LINEE DI PRODOTTI SONICWALL: IN SINTESI

Firewall di prossima generazione

Fascia alta: NS*sp* 12000
Serie NS*sp* 12800/12400
Sicurezza modulare avanzata per grandi aziende distribuite, data center e fornitori di servizi, che sfrutta la potenza della cloud intelligence

Fascia media: Serie NS*a*
NS*a* 9650/9450/9250/ 6650/5650/4650/3650/2650

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

Entry Level: Serie TZ
TZ600/TZ500/TZ400/TZ350/ TZ300/ SOHO 250/SOHO

Prevenzione delle minacce e piattaforma SD-WAN integrata per PMI e aziende distribuite

Virtuale: Serie NSv

Firewall virtuali con modelli di licenza flessibili per proteggere tutti i componenti critici della vostra infrastruttura cloud pubblica e privata

Sicurezza wireless

Serie SonicWave
SonicWave 432e/432i/432o 231c/224w/231o
Sicurezza e prestazioni appositamente studiate per la prossima generazione di dispositivi wireless, gestite tramite cloud o firewall

Accesso mobile sicuro

Serie SMA – SMA
EX9000/8200v/7200/ 6200/500v/400/200
Accesso semplice e sicuro, basato su politiche, alle risorse di rete e nel cloud

Serie Email Security

ESA 9000/7000/5000/
Software VM / Servizio Cloud
Una soluzione di protezione multilivello contro le minacce e-mail avanzate

Gestione e analisi

Capture Security Center
Global Management System (GMS)
Analytics
Il controllo e la conoscenza della rete sono fondamentali per la sicurezza

Serie WAN Acceleration

WXA 6000 (SW)
WXA 5000 (VM)/500 (SW)
Migliora in modo significativo la velocità di trasferimento delle applicazioni e incrementa la produttività dei dipendenti

Capture Client

Una piattaforma client unificata con diverse funzionalità di protezione dell'endpoint, tra cui protezione contro i malware, sandboxing, controllo dei dispositivi e ripristino allo stato precedente in caso d'infezione

Web Application Firewall (WAF)

Protezione delle applicazioni web, prevenzione della perdita di dati e conformità alle normative, on-premise o nel cloud

Cloud App Security

Una soluzione CASB che offre la sicurezza di prossima generazione delle applicazioni SaaS come Office 365 e G Suite, per la protezione di email, dati e credenziali utente dalle minacce avanzate e garantendo al tempo stesso la conformità nel cloud.

Servizi in abbonamento firewall di prossima generazione

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

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

Security-as-a-Service (SECaaS)

La nostra soluzione chiavi in mano per gestire la sicurezza di rete in outsourcing

Analisi approfondita della memoria

SonicWall RTDMI™ (Real-Time Deep Memory Inspection), una tecnologia in attesa di brevetto, individua proattivamente e blocca 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 più insidiose, tra cui i futuri exploit Meltdown.

Per ulteriori informazioni: www.sonicwall.com/en-us/products

Domande di valutazione

Firewall di prossima generazione

- Come misurate l'efficacia dei vostri controlli di sicurezza?
- Qual è il vostro piano di risoluzione per i problemi di sicurezza rilevati?
- Come limitate il rischio di eventuali applicazioni web vulnerabili utilizzate dai vostri utenti?
- Che tipo di connessione Internet utilizzate? Quale velocità?
- Siete costretti a sacrificare le performance per migliorare la sicurezza della rete?
- Quali misure adottate per proteggervi da nuove minacce come gli attacchi zero-day?
- Il vostro team di esperti informatici è in grado di applicare le patch entro 12 ore dal loro rilascio?
- 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 al gateway?
- Lo sapevate che la maggior parte delle sessioni web è crittografata e che il vostro firewall è in grado di decrittarle e analizzarle?
- Sapete se il firewall della vostra azienda 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 implementare zone di sicurezza adeguate e la microsegmentazione sulla vostra rete virtuale?
- Avete visibilità e controllo completi sul vostro traffico virtuale?
- Il vostro firewall attuale integra il supporto per PoE/PoE+ o vi serve uno switch per alimentare i dispositivi con funzionalità PoE?
- Vi interesserebbe ridurre i costi, sostituendo MPLS con SD-WAN per creare una rete privata sicura?
- Vi servono licenze in abbonamento per i firewall virtuali?

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?
- La vostra soluzione attuale monitora costantemente lo stato del vostro sistema?
- Siete in grado di ripristinare uno stato precedente non compromesso in caso di danni provocati da ransomware?
- Siete in grado d'impedire ai dispositivi sconosciuti e potenzialmente infetti la connessione agli endpoint?

Web Application Firewall

- Quale strategia usate attualmente per proteggere le vostre proprietà web e i server web strategici?
- Quali misure di sicurezza avete adottato per garantire il rispetto dei requisiti di sicurezza PCI?

Cloud App Security

- Utilizzate O365 o G Suite?
- Utilizzate Proofpoint o Mimecast per la sicurezza di O365/G Suite?
- Effettuate la scansione delle email interne O365?
- 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 compromesse?
- Riuscite a sapere chi accede ai dati, da dove e quando? (BYOD)

Sicurezza wireless

- 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 802.11ac Wave 2?
- Vi serve flessibilità per gestire gli access point – cloud rispetto alla gestione dei firewall?
- Avete pianificato la rete WiFi in modo efficace?
- Avete bisogno di scollegare gli AP dai firewall?
- Avete problemi a configurare le funzionalità di sicurezza avanzate nella rete WiFi?

Accesso mobile sicuro

- La vostra azienda ha trasferito applicazioni aziendali nel cloud, o prevede di farlo in futuro?
- Fornite ai vostri utenti Single-Sign On unificato per le applicazioni fisiche o per quelle nel cloud?
- I vostri dipendenti utilizzano Dropbox o le email personali per condividere file?
- I vostri dipendenti gestiscono diversi URL e password?
- Qual è la vostra attuale strategia di mobilità/BYOD?
- Avete visibilità su qualsiasi dispositivo che accede alla vostra rete?

Sicurezza e-mail

- Vi preoccupano le minacce avanzate diffuse tramite e-mail come ransomware, spear-phishing e Business Email Compromise (BEC)?
- La vostra soluzione di sicurezza e-mail attuale offre funzionalità di protezione contro le minacce avanzate?
- Vi preoccupa la possibilità che e-mail contenenti informazioni riservate possano essere divulgate?
- La vostra azienda è conforme a normative quali 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

- Quali problemi potreste risolvere unificando le vostre soluzioni di sicurezza in una piattaforma di gestione comune, dotata di un unico pannello di controllo?
- Quali difficoltà economiche e operative incontrate nella gestione della vostra infrastruttura di sicurezza?
- 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 accurato?
- Quali vantaggi otterrebbero la vostra azienda e la dirigenza da una visibilità completa sulle minacce informatiche e i rischi per il vostro business?

Accelerazione WAN

- La vostra azienda dispone di più uffici remoti in località diverse? Quanti sono?
- Gli uffici remoti sono collegati in rete con una connessione VPN o un circuito WAN dedicato (MPLS)?
- I vostri dipendenti utilizzano applicazioni come Microsoft Windows File Sharing, SharePoint, Office o FTP?
- Vorreste ridurre il consumo di banda e i relativi costi senza dover pagare per un aumento di capacità?

Per ulteriori informazioni: www.sonicwall.com/en-us/products

Datasheet-SonicWallProductLineAtAGlance-US-VG-MKTG5159

SONICWALL®