

Intrusion Prevention Service (IPS) opera in tandem con la funzione di ispezione dei contenuti al livello applicativo WatchGuard XTM per offrire protezione in tempo reale contro le minacce alla rete, inclusi attacchi SQL injection, XSS (cross-site scripting) e overflow del buffer.

Perché aggiungere un abbonamento IPS
IPS analizza il traffico su tutti i principali protocolli, utilizzando firme aggiornate continuamente per rilevare e bloccare tutti i tipi di minacce. E poiché IPS è integrato con le appliance di sicurezza WatchGuard XTM, costituisce una soluzione economica e facile da gestire, che non richiede l'acquisto e la manutenzione di hardware aggiuntivo.

Tre dei motivi più validi per aggiungere Intrusion Prevention Service alla vostra soluzione per la sicurezza: attacchi XSS (cross-site scripting), attacchi SQL injection e overflow del buffer.

Intrusion Prevention Service

Un abbonamento di sicurezza integrato per le appliance WatchGuard® XTM



IPS arresta gli attacchi alla rete

La funzione di ispezione del contenuto in base ai livelli applicativi di cui sono dotate le appliance WatchGuard XTM protegge contro gli attacchi alla rete quali spoofing, flood e DOS (denial of service). Intrusion Prevention Service aggiunge un altro livello di protezione con la rilevazione basata su firma delle intrusioni nella rete.

Le intrusioni nella rete vengono identificate e bloccate

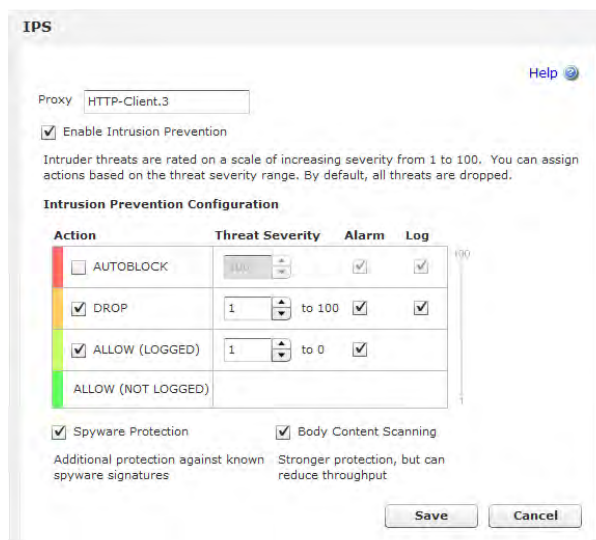
- Protezione completa contro un'ampia gamma di esposizioni e vulnerabilità note della sicurezza delle informazioni in applicazioni, database e sistemi operativi.
- Oltre 15.000 firme coprono un'ampia gamma di minacce, inclusi attacchi SQL injection, XSS (cross-site scripting), overflow del buffer, DSO (denial of service) e inclusioni di file remote.
- Il database delle firme aggiornato continuamente assicura una copertura tempestiva e ad ampio raggio. Vengono rilasciate nuove firme a mano a mano che emergono nuove minacce.
- Analizza tutti i protocolli più importanti, inclusi HTTP, HTTPS, FTP, TCP, UDP, DNS, SMTP e POP3, per bloccare attacchi di rete, alle applicazioni e basati sul protocollo.
- Impedisce allo spyware di insinuarsi nella rete bloccando lo spyware drive-by durante la navigazione e identificando lo spyware che cerca di contattare il suo host.

Controllo granulare sulla risposta alle minacce

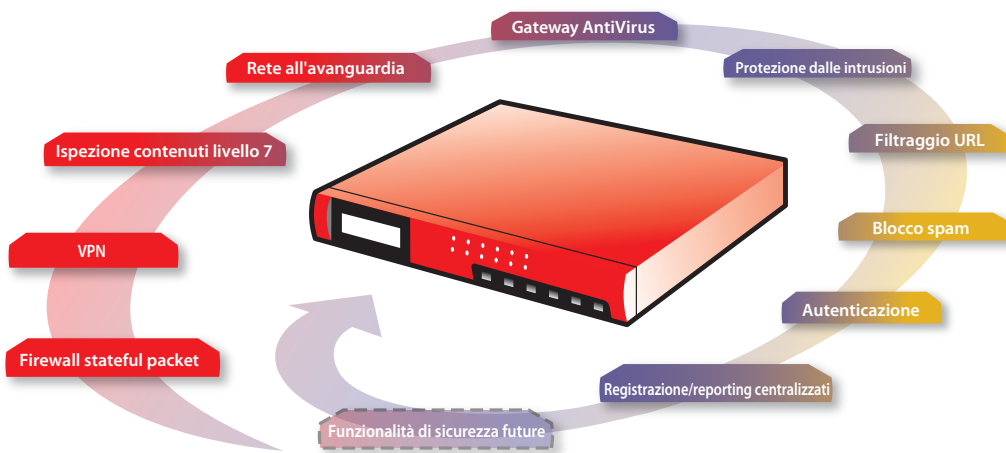
- Potete assegnare specifiche azioni da intraprendere a seconda del livello della minaccia. A ciascuna firma è assegnato un livello di gravità.
- Gli indirizzi IP identificati come fonte di un attacco possono essere bloccati automaticamente per impedire che ulteriore traffico maligno entri nella rete.
- L'elenco di siti bloccati assicura che una volta identificato con certezza un indirizzo IP come fonte di un attacco, futuri attacchi provenienti da quell'indirizzo saranno bloccati dinamicamente.
- È possibile escludere firme specifiche. Quando esistono, vengono forniti nomi CVE (Common Vulnerabilities and Exposures) per agevolare la condivisione dei dati tra strumenti separati per la sicurezza della rete.

Prevenzione delle intrusioni a un costo contenuto

- Con un solo abbonamento IPS potete assicurare la protezione a livello dell'intera rete per tutti gli utenti configurati dietro il firewall WatchGuard XTM.
- Per ridurre ulteriormente i costi, potete acquistare IPS nello stesso pacchetto della nostra suite di potenti abbonamenti di sicurezza, che include WebBlocker, spamBlocker, Gateway AntiVirus e LiveSecurity Service con supporto tecnico 24/7.



Sicurezza completamente integrata per una protezione completa



La soluzione per la sicurezza "tutto in uno"

Le appliance WatchGuard XTM sono utilizzabili con potenti abbonamenti di sicurezza per offrire protezione completa contro il malware. Tutte le funzionalità di sicurezza vengono gestite da un'intuitiva console, con funzioni di registrazione e reporting centralizzate, per visualizzare in tempo reale l'attività correlata alla sicurezza della rete.

Poiché il panorama delle minacce cambia continuamente, le soluzioni WatchGuard XTM sono progettate per essere in grado di aggiungere facilmente nuove funzionalità di difesa della rete attraverso appositi abbonamenti, per cui non sono necessari costosi aggiornamenti hardware.

Facile gestione degli abbonamenti di sicurezza

Tutte le funzionalità di sicurezza di cui è dotata la soluzione WatchGuard XTM, tra cui Gateway AntiVirus, possono essere gestite da una sola intuitiva console per la massima efficienza e facilità d'uso.

- Qualsiasi attività correlata alla sicurezza che venga identificata da Gateway AV viene registrata e memorizzata per facilitare il reporting e dar modo di intervenire immediatamente con azioni preventive o correttive.
- Gli amministratori IT hanno la flessibilità di definire l'intervento da effettuare quando il malware viene identificato – consentendo alla rete di permettere il traffico sospetto, bloccarlo o metterlo in quarantena in base al tipo, utente/gruppo e protocollo.
- Tutti gli strumenti di gestione, inclusi monitoraggio e reporting approfondito, sono inclusi con l'acquisto dell'appliance WatchGuard XTM; non occorre acquistare altro hardware o software.

Altri abbonamenti di sicurezza WatchGuard

WatchGuard offre una suite completa di servizi di sicurezza per rafforzare la protezione nelle aree cruciali di attacco. Unitamente a Intrusion Prevention Service, gli abbonamenti includono:

- **WebBlocker**, che filtra i contenuti e gli URL, e insieme all'ispezione HTTP e HTTPS, permette di tenere sotto controllo l'accesso ai siti che ospitano materiale eccezionale o che pongono rischi per la sicurezza delle rete, inclusi siti di spyware e phishing.
- **spamBlocker**, che blocca quasi il 100% delle e-mail indesiderate in tempo reale, prima che possano raggiungere il client o il server di posta interni. Offre un livello aggiuntivo di protezione della rete contro gli attacchi dei virus e include un sistema di quarantena dello spam dalle funzioni complete.
- **Gateway AntiVirus**, che offre protezione in tempo reale contro virus, trojan, worm, spyware e rogueware noti.

Acquistate il pacchetto completo per avere la massima operatività

Tutto quello di cui avete bisogno per la gestione completa delle minacce è disponibile in un comodo pacchetto di sicurezza WatchGuard che include firewall, VPN, abbonamenti di sicurezza e supporto tecnico.

Ciascun pacchetto di sicurezza include:

- Scelta dell'appliance WatchGuard XTM (serie 8 o 10)
- spamBlocker
- WebBlocker
- Gateway AntiVirus
- Intrusion Prevention Service
- Servizio LiveSecurity® che offre supporto tecnico 24/7, garanzia sull'hardware, aggiornamenti software e avvisi delle minacce.

Dall'acquisto iniziale alla gestione continuata della sicurezza, il pacchetto rende più efficiente e agevole garantire la sicurezza della rete. Ottenete così una soluzione completa a un prezzo eccellente, senza ulteriori addebiti, contratti o hardware da acquistare.

Avete l'appliance? Completatela con la suite software per la sicurezza*

Se disponete già di un'appliance WatchGuard XTM, potete trasformarla in una soluzione completa di gestione delle minacce con la suite software per la sicurezza, che include tutti gli abbonamenti di sicurezza elencati sopra, tra cui LiveSecurity che offre supporto tecnico qualificato. Un ottimo affare quando le acquistate insieme e riducete i costi!

*La suite software per la sicurezza non include l'appliance.

Per il pacchetto di sicurezza e la suite software per la sicurezza sono disponibili abbonamenti di uno, due e tre anni.

Contatti: Italy@watchguard.com • Web: www.watchguard.it • Informazioni commerciali Italia: 800-911938

Non sono qui fornite garanzie esplicite o implicite. Tutte le specifiche sono soggette a modifica e tutti i prodotti o le funzionalità futuri saranno forniti in base alla disponibilità. *2010 WatchGuard Technologies, Inc. Tutti i diritti riservati. WatchGuard, il logo WatchGuard e LiveSecurity sono marchi o marchi registrati di WatchGuard Technologies, Inc. negli Stati Uniti e/o in altri Paesi. Tutti gli altri marchi sono di proprietà dei rispettivi titolari. Num. parte WGCE6652_101609