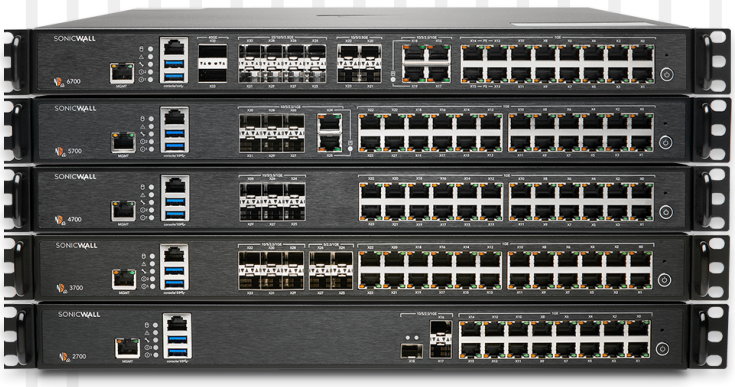
SonicWall Gen 7 NSaシリーズ

SonicWall Gen 7（第7世代）Network Security Appliance（NSa）の次世代ファイアウォール（NGFW）は、このクラスで最も低い総所有コストで、中堅企業から大企業向けに業界をリードするパフォーマンスを提供します。

侵入防止、VPN、アプリケーション制御、マルウェア分析、URLフィルタリング、DNSセキュリティ、Geo-IPおよびボットネットサービスなどの総合的なセキュリティ機能を備えたこの製品は、ボトルネックになることなく高度な脅威から境界を保護します。

ハイライト

- 1 RU – フォームファクタ
- 40G/25G/10G/5G/2.5G/1Gポートに対応
- 数ギガビットの脅威・マルウェア分析スループット
- 優れたTLSパフォーマンス（セッションとスループット）
- 拡張可能なストレージ
- 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
- エンタープライズ向けインターネット境界防御
- 最新のGeneration 7 SonicOSをサポート
- Secure SD-WAN機能
- 直感的なユーザーインターフェイスと集中管理機能
- TLS 1.3対応
- クラス最高のコストパフォーマンス
- SonicWall Capture Labs脅威研究チームが開発
- ネットワークを構築しやすい高密度ポート
- SonicWallスイッチ、SonicWaveアクセスポイント、Capture Client統合
- 冗長電源



Gen 7 NSaシリーズの仕様プレビュー。
完全なシステム仕様はこちら »

最大 19 Gbps	最大 800万	40G/25G/10G/ 5G/2.5G/1G
脅威防御 スループット	接続数	ポート

データシート

複数の40 GbEおよび10 GbEポートを含む高密度ポートを特長とするこのソリューションは、高可用性やデュアル電源によって、ネットワークおよびハードウェアの冗長性をサポートします。

SonicWall Gen 7（第7世代）Network Security Appliance（NSa）の次世代ファイアウォール（NGFW）は、このクラスで最も低い総所有コストで、中堅企業から大企業向けに業界をリードするパフォーマンスを提供します。

侵入防止、VPN、アプリケーション制御、マルウェア分析、URLフィルタリング、DNSセキュリティ、Geo-IP/ボットネットサービスなどの総合的なセキュリティ機能を備えたこの製品は、ボトルネックになることなく高度な脅威から境界を保護します。

Gen 7 NSaシリーズは、最新のハードウェアコンポーネントを使用してゼロから構築されており、暗号化されたトラフィックであっても、数ギガビットの脅威防御スループットを実現できるように設計されています。複数の40 GbEおよび10 GbEポートを含む高密度ポートを特長とするこのソリューションは、高可用性やデュアル電源によって、ネットワークおよびハードウェアの冗長性をサポートします。

Generation 7 – SonicOS 7およびセキュリティサービス

Gen 7 NSaシリーズには、最新のユーザーインターフェイス、直感的なワークフロー、そしてユーザー重視の設計原理を実現するためにゼロから構築された新しいオペレーティングシステムSonicOS 7.0が搭載されています。SonicOS 7は、企業レベルのワークフローを促進するために設計された複数の機能を提供します。容易なポリシー設定、ゼロタッチ導入、柔軟な管理を通じて、企業はセキュリティと業務効率の両方を改善することができます。

Gen 7 NSaシリーズは、SD-WAN、ダイナミックルーティング、レイヤ4～7の高可用性、高速VPN機能など、高度なネットワーク機能をサポートしています。さらに、ファイアウォールやスイッチ機能が統合されているだけでなく、スイッチとアクセスポイントの両方を管理できるシングルペインオブグラス（単一画面）インターフェイスを提供しています。

今日だけでなく、未来の高度なサイバー攻撃を軽減するために構築されたGen 7 NSaシリーズでは、SonicWallの高度なファイアウォールセキュリティサービスにアクセスできるため、企業のITインフラ全体を保護することができます。Cloud Application Security、クラウドベースのサンドボックスサービスCapture Advanced Threat Protection（ATP）、特許取得済みのReal-Time Deep Memory Inspection（RTDMI™）、Reassembly-Free Deep Packet Inspection（RFDPI）などのソリューションやサービス（TLS 1.3を含むすべてのトラフィックに対応）は、ゼロデイや暗号化された脅威など、最もステルス性が高く危険なマルウェアに対して包括的なゲートウェイププロテクションを提供します。

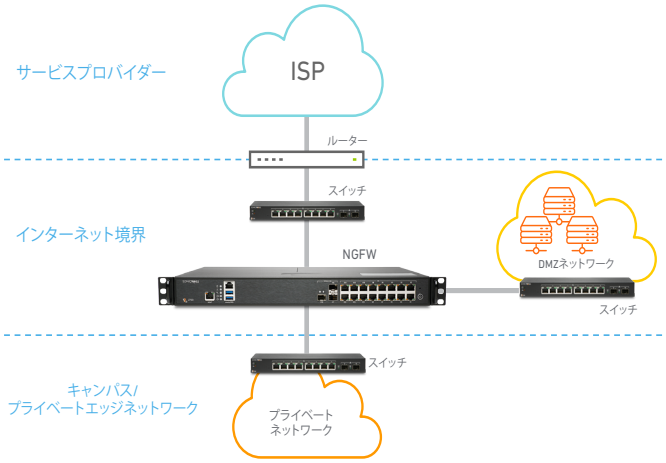
導入

Gen 7 NSaシリーズには、中堅企業や分散型企業向けに2つの主要な導入オプションがあります。

インターネット境界での導入

この標準導入オプションでは、Gen 7 NSaシリーズのNGFWが、インターネット上の悪意あるトラフィックからプライベートネットワークを保護し、以下のメリットを提供します:

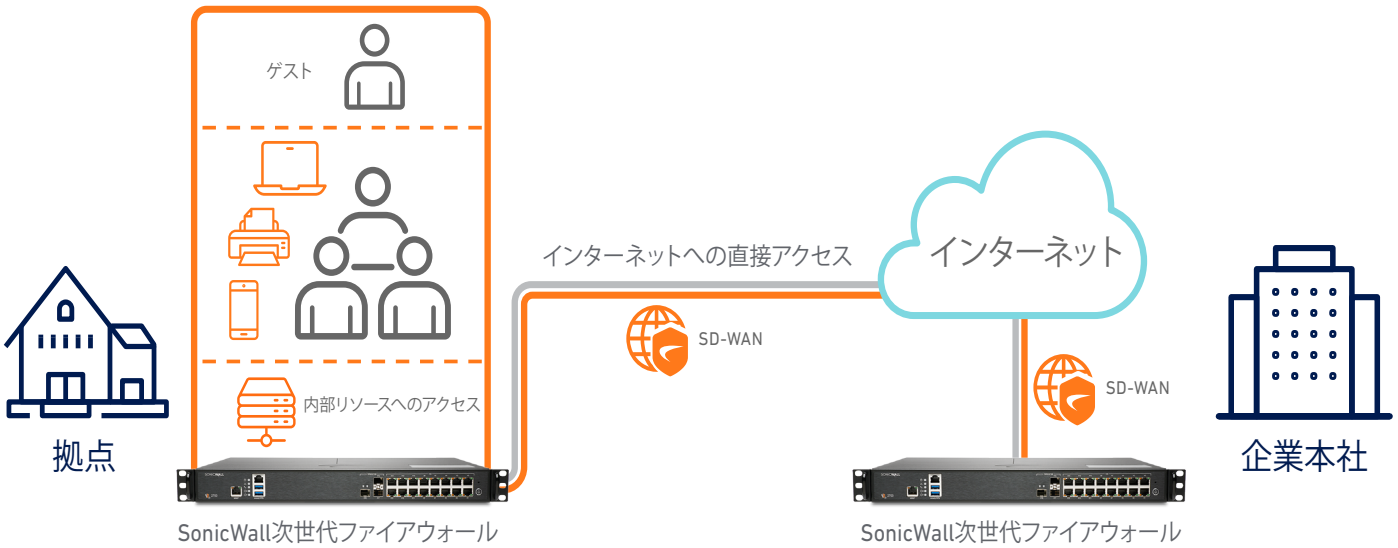
- クラス最高の性能とポート密度（40 GbE、10 GbE接続を含む）を備えた実証済みのNGFWソリューションの導入
- 性能に影響を与えることなく、TLS 1.3を含む暗号化されたトラフィックを可視化して検査し、検出回避手法を用いたインターネット上の脅威をブロック
- マルウェア分析、Cloud App Security、URLフィルタリング、レピュテーションサービスなどの統合されたセキュリティで企業を保護
- 高度なセキュリティ機能とネットワーク機能を備えた統合型NGFWソリューションでスペースとコストを削減
- 直感的なシングルペインオブグラス（単一画面）インターフェイスによる集中管理システムを使用して複雑さを軽減し、効率性を最大化



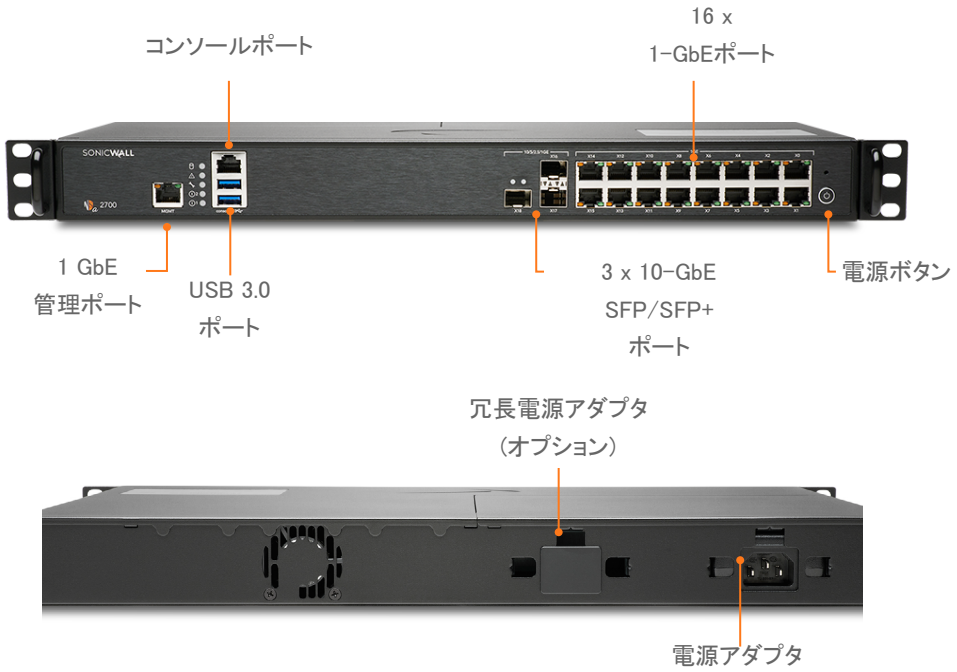
中堅企業および分散型企業

SonicWall Gen 7 NSaシリーズは、SD-WANに対応し、集中管理が可能なため、中堅企業や分散型企業に最適です。この導入オプションによる組織のメリット:

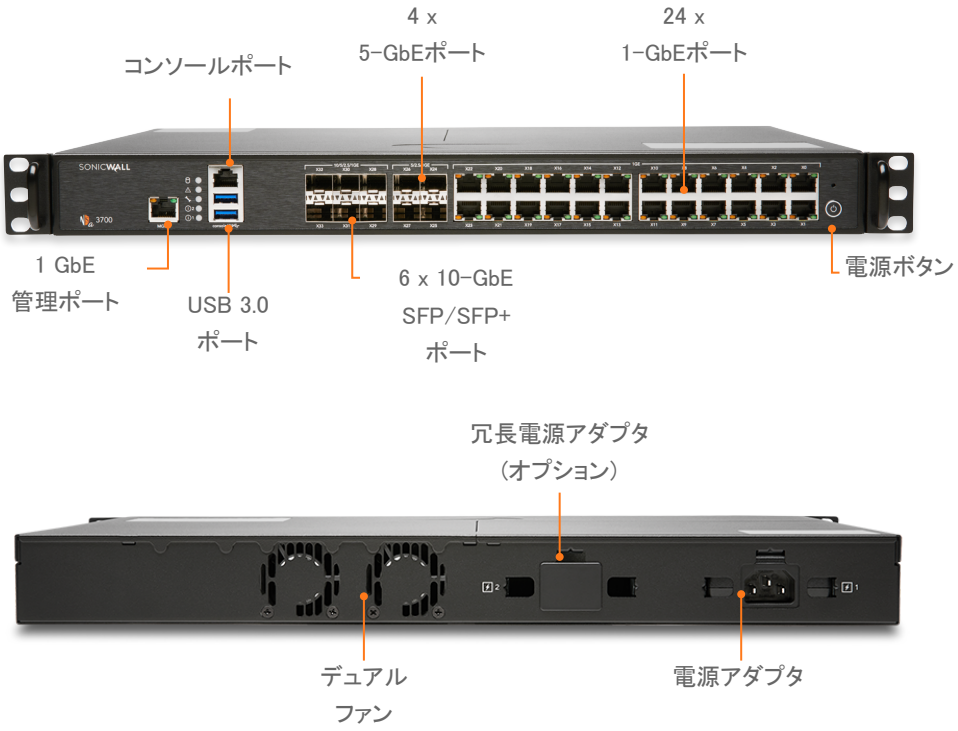
- マルチギガビットのパフォーマンスで脅威分析を行うNGFWに投資することにより、刻々と変化する将来の脅威情勢からネットワークを保護
- 企業本社でバックホールする代わりに、ダイレクトで安全なインターネットアクセスを分散型拠点に提供
- 分散型拠点は企業本社やパブリッククラウドの社内リソースに安全にアクセスできるようになるため、アプリケーションの遅延を大幅に低減可能
- TLS 1.3などの暗号化プロトコルを使用する脅威を自動的にブロックし、最先端の攻撃からネットワークを保護
- 直感的なシングルペインオブグラス（単一画面）インターフェイスによる集中管理システムを使用して複雑さを軽減し、効率性を最大化
- 高密度ポート（40 GbE、10 GbE接続を含む）を活用し、分散型企業とワイドエリアネットワークをサポート



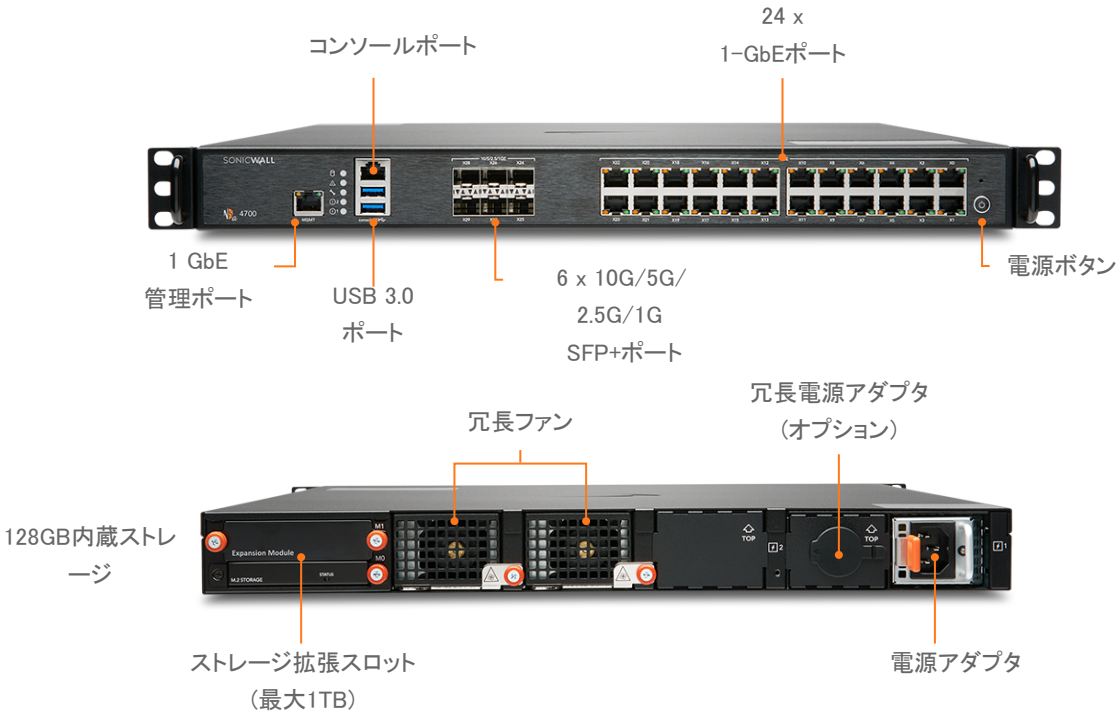
NSa 2700



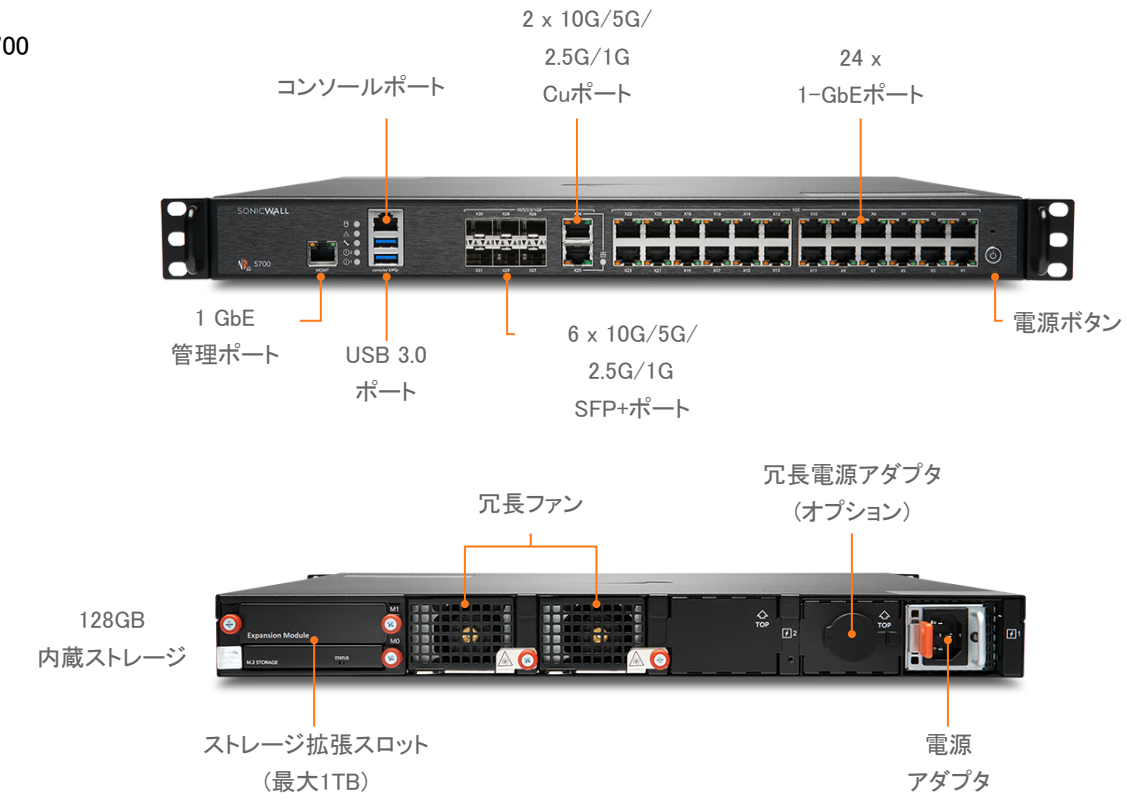
NSa 3700



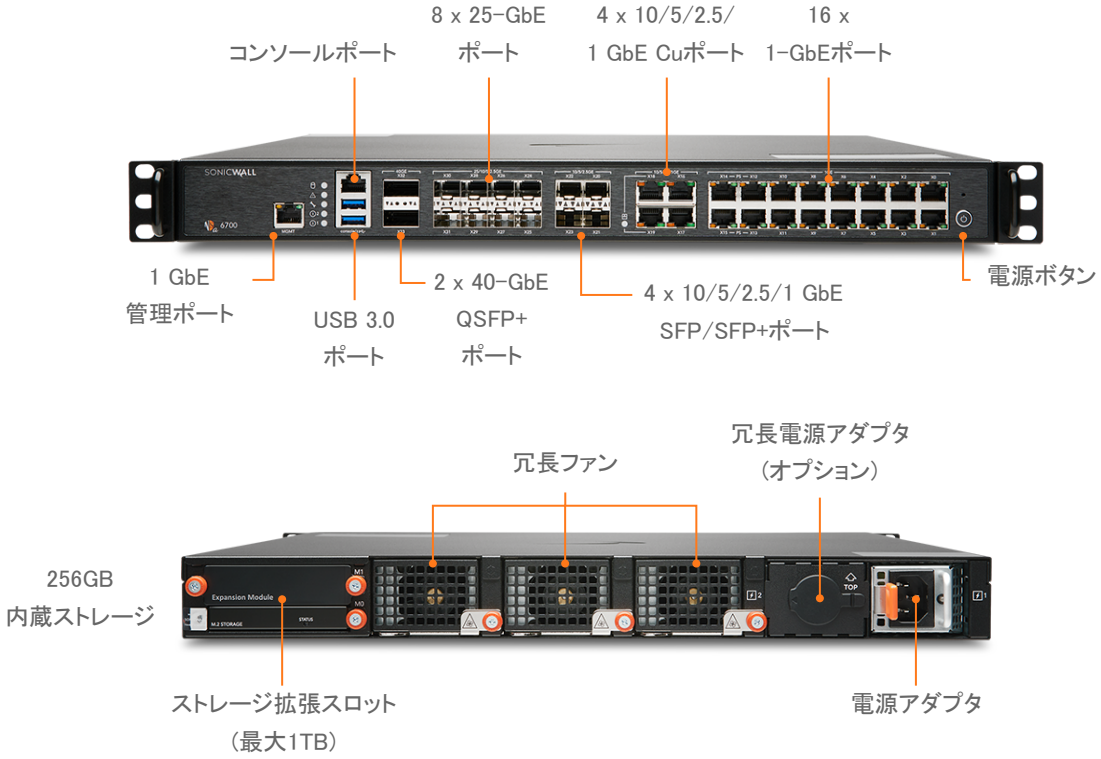
NSa 4700

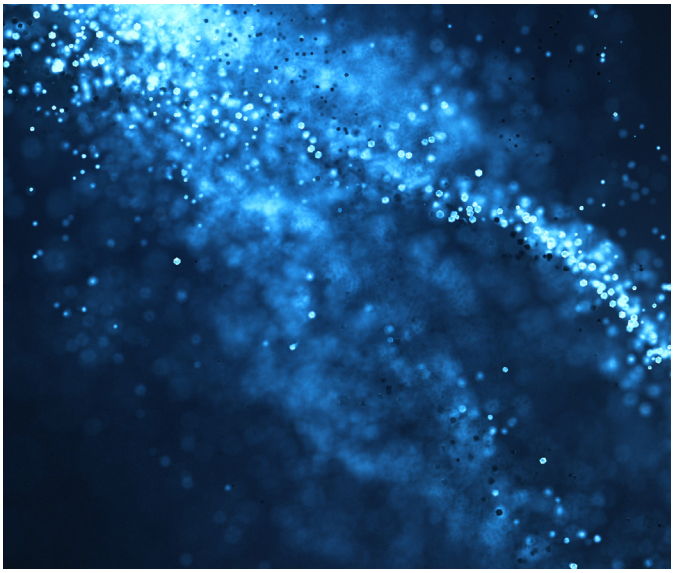


NSa 5700



NSa 6700





パートナーが提供するサービス

SonicWall ソリューションの計画、導入、最適化に関して支援をお求めですか？ SonicWallアドバンスド・サービス・パートナーは、お客様にワールドクラスの専門的なサービスをご提供いたします。詳細はこちら：

www.sonicwall.com/PES

Gen 7 NSaシリーズのシステム仕様

ファイアウォール	NSa 2700	NSa 3700	NSa 4700	NSa 5700	NSa 6700
オペレーティングシステム			SonicOS 7		
インターフェイス	16 x1GbE、3 x10G SFP+、2 USB 3.0、1 コンソール、1 管理ポート	24 x 1GbE、6 x10G SFP+、4 x 5G SFP+、2 USB 3.0、1 コンソール、1 管理ポート	6 x 10G/5G/2.5G/1G (SFP+)、24 x 1GbE Cu 2 USB 3.0、1 コンソール、1 管理ポート	6 x 10G/5G/2.5G/1G (SFP+); 2x 10G/5G/2.5G/1G (Cu); 24 x 1GbE Cu 2 USB 3.0、1 コンソール、1 管理ポート	2 x 40G、8 x 25G、4 x10G/5G/2.5/1G 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
ストレージ	64 GB M.2	128 GB M.2	128GB	128GB	256 GB M.2
拡張	ストレージ拡張スロット (最大256GB)	ストレージ拡張スロット (最大256GB)	ストレージ拡張スロット (最大1TB)	ストレージ拡張スロット (最大1TB)	ストレージ拡張スロット (最大1TB)
論理VLANおよびトンネルインターフェイス (最大)	256	256	512	512	512
SSOユーザー数	40,000	40,000	50,000	50,000	70,000
サポート対象のアクセスポイント数 (最大)	512	512	512	512	512
ファイアウォール/VPNパフォーマンス					
ファイアウォールインスペクションのスループット[1]	5.2 Gbps	5.5 Gbps	18 Gbps	28 Gbps	36 Gbps
脅威防御のスループット[2]	3.0 Gbps	3.5 Gbps	9.5 Gbps	15 Gbps	19 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]	3.6 Gbps	4.2 Gbps	11 Gbps	18 Gbps	20 Gbps
IPSのスループット[2]	3.4 Gbps	3.8 Gbps	10 Gbps	17 Gbps	20 Gbps
アンチマルウェアインスペクションのスループット[2]	2.9 Gbps	3.5 Gbps	9.5 Gbps	16 Gbps	18.5 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]	800 Mbps	850 Mbps	5 Gbps	7 Gbps	9 Gbps
IPSec VPNのスループット[3]	2.10 Gbps	2.2 Gbps	11 Gbps	15 Gbps	19 Gbps
接続数/秒	21,000	22,000	115,000	228,000	228,000
最大接続数 (SPI)	1,500,000	2,000,000	4,000,000	5,000,000	8,000,000
DPI-SSL最大接続数	125,000	150,000	350,000	350,000	750,000
最大接続数 (DPI)	500,000	750,000	2,000,000	3,500,000	6,000,000
VPN					
サイト間VPNトンネル数	2,000	3,000	4,000	6,000	6,000
IPSec VPNクライアント数 (最大)	50 (1000)	50 (1000)	500 (3000)	2000 (4000)	2000 (6000)
SSL VPNライセンス数 (最大)	2 (500)	2 (500)	2 (1000)	2 (1500)	2 (1500)
暗号化/認証	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				
サポート対象のGlobal VPNクライアントプラットフォーム	Windows 10		Microsoft® Windows Vista 32/64ビット、Windows 7 32/64ビット、Windows 8.0 32/64ビット、Windows 8.1 32/64ビット、Windows 10		
NetExtender	Windows 10およびLinux		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、Android、Kindle Fire、Chrome OS、Windows 10		Apple® iOS、Mac OS X、Google® Android™、Kindle Fire、Chrome、Windows 8.1 (Embedded)		
セキュリティサービス					
ディープパケットインスペクションサービス	ゲートウェイアンチウィルス、アンチスパイウェア、侵入防止、DPI SSL				

Gen 7 NSaシリーズのシステム仕様

ファイアウォール	NSa 2700	NSa 3700	NSa 4700	NSa 5700	NSa 6700
コンテンツフィルタリングサービス（CFS）	HTTP URL、HTTPS IP、キーワードとコンテンツのスキャン、ファイルタイプ（ActiveX、Java、プライバシーのCookieなど）に基づく包括的なフィルタリング				
Comprehensive Anti-Spam Service	あり				
アプリケーションの可視化	あり				
アプリケーションの制御	あり				
Capture Advanced Threat Protection（ATP）	あり				
ネットワーク					
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				
NATモード	1対1、1対多、多対1、多対多、フレキシブルNAT（重複IP）、PAT、トランスペアレントモード				
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				
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）				
ローカルユーザーデータベース	1000	1000	2500	2500	3200
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	あり	あり	保留中	保留中	保留中
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）				
Common Access Card（CAC）	あり				
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					
フォームファクタ	1Uラックマウント型				
ファン	1	2	2（取り外し可能）	2（取り外し可能）	3（取り外し可能）
電源	60W	90W	350W	350W	350W
最大消費電力（W）	21.5	36.3	108.1	128.1	139.2
冗長電源	100～240 VAC、50～60 Hz				
総発熱量	73.32 BTU	123.78 BTU	368.62 BTU	436.82 BTU	474.67 BTU
寸法	43 x 32.5 x 4.5 cm（16.9 x 12.8 x 1.8 インチ）	43 x 32.5 x 4.5 cm（16.9 x 12.8 x 1.8 インチ）	43 x 46.5 x 4.5 cm（16.9 x 18.1 x 1.8 インチ）	43 x 46.5 x 4.5 cm（16.9 x 18.1 x 1.8 インチ）	43 x 46.5 x 4.5 cm（16.9 x 18.1 x 1.8 インチ）
重量	4.0 kg（8.8ポンド）	4.6 kg（10.2ポンド）	7.8 Kg	7.8 Kg	8.1 Kg
WEEE重量	4.2 kg（9.3ポンド）	4.8 kg（10.6ポンド）	9.6 Kg	9.6 Kg	9.9 Kg
出荷時の重量	6.4 kg（14.1ポンド）	7 kg（15.4ポンド）	13.5 Kg	13.5 Kg	13.8 Kg
環境（動作/保管）	32° ～105° F（0° ～40° C）/-40° ～158° F（-40° ～70° C）				
湿度	5～95%（結露無きこと）	5～95%（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）	0-90% R.H（結露無きこと）
規制					
規制モデル番号	1RK51-109	1RK52-110	1RK53-115	1RK53-116	1RK54-118
主要な準拠規制	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				

[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。

SonicOS 7.0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
- APIのフルサポート
- SonicWallスイッチの統合
- SonicWall Wi-Fi 6 APの統合
- SD-WANの拡張性
- SD-WANのユーザビリティウィザード[1]
- 接続の拡張性（SPI、DPI、DPI SSL）
- ダッシュボードの改良[1]
- デバイス表示の改良
- 上位トラフィックとユーザー概要
- 脅威の分析情報
- 通知センター

TLS/SSL/SSHの復号化とインスペクション

- TLS 1.3（セキュリティを強化）[1]
- 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、ホスト名の包含/除外
- SSL制御
- CFSによるDPI-SSLの強化
- ゾーンまたはルールごとのきめ細かなDPI-SSL制御
- Capture advanced threat protection[2]
- Real-Time Deep Memory Inspection（RTDMI）
- クラウドベースのマルチエンジン分析[2]
- 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[2]
- 正体が判明するまでブロック
- Capture Client[2]

侵入防止[2]

- 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[2]

- 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
- クラウドマルウェア

アプリケーションの識別[2]

- アプリケーション制御
- 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[2]

- 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
- アプリケーション制御可能な統合ポリシーモデル
- コンテンツフィルタリングクライアント

VPN

- セキュアSD-WAN
- 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（OSPF、RIP、BGP）

ネットワーク

- 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（SonicWallスイッチ）
- 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）
- SonicWallワイヤレスコントローラー
- 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
- 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
- L2ブリッジモード、Nativeブリッジモード、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
- Common Access Card（CAC）のサポート

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、監視、サポート

- Capture Security Appliance（CSa）のサポート
- Capture Threat Assessmentt（CTA）v2.0
- 新しいデザインまたはテンプレート
- 業界と世界平均の比較
- 新しいUI/UX、直感的な機能レイアウト[1]
- ダッシュボード
- デバイス情報、アプリケーション、脅威
- トポロジ表示
- シンプルなポリシー作成と管理
- ポリシー/オブジェクト使用状況統計[1]
- 使用済 vs 未使用
- アクティブ vs 非アクティブ
- 静的データのグローバル検索
- ストレージのサポート[1]

SonicOS 7.0の機能概要（続き）

管理、監視、サポート（続き）

- 内部および外部ストレージの管理[1]
- WWAN USBカードのサポート（5G/LTE/4G/3G）
- Network Security Manager（NSM）のサポート
- Web GUI
- コマンドラインインターフェイス（CLI）
- ゼロタッチ登録とプロビジョニング
- CSCシンプルレポート機能[1]
- SonicExpressモバイルアプリのサポート
- SNMPv2/v3
- SonicWall Global Management System（GMS）による集中管理とレポート機能[2]
- レポート作成および分析用API
- 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
- BlueCoatセキュリティ分析プラットフォーム
- アプリケーションと帯域幅の可視化
- IPv4とIPv6の管理
- CD管理画面
- カスケード接続のスイッチを含むDell N-SeriesおよびX-Seriesスイッチ管理

デバッグと診断

- 強化されたパケット監視
- UIでのSSHターミナル

ワイヤレス

- SonicWave APクラウドおよびファイアウォール管理
- WIDS/WIPS
- 不正APの防止
- 高速ローミング（802.11k/r/v）
- 802.11sメッシュネットワーキング
- 自動チャネル選択
- RFスペクトル分析
- フロアプラン表示
- トポロジ表示
- バンドステアリング
- ビームフォーミング
- エアタイム（通信時間）の公平性
- Bluetooth Low Energy（BLE）
- MiFiエクステンダー
- RFの機能強化と改善
- ゲスト巡回割り当て

[1] SonicOS 7.0で利用可能な新機能
[2] サブスクリプションの追加が必要

SonicWall Gen 7 NSaシリーズの詳細

www.sonicwall.com/products/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