

# WatchGuard® XTMv

## Virtualizando la Seguridad para las Necesidades Empresariales Actuales

### Ejecute dispositivos virtuales en su infraestructura virtual

- Las principales funciones y servicios de Gestión Unificada de Amenazas (UTM)/Firewall de Última Generación (NGFW) en la infraestructura virtual
- Fácil de descargar, habilitar, implementar y administrar (WSM, web, CLI)
- Aproveche la flexibilidad y disponibilidad de vSphere y Hyper-V
- Múltiples modelos para organizaciones de todos los tamaños
- Campus, nube/hosting, consolidación de sucursales
- Implementación por cliente, departamento o aplicaciones

*Las organizaciones de todos los tamaños están optando por la virtualización para reducir costos y aumentar la eficiencia, disponibilidad y flexibilidad de sus recursos de TI. Pero la virtualización tiene un precio. Los entornos virtuales son complejos de administrar y son vulnerables a amenazas a la seguridad. Se debe preparar la TI. Ahora las aplicaciones pueden asegurarse, los recursos pueden maximizarse y su departamento de TI puede obtener los beneficios de tener un único sistema de administración unificado, sin riesgos visibles a la seguridad. WatchGuard XTMv lleva la mejor seguridad de red al mundo de la virtualización. Con monitoreo en tiempo real, soporte de WAN múltiple y soluciones escalables para adaptarse a negocios de todos los tamaños, sus entornos virtuales pueden ser tan seguros como su entorno físico.*

Las soluciones virtuales de WatchGuard le ofrecen una flexibilidad de implementación sin precedentes. Puede optar por implementar una combinación de dispositivos virtuales y de hardware, que funcionen en conjunto y administrados desde una plataforma centralizada común. Los dispositivos virtuales WatchGuard brindan todos los servicios de red y seguridad que ofrecen nuestros dispositivos físicos y pueden implementarse en ambientes por cliente, departamento o aplicaciones, para su infraestructura virtual.

### **Virtualice el firewall de puerta de enlace tradicional para una flexibilidad sin precedentes: protegiendo el límite interno**

WatchGuard XTMv no sólo protege el perímetro físico del centro de datos, sino también el "límite virtual". Ahora puede implementar fácilmente una política que protege los datos en la base de datos corporativa de la infraestructura de mensajería, o información confidencial sobre recursos humanos de datos financieros de otras divisiones, incluso cuando se ejecutan en los mismos servidores.

### **Consolide múltiples firewalls para lograr eficiencias de alto impacto: protección de múltiples clientes**

Los proveedores de servicios: hosting, en la nube o servicios de seguridad administrados, pueden implementar instancias múltiples de XTMv en los servidores en el perímetro de sus centros de datos. Estos firewalls virtuales están aislados unos de otros, de manera que a cada cliente se le pueden garantizar Acuerdos de Nivel de Servicio, (Service Level Agreements, SLA), y un cambio de configuración en uno no afecta a los demás. Y aun así todos pueden ser administrados por el proveedor a través de una única consola intuitiva.

### **Elimine los costos de hardware redundantes mientras que asegura a la vez las redes virtuales: consolidación de sucursales**

A medida que las sucursales y divisiones más grandes consolidan los servidores locales —archivos, impresiones, voz y más— en una caja, se puede implementar un firewall virtual en el servidor físico, aislando todo el tráfico de la Internet pública. Un único túnel VPN puede proporcionar una ruta segura hacia los centros de datos corporativos o nubes privadas virtuales, obteniendo ahorros en los costos en todos los lugares sin comprometer la seguridad.

## Ediciones de WatchGuard XTMv

	Oficina Pequeña	Oficina Mediana	Oficina Grande	Centro de Datos
<b>Rendimiento y Conexiones</b>				
Rendimiento de Firewall†	1 Gbps	2.5 Gbps	5 Gbps	Ilimitado
Interfaces virtuales*	8 - 10	8 - 10	8 - 10	8 - 10
Nodos admitidos (IPs LAN)	Ilimitado	Ilimitado	Ilimitado	Ilimitado
Conexiones concurrentes (bidireccionales)	30.000	350.000	1.250.000	2.500.000
Soporte VLAN	50	75	400	4.000
<b>Túneles VPN</b>				
VPN Para Sucursales	50	600	6000	10.000
VPN IPSec Móvil	5	50	800	Ilimitado
VPN SSL Móvil (incl./máx.)	10/50	10/600	6.000/6.000	Ilimitado
Usuarios Autenticados	200	2.500	5.000	Ilimitado

\*Recuentos de interfaz de red se basan en restricciones hipervisor. vSphere soporta hasta 10 adaptadores, Hyper-V admite hasta 8 adaptadores non-legacy.

<b>Seguridad de Última Generación</b>	
Firewall	Inspección de Paquetes Stateful, Inspección Profunda de Aplicaciones, Firewall de Proxy
Proxies de Aplicación	HTTP, HTTPS, SMTP, FTP, DNS, TCP, POP3
Protección contra Amenazas	Bloquea spyware, ataques DoS, paquetes fragmentados & malformados, amenazas combinadas & y más
VoIP	H.323, SIP, Configuración de Llamada/Seguridad de Sesión
Suscripciones de Seguridad	Application Control, Intrusion Prevention Service, Gateway AntiVirus, Reputation Enabled Defense, spamBlocker, WebBlocker
<b>Autenticación &amp; VPN</b>	
Encriptación	DES, 3DES, AES 128/192/256-bit
IPSec	SHA-1, MD5, IKE clave compartida inicial, certificados de terceros
SSL	Cliente liviano, Web
PPTP	Server & Passthrough
Failover de VPN	Si
Single Sign-On (Inicio de sesión único)	Autenticación Transparente en Directorio Activo
XAUTH	RADIUS, LDAP, LDAP Seguro, Directorio Activo de Windows
Otras Autenticaciones de Usuarios	VASCO, RSA SecurID, basada en Web, local, Terminal Services de Microsoft y Citrix
<b>Plataforma y Redes</b>	
Sistema Operativo (OS)	Fireware® XTM / Fireware XTM Pro
Soporte de Hypervisor	VMware vSphere 4.1, 5.0, 5.1 / Windows Server 2008 R2, 2012 (Hyper-V)
Asignación de Direcciones IP	Estático, DHCP (servidor, cliente, relay), DynDNS, PPPoE
Enrutamiento	Estático, Dinámico (BGP4, OSPF, RIP v1/v2), basado en políticas
QoS	8 colas de prioridad, DiffServ, modified strict queuing
Soporte VLAN	Puenteo, etiquetado, modo enrutado
NAT	Estático, dinámico, 1:1, IPSec NAT traversal, NAT basado en políticas, IP virtual
Otras Opciones de Red	Independencia del puerto, conmutación por error de WAN, balanceo de carga, transparente/modo directo
<b>Administración</b>	
Plataforma de Administración	WatchGuard System Manager (WSM) v.11.5.2 o superior
Alarmas y Notificaciones	SNMP v2/v3, Correo Electrónico, Alerta del Sistema de Administración
Soporte de Servidor	Generación de Registros, Informes, Cuarentena, WebBlocker, Administración
Web UI	Compatible con sistemas operativos Windows, Mac, Linux con los navegadores más comunes
CLI	Incluye conexión directa y mediante scripts

<b>Certificaciones</b>	
Red	IPv6 Ready Gold (enrutamiento)

### CON EL PODER DE FIREWARE® XTM

Las Ediciones para Oficinas Grandes y Centros de Datos de XTMv vienen con la versión Pro del sistema operativo Fireware XTM, con las características de Networking de avanzada que requieren las redes exigentes. La versión Pro está disponible como compra de actualización para las Ediciones para Oficinas Pequeñas y Medianas.

CARACTERÍSTICAS DE RED	FIREWARE XTM	FIREWARE XTM PRO
Enrutamiento	Estático, enrutamiento dinámico (RIP)	Dinámico (BGP4, OSPF, RIP v1/2), Basado en Políticas
NAT	Estático, dinámico, 1:1, IPSec traversal, basado en políticas	IP Virtual para balanceo de carga hacia servidores
SSL	10 túneles SSL disponibles	Cantidad máxima de túneles SSL disponibles por edición
Otras Características	Independencia de puertos, modo transparente/drop-in, failover de WAN múltiple	Balanceo de carga hacia servidores, balanceo de carga WAN múltiple

### GUÍA Y SOPORTE DE EXPERTOS

Se incluye una suscripción inicial al Servicio LiveSecurity® con cada solución XTMv. LiveSecurity proporciona soporte técnico de respuesta rápida, actualizaciones de software para que el código siempre esté actualizado y alertas de amenazas concisas.

### LA SEGURIDAD VIRTUAL VIENE EN PAQUETES

Proteja exhaustivamente su infraestructura virtual con el XTM Security Bundle. El paquete incluye la edición de XTMv que prefiera, además de Application Control, Intrusion Prevention Service, Gateway AV, WebBlocker, Reputation Enabled Defense y spamBlocker, como así también LiveSecurity\* con soporte y mantenimiento. Obtendrá un excelente valor al comprar todo junto y ahorrar.

\*XTMv Security Bundles para Ediciones para Oficina Pequeña/Mediana incluyen LiveSecurity estándar con soporte técnico 12 horas de lunes a viernes. XTMv Security Bundles para Oficinas Grandes y Centros de Datos incluyen LiveSecurity Plus con soporte técnico las 24 horas del día, los siete días de la semana.

†Las tasas de velocidad varían según el ambiente y la configuración, incluyendo la infraestructura de virtualización. Comuníquese con un distribuidor WatchGuard o llame directamente a WatchGuard para obtener ayuda para determinar el modelo adecuado para su red.

**VENTAS EN LOS EE. UU.** +(1) 800.734.9905

**VENTAS INTERNACIONALES** +(1) 206.613.0895

[www.watchguard.com](http://www.watchguard.com)