

Blocco di spyware e altre attività sospette in tempo reale

Gateway AntiVirus/Intrusion Prevention Service (Gateway AV/IPS) è un abbonamento di protezione integrato basato su firme per la famiglia Firebox® X di appliance UTM. Opera in tandem con la prevenzione attacchi Zero Day integrata del Firebox X per fornire una protezione superiore in tempo reale nei confronti di noti spyware, virus e attacchi applicativi quali trojan horse, overflow del buffer e iniezioni SQL. Facile da installare e gestire, Gateway AV/IPS mantiene informati su tutta l'attività antispyware, antivirus e di prevenzione intrusioni. Verifica continuamente le firme e aggiorna automaticamente il sistema quando sono disponibili nuove firme.

- **Incremento della protezione Zero Day integrata** per fornire la massima difesa nei confronti di spyware e altre minacce di rete
- **Supporta i protocolli più diffusi**, tra cui HTTP, FTP, SMTP e POP3
- **Blocco di sorgenti di attacco conosciute** per respingere gli attacchi ripetuti
- **Blocco di allegati infetti** per impedire l'esecuzione di codice dannoso sul desktop
- **Aggiornamento automatico delle firme** per una protezione costante
- **Elenco di siti bloccati** per impedire l'accesso ai siti di distribuzione spyware



Tecnologia eco-compatibile

Incremento della protezione integrata Zero Day

L'architettura intelligente multilivello del Firebox X, con protezione dagli attacchi Zero Day proattiva, fornisce già il blocco di numerosi virus, trojan horse, overflow del buffer e altre minacce applicative attraverso le funzionalità di rilevamento anomalie di protocollo e pattern matching. La scansione basata su firme di Gateway AV/IPS si integra con la protezione Zero Day bloccando le minacce veicolate dal traffico non sospetto. La combinazione della protezione Zero Day con la scansione basata su firme fornisce alla rete una serie di difese complete nei confronti di attacchi nocivi.

Protezione granulare dei file e del traffico

Gateway AV/IPS utilizza una scansione basata su firme allo scopo di identificare il codice nocivo conosciuto all'interno di file e traffico business-critical. Sottopone a scansione il traffico HTTP e blocca al gateway i tipi di file associati al malware in maniera tale che le minacce siano fermate prima che riescano ad accedere alla rete e a disattivare la protezione dei PC desktop e del server. Include inoltre difese antispyware integrate per impedire allo spyware di penetrare nella rete. Gateway AV/IPS fornisce flessibilità per consentire, arrestare e bloccare* il traffico sospetto, in base al tipo, all'utente/gruppo*, al protocollo e alla gravità.

Blocco di allegati infetti

Bloccando tutti gli allegati identificati come sospetti, Gateway AV/IPS impedisce l'esecuzione di codice nocivo nel PC desktop. Per fornire la protezione più solida ed efficiente*, Gateway AV/IPS esegue la scansione di una varietà di tipi di file compressi e codificati quali ZIP, TAR e GZIP.

Blocco di sorgenti di attacco conosciute

Una volta che un indirizzo IP è stato

identificato come sorgente di un attacco, i futuri attacchi provenienti da questo IP vengono bloccati in maniera attiva e dinamica. In questo modo è possibile impedire all'ulteriore traffico nocivo di accedere alla rete. Gateway AV/IPS fornisce inoltre whitelist configurabili che consentono di definire i sistemi che non devono venire bloccati. Con applicazioni e destinazioni affidabili disponibili per l'accesso continuato, l'organizzazione può condurre le consuete attività quotidiane.

Impareggiabile facilità di utilizzo

È possibile configurare e mettere in funzione Gateway AV/IPS in pochi minuti: l'interfaccia intuitiva assicura una gestione corrente semplice e lineare. Nelle appliance Firebox X Peak™ e Core™, e nelle appliance Firebox X Edge su reti Peak o Core, Gateway AV/IPS viene gestito tramite il potente WatchGuard System Manager (WSM). Le appliance stand-alone Firebox X Edge utilizzano una intuitiva interfaccia Web.

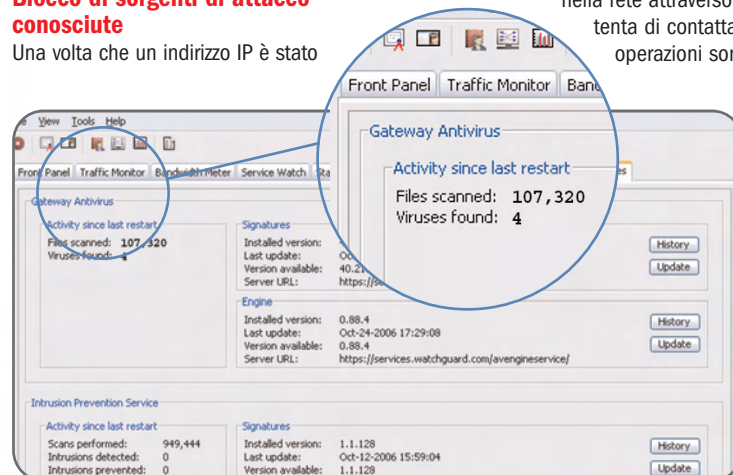
Aggiornamento automatico delle firme

Le firme vengono ininterrottamente aggiornate, per fornire alla rete una protezione aggiornata al minuto. Il database di firme è costituito da migliaia di firme di virus, inclusi WildList e virus zoo*, per fornire una copertura quanto più estesa possibile. È pertanto disponibile un database completamente verificato delle minacce più attive che assicura una maggiore accuratezza e un livello basso di falsi positivi.

Elenco di siti bloccati

L'elenco dei siti bloccati viene costantemente aggiornato allo scopo di proteggere la rete. L'antispyware a più livelli blocca l'accesso ai siti di spyware più conosciuti ed allo spyware* che tenta di penetrare nella rete attraverso la navigazione sul Web o che tenta di contattare il proprio host.* Tutte le operazioni sono registrate e sono disponibili per un agevole reporting.

*Disponibile su Firebox X Peak e Firebox X Core.



Gateway AV/IPS visto da Watchguard System Manager

Gateway AV/IPS blocca spyware e altro malware in tempo reale al gateway, prima che penetrino nella rete e disattivino la protezione di desktop e server.

Servizi di protezione in abbonamento potenziano la sicurezza

Per incrementare la funzionalità di prevenzione attacchi Zero Day del Firebox® X, è possibile aggiungere servizi di protezione per raggiungere livelli ancora superiori di protezione. In Firebox X è possibile attivare con facilità i servizi di protezione utilizzando una semplice chiave di licenza. È facile e non è necessario acquistare hardware aggiuntivo. Insieme a Gateway AV/IPS, la nostra suite di servizi di protezione include:

- **spamBlocker con quarantena:** il migliore sul mercato per distinguere in tempo reale gli attacchi di spamming dalle comunicazioni legittime, con una percentuale di e-mail bloccate che raggiunge il 97%. Lo spamming viene bloccato indipendentemente dalla lingua, dal contenuto o dal formato del messaggio. Include quarantena spamming completa.
- **WebBlocker:** consente di gestire la navigazione sul Web degli utenti per aumentare la produttività, prevenire eventuali responsabilità e diminuire i rischi per la protezione bloccando l'accesso a contenuti Web nocivi o inappropriati.

Questi servizi in abbonamento completamente integrati sono semplici da distribuire e gestire in Firebox X. Il costo di ogni servizio viene determinato per appliance e non per utente e pertanto un solo abbonamento fornisce protezione per tutta la rete e per tutti gli utenti configurati a monte del Firebox X.

Versione di prova GRATUITA per 30 giorni

È possibile ricevere la versione di prova gratuita per 30 giorni di **Gateway AntiVirus/Intrusion Prevention Service, spamBlocker e WebBlocker** per Firebox X Peak, Core o Edge. Per informazioni dettagliate, contattare il proprio rivenditore.

UTM Bundle - Unica soluzione, una sola licenza, un grande prezzo

Ora tutto il necessario per una completa gestione unificata delle minacce è disponibile in un comodo pacchetto, inclusa l'appliance. Un'offerta dalla convenienza eccezionale!

- Appliance Firebox X Peak, Core o Edge
- Abbonamenti di 1 anno a spamBlocker, Gateway AV/IPS e WebBlocker
- Abbonamento di 1 anno a LiveSecurity® Service per guida e supporto esperti

Firebox® X Peak™ UTM Bundle

| | |
|-----------------------------|---------|
| Firebox X5500e UTM Bundle | WG55503 |
| Firebox X6500e UTM Bundle | WG56503 |
| Firebox X8500e UTM Bundle | WG58503 |
| Firebox X8500e-F UTM Bundle | WG58513 |

Firebox® X Core™ UTM Bundle

| | |
|---------------------------|---------|
| Firebox X550e UTM Bundle | WG50553 |
| Firebox X750e UTM Bundle | WG50753 |
| Firebox X1250e UTM Bundle | WG51253 |

Firebox® X Edge UTM Bundle

| | |
|---|------------|
| Firebox X10e UTM Bundle | WG50016 |
| Firebox X20e UTM Bundle | WG50026 |
| Firebox X55e UTM Bundle | WG50061 |
| Firebox X10e Wireless UTM Bundle – Nord America | WG50017 |
| Firebox X10e Wireless UTM Bundle – Internazionale | WG50018 |
| Firebox X10e Wireless UTM Bundle – Cina | WG50019 |
| Firebox X10e Wireless UTM Bundle – Giappone | WG50018-JP |
| Firebox X20e Wireless UTM Bundle – Nord America | WG50027 |
| Firebox X20e Wireless UTM Bundle – Internazionale | WG50028 |
| Firebox X20e Wireless UTM Bundle – Cina | WG50029 |
| Firebox X20e Wireless UTM Bundle – Giappone | WG50028-JP |
| Firebox X55e Wireless UTM Bundle – Nord America | WG50062 |
| Firebox X55e Wireless UTM Bundle – Internazionale | WG50063 |
| Firebox X55e Wireless UTM Bundle – Cina | WG50064 |
| Firebox X55e Wireless UTM Bundle – Giappone | WG50063-JP |

UTM Software Suite per reti Firebox X

Con un singolo acquisto e a un prezzo eccezionale, è possibile aggiungere la nostra potente suite di servizi di protezione in abbonamento alla rete Firebox X e-Series esistente. UTM Software Suite trasforma Firebox X in una completa soluzione di gestione unificata delle minacce con:

- Abbonamenti di 1 anno a spamBlocker, Gateway AV/IPS e WebBlocker
- Abbonamento di 1 anno a LiveSecurity Service per guida e supporto esperti

Firebox® X Peak™ UTM Software Suite

| | |
|-------------------------------------|----------|
| Firebox X5500e UTM Software Suite | WG017449 |
| Firebox X6500e UTM Software Suite | WG017450 |
| Firebox X8500e UTM Software Suite | WG017451 |
| Firebox X8500e-F UTM Software Suite | WG017452 |

Firebox® X Core™ UTM Software Suite

| | |
|-----------------------------------|----------|
| Firebox X550e UTM Software Suite | WG017446 |
| Firebox X750e UTM Software Suite | WG017447 |
| Firebox X1250e UTM Software Suite | WG017448 |

Firebox® X Edge UTM Software Suite

| | |
|-----------------------------------|----------|
| Firebox X10e UTM Software Suite | WG017453 |
| Firebox X10e-W UTM Software Suite | WG017456 |
| Firebox X20e UTM Software Suite | WG017454 |
| Firebox X20e-W UTM Software Suite | WG017457 |
| Firebox X55e UTM Software Suite | WG017455 |
| Firebox X55e-W UTM Software Suite | WG017458 |

Gateway AV/IPS - Requisiti di sistema

Firebox X Edge

| | |
|--------------------|---|
| Software appliance | v8.6 |
| Amministrazione | Windows 2000, Windows NT, Windows XP o Windows Vista per supportare WatchGuard System Manager o l'interfaccia Web |
| Supporto | Abbonamento LiveSecurity Service attivo |

Firebox X Peak o Core

| | |
|--------------------|---|
| Software appliance | Fireware® 9.1 |
| Amministrazione | Windows 2000, Windows NT, Windows XP o Windows Vista per supportare WatchGuard System Manager |
| Supporto | Abbonamento LiveSecurity Service attivo |