SCHEDA DI
RICERCA CLIENTI

Firewall della serie SonicWALL Network Security Appliance (NSA)

Opportunità di mercato

- Le piccole/medie imprese necessitano di un firewall con sicurezza avanzata, prestazioni elevate e numerose funzioni di networking
- Le varie sedi di aziende distribuite richiedono una gestione centralizzata e un solido approccio di sicurezza globale
- Alternativa a dispositivi Cisco e altri firewall obsoleti con ispezione stateful packet, inadeguati per le minacce attuali

Problemi/punti critici del cliente

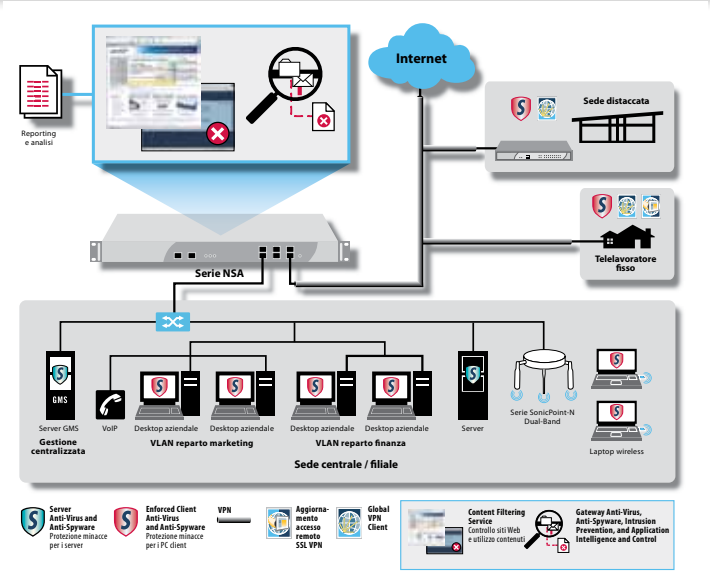
- I tradizionali firewall con ispezione Stateful Packet offrono una protezione minima contro le moderne e sofisticate minacce come malware e botnet
- La diffusione di applicazioni web-based rende difficile visualizzare e distinguere applicazioni produttive da quelle non produttive
- Con l'aggiunta di nuove sedi, le aziende non riescono più a implementare, monitorare e gestire separatamente i firewall in ogni sede

Utenza target

- 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 che cercano 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

I vantaggi di SonicWALL – Perché scegliere SonicWALL

- L'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: scansione di tutto il traffico (file di ogni dimensione, senza latenze o buffering/proxying) su ogni porta, e non su poche porte selezionate
- Visualizzazione e controllo del traffico delle applicazioni: analisi e rilevamento di consumi di banda eccessivi e controllo del traffico tramite potenti signature in base a utente, gruppo, orario pianificato
- Controller wireless sicuro: per una connettività 802.11 a/b/g/n sicura con i punti di accesso SonicWALL completamente controllati e gestiti dal firewall
- Eliminazione di apparecchiature e spese inutili: consolidamento di firewall, IPS, gateway anti-malware, SSL VPN, filtraggio web, analisi del flusso di traffico delle applicazioni e altro
- Supporto client SSL VPN multipiattaforma (Windows, Windows Mobile, Apple Mac OS, iOS, Google Android e Linux)



SONICWALL®
DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

SCHEDA DI
RICERCA CLIENTI

Firewall della serie SonicWALL Network Security Appliance (NSA)

Domande di valutazione

1. Attualmente usate 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 utilizzati per introdurre 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?

Concorrenza/fattori di differenziazione

Cisco

- Cisco offre ancora i firewall della linea ASA con ispezione stateful packet, che presenta falle nella protezione contro le minacce attuali
- Cisco sfrutta la notorietà del proprio brand per vendere costosi contratti di supporto e assistenza

Argomenti vincenti

- Spiegare che i firewall ASA di Cisco non riescono ad offrire prevenzione delle intrusioni e anti-malware simultaneamente
- I firewall ASA di Cisco hanno un TCO molto più alto; inoltre, a parità di prezzo, offrono molte meno funzionalità di SonicWALL

Fortinet

- Fortinet compete con SonicWALL nella superiorità a Cisco, ma ha gravi problemi di prestazioni a livello di DPI
- Fortinet utilizza principalmente l'ispezione stateful packet, che è inadeguata per le minacce odierne

Argomenti vincenti

- Fortinet offre prestazioni inadeguate per la prevenzione delle intrusioni e l'anti-malware
- Fortinet non offre la visualizzazione delle applicazioni e, di fatto, nessuna funzionalità di controllo delle applicazioni

Juniper

- La linea di firewall SRX di Juniper è basata su un sistema operativo router con funzioni di sicurezza annesse, che può creare potenziali colli di bottiglia e aumenta la complessità di gestione

Argomenti vincenti

- Il sistema JunOS di Juniper è estremamente complesso da installare, configurare e manutenere
- La serie SRX di Juniper è basata su proxy e offre prestazioni scarse quando si attivano i servizi DPI

Tabella di comparazione della serie Network Security Appliance (NSA)

Funzionalità	NSA 220/W-N	NSA 250M/W-N	NSA 2400/2400MX	NSA 3500	NSA 4500
Prestazioni firewall	600 Mbps	750 Mbps	775 Mbps	1,5 Gbps	2,75 Gbps
Prestazioni IPS	195 Mbps	250 Mbps	275 Mbps	750 Mbps	1,4 Gbps
Prestazioni DPI (protezione completa)	110 Mbps	130 Mbps	150 Mbps	240 Mbps	600 Mbps
Connessioni	85.000	110.000	225.000	325.000	500.000
Tunnel VPN	25	50	75	800	1.500
Interfacce	(7) 10/100/1000 GbE, 2 USB, console	(5) 10/100/1000 GbE, interfaccia modulo, 2 USB, console	(6) 10/100/1000 GbE, console	(6) 10/100/1000 GbE, 2 USB, console	(6) 10/100/1000 GbE, 2 USB, console

11/11 SW1489

SONICWALL®
DYNAMIC SECURITY FOR THE GLOBAL NETWORK™