WatchGuard®

SCHEDA INFORMATIVA PRODOTTO

Firebox® X Core™

e-Series

- **Protezione completa** per difendere la rete da minacce maligne
- **Prevenzione dagli attacchi Zero Day** blocca attivamente le nuove minacce
- **Novità! SSL VPN integrato**
- **Gestione della protezione di rete** per risparmiare tempo
- Abbonamenti di sicurezza **continuamente aggiornati** per una protezione allineata al minuto
- **Funzionalità integrate aggiornabili** per una maggiore convenienza
- **Team globale di esperti sulla protezione** sempre a disposizione

Tecnologia eco-compatibile

Soluzione completa nella gestione unificata delle minacce

Le soluzioni Unified Threat Management (UTM) Firebox® X Core™ forniscono la protezione più completa della propria classe, proteggendo la rete da spyware, spamming, virus, trojan horse, attacchi basati sul Web e altro malware. La forte protezione a più livelli riduce drasticamente i tempi e i costi associati alla gestione di soluzione multiple-point e aumenta in maniera significativa la protezione nei confronti di minacce combinate. Allo stesso tempo, le funzioni avanzate di rete gestite attraverso una intuitiva interfaccia utente assicurano una connettività dati aziendale veloce e protetta in una singola appliance di facile utilizzo.

Affidabile protezione a più livelli

Firebox X Core è realizzato sulla base di una architettura multilivello intelligente. 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

Quando le vulnerabilità del software consentono l'introduzione di nuovi attacchi di rete, le difese proattive del Firebox X Core assicurano la protezione della rete e degli utenti. Sofisticate tecnologie di proxy eseguono il controllo approfondito a livello applicativo per identificare e bloccare le minacce emergenti, assicurando la protezione automatica da spyware, trojan horse, worm, attacchi DoS, DDoS, corruzione del DNS, overflow del buffer e altri tipi di attacchi.

Gestione unificata intuitiva

WatchGuard® System Manager (WSM) rende più intuitiva la gestione centralizzata delle implementazioni del Firebox X, indipendentemente dalle dimensioni. Gli amministratori risparmieranno tempo e denaro utilizzando l'interfaccia per creare e distribuire con facilità le modifiche di configurazione, monitorare i dati in tempo reale, e generare report cronologici.

Funzionalità di protezione integrate per un maggiore controllo granulare

È possibile potenziare le difese in aree critiche di attacco aggiungendo potenti abbonamenti di sicurezza al Firebox X. Tutti i servizi in abbonamento sono gestiti centralmente utilizzando WSM e sono aggiornati costantemente per assicurare la protezione più aggiornata.

- ***Gateway AV/IPS con Anti-Spyware***
  Blocca spyware, trojan horse, virus e attacchi basati sul Web con una forte protezione basata su firme al gateway.
- ***spamBlocker con rilevamento virus***
  È la migliore soluzione antispamming del settore, con una percentuale di blocco di e-mail indesiderate che raggiunge quasi il 100% e protezione in tempo reale da attacchi di virus.
- ***WebBlocker***
  Aumenta la produttività e diminuisce i rischi di protezione bloccando l'accesso HTTP e HTPPS a contenuti Web nocivi o non appropriati.

Connettività remota protetta

La protezione dei telelavoratori, indipendentemente dalla loro posizione geografica, è più facile con Firebox X Core. Fornisce la più ampia gamma di funzionalità di accesso remoto della sua categoria, consentendo agli utenti fuori sede di accedere in sicurezza alla rete aziendale tramite

- IPSec
- SSL VPN
- PPTP

Include il Single Sign On per snellire l'autenticazione.

Guida e supporto esperti

LiveSecurity® Service di WatchGuard mette a vostra disposizione un team globale di esperti di sicurezza per semplificare le complesse attività della gestione IT. L'abbonamento LiveSecurity include una garanzia hardware con sostituzione anticipata, aggiornamenti software, supporto tecnico a risposta rapida, avvisi di vulnerabilità precisi al minuto e innovative risorse di formazione.

Protezione dell'investimento

Se si considerano i costi di implementazione, gestione e aggiornamento di più soluzioni 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 l'aumentare delle esigenze, è facile aggiungere nuove funzionalità per migliorare la sicurezza della propria organizzazione. Per ottenere maggiore 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 da Fireware® al software per appliance avanzate Fireware® Pro allo scopo di ampliare le funzionalità di rete con reti VLAN, l'alta affidabilità, e QoS. 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 di rete.

Il nostro impegno per l'ambiente

WatchGuard realizza 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 internazionali sull'utilizzo di sostanze pericolose e ha fatto della responsabilità ambientale una componente importante dei nostri requisiti strategici di business.

WatchGuard™

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 DNS (Domain Name Service), overflow del buffer e attacchi DoS (Denial of Service).

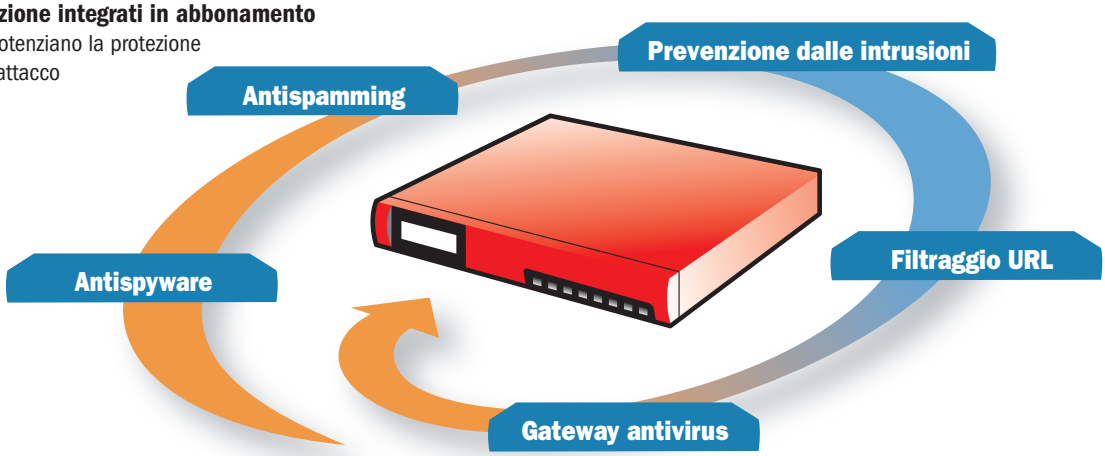
Che cosa è necessario fare

- Implementare **Firebox X Core** per una protezione dagli attacchi Zero Day effettiva
- 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 a livello applicativo 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
- **Gateway AV/IPS con antispyware** controlla il traffico Web alla ricerca di virus, trojan horse, bot e altro malware per la protezione granulare da minacce conosciute
- **Il cloaking del server Web** impedisce agli hacker di utilizzare i dati del sistema per attaccare la rete
- **WebBlocker** consente di limitare le risorse sul Web accessibili dai dipendenti sul luogo di lavoro al fine di aumentare
- **Il filtraggio URL del traffico HTTPS** impedisce agli utenti di aggirare le restrizioni e navigare in siti non consentiti
- **L'architettura intelligente multilivello opera con il proxy DNS** per proteggere da intrusioni di rete, attacchi DoS e corruzione della cache del server DNS
- **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 Core potenziano la protezione nell'area critica di attacco



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. Essa 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**, la migliore soluzione del settore per riconoscere in tempo reale il traffico e-mail legittimo dagli attacchi di spamming. SpamBlocker include un potente livello di protezione antivirus in grado di riconoscere e bloccare i virus veicolati dall'e-mail con una precisione che si avvicina al 100%

Vantaggi della protezione

- **Protezione Zero Day integrata** si affida ad una potente tecnologia proxy a livello applicativo per bloccare in maniera proattiva i tipi di file comunemente utilizzati per trasmettere malware via e-mail
- **spamBlocker** utilizza il rilevamento dello spamming in tempo reale per fornire protezione immediata, bloccando le e-mail indesiderate, indipendentemente da contenuto, lingua o formato del messaggio, incluso lo spamming basato su immagini
- La **quarantena per spamming e antivirus** tiene lo spamming e l'email sospetta lontano dalla rete, fornendo ad amministratori e utenti finali gli strumenti per analizzarla
- **Cloaking dei server SMTP** per impedire agli hacker di utilizzare i dati del sistema per attaccare la rete
- **Gateway AV integrato** 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
- **Scansione 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 X550e UTM Bundle WG50553	Firebox® X750e WG50750 X750e UTM Bundle WG50753	Firebox® X1250e WG51250 X1250e UTM Bundle WG51253
Velocità firewall†	300+ Mbps	750 Mbps	1.5 Gbps
Velocità VPN†	35 Mbps	50 Mbps	100 Mbps
Velocità AV†	50 Mbps	70 Mbps	100 Mbps
Gateway AV/IPS con Anti-Spyware	Opzionale	Opzionale	Opzionale
Filtraggio URL su HTTP e HTTPS	Opzionale	Opzionale	Opzionale
Blocco spamming con protezione attacchi virus	Opzionale	Opzionale	Opzionale
Interfacce 10/100	4	8	0
Interfacce 10/100/1000	0	0	8
Porta seriale	1	1	1
Supporto VLAN*	25	25	25
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.)	35/45	100/100	600/600
Tunnel VPN mobile IPSec (incl./max.)	5/75	50/100	400/400
Tunnel VPN mobile - SSL (incl./max.)	1/75	1/300	1/500
Limite database autenticazione utenti locali	250	1.000	5.000
Modello aggiornabile	Sì	Sì	No
Software appliance avanzate Fireware® Pro	Opzionale	Opzionale	Opzionale

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

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

Funzionalità

Funzionalità di protezione

- Stateful Packet Filtering
- Firewall con controllo approfondito a livello applicativo
- Proxy applicativi – HTTP, SMTP, FTP, DNS, TCP, POP3
- Blocco spyware
- Prevenzione DoS e DDoS e prevenzione progressiva DDoS
- Protocol Anomaly Detection
- Analisi del comportamento
- Pattern Matching
- Protezione riassemblamento pacchetti frammentati
- Protezione da pacchetti non validi
- Elenco statico e 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
  - SSL VPN
    - Thin Client, Web Exchange
- Server e passthrough PPTP
- Dead Peer Detection (RFC 3706)
- Crittografia basata sull'hardware
- Tunnel VPN drag-and-drop

Autenticazione utente

- Autenticazione Firebox trasparente tramite Active Directory (single sign on)
- XAUTH
  - RADIUS®, LDAP, Windows® Active Directory
- VASCO
- RSA SecurID®
- Basata sul Web
- Autenticazione locale

Assegnazione degli indirizzi IP

- Statico
- Client PPPoE
- Client, server, relay DHCP
- Client DNS dinamico

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

Networking**

- Porte indipendenti
- VLAN
  - Bridging, Tagging, Modalità routing
- Bilanciamento del carico del server e multi-WAN
- Supporto VoIP e videoconferenza

Protezione in abbonamento

- spamBlocker
  - Quarantena per spamming, email di massa e messaggi sospetti
  - Rilevamento virus
- Gateway AntiVirus/IPS con antispyware
- 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 basato su policy
- IP virtuale per bilanciamento del carico del server**

Logging/Reporting

- Aggregazione di log di più appliance
- Report compatibili con WebTrends® (WELF)
- Report HTML e PDF
- Database log SQL
- Canale log crittografato
- Syslog
- SNMP v2 e v3

Avvisi/notifiche

- SNMP
- Email
- Avvisi del sistema di gestione

Software di gestione††

- WatchGuard System Manager (WSM)

Certificazioni

- Common Criteria EAL4
- ICSA IPSec e ICSA Firewall
- West Coast Labs Checkmark

Supporto e manutenzione

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

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

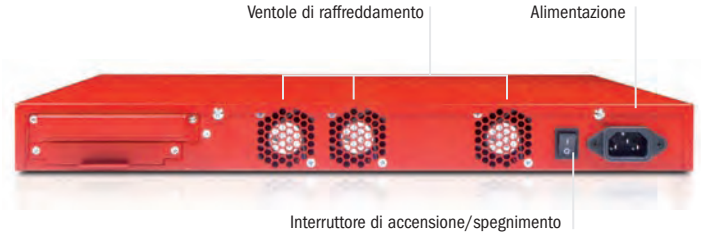
††Firebox X 550e prevede una licenza single-node WSM. Per creare tunnel drag-and-drop o per gestire centralmente appliance Firebox X Edge multiple da un X550e sono necessarie licenze di aggiornamento WSM opzionali.

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 VCA autosensing
Assorbimento di corrente	U.S.A. 60 Watt
	Resto del mondo: 860 Cal/min o 205 BTU/min
Montabile in armadio	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 delle esigenze delle reti in crescita, è possibile aggiornare Firebox X Core da Fireware a Fireware Pro, il software avanzato per appliance per gli ambienti di reti più impegnativi. Ora più potente che mai, Fireware Pro 10 fornisce:

- **Traffic Shaping** – 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 affidabilità** (attiva/passiva) – Offre ridondanza hardware con un'appliance in standby, oltre a failover WAN e failover VPN
- **Supporto VLAN** – Crea configurazioni di rete logiche piuttosto che fisiche le quali riducono i requisiti hardware, aumentano il controllo su più tipi di traffico, forniscono una interoperabilità più completa e facilitano la creazione di sottoreti
- **Bilanciamento del carico multi-WAN** – Distribuisce e bilancia il carico del traffico in uscita su più ISP per ottenere una maggiore efficienza della rete
- **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
- **Bilanciamento del carico del server** – Consente di proteggere con facilità le "server farms", ad esempio, di commercio elettronico rivolto al pubblico
- **SSL VPN** – Consente di proteggere con facilità le "server farms", ad esempio, di commercio elettronico rivolto al pubblico

Core™ UTM Bundle – Unica soluzione, una sola licenza, un grande prezzo

Tutto il necessario per una gestione unificata delle minacce in singolo e comodo con Firebox X Core e-Series UTM Bundle. Ogni pacchetto offre una convenienza eccezionale e include:

- Appliance di protezione Firebox X Core e-Series
- WebBlocker*
- spamBlocker*
- Gateway AV/IPS con Anti-Spyware*
- LiveSecurity® Service*

Dall'acquisto iniziale fino alla gestione corrente della protezione, un Firebox X Core e-Series Bundle snellisce la gestione della protezione di rete e fornisce 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 **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: +39-335-7030721 · WEB: www.watchguard.com

COMMON CRITERIA EAL4+ CERTIFIED · IPSec · Firewall · Firewall Level 1 · VPN · Web Filtering · Intrusion Prevention · Anti-Spam

WatchGuard™