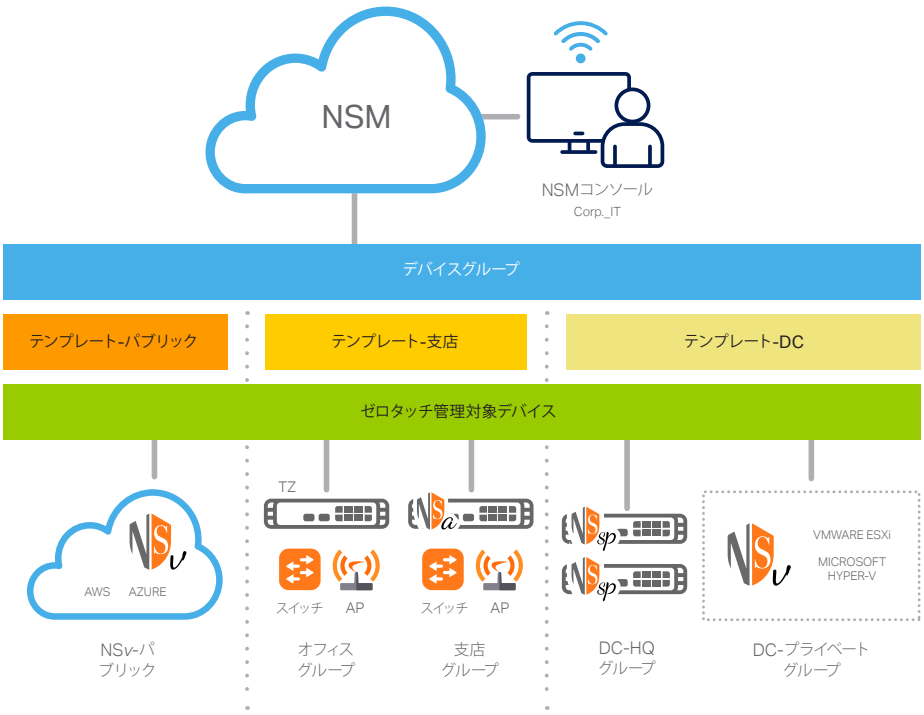
SONICWALL

# Network Security Manager

あらゆる規模の環境に適した統合ファイアウォール管理システム

中小企業や分散型企業、複数の企業など保護対象に関係なく、ネットワークセキュリティは、運用上の障害や目に見えないリスク、規制上の要求に直面する可能性があります。これまでの優れたファイアウォール管理の実践は、堅牢で信頼できるシステムと運用管理手段に依存していました。ですがSecurity Operation Centers（SOC）が適切に運用されていても、一般的なエラーや構成エラー、そしておそらくこうした規制への違反が課題であることに変わりはありません。

マルチテナント集中管理型ファイアウォールマネージャーであるSonicWall Network Security Manager（NSM）は、監査可能なワークフローを遵守することにより、すべてのファイアウォール操作をエラー無しに一元的に管理できます。固有の分析エンジンは、単一画面の可視性を提供し、すべてのファイアウォールログを統合し、関連付けることで脅威の監視と発見を可能にしました。またNSMは、すべての構成変更の完全な監査証跡ときめ細かいレポートを提供し、準拠の維持をサポートします。NSMは、あらゆる規模の組織に迅速かつ容易に適応可能で、少ない手間と時間で、多数のロケーションにわたって展開されている数千ものファイアウォールデバイスを備えたネットワーク管理までも実現します。




**導入効果：**

**ビジネス**

- セキュリティ管理にかかるオーバーヘッドを軽減
- 脅威環境とセキュリティ対策に関する知見
- SaaSによるCAPEXの低減

**運用**

- HW/SWの展開不要
- ファイアウォール管理サイロを排除
- リモートで簡単にいつくものファイアウォールを導入可能
- すべてのセキュリティ操作を可視化

**セキュリティ**

- すべての環境で一貫したセキュリティポリシーを監査、コミット、実施
- 問題やリスクを迅速に捕捉して対処
- 情報に基づくセキュリティポリシーの決定

## 容易な管理：ファイアウォール操作の一元化

NSMは、統合されたファイアウォール管理システムに必要なものをすべて提供します。テナントレベルの可視性、グループベースのデバイス制御、無制限の拡張性により、SonicWallのネットワークセキュリティ操作の一元的な管理とプロビジョニングを実現します。これには、すべてのファイアウォールデバイスやデバイスグループ、テナントの展開と管理、柔軟なローカル制御による環境全体で一貫したセキュリティポリシーの同期と実施、単一の動的ダッシュボードからの包括的な監視と詳細なレポート・分析機能が含まれます。NSMなら、ブラウザ対応デバイスを使ってどこからでもアクセスできる単一のクラウド専用コンソールにより、これらすべての操作を実行することが可能です。

### マルチテナント管理

ファイアウォール環境を複雑なマルチクラウドおよびマルチロケーションテナントで拡張する場合、ネットワークセグメントごとに異なるセキュリティニーズが存在するため、その環境に応じて拡張できるファイアウォール管理システムが必要になります。NSMは、すべての管理対象テナントにおいて、完全なマルチテナント管理と独立したポリシー管理の分離を実現します。この分離には、各テナントにファイアウォール操作を指示するNSMの管理機能が含まれます。割り当てられたテナントアカウントの境界内でデバイスグループ管理やポリシーの調整、その他すべての管理タスクを実行するために、すべてのテナントに独自のユーザー、グループ、役割を設定できます。

### デバイスグループ管理

デバイスグループでは、ファイアウォールデバイスをグループまたは階層グループとして作成および管理し、ファイアウォールのグループに構成テンプレートをコミットし展開する効果的な方法を提供します。これにより、選択したファイアウォールグループ全体で共通のポリシーやオブジェクト、要件を一貫性のある信頼性の高い方法で同期および実施できます。テンプレートにあるすべての承認済みポリシーへの変更は、そのテンプレートにリンクされているすべてのデバイスグループに自動的に適用されます。デバイスのグループ化は、管理や識別、関連付けを容易にするために、ネットワークタイプやロケーション、事業部、組織構造、相対的な属性の組み合わせといったあらゆる特性に基づいて細かく定義できます。

### テンプレートの管理、コミット、展開

NSMの簡略化されたワークフローにより、多くのロケーションで1台から数千台のファイアウォールデバイスを管理する構成テンプレートを容易かつ迅速に設計、検証、監査およびコミットできます。さまざまなファイアウォールポリシーや設定、関連オブジェクトを含むテンプレートは、デバイスから独立して定義され、同様の構成を必要とするデバイスまたはデバイスグループに一元的かつ自動的にプッシュするためにNSMが使用します。

## 効率性の向上：スマートに仕事をこなし、容易かつ迅速にセキュリティアクションを実行

NSMは、スマートに仕事をこなし、容易かつ迅速にセキュリティアクションを実行できる生産性管理ツールです。ビジネスプロセスを簡略化し、場合によってはセキュリティ運用と管理作業の実行における複雑さ・時間・オーバーヘッドを抑えつつ、ワークフローを自動化してより優れたセキュリティ関連の調整を実現するという原則に基づきNSMは設計されています。

### 手間いらずのゼロタッチデプロイ

NSMに統合されるゼロタッチデプロイサービスは、遠隔拠点や支部・支店へのSonicWallファイアウォールやスイッチ、アクセスポイントの展開および運用を手間をかけずに実現します。プロセス全体に必要なユーザー介入は最小限で、完全に自動化されています。ゼロタッチ対応デバイスは、直接インストール先のサイトに出荷されます。パッケージを開封して登録し、ネットワークにつないで電源をオンにすれば、接続されたすべてのデバイスは、即座に安全かつシームレスに操作できます。NSMで通信リンクが確立されると、あらかじめプロビジョニングされたデバイステンプレートが自動的にすべてのゼロタッチ対応デバイスにプッシュされます。これによって従来の現場での導入プロセスにおける時間やコスト、複雑さが排除されます。

### エラーのない変更管理

NSMは、ファイアウォールポリシーの変更管理およびSOCの監査要件に適う強力な自動化ワークフローへの即時アクセスを提供します。すなわち、展開前にファイアウォールポリシーの構成、比較、検証、レビュー、承認といった一連の厳密なプロセスを適用することで、エラーフリーのポリシー管理を実現します。承認グループには、さまざまな種類の組織が定める異なる承認および監査手順に準拠できる柔軟性があります。NSMは、完全に検証および監査されたセキュリティポリシーをプログラムとして展開し、運用効率の改善、リスク軽減、設定ミスやヒューマンエラーの排除を実現します。

### RESTful APIによる管理の自動化

NSM RESTful APIは、熟練したセキュリティ担当者がNSM独自の機能を管理するための標準的なアプローチを提供します。NSMとサードパーティの管理コンソール間の相互運用を容易にし、社内セキュリティチームの効率を高めることができます。APIサービスは、管理対象デバイスのファイアウォール操作を自動化するために使用されます。これには、テナントやデバイスグループの管理、監査構成、システムの健全性の確認操作などの日常業務が含まれます。

## 認識の向上：隠れたリスクを調査するアクティブな監視、レポート、分析

NSMのインタラクティブなダッシュボードには、リアルタイムのデータの監視、レポート作成、分析機能が搭載されており、問題のトラブルシューティングやリスクの調査、より強力な適応型セキュリティ対策の実施に向けたスマートなセキュリティポリシーの決定とアクションの実行をサポートします。

### 優れた可視性

NSMのレポート、分析、リスクの監視ダッシュボードは、テナント、グループ、デバイスの各レベルにおいて、SonicWallのセキュリティエコシステム全体を最長7日間、360度継続的に可視化します。また、ファイアウォールエコシステムを通過するすべてのネットワークトラフィックとデータ通信について、静的なほぼリアルタイムの分析を提供します。ログデータはすべて自動的に記録、集計、コンテキスト化され、有意義で実践的、かつ理解しやすい方法で表示されるため、データドリブンな洞察と状況認識に基づき、適切な防御・是正措置を発見、解釈、優先順位付けし、実施することができます。スケジュールレポートを使用すれば、監査可能な

データを任意に組み合わせてレポートを完全にカスタマイズすることも可能。履歴データによる分析や異常検出、セキュリティギャップの発見などを目的に、デバイスレベルで記録されたログを最長365日間表示するため、効果的なネットワークとセキュリティ操作を追跡、測定、実行できます。

**リスクの把握**

ドリルダウン機能とピボット機能の追加により、データをより詳細に調査して関連付け、高度な正確性と確信をもって隠れた脅威や問題を徹底的に検証し、発見できるようになりました。履歴レポートと、ユーザーベースおよびアプリケーションベースの分析、エンドポイントの可視性を組み合わせることで、出入りのトラフィックやアプリケーションの使用状況、ユーザーおよびデバイスのアクセス、脅威アクションなどに関連する多様なパターンや傾向を徹底的に分析できます。これにより、セキュリティリスクの発見だけでなく、修復を一元化するための状況認識や重要なインサイトや知識を取得しながら、環境全体で一貫したセキュリティの実施を促進・推進する結果を監視および追跡できます。

## 機能の概要

**管理**

- テナントおよびデバイスグループレベルの管理
- 構成テンプレート
- デバイスのグループ化
- コミットと展開のウィザード
- 構成の監査
- Config – Diff
- オフライン管理とスケジュール
- セキュリティファイアウォールポリシーの管理
- セキュリティVPNポリシーの管理
- SD-WANの管理
- 付加価値セキュリティサービスの管理
- 冗長性と高可用性
- ファイアウォールアプライアンスの設定ファイルのバックアップ
- RESTful API
- ファームウェアアップグレード
- 役割ベースの管理
- アクセスポイントとスイッチの管理

**モニタリング**

- デバイスの健全性とステータス
- ライセンスとサポートのステータス
- ネットワーク／脅威サマリー
- アラートおよび通知センター
- イベントログ
- トポロジビュー

**分析**

- ユーザーベースのアクティビティ
- アプリケーションの使用状況
- Capture Clientによる製品間の可視性
- リアルタイムの動的な可視化
- ドリルダウン機能とピボット機能

**レポート機能**

- スケジュールされたPDFレポート - テナント／グループ／デバイスレベル
- カスタマイズ可能なレポート
- 集中型ロギング
- マルチ脅威レポート
- ユーザー中心のレポート
- アプリケーションの使用状況レポート
- 帯域幅とサービスのレポート
- ユーザーごとの帯域幅レポート

## ライセンスおよびパッケージ

| 機能 | Essential | Advanced |
|---|---|---|
| テナントごとに数百台のデバイスを管理 | Yes | Yes |
| マルチテナント管理 | Yes | Yes |
| デバイスインベントリ | Yes | Yes |
| グループレベルでのポリシーのプッシュ | Yes | Yes |
| デバイスグループ | Yes | Yes |
| テンプレート | Yes | Yes |
| コミットと展開 | Yes | Yes |
| 構成の監査 | Yes | Yes |
| Config Diff | Yes | Yes |
| ワークフローの自動化 | Yes | Yes |
| API | Yes | Yes |
| ゼロタッチデプロイ | Yes | Yes |
| タスクのスケジューリング | Yes | Yes |

| 機能 | Essential | Advanced |
|---|---|---|
| バックアップ／リストア | Yes | Yes |
| ファームウェアアップグレード | Yes | Yes |
| アクセスポイントとスイッチの管理 | Yes | Yes |
| データのレポート日数 | 7日 | 365日 |
| グループ／テナントレベルのダッシュボード | Yes | Yes |
| Capture ATP（デバイスレベル） | Yes | Yes |
| Capture Threat Assessment（デバイスレベル） | Yes | Yes |
| グループレベルの可視性とレポート機能 | Yes | Yes |
| スケジュールレポート（デバイスグループレベル） | Yes | Yes |
| ユーザーベースの分析 | No | Yes |
| アプリケーション分析 | No | Yes |
| 脅威分析 | No | Yes |
| ドリルダウンとピボット | No | Yes |

| 製品 | SKU |
|---|---|
| NSM ESSENTIAL FOR SOHO 250（1年間） | 02-SSC-5219 |
| NSM ADVANCED FOR SOHO 250（1年間） | 02-SSC-5213 |
| NSM ESSENTIAL FOR TZ 350（1年間） | 02-SSC-5239 |
| NSM ADVANCED FOR TZ 350（1年間） | 02-SSC-5231 |
| NSM ESSENTIAL FOR TZ 400（1年間） | 02-SSC-5263 |
| NSM ADVANCED FOR TZ 400（1年間） | 02-SSC-5257 |
| NSM ESSENTIAL FOR TZ 500（1年間） | 02-SSC-5183 |
| NSM ADVANCED FOR TZ 500（1年間） | 02-SSC-5177 |
| NSM ESSENTIAL FOR TZ 570（1年間） | 02-SSC-4975 |
| NSM ADVANCED FOR TZ 570（1年間） | 02-SSC-4963 |
| NSM ESSENTIAL FOR TZ 600（1年間） | 02-SSC-5201 |
| NSM ADVANCED FOR TZ 600（1年間） | 02-SSC-5195 |
| NSM ESSENTIAL FOR TZ 670（1年間） | 02-SSC-5011 |
| NSM ADVANCED FOR TZ 670（1年間） | 02-SSC-4999 |
| NSM ESSENTIAL FOR NS*a* 2600/NS*a* 2650（1年間） | 02-SSC-5281 |
| NSM ADVANCED FOR NS*a* 2600/NS*a* 2650（1年間） | 02-SSC-5275 |
| NSM ESSENTIAL FOR NS*a* 3600/NS*a* 3650（1年間） | 02-SSC-5299 |
| NSM ADVANCED FOR NS*a* 3600/NS*a* 3650（1年間） | 02-SSC-5293 |
| NSM ESSENTIAL FOR NS*a* 4600/NS*a* 4650（1年間） | 02-SSC-5325 |
| NSM ADVANCED FOR NS*a* 4600/NS*a* 4650（1年間） | 02-SSC-5319 |
| NSM ESSENTIAL FOR NS*a* 5600/NS*a* 5650（1年間） | 02-SSC-5347 |
| NSM ADVANCED FOR NS*a* 5600/NS*a* 5650（1年間） | 02-SSC-5341 |
| NSM ESSENTIAL FOR NS*a* 6600/NS*a* 6650（1年間） | 02-SSC-5365 |
| NSM ADVANCED FOR NS*a* 6600/NS*a* 6650（1年間） | 02-SSC-5359 |

*複数年SKUおよびサポート契約にもご利用いただけます。全リストについては、お近くの再販業者またはSonicWallセールスにお問い合わせください。*

## インターネットブラウザ

- Microsoft® Internet Explorer 11.0以降、最新バージョンのMicrosoft Edge、Mozilla Firefox、Google Chrome、Safari。

## NSMの管理対象デバイス[1]

- SonicWall Network Security Appliance：SuperMassive 9000シリーズ[2]、E-Class NSA、NS*sp* 12000シリーズ[2]、NS*a*シリーズ、TZシリーズ、SOHO-W、SOHO 250、SOHO 250W
- SonicWall Network Security Virtual Appliance：NSvシリーズ
- SonicWall SonicWave、SonicPoint
- SonicWallスイッチ

[1] SonicOSバージョン6.xまたは7.xを実行するファイアウォールに対応します。
[2] 365日のレポート表示および30日の分析機能はサポートされていません。

## 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の現実に対処します。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。詳細は、www.sonicwall.comをご確認ください。

**SonicWall Inc.**
1033 McCarthy Boulevard | Milpitas, CA 95035 USA
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**



データシート-NSM-US-COG-2114