Wi-Fi Is Easy. Security Is the Challenge.

Wi-Fi doesn't give you a competitive advantage, it offers you a chance to compete. With benefits ranging from increased productivity to improved customer satisfaction, implementing a wireless network for your employees and guests has become the table stakes of doing business. But Wi-Fi also opens your business to significant risks, including malware attacks, rogue hotspots, Wi-Fi password cracking, and eavesdropping.

WATCHGUARD WIRELESS ACCESS POINTS

WatchGuard's Wireless Access Points extend best-in-class UTM (unified threat management) security – including application control, intrusion prevention, URL and web content filtering, virus and spam blocking and more – from your WatchGuard Firebox to the WLAN.

No matter what your wireless battleground is – remote offices, guest Wi-Fi, corporate access, public hotspots – WatchGuard AP devices allow your business to harness the power of mobile devices and wireless networking, both indoors and outdoors, without putting network assets at risk. A secure wireless network can be a game-changer for your business. Find out more about our wireless solutions at **www.watchguard.com/wireless**.

> "Being able to supply secure, reliable, high capacity Wi-Fi to guests, visitors and meeting rooms at speeds far greater than 54 Mbps has been transformative."
>
> – WatchGuard customer Fahyaz Khan, IT Manager, Kensington Close Hotel

About WatchGuard

WatchGuard has deployed nearly a million integrated, multi-function threat management appliances worldwide. Our signature red boxes are architected to be the industry's smartest, fastest, and meanest security devices with every scanning engine running at full throttle. Headquartered in Seattle, WA, WatchGuard has offices throughout North America, Europe, Asia Pacific, and Latin America. Visit www.watchguard.com to learn more.

Why Buy WatchGuard® Network Security Solutions

Network threats can come from anywhere, at any time, and can take you down before you even know they're there. Uniquely architected to be the industry's smartest, fastest and most effective network security products, WatchGuard solutions put IT security pros back in charge of their networks with widely deployable, enterprise-grade security and threat visibility tools suitable for any organization, regardless of budget, size, or complexity.

ENTERPRISE-GRADE SECURITY
At WatchGuard, we believe that every organization, large or small, should have access to the most effective security technologies on the market. Our unique product architecture enables customers to leverage best-in-class security services from the industry's most respected brands, minus the cost and complexity of multiple single-point solutions.

SIMPLICITY
Simplicity is the key to successful adoption of technology. As such, all of our products are not only easy to initially configure and deploy, they are also designed with an emphasis on centralized management, making ongoing policy and network management simple and straightforward. Security is complex, running it doesn't have to be.

PERFORMANCE
Organizations must take a layered approach to security when it comes to protecting their networks. Other manufacturers might offer faster throughput for one single security technology, but we engineered WatchGuard's platform to deliver the fastest throughput when it matters – with all security scanning engines turned on.

VISIBILITY
When it comes to network security, seeing is knowing, and knowing leads to action. WatchGuard's award-winning Dimension™ threat visibility tool enables busy IT managers to instantly identify and take action to resolve potential network security threats.

FUTURE-PROOF
WatchGuard's unique product architecture makes it quick and easy for our team to add new, innovative network security services to our UTM offerings faster than the competition. That same architecture makes it just as easy for us to upgrade or change our existing services as technologies evolve and best practices change – something that would be a massive and time-consuming development project for any of our competitors.

	Firebox T10/T10-W/T10-D[a]	Firebox T30/T30-W	Firebox T50/T50-W	Firebox M200	Firebox M300	Firebox M400	Firebox M440	Firebox M500	Firebox M4600 base + 4 x 10 Gb ports	Firebox M5600 base + 4 x 10 Gb ports
Throughput and Connections										
Firewall throughput	400 Mbps	620 Mbps	1.2 Gbps	3.2 Gbps	4.0 Gbps	8 Gbps	6.7 Gbps	8 Gbps	40 Gbps	60 Gbps
VPN throughput	100 Mbps	150 Mbps	270 Mbps	1.2 Gbps	2.0 Gbps	4.4 Gbps	3.2 Gbps	5.3 Gbps	10 Gbps	10 Gbps
AV throughput	120 Mbps	180 Mbps	235 Mbps	620 Mbps	1.2 Gbps	2.5 Gbps	2.2 Gbps	3.2 Gbps	9 Gbps	12 Gbps
IPS throughput	160 Mbps	240 Mbps	410 Mbps	1.4 Gbps	2.5 Gbps	4 Gbps	2.2 Gbps	5.5 Gbps	13 Gbps	18 Gbps
UTM throughput	90 Mbps	135 Mbps	165 Mbps	515 Mbps	800 Mbps	1.4 Gbps	1.6 Gbps	1.7 Gbps	8 Gbps	11 Gbps
Interfaces	3 x 1Gb	5[b] x 1 Gb	7[b] x 1 Gb	8 x 1 Gb	8 x 1 Gb	8 (incl. 2 SFP)[c]	25 1G copper[b] 2 10G SFP+	8 (incl. 2 SFP)[c]	8 x 1 Gb additional ports available*	8 x 1 Gb + 4 x 10 Gb fiber additional ports available*
I/O Interfaces	1 Serial / 1 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
Concurrent connections	50,000	200,000	300,000	1,700,000	3,300,000	3,800,000	4,000,000	9,200,000	7,500,000	12,700,000
New connections per second	2,300	3,400	4,600	20,000	48,000	84,000	62,000	95,000	160,000	240,000
VLAN support	10	50	75	100	200	300	400	500	1,000	Unrestricted
Authenticated users limit	200	500	500	500	500	Unrestricted	Unrestricted	Unrestricted	Unrestricted	Unrestricted
VPN Tunnels										
Branch Office VPN	5	40	50	50	75	100	300	500	5,000	Unrestricted
Mobile VPN IPSec	5	25	50	75	100	150	300	500	10,000	Unrestricted
Mobile VPN SSL / L2TP	5	25	50	75	100	150	300	500	10,000	Unrestricted
Wireless										
Wireless Access Points (APs)	All models include a Wi-Fi controller to centrally manage WatchGuard Access Points and extend UTM and NGFW security capabilities to the WLAN									
Max APs advised per model	2	10	20	30	40	50	50	75	100	150
Integrated Wireless	Integrated 802.11a/b/g/n available for Firebox T10-W. Integrated 802.11a/b/g/n/ac is available for Firebox T30-W and T50-W.									
Operating System Features										
General	Integrated 802.11a/b/g/n available for Firebox T10-W. Integrated 802.11a/b/g/n/ac is available for Firebox T30-W and T50-W.									
Advanced Networking[d]	Dynamic routing (BGP, OSPF, RIPv1,2) / Policy-based routing / NAT: static, dynamic, 1:1, IPSec traversal, policy-based PAT / Traffic shaping & QoS: 8 priority queues, DiffServ, modified strict queuing / Virtual IP for server load balancing									
Availability[d]	High availability – active/passive, and active/active for clustering (not available on wireless models) / VPN failover / Multi-WAN failover / Multi-WAN load balancing / Link aggregation (802.3ad dynamic, static, active/backup) as indoors									
Security Services										
NGFW Bundle	Application Control / Intrusion Prevention Service / 24 x 7 Support — Available for Firebox models M400 and higher									
UTM Bundle	Application Control / Intrusion Prevention Service / Gateway AntiVirus / WebBlocker / spamBlocker / Reputation Enabled Defense / Network Discovery / 24 x 7 Support									
Other Security Services	APT Blocker, Data Loss Prevention, Mobile Security — Available for all Firebox models									
Management Upgrades	Dimension Command is a suite of management tools for WatchGuard Dimension that allows administrators to manage policies directly from Dimension's visibility dashboards. Contact your WatchGuard reseller to see a demo and get details on an introductory one-year subscription promotion.									

*Firebox M4600 and M5600 throughput rates are determined using base configuration + 4 x 10 Gb ports. Both models ship with two empty bays that can accommodate any combination of the following: 4 x 10 Gb fiber, 8 x 1 Gb fiber, 8 x 1 Gb copper.

Throughput rates are determined using multiple flows through multiple ports and will vary depending on environment and configuration. Max firewall throughput tested using 1518 byte UDP packets based on RFC 2544 methodology. Contact your WatchGuard reseller or call WatchGuard directly (1.800.734.9905) for help determining the right model for your network. Visit **www.watchguard.com/sizingtool** for online assistance.

Every WatchGuard appliance includes these features:

Security Capabilities
- Stateful packet firewall, deep application inspection, application proxies: HTTP, HTTPS, SMTP, TCP-UDP, FTP, DNS
- 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
- VoIP: H.323 and SIP, call setup and session security

Logging & Reporting with WatchGuard Dimension™
- Real-time multi-appliance log aggregation and reporting
- Public & private cloud-ready
- Visibility at a glance with intuitive and interactive visualizations
- Spot trends, outliers and insights about network traffic and usage
- Over 100 reports including reports for PCI and HIPAA compliance
- Option to deliver reports (PDF, CSV) via email
- Anonymization to comply with privacy directives

Management Software
WatchGuard appliances can be managed with any of the following:
- Dimension Command for interactive real-time management of multiple appliances via web browser
- Web UI for managing single appliance via web browser
- WatchGuard System Manager for intuitive management of appliances via Windows client
- Command line interface (CLI) for direct access via scripting
- Simplified configuration and deployment with RapidDeploy

User Authentication
- Transparent Active Directory Authentication (single sign-on)
- RADIUS, LDAP, Secure LDAP, Windows Active Directory
- RSA SecurID® and VASCO
- Local database
- 802.1X for wireless appliances (Firebox T10-W, T30-W, T50-W)
- Microsoft® Terminal Services and Citrix XenApp environments supported

Support and Maintenance
- 24x7 Support and Gold Support are available as purchase options for Firebox models M200 and higher
- 24x7 Support is included in all NGFW Suites, and in UTM Suites for models M200 and higher
- Remote Installation Services for comprehensive assistance with initial setup, configuration, VPN installation
- Premium 4-Hour Hardware Replacement to ensure maximum uptime (not available in all regions)

[a]Not available in all geographic locations. Contact your WatchGuard reseller for more information. [b]Power Over Ethernet (PoE) options: Firebox T30 & T50 have 1 PoE port. Firebox M440 has PoE on 8 of 25 IG ports. [c]Comes with 6 built-in 10/100/1000 copper ports, two SFP transceiver slots. Optional 1Gb fiber or 1Gb copper transceivers can be used in either slot. [d]Some advanced networking features, including server load balancing, high availability, and dynamic routing are not available on Firebox T10 appliances. Visit www.watchguard.com/T10 for details.