WatchGuard®
PRODUCT DATASHEET

Firebox® X Core™
e-Series

- **Protezione completa** per difendere la rete da minacce maligne
- **Prevenzione dagli attacchi Zero Day** per sconfiggere minacce nuove e sconosciute prima che siano disponibili le firme
- **Gestione snellita della protezione di rete** per risparmiare tempo
- **Servizi antivirus, antispamming e filtraggio Web continuamente aggiornati** per una protezione aggiornata al minuto
- **Funzionalità integrate aggiornabili** per una maggiore convenienza
- **Team globale di esperti di protezione** sempre a disposizione

WatchGuard
Stronger Security, Simply Done™

Soluzione completa di gestione unificata delle minacce

Le soluzioni Unified Threat Management (UTM) di Firebox® X Core™ forniscono la protezione più completa della propria classe, integrando Stateful Packet Firewall, VPN, prevenzione dagli attacchi Zero Day effettiva, antispyware, antispamming, antivirus, prevenzione delle intrusioni e filtraggio URL in una singola appliance, riducendo in tal modo tempi e costi associati alla gestione di soluzioni multiple-point e rafforzando in modo significativo la protezione dagli attacchi di rete combinati.

Superiore protezione a multilivello

Firebox X Core è realizzata sulla base di Intelligent Layered Security (ILS) di WatchGuard. All'interno di questa architettura, i livelli di protezione operano insieme per rafforzare la sicurezza complessiva della rete, mentre la comunicazione collaborativa tra i diversi livelli riduce e ottimizza l'elaborazione necessaria. Il risultato è tutta la protezione necessaria per essere al sicuro senza sacrificare le prestazioni.

Protezione Zero Day effettiva

A differenza dei prodotti che si affidano semplicemente alla scansione basata su firme, Firebox X Core dispone di funzionalità critiche di protezione integrate che consentono di difendersi da classi di attacchi e dalle relative varianti senza la necessità di utilizzare le firme. Mentre altre reti rimangono vulnerabili nei confronti delle più recenti minacce fino a quando non è disponibile una firma, la vostra rete è protetta e sicura dal momento in viene accesa Firebox.

Gestione unificata senza costi nascosti

WatchGuard® System Manager (WSM) è l'intuitiva interfaccia grafica utilizzata per gestire tutte le funzionalità delle soluzioni UTM di Firebox X Core oltre che delle appliance Firebox X Peak® e Edge. WSM offre logging, creazione drag-and-drop di reti VPN e monitoraggio in tempo reale subito disponibili, senza costi nascosti o richieste di acquisti aggiuntivi. Grazie all'interfaccia utente singola per la gestione di tutti gli aspetti della soluzione di protezione, il risparmio di tempo e denaro è assicurato.

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 globale di esperti di protezione è sempre disponibile per fornire agli utenti tutto il supporto necessario per gestire al meglio la soluzione di protezione della rete. LiveSecurity Service offre aggiornamenti software, supporto tecnico esperto, avvisi di vulnerabilità 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.

Funzionalità di protezione integrate per un maggior controllo granulare

Ogni servizio di protezione di WatchGuard opera in maniera collaborativa con la prevenzione dagli attacchi Zero Day integrata di Firebox X Core per fornire una combinazione imbattibile di funzionalità di protezione. I servizi sono completamente integrati e il prezzo degli abbonamenti viene calcolato per appliance e non per utente per evitare l'aumento dei 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.

- *spamBlocker*
  È 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.

Protezione dell'investimento

Se si considerano i costi di implementazione, gestione e aggiornamento di più soluzioni di protezione per la gestione di un'ampia gamma di esigenze di protezione, risulta chiaro l'ottimo rapporto qualità prezzo delle soluzioni UTM di Firebox X Core. La protezione versatile, completamente integrata di una singola appliance consente di risparmiare denaro in relazione a ogni aspetto della soluzione, dall'acquisto iniziale fino ai contratti di assistenza.

Con il crescere delle esigenze, è facile aggiungere nuove funzionalità per potenziare la sicurezza della propria organizzazione. Per ottenere maggiore velocità e capacità, è possibile eseguire l'aggiornamento a un modello superiore della linea di prodotti scaricando una semplice chiave di licenza. Per soddisfare le esigenze delle reti più impegnative, è possibile eseguire l'aggiornamento al software per appliance avanzate Fireware® Pro allo scopo di ampliare le funzionalità di rete con l'alta disponibilità, la gestione del traffico e il routing dinamico. Tutte queste funzionalità sono disponibili senza acquistare nuovi componenti hardware. Nessun altro prodotto sul mercato protegge in maniera così diversificata l'investimento in soluzioni di protezione.

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).

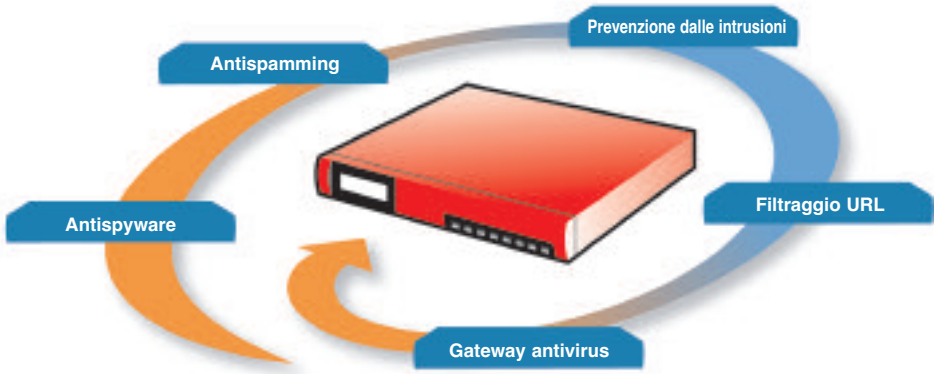
Che cosa è necessario fare

- 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** 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
- **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 venga 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



Blocco delle minacce via e-mail

Le aziende si affidano sempre di più alla posta elettronica. L'e-mail deve funzionare in modo uniforme e affidabile, senza mettere in pericolo la sicurezza della rete. Ma l'e-mail rimane il mezzo più comune per la diffusione di codice maligno nella vostra rete. Se a questo si aggiunge il problema continuo dello spamming, l'ambiente di posta elettronica può diventare uno dei sistemi IT più onerosi per l'azienda.

Che cosa è necessario fare

- Implementare **Firebox X Core** con protezione Zero Day effettiva
- Aggiungere un abbonamento a **Gateway AV/IPS** che esegue la scansione del traffico e-mail al fine di bloccare worm, virus, trojan horse e altro malware conosciuto
- Attivare un abbonamento a **spamBlocker**, il miglior servizio del settore per riconoscere in tempo reale il traffico e-mail legittimo dagli attacchi di spamming

Vantaggi della protezione

- **spamBlocker** utilizza il rilevamento dello spamming in tempo reale per fornire protezione immediata, con una percentuale di e-mail indesiderate bloccate che arriva al 97%, indipendentemente da contenuto, lingua o formato del messaggio
- **Protezione Zero Day integrata** per bloccare preventivamente i tipi di file comunemente utilizzati per trasmettere malware via e-mail
- **Cloaking del server Web** per impedire agli hacker di utilizzare i dati del sistema per attaccare la rete
- **Gateway AV** per offrire una protezione granulare dei file e degli allegati bloccando virus, worm e altro malware prima che possa penetrare nella rete e disattivare le applicazioni di protezione desktop
- **Ocansione AV della posta in uscita** per impedire all'azienda di inviare virus, worm e trojan horse a partner, clienti e altri destinatari al di fuori della rete

Specifiche	Firebox® X550e WG50550	Firebox® X750e WG50750	Firebox® X1250e WG51250
Velocità firewall*	125 Mbps	200 Mbps	300+ Mbps
Velocità VPN*	20 Mbps	50 Mbps	100 Mbps
Gateway AV/IPS	Opzionale	Opzionale	Opzionale
Filtraggio URL	Opzionale	Opzionale	Opzionale
Blocco spamming	Opzionale	Opzionale	Opzionale
Porta seriale	1	1	1
Interfacce 10/100	4	8	0
Interfacce 10/100/1000	0	0	8
Zone di protezione (incl.)	4	8	8
Sessioni contemporanee	25.000	75.000	200.000
Nodi supportati (IP LAN)	Illimitati	Illimitati	Illimitati
Tunnel VPN ufficio filiale (incl./max.)	1/10	100/100	400/400
Tunnel VPN utenti mobili (incl./max.)	5/10	50/100	400/400
Limite DB autenticazioni locale	250	1.000	5.000
Modello aggiornabile	No	Sì	No
Software appliance avanzate Fireware® Pro	Opzionale	Opzionale	Opzionale

*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 da 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, certificato Firebox
- Server PPTP
- Passthrough PPTP
- Dead Peer Detection (RFC 3706)
- Crittografia basata sull'hardware

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

Funzioni di ridondanza

- 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
- Impostazione di prioritarizzazione del traffico/QoS*
  - 2 livelli di 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

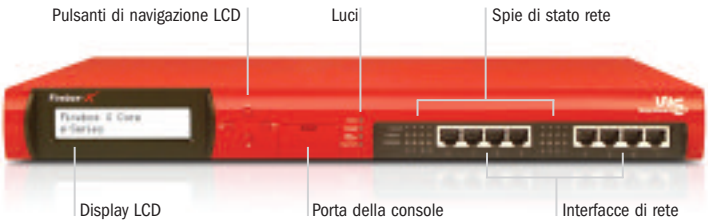
*Disponibile con l'aggiornamento al software per appliance avanzate Fireware Pro

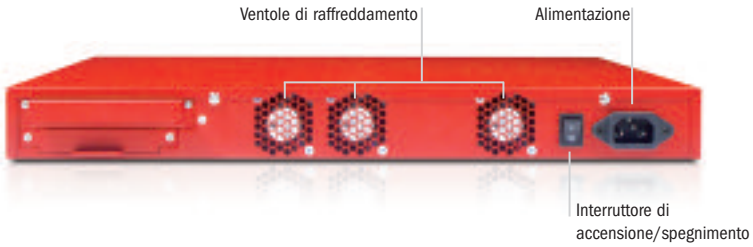
Dimensioni e alimentazione

Dimensioni dell'appliance	4.5 x 42.6 x 36.2 cm
Dimensioni della confezione	18.4 x 54.6 x 48.3 cm
Peso dell'appliance	4.39 Kg
Peso totale	6.21 Kg
Peso WEEE	4.81 Kg
Alimentazione CA	100-240 VAC Autosensing
Assorbimento di corrente	U.S.A. 60 Watts Resto del mondo: 52 Cal/min or 205 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 con WEEE/RoHS	Sì





Pronti per l'aggiornamento al software per appliance avanzate Fireware® Pro?

A fronte di esigenze di rete in crescita, è possibile aggiornare Firebox X Core da Fireware a Fireware Pro, il software per appliance avanzate di WatchGuard per ambienti di reti più impegnativi. Passare a Fireware Pro per:

- **Gestione e prioritarizzazione del traffico** – Garantisce alle applicazioni aziendali business-critical tutta la larghezza di banda necessaria
- **Routing dinamico (BGP, OSPF)** – Ottimizza flessibilità, ridondanza ed efficienza di rete attraverso l'aggiornamento dinamico delle tabelle di routing
- **Alta disponibilità (attiva/passiva)** – Offre ridondanza hardware per un'appliance in standby

Per informazioni dettagliate, contattare il proprio rivenditore.

GRATIS! Per 30 giorni

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

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

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