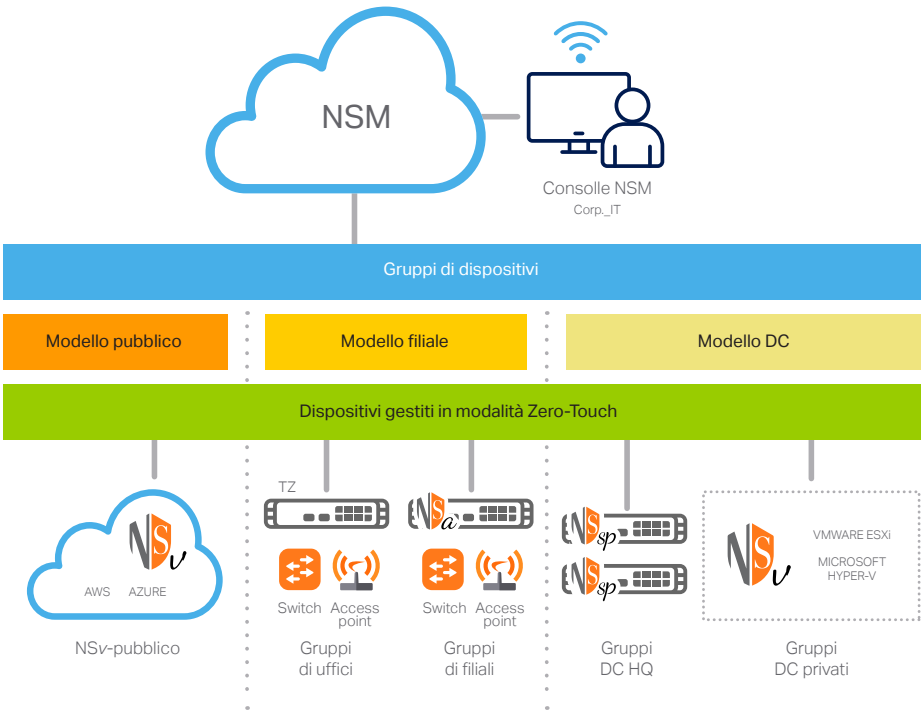
SONICWALL

Network Security Manager

Sistema di gestione firewall unificato modulabile per qualsiasi ambiente

Sia che si tratti di proteggere una piccola azienda, un'azienda distribuita o più aziende, la sicurezza della rete può essere messa in pericolo da problemi di carattere operativo, rischi sconosciuti ed obblighi normativi. Da sempre le buone prassi di gestione dei firewall sono state basate soprattutto su misure efficaci ed affidabili a livello di sistema e di controllo operativo. Tuttavia, gli errori comuni, le configurazioni errate e forse anche le violazioni dei controlli stessi continuano a rappresentare una sfida costante per una corretta gestione dei Security Operation Center (SOC).

SonicWall Network Security Manager (NSM), un gestore centralizzato di firewall multi-tenant, consente di gestire centralmente tutte le operazioni dei firewall senza errori aderendo a flussi di lavoro verificabili. Il suo motore analitico nativo offre visibilità da un unico punto di controllo e consente di monitorare e individuare le minacce unificando e correlando i registri di tutti i firewall. NSM consente inoltre di rispettare le norme in quanto garantisce un audit trail completo di tutte le modifiche della configurazione e una reportistica granulare. NSM è adatto per le organizzazioni di qualsiasi dimensione che gestiscono reti con migliaia di dispositivi firewall distribuiti in diverse sedi, il tutto con minore impegno e in minor tempo.



Vantaggi:

Commerciali

- Riduzione dei costi di gestione della sicurezza
- Conoscenza della situazione delle minacce e approccio alla sicurezza
- Riduzione dei costi d'investimento con SaaS

Operativi

- Nessun HW/SW da installare
- Eliminazione dei silos di gestione dei firewall
- Facilità di presa in carico di qualsiasi numero di firewall remoto
- Visibilità su tutte le attività di sicurezza

Sicurezza

- Verificare, destinare e attuare politiche di sicurezza coerenti in tutti gli ambienti
- Affrontare e rispondere rapidamente alle problematiche e ai rischi
- Prendere decisioni informate in materia di politiche di sicurezza

Avere la situazione sotto controllo. Gestire il funzionamento dei firewall da un'unica postazione

NSM mette a disposizione tutto ciò che serve per un sistema di gestione firewall unificato. Consente di avere visibilità a livello dei tenant, controllo dei dispositivi di gruppo e modularità illimitata per garantire e gestire centralmente le operazioni di sicurezza di rete di SonicWall. Sono comprese l'installazione e la gestione di tutti i dispositivi firewall, dei gruppi di dispositivi e dei tenant, la sincronizzazione e l'applicazione di politiche di sicurezza coerenti in ambienti con controlli locali flessibili e il monitoraggio generale da un pannello di controllo dinamico con reportistica e analisi dettagliate. NSM consente di fare tutto questo da un'unica consolle cloud nativa di facile uso, accessibile da qualsiasi posizione utilizzando qualsiasi dispositivo compatibile con i browser.

Gestione multi-tenant
Man mano che l'ambiente firewall cresce con tenant complessi multi-cloud e multi-location che hanno diverse esigenze di sicurezza per ogni segmento di rete, si ha bisogno di un sistema di gestione dei firewall che possa essere modulato in funzione dell'evoluzione dell'ambiente. NSM mette a disposizione una soluzione di gestione completa multi-tenant e l'isolamento indipendente del controllo delle politiche per tutti i tenant gestiti. La separazione riguarda tutte le caratteristiche e le funzioni gestionali di NSM, che determinano il funzionamento del firewall per ogni tenant. È possibile strutturare ogni tenant in modo che disponga di un proprio insieme di utenti, gruppi e ruoli per condurre la gestione del gruppo di dispositivi, quella delle politiche e tutte le altre attività amministrative entro i limiti dell'account assegnato al tenant.

Gestione dei gruppi di dispositivi
I gruppi di dispositivi sono un metodo efficace per creare e gestire dispositivi firewall come gruppi o gruppi gerarchici e per destinare e distribuire modelli di configurazione su gruppi di firewall. Ciò consente di sincronizzare e applicare politiche comuni e oggetti e/o impostare requisiti in tutti i gruppi firewall selezionati in modo coerente e affidabile. Tutte le modifiche della politica approvate nel modello vengono applicate automaticamente a tutto il gruppo di dispositivi collegato ad esso. Il raggruppamento dei dispositivi può essere definito in base a caratteristiche come tipo di rete, ubicazione, business unit, struttura organizzativa o una combinazione di attributi relativi per facilitare la gestione, l'identificazione e l'associazione.

Gestione modelli, destinazione e installazione
I flussi di lavoro semplificati di NSM consentono di progettare, convalidare, verificare e destinare facilmente e rapidamente modelli di configurazione per la gestione di uno o migliaia di dispositivi firewall in diverse sedi geografiche. I modelli con politiche firewall, impostazioni e oggetti correlati diversi vengono definiti indipendentemente dal dispositivo e vengono utilizzati da NSM per l'invio centralizzato e automatico a dispositivi o gruppi di dispositivi che richiedono configurazioni simili.

Maggiore efficienza. Lavorare in modo più intelligente e agire più rapidamente in materia di sicurezza con un minore impegno

NSM è uno strumento di gestione della produttività che consente di lavorare in modo più intelligente ed effettuare azioni di sicurezza più rapidamente e con meno sforzo. Questo approccio è basato sul principio della semplificazione e, in alcuni casi, dell'automazione delle diverse attività per ottenere una migliore coordinazione della sicurezza e dei processi decisionali, riducendo nel contempo la complessità, i tempi e i costi dell'esecuzione delle operazioni di sicurezza e delle attività amministrative.

Installazione semplificata in modalità Zero-Touch
Integrato in NSM è il servizio Zero-Touch Deployment, che consente di installare e rendere operativi i firewall, gli switch e gli access point SonicWall nelle sedi remote e secondarie in modo semplice e rapido. L'intero processo richiede un minimo intervento da parte dell'utente ed è completamente automatizzato. I dispositivi abilitati Zero-Touch vengono spediti direttamente alle sedi di installazione. Una volta disimballati, registrati, cablati sulla rete e alimentati, tutti i dispositivi collegati sono immediatamente operativi e la sicurezza e la connettività avvengono senza soluzione di continuità. Una volta stabiliti i collegamenti di comunicazione con NSM, i modelli dei dispositivi predisposti vengono automaticamente inviati a tutti i dispositivi abilitati alla modalità zero-touch. In questo modo vengono eliminati i tempi, i costi e la complessità del tradizionale processo di inserimento in loco.

Gestione dei cambiamenti senza errori
NSM consente l'accesso immediato a potenti flussi di lavoro automatizzati adeguati ai requisiti dei SOC per la gestione dei cambiamenti delle politiche e l'auditing dei firewall, garantendo al tempo stesso una gestione delle politiche priva di errori, attuando tutta una serie di processi di configurazione rigorosi che comprendono politiche di confronto, validazione, riesame e approvazione prima dell'installazione. I gruppi di approvazione si adeguano in modo flessibile alle diverse procedure di autorizzazione e audit dei vari tipi di organizzazioni. NSM attua programmaticamente politiche di sicurezza completamente convalidate e verificate per migliorare l'efficienza operativa, ridurre i rischi ed eliminare configurazioni errate ed errori umani.

Automazione della gestione con le API RESTful
Le API RESTful di NSM mettono a disposizione degli operatori di sicurezza esperti un approccio standard alla gestione delle caratteristiche specifiche di NSM in modo programmatico e senza dover ricorrere all'interfaccia di gestione web. Facilitano l'interoperabilità tra le consolle di gestione di NSM e quelle di terzi per aumentare l'efficienza del personale di sicurezza interno. I servizi API vengono utilizzati per automatizzare il funzionamento dei firewall per i singoli dispositivi gestiti. Si tratta di attività quotidiane comuni come tenant, gruppo di dispositivi e gestione del locatario, configurazioni di audit, esecuzione di controlli sulla salute del sistema etc..

Maggiore consapevolezza. Ricercare i rischi nascosti con monitoraggio, reportistica e analisi attivi

Il pannello di controllo interattivo di NSM utilizza numerosi dati di monitoraggio, reportistica e analisi in tempo reale, che aiutano a risolvere i problemi, indagano i rischi e guidano le decisioni sulle politiche di sicurezza intelligente e le relative azioni per un approccio alla sicurezza maggiormente adattivo.

Tutto sotto controllo da qualsiasi parte
Il pannello di controllo MSN per la reportistica, le analisi e la gestione del rischio consente fino a 7 giorni di visibilità continua a 360° dell'intero ecosistema di sicurezza di SonicWall a livello di tenant, gruppo o dispositivo. Fornisce un'analisi statica e quasi in tempo reale di tutto il traffico di rete e la comunicazione dei dati che passano attraverso l'ecosistema dei firewall. Tutti i dati di registro vengono automaticamente memorizzati, aggregati, contestualizzati e presentati in modo

logico, azionabile e facilmente utilizzabile per poter individuare, interpretare, dare priorità e porre in essere azioni difensive e correttive appropriate basate su informazioni a loro volta basate sui dati e sulla consapevolezza della situazione. La reportistica programmata consente di personalizzare completamente i report con qualsiasi combinazione di dati verificabili. Presenta fino a 365 giorni di registrazione memorizzati a livello di dispositivo per le analisi storiche, il rilevamento delle anomalie, l'individuazione delle lacune di sicurezza etc.. Tutto ciò aiuta a tracciare, misurare e gestire una rete e operazioni di sicurezza efficaci.

Conoscere i propri rischi
Grazie alle ulteriori funzioni di drill-down e pivoting è possibile indagare e correlare ulteriormente i dati per esaminare e individuare con maggiore precisione e fiducia le minacce nascoste e i problemi. Utilizzando una combinazione di report storici, analisi basate sugli utenti e sulle applicazioni e visibilità degli endpoint è possibile analizzare accuratamente diversi modelli e diverse tendenze associati al traffico in ingresso e in uscita, all'utilizzo delle applicazioni, agli accessi degli utenti e dei dispositivi, alle azioni di minaccia etc.. Grazie a tutte queste funzioni è possibile acquisire consapevolezza della situazione e preziose informazioni e conoscenze per individuare non solo i rischi di sicurezza, ma anche organizzare i rimedi, monitorando e tracciando al tempo stesso i risultati per promuovere e guidare l'attuazione coerente delle politiche di sicurezza in tutto l'ambiente di rete.

Riepilogo delle funzioni

Gestione

- Gestione a livello di tenant e gruppo di dispositivi
- Modelli di configurazione
- Raggruppamento dei dispositivi
- Procedura guidata di destinazione e installazione
- Verifiche di configurazione
- Config – Diff
- Gestione e programmazione offline
- Gestione delle politiche di sicurezza dei firewall
- Gestione delle politiche di sicurezza delle VPN
- Gestione SD-WAN
- Gestione dei servizi di sicurezza a valore aggiunto
- Ridondanza e disponibilità elevate
- Backup dei file con le preferenze per i firewall
- API RESTful
- Aggiornamento firmware
- Amministrazione basata sui ruoli
- Gestione degli access point e degli switch

Monitoraggio

- Stato e salute del dispositivo
- Stato delle licenze e dei contratti d'assistenza
- Riepilogo rete e minacce
- Centro di allerta e segnalazione
- Registri degli eventi
- Visualizzazione della topologia

Statistiche

- Attività basate sugli utenti
- Uso delle applicazioni
- Visibilità dei diversi prodotti con Capture Client
- Visualizzazione dinamica in tempo reale
- Funzioni di drill-down e pivoting

Reportistica

- Report PDF pianificati – A livello di tenant, gruppo e dispositivo
- Report personalizzabili
- Memorizzazione centralizzata
- Reportistica minacce multiple
- Reportistica incentrata sull'utente
- Reportistica dell'uso delle applicazioni
- Reportistica ampiezza di banda e servizi
- Reportistica ampiezza di banda per utente

Licenze e abbinamenti

Funzioni	Essential	Advanced
Gestione di centinaia di dispositivi per tenant	Sì	Sì
Gestione multi-tenant	Sì	Sì
Inventario dei dispositivi	Sì	Sì
Invio delle politiche a livello di gruppo	Sì	Sì
Gruppo di dispositivi	Sì	Sì
Modelli	Sì	Sì
Invio e installazione	Sì	Sì
Verifiche di configurazione	Sì	Sì
Config Diff	Sì	Sì
Automazione di flussi di lavoro	Sì	Sì
API	Sì	Sì
Zero-Touch Deployment	Sì	Sì
Programmazione attività	Sì	Sì

Funzioni	Essential	Advanced
Backup e ripristino	Sì	Sì
Aggiornamenti firmware	Sì	Sì
Gestione access point e switch	Sì	Sì
Durata dati reportistica	7 giorni	365 giorni
Pannello di controllo a livello di gruppo e di tenant	Sì	Sì
Capture ATP (a livello di dispositivo)	Sì	Sì
Acquisizione della valutazione delle minacce (a livello di dispositivo)	Sì	Sì
Visibilità e reportistica a livello di gruppo	Sì	Sì
Report programmati (a livello di gruppo di dispositivi)	Sì	Sì
Analisi basata sugli utenti	No	Sì
Analisi delle applicazioni	No	Sì
Analisi delle minacce	No	Sì
Drill-down e pivot	No	Sì

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

Sono disponibili anche SKU e contratti di supporto pluriennali. Per un elenco completo contattare il rivenditore preferito o SonicWall Sales.

Internet Browser

- Microsoft® Internet Explorer 11.0 o versione superiore e ultima versione di Microsoft Edge, Mozilla Firefox, Google Chrome e Safari.

Dispositivi gestiti da NSM[1]

- Dispositivi SonicWall Email Security SuperMassive 9000 Series[2], E-Class NSA, NS*sp* 12000 Series[2], NS*a* Series, TZ Series, SOHO-W, SOHO 250, SOHO 250W
- Appliance virtuali SonicWall Network Security NSv Series
- SonicWall SonicWave, SonicPoint
- Switch SonicWall

[1] Supporta i firewall che usano SonicOS versione 6.x o 7.x.
[2] 365 giorni di reportistica e 30 giorni di analisi non sono supportati.

SonicWall

SonicWall fornisce soluzioni di cibersicurezza 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 una visibilità in tempo reale e rendendo possibili economie innovative, SonicWall colma le lacune di cibersicurezza per aziende, enti pubblici e PMI in ogni parte del mondo. Per ulteriori informazioni visitare il sito www.sonicwall.com.

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

Datasheet-NSM-US-COG-2114