Firewall della serie Dell SonicWALL Network Security Appliance (NSA)

Opportunità

- Piccole, medie e grandi imprese emergenti che necessitano di una protezione di rete completa e ad alte prestazioni con funzionalità di rete versatili
- Sedi e filiali di aziende distribuite che richiedono una gestione centralizzata con un solido approccio di sicurezza globale
- Alternativa a dispositivi Cisco e altri firewall obsoleti per le minacce attuali (per i punti deboli dell'ispezione Stateful Packet, vedere Perché scegliere Dell™ SonicWALL™ qui di seguito)

Problemi/punti critici del cliente

- Il vostro firewall esistente è ormai obsoleto. I tradizionali firewall con ispezione Stateful Packet offrono una protezione minima contro le moderne e sofisticate minacce come malware e botnet
- La diffusione di applicazioni web-based rende difficile visualizzare e distinguere le applicazioni produttive da quelle non produttive
- Le prestazioni della vostra rete sono mediocri e avete poche possibilità di vedere e controllare cosa succede nella rete
- La vostra azienda ha aperto nuove sedi e avete difficoltà a implementare, monitorare e gestire separatamente i firewall in ogni sede
- La vostra organizzazione è passata a una rete Ethernet a 10 Gb

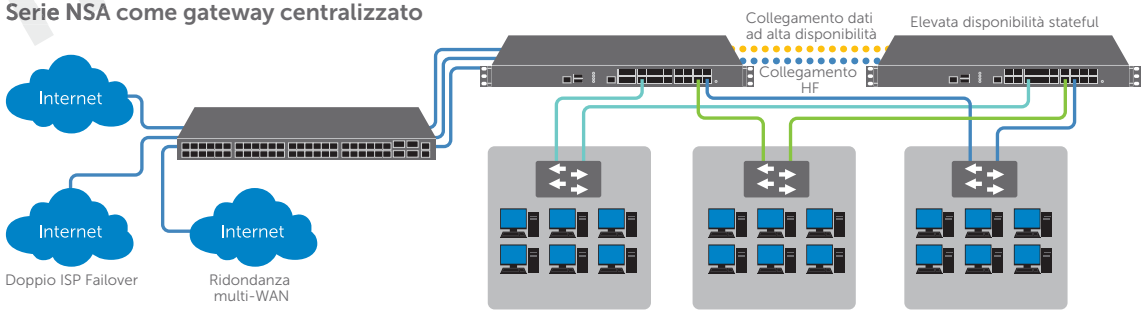
Principali destinatari

- Amministratori IT che sostituiscono infrastrutture di rete obsolete, consolidando diverse soluzioni singole in un'unica piattaforma che combina la sicurezza con funzioni di networking
- PMI alla ricerca di una potente protezione della rete
- Attività al dettaglio che devono conformarsi ai requisiti PCI e cercano funzioni ad alta disponibilità
- Reti distribuite che richiedono un basso TCO e gestione centralizzata

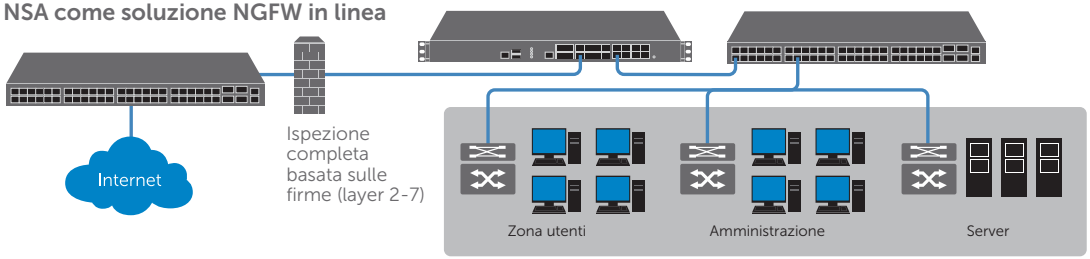
Vantaggi – Perché scegliere Dell SonicWALL

- **Architettura d'ispezione Deep Packet (DPI) ad altissime prestazioni:** offre prevenzione delle intrusioni, anti-malware e controllo delle applicazioni senza rallentare la rete
- **Protezione completa della rete con l'ispezione DPI:** scansiona tutto il traffico (file di ogni dimensione, senza latenze o buffering/proxying) su ogni porta, e non su poche porte selezionate. L'ispezione stateful non esamina i pacchetti di dati completi, lasciando la rete vulnerabile al malware che è nascosto dove l'ispezione stateful non può rilevarlo
- **Visualizzazione e controllo del traffico delle applicazioni:** analizza e rileva consumi di banda eccessivi e controlla il traffico tramite potenti signature in base a utente, gruppo, orario pianificato
- **Controller wireless sicuro:** garantisce connettività 802.11 a/b/g/n sicura con i punti di accesso SonicWALL completamente controllati e gestiti dal firewall
- **Vantaggi del consolidamento:** consente di eliminare apparecchiature e spese inutili, integrando firewall, IPS, gateway anti-malware, SSL VPN, filtraggio web, analisi del flusso di traffico delle applicazioni e altro in un unico dispositivo
- **Ampio supporto di dispositivi per l'accesso remoto:** connettività SSL VPN da dispositivi Windows, Apple® Mac OS, iOS, Google® Android™ e Linux®

Serie NSA come gateway centralizzato



Serie NSA come soluzione NGFW in linea



Firewall della serie Dell SonicWALL Network Security Appliance (NSA)

Domande di valutazione

1. Attualmente utilizzate la tecnologia d'ispezione Stateful Packet, che analizza solo le intestazioni dei pacchetti senza identificare le minacce nascoste nel payload dei pacchetti?
2. Sapete quali applicazioni girano nella vostra rete, in modo da poter assegnare priorità alle applicazioni aziendali e limitare o bloccare quelle improduttive?
3. Vorreste prevenire gli attacchi diretti a browser web o applicazioni Java o Flash e proteggervi da documenti maligni che introducono malware nella vostra rete?
4. Avete la necessità di gestire più firewall da un'unica postazione e creare policy unitarie per tutte le reti (sia wireless che cablate) della vostra azienda?
5. Avete aggiornato la vostra rete a 10 GbE o installato nuovi switch?

Concorrenza/fattori di differenziazione*

Cisco®

- Cisco vende la linea di firewall ASA-X, che non offre ai clienti la protezione completa garantita dai firewall di nuova generazione
- Cisco sfrutta la notorietà del proprio brand per vendere costosi contratti di supporto e assistenza
- La serie ASA-X di Cisco è ancora basata su moduli hardware separati per l'anti-malware e il controllo delle applicazioni, obbligando il cliente a scegliere tra i due moduli
- La serie ASA-X di Cisco ha un TCO molto più alto e, a parità di prezzo, offre molte meno funzionalità rispetto ai prodotti Dell SonicWALL
- La serie ASA-X di Cisco non ha ottenuto la valutazione "NSS Recommended" per nessun prodotto firewall o IPS

Fortinet®

- Fortinet compete con Dell SonicWALL nella superiorità a Cisco, ma offre prestazioni scarse a livello di DPI e ha limitazioni sulle dimensioni dei file da ispezionare (i file di grandi dimensioni non vengono ispezionati)
- Fortinet utilizza principalmente l'ispezione stateful packet, che è inadeguata per le minacce odierne
- Fortinet non offre la visualizzazione delle applicazioni e, di fatto, nessuna funzionalità di controllo delle applicazioni

Palo Alto Networks®

- Palo Alto Networks offre connessioni Ethernet a 10 Gb solo sui costosi firewall di fascia alta
- Palo Alto Networks non offre prodotti adatti alle esigenze di filiali e piccole sedi remote
- Palo Alto Networks non fornisce funzionalità come il wireless, obbligando i clienti ad acquistare prodotti e console gestionali di altri produttori
- Dell SonicWALL ha un TCO nettamente migliore, in particolare nel mercato di fascia media

Check Point®

- Check Point non offre connessioni di rete ad alta velocità (come Ethernet 10 Gb) per i clienti PMI che desiderano potenziare le loro reti
- Check Point ha costi di rinnovo elevati e, di conseguenza, un TCO più alto

*Al 5/13

Tabella di comparazione della serie Dell SonicWALL Network Security Appliance (NSA)

Funzionalità	NSA 220	NSA 250M	NSA 2400	NSA 3600	NSA 4600	NSA 5600	NSA 6600
Throughput firewall[1]	600 Mbps	750 Mbps	775 Mbps	3,4 Gbps	6,0 Gbps	9,0 Gbps	12,0Gbps
Throughput IPS[2]	195 Mbps	250 Mbps	275 Mbps	1,1 Gbps	2,0 Gbps	3,0 Gbps	4,5 Gbps
Throughput DPI completa[2]	110 Mbps	130 Mbps	150 Mbps	500 Mbps	800 Mbps	1,6 Gbps	3,0 Gbps
Connessioni massime (DPI)	85.000	110.000	225.000	175.000	250.000	500.000	600.000
Tunnel VPN	25	50	75	800	1.500	4.000	6.000
Interfacce	(7) GbE	(5) GbE, modulo di espansione	(6) GbE	2 x 10 GbE SFP+ 4 x 1 GbE SFP, 12 x 1 GbE 1 interfaccia di gestione GbE, modulo di espansione	2 x 10 GbE SFP+ 4 x 1 GbE SFP, 12 x 1 GbE 1 interfaccia di gestione GbE, modulo di espansione	2 x 10 GbE SFP+ 4 x 1 GbE SFP, 12 x 1 GbE 1 interfaccia di gestione GbE, modulo di espansione	4 x 10 GbE SFP+ 8 x 1 GbE SFP, 8 x 1 GbE 1 interfaccia di gestione GbE modulo di espansione

[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. Specifiche, funzionalità e disponibilità soggette a modifiche.