Linee di prodotti SonicWall: in sintesi

Firewall di nuova generazione

Fascia alta: Serie NS*sp*

I firewall sono progettati per grandi imprese distribuite, data center e fornitori di servizi di sicurezza gestiti (MSSP) e si contraddistinguono per la protezione ad alta velocità, l'alta densità di porte e throughput di ispezione firewall fino a 100 Gbps.

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.

I firewall SonicWall includono il filtraggio DNS e il filtraggio dei contenuti basato sulla reputazione per bloccare siti web e applicazioni dannose e consentono di impostare criteri per la visualizzazione dei contenuti web utilizzando punteggi di reputazione. La memoria ampliata per i file di audit, l'integrazione di Network Access Control (NAC) e gli aggiornamenti automatici aumentano la facilità d'uso.

Serie SonicWave

Sicurezza avanzata, prestazioni e scalabilità migliorate grazie al supporto Wi-Fi 6, gestione via cloud con SonicWall Wireless Network Manager o Network Security Manager.

Serie SMA

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

SonicWall Switch

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

Email Security

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

Global Management System (GMS)
Network Security Manager
Wireless Network Manager

Controllo centralizzato, gestione dei rischi e compliance. Report e informazioni dettagliate sul traffico e sulle minacce. Flussi di lavoro e aggiornamenti automatizzati.

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.

Per ulteriori informazioni su sonicwall.com

Domande di valutazione

Firewall di nuova generazione

- Come impedite l'accesso a siti Web dannosi o evitate la visualizzazione di contenuti inappropriati?
- Utilizzate soluzioni diverse per il filtraggio DNS e il filtraggio dei contenuti?
- 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? 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 motori di analisi sono integrati nella vostra sandbox?
- La vostra sandbox è in grado di trattenere i file sospetti al gateway?
- Sapete se il firewall della vostra attività ispeziona il traffico HTTPS?
- Avete subito interruzioni del servizio di rete o downtime 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 policy 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

La tecnologia Real-Time Deep Memory Inspection (RTDMI™) brevettata da SonicWall 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 motore identifica e mitiga le attuali minacce anche più insidiose, tra cui i futuri exploit Meltdown.

Serie SonicWave

- I vostri dipendenti/partner/clienti si lamentano della lentezza della rete Wi-Fi?
- Quale sarebbe il numero massimo di utenti wireless possibili in un qualsiasi momento?
- Vi preoccupano i costi necessari per aggiungere una soluzione wireless sicura alla vostra rete?
- Conoscete lo standard wireless 802.11ax?
- Vi serve flessibilità per gestire gli access point in varie sedi?
- 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?

SonicWall Switch

- 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?
- Avete bisogno di scollegare i vostri switch dai firewall?

Accesso mobile sicuro

- 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?

Email Security

- 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 a offrire servizi gestiti per la sicurezza delle e-mail ai vostri clienti? (MSSP)

Gestione e analisi

- Come gestite gli aggiornamenti del firmware?
- Come applicate le policy di sicurezza a tutta la vostra azienda?
- 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?
- Vi serve una gestione integrata dei dispositivi wireless e degli switch in un unico cruscotto?

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?