Serie NSA – Network Security Appliance

Firewall di nuova generazione

Le organizzazioni affrontano oggi sfide senza precedenti a livello di sicurezza. La sofisticazione e il volume degli attacchi aumentano in maniera esponenziale, provocando perdite di dati aziendali, personali e dei clienti, furti di proprietà intellettuale, danni all'immagine e perdita di produttività. La gestione della sicurezza è diventata più complessa. Prima di scegliere alternative è quindi necessario stabilire quali sono le priorità. L'aumento esplosivo di device personali come smartphone e tablet che si connettono alla rete, favorito dalla rivoluzione BYO (bring your own), rallenta le prestazioni e riduce la produttività aziendale. Inoltre, le applicazioni mobili di social media e video streaming consumano una quantità enorme di larghezza di banda. Questo fenomeno ha creato due differenti problematiche, ovvero come salvaguardare la sicurezza e garantire la produttività.
Per mantenere alte le prestazioni della rete, spesso i responsabili IT disattivano alcune funzionalità, con il rischio di compromettere la sicurezza.

Ora è possibile mantenere le organizzazioni sicure e produttive senza compromettere le prestazioni della rete. Dell™ SonicWALL™ serie NSA (Network Security Appliance) è una delle più potenti e sicure linee di firewall di nuova generazione. Basata sulla stessa architettura firewall di nuova generazione della nostra linea di punta SuperMassive, inizialmente sviluppata per le complesse esigenze di operatori di telecomunicazioni e grandi imprese, fornisce livelli di protezione e prestazioni di classe enterprise senza compromessi. Allo stesso tempo offre la rinomata facilità d'uso e il grande valore che contraddistinguono i prodotti Dell. Basata su anni di ricerca e sviluppo, la serie NSA è appositamente concepita per le esigenze di aziende distribuite, piccole e medie imprese, filiali aziendali, campus universitari e agenzie governative. La serie NSA affianca una rivoluzionaria architettura multi-core ad altissima scalabilità al brevettato* motore di prevenzione delle minacce Reassembly-Free Deep Packet Inspection® (RFDPI) a passaggio singolo. Questa combinazione offre un eccellente livello di protezione, prestazioni e scalabilità, supportato dal massimo numero di connessioni concorrenti, la più bassa latenza e il maggior numero di connessioni al secondo nella sua categoria, il tutto senza limitazioni delle dimensioni dei file. La nostra tecnologia è stata valutata e/o certificata da autorevoli società di verifica indipendenti di terze parti.

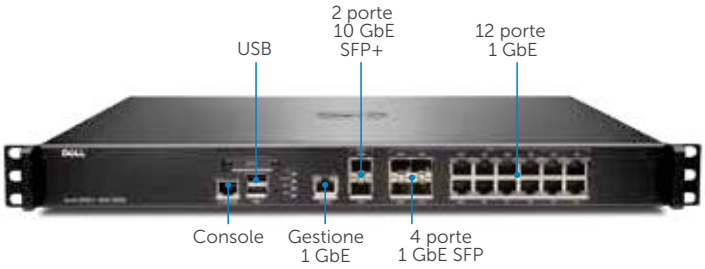
A differenza delle tradizionali tecnologie firewall e di prevenzione delle intrusioni della concorrenza, la serie NSA ispeziona tutto il traffico, indipendentemente dalla porta o dal protocollo. I firewall della serie NSA bloccano attacchi avanzati basati su malware crittografato con la velocità di decrittazione SSL in tempo reale più elevata del settore. L'integrazione con i server di autenticazione consente di applicare in modo efficace criteri di utilizzo accettabile attraverso controlli granulari delle applicazioni per gestire la larghezza di banda e ottimizzare la produttività. Rispetto a soluzioni obsolete composte da più prodotti che non sono in grado di condividere le informazioni sulle minacce, la serie NSA integra il firewall e il sistema IPS in un unico dispositivo. Questa "intelligenza connessa" applica criteri mirati per intensificare l'efficacia della protezione, riducendo drasticamente i tempi di gestione e i rischi per l'azienda. Con Dell SonicWALL Global Management System (GMS), le aziende distribuite possono gestire migliaia di appliance di sicurezza SonicWALL tramite un'unica interfaccia consolidata, semplificando la gestione e riducendo il costo totale di proprietà. La visualizzazione completa in tempo reale mostra quello che succede nella rete tramite report dettagliati, che possono essere elaborati direttamente sull'appliance o su tool esterni.

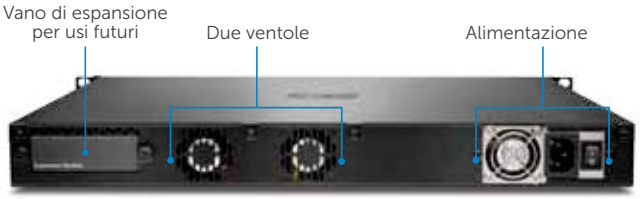
- **Protezione avanzata**
- **Architettura multi-core**
- **Prestazioni eccellenti**
- **Prevenzione delle intrusioni**
- **Anti-malware a livello gateway**
- **Accesso remoto sicuro**
- **Wireless sicuro**
- **Filtraggio URL**
- **Anti-spam a livello gateway**
- **Controllo delle applicazioni**
- **Gestione centralizzata**

*Brevetti USA 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723

I firewall di nuova generazione della serie Dell SonicWALL NSA utilizzano la più recente architettura hardware multi-core e l'ispezione approfondita dei pacchetti senza riassemblaggio per proteggere la rete da attacchi interni ed esterni senza compromettere le prestazioni. La serie NSA fornisce prevenzione delle intrusioni, ispezione di file e contenuti, intelligence e controllo delle applicazioni, alta disponibilità e funzioni di rete avanzate.

Network Security Appliance 3600



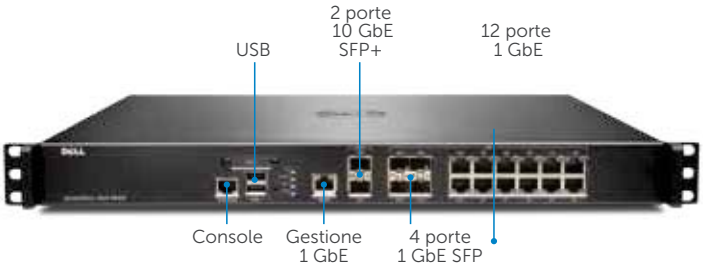


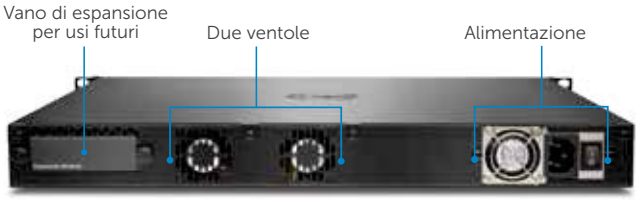
Dell SonicWALL NSA 3600 è ideale per filiali di aziende distribuite, piccole e medie imprese e ambienti retail.

Firewall	NSA 3600
Throughput[1] firewall	3,4 Gbps
Throughput[2] IPS	1,1 Gbps
Throughput[2] anti-malware	600 Mbps
Throughput[2] DPI completa	500 Mbps
Throughput[3] IMIX	900 Mbps
Connessioni DPI (max.)	175.000
Nuove connessioni/sec.	20.000/sec.

Descrizione	Codice
NSA 3600, solo firewall	01-SSC-3850
NSA 3600 TotalSecure (1 anno)	01-SSC-3853
Comprehensive Gateway Security Suite (1 anno)	01-SSC-4429
Gateway Anti-Malware/IPS (1 anno)	01-SSC-4435
Supporto Silver 24x7 (1 anno)	01-SSC-4302

Network Security Appliance 4600



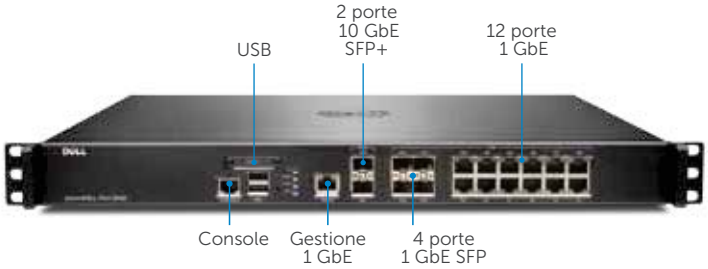


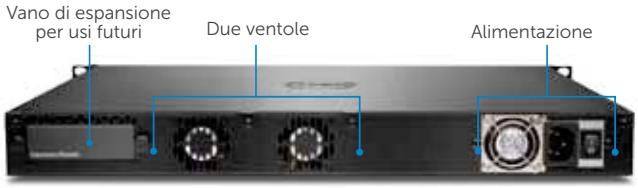
Dell SonicWALL NSA 4600 è ideale per filiali e reti aziendali di piccole e medie dimensioni con l'esigenza di maggiori prestazioni e throughput.

Firewall	NSA 4600
Throughput[1] firewall	6,0 Gbps
Throughput[2] IPS	2,0 Gbps
Throughput[2] anti-malware	1,1 Gbps
Throughput[2] DPI completa	800 Mbps
Throughput[3] IMIX	1,6 Gbps
Connessioni DPI (max.)	250.000
Nuove connessioni/sec.	40.000/sec.

Descrizione	Codice
NSA 4600, solo firewall	01-SSC-3840
NSA 4600 TotalSecure (1 anno)	01-SSC-3843
Comprehensive Gateway Security Suite (1 anno)	01-SSC-4405
Secure Upgrade Plus (3 anni)	01-SSC-4267
Supporto Silver 24x7 (1 anno)	01-SSC-4290

Network Security Appliance 5600



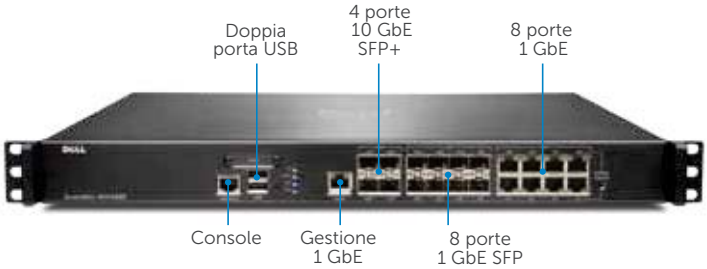


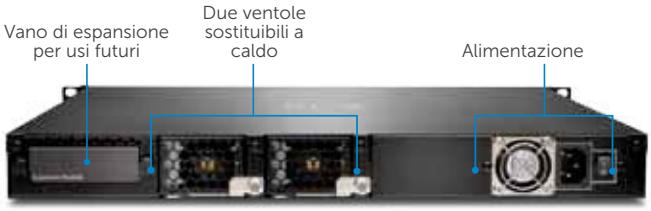
Dell SonicWALL NSA 5600 è ideale per reti aziendali distribuite, sedi distaccate e ambienti aziendali che richiedono solide capacità di throughput.

Firewall	NSA 5600
Throughput[1] firewall	9,0 Gbps
Throughput[2] IPS	3,0 Gbps
Throughput[2] anti-malware	1,7 Gbps
Throughput[2] DPI completa	1,6 Gbps
Throughput[3] IMIX	2,4 Gbps
Connessioni DPI (max.)	500.000
Nuove connessioni/sec.	60.000/sec.

Descrizione	Codice
NSA 5600, solo firewall	01-SSC-3830
NSA 5600 TotalSecure (1 anno)	01-SSC-3833
Comprehensive Gateway Security Suite (1 anno)	01-SSC-4234
Gateway Anti-Malware/IPS (1 anno)	01-SSC-4240
Supporto Gold 24x7 (1 anno)	01-SSC-4284

Network Security Appliance 6600





Dell SonicWALL NSA 6600 è ideale per grandi ambienti distribuiti e reti aziendali a gestione centralizzata che richiedono elevate prestazioni e grandi capacità di throughput.

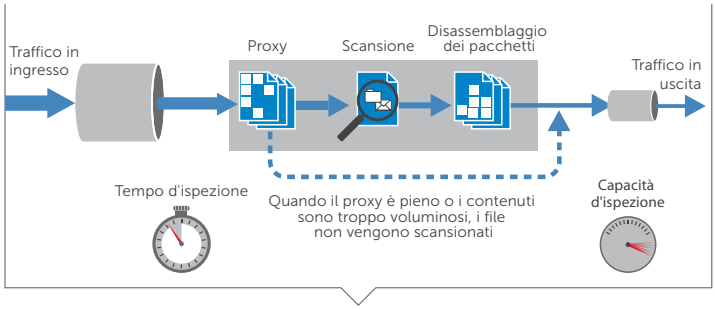
Firewall	NSA 6600
Throughput[1] firewall	12,0 Gbps
Throughput[2] IPS	4,5 Gbps
Throughput[2] anti-malware	3,0 Gbps
Throughput[2] DPI completa	3,0 Gbps
Throughput[3] IMIX	3,5 Gbps
Connessioni DPI (max.)	600.000
Nuove connessioni/sec.	90.000/sec.

Descrizione	Codice
NSA 6600, solo firewall	01-SSC-3820
NSA 6600 TotalSecure (1 anno)	01-SSC-3823
Comprehensive Gateway Security Suite (1 anno)	01-SSC-4210
Gateway Anti-Malware/IPS (1 anno)	01-SSC-4216
Supporto Gold 24x7 (1 anno)	01-SSC-4278

Motore RFDPI

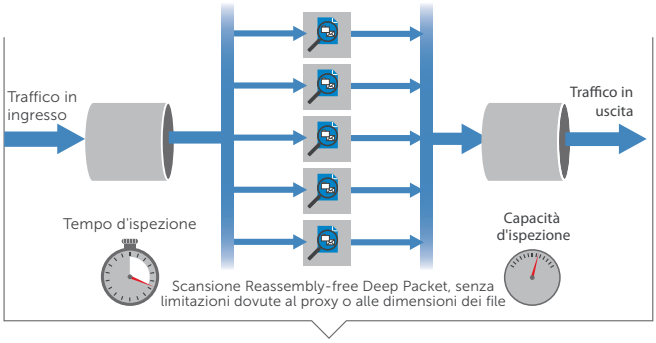
Il motore Dell SonicWALL RFDPI (Reassembly-Free Deep Packet Inspection) fornisce protezione dalle minacce e controllo avanzato delle applicazioni senza compromettere le prestazioni. Questo motore brevettato ispeziona il payload del traffico in transito per rilevare eventuali minacce ai livelli 3-7. Il motore RFDPI esamina i flussi di rete mediante ripetuti e approfonditi processi di normalizzazione e decrittazione, in modo da neutralizzare le tecniche di evasione avanzate che tentano di confondere i motori di rilevamento per introdurre furtivamente codice maligno nella rete. Una volta superata la necessaria elaborazione preliminare, che include anche la decrittazione 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 costantemente aggiornato sul firewall e confrontato con i database e, non appena viene rilevato un attacco o un altro evento paragonabile, viene adottata 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.

Elaborazione basata sull'assemblaggio dei pacchetti



Architettura della concorrenza

Elaborazione senza riassemblaggio dei pacchetti

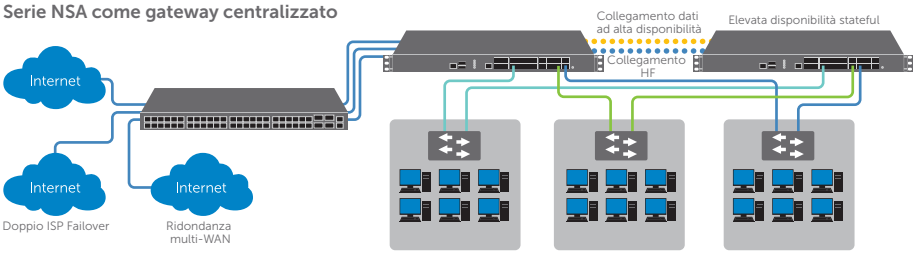


Architettura Dell SonicWALL

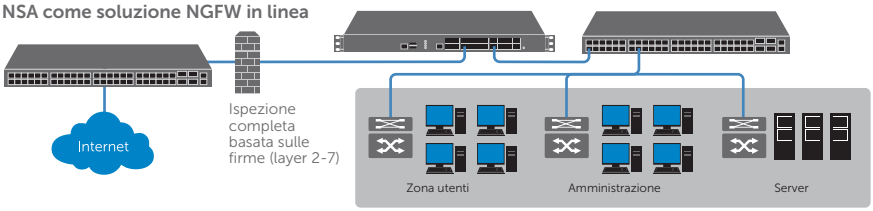
Implementazione flessibile e personalizzabile – La serie NSA in breve

Le soluzioni NSA (Network Security Appliance) di SonicWALL forniscono protezione firewall di ultima generazione basata sull'innovativa architettura hardware multi-core con tecnologia d'ispezione Reassembly-Free Deep Packet Inspection, senza rallentare le prestazioni della rete. Tutti i prodotti della serie NSA offrono servizi di fascia alta come prevenzione delle intrusioni ad alta velocità, ispezione di file e contenuti, potenti funzioni di controllo e intelligence delle applicazioni, funzionalità di networking avanzate e flessibilità di configurazione. Le appliance della serie NSA hanno un prezzo conveniente e possono essere implementate e gestite in diverse tipologie di reti aziendali, filiali e ambienti di rete distribuiti.

Serie NSA come gateway centralizzato



Serie NSA come soluzione NGFW in linea



SonicWALL

Sicurezza e protezione

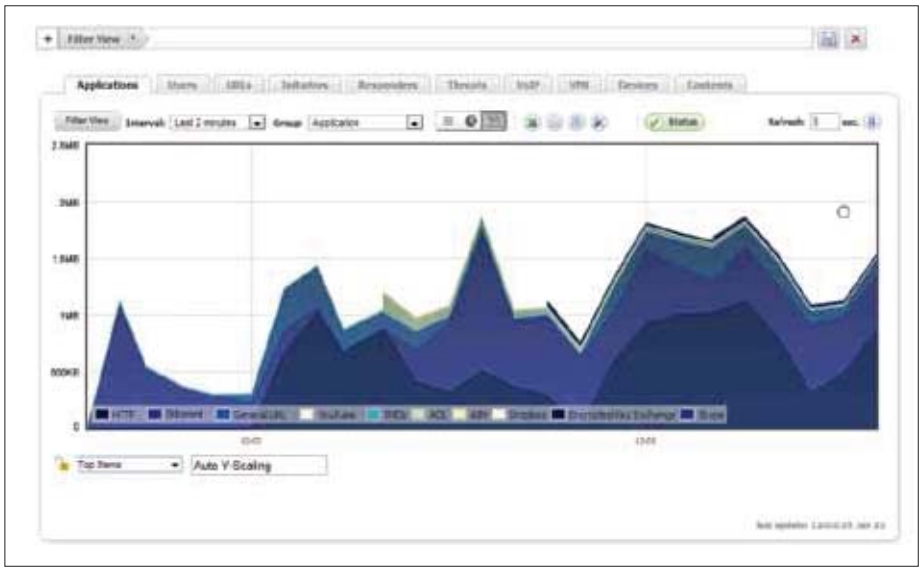
Il team interno dedicato alla ricerca delle minacce di Dell SonicWALL è costantemente impegnato a ricercare e sviluppare contromisure da implementare nei firewall in uso, in modo da mantenere aggiornata la protezione. Il team di ricerca utilizza più di un milione di sensori sparsi in tutto il mondo per raccogliere campioni di malware e dati telemetrici con informazioni sulle minacce più recenti, riversandoli poi nelle funzionalità di prevenzione delle intrusioni, ispezione anti-malware e rilevamento delle applicazioni. I clienti che utilizzano i firewall Dell SonicWALL di nuova generazione con le funzionalità più recenti ottengono così una protezione dalle minacce costantemente aggiornata, dato che i nuovi aggiornamenti hanno effetto immediato, senza bisogno di interruzioni o di riavvio dei dispositivi.

Le firme presenti sulle appliance sono concepite per fornire protezione da numerose classi di attacchi, e ogni singola firma può coprire fino a decine di migliaia di minacce uniche.

Oltre alle contromisure disponibili nell'appliance, i firewall NSA hanno anche accesso al servizio Dell SonicWALL CloudAV, che amplia le funzionalità di intelligence integrate nei dispositivi con oltre 12 milioni di firme. I firewall possono accedere al database CloudAV, mediante un protocollo proprietario leggero, per aumentare l'efficacia dell'ispezione eseguita dall'appliance. Grazie alle funzioni di geolocalizzazione degli IP e di filtraggio botnet, i firewall Dell SonicWALL di nuova generazione sono in grado di bloccare il traffico proveniente da domini o intere aree geografiche pericolose per ridurre il profilo di rischio della rete.

Controllo e intelligence delle applicazioni

L'intelligence delle applicazioni informa gli amministratori sul traffico applicativo che attraversa la loro rete, permettendogli di pianificare controlli delle applicazioni in base a priorità aziendali, limitare le applicazioni non produttive e bloccare le applicazioni potenzialmente pericolose. La visualizzazione in tempo reale identifica anomalie del traffico nel momento in cui si verificano, permettendo di adottare rimedi immediati contro potenziali attacchi in entrata o in uscita o colli di bottiglia a livello di prestazioni.



L'analisi del traffico delle applicazioni di Dell SonicWALL offre una visione granulare del traffico applicativo, dell'uso della larghezza di banda e delle minacce alla sicurezza, integrata da potenti funzioni di risoluzione dei problemi e analisi forense. Inoltre le funzionalità di Single Sign-On (SSO) sicuro migliorano l'esperienza degli utenti, aumentano la produttività e riducono le richieste di assistenza.

Il Dell SonicWALL Global Management System (GMS®) semplifica la gestione delle funzioni di intelligence e controllo delle applicazioni grazie all'intuitiva interfaccia basata sul Web.

Funzionalità

Motore RFDPI

Funzionalità	Descrizione
Reassembly-Free Deep Packet Inspection (RFDPI)	Questo brevettato motore d'ispezione proprietario esegue l'analisi ad alte prestazioni del traffico basato sui flussi in entrambe le direzioni, senza l'uso di proxy e senza buffering, per rilevare tentativi di intrusione o malware e identificare il traffico delle applicazioni a prescindere dalla porta utilizzata.
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 DPI (Deep Packet Inspection) senza proxy e senza buffering consente di ispezionare milioni di flussi di rete simultanei con una latenza bassissima e senza introdurre limitazioni sulle dimensioni dei file e dei flussi, ed è applicabile sia ai protocolli comuni che a flussi TCP grezzi.
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 a singola fase	L'architettura DPI a singola fase esegue simultaneamente la scansione 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.

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 Dell 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 richiedere il riavvio dei dispositivi o l'interruzione dei servizi.
Protezione IPS interzona	Aumenta la protezione interna segmentando la rete in più zone di sicurezza dotate di prevenzione delle intrusioni, impedendo alle minacce di propagarsi oltre i limiti delle singole zone.
Rilevazione e bloccaggio di botnet	Identifica e blocca il traffico di comando e controllo (CnC) generato da bot sulla rete locale e diretto a IP e domini riconosciuti come canali di propagazione del malware o noti come punti CnC.
Rilevamento e prevenzione di abusi/anomalie dei protocolli	Identifica 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 anti-evasione	I complessi metodi di normalizzazione e decodifica dei flussi e altre tecniche assicurano che le minacce basate su tecniche di evasione ai livelli 2-7 non possano entrare in rete senza essere rilevate.

Funzionalità

Prevenzione delle minacce

Funzionalità	Descrizione
Anti-malware a livello del gateway	Il motore Dell SonicWALL 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.
CloudAV	Un database residente sui server cloud di Dell SonicWALL, costantemente aggiornato con oltre 12 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 RFDPI.
Aggiornamenti di sicurezza 24 ore su 24	Il team di ricerca delle minacce di Dell SonicWALL analizza le nuove minacce e rilascia contromisure 24 ore al giorno, 7 giorni alla settimana. Gli aggiornamenti sulle nuove minacce vengono automaticamente inviati ai firewall dotati di servizi di sicurezza attivi, e sono immediatamente efficaci senza bisogno di riavvio o di interruzioni.
Ispezione SSL	Decifra e ispeziona in tempo reale il traffico SSL senza proxy alla ricerca di malware, intrusioni e fughe di dati, applicando le policy di controllo delle applicazioni, degli URL e dei contenuti per proteggere la rete dalle minacce nascoste nel traffico crittografato con SSL.
Ispezione bidirezionale di flussi TCP grezzi	Il motore RFDPI è in grado di scansionare flussi TCP grezzi 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.

Controllo e intelligence delle applicazioni

Funzionalità	Descrizione
Controllo delle applicazioni	Controlla le applicazioni – o singole funzionalità delle applicazioni – identificate dal motore RFDPI utilizzando un database in continua espansione, contenente oltre 4.300 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	Limita o assegna priorità alle applicazioni, o ad intere categorie di applicazioni, per massimizzare la larghezza di banda a disposizione delle applicazioni strategiche, eliminando o riducendo il traffico delle applicazioni indesiderate.
Visualizzazione del traffico interno/esterno	Identifica l'utilizzo della larghezza di banda e analizza il comportamento della rete, visualizzando in tempo reale il traffico delle applicazioni direttamente sul dispositivo e generando report sul traffico applicativo per analisi esterne tramite NetFlow/IPFix.
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.

Funzionalità

Firewall e networking

Funzionalità	Descrizione
Ispezione Stateful Packet	Tutto il traffico in transito nella rete viene ispezionato, analizzato e conformato alle policy di accesso del firewall.
Protezione da attacchi DDoS/DoS	La protezione SYN Flood offre una difesa contro gli attacchi DoS mediante tecnologie di black-listing al layer 3 (SYN proxy) e al layer 2 (SYN). Inoltre consente di proteggersi da attacchi DoS/DDoS tramite tecniche di protezione da UDP/ICMP Flood e limitando il numero di connessioni.
Implementazione flessibile	La serie NSA può essere implementata nelle tradizionali modalità NAT, Bridge (layer 2), Wire e Network Tap.
Alta disponibilità/clustering	La serie NSA supporta le modalità attiva/passiva con sincronizzazione dello stato, DPI attiva/attiva e clustering attivo/attivo ad alta disponibilità. La modalità DPI attiva/attiva trasferisce il carico di lavoro dell'ispezione deep packet ai core dell'appliance passiva per ottimizzare il throughput.
Bilanciamento del carico WAN	Bilancia il carico su più interfacce WAN con metodi basati sulle modalità round robin, percentuale e spill-over.
Routing basato sulle policy	Crea degli instradamenti basati sui protocolli per dirigere il traffico verso una connessione WAN specifica, con possibilità di commutare su una WAN secondaria in caso di caduta dell'alimentazione.
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.

Gestione e reporting

Funzionalità	Descrizione
Global Management System (GMS)	Dell SonicWALL GMS consente di monitorare, configurare e creare report per svariate appliance Dell SonicWALL da un'unica console di gestione dotata di un'interfaccia intuitiva, riducendo i costi di gestione e la complessità.
Potente gestione dei singoli dispositivi	Un'intuitiva interfaccia basata sul Web, un'interfaccia a riga di comando (CLI) completa e il supporto per SNMPv2/3 permettono una configurazione semplice e conveniente.
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 Dell SonicWALL Scrutinizer o altri tool che supportano IPFIX e NetFlow con estensioni.

Rete privata virtuale (VPN)

Funzionalità	Descrizione
VPN IPSec per connettività site-to-site	La VPN IPSec ad alte prestazioni consente alla serie NSA di agire come un concentratore VPN per migliaia di altri grandi ambienti di rete, home office o sedi distaccate.
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.

Funzionalità

Protezione basata su contenuto/contesto

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.
Filtraggio DPI basato su espressioni regolari	Previene le fughe di dati identificando e controllando i contenuti che attraversano la rete in base a corrispondenze con espressioni regolari.

Riepilogo delle funzionalità di SonicOS

Firewall
- Ispezione RFDPI (Reassembly-Free Deep Packet Inspection)
- Ispezione Deep Packet per SSL
- Ispezione Stateful Packet
- Riassemblaggio TCP
- Modalità Stealth
- Supporto CAC (Common Access Card)
- Protezione da attacchi DoS
- Protezione da attacchi UDP/ICMP/SYN flood

Prevenzione delle intrusioni
- Scansione basata sulle firme
- Aggiornamenti automatici delle firme
- Prevenzione delle minacce in uscita
- Lista di esclusione IPS
- Geolocalizzazione (GeoIP) e filtraggio basato sulla reputazione
- Corrispondenza con espressioni regolari

Anti-Malware
- Scansione anti-malware basata sui flussi
- Gateway anti-virus
- Gateway anti-spyware
- Decrittazione SSL
- Ispezione bidirezionale
- File senza limiti di dimensioni
- Database di minacce CloudAV

Controllo delle applicazioni
- Controllo delle applicazioni
- Blocco di componenti delle applicazioni
- Gestione della larghezza di banda delle applicazioni
- Creazione di firme per applicazioni personalizzate
- Visualizzazione del traffico delle applicazioni
- Prevenzione delle fughe di dati
- Creazione di report sulle applicazioni tramite NetFlow/IPFIX
- Monitoraggio delle attività degli utenti (SSO)
- Ampio database di firme delle applicazioni

Filtraggio dei contenuti Web
- Filtraggio URL
- Tecnologia anti-proxy
- Blocco in base a parole chiave
- Gestione della banda secondo categorie di valutazione CFS
- Modello di policy unificato con controllo delle applicazioni
- 56 categorie di filtraggio dei contenuti

VPN
- VPN IPSec per connettività site-to-site
- Accesso remoto tramite VPN SSL o client IPSec
- Gateway VPN ridondante
- Mobile Connect per Apple® iOS e Google® Android™
- VPN basato su routing (OSPF, RIP)

Networking
- Routing dinamico
- Controller wireless SonicPoint*
- Routing basato su policy
- NAT avanzato
- Server DHCP
- Gestione della larghezza di banda
- Aggregazione dei link
- Ridondanza delle porte
- Alta disponibilità A/P con State Sync
- Clustering A/A
- Bilanciamento del carico in entrata/in uscita
- Modalità Bridge (L2), Wire, Tap, NAT

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

Gestione e monitoraggio
- GUI basata sul Web
- Interfaccia a riga di comando (CLI)
- SNMPv2/v3
- Creazione di report su altri tool (Scrutinizer)
- Gestione e reporting centralizzati
- Logging
- Esportazione verso Netflow/IPFix
- Visualizzazione del traffico delle applicazioni
- Display di gestione LCD
- Gestione centralizzata delle policy
- Single Sign-On (SSO)
- Supporto Terminal Service/Citrix
- Integrazione con soluzioni di analisi forense di Solera Networks

Specifiche di sistema della serie NSA

	NSA 3600	NSA 4600	NSA 5600	NSA 6600
Sistema operativo	SonicOS 6.1			
Core di sicurezza	6	8	10	24
Interfacce 10 GbE	2 x 10 GbE SFP+			4 x 10 GbE SFP+
Interfacce 1 GbE	4 x 1 GbE SFP, 12 x 1 GbE			8 x 1 GbE SFP, 8 x 1 GbE (1 coppia LAN Bypass)
Interfacce di gestione	1 GbE, 1 Console			
Memoria (RAM)	2,0 GB	2,0 GB	4,0 GB	4,0 GB
Espansione	1 slot di espansione (sul retro)*, scheda SD*			
Throughput ispezione firewall[1]	3,4 Gbps	6,0 Gbps	9,0 Gbps	12,0 Gbps
Throughput DPI completa[2]	500 Mbps	800 Mbps	1,6 Gbps	3,0 Gbps
Throughput ispezione applicazioni[2]	1,1 Gbps	2,0 Gbps	3,0 Gbps	4,5 Gbps
Throughput IPS[2]	1,1 Gbps	2,0 Gbps	3,0 Gbps	4,5 Gbps
Throughput ispezione anti-malware[2]	600 Mbps	1,1 Gbps	1,7 Gbps	3,0 Gbps
Throughput IMIX[3]	900 Mbps	1,6 Gbps	2,4 Gbps	3,5 Gbps
Ispezione e decrittazione SSL (DPI SSL)[2]	300 Mbps	500 Mbps	800 Mbps	1,3 Gbps
Throughput VPN[3]	1,5 Gbps	3,0 Gbps	4,5 Gbps	5,0 Gbps
Connessioni al secondo	20.000/sec	40.000/sec	60.000/sec	90.000/sec
Connessioni massime (SPI)	325.000	500.000	750.000	1.000.000
Connessioni massime (DPI)	175.000	250.000	500.000	600.000
SonicPoint supportati (max.)	48	64	96	96
VPN				
Tunnel site-to-site	800	1.500	4.000	6.000
Client VPN IPSec (max.)	50 (1.000)	500 (3.000)	2.000 (4.000)	2.000 (6.000)
Licenze SSL VPN (max.)	2 (30)	2 (30)	2 (50)	2 (50)
Crittografia / autenticazione	DES, 3DES, AES (a 128, 192, 256 bit)/MD5, SHA-1			
Scambio chiavi	Gruppi Diffie-Hellman 1, 2, 5, 14			
VPN basato su routing	RIP, OSPF			
Networking				
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			
Protocolli di routing	BGP, OSPF, RIPv1/v2, route statici, routing basato su policy, multicast			
QoS	Priorità larghezza di banda, larghezza di banda massima / garantita, DSCP marking, 802.1p			
Autenticazione	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, database interno degli utenti, Terminal Services, Citrix			
VoIP	H323-v1-5 completo, SIP			
Standard	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3			
Certificazioni	VPNC, ICSA Firewall, ICSA Anti-Virus			
Certificazioni (in attesa)	FIPS 140-2, Common Criteria EAL1+			
CAC (Common Access Card)	In attesa di approvazione			
Hardware				
Alimentazione	Singolo alimentatore fisso, 250W			
Ventilazione	2 ventole fisse			2 ventole ridondanti, sostituibili a caldo
Tensione d'esercizio	100-240 VAC, 60-50 Hz			
Potenza max. assorbita (W)	74,3	86,7	90,9	113,1
Fattore di forma	1U rack-mount			
Misure	43,3x48,5x4,5 cm			
Peso	6,15 kg			6,77 kg
Peso sec. WEEE	6,46 kg			8,97 kg
Peso confezione	9,43 kg			11,85 kg
Principali normative di conformità	FCC Class A, CE, C-Tick, VCCI, KCC, UL, cUL, TÜV/GS, CB, NOM, RoHS, WEEE, ANATEL, BSMI			
Condizioni ambientali	da 0 a 40 °C			
Umidità	10-90%, non condensante.			

[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 per DPI completa/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. [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.

Informazioni per l'ordinazione della serie NSA

Prodotto	Codice
NSA 3600, 2 porte 10 GbE SFP+, 4 porte 1 GbE SFP, 12 porte 1 GbE in rame	01-SSC-3850
NSA 4600, 2 porte 10 GbE SFP+, 4 porte 1 GbE SFP, 12 porte 1 GbE in rame	01-SSC-3840
NSA 5600, 2 porte 10 GbE SFP+, 4 porte 1 GbE SFP, 12 porte 1 GbE in rame	01-SSC-3830
NSA 6600, 4 porte 10 GbE SFP+, 8 porte 1 GbE SFP, 8 porte 1 GbE in rame	01-SSC-3820
NSA 3600 – Supporto e abbonamenti ai servizi di protezione	**Codice**
Comprehensive Gateway Security Suite – Application Intelligence, prevenzione delle minacce, filtraggio dei contenuti con supporto per 3600 (1 anno)	01-SSC-4429
Prevenzione delle minacce – Prevenzione delle intrusioni, gateway anti-virus, gateway anti-spyware, cloud anti-virus per 3600 (1 anno)	01-SSC-4435
Supporto Silver 24x7 per NSA 3600 (1 anno)	01-SSC-4302
Content Filtering, edizione Premium Business per 3600 (1 anno)	01-SSC-4441
Comprehensive Anti-Spam Service per NSA 3600 (1 anno)	01-SSC-4447
NSA 4600 – Supporto e abbonamenti ai servizi di protezione	**Codice**
Comprehensive Gateway Security Suite – Application Intelligence, prevenzione delle minacce, filtraggio dei contenuti con supporto per 4600 (1 anno)	01-SSC-4405
Prevenzione delle minacce – Prevenzione delle intrusioni, gateway anti-virus, gateway anti-spyware, cloud anti-virus per 4600 (1 anno)	01-SSC-4411
Supporto Silver 24x7 per NSA 4600 (1 anno)	01-SSC-4290
Content Filtering, edizione Premium Business per 4600 (1 anno)	01-SSC-4417
Comprehensive Anti-Spam Service per NSA 4600 (1 anno)	01-SSC-4423
NSA 5600 – Supporto e abbonamenti ai servizi di protezione	**Codice**
Comprehensive Gateway Security Suite – Application Intelligence, prevenzione delle minacce, filtraggio dei contenuti con supporto per 5600 (1 anno)	01-SSC-4234
Prevenzione delle minacce – Prevenzione delle intrusioni, gateway anti-virus, gateway anti-spyware, cloud anti-virus per 5600 (1 anno)	01-SSC-4240
Supporto Gold 24x7 per NSA 5600 (1 anno)	01-SSC-4284
Content Filtering, edizione Premium Business per 5600 (1 anno)	01-SSC-4246
Comprehensive Anti-Spam Service per NSA 5600 (1 anno)	01-SSC-4252
NSA 6600 – Supporto e abbonamenti ai servizi di protezione	**Codice**
Comprehensive Gateway Security Suite – Application Intelligence, prevenzione delle minacce, filtraggio dei contenuti con supporto per 6600 (1 anno)	01-SSC-4210
Prevenzione delle minacce – Prevenzione delle intrusioni, gateway anti-virus, gateway anti-spyware, cloud anti-virus per 6600 (1 anno)	01-SSC-4216
Supporto Gold 24x7 per NSA 6600 (1 anno)	01-SSC-4278
Content Filtering, edizione Premium Business per 6600 (1 anno)	01-SSC-4222
Comprehensive Anti-Spam Service per NSA 6600 (1 anno)	01-SSC-4228
Moduli e accessori*	**Codice**
Modulo a corto raggio (Short Reach) 10GBASE-SR SFP+	01-SSC-9785
Modulo a lungo raggio (Long Reach) 10GBASE-LR SFP+	01-SSC-9786
Cavo Twinax 10GBASE SFP+ 1M	01-SSC-9787
Cavo Twinax 10GBASE SFP+ 3M	01-SSC-9788
Modulo a corta distanza (Short Haul) 1000BASE-SX SFP	01-SSC-9789
Modulo a lunga distanza (Long Haul) 1000BASE-LX SFP	01-SSC-9790
Modulo in rame 1000BASE-T SFP	01-SSC-9791
Gestione e reporting	**Codice**
Licenza software per Dell SonicWALL GMS (10 nodi)	01-SSC-3363
Supporto software E-Class 24x7 per Dell SonicWALL GMS 10 nodi (1 anno)	01-SSC-6514
Dell SonicWALL Scrutinizer Virtual Appliance con licenza per modulo software Flow Analytics (fino a 5 nodi) (comprensivo di supporto software 24x7 per 1 anno)	01-SSC-3443
Dell SonicWALL Scrutinizer con licenza per modulo software Flow Analytics (fino a 5 nodi) (comprensivo di supporto software 24x7 per 1 anno)	01-SSC-4002
Dell SonicWALL Scrutinizer con licenza per modulo software Advanced Reporting (fino a 5 nodi) (comprensivo di supporto software 24x7 per 1 anno)	01-SSC-3773

*Per un elenco completo dei moduli SFP e SFP+ supportati, contattare un ingegnere di sistemi Dell.

SonicWALL