

# WatchGuard® XTMv

Virtualizzazione della sicurezza per le esigenze delle aziende d'oggi

## Utilizzate appliance virtuali nella vostra infrastruttura virtuale

- Funzionalità e servizi UTM/NGFW primi in assoluto nell'infrastruttura virtuale
- Facili da scaricare, abilitare, installare e gestire (WSM, web, CLI)
- Sfruttano la flessibilità e le capacità di vSphere e Hyper-V
- Più modelli per aziende di qualsiasi dimensione
- Città universitarie, cloud/hosting, integrazione di filiali
- Installazione in base al cliente, al reparto o all'applicazione

*Aziende di tutte le dimensioni stanno ricorrendo alla virtualizzazione per ridurre i costi e aumentare l'efficienza, la disponibilità e la flessibilità delle loro risorse IT. Ma per la virtualizzazione si deve pagare un prezzo: gli ambienti virtuali sono complessi da gestire e prestano il fianco alle minacce per la sicurezza. Il reparto IT deve essere preparato. Adesso le applicazioni possono essere protette, le risorse possono essere massimizzate e il reparto IT può cogliere i vantaggi di avere un solo sistema di gestione, unificato – che non corra rischi per quanto riguarda la sicurezza. WatchGuard XTMv porta nel mondo della virtualizzazione le funzionalità di sicurezza di rete migliori nella loro classe. Con il monitoraggio in tempo reale, il supporto multiWAN e soluzioni scalabili adattabili a qualsiasi azienda indipendentemente dalle sue dimensioni, i vostri ambienti virtuali possono essere tanto sicuri quanto quello fisico.*

Le soluzioni virtuali WatchGuard offrono flessibilità ineguagliata di installazione. Potete scegliere di installare un mix di appliance hardware e virtuali, funzionanti insieme e gestite da una piattaforma centralizzata. Le appliance virtuali WatchGuard offrono tutti i servizi di sicurezza e di rete presenti nelle nostre appliance fisiche e possono essere installate in base al cliente, al reparto o all'applicazione, per la vostra infrastruttura virtuale.

## **Virtualizzate il tradizionale firewall gateway per ottenere flessibilità senza precedenti – proteggendo il confine interno**

WatchGuard XTMv protegge non solo il perimetro fisico del datacenter, ma anche il "confine virtuale". Adesso potete implementare facilmente criteri di protezione dei dati residenti nel database aziendale dall'infrastruttura di messaggistica o le informazioni sul personale riservate dai dati finanziari di altre divisioni – anche quando vengono utilizzati gli stessi server.

## **Integrate più firewall per ottenere efficienze ad alto impatto – protezione multi-tenant**

I service provider – di servizi hosting, cloud o di sicurezza gestita – possono impiegare istanze multiple di XTMv sui server lungo il perimetro dei loro datacenter. Questi firewall virtuali sono isolati l'uno dall'altro, così che è possibile garantire contratti a livello di servizio (SLA) a ciascun tenant e una modifica della configurazione di uno di essi non influisce sugli altri; ciò nonostante, possono essere gestiti tutti dal provider tramite una sola intuitiva console.

## **Eliminate i costi dell'hardware ridondante pur proteggendo le reti virtuali – integrazione delle filiali**

A mano a mano che le filiali e le divisioni integrano i server locali – file, stampa, voce e altro ancora – in un solo modulo, è possibile installare un firewall virtuale sul server fisico, isolando tutto il traffico da Internet pubblica. Un singolo tunnel VPN può fornire un percorso di ritorno sicuro ai datacenter aziendali o ai cloud privati virtuali – assicurando contenimenti dei costi in ogni sede senza andare a scapito della sicurezza.

## Edizioni WatchGuard XTMv

	Piccoli uffici	Medi uffici	Grandi uffici	Datacenter
<b>Velocità massima e connessioni</b>				
Velocità max firewall <sup>†</sup>	1 Gb/s	2,5 Gb/s	5 Gb/s	Senza limiti
Interfacce virtuali	10	10	10	10
Nodi supportati (IP rete locale)	Senza limiti	Senza limiti	Senza limiti	Senza limiti
Connessioni simultanee (bidirezionali)	30.000	350.000	1.250.000	2.500.000
Supporto VLAN	50	75	400	4.000
<b>Tunnel VPN</b>				
VPN ufficio remoto	50	600	6.000	10.000
IPSec VPN mobile	5	50	800	Senza limiti
SSL VPN mobile (incl/max)	10/50	10/600	6.000/6.000	Senza limiti
Utenti Autenticati	200	2.500	5.000	Senza limiti

### Next-Generation Security

Firewall	Stateful Packet Inspection, Deep Application Inspection, Proxy Firewall
Proxy applicativi	HTTP, HTTPS, SMTP, FTP, DNS, TCP, POP3
Protezione dalle minacce	Blocca spyware, attacchi DoS, pacchetti frammentati & malformati, minacce miste & altro ancora
VoIP	H.323, SIP, impostazione chiamata/sicurezza sessione
Abbonamenti di sicurezza	Application Control, Intrusion Prevention Service, Gateway AntiVirus, Reputation Enabled Defense, spamBlocker, WebBlocker

### VPN & autenticazione

Crittografia	DES, 3DES, AES a 128, 192/256 bit
IPSec	SHA-1, MD5, codice precondiviso IKE, cert. esterna
SSL	Thin client, Web
PPTP	Server & passthrough
Failover VPN	Sì
Single Sign-On	Autenticazione directory attiva trasparente
XAUTH	RADIUS, LDAP, Secure LDAP, Windows Active Directory
Altre autenticazioni utente	VASCO, RSA SecurID, basata su web, locale, Microsoft Terminal Services e Citrix

### Piattaforma e reti

Sistema operativo	Fireware® XTM / Fireware XTM Pro
Supporto Hypervisor	VMware vSphere 4.1, 5.0, 5.1 / Windows Server 2008 R2, 2012 (Hyper-V)
Assegnazione indirizzi IP	Statica, DHCP (server, client, relay), DynDNS, PPPoE
Instradamento	Statico, dinamico (BGP4, OSPF, RIP v1/2), basato sui criteri
QoS	8 code di priorità, diffserv, coda rigorosa modificata
Supporto VLAN	Modalità di instradamento, bridging, tagging
NAT	Statico, dinamico, 1:1, IPSec NAT trasversale, NAT basato sui criteri, IP virtuale
Altre reti	Indipendenza delle porte, failover WAN, bilanciamento del carico, modalità drop-in/trasparente

### Gestione

Piattaforma di gestione	WatchGuard System Manager (WSM) v.11.5.2 o successiva
Allarmi e notifiche	SNMP v2/v3, e-mail, avviso sistema di gestione
Supporto server	Registrazione, reporting, quarantena, WebBlocker, gestione
Interfaccia utente web	Supporta Windows, Mac e Linux con i browser più comuni
CLI	Include connessione diretta e script

### Certificazioni

Rete	IPv6 Ready Gold (instradamento)
------	---------------------------------

### SISTEMA OPERATIVO: FIREWARE® XTM

Le edizioni di XTMv per grandi uffici e datacenter escono dalla fabbrica con la versione Pro del sistema operativo Fireware XTM, offrendo le funzionalità avanzate di rete necessarie per reti di vaste dimensioni. La versione Pro può essere acquistata come aggiornamento delle edizioni per piccoli e medi uffici.

FUNZIONALITÀ DI RETE	FIREWARE XTM	FIREWARE XTM PRO
Instradamento	Statico, dinamico (RIP)	Dinamico (BGP4, OSPF, RIP v1/2), basato sui criteri
NAT	Statico, dinamico, 1:1, trasversale IPSec, basato sui criteri	IP virtuale per il bilanciamento del carico del server
SSL	10 tunnel SSL disponibili	Numero massimo di tunnel SSL disponibili per edizione
Altre funzionalità	Modalità drop-in/trasparente di indipendenza dalla porta, failover multiWAN	Bilanciamento del carico del server, bilanciamento del carico multiWAN

### GUIDA E SUPPORTO ESPERTI

Con ogni soluzione XTMv è incluso un abbonamento iniziale a LiveSecurity Service. LiveSecurity assicura assistenza tecnica in tempi molto brevi e aggiornamenti del software così che il programma è sempre aggiornato, e avvisi sulle minacce concisi.

### LA SICUREZZA VIRTUALE È INCLUSA NEL BUNDLE

Proteggete in modo completo la vostra infrastruttura virtuale con XTM Security Bundle, che include la scelta dell'edizione XTMv oltre a Application Control, Intrusion Prevention Service, Gateway AV, WebBlocker, Reputation Enabled Defense e spamBlocker nonché LiveSecurity\* per il supporto e la manutenzione. Un valore eccellente quando li acquistate insieme e riducete i costi!

\*XTMv Security Bundle per le edizioni per uffici di piccole/medie dimensioni include LiveSecurity standard con supporto tecnico 12/5. XTMv Security Bundle per grandi uffici e datacenter include LiveSecurity Plus con supporto tecnico 24/7.

<sup>†</sup>Le velocità massime dipendono dall'ambiente e dalla configurazione, compresa l'infrastruttura di virtualizzazione. Contattate il rivenditore WatchGuard autorizzato o chiamate direttamente WatchGuard per assistenza nella scelta del modello giusto per la vostra rete.

UFFICIO VENDITE ITALIA 800-911938 SITO WEB: [www.watchguard.it](http://www.watchguard.it)