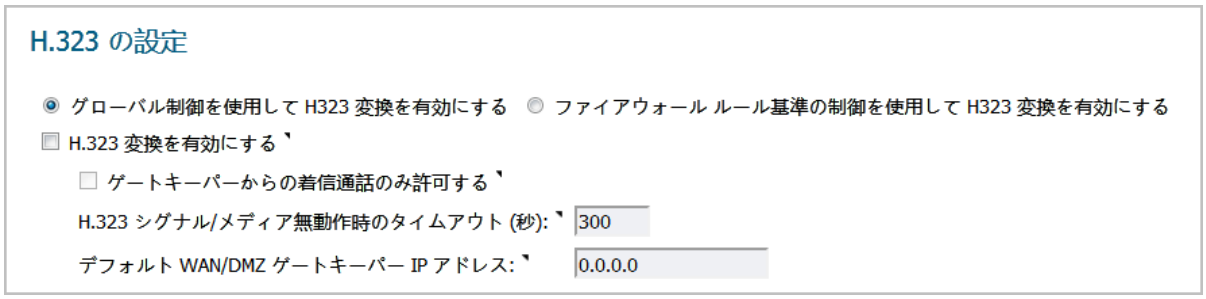
11 SIP エンドポイント登録の異常を追跡するには、「**SIP エンドポイント登録の異常追跡を有効にする**」オプションを選択します。このオプションは、既定では選択されていません。このオプションを選択すると、以下のオプションが使用できるようになります。

- **登録の追跡間隔 (秒)** - 異常をチェックする間隔を指定します。既定値は **300** 秒 (5 分) です。
- **失敗した登録のしきい値** - 登録失敗が何件になったら異常をチェックするかを指定します。既定値は **5** 件です。
- **エンドポイント遮断間隔 (秒)** - 既定値は **3600** 秒 (60 分) です。

12 次のどちらかを行います。

- 「**適用**」を選択します。
- 「H.323 の設定 (808 ページ)」に移動します。

H.323 の設定



H.323 の設定

H.323 の設定を行うには、以下の手順に従います。

1 「**管理 | システム セットアップ > VOIP | H.323 の設定**」に移動します。

2 H.323 変換をグローバルに有効にするか、ファイアウォール ルールごとに有効にするかを選択します。

- 「**グローバル制御を使用して H323 変換を有効にする**」。このオプションは、既定では選択されています。
- 「**ファイアウォール ルール基準の制御を使用して H323 変換を有効にする**」。『*SonicOS ポリシー*』の説明に従って、H.323 変換を制御するファイアウォール ルールを設定してください。

3 H.323 変換を設定しない場合は、「ステップ 5」に進みます。

1 「**H.323 変換を有効にする**」を選択して、ステートフル H.323 プロトコルに対応したパケットのコンテンツをファイアウォールで検査/修正できるようにします。このオプションは、既定で

は無効になっています。このオプションを選択すると、その他の H.323 オプションが使用できるようになります。

H.323 パケット内の動的 IP アドレスとトランスポート ポートとのマッピング (信頼済みネットワーク/ゾーンおよび信頼されていないネットワーク/ゾーン内での H.323 通話相手どうしの通信に必要) も、ファイアウォールによって実行されます。

ファイアウォールで H.323 固有処理の実行を省略する場合は、「**H.323 を有効にする**」を無効にしてください。

2 「**ゲートキーパーからの着信通話のみ許可する**」を選択すると、すべての着信通話がゲートキーパーの認証を受けます。認証に失敗した通話は、ゲートキーパーに拒絶されます。

3 「**H.323 シグナル/メディア無動作時のタイムアウト (秒)**」フィールドに、通話アイドル状態を許可する秒数を指定します。この時間の経過後は、ファイアウォールにより以降のトラフィックがブロックされます。通話は保留にされた場合、アイドル状態になります。既定値は **300** 秒 (5 分)、最小値は 60 秒 (1 分)、最大値は 122400 秒 (34 時間) です。

4 「**デフォルト WAN/DMZ ゲートキーパー IP アドレス**」フィールドの既定値は **0.0.0.0** です。このフィールドに既定の H.323 ゲートキーパー IP アドレスを入力すると、LAN ベースの H.323 機器がマルチキャスト アドレス `225.0.1.41` を使用して、ゲートキーパーを発見できるようになります。IP アドレスを入力しなかった場合は、LAN ベースの H.323 機器から送出されたマルチキャスト ディスカバリ メッセージに対して、設定済みマルチキャスト処理が施されます。

5 「**適用**」を選択します。

トピック:

- WAN インターフェースでの帯域幅の設定 (809 ページ)
- VoIP アクセス ルールの設定 (809 ページ)

WAN インターフェースでの帯域幅の設定

メモ：WAN インターフェースでの帯域幅管理 (BWM) と BWM の設定については、『*SonicOS ポリシー*』を参照してください。

VoIP アクセス ルールの設定

既定では、ファイアウォールのステートフル パケット検査によって、LAN からインターネットへの通信はすべて許可され、インターネットから LAN に送出されるトラフィックはすべて遮断されます。既定のアクセス ルールを拡張または指定変更する、追加のネットワーク アクセス ルールを定義することもできます。

WAN から VoIP サービス プロバイダを利用できるようにクライアントの VoIP アクセス許可を定義する場合は、ファイアウォール背後のクライアントによる VoIP 通話の送受信が許可されるように、送信元インターフェース/ゾーンと送信先インターフェース/ゾーンとの間のネットワーク アクセス ルールを設定してください。

ヒント：着信 IP トラフィックを許可する個別ルールは作成可能ですが、ファイアウォールは、SYN フラッドや Ping of Death 攻撃などのサービス妨害 (DoS) 攻撃に対する保護は無効にしません。

メモ：ネットワーク アクセス ルールに帯域幅管理を設定する前に、**WAN** インターフェースの「**管理 | システム セットアップ | ネットワーク > インターフェース**」で「帯域幅管理」を選択しておく必要があります。

SonicWall セキュリティ装置で VoIP トラフィックに対するアクセス ルールを追加する方法については、『*SonicOS ポリシー*』を参照してください。

VoIP ログ採取の設定

VoIP イベントのログ記録を有効にできます。このログは、「**調査 | ログ | イベント ログ**」に表示されます。VoIP のログ記録を有効にする方法については、『*SonicOS 調査*』を参照してください。

第 9 部

システム セットアップ | 仮想アシスト

- 仮想アシストの設定

52

仮想アシストの設定

トピック:

- 仮想アシストについて (812 ページ)
- 仮想アシストの柔軟性の最大化 (813 ページ)

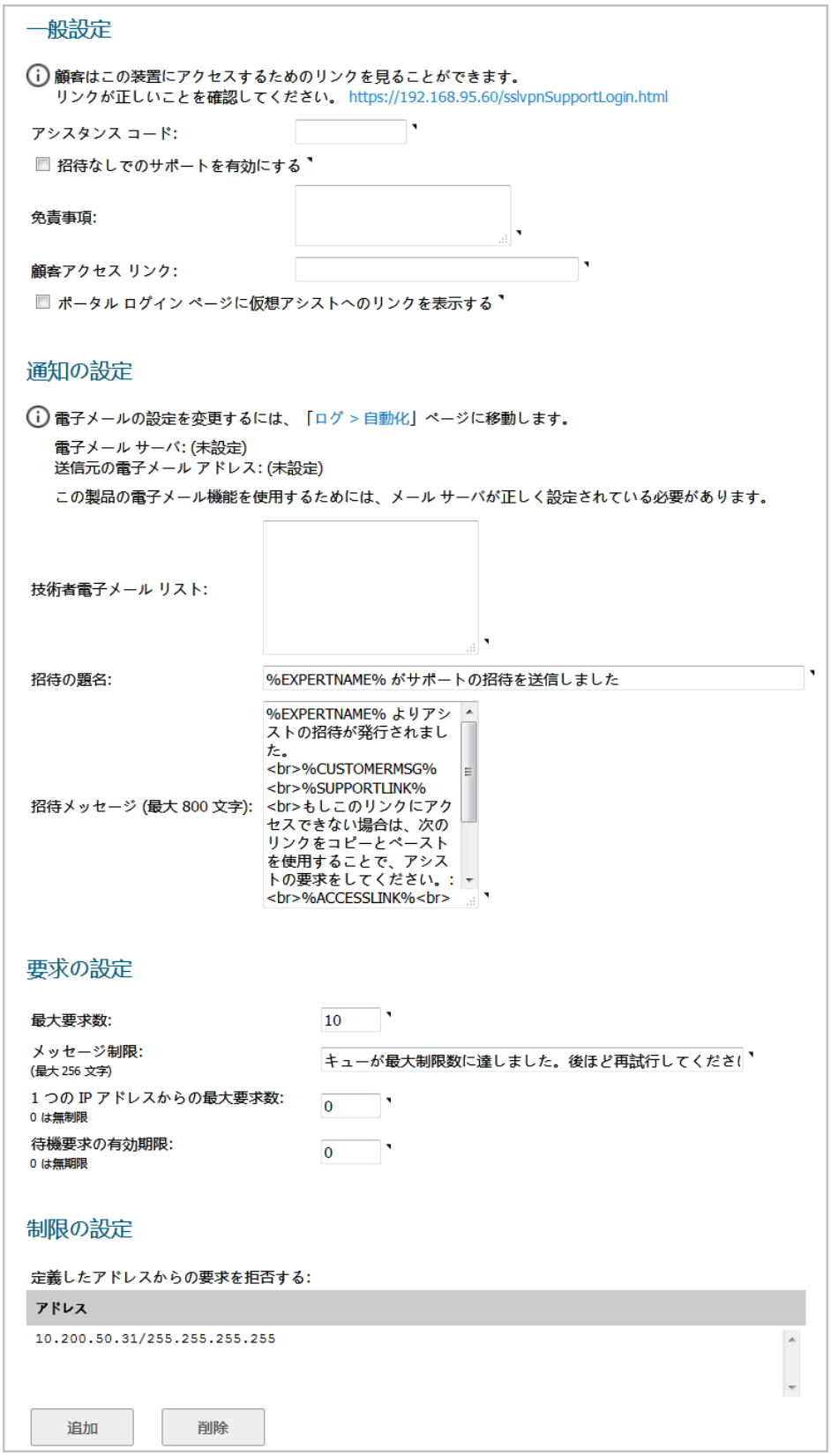
仮想アシストについて

仮想アシストを使用すると、顧客のいる場所に直接出向かなくても、顧客の技術的な問題をサポートすることができます。この機能はサポート担当者にとって、時間の大幅な節約につながるうえ、サポートの要求に柔軟に対応できるようになります。ユーザは顧客に対して、サポートを受けるための“キュー"への参加を許可または招待します。 その後で、顧客のコンピュータをリモートで制御することで各顧客を仮想的にアシストし、技術的な問題の診断と対応を行います。

メモ：仮想アシストを提供する技術者または管理者は、SonicWall セキュリティ装置のローカルネットワーク内に存在する必要があります。

仮想アシストの柔軟性の最大化

仮想アシストを制御するには、「**システム セットアップ > 仮想アシスト**」の設定を使用します。



仮想アシストの設定

仮想アシスト機能の柔軟性を最大限引き出すには、ある程度時間をかけて、すべての設定を適切に調整する必要があります。

トピック:

- ユーザにアクセスを提供する (814 ページ)
- 通知の設定 (815 ページ)
- 要求の管理 (816 ページ)
- 特定の IP アドレスからの要求の遮断 (817 ページ)

ユーザにアクセスを提供する

仮想アシストを通してサポートを受ける顧客に対してアクセスを提供する方法を決める必要があります。

- 招待の必要なく、仮想アシストのサポートを有効にする。
- 顧客にグローバルなアシスタンス コードを設定することで、システムにログインしてサポートを要求する顧客を制限することができます。コードには最大 8 文字を使用でき、「アシスタンス コード」フィールドに入力できます。顧客は技術者または管理者からの電子メールでこのコードを受け取ります。

ユーザにアクセスを提供するには:

1 「**管理 | システム セットアップ > 仮想アシスト**」に移動します。

2 顧客がサポートを要求するために入力する必要のあるグローバル コードを提供するには、「**アシスタンス コード**」フィールドに 8 文字以内の英数字を入力します。コードが不要であることを示すには、このフィールドを空白のままにします。

ヒント：アシスタンス コードには、サポートを求めてシステムに入ることができる顧客を制限する目的があります。

3 顧客が技術者から招待を受けなくても、サポート ログイン ウェブ ページからサポートを要求できるようにするには:

a 「**アシスタンス コード**」フィールドを空白のままにします。

b 「**招待なしでのサポートを有効にする**」を選択します。

メモ：このオプションが選択されていない場合、顧客は技術者から電子メールで招待を受けた場合にのみアシスタンスを受けることができます。顧客がログイン ページからサポートを要求できるようにするには、このオプションを選択してください。

4 顧客がサポートを受ける前に読んで同意する必要のある文言を作成するには、「**免責事項**」フィールドに免責事項を入力します。

5 ネットワークの外部から SSL VPN セキュリティ装置へのアクセスを提供するには、「**顧客アクセス リンク**」フィールドに URL を入力します。このフィールドを空白のままにした場合は、技術者がセキュリティ装置にアクセスするときに使うのと同じ URL が顧客に送信するサポートの招待に記載されます。

ヒント：SSL VPN セキュリティ装置が管理者のネットワークの外部から別の URL を使用してアクセスされる場合は、このオプションを設定してください。

6 顧客が技術者のログイン ページを表示した場合にサポート ログイン ページにリダイレクトするには、「**ポータル ログイン ページに仮想アシストへのリンクを表示する**」を選択します。

7 「**適用**」を選択します。

8 顧客に表示するアクセス リンクが正しいことを確認するには、「**一般設定**」の情報メッセージに表示されるリンクを選択します。「ステップ 5」で設定したアクセス リンクが表示されます。以下に例を示します。

> チケットの無い要求は許可されません。管理者が「招待なしでのサポートを有効にする」オプションを選択する必要があります。

通知の設定

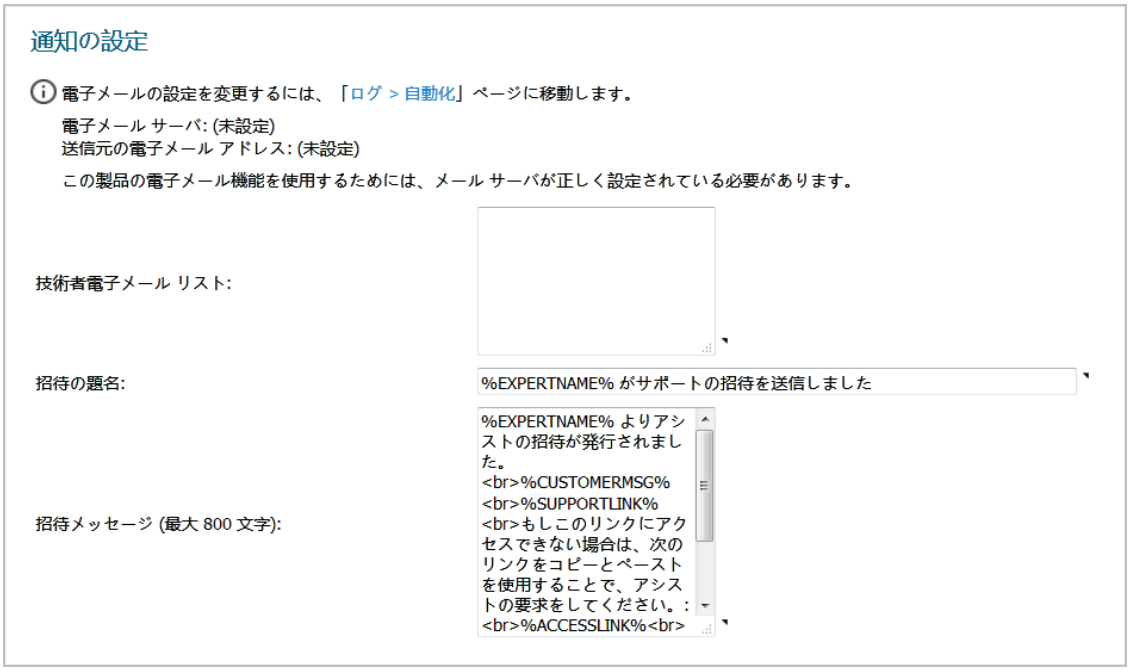
「**通知の設定**」セクションでは、招待および技術者への通知に関するさまざまな面をカスタマイズできます。

招待および技術者への通知をカスタマイズするには:

重要：通知を設定する前に、「**管理 | ログと報告 | ログの設定 | 自動化**」で電子メール サーバと電子メール アドレスを設定してください。このページをすばやく表示するには、「**通知の設定**」セクションの情報メッセージに表示されるリンクを選択します。電子メール サーバの設定については、『*SonicOS ログとレポート*』を参照してください。

1 「**管理 | システム セットアップ > 仮想アシスト**」に移動します。

2 「**通知の設定**」までスクロールします。



3 招待されていない顧客がサポート キューに入ったときに電子メールで通知を受け取る技術者の電子メール アドレスのリストを、「**技術者電子メール リスト**」フィールドで作成します。このリストに登録できる電子メールは最大 10 件です。各アドレスをセミコロンで区切って指定します。

4 サポートの招待の電子メールの件名をカスタマイズするには、「**招待の題名**」フィールドで「変数」テーブルに示す変数を用いて必要なテキストを入力します。件名のサンプルが提供されています。

変数

項目	説明
技術者名	%EXPERTNAME%
招待での顧客のメッセージ	%CUSTOMERMSG%
サポート用のリンク	%SUPPORTLINK%
SSL VPN へのリンク	%ACCESSLINK%

5 サポートの招待の電子メールの本文をカスタマイズするには、「**招待メッセージ**」フィールドで「変数」テーブルの変数を用いて必要なテキストを入力します。メッセージは最大 800 文字です。本文のサンプルが提供されています。

6 「**適用**」を選択します。

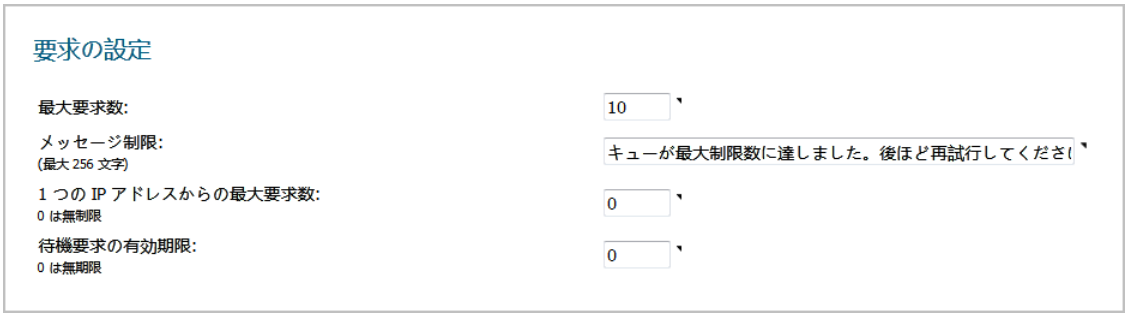
要求の管理

サポート要求の管理と制限は、「**要求の設定**」セクションで行います。

サポート要求の管理と制限を行うには:

1 「**管理 | システム セットアップ > 仮想アシスト**」に移動します。

2 「**要求の設定**」までスクロールします。



3 キュー内でサポートを待機する顧客の数を制限するには、「**最大要求数**」フィールドに上限を入力します。この上限に達すると、新しい要求は遮断されます。既定のサイズは **10** 件です。

4 要求の件数が上限に達して現在のキューに空きがなくなったとき、顧客にメッセージを表示するには、「**メッセージ制限**」フィールドにメッセージを入力します。作成できるメッセージは最大 256 文字です。メッセージのサンプルが提供されています。

5 同一の IP から受け入れる要求の件数を制限するには、「**1 つの IP アドレスからの最大要求数**」フィールドに上限を入力します。同じ顧客が仮想アシストのサポートを一度に何回も要求してキューに複数回入るという事態をこれで回避できます。上限を設定しない場合は **0** (既定値) を入力します。

6 要求が多い時間帯に、仮想アシストのサポートを求める顧客がいつまでも待機するという状況を防ぐために、サポートを受けていない顧客がキューにいられる時間の上限を設定できます。この上限は、「**待機要求の有効期限**」フィールドに分単位で入力します。上限を設定しない場合は **0** (既定値) を入力します。

7 「**適用**」を選択します。

特定の IP アドレスからの要求の遮断

不要または不正な送信元から要求を受けることがある場合には、指定した IP アドレスからの要求を遮断することができます。

特定の IP アドレスからの要求を遮断するには:

1 「**管理 | システム セットアップ > 仮想アシスト**」に移動します。

2 「**制限の設定**」までスクロールします。

3 「**追加**」を選択します。「**管理アドレス**」ダイアログが表示されます。

4 「**送信元アドレス種別**」で、送信元のアドレスの種別を選択します。

- **IP アドレス** - 既定
- **IP ネットワーク** - オプションが変化します。「ステップ 7」に進みます。

5 「**IP アドレス**」フィールドに、遮断する IP アドレスを入入力します。

6 「ステップ 9」へ進みます。

7 「**ネットワーク アドレス**」フィールドに、遮断するネットワーク アドレスを入力します。

8 「**サブネット マスク**」フィールドに、アドレスのサブネット マスクを入力します。

9 「**OK**」を選択します。「**定義したアドレスからの要求を拒否する**」テーブルにエントリが追加されます。

10 「**適用**」を選択します。

遮断するアドレスの削除

「定義したアドレスからの要求を拒否する」フィールドからエントリを削除するには:

1 「**管理 | システム セットアップ > 仮想アシスト**」に移動します。

2 「**制限の設定**」までスクロールします。

3 削除するエントリを選択します。

4 「**削除**」を選択します。

第 10 部

システム セットアップ | 付録

- オープン認証、ソーシャル ログイン、LHM の設定
- BGP の高度なルーティング
- IPv6
- SonicWall サポート

A

オープン認証、ソーシャル ログイン、LHM の設定

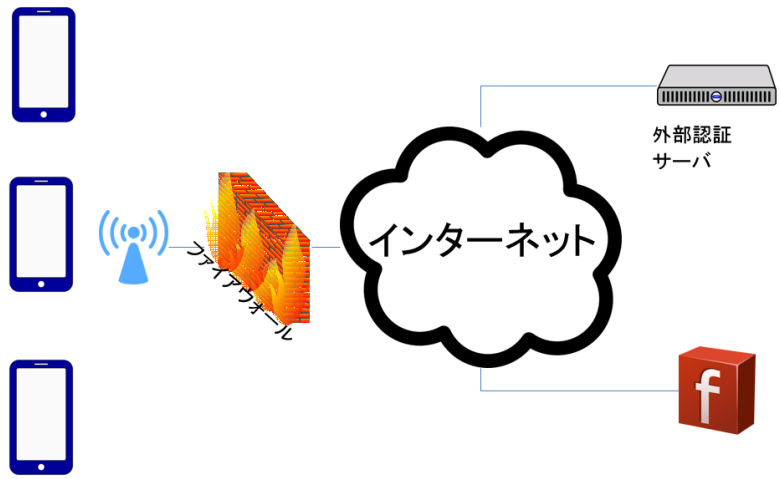
トピック:

- OAuth とソーシャル ログインについて (820 ページ)
- ライトウェイト ホットスポット メッセージング (LHM) について (824 ページ)
- ソーシャル ログインのためのフェイスブックの設定 (826 ページ)
- オープン認証とソーシャル ログインの設定 (828 ページ)
- ソーシャル ログイン設定の確認 (836 ページ)
- ソーシャル ログイン、LHM、ABE の使用 (837 ページ)

OAuth とソーシャル ログインについて

ソーシャル ログインは、シングル サイン オン認証の一形態で、ウェブサイトごとに新しいログイン アカウントを個別に作成する代わりに、フェイスブック、ツイッター、グーグル + などのソーシャル ネットワーキング サービスの既存のユーザ資格情報を利用してサードパーティのウェブサイトにサインインします。オープン認証 (OAuth) によるソーシャル ログイン機能は、パススルー認証を使用している、無線ゾーン、LAN ゾーン、または DMZ ゾーン上のゲスト サービスによって使用できます。「外部認証サーバ ログインのトポロジ」を参照してください。パススルー認証は、信頼済みドメイン内にあるドメイン コントローラに対して認証を実行する方法です。無線ゲスト サービスは、公衆 WiFi ホットスポットや企業のゲスト用 WiFi サービス設定で広く利用されています。

外部認証サーバ ログインのトポロジ



トピック:

- OAuth およびソーシャル ログインとは (821 ページ)
- OAuth とソーシャル ログインのメリット (821 ページ)
- OAuth とソーシャル ログインの仕組み (822 ページ)
- サポート対象プラットフォーム (823 ページ)

OAuth およびソーシャル ログインとは

OAuth は、権限の認可を行うためのオープン規格です。OAuth は、サーバ リソースへの "保護された委任アクセス" をリソース オーナーに代わってクライアント アプリケーションに提供します。リソース オーナーが自身の資格情報を共有することなく、サーバ リソースへのアクセスをサードパーティに認可するための手順を規定しています。

ソーシャル ログインは、ソーシャル サインインとも呼ばれ、シングル サイン オンの一形態で、ウェブサイトごとに新しいログイン アカウントを個別に作成する代わりに、フェイスブック、ツイッター、グーグル + などのソーシャル ネットワーキング サービスの既存のログイン情報を利用してサードパーティのウェブサイトにサインインします。

OAuth とソーシャル ログインのメリット

トピック:

- OAuth
- ソーシャル ログイン

OAuth

OAuth は、ユーザによるアプリケーション間でのデータの共有を支援する、よく知られたメカニズムです。OAuth を活用するには、ウェブ アプリケーション用のログイン プロバイダとして使用します。

その他の長所

- ネット上の顧客プロファイルが制限される
- 記録すべきパスワード数が少なくなる
- 信頼が問題になる可能性がある状況でのパスワード送信が不要
- OAuth プロバイダからのアクセスを防止できる
- ID 盗難のリスクが減少する。プロバイダが認証を担当する
- これまでに実績のある API による認証を用いることでバグによる障害のリスクが減少する
- データ サーバに対するストレージ要件が緩和される

短所

- 独自のアプリケーション向けにユーザ プロファイルを調整できない
- 既存のアカウントを持たないユーザが OAuth プロバイダでのアカウント作成時に混乱する

ソーシャル ログイン

ソーシャル ログインは、ログイン処理を簡素化するとともに、登録のためのやりとりの効率化を実現するために設計されています。

その他の長所

- 登録を短時間で行える
- 記憶するログイン情報が少なくなる
- ターゲットリッチなコンテンツ
- 複数の ID を使用できる
- 訪問者のデータを収集できる
- ユーザ エクスペリエンスを詳細化または個別化できる
- なじみのあるログイン環境を使用できる
- ログインの失敗が減る
- モバイルで使いやすい

短所

- 信頼レベルが低い
- 非ソーシャル ユーザが除外される
- データの正確さが失われる可能性がある
- ソーシャル ネットワークからのコンテンツが遮断される
- セキュリティの問題

OAuth とソーシャル ログインの仕組み

オープン認証 (OAuth) とソーシャル ログインの機能は、内部の無線サービスと無線ゾーン ゲスト サービスとしての SonicPoint の両方で使用できます。ゲストは、会社の企業用 WiFi を使用してインターネットにログインできます。無線ゲスト サービスは、公衆 WiFi ホットスポットや企業のゲスト用 WiFi サービス設定で広く利用されています。

OAuth とソーシャル ログインはどちらも、インターネット アクセスが含まれている無線ゲスト サービスを使用し、以下の接続方法のどちらかまたは両方を使用するように設定できます。

- リダイレクトなし (822 ページ)
- 開始ページへのリダイレクト (823 ページ)

リダイレクトなし

リダイレクトなしでは、暗号化が必須ではないオープンなインターネット アクセスがゲストに提供されるので、ゲストは提供されている WiFi に自由に接続できます。

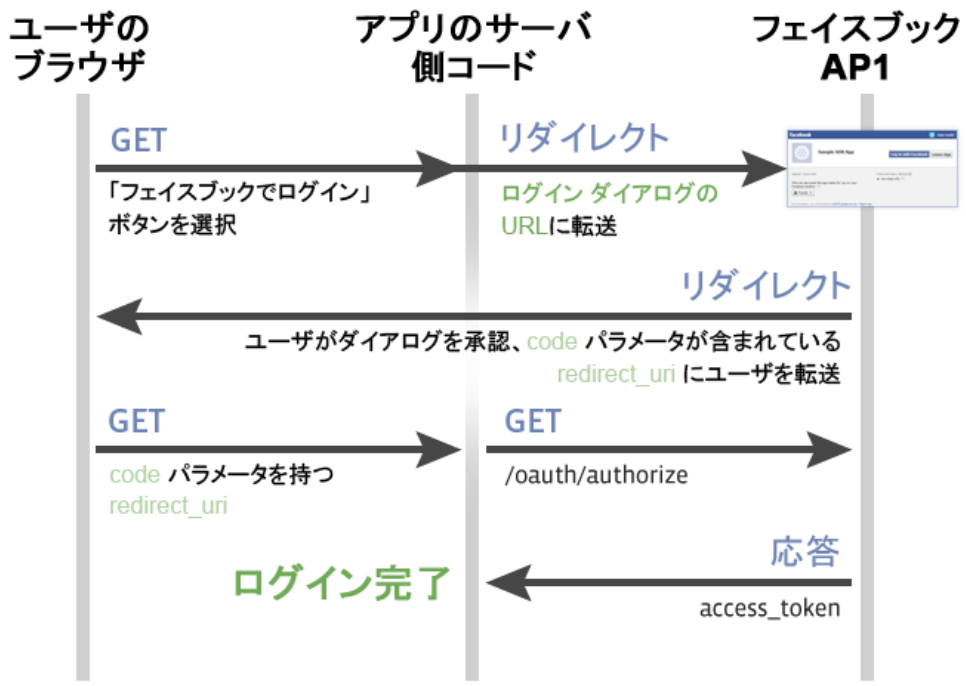
リダイレクトなしでは、利用可能な WiFi をゲストが使用するためにパスコードが必要になる、WPA/WEP パスフレーズまたはパスワードによるアクセスも提供できます。パスコードは、レシートなど、その他の手段によって提供することも可能です。

開始ページへのリダイレクト

開始ウェブ ページは、最も広く使用されているホットスポットアクセスを提供します。レイヤ 2 WiFi アクセスがオープンになっている場合、ゲストが最初のレイヤにアクセスすると開始ウェブ ページに誘導されます。「OAuth のフロー」を参照してください。その他のリダイレクト アクセスの選択肢として以下のものがあります。

- 開始ページでの認証なし
- ゲストが新しいログイン アカウントを作成したうえでそのアカウントでサインインできる
- 携帯電話への SMS によって送信されたコード、またはその他の方法を使用して、ゲストがサインアップできる
- モバイル アプリによって QR コードをスキャンする
- ソーシャル ログインの使用

OAuth のフロー



サポート対象プラットフォーム

オープン認証とソーシャル ログインは、以下の SonicWall ファイアウォールでサポートされています。

- SonicOS 6.2.7 以上を実行している
- GMS 8.3 を実行している GMS 管理下にある

開発と実稼働の要件

- フェイスブック アカウント
  - 開発者向けフェイスブックを有効にする
- 外部サーバ
  - パブリックにアクセス可能
  - ドメイン名を持つ
  - PHP サポート
  - SSL 証明書
- SonicWall ファイアウォール
  - 外部サーバから (IP または FQDN によって) 到達可能
  - 無線 (内部または SonicPoint)

ライトウェイト ホットスポット メッセージング (LHM) について

ライトウェイト ホットスポット メッセージング (LHM) では、SonicWall ゲスト サービス モデルを利用しています。このモデルでは、SonicWall セキュリティ装置によるネットワーク アクセスの差別化のためにユーザの分類と承認を行うことができます。例えば、ゲストサービスが有効な WLAN (無線 LAN) ゾーンに属するインターフェース経由で接続しているユーザがインターネット (非保護ネットワーク) へのアクセス権のみを持ち、LAN (保護ネットワーク) へのアクセス権を持たないように SonicWall を設定することができます。これにより、単一のファイアウォールによる信頼済みユーザとゲスト ユーザへの同時アクセスの提供が可能になります。

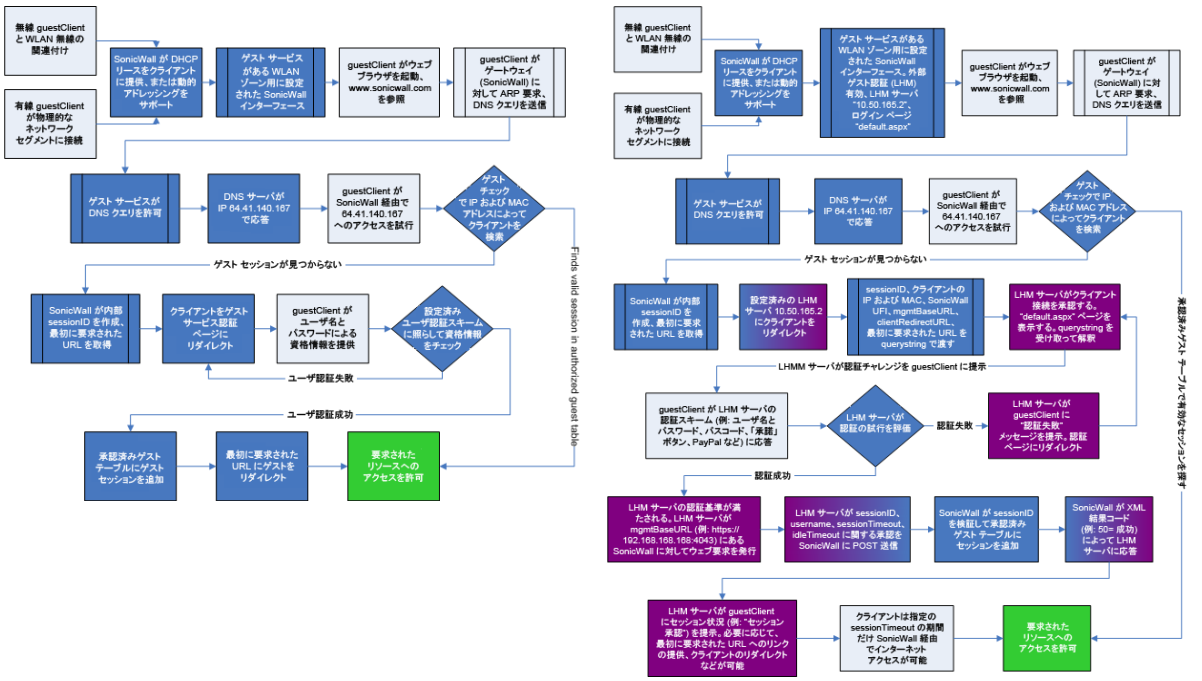
LHM は、認証と承認の処理を分離することでゲスト サービス モデルを拡張します。そうすることで、SonicWall の外部で認証を行うことができます。これにより、認証インターフェースの大規模なカスタマイズが可能になり、考えられる任意の種類の認証スキームを使用できるようになります。

「承認フローの比較」テーブルは、元のゲスト サービス承認フローと LHM 承認フローを横に並べて示したものです。

承認フローの比較

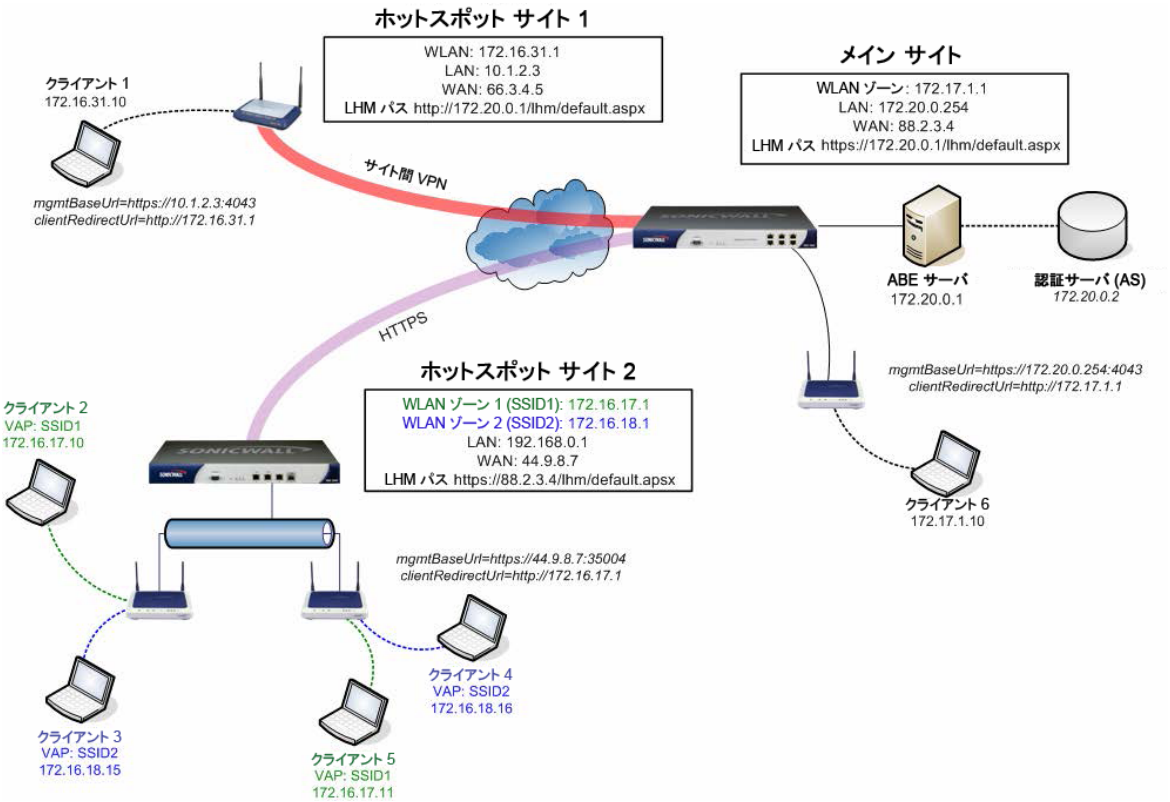
元のゲスト サービス承認フロー

LHM 承認フロー



LHM は、SonicWall 無線アクセス デバイス (SOHO W ファイアウォール、TZ 無線シリーズ ファイアウォール、管理用 SonicWall セキュリティ装置を持つ SonicPoint など) と、ホットスポット ユーザの認証、およびそうしたユーザへのパラメータによってバインド されたネットワーク アクセスの提供を行うための 認証バックエンド (ABE) との間の通信を行うための方法と構文を定義しています。「LHM の設定例」に一般的な設定を示します。

LHM の設定例



LHM を使用すると、ネットワーク オペレータは SonicWall の無線ゲスト サービスと既存の任意の ABE との間のインターフェースを提供することで、複数のホットスポット ロケーションの集中管理を行うことができます。LHM は、一般化された WISPr および GIS 仕様を改変したものです。

LHM は、幅広い環境ではなく、特に一般的な運用環境の要件を満たすために設計されました。具体的には、LHM を使用すると、ネットワーク オペレータの ABE 全体で発生する、ホットスポットのユーザ管理や認証を行うことができ、あらゆる方法のアカウント作成および管理のサポートと、サイトに対するいかなる範囲のカスタマイズやブランディングが可能になります。こうしたアプローチにより、特定の課金、会計処理、またはデータベース システムとの依存関係なしに、既存の環境への組み込みが可能です。また、ネットワーク オペレータは、外観からリダイレクトまで、サイトのデザインを無制限に制御できます。

IPv4 トラフィックと IPv6 トラフィックの認証を提供するために、SonicOS は 2 つの外部 Lightweight Hotspot Messaging (LHM) ウェブ サーバをサポートします。1 つは IPv4 用、もう 1 つは IPv6 用です。さまざまなトラフィック タイプが、対応する LHM サーバにリダイレクトされます。

ソーシャル ログインのためのフェイスブックの設定

トピック:

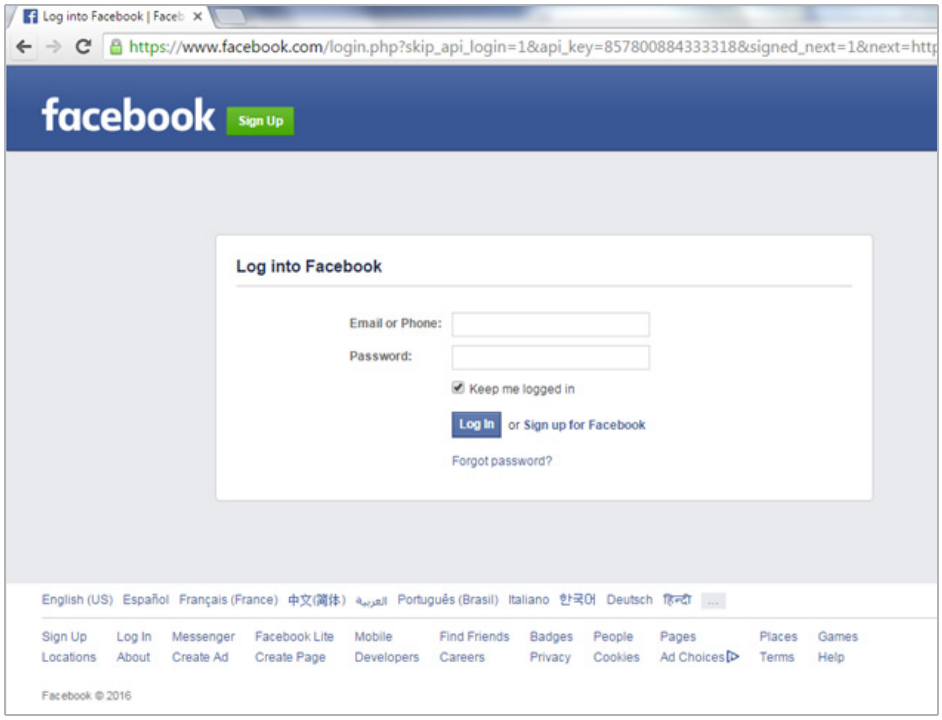
- フェイスブック設定 (827 ページ)
- クライアント OAuth 設定 (828 ページ)
- ゲスト状況 (デモ) (828 ページ)

フェイスブック設定

開発者向けフェイスブックにログインするには、以下の手順に従います。

1 ウェブ ブラウザを開きます。

2 開発者向けフェイスブックのアカウント (https://developers.facebook.com/) にログインします。

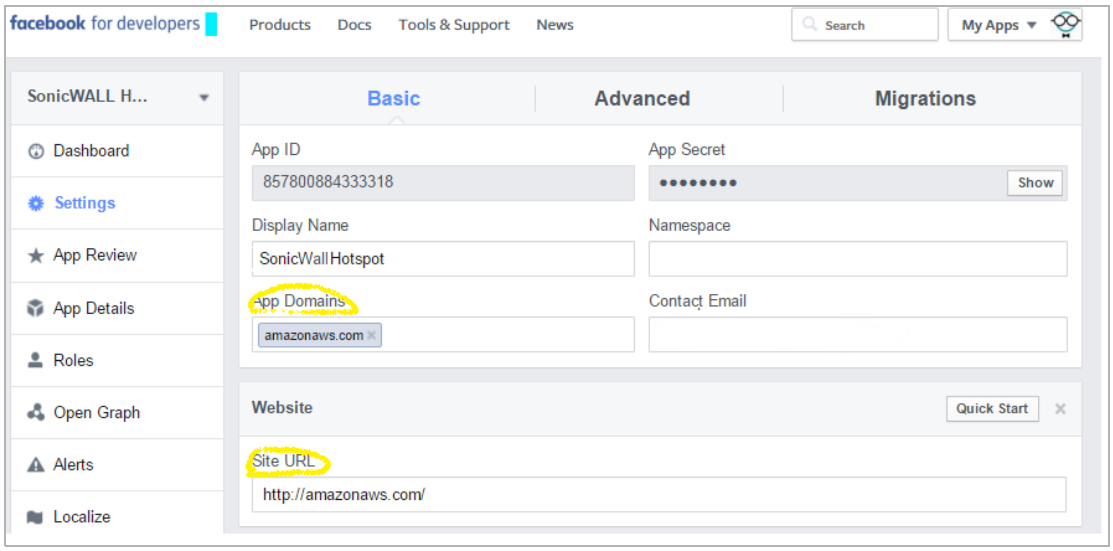


3 ログイン処理を完了するか、新しい開発者のアカウントのサインアップを行います。

4 左側の列にある「**設定**」を選択します。

「開発者向けフェイスブックの設定例」を参照してフォームに記入しますが、フェイスブックの「**設定**」は LHM サーバに合わせて調整します。

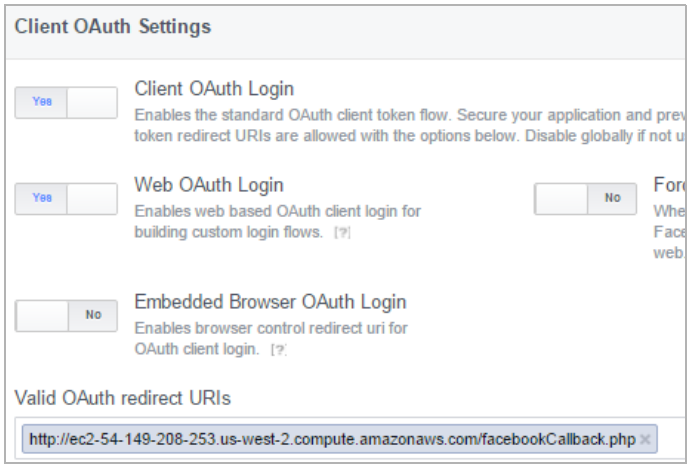
開発者向けフェイスブックの設定例



クライアント OAuth 設定

「OAuth フェイスブックの設定例」に示す設定を参考にして、開発者向けフェイスブック (https://developers.facebook.com/) でのクライアント OAuth 設定を調節する必要があります (「**製品 > フェイスブック ログイン > 設定**」)。

OAuth フェイスブックの設定例



ゲスト状況 (デモ)

無線クライアントが SonicWall WiFi へのアクセスを許可されている場合、所有者のアカウント名および情報は SonicOS に送信されます。この情報は、独自のデータベースに収集および保管できます。

オープン認証とソーシャル ログインの設定

トピック:

- ゲスト サービスの設定について (828 ページ)
- ソーシャル ログインの設定について (829 ページ)
- SonicOS でのソーシャル ログインの設定 (829 ページ)

ゲスト サービスの設定について

SonicOS はそれ自体のゲスト アカウント管理を提供していますが、ビジネス要件への適合性を高めるために独自の IT インフラストラクチャを使用できます。この設定は、外部ゲスト認証またはソーシャル ログインを設定することで行えます。「**ゲスト サービス**」は、SonicOS 無線ゾーン、LAN ゾーン、または DMZ ゾーン (「**管理 | システム セットアップ > ネットワーク > ゾーン**」) の「**ゾーンの追加/編集**」ダイアログで提供されます。

ソーシャル ログインの設定について

この機能は、エンド ユーザの面倒なログインを簡素化するとともに、信頼性の高い人口統計情報をウェブ開発者に提供します。

ソーシャル ログインを設定するための準備を行うには、以下の手順に従います。

1 無線ゾーン、LAN ゾーン、または DMZ ゾーンの作成を「新しいゾーンの追加 (430 ページ)」の説明に従って行い、セキュリティ機能を備えたネットワークゾーンを設定または編集します。

2 SonicOS では、外部サーバをライトウェイト ホットスポット メッセージング (LHM) サーバ IP アドレス オブジェクトまたは FQDN アドレス オブジェクトとして作成したり選択したりすることもできます。

SonicOS でのソーシャル ログインの設定

セキュリティ装置を適切に設定するには、ある程度の設定を行う必要があります。セキュリティ装置はほとんどのインターネット アプリケーションを遮断しますが、この機能を適切に動作させるには、いくつかを許可する必要があります。

重要：ソーシャル ログインを設定する前に、LHM サーバを稼働させておく必要があります。

ソーシャル ログイン用にセキュリティ装置を設定するには:

1 「**管理 | システム セットアップ > ネットワーク > ゾーン**」に移動して、無線セキュリティ機能を備えたネットワーク ゾーンを設定または編集します。ネットワーク ゾーンの追加の詳細については、「新しいゾーンの追加 (430 ページ)」を参照してください。

メモ：外部サーバをライトウェイト ホットスポット メッセージング (LHM) サーバ IP アドレス オブジェクトまたは FQDN アドレス オブジェクトとして作成したり選択したりすることもできます。

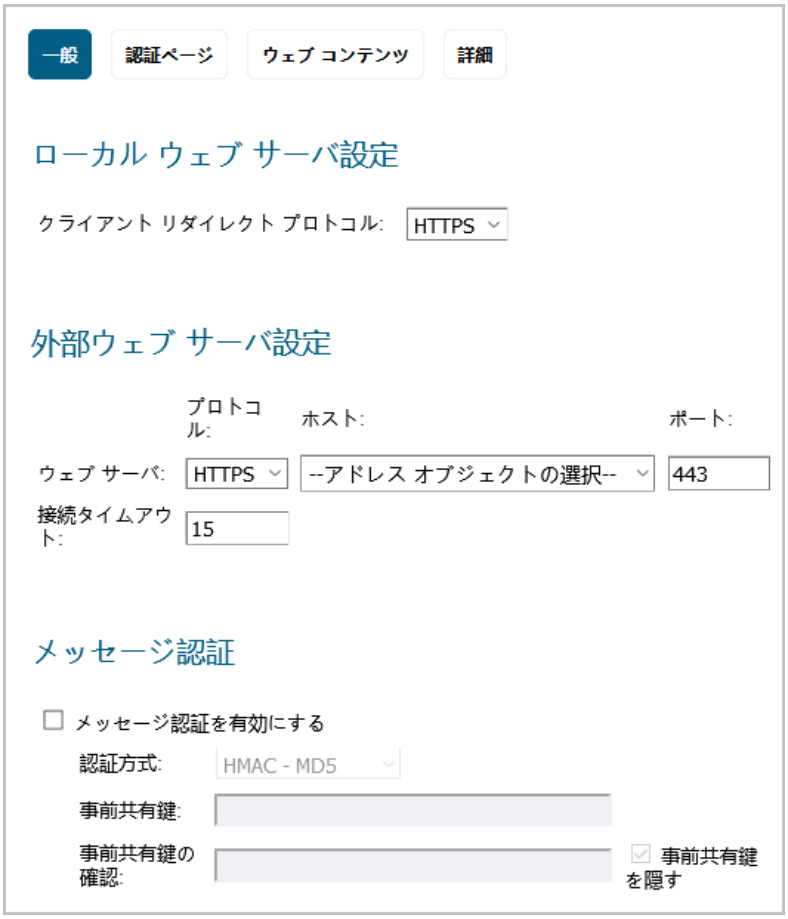
2 WLAN の「**編集**」アイコンを選択して、WLAN ネットワーク ゾーンにアクセスします。「**ゾーンの編集**」ダイアログが表示されます。

3 「**ゲスト サービス**」を選択します。

4 「**ゲスト サービスを有効にする**」を選択します。その他のアクションがアクティブになります。

5 「**外部ゲスト認証を有効にする**」を選択します。「**設定**」が有効になり、次の 4 つのオプションが使用できなくなります。

6 「**設定**」を選択します。「**外部ゲスト認証を有効にする**」ダイアログが表示されます。



7 「**ローカル ウェブ サーバ設定**」の「**クライアント リダイレクト プロトコル**」から、次のいずれかを選択します。

- **HTTPS** (既定)
- **HTTP**

認証サーバとユーザとの間の認証処理トラフィックを許可するために必要なパススルー認証ネットワーク ドメインが SonicOS によって自動的に作成されます。自動的に追加されるアドレス オブジェクト グループの名前は、「既定のソーシャル ログイン パス グループ」になります。このアドレス オブジェクト グループは、現在設定されている通信を許可するネットワークがある場合はそのネットワークに追加されます。ない場合は、「ソーシャル ログイン パス グループ」という名前の新しいグループに追加されます。

8 「**外部ウェブ サーバ設定**」では、LHM サーバが既に稼働している必要があります。

- プロトコルを選択します。「**HTTPS**」 (既定) または「**HTTP**」を選択します。
- LHM サーバに関連付けられているアドレス オブジェクトを「**ホスト**」から選択します。
- LHM サーバ上の選択したプロトコルで行われる操作の TCP ポート番号を「**ポート**」に入力します。既定値は **80** です。

- リダイレクト試行で LMH サーバが使用できないと見なされるまでの時間 (秒単位) を「**接続タイムアウト**」に入力します。既定値は **15** 分です。タイムアウトすると、「**ウェブコンテンツ**」タブで設定した `Server Down` (サーバ ダウン) メッセージがクライアントに提示されます。

9 メッセージ認証を有効にするには、「**メッセージ認証**」で「**メッセージ認証を有効にする**」を選択します。下位のオプションが利用可能になります。このオプションは、既定では選択されていません。

> **ヒント**：LHM サーバとの通信で HMAC ダイジェストおよび埋め込みクエリ文字列を使用します。これは、HTTP を使用した LHM サーバとの通信時にメッセージ改変の不安がある場合に役立ちます。オプション。

a 「**認証方式**」から以下を選択します。

- **HMAC - MD5** (既定)
- **HMAC - SHA1**
- **HMAC - SHA256**

b ハッシュ化 MAC の事前共有鍵を「**事前共有鍵**」フィールドに入力します。

> **ヒント**：事前共有鍵を使用する場合は、LHM サーバ スクリプトでも設定する必要があります。

c 「**事前共有鍵の確認**」フィールドに事前共有鍵をもう一度入力します。

d 両方のフィールドで事前共有鍵を表示する場合は、「**事前共有鍵を隠す**」をオフにします。このオプションは、既定では選択されています。

10 「**ソーシャル ネットワーク ログイン**」セクションで、「**ソーシャル ネットワーク ログインを有効にする**」を選択します。ソーシャル ネット ワークのオプションが有効になります。

11 オープン認証のために有効にするソーシャル ネットワークを 1 つ以上選択します。

- **フェイスブック**
- **グーグル**
- **ツイッター**

認証サーバとユーザとの間の認証処理トラフィックを許可するために必要なパススルー認証ネットワーク ドメインが SonicOS によって自動的に作成されます。自動的に追加されるアドレス オブジェクト グループの名前は、「**既定のソーシャル ログイン パス グループ**」になります。このアドレス オブジェクト グループは、現在設定されている通信を許可するネットワークがある場合はそのネットワークに追加されます。ない場合は、「**ソーシャル ログイン パス グループ**」という名前の新しいグループに追加されます。

12 「**認証ページ**」を選択します。

ヒント：これらのページはそれぞれ LHM サーバ上の一意のページである場合も、すべてのページが状況メッセージごとに個別のイベント ハンドラを持つ同一のページである場合もあります。新たに作成したスクリプトと連携させるための例を以下に示します。

13 **ログイン ページ**の場所 (`login.php` など) を開発者の入力ページに基づいて入力しますこれらのスクリプトは、独自の LHM サーバによってホストされているので、適切に機能していることを確認できるはずです。

14 残りのページの場所を入力します。

- **セッション期限切れページ** - セッションが期限切れになったときにクライアントがリダイレクトされるページです。セッションが期限切れになった後、ユーザは新しい LHM セッションを作成する必要があります。
- **無動作タイムアウト ページ** - 無動作タイマーが時間超過になったときにクライアントがリダイレクトされるページです。無動作タイマーが時間超過になった後も、そのセッションの残り時間がある限り、ユーザは同じ資格情報を用いて再びログインできます。
- **最大セッション ページ** - セッションの最大数に到達したときにクライアントがリダイレクトされるページです。
- **トラフィック超過ページ** - 最大トラフィックに達したときにクライアントがリダイレクトされるページです。

15 これらのオプションの設定が完了したら、「ステップ 27」に進みます。

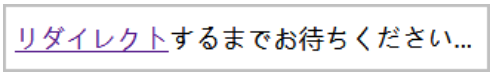
16 必要に応じて、「**ウェブ コンテンツ**」を選択します。

17 「**リダイレクト メッセージ**」には、クライアントに (通常 1 秒間だけ) 提示される既定のメッセージまたはカスタマイズしたメッセージを指定します。これで、セッションが LHM サーバにリダイレクトされる理由を説明します。このインタースティシャル ページは、(LHM サーバに直接アクセスするのではなく) SonicWall セキュリティ装置が LHM サーバの可用性を確認できるようにするために使用されます。次のどちらかを選択します。

- **既定値を使用** (既定)。「ステップ 20」に進みます。
- **カスタマイズ** - 「カスタマイズ」フィールドと「**プレビュー**」が有効になります。

18 「**カスタマイズ**」フィールドにカスタム メッセージを入力します。テキストには HTML フォーマットを含めることができます。

19 カスタマイズしたメッセージ (または既定のメッセージ) のプレビューを表示するには、「**プレビュー**」を選択します。「**外部ゲストのリダイレクト**」メッセージには、例えば、次のような既定のメッセージが表示されます。



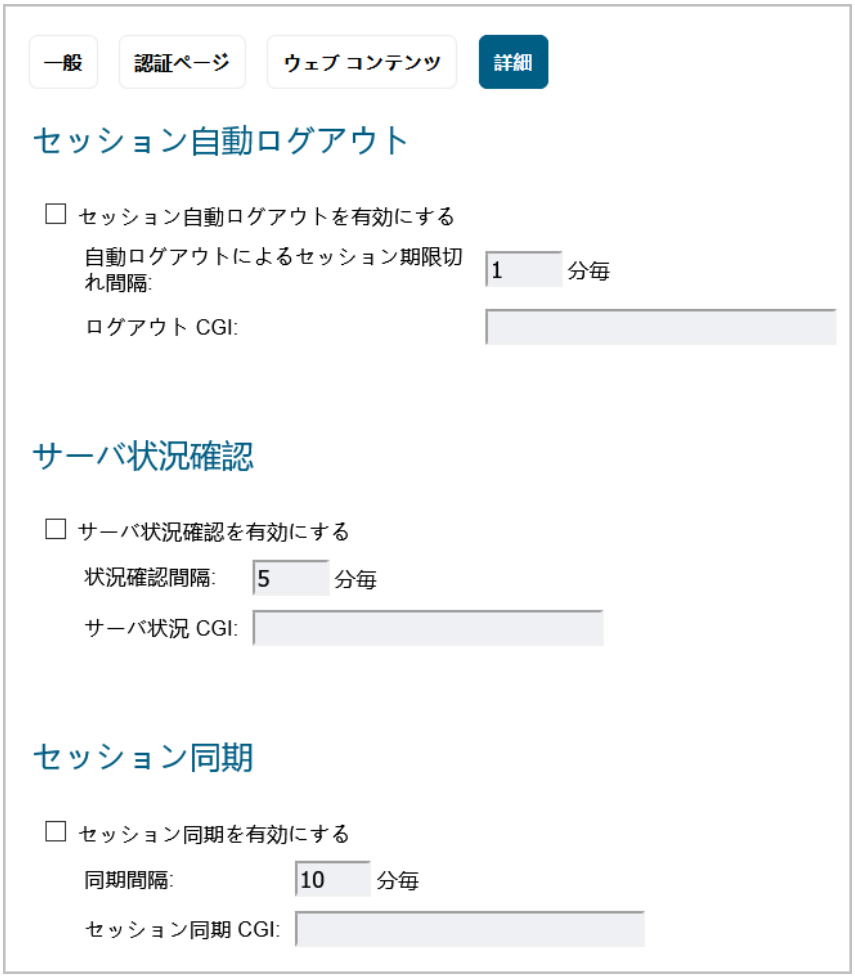
20 「**サーバ ダウン メッセージ**」には、LHM サーバが利用不可の状態にあることをリダイレクト実行側が確認したときに、クライアントに提示される既定のメッセージまたはカスタマイズしたメッセージを指定できます。次のどちらかを選択します。

- **既定値を使用** (既定)。「ステップ 21」に進みます。
- **カスタマイズ** - 「**カスタマイズ**」フィールドにカスタム メッセージを入力します。テキストには HTML フォーマットを含めることができます。

21 カスタマイズしたメッセージ (または既定のメッセージ) のプレビューを表示するには、「**プレビュー**」を選択します。「**無線サービスが利用できません**」メッセージには、例えば、次のような既定のメッセージが表示されます。

22 これらのオプションの設定が完了したら、「ステップ 27」に進みます。

23 必要であれば、「**詳細**」タブを選択します。



24 セッションの (自動または手動) ログアウト時の時間増分と、そのときに SonicWall セキュリティ装置が POST 送信を行うページを指定するには、「自動セッション ログアウト」セクションの「**セッション自動ログアウトを有効にする**」を選択します。2 つのサブオプションが使用可能になります。このオプションは、既定では選択されていません。

   a 自動セッションをログアウトするための時間増分を指定するには、「**自動ログアウトによるセッション期限切れ間隔**」フィールドに時間 (分) を指定します。既定値は **1** 分です。

   b ログアウトする Common Gateway Interface (CGI) を「**ログアウト CGI**」に入力します。

25 LHM サーバ上またはその背後にあるコンポーネント (バックエンド データベースなど) の可用性を決定する時間増分とセキュリティ装置の POST 送信対象ページを指定するには、「**サーバ状況確認**」セクションの「**サーバ状況確認を有効にする**」を選択します。2 つのサブオプションが使用可能になります。このオプションは、既定では選択されていません。

   a サーバ状況を確認するための時間増分を指定するには、時間 (分) を「**状況確認間隔**」フィールドに入力します。既定値は **1** 分です。

   b サーバ状況 CGI を「**サーバ状況 CGI**」に入力します。

26 セキュリティ装置がゲスト サービス セッション テーブル全体を POST 送信するときの時間増分と対象ページを指定するには、「**セッション同期**」セクションの「**セッション同期を有効にする**」を選択します。2 つのサブオプションが使用可能になります。このオプションは、既定では選択されていません。

   a ゲスト サービスのセッション テーブルをポストするときの時間増分を指定するには、時間 (分) を「**同期間隔**」フィールドに入力します。既定値は **10** 分です。

   b セッション同期 CGI を「**セッション同期 CGI**」フィールドに入力します。

27 「**OK**」を選択します。

ソーシャル ログイン設定の確認

オープン認証とソーシャル ログインが適切に設定されていることは、「**管理 | ポリシー > オブジェクト**」を表示することで確認できます。オブジェクトの詳細については、『*SonicOS ポリシー*』を参照してください。

設定を確認するには、以下の手順に従います。

1 「**管理 | ポリシー > オブジェクト > アドレス オブジェクト**」に移動します。

2 「**アドレス グループ**」を選択します。次のように表示されるはずです。

- ドメインが自動的に追加されています。
- フェイスブック、グーグル、ツイッターのログイン トラフィックのパススルーを首尾よく行うことができます。

ソーシャル ログイン、LHM、ABE の使用

トピック:

- ABE について (837 ページ)
- セッション ライフ サイクル (838 ページ)
- メッセージ形式 (846 ページ)
- LHM RESTful API (852 ページ)
- よくある質問と回答 (FAQ) (853 ページ)
- LHM スクリプト ライブラリ (860 ページ)

ABE について

ABE は、ユーザ インタラクションのためのコンテンツをホストするウェブ サーバ (WS) と、ディレクトリ サービス認証を提供する認証サーバ (AS、省略可能) で構成されます。AS は、RADIUS、LDAP、AD など、任意の種類のユーザ認証メカニズムとすることができます。唯一の要件は、WS が認証の目的で AS と通信できることです。WS と AS の管理は 1 台のサーバでも、別々のサーバでも行えます。

また、LHM は、AS が SonicWall セキュリティ装置の内部ユーザ データベースをユーザ認証のために使用するための機能も備えています。メッセージングの詳細については、「メッセージ形式 (846 ページ)」、「ローカル認証要求 (847 ページ)」、および「ローカル認証応答 (847 ページ)」を参照してください。

ABE は、結果コードやセッション情報を交換するためにホットスポット SonicWall と通信する必要があります。すべての通信は、HTTPS であり、(SonicWall セキュリティ装置の LAN、WAN、X0 インターフェースなどに対して) 直接、または SonicWall セキュリティ装置の管理インターフェース アドレスのいずれかに対して VPN トンネルを介して、行うことができます。LHM 管理インターフェースは、ルート (パス) ルックアップによって自動的に取得され、その管理インターフェースのみが、自動的に追加されたアクセス ルールによって LHM 管理メッセージングを受理します。

LHM 通信は、SonicWall セキュリティ装置上で定義する必要がある特定の LHM 管理ポートで発生します。この LHM 管理ポートは、標準の HTTPS 管理ポートとは異なるものでなければなりません。

ABE による SonicWall との通信を許可するとともに、クライアントを SonicWall 上の適切なインターフェースにリダイレクトするために、2 つのパラメータが SonicWall によって構築され、(とりわけ) ABE へのクライアント リダイレクトによって渡されます。次の通信パラメータは、ABE と SonicWall との間のすべての通信で使用する必要があります。

- *mgmtBaseUrl* - ABE が SonicWall と通信するために使用する IP アドレスとポート。これは HTTPS プロトコル指示子、選択されている LHM 管理インターフェースの IP、LHM ポート (`https://10.1.2.3:4043` など) で構成されます。
- *clientRedirectUrl* - セッションのさまざまな段階でクライアントがリダイレクトされる、SonicWall 上の IP アドレス (およびオプションのポート)。具体的には、TZW 上の LAN 管理 IP や SonicOS デバイス上の WLAN IP (`http://172.16.31.1` など) です。

パラメータ値は、セッション作成時 (「セッション作成 (838 ページ)」を参照) およびセッションの状態同期時 (「メッセージ形式 (846 ページ)」を参照) に SonicWall によって ABE に渡されます。また、すべての関連 URL を構成する際の基準として ABE によって使用される必要があります。ABE が参照している SonicWall セキュリティ装置には以下のページがあります。

- *wirelessServicesUnavailable.html* - ABE は利用不可というメッセージです。このリダイレクトは通常 SonicWall によって送信されますが、ABE によって参照されることもあります。テキストは設定可能です。
- *externalGuestRedirect.html* - セッション作成時に SonicWall によって提供される初期リダイレクト メッセージです。テキストは設定可能です。
- *externalGuestLogin.cgi* - ABE がセッション作成日時をポストするページです。
- *externalGuestLogoff.cgi* - ABE がセッション終了データをポストするページです。
- *localGuestLogin.cgi* - ABE が SonicWall の内部ユーザ データベースと照合してユーザ資格情報を認証するためのポスト先ページです。
- *createGuestAccount.cgi* - ABE が SonicWall の内部ユーザ データベースにゲスト アカウントを作成するためのポスト先ページです。
- *externalGuestUpdateSession.cgi* - ABE が既存のセッションの *sessionLifetime* および *idleTimeout* パラメータを更新するためのポスト先ページです (「セッション更新 (845 ページ)」を参照してください)。

SonicWall から ABE へ通信する場合は、ABE でホストされている URL (ホスト、ポート、ページ/リソースを含む) を SonicWall セキュリティ装置で完全に設定できます。ホストは、IP アドレスまたは完全修飾ドメイン名 (FQDN) のどちらかを使用して指定できます。FQDN を使用する場合、その名前は初回使用時に解決され、SonicWall によって IP アドレスとして保管されます。

セッション ライフ サイクル

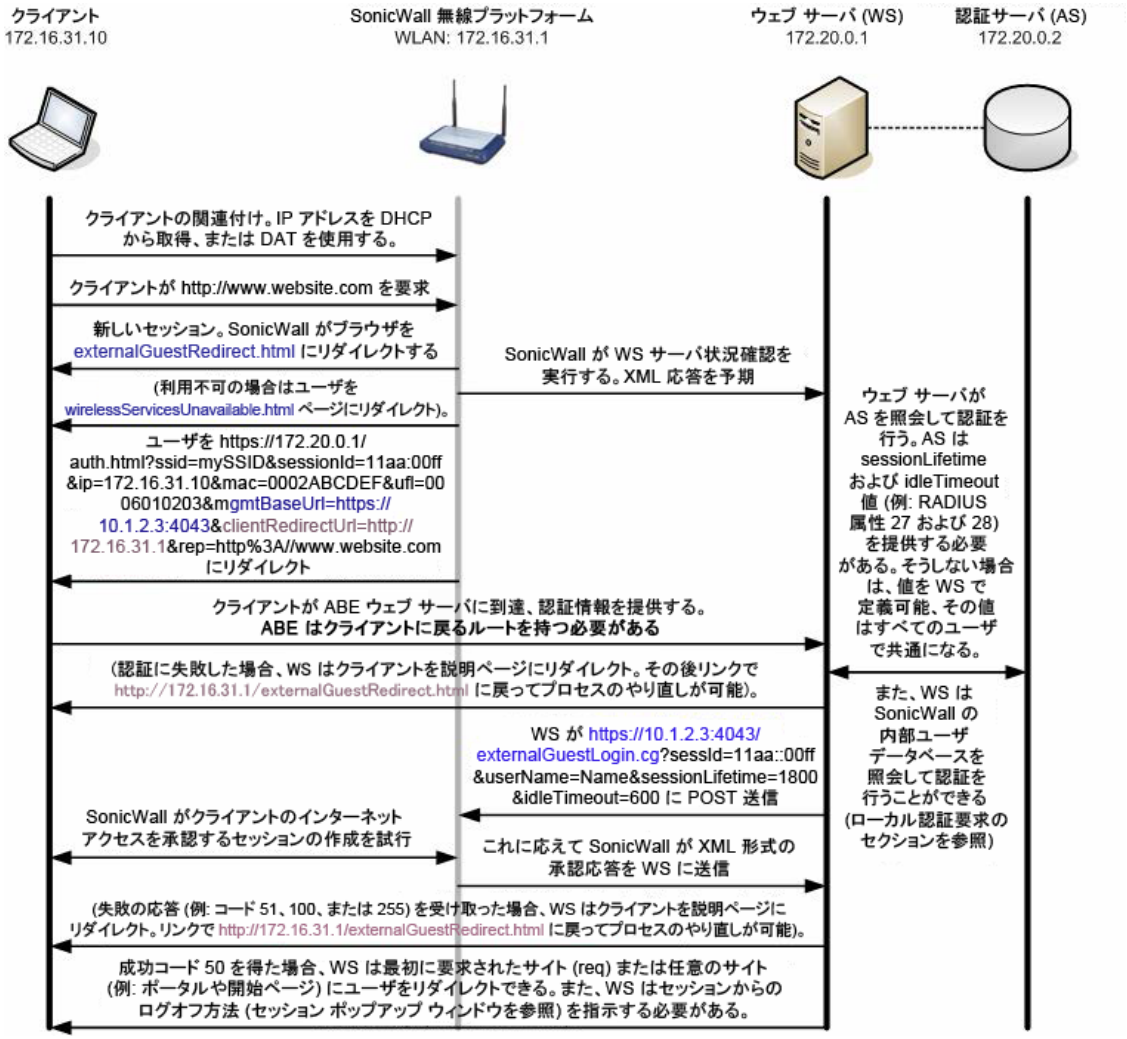
以降のセクションでは、セッション ライフ サイクルの各フェーズや、セッション ポップアップ ウィンドウ、ウェブ サーバ (WS) 状況チェック コンポーネントについて説明します。

- セッション作成 (838 ページ)
- セッション ポップアップ ウィンドウ (841 ページ)
- 無動作時タイムアウト (841 ページ)
- セッション タイムアウト (842 ページ)
- ユーザ ログアウト (842 ページ)
- 管理者ログアウト (オプション) (843 ページ)
- ウェブ サーバ状況確認 (844 ページ)
- セッション状態同期 (845 ページ)
- メッセージ認証 (845 ページ)
- セッション更新 (845 ページ)

セッション作成

無線クライアントがアクセスを試みたとき、SonicWall セキュリティ装置にそのクライアントに関して MAC アドレスに基づくアクティブなセッション情報が存在しないと、セッションの作成が行われます。

セッション作成フロー



1 無線クライアントが SonicWall との関連付けを行います。内部 DHCP サーバから IP アドレスを取得するか、動的アドレス変換 (DAT) による静的アドレス指定を使用します。

2 クライアントがウェブリソース `http://www.website.com` を要求します。

- SonicWall セキュリティ装置は、これが新しいセッションであることを確認します。

3 SonicWall セキュリティ装置は、内部でホストしている `externalGuestRedirect.html` ページにクライアントをリダイレクトします。`externalGuestRedirect.html` ページは、セッションが認証のためにリダイレクトされていることを説明する、管理者が設定できるテキストを提供します。

4 このリダイレクトの際、セキュリティ装置は、設定されているターゲットのリダイレクトページへ JavaScript でリダイレクトを試みることにより ABE の可用性をチェックします。

- WS へのリダイレクト失敗が指定された期間 (SonicWall で設定可能な 1 ～ 30 秒の値) 内に発生した場合、セキュリティ装置 はセッションを内部の `wirelessServicesUnavailable.html` ページにリダイレクトします。

5 SonicWall からは、JavaScript による可用性チェックに加えて、オプションの完全なウェブ サーバ状況確認も使用可能です (「ウェブ サーバ状況確認 (844 ページ)」を参照してください)。このオプションは、1 ～ 60 分の範囲で設定可能な間隔で実行されるように設定できます。エラー応

答コード 1、2、または 255 が生成された場合、セキュリティ装置はその応答をログに記録し、ブラウザを内部の `wirelessServicesUnavailable.html` ページにリダイレクトします。このページは、リソースについて説明する、管理者が設定できるテキストを提供します。

6 使用可能な場合、セキュリティ装置は AS にホストされている次の認証ポータルにクライアントをリダイレクトします。
`https://172.20.0.1/auth.html?ssid=mySSID&sessionId=11aa::00ff&ip=172.16.31.10&mac=0002ABCDEF&ufi=0006010203&mgmtBaseUrl=https://10.1.2.3:4043&clientRedirectUrl=http://172.16.31.1&req=http%3A//www.website.com`

- *ssid* - リダイレクトされるクライアントが関連付けられていた無線ネットワークの ESSID (無線ネットワーク名) です。
- *sessionId* - SonicWall によって生成された 16 バイト MD5 ハッシュ値の 32 バイト 16 進数表現であり、クライアントのインデックス付けのために SonicWall と WS によって使用されます (`11aa3e2f5da3e12ef978ba120d2300ff` など)。
- *ip* - クライアントの IP アドレスです。
- *mac* - クライアントの MAC アドレスです。
- *req* - 当初要求されていたウェブ サイトは、引数として認証サーバに渡されます。
- *ufi* - SonicWallファイアウォール識別子。必要に応じて、サイト識別のために使用されます。
- *mgmtBaseUrl* - IP がその後に通信する SonicWall のプロトコル、IP アドレス、ポートです。
- *clientRedirectUrl* - ABE がクライアントのリダイレクトで使用する SonicWall のプロトコル、IP アドレス (およびオプションのポート) です。
- *req* - 当初要求されていたクライアントの URL、エンコードされた URL (存在する場合) です。

7 クライアントは認証情報 (ユーザ名、パスワード、トークンなど) を提供します。

> **メモ：** WS は VPN、NAT、またはルートによってクライアントに到達可能である必要があります。

8 WS は AS に照会してユーザの検証を行います。

- AS はセッション特有の情報 (具体的には、セッション タイムアウト、無動作時タイムアウト) を提供します。
- セッション特有の値は、必要に応じて、AS から取得せずに WS によってグローバルに適用できます。一部の値はセキュリティ装置に渡すだけで済みます。
- タイムアウト値は、秒単位で表されており、1 ～ 863,913,600 (9999 日に相当) の範囲の値をとることができます。

9 認証に失敗した場合、WS はそのエラーについて説明するページにクライアントをリダイレクトする必要があります。プロセスを再起動するために `http(s)://172.16.31.1/externalGuestRedirect.html` に戻るリンクを提供する必要があります。

10 成功した場合、WS は HTTPS 経由または VPN 経由でセキュリティ装置に接続し、`https://10.1.2.3:4043/externalGuestLogin.cgi?sessId=11aa::00ff&userName=Name&sessionLifetime=1800&idleTimeout=600` に POST 送信します。

- セキュリティ装置は、セッションの作成を試み、結果を WS に同じ接続で送信します。結果については、「メッセージ形式 (846 ページ)」を参照してください。

11 エラー応答 (コード 51、100、255 など) を受け取った場合、WS はそのエラーについて説明するページにクライアントをリダイレクトする必要があります。プロセスをやり直すために `http(s)://172.16.31.1/externalGuestRedirect.html` に戻るリンクを提供できます。

12 成功した場合 (コード 50)、WS は当初要求されていたサイト (`req`) または任意のサイト (ポータルまたは開始ページ) にユーザをリダイレクトできます。また、WS はセッションからのログオフ方法 (ページのブックマーク登録、ポップアップ ウィンドウ、URL など) を指示する必要があります。

セッション ポップアップ ウィンドウ

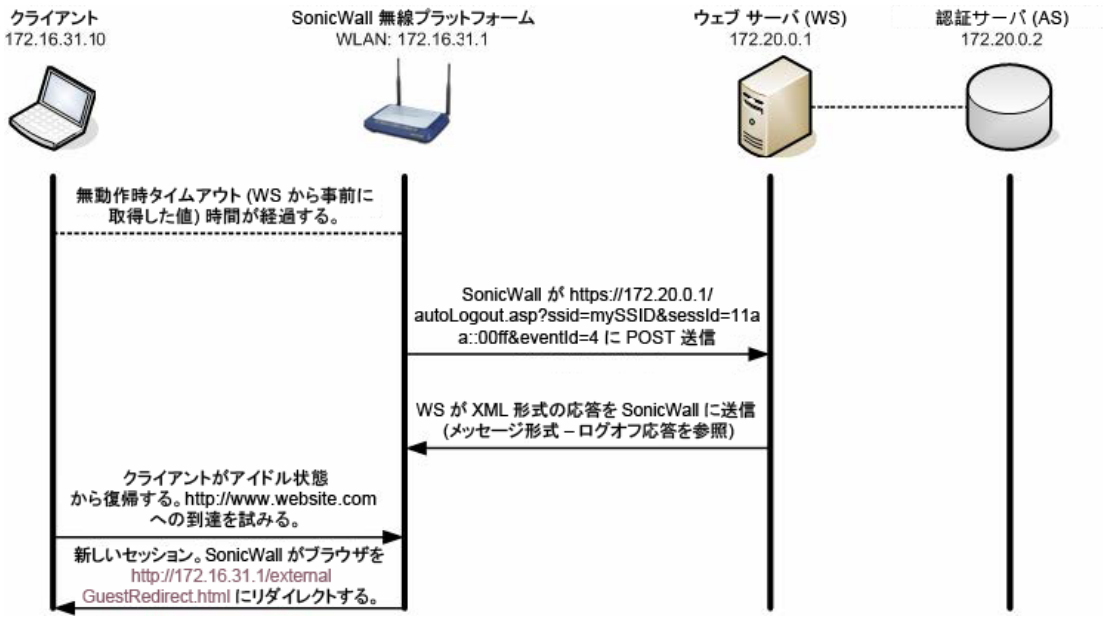
セッションはセッション ポップアップ ウィンドウによって管理することをお勧めします。これは、セッション作成の時点でインスタンス化されたブラウザ ウィンドウであって、セッション時間の情報 (存続時間、無動作時タイムアウト、タイマー カウントダウンなど) と「**ログアウト**」ボタンを提供するものである必要があります。サンプル コードが提供されています。

- 「**ログアウト**」を選択すると、セッションは終了し、ユーザ ログアウト イベントがトリガーされます。
- このウィンドウを閉じようとした際には、ウィンドウを閉じるとセッションが終了するという警告メッセージを表示する必要があります。
- ウィンドウを閉じるとセッションは終了し、ユーザ ログアウト イベントがトリガーされます。

無動作時タイムアウト

無動作時タイムアウトは (「セッション作成 (838 ページ)」の「ステップ 8」で指定した) 無動作時タイムアウト時間が経過すると発生します。

無動作時タイムアウト フロー



1 アイドル タイマー (「セッション作成 (838 ページ)」で設定したもの) が時間超過になります。

2 この時点でクライアントのブラウザが開かれていない場合があるため、このプロセスがリダイレクトによって開始されることはありません。代わりに、SonicWall は WS (`https://172.20.0.1/autoLogout.asp?ssid=mySSID&sessId=11aa::00ff&eventId=4`) への POST 送信を行います (ログオフ イベント ID については、「メッセージ形式 (846 ページ)」を参照してください)。

- PPOST 送信先のリソースは、セキュリティ装置上の「**管理 | システム セットアップ | ネットワーク > ゾーン**」から設定できます。WLAN ゾーンを編集します (「**ゾーンの編集**」ダイアログ: 「**ゲスト サービス > 外部ゲスト認証 > 詳細設定 > セッション自動ログアウト > ログアウト CGI**」)。
- WS によってホストされているページは、*sessId* と *eventId* の値を予期および解釈する必要があります。

3 WS は、XML による結果を WS に同じ接続で送信します。結果については、「ログオフ応答 (848 ページ)」を参照してください。

4 クライアントがアイドル状態から復帰してウェブ リソースへの到達を試みた場合、セキュリティ装置はユーザを内部の `externalGuestRedirect.html` ページにリダイレクトし、セッション作成処理をやり直します (「セッション作成 (838 ページ)」を参照してください)。

メモ：リソースを節約するために、無動作時タイムアウトは最大値である 10 分に設定することをお勧めします。

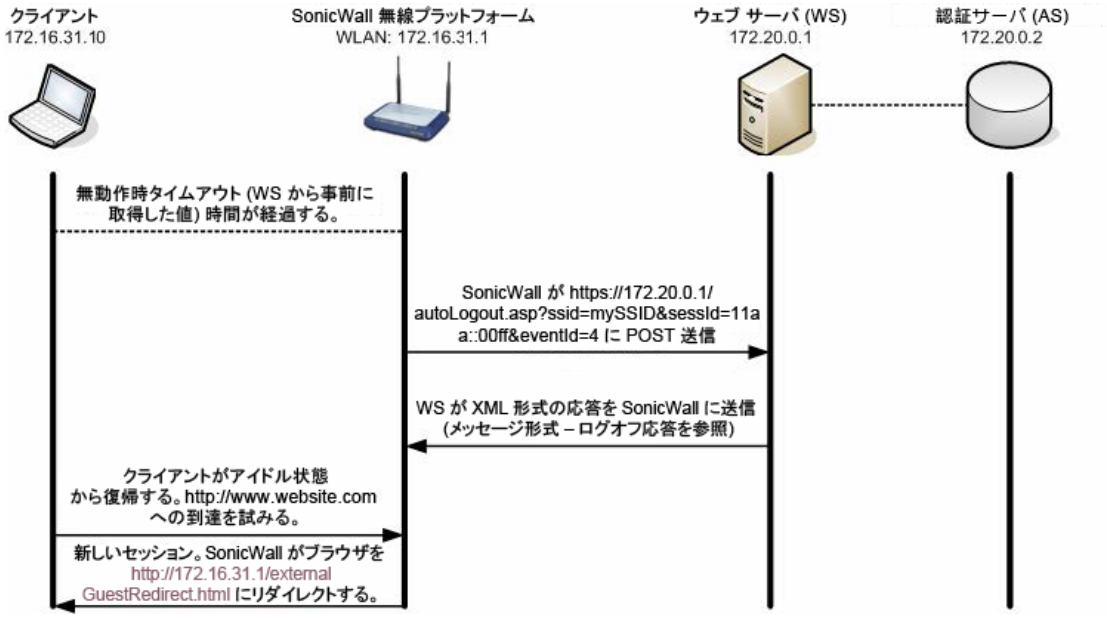
セッション タイムアウト

このイベントはセッションの存続期間を超過した場合に発生します。*eventId* 値がセッション タイムアウトでは 3、無動作時タイムアウトでは 4 である点を除き、交換は上記の無動作時タイムアウトと同じです。

ユーザ ログアウト

ユーザがセッション ポップアップ ウィンドウを閉じるか、セッション ポップアップ ウィンドウに用意されている「**ログアウト**」を使用して、自発的にセッションを終了すると、イベントが発生します。セッション ポップアップ ウィンドウは、ユーザ ログアウトのための好ましい方法ですが、この方法がなくても、セッションの存続期間の超過を許可することで同じ結果を得ることができます。後者の方法では、セッション ポップアップ ウィンドウに対する依存関係がなくなりますが、リソース管理の効率が低下します。

ユーザ ログアウト フロー



1 クライアントが「**ログアウト**」を使用してログアウトするか、セッション ポップアップ ウィンドウを閉じます。

2 WS が POST を `https://10.1.2.3:4043/externalGuestLogoff.cgi?sessId=11aa::00ff&eventId=1` に送信します (ログオフ イベント ID については、「メッセージ形式 (846 ページ)」を参照してください)。

- `sessId` - セッション作成時 (「セッション作成 (838 ページ)」を参照) にセキュリティ装置よって生成される値であり、クライアントのインデックス付けのためにセキュリティ装置および WS によって使用されます。
- `eventId` - ログオフ要求イベントを示します。

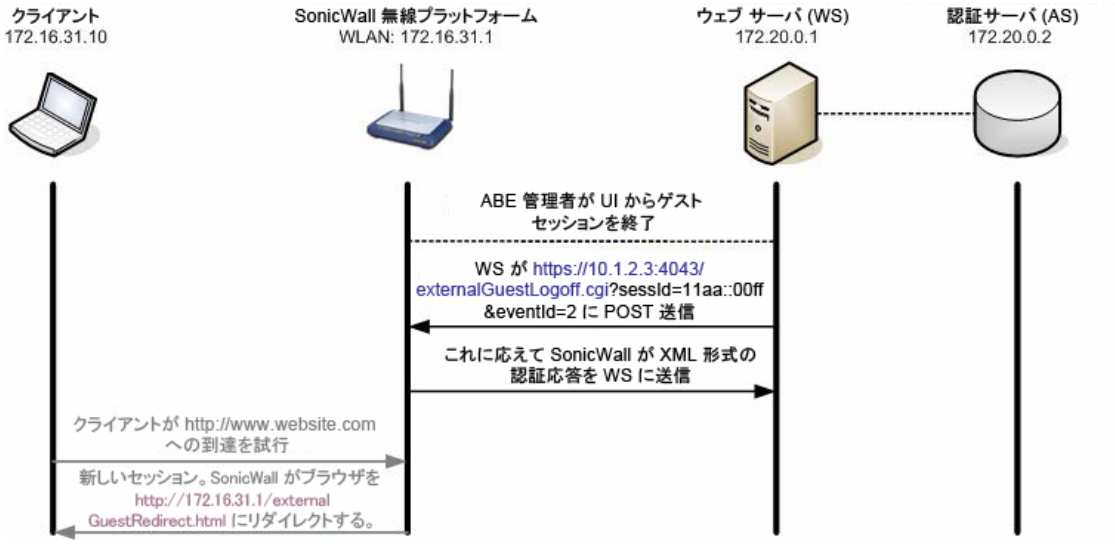
3 SonicWall セキュリティ装置は同じ接続を使用して結果を WS へ返します。結果については、「ログオフ応答 (848 ページ)」を参照してください。

4 クライアントがウェブ リソースへの到達を試みた場合、セキュリティ装置はユーザを内部の `http://172.16.31.1/externalGuestRedirect.html` ページにリダイレクトし、セッション作成処理をやり直します (「セッション作成 (838 ページ)」を参照してください)。

管理者ログアウト (オプション)

このイベントは、ABE 管理者がゲスト セッションからのログアウトを管理インターフェースから行った場合に発生します。現時点では、ABE によって確立されたゲスト セッションの終了を SonicOS 管理インターフェース単体で行うことはできません。ABE によって確立されたゲスト セッションは、SonicOS 管理インターフェースでそのように (または内部の WGS ゲスト セッションとは区別して) 表され、編集できません。

管理者ログアウト フロー



1 ABE 管理者が管理インターフェースからゲスト セッションを終了します。

2 WS がセキュリティ装置に POST を送信します: `https://10.1.2.3:4043/externalGuestLogoff.cgi?sessId=11aa::00ff&eventId=2`.に送信します (ログオフ イベント ID については、「メッセージ形式 (846 ページ)」を参照してください)。

- `sessId` - セッション作成時にセキュリティ装置によって生成される値であり、クライアントのインデックス付けのためにセキュリティ装置および WS によって使用されます。
- `eventId` - ログオフ要求イベントを示します。

3 SonicWall は結果を WS に同じ接続で送信します。結果については、「ログオフ応答 (848 ページ)」を参照してください。

4 クライアントがアイドル状態から復帰してウェブ リソースへの到達を試みた場合、セキュリティ装置はユーザを内部の `http://172.16.31.1/externalGuestRedirect.html` ページにリダイレクトし、セッション作成処理をやり直します (「セッション作成 (838 ページ)」を参照)。

ウェブ サーバ状況確認

単純なウェブ サーバ (WS) 可用性 (「セッション作成フロー (839 ページ)」の必須の「ステップ 4」で提供される、JavaScript によるリダイレクト) よりも粒度の細かい ABE 状況を提供する場合、SonicWall はサーバ運用状態を確認するために、保護された HTTP GET 操作を必要に応じて送信できます。ターゲット URL は設定可能であり、クエリの間隔も設定可能 (1 ～ 60 分) です。WS はサーバの現在の状態がリストされている XML 形式で応答を返します。詳細については、「メッセージ形式 (846 ページ)」を参照してください。

エラー応答コード (1、2、または 255) を受け取った場合 (WS そのものは利用可能であるがその他の ABE エラー状況が発生していることを示します)、SonicWall はこの応答をログに記録し、その後のすべての認証要求を内部の `wirelessServicesUnavailable.html` ページにリダイレクトします。このページは、リソースについて説明する、管理者が設定できるテキストを提供します。

セキュリティ装置は ABE への問い合わせ試行を設定されている間隔で継続し、応答コード 0 (サーバ稼働中) を受け取ると、(`wirelessServicesUnavailable.html` ページではなく) WS へのリダイレクトを再開します。

セッション状態同期

セキュリティ装置は、設定可能な間隔 (1 ～ 60 分) で、現在動作しているゲスト セッションすべての XML リストが含まれている保護された HTTP POST 操作を必要に応じて WS に送信します。CGI ポストは sessionList を動作しているゲスト セッションすべての XML リストとして提供します。詳細については、「メッセージ形式 (846 ページ)」を参照してください。

この機能そのものはセキュリティ装置上のチェックボックスによって有効化されますが、既定では無効になっています。ターゲット URL は設定可能です。

メッセージ認証

この機能により、セキュリティ装置と ABE の両者間で交換される CGI データが SonicWall セキュリティ装置/ABE デバイスから生成されたものであること、また改変されていないことが確認されます。有効になっている場合、hmac という追加の CGI パラメータが、交換されるすべての CGI データに追加されます。以下に、メッセージ認証が有効になっている場合のリダイレクト URL がどのように表示されるかの例を示します。

```
https://10.1.2.3/login.asp?sessionId=faad7f12ac26d5c2fe3236de2c149a22&ip=172.16.31.2&mac=00:90:4b:6a:37:32&ufi=0006B1020148&mgmtBaseUrl=https://10.0.61.222:4043/&clientRedirectUrl=http://192.168.168.168:80/&req=http%3A//www.google.com/&hmac=cd2399aeff26d5c2fe3236d211549acc
```

メモ：SonicWall セキュリティ装置 URL は、req 変数 (および req のみ) の値の範囲内で次の文字をエンコードします。

```
% = %25
: = %3A
= %20 (space)
? = %3F
+ = %2B
& = %26
= = %3D
```

先ほどの例では、HMAC シグネチャが次のデータを使用して生成されていました。

```
HMAC (
   faad7f12ac26d5c2fe3236de2c149a22 +
   172.16.31.2 +
   00:90:4b:6a:37:32 +
   0006B1020148 +
   https://10.0.61.222:4043/ +
   https://10.0.61.222:4043/ +
   http%3A//www.google.com/
)
```

メッセージ認証が有効になっている場合は、SonicWall デバイスが ABE に起因している CGI ポストデータの一部として HMAC シグネチャを予期しています。HMAC が見当たらないか正しくないことを SonicWall が検出した場合は、エラー コード 251 が返され、要求された操作 (ゲスト ログイン、アカウント作成など) は中断されます。

セッション更新

セッション更新を使用すると、セキュリティ装置 での既存セッションのセッション存続期間と無動作時タイムアウトの値を ABE が更新できます。これにより、例えば、ゲスト ユーザが追加の時間を購入したり、既存のセッションに時間を追加したりできます。

- セッション更新は、セッションの存続期間中の任意の時点で ABE から SonicWall に送信できます。
- *userName* および *sessionLifetime* の値は、メッセージ内に指定する必要があります。
- *sessID* 値を指定できます。これが含まれている場合、更新は指定されたセッションに関連したものになります。省略された場合、更新は指定された *userName* に一致するすべてのセッションに関連したものになります。

詳細については、「メッセージ形式 (846 ページ)」を参照してください。

メッセージ形式

トピック:

- 外部認証要求 (846 ページ)
- ローカル認証要求 (847 ページ)
- ローカル認証要求 (847 ページ)
- ローカル認証応答 (847 ページ)
- ログオフ要求 (848 ページ)
- ログオフ応答 (848 ページ)
- ウェブ サーバ状況確認 (844 ページ)
- セッション状態同期 (845 ページ)
- セッション状態同期応答 (850 ページ)
- ローカル アカウント作成要求 (850 ページ)
- ローカル アカウント作成応答 (851 ページ)
- 更新セッション要求 (851 ページ)
- 更新セッション応答 (852 ページ)

メモ：XML スキーマの場所は変更される場合があります。
SonicWall セキュリティ装置の IP アドレスとポートは *mgmtBaseUrl* 変数で定義されています。

外部認証要求

WS は保護された HTTP POST 操作を `https://SonicWall.ip.add.ress:port/externalGuestLogin.cgi` に送信します。ポストパラメータには以下の引数が含まれます。

- *sessId*: セッション ID
- *userName*: 完全なユーザ ID
- *sessionLifetime*: ユーザのセッション存続期間 (秒単位)
- *idleTimeout*: 最大の無動作時タイムアウト (秒単位)

外部認証応答

セキュリティ装置は次の形式の XML 応答を返します。

```
<?xml version="1.0" encoding="UTF-8">
<SonicWallAccessGatewayParam
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="http://www.SonicWall.com/
   SonicWallAccessGatewayParam.xsd">
   <AuthenticationReply>
      <ResponseCode>{ 応答コード }</ResponseCode>
      <ReplyMessage>{ 応答メッセージ }</ReplyMessage>
   </AuthenticationReply>
</SonicWallAccessGatewayParam>
```

{応答コード} には、「外部認証応答コード」テーブルにリストされている値のいずれかが含まれます。

外部認証応答コード

応答コード	応答の意味
50	ログインに成功
51	セッションの制限を超過
100	ログインに失敗 - アクセス拒否
251	メッセージ認証に失敗 - 不正な HMAC
253	セッション ID が不正
254	CGI パラメータが不正または見当たらない
255	Internal error 【PKI 障害: 内部エラー】

ローカル認証要求

WS は保護された HTTP POST 操作を `https://SonicWall.ip.add.ress:port/localGuestLogin.cgi` に送信します。ポスト パラメータには以下の引数が含まれます。

- *sessId*: セッション ID
- *userName*: 完全なユーザ ID
- *passwd*: ゲストの平文パスワード

ローカル認証応答

SonicWall は次の形式の XML 応答を返します。

```
<?xml version="1.0" encoding="UTF-8">
<SonicWallAccessGatewayParam
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="http://www.SonicWall.com/
   SonicWallAccessGatewayParam.xsd">
   <AuthenticationReply>
      <ResponseCode>{ 応答コード }</ResponseCode>
      <ReplyMessage>{ 応答メッセージ }</ReplyMessage>
   </AuthenticationReply>
</SonicWallAccessGatewayParam>
```

{応答コード} には、「ローカル認証応答コード」テーブルにリストされている値のいずれかが含まれます。

ローカル認証応答コード

応答コード	応答の意味
50	ログインに成功
51	セッションの制限を超過
52	不正なユーザ名/パスワード
100	ログインに失敗 - アクセス拒否
251	メッセージ認証に失敗 - 不正な HMAC
253	セッション ID が不正
254	CGI パラメータが不正または見当たらない
255	内部エラー

ログオフ要求

WS は保護された HTTP POST 操作を `https://SonicWall.ip.add.ress:port/externalGuestLogoff.cgi` に送信します。ポストパラメータには次の引数が含まれます。

- *sessId*: GW セッション ID
- *eventId*: ログオフ イベント ID。次のいずれかである必要があります。

ログオフ イベント ID	イベントの意味
1	ゲストが手動でログアウトした
2	管理者が指定されたゲストをログオフした
3	ゲスト セッションが期限切れになった
4	ゲストの無動作時タイムアウト時間超過

ログオフ応答

セキュリティ装置は次の形式の XML 応答を返します。

```
<?xml version="1.0" encoding="UTF-8">
<SonicWallAccessGatewayParam
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="http://www.SonicWall.com/
   SonicWallAccessGatewayParam.xsd">
   <LogoffReply>
        <ResponseCode>{応答コード}</ResponseCode>
        <ReplyMessage>{応答メッセージ}</ReplyMessage>
   </LogoffReply>
</SonicWallAccessGatewayParam>
```

{応答コード} には、「ログオフ応答コード」テーブルにリストされている値のいずれかが含まれます。

ログオフ応答コード

応答コード	応答の意味
150	ログオフに成功
251	メッセージ認証に失敗 - 不正な HMAC
253	セッション ID が不正
254	CGI パラメータが不正または見当たらない
255	Internal error 【PKI 障害: 内部エラー】

ウェブ サーバ状況確認

WS は XML 応答を次の形式で返します。

```
<?xml version="1.0" encoding="UTF-8">
<SonicWallAccessGatewayParam
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="http://www.SonicWall.com/
   SonicWallAccessGatewayParam.xsd">
   <ServerStatus >{ 状況コード }</ ServerStatus >
</SonicWallAccessGatewayParam>
```

{応答コード} には、「ウェブ サーバ状況確認応答コード」テーブルにリストされている値のいずれかが含まれます。

ウェブ サーバ状況確認応答コード

応答コード	応答の意味
0	サーバ稼働中
1	データベース休止中
2	設定エラー
255	Internal error 【PKI 障害: 内部エラー】

セッション状態同期

GW は、現在動作しているゲスト セッションすべての XML リストが含まれている保護された HTTP POST 操作を定期的に AS に送信します。ターゲット URL と期間はどちらも GW 管理者によって設定可能です。

CGI ポスト パラメータには次の引数が含まれます。

- *sessionList*: 動作している GW ゲスト セッションすべての XML リストです。

このセッション リストは XML 応答を次の形式で返します。

```
<?xml version="1.0" encoding="UTF-8">
<SonicWallAccessGatewayParam
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="http://www.SonicWall.com/
   SonicWallAccessGatewayParam.xsd">
   <SessionSync>
      <SessionCount>{ セッション回数 }</SessionCount>
      <SessionList>
      <Session>
```

```
        <Ssid>{ESSID}</Ssid>8
        <ID>{ セッション ID}</ID>
        <UserName>{ ユーザ名 }</UserName>
        <IP>{IP アドレス }</IP>
        <MAC>{MAC アドレス }</MAC>
        <Idle>
        { 無動作時間 （秒単位で表記 ）}
        </Idle>
        <SessionRemaining>
        { セッション残り時間 （秒単位で表記 ）}
        <SessionRemaining>
        <BaseMgmtUrl>
        {https://ip.add.re.ss:port}
        </BaseMgmtUrl>
        <RxBytes>
        { 合計受信バイト数 }
        </RxBytes>
        <TxBytes>
        { 合計送信バイト数 }
        </TxBytes>
        </Session>
    </SessionList>
</SessionSync>
</SonicWallAccessGatewayParam>
```

セッション状態同期応答

WS は XML 応答を次の形式で返します。

```
<?xml version="1.0" encoding="UTF-8">
<SonicWallAccessGatewayParam
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="http://www.SonicWall.com/
   SonicWallAccessGatewayParam.xsd">
   <SessionSync>
      <ResponseCode>{ 応答コード }</ResponseCode>
   </SessionSync>
</SonicWallAccessGatewayParam>
```

{応答コード} には、「セッション状態同期応答の応答コード」テーブルにリストされている値のいずれかが含まれます。

セッション状態同期応答の応答コード

応答コード	応答の意味
200	同期成功
201	同期失敗
255	Internal error 【PKI 障害: 内部エラー】

ローカル アカウント作成要求

WS は保護された HTTP POST 操作を `https://SonicWall.ip.add.ress:port/createGuestAccount.cgi` に送信します。ポスト パラメータには以下の引数が含まれます。

- *userName*: 完全なユーザ ID (最大長: 32)
- *passwd*: ゲストの平文パスワード (最大長: 64)
- *コメント*: オプション (最大長: 16)。Default=**NULL**
- *enforceUniqueLogin*: 必要に応じて、1=true (真)、0=false (偽)。Default=**1**
- *activateNow*: 必要に応じて、1=true (真)、0=false (偽)。Default=**0**
- *autoPrune*: 必要に応じて、1=true (真)、0=false (偽)。Default=**1**
- *accountLifetime*: ユーザのアカウント存続期間 (秒単位で表記)
- *sessionLifetime*: ユーザのセッション存続期間 (秒単位で表記)
- *idleTimeout*: 最大の無動作時タイムアウト (秒単位で表記)

ローカル アカウント作成応答

セキュリティ装置は次の形式の XML 応答を返します。

```
<?xml version="1.0" encoding="UTF-8">
<SonicWallAccessGatewayParam
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="http://www.SonicWall.com/
   SonicWallAccessGatewayParam.xsd">
   <AccountCreationReply>
      <ResponseCode>{ 応答コード }</ResponseCode>
      <ReplyMessage>{ 応答メッセージ }</ReplyMessage>
   </AccountCreationReply>
</SonicWallAccessGatewayParam>
```

{応答コード} には、「ローカル アカウント作成応答の応答コード」テーブルにリストされている値のいずれかが含まれます。

ローカル アカウント作成応答の応答コード

応答コード	応答の意味
10	アカウント作成に成功
11	最大アカウント制限
12	アカウントが存在
251	メッセージ認証に失敗 - 不正な HMAC
254	CGI パラメータが不正または見当たらない
255	Internal error 【PKI 障害: 内部エラー】

更新セッション要求

ABE からの POST は externalGuestUpdateSession.cgi でセキュリティ装置に対して次の形式で作成される可能性があります。

```
https://10.1.2.3:4043/externalGuestUpdateSession.cgi?sessId=11aa::00ff&userName=gue
st&sessionLifetime=600&idleTimeout=180
```

ポスト パラメータには以下の引数が含まれます。

- *sessID*: 値を指定できます。値が指定されない場合は、指定されたユーザ名に一致するすべてのゲスト セッションが更新されます。
- *userName*: 値を指定する必要があります。これは、更新されるユーザ セッション (セッション ID が指定されない場合は複数のセッションになる可能性があります) の名前を定義するためです。
- *sessionLifetime*: 値を指定する必要があります。これは、セッションに割り当てる秒数を定義するためです。1 ～ 863,913,600 の任意の数値を指定できます。
- *idleTimeout*: 値を指定できます。この引数は、
  - セッションに割り当てる秒数を定義します。
  - 1 ～ 863,913,600 の任意の数値をとることができます。
  - *sessionLifetime* と等しいかより小さな値でなければなりません。

  idleTimeout が指定されない場合は、セッションの既存の *idleTimeout* 値が維持されます。

更新セッション応答

セキュリティ装置は次の形式の XML 応答を返します。

```
<?xml version="1.0" encoding="UTF-8">
<SonicWallAccessGatewayParam
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="http://www.SonicWall.com/
   SonicWallAccessGatewayParam.xsd">
   <UpdateSessionReply>
      <ResponseCode>{ 応答コード }</ResponseCode>
      <ReplyMessage>{ 応答メッセージ }</ReplyMessage>
   </ UpdateSessionReply >
</SonicWallAccessGatewayParam>
```

{応答コード} には、「更新セッション応答の応答コード」テーブルにリストされている値のいずれかが含まれます。

更新セッション応答の応答コード

応答コード	応答の意味
210	セッション更新に成功
211	セッション更新に失敗
251	メッセージ認証に失敗 - 不正な HMAC
254	CGI パラメータが不正または見当たらない
255	Internal error 【PKI 障害: 内部エラー】

LHM RESTful API

SonicOS は LHM RESTful API をサポートします。

ライトウェイト ホットスポット メッセージング (LHM) は、SonicWall 無線アクセス デバイス (SOHO W、TZ シリーズ W、または 管理用 SonicWall セキュリティ装置を持つ SonicPoint など) と (ホットスポット ユーザを認証してパラメータで規定されたネットワーク アクセスを提供する) 認証バックエンド (ABE) との間で通信を行うための方法と構文を定義します。

RESTful API は、HTTP 要求を使用してデータを GET、PUT、POST、DELETE するアプリケーション プログラム インターフェース (API) です。RESTful ウェブ サービスとも呼ばれる RESTful API は REST (REpresentational State Transfer) 技術をベースとしています。これはウェブ サービスの開発でよく使われる設計スタイルと通信方法です。

よくある質問と回答 (FAQ)

トピック:

- LHM サーバ スクリプトは ASP で記述されている必要がありますか。 (853 ページ)
- これらの新しいスクリプトが ASP.NET で記述されていたのはなぜですか。 (854 ページ)
- どうすれば LHM を使用してゲスト サービスへのアクセスを有線接続のユーザに提供できますか。 (854 ページ)
- LHM を使用して、LDAP、RADIUS、ボタン、時刻、茶葉占い、調査、相対気圧、パスコードなどを認証子として用いたアクセスを実現できますか。 (854 ページ)
- SonicWall はそうした処理を行うスクリプトを私のために記述してくれますか。 (855 ページ)
- SonicWall によって提供されたサンプル スクリプトを使用したいと考えています。使用するためには何が必要ですか。 (855 ページ)
- LHM サーバはどこに配置できますか。 (856 ページ)
- ゲスト クライアントが LHM サーバに到達できなかったり、LHM サーバ上のページを読み込めなかったりするのはなぜですか。 (856 ページ)
- SonicWall と LHM サーバとの間の LHM 交換はどのように機能しますか (簡略版、通常の環境の場合)。 (856 ページ)
- すべての LHM 設定にはどんな意味があるのですか。どのように設定すればよいですか。 (857 ページ)
- LHM 管理ポートを既定の TCP 4043 から変更できますか。 (859 ページ)
- HMAC オプションを使用する必要がありますか。このオプションを使用したい場合、どのように使用すればよいですか。 (859 ページ)
- SonicWall はこれらのスクリプトに対するサポートを提供していますか。 (860 ページ)
- 新しいスクリプトの作成、御社のスクリプトの大きな拡張、または御社のスクリプトを動作させる方法の大幅な改良を行いました。SonicWall はこれらに関心がありますか。 (860 ページ)
- LHM スクリプト ライブラリ (860 ページ)

LHM サーバ スクリプトは ASP で記述されている必要がありますか。

いいえ。LHM サーバ スクリプトは、LHM の 2 つのコア要素であるウェブ要求と XML を処理できる任意のプラットフォームを使用して、記述できます。これには Perl、PHP、ASP、ASP.NET、J2EE が含まれます。

これらの新しいスクリプトが ASP.NET で記述されていたのはなぜですか。

新しいスクリプトで ASP.NET が選ばれた理由は、普及率が高く、多くの処理が適切に行われること、さらには XML の処理が容易になることにあります。

どうすれば LHM を使用してゲスト サービスへのアクセスを有線接続のユーザに提供できますか。

ゲスト サービス (以前の WGS、つまり無線ゲスト サービス) は、無線 (ホットスポット) ユーザのために設計されたものですが、有線インターフェース (PortShield 機能を持つ PRO 1260 の場合は複数のインターフェース) を SonicPoint 強制が無効になっている無線ゾーンに配置することで、有線ユーザのために利用することもできます。その場合、すべてのゲスト サービス オプション (とりわけ、LHM、動的アドレス変換、通信を許可/拒否するネットワーク) が有線ユーザに適用されます。

認証と承認の違いは何ですか。

*認証*は、ユーザがある種のチャレンジ (質問) に対して応答するプロセスを指します。質問は何に関するものであっても構いませんが、伝統的に `username:password` (ユーザ名とパスワード) が使用されます。LHM は、認証を抽象化することでこうした従来モデルの依存関係を壊します。認証者の役割は LHM によって果たされ、認証の方法を制限する要因は想像力のみです。以下の認証方法を考えます。

- 有効なユーザ名とパスワードを提供する
- コンピュータが生成した数を推測する
- このアンケートへの回答を完了する
- クイズで 80% 以上の正解率を達成する
- 「**承諾します**」を選択します。

認証後は、クライアントが何らかの処理を行うことを承認できます。

*承認*は、何かに対するアクセス権を付与するプロセスです。承認を有用なものにするには、クライアントによる保護されたリソースへのアクセスを止めることができる手段を承認者が持つ必要があります。LHM の場合は、承認者の役割をきわめて有効に果たすことができるように、SonicWall がクライアントの (有線または無線) ゲートウェイになっています。あるクライアントについて認証者から OK を受け取った後、SonicWall はゲスト サービス セッションを作成し、そのクライアントにインターネットへのアクセスを許可します。

LHM を使用して、LDAP、RADIUS、ボタン、時刻、茶葉占い、調査、相対気圧、パスコードなどを認証子として用いたアクセスを実現できますか。

はい。

SonicWall はそうした処理を行うスクリプトを私のために記述してくれますか。

当社では、例として一連のサンプル スクリプトを提供しており、お客様はこれらを自由に変更できますが、カスタム スクリプトの提供は行っていません。ただし、カスタム スクリプトを提供できる人物を紹介することは可能です。こうしたサービスを提供できる社員によるウェブ開発チームを持つ SonicWall パートナーは少なくありません。

SonicWall によって提供されたサンプル スクリプトを使用したいと考えています。使用するためには何が必要ですか。

以下が必要になります。

- IIS 5.0 以降を実行していて最新のサービス パックおよびホットフィックスが適用されている Microsoft Windows 2000、XP、2003 プラットフォーム。
- Microsoft .NET Framework 1.1 (以降): http://www.microsoft.com/downloads/details.aspx?FamilyId=262D25E3-F589-4842-8157-034D1E7CF3A3&displaylang=en
- 最新の .NET Framework サービス パック: http://www.microsoft.com/downloads/details.aspx?familyid=A8F5654F-088E-40B2-BBDB-A83353618B38&displaylang=en

スクリプトを使用するには、以下の手順に従います。

1 使用したい LHM スクリプト (複数可) を `wwwroot` ディレクトリ (通常は `C:\inetpub\wwwroot` にあります) にコピーします。

2 外部ゲスト認証を使用するように SonicWall 上のゲスト サービスを設定します (「すべての LHM 設定にはどんな意味があるのですか。どのように設定すればよいですか。 (857 ページ)」を参照してください)。

一部のスクリプト (特にデータベースを使用するもの) は書き込み権限を必要とします。設定によっては、2 人または 3 人の "ユーザ" が、書き込みを必要とするスクリプト ディレクトリに対する書き込みアクセス権を持っている必要があります。

- 最初のアカウント (すべてのプラットフォーム) は **IUSR_MACHINENAME** です (ここで *machinename* はローカル マシンの名前です)。
- 2 番目のアカウントは次のとおりです。
  - Windows XP の場合: **ASPNET** (ASP.NET マシン アカウント)。
  - その他のプラットフォームの場合: **IWAM_MACHINENAME** (ここで *machinename* はローカル マシンの名前です)。
- これらの権限を割り当てた後も、データベースの読み取り / 書き込みアクセスの失敗が続く場合は、**NETWORK SERVICE** アカウントに対する読み取り/書き込み権限の追加が必要である可能性があります。

ⓘ **メモ：** 1.1 よりも前のバージョンの .NET Framework にはドメイン コントローラ上でのユーザ権限の問題がありました (http://support.microsoft.com/default.aspx?scid=kb;en-us;Q315158)。1.1 (またはそれ以降) をインストールすることを強く推奨します。

3 環境を設定した後は、スクリプトをカスタマイズする必要があります。この作業は、`myvars.aspx` ファイルに興味深い設定可能ビットを配置することで、できるだけ簡単化されています。すべてのエントリに適切なコメントが付いているので、用途と構文がはっきりとわかるはずです。スクリプト自体のカスタマイズをさらに実行することもできますが、通常は不要です。

LHM サーバはどこに配置できますか。

LHM サーバは事実上、ゲスト サービスから到達可能な場所であればネットワーク内のどこにあっても構いません。複数のホットスポットについて LHM を管理できる集中型ネットワーク運用センターに配置することも、単一の SonicWall セキュリティ装置と併置することもできます。

ゲスト クライアントが LHM サーバに到達できなかったり、LHM サーバ上のページを読み込めなかったりするのはなぜですか。

ゲスト クライアントは LHM サーバと直接通信するため、SonicWall セキュリティ装置によってこの通信がプロキシされることはありません。つまり、次のことがいえます。

- ゲスト クライアントのサブネットは LHM サーバに到達可能である必要があります。
- LHM サーバはゲスト クライアントのサブネットへの到達方法 (ルート、NAT、または VPN によるもの) を知っている必要があります。
- ファイアウォール アクセス ルールはゲスト クライアントのサブネットが LHM サーバに到達できるように設定されている必要があります。

SonicWall と LHM サーバとの間の LHM 交換はどのように機能しますか (簡略版、通常の環境の場合)。

1 ゲスト クライアントは、関連付け、DHCP リースの取得、ウェブ ブラウザの起動を行います。

2 DNS は SonicWall セキュリティ装置によって許可されています。URL の FQDN は対応する IP アドレスに解決されます。

3 SonicWall セキュリティ装置は、ゲスト クライアントに認証済みのセッションがあるかどうかを確認します。

- それが新しいものである場合、SonicWall セキュリティ装置はクライアントを内部のリダイレクト ページ (「リダイレクトするまでお待ちください」) にリダイレクトします。

4 内部のリダイレクト ページは、ゲスト クライアントを LHM サーバにリダイレクトしようとします。

- 失敗した場合、クライアントは内部のサーバ ダウン (「無線インターネット アクセスは一時的に使用できません。もう一度試すにはここを選択してください」) ページにリダイレクトされます。

5 ゲスト クライアントは LHM サーバにリダイレクトされます。セキュリティ装置は、初期段階のセッションについて記述する `querystring` 情報 (`sessionID`、クライアントの MAC および IP アドレス、セキュリティ装置の LHM 管理 IP およびポート、UFI、最初に要求された URL など) をリダイレクト URL に埋め込みます。

- LHM サーバのスクリプトは `querystring` 情報を取得します。

- クライアントは LHM 開始ページを LHM サーバから直接取得します。

6 使用される認証モデル (username:password、passcode、「**承諾します**」ボタンなど) に応じて、LHM サーバはゲスト クライアントにアクセスの資格があるかどうかを決定します。

7 LHM サーバは、externalGuestLogin.cgi ページに対する設定済み管理ポート (TCP 4043 など) で SonicWall セキュリティ装置へのウェブ要求を開始します。

- LHM サーバは、sessionID (「ステップ 5」で取得したもの) の POST 送信を username (ユーザから取得したか作成したもの)、session-lifetime および idle-timeout (どちらも LHM サーバによって決定されたもの) と一緒に行います。

8 セキュリティ装置は、sessionID を検証し、セッションの作成を試みたうえで、ゲスト セッションを承認 (作成) できたかどうかが記された結果コードによってこの POST に応答します。

9 LHM サーバは、結果コードを解釈し、その結果 (Session Authorized - You may now start browsing (セッションは承認されました - これでブラウジングを開始できます)、Session creation failed - Rats (セッション作成に失敗しました - 残念)、Max sessions (最大セッション数) などをゲスト クライアントに報告します。

すべての LHM 設定にはどんな意味があるのですか。どのように設定すればよいですか。

ここでは、「ライトウェイト ホットスポット メッセージング (LHM) について (824 ページ)」に記されている完全な詳細情報を参照するのではなく、設定の意味とその方法だけを説明します。

無線 SonicOS 上での LHM 設定は「**ゾーンの編集 - WLAN**」ダイアログで行います。

トピック:

- 一般設定 (857 ページ)
- 認証ページ (858 ページ)
- ウェブ コンテンツ (858 ページ)
- 詳細 (859 ページ)

一般設定

ローカル ウェブ サーバ設定

クライアント リダイレクト プロトコル	「リダイレクトするまでお待ちください」ページによって初回の内部クライアント リダイレクトを実行する際に SonicWall セキュリティ装置によって使用されるプロトコル (HTTP または HTTPS) です。(このメッセージは「**ウェブ コンテンツ**」タブの「**リダイレクト メッセージ**」エリアで設定できます)。このステップは LHM サーバへのリダイレクトに先立って行います。

外部ウェブ サーバ設定

ウェブ サーバ プロトコル	LHM サーバ上で実行されているプロトコル (HTTP または HTTPS) です。
ウェブ サーバ ホスト	LHM サーバの IP または解決可能な FQDN です。

ウェブ サーバ ポート	LHM サーバで選択されているプロトコル向け操作の TCP ポートです。
接続タイムアウト	リダイレクト試行で LHM サーバが利用不可と見なされるまでの期間 (秒単位) です。タイムアウトした場合、クライアントには「**ウェブ コンテンツ**」タブで設定されている `Server Down` (サーバ ダウン) メッセージが提示されます。

メッセージ認証

メッセージ認証を有効にする	LHM サーバとの通信で HMAC ダイジェストおよび埋め込みクエリ文字列を使用します。これは、HTTP を使用した LHM サーバとの通信時にメッセージ改変の不安がある場合に役立ちます。オプション。
認証方法	「**MD5**」または「**SHA1**」を選択します。
事前共有鍵	ハッシュ化 MAC の事前共有鍵です。使用する場合は、LHM サーバ スクリプトでも設定する必要があります。

認証ページ

外部認証ページ

メモ：これらのページはそれぞれ LHM サーバ上の一意のページである場合も、すべてのページが状況メッセージごとに個別のイベント ハンドラを持つ同一のページである場合もあります。新たに作成したスクリプトと連携させるための例を以下に示します。

ログイン ページ	クライアントがリダイレクトされる最初のページです (`lhm/accept/default.aspx` など)。
セッション期限切れページ	セッションが期限切れになったときにクライアントがリダイレクトされるページです (`lhm/accept/default.aspx?cc=2` など)。セッションが期限切れになった後、ユーザは新しい LHM セッションを作成する必要があります。
無動作時タイムアウト ページ	無動作タイマーが時間超過になったときにクライアントがリダイレクトされるページです (`lhm/accept/default.aspx?cc=3` など)。無動作タイマーが時間超過になった後も、そのセッションの残り時間がある限り、ユーザは同じ資格情報を用いて再びログインできます。
最大セッション ページ	セッションの最大数に到達したときにクライアントがリダイレクトされるページです (`lhm/accept/default.aspx?cc=4` など)。

ウェブ コンテンツ

リダイレクト メッセージ

クライアントに (通常は 1 秒だけ) 提示される既定のメッセージまたはカスタマイズされたメッセージで、セッションが LHM サーバにリダイレクトされることを説明するものです。このインタースティシャル ページは、(LHM サーバに直接アクセスするのではなく) セキュリティ装置が LHM サーバの可用性を確認できるようにするために使用されます。

サーバ ダウン メッセージ

LHM サーバが利用不可の状態にあることをリダイレクト実行側が確認したときに、クライアントに提示される既定のメッセージまたはカスタマイズされたメッセージです。

詳細

パラメータはオプションです。

自動セッション ログアウト	セッションの (自動または手動) ログアウト時の時間増分と、そのときに SonicWall セキュリティ装置が POST 送信を行うページです。
サーバ状況確認	LHM サーバ上またはその背後にあるコンポーネント (バックエンド データベースなど) の可用性を決定するための時間増分と、そのために SonicWall が POST 送信を行うページです。
セッション同期	SonicWall がゲスト サービス セッション テーブル全体の POST 送信を行う時間増分とページです。これにより、LHM サーバは会計処理、請求、またはヒューリスティクスのためにゲスト ユーザの状態の同期をとることができます。

LHM 管理ポートを既定の TCP 4043 から変更できますか。

はい。これは、外部ゲスト認証のサービス オブジェクトのポート値を変更することにより、SonicOS で容易に行えます。

HMACオプションを使用する必要がありますか。このオプションを使用したい場合、どのように使用すればよいですか。

HMAC 機能はオプションです。この機能により、SonicWall によって LHM サーバに送信されたメッセージや LHM サーバによって SonicWall セキュリティ装置に送信されたメッセージが改変されていないことが保証されます。HMAC は、これら 2 つのピア間で受け渡しされる情報に対して (パスワードによって) 鍵がかけられたメッセージ認証コードを計算し、計算されたダイジェストをデータに追加することで、これを実現します。もう一方の側は、データを受信するとダイジェストそのものを計算し、その結果を送信された MAC と比較します。両者が一致した場合、データは改変されることなく配信されたことになります。保護されていない環境にいる場合や、セキュリティの心配がある場合は、HMAC オプションの使用を検討してください。

HMAC の使用を選択した場合は、独自の HMAC ルーチンを実装できますが、最も単純な方法は SonicWall が作成した `SonicSSL.dll` ライブラリと、OpenSSL の一部として自由に利用できる `libeay32.dll` を使用することです。どちらも、リクエストすれば SonicWall から入手できます。

HMAC を使用するには、以下の手順に従います。

1 `libeay32.dll` ファイルを LHM (IIS) サーバ上のパス (`C:\Windows\system32` フォルダなど) にコピーします。

2 `SonicSSL.dll` ファイルを同じサーバ上の任意の場所にコピーします。

3 `SonicSSL.dll` ファイルをコマンド `regsvr32 SonicSSL.dll` によって登録します。

この操作の後、LHM スクリプトでは Server.CreateObject (SonicSSL.Crypto) オブジェクトを HMAC 計算のために使用できるようになります。HMAC 機能は、「LHM スクリプト ライブラリ (860 ページ)」に記載のスクリプトに含まれています。

重要：SonicWall セキュリティ装置は querystring の req (最初に要求された URL) 部分の URL エンコード (特定の文字列の ASCII 表記から 16 進表記への変換) を行いますが、SonicWall による URL エンコードの方法は Microsoft の方法 (例えば、Request.QueryString で採用されているもの) とは若干異なります。こうした方法の違いにより、HMAC が実行される文字列がセキュリティ装置と LHM サーバの間で異なる可能性があります。提供されているスクリプトでは、querystring の req 部分を SonicWall による方法と一貫性のある形で手作業によってエンコードすることで、こうした点が補正されています。

SonicWall はこれらのスクリプトに対するサポートを提供していますか。

これらのスクリプトは、サンプルとして提供されており、SonicWall テクニカル サポートではサポートされていません。また、SonicWall サポートでも LHM バックエンド環境の設定を支援することはできません。将来の顧問サポート サービスではこうした問題に対処する可能性があります。

新しいスクリプトの作成、御社のスクリプトの大きな拡張、または御社のスクリプトを動作させる方法の大幅な改良を行いました。SonicWall はこれらに関心がありますか。

もちろんです。当社は、LHM を使用する新しい方法や、使用可能なスクリプトのライブラリに対して貢献してくれる人材を常に探しています。当社は、作成されたプラットフォームや使用している認証方法を問わず、LHM スクリプトの検討を行います。お客様のスクリプトについて説明した電子メールを products@SonicWall.com までお送りいただければ、当社のライブラリへの追加を検討いたします。スクリプトを送信していただくことにより、そのスクリプトを自由に変更および再配布できる権限が SonicWall に与えられるものとします。

LHM スクリプト ライブラリ

SonicWall LHM スクリプト ライブラリは、LHM をゲスト サービスで使用したり、そうした使用を望んだりしている人々のためのリソースとして役立つように構築されました。その目的は、だれもが変更したりそのまま使用したりできるスクリプトの大規模かつ多様で有用なコレクションを擁するまでにこのライブラリが発展するのを支援してくれる、多くの貢献者や利用者の関心を引くことにあります。

このライブラリに最初に寄贈されたのは 6 つのスクリプトです。一般的なユーザ要求 (accept、guestbook、および adauth) に応えるものと、あまり一般的でない要求 (lhmquiz、random、および paypal) に応えるものがあります。これらのスクリプトは Visual Studio .NET 開発環境の外側で作成されていたため、多様なスタイルをとることができます。ただし、以下の点はすべてのスクリプトに共通しています。

- 設定可能な変数のモジュール化 (ファイルのパス、サーバ IP アドレス、ポップアップ ログアウト ウィンドウの使用、ソルト値、タイマー設定など)。これらの設定可能な変数は、設定可能な要素の検索を行わなくても環境ごとの編集を 1 つの場所で行えるように、myvars.aspx ファイル内に集められています。
- 何が行われているかを詳細に説明する豊富なコメント。

スクリプト ディレクトリの最上位レベルにはchooser.aspx 開始ページが用意されています。このスクリプトは、SonicWall セキュリティ装置での LHM 設定を特定のスクリプトを指すように設定し直さなくても、デモ環境で下位レベルの (具体性の高い) スクリプトを選択できるように設計されています。つまり、セキュリティ装置上の LHM は、最上位レベルの chooser.aspx スクリプトを指すように設定でき、その場合はすべてのサブディレクトリ (random、accept、adauth など、より低レベルのスクリプト) が列挙されます。最上位レベルの chooser.aspx スクリプトは、ターゲットとなる下位レベルの default.aspx スクリプトを新しいウィンドウで開き、元の querystring 全体を渡します。

スクリプトのすべては default.aspx ページで開始され、クライアントのリダイレクトは必要に応じて自動的に実行されます。そのため、SonicWall での LHM 設定は適切なパスにある default.aspx ページを指している必要があります (lhm/accept/default.aspx、lhm/adauth/default.aspx など)。一部のスクリプトは別の管理機能ページを持ちます。これらについては、スクリプトの説明に注記があります。

また、各スクリプトでは logout.aspx ページも用意されています。このページの使用は、myvars の logoutPopup 変数によって制御できます。値 1 を設定すると、ポップアップ ログアウト ウィンドウの使用が有効になります。このウィンドウは、セキュリティ装置から成功の応答コード (50) を受け取った後、LHM 認証プロセスによって起動されます。スクリプトは、logout.aspx ウィンドウがセッション時間を追跡できるように sessID、mgmtBaseUrl、および sessTimer 変数をこのウィンドウに渡し、ユーザがセッションを手動で終了したい場合にはログアウト イベントを (mgmtBaseUrl にある) セキュリティ装置に POST 送信して 適切なセッション (sessID) を取得できます。

ログアウト ポップアップ ウィンドウの使用について

- ログアウト ポップアップを使用する必要はありません。セッションは、設定されている存続期間を過ぎると自然にタイムアウトします。ポップアップ ウィンドウは、ユーザに各自のセッションを手動で終了するためのメカニズムを提供しているにすぎません。
- このウィンドウは、JavaScript ポップアップによって起動されるので、ポップアップ ブロッカーによって遮断されます。
- このウィンドウを閉じてもセッションは中断されません。「**ログアウト**」のみがセッションを終了できます。
- カウントダウン タイマーはクライアント側で実行されるため、ページの再表示を防ぐための対策が講じられています。ページを再表示すると、クライアント側のカウントダウン タイマーはリセットされますが、実際のセッション タイマーへの影響はありません。F5 キーとマウス右クリックのイベントはキャプチャされて抑制されます。ただし、これはすべてのブラウザで機能するわけではありません。
- ログアウト ポップアップの使用は、スクリプト認証スキームの特性と一致している必要があります。
    - 一部のスクリプトでは、非排他的なログイン処理になっており、ユーザは繰り返しログインすることができます (Accept および ADAuth スクリプトなど)。これらの非独占的なスクリプトでのログアウト ポップアップ ウィンドウの使用は推奨されています。
    - 一部のスクリプトは、非独占的なものですが、一意性を維持すべきデータを収集します (Guestbook および LHMQuiz スクリプトなど)。これらの非独占的なスクリプトでのログアウト ポップアップの使用は許容されていますが、余分なデータの収集につながる可能性があります。
    - なかには独占的なスクリプトもあります。これは、ユーザ認証の後、何らかの費用を負担しないと認証プロセスを繰り返すことができないことを意味します (PayPal スクリプトや Random スクリプトで useDB が有効になっているものなど)。こうしたスクリプトでのログアウト ポップアップの使用は推奨されません。簡単にログインし直すための手段がユーザにはないためです。

こうしたスクリプトは、.NET の手順エラーに関する出力を非表示にする機能も備えています。これはテキストを背景の色に一致させて見えなくするものです。何らかのエラーまたはエラー条件が発生した場合は、エラー出力が提供され、ウェブページ上で Ctrl+A キーを押してすべてのテキストを選択することで、その内容を見ることができます。

以下に、各スクリプトの説明、機能、動作を示します。 新しいスクリプトがライブラリに追加された場合は、その理解、カスタマイズ、組み込みの参考になるように類似の説明が付与されます。

トピック:

- 承諾スクリプト (862 ページ)
- ADAuth スクリプト (875 ページ)
- ゲストブック スクリプト (891 ページ)
- LHMQuiz スクリプト (907 ページ)
- PayPal スクリプト (928 ページ)
- ランダム スクリプト (952 ページ)
- Chooser.aspx Script (975 ページ)

承諾スクリプト

認証モデル	ゲスト クライアントは「**承諾します**」を選択します。	
目的	規約の承諾、サービスの条件、またはようこそ画面をクライアントに提示します。	
myvars 変数	`logoutPopup`	ログアウト ポップアップ ウィンドウの使用を制御します。次のように設定します。 • **0**: ポップアップ ウィンドウを無効にします。 • **1**: ポップアップ ウィンドウを有効にします。
	`sessTimer`	秒単位のセッション タイマー。
	`idleTimer`	秒単位の無動作タイマー。
	ユーザ名	ゲスト セッションに適用されるユーザ名。このスクリプトはクライアントからユーザ名を取得しないため、次のことが可能です。 • すべてのクライアントに対してここで明示的に設定します。 • `useMAC` に設定してユーザ名を MAC アドレスに設定します。
	`strHmac`	オプションの HMAC 機能のための事前共有鍵。
	`hmacType`	HMAC 使用時に用いるダイジェスト種別: 「**MD5**」または「**SHA1**」を選択します。
	`logo`	ページ ヘッダーで使用するロゴ (画像) ファイルの名前。

セッション フロー	1 ゲスト クライアントは「**承諾します**」を選択します。 2 LHM ポスト文字列は、sessionID、ユーザ名 (MAC の既定値)、既定のセッション存続期間、および無動作存続期間で構成されます。 3 スクリプトは、セッションを承認するために SonicWall セキュリティ装置に対する LHM ポストを実行します。
追加の考慮事項	基本的な LHM 設定のみが必要です。

トピック:

- default.aspx (863 ページ)
- logout.aspx (869 ページ)
- myvars.aspx (874 ページ)

default.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWall authorizing the LHM session.
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
      As Boolean Implements ICertificatePolicy.CheckValidationResult
         Return True
   End Function
End Class

'Sample LHM redirect querystring:
'http://127.0.0.1/lhm/accept/default.aspx?sessionId=0b712fd83b9f5313db5af1cea6b1004
f&ip=10.50.165.231&mac=00:0e:35:bd:c9:37&ufi=0006b11184300&mgmtBaseUrl=https://10.5
0.165.193:4043/&clientRedirectUrl=https://10.50.165.193:444/&req=http%3A//www.googl
e.com/ig

Dim ip as String
Dim sessionId as String
Dim mac as String
Dim ufi as String
Dim mgmtBaseUrl as String
Dim clientRedirectUrl as String
Dim req as String
Dim hmac as String
Dim customCode as String
```

```
Sub Page_Load(src as Object, e as EventArgs)

   LHMResult.Text=""
   catchError.Text=""

   ip=Request.QueryString("ip")
   sessionId=Request.QueryString("sessionId")
   mac=Request.QueryString("mac")
   ufi=Request.QueryString("ufi")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
   clientRedirectUrl=Request.QueryString("clientRedirectUrl")
   req=Request.QueryString("req")
   hmac=Request.QueryString("hmac")
   customCode=Request.QueryString("cc")

   'customCode grabs the "cc=" querystring value sent by the SonicWall.This allows
you to use the same
   'page (e.g. this page) for the "Session Expiration" (?cc=2), "Idle Timeout"
(?cc=3) and "Max Sessions" (?cc=4) page.
   If customCode <> "" Then
      Select Case customCode
      Case "2"
         LHMResult.Text="<br><H3><font color=""red"">Your LHM session has expired.You
may try to initiate a new session.</font></H3>"
      Case "3"
         LHMResult.Text="<br><H3><font color=""red"">You have exceeded your idle
timeout.Please log back in.</font></H3>"
      Case "4"
         LHMResult.Text="<br><H3><font color=""red"">The maximum number of sessions
has been reached.Please try again later.</font></H3>"
      End Select
   End If

   'Set the userName to the grabbed client MAC address if so configured in myvars
   If userName = "useMAC" Then
      userName = mac
   End If

   'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWall
   'This is necessary for the POST to the SonicWall authorizing the LHM session.
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   'Note - the routine below for handling the hmac requires the use of the
SonicSSL.dll and libeay.dll libraries.
   'The DLL must be copied to the IIS server, and the SonicSSL dll must be registered
with "regsvr32 sonicssl.dll"
   If hmac <> "" Then

      'SonicWall URL Encode routine is different from Microsoft - this is the
SonicWall method
      req=Replace(req,"%","%25")
      req=Replace(req,":","%3A")
      req=Replace(req," ","%20")
      req=Replace(req,"?","%3F")
      req=Replace(req,"+","%2B")
      req=Replace(req,"&","%26")
      req=Replace(req,"=","%3D")

      Dim strHmacText as String
      Dim objCrypto as Object
```

```
      Dim strHmacGenerated
      Dim loginError as String

      'Initialize the Crypto object
      objCrypto = Server.CreateObject("SonicSSL.Crypto")

      'The text to be encoded
      strHmacText = sessionId & ip & mac & ufi & mgmtBaseUrl & clientRedirectUrl &
req

      'Calculate the hash with a key strHmac, the return value is a string converted
form the output sha1 binary.
      'The hash algorithm (MD5 or SHA1) is configured in myvars and in the Extern
Guest Auth config on the SonicWall
      If hmacType = "MD5" Then
         strHmacGenerated = objCrypto.hmac_md5(strHmacText, strHmac)
      Else
         strHmacGenerated = objCrypto.hmac_sha1(strHmacText, strHmac)
      End If

      If strHmacGenerated <> hmac Then
         Dim hmacFail as String
         hmacFail = "<font color=""red"">The HMAC failed validation.Please notify an
attendant.</font><br><br>"
         hmacFail+="<font color=""9CBACE"">Received HMAC: " & hmac & "<br>Calculated
HMAC: " & strHmacGenerated & "<br>"
         hmacFail+="Make sure the digest functions on the SonicWall and LHM server
match.<br>"
         hmacFail+="Also make sure the shared secret on the SonicWall and myvars
match</font>"
         catchError.Text=hmacFail
      End If

   End If

End Sub

Sub btnSubmit_Click(Sender As Object, E As EventArgs)

   'Let the user know that we are setting up the session, just in case it takes more
than a second
   LHMResult.Text = "Authorizing session.Please wait."

   'The LHM cgi on the SonicWall - this does not change
   Dim loginCgi as String = "externalGuestLogin.cgi"

   'Assemble the data to post back to the SonicWall to authorize the LHM session
   Dim loginParams as String = "sessId=" & sessionId & "&userName=" &
Server.URLEncode(userName) & "&sessionLifetime=" & sessTimer & "&idleTimeout=" &
idleTimer

   'Combine mgmtBaseUrl from the original redirect with the login cgi
   Dim postToSNWL as String = mgmtBaseUrl & loginCgi

   'Convert the loginParams to a well behaved byte array
   Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

   Try
      'Create the webrequest to the SonicWall
      Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)
```

```
      'Calculate the length of the byte array
      toSNWL.ContentLength = byteArray.Length

      'Set the method for the webrequest to POST
      toSNWL.Method = "POST"

      'Set the content type
      toSNWL.ContentType = "application/x-www-form-urlencoded"

      'Open the request stream
      Dim dataStream As Stream = toSNWL.GetRequestStream()

      'Write the byte array to the request stream
      dataStream.Write(byteArray, 0, byteArray.Length)

      'Close the Stream object
      dataStream.Close()

      'Get the response
      Dim snwlReply As WebResponse = toSNWL.GetResponse()

      'Display the status - looking for 200 = OK.
      'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

      'Grab the response and stuff it into an xml doc for possible review
      Dim snwlResponse as XmlDocument = New XmlDocument()
      snwlResponse.Load(snwlReply.GetResponseStream())

      'Set the xPath to the SNWL reply, and get the response
      Dim codePath as String =
"SonicWallAccessGatewayParam/AuthenticationReply/ResponseCode"

      'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

      'Response code 50 - Login Succeeded
      If snwlResponse.SelectSingleNode(codePath).InnerXml = "50"

         'Do we want to provide a logout popup window?
         If logoutPopup = "1" Then
            'Popup hack using Javascript for logout window
            Dim sb As New System.Text.StringBuilder()
            sb.Append("<script language='javascript'>")
            sb.Append("window.open('logout.aspx?sessId=")
            sb.Append(Server.URLEncode(CStr(sessionId)))
            sb.Append("&mgmtBaseUrl=")
            sb.Append(Server.URLEncode(CStr(mgmtBaseUrl)))
            sb.Append("&sessTimer=")
            sb.Append(Server.URLEncode(CStr(sessTimer)))
            sb.Append("','logOut','toolbar=no,")
            sb.Append("addressbar=no,menubar=no,")
            sb.Append("width=400,height=250');")
            sb.Append("<")
            sb.Append("/")
            sb.Append("script>")
            RegisterStartupScript("stp", sb.ToString)
         End If

         LHMResult.Text = "<br><b><font color=""green"">Session
Authorized:</font></b> You may now go to the URL you originally requested: <a
target=""_blank"" href=""" & req & """>" & req & "</a>"
```

```
      'Response code 51 - Session Limit Exceeded
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "51"
         LHMResult.Text = "<br><b><font color=""red"">Session Limit
Reached:</font></b> The maximum number of guest session has been reached.Sorry for
the inconvenience.Please close and relaunch your browser to try again."

      'Response code 100 - Login Failed.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "100"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> Your session cannot be created at this time.Sorry for the
inconvenience.Please close and relaunch your browser to try again."

      'Response code 251 - Bad HMAC.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed message authentication.Sorry
for the inconvenience.Please close and relaunch your browser to try again."

      'Response code 253 - Invalid SessionID.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed to match a known session
identity.Sorry for the inconvenience.Please close and relaunch your browser to try
again."

      'Response code 254 - Invalid CGI.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization was missing an essential
parameter.Sorry for the inconvenience.Please close and relaunch your browser to try
again."

      'Response code 255 - Internal Error.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified
error.Sorry for the inconvenience.Please close and relaunch your browser to try
again."

      End If

      'Close the streams
      dataStream.Close()
      snwlReply.Close()

      'If there is some asp.net error trying to talk to the SonicWall, print it in
the same color as the background.
      Catch ex as Exception
         catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified
error.Sorry for the inconvenience.Please close and relaunch your browser to try
again.If the problem persists, please notify an attendant."
      End Try
End Sub


</script>

<STYLE>
body {
```

```
  font-size: 10pt;
  font-family: verdana,helvetica,arial,sans-serif;
  color:#000000;
  background-color:#9CBACE;
}

tr.heading {
  background-color:#006699;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Accept Script</TITLE>
</HEAD>

<BODY>
<form id="frmValidator" runat="server">

<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
   <tr class="heading">
      <td width="50%" valign="center"><font color="white"><b>Welcome <%=
ip%></b></font></td>
      <td><center><img width="216" height="51" src="<%= logo%>"></center></td>
      <td width="50%" align="right" valign="center"><font color="white"><b>Powered
by SonicWall LHM</b> </font></td>
   </tr>
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>

<table width="100%" border="0" cellpadding="2" cellspacing="0">

   <tr>
   <td><br></td>
   </tr>
   <tr>
      <td align=left>
      By clicking the <b>Accept</b> button below, you accept the following terms of
service:<br><br><b>
      1.You will not try to download bad things.<br>
      2.You will not try to upload bad things.<br>
      3.You will not try to use all the bandwidth so that others have none.<br>
      4.You will be happy when the SonicWall blocks bad things from reaching
you.</b><br><br>
      </td>
      <td>
   </tr>
   <tr>
      <td><br><asp:button id="btnSubmit" class="button" text="  Accept  "
onClick="btnSubmit_Click" runat="server" /></td>
   </tr>
```

```
   <tr>
      <td><asp:Label id=LHMResult runat="server" /></td>
   </tr>
   <tr>
      <td><asp:Label id=catchError runat="server" /></td>
   </tr>
</table>
</form>
</BODY>
</HTML>
```

logout.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWall authorizing the LHM session.
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
      As Boolean Implements ICertificatePolicy.CheckValidationResult
         Return True
   End Function
End Class

Dim sessionId as String
Dim mgmtBaseUrl as String
Dim eventId as String = "&eventId=1"

'Grab the code and the session lifetime from the generator page
Sub Page_Load(src as Object, e as EventArgs)
   sessionId=Request.QueryString("sessId")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
   sessTimer=Request.QueryString("sessTimer")


   'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWall
   'This is necessary for the POST to the SonicWall authorizing the LHM session.
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   'When the page loads, make the loggedIn span visible
   loggedIn.Visible=True
   loggedOut.Visible=False

   Me.Button1.Attributes.Add("OnClick", "self.close()")
```

```
End Sub

'The Logout button
Sub btnSubmit_Click(Sender As Object, E As EventArgs)

   'Let the user know that we are setting up the session, just in case it takes more
than a second
   LHMResult.Text = "Authorizing session.Please wait."

   'The LHM cgi on the SonicWall - this does not change
   Dim loginCgi as String = "externalGuestLogoff.cgi"

   'Assemble the data to post back to the SonicWall to authorize the LHM session
   Dim loginParams as String = "sessId=" & sessionId & eventId

   'Combine mgmtBaseUrl from the original redirect with the login cgi
   Dim postToSNWL as String = mgmtBaseUrl & loginCgi

   'Convert the loginParams to a well behaved byte array
   Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

   Try
      'Make the loggedOut span visible
      loggedIn.Visible=False
      loggedOut.Visible=True

      'Create the webrequest to the SonicWall
      Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

      'Calculate the length of the byte array
      toSNWL.ContentLength = byteArray.Length

      'Set the method for the webrequest to POST
      toSNWL.Method = "POST"

      'Set the content type
      toSNWL.ContentType = "application/x-www-form-urlencoded"

      'Open the request stream
      Dim dataStream As Stream = toSNWL.GetRequestStream()

      'Write the byte array to the request stream
      dataStream.Write(byteArray, 0, byteArray.Length)

      'Close the Stream object
      dataStream.Close()

      'Get the response
      Dim snwlReply As WebResponse = toSNWL.GetResponse()

      'Display the status - looking for 200 = OK.
      'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

      'Grab the response and stuff it into an xml doc for possible review
      Dim snwlResponse as XmlDocument = New XmlDocument()
      snwlResponse.Load(snwlReply.GetResponseStream())

      'Set the xPath to the SNWL reply, and get the response
      Dim codePath as String =
"SonicWallAccessGatewayParam/LogoffReply/ResponseCode"
```

```
      'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

      'Response code 150 - Logout Succeeded
      If snwlResponse.SelectSingleNode(codePath).InnerXml = "150"
        LHMResult.Text = "<br><b><font color=""green"">Your session has been logged
out.<br><br>Thank you for using LHM Guest Services.</font></b>"

      'Response code 251 - Bad HMAC.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed message authentication.Sorry for the
inconvenience.Please close and relaunch your browser to try again."

      'Response code 253 - Invalid SessionID.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed to match a known session identity.Sorry for
the inconvenience.Please close and relaunch your browser to try again."

      'Response code 254 - Invalid CGI.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request was missing an essential parameter.Sorry for the
inconvenience.Please close and relaunch your browser to try again."

      'Response code 255 - Internal Error.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error.Sorry for the
inconvenience.Please close and relaunch your browser to try again."

      End If

      'Close the streams
      dataStream.Close()
      snwlReply.Close()

      'If there is some asp.net error trying to talk to the SonicWall, print it in
the same color as the background.
      Catch ex as Exception
        catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error.Sorry for the
inconvenience.Please close and relaunch your browser to try again.If the problem
persists, please notify an attendant."
      End Try
End Sub

</script>
<STYLE>
body {
   font-size: 10pt;
   font-family: verdana,helvetica,arial,sans-serif;
   color:#000000;
   background-color:#9CBACE;
}

tr.heading {
   font-size: 10pt;
   background-color:#006699;
}
```

```
tr.smalltext {
   font-size: 8pt;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
   font-size: 8pt;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Logout Page</TITLE>

<SCRIPT LANGUAGE="Javascript">

//'Javascript Seconds Countdown Timer
var SecondsToCountDown = <%= sessTimer%>;
var originalTime=" ";

function CountDown()
{
   clockStr="";

   dayStr=Math.floor(SecondsToCountDown/86400)%100000
   if(dayStr>0){
      if(dayStr>1){
         dayStr+=" days ";
      } else dayStr+=" day ";
      clockStr=dayStr;
   }
   hourStr=Math.floor(SecondsToCountDown/3600)%24
   if(hourStr>0){
      if(hourStr>1){
         hourStr+=" hours ";
      } else hourStr+=" hour ";
      clockStr+=hourStr;
   }
   minuteStr=Math.floor(SecondsToCountDown/60)%60
   if(minuteStr>0){
      if(minuteStr>1){
         minuteStr+=" minutes ";
      } else minuteStr+=" minute ";
      clockStr+=minuteStr;
   }
   secondStr=Math.floor(SecondsToCountDown/1)%60
   if(secondStr>0){
      if(secondStr>1){
         secondStr+=" seconds ";
      } else secondStr+=" second ";
      clockStr+=secondStr;
   }

   if(SecondsToCountDown > 0)
   {
      --SecondsToCountDown;
   }

   if(originalTime.length < 2)
```

```
   {
      originalTime = clockStr;
   }

   // Make sure the form is still there before trying to set a value
   if(document.frmValidator){
      document.frmValidator.originalTime.value = originalTime;
      document.frmValidator.countdown.value = clockStr;
   }

   setTimeout("CountDown()", 1000);
   if(SecondsToCountDown == 0)
   {
      document.frmValidator.countdown.value = "Session Expired";
   }
}

//'Disable right-click so that the window doesn't get refreshed since the countdown
is clientside.
document.oncontextmenu = disableRightClick;
function disableRightClick()
{
  return false;
}

//'Disable F5 key, too, on IE at least.
function noF5()
{
   var key_f5 = 116;
   if (key_f5==event.keyCode)
   {
      event.keyCode=0;
      return false;
   }
   return false;
}

document.onkeydown=noF5
document.onmousedown=disableRightClick

</SCRIPT>

</HEAD>

<BODY onload='CountDown()'>
<span id="loggedIn" runat="server">
<form id="frmValidator" runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"><font color="white"><b>SonicWall LHM Logout
Window</b></font></td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="smalltext"><td><br></td></tr>
   <tr class="smalltext">
      <td>Original Session Time:</td>
```

```
      <td><asp:textbox width=250 id="originalTime" runat="server" /></td>
   </tr>
   <tr class="smalltext">
      <td>Remaining Session Time:</td>
      <td><asp:textbox width=250 id="countdown" runat="server" /></td>
   </tr>
   <tr class="smalltext">
      <td colspan=2><br>You may use this window to manually logout your session at
any time, or you may safely close this window if you prefer to let your session
timeout automatically.</font></td>
   </td>
   <tr>
      <td colspan=2><center><asp:button id="btnSubmit" class="button" text="  Logout
" onClick="btnSubmit_Click" runat="server" /></center></td>
   </tr>
</table>
</form>
</span>

<span id="loggedOut" runat="server">
<form id="logout" runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"><font color="white"><b>SonicWall LHM Logout
Window</b></font></td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr>
      <td><asp:Label id=LHMResult runat="server" /></td>
   </tr>
   <tr>
      <td><asp:Label id=catchError runat="server" /></td>
   </tr>
   <tr><td><br></td></tr>
   <tr>
      <td><center><asp:button id="Button1" class="button" text="  Close  "
runat="server" /></center></td>
   </tr>
</table>
</form>
</span>

</BODY>
</HTML>
```

myvars.aspx

```
<script language="VB" runat="server">

'Set the logoutPopup window flag - 0 = no popup, 1 = popup
'The use of the logoutPopup in this script is encouraged because the login event is
non-exclusive.
Dim logoutPopup as String = "1"

'Set the LHM Session Timeout
Dim sessTimer as String = "3600"
```

```
'Set the LHM Idle Timeout
Dim idleTimer as String = "300"

'Set the username to record for LHM session since this does not gather one.Set to
userName="useMAC" to use the MAC address.
Dim userName="useMAC"
'Dim userName = "LHM Guest User"

'Set the secret for use with optional HMAC auth, as configured in the Extern Guest
Auth config on the SonicWall
Dim strHmac as String = "password"

'Set the digest method for the HMAC, either MD5 or SHA1
Dim hmacType as String = "MD5"
'Dim hmacType as String = "SHA1"

'Set the logo image to use
Dim logo as String = "SonicWall.gif"

'------------------------End of Configurable Settings-------------------------

</script>
```

ADAuth スクリプト

認証モデル

ゲスト クライアントはユーザ名とパスワードを入力します。その後、これらの資格情報は Active Directory または LDAP データベースを照会して認証されます。

目的

LDAP 経由で Active Directory を使用する古典的な承認モデルです。承認時に必要に応じてデータベースから LDAP 属性を取得することで、提供されるユーザごとのセッションタイマーおよび無動作タイマーの設定をサポートします。

myvars 変数

`logoutPopup` ログアウト ポップアップ ウィンドウの使用を制御します。次のように設定します。

- **0**: ポップアップ ウィンドウを無効にします。
- **1**: ポップアップ ウィンドウを有効にします。

`myLdapServer` 認証を提供する LDAP/AD サーバの IP アドレスまたは解決可能な FQDN です。

`myLdapDomain` LDAP/AD ドメイン名

`retrAttr` セッションおよび無動作タイマー値を認証側ユーザの LDAP 用 `attributes` (後で定義) から取得するかどうかを指定します。次のように設定します。

- **0**: 取得を無効にします。
- **1**: 取得を試みます。

useCN	reAttr が 1 の場合、このフラグは、コモンネーム (cn) を使用して属性を取得するか、それとも AD の既定ログイン名 (sAMAccountName) を使用するかを設定します。 **1** に設定すると、cn が使用されます。AD に照らして認証を行う場合、このフラグは **0** に設定しておく必要があります。
sessAttr	セッション タイマー (秒単位) の取得元となる LDAP 属性。値を取得できない場合や、取得した値が数値でない場合は、既定のセッション タイマー (sessTimer、以下を参照) が使用されます。
idleAttr	無動作タイマー (秒単位) の取得元となる LDAP 属性。値を取得できない場合や、取得した値が数値でない場合は、既定の無動作タイマー (idleTimer、以下を参照) が使用されます。
sessTimer	既定のセッション タイマー (秒単位)。
idleTimer	既定の無動作タイマー (秒単位)。
strHmac	オプションの HMAC 機能のための事前共有鍵。
hmacType	HMAC 使用時に用いるダイジェスト種別: 「**MD5**」または「**SHA1**」を選択します。
logo	ページ ヘッダーで使用するロゴ (画像) ファイルの名前。

セッション フロー

1 ゲスト クライアントはLDAP/ADのユーザ名とパスワードを入力します。
2 指定された資格情報は設定されている LDAP サーバとのバインドのために使用されます。
3 バインド試行が成功した場合、ユーザは認証されます。
4 reAttr フラグが設定されている場合、定義済みの sessAttr および idleAttr 属性 (pager、mobile など) を LDAP DB から取得するための試行が行われます。有効な結果が取得された場合、その結果が使用されます。そうでない場合は既定値が使用されます。
5 スクリプトは、セッションを承認するために SonicWall セキュリティ装置に対する LHM ポストを実行します。

追加の考慮事項

LHM サーバは、設定されている LDAP/AD サーバと、ルート、NAT、または VPN によって通信できる必要があります。reAttr オプションを使用する場合は、ユーザ固有の値が有効になるように LDAP 属性が定義されている必要があります。

メモ： pager および mobile 属性が選択されたのは、その使用頻度が低く、また Microsoft の「ユーザとコンピュータ」 MMC から直接設定できるためです。

トピック:

- default.aspx (877 ページ)
- logout.aspx (884 ページ)
- myvars.aspx (890 ページ)

default.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Math" %>
<%@ Import Namespace="System.DirectoryServices" %>
<%@ Import Namespace="System.Collections" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>
<%@ Assembly name="System.DirectoryServices, Version=1.0.3300.0,
Culture=neutral,PublicKeyToken=b03f5f7f11d50a3a"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWall authorizing the LHM session.
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
      As Boolean Implements ICertificatePolicy.CheckValidationResult
      Return True
   End Function
End Class

'Sample LHM redirect querystring:
'http://127.0.0.1/lhm/adauth/default.aspx?sessionId=0b712fd83b9f5313db5af1cea6b1004
f&ip=10.50.165.231&mac=00:0e:35:bd:c9:37&ufi=0006b11184300&mgmtBaseUrl=https://10.5
0.165.193:4043/&clientRedirectUrl=https://10.50.165.193:444/&req=http%3A//www.googl
e.com/ig

Dim ip as String
Dim sessionId as String
Dim mac as String
Dim ufi as String
Dim mgmtBaseUrl as String
Dim clientRedirectUrl as String
Dim req as String
Dim hmac as String
Dim customCode as String

Sub Page_Load(src as Object, e as EventArgs)

   LHMResult.Text=""
   catchError.Text=""
   authResult.Text=""

   ip=Request.QueryString("ip")
   sessionId=Request.QueryString("sessionId")
   mac=Request.QueryString("mac")
   ufi=Request.QueryString("ufi")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
   clientRedirectUrl=Request.QueryString("clientRedirectUrl")
   req=Request.QueryString("req")
```

```
   hmac=Request.QueryString("hmac")
   customCode=Request.QueryString("cc")

   'customCode grabs the "cc=" querystring value sent by the SonicWall.This allows
you to use the same
   'page (e.g. this page) for the "Session Expiration" (?cc=2), "Idle Timeout"
(?cc=3) and "Max Sessions" (?cc=4) page.
   If customCode <> "" Then
      Select Case customCode
      Case "2"
         LHMResult.Text="<br><H3><font color=""red"">Your LHM session has expired.You
may try to initiate a new session.</font></H3>"
      Case "3"
         LHMResult.Text="<br><H3><font color=""red"">You have exceeded your idle
timeout.Please log back in.</font></H3>"
      Case "4"
         LHMResult.Text="<br><H3><font color=""red"">The maximum number of sessions
has been reached.Please try again later.</font></H3>"
      End Select
   End If

   'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWall
   'This is necessary for the POST to the SonicWall authorizing the LHM session.
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   'Note - the routine below for handling the hmac requires the use of the
SonicSSL.dll and libeay.dll libraries.
   'The DLL must be copied to the IIS server, and the SonicSSL dll must be registered
with "regsvr32 sonicssl.dll"
   If hmac <> "" Then

      'SonicWall URL Encode routine is different from Microsoft - this is the
SonicWall method
      req=Replace(req,"%","%25")
      req=Replace(req,":","%3A")
      req=Replace(req," ","%20")
      req=Replace(req,"?","%3F")
      req=Replace(req,"+","%2B")
      req=Replace(req,"&","%26")
      req=Replace(req,"=","%3D")

      Dim strHmacText as String
      Dim objCrypto as Object
      Dim strHmacGenerated
      Dim loginError as String

      'Initialize the Crypto object
      objCrypto = Server.CreateObject("SonicSSL.Crypto")

      'The text to be encoded
      strHmacText = sessionId & ip & mac & ufi & mgmtBaseUrl & clientRedirectUrl &
req

      'Calculate the hash with a key strHmac, the return value is a string converted
form the output sha1 binary.
      'The hash algorithm (MD5 or SHA1) is configured in myvars and in the Extern
Guest Auth config on the SonicWall
      If hmacType = "MD5" Then
         strHmacGenerated = objCrypto.hmac_md5(strHmacText, strHmac)
      Else
```

```
        strHmacGenerated = objCrypto.hmac_sha1(strHmacText, strHmac)
      End If

      If strHmacGenerated <> hmac Then
        Dim hmacFail as String
        hmacFail = "<font color=""red"">The HMAC failed validation.Please notify an
attendant.</font><br><br>"
        hmacFail+="<font color=""9CBACE"">Received HMAC: " & hmac & "<br>Calculated
HMAC: " & strHmacGenerated & "<br>"
        hmacFail+="Make sure the digest functions on the SonicWall and LHM server
match.<br>"
        hmacFail+="Also make sure the shared secret on the SonicWall and myvars
match</font>"
        catchError.Text=hmacFail
      End If

   End If

End Sub

sub OnBtnClearClicked (Sender As Object, e As EventArgs)
   txtName.Text = ""
   txtPassword.Text = ""
   authResult.Text=""
   LHMResult.Text=""
   catchError.Text=""
end sub

Sub btnSubmit_Click(Sender As Object, E As EventArgs)

   'Try to connect to LDAP with the user supplied attributes
   Try
      Dim ldapPath as String = "LDAP://"& myLdapServer
      Dim ldapUser as String = myLdapDomain & "\" & txtName.Text
      Dim validateUser as New DirectoryEntry(ldapPath,ldapUser,txtPassword.Text)

      'This is the actual authentication piece
      Dim nativeCheck as Object = validateUser.NativeObject

      'If retrAttr is set in the myvars file, attempt to retrieve the session and
idle values from LDAP
      If retrAttr = "1" Then
        Dim mySearch as New DirectorySearcher(validateUser)

        'Check the myvars for selecting either sAMAccountName or cn
        If useCN = "0" Then
          mySearch.Filter = "(sAMAccountName=" & Server.URLEncode(txtName.Text) &
")"
        Else
          mySearch.Filter = "(cn=" & Server.URLEncode(txtName.Text) & ")"
        End If
        mySearch.PageSize="1"
        mySearch.PropertiesToLoad.Add(sessAttr)
        mySearch.PropertiesToLoad.Add(idleAttr)
        Dim adResult as SearchResult

        'If we get results on the attribute query, set timer values
        adResult = mySearch.FindOne
        If Not (adResult is Nothing) Then
          If (adResult.Properties.Contains(sessAttr)) Then
               'Check to see if the LDAP value returned is a number
```

```
                Dim isNumber as New RegEx("^\d+$")
                If (isNumber.IsMatch(adResult.Properties(sessAttr)(0).ToString()))
Then
                   sessTimer=adResult.Properties(sessAttr)(0).ToString()
                End If
           End If 'End If sessAttr
           If (adResult.Properties.Contains(idleAttr)) Then
                'Check to see if the LDAP value returned is a number
                Dim isNumber as New RegEx("^\d+$")
                If (isNumber.IsMatch(adResult.Properties(idleAttr)(0).ToString()))
Then
                   idleTimer=adResult.Properties(idleAttr)(0).ToString()
                End If
           End If 'End if idleAttr
        End If 'End if adResult is present
     End If 'End if retrAttr is in use

     authResult.Text="<font color=""green""><b>Credentials
Accepted.</b></font><br>Session Lifetime: " & round(sessTimer/60) & "
minutes.<br>Idle Timer: " & round(idleTimer/60) & " minutes."

     'Auth succeeded - move on to LHM Auth
     LHM()

     Catch ex as Exception
        catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
        authResult.Text="<font color=""Red""><b>Credentials
Rejected.</b></font><br>Please enter a valid username and password."
   End Try

End Sub

Sub LHM()

     'Let the user know that we are setting up the session, just in case it takes
more than a second
     LHMResult.Text = "Authorizing session.Please wait."

     'The LHM cgi on the SonicWall - this does not change
     Dim loginCgi as String = "externalGuestLogin.cgi"

     'Assemble the data to post back to the SonicWall to authorize the LHM session
     Dim loginParams as String = "sessId=" & sessionId & "&userName=" &
Server.URLEncode(txtName.Text) & "&sessionLifetime=" & sessTimer & "&idleTimeout=" &
idleTimer

     'Combine mgmtBaseUrl from the original redirect with the login cgi
     Dim postToSNWL as String = mgmtBaseUrl & loginCgi

     'Convert the loginParams to a well behaved byte array
     Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

     Try
        'Create the webrequest to the SonicWall
        Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

        'Calculate the length of the byte array
        toSNWL.ContentLength = byteArray.Length

        'Set the method for the webrequest to POST
        toSNWL.Method = "POST"
```

```
        'Set the content type
        toSNWL.ContentType = "application/x-www-form-urlencoded"

        'Open the request stream
        Dim dataStream As Stream = toSNWL.GetRequestStream()

        'Write the byte array to the request stream
        dataStream.Write(byteArray, 0, byteArray.Length)

        'Close the Stream object
        dataStream.Close()

        'Get the response
        Dim snwlReply As WebResponse = toSNWL.GetResponse()

        'Display the status - looking for 200 = OK.
        'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

        'Grab the response and stuff it into an xml doc for possible review
        Dim snwlResponse as XmlDocument = New XmlDocument()
        snwlResponse.Load(snwlReply.GetResponseStream())

        'Set the xPath to the SNWL reply, and get the response
        Dim codePath as String =
"SonicWallAccessGatewayParam/AuthenticationReply/ResponseCode"

        'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

        'Response code 50 - Login Succeeded
        If snwlResponse.SelectSingleNode(codePath).InnerXml = "50"

           'Do we want to provide a logout popup window?
           If logoutPopup = "1" Then
              'Popup hack using Javascript for logout window
              Dim sb As New System.Text.StringBuilder()
              sb.Append("<script language='javascript'>")
              sb.Append("window.open('logout.aspx?sessId=")
              sb.Append(Server.URLEncode(CStr(sessionId)))
              sb.Append("&mgmtBaseUrl=")
              sb.Append(Server.URLEncode(CStr(mgmtBaseUrl)))
              sb.Append("&sessTimer=")
              sb.Append(Server.URLEncode(CStr(sessTimer)))
              sb.Append("','logOut','toolbar=no,")
              sb.Append("addressbar=no,menubar=no,")
              sb.Append("width=400,height=250');")
              sb.Append("<")
              sb.Append("/")
              sb.Append("script>")
              RegisterStartupScript("stp", sb.ToString)
           End If

           LHMResult.Text = "<br><b><font color=""green"">Session
authorized:</font></b> You may now go to the URL you originally requested: <a
target=""_blank"" href=""" & req & """>" & req & "</a>"

        'Response code 51 - Session Limit Exceeded
        ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "51"
           LHMResult.Text = "<br><b><font color=""red"">Session Limit
Reached:</font></b> The maximum number of guest session has been reached.Sorry for
the inconvenience.Please close and relaunch your browser to try again."
```

```
        'Response code 100 - Login Failed.
        ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "100"
           LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> Your session cannot be created at this time.Sorry for the
inconvenience.Please close and relaunch your browser to try again."

        'Response code 251 - Bad HMAC.
        ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
           LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed message authentication.Sorry
for the inconvenience.Please close and relaunch your browser to try again."

        'Response code 253 - Invalid SessionID.
        ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
           LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed to match a known session
identity.Sorry for the inconvenience.Please close and relaunch your browser to try
again."

        'Response code 254 - Invalid CGI.
        ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
           LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization was missing an essential
parameter.Sorry for the inconvenience.Please close and relaunch your browser to try
again."

        'Response code 255 - Internal Error.
        ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
           LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified
error.Sorry for the inconvenience.Please close and relaunch your browser to try
again."

        End If

        'Close the streams
        dataStream.Close()
        snwlReply.Close()

        'If there is some asp.net error trying to talk to the SonicWall, print it in
the same color as the background.
        Catch ex as Exception
           catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
           LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified
error.Sorry for the inconvenience.Please close and relaunch your browser to try
again.If the problem persists, please notify an attendant."
     End Try
End Sub
</script>

<STYLE>
body {
  font-size: 10pt;
  font-family: verdana,helvetica,arial,sans-serif;
  color:#000000;
  background-color:#9CBACE;
}

tr.heading {
```

```
  background-color:#006699;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM ADAuth Script</TITLE>
</HEAD>

<BODY>
<form id="frmValidator" runat="server">

<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
   <tr class="heading">
      <td width="50%" valign="center"><font color="white"><b>LDAP/AD LHM
Authentication</b></font></td>
      <td><center><img width="216" height="51" src="<%= logo %>"></center></td>
      <td width="50%" align="right" valign="center"><font color="white"><b>Powered
by SonicWall LHM</b> </font></td>
   </tr>
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>

<table width="90%" border="0" cellpadding="2" cellspacing="0">
   <tr>
      <td><b>Welcome <%= ip%> to SonicWall's LHM AD/LDAP
Authenticator.</b><br><br>Enter your LDAP or Active Directory username and password
to obtain secure guest Internet access.<br><br>If your domain account specifies
session timeout values, those values will be applied to your account, otherwise you
will receive the default one hour (60 minutes) of access with a five minute idle
timeout.<br>
      </td>
   </tr>
</table>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white">Authentication domain:
<%=myLdapDomain%></td>
   </tr>
</table>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr>
      <td width="30%"><br>Enter your login name:</td>
      <td width="30%"><asp:TextBox id="txtName" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtName"
ControlToValidate="txtName" ErrorMessage="Please enter your name." runat="server"
/></td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your password:</td>
```

```
      <td width="30%"><asp:TextBox id="txtPassword" textmode="password"
runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtPassword"
ControlToValidate="txtPassword" ErrorMessage="Please enter your password."
runat="server" /></td>
   </tr>
   <tr>
      <td></td><td><asp:Label id=authResult runat="server" /> </td>
   </tr>
   <tr>
      <td></td>
      <td><asp:button id="btnSubmit" class="button" text="  Submit  "
onClick="btnSubmit_Click" runat="server" />
        
      <asp:button id="btnClear" class="button" text=" Clear All "
CausesValidation="False" onClick="OnBtnClearClicked" runat="server" />
      </td>
   </tr>
   <tr>
      <td colspan=2><asp:Label id=LHMResult runat="server" /></td>
   </tr>
   <tr>
      <td colspan=2><asp:Label id=catchError runat="server" /></td>
   </tr>
</table>
</form>
</BODY>
</HTML>
```

logout.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWall authorizing the LHM session.
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
      As Boolean Implements ICertificatePolicy.CheckValidationResult
      Return True
   End Function
End Class

Dim sessionId as String
Dim mgmtBaseUrl as String
Dim eventId as String = "&eventId=1"
```

```
'Grab the code and the session lifetime from the generator page
Sub Page_Load(src as Object, e as EventArgs)
   sessionId=Request.QueryString("sessId")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
   sessTimer=Request.QueryString("sessTimer")


   'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWall
   'This is necessary for the POST to the SonicWall authorizing the LHM session.
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   'When the page loads, make the loggedIn span visible
   loggedIn.Visible=True
   loggedOut.Visible=False

   Me.Button1.Attributes.Add("OnClick", "self.close()")

End Sub

'The Logout button
Sub btnSubmit_Click(Sender As Object, E As EventArgs)

   'Let the user know that we are setting up the session, just in case it takes more
than a second
   LHMResult.Text = "Authorizing session.Please wait."

   'The LHM cgi on the SonicWall - this does not change
   Dim loginCgi as String = "externalGuestLogoff.cgi"

   'Assemble the data to post back to the SonicWall to authorize the LHM session
   Dim loginParams as String = "sessId=" & sessionId & eventId

   'Combine mgmtBaseUrl from the original redirect with the login cgi
   Dim postToSNWL as String = mgmtBaseUrl & loginCgi

   'Convert the loginParams to a well behaved byte array
   Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

   Try
      'Make the loggedOut span visible
      loggedIn.Visible=False
      loggedOut.Visible=True

      'Create the webrequest to the SonicWall
      Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

      'Calculate the length of the byte array
      toSNWL.ContentLength = byteArray.Length

      'Set the method for the webrequest to POST
      toSNWL.Method = "POST"

      'Set the content type
      toSNWL.ContentType = "application/x-www-form-urlencoded"

      'Open the request stream
      Dim dataStream As Stream = toSNWL.GetRequestStream()

      'Write the byte array to the request stream
      dataStream.Write(byteArray, 0, byteArray.Length)
```

```
      'Close the Stream object
      dataStream.Close()

      'Get the response
      Dim snwlReply As WebResponse = toSNWL.GetResponse()

      'Display the status - looking for 200 = OK.
      'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

      'Grab the response and stuff it into an xml doc for possible review
      Dim snwlResponse as XmlDocument = New XmlDocument()
      snwlResponse.Load(snwlReply.GetResponseStream())

      'Set the xPath to the SNWL reply, and get the response
      Dim codePath as String =
"SonicWallAccessGatewayParam/LogoffReply/ResponseCode"

      'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

      'Response code 150 - Logout Succeeded
      If snwlResponse.SelectSingleNode(codePath).InnerXml = "150"
        LHMResult.Text = "<br><b><font color=""green"">Your session has been logged
out.<br><br>Thank you for using LHM Guest Services.</font></b>"

      'Response code 251 - Bad HMAC.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed message authentication.Sorry for the
inconvenience.Please close and relaunch your browser to try again."

      'Response code 253 - Invalid SessionID.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed to match a known session identity.Sorry for
the inconvenience.Please close and relaunch your browser to try again."

      'Response code 254 - Invalid CGI.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request was missing an essential parameter.Sorry for the
inconvenience.Please close and relaunch your browser to try again."

      'Response code 255 - Internal Error.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error.Sorry for the
inconvenience.Please close and relaunch your browser to try again."

      End If

      'Close the streams
      dataStream.Close()
      snwlReply.Close()

      'If there is some asp.net error trying to talk to the SonicWall, print it in
the same color as the background.
      Catch ex as Exception
        catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error.Sorry for the
```

```
inconvenience.Please close and relaunch your browser to try again.If the problem
persists, please notify an attendant."
      End Try
End Sub

</script>
<STYLE>
body {
   font-size: 10pt;
   font-family: verdana,helvetica,arial,sans-serif;
   color:#000000;
   background-color:#9CBACE;
}

tr.heading {
   font-size: 10pt;
   background-color:#006699;
}

tr.smalltext {
   font-size: 8pt;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
   font-size: 8pt;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Logout Page</TITLE>

<SCRIPT LANGUAGE="Javascript">

//'Javascript Seconds Countdown Timer
var SecondsToCountDown = <%= sessTimer%>;
var originalTime=" ";

function CountDown()
{
   clockStr="";

   dayStr=Math.floor(SecondsToCountDown/86400)%100000
   if(dayStr>0){
      if(dayStr>1){
         dayStr+=" days ";
      } else dayStr+=" day ";
      clockStr=dayStr;
   }
   hourStr=Math.floor(SecondsToCountDown/3600)%24
   if(hourStr>0){
      if(hourStr>1){
         hourStr+=" hours ";
      } else hourStr+=" hour ";
      clockStr+=hourStr;
   }
   minuteStr=Math.floor(SecondsToCountDown/60)%60
   if(minuteStr>0){
      if(minuteStr>1){
```

```
         minuteStr+=" minutes ";
      } else minuteStr+=" minute ";
      clockStr+=minuteStr;
   }
   secondStr=Math.floor(SecondsToCountDown/1)%60
   if(secondStr>0){
      if(secondStr>1){
         secondStr+=" seconds ";
      } else secondStr+=" second ";
      clockStr+=secondStr;
   }

   if(SecondsToCountDown > 0)
   {
      --SecondsToCountDown;
   }

   if(originalTime.length < 2)
   {
      originalTime = clockStr;
   }

   // Make sure the form is still there before trying to set a value
   if(document.frmValidator){
      document.frmValidator.originalTime.value = originalTime;
      document.frmValidator.countdown.value = clockStr;
   }

   setTimeout("CountDown()", 1000);
   if(SecondsToCountDown == 0)
   {
      document.frmValidator.countdown.value = "Session Expired";
   }
}

//'Disable right-click so that the window doesn't get refreshed since the countdown
is clientside.
document.oncontextmenu = disableRightClick;
function disableRightClick()
{
  return false;
}

//'Disable F5 key, too, on IE at least.
function noF5()
{
   var key_f5 = 116;
   if (key_f5==event.keyCode)
   {
      event.keyCode=0;
      return false;
   }
   return false;
}

document.onkeydown=noF5
document.onmousedown=disableRightClick

</SCRIPT>

</HEAD>
```

```
<BODY onload='CountDown()'>
<span id="loggedIn" runat="server">
<form id="frmValidator" runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"><font color="white"><b>SonicWall LHM Logout
Window</b></font></td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="smalltext"><td><br></td></tr>
   <tr class="smalltext">
      <td>Original Session Time:</td>
      <td><asp:textbox width=250 id="originalTime" runat="server" /></td>
   </tr>
   <tr class="smalltext">
      <td>Remaining Session Time:</td>
      <td><asp:textbox width=250 id="countdown" runat="server" /></td>
   </tr>
   <tr class="smalltext">
      <td colspan=2><br>You may use this window to manually logout your session at
any time, or you may safely close this window if you prefer to let your session
timeout automatically.</font></td>
   </td>
   <tr>
      <td colspan=2><center><asp:button id="btnSubmit" class="button" text="  Logout
" onClick="btnSubmit_Click" runat="server" /></center></td>
   </tr>
</table>
</form>
</span>

<span id="loggedOut" runat="server">
<form id="logout" runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"><font color="white"><b>SonicWall LHM Logout
Window</b></font></td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr>
      <td><asp:Label id=LHMResult runat="server" /></td>
   </tr>
   <tr>
      <td><asp:Label id=catchError runat="server" /></td>
   </tr>
   <tr><td><br></td></tr>
   <tr>
      <td><center><asp:button id="Button1" class="button" text="  Close  "
runat="server" /></center></td>
   </tr>
```

```
</table>
</form>
</span>

</BODY>
</HTML>
```

myvars.aspx

```
<script language="VB" runat="server">

'Set the logoutPopup window flag - 0 = no popup, 1 = popup
'The use of the logoutPopup in this script is encouraged because the login event is
non-exclusive.
Dim logoutPopup as String = "1"

'Set the LDAP server IP or Name
Dim myLdapServer as String = "10.50.128.40"

'Set the LDAP domain
Dim myLdapDomain as String = "sv.us.SonicWall.com"

'Set the retrAttr to 0 to use default session and idle timeouts
'Set the retrAttr to 1 to try to retrieve the session and idle timeouts from LDAP
attributes.
Dim retrAttr as String ="1"

'Set useCN=1 to use common name (e.g. "joe levy", non-Active Directory LDAP) for
attribute retrieval (retrAttr).
'Set useCN=0 to use saMACcountName (e.g. "jlevy", Active Directory / Windows) for
attribute retrieval.
Dim useCN as String = "0"

'If using retrAttr=1, you must define the ldap attributes from which to retrieve the
values
   'Set the ldap attribute from which to retrieve the session timeout value (use is
optional)
   Dim sessAttr as String = "pager"

   'Set the ldap attribute from which to retrieve the idle timeout value (use is
optional)
   Dim idleAttr as String = "mobile"

'If retrAttr=0, of if no attributes value can be retrieved, use the following
timeout values
   'Set the default LHM Session Timeout (for when no attributes is retrieved)
   Dim sessTimer as String = "3600"

   'Set the default LHM Idle Timeout (for when no attributes is retrieved)
   Dim idleTimer as String = "300"

'Set the secret for use with optional HMAC auth, as configured in the Extern Guest
Auth config on the SonicWall
Dim strHmac as String = "password"

'Set the digest method for the HMAC, either MD5 or SHA1
Dim hmacType as String = "MD5"
'Dim hmacType as String = "SHA1"

'Set the logo image to use
```

```
Dim logo as String = "SonicWall.gif"

'------------------------End of Configurable Settings-------------------------
</script>
```

ゲストブック スクリプト

認証モデル

ゲスト クライアントは名前、住所、電話番号、電子メール、URL (オプション)、およびコメント (オプション) の情報を入力します。

目的

マーケット情報を収集し、その情報を後で使用できるようにデータベースに書き込みます。

myvars 変数

`logoutPopup`	ログアウト ポップアップ ウィンドウの使用を制御します。次のように設定します。 • **0**: ポップアップ ウィンドウを無効にします。 • **1**: ポップアップ ウィンドウを有効にします。
`sessTimer`	秒単位のセッション タイマー。
`idleTimer`	秒単位の無動作タイマー。
`strHmac`	オプションの HMAC 機能のための事前共有鍵。
`hmacType`	HMAC 使用時に用いるダイジェスト種別: 「**MD5**」または「**SHA1**」を選択します。
`logo`	ページ ヘッダーで使用するロゴ (画像) ファイルの名前。

セッション フロー

1. ゲスト クライアントは自分の個人情報を入力して「送信」を選択します。
2. 入力された情報は、後で使用できるようにローカルの `.mdb` データベース ファイルに書き込まれます。
3. LHM ポスト文字列は、`sessionID`、ユーザ名 (ウェブフォームで入力されたもの)、既定のセッション存続期間、および無動作存続期間で構成されます。
4. スクリプトは、セッションを承認するために SonicWall セキュリティ装置に対する LHM ポストを実行します。

追加の考慮事項

このスクリプトはデータベースへの書き込みを行うため、**IUSR_MACHINENAME** および **IWAM_MACHINENAME** (または**ASPNET**) アカウントに対して書き込み権限を設定する必要があります (「SonicWall によって提供されたサンプル スクリプトを使用したいと考えています。使用するためには何が必要ですか。 (855 ページ)」を参照してください)。

トピック:

- default.aspx (891 ページ)
- logout.aspx (899 ページ)
- myvars.aspx (907 ページ)

default.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
```

```
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Data" %>
<%@ Import Namespace="System.Data.OleDB" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWall authorizing the LHM session.
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
      As Boolean Implements ICertificatePolicy.CheckValidationResult
      Return True
   End Function
End Class

'Sample LHM redirect querystring:
'http://127.0.0.1/lhm/guestbook/default.aspx?sessionId=0b712fd83b9f5313db5af1cea6b1
004f&ip=10.50.165.231&mac=00:0e:35:bd:c9:37&ufi=0006b11184300&mgmtBaseUrl=https://1
0.50.165.193:4043/&clientRedirectUrl=https://10.50.165.193:444/&req=http%3A//www.go
ogle.com/ig

Dim ip as String
Dim sessionId as String
Dim mac as String
Dim ufi as String
Dim mgmtBaseUrl as String
Dim clientRedirectUrl as String
Dim req as String
Dim hmac as String
Dim customCode as String

Sub Page_Load(src as Object, e as EventArgs)

   LHMResult.Text=""
   catchError.Text=""

   ip=Request.QueryString("ip")
   sessionId=Request.QueryString("sessionId")
   mac=Request.QueryString("mac")
   ufi=Request.QueryString("ufi")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
   clientRedirectUrl=Request.QueryString("clientRedirectUrl")
   req=Request.QueryString("req")
   hmac=Request.QueryString("hmac")
   customCode=Request.QueryString("cc")

   'customCode grabs the "cc=" querystring value sent by the SonicWall.This allows
you to use the same
   'page (e.g. this page) for the "Session Expiration" (?cc=2), "Idle Timeout"
(?cc=3) and "Max Sessions" (?cc=4) page.
   If customCode <> "" Then
      Select Case customCode
```

```
      Case "2"
         LHMResult.Text="<br><H3><font color=""red"">Your LHM session has expired.You
may try to initiate a new session.</font></H3>"
      Case "3"
         LHMResult.Text="<br><H3><font color=""red"">You have exceeded your idle
timeout.Please log back in.</font></H3>"
      Case "4"
         LHMResult.Text="<br><H3><font color=""red"">The maximum number of sessions
has been reached.Please try again later.</font></H3>"
      End Select
   End If

   'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWall
   'This is necessary for the POST to the SonicWall authorizing the LHM session.
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   'Note - the routine below for handling the hmac requires the use of the
SonicSSL.dll and libeay.dll libraries.
   'The DLL must be copied to the IIS server, and the SonicSSL dll must be registered
with "regsvr32 sonicssl.dll"
   If hmac <> "" Then

      'SonicWall URL Encode routine is different from Microsoft - this is the
SonicWall method
      req=Replace(req,"%","%25")
      req=Replace(req,":","%3A")
      req=Replace(req," ","%20")
      req=Replace(req,"?","%3F")
      req=Replace(req,"+","%2B")
      req=Replace(req,"&","%26")
      req=Replace(req,"=","%3D")

      Dim strHmacText as String
      Dim objCrypto as Object
      Dim strHmacGenerated
      Dim loginError as String

      'Initialize the Crypto object
      objCrypto = Server.CreateObject("SonicSSL.Crypto")

      'The text to be encoded
      strHmacText = sessionId & ip & mac & ufi & mgmtBaseUrl & clientRedirectUrl &
req

      'Calculate the hash with a key strHmac, the return value is a string converted
form the output sha1 binary.
      'The hash algorithm (MD5 or SHA1) is configured in myvars and in the Extern
Guest Auth config on the SonicWall
      If hmacType = "MD5" Then
         strHmacGenerated = objCrypto.hmac_md5(strHmacText, strHmac)
      Else
         strHmacGenerated = objCrypto.hmac_sha1(strHmacText, strHmac)
      End If

      If strHmacGenerated <> hmac Then
         Dim hmacFail as String
         hmacFail = "<font color=""red"">The HMAC failed validation.Please notify an
attendant.</font><br><br>"
         hmacFail+="<font color=""9CBACE"">Received HMAC: " & hmac & "<br>Calculated
HMAC: " & strHmacGenerated & "<br>"
```

```
        hmacFail+="Make sure the digest functions on the SonicWall and LHM server
match.<br>"
        hmacFail+="Also make sure the shared secret on the SonicWall and myvars
match</font>"
        catchError.Text=hmacFail
      End If

   End If

End Sub

sub OnBtnClearClicked (Sender As Object, e As EventArgs)
   txtName.Text = ""
   txtAddress.Text = ""
   txtCity.Text = ""
   txtState.Text = ""
   txtZip.Text = ""
   txtPhone.Text = ""
   txtEMail.Text = ""
   txtURL.Text = ""
   txtComment.Text = ""
   LHMResult.Text=""
   catchError.Text=""
end sub

Sub btnSubmit_Click(Sender As Object, E As EventArgs)

   Try
      'Try to write the submitted info to the database file
      Dim strConn as string = "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" &
server.mappath("guestbook.mdb") & ";"

      Dim MySQL as string = "INSERT INTO Guestbook (Name, Address, City, State, Zip,
Phone, EMail, URL, Comment) VALUES ('" & txtName.Text & "','" & txtAddress.Text &
"','" & txtCity.Text & "','" & txtState.Text & "','" & txtZip.Text & "','" &
txtPhone.Text & "','" & txtEMail.Text & "','" & txtURL.Text & "','" &
txtComment.Text & "')"
      Dim MyConn as New OleDBConnection (strConn)
      Dim cmd as New OleDBCommand (MySQL, MyConn)
      MyConn.Open ()
      cmd.ExecuteNonQuery ()
      MyConn.Close ()

      Catch ex as Exception
         catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
   End Try

   'Let the user know that we are setting up the session, just in case it takes more
than a second
   LHMResult.Text = "Authorizing session.Please wait."

   'The LHM cgi on the SonicWall - this does not change
   Dim loginCgi as String = "externalGuestLogin.cgi"

   'Assemble the data to post back to the SonicWall to authorize the LHM session
   Dim loginParams as String = "sessId=" & sessionId & "&userName=" &
Server.URLEncode(txtName.Text) & "&sessionLifetime=" & sessTimer & "&idleTimeout=" &
idleTimer

   'Combine mgmtBaseUrl from the original redirect with the login cgi
   Dim postToSNWL as String = mgmtBaseUrl & loginCgi
```

```
   'Convert the loginParams to a well behaved byte array
   Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

   Try
      'Create the webrequest to the SonicWall
      Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

      'Calculate the length of the byte array
      toSNWL.ContentLength = byteArray.Length

      'Set the method for the webrequest to POST
      toSNWL.Method = "POST"

      'Set the content type
      toSNWL.ContentType = "application/x-www-form-urlencoded"

      'Open the request stream
      Dim dataStream As Stream = toSNWL.GetRequestStream()

      'Write the byte array to the request stream
      dataStream.Write(byteArray, 0, byteArray.Length)

      'Close the Stream object
      dataStream.Close()

      'Get the response
      Dim snwlReply As WebResponse = toSNWL.GetResponse()

      'Display the status - looking for 200 = OK.
      'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

      'Grab the response and stuff it into an xml doc for possible review
      Dim snwlResponse as XmlDocument = New XmlDocument()
      snwlResponse.Load(snwlReply.GetResponseStream())

      'Set the xPath to the SNWL reply, and get the response
      Dim codePath as String =
"SonicWallAccessGatewayParam/AuthenticationReply/ResponseCode"

      'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

      'Response code 50 - Login Succeeded
      If snwlResponse.SelectSingleNode(codePath).InnerXml = "50"

         'Do we want to provide a logout popup window?
         If logoutPopup = "1" Then
            'Popup hack using Javascript for logout window
            Dim sb As New System.Text.StringBuilder()
            sb.Append("<script language='javascript'>")
            sb.Append("window.open('logout.aspx?sessId=")
            sb.Append(Server.URLEncode(CStr(sessionId)))
            sb.Append("&mgmtBaseUrl=")
            sb.Append(Server.URLEncode(CStr(mgmtBaseUrl)))
            sb.Append("&sessTimer=")
            sb.Append(Server.URLEncode(CStr(sessTimer)))
            sb.Append("','logOut','toolbar=no,")
            sb.Append("addressbar=no,menubar=no,")
            sb.Append("width=400,height=250');")
            sb.Append("<")
            sb.Append("/")
```

```
            sb.Append("script>")
            RegisterStartupScript("stp", sb.ToString)
         End If

         LHMResult.Text = "<br><b><font color=""green"">Session
authorized:</font></b> You may now go to the URL you originally requested: <a
target=""_blank"" href=""" & req & """>" & req & "</a>"

      'Response code 51 - Session Limit Exceeded
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "51"
         LHMResult.Text = "<br><b><font color=""red"">Session Limit
Reached:</font></b> The maximum number of guest session has been reached.Sorry for
the inconvenience.Please close and relaunch your browser to try again."

      'Response code 100 - Login Failed.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "100"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> Your session cannot be created at this time.Sorry for the
inconvenience.Please close and relaunch your browser to try again."

      'Response code 251 - Bad HMAC.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed message authentication.Sorry
for the inconvenience.Please close and relaunch your browser to try again."

      'Response code 253 - Invalid SessionID.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed to match a known session
identity.Sorry for the inconvenience.Please close and relaunch your browser to try
again."

      'Response code 254 - Invalid CGI.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization was missing an essential
parameter.Sorry for the inconvenience.Please close and relaunch your browser to try
again."

      'Response code 255 - Internal Error.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified
error.Sorry for the inconvenience.Please close and relaunch your browser to try
again."

      End If

      'Close the streams
      dataStream.Close()
      snwlReply.Close()

      'If there is some asp.net error trying to talk to the SonicWall, print it in
the same color as the background.
      Catch ex as Exception
         catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified
error.Sorry for the inconvenience.Please close and relaunch your browser to try
again.If the problem persists, please notify an attendant."
```

```
      End Try
End Sub
</script>

<STYLE>
body {
  font-size: 10pt;
  font-family: verdana,helvetica,arial,sans-serif;
  color:#000000;
  background-color:#9CBACE;
}

tr.heading {
  background-color:#006699;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Guestbook Script</TITLE>
</HEAD>

<BODY>
<form id="frmValidator" runat="server">

<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
   <tr class="heading">
      <td width="50%" valign="center"><font color="white"><b>LHM
Guestbook</b></font></td>
      <td><center><img width="216" height="51" src="<%= logo %>"></center></td>
      <td width="50%" align="right" valign="center"><font color="white"><b>Powered
by SonicWall LHM</b> </font></td>
   </tr>
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>

<table width="90%" border="0" cellpadding="2" cellspacing="0">
   <tr>
      <td>Welcome <%= ip%> to SonicWall's LHM Guestbook.In exchange for providing us
with your contact information,
      along with your permission to occasionally contact you while you are in the
middle of dinner, we will
      provide you with <b>one complimentary hour of secure Internet access.</b><br>
      </td>
   </tr>
</table>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3><font color="white"><center><b>Thank you for your
participation.</b></center></td>
   </tr>
```

```
</table>
<table width="100%" border="0" cellpadding="0" cellspacing="0">
   <tr>
      <td width="30%"><br>Enter your full name:</td>
      <td width="30%"><asp:TextBox id="txtName" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtName"
ControlToValidate="txtName" ErrorMessage="Please enter your name." runat="server"
/></td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your address:</td>
      <td width="30%"><asp:TextBox id="txtAddress" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtAddress"
ControlToValidate="txtAddress" ErrorMessage="Please enter your address."
runat="server" /></td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your city:</td>
      <td width="30%"><asp:TextBox id="txtCity" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtCity"
ControlToValidate="txtCity" ErrorMessage="Please enter your city." runat="server"
/></td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your State:</td>
      <td width="30%"><asp:TextBox id="txtState" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtState"
ControlToValidate="txtState" ErrorMessage="Please enter your State." runat="server"
/></td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your zip code:</td>
      <td width="30%"><asp:TextBox id="txtZip" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtZip"
ControlToValidate="txtZip" ErrorMessage="Please enter your zip
code."Display="Dynamic" runat="server" />
      <asp:RegularExpressionValidator id=regEx1 runat="server" Display="Dynamic"
ControlToValidate="txtZip" ErrorMessage="Please enter in the format #####"
ValidationExpression="^\d{5}"></asp:RegularExpressionValidator>
      </td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your phone number:</td>
      <td width="30%"><asp:TextBox id="txtPhone" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtPhone"
ControlToValidate="txtPhone" ErrorMessage="Please enter your phone
number."Display="Dynamic" runat="server" />
      <asp:RegularExpressionValidator id=regEx2 runat="server" Display="Dynamic"
ControlToValidate="txtPhone" ErrorMessage="Please enter in the format ###-###-####"
ValidationExpression="((\(\d{3}\)?)|(\d{3}-))?\d{3}-
\d{4}"></asp:RegularExpressionValidator>
      </td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your email address:</td>
      <td width="30%"><asp:TextBox id="txtEmail" runat="server" /></td>
      <td width="40%"><asp:RegularExpressionValidator id=regEx3 runat="server"
ControlToValidate="txtEmail" ValidationExpression=".*@.*\..*"ErrorMessage="Please
enter a valid email address."Display="Dynamic" />
      </asp:RegularExpressionValidator>
```

```
      <asp:RequiredFieldValidator id="valTxtEnail" runat="server"
ControlToValidate="txtEmail" ErrorMessage="Please enter you email
address."Display="Dynamic" />
      </asp:RequiredFieldValidator>
      </td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your web site URL (optional):</td>
      <td width="30%"><asp:TextBox id="txtURL" runat="server" /></td>
   </tr>
   <tr>
      <td valign="top" width="30%"><br>Enter a comment (optional):</td>
      <td width="30%"><asp:TextBox id="txtComment" width="300px" height="100px"
textmode="MultiLine" tabindex="4" runat="server" /></td>
   </tr>
   <tr>
      <td></td>
      <td><br><asp:button id="btnSubmit" class="button" text=" Submit "
onClick="btnSubmit_Click" runat="server" />
        
      <asp:button id="btnClear" class="button" text=" Clear All "
CausesValidation="False" onClick="OnBtnClearClicked" runat="server" />
      </td>
   </tr>
   <tr>
      <td colspan=2><asp:Label id=LHMResult runat="server" /></td>
   </tr>
   <tr>
      <td colspan=2><asp:Label id=catchError runat="server" /></td>
   </tr>
</table>
</form>
</BODY>
</HTML>
```

logout.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Data" %>
<%@ Import Namespace="System.Data.OleDB" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWall authorizing the LHM session.
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
      As Boolean Implements ICertificatePolicy.CheckValidationResult
```

```
      Return True
   End Function
End Class

'Sample LHM redirect querystring:
'http://127.0.0.1/lhm/guestbook/default.aspx?sessionId=0b712fd83b9f5313db5af1cea6b1
004f&ip=10.50.165.231&mac=00:0e:35:bd:c9:37&ufi=0006b11184300&mgmtBaseUrl=https://1
0.50.165.193:4043/&clientRedirectUrl=https://10.50.165.193:444/&req=http%3A//www.go
ogle.com/ig

Dim ip as String
Dim sessionId as String
Dim mac as String
Dim ufi as String
Dim mgmtBaseUrl as String
Dim clientRedirectUrl as String
Dim req as String
Dim hmac as String
Dim customCode as String

Sub Page_Load(src as Object, e as EventArgs)

   LHMResult.Text=""
   catchError.Text=""

   ip=Request.QueryString("ip")
   sessionId=Request.QueryString("sessionId")
   mac=Request.QueryString("mac")
   ufi=Request.QueryString("ufi")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
   clientRedirectUrl=Request.QueryString("clientRedirectUrl")
   req=Request.QueryString("req")
   hmac=Request.QueryString("hmac")
   customCode=Request.QueryString("cc")

   'customCode grabs the "cc=" querystring value sent by the SonicWall.This allows
you to use the same
   'page (e.g. this page) for the "Session Expiration" (?cc=2), "Idle Timeout"
(?cc=3) and "Max Sessions" (?cc=4) page.
   If customCode <> "" Then
      Select Case customCode
      Case "2"
         LHMResult.Text="<br><H3><font color=""red"">Your LHM session has expired.You
may try to initiate a new session.</font></H3>"
      Case "3"
         LHMResult.Text="<br><H3><font color=""red"">You have exceeded your idle
timeout.Please log back in.</font></H3>"
      Case "4"
         LHMResult.Text="<br><H3><font color=""red"">The maximum number of sessions
has been reached.Please try again later.</font></H3>"
      End Select
   End If

   'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWall
   'This is necessary for the POST to the SonicWall authorizing the LHM session.
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   'Note - the routine below for handling the hmac requires the use of the
SonicSSL.dll and libeay.dll libraries.
```

```
   'The DLL must be copied to the IIS server, and the SonicSSL dll must be registered
with "regsvr32 sonicssl.dll"
   If hmac <> "" Then

      'SonicWall URL Encode routine is different from Microsoft - this is the
SonicWall method
      req=Replace(req,"%","%25")
      req=Replace(req,":","%3A")
      req=Replace(req," ","%20")
      req=Replace(req,"?","%3F")
      req=Replace(req,"+","%2B")
      req=Replace(req,"&","%26")
      req=Replace(req,"=","%3D")

      Dim strHmacText as String
      Dim objCrypto as Object
      Dim strHmacGenerated
      Dim loginError as String

      'Initialize the Crypto object
      objCrypto = Server.CreateObject("SonicSSL.Crypto")

      'The text to be encoded
      strHmacText = sessionId & ip & mac & ufi & mgmtBaseUrl & clientRedirectUrl &
req

      'Calculate the hash with a key strHmac, the return value is a string converted
form the output sha1 binary.
      'The hash algorithm (MD5 or SHA1) is configured in myvars and in the Extern
Guest Auth config on the SonicWall
      If hmacType = "MD5" Then
         strHmacGenerated = objCrypto.hmac_md5(strHmacText, strHmac)
      Else
         strHmacGenerated = objCrypto.hmac_sha1(strHmacText, strHmac)
      End If

      If strHmacGenerated <> hmac Then
         Dim hmacFail as String
         hmacFail = "<font color=""red"">The HMAC failed validation.Please notify an
attendant.</font><br><br>"
         hmacFail+="<font color=""9CBACE"">Received HMAC: " & hmac & "<br>Calculated
HMAC: " & strHmacGenerated & "<br>"
         hmacFail+="Make sure the digest functions on the SonicWall and LHM server
match.<br>"
         hmacFail+="Also make sure the shared secret on the SonicWall and myvars
match</font>"
         catchError.Text=hmacFail
      End If

   End If

End Sub

sub OnBtnClearClicked (Sender As Object, e As EventArgs)
   txtName.Text = ""
   txtAddress.Text = ""
   txtCity.Text = ""
   txtState.Text = ""
   txtZip.Text = ""
   txtPhone.Text = ""
   txtEMail.Text = ""
```

```
   txtURL.Text = ""
   txtComment.Text = ""
   LHMResult.Text=""
   catchError.Text=""
end sub

Sub btnSubmit_Click(Sender As Object, E As EventArgs)

   Try
      'Try to write the submitted info to the database file
      Dim strConn as string = "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" &
server.mappath("guestbook.mdb") & ";"

      Dim MySQL as string = "INSERT INTO Guestbook (Name, Address, City, State, Zip,
Phone, EMail, URL, Comment) VALUES ('" & txtName.Text & "','" & txtAddress.Text &
"','" & txtCity.Text & "','" & txtState.Text & "','" & txtZip.Text & "','" &
txtPhone.Text & "','" & txtEMail.Text & "','" & txtURL.Text & "','" &
txtComment.Text & "')"
      Dim MyConn as New OleDBConnection (strConn)
      Dim cmd as New OleDBCommand (MySQL, MyConn)
      MyConn.Open ()
      cmd.ExecuteNonQuery ()
      MyConn.Close ()

      Catch ex as Exception
         catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
   End Try

   'Let the user know that we are setting up the session, just in case it takes more
than a second
   LHMResult.Text = "Authorizing session.Please wait."

   'The LHM cgi on the SonicWall - this does not change
   Dim loginCgi as String = "externalGuestLogin.cgi"

   'Assemble the data to post back to the SonicWall to authorize the LHM session
   Dim loginParams as String = "sessId=" & sessionId & "&userName=" &
Server.URLEncode(txtName.Text) & "&sessionLifetime=" & sessTimer & "&idleTimeout=" &
idleTimer

   'Combine mgmtBaseUrl from the original redirect with the login cgi
   Dim postToSNWL as String = mgmtBaseUrl & loginCgi

   'Convert the loginParams to a well behaved byte array
   Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

   Try
      'Create the webrequest to the SonicWall
      Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

      'Calculate the length of the byte array
      toSNWL.ContentLength = byteArray.Length

      'Set the method for the webrequest to POST
      toSNWL.Method = "POST"

      'Set the content type
      toSNWL.ContentType = "application/x-www-form-urlencoded"

      'Open the request stream
      Dim dataStream As Stream = toSNWL.GetRequestStream()
```

```
      'Write the byte array to the request stream
      dataStream.Write(byteArray, 0, byteArray.Length)

      'Close the Stream object
      dataStream.Close()

      'Get the response
      Dim snwlReply As WebResponse = toSNWL.GetResponse()

      'Display the status - looking for 200 = OK.
      'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

      'Grab the response and stuff it into an xml doc for possible review
      Dim snwlResponse as XmlDocument = New XmlDocument()
      snwlResponse.Load(snwlReply.GetResponseStream())

      'Set the xPath to the SNWL reply, and get the response
      Dim codePath as String =
"SonicWallAccessGatewayParam/AuthenticationReply/ResponseCode"

      'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

      'Response code 50 - Login Succeeded
      If snwlResponse.SelectSingleNode(codePath).InnerXml = "50"

         'Do we want to provide a logout popup window?
         If logoutPopup = "1" Then
            'Popup hack using Javascript for logout window
            Dim sb As New System.Text.StringBuilder()
            sb.Append("<script language='javascript'>")
            sb.Append("window.open('logout.aspx?sessId=")
            sb.Append(Server.URLEncode(CStr(sessionId)))
            sb.Append("&mgmtBaseUrl=")
            sb.Append(Server.URLEncode(CStr(mgmtBaseUrl)))
            sb.Append("&sessTimer=")
            sb.Append(Server.URLEncode(CStr(sessTimer)))
            sb.Append("','logOut','toolbar=no,")
            sb.Append("addressbar=no,menubar=no,")
            sb.Append("width=400,height=250');")
            sb.Append("<")
            sb.Append("/")
            sb.Append("script>")
            RegisterStartupScript("stp", sb.ToString)
         End If

         LHMResult.Text = "<br><b><font color=""green"">Session
authorized:</font></b> You may now go to the URL you originally requested: <a
target=""_blank"" href=""" & req & """>" & req & "</a>"

      'Response code 51 - Session Limit Exceeded
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "51"
         LHMResult.Text = "<br><b><font color=""red"">Session Limit
Reached:</font></b> The maximum number of guest session has been reached.Sorry for
the inconvenience.Please close and relaunch your browser to try again."

      'Response code 100 - Login Failed.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "100"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> Your session cannot be created at this time.Sorry for the
inconvenience.Please close and relaunch your browser to try again."
```

```
      'Response code 251 - Bad HMAC.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed message authentication.Sorry
for the inconvenience.Please close and relaunch your browser to try again."

      'Response code 253 - Invalid SessionID.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed to match a known session
identity.Sorry for the inconvenience.Please close and relaunch your browser to try
again."

      'Response code 254 - Invalid CGI.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization was missing an essential
parameter.Sorry for the inconvenience.Please close and relaunch your browser to try
again."

      'Response code 255 - Internal Error.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified
error.Sorry for the inconvenience.Please close and relaunch your browser to try
again."

      End If

      'Close the streams
      dataStream.Close()
      snwlReply.Close()

      'If there is some asp.net error trying to talk to the SonicWall, print it in
the same color as the background.
      Catch ex as Exception
         catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified
error.Sorry for the inconvenience.Please close and relaunch your browser to try
again.If the problem persists, please notify an attendant."
      End Try
End Sub
</script>

<STYLE>
body {
  font-size: 10pt;
  font-family: verdana,helvetica,arial,sans-serif;
  color:#000000;
  background-color:#9CBACE;
}

tr.heading {
  background-color:#006699;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
```

```
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Guestbook Script</TITLE>
</HEAD>

<BODY>
<form id="frmValidator" runat="server">

<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
   <tr class="heading">
      <td width="50%" valign="center"><font color="white"><b>LHM
Guestbook</b></font></td>
      <td><center><img width="216" height="51" src="<%= logo %>"></center></td>
      <td width="50%" align="right" valign="center"><font color="white"><b>Powered
by SonicWall LHM</b> </font></td>
   </tr>
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>

<table width="90%" border="0" cellpadding="2" cellspacing="0">
   <tr>
      <td>Welcome <%= ip%> to SonicWall's LHM Guestbook.In exchange for providing us
with your contact information,
      along with your permission to occasionally contact you while you are in the
middle of dinner, we will
      provide you with <b>one complimentary hour of secure Internet access.</b><br>
      </td>
   </tr>
</table>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3><font color="white"><center><b>Thank you for your
participation.</b></center></td>
   </tr>
</table>
<table width="100%" border="0" cellpadding="0" cellspacing="0">
   <tr>
      <td width="30%"><br>Enter your full name:</td>
      <td width="30%"><asp:TextBox id="txtName" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtName"
ControlToValidate="txtName" ErrorMessage="Please enter your name." runat="server"
/></td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your address:</td>
      <td width="30%"><asp:TextBox id="txtAddress" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtAddress"
ControlToValidate="txtAddress" ErrorMessage="Please enter your address."
runat="server" /></td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your city:</td>
      <td width="30%"><asp:TextBox id="txtCity" runat="server" /></td>
```

```
      <td width="40%"><asp:RequiredFieldValidator id="valTxtCity"
ControlToValidate="txtCity" ErrorMessage="Please enter your city." runat="server"
/></td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your State:</td>
      <td width="30%"><asp:TextBox id="txtState" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtState"
ControlToValidate="txtState" ErrorMessage="Please enter your State." runat="server"
/></td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your zip code:</td>
      <td width="30%"><asp:TextBox id="txtZip" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtZip"
ControlToValidate="txtZip" ErrorMessage="Please enter your zip
code."Display="Dynamic" runat="server" />
      <asp:RegularExpressionValidator id=regEx1 runat="server" Display="Dynamic"
ControlToValidate="txtZip" ErrorMessage="Please enter in the format #####"
ValidationExpression="^\d{5}"></asp:RegularExpressionValidator>
      </td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your phone number:</td>
      <td width="30%"><asp:TextBox id="txtPhone" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtPhone"
ControlToValidate="txtPhone" ErrorMessage="Please enter your phone
number."Display="Dynamic" runat="server" />
      <asp:RegularExpressionValidator id=regEx2 runat="server" Display="Dynamic"
ControlToValidate="txtPhone" ErrorMessage="Please enter in the format ###-###-####"
ValidationExpression="((\(\d{3}\)?)|(\d{3}-))?\d{3}-
\d{4}"></asp:RegularExpressionValidator>
      </td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your email address:</td>
      <td width="30%"><asp:TextBox id="txtEmail" runat="server" /></td>
      <td width="40%"><asp:RegularExpressionValidator id=regEx3 runat="server"
ControlToValidate="txtEmail" ValidationExpression=".*@.*\..*"ErrorMessage="Please
enter a valid email address."Display="Dynamic" />
      </asp:RegularExpressionValidator>
      <asp:RequiredFieldValidator id="valTxtEnail" runat="server"
ControlToValidate="txtEmail" ErrorMessage="Please enter you email
address."Display="Dynamic" />
      </asp:RequiredFieldValidator>
      </td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your web site URL (optional):</td>
      <td width="30%"><asp:TextBox id="txtURL" runat="server" /></td>
   </tr>
   <tr>
      <td valign="top" width="30%"><br>Enter a comment (optional):</td>
      <td width="30%"><asp:TextBox id="txtComment" width="300px" height="100px"
textmode="MultiLine" tabindex="4" runat="server" /></td>
   </tr>
   <tr>
      <td></td>
      <td><br><asp:button id="btnSubmit" class="button" text="  Submit  "
onClick="btnSubmit_Click" runat="server" />
        
```

```
      <asp:button id="btnClear" class="button" text=" Clear All "
CausesValidation="False" onClick="OnBtnClearClicked" runat="server" />
      </td>
   </tr>
   <tr>
      <td colspan=2><asp:Label id=LHMResult runat="server" /></td>
   </tr>
   <tr>
      <td colspan=2><asp:Label id=catchError runat="server" /></td>
   </tr>
</table>
</form>
</BODY>
</HTML>
```

myvars.aspx

```
<script language="VB" runat="server">

'Set the logoutPopup window flag - 0 = no popup, 1 = popup
'The use of the logoutPopup in this script is discouraged because although the login
event
'is non-exclusive, the login event produces data where redundancy is undesirable.
Dim logoutPopup as String = "0"

'Set the LHM Session Timeout
Dim sessTimer as String = "3600"

'Set the LHM Idle Timeout
Dim idleTimer as String = "300"

'Set the secret for use with optional HMAC auth, as configured in the Extern Guest
Auth config on the SonicWall
Dim strHmac as String = "password"

'Set the digest method for the HMAC, either MD5 or SHA1
Dim hmacType as String = "MD5"
'Dim hmacType as String = "SHA1"

'Set the logo image to use
Dim logo as String = "SonicWall.gif"

'------------------------End of Configurable Settings-------------------------

</script>
```

LHMQuiz スクリプト

認証モデル

ゲスト クライアントは簡単な試験を受けます。合格スコアが認証の資格情報となります。

目的

ネットワーク アクセスが授業の環境で提供されることはよくあります。取り上げられている教材のテストの合格スコアを認証の手段として使用することで、インストラクタは、コースの教材内容が習得されたことを確認でき、インターネットへの抑えがたい衝動によって受講者の集中力が低下することもありません。また、このスクリプトは合格したテストを受験者に、不合格となったテストを試験監督/インストラクタに電子メールでそれぞれ送信します。

myvars 変数

logoutPopup	ログアウト ポップアップ ウィンドウの使用を制御します。次のように設定します。 • **0**: ポップアップ ウィンドウを無効にします。 • **1**: ポップアップ ウィンドウを有効にします。
passingScore	試験に合格するために必要なスコア (百分率を表す整数)。
quizFile	試験の XML ソースのファイル名 (quiz.xml、shortquiz.xml など)。
quizName	スクリプト全体で使用される、試験の名前。
quizFrom	試験内容を電子メールで送信する際に使用される From: email アドレス。
quizTo	不合格となった試験が送信される To: email アドレス (試験監督やインストラクタのアドレス)。
imagePath	電子メールには正解および不正解の答えに関する添付ファイルが含まれます。この変数はそうした画像ファイルのパスを設定します。通常、スクリプト ファイルそのものと同じパスに設定します。
smtpServer	試験の結果を配信するために使用される SMTP サーバの IP アドレスまたは解決可能な FQDN です。ローカルの IIS SMTP サーバ インスタンスを使用する場合は、127.0.0.1 に設定できます。
sessTimer	秒単位のセッション タイマー。
idleTimer	秒単位の無動作タイマー。
strHmac	オプションの HMAC 機能のための事前共有鍵。
hmacType	HMAC 使用時に用いるダイジェスト種別: 「**MD5**」または「**SHA1**」を選択します。
logo	ページ ヘッダーで使用するロゴ (画像) ファイルの名前。

セッション フロー

1. ゲスト クライアントは自分のフルネームと電子メール アドレスを入力するように求められます。完了後の合格試験を配信するために、正しく有効な電子メール アドレスが必要です。
2. 名前と電子メールの入力後、ゲスト クライアントは quiz.aspx ページにリダイレクトされます。そこでは多肢選択式の試験が実施されます。
3. 試験の問題そのものは、quiz.xsd (XML スキーマ定義) ファイルで定義された quiz.xml ファイルに含まれています。quiz.xml ファイルを編集すると試験の内容をカスタマイズできますが、quiz.xsd ドキュメントは確実に必要な場合以外は編集しないでください。

   次の 2 つのバージョンの試験が含まれています。quiz.xml (10 問含まれています) と shortquiz.xml (スクリプトの動作確認のために 2 問だけ含まれています) です。この試験は任意の数の問題をサポートしています。また、各問題は任意の数の選択肢をサポートしていますが、そのうち 1 つの選択肢だけを correct=yes によって正解としてマークする必要があります。用意されている quiz.xml ファイルは、必要に応じて、きわめて直接的な方法で変更できます。

4 試験の最後には、結果が表示されます。スコアによって動作は次のように異なります。

- スコアが足らずに不合格となった場合、試験結果はインストラクタ (myvars で定義されている電子メール アドレス) に電子メールで送信され、ゲスト クライアントは試験をもう一度受けるように促されます。LHM セッションは承認されません。
- 合格スコアをクリアした場合、試験結果は受験者に電子メールで送信され、LHM セッションは承認されます。

電子メール送信の対象となる試験は HTML 形式で送信され、そこには checkmark.gif と block.gif という (正解および不正解を示す) グラフィックスが電子メールに表示できるように含まれています。

5 試験に合格した場合、LHM ポスト文字列は、sessionID、ユーザ名 (ウェブフォームで入力されたもの)、既定のセッション存続期間、および無動作存続期間で構成されます。

6 スクリプトは、セッションを承認するために SonicWall セキュリティ装置に対する LHM ポストを実行します。

追加の考慮事項

試験結果を配信するには SMTP サーバへのアクセスが必要です。スクリプトではこのサーバによって電子メールをリレーするため、SMTP サーバは LHM サーバからのリレーを許可するように設定されている必要があります。これを実現する最も適切な方法は、LHM サーバの IP アドレスからのリレーを許可するように SMTP サーバを設定することです。

ほとんどの IIS インストールにはローカル SMTP サーバが含まれているので、このローカル SMTP サーバを電子メール配信のために使用すると便利です。そのためには、myvars の smtpServer 変数を 127.0.0.1 に設定します。

ローカル SMTP サーバを電子メール配信のために使用する場合でも、リレーを許可する必要があります。ほとんどの設定では、以下の方法でこれを実行します。

1 IIS MMC コンフィギュレータに移動します。

2 「**既定の SMTP 仮想サーバ**」を右クリックします。

3 「**プロパティ**」を選択します。

4 「**アクセス**」を選択します。

5 「**リレー**」を選択します。

6 アクセス許可リストにアドレス 127.0.0.1 を追加します。

非ローカルの SMTP サーバを使用する場合、その SMTP サーバは、LHM サーバがそれ自体の実際の IP アドレスによってリレーを行うことを許可するように設定されている必要があります。

トピック:

- default.aspx (910 ページ)
- logout.aspx (913 ページ)
- myvars.aspx (919 ページ)
- quiz.aspx (920 ページ)

default.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>

<!-- #INCLUDE file="myvars.aspx" -->

<script runat="server">

'Sample LHM redirect querystring:
'http://10.50.165.231/xmlquiz/default.aspx?sessionId=0b712fd83b9f5313db5af1cea6b1004f&ip=10.50.165.231&mac=00:0e:35:bd:c9:37&ufi=0006b11184300&mgmtBaseUrl=https://10.50.165.193:4043/&clientRedirectUrl=https://10.50.165.193:444/&req=http%3A//www.google.com/ig

Dim ip as String
Dim sessionId as String
Dim mac as String
Dim ufi as String
Dim mgmtBaseUrl as String
Dim clientRedirectUrl as String
Dim req as String
Dim hmac as String
Dim emailAddr as String
Dim userName as String
Dim customCode as String

Sub Page_Load(src as Object, e as EventArgs)
   ip=Request.QueryString("ip")
   sessionId=Request.QueryString("sessionId")
   mac=Request.QueryString("mac")
   ufi=Request.QueryString("ufi")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
   clientRedirectUrl=Request.QueryString("clientRedirectUrl")
   req=Request.QueryString("req")
   hmac=Request.QueryString("hmac")
   customCode=Request.QueryString("cc")

   'customCode grabs the "cc=" querystring value sent by the SonicWall.This allows you to use the same
   'page (e.g. this page) for the "Session Expiration" (?cc=2), "Idle Timeout" (?cc=3) and "Max Sessions" (?cc=4) page.
   If customCode <> "" Then
      Select Case customCode
      Case "2"
         LHMResult.Text="<br><H3><font color=""red"">Your LHM session has expired.You may try to initiate a new session.</font></H3>"
      Case "3"
         LHMResult.Text="<br><H3><font color=""red"">You have exceeded your idle timeout.Please log back in.</font></H3>"
      Case "4"
         LHMResult.Text="<br><H3><font color=""red"">The maximum number of sessions has been reached.Please try again later.</font></H3>"
      End Select
   End If

   'Note - the routine below for handling the hmac requires the use of the SonicSSL.dll and libeay.dll libraries.
   'The DLL must be copied to the IIS server, and the SonicSSL dll must be registered with "regsvr32 sonicssl.dll"
   If hmac <> "" Then
```

```
      'SonicWall URL Encode routine is different from Microsoft - this is the
SonicWall method
      req=Replace(req,"%","%25")
      req=Replace(req,":","%3A")
      req=Replace(req," ","%20")
      req=Replace(req,"?","%3F")
      req=Replace(req,"+","%2B")
      req=Replace(req,"&","%26")
      req=Replace(req,"=","%3D")

      Dim strHmacText as String
      Dim objCrypto as Object
      Dim strHmacGenerated
      Dim loginError as String

      'Initialize the Crypto object
      objCrypto = Server.CreateObject("SonicSSL.Crypto")

      'The text to be encoded
      strHmacText = sessionId & ip & mac & ufi & mgmtBaseUrl & clientRedirectUrl &
req

      'Calculate the hash with a key strHmac, the return value is a string converted
form the output sha1 binary.
      'The hash algorithm (MD5 or SHA1) is configured in myvars and in the Extern
Guest Auth config on the SonicWall
      If hmacType = "MD5" Then
         strHmacGenerated = objCrypto.hmac_md5(strHmacText, strHmac)
      Else
         strHmacGenerated = objCrypto.hmac_sha1(strHmacText, strHmac)
      End If

      If strHmacGenerated <> hmac Then
         Dim hmacFail as String
         hmacFail = "<font color=""red"">The HMAC failed validation.Please notify an
attendant.</font><br><br>"
         hmacFail+="<font color=""9CBACE"">Received HMAC: " & hmac & "<br>Calculated
HMAC: " & strHmacGenerated & "<br>"
         hmacFail+="Make sure the digest functions on the SonicWall and LHM server
match.<br>"
         hmacFail+="Also make sure the shared secret on the SonicWall and myvars
match</font>"
         catchError.Text=hmacFail
      End If

   End If

End Sub

'When the submit button is clicked, pass the variables we need and load the quiz
Sub btnSubmit_Click(Sender As Object, E As EventArgs)

   Context.Items.Add("req", req)
   Context.Items.Add("sessionId", sessionId)
   Context.Items.Add("emailAddr",clientEmail.Text)
   Context.Items.Add("userName",clientName.Text)
   Context.Items.Add("mgmtBaseUrl",mgmtBaseUrl)
   Server.Transfer("quiz.aspx",true)

End Sub
```

```
</script>

<STYLE>
body {
  font-size: 10pt;
  font-family: verdana,helvetica,arial,sans-serif;
  color:#000000;
  background-color:#9CBACE;
}

tr.heading {
  background-color:#006699;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Quiz Script</TITLE>
</HEAD>

<BODY>
<form id="frmValidator" runat="server">

<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
   <tr class="heading">
      <td width="50%" valign="center"><font color="white"><b>LHM Quiz
Authorization</b></font></td>
      <td><center><img width="216" height="51" src="SonicWall.gif"></center></td>
      <td width="50%" align="right" valign="center"><font color="white"><b>Powered
by SonicWall LHM</b> </font></td>
   </tr>
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr>
      <td width="30%"><br>Enter your full name:</td>
      <td width="20%"><asp:TextBox id="clientName" runat="server" /></td>
      <td ><asp:RequiredFieldValidator id="valTxtName"
ControlToValidate="clientName" ErrorMessage="Please enter your
name."Display="Dynamic" runat="server" /></td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your real email address:</td>
      <td width="20%"><asp:TextBox id="clientEmail" runat="server" /></td>
      <td ><asp:RegularExpressionValidator id="fromEmail" runat="server"
ControlToValidate="clientEmail"
ValidationExpression=".*@.*\..*"ErrorMessage="Please enter a valid email
address."Display="Dynamic" />
      </asp:RegularExpressionValidator>
```

```
      <asp:RequiredFieldValidator id="fromRequired" runat="server"
ControlToValidate="clientEmail" ErrorMessage="Please enter your email
address."Display="Dynamic" />
      </asp:RequiredFieldValidator>
      </td>
   </tr>
   <tr>
      <td></td>
      <td><asp:button id="btnSubmit" class="button" text="  Submit  "
onClick="btnSubmit_Click" runat="server" /><br></td>
   </tr>

   <tr class="heading">
      <td colspan=3 align="left"><font color="white"><b>Welcome Quiztaker <%=
ip%></b></font></td>
   </tr>
</table>
<table width="70%" border="0" cellpadding="2" cellspacing="0">
   <tr>
      <td>
      <br>You have been redirected here by Lightweight Hotspot Messaging.
      This environment has been setup to demonstrate the flexibility of LHM,
including
      support for both wired and wireless clients, and also the ability for LHM to
use
      more than just username and password authentication for providing
access.<br><br>
      The page that you are about to continue on to is a <%= quizName %> written in
ASP.net.
      A passing score of <%= passingScore%>% will serve as the authentication for
LHM, and will grant
      you network access.You must pass the test to continue, and will be prompted to
retake
      the entire quiz if you you do not pass.<br><br>
      When you are done, the completed test will be emailed to you at the address you
      specify above.<br><br>
      So it's not just a good way to prove your understanding of some
      key SonicOS concepts, but also a practical example of the versatility of LHM.
      </td>
   </tr>
   <tr>
      <td><asp:Label id=LHMResult runat="server" /></td>
   </tr>
   <tr>
      <td colspan=2><asp:Label id=catchError runat="server" /></td>
   </tr>
</table>
</form>
</BODY>
</HTML>
```

logout.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
```

```
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWall authorizing the LHM session.
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
      As Boolean Implements ICertificatePolicy.CheckValidationResult
      Return True
   End Function
End Class

Dim sessionId as String
Dim mgmtBaseUrl as String
Dim eventId as String = "&eventId=1"

'Grab the code and the session lifetime from the generator page
Sub Page_Load(src as Object, e as EventArgs)
   sessionId=Request.QueryString("sessId")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
   sessTimer=Request.QueryString("sessTimer")


   'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWall
   'This is necessary for the POST to the SonicWall authorizing the LHM session.
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   'When the page loads, make the loggedIn span visible
   loggedIn.Visible=True
   loggedOut.Visible=False

   Me.Button1.Attributes.Add("OnClick", "self.close()")

End Sub

'The Logout button
Sub btnSubmit_Click(Sender As Object, E As EventArgs)

   'Let the user know that we are setting up the session, just in case it takes more
than a second
   LHMResult.Text = "Authorizing session.Please wait."

   'The LHM cgi on the SonicWall - this does not change
   Dim loginCgi as String = "externalGuestLogoff.cgi"

   'Assemble the data to post back to the SonicWall to authorize the LHM session
   Dim loginParams as String = "sessId=" & sessionId & eventId

   'Combine mgmtBaseUrl from the original redirect with the login cgi
   Dim postToSNWL as String = mgmtBaseUrl & loginCgi

   'Convert the loginParams to a well behaved byte array
   Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)
```

```
   Try
      'Make the loggedOut span visible
      loggedIn.Visible=False
      loggedOut.Visible=True

      'Create the webrequest to the SonicWall
      Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

      'Calculate the length of the byte array
      toSNWL.ContentLength = byteArray.Length

      'Set the method for the webrequest to POST
      toSNWL.Method = "POST"

      'Set the content type
      toSNWL.ContentType = "application/x-www-form-urlencoded"

      'Open the request stream
      Dim dataStream As Stream = toSNWL.GetRequestStream()

      'Write the byte array to the request stream
      dataStream.Write(byteArray, 0, byteArray.Length)

      'Close the Stream object
      dataStream.Close()

      'Get the response
      Dim snwlReply As WebResponse = toSNWL.GetResponse()

      'Display the status - looking for 200 = OK.
      'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

      'Grab the response and stuff it into an xml doc for possible review
      Dim snwlResponse as XmlDocument = New XmlDocument()
      snwlResponse.Load(snwlReply.GetResponseStream())

      'Set the xPath to the SNWL reply, and get the response
      Dim codePath as String =
"SonicWallAccessGatewayParam/LogoffReply/ResponseCode"

      'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

      'Response code 150 - Logout Succeeded
      If snwlResponse.SelectSingleNode(codePath).InnerXml = "150"
        LHMResult.Text = "<br><b><font color=""green"">Your session has been logged
out.<br><br>Thank you for using LHM Guest Services.</font></b>"

      'Response code 251 - Bad HMAC.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed message authentication.Sorry for the
inconvenience.Please close and relaunch your browser to try again."

      'Response code 253 - Invalid SessionID.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed to match a known session identity.Sorry for
the inconvenience.Please close and relaunch your browser to try again."

      'Response code 254 - Invalid CGI.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
```

```
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request was missing an essential parameter.Sorry for the
inconvenience.Please close and relaunch your browser to try again."

      'Response code 255 - Internal Error.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error.Sorry for the
inconvenience.Please close and relaunch your browser to try again."

      End If

      'Close the streams
      dataStream.Close()
      snwlReply.Close()

      'If there is some asp.net error trying to talk to the SonicWall, print it in
the same color as the background.
      Catch ex as Exception
        catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error.Sorry for the
inconvenience.Please close and relaunch your browser to try again.If the problem
persists, please notify an attendant."
      End Try
End Sub

</script>
<STYLE>
body {
   font-size: 10pt;
   font-family: verdana,helvetica,arial,sans-serif;
   color:#000000;
   background-color:#9CBACE;
}

tr.heading {
   font-size: 10pt;
   background-color:#006699;
}

tr.smalltext {
   font-size: 8pt;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
   font-size: 8pt;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Logout Page</TITLE>

<SCRIPT LANGUAGE="Javascript">

//'Javascript Seconds Countdown Timer
var SecondsToCountDown = <%= sessTimer%>;
var originalTime=" ";
```

```
function CountDown()
{
   clockStr="";

   dayStr=Math.floor(SecondsToCountDown/86400)%100000
   if(dayStr>0){
      if(dayStr>1){
         dayStr+=" days ";
      } else dayStr+=" day ";
      clockStr=dayStr;
   }
   hourStr=Math.floor(SecondsToCountDown/3600)%24
   if(hourStr>0){
      if(hourStr>1){
         hourStr+=" hours ";
      } else hourStr+=" hour ";
      clockStr+=hourStr;
   }
   minuteStr=Math.floor(SecondsToCountDown/60)%60
   if(minuteStr>0){
      if(minuteStr>1){
         minuteStr+=" minutes ";
      } else minuteStr+=" minute ";
      clockStr+=minuteStr;
   }
   secondStr=Math.floor(SecondsToCountDown/1)%60
   if(secondStr>0){
      if(secondStr>1){
         secondStr+=" seconds ";
      } else secondStr+=" second ";
      clockStr+=secondStr;
   }

   if(SecondsToCountDown > 0)
   {
      --SecondsToCountDown;
   }

   if(originalTime.length < 2)
   {
      originalTime = clockStr;
   }

   // Make sure the form is still there before trying to set a value
   if(document.frmValidator){
      document.frmValidator.originalTime.value = originalTime;
      document.frmValidator.countdown.value = clockStr;
   }

   setTimeout("CountDown()", 1000);
   if(SecondsToCountDown == 0)
   {
      document.frmValidator.countdown.value = "Session Expired";
   }
}

//'Disable right-click so that the window doesn't get refreshed since the countdown
is clientside.
document.oncontextmenu = disableRightClick;
function disableRightClick()
```

```
{
  return false;
}

//'Disable F5 key, too, on IE at least.
function noF5()
{
   var key_f5 = 116;
   if (key_f5==event.keyCode)
   {
      event.keyCode=0;
      return false;
   }
   return false;
}

document.onkeydown=noF5
document.onmousedown=disableRightClick

</SCRIPT>

</HEAD>

<BODY onload='CountDown()'>
<span id="loggedIn" runat="server">
<form id="frmValidator" runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"><font color="white"><b>SonicWall LHM Logout
Window</b></font></td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="smalltext"><td><br></td></tr>
   <tr class="smalltext">
      <td>Original Session Time:</td>
      <td><asp:textbox width=250 id="originalTime" runat="server" /></td>
   </tr>
   <tr class="smalltext">
      <td>Remaining Session Time:</td>
      <td><asp:textbox width=250 id="countdown" runat="server" /></td>
   </tr>
   <tr class="smalltext">
      <td colspan=2><br>You may use this window to manually logout your session at
any time, or you may safely close this window if you prefer to let your session
timeout automatically.</font></td>
   </td>
   <tr>
      <td colspan=2><center><asp:button id="btnSubmit" class="button" text="  Logout
" onClick="btnSubmit_Click" runat="server" /></center></td>
   </tr>
</table>
</form>
</span>

<span id="loggedOut" runat="server">
<form id="logout" runat="server">
```

```
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"><font color="white"><b>SonicWall LHM Logout
Window</b></font></td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr>
      <td><asp:Label id=LHMResult runat="server" /></td>
   </tr>
   <tr>
      <td><asp:Label id=catchError runat="server" /></td>
   </tr>
   <tr><td><br></td></tr>
   <tr>
      <td><center><asp:button id="Button1" class="button" text="  Close  "
runat="server" /></center></td>
   </tr>
</table>
</form>
</span>

</BODY>
</HTML>
```

myvars.aspx

```
<script language="VB" runat="server">

'Set the logoutPopup window flag - 0 = no popup, 1 = popup
'The use of the logoutPopup in this script is discouraged because although the login
event
'is non-exclusive, the login event produces data where redundancy is undesirable.
Dim logoutPopup as String = "0"

'Set the passing score
Dim passingScore as Integer = 80

'Set the filename of the quiz XML source
Dim quizFile as String = "quiz.xml"
'Dim quizFile as String = "shortquiz.xml"

'Set the name of the Quiz
Dim quizName as String = "SonicOS Quiz"

'Set the emailed quiz results "from" email address
Dim quizFrom as String = "joelevy@SonicWall.com"

'Set the email address to send failed test results to (the proctor/instructor)
Dim quizTo as String = "joelevy@SonicWall.com"

'Set the path for check and block embedded images - usually the same path as the quiz
Dim imagePath as String = "C:\inetpub\wwwroot\lhm\lhmquiz\"

'Set the IP or resolvable FQDN for the SMTP Server
```

```
'Make sure the server is configured to relay from the IP address of this server
'If setting to 127.0.0.1 (local IIS SMTP), you need to allow IIS SMTP to relay from
127.0.0.1
Dim smtpServer as String = "127.0.0.1"

'Set the LHM Session Timeout
Dim sessTimer as String = "86400"

'Set the LHM Idle Timeout
Dim idleTimer as String = "3600"

'Set the secret for use with optional HMAC auth, as configured in the Extern Guest
Auth config on the SonicWall
Dim strHmac as String = "password"

'Set the digest method for the HMAC, either MD5 or SHA1
Dim hmacType as String = "MD5"
'Dim hmacType as String = "SHA1"

'Set the logo image to use
Dim logo as String = "SonicWall.gif"

'------------------------End of Configurable Settings-------------------------

</script>
```

quiz.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>
<%@ Import Namespace="System.Web" %>
<%@ Import Namespace="System.Web.Mail" %>

<!-- Original quiz code from www.codeproject.com -->

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWall authorizing the LHM session.
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
      As Boolean Implements ICertificatePolicy.CheckValidationResult
      Return True
   End Function
End Class

'Set the path to the XML quiz data
Dim strXmlFilePath as String = Server.MapPath(quizFile)
```

```
'Setup our variables
Dim emailAddr as String
Dim userName as String
Dim req as String
Dim sessionId as String
Dim mgmtBaseUrl as String
Dim xDoc as XmlDocument = New XmlDocument()
Dim intTotalQuestion as Integer
Dim intQuestionNo as Integer = 1
Dim intScore as Integer = 0
Dim arrAnswerHistory as new ArrayList()
Dim arrRightOrWrong as new ArrayList()
Dim arrCorrect as new ArrayList()

Sub Page_Load(src as Object, e as EventArgs)

   LHMResult.Text=""
   catchError.Text=""

   'Grab context items set in default.aspx
   emailAddr = Context.Items("emailAddr")
   userName = Context.Items("userName")
   req = Context.Items("req")
   sessionId = Context.Items("sessionId")
   mgmtBaseUrl = Context.Items("mgmtBaseUrl")

   'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWall
   'This is necessary for the POST to the SonicWall authorizing the LHM session.
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   'Load xml data
   xDoc.Load(strXmlFilePath)

   'Start a new quiz?
   If Not Page.IsPostBack Then

      'Yes.Count total question
      intTotalQuestion = xDoc.SelectNodes("/quiz/mchoice").Count

      'Record start time
      ViewState("StartTime") = DateTime.Now

      ShowQuestion(intQuestionNo)
   End If
End Sub

Sub btnSubmit_Click(src as Object, e as EventArgs)

   'Retrieve variables from ViewState
   intTotalQuestion = ViewState("TotalQuestion")
   intQuestionNo = ViewState("QuestionNo")
   intScore = ViewState("Score")
   arrAnswerHistory = ViewState("AnswerHistory")
   arrRightOrWrong = ViewState("RightOrWrong")
   arrCorrect = ViewState("AnswerList")
   req = ViewState("origReq")
   userName = ViewState("origUserName")
   emailAddr = ViewState("origEmailAddr")
   mgmtBaseUrl = ViewState("mgmtUrl")
   sessionId = ViewState("sessID")
```

```
   'Correct answer?
   If rblAnswer.SelectedItem.Value = ViewState("CorrectAnswer") Then
      intScore += 1
      arrRightOrWrong.Add(0)
   Else
      arrRightOrWrong.Add(rblAnswer.SelectedItem.Value)
   End If

   'Remember all selected answers
   arrAnswerHistory.Add(rblAnswer.SelectedItem.Value)
   arrCorrect.Add(ViewState("CorrectAnswer"))

   'End of quiz?
   If intQuestionNo=intTotalQuestion Then

      'Yes.Show the result.
      QuizScreen.Visible = False
      ResultScreen.Visible = True

      'Render result screen
      ShowResult()

   Else

      'Not yet.Show another question.
      QuizScreen.Visible = True
      ResultScreen.Visible = False
      intQuestionNo += 1

      'Render next question
      ShowQuestion(intQuestionNo)
   End If
End Sub

Sub ShowQuestion(intQuestionNo as Integer)
   Dim xNodeList as XmlNodeList
   Dim xNodeAttr as Object
   Dim strXPath as String
   Dim i as Integer
   Dim tsTimeSpent as TimeSpan

   strXPath = "/quiz/mchoice[" & intQuestionNo.ToString() & "]"

   'Extract question
   lblQuestion.Text = intQuestionNo.ToString() & "." &
xDoc.SelectSingleNode(strXPath & "/question").InnerXml

   'Extract answers
   xNodeList = xDoc.SelectNodes(strXPath & "/answer")

   'Clear previous listitems
   rblAnswer.Items.Clear

   For i = 0 to xNodeList.Count-1

      'Add item to radiobuttonlist
      rblAnswer.Items.Add(new ListItem(xNodeList.Item(i).InnerText, i+1))

      'Extract correct answer
      xNodeAttr = xNodeList.Item(i).Attributes.ItemOf("correct")
```

```
      If not xNodeAttr is Nothing Then
         If xNodeAttr.Value = "yes" Then
            ViewState("CorrectAnswer") = i+1
         End If
      End If
   Next

   'Output Total Question and passing score
   lblTotalQuestion.Text = intTotalQuestion
   lblPassingScore.Text = passingScore

   'Output Time Spent
   tsTimeSpent = DateTime.Now.Subtract(ViewState("StartTime"))
   lblTimeSpent.Text = tsTimeSpent.Minutes.ToString() & ":"&
tsTimeSpent.Seconds.ToString()

   'Store data to viewstate
   ViewState("TotalQuestion") = intTotalQuestion
   ViewState("Score") = intScore
   ViewState("QuestionNo") = intQuestionNo
   ViewState("AnswerHistory") = arrAnswerHistory
   ViewState("RightOrWrong") = arrRightOrWrong
   ViewState("AnswerList") = arrCorrect
   ViewState("origReq")=req
   ViewState("origUserName")=userName
   ViewState("origEmailAddr")=emailAddr
   ViewState("mgmtUrl")=mgmtBaseUrl
   ViewState("sessID")=sessionID

End Sub

Sub ShowResult()
   Dim strResult as String
   Dim intCompetency as Integer
   Dim i as Integer
   Dim strXPath as String
   Dim tsTimeSpent as TimeSpan

   tsTimeSpent = DateTime.Now.Subtract(ViewState("StartTime"))

   strResult  = "<center>"

   if passingScore <= Int(intScore/intTotalQuestion*100).ToString()
      strResult += "<h2><font color=""green"">You Passed!</h3></font>"
   else
      strResult += "<h2><font color=""red"">You Failed!</h3><b>Please review the
answers and retake the test.</b><br></font>"
   End If

   strResult += "User Name: " & userName & "<br>"
   strResult += "Elapsed Time: " & tsTimeSpent.Minutes.ToString() & ":"&
tsTimeSpent.Seconds.ToString() & "<br>"
   strResult += "Correct Answers: " & intScore.ToString() & " out of " &
intTotalQuestion.ToString() & "<br>"
   strResult += "Your Percentage: " & Int(intScore/intTotalQuestion*100).ToString()
& "%<br>"
   strResult += "Required Percentage:"& passingScore.ToString() & "%<br>"
   strResult += "</center>"

   strResult += "<h3>Quiz Results</h3>"
   For i = 1 to intTotalQuestion
```

```
      strXPath = "/quiz/mchoice[" & i.ToString() & "]"
      strResult += "<b>" & i.ToString() & "." & xDoc.SelectNodes(strXPath &
"/question").Item(0).InnerXml & "</b><br>"
      If arrRightOrWrong.Item(i-1)=0 Then
         strResult += "<img src = ""checkMark.gif""><font color=""green""> "
         strResult += "<b>You answered:</b> " & xDoc.SelectNodes(strXPath &
"/answer[" & arrAnswerHistory.Item(i-1).ToString() & "]").Item(0).InnerXml &
"</font><br><br>"
      Else
         strResult += "<img src = ""Block.gif""><font color=""red""> "
         strResult += "<b>You answered:</b> " & xDoc.SelectNodes(strXPath &
"/answer[" & arrAnswerHistory.Item(i-1).ToString() & "]").Item(0).InnerXml & "<br>"
         strResult += "The correct anwer is: " & xDoc.SelectNodes(strXPath &
"/answer[" & arrCorrect.Item(i-1).ToString() & "]").Item(0).InnerXml &
"</font><br><br>"
      End If
   Next

   'Setup the common Mail settings
   Dim objMail As MailMessage
   objMail = New MailMessage()
   objMail.From = quizFrom
   objMail.Body = strResult
   objMail.BodyFormat = MailFormat.Html

   'Path to the attachments for the Check and X images - update these in myvars.aspx
   objMail.Attachments.Add(New MailAttachment(imagePath & "block.gif"))
   objMail.Attachments.Add(New MailAttachment(imagePath & "checkMark.gif"))

   'Address of the SMTP server - can be localhost if SMTP is running on IIS - in
myvars.aspx
   SmtpMail.SmtpServer = smtpServer

   'Determine pass/fail
   If passingScore <= Int(intScore/intTotalQuestion*100).ToString()

      'Mail the passing test result to the test-taker
      'Be sure to update the mail fields in myvars.aspx
      objMail.To =emailAddr
      objMail.Subject = quizName & " Results for " & emailAddr

      'Send the mail
      SmtpMail.Send(objMail)
      strResult +="Your test is being emailed to you at " & emailAddr

      'Send the session Auth message to LHM
      postLHM()

   else
      'Mail failing test results to the instuctor
      objMail.To =quizTo
      objMail.Subject = "Failing " & quizName & " Test Results for " & emailAddr

      'Send the mail
      SmtpMail.Send(objMail)
      strResult += "<a href=""quiz.aspx"">Click here to retake the quiz</a>"
   End If

   'Write it
   lblResult.Text = strResult
```

```
End Sub

Sub postLHM()

   'The LHM cgi on the SonicWall - this does not change
   Dim loginCgi as String = "externalGuestLogin.cgi"

   'Assemble the data to post back to the SonicWall to authorize the LHM session
   Dim loginParams as String = "sessId=" & sessionId & "&userName=" &
Server.URLEncode(userName) & "&sessionLifetime=" & sessTimer & "&idleTimeout=" &
idleTimer

   'Combine mgmtBaseUrl from the original redirect with the login cgi
   Dim postToSNWL as String = mgmtBaseUrl & loginCgi

   'Convert the loginParams to a well behaved byte array
   Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

   Try
      'Let the user know that we are setting up the session, just in case it takes
more than a second
      LHMResult.Text = "Authorizing session.Please wait."

      'Create the webrequest to the SonicWall
      Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

      'Calculate the length of the byte array
      toSNWL.ContentLength = byteArray.Length

      'Set the method for the webrequest to POST
      toSNWL.Method = "POST"

      'Set the content type
      toSNWL.ContentType = "application/x-www-form-urlencoded"

      'Open the request stream
      Dim dataStream As Stream = toSNWL.GetRequestStream()

      'Write the byte array to the request stream
      dataStream.Write(byteArray, 0, byteArray.Length)

      'Close the Stream object
      dataStream.Close()

      'Get the response
      Dim snwlReply As WebResponse = toSNWL.GetResponse()

      'Display the status - looking for 200 = OK.
      'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

      'Grab the response and stuff it into an xml doc for possible review
      Dim snwlResponse as XmlDocument = New XmlDocument()
      snwlResponse.Load(snwlReply.GetResponseStream())

      'Set the xPath to the SNWL reply, and get the response
      Dim codePath as String =
"SonicWallAccessGatewayParam/AuthenticationReply/ResponseCode"

      'Response code 50 - Login Succeeded

      If snwlResponse.SelectSingleNode(codePath).InnerXml = "50"
```

```
        'Do we want to provide a logout popup window?
        If logoutPopup = "1" Then
           'Popup hack using Javascript for logout window
           Dim sb As New System.Text.StringBuilder()
           sb.Append("<script language='javascript'>")
           sb.Append("window.open('logout.aspx?sessId=")
           sb.Append(Server.URLEncode(CStr(sessionId)))
           sb.Append("&mgmtBaseUrl=")
           sb.Append(Server.URLEncode(CStr(mgmtBaseUrl)))
           sb.Append("&sessTimer=")
           sb.Append(Server.URLEncode(CStr(sessTimer)))
           sb.Append("','logOut','toolbar=no,")
           sb.Append("addressbar=no,menubar=no,")
           sb.Append("width=400,height=250');")
           sb.Append("<")
           sb.Append("/")
           sb.Append("script>")
           RegisterStartupScript("stp", sb.ToString)
        End If

        LHMResult.Text = "<br><b><font color=""green"">Session
authorized:</font></b> You may now go to the URL you originally requested: <a
target=""_blank"" href=""" & req & """>" & req & "</a>"

     'Response code 51 - Session Limit Exceeded
     ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "51"
        LHMResult.Text = "<br><b><font color=""red"">Session Limit
Reached:</font></b> The maximum number of guest session has been reached.Sorry for
the inconvenience.Please close and relaunch your browser to try again."

     'Response code 100 - Login Failed.
     ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "100"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> Your session cannot be created at this time.Sorry for the
inconvenience.Please close and relaunch your browser to try again."

     'Response code 251 - Bad HMAC.
     ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed message authentication.Sorry
for the inconvenience.Please close and relaunch your browser to try again."

     'Response code 253 - Invalid SessionID.
     ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed to match a known session
identity.Sorry for the inconvenience.Please close and relaunch your browser to try
again."

     'Response code 254 - Invalid CGI.
     ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization was missing an essential
parameter.Sorry for the inconvenience.Please close and relaunch your browser to try
again."

     'Response code 255 - Internal Error.
     ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified
```

```
error.Sorry for the inconvenience.Please close and relaunch your browser to try
again."

      End If

      'Close the streams
      dataStream.Close()
      snwlReply.Close()

      'If there is some asp.net error trying to talk to the SonicWall, print it
      'in the same color as the background, but still show the quiz results.
      Catch ex as Exception
         catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified
error.Sorry for the inconvenience.Please close and relaunch your browser to try
again.If the problem persists, please notify an attendant."
   End Try
End Sub

</script>
<html>
<head>
<title><%= quizName %> </title>
</head>
<style>
body {
  font-size: 10pt;
  font-family: verdana,helvetica,arial,sans-serif;
  color:#000000;
  background-color:#9CBACE;
}

tr.heading {
  background-color:#006699;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
}
</style>

<HTML>
<HEAD>
<TITLE>LHM Quiz Script</TITLE>
</HEAD>

<body>
<span id="QuizScreen" runat="server">
<form runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
   <tr class="heading">
      <td width="50%" valign="center"><font color="white"><b><%= quizName %>  - <%=
userName%></b></font></td>
      <td><center><img width="216" height="51" src="<%= logo %>"></center></td>
      <td width="50%" align="right" valign="center"><font color="white"><b>This quiz
has <asp:label id="lblTotalQuestion" runat="server" /> questions</b></font></td>
```

```
   </tr>
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr>
      <td colspan="2">
         <b><asp:label id="lblQuestion" runat="server" /></b><br>
         <asp:radiobuttonlist id="rblAnswer" RepeatDirection="vertical"
TextAlign="right" RepeatLayout="table" runat="server" /><br>
         <asp:button id="btnSubmit" class="button" text="  Submit  "
onClick="btnSubmit_Click" runat="server" />
         <asp:requiredfieldvalidator ControlToValidate="rblAnswer"
ErrorMessage="Please select an answer" runat="server" />
      </td>
   </tr>
   <tr class="heading">
      <td width="70%"><font color="white"><b>Score required to pass <asp:label
id="lblPassingScore" runat="server" />%</b></font></td>
      <td width="30%" align="right"><font color="white"><b>Time spent <asp:label
id="lblTimeSpent" runat="server" /></b></font></td>
   </tr>
</table>
</form>
</span>

<span id="ResultScreen" runat="server"> <asp:label id="lblResult" runat="server" />
<br>
<asp:Label id=LHMResult runat="server" />
<asp:Label id=catchError runat="server" />
</span>

</body>
</html>
```

PayPal スクリプト

認証モデル

ゲスト クライアントは「**すぐに購入**」ボタンによる 1 時間または 24 時間アクセスを自らの PayPal アカウントを使用して購入します。支払いはホットスポット プロバイダの PayPal マーチャント アカウントに対して PayPal 経由で行われます。

目的

インターネットで売買を行うほとんどの人は PayPal を使用しています。購入者アカウントの設定や、あらゆる支払い形態 (クレジット カード、バンク カード、当座預金口座) へのアカウントの関連付けが非常に簡単に行えます。

購入者専用アカウントからマーチャント アカウントへのアップグレードもほとんど同じくらい簡単です。マーチャント アカウントを持つことで、PayPal ユーザは商品やサービスに対する他の PayPal ユーザからの支払いを受け入れることができます。資金振替は PayPal 経由で実行され、マーチャントにはオンラインで取引を行う手段が提供され、いかなる複雑な支払い処理の設定も行うことなく、どんな形態の支払いでも受け入れることができます。これにより、有料のホットスポット プロバイダになるうえで最大かつただ 1 つの障害となっているものを取り除くことができます。

Paypal には「**すぐに購入**」という機能があり、これによってワンクリックでトランザクションを処理できます。これらのボタンは、PayPal の支援によって生成されるフォームであり、購入するアイテムやサーバに関する情報を格納しています。購入者が「**すぐに購入**」を選択すると、セッションはトランザクションの詳細 (販売者、アイテム、価格など) が含まれている querystring (クエリ文字列) を使用して PayPal サイトにリダイレクトされます。この PayPal スクリプトでは、「**すぐに購入**」 (サーバ側ではなくクライアント側のコード) を使用せずに、サーバ側の「すぐに購入」カスタム ルーチンを使用しています。

「すぐに購入」リダイレクトには自動復帰用のパスも含まれています。自動復帰は、PayPal トランザクションの後に購入者をマーチャントのサイトに送り返す PayPal 機能です。自動復帰は PDT (pdtPath、以下で説明します) の使用時に必要です。

また、「すぐに購入」のカスタム リダイレクトにより、LHM の sessionID および mgmtBaseUrl が PayPal への「すぐに購入」リダイレクトのカスタム文字列に埋め込まれます。これにより、セッションがいったん LHM サーバを離れてから (PDT のための自動復帰によって) 戻ってきた場合でも、セッションを追跡できます。

基本的な PayPal 支払いシステムには、電子メールによるマーチャントへの支払い通知の機能を備えています。これは物理的な商品の場合に好都合です。購入/出荷のトランザクションはリアルタイムで行う必要がないためです。マーチャントは製品を出荷するまで何時間または何日でも待つことができます。ホットスポットの購入など、即時の納入を必要とするトランザクションでは、リアルタイム性のより高い支払い方法が必要になります。

PayPal では 2 つの支払い通知方法を提供しています。

- 即時支払い通知 (IPN): 特定のトランザクションの支払いが完了したことを示すマーチャント サイトに対するウェブサービス呼び出しを PayPal が実行することで機能します。残念ながら、この処理は常にリアルタイムで行われるわけではありません (この非同期通知が届くまでに最大 20 分かかることがあります)。そのため、スクリプトではこの通知が採用されませんでした(IPN の詳細については、https://www.paypal.com/cgi-bin/webscr?cmd=p/xcl/rec/ipn-intro-outside を参照してください)。
- 支払いデータ転送 (PDT: http://www.paypal.com/cgi-bin/webscr?cmd=p/xcl/rec/pdt-intro-outside を参照してください)。この方法は、PayPal の自動復帰手法の使用によって確実にリアルタイムで行われます。PDT は、マーチャントへのトランザクション状態 (SUCCESS または FAIL) や payment_status (Completed、Pending、Denied、Failed、Refunded、Reversed、または Cancelled_Reversal) の即時通知を実現します。トランザクションや支払いの状況を直ちに知らせることで、対価の未回収が生じるリスクなしにサービスの即時提供が可能になります。

myvars 変数

`logoutPopup` ログアウト ポップアップ ウィンドウの使用を制御します。次のように設定します。

- **0**: ポップアップ ウィンドウを無効にします。
- **1**: ポップアップ ウィンドウを有効にします。

debugFlag	PayPal の PDT 転送用のデバッグ出力を設定します。 • **0**: オフ • **1**: オン
pdtPath	PDT 自動復帰によるゲスト クライアントのリダイレクト先のパス (上記の「目的」セクションを参照してください)。
paypalCGI	PayPal トランザクションでゲートウェイの役割を果たす PayPal CGI の URL。URL そのものは変更してはいけませんが、次の 2 つのオプションがあります。 • ライブ (実際の) PayPal サイト。 • テストに使用できる PayPal サンドボックス (PayPal デベロッパー ネットワークに含まれます)。
myBusiness	ホットスポット プロバイダの電子メール アドレス (PayPal が企業を認識する方法)。トランザクションで支払いを受け取るマーチャント アカウントの電子メール アドレスと一致している必要があります。
token	支払いデータ転送オプションによってそれぞれのマーチャントに対して一意のトークンが生成されます。PayPal から提供された一意のトークンをここに指定できます。トークンは正しいものでなければなりません。そうでない場合、(実際の PayPal トランザクションではなく) PDT が失敗します。
itemName1 itemName2	2 つのアクセス オプションの名前 (`1 Hour Secure Internet Access`、`24 Hours Secure Internet Access` など)。
itemNumber1 itemNumber2	2 つのアクセス オプション用のアイテム番号 (ほとんどの場合は PayPal による内部の恣意的な参照用。`1hour`、`24hour` など)。
itemTimer1 itemTimer2	2 つのアクセス オプション用の秒単位のセッション タイマー (1 時間の場合は `3600`、24 時間の場合は `86400` など)。
itemAmount1 itemAmount2	2 つのアクセス オプション用の米ドル価格 (1 セントの場合は `0.01`、2 セントの場合は `0.02` など)。プロモーション価格設定の制限時間。
itemButton1 itemButton2	2 つのアクセス オプション用のボタン テキスト (`1 Hour Access - $0.01`、`24 Hours Access - $0.02` など)。
strHmac	オプションの HMAC 機能のための事前共有鍵。
hmacType	HMAC 使用時に用いるダイジェスト種別: 「**MD5**」または「**SHA1**」を選択します。
logo	ページ ヘッダーで使用するロゴ (画像) ファイルの名前。

セッション フロー

1 ゲスト クライアントはウェブ ブラウザを起動し、LHM によって http://*<lhmserver>*/paypal/default.aspx にリダイレクトされます。ここで、*<lhmserver>* は利用している LHM サーバです。

2 ゲスト クライアント (購入者) が「**すぐに購入**」ボタンのいずれかを選択します (「**1 時間のアクセス - $0.01**」など)。

3 クライアントは、マーチャント、アイテム、LHM セッション (カスタム変数内)、および自動復帰 URL (pdtPath として myvars 内に定義) に関するすべての情報が含まれている querystring によって PayPal サイトにリダイレクトされます。

pdtPath は LHM サーバ上にあります。このパスは default.aspx パス (SonicWall セキュリティ装置上で設定されているもの) と同じであって pdt.aspx ファイルを指している必要があります。このように、PayPal トランザクションが完了して PayPal によるリダイレクトでクライアントがマーチャント サイトに戻ってくると、クライアントは再び http://*<lhmserver>*/paypal/pdt.aspx ページにリダイレクトされます。

LHM サーバそのものでは機密情報が入力されていないため、LHM サーバでは HTTP を使用できます。PayPal トランザクションはゲスト クライアントと PayPal との間で HTTPS 経由で処理されます。

「すぐに購入」リダイレクト文字列の例:

```
https://www.sandbox.paypal.com/cgi-bin/webscr?cmd=_xclick&business=demo@SonicWall.com&item_name=1%20Hour%20Access&item_number=1hour&amount=0.01&currency_code=USD&lc=US&bn=PP-BuyNowBF&no_note=1&no_shipping=1&cancel_return=http://lhmserverpaypal/default.aspx&return=http://lhmserver/lhm/paypal/pdt.aspx&custom=35378e67833faa3de83aa3b771https%3a%2f%2f172.16.17.1%3a4043%2f
```

4 ゲスト クライアントは PayPal にログイン (または必要に応じて新規アカウントを作成) して PayPal によるトランザクションを完了します。トランザクションの完了後、クライアントはリダイレクトによって http://*<lhmserver>*/paypal/pdt.aspx に戻ってきます。このリダイレクトに含まれているのは querystring です。そこには、トランザクション ID (tx)、状況 (st)、数量 (amt)、通貨の種別 (cc)、カスタム値 (cm)、および暗号化されたシグネチャ (sig) が格納されています。

リダイレクト文字列の例:

```
http://lhmserver/lhm/paypal/pdt.aspx?tx=4LN76482JF4605045&st=Completed&amt=0.01&cc=USD&cm=35378e67833faa3b771https%3a%2f%2f172%2e16%2e17%2e1%3a4043%2f&sig=qdsNC4flKwtPviggoGAXCpeV9gS%2f2E%2bGGVbTZ3STrUV1Ci9K3c2zTdJMuuKCmRiif1SybsZtUqDYqzzfMg64AF3PKCk85rrPubYT4K4aC
```

5 上記の URL で pdt.aspx スクリプトにアクセスしているゲスト クライアントは、LHM サーバ上で PDT 処理を開始します。スクリプトは、(PDT トランザクションであることを示す) cmd=_notify-synch や、tx (トランザクション ID)、マーチャントのトークン (myvars で定義されています) が設定されている at 変数で構成される querystring を作成します。その後、この文字列は paypalCGI URL (myvars で定義されているもの) に POST 送信されます。

6 PayPal は SUCCESS (成功) または FAIL (失敗) のコードによってこの POST に応答します。

- FAIL (失敗) - スクリプトは PayPal トランザクションが失敗したことをクライアントに示し、クライアントは支援を求めるように促されます。

- SUCCESS(成功)-トランザクションに関する次のような詳細情報が提供されます。

```
SUCCESS
txn_type=web_accept
payment_date=00%3A39%3A48+Oct+30%2C+2005+PDT
last_name=Niqual
item_name=1+Hour+Secure+Internet+Access
payment_gross=0.01
mc_currency=USD
business=lhmdemo%40SonicWall.com
payment_type=instant
payer_status=verified
tax=0.00
payer_email=lhmClient%40SonicWall.com
txn_id=84K306380G150640T
quantity=1
receiver_email=lhmdemo%40SonicWall.com
first_name=Sah
payer_id=XWRZGABD6UV2W
receiver_id=REW4W5WANU294
item_number=1hour
payment_status=Completed
payment_fee=0.01
mc_fee=0.01
shipping=0.00
mc_gross=0.01
custom=35378e67833faa3de833755d3aa3b771https%3
A//172.16.17.1%3A4043/
charset=windows-1252
```

7 スクリプトは payment_status をチェックして、支払いが完了したことを確認します。完了していない場合は、incomplete-payment (支払い未完了) メッセージがユーザに提示されます。

8 payment_status が完了になっている場合、スクリプトはクライアント名、アイテム名、数量、トランザクション ID、ビジネス、クライアントの受領書を生成するためのカスタム変数、LHM セッションのユーザ名の取得や、LHM の sessionID および mgmtBaseUrl の識別も行います。

9 スクリプトは PayPal トランザクション受領書をゲスト クライアントに提示します。

10 スクリプトは、セッションを承認するために SonicWall セキュリティ装置に対する LHM ポストを実行します。

追加の考慮事項

PayPal マーチャント アカウントが必要です。

PayPal アカウントが自動復帰および PDT 用に設定されている必要があります (http://www.paypal.com/cgi-bin/webscr?cmd=p/xcl/rec/pdt-techview-outside を参照してください)。

テストのために、PayPal デベロッパー ネットワーク (https://developer.paypal.com) を利用して (無料の) PayPal サンドボックス アカウント (https://www.sandbox.paypal.com) を設定することが強く推奨されます。

重要：ゲスト クライアントは PayPal サイトに直接リダイレクトされるため、PayPal サイト IP アドレスはすべて SonicWall セキュリティ装置のゲスト サービス設定で許可されたネットワークとして設定されている必要があります。次のようなボタンがあります。

www.paypal.com

```
64.4.241.32
64.4.241.33
216.113.188.32
216.113.188.35
216.113.188.66
216.113.188.67
```

www.paypalobjects.com

```
216.113.188.25
64.4.241.62
216.113.188.9
```

www.sandbox.paypal.com

```
66.135.197.160
```

developer.paypal.com

```
66.135.197.163
```

トピック:

- default.aspx (933 ページ)
- logout.aspx (938 ページ)
- myvars.aspx (944 ページ)
- pdt.aspx (945 ページ)

default.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWall authorizing the LHM session.
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
      As Boolean Implements ICertificatePolicy.CheckValidationResult
      Return True
   End Function
End Class

'Note: For PayPal authorization to work, it is necessary to set up the PayPal sites
(www.paypal.com, www.paypalobjects.com, and www.sandbox.paypal.com) as a bypass
network on WGS.This is so that WGS/LHM users can access PayPal directly to complete
the payment transactions.This list currently includes the following addresses:
```

```
[64.4.241.32, 64.4.241.33, 216.113.188.32, 216.113.188.35, 216.113.188.66,
216.113.188.67], [216.113.188.25, 64.4.241.62, 216.113.188.9] and [66.135.197.160].

'Sample LHM redirect querystring:
'http://127.0.0.1/lhm/paypal/default.aspx?sessionId=0b712fd83b9f5313db5af1cea6b1004
f&ip=10.50.165.231&mac=00:0e:35:bd:c9:37&ufi=0006b11184300&mgmtBaseUrl=https://10.5
0.165.193:4043/&clientRedirectUrl=https://10.50.165.193:444/&req=http%3A//www.googl
e.com/ig

Dim ip as String
Dim sessionId as String
Dim mac as String
Dim ufi as String
Dim mgmtBaseUrl as String
Dim clientRedirectUrl as String
Dim req as String
Dim hmac as String
Dim customCode as String

Sub Page_Load(src as Object, e as EventArgs)

   ip=Request.QueryString("ip")
   sessionId=Request.QueryString("sessionId")
   mac=Request.QueryString("mac")
   ufi=Request.QueryString("ufi")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
   clientRedirectUrl=Request.QueryString("clientRedirectUrl")
   req=Request.QueryString("req")
   hmac=Request.QueryString("hmac")
   customCode=Request.QueryString("cc")

   'customCode grabs the "cc=" querystring value sent by the SonicWall.This allows
you to use the same
   'page (e.g. this page) for the "Session Expiration" (?cc=2), "Idle Timeout"
(?cc=3) and "Max Sessions" (?cc=4) page.
   If customCode <> "" Then
      Select Case customCode
      Case "2"
         LHMResult.Text="<br><H3><font color=""red"">Your LHM session has expired.You
may try to initiate a new session.</font></H3>"
      Case "3"
         LHMResult.Text="<br><H3><font color=""red"">You have exceeded your idle
timeout.Please log back in.</font></H3>"
      Case "4"
         LHMResult.Text="<br><H3><font color=""red"">The maximum number of sessions
has been reached.Please try again later.</font></H3>"
      End Select
   End If

   'Set the button Text for the two buttons with the variable configured in myvars
   btnBuyNow1.Text=itemButton1
   btnBuyNow2.Text=itemButton2

   'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWall
   'This is necessary for the POST to the SonicWall authorizing the LHM session.
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   'Note - the routine below for handling the hmac requires the use of the
SonicSSL.dll and libeay.dll libraries.
```

```
   'The DLL must be copied to the IIS server, and the SonicSSL dll must be registered
with "regsvr32 sonicssl.dll"
   If hmac <> "" Then

      'SonicWall URL Encode routine is different from Microsoft - this is the
SonicWall method
      req=Replace(req,"%","%25")
      req=Replace(req,":","%3A")
      req=Replace(req," ","%20")
      req=Replace(req,"?","%3F")
      req=Replace(req,"+","%2B")
      req=Replace(req,"&","%26")
      req=Replace(req,"=","%3D")

      Dim strHmacText as String
      Dim objCrypto as Object
      Dim strHmacGenerated
      Dim loginError as String

      'Initialize the Crypto object
      objCrypto = Server.CreateObject("SonicSSL.Crypto")

      'The text to be encoded
      strHmacText = sessionId & ip & mac & ufi & mgmtBaseUrl & clientRedirectUrl &
req

      'Calculate the hash with a key strHmac, the return value is a string converted
form the output sha1 binary.
      'The hash algorithm (MD5 or SHA1) is configured in myvars and in the Extern
Guest Auth config on the SonicWall
      If hmacType = "MD5" Then
         strHmacGenerated = objCrypto.hmac_md5(strHmacText, strHmac)
      Else
         strHmacGenerated = objCrypto.hmac_sha1(strHmacText, strHmac)
      End If

      If strHmacGenerated <> hmac Then
         Dim hmacFail as String
         hmacFail = "<font color=""red"">The HMAC failed validation.Please notify an
attendant.</font><br><br>"
         hmacFail+="<font color=""9CBACE"">Received HMAC: " & hmac & "<br>Calculated
HMAC: " & strHmacGenerated & "<br>"
         hmacFail+="Make sure the digest functions on the SonicWall and LHM server
match.<br>"
         hmacFail+="Also make sure the shared secret on the SonicWall and myvars
match</font>"
         catchError.Text=hmacFail
      End If

   End If

End Sub

Sub btnBuyNow_Click(Sender As Object, E As EventArgs)

'sample redirect generated by this routine:
'https://www.paypal.com/cgi-
bin/webscr?cmd=_xclick&business=jlevy@SonicWall.com&item_name=24%20Hour%20Secure%20
Internet%20Access&item_number=24hour&amount=0.02&currency_code=USD&lc=US&bn=PP-
BuyNowBF&no_note=1&no_shipping=1&cancel_return=http://127.0.0.1/lhm/paypal/default.
aspx&return=http://www.moosifer.com/pdt.aspx
```

```
'sample redirect from the paypal server back the LHM server on transaction
completion (modified).
'http://127.0.0.1/lhm/paypal/pdt.aspx?tx=4PG453F7LS133715V&st=Completed&amt=0.02&cc
=USD&cm=&sig=EZhZtJygi7RTXulJt4SEhVBRi%2bJwLaC9z9kRLsrsXk4gQKnzvI5vjGy0vdhKPXAVyhbh
%2bwBxWon2cieEQDJ9P6R9qqjuKnzvI5vjGy0vdhKPXAVyJ3GtOq5Jd3%2fvTY3s7FrRcKdKnzvI5vjGy0v
dhKPXAVyyEKNxY3d

   Dim str, itemName, itemNumber, itemAmount As String
   Dim sb As New StringBuilder()

   'Determine which button was pressed, and set item attributes appropriately
   Select Case Sender.Text
      Case itemButton1
         itemName = itemName1
         itemNumber = itemNumber1
         itemAmount = itemAmount1
      Case itemButton2
         itemName = itemName2
         itemNumber = itemNumber2
         itemAmount = itemAmount2
   End Select

   'The paypal CGI URL - You can select either the real CGI or the sandbox CGI in
myvars
   sb.Append(paypalCGI & "?")
   'The cmd passed to PayPal - do not change!
   sb.Append("cmd=_xclick")
   'The email address of the paypal merchant receiving payment.Replace in myvars with
your paypal email address.
   sb.Append("&business=" & myBusiness)
   'The name of the item being purchased.This is the first item option (e.g. 1
hour).Set in myvars
   sb.Append("&item_name=" & itemName)
   'The optional item id
   sb.Append("&item_number=" & itemNumber)
   'The price being charged for the item (access)
   sb.Append("&amount=" & itemAmount)
   'The currency
   sb.Append("&currency_code=USD")
   'The country
   sb.Append("&lc=US")
   'The banana nullifier
   sb.Append("&bn=PP-BuyNowBF")
   'Disables the note option on the transaction
   sb.Append("&no_note=1")
   'Disables the shipping option on the transaction
   sb.Append("&no_shipping=1")
   'Build the path to return the client to (the LHM server address) on a cancelled
transaction
   sb.Append("&cancel_return=http://"& Request.ServerVariables("SERVER_NAME") &
Request.ServerVariables("URL"))
   'The return (success page) path to return the buyer to after the transaction.This
is the PDT receiver/processor page.
   sb.Append("&return=" & pdtPath)
   'The LHM sessionID - append this so that it can be returned to us later by the PDT
transaction - do not change!
   sb.Append("&custom=" & sessionId & Server.URLEncode(mgmtBaseUrl))
   'Optional notify_url that paypal will asynchronously send IPN confirmation to.Not
used since it's not real-time.
   'sb.Append("&notify_url=http://www.moosifer.com/ipn.aspx")
```

```
   str = sb.ToString
   Response.Redirect(str)

End Sub

</script>

<STYLE>
body {
  font-size: 10pt;
  font-family: verdana,helvetica,arial,sans-serif;
  color:#000000;
  background-color:#9CBACE;
}

tr.heading {
  background-color:#006699;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM PayPal Script</TITLE>
</HEAD>

<BODY>
<form id="frmValidator" runat="server">

<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
   <tr class="heading">
      <td width="50%" valign="center"><font color="white"><b>LHM Access with PayPal
Buy Now</b></font></td>
      <td><center><img width="216" height="51" src="<%= logo%>"></center></td>
      <td width="50%" align="right" valign="center"><font color="white"><b>Powered
by SonicWall LHM</b> </font></td>
   </tr>
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>

<table width="100%" border="0" cellpadding="2" cellspacing="0">

   <tr>
      <td colspan=3><br></td>
   </tr>
   <tr>
      <td colspan=3 align="left">Purchase Secure Internet Access through SonicWall's
LHM and PayPal's Buy Now feature.
      <br><br>The two Buy Now buttons below will send you to PayPal's website where
you can use your PayPal account to pay <b>$<%= itemAmount1 %> for <%= itemName1
%></b>, or <b>$<%= itemAmount2 %> for <%= itemName2 %></b>.
      <br><br>
```

```
      PayPal will then redirect you to this site to initiate the Payment Data
Transfer (PDT) exchange.The PDT exchange begins with the LHM server posting a paypal
constructed querystring back to PayPal.The response to the post will then be parsed
by the LHM server to determine if the PayPal transaction was successful.After all
data are exchanged and verified, LHM will authorize access on the SonicWall for the
period of time purchased.
      <br><br>
      The clock for access will start immediately upon successful session
authorization, and can be used on the local SonicWall appliance by the client (as
tracked by IP and MAC address) so long as session time remains.The idle timeout will
effectively be disabled by setting the idle timer to the same value as the session
timer.
      <br><br>
      Please select "<%= itemName1 %>" or "<%= itemName2 %>" below.You will be
redirected to the PayPal site, and will be returned to this site on transaction
completion.

      <br><br>
      </td>
   </tr>
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
   <tr class="heading">
      <td align="center"><asp:Button ID="btnBuyNow1" Class="button"
OnClick="btnBuyNow_Click" runat="server" />
        <asp:Button ID="btnBuyNow2" Class="button" OnClick="btnBuyNow_Click"
runat="server" /></td>
   </tr>
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
   <tr>
      <td colspan=3><asp:Label id=LHMResult runat="server" /></td>
   </tr>
   <tr>
      <td colspan=3><asp:Label id=catchError runat="server"/></td>
   </tr>
</table>

</form>
</BODY>
</HTML>
```

logout.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
```

```
'This is necessary for the POST to the SonicWall authorizing the LHM session.
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
      As Boolean Implements ICertificatePolicy.CheckValidationResult
      Return True
   End Function
End Class

Dim sessionId as String
Dim mgmtBaseUrl as String
Dim eventId as String = "&eventId=1"

'Grab the code and the session lifetime from the generator page
Sub Page_Load(src as Object, e as EventArgs)
   sessionId=Request.QueryString("sessId")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
   sessTimer=Request.QueryString("sessTimer")


   'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWall
   'This is necessary for the POST to the SonicWall authorizing the LHM session.
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   'When the page loads, make the loggedIn span visible
   loggedIn.Visible=True
   loggedOut.Visible=False

   Me.Button1.Attributes.Add("OnClick", "self.close()")

End Sub

'The Logout button
Sub btnSubmit_Click(Sender As Object, E As EventArgs)

   'Let the user know that we are setting up the session, just in case it takes more
than a second
   LHMResult.Text = "Authorizing session.Please wait."

   'The LHM cgi on the SonicWall - this does not change
   Dim loginCgi as String = "externalGuestLogoff.cgi"

   'Assemble the data to post back to the SonicWall to authorize the LHM session
   Dim loginParams as String = "sessId=" & sessionId & eventId

   'Combine mgmtBaseUrl from the original redirect with the login cgi
   Dim postToSNWL as String = mgmtBaseUrl & loginCgi

   'Convert the loginParams to a well behaved byte array
   Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

   Try
      'Make the loggedOut span visible
      loggedIn.Visible=False
      loggedOut.Visible=True

      'Create the webrequest to the SonicWall
      Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)
```

```
      'Calculate the length of the byte array
      toSNWL.ContentLength = byteArray.Length

      'Set the method for the webrequest to POST
      toSNWL.Method = "POST"

      'Set the content type
      toSNWL.ContentType = "application/x-www-form-urlencoded"

      'Open the request stream
      Dim dataStream As Stream = toSNWL.GetRequestStream()

      'Write the byte array to the request stream
      dataStream.Write(byteArray, 0, byteArray.Length)

      'Close the Stream object
      dataStream.Close()

      'Get the response
      Dim snwlReply As WebResponse = toSNWL.GetResponse()

      'Display the status - looking for 200 = OK.
      'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

      'Grab the response and stuff it into an xml doc for possible review
      Dim snwlResponse as XmlDocument = New XmlDocument()
      snwlResponse.Load(snwlReply.GetResponseStream())

      'Set the xPath to the SNWL reply, and get the response
      Dim codePath as String =
"SonicWallAccessGatewayParam/LogoffReply/ResponseCode"

      'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

      'Response code 150 - Logout Succeeded
      If snwlResponse.SelectSingleNode(codePath).InnerXml = "150"
        LHMResult.Text = "<br><b><font color=""green"">Your session has been logged
out.<br><br>Thank you for using LHM Guest Services.</font></b>"

      'Response code 251 - Bad HMAC.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed message authentication.Sorry for the
inconvenience.Please close and relaunch your browser to try again."

      'Response code 253 - Invalid SessionID.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed to match a known session identity.Sorry for
the inconvenience.Please close and relaunch your browser to try again."

      'Response code 254 - Invalid CGI.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request was missing an essential parameter.Sorry for the
inconvenience.Please close and relaunch your browser to try again."

      'Response code 255 - Internal Error.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
```

```
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error.Sorry for the
inconvenience.Please close and relaunch your browser to try again."

      End If

      'Close the streams
      dataStream.Close()
      snwlReply.Close()

      'If there is some asp.net error trying to talk to the SonicWall, print it in
the same color as the background.
      Catch ex as Exception
         catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
         LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error.Sorry for the
inconvenience.Please close and relaunch your browser to try again.If the problem
persists, please notify an attendant."
      End Try
End Sub

</script>
<STYLE>
body {
   font-size: 10pt;
   font-family: verdana,helvetica,arial,sans-serif;
   color:#000000;
   background-color:#9CBACE;
}

tr.heading {
   font-size: 10pt;
   background-color:#006699;
}

tr.smalltext {
   font-size: 8pt;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
   font-size: 8pt;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Logout Page</TITLE>

<SCRIPT LANGUAGE="Javascript">

//'Javascript Seconds Countdown Timer
var SecondsToCountDown = <%= sessTimer%>;
var originalTime=" ";

function CountDown()
{
   clockStr="";

   dayStr=Math.floor(SecondsToCountDown/86400)%100000
```

```
   if(dayStr>0){
      if(dayStr>1){
         dayStr+=" days ";
      } else dayStr+=" day ";
      clockStr=dayStr;
   }
   hourStr=Math.floor(SecondsToCountDown/3600)%24
   if(hourStr>0){
      if(hourStr>1){
         hourStr+=" hours ";
      } else hourStr+=" hour ";
      clockStr+=hourStr;
   }
   minuteStr=Math.floor(SecondsToCountDown/60)%60
   if(minuteStr>0){
      if(minuteStr>1){
         minuteStr+=" minutes ";
      } else minuteStr+=" minute ";
      clockStr+=minuteStr;
   }
   secondStr=Math.floor(SecondsToCountDown/1)%60
   if(secondStr>0){
      if(secondStr>1){
         secondStr+=" seconds ";
      } else secondStr+=" second ";
      clockStr+=secondStr;
   }

   if(SecondsToCountDown > 0)
   {
      --SecondsToCountDown;
   }

   if(originalTime.length < 2)
   {
      originalTime = clockStr;
   }

   // Make sure the form is still there before trying to set a value
   if(document.frmValidator){
      document.frmValidator.originalTime.value = originalTime;
      document.frmValidator.countdown.value = clockStr;
   }

   setTimeout("CountDown()", 1000);
   if(SecondsToCountDown == 0)
   {
      document.frmValidator.countdown.value = "Session Expired";
   }
}

//'Disable right-click so that the window doesn't get refreshed since the countdown
is clientside.
document.oncontextmenu = disableRightClick;
function disableRightClick()
{
  return false;
}

//'Disable F5 key, too, on IE at least.
function noF5()
```

```
{
   var key_f5 = 116;
   if (key_f5==event.keyCode)
   {
      event.keyCode=0;
      return false;
   }
   return false;
}

document.onkeydown=noF5
document.onmousedown=disableRightClick

</SCRIPT>

</HEAD>

<BODY onload='CountDown()'>
<span id="loggedIn" runat="server">
<form id="frmValidator" runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"><font color="white"><b>SonicWall LHM Logout
Window</b></font></td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="smalltext"><td><br></td></tr>
   <tr class="smalltext">
      <td>Original Session Time:</td>
      <td><asp:textbox width=250 id="originalTime" runat="server" /></td>
   </tr>
   <tr class="smalltext">
      <td>Remaining Session Time:</td>
      <td><asp:textbox width=250 id="countdown" runat="server" /></td>
   </tr>
   <tr class="smalltext">
      <td colspan=2><br>You may use this window to manually logout your session at
any time, or you may safely close this window if you prefer to let your session
timeout automatically.</font></td>
   </td>
   <tr>
      <td colspan=2><center><asp:button id="btnSubmit" class="button" text="  Logout
" onClick="btnSubmit_Click" runat="server" /></center></td>
   </tr>
</table>
</form>
</span>

<span id="loggedOut" runat="server">
<form id="logout" runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="heading">
```

```
     <td colspan=2 align="center"><font color="white"><b>SonicWall LHM Logout
Window</b></font></td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr>
      <td><asp:Label id=LHMResult runat="server" /></td>
   </tr>
   <tr>
      <td><asp:Label id=catchError runat="server" /></td>
   </tr>
   <tr><td><br></td></tr>
   <tr>
      <td><center><asp:button id="Button1" class="button" text="  Close  "
runat="server" /></center></td>
   </tr>
</table>
</form>
</span>

</BODY>
</HTML>
```

myvars.aspx

```
<script language="VB" runat="server">

'Set the logoutPopup window flag - 0 = no popup, 1 = popup
'The use of the logoutPopup in this script is discouraged because the login event is
exclusive.
Dim logoutPopup as String = "0"

'Set the debug flag (0 = off, 1 = on)
Dim debugFlag as String = "0"

'Set the path and file for the PDT responder script - this should be the same path as
the LHM settings
'configured on the SonicWall "External Web Server Settings" page, but pointing to
the PDT handler script.
'Refer to http://www.paypal.com/cgi-bin/webscr?cmd=p/xcl/rec/pdt-techview-outside
for information on PDT
Dim pdtPath as String = "http://10.50.165.2/lhm/paypal/pdt.aspx"

'Set the path the PayPal processing CGI.Use the sandbox
(https://developer.paypal.com) and (https://www.sandbox.paypal.com) for testing
'Using the sandbox requires a developer network account and login.
Dim paypalCGI as String = "https://www.sandbox.paypal.com/cgi-bin/webscr"
'Dim paypalCGI as String = "https://www.paypal.com/cgi-bin/webscr"

'Set the email address of the PayPal merchant account to which payment will be made
'The following is a valid sandbox account, but requires authentication by the parent
(real) account.
'You must replace this with you own (real or sandbox account) for use.
Dim myBusiness as String = "lhmdemo@SonicWall.com"

'Set this to token from PayPal account.It must be your actual, valid token.
'Refer to http://paypaltech.com/PDTGen/PDTtokenhelp.htm for information on the
identity token
```

```
'The following is a valid sandbox token, but requires authentication by the parent
(real) account.
'You must replace this with you own (real or sandbox token) for use.
Dim token as String = "ucistq6vmKGWPxwJbrTJFDhFq889RxYt_6Mkz_3viraSzjiQJ5iPYCZ5Mdq"

'Set the names for the purchase item options (e.g. 1 hour Access, 3 hours access,
etc.)
Dim itemName1 as String = "1 Hour Secure Internet Access"
Dim itemName2 as String = "24 Hours Secure Internet Access"

'Set the paypal querystring number for purchase item options (e.g. 1hour, 60mins,
itemone, etc.)
Dim itemNumber1 as String = "1hour"
Dim itemNumber2 as String = "24hour"

'Set the purchase item options session and idle timers (timers use the same value
since we do not want sessions idling out)
Dim itemTimer1 as String = "3600"'One hour, in minutes
Dim itemTimer2 as String = "86400"'24 hours

'Set the costs in dollars for purchase item options (e.g. one penny = 0.01, one
dollar = 1.00, etc.)
Dim itemAmount1 as String = "0.01"
Dim itemAmount2 as String = "0.02"

'Set the button names and descriptions for purchase item options
Dim itemButton1 as String = "1 Hour Access - $0.01"
Dim itemButton2 as String = "24 Hours Access - $0.02"

'Set the secret for use with optional HMAC auth, as configured in the Extern Guest
Auth config on the SonicWall
Dim strHmac as String = "password"

'Set the digest method for the HMAC, either MD5 or SHA1
Dim hmacType as String = "MD5"
'Dim hmacType as String = "SHA1"

'Set the logo image to use
Dim logo as String = "SonicWall.gif"
'------------------------End of Configurable Settings-------------------------

</script>
```

pdt.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWall authorizing the LHM session.
```

```
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
      As Boolean Implements ICertificatePolicy.CheckValidationResult
      Return True
   End Function
End Class

'Sample LHM redirect querystring:
'http://127.0.0.1/lhm/paypal/default.aspx?sessionId=0b712fd83b9f5313db5af1cea6b1004
f&ip=10.50.165.231&mac=00:0e:35:bd:c9:37&ufi=0006b11184300&mgmtBaseUrl=https://10.5
0.165.193:4043/&clientRedirectUrl=https://10.50.165.193:444/&req=http%3A//www.googl
e.com/ig

Dim ip as String
Dim sessionId as String
Dim mac as String
Dim ufi as String
Dim mgmtBaseUrl as String
Dim clientRedirectUrl as String
Dim req as String
Dim sessTimer as String
Dim idleTimer as String
Dim userName as String
Dim hmac as String
Dim firstname, lastName, itemName, mcGross, mcCurrency, itemNumber, business, txn,
payStatus As String

Sub Page_Load(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles
MyBase.Load

   'Use the override class to accept untrusted certificates from the SonicWall
   'This is necessary for the POST to the SonicWall authorizing the LHM session.
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   Dim tx, PDTvalidateQuery As String
   Dim strResponse As HttpWebResponse
   Dim temp As String
   Dim PDTArray() As String
   Dim iParts, sResults(0, 0), aParts(), sParts(), sKey, sValue, snwlCustom As String
   Dim i As Integer

   'Set tx to value of tx passed in via Querystring from PayPal
   tx = Request.QueryString("tx")

   'Set string = to the cmd value, tx and at that needs to be
   'POSTed back to PayPal to validate the PDT
   PDTvalidateQuery = "cmd=_notify-synch&tx=" & tx & "&at=" & token

   'Now we need to POST this info back to PayPal for validation of the PDT
   'Create the request back
   Dim req As HttpWebRequest = CType(WebRequest.Create(paypalCGI), HttpWebRequest)

   'Set values for the request back
   'set method
    req.Method = "POST"
    'set content type
    req.ContentType = "application/x-www-form-urlencoded"
    'set length
```

```
    req.ContentLength = PDTvalidateQuery.Length

   'Write the request back to PayPal
   Dim stOut As StreamWriter = New StreamWriter(req.GetRequestStream(),
Encoding.ASCII)
   stOut.Write(PDTvalidateQuery)
   stOut.Close()

   Try
      strResponse = CType(req.GetResponse(), HttpWebResponse)
   Catch ex As SystemException
      catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
   End Try

         'Once we write the stream back to PayPal, we need to read the response.

         Dim IPNResponseStream As Stream = strResponse.GetResponseStream
         Dim encode As Encoding = System.Text.Encoding.GetEncoding("utf-8")
         Dim readStream As New StreamReader(IPNResponseStream, encode)

         'Read the response in String variable "temp"
         temp = readStream.ReadToEnd

      'Debug flag, set in myvars - prints the whole output from the POST reply
      If debugFlag = "1" Then
         OutputEntirePDTString(temp)
      End If

         'Check to see if the 1st line of the response was "SUCCESS"
         If Mid(temp, 1, 7) = "SUCCESS" Then

             'if it is SUCCESS, the code below puts the response in a nice array
             temp = Mid(temp, 9)
             sParts = Split(temp, vbLf)
             iParts = UBound(sParts) - 1
             ReDim sResults(iParts, 1)

             For i = 0 To iParts

                 aParts = Split(sParts(i), "=")
                 sKey = aParts(0)
                 sValue = aParts(1)
                 sResults(i, 0) = sKey
                 sResults(i, 1) = sValue

                 'You can add more case statements here for other returned variables

           Try
                 Select Case sKey
                     Case "first_name"
                         firstname = Server.URLDecode(sValue)
                     Case "last_name"
                         lastName = Server.URLDecode(sValue)
                     Case "item_name"
                         itemName = Server.URLDecode(sValue)
                     Case "mc_gross"
                         mcGross = sValue
                     Case "mc_currency"
                         mcCurrency = sValue
             Case "item_number"
                itemNumber = Server.URLDecode(sValue)
```

```
            Case "business"
               business = Server.URLDecode(sValue)
            Case "txn_id"
               txn = sValue
            Case "payment_status"
               payStatus = sValue
                   Case "custom"
               snwlCustom = sValue
               sessionID = snwlCustom.SubString(0,32)
               mgmtBaseUrl=(Server.URLDecode(Mid(snwlCustom,33)))
               End Select
        Catch ex as Exception
           catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
        End Try

            Next

        If payStatus = "Completed" Then
           'Transaction Succeeded - Give the Guest a receipt
           Dim receipt as String

           receipt =  "<h3>Transaction Succeeded.Thank you for selecting SonicWall
LHM.</h3><br>"
           receipt + = "<b>Transaction Invoice:</b><br><br>"
           receipt + = "Name: " & firstname & " " & lastName & "<br>"
           receipt + = "Description: " & itemName & "<br>"
           receipt + = "Amount: " & mcCurrency & " " & mcGross &"<br>"
           receipt + = "Paid to: " & business &"<br>"
           receipt + = "Transaction ID: " & txn &"<br>"
           receipt + = "<br><br>"

           paypalResult.Text = receipt

           LHMResult.Text = "Authorizing your LHM session."

           'Setup the LHM session variables and call LHM Routine
           'Set the session and idle timers to match the variables set in myvars
           If itemNumber = itemNumber1 Then
              sessTimer=itemTimer1
              idleTimer=itemTimer1
           Else
              sessTimer=itemTimer2
              idleTimer=itemTimer2
           End If

           userName = firstname & " " & lastName

           LHM()
        Else
           'The transaction itself was a success, but the payment status was not
Completed.
           paypalResult.Text = "The transaction succeeded, but the payment was not
completed.The session cannot be authorized at this time."
        End If

        Else
            ' If PDT response is not "SUCCESS"
           paypalResult.Text = "The PayPal transaction did not succeed.The returned
status is: <b>" &  temp & "</b>"
        End If
```

```
        'Close the streams
        readStream.Close()
        strResponse.Close()

    End Sub

   'This is the parser for the debug function to print the entire resonse to the PDT
POST
    Private Function OutputEntirePDTString(ByVal myPDTString As String) As String
        Dim tempString() As String = Split(myPDTString, vbLf)
        Dim x As Integer
        For x = 0 To tempString.GetUpperBound(0)
            Response.Write(tempString(x) & "<br>")
        Next
    End Function

Sub LHM()

   'Let the user know that we are setting up the session, just in case it takes more
than a second
   LHMResult.Text = "Authorizing session.Please wait."

   'The LHM cgi on the SonicWall - this does not change
   Dim loginCgi as String = "externalGuestLogin.cgi"

   'Assemble the data to post back to the SonicWall to authorize the LHM session
   Dim loginParams as String = "sessId=" & sessionId & "&userName=" &
Server.URLEncode(userName) & "&sessionLifetime=" & sessTimer & "&idleTimeout=" &
idleTimer

   'Combine mgmtBaseUrl from the original redirect with the login cgi
   Dim postToSNWL as String = mgmtBaseUrl & loginCgi

   'Convert the loginParams to a well behaved byte array
   Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

   Try
      'Create the webrequest to the SonicWall
      Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

      'Calculate the length of the byte array
      toSNWL.ContentLength = byteArray.Length

      'Set the method for the webrequest to POST
      toSNWL.Method = "POST"

      'Set the content type
      toSNWL.ContentType = "application/x-www-form-urlencoded"

      'Open the request stream
      Dim dataStream As Stream = toSNWL.GetRequestStream()

      'Write the byte array to the request stream
      dataStream.Write(byteArray, 0, byteArray.Length)

      'Close the Stream object
      dataStream.Close()

      'Get the response
      Dim snwlReply As WebResponse = toSNWL.GetResponse()
```

```
      'Display the status - looking for 200 = OK.
      'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

      'Grab the response and stuff it into an xml doc for possible review
      Dim snwlResponse as XmlDocument = New XmlDocument()
      snwlResponse.Load(snwlReply.GetResponseStream())

      'Set the xPath to the SNWL reply, and get the response
      Dim codePath as String =
"SonicWallAccessGatewayParam/AuthenticationReply/ResponseCode"

      'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

      'Response code 50 - Login Succeeded

      If snwlResponse.SelectSingleNode(codePath).InnerXml = "50"

         'Do we want to provide a logout popup window?
         If logoutPopup = "1" Then
            'Popup hack using Javascript for logout window
            Dim sb As New System.Text.StringBuilder()
            sb.Append("<script language='javascript'>")
            sb.Append("window.open('logout.aspx?sessId=")
            sb.Append(Server.URLEncode(CStr(sessionId)))
            sb.Append("&mgmtBaseUrl=")
            sb.Append(Server.URLEncode(CStr(mgmtBaseUrl)))
            sb.Append("&sessTimer=")
            sb.Append(Server.URLEncode(CStr(sessTimer)))
            sb.Append("','logOut','toolbar=no,")
            sb.Append("addressbar=no,menubar=no,")
            sb.Append("width=400,height=250');")
            sb.Append("<")
            sb.Append("/")
            sb.Append("script>")
            RegisterStartupScript("stp", sb.ToString)
         End If

         LHMResult.Text = "<br><b><font color=""green"">Session
authorized:</font></b> You may now begin your secure Internet access session."

      'Response code 51 - Session Limit Exceeded
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "51"
         LHMResult.Text = "<br><b><font color=""red"">Session Limit
Reached:</font></b> The maximum number of guest session has been reached.Sorry for
the inconvenience.Please close and relaunch your browser to try again."

      'Response code 100 - Login Failed.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "100"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> Your session cannot be created at this time.Sorry for the
inconvenience.Please close and relaunch your browser to try again."

      'Response code 251 - Bad HMAC.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed message authentication.Sorry
for the inconvenience.Please close and relaunch your browser to try again."

      'Response code 253 - Invalid SessionID.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
```

```
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed to match a known session
identity.Sorry for the inconvenience.Please close and relaunch your browser to try
again."

     'Response code 254 - Invalid CGI.
     ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization was missing an essential
parameter.Sorry for the inconvenience.Please close and relaunch your browser to try
again."

     'Response code 255 - Internal Error.
     ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified
error.Sorry for the inconvenience.Please close and relaunch your browser to try
again."

     End If

     'Close the streams
     dataStream.Close()
     snwlReply.Close()

     'If there is some asp.net error trying to talk to the SonicWall, print it in
the same color as the background.
     Catch ex as Exception
        catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified
error.Sorry for the inconvenience.Please close and relaunch your browser to try
again.If the problem persists, please notify an attendant."
     End Try
End Sub

</script>

<STYLE>
body {
  font-size: 10pt;
  font-family: verdana,helvetica,arial,sans-serif;
  color:#000000;
  background-color:#9CBACE;
}

tr.heading {
  background-color:#006699;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM PayPal Script</TITLE>
</HEAD>
```

```
<BODY>

<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
   <tr class="heading">
      <td width="50%" valign="center"><font color="white"><b>LHM Access with PayPal
Buy Now</b></font></td>
      <td><center><img width="216" height="51" src="<%= logo%>"></center></td>
      <td width="50%" align="right" valign="center"><font color="white"><b>Powered
by SonicWall LHM</b> </font></td>
   </tr>
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>

<table width="100%" border="0" cellpadding="2" cellspacing="0">

   <tr>
   <td><br></td>
   </tr>
   <tr>
      <td><asp:Label id=paypalResult runat="server" /></td>
   </tr>
   <tr>
      <td><asp:Label id=LHMResult runat="server" /></td>
   </tr>
   <tr>
      <td><asp:Label id=catchError runat="server" /></td>
   </tr>
</table>
</BODY>
</HTML>
```

ランダム スクリプト

認証モデル

ゲスト クライアントは、アルゴリズムによって検証され、ランダムに生成されたパスコードを入力します。

目的

従来のパスコード認証では、パスコードを使用前に生成して認証側プラットフォーム上に保存しておく必要があります。例えば、無線ゲストサービスでは、アカウントが使用される特定の SonicWall セキュリティ装置上でアカウントを生成する必要があります。このランダム スクリプトでは、パスコードを生成および検証するためのソルト化されたアルゴリズムを使用することで、こうした依存関係が排除されます。つまり、パスコードをどこにも保存する必要がなく、ソルトが同じである限り、パスコードは完全に移動可能です (異なる LHM サーバを照会する場合であっても任意のサイトで使用できます)。

このことの実用的意義は、ゲスト アカウントのパスコードを一括で生成し、配布して、今後いつでも使用できることにあります。例えば、パスコードを (特定のソルトを使用して) 生成し、(例えば、証明書、名刺、スクラッチ カードに) 印刷して、LHM サーバが同じアルゴリズム的なソルトを採用している任意のサイトで使用することができます。パスコードには、(相対的でなく) 絶対的な有効期限を与えることができます。この期限を過ぎると、ソルトを変更して期限切れのパスコードを無効化できます。

複数のサイトにわたって一連のパスコードを検証するために使用可能な一般的なソルトと同じ方法で、一意のソルトによって、あるサイトで生成されたパスコードを、異なるソルトによる別のサイトでは使用できないようにすることができます。すべてのパスコードの生成と検証に一般的なアルゴリズムを使用しても、ハッシュ関数にソルトを追加することで必要に応じて一意性を実現できます。

`default.aspx` スクリプト以外に、`generator.aspx` スクリプトがあります。このスクリプトではパスコードが生成されます。どこでも 1 ～ 999 個のパスコードを一度に生成できます。生成した後、個々のパスコードを印刷したり、全体のリストを `.csv` ファイルにエクスポートしたりできます。

サポートされていた 2 つのクラスのパスコードは1 時間のものと 24 時間のものです。どちらの種別のパスコードも、生成器 (generator) スクリプトによって生成できます。

生成アルゴリズムのしくみは次のとおりです。

1. 文字数が `randChars` (既定値が 6 の整数、`myvars` 内に定義されています) のランダム コード (ルートパスコード) を生成します。ランダム コード生成器の文字セットは `default.aspx` ファイル内で変更できます。
2. ソルト (ソルト文字列として `myvars` 内に定義されています) が接頭辞としてルートパスコードに追加されます。
3. 次に、結果として得られた文字列に対して SHA1 ハッシュが計算されます。続いて、3 つのペアの文字がハッシュから取得されます。
   - 1 時間のパスコードの場合、408 ペアが取得されます (文字 4,5 + 0,1 + 8,9)。
   - 24 時間のパスコードの場合、752 ペアが取得されます (文字 7,8 + 5,6 + 2,3)。
4. その後、ハッシュから選ばれた 6 つの文字が連結されてルートパスコードになります。
5. 結果として配布可能なパスコードが得られます。

検証アルゴリズムは、次のように逆の順序で機能します。

1 ゲスト クライアントは自らのパスコード (これを enteredCode とします) を入力します。

2 スクリプトは入力されたコードの最初の randChars 文字を取得します (これをルートパスコードとします)。

3 ソルトはルートパスコードに接頭辞として追加されたものであり、SHA1 ハッシュが計算されます。408 ペアの文字が取得され、ルート パスコードに付加されます。次に、この 408 ペアと enteredCode とのマッチングを行います。

- 408ペアが一致した場合は、1時間のパスコードとして検証されたことになります。
- 408 ペアが一致しなかった場合は、752 ペアとのマッチングを試みます。これが enteredCode に一致した場合は、24 時間のパスコードとして検証されたことになります。
- どちらも一致しなかった場合、コードは不正です。

enteredCode の検証が済んだ後、usedcodes.mdb データベースに対するクエリによってこのコードが使用済みであるかどうかを確認します。enteredCode がデータベースに見つからなかった場合、LHM セッション承認シーケンスが開始され、MAC アドレスが userName (ユーザ名) として使用されます。LHM セッションが承認されて LHM サーバが確認を受信した後、enteredCode から得られたルートパスコードが再利用できないように usedcodes.mdb データベースに書き込まれます。ソルトが変更された場合は、データベースを消去することをお勧めします。

myvars 変数

logoutPopup	ログアウト ポップアップ ウィンドウの使用を制御します。次のように設定します。 • **0**: ポップアップ ウィンドウを無効にします。 • **1**: ポップアップ ウィンドウを有効にします。
useDB	使用されるパスコード データベースの使用を制御します。useDB の値によって処理は次のように異なります。 • **0** の場合、データベースに対する読み取りも書き込みも行われず、パスコードを繰り返し使用できます。 • **1** の場合、使用されたパスコードはデータベースに書き込まれ、新しい認証処理では、データベースをチェックして、パスコードが使用済みであるかどうかを確認します。
randChars	ルートパスコードに含めるランダム文字の数。既定値は 6 です。この場合、パスコードは 12 文字になります。ハッシュ コンポーネントでは常に 6 文字がさらに追加されるためです。
salt	ハッシュの計算時に使用されるソルト。不必要なパスコードの移行/衝突を避けるために、必ず適切なソルトを使用してください。
sessTimer	秒単位のセッション タイマー。
idleTimer	秒単位の無動作タイマー。
strHmac	オプションの HMAC 機能のための事前共有鍵。

hmacType	HMAC 使用時に用いるダイジェスト種別: 「**MD5**」または「**SHA1**」を選択します。
logo	ページ ヘッダーで使用するロゴ (画像) ファイルの名前。

セッション フロー

1. ゲスト クライアントは自らのパスコードを入力します。
2. パスコードがアルゴリズムによって検証されます (上記の「**目的**」セクションを参照してください)。
3. コードが検証された場合は、前回の使用の有無が `usedcodes.mdb` データベースでチェックされます。
4. データベースに存在しない場合、LHM セッション (1 時間または 24 時間) が開始され、MAC アドレスがユーザ名として使用されます。
5. LHM セッションの開始後、スクリプトはルートパスコードを再利用できないように `usedcodes.mdb` データベースに書き込みます。
6. スクリプトは、セッションを承認するために SonicWall セキュリティ装置に対する LHM ポストを実行します。

追加の考慮事項

このスクリプトはデータベースへの書き込みを行うため、**IUSR_MACHINENAME** および **IWAM_MACHINENAME** (または **ASPNET**) アカウントに対して書き込み権限を設定する必要があります (「SonicWall によって提供されたサンプル スクリプトを使用したいと考えています。使用するためには何が必要ですか。 (855 ページ)」を参照してください)。

`generator.aspx` スクリプトは、ウェブ サーバ上の保護された (パブリックにアクセスできない) 領域には置かないでください。

トピック:

- default.aspx (955 ページ)
- generator.aspx (964 ページ)
- logout.aspx (968 ページ)
- myvars.aspx (974 ページ)
- print.aspx (974 ページ)

default.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Data" %>
<%@ Import Namespace="System.Data.OleDB" %>
<%@ Import Namespace="System.Security" %>
<%@ Import Namespace="System.Security.Cryptography" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWall authorizing the LHM session.
```

```
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
      As Boolean Implements ICertificatePolicy.CheckValidationResult
      Return True
   End Function
End Class

'Sample LHM redirect querystring:
'http://127.0.0.1/lhm/random/default.aspx?sessionId=0b712fd83b9f5313db5af1cea6b1004
f&ip=10.50.165.231&mac=00:0e:35:bd:c9:37&ufi=0006b11184300&mgmtBaseUrl=https://10.5
0.165.193:4043/&clientRedirectUrl=https://10.50.165.193:444/&req=http%3A//www.googl
e.com/ig

Dim ip as String
Dim sessionId as String
Dim mac as String
Dim ufi as String
Dim mgmtBaseUrl as String
Dim clientRedirectUrl as String
Dim req as String
Dim hmac as String
Dim customCode as String

Dim passCode as String
Dim grabCode as String

Sub Page_Load(Source as Object, E as EventArgs)

   LHMResult.Text=""
   catchError.Text=""
   authResult.Text=""

   ip=Request.QueryString("ip")
   sessionId=Request.QueryString("sessionId")
   mac=Request.QueryString("mac")
   ufi=Request.QueryString("ufi")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
   clientRedirectUrl=Request.QueryString("clientRedirectUrl")
   req=Request.QueryString("req")
   hmac=Request.QueryString("hmac")
   customCode=Request.QueryString("cc")

   'customCode grabs the "cc=" querystring value sent by the SonicWall.This allows
you to use the same
   'page (e.g. this page) for the "Session Expiration" (?cc=2), "Idle Timeout"
(?cc=3) and "Max Sessions" (?cc=4) page.
   If customCode <> "" Then
      Select Case customCode
      Case "2"
         LHMResult.Text="<br><H3><font color=""red"">Your LHM session has expired.You
may try to initiate a new session.</font></H3>"
      Case "3"
         LHMResult.Text="<br><H3><font color=""red"">You have exceeded your idle
timeout.Please log back in.</font></H3>"
      Case "4"
         LHMResult.Text="<br><H3><font color=""red"">The maximum number of sessions
has been reached.Please try again later.</font></H3>"
      End Select
```

```
   End If

   'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWall
   'This is necessary for the POST to the SonicWall authorizing the LHM session.
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   'Note - the routine below for handling the hmac requires the use of the
SonicSSL.dll and libeay.dll libraries.
   'The DLL must be copied to the IIS server, and the SonicSSL dll must be registered
with "regsvr32 sonicssl.dll"
   If hmac <> "" Then

      'SonicWall URL Encode routine is different from Microsoft - this is the
SonicWall method
      req=Replace(req,"%","%25")
      req=Replace(req,":","%3A")
      req=Replace(req," ","%20")
      req=Replace(req,"?","%3F")
      req=Replace(req,"+","%2B")
      req=Replace(req,"&","%26")
      req=Replace(req,"=","%3D")

      Dim strHmacText as String
      Dim objCrypto as Object
      Dim strHmacGenerated
      Dim loginError as String

      'Initialize the Crypto object
      objCrypto = Server.CreateObject("SonicSSL.Crypto")

      'The text to be encoded
      strHmacText = sessionId & ip & mac & ufi & mgmtBaseUrl & clientRedirectUrl &
req

      'Calculate the hash with a key strHmac, the return value is a string converted
form the output sha1 binary.
      'The hash algorithm (MD5 or SHA1) is configured in myvars and in the Extern
Guest Auth config on the SonicWall
      If hmacType = "MD5" Then
         strHmacGenerated = objCrypto.hmac_md5(strHmacText, strHmac)
      Else
         strHmacGenerated = objCrypto.hmac_sha1(strHmacText, strHmac)
      End If

      If strHmacGenerated <> hmac Then
         Dim hmacFail as String
         hmacFail = "<font color=""red"">The HMAC failed validation.Please notify an
attendant.</font><br><br>"
         hmacFail+="<font color=""9CBACE"">Received HMAC: " & hmac & "<br>Calculated
HMAC: " & strHmacGenerated & "<br>"
         hmacFail+="Make sure the digest functions on the SonicWall and LHM server
match.<br>"
         hmacFail+="Also make sure the shared secret on the SonicWall and myvars
match</font>"
         catchError.Text=hmacFail
      End If

   End If

End Sub
```

```
sub OnBtnClearClicked (Sender As Object, e As EventArgs)
   enteredCode.Text = ""
   LHMResult.Text=""
   catchError.Text=""
end sub

Sub btnSubmit_Click(Sender As Object, E As EventArgs)

   'The following subroutine validates client provided passcodes.
   'The first 6 characters (definable in myars) are grabbed.
   'These characters are then run though a SHA1 hash with a salt that is defined in
myvars.

   '3 pairs of substrings are then retrieved from the hash.
   'The code is validated if the 3 pairs concatenated to the randChars (defined in
myvars) characters consist of the following:

   'Validating the 4 0 8 pairs (4,5+0,1+8,9 characters) will provide 1 hour of guest
access.
   'Validating the 7 5 2 pairs (7,8+5,6+2,3 characters) will provide 24 hours of
guest access.

   grabCode = enteredCode.Text.SubString(0,randChars)

   'Manually compute SHA1 on salt+randomCode, and convert result to base64 - gives
stranger output
   Dim sha1 As sha1 = sha1.Create()
   Dim manualHash As Byte() = sha1.ComputeHash(Encoding.UTF8.GetBytes(salt &
grabCode))
   Dim hashResult as String = Convert.ToBase64String(manualHash)

   'Alternatively, use forms hash routine - only provides upper case A-Z + 0-9
output.
   'Dim hashResult as String =
FormsAuthentication.HashPasswordForStoringInConfigFile(salt & randomCode,"SHA1")

   'First try to match on 1 hour code
   passCode  = ""
   passCode = grabCode & hashResult.SubString(4, 2)
   passCode = passCode & hashResult.SubString(0, 2)
   passCode = passCode & hashResult.SubString(8, 2)
   If enteredCode.Text = passCode Then
      sessTimer = "3600"
      authResult.Text="<font color=""green""><b>1 hour code validated.</b></font>"

      'Check the used passcode DB if useDB is enabled in myvars.
      If useDB = "1" Then
         wasItUsed()
      End If
   Else
      'Now try to match on 24 hour code
      passCode = ""
      passCode = grabCode & hashResult.SubString(7, 2)
      passCode = passCode & hashResult.SubString(5, 2)
      passCode = passCode & hashResult.SubString(2, 2)
      If enteredCode.Text = passCode Then
         sessTimer = "86400"
         authResult.Text="<font color=""green""><b>24 hour code
validated.</b></font>"
```

```
        'Check the used passcode DB if useDB is enabled in myvars.
        If useDB = "1" Then
           wasItUsed()
        End If

     Else
        authResult.Text="<font color=""Red""><b>Passcode cannot be
validated.</b><br>The passcode is case-sensitive.<br>Please try again.</font>"
     End if
   End If

End Sub

Sub wasItUsed ()

   'Check to see if the root (randChars) of the passcode is already in the used
database.
   Dim strConn as string = "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" &
server.mappath("usedcodes.mdb") & ";"
   Dim MySQL as string = "SELECT * From passCodes Where passCode = '" & grabCode &
"'"
   Dim MyConn as New OleDBConnection (strConn)
   Dim cmd as New OleDBCommand (MySQL, MyConn)
   Dim objDR As OleDbDataReader
   Dim isUsed As Boolean

   MyConn.Open()
   objDR = cmd.ExecuteReader()
   isUsed = objDR.Read()
   objDR.Close()
   MyConn.Close()

   'If the passcode is not found in the database
   if isUsed = False
      LHM()
   Else
      authResult.Text="<font color=""Red""><b>Passcode has already been
used.</b><br>Please see an attendant for assistance.</font>"
   End If

End Sub

Sub writeToDB ()

   'Try to write the submitted (only randChars characters instead of the whole
passcode) info to the database file
   Try
      Dim strConn as string = "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" &
server.mappath("usedcodes.mdb") & ";"

      Dim MySQL as string = "INSERT INTO passCodes (passCode) VALUES ('" & grabCode &
"')"
      Dim MyConn as New OleDBConnection (strConn)
      Dim cmd as New OleDBCommand (MySQL, MyConn)
      MyConn.Open ()
      cmd.ExecuteNonQuery ()
      MyConn.Close ()

      Catch ex as Exception
         catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
   End Try
```

```
End Sub

Sub LHM()

   'The writeToDB sub is in the Response code 50 - Login Succeeded routine, after the
LHM exchange succeeds.You may move it to the top to write the passcode to the DB
before the LHM transaction for testing purposes.
   'writeToDB ()

   enteredCode.Text = "Code Accepted."

   'Let the user know that we are setting up the session, just in case it takes more
than a second
   LHMResult.Text = "Authorizing session.Please wait."

   'The LHM cgi on the SonicWall - this does not change
   Dim loginCgi as String = "externalGuestLogin.cgi"

   'Assemble the data to post back to the SonicWall to authorize the LHM session
   Dim loginParams as String = "sessId=" & sessionId & "&userName=" & mac &
"&sessionLifetime=" & sessTimer & "&idleTimeout=" & idleTimer

   'Combine mgmtBaseUrl from the original redirect with the login cgi
   Dim postToSNWL as String = mgmtBaseUrl & loginCgi

   'Convert the loginParams to a well behaved byte array
   Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

   Try
      'Create the webrequest to the SonicWall
      Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

      'Calculate the length of the byte array
      toSNWL.ContentLength = byteArray.Length

      'Set the method for the webrequest to POST
      toSNWL.Method = "POST"

      'Set the content type
      toSNWL.ContentType = "application/x-www-form-urlencoded"

      'Open the request stream
      Dim dataStream As Stream = toSNWL.GetRequestStream()

      'Write the byte array to the request stream
      dataStream.Write(byteArray, 0, byteArray.Length)

      'Close the Stream object
      dataStream.Close()

      'Get the response
      Dim snwlReply As WebResponse = toSNWL.GetResponse()

      'Display the status - looking for 200 = OK.
      'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

      'Grab the response and stuff it into an xml doc for possible review
      Dim snwlResponse as XmlDocument = New XmlDocument()
      snwlResponse.Load(snwlReply.GetResponseStream())
```

```
      'Set the xPath to the SNWL reply, and get the response
      Dim codePath as String =
"SonicWallAccessGatewayParam/AuthenticationReply/ResponseCode"

      'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

      'Response code 50 - Login Succeeded

      If snwlResponse.SelectSingleNode(codePath).InnerXml = "50"

         'Do we want to provide a logout popup window?
         If logoutPopup = "1" Then
            'Popup hack using Javascript for logout window
            Dim sb As New System.Text.StringBuilder()
            sb.Append("<script language='javascript'>")
            sb.Append("window.open('logout.aspx?sessId=")
            sb.Append(Server.URLEncode(CStr(sessionId)))
            sb.Append("&mgmtBaseUrl=")
            sb.Append(Server.URLEncode(CStr(mgmtBaseUrl)))
            sb.Append("&sessTimer=")
            sb.Append(Server.URLEncode(CStr(sessTimer)))
            sb.Append("','logOut','toolbar=no,")
            sb.Append("addressbar=no,menubar=no,")
            sb.Append("width=400,height=250');")
            sb.Append("<")
            sb.Append("/")
            sb.Append("script>")
            RegisterStartupScript("stp", sb.ToString)
         End If

         LHMResult.Text = "<br><b><font color=""green"">Session
authorized:</font></b> You may now go to the URL you originally requested: <a
target=""_blank"" href=""" & req & """>" & req & "</a>"

         'Write the passcode the DB if the LHM session succeeds and if useDB = 1.
         If useDB = "1" Then
            writeToDB ()
         End If

      'Response code 51 - Session Limit Exceeded
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "51"
         LHMResult.Text = "<br><b><font color=""red"">Session Limit
Reached:</font></b> The maximum number of guest session has been reached.Sorry for
the inconvenience.Please close and relaunch your browser to try again."

      'Response code 100 - Login Failed.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "100"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> Your session cannot be created at this time.Sorry for the
inconvenience.Please close and relaunch your browser to try again."

      'Response code 251 - Bad HMAC.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed message authentication.Sorry
for the inconvenience.Please close and relaunch your browser to try again."

      'Response code 253 - Invalid SessionID.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed to match a known session
```

```
identity.Sorry for the inconvenience.Please close and relaunch your browser to try
again."

     'Response code 254 - Invalid CGI.
     ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization was missing an essential
parameter.Sorry for the inconvenience.Please close and relaunch your browser to try
again."

     'Response code 255 - Internal Error.
     ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified
error.Sorry for the inconvenience.Please close and relaunch your browser to try
again."

     End If

     'Close the streams
     dataStream.Close()
     snwlReply.Close()

     'If there is some asp.net error trying to talk to the SonicWall, print it in
the same color as the background.
     Catch ex as Exception
        catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified
error.Sorry for the inconvenience.Please close and relaunch your browser to try
again.If the problem persists, please notify an attendant."
     End Try
End Sub


</script>

<STYLE>
body {
  font-size: 10pt;
  font-family: verdana,helvetica,arial,sans-serif;
  color:#000000;
  background-color:#9CBACE;
}

tr.heading {
  background-color:#006699;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Random Script</TITLE>
</HEAD>

<BODY>
```

```
<form id="frmValidator" onKeyPress="if(event.keyCode==13)
{document.getElementById('btnSubmit').click(); return false}" runat="server">

<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
   <tr class="heading">
      <td width="50%" valign="center"><font color="white"><b>Algorithmic
Authentication</b></font></td>
      <td><center><img width="216" height="51" src="<%= logo %>"></center></td>
      <td width="50%" align="right" valign="center"><font color="white"><b>Powered
by SonicWall LHM</b> </font></td>
   </tr>
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>

<table width="90%" border="0" cellpadding="2" cellspacing="0">
   <tr>
      <td><b>Welcome <%= ip%> to SonicWall's LHM Algorithmic
Authenticator.</b><br><br>Enter your unique randomly generated passcode to obtain
secure guest Internet access.<br><br>Valid passcodes are not stored anywhere, so
validation is not performed against any kind of database.Instead, when a passcode is
entered, it is algorithmically validated.After a passcode is successfully used, it
is written to a "used passcode" database so that it cannot be reused.<br><br>The
validator will recognize 1 hour and 24 hour passcodes - these characteristics were
encoded within the passcodes themselves during generation.<br><br>
      </td>
   </tr>
</table>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr><br>
      <td width="30%">Enter your passcode:</td>
      <td width="30%"><asp:TextBox id="enteredCode" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valEnteredCode"
ControlToValidate="enteredCode" ErrorMessage="Please enter your passcode."
runat="server" /></td>
   </tr>
   <tr>
      <td></td><td colspan=2><asp:Label id=authResult runat="server" /> </td>
   </tr>
   <tr>
      <td></td>
      <td><asp:button id="btnSubmit" class="button" text="  Submit  "
onClick="btnSubmit_Click" runat="server" />
        
      <asp:button id="btnClear" class="button" text=" Clear "
CausesValidation="False" onClick="OnBtnClearClicked" runat="server" />
      </td>
   </tr>
   <tr>
      <td colspan=2><asp:Label id=LHMResult runat="server" /></td>
   </tr>
   <tr>
```

```
      <td colspan=2><asp:Label id=catchError runat="server" /></td>
   </tr>
</table>
</form>
</BODY>
</HTML>
```

generator.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Data" %>
<%@ Import Namespace="System.Data.OleDB" %>
<%@ Import Namespace="System.Security" %>
<%@ Import Namespace="System.Security.Cryptography" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

Dim genCodes As New ArrayList()
Dim codeType As String

Sub Page_Load(Source as Object, E as EventArgs)
   If Not isPostBack Then
      Heading.Text=" "
      btnExport.Visible = False
   End If
End Sub

Sub btnSubmit_Click(Sender As Object, E As EventArgs)
   'The following generates passcodes beginning with a random character generator.
   'The number of characters in randomCode is configurable in myvars.
   'The randomCode output is then run though a SHA1 hash with a salt that is defined
in myvars.
   'Note: If you are using this in a live environment, it is important to change the
salt to prevent algorithm compromise.

   '3 pairs of substrings are then retrieved from the hash, and concatenated to the
randomCode to form the passcode.

   'In the current sample implementation:
   'The 4 0 8 pairs (4,5+0,1+8,9 characters) from the hash will provide 1 hour of
guest access.
   'The 7 5 2 pairs (7,8+5,6+2,3 characters) from the hash will provide 24 hours of
guest access.

   Dim myLooper As Integer
   Dim passCode as String

      For myLooper = 1 to Convert.ToInt32(codeCount.Text)

         Dim x As Integer = 0
         Dim isitRand as boolean = False
         Dim intRand as Integer = 0
```

```
        Dim randomCode as String = ""

        For x = 1 to randChars
           Do Until isItRand = True
              '48 to 57 for numbers, 65 to 90 for uppercase, 97 to 122 for lowercase
              intRand = Int((122 - 48 + 1) * Rnd + 48)
              'Select the legal characterset for randomCode by including legal
characters below.
              If InStr(1, "abcdefgh jk mn pqrstuvwxyzABCDEFGH JKLMN PQRSTUVWXYZ
23456789 ",Chr(intRand), 1) Then
                 isItRand = True
              End If
           Loop
           randomCode = randomCode & Chr(intRand)
           isItRand = False
        Next

        'Manually compute SHA1 on salt+randomCode, and convert result to base64 -
gives stranger output
        Dim sha1 As sha1 = sha1.Create()
        Dim manualHash As Byte() = sha1.ComputeHash(Encoding.UTF8.GetBytes(salt &
randomCode))
        Dim hashResult as String = Convert.ToBase64String(manualHash)

        'Alternatively, use forms hash routine - only provides upper case A-Z + 0-9
output.
        'Dim hashResult as String =
FormsAuthentication.HashPasswordForStoringInConfigFile(salt & randomCode,"SHA1")

        If dropDownList1.SelectedItem.Value = "1 Hour" Then
           passCode = randomCode & hashResult.SubString(4, 2)
           passCode = passCode & hashResult.SubString(0, 2)
           passCode = passCode & hashResult.SubString(8, 2)
           genCodes.Add(passCode)
        Else
           passCode = randomCode & hashResult.SubString(7, 2)
           passCode = passCode & hashResult.SubString(5, 2)
           passCode = passCode & hashResult.SubString(2, 2)
           genCodes.Add(passCode)
        End If

     Next

     btnExport.Visible = True
     heading.Text = "Your " & codeCount.Text & " <b>" &
dropDownList1.SelectedItem.Value & "</b> Passcodes:"
     genOutput.DataSource = genCodes
     genOutput.DataBind()
     codeCount.Text=""

     'Store the genCodes array in session state for retrieval for printing and
exporting
     Session("myGenCodes") = genCodes
     Session("codeType") = dropDownList1.SelectedItem.Value

  End Sub

  Sub printIt(Src As Object, e As DataListCommandEventArgs)
     If not Session.Item("myGenCodes") is Nothing Then
        genCodes=Session.Item("myGenCodes")
        codeType=Session.Item("codeType")
```

```
        'response.write(CStr(genCodes.Item(e.Item.ItemIndex)))

        'Popup hack using Javascript so that individual entries can be printed from
the DataList
        Dim sb As New System.Text.StringBuilder()
        sb.Append("<script language='javascript'>")
        sb.Append("window.open('print.aspx?genCode=")
        sb.Append(Server.URLEncode(CStr(genCodes.Item(e.Item.ItemIndex))))
        sb.Append("&sessLife=")
        sb.Append(Server.URLEncode(codeType))
        sb.Append("','printCode','toolbar=no,")
        sb.Append("addressbar=no,menubar=no,")
        sb.Append("width=400,height=250');")
        sb.Append("<")
        sb.Append("/")
        sb.Append("script>")
        RegisterStartupScript("stp", sb.ToString)
      End If

   End Sub

   Sub exporter(Sender As Object, E As EventArgs)

   If not Session.Item("myGenCodes") is Nothing Then
      genCodes=Session.Item("myGenCodes")

      'Convert the genCodes array to a string with CRs for later conversion to a byte
array
      Dim i as Integer
      Dim genCodeString as String
      for i = 0 To genCodes.Count - 1
         genCodeString += CStr(genCodes.Item(i)) & Chr(13)
      Next

      'response.write(genCodeString)

      'Create the byte array and send it to the browser as genCodes.csv
      Dim data() As Byte = System.Text.ASCIIEncoding.ASCII.GetBytes(genCodeString)
      Response.Clear()
      Response.AddHeader("Content-Type", "application/Excel")
      Response.AddHeader("Content-Disposition", "inline;filename=genCodes.csv")
      Response.BinaryWrite(data)
      Response.End()
   End If

End Sub

</script>

<STYLE>
body {
  font-size: 10pt;
  font-family: verdana,helvetica,arial,sans-serif;
  color:#000000;
  background-color:#9CBACE;
}

tr.heading {
  background-color:#006699;
}
```

```
.button {
   border: 1px solid #000000;
   background-color: #ffffff;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Random Script</TITLE>
</HEAD>

<BODY>
<form id="frmValidator" runat="server">

<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
   <tr class="heading">
      <td width="50%" valign="center"><font color="white"><b>Algorithmic
Authentication</b></font></td>
      <td><center><img width="216" height="51" src="<%= logo %>"></center></td>
      <td width="50%" align="right" valign="center"><font color="white"><b>Passcode
Generator</b> </font></td>
   </tr>
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>

<table width="90%" border="0" cellpadding="2" cellspacing="0">
   <tr>
      <td><b>Welcome to SonicWall's LHM Algorithmic Generator.</b><br><br>This will
allow you to create randomly generated passcodes for secure guest Internet
access.<br><br>Valid passcodes are not stored anywhere, so validation is not
performed against any kind of database.Instead, when a passcode is entered, it is
algorithmically validated.Once a passcode is successfully used, it is written to a
"used passcode" database so that it cannot be reused.<br><br>The validator will
recognize 1 hour and 24 hour passcodes - these characteristics were encoded within
the passcodes themselves during generation.<br><br>
      </td>
   </tr>
</table>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr><br>
      <td width="15%">Passcode type:</td>
      <td width="10%"><asp:DropDownList id="DropDownList1" runat="server">
          <asp:ListItem>1 Hour</asp:ListItem>
          <asp:ListItem>24 Hours</asp:ListItem>
       </asp:DropDownList></td>
      <td width="20%">Number to generate:</td>
      <td width="20%"><asp:TextBox id="codeCount" runat="server" /></td>
      <td width="50%"><asp:RequiredFieldValidator id="valcodeCount"
ControlToValidate="codeCount" ErrorMessage="Enter a value."Font-Size="10"
Display="Dynamic"  runat="server" />
```

```
      <asp:RangeValidator id="Range1" ControlToValidate="codeCount" MinimumValue="1"
MaximumValue="999" Type="Integer" Font-Size="10" ErrorMessage="Values from 1 to
999." runat="server" /></td>
   </tr>
   <tr>
      <td colspan=3></td>
      <td><asp:button id="btnSubmit" class="button" text=" Submit "
onClick="btnSubmit_Click" runat="server" />  <asp:button id="btnExport"
class="button" text=" Export " CausesValidation="False" onClick="exporter"
runat="server" /><br></td>
      <td><br></td>

   </tr>
   <tr><tr class="heading">
      <td colspan=5><font color="white"><asp:Label id=heading runat="server" /></td>
   </tr>
   <tr><td><br></td></tr>
</table>

<asp:DataList id="genOutput" Runat="Server" RepeatColumns="4"
RepeatDirection="Horizontal" CellPadding="0" Cellspacing="0" GridLines="Both"
align="center" OnItemCommand="printIt">
  <ItemTemplate>
   <td>
   <asp:Label Text='<%# Container.DataItem %>' Runat="Server"/>
   </td>
   <td>
   <asp:ImageButton id="print" runat="server" ImageUrl="print.gif"
EnableViewState="False" CausesValidation="False" CommandName='<%#
Container.DataItem %>' />
   </td>
  </ItemTemplate>
</asp:DataList>

</form>
</BODY>
</HTML>
```

logout.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWall authorizing the LHM session.
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
```

```
      As Boolean Implements ICertificatePolicy.CheckValidationResult
      Return True
   End Function
End Class

Dim sessionId as String
Dim mgmtBaseUrl as String
Dim eventId as String = "&eventId=1"

'Grab the code and the session lifetime from the generator page
Sub Page_Load(src as Object, e as EventArgs)
   sessionId=Request.QueryString("sessId")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
   sessTimer=Request.QueryString("sessTimer")


   'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWall
   'This is necessary for the POST to the SonicWall authorizing the LHM session.
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   'When the page loads, make the loggedIn span visible
   loggedIn.Visible=True
   loggedOut.Visible=False

   Me.Button1.Attributes.Add("OnClick", "self.close()")

End Sub

'The Logout button
Sub btnSubmit_Click(Sender As Object, E As EventArgs)

   'Let the user know that we are setting up the session, just in case it takes more
than a second
   LHMResult.Text = "Authorizing session.Please wait."

   'The LHM cgi on the SonicWall - this does not change
   Dim loginCgi as String = "externalGuestLogoff.cgi"

   'Assemble the data to post back to the SonicWall to authorize the LHM session
   Dim loginParams as String = "sessId=" & sessionId & eventId

   'Combine mgmtBaseUrl from the original redirect with the login cgi
   Dim postToSNWL as String = mgmtBaseUrl & loginCgi

   'Convert the loginParams to a well behaved byte array
   Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

   Try
      'Make the loggedOut span visible
      loggedIn.Visible=False
      loggedOut.Visible=True

      'Create the webrequest to the SonicWall
      Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

      'Calculate the length of the byte array
      toSNWL.ContentLength = byteArray.Length

      'Set the method for the webrequest to POST
      toSNWL.Method = "POST"
```

```
      'Set the content type
      toSNWL.ContentType = "application/x-www-form-urlencoded"

      'Open the request stream
      Dim dataStream As Stream = toSNWL.GetRequestStream()

      'Write the byte array to the request stream
      dataStream.Write(byteArray, 0, byteArray.Length)

      'Close the Stream object
      dataStream.Close()

      'Get the response
      Dim snwlReply As WebResponse = toSNWL.GetResponse()

      'Display the status - looking for 200 = OK.
      'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

      'Grab the response and stuff it into an xml doc for possible review
      Dim snwlResponse as XmlDocument = New XmlDocument()
      snwlResponse.Load(snwlReply.GetResponseStream())

      'Set the xPath to the SNWL reply, and get the response
      Dim codePath as String =
"SonicWallAccessGatewayParam/LogoffReply/ResponseCode"

      'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

      'Response code 150 - Logout Succeeded
      If snwlResponse.SelectSingleNode(codePath).InnerXml = "150"
        LHMResult.Text = "<br><b><font color=""green"">Your session has been logged
out.<br><br>Thank you for using LHM Guest Services.</font></b>"

      'Response code 251 - Bad HMAC.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed message authentication.Sorry for the
inconvenience.Please close and relaunch your browser to try again."

      'Response code 253 - Invalid SessionID.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed to match a known session identity.Sorry for
the inconvenience.Please close and relaunch your browser to try again."

      'Response code 254 - Invalid CGI.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request was missing an essential parameter.Sorry for the
inconvenience.Please close and relaunch your browser to try again."

      'Response code 255 - Internal Error.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error.Sorry for the
inconvenience.Please close and relaunch your browser to try again."

      End If

      'Close the streams
```

```
      dataStream.Close()
      snwlReply.Close()

      'If there is some asp.net error trying to talk to the SonicWall, print it in
the same color as the background.
      Catch ex as Exception
         catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
         LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error.Sorry for the
inconvenience.Please close and relaunch your browser to try again.If the problem
persists, please notify an attendant."
      End Try
End Sub

</script>
<STYLE>
body {
   font-size: 10pt;
   font-family: verdana,helvetica,arial,sans-serif;
   color:#000000;
   background-color:#9CBACE;
}

tr.heading {
   font-size: 10pt;
   background-color:#006699;
}

tr.smalltext {
   font-size: 8pt;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
   font-size: 8pt;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Logout Page</TITLE>

<SCRIPT LANGUAGE="Javascript">

//'Javascript Seconds Countdown Timer
var SecondsToCountDown = <%= sessTimer%>;
var originalTime=" ";

function CountDown()
{
   clockStr="";

   dayStr=Math.floor(SecondsToCountDown/86400)%100000
   if(dayStr>0){
      if(dayStr>1){
         dayStr+=" days ";
      } else dayStr+=" day ";
      clockStr=dayStr;
   }
   hourStr=Math.floor(SecondsToCountDown/3600)%24
```

```
   if(hourStr>0){
      if(hourStr>1){
         hourStr+=" hours ";
      } else hourStr+=" hour ";
      clockStr+=hourStr;
   }
   minuteStr=Math.floor(SecondsToCountDown/60)%60
   if(minuteStr>0){
      if(minuteStr>1){
         minuteStr+=" minutes ";
      } else minuteStr+=" minute ";
      clockStr+=minuteStr;
   }
   secondStr=Math.floor(SecondsToCountDown/1)%60
   if(secondStr>0){
      if(secondStr>1){
         secondStr+=" seconds ";
      } else secondStr+=" second ";
      clockStr+=secondStr;
   }

   if(SecondsToCountDown > 0)
   {
      --SecondsToCountDown;
   }

   if(originalTime.length < 2)
   {
      originalTime = clockStr;
   }

   // Make sure the form is still there before trying to set a value
   if(document.frmValidator){
      document.frmValidator.originalTime.value = originalTime;
      document.frmValidator.countdown.value = clockStr;
   }

   setTimeout("CountDown()", 1000);
   if(SecondsToCountDown == 0)
   {
      document.frmValidator.countdown.value = "Session Expired";
   }
}

//'Disable right-click so that the window doesn't get refreshed since the countdown
is clientside.
document.oncontextmenu = disableRightClick;
function disableRightClick()
{
  return false;
}

//'Disable F5 key, too, on IE at least.
function noF5()
{
   var key_f5 = 116;
   if (key_f5==event.keyCode)
   {
      event.keyCode=0;
      return false;
   }
```

```
   return false;
}

document.onkeydown=noF5
document.onmousedown=disableRightClick

</SCRIPT>

</HEAD>

<BODY onload='CountDown()'>
<span id="loggedIn" runat="server">
<form id="frmValidator" runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"><font color="white"><b>SonicWall LHM Logout
Window</b></font></td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="smalltext"><td><br></td></tr>
   <tr class="smalltext">
      <td>Original Session Time:</td>
      <td><asp:textbox width=250 id="originalTime" runat="server" /></td>
   </tr>
   <tr class="smalltext">
      <td>Remaining Session Time:</td>
      <td><asp:textbox width=250 id="countdown" runat="server" /></td>
   </tr>
   <tr class="smalltext">
      <td colspan=2><br>You may use this window to manually logout your session at
any time, or you may safely close this window if you prefer to let your session
timeout automatically.</font></td>
   </td>
   <tr>
      <td colspan=2><center><asp:button id="btnSubmit" class="button" text="  Logout
" onClick="btnSubmit_Click" runat="server" /></center></td>
   </tr>
</table>
</form>
</span>

<span id="loggedOut" runat="server">
<form id="logout" runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"><font color="white"><b>SonicWall LHM Logout
Window</b></font></td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr>
      <td><asp:Label id=LHMResult runat="server" /></td>
```

```
   </tr>
   <tr>
      <td><asp:Label id=catchError runat="server" /></td>
   </tr>
   <tr><td><br></td></tr>
   <tr>
      <td><center><asp:button id="Button1" class="button" text="  Close  "
runat="server" /></center></td>
   </tr>
</table>
</form>
</span>

</BODY>
</HTML>
```

myvars.aspx

```
<script language="VB" runat="server">

'Set the logoutPopup window flag - 0 = no popup, 1 = popup
'The use of the logoutPopup in this script is discouraged because the login event is
exclusive.
'The login event can be made non exclusive in this script by setting useDB to 0.
Dim logoutPopup as String = "0"

'Set the use of the database for storing and checking used passcodes.0 = do not use
DB, 1 = use DB.
Dim useDB as String = "1"

'The number of characters in the randomCode
Dim randChars as Integer = 6

'Set the salt the generation of the SHA1 hash
Dim salt as String = "moosifer"

'The LHM Session Timeout is set by the passcode in this script
Dim sessTimer as String

'Set the LHM Idle Timeout
Dim idleTimer as String = "300"

'Set the secret for use with optional HMAC auth, as configured in the Extern Guest
Auth config on the SonicWall
Dim strHmac as String = "password"

'Set the digest method for the HMAC, either MD5 or SHA1
Dim hmacType as String = "MD5"
'Dim hmacType as String = "SHA1"

'Set the logo image to use
Dim logo as String = "SonicWall.gif"

'------------------------End of Configurable Settings-------------------------

</script>
```

print.aspx

```
<!-- #INCLUDE file="myvars.aspx" -->
```

```
<script language="VB" runat="server">

Dim genCode as String
Dim sessLife as String

'Grab the code and the session lifetime from the generator page
Sub Page_Load(src as Object, e as EventArgs)
   genCode=Request.QueryString("genCode")
   sessLife=Request.QueryString("sessLife")
End Sub

</script>
<STYLE>
body {
  font-size: 10pt;
  font-family: verdana,helvetica,arial,sans-serif;
  color:#000000;
  background-color:#9CBACE;
}
tr.heading {
  background-color:#006699;
}
</STYLE>
<BODY>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=2 align="center"><font color="white"> </td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"><img width="216" height="51" src="<%= logo
%>"></td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"><font color="white"> </td>
   </tr>
   <tr><td><br><br></td></tr>
   <tr>
      <td>Your Pass Code is:</td>
      <td><b><%= genCode%></b></td>
   </tr>
   <tr><td><br></td></tr>
   <tr>
      <td>Session Lifetime is:</td>
      <td><b><%= sessLife%></b></td>
   </tr>
</table>

<script language='javascript'>window.print();</script>

</BODY>
</HTML>
```

Chooser.aspx Script

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
```

```
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<script language="VB" runat="server">

Dim ip as String
Dim sessionId as String
Dim mac as String
Dim ufi as String
Dim mgmtBaseUrl as String
Dim clientRedirectUrl as String
Dim req as String
Dim hmac as String
Dim customCode as String
Dim qString as String

Sub Page_Load(src as Object, e as EventArgs)

   'Grab the querystring one element at a time since we need to do a custom URL
encode on the req variable
   sessionId=Request.QueryString("sessionId")
   ip=Request.QueryString("ip")
   mac=Request.QueryString("mac")
   ufi=Request.QueryString("ufi")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
   clientRedirectUrl=Request.QueryString("clientRedirectUrl")
   req=Request.QueryString("req")
   hmac=Request.QueryString("hmac")
   customCode=Request.QueryString("cc")

   'SonicWall URL Encode routine is different from Microsoft - this is the SonicWall
method
   req=Replace(req,"%","%25")
   req=Replace(req,":","%3A")
   req=Replace(req," ","%20")
   req=Replace(req,"?","%3F")
   req=Replace(req,"+","%2B")
   req=Replace(req,"&","%26")
   req=Replace(req,"=","%3D")

   'Rebuild the querystring variable
   qString = "sessionId=" & sessionId & "&ip=" & ip & "&mac=" & mac & "&ufi=" & ufi &
"&mgmtBaseUrl=" & mgmtBaseUrl & "&clientRedirectUrl=" & clientRedirectUrl & "&req="
& req

   'Add the optional hmac and cc vars if they are there.
   If hmac <> "" Then
      qString+="&hmac=" & hmac
   End If

   If customCode <> "" Then
      qString+="&cc=" & customCode
   End If

   'Bind the directory data
   Dim lhmDir As New DirectoryInfo(Server.MapPath("."))
   lhmList.DataSource = lhmDir.GetDirectories
   lhmList.DataBind()
```

```
End Sub

</script>

<STYLE>
body {
  font-size: 10pt;
  font-family: verdana,helvetica,arial,sans-serif;
  color:#000000;
  background-color:#9CBACE;
}

tr.heading {
  background-color:#006699;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
}

tr.hidden {
   font-size: 5pt;
   color:#9CBACE;
}

</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Script Chooser</TITLE>
</HEAD>

<BODY>

<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
   <tr class="heading">
      <td width="50%" valign="center"><font color="white"><b>LHM Script
Chooser</b></font></td>
      <td><center><img width="216" height="51" src="SonicWall.gif"></center></td>
      <td width="50%" align="right" valign="center"><font
color="white"><b></b> </font></td>
   </tr>
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>

<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr><td><br></td></tr>
   <tr><td><H3>Please select one of the LHM Scripts below</H3></td></tr>
   <tr><td>Your original querystring information will be passed to the target script,
and it will open in a new window.</td></tr>
   <tr><td><br></td></tr>
</table>

<asp:Repeater id="lhmList" runat="server">
   <ItemTemplate >
```

```
        <li><a href = <%# DataBinder.Eval(Container.DataItem, "Name").ToString() &
"/default.aspx?"& qString & " target=""_blank""" %> >
        <%# DataBinder.Eval(Container.DataItem, "Name").ToString() %>
        </a>
        </li>
    </ItemTemplate>
 </asp:Repeater>

<table>
<tr class="hidden">
<td>default.aspx?sessionId=0b712fd83b9f5313db5af1cea6b1004f&ip=10.50.165.231&mac=00
:0e:35:bd:c9:37&ufi=0006b11184300&mgmtBaseUrl=https://10.50.165.193:4043/&clientRed
irectUrl=https://10.50.165.193:444/&req=http%3A//www.google.com/ig</td></tr>
</table>

</BODY>
</HTML>
```

B

IPv6

トピック:

- IPv6 (979 ページ)
  - IPv6 について (979 ページ)
  - IPv6 の設定 (985 ページ)
  - IPv6 可視化 (1011 ページ)
  - IPv6 高可用性監視 (1012 ページ)
  - IPv6 の診断と監視 (1013 ページ)

IPv6

この付録では、IPv6 の実装の概要と、IPv6 の動作、およびネットワークに合わせて IPv6 を設定する方法を説明します。

トピック:

- IPv6 について (979 ページ)
- IPv6 の設定 (985 ページ)
- IPv6 可視化 (1011 ページ)
- IPv6 高可用性監視 (1012 ページ)
- IPv6 の診断と監視 (1013 ページ)

IPv6 について

トピック:

- IPv6 Ready 認証 (980 ページ)
- IPv6 テクノロジーの概要 (980 ページ)
- IPv6 の利点 (982 ページ)
- SonicWall で現在サポートされている IPv6 サービスおよび機能 (983 ページ)
- SonicWall で現在サポートされていない IPv6 機能 (983 ページ)
- サポートされている IPv6 関連 RFC (983 ページ)
- サポートされていない IPv6 関連 RFC (985 ページ)

IPv6 Ready 認証

SonicWall は、IPv6 の配備に関する技術的なガイダンスを提供している世界的なコンソーシアムである IPv6 Forum によって指定されている "IPv6 Ready" の Phase-1 および Phase-2 の要件を満たしています。IPv6 Ready Logo プログラムは、現在 IPv6 が利用可能でいつでも使用できる状態にあることを示すことでユーザの信頼感を高めることを目的とした、適合性および相互運用性に関するテスト プログラムです。

IPv6 Ready の一連のテストは、基本的なレベルで最小の範囲を押さえた Phase-1 と、より網羅性の高い Phase-2 に分かれています。

- Phase-1 (シルバー) ロゴ: 最初の段階であるこのロゴは、製品に IPv6 の必須のコア プロトコルが含まれ、他の IPv6 実装との相互運用が可能なことを示します。
- Phase-2 (ゴールド) ロゴ: この "IPv6 Ready" の段階は、適切なケア、技術的なコンセンサス、および明確な技術的リファレンスの存在を意味します。この IPv6 Ready ロゴは、製品が IPv6 Logo Committee (v6LC) によって提示された厳しい要件を首尾よく満たしていることを示しています。

SonicWall は Phase-2 (ゴールド) の IPv6 Ready ステータスの認証を受けています。将来的な Phase-3 レベルの IPv6 Ready の範囲については、現在策定中です。

詳細については、http://www.ipv6ready.org/ を参照してください。

メモ：IPv6 用ウィザードは SonicOS ではサポートされません。

IPv6 テクノロジーの概要

インターネットに接続されるすべての機器 (コンピュータ、プリンタ、スマートフォン、スマート メーターなど) には IP アドレスが必要です。インターネット プロトコル バージョン 4 (IPv4) は、約 43 億個の一意な IP アドレスを提供します。インターネット、モバイル フォン、および VoIP テレフォニーの利用の急激かつ世界的な拡大により、この 43 億個の IP アドレスはまもなく枯渇してしまいます。

2011 年 2 月 3 日、IANA (Internet Assigned Numbers Authority) は最後まで残っていた IPv4 アドレスのブロック群を地域インターネット レジストリ (RIR) に分配しました。今年の後半、各 RIR がこれらのアドレスを ISP に割り振ってしまうと、全世界で新しい IPv4 アドレスの供給ができなくなります。

幸い、IETF (Internet Engineering Task Force) がこの日に備えた計画の立案を 1992 年頃に開始し、1998 年には インターネット プロトコル、バージョン 6 (IPv6) を定義する RFC 2460 が公開されました。アドレス長を 32 ビットから 128 ビットに増やすことで、IPv6 では使用可能なアドレス数が IPv4 よりも大幅に増加しています。

- IPv4: 4,294,967,296 アドレス
- IPv6: 340,282,366,920,938,463,463,374,607,431,768,211,456 アドレス

IPv6 アドレスについて

IPv6 アドレスは、次のように、コロンで区切られた 4 桁の 16 進数から成るグループ 8 つの並びで記述されます。

```
XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX
```

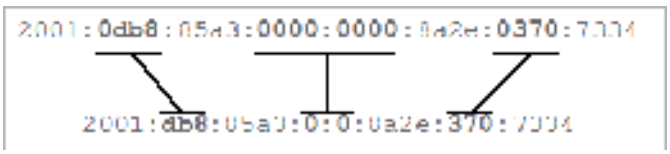
IPv6 アドレスは論理的には 2 つの部分に分かれています。64 ビットの (サブ) ネットワーク接頭辞と、同じく 64 ビットのインターフェース ID です。IPv6 アドレスの例を示します。

```
2001:0db8:85a3:0000:0000:8a2e:0370:7334
```

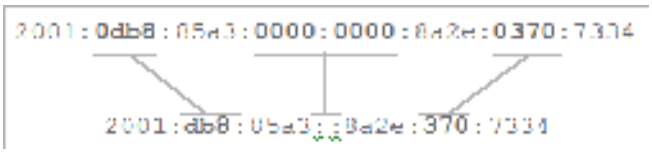
メモ：IPv6 アドレス中の 16 進数に大文字と小文字の区別はありません。

IPv6 アドレスの表記は、次の 2 つのルールを使用して簡略化できます。

1 16 ビット値内の先頭にある 0 の並びは省略できます。そのため、先ほどの完全な表記の例は、次のような省略形にすることができます。



2 4 つの 0 から成るグループ (厳密には 16 ビット分の 0) が続く場合は、その数にかかわらず連続する 2 つのコロン (::) で表現できます。これら 2 つのルールを組み合わせると、例に挙げたアドレスの完全な表記は、次のように省略できます。



ヒント：ダブル コロン (::) は空のアドレス 0:0:0:0:0:0:0:0 の省略形です。

IPv6 アドレスの種別

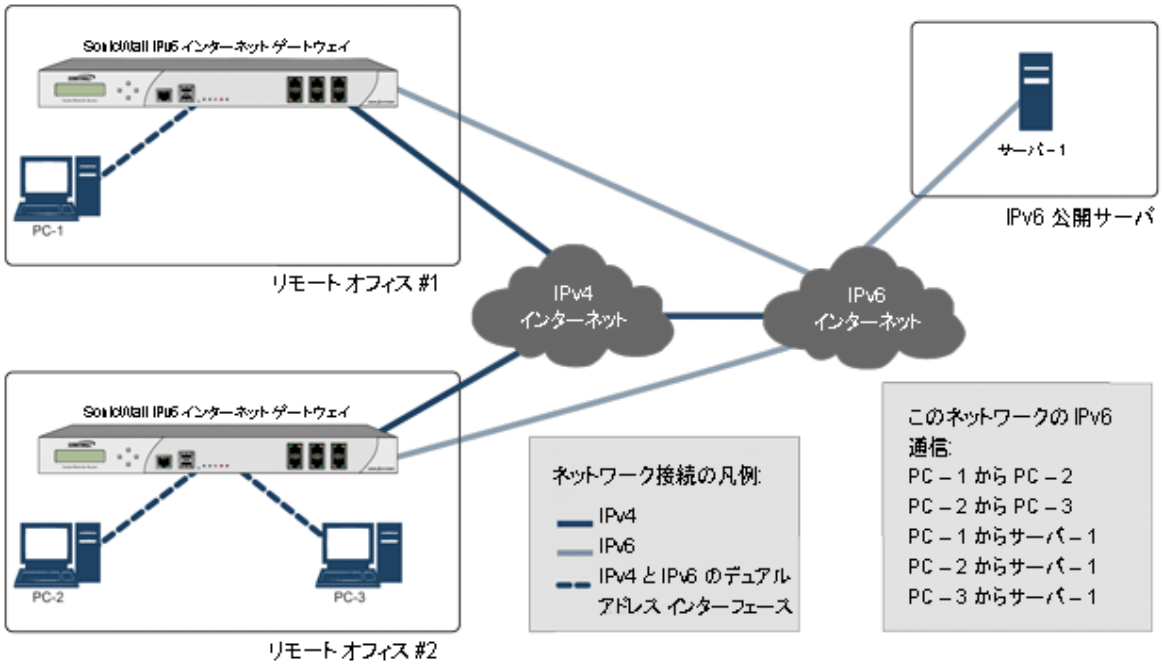
アドレスの種別	完全なアドレス	簡略化されたアドレス
ユニキャスト アドレス	1080:0:0:0:8:800:200C:417A	1080::8:800:200C:417A
マルチキャスト アドレス	FF01:0:0:0:0:0:0:101	FF01::101
ループバック アドレス	0:0:0:0:0:0:0:1	::1
未指定アドレス	0:0:0:0:0:0:0:0	::

メモ：IPv6 インターネットに接続するためには、ネットワークに IPv4 のインターネット接続が必要です。

メモ：ローカル ネットワーク サイトのコンピュータでは、IPv6 スタックが有効になっている必要があります。

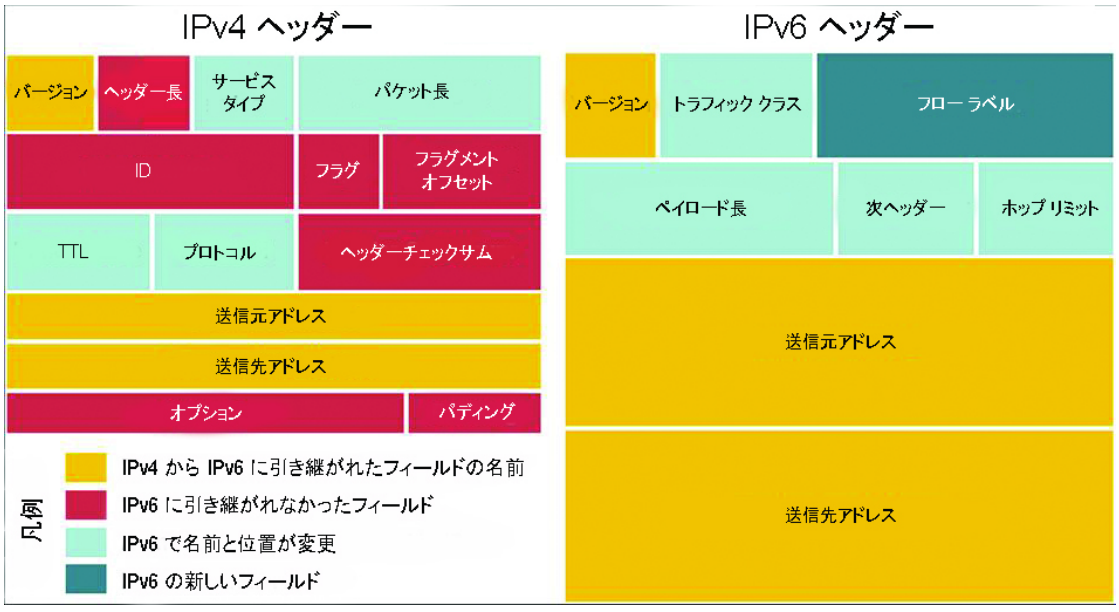
「一般的な IPv6 配備」に、一般的な IPv6 配備の接続モデルの簡略図を示します。

一般的な IPv6 配備



「IPv4 と IPv6 のヘッダー要素の比較」は、IPv4 と IPv6 のヘッダー要素を比較したものです。

IPv4 と IPv6 のヘッダー要素の比較



IPv6 の利点

IPv6 には、IPv4 による制限を緩和するための重要な機能がいくつかあります。この新しい IP 規格は、いくつかの重要な点で IPv4 を拡張しています。

- 6to4 トンネル (IPv6 ノードが IPv4 ネットワークを介して外部の IPv6 サービスに接続できるようにします)

    - 6to4 自動トンネル
    - GRE トンネル
- IPv6 手動トンネル
- 簡素化された新しい IPv6 ヘッダー形式
- 膨大な数の IPv6 アドレスが利用可能
- 効率的かつ階層的なアドレス指定およびルーティング インフラストラクチャ
- 近隣者発見プロトコル (NDP) および DHCPv6 を使用した、ホストおよびルータへの自動アドレス割り当て
- ステートレスなアドレス設定とステートフルなアドレス設定
- ビルトイン セキュリティ - AH および ESP (強く推奨)
- QoS のより適切なサポート - ヘッダー内のフロー ラベル
- 近隣ノードとの対話のための新しいプロトコル
- 拡張ヘッダーを使用した新しい機能に対応できる拡張性
    - 拡張ヘッダー検出レポートおよびログのサポート
    - 拡張ヘッダー順序確認の強制
    - ホップバイホップ拡張ヘッダーのサポート
    - インバウンドの種別 0 ルーティング ヘッダー パケットの確認

SonicWall で現在サポートされている IPv6 サービスおよび機能

現在サポートされている IPv6 サービスおよび機能の完全なリストについては、ナレッジ ベース記事『*Supported/Unsupported IPv6 Features in SonicOS 6.2.x firmware (SonicOS 6.x.x ファームウェアのサポート対象/対象外の IPv6 機能)*』を参照してください。

SonicWall で現在サポートされていない IPv6 機能

メモ：SonicOS はデュアル IP スタックのファームウェアです。IPv6 でサポートされていない機能であっても IPv4 でサポートされているものがあります。

現在サポートされていない IPv6 サービスおよび機能の完全なリストについては、ナレッジ ベース記事『*Supported/Unsupported IPv6 Features in SonicOS 6.2.x firmware (SonicOS 6.x.x ファームウェアのサポート対象/対象外の IPv6 機能)*』を参照してください。

サポートされている IPv6 関連 RFC

このセクションでは、SonicOS でサポートされている IPv6 関連の RFC の一覧を示します。

- TCP/IP スタックおよびネットワーク プロトコル (984 ページ)
- IPsec 適合 (985 ページ)
- NAT 適合 (985 ページ)
- DNS 適合 (985 ページ)

TCP/IP スタックおよびネットワーク プロトコル

- RFC 1886『IP バージョン 6 をサポートするための DNS 拡張』『IPAPPL DNS クライアント』
- RFC 1981『Path MTU Discovery for IPv6 (IP バージョン 6のためのパス MTU 発見)』
- RFC 2113『IP Router Alert Option (IP ルータ アラート オプション)』
- RFC 2373『IPv6 Addressing Architecture (IPv6 のアドレス指定手法)』
- RFC 2374『An IPv6 Aggregatable Global Unicast Address Format (IPv6 の統合可能グローバル ユニキャスト アドレス形式)』(3587 により廃止)
- RFC 2375『IPv6 Multicast Address Assignments (IPv6 マルチキャスト アドレスの割り当て)』
- RFC 2460『IPv6 specification (IPv6 仕様)』
- RFC 2461『Neighbor discovery for IPv6 (IPv6 の近隣者発見)』
- RFC 2462『IPv6 Stateless Address Autoconfiguration (IPv6 のステートレス アドレス自動設定)』
- RFC 2463『ICMPv6 for IPv6 specification (IPv6 仕様向け ICMPv6)』
- RFC 2464『Transmission of IPv6 Packets over Ethernet Networks (イーサネット ネットワーク上での IPv6 パケットの送信)』
- RFC 2473『Generic Packet Tunneling in IPv6 Specification (IPv6 仕様における汎用パケット トンネル)』
- RFC 2474『Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers (IPv4 および IPv6 ヘッダー内の Differentiated Services フィールド (DS フィールド) の定義)』
- RFC 2545『Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing (IPv6 のドメイン間ルーティングでの BGP-4 マルチプロトコル拡張の使用方法)』
- RFC 2553『Basic Socket Interface Extensions for IPv6 (IPv6 向けの基本的なソケット インターフェース拡張)』
- RFC 2710『Multicast Listener Discovery (MLD) for IPv6 (IPv6 でのマルチキャスト リスナー発見 (MLD))』
- RFC 2711『IPv6 Router Alert Option (IPv6 のルータ アラート オプション)』
- RFC 2784『Generic Routing Encapsulation (汎用的なルーティング カプセル化)』
- RFC 2893『Transition Mechanisms for IPv6 Hosts and Routers (IPv6 ホストおよびルータの移行メカニズム)』
- RFC 2991『Multipath Issues in Unicast and Multicast Next-Hop Selection (マルチキャスト ネクストホップ選択でのマルチパス問題)』
- RFC 3056『Connection of IPv6 Domains via IPv4 Clouds (IPv4 クラウドを介した IPv6 ドメインの接続)』
- RFC 3484『Default Address Selection for Internet Protocol version 6 (IPv6) (インターネット プロトコル バージョン 6 (IPv6) の既定のアドレス選択)』 (ポリシー フックなし)
- RFC 3493『Basic Socket Interface Extensions for IPv6 (IPv6 向けの基本的なソケット インターフェース拡張)』
- RFC 3513『Internet Protocol Version 6 (IPv6) Addressing Architecture (インターネット プロトコル バージョン 6 (IPv6) のアドレス指定手法)』
- RFC 3542『Advanced Sockets Application Program Interface (API) for IPv6 (IPv6 向けの高度なソケット アプリケーション プログラム インターフェース (API))』
- RFC 3587『IPv6 Global Unicast Address Format (IPv6 のグローバル ユニキャスト アドレス形式)』 (これにより 2374 は廃止)

IPsec 適合

- RFC 1826『IP Authentication Header (IP 認証ヘッダー)』 [旧 AH]
- RFC 1827『IP Encapsulating Security Payload (ESP) (セキュリティ ペイロードの IP カプセル化)』 [旧 ESP]

NAT 適合

- RFC 2663『IP Network Address Translator (NAT) Terminology and Considerations (IP ネットワーク アドレス変換 (NAT) に関する用語と考慮事項)』
- RFC 3022『Traditional IP Network Address Translator (Traditional NAT) (従来の IP ネットワーク アドレス変換 (従来の NAT))』

DNS 適合

- RFC 1886『DNS Extensions to support IP version 6 (IP バージョン 6 をサポートするための DNS 拡張)』

サポートされていない IPv6 関連 RFC

このセクションでは、SonicOS でサポートされていない IPv6 関連の RFC の一覧を示します。

- RFC 2002『IP Mobility Support (IP モビリティ サポート)』
- RFC 2766『Network Address Translation - Protocol Translation (NAT-PT) (ネットワーク アドレス変換 - プロトコル変換 (NAT-PT))』
- RFC 2472『IP Version 6 over PPP (PPP 上の IP バージョン 6)』
- RFC 2452『IP Version 6 Management Information Base for the Transmission Control Protocol (伝送制御プロトコル向けの IP バージョン 6 管理情報ベース)』
- RFC 2454『IP Version 6 Management Information Base for the User Datagram Protocol (ユーザ データグラム プロトコル向けの IP バージョン 6 管理情報ベース)』
- RFC 2465『Management Information Base for IP Version 6: Textual Conventions and General Group (IP バージョン 6 向けの管理情報ベース: テキスト化規則と一般グループ)』

IPv6 の設定

トピック:

- IPv6 インターフェースの設定 (986 ページ)
- IPv6 トンネル インターフェースの設定 (997 ページ)
- IPv6 を使用した SonicWall 管理インターフェースへのアクセス (1008 ページ)
- IPv6 ネットワークの設定 (1008 ページ)
- IPv6 アクセス ルールの設定 (1010 ページ)
- IPv6 の詳細なファイアウォール設定 (1010 ページ)
- IPv6 IPSec VPN の設定 (1010 ページ)
- IPv6 の SSL VPN 設定 (1011 ページ)

IPv6 インターフェースの設定

IPv6 インターフェースを設定するには、「**管理 | システム セットアップ | ネットワーク > インターフェース**」ページで「**インターフェース設定**」テーブルの右上隅にある「**表示する IP バージョン**」で「**IPv6**」を選択します。

既定では、すべての IPv6 インターフェースは IP アドレスなしでルートされるように現れます。1 つのインターフェースに複数の IPv6 アドレスを追加することができます。自動 IP 割り当ては WAN インターフェースに対してのみ設定できます。

メモ：PortShield インターフェースは IPv6 ではサポートされません。

それぞれのインターフェースはルータ広告を受信する、または、受信しないように設定できます。それぞれのインターフェース上で IPv6 を有効または無効に設定できます。

メモ：インターフェースへのゾーン割り当ては、IPv6 モードに切り替える前に IPv4 インターフェースのページ上で設定する必要があります。

トピック:

- IPv6 インターフェース設定の制約 (986 ページ)
- インターフェースを IPv6 静的モードで設定する (987 ページ)
- IPv6 詳細オプションと複数 IPv6 アドレスを設定する (988 ページ)
- ルータ広告の設定 (989 ページ)
- ルータ広告接頭辞の設定 (990 ページ)
- インターフェースを DHCPv6 モードに設定する (991 ページ)
- IPv6 インターフェースに対する詳細設定 (993 ページ)
- DHCPv6 プロトコル情報の表示 (994 ページ)
- インターフェースを自動モードに設定する (995 ページ)
- PPPoE (996 ページ)
- VLAN サブインターフェースを設定する (997 ページ)
- ワイヤ モードでのインターフェースの設定 (997 ページ)

IPv6 インターフェース設定の制約

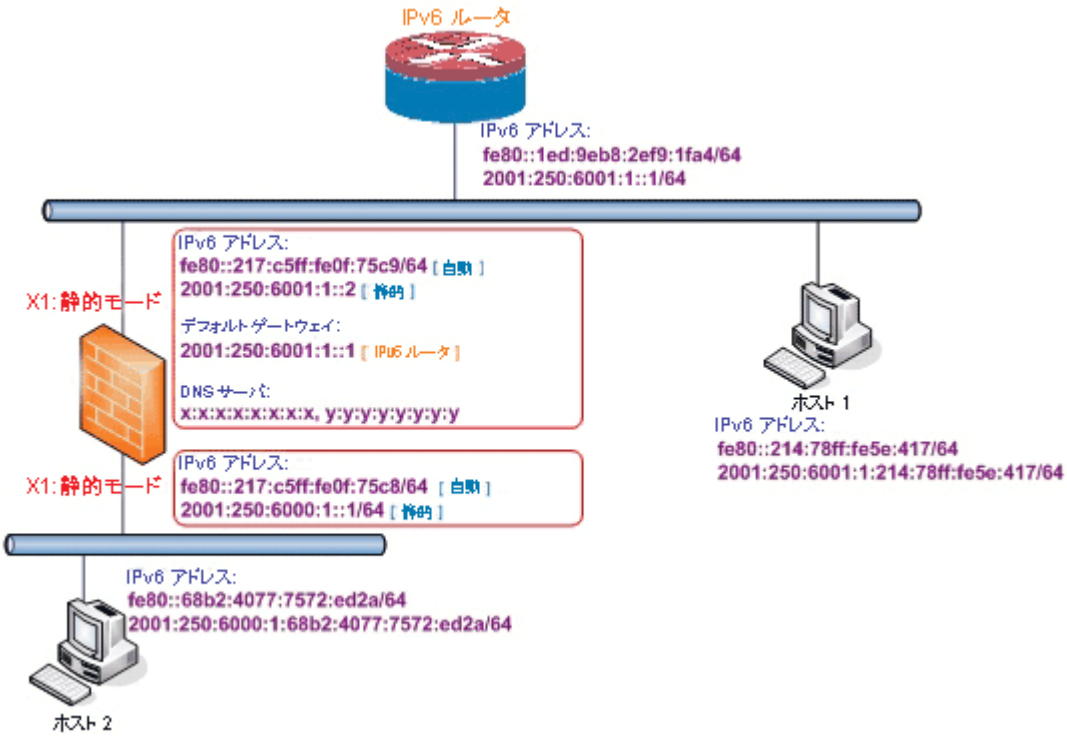
- HA インターフェースは IPv6 用に設定できません。
- スイッチ ポート グループでは親インターフェースのみ IPv6 インターフェースとして設定可能なため、スイッチ ポート グループのすべての子供はこのリストから除外する必要があります。
- ゾーンおよびレイヤ 2 ブリッジ グループは、インターフェースの IPv4 と IPv6 で設定が共有されます。それらが IPv4 側で設定されると、同一インターフェースの IPv6 側でも同じ設定が使用されます。
- デフォルト ゲートウェイと DNS サーバは WAN ゾーン インターフェースにのみ設定可能です。
- IPv6 でワイヤ モードはサポートされていますが、設定の変更は一切できません。その代わり、IPv4 で設定した設定オプションがそのまま引き継がれます。

インターフェースを IPv6 静的モードで設定する

静的モードは、自動割当アドレスとは対照的に、静的 IPv6 アドレスを割り当てる方法を提供します。静的モードを使用してもなお、IPv6 インターフェースはルータ広告を受け取り、自律アドレスを適切な接頭辞オプションから習得することが可能です。静的モードは IPv6 インターフェース上のステートレス アドレス自動設定の動作を、ユーザが手動で無効にしない限り妨害しません。

「IPv6 静的モードの設定」に、静的モードで設定された IPv6 のサンプル トポロジを示します。

IPv6 静的モードの設定



このモード下では、3 種類の IPv6 アドレスを割り当てることが可能です。

- 自動アドレス
- 自律アドレス
- 静的アドレス

インターフェースを静的 IPv6 アドレス用に設定するには、以下の手順に従います。

1 「**管理 | システム セットアップ | ネットワーク > インターフェース**」ページに移動します。

2 ページの右上隅にある「**IPv6**」を選択します。装置の IPv6 アドレスが表示されます。

3 IPv6 アドレスを設定したいインターフェースの「**設定**」を選択します。「**インターフェースの編集**」ダイアログが表示されます。

> **メモ**：インターフェースへのゾーン割り当ては IPv4 アドレス設定ページで設定する必要があります。IPv6 インターフェースに対するゾーン割り当てを編集するには、ページ右上にある「**IPv4**」を選択して、インターフェースのゾーンを編集してから、IPv6 インターフェースのページに戻ります。

4 「**ネットワーク モード**」ドロップダウン メニューで「**静的**」を選択します。

5 インターフェースの **IPv6 アドレス**を入力します。

6 アドレスの**接頭辞長**を入力します。

7 プライマリ WAN インターフェースの場合、「**デフォルト ゲートウェイ**」の IPv6 アドレスを入力します。プライマリ WAN インターフェースでない場合は、デフォルト ゲートウェイの登録はすべて無視されるので、「::」のままにしておいて構いません(ダブル コロンは空のアドレス 0:0:0:0:0:0:0:0 の省略形です)。

8 プライマリ WAN インターフェースの場合は、**DNS サーバ**の IPv6 アドレスを最大 3 つ入力します。この場合もまた、プライマリ WAN インターフェースではない場合は、すべての DNS サーバの登録が無視されます。

9 インターフェースをネットワークと接頭辞情報を配布する通知インターフェースにするには、「**ルータ広告を有効にする**」を選択します。

10 インターフェース通知接頭辞リスト内に既定の接頭辞を追加するには、「**IPv6 プライマリ静的アドレスのサブネット接頭辞を広告する**」を選択します。この接頭辞はインターフェースの IPv6 プライマリ静的アドレスのサブネット接頭辞です。このオプションは同じサブネット内につながっている、すべてのホストに役立ちます。

IPv6 詳細オプションと複数 IPv6 アドレスを設定する

IPv6 インターフェースの詳細オプションを編集する、または複数の静的 IPv6 アドレスを設定するには、以下の手順に従います。

1 「**インターフェースの編集**」ダイアログで、「**詳細**」タブを選択します。

2 インターフェースに対して複数の静的 IPv6 アドレスを設定するには、「**アドレスの追加**」を選択します。「**インターフェース IPv6 アドレスの追加**」ダイアログが表示されます。

> ⓘ **メモ**：複数の IPv6 アドレスは、静的 IPv6 アドレス モードで設定されているインターフェースに対してのみ追加可能です。**自動**または **DHCPv6** モードに対しては、複数の IPv6 アドレスを設定できません。

3 インターフェースの追加アドレスとなる **IPv6 アドレス**を入力します。

4 アドレスの**接頭辞長**を入力します。

5 インターフェース通知接頭辞リスト内に既定の接頭辞を追加するには、「**IPv6 アドレスのサブネット接頭辞を広告する**」を選択します。この接頭辞はインターフェースの IPv6 プライマリ静的アドレスのサブネット接頭辞です。このオプションは同じサブネット内につながっている、すべてのホストに役立ちます。

6 「**OK**」を選択します。

7 「**詳細**」タブの「**詳細設定**」という見出しの下で、以下の追加オプションを設定できます。

- インターフェースにすべての IPv6 トラフィックの処理を停止させるには、「**インターフェース上のすべての IPv6 トラフィックを無効にする**」を選択します。IPv6 トラフィックを無効にすると、非 IPv6 トラフィックに対するファイアウォールのパフォーマンスを向上させることができます。このオプションは、既定では選択されていません。

  > ⓘ **ヒント**：ファイアウォールが純粋な IPv4 環境に配備されている場合、SonicWall ではこのオプションを有効にすることを推奨しています。

- ファイアウォールがルータ広告を受信するようにするには、「**ルータ広告を受信する**」を選択します。無効にした場合、インターフェースはすべての着信ルータ広告メッセージを遮断するので、悪意のあるネットワーク パラメータ (例えば接頭辞情報やデフォル

ト ゲートウェイ) 受信の可能性を排除することによるセキュリティ向上が可能です。このオプションは、既定では選択されています。

メモ：このオプションが無効になっている場合、割り当てられたすべての自律的 IPv6 アドレスがこのインターフェースから削除されます。

このオプションは**自動**モードでは表示されません。**自動**モードでは常に有効です。

- このインターフェースに自律的 IPv6 アドレスを割り当てることを許可するには、「**ステートレス アドレス自動設定を有効にする**」を選択します。非選択にした場合は、このインターフェースからすべての割り当てられた自律的 IPv6 アドレスが削除されます。

  このオプションは**自動**モードでは表示されません。**自動**モードでは常に有効です。

- インターフェースに仮アドレスが割り当てられる前の重複アドレス検知 (DAD) 実行時に送信される、連続した近隣者要請メッセージの数を指定するには、「**重複アドレス検知の送信**」にその数を入力します。最小値は 0、最大値は 9、既定値は **1** です。0 を指定すると、このインターフェースでは DAD は実行されません。
- 「**近隣者発見の基準到達可能時間 (秒)**」には、インターフェースのランダムな到達可能時間値の計算に使用する基準値を秒単位で入力します。最小値は 0、最大値は 9999、既定値は **30** です。

  値 0 は、このパラメータが指定されないことを示し、その場合は「**ネットワーク > 近隣者発見**」のグローバル設定が使用されます。ただし、RA がこのインターフェースで有効になっている場合は、「**ルータ広告**」タブの「**到達可能時間**」オプションの値が使用されます。
- インターフェース毎の最大 NDP サイズを有効にするには、「**インターフェース毎の最大 NDP サイズを有効にする**」を選択します。システム リソースが使い果たされるのを防ぐために、どのインターフェースにも最大 NDP サイズを設定してください。
  - 「インターフェース毎の最大 NDP サイズ」フィールドに最大 NDP サイズを入力します。最小値は 64、最大値は 9999、既定値は **128** (WAN インターフェースの場合) または **1200** (その他の場合) です。
- IPv6 ノードは、同一リンク上の重複 IPv6 アドレスを検出するために、IPv4 の重複回避用 ARP (Gratuitous ARP) に似た近隣者要請メッセージを使います。DAD はどのユニキャスト アドレス (エニーキャスト アドレスを除く) 上でも、IPv6 インターフェースに仮アドレスを割り当てる前に実行される必要があります。

ルータ広告の設定

ルータ広告により、IPv6 ルータが DNS リカーシブ サーバ アドレスを IPv6 ホストに通知可能になります。IPv6 ホストのアドレスが IPv6 ステートレス アドレス自動設定を通して自動設定され、かつサーバ アドレスを取得してそのサーバと通信する際の遅延が大きな問題になる環境のネットワーク内でルータ広告ベースの DNS 設定は有用で任意の代替になります。ルータ広告により、ホストはそれぞれのリンク上で最も近いサーバのアドレスを入手できます。加えて、リンクに対する設定情報を提供する同一の RA メッセージからこれらのアドレスを学習し、それにより追加のプロトコルの実行を回避します。これは Mobile IPv6 のような、いくつかのモバイル環境で有益になり得ます。SonicWall の IPv6 実装は、RFC 4861 の ルータおよび接頭辞発見に完全に適合しています。

メモ：ルータ広告は、インターフェースが静的モードの場合にのみ有効にできます。

IPv6 インターフェースに対してルータ広告を設定するには、以下の手順に従います。

1 「**インターフェースの編集**」ダイアログ ボックスで、「**ルータ広告**」タブを選択します。

2 「**ルータ広告を有効にする**」チェックボックスを選択して、これをネットワークと接頭辞情報を配信する通知側インターフェースにします。

3 オプションで、以下のルータ広告設定を編集できます。

- **ルータ広告間隔範囲 (秒)** - インターフェースから、要請されていないマルチキャスト ルータ広告の送信を許可する間隔の秒数です。広告が送信される間隔は、最小間隔から最大間隔までの範囲のランダムな値となります。
  - 最小間隔 - ルータ広告の送信で許容される最短の間隔を入力します。最小時間は 3 秒、最大時間は 1350 秒、既定の最小時間は **200** 秒です。
  - 最大間隔 - ルータ広告の送信で許容される最長の間隔を入力します。最小時間は 4 秒、最大時間は 1800 秒、既定の最大時間は **600** 秒です。
- **リンク MTU** - インターフェース リンクに対する推奨 MTU を入力します。最小値は 0、最大値は 99,999、既定値は **0** (ファイアウォールがそのリンクでリンク MTU を通知しないことを意味します) です。
- **到達可能時間 (秒)** - ノードが到達可能の確認を受信した後で、近隣者が到達可能であると見なす時間です。最小値は 0、最大値は 9,999,999,999、既定値は **0** (このパラメータがファイアウォールによって指定されないことを意味します) です。
- **再送信時間** - 近隣者要請メッセージを再送出する間隔を入力します。最小値は 0、最大値は 9,999,999,999、既定値は **0** (このパラメータがファイアウォールによって指定されないことを意味します) です。
- **現在のホップ制限** - 送信 IP パケットに対する IP ヘッダーのホップ カウント フィールドに設定される既定値を入力します。最小値は 0 であり、この値はファイアウォールによってこのパラメータが指定されないことを意味します。最大値は 255、既定値は **64** です。
- **ルータ存続期間 (秒)** - ファイアウォールを既定のルータとして受け入れるライフタイムを入力します。最小値は 0 秒であり、この値はルータが既定のルータでないことを意味します。最大時間は 9000 秒、既定値は **1800** 秒です。
- **ルータ優先度** - 通知側の既定ルータをその他の既定ルータよりも優先するかどうかを示します。「**高**」、「**中**」 (既定値)、または「**低**」をドロップダウン メニューから選択します。

4 ルータ広告メッセージ内に管理アドレス設定フラグを設定するには、「**管理**」チェックボックスを選択します。設定されている場合、このフラグは IPv6 アドレスが DHCP を通して利用可能であることを示します。

5 ルータ広告メッセージ内に他の設定フラグを設定するには、「**その他設定**」チェックボックスを選択します。設定されている場合、このフラグは他の設定情報が DHCP を通して利用可能であることを示します。

ルータ広告接頭辞の設定

通知用の接頭辞により、オンリンク決定とアドレス自動設定のための接頭辞がホストに提供されます。

ルータ広告接頭辞を設定するには、以下の手順に従います。

1 「**インターフェースの編集**」ダイアログの「**ルータ広告**」タブにある「**接頭辞リストの設定**」テーブルに移動します。

2 「**接頭辞の追加**」を選択します。「**通知用接頭辞の追加**」ダイアログが表示されます。

3 ルータ広告メッセージで通知される「**接頭辞**」を入力します。

4 接頭辞がオンリンク決定の目的に対して有効な期間を設定する「**有効存続期間 (分)**」を入力します。最小値は 1、最大値は 71,582,789 (これはライフタイムが無限であることを意味します)、既定値は **43200** 分です。

5 ステートレス アドレス自動設定を通して接頭辞から生成されるアドレスを残存させる期間を設定する「**優先存続期間 (分)**」を入力します。最小値は 1、最大値は 71,582,789 (これはライフタイムが無限であることを意味します)、既定値は **10080** 分です。

6 オプションで、この接頭辞をオンリンク決定のために使用できることを示す、接頭辞情報オプション内のリンク上フラグを有効にするには「**リンク上**」チェックボックスを選択します。

7 オプションで、この接頭辞をステートレス アドレス設定のために使用できることを示す、接頭辞情報オプション内の自律アドレス設定フラグを有効にするには「**自律**」チェックボックスを選択します。

8 「**OK**」を選択します。

インターフェースを DHCPv6 モードに設定する

DHCPv6 (IPv6 用 DHCP) は、IPv6 ホストに対してステートフル アドレス設定またはステートレス アドレス設定を提供する、クライアント/サーバ プロトコルです。DHCPv6 クライアントは、インターフェースが DHCPv6 モードで設定されている場合に、IPv6 アドレスおよびネットワーク パラメータを学習することが可能です。

DHCPv6 は、2 つの異なる設定モードを定義します。

- **DHCPv6 ステートフル モード**: DHCPv6 クライアントは IPv6 アドレスと共にその他のネットワーク パラメータ (例えば DNS サーバ、ドメイン名) を要求します。
- **DHCPv6 ステートレス モード**: DHCPv6 クライアントは IPv6 アドレス以外のネットワーク パラメータのみを要求します。

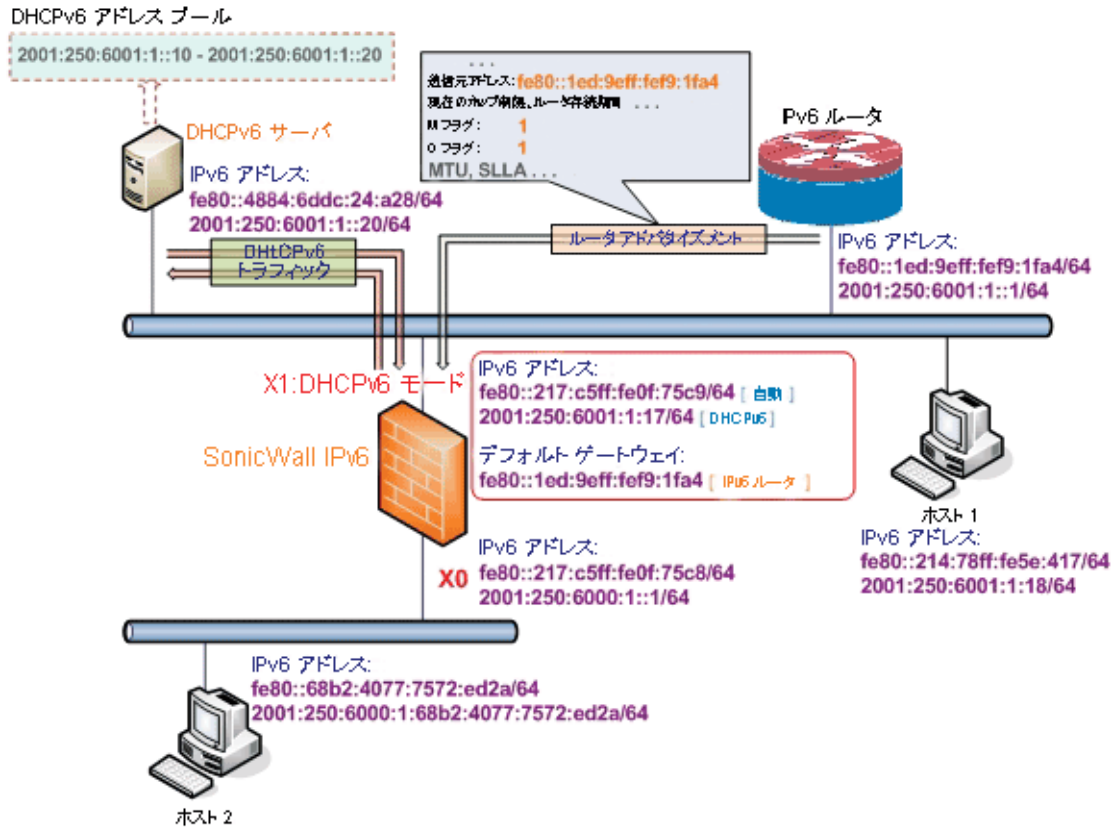
どのモードを選択するかは、通知されるルータ広告メッセージ内の管理 (M) アドレス設定、およびその他 (O) 設定フラグに応じて異なります。

DHCPv6 インフラ

フラグ		設定
M	O	
0	0	DHCPv6 インフラなし
1	1	IPv6 アドレスと、その他ネットワーク パラメータ設定の両方に対してDHCPv6 を使う IPv6 ホスト
0	1	IPv6 アドレス割り当てのみに DHCPv6 を使う IPv6 ホスト
1	0	その他のネットワーク パラメータ設定のみに対して DHCPv6 を使う IPv6 ホスト (DHCPv6 ステートレス)

「DHCPv6 トポロジ」に、DHCPv6 トポロジの例を示します。

DHCPv6 トポロジ



DHCPv6 では、以下の 3 種類の IPv6 アドレスが割り当て可能です。

- 自動アドレス
- 自律アドレス
- DHCPv6 クライアントを介して割り当てられる IPv6 アドレス

インターフェースを DHCPv6 アドレス用に設定するには、以下の手順に従います。

1 「**管理 | システム セットアップ | ネットワーク > インターフェース**」に移動します。

2 未定義インターフェースを設定する場合は、ページの右上隅にある「**IPv4**」を選択します。

3 設定するインターフェースの「**編集**」を選択します。「**インターフェースの編集**」ダイアログが表示されます。

4 「**ゾーン**」ドロップダウン メニューから「**WAN**」を選択します。その他のオプションが表示されます。

5 「**ネットワーク モード**」ドロップダウン メニューから「**DHCP**」を選択します。

6 「**OK**」を選択します。

7 ページの右上隅にある「**IPv6**」を選択します。装置の IPv6 アドレスが表示されます。

8 IPv6 アドレスを設定したいインターフェースの「**設定**」を選択します。「**インターフェースの編集**」ダイアログが表示されます。

9 「**ネットワーク モード**」ドロップダウン メニューから「**DHCPv6**」を選択します。オプションが次のように変化します。

10 DHCPv6 モード用に設定する IPv6 インターフェースに対しては、以下のオプションを設定できます。

- **DHCPv6 接頭辞委任を有効にする** - 有効にすると、次のオプションが使用できるようになります。
  - **委任された優先接頭辞を送信する** - DHCAPv6 クライアントに対して、委任された優先接頭辞 (2 つのフィールドで指定) の送信を要求する場合は、このオプションを有効にします。
  - **起動時に以前の委任された接頭辞の更新指示を送信する** - DHCPv6 クライアントに対して、ファイアウォールの起動時に以前割り当てられた、委任された接頭辞の更新を要求する場合は、このオプションを有効にします。
- **急速コミット オプションを使用する** - 有効にすると、DHCPv6 クライアントはアドレス割り当てのための 2 つのメッセージ交換で「急速コミット オプション」を使用します。
- **起動時に以前の IP の更新指示を送信する** - 有効にすると、DHCPv6 クライアントはファイアウォールの起動時に、以前に割り当てられたアドレスの更新を試みます。

11 インターフェースの「**DHCPv6 モード**」を選択します。RFC 要求により、DHCPv6 クライアントはルータ広告メッセージに応じて、選択する必要があるモード (ステートフルかステートレス) を決定します。この定義により、DHCPv6 モードを単独で決定するためのユーザの選択肢が制限されます。SonicWall による DHCPv6 の実装では、次の 2 種類のモードを定義して適合性と柔軟性のバランスを取っています。

- **自動** - IPv6 インターフェースは、ステートフル/ステートレス自動設定を使い、受信した最新のルータ広告メッセージ内の M および O 設定に従って、IPv6 アドレスを設定します。「DHCPv6 インフラ」テーブルを参照してください。
- **手動** - DHCPv6 モードは、受信したルータ広告に関係なく手動で設定されます。

「**ステートレス情報のみ要求する**」オプションにより、どちらの DHCPv6 モードが使用されるかが決まります。このオプションが非選択の場合は、DHCPv6 クライアントはステートフル モードで動作し、選択されている場合は、DHCPv6 クライアントはステートレス モードでネットワーク パラメータのみ取得します。

12 オプションで、「**ステートレス情報のみ要求する**」チェックボックスを選択して、DHCPv6 クライアントが DHCPv6 サーバに対してネットワーク パラメータ設定のみ要求するようにします。IPv6 アドレスは、ステートレス自動設定を通して割り当てられます。

13 オプションで、「**管理**」ログインまたは「**ユーザ ログイン**」を設定できます。

14 または、「**詳細**」タブを選択して詳細オプションを設定するか、「**プロトコル**」タブを選択して DHCPv6 ステートフルおよびステートレス設定情報を参照します。

15 「**OK**」を選択して、設定を完了します。

IPv6 インターフェースに対する詳細設定

IPv6 インターフェースの詳細設定を行うには、以下の手順に従います。

1 「**インターフェースの編集**」ダイアログで、「**詳細**」タブを選択します。

2 インターフェースにすべての IPv6 トラフィックの処理を停止させるには、「**インターフェース上のすべての IPv6 トラフィックを無効にする**」を選択します。IPv6 トラフィックを無効にすると、非 IPv6 トラフィックに対するファイアウォールのパフォーマンスを向上させることができます。このオプションは、既定では選択されていません。

> **ヒント**：ファイアウォールが純粋な IPv4 環境に配備されている場合、SonicWall ではこのオプションを有効にすることを推奨しています。

3 ファイアウォールがルータ広告を受信するようにするには、「**ルータ広告を受信する**」を選択します。無効にした場合、インターフェースはすべての着信ルータ広告メッセージを遮断するので、悪意のあるネットワーク パラメータ (例えば接頭辞情報やデフォルト ゲートウェイ) 受信の可能性を排除することによるセキュリティ向上が可能です。このオプションは、既定では選択されていません。

メモ：このオプションが無効になっている場合、割り当てられたすべての自律的 IPv6 アドレスがこのインターフェースから削除されます。

このオプションは自動モードでは表示されません。自動モードでは常に有効です。

このオプションを選択すると、「ステートレス アドレス自動設定を有効にする」オプションが使用できるようになります。

- このインターフェースに自律的 IPv6 アドレスを割り当てることを許可するには、「**ステートレス アドレス自動設定を有効にする**」を選択します。非選択にした場合は、割り当てられたすべての自律的 IPv6 アドレスがこのインターフェースから削除されます。

  メモ：このオプションが無効になっている場合、割り当てられたすべての自律的 IPv6 アドレスがこのインターフェースから削除されます。

  このオプションは自動モードでは表示されません。自動モードでは常に有効です。

4 このインターフェースに仮アドレスが割り当てられる前の重複アドレス検知 (DAD) 実行時に送信される、連続した近隣者要請メッセージの数を指定するには、「**重複アドレス検知の送信**」にその数値を入力します。最小値は 0 であり、これはインターフェースで DAD が実行されないことを示します。最大値は 9、既定値は **1** です。

IPv6 ノードは、同一リンク上の重複 IPv6 アドレスを検出するために、IPv4 の重複回避用 ARP (Gratuitous ARP) に似た近隣者要請メッセージを使います。DAD はどのユニキャスト アドレス (エニーキャスト アドレスを除く) 上でも、IPv6 インターフェースに仮アドレスを割り当てる前に実行される必要があります。

5 「**近隣者発見の基準到達可能時間 (秒)**」には、インターフェースのランダムな到達可能時間値の計算に使用する基準値を秒単位で入力します。最小値は 0、最大値は 9999、既定値は **30** です。

値 0 は、このパラメータが指定されないことを示し、その場合は「**ネットワーク > 近隣者発見**」のグローバル設定が使用されます。ただし、RA がこのインターフェースで有効になっている場合は、「**ルータ広告**」タブの「**到達可能時間**」オプションの値が使用されます。

6 インターフェース毎の最大 NDP サイズを有効にするには、「**インターフェース毎の最大 NDP サイズを有効にする**」を選択します。システム リソースが使い果たされるのを防ぐために、どのインターフェースにも最大 NDP サイズを設定してください。このオプションは、既定では選択されています。

「インターフェース毎の最大 NDP サイズ」フィールドに最大 NDP サイズを入力します。最小値は 64、最大値は 9999、既定値は **128** (WAN インターフェースの場合) または **1200** (その他の場合) です。

DHCPv6 プロトコル情報の表示

IPv6 インターフェースを DHCPv6 モードで設定する場合、「**プロトコル**」タブに追加の DHCPv6 情報が表示されます。

- **DHCPv6 一般情報**
  - **DHCPv6 状況**: インターフェースの設定によって異なります。
    - ステートレス モードで設定されている場合、DHCPv6 状況は「ステートレス」です。

- ステートフル モードで設定されている場合、DHCPv6 状況は「**有効**」か「**無効**」のどちらかになります。

  インターフェースがステートフル DHCPv6 モード の場合、**コメント** アイコンにマウス カーソルを合わせると、インターフェースに対する現在のルータ広告情報が表示されます。

- **DHCPv6 サーバ**: DHCPv6 サーバの IPv6 アドレスです。
- **DHCPv6 DUID**: DUID (DHCP 一意識別子) またはホストの識別子です。

- **DHCPv6 で取得したステートフル アドレス**: 取得したステートフル IPv6 アドレスの情報を表示します。

  - IAID (Identity Association Identifier)
  - 種別
  - IPv6 アドレス
  - リース存続期間

- **DHCPv6 で取得したステートレス設定**
  - **DNS サーバ 1/2/3**: DNS サーバの IPv6 アドレスです。

  該当するボタンを選択することで、DNS サーバを再取得、リリース、または再表示できます。

- **DHCPv6 によって取得した委任された接頭辞**: 取得した、ステートフル IPv6 アドレスの委任された接頭辞の情報を表示します。

  - IAID
  - 種別
  - IPv6 接頭辞
  - 接頭辞長
  - リース存続期間

  該当するボタンを選択することで、接頭辞を再取得、リリース、または再表示できます。

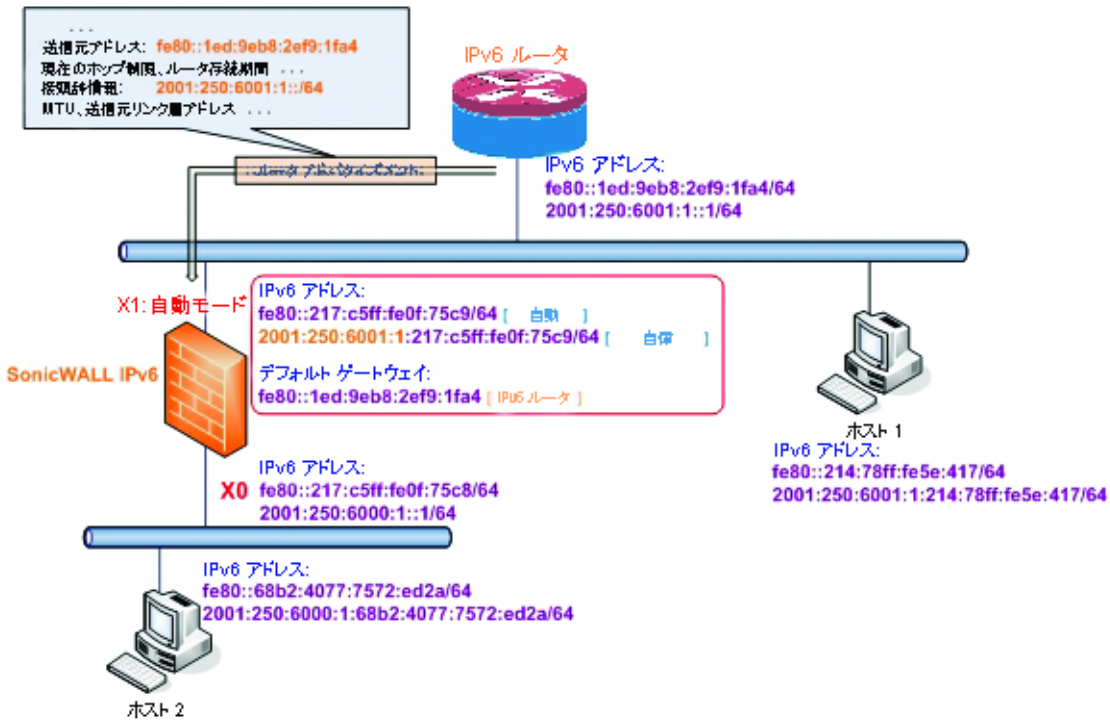
インターフェースを自動モードに設定する

自動モードは IPv6 アドレスの割り当てに IPv6 のステートレス アドレス自動設定を使います。このモードには、ネットワーク管理者による手動のアドレス設定は不要です。セキュリティ装置はネットワークをリッスンし、近隣ルータからの接頭辞情報を受信します。IPv6 ステートレス アドレス自動設定機能は、IPv6 アドレス割り当て、アドレス競合や期限切れに対するアドレス削除、およびオンリンク ルータから収集した情報に基づくデフォルト ゲートウェイ選択といった、すべての詳細設定を実行します。

メモ：自動モードは WAN ゾーンに対してのみ設定可能です。セキュリティを考慮して、LAN ゾーン インターフェースでは自動モードは利用できません。

「IPv6 自動モードの設定」に、自動モードで設定された IPv6 トポロジの例を示します。

IPv6 自動モードの設定



このモードでは、以下の 2 種類の IPv6 アドレスが割り当て可能です。

- 自動アドレス - インターフェースの既定のリンクローカル アドレスです。これはタイムアウトすることがなく、編集や削除ができません。
- 自律アドレス - ステートレス アドレス自動設定から割り当てられます。ユーザは、有効な存続期間が過ぎるのを待ちたくない場合に、アドレスを手動で削除できます。

IPv6 インターフェースを自動モードに設定するには、以下の手順に従います。

1 「**管理 | システム セットアップ | ネットワーク > インターフェース**」に移動します。

2 ページの右上隅にある「**IPv6**」を選択して IPv6 アドレスを表示します。

3 IPv6 アドレスを設定したいインターフェースの「**設定**」を選択します。「**インターフェースの編集**」ダイアログが表示されます。

4 「**ネットワーク モード**」ドロップダウン メニューから「**自動**」を選択します。

5 オプションで、インターフェースに仮アドレスを割り当てる前の重複アドレス検出 (DAD) 実行中に送信される連続した近隣者要請メッセージの数を指定するには、「**詳細**」タブの「**重複アドレス検知の送信**」にその数を入力します。0 を指定すると、このインターフェースでは DAD は実行されません。

6 「**OK**」を選択します。

PPPoE

IPv6 では PPPoE クライアント モードのみがサポートされています。

VLAN サブインターフェースを設定する

IPv6 での VLAN サブインターフェースの設定手順は、IPv4 での設定と同じです。詳細については、「仮想インターフェース (VLAN サブインターフェース) (327 ページ)」を参照してください。

すべての VLAN サブインターフェースは、IPv6 での設定前に IPv4 で設定する必要があります。

ワイヤ モードでのインターフェースの設定

メモ：ワイヤ モードは NSA 2600 以降の装置でサポートされます。

IPv6 でのワイヤ モード インターフェースの設定手順は、IPv4 での設定と同じです。詳細については、「ワイヤ モードでのインターフェースの設定 (335 ページ)」を参照してください。

ワイヤ モード インターフェースはすべて IPv4 で設定する必要があります。IPv6 でワイヤ モード設定を編集することはできません。IPv4 で有効にした機能 (「リンク状況伝達」など) はすべて IPv6 に適用されます。

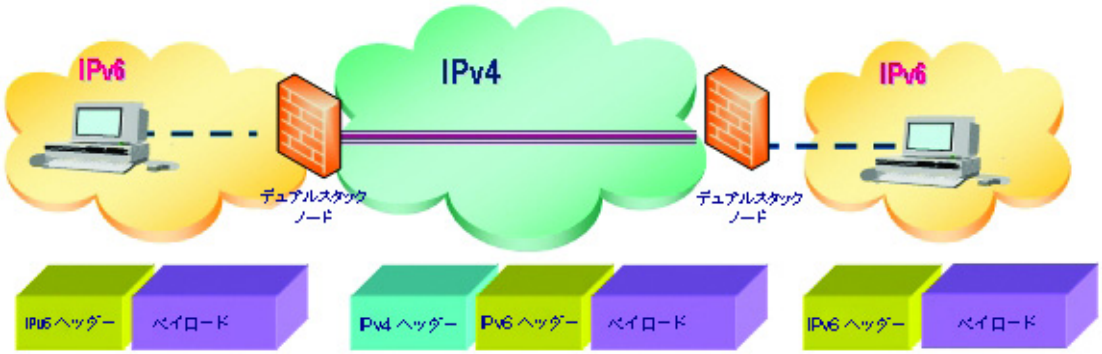
IPv6 トンネル インターフェースの設定

このセクションでは、IPv6 ネットワークを通して IPv4 パケットをトンネルする、また IPv4 ネットワークを通して IPv6 パケットをトンネルする方法について説明します。例えば、IPv4 ネットワーク上で IPv6 パケットを通過させるために、IPv6 パケットはトンネルの入り口側で IPv4 パケット内にカプセル化されます。カプセル化されたパケットがトンネルの出口に到着すると、IPv4 パケットはカプセル化解除されます。

トンネルは自動または手動設定どちらでも可能です。設定されたトンネルは、カプセル化するノード上の設定情報から、エンドポイント アドレスを決定します。自動トンネルは、付加された IPv6 データグラムのアドレスから IPv4 エンドポイントを決定します。IPv4 マルチキャスト トンネルは近隣者発見を通してエンドポイントを決定します。

「IPv6-to-IPv4 トンネル インターフェース」に IPv6-to-IPv4 トンネルを示します。

IPv6-to-IPv4 トンネル インターフェース



トピック:

- 6to4 自動トンネルを設定する (998 ページ)
- 非 2002 接頭辞へのアクセスのための 6to4 リレーの設定 (999 ページ)
- 手動 IPv6 トンネルを設定する (999 ページ)

- GRE IPv6 トンネルを設定する (1001 ページ)
- IPv6 接頭辞委任 (1001 ページ)
- 6rd トンネル インターフェース (1003 ページ)
- ISATAP トンネルを設定する (1005 ページ)

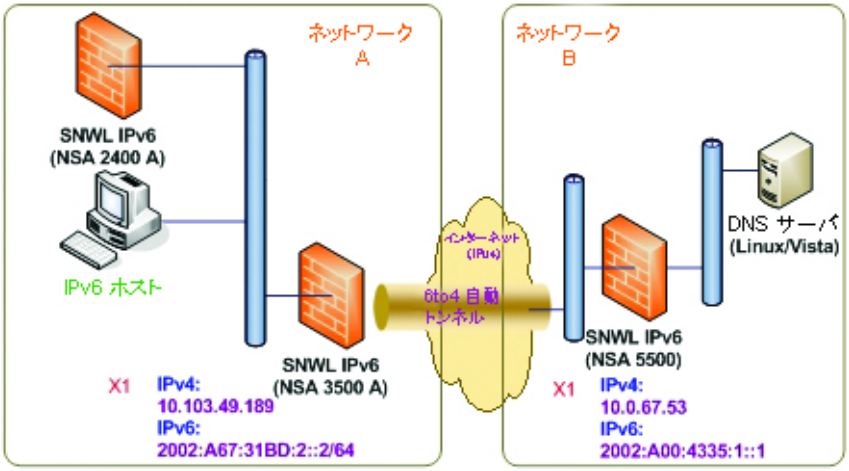
6to4 自動トンネルを設定する

6to4 自動トンネルは、トンネル エンドポイントをカプセル化された IPv6 データグラムから抽出する自動トンネルです。手動設定は不要です。

6to4 トンネルは `2002:tunnel-IPv4-address::/48` という形式の接頭辞を使用して、IPv4 上で IPv6 トラフィックをトンネルします (例えばトンネルの IPv4 終点がアドレス "a01:203" を持つ場合、6to4 トンネル接頭辞は "2002:a01:203::1" です)。ルータは IPv6 クライアントに `2002:[IPv4]:xxxx/64` という形式の接頭辞を通知します。完全な情報については、RFC 3056 を参照してください。

「6to4 自動トンネル トポロジ」に、6to4 自動トンネル トポロジの例を示します。

6to4 自動トンネル トポロジ



「IPv6-to-IPv4 トンネル インターフェース」では、顧客がトンネル エンドポイントを指定する必要はなく、6to4 自動トンネルを有効にする必要があるだけです。2002 の接頭辞を持つすべてのパケットはトンネルにルーティングされ、トンネルの IPv4 宛先は、IPv6 の宛先アドレスから抽出されます。

6to4 トンネルは容易に設定して使用できます。ユーザはグローバル IPv4 アドレスと、接頭辞が 2002 の IPv6 アドレスを持つ必要があります。そのため一般的には、ユーザは接頭辞 が 2002 のネットワーク リソースにしかアクセスできません。

メモ：6to4 自動トンネルは、セキュリティ装置上に 1 つだけ設定できます。

メモ：VPN トンネル インターフェースによって、IPv6 リンク ローカル アドレスが自動的に作成されています。

ファイアウォールで6to4 自動トンネルを設定するには、以下の手順を実行します。

1 「**管理 | システム セットアップ | ネットワーク > インターフェース**」に移動します。

2 次のどちらかを行います。

- 「**インターフェースの追加**」を選択します。

- 「**インターフェースの追加**」ドロップダウン メニューから「**トンネル インターフェース**」を選択します。

「**インターフェースの編集**」ダイアログが表示されます。

3 6to4 トンネル インターフェースの「**ゾーン**」を選択します。通常は WAN インターフェースです。

4 「**トンネル種別**」ドロップダウン メニューから「**6to4 自動トンネル インターフェース**」を選択します。

5 「**名前**」フィールドで名前を指定します。インターフェースの「**名前**」は既定で「**6to4AutoTun**」に設定されます。

6 「**IPv6 6to4 トンネルを有効にする**」チェックボックスを選択します。既定では、このオプションは無効になっています。

7 必要に応じて、1 つ以上の**管理**ログイン プロトコルを設定できます。**HTTPS**、**Ping**、または **SNMP** が選択できます。

> **メモ**：「**HTTPS**」を選択すると、「**HTTP から HTTPS へのリダイレクトを有効にするためのルールを追加する**」オプションが自動的に有効になります。このオプションは、他のプロトコルでは選択できません。このオプションの詳細については、「HTTP/HTTPS リダイレクト (286 ページ)」を参照してください。

8 必要に応じて、次の**ユーザ ログイン** プロトコルの一方または両方を設定できます: **HTTP** または **HTTPS**。

> **メモ**：「**HTTPS**」のみを選択すると、「**HTTP から HTTPS へのリダイレクトを有効にするためのルールを追加する**」オプションが自動的に有効になります。このオプションの詳細については、「HTTP/HTTPS リダイレクト (286 ページ)」を参照してください。「**HTTP**」も選択した場合は、「**HTTP から HTTPS へのリダイレクトを有効にするためのルールを追加する**」オプションは選択解除され、選択できなくなります。

9 「**OK**」を選択します。

非 2002 接頭辞へのアクセスのための 6to4 リレーの設定

6to4 自動トンネルは既定では、接頭辞が 2002 の宛先にしかアクセスできません。6to4 リレー機能を使うと、非 2002 接頭辞の宛先にアクセスできます。

6to4 リレーを有効にするには、以下の手順に従います。

1 「**管理 | システム セットアップ | ネットワーク > ルーティング**」に移動します。

2 「**追加**」を選択して、接頭辞が 2003 の宛先へのすべてのトラフィックを 6to4 自動トンネル インターフェース経由でルーティングできるルート ポリシーを作成します。

この静的ルートは、6to4 トンネルを通して 2002: 以外の接頭辞を持つ IPv6 宛先へのアクセスを可能にするリレー機能を有効にするために 6to4 自動トンネル インターフェース上に追加できます。

> **メモ**：ゲートウェイは 2002: という 接頭辞を持つ IPv6 アドレスでなければならないことに注意してください。

手動 IPv6 トンネルを設定する

ファイアウォールで6to4 トンネルを設定するには、以下の手順を実行します。

1 「**管理 | システム セットアップ | ネットワーク > インターフェース**」に移動します。

2 「**インターフェースの追加**」を選択します。「**インターフェースの編集**」ダイアログが表示されます。

3 トンネル インターフェースの「**ゾーン**」を選択します。

4 「**トンネル種別**」ドロップダウン メニューから「**IPv6 手動トンネル インターフェース**」を選択します。このオプションは既定の設定です。

5 トンネル インターフェースの「**名前**」を入力します。

6 「**トンネル インターフェース IPv6 アドレス**」フィールドにアドレスを入力します。このフィールドは既に :: で始まっています。

7 トンネルに関連付けるインターフェースを「**関連付け先**」ドロップダウン メニューから選択します。既定は「**X1**」です。

8 「**リモート IPv4 アドレス**」ドロップダウン メニューからトンネル エンドポイントの IPv4 アドレス オブジェクトを選択します。

9 「**リモート IPv6 ネットワーク**」ドロップダウン メニューから IPv6 アドレス オブジェクトを選択します。グループ、範囲、ネットワーク、またはホストを選択できます。

10 必要に応じて、1 つ以上の**管理**ログイン プロトコルを設定できます。**HTTPS**、**Ping**、または **SNMP** が選択できます。

> ⓘ **メモ**：「**HTTPS**」を選択すると、「**HTTP から HTTPS へのリダイレクトを有効にするためのルールを追加する**」オプションが自動的に有効になります。このオプションの詳細については、「HTTP/HTTPS リダイレクト (286 ページ)」を参照してください。このオプションは、他のプロトコルでは選択できません。

11 必要に応じて、次の**ユーザ ログイン** プロトコルの一方または両方を設定できます: **HTTP** または **HTTPS**。

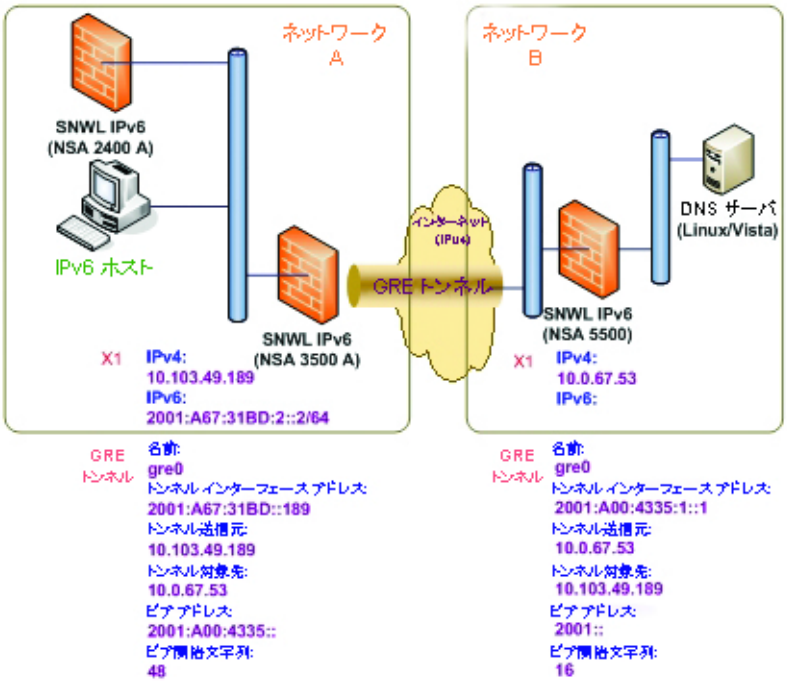
> ⓘ **メモ**：「**HTTPS**」のみを選択すると、「**HTTP から HTTPS へのリダイレクトを有効にするためのルールを追加する**」オプションが自動的に有効になります。このオプションの詳細については、「HTTP/HTTPS リダイレクト (286 ページ)」を参照してください。「**HTTP**」も選択した場合は、「**HTTP から HTTPS へのリダイレクトを有効にするためのルールを追加する**」オプションは選択解除され、選択できなくなります。

12 「**OK**」を選択します。

GRE IPv6 トンネルを設定する

GRE は IPv4 または IPv6 上で IPv4 および IPv6 をトンネルするために使用できます。GRE トンネルは、両側のエンドポイントを手動で指定する静的トンネルです。「GRE IPv6 トンネルの設定」に、GRE IPv6 トンネルの例を示します。

GRE IPv6 トンネルの設定



GRE トンネルの設定は手動トンネルと似ていますが、「**トンネル種別**」に「**GRE トンネル インターフェース**」を選択することが異なります。

IPv6 接頭辞委任

DHCPv6 接頭辞委任 (DHCPv6-PD) とも呼ばれる IPv6 接頭辞委任は、DHCPv6 に対する拡張機能です。DHCPv6 では、アドレスが DHCPv6 サーバによって IPv6 ホストに割り当てられます。DHCPv6-PD では、完全な IPv6 サブネット アドレスと他のパラメータが DHCPv6-PD サーバによって DHCPv6-PD クライアントに割り当てられます。

DHCPv6-PD が有効になっている場合、WAN ゾーンに接続されているすべての DHCPv6 インターフェースに DHCPv6-PD が適用されます。DHCPv6-PD は、DHCPv6 と共存する追加のサブネット設定モードです。

IPv6 アドレスは、DHCPv6-PD サーバによって提供される接頭辞と、DHCPv6-PD クライアントによって提供される接尾辞を組み合わせたものになります。接頭辞長は既定で 64 ですが、この値は編集できません。

ファイアウォールを起動すると、*DHCPv6 委任による接頭辞*という既定のアドレス オブジェクト グループが自動的に作成されます。アップストリーム インターフェースから委任された接頭辞は、このグループのメンバーです。

IPv6 接頭辞委任の設定は、以下に対して行います。

- アップストリーム インターフェース
- 1 つ以上のダウンストリーム インターフェース

アップストリーム インターフェースが接頭辞委任を DHCPv6-PD サーバから学習すると、SonicOS は IPv6 アドレスの接頭辞を計算してすべてのウンストリーム インターフェースに適用し、ダウンストリーム インターフェースはこの情報を各自のネットワーク セグメント内のすべてのホストに通知します。

このセクションでは、以下の設定手順について説明します。

- アップストリーム インターフェースでの IPv6 接頭辞委任の設定 (1002 ページ)
- ダウンストリーム インターフェースでの IPv6 接頭辞の設定 (1002 ページ)

重要：ネットワーク内で接頭辞委任を無効にする前に、まずアップストリーム インターフェースで接頭辞委任を破棄することを推奨します。

アップストリーム インターフェースでの IPv6 接頭辞委任の設定

アップストリーム インターフェースで IPv6 接頭辞委任を設定するには:

1. 「**管理 | システム セットアップ | ネットワーク > インターフェース**」に移動します。
2. 「**表示する IP バージョン**」で「**IPv6**」を選択します。
3. アップストリーム インターフェースとして設定したいインターフェースの「**設定**」列にある「**編集**」アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。

   メモ：「**ゾーン**」は常に「**WAN**」です。

4. 「**ネットワーク モード**」メニューから、「**DHCPv6**」を選択します。
5. 「**DHCPv6 接頭辞委任を有効にする**」オプションを選択します。
6. 「**DHCPv6 モード**」メニューから、「**手動**」を選択します。
7. 設定された DHCPv6 情報を確認するには、「**プロトコル**」タブを選択します。

   「**DHCPv6 一般情報**」パネルには、**DHCPv6 DUID** が表示されます。

   「**DHCPv6 で取得したステートフル アドレス**」パネルには、ステートフル **IAID** が表示されます。

   「**DHCPv6 によって取得した委任された接頭辞**」パネルには、委任された **IAID** が表示されます。
8. 「**更新**」を選択します。その他の列の情報が表示されます。

ダウンストリーム インターフェースでの IPv6 接頭辞の設定

ダウンストリーム インターフェースで IPv6 接頭辞委任を設定するには:

1. 「**管理 | システム セットアップ | ネットワーク > インターフェース**」に移動します。
2. 「**IPv6**」オプションを選択します。
3. ダウンストリーム インターフェースとして設定したいインターフェースの「**設定**」列にある「**編集**」アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。
4. 「**ルータ広告を有効にする**」オプションを選択します。
5. 「**詳細**」タブを選択します。

   アップストリームの接頭辞が取得されている場合は、「**IPv6 アドレス**」パネルにその接頭辞が表示されます。
6. アップストリームの接頭辞が取得できていない場合は、「**IPv6 アドレス**」パネルに代替アドレスが表示されます。
7. 「**アドレスの追加**」を選択して、「**IPv6 アドレスの追加**」ダイアログを表示します。

8 「**委任されたダウンストリーム IPv6 アドレスを追加する**」オプションを選択します。

9 (省略可能)「**静的 IPv6 アドレスのサブネット接頭辞を広告する**」オプションを選択します。

10 「**ルータ広告**」タブを選択します。

11 「**ルータ広告を有効にする**」オプションを選択します。

「**一般**」タブにある「**静的 IPv6 アドレスのサブネット接頭辞を広告する**」オプションを選択した場合は、接頭辞が「**接頭辞リストの設定**」パネルに表示されます。

12 新しい IPv6 PD インターフェースを確認するには、「**管理 | システム セットアップ | ネットワーク > ルーティング**」に移動します。

13 「**IPv6**」オプションを選択します。

接頭辞委任による 2 つの新しい IPv6 インターフェース (アップストリームおよびダウンストリーム) が表示されます。

6rd トンネル インターフェース

IPv6 の急速配備 (6rd) では、IPv4 ネットワーク全体に IPv6 を迅速かつ容易に配備できます。6rd では、サービス プロバイダの既存の IPv6 アドレス接頭辞を利用して、6rd の運用ドメインが、サービス プロバイダのネットワークに制限され、サービス プロバイダの直接的な管理下に置かれるようにします。

6rd トンネル インターフェースは、6rd のカプセル化された IPv6 パケットを IPv4 ネットワーク内で転送する仮想インターフェースです。

メモ：6rd トンネル インターフェースは、物理インターフェースまたは仮想インターフェースにバインドされている必要があります。

6rd の配備が行われると、IPv6 サービスはネイティブの IPv6 と等価です。IPv4 アドレスに対する IPv6 アドレスの 6rd 割付は、IPv6 接頭辞からの IPv4 トンネル エンドポイントの自動決定を実現し、6rd のステートレス運用を可能にします。

6rd ドメインは、数台の 6rd カスタマー エッジ (CE) ルータと 1 台以上の 6rd ボーダー リレー (BR) ルータで構成されます。6rd によってカプセル化された IPv6 パケットは、サービス プロバイダ ネットワーク内の IPv4 ルーティング トポロジに従います。

カスタマー エッジ ルータとボーダー リレー ルータを使用した一般的な 6rd 実装に必要な 6rd トンネル インターフェースは、1 つだけです。複数の 6rd ドメインでサービスを提供するボーダー リレー ルータは、複数のトンネル インターフェースを持っている場合があります。ただし、それぞれの 6rd ドメインで持つことができる 6rd トンネル インターフェースは 1 つだけです。

IPv6 パケットは、サービス プロバイダの 6rd ドメインに出入りする際にボーダー リレーを通過します。6rd はステートレスなので、パケットはエニーキャスト方式を使用してボーダー リレーに送信できます。この方式では、1 つの送信元からのパケットが受信者候補のグループ内の最も近いノード、またはすべてが同じ送信先アドレスによって識別される複数のノードにルーティングされます。

サービス プロバイダは、6rd を 1 つのドメイン、または複数のドメインに配備できます。1 つの 6rd ドメインは 6rd 接頭辞を 1 つしか持てません。異なる 6rd ドメインは別々の 6rd 接頭辞を使用する必要があります。

「**管理 | システム セットアップ | ネットワーク > ルーティング**」の「**ルート ポリシー**」パネルには、6rd トンネル インターフェース用の 4 つの既定のルート ポリシーがあります。

次の 2 つの設定モードがあります。

- 手動
- DHCP

次の 4 つの 6rd パラメータは手動で設定できます。また、設定モードとして DHCP を選択している場合は、DHCPv4 サーバによって自動的に設定することもできます。

- IPv4 マスク長
- 6rd 接頭辞
- 6rd 接頭辞長
- 6rd BR IPv4 アドレス

DHCP モードでは、6rd パラメータをバインドされたインターフェースから受け取ります。手動モードでは、6rd パラメータを手動で設定する必要があります。

6rd トンネル インターフェースの設定

6rd トンネル インターフェースは、その他の IPv6 トンネル インターフェースと同じように設定できます。6rd トンネル インターフェースを設定するには、バインドされたインターフェースが必要です。

6rd トンネル インターフェースを設定するには:

1 「**管理 | システム セットアップ | ネットワーク > インターフェース**」に移動します。

2 「**表示する IP バージョン**」で「**IPv6**」を選択します。

3 「**インターフェース設定**」パネルの一番下にある「**インターフェースの追加**」を選択します。

> **メモ：**「**プロトコル**」タブは、「設定モード」として「DHCP」を選択している場合にのみ表示されます。

4 「**ゾーン**」ドロップダウン メニューから「**WAN**」を選択します。

5 「**インターフェース種別**」メニューは無効になっています。この設定は既に「ステップ 3」で「**インターフェースの追加**」メニューから選択した「**トンネル インターフェース**」になっています。

6 「**トンネル種別**」メニューから「**6rd トンネル インターフェース**」を選択します。

7 「名前」ボックスにトンネル インターフェースの名前を入力します (例: **6rd Tunnel**)。

8 「**トンネル インターフェース IPv6 アドレス**」フィールドに、トンネル インターフェースの IPv6 アドレスを入力します。例えば、"**2001::2**" と入力します。

9 「**接頭辞長**」フィールドに、IPv6 接頭辞の長さを入力します。例えば、"**64**" と入力します。

10 「**関連付け先**」ドロップダウン メニューから適切なインターフェース (**X1** など) を選択します。

11 「**設定モード**」ドロップダウン メニューから適切なモードを選択します。「**手動**」または「**DHCP**」を選択します。

> **メモ：**「**設定モード**」として「**手動**」を選択した場合は、「ステップ 12」～「ステップ 15」を実行します。
>
> 「**設定モード**」として「**DHCP**」を選択した場合は、「ステップ 12」～「ステップ 15」をスキップします。

12 「**6rd 接頭辞**」フィールドに 6rd 接頭辞 (**2222:2222::** など) を入力します(「**手動**」モードのみ)。

13 「**6rd 接頭辞長**」フィールドに 6rd 接頭辞の長さ (**32** など) を入力します (「**手動**」モードのみ)。

14 「**IPv4 マスク長**」フィールドに IPv4 サブネット マスクの長さを入力します (「**手動**」モードのみ)。

15 「**BR IPv4 アドレス**」フィールドに、6rd ボーダー リレーの IPv4 アドレスを入力します (「**手動**」モードのみ)。

16 (オプション) 「**コメント**」フィールドにトンネル インターフェースを説明するコメントを入力します。

17 「**デフォルト ルートに自動的に追加する**」オプションを選択します。

18 適切な「**管理**」オプションまたは「**ユーザ ログイン**」オプションを選択します。

「**設定モード**」として「**手動**」を選択した場合は、「**一般**」タブに 6rd トンネル インターフェースの設定が表示されます。

「**設定モード**」として「**DHCP**」を選択した場合は、「**プロトコル**」タブに 6rd トンネル インターフェースの設定が表示されます。

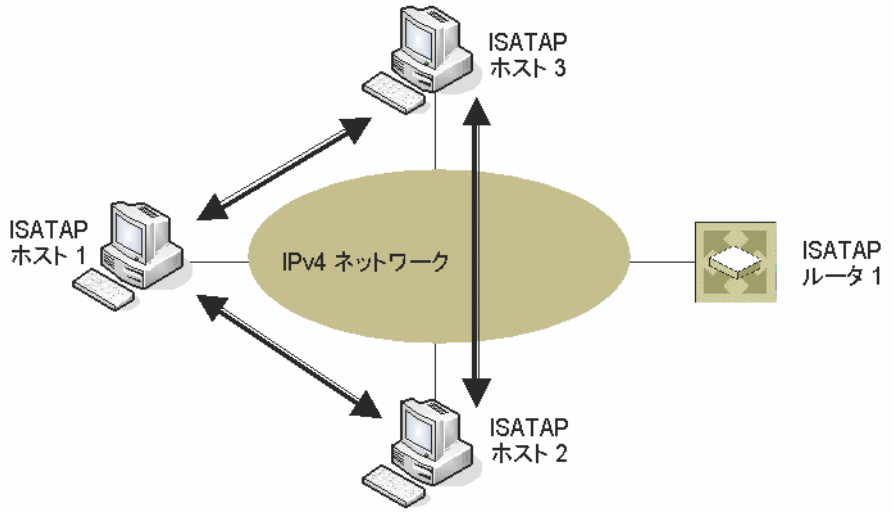
ISATAP トンネルを設定する

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) を使用すると、IPv4 のみのインフラストラクチャに IPv6 との接続性を持たせることができます。ISATAP は、IPv4 ネットワーク経由でデュアルスタック (IPv6/IPv4) ノードどうしを接続したり、IPv6 ノードどうしを接続したりするシンプルなトンネリング メカニズムです。IPv4 ネットワークは、ISATAP にとって IPv6 のリンク レイヤとみなされます。

ISATAP は、ISATAP ホスト間、および ISATAP ホストと IPv6 ネットワーク上のホストとの間のユニキャスト接続を提供するなどのシナリオで利用できます。

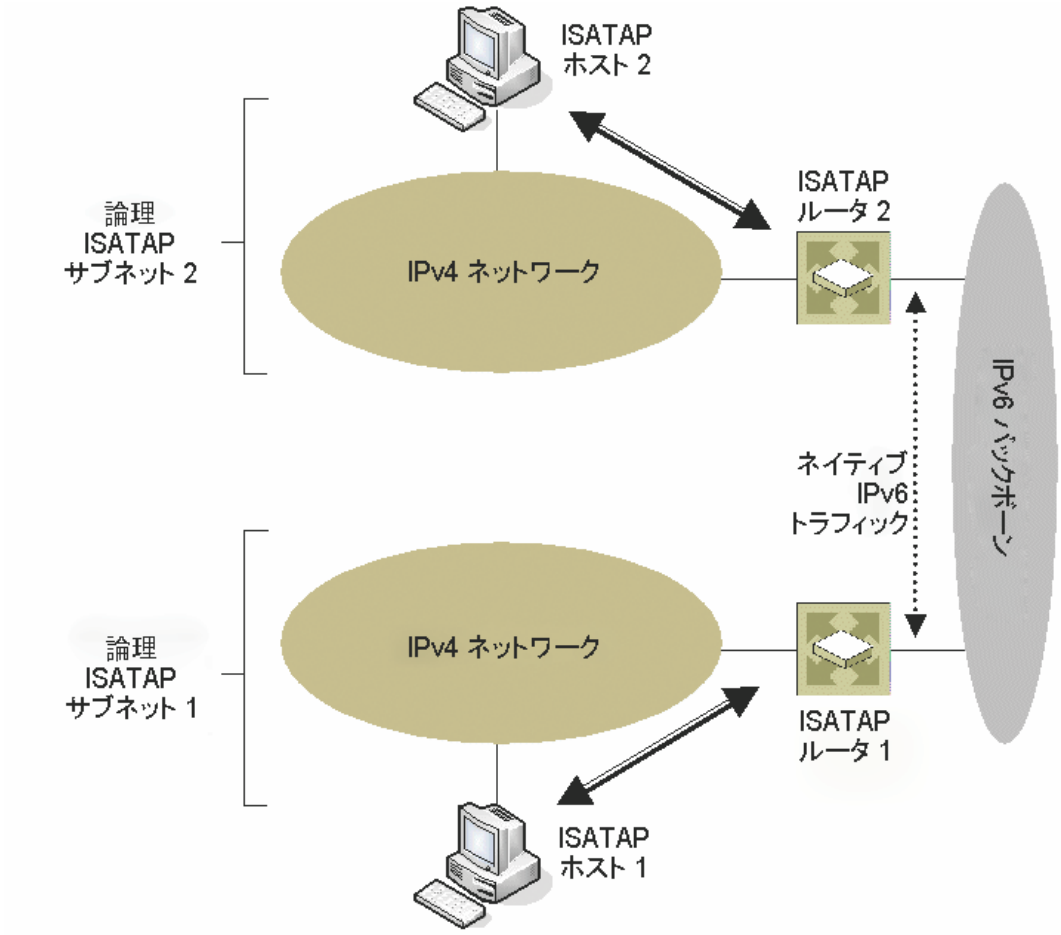
「同一の論理 ISATAP サブネット上にある ISATAP ホスト間のトラフィック」は、同一の論理 ISATAP サブネット上にある ISATAP ホスト間の ISATAP トラフィックを示しています。

同一の論理 ISATAP サブネット上にある ISATAP ホスト間のトラフィック



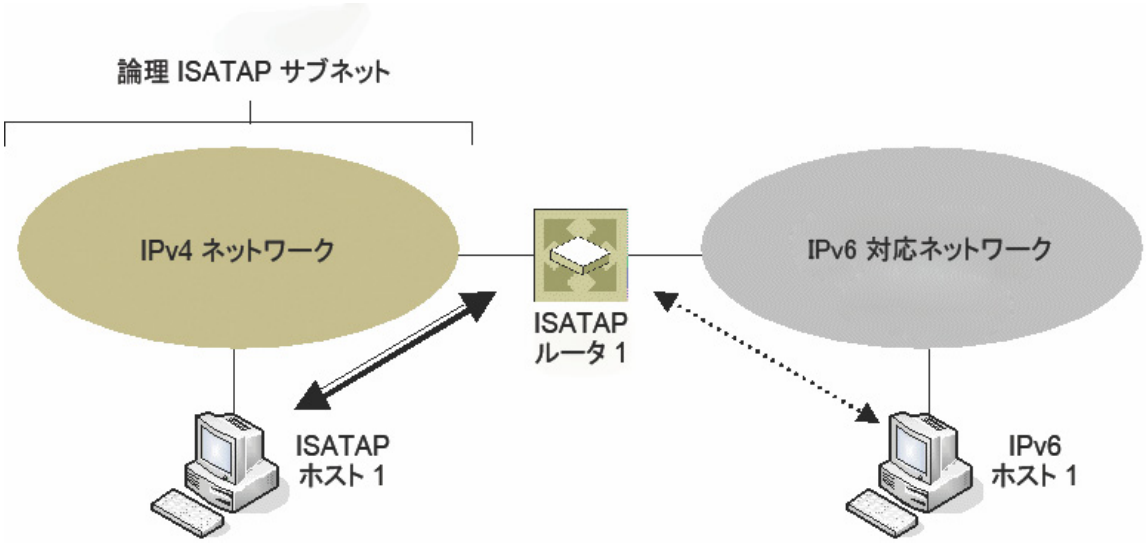
「異なる ISATAP サブネット上にある ISATAP ホスト間のトラフィック」は、異なる ISATAP サブネット上にあるホスト間の ISATAP トラフィックを示しています。

異なる ISATAP サブネット上にある ISATAP ホスト間のトラフィック



「ISATAP ホストと IPv6 ネットワーク上のホストの間のパケットの送信」は、ISATAP ホストと IPv6 ネットワーク上のホストの間のパケットの送信を示しています。

ISATAP ホストと IPv6 ネットワーク上のホストの間のパケットの送信



「ISATAP ホストと IPv6 ネットワーク上のホストの間のパケットの送信」に示すシナリオでは、ISATAP ホストどうしは ISATAP ルータまたは IPv6 ネットワークを経由することなく直接通信できます。これにより、IPv6 対応のアプリケーションが既存の IPv4 インフラストラクチャの接続環境を活用できます。

その他の 2 つのシナリオでは、ISATAP ルータの IPv6 インターフェースを IPv6 ネットワークに接続する必要があります。これにより、ISATAP インターフェースにつながる IPv4 ネットワークと IPv6 インターフェースの間の転送が可能になります。

ISATAP は、ホストとルータの両方に実装して実行する必要があります。デュアルスタックのサポートは、Windows XP と Windows 7 では既定で有効になっています。

SonicOS が ISATAP に対応しているため、セキュリティ装置は LAN 側インターフェースで ISATAP ルータとして機能し、ISATAP トンネリング インターフェースと IPv6 ネットワークに接続された IPv6 インターフェースの間で IPv6 パケットを転送します。

ISATAP トンネルを設定するには、以下の手順に従います。

1 「**管理 | システム セットアップ | ネットワーク > インターフェース**」の「**表示する IP バージョン**」で、「**IPv6**」を選択します。

2 「**インターフェースの追加**」を選択します。

3 「**一般**」タブで、トンネル インターフェースの「**ゾーン**」を選択します。

4 「**トンネル種別**」ドロップダウン リストから、「**ISATAP トンネル インターフェース**」を選択します。

5 トンネル インターフェースの「**名前**」を入力します。

6 **関連付け先 IPv4 アドレス** - ドロップダウン メニューからインターフェースを選択します。ISATAP トンネルは、6over4 トンネルの IPv4 エンド アドレスとして関連付け先インターフェースの IPv4 アドレスを使用します。

7 **IPv6 サブネット接頭辞** - ドロップダウン メニューからアドレス オブジェクトを選択します (または「アドレス オブジェクトの作成」を選択します)。IPv6 サブネット接頭辞は、64 ビットの接頭辞です。ISATAP ホストは、これを ISATAP アドレスの自動設定に使用します。

8 **トンネル インターフェース リンク MTU** - インターフェース リンクに対する推奨 MTU です。値 0 は、ファイアウォールがこのリンクに対してリンク MTU を通知しないことを意味します。

9 「**コメント**」フィールドに、必要に応じてコメント テキストを入力します。このテキストは、「**インターフェース**」テーブルの「**コメント**」列に表示されます。

10 このインターフェースを介したファイアウォールのリモート管理を有効にするには、サポートされている管理プロトコルを選択します。**HTTPS**、**Ping**、または **SNMP** が選択できます。

11 限定的な管理権限を持つ選ばれたユーザがセキュリティ装置にログインすることを許可するには、「**ユーザ ログイン**」で、「**HTTP**」と「**HTTPS**」のいずれかまたは両方を選択します。

さらに、「**管理 | セキュリティ設定 | ファイアウォール設定 | 詳細設定**」で、SonicOS が ISATAP ホストの問い合わせを解決する方法を指定することもできます。ファイアウォールの詳細設定については、『*SonicOS セキュリティ設定*』を参照してください。

12 「**IPv6 の詳細設定**」セクションを見つけます。

- **ISATAP の NetBIOS 名クエリ応答を有効にする** - このオプションを選択すると、ファイアウォールが NetBIOS クエリに応答するようになり、ISATAP ホストによる NetBIOS 名から IPv4 アドレスへの名前解決をサポートします。
- **解決済みの名前 ISATAP の有効期間 (秒)** - 時間を秒単位で入力します。

IPv6 を使用した SonicWall 管理インターフェースへのアクセス

セキュリティ装置上で IPv6 アドレス指定を設定した後、ブラウザの URL フィールドにセキュリティ装置の IPv6 アドレスを入力することで、SonicWall 管理インターフェースにアクセスできます。

IPv6 ネットワークの設定

トピック:

- IPv6 の DNS (1008 ページ)
- アドレス オブジェクト (1008 ページ)
- ポリシーベース ルーティング (1008 ページ)
- IPv6 NAT ポリシー (1009 ページ)
- 近隣者発見プロトコル (1009 ページ)
- DHCPv6 の設定 (1010 ページ)

IPv6 の DNS

IPv6 用の DNS は IPv4 用と同じ方法で設定されます。「**管理 | システム セットアップ | ネットワーク > DNS**」の左上にある「**表示する IP バージョン**」で「**IPv6**」を選択します。

アドレス オブジェクト

IPv6 アドレス オブジェクトとアドレス グループは IPv4 アドレス オブジェクトと同じ方法で追加できます。アドレス オブジェクトの設定については、『*SonicOS ポリシー*』を参照してください。

メモ：種別がホスト、範囲、ネットワークのアドレス オブジェクトがサポートされます。現時点では IPv6 ホストに対して、MAC と FQDN の動的アドレス オブジェクトはサポートされません。

IPv4 インターフェースは各インターフェースに対して既定のアドレス オブジェクト (DAO) とアドレス オブジェクト グループのペアを定義します。IPv4 DAO の基本ルールでは、各 IPv4 アドレスが次の 2 つのアドレス オブジェクトに対応します。インターフェース IP とインターフェース サブネットです。ゾーン インターフェース IP、ゾーン サブネット、すべてのインターフェース IP、すべてのインターフェース管理 IP などの AO グループのペアも存在します。

IPv6 インターフェースは、各インターフェースのために同じ DAO セットを作成します。複数の IPv6 を 1 つのインターフェースに割り当てることが可能なため、それらすべてのアドレスを動的に追加、編集、削除できます。したがって、IPv6 DAO は動的に作成され、削除される必要があります。

これを処理するために、DAO は IPv6 インターフェースに対して動的に生成されません。制限によりインターフェース DAO を参照する必要がある他のモジュールをサポートする、限られたインターフェース DAO だけが作成されます。

ポリシーベース ルーティング

IPv6 に対してポリシー ベースのルーティングを完全にサポートするには、「**管理 | システム セットアップ | ネットワーク > ルーティング**」でルート ポリシーに対して IPv6 アドレス オブジェクトとゲートウェイを選択します。

次世代 RIP (RIPng) は、IPv6 ベースのネットワークを通して、ルート計算のための情報を交換することを可能にする、IPv6 に対するルーティング情報プロトコルです。

RIP と RIPng を切り替えるラジオ ボタンがあります。

IPv6 NAT ポリシー

IPv6 または NAT64 に対する NAT ポリシーは、「**管理 | ポリシー | ルール | NAT ポリシー**」で設定可能です。IPv6 NAT ポリシーを設定する場合、送信元と送信先オブジェクトには、NAT64 の IP バージョンが指定されていない限り、IPv6 アドレス オブジェクトのみ使用可能です。NAT ポリシーの設定の詳細については、『*SonicOS ポリシー*』を参照してください。

メモ：現時点では NAT ポリシーに対する IPv6 監視はサポートされていません。

NAT64 ステートフル検査ネットワーク ストリームのサポート

ステートフル検査ネットワーク ストリーム (通常、アプリケーション層のデータを含みます) では、キャッシュ エントリをその場で作成する必要があります。これらのキャッシュ エントリは、パケット フィルタのルール テーブルに基づいて通常は無効になっていますが、アプリケーション層のデータ内の特定のディレクティブ (FTP データ接続用の受信キャッシュ エントリの追加など) によって許可されます。

SonicOS では、これらのネットワーク ストリームが、HTTPS や SNMP のような一般的なアプリケーション層プロトコル ストリームとは異なる形で処理されます。これらのステートフル検査ネットワーク ストリームとしては、FTP、TFTP、H.323、MSN、Oracle、PPTP、RTSP、RealAudio があります。ステートフル検査ネットワーク ストリームでは、クライアントとサーバが制御チャンネル経由で互いに通信する際にデータ キャッシュの作成を予期する必要があります。

当社のシステムは、NAT64 で FTP (アクティブおよびパッシブ モードを含む) および TFTP プロトコルを適切にサポートしています。

近隣者発見プロトコル

近隣者発見プロトコル (NDP) は、IPv4 の ICMP と ARP が実現するいくつかのタスクを実行するために IPv6 の一部として作成された、新しいメッセージング プロトコルです。ARP と同じように、近隣者発見によって動的登録のキャッシュが構築され、管理者は静的な近隣者発見の登録を設定できます。下記の表は従来の IPv4 近隣者メッセージと類似した IPv6 近隣者メッセージおよび機能を示します。

IPv4 と IPv6 の近隣者メッセージ

IPv4 近隣者メッセージ	IPv6 近隣者メッセージ
ARP 要求メッセージ	近隣者要請メッセージ
ARP リレー メッセージ	近隣者広告メッセージ
ARP キャッシュ	近隣者キャッシュ
重複回避用 ARP	重複アドレス検出
ルータ要請メッセージ (オプション)	ルータ要請 (必須)
ルータ広告メッセージ (オプション)	ルータ広告 (必須)
リダイレクト メッセージ	リダイレクト メッセージ

静的 NDP 機能により、レイヤ 3 IPv6 アドレスとレイヤ 2 MAC アドレスとの間に静的割付を作成できます。

静的NDP 登録を設定するには、以下の手順を実行します。

1 「**管理 | システム セットアップ | ネットワーク > 近隣者発見**」に移動します。

2 「**追加**」を選択します。

3 「**IP アドレス**」フィールドに、リモート機器の IPv6 アドレスを入力します。

4 「**インターフェース**」ドロップダウン メニューから、この登録で使用するファイアウォール上のインターフェースを選択します。

5 「**MAC アドレス**」フィールドに、リモート機器の MAC アドレスを入力します。

6 「**OK**」を選択します。静的 NDP 登録が追加されます。

NDP キャッシュ テーブルに、現在のすべての IPv6 近隣者が表示されます。以下の種別の近隣者が表示されます。

- REACHABLE - 近隣者は 30 秒以内で到達可能であると認識されています。
- STALE - 近隣者は既に到達可能であると認識されていなく、その近隣者に 1200 秒以内にトラフィックが送信されています。
- STATIC - 近隣者は静的近隣者として手動で設定されました。

DHCPv6 の設定

DHCPv6 サーバは、「**管理 | システム セットアップ | ネットワーク > DNS**」の「**表示する IP バージョン**」で「**IPv6**」を選択した後に IPv4 と同様に設定できます。

IPv6 アクセス ルールの設定

IPv6 アクセス ルールは、IPv4 アドレス オブジェクトの代わりに IPv6 アドレス オブジェクトを選択することで、IPv4 アクセスと同様の方法で設定できます。ファイアウォール アクセス ルールの詳細については、『*SonicOS ポリシー*』を参照してください。

IPv6 アクセス ルールを追加する際、送信元および送信先には IPv6 アドレス オブジェクトのみ使用できます。

IPv6 の詳細なファイアウォール設定

パケット制限やトラフィック制限などの IPv6 の詳細なファイアウォール設定は、「**管理 | セキュリティ設定 | ファイアウォール設定 | 詳細設定**」で設定できます。ファイアウォールの詳細設定については、『*SonicOS セキュリティ設定*』を参照してください。

IPv6 IPSec VPN の設定

IPv6 に対する IPSec VPN は、「**管理 | 接続性 | VPN | 設定**」の左上にある「**表示する IP バージョン**」で「**IPv6**」を選択した後、IPv4 VPN と同様の方法で設定できます。VPN の設定については、『*SonicOS 接続*』を参照してください。

現在 IPv6 でサポートされていない特定の VPN 機能があります。

- IKEv2 はサポートされていますが、JKE は現在サポートされていません。
- GroupVPN はサポートされていません。
- VPN を越えた DHCP はサポートされていません。

IPv6 VPN ポリシーを設定する際には、ダイアログの「**一般**」で、IPv6 アドレスを使用してゲートウェイを設定する必要があります。FQDN はサポートされていません。IKE 認証の設定時には、ローカルおよびピアの IKE ID に IPv6 アドレスを使用できます。

VPN ポリシーの「**ネットワーク**」では、IPV6 アドレス オブジェクト (または IPv6 アドレス オブジェクトを含むアドレス グループ) を「**ローカル ネットワーク**」および「**リモート ネットワーク**」で選択する必要があります。

VPN を越えた DHCP はサポートされていません。そのため、保護されたネットワーク用の DHCP オプションは使用できません。

「**ローカル ネットワーク**」の「**すべてのアドレス**」オプションと、「**リモート ネットワーク**」の「**強制トンネル**」オプションは削除されました。すべて 0 の IPv6 ネットワーク アドレス オブジェクトを同じ機能や動作に対して選択できます。

「**プロポーザル**」での設定は、IPv6 のみが **IKEv2 モード**をサポートしている点を除き、IPv6 と IPv4 で同じです。

「**詳細**」では、「**キープ アライブを有効にする**」と「**IKEv2 設定**」のみを IPv6 VPN ポリシーに対して設定できます。

メモ：インターフェースは複数の IPv6 アドレスを持つことができるので、トンネルのローカルアドレスは定期的に変化することがあります。ユーザが一貫性のある IP アドレスを必要としている場合は、ゾーンではなくインターフェースにバインドされるように VPN ポリシーを設定し、アドレスを手動で指定します。このアドレスは、そのインターフェースに対する IPv6 アドレスの 1 つでなければなりません。

IPv6 の SSL VPN 設定

SonicOS は IPv6 アドレスによるユーザ向けの NetExtender 接続をサポートしています。「**管理 | 接続 | SSL VPN | クライアント設定**」で、まず従来の IPv6 IP アドレス プールを設定し、次に IPv6 IP プールを設定します。クライアントには、IPv4 と IPv6 の 2 つの内部アドレスが割り当てられます。SSL VPN の設定の詳細については、『*SonicOS 6.5 接続*』を参照してください。

「**管理 | 接続性 | SSL VPN | クライアント設定**」の「**デバイス プロファイルの編集**」ダイアログで、事前定義されたすべての IPv6 アドレス オブジェクトを含むすべてのアドレス オブジェクトからクライアント ルートを選択できます。

メモ：IPv6 FQDN がサポートされています。

IPv6 可視化

AppFlow 報告およびライブ監視のための IPv6 可視化は、IPv4 可視化を拡張したものであり、管理インターフェースにおけるインターフェース/アプリケーションの速度のリアルタイム監視とセッションの可視化を実現します。組織内外へ送信されるコンテンツを管理するために、従業員がどのウェブサイトにアクセスしているか、ネットワーク内でどのアプリケーションとサービスが、どのような範囲で使用されているかを確認できます。これらの可視化ツールの詳細については、『*SonicOS 6.5 調査*』と『*SonicOS 6.5 監視*』をそれぞれ参照してください。

IPv6 可視化機能の制限

IPv6 の可視化には、次に示す機能上の制限があります。

- IPv6 の URL 格付けはサポートされていません。CFS は IPv6 のすべての面をサポートしているわけではないからです。
- IPv6 の国情報はサポートされていません。
- IPv6 の外部報告はサポートされていません。

IPv6 可視化の設定

AppFlow 監視およびライブ監視の可視化の設定は、IPv6 や IPv4 の場合と同じです。これらの可視化ツールの詳細については、『*SonicOS 調査*』と『*SonicOS 監視*』をそれぞれ参照してください。

IPv6 高可用性監視

IPv6 の高可用性 (HA) 監視は、IPv4 での HA 監視の拡張版として実装されています。IPv6 に対する HA 監視を設定した後は、プライマリとバックアップの両方の装置を IPv6 監視アドレスから管理でき、IPv6 監視によって HA ペアのネットワーク状況を検出できます。

「**管理 | システム セットアップ | 高可用性 > 監視設定**」で、IPv6 と IPv4 を交互に切り替えて表示すれば双方の IP バージョンを簡単に設定できます。

トピック:

- IPv6 高可用性監視機能の制限 (1012 ページ)
- IPv6 高可用性監視 (1012 ページ)
- IPv6 高可用性監視の設定 (1013 ページ)

IPv6 高可用性監視機能の制限

IPv6 HA 監視機能の制限は次のとおりです。

- IPv6 HA 監視の設定ページでは「物理リンク監視」プロパティを変更できません。このプロパティは IPv4 の HA 監視設定ページで設定します。
- IPv6 HA 監視の設定ページでは「仮想 MAC の上書き」プロパティを変更できません。このプロパティは IPv4 の HA 監視設定ページで設定します。
- HA 監視は IPv4 と IPv6 の両方で同時には有効にできません。つまり、IPv4 の監視が有効になっている場合は IPv6 の監視を無効にする必要があり、その逆もまた同様です。

IPv6 高可用性監視

ICMPv6 パケットは、IPv6 アドレスを監視するためにプライマリとバックアップの各装置から定期的に送信され、監視対象 IPv6 アドレスからの応答が監視されます。監視対象 IPv6 アドレスにアクティブなセキュリティ装置が到達できず、アイドル状態のセキュリティ装置が到達できる場合は、このバックアップのセキュリティ装置のほうがネットワーク状況が良いのでフェイルオーバーが開始されます。

IPv6 HA 監視では、IPv6 アドレス、ICMPv6 エコー要求、および ICMPv6 エコー応答が使用されます。プライマリとバックアップの各装置のネットワーク状況の判断に使用されるロジックは、IPv4 と IPv6 で同じです。

IPv6 高可用性監視の設定

IPv6 HA 監視の設定ページは、IPv4 のものを継承しているので、設定手順はほとんど同じです。IPv6 を選択するだけです。その後の設定の詳細については、「IPv6 (979 ページ)」を参照してください。

IPv6 HA 監視の設定時には、次の点を考慮します。

- 「**物理リンク監視**」および「**仮想 MAC**」は、レイヤ 2 のプロパティなので、淡色表示になっています。つまり、これらのプロパティは IPv4 と IPv6 の両方で使用されるので、IPv4 監視のページで設定する必要があります。
- プライマリ/バックアップの IPv6 アドレスはインターフェースの同じサブネット内に存在する必要があり、プライマリ/バックアップ セキュリティ装置のグローバル IP またはリンクローカル IP と同じにすることはできません。
- プライマリ/バックアップの監視 IP を :: 以外に設定する場合は、それらを同じにすることはできません。
- 「**管理**」が有効になっている場合は、プライマリ/バックアップの監視 IP を未指定 (::) にはできません。
- プローブ チェックボックスを有効にする場合は、プローブの IP を未指定にすることはできません。

IPv6 の診断と監視

SonicOS では、次のような IPv6 用の診断ツールを重視しています。

- パケット監視 (1013 ページ)
- IPv6 の Ping (1013 ページ)
- IPv6 の DNS 名調査と名前の逆引き (1013 ページ)

パケット監視

「**調査 | ツール | パケット監視**」は IPv6 を完全にサポートしています。さらに、パケット監視のフィルタには IPv6 キーワードを使用できます。パケット監視の詳細については、『*SonicOS 調査*』を参照してください。

IPv6 の Ping

ドメイン名を Ping すると、最初に返された IP アドレスを使用して実際の Ping の送信元アドレスが表示されます。IPv4 と IPv6 の両方のアドレスが返された場合、既定ではセキュリティ装置によって IPv4 アドレスに対する Ping が実行されます。Ping ツールには「**IPv6 ネットワーク優先**」オプションが含まれており、これが有効になっていると、セキュリティ装置は IPv6 アドレスに対する Ping を行います。IPv6 への Ping の詳細については、『*SonicOS 調査*』を参照してください。

IPv6 の DNS 名調査と名前の逆引き

IPv6 の DNS 名調査または名前の逆引きの実行時には、DNS サーバアドレスを入力する必要があります。IPv6 と IPv4 のどちらのアドレスでも使用できます。これらのツールの詳細については、『*SonicOS 調査*』を参照してください。

C

BGP の高度なルーティング

トピック:

- BGP の高度なルーティング (1014 ページ)
  - BGP について (1014 ページ)
  - 注意 (1022 ページ)
  - BGP の設定 (1023 ページ)
  - BGP 設定の確認 (1033 ページ)
  - Ipv6 BGP (1036 ページ)

BGP の高度なルーティング

この付録では、SonicWall における BGP (Border Gateway プロトコル) の実装の概要と、BGP の動作、およびネットワークに合わせて BGP を設定する方法を説明します。

メモ：BGP は、TZ シリーズ装置で SonicOS 拡張のライセンスを購入するとサポートされます。SOHO 無線装置では BGP はサポートされません。

トピック:

- BGP について (1014 ページ)
- 注意 (1022 ページ)
- BGP の設定 (1023 ページ)
- BGP 設定の確認 (1033 ページ)
- Ipv6 BGP (1036 ページ)

BGP について

トピック:

- BGP とは (1015 ページ)
- 背景情報 (1015 ページ)
- 自律システム (1016 ページ)
- VPN トンネル インターフェース経由の BGP (1017 ページ)
- BGP を使用する理由 (1017 ページ)

- BGP の動作 (1018 ページ)
- BGP の用語 (1021 ページ)

BGP とは

BGP は、明確に定義され、個別に管理されるネットワーク ドメインである自律システム (AS) 間でルーティング情報を伝達するために使用される、大規模ルーティング プロトコルです。BGP サポートは、SonicWall セキュリティ装置がネットワークの AS の端点にある従来の BGP ルータの代わりをすることを考慮しています。現在の SonicWall の BGP 実装は、ネットワークが 1 つの ISP をインターネット プロバイダとして使い、そのプロバイダへの接続が 1 つだけのシングルプロバイダ/シングルホーム環境に対して最も適しています。SonicWall BGP はまた、ネットワークが 1 つの ISP を使っているが、そのプロバイダへの少数の異なるルートがあるシングルプロバイダ/マルチホーム環境のサポートも可能です。BGP は、SonicOS 管理インターフェースの「**ネットワーク > ルーティング**」ページで有効にしてから、SonicOS のコマンド ライン インターフェース (CLI、『*SonicOS CLI リファレンス ガイド*』を参照) を通じて完全に設定します。

「BGP ライセンス要件」テーブルに BGP ライセンス要件を示します。

BGP ライセンス要件

プラットフォーム	必要な追加ライセンス
SM 9600	なし (BGP のライセンスは含まれています)
SM 9400	なし (BGP のライセンスは含まれています)
SM 9200	なし (BGP のライセンスは含まれています)
NSA 6600	なし (BGP のライセンスは含まれています)
NSA 5600	なし (BGP のライセンスは含まれています)
NSA 4600	なし (BGP のライセンスは含まれています)
NSA 3600	SonicOS 拡張のライセンス 01-SSC-7091
NSA 2650	SonicOS 拡張のライセンス
NSA 2600	SonicOS 拡張のライセンス
TZ600	SonicOS 拡張のライセンス
TZ500/TZ500 W	SonicOS 拡張のライセンス
TZ400/TZ400 W	SonicOS 拡張のライセンス
TZ350/TZ350W	該当なし
TZ300/TZ300 W	該当なし
SOHO 250/250 W/SOHO W	該当なし

メモ：ライセンスは www.MySonicWall.com で購入できます。

背景情報

ルーティング プロトコルは、単にネットワーク上を伝送されるパケットではなく、個々のルータおよびルータ グループがネットワーク トポロジを検出し、まとめ、伝達するすべてのメカニズムで構成されます。ルーティング プロトコルは、指定されたとおりにそのプロトコルに従う各構成要素に応じて、異なる分散アルゴリズムを使用します。また、あるネットワーク ドメイン内のルートが、ネットワーク ノード間のリンクの状況の変化に合わせて動的に変化する場合に、最も役立ちます。

通常、ルーティング プロトコルは次の 2 つのデータベースとやりとりを行います。

- **Routing Information Base (RIB)** - ルーティング プロトコル自体が必要とするすべてのルート情報を保存するために使用されます。
- **Forward Information Base (FIB)** - 実際のパケット転送に使用されます。

RIB から選択される最適ルートを使用して、FIB が設定されます。各ルーティング プロトコルがルーティングの更新を受信すると、あるいは機器の接続が変更されると、RIB と FIB の両方が動的に変化します。

ルーティング プロトコルには次の 2 つの基本クラスがあります。

- **内部ゲートウェイ プロトコル (IGP)** - 内部ゲートウェイ プロトコルは、1 つの AS の内部に存在するネットワーク内でルートを伝達するためのルーティング プロトコルです。IGP には 2 つの世代があります。第 1 世代は、距離ベクトル プロトコルで構成されています。第 2 世代は、リンク状態プロトコルで構成されています。距離ベクトル プロトコルは比較的単純ですが、多数のルータにスケーリングすると問題が発生します。リンク状態プロトコルはより複雑ですが、スケーリング機能に優れています。既存の距離ベクトル プロトコルは、内部ゲートウェイ ルーティング プロトコル (IGRP)、拡張内部ゲートウェイ ルーティング プロトコル (EIGRP)、ルーティング情報プロトコル (RIP)、および RIP の拡張バージョンである RIPv2 です。IGRP と EIGRP は、Cisco の独自仕様プロトコルです。現在使用されているリンク状態プロトコルは、オープン ショーテスト パス ファースト (OSPF) と、あまり使われていない中間システム間連携 (IS-IS) プロトコルです。

  SonicOS は、ルーティングの最も一般的な内部ゲートウェイ プロトコルである OSPFv2 と RIPv1/v2 プロトコルの 2 つをサポートして、顧客が SonicWall 製品を IGP ネットワークで利用できるようにすると共に、従来のルータを別個に導入する追加コストを不要にしています。

- **外部ゲートウェイ プロトコル (EGP)** - 標準のユビキタスな外部ゲートウェイ プロトコルは、BGP (正確には BGP4) です。BGP は、自律システム (AS) と呼ばれる明確に定義されたネットワーク ドメイン間でルーティング情報とポリシーを伝達する、大規模ルーティング プロトコルです。自律システムは、他の自律システムから独立して、個別に管理されるネットワーク ドメインです。BGP は、自律システム間でのルートおよびルート ポリシーの変換に使用されます。一般的に、ISP は BGP を利用して、顧客や他の ISP とのルートおよびルート ポリシーを変換します。

  各自律システムには、16 ビットの番号が割り当てられています。IP アドレスと同様に、AS 番号はパブリックまたはプライベートです。パブリック AS 番号は限定的なリソースで、要素の数に基づいて配布されます。通常、大規模ネットワークを 2 つ以上の ISP にマルチホーム化している ISP 顧客はパブリック AS を持ちますが、より小規模な顧客は、ISP プロバイダが管理するプライベート AS を与えられます。

  SonicWall 製品がエンタープライズレベルの要件をサポートするようになったのに伴い、SonicWall 製品を従来の BGP ルータの代わりに AS のエッジに配置したいと考える顧客もいます。

自律システム

各自律システムには、16 ビットの番号が割り当てられています。IP アドレスと同様に、AS 番号はパブリックまたはプライベートです。パブリック AS 番号は限定的なリソースで、要素の数に基づいて配布されます。通常、大規模ネットワークを 2 つ以上の ISP にマルチホーム化している ISP 顧客はパブリック AS を持ちますが、より小規模な顧客は、ISP プロバイダが管理するプライベート AS を与えられます。

BGP トポロジの種類

BGP は、非常に柔軟で複雑なルーティング プロトコルです。そのため、BGP ルータは、インターネット コア ルータ、中間 ISP ルータ、ISP 顧客構内設備 (CPE)、または小規模プライベート BGP ネットワーク内のルータなど、さまざまなトポロジ設定に配置できます。さまざまなトポロジに必要な BGP ルートの数は、コア ルータの 300,000 以上から、単一 ISP を使用し、AS 外部のすべての宛先に既定のルーティングを利用する ISP 顧客の 0 まで大きく異なります。一般に、ISP 顧客は、ISP から受信するルートの数にかかわらず、エッジ ルータ (CPE) から ISP に対して BGP を実行する必要があります。これによって、ISP 顧客は外部にどのネットワークを通知するかを制御できます。顧客が自身で所有していないネットワークまたはネットワーク統合を通知し、インターネット トラフィックがそのネットワークにブラックホールのように吸い込まれるというおそれは常にあります。実際には、ISP プロバイダは顧客からの不正な通知を注意深くフィルタリングしているので (BGP の強みの 1 つです)、このようなことはほとんど起こりません。

BGP ネットワークには、3 つの基本区分があります。

- **シングルプロバイダ/シングルホーム** - ネットワークは単一の ISP (シングルプロバイダ) から単一のルート (シングルホーム) を受信します。ISP 顧客が ISP から受信するルートの数は、AS の性質によって異なります。インターネット プロバイダとして ISP を 1 つだけ使用し、そのプロバイダに対して単一の接続を持つ (シングルプロバイダ/シングルホーム) ISP 顧客は、ルートを受信する必要がありません。AS 外部宛てのすべてのトラフィックは、ISP に送信されます。このような顧客は、内部ネットワークの一部またはすべてを引き続き ISP に通知することも可能です。
- **シングルプロバイダ/マルチホーム** - ネットワークは単一の ISP (シングルプロバイダ) から複数のルート (マルチホーム) を受信します。単一の ISP を利用しているが、その ISP に対して複数の接続を持つ ISP 顧客は、各 ISP ゲートウェイで既定のルート (0.0.0.0/0) のみを受信できます。1 つの ISP 接続がダウンした場合、接続されている CPE ルータから内部ルータに送信された通知済みの既定のルートが取り消され、インターネット トラフィックは ISP への接続を持つ CPE ルータに流れるようになります。顧客への特定の接続がダウンした場合、顧客の内部ネットワークも各 CPE ルータ ゲートウェイで ISP に通知され、ISP は代替パスを使用できるようになります。
- **マルチプロバイダ/マルチホーム** - 複数の ISP を使用する (マルチプロバイダ/マルチホーム) ISP 顧客には、ISP ごとに 1 つ以上の個別のゲートウェイ ルータがあります。この場合、顧客の AS はパブリック AS でなければなりません。また、トランジット AS あるいは非トランジット AS のどちらでも構いません。トランジット AS は、別の ISP から到達可能なネットワークを宛先とするトラフィックを、ある ISP から受信し、転送します (トラフィックの宛先は顧客の AS 内ではありません)。非トランジット AS は、その AS を宛先とするトラフィックのみを受信します。その他のトラフィックはすべて破棄されます。一般に、トランジット AS 内の BGP ルータは、各 ISP から完全 BGP ルート テーブルの大部分 (多くの場合はすべて) を受信します。

VPN トンネル インターフェース経由の BGP

BGP インターフェースは、番号付けされたトンネル インターフェースと番号付けされていないトンネル インターフェースの両方をサポートしています。この機能は、BGP と番号付けされていないトンネル インターフェースを設定できるすべてのプラットフォームでサポートされています。

BGP を使用する理由

- インターネット上の大規模ネットワーク以外でも、BGP はマルチホーム、負荷分散、および冗長性の標準です。

- **シングルプロバイダ/シングルホーム** - 一般的には BGP の有力候補ではありませんが、BGP を使用すると ISP にネットワークを通知できます。シングルホーム ネットワークは RIR からパブリック AS を取得できません。
- **シングルプロバイダ/マルチホーム** - 一般的に、RFC2270 の提案に従って、単一のプライベート AS (64512 ～ 65535) を使用して BGP のメリットを得つつ、パブリック ASN を維持するのに使用されます。
- **マルチプロバイダ/マルチホーム** - 冗長性が高く、一般的には各 ISP に対して専用ルータを使用します。パブリック ASN が必要です。大量のメモリ フットプリントを使用します。

- ルートの要約によってルーティングがスケーラブルになります。

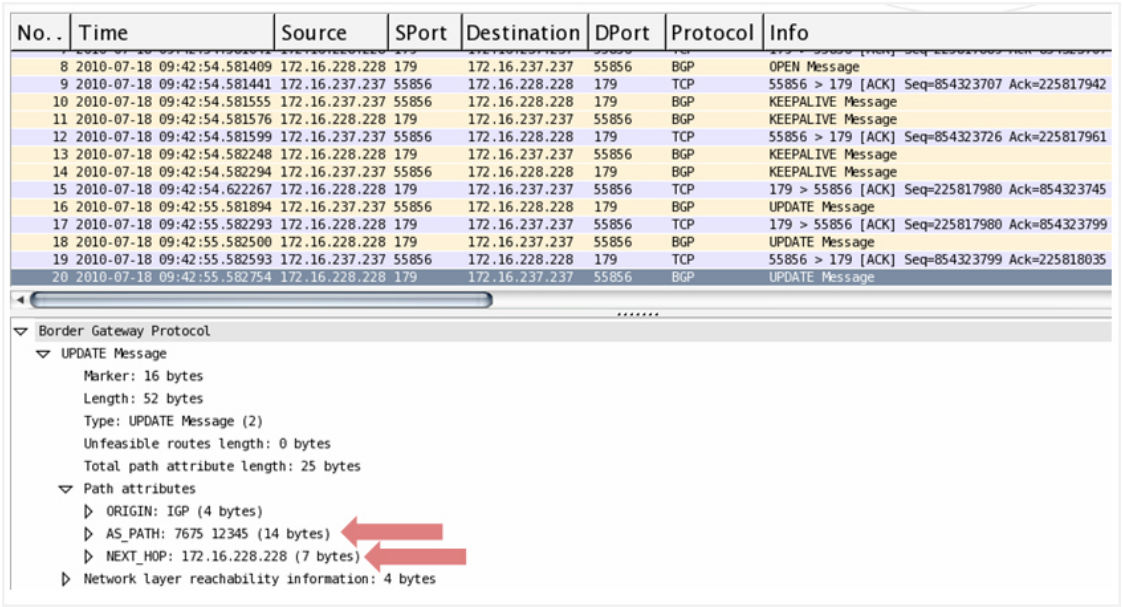
BGP の動作

BGP は、TCP ポート 179 を通信に使用します。BGP は、宛先に対するエンドツーエンドのパス記述を含む、パスベクトル プロトコルと見なされます。BGP 近隣は、内部 (iBGP) または外部 (eBGP) のどちらかにすることができます。

- **iBGP** - 近隣者は同一 AS 内に存在します。
- **eBGP** - 近隣者は別の AS 内に存在します。

パスは、さまざまなパス属性でタグ付けされた UPDATE メッセージで通知されます。AS_PATH と NEXT_HOP は、BGP UPDATE メッセージでルートのパスを記述する、最も重要な 2 つの属性です。

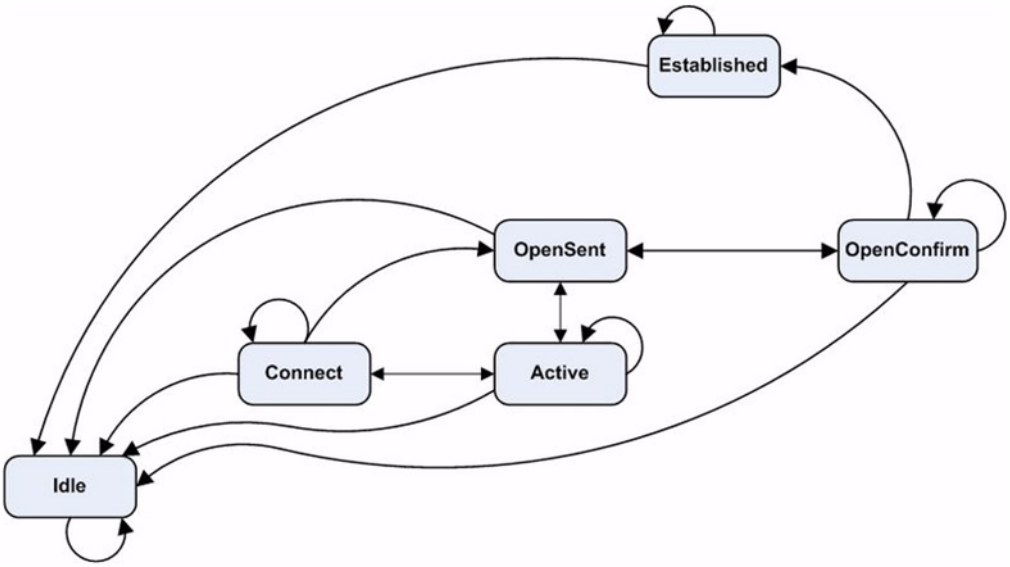
- **AS_PATH**: ルートの送信元と送信先の AS を示します。以下の例では、AS_PATH は AS 7675 から AS 12345 宛てです。内部 BGP の場合、AS_PATH は送信元と送信先の両方に同一 AS を指定します。
- **NEXT_HOP**: パスが到達する次のルータの IP アドレスを示します。AS 境界を越えて通知されるパスは、境界ルータの NEXT_HOP アドレスを継承します。BGP は、内部ルーティング プロトコルを使用して NEXT_HOP アドレスに到達します。



BGP の有限状態機械

BGP を定義した RFC 1771 には、以下の状態機械に関する BGP の動作が記述されています。図の下の表に、さまざまな状態に関する追加情報を示します。

BGP の有限状態機械



BGP の有限状態の説明

状態	説明
Idle	新しい BGP セッション確立後、または既存セッションのリセット後、Start イベントを待機中。エラーが発生した場合は、Idle 状態に戻ります。Start イベント後、BGP は初期化を行い、接続リトライ タイマーをリセットし、TCP 転送接続を開始し、接続をリッスンします。
Connect	TCP 層が使用可能になると、OpenSent に遷移し、OPEN を送信します。TCP 層が存在しない場合は、Active に遷移します。接続リトライ タイマーが期限切れになった場合は、Connect のままで、タイマーをリセットし、転送接続を開始します。それ以外の場合は、Idle に戻ります。
Active	ピアとの TCP 接続の確立を試みます。成功した場合は、OpenSent に遷移し、OPEN を送信します。接続リトライが期限切れになった場合は、タイマーを再起動し、Connect に戻ります。また、別のピアによって接続をアクティブにリッスンします。その他のイベントが発生した場合は、Idle に戻ります。 Connect から Active へのフラッピングは、TCP の再送やピアの到達不可能性など、TCP 転送の問題があることを示します。
OpenSent	ピアからの OPEN メッセージを待機中。受信時に検証を行います。検証が失敗した場合は、NOTIFICATION を送信し、Idle に戻ります。成功した場合は、KEEPALIVE を送信し、キープアライブ タイマーをリセットします。保留時間をネゴシエートします。小さい値の方が採用されます。ゼロの場合は、保留タイマーとキープアライブ タイマーは再起動されません。

BGP の有限状態の説明 (続き)

状態	説明
OpenConfirm	KEEPALIVE または NOTIFICATION を待機します。KEEPALIVE を受信した場合は、Established に遷移します。UPDATE または KEEPALIVE を受信した場合は、保留タイマーを再起動します (ネゴシエートされた保留時間がゼロの場合を除く)。NOTIFICATION を受信した場合は、Idle に遷移します。 定期的な KEEPALIVE メッセージが送信されます。TCP 層が遮断された場合は、Idle に遷移します。エラーが発生した場合は、エラー コードを含む NOTIFICATION を送信し、Idle に遷移します。
Established	セッションが使用可能になり、交換がピアで更新されます。NOTIFICATION を受信した場合は、Idle に遷移します。更新にエラーがないかチェックします。エラーがあった場合は、NOTIFICATION を送信し、Idle に遷移します。保留時間が期限切れになった場合は、TCP を切断します。

BGP メッセージ

BGP 通信には、以下の種類のメッセージが含まれます。

- **Open** - TCP セッション確立後、BGP ピア間の最初のメッセージ。ASN、保留時間、およびマルチプロダクト拡張やルートリフレッシュ機能など、ピアリング セッションの確立に必要な情報が含まれます。
- **Update** - このメッセージには、ルートの告知または取り消しなどのパス情報が含まれます。
- **Keepalive** - TCP 層を使用可能な状態に保ち続け、生存性を通知するための定期的メッセージ。
- **Notification** - BGP セッションを終了させるための要求。致命的ではない通知には、エラー コード "cease" が含まれます。サブコードは、「通知のサブコード」テーブルに示すように、さらに詳しい情報を提供します。

  通知のサブコード

サブコード	説明
1 - 到達したプレフィックスの最大数	設定されている "近隣の最大プレフィックス" 値を超えました
2 - 管理上のシャットダウン	セッションが管理上シャットダウンされました
3 - ピア未設定	ピアの設定が削除されました
4 - 管理上のリセット	セッションが管理上リセットされました
5 - 接続拒否	BGP セッションの拒否 (一時的な場合もあります)
6 - その他の設定変更	何らかの理由でセッションが管理上リセットされました

- **ルートリフレッシュ** - ピアに対するルート再送の要求。

BGP 属性

BGP の UPDATE メッセージには、「BGP の UPDATE メッセージの属性」テーブルに示すような属性を含めることができます。

BGP の UPDATE メッセージの属性

値	コード
1	ORIGIN
2	AS_PATH
3	NEXT_HOP
4	MULTI_EXIT_DISC
5	LOCAL_PREF
6	ATOMIC_AGGREGATE
7	AGGREGATOR
8	COMMUNITY
9	ORIGINATOR_ID
10	CLUSTER_LIST
11	DPA
12	ADVERTISER (履歴)
13	RCID_PATH / CLUSTER_ID (履歴)
14	MP_REACH_NLRI
15	MP_UNREACH_NLRI
16	EXTENDED COMMUNITIES
17	AS4_PATH
18	AS4_AGGREGATOR
19	SAFI 固有属性 (SSA) (廃止)
20	コネクタ属性 (廃止)
21	AS_PATHLIMIT (廃止)
22	PMSI_TUNNEL
23	トンネル カプセル化属性
24	トラフィック エンジニアリング
25	IPv6 アドレス固有の拡張コミュニティ
26	AIGP (一時的 - 2011 年 2 月 23 日に失効)
27 ～ 254	未定義
255	開発用に確保

BGP 属性の詳細については、次のリンクを参照してください:
http://www.iana.org/assignments/bgp-parameters/bgp-parameters.xml

BGP の用語

ARD	自律ルーティング ドメイン - 共通の管理ルーティング ポリシーを持つネットワーク/ルータの集まり。
AS	自律システム - 識別番号が割り当てられ、一般的には境界ルータで BGP4 を実行している ARD。
BGP4	ボーダー ゲートウェイ プロトコル 4最も一般的な EGP。

CIDR	Classless Inter-Domain Routing。ルート統合を通じて効率的なルート通知を可能にします。
CPE	顧客構内設備 - 顧客のネットワークのエッジにあり、ISP とのやりとりに使用される機器。
EGP	外部ゲートウェイ プロトコル - 自律システム間でのルーティング情報の伝達に使用される任意のプロトコル (実際には BGP4)。
完全ルート	グローバル BGP ルート テーブル全体。
FIB	Forwarding Information Base - SonicWall の既存のルート テーブルで、パケットの転送時に送信インターフェースとネクスト ホップを探すために使用されます。
Looking Glass*	Looking Glass (LG) サーバは、LG サーバを実行している組織のルータに関する読み取り専用ビューです。一般的に、公的にアクセス可能な Looking Glass サーバは、ISP または NOC によって実行されます。
マルチホーム	1 つ以上の ISP に対して複数の接続を持つ ISP 顧客。
マルチプロバイダ	複数の ISP を利用してインターネットに接続する ISP 顧客。
NSM	ネットワーク サービス モジュール - FIB および RIB へのインターフェースを一元管理する ZebOS のコンポーネン。個々のルーティング プロトコル デーモンは、すべての RIB 更新について NSM とやりとりを行います。NSM は、RIB からの最適ルート情報でのみ FIB を更新します。
部分ルート	完全 BGP ルート テーブルの一部で、通常は ISP のドメインの一部である宛先に固有です。
RIB	Route Information Base - NSM が所有する実行時データベースで、収集されたすべてのルート情報の保存に使用され、ルーティング プロトコルによって使用されます。

注意

縮尺	現在、SonicOS では 512 ～ 2,048 のポリシーベース ルート (PBR) をサポートしています。これは、ルーティング テーブル全体に対して、あるいはルーティング テーブルの一部に対しても、十分ではありません。RIB に存在するルートの数は、(FIB である) PBR にインストールされている数より多い場合があります。複数の競合するルートをルーティング プロトコルから受信している場合は、このような状況が発生します。特定のネットワーク宛先への競合するルートが RIB に含まれているケースごとに、それらのルートから 1 つだけ選択して、FIB にインストールしてください。 現在、SonicWall の実装は、シングルプロバイダ/シングルホームの顧客に最も適しています。シングルプロバイダ/マルチホーム インストールは、既定のルートを ISP から受信している場合や、きわめて少数の ISP 固有のルートを顧客が受信する場合にも適しています。後者の場合には、内部ルータが、ISP のネットワーク ドメイン内ではあるが AS の外部にある宛先への最適パスを選択できます (これは部分ルートと呼ばれます)。
負荷分散	現在、SonicOS または Zebos でマルチパス (「最大パス」機能) はサポートされていません。したがって、ネットワークを分割しなければ負荷分散を行えません。
ループバック	現在、ループバック インターフェースはサポートされていません。
NAT	BGP はルーティング用です。NAT とはうまく共存できません。
非対称パス	現在、ステートフル セキュリティ装置は非対称パスを処理しません (特に複数のセキュリティ装置を越える場合)。

BGP の設定

トピック:

- BGP の IPSec 設定 (1023 ページ)
- BGP の基本設定 (1024 ページ)
- BGP パス選択プロセス (1025 ページ)
- AS_PATH プリペンド (1028 ページ)
- Multiple Exit Discriminator (MED) (1029 ページ)
- BGP コミュニティ (1030 ページ)
- 同期と自動要約 (1031 ページ)
- 偶発的なトランジット AS の防止 (1031 ページ)
- 負荷共有のためのマルチホーム BGP の使用 (1033 ページ)

BGP の IPSec 設定

BGP は、パケットを平文で送信します。したがって、セキュリティを強化するため、BGP セッションに使用する IPSec トンネルを設定することをお勧めします。IPSec トンネルと BGP の設定は、互いに独立しています。BGP 用 IPSec トンネルの設定については、『*SonicOS 接続*』を参照してください。

BGP 用 IPSec トンネルを設定するには、以下の手順に従います。

1 IPSec トンネルは、SonicOS 管理インターフェースの「**管理 | 接続性 | VPN**」設定セクションで完全に設定できます。IPSec トンネルの設定時には、以下のオプションが設定されていることを確認します。

オプション	値
ポリシー種別	**サイト間** **メモ：** IPSec 経由の BGP には、サイト間 VPN トンネルを使用する必要があります。
プライマリ IPSec ゲートウェイ名またはアドレス	リモート ピアの IP アドレス
ローカル IKE ID	SonicWall セキュリティ装置の IP アドレスに移動します。
ピア IKE ID	リモート ピアの IP アドレス
**ネットワーク	対象先ネットワークをリストより選択**	リモート ピアの IP アドレス
**詳細	キープ アライブを有効にする**	有効

重要：IPSec 経由の BGP の設定時には、以下の手順に従います。

1 IPSec トンネルを設定します。

2 BGP を設定する前に、トンネル経由での接続を確認します。

メモ：VPN ポリシーの設定方法については、『*SonicOS 接続*』を参照してください。

2 「**管理 | システム セットアップ | ネットワーク > ルーティング**」ページで、ルート ポリシーの追加時に「**サービス**」オプションで「**BGP**」を選択して、BGP を有効にします。ルート ポリシーの追加方法については、「BGP の高度なルーティングの設定 (528 ページ)」を参照してください。BGP の基本設定については、「BGP の基本設定 (1024 ページ)」を参照してください。

3 SonicOS コマンド ライン インターフェースによるルートの設定を終了します。SonicOS CLI については、『*SonicOS コマンドライン インターフェース ガイド*』を参照してください。

4 セキュリティ装置で VPN ポリシーを設定したら、リモート ピアでの対応する IPSec 設定を行います。

5 リモート ピアでの IPSec 設定が完了したら、「**管理 | 接続性 | VPN | 基本設定**」に戻り、IPSec トンネルを初期化するために VPN ポリシーを有効にします。

6 SonicWall セキュリティ装置の Ping 診断を使用して BGP ピアの IP アドレスに Ping を行います。Ping 診断の詳細については、『*SonicOS 調査*』を参照してください。

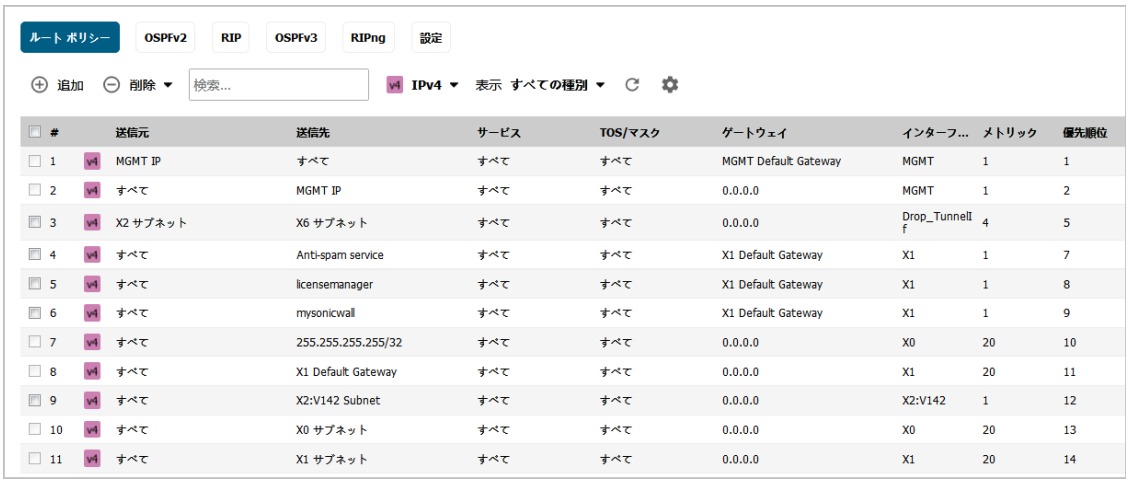
7 Wireshark を使用して要求と応答が ESP パケットにカプセル化されていることを確認します。

メモ：この例の設定では、ルーティングされたトラフィックは BGP 用の IPSec トンネルを通りません。ルーティングされたトラフィックは、平文で送受信されます。ルーティングされたすべてのネットワーク トラフィックではなく BGP を保護することが目的なので、ほとんどの場合、これが望ましい動作です。

BGP の基本設定

SonicWall セキュリティ装置上で BGP を設定するには、以下の手順に従います。

1 「**管理 | システム セットアップ | ネットワーク > ルーティング**」に移動します。

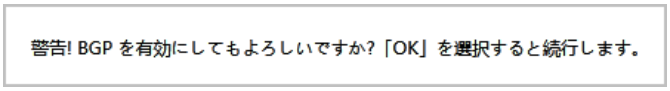


#	送信元	送信先	サービス	TOS/マスク	ゲートウェイ	インターフ...	メトリック	優先順位
1	MGMT IP	すべて	すべて	すべて	MGMT Default Gateway	MGMT	1	1
2	すべて	MGMT IP	すべて	すべて	0.0.0.0	MGMT	1	2
3	X2 サブネット	X6 サブネット	すべて	すべて	0.0.0.0	Drop_TunnelIf	4	5
4	すべて	Anti-spam service	すべて	すべて	X1 Default Gateway	X1	1	7
5	すべて	licensemanager	すべて	すべて	X1 Default Gateway	X1	1	8
6	すべて	mysonicwall	すべて	すべて	X1 Default Gateway	X1	1	9
7	すべて	255.255.255.255/32	すべて	すべて	0.0.0.0	X0	20	10
8	すべて	X1 Default Gateway	すべて	すべて	0.0.0.0	X1	20	11
9	すべて	X2:V142 Subnet	すべて	すべて	0.0.0.0	X2:V142	1	12
10	すべて	X0 サブネット	すべて	すべて	0.0.0.0	X0	20	13
11	すべて	X1 サブネット	すべて	すべて	0.0.0.0	X1	20	14

2 「**設定**」を選択します。

3 「**ルーティング モード**」で、「**高度なルーティング**」を選択します。

4 「**BGP**」で、「**有効 (CLI での設定)**」を選択します。確認メッセージが表示されます。



メモ：管理インターフェースから BGP が有効になった後、SonicOS のコマンドライン インターフェース (CLI) を使用して、BGP 設定の仕様が実行されます。SonicOS CLI への接続方法の詳細については、『*SonicOS コマンドライン インターフェース ガイド*』を参照してください:

5 コンソール インターフェースから SonicOS CLI にログインします。

6 **configure** コマンドを入力して、設定モードに入ります。

7 **configure routing bgp** コマンドを入力して、BGP CLI に入ります。次のプロンプトが表示されます。

```
ZebOS version 7.7.0 IPIRouter 7/2009

ARS BGP>
```

8 これで、BGP の非設定モードに入りました。**?** と入力すると非設定コマンドの一覧が表示されます。

9 **show running-config** と入力して、現在の BGP 動作設定を確認します。

10 BGP 設定モードに入るには、**configure terminal** コマンドを入力します。設定コマンドの一覧が表示されます。

11 設定が完了したら、**write file** コマンドを入力します。装置が高可用性ペアまたはクラスタの一部である場合は、設定の変更が他の装置に自動的に伝達されます。

BGP パス選択プロセス

「BGP パス選択プロセスの属性」テーブルに、BGP パス選択プロセスの設定に使用する属性を示します。

BGP パス選択プロセスの属性

項目	説明
重み	近隣から取得したルートの中で、最も高い重みが設定されているものが優先されます。ローカル ルータにのみ関係します。
ローカル プリファレンス	管理上、ある近隣から取得したルートが優先されます。AS 全体で共有されます。
ネットワーク または **統合** パス	**network** コマンドおよび **aggregate-address** コマンドからローカルに開始されたパスが優先されます。
AS_PATH	AS_PATH が最も短いパスが優先されます。
起点	(UPDATE メッセージで通知される) 起点タイプが最も低いパスが優先されます。`IGP < EGP < Incomplete` (不完全) の順になります。
Multi Exit Discriminator (MED)	起点 AS へのパスについて、パスのプリファレンス情報を近隣に提供します。
最新性	最近受信したパスが優先されます。
ルータ ID	最も低いルータ ID を持つルータからのパスが優先されます。

重み

weight コマンドは、アドレスファミリごとに 1 つの重み値を、近隣から取得したすべてのルートに割り当てます。複数のピアから同じプレフィックスが取得された場合は、最も高い重みを持つルートが優先されます。重みはローカル ルータにのみ関係します。

set weight コマンドで割り当てられる重みは、このコマンドで割り当てられる重みより優先されます。

ピアグループに対して重みを設定すると、そのピアグループのすべてのメンバーが同じ重みを持ちます。weight コマンドを使用して、特定のピアグループ メンバーに異なる重みを割り当てることもできます。

以下に重み設定の例を示します。

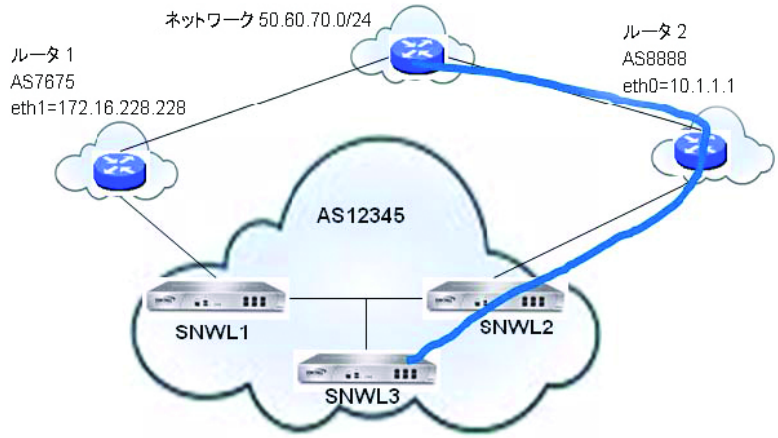
```
router bgp 12345
   neighbor 12.34.5.237 remote-as 12345
   neighbor 12.34.5.237 weight 60


router bgp 12345
   neighbor group1 peer-group
   neighbor 12.34.5.237 peer-group group1
   neighbor 67.78.9.237 peer-group group1
   neighbor group1 weight 60
```

ローカル プリファレンス

ローカル プリファレンス属性は、装置のルーティング テーブルにある各外部ルートの優先度を示すのに使用されます。ローカル プリファレンス属性は、同一 AS 内の機器に送信されるすべての UPDATE メッセージに含まれます。ローカル プリファレンスは、外部 AS には伝達されません。「BGP のローカル プリファレンス トポロジ」は、ローカル プリファレンスが近隣 AS 間のルートにどのように影響を与えるかを説明するトポロジの例を示しています。

BGP のローカル プリファレンス トポロジ



「SNWL1 および SNWL2 の設定」テーブルに示す BGP 設定が SNWL1 および SNWL2 に入力されています。SNWL2 のローカル プリファレンスの方が高いので、SNWL2 が AS 12345 (SonicWall AS) によって外部 AS に通知される優先ルートになります。

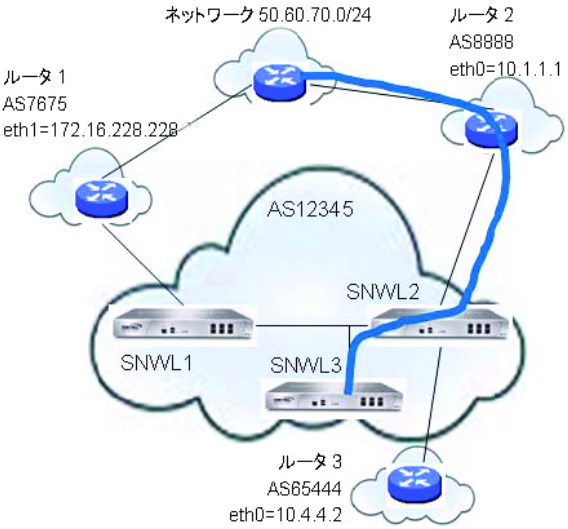
SNWL1 および SNWL2 の設定

SNWL1 の設定	SNWL2 の設定
x0 = 12.34.5.228	x0 = 12.34.5.237
x1 = 172.16.228.45	x1 = 10.1.1.2
----------	----------
router bgp 12345	router bgp 12345
neighbor 172.16.228.228 remote-as 7675	neighbor 10.1.1.1 remote-as 8888
neighbor 12.34.5.237 remote-as 12345	neighbor 12.34.5.228 remote-as 12345
bgp default local-preference 150	bgp default local-preference 200

ルート マップで使用されるローカル プリファレンス

ルート マップはアクセス制御リストに似ています。ルート マップは、装置によるルートの処理方法を決定する一連の許可文や拒否文で構成されます。ルート マップは、送信トラフィックではなく受信トラフィックに適用されます。「ルート マップを使用した BGP ローカル プリファレンス トポロジ」 は、ローカル プリファレンスの設定にルート マップを使用するトポロジの例を示しています。

ルート マップを使用した BGP ローカル プリファレンス トポロジ



「ルート マップを使用した SNWL1 および SNWL2 の設定」テーブルに示す BGP 設定が SNWL1 および SNWL2 に入力されています。

ルート マップを使用した SNWL1 および SNWL2 の設定

SNWL1 の設定	SNWL2 の設定
x1 = 172.16.228.45	x0 = 12.34.5.237 x1 = 10.1.1.2 x4 = 10.4.4.1
----------	----------
router bgp 12345 neighbor 172.16.228.228 remote-as 7675 neighbor 12.34.5.237 remote-as 12345 bgp default local-preference 150	router bgp 12345 neighbor 10.1.1.1 remote-as 9999 neighbor 10.1.1.1 route-map rmap1 in neighbor 12.34.5.237 remote-as 12345 .... ip as-path access-list 100 permit ^8888$ ... route-map rmap1 permit 10 match as-path 100 set local-preference 200 route-map rmap1 permit 20 set local-preference 150

SNWL2 (rmap1) に設定されているルート マップは、近隣 `10.1.1.1` からの受信ルートに適用するように設定されています。次の 2 つの許可条件があります。

- **route-map rmap1 permit 10**: この許可条件は、AS 8888 からのトラフィックを許可し、AS 8888 からのルートをローカル プリファレンス 200 に設定するように構成されているアクセス リスト 100 に一致します。
- **route-map rmap1 permit 10**: この許可条件は、アクセス リスト 100 に一致しないその他すべてのトラフィック (すなわち 8888 以外の AS から受信するトラフィック) をローカル プリファレンス 150 に設定します。

AS_PATH プリペンド

AS_PATH プリペンドは、パス更新の先頭に AS 番号を追加する方法です。これによって、このルートのパスが長くなるため、優先度が低くなります。

AS_PATH プリペンドは、送信パスにも受信パスにも適用できます。近隣によって無効にされる場合、AS_PATH プリペンドが適用されないことがあります。

送信パスと受信パスの設定

送信パスの設定	受信パスの設定
router bgp 12345	router bgp 7675
bgp router-id 10.50.165.233	bgp router-id 10.50.165.228
network 12.34.5.0/24	network 7.6.7.0/24
neighbor 10.50.165.228 remote-as 7675	neighbor 10.50.165.233 remote-as 12345
neighbor 10.50.165.228 route-map long out	neighbor 10.50.165.233 route-map prepend in
!	!
route-map long permit 10	route-map prepend permit 10
set as-path prepend 12345 12345	set as-path prepend 12345 12345

この設定によって、近隣 10.50.165.233 に AS_Path プリペンド 12345 12345 でルートがインストールされます。これは、**show ip bgp** コマンドを入力すると表示されます。

```
ARS BGP>show ip bgp
BGP table version is 98, local router ID is 10.50.165.228
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, l - labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 12.34.5.0/24     10.50.165.233            0             0 12345 12345 12345 i
*> 7.6.7.0/24       0.0.0.0                        100  32768 i
Total number of prefixes 2
```

Multiple Exit Discriminator (MED)

set metric コマンドをルート マップで使用して、パスの優先度を高くしたり、低くしたりできます。

```
router bgp 7675
network 7.6.7.0/24
   neighbor 10.50.165.233 remote-as 12345
   neighbor 10.50.165.233 route-map highmetric out
!
route-map highmetric permit 10
   set metric 300
```

Multi Exit Discriminator (MED) は、パスの優先度に影響を与えることができるオプションの属性です。この属性は非通過です。つまり、単一の装置に設定されるもので、UPDATE メッセージで近隣に通知されません。このセクションでは、「bgp always-compare-med コマンド (1029 ページ)」と「bgp deterministic-med コマンド (1030 ページ)」の使用について検討します。

bgp always-compare-med コマンド

bgp always-compare-med コマンドを使用すると、パス選択のために、異なる AS からのパスの MED 値を比較することができます。より低い MED を持つパスが優先されます。

例として、BGP テーブルに以下のルートがあり、**always-compare-med** コマンドが有効であると考えてみましょう。

```
Route1: as-path 7675, med 300
Route2: as-path 200, med 200
Route3: as-path 7675, med 250
```

Route2 の MED が最も低いので、選択されるパスになります。

always-compare-med コマンドが無効の場合、Route1 と Route2 の AS パスは異なるので、比較の際に MED は考慮されません。Route1 と Route3 についてのみ MED が比較されます。

bgp deterministic-med コマンド

選択されるルートは、**bgp deterministic-med** コマンドにも影響を受けます。このコマンドは、同一自律システム内の異なるピアによって通知されるルートから選択する際に、MED を比較します。

bgp deterministic-med コマンドが有効の場合、同一 AS からのルートはまとめてグループ化され、各グループの最適ルートが比較されます。BGP テーブルが以下の場合、

```
Route1: as-path 200, med 300, internal
Route2: as-path 400, med 200, internal
Route3: as-path 400, med 250, external
```

BGP には Route1 のグループと、Route2 と Route3 からなる第 2 のグループ (同一 AS) があります。

各部グループの最適ルートが比較されます。Route1 は AS 200 からの唯一のルートなので、そのグループの最適ルートになります。

Route1 は、グループ AS 400 の最適ルート (MED が最も低い) である Route2 と比較されます。

2 つのルートは同一 AS からのものではないので、比較において MED は考慮されません。外部 BGP ルートは内部 BGP ルートより優先されるため、Route3 が最適ルートになります。

BGP コミュニティ

コミュニティは、いくつかの共通プロパティを共有し、通過 BGP コミュニティ属性を使用して設定できる、プレフィックスのグループです。1 つのプレフィックスは、複数のコミュニティ属性を持つことができます。ルータは、1 つ、一部、またはすべての属性に従って動作することができます。BGP コミュニティは、一種のタグ付けと考えることができます。以下に BGP コミュニティの設定例を示します。

```
router bgp 12345
   bgp router-id 10.50.165.233
   network 12.34.5.0/24
   network 23.45.6.0/24
   neighbor 10.50.165.228 remote-as 7675
   neighbor 10.50.165.228 send-community
   neighbor 10.50.165.228 route-map comm out
!
access-list 105 permit 12.34.5.0/24
access-list 110 permit 23.45.6.0/24
!
route-map comm permit 10
   match ip address 105
   set community 7675:300
!
route-map comm permit 20
   match ip address 110
   set community 7675:500
!
router bgp 7675
```

```
   bgp router-id 10.50.165.228
   network 7.6.7.0/24
   neighbor 10.50.165.233 remote-as 12345
   neighbor 10.50.165.233 route-map shape in
!
ip community-list 1 permit 7675:300
ip community-list 2 permit 7675:500
!
route-map shape permit 10
   match community 1
   set local preference 120
route-map shape permit 20
   match community 2
   set local preference 130
```

同期と自動要約

同期設定により、iBGP 近接から取得したルートをルータが通知するかどうかを、IGP 内にこれらのルートが存在するかどうかに基づいて制御します。同期を有効にすると、BGP は OSPF または RIP (外部ゲートウェイ プロトコルである BGP とは逆に内部ゲートウェイ プロトコル) を通じて到達可能なルートのみを通知します。同期は、BGP ルート通知に関する問題の原因として一般的です。

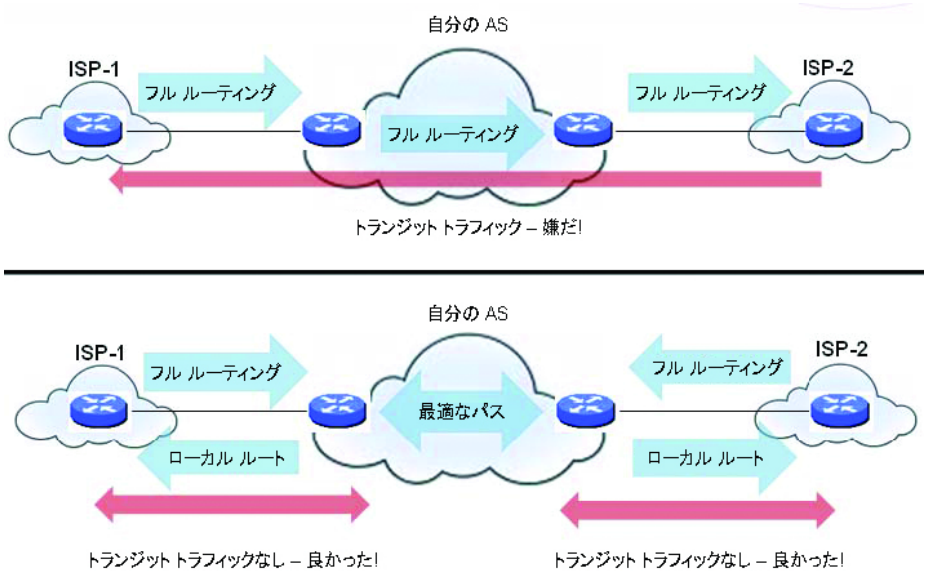
自動要約設定により、ルートをクラスフルに通知するかどうかを制御します。自動要約も、BGP 設定に関する問題の原因として一般的です。

既定では、自動要約と同期は Zebos で無効になっています。

偶発的なトランジット AS の防止

既に説明したとおり、AS ピアは、トランジット ピア (外部 AS から別の外部 AS へのトラフィックを許可する) にすることも、非トランジット ピア (すべてのトラフィックをその AS 上で開始または終了する必要がある) にすることもできます。「トランジット ピアと非トランジット ピア」を参照してください。トランジット ピアのルーティング テーブルのほうが大幅に大きくなります。一般的には、SonicWall セキュリティ装置をトランジット ピアとして設定する必要はありません。

トランジット ピアと非トランジット ピア



セキュリティ装置を間違ってトランジット ピアにしないようにするには、受信フィルタと送信フィルタを次のように設定します。

- 送信フィルタ (1032 ページ)
- 受信フィルタ (1032 ページ)

送信フィルタ

ローカル AS から開始されるルートのみ送信を許可する:

```
ip as-path access-list 1 permit ^$


router bgp 12345
   bgp router-id 10.50.165.233
   network 12.34.5.0/24
   neighbor 10.50.165.228 remote-as 7675
   neighbor 10.50.165.228 filter-list 1 out
   neighbor 172.1.1.2 remote-as 9999
   neighbor 10.50.165.228 filter list 1 out
```

所有するプレフィックスのみ送信を許可する:

```
ip prefix-list myPrefixes seq 5 permit 12.34.5.0/24
ip prefix-list myPrefixes seq 10 permit 23.45.6.0/24


router bgp 12345
   bgp router-id 10.50.165.233
   network 12.34.5.0/24
   network 23.45.6.0/24
   neighbor 10.50.165.228 remote-as 7675
   neighbor 172.1.1.2 remote-as 9999
   neighbor 10.50.165.228 prefix-list myPrefixes out
   neighbor 172.1.1.2 prefix-list myPrefixes out
```

受信フィルタ

所有するプライベート受信プレフィックスをすべて破棄する。

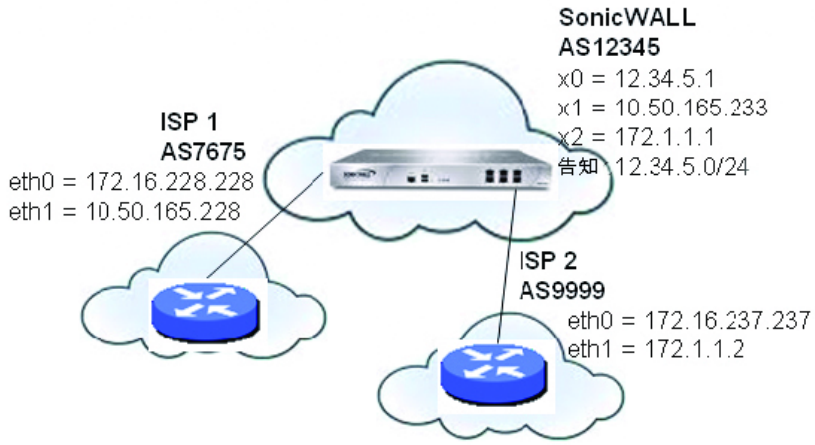
```
ip prefix-list unwantedPrefixes seq 5 deny 12.34.5.0/24 le 32
ip prefix-list unwantedPrefixes seq 10 deny 23.45.6.0/24 le 32
ip prefix-list unwantedPrefixes seq 20 deny 10.0.0.0/8 le 32
ip prefix-list unwantedPrefixes seq 21 deny 172.16.0.0/12 le 32
ip prefix-list unwantedPrefixes seq 22 deny 192.168.0.0/16 le 32
ip prefix-list unwantedPrefixes seq 30 permit 0.0.0.0/0 le 32


router bgp 12345
   bgp router-id 10.50.165.233
   network 12.34.5.0/24
   network 23.45.6.0/24
   neighbor 10.50.165.228 remote-as 7675
   neighbor 172.1.1.2 remote-as 9999
   neighbor 10.50.165.228 prefix-list unwantedPrefixes in
   neighbor 172.1.1.2 prefix-list unwantedPrefixes in
```

負荷共有のためのマルチホーム BGP の使用

「負荷共有トポロジ用のマルチホーム BGP」に示すトポロジは、SonicWall セキュリティ装置がマルチホーム BGP ネットワークを使用して 2 つの ISP 間で負荷を共有している場合の例です。

負荷共有トポロジ用のマルチホーム BGP



SonicWall セキュリティ装置は次のように設定されています。

```
router bgp 12345
   bgp router-id 10.50.165.233
   network 12.34.5.0/24
   neighbor 10.50.165.228 remote-as 7675
   neighbor 10.50.165.228 route-map ISP1 out
   neighbor 172.1.1.2 remote-as 9999
   neighbor 10.50.165.228 route-map ISP2 out
!
route-map ISP1 permit 10
match ip address 1
set weight 100

route-map ISP1 permit 20
match ip address 2

route-map ISP2 permit 10
match ip address 1


route-map ISP2 permit 20
match ip address 2
set weight 100


access-list 1 permit 12.34.5.0/25
access-list 2 deny 12.34.5.0/25
access-list 2 permit any
```

BGP 設定の確認

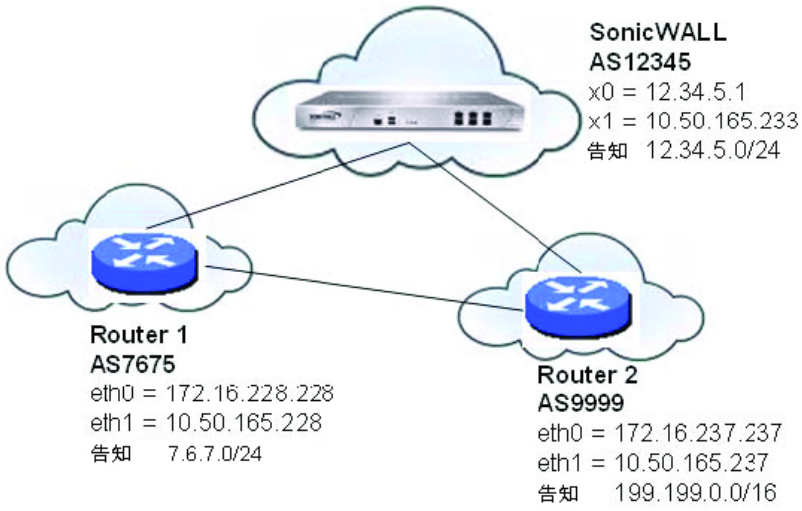
トピック:

- BGP ルートの表示 (1034 ページ)
- BGP デバッグおよびログの設定 (1035 ページ)

BGP ルートの表示

「BGP トポロジ」は、SonicWall セキュリティ装置で BGP が 2 つの異なる AS 上の 2 つのルータに接続するように設定されている、基本的な BGP トポロジを示したものです。

BGP トポロジ



このネットワークの FIB 内のルートは、SonicOS 管理インターフェースでも、CLI を使用することによっても表示できます。

トピック:

- 管理インターフェースでの FIB ルートの表示 (1034 ページ)
- CLI での FIB ルートの表示 (1034 ページ)
- CLI での RIB ルートの表示 (1035 ページ)

管理インターフェースでの FIB ルートの表示

SonicOS 管理インターフェースで「**管理 | システム セットアップ | ネットワーク > ルーティング > 設定**」から「**BGP 状況**」を選択することにより BGP 設定の要約を確認できます。「**BGP 状況**」ダイアログには、**show ip bgp summary** コマンドと **show ip bgp neighbor** コマンドの出力が表示されます。

FIB 内の BGP ルートも、「CLI での FIB ルートの表示 (1034 ページ)」で説明しているとおり、CLI によって表示できます。

CLI での FIB ルートの表示

FIB ルートを CLI で表示するには、以下を実行します。

```
SonicWall> configure
(config[SonicWall])> route ars-nsm

ZebOS version 7.7.0 IPIRouter 7/2009
ARS NSM>show ip route
```

```
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

B       7.6.7.0/24 [20/0] via 10.50.165.228, X1, 05:08:31
B       199.199.0.0/16 [20/0] via 10.50.165.237, X1, 05:08:31
C       10.50.165.192/26 is directly connected, X1
C       127.0.0.0/8 is directly connected, lo0
C       12.34.5.0/24 is directly connected, X0
```

CLI での RIB ルートの表示

RIB ルートを CLI で表示するには、以下の手順に従います。

```
ARS BGP>show ip bgp

BGP table version is 98, local router ID is 10.50.165.233

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, l -
labeled

              S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path

*> 7.6.7.0/24       10.50.165.228            0             0 7675 i

*> 12.34.5.0/24     0.0.0.0                        100  32768 i

*> 199.199.0.0/16   10.50.165.228            0             0 7675 9999 i

Total number of prefixes 3
```

メモ：最後のルートは AS7675 から取得された AS9999 へのパスです。

BGP デバッグおよびログの設定

SonicWall BGP は、BGP トラフィックに関連するログ イベントを表示するための包括的なデバッグ コマンドを提供しています。BGP ログ採取は、CLI で 「BGP デバッグ キーワード」テーブルに示すキーワードのいずれかを付けて **debug bgp** コマンドを使用することで設定できます。

BGP デバッグ キーワード

BGP デバッグ キーワード	有効化の対象
all	すべての BGP デバッグ
dampening	BGP ダンプニングのデバッグ
events	BGP イベントのデバッグ
filters	BGP フィルタのデバッグ
fsm	BGP の有限状態機械 (FSM) のデバッグ
keepalives	BGP キープアライブのデバッグ
nht	NHT メッセージのデバッグ
nsm	NSM メッセージのデバッグ
updates	受信/送信 BGP 更新のデバッグ

BGP デバッグを無効にするには、コマンドの前に "no" と入力します。例えば、イベントのデバッグを無効にするには、**no debug events** コマンドを入力します。

BGP ログ メッセージは、SonicOS GUI の「**管理 | 調査 | ログ | イベント ログ**」でも表示できます。BGP メッセージは、ログ メッセージの「**高度なルーティング**」種別の一部として表示されます。ログとログ採取の詳細については、『*SonicOS ログとレポート*』を参照してください。

直接接続されていない BGP ピアを許可するには、**neighbor** コマンドで **ebgp-multihop** キーワードを使用します。以下に例を示します。

```
neighbor 10.50.165.228 ebgp-multihop
```

Ipv6 BGP

IPv6 Border Gateway protocol (BGP) は、自律システム (AS) 間で IPv6 のルーティング情報をやりとりするプロトコルです。IPv6 BGP をサポートする SonicWall セキュリティ装置は、ネットワークの AS のエッジにある従来の BGP ルータの代わりに配置できます。

IPv6 BGP は、「**管理 | システム セットアップ | ネットワーク > ルーティング**」で有効にしますが、SonicOS コマンド ライン インターフェース (CLI) で設定する必要があります。

以下の制限が適用されます。

- IPv6 BGP は、NSA プラットフォームのみでサポートされます。
- IPv6 BGP は、IPv6 の機能と ZebOS (Zebra OS) に依存します。
- MPLS/VPN は IPv6 BGP ではサポートされません。

トピック:

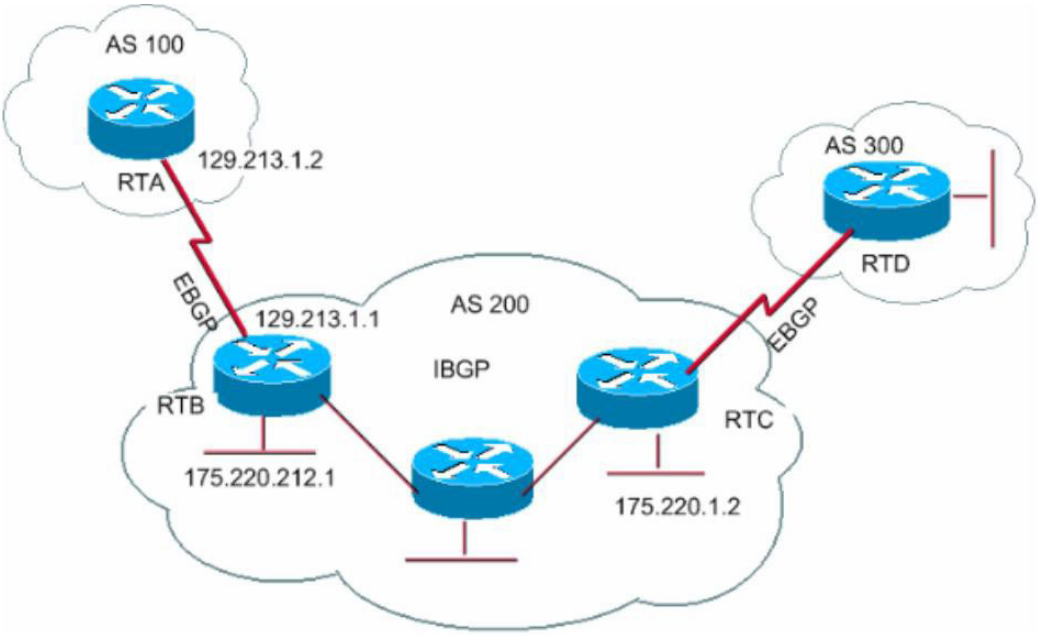
- 複数の自律システムの設定 (1037 ページ)
- IPv6 での BGP の基本設定 (1038 ページ)
- EBGP マルチホップの設定 (1038 ページ)
- IPv6 BGP 送信ルート フィルタリングの設定 (1039 ページ)
- IPv6 BGP 配布リストの設定 (1040 ページ)
- IPv6 BGP ルートマップ (1041 ページ)
- AS 正規表現の設定 (1042 ページ)
- EBGP のルート選択 (1044 ページ)
- IPv6 BGP の同期 (1047 ページ)
- BGP ルート リフレクション (1048 ページ)
- IPv6 BGP ローカル プリファレンス (1051 ページ)
- BGP ピア グループの更新ポリシー (1054 ページ)
- BGP 連合 (1056 ページ)

複数の自律システムの設定

1 つの自律システム (AS) に複数の BGP ルータがある場合、その AS は他の AS にトランジット サービスを提供できます。異なる AS に属するルータ間で BGP が動作する場合、BGP は外部 BGP (eBGP) を使用します。同じ AS に属するルータ間で BGP が動作する場合、BGP は内部 BGP (iBGP) を使用します。

「複数の BGP ルータが設定された自律システム」では、AS 200 が AS 100 と AS 300 のトランジット AS です。

複数の BGP ルータが設定された自律システム



「複数の BGP ルータが設定された自律システム」に示すように複数の AS を設定するには、ルータ RTA、RTB、RTC を次のように設定します。

RTA 上で以下を実行

```
router bgp 100
   neighbor 129.213.1.1 remote-as 200

address-family ipv6
   redistribute connected
   neighbor 129.213.1.1 activate
```

RTB 上で以下を実行

```
router bgp 200
   neighbor 129.213.1.2 remote-as 100
   neighbor 175.220.1.2 remote-as 200

address-family ipv6
   redistribute connected
   neighbor 129.213.1.2 activate
   neighbor 175.220.1.2 activate
```

RTC 上で以下を実行

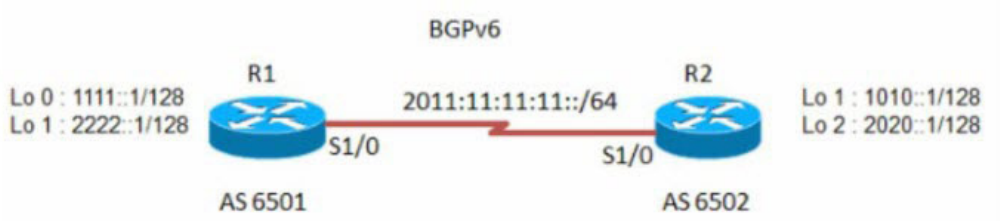
```
router bgp 200
   neighbor 175.220.212.1 remote-as 200
```

```
address-family ipv6
   neighbor 175.220.212.1 activate
   neighbor 175.220.212.1 activate
```

IPv6 での BGP の基本設定

IPv6 の BGP ピアルータは、IPv4 と IPv6 のルート情報のいずれかを IPv6 アドレス ファミリーと IPv4 アドレス ファミリーのいずれかで送信するように設定できます。「IPv6 での BGP の基本設定」テーブルを参照してください。

IPv6 での BGP の基本設定



IPv6 での BGP の基本設定を行うには、以下の手順に従います。

1 ルータ R1 と R2 を次のように設定します。

R1 上で以下を実行

```
router bgp 6501
   bgp router-id 1.1.1.1
   neighbor 2011:11:11:11::2 remote-as 6502

address-family ipv6
   neighbor 2011:11:11:11::2 activate

exit-address-family
```

R2 上で以下を実行

```
router bgp 6502
   bgp router-id 2.2.2.2
   neighbor 2011:11:11:11::1 remote-as 6501


address-family ipv6
   network 1010::1/128
   network 2020::1/128
   neighbor 2011:11:11:11::1 activate
```

EBGP マルチホップの設定

EBGP マルチホップを使用すると、直接接続されていない 2 つの外部ピア間の近隣接続を確立できます。マルチホップが利用できるのは eBGP のみで、iBGP では利用できません。セキュリティ装置が直接接続されていない外部ピアを持つ場合、**ebgp-multihop** コマンドを使用して近隣接続を確立できます。

EBGP マルチホップを設定するには、以下の手順に従います。

1 ルータ R1 と R2 を次のように設定します。

R1 上で以下を実行

```
router bgp 6501
   bgp router-id 1.1.1.1
   neighbor 2011:11:11:11::2 remote-as 6502
   neighbor 2011:11:11:11::2 ebgp-multihop


address-family ipv6
   neighbor 2011:11:11:11::2 activate
exit-address-family
```

R2 上で以下を実行

```
router bgp 6502
   bgp router-id 2.2.2.2
   neighbor 2011:11:11:11::1 remote-as 6501
   neighbor 2011:11:11:11::1 ebgp-multihop


address-family ipv6
   network 1010::1/128
   network 2020::1/128
   neighbor 2011:11:11:11::1 activate
```

IPv6 BGP 送信ルート フィルタリングの設定

IPv6 BGP 送信ルート フィルタリング (ORF) を使用すると、不要なルーティング更新情報を送信元でフィルタ オフすることにより、ピア·ルータ間で送信される BGP 更新の数を最小限にできます。

IPv6 BGP 送信ルート フィルタリング (ORF) を設定するには、以下の手順に従います。

1 ルータ R1 と R2 を次のように設定します。

R1 上で以下を実行

```
router bgp 6501
   bgp router-id 1.1.1.1
   neighbor 2011:11:11:11::2 remote-as 6502


address-family ipv6
   redistribute connected
   neighbor 2011:11:11:11::2 activate
   neighbor 2011:11:11:11::2 prefix-list pref1 in
   neighbor 2011:11:11:11::2 prefix-list pref2 out
exit-address-family


ipv6 prefix-list pref1 seq 10 deny 1010::1/128
ipv6 prefix-list pref1 seq 20 permit any
ipv6 prefix-list pref2 seq 10 deny 1111::1/128
ipv6 prefix-list pref2 seq 20 permit any
```

R2 上で以下を実行

```
router bgp 6502
   bgp router-id 2.2.2.2
   neighbor 2011:11:11:11::1 remote-as 6501


address-family ipv6
   redistribute connected
   neighbor 2011:11:11:11::1 activate
```

R1 と R2 のルートを確認するには、**show bgp ipv6 unicast** コマンドを使用します。

R1 のルートには、IPv6 アドレス 1010::1/128 が表示されるはずです。

R2 のルートには、IPv6 アドレス 1111::1/128 が表示されるはずです。

R1 上で以下を実行

```
R1> show bgp ipv6 unicast
```

R2 上で以下を実行

```
R2> show bgp ipv6 unicast
```

IPv6 BGP 配布リストの設定

IPv6 BGP 配布リストを使用すると、不要なルーティング更新情報を送信元でフィルタ オフすることにより、ピア·ルータ間で送信される BGP 更新の数を最小限にできます。

IPv6 BGP 配布リストを設定するには、以下の手順に従います。

1 ルータ R1 と R2 を次のように設定します。

R1 上で以下を実行

```
router bgp 6501
   bgp router-id 1.1.1.1
   neighbor 2011:11:11:11::2 remote-as 6502


address-family ipv6
   redistribute connected
   neighbor 2011:11:11:11::2 activate
   neighbor 2011:11:11:11::2 distribute-list acl1 in
   neighbor 2011:11:11:11::2 distribute-list acl2 out
exit-address-family


ipv6 access-list acl1 deny 1010::1/128
ipv6 access-list acl1 permit any
ipv6 access-list acl2 deny 1111::1/128
ipv6 access-list acl2 permit any
```

R2 上で以下を実行

```
router bgp 6502
   bgp router-id 2.2.2.2
   neighbor 2011:11:11:11::1 remote-as 6501
```

```
address-family ipv6
   redistribute connected
   neighbor 2011:11:11:11::1 activate
```

R1 と R2 のルートを確認するには、**show bgp ipv6 unicast** コマンドを使用します。

R1 のルートには、IPv6 アドレス 1010::1/128 が表示されるはずです。

R2 のルートには、IPv6 アドレス 1111::1/128 が表示されるはずです。

R1 上で以下を実行

```
R1> show bgp ipv6 unicast
```

R2 上で以下を実行

```
R2> show bgp ipv6 unicast
```

IPv6 BGP ルートマップ

IPv6 BGP ルートマップを使用すると、不要なルーティング更新情報を送信元でフィルタ オフすることにより、ピア·ルータ間で送信される BGP 更新の数を最小限にできます。

IPv6 BGP ルート マップを設定するには、以下の手順に従います。

1 ルータ R1 と R2 を次のように設定します。

R1 上で以下を実行

```
router bgp 6501
   bgp router-id 1.1.1.1
   neighbor 2011:11:11:11::2 remote-as 6502


address-family ipv6
   redistribute connected
   neighbor 2011:11:11:11::2 activate
   neighbor 2011:11:11:11::2 route-map map1 in
   neighbor 2011:11:11:11::2 route-map map2 out
exit-address-family


ipv6 access-list acl1 deny 1010::1/128
ipv6 access-list acl1 permit any
ipv6 access-list acl2 deny 1111::1/128
ipv6 access-list acl2 permit any
!
route-map map1 permit 1 match ipv6 address acl1
!
route-map map2 permit 1 match ipv6 address acl2
!
```

R2 上で以下を実行

```
router bgp 6502
   bgp router-id 2.2.2.2
   neighbor 2011:11:11:11::1 remote-as 6501
```

```
address-family ipv6
   redistribute connected
   neighbor 2011:11:11:11::1 activate
```

R1 と R2 のルートを確認するには、**show bgp ipv6 unicast** コマンドを使用します。

R1 上で以下を実行

```
R1> show bgp ipv6 unicast
```

R1 のルートには、IPv6 アドレス 1010::1/128 が表示されるはずです。

R2 上で以下を実行

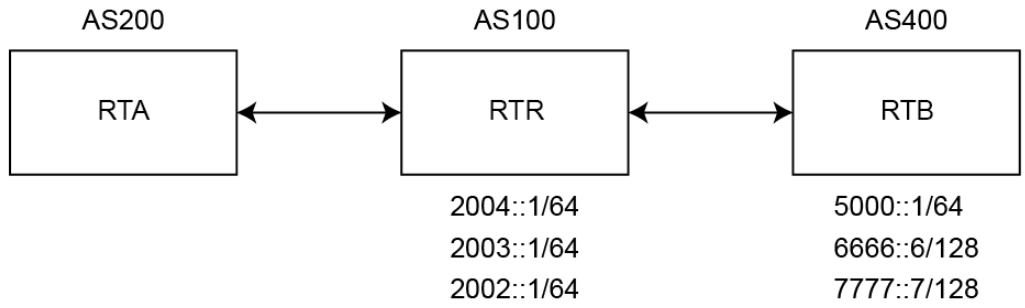
```
R2> show bgp ipv6 unicast
```

R2 のルートには、IPv6 アドレス 1111::1/128 が表示されるはずです。

AS 正規表現の設定

正規表現を設定すると、AS からのアドレスを照合することができ、アドレスの禁止または許可に使用できます。「自律システム正規表現の設定」テーブルを参照してください。

自律システム正規表現の設定



RTB は以下のルートを通知します。

- 2004::/64
- 2003::/64
- 2002::/64

RTC は以下のルートを通知します。

- 5000::/64
- 6666::6/128
- 7777::7/128

ルータ RTA のルートを確認するには、以下の手順に従います。

1 **show bgp ipv6 unicast** コマンドを使用します。

RTA 上で以下を実行

```
RTA> show bgp ipv6 unicast

BGP table version is 4, local router ID is 10.0.1.2
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal, l - labeled
S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network          Next Hop            Metric     LocPrf    Weight    Path
*> 2002::/64      ::ffff:a00:101     0          0         100       i
*> 2003::/64      ::ffff:a00:101     0          0         100       i
*> 2004::/64      ::ffff:a00:101     0          0         100       i
*> 5000::/64      ::ffff:a00:101     0          0         100       400i
*> 6666::6/128    ::ffff:a00:101     0          0         100       400
*> 7777::7/128    ::ffff:a00:101     0          0         100       400
```

RTA でAS 正規表現を設定し、AS100 が発信元のルートをすべて禁止するには、以下の手順を実行します。

```
router bgp 200
   neighbor 10.0.1.1 remote-as 100
   neighbor 10.0.1.1 update-source X2
   neighbor 2004::1 remote-as 100
   neighbor 2004::1 update-source X2
!
address-family ipv6
   neighbor 10.0.1.1 activate
   neighbor 10.0.1.1 filter-list 1 in
   neighbor 2004::1 activate
   exit-address-family


ip as-path access-list 1 deny ^100$
ip as-path access-list 1 permit .*
```

ルータ RTA のルートを確認するには、以下の手順に従います。

1 **show bgp ipv6 unicast** コマンドを使用します。

RTA 上で以下を実行

```
RTA> show bgp ipv6 unicast

BGP table version is 4, local router ID is 10.0.1.2

Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal, l - labeled

S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete

Network          Next Hop            Metric     LocPrf    Weight    Path
*> 5000::/64      ::ffff:a00:101     0          0         100       400i
*> 6666::6/128    ::ffff:a00:101     0          0         100       400i
```

```
*> 7777::7/128    ::ffff:a00:101     0          0         100       400i

Total number of prefixes 3
```

AS100 から学習したすべてのルートを禁止するように AS パスを変更するには、以下の手順を実行します。

RTA 上で以下を実行

```
router bgp 200
   neighbor 10.0.1.1 remote-as 100
   neighbor 10.0.1.1 update-source X2
   neighbor 2004::1 remote-as 100
   neighbor 2004::1 update-source X2
!
address-family ipv6
   neighbor 10.0.1.1 activate
   neighbor 10.0.1.1 filter-list 1 in
   neighbor 2004::1 activate
exit-address-family

ip as-path access-list 1 deny _100_
ip as-path access-list 1 permit .*
```

ルータ RTA のルートを確認するには、以下の手順に従います。

1 **show bgp ipv6 unicast** コマンドを使用します。

RTA 上で以下を実行

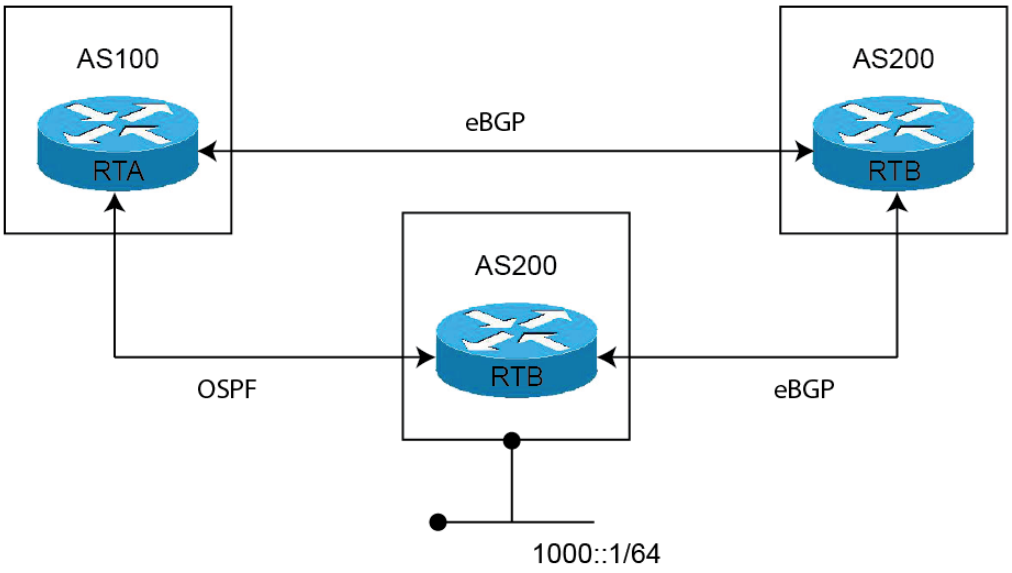
```
RTA> show bgp ipv6 unicast
```

EBGP のルート選択

ルートは、そのルート上で動作するルーティング プロトコルの管理距離に基づいて選択されます。管理距離が小さいルーティング プロトコルは、管理距離が大きいルーティング プロトコルよりも優先されます。EBGP の管理距離は 20 です。OSPF の管理距離は 110 です。

「自律システムの EBGP のルート選択の設定」テーブルは、3 つの AS と、BGP ルータで使用中のルーティング プロトコルを示しています。

自律システムの EBGP のルート選択の設定



AS300 の RTC ルータは、AS100 と AS200 の両方にルート 1000::/64 を通知します。

RTC (AS300) から RTA (AS100) へのルートでは OSPF が実行されています。

RTC (AS300) から RTB (AS200) へのルートでは eBGP が実行されています。

RTA (AS100) から RTB (AS200) へのルートでは eBGP が実行されています。

RTA (AS100) は、ルート 1000::/64 に関する更新を OSPF と eBGP の両方から受信します。eBGP の管理距離は OSPF の管理距離よりも小さいため、eBGP から学習したルートが選択され、RTA のルーティングテーブルに追加されます。

RTA 上で以下を実行

```
router bgp 100
   neighbor 3001::1 remote-as 200
!
address-family ipv6
   distance bgp 150 150 150
   neighbor 3001::1 activate
exit-address-family
```

RTB 上で以下を実行

```
router bgp 200
   bgp log-neighbor-changes
   neighbor 1001::1 remote-as 300
   neighbor 2003::1 remote-as 100

address-family ipv6
   network 6666::6/128
   neighbor 1001::1 activate
   neighbor 2003::1 activate
exit-address-family
```

RTC 上で以下を実行

```
router bgp 300
```

```
   neighbor 3002::1 remote-as 200
!
address-family ipv6 network 1000::/64
   neighbor 3002::1 activate
exit-address-family
```

ルータ RTA のルートを確認するには、**show ipv6 route** コマンドを使用します。

```
RTA> show ipv6 route

IPv6 Routing Table

Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B
- BGP
Timers: Uptime


B   1000::/64 [20/0] via fe80::204:27ff:fe0c:b006, X1, 00:01:07
C   2003::/64 via ::, X1, 00:30:50
B   6666::6/128 [20/0] via fe80::204:27ff:fe0c:b006, X1, 00:01:07
C   fe80::/64 via ::, X1, 00:30:53
```

RTC は RTA に直接接続しているため、実際には BGP から学習したルートよりも OSPF のルートのほうが好ましいルートです。RTA と RTC の間のルートが選択されてルーティング テーブルに追加されるようにするには、**distance** コマンドを使用して、BGP ルートの既定の管理距離が OSPF ルートよりも大きくなるようにします。以下に例を示します。

```
   distance bgp 150 150 150
```

backdoor neighbor コマンドを使用して BGP ルートを優先ルートに設定することもできます。以下に例を示します。

RTA 上で以下を実行

```
router bgp 100
   neighbor 3001::1 remote-as 200
!
address-family ipv6
   network 1000::/64
   backdoor neighbor 3001::1 activate
exit-address-family
```

ルータ RTA のルートを確認するには、以下の手順に従います。

1. **show ipv6 route** コマンドを使用します。

```
RTA> show ipv6 route

IPv6 Routing Table


Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B
- BGP
Timers: Uptime


O   1000::/64 [110/2] via fe80::217:c5ff:feb4:57f2, X4, 00:30:53
C   2003::/64 via ::, X1, 00:31:18
B   6666::6/128 [20/0] via fe80::204:27ff:fe0c:b006, X1, 00:00:03
C   fe80::/64 via ::, X1, 00:31:21
```

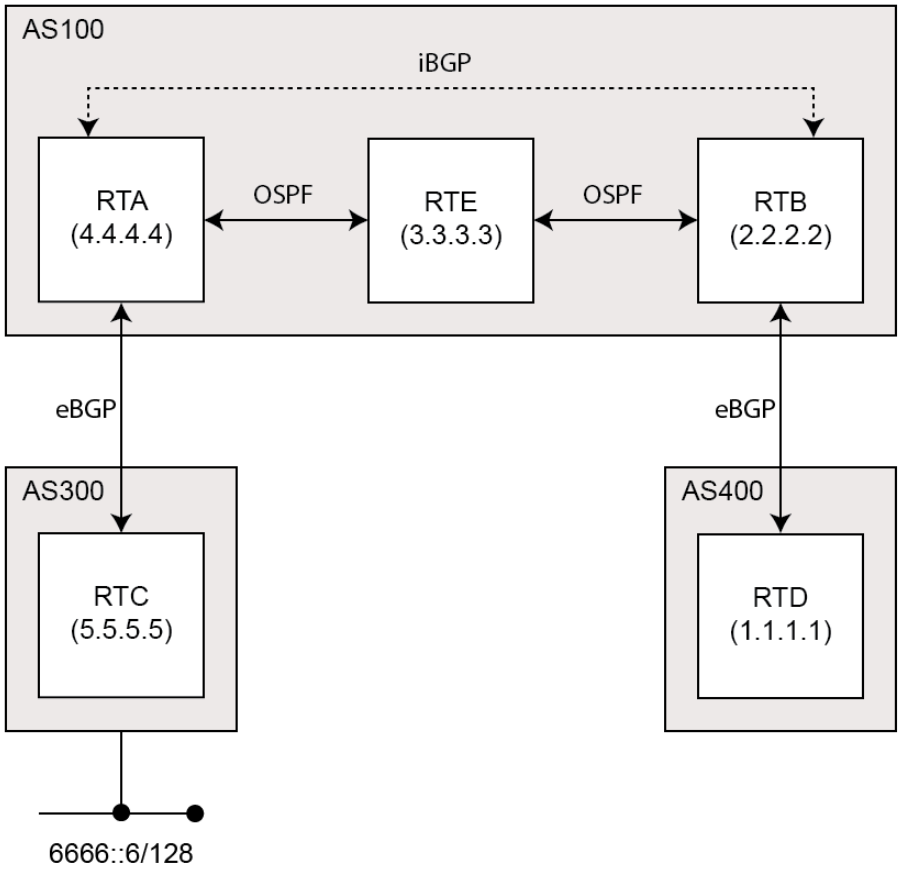
IPv6 BGP の同期

IPv6 BGP の同期は、すべての利用可能なルートおよびネットワークの IPv6 アドレスを使用してすべての BGP ルータを最新に保つ機能です。

BGP 同期では、ある AS (AS100) が別の AS (AS300) からのトラフィックを 3 番目の AS (AS400) に渡す場合、BGP は AS100 のすべてのルータが IGP からルートを学習するまでそのルートを通知しません。この例では、IGP は iBGP になります。iBGP が AS100 内のすべてのルータにそのルートを伝播するまで、AS100 は待つ必要があります。その後、eBGP は外部 AS にルートを通知します。

この例では、RTB が iBGP でアドレス `6666::6/128` を学習した後、RTB がそのアドレスを RTD に通知します。

IPv6 BGP の同期の例



メモ： `6666::6/128` への静的ルートを RTB に追加し、他のルータが `6666::6/128` に到達できることを確認することで、IGP が既にルート情報を伝播したと RTB に思い込ませることができます。

この例では、RTC (AS2) がアドレス `6666::6/128` を RTA (AS100) に通知します。AS100 内では RTA と RTB が iBGP を実行しているので、RTB はアドレス `6666::6/128` を学習し、ネクスト ホップ `5.5.5.5` (RTC) 経由でこのアドレスに到達できます。ネクスト ホップは iBGP 経由で伝送されます。ただし、ネクスト ホップ (RTC) に到達するには、RTB は RTE 経由でトラフィックを送信する必要がありますが、RTE は IP アドレス `6666::6/128` を知りません。

RTB が 6666::6/128 を RTD (AS400) に通知すると、RTD から 6666::6/128 に向かうトラフィックは AS100 の RTB と RTE を通過する必要があります。ところが、RTE はまだ 6666::6/128 を学習していないので、RTE ですべてのパケットが破棄されます。

AS100 の RTB で BGP の同期を設定するには、以下の手順を実行します。

RTB 上で以下を実行

```
router bgp 100
   neighbor 10.103.10.129 remote-as 100
   neighbor 3001::1 remote-as 100
   neighbor 3001::1 update-source X4
   neighbor 5000::1 remote-as 400
   neighbor 5000::1 update-source X2
!
address-family ipv6
   synchronization
   neighbor 10.103.10.129 activate
   neighbor 3001::1 activate
   neighbor 5000::1 activate
exit-address-family
```

1 つの AS から中継する AS を通じて別の AS にトラフィックを送信することがない場合は、同期を無効にできます。中継 AS 内のすべてのルータが BGP を実行する場合は同期を無効にすることもできます。同期を無効にすると、IGP で送信するルートが減少し、BGP の収束が速くなります。

AS100 の RTB で BGP の同期を無効にするには、以下の手順を実行します。

RTB 上で以下を実行

```
router bgp 100
   neighbor 10.103.10.129 remote-as 100
   neighbor 3001::1 remote-as 100
   neighbor 3001::1 update-source X4
   neighbor 5000::1 remote-as 400
   neighbor 5000::1 update-source X2
!
address-family ipv6
   neighbor 10.103.10.129 activate
   neighbor 3001::1 activate
   neighbor 5000::1 activate
exit-address-family
```

BGP ルート リフレクション

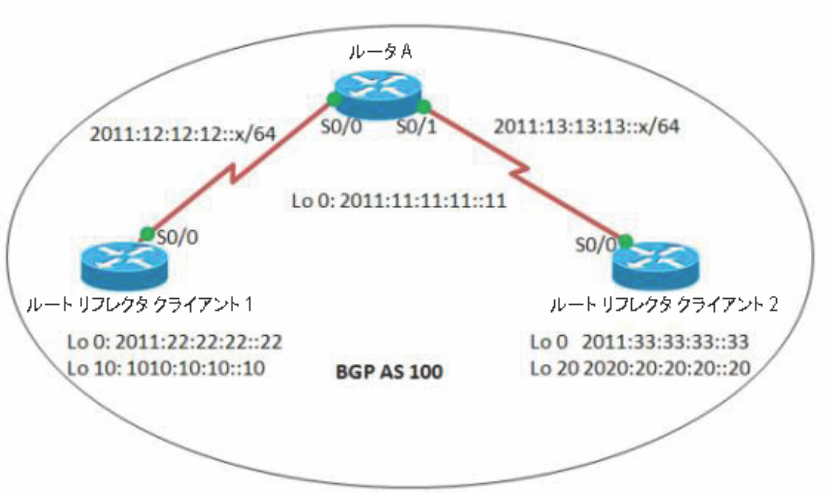
既定では、AS 内のすべての iBGP ルータはフルメッシュ 構成にする必要があります。つまり、各ルータを他のすべてのルータのピアに設定しなければなりません。

ルート リフレクションを使用すると、iBGP ルータをすべてフル メッシュにする必要はなくなります。ルート リフレクションによって、各 iBGP ルータが AS 内の他のすべてのルータとやりとりする必要性が解消します。1 台の iBGP ルータをルート リフレクタとして指定すると、そのルータは iBGP で学習したルートを複数の iBGP クライアントに送信できます。

ルータをルート リフレクタとして設定すると、そのルータは他の iBGP ルータが iBGP で得られたルートを取得できる単一のポイントとして機能します。ルート リフレクタは、AS 内の他のすべてのルータにとって、ピアではなくサーバとして機能します。他のすべての iBGP ルータは、ルート リフレク

タ クライアントになります。ルータは、1 つ以上のルート リフレクタ クライアントが存在するかぎりルート リフレクタです。

BGP ルート リフレクションの設定



AS 内でルート リフレクションを設定するには、以下の手順を実行します。

RouterA 上で以下を実行

```
interface Serial0/0
   ipv6 address 2011:12:12:12::1/64
   ipv6 address 10:12:12:12::1/0

interface Serial0/1
   ipv6 address 2011:13:13:13::1/64
   ipv6 address 10:12:12:12::1/0

router bgp 100

bgp router-id 1.1.1.1
no bgp default ipv4-unicast
bgp log-neighbor-changes
   neighbor 2011:22:22:22::22 remote-as 100
   neighbor 2011:22:22:22::22 update-source Loopback0
   neighbor 2011:33:33:33::33 remote-as 100
   neighbor 2011:33:33:33::33 update-source Loopback0
!
address-family ipv6
   neighbor 2011:22:22:22::22 activate
   neighbor 2011:22:22:22::22 route-reflector-client
   neighbor 2011:33:33:33::33 activate
   neighbor 2011:33:33:33::33 route-reflector-client
exit-address-family
!
ipv6 router ospf 10
   router-id 1.1.1.1
```

RRClient1 上で以下を実行

```
interface Loopback0
   ipv6 address 2011:22:22:22::22/128
   ipv6 address 10:12:12:12::1/0
!
interface Loopback10
   ipv6 address 1010:10:10:10::10/128

interface Serial0/0
   ipv6 address 2011:12:12:12::2/64
   ipv6 address 10:12:12:12::1/0
!
router bgp 100
   bgp router-id 2.2.2.2
   bgp log-neighbor-changes
      neighbor 2011:11:11:11::11 remote-as 100
      neighbor 2011:11:11:11::11 update-source Loopback0
!
address-family ipv6
   neighbor 2011:11:11:11::11 activate
   network 1010:10:10:10::10/128
exit-address-family
!
ipv6 router ospf 10
   router-id 2.2.2.2
```

RRClient2 (ルート リフレクタ クライアント 2) 上で以下を実行

```
interface Loopback0
   ipv6 address 2011:33:33:33::33/128
   ipv6 address 10:12:12:12::1/0
!
interface Loopback20
   ipv6 address 2020:20:20:20::20/128
!
interface Serial0/0
   no ip address
   ipv6 address 2011:13:13:13::2/64
   ipv6 address 10:12:12:12::1/0
!
router bgp 100
   bgp router-id 3.3.3.3
   bgp log-neighbor-changes
      neighbor 2011:11:11:11::11 remote-as 100
      neighbor 2011:11:11:11::11 update-source Loopback0
!
address-family ipv6
   neighbor 2011:11:11:11::11 activate
   network 2020:20:20:20::20/128
exit-address-family
!
ipv6 router ospf 10
   router-id 3.3.3.3
   log-adjacency-changes
```

ルートを確認するには、以下の手順に従います。

1 **show bgp ipv6 unicast** コマンドを使用します。

RRClient1 上で以下を実行

```
RRClient1> show bgp ipv6 unicast
```

ルート 2020:20:20:20::20/128 が表示されます。

RRClient2 上で以下を実行

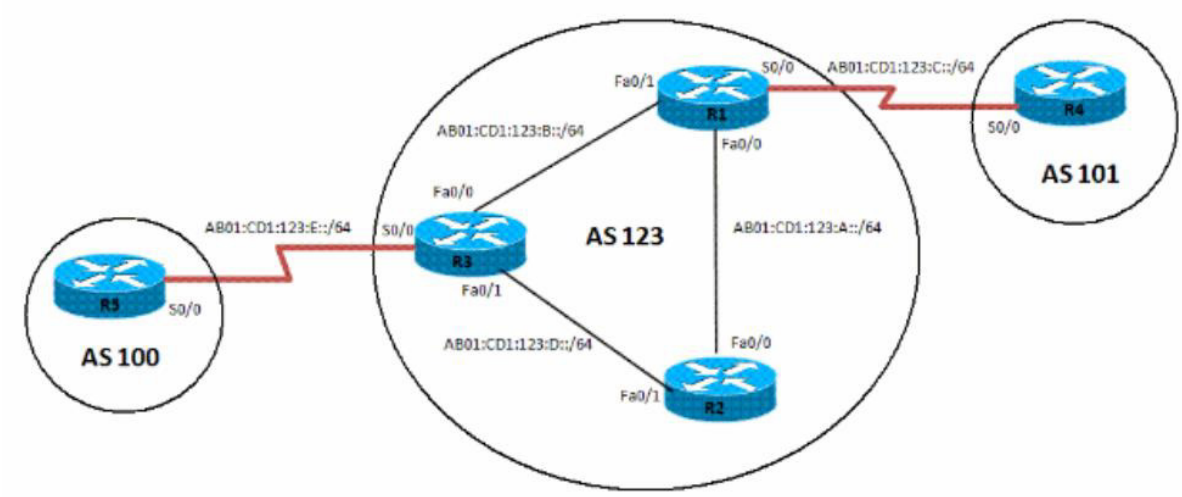
```
RRClient2> show bgp ipv6 unicast
```

ルート 1010:10:10:10::10/128 が表示されます。

IPv6 BGP ローカル プリファレンス

ローカル プリファレンスは、特定のネットワークへの任意のルートを AS からそのネットワークへの優先的な出口ルートとして指定する機能です。ローカル プリファレンスが最大のルートが優先ルートになります。ローカル プリファレンスの既定値は 100 ですが、この値は **set local-preference** コマンドで変更できます。

IPv6 BGP ローカル プリファレンスの設定



AS 内で優先ルートのローカル プリファレンスを設定するには、以下の手順を実行します。

R1 上で以下を実行

```
interface Loopback0
   ipv6 address 1111:111:111:A::/64 eui-64
   ipv6 address 10:12:12:12::1/0

interface FastEthernet0/0
   ipv6 address AB01:CD1:123:A::/64 eui-64
   ipv6 address 10:12:12:12::1/0
!
interface Serial0/0
   ipv6 address AB01:CD1:123:C::/64 eui-64
!
interface FastEthernet0/1
   ipv6 address AB01:CD1:123:B::/64 eui-64
   ipv6 address 10:12:12:12::1/0
```

```
!
   ipv6 router ospf 10 router-id 1.1.1.1 log-adjacency-changes
   redistribute connected route-map CONNECTED
!
route-map CONNECTED permit 10
   match interface Serial0/0
!
router bgp 123
bgp router-id 1.1.1.1
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 remote-as 123
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 update-source Loopback0
   neighbor 3333:333:333:A:C603:3FF:FEF0:0 remote-as 123
   neighbor 3333:333:333:A:C603:3FF:FEF0:0 update-source Loopback0
   neighbor AB01:CD1:123:C:C604:16FF:FE98:0 remote-as 101
   neighbor AB01:CD1:123:C:C604:16FF:FE98:0 ebgp-multihop 5
!
address-family ipv6
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 activate
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 next-hop-self
   neighbor 3333:333:333:A:C603:3FF:FEF0:0 activate
   neighbor 3333:333:333:A:C603:3FF:FEF0:0 next-hop-self
   neighbor AB01:CD1:123:C:C604:16FF:FE98:0 activate exit-address-family
```

R2 上で以下を実行

```
interface Loopback0
   ipv6 address 2222:222:222:A::/64 eui-64
   ipv6 address 10:12:12:12::1/0
!
interface FastEthernet0/0
   ipv6 address AB01:CD1:123:A::/64 eui-64
   ipv6 address 10:12:12:12::1/0
!
interface FastEthernet0/1
   ipv6 address AB01:CD1:123:D::/64 eui-64
   ipv6 address 10:12:12:12::1/0
!
   ipv6 router ospf 10 router-id 2.2.2.2 log-adjacency-changes
!
router bgp 123
bgp router-id 2.2.2.2
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 remote-as 123
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 update-source Loopback0
   neighbor 3333:333:333:A:C603:3FF:FEF0:0 remote-as 123
   neighbor 3333:333:333:A:C603:3FF:FEF0:0 update-source Loopback0

address-family ipv6
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 activate
   neighbor 3333:333:333:A:C603:3FF:FEF0:0 activate
exit-address-family
```

R3 上で以下を実行

```
interface Loopback0
   ipv6 address 3333:333:333:A::/64 eui-64
   ipv6 address 10:12:12:12::1/0
!
interface FastEthernet0/0
```

```
   ipv6 address AB01:CD1:123:B::/64 eui-64
   ipv6 address 10:12:12:12::1/0
!
interface Serial0/0
   ipv6 address AB01:CD1:123:E::/64 eui-64
!
interface FastEthernet0/1
   ipv6 address AB01:CD1:123:D::/64 eui-64
   ipv6 address 10:12:12:12::1/0
!
ipv6 router ospf 10
   router-id 3.3.3.3
   redistribute connected route-map CONNECTED
!
router bgp 123
   no synchronization
   bgp router-id 3.3.3.3
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 remote-as 123
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 update-source Loopback0
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 remote-as 123
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 update-source Loopback0
   neighbor AB01:CD1:123:E:C605:16FF:FE98:0 remote-as 202
   neighbor AB01:CD1:123:E:C605:16FF:FE98:0 ebgp-multihop 5
!
address-family ipv6
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 activate
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 next-hop-self
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 route-map LOCAL_PREF out
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 activate
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 next-hop-self
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 route-map LOCAL_PREF out
   neighbor AB01:CD1:123:E:C605:16FF:FE98:0 activate
exit-address-family
!
ipv6 prefix-list 10 seq 5 permit BC01:BC1:10:A::/64
!
route-map LOCAL_PREF permit 10
   match ipv6 address prefix-list 10
   set local-preference 500
!
route-map LOCAL_PREF permit 20
!
route-map CONNECTED permit 10
   match interface Serial0/0
```

R4 上で以下を実行

```
interface Serial0/0
   ipv6 address AB01:CD1:123:C::/64 eui-64
!
interface Loopback10
   ipv6 address BC01:BC1:10:A::/64 eui-64
!
interface Loopback11
   ipv6 address BC02:BC1:11:A::/64 eui-64
!
interface Loopback12
   ipv6 address BC03:BC1:12:A::/64 eui-64

router bgp 101
bgp router-id 4.4.4.4
```

```
   neighbor AB01:CD1:123:C:C601:3FF:FEF0:0 remote-as 123
!
address-family ipv6
   neighbor AB01:CD1:123:C:C601:3FF:FEF0:0 activate
   network BC01:BC1:10:A::/64 network BC02:BC1:11:A::/64
   network BC03:BC1:12:A::/64 exit-address-family
```

R5 上で以下を実行

```
interface Serial0/0
   ipv6 address AB01:CD1:123:E::/64 eui-64
   clock rate 2000000
!
interface Loopback10
   ipv6 address BC01:BC1:10:A::/64 eui-64
!
interface Loopback11
   ipv6 address BC02:BC1:11:A::/64 eui-64
!
interface Loopback12
   ipv6 address BC03:BC1:12:A::/64 eui-64
!
router bgp 202
bgp router-id 5.5.5.5
   neighbor AB01:CD1:123:E:C603:3FF:FEF0:0 remote-as 123
   neighbor AB01:CD1:123:E:C603:3FF:FEF0:0 ebgp-multihop 5
!
address-family ipv6
   neighbor AB01:CD1:123:E:C603:3FF:FEF0:0 activate
   network BC01:BC1:10:A::/64
   network BC02:BC1:11:A::/64
   network BC03:BC1:12:A::/64
exit-address-family
```

ルートを確認するには、以下の手順に従います。

1 **show bgp ipv6 unicast** コマンドを使用します。

R2 上で以下を実行

```
R2> show bgp ipv6 unicast
```

ローカル プリファレンスを設定する前は、R2 は学習したすべての IPv6 アドレスのネクスト ホップとして R1 を持っていました。R3 でローカル プリファレンスを 500 に設定した後は、R2 はプリフィックス BC01:BC1:10:A::/64 に対して異なる優先出口ルートを持つようになります。R2 は、これでローカル プリファレンスとして指定された R3 の出口パスを通ってプリフィックス BC01:BC1:10:A::/64 に到達できるようになりました。

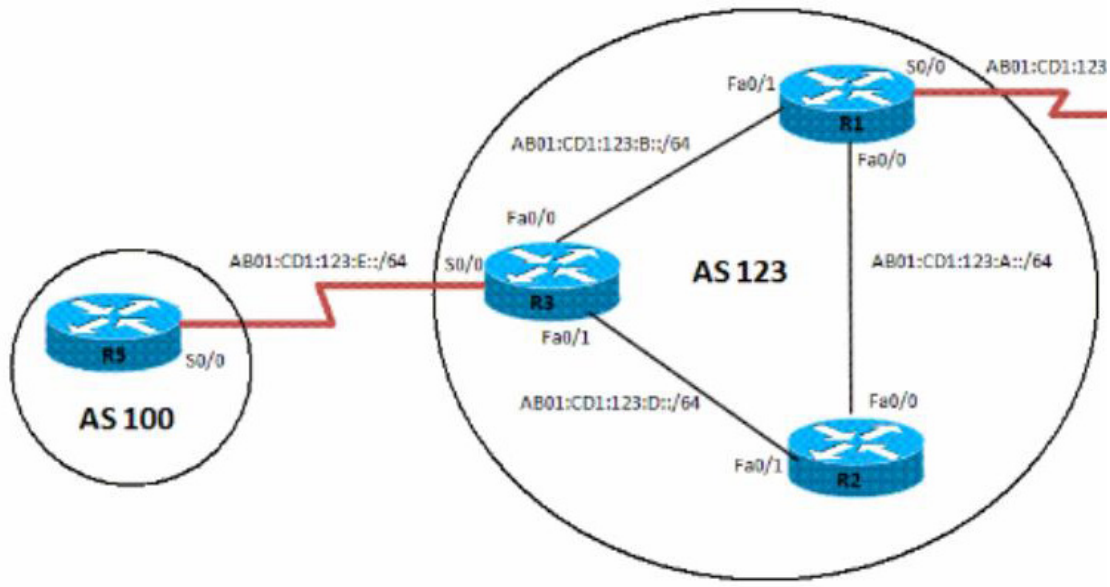
BGP ピア グループの更新ポリシー

BGP ピア グループとは、同じ更新ポリシーを共有する BGP 近隣のグループを指します。通常、更新ポリシーは、ルート マップ、配布リスト、およびフィルタ リストで設定します。

ピア グループを定義してグループに近隣を追加すると、そのピア グループに割り当てた更新ポリシーはグループ内のすべての近隣に適用されます。それぞれの近隣にポリシーを定義する必要がなくなります。

ピア グループのメンバーは、そのピア グループの設定をすべて継承します。更新ポリシーをオーバーライドするように特定のメンバーを設定することは可能ですが、受信トラフィックに設定されたポリシーに限られます。グループ ポリシーが送信トラフィックに適用される場合は、ポリシーをオーバーライドするようにメンバーを設定することはできません。

BGP ピア グループの更新ポリシーの設定



IPv6 BGP ピア グループとその更新ポリシーを設定するには、次の手順を実行します。

R3 上で以下を実行

```
router bgp 123
   no synchronization
   bgp router-id 3.3.3.3
neighbor interalmap peer-group
   neighbor interalmap remote-as 123
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 peer-group interalmap
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 peer-group interalmap
   neighbor AB01:CD1:123:E:C605:16FF:FE98:0 remote-as 202
   neighbor AB01:CD1:123:E:C605:16FF:FE98:0 ebgp-multihop 5
!
address-family ipv6
   neighbor interalmap activate
   neighbor interalmap route-map 1 out
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 peer-group interalmap
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 peer-group interalmap
exit-address-family
!
ipv6 prefix-list 10 seq 5 permit BC01:BC1:10:A::/64
!
route-map 1 permit 10
   match ipv6 address prefix-list 1 set tag 333
   set metric 273
   set local-preference 312
```

正しいローカル プリファレンス ルートが設定されたことを確認するには、以下の手順に従います。

1 **show bgp ipv6 unicast** コマンドを使用します。

R3 上で以下を実行

```
R3> show bgp ipv6 unicast
```

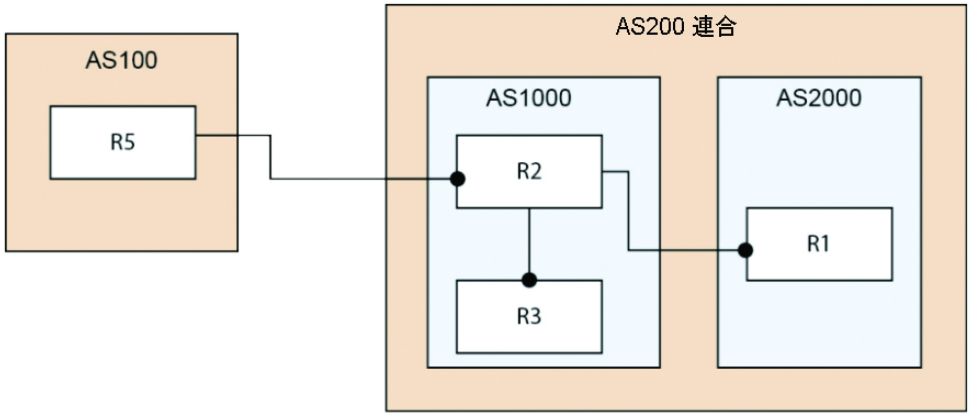
IPv6 アドレス BC01:BC1:10:A::/64 が AS100 から R1 と R2 に送信されたこと、およびメトリックとローカル プリファレンスが対応するルート マップ設定に設定されたことを確認します。

BGP 連合

AS を複数の AS に分割し、これらの AS を単一の連合に割り当てることができます。BGP 連合を実装すると、AS の iBGP メッシュ サイズが小さくなると共に、連合は引き続き単一の AS として外部のピアに通知できます。

連合内のそれぞれの AS はフル メッシュの iBGP を実行すると同時に、連合内の他の AS との間で eBGP 接続を実行します。連合内の eBGP ピアどうしは、iBGP を使用しているかのようにルーティング情報を交換します。このとき、連合はネクスト ホップ、メトリック、ローカル プリファレンスなどの情報を維持します。連合は、外部からは単一の AS として見えます。

BGP 連合の設定



BGP 連合を設定するには、次の手順を実行します。

R1 上で以下を実行

```
router bgp 2000
   bgp log-neighbor-changes
   bgp confederation identifier 200
   bgp confederation peers 1000
   neighbor 2003::1 remote-as 1000
!
address-family ipv4
   neighbor 2003::1 activate
exit-address-family
!
address-family ipv6
   network 3002::/64
   network 4000::/64
```

```
   neighbor 2003::1 activate
exit-address-family
```

R2 上で以下を実行

```
router bgp 1000
   bgp confederation identifier 200
   neighbor 10.0.1.1 remote-as 1000
!
address-family ipv6
   neighbor 10.0.1.1 activate
exit-address-family
```

R3 上で以下を実行

```
router bgp 1000
   bgp confederation identifier 200
   bgp confederation peers 2000
   neighbor 10.0.1.2 remote-as 1000
   neighbor 3001::1 remote-as 2000
   neighbor 5000::1 remote-as 100
   neighbor 5000::1 update-source X2
!
address-family ipv6
   neighbor 10.0.1.2 activate
   neighbor 3001::1 activate
   neighbor 5000::1 activate
exit-address-family
```

R5 上で以下を実行

```
router bgp 100
   bgp router-id 5.5.5.5
   bgp log-neighbor-changes
   neighbor 2002::1 remote-as 200
!
address-family ipv6
   network 6666::6/128
   network 7777::7/128
   neighbor 2002::1 activate
exit-address-family
```

R5 が通知した以下のルートをR1、R2、R3 が学習できることを確認します。

`6666::6/128` および `7777::7/128s`

R2 と R1 が直接接続されていないにもかかわらず、R2 が R1 から以下のルートを学習できることを確認します。

`3002::/64` および `4000::/64`

メモ：IPv6 BGP 設定データおよび IPv6 BGP ルートは 「Terminate and Stay Resident」(TSR) ファイルにダンプされます。

メモ：IPv6 BGP では ZebOS のデバッグ インターフェースを使用します。すべてのデバッグ スイッチの既定の設定はクローズです。CLI のコンソールで **debug** コマンドを入力すると該当するデバッグ スイッチがオープンします。

D

SonicWall サポート

有効なメンテナンス契約が付属する SonicWall 製品をご購入になったお客様や、トライアル バージョンをお持ちのお客様は、テクニカル サポートを利用できます。

サポート ポータルには、問題を自主的にすばやく解決するために使用できるセルフヘルプ ツールがあり、24 時間 365 日ご利用いただけます。サポート ポータルにアクセスするには、https://www.sonicwall.com/ja-jp/support に移動します。

サポート ポータルでは、次のことができます。

- ナレッジ ベースの記事や技術文書を閲覧する。
- ビデオ チュートリアルを視聴する。
- MySonicWall にアクセスする。
- SonicWall のプロフェッショナル サービスに関して情報を得る。
- SonicWall サポート サービスおよび保証に関する情報を確認する。
- トレーニングや認定プログラムに登録する。
- テクニカル サポートやカスタマー サービスを要求する。

SonicWall サポートへの連絡方法は、https://www.sonicwall.com/ja-jp/support/contact-support をご覧ください。

このドキュメントについて

凡例

警告：物的損害、けが、または死亡に至る可能性があることを示しています。

注意：手順に従わないとハードウェアの破損やデータの消失が生じるおそれがあることを示しています。

重要、メモ、ヒント、モバイル、またはビデオ: 補足情報があることを示しています。

SonicOS 6.5 システム設定
更新日 - 2019 年 9 月
ソフトウェア バージョン - 6.5.4
232-002572-04 Rev A

オープン ソース コード

SonicWall では、該当する場合は、GPL、LGPL、AGPL のような制限付きライセンスによるオープン ソース コードについて、コンピュータで読み取り可能なコピーをライセンス要件に従って提供できます。コンピュータで読み取り可能なコピーを入手するには、"SonicWall Inc." を受取人とする 25.00 米ドルの支払保証小切手または郵便為替と共に、書面による要求を以下の宛先までお送りください。

General Public License Source Code Request
SonicWall Inc. Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035