WatchGuard®
PRODUCT DATASHEET

Firebox® X Peak™
e-Series

- **Completa gestione unificata delle minacce** per la protezione da nocive minacce di rete
- **Protezione Zero Day** per bloccare preventivamente attacchi nuovi e sconosciuti senza firme
- **Raddoppia le prestazioni** dei modelli precedenti e fornisce 8 porte Ethernet a 10/100/1000 gigabit
- **Gestisce le risorse,** ottimizza il traffico e aumenta i tempi di attività della rete
- **Semplice configurazione e gestione** di servizi e appliance Firebox Xs
- **Funzionalità di protezione integrate** per un maggiore controllo granulare

WatchGuard®
Stronger Security, Simply Done™

Protezione a 10/100/1000 gigabit per reti esigenti

Firebox® X Peak™ è la linea a più elevate prestazioni di appliance Unified Threat Management (UTM) di WatchGuard® e offre una protezione Zero Day effettiva subito disponibile, con velocità di firewall che raggiunge un gigabit al secondo. L'integrazione di potenti funzionalità di protezione con funzioni di networking avanzate consente a Firebox X Peak di fornire una superiore soluzione globale che risponde alle esigenze degli ambienti di rete più impegnativi.

Completa gestione unificata delle minacce

Firebox X Peak fornisce una protezione completa integrando Stateful Packet Firewall, VPN, protezione da attacchi Zero Day effettiva, antivirus gateway, prevenzione delle intrusioni, antispyware, antispamming e filtraggio URL in una singola appliance consentendo di ridurre in tal modo i tempi e i costi associati alla gestione di soluzioni multiple-point.

Protezione Zero Day effettiva

Intelligent Layered Security (ILS) in Firebox X Peak offre una protezione Zero Day effettiva immediatamente disponibile. Fornisce protezione nei confronti di minacce nuove e sconosciute prima che la vulnerabilità sia scoperta e che sia creato e lanciato un attacco. Molti produttori forniscono solo soluzioni di protezione basate su firma che richiedono costi di licenza separati. Queste soluzioni reattive in realtà lasciano i clienti esposti a nuovi tipi di minacce.

Firebox X a più elevate prestazioni

Con firewall fino a 2.0 Gbps e VPN fino a 600 Mbps, Firebox X Peak fornisce le prestazioni più elevate e la migliore scalabilità tra le soluzioni UTM della nostra linea di prodotti. Firebox X Peak ha otto porte Ethernet a 10/100/1000 gigabit Ethernet su tutti i modelli per supportare infrastrutture di backbone LAN ad alta velocità, oltre a connessioni WAN gigabit. Al fine di ottimizzarne l'utilizzo, ognuna delle otto porte è configurabile come interna, esterna oppure opzionale.

Funzionalità avanzate di networking

Le funzioni avanzate di networking di Firebox X Peak gestiscono risorse, ottimizzano il traffico e aumentano i tempi di attività della rete in maniera intelligente. Il failover interfaccia e la condivisione del carico multi-WAN migliorano le prestazioni e l'affidabilità, mentre il routing dinamico, la gestione del traffico e la configurazione della prioritarizzazione forniscono funzionalità di rete superiori per dati e comunicazioni mission-critical della rete.

Gestione semplice e intuitiva

WatchGuard System Manager (WSM), incluso in Firebox X Peak, consente di snellire l'amministrazione delle funzionalità di protezione della rete. Con un'interfaccia utente grafica, rapidi configurazioni guidate e impostazioni predefinite intelligenti, WSM semplifica il processo di installazione. In WSM sono inclusi senza costi nascosti logging e reporting completi, monitoraggio interattivo in tempo reale e creazione drag-and-drop di VPN.

Funzionalità di protezione integrate per un maggiore controllo granulare

Ogni servizio di protezione WatchGuard opera in maniera collaborativa con la prevenzione dagli attacchi Zero Day integrata di Firebox X Peak per assicurare un'imbattibile combinazione di funzionalità di protezione. Queste funzionalità sono completamente integrate in Firebox e non è necessario hardware aggiuntivo. Il prezzo degli abbonamenti è stabilito per appliance e non per utente e non vi sono pertanto ulteriori costi. Tutti i servizi sono continuamente aggiornati per offrire una protezione aggiornata al minuto e sono gestiti centralmente insieme a WSM per fornire viste in tempo reale di tutte le attività dei servizi.
I servizi includono:

- *spamBlocker*
  Il migliore servizio antispamming del settore, con una percentuale di blocco di e-mail indesiderate che raggiunge il 97%.
- *Gateway AV/IPS*
  Robusta protezione al gateway basata su firme contro virus, spyware, trojan horse e attacchi basati sul Web conosciuti.
- *WebBlocker*
  Per aumentare la produttività e diminuire i rischi per la protezione attraverso il blocco dell'accesso a contenuti Web nocivi e la gestione della navigazione in Internet degli utenti.

Aggiornamento ed scalabilità completi del modello

A fronte di requisiti di protezione della rete in trasformazione, è possibile estendere e proteggere il proprio investimento in soluzioni di protezione. È possibile, ad esempio, aumentare la capacità e la velocità del firewall o della VPN oppure aggiungere i servizi di protezione desiderati senza dover sostituire componenti hardware.

- Unica appliance di protezione UTM completamente aggiornabile disponibile oggi sul mercato, Firebox X Peak consente di accrescere in modo semplice prestazioni, capacità e funzioni di networking per rispondere a esigenze in crescita.
- Firebox X Peak può essere aggiornata per supportare il crescente fabbisogno dell'azienda con una semplice chiave di licenza. Non è necessaria alcuna sostituzione di componenti del sistema.

Blocco di attacchi basati sul Web

Il Web è uno degli strumenti più preziosi per l'azienda ma può anche rappresentare una seria minaccia per la propria rete. Gli utenti del Web non gestiti possono inavvertitamente o deliberatamente creare punti di vulnerabilità, introducendo bot e spyware in grado di mettere a rischio i dati aziendali sensibili e di aumentare in maniera significativa il volume delle richieste di assistenza telefonica all'helpdesk. Le reti vulnerabili sono esposte a corruzione della cache del server DNS, overflow del buffer e attacchi DoS (Denial of Service).

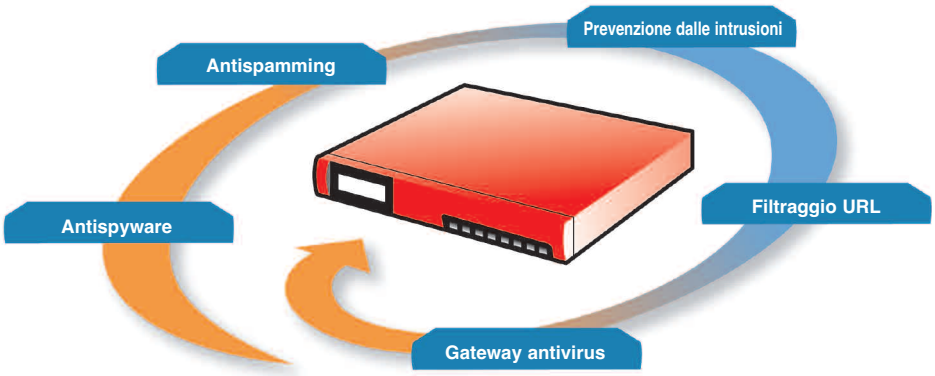
Che cosa è necessario fare

- Implementare **Firebox X Peak** per una protezione dagli attacchi Zero Day effettiva e prestazioni a livello di gigabit
- Attivare abbonamenti a **WebBlocker** per controllare la navigazione in Internet non autorizzata e a **Gateway AV/IPS** IPS per bloccare in tempo reale il traffico Web sospetto e i file scaricati

Vantaggi della protezione

- **Il gateway anti-virus** controlla il traffico Web alla ricerca di virus e altro malware e blocca i tentativi di spyware
- **Il cloaking del server Web** impedisce agli hacker di utilizzare i dati del sistema per attaccare la rete
- **Il filtraggio URL** consente di controllare la navigazione in Internet degli utenti per aumentare la produttività, proteggere la larghezza di banda della rete, ridurre i rischi di protezione e diminuire le responsabilità legali derivanti dalla presenza di contenuti non appropriati sul luogo di lavoro
- **La protezione effettiva Zero Day** protegge la rete nei confronti di minacce nuove e sconosciute prima che la vulnerabilità sia scoperta e sia creato e lanciato un attacco
- **Le funzionalità di antispyware multilivello** bloccano l'accesso ai siti di spyware, lo spyware che tenta di penetrare nella rete attraverso la navigazione sul Web e lo spyware che tenta di contattare il proprio host
- **I proxy HTTP** offrono protezione nei confronti di intrusioni di rete, attacchi DoS e corruzione della cache del server DNS
- **Le robuste funzionalità IPS** controllano l'utilizzo della messaggistica immediata (IM) e delle applicazioni Peer-to-Peer (P2P), due dei più comuni veicoli di distribuzione dello spyware
- **Logging, reporting e avvisi integrati** offrono dettagli approfonditi relativi all'attività di rete, consentendo di intraprendere misure preventive o correttive immediate

Firebox X: Protezione integrata



Protezione di uffici remoti e utenti mobili

A fronte di un numero sempre maggiore di telelavoratori o di utenti di risorse satellitari, aumenta di conseguenza la necessità di connessioni remote protette e affidabili a risorse e dati. Problemi quali la gestione e il reporting centralizzati, l'impostazione di criteri di protezione uniformi, l'interoperabilità con le risorse e le applicazioni di rete esistenti e una connettività remota affidabile, devono essere valutati attentamente. È fondamentale garantire che i dispositivi remoti soddisfino i criteri di protezione prima di accedere alla rete.

Che cosa è necessario

- Implementare **Firebox X Peak** per una gestione unificata delle minacce e per prestazioni a livello di gigabit
- Aggiungere **Firebox SSL VPN Gateway** per offrire un accesso universale protetto a utenti mobili e telelavoratori, **Firebox X Edge** per disporre di una eccezionale protezione del perimetro della rete cablata o wireless di uffici e filiali remote e gestire tutto attraverso **WatchGuard System Manager**

Vantaggi della protezione

- **Gestione centralizzata di criteri e VPN** che consente di applicare in modo uniforme i criteri di protezione per tutte le sedi e gli utenti
- **Accesso remoto protetto con controlli di sicurezza endpoint** che consente agli utenti mobili e ai telelavoratori un accesso remoto affidabile alle risorse di rete e assicura che i dispositivi utilizzati siano protetti prima di accedere alla rete
- **Potente gestione unificata delle minacce** per uffici remoti e telelavoratori che assicura che gli utenti e le reti estese sono protetti da spyware, virus, attacchi DOS e altre minacce dinamiche
- **Facile configurazione drag-and-drop di VPN per filiali** che fornisce la connettività operativa dell'ufficio remoto con pochi clic mantenendo bassi i costi associati all'IT
- **Prestazioni a livello di gigabit** che offrono affidabilità, ridondanza e flessibilità per diversi ambienti di connettività di rete e per le future esigenze di reti in crescita

Specifiche	Firebox® X5500e	Firebox® X6500e	Firebox® X8500e	Firebox® X8500e-F
	WG55500	WG56500	WG58500	WG58510
Velocità firewall*	900 Mbps	1.5 Gbps	2.0 Gbps	2.0 Gbps
Velocità VPN*	400 Mbps	600 Mbps	600 Mbps	600 Mbps
Gateway AV/IPS	Opzionale	Opzionale	Opzionale	Opzionale
Filtraggio URL	Opzionale	Opzionale	Opzionale	Opzionale
Blocco spamming	Opzionale	Opzionale	Opzionale	Opzionale
Interfacce 10/100/1000	8	8	8	8 (4 rame/4 fibra)
Porta seriale	1	1	1	1
Zone di protezione (incl.)	8	8	8	4 RJ45, 4 SFP GBIC
Sessioni contemporanee	500.000	750.000	1.000.000	1.000.000
Nodi supportati (IP LAN)	Illimitati	Illimitati	Illimitati	Illimitati
Tunnel VPN filiali (incl./max.)	400/400	400/400	400/400	400/400
Tunnel VPN utenti mobili (incl./max.)	1.200/4.000	1.600/5.000	2.000/10.000	2.000/10.000
Limite DB autenticazione utenti locali	5.000	6.000	8.000	8.000
Modello aggiornabile	Sì	Sì	No	No

*Le velocità variano in base all'ambiente e alla configurazione

Funzionalità

Funzionalità di protezione

- Firewall Stateful Packet
- Firewall per il controllo approfondito delle applicazioni
- Proxy di applicazione - HTTP, SMTP, FTP, DNS, TCP
- Prevenzione DoS e DDoS
- Prevenzione progressiva DDoS
- Protocol Anomaly Detection
- Analisi del comportamento
- Pattern Matching
- Protezione del riassemblamento di pacchetti frammentati
- Protezione dai pacchetti non validi
- Elenco statico delle origini bloccate
- Elenco dinamico delle origini bloccate
- Regole basate sul tempo

VPN

- Crittografia (DES, 3DES, AES 128-, 192-, 256-bit)
- IPSec
  - SHA-1, MD5
  - IKE - Chiave precondivisa
- Server PPTP
- Passthrough PPTP
- Dead Peer Detection (RFC 3706)
- Crittografia basata sull'hardware

User Authentication

- XAUTH
  - RADIUS®
  - LDAP
  - Windows® Active Directory
- RSA SecurID®
- Basata sul Web
- Autenticazione locale

X8500e-F Fiber Interface

- Multi-mode Fiber (MMF)
- 1000 Base SX
- 850 nm
- Connettori LC

IP Address Assignment

- Porte indipendenti
- Statico
- Client PPPoE
- Client DNS dinamico
- Server DHCP
- Client DHCP
- DHCP Relay

Redundancy Features

- Alta disponibilità
  - Alta disponibilità attiva/passiva
  - Sincronizzazione configurazione
  - Sincronizzazione sessioni
  - Sincronizzazione tunnel VPN
- Failover Multi-WAN
  - Porte failover WAN - 4
  - Modalità Failover WAN (attiva/passiva)

Condivisione del carico

- Condivisione del carico round robin
- Fino a 4 porte

Gestione e prioritarizzazione del traffico

- Larghezza di banda massima
- Numero di connessioni massime/secondo
- Prioritarizzazione del traffico basata su criteri
- Qualità del servizio
  - 2 Impostazione della prioritarizzazione

Routing

- Routing statico
- RIPv1, v2
- BGP4
- OSPF

Modalità di funzionamento

- Modalità trasparente/drop-in (livello 2)
- Modalità routing (livello 3)

Conversione indirizzi

- NAT statico (conversione porta)
- NAT dinamico
- NAT one-to-one
- IPSec NAT Traversal
- NAT basata su criteri

Logging/Reporting

- Aggregazione di log di più appliance
- Report compatibili con WebTrends® (WELF)
- Reports HTML
- Formato log XML
- Canale log crittografato
- Syslog
- SNMP

Avvisi/notifiche

- SNMP
- E-mail
- Avvisi del sistema di gestione
- Avvisi del programma personalizzato
- Configurazione w/GUI offline

Software di gestione

- WatchGuard System Manager (WSM)

Certificazioni

- EAL-4 – In attesa

Supporto e manutenzione

- Garanzia hardware di 1 anno
- Abbonamento LiveSecurity® Service di 90 giorni

Dimensioni e alimentazione

Dimensioni dell'appliance	4.5 x 42.6 x 36.2 cm
Dimensioni della confezione	18.4 x 54.6 x 48.2 cm
Peso dell'appliance	5.62 Kg
Peso totale	6.25 Kg
Peso WEEE	4.81 Kg
Alimentazione CA	9-250 VAC Autosensing
Assorbimento di corrente	U.S.A. 80 Watts Resto del mondo: 69 Cal/min o 273 BTU/min
Montabile su scaffale	Sì

Caratteristiche ambientali

Temperatura operativa	da 0 a 45° C
Temperatura non operativa	da -40 a 70° C
Umidità operativa	10 - 85%
Umidità non operativa	10 - 95% in assenza di condensa a 55° C
Vibrazione casuale non operativa	da 7 - 28 Hz 0.001 a 0.01 G2 per Hz
Rumore acustico	54 dBA a 20 - 25° C
Shock meccanico operativo	20 G con onda sinusoidale 1/2 durata 11 Msec
Conforme WEEE/RoHS	Sì

Guida e supporto esperti

Il servizio LiveSecurity di WatchGuard è il servizio combinato di supporto e manutenzione più completo disponibile nel settore. Il nostro team di esperti consente all'utente di gestire al meglio la protezione di rete. LiveSecurity Service offre aggiornamenti software, supporto tecnico esperto, avvisi di protezione precisi al minuto, sostituzione anticipata dell'hardware e risorse di self-help quali training, certificazione e programmi di esercitazione. Un servizio di supporto extra è disponibile per le aziende con requisiti Internet mission-critical.

GRATIS! Per 30 giorni

È possibile ricevere la versione di prova gratuita per 30 giorni di **spamBlocker, WebBlocker** e **Gateway AV/IPS** con l'acquisto di un Firebox X Peak. Per informazioni dettagliate, contattare il proprio rivenditore.

Per ulteriori informazioni su Firebox X Peak, visitare www.watchguard.com/appliances

E-MAIL: italy@watchguard.com · VENDITE: +39-011-9542227 · WEB: www.watchguard.com

Numero di parte WGCE66358_0506

WatchGuard