クラウドサービスや分散型ネットワーク環境のセキュリティ対策に最適

SonicWall NSaシリーズ 中規模向けUTM

■高性能ソリューションにおける最先端の脅威を防止

ハイパフォーマンス 次世代ファイアウォール	高速100/40/25/10GbEポートを搭載。冗長電源および交換可能電源、内蔵ストレージに対応したUTM高密度ポートのファイアウォールを使用してSMBまたはエンタープライズ組織を保護
高度な脅威から保護	SonicWallの特許技術RTDMIテクノロジを使用して、ゼロデイ、ランサムウェア攻撃から防御 Capture ATPにより高度な攻撃からネットワークとデータを保護する
暗号化された 脅威に対する防御	増加する暗号化された通信をスキャンし、サイバー攻撃の脅威からネットワークを保護 TLS / SSLおよびSSHトラフィックをリアルタイムで復号化および検査を実施
継続的な管理と 簡単な設定	クラウド/オンプレのNSM(マネージメントコンソール)と連携し、ネットワークセキュリティの管理、レポート、分析を提供運用しやすいローカライズされたWEBUIを実装
優れた冗長構成機能と コストパフォーマンス	コストパフォーマンスを最小限に抑えるために、すべてのセキュリティサービスを１つのパッケージで提供。さらに1台分のライセンスで冗長ペア構成を実現

■各種機能概要

通信コントロール（APPベースルーティング/SD-WAN）
- アプリケーションベースのルートポリシーで通過パスをコントロール
- SD-WANで優先通信の経路を安定確保
- クラウド管理(NSM)からの操作で複数の装置を一元管理

VPN
- IPSec VPNを使用したサイト間VPN IPv4/IPv6 をサポート
- SSLVPN Client から接続可能(VPNクライアントアプリは複数のOSに対応)

SSLインスペクション
- 通過するSSL暗号化通信をリアルタイムで復号しパケット検査を実施
- 各セキュリティ機能と併用することで暗号化通信に潜む脅威を除去する

ゲートウェイアンチウィルス
- ローカルDB(約20,000)とクラウド上のDB(約4,300万)でワールドワイドのウィルスを除去

アンチスパイウェア
- 約3,000種類のシグネチャを使用して様々なスパイウェアを除去
- シグネチャは世界中のセンサーからリアルタイムで収集した情報から自社開発

侵入検知/防御
- 計30カテゴリ/約5,000種類のクラウド上のDBから日々更新したシグネチャを使用して様々なプラットフォームが持つ脆弱性に対する攻撃から保護
- NetSecOPEN*1 ラボテストにて検知率100%の防御実績

アプリケーションの可視化/コントロール
- 約1,500種類のアプリケーションを識別し、許可、禁止、パケット監視や帯域制御を実現可能

Botnet/地域IPフィルタ
- ハッカーに遠隔操作されたボットネットからの通信を遮断
- 特定の国からのアクセスを制御することが可能

コンテンツフィルタリング
- 計56カテゴリ、約2000万を超えるURLデータベースを保有
- フィッシング対策協議会会員、国内で報告されたフィッシングサイトにも対応

サンドボックス
- 2種類のプレフィルタ、4種類のサンドボックスエンジンによりマルウェアの検知回避を困難にし、メモリの振舞いを監視してCPU脆弱性への攻撃を検知する。複数エンジンの解析精度はICSAラボ*2で検知率100%を実現

■SonicWall NSaシリーズ システム仕様一覧

*1 ネットワークセキュリティに焦点を当てた会員制の非営利団体
*2 ネットワークセキュリティおよび医療向け IT 製品のための主要な独立テスト機関

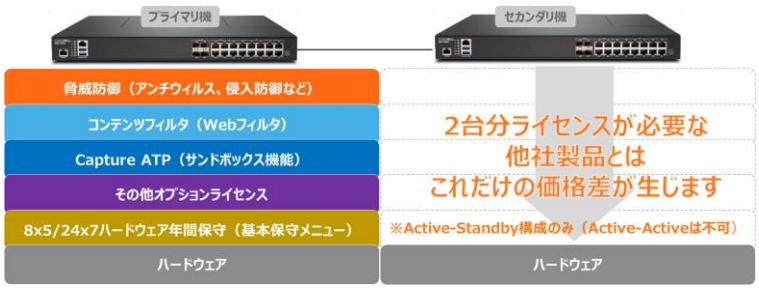
NSaシリーズ	NSa 2700	NSa 3700	NSa4700	NSa 5700	NSa 6700
ファイアウォールスループット（Gbps）	5.2	5.5	18.0	28.0	36.0
脅威保護スループット（Gbps）	**3.0**	**3.5**	**9.5**	**15.0**	**19.0**
DPI-SSLスループット（Gbps）	0.8	0.85	5.0	7.0	9.0
最大接続数(SPI)	1,500,000	2,000,000	4,000,000	5,000,000	8,000,000
最大接続数(DPI)	500,000	750,000	2,000,000	3,500,000	6,000,000
高速インターフェイス	3x 10GbE	6x 10GbE 4x 5GbE	6x 10GbE	8x 10GbE	2x 40GbE 8x 25GbE, 8x 10GbE
総ポート数	19	34	30	32	34

1．メーカー本体がサポートセンターを運営

SonicWallにて採用されたテクニカルサポート社員が高い技術力で速やかな対応を実現

- 日本語での対応（英語対応も可）
- 電話・Webからお手軽にお問い合わせ開始
- 構築業者様やエンドユーザー様から直接お問い合わせ可能
- 設定変更、トラブルシューティングのお問い合わせ
- マネージドセキュリティサービス（MSS）提供会社も利用可能
- 本国開発チームと連携可能な組織体制

2．シングル構成も冗長構成もランニングコストが変わらない



HA（機器の冗長化）を構成した場合、セキュリティライセンス、基本保守契約は1台分の費用で運用可能です。また、プライマリ機設定後、LANケーブルを接続してセカンダリ機の電源を入れると設定は自動でコピーされます。

3．検査するファイルサイズに制限なし

特許技術「RFDPI」を使用してデータ解析を行う為、検査できるファイルサイズの制限がなく、大容量ファイルに隠れる脅威を見逃しません。Windowsファイル共有(CIFS/NetBIOS)をはじめとする幅広いプロトコルを検査できます(約50種類)

4．SonicWall UTMはスループットが落ちにくい

最新の脅威に対抗するためには、UTM の多数のセキュリティ機能をフルに活用しなければなりません。一般的なUTMは、セキュリティ機能を有効化する度に、パフォーマンスが急激に低下すると言われています。スループットを確保するために、一部の機能を犠牲にするケースもあります。SonicWallUTM は、独自のテクノロジーによって、すべてのセキュリティ機能を有効にしても高いパフォーマンスを維持できます。

※ 2023年1月現在
※ 本機能は予告なく変更になる可能性がございます。

SONICWALL®
ソニックウォール・ジャパン株式会社
〒105-0003東京都港区西新橋2-9-1 PMO西新橋9階
https://www.sonicwall.com/jp-ja/