

Serie SonicWall NSa Gen 8 di fascia media

Protezione avanzata contro le minacce per aziende distribuite e campus

I nuovi next-generation firewall SonicWall di fascia media della serie Network Security appliance (NSa) offrono a medie e grandi aziende prestazioni di prevenzione delle minacce leader del settore con il costo totale di proprietà più basso della categoria. I firewall sono l'elemento essenziale della soluzione di protezione contro le minacce, che include la gestione centralizzata semplificata dei firewall, il supporto Zero Trust, licenze flessibili con servizi firewall gestiti opzionali e una garanzia informatica integrata per la mitigazione dei rischi.

I firewall di Generazione 8 (Gen 8) offrono 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, proteggendo il perimetro di rete da minacce avanzate senza creare colli di bottiglia.



NSa 2800



NSa 3800



NSa 4800



NSa 5800

La serie NSa Gen 8 in breve.

Specifiche complete »

**Fino a
7 Gb/s**

Throughput di prevenzione delle minacce

**Fino a
30 Gb/s**

Throughput firewall

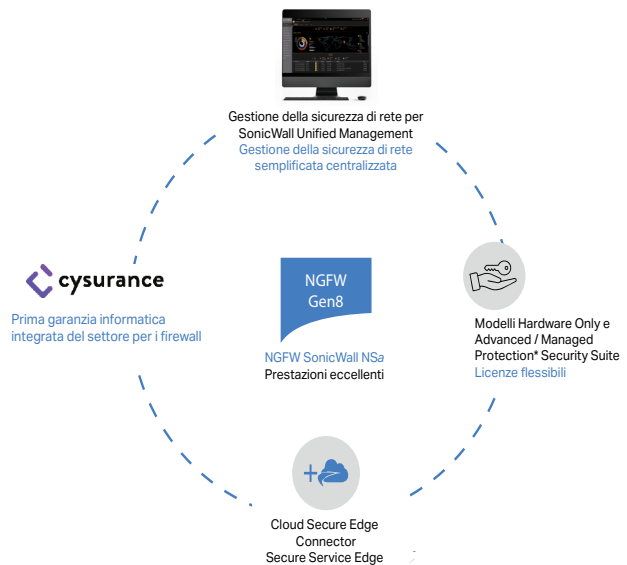
**Fino a
8 milioni**

Connessioni

CARATTERISTICHE PRINCIPALI

- Fattore di forma: 1U rack-mount
- 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)
- Eccellente rapporto prezzo/prestazioni
- Memoria espandibile
- Filtraggio DNS avanzato
- Servizio di filtraggio dei contenuti (CFS 5.0) basato sulla reputazione
- Gestione centralizzata semplificata di applicazioni SaaS e on-premise tramite [Network Security Manager](#)
- Gestione firewall Wi-Fi 6
- Supporto per [SonicWall Unified Management](#)
- Predisposizione per Internet edge aziendale
- Funzionalità SD-WAN sicura
- Supporto per TLS 1.3
- Licenze semplificate, tra cui Hardware Only, Advanced Protection Security Suite e Managed Protection Security Suite
- Supportata dal team di ricerca delle minacce dei SonicWall Capture Labs
- Integrazione con switch SonicWall, access point SonicWave e Capture Client
- Supporto per [Cloud Secure Edge Connector](#)
- [Garanzia integrata](#) di Cysurance fino a 200.000 dollari, inclusa nelle suite di servizi

I firewall NSa Gen 8 garantiscono una solida protezione grazie a una soluzione completa che include protezione contro le minacce, gestione centralizzata, report e analisi, opzioni di sicurezza e servizi gestiti, integrazione di Secure Service Edge (SSE) e garanzia informatica.



Hardware

I firewall della serie NSa Gen 8, realizzati con i più moderni componenti hardware, forniscono la prevenzione delle minacce a velocità multi-gigabit anche per il traffico crittografato. Le soluzioni firewall offrono un'elevata densità di porte e supportano la ridondanza hardware e di rete con elevata disponibilità e due adattatori di alimentazione, tra cui uno per la ridondanza.

Architettura

La serie NSa Gen 8 utilizza SonicOS 8, un nuovo sistema operativo che offre una moderna interfaccia utente, flussi di lavoro intuitivi e un approccio che mette l'utente in primo piano. [SonicOS 8](#) fornisce 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 NSa 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, i dispositivi offrono un unico pannello di controllo per gestire sia gli switch che gli access point.

Servizi di sicurezza e protezione dalle minacce

Creata per mitigare gli attacchi informatici avanzati attuali e futuri, la serie NSa Gen 8 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, la tecnologia brevettata 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 la maggior parte dei malware nascosti e pericolosi, comprese le minacce zero-day e crittografate.

Le licenze semplificate includono le opzioni Hardware Only, Advanced Protection Service Suite (APSS) e Managed Protection Service Suite (MPSS) per soddisfare qualsiasi esigenza. MPSS ottimizza le risorse mediante servizi gestiti per i firewall.

L'integrazione di Cloud Secure Edge Connector offre un accesso sicuro alle applicazioni private dietro i firewall. Gli utenti e i dispositivi possono seguire un approccio Zero Trust per accedere alle applicazioni.

Garanzia informatica

Insieme alla suite di sicurezza viene offerta una garanzia informatica incorporata che consente di mitigare i costi in caso di violazioni della sicurezza e soddisfare i requisiti di conformità, garantendo una maggiore tranquillità.

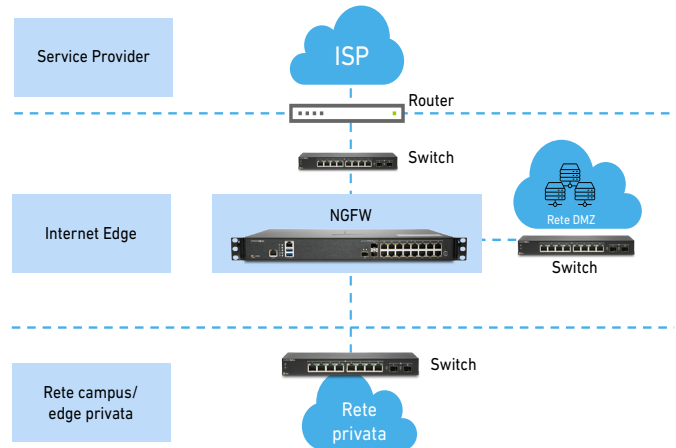
Implementazioni

La serie NSa Gen 8 offre due opzioni di implementazione principali per le medie imprese e le aziende distribuite:

Implementazioni Internet Edge

In questa configurazione d'installazione standard, il firewall NGFW della serie NSa Gen 8 protegge le reti private dal traffico dannoso proveniente da Internet, permettendo di:

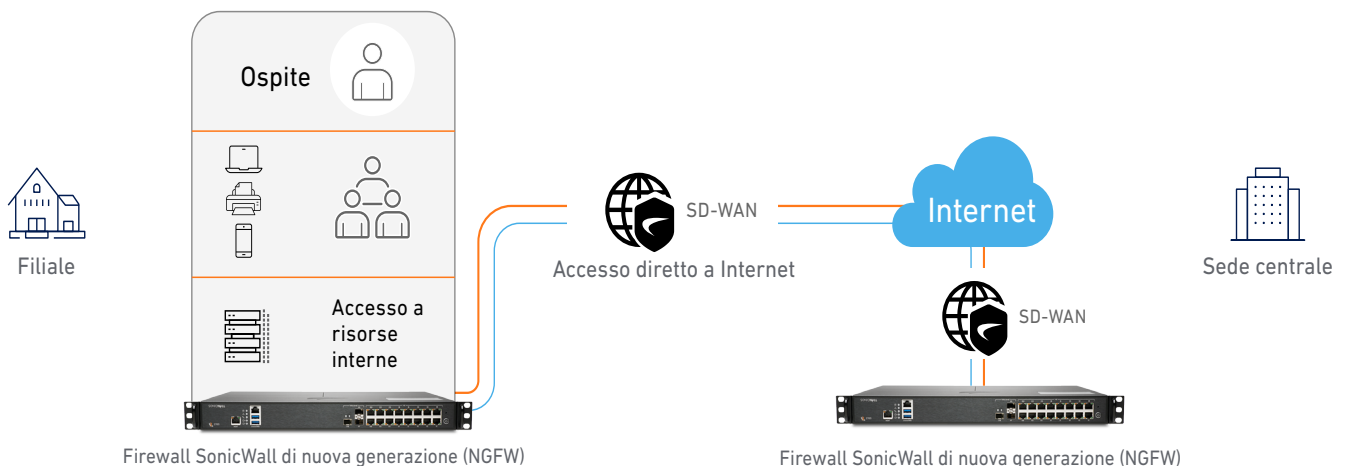
- Implementare una soluzione NGFW con le migliori prestazioni della sua categoria
- Ottenere visibilità e ispezionare il traffico crittografato, incluso quello TLS 1.3, per bloccare le minacce elusive provenienti da Internet – il tutto senza compromettere le prestazioni
- Proteggere l'azienda con funzioni 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'unica interfaccia intuitiva



Medie imprese e aziende distribuite

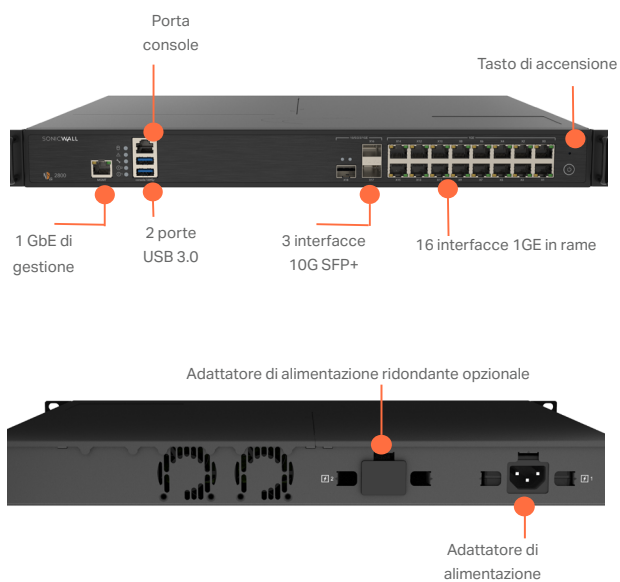
La serie SonicWall NSa Gen 8 supporta l'SD-WAN e può essere gestita centralmente, fornendo una soluzione ideale per aziende distribuite e imprese di medie dimensioni. Questa implementazione consente alle aziende di:

- 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

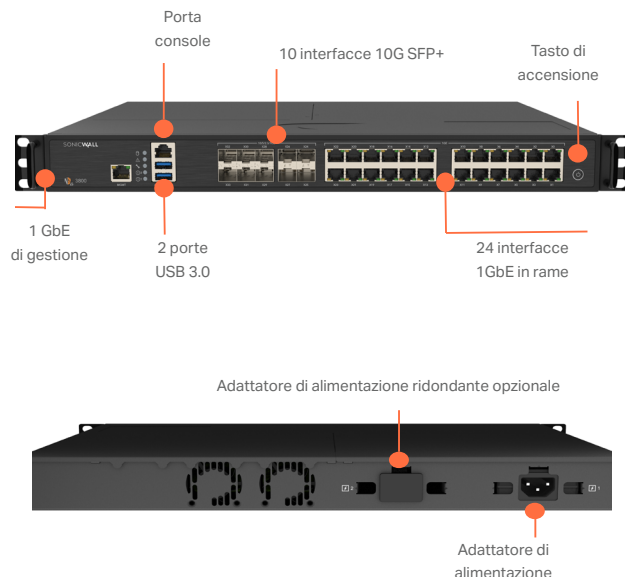


Serie SonicWall NSa Gen 8

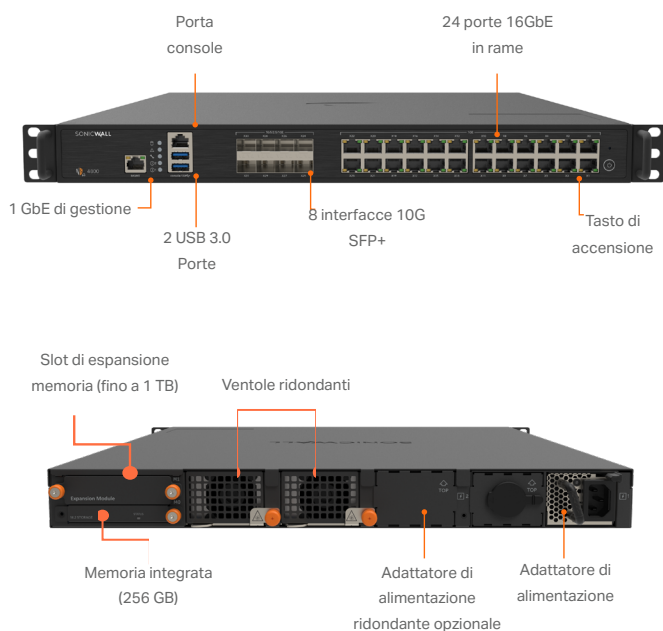
NSa 2800



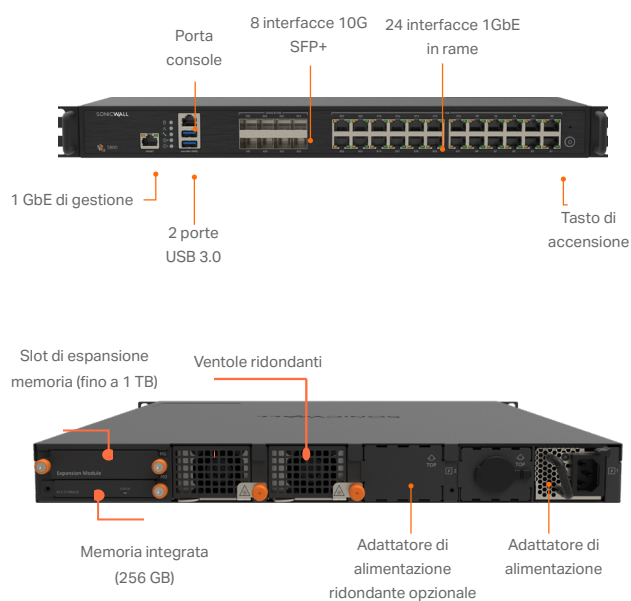
NSa 3800



NSa 4800



NSa 5800



Specifiche di sistema della serie NSa Gen 8

Firewall	NSa 2800	NSa 3800	NSa 4800	NSa 5800
Sistema operativo	SonicOS 8			
Interfacce	16 x 1GbE, 3 x 10G SFP+, 2 USB 3.0, 1 console, 1 porta di gestione	24 x 1GbE, 10 x 10G SFP+, 2 USB 3.0, 1 console, 1 porta di gestione	24 x 1GbE in rame, 8 x 10G SFP+, 1 console (RJ45 - DB9), 2 USB (tipo A)	24 x 1GbE in rame, 8 x 10G SFP+, 1 console (RJ45 - DB9), 2 USB (tipo A)
Memoria / (espansione)	128 Gb (fino a 512 GB)	256 Gb (fino a 512 GB)	256 GB (fino a 1 TB)	256 GB (fino a 1 TB)
Gestione centralizzata	Network Security Manager (NSM) 3.0 e superiore, CLI, SSH, Web UI, API REST			
Interfacce VLAN logiche e tunnel (max.)	256	256	512	512
Utenti Single Sign-On SAML ¹	40.000	40.000	50.000	50.000
Punti di accesso supportati (max.)	512	512	512	512
Prestazioni firewall/VPN				
Throughput di ispezione firewall ²	8 Gb/s	12 Gb/s	20 Gb/s	30 Gb/s
Throughput di prevenzione delle minacce ³	6 Gb/s	8 Gb/s	13 Gb/s	24 Gb/s
Throughput di ispezione applicazioni ³	7 Gb/s	9 Gb/s	13 Gb/s	24 Gb/s
Throughput IPS ²	7 Gb/s	8 Gb/s	13 Gb/s	24 Gb/s
Throughput di ispezione anti-malware ³	6 Gb/s	8 Gb/s	13 Gb/s	24 Gb/s
Throughput ispezione e decrittografia TLS/SSL ³	1,8 Gb/s	3 Gb/s	4,2 Gb/s	8 Gb/s
Throughput VPN IPSec ⁴	5,5 Gb/s	8 Gb/s	10 Gb/s	21 Gb/s
Connessioni al secondo	50.000	90.000	140.000	240.000
Connessioni SPI (max.)	2.000.000	3.000.000	5.000.000	8.000.000
Connessioni DPI (max.)	1.000.000	1.200.000	3.000.000	5.000.000
Connessioni TLS (max.)	150.000	300.000	600.000	750.000
VPN e ZTNA				
Tunnel VPN site-to-site	2.000	3.000	4.000	6.000
Client VPN IPSec (max)	50 (1.000)	50 (1.000)	500 (3.000)	2.000 (4.000)
Licenze VPN SSL (max)	2 (500)	2 (500)	2 (1.000)	2 (1.500)
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 Over VPN, IPSec NAT Traversal, gateway VPN ridondante, VPN basata su routing			
Piattaforme client supportate per la VPN globale	Microsoft® Windows 10 e Windows 11			
NetExtender	Microsoft® Windows 10 e Windows 11, Linux			
Mobile Connect	Apple® iOS, Mac OS X, Google® Android™			
Accesso privato SonicWall basato su Cloud Secure Edge ⁵	Incluso nel programma di fidelizzazione 3&Free			
Servizi di sicurezza				
Servizi Deep Packet Inspection	Antispyware e antivirus per gateway, prevenzione delle intrusioni, decrittografia TLS			
Content Filtering Service (CFS)	Filtraggio degli URL basato sulla reputazione, scansione di URL HTTP, IP HTTPS, parole chiave e contenuti, filtraggio completo basato su tipi di file come ActiveX, Java, cookie per la privacy, elenchi di siti consentiti/vietati			

Specifiche di sistema della serie NSa Gen 8

Firewall	NSa 2800	NSa 3800	NSa 4800	NSa 5800
Servizio anti-spam completo	●	●	●	●
Visualizzazione delle applicazioni	●	●	●	●
Controllo delle applicazioni	●	●	●	●
Capture Advanced Threat Protection	●	●	●	●
Filtraggio DNS	●	●	●	●
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	BGP, 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, 802.1e (WMM)			
Autenticazione	LDAP (domini multipli), XAUTH/RADIUS, TACACS+, SAML SSO ¹ , accounting Radius, NTLM, database utenti interno, 2FA, servizi Terminal, Citrix, Common Access Card (CAC)			
Database utenti locale	1000	1000	1000	1000
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	IPv6/USGv6			
Alta disponibilità	Attiva/Passiva con sincronizzazione dello stato			
Hardware				
Fattore di forma	1U rack-mount			
Alimentazione	90 W	150 W	450 W	450 W
Potenza max. assorbita (W)	52,8	102,3	110,4	119,4
Tensione di esercizio (AC)	100-240 V AC, 50-60 Hz	100-240 V AC, 50-60 Hz	100-240 V AC, 50-60 Hz	100-240 V AC, 50-60 Hz
Dissipazione di calore totale (BTU)	180,01	341	377,4	407,5
Dimensioni (unità: cm)	43 x 32,5 x 4,5 Confezione: 57,5 x 47,5 x 18,5	43 x 32,5 x 4,5 57,5 x 47,5 x 18,5	43 x 46 x 4,5 Confezione: 69,5 x 59,5 x 21	43 x 46 x 4,5 Confezione: 69,5 x 59,5 x 21
Peso	4,6 kg	4,6 kg	7,4 kg	7,4 kg
Peso RAEE	4,8 kg	4,8 kg	9,3 kg	9,3 kg
Peso con la confezione	7,2 kg	7,2 kg	13,2 kg	13,2 kg
Condizioni ambientali (in funzionamento/stoccaggio)	da 0 °C a +40 °C / da -40 °C a +70 °C		da 0 °C a +40 °C / da -40 °C a +70 °C	
Umidità	5-95% senza condensa	5-95% senza condensa	5-95% senza condensa	5-95% senza condensa
Normative				
Principali normative di conformità: NSa 2800 e 3800	FCC Classe A, ICES Classe A, CE (EMC, LVD, RoHS), UL, cUL, DGN Notice by UL (Messico), ANATEL, WEEE, REACH, SCIP, RCM, MIC Terminal, VCCI Classe A, KCC/MSIP, BSMI, MTCTE/TEC, CB			
Principali normative di conformità: NSa 4800 e 5800	FCC Classe A, ICES Classe A, CE (EMC, LVD, RoHS), UL, cUL, DGN Notice by UL (Messico), ANATEL, WEEE, REACH, SCIP, RCM, VCCI Classe A, KCC/MSIP, BSMI, MTCTE/TEC, CB			
Numeri di modello normativi	1RK56-11C	1RK57-122	1RK58-123	1RK58-123

¹ Il Single Sign-On SAML è disponibile in SonicOS 8.1, che sarà rilasciato a breve.

² 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.

³ Rilevazione throughput per prevenzione minacce/Gateway AV/antispyware/IPS tramite strumenti di test delle performance Keysight HTTP standard nel settore. 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.

⁴ 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.

⁵ Incluso nel pacchetto di 3 anni

Riepilogo delle funzioni di SonicOS 8

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
- Integrazione AP SonicWall Wi-Fi 6
- Scalabilità SD-WAN
- Procedura guidata di usabilità SD-WAN
- Scalabilità delle connessioni (SPI, DPI, TLS)

Dashboard ottimizzata

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

Capture Advanced Threat Protection¹

- Real-Time Deep Memory Inspection
- Analisi multi-engine basata sul cloud¹
- Sandbox virtuale
- Analisi a livello hypervisor
- Emulazione di sistema completa
- Ispezione di un'ampia varietà di file
- Invio automatizzato e manuale
- Informazioni sulle minacce con aggiornamenti in tempo reale¹
- Blocco fino al verdetto
- Capture Client²

Prevenzione delle intrusioni¹

- Scansione basata sulle firme
- Integrazione del controllo accessi alla rete con Aruba ClearPass
- Aggiornamenti automatici delle firme
- Ispezione bidirezionale
- Funzionalità per regole IPS granulari
- Identificazione tramite GeoIP
- Filtraggio Botnet con elenco dinamico

- Corrispondenza con espressioni regolari

Anti-malware¹

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

Identificazione delle applicazioni¹

- Controllo delle applicazioni
- Gestione della larghezza di banda delle applicazioni
- Creazione di firme per applicazioni personalizzate
- Prevenzione di perdite di dati
- Creazione di rapporti 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 Web¹

- Filtraggio URL
- Proxy avoidance
- Blocco in base a parole chiave
- Servizio di filtraggio dei contenuti (CFS 5.0) basato sulla reputazione
- Filtraggio DNS
- 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 e ZTNA

- Secure SD-WAN
- Provisioning automatico delle VPN
- VPN IPSec per una connettività Site-to-Site
- Accesso remoto tramite VPN SSL e client IPSec
- Gateway per la rete VPN ridondante
- Mobile Connect per iOS, Mac OS X, Windows e Android
- VPN basata sul routing (OSPF, RIP, BGP)
- Accesso privato sicuro tramite Cloud Secure Edge

Connettività di rete

- PortShield
- Frame Jumbo
- Indagine del percorso MTU
- Registrazione avanzata
- VLAN trunking
- Mirroring delle porte (switch SonicWall)
- 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
- Gatekeeper H.323 e supporto per proxy SIP

Gestione, monitoraggio e supporto

- Supporto Capture Security Appliance (CSa)
- 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
- Dashboard
- Informazioni sui dispositivi, applicazioni, minacce
- Visualizzazione della topologia
- Definizione e gestione semplificate delle policy
- Statistiche d'uso per policy e oggetti
- Utilizzato / non utilizzato
- Attivo / non attivo
- Ricerca globale di dati statici
- Supporto memorizzazione

Riepilogo delle funzioni di SonicOS 8.0 (continua)

Gestione, monitoraggio e supporto (continua)

- Gestione memoria interna ed esterna
- Supporto scheda USB WWAN (5G/LTE/4G/3G)
- Supporto Network Security Manager (NSM)
- SonicWall Unified Management e SonicWall AI for Monitoring and Insight (SAMI)
- GUI Web
- CLI (Command Line Interface)
- Registrazione e provisioning zero-touch
- Reportistica semplificata CSC
- Supporto app mobile SonicExpress
- SNMPv2/v3
- API per report e analisi
- Logging
- Esportazione per Netflow/IPFix

- Backup della configurazione basato su cloud
- Piattaforma Security Analytics di BlueCoat
- Visualizzazione della larghezza di banda e delle applicazioni
- Gestione IPv4 e IPv6
- Schermata di gestione CD
- Gestione degli switch Dell serie N e X, compresi gli switch a cascata

Debugging e diagnostica

- Monitoraggio ottimizzato dei pacchetti
- Terminale SSH su interfaccia utente

Wireless

- Gestione firewall e AP SonicWave nel cloud
- WIDS/WIPS
- Prevenzione di access point non autorizzati
- Fast roaming (802.11k/r/v)
- Connettività di rete 802.11s mesh
- Selezione automatica dei canali
- Analisi dello spettro RF
- Vista planimetrica
- Visualizzazione della topologia
- Band steering
- Beamforming
- AirTime fairness
- Bluetooth Low Energy
- MiFi extender
- Migliorie e potenziamenti RF
- Quota ciclica ospite

¹ Richiede l'abbonamento alla Security Suite

Maggiori informazioni sulla serie SonicWall NSa Gen 8

www.sonicwall.com/products/firewalls

[SonicWall, Inc.](#)

1033 McCarthy Boulevard | Milpitas, CA 95035 | Per maggiori informazioni consultare il nostro sito web.

© 2025 SonicWall Inc. TUTTI I DIRITTI RISERVATI.

SonicWall è un marchio o marchio registrato di SonicWall Inc. e/o delle sue affiliate negli Stati Uniti e/o in altri Paesi. Tutti gli altri marchi e marchi registrati appartengono ai rispettivi proprietari. Le informazioni contenute nel presente documento si riferiscono ai prodotti di SonicWall Inc. e/o delle sue affiliate. Né il presente documento né la vendita di prodotti SonicWall costituiscono alcuna licenza, espressa o implicita, di estoppel o di altro tipo, né garantiscono diritti di proprietà intellettuale. Salvo quanto specificato nei termini e nelle condizioni stabiliti nel contratto di licenza di questo prodotto, SonicWall e/o le sue affiliate non si assumono alcuna responsabilità ed escludono garanzie di qualsiasi tipo, esplicite, implicite o legali, in relazione ai propri prodotti, incluse, in via esemplificativa, qualsiasi garanzia implicita di commerciabilità, idoneità a scopi specifici o violazione di diritti altrui. SonicWall e/o le sue affiliate declinano ogni responsabilità per danni di qualunque tipo, siano essi diretti, indiretti, consequenziali, punitivi, speciali o incidentali (inclusi, senza limitazioni, danni per mancato guadagno, interruzioni dell'attività o perdite di dati) derivanti dall'utilizzo o dall'impossibilità di utilizzare il presente documento, anche nel caso in cui SonicWall e/o le sue affiliate siano state avvertite dell'eventualità di tali danni. SonicWall e/o le sue affiliate non rilasciano alcuna garanzia o dichiarazione relativamente alla precisione o completezza dei contenuti del presente documento e si riservano il diritto di apportare modifiche, in qualsiasi momento e senza preavviso, alle specifiche e alle descrizioni dei prodotti. SonicWall Inc. e/o le sue affiliate non si assumono alcun impegno di aggiornare le informazioni contenute in questo documento.

Solution Brief - SonicWall Unified Management

sonicwall.com



SONICWALL[®]