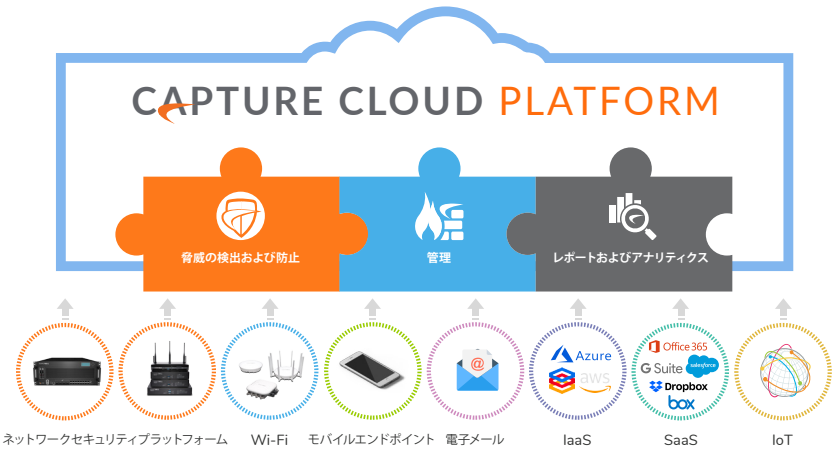
SONICWALL

SonicWallネットワークセキュリティ・バーチャル (NSv) ファイアウォールシリーズ

パブリック、プライベートまたはハイブリッドクラウド環境向けの次世代セキュリティ

仮想化やクラウドなど、最新のネットワークアーキテクチャを設計、実装、導入することは、多くの組織にとって、これからも革新的な戦略の1つであり続けるでしょう。データセンターの仮想化、クラウドへの移行、あるいはその両方を実施すれば、運用上でも経済上でも著しいメリットがあるということが実証されています。しかし、仮想環境における脆弱性については多くの報告があります。セキュリティへ影響や課題をもたらすものが、新たに見つかりつつあります。アプリケーションサービスを安全に、効率よく、拡張可能な方法で提供すると同時に、仮想マシン (VM)、アプリケーションのワークロード、データを含む、仮想フレームワークの全部分において害を成してくる脅威に対抗することを最優先事項に加えておかなければなりません。

SonicWallネットワークセキュリティ・バーチャル (NSv) ファイアウォールシリーズは、業務上重要なサービスや活動に深刻な影響を与えるセキュリティ上のリスクや脆弱性を抑制することにより、セキュリティチームを支援します。NSv次世代ファイアウォールは、2つの高度なセキュリティテクノロジーを統合して脅威に対する最先端の抑止環境を実現し、ネットワークを一歩先に進めます。SonicWallが特許出願中のReal-Time Deep Memory Inspection (RTDMI™) 技術により、数々の賞を受賞したマルチエンジンのサンドボックスであるCapture Advanced Threat Protection (ATP) サービスが強化されています。このRTDMIエンジンは、メモリ内部を直接検査し、マスマーケット、ゼロデイの脅威、未知のマルウェアを先取りして検出してブロックします。リアルタイムアーキテクチャにより、SonicWall RTDMIテクノロジーは、その高い精度で誤検出を最小限に抑えながら、100ナノ秒以内で生じる武器化したマルウェアによる高度な攻撃を特定して軽減します。これを組み合わせることにより、当社特許取得済み*Reassembly-Free Deep Packet Inspection (RFDPI®) 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直接検証し、全パケット、全バイトに至るまで検査を行います。



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

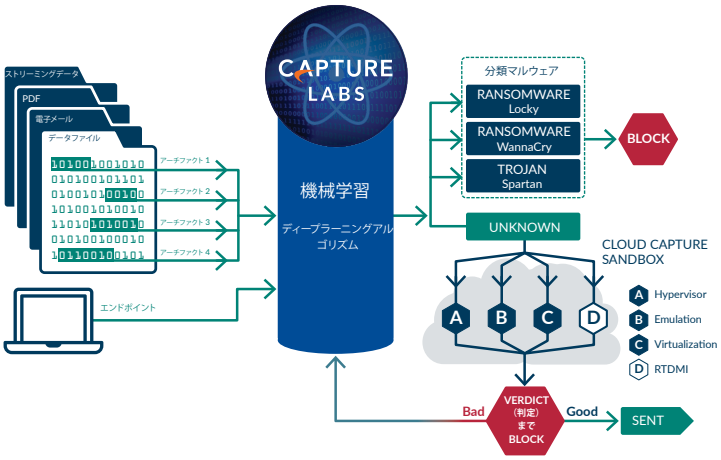
導入効果

パブリックおよびプライベートのクラウドアプリケーション

- 自動化リアルタイムの侵入検知および防止機能をもつ次世代ファイアウォール
- 特許出願中のReal-Time Deep Memory Inspection (RTDMI) 技術
- 特許取得済み、Reassembly-Free Deep Packet Inspection (RFDPI) 技術
- エンドツーエンドの包括的な可視性と制御
- アプリケーションのインテリジェンスと制御
- セグメンテーション・セキュリティとセキュリティ・ゾーニング
- プライベートクラウド (ESXi、Hyper-V) およびパブリッククラウド (AWS、Azure) プラットフォームにわたるサポート
- BYOLおよびPAYGのライセンスモデル

仮想マシンの保護

- Capture ATPによるゼロデイ脅威の保護
- データの機密性
- データ漏洩防止による安全な通信
- トラフィックの検証、インスペクションおよびモニタリング
- システムの安全性と完全性
- 仮想ネットワークの回復性と可用性



NSv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適用しており、組織が必要とする自動化リアルタイム方式の侵入に対する検知および防御機能を提供します。このプラットフォームでは、クラウドベースの脅威防止やネットワーク管理に加え、組織規模を問わずレポート作成と分析を行うことが可能です。さらに、このプラットフォームには、Capture ATPなどの複数ソースから収集された脅威インテリジェンスのほか、世界各地に配置されている100万以上のSonicWallセンサーが統合されています。NSvシリーズは、侵入防止、マルウェア対策、Web/URLフィルタリングなどの機能に加え、このSonicWall Capture Cloud Platformの適用により、ゲートウェイで最も人目を盗む脅威であっても確実にブロックします。

NSvは、簡単に導入しプロビジョニングすることができ、通常は仮想ネットワーク (VN) または仮想プライベートクラウド (VPC) 間に置かれます。これによって、自動化された侵害防止のために仮想マシン間の通信やデータ交換をキャプチャ可能となり、さらに、データの機密性およびVMの安全性・完全性に向けた、厳格なアクセス制御方式が確立できます。セキュリティへの脅威 (たとえば、仮想マシン間攻撃、サイドチャネル攻撃、ネットワーク関連の侵入行為全般、アプリケーションとプロトコルの脆弱性など) に対しては、SonicWallが有するセキュリティ検査サービス[1]の包括的なパッケージにより、無効化を達成できます。すべてのVMトラフィックが脅威分析エンジンの対象であり、このエンジンに含まれるものとしては、侵入防止、ゲートウェイアンチウィルス/アンチスパイウェア、クラウドアンチウィルス、ボットネットフィルタリング、アプリケーション制御、RTDMI技術マルチエンジンのサンドボックスがあります。

セグメンテーションによるセキュリティ

APT（Advanced Persistent Threat：標的型攻撃）に対して最適な効果を発揮するためには、ネットワークセキュリティのセグメンテーションに、高度な脅威に対する動的かつ強制的な障壁を1つのセットに統合して適用する必要があります。セグメンテーションに基づくセキュリティ機能を用いて、NSvは類似のインターフェイスをグループ化し、グループごとにポリシーを適用できます。それぞれのインターフェイスに対して同じポリシーを記述する必要はありません。VN内にセキュリティポリシーを適用することにより、セグメンテーションでネットワークのリソースを別々のセグメントに分類するよう設定でき、さらに、これらのセグメント間におけるトラフィックを許可、あるいは制限するような設定も可能です。このようにすれば、重要な内部リソースへのアクセスを厳密に制御することができます。

NSvは、ユーザーを識別する資格情報、地域IPによる位置情報、モバイルなエンドポイントのセキュリティ水準といった、動的な基準によるセグメンテーション制限を自動的に実施可能です。NSvはまた、セキュリティを拡大するために、マルチギガビットのネットワークスイッチングを、セキュリティセグメントポリシーおよびその適用に統合することもできます。さらに、ネットワーク全体にわたるスイッチング箇所でトラフィックにセグメントポリシーを適用し、セグメントセキュリティの実施を、世界規模で一元的に管理します。

セグメントによる効果は、セグメント間に実施可能なセキュリティに左右されるため、NSvは侵入防止システム (IPS) を利用して、入ってくるトラフィックと出ていくトラフィックをVLANセグメントでスキャンし、内部ネットワークトラフィックのセキュリティを高めます。Nsvは、各セグメントに向け、多数のインターフェイスに対するフルレンジのセキュリティサービスを、適用可能ポリシーに基づいて実施します。

柔軟な導入ユースケース

高可用性 (HA) 実現に向けたインフラストラクチャによるサポートを利用して、NSvはSDDC (Software Defined Data Center：ソフトウェア定義のデータセンター) に対する拡張性と可用性への要求を満たします。さらに、システムの回復力、サービスの信頼性、規制への準拠を維持します。パブリック/プライベートおよびハイブリッドの、広範囲にわたる導入ユースケースに最適化されたNSvは、サービスレベルの変化に対応し、VM、VMのアプリケーションワークロード、データ資産の可用性と安全性を確保します。これらはすべて、マルチギガビット/秒の速度と低いレイテンシで実現できます。

組織は、物理的なファイアウォールの持つセキュリティ上の恩恵をすべて享受すると同時に、仮想化による運用上および経済上での利益も獲得します。これには、システムの拡張性、運用における俊敏性、プロビジョニングの素早さ、管理の容易性、コストの削減が含まれます。

NSvシリーズは、仮想化・クラウド化された広範囲の導入ユースケースに向けて入念にパッケージ化された、多数の仮想フレーバーで利用できます。NSvシリーズは、脅威防御と暗号化されたトラフィックの検査におけるマルチギガビット級のパフォーマンスを提供します。さらには、容量レベルの増加への対応、仮想ネットワークの安全維持、アプリケーションワークロードとデータ資産の可用性および安全性の確保が可能です。

集中管理

NSvは、SonicWall Global Management System (GMS[2]) またはCapture Security Center[2]よる、集中的な管理のもとに導入されます。これらは、SonicWallによるクラウドセキュリティの管理、監視、レポート、分析を行うオープンかつ拡張可能なプラットフォームであり、「サービスとしてのコスト効率 (cost-effective as-a-service)」という形で提供されます。

Capture Security Centerは、SonicWallによる仮想・物理ファイアウォールのエコシステム全体をより明瞭、正確、迅速に管理するための最良の可視性、俊敏性、容量について、すべて一元的に提供します。

SonicOS 7によるSonicWall統合ポリシーエンジン

SonicWall統合ポリシーエンジンは、NSvシリーズをはじめとするSonicWallのオンプレミスおよび仮想ファイアウォール全体にわたるさまざまなセキュリティポリシーの統合管理システムを実現します。

集中管理

- 包括的なセキュリティ管理、分析レポート作成、およびコンプライアンスといった機能へのアクセスを容易にする単一のパスを確立し、ネットワークセキュリティ防御プログラムを統合
- ワークフローを自動化および相関させ、セキュリティガバナンス、コンプライアンス、およびリスク管理について完全にコーディネートされた戦略を形成

コンプライアンス

- PCI、HIPAA、SOXのセキュリティレポート自動化により、規制機関や監査人が恩恵を享受
- 監査可能なセキュリティデータのあらゆる組み合わせをカスタマイズ、特定のコンプライアンス規制への準拠を支援

リスク管理

- 共有セキュリティフレームワーク全体でのコラボレーション、コミュニケーション、情報共有を迅速に推進
- タイムクリティカルかつ統合された脅威情報に基づいてセキュリティポリシーを決定し、より高度なセキュリティ効率を実現

GMSにより、セキュリティガバナンス、コンプライアンス、およびリスク管理に対する総合的なアプローチが可能です。

このエンジンには、根本的に異なるアプローチをサポートする新しいウェブインターフェースが搭載されています。

エンジンでは、アクション可能なアラートとポイント・アンド・クリック方式によるシンプルな操作性により、コンテキストに応じたセキュリティ・ポリシーを直感的に設定できます。

見た目も従来よりも魅力的なものになっています。ファイアウォールの単一ペインビューでは、インターフェイスにて各種のセキュリティルールの有効性に関する情報を確認できます。

さらに、ゲートウェイアンチウィルス、アンチスパイウェア、コンテンツフィルタリング、侵入防止、geo-IPフィルタリング、および暗号化トラフィックのディープパケットインスペクションに関する定義済みルールをシームレスに変更できます。

この統合ポリシーエンジンは、さらに合理化されたエクスペリエンス環境を実現します。これにより、設定エラーの削減、展開時間の短縮、全体的なセキュリティ体制の改善を図ります。

フレキシブルライセンス

NSvは、Bring Your Own License (BYOL) およびPay As You Go (PAYG) ライセンスをサポートします。NSvのBYOLライセンスは、日本ではSonicWallのパートナーまたはリセーラから購入できます。PAYGライセンスは、AWS Marketplaceから直接購入できます。このライセンスタイプは使用量ベースのライセンスであり、使用量に応じて時間単位または年単位で支払いが行われます。

機能

SonicOSプラットフォーム

SonicOSのアーキテクチャは、NSvおよびNsaシリーズ、SuperMassiveシリーズ、TZシリーズを含めた、SonicWallによる仮想・物理ファイアウォールの中核を成します。その機能や特色の詳細なリストについては、SonicWallSonicOSプラットフォームのデータシートをご覧ください。

自動化された侵害防止[1]

NSvは、SonicWallのRTDMI技術により、ハイパフォーマンスな侵入およびマルウェアの防止、クラウドベースのサンドボックスなど、高度な脅威から全面的に保護します。

24時間体制のセキュリティ[1]

NSvは、横移動（組織内部）の保護に加えて、送受信トラフィックの保護も確実にこなします。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。リブートや中断は不要です。

ゼロデイ防御[1]

NSvは、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保護してくれます。

脅威API

NSvは、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、高度な脅威に対抗します。

境界防御

NSvは、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ことを阻止することで、内部セキュリティを強化します。種々のインターフェイスを通過するトラフィックに向けて、アクセスルールおよびNATポリシーを作成、適用することで、NSvはさまざまな基準の下に内外からのネットワークアクセスを許可/拒否することができます。

アプリケーションインテリジェンスおよび制御[1]

NSvは、アプリケーションに固有なポリシーを用いて、NSvはユーザー、Eメールアドレス、スケジュール、IPサブネットに基づいたネットワークトラフィックへの精細な制御を可能にします。さらに、特定のパラメータやネットワークにおけるアプリケーション固有の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コントロールします。内部または外部からのネットワークアクセスは、さまざまな基準の下に許可/拒否されます。

データ漏洩の防止

NSvは、データのストリームをスキャンして、キーワードについて調べる機能を提供します。この機能により、特定のファイル名、ファイル形式、Eメール添付ファイル、添付ファイル形式、特定タイトルのEメール、特定のキーワードもしくはバイトパターンを含むEメールおよび添付ファイルなどの転送が制限されます。

アプリケーション層の帯域幅管理

NSvはパケット監視を用いて、さまざまな候補から帯域幅管理設定を選択し、アプリケーションによるネットワーク帯域幅の使用量を削減することができます。これは、ネットワークに対する制御を強めるために役立ちます。

[1] *SonicWall Advanced Gateway Security Services (AGSS) への登録が必要です。*
[2] *SonicWall Global Management SystemおよびCapture Security Centerには、別途にライセンスまたはサブスクリプションが必要です。*

安全な通信

NSvは、仮想マシンのグループ間におけるデータ交換が安全に実行される状態を維持するため、分離（アイソレーション）、機密性、完全性、セグメンテーションの利用によるネットワーク内の情報フロー制御を有しています。

アクセス制御

NSvは、指定の条件セットを満たすVMに対してのみ、VLANを介して他のVMに属するデータにアクセス可能になるよう確認を行います。

ユーザー認証

NSvは、認証を受けていないユーザーによるVMおよびワークロードへのアクセスを制御、または制限するポリシーを作成します。

データの機密性

NSvは、保護されたデータおよびサービスへの不正なアクセスと、情報の盗難をブロックします。

仮想ネットワークの回復性と可用性

NSvは、アプリケーションサービスと通信の中断と劣化を防止します。

システムの安全性と完全性

NSvはVMシステムとサービスの不正な乗っ取りを阻止します。

トラフィックを検証、検査、監視するメカニズム

NSvは不正行為や悪意のある振る舞いを検出し、VMのワークロードを狙った攻撃を阻止します。

導入オプション

NSvは、仮想化・クラウド化された多様なプラットフォーム上に、さまざまなプライベート/パブリッククラウドセキュリティのユースケースに向けて導入することができます。

フレキシブルライセンスモデル

SonicWallでは、永久および非永久ライセンスモデルを提供します。永久ライセンスは、従来の運用モデルであり、ファイアウォールとセキュリティサービスのライセンスを別途購入する必要があります。このため、これらのライセンスでは個別に期限切れが生じます。非永久ライセンスは、独自の提供品であり、ファイアウォールとセキュリティ・サービスのライセンスがバンドルされ、同時に期限切れになります。パブリッククラウド導入の場合には、永久ライセンスと非永久ライセンスの両方とも、Bring Your Own License (BYOL) モデルとして利用できます。

SonicWallの非永久すなわちサブスクリプションライセンスモデルには、1つのSKUにファイアウォールソフトウェアとセキュリティサービスがバンドルされており、柔軟性と簡便性を備えています。これは、プライベートクラウド（ESXiおよびHyper-V）とパブリッククラウド（AWS、Azure）の両方で利用可能です。サービス期限切れになる前の時点で、サービス期限切れ通知が送信されます。

非永久ライセンスモデルには、IPS/App Control Subscription、TotalSecure Subscription、TotalSecure Advanced Subscriptionの3タイプがあり、1年間有効です。NSvソフトウェアは、提供のタイプに依り、侵入防止システム (IPS)、アプリケーション制御、サポート、キャプチャセキュリティセンター (CSC)、包括型ゲートウェイセキュリティスイート (CGSS)、またはアドバンストゲートウェイセキュリティスイート (AGSS) の組み合わせでバンドルされています。

NSvシリーズのシステム仕様

ファイアウォール全般	NSv 10	NSv 25	NSv 50	NSv 100
オペレーティングシステム	SonicOS[1]			
サポートされるハイパーバイザ	VMware ESXi v5.5/v6.0/v6.5/v6.7、Microsoft Hyper-V Win 2012/2016、KVM Ubuntu 16.04/CentOS 7			
サポートされるパブリッククラウドプラットフォーム（インスタンスタイプ）	AWS (c5.large)、Azure (Std D2 v2)			
ライセンス	BYOL、PAYG[2]			
サポートされる最大vCPU	2	2	2	2
インターフェース数 (ESXi/Hyper-V/KVM)	8/8/8	8/8/8	8/8/8	8/8/8
管理プレーン/データプレーンの最大コア数	1/1	1/1	1/1	1/1
必要最低メモリ[3]	4 GB	4 GB	4 GB	4 GB
最大メモリ[4]	6 GB	6 GB	6 GB	6 GB
サポートされるIP数/ノード	10	25	50	100
必要最低ストレージ	60 GB			
SSOユーザー数	25	50	100	100
ロギング	Analytics、ローカルログ、Syslog			
高可用性	アクティブ/パッシブ			
ファイアウォール/VPNパーフォーマンス[6]	**NSv 10**	**NSv 25**	**NSv 50**	**NSv 100**
ファイアウォールインスペクションスループット	2 Gbps	2.5 Gbps	3 Gbps	3.5 Gbps
フルDPIスループット (GAV/GAS/IPS)	450 Mbps	550 Mbps	650 Mbps	750 Mbps
アプリケーションインスペクションスループット	1 Gbps	1.25 Gbps	1.5 Gbps	1.75 Gbps
IPSスループット	1 Gbps	1.25 Gbps	1.5 Gbps	1.75 Gbps
アンチマルウェアインスペクションスループット	450 Mbps	550 Mbps	650 Mbps	750 Mbps
IMIXスループット	750 Mbps	850 Mbps	950 Mbps	1100 Mbps
TLS/SSL DPIスループット	650 Mbps	750 Mbps	850 Mbps	950 Mbps
VPNスループット	500 Mbps	550 Mbps	600 Mbps	650 Mbps
1秒あたりの接続数	1,800	5,000	8,000	10,000
最大接続数 (SPI)	2,500	6,250	12,500	25,000
最大接続数 (DPI)	2,500	6,250	12,500	25,000
TLS/SSL DPI接続数	500	1,000	2,000	4,000
VPN	**NSv 10**	**NSv 25**	**NSv 50**	**NSv 100**
サイト間VPNトンネル数	10	10	25	50
IPSec VPNクライアント	10(10)	10(10)	10(25)	10(25)
SSL VPNクライアント（付属）[7]	2	2	2	2
SSL VPNクライアント（最大）[7]	50	50	50	50
暗号化/認証	DES、3DES、AES（128、192、256-ビット）/MD5、SHA-1、Suite B、Common Access Card (CAC)			
鍵交換	Diffie Hellmanグループ1、2、5および14v			
ルートベースのVPN	RIP、OSPF、BGP			
ネットワーク機能	**NSv 10**	**NSv 25**	**NSv 50**	**NSv 100**
IPアドレス割り当て	静的、DHCP、内部DHCPサーバ、DHCPリレー			
NATモード	1対1、多対1、1対多、フレキシブルNAT（複IP）、PAT			
最大VLAN	25	25	50	50
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	XAUTH/RADIUS、Active Directory、SSO、LDAP、Novell、内部ユーザデータベース、Terminal Services、Citrix			
VoIP	SIP			
規格	TCP/IP、ICMP、HTTP、HTTPS、IPSec、ISAKMP/IKE、SNMP、DHCP、L2TP、PPTP、RADIUS			
最大SD-WANグループ数	12	12	18	32
製品あたりの最大SD-WANメンバー数	24	24	36	64

NSvシリーズのシステム仕様（続き）

ファイアウォール全般	NSv 200	NSv 300	NSv 400	NSv 800	NSv 1600
オペレーティングシステム	SonicOS[1]				
サポートされるハイパーバイザ	VMware ESXi v5.5/v6.0/v6.5/v6.7、Microsoft Hyper-V、KVM Ubuntu 16.04/CentOS 7				
サポートされるパブリッククラウドプラットフォーム（インスタンスタイプ）	AWS (c5.large)、Azure (Std D2 v2)	該当なし	AWS (c5.xlarge)、Azure (Std D3 v2)	AWS (c5.2xlarge)、Azure (Std D4 v2)	AWS (c5.4xlarge)、Azure (Std D5 v2)
ライセンス	BYOL、PAYG[2]				
サポートされる最大vCPU	2	3	4	8	16
インターフェース数 (ESXi/Hyper-V/KVM/AWS/Azure)	8/8/8/2/2	8/8/8/-/-	8/8/8/4/4	8/8/8/8/8	8/8/8/8/8
管理プレーン/データプレーンの最大コア数	1/1	1/2	1/3	1/7	1/15
必要最低メモリ[3]	6 GB	6 GB	8 GB	10 GB	12 GB
最大メモリ[4]	6 GB	8 GB	10 GB	14 GB	18 GB
サポートされるIP数/ノード	無制限	無制限	無制限	無制限	無制限
必要最低ストレージ	60 GB				
SSOユーザー数	500	5,000	10,000	15,000	20,000
ロギング	アナライザー、ローカルログ、Syslog				
高可用性	アクティブ/パッシブ[5]				
ファイアウォール/VPNパーフォーマンス[6]	**NSv 200**	**NSv 300**	**NSv 400**	**NSv 800**	**NSv 1600**
ファイアウォールインスペクションスループット	4.1 Gbps	5.9 Gbps	7.8 Gbps	13.9 Gbps	17.2 GBPS
フルDPIスループット (GAV/GAS/IPS)	900 Mbps	1.6 Gbps	2.2 Gbps	4.0 Gbps	6.4 Gbps
アプリケーションインスペクションスループット	2.3 Gbps	3.4 Gbps	4.1 Gbps	5.5 Gbps	6.4 Gbps
IPSスループット	2.3 Gbps	3.4 Gbps	4.1 Gbps	5.5 Gbps	6.7 GBPS
アンチマルウェアインスペクションスループット	900 Mbps	1.6 Gbps	2.2 Gbps	4.0 Gbps	6.6 Gbps
IMIXスループット	1.5 Gbps	2.3 Gbps	2.8 Gbps	4.2 Gbps	5.3 Gbps
TLS/SSL DPIスループット	1.1 Gbps	1.2 Gbps	1.8 Gbps	3.4 Gbps	5.1 GBPS
VPNスループット	750 Mbps	1.4 Gbps	1.9 Gbps	4.2 Gbps	8.4 Gbps
1秒あたりの接続数	13,760	24,360	37,270	75,640	125,000
最大接続数 (SPI)	225,000	1M	1.5M	3M	4M
最大接続数 (DPI)	125,000	500,000	1.5M	2M	2.5M
TLS/SSL DPI接続数	8,000	12,000	20,000	30,000	50,000
VPN	**NSv 200**	**NSv 300**	**NSv 400**	**NSv 800**	**NSv 1600**
サイト間VPNトンネル数	75	100	6000	10,000	25,000
IPSec VPNクライアント（最大）	50(1000)	50(1000)	2000(4000)	2000(6000)	2000(10,000)
SSL VPNクライアント（付属）[7]	2	2	2	2	2
SSL VPNクライアント（最大）[7]	100	150	200	300	400
暗号化/認証	DES、3DES、AES（128、192、256-ビット）/MD5、SHA-1、Suite B、Common Access Card (CAC)				
鍵交換	Diffie Hellmanグループ1、2、5および14v				
ルートベースのVPN	RIP、OSPF、BGP				
ネットワーク機能	**NSv 200**	**NSv 300**	**NSv 400**	**NSv 800**	**NSv 1600**
IPアドレス割り当て	静的、DHCP、内部DHCPサーバ、DHCPリレー				
NATモード	1対1、多対1、1対多、フレキシブルNAT（複IP）、PAT				
最大VLAN[8]	128	128	128	128	128
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	XAUTH/RADIUS、Active Directory、SSO、LDAP、Novell、内部ユーザデータベース、Terminal Services、Citrix				
VoIP	SIP				
規格	TCP/IP、ICMP、HTTP、HTTPS、IPSec、ISAKMP/IKE、SNMP、DHCP、L2TP、PPTP、RADIUS				
最大SD-WANグループ数	38	38	70	102	102
製品あたりの最大SD-WANメンバー数	76	76	140	204	204

[1]現時点で、SonicOS 6.5.4をサポートしています。
[2]PAYGは現在AWSでのみ利用可能です。
[3]Jumboフレームが無効の場合のメモリ。
[4]Jumboフレームが有効の場合のメモリ。Jumboフレームには追加のメモリが必要です。JumboフレームはAzureとAWSに対応しません。
[5]VMware ESXiプラットフォームとMicrosoft Hyper-Vで利用可能な高可用性およびHAについては、AzureとAWSに対応しません。

[6]パフォーマンス公表値は仕様に準拠しており、実際のパフォーマンスについてはハードウェアやネットワークの状態、ファイアウォール設定とアクティブ化されたサービスによって異なる場合があります。パフォーマンスおよび容量は、基盤となる仮想化インフラストラクチャによっても異なる場合があります。パフォーマンスと容量の要件を満たすために、環境内で追加テストを行うことをお勧めします。パーフォーマンス測定基準は、SonicOSv 6.5.0.2を実行するインテルXeon Wプロセッサー（W-2195 2.3GHz、4.3GHzターボ、24.75 Mキャッシュ）とVMware vSphere 6.5を用いて確認されています。
[7]SSL VPN数の増加分は、SonicOS 6.5.4.4-44v-21-723ファームウェア以降でのみご利用いただけます。
[8]VLANインターフェースは、AzureとAWSに対応しません。
テスト方法：RFC 2544（ファイアウォール用）に基づいた最大パフォーマンス。業界標準のSpirent WebAvalanche HTTPパフォーマンステストおよびIxiaテストツールを用いて測定したフルDPI/Gateway AV/Anti-Spyware/IPSのスループット。テストは、複数のポートペアを介した複数のフローで行われます。VPNスループットは、RFC 2544に準拠した1418バイトのパケットサイズにあるUDPトラフィックを用いて測定されます。上記の仕様および機能については、変更される場合があります。

機能

RFDPIエンジン	
機能	**説明**
Reassembly-Free Deep Packet Inspection (RFDPI)	この特許取得済み独自仕様の高性能インスペクションエンジンは、プロキシやバッファリングなし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、侵入の試みやマルウェアを検出し、ポートに関係なく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	インバウンドトラフィックとアウトバウンドトラフィックの双方向からの脅威を同時にスキャンすることで、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の攻撃用の起動プラットフォームにならないよう、確実に機能します。
ストリームベースのインスペクション	プロキシレスの非バッファリングインスペクション技術は、ファイルとストリームサイズの制限することなく、数百万の同時ネットワークストリームのDPIに対応する超低レイテンシ性能を備えており、一般プロトコルのほか、生TCPストリームに適用できます。
高度な並列処理と拡張性	このRFDPIエンジンの独自設計では、マルチコアアーキテクチャと連携させることで、要求の厳しいネットワークでのトラフィックスパイクに対処するために、高いDPIスループットと新たなセッション確立レートが得られます。
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の識別を同時にスキャンすることにより、DPIレイテンシを大幅に削減し、あらゆる脅威情報が単一のアーキテクチャで関連付けられるようにします。

ファイアウォールとネットワーク	
機能	**説明**
REST API	このファイアウォールは、すべての独自開発されたOEMとサードパーティのインテリジェンスフィードを受信しそれを利用することで、ゼロデイ、悪意のある内部関係者、資格情報の侵害、ランサムウェア、標的型攻撃など、高度な脅威に対抗することができます。
ステートフルパケットインスペクション (SPI)	全てのネットワークトラフィックがインスペクション、分析され、ファイアウォールアクセスポリシーに準拠するようになります。
高可用性[1]	NSvシリーズは、状態同期によるActive/Passive (A/P) に対応します。
DDoS/DoS攻撃防御	SYNフラッド保護は、レイヤ3 SYNプロキシとレイヤ2 SYNブラックリスト技術を共用することで、DoS攻撃に対する防御を提供します。さらに、UDP/ICMPフラッド保護と接続レート制限により、DoS/DDoSから保護します。
IPv6サポート	IPv4に代わるInternet Protocolバージョン6 (IPv6) は、まだ初期段階にあります。SonicOSにより、ハードウェアがフィルタリングとワイヤモードの実装をサポートします。
フレキシブルに導入できるオプション	NSvシリーズは、従来のNAT、レイヤ2ブリッジ、ワイヤモードおよびネットワーク・タップ・モードで導入できます。
WANロードバランサー	Round Robin、SpilloverあるいはPercentageメソッドにより、複数のWANインタフェースの負荷分散を行います。
高度なサービス品質 (QoS)	802.1p、DSCPタグ、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。
SIPプロキシサポート	着信コールに対しすべてSIPプロキシによって許可および認証を要求することにより、スパムコールをブロックします。
生体認証	ネットワークアクセスのユーザーIDを安全に認証できるよう、簡単に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に対応します。
オープン認証とソーシャルログイン	ゲストユーザが、Facebook、Twitter、Google+などのソーシャルネットワーキングサービスから資格情報を用いてサインインし、パススルー認証を使用してホストのワイヤレス、LANまたはDMZゾーン経由でインターネットやその他のゲストサービスにアクセスできるようにします。

管理とレポート作成	
機能	**説明**
クラウドベースおよびオンプレミス管理	SonicWallアプライアンスの設定および管理は、SonicWall Capture Security Centerからのクラウド経由、SonicWall Global Management System (GMS) からオンプレミスで行うことができます。
強力な単一デバイス管理	直感的なWebベースのインターフェイスにより、包括的なコマンドラインインターフェイスとSNMPv2/3のサポートに加えて、迅速かつ簡便な設定が可能です。
IPX/NetFlowアプリケーションフローレポート	SonicWall Analyticsなどのツール、またはIPFIXと拡張機能付きNetFlowをサポートするその他のツールを利用し、リアルタイムの履歴モニタリングおよびレポートとして、IPFIXまたはNetFlowプロトコルを介してアプリケーショントラフィック分析および使用状況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**
自動プロビジョニングVPN	SonicWallファイアウォール間の初期サイト間VPNゲートウェイのプロビジョニングを自動化すると同時に、セキュリティと接続を瞬時に自動実行することにより、複雑な分散ファイアウォールの配備を簡素化し、作業をシンプル化して削減します。
サイト間接続用のIPSec VPN	NSvシリーズは、高性能のIPSec VPNにより、他の何千もの大規模サイト、支社または本社のVPNコンセントレータとして機能します。
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容易に管理できるIPSecクライアントを利用することで、さまざまなプラットフォームから電子メール、ファイル、コンピューター、イントラネットサイト、および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を使用する場合は、プライマリVPNとセカンダリVPNを構成することで、すべてのVPNセッションのシームレスで自動のフェールオーバーとフェールバックが可能となります。

[1]高可用性は現在、AWSおよびAzureに対応しません。

SONICWALL®

ルートベースのVPN	VPNリンク上でダイナミックルーティングを実行する機能を用いれば、代替ルートを介してエンドポイント間でトラフィックをシームレスに再ルーティングすることで、一時的なVPNトンネル障害が発生した場合でも継続的なアップタイムが保証されます。

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トラッキング	DPIから得られた広範な情報と組み合わせたAD/LDAP/Citrix1/ターミナルサービス1のSSO統合により、ユーザーの識別およびアクティビティがシームレスに利用可能です。
GeoIP国別トラフィック識別	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および制御します。これにより、既知または疑わしい脅威活動による攻撃を阻止し、ネットワークから発信される疑わしいトラフィックを調査します。IPアドレスに関連付けられた不正な国またはボットネットタグを上書きするためのカスタム国およびボットネットリストを作成できます。誤分類によるIPアドレスの不要なフィルタリングを排除します。
正規表現DPIフィルタリング	正規表現マッチングを介してネットワークを横断するコンテンツを識別・制御することで、データ漏洩を防止します。カスタムの国およびボットネットリストを作成することで、IPアドレスに関連付けられた不正な国またはボットネットタグに上書きします。

不正侵入防止サービス

CAPTURE ADVANCED THREAT PROTECTION (ATP)	
機能	**説明**
マルチエンジンサンドボックス	マルチエンジンサンドボックスプラットフォームは、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レベル分析技術を備えており、疑わしいコードを実行してその動作を分析し、悪意のあるアクティビティに対し包括的に可視化します。
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ーに「明かす」よう仕向けることにより、マスマーケット攻撃およびゼロデイ攻撃の脅威と未知のマルウェアを先を見越して検出し、ブロックします。
Verdict（判定）までブロック	潜在的に悪意のあるファイルのネットワーク侵入を阻止するため、分析用にクラウドに送信されたファイルは、判定が下されるまでゲートウェイに保持されます。
幅広いファイル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のほか、Windows、Android、Mac OS X、マルチブラウザ環境などの複数のオペレーティングシステムなど、各種のファイルタイプを対象に、個別にまたはグループ化して解析します。
シグネチャの迅速展開	ファイルが悪意のあるものとして識別されると、SonicWall Capture ATPサブスクリプション、Gateway Anti-VirusおよびIPSシグネチャデータベース、URL、IP、ドメインレピュテーションデータベースを備えたファイアウォールに、48時間以内にシグネチャが即座に展開されます。
Capture Client	Capture Clientとは、次世代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などの複合エンドポイント保護機能を装備した統合クライアントプラットフォームです。ここでは、階層型保護テクノロジー、包括的なレポート作成、エンドポイント保護の実施が適用されます。

暗号化された脅威の防止	
機能	**説明**
TLS/SSLの解読とインスペクション	プロキシを用いずにTLS/SSLで暗号化されたトラフィックをその場で復号化し、マルウェア、侵入、データ漏洩などを検査します。そして、アプリケーション、URL、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を阻止します。NSvシリーズ全モデルのセキュリティサブスクリプションに含まれています。
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) は、SSHトンネルを通過するデータを復号化しインスペクションすることで、SSHを利用した攻撃を阻止します。

侵入防止	
機能	**説明**
対抗策ベースの保護	緊密に統合された侵入防止システム (IPS) では、シグニチャやその他の対策によってパケットのペイロードをスキャンし、脆弱性や不正利用を検出します。これにより、さまざまな攻撃や脆弱性を阻止します。
シグネチャの自動更新	SonicWall Threat Research Teamは、50以上の攻撃カテゴリを含めたIPS対策の広範なリストを継続的に調査・更新しています。こうした新たな更新は、再起動やサービス中断を行う必要なく、即座に有効になります。
ゾーン内IPS保護	侵入防止機能を用い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ます。
Botnetコマンドおよびコントロール (CnC) 検出およびブロック	ローカルネットワーク上のボットからIPおよびドメインに送信されるコマンドおよび制御トラフィックを識別してブロックします。こうしたトラフィックは、伝播するマルウェアとして識別されるか、既知のCnCポイントとなります。
プロトコルの不正使用/異常	IPSをすり抜けるためにプロトコルを悪用する攻撃を識別し、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ため、ゼロデイ攻撃からも保護してくれます。
回避手法の阻止	広範なストリームの正規化、デコード、その他の手法により、レイヤー2～7の回避手法を利用する脅威が検知をすり抜けてネットワークに侵入することを確実に阻止します。

脅威の防止

機能	説明
Gatewayマルウェア対策	RFDPIエンジンは、全ポートとTCPストリームにわたって無制限の長さ・サイズにあるファイル内に存在するウイルス、トロイの木馬、キーロガー、その他のマルウェアに対して、インバウンド、アウトバウンド、ゾーン内トラフィックをもれなくスキャンします。
Capture Cloudマルウェア保護	SonicWallクラウドサーバには、継続的に更新される数千万の脅威シグネチャに関するデータベースが常駐されており、オンボードのシグネチャのデータベース機能を強化するために利用されます。これにより、RFDPIが脅威を広範囲にカバーできるようになります。
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。リブートや中断は不要です。
双方向生TCPインスペクション	RFDPIエンジンは、任意のポート上の生のTCPストリームを双方向にスキャンすることにより、いくつかの既知のポートを保護することに重点を置いた旧式のセキュリティシステムによる攻撃を防ぐことができます。
広範なプロトコルサポート	生のTCPがデータ送信されないHTTP/S、FTP、SMTP、SMBv1/v2などの一般的なプロトコルを識別します。ペイロードが標準的な既知のポートで実行されていない場合にも、ペイロードをデコードしてマルウェア検査を行います。

アプリケーションのインテリジェンスと制御

機能	説明
アプリケーション制御	数千を超えるアプリケーションシグネチャの継続的に拡大するデータベースに対し、RFDPIエンジンによって識別される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することで、ネットワークセキュリティを強化し、その生産性を高めます。
カスタムアプリケーションID	ネットワークをさらに制御するために、ネットワーク通信内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・カテゴリーに対して使用可能な帯域幅を詳細に割り当て、調整します。一方で、重要でないアプリケーショントラフィックを抑制します。
きめ細かい通信制御	スケジュール、ユーザーグループ、除外リスト、さらにはLDAP/ADターミナルサービス/Citrix統合による完全なSSOユーザー識別による一連のアクションに基づいて、各アプリケーションまたはひとつのアプリケーションの特定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
コンテンツの内部/外部フィルタリング	Content Filtering ServiceおよびContent Filtering Clientにより、受け入れ可能な使用ポリシーを実行し、好ましくない情報または非生産的なイメージを含むHTTP/HTTPS Web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	ファイアウォール境界の外側にある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よう、ポリシー適用範囲を拡張します。
きめ細かいコンテンツ制御	定義済みのカテゴリまたはカテゴリの組み合わせにより、コンテンツをブロックします。フィルタリングは、学校や営業時間などの時間帯ごとにスケジュール化し、個々のユーザーまたはグループに適用できます。
Webキャッシュ	URLレーティングはSonicWallファイアウォールの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その後のアクセスの応答時間は、ほんの一瞬です。

ウイルス対策とスパイウェア対策の強化

機能	説明
多層保護	このファイアウォール機能を境界の最初の防御層として利用することで、エンドポイント保護と組み合わせて、ラップトップ、USBドライブ、その他に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します。
自動強制オプション	ネットワークにアクセスする全コンピューター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、アクティブになります。これにより、デスクトップのウイルス対策管理にかかる一般コストを削減することができます。
導入およびインストールの自動化オプション	コンピューター毎の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導入とインストールをネットワーク全体で自動的に行います。これで、管理オーバーヘッドを最小限に抑えることができます。
次世代のウイルス対策	Capture Clientでは、静的人工知能 (AI) エンジンによって脅威を特定することにより、脅威が実行されて感染する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保護により、機密データの送信前にデスクトップおよびノートパソコン上で一連のスパイウェアプログラムのインストールをスキャンしてブロックします。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を向上させます。

SonicOS機能の概要

グローバルコントロールオーバー

- IPv6の可視性の一元管理
- IPv6トラフィック処理をグローバルに無効化
- デフォルトのVPNポリシー、設定画面、および自動生成規則の無効化

ログインおよびユーザーセキュリティ

- IPアドレス範囲によるログイン試行に基づくユーザーのロックアウト
- CLIからのユーザーのロックアウト
- 初回ログイン時にパスワードの変更を強制する
- Two-Factor認証 (TOTP) のサポート
- ゲストユーザーポリシーのゼロタッチポータルサポート
- ゲストサービスIPv6サポート
- TACACS+アカウンティングのサポート
- 全ユーザーのクォータ制御
- 動的ボットネットHTTP認証

ネットワークとシステム

- SD-WANサポート
- DNSセキュリティ/DNSシンクホールのサポート
- TCP DNS上のFQDN
- NAT用のFQDNアドレスオブジェクト
- DHCPv6リレー
- H.323 VoIPアプリケーション層ゲートウェイのIPv6アドレス指定モード
- マルチコントロールプレーン (CP) コアサポート
- データプレーンオフロードによるHTTP/HTTPSリダイレクション
- データプレーンへのIPヘルパーオフロード
- ローカルストレージ上のファームウェアバックアップビット
- 高可用性サービス
- 高可用性ファームウェアアップロードサポート
- スタティックルートとダイナミックルートのポリシーベースのルーティング最適化
- パフォーマンス/スループットの向上
- ファイアウォール状態を監視するウォッチドッグ機能
- VPN番号付きトンネルインターフェイス上の高度なルーティングの拡張性の向上
- OSS Noklava v10.5.0 ASN.1コンパイラに基づくH.323ライブラリの更新
- タスクスレッドの優先順位の更新
- SSLVPNとデータプレーンのブックマーク

セキュリティサービス

- 判定が出るまでATPブロックを保留
- 非HTTPプロトコルのATP対応ファイル名表示の取得
- 個々のYouTube動画のCFSブロック
- HTTPSコンテンツフィルタリングとDPI-SSLを同時にサポート
- 次世代ウイルス対策 (SentinelOne) およびDPI-SSLの実施
- Wan DDOS保護パフォーマンスの向上

ポリシー/オブジェクト

- アクセスルールの強化
- アプリケーションベースのルーティング
- 動的アドレスオブジェクト
- CFSポリシーの除外
- ポリシーベースのHTTPSコンテンツフィルタオブジェクト
- コンテンツフィルタオブジェクトでのURIリストグループのサポート
- HTTP要求に対するCFSカスタムヘッダーの挿入
- ルールおよびオブジェクトのUUID
- CFSポリシーのUUID
- NATポリシーに対する送信元MACの上書き

DPI-SSL/DPI-SSH

- DPI-SSL動的クラウドベースのホワイトリスト
- SSHポート転送のDPI-SSHブロッキング
- X11転送のDPI-SSHブロッキング
- パケットミラー/パケットキャプチャでのSSL復号化ポートの保存
- ゾーン当りのDPI-SSL詳細制御
- アクセスルールベースのDPI-SSL制御
- DPI-SSLクライアントが期限切れのCA証明書をブロックまたは許可
- TLS証明書ステータス要求拡張
- ローカルCRLのサポート
- 強化されたDPI-SSL証明書の検証
- ECDSA関連暗号のサポート
- OpenSSL LTSリリースの連邦認証サポート

ロギング、監視およびレポート作成

- 特定パケットでのDPI実行を検証する機能
- アプリケーション制御用のファイル名とURIのロギング
- 管理者用に表示されるログオンレコード
- 構成の監査
- TCP接続のNATマッピングのロギング
- ログ自動化のためのFTPサポート
- NSv用Capture Security Center (CSC) レポート作成及び分析サポート
- 電子メールの送信者/受信者のATPロギング取得
- キャプチャ脅威評価クライアントの機能強化 (SWARM v3)
- SFR (SWARM) 統計データのリセット機能
- SonicFlowレポートの出力言語を選択するオプション

API

- SonicOS APIフェーズ1
- SonicOS API認証のサポート
- SonicOS APIフェーズ2
- LHM RESTful API

SonicOS Web管理UI

- SonicOSグローバル検索
- コンテンツ・ページの操作性の向上
- ユーザーごとのクライアント側UI設定ストレージ
- SonicOSのWeb管理画面にフレンドリ名を固定
- リファクタリングされたSonicOS Webインターフェイスレイアウト

NSvシリーズオーダー情報

製品	ESXI SKU	HYPER-V SKU	AZURE SKU	AWS SKU	KVM SKU
SonicWall NSv 10 Virtual Appliance TotalSecure Advanced Edition（1年）	01-SSC-5875	02-SSC-1387	02-SSC-3426	02-SSC-3452	02-SSC-3494
SonicWall NSv 25 Virtual Appliance TotalSecure Advanced Edition（1年）	01-SSC-5923	02-SSC-1395	02-SSC-3454	02-SSC-3464	02-SSC-3497
SonicWall NSv 50 Virtual Appliance TotalSecure Advanced Edition（1年）	01-SSC-5926	02-SSC-1399	02-SSC-3470	02-SSC-3474	02-SSC-3504
SonicWall NSv 100 Virtual Appliance TotalSecure Advanced Edition（1年）	01-SSC-5929	02-SSC-1405	02-SSC-3480	02-SSC-3489	02-SSC-3513
SonicWall NSv 200 Virtual Appliance TotalSecure Advanced Edition（1年）	01-SSC-5950	02-SSC-1412	02-SSC-0868	02-SSC-0906	02-SSC-3519
SonicWall NSv 300 Virtual Appliance TotalSecure Advanced Edition（1年）	01-SSC-5964	02-SSC-1420	—	—	02-SSC-3526
SonicWall NSv 400 Virtual Appliance TotalSecure Advanced Edition（1年）	01-SSC-6084	02-SSC-1427	02-SSC-0888	02-SSC-0912	02-SSC-3531
SonicWall NSv 800 Virtual Appliance TotalSecure Advanced Edition（1年）	01-SSC-6101	02-SSC-1429	02-SSC-0889	02-SSC-0914	02-SSC-3533
SonicWall NSv 1600 Virtual Appliance TotalSecure Advanced Edition（1年）	01-SSC-6109	02-SSC-1436	02-SSC-0895	02-SSC-0921	02-SSC-3540
製品	ESXI SKU	HYPER-V SKU	AZURE SKU	AWS SKU	KVM SKU
SonicWall NSv 10 Virtual Appliance TotalSecure Advanced Edition（3年）	01-SSC-5873	02-SSC-1386	02-SSC-3427	02-SSC-3453	02-SSC-3491
SonicWall NSv 25 Virtual Appliance TotalSecure Advanced Edition（3年）	01-SSC-5890	02-SSC-1397	02-SSC-3457	02-SSC-3465	02-SSC-3498
SonicWall NSv 50 Virtual Appliance TotalSecure Advanced Edition（3年）	01-SSC-5924	02-SSC-1398	02-SSC-3471	02-SSC-3472	02-SSC-3505
SonicWall NSv 100 Virtual Appliance TotalSecure Advanced Edition（3年）	01-SSC-5928	02-SSC-1404	02-SSC-3478	02-SSC-3486	02-SSC-3514
SonicWall NSv 200 Virtual Appliance TotalSecure Advanced Edition（3年）	01-SSC-5951	02-SSC-1411	02-SSC-0866	02-SSC-0903	02-SSC-3515
SonicWall NSv 300 Virtual Appliance TotalSecure Advanced Edition（3年）	01-SSC-5965	02-SSC-1419	—	—	02-SSC-3523
SonicWall NSv 400 Virtual Appliance TotalSecure Advanced Edition（3年）	01-SSC-6089	02-SSC-1426	02-SSC-0887	02-SSC-0911	02-SSC-3527
SonicWall NSv 800 Virtual Appliance TotalSecure Advanced Edition（3年）	01-SSC-6102	02-SSC-1428	02-SSC-0891	02-SSC-0913	02-SSC-3538
SonicWall NSv 1600 Virtual Appliance TotalSecure Advanced Edition（3年）	01-SSC-6108	02-SSC-1435	02-SSC-0897	02-SSC-0920	02-SSC-3542

**SKUの完全リストについては、最寄りのSonicWall代理店までお問い合わせください。*

SonicWallについて

SonicWallは、Boundless Cybersecurityを提供することにより、誰もがリモート/モバイルで危険にさらされながら仕事をするという超分散化時代のビジネス環境に対処します。未知の領域を探求し、リアルタイムの可視性を提供しながら経済的大躍進をも実現しているSonicWallは、サイバーセキュリティ業務上の課題を解決して世界中の大企業や政府、SMBをサポートします。詳しくはwww.sonicwall.comをご覧ください。

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

Datasheet-NSvVirtualFirewalls-US-VG-2088