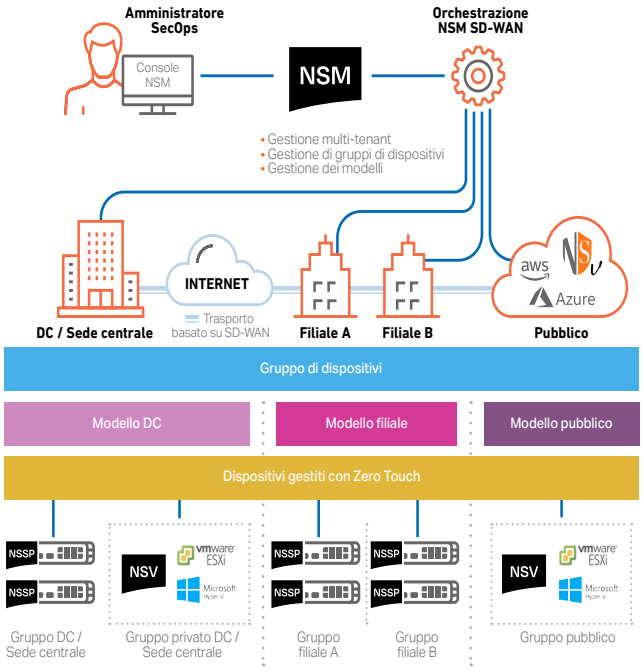
SONICWALL

Network Security Manager On-Premise

Pieno controllo sulla sicurezza e sulla conformità

Che si tratti di proteggere una piccola attività, un'impresa distribuita, diverse aziende o una rete chiusa, la sicurezza di rete può essere messa a dura prova da complessità operative, rischi nascosti e requisiti normativi. Storicamente, una gestione efficiente dei firewall si basa principalmente su sistemi affidabili e misure di controllo operativo. Tuttavia, errori frequenti, configurazioni errate e forse anche violazioni di tali controlli continuano a essere sfide costanti per i Security Operation Center (SOC) ben gestiti.



CARATTERISTICHE PRINCIPALI

Aziendali

- Gestione semplificata della sicurezza
- Conoscenza del panorama delle minacce e della postura di sicurezza
- Migliore efficienza del reparto 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
- 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

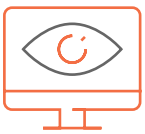
- Verifica, registrazione e applicazione di policy di sicurezza coerenti in tutti gli ambienti
- Definizione di configurazioni SD-WAN coerenti in tutti i siti
- Ricerca delle minacce e reazione rapida a rischi e problematiche
- Monitoraggio e tracciamento dei risultati degli interventi di policy con maggiore chiarezza
- Prevenzione di autenticazioni non autorizzate 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 garantire la conformità mediante l'applicazione coerente delle policy in tutti i firewall, fornendo registri di controllo 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 (incluso il filtraggio DNS e dei contenuti) in tutti gli ambienti con controlli locali flessibili e il monitoraggio di ogni attività da una dashboard dinamica con report e analisi dettagliate. Inoltre, NSM consente di gestire tutte queste funzionalità 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 in funzione dell'ambiente. NSM offre la gestione multi-tenant completa e l'isolamento di policy indipendenti per tutti i tenant gestiti. NSM consente di applicare modifiche alla configurazione per tutti i tenant, migliorando l'efficienza operativa degli MSP/MSSP. 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 registrare e implementare modelli di configurazione su gruppi di firewall. In questo modo è possibile sincronizzare e applicare policy e oggetti e impostare requisiti per qualsiasi gruppo 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 dei 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 le attività di gestione, identificazione e associazione.

Gestione, registrazione 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 vengono definiti indipendentemente dai dispositivi. NSM utilizza questi modelli 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 nell'intera azienda tramite un workflow intuitivo e autoguidato. Inoltre stabilisce e applica centralmente le configurazioni per l'indirizzamento del traffico basato sulle applicazioni e del traffico di altro tipo 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 per 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 della VPN con un processo guidato di installazione passo-passo, consentendo agli amministratori di sistema di stabilire la connettività e le comunicazioni tra un sito e l'altro in modo rapido e senza errori tramite un workflow autoguidato e ripetibile. Inoltre, il monitoraggio VPN consente di tenere costantemente sotto controllo le VPN utilizzate, offrendo una visibilità completa su attività, stato e prestazioni dell'intero ambiente VPN. Gli amministratori di rete possono utilizzare 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 l'impegno dedicati ogni giorno alle operazioni di sicurezza e alle attività amministrative.

Implementazione Zero Touch semplificata

NSM integra il servizio di implementazione completamente automatizzata Zero Touch, che consente di distribuire 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 con funzionalità Zero Touch vengono spediti direttamente ai siti di installazione. Una volta registrati e collegati alla rete, tutti i dispositivi connessi sono immediatamente operativi, con funzionalità di sicurezza e connettività perfettamente funzionanti. I template predisposti per i dispositivi vengono inviati automaticamente a tutti i dispositivi connessi una volta che vengono stabiliti i collegamenti di comunicazione con NSM. Tutto ciò 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 mediante 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 garantire la conformità alle procedure di controllo interne di vari team funzionali. NSM consente di migliorare l'efficienza operativa, ridurre i rischi ed evitare configurazioni errate attraverso il processo di 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 interno addetto alla sicurezza. 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, la configurazione delle verifiche, 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 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. Grazie agli avvisi in tempo reale, gli amministratori possono agire in modo rapido e preciso per garantire un'operatività ottimale, aiutando le aziende a evitare costose interruzioni dell'operatività e incidenti di sicurezza.

Vedere ogni cosa ovunque

NSM con Reporting e Analytics[1,2] offre, a seconda del tipo di licenza, fino a 365 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. In questo modo è 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 con analisi cronologiche, rilevamento di anomalie, individuazione delle falle di sicurezza e altro ancora. Tutto questo facilita il monitoraggio, la misurazione e l'attuazione di operazioni di rete e sicurezza efficaci.

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 relativi al traffico in ingresso/uscita, all'uso delle applicazioni, all'accesso di utenti e dispositivi, azioni sulle minacce e altro ancora. Queste funzionalità consentono di acquisire consapevolezza della situazione, informazioni preziose e conoscenze per scoprire i rischi di sicurezza e per orchestrare i rimedi, oltre a monitorare e tracciare i risultati per favorire un'applicazione coerente della sicurezza in tutto l'ambiente.

Ottimizzare la 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 a rischio 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. Genera istantanee accurate e report dettagliati che classificano le attività web degli utenti in gruppi di produttività, come ad esempio gruppi produttivi, non produttivi, accettabili, non accettabili o personalizzati, aiutando le organizzazioni a comprendere e controllare meglio l'uso di Internet.

Implementazione flessibile

Per garantire il totale controllo e conformità del sistema, è possibile implementare NSM On-Premises nel cloud pubblico di Microsoft Azure o come appliance virtuale in un cloud privato su VMWare, Microsoft Hyper-V o KVM. Queste opzioni di implementazione 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 garantire 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 ricorrere a 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. L'accesso degli utenti è consentito solo quando il login avviene da un elenco selezionato di indirizzi IP di origine autorizzati ed è protetto dall'autenticazione a due fattori (2FA).

Cloud Secure Edge

Cloud Secure Edge (CSE) di SonicWall è una soluzione di sicurezza basata sul cloud che offre l'accesso sicuro ad applicazioni e dati per lavoratori remoti e ibridi. Con l'integrazione di Cloud Secure Edge Connector, gli utenti di NSM possono accedere alla nostra tecnologia Cloud Secure Edge, che offre un accesso privato sicuro agli utenti remoti con funzionalità Zero Trust. Cloud Secure Edge integra gateway web sicuri, accesso alla rete Zero Trust e protezione dalle minacce avanzate per proteggere utenti e dispositivi indipendentemente dalla loro posizione. A partire da SonicOS 7.1.2, qualsiasi organizzazione può utilizzare Cloud Secure Edge Connector per stabilire una connessione ai cluster Internet e cloud ospitati da risorse aziendali. Il connettore stabilisce poi dei tunnel sicuri per i vari livelli di accesso della rete edge globale.

Licenze e pacchetti

Licenze	
Funzionalità	**Advanced Protection**
Report di base per 7 giorni (riepilogativo) - Solo con SaaS	
Reportistica avanzata	7 giorni
Analisi avanzata	7 giorni

Gestione	
Funzionalità	**NSM On-Premise – Gestione**
Tenant	✓
Inventario dispositivi	✓
Invio di policy a livello di gruppo	✓
Gruppo di dispositivi	✓
Modelli	✓
Registrazione e implementazione (automazione dei flussi di lavoro)	✓
Verifica della configurazione	✓
Riepilogo modifiche alla configurazione (Config Diff)	✓
Sincronizzazione automatica delle configurazioni	✓
Automazione dei flussi di lavoro	✓
API	✓
Implementazione Zero Touch	✓
Orchestrazione e monitoraggio SD-WAN	✓
Orchestrazione e monitoraggio VPN	✓
Pianificazione delle attività	✓
Backup/ripristino	✓
Aggiornamenti del firmware	✓
Gestione di access point e switch dal firewall	✓
Filtraggio DNS avanzato*	✓
Controllo accessi alla rete	✓
Filtraggio dei contenuti basato sulla reputazione*	✓
Integrazione con Cloud Secure Edge Connector	✓
Applicazione per la migrazione dei firewall	✓
Gestione con un semplice clic	✓
Vista dei firewall offline	✓

*Richiede la licenza base di NSM On-Premise per aggiungere la licenza di reportistica e analisi

SONICWALL®

Licenze e pacchetti, continua

Reportistica	
Funzionalità	**NSM On-Premise – Analisi e report avanzati per 7 e 365 giorni[2]**
Dashboard a livello di gruppo/tenant	✓
Capture ATP (a livello di dispositivo)	✓
Capture Threat Assessment (a livello di dispositivo)	✓
Report sulla produttività[4]	✓
Report VPN	✓
Report personalizzati	✓
Programmazione dei report	✓
(flusso, CTA e gestione)	✓
Report di riepilogo dell'attività dei firewall	✓
Report sugli attacchi	✓

Analisi	
Funzionalità	**NSM On-Premise – Analisi e report avanzati per 7 e 365 giorni[2]**
Analisi basate sugli utenti	✓
Analisi delle applicazioni	✓
Analisi forensi della rete e ricerca minacce con drill-down e pivoting	✓

Riepilogo delle funzionalità

Gestione

- Integrazione con Cloud Secure Edge Connector
- Network Access Control (NAC)
- Gestione a livello di tenant e gruppi di dispositivi
- Modelli di configurazione
- Raggruppamento di dispositivi
- Conversione della configurazione di un dispositivo in un modello
- Procedura guidata di implementazione
- Funzionalità di migrazione dei firewall
- 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
- Aggiornamenti automatici del firmware
- Amministrazione basata sui ruoli

Monitoraggio[1,2]

- Integrità e stato dei dispositivi
- Stato delle licenze e del supporto
- Riepilogo rete/minacce
- Centro avvisi e notifiche
- Monitoraggio dei dispositivi offline
- Log degli eventi
- Visualizzazione della topologia
- Avvisi su modifiche dei firewall locali

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

Reportistica[1,2]

- Report PDF programmati - A livello di 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
- Report di riepilogo dell'attività dei firewall
- Report sugli attacchi
- Report sull'utilizzo della VPN

Sicurezza

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

*Supportato su SonicOS 7.1 e superiore

SONICWALL®

Requisiti di sistema di NSM On-Premise

- Hypervisor: ESXi 7.0, 8.0, 2019, 2022, Microsoft Hyper-V e KVM
- Cloud pubblico: Azure
- Risorse di calcolo minime: 4 core vCPU, 16 GB di memoria RAM, 250 GB di spazio di archiviazione

Dispositivi gestiti[5]

- NSsp 15700, NSsp 13700, NSsp 11700, NSsp 10700, NSsp
- Serie 12000, serie SuperMassive 9000, serie NSa, serie TZ, TZ80, SOHO-W, SOHO 250, SOHO 250W
- Appliance di sicurezza di rete SonicWall virtuali: Serie NSv
- Il supporto per SonicWave include gli access point abilitati per Wi-Fi[6] [4]
- Switch SonicWall[4]

[1] NSM On-Premise 3.0 supporta nativamente la reportistica e le analisi. Ora offre le stesse funzionalità di NSM SaaS.
[2] On-Premise non supporta la reportistica e l'analisi per i prodotti Gen 6 / Gen 6.5
[3] Richiede la licenza AGSS/CGSS attivata sui firewall di ge-nerazione 6/6.5
[4] Gestito solo se connesso a un firewall gestito da NSM.
[5] Tutti i prodotti alla fine del ciclo di vita non sono supportati su NSM.
[6] L'hardware di 6ª generazione non supporta la reportistica e l'analisi di NSM On-Premise.

Implementa e gestisci tutti i firewall, gli switch e gli access point connessi da un'unica in-terfaccia di facile utilizzo.

www.sonicwall.com/nsm

SonicWall

SonicWall è un precursore della sicurezza informatica con oltre 30 anni di esperienza e di impegno continuo verso i propri partner. Grazie alla capacità di creare, scalare e gestire la sicurezza informatica in ambienti cloud, ibridi e tradizionali in tempo reale, SonicWall può fornire in modo rapido ed economico soluzioni di sicurezza dedicate a qualsiasi tipo di organizzazione in tutto il mondo. Mediante i dati del proprio centro di ricerca sulle minacce, SonicWall garantisce una protezione completa contro gli attacchi informatici più elusivi e fornisce informazioni pratiche sulle minacce ai partner, ai clienti e alla comunità di cybersecurity.

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