

Datasheet

SonicWall NSsp™ 15700

La SonicWall Network Security services platform™ (NSsp) 15700 è un firewall di prossima generazione con un elevato numero di porte ed interfacce con velocità multi-gig, in grado di elaborare diversi milioni di connessioni per le minacce zero-day e avanzate. Progettato per le grandi aziende, le università, gli enti pubblici e i fornitori di servizi di sicurezza gestiti (MSSP), blocca gli attacchi in tempo reale senza penalizzare le prestazioni. È stato concepito in funzione della massima affidabilità e della fornitura ininterrotta di servizi alle organizzazioni.

Firewall di livello aziendale ad alta velocità

Man mano che le aziende si evolvono di pari passo con un incremento dei dispositivi gestiti e non, delle reti, dei carichi di lavoro dei cloud, delle applicazioni SaaS, degli utenti, della velocità di Internet e delle connessioni crittografate, un firewall che non fosse in grado di soddisfare tutte queste esigenze costituirebbe un collo di bottiglia per i sistemi informatici. I firewall dovrebbero essere un punto di forza e non un anello debole.

Le interfacce multiple 100G/40G/10G di SonicWall NSsp 15700 consentono di elaborare diversi milioni di connessioni

simultanee crittografate o meno, con una tecnologia di prevenzione delle minacce che non conosce rivali. Dal momento che il 70% di tutte le sessioni è crittografato, poter contare su un firewall in grado di elaborare ed esaminare un simile traffico senza interferire con l'operatività dell'utente finale è essenziale per la produttività e la sicurezza delle informazioni.

L'interfaccia delle politiche unificate di NSsp 15700 consente alle organizzazioni di semplificare e creare intuitivamente politiche di accesso e di sicurezza in un'unica interfaccia unificata.

Gestione e reportistica semplificate

La gestione corrente, il monitoraggio e la reportistica delle attività di rete sono gestite tramite SonicWall Network Security Manager (imminente), che mette a disposizione un pannello di controllo intuitivo per la gestione del funzionamento del firewall e report storici, il tutto da un'unica fonte. Le procedure semplificate di installazione e configurazione e la facilità di gestione consentono alle organizzazioni di ridurre il costo totale della proprietà e di ottenere un elevato ritorno sull'investimento.



Vantaggi di SonicWall NSsp 15700:

- Elevato numero di porte
- Porte da 100 GbE
- Firewall multi-istanza
- Si integra con i servizi di sandboxing interni e nel cloud
- Compatibilità SD-Branch
- Gestione da un unico pannello di controllo tramite cloud o firewall
- Memoria integrata ed espandibile
- Alimentazione ridondante
- Supporto SonicOSX 7.0
- Supporto TLS 1.3
- Supporta milioni di connessioni TLS contemporanee
- Basso costo totale di proprietà

Installazione

Firewall di prossima generazione (NGFW)

- Gestito da un unico pannello di controllo
- NSsp 15700 si integra con il resto dell'ecosistema di soluzioni SonicWall
- Visibilità completa della rete per controllare che cosa fanno le applicazioni, i dispositivi e gli utenti per attuare le politiche ed eliminare le minacce e i colli di bottiglia della larghezza di banda
- Integrazione con Capture ATP con RTDMI per sandboxing basato su cloud o Capture Security appliance per il rilevamento interno del malware

Ispezione dei pacchetti profondi SSL/TLS (DPI-SSL) per evidenziare le minacce nascoste

- NSsp 15700 consente l'ispezione simultanea di diversi milioni di connessioni TLS/SSL e SSH crittografate indipendentemente dalla porta e dal protocollo
- Le regole di inclusione e di esclusione consentono la personalizzazione in base ai requisiti di conformità e/o legali specifici delle organizzazioni
- Supporto per suite di cifratura TLS fino a TLS 1.3

Segmentazione e connettività di rete

- Funzionamento su diverse reti segmentate, cloud e definizioni di servizi con modelli, gruppi di dispositivi e politiche esclusivi su più dispositivi e tenant
- MSSPs può anche supportare più clienti con una clean pipe e politiche esclusive

Firewall multi-istanza

- La multi-istanza è la prossima generazione della multi-tenancy
- Ogni tenant è isolato con risorse informatiche dedicate per evitare l'esaurimento delle risorse
- Dispone di porte e tenant fisici e logici
- Supporta politiche tenant indipendenti e la gestione della configurazione
- Sfrutta l'indipendenza dalle versioni e il supporto di disponibilità elevata (HA) per i tenant

Funzione in modalità Wire

- Modalità Bypass per inserire rapidamente e praticamente senza interruzioni i firewall hardware nelle reti
- Modalità Inspect per estendere la modalità Bypass senza modificare funzionalmente il percorso dei pacchetti a basso rischio e latenza zero
- Modalità Secure per interporre attivamente i processori multi-core del firewall nel percorso di elaborazione dei pacchetti
- Modalità Tap per acquisire uno stream di pacchetti mirrored attraverso un'unica porta switch sul firewall, eliminando l'esigenza di inserimento fisico intermediato

Protezione avanzata contro le minacce

- SonicWall Capture Advanced Threat Protection™ (ATP) viene utilizzata da oltre 150.000 clienti nel mondo attraverso tutta una serie di soluzioni e aiuta a scoprire e bloccare più di 1.200 nuove forme di malware per ogni giorno lavorativo
- Per i clienti con esigenze di conformità e di prestazioni, NSsp 15700 si integra con Capture Security appliance (CSa), un dispositivo locale che utilizza Real-Time Deep Memory Inspection™ (RTDMI), una tecnologia di analisi dei file in memoria.

Capture Cloud Platform

- Capture Cloud Platform di SonicWall offre la prevenzione delle minacce basata sul cloud e la gestione della rete oltre a funzionalità di reportistica 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 valutati.
- Definizione e attuazione di politiche che consentano o neghino l'accesso ai siti in base all'identità individuale o di gruppo, o all'ora del giorno, per più di 50 categorie predefinite

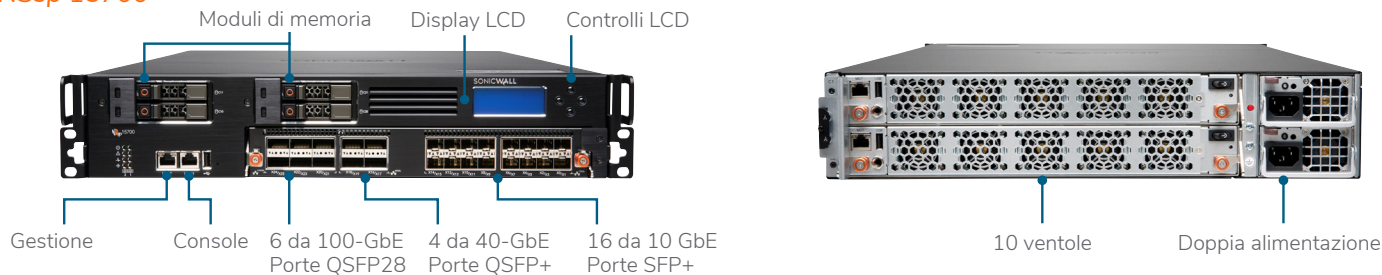
Intrusion Prevention System (IPS)

- Mette a disposizione un engine di ispezione dei pacchetti profondi di prestazioni elevate per la protezione estesa dei principali servizi di rete, come Internet, posta elettronica, trasferimento file, servizi Windows e DNS
- Progettato per la protezione dalle vulnerabilità delle applicazioni e da worm, trojan ed exploit peer-to-peer, spyware e backdoor
- Il linguaggio di signature estensibile consente una difesa anticipata nei confronti delle applicazioni e delle vulnerabilità dei protocolli scoperti di recente.
- SonicWall IPS consente di evitare gli oneri in termini di costi e di tempi legati al mantenimento e all'aggiornamento delle signature dei nuovi attacchi tramite l'architettura leader industriale Distributed Enforcement Architecture (DEA) di SonicWall

Internet delle cose e controllo delle applicazioni

- NSsp 15700 cataloga migliaia di applicazioni tramite App Control e ne effettua il monitoraggio del traffico per individuare comportamenti anomali tramite il firewall delle applicazioni integrato
- Segmento gestito da dispositivi non gestiti con profili di gestione e accesso esclusivi

NSsp 15700



Specifiche di SonicWall NSsp 15700

| CARATTERISTICHE GENERALI DEI FIREWALL | NSsp 15700 |
|---|---|
| Sistema operativo | SonicOSX 7 |
| Interfacce | 6 QSFP28 da 100-GbE, 4 QSFP+ da 40-GbE, 16 SFP+ da 10 GbE |
| Archiviazione integrata | 2 SSD da 480 GB |
| Gestione | CLI, SSH, Web UI, API REST |
| Utenti SSO | 100.000 |
| Accesso | Analyzer, Local Log, Syslog, IPFIX, NetFlow |
| FIREWALL/PRESTAZIONI VPN | NSsp 15700 |
| Throughput di ispezione del firewall | 105 Gbps |
| Throughput di prevenzione delle minacce | 82 Gbps |
| Throughput di ispezione delle applicazioni | 86 Gbps |
| Throughput IPS | 76,5 Gbps |
| Throughput IMIX | 28,5 Gbps |
| Throughput con decrittazione e ispezione (SSL DPI) | 21 Gbps |
| Throughput VPN | 32 Gbps |
| Connessioni al secondo | 800k |
| Numero massimo di connessioni (SPI) | 80M |
| Numero massimo di connessioni (DPI) | 50M |
| Numero massimo di connessioni (SSL DPI) | 3M |
| VPN | NSsp 15700 |
| Tunnel VPN da sede a sede | 25.000 |
| Client VPN IPSec (max) | 2.000 (10.000) |
| Client VPN SSL NetExtender (numero massimo) | 2 (3.000) |
| Crittografia/autenticazione | DES, 3DES, AES (128, 192, 256 bit), MD5, SHA-1, crittografia Suite B |
| Scambio chiavi | Gruppi Diffie-Hellman 1, 2, 5, 14v |
| VPN basata su routing | RIP, OSPF, BGP |
| 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 | Microsoft® Windows Vista 32/64-bit, Windows 7 32/64-bit, Windows 8.0 32/64-bit, Windows 8.1 32/64-bit, Windows 10 |
| NetExtender | Microsoft Windows Vista 32/64-bit, Windows 7, Windows 8.0 32/64-bit, Windows 8.1 32/64-bit, Mac OS X 10.4+, Linux FC3+/Ubuntu 7+/OpenSUSE |
| Mobile Connect | Apple® iOS, Mac OS X, Google® Android™, Kindle Fire, Chrome, Windows 8.1 (incorporato) |
| CONNETTIVITÀ DI RETE | NSsp 15700 |
| Firewall multi-istanza | Numero massimo di tenant 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 |
| Interfacce VLAN | 512 |
| Modalità Wire | Sì |
| Protocolli di routing | BGP, OSPF, RIPv1/v2, static route, routing basato sulle politiche |

Specifiche di SonicWall NSsp 15700

| | |
|--|--|
| Qualità del servizio (QoS) | Priorità della larghezza di banda, larghezza di banda massima, larghezza di banda garantita, contrassegno DSCP, 802.1p |
| Autenticazione | LDAP, XAUTH/RADIUS, SSO, Novell, database utenti interno, Terminal Services, Citrix |
| VoIP | H.323-v1-5 completo, SIP |
| Standard | TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3 |
| Certificazioni (in corso) | ICSA Firewall, ICSA Anti-Virus, FIPS 140-2, Common Criteria NDPP (Firewall e IPS), UC APL, USGv6, CsFC |
| Elevata disponibilità | Attivo/Passivo con sincronizzazione statica, Attivo/Attivo DPI con sincronizzazione statica, Attivo/Attivo Clustering |
| HARDWARE | NSsp 15700 |
| Alimentazione | Doppia, ridondante, 1.200W |
| Ventole | 10 |
| Alimentazione in ingresso | 100-240 Vca, 50-60 Hz |
| Potenza max assorbita (W) | 1065 |
| Fattore di forma | Montabile su rack 2U |
| Dimensioni | 68,6 x 43,8 x 8,8 cm |
| Peso | 26 kg |
| Peso RAEE | 30,1 Kg |
| Peso con la confezione | 37,3 Kg |
| Dimensioni di spedizione | 28 x 63 x 86 (cm) |
| Principali normative di conformità | FCC Classe A, ICES Classe A, CE (EMC Classe A, LVD, RoHS), C-Tick, VCCI Classe A, MSIP/KCC Classe A, UL, cUL, TUV/GS, CB, notifica UL DGN Messico, RAEE, REACH, ANATEL, BSMI |
| Condizioni ambientali (in funzionamento/ stoccaggio) | 0-40 °C / - 40 - 70 °C |
| Umidità | 10-95%, non condensante |

Riepilogo delle funzioni di SonicOSX

Firewall

- Ispezione Stateful Packet
- Reassembly-Free Deep Packet Inspection
- Protezione da attacchi DDoS (UDP/ICMP/SYN flood)
- Supporto di IPv4/IPv6
- Autenticazione biometrica per l'accesso remoto
- Proxy DNS
- API REST
- Integrazione switch SonicWall

Politica di sicurezza unificata

- La politica unificata abbina le regole del Layer 4 a quelle del Layer 7:
 - IP/porta/servizio di origine/destinazione
 - Controllo delle applicazioni
 - Filtraggio CFS/Web
 - Attuazione dei servizi di sicurezza Single Pass
 - IPS/GAV/AS/Capture ATP
- Gestione delle regole:
 - Clonazione
 - Analisi delle regole nascoste
 - Editing nella cella
 - Editing di gruppo
- Gestione 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 di host
- Controllo SSL
- Controlli DPI SSL granulari basati su zone o regole
- Politiche di decrittazione per SSL/TLS e SSH

Capture Advanced Threat Protection²

- 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
- Intelligenza delle minacce con aggiornamenti in tempo reale
- Blocco fino al verdetto
- Integrazione Capture Client

Prevenzione delle intrusioni²

- Scansione basata sulle firme
- Aggiornamenti automatici delle firme
- Ispezione bidirezionale
- Funzionalità per regole IPS granulari
- Implementazione GeolP
- Filtraggio botnet con elenco dinamico
- Corrispondenza con espressioni regolari

Anti-malware²

- 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 applicazioni²

- Controllo delle applicazioni
- Gestione della larghezza di banda delle applicazioni
- Creazione di signature per applicazioni personalizzate
- Prevenzione della perdita di dati
- Creazione di report sulle applicazioni tramite NetFlow/IPFIX
- Ampio database di signature delle applicazioni

Visualizzazione e analisi del traffico

- Attività degli utenti
- Utilizzo applicazioni/larghezza di banda/minacce
- Analisi basate su cloud

Filtraggio dei contenuti HTTP/HTTPS Web²

- Filtraggio degli URL
- Proxy avoidance
- Blocco in base a parole chiave
- Filtraggio basato sulle politiche (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 la connettività da sede a sede
- VPN SSL e accesso remoto da 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

- Architettura multi-istanza
- PortShield
- Frame Jumbo
- Individuazione percorsi MTU
- Registrazione avanzata
- VLAN trunking
- Port mirroring
- QoS layer 2
- Sicurezza delle porte
- Routing dinamico (RIP/OSPF/BGP)
- Routing basato sulle politiche (ToS/metrico ed ECMP)
- NAT
- Server DHCP
- Gestione della larghezza di banda
- Aggregazione dei link¹ (statica e dinamica)
- Porte ridondanti¹
- Alta disponibilità A/P con sincronizzazione statica
- Clustering A/A¹
- Bilanciamento del carico in ingresso/in uscita
- Alta disponibilità – Active/Standby con sincronizzazione statica
- Modalità wire/virtual wire, modalità tap, modalità NAT
- Routing asimmetrico

VoIP

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

Gestione e monitoraggio

- GUI Web
- CLI (Command Line Interface)
- Registrazione e provisioning Zero-Touch
- Supporto app mobile SonicExpress
- SNMPv2/v3
- Gestione e reportistica centralizzate con SonicWall Global Management System (GMS)²
- Accesso
- 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

¹ Non supportato su firewall serie NSv

² Richiede un abbonamento aggiuntivo.

| Prodotto | SKU |
|---|-------------|
| SONICWALL NSSP 15700 | 02-SSC-2722 |
| ESSENTIAL GATEWAY SECURITY SUITE BUNDLE FOR NSSP 15700 1 ANNO | 02-SSC-4739 |
| ESSENTIAL GATEWAY SECURITY SUITE BUNDLE FOR NSSP 15700 3 ANNI | 02-SSC-4740 |
| ESSENTIAL GATEWAY SECURITY SUITE BUNDLE FOR NSSP 15700 5 ANNI | 02-SSC-4741 |
| 24X7 SUPPORT FOR NSSP 15700 1 ANNO | 02-SSC-4733 |
| 24X7 SUPPORT FOR NSSP 15700 3 ANNI | 02-SSC-4734 |
| 24X7 SUPPORT FOR NSSP 15700 5 ANNI | 02-SSC-4735 |

| Abbinamenti | SKU |
|---|-------------|
| SONICWALL NSSP 15700 TOTALSECURE ESSENTIAL EDITION 1 ANNO | 02-SSC-4764 |
| SONICWALL NSSP 15700 TOTALSECURE ESSENTIAL EDITION 3 ANNI | 02-SSC-4766 |
| SONICWALL NSSP 15700 TOTALSECURE ESSENTIAL EDITION 5 ANNI | 02-SSC-4765 |

| Accessori | SKU |
|---|-------------|
| 10GB-SR SFP+ SHORT REACH FIBER MODULE MULTI-MODE NO CABLE | 01-SSC-9785 |
| 10GB-LR SFP+ LONG REACH FIBER MODULE SINGLE-MODE NO CABLE | 01-SSC-9786 |
| 10GB SFP+ COPPER WITH 1M TWINAX CABLE | 01-SSC-9787 |
| 10GB SFP+ COPPER WITH 3M TWINAX CABLE | 01-SSC-9788 |
| 1GB-SX SFP SHORT HAUL FIBER MODULE MULTI-MODE NO CABLE | 01-SSC-9789 |
| 1GB-LX SFP LONG HAUL FIBER MODULE SINGLE-MODE NO CABLE | 01-SSC-9790 |
| 1GB-RJ45 SFP COPPER MODULE NO CABLE | 01-SSC-9791 |
| SONICWALL SFP+ 10GBASE-T TRANSCEIVER COPPER RJ45 MODULE | 02-SSC-1874 |

SonicWall

SonicWall fornisce soluzioni di cybersecurity illimitata per l'era iperdistribuita in una realtà lavorativa in cui tutto è all'insegna del telelavoro, della mobilità e della mancanza di sicurezza. Conoscendo l'ignoto, offrendo una visibilità in tempo reale e rendendo possibili economie innovative, SonicWall colma le lacune di cybersecurity per aziende, enti pubblici e PMI in ogni parte del mondo. Per ulteriori informazioni visitare www.sonicwall.com.