SONICWALL

Serie SonicWall Network Security appliance (NSa)

Efficacia e prestazioni di sicurezza riconosciute a livello industriale per reti di medie dimensioni, filiali ed aziende distribuite

La serie SonicWall Network Security appliance (NSa) offre a tutta una serie di organizzazioni, dalle reti aziendali di medie dimensioni, alle imprese distribuite e ai data center, la prevenzione avanzata delle minacce nell'ambito di una piattaforma di sicurezza ad alte prestazioni. Utilizzando tecnologie innovative di deep learning all'interno della piattaforma SonicWall Capture Cloud, la serie NSa fornisce il rilevamento automatizzato delle intrusioni in tempo reale e la prevenzione richiesti dalle organizzazioni.

Prevenzione delle minacce all'avanguardia con prestazioni di livello superiore

Le odierne minacce per le reti sono altamente evasive e sempre più difficili da identificare utilizzando i metodi di rilevamento tradizionali. Per essere sempre pronti agli attacchi sempre più sofisticati è necessario un approccio più moderno che sfrutti pesantemente l'intelligence della sicurezza sul cloud. Senza tale intelligence sul cloud, le soluzioni di sicurezza gateway non possono tenere il passo con le complesse minacce odierne. La serie di firewall di nuova generazione NSa (NGFW) integra due tecnologie di sicurezza avanzate per fornire prevenzione all'avanguardia dalle minacce in modo da far sì che la vostra rete sia sempre un passo più avanti. A migliorare il servizio multi-engine Capture Advanced Threat Protection (ATP) di SonicWall è giunta la nostra tecnologia Real-Time Deep Memory Inspection (RTDMI™), in attesa di brevetto. L'engine RTDMI rileva e blocca in anticipo le minacce di massa, le minacce zero-day e i malware sconosciuti eseguendo ispezioni direttamente nella memoria. Grazie all'architettura in tempo reale, la tecnologia RTDMI è precisa, riduce al minimo i falsi positivi e identifica e attenua gli attacchi sofisticati durante i quali l'armamentario del malware resta esposto per meno di 100 nanosecondi. In abbinamento, viene utilizzato l'engine RFDPI (Reassembly-Free Deep Packet Inspection) a singola fase di SonicWall brevettato* per esaminare ogni byte di ogni pacchetto, ispezionando il traffico in entrata e in uscita sul firewall. Sfruttando la piattaforma SonicWall Capture Cloud, in aggiunta alle funzionalità on-box che comprendono prevenzione delle intrusioni, anti-malware e filtraggio Web/URL, la serie NSa blocca anche le minacce più insidiose a livello di gateway.

Inoltre, i firewall SonicWall offrono una protezione completa eseguendo decrittazione ed ispezione complete delle connessioni TLS/SSL ed SSH crittografate, indipendentemente dalla porta o dal protocollo. Il firewall esamina ogni singolo pacchetto in profondità (intestazione e dati) alla ricerca di non conformità del protocollo, minacce, zero-day, intrusioni e persino criteri definiti. L'engine di Deep Packet Inspection rileva e previene gli attacchi nascosti che sfruttano la crittografia, blocca i download di malware crittografato, interrompe la diffusione di infezioni e le comunicazioni di comando e controllo (C&C), oltre alla fuoriuscita dei dati. Le regole di inclusione ed esclusione consentono di stabilire quale traffico deve essere sottoposto alla decrittazione e all'ispezione in base a requisiti di conformità specifici dell'azienda e/o legali.

Quando le organizzazioni attivano funzioni di Deep Packet Inspection come IPS, anti-virus, anti-spyware, decrittazione/ispezione TLS/SSL ed altre funzionalità sui firewall, le prestazioni della rete spesso rallentano, anche drasticamente. I firewall della serie NSa, tuttavia, presentano

Vantaggi:

- Prevenzione delle minacce e prestazioni di livello superiore
- Tecnologia Real-Time Deep Memory Inspection in attesa di brevetto
- Tecnologia Reassembly-Free Deep Packet Inspection brevettata
- Prevenzione delle minacce integrata e basata su cloud
- Decrittazione e ispezione TLS/SSL
- Efficacia della sicurezza comprovata nel settore
- Architettura hardware multi-core
- Team Capture Labs dedicato alla ricerca delle minacce

Controllo della rete e flessibilità

- SD-WAN sicura
- Potente sistema operativo SonicOS
- Intelligenza e controllo delle applicazioni
- Segmentazione della rete tramite VLAN
- Wireless sicuro ad alta velocità

Semplicità di installazione, configurazione e gestione

- Zero-Touch Deployment
- Gestione centralizzata basata su cloud e on-premise
- Linea scalabile di firewall
- Basso costo totale di proprietà

Brevetti USA 7.310.815, 7.600.257, 7.738.380, 7.835.361, 7.991.723

un'architettura hardware multi-core che utilizza microprocessori specializzati per la sicurezza. In combinazione con i nostri motori RTDMI ed RFDPI, questa struttura esclusiva elimina i fenomeni di degrado delle prestazioni delle reti con altri firewall.

Controllo della rete e flessibilità

Il nucleo della serie NSa è costituito da SonicOS, il sistema operativo ricco di funzionalità di SonicWall. SonicOS offre alle organizzazioni il controllo della rete e la flessibilità di cui necessitano attraverso l'intelligence e il controllo delle applicazioni, la visualizzazione in tempo reale, un sistema di prevenzione delle intrusioni (IPS) con sofisticate tecnologie anti-evasione, VPN (Virtual Private Networking) ad alta velocità ed altre solide funzionalità di sicurezza.

Utilizzando funzionalità di Application Intelligence and Control, gli amministratori di rete possono identificare e distinguere le applicazioni produttive da quelle improduttive o potenzialmente pericolose e controllare tale traffico attraverso potenti politiche a livello di applicazione, su base utente e su base gruppo (insieme a pianificazioni ed elenchi di eccezioni). Le applicazioni fondamentali per l'attività aziendale possono avere la priorità e ricevere l'assegnazione di una maggiore larghezza di banda, mentre le applicazioni non essenziali ricevono larghezza di banda limitata.

Il monitoraggio e la visualizzazione in tempo reale forniscono una rappresentazione grafica delle applicazioni, degli utenti e dell'utilizzo della larghezza di banda per una visione granulare del traffico sull'intera rete.

Per le organizzazioni distribuite che necessitano di una flessibilità avanzata per la propria struttura di rete, la tecnologia SD-WAN di SonicOS è il complemento ideale per i firewall NSa installati presso la sede centrale o in sedi remote e filiali. Invece di affidarsi a tecnologie legacy più costose come MPLS e T1, le imprese che utilizzano la tecnologia SD-WAN possono scegliere servizi Internet pubblici a basso costo continuando ad ottenere un elevato livello di disponibilità delle applicazioni e prestazioni prevedibili.

In ogni firewall della serie NSa è integrato un controller di accesso wireless che consente alle organizzazioni di estendere il perimetro della rete in modo sicuro attraverso l'utilizzo della tecnologia wireless. La combinazione dei firewall SonicWall e degli access point wireless SonicWave 802.11ac Wave 2 crea una soluzione di sicurezza della rete wireless che coniuga una tecnologia firewall di nuova generazione, leader del settore, e il wireless ad alta velocità per garantire sicurezza e prestazioni di rete di livello imprenditoriale sulla rete wireless.

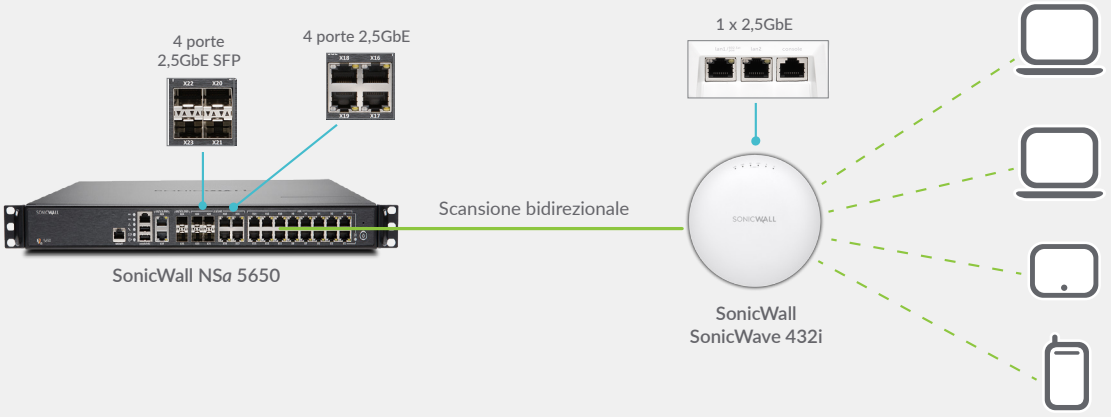
Semplicità di installazione, configurazione e gestione

Come tutti i firewall SonicWall, la serie NSa presenta una stretta integrazione delle principali tecnologie di sicurezza, connettività e flessibilità in un'unica soluzione completa. Tale soluzione comprende gli access point wireless SonicWave e la serie SonicWall WAN Acceleration (WXA), entrambi rilevati e serviti automaticamente dal firewall di gestione NSa. Il consolidamento di più funzionalità elimina la necessità di acquistare e installare singoli prodotti che non sempre funzionano bene gli uni con gli altri, riducendo così la complessità di implementazione in rete e di configurazione, con conseguente risparmio di tempo e denaro.

La gestione centralizzata, i report, le licenze e l'analisi in cloud sono gestiti tramite il SonicWall Capture Security Center. Un componente fondamentale del Capture Security Center è l'installazione zero-touch (Zero-Touch Deployment). Questa funzione basata sul cloud semplifica e velocizza l'installazione e il provisioning dei firewall SonicWall presso le sedi remote e le filiali aziendali. Le procedure semplificate di installazione e configurazione e la facilità di gestione consentono alle organizzazioni di ridurre il costo totale di proprietà e ottenere un elevato ritorno sull'investimento.

Wireless sicuro ad alta velocità

Abbinando un firewall di nuova generazione della serie NSa ad un access point wireless SonicWave 802.11ac Wave 2 si ottiene una soluzione di sicurezza per rete wireless ad alta velocità. I firewall della serie NSa e gli access point SonicWave sono entrambi dotati di porte da 2,5 GbE che consentono il throughput wireless multi-gigabit reso possibile dalla tecnologia wireless Wave 2. Il firewall esegue la scansione di tutto il traffico wireless in entrata e in uscita sulla rete utilizzando la tecnologia Deep Packet Inspection e quindi elimina le minacce pericolose, come il malware e le intrusioni, anche su connessioni crittografate. Ulteriori funzionalità di sicurezza e controllo, come Content Filtering, Application Intelligence and Control e Capture Advanced Threat Protection, possono essere eseguite sulla rete wireless per fornire ulteriori livelli di protezione.

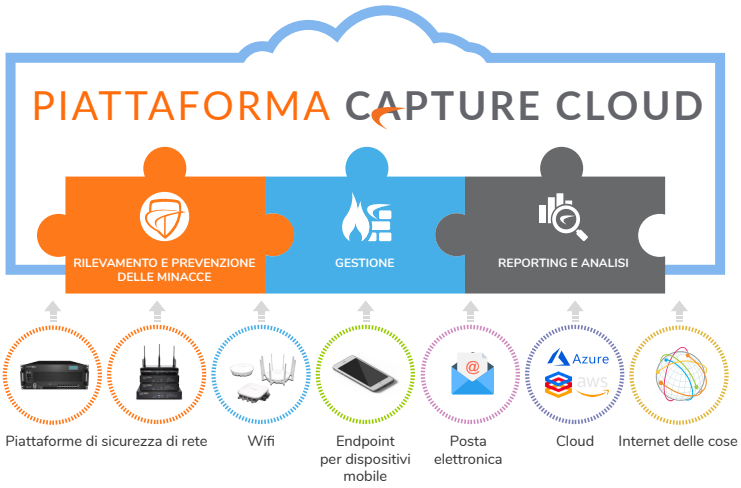


Capture Cloud Platform

La piattaforma Capture Cloud di SonicWall offre la prevenzione delle minacce basata sul cloud e la gestione della rete oltre a funzionalità di reportistica e analisi per organizzazioni di qualsiasi dimensione. La piattaforma consolida le informazioni sulle minacce raccolte da molteplici fonti, tra cui il nostro premiato servizio sandbox di rete multi-engine Capture Advanced Threat Protection, e oltre 1 milione di sensori SonicWall situati in tutto il mondo.

Se i dati in arrivo nella rete contengono codice maligno precedentemente non rilevato, il team interno Capture Labs di SonicWall dedicato alla ricerca delle minacce sviluppa segnature che vengono archiviate nel database della piattaforma Capture Cloud e distribuite ai firewall dei clienti per aggiornare la protezione. I nuovi aggiornamenti vengono attivati immediatamente senza riavvii o interruzioni. Le segnature residenti nell'apparecchiatura forniscono protezione da numerose classi di attacchi, coprendo decine di migliaia di singole minacce. Oltre alle contromisure sull'apparecchiatura, i firewall NSa hanno anche accesso continuo al database della piattaforma Capture Cloud, che amplia le informazioni sulle segnature integrate con decine di milioni di segnature.

La piattaforma Capture Cloud fornisce la prevenzione delle minacce e offre un unico pannello di gestione da cui gli amministratori possono facilmente creare report in tempo reale e storici sull'attività di rete.



Protezione contro le minacce avanzate

Al centro della prevenzione automatica delle violazioni in tempo reale vi sono due tecnologie di rilevamento del malware avanzate: Capture Advanced Threat Protection™ (Capture ATP) e Capture Security appliance™ (CSa).

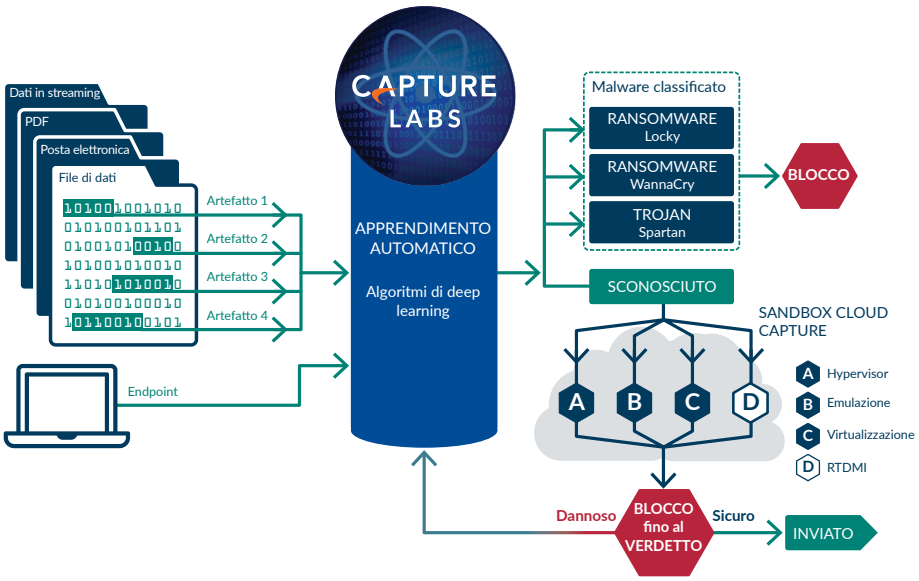
Capture ATP è una piattaforma di sandbox multi-engine basata sul cloud, che comprende Real-Time Deep Memory Inspection™ (RTDMI), sandboxing virtualizzato, emulazione completa del sistema e tecnologia di analisi a livello di hypervisor. CSa è un dispositivo per installazione interna dotato di tecnologia RTDMI, che utilizza tecniche dinamiche e statiche basate sulla memoria per emettere verdetti definitivi e precisi. Entrambe le soluzioni ampliano la protezione contro le minacce avanzate al rilevamento e alla prevenzione degli attacchi zero-day in tutta una gamma di soluzioni SonicWall come i firewall di prossima generazione.

I file sospetti vengono inviati a una delle due soluzioni dove vengono analizzati utilizzando algoritmi di deep learning con la possibilità di trattenerli nel gateway fino a quando non viene stabilito un verdetto.

Nel caso di Capture ATP, quando i file vengono identificati come nocivi vengono bloccati e viene immediatamente creato un hash nel database Capture ATP per tutti i clienti per beneficiare del blocco degli attacchi successivi. In ultima analisi queste segnature vengono inviate ai firewall per realizzare difese statiche. Per motivi di privacy ed esigenze di conformità i risultati prodotti da CSa non vengono diffusi fuori dall'organizzazione.

Questi servizi analizzano un'ampia gamma di sistemi operativi e tipologie di file, tra cui programmi eseguibili, DLL, PDF, documenti MS Office, archivi, JAR e APK.

Per una protezione completa degli endpoint, SonicWall Capture Client abbina la tecnologia antivirus di prossima generazione alla sandbox multi-engine basata sul cloud di SonicWall integrandola facoltativamente con firewall SonicWall.



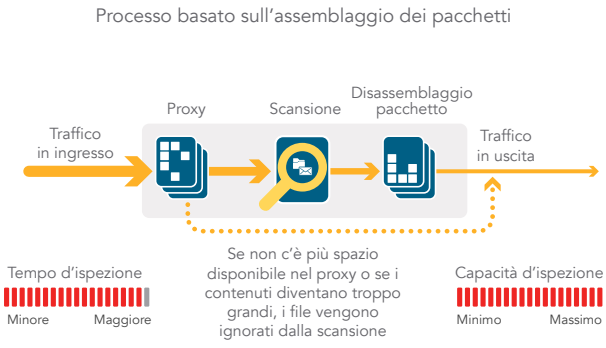
SONICWALL®

Engine Reassembly-Free Deep Packet Inspection

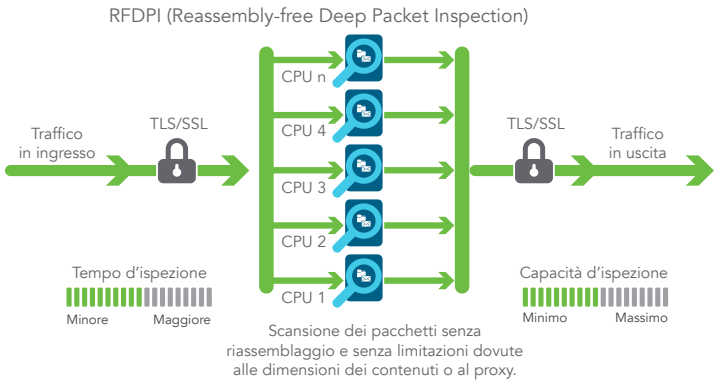
La tecnologia Reassembly-Free Deep Packet Inspection (RFDPI) di SonicWall è un sistema di ispezione a singolo passaggio e bassa latenza che esegue analisi ad alta velocità del traffico bidirezionale in base al flusso, senza proxy o buffering, per scoprire efficacemente i tentativi di intrusione e download di malware esaminando il traffico applicativo indipendentemente dalla porta e dal protocollo. Questo engine proprietario ispeziona i payload del traffico in transito per rilevare eventuali minacce ai livelli 3-7 ed esamina i flussi di rete, con procedure complesse e ripetute di normalizzazione e decrittazione, per sventare le tecniche di evasione avanzata che tentano di confondere i motori di rilevamento e introdurre codice dannoso nella rete.

Una volta superata la necessaria elaborazione preliminare, che comprende anche la decrittazione TLS/SSL, ogni pacchetto viene analizzato in base a un'unica rappresentazione di memoria proprietaria di tre database di segnature: attacchi intrusivi, malware e applicazioni. Lo stato di connessione viene quindi fatto progredire in modo che rappresenti la posizione del flusso riferita a questi database, finché non rileva uno stato di attacco o un altro evento "corrispondente".

Nella maggior parte dei casi, la connessione viene terminata e vengono generati eventi di log e di notifica. Nella maggior parte dei casi, la connessione viene terminata e vengono generati eventi di log e di notifica. L'engine può anche essere configurato per eseguire solo l'ispezione oppure, in caso di rilevamento delle applicazioni, per fornire servizi di gestione della larghezza di banda al livello 7 per il rimanente flusso dell'applicazione non appena viene identificata l'applicazione.



Architettura competitiva basata su proxy



Architettura SonicWall basata sullo stream

Gestione e reportistica centralizzate

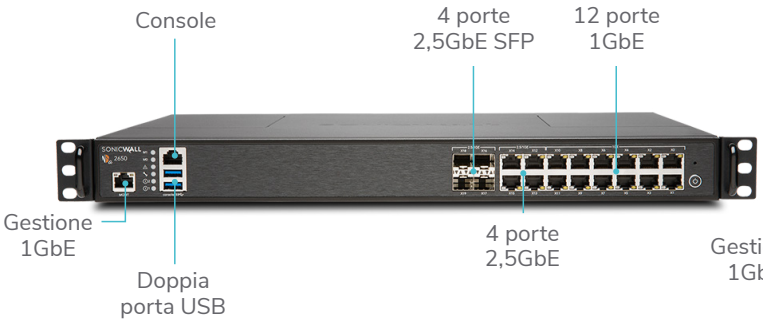
Per le organizzazioni ad elevata regolamentazione che desiderano creare una strategia coordinata di gestione della sicurezza, compliance e gestione del rischio, SonicWall offre agli amministratori una piattaforma unificata, sicura ed espandibile per gestire i firewall SonicWall, gli access point wireless e gli switch Dell delle serie N e X attraverso un processo di workstream correlato e verificabile. Le imprese possono consolidare facilmente la gestione delle apparecchiature di sicurezza, ridurre la complessità amministrativa e di risoluzione dei problemi e gestire tutti gli aspetti operativi dell'infrastruttura di sicurezza, compresa la gestione e l'applicazione centralizzata delle politiche, il monitoraggio degli eventi in tempo reale, le attività degli utenti, l'identificazione delle applicazioni, l'analisi investigativa e dei flussi, la conformità e la reportistica di verifica e altro ancora. Inoltre, le imprese soddisfano i requisiti di gestione delle modifiche del firewall attraverso l'automazione del flusso di lavoro, che fornisce l'agilità e la sicurezza necessarie per implementare le giuste politiche del firewall al momento giusto e in conformità con le normative di compliance. Le soluzioni di gestione e reportistica di SonicWall, disponibili in versione on-premise come SonicWall Global Management System e in cloud come Capture Security Center, offrono un metodo coerente per gestire la sicurezza della rete in base ai processi aziendali e ai livelli di servizio, semplificando notevolmente la gestione del ciclo di vita degli ambienti di sicurezza nel loro insieme rispetto alla gestione dispositivo per dispositivo.

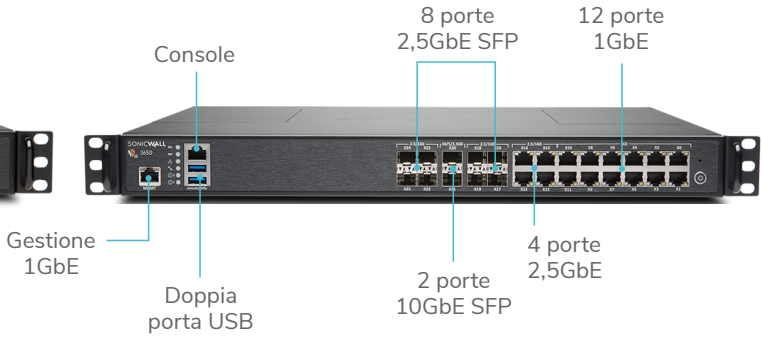
NSa 2650

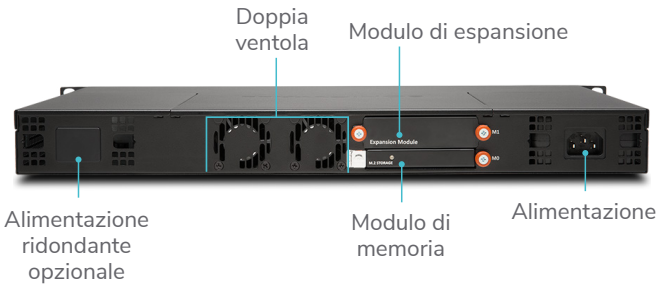
L'NSa 2650 offre prevenzione delle minacce ad alta velocità su migliaia di connessioni crittografate e su un numero ancora maggiore di connessioni non crittografate per organizzazioni di medie dimensioni e imprese distribuite.

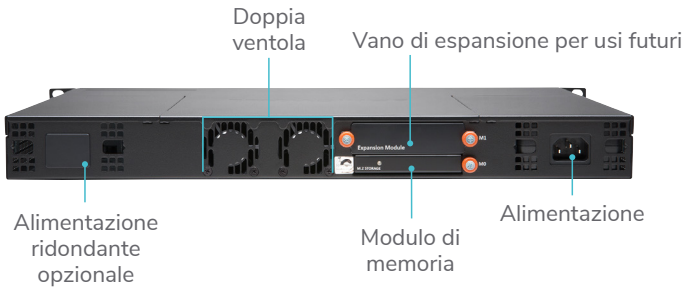
NSa 3650

Il SonicWall NSa 3650 è l'ideale per filiali e reti aziendali di piccole e medie dimensioni con l'esigenza di maggiori prestazioni e throughput.







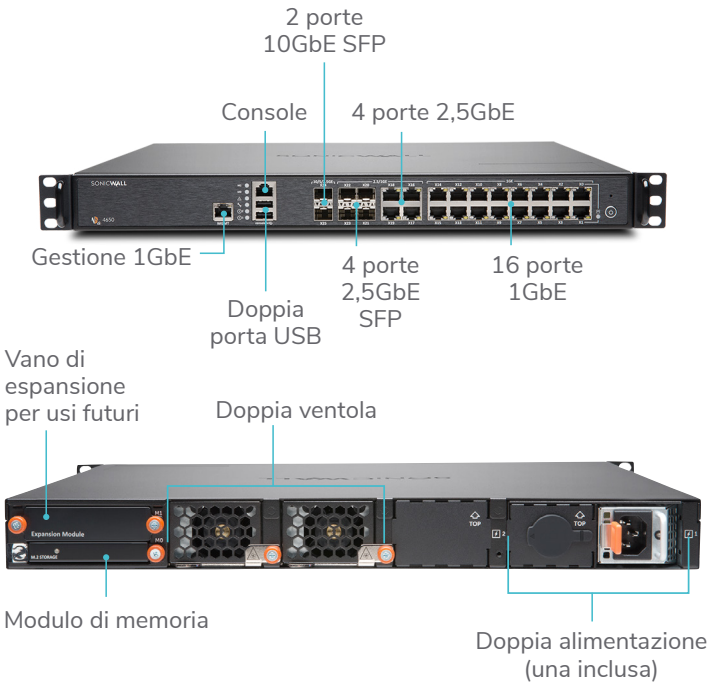


Firewall	NSa 2650
Throughput del firewall	3,0 Gbps
Throughput IPS	1,4 Gbps
Throughput antimalware	1,3 Gbps
Throughput di prevenzione delle minacce	1,5 Gbps
Numero massimo di connessioni	1.000.000
Nuove connessioni/sec	14.000/sec
Modulo di memoria	16 GB
Descrizione	**SKU**
Solo firewall NSa 2650	01-SSC-1936
NSa 2650 TotalSecure Advanced (1 anno)	01-SSC-1988

Firewall	NSa 3650
Throughput del firewall	3,75 Gbps
Throughput IPS	1,8 Gbps
Throughput antimalware	1,5 Gbps
Throughput di prevenzione delle minacce	1,75 Gbps
Numero massimo di connessioni	2.000.000
Nuove connessioni/sec	14.000/sec
Modulo di memoria	32 GB
Descrizione	**SKU**
Solo firewall NSa 3650	01-SSC-1937
NSa 3650 TotalSecure Advanced (1 anno)	01-SSC-4081

NSa 4650

SonicWall NSa 4650 garantisce la crescita di organizzazioni di medie dimensioni e sedi di filiali con funzionalità di livello imprenditoriale e prestazioni senza compromessi.



Firewall	NSa 4650
Throughput del firewall	6,0 Gbps
Throughput IPS	2,3 Gbps
Throughput antimalware	2,45 Gbps
Throughput di prevenzione delle minacce	2,5 Gbps
Numero massimo di connessioni	3.000.000
Nuove connessioni/sec	40.000/sec
Modulo di memoria	32 GB

Descrizione	SKU
Solo firewall NSa 4650	01-SSC-1938
NSa 4650 TotalSecure Advanced (1 anno)	01-SSC-4094

NSa 5650

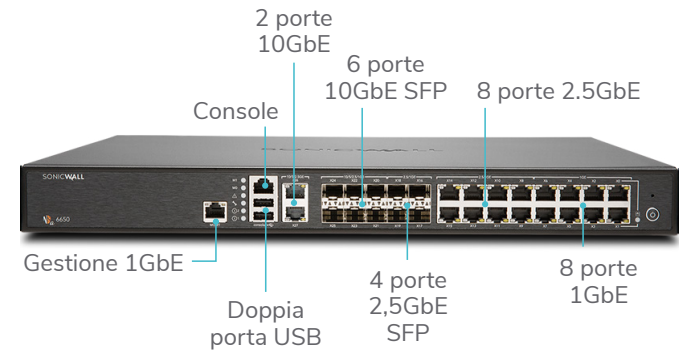
SonicWall NSa 5650 è l'ideale per ambienti distribuiti, filiali e aziendali che richiedono un throughput significativo e un'elevata densità di porte.

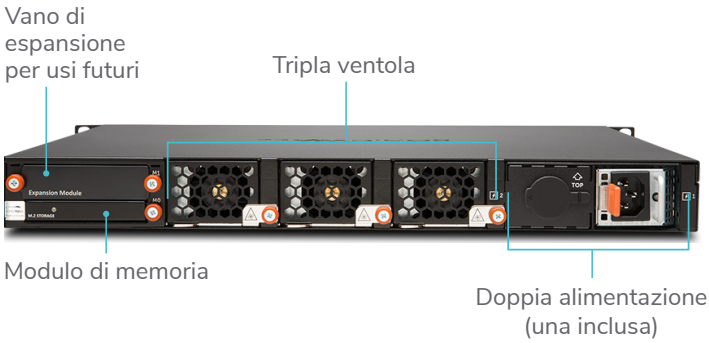
Firewall	NSa 5650
Throughput del firewall	6,25 Gbps
Throughput IPS	3,4 Gbps
Throughput antimalware	2,8 Gbps
Throughput di prevenzione delle minacce	3,4 Gbps
Numero massimo di connessioni	4.000.000
Nuove connessioni/sec	40.000/sec
Modulo di memoria	64 GB

Descrizione	SKU
Solo firewall NSa 5650	01-SSC-1939
NSa 5650 TotalSecure Advanced (1 anno)	01-SSC-4342

NSa 6650

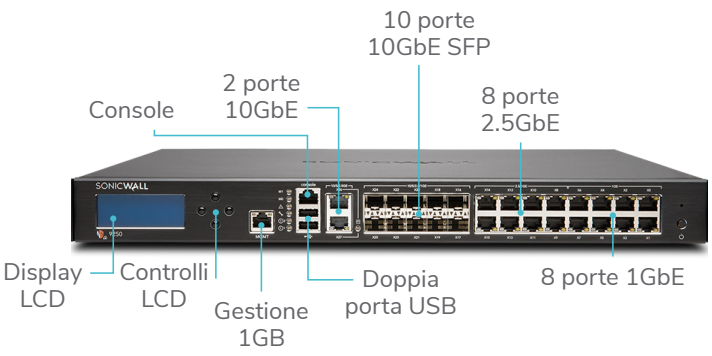
SonicWall NSa 6650 è ideale per grandi ambienti distribuiti e reti aziendali a gestione centralizzata che richiedono elevate prestazioni e grandi capacità di throughput.

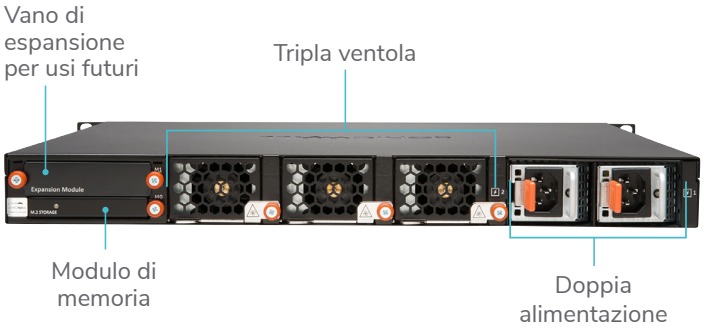




NSa 9250/9450/9650

SonicWall NSa 9250/9450/9650 offre scalabilità e sicurezza approfondita a velocità multi-gigabit per imprese distribuite e data center.





Firewall	NSa 6650
Throughput del firewall	12,0 Gbps
Throughput IPS	6,0 Gbps
Throughput antimalware	5,4 Gbps
Throughput di prevenzione delle minacce	5,5 Gbps
Numero massimo di connessioni	5.000.000
Nuove connessioni/sec	90.000/sec
Modulo di memoria	64 GB
Descrizione	**SKU**
Solo firewall NSa 6650	01-SSC-1940
NSa 6650 TotalSecure Advanced (1 anno)	01-SSC-2209

Firewall	NSa 9250	NSa 9450	NSa 9650
Throughput del firewall	12,0 Gbps	17,1 Gbps	17,1 Gbps
Throughput IPS	7,2 Gbps	10,2 Gbps	10,3 Gbps
Throughput antimalware	6,5 Gbps	8,0 Gbps	8,5 Gbps
Throughput di prevenzione delle minacce	6,5 Gbps	9,0 Gbps	9,4 Gbps
Numero massimo di connessioni	7.500.000	10.000.000	12.500.000
Nuove connessioni/sec	90.000/sec	130.000/sec	130.000/sec
Moduli di memoria	1 TB, 128 GB	1 TB, 128 GB	1 TB, 256 GB
Descrizione	**SKU**	**SKU**	**SKU**
Solo firewall NSa	01-SSC-1941	01-SSC-1942	01-SSC-1943
NSa TotalSecure Advanced (1 anno)	01-SSC-2854	01-SSC-4358	01-SSC-3475

Funzioni

ENGINE RFDPI

Funzione	Descrizione
Reassembly-Free Deep Packet Inspection (RFDPI)	Si tratta di un engine di ispezione proprietario, brevettato e di prestazioni elevate, che esegue analisi bidirezionali del traffico basate sui flussi senza proxy o buffering allo scopo di individuare tentativi di intrusione, rilevare malware e identificare il traffico delle applicazioni in qualsiasi porta.
Ispezione bidirezionale	Con la scansione contemporanea del traffico in ingresso e in uscita per il rilevamento delle minacce, questa opzione impedisce l'utilizzo della rete come vettore di malware e come piattaforma per sferrare attacchi qualora venga introdotto un computer infetto.
Ispezione basata sui flussi	La tecnologia di ispezione priva di proxy e buffering genera una latenza estremamente bassa per le attività di ispezione DPI su milioni di flussi di rete simultanei, senza limiti per la dimensione dei flussi e dei file. Inoltre può essere applicata sia a protocolli comuni, sia a flussi TCP primari.
Architettura altamente parallela e modulabile	L'esclusivo engine RFDPI basato su architettura multi-core consente un'elevata velocità di DPI e la creazione di nuove sessioni in tempi estremamente brevi, agevolando la gestione dei picchi di traffico in reti complesse.
Ispezione single-pass	Un'architettura DPI single-pass consente di rilevare contemporaneamente malware e intrusioni e identificare le applicazioni, riducendo notevolmente la latenza dell'ispezione DPI e correlando tutte le informazioni sulle minacce in un'unica architettura.

Funzione	Descrizione
SD-WAN sicura	SD-WAN sicura è una valida alternativa a tecnologie più costose come MPLS, che permette alle imprese distribuite di creare, utilizzare e gestire reti sicure ad alte prestazioni negli uffici remoti per condividere dati, applicazioni e servizi utilizzando servizi Internet pubblici prontamente disponibili e a basso costo.
API REST	Consentono al firewall di ricevere e sfruttare tutti i feed di intelligenza proprietari dei produttori di dispositivi originali e di terzi per contrastare minacce avanzate come zero-day, utenti malintenzionati, credenziali compromesse, ransomware e minacce persistenti avanzate.
Ispezione Stateful Packet	Tutto il traffico della rete viene ispezionato, esaminato e reso conforme alle politiche di accesso del firewall.
Alta disponibilità/clustering	La serie NSa supporta le modalità ad alta disponibilità Attivo/Passivo (A/P) con sincronizzazione dello stato, DPI Attivo/Attivo (A/A) e clustering Attivo/Attivo. La modalità DPI Attivo/Attivo trasferisce il carico di lavoro dell'ispezione deep packet ai core dell'appliance passiva per ottimizzare il throughput.
Protezione da attacchi DDoS/DoS	La protezione da flood SYN offre una difesa contro gli attacchi DoS mediante tecnologie di blacklisting al layer 3 (SYN proxy) e al layer 2 (SYN). Inoltre, protegge da DoS/DDoS attraverso la protezione da flood UDP/ICMP e la limitazione della velocità di connessione.
Supporto IPv6	Il protocollo IPv6 (Internet Protocol versione 6) è in procinto di sostituire il protocollo IPv4. Con SonicOS, l'hardware supporta il filtraggio e le implementazioni in modalità Wire.
Opzioni di implementazione flessibili	La serie NSa può essere installata nelle tradizionali modalità NAT, bridge Layer 2, Wire e Network Tap.
Bilanciamento del carico WAN	Bilancia il carico su più interfacce WAN con metodi basati sulle modalità round robin, percentuale o spill-over.
Qualità del servizio (QoS) avanzata	Garantisce l'integrità delle comunicazioni strategiche tramite tagging 802.1p e DSCP e rimappatura del traffico VoIP sulla rete.
Supporto gatekeeper H.323 e proxy SIP	Blocca le chiamate di spam richiedendo che tutte le chiamate in entrata siano autorizzate e autenticate dal gatekeeper H.323 o dal proxy SIP.
Gestione di switch N-Series e X-Series di Dell singoli e in cascata	Gestione delle impostazioni di sicurezza di porte aggiuntive, tra cui Portshield, HA, PoE e PoE+, attraverso un unico pannello di controllo utilizzando il dashboard di gestione del firewall per gli switch di rete serie N e serie X di Dell.
Autenticazione biometrica	Supporto dell'autenticazione per dispositivi mobili come il riconoscimento delle impronte digitali, che non può essere facilmente condivisa o duplicata, per autenticare in modo sicuro l'identità degli utenti che accedono alla rete.
Autenticazione aperta e social login	Consente agli utenti ospiti di utilizzare le loro credenziali da servizi di social network come Facebook, Twitter o Google+ per accedere a Internet e ad altri servizi come ospiti attraverso la rete wireless, la LAN o le zone DMZ di un host tramite autenticazione pass-through.

GESTIONE E REPORTISTICA

Funzione	Descrizione
Gestione basata sul cloud e in sede	La configurazione e la gestione delle apparecchiature SonicWall sono disponibili via cloud attraverso il SonicWall Capture Security Center e in sede tramite il SonicWall Global Management System (GMS).
Gestione avanzata con un unico dispositivo	Configurazione comoda e veloce tramite l'interfaccia web intuitiva, oltre a un'interfaccia CLI completa e al supporto per SNMPv2/3.
Report sul flusso delle applicazioni con IPFIX/ NetFlow	Le statistiche di traffico e i dati sull'uso delle applicazioni possono essere esportati tramite i protocolli IPFIX o NetFlow per il monitoraggio e la creazione di report in tempo reale e storici con strumenti come SonicWall Scrutinizer o altri che supportano IPFIX e NetFlow con estensioni.

RETE PRIVATA VIRTUALE (VPN)

Funzione	Descrizione
Provisioning automatico delle VPN	Semplifica l'installazione dei firewall in ambienti distribuiti complessi automatizzando il provisioning iniziale del gateway VPN da sede a sede tra i firewall SonicWall, garantendo l'applicazione istantanea e automatica della sicurezza e della connettività.
VPN IPSec per la connettività da sede a sede	La rete VPN IPSec ad alte prestazioni consente di utilizzare la serie NSa come concentratore di VPN per migliaia di utenti privati, filiali o altri siti di grandi dimensioni.
Accesso remoto tramite VPN SSL o client IPSec	Sfruttando la tecnologia VPN SSL senza client o un client IPSec semplice da gestire, è possibile accedere in tutta semplicità a messaggi di posta elettronica, file, computer, siti intranet e applicazioni da un'ampia serie di piattaforme.

Gateway per la rete VPN ridondante	Se si utilizzano più WAN, è possibile configurare una VPN principale e una secondaria per consentire failover e failback automatizzati e trasparenti per tutte le sessioni VPN.
VPN basata su routing	La possibilità di eseguire il routing dinamico tramite collegamenti VPN garantisce un'operatività continua anche in caso di guasto temporaneo al tunnel VPN, perché il traffico viene instradato senza interruzioni tra gli endpoint attraverso percorsi alternativi.

SENSIBILITÀ AL CONTESTO/AL CONTENUTO

Funzione	Descrizione
Tracciamento delle attività degli utenti	Per consentire il tracciamento delle attività e l'identificazione degli utenti le tecnologie AD/LDAP/Citrix1/Terminal Services 1 SSO integrate si combinano con le informazioni esaustive ricavate dall'ispezione DPI.
GeoIP per l'identificazione del traffico da determinati paesi	Con questa opzione è possibile identificare e controllare il traffico di rete in ingresso o in uscita da determinati paesi. Lo scopo è proteggere dagli attacchi provenienti da origini note o sospette di attività pericolose o analizzare il traffico sospetto che ha origine nella rete. Possibilità di creare elenchi personalizzati di paesi e botnet per ignorare il tag non corretto di un paese o una botnet associati a un indirizzo IP. Elimina il filtraggio non voluto degli indirizzi IP dovuto ad errata classificazione.
Filtro DPI con espressioni regolari	Questa opzione identifica e controlla i contenuti che attraversano la rete mediante la corrispondenza delle espressioni regolari per impedire perdite di dati. Consente di creare elenchi personalizzati di paesi e botnet per ignorare il tag non corretto di un paese o una botnet associati a un indirizzo IP.

Servizi in abbonamento per la prevenzione delle violazioni

CAPTURE ADVANCED THREAT PROTECTION

Funzione	Descrizione
Sandboxing multi-engine	La piattaforma sandbox multi-engine, che comprende l'emulazione completa del sistema e tecnologie di analisi a livelli hypervisor, esegue il codice sospetto nell'ambiente sandbox virtualizzato, ne analizza il comportamento e fornisce visibilità completa sulle attività dannose.
Real-Time Deep Memory Inspection (RTDMI)	Questa tecnologia basata su cloud, in attesa di brevetto, rileva e blocca i malware che non evidenziano comportamenti dannosi e nascondono il loro armamentario tramite crittografia. Forzando il malware a scoprire il suo armamentario nella memoria, l'engine RTDMI rileva e blocca in anticipo le minacce generalizzate, quelle zero-day ed i malware sconosciuti.
Blocco fino al verdetto	Per impedire l'ingresso di file potenzialmente dannosi nella rete, i file inviati al cloud per l'analisi possono essere trattenuti al gateway finché non viene determinata la loro natura.
Analisi di un'ampia gamma di tipi e dimensioni di file	Supporta l'analisi di un'ampia gamma di tipi di file, sia individualmente, sia come gruppo, compresi programmi eseguibili (PE), DLL, PDF, documenti MS Office, archivi, JAR e APK, oltre a svariati sistemi operativi, tra cui Windows, Android, Mac OS X e ambienti multi-browser.
Rapida distribuzione delle segnature	Quando un file è identificato come dannoso, viene immediatamente distribuita una segnatura ai firewall con abbonamento a SonicWall Capture ATP, ai database delle segnature per Gateway Anti-Virus e IPS, nonché ai database di URL, IP e reputazione dei domini nel giro di 48 ore.
Capture Client	Capture Client è una piattaforma client unificata che presenta numerose funzioni di protezione dell'endpoint, tra cui quella avanzata contro i malware e supporto per la visibilità del traffico crittografato. La piattaforma sfrutta tecnologie di protezione su più livelli, reporting completo e applicazione della protezione degli endpoint.

CAPTURE SECURITY APPLIANCE (CSa)

Funzione	Descrizione
Rilevamento del malware basato sulla conformità	Analizza i file sospetti direttamente nel proprio ambiente senza inviare il file con i risultati a cloud esterni.
Integrazioni preinstallate	CSa supporta integrazioni preinstallate con altre soluzioni di sicurezza (sicurezza firewall e posta elettronica) di SonicWall.
Protezione quasi in tempo reale	La tecnologia brevettata RTDMI di SonicWall aiuta a rilevare rapidamente il malware, anche quello sconosciuto, che può essere bloccato da CSa fino al verdetto di validazione sui firewall SonicWall di prossima generazione.
Installazione	CSa può essere configurato su reti private collegate direttamente a un unico edge firewall o essere raggiungibile direttamente da Internet o utilizzando VPN sui firewall delle filiali.

PREVENZIONE DELLE MINACCE CRITTOGRAFATE

Funzione	Descrizione
Decrittazione e ispezione TLS/SSL	Esegue la decrittazione e l'ispezione del traffico crittografato TLS/SSL in tempo reale, senza proxy, di malware, intrusioni e fughe di dati, e applica politiche di controllo di applicazioni, URL e contenuti per proteggere la rete dalle minacce nascoste nel traffico crittografato. Opzione compresa negli abbonamenti di sicurezza per tutti i modelli della serie NSa.
Ispezione SSH	La Deep Packet Inspection di SSH (DPI-SSH) esegue la decrittazione e l'ispezione dei dati che attraversano il tunnel SSH per prevenire gli attacchi che sfruttano SSH.

PREVENZIONE DELLE INTRUSIONI

Funzione	Descrizione
Protezione basata su contromisure	Il sistema di prevenzione delle intrusioni (IPS) integrato utilizza le segnature e altre contromisure per eseguire la scansione dei payload dei pacchetti in cerca di exploit e vulnerabilità, coprendo un'ampia serie di attacchi e vulnerabilità.
Aggiornamenti automatici delle segnature	Il team SonicWall Threat Research ricerca continuamente nuovi aggiornamenti e li installa in numerose contromisure IPS, che interessano oltre 50 categorie di attacchi. Gli aggiornamenti sono subito attivi senza la necessità di riavvii o interruzioni del servizio.
Protezione IPS interna alle zone	La segmentazione della rete in varie zone di sicurezza, protette dalle intrusioni, consente di potenziare la sicurezza interna poiché impedisce alle minacce di propagarsi oltre i confini di una zona.

Rilevamento e blocco di comando e controllo Botnet (CnC)	Questa opzione consente di individuare e bloccare il traffico di comando e controllo proveniente dai bot nella rete locale e diretto ai domini e agli indirizzi IP che sono stati identificati come fonte di propagazione di malware o punti CnC noti.
Anomalia/abuso di protocolli	Individua e blocca gli attacchi che sfruttano i protocolli noti per tentare di eludere il controllo IPS.
Protezione zero-day	Per proteggere la rete dagli attacchi zero-day, questa opzione assicura aggiornamenti costanti a fronte delle tecniche e dei metodi di exploit più recenti, coprendo migliaia di singoli exploit.
Tecnologia antievasione	La normalizzazione estesa dei flussi, la decodifica e altre tecniche assicurano che le minacce basate su tecniche di evasione ai livelli 2-7 non possano entrare in rete senza essere rilevate.

PREVENZIONE DELLE MINACCE

Funzione	Descrizione
Antimalware a livello gateway	L'engine RFDPI sottopone a scansione tutto il traffico in ingresso, in uscita e interno alle zone in cerca di virus, trojan, keylogger e altri malware, interessando file di dimensioni e lunghezza illimitate in tutte le porte e in tutti i flussi TCP.
Protezione Capture Cloud contro il malware	Un database residente sui server cloud SonicWall, costantemente aggiornato con decine di milioni di segnature delle minacce, viene consultato per ottimizzare le capacità del database di segnature integrato nel dispositivo, garantendo così un'ampia copertura delle minacce da parte dell'engine RFDPI.
Aggiornamenti di sicurezza costanti	I nuovi aggiornamenti sulle minacce vengono inviati automaticamente ai firewall sul campo con servizi di sicurezza attivi e sono subito attivi senza riavvii o interruzioni.
Ispezione bidirezionale dei TCP primari	L'engine RFDPI è in grado di scansionare flussi TCP primari in entrambe le direzioni su qualsiasi porta, bloccando gli attacchi che tentano di passare attraverso sistemi di sicurezza obsoleti, concepiti per proteggere solo poche porte note.
Ampio supporto di protocolli	Oltre a identificare i protocolli più comuni come HTTP/S, FTP, SMTP, SMBv1/v2 e altri, che non inviano dati nel TCP primario, questa opzione consente di decodificare i payload in cerca di malware, anche se non sono eseguiti in porte standard note.

INTELLIGENZA E CONTROLLO DELLE APPLICAZIONI

Funzione	Descrizione
Controllo delle applicazioni	Per potenziare la sicurezza e la produttività della rete vengono controllate le applicazioni, o le singole funzioni delle stesse, identificate dall'engine RFDPI utilizzando un database in continua espansione, contenente migliaia di segnature di applicazioni.
Identificazione di applicazioni personalizzate	Controlla le applicazioni personalizzate generando segnature basate su parametri specifici o su modelli di comunicazione in rete univoci per ogni applicazione, in modo da garantire un maggiore controllo sulla rete.
Gestione della larghezza di banda delle applicazioni	Il traffico delle applicazioni superflue viene bloccato, mentre la larghezza di banda disponibile viene regolamentata e allocata in modo granulare per le applicazioni o le categorie di applicazioni più importanti.
Controllo granulare	Consente di controllare le applicazioni o i componenti specifici di un'applicazione in base a pianificazioni, gruppi di utenti, elenchi di esclusione e una serie di attività con identificazione SSO degli utenti completa, mediante l'integrazione di LDAP/AD/Terminal Services/Citrix.

FILTRAGGIO DEI CONTENUTI

Funzione	Descrizione
Filtraggio dei contenuti interno/esterno	Mette in atto le politiche di utilizzo accettabili e blocca l'accesso a siti web HTTP/HTTPS contenenti informazioni o immagini discutibili o non produttive con Content Filtering Service e Content Filtering Client.
Enforced Content Filtering Client	Estende l'applicazione delle politiche per bloccare i contenuti Internet per dispositivi Windows, Mac OS, Android e Chrome situati all'esterno del perimetro del firewall.
Controlli granulari	L'uso di categorie predefinite o di una combinazione qualsiasi di categorie consente di bloccare determinati contenuti. Il filtraggio può essere pianificato in base all'ora del giorno, ad esempio durante l'orario scolastico o lavorativo, e applicato a gruppi o singoli utenti.
Cache Web	Le classificazioni degli URL sono memorizzate nella cache locale del firewall SonicWall, in modo che il tempo di risposta per l'accesso successivo ai siti web visitati con maggior frequenza sia inferiore a un secondo.

ANTIVIRUS E ANTISPYWARE APPLICATI

Funzione	Descrizione
Protezione su più livelli	Utilizza le funzioni del firewall come primo livello di difesa perimetrale, insieme alla protezione degli endpoint, per bloccare i virus che entrano nella rete tramite laptop, chiavette USB e altri sistemi non protetti.
Opzione di applicazione automatizzata	Assicura che ogni computer che accede alla rete abbia installato e attivato il software antivirus appropriato e/o il certificato DPI-SSL, eliminando i costi comunemente associati alla gestione dell'antivirus desktop.
Distribuzione e installazione automatizzate	La distribuzione e l'installazione macchina per macchina dei client antivirus e antispyware sono automatizzate sull'intera rete, il che riduce al minimo l'impegno amministrativo.
Antivirus di prossima generazione	Capture Client utilizza un engine statico di intelligenza artificiale (AI) per determinare le minacce prima che possano essere eseguite e per ripristinare uno stato precedente non infetto.
Protezione antispyware	La potente protezione contro gli spyware garantisce il massimo livello di prestazioni e sicurezza analizzando e bloccando i programmi spyware più diffusi e pericolosi, prima che questi possano carpire dati sensibili da computer fissi o portatili.

Riepilogo delle funzioni di SonicOS

Firewall

- Ispezione Stateful Packet
- Reassembly-Free Deep Packet Inspection
- Protezione da attacchi DDoS (UDP/ICMP/SYN flood)
- IPv4/IPv6
- Autenticazione biometrica per l'accesso remoto
- Proxy DNS
- API REST

Decrittazione e ispezione TLS/SSL/SSH[1]

- Deep Packet Inspection per TLS/SSL/SSH
- Inclusione/esclusione di oggetti, gruppi o nomi di host
- Controllo TLS/SSL
- Controlli DPI SSL granulari in base a zone o regole

Capture Advanced Threat Protection[1]

- Real-Time Deep Memory Inspection
- Analisi multi-engine basata sul cloud
- Sandbox virtuale
- Analisi a livello hypervisor
- Emulazione di sistema completa
- Ispezione di un'ampia varietà di file
- Invio automatizzato e manuale
- Intelligenza delle minacce con aggiornamenti in tempo reale
- Blocco fino al verdetto
- Capture Client

Prevenzione delle intrusioni[1]

- Scansione basata sulle segnature
- Aggiornamenti automatici delle segnature
- Ispezione bidirezionale
- Funzionalità per regole IPS granulari
- Implementazione GeoIP
- Filtraggio botnet con elenco dinamico
- Corrispondenza con espressioni regolari

Anti-malware[1]

- Scansione antimalware basata sui flussi
- Antivirus per gateway
- Antispyware per gateway
- Ispezione bidirezionale
- Nessun limite alle dimensioni dei file
- Database dei malware cloud

Identificazione delle applicazioni[1]

- Controllo delle applicazioni
- Gestione della larghezza di banda delle applicazioni
- Creazione di segnature per applicazioni personalizzate
- Prevenzione della perdita di dati
- Creazione di report sulle applicazioni tramite NetFlow/IPFIX
- Ampio database di segnature delle applicazioni

Visualizzazione e analisi del traffico

- Attività degli utenti
- Utilizzo applicazioni/larghezza di banda/minacce
- Analisi basate su cloud

Filtraggio dei contenuti HTTP/HTTPS Web[1]

- Filtraggio degli URL
- Proxy avoidance
- Blocco in base a parole chiave
- Filtraggio basato sulle politiche (esclusione/ inclusione)
- Inserimento intestazione HTTP
- Categorie di classificazione CFS per la gestione della larghezza di banda
- Modello di politica unificato con controllo delle applicazioni
- Content Filtering Client

VPN

- Provisioning automatico delle VPN
- VPN IPSec per la connettività da sede a sede
- VPN SSL e accesso remoto da client IPSec
- Gateway per la rete VPN ridondante
- Mobile Connect per iOS, Mac OS X, Windows, Chrome, Android e Kindle Fire
- VPN basata sul routing (OSPF, RIP, BGP)

Connettività di rete

- SD-WAN sicura
- PortShield
- Frame Jumbo
- Registrazione avanzata
- VLAN trunking
- RSTP (Rapid Spanning Tree Protocol)
- Port mirroring
- QoS layer 2
- Sicurezza delle porte
- Routing dinamico (RIP/OSPF/BGP)
- Controller wireless SonicWall
- Routing basato sulle politiche (ToS/metrico ed ECMP)
- NAT
- Sicurezza DNS
- Server DHCP
- Gestione della larghezza di banda
- Aggregazione dei link (statica e dinamica)
- Porte ridondanti
- Alta disponibilità A/P con sincronizzazione statica
- Clustering A/A
- Bilanciamento del carico in ingresso/in uscita
- Bridge L2, modalità wire/virtual wire, modalità tap, modalità tap
- Failover WAN 3G/4G
- Routing asimmetrico
- Supporto CAC (Common Access Card)

Wireless

- WIDS/WIPS
- Analisi dello spettro di RF
- Prevenzione di rogue AP
- Fast roaming (802.11k/r/v)
- Selezione automatica dei canali
- Visualizzazione in pianta/della topologia
- Band steering
- Beamforming
- AirTime Fairness
- MiFi Extender
- Quota ciclica ospite
- Portale ospite LHM

VoIP

- Controllo QoS granulare
- Gestione della larghezza di banda
- Trasformazioni SIP e H.323 per regola di accesso
- Supporto gatekeeper H.323 e proxy SIP

Gestione e monitoraggio

- Capture Security Center, GMS, Web UI, CLI, API REST, SNMPv2/v3
- Accesso
- Esportazione per Netflow/IPFix
- Backup della configurazione basato su cloud
- Piattaforma Security Analytics di BlueCoat
- Gestione access point SonicWall
- Gestione degli switch N-Series e X-Series di Dell inclusi gli switch a cascata

Archiviazione locale

- Log
- Reportistica
- Backup del firmware

[1]*Richiede un abbonamento aggiuntivo*

Specifiche di sistema della serie NSa

Firewall in generale	NSa 2650	NSa 3650	NSa 4650	NSa 5650
Sistema operativo	SonicOS 6.5.4			
Interfacce	4 x 2,5-GbE SFP, 4 x 2,5-GbE, 12 x 1-GbE, Gestione 1 GbE, 1 Console	2 x 10-GbE SFP+, 8 x 2,5-GbE SFP, 4 x 2,5-GbE, 12 x 1-GbE, Gestione 1 GbE, 1 Console	2 x 10-GbE SFP+, 4 x 2,5-GbE SFP, 4 x 2,5-GbE, 16 x 1-GbE, Gestione 1 GbE, 1 Console	2 x 10-GbE SFP+, 2 x 10-GbE, 4 x 2,5-GbE SFP, 4 x 2,5-GbE, 16 x 1-GbE, Gestione 1 GbE, 1 Console
Espansione	1 slot di espansione (sul retro)*			
Archiviazione integrata (SSD)	16 GB	32 GB	32 GB	64 GB
Gestione	CLI, SSH, Web UI, Capture Security Center, GMS, API REST			
Utenti SSO	40.000	50.000	60.000	70.000
Numero massimo di access point supportati	48	96	128	192
Accesso	Analyzer, Local Log, Syslog			
Prestazioni firewall/VPN	**NSa 2650**	**NSa 3650**	**NSa 4650**	**NSa 5650**
Throughput ispezione firewall[1]	3,0 Gbps	3,75 Gbps	6,0 Gbps	6,25 Gbps
Throughput di prevenzione delle minacce[2]	1,5 Gbps	1,75 Gbps	2,5 Gbps	3,4 Gbps
Throughput ispezione applicazioni[2]	1,85 Gbps	2,1 Gbps	3,0 Gbps	4,25 Gbps
Throughput IPS[2]	1,4 Gbps	1,8 Gbps	2,3 Gbps	3,4 Gbps
Throughput ispezione anti-malware[2]	1,3 Gbps	1,5 Gbps	2,45 Gbps	2,8 Gbps
Throughput decrittazione e ispezione TLS/SSL (SSL/DPI)[2]	300 Mbps	320 Mbps	675 Mbps	800 Mbps
Throughput VPN[3]	1,45 Gbps	1,5 Gbps	3,0 Gbps	3,5 Gbps
Connessioni al secondo	14.000/sec	14.000/sec	40.000/sec	40.000/sec
Numero massimo di connessioni (SPI)	1.000.000	2.000.000	3.000.000	4.000.000
Numero massimo di connessioni (DPI)	500.000	750.000	1.000.000	1.500.000
Numero massimo di connessioni (SSL DPI)	100.000/60.000	100.000/40.000	175.000/145.000	175.000/125.000
VPN	**NSa 2650**	**NSa 3650**	**NSa 4650**	**NSa 5650**
Tunnel site-to-site	1.000	3.000	4.000	6.000
Client VPN IPSec (max)	50 (1.000)	500 (3.000)	2.000 (4.000)	2.000 (6.000)
Client SSL VPN NetExtender (max)	2 (350)	2 (500)	2 (1.000)	2 (1.500)
Crittografia/Autenticazione	DES, 3DES, AES (128, 192, 256 bit), MD5, SHA-1, crittografia Suite B			
Scambio chiavi	Gruppi Diffie-Hellman 1, 2, 5, 14v			
VPN basata su routing	RIP, OSPF, BGP			
Connettività di rete	**NSa 2650**	**NSa 3650**	**NSa 4650**	**NSa 5650**
Assegnazione indirizzo IP	Statica (DHCP, PPPoE, L2TP e client PPTP), server DHCP interno, DHCP relay			
Modalità NAT	1:1, many:1, 1:many, NAT flessibile (IP sovrapposti), PAT, modalità trasparente			
Interfacce VLAN	256	256	400	500
Protocolli di routing	BGP, OSPF, RIPv1/v2, static route, routing basato sulle politiche			
Qualità del servizio (QoS)	Priorità della larghezza di banda, larghezza di banda massima, larghezza di banda garantita, contrassegno DSCP, 802.1p			
Autenticazione	LDAP (domini multipli), XAUTH/RADIUS, SSO, Novell, database utenti interno, Terminal Services, Citrix, Common Access Card (CAC)			
VoIP	H323-v1-5 completo, SIP			
Standard	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3			
Certificazioni (in corso)	ICSA Firewall, ICSA Anti-Virus, FIPS 140-2, Common Criteria NDPP (Firewall e IPS), UC APL, USGv6, CsFC			
Elevata disponibilità[5]	Attiva/Passiva con State Sync	Attiva/Passiva con State Sync Attiva/Attiva Clustering		Attivo/Passivo con sincronizzazione statica, Attivo/Attivo DPI con sincronizzazione statica, Attivo/Attivo Clustering
Hardware	**NSa 2650**	**NSa 3650**	**NSa 4650**	**NSa 5650**
Alimentazione	Doppia, ridondante 120W (una inclusa)		Doppia, ridondante 350W (una inclusa)	
Ventole	Doppia, fissa		Doppia, rimovibile	
Alimentazione in ingresso	100-240 Vca, 50-60 Hz			
Potenza max assorbita (W)	37,2	46	93,6	103,6
MTBF @25°C in ore	162.231	156.681	154.529	153.243
MTBF @25°C in anni	18,5	17,9	17,6	17,5
Fattore di forma	Montabile su rack 1U			
Dimensioni	43 x 32,5 x 4,5 cm		43 x 41,5 x 4,5 cm	
Peso	5,2 kg	5,3 kg	6,9 kg	6,9 kg
Peso RAEE	5,5 kg	5,6 kg	8,9 kg	8,9 kg
Peso con la confezione	7,7 kg	7,8 kg	11,3 kg	11,3 kg
Principali normative di conformità	FCC Classe A, ICES Classe A, CE (EMC, LVD, RoHS), C-Tick, VCCI Classe A, UL/cUL, TUV/GS, CB, CoC UL (Messico), RAEE, REACH, BSMI, KCC/MSIP, ANATEL			
Condizioni ambientali (in funzionamento/ stoccaggio)	0-40 °C / -40 - 70 °C			
Umidità	10-90%, non condensante			

Specifiche di sistema della serie NSa (cont.)

Firewall in generale	NSa 6650	NSa 9250	NSa 9450	NSa 9650
Sistema operativo	SonicOS 6.5.4			
Interfacce	6 x 10-GbE SFP+, 2 x 10-GbE, 4 x 2,5-GbE SFP, 8 x 2,5-GbE, 8 x 1-GbE, Gestione 1 GbE, 1 Console	10 x 10-GbE SFP+, 2 x 10-GbE, 8 x 2,5-GbE, 8 x 1-GbE, Gestione 1 GbE, 1 Console	10 x 10-GbE SFP+, 2 x 10-GbE, 8 x 2,5-GbE, 8 x 1-GbE, Gestione 1 GbE, 1 Console	10 x 10-GbE SFP+, 2 x 10-GbE, 8 x 2,5-GbE, 8 x 1-GbE, Gestione 1 GbE, 1 Console
Espansione	1 slot di espansione (sul retro)*			
Archiviazione integrata (SSD)	64 GB	1TB, 128 GB	1TB, 128 GB	1TB, 256 GB
Gestione	CLI, SSH, Web UI, Capture Security Center, GMS, API REST	CLI, SSH, Web UI, GMS, API REST		
Utenti SSO	70.000	80.000	90.000	100.000
Numero massimo di access point supportati	192	192	192	192
Accesso	Analyzer, Local Log, Syslog, IPFIX, NetFlow			
Prestazioni firewall/VPN	**NSa 6650**	**NSa 9250**	**NSa 9450**	**NSa 9650**
Throughput ispezione firewall[1]	12,0 Gbps	12,0 Gbps	17,1 Gbps	17,1 Gbps
Throughput di prevenzione delle minacce[2]	5,5 Gbps	6,5 Gbps	9,0 Gbps	9,4 Gbps
Throughput ispezione applicazioni[2]	6,0 Gbps	7,8 Gbps	10,8 Gbps	11,5 Gbps
Throughput IPS[2]	6,0 Gbps	7,2 Gbps	10,2 Gbps	10,3 Gbps
Throughput ispezione anti-malware[2]	5,4 Gbps	6,5 Gbps	8,0 Gbps	8,5 Gbps
Throughput decrittazione e ispezione TLS/SSL (SSL/DPI)[2]	1,45 Gbps	1,5 Gbps	2,1 Gbps	2,25 Gbps
Throughput VPN[3]	6,0 Gbps	6,75 Gbps	10,0 Gbps	10,0 Gbps
Connessioni al secondo	90.000/sec	90.000/sec	130.000/sec	130.000/sec
Numero massimo di connessioni (SPI)	5.000.000	7.500.000	10.000.000	12.500.000
Numero massimo di connessioni (DPI)	2.000.000	3.000.000	4.000.000	5.000.000
Numero massimo di connessioni (SSL DPI)	250.000/170.000	250.000/170.000	450.000/290.000	550.000/320.000
VPN	**NSa 6650**	**NSa 9250**	**NSa 9450**	**NSa 9650**
Tunnel site-to-site	8.000	12.000	12.000	12.000
Client VPN IPSec (max)	2.000 (6.000)	2.000 (6.000)	2.000 (6.000)	2.000 (6.000)
Client SSL VPN NetExtender (max)	2 (2.000)	2 (3.000)	2 (3.000)	50 (3.000)
Crittografia/Autenticazione	DES, 3DES, AES (128, 192, 256 bit), MD5, SHA-1, crittografia Suite B			
Scambio chiavi	Gruppi Diffie-Hellman 1, 2, 5, 14v			
VPN basata su routing	RIP, OSPF, BGP			
Connettività di rete	**NSa 6650**	**NSa 9250**	**NSa 9450**	**NSa 9650**
Assegnazione indirizzo IP	Statica (DHCP, PPPoE, L2TP e client PPTP), server DHCP interno, DHCP relay			
Modalità NAT	1:1, many:1, 1:many, NAT flessibile (IP sovrapposti), PAT, modalità trasparente			
Interfacce VLAN	512			
Protocolli di routing	BGP, OSPF, RIPv1/v2, static route, routing basato sulle politiche			
Qualità del servizio (QoS)	Priorità della larghezza di banda, larghezza di banda massima, larghezza di banda garantita, contrassegno DSCP, 802.1p			
Autenticazione	LDAP (domini multipli), XAUTH/RADIUS, SSO, Novell, database utenti interno, Terminal Services, Citrix, Common Access Card (CAC)			
VoIP	H323-v1-5 completo, SIP			
Standard	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3			
Certificazioni (in corso)	ICSA Firewall, ICSA Anti-Virus, FIPS 140-2, Common Criteria NDPP (Firewall e IPS), UC APL, USGv6, CsFC			
Elevata disponibilità[5]	Attivo/Passivo con sincronizzazione statica, Attivo/Attivo DPI con sincronizzazione statica, Attivo/Attivo Clustering			
Hardware	**NSa 6650**	**NSa 9250**	**NSa 9450**	**NSa 9650**
Alimentazione	Doppia, ridondante 350W (una inclusa)	Doppia, ridondante, 350W		
Ventole	Tripla, rimovibile			
Alimentazione in ingresso	100-240 Vca, 50-60 Hz			
Potenza max assorbita (W)	144,3	86,7	90,9	113,1
MTBF @25°C in ore	157.193	139.783	134.900	116.477
MTBF @25°C in anni	17,9	15,96	15,4	13,3
Fattore di forma	Montabile su rack 1U			
Dimensioni	43 x 41,5 x 4,5 cm			
Peso	8,1 kg	8,1 kg		
Peso RAEE	10,2 kg	10,2 kg		
Peso con la confezione	12,6 kg	12,6 kg		
Principali normative di conformità	FCC Classe A, ICES Classe A, CE (EMC, LVD, RoHS), C-Tick, VCCI Classe A, UL, cUL, TÜV/GS, CB, CoC UL (Messico), RAEE, REACH, ANATEL, BSMI			
Condizioni ambientali (in funzionamento/ stoccaggio)	0-40 °C / -40 - 70 °C			
Umidità	10-90%, non condensante			

[1] Metodologie di test: Prestazioni massime come da RFC 2544 (per il firewall). Le prestazioni effettive possono variare a seconda delle condizioni di rete e dei servizi attivati.
[2] Rilevazione throughput per prevenzione minacce/Gateway AV/Anti-Spyware/IPS tramite il test di performance Spirent WebAvalanche HTTP standard nell'industria e gli strumenti di test Ixia. Il test viene eseguito con più flussi attraverso varie coppie di porte. Rilevazione throughput di prevenzione delle minacce con Gateway AV, Anti-Spyware, IPS e Application Control attivati. Prestazioni DPI SSL misurate sul traffico HTTPS con IPS attivato.
[3] Throughput VPN misurato mediante il traffico UDP con pacchetti di 1.280 byte in base al valore RFC 2544. Tutte le specifiche, le funzioni e le informazioni sulla disponibilità sono soggette a modifiche.
[4] Ogni 125.000 connessioni DPI ridotte, il numero di connessioni DPI SSL disponibili aumenta di 3.000, tranne che per NSa 9250 e superiore.
[5] Clustering attivo/attivo e DPI attiva/attiva con State Sync richiedono l'acquisto della licenza estesa, tranne che per NSa 9250 e superiori.
**Uso futuro. Tutte le specifiche, le funzioni e le informazioni sulla disponibilità sono soggette a modifiche.*

Informazioni per l'ordinazione della serie NSa

NSa 2650	SKU
NSa 2650 TotalSecure Advanced Edition (1 anno)	01-SSC-1988
Advanced Gateway Security Suite – Capture ATP, Threat Prevention e assistenza 24x7 per NSa 2650 (1 anno)	01-SSC-1783
Capture Advanced Threat Protection per NSa 2650 (1 anno)	01-SSC-1935
Threat Prevention–Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus per NSa 2650 (1 anno)	01-SSC-1976
Assistenza 24x7 per NSa 2650 (1 anno)	01-SSC-1541
Content Filtering Service per NSa 2650 (1 anno)	01-SSC-1970
Capture Client	In base al numero di utenti
Servizio completo antispam per NSa 2650 (1 anno)	01-SSC-2001

NSa 3650	SKU
NSa 3650 TotalSecure Advanced Edition (1 anno)	01-SSC-4081
Advanced Gateway Security Suite – Capture ATP, Threat Prevention e assistenza 24x7 per NSa 3650 (1 anno)	01-SSC-3451
Capture Advanced Threat Protection per NSa 3650 (1 anno)	01-SSC-3457
Threat Prevention–Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus per NSa 3650 (1 anno)	01-SSC-3632
Assistenza 24x7 per NSa 3650 (1 anno)	01-SSC-3439
Content Filtering Service per NSa 3650 (1 anno)	01-SSC-3469
Capture Client	In base al numero di utenti
Servizio completo antispam per NSa 3650 (1 anno)	01-SSC-4030

NSa 4650	SKU
NSa 4650 TotalSecure Advanced Edition (1 anno)	01-SSC-4094
Advanced Gateway Security Suite – Capture ATP, Threat Prevention e assistenza 24x7 per NSa 4650 (1 anno)	01-SSC-3493
Capture Advanced Threat Protection per NSa 4650 (1 anno)	01-SSC-3499
Threat Prevention–Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus per NSa 4650 (1 anno)	01-SSC-3589
Assistenza 24x7 per NSa 4650 (1 anno)	01-SSC-3487
Content Filtering Service per NSa 4650 (1 anno)	01-SSC-3583
Capture Client	In base al numero di utenti
Servizio completo antispam per NSa 4650 (1 anno)	01-SSC-4062

NSa 5650	SKU
NSa 5650 TotalSecure Advanced Edition (1 anno)	01-SSC-4342
Advanced Gateway Security Suite – Capture ATP, Threat Prevention e assistenza 24x7 per NSa 5650 (1 anno)	01-SSC-3674
Capture Advanced Threat Protection per NSa 5650 (1 anno)	01-SSC-3680
Threat Prevention – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus per NSa 5650 (1 anno)	01-SSC-3698
Assistenza 24x7 per NSa 5650 (1 anno)	01-SSC-3660
Content Filtering Service per NSa 5650 (1 anno)	01-SSC-3692
Capture Client	In base al numero di utenti
Servizio completo antispam per NSa 5650 (1 anno)	01-SSC-4068

NSa 6650	SKU
NSa 6650 TotalSecure Advanced Edition (1 anno)	01-SSC-2209
Advanced Gateway Security Suite – Capture ATP, Threat Prevention e assistenza 24x7 per NSa 6650 (1 anno)	01-SSC-8761
Capture Advanced Threat Protection per NSa 6650 (1 anno)	01-SSC-8930
Threat Prevention – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus per NSa 6650 (1 anno)	01-SSC-8979
Assistenza 24x7 per NSa 6650 (1 anno)	01-SSC-8663
Content Filtering Service per NSa 6650 (1 anno)	01-SSC-8972
Capture Client	In base al numero di utenti
Servizio completo antispam per NSa 6650 (1 anno)	01-SSC-9131

NSa 9250	SKU
NSa 9250 TotalSecure Advanced Edition (1 anno)	01-SSC-2854
Advanced Gateway Security Suite – Capture ATP, Threat Prevention e assistenza 24x7 per NSa 9250 (1 anno)	01-SSC-0038
Capture Advanced Threat Protection per NSa 9250 (1 anno)	01-SSC-0121
Threat Prevention – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus per NSa 9250 (1 anno)	01-SSC-0343
Assistenza 24x7 per NSa 9250 (1 anno)	01-SSC-0032
Content Filtering Service per NSa 9250 (1 anno)	01-SSC-0331
Capture Client	In base al numero di utenti

Informazioni per l'ordinazione della serie NSa (cont.)

NSa 9450	SKU
NSa 9450 TotalSecure Advanced Edition (1 anno)	01-SSC-4358
Advanced Gateway Security Suite – Capture ATP, Threat Prevention e assistenza 24x7 per NSa 9450 (1 anno)	01-SSC-0414
Capture Advanced Threat Protection per NSa 9450 (1 anno)	01-SSC-0855
Threat Prevention – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus per NSa 9450 (1 anno)	01-SSC-1196
Assistenza 24x7 per NSa 9450 (1 anno)	01-SSC-0407
Content Filtering Service per NSa 9450 (1 anno)	01-SSC-1158
Capture Client	In base al numero di utenti

NSa 9650	SKU
NSa 9650 TotalSecure Advanced Edition (1 anno)	01-SSC-3475
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, assistenza 24x7 per NSa 9650 (1 anno)	01-SSC-2036
Capture Advanced Threat Protection per NSa 9650 (1 anno)	01-SSC-2042
Threat Prevention – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus per NSa 9650 (1 anno)	01-SSC-2142
Assistenza 24x7 per NSa 9650 (1 anno)	01-SSC-1989
Content Filtering Service per NSa 9650 (1 anno)	01-SSC-2136
Capture Client	In base al numero di utenti

Moduli e accessori*	SKU
Modulo a corto raggio (Short Reach) 10GBASE-SR SFP+	01-SSC-9785
Modulo a lungo raggio (Long Reach) 10GBASE-LR SFP+	01-SSC-9786
Cavo Twinax 10GBASE SFP+ 1M	01-SSC-9787
Cavo Twinax 10GBASE SFP+ 3M	01-SSC-9788
Modulo a corta distanza (Short Haul) 1000BASE-SX SFP	01-SSC-9789
Modulo a lunga distanza (Long Haul) 1000BASE-LX SFP	01-SSC-9790
Modulo in rame 1000BASE-T SFP	01-SSC-9791

**Per l'elenco completo dei moduli SFP e SFP+ supportati rivolgersi ai rivenditori locali SonicWall*

Offerta abbinata firewall SonicWall NSa/NSv

I seguenti firewall della serie NSa hanno diritto ad una licenza annuale gratuita sul corrispondente abbonamento NSv Virtual Appliance TotalSecure*.

Firewall NSa	NSv Firewall corrispondente
NSa 5650	NSv 200
NSa 6650	NSv 200
NSa 9250	NSv 400
NSa 9450	NSv 400
NSa 9650	NSv 400

** L'abbonamento NSv Virtual Appliance TotalSecure comprende NSv virtual firewall, Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention and Application Firewall Service, Content Filtering Service e assistenza 24x7.*

Codici RMN:

NSa 2650 - 1RK38-0C8
NSa 3650 - 1RK38-0C7
NSa 4650 - 1RK39-0C9
NSa 5650 - 1RK39-0CA
NSa 6650 - 1RK39-0CB
NSa 9250 - 1RK39-0CC
NSa 9450 - 1RK39-0CD
NSa 9650 - 1RK39-0CE

Servizi attivati dai partner

Serve aiuto per pianificare, installare od ottimizzare la soluzione SonicWall? I SonicWall Advanced Services Partner hanno seguito corsi di formazione per fornire servizi professionali di livello mondiale. Ulteriori informazioni sul sito www.sonicwall.com/PES.

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 www.sonicwall.com

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

Datasheet-NetworkSecurityAppliance-COG-2464