SonicWall Network Security appliance (NSa) シリーズ

中規模ネットワーク、分散エンタープライズ、およびデータセンター向けの、
業界が認めるセキュリティ効果とパフォーマンス

SonicWall Network Security appliance (NS*a*) シリーズは、中規模ネットワークから、分散エンタープライズ、データセンターにわたる規模の組織に、高パフォーマンスのセキュリティプラットフォームにおいて高度な脅威防御を提供します。SonicWall Capture Cloud Platformで革新的な深層学習テクノロジーを活用するNS*a*シリーズは、組織が必要とするリアルタイムでの侵害の自動検知と防御を提供します。

優れた性能の最先端脅威防御

今日のネットワーク脅威は回避力が高く、従来の検出方法では特定することがきわめて困難になっています。このような高度な攻撃への対策には、クラウドにおけるセキュリティインテリジェンスを積極的に活用する、より現代的なアプローチが求められます。クラウドインテリジェンスなくして、ゲートウェイセキュリティソリューションは、今日の複雑な脅威に追いつくことができません。NS*a*シリーズの次世代ファイアウォール (NGFWs) は、ご利用のネットワークのセキュリティ対策を最新のものとする最先端の脅威防御を提供するために、2つの高度なセキュリティテクノロジーを統合しています。SonicWallのマルチエンジンCapture Advanced Threat Protection (ATP) サービスを強化することによって誕生したのが、特許申請中のReal-Time Deep Memory Inspection (リアルタイム ディープ メモリ インスペクション、RTDMI™) テクノロジーです。RTDMIエンジンは、メモリ内を直接検査して大量に出回っているゼロデイ攻撃、未知のマルウェアを自主的に検出し、ブロックします。SonicWall RTDMIテクノロジーは、リアルタイムアーキテクチャにより、正確で、間違いが極めて少なく、マルウェアの武器が100ナノ秒未満しか露出しないような高度な攻撃を特定および緩和することができます。これと併用して、SonicWallの特許取得済み*のシングルパス Reassembly-Free Deep Packet Inspection (RFDPI) 脅威防御エンジンが、ファイアウォール上でインバウンドとアウトバウンド両方のトラフィックを検査し、すべてのパケットの全バイトを検証します。侵入防御、マルウェア対策およびウェブ/URLフィルタリングなどのNS*a*シリーズのオンボックス機能に追加して、SonicWall Capture Cloud Platformをご利用いただくことにより、NS*a*シリーズは最も悪質な脅威でさえもゲートウェイでブロックすることができます。

さらに、SonicWallのファイアウォールは、ポートとプロトコルにかかわらず、TLS/SSLおよびSSHで暗号化された接続を完全に復号化して検査し、完璧な保護を提供。深層部のパケット (ヘッダーとデータ) をくまなく調べプロトコルへの非準拠、脅威、ゼロデイ、侵入、および定義された条件を探します。ディープ パケット インスペクション エンジンは、暗号方式を利用する隠れた攻撃を検出・防御し、暗号化されたマルウェアのダウンロードをブロックし、感染の拡大を止め、コマンドとコントロール (C&C) の伝達やデータの窃盗を阻止します。受け入れ・除外ルールは、その組織で特有のコンプライアンスと法的要件に応じて、暗号化と検査の対象となるトラフィックをカスタマイズするための完全な制御を可能にします。

IPS、ウイルス対策、スパイウェア対策、TLS/SSL暗号解除/インスペクション、ファイアウォール上のその他の機能などのディープ パケット インスペクション機能を有効化すると、ネットワークのパフォーマンスが遅くなりがちで、かなりのスローダウンになることもありますが、NS*a*シリーズのファイアウォールは、マルチコアハードウェアアーキテクチャであるため、特化したマイクロプロセッサを使用しており、RTDMIエンジンとRFDPIエンジンを統合するこの独特な設計は、他のファイアウォールで発生しやすいネットワークにおけるパフォーマンスの低下を排除します。

メリット:

優れた脅威防御とパフォーマンス

- 特許申請中のリアルタイムのディープメモリインスペクション テクノロジー
- 特許を取得しているReassembly-Free Deep Packet Inspection (RFDPI) 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
- 業界が認めるセキュリティ効果
- マルチコアハードウェアアーキテクチャ
- 専用のCapture Labs脅威調査チーム

ネットワークの制御と柔軟性

- 安全なSD-WAN
- 強力なSonicOSオペレーティングシステム
- アプリケーションのインテリジェンスと制御
- VLANによるネットワークのセグメンテーション
- 高速ワイヤレスのセキュリティ

容易な展開、設定、継続的管理

- ゼロタッチデプロイ
- クラウドベースおよびオンプレミスでの集中管理
- スケーラブルなファイアウォール製品ライン
- 低い所有総コスト

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

ネットワークの制御と柔軟性

NS*a*シリーズの中心にあるのは、多くの機能を搭載したSonicWallのオペレーティングシステム、SonicOSです。SonicOSは、アプリケーション インテリジェンスとコントロール、リアルタイムの可視化、そして回避に対抗する高度なテクノロジー、高速仮想プライベートネットワーク (VPN) および他の強力なセキュリティ機能を搭載する侵入防御システム (IPS) によって、組織が求めるネットワークの制御と柔軟性を提供します。

アプリケーション インテリジェンスとコントロールを使用することによって、ネットワーク管理者は、生産的なアプリケーションを非生産的または危険な可能性があるアプリケーションから区別したり、ユーザー毎とグループ毎の両方に対する強力なアプリケーションレベルのポリシーを通じてトラフィックを制御したりできます。ビジネスに不可欠なアプリケーションを優先化し、より多くの帯域幅を割り当てる一方で、不可欠ではないアプリケーションの帯域幅を限定することができます。リアルタイムのモニタリングと可視化は、ネットワーク全体にわたる細部に及ぶインサイトを目的として、アプリケーション、ユーザーおよび帯域幅の使用を画像により表示することができます。

ネットワークデザインに高度な柔軟性を求める分散型の組織においては、SonicOSのSD-WANテクノロジーが、本社または遠隔地の支店・支部で導入されているNSaファイアウォールの完璧な補足となることでしょう。MPLSやT1のようなより高額な従来のテクノロジーに依存する代わりに、SD-WANを使用する組織は、アプリケーションの高可用性と予測可能なパフォーマンスを維持しながら、低コストの公衆インターネットサービスを選択できます。

NS*a*シリーズのファイアウォールすべてに、ワイヤレステクノロジーを利用してネットワークの範囲を安全に拡大することを可能にするワイヤレスアクセスコントローラーが組み込まれています。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を共に使用することで、ワイヤレスネットワーク全体にわたり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もたらすことのできる、業界をリードする次世代のファイアウォールテクノロジーと高速ワイヤレスを組み合わせたワイヤレスネットワークセキュリティのソリューションを創り出します。

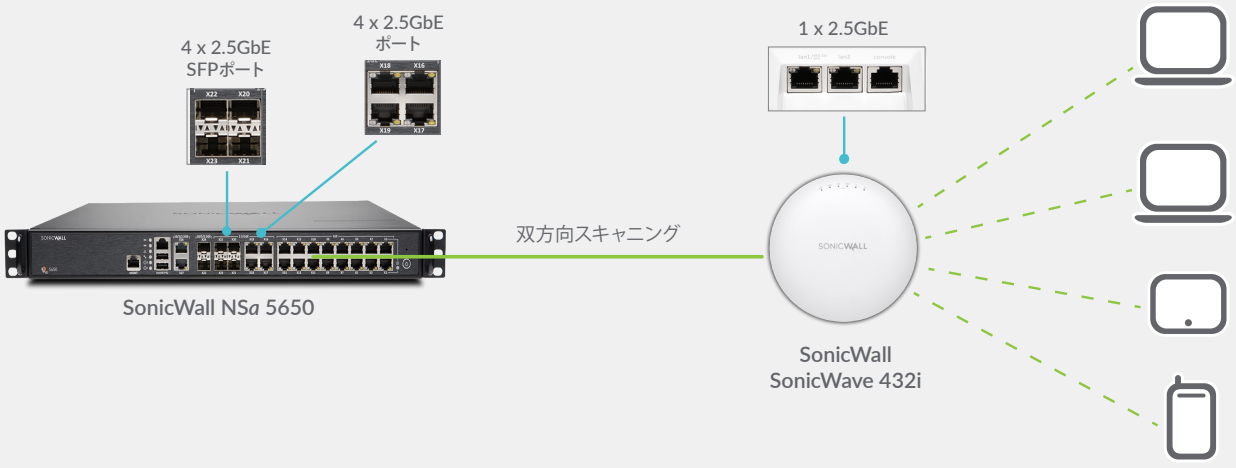
展開、設定、継続的管理が容易に

すべてのSonicWallファイアウォールと同様に、NS*a*シリーズは、主要なセキュリティ、接続性、および柔軟性のためのテクノロジーを単一の包括的なソリューションに統合させています。これには、SonicWaveワイヤレスアクセスポイントとSonicWall WAN Acceleration (WXA) シリーズが含まれており、これらは、管理しているNS*a*ファイアウォールによって自動的に検知および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って、同時には機能しないこともあるポイント製品を購入しインストールする必要がなくなります。これにより、ネットワーク内にソリューションを展開し、構成に要される作業を削減することができ、時間と経費の削減につながります。

クラウドベースで行われる集中管理、レポーティング、ライセンス許諾、および解析は、SonicWall Capture Security Centerを通じて処理されます。Capture Security Centerの主要コンポーネントは、ゼロタッチデプロイです。このクラウドベースの機能は、遠隔地および支店・支社からのSonicWallファイアウォールの展開とプロビジョニングを簡略化・迅速化し、この簡略化された展開と設定は容易な管理と共に、組織が所有総コストを削減し、高い投資利益率を達成するのに役立ちます。

安全で高速のワイヤレス

NS*a*シリーズの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ることで、高速のワイヤレスネットワークセキュリティソリューションが誕生しました。NS*a*シリーズのファイアウォールとSonicWaveのアクセスポイントは共に、Wave 2ワイヤレステクノロジーで提供されるマルチギガビットのワイヤレススループットを可能にする2.5 GbEポートを搭載しています。ファイアウォールは、ディープ パケット インスペクション 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、暗号化された接続からでさえも、マルウェアや侵入などの有害な脅威を排除します。また、さらなる保護レイヤを提供するために、コンテンツフィルタリング、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などの追加のセキュリティと制御機能もワイヤレスネットワークで実行することができます。

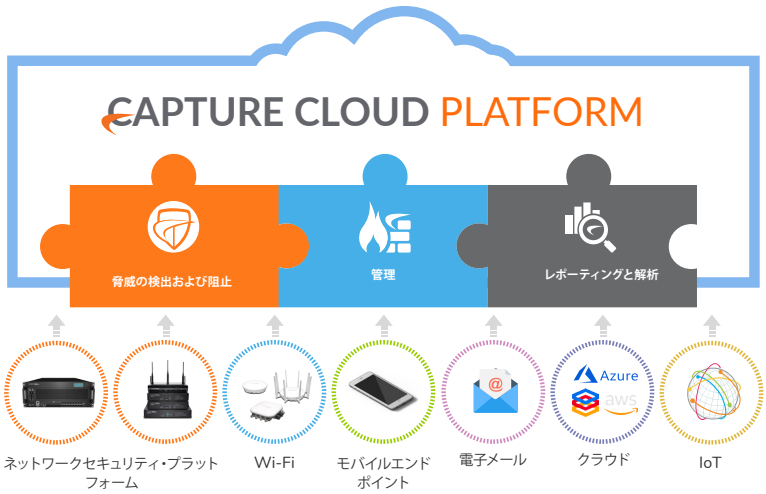


Capture Cloud Platform

SonicWallのCapture Cloud Platformは、組織の規模にかかわらず、クラウドベースの脅威防御とネットワーク管理、さらにレポーティングと解析を提供します。このプラットフォームは、当社の受賞経験を持つマルチエンジンネットワーク・サンドボックスサービス、Capture Advanced Threat Protection、そして世界中に張り巡らされた100万以上のSonicWallセンサーを含む複数の情報源から収集した脅威インテリジェンスを集約しています。

ネットワークに入り込むデータが過去に見られない悪意のあるコードを含んでいるのが判明した場合、Capture Cloud Platformデータベースに保存され、最新の保護のためにお客様のファイアウォールに展開されるシグネチャを、SonicWallの専任Capture Labs脅威調査チームが開発します。新しいアップデートも再起動や中断なく直ちに発効。シグネチャは機器に残り、何万もの個別の攻撃に対処し、あらゆるクラスの攻撃を阻止します。機器の対策に加え、NSaファイアウォールは、Capture Cloud Platformデータベースへ継続的にアクセスし、これによりオンボードのシグネチャインテリジェンスが何千万ものシグネチャに拡大されます。

Capture Cloud Platformは、脅威防御のほかに、単一画面（シングルペインオブグラス）管理を提供するため、管理者はネットワーク活動に関するリアルタイムおよび過去のレポートを簡単に作成することができます。

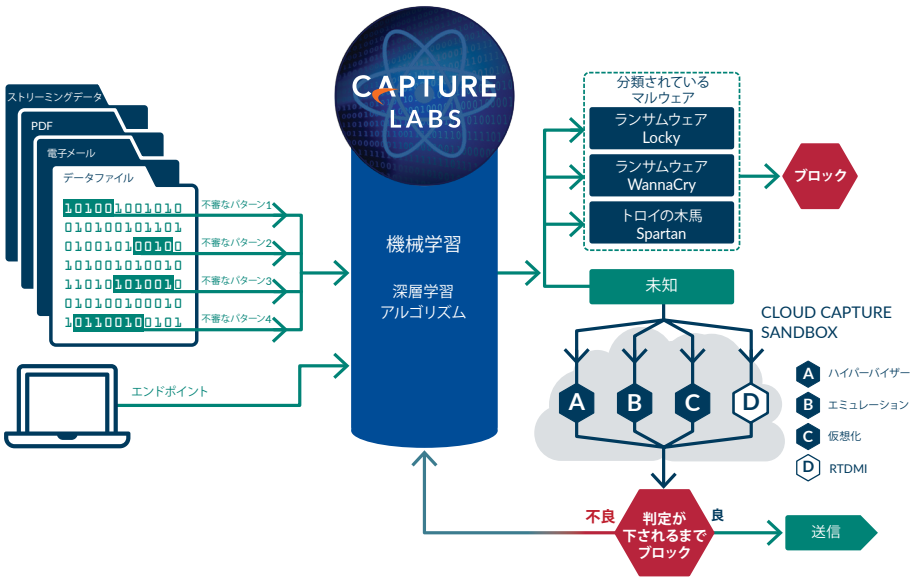


高度な脅威防御

SonicWallのリアルタイムの自動脅威防御の中心となるのはSonicWall Capture Advanced Threat Protectionサービスです。これは、クラウドベースのマルチエンジンサンドボックスで、ファイアウォールの脅威防御をゼロデイ攻撃の検知と阻止に拡大しています。疑いのあるファイルはクラウドに送信され、ここで深層学習アルゴリズムを活用して解析されます。また、判定が決定するまでファイルをゲートウェイで保持するオプションもあります。Real-Time Deep Memory Inspection、仮想サンドボックス、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解析テクノロジーを含むマルチエンジン サンドボックス プラットフォームは、疑われるコードを実行し、その行動を解析します。ファイルは悪意があるものと特定されるとブロックされ、Capture ATP内に直ちにハッシュが作成されます。その後すぐに、ファイアウォールにシグネチャが送られ、これに続く攻撃を阻止します。

実行可能なプログラム、DLL、PDF、MS Officeドキュメント、アーカイブ、JAR、APKを含む、広範なオペレーティングシステムとファイルのタイプが解析されます。

エンドポイントの完全な保護のために、SonicWall Capture Clientは、次世代のウイルス対策テクノロジーとSonicWallのクラウドベースのマルチエンジンサンドボックスを組み合わせます。

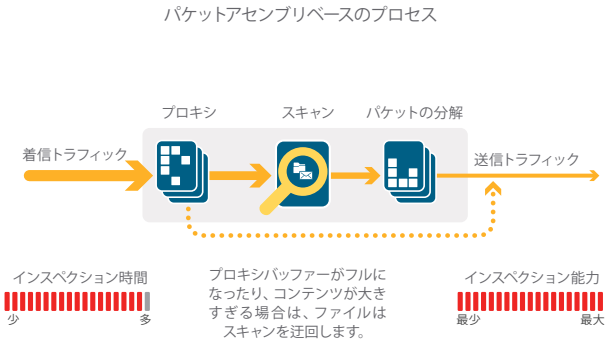


Reassembly-Free Deep Packet Inspectionエンジン

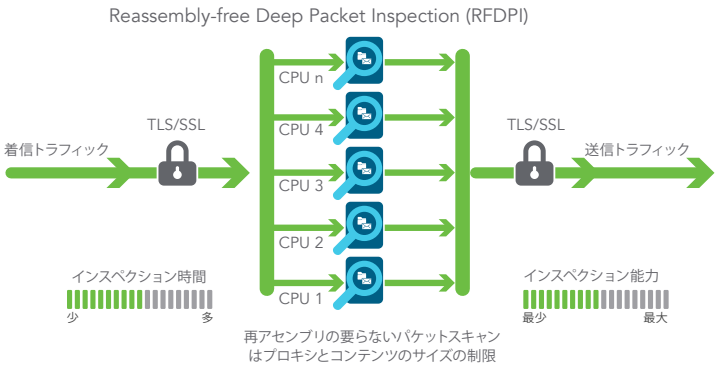
SonicWall Reassembly-Free Deep Packet Inspection（RFDPI）は、プロキシもバッファリングも使用することなく、侵入の試みとマルウェアのダウンロードを効果的に発見したり、ポートにかかわらずアプリケーションのトラフィックを特定するために、ストリームベースの双方向性トラフィック解析を高速で実行する、シングルパスイン、低レイテンシーのインスペクションシステムです。当社が専有のこのエンジンは、第3～7層で脅威を検知するためにストリーミングトラフィックのペイロードインスペクションに依存し、検出エンジンを混乱させ、ネットワークに悪意のあるコードを侵入させようとする高度な回避法を無効にするために反復型の著しい正常化と復号化を通じてネットワークのストリームを検証します。

パケットにTLS/SSL復号化を含む必要な再処理が実施された後、パケットは、侵入攻撃、マルウェアおよびアプリケーションという3つのシグネチャデータベースの単一の専有メモリ表示に照らし合わせて解析されます。接続の状態は、これらのデータベースに照らし合わせてストリームの位置を示すために、攻撃またはその他の「一致」イベントに遭遇するまで進行し、このどちらの場合にも事前設定された行動が取られます。

ほとんどの場合、接続は終了し、適切なジョギングと通知のイベントが作成されます。しかし、エンジンはインスペクションのみに、あるいはアプリケーションが検知された場合は、アプリケーションの特定後すぐに、アプリケーションのストリームの残りについて第7層の広域幅管理サービスが提供されるように設定することもできます。



競争的プロキシベースのアーキテクチャ



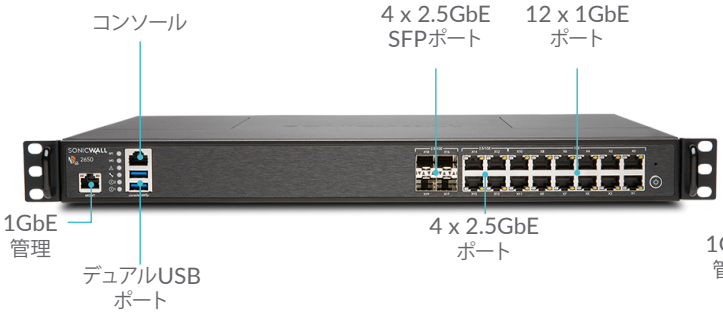
SonicWallストリームベースアーキテクチャ

集中管理とレポーティング

完全に調整されたセキュリティガバナンス、コンプライアンスおよびリスク管理の戦略達成を望む、多くの規制下にある組織には管理者向けにSonicWallが、SonicWallのファイアウォール、ワイヤレスアクセスポイント、およびDell NシリーズとXシリーズのスイッチを相関性があり監査可能なワークストリームプロセスで管理するための統一された安全な拡張可能なプラットフォームを提供します。企業はセキュリティ機器の管理、管理とトラブルシューティングの複雑さの低減、セキュリティインフラストラクチャの運用面におけるすべての管理を容易に統合することができます。これには、一元化されたポリシーの管理と実行、リアルタイムのイベントモニタリング、ユーザーの活動、アプリケーションの特定、フロー解析、フォレンジック、コンプライアンスと監査に関する報告その他が含まれます。さらに企業は適時、法令遵守の規則に従いながら適切なファイアウォールポリシーを展開するための俊敏性と確信を提供するワークフローの自動化を通してファイアウォールの変更管理要件を満たします。オンプレミス用のSonicWall Global Management SystemとクラウドのCapture Security Centerで利用可能なSonicWall管理、およびレポーティングソリューションは、ビジネスプロセスとサービスレベル別のネットワークセキュリティを管理するための明確な方法を提供し、デバイスごとの管理と比べ、総合的なセキュリティ環境のライフサイクル管理を劇的に簡略化します。

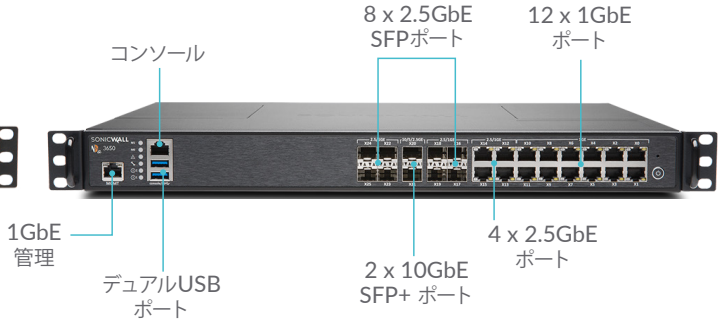
NS*a* 2650

NS*a* 2650は、中規模組織と分散エンタープライズの、数千にものぼる暗号化接続と、それを超える数の暗号化なしの接続における、高速の脅威防御機能を提供します。



NS*a* 3650

SonicWall NS*a* 3650は、スループットの能力とパフォーマンスに懸念をお持ちの支社・支店、中小企業環境に最適です。

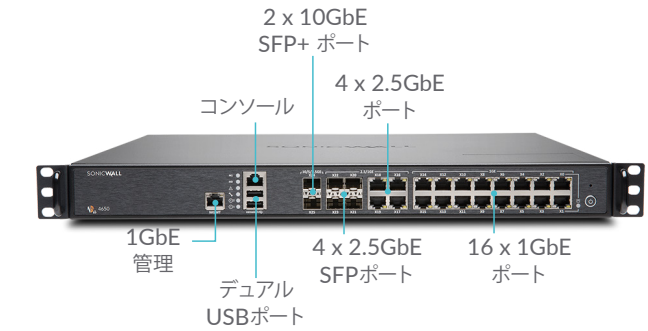


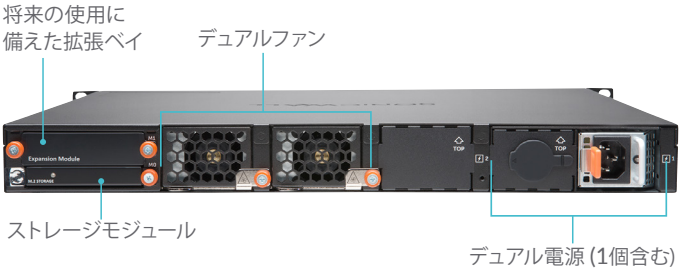
ファイアウォール	NS*a* 2650
ファイアウォールスループット	3.0 Gbps
IPSスループット	1.4 Gbps
アンチマルウェアスループット	1.3 Gbps
脅威防止スループット	1.5 Gbps
最大コネクション数	1,000,000
新規コネクション数/秒	14,000/秒
ストレージモジュール	16 GB
説明	**SKU**
NS*a* 2650 ファイアウォールのみ	01-SSC-1936
NS*a* 2650 TotalSecure Advanced (1年間)	01-SSC-1988

ファイアウォール	NS*a* 3650
ファイアウォールスループット	3.75 Gbps
IPSスループット	1.8 Gbps
アンチマルウェアスループット	1.5 Gbps
脅威防止スループット	1.75 Gbps
最大コネクション数	2,000,000
新規コネクション数/秒	14,000/秒
ストレージモジュール	32 GB
説明	**SKU**
NS*a* 3650 ファイアウォールのみ	01-SSC-1937
NS*a* 3650 TotalSecure Advanced (1年間)	01-SSC-4081

NS*a* 4650

The SonicWall NS*a* 4650は、エンタープライズクラスの機能と妥協しないパフォーマンスを提供し、成長を続ける中規模の組織や支社・支店に適しています。

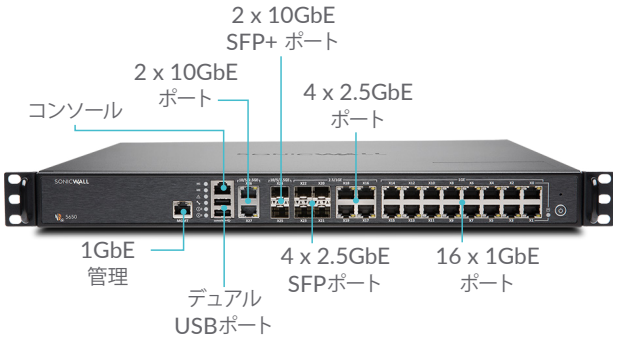


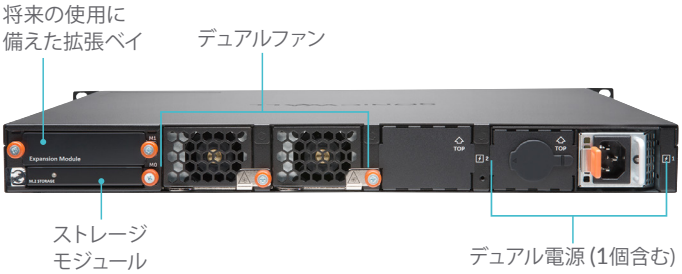


ファイアウォール	NS*a* 4650
ファイアウォールスループット	6.0 Gbps
IPSスループット	2.3 Gbps
アンチマルウェアスループット	2.45 Gbps
脅威防止スループット	2.5 Gbps
最大コネクション数	3,000,000
新規コネクション数/秒	40,000/秒
ストレージモジュール	32 GB
説明	**SKU**
NS*a* 4650 ファイアウォールのみ	01-SSC-1938
NS*a* 4650 TotalSecure Advanced (1年間)	01-SSC-4094

NS*a* 5650

SonicWall NS*a* 5650は、大規模のスループットとポートの高密度を必要とする、分散した支社・支店および企業環境に最適です。

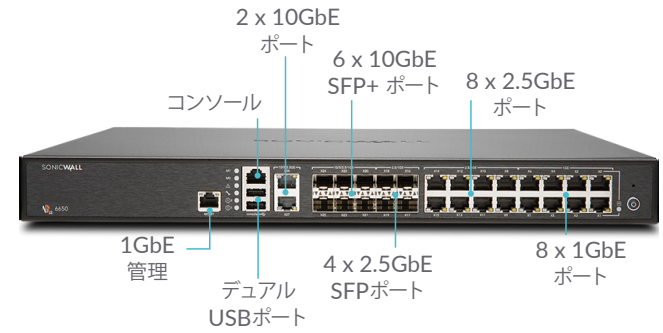




ファイアウォール	NS*a* 5650
ファイアウォールスループット	6.25 Gbps
IPSスループット	3.4 Gbps
アンチマルウェアスループット	2.8 Gbps
脅威防止スループット	3.4 Gbps
最大コネクション数	4,000,000
新規コネクション数/秒	40,000/秒
ストレージモジュール	64 GB
説明	**SKU**
NS*a* 5650 ファイアウォールのみ	01-SSC-1939
NS*a* 5650 TotalSecure Advanced (1年間)	01-SSC-4342

NS*a* 6650

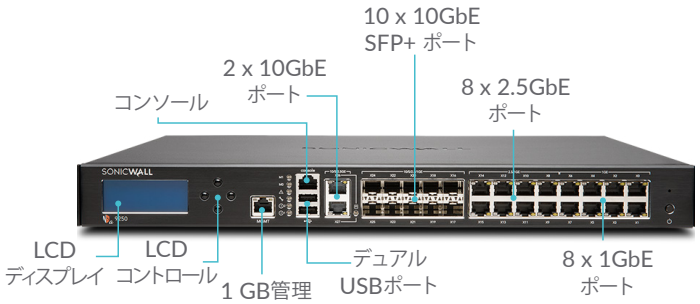
The SonicWall NS*a* 6650 は、スループットの能力とパフォーマンスの両方で高度なものを求める大規模の分散および企業の本社拠点に最適です。



ファイアウォール	NS*a* 6650
ファイアウォールスループット	12.0 Gbps
IPSスループット	6.0 Gbps
アンチマルウェアスループット	5.4 Gbps
脅威防止スループット	5.5 Gbps
最大コネクション数	5,000,000
新規コネクション数/秒	90,000/秒
ストレージモジュール	64 GB
説明	**SKU**
NS*a* 6650 ファイアウォールのみ	01-SSC-1940
NS*a* 6650 TotalSecure Advanced (1年間)	01-SSC-2209

NS*a* 9250/9450/9650

SonicWall NS*a* 9250/9450/9650は、分散エンタープライズとデータセンターにスケーラブル、より高度なセキュリティ、マルチギガビットの速度を提供します。



ファイアウォール	NS*a* 9250	NS*a* 9450	NS*a* 9650
ファイアウォールスループット	12.0 Gbps	17.1 Gbps	17.1 Gbps
IPSスループット	7.2 Gbps	10.2 Gbps	10.3 Gbps
アンチマルウェアスループット	6.5 Gbps	8.0 Gbps	8.5 Gbps
脅威防止スループット	6.5 Gbps	9.0 Gbps	9.4 Gbps
最大コネクション数	7,500,000	10,000,000	12,500,000
新規コネクション数/秒	90,000/秒	130,000/秒	130,000/秒
ストレージモジュール	1 TB、128 GB	1 TB、128 GB	1 TB、256 GB
説明	**SKU**	**SKU**	**SKU**
NS*a*ファイアウォールのみ	01-SSC-1941	01-SSC-1942	01-SSC-1943
NS*a* TotalSecure Advanced (1年間)	01-SSC-2854	01-SSC-4358	01-SSC-3475

機能

RFDPIエンジン	
機能	説明
Reassembly-Free Deep Packet Inspection (RFDPI)	特許取得済み、高パフォーマンスの当社専有のこのインスペクションエンジンは、プロキシもバッファリングも使用することなく、侵入の試みとマルウェアを発見したり、またポートにかかわらずアプリケーションのトラフィックを特定するために、ストリームベースの双方向の解析を実施します。
双方向のインスペクション	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脅威を同時にスキャンし、ネットワークがマルウェアを拡散するために使用されたり、また万が一感染した機器が内部に持ち込まれた際に、そこから攻撃を開始するプラットフォームとして使用されないようにします。
ストリームベースのインスペクション	プロキシもバッファリングも使用しないインスペクション テクノロジーは、ファイルもストリームサイズの制限もなく、同時に行われる何百万ものネットワークストリームのあるDPIに対してレイテンシーのきわめて低いパフォーマンスを提供するため、一般的なプロトコルに加えて生のTCPストリームに適用できます。
きわめてパラレルでスケーラブル	RFDPIエンジンのユニークなデザインは、マルチコアアーキテクチャと機能し、要求の多いネットワークでトラフィックのスパイクに対応するため、高DPIスループットときわめて高い新しいセッション設定率を提供します。
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、侵入およびアプリケーションを特定するためのスキャンを同時に行い、DPIレイテンシーを大幅に低減し、単一アーキテクチャ内ですべての脅威情報を関連付けます。

機能	説明
安全なSD-WAN	MPLSなどのより高額なテクノロジーの代わりとなるSecure SD-WANは、分散型のエンタープライズ組織が、利用しやすい、低コストの公衆インターネットサービスを使用してデータ、アプリケーション、およびサービスを共有できることを目的として、安全で高パフォーマンスのネットワークをリモート拠点にわたり、構築、運用、および管理できるようにします。
REST API	ファイアウォールが、製造元および第三者の専有インテリジェンスフィードをすべて受け取って活用し、ゼロデイ、悪意のあるインサイダー、不正認証情報、ランサムウェア、高度な標的型攻撃などの高度な脅威と闘うことを可能にします。
ステートフル パケット インスペクション	ネットワークトラフィックはすべて、検査と解析をされ、ファイアウォールアクセスポリシーに従って取り込まれます。
高可用性/クラスタリング	NSaシリーズは、状態の同期化ではActive/Passive (A/P) を、そしてActive/Active (A/A) DPIおよびActive/Activeのクラスタリング高可用性モードをサポートします。Active/Active DPIは、スループットを高めるために受動的 (passive) な機器のコアにディープ パケット インスペクションの負荷をアンロードします。
DDoS/DoS攻撃防御	SYNフラッド保護は、第3層のSYNプロキシと第2層のSYNブラックリスト化テクノロジーを使ってDoS攻撃に対する防御を提供します。さらに、UDP/ICMPフラッド保護を通じてDoS/DDoS攻撃に対しても保護を提供し、コネクション率を制限します。
IPv6対応	インターネットプロトコル・バージョン6 (IPv6) は、IPv4にとって代わる初期の段階にあります。SonicOSを使って、ハードウェアはフィルタリングとワイヤーモードの実装をサポートします。
柔軟な展開オプション	NSaシリーズは、従来のNAT、第2層ブリッジ、ワイヤ、およびネットワークタップの各モードで展開できます。
WANロードバランシング	Round Robin、Spillover、またはPercentageのいずれかの方法を使用するロードバランス・マルチWANインターフェース。
高度なサービスの質 (QoS)	802.1p、DSCPタグ付け、ネットワーク上でのVoIPトラフィックの再マッピングを通じ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プロキシサポート	受信する電話がすべてH.323ゲートキーパーまたはSIPプロキシで許可または認証されることを義務付けることにより、スパムコールをブロックします。
シングルまたはカスケード化されたDell NシリーズおよびXシリーズのスイッチ管理	Dell NシリーズおよびXシリーズのネットワークスイッチ用のファイアウォール管理ダッシュボードを使用して、シングルペインオブグラスの下で、Portshield、HA、PoEおよびPoE+を含む追加ポートのセキュリティ設定を管理します。
バイオメトリック認証	ネットワークアクセスのためにユーザーのアイデンティティを安全に認証するため、同じものを容易に複製できない、あるいは共有不可能である指紋認識などのモバイルデバイス認証をサポートします。
オープン認証およびソーシャルログイン	ゲストユーザーが、ホストのワイヤレス、LANまたはDMZゾーンを通じてパススルー認証を使い、ソーシャルネットワーキングサービス (Facebook、Twitter、Google+など) の認証情報を使ってインターネットおよび他のゲストサービスにサインインおよびアクセスすることを可能にします。

管理とレポーティング	
機能	説明
クラウドベースおよびオンプレミスの管理	SonicWallの装置の設定と管理は、SonicWall Capture Security Centerを通じてクラウドで、また、SonicWall Global Management System (GMS) を利用してオンプレミスで行えます。
強力な単一デバイス管理	包括的なコマンドラインのインターフェースおよびSNMPv2/3のサポートに加え、直感的なウェブベースのインターフェースは迅速で便利な構成を可能にします。
IPFIX/NetFlowによるアプリケーションフローのレポーティング	SonicWall Scrutinizer、または拡張IPFIXやNetFlowに対応する他のツールを使用して、リアルタイムと過去の記録のモニタリングとレポーティングのためにIPFIXまたはNetFlowプロトコルを通じて、アプリケーションのトラフィック解析と使用量データをエクスポートします。

仮想プライベートネットワーク (VPN)	
機能	説明
自動プロビジョンVPN	SonicWallファイアウォール間で、セキュリティと接続性が瞬時かつ自動的に発生するようにしながら、最初の施設間のVPNゲートウェイのプロビジョニングを自動化することよって、複雑な分散型ファイアウォールの展開を、手がかからないところまで簡略化および削減します。
企業施設間のIPSec VPN接続性	高パフォーマンスのIPSec VPNは、NSaシリーズが、何千もの他の大規模な施設、支社オフィスまたは自宅オフィスのためにVPNコネクタとして行動することを可能にします。
SSL VPNまたはIPSecクライアントのリモートアクセス	さまざまなプラットフォームから電子メール、ファイル、コンピュータ、イントラネットサイト、およびアプリケーションへの簡単なアクセスのためにクラアントレスのSSL VPNテクノロジーまたは管理が簡単なIPSecクライアントを利用します。
冗長VPNゲートウェイ	複数のWANを使用している際には、VPNの全セッションにおいて、一次および二次のVPNをシームレスに自動のフェイルオーバーやフェイルバックできるように構成することが可能です。
ルートベースVPN	代替ルートを経由して、トラフィックをエンドポイント間でシームレスに再ルーティングことにより、VPNリンクにおいて動的ルーティングを実施する機能は、VPNトンネルが一時的に使用できない場合に、継続的なアップタイムを可能にします。

コンテンツ/コンテキスト認識	
機能	説明
ユーザーアクティビティの追跡	DPIを通じて取得された膨大な情報と組み合わせ、シームレスなAD/LDAP/Citrix/Terminal Services SSOの統合を通じてユーザーの身元確認と活動がわかるようになります。
GeoIP国トラフィック特定	特定の国に出入りするネットワークトラフィックを識別して制御し、既知のまたは疑わしい脅威活動元からの攻撃から保護するか、ネットワークから発生する疑わしいトラフィックを調査します。カスタムで国およびボットネットリストを作成し、IPアドレスに関連付けられた誤った国またはボットネットタグを上書きすることができる機能です。誤った分類によるIPアドレスの不要なフィルタリングを排除します。
正規表現によるDPIフィルタリング	正規表現によるマッチングにより、ネットワークで交わされるコンテンツを識別および制御し、データ漏洩を防ぎます。カスタムで国およびボットネットリストを作成して、IPアドレスに関連付けられた誤った国またはボットネットタグを上書きすることができる機能を提供します。

侵害防御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 サンドボックス	仮想化サンドボックス、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解析テクノロジーを含むマルチエンジン サンドボックス プラットフォームは、疑わしいコードを実行し、動作を解析し、悪意のあるアクティビティの包括的な可視化を行います。
Real-Time Deep Memory Inspection (RTDMI)	SonicWallのRTDMIテクノロジーは、悪意のある動作を示さない、暗号化によって武器を潜ませているマルウェアを検出してブロックします。そしてRTDMIのエンジンは、マルウェアがその武器をメモリに「明かす」よう仕向けることにより、大量に出回っているゼロデイ攻撃の脅威と未知のマルウェアを事前に検出し、ブロックします。
判定が下されるまでブロック	悪意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に、結果が出るまで、解析のためにクラウド・サービスに送信されたファイルをゲートウェイで保持します。
幅広いファイルのタイプとサイズの解析	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、さらにWindows、Android、Mac OS Xを含む複数のオペレーティングシステム、およびマルチブラウザ環境を含む、幅広いファイルタイプの個別あるいはグループとしての解析をサポートします。
シグネチャを迅速に展開	ファイルが悪意のあるものとして識別された場合、48時間以内に、SonicWall Capture ATPサブスクリプション、ゲートウェイ型アンチウイルスおよびIPSシグネチャのデータベース、URL、IPおよびドメインレピュテーションのデータベースを備えたファイアウォールにシグネチャが即時に展開されます。
Capture Client	Capture Clientは、高度なマルウェア対策や暗号化されたトラフィックの可視化サポートを含む、複合エンドポイント保護機能を提供する統合クライアントプラットフォームです。階層化された保護テクノロジー、包括的なレポーティング、およびエンドポイント保護の実施を活用します。
暗号化された脅威の防御	
機能	説明
TLS/SSLの復号化およびインスペクション	TLS、SSLで暗号化されたトラフィックをプロキシを使用せずにマルウェア、侵入、およびデータ漏洩についてリアルタイムで復号および検査し、アプリケーション、URL、およびコンテンツ制御ポリシーを適用して、暗号化されたトラフィックに隠された脅威から保護します。全NSaシリーズモデルのセキュリティサブスクリプションが含まれます。
SSH インスペクション	SSH (DPI-SSH) のディープパケットインスペクションは、SSHトンネルを通過するデータを復号および検査して、SSHを活用する攻撃を防止します。
侵入防止	
機能	説明
対策ベースの保護	緊密に統合された侵入防止システム (IPS) は、広範な攻撃と脆弱性をカバーし、シグネチャや他の対策を活用して、脆弱性とエクスプロイトを調べるためにパケットペイロードをスキャンします。
自動シグネチャアップデート	SonicWall脅威調査チームは、継続的に調査し、50を超える攻撃カテゴリをカバーするIPS対策の広範なリストのアップデートを展開しています。新しいアップデートは、再起動やサービスの中断を必要とせずに即座に有効となります。
ゾーン内IPS保護	侵入防止によってネットワークを複数のセキュリティゾーンにセグメント化することで内部セキュリティを強化し、脅威がゾーンの境界を越えて侵入してくるのを防ぎます。
ボットネットのコマンドと制御 (CnC) の検知とブロック	ローカルネットワークのボットから、マルウェアの伝達をしている、または既知のCnCポイントであると特定されたIPおよびドメインへの、コマンドおよび制御のトラフィックを識別し、ブロックします。
プロトコルの悪用/異常	IPSを回避するためのプロトコルを悪用する攻撃を識別してブロックします。
ゼロデイ攻撃からの保護	何千もの個々のエクスプロイトを対象とする最新のエクスプロイト方法と技術を常にアップデートすることにより、ゼロデイ攻撃からネットワークを保護します。
回避に対抗するテクノロジー	広範なストリームの正常化、デコード、その他の方法により、第2〜7層における回避方法を利用して脅威が検出されることなくネットワークに侵入しないようにします。
脅威防御	
機能	説明
ゲートウェイアンチマルウェア	RFDPIエンジンは、すべてのポートとTCPストリームにわたって、長さやサイズが無制限のファイル内のウイルス、トロイの木馬、キーロガー、およびその他のマルウェアを検出するために、インバウンド、アウトバウンド、およびゾーン内トラフィックをすべてスキャンします。
Capture Cloudマルウェア防御	SonicWallクラウドサーバーに存在し、何千万もの継続的に更新されるため脅威シグネチャのデータベースは、オンボードシグネチャデータベースの機能を強化するために参照され、RFDPIが広範囲の脅威を対象とするようにします。
24時間体制のセキュリティ更新	新しい脅威の更新は、アクティブなセキュリティサービスがあるフィールドのファイアウォールに自動的にプッシュされ、再起動や中断することなく即座に有効になります。
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にスキャンすることができ、いくつかのよく知られたポートの保護に焦点を当てている旧式のセキュリティシステムによって侵入される攻撃を防ぎます。
広範なプロトコルのサポート	生のTCPでデータを送信しないHTTP/S、FTP、SMTP、SMBv1/v2などの一般的なプロトコルを識別し、標準の既知のポートで実行されていない場合であっても、マルウェアインスペクション用のペイロードをデコードします。
アプリケーションのインテリジェンスと制御	
機能	説明
アプリケーションの制御	ネットワークセキュリティを強化し、ネットワークの生産性を向上させるために、拡大し続ける数千を超えるアプリケーションシグネチャを含むデータベースに照らし合わせて、RFDPIエンジンによって特定されたアプリケーションまたは個々のアプリケーション機能を制御します。

カスタムアプリケーションの特定	ネットワークの制御を向上させるために、ネットワーク通信のアプリケーションに固有の特定のパラメーターまたはパターンに基づいてシグネチャを作成することにより、カスタムアプリケーションを制御します。
アプリケーション帯域幅の管理	重要ではないアプリケーショントラフィックを抑制しながら、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の利用可能な帯域幅をきめ細かく割り当て、調整します。
きめ細かい制御	スケジュール、ユーザーグループ、除外リスト、およびLDAP/AD/ターミナルサービス/Citrix統合を介した完全なSSOユーザー識別による一連のアクションに基づいて、アプリケーションまたは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	許容可能な使用ポリシーを適用し、コンテンツフィルタリングサービスおよびコンテンツフィルタリングクライアントを使用して、好ましくないまたは生産的でない情報や画像を含むHTTP/ HTTPSウェブサイトへのアクセスをブロックします。
強制コンテンツフィルタリングクライアント	ファイアウォールの境界外にあるWindows、Mac OS、Android、Chromeデバイスのインターネットコンテンツをブロックするためにポリシーの適用を拡張します。
きめ細かい制御	定義済みのカテゴリまたは任意で組み合わせたカテゴリを使用して、コンテンツをブロックします。フィルタリングは、授業が行われている時や営業時間などの時刻ごとにスケジュールし、個々のユーザーまたはグループに適用することができます。
ウェブキャッシング	URLの評価は、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、頻繁にアクセスするサイトへの後続のアクセスへの応答時間はほんのわずかです。

ウイルスおよびスパイウェア対策の実施

機能	説明
多層での保護	ラップトップ、大容量USBメモリー、その他の保護されていないシステムを介してネットワークに侵入するウイルスをブロックするエンドポイント保護に組み合わせ、ファイアウォール機能を境界での防御の最初の層として利用します。
自動実行オプション	ネットワークにアクセスするすべてのコンピュータに適切なウイルス対策ソフトウェアやDPI-SSL証明書がインストールされ、アクティブになっていることを確認し、通常デスクトップでのウイルス対策管理に伴うコストを排除します。
自動展開およびインストールのオプション	アンチウイルスおよびアンチスパイウェアクライアントのコンピュータごとの展開とインストールは、ネットワーク全体で自動的に行われ、管理のためのオーバーヘッドを最小限に抑えます。
次世代のウイルス対策	キャプチャクライアントが静的人工知能 (AI) エンジンを使用して、脅威が実行される前にそれを判断し、感染前の状態にロールバックします。
スパイウェアからの保護	強力なスパイウェア保護機能によってスキャンを行い、スパイウェアが機密データを送信する前にデスクトップおよびラップトップへの包括的な種類のスパイウェアプログラムのインストールブロックし、デスクトップのセキュリティとパフォーマンスを向上させます。

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
- リモートアクセスのためのバイオメトリック認証
- DNSプロキシ
- REST API

TLS/SSL/SSH復号化およびインスペクション[1]

- LS/SSL/SSH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、ホスト名の受け入れ/除外
- TLS/SSL制御
- きめ細かいDPI SSL制御 (ゾーンまたはルール別)

Capture Advanced Threat Protection[1]

- Real-Time Deep Memory Inspection
- クラウドベースのマルチエンジン解析
- 仮想化されたサンドボックス
- ハイパーバイザーレベル解析
- フルシステム エミュレーション
- 広範なファイルタイプの検査
- 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更新
- 判定が下されるまでブロック
- Capture Client

侵入防止[1]

- シグネチャベースのスキャン
- 自動シグネチャアップデート
- 双方向のインスペクション
- 粒度の細かいIPSルール機能
- GeoIPの実施
- 動的リストによるボットネットフィルタリング
- 正規表現マッチング

マルウェア対策[1]

- ストリームベースのマルウェアスキャン
- ゲートウェイ型アンチウイルス
- ゲートウェイアンチスパイウェア
- 双方向のインスペクション
- 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
- 追加帯域幅の管理
- カスタムのアプリケーションとシグネチャの作成
- データ漏洩の防御
- NetFlow/IPFIXを介したアプリケーションレポーティング
- 包括的なアプリケーションのシグネチャデータベース

トラフィックの可視化と解析

- 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
- クラウドベースの解析

HTTP/HTTPSウェブコンテンツフィルタリング[1]

- URLフィルタリング
- プロキシ回避
- キーワードブロック
- ポリシーベースのフィルタリング (除外/受け入れ)
- HTTPヘッダー挿入
- 帯域幅管理CFSの評価カテゴリ
- アプリ制御機能付き統一ポリシーモデル
- コンテンツフィルタリングクライアント

VPN

- 自動プロビジョンVPN
- 拠点間接続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およびKindle Fireへのモバイル接続
- ルートベースVPN (OSPF, RIP, BGP)

ネットワーク

- 安全なSD-WAN
- PortShield
- 大型フレーム
- 向上されたロギング
- VLANトランキング
- RSTP (Rapid Spanning Tree Protocol)
- ポートミラーイング
- 第2層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
- DNSセキュリティ
- DHCPサーバー
- 帯域幅管理
- リンクの集約 (静的および動的)
- ポートの冗長性
- A/P 高可用性 (状態の同期化を含む)
- A/A クラスタリング
- インバウンド/アウトバウンド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、モードをタップ
- 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

- WIDS/WIPS
- RFスペクトル解析
- 不正AP防御
- 高速ローミング (802.11k/r/v)
- 自動チャネル選択
- フロアプランビュー/トポロジービュー
- バンドステアリング
- ビームフォーミング
- AirTimeフェアネス
- MiFi拡張
- ゲストの周期的割り当て
- LHMゲストポータル

VoIP

- きめの細かいQoS制御
- 帯域幅管理
- SIPおよびH.323変換 (アクセスルールごと)
- H.323ゲートキーパーおよびSIPプロキシサポート

管理とモニタリング

- Capture Security Center、GMS、Web UI、CLI、REST API、SNMPv2/v3
- ロギング
- Netflow/IPFixレポーティング
- クラウドベースの構成バックアップ
- BlueCoatセキュリティ解析プラットフォーム
- SonicWallアクセスポイント管理
- カスケードスイッチを含むDell NシリーズおよびXシリーズのスイッチ管理

ローカルストレージ

- ログ
- レポート
- ファームウェアのバックアップ

[1]追加のサブスクリプションが必要です

SONICWALL®

NSaシリーズのシステム仕様

ファイアウォール全般	NSa 2650	NSa 3650	NSa 4650	NSa 5650
オペレーティングシステム	SonicOS 6.5.4			
インターフェース	4 x 2.5-GbE SFP、 4 x 2.5-GbE、 12 x 1-GbE、 1 GbE管理、 コンソール1台	2 x 10-GbE SFP+、 8 x 2.5-GbE SFP、 4 x 2.5-GbE、 12 x 1-GbE、 1 GbE管理、 コンソール1台	2 x 10-GbE SFP+、 4 x 2.5-GbE SFP、 4 x 2.5-GbE、 16 x 1-GbE、 1 GbE管理、 コンソール1台	2 x 10-GbE SFP+、 2 x 10-GbE、 4 x 2.5-GbE SFP、 4 x 2.5-GbE、 16 x 1-GbE、 1 GbE管理、 コンソール1台
拡張	1 拡張スロット (背面)*			
ビルトインのストレージ (SSD)	16 GB	32 GB	32 GB	64 GB
管理	CL、SSH、Web UI、Capture Security Center、GMS、REST API			
SSOユーザー	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	48	96	128	192
ロギング	Analyzer、Local Log、Syslog			

ファイアウォール/VPNのパフォーマンス	NSa 2650	NSa 3650	NSa 4650	NSa 5650
ファイアウォールインスペクションスループット[1]	3.0 Gbps	3.75 Gbps	6.0 Gbps	6.25 Gbps
脅威防止スループット[2]	1.5 Gbps	1.75 Gbps	2.5 Gbps	3.4 Gbps
アプリケーションインスペクションスループット[2]	1.85 Gbps	2.1 Gbps	3.0 Gbps	4.25 Gbps
IPSスループット[2]	1.4 Gbps	1.8 Gbps	2.3 Gbps	3.4 Gbps
マルウェア対策インスペクションスループット[2]	1.3 Gbps	1.5 Gbps	2.45 Gbps	2.8 Gbps
TLS/SSL復号化インスペクションスループット (DPI SSL)[2]	300 Mbps	320 Mbps	675 Mbps	800 Mbps
VPNスループット[3]	1.45 Gbps	1.5 Gbps	3.0 Gbps	3.5 Gbps
コネクション数/秒	14,000/秒	14,000/秒	40,000/秒	40,000/秒
最大コネクション数 (SPI)	1,000,000	2,000,000	3,000,000	4,000,000
最大コネクション数 (DPI)	500,000	750,000	1,000,000	1,500,000
DPI SSLコネクション数 (標準/最大)	60,000/100,000	40,000/100,000	145,000/175,000	125,000/175,000

VPN	NSa 2650	NSa 3650	NSa 4650	NSa 5650
サイト間トンネル	1,000	3,000	4,000	6,000
IPSec VPNクライアント (最大)	50 (1,000)	500 (3,000)	2,000 (4,000)	2,000 (6,000)
SSL VPN NetExtenderクライアント (最大)	2 (350)	2 (500)	2 (1,000)	2 (1,500)
暗号化/認証	DES、3DES、AES (128, 192, 256ビット)/MD5、SHA-1、Suite B暗号方式			
キー交換	Diffie Hellman グループ 1、2、5、14v			
ルートベースVPN	RIP、OSPF、BGP			

ネットワーク	NSa 2650	NSa 3650	NSa 4650	NSa 5650
IPアドレス割り当て	固定 (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IP)、PAT、トランスペアレントモード			
VLANインターフェース	256	256	400	500
ルーティングプロトコル	BGP、OSPF、RIPv1/v2、スタティックルート、ポリシーベースルーティング			
QoS	帯域幅優先度、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、ターミナルサービス、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			
認証規格 (申請中)	ICSA Firewall、ICSA Anti-Virus、FIPS 140-2、Common Criteria NDPP (Firewall and IPS)、UC APL、USGv6, CsFC			
高可用性[5]	Active/Passive (State Sync)	Active/Passive (State Sync) Active/Active クラスタリング		Active/Passive (State Sync)、 Active/Active DPI (State Sync)、 Active/Active クラスタリング

ハードウェア	NSa 2650	NSa 3650	NSa 4650	NSa 5650
電源	デュアル、冗長 120W (1個含む)		デュアル、冗長 350W (1個含む)	
ファン	デュアル、固定		デュアル、取り外し可能	
入力電源	100〜240 VAC、50〜60 Hz			
最大消費電力 (W)	37.2	46	93.6	103.6
MTBF @25°C (時間)	162,231	156,681	154,529	153,243
MTBF @25°C (年)	18.5	17.9	17.6	17.5
フォームファクタ	1U ラックマウント型			
寸法	43 x 32.5 x 4.5 cm		43 x 41.5 x 4.5 cm	
重量	5.2 kg	5.3 kg	6.9 kg	6.9 kg
WEEE重量	5.5 kg	5.6 kg	8.9 kg	8.9 kg
出荷時の重量	7.7 kg	7.8 kg	11.3 kg	11.3 kg
主要な法規制準拠	FCC Class A、CE (EMC、LVD、RoHS)、C-Tick、VCCI Class A、MSIP/KCC Class A、UL、cUL、TUV/GS、CB、Mexico CoC by UL、WEEE、REACH、ANATEL、BSMI			
環境 (操作/ストレージ)	0〜40℃/-40〜70℃			
湿度	10〜90 % (結露しないこと)			

Nsaシリーズのシステム仕様 (続き)

ファイアウォール全般	NSa 6650	NSa 9250	NSa 9450	NSa 9650
オペレーティングシステム	SonicOS 6.5.4			
インターフェース	6 x 10-GbE SFP+、 2 x 10-GbE、 4 x 2.5-GbE SFP、 8 x 2.5-GbE、 8 x 1-GbE、 1 GbE管理、 コンソール1台	10 x 10-GbE SFP+、 2 x 10-GbE、 8 x 2.5-GbE、 8 x 1-GbE、 1 GbE管理、 コンソール1台	10 x 10-GbE SFP+、 2 x 10-GbE、 8 x 2.5-GbE、 8 x 1-GbE、 1 GbE管理、 コンソール1台	10 x 10-GbE SFP+、 2 x 10-GbE、 8 x 2.5-GbE、 8 x 1-GbE、 1 GbE管理、 コンソール1台
拡張	1 拡張スロット (背面)*			
ビルトインのストレージ (SSD)	64 GB	1TB、128 GB	1TB、128 GB	1TB、256 GB
管理	CL、SSH、Web UI、 Capture Security Center、 GMS、REST API	CL、SSH、Web UI、GMS、REST API		
SSOユーザー	70,000	80,000	90,000	100,000
サポートされる最大アクセスポイント数	192	192	192	192
ロギング	Analyzer、Local Log、Syslog、IPFIX、NetFlow			

ファイアウォール/VPNのパフォーマンス	NSa 6650	NSa 9250	NSa 9450	NSa 9650
ファイアウォールインスペクションスループット[1]	12.0 Gbps	12.0 Gbps	17.1 Gbps	17.1 Gbps
脅威防止スループット[2]	5.5 Gbps	6.5 Gbps	9.0 Gbps	9.4 Gbps
アプリケーションインスペクションスループット[2]	6.0 Gbps	7.8 Gbps	10.8 Gbps	11.5 Gbps
IPSスループット[2]	6.0 Gbps	7.2 Gbps	10.2 Gbps	10.3 Gbps
マルウェア対策インスペクションスループット[2]	5.4 Gbps	6.5 Gbps	8.0 Gbps	8.5 Gbps
TLS/SSL復号化インスペクションスループット (DPI SSL)[2]	1.45 Gbps	1.5 Gbps	2.1 Gbps	2.25 Gbps
VPNスループット[3]	6.0 Gbps	6.75 Gbps	10.0 Gbps	10.0 Gbps
コネクション数/秒	90,000/秒	90,000/秒	130,000/秒	130,000/秒
最大コネクション数 (SPI)	5,000,000	7,500,000	10,000,000	12,500,000
最大コネクション数 (DPI)	2,000,000	3,000,000	4,000,000	5,000,000
DPI SSLコネクション数 (標準/最大)	170,000 /250,000	170,000/250,000	290,000/450,000	320,000/550,000

VPN	NSa 6650	NSa 9250	NSa 9450	NSa 9650
サイト間トンネル	8,000	12,000	12,000	12,000
IPSec VPNクライアント (最大)	2,000 (6,000)	2,000 (6,000)	2,000 (6,000)	2,000 (6,000)
SSL VPN NetExtenderクライアント (最大)	2 (2,000)	2 (3,000)	2 (3,000)	50 (3,000)
暗号化/認証	DES、3DES、AES (128, 192, 256ビット)/MD5、SHA-1、Suite B暗号方式			
キー交換	Diffie Hellman グループ 1、2、5、14v			
ルートベースVPN	RIP、OSPF、BGP			

ネットワーク	NSa 6650	NSa 9250	NSa 9450	NSa 9650
IPアドレス割り当て	固定 (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IP)、PAT、トランスペアレントモード			
VLANインターフェース	512			
ルーティングプロトコル	BGP、OSPF、RIPv1/v2、スタティックルート、ポリシーベースルーティング			
QoS	帯域幅優先度、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、ターミナルサービス、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			
認証規格 (申請中)	ICSA Firewall、ICSA Anti-Virus、FIPS 140-2、Common Criteria NDPP (Firewall and IPS)、UC APL、USGv6, CsFC			
高可用性[5]	Active/Passive (State Sync)、Active/Active DPI (State Sync)、Active/Active クラスタリング			

ハードウェア	NSa 6650	NSa 9250	NSa 9450	NSa 9650
電源	デュアル、冗長 350W (1個含む)	デュアル、冗長、350W		
ファン	トリプル、取り外し可能			
入力電源	100〜240 VAC、50〜60 Hz			
最大消費電力 (W)	144.3	86.7	90.9	113.1
MTBF @25°C (時間)	157,193	139,783	134,900	116,477
MTBF @25°C (年)	17.9	15.96	15.4	13.3
フォームファクタ	1U ラックマウント型			
寸法	43 x 41.5 x 4.5 cm			
重量	8.1 kg	8.1 kg		
WEEE重量	10.2 kg	10.2 kg		
出荷時の重量	12.6 kg	12.6 kg		
主要な法規制準拠	FCC Class A、CE (EMC、LVD、RoHS)、C-Tick、VCCI Class A、MSIP/KCC Class A、UL、cUL、TUV/GS、CB、Mexico CoC by UL、 WEEE、REACH、ANATEL、BSMI			
環境 (操作/ストレージ)	0〜40℃/-40〜70℃			
湿度	10〜90 % (結露しないこと)			

[1]テスト手法：最大スループットは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/ゲートウェイアンチウイルス/アンチスパイウェア/IPS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およびIxiaテストツールを使用して測定しています。テストには、複数のポートペアに対する複数フローを用いて行っています。脅威防御スループットは、ゲートウェイアンチウイルス、アンチスパイウェア、IPSおよびアプリケーション制御を有効にして測定しています。DPI SSLパフォーマンスは、IPSを有効にしてHTTPSで測定しています。
[3] VPNスループットは、RFC 2544準拠のパケットサイズ (1,280バイト) のUDPトラフィックを使用して測定しています。すべての仕様、機能、および在庫状況は、変更されることがあります。
[4]125,000 DPIの接続減少ごとに、利用可能なDPI SSL接続は3,000増加します。ただし、NSa 9250以上にはこれは適用されません。
[5] Active/Activeクラスタリングと Active/Active DPI with State Syncには、拡張ライセンスの購入が必要となります。ただし、NSa 9250以上にはこれは適用されません。
**将来使用。すべての仕様、機能、および在庫状況は、変更されることがあります。*

NSaシリーズのご注文に関する情報

NSa 2650	SKU
NSa 2650 TotalSecure Advanced Edition (1-year)	01-SSC-1988
NSa 2650向けのAdvanced Gateway Security Suite – Capture ATP、脅威防御、ファイアウォール管理とレポーティング、Shadow ITの可視化、および毎日24時間体制のサポート (1年間)	01-SSC-1783
NSa 2650向けCapture Advanced Threat Protection (1年間)	01-SSC-1935
脅威防御 – 侵入防止、ゲートウェイ型アンチウイルス、ゲートウェイ型アンチスパイウェア、NSa 2650向けクラウドアンチウイルス (1年間)	01-SSC-1976
NSa2650向け毎日24時間体制のサポート (1年間)	01-SSC-1541
NSa 2650向けコンテンツフィルタリングサービス (1年間)	01-SSC-1970
Capture Client	ユーザー数に基づく
NSa 2650向け包括的アンチスパムサービス (1年間)	01-SSC-2001
NSa 3650	**SKU**
NSa 3650 TotalSecure Advanced Edition (1-year)	01-SSC-4081
NSa 3650向けのAdvanced Gateway Security Suite – Capture ATP、脅威防御、ファイアウォール管理とレポーティング、Shadow ITの可視化、および毎日24時間体制のサポート (1年間)	01-SSC-3451
NSa 3650向けCapture Advanced Threat Protection (1年間)	01-SSC-3457
脅威防御 – 侵入防止、ゲートウェイ型アンチウイルス、ゲートウェイ型アンチスパイウェア、NSa 3650向けクラウドアンチウイルス (1年間)	01-SSC-3632
NSa3650向け毎日24時間体制のサポート (1年間)	01-SSC-3439
NSa 3650向けコンテンツフィルタリングサービス (1年間)	01-SSC-3469
Capture Client	ユーザー数に基づく
NSa 3650向け包括的アンチスパムサービス (1年間)	01-SSC-4030
NSa 4650	**SKU**
NSa 4650 TotalSecure Advanced Edition (1-year)	01-SSC-4094
NSa 4650向けのAdvanced Gateway Security Suite – Capture ATP、脅威防御、ファイアウォール管理とレポーティング、Shadow ITの可視化、および毎日24時間体制のサポート (1年間)	01-SSC-3493
NSa 4650向けCapture Advanced Threat Protection (1年間)	01-SSC-3499
脅威防御 – 侵入防止、ゲートウェイ型アンチウイルス、ゲートウェイ型アンチスパイウェア、NSa 4650向けクラウドアンチウイルス (1年間)	01-SSC-3589
NSa4650向け毎日24時間体制のサポート (1年間)	01-SSC-3487
NSa 4650向けコンテンツフィルタリングサービス (1年間)	01-SSC-3583
Capture Client	ユーザー数に基づく
NSa 4650向け包括的アンチスパムサービス (1年間)	01-SSC-4062
NSa 5650	**SKU**
NSa 5650 TotalSecure Advanced Edition (1-year)	01-SSC-4342
NSa 5650向けのAdvanced Gateway Security Suite – Capture ATP、脅威防御、ファイアウォール管理とレポーティング、Shadow ITの可視化、および毎日24時間体制のサポート (1年間)	01-SSC-3674
NSa 5650向けCapture Advanced Threat Protection (1年間)	01-SSC-3680
脅威防御 – 侵入防止、ゲートウェイ型アンチウイルス、ゲートウェイ型アンチスパイウェア、NSa 5650向けクラウドアンチウイルス (1年間)	01-SSC-3698
NSa5650向け毎日24時間体制のサポート (1年間)	01-SSC-3660
NSa 5650向けコンテンツフィルタリングサービス (1年間)	01-SSC-3692
Capture Client	ユーザー数に基づく
NSa 5650向け包括的アンチスパムサービス (1年間)	01-SSC-4068
NSa 6650	**SKU**
NSa 6650 TotalSecure Advanced Edition (1-year)	01-SSC-2209
NSa 6650向けのAdvanced Gateway Security Suite – Capture ATP、脅威防御、ファイアウォール管理とレポーティング、Shadow ITの可視化、および毎日24時間体制のサポート (1年間)	01-SSC-8761
NSa 6650向けCapture Advanced Threat Protection (1年間)	01-SSC-8930
脅威防御 – 侵入防止、ゲートウェイ型アンチウイルス、ゲートウェイ型アンチスパイウェア、NSa 6650向けクラウドアンチウイルス (1年間)	01-SSC-8979
NSa6650向け毎日24時間体制のサポート (1年間)	01-SSC-8663
NSa 6650向けコンテンツフィルタリングサービス (1年間)	01-SSC-8972
Capture Client	ユーザー数に基づく
NSa 6650向け包括的アンチスパムサービス (1年間)	01-SSC-9131
NSa 9250	**SKU**
NSa 9250 TotalSecure Advanced Edition (1-year)	01-SSC-2854
NSa 9250向けのAdvanced Gateway Security Suite – Capture ATP、脅威防御、ファイアウォール管理とレポーティング、Shadow ITの可視化、および毎日24時間体制のサポート (1年間)	01-SSC-0038
NSa 9250向けCapture Advanced Threat Protection (1年間)	01-SSC-0121
脅威防御 – 侵入防止、ゲートウェイ型アンチウイルス、ゲートウェイ型アンチスパイウェア、NSa 9250向けクラウドアンチウイルス (1年間)	01-SSC-0343
NSa9250向け毎日24時間体制のサポート (1年間)	01-SSC-0032
NSa 9250向けコンテンツフィルタリングサービス (1年間)	01-SSC-0331
Capture Client	ユーザー数に基づく
NSa 9450	**SKU**
NSa 9450 TotalSecure Advanced Edition (1-year)	01-SSC-4358
NSa 9450向けのAdvanced Gateway Security Suite – Capture ATP、脅威防御、ファイアウォール管理とレポーティング、Shadow ITの可視化、および毎日24時間体制のサポート (1年間)	01-SSC-0414
NSa 9450向けCapture Advanced Threat Protection (1年間)	01-SSC-0855

NSaシリーズのご注文に関する情報 (続き)

NSa 9450	SKU
脅威防御 – 侵入防止、ゲートウェイ型アンチウイルス、ゲートウェイ型アンチスパイウェア、NSa 9450向けクラウドアンチウイルス (1年間)	01-SSC-1196
NSa 9450 0向け毎日24時間体制のサポート (1年間)	01-SSC-0407
NSa 9450向けコンテンツフィルタリングサービス (1年間)	01-SSC-1158
Capture Client	ユーザー数に基づく
NSa 9650	**SKU**
NSa 9650 TotalSecure Advanced Edition (1-year)	01-SSC-3475
NSa 9650向けのAdvanced Gateway Security Suite – Capture ATP、脅威防御、ファイアウォール管理とレポーティング、Shadow ITの可視化、および毎日24時間体制のサポート (1年間)	01-SSC-2036
NSa 9650向けCapture Advanced Threat Protection (1年間)	01-SSC-2042
脅威防御 – 侵入防止、ゲートウェイ型アンチウイルス、ゲートウェイ型アンチスパイウェア、NSa 9650向けクラウドアンチウイルス (1年間)	01-SSC-2142
NSa 9650 0向け毎日24時間体制のサポート (1年間)	01-SSC-1989
NSa 9650向けコンテンツフィルタリングサービス (1年間)	01-SSC-2136
Capture Client	ユーザー数に基づく
モジュールと付属品*	**SKU**
10GBASE-SR SFP+ Short Reach Module	01-SSC-9785
10GBASE-LR SFP+ Long Reach Module	01-SSC-9786
10GBASE SFP+ 1M Twinax Cable	01-SSC-9787
10GBASE SFP+ 3M Twinax Cable	01-SSC-9788
1000BASE-SX SFP Short Haul Module	01-SSC-9789
1000BASE-LX SFP Long Haul Module	01-SSC-9790
1000BASE-T SFP Copper Module	01-SSC-9791

*サポートされるSFPおよびSFP+モジュールの完全なリストについては、最寄りのSonicWall代理店までお問い合わせください。

SonicWall NSa/NSv ファイアウォールバンドル

次のNSaシリーズのファイアウォールは、対応するNSv Virtual Appliance TotalSecureの1年間のサブスクリプション* を無料で受け取る資格があります。

対象となるNSaのファイアウォール	対応するNSvのファイアウォール
NSa 5650	NSv 200
NSa 6650	NSv 200
NSa 9250	NSv 400
NSa 9450	NSv 400
NSa 9650	NSv 400

NSv Virtual Appliance TotalSecureのサブスクリプションには、NSvの仮想ファイアウォール、ゲートウェイ型アンチウイルス、アンチスパイウェア、侵入防止およびアプリケーションファイアウォールサービス、コンテンツフィルタリングサービス、および毎日24時間体制のサポートが含まれています。

規制モデル番号:

NSa 2650 - 1RK38-0C8
NSa 3650 - 1RK38-0C7
NSa 4650 - 1RK39-0C9
NSa 5650 - 1RK39-0CA
NSa 6650 - 1RK39-0CB
NSa 9250 - 1RK39-0CC
NSa 9450 - 1RK39-0CD
NSa 9650 - 1RK39-0CE

パートナー イネーブルド サービス

SonicWallのソリューションをプラン、展開、または最適化するための支援が必要ですか?SonicWall Advanced Services Partnersは、お客様にワールドクラスのサービスを提供するための訓練を受けています。詳細は、www.sonicwall.com/PESからご覧いただけます。

SonicWallについて

SonicWallは27年以上にわたってサイバー犯罪と戦い、世界中の中小企業や各種事業組織、政府機関を守り続けています。受賞歴のある当社のリアルタイム侵害検出・防止ソリューションは、SonicWall Capture Labsの研究によってその効果が裏付けられています。このソリューション群は、実に215以上の国と地域で、100万以上のネットワークとその中の電子メールやアプリケーション、データを保護しています。これによって多くの組織がより効果的に稼働し、セキュリティ上の懸念を軽減しているのです。詳しくは、www.sonicwall.comをご覧いただくか、Twitter、LinkedIn、 Facebook、Instagramをフォローしてください。

SonicWall Inc.
SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035 USA
その他の情報については、当社ウェブサイトをご覧ください。
www.sonicwall.com

Datasheet-NetworkSecurityAppliance-US-VG-MKTG5872