

SonicWALL



Intrusion  
Prevention  
Service

## SonicWALL Intrusion Prevention Service

- ▷ Utilizza un motore d'ispezione deep packet configurabile e ad altissime prestazioni, per la massima protezione della rete
- ▷ Offre un database aggiornato dinamicamente con oltre 1.700 signature di attacchi e vulnerabilità
- ▷ Previene le vulnerabilità conosciute di buffer overflow nel software e diversi worm, cavalli di Troia ed exploit tramite backdoor
- ▷ Gestisce l'uso delle applicazioni di instant messaging e peer-to-peer, riducendo rischi e responsabilità legali e aumentando la produttività
- ▷ Protegge la rete dagli attacchi provenienti sia dall'esterno (WAN) che da sezioni interne della LAN

I tentativi di intrusione in rete effettuati ogni giorno dagli hacker diventano sempre più sofisticati. Negli ultimi anni, gli attacchi maligni indirizzati alle vulnerabilità delle applicazioni, come Nimda, Code Red, SQL Slammer e MS Blaster hanno infettato computer in tutto il mondo. Più di recente, le minacce sono arrivate tramite applicazioni peer-to-peer e di instant messaging. A causa della natura sempre più dinamica e dannosa di questi attacchi, per le aziende è indispensabile utilizzare soluzioni firewall che offrano il massimo grado di rilevazione e prevenzione

SonicWALL® IPS è un servizio di prevenzione delle intrusioni scalabile, in grado di offrire protezione completa dagli exploit alle applicazioni e dal traffico anomalo su tutti i segmenti della rete. Dotato di un motore di ispezione deep packet configurabile e ad altissime prestazioni e di un database aggiornato dinamicamente con oltre 1.700 signature, SonicWALL IPS protegge dalle vulnerabilità conosciute di buffer overflow nel software, da diversi worm e cavalli di Troia, exploit di applicazioni e dall'uso di applicazioni peer-to-peer e di instant messaging. Il linguaggio estendibile delle signature utilizzato nel motore di ispezione approfondita dei pacchetti (deep packet inspection) fornisce una difesa proattiva contro le vulnerabilità delle applicazioni scoperte di recente.

Il rischio di un attacco dall'interno della rete è ormai probabile quanto un attacco dall'esterno. La protezione delle informazioni confidenziali da un accesso non autorizzato attraverso i vari reparti aziendali è di importanza critica. SonicWALL IPS offre agli amministratori di rete gli strumenti per migliorare la prevenzione delle intrusioni, non solo tra la rete aziendale e Internet, ma anche tra sezioni interne della rete (Figura 3). Il servizio di prevenzione delle intrusioni risolve anche potenziali vulnerabilità interne bloccando l'uso di applicazioni di instant messaging e file sharing peer-to-peer, chiudendo così eventuali backdoor che potrebbero compromettere la sicurezza della rete.

L'ampio database di signature di SonicWALL IPS è adattabile alle esigenze di reti di tutte le dimensioni. L'impostazione individuale delle signature, combinata alla possibilità di configurare un serie di policy di rilevamento o prevenzione per ogni zona di rete, riduce il numero di falsi positivi riscontrato in altre soluzioni di prevenzione delle intrusioni.

SonicWALL IPS crea un registro di tutti i tentativi di intrusione, con l'opzione di filtrare gli attacchi subito in base al livello di priorità. Sia ViewPoint® che il Global Management System di SonicWALL offrono funzioni di reporting granulare in base alla fonte e alla destinazione dell'attacco e al tipo di intrusione, per una visione dettagliata delle attività maligne in qualsiasi punto della rete.

Le potenti prestazioni, le innovative funzionalità e le opzioni di gestione avanzata del servizio di prevenzione delle intrusioni SonicWALL IPS garantiscono alle aziende la protezione completa della rete a un costo di proprietà totale contenuto.

### ARCHITETTURA DI ISPEZIONE DEEP PACKET SONICWALL

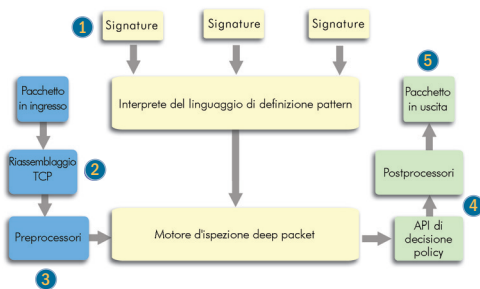


Figura 1)

- 1) È possibile definire signature che riconoscono e offrono protezione contro protocolli noti e ignoti, applicazioni ed exploit.
- 2) I pacchetti TCP che arrivano in ordine non corretto vengono riassemblati dal framework di ispezione approfondita.
- 3) Durante la preelaborazione viene normalizzato il payload del pacchetto.
- 4) I postprocessori possono lasciar passare il pacchetto senza modifiche, scartarlo o reimpostare la connessione TCP.
- 5) L'architettura di ispezione deep packet SonicWALL supporta il confronto completo delle firme tra i frammenti TCP senza necessità di riassemblaggio (se i pacchetti arrivano nell'ordine corretto).

## CARATTERISTICHE E VANTAGGI DI SONICWALL INTRUSION PREVENTION SERVICE (IPS)

**Tecnologia di ispezione deep packet integrata.** SonicWALL IPS è dotato di un motore di ispezione deep packet configurabile e ad altissime prestazioni che, mediante l'uso di algoritmi di ricerca parallela fino al livello dell'applicazione, offre funzioni di prevenzione degli attacchi superiori rispetto ai tradizionali firewall a tecnologia Stateful Packet Inspection. L'elaborazione parallela riduce l'impatto sulle prestazioni del firewall, aumentando così l'efficienza della memoria e il livello di throughput dei dispositivi SonicWALL.

**Prevenzione delle intrusioni dall'interno.** Un ulteriore livello di protezione dagli attacchi maligni è offerto dalla possibilità di applicare la prevenzione delle intrusioni non solo tra la rete aziendale e Internet, ma anche tra sezioni interne della rete.

**Ampio database di signature.** SonicWALL IPS utilizza un database con oltre 1.700 firme che rilevano il pericolo e offrono protezione contro gli exploit alle applicazioni, le vulnerabilità, i worm e l'uso di applicazioni peer-to-peer e di instant messaging. Il database viene costantemente aggiornato da SonicWALL in modo da proteggere le reti dagli exploit anche più recenti.

**Aggiornamento dinamico del database delle signature.** Il database delle signature viene aggiornato automaticamente attraverso l'architettura di applicazione distribuita SonicWALL, garantendo la protezione costante dagli attacchi e riducendo il costo totale di proprietà.

**Soluzione scalabile.** SonicWALL IPS è una soluzione scalabile per i dispositivi SonicWALL TZ 170 e serie PRO che protegge le reti di piccole, medie e grandi dimensioni da exploit di applicazioni, worm e traffico dannoso.

**Controllo delle applicazioni.** SonicWALL IPS consente di monitorare e gestire l'uso di programmi di instant messaging e file sharing peer-to-peer, chiudendo potenziali backdoor utilizzabili per compromettere la sicurezza della rete e aumentando al contempo la produttività e la larghezza di banda disponibile.

**Distribuzione e gestione semplificata.** Grande semplicità di implementazione e gestione nelle reti distribuite grazie alla possibilità di creare policy globali tra le zone di sicurezza e classificare gli attacchi in base alla priorità.

**Gestione granulare.** Grazie all'intuitiva interfaccia utente e alla configurabilità granulare delle policy, gli amministratori di rete possono creare una serie preconfigurata di policy di rilevamento o prevenzione per il proprio ambiente di rete e ridurre il numero di falsi positivi, identificando le minacce immediate.

**Funzioni di logging e reporting.** SonicWALL IPS crea un registro completo di tutti i tentativi di intrusione, con l'opzione di filtraggio in base a livelli di priorità. Il reporting granulare in base alla fonte e alla destinazione dell'attacco e al tipo di intrusione è disponibile tramite ViewPoint e Global Management System di SonicWALL.

## PREVENZIONE DELLE INTRUSIONI SONICWALL

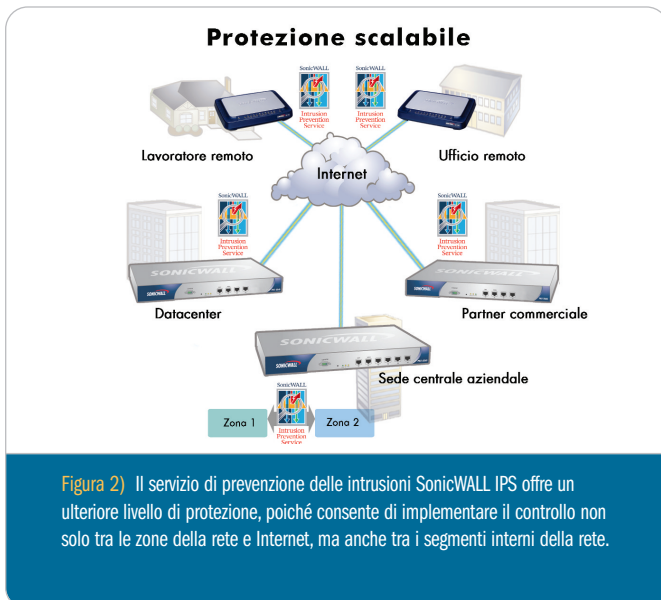


Figura 2) Il servizio di prevenzione delle intrusioni SonicWALL IPS offre un ulteriore livello di protezione, poiché consente di implementare il controllo non solo tra le zone della rete e Internet, ma anche tra i segmenti interni della rete.



Figura 3) SonicWALL IPS è una soluzione scalabile per i dispositivi SonicWALL TZ 170 e serie PRO, che fornisce protezione completa da exploit di applicazioni, worm e traffico anomalo per tutte le connessioni Internet e VPN.

## REQUISITI MINIMI DI SISTEMA PER SONICWALL INTRUSION PREVENTION SERVICE

Dispositivo di sicurezza Internet TZ 170 o della serie PRO SonicWALL con firmware SonicOS 2.2 o superiore

## CODICI PRODOTTO DI SONICWALL INTRUSION PREVENTION SERVICE

- 01-SSC-5750 SonicWALL Intrusion Prevention Service, versione base per TZ 170, 10 nodi, 1 anno (non include supporto delle signature a livello di applicazione per server)
- 01-SSC-5751 SonicWALL Intrusion Prevention Service per TZ 170, 1 anno
- 01-SSC-5757 SonicWALL Intrusion Prevention Service per PRO 2040, 1 anno
- 01-SSC-5758 SonicWALL Intrusion Prevention Service per PRO 3060, 1 anno
- 01-SSC-5759 SonicWALL Intrusion Prevention Service per PRO 4060, 1 anno

Per ulteriori informazioni sul Servizio di prevenzione delle intrusioni SonicWALL IPS e la nostra linea completa di servizi per la sicurezza, visitare <http://www.sonicwall.com/products/vpnsoft.html>.

### SonicWALL, Inc.

1143 Borregas Avenue Tel.: +1 408.745.9600 www.sonicwall.com  
Sunnyvale, CA 94089-1306 Fax: +1 408.745.9300

© 2004 SonicWALL, Inc. SonicWALL è un marchio registrato di SonicWALL, Inc. I nomi di altri prodotti o società qui menzionati possono essere marchi e/o marchi registrati delle rispettive società. Con riserva di modifiche.  
DS\_0404\_IPS\_A4 / F067\_IPS\_DS\_A4\_v1



I dispositivi SonicWALL per la sicurezza in Internet certificati ICSA ottengono costantemente riconoscimenti da parte delle pubblicazioni leader del settore.

**Siosistemi**  
PEOPLE YOU CAN TRUST  
Distributore per l'Italia:  
SIOSISTEMI SPA  
Via Cefalonia 58 - 25124 Brescia  
Tel. +39 030 24411 - Fax +39 030 2441600

**SONICWALL**