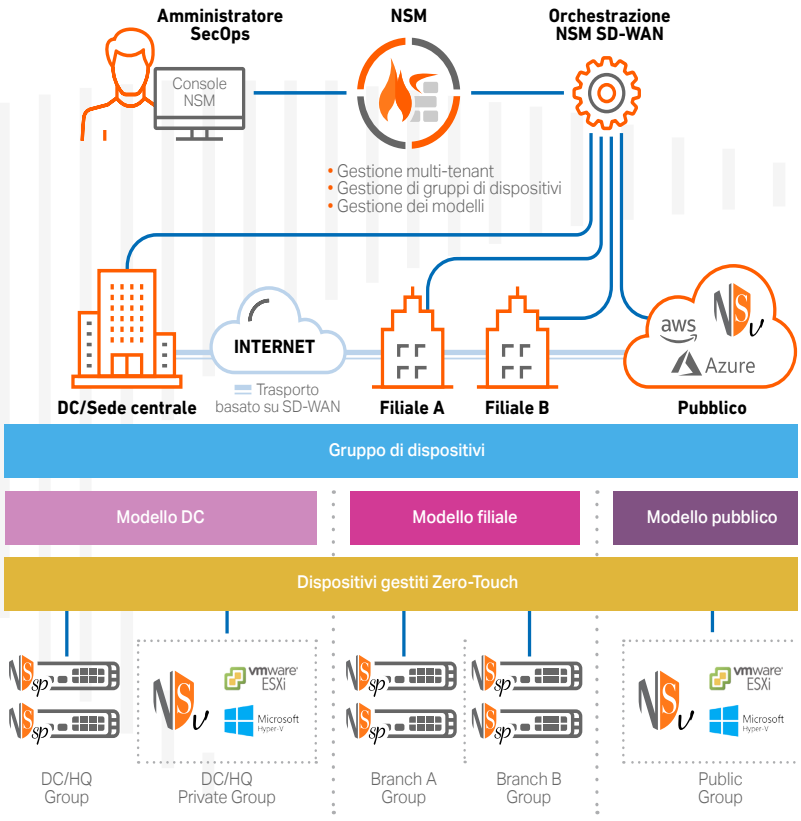
SONICWALL

Network Security Manager

Sistema unificato e scalabile di gestione firewall per qualsiasi ambiente

Che si tratti di proteggere una piccola attività, un'impresa distribuita, più attività o una rete chiusa, la sicurezza di rete può trovarsi sopraffatta da disordini operativi, rischi occulti ed esigenze normative. Storicamente, le prassi di gestione efficiente dei firewall si basano principalmente su sistemi affidabili e misure di controllo operativo. Tuttavia, errori frequenti, configurazioni errate e forse anche violazioni di tali controlli continuano ad essere sfide costanti per i Security Operation Center (SOC) ben gestiti.



CARATTERISTICHE PRINCIPALI

Business

- Riduzione dei costi di gestione della sicurezza
- Conoscenza del panorama delle minacce e della situazione di sicurezza
- Migliore efficienza dell'organizzazione IT e minor rischio di burnout per gli amministratori
- Prevenzione di costose interruzioni dell'operatività e incidenti di sicurezza

Operatività

- Eliminazione dei silos di gestione dei firewall
- Facile integrazione di qualsiasi numero di firewall in remoto
- Risposta rapida a problemi di sistema critici per garantire prestazioni ottimali della rete
- Definizione di configurazioni e policy coerenti per tutti i dispositivi gestiti
- Rapida implementazione di reti SD-WAN

Sicurezza

- Verifica, attuazione e messa in pratica di policy di sicurezza coerenti in tutti gli ambienti
- Definizione di configurazioni SD-WAN coerenti in tutti i siti
- Rilevamento delle minacce e reazione rapida a rischi e problematiche
- Monitoraggio e tracciamento dei risultati degli interventi di policy con maggiore chiarezza
- Prevenzione dell'autenticazione non autorizzata degli utenti, comprese le minacce interne

Gestione centralizzata. Sicurezza migliorata.

www.sonicwall.com/nsm

SCHEDA TECNICA

SonicWall Network Security Manager (NSM), un sistema centralizzato di gestione firewall multi-tenant, consente di gestire centralmente tutte le operazioni dei firewall, senza errori, applicando workflow verificabili. Reporting e Analytics[1,2] offrono visibilità da un unico pannello di gestione e consentono di monitorare e scoprire le minacce unificando e correlando i log su tutti i firewall. NSM contribuisce inoltre a mantenere la conformità grazie all'applicazione uniforme delle policy a tutti i firewall e tramite audit trail dettagliati per ogni modifica della configurazione e report granulari. La soluzione è scalabile per aziende di qualsiasi dimensione che gestiscono reti con centinaia di dispositivi firewall distribuiti in vari tenant o più sedi. NSM fa tutto con meno fatica e in meno tempo.

Mantenere il controllo: coordinazione delle operazioni dei firewall da un'unica posizione

NSM offre tutto il necessario per ottenere un sistema unificato di gestione dei firewall. Offre visibilità a livello dei tenant, controllo dei dispositivi in base a gruppi e scalabilità illimitata per configurare e gestire centralmente le attività di sicurezza della rete SonicWall. Tali attività includono l'implementazione e la gestione di tutti i dispositivi firewall, tutti i gruppi di dispositivi e tutti i tenant, la sincronizzazione e l'applicazione di policy di sicurezza coerenti (tra cui DNS e filtraggio dei contenuti) negli ambienti con controlli locali flessibili e il monitoraggio di ogni aspetto da una dashboard dinamica con report e analisi dettagliate. NSM consente anche il controllo degli accessi alla rete tramite l'integrazione di Aruba ClearPass. Inoltre, NSM consente di gestire il tutto da un'unica console facile da utilizzare e accessibile da ogni postazione con qualsiasi dispositivo dotato di browser.

Gestione multi-tenant

A mano a mano che l'ambiente firewall cresce, sorge la necessità di un sistema di gestione dei firewall che sia scalabile insieme all'ambiente. NSM offre un sistema di gestione multi-tenant completo e il controllo isolato di policy indipendenti per tutti i tenant gestiti. Questa separazione riguarda tutte le funzionalità gestionali di NSM, che determinano il funzionamento del firewall per ciascun tenant. È possibile configurare ogni tenant con il proprio insieme di utenti, gruppi e ruoli per eseguire la gestione dei gruppi di dispositivi, l'orchestrazione delle policy e tutte le altre attività amministrative entro i limiti dell'account assegnato al tenant.

Gestione di gruppi di dispositivi

Device Group offre un metodo efficace per creare e gestire dispositivi firewall sotto forma di gruppi o raggruppamenti gerarchici e per attuare e implementare modelli di configurazione su gruppi di firewall. In questo modo è possibile sincronizzare e applicare policy, oggetti e requisiti di impostazione sui vari gruppi di firewall selezionati in modo coerente e affidabile. Tutte le modifiche alle policy approvate nel modello vengono applicate automaticamente a tutti i gruppi di dispositivi collegati a quel modello. Il raggruppamento di dispositivi può essere stabilito in modo granulare in base a qualsiasi caratteristica, come tipo di rete, posizione, unità aziendale, struttura organizzativa o una combinazione di tali attributi, per facilitare la gestione, l'identificazione e l'associazione.

Gestione, attuazione e implementazione di modelli

I flussi di lavoro semplificati di NSM consentono di progettare, convalidare, verificare, approvare e implementare facilmente e rapidamente i modelli di configurazione per la gestione di uno o di centinaia di dispositivi firewall in molte posizioni geografiche. I modelli con varie policy firewall, impostazioni e oggetti correlati sono stabiliti indipendentemente dal dispositivo e vengono utilizzati da NSM per l'invio centralizzato e automatico a dispositivi o gruppi di dispositivi che richiedono configurazioni simili.

I modelli combinati con le rispettive variabili consentono di implementare e gestire centralmente centinaia di firewall remoti, nonché di stabilire una configurazione coerente preservando valori univoci e specifici per ciascun dispositivo, come IP di interfaccia, configurazione DNS, nome host del firewall ecc. Le aziende distribuite possono facilmente integrare e proteggere nuove filiali e siti remoti utilizzando un unico modello, senza bisogno di configurazioni manuali e separate per ciascun dispositivo in ciascuna posizione.

Orchestrazione e monitoraggio SD-WAN

NSM semplifica l'implementazione di reti SD-WAN a livello dell'intera azienda tramite un workflow intuitivo e autoguidato. Inoltre stabilisce e applica centralmente il traffico basato sulle applicazioni e altre configurazioni di gestione del traffico tra centinaia di siti, come filiali e negozi

al dettaglio. NSM consente anche di monitorare lo stato e le prestazioni dell'intero ambiente SD-WAN al fine di garantire configurazioni coerenti, ottenere prestazioni ottimali delle applicazioni e consentire ai team dell'infrastruttura di rete di individuare e risolvere rapidamente i problemi.

Orchestrazione e monitoraggio VPN

NSM semplifica le configurazioni e le policy VPN con un processo di installazione passo-passo basato su procedure guidate, consentendo quindi agli amministratori di sistema di stabilire la connettività e le comunicazioni tra un sito e l'altro in modo rapido e senza errori utilizzando un workflow autoguidato e ripetibile. Inoltre, il monitoraggio VPN aiuta a mantenere il polso della situazione delle VPN utilizzate, offrendo una visibilità completa su attività, stato e prestazioni dell'intero ambiente VPN. Gli amministratori di rete possono sfruttare queste informazioni per monitorare lo stato della connessione, i dati trasferiti e la larghezza di banda consumata sui tunnel VPN interessati. Gli avvisi consentono agli amministratori di mantenere l'integrità delle connessioni VPN in modo proattivo, garantendo quindi una connettività continua tra i siti.

Maggiore efficacia: lavorare in modo più intelligente con interventi di sicurezza più veloci e meno impegnativi

NSM è uno strumento di gestione della produttività che consente di lavorare in modo più intelligente e attuare interventi di sicurezza più veloci e meno impegnativi. La sua struttura si basa su processi aziendali, sul principio della semplificazione e, in alcuni casi, sull'automazione dei flussi di lavoro per migliorare il coordinamento della sicurezza. Inoltre aiuta a ridurre la complessità, il tempo e i sovraccarichi nell'esecuzione delle operazioni quotidiane di sicurezza e delle attività amministrative.

Implementazione Zero-Touch semplificata

NSM integra il servizio di implementazione completamente automatizzata Zero-Touch, che consente di implementare e rendere operativi firewall, switch e access point SonicWall in sedi remote e filiali con grande facilità. L'intero processo richiede un intervento minimo da parte dell'utente ed è completamente automatizzato. I dispositivi abilitati all'implementazione "zero-touch" vengono spediti direttamente ai siti di installazione. Una volta registrati e collegati alla rete, tutti i dispositivi connessi sono immediatamente operativi, con sicurezza e connettività perfettamente funzionanti. I modelli predisposti per i dispositivi vengono inviati automaticamente a tutti i dispositivi connessi una volta che vengono stabiliti i collegamenti di comunicazione con NSM. Tutto questo elimina i tempi, i costi e la complessità dei tradizionali processi di onboarding in loco.

Gestione delle modifiche senza errori

NSM consente l'accesso immediato a potenti workflow automatizzati, conformi ai requisiti di controllo e gestione delle modifiche alle policy firewall dei SOC. Inoltre permette di modificare le policy senza errori applicando una serie di procedure rigorose che comprendono il confronto, la convalida e l'autorizzazione delle configurazioni prima dell'implementazione. I gruppi di approvazione sono flessibili per essere conformi alle procedure di audit interne di vari team funzionali. NSM consente di migliorare l'efficienza operativa, ridurre i rischi ed eliminare configurazioni errate con il processo di workflow con approvazione obbligatoria.

Automazione della gestione con API RESTful

Le API RESTful di NSM consentono agli operatori di sicurezza più esperti di utilizzare un approccio standard alla gestione delle funzionalità specifiche di NSM in modo programmatico senza un'interfaccia di gestione Web. Questo facilita l'interoperabilità tra NSM e le console di gestione di terze parti, aumentando l'efficienza del team di sicurezza interno. I servizi API possono automatizzare le operazioni del firewall per qualsiasi dispositivo gestito e comprendono tipiche attività quotidiane come la gestione di gruppi di dispositivi e tenant, configurazioni di audit, l'esecuzione di controlli di integrità del sistema e altro ancora.

Maggiore consapevolezza: indagini sui rischi nascosti con monitoraggio, analisi e report attivi[1,2]

La dashboard interattiva di NSM offre funzioni di monitoraggio, report e dati di analisi in tempo reale. Queste informazioni aiutano a risolvere i problemi, indagare sui rischi e adottare policy di sicurezza intelligenti per un approccio di sicurezza più adattivo.

Gli amministratori possono agire in modo rapido e preciso con avvisi in tempo reale per garantire un'operatività ottimale, aiutando le aziende a evitare costose interruzioni dell'operatività e incidenti di sicurezza.

Visibilità su ogni risorsa, ovunque sia

NSM, in combinazione con Analytics,[1,2] offre fino a 7 giorni di visibilità continua sull'intero ecosistema di sicurezza SonicWall a livello di tenant, gruppo o dispositivo. Inoltre fornisce analisi statiche, quasi in tempo reale, di tutto il traffico di rete e delle comunicazioni di dati che attraversano l'ecosistema firewall. Tutti i dati del log vengono automaticamente registrati, aggregati, contestualizzati e presentati in maniera significativa, utilizzabile e facilmente fruibile. È quindi possibile eseguire operazioni di rilevamento e interpretazione, assegnare priorità e adottare azioni difensive e correttive adeguate utilizzando informazioni basate sui dati e con consapevolezza della situazione. I report programmati possono essere personalizzati con qualsiasi combinazione di dati sul traffico e offrono fino a

365 giorni di log registrati a livello di dispositivo, gruppo di dispositivi o tenant per analisi cronologiche, rilevamento di anomalie, individuazione delle falle di sicurezza e altro ancora. Tutto questo facilita il monitoraggio, la misurazione e l'attuazione di efficaci operazioni di rete e sicurezza.

Comprendere l'esposizione al rischio

Con l'aggiunta di funzionalità di drill-down e pivoting è possibile indagare più a fondo e correlare i dati per esaminare e scoprire minacce e problemi nascosti con maggiore precisione e sicurezza. Utilizzando una combinazione di report storici, analisi basate su utenti e applicazioni e visibilità sugli endpoint, è possibile analizzare in modo approfondito vari modelli e tendenze correlati al traffico in ingresso/uscita, l'uso delle applicazioni, l'accesso di utenti e dispositivi, azioni sulle minacce e altro ancora. Il tutto permette di acquisire consapevolezza della situazione e preziose informazioni e nozioni non soltanto per scoprire i rischi per la sicurezza, ma anche per orchestrare i rimedi durante il monitoraggio e il tracciamento dei risultati per promuovere un'applicazione coerente della sicurezza in tutto l'ambiente.

Ottimizzazione della produttività della forza lavoro

User Analytics[1,2] offre una visione ampia e trasparente delle applicazioni Web e delle attività di utilizzo di Internet della forza lavoro. Le funzionalità di drill-down consentono agli analisti di esaminare e analizzare in modo semplice e rapido i punti di interesse dei dati a livello di utente e di stabilire misure basate su policy comprovate per utenti e applicazioni rischiose nel momento in cui vengono rilevate. Inoltre, Productivity Reports[1,2] fornisce informazioni sull'utilizzo di Internet e sul comportamento dei dipendenti in un periodo specificato. Lo strumento genera istantanee accurate e report dettagliati che classificano le attività Web degli utenti per gruppi di produttività, come ad esempio gruppi produttivi, non produttivi, accettabili, non accettabili o definiti dall'utente, aiutando le organizzazioni a comprendere e controllare meglio l'utilizzo di Internet.

Implementazione flessibile

I clienti possono implementare NSM in vari modi per soddisfare al meglio i propri requisiti operativi, normativi e di budget.

NSM è disponibile come servizio SaaS gestito in hosting da SonicWall, accessibile tramite Internet e senza necessità di manutenzione. NSM SaaS offre una scalabilità su richiesta, riducendo i costi operativi. Non occorre installare hardware o software, programmare la manutenzione, personalizzare il software, eseguire configurazioni o aggiornamenti, tenere conto di tempi di inattività, ammortamento e costi di ritiro. Tutte queste spese vengono eliminate e sostituite da un abbonamento annuale dal costo basso e prevedibile.

Per avere totale controllo e conformità del sistema, è possibile implementare NSM nel cloud pubblico di Microsoft Azure o come appliance virtuale in un cloud privato su VMWare, Microsoft Hyper-V o KVM, che offrono tutti i vantaggi operativi ed economici della virtualizzazione, tra cui scalabilità e agilità del sistema, velocità di provisioning del sistema, semplicità di gestione e riduzione dei costi.

Funzionalità di sicurezza

Le aziende statali, pubbliche, sanitarie, farmaceutiche e di altro tipo spesso implementano reti chiuse per mantenere la privacy e l'isolamento delle loro applicazioni mission-critical e dei sistemi informatici più sensibili, come i sistemi per documentazione riservata, SCADA e strutture di ricerca. NSM supporta gli ambienti di rete chiusi e offre agli amministratori un metodo per eseguire offline le operazioni di onboarding, gestione delle licenze, applicazione di patch e aggiornamenti del sistema NSM e dei firewall, il tutto sotto la sua gestione e senza dover contattare il SonicWall License Manager o MySonicWall.

Per una maggiore sicurezza, NSM applica diverse misure di controllo dell'accesso agli account per impedire l'accesso non autorizzato all'interfaccia di gestione di NSM. Inoltre concede controlli amministrativi specifici in base ai ruoli dell'utente e attiva il blocco degli account in base a un numero specificato di tentativi di accesso non riusciti. Inoltre, l'accesso degli utenti è consentito solo quando si accede da un elenco specificato di indirizzi IP di origine autorizzati ed è protetto dall'autenticazione a due fattori (2FA)[3].

Riepilogo delle funzionalità

Gestione

- Network Access Control (NAC) con Aruba Clearpass
- Gestione a livello di tenant e gruppi di dispositivi
- Modelli di configurazione
- Raggruppamento di dispositivi
- Conversione da configurazione del dispositivo a modello
- Procedura guidata di implementazione
- Verifiche della configurazione
- Riepilogo modifiche alla configurazione (Config Diff)
- Gestione e pianificazione offline
- Gestione delle policy di sicurezza dei firewall
- Gestione delle policy di sicurezza VPN
- Amministrazione della SD-WAN
- Sincronizzazione dei servizi di sicurezza
- Alta disponibilità
- Backup della configurazione
- API RESTful
- Aggiornamento firmware multi-dispositivo
- Amministrazione basata sui ruoli
- Gestione di access point e switch
- Intelligent Platform Monitoring (IPM)[3]
- Gestione dei certificati multi-dispositivo

Monitoraggio[1,2]

- Integrità e stato dei dispositivi
- Stato delle licenze e del supporto
- Riepilogo rete/minacce
- Centro avvisi e notifiche
- Log degli eventi
- Visualizzazione della topologia

Analisi[1,2]

- Attività basate sull'utente
- Utilizzo delle applicazioni
- Visibilità su più prodotti con Capture Client
- Visualizzazione dinamica in tempo reale
- Funzionalità di drill-down e pivoting

Reporting[1,2]

- Report PDF programmati - Livello tenant/gruppo/dispositivo
- Report personalizzabili
- Sistema di logging centralizzato
- Report su minacce multiple
- Report basati sugli utenti
- Report sull'utilizzo delle applicazioni
- Report su larghezza di banda e servizi
- Report sulla larghezza di banda per utente
- Report sulla produttività

Sicurezza

- Supporto per reti chiuse
- Blocco degli account
- Controllo dell'accesso agli account
- Supporto 2FA[3]
- Supporto TFA dell'app di autenticazione

Licenze e pacchetti

Gestione

Funzionalità	NSM SaaS Essential	NSM SaaS Advanced	NSM On-Prem[2]
Tenant	Sì	Sì	Sì
Inventario dispositivi	Sì	Sì	Sì
Policy di invio a livello di gruppo	Sì	Sì	Sì
Gruppo di dispositivi	Sì	Sì	Sì
Modelli	Sì	Sì	Sì
Attuazione e implementazione (automazione del workflow)	Sì	Sì	Sì
Verifica della configurazione	Sì	Sì	Sì
Config Diff	Sì	Sì	Sì
Automazione dei flussi di lavoro	Sì	Sì	Sì
API	Sì	Sì	Sì
Implementazione Zero-Touch	Sì	Sì	Sì
Orchestrazione e monitoraggio SD-WAN	Sì	Sì	Sì
Orchestrazione e monitoraggio VPN	Sì	Sì	Sì
Pianificazione attività	Sì	Sì	Sì
Backup/ripristino	Sì	Sì	Sì
Aggiornamenti del firmware	Sì	Sì	Sì
Gestione di access point e switch	Sì	Sì	Sì
Filtraggio DNS avanzato	Sì	Sì	Sì
Network Access Control con Aruba Clearpass	Sì	Sì	Sì
Filtraggio dei contenuti basato sulla reputazione	Sì	Sì	Sì

Licenze e pacchetti, continua

Reporting			
Funzionalità	**NSM SaaS Essential**	**NSM SaaS Advanced**	**NSM On-Prem[2]**
Dashboard a livello di gruppo/tenant	Sì	Sì	No
Capture ATP (a livello di dispositivo)	Sì	Sì	Sì
Capture Threat Assessment (a livello di dispositivo)	Sì	Sì	Sì
Report sulla produttività[5]	No	Sì	No
Report VPN	No	Sì	No
Report personalizzati	Sì	Sì	No
Report pianificati (flusso, CTA e gestione)	Sì (tranne report di flusso)	Sì	Sì
Giorni di report dei dati	7 giorni	365 giorni	365 giorni

Analisi			
Funzionalità	**NSM SaaS Essential**	**NSM SaaS Advanced**	**NSM On-Prem[2]**
Analisi basate sull'utente	No	Sì	Sì
Analisi delle applicazioni	No	Sì	Sì
Analisi forensi della rete e ricerca minacce con drill-down e pivoting	No	Sì	Sì
Cloud App Security – Rilevamento di shadow IT	Sì	Sì	No

Requisiti di sistema

Browser

- Microsoft® Internet Explorer 11.0 o versioni successive e la versione più recente di Microsoft Edge, Mozilla Firefox, Google Chrome e Safari

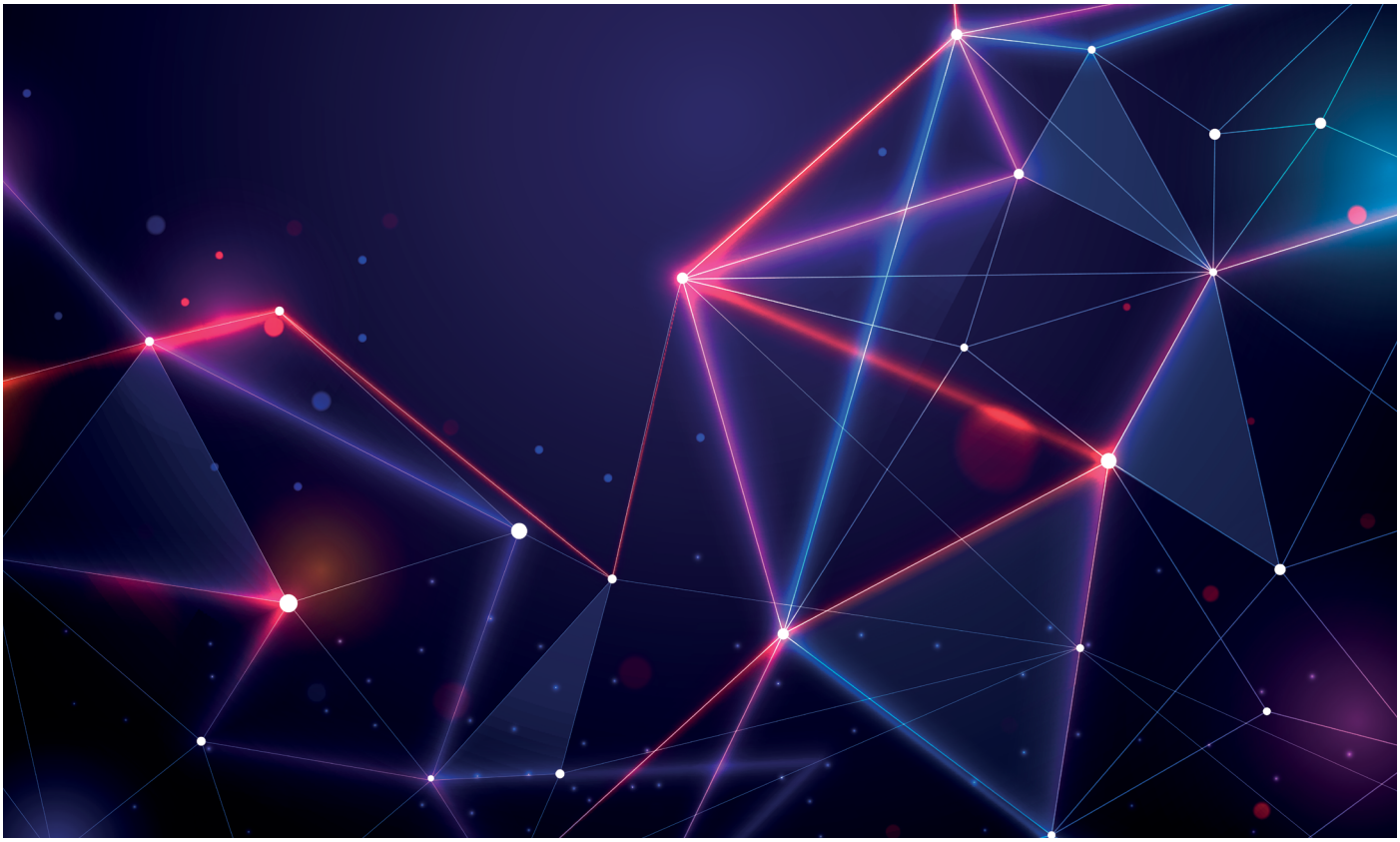
Requisiti di sistema NSM On-Prem

- Hypervisor: ESXi 7.0, 6.7 e Hyper-V 2016, 2019, KVM
- Cloud pubblico: Azure
- Risorse di calcolo minime: 4 vCPU, 24 GB di memoria per la gestione di 1-500 firewall, 250 GB di spazio di archiviazione

Dispositivi gestiti

- Serie NS*sp* 15700, NS*sp* 13700, NS*sp* 12000[4], serie SuperMassive 9000[4], serie NSA, serie NS*a*, serie TZ, SOHO-W, SOHO 250, SOHO 250W
- I dispositivi e il firmware di 5ª generazione, inclusi i dispositivi SOHO non wireless con SonicOS 5.9, non sono supportati.
- Appliance di sicurezza di rete SonicWall virtuali: Serie NS*v*
- SonicWall SonicWave[6], SonicPoint
- Il supporto per SonicWave include access point abilitati al Wi-Fi6
- SonicWall Switch

[1] NSM SaaS comprende funzionalità di reporting e analisi.
[2] NSM On-Prem richiede un'installazione e una licenza separate di SonicWall Analytics On-Prem per le funzioni di reporting e analisi.
[3] Disponibile solo su NSM On-Prem.
[4] 365 giorni di reporting e 30 giorni di analisi non supportati.
[5] Richiede la licenza AGSS/CGSS attivata sui firewall di generazione 6/6.5, la licenza Essential Protection sui firewall di generazione 7
[6] Il supporto per SonicWave include access point abilitati al Wi-Fi6



Implementazione e gestione di tutti i firewall, switch e access point collegati, il tutto in un'unica interfaccia di facile utilizzo.

www.sonicwall.com/nsm

SonicWall

SonicWall fornisce soluzioni di cybersecurity innovative per la nuova normalità iperdistribuita, in una realtà lavorativa in cui tutto è all'insegna del telelavoro, della mobilità e in cui la sicurezza dei dati rappresenta un elemento fondamentale. Con la sua capacità di individuare le minacce più elusive e offrendo una visibilità in tempo reale, SonicWall rende possibili economie innovative e colma le lacune della cybersecurity per aziende, enti pubblici e PMI in ogni parte del mondo. Per maggiori informazioni visitare www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Per maggiori informazioni consultare il nostro sito web.
www.sonicwall.com

SONICWALL

© 2023 SonicWall Inc. TUTTI I DIRITTI RISERVATI.
SonicWall è un marchio o marchio registrato di SonicWall Inc. e/o delle sue affiliate negli Stati Uniti e/o in altri Paesi. Tutti gli altri marchi e marchi registrati appartengono ai rispettivi proprietari. Le informazioni contenute nel presente documento si riferiscono ai prodotti di SonicWall Inc. e/o delle sue affiliate. Né il presente documento né la vendita di prodotti SonicWall costituiscono alcuna licenza, espressa o implicita, di estoppel o di altro tipo, né garantiscono diritti di proprietà intellettuale. Salvo quanto specificato nei termini e nelle condizioni stabiliti nel contratto di licenza di questo prodotto, SonicWall e/o le sue affiliate non si assumono alcuna responsabilità ed escludono garanzie di qualsiasi tipo, esplicite, implicite o legali, in relazione ai propri prodotti, incluse, in via esemplificativa, qualsiasi garanzia implicita di commerciabilità, idoneità a scopi specifici o violazione di diritti altrui. SonicWall e/o le sue affiliate declinano ogni responsabilità per danni di qualunque tipo, siano essi diretti, indiretti, consequenziali, punitivi, speciali o incidentali (inclusi, senza limitazioni, danni per mancato guadagno, interruzioni dell'attività o perdite di dati) derivanti dall'utilizzo o dall'impossibilità di utilizzare il presente documento, anche nel caso in cui SonicWall e/o le sue affiliate siano state avvertite dell'eventualità di tali danni. SonicWall e/o le sue affiliate non rilasciano alcuna garanzia o dichiarazione relativamente alla precisione o completezza dei contenuti del presente documento e si riservano il diritto di apportare modifiche, in qualsiasi momento e senza preavviso, alle specifiche e alle descrizioni dei prodotti. SonicWall Inc. e/o le sue affiliate non si assumono alcun impegno di aggiornare le informazioni contenute in questo documento.

Datasheet-NSM-A4-JK-10177