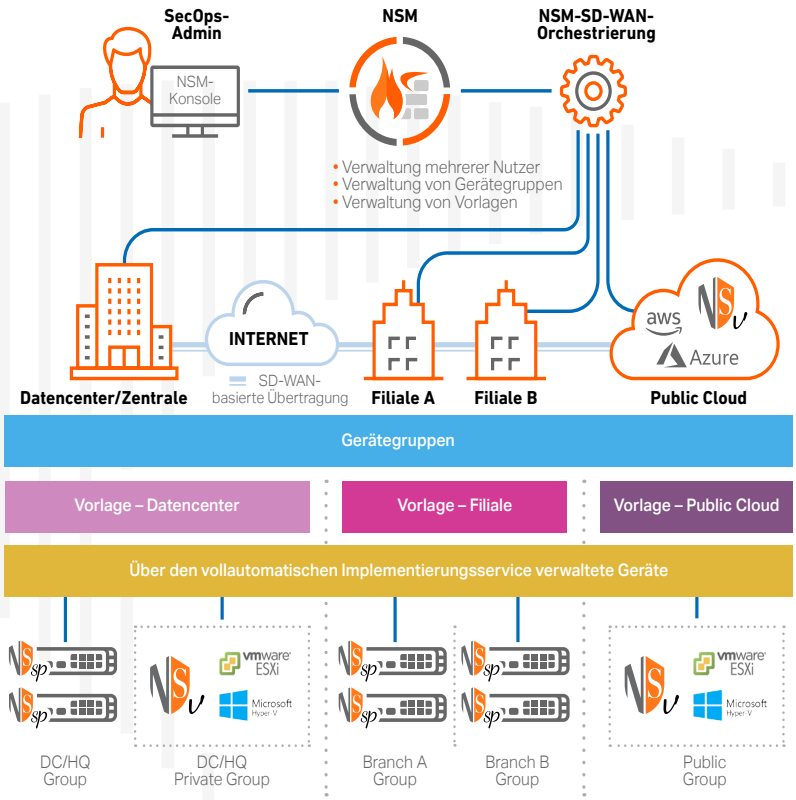
SONICWALL

Network Security Manager

Einheitliches, für beliebige Umgebungen skalierbares Firewall-Management-System

Egal, ob Sie eine kleine Firma, ein verteiltes Unternehmen, mehrere Organisationen oder ein geschlossenes Netzwerk schützen müssen – unstrukturierte Prozesse, unvorhergesehene Risiken und gesetzliche Vorgaben können Ihrer Netzwerksicherheit ganz schön zu schaffen machen. Früher beschränkten sich effiziente Firewall-Management-Praktiken vorwiegend auf die Zuverlässigkeit der Systeme und die Überwachung des Betriebs. Doch häufige Fehler, Fehlkonfigurationen und vielleicht sogar Missachtungen dieser Kontrollen sind selbst in gut organisierten Security-Operations-Centern (SOCs) nach wie vor eine Herausforderung.



HIGHLIGHTS

Geschäft

- Geringerer Aufwand für das Sicherheitsmanagement
- Überblick über Bedrohungslandschaft und Sicherheitsstatus
- Höhere IT-Effizienz bei geringerem Administrationsaufwand
- Vermeidung kostspieliger Geschäftsunterbrechungen und Sicherheitsvorfälle

Betrieb

- Beseitigung von Firewall-Management-Silos
- Einfaches Remote-Onboarding beliebig vieler Firewalls
- Schnelle Reaktion bei kritischen Systemproblemen, was eine optimale Netzwerkperformance gewährleistet
- Einheitliche Konfiguration und Richtlinien über alle verwalteten Geräte hinweg
- Schnelle Implementierung von SD-WAN-Netzwerken

Sicherheit

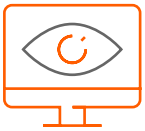
- Prüfung, Zuweisung und Durchsetzung einheitlicher Sicherheitsrichtlinien in allen Umgebungen
- Einheitliche SD-WAN-Konfigurationen an allen Standorten
- Schnelle Erkennung von Bedrohungen, rasche Reaktion auf Probleme und Risiken
- Bessere Überwachung und Nachverfolgung der Ergebnisse regelbasierter Aktionen
- Verhindern einer unautorisierten Benutzerauthentifizierung einschließlich Bedrohungen durch Insider

Zentrale Verwaltung. Mehr Sicherheit.

www.sonicwall.com/nsm

DATENBLATT

Der SonicWall Network Security Manager (NSM), ein zentralisierter Multi-Tenant-Firewall-Manager, ermöglicht eine fehlerfreie und zentrale Verwaltung sämtlicher Firewall-Prozesse gemäß prüfbaren Workflows. Durch Reporting und Analytics[1,2] können Sie die Protokolle aller Firewalls zusammenführen und abgleichen und so Bedrohungen aufdecken und überwachen – alles mithilfe einer einzigen Konsole. Neben einer einheitlichen Regeldurchsetzung über alle Firewalls hinweg bietet NSM zudem detaillierte Audit-Trails von allen Konfigurationsänderungen sowie granulares Reporting, sodass Sie Compliance-Vorschriften besser einhalten können. Die Lösung lässt sich für beliebig große Organisationen skalieren und unterstützt die Verwaltung von Netzwerken mit Hunderten von Firewalls über mehrere Nutzer oder Standorte hinweg. Dabei reduziert NSM den Zeit- und sonstigen Aufwand erheblich.



Volle Kontrolle durch zentrale Orchestrierung der Firewall-Prozesse

NSM bietet Ihnen alles, was Sie für ein einheitliches Firewall-Management-System brauchen. Dank einer umfassenden Transparenz auf Benutzerebene, einer gruppenbasierten Gerätesteuerung und einer unbegrenzten Skalierbarkeit können Sie Ihre SonicWall-Netzwerksicherheitsprozesse zentral bereitstellen und verwalten. Dazu gehören die Implementierung und Verwaltung aller Firewall-Appliances, Gerätegruppen und Nutzer, die Synchronisierung und Durchsetzung einheitlicher Sicherheitsrichtlinien einschließlich DNS und Content-Filterung in Ihren Umgebungen mithilfe flexibler lokaler Kontrollen sowie eine umfassende Überwachung mit detaillierten Berichten und Analysen über ein dynamisches Dashboard. NSM unterstützt auch die Netzwerkzugriffskontrolle durch eine Integration mit Aruba ClearPass. Besonders praktisch: Mit NSM können Sie all diese Aufgaben über eine einzige anwenderfreundliche Konsole erledigen, auf die Sie von jedem Ort aus über beliebige browserfähige Geräte zugreifen können.

Verwaltung mehrerer Nutzer

Wenn Ihre Firewall-Umgebung größer wird, benötigen Sie ein Firewall-Management-System, das mitwächst. NSM ermöglicht eine umfassende Verwaltung mehrerer Nutzer sowie eine unabhängige, getrennte Richtlinienkontrolle für alle verwalteten Nutzer. Diese Trennung umfasst alle Management-Features und -Funktionen von NSM, die den Firewall-Betrieb für die einzelnen Nutzer regeln. Sie können für jeden Nutzer eine Reihe eigener User, Gruppen und Rollen einrichten, um die Gerätegruppenverwaltung, Richtlinien-Orchestrierung und alle anderen administrativen Aufgaben im Rahmen des zugewiesenen Nutzerkontos durchzuführen.

Verwaltung von Gerätegruppen

Die Funktion „Device Group“ bietet eine effektive Methode für die Zuweisung und Verwaltung von Firewall-Geräten als Gruppen oder hierarchische Gruppen und für die Einrichtung und Implementierung von Konfigurationsvorlagen für die Firewall-Gruppen. So können Sie Richtlinien, Objekte und Einstellungen über alle ausgewählten Firewall-Gruppen hinweg einheitlich und zuverlässig synchronisieren und anwenden. Alle genehmigten Richtlinienänderungen in der Vorlage werden automatisch auf alle Gerätegruppen angewendet, die mit dieser Vorlage verknüpft sind. Die Gruppierung von Geräten kann auf Basis beliebiger Eigenschaften wie Netzwerktyp, Standort, Geschäftseinheit, Organisationsstruktur oder einer Kombination solcher Attribute präzise definiert werden. Dies vereinfacht die Verwaltung, Identifizierung und Zuordnung.

Verwaltung, Zuweisung und Implementierung von Vorlagen

NSM vereinfacht Workflows um ein Vielfaches, sodass Sie schnell und leicht Konfigurationsvorlagen entwerfen, validieren, prüfen, genehmigen und zuweisen können, mit denen sich eine oder Hunderte Firewalls an vielen unterschiedlichen Standorten verwalten lassen. Vorlagen mit unterschiedlichen Firewall-Richtlinien, Einstellungen und verwandten Objekten werden unabhängig vom Gerät definiert und von NSM genutzt, um Geräten oder Gerätegruppen, die ähnlich konfiguriert werden müssen, zentral und automatisch Konfigurationen zu senden.

Durch die Kombination von Vorlagen und Template-Variablen können Sie Hunderte von Remote-Firewalls zentral implementieren und bereitstellen, eine einheitliche Konfiguration sicherstellen und gleichzeitig für jedes Gerät eindeutige gerätespezifische Parameter wie Schnittstellen-IPs, DNS-Konfiguration, Firewall-Hostname etc. beibehalten. Verteilte Unternehmen können neue Filialen und Remote-Standorte ganz unkompliziert mit einer einzigen Vorlage onboarden und schützen. Somit entfällt die manuelle Einrichtung für jedes Gerät an jedem Standort.

SD-WAN-Orchestrierung und -Monitoring

NSM vereinfacht die Implementierung unternehmensweiter SD-WAN-Netzwerke über einen intuitiven selbstgesteuerten Workflow. Konfigurationen für anwendungsbasierten Datenverkehr und andere Traffic-Steering-Konfigurationen zwischen Hunderten Standorten wie Filialen und Zweigniederlassungen werden zentral eingerichtet und umgesetzt. Darüber hinaus können Sie dank NSM den Zustand und die Performance Ihrer gesamten SD-WAN-Umgebung überwachen, um einheitliche Konfigurationen sicherzustellen, eine optimale Anwendungsperformance zu erzielen und Netzwerkinfrastrukturteams eine schnelle Untersuchung und Lösung von Problemen zu ermöglichen.

VPN-Orchestrierung und -Monitoring

NSM vereinfacht VPN-Konfigurationen und -Richtlinien mithilfe eines simplen wizardbasierten Schritt-für-Schritt-Set-ups. Systemadministratoren können über einen wiederholbaren selbstgesteuerten Workflow schnell und fehlerfrei Site-to-Site-Verbindungen bzw. eine effiziente Kommunikation herstellen. Dank VPN-Monitoring können Sie Ihre VPNs jederzeit im Blick behalten und etwa die Aktivitäten, den Zustand und die Performance Ihrer gesamten VPN-Umgebung komplett einsehen. Diese Informationen können Netzwerkadministratoren nutzen, um den Verbindungsstatus, die übertragenen Daten und die über diese VPN-Tunnel verbrauchte Bandbreite zu überwachen. Mithilfe von Warnmeldungen können Administratoren die Integrität von VPN-Verbindungen proaktiv gewährleisten und eine kontinuierliche Konnektivität zwischen den Standorten sicherstellen.

Mehr Effektivität durch smarte Prozesse und schnellere, weniger aufwendige Sicherheitsmaßnahmen

NSM ist ein produktivitätssteigerndes Managementtool, mit dem Sie intelligenter arbeiten und Sicherheitsmaßnahmen schneller und mit weniger Aufwand einführen können. Sein Design orientiert sich an relevanten Geschäftsprozessen und zielt darauf ab, Workflows zu vereinfachen und – wo sinnvoll – zu automatisieren, um die Koordination der Sicherheitsfunktionen zu verbessern. Darüber hinaus trägt NSM dazu bei, die Komplexität sowie den Zeit- und sonstigen Aufwand von täglichen Sicherheitsprozessen und Administrationsaufgaben zu reduzieren.

Mühelose vollautomatische Implementierung

Der im NSM integrierte Zero-Touch-Deployment-Service ermöglicht es Ihnen, Firewalls, Switches und Access-Points von SonicWall ganz unkompliziert an Filialen und Remote-Standorten zu implementieren und in Betrieb zu nehmen. Der komplette Prozess erfordert nur einen minimalen Benutzereingriff und ist vollständig automatisiert. Geräte, die diesen vollautomatischen Implementierungsservice bieten, werden direkt an die Installationsstandorte geliefert. Sobald sie registriert und mit dem Netzwerk verbunden sind, können alle vernetzten Geräte sofort in Betrieb genommen werden. Dabei werden eine nahtlose Sicherheit und Konnektivität gewährleistet. Nach Herstellung einer Verbindung zum NSM werden vorkonfigurierte Gerätevorlagen automatisch an alle vernetzten Geräte gesendet. All dies reduziert die Komplexität sowie den Zeit- und Kostenaufwand im Vergleich zu traditionellen On-Site-Onboarding-Prozessen um ein Vielfaches.

Fehlerfreies Changemanagement

NSM ermöglicht einen unmittelbaren Zugriff auf leistungsstarke automatisierte Workflows, die den SOC-Anforderungen an das Auditing und die Verwaltung von Richtlinienänderungen an der Firewall gerecht werden. Eine Reihe strenger Prozesse, wie zum Beispiel der Vergleich, die Prüfung und die Autorisierung der Konfiguration vor der Implementierung, sorgt für fehlerfreie Richtlinienänderungen. Die Freigabegruppen sind flexibel und entsprechen den internen Auditverfahren unterschiedlicher funktioneller Teams. Dank des obligatorischen Genehmigungsprozesses können Sie mit NSM die operative Effizienz verbessern, Risiken minimieren und Fehlkonfigurationen verhindern.

Automatisierte Verwaltung mit RESTful-APIs

Die RESTful-APIs von NSM bieten versierten Sicherheitskräften einen Standardansatz, um NSM-spezifische Features ohne Web-Managementoberfläche programmatisch zu verwalten. Dabei steigert die Interoperabilität zwischen NSM und Verwaltungskonsolen Dritter die Effizienz interner Sicherheitsteams. Die API-Services können Firewall-Prozesse für beliebige verwaltete Geräte automatisieren, wie etwa typische tägliche Aufgaben wie die Verwaltung von Gerätegruppen und Nutzern, Audit-Konfigurationen und die Prüfung des Systemzustands.

Umfassenderer Einblick: verborgene Risiken durch aktive Überwachung, Berichte und Analysen prüfen[1,2]

Das interaktive NSM-Dashboard ermöglicht Echtzeit-Monitoring und -Reporting und stellt Analysedaten zur Verfügung, mit denen Sie Probleme beheben, Risiken untersuchen und intelligente Sicherheitsrichtlinien für eine adaptivere Sicherheitsstrategie umsetzen können.

Mithilfe von Echtzeit-Warnmeldungen können Administratoren schnell und präzise handeln und so einen optimalen Betrieb sicherstellen. Das hilft wiederum, kostspielige Geschäftsunterbrechungen und Sicherheitsvorfälle zu vermeiden.

Umfassende Einblicke

In Kombination mit Analytics[1,2] bietet Ihnen NSM über einen Zeitraum von bis zu sieben Tagen einen kontinuierlichen Überblick über die Benutzer, Gruppen oder Geräte Ihres gesamten SonicWall-Sicherheitsökosystems. Dazu gehören statische und echtzeitnahe Analysen des kompletten Netzwerkverkehrs und der gesamten Datenkommunikation im Firewall-Ökosystem. Alle Protokolldaten werden automatisch erfasst, aggregiert, kontextualisiert und auf aussagekräftige, übersichtliche und leicht nutzbare Weise präsentiert. So können Sie die Daten ermitteln, interpretieren

und priorisieren und auf der Grundlage datenbasierter und situationsbezogener Erkenntnisse angemessene Abwehr- und Korrekturmaßnahmen treffen. Durch zeitgesteuertes Reporting können Sie Ihre Berichte personalisieren und dabei beliebige Traffic-Daten kombinieren. Bis zu 365 Tage können auf Ebene der Geräte, Gerätegruppen oder Nutzer protokolliert werden. Die Logs lassen sich dann beispielsweise für historische Analysen, die Erkennung von Anomalien und die Identifizierung von Sicherheitslücken nutzen. Diese Informationen helfen, effektive Netzwerk- und Sicherheitsprozesse auszuführen, nachzuverfolgen und zu messen.

Das Risiko verstehen

Mit den zusätzlichen Drill-down- und Pivoting-Funktionen können Sie die Daten weiter untersuchen und abgleichen, um verborgene Bedrohungen und Probleme zuverlässiger aufzudecken und genauer unter die Lupe zu nehmen. Historische Berichte, benutzer- und anwendungsbasierte Analysen und transparente Informationen zu Endpunkten ermöglichen es Ihnen, verschiedene Muster und Trends im Hinblick auf ein- und ausgehenden Verkehr, Anwendungsnutzung, Benutzer- und Gerätezugriff, Bedrohungsaktionen usw. gründlich zu analysieren. Diese situationsbezogenen Informationen und wertvollen Erkenntnisse helfen Ihnen dabei, Sicherheitsrisiken aufzudecken und Fehler zu beheben. Außerdem können Sie die Ergebnisse überwachen und nachverfolgen, um die Einhaltung der Sicherheitsmaßnahmen in Ihrer gesamten Umgebung konsequent zu gewährleisten.

Optimierung der Mitarbeiterproduktivität

Benutzeranalysen[1,2] bieten Ihnen einen umfassenden und transparenten Überblick über die Webanwendungs- und Internetnutzung Ihrer Mitarbeiter. Analysten können durch Drill-down-Funktionen interessante Datenpunkte schnell, einfach und flexibel auf Benutzerebene untersuchen. Werden dabei riskante Anwendungen bzw. auffällige Benutzer identifiziert, lassen sich hierfür evidenzbasierte und richtliniengesteuerte Maßnahmen einrichten. Darüber hinaus bieten Produktivitätsberichte[1,2] einen Einblick in die Internetnutzung und das Verhalten von Mitarbeitern über einen bestimmten Zeitraum. Dank der generierten Snapshots und Drill-down-Berichte lassen sich die Webaktivitäten der Nutzer in Produktivitätsgruppen wie „produktiv“, „unproduktiv“, „akzeptabel“, „inakzeptabel“ oder auch in benutzerdefinierte Gruppen einteilen. Auf diese Weise erhalten Organisationen einen besseren Einblick in die Internetnutzung und können diese effektiver überwachen.

Flexible Implementierung

NSM lässt sich auf verschiedene Weisen implementieren, sodass Kunden ihre individuellen betrieblichen Anforderungen, Budgetvorgaben sowie gesetzliche Vorschriften optimal erfüllen können.

NSM ist auch als wartungsfreie, von SonicWall gehostete SaaS-Lösung verfügbar. Sie können über das Internet darauf zugreifen und die Lösung bei Bedarf skalieren, was Ihre Betriebskosten senkt. Sie müssen weder Hardware oder Software implementieren, noch fallen Kosten für Wartungspläne, Software-Personalisierung, Konfigurationen oder Upgrades, Ausfallzeiten, Abschreibungen und Außerbetriebsetzung an. Statt all dieser Ausgaben entsteht lediglich eine geringe, genau planbare jährliche Abogebühr.

Für eine umfassende Systemkontrolle und Compliance können Sie NSM in der Public Cloud Microsoft Azure oder als virtuelle Appliance in einer Private Cloud auf VMware, Microsoft Hyper-V oder KVM implementieren. Mit diesen Optionen profitieren Sie von allen betrieblichen und wirtschaftlichen Vorteilen der Virtualisierung, wie einer hohen Skalierbarkeit und Flexibilität, einer schnellen Systembereitstellung, einer einfachen Verwaltung sowie niedrigeren Kosten.

Sicherheitsfunktionen

Staatliche und öffentliche Einrichtungen, Healthcare- und Pharmaunternehmen sowie andere große Organisationen nutzen häufig geschlossene Netzwerke, um ihre geschäftskritischen Anwendungen und sensiblen Informationssysteme wie Verschlusssachen, SCADA und Forschungseinrichtungen abzuschirmen und zu schützen. NSM unterstützt geschlossene Netzwerkumgebungen mit einer Offline-Option für Onboarding, Lizenzierung, Patching und Upgrade des NSM-Systems und der verwalteten Firewalls, ohne den SonicWall License Manager und MySonicWall kontaktieren zu müssen.

Darüber hinaus nutzt NSM eine Reihe von Kontrollmaßnahmen für den Zugriff auf Konten, um einen unerlaubten Zugang zur NSM-Verwaltungsschnittstelle zu vermeiden und zusätzliche Sicherheit zu gewährleisten. Dabei werden je nach Benutzerrolle spezifische administrative Kontrollen sichergestellt, und ab einer bestimmten Zahl fehlgeschlagener Log-in-Versuche wird das Konto gesperrt. Ein Zugriff ist außerdem nur möglich, wenn sich der Benutzer von einer Liste erlaubter Quell-IP-Adressen mittels Zwei-Faktor-Authentifizierung (2FA)[3] einloggt.

Die Funktionen im Überblick

Verwaltung

- Netzwerkzugriffskontrolle (NAC) mit Aruba ClearPass
- Verwaltung auf Ebene der Nutzer und Gerätegruppen
- Konfigurationsvorlagen
- Gerätegruppierung
- Erstellung einer Vorlage auf Basis der Gerätekonfiguration
- Assistent für Zuweisung und Implementierung
- Konfigurationsaudits
- Konfiguration – Diff
- Offline-Management und -Scheduling
- Verwaltung von Firewall-Sicherheitsregeln
- Verwaltung von VPN-Sicherheitsregeln
- Verwaltung des SD-WAN
- Synchronisierung von Sicherheitsservices
- Hochverfügbarkeit
- Konfigurationsbackups
- RESTful-API
- Firmware-Upgrade für mehrere Geräte
- Rollenbasierte Administration
- Access-Point- und Switch-Management
- Intelligentes Plattform-Monitoring (IPM)[3]
- Zertifikatsverwaltung für mehrere Geräte

Monitoring[1,2]

- Gerätezustand und -status
- Lizenz- und Supportstatus
- Überblick über Netzwerk/Bedrohungen
- Alarm- und Benachrichtigungszentrale
- Ereignisprotokolle
- Topology View

Analytics[1,2]

- Benutzerbasierte Aktivitäten
- Anwendungsnutzung
- Produktübergreifende Transparenz mit Capture Client
- Dynamische Echtzeitvisualisierung
- Drill-down- und Pivoting-Funktionen

Reporting[1,2]

- Zeitgesteuerte PDF-Berichte auf Benutzer-, Gruppen- oder Geräteebene
- Personalisierbare Berichte
- Zentrales Logging
- Berichte zu verschiedenen Bedrohungen
- Berichte zu Benutzern
- Berichte zur Anwendungsnutzung
- Berichte zu Bandbreite und Services
- Reporting zur genutzten Bandbreite pro Benutzer
- Produktivitätsberichte

Sicherheit

- Unterstützung für geschlossene Netzwerke
- Kontosperrung
- Kontozugriffskontrolle
- 2FA-Unterstützung[3]
- Authentifizierungs-App mit 2FA-Unterstützung

Lizenzen und Pakete

Verwaltung			
Funktion	**NSM SaaS Essential**	**NSM SaaS Advanced**	**NSM On-Prem[2]**
Nutzer	Ja	Ja	Ja
Geräteinventar	Ja	Ja	Ja
Durchsetzung von Richtlinien auf Gruppenebene	Ja	Ja	Ja
Gerätegruppe	Ja	Ja	Ja
Vorlagen	Ja	Ja	Ja
Zuweisung und Implementierung (Workflow-Automatisierung)	Ja	Ja	Ja
Konfigurationsaudit	Ja	Ja	Ja
Konfiguration – Diff	Ja	Ja	Ja
Workflow-Automatisierung	Ja	Ja	Ja
API	Ja	Ja	Ja
Vollautomatische Implementierung	Ja	Ja	Ja
SD-WAN-Orchestrierung und -Monitoring	Ja	Ja	Ja
VPN-Orchestrierung und -Monitoring	Ja	Ja	Ja
Aufgabenplanung	Ja	Ja	Ja
Back-up/Wiederherstellung	Ja	Ja	Ja
Firmware-Upgrades	Ja	Ja	Ja
Access-Point- und Switch-Management	Ja	Ja	Ja
Erweiterte DNS-Filterung	Ja	Ja	Ja
Netzwerkzugriffskontrolle mit Aruba ClearPass	Ja	Ja	Ja
Reputationsbasiertes Content-Filtering	Ja	Ja	Ja

Lizenzen und Pakete (Fortsetzung)

Reporting			
Funktion	**NSM SaaS Essential**	**NSM SaaS Advanced**	**NSM On-Prem[2]**
Dashboard auf Gruppen-/ Nutzerebene	Ja	Ja	Nein
Capture ATP (Geräteebene)	Ja	Ja	Ja
Capture Threat Assessment (Geräteebene)	Ja	Ja	Ja
Produktivitätsberichte[5]	Nein	Ja	Nein
VPN-Berichte	Nein	Ja	Nein
Benutzerdefinierte Berichte	Ja	Ja	Nein
Zeitgesteuerte Berichte (Flow, CTA und Management)	Ja (außer Flow-Bericht)	Ja	Ja
Zeitraum der Berichtsdaten	7 Tage	365 Tage	365 Tage

Analysen			
Funktion	**NSM SaaS Essential**	**NSM SaaS Advanced**	**NSM On-Prem[2]**
Nutzerbasierte Analysen	Nein	Ja	Ja
Anwendungsanalysen	Nein	Ja	Ja
Forensische Netzwerkanalysen und Threat-Hunting mittels Drill-down und Pivoting	Nein	Ja	Ja
Cloud App Security – Aufspüren von Schatten-IT	Ja	Ja	Nein

Systemanforderungen

Internet-Browser

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

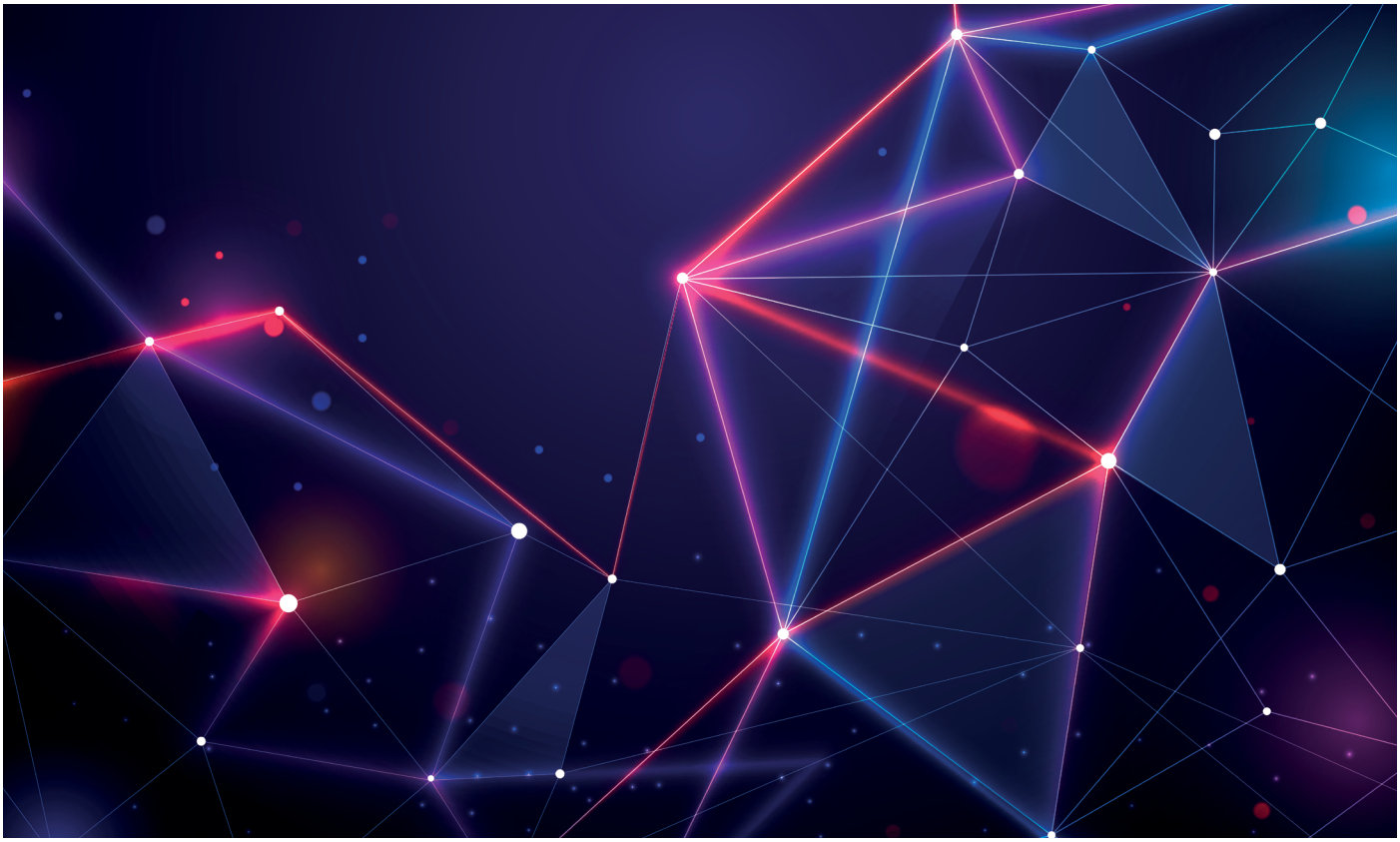
Systemanforderungen von NSM On-Prem

- Hypervisor: ESXi 7.0, 6.7 und Hyper-V 2016, 2019, KVM
- Public Cloud: Azure
- Mindestens erforderliche Rechenressourcen: 4 vCPUs, 24-GB-Arbeitsspeicher zur Verwaltung von 1 bis 500 Firewalls, 250-GB-Festplattenspeicher

Verwaltete Geräte

- NS*sp* 15700, NS*sp* 13700, NS*sp* 12000 Series[4], SuperMassive 9000 Series[4], NSA Series, NS*a* Series, TZ Series, SOHO-W, SOHO 250, SOHO 250W
- Appliances und Firmware der 5. Generation einschließlich nicht kabellosen SOHO-Geräten mit SonicOS 5.9 werden nicht unterstützt
- SonicWall Network Security Virtual Appliances: NS*v* Series
- SonicWall SonicWave[6], SonicPoint
- SonicWave-Unterstützung umfasst Wi-Fi-6-fähige Access-Points
- SonicWall Switch

[1] NSM SaaS enthält Reporting- und Analyse-Features.
[2] NSM On-Prem erfordert eine separate Installation von SonicWall Analytics On-Prem sowie eine Lizenz für die Reporting- und Analyse-Features.
[3] Nur mit NSM On-Prem verfügbar.
[4] 365 Tage Reporting und 30 Tage Analytics werden nicht unterstützt.
[5] Erfordert eine aktivierte AGSS-/CGSS-Lizenz auf Firewalls der Generation 6/6.5 sowie eine Essential-Protection-Lizenz auf Firewalls der Generation 7.
[6] SonicWave-Unterstützung umfasst Wi-Fi-6-fähige Access-Points



Implementierung und Verwaltung aller Firewalls, vernetzten Switches und Access-Points über eine einzige benutzerfreundliche Oberfläche.

www.sonicwall.com/nsm

Über SonicWall

SonicWall bietet grenzenlose Cybersicherheit für eine extrem dezentrale Arbeitswelt, in der jeder remote, mobil und potenziell gefährdet ist. Durch die Identifizierung unbekannter Bedrohungen, moderne Echtzeit-Überwachungsfunktionen und eine herausragende Wirtschaftlichkeit hilft SonicWall großen Unternehmen, Behörden und KMUs weltweit, die Cybersicherheitslücke zu schließen. Weitere Informationen erhalten Sie unter www.sonicwall.de.

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

SONICWALL

Datasheet-NSM-A4-JK-10177