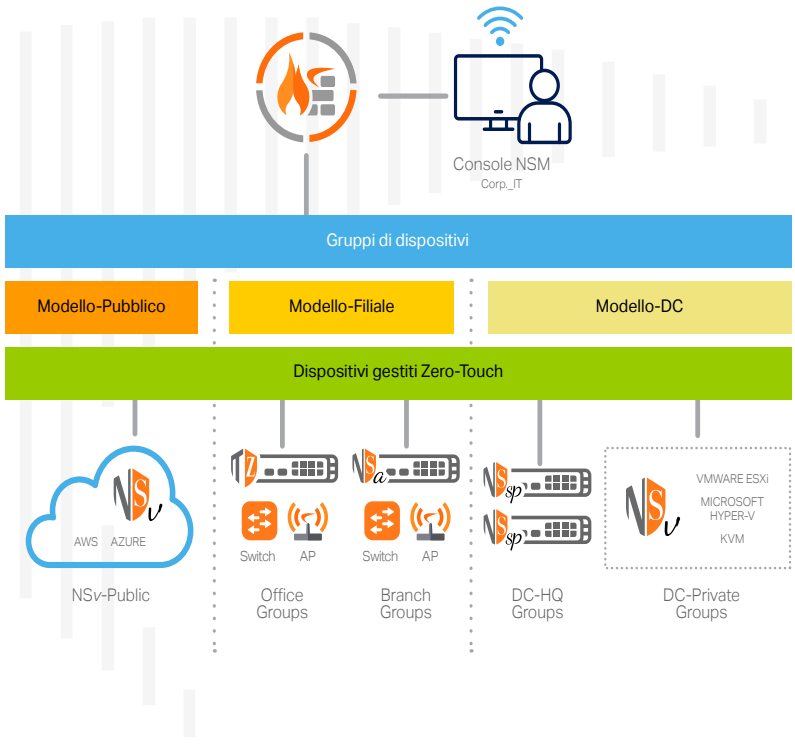
# Network Security Manager

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
- Riduzione delle spese di capitale con SaaS

### Operatività

- Eliminazione dei silos di gestione dei firewall
- Facile integrazione di qualsiasi numero di firewall in remoto
- Visibilità in tutte le operazioni di sicurezza
- Definizione di configurazione e policy coerenti tra tutti i dispositivi gestiti
- Facilitazione di una rapida implementazione di reti SD-WAN

### Sicurezza

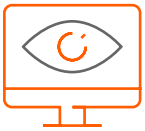
- Audit, commit e messa in pratica di policy di sicurezza coerenti in tutti gli ambienti
- Definizione di configurazioni SD-WAN coerenti in tutti i siti
- Caccia e reazione alle problematiche ai rischi con velocità
- Monitoraggio e tracciamento dei risultati degli interventi di policy con maggiore chiarezza
- Prevenzione dell'accesso non autorizzato, 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 punto 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 in quanto fornisce audit trail completi su ogni modifica della configurazione e reporting granulare. La soluzione è scalabile per organizzazioni di qualsiasi dimensione che gestiscono reti con migliaia di dispositivi firewall distribuiti in più sedi. NSM fa tutto con meno fatica e in meno tempo.



## Mantenere il controllo: coordinamento 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 di tenant, controllo dei dispositivi in base ai gruppi e scalabilità illimitata per gestire e fornire centralmente le operazioni di sicurezza di rete SonicWall, che 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 negli ambienti con controlli locali flessibili e il monitoraggio di ogni aspetto da un dashboard dinamico con report e analytics dettagliati. Inoltre, NSM consente di gestire tutto da un'unica console user-friendly a cui è possibile accedere da qualsiasi postazione utilizzando qualsiasi dispositivo abilitato tramite 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 una gestione multi-tenant completa e l'isolamento indipendente del controllo delle policy tra tutti i tenant gestiti. Questa separazione racchiude tutte le caratteristiche e le funzioni di gestione di NSM che determinano il funzionamento del firewall per ciascun tenant. È possibile configurare ogni tenant in modo che disponga del proprio set di utenti, gruppi e ruoli per guidare la gestione dei gruppi di dispositivi, l'orchestrazione delle policy e tutte le altre attività amministrative entro i limiti dell'account tenant assegnato.

### 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 provvedere al commit ed all'implementazione di modelli di configurazione su gruppi di firewall, che consentono di 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 gestione, identificazione e associazione.

### Gestione dei modelli, commit e implementazione

I workflow semplificati di NSM consentono di progettare, convalidare, verificare, approvare e confermare facilmente e rapidamente i modelli di configurazione per la gestione di uno o di migliaia 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 eseguire il push centralizzato e automatico su dispositivi o gruppi di dispositivi che richiedono configurazioni simili.

I modelli combinati con le Template Variable consentono di implementare e rifornire centralmente migliaia 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 e rendendo superflue le 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 migliaia di siti, come filiali e negozi al dettaglio. In aggiunta, NSM consente 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 workflow 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 completamente automatizzata con grande facilità

In NSM è integrato il servizio di implementazione completamente automatizzata Zero-Touch Deployment 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 «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 integrazione (onboarding) in loco.

### Gestione delle modifiche senza errori

NSM consente l'accesso immediato a potenti workflow automatizzati conformi ai requisiti di gestione e audit delle modifiche alle policy firewall dei SOC. Inoltre permette modifiche alle policy senza errori attraverso l'applicazione di 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 per aumentare 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, esecuzione di controlli di integrità del sistema e altro ancora.

## Maggiore consapevolezza: indagini sui rischi nascosti con monitoraggio, reporting e analytics attivi[1,2]

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

### Osserva tutto, ovunque sia

NSM, in combinazione con gli Analytics,[1,2] offre fino a 7 giorni di visibilità continua a 360° sull'intero ecosistema di sicurezza SonicWall a livello di tenant, gruppo o dispositivo e 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, interpretazione, assegnare priorità e adottare interventi difensivi e correttivi adeguati in base alle informazioni corroborate dai dati e con consapevolezza della situazione. I report programmati consentono di personalizzare i report con qualsiasi combinazione di dati sul traffico e offrono fino a 365 giorni di

log registrati a livello di dispositivo per analisi cronologiche, rilevamento di anomalie, individuazione delle falle di sicurezza e altro ancora. Tutto questo aiuta nel monitoraggio, nella misurazione e nell'esecuzione di efficaci operazioni di rete e sicurezza.

### Comprensione del rischio

Con l'aggiunta di funzionalità di drill-down e pivoting è possibile indagare più a fondo e mettere in correlazione i dati per esaminare e scoprire minacce e problemi nascosti con maggiore precisione e sicurezza. Utilizzando una combinazione di report storici, analytics basate su utenti e applicazioni, e con 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 e guidare l'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 orientare e analizzare facilmente e rapidamente i punti di interesse dei dati a livello di utente e di stabilire misure controllate da policy comprovate per utenti e applicazioni rischiose mentre si sviluppano nel processo di rilevamento. Inoltre, i Productivity Report[1,2] forniscono informazioni sull'utilizzo di Internet e sul comportamento dei dipendenti in un periodo specificato. Lo strumento genera istantanee d'impatto e report dettagliati che classificano le attività Web degli utenti per gruppi di produttività, come 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.

Per ottenere un'esperienza senza manutenzione, NSM è disponibile come offerta SaaS con hosting di SonicWall e accessibile tramite Internet. Con NSM SaaS è possibile ottenere una scalabilità su richiesta riducendo i costi operativi. Non vi è alcuna necessità di implementare 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 organizzazioni 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 offline per eseguire le operazioni di onboarding, la gestione delle licenze, delle patch e degli aggiornamenti del sistema NSM e dei firewall sotto la sua gestione senza dover contattare il SonicWall License Manager e 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 utente è consentito, inoltre, 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

- Gestione a livello di tenant e gruppo di dispositivi
- Modelli di configurazione
- Raggruppamento di dispositivi
- Conversione da configurazione del dispositivo a modello
- Procedura guidata di commit e implementazione
- Audit della configurazione
- Config – Diff
- Gestione e pianificazione offline
- Gestione delle policy di sicurezza dei firewall
- Gestione delle policy di sicurezza VPN
- Gestione di SD-WAN
- Gestione dei servizi di sicurezza
- Alta disponibilità
- Backup della configurazione
- API RESTful
- Aggiornamento del 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 della licenza e del supporto
- Riepilogo rete/minacce
- Centro avvisi e notifiche
- Log eventi
- Visualizzazione della topologia

### Analytics[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
- Rapporto su minacce multiple
- Report basato sugli utenti
- Report sull'utilizzo dell'applicazione
- Report su larghezza di banda e servizi
- Creazione di report sulla larghezza di banda per utente

### Sicurezza

- Supporto per rete chiusa
- 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 push a livello di gruppo | Sì | Sì | Sì |
| Gruppo di dispositivi | Sì | Sì | Sì |
| Modelli | Sì | Sì | Sì |
| Commit e implementazione (automazione del workflow) | Sì | Sì | Sì |
| Audit 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 |

## Licenze e pacchetti, continua

### Reporting

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

### Analisi

| Funzionalità | NSM SaaS Essential | NSM SaaS Advanced | NSM On-Prem[2] |
|---|---|---|---|
| Analytics basati sull'utente – Livello dispositivo | No | Sì | No |
| Analytics delle applicazioni – Livello dispositivo | No | Sì | No |
| Analytics delle minacce – Livello dispositivo | No | Sì | No |
| Drill-down e pivot – Livello dispositivo | No | 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, 6.5 e Hyper-V 2016, 2019
- Risorse di calcolo minime: 4 vCPU, 16 GB di memoria, 250 GB di spazio di archiviazione

### Dispositivi gestiti

- NS*sp* 15700, NS*sp* 13700, NS*sp* Serie 12000[4], SuperMassive Serie 9000[4], E-Class 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, SonicPoint
- 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 analytics.
[3] Disponibile solo su NSM On-Prem.
[4] 365 giorni di reporting e 30 giorni di analytics non supportati.
[5] Richiede l'abilitazione della licenza AGSS/CGSS su firewall di generazione 6/6.5 e la licenza Essential Protection su firewall di generazione 7.

**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 illimitata per l'era iperdistribuita in una realtà lavorativa in cui tutto è all'insegna del telelavoro, della mobilità e della mancanza di sicurezza. Conoscendo l'ignoto, offrendo visibilità in tempo reale e rendendo possibili economie innovative, SonicWall colma le lacune della cybersecurity per aziende, enti pubblici e PMI in ogni parte del mondo. Per maggiori informazioni potete visitare www.sonicwall.com o seguirci su Twitter, LinkedIn, Facebook e Instagram.

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