



Maggiore protezione per aziende in crescita

Firebox[®]X Core™, la nostra linea principale di appliance di protezione integrate fornisce una forte protezione disponibile immediatamente. Potente ma semplice da gestire, con un'intuitiva interfaccia utente, Firebox X Core utilizza più livelli di protezione per controllare il traffico di rete e bloccare attivamente virus, worm, spyware, trojan horse e minacce combinate senza affidarsi alle firme.

Protezione integrata

Firebox X Core fornisce una protezione completa integrando Stateful Packet Firewall, VPN, Intelligent Layered Security, antivirus gateway, Intrusion Prevention, filtro dei contenuti Web e consentendo di ridurre in tal modo i tempi e i costi associati alla gestione di soluzioni multiple-point.

Espansione per la crescita

Unica appliance di protezione integrata completamente aggiornabile disponibile attualmente sul mercato, Firebox X Core consente di accrescere in modo semplice prestazioni, capacità e funzioni di networking per rispondere alle esigenze di aziende in crescita.

- **Aumento delle prestazioni** – Per ottenere prestazioni superiori è possibile aggiornare Firebox X Core a qualsiasi modello superiore della linea attraverso una semplice chiave di licenza
- **Aggiunta di opzioni di protezione** – Alle chiavi di licenza consentono di aggiungere opzioni quali gateway antivirus, prevenzione delle intrusioni, filtro dei contenuti Web e blocco dello spamming
- **Aggiornamento a Fireware™ Pro** – Il nostro sistema operativo avanzato di rete consente di rispondere alle esigenze delle reti più impegnative

Esperienza utente intuitiva

Firebox X Core viene configurato e gestito da WatchGuard® System Manager (WSM), un'interfaccia utente intuitiva che semplifica la protezione di rete per gli esperti IT e assicura l'indispensabile semplicità di utilizzo agli amministratori di rete meno esperti. WSM include:

- **Impostazioni predefinite intelligenti** – Predefinite in WatchGuard System Manager, assicurano protezione dal momento in cui il cliente accende l'appliance Firebox

WatchGuard® fornisce subito una maggiore protezione

La protezione ILS (Intelligent Layered Security) è il cuore di Firebox X Core e fornisce una protezione potente e attiva. ILS esamina il traffico per identificare e bloccare minacce maligne che includono virus, worm, spyware, trojan horse e minacce combinate. Attraverso la comunicazione dinamica e collaborativa tra i diversi livelli, ILS assicura una robusta protezione ottimizzando allo stesso tempo le prestazioni del sistema.

- **Protezione immediatamente disponibile** Il livello di controllo approfondito delle applicazioni di ILS analizza il traffico per individuare tutto quanto non sia conforme a protocolli, comportamenti e schemi standard in Internet. È possibile avere subito a disposizione funzionalità di protezione nei confronti di minacce emergenti durante il periodo di vulnerabilità che precede la disponibilità di nuove firme.
- **Ottimizzato per prestazioni migliorate** ILS fornisce una comunicazione collaborativa tra i differenti livelli di protezione per mantenere sempre scorrevole il flusso dei dati.
- **Blocco di attacchi virus** Gli host che mostrano un comportamento sospetto, quale scansione delle porte e attacchi DoS, vengono identificati e aggiunti all'elenco di siti bloccati. Il traffico successivo proveniente da questi host viene bloccato automaticamente.
- **Cloaking di rete** Per rendere inaccessibili i servizi di rete per gli hacker alla ricerca di opportunità di intrusione.

- **Strumenti per una semplice personalizzazione** – Facilmente configurabile sulle specifiche esigenze aziendali grazie a funzionalità quali creazione di reti VPN mediante selezione e trascinato (drag-and-drop), procedure guidate intuitive e policy di protezione flessibili
- **Monitoraggio interattivo in tempo reale e reporting completo** – È sempre possibile essere a conoscenza di quanto accade in rete e intraprendere azioni immediate preventive o correttive

Guida e supporto esperti

LiveSecurity® Service di WatchGuard fornisce supporto e guida per mantenersi sempre protetti. È il servizio di supporto e manutenzione più completo disponibile sul mercato. Il servizio basato su abbonamento offre:

- **Avvisi di vulnerabilità precisi al minuto**
- **Aggiornamenti software**
- **Supporto tecnico**
- **Sostituzione anticipata dell'hardware**
- **Training, esercitazioni e risorse di self-help**

	X500 WG40500		X700 WG40700		X1000 WG41000		X2500 WG42500	
CLIENTE TARGET ▶	Piccole aziende che richiedono un'appliance abbordabile e integrata, dal semplice funzionamento.		Piccole aziende/filiali che richiedono un'appliance abbordabile e integrata in grado di crescere con le esigenze dell'azienda.		Medie aziende che richiedono soluzioni di protezione multilivello con una gestione centralizzata.		Aziende di medie dimensioni o distribuite che richiedono la massima protezione e connettività remota.	
Sistema operativo	WFS Standard	Fireware Pro Aggiornamento avanzato	WFS Standard	Fireware Pro Aggiornamento avanzato	WFS Standard	Fireware Pro Aggiornamento avanzato	WFS Standard	Fireware Pro Aggiornamento avanzato
Velocità firewall	100	110	150	160	225	240	275+	300+
Velocità	20	30	40	60	75	100	100	130
Sessioni concorrenti	20,000	25,000	50,000	75,000	200,000	200,000	500,000	500,000
Antivirus gateway per e-mail	Opzionale	-	Opzionale	-	Opzionale	-	Opzionale	-
Gateway AntiVirus/IPS	-	Opzionale	-	Opzionale	-	Opzionale	-	Opzionale
Filtro contenuti Web	Opzionale	Opzionale	Opzionale	Opzionale	Opzionale	Opzionale	Opzionale	Opzionale
Blocco spamming	Opzionale	-	Opzionale	-	Opzionale	-	Opzionale	-
Interfacce (incluse/totali)	3/6*	6	3/6*	6	3/6*	6	3/6*	6
Tunnel VPN filiali	0**	0**	100	100	500	500	1,000	1,000
Tunnel VPN utenti mobili	50	50	100	100	1,000	1,000	1,000	1,000
Licenze client utenti mobili (incluse)	5	5	10	10	50	50	1,000	1,000
Gestione VPN centralizzata	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
Licenze antivirus desktop gestite	5	5	5	5	5	5	5	5
Utenti (indirizzi IP LAN)	Illimitati	Illimitati	Illimitati	Illimitati	Illimitati	Illimitati	Illimitati	Illimitati
Utenti autorizzati	250	250	250	250	1,000	1,000	5,000	5,000
Funzioni avanzate di networking								
Failover WAN e condivisione carico	-	Sì	-	Sì	-	Sì	-	Sì
Gestione traffico e QoS	-	Sì	-	Sì	-	Sì	-	Sì
Porte indipendenti	-	Sì	-	Sì	-	Sì	-	Sì
Alta disponibilità (attiva/passiva)	Opzionale*	Sì	Opzionale*	Sì	Opzionale*	Sì	Opzionale*	Sì
Routing dinamico (BGP4, OSPF, RIP)	-	Sì	-	Sì	-	Sì	-	Sì
WatchGuard System Manager (WSM)	7.x	8.x	7.x	8.x	7.x	8.x	7.x	8.x
Logging protetto	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
SNMP	-	Sì	-	Sì	-	Sì	-	Sì
Reporting (HTML, NetIQ WebTrends)	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
Garanzia hardware	1 anno	1 anno	1 anno	1 anno	1 anno	1 anno	1 anno	1 anno
Abbonamento iniziale LiveSecurity® Service	90 giorni	90 giorni	90 giorni	90 giorni	90 giorni	90 giorni	90 giorni	90 giorni
Assorbimento di corrente	U.S.A.: 50 Watt Resto del mondo: 717 Cals/min, 2,9 BTU/min							
Dimensioni e peso	Profondità = 240mm		Larghezza = 426mm		Altezza = 45mm		Peso = 4,39 kg	

*Disponibile con il bundle di aggiornamento 3 porte/alta disponibilità **Aggiornabile a 50 tunnel VPN filiali

Siete pronti per Fireware™ Pro?

Il robusto sistema operativo WatchGuard Firebox System (WFS) è incluso in Firebox X Core. Di fronte a esigenze di rete in crescita, è possibile eseguire l'aggiornamento a Fireware™ Pro, il sistema operativo avanzato di rete e protezione destinato alle reti più impegnative. Passate a Fireware Pro per:

- **Maggiore controllo** – Per il controllo granulare degli allegati in arrivo nella rete. Fornisce la possibilità di accettare tipi e ubicazioni di file in base all'URL in modo da bloccare le minacce senza interrompere le attività chiave della rete.
- **Failover multi-WAN e load sharing** – Consente di utilizzare fino a quattro connessioni ISP per distribuire il traffico e fornire il failover, aumentando prestazioni e disponibilità della rete.

- **Gestione del traffico e QoS basati su policy** – Assicura che tutte le applicazioni cruciali per l'azienda abbiano a disposizione tutta la larghezza di banda necessaria.
- **Porte indipendenti** – È possibile configurare qualsiasi porta come esterna, opzionale (DMZ) oppure interna (Trusted).
- **High Availability (attiva/passiva)** – Offre ridondanza hardware con un'appliance in standby.
- **Routing dinamico (BGP, OSPF, RIP)** – Ottimizza flessibilità, ridondanza ed efficienza della rete attraverso l'aggiornamento dinamico delle tabelle di routing.
- **Gateway AntiVirus/Intrusion Prevention Service** – Disponibile come opzione per gli utenti di Firebox X Core che eseguono l'aggiornamento a Fireware Pro.

Per ulteriori informazioni su Firebox X Core, visitare www.watchguard.com/products/fbxcare.asp

INDIRIZZO:
505 Fifth Avenue South
Suite 500
Seattle, WA 98104

E-MAIL:
italy@watchguard.com

VEDITE ITALIA:
+39-011-9542227

FAX:
+39-011-9542228

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.

© 2005 WatchGuard Technologies, Inc. Tutti i diritti riservati. WatchGuard, il logo WatchGuard, Firebox, Fireware, 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 WGCI66240_0405

Per informazioni dettagliate su quale linea di prodotti di protezione WatchGuard è più adatta alle vostre esigenze, visitare l'indirizzo: www.watchguard.com/compare