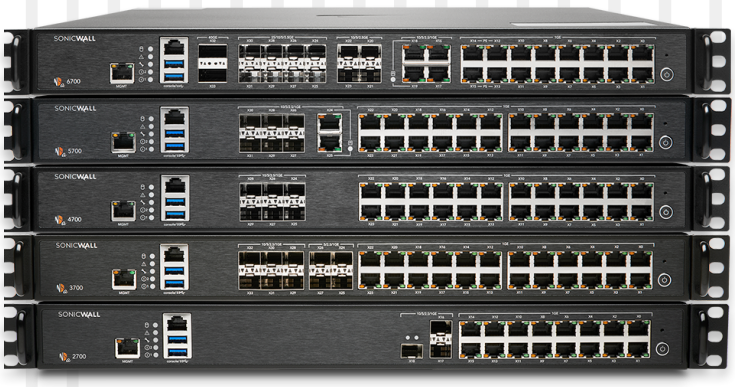
Serie SonicWall NSa Gen 7

La serie di firewall SonicWall Network Security Appliance (NSa) 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 NSa 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
- Sicurezza DNS
- Servizio di filtraggio dei contenuti (CFS 5.0) basato sulla reputazione
- Gestione firewall Wi-Fi 6
- Integrazione del controllo accessi alla rete con Aruba ClearPass
- Predisposizione per Internet edge aziendale
- Nuovo SonicOS di 7ª generazione
- Funzionalità SD-WAN sicura
- Interfaccia utente intuitiva con gestione centralizzata
- Supporto per TLS 1.3
- Eccellente rapporto prezzo/prestazioni
- Supportata dal team di ricerca delle minacce dei SonicWall Capture Labs
- Alta densità di porte per una semplice connettività di rete
- Integrazione con SonicWall Switch, SonicWave Access Point e Capture Client
- Alimentazione ridondante

SCHEDA TECNICA

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.

Gen 7 – SonicOS 7 e servizi di sicurezza

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 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* Gen 7 supporta funzionalità di rete avanzate quali SD-WAN, routing dinamico, alta disponibilità ai layer 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, 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.

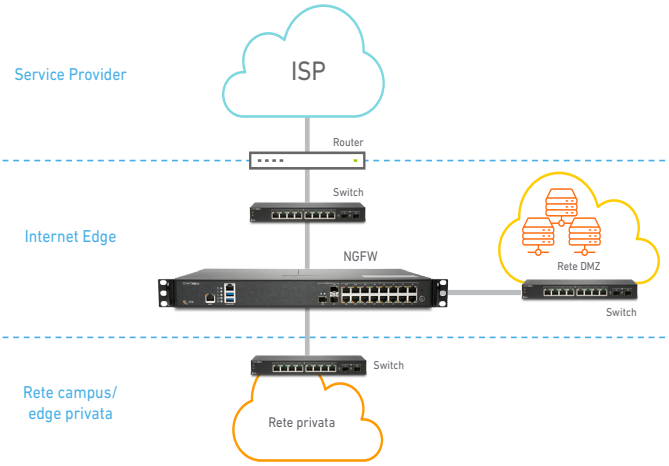
Installazione

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:

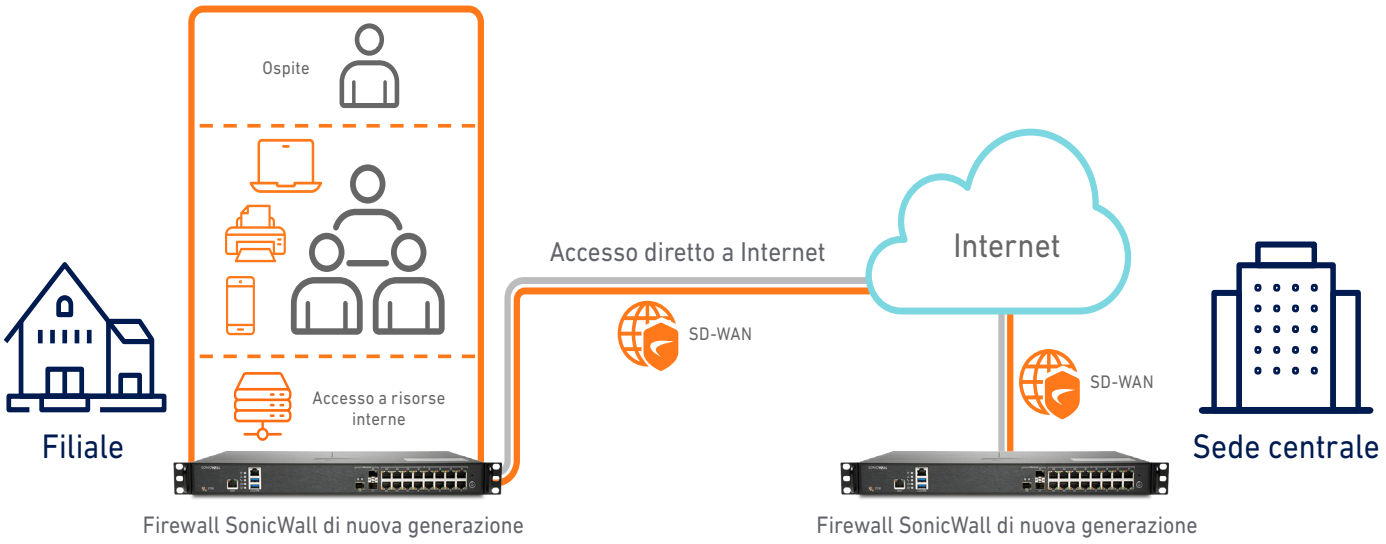
- Implementare una soluzione NGFW collaudata con il massimo livello di prestazioni e densità di porte (inclusa la connettività 40 GbE e 10 GbE) della sua categoria
- Ottenere visibilità e ispezionare il traffico crittografato, incluso quello TLS 1.3, per bloccare le minacce elusive provenienti da Internet – 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



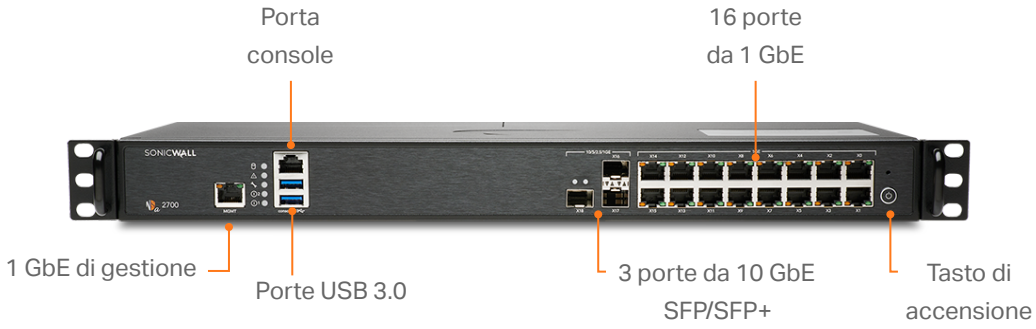
Medie imprese e aziende distribuite

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:

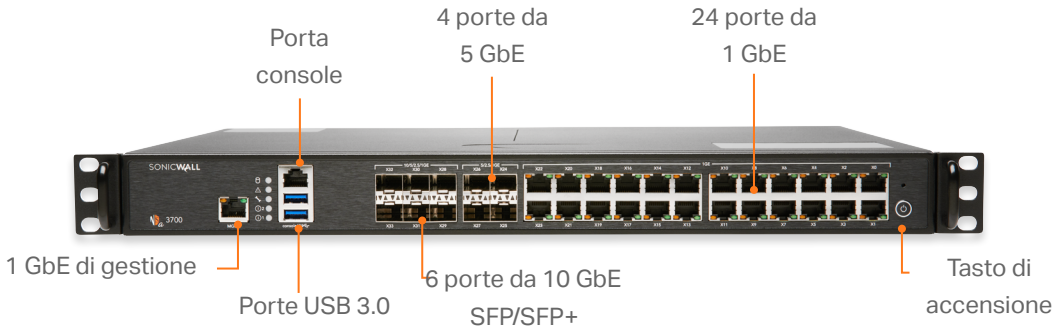
- Proteggersi dalle minacce future in continua evoluzione, investendo in un firewall NGFW con analisi delle minacce a velocità multi-gigabit
- Fornire un accesso Internet diretto e sicuro alle filiali distribuite, evitando il backhauling del traffico attraverso la sede centrale dell'azienda
- Consentire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

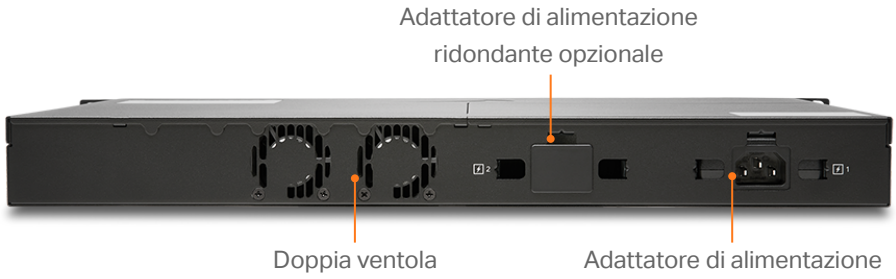


NS*a* 2700



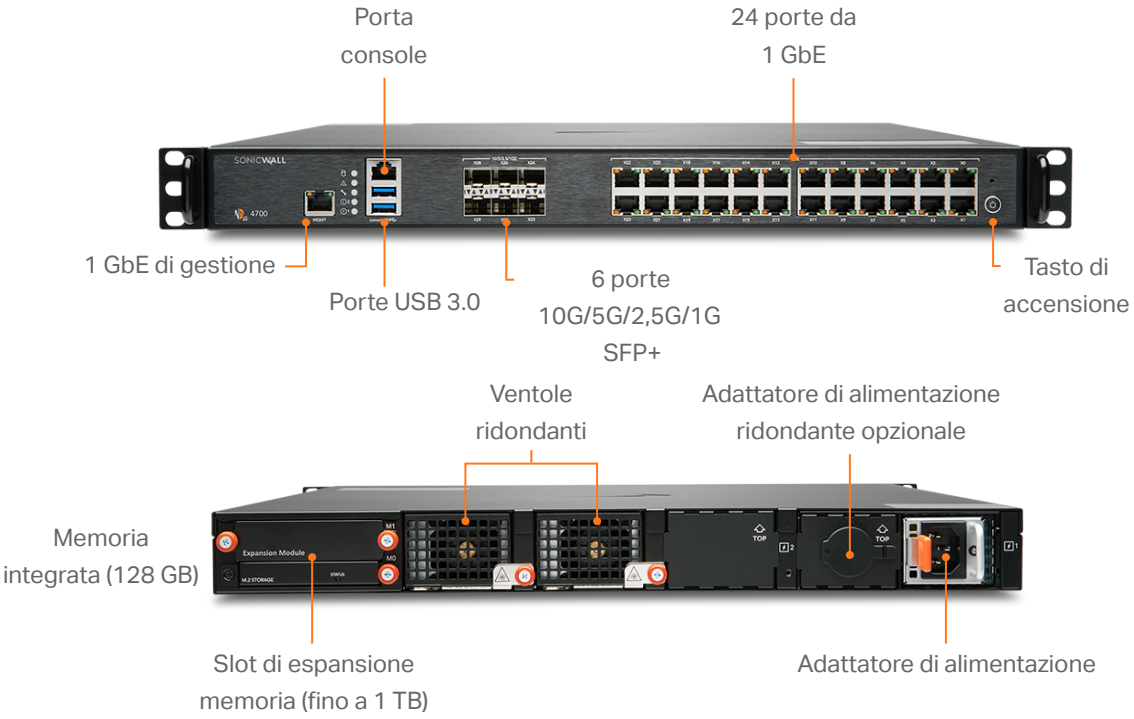
NS*a* 3700



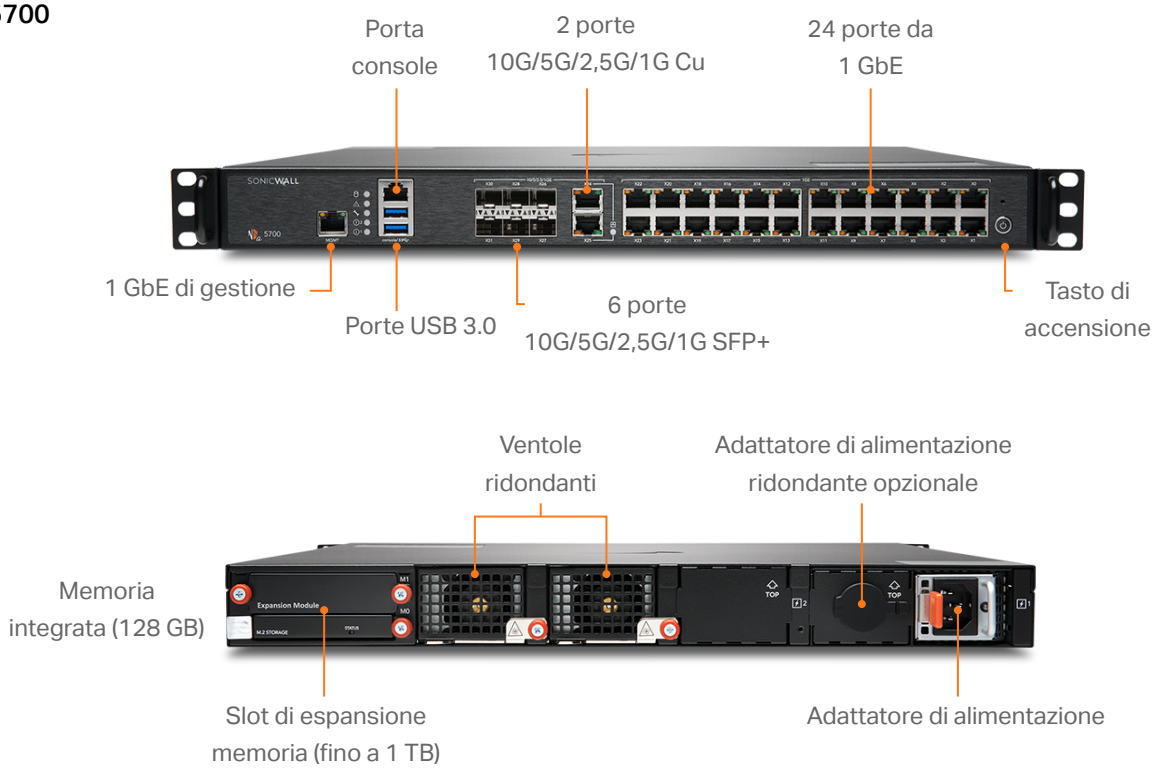


Serie SonicWall NS*a* Gen 7 (continua)

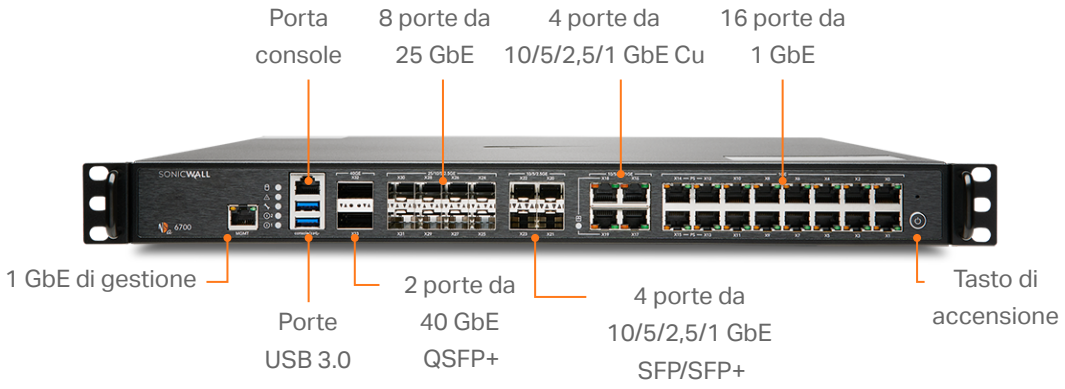
NS*a* 4700

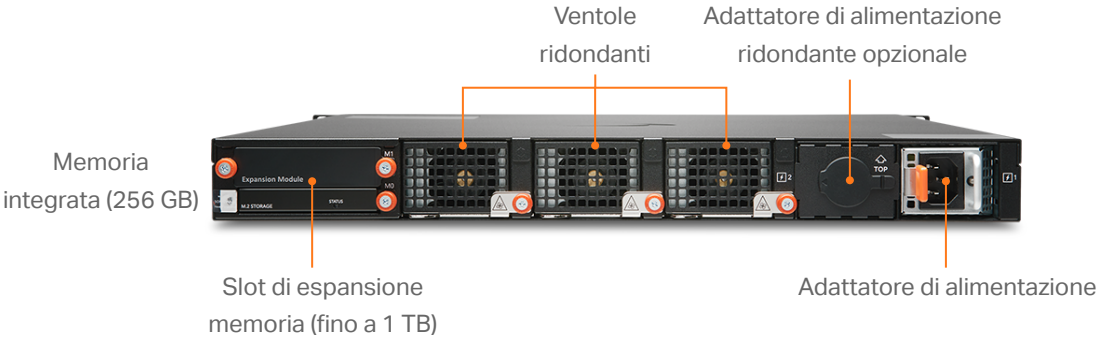


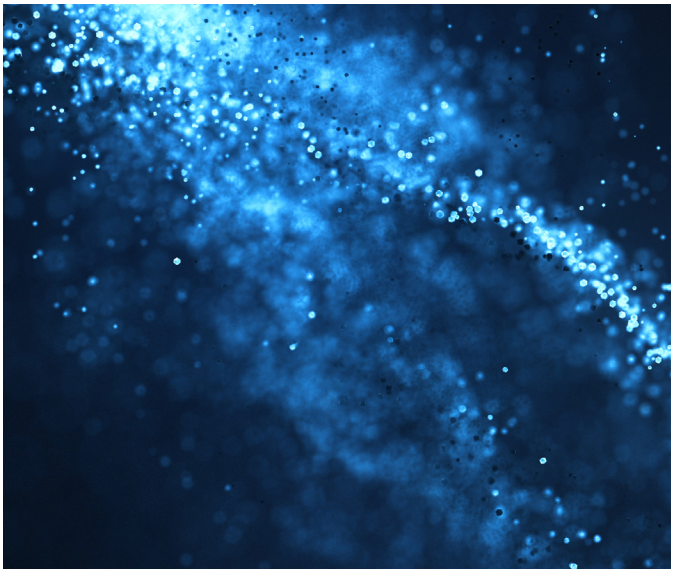
NS*a* 5700



NS*a* 6700







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

Specifiche di sistema della serie NS*a* Gen 7

Firewall	NS*a* 2700	NS*a* 3700	NS*a* 4700	NS*a* 5700	NS*a* 6700
Sistema operativo	SonicOS 7				
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	6 x 10G/5G/2,5G/ 1G (SFP+); 2x 10G/5G/2,5G/ 1G (Cu); 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
Archiviazione	64 GB M.2	128 GB M.2	128 GB	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)	Slot di espansione memoria (fino a 1 TB)
Interfacce VLAN logiche e tunnel (max.)	256	256	512	512	512
Utenti SSO	40.000	40.000	50.000	50.000	70.000
Punti di accesso supportati (max.)	512	512	512	512	512
Firewall/prestazioni VPN					
Throughput di ispezione firewall[1]	5,2 Gb/s	5,5 Gb/s	18 Gb/s	28 Gb/s	36 Gb/s
Throughput di prevenzione delle minacce[2]	3,0 Gb/s	3,5 Gb/s	9,5 Gb/s	15 Gb/s	19 Gb/s
Throughput di ispezione applicazioni[2]	3,6 Gb/s	4,2 Gb/s	11 Gb/s	18 Gb/s	20 Gb/s
Throughput IPS[2]	3,4 Gb/s	3,8 Gb/s	10 Gb/s	17 Gb/s	20 Gb/s
Throughput di ispezione anti-malware[2]	2,9 Gb/s	3,5 Gb/s	9,5 Gb/s	16 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	7 Gb/s	9 Gb/s
Throughput VPN IPSec[3]	2,10 Gb/s	2,2 Gb/s	11 Gb/s	15 Gb/s	19 Gb/s
Connessioni al secondo	21.000	22.000	115.000	228.000	228.000
Connessioni max. (SPI)	1.500.000	2.000.000	4.000.000	5.000.000	8.000.000
Connessioni max DPI-SSL	125.000	150.000	350.000	350.000	750.000
Connessioni max. (DPI)	500.000	750.000	2.000.000	3.500.000	6.000.000
VPN					
Tunnel VPN site-to-site	2.000	3.000	4.000	6.000	6.000
Client VPN IPSec (max)	50 (1000)	50 (1000)	500 (3000)	2000 (4000)	2000 (6000)
Licenze VPN SSL (max)	2 (500)	2 (500)	2 (1000)	2 (1500)	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 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 del 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				

Specifiche di sistema della serie NS*a* Gen 7

Firewall	NS*a* 2700	NS*a* 3700	NS*a* 4700	NS*a* 5700	NS*a* 6700
Comprehensive Anti-Spam Service	Supportato				
Visualizzazione delle applicazioni	Sì				
Application Control	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, 802.1e (WMM)				
Autenticazione	LDAP (domini multipli), XAUTH/RADIUS, TACACS+, SSO, accounting Radius, NTLM, database utenti interno, 2FA, servizi Terminal, Citrix, Common Access Card (CAC)				
Database utenti locale	1000	1000	2500	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				
Conformità FIPS 140-2	Sì	Sì	In attesa di approvazione	In attesa di approvazione	In attesa di approvazione
Certificazioni	ICSA Enterprise Firewall, ICSA Antivirus, IPv6/USGv6				
Certificazioni (in corso di elaborazione)	Common Criteria NDPP Firewall con VPN 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)	3 (rimovibili)
Alimentazione	60 W	90 W	350 W	350 W	350 W
Potenza max. assorbita (W)	21,5	36,3	108,1	128,1	139,2
Alimentazione ridondante	100-240 VAC, 50-60 Hz				
Dissipazione di calore totale	73,32 BTU	123,78 BTU	368,62 BTU	436,82 BTU	474,67 BTU
Dimensioni	43 x 32,5 x 4,5 cm (16,9 x 12,8 x 1,8 in)	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)	43 x 46,5 x 4,5 cm (16,9 x 18,1 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	7,8 kg	8,1 kg
Peso RAEE	4,2 kg / 9,3 lbs	4,8 kg / 10,6 lbs	9,6 kg	9,6 kg	9,9 kg
Peso con la confezione	6,4 kg / 14,1 lbs	7 kg / 15,4 lbs	13,5 kg	13,5 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	5-95% senza condensa	0-90% relativa, senza condensa	0-90% relativa, senza condensa	0-90% relativa, senza condensa
Normative					
Numeri di modello normativi	1RK51-109	1RK52-110	1RK53-115	1RK53-116	1RK54-118
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 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.

[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.

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
- Integrazione AP SonicWall Wi-Fi 6
- Scalabilità SD-WAN
- Procedura guidata di 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
- 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
- Funzionalità per regole IPS granulari
- Identificazione tramite 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 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 HTTP/HTTPS[2]

- Filtraggio degli 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

- 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, Chrome, Android e Kindle Fire
- VPN basata sul 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
- Gatekeeper H.323 e supporto per 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

Riepilogo delle funzioni di SonicOS 7.0 (continua)

- Statistiche d'uso per policy e oggetti[1]
- Utilizzato / non utilizzato
- Attivo / non attivo
- Ricerca globale di dati statici
- Supporto di memorizzazione[1]

Gestione, monitoraggio e supporto (continua)

- Gestione memoria interna ed esterna[1]
- Supporto scheda USB WWAN (5G/LTE/4G/3G)
- Supporto Network Security Manager (NSM)
- 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 7

www.sonicwall.com/products/firewalls

SonicWall

SonicWall fornisce soluzioni di cybersecurity stabili, scalabili e senza soluzione di continuità per la nuova normalità iperdistribuita, in una realtà lavorativa in cui tutto è all'insegna del telelavoro, della mobilità e in cui la sicurezza dei dati rappresenta un elemento fondamentale. Con la sua capacità di individuare le minacce più elusive e offrendo una visibilità in tempo reale, SonicWall rende possibili economie innovative e colma le lacune della cybersecurity per aziende, enti pubblici e PMI in ogni parte del mondo. Per maggiori informazioni visitare www.sonicwall.com.

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