



5. Inspect HTTPS traffic—while safeguarding privacy:

An increasing proportion of Internet traffic runs over encrypted HTTPS channels. Though the “S” on the end of HTTPS stands for “secure,” the encryption of these transactions renders the traffic invisible to traditional firewalls. Full inbound and outbound HTTPS inspection in WatchGuard XTM closes the loophole that other security products leave wide open. URL filtering, AV scanning, and a host of other security functions carried out on HTTPS traffic, identify and stop threats before they can affect your business.. Additionally, the data is not exposed to human eyes, so the risk of an intentional or unintentional privacy violation is eliminated.

6. Make Voice over IP Simple and Safe For Your Business:

Voice over IP (VoIP) is an extremely useful tool in business today for decreasing telecommunication costs and increasing productivity. However, it carries inherent risks, because the VoIP protocols are complex and varied in their implementations. WatchGuard XTM provides application-layer VoIP security, allowing businesses to take advantage of VoIP while minimizing exposure and risk to critical systems and data. With the XTM Series, organizations don’t have to “wire around the firewall” to take advantage of the huge cost savings and communication capabilities VoIP offers.

7. Making the Most of the Network:

As Internet use has increased, so have temptations, distractions, and security risks online. Organizations require more than a simple “allow/deny” security policy. WatchGuard XTM includes a rich set of tools for maximizing the business value of every dollar spent on Internet connectivity. Traffic Shaping and QoS tools allow organizations to define which types of traffic are most important, and which types are less important or prohibited, ensuring that business traffic always wins out over recreational or discretionary traffic. VPN failover, WAN failover, and High Availability features ensure that mission-critical data keeps flowing, even in the event of failure or degradation of equipment or connectivity.

8. Best-In-Class Security:

Attackers and malware constantly advance, making use of an extensive worldwide underground market for crimeware.

To defend against these threats, WatchGuard XTM also works globally, combining advanced capabilities from the world’s best suppliers of security technology to complement WatchGuard’s award-winning foundation. This “all-star lineup” outpaces firewalls from other vendors who rely only on in-house technology rather than acknowledged best-in-class capabilities for specialized functions. At the same time, the deep integration of these functions and an intuitive user interface streamline the creation and monitoring of the holistic security policy, giving customers best-in-class security while eliminating the complexity and cost of managing disparate point solutions.

9. Connect Your People Securely:

Virtual Private Networking (VPN) is ultimately about securely connecting people to the resources they need. Businesses today have distributed workforces and need to provide privacy over public lines. By deploying VPNs businesses can deliver secure, encrypted connectivity for traveling employees, remote offices and telecommuters that require access to critical corporate network resources. WatchGuard XTM provides a multitude of ways to easily and securely create and manage these connections. The unique “drag and drop VPN” enables an organization to connect offices almost instantly, without error, even when dynamic IP addresses are in use. Mobile VPN enables road warriors, virtual employees, collaborators, and any other authorized person to connect to corporate resources from anywhere, at any time, from a variety of devices including laptops, smartphones, and the popular Apple® iOS devices. You can rest assured that with VPN support your critical corporate network resources are protected.

10. User Friendly:

WatchGuard recognizes that many small businesses do not have a dedicated IT security staff. With this recognition comes a dedication to creating interfaces that take the hard work and guess work out of business security. Task flows are designed for maximum efficiency, and interfaces use plain language that enables even security novices to create, monitor, and audit strong security and acceptable use policies.



The WatchGuard® XTM Story

Since 1996, WatchGuard Technologies has provided over one-half million network security appliances to hundreds of thousands of customers worldwide. While the technologies, performance, and individual features of those products have evolved and grown tremendously over that time, the underlying WatchGuard philosophy has remained the same: to deliver strong security that is easy to manage and monitor, at an excellent price. WatchGuard’s XTM family of all-in-one solutions delivers enterprise-grade network protection for small to midsize businesses, keeping your network secure, employee productivity high, and turning the Internet from a security risk to a business empowerment tool.



1. Complete Security Capabilities Now & into the Future:

WatchGuard XTM enables organizations to define, enforce, and audit a strong security and acceptable use policy, with a range of capabilities unmatched in its class, and could be deemed an “IT-Security-Department-In-A-Box”. With WatchGuard XTM, organizations can:

- **Defend Resources** with powerful firewall, anti-malware, and intrusion prevention.
- **Connect Offices Securely** together and allow road warriors and virtual employees to access corporate resources from anywhere, anytime, with nearly any device.
- **Enforce Acceptable Use** with Application Control, WebBlocker, spamBlocker, and Reputation Enabled Defense, tools that safeguard employee usage of the Internet while providing administrators deep visibility into usage patterns.

2. Stay Secure on a Tight Budget:

XTM appliances deliver among the best price-performance in the industry, ensuring that, regardless of your organization’s size, you can get rock-solid security as well as performance that allows your business to proceed unimpeded. What’s more, with XTM’s unique model upgradability, you can choose the appliance that fits your needs today, with the ability to upgrade to a higher model within the series via a simple license key. An assortment of upgrade packages makes it easy to custom-tailor the solution to the organization’s exact needs.

3. Know What is Happening On Your Company’s Network:

“Visibility IS security” – and great visibility is one of the most important ways to ensure compliance with policies. The XTM Series and WatchGuard System Manager (WSM) enable a business to gain deep real-time and historical insights into the network and user events and activities. Interactive real-time monitoring features help pinpoint significant activities as they happen, and let the administrator take immediate corrective or diagnostic actions directly from the monitoring interface. WSM’s centralized logging features unique TCP-based, encrypted log channels for maximum reliability and security, while Report Manager includes over 60 predefined reports, with an intuitive user interface that uses plain language, easy to read graphics, and drill-down and pivot controls.

4. Centrally Manage Your Organization’s Security:

Distributed organizations and Managed Security Services Providers (MSSPs) need the ability to manage large numbers of appliances from a single location, with simplicity and scalability. WatchGuard System Manager, bundled with every XTM appliance, is rich in tools that support policy creation, management and enforcement across multiple locations. Role-Based Access Control supports the delegation of duties according to function within the organization, and every function can be centrally managed—including firewall, VPN, intrusion prevention, URL filtering, web security, anti-virus and anti-spam services, appliance software updates and more. And, beyond the centralized management capabilities in WSM, WatchGuard XTM solutions may be managed via a Web UI or a Command Line Interface (CLI), for ultimate sflexibility.



WatchGuard® XTM Products at a glance

| | XTM 2 Series* | | | XTM 3 | XTM 5 Series | | | | XTM 8 Series | | | XTM 10 | XTM 20 |
|---|--|---------------|---------------|--|------------------|------------------|------------------|------------------|------------------|------------------|------------------|--|-----------------------|
| | XTM 21 | XTM 22 | XTM 23 | XTM 330 | XTM 505 | XTM 510 | XTM 520 | XTM 530 | XTM 810 | XTM 820 | XTM 830 | XTM 1050 | XTM 2050 |
| Throughput and Connections | | | | | | | | | | | | | |
| Firewall throughput** | 110 Mbps | 150 Mbps | 195 Mbps | 850 Mbps | 850 Mbps | 1.4 Gbps | 1.9 Gbps | 2.3 Gbps | 3 Gbps | 4 Gbps | 5 Gbps | 10 Gbps | 20 Gbps |
| VPN throughput** | 35 Mbps | 55 Mbps | 55 Mbps | 150 Mbps | 210 Mbps | 350 Mbps | 550 Mbps | 750 Mbps | 1 Gbps | 1.4 Gbps | 1.6 Gbps | 1.6 Gbps | 1.6 Gbps |
| XTM aggregate throughput** | 18 Mbps | 30 Mbps | 40 Mbps | 70 Mbps | 275 Mbps | 400 Mbps | 600 Mbps | 800 Mbps | 1 Gbps | 1.3 Gbps | 1.6 Gbps | 2 Gbps | up to 10 Gbps |
| Interfaces 10/100 | 3 | 3 | 3 | 0 | 1 | 1 | 1 | 1 | - | - | - | - | - |
| Interfaces 10/100/1000 | 3 | 3 | 3 | 7 | 6 | 6 | 6 | 6 | 10 | 10 | 10† | 12 (optional four 1G SFP+ or one 10G SFP+) | 16 (and two 10G SFP+) |
| I/O Interfaces | 2 USB | 2 USB | 2 USB | 1 Serial / 2 USB | 1 Serial / 2 USB | 1 Serial / 2 USB | 1 Serial / 2 USB | 1 Serial / 2 USB | 1 Serial / 2 USB | 1 Serial / 2 USB | 1 Serial / 2 USB | 1 Serial / 2 USB | 1 Serial / 2 USB |
| Nodes supported (LAN IPs) | Unrestricted | Unrestricted | Unrestricted | Unrestricted | Unrestricted | Unrestricted | Unrestricted | Unrestricted | Unrestricted | Unrestricted | Unrestricted | Unrestricted | Unrestricted |
| Concurrent connections (bi-directional) | 10,000 | 20,000 | 30,000 | 40,000 | 40,000 | 50,000 | 100,000 | 350,000 | 500,000 | 750,000 | 1,000,000 | 2,500,000 | 2,500,000 |
| VLAN support (incl/max) | 20/50*** | 20/50*** | 50 | 75 | 75 | 75 | 75 | 75 | 200 | 300 | 400 | 500 | 500 |
| Local user database limit | 100 | 200 | 200 | 500 | 500 | 500 | 1,000 | 2,500 | 4,000 | 5,000 | 6,000 | 10,000 | 10,000 |
| VPN Tunnels | | | | | | | | | | | | | |
| Branch Office VPN | 5 | 20 | 50 | 50 | 65 | 75 | 200 | 600 | 1,000 | 2,000 | 6,000 | 7,000 | 10,000 |
| Mobile VPN IPsec (incl/max) | 1/11 | 5/25 | 5/55 | 5/55 | 5/75 | 25/100 | 50/300 | 400/1,000 | 600/2,000 | 700/6,000 | 800/8,000 | 15,000/15,000 | 20,000 |
| Mobile VPN SSL (incl/max) | 1/11*** | 1/25*** | 55/55 | 55 | 1/65*** | 1/75*** | 1/300*** | 1/600*** | 1,000/1,000 | 4,000/4,000 | 6,000/6,000 | 15,000/15,000 | 20,000 |
| Wireless Security | | | | | | | | | | | | | |
| Wireless LAN* | 802.11a/b/g/n | 802.11a/b/g/n | 802.11a/b/g/n | - | - | - | - | - | - | - | - | - | - |
| Wireless WAN | Available with purchase and deployment of WatchGuard® 3G Extend wireless bridge accessory / Supports over 50 cellular modem cards and ISP plan options / USB model includes CE certification | | | - | - | - | - | - | - | - | - | - | - |
| Advanced OS | | | | | | | | | | | | | |
| Fireware® XTM Pro | Optional | Optional | Included | Included | Optional | Optional | Optional | Optional | Included | Included | Included | Included | Included |
| Networking Features | | | | | | | | | | | | | |
| Standard | NAT: static, dynamic, 1:1, IPsec traversal, policy-based PAT / Traffic shaping and QoS: 8 priority queues, DiffServ, modified strict queuing / IP address assignment: static, DynDNS, PPPoE, DHCP (server, client, relay) / Port independence / VLAN support / VPN failover / WAN failover†† / Multi-WAN failover†† / Transparent/drop-in mode | | | | | | | | | | | | |
| Advanced OS | Dynamic routing (BGP, OSPF, RIPv1,v2) / Policy-based routing / Multi-WAN failover / Multi-WAN load balancing | | | High availability (active/passive, and active/active for clustering)^ / Dynamic routing (BGP, OSPF, RIPv1,v2) / Policy-based routing / Multi-WAN load sharing / Multi-WAN load balancing / Virtual IP for server load balancing^ | | | | | | | | | |
| Support and Maintenance | | | | | | | | | | | | | |
| LiveSecurity® Service | XTM 2 Series has initial 90-day, 1-year, or 3-year LiveSecurity subscriptions available | | | XTM 3, 5, 8, 10, and 20 Series appliances have initial 1-year or 3-year LiveSecurity subscriptions / LiveSecurity Plus, Gold, and Platinum level service are available as a purchase upgrade | | | | | | | | | |

No matter which XTM appliance you choose, you'll enjoy:

Security Features

- Stateful packet firewall, deep application inspection, application proxies: HTTP, HTTPS, SMTP, FTP, DNS, TCP, POP3
- Blocks spyware, DoS attacks, fragmented packets, malformed packets, blended threats and more
- Protocol anomaly detection, behavior analysis, pattern matching
- Static and dynamic blocked sources list
- Time-based rules
- Instant messaging, P2P, and Skype allow/deny
- VoIP: H.323 and SIP, call setup and session security

Security Subscriptions

- Available in 1-year or 3-year subscriptions
- Application Control
 - Intrusion Prevention Service
 - WebBlocker
 - Gateway AntiVirus
 - spamBlocker
 - Reputation Enabled Defense
- Buy an XTM Bundle and get all subscriptions plus appliance and support and maintenance contract at a great price.

Management Software

- All WatchGuard XTM appliances can be managed with the IT administrator's choice of:
- Command line interface with direct connects and scripting
 - Web UI for single device management from anywhere
 - WatchGuard System Manager (WSM) – an intuitive, centralized console that provides interactive real-time monitoring and logging for network-wide system status at a glance. Includes drag-and-drop VPN creation and rich historical reporting

User Authentication

- Transparent Active Directory Authentication (single sign-on)
- XAUTH for Radius, LDAP, Secure LDAP, Windows Active Directory
- RSA SecurID® and VASCO
- Web-based, local
- 802.1X for XTM 2 Series wireless
- Microsoft Terminal Services and Citrix

Logging and Reporting

- Multi-appliance log aggregation
- HTML and PDF reports
- SQL log database
- Encrypted, TCP-based log channel
- SNMP v2 & v3
- Syslog
- Logging and reporting with server health status
- Web-based configurable reports portal

*All XTM 2 Series appliances are available in a wireless version, under model numbers XTM 21-W, 22-W, and 23-W. **Throughput rates will vary depending on environment and configuration. Contact your WatchGuard reseller or call WatchGuard directly (1.800.734.9905) for help determining the right model for your network. ***Maximum number available with upgrade to Fireware XTM Pro advanced OS. †XTM 830 appliances come with 6 copper and 4 fiber 10/100/1000 interfaces under model number WatchGuard XTM 830-F. ††Requires Fireware Pro upgrade on XTM 21, 21-W, 22, and 22-W appliances. ^High availability and server load balancing are not currently available on the XTM 330.