Serie SonicWall NS*a* Gen 8 di fascia media

Protezione avanzata contro le minacce per aziende distribuite e campus

I nuovi firewall SonicWall Network Security appliance (NS*a*) 2800 e 3800 di fascia media di ultima generazione 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 8ª generazione (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.

NS*a* 3800

NS*a* 2800

NS*a* 2800 e 3800 Gen 8 in breve. Specifiche complete »

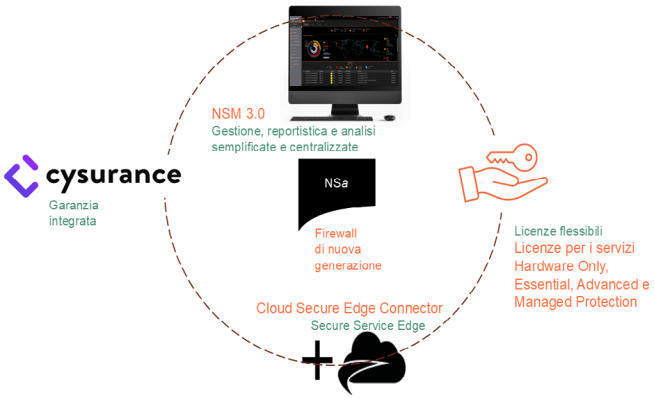
Fino a 8 Gb/s	Fino a 12 Gb/s	Fino a 3 milioni
Throughput di prevenzione delle minacce	Throughput firewall	Connessioni

SCHEDA TECNICA

CARATTERISTICHE PRINCIPALI

- Fattore di forma: 1U rack-mount
- 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 SonicPlatform
- Predisposizione per Internet edge aziendale
- Funzionalità SD-WAN sicura
- Supporto per TLS 1.3
- Licenze flessibili, tra cui Hardware Only, Essential, Advanced e Managed Protection Service 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 Cysurance fino a 200.000 dollari integrata nelle suite di servizi

I firewall NS*a* 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

NS*a* 2800 e 3800, 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, tra cui diverse porte 10 GbE, e supportano la ridondanza di rete e hardware con elevata disponibilità e doppia alimentazione.

Architettura

La serie NS*a* 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 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.

NS*a* 2800 e 3800 supportano funzionalità di rete avanzate quali SD-WAN, routing dinamico, elevata 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 gli access point.

Servizi di sicurezza e protezione dalle minacce

Creata per mitigare gli attacchi informatici avanzati attuali e futuri, la serie NS*a* 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 malware nascosti e pericolosi, comprese le minacce zero-day e crittografate.

Le licenze flessibili includono le opzioni Hardware Only, Essential, Advanced e Managed Protection Service Suite (MPSS) per soddisfare esigenze specifiche. 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 aderire a un framework zero-trust per l'accesso alle applicazioni.

Garanzia informatica

Insieme ai servizi di sicurezza viene offerta una garanzia informatica incorporata per mitigare i costi in caso di violazioni della sicurezza e soddisfare i requisiti di conformità, garantendo una maggiore tranquillità.

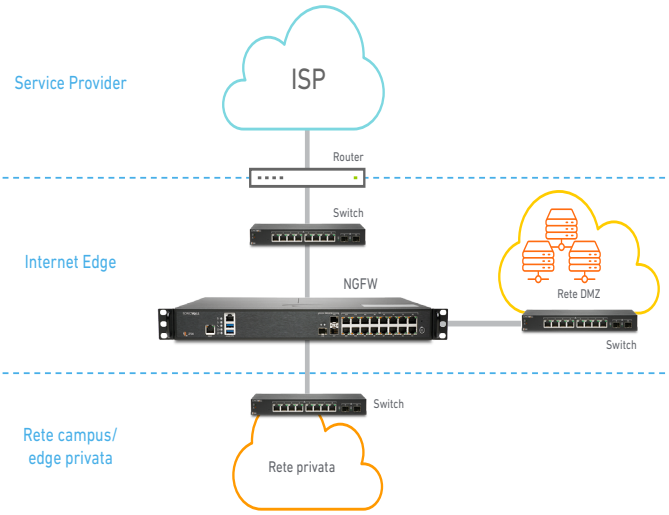
Implementazioni

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

Implementazioni Internet Edge

In questa opzione d'implementazione standard, il firewall di nuova generazione della serie NS*a* Gen 8 protegge le reti private dal traffico dannoso proveniente da Internet, permettendo di:

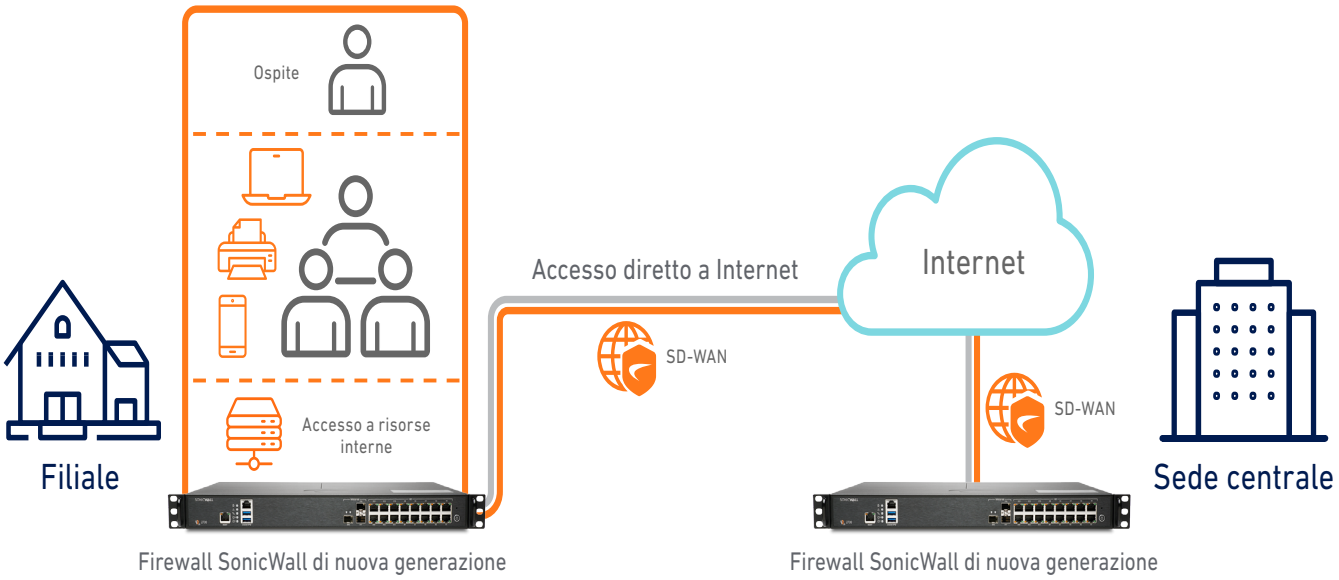
- Implementare una soluzione NGFW con le migliori prestazioni della sua categoria
- Ottenere visibilità e ispezionare il traffico crittografato, incluso quello TLS 1.3, per bloccare le minacce elusive provenienti da Internet – il tutto senza compromettere le prestazioni
- Proteggere l'azienda con funzioni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



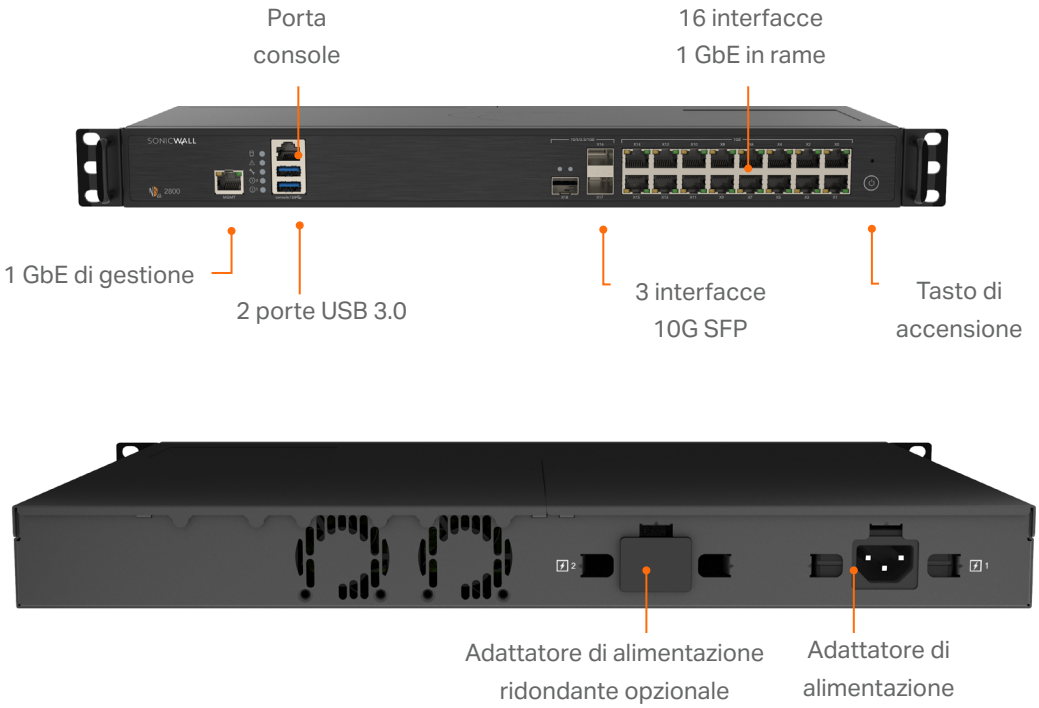
Medie imprese e aziende distribuite

La serie SonicWall NS*a* 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:

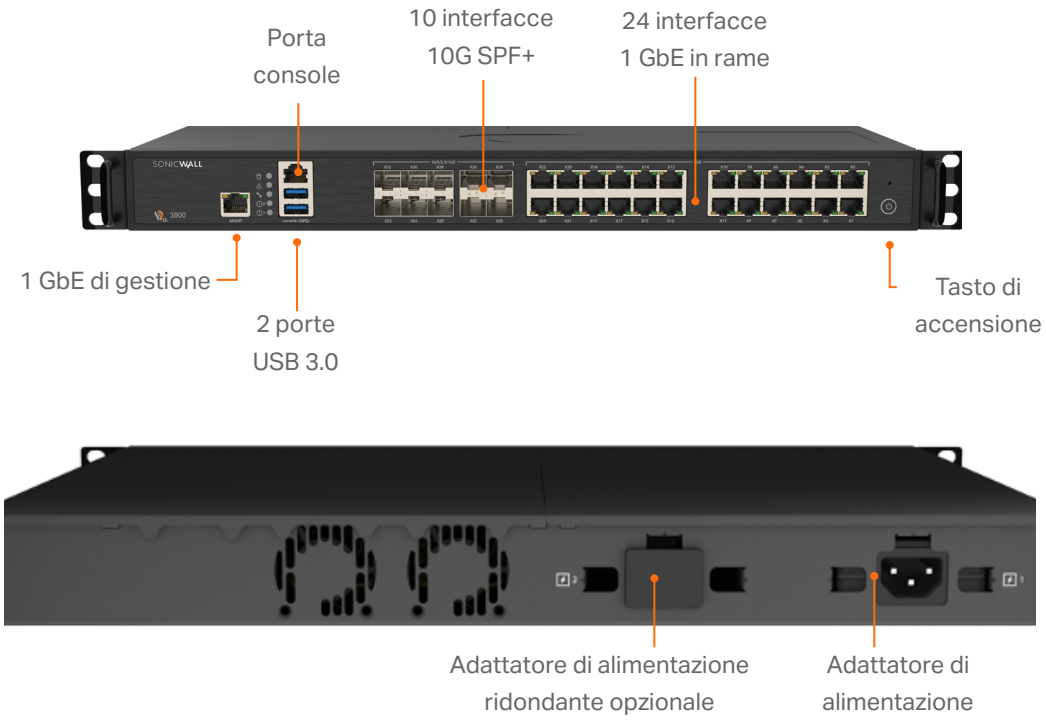
- Proteggersi dalle minacce future in continua evoluzione, investendo in un firewall NGFW con analisi delle minacce a velocità multi-gigabit
- Fornire un accesso Internet diretto e sicuro alle filiali distribuite, evitando il backhauling del traffico attraverso la sede centrale dell'azienda
- Consentire 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



NS*a* 2800



NS*a* 3800



Specifiche di sistema della serie NS*a* Gen 8

Firewall	NS*a* 2800	NS*a* 3800
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, 6 x 10G SFP+, 4 x 5G SFP+, 2 USB 3.0, 1 console, 1 porta di gestione
Archiviazione	128 GB M.2	256 GB M.2
Slot di espansione memoria	Slot di espansione memoria (fino a 512 GB)	Slot di espansione memoria (fino a 512 GB)
Gestione centralizzata	Network Security Manager (NSM) 3.0 e superiore, CLI, SSH, Web UI, API REST	
Interfacce VLAN logiche e tunnel (max.)	256	256
Utenti Single Sign-On SAML[1]	40.000	40.000
Punti di accesso supportati (max.)	512	512
Prestazioni firewall/VPN		
Throughput di ispezione firewall[2]	8 Gb/s	12 Gb/s
Throughput di prevenzione delle minacce[3]	6 Gb/s	8 Gb/s
Throughput di ispezione applicazioni[3]	7 Gb/s	9 Gb/s
Throughput IPS[2]	7 Gb/s	8 Gb/s
Throughput di ispezione anti-malware[3]	6 Gb/s	8 Gb/s
Throughput ispezione e decrittografia TLS/SSL[3]	1,8 Gb/s	3 Gb/s
Throughput VPN IPSec[4]	5,5 Gb/s	8 Gb/s
Connessioni al secondo	50.000	90.000
Connessioni SPI (max.)	2.000.000	3.000.000
Connessioni DPI (max.)	1.000.000	1.200.000
Connessioni TLS (max.)	150.000	300.000
VPN e ZTNA		
Tunnel VPN site-to-site	2.000	3.000
Client VPN IPSec (max)	10 (1000)	50 (1000)
Licenze VPN SSL (max)	2 (500)	2 (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 route	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 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 basato su tipi di file come ActiveX, Java, cookie per la privacy, elenchi di siti consentiti/vietati	

Specifiche di sistema della serie NS*a* Gen 8

Firewall	NS*a* 2800	NS*a* 3800
Servizio anti-spam completo	Sì	Sì
Visualizzazione delle applicazioni	Sì	Sì
Controllo delle applicazioni	Sì	Sì
Capture Advanced Threat Protection	Sì	Sì
Filtraggio DNS	Sì	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	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
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 attesa: IPv6	
Alta disponibilità	Attiva/Passiva con sincronizzazione dello stato	
Hardware		
Fattore di forma	1U rack-mount	
Alimentazione	90 W	150 W
Potenza max. assorbita (W)	52,8	102,3 W
Tensione d'esercizio	100-240 V AC, 50-60 Hz, 4 A	100-240 V AC, 50-60 Hz, 12,5 A
Dissipazione di calore totale (BTU)	180,01	341
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
Peso	4,6	4,6
Peso RAEE	4,8	4,8
Peso con la confezione	7,2	7,2
Condizioni ambientali (in funzionamento/ stoccaggio)	da 0 °C a +40 °C / da -40 °C a +70 °C	
Umidità	5-95% senza condensa	5-95% 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[6], BSMI	
Numeri di modello normativi	1RK56-11C	1RK57-122

[1] Il Single Sign-On SAML è disponibile su 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/Anti-Spyware/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

[6] Disponibile in una fase successiva

Riepilogo delle funzioni di SonicOS 8.0

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
- Integrazione AP SonicWall Wi-Fi 6
- Scalabilità SD-WAN
- Procedura guidata di usabilità SD-WAN[1]
- Scalabilità delle connessioni (SPI, DPI, TLS)
- Dashboard ottimizzata[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 TLS con CFS
- Controlli DPI SSL granulari in base a zone o regole
- Capture Advanced Threat Protection[2]
- Real-Time Deep Memory Inspection
- Analisi multi-engine basata sul cloud[2]
- 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 reale[2]
- Blocco fino al verdetto
- Capture Client[2]

Prevenzione delle intrusioni[2]

- Scansione basata sulle firme
- Integrazione del controllo accessi alla rete con Aruba ClearPass
- Aggiornamenti automatici delle firme
- Ispezione bidirezionale
- Regole IPS granulari
- Geolocalizzazione degli IP
- 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
- Database di malware nel 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 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 Web[2]

- 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 (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
- 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[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]

Riepilogo delle funzioni di SonicOS 8.0 (continua)

Gestione, monitoraggio e supporto (continua)

- Gestione memoria interna ed esterna[1]
- Supporto scheda USB WWAN (5G/LTE/4G/3G)
- Supporto Network Security Manager (NSM)
- Supporto di SonicPlatform e SonicBot
- GUI Web
- CLI (Command Line Interface)
- Registrazione e provisioning zero-touch
- Reportistica semplificata CSC[1]
- Supporto app mobile SonicExpress
- SNMPv2/v3
- Gestione e reportistica centralizzate con SonicWall Global Management System (GMS)[2]
- 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] Nuova funzione, disponibile su SonicOS 7.0
[2] Richiede un abbonamento aggiuntivo

Maggiori informazioni sulla serie SonicWall NSa Gen 8

www.sonicwall.com/products/firewalls

SonicWall

SonicWall è un precursore della sicurezza informatica con oltre 30 anni di esperienza e di impegno continuo verso i propri partner. Grazie alla capacità di creare, scalare e gestire la sicurezza informatica in ambienti cloud, ibridi e tradizionali in tempo reale, SonicWall può fornire in modo rapido ed economico soluzioni di sicurezza dedicate a qualsiasi tipo di organizzazione in tutto il mondo. Mediante i dati del proprio centro di ricerca sulle minacce, SonicWall garantisce una protezione completa contro gli attacchi informatici più elusivi e fornisce informazioni pratiche sulle minacce ai partner, ai clienti e alla comunità di cybersecurity.

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