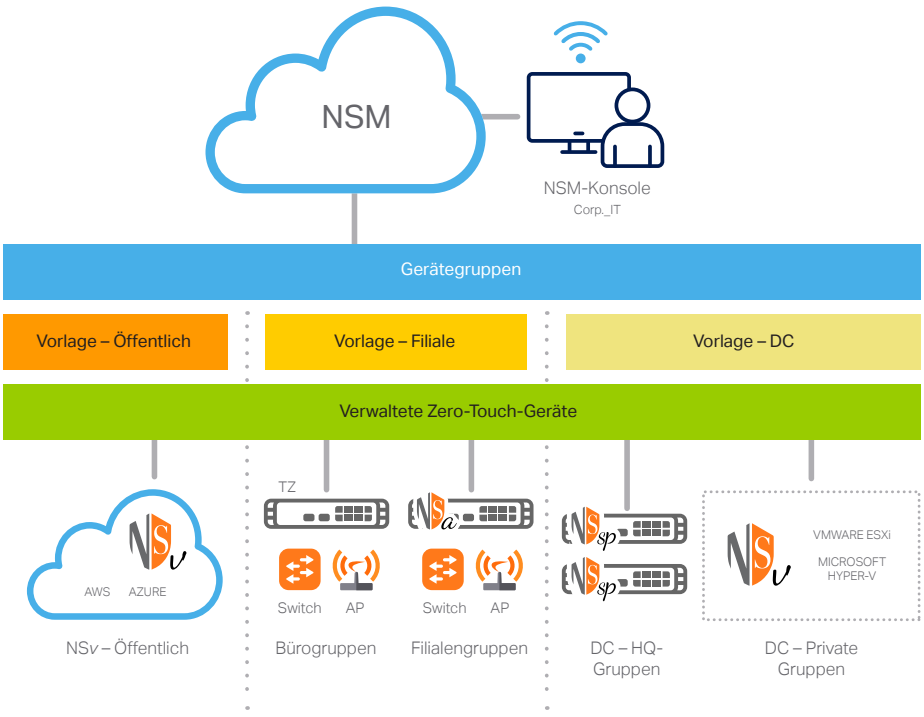
SONICWALL

Network Security Manager

Einheitliches und für jede Umgebung skalierbares Firewall-Management-System

Sowohl bei kleinen und verteilten Unternehmen als auch bei großen Unternehmensgruppen kann sich der Netzwerkschutz aufgrund von Verwaltungsfehlern, unvorhersehbaren Risiken und regulatorischen Auflagen schnell zu einer Herausforderung entwickeln. Gute Praktiken für die Firewall-Verwaltung basierten bisher hauptsächlich auf einem robusten und zuverlässigen System sowie betrieblichen Kontrollmaßnahmen. Doch häufige Fehler, Fehlkonfigurationen und Nichteinhaltung dieser Kontrollen stellen auch in den bestgeführten Security Operation Centers (SOCs) konstante Herausforderungen dar.

SonicWall Network Security Manager (NSM) ist ein zentralisierter Firewall-Manager für mehrere Mandanten und ermöglicht durch den Einsatz von auditierbaren Arbeitsabläufen eine fehlerfreie zentrale Verwaltung aller Firewall-Funktionen. Die native Analyse-Engine sorgt für zentrale Transparenz und ermöglicht eine effektive Überwachung und Aufdeckung von Bedrohungen durch Vereinheitlichung und Korrelation der Protokolle über alle Firewalls hinweg. Der NSM unterstützt auch die Aufrechterhaltung der Konformität, da für alle Konfigurationsänderungen ein kompletter Audit-Trail und granulare Berichte erstellt werden. Der NSM lässt sich problemlos für jede Unternehmensgröße skalieren – von kleinen Organisationen bis hin zu Netzwerken mit Tausenden von Firewall-Appliances an zahlreichen Standorten – und all das mit weniger Arbeits- und Zeitaufwand.



Vorteile:

Geschäft

- Senkung der Kosten für das Sicherheitsmanagement
- Kenntnis der Bedrohungslandschaft und des Sicherheitslevels
- Senkung der CAPEX mit SaaS

Betrieb

- Keine Implementierung von HW/SW
- Beseitigung von Firewall-Management-Silos
- Leichtes Remote-Onboarding einer beliebigen Anzahl von Firewalls
- Transparenz bei allen Sicherheitsvorgängen

Sicherheit

- Prüfung, Festlegung und Durchsetzung von einheitlichen Sicherheitsrichtlinien in allen Umgebungen
- Schnelle Auffindung und Reaktion auf Probleme und Risiken
- Informierte Entscheidungen bzgl. Sicherheitsregeln

Umfassende Kontrolle: Alle Firewall-Funktionen können von einer zentralen Stelle aus gesteuert werden

NSM bietet Ihnen alles, was Sie für ein einheitliches Firewall-Management-System benötigen. Sie erhalten Transparenz auf Mandantenebene, gruppenbasierte Gerätesteuerung und unbegrenzte Skalierbarkeit für die zentrale Verwaltung und Bereitstellung Ihrer SonicWall Network Security Funktionen. Dazu gehören die Einbindung und Verwaltung aller Firewall-Appliances, Gerätegruppen und Mandanten, die Synchronisierung und Durchsetzung einheitlicher Sicherheitsrichtlinien in Ihren Umgebungen mit flexiblen lokalen Kontrollen und die komplette Überwachung über ein dynamisches Dashboard mit detaillierten Berichten und Analysen. Mit NSM können alle diese Aufgaben über eine funktionsreiche zentrale Benutzeroberfläche abgewickelt werden, die von jedem Ort aus über ein browserfähiges Endgerät zugänglich ist.

Verwaltung mehrerer Mandanten
Für Ihre konstant wachsende Firewall-Umgebung mit komplexen an mehreren Orten und in mehreren Clouds basierten Mandanten, bei denen für jedes Netzwerksegment unterschiedliche Sicherheitsanforderungen gelten, benötigen Sie ein entsprechend skalierbares Firewall-Management-System. NSM bietet ein komplettes Multi-Tenant-Management und eine unabhängige, getrennte Richtlinienkontrolle für alle verwalteten Mandanten. Diese Trennung gilt für alle Management-Features und Funktionen des NSM, die den Betrieb der Firewall für jeden Mandanten regeln. Sie können für jeden Mandanten einen eigenen Satz von Benutzern, Gruppen und Rollen erstellen, um die Gerätegruppenverwaltung, die Orchestrierung von Richtlinien und alle anderen administrativen Aufgaben innerhalb der Grenzen des zugewiesenen Mandantenkontos durchzuführen.

Verwaltung von Gerätegruppen
Die Funktion „Device Group“ bietet eine effektive Methode zum Erstellen und Verwalten von Firewall-Appliances als Gruppe oder hierarchische Gruppen und zum Festlegen und Einbinden von Konfigurationsvorlagen für diese Firewall-Gruppen. Auf diese Weise können allgemeine Richtlinien, Objekte und/oder Anforderungen über alle ausgewählten Firewall-Gruppen hinweg einheitlich und zuverlässig synchronisiert und durchgesetzt werden. Alle genehmigten Richtlinienänderungen in der Vorlage werden automatisch auf alle mit dieser Vorlage verknüpften Gerätegruppen angewendet. Die Gruppierung von Geräten kann anhand von Merkmalen wie Netzwerktyp, Standort, Geschäftseinheit, Organisationsstruktur oder einer Kombination aus relativen Attributen granular definiert werden, wodurch Verwaltung, Identifizierung und Zuordnung wesentlich erleichtert werden.

Verwaltung, Festlegung und Einbindung von Vorlagen
Die durch den NSM vereinfachten Arbeitsabläufe ermöglichen die einfache und schnelle Erstellung, Validierung, Prüfung und Anwendung von Konfigurationsvorlagen für die Verwaltung von Tausenden von Firewall-Appliances an zahlreichen geografischen Standorten. Vorlagen mit verschiedenen Firewall-Richtlinien, Einstellungen und verwandten Objekten werden geräteunabhängig definiert und von NSM verwendet, um Geräte oder Gerätegruppen, die ähnliche Konfigurationen erfordern, zentral und automatisch anzusteuern.

Gesteigerte Effektivität: Intelligentere Arbeitsabläufe und schnelle Durchsetzung von Sicherheitsmaßnahmen mit weniger Aufwand

NSM ist ein produktivitätssteigerndes Management-Tool, mit dem Sie intelligenter arbeiten und mit weniger Aufwand schneller Sicherheitsmaßnahmen ergreifen können. Das durch Geschäftsabläufe geleitete Konzept beruht auf der Vereinfachung und in manchen Fällen auf der Automatisierung von Arbeitsabläufen und führt zu einer besseren Sicherheitskoordination und Entscheidungsfindung. Gleichzeitig werden die bei der Durchführung und Verwaltung der Sicherheitsmaßnahmen entstehenden Komplexitäten, Zeitaufwendungen und Kosten reduziert.

Müheloses Zero-Touch-Deployment
Mit dem in NSM integrierten Zero-Touch-Deployment-Service können SonicWall Firewalls, Switches und Access Points mühelos an Remote-Standorten und Zweigniederlassungen eingebunden und betrieben werden. Der gesamte Prozess läuft vollautomatisch ab und erfordert nur minimale Benutzereingriffe. Zero-Touch-fähige Geräte werden direkt an die Installationsstandorte geliefert. Die Geräte müssen nur ausgepackt, registriert, mit dem Netzwerk verbunden und an das Stromnetz angeschlossen werden. Sie sind dann sofort einsatzbereit und sorgen für nahtlose Sicherheit und Konnektivität. Nach Herstellung der Kommunikationsverbindungen mit dem NSM werden vorkonfigurierte Gerätevorlagen automatisch per Push-Funktion an alle Zero-Touch-fähigen Geräte geleitet. Gegenüber dem herkömmlichen vor Ort durchgeführten Onboarding-Prozess wird hiermit der Zeit- und Kostenaufwand sowie die Komplexität reduziert.

Fehlerfreies Change-Management
NSM bietet sofortigen Zugriff auf leistungsstarke automatisierte Arbeitsabläufe, die den Anforderungen von SOCs an das Änderungsmanagement und Auditing von Firewall-Richtlinien entsprechen. Dieser Prozess ermöglicht es, eine strenge Vorgehensweise für die Konfiguration, den Vergleich, die Validierung, die Prüfung und die Genehmigung von Firewall-Richtlinien vor der Implementierung durchzusetzen. Auf diese Weise wird die Richtigkeit von Richtlinienänderungen sichergestellt. Die Freigabegruppen sind flexibel und können so den Genehmigungs- und Auditverfahren verschiedener Arten von Organisationen gerecht werden. NSM setzt richtungsweisende komplett validierte und geprüfte Sicherheitsrichtlinien ein, um die betriebliche Effizienz zu verbessern, Risiken zu mindern und Fehlkonfigurationen sowie menschliche Fehler auszuschalten.

Automatisierung der Verwaltung mit RESTful API
RESTful APIs von NSM bieten den Sicherheitsfachkräften einen Standardansatz für die programmatische Verwaltung von NSM-spezifischen Funktionen ohne die Notwendigkeit einer Management-Web-Benutzeroberfläche. Dadurch wird die Interoperabilität zwischen NSM und Management-Konsolen von Drittanbietern ermöglicht und zugleich die Effizienz Ihres internen Sicherheitsteams gesteigert. Die API-Dienste werden für die Automatisierung der Firewall-Funktionen aller verwalteten Geräte genutzt. Dazu gehören alltägliche Aufgaben wie die Verwaltung von Mandanten, Gerätegruppen, Audit-Konfigurationen sowie die Durchführung von Systemprüfungen und vieles mehr.

Verstärktes Bewusstsein: Untersuchung versteckter Risiken mit aktiver Überwachung, Berichterstattung und Analyse

Das interaktive NSM-Dashboard bietet Echtzeit-Überwachung, Reporting und Analysedaten für die Fehlersuche, Risikoermittlung, sicherheitsspezifische Entscheidungsfindung und Durchsetzung von Richtlinienmaßnahmen und sorgt somit für ein stärkeres adaptives Sicherheitslevel.

Umfassende Transparenz
Das NSM-Dashboard für Reporting, Analysen und Risikoüberwachung bietet eine bis sieben Tage erfassende kontinuierliche 360°-Sichtbarkeit des gesamten SonicWall-Sicherheitsökosystems auf Mandanten-, Gruppen- oder Geräteebene. Dazu gehört eine statische und nahezu Echtzeit-Analyse des gesamten Netzwerkverkehrs und der Datenkommunikation, die das Firewall

Ökosystem passieren. Alle Protokolldaten werden automatisch aufgezeichnet, aggregiert, kontextualisiert und auf eine sinnvolle, umsetzbare und leicht verständliche Weise präsentiert. Auf Basis dieser datengesteuerten Erkenntnisse und der situationsbezogenen Übersicht können auf leichte Weise geeignete defensive und korrigierende Maßnahmen identifiziert, ausgelegt, priorisiert und durchgeführt werden. Regelmäßig ausgegebene Berichte können mit jeder beliebigen Kombination von auditierbaren Daten bedarfsgerecht angepasst werden. Bis zu 365 Tage können auf Geräteebene protokolliert und für historische Analysen, Erkennung von abnormalen Aktivitäten, Entdeckung von Sicherheitslücken und vielem mehr genutzt werden. Dadurch werden die Verfolgung, Messung und Ausführung eines effektiven Netzwerk- und Sicherheitsbetriebs ermöglicht.

Verständnis des Risikos
Mithilfe von zusätzlichen Drilldown- und Pivoting-Funktionen lassen sich Daten noch gründlicher untersuchen und korrelieren, um versteckte Bedrohungen und Probleme mit erhöhter Genauigkeit und Zuverlässigkeit aufzudecken. Eine Kombination aus historischem Reporting, benutzer- und anwendungsbasierten Analysen und Endpunkttransparenz ermöglicht die gründliche Analyse von verschiedenen Mustern und Trends im Zusammenhang mit eingehendem und ausgehendem Verkehr, Anwendungsnutzung, Benutzer- und Gerätezugriff, Bedrohungsaktionen und vielem mehr. Sie erhalten einen situativen Überblick und wertvolle Einblicke und Erkenntnisse, die Ihnen bei der Aufdeckung und Behebung von Sicherheitsrisiken helfen. Gleichzeitig können Sie die Ergebnisse überwachen und verfolgen, um eine konstante Durchsetzung der Sicherheitsmaßnahmen in Ihrem gesamten System voranzutreiben.

Funktionen im Überblick

Verwaltung

- Verwaltung auf Mandanten- und Gerätegruppenebene
- Konfigurationsvorlagen
- Gerätegruppierung
- Festlegungs- und Implementierungsassistent
- Konfigurationsaudits
- Konfig. – Diff
- Offline-Management und -Terminierung
- Management der Security Firewall-Richtlinien
- Management der Security VPN-Richtlinien
- Management des SD-WAN
- Management der Value Added Security Services
- Redundanz und hohe Verfügbarkeit
- Sicherung der Einstellungsdateien für die Firewall-Appliance
- RESTful API
- Firmware-Upgrade
- Rollenbasierte Administration
- Access Point- und Switch-Management

Überwachung

- Gerätezustand und -status
- Lizenz- und Supportstatus
- Netzwerk/Bedrohungen im Überblick
- Alarm- und Benachrichtigungszentrale
- Ereignisprotokolle
- Topology Ansicht

Analytics

- Benutzerbasierte Analysen
- Anwendungsnutzungs-Reporting
- Produktübergreifende Transparenz mit Capture Client
- Dynamische Visualisierung in Echtzeit
- Drilldown- und Pivoting-Funktionen

Wireless-Access-Points

- Regelmäßige PDF-Berichte – auf Mandanten-/Gruppen-/Geräteebene
- Anpassbare Berichte
- Zentrale Protokollierung
- Multi-Threat-Reporting
- Reporting auf Benutzerebene
- Reporting auf Anwendungsebene
- Bandbreiten- und Dienste-Reporting
- Bandbreiten-Reporting nach Benutzer

Lizenzierung und Pakete

Funktionen	Essential	Advanced
Verwaltung von Hunderten von Geräten pro Mandant	Ja	Ja
Verwaltung mehrerer Mandanten	Ja	Ja
Gerätebestand	Ja	Ja
Anwendung von Richtlinien auf Gruppenebene per Push	Ja	Ja
Gerätegruppe	Ja	Ja
Vorlagen	Ja	Ja
Festlegung und Implementierung	Ja	Ja
Konfigurationsaudit	Ja	Ja
Konfigurations-Diff	Ja	Ja
Workflow-Automatisierung	Ja	Ja
API	Ja	Ja
Zero-Touch-Deployment	Ja	Ja
Aufgabenterminierung	Ja	Ja

Funktionen	Essential	Advanced
Sicherung/Wiederherstellung	Ja	Ja
Firmware-Upgrades	Ja	Ja
Access Point- und Switch-Management	Ja	Ja
Tage der Berichtsdaten	7 Tage	365 Tage
Dashboard für Gruppen-/Mandantenebene	Ja	Ja
Capture ATP (Geräteebene)	Ja	Ja
Capture Threat Assessment (Geräteebene)	Ja	Ja
Sichtbarkeit und Reporting auf Gruppenebene	Ja	Ja
Regelmäßige Berichte (Gerätegruppenebene)	Ja	Ja
Benutzerbasierte Analysen	Nein	Ja
Anwendungsanalysen	Nein	Ja
Bedrohungsanalysen	Nein	Ja
Drilldown und Pivoting	Nein	Ja

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

Artikel und Supportverträge sind auch für mehrere Jahre erhältlich. Für eine vollständige Liste wenden Sie sich bitte an Ihren bevorzugten Wiederverkäufer oder an SonicWall Sales.

Internet Browser

- Microsoft® Internet Explorer 11.0 oder höher und die neueste Version von Microsoft Edge, Mozilla Firefox, Google Chrome und Safari.

Durch NSM verwaltete Geräte[1]

- SonicWall Network Security Appliances: SuperMassive 9000 Series[2], E-Class NSA, NS*sp* 12000 Series[2], NS*a* Series, TZ Series, SOHO-W, SOHO 250, SOHO 250W
- SonicWall Network Security Virtual Appliances: NSv Series
- SonicWall SonicWave, SonicPoint
- SonicWall Switch

[1] Unterstützt Firewalls unter SonicOS Version 6.x oder 7.x.
[2] 365 Tage Reporting und 30 Tage Analysen werden nicht unterstützt.

Über SonicWall

SonicWall bietet Boundless Cybersecurity für das hyperverteilte Umfeld einer neuen Arbeitsrealität, in der jeder remote, mobil und ungeschützt ist. Indem SonicWall das Unbekannte kennt, Echtzeit-Transparenz und skalierbare Ökonomien ermöglicht, werden Cybersicherheitslücken bei Unternehmen, Regierungen und KMU weltweit geschlossen. Weitere Informationen finden Sie auf www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035 USA
Weitere Informationen erhalten Sie auf unserer Website.
www.sonicwall.com

Datasheet-NSM-US-COG-2114