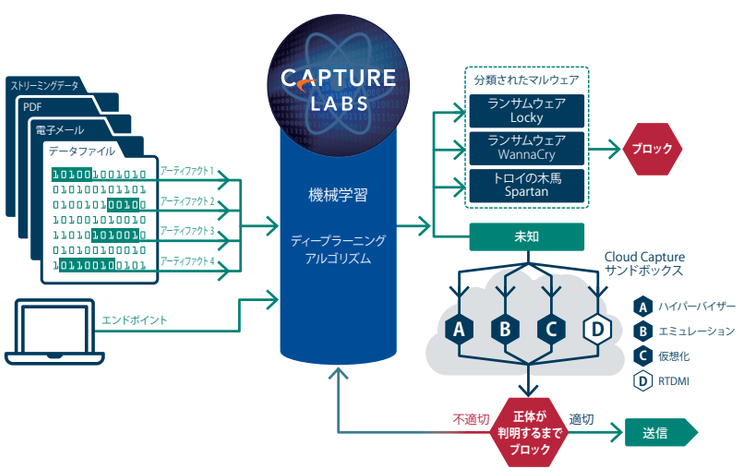
SonicWall Network Security virtual (NSv) シリーズ

プライベート / パブリックおよびハイブリッドのクラウド環境に向けた
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の設計、実装、展開は、多くの組織にとって革新的な戦略になり続けています。データセンターの仮想化、クラウドへの移行、またはその両方の組み合わせは、運用上および経済上の大きな利点を実証しました。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、セキュリティへ影響や課題をもたらす脆弱性が、新しく見つかり続けています。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し、それと同時に、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な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。

セキュリティ上のリスクや脆弱性によって、業務上重要なサービスおよび活動に深刻な混乱がもたらされる可能性があります。SonicWall Network Security virtual (NSv) ファイアウォールは、セキュリティチームがこういったリスクや脆弱性を低減するために役立ちます。SonicWall の物理的なファイアウォールと同等の Reassembly-Free Deep Packet Inspection (RFDPI)、セキュリティ制御、ネットワーキングサービスなど、フル機能のセキュリティツールとサービスにより、NSv はプライベートクラウド環境またはパブリッククラウド環境の重要なコンポーネントすべてを効果的に保護します。

NSv はマルチテナントな仮想環境へ簡単に導入、プロビジョニングでき、通常、仮想ネットワーク (VN) の間に置かれます。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を確立できます。一連の包括的な SonicWall のセキュリティ検査サービス [1] によって、セキュリティ上の脅威 (クロスバーチャルマシンやサイドチャネル攻撃、一般的なネットワークベースの侵入、アプリケーションやプロトコルの脆弱性など) が正常に無効化されます。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イルス / アンチスパイウェア、クラウドアンチウイルス、ボットネットフィルタリング、アプリケーション制御、マルチエンジンのサンドボックスである Capture Advanced Threat Protection があります。



メリット：

パブリックおよびプライベートのクラウドセキュリティ

- パフォーマンスに影響を与えずに、クラウドの俊敏性、スケーラビリティ、セキュリティと組み合わされた次世代のファイアウォール機能を実現
- 自動化されたリアルタイム脅威防止のための仮想インフラストラクチャを完全に可視化および制御
- セキュリティポリシーの適切な配置を確保
- VM の場所を問わず、安全なアプリケーション実行ルールをアプリケーション、ユーザー、デバイスごとに提供
- 適切なセキュリティゾーニングとアイソレーションでマルチテナントやマイクロセグメンテーションを活用
- プライベートクラウドプラットフォーム (ESXi、Hyper-V[3]) およびパブリッククラウドプラットフォーム (AWS[3]、Azure) 全体にわたるプラットフォームサポート
- 柔軟なライセンスモデル

仮想マシンの保護

- Capture Advanced Threat Protection (ATP) による、ゼロデイ脆弱性からの防御
- 仮想システムに対する不正な乗っ取りを防止
- 保護されたデータ資産への不正なアクセスを阻止
- マルウェアの拡散、OS のコマンド実行、ファイルシステムのブラウジング、C&C 通信など、悪意ある活動および侵入行為をブロック
- 仮想エコシステムの全体もしくは一部におけるサービス中断を防止

セグメンテーションによるセキュリティ

APT (Advanced Persistent Threat: 持続的標的型脅威) に対する有効性を最適にするため、ネットワークセキュリティのセグメンテーションでは、高度な脅威に対し動的で強制可能な複数の防壁をまとめて適用する必要があります。NSv は、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、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できます。

NSv は、ユーザーを識別する資格情報、Geo-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。Nsv は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、全体的、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 は侵入防止サービス (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、実施ポリシーに基づいて実施します。

柔軟な導入、使用

高可用性 (HA) 実装のインフラストラクチャサポートにより、Nsv はソフトウェア定義データセンター (SDDC) のスケーラビリティと可用性要件を満たします。NSv はシステムの回復力、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、ハイブリッドの幅広い導入、利用に最適化された Nsv は、サービスレベルの変更に対応し、VM とそのアプリケーションのワークロードとデータ資産を利用できるようにし、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されます。

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利用状況に向けて入念にパッケージ化された、多数の仮想的特徴で利用できます。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。そのため、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、宅内設置の SonicWall GMS[2] およびコスト効率の良いクラウドサービス SonicWall Capture Security Center[2] による、集中的な管理のもとに導入されます。SonicWall Capture Security Center は、オープンかつ拡張可能なクラウドセキュリティ運用監視、レポートと分析のソフトウェアです。

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、容量を、すべて一元的に提供します。

特徴

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、SonicWall SonicOS 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]

これには、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、高度な脅威からの全面的な保護が含まれます。

24 時間体制のセキュリティ [1]

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。

パートナー提供サービス

SonicWall ソリューションを計画、導入、最適化するサポートが必要ですか。SonicWall Advanced Services Partner は、世界規模のプロフェッショナルサービスを提供するように訓練されています。詳細については、www.sonicwall.com/PES をご覧ください。

ゼロデイ防御 [1]

Nsv は何千種類にも及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の、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のを阻止することで、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]

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提供します。NSv は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。

集中管理

- 包括的なセキュリティ管理、分析レポート、コンプライアンスの容易な方法を確立し、ネットワークセキュリティの防衛計画を統合
- ワークフローの自動化と関連付けを行って、十分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、リスク管理の戦略を構築

コンプライアンス

- PCI、HIPAA、SOX のセキュリティレポートの自動化により、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することで、特定のコンプライアンス規制の準拠を推進

リスク管理

- 迅速に行動し、共有セキュリティフレームワーク全体にわたってコラボレーション、コミュニケーション、知識伝達を促進
- 脅威についての、タイムリーかつ統合された情報に基づいて、セキュリティポリシーを決定し、セキュリティの効率性を向上

GMS は、セキュリティガバナンス、コンプライアンス、およびリスク管理への総体的アプローチを提供します。

データ漏洩防止

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。これにより、特定のファイル名、ファイルタイプ、E メールの添付ファイル、添付ファイルの種類、特定の件名の E メール、特定のキーワードまたはバイトパターンの E メールまたは添付ファイル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できます。これは、ネットワークに対する制御を強めるのに役立ちます。

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、既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 が持つデータにアクセス可能であるという認証を与えます。

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。

[1] SonicWall Advanced Gateway Security Services (AGSS) のサブスクリプションが必要です。
[2] SonicWall Global Management System および Capture Security Center には個別のライセンスまたはサブスクリプションが必要です。
[3] Hyper-V および AWS Marketplace の提供待ち

SONICWALL®

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ー	VMware ESXi v5.5 / v6.0 / v6.5、Microsoft Hyper-V			
ライセンスの種類	無期限、期限付き	無期限	無期限、期限付き	無期限
サポートされる vCPU の最大数	2	2	2	2
インターフェイス数 (ESXi)	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
最小メモリ[2]	4 GB	4 GB	4 GB	4 GB
最大メモリ[3]	6 GB	6 GB	6 GB	6 GB
サポートされる IP 数 / ノード	10	25	50	100
最小ストレージ	60 GB			
SSO ユーザー数	25	50	100	100
ロギング	Analyzer、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 パフォーマンス[5]	**NSv 10**	**NSv 25**	**NSv 50**	**NSv 100**
ファイアウォールインスペクションのスループット	2 Gbps	2.5 Gbps	3 Gbps	3.5 Gbps
フル DPI のスループット (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のスループット	1 Gbps	1.25 Gbps	1.5 Gbps	1.75 Gbps
IPS のスループット	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のスループット	450 Mbps	550 Mbps	650 Mbps	750 Mbps
IMIX のスループット	750 Mbps	850 Mbps	950 Mbps	1100 Mbps
TLS/SSL DPI の スループット	650 Mbps	750 Mbps	850 Mbps	950 Mbps
VPN のスループット	500 Mbps	550 Mbps	600 Mbps	650 Mbps
接続数 / 秒	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	25	25
SSL VPN NetExtender クライアント数 (最大)	2 (10)	2 (25)	2 (25)	2 (25)
暗号化 / 認証	DES、3DES、AES (128、192、256 ビット)/MD5、SHA-1、Suite B、Common Access Card (CAC)			
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	**NSv 10**	**NSv 25**	**NSv 50**	**NSv 100**
IP アドレスの割り当て	静的、DHCP、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			
VLAN インターフェイス	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、内部ユーザーデータベース、Terminal Services、Citrix			
VoIP	SIP			
標準	TCP/IP、ICMP、HTTP、HTTPS、IPSec、ISAKMP/IKE、SNMP、DHCP、L2TP、PPTP、RADIUS			

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ー	VMware ESXi v5.5 / v6.0 / v6.5、Microsoft Hyper-V				
ライセンスの種類	無期限、有期	無期限	無期限、有期	無期限、有期	無期限
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)	N/A	AWS (c5.xlarge)、Azure (Std D3 v2)	AWS (c5.2xlarge)、Azure (Std D4 v2)	AWS (c5.4xlarge)、Azure (Std D5 v2)
サポートされる vCPU の最大数	2	3	4	8	16
インターフェイス数 (ESXi/AWS/Azure)	8/3/2	8/-/-	8/4/4	8/4/8	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
最小メモリ[2]	4 GB	6 GB	8 GB	10 GB	12 GB
最大メモリ[3]	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
最小ストレージ	60 GB				
SSO ユーザー数	500	5,000	10,000	15,000	20,000
ロギング	Analyzer、ローカルログ、Syslog				
高可用性	アクティブ / パッシブ[4]				
ファイアウォール /VPN パフォーマンス[5]	**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のスループット	4.1 Gbps	5.9 Gbps	7.8 Gbps	13.9 Gbps	17.2 Gbps
フル DPI のスループット (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のスループット	2.3 Gbps	3.4 Gbps	4.1 Gbps	5.5 Gbps	6.4 Gbps
IPS のスループット	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のスループット	900 Mbps	1.6 Gbps	2.2 Gbps	4.0 Gbps	6.6 Gbps
IMIX のスループット	1.5 Gbps	2.3 Gbps	2.8 Gbps	4.2 Gbps	5.3 Gbps
TLS/SSL DPI のスループット	1.1 Gbps	1.2 Gbps	1.8 Gbps	3.4 Gbps	5.1 Gbps
VPN のスループット	750 Mbps	1.4 Gbps	1.9 Gbps	4.2 Gbps	8.4 Gbps
接続数 / 秒	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 クライアント数 (最大)	50 (1,000)	50 (1,000)	2,000 (4,000)	2,000 (6,000)	2,000 (10,000)
SSL VPN NetExtender クライアント数 (最大)	2 (100)	2 (100)	2 (100)	2 (100)	2 (100)
暗号化 / 認証	DES、3DES、AES (128、192、256 ビット)/MD5、SHA-1、Suite B、Common Access Card (CAC)				
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	**NSv 200**	**NSv 300**	**NSv 400**	**NSv 800**	**NSv 1600**
IP アドレスの割り当て	静的、DHCP、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				
VLAN インターフェイス	50	256	500	512	512
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、内部ユーザーデータベース、Terminal Services、Citrix				
VoIP	SIP				
標準	TCP/IP、ICMP、HTTP、HTTPS、IPSec、ISAKMP/IKE、SNMP、DHCP、L2TP、PPTP、RADIUS				

[1] 現在 SonicOS 6.5.0 をサポート。2018 年末から SonicOS 6.5.2 をサポート。
[2] ジャンボフレーム付きメモリ使用不可。
[3] ジャンボフレーム付きメモリ使用可能。ジャンボフレームを使用する場合、追加のメモリが必要です。
[4] VMware ESXi プラットフォームおよび Microsoft Hyper-V で利用可能な高可用性。
[5] 公開されたパフォーマンス数値は規定条件によるものであり、実際のパフォーマンスは基となるハードウェア、ネットワーク条件、ファイアウォールの設定、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。パフォーマンスと容量も、基をなす仮想化インフラストラクチャによっては変わる場合があり、パフォーマンスと容量の要件が満たされるよう、お客様の環境内で追加のテストを行うことをお勧めします。パフォーマンス値は、VMware vSphere 6.5 で SonicOSv6.5.0.2 を実行する Intel Xeon W Processor (W-2195 2.3GHz、4.3GHz Turbo、24.75M Cache) を使用して測定されました。
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。
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。
VPN のスループットは、RFC 2544 準拠のパケットサイズ (1418 バイト) の UDP トラフィックを使用して測定しています。すべての仕様および機能は、変更されることがあります。

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	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、持続的標的型脅威などの、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 [1]	NSv シリーズは、状態同期によるアクティブ / パッシブ (A/P) をサポートします。
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	NSv 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。
SIP プロキシサポート	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。
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、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
クラウドベースおよびオンプレミスの管理	SonicWall アプライアンスの構成および管理は、SonicWall Capture Security Center を使用してクラウド経由で、および SonicWall Global Management System (GMS) を使用して宅内で行うことができます。
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、NSv 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、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。

[1] AWS と Azure では、現在高可用性はサポートされていません

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 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独自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、個別にまたはグループとして分析します。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。すべての NSv シリーズ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アンドコントロール (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	何千種類にも及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。リブートや中断は不要です。
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 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、数千に及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することにより制御することで、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やアプリケーションカテゴリに帯域幅を割り当てたり、重要度の低いアプリケーションのトラフィックを規制したりして、アプリケーションの帯域幅をきめ細かく調整します。
詳細な制御	LDAP/AD/Terminal Services/Citrix 統合を利用した SSO ユーザーの完全な識別により、スケジュール、ユーザーグループ、除外リスト、さまざまなアクションに応じて、アプリケーションやアプリケーションの特定コンポーネントをコントロールします。

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およびコンテンツフィルタリングクライアントを利用して、使用許諾ポリシーを適用し、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 HTTP/HTTPS Web サイトへのアクセスをブロックします。
コンテンツフィルタリングクライアント強制	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。

ライセンス	
機能	説明
Bring Your Own License (BYOL、持込ライセンス) 無期限	NSv は、BYOL の無期限ライセンスとして 1/3/5 年利用可能です。ファイアウォールライセンスには有効期限がありませんが、セキュリティサービスライセンスには有効期限があります。
Bring Your Own License (BYOL、持込ライセンス) 期限付き	NSv は、BYOL の有期ライセンスとして 12 か月利用可能です。ファイアウォールとセキュリティサービスは単一の SKU として利用でき、同時に失効します。

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
- 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
- ゾーンまたはルールごとの詳細な DPI 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 / 帯域幅 / 脅威の使用状況
- 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
- プロキシ回避
- 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 [2]
- RSTP (Rapid Spanning Tree Protocol)
- 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)
- 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
- 状態同期による A/P 高可用性 [3]
- インバウンド / アウトバウンドのロードバランシング
- ワイヤモード [4]
- 非対称ルーティング
- Common Access Card (CAC) のサポート

VoIP

- 詳細な QoS 制御
- 帯域幅管理
- アクセスルールごとの SIP 変換
- SIP プロキシサポート

管理と監視

- Capture Security Center、GMS、Web UI、CLI、REST API、SNMPv2/v3
- ロギング
- Netflow/IPFix エクスポート
- クラウドベースの構成バックアップ

ストレージ

- ログ
- レポート
- ファームウェアバックアップ

[1] サブスクリプションの追加が必要です
[2] AWS/Azure では VLAN インターフェイスはサポートされていません
[3] AWS/Azure では高可用性はサポートされていません
[4] AWS/Azure ではワイヤモードはサポートされていません

SONICWALL

当社について

27 年以上にわたり、SonicWall はサイバー犯罪界と戦い続けてきており、小規模、中規模のビジネスや企業を世界的規模で守り続けています。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 215 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。詳細については、www.sonicwall.com を参照ください。また、Twitter、LinkedIn、Facebook、Instagram で弊社をフォローしてください。

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

Datasheet-NSvVirtualFirewalls-US-VG-MKTG4359

SONICWALL®