BOUNDLESS CYBERSECURITY

# 2021 LINEA DI PRODOTTI

## Edizione autunnale

SONICWALL®

# Linee di prodotti SonicWall: in sintesi

**Firewall di prossima generazione**
**Fascia alta: Serie NS*sp***
Firewall multi-istanza progettato per grandi imprese distribuite, data center e fornitori di servizi di sicurezza gestiti (MSSP) che si contraddistinguono per la protezione ad alta velocità, l'alta densità di porte e l'isolamento vero dei tenant con la Unified Policy.

**Fascia media: Serie NS*a***
Efficacia e prestazioni di sicurezza riconosciute a livello industriale per reti di medie dimensioni, filiali e aziende distribuite.

**Entry Level: Serie TZ**
Prevenzione delle minacce e piattaforma SD-WAN integrate per chi lavora da casa e presso PMI e SD-Branch.

**Virtuale: Serie NS*v***
Firewall virtuali con modelli di licenza flessibili per proteggere tutti i componenti critici delle infrastrutture cloud pubbliche e private.

**Sicurezza wireless**
**Serie SonicWave**
Sicurezza e prestazioni appositamente studiate per i dispositivi wireless di prossima generazione, gestiti tramite cloud o firewall.

**Serie SMA**
Accesso semplice e sicuro, basato sulle politiche, alle risorse di rete e nel cloud.

**Switch SonicWall**
Garantisce la commutazione intelligente per la connettività sicura di prossima generazione per PMI e SD-Branch.

**Serie ESA**
Una soluzione di protezione multilivello contro le minacce avanzate trasmesse per posta elettronica disponibile come apparecchiatura fisica, VM o SaaS in cloud.

**Capture Security appliance (CS*a*)**
Verifica dei file e prevenzione dei malware effettuate internamente.

**Gestione e analisi**
**Capture Security Center**
**Global Management System (GMS)**
**Network Security Manager**
**Wireless Network Manager**
Il controllo e la conoscenza della rete sono fondamentali per la sicurezza.

**Capture Client**

Una piattaforma client unificata con un pannello di controllo globale che mette a disposizione funzioni di protezione dell'endpoint, tra cui protezione avanzata dai malware, sandboxing, intelligence delle vulnerabilità delle applicazioni e ripristino allo stato precedente in caso di infezione.

**Cloud Edge Secure Access**
Una potente applicazione SaaS con semplici funzioni network-as-a-service per connettività site-to-site e cloud ibrido per AWS, Azure e Google Cloud, che abbina gli approcci alla sicurezza Zero-Trust e Least-Privilege in un'unica offerta integrata.

**Cloud App Security**
Una soluzione nativa per il cloud con la sicurezza di prossima generazione delle applicazioni SaaS come Office 365 e G Suite, per la protezione della posta elettronica, dei dati e delle credenziali utente contro le minacce avanzate, garantendo al tempo stesso la conformità nel cloud.

**Servizi in abbonamento firewall di prossima generazione**
**Threat Protection Service Suite** comprende i servizi di sicurezza di base necessari per garantire che la rete sia protetta dalle minacce in un unico pacchetto che si caratterizza per il valido rapporto qualità-prezzo. Disponibile solo per la serie TZ270/370/470, il pacchetto comprende antivirus per gateway, prevenzione delle intrusioni e controllo delle applicazioni, servizio di filtraggio del contenuti, visibilità della rete e assistenza 24x7.

**Essential Protection Services Suite** fornisce tutti i servizi di sicurezza essenziali necessari per la protezione dalle minacce note e sconosciute. La soluzione comprende Capture Advanced Threat Protection con tecnologia RTDMI, antivirus sul gateway, prevenzione delle intrusioni e controllo delle applicazioni, servizio di filtraggio dei contenuti, servizio antispam .

**Advanced Protection Services Suite** contiene tutti i servizi di protezione per la sicurezza avanzata della rete. Il pacchetto comprende i servizi Essential più la gestione del cloud e la reportistica basata sul cloud per 7 giorni.

**Advanced Gateway Security Suite (AGSS)** è disponibile come servizio aggiuntivo per tutti i firewall SonicWall fisici e virtuali, per la protezione dalle minacce più avanzate e sconosciute.

Compresi nella Advanced Gateway Security Suite (AGSS); abbinati al firewall di prossima generazione nell'edizione TotalSecure Advanced

- Capture Advanced Threat Protection (ATP), la sandbox multiengine basata sul cloud
- Antivirus e Antispyware sul gateway
- Servizio di prevenzione delle intrusioni
- Controllo delle applicazioni
- Servizio di filtraggio dei contenuti e del web
- Supporto 24x7

**Security-as-a-Service (SECaaS)**
La nostra soluzione chiavi in mano per gestire la sicurezza di rete in outsourcing.

*Per ulteriori informazioni su sonicwall.com*

# Domande di valutazione

## Firewall di prossima generazione

- Siete in grado di restare al passo con l'aumento della larghezza di banda risultante che comporta esigenze prestazionali gigabit o multi-gigabit?
- Il vostro firewall attuale è in grado di eseguire l'ispezione delle minacce alla velocità delle minacce in arrivo?
- Quali sono i vostri criteri per quanto riguarda i requisiti prestazionali?
- Numero totale di utenti e reti dietro al firewall?
- Numero totale di sessioni e di connessioni in condizioni di picco?
- Quanti siti e utenti remoti si collegheranno al firewall?
- Come misurate l'efficacia dei vostri controlli di sicurezza?
- Che tipo di connessione Internet utilizzate? Con quale velocità?
- Quali misure adottate per proteggervi da nuove minacce come gli attacchi zero-day?
- La vostra sandbox è in grado di rilevare e bloccare le minacce nascoste in profondità nella memoria?
- Quanti engine sono integrati nella sandbox?
- La vostra sandbox è in grado di trattenere i file sospetti sul gateway prima che vengano trasferiti?
- Sapete se il firewall della vostra azienda ispeziona il traffico HTTPS?
- Avete subito interruzioni del servizio di rete o tempi morti durante l'ispezione del traffico HTTPS?
- Il vostro firewall virtuale è affidabile quanto il firewall fisico?
- Come proteggete i vostri ambienti cloud pubblici o privati?
- Siete in grado di attuare zone di sicurezza adeguate e la microsegmentazione sulla vostra rete virtuale?
- Avete una visibilità e un controllo completi del vostro traffico virtuale?
- Vi interesserebbe ridurre i costi, sostituendo MPLS con SD-WAN per creare una rete privata sicura?

## Capture Client

- I vostri endpoint richiedono una protezione avanzata costante contro il ransomware e le minacce crittografate?
- Siete in grado di applicare la conformità alle politiche e la gestione delle licenze a tutti gli endpoint?
- Avete difficoltà a tenere sotto controllo gli endpoint e a gestire l'infrastruttura di sicurezza?
- Il vostro prodotto di protezione degli endpoint è collegato a un ambiente sandbox?
- Siete in grado di catalogare le applicazioni installate sugli endpoint e di sapere quante vulnerabilità sono presenti al loro interno?
- La vostra soluzione attuale effettua il monitoraggio costante dello stato del vostro sistema?
- Siete in grado di ripristinare uno stato precedente non compromesso in caso di danni provocati dal ransomware?
- Con quale rapidità è possibile aggiungere o modificare le politiche per i tenant?

## Cloud App Security

- Utilizzate O365 o G Suite?
- Utilizzate Proofpoint o Mimecast per la sicurezza di O365/G Suite?
- Effettuate la scansione dei messaggi di posta elettronica O365 interni?
- Quante applicazioni SaaS sanzionate utilizza la vostra organizzazione?
- Avete difficoltà a garantire la conformità per i dati memorizzati nelle applicazioni SaaS?
- Come fate a sapere se le vostre credenziali utente sono state compromesse?
- Riuscite a sapere chi accede ai dati, da dove e quando? (BYOD)

## Analisi approfondita della memoria

SonicWall RTDMI™ (Real-Time Deep Memory Inspection), una tecnologia in attesa di brevetto, individua e blocca in anticipo il malware sconosciuto tramite l'ispezione approfondita della memoria in tempo reale. Ora disponibile con Capture Advanced Threat Protection (ATP), il servizio di sandboxing nel cloud di SonicWall, questo engine identifica e mitiga le attuali minacce - anche quelle più insidiose - tra cui i futuri exploit Meltdown.

## Serie SonicWave

- I vostri dipendenti, partner o clienti si lamentano della lentezza della rete Wi-Fi?
- Quale sarebbe il numero massimo di utenti wireless possibile in un qualsiasi momento?
- Vi preoccupano i costi necessari per aggiungere una soluzione wireless sicura alla vostra rete?
- Conoscete lo standard wireless 802.11ac Wave 2?
- Vi serve flessibilità per gestire gli access point - cloud rispetto alla gestione dei firewall?
- Avete pianificato la rete Wi-Fi in modo efficace?
- Avete bisogno di scollegare gli AP dai firewall?
- Avete problemi a configurare le funzioni di sicurezza avanzate nella rete Wi-Fi?
- I servizi per gli ospiti sono importanti per voi?
- Avete bisogno di un portale di accesso personalizzato per la presa in carico dell'ospite?

## Switch SonicWall

- Servono access switch capaci con prestazioni gigabit per alimentare dispositivi compatibili PoE?
- È importante per voi un'unica postazione di sicurezza con visibilità e gestione unificate?
- Avete problemi a livello di soluzioni con gli switch di terzi che funzionano con l'ecosistema di SonicWall?

## Secure Mobile Access

- Qual è la vostra attuale strategia di accesso per chi utilizza il telelavoro?
- Che cosa ne pensate dell'adozione di un approccio di accesso alla rete di tipo zero-trust?
- In che modo fornite agli utenti un accesso sicuro alle risorse aziendali e alle applicazioni interne e a quelle nel cloud?
- Avete la visibilità su qualsiasi utente e su qualsiasi dispositivo che accede alla vostra rete?
- Quale strategia utilizzate attualmente per proteggere le vostre proprietà web e i server web strategici?

## Sicurezza della posta elettronica

- Vi preoccupano le minacce avanzate diffuse tramite posta elettronica, come ransomware, spear-phishing e compromissione delle email aziendali (BEC)?
- La vostra attuale soluzione di sicurezza della posta elettronica dispone di funzioni di protezione contro le minacce avanzate?
- Vi preoccupa la possibilità che messaggi di posta elettronica contenenti informazioni riservate possano essere divulgati?
- La vostra azienda è in regola con le normative GDPR, Sarbanes-Oxley, GLBA o HIPAA?
- Siete interessati ad offrire ai clienti servizi gestiti per la sicurezza della posta elettronica? (MSSP)

## Gestione e analisi

- Quali problemi potreste risolvere unificando le vostre soluzioni di sicurezza in una piattaforma di gestione comune, dotata di un unico pannello di controllo?
- Quali vantaggi operativi otterreste se foste in grado di gestire centralmente tutti i firewall, gli access point e gli switch da qualsiasi sede utilizzando una consolle nel cloud?
- Quanto siete certi di poter dimostrare la conformità a norme di sicurezza informatica come PCI, HIPPA e GDPR?
- Come cambierebbe il vostro approccio alla sicurezza se foste in grado di rilevare e reagire alle minacce e ai rischi in modo migliore, più rapido e preciso?
- Quali vantaggi otterrebbero la vostra azienda e la dirigenza da una visibilità completa delle minacce informatiche e dei rischi per la vostra attività?

## Cloud Edge Secure Access

- Gestite molti dati sensibili? Vi preoccupano gli utenti con privilegi eccessivi?
- Vi preoccupano le crescenti normative sulla protezione dei dati e sulla sicurezza delle informazioni?
- Avete bisogno di controllare le interazioni tra dipendenti, partner commerciali esterni e risorse sensibili?
- Quante filiali avete? Quanto sono efficaci le vostre procedure di presa in carico delle nuove filiali?
- Quanto tempo occorre per poter prendere in carico in condizioni di sicurezza un utente remoto?


Datasheet-SonicWallProductLineAtAGlance-A4-VG-4116

SONICWALL®

# Firewall sizing guide

| | | TZ APPLIANCES | | | | |
|---|---|---|---|---|---|---|
| | | TZ270 | TZ370 | TZ470 | TZ570 | TZ670 |
| Firmware | | SonicOS 7 | SonicOS 7 | SonicOS 7 | SonicOS 7 | SonicOS 7 |
| Interfaces | 1 GbE copper | 8 | 8 | 8 | 8 | 8 |
| | 2.5 GbE copper | | | | | |
| | 1 GbE SFP | | | | | |
| | 2.5 GbE SFP | | | 2 | | |
| | 2.5 GbE SFP+ | | | | | |
| | 5 GbE SFP | | | | 2 | |
| | 10 GbE | | | | | |
| | 10 GbE SFP+ | | | | | 2 |
| | 28 GbE SFP+ | | | | | |
| | 40 GbE QSFP+ | | | | | |
| | 100 GbE QSFP28 | | | | | |
| Dual Power Supply | | No (Spare possible) | No (Spare possible) | No (Spare possible) | External as an option | External as an option |
| Hard Disk (Logs storage) | | Up to 256 GB optional | Up to 256 GB optional | Up to 256 GB optional | Up to 256 GB optional | 32 GB expandable up to 256 GB optional |
| Rackable | | Optional rack kit | Optional rack kit | Optional rack kit | Optional rack kit | Optional rack kit |
| Users | Recommended simultaneous users | <25 | <50 | <80 | <150 | <200 |
| Speed | Firewall | 2,0 Gbps | 3,0 Gbps | 3,5 Gbps | 4,0 Gbps | 5,0 Gbps |
| | IPS | 1,0 Gbps | 1,5 Gbps | 2,0 Gbps | 2,5 Gbps | 3,0 Gbps |
| | Inspection Anti-Malware | 750 Mbps | 1,0 Gbps | 1,5 Gbps | 2,0 Gbps | 2,5 Gbps |
| | SSL Inspection and Decryption (DPI SSL) | 300 Mbps | 500 Mbps | 600 Mbps | 750 Mbps | 800 Mbps |
| TCP/IP Connections | SSL Inspection and Decryption (DPI SSL) | 25.000 | 30.000 | 35.000 | 50.000 | 75.000 |
| VPN | Site-to-site IPSec VPN | 50 | 100 | 150 | 200 | 250 |
| | Clients VPN IPSec | 5(200) | 5(200) | 5(200) | 10(500) | 10(500) |
| | Clients VPN SSL | 1(50) | 2(100) | 2(150) | 2(200) | 2(250) |



SONICWALL®

# Firewall sizing guide

| | | NSa APPLIANCES | | | | | NSsp APPLIANCES | | |
|---|---|---|---|---|---|---|---|---|---|
| | | NSa 2700 | NSa 3700 | NSa 4700 | NSa 9250 | NSa 9450 | NSa 9650 | NSa 9800 | NSsp 12400 | NSsp 12800 | NSsp 15700 |
| Firmware | | SonicOS 7 | SonicOS 7 | SonicOS 7 | SonicOS 6 | SonicOS 6 | SonicOS 6 | SonicOS 6 | SonicOS 6 | SonicOS 6 | SonicOSX 7 |
| Interfaces | 1 GbE copper | 16 | 24 | | 8 | 8 | 8 | 8 | | | |
| | 2.5 GbE copper | | | | | | | | | | |
| | 1 GbE SFP | | | 24 | 8 | 8 | 8 | | | | |
| | 2.5 GbE SFP | | | | | | | 12 | | | |
| | 2.5 GbE SFP+ | | 4 | | | | | | | | |
| | 5 GbE SFP | | | | | | | | | | |
| | 10 GbE | | | | 2 | 2 | 2 | | | | |
| | 10 GbE SFP+ | 3 | 6 | 6 | 2 | 2 | 10 | 4 | 4 | 4 | 4 |
| | 28 GbE SFP+ | | | | | | | | | | |
| | 40 GbE QSFP+ | | | | | | | | 4 | 4 | 4 |
| | 100 GbE QSFP28 | | | | | | | | | | 6 |
| Dual Power Supply | | Internal as an option | Internal as an option | Internal as an option | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Hard Disk (Logs storage) | | 128 GB expandable up to 256 GB optional | 128 GB expandable up to 256 GB optional | 128 GB expandable up to 1 TB optional | | | | | | | |
| Rackable | | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Users | Recommended simultaneous users | <250 | <400 | <600 | <1500 | <2500 | <3000 | <3500 | <8000 | <8000 | <8000 |
| Speed | Firewall | 5,2 Gbps | 5,5 Gbps | 18,0 Gbps | 12,0 Gbps | 17,1 Gbps | 17,1 Gbps | 32 Gbps | 58,4 Gbps | 120 Gbps | Performance distributed according to the number of instances (multi Tenants) |
| | IPS | 3,4 Gbps | 3,8 Gbps | 10,0 Gbps | 7,2 Gbps | 10,2 Gbps | 10,3 Gbps | 21,3 Gbps | 36,8 Gbps | 73,0 Gbps | |
| | Inspection Anti-Malware | 2,9 Gbps | 3,5 Gbps | 9,5 Gbps | 6,5 Gbps | 8,0 Gbps | 8,5 Gbps | 11 Gbps | 33,5 Gbps | 67,5 Gbps | |
| | SSL Inspection and Decryption (DPI SSL) | 800 Mbps | 850 Mbps | 5,0 Gbps | 1,5 Gbps | 2,1 Gbps | 2,25 Gbps | 3,5 Gbps | 8,1 Gbps | 17,6 Gbps | |
| TCP/IP Connections | SSL Inspection and Decryption (DPI SSL) | 125.000 | 150.000 | 350.000 | 250.000 | 450.000 | 550.000 | 650.000 | 1.300.000 | 2.600.000 | |
| VPN | Site-to-site IPSec VPN | 2.000 | 3.000 | 4.000 | 6.000 | 12.000 | 12.000 | 25.000 | 25.000 | 25.000 | |
| | Clients VPN IPsec | 50(1000) | 50(1000) | 500(3000) | 2000(6000) | 2000(6000) | 2000(6000) | 2000(10000) | 2000(10000) | 2000(10000) | |
| | Clients VPN SSL | 2(500) | 2(500) | 2(1000) | 2(1500) | 2(3000) | 50(3000) | 2(3000) | 2(3000) | 2(3000) | |

SONICWALL®

Alias
www.alias.it

Alias
www.alias.it

SONICWALL®

# SonicWall Serie TZ (Gen 7)

## Piattaforma SD-Branch integrata per le PMI e le filiali di prossima generazione

L'ultimo modello della serie TZ di SonicWall è il primo firewall di prossima generazione (NGFW) in formato dektop dotato di interfacce Ethernet da 10 o 5 Gigabit. La serie comprende una vasta gamma di prodotti adatti per diversi casi d'uso.

Progettati per le PMI e le imprese distribuite con sedi SD-Branch, i firewall della serie TZ di 7ª generazione (Gen 7) si contraddistinguono per l'efficacia della sicurezza, riconosciuta a livello industriale, e per il miglior rapporto qualità-prezzo. Questi NGFW tengono conto di quelle che sono le tendenze in fase di espansione della crittografia web, dei dispositivi connessi e della mobilità ad alta velocità, fornendo una soluzione che soddisfa l'esigenza di rilevamento automatico e di prevenzione delle violazioni in tempo reale.

I prodotti della serie TZ Gen 7 sono completamente modulari, con una densità di porte elevata (fino a 10). Sono dotati di una memoria integrata e di una espandibile fino a 256GB, che consente diverse funzioni tra cui registrazione, reportistica, memorizzazione in cache, backup del firmware etc.. In alcuni modelli un secondo alimentatore opzionale garantisce una maggiore ridondanza in caso di guasti.

L'installazione dei sistemi TZ Gen 7 risulta ulteriormente semplificata grazie alla modalità Zero-Touch, che consente di installare contemporaneamente i firewall in più sedi con un minimo intervento dei tecnici informatici. I nuovi sistemi, basati su hardware di prossima generazione, presentano funzioni di firewall, switching e wireless, oltre a consentire la gestione da un unico pannello di controllo degli switch SonicWall e degli access point SonicWave. Essi rendono inoltre possibile un'integrazione rigorosa con Capture Client per una sicurezza completa dell'endpoint.

### Architettura SonicOS e servizi di sicurezza

L'architettura SonicOS è l'elemento centrale dei firewall di prossima generazione TZ. I modelli TZ Gen 7 utilizzano il versatile sistema operativo SonicOS 7.0, dotato di nuove moderne funzioni di interfaccia ed esperienza utente UX/UI, di sicurezza avanzata, di networking e gestionali. Il nuovo sistema operativo comprende SD-WAN, supporto TLS 1.3, visualizzazione in tempo reale, rete privata virtuale (VPN) ad alta velocità e altre potenti funzioni di sicurezza.

Le minacce sconosciute vengono inviate per l'analisi alla sandbox multiengine basata sul cloud Capture Advanced Threat Protection (ATP) di SonicWall. Capture ATP è ulteriormente migliorata grazie alla nostra tecnologia in attesa di brevetto Real-Time Deep Memory Inspection (RTDMI™). L'engine RTDMI di Capture ATP rileva e blocca il malware e le minacce zero-day analizzandole direttamente in memoria.

Grazie all'abbinamento di Capture ATP con la tecnologia RTDMI, in aggiunta ai servizi di sicurezza come Reassembly-Free Deep Packet Inspection (RFDPI), alla protezione antivirus e antispyware, al sistema di prevenzione delle intrusioni, all'intelligenza e al controllo delle applicazioni, ai servizi di filtraggio dei contenuti e alla funzione DPI-SSL, i firewall della serie TZ sono in grado di bloccare malware, ransomware e altre minacce avanzate in corrispondenza del gateway. Per ulteriori informazioni consultare il Datasheet di SonicOS e Security Services.

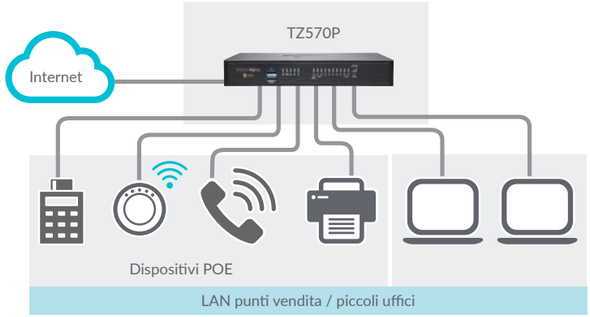

### Punti salienti:

- Interfacce 10/5/2.5/1 GBE in formato desktop
- Compatibilità SD-Branch
- Funzione Secure SD-WAN
- Presa in carico delle app SonicExpress
- Installazione zero-touch
- Gestione da un unico pannello di controllo tramite cloud o firewall
- Integrazione switch SonicWall, access point SonicWave e Capture Client
- Memoria integrata ed espandibile
- Alimentazione ridondante
- Elevato numero di porte
- Failover cellulare
- SonicOS 7.0
- Supporto TLS 1.3
- Prestazioni innovative
- Elevato numero di connessioni
- Prestazioni DPI rapide
- Basso costo totale della proprietà

## Installazione

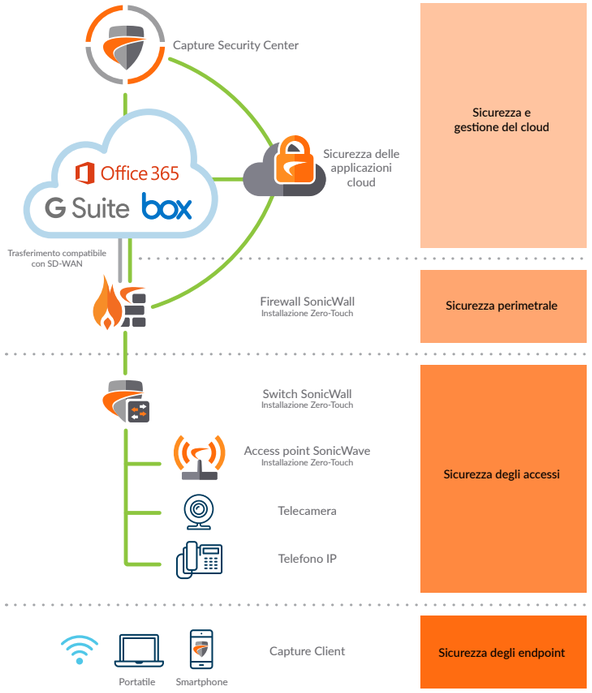
PMI

- Risparmiare spazio e denaro con una soluzione di sicurezza integrata per gateway con funzioni di firewalling, switching e wireless
- Ridurre la complessità e far funzionare l'attività senza dover contare sui tecnici informatici, con facilità di presa in carico tramite l'app SonicExpress e la funzione di installazione Zero-Touch, oltre alla praticità della gestione da un unico pannello di controllo
- Raggiungere la continuità aziendale fornendo un failover per la connettività cellulare
- Proteggere la rete dagli attacchi con una soluzione di sicurezza completa comprendente VPN, IPS, CFS, AV etc..
- Sfruttare l'alta densità delle porte per alimentare più dispositivi PoE, come telefoni e telecamere IP con TZ570P
- Aumentare la produttività dei dipendenti bloccando l'accesso non autorizzato con politiche di segmentazione del traffico e di accesso



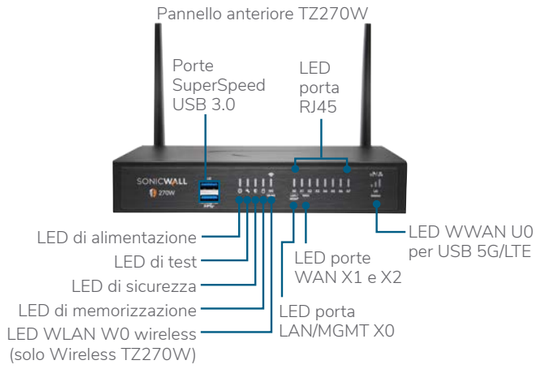

Imprese distribuite con SD-Branch

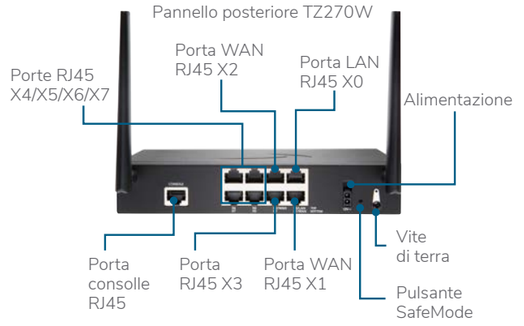
- Migliorare l'esperienza dei clienti e la capacità di adattamento alle mutevoli esigenze aziendali consentendo la connettività della filiale di prossima generazione con SD-Branch
- Perseguire la crescita aziendale investendo in dispositivi di prossima generazione dotati di multi-gigabit e funzioni di sicurezza avanzate compatibili con le future trasformazioni delle reti e delle condizioni di sicurezza
- Proteggere le reti sicure dagli attacchi più avanzati con funzioni di sicurezza avanzate e blocco automatico delle minacce sul traffico decriptato tramite protocolli come TLS 1.3
- Sfruttare la sicurezza di rete end-to-end con l'integrazione senza soluzione di continuità degli access point SonicWave, degli switch SonicWall e di Capture Client
- Garantire una comunicazione senza interruzioni mentre i punti vendita parlano con la sede centrale attraverso una facile connettività VPN che consente agli amministratori informatici di creare una configurazione hub and spoke per il trasferimento sicuro dei dati tra tutte le sedi
- Migliorare l'efficienza aziendale, le prestazioni e ridurre i costi sfruttando le migliorie hardware e software dei modelli TZ Gen 7, oltre a funzionalità come la tecnologia SD-WAN
- Adeguare in modo semplice e rapido le applicazioni SonicExpress e la funzione Zero-Touch
- Garantire la continuità aziendale fornendo un failover per la connettività cellulare
- Mantenere la conformità alle caratteristiche di sicurezza e sfruttare le capacità di archiviazione integrata e di quella espandibile per memorizzare i registri a fini di verifica




## SonicWall serie TZ270

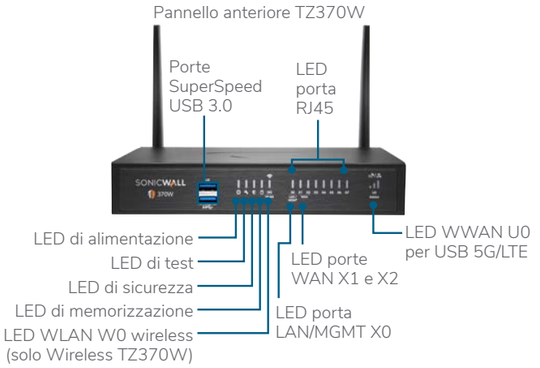
Progettati per il telelavoro e le le filiali senza sprechi (lean branches), i firewall della serie TZ270 si contraddistinguono per l'efficacia della sicurezza riconosciuta a livello industriale e per il miglior rapporto qualità-prezzo.

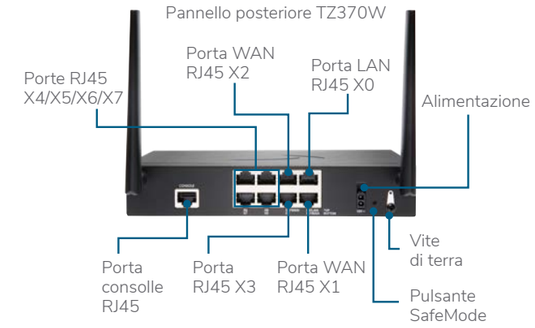



## SonicWall serie TZ370

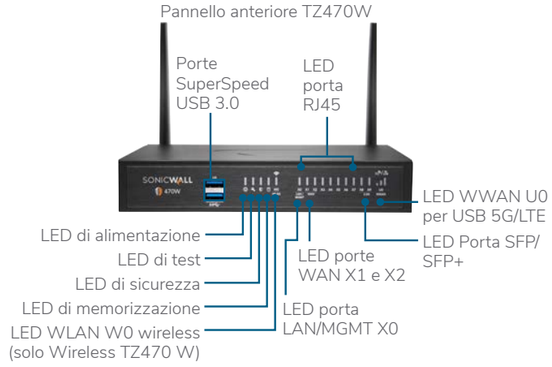
Progettati per le organizzazioni di piccole dimensioni e le filiali senza sprechi (lean branches), i firewall della serie TZ370 si contraddistinguono per l'efficacia della sicurezza riconosciuta a livello industriale e per il miglior rapporto qualità-prezzo.

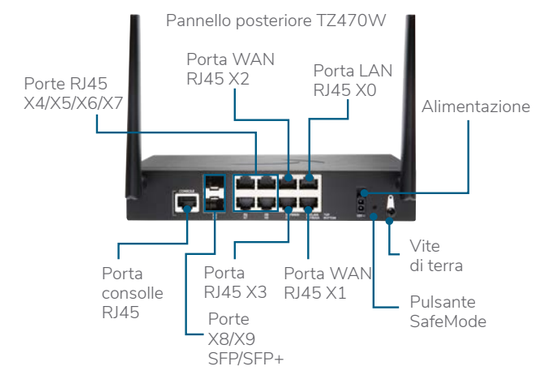



## SonicWall serie TZ470

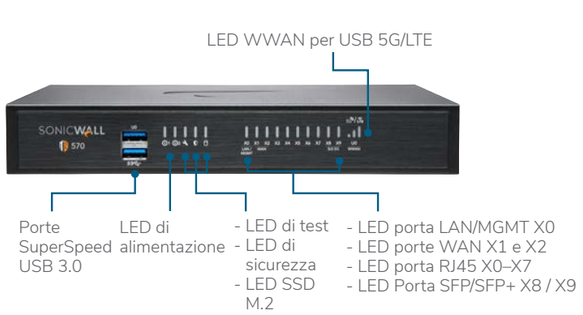
Progettati per le organizzazioni di piccole dimensioni e le imprese distribuite con sedi SD-Branch, i firewall della serie TZ470 si contraddistinguono per l'efficacia della sicurezza riconosciuta a livello industriale e per il miglior rapporto qualità-prezzo.

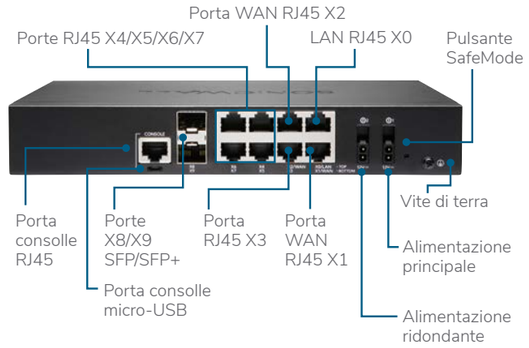


## SonicWall serie TZ570

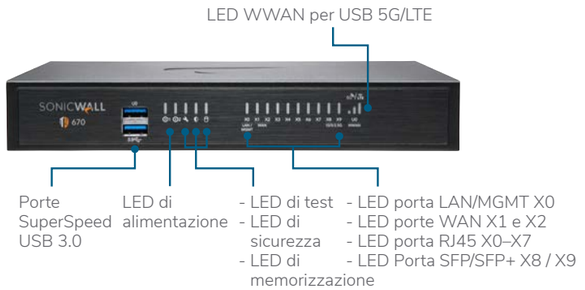
Progettati per le PMI e le imprese distribuite con sedi SD-Branch, i firewall della serie TZ570 si contraddistinguono per l'efficacia della sicurezza riconosciuta a livello industriale e per il miglior rapporto qualità-prezzo.

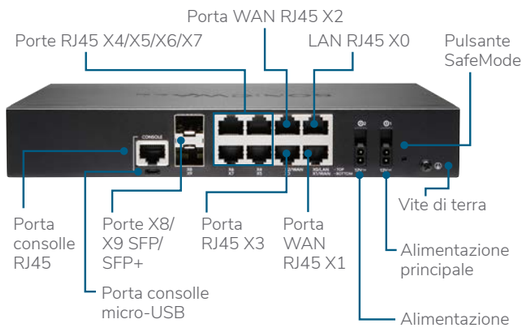



## SonicWall serie TZ670

Progettato per le organizzazioni di media grandezza e le imprese distribuite con sedi SD-Branch, il firewall TZ670 si contraddistingue per l'efficacia della sicurezza riconosciuta a livello industriale e per il miglior rapporto qualità-prezzo.




## Specifiche di sistema SonicWall serie TZ Gen 7

| CARATTERISTICHE GENERALI DEI FIREWALL | SERIE TZ270 | SERIE TZ370 | SERIE TZ470 | SERIE TZ570 | SERIE TZ670 |
|---|---|---|---|---|---|
| Sistema operativo | | SonicOS 7.0 | | | |
| Interfacce | 8x1GbE, USB 3.0, 1 console | 8x1GbE, USB 3.0, 1 console | 8x1GbE, 2x2.5GbE, USB 3.0, 1 console | 8x1GbE, 2x5GbE, USB 3.0, 1 console | 8x1GbE, 2x10GbE, USB 3.0, 1 console |
| Supporto wireless | 2x2 802.11ac Wave 2 (TZ270W) | 2x2 802.11ac Wave 2 (TZ370W) | 2x2 802.11ac Wave 2 (TZ470W) | 2x2 802.11ac Wave 2 (TZ570W) | N/D |
| Supporto PoE (Power over Ethernet) | N/D | N/D | N/D | 5 PoE oppure 3PoE+ (TZ570P) | N/D |
| Slot di espansione memoria (in basso) | | Opzionale fino a 256 GB | | | Opzionale fino a 256 GB, 32 GB compresi |
| Gestione | | Network Security Manager, CLI, SSH, Web UI, GMS, API RET | | | |
| Alimentazione ridondante | N/D | N/D | N/D | Sì | Sì |
| Utenti Single Sign-On (SSO) | 1.000 | 1.000 | 2.500 | 2.500 | 2.500 |
| Interfacce VLAN | 64 | 128 | 128 | 256 | 256 |
| Access point supportati (max) | 16 | 16 | 32 | 32 | 32 |

## Specifiche di sistema SonicWall serie TZ Gen 7 – cont.

| FIREWALL/PRESTAZIONI VPN | SERIE TZ270 | SERIE TZ370 | SERIE TZ470 | SERIE TZ570 | SERIE TZ670 |
|---|---|---|---|---|---|
| Throughput di ispezione firewall[1] | 2 Gbps | 3 Gbps | 3,5 Gbps | 4 Gbps | 5 Gbps |
| Throughput di prevenzione delle minacce[2] | 750 Mbps | 1 Gbps | 1,5 Gbps | 2 Gbps | 2,5 Gbps |
| Throughput di ispezione applicazioni[2] | 1 Gbps | 1,5 Gbps | 2 Gbps | 2,5 Gbps | 3 Gbps |
| Throughput IPS[2] | 1 Gbps | 1,5 Gbps | 2 Gbps | 2,5 Gbps | 3 Gbps |
| Throughput di ispezione anti-malware[2] | 750 Mbps | 1 Gbps | 1,5 Gbps | 2 Gbps | 2,5 Gbps |
| Throughput con decrittazione e ispezione (SSL/DPI)[2] | 300 Mbps | 500 Mbps | 600 Mbps | 750 Mbps | 800 Mbps |
| Throughput con VPN IPSec[3] | 750 Mbps | 1,3 Gbps | 1,5 Gbps | 1,8 Gbps | 2,1 Gbps |
| Connessioni al secondo | 6.000 | 9.000 | 12.000 | 16.000 | 25.000 |
| Numero massimo di connessioni (SPI) | 750.000 | 900.000 | 1.000.000 | 1.250.000 | 1.500.000 |
| Numero massimo di connessioni (DPI) | 150.000 | 200.000 | 250.000 | 400.000 | 500.000 |
| Numero massimo di connessioni (SSL DPI) | 25.000 | 30.000 | 35.000 | 50.000 | 75.000 |
| **VPN** | **SERIE TZ270** | **SERIE TZ370** | **SERIE TZ470** | **SERIE TZ570** | **SERIE TZ670** |
| Tunnel VPN da sede a sede | 50 | 100 | 150 | 200 | 250 |
| Client VPN IPSec (max) | 5 (200) | 5 (200) | 5 (200) | 10 (500) | 10 (500) |
| Licenze VPN SSL (max) | 1 (50) | 2 (100) | 2 (150) | 2 (200) | 2 (250) |
| 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 | | | | |
| Certificati supportati | Verisign, Thawte, Cybertrust, RSA Keon, Entrust e Microsoft CA per VPN da SonicWall a SonicWall, SCEP | | | | |
| Caratteristiche VPN | Dead Peer Detection, DHCP su VPN, attraversamento NAT con IPSec, gateway della VPN ridondante, VPN basata su routing | | | | |
| Piattaforme del client della VPN globale supportate | Microsoft® Windows 10 | | | | |
| NetExtender | Microsoft® Windows 10, Linux | | | | |
| Mobile Connect | Apple® iOS, Mac OS X, Google® Android™, Kindle Fire, Chrome OS, Windows 10 | | | | |

| SERVIZI DI SICUREZZA | SERIE TZ270 | SERIE TZ370 | SERIE TZ470 | SERIE TZ570 | SERIE TZ670 |
|---|---|---|---|---|---|
| Servizi Deep Packet Inspection | Antispyware e antivirus per gateway, prevenzione delle intrusioni, SSL DPI | | | | |
| Content Filtering Service (CFS) | Scansione URL HTTP, IP HTTPS, parole chiave e contenuti, filtraggio basato sui tipi di file come ActiveX, Java<br>Cookie per la privacy, elenchi siti consentiti/vietati | | | | |
| Servizio antispam completo | Sì | | | | |
| Visualizzazione delle applicazioni | Sì | | | | |
| Controllo delle applicazioni | Sì | | | | |
| Capture Advanced Threat Protection | Sì | | | | |
| **NETWORKING** | **SERIE TZ270** | **SERIE TZ370** | **SERIE TZ470** | **SERIE TZ570** | **SERIE TZ670** |
| Assegnazione indirizzo IP | Statico (DHCP, PPPoE, L2TP e client PPTP), server DHCP interno, relay DHCP | | | | |
| Modalità NAT | 1:1, 1:many, many:1, many:many, NAT flessibile (IP sovrapposti), PAT, modalità trasparente | | | | |
| 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 (WMM) | | | | |
| Autenticazione | LDAP (domini multipli), XAUTH/ RADIUS, SSO, Novell, database utenti interno, Terminal Services, Citrix, Common Access Card (CAC) | | | | |
| Database utenti locali | 150 | 250 | 250 | 250 | 250 |
| VoIP | H323-v1-5 completo, SIP | | | | |
| Standard | TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3 | | | | |

SONICWALL®

SONICWALL®

# Serie SonicWall NS*a* Gen 7

La serie di firewall SonicWall Network Security Appliance (NS*a*) di 7ª generazione (Gen 7) offre a medie e grandi aziende prestazioni leader del settore con il costo totale di proprietà più basso della categoria.

Grazie a funzionalità di sicurezza complete come prevenzione delle intrusioni, VPN, controllo delle applicazioni, analisi del malware, filtraggio degli URL, sicurezza DNS e servizi Geo-IP e di filtraggio botnet, protegge il perimetro di rete da minacce avanzate senza creare colli di bottiglia.

**La serie NS*a* Gen 7 in breve.** Specifiche complete »

| Fino a 19 Gb/s | Fino a 8 milioni | 40G/25G/10G/ 5G/2,5G/1G |
|---|---|---|
| Throughput di prevenzione delle minacce | Connessioni | Porte |

## CARATTERISTICHE PRINCIPALI

- Fattore di forma 1 RU
- Supporto per porte da 40G/25G/10G/5G/2,5G/1G
- Analisi minacce e malware a velocità multi-gigabit
- Prestazioni TLS superiori (sessioni e throughput)
- Memoria espandibile
- Predisposizione per Internet edge aziendale
- Nuovo SonicOS di 7ª generazione
- Funzionalità SD-WAN sicura
- Pannello di gestione intuitivo
- Supporto per TLS 1.3
- Eccellente rapporto prezzo/prestazioni
- Prestazioni DPI veloci
- Basso TCO
- Alta densità di porte per una semplice connettività di rete
- Integrazione con SonicWall Switch, SonicWave Access Point e Capture Client
- Alimentazione ridondante

**Trovate la soluzione SonicWall giusta per la vostra azienda:**

sonicwall.com/products

SONICWALL®

**La soluzione offre un'elevata densità di porte, tra cui diverse porte 40 GbE e 10 GbE, e supporta la ridondanza di rete e hardware con elevata disponibilità e doppia alimentazione.**

La serie di firewall SonicWall Network Security Appliance (NS*a*) di 7ª generazione (Gen 7) offre a medie e grandi aziende prestazioni leader del settore con il costo totale di proprietà più basso della categoria.

Grazie a funzionalità di sicurezza complete come prevenzione delle intrusioni, VPN, controllo delle applicazioni, analisi del malware, filtraggio degli URL, sicurezza DNS e servizi Geo-IP e Bot-net, protegge il perimetro di rete da minacce avanzate senza creare colli di bottiglia.

La serie NS*a* Gen 7 è stata riprogettata con i componenti hardware più recenti, sviluppati per garantire una prevenzione delle minacce a velocità multi-gigabit, anche per il traffico crittografato. La soluzione offre un'elevata densità di porte, tra cui diverse porte 40 GbE e 10 GbE, e supporta la ridondanza di rete e hardware con elevata disponibilità e doppia alimentazione.

### SonicOS 7.0 e servizi di sicurezza di 7ª generazione

La serie NS*a* Gen 7 utilizza SonicOS 7.0, un nuovo sistema operativo appositamente realizzato per fornire una moderna interfaccia utente, flussi di lavoro intuitivi e un approccio che mette l'utente in primo piano. SonicOS 7.0 offre diverse funzionalità concepite per facilitare i flussi di lavoro aziendali. Offre un semplice sistema di configurazione delle policy, installazione zero-touch e gestione flessibile per consentire alle aziende di migliorare la sicurezza e l'efficienza operativa.

La serie NS*a* di 7ª generazione supporta funzionalità di rete avanzate quali SD-WAN, routing dinamico, alta disponibilità ai livelli 4-7 e funzioni VPN ad alta velocità. Oltre a integrare funzionalità firewall e switch, l'appliance offre un unico pannello di controllo per gestire sia gli switch che i punti di accesso.

Creata per mitigare gli attacchi informatici avanzati attuali e futuri, la serie NS*a* Gen 7 offre l'accesso ai servizi di sicurezza firewall avanzati di SonicWall, che permettono di proteggere l'intera infrastruttura IT. Soluzioni e servizi come Cloud Application Security, la sandbox Capture Advanced Threat Protection (ATP) basata sul cloud, l'ispezione Real-Time Deep Memory Inspection (RTDMI™) e Reassembly-Free Deep Packet Inspection (RFDPI) per ogni tipo di traffico, TLS 1.3 incluso, offrono la protezione completa dei gateway contro malware nascosti e pericolosi, comprese le minacce zero-day e crittografate.

SONICWALL®

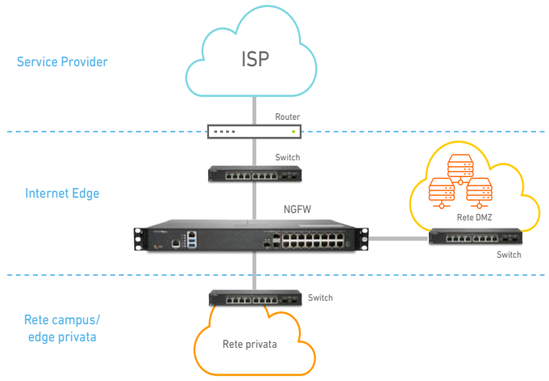
## Installazione

La serie NS*a* Gen 7 offre due opzioni di implementazione principali per le medie imprese e le aziende distribuite:

### Installazione Internet Edge

In questa configurazione d'installazione standard, il firewall NGFW della serie NS*a* Gen 7 protegge le reti private dal traffico dannoso proveniente da Internet, permettendo di:

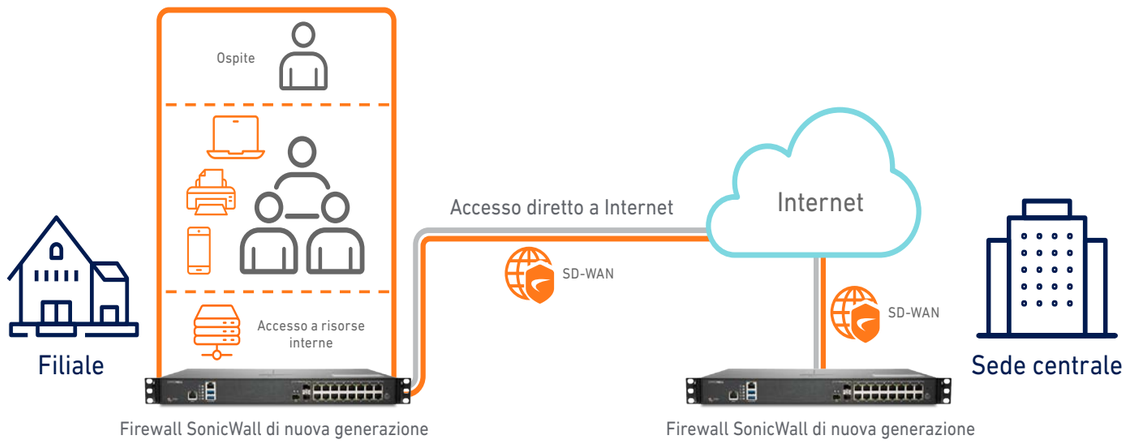
- Implementare una soluzione NGFW collaudata con il massimo livello di prestazioni e densità di porte (inclusa la connettività 40 GbE e 10 GbE) della sua categoria
- Ottenere visibilità e ispezionare il traffico crittografato, incluso quello TLS 1.3, per bloccare le minacce elusive provenienti da Internet – il tutto senza compromettere le prestazioni
- Proteggere l'azienda con funzioni di sicurezza integrate quali analisi del malware, sicurezza delle applicazioni cloud, filtraggio degli URL e servizi di reputazione
- Risparmiare spazio e denaro con una soluzione NGFW integrata che offre caratteristiche di sicurezza e networking avanzate
- Ridurre la complessità e massimizzare l'efficienza mediante un sistema di gestione centrale dotato di un'interfaccia di controllo intuitiva




### Medie imprese e aziende distribuite

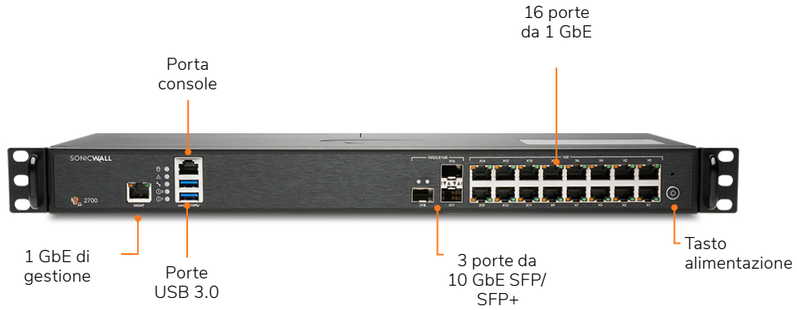
La serie SonicWall NS*a* Gen 7 supporta l'SD-WAN e può essere gestita centralmente, fornendo una soluzione ideale per aziende distribuite e imprese di medie dimensioni. Questa implementazione consente alle aziende di:

- Proteggersi dalle minacce future in continua evoluzione, investendo in un firewall NGFW con analisi delle minacce a velocità multi-gigabit
- Fornire un accesso Internet diretto e sicuro alle filiali distribuite, evitando il backhauling del traffico attraverso la sede centrale dell'azienda
- Consentire alle filiali distribuite di accedere in sicurezza alle risorse aziendali nella sede centrale o in un cloud pubblico, migliorando sensibilmente la latenza delle applicazioni
- Bloccare automaticamente le minacce che sfruttano protocolli crittografati come TLS 1.3, proteggendo così le reti dagli attacchi più avanzati.
- Ridurre la complessità e massimizzare l'efficienza mediante un sistema di gestione centrale dotato di un'interfaccia di controllo intuitiva
- Sfruttare un'elevata densità di porte con connettività 40 G e 10 GbE per supportare reti aziendali WAN e distribuite



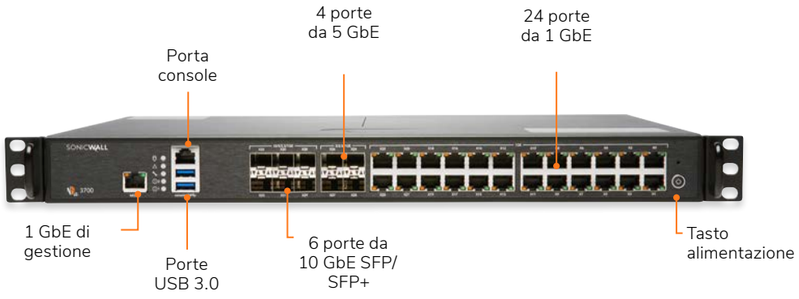

## Serie SonicWall NS*a* Gen 7

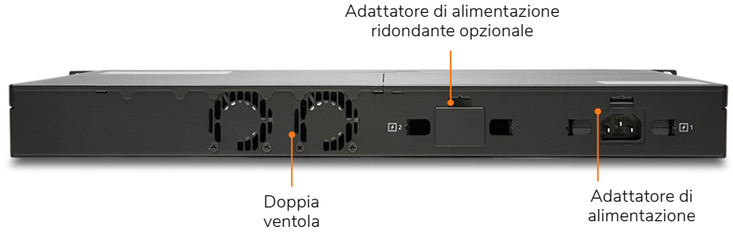
### NS*a* 2700





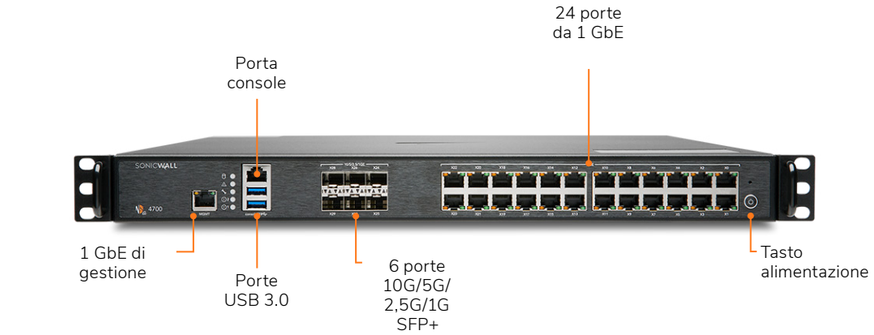
### NS*a* 3700



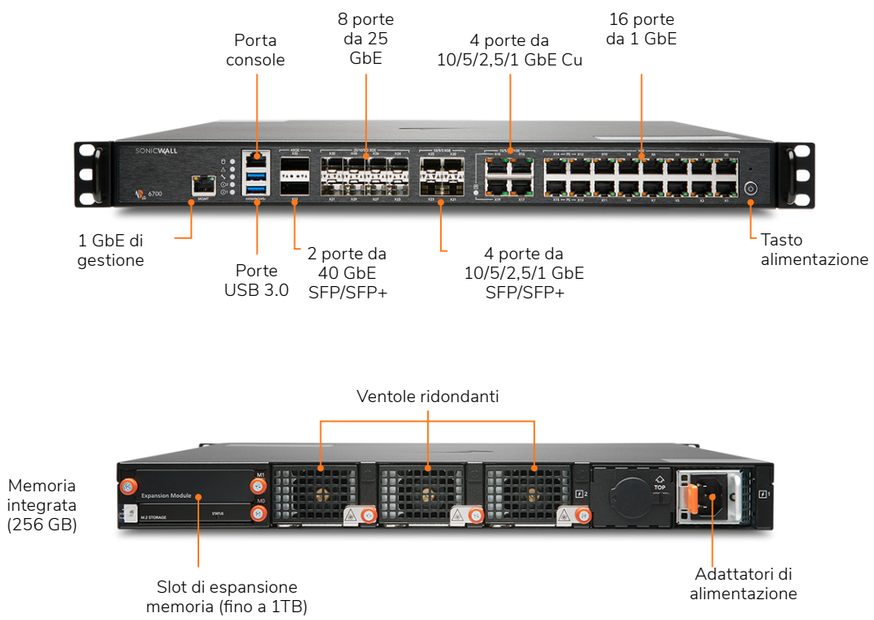



## Serie SonicWall NS*a* Gen 7 (continua)

### NS*a* 4700




### NS*a* 6700




## Specifiche di sistema della serie NS*a* Gen 7

| Firewall | NS*a* 2700 | NS*a* 3700 | NS*a* 4700 | NS*a* 6700 |
|---|---|---|---|---|
| Sistema operativo | SonicOS 7.0 | | | |
| Interfacce | 16x1GbE, 3x10G SFP+, 2 USB 3.0, 1 console, 1 porta di gestione | 24x1GbE, 6x10G SFP+, 4x5G SFP+, 2 USB 3.0, 1 console, 1 porta di gestione | 6 x 10G/5G/2,5G/1G (SFP+); 24 x 1GbE Cu 2 USB 3.0, 1 console, 1 porta di gestione | 2x40G; 8x25G, 4 x10G/5G/2,5/1G SFP+, 4 x 10G/5G/2,5G/1G (Cu); 16 x 1GbE (Cu) 2 USB 3.0, 1 console, 1 porta di gestione |
| Memoria | 64 GB M.2 | 128 GB M.2 | 128 GB | 256 GB M.2 |
| Espansione | Slot di espansione memoria (fino a 256 GB) | Slot di espansione memoria (fino a 256 GB) | Slot di espansione memoria (fino a 1 TB) | Slot di espansione memoria (fino a 1 TB) |
| Interfacce VLAN | 256 | 256 | 512 | 512 |
| Punti di accesso supportati (max.) | 32 | 32 | 512 | 512 |
| **Firewall/prestazioni VPN** | | | | |
| Throughput di ispezione firewall[1] | 5,2 Gb/s | 5,5 Gb/s | 18 Gb/s | 36 Gb/s |
| Throughput di prevenzione delle minacce[2] | 3,0 Gb/s | 3,5 Gb/s | 9,5 Gb/s | 19 Gb/s |
| Throughput di ispezione applicazioni[2] | 3,6 Gb/s | 4,2 Gb/s | 11 Gb/s | 20 Gb/s |
| Throughput IPS[2] | 3,4 Gb/s | 3,8 Gb/s | 10 Gb/s | 20 Gb/s |
| Throughput ispezione anti-malware[2] | 2,9 Gb/s | 3,5 Gb/s | 9,5 Gb/s | 18,5 Gb/s |
| Throughput con decrittazione e ispezione TLS/SSL (SSL DPI)[2] | 800 Mb/s | 850 Mb/s | 5 Gb/s | 9 Gb/s |
| Throughput VPN IPSec[3] | 2,10 Gb/s | 2,2 Gb/s | 11 Gb/s | 19 Gb/s |
| Connessioni al secondo | 21.500 | 22.500 | 115.000 | 153.000 |
| Connessioni max. (SPI) | 1.500.000 | 2.000.000 | 4.000.000 | 8.000.000 |
| Connessioni max. DPI-SSL | 125.000 | 150.000 | 350.000 | 750.000 |
| Connessioni max. (DPI) | 500.000 | 750.000 | 2.000.000 | 6.000.000 |
| **VPN** | | | | |
| Tunnel VPN site-to-site | 2.000 | 3.000 | 4.000 | 6.000 |
| Client VPN IPSec (max) | 50 (1000) | 50 (1000) | 500 (3000) | 2000 (6000) |
| Licenze VPN SSL (max) | 2 (500) | 2 (500) | 2 (1000) | 2 (1500) |
| Crittografia/autenticazione | DES, 3DES, AES (128, 192, 256 bit)/MD5, SHA-1, crittografia Suite B | | | |
| Key exchange | Gruppi Diffie-Hellman 1, 2, 5, 14v | | | |
| VPN basata su routing | RIP, OSPF, BGP | | | |
| Certificati supportati | Verisign, Thawte, Cybertrust, RSA Keon, Entrust e Microsoft CA per VPN da SonicWall a SonicWall, SCEP | | | |
| Caratteristiche VPN | Dead Peer Detection, DHCP su VPN, attraversamento NAT con IPSec, gateway della VPN ridondante, VPN basata su routing | | | |
| Piattaforme client della VPN globale supportate | Windows 10 | | Microsoft® Windows Vista a 32/64 bit, Windows 7 a 32/64 bit, Windows 8.0 a 32/64 bit, Windows 8.1 a 32/64 bit, Windows 10 | |
| NetExtender | Windows 10 e Linux | | Microsoft Windows Vista a 32/64 bit, Windows 7, Windows 8.0 a 32/64 bit, Windows 8.1 a 32/64 bit, Mac OS X 10.4 e versioni successive, Linux FC3 e versioni successive/Ubuntu 7 e versioni successive/OpenSUSE | |
| Mobile Connect | Apple iOS, Mac OS X, Android, Kindle Fire, Chrome OS, Windows 10 | | Apple® iOS, Mac OS X, Google® Android™, Kindle Fire, Chrome, Windows 8.1 (incorporato) | |
| **Servizi di sicurezza** | | | | |
| Servizi Deep Packet Inspection | Antispyware e antivirus per gateway, prevenzione delle intrusioni, SSL DPI | | | |
| Content Filtering Service (CFS) | Scansione HTTP URL, HTTPS IP, parole chiave e contenuti, filtraggio basato su tipi di file come ActiveX, Java, cookie per la privacy, liste di autorizzazione/blocco | | | |

SONICWALL®

SONICWALL®

## Specifiche di sistema della serie NS*a* Gen 7

| Firewall | NS*a* 2700 | NS*a* 3700 | NS*a* 4700 | NS*a* 6700 |
|---|---|---|---|---|
| Comprehensive Anti-Spam Service | Supportato | | | |
| Visualizzazione delle applicazioni | Sì | | | |
| Controllo delle applicazioni | Sì | | | |
| Capture Advanced Threat Protection | Sì | | | |
| **Connettività di rete** | | | | |
| Assegnazione indirizzo IP | Statica (DHCP, PPPoE, L2TP e client PPTP), server DHCP interno, DHCP relay | | | |
| Modalità NAT | 1:1, 1:many, many:1, many:many, NAT flessibile (IP sovrapposti), PAT, modalità trasparente | | | |
| Protocolli di routing | BGP4, OSPF, RIPv1/v2, route statici, routing basato su policy | | | |
| Qualità del servizio (QoS) | Priorità della larghezza di banda, larghezza di banda massima, larghezza di banda garantita, contrassegno DSCP, 802.1p (WMM) | | | |
| Autenticazione | LDAP (domini multipli), XAUTH/RADIUS, SSO, Novell, database utenti interno, Terminal Services, Citrix, Common Access Card (CAC) | | | |
| Database utenti locale | 250 | 250 | 2500 | 3200 |
| VoIP | Full H323-v1-5, SIP | | | |
| Standard | TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3 | | | |
| Certificazioni (in corso) | FIPS 140-2 (con Suite B) Level 2, UC APL, VPNC, IPv6 (Phase 2), ICSA Network Firewall, ICSA Anti-virus, Common Criteria NDPP (Firewall e IPS) | | | |
| Common Access Card (CAC) | Supportato | | | |
| Alta disponibilità | Attiva/Passiva con sincronizzazione dello stato | | | |
| **Hardware** | | | | |
| Fattore di forma | 1U rack-mount | | | |
| Ventole | 1 | 2 | 2 (rimovibili) | 2 (rimovibili) |
| Alimentazione | 60W | 90W | 1x350W | 1x350W |
| Potenza max. assorbita (W) | 21,5 | 36,3 | 135,8 | 139,2 |
| Alimentazione in ingresso | 100-240 VAC, 50-60 Hz | | | |
| Dissipazione di calore totale | 73,32 BTU | 123,78 BTU | 463,1 | 474,7 |
| Dimensioni | 43 x 32,5 x 4,5 cm (16,9 x 12,8 x 1,8 in) | | 43 x 46,5 x 4,5 cm (16,9 x 18,1 x 1,8 in) | |
| Peso | 4,0 kg / 8,8 lbs | 4,6 kg / 10,2 lbs | 7,8 kg | 8,1 kg |
| Peso RAEE | 4,2 kg / 9,3 lbs | 4,8 kg / 10,6 lbs | 9,6 kg | 9,9 kg |
| Peso con la confezione | 6,4 kg / 14,1 lbs | 7 kg / 15,4 lbs | 13,5 kg | 13,8 kg |
| Condizioni ambientali (in funzionamento/stoccaggio) | 0-40 °C (32-105 °F) / da -40 a 70 °C (da -40 a 158 °F) | | | |
| Umidità | 5-95% senza condensa | | 0-90% relativa, senza condensa | |
| **Normative** | | | | |
| Principali normative di conformità | FCC Classe A, CE (EMC, LVD, RoHS), C-Tick, VCCI Classe A, MSIP/KCC Classe A, UL, cUL, TÜV/GS, CB, CoC UL (Messico), RAEE, REACH, ANATEL, BSMI | | | |

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.

3. Throughput VPN rilevato con il traffico UDP usando pacchetti da 1418 byte, crittografia AESGMAC16-256 in conformità a RFC 2544. Tutte le specifiche, le funzioni e le informazioni sulla disponibilità sono soggette a modifiche.

## SERVIZI OFFERTI DAI PARTNER

**Serve aiuto per pianificare, ottimizzare o installare una soluzione SonicWall? I SonicWall Advanced Services Partners hanno seguito corsi di formazione per fornire servizi professionali di livello mondiale. Per maggiori informazioni:**

www.sonicwall.com/PES

SONICWALL®

## Riepilogo delle funzioni di SonicOS 7.0

### Firewall

- Ispezione Stateful Packet
- Ispezione Reassembly-Free Deep Packet
- Protezione da attacchi DDoS (UDP/ICMP/SYN flood)
- Supporto IPv4/IPv6
- Autenticazione biometrica per l'accesso remoto
- Proxy DNS
- Supporto API completo
- Integrazione switch SonicWall
- Modularità SD-WAN
- Procedura guidata usabilità SD-WAN [1]
- Scalabilità connessioni (SPI, DPI, DPI SSL)
- Pannello di controllo migliorato[1]
- Visualizzazione migliorata dei dispositivi
- Riepilogo traffico e utenti principali
- Informazioni sulle minacce
- Centro notifiche

### Decrittazione e ispezione TLS/SSL/SSH

- TLS 1.3 con sicurezza migliorata[1]
- Deep Packet Inspection per TLS/SSL/SSH
- Inclusione/esclusione di oggetti, gruppi o nomi di host
- Controllo SSL
- Miglioramenti per DPI-SSL con CFS
- Controlli DPI SSL granulari in base a zone o regole

### Prevenzione delle intrusioni[2]

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

### Anti-malware[2]

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

### Identificazione delle applicazioni[2]

- Controllo delle applicazioni
- Gestione della larghezza di banda delle applicazioni
- Creazione di firme per applicazioni personalizzate
- Prevenzione di perdite di dati
- Creazione di report sulle applicazioni tramite NetFlow/IPFIX
- Database completo di firme delle applicazioni

### Visualizzazione e analisi del traffico

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

### Filtraggio dei contenuti Web HTTP/HTTPS[2]

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

### VPN

- Secure SD-WAN
- Provisioning automatico delle VPN
- VPN IPSec per la connettività Site-to-Site
- Accesso remoto tramite VPN SSL e client IPSec
- Gateway VPN ridondante
- Mobile Connect per iOS, Mac OS X, Windows, Chrome, Android e Kindle Fire
- VPN basata su routing (OSPF, RIP, BGP)

### Connettività di rete

- PortShield
- Frame Jumbo
- Indagine del percorso MTU
- Registrazione avanzata
- VLAN trunking
- Mirroring delle porte (SonicWall Switch)
- QoS livello 2
- Sicurezza delle porte
- Routing dinamico (RIP/OSPF/BGP)
- Controller wireless SonicWall
- Routing basato su policy (ToS/metrico ed ECMP)
- NAT
- Server DHCP
- Gestione della larghezza di banda
- Elevata disponibilità A/P con sincronizzazione dello stato
- Bilanciamento del carico in ingresso/in uscita
- Elevata disponibilità Attivo/Standby con sincronizzazione dello stato
- Modalità Bridge (L2), Wire/Wire virtuale, Tap, NAT
- Routing asimmetrico
- Supporto CAC (Common Access Card)

### VoIP

- Controllo QoS granulare
- Gestione della larghezza di banda
- DPI per il traffico VoIP
- Supporto per gatekeeper H.323 e proxy SIP

### Gestione, monitoraggio e supporto

- Supporto Capture Security Appliance (CS*a*)
- Capture Threat Assessment (CTA) v2.0
- Progettazione o template di nuova concezione
- Confronti con la media di settore e globale
- Nuova UI/UX, layout intuitivo delle funzioni[1]
- Pannello di controllo
- Informazioni sui dispositivi, applicazioni, minacce
- Visualizzazione della topologia
- Definizione e gestione semplificate delle policy
- Statistiche d'uso per policy e oggetti[1]
- Utilizzato / non utilizzato
- Attivo / non attivo
- Ricerca globale di dati statici
- Supporto di memorizzazione[1]

SONICWALL®

# NSv 270/470/870

The SonicWall Network Security virtual NSv 270/470/870 firewalls, deliver enterprise-class security, streamlined management, complete visibility, flexible deployment, while delivering superior performance for virtual workloads.

Vulnerabilities within virtual environments are discovered regularly that yield serious security implications and challenges. But protecting all these security vectors requires the ability to also consistently apply the right security policy to the right network control point, as some security failures can be attributed to ineffective policies or misconfigurations.

## HIGHLIGHTS

### Public and private cloud security

- Next-gen firewall with automated real-time breach detection and prevention capabilities
- Patent-pending Real-Time Deep Memory Inspection (RTDMI) technology
- Patented Reassembly-Free Deep Packet Inspection (RFDPI) technology
- Complete end-to-end visibility and streamlined management with Unified Policy
- Application intelligence and control
- Segmentation security and security zoning
- Support across private cloud (ESXi, Hyper-V, KVM, Nutanix) and public cloud (AWS, Azure) platforms

### Virtual machine protection

- Data confidentiality
- Secure communication with data leakage prevention
- Traffic validation, inspection and monitoring
- Virtual network resilience and availability
- SonicOSX 7.0

**Find the right SonicWall solution for your enterprise:**

sonicwall.com/NSv

NSv firewall series help security teams reduce these types of security risks and vulnerabilities, which can cause serious disruption to business-critical services and operations. It enables enterprises to control dynamic traffic passing through a firewall and provides visibility and insight into disparate policies. It help simplify management tasks, reduce configuration errors and speed up deployment time, all of which contribute to a better overall security posture.

## SonicOSX and Security Services

The SonicOSX architecture is at the core of NSv 240/470/870 firewalls. It is powered by the feature rich SonicOSX 7.0 operating system with new modern looking UX/UI, advanced security, networking and management capabilities.

Built from the ground up, SonicOSX 7.0 features Unified Policy that offers integrated management of various security policies. Easily provision layer 3 to layer 7 controls in a single rule base on every firewall, providing a centralized location for configuring policies. The new web interface presents meaningful visualizations of threat information, and displays actionable alerts prompting you to configure contextual security policies with point-and-click simplicity.

NSv further integrates SD-WAN, TLS 1.3 support, real-time visualization, high-speed virtual private networking (VPN) and other robust security features. Unknown threats are sent to SonicWall's cloud-based Capture Advanced Threat Protection (ATP) multiengine sandbox for analysis. Enhancing Capture ATP is our patent-pending Real-Time Deep Memory Inspection (RTDMI™) technology. As one of Capture ATP's engine, RTDMI detects and blocks malware and zero-day threats by inspecting directly in memory.

By leveraging Capture ATP with RTDMI technology, in addition to security advanced services, NSv series firewalls stop malware, ransomware and other advanced threats at the gateway.

## Deployments

### 1. Cloud Edge and Data Center Secure Public Clouds

- Secure workloads on Amazon Web Services (AWS) and Microsoft Azure
- Protect cloud applications and cloud infrastructures from cyber threats with advanced next-generation firewall features that incorporates VPN, IPS, CFS, AV and much more
- Decrypt encrypted traffic easily and utilize TLS 1.3 support for improved security
- Ensure compliance with regulatory standards by implementing threat prevention and segmentation capabilities
- Appropriately scale and right-size your infrastructure
- Gain complete visibility and control of traffic across multiple regions and availability zones with Unified Policy
- Attain cost benefit and efficiency by shifting from CAPEX to OPEX
- Secure Private Clouds
- Secure virtualized compute resources and hypervisors to protect private cloud workloads on VMware ESXi, Microsoft Hyper-V, Nutanix and KVM
- Prevent threats with complete visibility into intra-host communication between virtual machines
- Ensure appropriate application of security policies throughout the virtual environment
- Deliver safe application enablement rules by application, user and device, regardless of VM location
- Implement proper security zoning and isolations
- Gain complete visibility and streamlined provisioning of traffic across multiple locations and availability zones with Unified Policy
- Decrypt encrypted traffic easily and utilize TLS 1.3 support for improved security

### 2. Internet Edge

- Protect corporate resources from attacks at the Internet gateway.
- Secure Internet edge from the most advanced attacks with advanced security features and automatically block threats
- Ensure compliance with regulatory standards by implementing threat prevention and segmentation capabilities
- Improve business efficiency, performance and reduce costs by leveraging SonicOSX enhancements
- Segment critical PoS (Point of Sale) systems, to ensure business continuity
- Gain complete visibility and control of traffic across multiple regions and availability zones with Unified Policy

## NSv Series System Specifications

| Firewall General | NSv 270 | NSv 470 | NSv 870 |
|---|---|---|---|
| Operating system | SonicOSX[12] | | |
| Supported Hypervisors | VMware ESXi v5.5 / v6.0 / v6.5 / v6.7, Microsoft Hyper-V, KVM Ubuntu 16.04 / CentOS 7, Nutanix AHV (AOS 5.15 LTS/Prism Central 5.16.1.2)[11] | | |
| Supported Public Cloud Platforms (Instance Type)[1] | AWS (c5.large), Azure (Std D2 v2) | AWS (c5.xlarge), Azure (Std D3 v2) | AWS (c5.2xlarge), Azure (Std D4 v2) |
| Licensing | BYOL, PAYG[2] | | |
| Max Supported vCPUs | 2 | 4 | 8 |
| Interface Count (ESXi/Hyper-V/KVM/Nutanix/AWS/Azure) | 8/8/8/8/2/2 | 8/8/8/8/4/4 | 8/8/8/8/8/8 |
| Max Mgmt/DataPlane Cores | 1/1 | 1/3 | 1/7 |
| Min Memory[3] | 6 GB | 8 GB | 10 GB |
| Max Memory[4] | 6 GB | 10 GB | 14 GB |
| Supported IP/Nodes | Unlimited | | |
| Minimum Storage | 60 GB | | |
| SSO users | 500 | 10,000 | 15,000 |
| Logging | Analyzer, Local Log, Syslog | | |
| High availability | Active/Passive[5] | | |
| **Firewall/VPN Performance[6,8]** | **NSv 270** | **NSv 470** | **NSv 870** |
| Firewall Inspection Throughput | 6 Gbps | 9 Gbps | 14 Gbps |
| Threat Prevention Throughput | 1.6 Gbps | 2.9 Gbps | 8 Gbps |
| IPS Throughput | 4 Gbps | 6 Gbps | 8 Gbps |
| TLS/SSL DPI Throughput | 800 Mbps | 2 Gbps | 4 Gbps |
| VPN Throughput[9] | 1.4 Gbps | 3.5 Gbps | 8 Gbps |
| Connections per second | 13,760 | 37,270 | 75,640 |
| Maximum connections (SPI) | 225,000 | 1.5M | 3M |
| Maximum connections (DPI) | 125,000 | 1.5M | 2M |
| TLS/SSL DPI Connections | 8,000 | 20,000 | 30,000 |
| **VPN** | **NSv 270** | **NSv 470** | **NSv 870** |
| Site-to-Site VPN Tunnels | 75 | 6000 | 10,000 |
| IPSec VPN clients (Maximum) | 50(1000) | 2000(4000) | 2000(6000) |
| SSL VPN Clients Included[7] | 2 | 2 | 2 |
| SSL VPN Clients Maximum[7] | 100 | 200 | 300 |
| Encryption/authentication | DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1, Suite B, Common Access Card (CAC) | | |
| Key exchange | Diffie Hellman Groups 1, 2, 5, 14v | | |
| Route-based VPN | RIP, OSPF, BGP | | |
| **Networking** | **NSv 270** | **NSv 470** | **NSv 870** |
| IP address assignment | Static, DHCP, internal DHCP server[10], DHCP relay[10] | | |
| NAT modes | 1:1, many:1, 1:many, flexible NAT (overlapping IPs), PAT | | |
| Max VLAN[8] | 128 | 128 | 128 |
| Routing protocols | BGP, OSPF, RIPv1/v2, static routes, policy-based routing | | |
| QoS | Bandwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking, 802.1p | | |
| Authentication | XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, internal user database, Terminal Services, Citrix | | |

*[1]Pending availability.*
*[2]PAYG is currently available only on AWS.*
*[3]Memory with Jumbo frame disabled.*
*[4]Memory with Jumbo frame enabled. Additional memory is required for Jumbo frames. Jumbo frames are not supported on Azure and AWS.*
*[5]High availability is available on VMware ESXi platform, KVM, Azure, Microsoft Hyper-V and Nutanix. HA is not supported on AWS.*
*[6]Published performance numbers are up to the specification and the actual performance may vary depending on underlying hardware, network conditions; firewall configuration and activated services. Performance and capacities may also vary based on underlying virtualization infrastructure, and we recommend additional testing within your environment to ensure your performance and capacity requirements are met. Performance metrics were observed using Intel Xeon W Processor (W-2195 2.3GHz, 4.3GHz Turbo, 24.75M Cache) running SonicOSv 6.5.0.2 with VMware vSphere 6.5.*
*[7]Increased SSL VPN number will be available only from SonicOS 6.5.4.4-44v-21-723 firmware and onwards.*
*[8]VLAN interfaces are not supported on Azure and AWS. Testing Methodologies: Maximum performance based on RFC 2544 (for firewall). Threat Prevention/GatewayAV/ Anti-Spyware/IPS throughput measured using industry standard Keysight HTTP performance test tools. Testing done with multiple flows through multiple port pairs. Threat Prevention throughput measured with Gateway AV, Anti-Spyware, IPS and Application Control enabled with default firewall settings. VPN throughput measured with UDP traffic using 1418 byte packet size AESGMAC16-256 Encryption adhering to RFC 2544. All specifications, features and availability are subject to change.*
*[9]All performance parameters are tested using Dell R740 with SR-IOV and Turbo boost.*
*[10]Supported on Private Cloud and not on Public Cloud Platforms.*
*[11]Nutanix AHV is supported on SonicWall NSv 270/470/870 running SonicOSX 7.0.0 firmware and onwards.*
*[12]SonicOSX 7.0.1 onwards user will be able to select and switch between Classic/Global and Policy mode.*

## SonicOSX 7.0 feature summary

### Firewall

- Stateful packet inspection
- Reassembly-Free Deep Packet Inspection
- DDoS attack protection (UDP/ICMP/SYN flood)
- IPv4/IPv6 support
- Biometric authentication for remote access
- DNS proxy
- REST APIs
- SonicWall Switch integration[1]
- SD-WAN
  - SD-WAN Scalability
  - SD-WAN Usability Wizard
- API
  - Full API Support
- Multi-Tenancy[3]
  - Multi-Tenant Support
  - Tenant View with Firmware Support per Tenant
- Switch between Classic/Global and Policy mode[4]

### Unified Policy

- Unified Policy combines layer 3 to layer 7 rules:
  - Source/Destination IP/Port/Service
  - Application Control
  - CFS/Web Botnet/Geo-IP
  - Rule Diagram
  - Single Pass Security Services enforcement - IPS/GAV/AS/Capture ATP
  - Profile Based Objects for Endpoint Security/BWM/QoS/CFS/ Intrusion Prevention
- Action Profiles for Security/DoS Rules
- Rule management:
  - Cloning
  - Shadow rule analysis
  - In-cell editing
  - Rule Export
  - Group editing
- Managing views
  - Used/un-used rules
  - Active/in-active rules
  - Sections/Custom Grouping
  - Customizable Grid/Layout

### TLS/SSL/SSH decryption and inspection

- TLS1.3
- Supporting TLS 1.3 with enhanced security
- Deep packet inspection for TLS/SSL/SSH
- Inclusion/exclusion of objects, groups or hostnames
- SSL control
- Granular DPI SSL controls per zone or rule

### Capture advanced threat protection[2]

- Real-Time Deep Memory Inspection
- Cloud-based multi-engine analysis
- Virtualized sandboxing
- Hypervisor level analysis
- Full system emulation
- Broad file type examination
- Automated & manual submission
- Real-time threat intelligence updates
- Block until verdict
- Capture Client

### Intrusion prevention[2]

- Signature-based scanning
- Automatic signature updates
- Bi-directional inspection engine
- Granular IPS rule capability
- GeoIP enforcement
- Botnet filtering with dynamic list
- Regular expression matching

### Anti-malware[2]

- Stream-based malware scanning
- Gateway anti-virus
- Gateway anti-spyware
- Bi-directional inspection
- No file size limitation
- Cloud malware database

### Application identification[2]

- Application control
- Application bandwidth management
- Custom application signature creation
- Data leakage prevention
- Application reporting over NetFlow/IPFIX
- Comprehensive application signature database

### Traffic visualization and analytics

- User activity
- Application/bandwidth/threat usage
- Cloud-based analytics

### HTTP/HTTPS Web content filtering[2]

- URL filtering
- Proxy avoidance
- Keyword blocking
- Policy-based filtering (exclusion/inclusion)
- HTTP header insertion
- Bandwidth manage CFS rating categories
- Unified policy model with app control
- Content Filtering Client

### VPN

- Secure SD-WAN
- Auto-provision VPN
- IPSec VPN for site-to-site connectivity
- SSL VPN and IPSec client remote access
- Redundant VPN gateway
- Mobile Connect for iOS, Mac OS X, Windows, Chrome, Android and Kindle Fire
- Route-based VPN (RIP/OSPF/BGP)

### Enhanced Dashboard

- Enhanced Device View
- Top Traffic and User summary
- Insights to threats
- Notification Center
- Enhanced Packet Monitoring
- SSH Terminal on UI
- New Design/Template
- Industry and Global Average Comparison

### Networking

- PortShield[1]
- Jumbo frames
- Path MTU discovery
- Enhanced logging
- VLAN trunking
- Port mirroring (NSa 2650 and above)
- Layer-2 QoS
- Port security
- Dynamic routing (RIP/OSPF/BGP)
- SonicWall wireless controller[1]

SONICWALL®

SONICWALL®

- Policy-based routing (ToS/ metric and ECMP)
- NAT
- DHCP server
- Bandwidth management
- Link aggregation[1] (static and dynamic)
- Port redundancy[1]
- A/P high availability with state sync
- A/A clustering[1]
- Inbound/outbound load balancing
- L2 bridge,[1] wire/virtual wire mode, tap mode, NAT mode
- 3G/4G WAN failover[1]
- Asymmetric routing
- Common Access Card (CAC) support
- SonicCoreX and SonicOS Containerization

### Decryption Policy

- Unified Policy for SSL/TLS traffic

### DoS Policy

- Unified Policy for DoS/DDoS attack prevention

### VoIP

- Granular QoS control
- Bandwidth management
- DPI for VoIP traffic
- H.323 gatekeeper and SIP proxy support

### Management and monitoring

- Web GUI
- Command-line interface (CLI)
- Zero-Touch registration & provisioning
- SonicExpress mobile app support
- SNMPv2/v3
- Centralized management and reporting with Network Security Manager (NSM)[2]
- Logging
- Netflow/IPFix exporting
- Cloud-based configuration backup
- BlueCoat security analytics platform
- Application and bandwidth visualizer
- IPv4 and IPv6 Management
- Off-box reporting (Scrutinizer)
- LCD management screen[1]
- Dell N-Series and X-Series switch management including cascaded switches[1]
- CSC Simple Reporting

### Wireless[1]

- SonicWave AP cloud management
- WIDS/WIPS
- Rogue AP prevention
- Fast roaming (802.11k/r/v)
- 802.11s mesh networking
- Auto-channel selection
- RF spectrum analysis
- Floor plan view
- Topology view
- Band steering
- Beamforming
- AirTime fairness
- Bluetooth Low Energy
- MiFi extender
- Guest cyclic quota
- LHM guest portal

[1] Not supported on NS*v* Series firewalls
[2] Requires added subscription
[3] Available only on NSsp firewalls
[4] Available on SonicOSX 7.0.1 onwards

SONICWALL®

# Serie SonicWall NS*sp* Gen 7

La serie SonicWall Network Security services platform™ (NS*sp*) offre firewall di nuova generazione con elevata densità di porte e interfacce a velocità multi-gigabit, in grado di gestire milioni di connessioni alla ricerca di minacce zero-day e avanzate. Progettati per grandi aziende, istituti di istruzione superiore, enti pubblici e MSSP, eliminano gli attacchi in tempo reale senza rallentare le prestazioni. I firewall sono progettati per garantire un'elevata affidabilità, fornendo servizi senza interruzioni alle aziende.


**NS*sp* in breve** Specifiche complete »

| 100 GbE | Fino a 100 Gb/s | 80 milioni |
|---|---|---|
| Porte | Throughput ispezione firewall | Connessioni max. (NS*sp* 15700) |

## CARATTERISTICHE PRINCIPALI

### Serie SonicWall NS*sp*

- Alta densità di porte
- Porte da 100 GbE
- Integrazione con sandbox on-premise e in cloud
- Gestione da un unico pannello
- Throughput di prevenzione minacce oltre 80 Gb/s
- Alimentazione ridondante
- Throughput di ispezione firewall fino a 100 Gb/s
- Supporto per TLS 1.3
- Supporto di milioni di connessioni TLS simultanee
- Basso costo totale di proprietà

**Maggiori informazioni sulla serie SonicWall NS*sp* Gen 7:**

sonicwall.com/NS*sp*

SONICWALL®

## Firewall di classe enterprise

Man mano che le aziende evolvono, aumentano anche i dispositivi gestiti e non gestiti, le reti, i carichi di lavoro nel cloud, le applicazioni SaaS, gli utenti, la velocità di Internet e le connessioni crittografate. Un firewall che non è in grado di supportare tutte queste utenze diventa un collo di bottiglia. Un firewall deve essere un punto di forza, non un punto debole.

Le interfacce multiple a 100G/40G/25G/10G dei firewall SonicWall NS*sp* consentono di gestire milioni di connessioni simultanee, crittografate e non crittografate, con una tecnologia di prevenzione delle minacce senza precedenti. Considerando che il 70% delle sessioni sono crittografate, per garantire la produttività e la sicurezza delle informazioni è fondamentale disporre di un firewall in grado di elaborare ed esaminare questo traffico senza compromettere l'esperienza d'uso.

Le policy unificate di NS*sp* permettono alle aziende di creare policy di accesso e sicurezza da un'unica interfaccia in modo semplice e intuitivo.

## Gestione e reportistica semplificate

La gestione, il monitoraggio e il reporting continuo delle attività di rete sono gestiti tramite il Network Security Manager di SonicWall, che offre un pannello di controllo intuitivo per gestire le operazioni dei firewall e fornire report storici, il tutto da un'unica fonte. Le procedure semplificate di installazione e configurazione e la facilità di gestione consentono alle aziende di ridurre il costo totale di proprietà e ottenere un elevato ritorno sull'investimento.

## Installazione

### Next-Generation Firewall (NGFW)

- Gestione da un unico pannello di controllo
- La serie NS*sp* si integra con il resto dell'ecosistema di soluzioni SonicWall
- Piena visibilità sulla rete per vedere il comportamento di applicazioni, dispositivi e utenti, in modo da applicare policy ed eliminare le minacce e i colli di bottiglia della larghezza di banda
- Integrazione con Capture ATP con RTDMI per le sandbox basate su cloud o con Capture Security Appliance per il rilevamento di malware on-premise

### Ispezione Deep Packet del traffico SSL/TLS (DPI-SSL) per rilevare minacce nascoste

- I firewall NS*sp* consentono di ispezionare milioni di connessioni TLS/SSL ed SSH crittografate simultanee, indipendentemente dalla porta o dal protocollo
- Le regole di inclusione ed esclusione consentono di personalizzare i controlli in base a requisiti di conformità specifici dell'azienda e/o legali
- Supporto di suite di cifratura fino a TLS 1.3

### Segmentazione e connettività di rete

- Funzionamento su diverse reti segmentate, ambienti cloud o servizi definiti con modelli, policy e gruppi di dispositivi univoci per diversi dispositivi e tenant
- Gli MSSP possono anche supportare più clienti con un servizio clean pipe e policy univoche

### Firewall multi-istanza

- La multi-istanza è la nuova generazione della multi-tenancy
- Ogni tenant è isolato con risorse di calcolo dedicate per evitare l'esaurimento delle risorse
- Dispone di porte e tenant fisici e logici
- Supporta la gestione di policy e configurazioni indipendenti per i tenant
- Sfrutta l'indipendenza dalle versioni e il supporto ad alta disponibilità (HA) per i tenant

### Funzioni in modalità Wire

- Modalità Bypass per inserire rapidamente e quasi senza interruzioni i firewall hardware in una rete
- Modalità Inspect per estendere la modalità Bypass senza modificare la funzionalità del percorso dei pacchetti a basso rischio e zero latenza
- Modalità Secure per interporre attivamente i processori multi-core del firewall nel percorso di elaborazione dei pacchetti
- Modalità Tap per acquisire un flusso di pacchetti in mirroring attraverso un'unica porta switch sul firewall, eliminando la necessità di un inserimento fisico intermedio

### Protezione contro le minacce avanzate

- SonicWall Capture Advanced Threat Protection™ (ATP), utilizzato da oltre 150.000 clienti nel mondo in diverse soluzioni, permette di scoprire e bloccare più di 1.200 nuove forme di malware ogni giorno lavorativo
- NS*sp* si integra con Capture Security appliance per rilevare e bloccare minacce sconosciute tramite una sandbox on-premise che usa la tecnologia Real-Time Deep Memory Inspection™ (RTDMI).

### Piattaforma Capture Cloud

- La piattaforma Capture Cloud di SonicWall offre la prevenzione delle minacce basata sul cloud e la gestione della rete, oltre a funzionalità di reporting e analisi, per organizzazioni di qualsiasi dimensione.

### Servizi di filtraggio dei contenuti

- Verifica dei siti web richiesti a fronte di un imponente database nel cloud che contiene milioni di URL, indirizzi IP e siti web classificati.
- Creazione e applicazione di policy che autorizzano o negano l'accesso ai siti in base all'identità individuale o di gruppo, o all'ora del giorno, per oltre 50 categorie predefinite



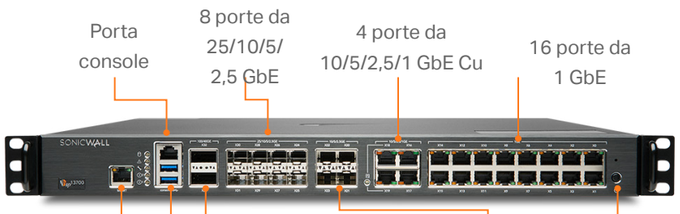
### Sistema di prevenzione delle intrusioni (IPS)

- Offre un motore di ispezione approfondita dei pacchetti configurabile e ad alte prestazioni per la protezione estesa dei principali servizi di rete, come navigazione Web, posta elettronica, trasferimento file, servizi Windows e DNS
- Progettato per fornire protezione dalle vulnerabilità delle applicazioni e da worm, trojan, exploit peer-to-peer, spyware e backdoor exploit
- Il linguaggio ampliabile delle firme consente una difesa proattiva nei confronti delle vulnerabilità scoperte di recente in applicazioni e protocolli
- SonicWall IPS elimina i lunghi e costosi interventi di manutenzione e aggiornamento delle firme per i nuovi attacchi grazie all'architettura leader del settore Distributed Enforcement Architecture (DEA) di SonicWall

### IoT e controllo delle applicazioni

- NS*sp* cataloga migliaia di applicazioni tramite il controllo delle applicazioni e monitora il loro traffico per rilevare comportamenti anomali

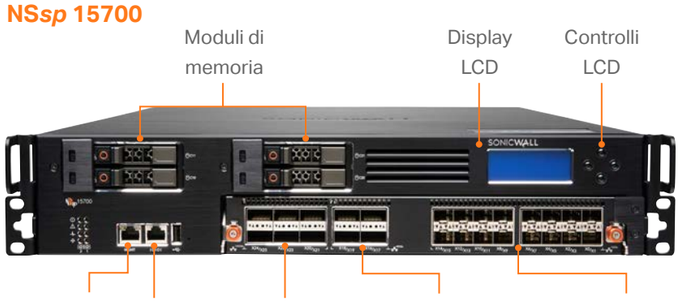
## NS*sp* 13700

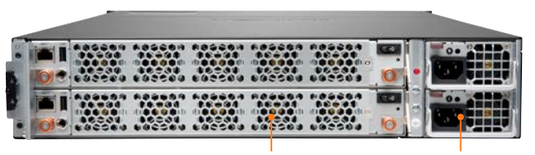




Memoria integrata (512 GB)
Slot di espansione (fino a 1 TB)
3 ventole

## NS*sp* 15700



## Specifiche tecniche SonicWall NS*sp* 13700 e 15700

| Firewall in generale | NS*sp* 13700 | NS*sp* 15700 |
|---|---|---|
| Sistema operativo | SonicOS 7.0 | SonicOSX 7.0 |
| Interfacce | 2x100/40 GbE QSFP28, 8x25/10/5/2,5 GbE SFP28, 4x10/5/2,5 GbE SFP+, 4x10/5/2,5/1 GbE Cu, 16x1 GbE 2 USB 3.0, 1 console, 1 porta gestione | 6 x 100 GbE QSFP28, 4 x 40 GbE QSFP+, 16 x 10 GbE SFP+ |
| Memoria integrata | 512 GB M.2 | 2 x 480 GB SSD |
| Gestione | CLI, SSH, Web UI, API REST | |
| Utenti SSO | 100.000 | |
| Registrazione di log | Analyzer, registro locale, Syslog, IPFIX, NetFlow | |

| Firewall/prestazioni VPN | NS*sp* 13700 | NS*sp* 15700 |
|---|---|---|
| Throughput di ispezione firewall[1] | 60 Gb/s | 105 Gb/s |
| Throughput di prevenzione delle minacce[2] | 45,5 Gb/s | 82 Gb/s |
| Throughput di ispezione applicazioni[2] | 57 Gb/s | 86 Gb/s |
| Throughput IPS[2] | 48 Gb/s | 76,5 Gb/s |
| Throughput IMIX | 20 Gb/s | 28,5 Gb/s |
| Throughput con decrittazione e ispezione TLS/SSL (SSL DPI)[2] | 16,5 Gb/s | 21 Gb/s |
| Throughput VPN[3] | 29 Gb/s | 32 Gb/s |
| Connessioni al secondo | 170.000 | 800.000 |
| Connessioni max. (SPI) | 14 mln. | 80 mln. |
| Connessioni max. (DPI) | 12 mln. | 50 mln. |
| Connessioni max. (DPI SSL) | 1,5 mln. | 3 mln. |

| VPN | NS*sp* 13700 | NS*sp* 15700 |
|---|---|---|
| Tunnel VPN site-to-site | 12.000 | 25.000 |
| Client VPN IPSec (max) | 2000 (6000) | 2000 (10000) |
| Licenze VPN SSL (max) | 2 (3000) | |
| Autenticazione/crittografia | DES, 3DES, AES (128, 192, 256 bit)/MD5, SHA-1, crittografia Suite B | |
| Key exchange | Gruppi Diffie-Hellman 1, 2, 5, 14v | |
| VPN basata su routing | RIP, OSPF, BGP | |
| Caratteristiche VPN | Dead Peer Detection, DHCP su VPN, attraversamento NAT con IPSec, gateway VPN ridondante, VPN basata su routing | |
| Piattaforme client della VPN globale supportate | Microsoft® Windows Vista a 32/64 bit, Windows 7 a 32/64 bit, Windows 8.0 a 32/64 bit, Windows 8.1 a 32/64 bit, Windows 10 | |
| NetExtender | Microsoft Windows Vista a 32/64 bit, Windows 7, Windows 8.0 a 32/64 bit, Windows 8.1 a 32/64 bit, Mac OS X 10.4 e versioni successive, Linux FC3 e versioni successive/Ubuntu 7 e versioni successive/OpenSUSE | |
| Mobile Connect | Apple® iOS, Mac OS X, Google® Android™, Kindle Fire, Chrome, Windows 8.1 (incorporato) | |

| Connettività di rete | NS*sp* 13700 | NS*sp* 15700 |
|---|---|---|
| Firewall multi-istanza | N/D | Tenant massimi per hardware: 12 |
| 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 | 1024 | |
| Modalità Wire | – | Sì |
| Protocolli di routing | BGP4, OSPF, RIPv1/v2, route statici, routing basato su policy | BGP, OSPF, RIPv1/v2, route statici, routing basato su policy |

## Specifiche tecniche SonicWall NS*sp* 13700 e 15700

| Connettività di rete | NS*sp* 13700 | NS*sp* 15700 |
|---|---|---|
| Qualità del servizio (QoS) | Priorità della larghezza di banda, larghezza di banda massima, larghezza di banda garantita, contrassegno DSCP, 802.1p (WMM) | |
| Autenticazione | LDAP (domini multipli), XAUTH/RADIUS, SSO, Novell, database utenti interno, Terminal Services, Citrix, Common Access Card (CAC) | |
| VoIP | Full H323-v1-5, SIP | |
| Standard | TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3 | |
| Certificazioni (in corso) | FIPS 140-2 (con Suite B) Level 2, UC APL, VPNC, IPv6 (Phase 2), ICSA Network Firewall, ICSA Anti-virus, Common Criteria NDPP (Firewall e IPS) | |
| Alta disponibilità | Attiva/Passiva con sincronizzazione dello stato | |

| Hardware | NS*sp* 13700 | NS*sp* 15700 |
|---|---|---|
| Alimentazione | 2x350 W | Doppia, ridondante, 1.200 W |
| Ventole | 3 (rimovibili) | 10 |
| Alimentazione in ingresso | 100-240 VAC, 50-60 Hz | 100-240 VAC, 50-60 Hz |
| Potenza max. assorbita (W) | 181,2 | 1065 |
| Fattore di forma | 1U rack-mount | 2U rack-mount |
| Dimensioni | 43 x 32,5 x 4,5 cm (16,9 x 12,8 x 1,8 in) | 68,6 x 43,8 x 8,8 cm |
| Peso | 9,1 kg | 26 kg |
| Peso RAEE | 11 kg | 30,1 kg |
| Peso con la confezione | 14,9 kg | 37,3 kg |
| Principali normative di conformità | FCC Classe A, CE (EMC, LVD, RoHS), C-Tick, VCCI Classe A, MSIP/KCC Classe A, UL, cUL, TÜV/GS, CB, CoC UL (Messico), RAEE, REACH, ANATEL, BSMI | FCC Class A, ICES Classe A, CE (EMC Classe A, LVD, RoHS), C-Tick, VCCI Classe A, MSIP/KCC Classe A, UL, cUL, TÜV/GS, CB, notifica DGN UL (Messico), RAEE, REACH, ANATEL, BSMI |
| Condizioni ambientali (in funzionamento/stoccaggio) | 0-40 °C (32-105 °F) / da -40 a 70 °C (da -40 a 158 °F) | |
| Umidità | 0-90% relativa, senza condensa | 10-95% senza condensa |

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.
3. Rilevazione throughput VPN tramite traffico UDP con pacchetti da 1280 byte, in conformità a RFC 2544. Tutte le specifiche, le funzioni e le informazioni sulla disponibilità sono soggette a modifiche.


SONICWALL®

# SonicWave Series Wireless Access Points

Secure, Cloud-managed Wireless Solutions

SonicWall SonicWave series wireless access points (APs) combine high-performance IEEE 802.11ac Wave 2 wireless technology with flexible deployment options. These highly secure APs can be managed via the cloud using SonicWall Wireless Network Manager (WNM) or through SonicWall's industry-leading next-generation firewalls. The result is a solution that could be untethered from the firewall to provide a superior experience for Wi-Fi users that's as secure as any wired connection.


**Mounting Options.** View full specs »

| Indoor Wall | Indoor Ceiling | Outdoor |
|---|---|---|
| SonicWave 224w | SonicWave 231c<br>SonicWave 432e<br>SonicWave 432i | SonicWave 231o<br>SonicWave 432o |

## HIGHLIGHTS

### Intuitive cloud management

- Integrated Switch management
- Alerts and rich analytics
- Automatic firmware updates
- Integrated WiFi Planner tool
- Easily switch to firewall management

### Enhanced user experience

- 802.11ac Wave 2
- Auto channel selection
- Application control and visibility
- RF spectrum analysis
- AirTime Fairness and fast roaming

### Best-in-class wireless security

- Dedicated third scanning radio
- WPA3 support
- Capture ATP and content filtering service
- Deep packet inspection technology

### Zero-Touch Deployment powered by SonicExpress mobile app

- Easy registration and onboarding
- Auto-detection and auto-provisioning
- App available on iOS and Android

### Ruggedized outdoor design

- IP67 rated, industrial-grade enclosure

**Find the right SonicWall solution for your small business and branch:**

sonicwall.com/secure-wireless

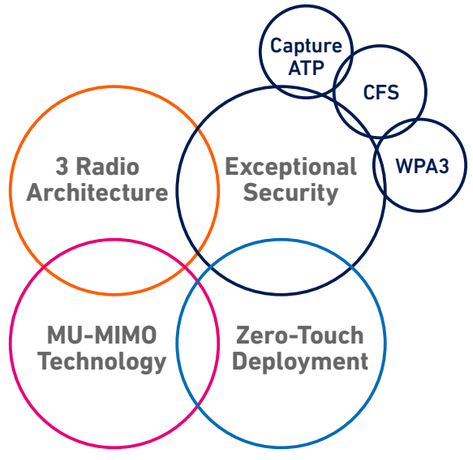
## Intuitive cloud management

SonicWall WNM provides an intuitive user interface to manage all SonicWave APs from a single pane of glass via SonicWall Capture Security Center (CSC). Additionally, the dashboard provides integrated SonicWall Switch management, providing centralized management of switches and APs. Easily monitor and manage networks with alerts and rich analytics updated in real-time. Always stay up-to-date with the current features and enhancements from the latest firmware. Updates are pushed automatically to APs, eliminating manual updates and chances of human error.

## Enhanced user experience

SonicWave APs take advantage of the capabilities in 802.11ac Wave 2 and advanced RF capabilities to deliver high-speed wireless performance. MU-MIMO technology allows the APs to communicate to multiple client devices at the same time, improving the overall network performance, efficiency and user experience. In combination, mesh technology supported on SonicWave APs enables ease of installation and deployment. Mesh networks are easy to set up, effortless to expand, and require fewer cables and less manpower to deploy, reducing installation costs.

With multiple transmitting and receiving antennas, SonicWave APs are engineered to optimize signal quality, range and reliability for wireless devices. SonicWave APs supports fast roaming, so that users can roam from one location to another seamlessly. Feature-rich portfolio includes air-time fairness, band steering, and signal analysis tools for monitoring and troubleshooting.




## Best-in-class wireless security

SonicWall firewalls scan all wireless traffic coming into and going out of the network using deep packet inspection technology and then remove harmful threats such as malware and intrusions, even over SSL/TLS encrypted connections. Other security and control capabilities such as content filtering, application control and intelligence and Capture Advanced Threat Protection (ATP) provide added layers of protection.

Capture ATP is our award-winning multi-engine sandboxing service that features SonicWall's patent-pending Real-Time Deep Memory Inspection (RTDMI™) technology. The RTDMI engine of Capture ATP proactively detects and blocks mass market, zero-day threats and unknown malware by inspecting directly in memory. Because of the real-time architecture, SonicWall RTDMI technology is precise, minimizes false positives, and identifies and mitigates sophisticated attacks where the malware's weaponry is exposed for less than 100 nanoseconds.

## Manage SonicWave APs independently — even where firewalls are not deployed.

Most SonicWave APs include three radios, where the third radio is dedicated to security and performs rogue AP detection, passive scanning and packet capturing. The SonicWave solution also integrates additional security-related features including wireless intrusion detection and prevention, virtual AP segmentation, wireless guest services, RF monitoring and wireless packet capture.

## Simplified firewall management

Deployment and setup of APs are greatly simplified, reducing total cost of ownership. Optionally, SonicWave APs can be managed by SonicWall next-gen firewalls. Integrated into every SonicWall firewall is a wireless controller that auto-detects and auto-provisions SonicWave APs across the network.

Management and monitoring for wireless and security are handled centrally through the firewall, providing network administrators with a single pane of glass from which to manage all aspects of the network.

## Zero-Touch Deployment (ZTD) powered by SonicExpress app

Easily register and onboard SonicWave APs with the help of SonicWall SonicExpress mobile app. The APs are automatically detected and provisioned with Zero-Touch Deployment. Available on iOS and Android, SonicExpress mobile app lets network admins monitor and manage networks.

## Design with WiFi Planner

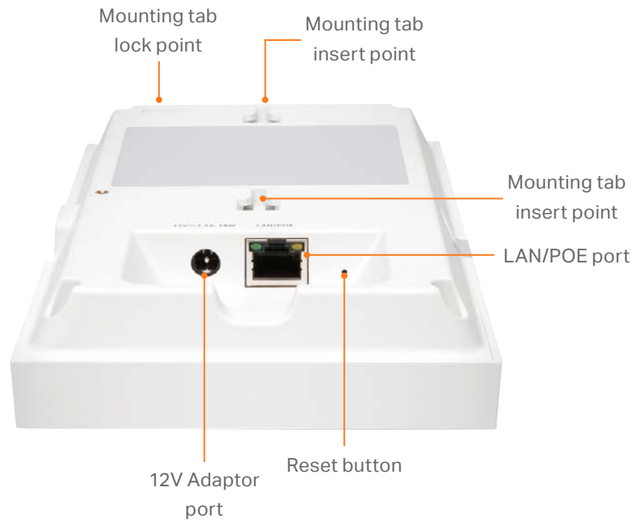
SonicWall WiFi planner is a cloud-based, advanced wireless site survey tool that enables to optimally design and deploy a wireless network for enhanced wireless user experience.

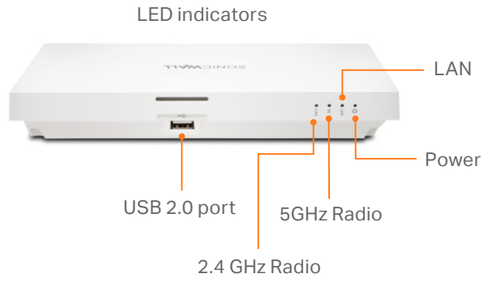
## Ruggedized outdoor design

SonicWave outdoor APs are built to withstand rough outdoor conditions with industrial-grade enclosure. These APs are IP67 rated, which ensures protection against dust and water immersion.

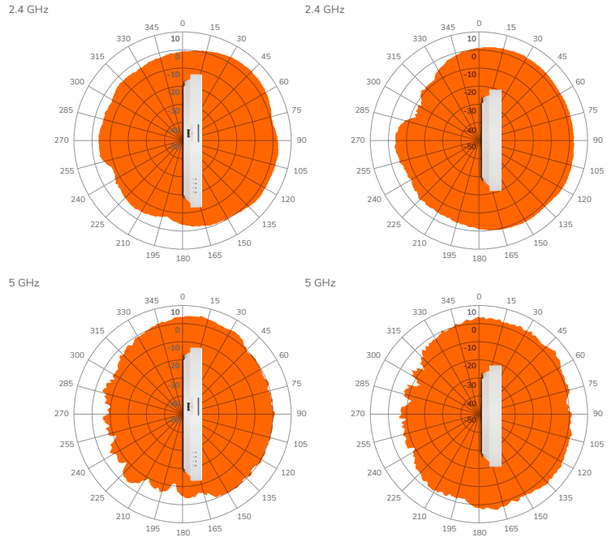



## SonicWave 231c – The Ceiling Mount AP



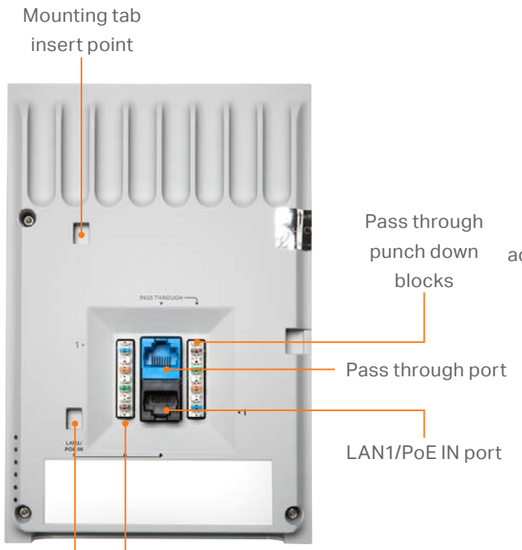

### RF coverage maps

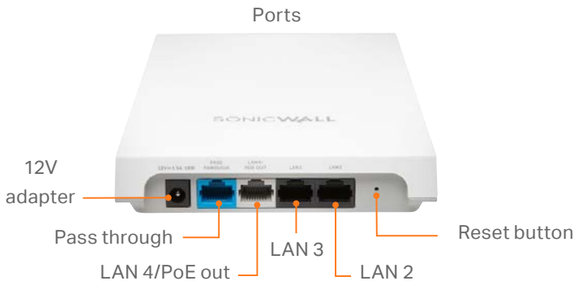


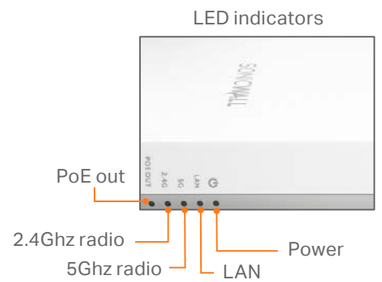

SONICWALL®

SONICWALL®

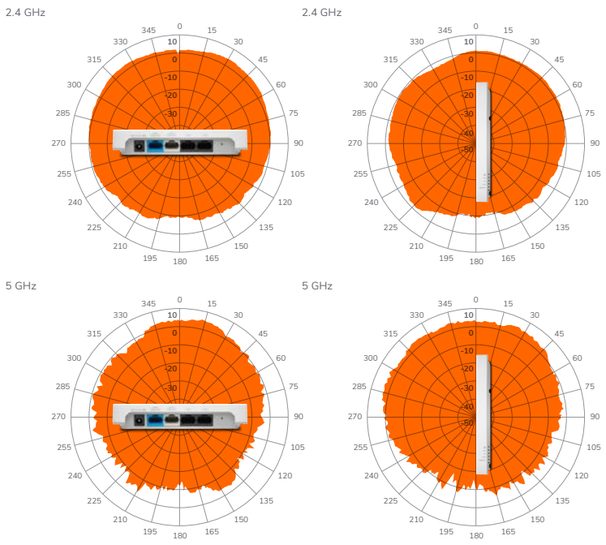
## SonicWave 224w – The Wall Mount AP



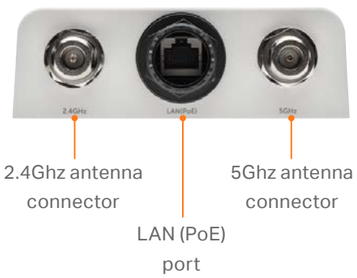




### RF coverage maps

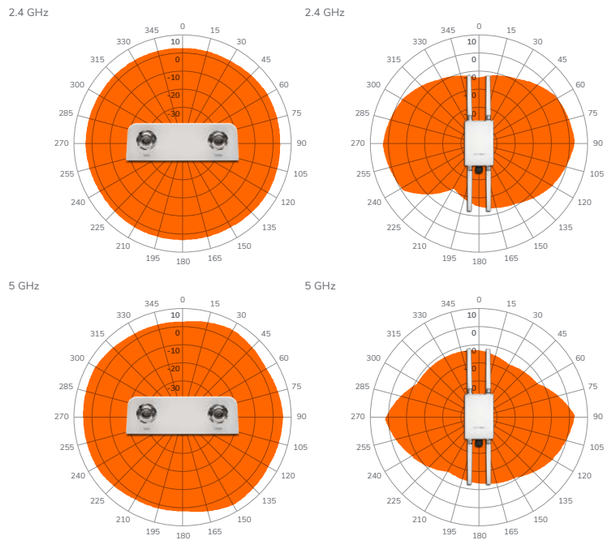



## SonicWave 231o – The Outdoor Mount AP






### RF coverage maps




SONICWALL®

SONICWALL®

## SonicWave 200 Series Specifications

| HARDWARE SPECIFICATIONS | SONICWAVE 231c | SONICWAVE 224w | SONICWAVE 231o |
|---|---|---|---|
| Location | Ceiling | Wall | Outdoor |
| Radio | | 2x2 802.11ac Wave 2 | |
| Dedicated 3rd scanning radio | Yes | No | Yes |
| 5G/4G/LTE USB modem support | Yes | No | No |
| Bluetooth Low Energy (BLE) radio | Yes | Yes | Yes |
| Antenna type | Internal | Internal | Omni-Antenna |
| Dimensions | 118mmx214mmx34m | 122mmx188mmx18mm | 190mmx120mmx42mm |
| Shipping dimension | 150mm x240mm x 73mm | 150mm x240mm x 73mm | 265mmx450mmx78mm |
| Unit weight | 0.4 kg | 0.4 kg | 0.7 kg |
| WEEE weight | 0.7 Kg | 0.7 Kg | 2.0 kg |
| Shipping weight | 0.7 Kg | 0.7 Kg | 2.0 kg |
| PoE | 802.3at<br>802.3af (compatible) | 802.3at<br>802.3af (compatible) | 802.3at<br>802.3af (compatible) |
| | DC 12V adapter (optional) | DC 12V adapter (optional) | (PoE sold separately) |
| Maximum power consumption (W) | 12W | 12W | 12W |
| Status indicators | 4 | 5 | 4 |
| Wired network ports | 1 x 10/100/1000 auto-sensing RJ-45 | 3 x 10/100/1000, 2x 10/100/1000 PoE pass through, 1 LAN PoE Out LAN ports | 1 x 10/100/1000 auto-sensing RJ-45 |
| Accessories included | Ceiling/wall mounting kit | | NEMA 4X Mounting kit and external antennas |
| Virtual access points/SSID group | Up to 8 per access point | | |
| Chassis | Rectangle | | |
| USB WAN card security clamp | Yes | N/A | N/A |

| STANDARDS AND COMPLIANCE | SONICWAVE 231c | SONICWAVE 224w | SONICWAVE 231o |
|---|---|---|---|
| IEEE Standards | 802.11ac Wave 2, 802.11ac, 802.11n, 802.11g, 802.11b, 802.11a, 802.11e, 802.11i, 802.11r, 802.11k, 802.11v, 802.11w | | |
| Compliance | IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, IEEE 802.11e, IEEE 802.11i, IEEE 802.3at, IEEE 802.3bz, WPA, TKIP, AES, IEEE 802.11r, IEEE 802.11k, IEEE 802.11v, IEEE 802.11w | | |
| Wi-Fi Alliance Certification ID | WFA78807 | WFA78829 | WFA78878 |
| Plenum rated | Yes | No | No |
| Regulatory | FCC, IC/ISED, CE, RCM, NCC, TELEC, KCC | | |
| Safety Approvals | UL E211396, UL 62368-1, UL 60950-1cUL CAN/CSA C22.2 No. 62368-1-14, CAN/CSA C22.2 No. 62368-1-14 EN 60950-1 Or EN 62368-1 IEC 60950-1, IEC 62368-1, Europe: EN 60950-1, EN 62368-1, Taiwan: CNS 1336-1 | | |
| Radio Approvals | USA: FCC Part 15C, 15,E Canada: ISED RSS-247, Europe: (RED) EN 300 328, EN 301 893, Aus/NZ: AS/NZs 4268, Taiwan: NCC LP002, Additional country approvals for Japan, Korea, China, India, Brazil | | |
| EMI Approvals | USA: FCC P15B, Canada: ICES-003, Europe: EN 301 489-1, -17, EN 55032, EN 55024, Aus/NZ: CISPR 32, Japan: VCCI, Taiwan: CNS 13438 | | |
| Exposure Approvals | USA: FCC Part 2, Canada: RSS-102, Europe: EN 50385, Aus/Nz: ASNZS 2772 | | |
| MIMO | MU-MIMO 2x2 (2 streams) | | |
| Max/Recommended connected clients per radio | 128/32 | | |
| USB WAN failover and load balancing | Yes | N/A | N/A |

| ENVIRONMENTAL | SONICWAVE 231c | SONICWAVE 224w | SONICWAVE 231o |
|---|---|---|---|
| Temperature range | 0° to 40°C | 0° to 40°C | -30° to 60°C |
| Humidity | 0%~95% typical, elevation 50,000 ft | 0%~95% typical, elevation 50,000 ft | 5%~90% typical |

| RADIO SPECIFICATIONS | SONICWAVE 231c | SONICWAVE 224w | SONICWAVE 231o |
|---|---|---|---|
| Radios | 3 radios - 5GHz, 2.4GHz and security radio | 2 radios - 5GHz and 2.4GHz | 3 radios - 5GHz, 2.4GHz and security radio |
| Frequency bands | IEEE 802.11 b/g/n: 2.412-2.484 GHz; IEEE 802.11a/n/ac: 5.150-5.250 GHz (UNII-1), 5.250-5.350 GHZ (UNII-2), 5.470-5.600, 5.660-5.725 GHz (UNII-2e), 5.725-5.825 GHz (UNII-3) | | |
| Operating channels | 2.4GHz channels : 1-13;<br>5 GHz channels: 36-64, 100-140, 149-165 | | |
| Transmit output power | Based on the regulatory domain product is installed in and specified by the system administrator | | |
| Transmit power control | Supported | | |
| Data rates supported | 867 Mbps for 5GHz radio, 400Mbps for 2.4GHz radio | | |
| Modulation technology spectrum | 802.11ac: Orthogonal Frequency Division Multiplexing (OFDM) | | |

| SECURITY | SONICWAVE 231c | SONICWAVE 224w | SONICWAVE 231o |
|---|---|---|---|
| Data encryption | WPA3, WPA2, IPSec, 802.11i, WPA; 64/128/152-bit WEP, TKIP, AES, SSL VPN** | | |
| SSL-VPN client* | NetExtender, Connect Tunnel | | |
| Advanced security services | Capture ATP, CFS, Geo-IP, Botnet, Anti-virus (Cloud) | | |

| AUTHENTICATION | SONICWAVE 231c | SONICWAVE 224w | SONICWAVE 231o |
|---|---|---|---|
| Authentication | RADIUS, Active Directory, single sign-on (SSO), local user | | |
| Captive Portal | Click-through, external server, social account (facebook, google, twitter and linkedin), sign on | | |
| Captive Portal Sign On | Local users, RADIUS, LDAP, OTP, AD | | |

| REPORTING | SONICWAVE 231c | SONICWAVE 224w | SONICWAVE 231o |
|---|---|---|---|
| Alerts | Critical alert notification via SMS | | |

*SonicWave acts as an SSL-VPN client
**When used with SonicWall Secure Mobile Access Series appliance

## SonicWave 400 Series Specifications

| HARDWARE SPECIFICATIONS | SONICWAVE 432e | SONICWAVE 432i | SONICWAVE 432o |
|---|---|---|---|
| Location | Indoor | Indoor | Outdoor |
| Dimensions | 8.5 (D) x 2.0 (H) in<br>21.6 (D) x 5.1 (H) cm | 8.5 (D) x 2.0 (H) in<br>21.6 (D) x 5.1 (H) cm | 9.5 (W) x 9.3 (D) x 2.4 (H) in<br>24.1 (W) x 23.6 (D) x 6.1 (H) cm |
| Weight | 1.1 kg / 2.5 lbs | 1.0 kg / 2.2 lbs | 2.2 kg / 4.9 lbs |
| WEEE weight | 1.4 kg / 3.1 lbs | 1.2 kg / 2.6 lbs | 4.1 kg / 9.1 lbs |
| Shipping weight | 1.7 kg / 3.8 lbs | 1.5 kg / 3.3 lbs | 4.7 kg / 10.4 lbs |
| PoE injector | | 802.3at | |
| Maximum power consumption (W) | 18.8 W | 18.8 W | 21.2 W |
| Status indicators | Six (6) LED (WLAN/Link) (LAN/Link) Power, Test | | |
| Antennas | 4+4 (SMA 2.4 GHz + TNC 5 GHz) | 8 fully internal | 8 N-type dipole |
| Wired network ports | (1) 10/100/1000 auto-sensing RJ-45 for Ethernet and Power over Ethernet (PoE); (1) 100/1000/2.5 GbE auto-sensing RJ-45 for Ethernet; (1) RJ-45 console; (1) USB 2.0 (except 432o) | | |
| 5G/4G/LTE USB modem support | Yes | Yes | Yes |

SONICWALL®

SONICWALL®

| HARDWARE SPECIFICATIONS | SONICWAVE 432e | SONICWAVE 432i | SONICWAVE 432o |
|---|---|---|---|
| Accessories included | Wall/ceiling mount kit | Wall/ceiling mount kit | Pole mount kit |
| Virtual access points/SSID group | | Up to 8 per access point | |
| Chassis | | UL 1024 plenum rated | |
| USB WAN card security clamp | Yes | Yes | N/A |

| STANDARDS AND COMPLIANCE | SONICWAVE 432e | SONICWAVE 432i | SONICWAVE 432o |
|---|---|---|---|
| IEEE Standards | 802.11ac Wave 2, 802.11ac, 802.11n, 802.11g, 802.11b, 802.11a, 802.11e, 802.11i, 802.11r, 802.11k, 802.11v, 802.11w | | |
| Compliance | IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, IEEE 802.11e, IEEE 802.11i, IEEE 802.3at, IEEE 802.3bz, WPA, TKIP, AES, IEEE 802.11r, IEEE 802.11k, IEEE 802.11v, IEEE 802.11w | | |
| Wi-Fi Alliance Certification ID | WFA74776 | WFA74777 | WFA74189 |
| Regulatory | FCC/ICES Class B, CE, RCM/ACMA, VCCI Class B, TELEC, BSMI, NCC, MSIP, ANATEL, Customs Union, RoHS (Europe/China), WEEE | | |
| Safety Approvals | UL E211396, UL 62368-1, UL 60950-1 cUL CAN/CSA C22.2 No. 62368-1-14, CAN/CSA C22.2 No. 62368-1-14, EN 60950-1 Or EN 62368-1, IEC 60950-1, IEC 62368-1, Europe: EN 60950-1, EN 62368-1, Taiwan: CNS 1336-1 | | |
| Radio Approvals | USA: FCC Part 15C, 15E, Canada: ISED RSS-247, Europe: (RED) EN 300 328, EN 301 893, Aus/NZ: AS/NZs 4268, Taiwan: NCC LP002, Additional country approvals for Japan, Korea, China, India, Brazil | | |
| EMI Approvals | USA: FCC P15B, Canada: ICES-003, Europe: EN 301 489-1, -17, EN 55032, EN 55024, Aus/NZ: CISPR 32, Japan: VCCI, Taiwan: CNS 13438 | | |
| Exposure Approvals | USA: FCC Part 2, Canada: RSS-102, Europe: EN 50385, Aus/Nz: ASNZS 2772 | | |
| MIMO | MU-MIMO 4x4 (4 streams) | | |
| Max/Recommended connected clients per radio | 128/48 | | |
| Safety | UL, cUL, TUV/GS, CB, CE, BSMI, Mexico CoC, Customs Union | | |
| USB WAN failover and load balancing | Yes | Yes | N/A |

| ENVIRONMENTAL | SONICWAVE 432e | SONICWAVE 432i | SONICWAVE 432o |
|---|---|---|---|
| Temperature range | 32 to 104°F, 0 to 40°C | | -40 to 140°F, -40 to 60°C |
| Humidity | 10 - 95%, non-condensing | | |

| RADIO SPECIFICATIONS | SONICWAVE 432e | SONICWAVE 432i | SONICWAVE 432o |
|---|---|---|---|
| Radios | Dual: 4x4 11n + 4x4 11ac MU-MIMO; Dedicated third scanning radio; Bluetooth Low Energy radio | | |
| Frequency bands | 802.11a: 5.180-5.825 GHz, 802.11b/g: 2.412-2.472 GHz, 802.11n: 2.412-2.472 GHz, 5.180-5.825 GHz, 802.11ac: 2.412-2.472 GHz, 5.180-5.825 GHz | | |
| Operating channels | 802.11a: US and Canada 12, Europe 11, Japan 4, Singapore 4, Taiwan 4, 802.11b/g: US and Canada 1-11, Europe 1-13, Japan 1-14 (14-802.11b only), 802.11n (2.4 GHz): US and Canada 1-11, Europe 1-13, Japan 1-13 802.11n (5 GHz): US and Canada 36-48/149-165, Europe 36-48, Japan 36-48, Spain 36-48/52-64 802.11ac: US and Canada 36-48/149-165, Europe 36-48, Japan 36-48, Spain 36-48/52-64 | | |
| Transmit output power | Based on the regulatory domain specified by the system administrator | | |
| Transmit power control | Supported | | |
| Data rates supported | 802.11a: 6,9,12,18,24,36,48,54 Mbps per channel, 802.11b: 1,2,5.5,11 Mbps per channel, 802.11g: 6,9,12,18,24,36,48,54 Mbps per channel, 802.11n: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 15, 30, 45, 60, 90, 120, 135, 150 Mbps per channel, 802.11ac: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 86.7, 96.3, 15, 30, 45, 60, 90, 120, 135, 150, 180, 200, 32.5, 65, 97.5, 130, 195, 260, 292.5, 325, 390, 433.3, 65, 130, 195, 260, 390, 520, 585, 650, 780, 866.7, 1040, 1170, 1300, 1560, 1733.4 Mbps per channel | | |
| Modulation technology spectrum | 802.11a: Orthogonal Frequency Division Multiplexing (OFDM), 802.11b: Direct Sequence Spread Spectrum (DSSS), 802.11g: Orthogonal Frequency Division Multiplexing (OFDM)/Direct Sequence Spread Spectrum (DSSS), 802.11n: Orthogonal Frequency Division Multiplexing (OFDM), 802.11ac: Orthogonal Frequency Division Multiplexing (OFDM) | | |

SONICWALL®

SONICWALL®

# Switch SonicWall

Gli switch SonicWall si caratterizzano per lo switching di rete a velocità elevata, che garantisce prestazioni e gestibilità senza confronti. Le condizioni di sicurezza unificate, l'elevata densità di porte, le opzioni Power over Ethernet (PoE) e le prestazioni a livello multi-gigabit ne fanno l'ideale per le PMI e la tecnologia Software-Defined Branch (SD-Branch). Ciò consente alle aziende di qualsiasi dimensione di affrontare la trasformazione digitale restando al passo con i cambiamenti degli ambienti di rete e della sicurezza.

La soluzione SonicWall Secure SD-Branch trasforma la modalità di lavoro degli utenti delle filiali mettendo a disposizione una piattaforma unificata che consente l'installazione delle filiali nel giro di pochi minuti e la visibilità e il rilevamento delle minacce centralizzati da un unico pannello di controllo. La soluzione SonicWall SD-Branch comprende firewall SonicWall di prossima generazione con SD-WAN sicura, Capture Security Center con installazione Zero-Touch, switch SonicWall, access point (AP) SonicWave, Capture Client e Cloud App Security. Grazie alla flessibilità offerta da SonicWall Secure SD-Branch, le organizzazioni possono ora diventare più agili, aperte e incentrate sul cloud.

Gli switch SonicWall, che sono un elemento integrante della trasformazione delle filiali di prossima generazione sono gestiti attraverso firewall per consentire la gestione centralizzata da un unico pannello di controllo dell'intera infrastruttura SonicWall. Grazie alla stretta integrazione con i firewall, SonicWall Secure SD-Branch beneficia di condizioni di sicurezza unificate e costituisce una soluzione di sicurezza end-to-end che semplifica l'installazione la gestione e la risoluzione delle avarie. Ciò garantisce una sicurezza senza soluzione di continuità ed elimina le lacune delle condizioni di sicurezza che possono verificarsi con gli switch di terzi.

L'abbinamento con gli switch SonicWall consente l'installazione Zero-Touch, con possibilità di mettere rapidamente in funzione i dispositivi nelle filiali diffuse a livello globale. Gli amministratori possono installare gli switch in modo rapido e sicuro presso nuove sedi senza dover ricorrere a costoso personale specializzato in loco.

Questi switch impilabili, ricchi di funzioni, sono disponibili in formato compatto con una concezione a risparmio energetico. Disponibili in sette modelli, che vanno da 8 a 48 tra porte Ethernet gigabit e 10 gigabit, gli switch funzionano in modo integrato con i firewall SonicWall di prossima generazione e gli access point SonicWave per realizzare una rete sicura multi-gigabit end-to-end. Le porte Ethernet dispongono di opzioni PoE per alimentare diversi dispositivi come AP, telefoni VOIP e telecamere IP.

È possibile dare priorità a determinati tipi di traffico in rete come VOIP per videoconferenze lavorando da casa, con funzioni come QoS. È possibile segmentare facilmente i dispositivi in rete e garantire la conformità. La segregazione può essere effettuata definendo politiche o VLAN. Funzioni come l'autenticazione 802.1X consentono alle aziende di mantenere la conformità PCI.

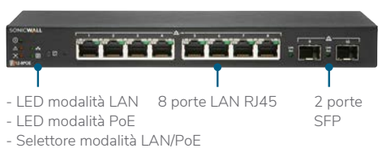
Vantaggi:

- Compatibilità SD-Branch
- Gestione da firewall
- Installazione Zero-Touch
- Condizioni di sicurezza unificate
- Switching di livello 2
- Prestazioni multi-gigabit
- Modelli a 8/24/48 porte
- Diverse opzioni PoE
- Supporto QoS
- Possibilità di impilamento switch
- Segmentazione e conformità
- Formato compatto
- Concezione a risparmio energetico

## Offerta di prodotti

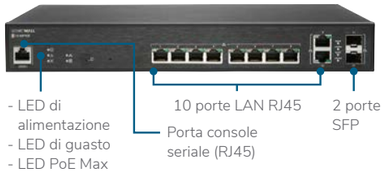
| Modello | Numero di porte Ethernet Gigabit | Numero di porte SFP/SFP+ | Versione PoE |
|---|---|---|---|
| SWS12-8 | 8 | 2 SFP | Non-PoE |
| SWS12-8POE | 8 | 2 SFP | PoE |
| SWS12-10FPOE | 10 | 2 SFP | Full PoE |
| SWS14-24 | 24 | 4 SFP+ | Non-PoE |
| SWS14-24FPOE | 24 | 4 SFP+ | Full PoE |
| SWS14-48 | 48 | 4 SFP+ | Non-PoE |
| SWS14-48FPOE | 48 | 4 SFP+ | Full PoE |

SWS12-8


SWS12-8POE

SWS12-10FPOE




SWS14-24



SWS14-24FPOE

SWS14-48



SWS14-48FPOE

## Specifiche

| Hardware | SWS12-8 | SWS12-8POE | SWS12-10FPOE | SWS14-24 | SWS14-24FPOE | SWS14-48 | SWS14-48FPOE |
|---|---|---|---|---|---|---|---|
| 1G Cu | 8 | 8 | 10 | 24 | 24 | 48 | 48 |
| 1G SFP | 2 | 2 | 2 | - | - | - | - |
| 10G SFP+ | - | - | - | 4 | 4 | 4 | 4 |
| Interfacce totali | 10 | 10 | 12 | 28 | 28 | 52 | 52 |
| Memoria (MB) | 256 | 256 | 256 | 512 | 512 | 512 | 512 |
| Flash (MB) | 32 | 32 | 32 | 128 | 128 | 128 | 128 |
| Packet Buf. | 512K | 512K | 512K | 1.5M | 1.5M | 2M | 2M |
| Tabella Mac | 8K | 8K | 8K | 32K | 32K | 32K | 32K |
| Switching (Gbps) | 20 | 20 | 24 | 128 | 128 | 176 | 176 |
| Ventola | - | - | 1 | - | 2 | 1 | 1 |
| Standard PoE | - | 802.3af | 802.3af/at | - | 802.3af/at | - | 802.3af/at |
| Potenza PoE (Watt) | - | 55 | 130 | - | 410 | - | 740 |
| Alimentazione | Alimentatore 24 W | Alimentatore 65 W | 180 W fissi | 25 W fissi | 480 W fissi | 60 W fissi | 900 W fissi |
| Sorgente di alimentazione | Alimentatore 12 Vcc | Alimentatore 54 Vcc | 100-240 Vca, 50-60 Hz | 100-240 Vca, 50-60 Hz | 100-240 Vca, 50-60 Hz | 100-240 Vca, 50-60 Hz | 100-240 Vca, 50-60 Hz |
| Consumo di corrente (medio/massimo) | 5,7 W | 73,3 W | 152,8 W | 36 W | 500,4 W | 54 W | 530 W |
| Attuale | 2,0 A | 1,2 A | 2,5 A | 0,7 A | 7,0 A | 1,5 A | 12,0 A |
| Dissipazione termica | 19,4 | 249,5 | 521,1 | 122,8 | 1706,4 | 184,2 | 1807,3 |
| Amperaggio minimo del cavo di alimentazione* | 10 Amp | 10 Amp | 10 Amp | 10 Amp | 10 Amp | 10 Amp | 12 Amp |
| Temperatura di funzionamento | 0 - 40 °C | 0 - 40 °C | 0 - 40 °C | 0 - 40 °C | 0 - 40 °C | 0 - 40 °C | 0 - 40 °C |
| Temperatura di conservazione | -40 - 70 °C | -40 - 70 °C | -40 - 70 °C | -40 - 70 °C | -40 - 70 °C | -40 - 70 °C | -40 - 70 °C |
| Umidità | 10-95% U.R. | 10-95% U.R. | 10-95% U.R. | 10-95% U.R. | 10-95% U.R. | 10-95% U.R. | 10-95% U.R. |
| Dimensioni (L x A x P) | 240 x 105 x 27 mm | 240 x 105 x 27 mm | 330 x 230 x 44 mm | 440 x 200 x 44 mm | 440 x 260 x 44 mm | 440 x 260 x 44 mm | 440 x 310 x 44 mm |
| Peso | 0,62 kg | 0,64 kg | 2,5 kg | 1,8 kg | 3,9 kg | 3,2 kg | 4,8 kg |
| Porta console seriale RJ-45 | - | - | - | 1 | 1 | 1 | 1 |
| Fattore di forma | Desktop | Desktop | Desktop | 1U | 1U | 1U | 1U |
| MTBF a 25°C in ore | 1.387.712 | 548.553 | 180.837 | 1.273.866 | 157.763 | 222.974 | 100.645 |
| MTBF a 25°C in anni | 158 | 62 | 20 | 145 | 18 | 25 | 11 |
| Consumo di corrente (medio/massimo) | 5,7 W | 73,3 W | 152,8 W | 36 W | 500,4 W | 54 W | 530 W |
| Capacità di switching (duplex) in Gbps | 20 | 20 | 24 | 128 | 128 | 176 | 176 |
| VLAN | 4096 | 4096 | 4096 | 4096 | 4096 | 4096 | 4096 |
| Modello normativo | APL51-0E1 | APL52-0E2 | 1RK43-0E3 | 1RK44-0E4 | 1RK45-0E5 | 1RK46-0E6 | 1RK47-0E7 |
| Approvazioni normative | FCC Classe A, ICES Classe A, CE (EMC Classe A, LVD, RoHS), C-Tick, VCCI Classe A, UL cUL, TUV/GS, CB, notifica UL DGN Messico, RAEE, REACH, BSMI, KCC/MSIP, ANATEL | | | | | | |

* Verificare con il personale di vendita locale o con i rivenditori per esser certi di utilizzare il cavo di alimentazione corretto

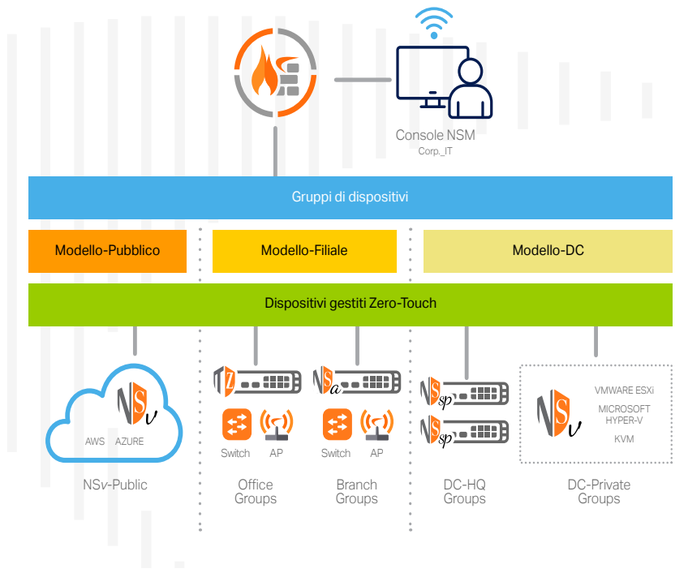
SONICWALL®

SONICWALL®

# Network Security Manager

Sistema unificato e scalabile di gestione firewall per qualsiasi ambiente

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




## CARATTERISTICHE PRINCIPALI

### Business

- Riduzione dei costi di gestione della sicurezza
- Conoscenza del panorama delle minacce e della situazione di sicurezza
- 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

SONICWALL®

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.

SONICWALL®

### 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].



SONICWALL®

## 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 |

SONICWALL®

## 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 |


SONICWALL®

# SonicWall Capture Client

Le minacce in continua espansione del ransomware e di altri attacchi malware dannosi hanno dimostrato che le soluzioni di protezione dei client non possono essere valutate esclusivamente in base alla conformità dell'endpoint. La tecnologia antivirus tradizionale utilizza un approccio controverso basato sulle segnature, che non è riuscito a tenere il passo delle tecniche di malware e di evasione emergenti. Inoltre, con la proliferazione del telelavoro, della mobilità e del BYOD, c'è urgente necessità di avere una protezione coerente degli endpoint dovunque si trovino.

SonicWall Capture Client è un endpoint unificato caratterizzato da funzioni di protezione multiple. Tramite l'engine di protezione dai malware di prossima generazione messo a punto da SentinelOne, Capture Client utilizza tecniche avanzate di protezione dalle minacce, come l'apprendimento automatico, l'integrazione della sandbox di rete e il ripristino dei sistemi all'ultima configurazione non compromessa. Inoltre consente l'ispezione approfondita del traffico TLS crittografato (DPI-SSL) sui firewall SonicWall tramite l'installazione e la gestione di certificati TLS affidabili.

Capture Client coabita con il client Global VPN di SonicWall, e le politiche per tutti i prodotti possono essere gestite da un'unica consolle nel cloud. Capture Client può essere facilmente integrato in qualsiasi client installato tramite politiche di gruppo Microsoft Active Directory, altre tecniche di installazione software di terzi o ancora mediante fornitura di URL personalizzati, dove i client possono effettuare il download e l'autoinstallazione in modo silente senza ulteriori interventi.

Inoltre, grazie all'integrazione con i firewall SonicWall, Capture Client consente un'installazione zero-touch su client non protetti con funzioni di attivazione opzionali.

## Caratteristiche e vantaggi

**Monitoraggio comportamentale continuo del client**: contribuisce a definire un profilo completo delle attività dei file, delle applicazioni, dei processi e di rete, il che rende possibile la protezione dai malware basati o meno su file e fornisce una visione a 360 gradi degli attacchi, con la relativa intelligenza azionabile per le indagini.

**Tecniche di protezione multilivello di tipo euristico**: comprendono l'intelligenza del cloud, l'analisi statica avanzata e la protezione comportamentale dinamica, il che contribuisce alla protezione e al contrasto contro i malware noti e non.

**Nessuna esigenza di scansioni regolari e di aggiornamenti periodici**: massimo livello di protezione in qualsiasi momento senza penalizzare la produttività degli utenti. Capture Client esegue una scansione completa al momento dell'installazione e successivamente effettua il monitoraggio continuo per individuare attività sospette.

**Integrazione di Capture Advanced Threat Protection (ATP)**: trasferisce automaticamente i file sospetti per l'analisi avanzata in sandbox tramite manipolazione del codice che l'endpoint non è in grado di eseguire. Blocca un maggior numero di minacce prima che vengano eseguite, come il malware a scoppio ritardato. Gli amministratori possono anche consultare il database delle valutazioni dei file di Capture ATP senza

## Vantaggi:

- Gestione indipendente basata su cloud
- Sinergia con i firewall SonicWall
- Attuazione delle politiche di sicurezza
- Gestione dei certificati DPI-SSL
- Monitoraggio continuo del comportamento
- Determinazione accurata tramite apprendimento automatico
- Tecniche multilivello basate su metodi euristici
- Intelligenza delle vulnerabilità delle applicazioni
- Capacità di ripristino esclusive
- Facilità di inserimento white list/ blanck list
- Sandbox cloud Capture Advanced Threat Protection (ATP) per analisi automatica dei malware
- Condivisione dell'intelligenza delle minacce per la verifica manuale dei file senza bisogno di trasferimento
- Filtraggio dei contenuti
- Controllo dispositivi

**Capacità di ripristino esclusive**: supporta anche politiche che non si limitano ad eliminare completamente la minaccia, ma riportano il cloud preso di mira allo stato precedente l'inizio dell'attività del malware, il che elimina l'esigenza di ripristino manuale in caso di ransomware e di attacchi simili in ambiente Windows.

**Intelligenza delle vulnerabilità delle applicazioni**: mette a disposizione degli amministratori la possibilità di catalogare tutte le applicazioni nei singoli endpoint protetti e gli eventuali rischi ad esse associati. Il rischio è basato sulla presenza di eventuali vulnerabilità conosciute con informazioni dettagliate sulle CVE e sui livelli di gravità dichiarati per quella versione, mettendo a disposizione degli amministratori l'intelligenza azionabile per definire le priorità degli aggiornamenti e ridurre la superficie di attacco degli endpoint.

**Integrazione opzionale con firewall SonicWall di 6ª generazione e successivi**: consente l'installazione zero-touch e la conformità avanzata dell'endpoint, oltre ad abilitare l'attivazione dell'ispezione deep packet del traffico crittografato (DPI-SSL) installando certificati affidabili sui singoli endpoint.

**Filtraggio dei contenuti**: consente alle organizzazioni di bloccare gli indirizzi IP e i domìni dei siti dannosi, e di aumentare la produttività degli utenti riducendo l'ampiezza di banda o limitando l'accesso a contenuti web dubbi o improduttivi.

**Controllo dispositivi**: consente alle organizzazioni di impedire ai dispositivi potenzialmente infettati di collegarsi agli endpoint grazie a politiche granulari di inserimento nelle white list.

**Gestione centralizzata e reportistica di protezione del client**: la consolle di gestione SonicWall basata su cloud funge da unico pannello di controllo per la gestione a livello del client, compresi la protezione contro il malware di prossima generazione, la gestione dei certificati DPI-SSL e il filtraggio dei contenuti

La consolle di gestione è una piattaforma multi-tenant basata su cloud, offerta senza maggiorazione di costo, Prevede la reportistica sulla protezione dei client e la gestione delle politiche, supportando politiche di controllo accessi minuziose, compresa la possibilità di assegnare le politiche sulla base degli attributi di Microsoft Active Directory. Ciò consente ai fornitori di servizi gestiti (MSP) di effettuare la gestione e la reportistica sui client di diversi clienti, mentre i singoli clienti possono effettuare la gestione e la reportistica solo dei loro client.

La consolle di gestione funge inoltre da piattaforma di indagine, contribuendo a individuare la causa profonda delle minacce malware rilevate e fornendo intelligenza azionabile per impedire che le stesse si ripresentino. Ad esempio, gli amministratori possono visualizzare agevolmente quali applicazioni sono in funzione su un client, il che a sua volta può contribuire a individuare le macchine che possano eseguire software vulnerabile o non autorizzato.

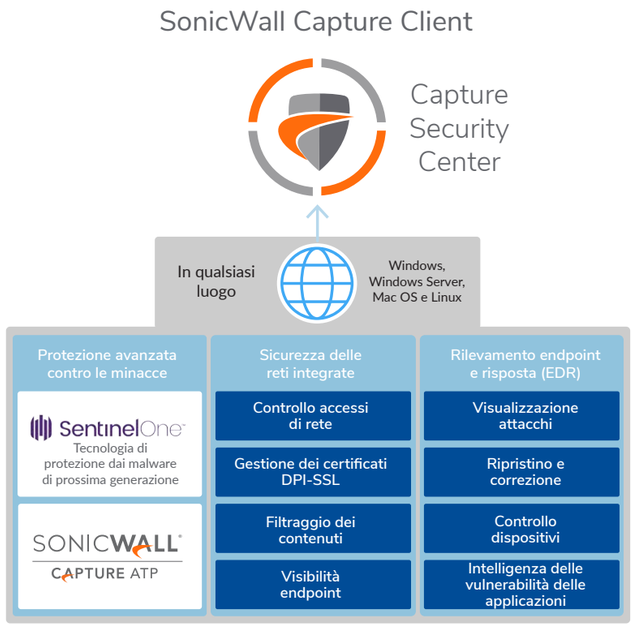
## Offerte e supporto piattaforme

SonicWall Capture Client è disponibile in due versioni:

**SonicWall Capture Client Basic** contiene tutte le funzioni di protezione e rimedio contro i malware di prossima generazione tipiche di SonicWall, con possibilità di supporto DPI-SSL.

**SonicWall Capture Client Advanced** contiene tutte le funzioni della versione Basic sopra riportate, più funzionalità di ripristino avanzate, integrazione Capture ATP, visualizzazione degli attacchi, intelligenza delle vulnerabilità delle applicazioni e filtraggio dei contenuti.

Entrambe le offerte sono disponibili per Windows 7 (e versioni successive) e per Mac OSX.



## CONFRONTO DELLE FUNZIONI

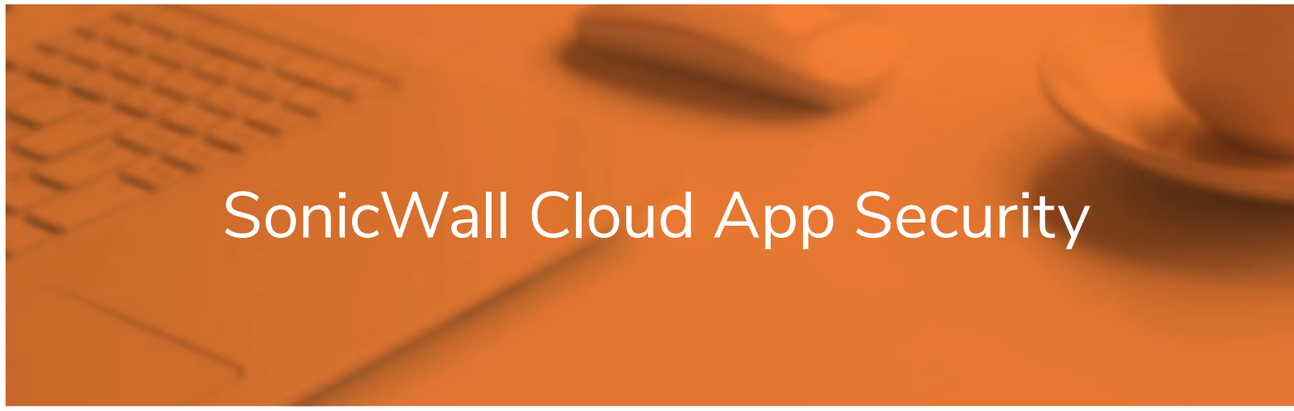
| Funzione | Basic | Advanced |
|---|---|---|
| Gestione cloud, reportistica e analisi (CSC) | ✓ | ✓ |
| **Sicurezza delle reti integrate** | | |
| Visibilità endpoint | ✓ | ✓ |
| Installazione certificati DPI-SSL | ✓ | ✓ |
| Filtraggio dei contenuti | – | ✓ |
| **Protezione avanzata contro le minacce** | | |
| **Antimalware di prossima generazione** | ✓ | ✓ |
| Capture Advanced Threat Protection Sandboxing | – | ✓ |
| **Rilevamento endpoint e risposta** | | |
| Visualizzazione attacchi | – | ✓ |
| Ripristino e correzione | – | ✓ |
| Controllo dispositivi | – | ✓ |
| Intelligenza delle vulnerabilità delle applicazioni | – | ✓ |

## REQUISITI DI SISTEMA

| Sistemi operativi |
|---|
| Windows 7 e versioni successive |
| Windows Server 2008 R2 e versioni successive |
| Mac OS/OSX 10.10 e versioni successive |
| **Hardware** |
| 1 GHz Dual-core CPU o migliore |
| 1 GB RAM o maggiore se richiesta dal sistema operativo (consigliati 2 GB) |
| 2 GB di spazio libero su disco |

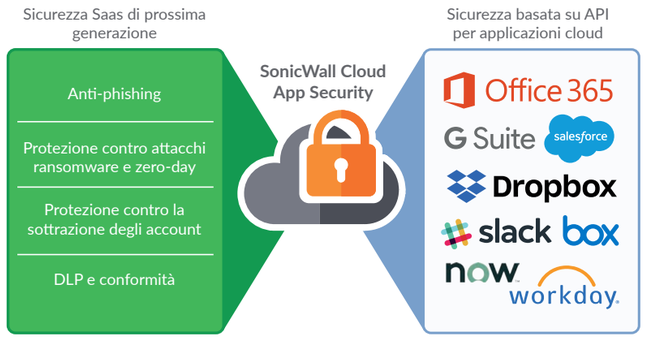
SONICWALL®

SONICWALL®



# SonicWall Cloud App Security

SonicWall Cloud App Security offre la sicurezza di prossima generazione delle applicazioni SaaS come Office 365 e G Suite, proteggendo email, dati e credenziali utente dalle minacce avanzate e garantendo al tempo stesso la conformità nel cloud. Se si sta passando al cloud, SonicWall offre la migliore sicurezza in assoluto basata su API con un basso TCO, minimi costi d'installazione e un'esperienza utente senza soluzioni di continuità.




**Visibilità:** Identificazione di tutti i servizi cloud (sanzionati e non) utilizzati dai dipendenti dell'organizzazione, compresa la visibilità del traffico est-ovest (da cloud a cloud), dal momento che gli utenti possono autenticarsi su applicazioni non sanzionate utilizzando software sanzionati, come Office 365.

**Sicurezza della posta elettronica di prossima generazione:** Dal momento che la posta elettronica sta diventando l'applicazione SaaS più diffusa, proteggere questo importante vettore è fondamentale per la sicurezza SaaS. La soluzione prevede il trasferimento degli allegati nella sandbox, la protezione avanzata degli URL e la protezione BEC (Business Email Compromise).

**Protezione avanzata contro le minacce:** Prevenzione della propagazione dei malware tramite app come OneDrive, Box e Dropbox con scansione in tempo reale delle minacce conosciute e sandboxing Capture ATP per le minacce zero-day e sconosciute.

**Sicurezza dei dati:** Attuazione di politiche di sicurezza data-centriche, che consentono controlli d'accesso granulari, impedendo il caricamento di file sensibili o riservati. La soluzione comprende strumenti politici basati sui ruoli, classificazione dei dati e tecnologie per la prevenzione delle perdite di dati per il monitoraggio dell'attività degli utenti e il blocco o la limitazione degli accessi.

**Conformità:** La soluzione raccoglie un audit trail completo per ogni azione, compresi gli eventi in tempo reale e quelli storici e mette a disposizione semplici modelli DLP per l'effettuazione dei controlli delle politiche e la conformità normativa in tempo reale.

## Vantaggi:

### Sicurezza della posta elettronica di prossima generazione

- Blocco dei ransomware, degli attacchi zero-day e delle email di phishing mirato prima che raggiungano la casella di posta in arrivo dell'utente
- Il trasferimento degli allegati nella sandbox e la protezione avanzata degli URL assicurano una protezione avanzata contro le minacce
- Scansione del traffico email in ingresso, in uscita e interno in Office 365 e G Suite
- Blocco degli attacchi di impersonazione tramite apprendimento automatico e intelligenza artificiale (AI)
- Richiamo di email nocive dalle caselle della posta in arrivo degli utenti dopo l'invio

### Sicurezza SaaS di prossima generazione (CASB)

- Visibilità e controllo a livello granulare sulle applicazioni informatiche sanzionate e nascoste
- Copertura completa sul traffico user-to-cloud e cloud-to-cloud
- Prevenzione dell'upload di dati sensibili e della condivisione non autorizzati dei file
- Definizione di politiche coerenti in materia di sicurezza dei dati sulle applicazioni sanzionate
- Protezione contro la sottrazione degli account (ATO), minacce interne, credenziali compromesse
- Blocco della propagazione di ransomware e malware zero-day nel cloud
- Attuazione di politiche normative sulla conformità tramite semplici modelli DLP
- Identificazione delle violazioni e delle lacune di sicurezza tramite l'analisi degli eventi storici e in tempo reale

### La sicurezza diventa semplice e accessibile

- Esperienza utente completa con accesso da qualsiasi dispositivo e da qualunque postazione
- Eliminazione di punti deboli, problematiche di latenza e necessità di riorientare il traffico tramite proxy
- Automazione dell'individuazione delle applicazioni nel cloud in abbinamento a SonicWall NGFW
- Riduzione del costo totale di proprietà (TCO) grazie alla rapidità d'installazione e alla facilità d'uso

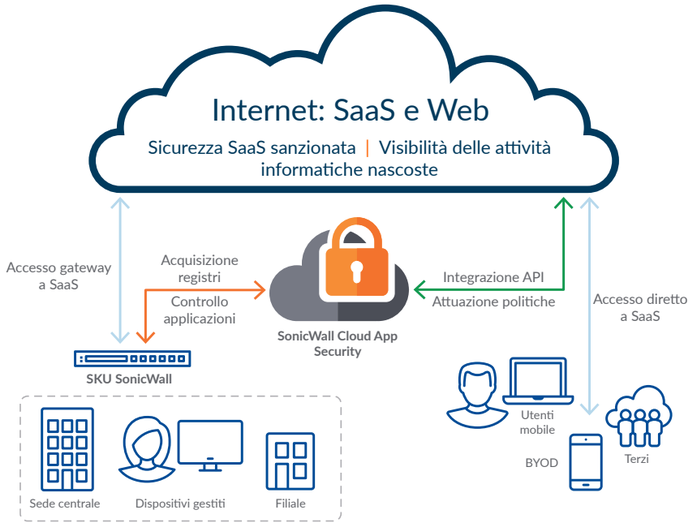
## Panoramica della soluzione

### Descrizione della soluzione SonicWall

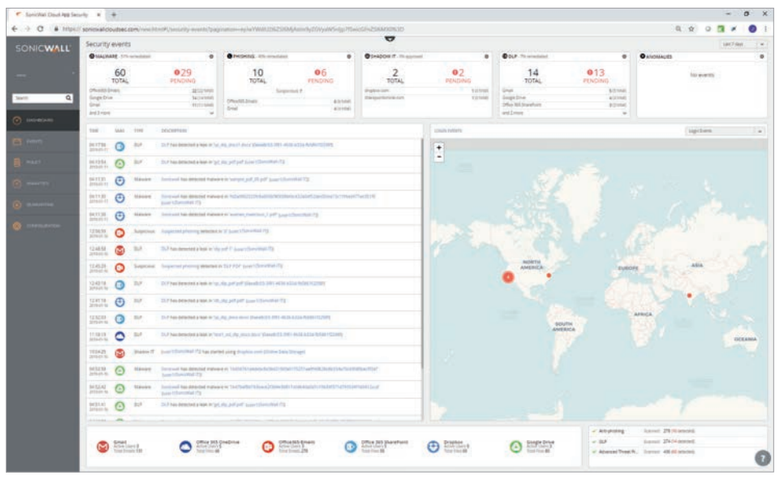
La soluzione SonicWall Cloud App Security consente la scansione fuori banda del traffico alle applicazioni SaaS sanzionate e non tramite API e analisi dei registri del traffico.

La soluzione si integra perfettamente con le applicazioni SaaS sanzionate utilizzando API native, mettendo a disposizione funzionalità CASB: visibilità, protezione avanzata delle minacce, prevenzione di perdite di dati (DLP) e conformità. Utilizzata in abbinamento a un firewall di prossima generazione (NGFW) SonicWall, Cloud App Security consente la visibilità e il controllo della visibilità delle attività informatiche nascoste per l'uso del cloud in rete.

La soluzione consente ai responsabili informatici di installare le applicazioni SaaS senza compromettere la sicurezza e la conformità. Gli amministratori possono definire da un'unica console le politiche coerenti per tutte le applicazioni SaaS installate a livello dell'organizzazione. È possibile utilizzare i modelli di report DLP e di conformità predefiniti per chiudere rapidamente le falle di sicurezza e definire politiche personalizzate per soddisfare le esigenze aziendali e normative. Sia che si debbano gestire pochi utenti o centinaia di migliaia di dipendenti in ogni parte del mondo, la soluzione può essere modulata in funzione delle proprie esigenze, senza bisogno d'installare e gestire alcun hardware.



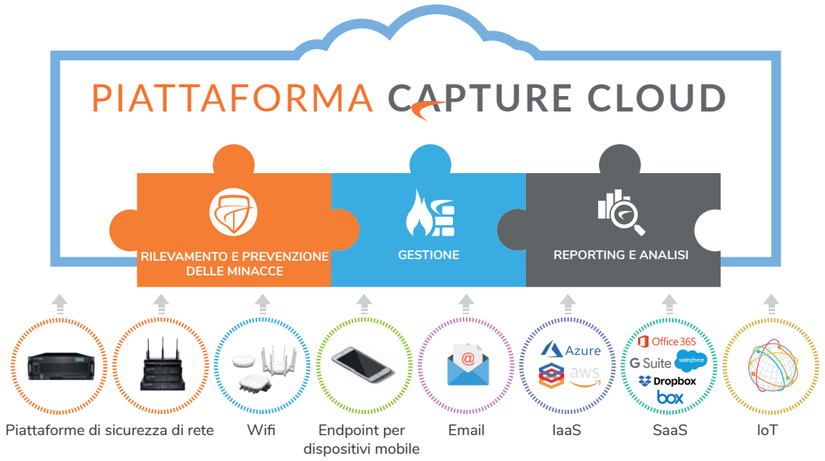

*Sicurezza SaaS basata su API con funzioni CASB*



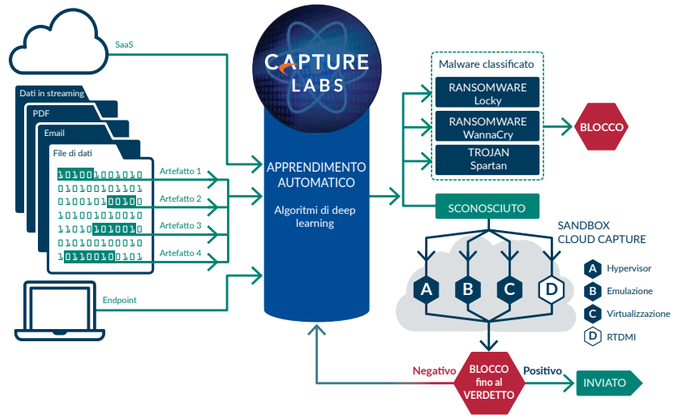
Il pannello di controllo in tempo reale consente agli amministratori di monitorare l'uso delle applicazioni a rischio, tracciare l'attività degli utenti, il volume delle transazioni e la sede in cui le applicazioni vengono utilizzate. La soluzione garantisce l'adozione sicura delle applicazioni SaaS senza ricadute sulla produttività del personale.

### Integrazione con la piattaforma Capture Cloud di SonicWall

SonicWall Cloud App Security è un servizio cloud nativo strutturato mediante la piattaforma di cattura cloud e reso disponibile mediante Capture Security Center. 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. Capture Security Center consente la gestione da un'unica finestra e gli amministratori hanno la possibilità di creare con facilità report in tempo reale e storici sull'attività di rete e cloud.




Per proteggere le applicazioni SaaS, SonicWall Cloud App Security utilizza la piattaforma Capture Cloud, che abbina l'intelligence globale della sicurezza della Capture Threat Network con la prevenzione avanzata delle minacce della sandbox multi-engine Capture ATP. Questo approccio permette a SonicWall di ampliare le funzioni di prevenzione delle violazioni automatizzate in tempo reale negli ambienti SaaS, consentendo alle organizzazioni di passare al cloud. Le API native si integrano direttamente con i servizi cloud, consentendo alla soluzione di effettuare la scansione dei file in applicazioni come OneDrive o Dropbox tramite il servizio Capture ATP con Real-Time Deep Memory Inspection™ (RTDMI™), impedendo l'accesso in rete a ransomware e zero-day.





SONICWALL®

## Sicurezza completa per Office 365 e G Suite

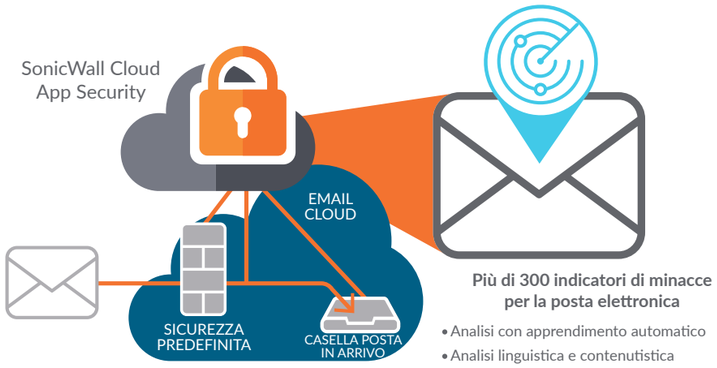
### Sicurezza di prossima generazione per la posta elettronica nel cloud

SonicWall Cloud App Security comprende la funzione di sicurezza della posta elettronica di prossima generazione progettata per le piattaforme di posta elettronica in cloud. Normalmente, quando le organizzazioni spostano la posta elettronica nel cloud, fanno esclusivamente affidamento sulla sicurezza offerta dal fornitore del servizio o la integrano con un proxy MTA tradizionale. I gateway di posta elettronica esterni, tuttavia, potrebbero non essere sufficienti per rilevare e bloccare le minacce di oggi.

Oltre ai tradizionali livelli di sicurezza della posta elettronica dei controlli SPF, DKIM e DMARC, ed al filtraggio degli URL tramite le principali fonti di dati per le blacklist degli URL, l'esclusiva architettura di Cloud App Security offre una protezione che le soluzioni con gateway esterni non sono in grado di dare, ovvero:

- Aggiunge un livello di protezione contro le minacce avanzate: Cloud App Security blocca i messaggi di phishing che Office 365 e G Suite non sono riusciti ad intercettare. La soluzione utilizza l'apprendimento automatico, l'intelligenza artificiale e l'analisi dei big data per offrire potenti funzioni anti-phishing, sandboxing degli allegati, protezione avanzata degli URL e protezione contro l'impersonazione.
- Monitora le email in arrivo, in uscita e interne: l'integrazione del SaaS in Cloud App Security consente di scansionare e mettere in quarantena tutte le email prima che arrivino nella casella di posta in arrivo dell'utente, sia che provengano dall'esterno dell'organizzazione, sia da un account interno compromesso.
- Scansiona i messaggi storici per individuare eventuali minacce: alla prima connessione Cloud App Security scansiona i messaggi storici (anche quelli degli account chiusi) per individuare potenziali violazioni o account compromessi.
- Richiamo messaggi a livello globale: i messaggi dannosi possono essere modificati o richiamati in qualsiasi momento indipendentemente dal fatto che siano dannosi, contengano informazioni riservate o siano stati trasmessi perché accidentalmente un dipendente ha selezionato "rispondi a tutti".

Poiché la protezione della posta elettronica di Cloud App Security viene applicata a monte della casella di posta in arrivo ma a valle dei filtri inattivi Microsoft o Google (come pure degli eventuali gateway MTA installati), i suoi algoritmi di apprendimento automatico sono tarati espressamente per individuare le minacce che non sono state ancora intercettate. Inoltre, Cloud App Security è in grado di integrare i risultati delle scansioni native nei suoi algoritmi di rilevamento.




- Integrazione totale con Office 365 o G Suite
- Controllo totale delle caselle di posta elettronica: in arrivo, in uscita, interne

**Più di 300 indicatori di minacce per la posta elettronica**

- Analisi con apprendimento automatico
- Analisi linguistica e contenutistica
- Servizio sandboxing Capture ATP
- Protezione avanzata degli URL

*La protezione virtuale in linea blocca i messaggi dannosi prima che raggiungano la casella di posta in arrivo degli utenti*

SONICWALL®

## Caratteristiche

| FUNZIONALITÀ | | VANTAGGIO |
|---|---|---|
| **Visibilità** | Cloud Application Discovery | Individua automaticamente le applicazioni nel cloud utilizzando i file di registro dei firewall SonicWall per individuare le attività nascoste in rete |
| | Visibilità dell'uso del cloud | Visualizzazione grafica in tempo reale delle applicazioni in uso, del volume di traffico, dell'attività degli utenti e delle sedi |
| | Valutazione dei rischi delle applicazioni | Assunzione di decisioni informate di blocco/sblocco delle applicazioni sulla base della valutazione del rischio |
| | Monitoraggio eventi | Monitoraggio delle singole azioni, compresi gli eventi in tempo reale e quelli storici, effettuato nell'ambiente SaaS aziendale |
| **Sicurezza della posta elettronica di prossima generazione** | Anti-phishing | Blocco degli attacchi di phishing progettati per aggirare la sicurezza predefinita di Office 365 o G Suite |
| | Anti-spoofing | Protezione del marchio aziendale e degli utenti dalle frodi mediante posta elettronica e dagli attacchi di impersonazione |
| | Sandboxing degli allegati | Blocca gli allegati nocivi ai messaggi di posta elettronica per impedire che arrivino nella casella di posta in arrivo degli utenti |
| | Protezione avanzata degli URL | Garantisce la protezione degli utenti dagli URL nocivi integrati |
| **Protezione avanzata contro le minacce** | Protezione contro i malware zero-day | Impedisce la memorizzazione e la propagazione dei malware tramite applicazioni come Box, Dropbox, OneDrive e G Drive |
| | Protezione contro la sottrazione degli account | Protegge le credenziali SaaS individuando il comportamento anomalo degli utenti, le violazioni dei permessi e la variazione delle configurazioni |
| **Sicurezza dei dati** | Classificazione dei dati | Identifica i dati sensibili o riservati ed applica le politiche a livello di SaaS per controllare come possono essere condivise le informazioni |
| | Controllo accessi incentrato sui dati | Gestisce i permessi dei file sulla base del tipo di dati che contengono |
| | Individuazione delle anomalie tramite flussi di lavoro | Garantisce che la messa in sicurezza dei dati non abbia ricadute sull'attività mediante esecuzione in tempo reale |
| **Conformità** | Modelli di conformità | Riduce il carico di lavoro amministrativo utilizzando semplici modelli di conformità per soddisfare i requisiti per SOX, PCI, HIPAA e GDPR |
| | Audit trail | Accede ai dati degli eventi storici per le verifiche di conformità retrospettiva e reportistica in tempo reale |
| | Attuazione delle politiche | Attua la conformità in tempo reale con ogni SaaS per controllare i permessi di accesso, spostare file, bloccare e modificare messaggi di posta elettronica e comunicare con utenti ed amministratori |

SONICWALL®

SONICWALL®

# SONICWALL SECURE MOBILE ACCESS (SMA)

Accesso sicuro dovunque e in qualsiasi momento a risorse aziendali in ambienti multi-cloud basato sull'identità, l'ubicazione e l'affidabilità di utenti e dispositivi.

SonicWall SMA costituisce un gateway di accesso sicuro unificato che consente alle organizzazioni di accedere - in qualsiasi luogo e in qualsiasi momento e su qualsiasi dispositivo - a risorse aziendali mission critical. L'engine delle politiche di controllo granulare degli accessi di SMA, l'autorizzazione dei dispositivi in base al contesto, la VPN a livello di applicazione e l'autenticazione avanzata con Single Sign-On consentono alle aziende di adottare il BYOD e la mobilità in un ambiente multi-cloud.

**Mobilità e BYOD**
Per le organizzazioni che desiderano adottare il BYOD, lavorare in modo flessibile o consentire l'accesso a terzi, SMA diventa il punto di attuazione centrale per tutti questi aspetti. SMA offre la migliore sicurezza nel settore per ridurre al minimo le minacce in superficie, rendendo più sicure le organizzazioni grazie al supporto dei più recenti algoritmi di crittografia e cifrari. SMA di SonicWall consente agli amministratori di fornire un accesso mobile sicuro e privilegi basati sulle identità in modo che gli utenti finali ottengano un accesso semplice e veloce alle applicazioni, ai dati e alle risorse aziendali di cui hanno bisogno. Allo stesso tempo, le aziende possono definire criteri di BYOD sicuro per proteggere le proprie reti e i dati aziendali da accessi non autorizzati e dal malware.

**Il passaggio al cloud**
Per le aziende che si apprestano a compiere la migrazione verso il cloud, SMA offre un'infrastruttura Single Sign-On (SSO) che utilizza un singolo portale web per autenticare gli utenti in un ambiente informatico ibrido. L'esperienza di accesso è coerente e trasparente, indipendentemente dal fatto che la risorsa aziendale si trovi in sede, nel web o in un cloud in hosting. SMA inoltre si integra con le principali tecnologie di autenticazione multifattoriale attualmente disponibili in campo industriale per garantire una maggiore sicurezza.

**Fornitori di servizi gestiti**
SMA propone una soluzione chiavi in mano per offrire un elevato grado di continuità e modularità aziendale sia alle organizzazioni con proprie infrastrutture, sia ai provider di servizi gestiti. SMA è in grado di supportare fino a 20.000 connessioni simultanee su una singola apparecchiatura, con una modularità verticale fino a centinaia di migliaia di utenti tramite un clustering intelligente. I data center possono ridurre i costi con il clustering attivo/attivo e con un bilanciatore di carico dinamico integrato, che consente di riallocare il traffico globale verso il data center più ottimizzato in tempo reale e in base alle esigenze dell'utente. Gli strumenti SMA mettono le aziende specializzate in condizione di fornire servizi con tempi di indisponibilità zero, consentendo loro di soddisfare i requisiti più esigenti dei Service Level Agreement (SLA).

SMA fornisce ai reparti informatici la migliore esperienza e l'accesso più sicuro possibile a seconda dello scenario d'uso. Disponibile come apparecchiatura fisica hardened o potente apparecchiatura virtuale, SMA si inserisce senza soluzione di continuità nelle infrastrutture interne e/o nel cloud esistenti. Le organizzazioni possono scegliere tra una gamma di soluzioni per l'accesso sicuro basato sul web completamente clientless per terzi o dipendenti tramite dispositivi personali, oppure un più tradizionale accesso completo a tunnel VPN basato su client per i dirigenti da qualsiasi tipo di dispositivo. SonicWall SMA ha una soluzione sia per le organizzazioni che devono fornire un accesso sicuro e affidabile a cinque utenti da un'unica postazione, sia per le imprese che necessitano di modularità fino a migliaia di utenti in reti distribuite globalmente.

SonicWall SMA consente alle organizzazioni di adottare mobilità e BYOD senza timori, e di passare più facilmente al cloud. SMA consente più autonomia ai lavoratori, mettendo a loro disposizione modalità di accesso valide per tutti.

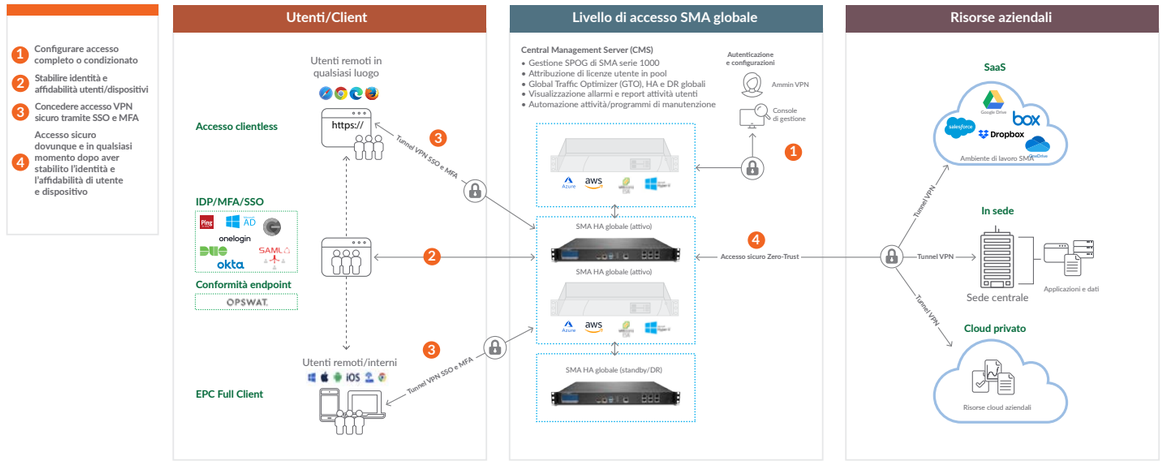
**Vantaggi:**

- Accesso sicuro unificato a tutte le risorse di rete e nel cloud "in qualsiasi momento, per qualsiasi dispositivo e per qualsiasi applicazione"
- Controllare chi accede a quali risorse definendo politiche granulari tramite il robusto engine di controllo degli accessi
- Aumentare la produttività consentendo il Single Sign-On federato a qualsiasi applicazione SaaS o locale con un singolo URL
- Ridurre il costo totale della proprietà e la complessità della gestione degli accessi consolidando le componenti delle infrastrutture in un ambiente informatico ibrido
- Sapere quali dispositivi cercano di collegarsi e concedere l'accesso sulla base delle politiche e dello stato di salute degli endpoint
- Impedire le violazioni da parte del malware scansionando tutti i file caricati in rete tramite la sandbox Capture ATP
- Proteggersi contro gli attacchi basati sul web e garantire la conformità PCI con l'add-on Web Application Firewall
- Bloccare gli attacchi DDoS e zombie tramite il rilevamento Geo IP e la protezione Botnet
- Disporre della funzionalità sicura con agente nativo tramite accesso clientless HTML5 basato su web browser senza l'impegno di dover installare e mantenere agenti sui dispositivi endpoint
- Ottenere informazioni approfondite fruibili per prendere le decisioni giuste con il monitoraggio in tempo reale e la reportistica completa
- Installare sotto forma di apparecchiature fisiche o virtuali in cloud privati su ESXi o Hyper-V, o in ambienti cloud pubblici AWS o Microsoft Azure
- Abilitare l'emissione dinamica delle licenze di accesso basate sulla domanda in tempo reale, con indirizzamento automatico dell'endpoint alla connessione più performante e dalla latenza più bassa
- Riduzione dei costi iniziali grazie al bilanciamento del carico integrato senza hardware o servizi aggiuntivi, senza alcun impatto per l'utente sul failover dell'apparecchiatura
- Assicurazione contro le interruzioni di servizio o i picchi stagionali grazie all'immediata modularità della capacità

## Installazione SMA

**Un gateway dalla sicurezza potenziata per l'accesso sicuro, sempre e ovunque, da qualsiasi dispositivo**

I gateway SMA mettono a disposizione un accesso remoto sicuro end-to-end completo alle risorse aziendali che si trovano in sede, nel cloud e in datacenter ibridi. Si tratta di apparecchiature che utilizzano controlli di accesso basati sulle politiche e sull'identità, autenticazione contestuale dei dispositivi e VPN a livello di applicazioni per consentire l'accesso a dati, risorse e applicazioni dopo aver stabilito l'identità e l'affidabilità dell'utente, dell'ubicazione e del dispositivo. Vengono installate in modo flessibile sotto forma di apparecchiature Linux hardened o di apparecchiature virtuali in cloud privati su ESXi o Hyper-V, o in ambienti cloud pubblici AWS o Microsoft Azure.




*Installazione SMA nel cloud / in sede*

**Installazione flessibile con apparecchiature fisiche e virtuali**

SonicWall SMA può essere installato come apparecchiatura hardened ad alte prestazioni o come apparecchiatura virtuale, sfruttando le risorse di calcolo condivise per ottimizzare l'utilizzo, facilitare la migrazione e ridurre i costi di investimento. I dispositivi hardware sono basati su un'architettura multi-core ad elevate prestazioni che offre accelerazione SSL, throughput VPN e potenti proxy per garantire un accesso sicuro e affidabile. Per le organizzazioni regolamentate e per quelle federali, SMA è disponibile anche con certificazione FIPS 140-2 Level 2. Le apparecchiature virtuali SMA offrono le stesse caratteristiche avanzate di accesso sicuro delle principali piattaforme virtuali o del cloud, come Microsoft Hyper-V, VMware ESX e AWS.

**Licenze d'uso utilizzabili da diverse apparecchiature**

Le organizzazioni che dispongono di apparecchiature distribuite su scala globale possono beneficiare dell'oscillazione della domanda di licenze d'uso legata ai fusi orari. Indipendentemente dal fatto che un'organizzazione utilizzi licenze VPN complete o licenze ActiveSync di base, la gestione centralizzata di SMA riassegna le licenze alle apparecchiature gestite nelle aree geografiche in cui si sono avuti picchi di domanda dalle applicazioni di altre zone geografiche, nelle quali l'uso è diminuito per via dell'assenza dal lavoro degli utenti nelle ore notturne.

**Visibilità di rete con profilatura dei dispositivi sulla base delle situazioni contingenti**

Il sistema di autenticazione di fascia alta, che tiene conto delle situazioni contingenti, consente l'accesso solo ai dispositivi affidabili e agli utenti autorizzati. Anche i portatili e i PC vengono analizzati per rilevare la presenza o l'assenza di software di sicurezza, certificati client e ID dei dispositivi. Prima di consentire l'accesso i dispositivi mobili vengono analizzati per verificare le informazioni di sicurezza essenziali come jailbreak o stato della root, ID del dispositivo, stato dei certificati e versione del sistema operativo. Ai dispositivi che non soddisfano i requisiti della politica non viene concesso l'accesso alla rete e l'utente viene avvisato della mancata conformità.

**Esperienza coerente da un unico portale web**

Gli utenti non devono ricordarsi tutti gli URL delle singole applicazioni o conservare segnalibri dettagliati. SMA dispone di un portale di accesso centralizzato che fornisce agli utenti un URL per accedere a tutte le applicazioni fondamentali da un browser web standard. Quando l'utente ha effettuato l'accesso da un browser, nella finestra del browser viene visualizzato un portale web personalizzabile destinato agli utenti, con un unico punto di controllo per accedere a qualsiasi applicazione SaaS o locale. Il portale visualizza solamente i collegamenti e i segnalibri personalizzati relativi a un gruppo, a un utente o a un dispositivo endpoint specifico. Il portale è una piattaforma agnostica e supporta tutte le principali piattaforme, compresi i dispositivi Windows, Mac OS, Linux, iOS e Android, oltre a supportare numerosi browser per tutti questi dispositivi.

**Single Sign-On federato alle applicazioni SaaS e a quelle locali**

Eliminare l'esigenza di password multiple e porre fine alle cattive prassi di sicurezza come il riutilizzo delle password. SMA consente un SSO federato alle applicazioni SaaS ospitate nel cloud e a quelle fuori sede. SMA si integra con diversi server di autenticazione, autorizzazione e contabilità e tecnologie leader nel campo dell'autenticazione multifattoriale per una maggiore sicurezza. Il Single Sign-On sicuro viene fornito solo ai dispositivi endpoint autorizzati dopo che SMA verifica l'integrità

SONICWALL®

e la conformità degli endpoint. L'engine della politica di accesso garantisce che gli utenti possano visualizzare solo le applicazioni autorizzate e concedere l'accesso previa autenticazione andata a buon fine. La soluzione supporta un SSO federato anche quando si utilizzano client VPN, mettendo a disposizione dei clienti un'esperienza di autenticazione senza soluzione di continuità sia che utilizzino un accesso sicuro basato su client o clientless.

### Prevenire le violazioni e le minacce avanzate

SonicWall SMA aggiunge un livello di sicurezza d'accesso per migliorare la sicurezza e ridurre la superficie di accesso per le minacce.

- SMA si integra con la sandbox multi-engine basata su cloud SonicWall Capture ATP per effettuare la scansione di tutti i file caricati dagli utenti con endpoint non gestiti o da quelli fuori dalla rete aziendale. Ciò garantisce che gli utenti abbiano lo stesso livello di protezione dalle minacce avanzate, come ransomware o il malware zero-day, quando sono in viaggio come se fossero in ufficio[1].
- Il servizio SonicWall Web Application Firewall mette a disposizione delle aziende una soluzione affidabile e integrata per rendere sicure le applicazioni interne basate sul web. Ciò consente ai clienti di garantire la riservatezza dei dati e che i servizi web interni non vengano compromessi in presenza di accessi da parte di utenti malintenzionati o fraudolenti.
- Il rilevamento di Geo-IP e Botnet protegge le organizzazioni dagli attacchi DDoS e zombie e dagli endpoint compromessi che funzionano come botnet.

### Accesso clientless sicuro basato sul browser senza soluzione di continuità

La natura "clientless" di SonicWall SMA significa che gli amministratori non devono installare manualmente componenti fat client sui computer da utilizzare per l'accesso remoto. In questo modo si elimina qualsiasi dipendenza da Java e l'impegno per il reparto informatico, aumentando di conseguenza in modo notevole la possibilità di accesso remoto. Ciò significa che, in assenza di requisiti di pre-installazione o di pre-configurazione, i telelavoratori autorizzati possono operare da qualsiasi computer, in qualsiasi parte del mondo, ed accedere in modo sicuro alle risorse aziendali. Nella sua forma più pura, l'accesso sicuro è basato rigorosamente sul browser tramite HTML5, il che offre agli utenti un'esperienza senza soluzione di continuità e unificata.

### Offrire un'esperienza "Always On"

Per consentire agli utenti un'esperienza senza soluzione di continuità, SMA mette a disposizione una Always On VPN per i dispositivi Windows gestiti. Gli amministratori possono configurare le impostazioni in modo che venga stabilita automaticamente una connessione VPN ogniqualvolta un client endpoint autorizzato rileva la presenza di una rete pubblica o non affidabile. Ogni accesso al dispositivo Windows mette a disposizione dell'utente una connessione sicura con le risorse aziendali. Gli utenti non devono effettuare l'accesso sui loro client VPN né gestire ulteriori password. Ciò consente un'esperienza senza soluzione di continuità per gli utenti mobili per accedere alle risorse critiche esattamente come se si trovassero in ufficio e consente agli amministratori dei sistemi informatici di mantenere il controllo sui dispositivi gestiti, migliorando la sicurezza dell'organizzazione.

### Gestione intuitiva e reportistica completa

SonicWall offre una piattaforma di gestione intuitiva basata sul web, Central Management Server (CMS), per semplificare la gestione delle apparecchiature e fornire ampie funzionalità di reportistica. L'interfaccia utente grafica di facile uso agevola la gestione di apparecchiature e politiche singole o multiple. Ogni pagina mostra come sono configurati i parametri di tutte le macchine in gestione. La gestione unificata delle politiche consente di creare e monitorare le politiche e le configurazioni di accesso. Un'unica politica può controllare l'accesso da parte di utenti, dispositivi e applicazioni, a dati, server e reti. I responsabili informatici possono automatizzare le attività di routine e quelle pianificate, liberando i team addetti alla sicurezza dai compiti ripetitivi affinché si concentrino su attività di sicurezza strategiche, come la risposta agli eventi imprevisti. Essi, inoltre, acquisiscono utili indicazioni sulle tendenze d'accesso degli utenti e sullo stato di salute dell'intero sistema attraverso una reportistica di facile uso e la funzione di log centralizzata.

### Consentire la disponibilità dei servizi 24x7

Le organizzazioni hanno l'esigenza di mantenere i servizi forniti attivi e funzionanti con un elevato grado di affidabilità per consentire l'accesso sicuro alle applicazioni critiche in qualsiasi momento. Le apparecchiature SMA supportano la modalità tradizionale attivo/passivo ad alta disponibilità (HA) per organizzazioni che dispongono di un unico data center, o la modalità attivo/attivo HA globale o il clustering attivo/standby per i data center locali o distribuiti. Entrambi i modelli HA consentono agli utenti un'esperienza uniforme con failover a impatto zero e persistenza di sessione.

### Implementazione del client VPN in base alle vostre esigenze

È possibile scegliere tra un'ampia gamma di client VPN per fornire un accesso remoto sicuro e vincolante a vari endpoint, compresi portatili, smartphone e tablet.

| Client VPN | SO supportato | Modello SMA supportato | Caratteristica principale |
|---|---|---|---|
| **Mobile Connect** | iOS, OS X, Android, Chrome OS, Windows 10 | Tutti i modelli | Fornisce l'autenticazione biometrica, tramite VPN app e implementazione del controllo degli endpoint |
| **Connect Tunnel (Thin Client)** | Windows, Mac OS e Linux | 6200, 6210, 7200, 7210, 8200v, 9000 | Fornisce un'esperienza completa "come in ufficio" con un solido controllo degli endpoint |
| **NetExtender (Thin Client)** | Windows e Linux | 210, 410, 500v | Implementa politiche di accesso granulari ed estende l'accesso alla rete tramite client nativi |

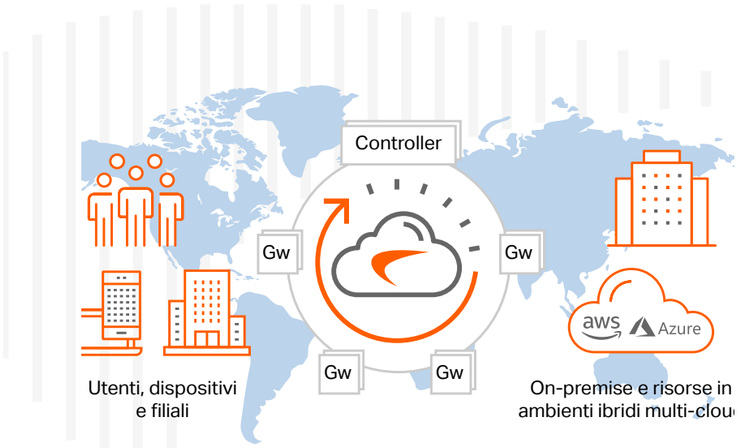
SONICWALL®

# Cloud Edge Secure Access

Fornisce l'accesso alla rete zero-trust su scala globale in pochi minuti

SonicWall Cloud Edge Secure Access offre un semplice servizio NaaS (Network-as-a-Service) per la connettività site-to-site e in cloud ibrido per AWS, Azure, Google Cloud e molti altri. Grazie alle tecnologie di sicurezza Zero-Trust e Least-Privilege e alla microsegmentazione software-defined, gli utenti e i dispositivi possono accedere unicamente alle risorse necessarie.

Le aziende possono così offrire la flessibilità del telelavoro, mantenere la flessibilità operativa e, allo stesso tempo, proteggere le risorse ad alto valore aggiunto dalle




**Le funzioni in breve.** Riepilogo completo delle funzioni »

| 10-1.000+ | 5-15 min. | 30+ PoP |
|---|---|---|
| Possibili utenti | Tempo d'installazione | In Europa, USA, Medio Oriente e Asia |

## CARATTERISTICHE PRINCIPALI

- Accesso Zero-Trust con policy di microsegmentazione software-defined per prevenire la diffusione di violazioni.
- Autenticazione Single Sign-On e a più fattori mediante i servizi LDAP, Okta, Google e Azure Identity Provider.
- Network Traffic Control (NTC) consente la protezione a livello di firewall definendo chi (e da dove) può accedere a reti e servizi specifici.
- Device Posture Check (DPC) concede l'accesso alla rete solo ai dispositivi autenticati e conformi.
- App client disponibili per i sistemi operativi macOS, Win10, Android e iOS.
- Accesso Remote Desktop senza client tramite RDP, VNC, SSH e HTTP/HTTPS per l'accesso via web con qualsiasi dispositivo pubblico.
- Migliore esperienza d'uso con i moderni e veloci tunnel WireGuard.
- La VPN sempre attiva emula un'esperienza come in ufficio e mantiene un livello di sicurezza elevato negli hotspot pubblici.
- Semplice interfaccia di configurazione delle policy con drag-and-drop per risparmiare tempo e pannello di controllo per semplificare i controlli di conformità.
- Il monitoraggio della rete offre una panoramica completa del modello di traffico e del livello di sicurezza di utenti, gruppi e server.

**L'accesso in modalità Zero Trust limita l'esposizione alle aree sensibili della rete e salvaguardia le risorse aziendali**

www.sonicwall.com/cloud-edge

SONICWALL®

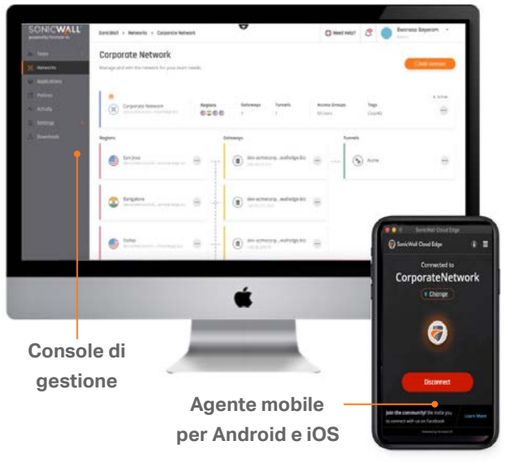
Le soluzioni VPN tradizionali non sono state create per il cloud e presentano alcuni problemi essenziali: la fiducia implicita, che consente alle minacce di muoversi lateralmente all'interno della rete, i tempi d'installazione relativamente lunghi e una maggiore latenza nel cloud a causa del ripetuto reinstradamento del traffico (hair-spinning), che incide sulla qualità dell'esperienza degli utenti.

Gartner prevede che entro il 2023 il 60% delle imprese eliminerà gradualmente la maggior parte delle reti private virtuali (VPN) ad accesso remoto per passare a soluzioni di accesso alla rete zero-trust (ZTNA).

## Infrastruttura progettata per una rapida scalabilità e l'implementazione globale

SonicWall Cloud Edge Secure Access è basato sull'avanzata architettura Software-Defined Perimeter (SDP) nativa del cloud, che consente una rapida implementazione e l'onboarding self-service.

- **Installazione più rapida** – In meno di 15 minuti un responsabile IT può registrarsi, creare un gateway e configurare policy granulari basate sul contesto della rete e degli utenti.
- **Onboarding veloce degli utenti** – Un utente finale può scegliere di connettersi tramite il proprio dispositivo o un'applicazione desktop client, oppure di evitare l'installazione del client se utilizza un computer pubblico, a condizione che sia disponibile un browser. Con il modello d'installazione self-service, l'onboarding può essere completato in 5 minuti.




L'architettura SDP è intrinsecamente sicura perché separa il controller di autenticazione degli utenti e dei dispositivi dai gateway, che fungono da garanti dell'affidabilità. Grazie alla distribuzione dei gateway vicino alle sedi degli utenti finali, Cloud Edge Secure Access può essere rapidamente ampliato per mantenere prestazioni elevate e consentire un'esperienza ottimale nel cloud.

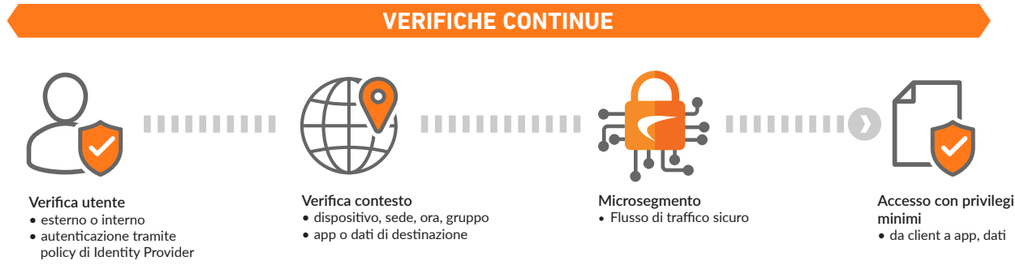
La separazione delle funzioni consente inoltre a Cloud Edge Secure Access di bloccare cyber minacce comuni come attacchi DDos, SYN flood e Slowloris.

## Sicurezza a livello di micro-perimetro definita dal software che segue gli utenti

Oggi i dipendenti desiderano la flessibilità di lavorare da qualsiasi luogo, mentre le aziende vogliono sfruttare le efficienze operative e i risparmi sui costi offerti dal cloud. In questa nuova realtà invertita, dove il lavoro si svolge all'esterno delle postazioni centralizzate e della protezione fisica del firewall, è necessario integrare l'attuale modello di servizi on-premise con un agile modello di sicurezza che "segue" l'utente.

Con SonicWall Cloud Edge Secure Access il perimetro è definito dal software, vale a dire che ogni segmento di micro perimetro racchiude un particolare tipo di flusso di traffico definito dalle policy di accesso. Il segmento inizia dall'utente e si estende a reti, servizi o asset specifici in qualsiasi ambiente cloud, garantendo un approccio molto più versatile.






## Accesso Zero-Trust alla rete

### Non fidarsi di nulla e verificare tutto

Le policy Zero-Trust consentono agli utenti esterni in possesso dei requisiti adeguati di accedere in sicurezza a una serie di risorse di rete con il supporto di:

- **Autenticazione federata SSO e multifattoriale** – Questa combinazione offre agli utenti un unico portale per autenticarsi in un ambiente IT ibrido, creando un'esperienza coerente e senza soluzione di continuità.
- **Integrazione con i principali fornitori di gestione delle identità basati su cloud** – Le aziende possono estendere la durata operativa delle risorse interne esistenti o passare ai moderni servizi di gestione delle identità basati su cloud, forniti da società come Azure AD, Google Authenticator e Okta.
- **Accesso basato sul contesto con Device Posture Check (PDC)** – Autorizza l'accesso alla rete solo ai dispositivi conformi e autorizzati che superano le verifiche di integrità del sistema operativo e di assenza di malware, garantendo che nessun malware possa entrare nell'infrastruttura.
- **Microsegmentazione software-defined** – Network Traffic Control (NTC) segmenta con precisione tutto il traffico in entrata per impedire che malware o utenti non autorizzati compromettano le risorse della rete e i dati sensibili.
- **Controllo degli accessi basato sul minimo privilegio** – Le aziende possono controllare le interazioni degli utenti con le risorse in base ad attributi rilevanti, tra cui l'identità dell'utente e di gruppo e la sensibilità dei dati.

## Lavorare in sicurezza ovunque

### Da postazioni attendibili agli hotspot pubblici

- **Protezione Wi-Fi automatica** – Cloud Edge Secure Access per Windows e Mac OS monitora in modo proattivo l'ambiente e attiva automaticamente una connessione di accesso sicura negli hotspot pubblici. Questo livello di protezione aggiuntivo blocca le intercettazioni Wi-Fi, che sono sempre più comuni e possono comportare furti di dati e violazioni della conformità.
- **Kill switch** – Quando una connessione di accesso protetta viene interrotta, questo strumento sospende immediatamente la connessione Internet del dispositivo per impedire potenziali violazioni e furti di dati.
- **Reti Wi-Fi affidabili** – Quando un SSID viene specificato come "attendibile", la funzione di protezione Wi-Fi automatica non si attiva.
- **VPN/applicazioni sempre attive** – Questa pratica funzione ricollega automaticamente un utente all'applicazione o a una serie di applicazioni senza richiedere di nuovo il login o l'autenticazione.

## Interconnettività site-to-site o Network-as-a-Service (NaaS)

Grazie ai servizi di connettività site-to-site e Network-as-a-Service (NaaS) di Cloud Edge Secure Access, gli amministratori IT possono collegare velocemente filiali dislocate in luoghi geograficamente distanti. Il NaaS permette di connettere in modo rapido e sicuro chioschi mobili, negozi e punti vendita alle risorse nel cloud senza ricorrere a costose soluzioni MPLS.

- **Servizi di interconnessione site-to-site o site-to-cloud** – La soluzione consente di connettersi facilmente agli ambienti cloud più diffusi, come AWS, Azure e Google Cloud, o di creare una connessione di comunicazione sicura tra reti dislocate in sedi diverse.
- **Implementazione multi-regionale** – Gli amministratori possono installare gateway Cloud Edge dedicati in diverse sedi per offrire velocità e prestazioni ottimali alle filiali e ai dipendenti internazionali.

SONICWALL®

- **Backbone globale ad alte prestazioni** – Il servizio SonicWall Cloud Edge è disponibile in tutto il mondo. L'infrastruttura garantisce una latenza minima grazie ai gateway distribuiti vicino alle sedi dei clienti e al bilanciamento del carico tra i server.
- **Tunnel sicuro WireGuard all'avanguardia** – Un responsabile IT può utilizzare qualsiasi router o firewall della filiale con IPsec per collegarsi al gateway Cloud Edge più vicino. SonicWall consiglia il tunnel WireGuard, che offre prestazioni molto più veloci e può essere eseguito su un server Linux della filiale per collegarsi al gateway più vicino.

**Supporto multi-tenancy nativo con portale dedicato ad ogni cliente e servizi di abbonamento a livelli per aiutare gli MSSP ad aumentare la redditività.**

## Riepilogo delle funzionalità

### Scalabilità e prestazioni

- Da decine a migliaia di utenti
- 1 Gb/s per ogni gateway cliente
- Scalabilità orizzontale in cloud con più gateway

### Funzionalità della piattaforma cloud

- Stato del servizio cloud: https://www.sonicwall.com/support
- Gestione cloud inclusa
- Infrastruttura gestita da SonicWall
- Servizi gestiti da MSSP e clienti
- Gateway cloud e indirizzi IP dedicati per ogni cliente
- Bilanciamento del carico su gateway ridondanti incluso
- Scelta della connettività IPsec e WireGuard tra due siti
- Scelta del server DNS interno o predefinito

### Funzionalità di sicurezza Zero-Trust

- Accesso clientless tramite HTTP, HTTPS, RDP, VNC, SSH
- App client disponibile per piattaforme Windows, Mac, iOS e Android
- Verifiche dei dispositivi e del contesto (con DPC, accesso basato sul tempo, monitoraggio continuo di utenti e dispositivi)
- Applicazione di policy di minimo privilegio per l'accesso (con politiche di controllo degli accessi)
- Microsegmentazione software-defined (con NTC)
- Segmentazione basata su policy e applicabile per gruppo, rete, utente, applicazione, servizi, dispositivo
- Controllo e monitoraggio del flusso di traffico di rete in micro-segmenti tra utenti, gruppi e servizi in base a regole personalizzabili
- Policy di controllo granulare degli accessi basate su utente, applicazione, Geo IP, geolocalizzazione (paese), tipo di browser, sistema operativo, data e ora

### Sicurezza negli hotspot pubblici

- Lo split tunneling consente l'interruzione locale del traffico delle subnet
- Kill Switch impedisce una potenziale violazione interrompendo la connessione Internet del dispositivo per prevenire esfiltrazioni di dati
- La protezione Wi-Fi automatica protegge automaticamente i dispositivi dei dipendenti quando si collegano a Wi-Fi pubblici non protetti
- Il filtraggio DNS blocca l'accesso a determinati siti web, categorie di siti e indirizzi IP

### Autenticazione

- Supporto Single Sign-On per fornitori come Okta, G Suite, Azure AD e Active Directory LDAP
- Autenticazione a due fattori integrata tramite SMS o DUO Security e integrazione con Google Authenticator 2FA
- Verifica di sicurezza e conformità dei dispositivi prima dell'accesso alla rete con Device Posture Check

### Interoperabilità tra firewall e router aziendali

- SonicWall, Check Point, Fortinet, Palo Alto Networks, WatchGuard, Sophos, Xyxel, UniFi, pfSense, Cisco e Untangle

### Monitoraggio, registrazione e supporto

- Soluzione cloud completamente gestita con supporto 24x7 incluso
- Controlli di attività e report per monitorare login, installazioni gateway, connessioni di dispositivi e app
- Integrazione SIEM per acquisire, conservare e distribuire informazioni ed eventi di sicurezza in tempo reale a tutte le applicazioni SIEM
- Elenco automatico dei dispositivi che si collegano alla rete e log corrispondenti.
- Integrazione con Splunk per la percentuale di clic

### Conformità

- ISO 27001 e 27002, SOC-2 tipo 2

SONICWALL®

SONICWALL®

## Contattaci SonicWall:


Luis Fisas - Director South Europe - lfisas@sonicwall.com
Cristiana Valentinetti - Channel Account Manager Center-South Italy - cvalentinetti@SonicWall.com
Valerio Branca - Channel Account Manager North Italy - vbranca@SonicWall.com
Fabrizio Corradini - Director, Strategic Account South EMEA - fcorradini@sonicwall.com
Alberto Nardi - Strategic Account Manager Italy & France - anardi@sonicwall.com
Mafalda Barbuto - Inside Channel Account Manager - mbarbuto@sonicwall.com
Sven Kicivoj - Inside Channel Account Manager - skicivoj@SonicWall.com
Luca Pesce - Sales Engineer North Italy - lpesce@sonicwall.com
Federico Diamantini - Sales Engineer Center-South Italy - fdiamantini@SonicWall.com
Jessica Ferrerons - Marketing Manager South EMEA - jferrerons@sonicwall.com


SONICWALL®