WatchGuard®

SCHEDA INFORMATIVA PRODOTTO

Firebox® X Edge

e-Series

- **Prevenzione attiva da attacchi integrati** per salvaguardarsi da minacce nuove ed emergenti
- **Abbonamenti di sicurezza costantemente aggiornati** per una protezione aggiornata al minuto
- **Opzioni di networking affidabili e flessibili** assicurano che gli uffici remoti e le filiali siano sempre protetti e collegati
- **Semplice gestione e impostazione priorità** del traffico di rete con QoS
- **Gestione della protezione intuitiva e unificata** per semplificare in maniera significativa l'amministrazione della rete
- **Scalabile e aggiornabile** per proteggere l'investimento della soluzione di protezione
- **Team globale di esperti nella sicurezza** sempre a disposizione
- **Conforme RoHS e WEEE**

Tecnologia eco-compatibile

Protezione forte e affidabile per le reti delle piccole aziende

Le reti delle piccole aziende richiedono la stessa protezione completa cui si affidano le aziende più grandi ma senza la complessità delle grandi reti. Oggi le piccole aziende possono raggiungere facilmente questo obiettivo con l'appliance di protezione Firebox® X Edge e-Series di WatchGuard. Firebox X Edge è una soluzione completa di gestione unificata delle minacce (UTM) che blocca attacchi Zero Day, spyware, virus, trojan horse, spamming e minacce combinate per assicurare la protezione dei dati. I tunnel VPN e per uffici filiali facili da configurare forniscono un accesso remoto criptato alle risorse di rete, mentre le funzionalità di failover WAN e VPN consentono di assicurare la connettività e i tempi di attività. Le flessibili funzionalità di rete consentono inoltre l'impostazione della priorità per il traffico e la larghezza di banda al fine di raggiungere la massima efficienza e prestazioni di rete. Con una intuitiva e ricca interfaccia utente, Edge è una scelta eccellente per aziende con risorse IT limitate ed è disponibile in modelli wireless e cablati per rispondere a specifiche esigenze di rete.

Prevenzione attacchi Zero Day effettiva

La robusta protezione di rete fornita da Firebox X Edge si basa su sofisticate tecnologie di proxy. Le difese proattive e integrate bloccano molti tipi di attacco inclusi overflow del buffer, corruzione del DNS, e attacchi DoS/DDoS. Questo esclusivo livello di protezione Zero Day è di gran lunga superiore ai prodotti che per bloccare le minacce conosciute si affidano semplicemente al filtraggio pacchetti e alla tecnologia basata sulle firme. Mette a disposizione robuste difese dal momento in cui viene accesa l'appliance Firebox.

Protezione aggiuntiva nelle aree critiche di attacco

I potenti abbonamenti di sicurezza forniscono livelli aggiuntivi di protezione di rete. Completamente integrati nell'appliance Edge e costantemente aggiornati, collaborano con le difese integrate per assicurare una completa gestione unificata delle minacce.

- **spamBlocker**
  Offre una percentuale di blocco in tempo reale di email indesiderate che raggiunge il 97%, indipendentemente da contenuto, formato o lingua
- **WebBlocker**
  Aumenta la produttività, elimina le responsabilità legali e diminuisce i rischi di protezione bloccando l'accesso a contenuti Web nocivi e non appropriati
- **Gateway AntiVirus/Intrusion Prevention Service**
  Blocca spyware, trojan horse, virus conosciuti, iniezioni SQL e violazioni della policy al gateway

Gestione centralizzata di più appliance

Quando si distribuiscono più appliance Firebox X Edge come endpoint per una rete Firebox® X Core™ o Firebox® X Peak™, le appliance Edge sono gestite centralmente utilizzando WatchGuard System Manager (WSM). WSM snellisce la gestione VPN e della configurazione, consentendo di inviare gli aggiornamenti software a tutte le appliance Edge gestite, di impostare policy di protezione unificate attraverso tutta la rete e creare con facilità tunnel VPN in drag-and-drop. WSM fornisce inoltre logging completo, flessibili criteri di protezione e strumenti di monitoraggio in tempo reale.

Funzionalità complete di networking

Opzioni di networking affidabili e flessibili assicuranco che le piccole aziende e gli uffici remoti siano sempre protetti e connessi.

Gestione del traffico sicura ed efficiente

- Protezione per più indirizzi IP esterni
- Supporto per Dynamic NAT, 1:1 NAT e PAT (Port Address Translation)
- Riduzione dei tempi di inattività della rete con il failover WAN su una porta secondaria o una connessione dial-up attraverso la porta seriale
- Ottimizzazione della connettività con il failover VPN completo

Qualità del servizio (QoS) configurabile ed affidabile

- Impostare la priorità di assegnazione dinamica della larghezza di banda per dare precedenza al traffico mission-critical e time-sensitive, come VoIP, sul traffico di importanza meno critica per l'organizzazione

Impareggiabile semplicità di utilizzo

Firebox X Edge viene gestito attraverso un'intuitiva interfaccia Web semplice e diretta. Facile da configurare e utilizzare, consente al responsabile IT di ridurre i tempi di amministrazione della rete e fornisce agli amministratori meno esperti tutta l'indispensabile semplicità di utilizzo.

Flessibile protezione wireless

I modelli wireless includono un punto di accesso wireless 802.11b/g con opzioni di protezione WPA, WPA2 e WEP.

- Tre distinte zone di protezione (VAP) forniscono agli amministratori il controllo sui privilegi di accesso a Internet per differenti gruppi di utenti

Protezione dell'investimento di sicurezza

Mentre l'azienda cresce, è possibile eseguire l'aggiornamento alla capacità e alle funzionalità di protezione di un modello superiore della gamma applicando una semplice chiave di licenza software. È facile, e non è necessario acquistare hardware aggiuntivo.

WatchGuard™

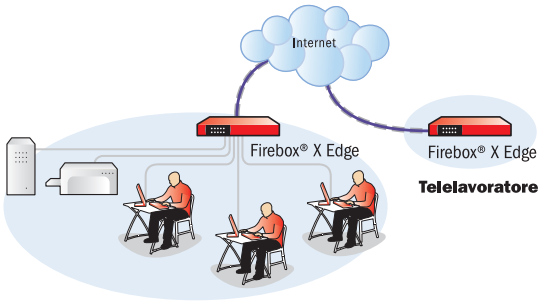
Stronger Security, Simply Done™

Mantieni la tua azienda protetta e collegata

La gestione della rete di una piccola azienda è un'attività impegnativa. Di fronte alle numerose minacce nocive provenienti da Internet, è necessario disporre di una solida protezione della rete che include una prevenzione degli attacchi attiva: qualcosa che un semplice router non è in grado di fornire. La soluzione deve integrare difese multilivello che blocchino spamming, spyware, virus ed attacchi basati su Web. Le piccole aziende devono inoltre affrontare numerose problematiche che riguardano anche le grandi aziende, incluse le esigenze di numerose applicazioni, alti volumi di traffico e connettività protetta per gli utenti remoti. Se si considerano inoltre le risorse limitate delle piccole aziende, è necessario individuare una soluzione semplice da utilizzare ed in grado di espandersi insieme all'azienda.

La soluzione: **Firebox X Edge** di WatchGuard - Un'appliance progettata per rispondere alle esigenze di networking delle piccole aziende.

Protezione di rete per piccole aziende

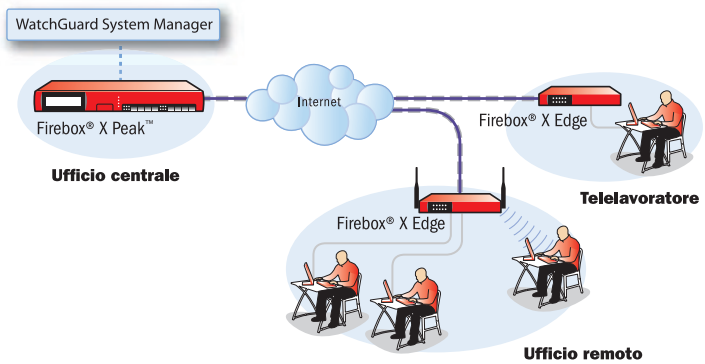


Protezione del perimetro di rete

Estendere una robusta protezione di rete dall'ufficio centrale fino alle filiali e agli uffici remoti non dovrebbe rappresentare un'attività onerosa in termini di risorse per il reparto IT. È necessaria la stessa potente protezione nel perimetro della rete ed essere inoltre in grado di gestire l'intero sistema da una singola ubicazione centrale. Per ottenere la massima efficienza ed efficacia dei costi, tutti i componenti della soluzione di protezione devono interoperare in maniera completamente integrata, fornendo la possibilità di impostare policy di protezione uniformi per l'intera rete aggiornabili globalmente con pochi clic del mouse. L'appliance dell'ufficio remoto e della filiale, cablata o wireless, deve disporre di funzionalità avanzate di networking per garantire che il traffico tra gli uffici e la banda siano gestiti in base alla priorità.

La soluzione: **Firebox X Edge** di WatchGuard - la soluzione ideale per estendere la potenza del Firebox X Core o Firebox X Peak dall'ufficio centrale fino agli uffici remoti o alle filiali.

Protezione di uffici remoti e siti di telelavoratori



Perché scegliere Firebox X Edge per la tua piccola azienda?

- **Semplice configurazione e gestione** attraverso un'intuitiva interfaccia utente Web. Non è necessario essere un esperto informatico per configurare l'appliance
- **Robusta protezione immediatamente disponibile,** con impostazioni predefinite intelligenti e configurazioni guidate che forniscono una solida protezione fin dal primo giorno di utilizzo
- **Abbonamenti di antispamming, antispyware, antivirus, prevenzione intrusioni e filtraggio URL completamente integrati** per fornire una completa soluzione di gestione unificata delle minacce per mantenere sicura la rete
- **Opzioni di networking affidabili e flessibili** [] inclusi 1:1 NAT, Dynamic NAT, PAT (Port Address Translation) e supporto per indirizzi IP esterni multipli
- **Funzionalità di gestione del traffico e QoS (Quality of Service)** che assicurano che il traffico mission-critical, ad esempio VoIP, abbia la precedenza sulla larghezza di banda gestita
- **Tempi di inattività di rete ridotti** con funzionalità di failover WAN/WAN nel caso di disconnessione della linea alla porta WAN principale
- **Servizi per ospiti e protezione wireless,** che consentono alle aziende di fornire un accesso Internet controllato per utenti ospiti, senza compromettere la protezione della rete
- **Accesso protetto a risorse di rete critiche** per telelavoratori che lavorano da workstation fuori sede, con autenticazione e VPN per utenti mobili
- **Aumento della capacità e delle funzionalità di networking/protezione** a fronte di esigenze in crescita utilizzando una semplice chiave di licenza software - non è necessario nuovo hardware

Perché scegliere Firebox X Edge per uffici remoti/filiali?

- Le funzionalità di **gestione unificata delle minacce** (UTM) includono prevenzione attacchi Zero Day, antispyware, antispamming, antivirus, prevenzione delle intrusioni e filtraggio URL che forniscono una potente protezione a più livelli lungo il perimetro della rete
- La **gestione configurazione centralizzata** fornita da WatchGuard System Manager (WSM) nell'appliance Firebox X Core o Peak semplifica in maniera significativa l'amministrazione di uffici remoti/filiali
- **Protezione della connettività** tra uffici con tunnel VPN per uffici filiali semplici da configurare. Con WSM, è possibile creare tunnel VPN drag-and-drop in tre semplici passaggi, risparmiando tempo prezioso di configurazione e manutenzione
- Gli **aggiornamenti del software per appliance** sono inviati alle appliance Edge remote con WSM in modo che le policy di protezione sia applicate in maniera rapida e universale e il software per l'appliance risulti sempre aggiornato
- Le **funzionalità avanzate di networking** di Firebox X Edge includono 1:1 NAT, Dynamic NAT, PAT (Port Address Translation) e supporto di IP esterni multipli per fornire opzioni di networking affidabili e flessibili
- **QoS con gestione dinamica del traffico** assicura che sia gestita la larghezza di banda e che sia impostata la priorità del traffico mission-critical, ad esempio VoIP, sul traffico di importanza non critica
- **Collegamento di ospiti in rete senza compromettere la protezione**
  I servizi wireless per ospiti forniscono un accesso Internet controllato e protetto, utilizzando il punto di accesso wireless dell'appliance Edge

Specifiche	Firebox® X10e WG50010	Firebox® X10e-W WG50011 N. America WG50012 Internazionale WG50015 Cina WG50012-JP Giappone	Firebox® X20e WG50020	Firebox® X20e-W WG50021 N. America WG50022 Internazionale WG50025 Cina WG50022-JP Giappone	Firebox® X55e WG50055	Firebox® X55e-W WG50056 N. America WG50057 Internazionale WG50060 Cina WG50057-JP Giappone
Modello aggiornabile	da X20e o X55e	a X20e-W o X55e-W	a X55e	a X55e-W	N/D	N/D
Velocità firewall†	100 Mbps		100 Mbps		100 Mbps	
Velocità VPN†	35 Mbps		35 Mbps		35 Mbps	
Gateway AV/IPS	Opzionale		Opzionale		Opzionale	
Blocco spamming	Opzionale		Opzionale		Opzionale	
Filtraggio URL	Opzionale		Opzionale		Opzionale	
Porte seriali	1		1		1	
Interfacce 10/100	6		6		6	
Zone di protezione (incl.)	2		2		2	
Sessioni contemporanee	6,000		8,000		10,000	
Nodi supportati (IP LAN)	15 (aggiornabili a 20)		30		Illimitati	
Tunnel VPN ufficio filiale	5		15		25	
Tunnel VPN utenti mobili (incl./max.)	1/11		5/25		5/55	
Limite DB autenticazione utenti locali	200		200		200	
WAN Failover	Opzionale		Opzionale		Incluso	
VPN Failover	Incluso		Incluso		Incluso	

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

Funzionalità

Funzionalità di protezione

- Firewall Stateful Packet Filter
- Controllo approfondito a livello applicativo in uscita
  - HTTP
  - FTP
  - POP3
- Controllo approfondito a livello applicativo in entrata
  - SMTP
- Protocol Anomaly Detection
- Pattern Matching
- Protezione riassemblaggio pacchetti frammentati
- Protezione pacchetti errati
- Elenco statico origini bloccate

VPN

- Crittografia (DES, 3DES, AES)
- IPSec
  - SHA-1, MD5
  - IKE - Chiave precondivisa, certificato Firebox, certificati terze parti (x.509)
- Passthrough IPSec
- Passthrough PPTP
- Dead Peer Detection (RFC 3706)
- Crittografia basata sull'hardware
- Supporto PPTP (10 utenti)

Autenticazione utenti

- XAUTH
  - LDAP
  - Windows® Active Directory
- Autenticazione locale
- Windows® NT
- Windows® 2000
- Windows® 2003

Assegnazione indirizzi IP

- Statico
- Client PPPoE
- Server DHCP
- Client DHCP
- DHCP Relay

Funzioni di ridondanza

- Failover WAN
- Failover WAN su modem seriale
- Failover VPN

Gestione e priorità traffico

- Impostazione priorità traffico basata su policy
- Impostazione priorità traffico VPN
- Full Marking Support
  - Diffserv
  - Servizi IP
- QoS (4 code di impostazione priorità)
  - Interattivo
  - Alto
  - Medio
  - Basso

Networking avanzato

- NAT statico
- NAT dinamico
- 1:1 NAT
- IPSec NAT Traversal
- PAT (Port Address Translations) basate su policy
- Fino a 8 indirizzi IP esterni
- Routing statico
- DNS dinamico

Modalità di funzionamento

- Switch integrato 3 porte (livello 2)
- Modalità routing (livello 3)

Software di gestione

- Interfaccia grafica utente Web
- WatchGuard System Manager (WSM) v9.1 o superiore

Logging/Reporting

- Report WSM di protezione e attività
- Report di attività della protezione in abbonamento basati su Web
- Syslog
- Report compatibili con WebTrends® (disponibile per gli utenti WSM)
- Report HTML (disponibile per gli utenti WSM)
- Canale log criptato

Software per appliance

- v8.x o superiore

Funzionalità per la protezione wireless

- Wireless Guest Services
- 802.11b/g
- WPA
- WPA2
- WEP

Certificazioni

- Common Criteria EAL4
- West Coast Labs Checkmark
  - Firewall Level 1, VPN, Web Filtering, Intrusion Prevention, Anti-Spam

Supporto e manutenzione

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

Dimensioni e alimentazione

Dimensioni appliance	
Cablata	7,4" x 6,5" x 1,4" (18,8 x 16,5 x 3,6 cm)
Wireless (antenne estese)	10,6" x 6,5" x 7,3" (26,9 x 16,5 x 18,5 cm)
Dimensioni confezione	
Cablata	13,3" x 11,9" x 4,4" (33,8 x 30,2 x 11,2 cm)
Wireless	13,3" x 11,9" x 4,4" (33,8 x 30,2 x 11,2 cm)
Peso appliance	
Cablata	1,8 lbs (0,8 Kg)
Wireless	1,9 lbs (0,9 Kg)
Peso totale	
Cablata	3,3 lbs (1,5 Kg)
Wireless	3,8 lbs (1,7 Kg)
Peso WEEE	
Cablata	2,0 lbs (0,9 Kg)
Wireless	2,1 lbs (1,0 Kg)

Alimentazione CA	100-240 VCA autosensing
Assorbimento corrente	U.S.: 12 Watts
	Resto del mondo: 172 Cal/min o 41 BTU/hr
Montabile su scaffale	No

Caratteristiche ambientali

Temperatura operativa	da 0 a 45° C
Temperatura non operativa	da -10 a 70° C
Umidità operativa	10 - 85%
Umidità non operativa	5 - 90% in assenza di condensa a 55° C
Vibrazione casuale non operativa	da 7 - 28 Hz 0,001 a 0,01 G2 per Hz
Shock meccanico operativo	20 G con onda sinusoidale 1/2 durata 11 Msec
Conforme WEEE/RoHS	Sì

Firebox X Edge

Firebox X Edge Wireless

Guida e supporto esperti

LiveSecurity® Service fornisce servizi di supporto innovativi e di alto valore per amministratori IT. Questo versatile programma offre:

- Garanzia hardware con sostituzione anticipata hardware
- Supporto tecnico con tempo di risposta target di 4 ore
- Aggiornamenti software per funzionalità avanzate e nuove funzioni
- Avvisi sintetici sulle minacce con istruzioni chiare
- Innovativi strumenti di training sulla sicurezza

Al momento dell'acquisto di un'appliance Firebox X Edge, selezionare l'abbonamento iniziale di 90 giorni o 1 anno a LiveSecurity.

Unica soluzione, una sola licenza, un grande prezzo.

Firebox X Edge e-Series UTM Bundle fornisce tutto il necessario per una completa gestione unificata delle minacce per la piccola azienda o l'ufficio remoto. Ogni pacchetto offre una convenienza eccezionale e include:

- Appliance Firebox X Edge e-Series
- Gateway AV/IPS (1 anno)
- spamBlocker (1 anno)
- WebBlocker (1 anno)
- LiveSecurity Service (1 anno)

Dall'acquisto iniziale fino alla gestione corrente della sicurezza , il Firebox X Edge e-Series UTM Bundle snellisce la gestione della sicurezza fornendo allo stesso tempo una potente protezione della rete. Acquista il bundle e risparmia!

Prova GRATUITA di 30 giorni

È possibile ricevere la versione di prova gratuita per 30 giorni di **Gateway AntiVirus/IPS, spamBlocker e WebBlocker** acquistando Firebox X Edge. Per informazioni dettagliate, contattare il proprio rivenditore.

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

E-MAIL: italy@watchguard.com · VENDITE: +39-335-7030721 · WEB: www.watchguard.com

IPSec · Firewall Level 1 · VPN · Web Filtering · Intrusion Prevention · Anti-Spam

WatchGuard