Datasheet

WatchGuard® XTMv

Virtualizing Security for Today's Business Needs

Run virtual appliances on your virtual infrastructure

- Leading UTM/NGFW features and services in virtual infrastructure
- Easy to download, enable, deploy, and manage (WSM, web, CLI)
- Leverages vSphere flexibility and availability
- Multiple models for organizations of all sizes
- Campuses, cloud/hosting, branch consolidation
- Per-customer, -department, or -app deployment

Organizations of all sizes are turning to virtualization to reduce costs and increase the efficiency, availability, and flexibility of their IT resources. But virtualization comes at a cost. Virtual environments are complex to manage and vulnerable to security threats. IT must be prepared. Now applications can be secured, resources can be maximized and your IT department can reap the rewards of having a single, unified management system—without a security risk in sight. WatchGuard XTMv brings best-in-class network security to the world of virtualization. With real-time monitoring, multi-WAN support and scalable solutions to fit any sized business, your virtual environments can be just as secure as your physical one.

WatchGuard's virtual solutions provide you with unmatched deployment flexibility. You can choose to deploy a mix of hardware and virtual appliances, operating together and managed from a common centralized management platform. WatchGuard virtual appliances feature all of the security and networking services found in our physical appliances and can be deployed in a per-customer, -department, or -app scenarios, for your virtual infrastructure.

Virtualize the traditional gateway firewall for unprecedented flexibility – *protecting the internal edge*

WatchGuard XTMv protects not only the physical perimeter of the datacenter, but the "virtual edge." Now you can easily implement policy that protects the data in the corporate database from the messaging infrastructure, or confidential HR information from financial data from other divisions – even when running on the same servers.

Consolidate multiple firewalls for high-impact efficiencies – *multi-tenant protection*

Service providers – hosting, cloud, or managed security services – can deploy multiple instances of XTMv on servers at the perimeter of their datacenters. These virtual firewalls are isolated from each other, so service level agreements (SLAs) can be guaranteed to each tenant, and a configuration change to one doesn't affect the others. And yet they can all be managed by the provider using a single intuitive console.

Eliminate redundant hardware costs while securing the virtual networks – *branch consolidation*

As larger branches and divisions consolidate local servers – file, print, voice, and more – onto one box, a virtual firewall can be deployed on the physical server, insulating all traffic from the public Internet. A single VPN tunnel can provide a secure path back to corporate datacenters or virtual private clouds – yielding cost savings at every location without compromising security.

WatchGuard XTMv Editions

	Small Office	Medium Office	Large Office	Datacenter
Throughput and Connections				
Firewall throughput†	1 Gbps	2.5 Gbps	5 Gbps	Unrestricted
Virtual interfaces	10	10	10	10
Nodes supported (LAN IPs)	Unrestricted	Unrestricted	Unrestricted	Unrestricted
Concurrent connections (bi-directional)	30,000	350,000	1,250,000	2,500,000
VLAN support	50	75	400	4,000
VPN Tunnels				
Branch Office VPN	50	600	6,000	10,000
Mobile VPN IPSec	5	50	800	Unrestricted
Mobile VPN SSL (incl/max)	10/50	10/600	6,000/6,000	Unrestricted

Next-Generation Security	
Firewall	Stateful Packet Inspection, Deep Application Inspection, Proxy Firewall
Application Proxies	HTTP, HTTPS, SMTP, FTP, DNS, TCP, POP3
Threat Protection	Blocks spyware, DoS attacks, fragmented & malformed packets, blended threats & more
VoIP	H.323, SIP, Call Setup/Session Security
Security Subscriptions	Application Control, Intrusion Prevention Service, Gateway AntiVirus, Reputation Enabled Defense, spamBlocker, WebBlocker
VPN & Authentication	
Encryption	DES, 3DES, AES 128/192/256-bit
IPSec	SHA-1, MD5, IKE pre-shared key, 3rd party cert
SSL	Thin client, Web
PPTP	Server & Passthrough
VPN Failover	Yes
Single Sign-On	Transparent Active Directory Authentication
XAUTH	RADIUS, LDAP, Secure LDAP, Windows Active Directory
Other User Authentication	VASCO, RSA SecurID, Web-based, Local, Microsoft Terminal Services and Citrix
Platform and Networking	
Operating System	Fireware® XTM / Fireware XTM Pro
Hypervisor Support	VMware vSphere 4.1, 5.0
IP Address Assignment	Static, DHCP (server, client, relay), DynDNS, PPPoE
Routing	Static, dynamic (BGP4, OSPF, RIP v1/v2), Policy-based
QoS	8 priority queues, diffserv, modified strict queuing
VLAN Support	Bridging, tagging, routed mode
NAT	Static, dynamic, 1:1, IPSec NAT traversal, Policy-based NAT, Virtual IP
Other Networking	Port independence, WAN failover, load balancing, transparent/drop-in mode
Management	
Management Platform	WatchGuard System Manager (WSM) v.11.5.2 or higher
Alarms and Notifications	SNMP v2/v3, Email, Management System Alert
Server Support	Logging, Reporting, Quarantine, WebBlocker, Management
Web UI	Supports Windows, Mac, Linux OS with most common browsers
CLI	Includes direct connect and scripting

Certifications	
Network	IPv6 Ready Gold (routing)

POWERED BY FIREWARE® XTM

Large Office and Datacenter Editions of XTMv ship with the Pro version of the Fireware XTM operating system, providing the advanced networking features that demanding networks require. The Pro version is available as a purchase upgrade for Small and Medium Office Editions.

NETWORKING FEATURES	FIREWARE XTM	FIREWARE XTM PRO
Routing	Static, dynamic routing (RIP)	Dynamic (BGP4, OSPF, RIP v1/2), Policy-based
NAT	Static, dynamic, 1:1, IPSec traversal, policy-based	Virtual IP for server load balancing
SSL	10 SSL tunnels available	Maximum number of SSL tunnels available per edition
Other Features	Port Independence, transparent/drop-in mode, multi-WAN failover	Server load balancing, multi-WAN load balancing

EXPERT GUIDANCE AND SUPPORT

An initial subscription to LiveSecurity Service is included with every XTMv solution. LiveSecurity provides rapid-response technical support, software updates so code is always up to date, and concise threat alerts.

VIRTUAL SECURITY COMES BUNDLED

Comprehensively protect your virtual infrastructure with the XTM Security Bundle. The Bundle includes your choice of XTMv edition, plus Application Control, Intrusion Prevention Service, Gateway AV, WebBlocker, Reputation Enabled Defense, and spamBlocker, as well as LiveSecurity* for support and maintenance. An excellent value when you buy together and save!

*XTMv Security Bundles for Small/Medium Office Editions include standard LiveSecurity with 12/5 tech support. XTMv Security Bundles for Large Offices and Datacenters include LiveSecurity Plus with 24/7 tech support.

†Throughput rates will vary based on environment and configuration, including the virtualization infrastructure. Contact your WatchGuard reseller or call WatchGuard directly for help determining the right model for your network.

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 www.watchguard.com