SONICWALL

SonicWallミドルレンジ Gen 8 NSaシリーズ

分散型大企業や学校のキャンパス向けのクラス最高の脅威防御

SonicWallの最新のミドルレンジ次世代ファイアウォールであるNetwork Security Appliance（NSa）2800および3800は、このクラスで最も低い総所有コストで、業界をリードする脅威防御パフォーマンスを中堅企業や大企業に提供します。ファイアウォールは、シンプルな集中制御型のファイアウォール管理、ゼロトラストの実現、マネージドファイアウォールサービスを選択できる柔軟性の高いライセンスの提供が可能な脅威防御ソリューションの基盤です。

Gen8ファイアウォールは侵入防止、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提供し、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。

NSa 3800

NSa 2800

ハイライト

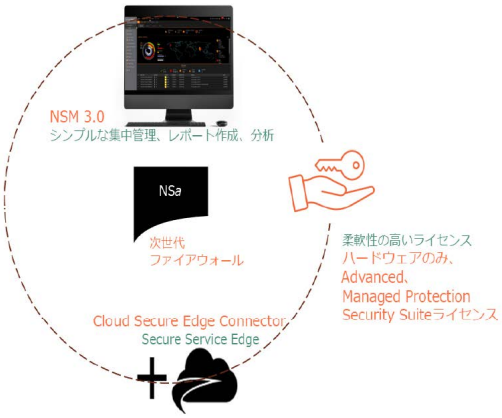
- フォームファクタ：1Uラックマウント型
- 数ギガビットの脅威・マルウェア分析スループット
- 優れたTLSパフォーマンス（セッションとスループット）
- クラス最高のコストパフォーマンス
- 拡張可能なストレージ
- 高度なDNSフィルタリング
- レピュテーションベースのコンテンツフィルタリングサービス（CFS 5.0）
- Network Security Managerによるシンプルな集中型のSaaSとオンプレミス管理
- Wi-Fi 6ファイアウォールの管理
- SonicPlatformのサポート
- エンタープライズ向けインターネット境界防御
- Secure SD-WAN機能
- TLS 1.3対応
- 柔軟性の高いライセンス：ハードウェアのみ、Essential、Advanced、Managed Protection Service Suites
- SonicWall Capture Labs脅威研究チームが開発
- SonicWallスイッチ、SonicWaveアクセスポイント、Capture Client統合
- Cloud Secure Edge Connectorのサポート

Gen 8 NSa2800および3800の仕様プレビュー。
完全なシステム仕様はこちら »

最大 8 Gbps	最大 12 Gbps	最大 300万
脅威防御スループット	ファイアウォールスループット	接続数

データシート

Gen 8 NSaファイアウォールは、脅威防御、集中管理、レポート作成と分析、セキュリティとマネージドサービスのオプション、Secure Service Edge（SSE）の統合が含まれた包括的なソリューションによって強力なセキュリティを促進します。



ハードウェア

NSa 2800および3800は、最新のハードウェアコンポーネントを使用して構築されており、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します。複数の10GbEポートを含む高密度ポートを特長とするこのファイアウォールソリューションは、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。

アーキテクチャ

Gen 8 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新しいオペレーティングシステムである、SonicOS8が搭載されています。SonicOS8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。

NSa 2800および3800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。

脅威防御とセキュリティサービス

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Gen8 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である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。

柔軟性の高いライセンスには、ハードウェアのみ、Advanced、Managed Protection Service Suite（MPSS）があり、固有のニーズに対応できます。MPSSは、ファイアウォール向けのマネージドサービスでリソースを強化します。

Cloud Secure Edge Connectorの統合は、ファイアウォールの先にあるプライベートアプリケーションへの安全なアクセスを提供します。ユーザーとデバイスは、ゼロトラストフレームワークに従ってアプリケーションにアクセスできます。

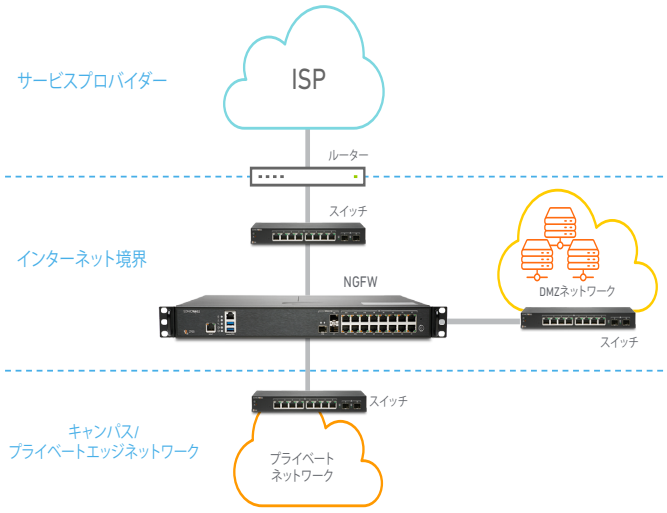
導入

Gen 8 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 8 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:

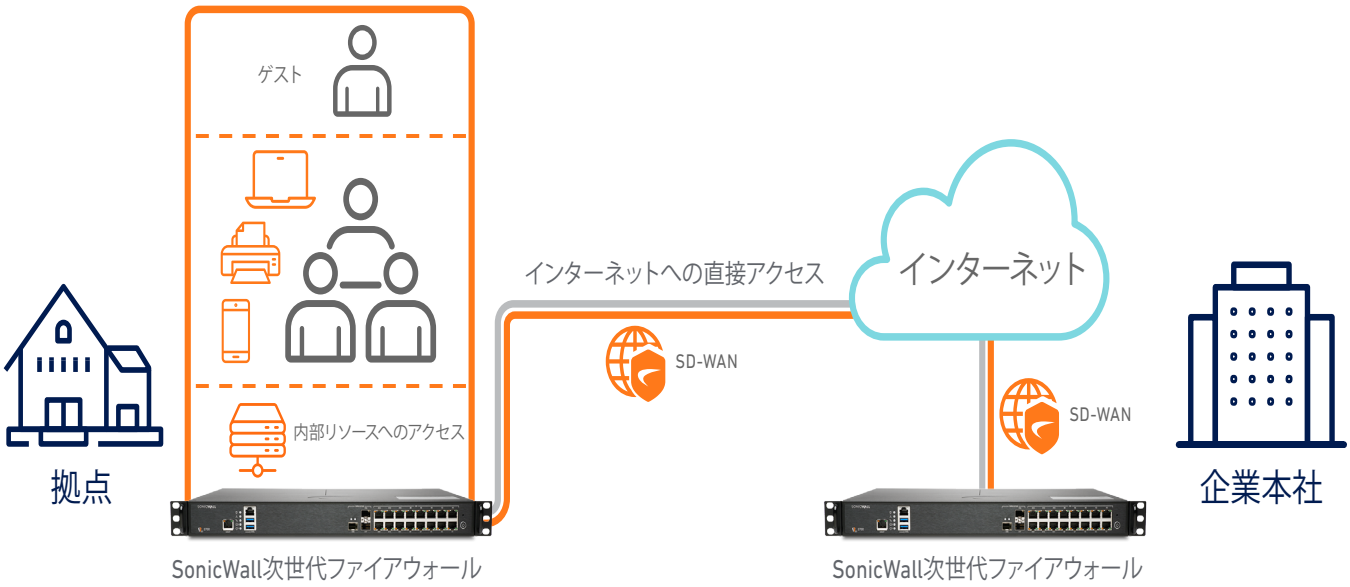
- クラス最高の性能を備えた実証済みのNGFWソリューションの導入
- 性能に影響を与えることなく、TLS 1.3を含む暗号化されたトラフィックを可視化して検査し、検出回避手法を用いたインターネット上の脅威をブロック
- マルウェア分析、Cloud App Security、URLフィルタリング、レピュテーションサービスなどの統合されたセキュリティで企業を保護
- 高度なセキュリティ機能とネットワーク機能を備えた統合型NGFWソリューションでスペースとコストを削減
- 直感的なシングルペインオブグラス(単一画面)インターフェイスによる集中管理システムを使用して複雑さを軽減し、効率性を最大化



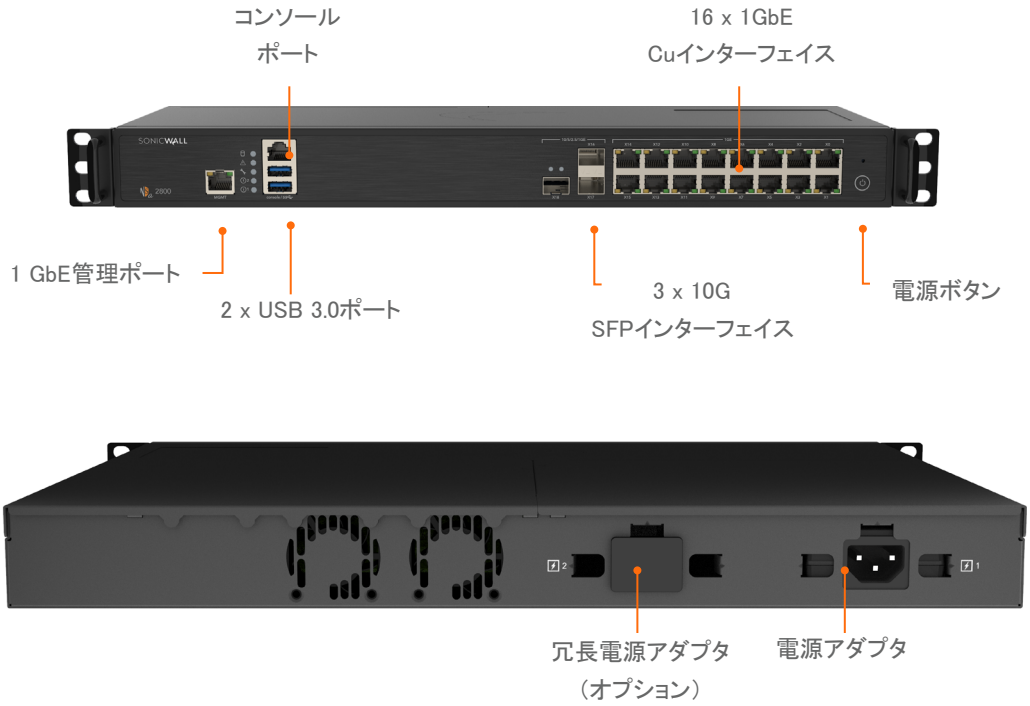
中堅企業および分散型企業

SonicWall Gen 8 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は次のとおりです。

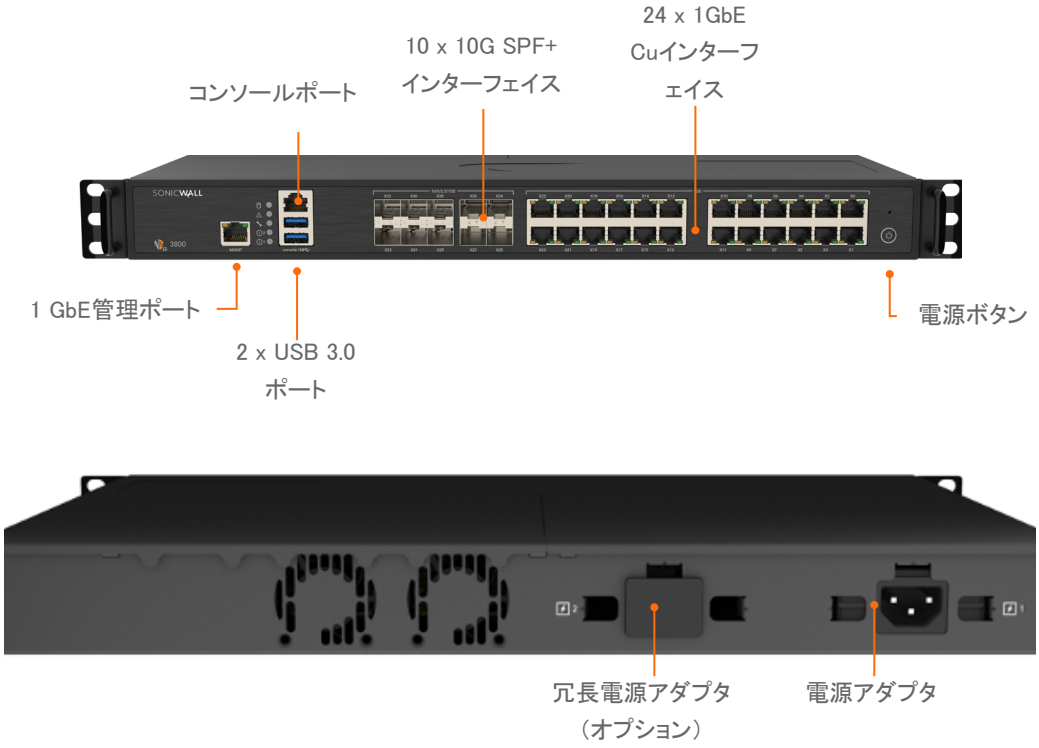
- マルチギガビットのパフォーマンスで脅威分析を行うNGFWに投資することにより、刻々と変化する将来の脅威情勢からネットワークを保護
- 企業本社でバックホールする代わりに、ダイレクトで安全なインターネットアクセスを分散型拠点に提供
- 分散型拠点は企業本社やパブリッククラウドの社内リソースに安全にアクセスできるようになるため、アプリケーションの遅延を大幅に低減可能
- TLS 1.3などの暗号化プロトコルを使用する脅威を自動的にブロックし、最先端の攻撃からネットワークを保護
- 直感的なシングルペインオブグラス(単一画面)インターフェイスによる集中管理システムを使用して複雑さを軽減し、効率性を最大化
- 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 2800



NSa 3800



Gen 8 NSaシリーズのシステム仕様

ファイアウォール	NSa 2800	NSa 3800
オペレーティングシステム	SonicOS 8	
インターフェイス	16 x 1GbE、 3 x 10G SFP+、 2 x USB 3.0、 1 x コンソール、 1 x 管理ポート	24 x 1GbE、 6 x 10G SFP+、 4 x 5G SFP+、 2 x USB 3.0、 1 x コンソール、 1 x 管理ポート
ストレージ	128 GB M.2	256 GB M.2
ストレージ拡張スロット	ストレージ拡張スロット（最大512GB）	ストレージ拡張スロット（最大512GB）
集中管理	Network Security Manager（NSM）3.0以降、CLI、SSH、Web UI、REST API	
論理VLANおよびトンネルインターフェイス（最大）	256	256
SAMLシングルサインオンのユーザー数[1]	40,000	40,000
サポート対象のアクセスポイント数（最大）	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[2]	8 Gbps	12 Gbps
脅威防御のスループット3	6 Gbps	8 Gbps
アプリケーションインスペクションのスループット[3]	7 Gbps	9 Gbps
IPSのスループット2	7 Gbps	8 Gbps
アンチマルウェアインスペクションのスループット[3]	6 Gbps	8 Gbps
TLS/SSLインスペクションと復号化のスループット[3]	1.8 Gbps	3 Gbps
IPSec VPNのスループット[4]	5.5 Gbps	8 Gbps
接続数/秒	50,000	90,000
最大接続数（SPI）	2,000,000	3,000,000
最大接続数（DPI）	1,000,000	1,200,000
最大接続数（TLS）	150,000	300,000
VPNおよびZTNA		
サイト間VPNトンネル数	2,000	3,000
IPSec VPNクライアント数（最大）	10（1000）	50（1000）
SSL VPNライセンス数（最大）	2（500）	2（500）
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	Microsoft® Windows 10およびWindows 11	
NetExtender	Microsoft® Windows 10およびWindows 11、Linux	
Mobile Connect	Apple® iOS、Mac OS X、Google® Android™	
Cloud Secure EdgeによるSonicWall Private Access[5]	3 & Freeロイヤルティプログラムの対象	
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、TLS復号化	
コンテンツフィルタリングサービス（CFS）	レピュテーションベースのURLフィルタリング、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	

Gen 8 NSaシリーズのシステム仕様

ファイアウォール	NSa 2800	NSa 3800
Comprehensive Anti-Spam Service	あり	あり
アプリケーションの可視化	あり	あり
アプリケーション制御	あり	あり
Capture Advanced Threat Protection(ATP)	あり	あり
DNSフィルタリング	あり	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	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+、SAML SSO[1]、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
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	
認定標準	申請中:IPv6	
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	
電源	90W	150W
最大消費電力(W)	52.8	102.3W
入力電圧	100～240 VAC、50～60 Hz、4 A	100～240 VAC、50～60 Hz、12.5 A
総発熱量(BTU)	180.01	341
寸法(単位:cm)	43 x 32.5 x 4.5 出荷時:57.5 x 47.5 x 18.5	43 x 32.5 x 4.5 57.5 x 47.5 x 18.5
重量	4.6	4.6
WEEE重量	4.8	4.8
出荷時の重量	7.2	7.2
環境(動作/保管)	0°C～+40°C / −40°C～+70°C	
湿度	5～95%(結露無きこと)	5～95%(結露無きこと)
規制		
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[6]、BSMI	
規制モデル番号	1RK56-11C	1RK57-122

[1] SAMLシングルサインオンは、今後リリース予定のSonicOS 8.1で利用できます。

[2] 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。

[3] 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。

[4] 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。

[5] 3年契約のバンドルに付帯

[6] 今後のステージで利用可能

SonicOS 8.0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、TLS）
- 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TLS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 protection2
- 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 Client2

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
- クラウドのマルウェアデータベース

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

ウェブ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およびZTNA

- 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、AndroidのMobile Connect
- ルートベースVPN（OSPF、RIP、BGP）
- Cloud Secure Edgeによる Secure Private Access

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 8.0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
- SonicPlatformとSonicBot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 8 NSaシリーズの詳細

www.sonicwall.com/products/firewalls

SonicWallについて

SonicWallは、30年以上の実績を誇り、絶えずパートナー企業を重視しているサイバーセキュリティの先駆者です。クラウド、ハイブリッド、従来型ネットワークが混在する環境にリアルタイムでセキュリティを構築、拡張、管理するSonicWallは、世界中のあらゆる組織に専用のセキュリティソリューションを短時間で経済的に提供します。SonicWallは、自社の脅威研究センターのデータに基づいて、巧妙なサイバー攻撃に対するシームレスな保護を提供し、パートナー、お客様、サイバーセキュリティコミュニティに実用的な脅威インテリジェンスを提供します。

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