



Soluzione completa di 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. Questa robusta 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 realizzata 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 rendono possibili nuovi tipi di attacchi, le difese proattive integrate di Firebox X Core 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.

Gestione unificata intuitiva

WatchGuard® System Manager (WSM) è l'intuitiva interfaccia grafica utilizzata per gestire centralmente tutte le funzionalità delle soluzioni Firebox X Core UTM. Gli amministratori sono in grado di accedere a potenti strumenti di monitoraggio e reporting cronologici e in tempo che forniscono una eccellente visibilità della protezione delle rete e dell'attività degli utenti senza costi nascosti o la necessità di acquisti aggiuntivi. L'utilizzo di una singola interfaccia per gestire tutti gli aspetti della propria soluzione di protezione, inclusa la distribuzione di più appliance, consente di risparmiare tempo e denaro.

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 Core per fornire una combinazione imbattibile di funzionalità di protezione. Questi livelli di protezione aggiuntivi sono completamente integrati e il prezzo degli abbonamenti viene calcolato per appliance e non per utente allo scopo di evitare l'aumento dei costi. Tutti i servizi in abbonamento 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.

Gateway AV/IPS con Anti-Spyware

Blocca spyware, trojan horse, virus e attacchi basati sul Web con una robusta protezione basata su firme al gateway.

spamBlocker con quarantena

È il migliore servizio antispamming del settore, con una percentuale di blocco di e-mail indesiderate che raggiunge il 97%, con funzionalità complete di quarantena.

WebBlocker

Sorveglia i confini del Web accessibile dai dipendenti dal luogo di lavoro e protegge la rete dai siti maligni.

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 potenziare 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 Firewall® al software per appliance avanzate Firewall® Pro allo scopo di ampliare le funzionalità di rete con reti VLAN, l'alta affidabilità, routing dinamico 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 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.

- **Protezione completa** per difendere la rete da minacce maligne
- **Prevenzione dagli attacchi Zero Day** blocca attivamente le nuove minacce
- **Gestione della protezione di rete** per risparmiare tempo
- Servizi di protezione **continuamente aggiornati** per una protezione allineata al minuto
- **Funzionalità integrate aggiornabili** per una maggiore convenienza
- **Team globale di esperti sulla protezione** sempre a disposizione
- **Conforme a RoHS/WEEE**



Tecnologia eco-compatibile



Stronger Security, Simply Done™

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 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

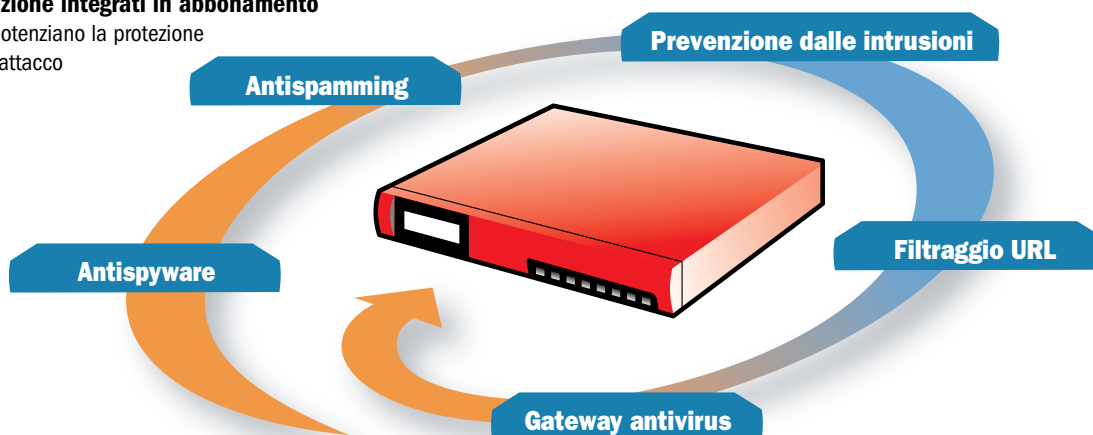
Vantaggi della protezione

- **Protezione Zero day**, 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 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
- **Il filtraggio URL** consente di limitare le risorse sul Web accessibili dai dipendenti sul luogo di lavoro al fine di aumentare la produttività e prevenire responsabilità legali, proteggendo al tempo stesso da contenuti 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 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. 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 conosciuti
- 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

- **Protezione Zero Day integrata** attraverso una potente tecnologia proxy per bloccare preventivamente 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, con una percentuale di e-mail indesiderate bloccate che arriva al 97%, indipendentemente da contenuto, lingua o formato del messaggio, incluso lo spamming basato su immagini
- La **quarantena** mantiene separati lo spamming e l'email sospetta dalla legittima email di importanza critica per l'organizzazione, 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 firewall¹	300+ Mbps	300+ Mbps	300+ Mbps
Velocità VPN¹	35 Mbps	50 Mbps	100 Mbps
Velocità AV¹	50 Mbps	70 Mbps	100 Mbps
Gateway AV/IPS con Anti-Spyware	Opzionale	Opzionale	Opzionale
Filtraggio URL	Opzionale	Opzionale	Opzionale
Blocco spamming	Opzionale	Opzionale	Opzionale
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
Porta seriale	1	1	1
VLAN*	25	25	25
Tunnel VPN ufficio filiale (incl./max.)	35/45	100/100	600/600
Tunnel VPN utenti mobili (incl./max.)	5/75	50/100	400/400
Limite database autenticazione utenti locali	250	1.000	5.000
Modello aggiornabile	Sì	Sì	No
Software appliance avanzate Fireware® Pro	Opzionale	Opzionale	Opzionale

¹ 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
- 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 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
- 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
- RIPv1, v2
- Routing dinamico*
 - BGP4, OSPF
 - RIPv1, v2
- Routing basato su policy*

Networking

- VLAN*
 - Bridging, Tagging, Modalità routing
- Bilanciamento del carico del 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 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
- 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
- West Coast Labs Checkmark
 - Firewall Level 1, VPN, Web Filtering, Intrusion Prevention, Anti-Spam

Supporto e manutenzione

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

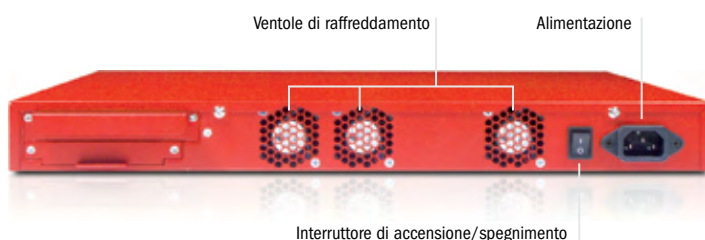
*Disponibile con l'aggiornamento del software per appliance avanzate Fireware Pro

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 di WatchGuard per gli ambienti di reti più impegnativi. Ora più potente che mai, Fireware Pro 9.1 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
- **VLAN** - Crea configurazioni di rete logiche piuttosto che fisiche che 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

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 Firebox X Core e-Series X550e, X750e o X1250e
- 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

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, Fireware, LiveSecurity, Peak, Core, LiveSecurity 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 WGCE66360_090607

