SonicWall Network Security services platform (NS*sp*) serie 12000

Protezione scalabile e all'avanguardia basata sulla potenza dell'intelligence cloud.

La piattaforma di servizi per la sicurezza di rete SonicWall della serie NS*sp* 12000 adotta un moderno approccio al rilevamento e alla prevenzione delle minacce, combinando l'intelligence nel cloud alla protezione basata su appliance in una piattaforma scalabile ad alta velocità. Progettati per grandi imprese distribuite, data center e service provider, i firewall di nuova generazione (NGFW) della serie NS*sp* utilizzano le innovative tecnologie di sicurezza con deep learning della piattaforma Capture Cloud per fornire una protezione efficace contro le minacce informatiche più avanzate senza rallentare le prestazioni.

Sicurezza per le imprese

Il volume e la sofisticazione degli odierni attacchi alla rete continuano ad aumentare. Per identificare e bloccare le minacce zero-day sconosciute e le intrusioni è necessario un approccio in grado di ampliare la protezione integrata con l'intelligence sulla sicurezza nel cloud. Senza tale intelligence nel cloud, le soluzioni di sicurezza gateway aziendali non sono in grado di rimanere un passo avanti rispetto alle complesse minacce odierne.

La serie SonicWall NS*sp* riceve le informazioni sulle minacce raccolte dal nostro team Capture Labs dedicato alla ricerca delle minacce e le combina alla protezione integrata per fornire una protezione costantemente aggiornata. Il servizio Capture Advanced Threat Protection (ATP) di SonicWall basato sul cloud utilizza la tecnologia Real-Time Deep Memory Inspection (RTDMI™) in attesa di brevetto per rilevare e bloccare in modo proattivo le minacce zero-day comuni e i malware sconosciuti mediante l'analisi diretta nella memoria. Grazie all'architettura in tempo reale, la tecnologia RTDMI di SonicWall è precisa, riduce al minimo i falsi positivi ed identifica e attenua gli attacchi sofisticati in cui le armi del malware sono esposte per meno di 100 nanosecondi. La protezione basata su cloud è ottimizzata dal motore RFDPI® (Reassembly-Free Deep Packet Inspection) a singola fase brevettato* da SonicWall, che esamina il traffico sia in entrata che in uscita sul firewall. Sfruttando la piattaforma SonicWall Capture Cloud, in aggiunta alle funzionalità integrate che includono la prevenzione delle intrusioni, funzionalità anti-malware e filtraggio Web/URL, la serie NS*sp* è in grado di fornire la prevenzione automatizzata delle violazioni in tempo reale di cui hanno bisogno le imprese.

Con l'aumento del numero di connessioni web crittografate, è essenziale che i firewall NGFW ispezionino il traffico crittografato alla ricerca di minacce nascoste. I firewall SonicWall offrono una protezione completa eseguendo decrittazione ed ispezione complete di centinaia di migliaia di connessioni TLS/SSL ed SSH crittografate, indipendentemente dalla porta o dal protocollo. Il firewall esamina ogni singolo pacchetto in profondità alla ricerca di anomalie del protocollo, minacce, zero-day, intrusioni e persino criteri definiti. Il motore d'ispezione Deep Packet rileva e previene gli attacchi nascosti che sfruttano la crittografia, blocca il download di malware crittografato, interrompe la diffusione di infezioni e le comunicazioni di comando e controllo (C&C) e la fuoriuscita dei dati. Le regole di inclusione ed esclusione consentono un controllo totale per la personalizzazione del traffico da sottoporre a decrittazione ed ispezione in base alla specifica compliance dell'organizzazione e/o a requisiti legali specifici.

Quando le organizzazioni crescono, l'esigenza di una protezione scalabile assume maggiore importanza. SonicWall supporta le reti aziendali in crescita con una soluzione che elimina la

Vantaggi:

Prevenzione delle minacce e prestazioni elevate

- Tecnologia Real-Time Deep Memory Inspection in attesa di brevetto
- Tecnologia Reassembly-Free Deep Packet Inspection brevettata
- Prevenzione delle minacce basata sul cloud e integrata
- Decrittazione e ispezione TLS/SSL
- Efficacia della sicurezza collaudata nel settore
- Interfacce 40 GbE e 10 GbE multiple
- Team Capture Labs dedicato alla ricerca delle minacce

Controllo della rete e flessibilità

- Potente sistema operativo SonicOS
- Controllo e intelligence delle applicazioni
- Segmentazione della rete e suddivisione in zone
- Implementazione alla periferia della rete o nel nucleo del data center

Scalabilità e affidabilità

- Numero elevato di connessioni DPI-SSL
- Opzioni di alimentazione multiple
- Modulo di memoria integrato
- Alimentatori e ventole ridondanti

preoccupazione di dover aggiungere maggiore potenza di elaborazione. Il modello NS*sp* 12400 include quattro moduli processore aggiornabili a otto moduli, mentre il modello NS*sp* 12800 dispone di otto moduli processore di serie.

Quando si attivano funzioni di Deep Packet Inspection come IPS, antivirus, antispyware e decrittazione/ispezione TLS/SSL sul firewall, le prestazioni della rete spesso rallentano, anche drasticamente. I firewall di nuova generazione della serie NS*sp*, tuttavia, sono dotati di interfacce 40 GbE ad alta velocità e di un'architettura hardware multi-core che utilizza microprocessori specializzati per la sicurezza. In combinazione con i nostri motori RTDMI ed RFDPI, questa struttura esclusiva elimina i fenomeni di degrado delle prestazioni che le reti subiscono con altri firewall.

Controllo della rete e flessibilità

Il cuore della serie NS*sp* è costituito da SonicOS, il sistema operativo ricco di funzionalità di SonicWall. SonicOS offre alle organizzazioni il controllo della rete e la flessibilità di cui necessitano attraverso l'intelligence e il controllo delle applicazioni, la visualizzazione in tempo reale, un sistema di prevenzione delle intrusioni (IPS) con sofisticate tecnologie anti-evasione, VPN (Virtual Private Networking) ad alta velocità e ulteriori funzionalità di sicurezza.

Mediante il controllo e l'intelligence delle applicazioni, gli amministratori di rete possono identificare e distinguere le applicazioni produttive da quelle improduttive o potenzialmente pericolose e controllare tale traffico attraverso potenti policy a livello di applicazione basate su singoli utenti o su gruppi (insieme a pianificazioni ed elenchi di eccezioni).

Alle applicazioni fondamentali per l'attività aziendale viene assegnata una priorità elevata e più larghezza di banda, mentre le applicazioni non essenziali ricevono larghezza di banda limitata. Il monitoraggio e la visualizzazione in tempo reale forniscono una rappresentazione grafica delle applicazioni, degli utenti e dell'utilizzo della larghezza di banda, offrendo una visione granulare del traffico che attraversa la rete.

Per le aziende che desiderano una flessibilità avanzata per la propria struttura di rete, SonicOS offre gli strumenti per segmentare la rete in zone attraverso l'uso di LAN virtuali (VLAN). In questo modo, gli amministratori di rete possono creare un'interfaccia LAN virtuale che consente di separare la rete in uno o più gruppi logici.

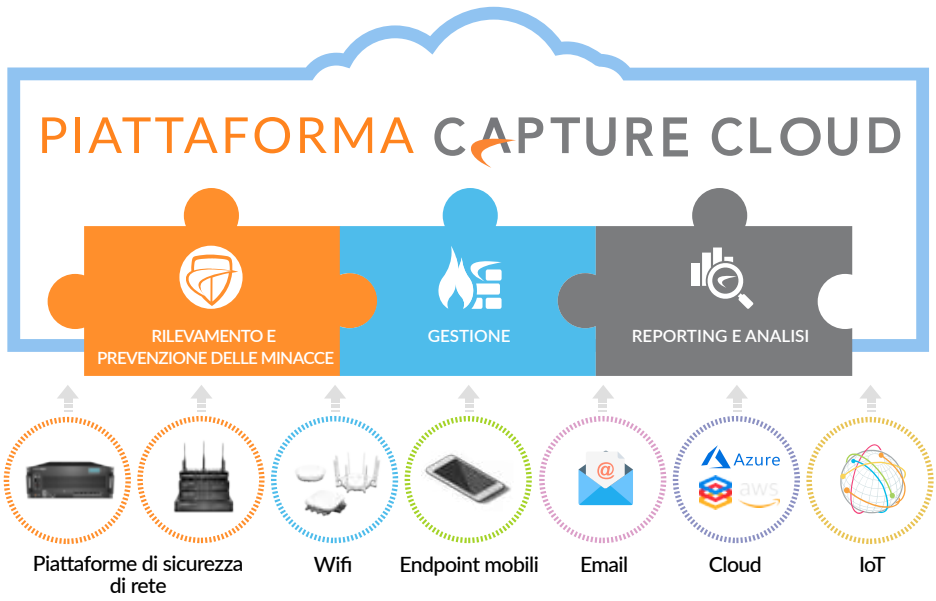
Gestione e reporting semplificati

Le attività di gestione, monitoraggio e reporting delle attività di rete sono gestite tramite il SonicWall Global Management System (GMS), che offre agli amministratori un unico dashboard intuitivo per gestire tutti gli aspetti della rete in tempo reale. La distribuzione e l'installazione semplificate e la facilità di gestione consentono alle organizzazioni di ridurre il costo totale di proprietà e ottenere un elevato ritorno dell'investimento.

Partner Enabled Services
Serve aiuto per pianificare, ottimizzare o implementare una soluzione SonicWall? Gli Advanced Services Partner di SonicWall sono qualificati per fornire servizi professionali di altissimo livello. Per maggiori informazioni: www.sonicwall.com/PES.

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. La piattaforma consolida le informazioni sulle minacce raccolte da molteplici fonti, tra cui il nostro pluripremiato servizio di sandboxing di rete multi-engine Capture Advanced Threat Protection, e oltre 1 milione di sensori SonicWall situati in tutto il mondo.



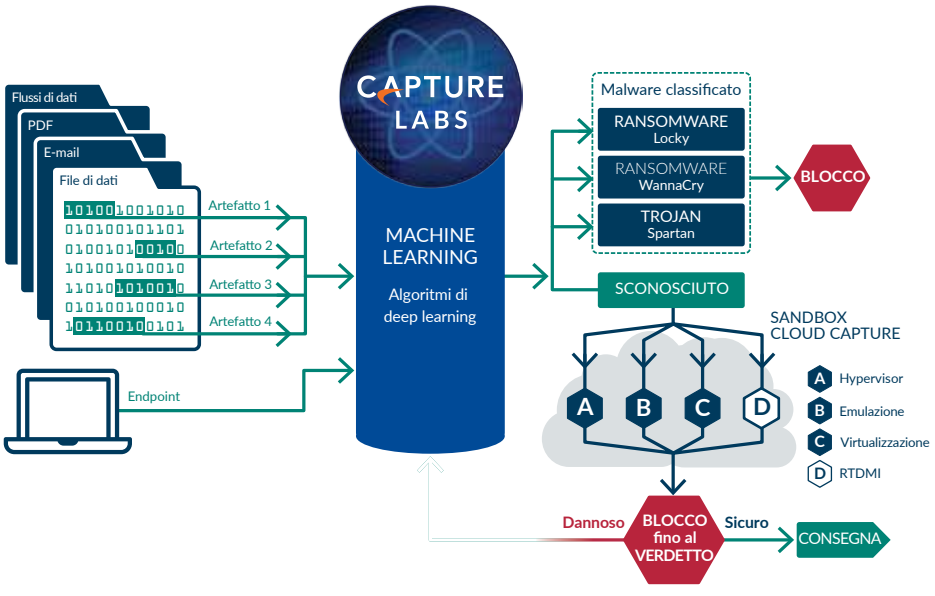
Se i dati in arrivo nella rete contengono codice maligno precedentemente non rilevato, il team Capture Labs interno a SonicWall, dedicato alla ricerca delle minacce, sviluppa firme che vengono archiviate nel database della piattaforma Capture Cloud e distribuite ai firewall dei clienti per aggiornare la protezione. I nuovi aggiornamenti hanno effetto immediato senza riavvii o interruzioni. Le firme presenti sulle appliance forniscono protezione da numerose classi di attacchi, e ogni singola firma può coprire decine di migliaia di minacce uniche. Oltre alle contromisure sulla appliance, i firewall NS*sp* hanno anche accesso continuo al database della piattaforma Capture Cloud, che amplia le informazioni sulle firme integrate con decine di milioni di firme.

Inoltre, la piattaforma Capture Cloud fornisce un unico pannello di gestione e gli amministratori possono facilmente creare report sia in tempo reale che storici sull'attività di rete.

Protezione contro le minacce avanzate

Al centro della prevenzione automatizzata delle violazioni in tempo reale di SonicWall si trova il servizio SonicWall Capture Advanced Threat Protection, una sandbox multi-engine basata su cloud che estende la protezione dalle minacce del firewall per rilevare e prevenire le minacce zero-day. I file sospetti vengono inviati al cloud dove vengono analizzati utilizzando algoritmi di deep learning con la possibilità di trattenerli al gateway fino a quando non viene emesso un verdetto. La piattaforma sandbox multi-engine, che include la tecnologia Real-Time Deep Memory Inspection, sandboxing virtualizzato, emulazione di sistema completa e tecnologia di analisi a livello hypervisor, esegue il codice sospetto e analizza il comportamento. Quando un file viene identificato come maligno, viene bloccato e viene creato immediatamente un hash all'interno di Capture ATP. Poco dopo, una firma viene inviata ai firewall per prevenire gli attacchi successivi.

Il servizio analizza un'ampia gamma di sistemi operativi e tipi di file, tra cui programmi eseguibili, DLL, PDF, documenti MS Office, archivi, JAR e APK.



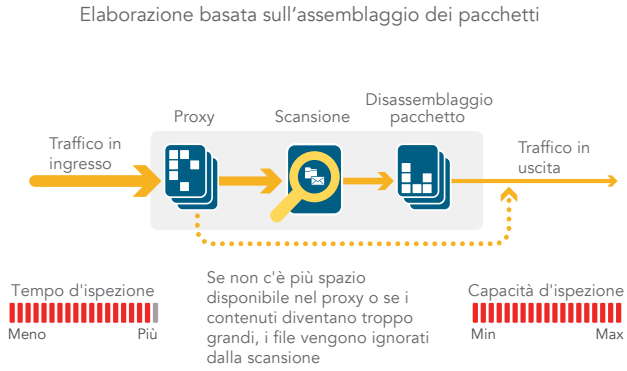
SONICWALL

Motore Reassembly-Free Deep Packet Inspection

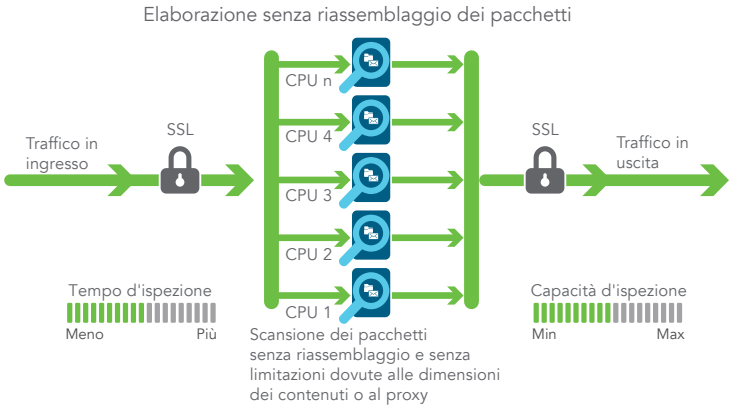
La tecnologia Reassembly-Free Deep Packet Inspection (RFDPI) di SonicWall è un sistema di ispezione a singolo passaggio e bassa latenza che esegue analisi ad alta velocità del traffico bidirezionale in base al flusso, senza proxy o buffering, per scoprire efficacemente i tentativi di intrusione e download di malware esaminando il traffico applicativo indipendentemente dalla porta e dal protocollo. Questo motore proprietario si affida allo streaming per l'ispezione del payload del traffico per rilevare le minacce sui Layer 3-7 e fa passare i flussi di rete attraverso ampie e ripetute fasi di normalizzazione e decrittazione, al fine di neutralizzare le tecniche avanzate di evasione che cercano di confondere i motori di rilevamento e di introdurre codice maligno nella rete.

Una volta superata la necessaria elaborazione preliminare, che include anche la decrittazione TLS/SSL, ogni pacchetto viene analizzato in base a un'unica rappresentazione di memoria proprietaria di tre database di firme: attacchi intrusivi, malware e applicazioni. Lo stato di connessione viene quindi fatto progredire in modo che rappresenti la posizione del flusso riferita a questi database, finché non rileva uno stato di attacco o un altro evento "corrispondente". A questo punto viene intrapresa un'azione predefinita.

Nella maggior parte dei casi, la connessione viene terminata e vengono generati eventi di log e di notifica. Il motore può anche essere configurato per eseguire solo l'ispezione oppure, in caso di rilevamento delle applicazioni, per fornire servizi di gestione della larghezza di banda al livello 7 per il rimanente flusso dell'applicazione non appena viene identificata l'applicazione.



Architettura della concorrenza

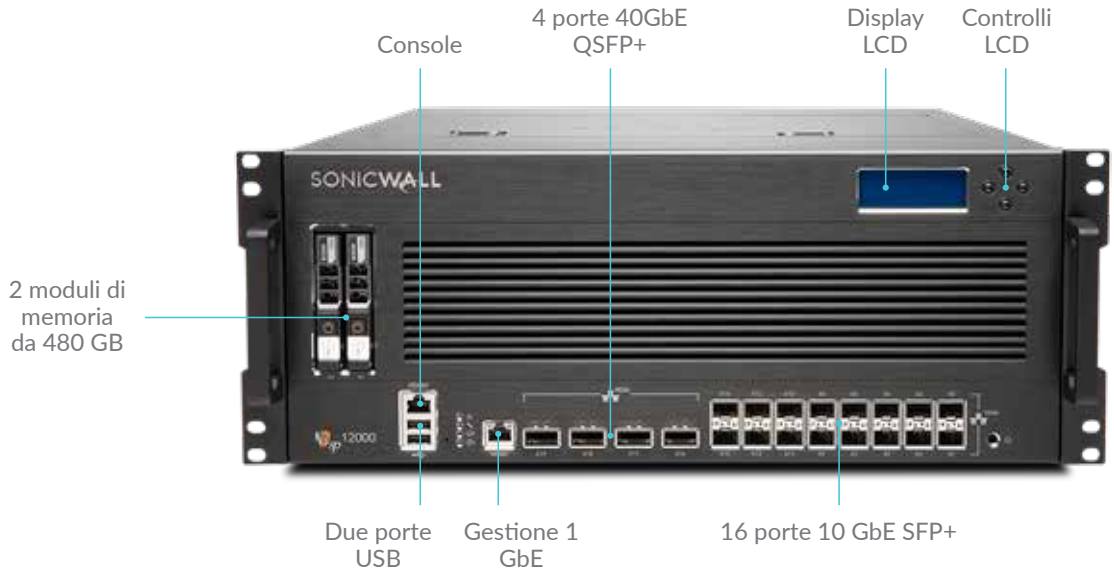


Architettura SonicWall

Gestione centralizzata e reporting

Per le organizzazioni ad elevata regolamentazione che desiderano creare una strategia coordinata di gestione della sicurezza, compliance e gestione del rischio, SonicWall offre agli amministratori una piattaforma unificata, sicura ed espandibile per gestire i firewall SonicWall, gli access point wireless e le soluzioni di accelerazione WAN attraverso un processo di workstream correlato e verificabile. Le imprese possono consolidare facilmente la gestione delle appliance di sicurezza, ridurre la complessità amministrativa e di risoluzione dei problemi e gestire tutti gli aspetti operativi dell'infrastruttura di sicurezza, compresa la gestione e l'applicazione centralizzata delle policy, il monitoraggio degli eventi in tempo reale, le attività degli utenti, l'identificazione delle applicazioni, l'analisi forense e dei flussi, la creazione di rapporti di controllo e conformità e altro ancora. Inoltre, le imprese soddisfano i requisiti di gestione delle modifiche del firewall attraverso l'automazione del flusso di lavoro, che fornisce l'agilità e la sicurezza necessarie per implementare le giuste policy del firewall al momento giusto e in conformità con le normative di compliance. SonicWall Global Management System (GMS), la soluzione di gestione e reporting on-premise di SonicWall, offre un metodo coerente per gestire la sicurezza della rete in base ai processi aziendali e ai livelli di servizio, semplificando notevolmente la gestione del ciclo di vita degli ambienti di sicurezza nel loro insieme rispetto alla gestione dispositivo per dispositivo.

Serie NS*sp* 12000



Firewall	NS*sp* 12400	NS*sp* 12800
Throughput ispezione firewall	58,4 Gbps	120,3 Gbps
Throughput IPS	36,8 Gbps	73,0 Gbps
Throughput ispezione anti-malware	33,5 Gbps	67,5 Gbps
Throughput prevenzione delle minacce	33,5 Gbps	67,5 Gbps
Throughput IMIX	14,8 Gbps	29,0 Gbps
Connessioni max. (DPI)	16.000.000	32.000.000
Nuove connessioni/sec	430.000/sec	860.000/sec
Modulo di memoria	2 x 480 GB	2 x 480 GB
Descrizione	**SKU**	**SKU**
NS*sp*, solo firewall	01-SSC-1206	01-SSC-1207
NS*sp* TotalSecure Advanced (1 anno)	01-SSC-7883	01-SSC-9139

Riepilogo delle funzionalità di SonicOS

Firewall

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

Decrittazione e ispezione TLS/SSL/SSH[1]

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

Capture Advanced Threat Protection[1]

- Real-Time Deep Memory Inspection
- Analisi multi-engine basata sul cloud
- Sandboxing virtualizzato
- Analisi a livello hypervisor
- Emulazione completa del sistema
- Ispezione di un'ampia varietà di file
- Invio automatico e manuale
- Aggiornamenti in tempo reale dell'intelligence contro le minacce
- Blocco fino al verdetto
- Capture Client

Prevenzione delle intrusioni[1]

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

Anti-malware[1]

- Scansione antimalware basata sui flussi
- Gateway anti-virus
- Gateway anti-spyware
- Ispezione bidirezionale
- File senza limiti di dimensioni
- Database malware su 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 report sulle applicazioni tramite NetFlow/IPFIX
- Ampio database di firme delle applicazioni

Visualizzazione e analisi del traffico

- Attività degli utenti
- Utilizzo applicazioni/larghezza di banda/minacce

Filtraggio dei contenuti Web[1]

- Filtraggio degli URL
- Proxy avoidance
- Blocco in base a parole chiave
- Inserimento intestazione HTTP
- Gestione della banda secondo categorie di valutazione CFS
- Modello di policy unificato con controllo delle applicazioni
- Content Filtering Client

VPN

- Provisioning automatico delle VPN
- VPN IPSec per la connettività site-to-site
- Accesso remoto tramite VPN SSL o client IPSec
- Gateway VPN ridondante
- Mobile Connect per iOS, Mac OS X, Windows, Chrome, Android e Kindle Fire
- VPN basata su routing (OSPF, RIP, BGP)

Connettività di rete

- PortShield
- Frame Jumbo
- Logging migliorato
- VLAN trunking
- RSTP (Rapid Spanning Tree Protocol)
- Mirroring delle porte
- Sicurezza delle porte
- QoS layer 2
- Routing dinamico (RIP/OSPF/BGP)
- Routing basato su policy
- NAT
- DNS/Proxy DNS
- Server DHCP
- Gestione della larghezza di banda
- Aggregazione dei link (statica e dinamica)
- Ridondanza delle porte
- Alta disponibilità A/P con sincronizzazione dello stato
- Clustering attivo/attivo
- Bilanciamento del carico in entrata/in uscita
- Bridge L2, modalità Wire/Virtual Wire, modalità Tap
- Routing asimmetrico
- Supporto CAC (Common Access Card)

Wireless

- WIDS/WIPS
- Analisi dello spettro RF
- Prevenzione di access point non autorizzati
- Fast roaming (802.11k/r/v)
- Visualizzazione in pianta/della topologia
- Band steering
- Beamforming
- AirTime Fairness
- MiFi Extender
- Quota ciclica ospite
- Portale ospite LHM

VoIP

- Controllo QoS granulare
- Gestione della larghezza di banda
- Trasformazioni SIP e H.323 per regola di accesso
- Supporto per gatekeeper H.323 e proxy SIP

Gestione e monitoraggio

- GMS, Web, UI, CLI, API REST, SNMPv2/v3
- Accesso
- Esportazione verso Netflow/IPFix
- Backup della configurazione basato su cloud
- Piattaforma Security Analytics di BlueCoat
- Gestione dei punti di accesso SonicWall

Archiviazione

- Log
- Report
- Backup del firmware

[1]Richiede un abbonamento aggiuntivo

SONICWALL

Caratteristiche

Motore RFDPI	
Funzionalità	Descrizione
Reassembly-Free Deep Packet Inspection (RFDPI)	Questo motore di ispezione proprietario brevettato ad alte prestazioni esegue analisi bidirezionali del traffico basate sui flussi, senza proxy o buffering, per rilevare tentativi di intrusione e malware e per identificare il traffico delle applicazioni indipendentemente dalla porta.
Ispezione bidirezionale	Scansiona simultaneamente il traffico in entrata e in uscita alla ricerca di minacce, per garantire che la rete non venga utilizzata per distribuire malware o come piattaforma per lanciare attacchi nel caso in cui una macchina infetta sia stata introdotta nella rete.
Ispezione basata sui flussi	La tecnologia di ispezione priva di proxy e buffering genera una latenza estremamente bassa per l'ispezione DPI di milioni di flussi di rete simultanei, senza limiti per la dimensione dei flussi e dei file, e può essere applicata sia a protocolli comuni che a flussi TCP primari.
Architettura altamente parallela e scalabile	L'esclusivo motore RFDPI basato su architettura multi-core offre l'ispezione DPI ad alta velocità e consente di creare nuove sessioni in tempi estremamente brevi, agevolando la gestione dei picchi di traffico in reti complesse.
Ispezione single-pass	Un'architettura DPI a passaggio singolo esegue simultaneamente l'analisi di malware e intrusioni e l'identificazione delle applicazioni, riducendo drasticamente la latenza dell'ispezione DPI e garantendo che tutte le informazioni sulle minacce siano correlate in un'unica architettura.
Firewall e connettività di rete	
Funzionalità	Descrizione
API REST	Consentono ai firewall di ricevere e utilizzare tutti i feed di intelligence proprietari, dei produttori di dispositivi originali e di terze parti per combattere minacce avanzate come zero-day, utenti malintenzionati, credenziali compromesse, ransomware e minacce persistenti avanzate.
Ispezione Stateful Packet	Tutto il traffico in transito nella rete viene ispezionato, analizzato e conformato alle policy di accesso del firewall.
Alta disponibilità/clustering	La serie NS*sp* supporta le modalità ad alta disponibilità attiva/passiva (A/P) con sincronizzazione dello stato, DPI attiva/attiva (A/A) e clustering attivo/attivo. La modalità DPI attiva/attiva trasferisce il carico di lavoro dell'ispezione deep packet ai core dell'appliance passiva per ottimizzare il throughput.
Protezione da attacchi DDoS/DoS	La protezione da flood SYN offre una difesa contro gli attacchi DoS mediante tecnologie di blacklisting al layer 3 (SYN proxy) e al layer 2 (SYN). Inoltre, protegge da DoS/DDoS attraverso la protezione da flood UDP/ICMP e la limitazione della velocità di connessione.
Supporto di IPv6	L'Internet Protocol versione 6 (IPv6) è nelle fasi iniziali di sostituzione dell'IPv4. Con SonicOS, l'hardware supporta il filtraggio e le implementazioni in modalità cablata.
Opzioni di installazione flessibili	La serie NS*sp* può essere implementata nelle tradizionali modalità NAT, bridge Layer 2, Wire e Network Tap.
Bilanciamento del carico WAN	Bilancia il carico su più interfacce WAN con metodi Round Robin, Spillover o Percentage.
Qualità del servizio (QoS) avanzata	Garantisce l'integrità delle comunicazioni strategiche tramite tagging 802.1p e DSCP e rimappatura del traffico VoIP sulla rete.
Supporto per gatekeeper H.323 e proxy SIP	Blocca le chiamate di spam richiedendo che tutte le chiamate in entrata siano autorizzate e autenticate dal gatekeeper H.323 o dal proxy SIP.
Autenticazione biometrica	Supporta l'autenticazione dei dispositivi mobili come il riconoscimento delle impronte digitali che non può essere facilmente duplicata o condivisa in modo da autenticare in modo sicuro l'identità degli utenti per l'accesso alla rete.
Autenticazione aperta e login social	Consente agli utenti ospiti di utilizzare le proprie credenziali da servizi di social network come Facebook, Twitter o Google+ per accedere a Internet e ad altri servizi come ospiti attraverso la rete wireless, la LAN o le zone DMZ di un host tramite autenticazione pass-through.
Gestione e reporting	
Funzionalità	Descrizione
Global Management System (GMS)	Configurazione e gestione delle appliance SonicWall disponibili on-premise tramite il SonicWall Global Management System (GMS).
Potente gestione dei singoli dispositivi	Un'intuitiva interfaccia basata sul Web, un'interfaccia a riga di comando completa e il supporto per SNMPv2/3 permettono una configurazione semplice e pratica.
Report sul flusso delle applicazioni con IPFIX/NetFlow	Le analisi del traffico e i dati sull'uso delle applicazioni possono essere esportati tramite i protocolli IPFIX o NetFlow per il monitoraggio e la creazione di report in tempo reale e storici con strumenti come SonicWall Analytics o altri tool che supportano IPFIX e NetFlow con estensioni.
Virtual Private Networking (VPN)	
Funzionalità	Descrizione
Provisioning automatico delle VPN	Semplifica l'installazione dei firewall in ambienti distribuiti complessi automatizzando il provisioning iniziale del gateway VPN da sito a sito tra i firewall SonicWall, garantendo l'applicazione istantanea e automatica della sicurezza e della connettività.
VPN IPSec per la connettività site-to-site	La VPN IPSec ad alte prestazioni consente alla serie NS*sp* di agire come concentratore VPN per migliaia di altri siti di maggiori dimensioni, sedi distaccate o uffici domestici.
Accesso remoto tramite VPN SSL o client IPSec	Utilizza la tecnologia VPN SSL clientless oppure un client IPSec di facile gestione per offrire un accesso semplificato a posta elettronica, file, computer, siti intranet e applicazioni da svariate piattaforme.
Gateway VPN ridondante	Se si utilizzano più WAN, è possibile configurare una VPN principale e una secondaria per assicurare failover e failback automatizzati e trasparenti per tutte le sessioni VPN.
VPN basato su routing	La capacità di eseguire il routing dinamico tramite collegamenti VPN garantisce la continuità delle connessioni in caso di interruzione temporanea del tunnel VPN, con un reinstradamento trasparente del traffico tra gli endpoint attraverso percorsi alternativi.

Sensibilità al contesto/al contenuto	
Funzionalità	Descrizione
Monitoraggio delle attività degli utenti	L'identificazione degli utenti e il monitoraggio delle loro attività vengono realizzati tramite l'integrazione SSO trasparente con AD/LDAP/Citrix/Terminal Services combinati a dettagliate informazioni ottenute dall'ispezione DPI.
Identificazione del traffico in base al paese (GeoIP)	Identifica e controlla il traffico di rete diretto verso o proveniente da determinati paesi, sia per proteggere da attacchi originati in luoghi noti o potenzialmente rischiosi, sia per esaminare il traffico sospetto generato all'interno della rete. Possibilità di creare elenchi personalizzati di paesi e botnet per ignorare il tag non corretto di un paese o una botnet associato a un indirizzo IP, eliminando così il filtraggio indesiderato di indirizzi IP a causa di errori di classificazione.
Filtraggio DPI basato su espressioni regolari	Previene le perdite di dati identificando e controllando i contenuti che attraversano la rete in base alla corrispondenza con espressioni regolari. Consente inoltre di creare elenchi personalizzati di paesi e botnet per ignorare il tag non corretto di un paese o una botnet associato a un indirizzo IP.

Servizi in abbonamento per la prevenzione delle violazioni

Capture Advanced Threat Protection	
Funzionalità	Descrizione
Sandboxing multi-engine	La piattaforma sandbox multi-engine, che include emulazione completa del sistema e tecnologie di analisi a livelli hypervisor, esegue il codice sospetto nell'ambiente sandbox virtualizzato, ne analizza il comportamento e fornisce visibilità completa sulle attività malevole.
Real-Time Deep Memory Inspection (RTDMI)	Questa tecnologia basata su cloud in attesa di brevetto rileva e blocca il malware che non mostra alcun comportamento maligno e che cela le sue armi tramite crittografia. Obbligando il malware a svelare le proprie armi nella memoria, il motore RTDMI rileva e blocca in modo proattivo minacce di massa, zero-day e malware sconosciuto.
Blocco fino al verdetto	Per evitare che i file potenzialmente dannosi entrino nella rete, i file inviati al cloud per l'analisi possono essere trattenuti al gateway fino all'emissione di un verdetto.
Analisi di un'ampia gamma di tipi e dimensioni di file	Supporta l'analisi di un'ampia gamma di tipi di file, inclusi programmi eseguibili (PE), DLL, PDF, documenti MS Office, archivi, JAR e APK, oltre a svariati sistemi operativi, inclusi Windows, Android, Mac OS X e ambienti multi-browser.
Rapida distribuzione delle firme	Quando un file viene identificato come maligno, viene immediatamente distribuita una firma ai firewall con abbonamento a SonicWall Capture ATP, ai database delle firme per Gateway Anti-Virus e IPS, nonché ai database di URL, IP e reputazione dei domini nel giro di 48 ore.
Capture Client	Capture Client è una piattaforma client unificata che offre molteplici funzionalità di protezione degli end point, tra cui la protezione avanzata da malware e supporto per la visibilità del traffico crittografato. La piattaforma sfrutta tecnologie di protezione su più livelli, reporting completo e applicazione della protezione degli end point.
Prevenzione delle minacce crittografate	
Funzionalità	Descrizione
Decrittazione e ispezione TLS/SSL	Esegue la decrittazione e l'ispezione del traffico crittografato TLS/SSL in tempo reale, senza proxy, alla ricerca di malware, intrusioni e fughe di dati, e applica policy di controllo di applicazioni, URL e contenuti per proteggere dalle minacce nascoste nel traffico crittografato. Inclusa negli abbonamenti di sicurezza per tutti i modelli della serie NSsp.
Ispezione SSH	La Deep Packet Inspection dell'SSH (DPI-SSH) esegue la decrittazione e l'ispezione dei dati che attraversano il tunnel SSH per prevenire gli attacchi che sfruttano l'SSH.
Prevenzione delle intrusioni	
Funzionalità	Descrizione
Protezione basata su contromisure	Il sistema di prevenzione delle intrusioni IPS (Intrusion Prevention System) utilizza le firme e altre contromisure per scansionare i payload dei pacchetti alla ricerca di vulnerabilità ed exploit, offrendo protezione da un ampio spettro di attacchi e vulnerabilità.
Aggiornamenti automatici delle firme	Il team di ricerca delle minacce di SonicWall esegue incessantemente ricerche e distribuisce gli aggiornamenti in un ampio elenco di contromisure IPS che copre oltre 50 categorie di attacchi. I nuovi aggiornamenti sono immediatamente efficaci, senza la necessità di riavvii o interruzioni del servizio.
Protezione IPS interna alle zone	Aumenta la protezione interna segmentando la rete in varie zone di sicurezza dotate di prevenzione delle intrusioni, impedendo alle minacce di propagarsi oltre i confini delle singole zone.
Rilevamento e blocco di comando e controllo (CnC) delle botnet	Identifica e blocca il traffico di comando e controllo (CnC) generato da bot nella rete locale e diretto agli IP e ai domini che sono stati identificati come fonte di propagazione di malware o punti CnC noti.
Abuso/anomalia di protocolli	Individua e blocca gli attacchi che sfruttano i protocolli noti nel tentativo di eludere il controllo IPS.
Protezione da attacchi zero-day	Protegge la rete dagli attacchi zero-day con aggiornamenti costanti sui metodi e sulle tecniche di exploit più recenti, fornendo protezione da migliaia di singoli exploit.
Tecnologia antievasione	La normalizzazione estesa dei flussi, la decodifica e altre tecniche assicurano che le minacce basate su tecniche di evasione ai livelli 2-7 non possano entrare in rete senza essere rilevate.

Prevenzione delle minacce	
Funzionalità	Descrizione
Antimalware a livello del gateway	Il motore RFDPI scansiona tutto il traffico in entrata, in uscita e tra le zone interne della rete alla ricerca di virus, trojan, key logger e altro malware in file di qualsiasi lunghezza e dimensione, su tutte le porte e tutti i flussi TCP.
Protezione contro il malware Capture Cloud	Un database residente sui server cloud SonicWall, costantemente aggiornato con decine di milioni di firme delle minacce, viene consultato per ottimizzare le capacità del database di firme integrato nel dispositivo, garantendo così un'ampia copertura delle minacce da parte del motore RFDPI.
Aggiornamenti di sicurezza costanti	I nuovi aggiornamenti sulle minacce vengono inviati automaticamente ai firewall dotati di servizi di sicurezza attivi e sono subito efficaci senza riavvii o interruzioni.
Ispezione bidirezionale dei TCP primari	Il motore RFDPI è in grado di scansionare flussi TCP primari in entrambe le direzioni su qualsiasi porta, bloccando gli attacchi che tentano di passare attraverso sistemi di sicurezza obsoleti, concepiti per proteggere solo poche porte note.
Ampio supporto di protocolli	Identifica i comuni protocolli come HTTP/S, FTP, SMTP, SMBv1/v2 e altri che non inviano dati nel formato TCP grezzo, e decodifica i payload per eseguire l'ispezione anti-malware anche se questi non utilizzano le tradizionali porte standard.

Application Intelligence and Control	
Funzionalità	Descrizione
Controllo delle applicazioni	Controlla le applicazioni, o singole funzionalità delle applicazioni, identificate dal motore RFDPI utilizzando un database in continua espansione, contenente migliaia di firme di applicazioni, per aumentare la sicurezza e la produttività della rete.
Identificazione di applicazioni personalizzate	Controlla le applicazioni personalizzate generando firme basate su parametri specifici o su modelli di comunicazione in rete univoci per ogni applicazione, in modo da garantire un maggiore controllo sulla rete.
Gestione della larghezza di banda delle applicazioni	Consente l'allocazione granulare e la regolazione della larghezza di banda disponibile per applicazioni o categorie di applicazioni critiche, impedendo nel contempo il traffico di applicazioni non essenziali.
Controllo granulare	Controlla le applicazioni, o componenti specifici di un'applicazione, in base a pianificazioni, gruppi di utenti, elenchi di esclusione e numerose altre azioni con identificazione completa dell'utente tramite SSO (Single Sign-On) e integrazione LDAP/AD/Terminal Service/Citrix.
Filtraggio dei contenuti	
Funzionalità	Descrizione
Filtraggio dei contenuti interno/esterno	Il Content Filtering Service applica le policy di utilizzo accettabili e blocca l'accesso a siti Web contenenti informazioni o immagini discutibili o non produttive.
Enforced Content Filtering Client	Estende l'applicazione dei criteri per bloccare i contenuti Internet per dispositivi Windows, Mac OS, Android e Chrome situati all'esterno del perimetro del firewall.
Controlli granulari	Bloccano i contenuti utilizzando categorie predefinite o qualsiasi combinazione di categorie. Il filtraggio può essere pianificato in base all'ora del giorno, ad esempio durante gli orari scolastici o di lavoro, e applicato a singoli utenti o gruppi.
Cache Web	Le valutazioni degli URL sono archiviate localmente nella cache del firewall SonicWall, garantendo tempi di accesso praticamente immediati per i siti più visitati.
Anti-virus e anti-spyware implementati	
Funzionalità	Descrizione
Protezione multilivello	Utilizza le funzionalità del firewall come primo livello di difesa sul perimetro, insieme alla protezione degli endpoint per bloccare i virus che entrano nella rete tramite laptop, chiavette USB e altri sistemi non protetti.
Opzione di implementazione automatizzata	Assicura che ogni computer che accede alla rete abbia installato e attivato il software antivirus appropriato e/o il certificato DPI-SSL, eliminando i costi comunemente associati alla gestione dell'antivirus desktop.
Distribuzione e implementazione automatizzate	La distribuzione e l'installazione macchina per macchina dei client antivirus e anti-spyware sono automatizzate sull'intera rete, riducendo al minimo l'impegno amministrativo.
Antivirus di nuova generazione	Capture Client utilizza un motore statico di intelligenza artificiale (AI) per determinare le minacce prima che possano essere eseguite e per ripristinare uno stato precedente non infetto.
Protezione antispyware	La potente protezione contro gli spyware garantisce il massimo livello di prestazioni e sicurezza analizzando e bloccando i programmi spyware più diffusi e pericolosi, prima che questi possano carpire dati sensibili da computer fissi o portatili.

Specifiche di sistema della serie NS*sp*

Firewall in generale	NS*sp* 12400	NS*sp* 12800
Sistema operativo	SonicOS 6.5.1.8	
Core di elaborazione di sicurezza	128	256
Interfacce	4 x 40 GbE QSFP+, 16 x 10 GbE SFP+, 1 GbE di gestione, 1 Console	4 x 40 GbE QSFP+, 16 x 10 GbE SFP+, 1 GbE di gestione, 1 Console
Archiviazione integrata	2 x 480 GB	
Gestione	CLI, SSH, Web UI, GMS, API REST	
Utenti SSO	110.000	110.000
Access point max. supportati	128	128
Accesso	Analyzer, registro locale, Syslog, IPFIX, NetFlow	
Firewall/prestazioni VPN	**NS*sp* 12400**	**NS*sp* 12800**
Throughput ispezione firewall[1]	58,4 Gbps	120,3 Gbps
Throughput prevenzione delle minacce[2]	33,5 Gbps	67,5 Gbps
Throughput ispezione applicazioni[2]	45,5 Gbps	91,0 Gbps
Throughput IPS[2]	36,8 Gbps	73,0 Gbps
Throughput ispezione antimalware[2]	33,5 Gbps	67,5 Gbps
Throughput IMIX	14,8 Gbps	29,0 Gbps
Throughput decrittazione e ispezione TLS/SSL (SSL DPI)[2]	8,1 Gbps	17,6 Gbps
Throughput VPN[3]	24,5 Gbps	47,0 Gbps
Connessioni al secondo	430.000/sec	860.000/sec
Connessioni max. (SPI)	40.000.000	80.000.000
Connessioni max. (DPI)	16.000.000	32.000.000
Connessioni max. (DPI SSL)	800.000	1.600.000
VPN	**NS*sp* 12400**	**NS*sp* 12800**
Tunnel VPN site-to-site	25.000	25.000
Client VPN IPSec (max)	2.000 (10.000)	2.000 (10.000)
Client NetExtender SSL VPN (max)	2 (3.000)	2 (3.000)
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 basato su routing	RIP, OSPF, BGP	
Connettività di rete	**NS*sp* 12400**	**NS*sp* 12800**
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	512
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, 802.1p	
Autenticazione	LDAP, XAUTH/RADIUS, SSO, Novell, database utenti interno, Terminal Services, Citrix, Common Access Card (CAC)	
VoIP	Full H323-v1-5, 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	
Alta disponibilità	Attiva/passiva con State Sync, DPI attiva/attiva con State Sync, clustering attivo/attivo	
Hardware	**NS*sp* 12400**	**NS*sp* 12800**
Alimentazione	Doppia, ridondante, 1.200 W	
Ventole	Doppie, rimovibili	
Tensione d'esercizio	100-240 VAC, 50-60 Hz	
Consumo energetico massimo (W)	679	965
MTBF a 25 °C in ore	113.114	91.118
MTBF a 25 °C in anni	12,9	10,4
Fattore di forma	Montabile su rack 4U	
Dimensioni	61 x 43 x 18 cm (24,0 x 16,9 x 7,1 in)	
Peso	26,9 kg (59,3 lb)	30,5 kg (67,2 lb)
Peso WEEE	30,7 kg (67,7 lb)	34,3 kg (75,6 lb)
Peso con la confezione	37,7 kg (83,1 lb)	41,3 kg (91,1 lb)
Normative principali	FCC Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, MSIP/KCC Class A, UL, cUL, TÜV/GS, CB, Mexico CoC by UL, WEEE , REACH, ANATEL, BSMI	
Condizioni ambientali (in funzionamento/stoccaggio)	0-40 °C (32-105 °F) / da -40 a 70 °C (da -40 a 158 °F)	
Umidità	10-95% senza condensa	

[1] Metodologie di test: prestazioni massime come da RFC 2544 (per il firewall). Le prestazioni effettive possono variare in base alle condizioni della rete e ai servizi attivati.
[2] Rilevazione throughput completa per DPI/Gateway AV/Anti-Spyware/IPS tramite il test di performance Spirent WebAvalanche HTTP standard nell'industria e gli strumenti di test Ixia. Test eseguiti con flussi multipli attraverso coppie di porte multiple. Rilevazione throughput di prevenzione delle minacce con Gateway AV, Anti-Spyware, IPS e Application Control attivati. Prestazioni DPI SSL misurate sul traffico HTTPS con IPS attivato.
[3] Rilevazione throughput VPN tramite traffico UDP con pacchetti da 1280 byte, in conformità a RFC 2544. Specifiche, funzionalità e disponibilità soggette a modifiche.
[*] Uso futuro. Specifiche, funzionalità e disponibilità soggette a modifiche.

Informazioni per l'ordinazione della serie NS*sp* 12000

NS*sp* 12400	SKU
NS*sp* 12400 TotalSecure Advanced Edition (1 anno)	01-SSC-7883
Advanced Gateway Security Suite – Capture ATP, prevenzione delle minacce, Content Filtering e supporto 24x7 per NS*sp* 12400 (1 anno)	01-SSC-6588
Capture Advanced Threat Protection per NS*sp* 12400 (1 anno)	01-SSC-6598
Prevenzione delle minacce – Prevenzione delle intrusioni, gateway antivirus, gateway antispyware, cloud antivirus per NS*sp* 12400 (1 anno)	01-SSC-7853
Supporto 24x7 per NS*sp* 12400 (1 anno)	01-SSC-6384
Content Filtering Service per NS*sp* 12400 (1 anno)	01-SSC-7698
NS*sp* 12800	**SKU**
NS*sp* 12800 TotalSecure Advanced Edition (1 anno)	01-SSC-9139
Advanced Gateway Security Suite – Capture ATP, prevenzione delle minacce, Content Filtering e supporto 24x7 per NS*sp* 12800 (1 anno)	01-SSC-6591
Capture Advanced Threat Protection per NS*sp* 12800 (1 anno)	01-SSC-7178
Prevenzione delle minacce – Prevenzione delle intrusioni, gateway antivirus, gateway antispyware, cloud antivirus per NS*sp* 12800 (1 anno)	01-SSC-7879
Supporto 24x7 per NS*sp* 12800 (1 anno)	01-SSC-6498
Content Filtering Service per NS*sp* 12800 (1 anno)	01-SSC-7850
Moduli e accessori*	**SKU**
Modulo processore per la serie NS*sp* 12000	01-SSC-1211
Modulo SSD per la serie NS*sp* 12000	01-SSC-1212
Ventola di sistema per la serie NS*sp* 12000	01-SSC-1213
Alimentatore CA per la serie NS*sp* 12000	01-SSC-1215

**Per un elenco completo dei moduli SFP e SFP+ supportati, contattare il rivenditore SonicWall locale.*

Numeri di modello normativi:

NS*sp* 12400/12800 – 4RK02-0C0

Informazioni su SonicWall

Da oltre 27 anni SonicWall combatte il crimine informatico proteggendo piccole, medie e grandi imprese in ogni parte del mondo. La nostra combinazione di prodotti e partner ha permesso di realizzare una soluzione di rilevamento e prevenzione automatizzata delle violazioni in tempo reale ottimizzata per le esigenze specifiche di oltre 500.000 organizzazioni in più di 215 paesi e regioni, per consentire loro di fare più affari con maggior sicurezza.

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

© 2018 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.
Datasheet-NSsp-US-KJ-MKTG4029