Serie SonicWall NS*sp* Gen 7

La serie SonicWall Network Security services platform™ (NS*sp*) è una famiglia di firewall ad alte prestazioni progettata per fornire servizi di sicurezza avanzata ad aziende di grandi dimensione, istituti di istruzione, enti pubblici e MSSP. I firewall della famiglia NSsp forniscono i massimi standard di sicurezza in tempo reale senza rallentare l'operatività aziendale. Progettati per garantire un'elevata affidabilità, sono dotati di una elevata densità di porte e interfacce a velocità multi-gigabit con le quali sono in grado di gestire milioni di connessioni alla ricerca di minacce zero-day e avanzate.

CARATTERISTICHE PRINCIPALI

Serie SonicWall NS*sp*

- Alta densità di porte
- Porte da 100 GbE
- Integrazione con sandbox on-premise e in cloud
- Interfaccia utente intuitiva con gestione centralizzata
- 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
- Throughput di prevenzione minacce oltre 80 Gb/s
- Alimentazione ridondante
- Throughput di ispezione firewall fino a 100 Gb/s
- Supporto per TLS 1.3
- Supporto di milioni di connessioni TLS simultanee
- Basso costo totale di proprietà
- Supportata dal team di ricerca delle minacce dei SonicWall Capture Labs

NS*sp* in breve Specifiche complete »

100 GbE	Fino a 100 Gbps	80 mln.
Porte	Throughput ispezione firewall	Connessioni max. (NS*sp* 15700)

Maggiori informazioni sulla serie SonicWall NS*sp* Gen 7:

sonicwall.com/NS*sp*

SCHEDA TECNICA

Firewall di classe enterprise

Man mano che le aziende evolvono, aumentano anche i dispositivi gestiti e non gestiti, le reti, i carichi di lavoro nel cloud, le applicazioni SaaS, gli utenti, la velocità di Internet e le connessioni crittografate. Un firewall che non è in grado di supportare tutte queste utenze diventa un collo di bottiglia. Un firewall deve essere un punto di forza, non un punto debole.

Le interfacce multiple a 100G/40G/25G/10G del firewall SonicWall NS*sp* consentono di gestire milioni di connessioni simultanee, crittografate e non crittografate, con una tecnologia di prevenzione delle minacce senza precedenti. Considerando che il 70% delle sessioni sono crittografate, per garantire la produttività e la sicurezza delle informazioni è fondamentale disporre di un firewall in grado di elaborare ed esaminare questo traffico senza compromettere l'esperienza d'uso.

Le policy unificate di NS*sp* 15700 permettono alle aziende di creare policy di accesso e sicurezza da un'unica interfaccia in modo semplice e intuitivo.

Gestione e reportistica semplificate

La gestione, il monitoraggio e il reporting continuo delle attività di rete sono gestiti tramite il Network Security Manager di SonicWall, che offre un pannello di controllo intuitivo per gestire le operazioni dei firewall e fornire report storici, il tutto da un'unica fonte. Le procedure semplificate di installazione e configurazione e la facilità di gestione consentono alle aziende di ridurre il costo totale di proprietà e ottenere un elevato ritorno sull'investimento.

Implementazione

Next-Generation Firewall (NGFW)

- Gestione da un unico pannello di controllo
- NS*sp* si integra con il resto dell'ecosistema di soluzioni SonicWall
- Piena visibilità sulla rete per monitorare il comportamento di applicazioni, dispositivi e utenti, in modo da applicare policy ed eliminare le minacce e i colli di bottiglia della larghezza di banda
- Integrazione con Capture ATP e il brevettato RTDMI per le sandbox basate su cloud o con Capture Security Appliance per il rilevamento di malware on-premise

Ispezione Deep Packet del traffico SSL/TLS (DPI-SSL) per rilevare minacce nascoste

- I firewall NS*sp* consentono di ispezionare milioni di connessioni TLS/SSL ed SSH crittografate simultanee, indipendentemente dalla porta o dal protocollo
- Le regole di inclusione ed esclusione consentono di personalizzare i controlli in base a requisiti di conformità specifici dell'azienda e/o legali
- Supporto di suite di cifratura fino a TLS 1.3

Segmentazione e connettività di rete

- Funzionamento su diverse reti segmentate, ambienti cloud o servizi definiti con modelli, policy e gruppi di dispositivi univoci per diversi dispositivi e tenant
- Gli MSSP possono anche supportare più clienti con un servizio clean pipe e policy univoche

Firewall multi-istanza (solo per NS*sp* 15700)

- La multi-istanza è la nuova generazione della multi-tenancy
- Ogni tenant è isolato con risorse di calcolo dedicate per evitare l'esaurimento delle risorse
- Dispone di porte e tenant fisici e logici
- Supporta la gestione di policy e configurazioni indipendenti per i tenant
- Sfrutta l'indipendenza dalle versioni e il supporto ad alta disponibilità (HA) per i tenant

Funzioni in modalità Wire

- Modalità Bypass per integrare i firewall hardware in una rete rapidamente e quasi senza interruzioni
- Modalità Inspect per estendere la modalità Bypass senza modificare la funzionalità del percorso dei pacchetti a basso rischio e zero latenza
- Modalità Secure per interporre attivamente i processori multi-core del firewall nel percorso di elaborazione dei pacchetti
- Modalità Tap per acquisire un flusso di pacchetti in mirroring attraverso un'unica porta switch sul firewall, eliminando la necessità di un inserimento fisico intermedio

Protezione contro le minacce avanzate

- SonicWall Capture Advanced Threat Protection™ (ATP), utilizzato da oltre 150.000 clienti nel mondo in diverse soluzioni, permette di scoprire e bloccare più di 1.200 nuove forme di malware ogni giorno lavorativo
- NS*sp* si integra con Capture Security appliance per rilevare e bloccare minacce sconosciute tramite una sandbox on-premise che usa la tecnologia Real-Time Deep Memory Inspection™ (RTDMI).

Piattaforma Capture Cloud

- La piattaforma Capture Cloud di SonicWall offre la prevenzione delle minacce basata sul cloud e la gestione della rete, oltre a funzionalità di reporting e analisi, per organizzazioni di qualsiasi dimensione.

Servizi di filtraggio dei contenuti

- Verifica dei siti web richiesti a fronte di un imponente database nel cloud che contiene milioni di URL, indirizzi IP e siti web classificati.
- Creazione e applicazione di policy che autorizzano o negano l'accesso ai siti in base all'identità individuale o di gruppo, o all'ora del giorno.
- Il filtraggio dei contenuti basato sulla reputazione (CFS 5.0) consente di applicare policy sull'uso di Internet e di controllare l'accesso interno a contenuti web inappropriati, improduttivi e potenzialmente illegali grazie al

filtraggio completo dei contenuti di 93 categorie web. Il filtraggio dei contenuti basato sulla reputazione fornisce un punteggio di reputazione che prevede il rischio di sicurezza di un URL.

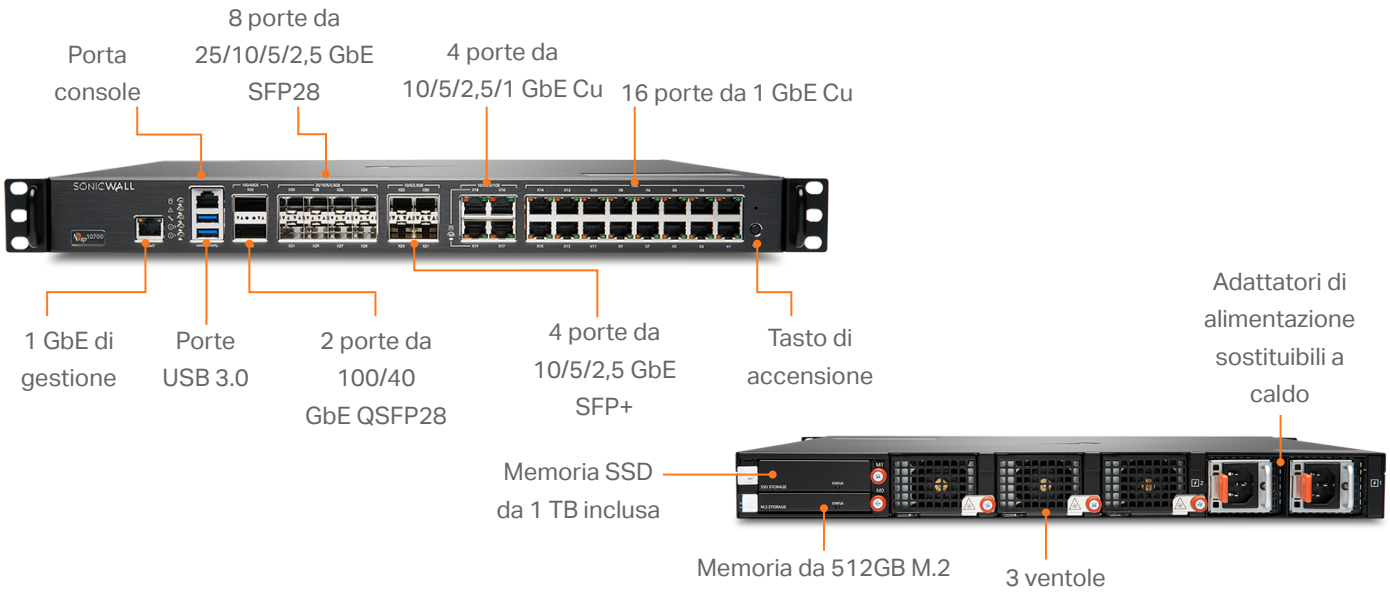
Sistema di prevenzione delle intrusioni (IPS)

- Offre un motore di ispezione approfondita dei pacchetti configurabile e ad alte prestazioni per la protezione estesa dei principali servizi di rete, come navigazione Web, posta elettronica, trasferimento di file, servizi Windows e DNS
- Progettato per fornire protezione dalle vulnerabilità delle applicazioni e da worm, trojan, spyware e backdoor exploit
- Il linguaggio estensibile delle firme consente una difesa proattiva nei confronti delle vulnerabilità scoperte di recente in applicazioni e protocolli.
- SonicWall IPS elimina i lunghi e costosi interventi di manutenzione e aggiornamento delle firme per i nuovi attacchi grazie all'architettura leader del settore Distributed Enforcement Architecture (DEA) di SonicWall

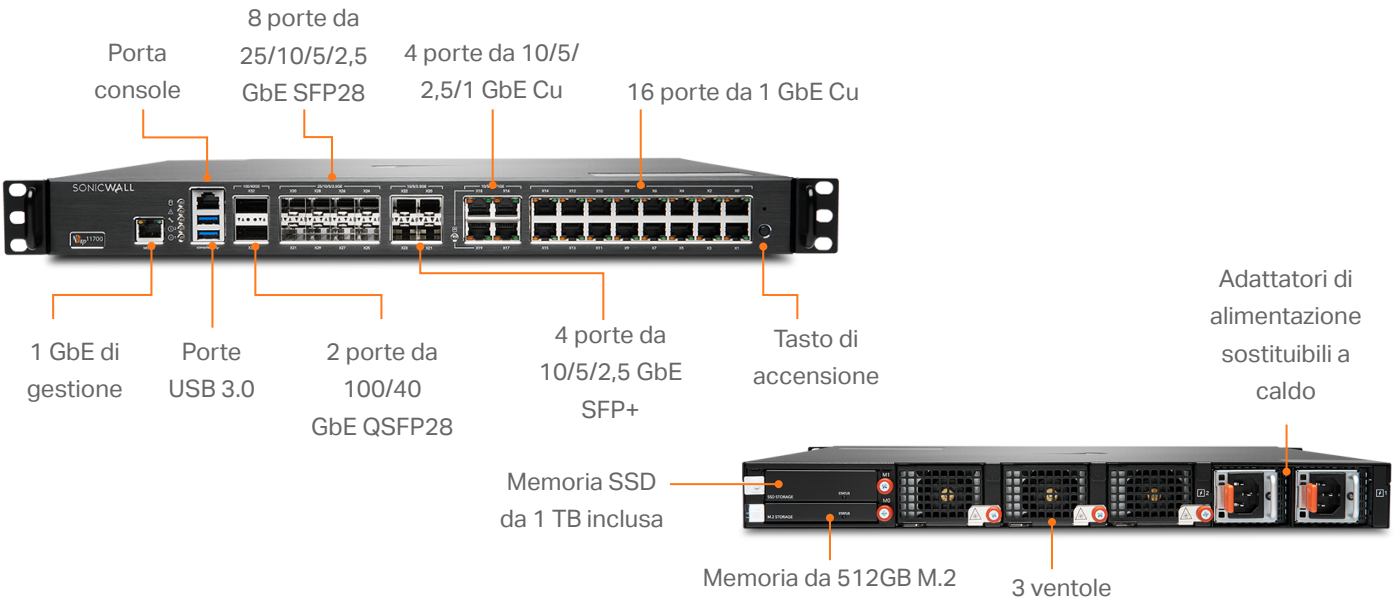
IoT e controllo delle applicazioni

- NS*sp* cataloga migliaia di applicazioni tramite il controllo delle applicazioni e monitora il loro traffico per rilevare comportamenti anomali

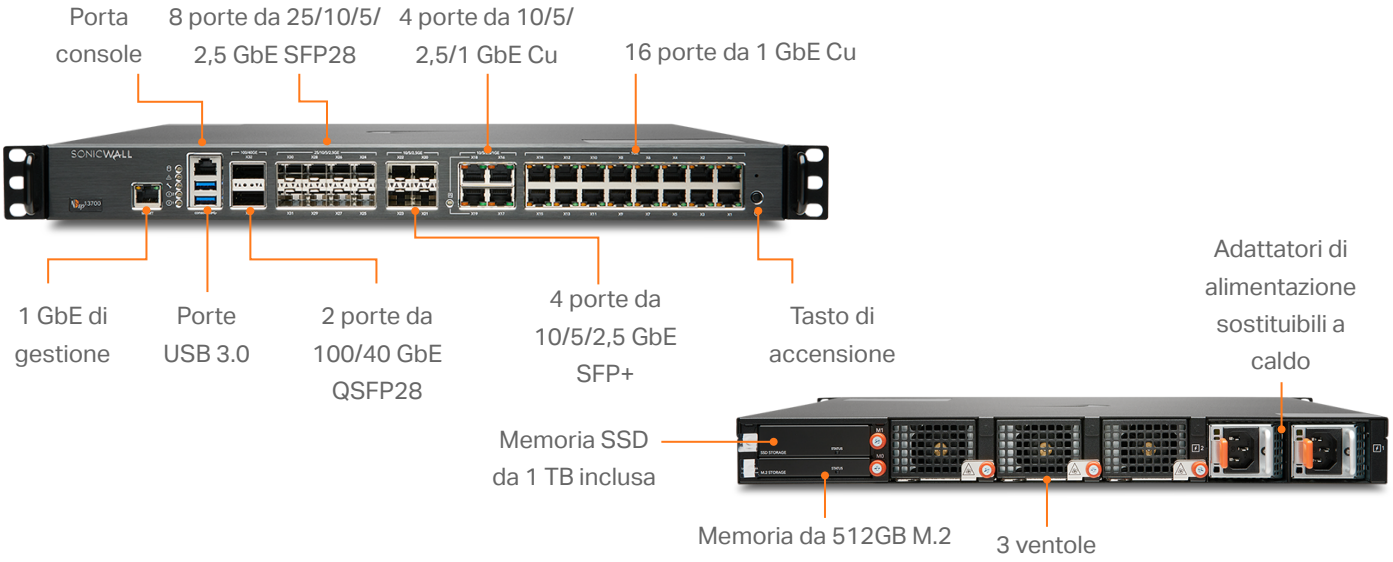
NS*sp* 10700



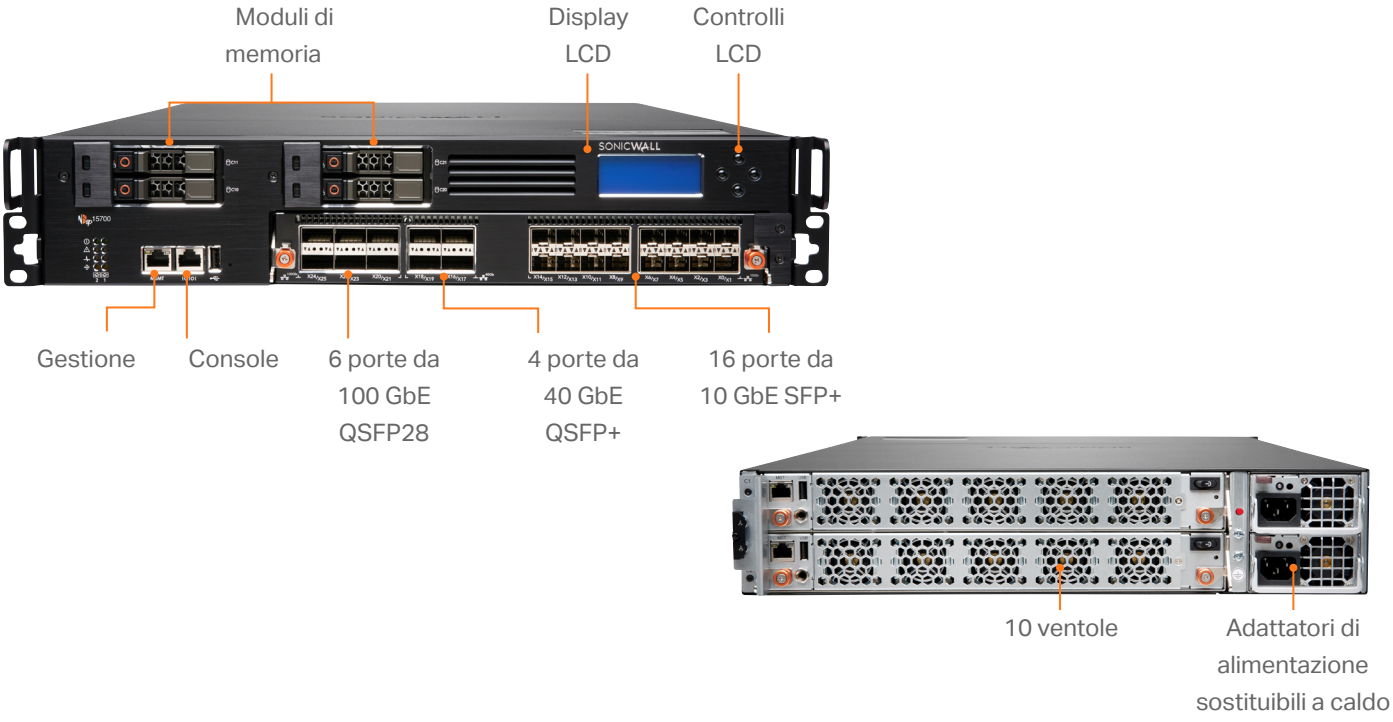
NS*sp* 11700



NS*sp* 13700



NS*sp* 15700



Specifiche tecniche della serie SonicWall NS*sp*

Firewall in generale	NS*sp* 10700	NS*sp* 11700	NS*sp* 13700	NS*sp* 15700
Sistema operativo	SonicOS 7.0.1	SonicOS 7.0.1	SonicOS 7.0.1	SonicOSX 7.0.1
Interfacce	2x100/40 GbE QSFP28, 8x25/10/5/2,5 GbE SFP28 4x10G/5G/2,5G/1G (SFP+), 4 x 10G/5G/2,5G/1G (Cu); 16 x 1GbE (Cu) 2 USB 3.0, 1 Console, 1 porta di gestione	2x100/40 GbE QSFP28, 8x25/10/5/2,5 GbE SFP28 4x10G/5G/2,5G/1G (SFP+), 4 x 10G/5G/2,5G/1G (Cu); 16 x 1GbE (Cu) 2 USB 3.0, 1 Console, 1 porta di gestione	2x100/40 GbE QSFP28, 8x25/10/5/2,5 GbE SFP28, 4x10/5/2,5 GbE SFP+, 4x10/5/2,5/1 GbE Cu, 16x1 GbE 2 USB 3.0, 1 console, 1 porta gestione	6 x 100 GbE QSFP28, 4 x 40 GbE QSFP+, 16 x 10 GbE SFP+ 3 USB 3.0, 1 Console, 1 porta di gestione
Memoria totale	1,5 TB	1,5 TB	1,5 TB	2 SSD da 480 GB
Gestione	CLI, SSH, Web UI, API REST			
Utenti SSO	100.000			
Access point supportati (max.)	512	512	512	512
Logging	Analytics, registro locale, Syslog, IPFIX, NetFlow			

Firewall/prestazioni VPN	NS*sp* 10700	NS*sp* 11700	NS*sp* 13700	NS*sp* 15700
Throughput di ispezione firewall[1]	42 Gb/s	47 Gb/s	60 Gb/s	105 Gb/s
Throughput di prevenzione delle minacce[2]	28 Gb/s	37 Gb/s	45,5 Gb/s	82 Gb/s
Throughput di ispezione applicazioni[2]	30 Gb/s	44 Gb/s	57 Gb/s	86 Gb/s
Throughput IPS[2]	28 Gb/s	37 Gb/s	48 Gb/s	76,5 Gb/s
Throughput con decrittazione e ispezione TLS/SSL (SSL DPI)[2]	10 Gb/s	11,5 Gb/s	16,5 Gb/s	21 Gb/s
Throughput VPN[3]	22,5 Gb/s	26,7 Gb/s	29 Gb/s	32 Gb/s
Connessioni al secondo	280.000	280.000	280.000	800.000
Connessioni max. (SPI)	15.000.000	20.000.000	25.000.000	40.000.000
Connessioni max. (DPI)	12.000.000	17.000.000	22.000.000	40.000.000
Connessioni max. (DPI SSL)	1.500.000	1.750.000	2.000.000	4.000.000

VPN	NS*sp* 10700	NS*sp* 11700	NS*sp* 13700	NS*sp* 15700
Tunnel VPN site-to-site	6.000	12.000	12.000	25.000
Client VPN IPSec (max)	2000 (6000)	2000 (6000)	2.000 (6.000)	2.000 (10.000)
Licenze VPN SSL (max)	100 (3000)	100 (3000)	100 (3000)	256 (3000)
Autenticazione/crittografia	DES, 3DES, AES (128, 192, 256 bit)/MD5, SHA (1.256.384.512), crittografia Suite B		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 su VPN, attraversamento NAT con IPSec, gateway VPN ridondante, VPN basata su routing			
Piattaforme client della VPN globale supportate	Microsoft® Windows 11, Windows 10 a 32/64 bit			
NetExtender	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, Google® Android™, Kindle Fire, Chrome, Windows 8.1 (incorporato)			

Connettività di rete	NS*sp* 10700	NS*sp* 11700	NS*sp* 13700	NS*sp* 15700
Firewall multi-istanza	N/D	N/D	N/D	Tenant massimi per hardware: 12
Assegnazione indirizzo IP	Statica (DHCP, PPPoE, L2TP e client PPTP), server DHCP interno, DHCP relay			
Modalità NAT	1:1, many:1, 1:many, NAT flessibile (IP sovrapposti), PAT, modalità trasparente			

Specifiche tecniche della serie SonicWall NS*sp*

Connettività di rete	NS*sp* 10700	NS*sp* 11700	NS*sp* 13700	NS*sp* 15700
Interfacce VLAN logiche e tunnel (max.)	1024			
Modalità Wire	–	–	–	Sì
Protocolli di routing	BGP4, OSPF, RIPv1/v2, route statici, routing basato su policy	BGP4, OSPF, RIPv1/v2, route statici, routing basato su policy	BGP4, OSPF, RIPv1/v2, route statici, routing basato su policy	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, 802.1p (WMM)			
Autenticazione	LDAP (domini multipli), XAUTH/RADIUS, TACACS+, SSO, accounting Radius, NTLM, database utenti interno, 2FA, servizi Terminal, Citrix, Common Access Card (CAC)		LDAP (domini multipli), XAUTH/RADIUS, SSO, Novell, database utenti interno, Terminal Services, Citrix, Common Access Card (CAC)	
Database utenti locale	4.000	4.000	4.000	5.000
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	In attesa	In attesa	In attesa	Sì
Certificazioni	ICSA Enterprise Firewall, ICSA Antivirus, IPv6/USGv6			
Certificazioni (in corso)	Common Criteria NDPP Firewall con VPN e IPS			
Alta disponibilità	Attiva/Passiva con sincronizzazione dello stato			

Hardware	NS*sp* 10700	NS*sp* 11700	NS*sp* 13700	NS*sp* 15700
Alimentazione	2x350 W	2x350 W	2x350 W	Doppia, ridondante, 1.200 W
Ventole	3 (rimovibili)	3 (rimovibili)	3 (rimovibili)	10
Alimentazione ridondante	100-240 VAC, 50-60 Hz			
Potenza max. assorbita (W)	155,3	155,3	181,2	834,4
Dissipazione di calore totale	529,57 BTU	529,57 BTU	617,89 BTU	2845,3 BTU
Fattore di forma	1U rack-mount	1U rack-mount	1U rack-mount	2U rack-mount
Dimensioni	43 x 46 x 4,5 cm (16,9 x 18,1 x 1,8 in)	43 x 46 x 4,5 cm (16,9 x 18,1 x 1,8 in)	43 x 46 x 4,5 cm (16,9 x 18,1 x 1,8 in)	68,6 x 43,8 x 8,8 cm
Peso	9,1 kg	9,1 kg	9,1 kg	26 kg
Peso RAEE	11 kg	11 kg	11 kg	30,1 kg
Peso con la confezione	14,9 kg	14,9 kg	14,9 kg	37,3 kg
Condizioni ambientali (in funzionamento/stoccaggio)	0-40 °C (32-105 °F) / da -40 a 70 °C (da -40 a 158 °F)			
Umidità	0-90% relativa, senza condensa	0-90% relativa, senza condensa	0-90% relativa, senza condensa	10-95% senza condensa
Normative	**NS*sp* 10700**	**NS*sp* 11700**	**NS*sp* 13700**	**NS*sp* 15700**
Numeri di modello normativi	1RK54-118	1RK54-119	1RK54-118	2RK05-0FE
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	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	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	FCC Class A, ICES Classe A, CE (EMC Classe A, LVD, RoHS), C-Tick, VCCI Classe A, MSIP/KCC Classe A, UL, cUL, TÜV/GS, CB, notifica DGN 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 funzionalità SonicOSX e SonicOS

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
- API REST
- Integrazione switch SonicWall
- Integrazione AP SonicWall Wi-Fi 6

Policy di sicurezza unificata

- La policy unificata abbina le regole dei livelli 4 e 7:
  - IP/porta/servizio di origine/destinazione
  - Application Control
  - Filtraggio CFS/Web
  - Applicazione dei servizi di sicurezza Single Pass
  - IPS/GAV/AS/Capture ATP
- Gestione delle regole:
  - Clonazione
  - Analisi di regole nascoste
  - Modifica nelle celle
  - Modifica di gruppi
- Gestione delle viste
  - Regole utilizzate/non utilizzate
  - Regole attive/inattive
  - Sezioni

Decrittazione e ispezione TLS/SSL/SSH

- TLS 1.3
- Deep Packet Inspection per TLS/SSL/SSH
- Inclusione/esclusione di oggetti, gruppi o nomi host
- Controllo SSL
- Controlli DPI-SSL granulari basati su zone o regole
- Policy di decrittazione per SSL/TLS e SSH

Capture Advanced Threat Protection[1]

- Real-Time Deep Memory Inspection
- Analisi multi-engine basata sul cloud
- 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
- Blocco fino al verdetto
- Integrazione con Capture Client

Prevenzione delle intrusioni[1]

- 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[1]

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

Identificazione delle applicazioni[1]

- 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[1]

- 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
- Content Filtering Client

VPN

- 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

- Firewall multi-istanza (solo su NS*sp* 15700)
- PortShield
- Frame Jumbo
- Indagine del percorso MTU
- Registrazione avanzata
- VLAN trunking
- Mirroring delle porte
- QoS livello 2
- Sicurezza delle porte
- Routing dinamico (RIP/OSPF/BGP)
- Routing basato su policy (ToS/metrico ed ECMP)
- NAT
- Server DHCP
- Gestione della larghezza di banda
- Aggregazione dei link (statica e dinamica)
- Ridondanza delle porte
- Alta disponibilità A/P con sincronizzazione dello stato
- Bilanciamento del carico in ingresso/in uscita
- Alta disponibilità - Attiva/Standby con sincronizzazione dello stato
- Modalità Wire/Virtual wire, Tap, NAT
- Routing asimmetrico

VoIP

- Controllo QoS granulare
- Gestione della larghezza di banda
- DPI per il traffico VoIP
- Gatekeeper H.323 e supporto per proxy SIP

Gestione e monitoraggio

- GUI Web
- CLI (Command Line Interface)
- Registrazione e provisioning zero-touch
- API Rest

Gestione e monitoraggio (continua)

- Supporto app mobile SonicExpress
- SNMPv2/v3
- Gestione e reportistica centralizzate con SonicWall Network Security Manager (NSM)[1]
- Logging
- Esportazione per Netflow/IPFix
- Backup della configurazione basato su cloud
- Visualizzazione della larghezza di banda e delle applicazioni
- Gestione IPv4 e IPv6

[1] Richiede un abbonamento aggiuntivo

Trovate il firewall SonicWall giusto per la vostra azienda

www.sonicwall.com/firewalls

SonicWall

SonicWall fornisce soluzioni di cybersecurity stabili, scalabili e trasparenti 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 possibile economie innovative e colma le lacune della cybersecurity per aziende, enti pubblici e PMI in ogni parte del mondo. Per maggiori informazioni potete visitare www.sonicwall.com.

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