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と分散型企業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。NSa シリーズは、SonicWall Capture Cloud Platform の革新的なディープラーニング技術を利用して、組織が必要とする自動化されたリアルタイムの侵害の検出と防御を実現します。

パフォーマンスに優れた最先端の脅威防御

今日のネットワークに潜む脅威は、検出の回避に長けており、従来の検出方法を使用して特定することがますます困難になっています。高度な攻撃の先を行くには、クラウドのセキュリティインテリジェンスをフル活用した最新のアプローチが必要です。ゲートウェイセキュリティソリューションが今日の複雑な脅威に対応するには、クラウドインテリジェンスが不可欠です。NSa シリーズの次世代ファイアウォール (NGFW) は、2 つの高度なセキュリティ技術を統合して、一歩先を行く最先端のネットワーク脅威防御を実現します。マルチエンジンの SonicWall Capture Advanced Threat Protection (ATP) サービスを強化したのが、特許出願中の技術である Real-Time Deep Memory Inspection (RTDMI™) です。RTDMI エンジンはメモリ内を直接検査することで、大量に出回っているゼロデイ脅威と未知のマルウェアをプロアクティブに検出し、ブロックします。リアルタイムアーキテクチャにより、正確性に優れる SonicWall RTDMI 技術は誤検出を最小限に抑制し、マルウェアの武器を検出できる時間が 0.0001 ミリ秒にも満たない高度な攻撃を特定して軽減します。RTDMI と併用することで、SonicWall の特許取得済み * シングルパス Reassembly-Free Deep Packet Inspection (RFDPI) 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ファイアウォールで同時に検査します。侵入防止、マルウェア対策、Web/URL フィルタリングなどのオンボックス機能に加えて、SonicWall Capture Cloud Platform を活用することで、NSa シリーズは最新の潜伏性の脅威もゲートウェイでブロックします。

また、SonicWall ファイアウォールは、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、さらには定義された基準を検索します。ディープパケットインスペクションエンジンは、暗号化を利用した隠れた攻撃を検出して防ぎ、暗号化されたマルウェアのダウンロードをブロックし、感染の拡大を止めて、コマンド & コントロール (C&C) 通信とデータ漏洩を阻止します。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 IPS、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。RTDMI および RFDPI エンジンと組み合わせたこの独自の設計に

** 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

- 特許出願中の Real-Time Deep Memory Inspection テクノロジー
- 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

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。

ネットワークの制御と柔軟性

NS*a* 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および制御を使用して、アプリケーションが生産的なものであるか、非生産的または潜在的に危険なものであるかを特定、分類し、強力なアプリケーションレベルのポリシーでユーザー別またはグループ別にトラフィックを制御できます。その際、スケジュールや例外リストも併用します。業務上重要なアプリケーションでは帯域幅を優先的に使用し、重要度の低いアプリケーションでは帯域幅を抑制するように設定できます。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 NS*a* 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。

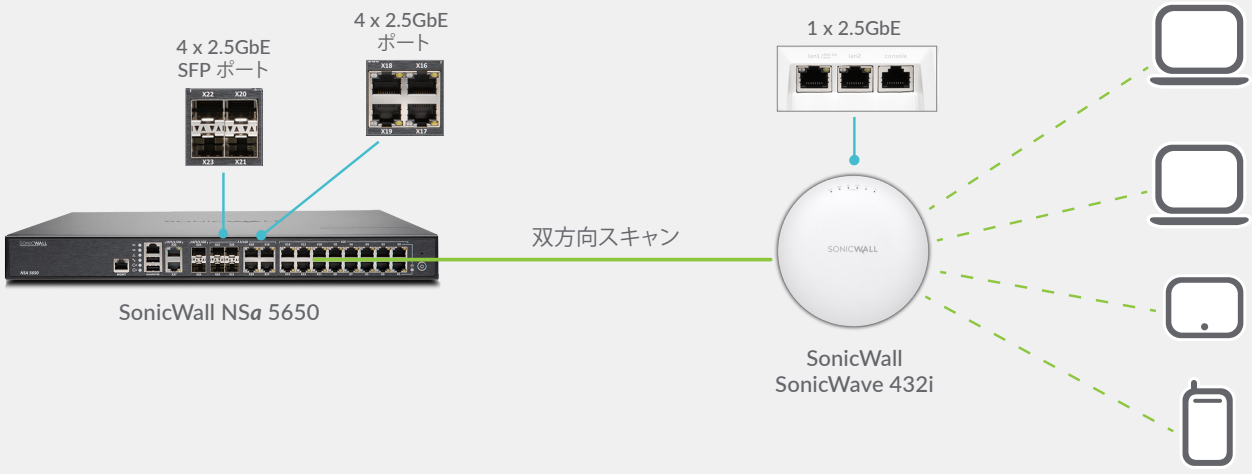
簡単な導入、セットアップ、および継続的な管理

すべての SonicWall ファイアウォールと同じように、NS*a* 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 NS*a* 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、監視、レポートは、ファイアウォールまたは SonicWall Capture Security Center 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

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。NS*a* シリーズの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。この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。



Capture Cloud Platform

SonicWall Capture Cloud Platform は、クラウドベースの脅威防御とネットワーク管理のほか、レポートと分析の機能をあらゆる規模の組織に提供します。このプラットフォームは、さまざまなソースから収集した脅威インテリジェンスを統合します。たとえば、賞を獲得したマルチエンジンの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、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を収集します。

ネットワークに入ってくるデータで未知の不正なコードが検出されると、SonicWall の社内に設置された専任の Capture Labs 脅威研究チームがシグネチャを開発します。このシグネチャは Capture Cloud Platform のデータベースに格納され、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されます。新たな更新内容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し、1 つのシグネチャで何万もの異なる脅威に対応します。NS*a* ファイアウォールは、アプライアンス上の対抗策に加えて、Capture Cloud Platform データベースに継続的にアクセスすることもできます。このデータベースにより、オンボードのシグネチャインテリジェンスは数千万のシグネチャで拡張されます。

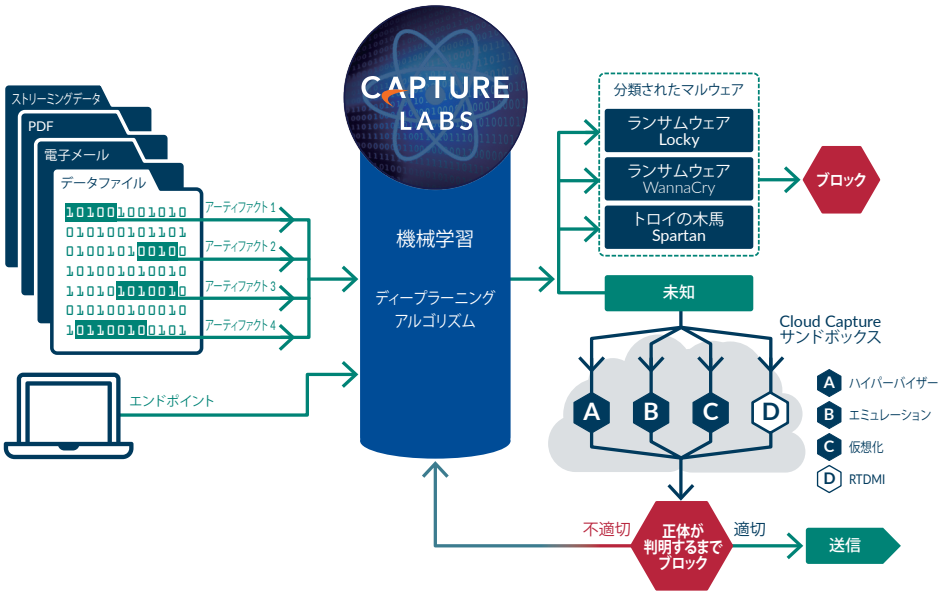
Capture Cloud Platform は、脅威防御に加えて一元的な管理を実現します。管理者は、ネットワークアクティビティに関するリアルタイムレポートと履歴レポートを容易に作成できます。

高度な脅威防御

自動化されたリアルタイムの侵入防止の中核を担うのが SonicWall Capture Advanced Threat Protection サービスです。このセキュリティサービスは、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防御を拡張してゼロデイ脅威を検出、防止します。疑わしいファイルはクラウドに送信され、ディープラーニングアルゴリズムを使用して分析され、判定が下るまでゲートウェイで保持することもできます。Real-Time Deep Memory Inspection、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。悪意のあるファイルであることが確認されると、そのファイルはブロックされ、Capture ATP 内でハッシュが即座に作成されます。この直後、以降の攻撃を防ぐためにシグネチャがファイアウォールに送られます。

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。

SonicWall Capture Client では、エンドポイントを全面的に保護するために、次世代のアンチウイルス技術と SonicWall のクラウドベースのマルチエンジンサンドボックスが統合されています。

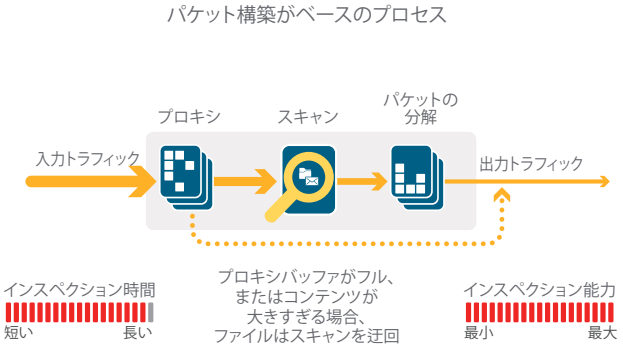


Reassembly-Free Deep Packet Inspection エンジン

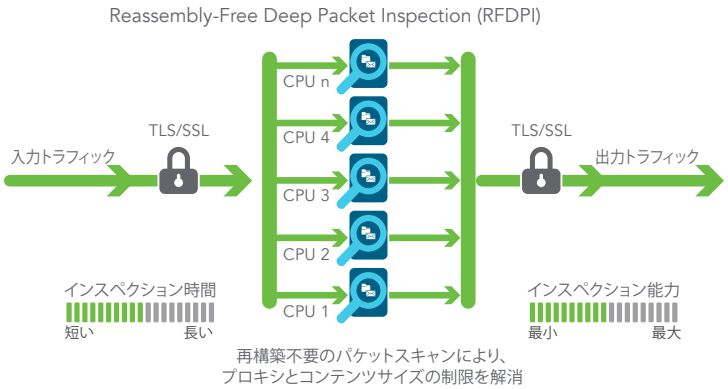
SonicWall Reassembly-Free Deep Packet Inspection (RFDPI) は、プロキシやバッファを必要とせずにストリームベースの双方向トラフィック分析を高速で実行するシングルパス、低レイテンシのインスペクションシステムであり、侵入の試みやマルウェアのダウンロードを効率的に発見すると同時に、ポートやプロトコルにかかわらずアプリケーションのトラフィックを特定します。この独自のエンジンは、レイヤ 3 ～ 7 で脅威を検出するストリーミングトラフィックペイロードのインスペクションに基づいて動作し、検出エンジンを混乱させて悪意のあるコードをネットワークに忍び込ませ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



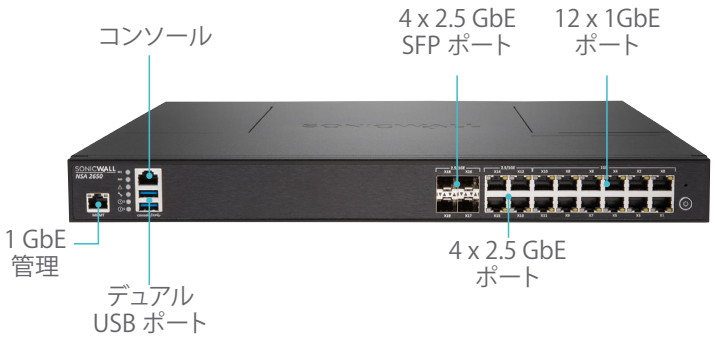
SonicWall のストリームベースのアーキテクチャ

グローバル管理およびレポート機能

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 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。企業は、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。さらに、企業はファイアウォールの変更管理要件をワークフローの自動化で満たします。この自動化により、適切なファイアウォールポリシーを適切なときに俊敏かつ確実に導入して、コンプライアンス規制に準拠することができます。オンプレミスでは SonicWall Global Management System、クラウドでは Capture Security Center をそれぞれ利用できる SonicWall の管理 / レポートソリューションは、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法を備えているので、デバイス単位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。

Network Security Appliance NS*a* 2650

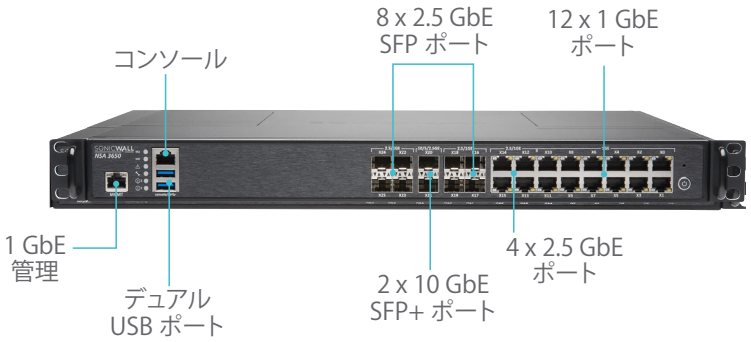
NS*a* 2650 は、中規模組織と分散エンタープライズの、数千の暗号化された接続と、それを超える数の暗号化されていない接続における、高速の脅威防御機能を提供します。

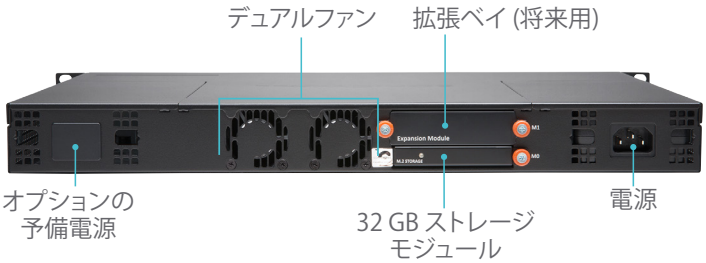


ファイアウォール	NS*a* 2650
ファイアウォールのスループット	3.0 Gbps
IPS のスループット	1.4 Gbps
アンチマルウェアのスループット	600 Mbps
フル DPI のスループット	600 Mbps
IMIX のスループット	700 Mbps
最大 DPI 接続数	500,000
新規接続数/秒	14,000/秒

Network Security Appliance NS*a* 3650

SonicWall NS*a* 3650 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。

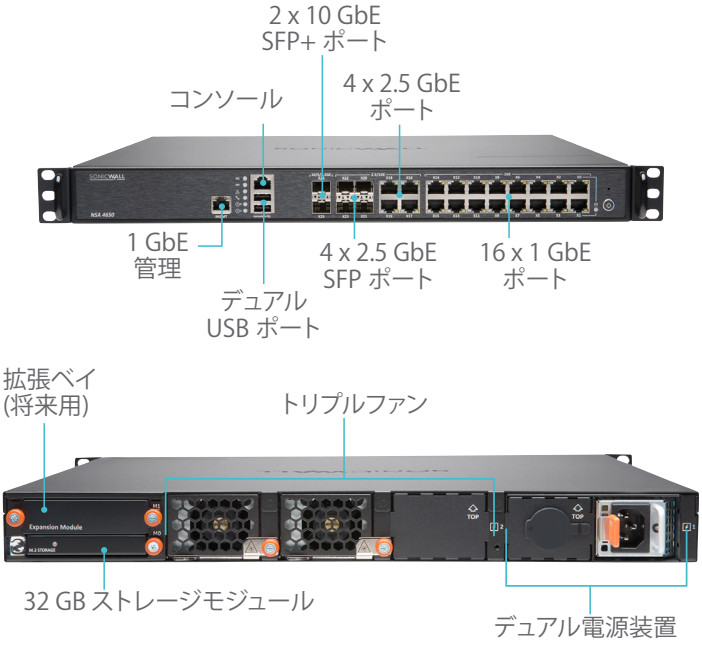




ファイアウォール	NS*a* 3650
ファイアウォールのスループット	3.75 Gbps
IPS のスループット	1.8 Gbps
アンチマルウェアのスループット	800 Mbps
フル DPI のスループット	730 Mbps
IMIX のスループット	900 Mbps
最大 DPI 接続数	750,000
新規接続数/秒	14,000/秒

Network Security Appliance NS*a* 4650

SonicWall NS*a* 4650 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	NS*a* 4650
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	2.3 Gbps
アンチマルウェアのスループット	1.25 Gbps
フル DPI のスループット	1.2 Gbps
IMIX のスループット	1.3 Gbps
最大 DPI 接続数	1,000,000
新規接続数/秒	40,000/秒

Network Security Appliance NS*a* 5650

SonicWall NS*a* 5650 は、高いスループットとポート密度を必要とする、分散したブランチオフィスや企業環境に最適です。

ファイアウォール	NS*a* 5650
ファイアウォールのスループット	6.25 Gbps
IPS のスループット	3.4 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	1.7 Gbps
IMIX のスループット	1.45 Gbps
最大 DPI 接続数	1,500,000
新規接続数/秒	40,000/秒

各種機能

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、すべての脅威情報を 1 つのアーキテクチャ内で確実に関連付けます。
ファイアウォールとネットワーキング	
機能	説明
REST 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を検査および分析し、ファイアウォールのアクセスポリシーに準拠させます。
高可用性/クラスタリング	NS*a* 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 攻撃を防御します。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	NS*a* 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。
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、およびレポート作成を行い、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。
サイト間接続型 IPSec VPN	ハイパフォーマンス IPSec VPN により、NS*a* 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 VPN	VPN リンク経由で動的ルーティングを実行する機能によって、エンドポイント間で代替ルート経由でトラフィックをシームレスに再ルーティングし、一時的な VPN トンネル障害時も確実にアップタイムを維持できます。

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	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 国別のトラフィック識別	特定の国へ、または特定の国からのネットワークトラフィックを識別してコントロールし、既知または疑わしい脅威の発信元からの攻撃を防御したり、ネットワークから発信されてい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
マルチエンジンサンドボックス	仮想サンドボックス、フルシステムエミュレーション、およびハイパーバイザーレベルの分析テクノロジーが搭載されたマルチエンジン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、動作を分析して、悪意のあるアクティビティに対する包括的な可視性を提供します。
Real-Time Deep Memory Inspection (RTDMI)	この特許出願中のクラウドベースの技術は、表立って悪意のある動作を実行せずにカスタム暗号化で武器を隠しているマルウェアを検出し、ブロックします。RTDMI エンジンは、メモリ内で武器を示すようにマルウェアに強制することで、大量に出回っているゼロデイ脅威と未知のマルウェアをプロアクティブに検出し、ブロックします。
正体が判明するまでブロック	脅威となり得るファイルがネットワークに侵入しないよう、分析対象としてクラウドに送られたファイルは、正体が判明するまでゲートウェイで保留にしておくことができます。
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	ファイルが不正であると特定されると、SonicWall Capture ATP サブスクリプションによってシグネチャがただちにファイアウォールへ導入され、ゲートウェイアンチウイルスおよび IPS シグネチャデータベースのほか、URL、IP、ドメインのレピュテーション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。
Capture Client	Capture Client は、高度なマルウェア防御、暗号化トラフィックへの可視化サポートなど、複数の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。このプラットフォームでは、多層型の保護技術、包括的なレポート機能、エンドポイント保護を利用できます。
暗号化された脅威防御	
機能	説明
TLS/SSL の復号化と検査	TLS/SSL 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、暗号化されたトラフィックに潜む脅威を防御します。NS*a* 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、シグネチャや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、幅広い種類の攻撃や脆弱性をカバーします。
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およびコントロール (CnC) の検知およびブロック	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。
プロトコル違反/異常	IPS による防御をすり抜けようと、プロトコルを不正に使用する攻撃を検知し、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が利用する最新の手口やテクニックに対抗できるように常に更新されているので、ゼロデイ攻撃からもネットワークを保護できます。
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
ゲートウェイでのマルウェア対策	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。
Capture Cloud のマルウェア対策	SonicWall のクラウドサーバーには数千万件に及ぶ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 TCP の生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 & コントロール	
機能	説明
アプリケーションの制御	RFDPI エンジンが識別するアプリケーションやアプリケーションの諸機能を、数千におよぶアプリケーションシグネチャが格納され、継続的に拡張されているデータベースと照合して制御することで、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
内部および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を利用して、利用ポリシーを適用し、好ましくない、または非生産的な情報や画像を掲載している 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	事前定義されてたカテゴリや、カテゴリの組み合わせを指定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時間中や営業時間中といった時間帯ごとに設定できるほか、個々のユーザーやグループに対して適用することもできます。
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への後続のアクセスには一瞬で応答が返されます。
アンチウイルス/アンチスパイウェアの適用	
機能	説明
マルチレイヤ保護	境界保護の最初のレイヤとしてファイアウォール機能を活用し、エンドポイント保護とを組み合わせることで、ノートパソコン、USB メディア、およびその他の保護されていないシステムからネットワークにウイルスが侵入するのを防ぎます。
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適切なアンチウイルスソフトウェアや DPI-SSL 証明書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	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マシンごとに自動的に行われるため、管理の余分な手間を最小限に抑えることができます。
次世代アンチウイルス	Capture Client は、静的な人工知能 (AI) エンジンを使用して実行可能になる前に脅威を判定し、以前の感染前の状態にロールバックします。
スパイウェア対策	強力なスパイウェア対策保護が多様なスパイウェアプログラムを検出し、デスクトップやノートパソコンにインストールされて機密情報を送信される前に、そのスパイウェアをブロックします。これにより、デスクトップのセキュリティとパフォーマンスが大幅に高まります。

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生体認証
- DNS プロキシ
- REST API

TLS/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
- TLS/SSL 制御

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更新
- 正体が判明するまでブロック
- Capture Client

侵入防止 [1]

- シグネチャベースのスキャン
- 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 [1]

- アプリケーションの制御
- 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
- アプリケーションの使用状況
- クラウドベースの分析

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
- 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

- 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、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
- 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
- DNS/DNS プロキシ
- 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

- WIDS/WIPS
- RF スペクトル分析
- 不正 AP 防御
- 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
- LHM ゲストポータル

VoIP

- 詳細な QoS 制御
- 帯域幅の管理
- アクセスルールごとの SIP および H.323 変換
- H.323 ゲートキーパーおよび SIP プロキシのサポート

管理と監視

- Capture Security Center、GMS、Web UI、CLI、REST API、SNMPv2/v3
- 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
- SonicWall アクセスポイント管理
- 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 2650	NSa 3650	NSa 4650	NSa 5650
オペレーティングシステム	SonicOS 6.5.1			
セキュリティ処理コア数	4	4	10	10
インターフェイス	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+、 8 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 2.5 GbE SFP、 4 x 2.5 GbE、 16 x 1 GbE、 1 GbE 管理、 1 コンソール	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、 1 コンソール
拡張	1 拡張スロット (背面)*			
組み込みのストレージ	16 GB	32 GB	32 GB	64 GB
管理	CLI、SSH、Web UI、Capture Security Center、GMS、REST API			
SSO ユーザー数	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
ログ	アナライザ、ローカルログ、システムログ			
ファイアウォール/VPN 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のスループット[1]	3.0 Gbps	3.75 Gbps	6.0 Gbps	6.25 Gbps
フル DPI のスループット[2]	600 Mbps	730 Mbps	1.2 Gbps	1.7 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]	1.4 Gbps	2.1 Gbps	3.0 Gbps	4.25 Gbps
IPS のスループット[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のスループット[2]	600 Mbps	800 Mbps	1.25 Gbps	1.7 Gbps
IMIX のスループット	700 Mbps	900 Mbps	1.3 Gbps	1.45 Gbps
TLS/SSL 復号化とインスペクションのスループット (DPI SSL)[2]	250 Mbps	300 Mbps	500 Mbps	800 Mbps
VPN のスループット[3]	1.3 Gbps	1.5 Gbps	3.0 Gbps	3.5 Gbps
接続数/秒	14,000/秒	14,000/秒	40,000/秒	40,000/秒
最大接続数 (SPI)	1,000,000	2,000,000	3,000,000	4,000,000
最大接続数 (DPI)	500,000	750,000	1,000,000	1,500,000
最大接続数 (DPI SSL)	18,000	24,000	30,000	37,000
デフォルトの接続 (DPI/DPI SSL)[4]	500,000/12,000	625,000/15,000	750,000/18,000	1,000,000/19,000
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 クライアント数 (最大)	50 (1,000)	500 (3,000)	2,000 (4,000)	2,000 (6,000)
SSL VPN NetExtender クライアント数 (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	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	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 (進行中)	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、USGv6、CsFC			
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 2650**	**NSa 3650**	**NSa 4650**	**NSa 5650**
電源	デュアル、冗長 120W (1 台が付属)		デュアル、冗長 350W (1 台が付属)	
ファン	デュアル、固定		トリプル、取り外し可能	
入力電源	100 ～ 240 VAC、60 ～ 50 Hz			
最大消費電力 (W)	37.2	46.0	93.6	103.6
25ºC での MTBF (時間)	162,231	156,681	154,529	153,243
25ºC での MTBF (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 (16.9 x 12.8 x 1.8 インチ)		43 x 41.5 x 4.5 cm (16.9 x 16.3 x 1.8 インチ)	
重量	5.2 kg (11.5 ポンド)	5.3 kg (11.7 ポンド)	6.9 kg (15.2 ポンド)	6.9 kg (15.2 ポンド)
WEEE 重量	5.5 kg (12.1 ポンド)	5.6 kg (12.3 ポンド)	8.9 kg (19.6 ポンド)	8.9 kg (19.6 ポンド)
出荷時の重量	7.7 kg (17.0 ポンド)	7.8 kg (17.2 ポンド)	11.3 kg (24.9 ポンド)	11.3 kg (24.9 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			
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。IPS 有効の HTTPS トラフィックで測定された DPI SSL のパフォーマンスです。
[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。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] 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 3,000 ずつ増えます。
* 将来用。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。

法令遵守モデル番号

NS*a* 2650 - 1RK38-0C8
NS*a* 3650 - 1RK38-0C7
NS*a* 4650 - 1RK39-0C9
NS*a* 5650 - 1RK39-0CA

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.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

© 2018 SonicWall Inc. ALL RIGHTS RESERVED. SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.
Datasheet-NetworkSecurityAppliance-US-KJ-MKTG1745

SONICWALL®