Next-Generation Firewall

For The Enterprise

Businesses today need more than a traditional firewall to protect their assets. As business collaboration increases and employees increasingly use the multitude of tools available to them – many of which were never designed for business use – enterprise data security and compliance requirements become a challenge. People work in a way that's faster, easier, and more intuitive – whether they're on the road, in the office, at an airport, or at home. And applications that weren't designed for business can – and do – bypass traditional firewalls and enter a network, regardless of how carefully the IT staff may have tried to lock down the environment. This means it is essential that businesses implement security tools designed with today's environments in mind.

It is not good enough anymore to believe a traditional firewall will stand against the attacks and accidents that threaten to compromise business systems. Enterprises today need to defend corporate resources, prevent data theft, securely connect users, enforce acceptable use, and prevent network attacks, all while having visibility into what is happening. What does it take to stay on top of security? A next-generation firewall (NGFW) that "understands" real-world corporate network traffic in order to reliably secure it against hackers, malware, network attacks, intrusion attempts, data theft, and other cybercrime, while securely connecting offices, remote and virtual employees, and providing real-time and historical visibility into network, security, and user events.

WatchGuard's NGFW products provide true line-speed security inspection on all traffic and support multi-gigabit packet filtering throughput. In addition, the NGFW line provides application control; connects offices via unique Drag and Drop VPN; connects people via SSL and IPSec VPN; and gives the enterprise unparalleled visibility into real-time and historical user, network, and security activities. With WatchGuard's NGFW, businesses can define, enforce, and audit strong security and acceptable use policies, resulting in increased employee productivity and less risk to critical intellectual property or customer data.

What is a next-generation firewall?

Key Next-Generation Firewall Characteristics:

- High-performance security inspection that blocks attacks and unwanted traffic without hindering mission-critical Internet usage
- A platform for network traffic inspection and network security policy enforcement, with the following minimum features:
  - Standard Firewall Capabilities:
    - Packet Filtering
    - Network Address Translation (NAT)
    - Stateful Protocol Inspection
    - Virtual Private Networking (VPN)
  - Integrated Network Intrusion Prevention (IPS)
  - Application Awareness and Control
  - Additional Intelligence: Directory integration to tie security policies to users and groups; cloud-based reputation services to stop traffic from dangerous sources
  - Real-time and historical visibility into user, network, and security activity

Benefits of WatchGuard Application Control:

Granular control – Due to the varied ways that people can use applications, it's critical to control one or more aspects of an application while being able to disallow other aspects of it. Examples of this are allowing the use of Windows Live Messenger for instant messaging but not for file transfer, or allowing access to Facebook but not to Facebook games.

Breadth of application signatures – Extensive list of supported applications that are updated and maintained. WatchGuard application signatures are automatically updated without requiring an upgrade of the entire NGFW appliance as new applications are released and application behaviors change.

Ability to identify encrypted applications – WatchGuard Application Control's unique behavior analysis functionality can discover even well disguised applications that attempt to bypass security measures by encrypting application data and traffic as it traverses the Internet.

Fine-Grained Application Control

The web is the primary source of security threats to organizations today, and web applications are often the main entry point for attackers. Hackers find it convenient to use social networks as a launch pad for social engineering attacks against employees in an organization. Given that web traffic and web applications are the source of so many security risks, IT administrators can cut down the potential threat vectors by limiting their users to only those applications and application sub-functions that are necessary for business purposes.

WatchGuard's Application Control capabilities empower administrators to exercise fine-grained control over hundreds of applications, and understand which applications are being used and by whom. Administrators can enforce acceptable use policies for users and groups by category, application, and application sub-functions. For example, they can define a policy that allows the marketing department to access Facebook, but not Facebook games.

Intrusion Prevention Service – Increase Network Reliability and Performance

Malicious activity can run amok on corporate networks if both network traffic and/or systems activities are not monitored. WatchGuard's Intrusion Prevention Service (IPS) works in tandem with other layers of security inspection in the Fireware XTM OS to provide real-time protection against network threats, including spyware, SQL injections, cross-site scripting, and buffer overflows. IPS scans traffic on all protocols, using continually updated signatures to detect and block all types of threats.

Benefits:

Never leave your network exposed

- Signatures are updated without interruption as new threats emerge.

Flexibility to define action

- Identify malware and allow, block or logs questionable traffic based on type, user/group, protocol and severity.

Highly effective scanning

- Scan all protocols, including HTTP, HTTPS, FTP, TCP, UDP, DNS, SMTP and POP3 to block network, applications and protocol-based attacks.

Support Programs

Enterprises not only need an NGFW, but a strong support program that has their back. WatchGuard provides LiveSecurity® Plus with every NGFW Bundle. Customers can upgrade to LiveSecurity Gold or LiveSecurity Platinum for extended protection. WatchGuard recommends LiveSecurity Platinum for its enterprise customers.

	Environment	24 x 7 Web and Telephone Support	1 Hour Response Time	Unlimited Annual Support	Designated Technical Account Manager (TAM*)
LiveSecurity Plus	Any	✓			
LiveSecurity Gold	Any	✓	✓	✓	
LiveSecurity Platinum	Large, Mission-Critical Environments	✓	✓	✓	✓

*Schedules Quarterly Account Reviews to review the ongoing status of your WatchGuard solution. Topics include: Summary of incidents logged and resolution status; review of any open incidents; architecture reviews; updates on new firmware releases.

Advance Hardware Replacement Program

Businesses today cannot afford to have downtime as a result of network equipment failures. Replacements are needed without delay when parts fail, even if they are redundant backups. That is why WatchGuard offers an Advance Hardware Replacement program.

WatchGuard will ship a replacement via pre-paid, next-day air freight in advance of receiving the returned appliance. For customers with mission-critical requirements, and extremely time-critical applications, WatchGuard also offers a premium 4-Hour Advance Hardware Replacement (RMA) program.*

* Customer is required to ship defective part back to WatchGuard HQ.

Premium 4-Hour Hardware Replacement*

WatchGuard provides 24x7 4-hour hardware replacement as an optional upgrade. Within 4 hours of approval by WatchGuard support, replacement appliances are delivered on-site.

* Not available in all geographic locations. Please contact your WatchGuard reseller or WatchGuard sales to determine availability in your region.

ADDRESS 505 Fifth Avenue South, Suite 500, Seattle, WA 98104 WEB www.watchguard.com U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895