SonicWall Network Security Appliance (NSA) シリーズ

業界で実証された、中規模ネットワークのセキュリティ効果とパフォーマンス

SonicWall Network Security Appliance (NSA) シリーズは、中規模ネットワーク、ブランチオフィス、および分散エンタープライズのための、ハイパフォーマンスセキュリティプラットフォームにおける高度な脅威防御を実現します。次世代ファイアウォールテクノロジーと、特許取得済み * の Reassembly-Free Deep Packet Inspection (RFDPI) エンジンとを、マルチコアアーキテクチャ上で組み合わせた NSA シリーズは、組織に必要なセキュリティ、パフォーマンス、制御を提供します。

優れた脅威防御とパフォーマンス

NSA シリーズの次世代ファイアウォール (NGFW) には、優れた脅威防御を実現する高度なセキュリティテクノロジーが組み込まれています。特許取得済みのシングルパス RFDPI 脅威防御エンジンは、すべてのパケットのすべてのバイトを調べて、インバウンドとアウトバウンドのトラフィックを同時に検査します。NSA シリーズは、クラウドベースの SonicWall Capture マルチエンジンサンドボックスサービスに加え、侵入防止、アンチマルウェア、Web/URL フィルタリングなどのオンボックス機能を活用して、ゼロデイ脅威をゲートウェイで阻止します。大規模なファイルに潜んでいる脅威を検査できない他のセキュリティ製品とは異なり、NSA ファイアウォールはすべてのポートとプロトコルにわたり、あらゆるサイズのファイルをスキャンします。SonicWall NGFW のセキュリティアーキテクチャは、NSS Labs により、5 年間連続で業界最高のセキュリティ効果を持つ技術として評価されています。

また、SonicWall NGFW は、トランスポートやプロトコルに関係なく、TLS/SSL および SSH で暗号化された接続、およびプロキシ不可能なアプリケーションの、完全な復号化とインスペクションを実行することによって、全面的な保護を実現します。ファイアウォールは、すべてのパケット (ヘッダーとデータ) の内部を詳細に検査して、プロトコル違反、脅威、ゼロデイ、侵入、そして定義された基準を検索します。これは、暗号を悪用した隠れた攻撃の検出と防止、暗号化されたマルウェアのダウンロードの阻止、感染の拡大の防止、コマンドとコントロール (C&C) 通信とデータ漏洩の阻止を目的としたものです。包含および除外のルールにより、具体的な組織のコンプライアンス要件や法的要件に基づいて、復号化とインスペクションの対象になるトラフィックを完全に制御してカスタマイズすることができます。

組織のファイアウォールで侵入防止、アンチウイルス、アンチスパイウェア、TLS/SSL 復号化 / インスペクションなどのディープ・パケット・インスペクション機能を有効にすると、ネットワークのパフォーマンスが低下することがよくあり、場合によっては大幅に悪化します。一方、NSA シリーズのファイアウォールは、専用のセキュリティマイクロプロセッサを利用するマルチコアのハードウェアアーキテクチャを採用しています。RFDPI エンジンと組み合わせたこの独自の設計により、他のファイアウォールを使用した場合のようなネットワークパフォーマンスの低下が起こりません。

今日のセキュリティ環境では、外部の機関から提供される脅威の情報のみに頼っているわけにはいきません。このため、SonicWall は社内で独自の Capture Labs 脅威研究チームを 15 年以上前に結成しました。この専門チームは、SonicWall Capture Threat Network 上の 100 万個を超えるセンサーからのデータを収集、分析、調査します。また、SonicWall は業界で連携して進めている取り組みにも参加し、脅威の調査コミュニティと協力して、攻撃と脆弱性のサンプルを収集し、共有しています。こうして共有され

** 米国特許 7,310,815、7,600,257、7,738,380、7,835,361、7,991,723*

導入効果：

優れた脅威防御とパフォーマンス

- 特許を取得した Reassembly-Free Deep Packet Inspection テクノロジー
- オンボックスおよびクラウドベースの脅威防御
- TLS/SSL の復号化およびインスペクション
- 業界で認められたセキュリティの有効性
- マルチコアのハードウェアアーキテクチャ
- 専門の Capture Labs 脅威研究チーム

ネットワークの制御と柔軟性

- 強力な SonicOS オペレーティングシステム
- アプリケーションインテリジェンスおよび制御
- VLAN によるネットワークのセグメント化
- 高速のワイヤレスセキュリティ

簡単な導入、セットアップ、および継続的な管理

- 緊密に統合されたソリューション
- 集中管理
- 複数のハードウェアプラットフォームで一貫したスケーラビリティ
- 総所有コストの削減

た脅威情報は、お客様のファイアウォールに自動的に導入されるリアルタイムの対抗策を開発するために使用されます。

ネットワークの制御と柔軟性

NSA シリーズの中核をなすのは、SonicWall の機能豊富なオペレーティングシステムである SonicOS です。SonicOS は、アプリケーションインテリジェンスと制御、リアルタイムでの可視化、高度な回避防御テクノロジーを備えた侵入防止システム (IPS)、高速の仮想プライベートネットワーキング (VPN)、その他の堅固なセキュリティ機能により、組織に必要なネットワークの制御と柔軟性を実現します。

ネットワーク管理者は、アプリケーションインテリジェンスと制御を通じて、生産性の高いアプリケーションを特定して非生産的なアプリケーションや危険な可能性のあるアプリケーションと区別し分類することができるほか、ユーザー単位およびグループ単位の強力なアプリケーションレベルのポリシーを (スケジュールおよび例外リストと組み合わせて) 使用して、そうしたアプリケーションのトラフィックを制御することができます。より大きな帯域幅をビジネスに重要なアプリケーションに優先的に割り振って、重要ではないアプリケーションの帯域幅は制限することができます。リアルタイムでの監視と可視化により、アプリケーション、ユーザー、および帯域幅の使用状況がグラフィカルに表現され、ネットワーク全体のトラフィックをきめ細かく洞察できます。

ネットワーク設計において高度な柔軟性が求められる組織のために、SonicOS は仮想 LAN (VLAN) を使用してネットワークをセグメント化するツールを提供しています。これにより、ネットワーク管理者は仮想 LAN インターフェイスを作成して、ネットワークを 1 つ以上の論理グループに分離することができます。管理者は、他の VLAN 上にあるデバイスとの通信レベルを決定するルールを作成します。

組織では、すべての NSA シリーズのファイアウォールに搭載されているワイヤレスアクセスコントローラにより、ワイヤレステクノロジーを使用してネットワークの境界を安全に広げることができます。SonicWall ファイアウォールと SonicWave* 802.11ac Wave 2 ワイヤレスアクセスポイントが一体となったワイヤレスネットワーク向けセキュリティソリューションは、業界をリードする次世代ファイアウォールテクノロジーと高速のワイヤレス通信を組み合わせて、ワイヤレスネットワーク全体でエンタープライズクラスのネットワークセキュリティとパフォーマンスを実現します。

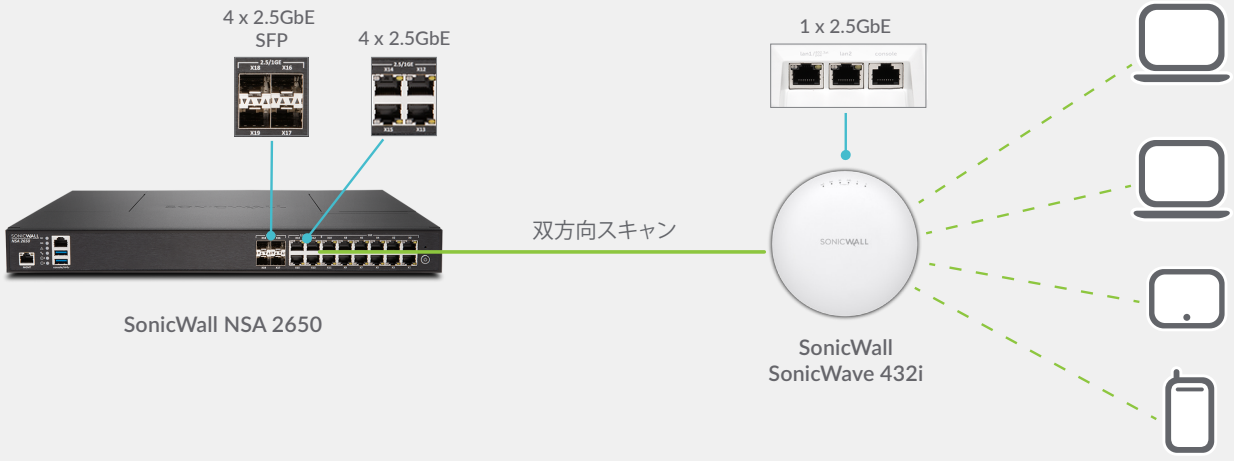
簡単な導入、セットアップ、および継続的な管理

すべての SonicWall ファイアウォールと同じように、NSA シリーズは、重要なセキュリティ、接続、柔軟性を実現するテクノロジーを 1 つの包括的なソリューションに緊密に統合しています。このソリューションには SonicWave ワイヤレスアクセスポイントと SonicWall WAN Acceleration Appliance (WXA) シリーズが含まれており、それらを管理する NSA ファイアウォールによっていずれもが自動的に検出され、プロビジョニングされます。複数の機能を統合することにより、必ずしもうまく連動するとは限らない製品を個別に購入してインストールする必要がなくなります。これにより、ソリューションをネットワークに導入して構成するために必要な作業が減り、時間と費用の両方を節約できます。

ネットワークセキュリティの継続的な管理と監視は、ファイアウォールまたは SonicWall Global Management System (GMS) によって中央で処理されるので、ネットワーク管理者はネットワークのあらゆる面を一元的に管理できます。導入とセットアップが簡素化されると同時に、管理が容易であるという利点も兼ね備えているため、組織で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。

セキュアで高速なワイヤレス通信

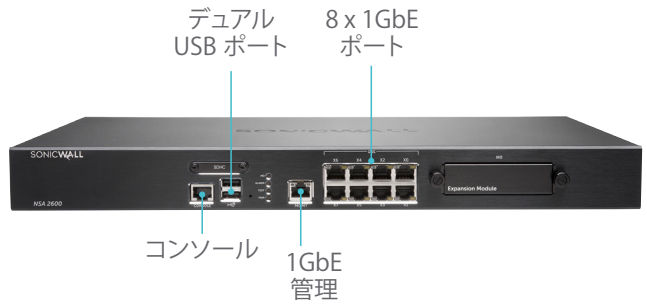
NSA 2650 次世代ファイアウォールと SonicWall SonicWave 802.11ac Wave 2 ワイヤレスアクセスポイントを組み合わせれば、高速ワイヤレスネットワーク向けセキュリティソリューションを構築できます。SonicWall NSA 2650 ファイアウォールと SonicWave アクセスポイントは両方とも、Wave 2 ワイヤレステクノロジーで提供される数ギガビットのワイヤレススループットに対応する、2.5 GbE ポートを装備しています。NSA 2650 は、ディープ・パケット・インスペクションというテクノロジーを使用して、ネットワークを出入りするすべてのワイヤレストラフィックをスキャンし、暗号化された接続を経由していたとしても、マルウェアや侵入などの有害な脅威を除去します。コンテンツフィルタ、アプリケーション制御およびインテリジェンス、Capture Advanced Threat Protection など、追加のセキュリティ機能と制御機能をワイヤレスネットワーク上で実行して、保護の層を厚くすることができます。

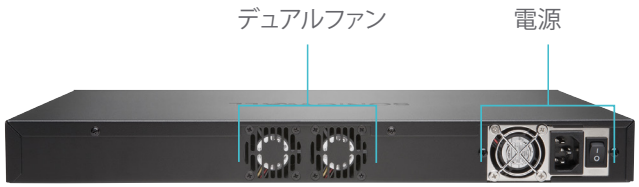


** SonicWave は、日本では 2018 年 1 月発売開始予定です。*

Network Security Appliance 2600

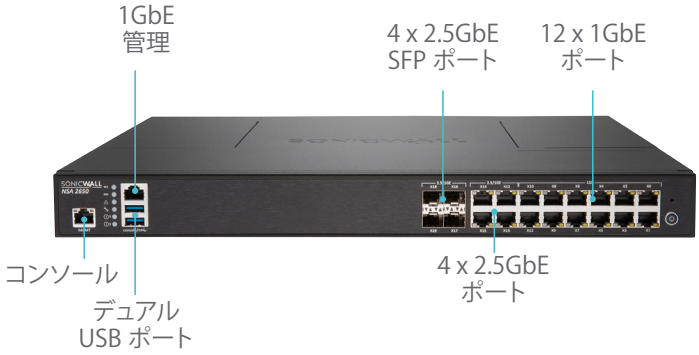
SonicWall NSA 2600 は、拡大する小規模組織、ブランチオフィス、キャンパスなどのニーズに対応するように設計されています。





Network Security Appliance NSA 2650

NSA 2650 は、中規模組織と分散エンタープライズの、数千の暗号化された接続と、それを超える数の暗号化されていない接続における、高速の脅威防御機能を提供します。

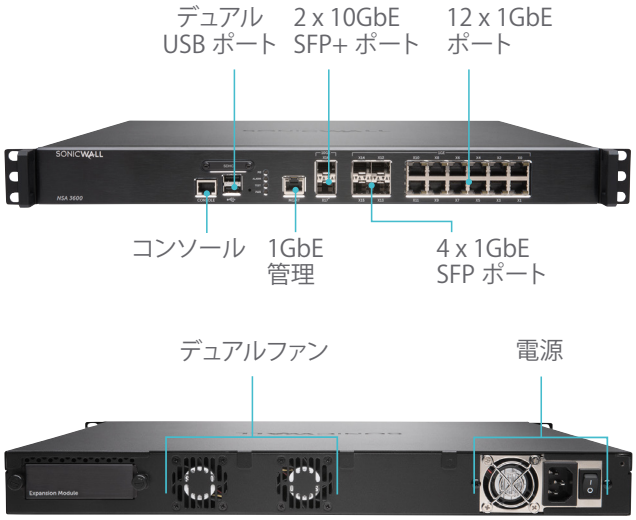


ファイアウォール	NSA 2600
ファイアウォールのスループット	1.9 Gbps
IPS のスループット	700 Mbps
アンチマルウェアのスループット	400 Mbps
フル DPI のスループット	300 Mbps
IMIX のスループット	600 Mbps
最大 DPI 接続数	250,000
1 秒当たりの新規接続数	15,000/秒

ファイアウォール	NSA 2650
ファイアウォールのスループット	3.0 Gbps
IPS のスループット	1.4 Gbps
アンチマルウェアのスループット	600 Mbps
フル DPI のスループット	600 Mbps
IMIX のスループット	700 Mbps
最大 DPI 接続数	500,000
1 秒当たりの新規接続数	15,000/秒

Network Security Appliance 3600

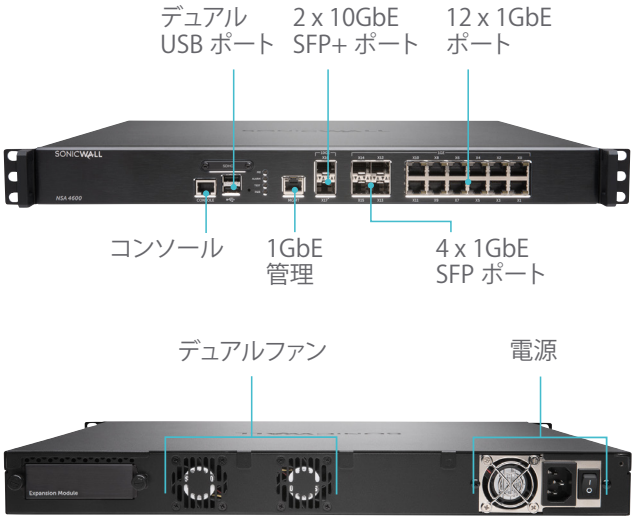
SonicWall NSA 3600 は、スループット容量とパフォーマンスを重視する、ブランチオフィスおよび小〜中規模企業の環境に最適です。



ファイアウォール	NSA 3600
ファイアウォールのスループット	3.4 Gbps
IPS のスループット	1.1 Gbps
アンチマルウェアのスループット	600 Mbps
フル DPI のスループット	500 Mbps
IMIX のスループット	900 Mbps
最大 DPI 接続数	375,000
1 秒当たりの新規接続数	20,000/秒

Network Security Appliance 4600

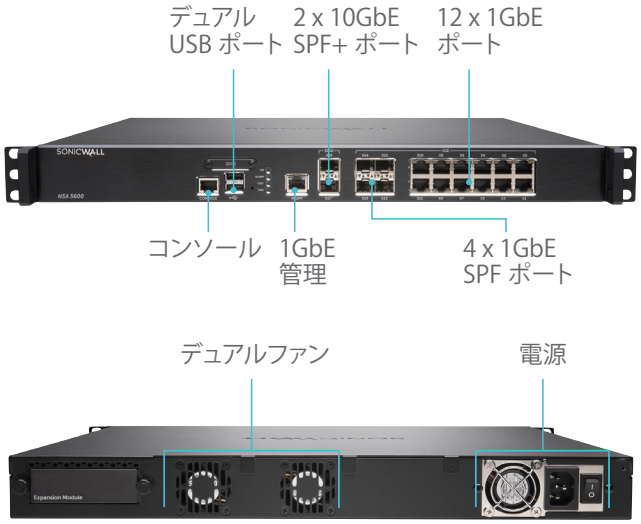
SonicWall NSA 4600 は、エンタープライズクラスの機能と妥協のないパフォーマンスにより、拡大する中規模組織とブランチオフィスを保護します。



ファイアウォール	NSA 4600
ファイアウォールのスループット	6.0 Gbps
IPS のスループット	2.0 Gbps
アンチマルウェアのスループット	1.1 Gbps
フル DPI のスループット	800 Mbps
IMIX のスループット	1.6 Gbps
最大 DPI 接続数	1,000,000
1 秒当たりの新規接続数	40,000/秒

Network Security Appliance 5600

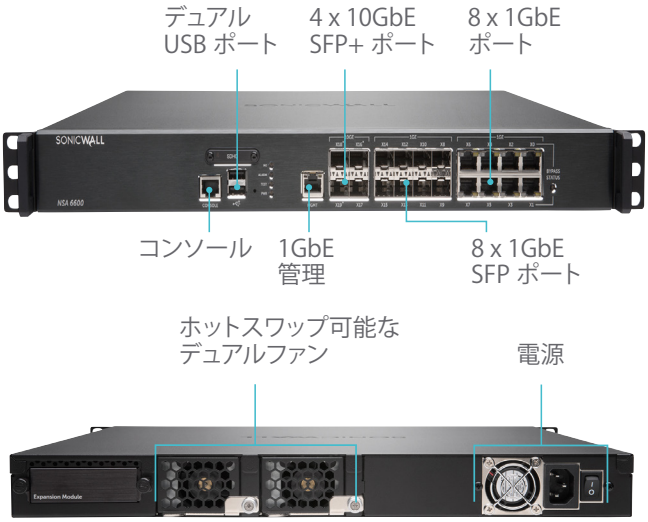
SonicWall NSA 5600 は、高いスループットを必要とする分散したブランチオフィスおよび企業の環境に最適です。



ファイアウォール	NSA 5600
ファイアウォールのスループット	9.0 Gbps
IPS のスループット	3.0 Gbps
アンチマルウェアのスループット	1.7 Gbps
フル DPI のスループット	1.6 Gbps
IMIX のスループット	2.4 Gbps
最大 DPI 接続数	1,000,000
1 秒当たりの新規接続数	60,000/秒

Network Security Appliance 6600

SonicWall NSA 6600 は、高いスループット容量とパフォーマンスを必要とする大規模な分散環境、および企業の中央サイトの環境に最適です。



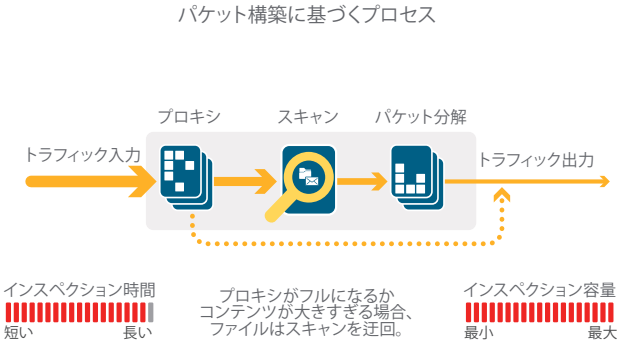
ファイアウォール	NSA 6600
ファイアウォールのスループット	12.0 Gbps
IPS のスループット	4.5 Gbps
アンチマルウェアのスループット	3.0 Gbps
フル DPI のスループット	3.0 Gbps
IMIX のスループット	3.5 Gbps
最大 DPI 接続数	1,000,000
1 秒当たりの新規接続数	90,000/秒

Reassembly-Free Deep Packet Inspection エンジン

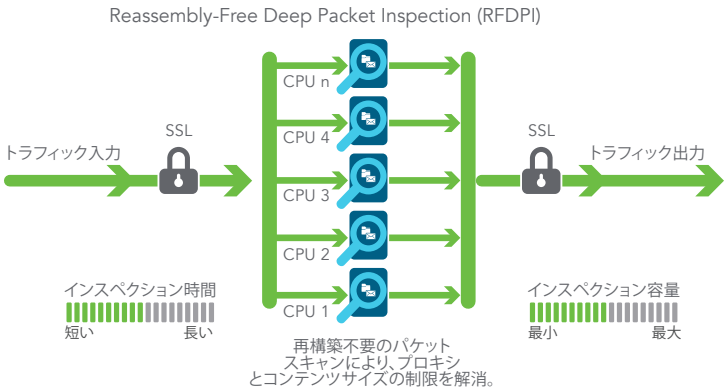
SonicWall Reassembly-Free Deep Packet Inspection (RFDPI) は、プロキシやバッファを必要とせずにストリームベースの双方向トラフィック分析を高速で実行するシングルパス、低レイテンシのインスペクションシステムであり、侵入の試みやマルウェアのダウンロードを効率的に発見すると同時に、ポートやプロトコルにかかわらずアプリケーションのトラフィックを特定します。この独自のエンジンは、レイヤ 3 ～ 7 で脅威を検出するストリーミングトラフィックペイロードのインスペクションに基づいて動作し、検出エンジンを混乱させて悪意のあるコードをネットワークに忍び込ませることを狙った高度な回避方法を無効化するために、ネットワークストリームに対して大規模な正規化と復号化を繰り返し実行します。

パケットは、SSL 復号化などの必要な前処理が行われた後、3 つのシグネチャデータベース (侵入攻撃、マルウェア、およびアプリケーション) の単一かつ独自のメモリ表現と照らし合わせて分析されます。これにより、接続の状態はそれらのデータベースに応じたストリームの位置まで進められ、それが攻撃やその他の「一致」イベントの状態に至ると、あらかじめ設定されたアクションが実行されます。

ほとんどの場合、接続は終了し、適切なログと通知イベントが生成されます。一方で、インスペクション専用にエンジンを構成することもできます。また、アプリケーションを検出する場合は、アプリケーションが識別されると同時に、それ以降のアプリケーションストリームに対してレイヤ 7 帯域幅管理サービスが提供されるようにすることもできます。



競合するプロキシベースのアーキテクチャ

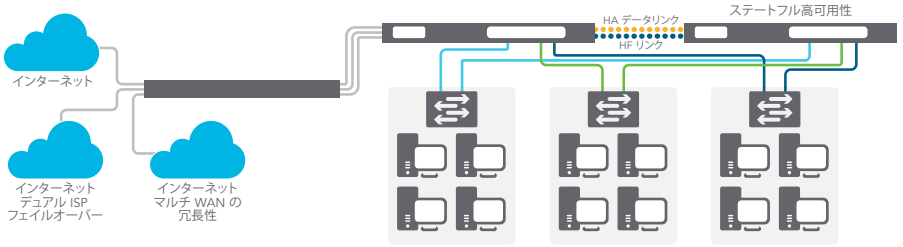


SonicWall のストリームベースのアーキテクチャ

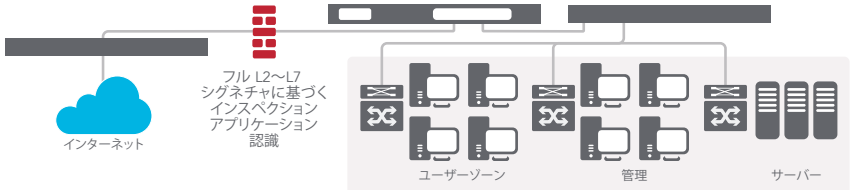
柔軟性に優れたカスタマイズ可能な導入オプション – NSA シリーズの概要

すべての SonicWall NSA ファイアウォールが、画期的なマルチコアのハードウェア設計と RFDPI を活用して、ネットワークパフォーマンスを低下させることなく、内部と外部のネットワークを保護します。NSA シリーズ NGFW では、高速の侵入防止、ファイルとコンテンツのインスペクション、強力なアプリケーションインテリジェンスと制御が、幅広い高度なネットワーキング機能や柔軟な構成機能と組み合わされています。NSA シリーズは、大規模ネットワーク、ブランチオフィスネットワーク、分散ネットワークといった多種多様な環境で容易に導入して管理できる、低価格のプラットフォームを提供します。

中央サイトゲートウェイとしての NSA シリーズ



インライン NGFW ソリューションとしての NSA シリーズ



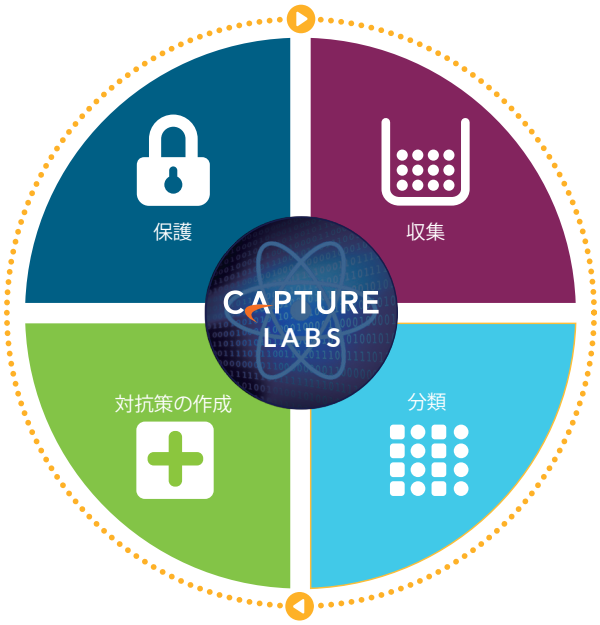
SONICWALL

Capture Labs

SonicWall 社内に設置された専任の Capture Labs 脅威研究チームは、最新の保護を実現するためにお客様のファイアウォールに導入する対抗策の研究と開発に取り組んでいます。このチームは、潜在的な脅威に関するデータをいくつかのソースから収集しています。たとえば、賞を獲得したネットワークサンドボックスサービスである Capture Advanced Threat Protection や、トラフィックを監視して新たに現れた脅威を検出する、世界中に配置された 100 万個を超える SonicWall のセンサーなどからデータが収集されます。データは SonicWall のディープラーニングアルゴリズムを使用した機械学習によって分析され、コードから DNA が抽出されて、悪意のあるコードとして知られているいずれかの形態に関連しているかどうかが調べられます。

SonicWall NGFW のお客様のために、脅威からの保護に必要なデータは 24 時間体制で継続的に更新されます。新たな更新は即時に有効になり、リブートや中断は不要です。アプライアンスで用意されているシグネチャは、幅広い種類の攻撃を防御できるように設計されており、1 つのシグネチャで数万種類の異なる脅威に対応します。

NSA アプライアンスは、アプライアンス上の対抗策のほかに、SonicWall CloudAV にもアクセスすることができ、オンボードのシグネチャインテリジェンスが 2000 万種類以上のシグネチャによって拡張されます。ファイアウォールは専用の軽量プロトコルを使用してこの CloudAV データベースにアクセスし、アプライアンス上で実行されるインスペクションを強化します。組織では、クラウドベースのマルチエンジンサンドボックスである Capture Advanced Threat Protection を使用して、疑わしいファイルとコードを隔離された環境で検査し、ゼロデイ攻撃などの高度な脅威を阻止することができます。

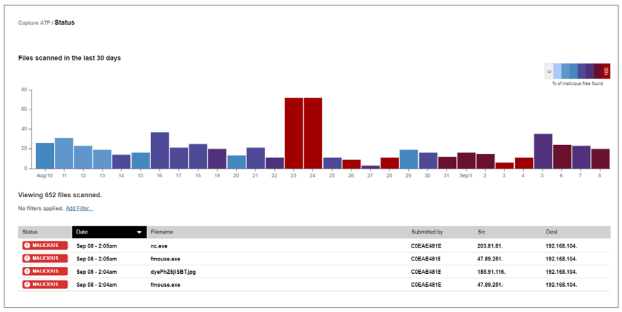


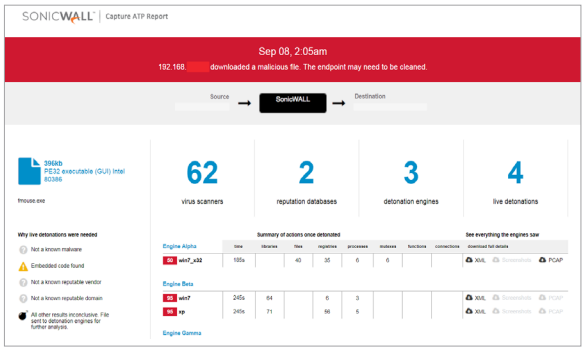
高度な脅威保護

SonicWall Capture Advanced Threat Protection Service は、クラウドベースのマルチエンジンサンドボックスであり、ファイアウォールの脅威保護を拡張してゼロデイ脅威を検出し、防止します。疑わしいファイルはクラウドに送信されて分析されますが、判定が下されるまでゲートウェイで保持しておくこともできます。仮想サンドボックス機能、フルシステムエミュレーション、ハイパーバイザーレベルの分析テクノロジーを備えたマルチエンジンのサンドボックスプラットフォームが、疑わしいコードを実行して動作を分析します。ファイルが悪意のあるものとして特定されると、Capture 内でハッシュがただちに作成された後、以降の攻撃を防止するためにシグネチャがファイアウォールに送信されます。

サービスは、幅広いオペレーティングシステムと、実行可能プログラム、DLL、PDF、MS Office ドキュメント、アーカイブ、JAR、APK などの、さまざまな種類のファイルを分析します。

Capture は、サービスに送信されたファイルの分析結果の詳細が一目でわかる脅威分析ダッシュボードとレポートを提供します。





たとえば、送信元、送信先、要約のほか、実行されたマルウェアの活動の詳細が表示されます。

SONICWALL®

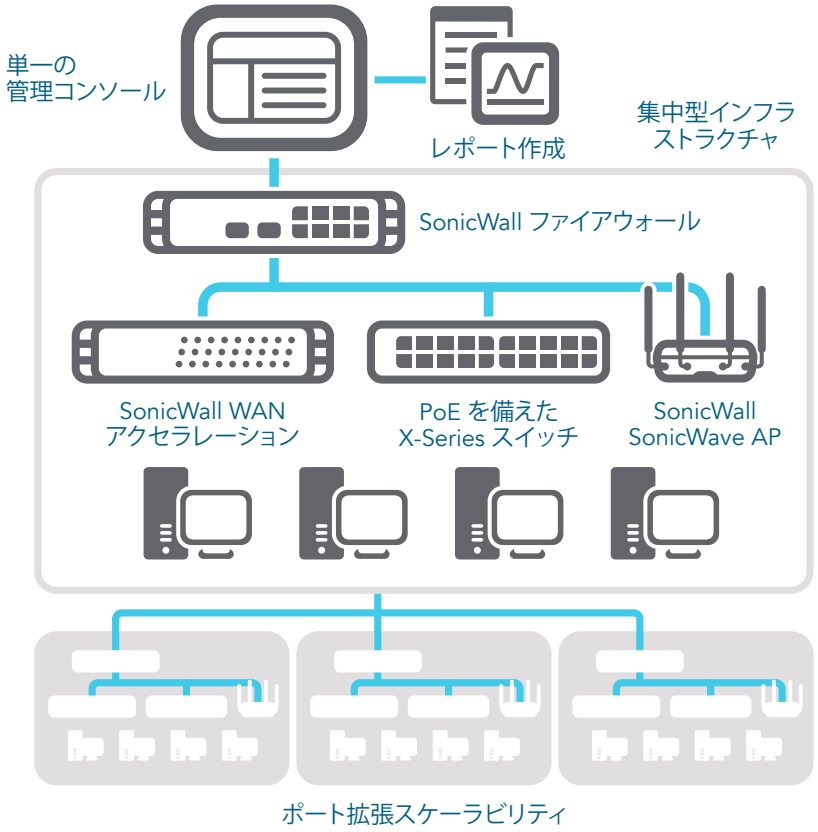
グローバル管理とレポート作成

綿密に調整されたセキュリティガバナンス、コンプライアンス、リスク管理戦略を実施する必要がある、厳しい規制下にある組織のために、SonicWall Global Management System (GMS®) は、相関性のある監査可能なワークストリームプロセスによって SonicWall ファイアウォール、ワイヤレスアクセスポイント、Dell X-Series スイッチを管理する、統合された、セキュアで拡張可能なプラットフォームを管理者に提供します。企業では、GMS を使用して、セキュリティアプライアンスの管理を容易に統合し、管理とトラブルシューティングの複雑さを軽減して、セキュリティインフラストラクチャの運用をあらゆる面で管理することができます。たとえば、中央でのポリシーの管理と適用、リアルタイムでのイベント監視、ユーザーアクティビティ、アプリケーションの識別、フロー分析とフォレンジックス、コンプライアンスおよび監査用のレポート作成などの機能を備えています。GMS は、ワークフロー自動化機能によって企業のファイアウォールの変更管理要件も満たします。GMS のワークフロー自動化により、あらゆる企業が俊敏かつ確実に、適切なファイアウォールポリシーを適切なときに導入して、コンプライアンス規制に準拠することができます。GMS には、ソフトウェア、クラウド、仮想アプライアンスの各オプションが用意されており、ビジネスプロセスやサービスレベルごとにネットワークセキュリティを管理する一貫した手段を備えているので、デバイス単位での管理に比べて、セキュリティ環境全体のライフサイクル管理が大幅に簡素化されます。

SonicWall GMS によるセキュアなコンプライアンスの実施

導入効果

- 集中管理
- エラーフリーのポリシー管理
- 強力なアクセス制御
- 包括的な監査証跡
- PCI、HIPAA、SOX レポートテンプレート
- 運用コストの削減



機能

RFDPI エンジン	
機能	説明
Reassembly-Free Deep Packet Inspection (RFDPI)	この特許を取得した独自のハイパフォーマンスインスペクションエンジンは、プロキシやバッファを必要とせずにストリームベースの双方向トラフィック分析を実行して、侵入の試みやマルウェアを発見し、ポートにかかわらずアプリケーショントラフィックを特定します。
双方向インスペクション	インバウンドとアウトバウンドの両方のトラフィックで同時に脅威をスキャンして、ネットワークがマルウェアの配布に使用されておらず、感染したマシンが内部に持ち込まれた場合に攻撃の踏み台にもならないことを確認します。
ストリームベースのインスペクション	プロキシとバッファを必要としないインスペクションテクノロジーにより、ファイルとストリームサイズに制限を設けることなく数百万の同時ネットワークストリームの DPI をきわめて低いレイテンシで実行でき、一般的なプロトコルにも生の TCP ストリームにも適用できます。
高い並列性とスケーラビリティ	独自設計の RFDPI エンジンがマルチコアアーキテクチャと連動して、高い DPI スループットときわめて高速での新規セッション確立を実現し、要求の厳しいネットワークでのトラフィックの急増に対処します。
シングルパスインスペクション	シングルパス DPI アーキテクチャは、マルウェア、侵入、アプリケーション識別のスキャンを同時に行い、DPI のレイテンシを劇的に低減します。また、すべての脅威情報が 1 つのアーキテクチャ内で確実に関連付けられます。

ファイアウォールとネットワーキング	
機能	説明
脅威 API	すべてのファイアウォールが、自社製、OEM 製、サードパーティ製のあらゆるインテリジェンスフィードを取り込んで活用し、ゼロデイ、悪意のある内部関係者、資格情報の漏洩、ランサムウェア、手の込んだ持続的な脅威などの、高度な脅威に対抗します。
ステートフル・パケット・インスペクション	すべてのネットワークトラフィックが検査され、分析されて、ファイアウォールアクセスポリシーに準拠していることが確認されます。
高可用性/クラスタリング	NSA シリーズは、状態同期によるアクティブ/パッシブ (A/P)、アクティブ/アクティブ (A/A) DPI、およびアクティブ/アクティブクラスタリングの高可用性モードをサポートします。アクティブ/アクティブ DPI は、ディープ・パケット・インスペクションの負荷をパッシブアプライアンス上のコアに分散して、スループットを高めます。
DDoS/DoS 攻撃からの保護	SYN フラッド保護は、レイヤ 3 SYN プロキシとレイヤ 2 SYN ブラックリストテクノロジーの両方を使用して、DOS 攻撃に対する防御を実現します。さらに、UDP/ICMP フラッド保護と接続速度の制限を使用して DOS/DDoS から保護します。
IPv6 のサポート	インターネットプロトコルバージョン 6 (IPv6) は、IPv4 からの移行における初期段階にあります。SonicOS により、ハードウェアでフィルタリングとワイヤモードの実装がサポートされるようになります。
柔軟な導入オプション	NSA シリーズは、従来型の NAT、レイヤ 2 ブリッジ、ワイヤ、およびネットワークタップの各モードで導入できます。
WAN ロードバランシング	ラウンドロビン、スピルオーバー、またはパーセンテージの各方式を使用して、複数の WAN インターフェイス間で負荷を分散します。ポリシーベースのルーティングにより、優先 WAN 接続にトラフィックを誘導するルートをプロトコルに基づいて作成します。障害が発生した場合は、セカンダリ WAN へのフェイルバックが可能です。
高度なサービス品質 (QoS)	802.1p、DSCP タグ付け、ネットワーク上の VoIP トラフィックの再マッピングによって、重要な通信を保証します。
H.323 ゲートキーパーおよび SIP プロキシのサポート	H.323 ゲートキーパーまたは SIP プロキシによって、すべての着信呼び出しに許可と認証を求めることで、スパム呼び出しを阻止します。
単体およびカスケード接続された Dell X-Series スイッチの管理	Dell の X-Series ネットワークスイッチの追加ポートのセキュリティ設定 (Portshield、HA、POE、POE+ など) を、ファイアウォール管理ダッシュボードを使用して一元的に管理します。
生体認証	簡単には複製または共有できない指紋認識などのモバイルデバイス認証をサポートしており、ネットワークアクセス用のユーザー ID をセキュアに認証します。
オープン認証とソーシャルログイン	ゲストユーザーが、パススルー認証を使用して、ホストのワイヤレスゾーン、LAN ゾーン、または DMZ ゾーン経由で、Facebook、Twitter、Google+ などのソーシャルネットワーキングサービスの資格情報でインターネットやその他のゲストサービスにサインインし、アクセスすることができます。

管理とレポート作成	
機能	説明
Global Management System (GMS)	SonicWall GMS は、直観的なインターフェイスを備えた単一の管理コンソールから、複数の SonicWall アプライアンスに対する監視、構成、およびレポートを行い、管理コストと複雑さを低減します。
強力な単一デバイス管理	包括的なコマンドラインインターフェイスを備え、SNMPv2/3 をサポートしているほか、直観的な Web ベースのインターフェイスによる迅速かつ容易な構成が可能です。
IPFIX/NetFlow アプリケーションフローレポート	アプリケーションのトラフィックの分析データと使用状況のデータを IPFIX または NetFlow プロトコルを通じてエクスポートして、リアルタイムでの、および過去に遡っての監視とレポートを行います。そのために、SonicWall Scrutinizer などのツールや、拡張機能を備えた、IPFIX および NetFlow をサポートするその他のツールも使用できます。
仮想プライベートネットワーキング (VPN)	
機能	説明
VPN の自動プロビジョニング	SonicWall ファイアウォール間における初期のサイト間 VPN ゲートウェイのプロビジョニングを自動化することにより、複雑な分散ファイアウォールの導入が簡素化され、わずかな作業で済むようになるとともに、セキュリティと接続性が瞬時に、そして自動的に確保されます。
サイト間接続のための IPSec VPN	ハイパフォーマンス IPSec VPN により、NSA シリーズは他の数千箇所の大規模サイト、ブランチオフィス、またはホームオフィスに対する VPN コンセントレーターとして機能します。
SSL VPN または IPSec クライアントのリモートアクセス	クライアントレス SSL VPN テクノロジー、または管理の容易な IPSec クライアントを使用して、さまざまなプラットフォームから E メール、ファイル、コンピューター、イントラネットサイト、アプリケーションに簡単にアクセスできます。

冗長 VPN ゲートウェイ	複数の WAN を使用する場合に、プライマリ VPN とセカンダリ VPN を、すべての VPN セッションのシームレスな自動フェイルオーバーとフェイルバックが可能になるよう構成できます。
ルートベースの VPN	VPN リンク上での動的ルーティングの実行機能により、VPN トンネルに一時的に障害が発生した場合にも、代替ルートを経由してエンドポイント間のトラフィックがシームレスに再ルーティングされるので、継続的な稼働を維持できます。
コンテンツ/コンテキストの認識	
機能	説明
ユーザーアクティビティの追跡	ユーザーの識別とアクティビティの追跡は、シームレスな AD/LDAP/Citrix1/Terminal Services1 SSO 統合と DPI で取得した広範な情報を併用することで可能になります。
GeoIP による国別のトラフィック識別	特定の国との間で送受信されるネットワークトラフィックを識別して制御し、脅威をもたらす活動が行われていることが明らかであるか、疑われる場所からの攻撃を防御したり、ネットワークから転送されてくる疑わしいトラフィックを調査したりします。国やボットネットのカスタムリストを作成して、IP アドレスに誤って関連付けられている国やボットネットのタグを無効にすることができます。誤分類による IP アドレスの不要なフィルタリングを防止します。
正規表現による DPI フィルタリング	正規表現マッチングにより、ネットワークを通過するコンテンツを識別、制御してデータの漏洩を防ぎます。国やボットネットのカスタムリストを作成して、IP アドレスに誤って関連付けられている国やボットネットのタグを無効にすることができます。

侵入防止サブスクリプションサービス

Capture Advanced Threat Protection	
機能	説明
マルチエンジンのサンドボックス	仮想サンドボックス機能、フルシステムエミュレーション、ハイパーバイザーレベルの分析テクノロジーを備えたマルチエンジンのサンドボックスプラットフォームが、疑わしいコードを実行して動作を分析します。これにより、広範囲にわたる悪意のあるアクティビティが可視化されます。
判定が下されるまでブロック	悪意がある可能性のあるファイルがネットワークに侵入するのを防ぐため、分析対象としてクラウドに送信されたファイルを、判定が下されるまでゲートウェイで保持することができます。
さまざまな種類とサイズのファイル分析	実行可能プログラム (PE)、DLL、PDF、MS Office ドキュメント、アーカイブ、JAR、APK など、さまざまな種類のファイルを分析します。さらに、複数のオペレーティングシステム (Windows、Android、Mac OS X) やマルチブラウザ環境にも対応します。
シグネチャの迅速な導入	ファイルが悪意のあるものとして特定されると、SonicWALL Capture サブスクリプションが有効なファイアウォールに対してシグネチャがただちに配布されます。また、ゲートウェイアンチウイルスおよび IPS シグネチャのデータベースのほか、URL、IP、ドメインレピュテーションのデータベースにもシグネチャが 48 時間以内に送られます。

暗号化された脅威防御	
機能	説明
SSL/TLS の復号化およびインスペクション	SSL/TLS で暗号化されたトラフィックを復号化して、マルウェア、侵入、データ漏洩がないかどうかを、プロキシ化せずにその場で検査します。さらに、アプリケーション、URL、コンテンツの制御ポリシーを適用して、SSL で暗号化されたトラフィックに潜む脅威を防御します。NSA シリーズの全モデルのセキュリティサブスクリプションに付属しています。
SSH インスペクション	SSH のディープ・パケット・インスペクション (DPI-SSH) により、SSH トンネルを通過するデータを復号化して検査し、SSH を利用する攻撃を防ぎます。
侵入防止	
機能	説明
対抗策に基づく保護	緊密に統合された侵入防止システム (IPS) では、シグネチャその他の対抗策を活用してパケットペイロードに脆弱性やエクスプロイトがないかスキャンし、攻撃や脆弱性に幅広く対処します。
シグネチャの自動更新	SonicWall の脅威調査チームは継続的に脅威を研究し、50 を超える攻撃分野をカバーする広範な IPS 対抗策のリストを随時更新しています。新たな更新は即座に適用され、再起動する必要も、サービスが中断されることもありません。
ゾーン内での IPS 保護	侵入防止機能を備えた複数のセキュリティゾーンにネットワークをセグメント化し、脅威がゾーンの境界を越えて拡散するのを阻止することで、内部セキュリティを強化します。
ボットネットによるコマンドとコントロール (CnC) の検出とブロック	ローカルネットワーク上のボットが、マルウェアの拡散元として特定された IP やドメイン、または既知の CnC ポイントである IP やドメインに CnC トラフィックを送信した場合に、それを特定してブロックします。
プロトコルの不正使用/異常	プロトコルを悪用して IPS をひそかに通過しようとする攻撃を特定してブロックします。
ゼロデイ防御	何千種類にもおよぶエクスプロイトの最新の方法や技術に対抗できるように随時更新することで、ゼロデイ攻撃からネットワークを保護します。
回避防止テクノロジー	ストリームの大規模な正規化、デコード、およびその他の技術により、レイヤ 2〜7 の検出回避手法を用いた脅威がネットワークに侵入するのを防ぎます。
脅威防御	
機能	説明
ゲートウェイでのアンチマルウェア	RFDPI エンジンは、インバウンドトラフィック、アウトバウンドトラフィック、ゾーン内のトラフィックをすべてスキャンして、ウイルス、トロイの木馬、キーロガー、その他のマルウェアがファイルに潜んでないかどうかを調べます。ファイルの長さやサイズに制限はなく、すべてのポートと TCP ストリームがスキャンの対象となります。
CloudAV のマルウェア防御	SonicWall のクラウドサーバーには 2000 万件を超える脅威のシグネチャのデータベースがあり、継続的に更新されています。このデータベースを参照することにより、オンボードのシグネチャデータベースの機能を補強して、RFDPI で扱う脅威の範囲を広げることができます。

24 時間体制のセキュリティ更新	新たな脅威の更新は、セキュリティサービスが有効な現場のファイアウォールへ自動的に送信され、即座に適用されます。再起動する必要も、サービスが中断されることもありません。
双方向の生の TCP インスペクション	RFDPI エンジンはすべてのポートで生の TCP ストリームを双方向でスキャンできるため、少数のウェルノウンポートのみを重点的に保護する旧式のセキュリティシステムをすり抜けようとする攻撃でも阻止できます。
広範なプロトコルのサポート	HTTP/S、FTP、SMTP、SMBv1/v2 など、生の TCP でデータを送信しない一般的なプロトコルを識別し、標準のウェルノウンポートで実行されていない場合でもペイロードをデコードしてマルウェアを検査します。

アプリケーションインテリジェンスおよび制御	
機能	説明
アプリケーションの制御	RFDPI エンジンが、アプリケーションとその諸機能を、数千におよぶアプリケーションシグネチャが格納されていて、継続的に拡張されているデータベースと照合することにより識別します。そして、それらの識別されたアプリケーションとその諸機能を制御することで、ネットワークのセキュリティと生産性を高めます。
カスタムアプリケーションの識別	特定のパラメータまたはアプリケーション固有のネットワーク通信パターンに基づいてシグネチャを作成することで、カスタムアプリケーションを制御し、ネットワークの管理を強化します。
アプリケーションの帯域幅管理	重要なアプリケーションまたはアプリケーションカテゴリに対して使用可能な帯域幅の割り当てと調整をきめ細かく行い、重要性の低いアプリケーションのトラフィックは抑制します。
詳細な制御	LDAP/AD/Terminal Services/Citrix 統合により SSO ユーザーを完全に識別し、スケジュール、ユーザーグループ、除外リスト、各種アクションに基づいて、アプリケーションやアプリケーションの特定のコンポーネントを制御します。

コンテンツフィルタリング	
機能	説明
内部/外部のコンテンツフィルタリング	コンテンツフィルタリングサービスは、使用ポリシーを適用することにより、好ましくない、または非生産的な情報や画像が掲載されている Web サイトへのアクセスをブロックします。
エンフォースドコンテンツフィルタリングクライアント	ポリシーの適用範囲を拡大し、ファイアウォールの境界外にある Windows、Mac OS、Android、Chrome のデバイスに対してもインターネットコンテンツをブロックします。
詳細な制御	事前定義されているカテゴリまたはカテゴリの任意の組み合わせを使用してコンテンツをブロックします。授業中や営業時間などの時間帯でフィルタリングをスケジュールして、個々のユーザーやグループに適用することができます。
Web キャッシュ	URL のレーティングは SonicWall ファイアウォールでローカルにキャッシュされるため、頻繁に訪問するサイトの場合、以降のアクセスに要する応答時間はほんの一瞬です。
エンフォースドアンチウイルス/アンチスパイウェア	
機能	説明
マルチレイヤ保護	境界における保護の最初のレイヤとなるファイアウォールの機能と、エンドポイントの保護とを組み合わせて、ノートパソコンや USB メモリ、その他の保護されていないシステムを経由してネットワークに侵入するウイルスをブロックします。
自動適用オプション	ネットワークにアクセスするすべてのコンピューターに最新バージョンのアンチウイルス/アンチスパイウェアのシグネチャをインストールして有効化します。これにより、デスクトップのアンチウイルス/アンチスパイウェア管理で通常発生するコストを削減できます。
自動化された導入とインストールのオプション	各マシンへのアンチウイルス/アンチスパイウェアクライアントの導入とインストールがネットワーク経由で自動的に行われるため、管理の余計な手間を最小限に抑えることができます。
常に有効な自動ウイルス対策	すべてのデスクトップとファイルサーバーに対してアンチウイルス/アンチスパイウェアの更新が頻繁かつ透過的に配信されるため、エンドユーザーの生産性が向上し、セキュリティ管理が軽減されます。
スパイウェア対策	強力なスパイウェア対策により、広範なスパイウェアプログラムがスキャンされ、デスクトップやノートパソコンへのインストールがブロックされます。これにより、機密データの送信が事前に防止され、デスクトップのセキュリティとパフォーマンスが向上します。

SonicOS の機能の概要

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
- Reassembly-Free Deep Packet Inspection
- DDoS 攻撃の防御 (UDP/ICMP/SYN フラッド)
- IPv4/IPv6 のサポート
- リモートアクセスのための生体認証
- DNS プロキシ
- 脅威 API

SSL/SSH の復号化およびインスペクション [1]

- TLS/SSL/SSH に対応したディープ・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

Capture Advanced Threat Protection[1]

- 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
- ハイパーバイザーレベルの分析
- フルシステムエミュレーション
- さまざまな種類のファイルの調査
- 自動および手動の送信
- リアルタイムの脅威インテリジェンスの更新
- 自動ブロック機能

侵入防止 [1]

- シグネチャベースのスキャン
- シグネチャの自動更新
- 双方向インスペクション
- 詳細な 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
- ゲートウェイでのアンチウイルス
- ゲートウェイでの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
- アプリケーショントラフィックの可視化
- アプリケーションコンポーネントのブロック
- アプリケーションの帯域幅管理
- カスタムのアプリケーションシグネチャの作成
- データ漏洩防止
- NetFlow/IPFIX によるアプリケーションレポートの作成
- ユーザーアクティビティの追跡 (SSO)
- 包括的なアプリケーションシグネチャデータベース

Web コンテンツフィルタリング [1]

- URL フィルタリング
- アンチプロキシテクノロジー
- キーワードブロック
- 帯域幅管理 CFS 評価カテゴリ
- アプリケーションの制御が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

- VPN の自動プロビジョニング
- サイト間接続のための IPSec VPN
- SSL VPN および IPSec クライアントのリモートアクセス
- 冗長 VPN ゲートウェイ
- iOS、Mac OS X、Windows、Chrome、Android、Kindle Fire のモバイル接続
- 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
- IPv6
- パス MTU 検出
- 強化されたログ機能
- VLAN トランキング
- RSTP (Rapid Spanning Tree Protocol)
- ポートミラーリング
- レイヤ 2 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
- 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
- 帯域幅管理
- リンクアグリゲーション (静的および動的)
- ポートの冗長性
- 状態同期による A/P 高可用性
- A/A クラスタリング
- インバウンド / アウトバウンドのロードバランシング
- L2 ブリッジ、ワイヤ / 仮想ワイヤモード、タップモード
- 3G/4G WAN フェイルオーバー
- 非対称ルーティング
- Common Access Card (CAC) のサポート

ワイヤレス

- MU-MIMO
- 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
- エアタイムフェアネス
- MiFi エクステンダ
- ゲスト循環割り当て

VoIP

- 詳細な QoS 制御
- 帯域幅管理
- 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 プロキシのサポート

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)
- SNMPv2/v3
- 集中化された管理とレポート作成
- ログ
- Netflow/IPFix エクスポート
- クラウドベースの構成バックアップ
- BlueCoat Security Analytics Platform
- アプリケーションと帯域幅の可視化
- IPv4 および IPv6 の管理
- カスケード接続のスイッチを含む Dell X-Series スイッチ管理

[1] *サブスクリプションの追加が必要です。*

SONICWALL

NSA シリーズのシステム仕様

ファイアウォール全般	NSA 2600	NSA 2650	NSA 3600	NSA 4600	NSA 5600	NSA 6600
オペレーティングシステム	SonicOS 6.5					
セキュリティ処理コア数	4	4	6	8	10	24
インターフェイス	8 x 1 GbE、1 GbE 管理、1 コンソール	4 x 2.5 GbE SFP、4 x 2.5 GbE、12 x 1 GbE、1 GbE 管理、1 コンソール	2 x 10 GbE SFP+、4 x 1 GbE SFP、12 x 1 GbE、1 GbE 管理、1 コンソール	2 x 10 GbE SFP+、4 x 1 GbE SFP、12 x 1 GbE、1 GbE 管理、1 コンソール	2 x 10 GbE SFP+、4 x 1 GbE SFP、12 x 1 GbE、1 GbE 管理、1 コンソール	4 x 10 GbE SFP+、8 x 1 GbE SFP、8 x 1 GbE、1 GbE 管理、1 コンソール
拡張	1 拡張スロット (背面)*、SD カード*	1 拡張スロット (背面)*、16 GB ストレージモジュール	1 拡張スロット (背面)*、SD カード*			
管理	CLI、SSH、GUI、GMS					
SSO ユーザー数	30,000	40,000	40,000	50,000	60,000	70,000
サポートされる最大アクセスポイント数	32	48	48	64	96	128
ログ	アナライザ、ローカルログ、Syslog					
ファイアウォール/VPN パフォーマンス	**NSA 2600**	**NSA 2650**	**NSA 3600**	**NSA 4600**	**NSA 5600**	**NSA 6600**
ファイアウォールインスペクションのスループット[1]	1.9 Gbps	3.0 Gbps	3.4 Gbps	6.0 Gbps	9.0 Gbps	12.0 Gbps
フル DPI のスループット[2]	300 Mbps	600 Mbps	500 Mbps	800 Mbps	1.6 Gbps	3.0 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]	700 Mbps	1.4 Gbps	1.1 Gbps	2.0 Gbps	3.0 Gbps	4.5 Gbps
IPS のスループット[2]	700 Mbps	1.4 Gbps	1.1 Gbps	2.0 Gbps	3.0 Gbps	4.5 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]	400 Mbps	600 Mbps	600 Mbps	1.1 Gbps	1.7 Gbps	3.0 Gbps
IMIX のスループット	600 Mbps	700 Mbps	900 Mbps	1.6 Gbps	2.4 Gbps	3.5 Gbps
TLS/SSL インスペクションおよび復号化 (DPI SSL)[2]	200 Mbps	300 Mbps	300 Mbps	500 Mbps	800 Mbps	1.3 Gbps
VPN のスループット[3]	1.1 Gbps	1.5 Gbps	1.5 Gbps	3.0 Gbps	4.5 Gbps	5.0 Gbps
1 秒当たりの接続数	15,000/秒	15,000/秒	20,000/秒	40,000/秒	60,000/秒	90,000/秒
最大接続数 (SPI)	500,000	1,000,000	750,000	1,000,000	1,500,000	1,500,000
最大接続数 (DPI)[4]	250,000	500,000	375,000	500,000	1,000,000	1,000,000
デフォルト/最大接続数 (DPI SSL)[4]	1,000/1,000	12,000/13,500	2,000/2,750	3,000/4,500	4,000/8,500	6,000/10,500
VPN	**NSA 2600**	**NSA 2650**	**NSA 3600**	**NSA 4600**	**NSA 5600**	**NSA 6600**
サイト間トンネル	250	1,000	1,000	3,000	4,000	6,000
IPSec VPN クライアント数 (最大)	10 (250)	50 (1,000)	50 (1,000)	500 (3,000)	2,000 (4,000)	2,000 (6,000)
SSL VPN NetExtender クライアント数 (最大)	2 (250)	2 (350)	2 (350)	2 (500)	2 (1000)	2 (1500)
暗号化/認証	DES、3DES、AES (128、192、256 ビット)/MD5、SHA-1、Suite B 暗号方式					
鍵交換	Diffie Hellman グループ 1、2、5、14v					
ルートベースの VPN	RIP、OSPF					
ネットワーク	**NSA 2600**	**NSA 2650**	**NSA 3600**	**NSA 4600**	**NSA 5600**	**NSA 6600**
IP アドレスの割り当て	静的 (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、多対 1、1 対多、フレキシブル NAT (重複 IPS)、PAT、トランスペアレントモード					
VLAN インターフェイス数	256	256	256	256	400	500
ルーティングプロトコル	BGP、OSPF、RIPv1/v2、静的ルート、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、802.1p					
認証	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)					
VoIP	フル H323-v1-5、SIP					
標準	TCP/IP、ICMP、HTTP、HTTPS、IPSec、ISAKMP/IKE、SNMP、DHCP、PPPoE、L2TP、PPTP、RADIUS、IEEE 802.3					
認定	ICSA ファイアウォール、ICSA アンチウイルス、FIPS 140-2、コモンクライテリア NDPP (ファイアウォールおよび IPS)、UC APL					
高可用性	状態同期によるアクティブ/パッシブ		状態同期によるアクティブ/パッシブ アクティブ/アクティブクラスタリング		状態同期によるアクティブ/パッシブ、 状態同期によるアクティブ/アクティブ DPI、 アクティブ/アクティブクラスタリング	
ハードウェア	**NSA 2600**	**NSA 2650**	**NSA 3600**	**NSA 4600**	**NSA 5600**	**NSA 6600**
電源	単一、固定 200W	デュアル、冗長 120W (1 台が付属)	単一、固定 250W			
ファン	デュアル、固定					デュアル、冗長、 ホットスワップ可能
電源入力	100～240 VAC、60～50 Hz					
最大消費電力 (W)	49.4	74.3	74.3	86.7	90.9	113.1
25°C での MTBF (時間)	176,540	146,789	146,789	139,783	134,900	116,477
25°C での MTBF (年)	20.15	16.76	16.76	15.96	15.40	13.30
フォームファクタ	1U ラックマウント型					
寸法	4.5 x 48.5 x 43 cm (1.75 x 19.1 x 17 インチ)					
重量	4.6 kg (10.1 ポンド)	6.15 kg (13.56 ポンド)	6.15 kg (13.56 ポンド)			6.77 kg (14.93 ポンド)
WEEE 重量	5.0 kg (11.0 ポンド)	6.46 kg (14.24 ポンド)	6.46 kg (14.24 ポンド)			8.97 kg (19.78 ポンド)
出荷時の重量	6.5 kg (14.3 ポンド)	9.43 kg (20.79 ポンド)	9.43 kg (20.79 ポンド)			11.85 kg (26.12 ポンド)
主な規制	FCC Class A、CE (EMC、LVD、RoHS)、C-Tick、VCCI Class A、MSIP/KCC Class A、UL、cUL、TUV/GS、CB、 UL によるメキシコ CoC、WEEE、REACH、ANATEL、BSMI、CU					
環境 (動作/保管)	0～40°C (32～105°F)/-40～70°C (-40～158°F)					
湿度	10～90% (結露しないこと)					

[1] テスト手法：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] フル DPI/ 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 Spirent WebAvalanche HTTP パフォーマンステストツールと Ixia テストツールを使用して測定しています。テストには、複数のポートペアで複数のフローを使用しました。
[3] VPN のスループットは、RFC 2544 準拠のパケットサイズ 1280 バイトの UDP トラフィックを使用して測定しました。仕様、機能、使用の可否については、いずれも変更されることがあります。
[4] DPI 接続の数を 125,000 減らすごとに、使用可能な DPI SSL 接続の数が 750 ずつ増えます。
* 将来的に使用するための予備。仕様、機能、使用の可否については、いずれも変更されることがあります。

SONICWALL®

当社について

創設後 25 年以上にわたり、SonicWall はこの業界の信頼できるセキュリティパートナーとして存在しています。ネットワークセキュリティから、アクセスセキュリティ、電子メールセキュリティまで、SonicWall は自社の製品ポートフォリオを継続的に進化させることで、組織の革新、促進、成長を可能にします。世界の約 200 の国と地域に 100 万台を超えるセキュリティデバイスを持つ SonicWall は、お客様が自信を持って未来を受け入れられるようにします。

SonicWall, Inc.
5455 Great America Parkway | Santa Clara, CA 95054
Refer to our website for additional information.
www.sonicwall.com

Datasheet-NetworkSecurityAppliance-US-VG-MKTG659

SONICWALL®