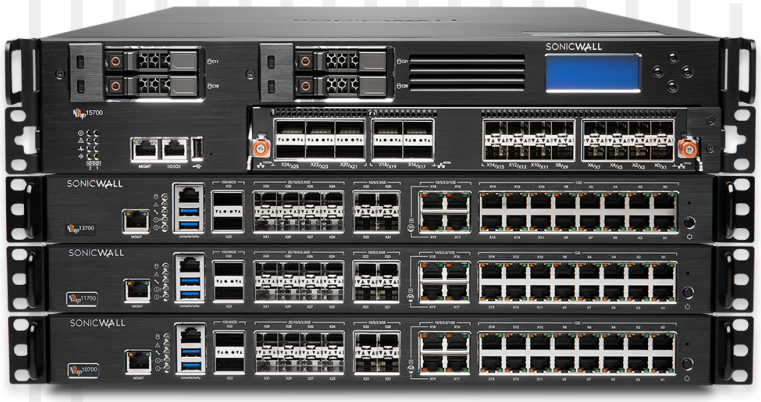
SonicWall Gen 7 NS*sp*シリーズ

SonicWallネットワークセキュリティサービスプラットフォーム™ (NS*sp*) シリーズは、高いポート密度とマルチギガビット速度のインターフェイスを備えた次世代ファイアウォールにより、数百万の接続を処理してゼロデイや高度な脅威からネットワークを保護します。大企業、大学、高等教育機関関、政府機関、MSSP向けに設計されたこの製品は、パフォーマンスを低下させることなく、リアルタイムで攻撃を排除します。信頼性が高く、中断のないサービスを組織に提供できるように設計されています。



NS*sp*の仕様プレビュー。完全なシステム仕様はこちら »

100 GbE	最大100 Gbps	80M
ポート	ファイアウォールインスペクションのスループット	最大接続数 (NSsp 15700)

ハイライト

SonicWall NS*sp*シリーズ

- 高いポート密度
- 100 GbEポート
- オンプレミスおよびクラウドベースのサンドボックスとの統合
- 直感的なユーザーインターフェイスと集中管理機能
- DNSセキュリティ
- レピュテーションベースのコンテンツフィルタリングサービス(CFS 5.0)
- Wi-Fi 6ファイアウォールの管理
- Aruba ClearPassによるネットワークアクセス制御の統合
- 80 Gbps以上の脅威防御スループット
- 冗長電源
- 最大100 Gbpsのファイアウォールインスペクションスループット
- TLS 1.3対応
- 数百万の同時TLS接続に対応
- 低い総所有コスト (TCO)
- SonicWall Capture Labs脅威研究チームが開発

SonicWall Gen 7 NS*sp*シリーズの詳細:

sonicwall.com/NSsp

データシート

エンタープライズクラスのファイアウォール

マネージド/アンマネージドデバイス、ネットワーク、クラウドクラウドワークロード（仮想マシン）ド、SaaSアプリケーション、ユーザー、インターネット速度、暗号化接続の増加に伴ってビジネスが進化すると、これらのうちどれか1つにも対応できないファイアウォールはボトルネックとなります。ファイアウォールは力の源となるべきであり、弱点であってはなりません。

SonicWall NS*sp*ファイアウォールには複数のインターフェイス（100G/40G/25G/10G）が備わっているため、比類のない脅威防御テクノロジーによって数百万の暗号化/非暗号化同時接続を処理することができます。全セッションの70%以上が暗号化されている現在、生産性と情報セキュリティを実現するためにはエンドユーザーの操作性に影響を与えることなくトラフィックを処理し、検査できるファイアウォールを持つことが非常に重要です。

NS*sp* 15700のユニファイドポリシーにより、組織はアクセスポリシーとセキュリティポリシーを単一のインターフェイスで簡単かつ直感的に作成できるようになります。

簡素化された管理方法とレポーティング

ネットワーク活動の継続的な管理、監視、レポート作成は、SonicWall Network Security Managerによって行われます。ここではファイアウォールの動作を管理するための直感的なダッシュボードが提供されるだけでなく、履歴レポートも単一のソースから提供されます。これによって導入と設定も簡単になり、容易に管理できるため、組織は総所有コストを削減して、高い投資収益率を実現することができます。

展開

次世代ファイアウォール（NGFW）

- 単一の画面で管理
- NS*sp*は、SonicWallエコシステムのその他のソリューションと統合可能
- ネットワークを完全に可視化することでアプリケーション、デバイス、ユーザーの動作を確認し、ポリシーを適用して脅威や帯域幅のボトルネックを解消
- クラウドベースのサンドボックスサービスである特許取得済みのRTDMIを搭載したCapture ATP、またはオンプレミスのマルウェア検出に対応するCapture Security Appliance（CSA）と統合可能

SSL/TLSのディープパケットインスペクション(DPI-SSL)インスペクションで隠れた脅威を検出

- NS*sp*はポートやプロトコルに関係なく、数百万以上の同時接続のTLS/SSLおよびSSHの暗号化通信を検査
- 包含および除外ルールにより、組織の具体的なコンプライアンス要件や法的要件に基づいてカスタマイズ可能
- TLS 1.3までのTLS暗号スイートに対応

セグメンテーションおよびネットワーキング

- 複数のセグメント化されたネットワーク、クラウド、サービス定義にまたがって運用し、複数のデバイスやテナントで固有のテンプレート、デバイスグループおよびポリシーを設定可能
- MSSPは固有のポリシーに沿って、複数の顧客をClean Pipeでサポート可能

マルチインスタンスファイアウォール（NS*sp* 15700のみ）

- マルチインスタンスは次世代のマルチテナンシー
- 各テナントはリソースの枯渇を回避するために専用のコンピューティングリソースで分離
- 物理的および論理的なポート/テナントを装備
- 独立したテナントポリシーと構成管理をサポート
- テナントのバージョン独立性と高可用性（HA）への対応を活用

ワイヤモード機能

- ファイアウォールのハードウェアを迅速かつ中断なしでネットワークに導入できるバイパスモード
- 低リスク、待機時間ゼロのパケットパスを機能的に変更することなく、バイパスモードを拡張するインスペクトモード
- ファイアウォール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在させるセキュアモード
- ファイアウォールの単一スイッチポート経由でミラーリングされたパケットストリームを取得するため、物理的な中間挿入が不要になるタップモード

高度な脅威からの保護

- 様々なソリューションを通じて世界各地の15万人以上のお客様にご利用いただいているSonicWall Capture Advanced Threat Protection™（ATP）は、1営業日あたり1,200以上の新しい形態のマルウェアの発見および阻止に貢献
- NS*sp*はCapture Security Appliance（CSA）と連携して、Real-Time Deep Memory Inspection™（RTDMI）を使用したオンプレミスのサンドボックスにより未知の脅威を検出してブロック

Capture Cloud Platform

- SonicWallのCapture Cloud Platformは、クラウドベースの脅威防御とネットワーク管理のほか、レポートと分析の機能をあらゆる規模の組織に提供

コンテンツフィルタリングサービス

- 要求されたウェブサイトを、数百万の評価済みURL、IPアドレス、ウェブサイトを含むクラウド上の巨大なデータベースと比較
- 個人やグループの識別情報または時間帯に基づいてサイトへのアクセスを許可または拒否するポリシーを作成および適用可能。
- レピュテーションベースのコンテンツフィルタリングサービス（CFS 5.0）は、93のWebカテゴリをカバーする包括的なコンテンツフィルタリングにより、インターネット利用ポリシーの適用を可能にし、不適切、非生産的、違法の可能性があるWebコンテンツへの内部アクセスを制御します。レピュテーションベースのコンテンツフィルタリングは、URLのセキュリティリスクを予測するレピュテーションスコアを提供します。

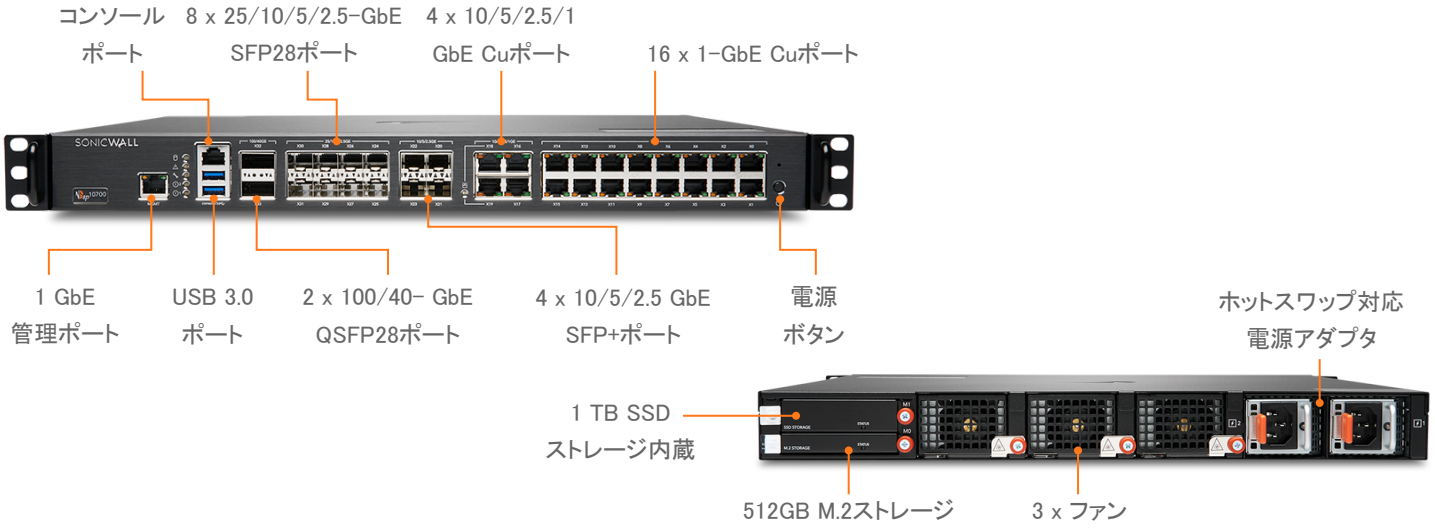
侵入防止システム（IPS）

- 設定可能な高性能ディープパケットインスペクションエンジンを提供することにより、ウェブ、電子メール、ファイル転送、Windowsサービス、DNSなど主要なネットワークサービスの保護を拡張
- アプリケーションの脆弱性を保護するだけでなく、ワーム、トロイの木馬、スパイウェア、バックドアなどの悪用からも保護
- 拡張可能なシグネチャ言語により、新たに発見されたアプリケーションやプロトコルの脆弱性を予測するプロアクティブな防御
- SonicWall IPSは、業界をリードするSonicWallの分散執行型手法（DEA）により、新しい攻撃に対するシグネチャの維持と更新にかかるコストと時間を軽減

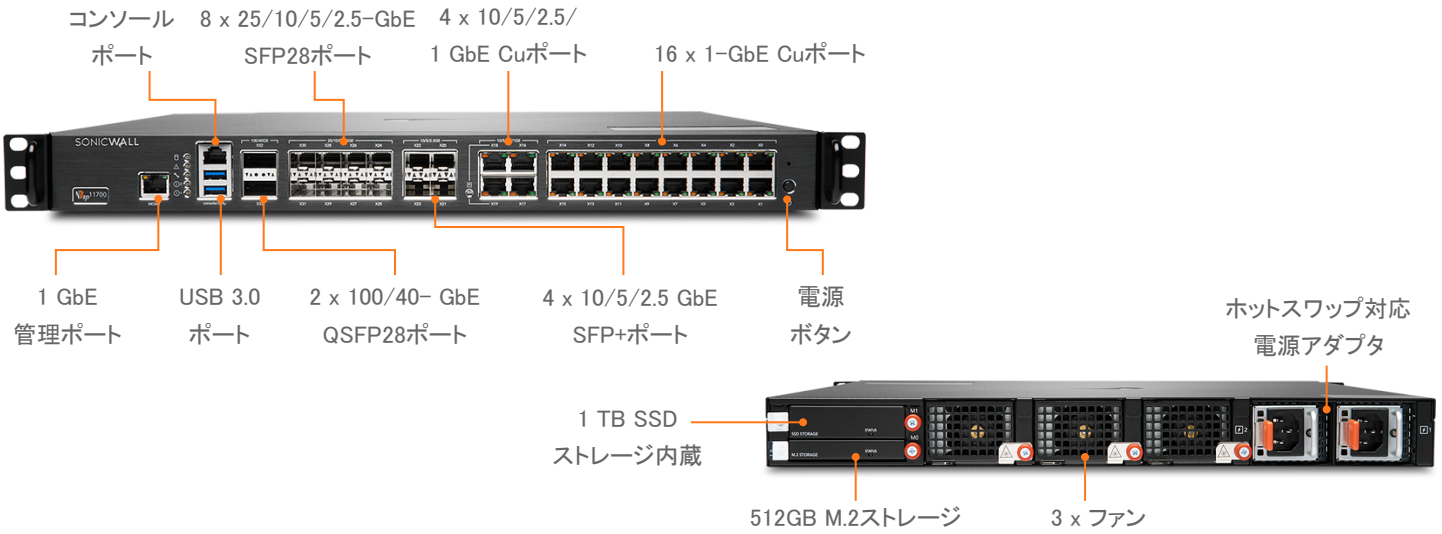
IoTおよびアプリケーション制御

- NSspはアプリケーション制御を通じて何千ものアプリケーションをカタログ化し、それらのトラフィックを監視して異常な動作を検出

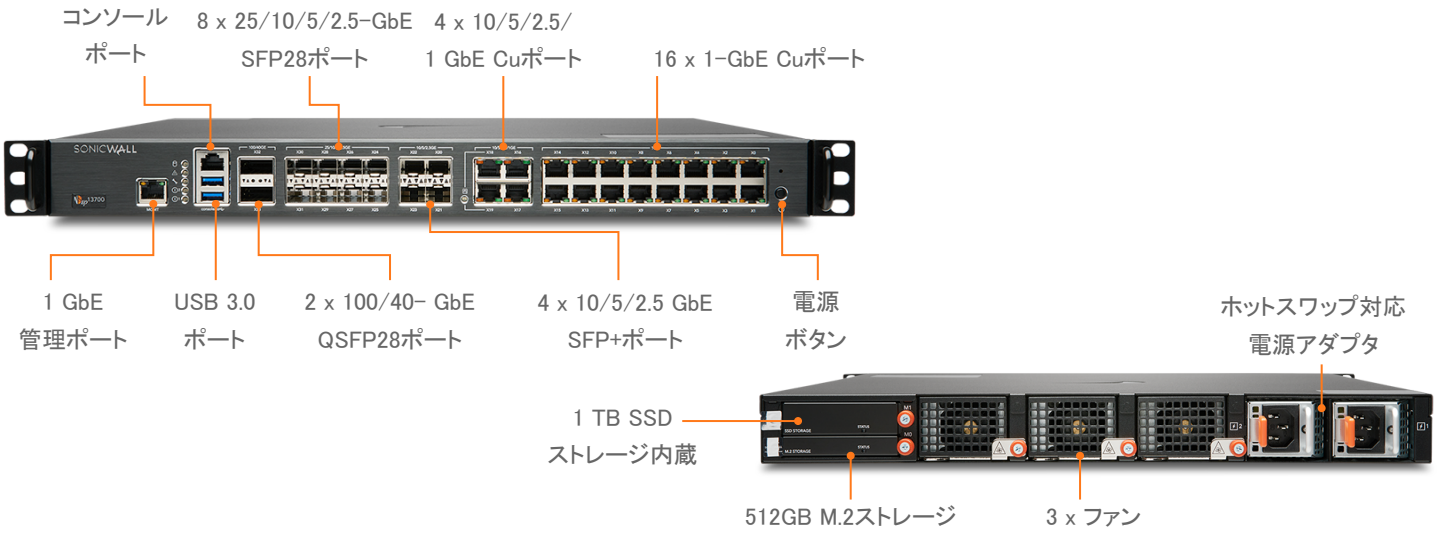
NSsp 10700



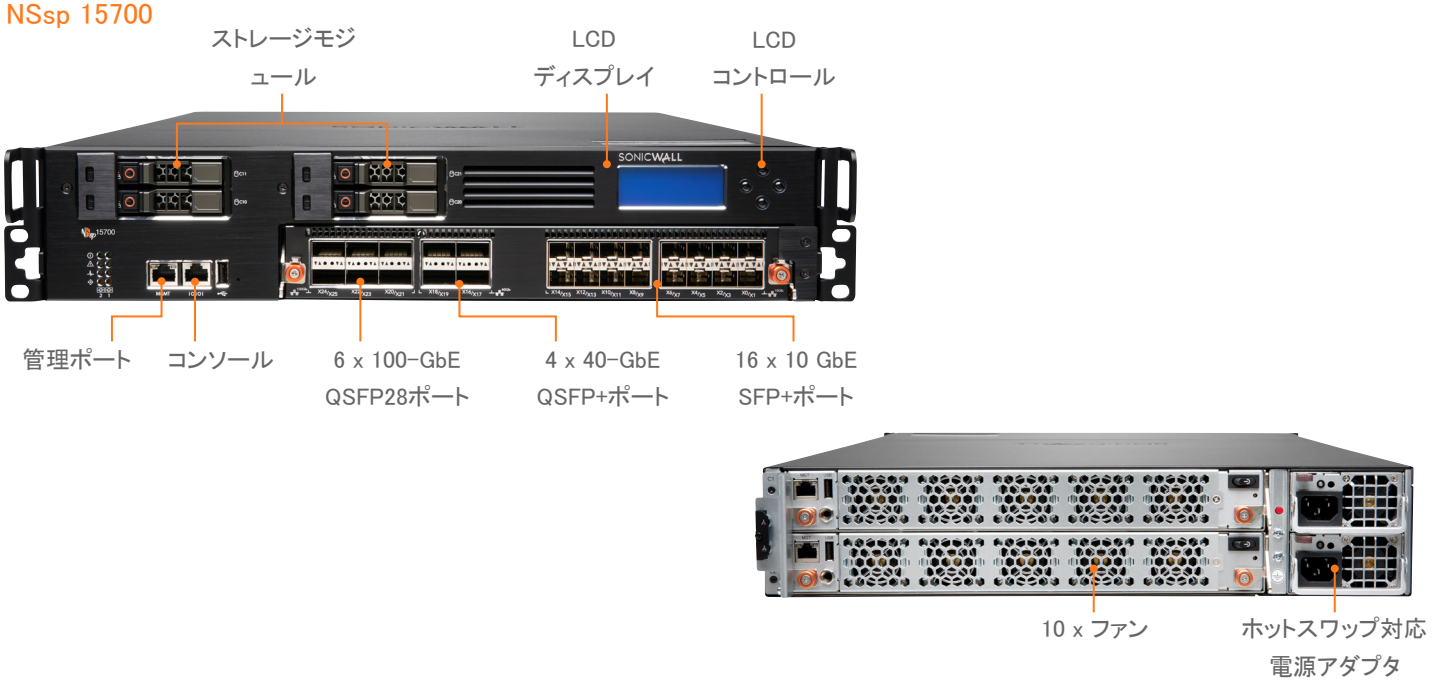
NSsp 11700



NSsp 13700



NSsp 15700



SonicWall NSspシリーズ仕様

ファイアウォールの概要	NSsp 10700	NSsp 11700	NSsp 13700	NSsp 15700
オペレーティングシステム	SonicOS 7.0.1	SonicOS 7.0.1	SonicOS 7.0.1	SonicOSX 7.0.1
インターフェイス	2x100/40-GbE QSFP28、 8x25/10/5/2.5-GbE SFP28 4x10G/5G/2.5G/1G (SFP+)、 4 x 10G/5G/2.5G/1G (Cu); 16 x 1GbE (Cu) 2 USB 3.0、1 コンソール、 1 管理ポート	2x100/40-GbE QSFP28、 8x25/10/5/2.5-GbE SFP28 4x10G/5G/2.5G/1G (SFP+)、 4 x 10G/5G/2.5G/1G (Cu); 16 x 1GbE (Cu) 2 USB 3.0、1 コンソール、 1 管理ポート	2x100/40-GbE QSFP28、 8x25/10/5/2.5-GbE SFP28、 4x10/5/2.5-GbE SFP+、 4x10/5/2.5/1-GbE Cu、 16x1-GbE 2 USB 3.0、1 コンソール、 1 管理ポート	6 x 100-GbE QSFP28、 4 x 40-GbE QSFP+、 16 x 10 GbE SFP+ 3 USB 3.0、1 コンソール、 1 管理ポート
合計ストレージ	1.5TB	1.5TB	1.5TB	2 x 480 GB SSD
管理手段	CLI、SSH、Web UI、REST API			
SSOユーザー数	100,000			
サポート対象のアクセスポイント数 (最大)	512	512	512	512
ログ機能	Analytics、ローカルログ、Syslog、IPFIX、NetFlow			

ファイアウォール/ VPNパフォーマンス	NSsp 10700	NSsp 11700	NSsp 13700	NSsp 15700
ファイアウォールインスペクションの スループット[1]	42 Gbps	47 Gbps	60 Gbps	105 Gbps
脅威防御のスループット[2]	28 Gbps	37 Gbps	45.5 Gbps	82 Gbps
アプリケーションインスペクションの スループット[2]	30 Gbps	44 Gbps	57 Gbps	86 Gbps
IPSのスループット[2]	28 Gbps	37 Gbps	48 Gbps	76.5 Gbps
TLS/SSLインスペクションと復号化の スループット (DPI SSL)[2]	10 Gbps	11.5 Gbps	16.5 Gbps	21 Gbps
VPNのスループット[3]	22.5 Gbps	26.7 Gbps	29 Gbps	32 Gbps
接続数/秒	280,000	280,000	280,000	800,000
最大接続数 (SPI)	15,000,000	20,000,000	25,000,000	40,000,000
最大接続数 (DPI)	12,000,000	17,000,000	22,000,000	40,000,000
最大接続数 (DPI SSL)	1,500,000	1,750,000	2,000,000	4,000,000

VPN	NSsp 10700	NSsp 11700	NSsp 13700	NSsp 15700
サイト間VPNトンネル数	6,000	12,000	12,000	25,000
IPSec VPNクライアント数 (最大)	2000 (6000)	2000 (6000)	2000 (6000)	2000 (10000)
SSL VPNライセンス数 (最大)	100 (3000)	100 (3000)	100 (3000)	256 (3000)
暗号化/認証	DES、3DES、AES (128、192、256ビット)/MD5、 SHA (1,256,384,512) Suite B暗号化		DES、3DES、AES (128、192、256ビット)/MD5、SHA-1、 Suite B暗号化	
キー交換	Diffie Hellmanグループ1、2、5、14v			
ルートベースVPN	スタティックRIP、OSPF、BGP			
証明書のサポート	Verisign、Thawte、Cybertrust、RSA Keon、Entrust、SonicWall-to-SonicWall VPN用のMicrosoft CA、SCEP			
VPN機能	Dead Peer Detection、DHCP Over VPN、IPSec NATトラバーサル、 冗長VPNゲートウェイ、ルートベースVPN			
Global VPNクライアントのサポート対象 プラットフォーム	Microsoft® Windows 11、Windows 10(64ビット、32ビット)			
NetExtender	Microsoft Windows Vista 32/64ビット、Windows 7、Windows 8.0 32/64ビット、 Windows 8.1 32/64ビット、Mac OS X 10.4+、Linux FC3+/Ubuntu 7+/OpenSUSE			
Mobile Connect	Apple® iOS、Mac OS X、Google® Android™、Kindle Fire、Chrome、Windows 8.1 (Embedded)			

ネットワーク	NSsp 10700	NSsp 11700	NSsp 13700	NSsp 15700
マルチインスタンスファイアウォール	なし	なし	なし	ハードウェアあたりの 最大テナント数:12
IPアドレスの割り当て	スタティック (DHCP、PPPoE、L2TP、PPTPクライアント)、内部DHCPサーバー、DHCPリレー			

SonicWall NSspシリーズ仕様

ネットワーク	NSsp 10700	NSsp 11700	NSsp 13700	NSsp 15700
NATモード	1対1、多対1、1対多、フレキシブルNAT（重複IP）、PAT、トランスペアレントモード			
論理VLANおよびトンネルインターフェイス（最大）	1024			
ワイヤモード	–	–	–	あり
ルーティングプロトコル	BGP4、OSPF、RIPv1/v2、スタティックルート、ポリシーベースのルーティング	BGP4、OSPF、RIPv1/v2、スタティックルート、ポリシーベースのルーティング	BGP4、OSPF、RIPv1/v2、スタティックルート、ポリシーベースのルーティング	BGP、OSPF、RIPv1/v2、スタティックルート、ポリシーベースのルーティング
QoS	帯域幅の優先度、最大帯域幅、保証帯域幅、DSCPマーキング、802.1e（WMM）			
認証	LDAP（複数ドメイン）、XAUTH/RADIUS、TACACS+、SSO、Radiusアカウント管理NTLM、内部ユーザーデータベース、2FA、Terminal Services、Citrix、Common Access Card（CAC）		LDAP（複数ドメイン）、XAUTH/RADIUS、SSO、Novell、内部ユーザーデータベース、Terminal Services、Citrix、Common Access Card（CAC）	
ローカルユーザーデータベース	4,000	4,000	4,000	5,000
VoIP	フルH323-v1-5、SIP			
準拠標準	TCP/IP、UDP、ICMP、HTTP、HTTPS、IPSec、ISAKMP/IKE、SNMP、DHCP、PPPoE、L2TP、PPTP、RADIUS、IEEE 802.3			
FIPS 140-2準拠	保留中	保留中	保留中	あり
認定標準	ICSAエンタープライズファイアウォール、ICSAアンチウイルス、IPv6/USGv6			
認定（進行中）	コモンクライテリアNDPPファイアウォール（VPNとIPS）			
高可用性	ステートフル同期によるアクティブ/パッシブ			

ハードウェア	NSsp 10700	NSsp 11700	NSsp 13700	NSsp 15700
電源	2x350W	2x350W	2x350W	デュアル、冗長、1,200W
ファン	3（取り外し可能）	3（取り外し可能）	3（取り外し可能）	10
冗長電源	100～240 VAC、50～60 Hz			
最大消費電力（W）	155.3	155.3	181.2	834.4
総発熱量	529.57 BTU	529.57 BTU	617.89 BTU	2845.3 BTU
フォームファクタ	1Uラックマウント型	1Uラックマウント型	1Uラックマウント型	2Uラックマウント型
寸法	43 x 46 x 4.5 cm（16.9 x 18.1 x 1.8インチ）	43 x 46 x 4.5 cm（16.9 x 18.1 x 1.8インチ）	43 x 46 x 4.5 cm（16.9 x 18.1 x 1.8インチ）	68.6 x 43.8 x 8.8 cm
重量	9.1 Kg	9.1 Kg	9.1 Kg	26 Kg
WEEE重量	11 Kg	11 Kg	11 Kg	30.1 Kg
出荷時の重量	14.9 Kg	14.9 Kg	14.9 Kg	37.3 Kg
環境（動作/保管）	32°～105°F（0°～40°C）/-40°～158°F（-40°～70°C）			
湿度	0-90% R.H（結露無きこと）	0-90% R.H（結露無きこと）	0-90% R.H（結露無きこと）	10～95%（結露無きこと）

規制	NSsp 10700	NSsp 11700	NSsp 13700	NSsp 15700
規制モデル番号	1RK54-118	1RK54-119	1RK54-118	2RK05-0FE
主な規制	FCCクラスA, CE（EMC、LVD、RoHS）、C-Tick, VCCIクラスA、MSIP/KCCクラスA、UL、cUL、TUV/GS、CB、UL Mexico CoC、WEEE、REACH、ANATEL、BSMI	FCCクラスA, CE（EMC、LVD、RoHS）、C-Tick, VCCIクラスA、MSIP/KCCクラスA、UL、cUL、TUV/GS、CB、UL Mexico CoC、WEEE、REACH、ANATEL、BSMI	FCCクラスA, CE（EMC、LVD、RoHS）、C-Tick, VCCIクラスA、MSIP/KCCクラスA、UL、cUL、TUV/GS、CB、UL Mexico CoC、WEEE、REACH、ANATEL、BSMI	FCCクラスA、ICESクラスA、CE（EMCクラスA、LVD、RoHS）、C-Tick、VCCIクラスA、MSIP/KCCクラスA、UL、cUL、TUV/GS、CB、ULによるメキシコDGNへの通知、WEEE、REACH、ANATEL、BSMI

[1] テスト方法：最大パフォーマンスはRFC 2544（ファイアウォール）に基づいています。実際のパフォーマンスはネットワークの状態と使用するサービスによって異なる場合があります。

[2] 脅威防御/ゲートウェイAV/アンチスパイウェア/IPSのスループットは、業界標準のKeysight HTTPパフォーマンステストツールを使用して測定しています。テストは、複数のポートペアでの複数のフローで行われました。脅威防御のスループットは、ゲートウェイAV、アンチスパイウェア、IPSおよびアプリケーションの制御を有効にして測定しています。

[3] VPNのスループットは、RFC 2544に準拠したAESGMAC16-256暗号を使用したパケットサイズ1418バイトのUDPトラフィックにより測定されています。仕様、機能、使用の可否については、いずれも変更される場合があります。

SonicOSXおよびSonicOSの機能概要

ファイアウォール

- ステートフルパケットインスペクション（SPI）
- Reassembly-Free Deep Packet Inspection（RFDPI）
- DDoS攻撃の防御（UDP/ICMP/SYNフラッド）
- IPv4/IPv6対応
- リモートアクセスのための生体認証
- DNSプロキシ
- REST API
- SonicWallスイッチの統合
- SonicWall Wi-Fi 6 APの統合

統合セキュリティポリシー

- レイヤー4からレイヤー7のルールを統合したユニファイドポリシー：
  - 送信元/送信先IP/ポート/サービス
  - アプリケーションの制御
  - CFS/ウェブフィルタリング
  - シングルパスセキュリティサービスの実施
  - IPS/GAV/AS/Capture ATP
- ルール管理：
  - クローニング
  - シャドウルール分析
  - セル内編集
  - グループ編集
- 表示管理
  - 使用済み/未使用ルール
  - アクティブ/非アクティブルール
  - セクション

TLS/SSL/SSHの復号化とインスペクション

- TLS 1.3
- TLS/SSL/SSH対応のディープパケットインスペクション
- オブジェクト、グループまたはホスト名の包含/除外
- SSL制御
- ゾーンまたはルールごとのきめ細かなDPI-SSL制御
- SSL/TLSおよびSSHの復号化ポリシー

Capture Advanced Threat Protection[1]

- Real-Time Deep Memory Inspection（RTDMI）
- クラウドベースのマルチエンジン分析
- 仮想サンドボックス
- ハイパーバイザレベルの分析
- フルシステムエミュレーション
- 広範な種類のファイルの検査
- 自動および手動による送信
- リアルタイムの脅威インテリジェンスの更新
- 正体が判明するまでブロック
- Capture Client統合

侵入防止[1]

- シグネチャベースのスキャン
- Aruba ClearPassによるネットワークアクセス制御の統合
- シグネチャの自動更新
- 双方向インスペクション
- きめ細かなIPSルール機能
- GeoIPの適用
- 動的リストによるボットネットのフィルタリング
- 正規表現マッチング

アンチマルウェア[1]

- ストリームベースのマルウェアスキャン
- 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
- 双方向インスペクション
- ファイルサイズの制限なし
- クラウドのマルウェアデータベース

アプリケーションの識別[1]

- アプリケーションの制御
- アプリケーションの帯域幅管理
- カスタムアプリケーションのシグネチャ作成
- データ漏洩防止
- NetFlow/IPFIXによるアプリケーションレポート機能
- 包括的なアプリケーションシグネチャのデータベース

トラフィックの可視化と分析

- ユーザーアクティビティ
- アプリケーション/帯域幅/脅威の使用状況
- クラウドベースの分析

HTTP/HTTPS Webコンテンツフィルタリング[1]

- URLフィルタリング
- プロキシの回避
- キーワードによるブロック
- レピュテーションベースのコンテンツフィルタリングサービス（CFS 5.0）
- DNSフィルタリング
- ポリシーベースのフィルタリング（除外/包含）
- HTTPヘッダーの挿入
- 帯域幅管理CFS評価カテゴリ
- コンテンツフィルタリングクライアント

VPN

- VPNの自動プロビジョニング
- サイト間接続型IPSec VPN
- SSL VPNおよびIPSecクライアントリモートアクセス
- 冗長VPNゲートウェイ
- iOS、Mac OS X、Windows、Chrome、AndroidおよびKindle FireのMobile Connect
- ルートベースVPNスタティック、（OSPF、RIP、BGP）

ネットワーク

- マルチインスタンスファイアウォール（NS*sp* 15700のみ）
- PortShield
- ジャンボフレーム
- Path MTU Discovery
- 強化されたログ機能
- VLANトランキング
- ポートミラーリング
- レイヤ2のQoS
- ポートセキュリティ
- 動的ルーティング（RIP/OSPF/BGP）
- ポリシーベースのルーティング（ToS/メトリックおよびECMP）
- NAT
- DHCPサーバー
- 帯域幅の管理
- リンクアグリゲーション（スタティック、ダイナミック）
- ポート冗長性
- 状態同期によるA/P高可用性
- インバウンド/アウトバウンド負荷分散機能
- 高可用性 – 状態同期によるアクティブ/スタンバイ
- ワイヤ/仮想ワイヤモード、タップモード、NATモード
- 非対称ルーティング

VoIP

- よりきめ細かなQoS制御
- 帯域幅の管理
- VoIPトラフィックに対するDPI
- H.323ゲートキーパーおよびSIPプロキシサポート

管理および監視

- Web GUI
- コマンドラインインターフェイス（CLI）

管理および監視（続き）

- ゼロタッチ登録とプロビジョニング
- Rest API
- SonicExpressモバイルアプリのサポート
- SNMPv2/v3
- SonicWall Network Security Manager（NSM）による集中管理とレポート機能[1]
- ログ機能
- Netflow/IPFixによるエクスポート
- クラウドベースの構成バックアップ
- アプリケーションと帯域幅の可視化
- IPv4とIPv6の管理

[1] サブスクリプションの追加が必要

最適なSonicWallファイアウォールをお選びください

www.sonicwall.com/firewalls

SonicWallについて

SonicWallは、安定した、拡張可能で、シームレスなサイバーセキュリティを提供することにより、誰もがリモート/モバイルで危険にさらされながら仕事をするという超分散化時代のビジネスの現実に対処します。未知の領域を探求し、リアルタイムの可視性を提供しながら経済の大躍進を実現しているSonicWallは、サイバーセキュリティ業務上の課題を解決して世界中の企業や政府、中小企業をサポートします。詳しくはwww.sonicwall.comをご覧ください。

SonicWall Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
詳細は当社ウェブサイトをご覧ください。
www.sonicwall.com