



- **Completa gestione unificata delle minacce** per proteggere la rete da pericolosi attacchi
- **Protezione Zero Day effettiva** per bloccare preventivamente le nuove minacce
- **Otto 8 porte Ethernet a 10/100/1000 gigabit** per la connettività ad alta velocità
- **Funzionalità avanzate di networking** per controllare le risorse e traffico e aumentare i tempi di attività della rete
- **Semplice configurazione e gestione** di tutti i servizi e le appliance
- **Funzionalità di protezione integrate in abbonamento** per un maggiore controllo granulare
- **Conforme a RoHS/WEEE**



Tecnologia eco-compatibile



Stronger Security. Simply Done™

Protezione gigabit per reti esigenti

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

Completa gestione unificata delle minacce

Firebox X Peak fornisce la protezione più completa della sua classe. La prevenzione attacchi Zero Day integrata, Stateful Packet Firewall e le funzionalità VPN complete sono combinate con gli abbonamento opzionali a servizi di protezione che forniscono potenti difese a più livelli. Le funzionalità di antispyware, prevenzione intrusioni, antivirus, antispamming con quarantena e filtraggio URL sono completamente integrate in una robusta appliance, riducendo drasticamente i tempi e i costi associati alla gestione di soluzioni multiple-point.

Protezione Zero Day effettiva

Quando le vulnerabilità del software rendono possibili nuovi tipi di attacchi, le difese proattive integrate di Firebox X Peak sono già all'opera per mantenere sicura la vostra rete. Il controllo applicativo approfondito, basato su sofisticate tecnologie proxy, identifica e blocca minacce nuove o sconosciute appena si manifestano. La protezione automatica nei confronti di spyware, trojan horse, worm, DoS, DDos, corruzione DNS, overflow del buffer e altri attacchi è assicurata.

Elevate prestazioni

Con velocità firewall maggiore di 2 Gbps e una velocità VPN fino a 600 Mbps, Firebox X Peak fornisce le prestazioni più elevate e la migliore scalabilità di qualsiasi soluzione UTM della nostra linea di prodotti. Con otto porte Gigabit Ethernet a 10/100/1000 su tutti i modelli, supporta 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 e ottimizzano il traffico, assicurando che una connettività affidabile aumenti i tempi di attività della rete.

- **VLAN** riduce i requisiti hardware e fornisce una interoperabilità più completa
- **Il bilanciamento carico multi-WAN, l'alta affidabilità e il failover WAN e VPN** aumentano prestazioni, ridondanza e affidabilità
- **Il routing dinamico e il traffic shaping** ottimizzano flessibilità ed efficienza della rete
- **Il routing basato su policy** consente di specificare l'interfaccia di uscita per ogni servizio al fine di potenziare la gestione della larghezza di banda della rete e ridurre i costi
- **Il bilanciamento del carico del server** semplifica la protezione di "server farms", ad esempio, di commercio elettronico rivolte al pubblico

Gestione unificata intuitiva

WatchGuard® System Manager (WSM) è una interfaccia utente grafica utilizzata per gestire centralmente tutte le funzionalità di Firebox X Peak. Dal momento che è disponibile un'interfaccia unica di gestione, anche in versione multibox, è possibile utilizzare subito la soluzione ed essere sempre pronti. Nel WSM sono inclusi senza costi nascosti logging e reporting completi, monitoraggio interattivo in tempo reale e creazione drag-and-drop delle VPN.

Funzionalità di protezione integrate per un maggiore controllo granulare

Ogni servizio di protezione WatchGuard in abbonamento opera in maniera collaborativa con la prevenzione 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 ulteriori costi. Continuamente aggiornati, forniscono una protezione allenata al minuto e sono gestiti centralmente tramite WSM per ottenere viste in tempo reale di tutte le attività dei servizi. Gli abbonamenti includono:

- **WebBlocker**
Per aumentare la produttività, prevenire responsabilità legali e diminuire i rischi per la protezione attraverso il blocco dell'accesso a contenuti Web nocivi.
- **spamBlocker con quarantena**
È il migliore servizio antispamming del settore, con una percentuale di blocco di e-mail indesiderate che raggiunge il 97%.
- **Gateway AV/IPS con Anti-Spyware**
Blocca spyware, virus, trojan horse e attacchi Web conosciuti tramite una protezione basata su firme.

Aggiornamento e scalabilità completi del modello

A fronte di requisiti di incremento di protezione delle reti, è possibile espandere la capacità o aggiungere servizi in abbonamento utilizzando semplici chiavi di licenza software scaricabili per evitare costosi aggiornamenti hardware.

Il nostro impegno per l'ambiente

WatchGuard è impegnata nella realizzazione di prodotti che utilizzano l'energia in maniera efficiente e utilizza materiali riciclabili per la appliance e gli imballaggi. WatchGuard è completamente conforme alle direttive dell'Unione Europea sull'utilizzo di sostanze pericolose e ha fatto della responsabilità ambientale una componente importante dei nostri requisiti strategici di business.

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

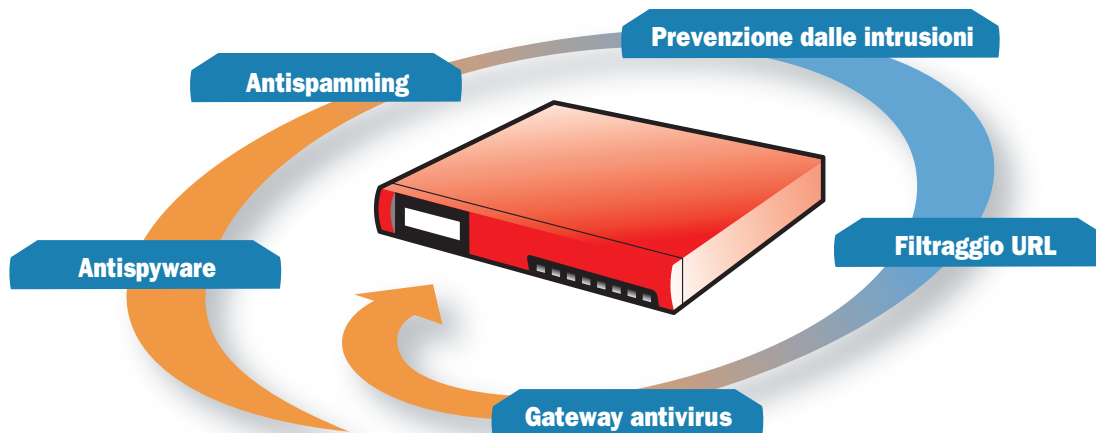
- Implementare **Firebox X Peak** per una protezione dagli attacchi Zero Day effettiva e prestazioni a livello di più gigabit
- Attivare abbonamenti a **WebBlocker** per controllare la navigazione in Internet non autorizzata e a **Gateway AV/IPS** per bloccare in tempo reale il traffico Web sospetto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

Vantaggi della protezione

- **Protezione Zero Day effettiva** attraverso potenti tecnologie proxy integrate difende la vostra rete nei confronti di minacce sconosciute quando le vulnerabilità del software applicativo rendono possibili questo nuovo tipo di attacchi

- **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
- **Il gateway antivirus** controlla il traffico Web alla ricerca di virus, trojan horse, bot e altro malware assicurando protezione granulare dalle minacce conosciute
- **Il cloaking del server Web** impedisce agli hacker di utilizzare i dati del sistema per attaccare la rete
- **Il filtraggio URL** consente di limitare i contenuti Web accessibili dai dipendenti sul luogo di lavoro al fine di aumentare la produttività e prevenire responsabilità legali, proteggendo al tempo stesso la rete da siti nocivi
- **L'architettura intelligente multilivello opera con il proxy DNS** per proteggere da 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

I servizi di protezione integrati in abbonamento di Firebox X Peak potenziano la protezione nell'area critica di attacco.



Protezione di uffici remoti e utenti mobili

A fronte di un numero sempre maggiore di telelavoratori, 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 policy 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 prestazioni a livello di più gigabit
- Aggiungere appliance **Firebox X Edge** ottenere una eccezionale protezione perimetrale della rete wireless o cablata per gli uffici remoti e le filiali e gestire centralmente tutte le funzionalità di protezione con il **WatchGuard System Manager (WSM)** di semplice utilizzo.

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 alle risorse di rete** tramite tunnel VPN criptati per filiali e utenti mobili per aumentare la produttività e la flessibilità per i dipendenti che operano esternamente alla sede centrale
- **Potente gestione unificata delle minacce** per uffici remoti e per i 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 più gigabit** che offrono affidabilità, ridondanza e flessibilità per diversi ambienti di connettività di rete e per le future esigenze delle reti in crescita

Specifiche	Firebox® X5500e WG55500 X5500e UTM Bundle WG55503	Firebox® X6500e WG56500 X6500e UTM Bundle WG56503	Firebox® X8500e WG58500 X8500e UTM Bundle WG58503	Firebox® X8500e-F WG58510 X8500e-F UTM Bundle WG58513
Velocità firewall*	2.0+ Gbps	2.0+ Gbps	2.0+ Gbps	2.0+ Gbps
Velocità VPN*	400 Mbps	600 Mbps	600 Mbps	600 Mbps
Velocità AV*	140 Mbps	170 Mbps	200 Mbps	200 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
VLAN	75	75	75	75
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 ufficio filiale (incl./max.)	750/750	750/750	750/750	750/750
Tunnel VPN utenti mobili (incl./max.)	600/600	600/600	600/600	600/600
Limite database 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

- Stateful Packet Filtering
- Firewall con controllo approfondito a livello applicativo
- Blocco spyware
- Proxy di applicazione - HTTP, SMTP, FTP, DNS, TCP, POP3
- Prevenzione DoS e DDoS
- Prevenzione progressiva DDoS
- Protocol Anomaly Detection
- Analisi del comportamento
- Pattern Matching
- Protezione del riassetto pacchetti frammentati
- Protezione da pacchetti non validi
- Elenco statico delle origini bloccate
- Elenco dinamico delle origini bloccate
- Regole basate sul tempo
- Consenti/nega messaggistica immediata e P2P

Reti private virtuali

- VPN
 - Crittografia (DES, 3DES, AES 128-, 192-, 256 bit)
 - IPSec
 - SHA-1, MD5
 - IKE Chiave precondivisa, certificato terze parti Firebox
- Server PPTP
- Passthrough PPTP
- Dead Peer Detection (RFC 3706)
- Crittografia basata sull'hardware
- Tunnel VPN drag-and-drop

Autenticazione utente

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

Assegnazione degli indirizzi IP

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

- Client DNS dinamico

Interfaccia fibra X8500e-F

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

Alta affidabilità

- Alta affidabilità attiva/passiva
- Sincronizzazione configurazione
- Sincronizzazione sessioni
- Sincronizzazione tunnel VPN

Failover WAN

- Failover VPN
- Modalità WAN
 - Spill-over
 - Round Robin
 - Failover
 - ECMP
 - Weighted Round Robin

Traffic Shaping

- Quality of Service
 - 8 code di priorità
 - DiffServ
 - Modified Strict Queuing

Routing

- Routing statico
- RIPv1, v2
- Routing dinamico
 - BGP4, OSPF
 - RIPv1, v2
- Routing basato su policy

Networking

- VLAN
 - Bridging, Tagging, Modalità di routing
- Bilanciamento del carico server

Servizi di protezione in abbonamento

- spamBlocker

- Quarantena per spamming, email di massa e messaggi sospetti

- Gateway AntiVirus/IPS con antispyware
 - Scansione AV di file di dimensioni illimitate
- WebBlocker

Modalità di funzionamento

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

Conversione indirizzi di rete (NAT)

- NAT statico (inoltro porta)
- NAT dinamico
- NAT one-to-one
- IPSec NAT Traversal
- NAT basata su criteri
- IP virtuale per bilanciamento del carico del server

Logging/Reporting

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

Avvisi/notifiche

- SNMP
- Email
- Avvisi del sistema di gestione

Software di gestione

- WatchGuard System Manager (WSM)

Certificazioni

- Common Criteria EAL4
- ICSA IPSec
- ICSA Firewall

Supporto e manutenzione

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

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	100-240 VCA autosensing
Assorbimento di corrente	U.S.A. 80 Watt Resto del mondo: 1146 Cal/min o 273 BTU/min
Montabile in armadio	Si

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	Si



Disponibile anche con 4 porte rame e quattro fibra nel modello X8500e-F

Guida e supporto esperti

LiveSecurity® di WatchGuard è il servizio di supporto e manutenzione più completo disponibile nel settore e mette a vostra disposizione un team globale di esperti di sicurezza per semplificare le complesse attività della gestione IT. LiveSecurity Service fornisce:

- Garanzia hardware con sostituzione anticipata dell'hardware
- Aggiornamenti software
- Supporto tecnico con risposta rapida
- Avvisi di protezione precisi al minuto con chiare istruzioni su come affrontare le nuove minacce e link diretti alle patch dei produttori per risparmiare tempo prezioso
- Innovative risorse di formazione, inclusi video, podcast e comodi moduli di training sulla sicurezza per gli utenti finali

Al momento dell'acquisto di una appliance Firebox X Peak è possibile scegliere tra un abbonamento iniziale di 90 giorni oppure 1 anno a LiveSecurity Service. Un servizio di supporto extra è disponibile per le aziende con requisiti Internet mission-critical.

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

Tutto il necessario per la gestione unificata delle minacce in un'appliance ad alte prestazioni è ora disponibile in un comodo pacchetto. Il bundle offre una convenienza eccezionale e include:

- Appliance di protezione Firebox X Peak e-Series
- WebBlocker*
- spamBlocker*
- Gateway AV/IPS con antispyware*
- LiveSecurity® Service

Dall'acquisto iniziale fino alla gestione corrente della protezione, Firebox X Peak e-Series UTM Bundle snellisce la gestione della protezione di rete fornendo la migliore soluzione UTM della sua classe. Acquista il bundle e risparmia!

*Abbonamento di 1 anno

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: +39-335-7030721 · WEB: www.watchguard.com

Non sono qui fornite garanzie esplicite o implicite. Tutte le specifiche sono soggette a modifica e tutti i prodotti o funzionalità futuri saranno forniti in base alla disponibilità. © 2007 WatchGuard Technologies, Inc. Tutti i diritti riservati. WatchGuard, il logo WatchGuard, Firebox, Firewall, LiveSecurity, Peak, Core e Stronger Security, Simply Done sono marchi o marchi registrati di WatchGuard Technologies, Inc. negli Stati Uniti e/o in altri paesi. Tutti gli altri marchi e nomi commerciali sono di proprietà dei rispettivi titolari. Num. parte WGC66358_090607

