

Document Presented By Wick Hill and DNA IT



River Court,
Albert Drive,
Woking, Surrey
GU21 5RP
01483 227600
info@wickhill.co.uk
www.wickhill.com/watchguard



Unit J 2,
Maynooth Business Campus,
Maynooth,
Co.Kildare
+353 1 651 0300
sales@dnait.ie
www.dnait.ie



Practical Advantages of Fireware® XTM for Hands-On IT Administrators

July 2009

Introduction: True or False?

“Firewalls are commodities, with no substantial difference among various models.”

The IT world accepts this statement as conventional wisdom. And, in the most general sense, all firewalls do the same basic task of checking incoming and outgoing data packets against a list of rules that define what traffic to allow and what traffic to block. But some firewalls do it better than others, some are easier to configure than others, and some started with better design assumptions than others.

The idea that “firewalls are really all the same because they do the same thing” doesn’t hold up to real-world experience. Following the same logic, since all automobiles do basically the same task of transporting a driver, you could reason that there is no meaningful difference between a 1988 Geo Prizm and a 2010 Mercedes E-Class sedan. But if you’ve actually driven those automobiles, you know there is a world of difference – in every aspect – from handling to ergonomics to appearance.

This paper is written for IT professionals currently comparing the merits of various network security appliances. If the notion of firewalls being commodities was ever true, it certainly is not now. In this era of unified threat management (UTM) devices, firewalling is just one aspect of a multi-faceted perimeter defense appliance. This paper seeks to focus the comparison on one facet: what is the experience of actually using a WatchGuard® Fireware® XTM appliance?

For the purposes of comparison, set aside abstract issues such as risk management and regulatory compliance. Set aside political implications about what brands your organization favors. Accept as a given that all firewalls provide some rudimentary level of security. For these few pages, let’s narrowly consider the network firewall from the perspective of the hands-on IT pro who actually configures and uses it. Does a WatchGuard Firebox® X or Fireware XTM 1050 appliance stand out from the “commodity crowd” in any way that will make a difference to the administrator?

We know that it does, and in this paper we'll explain some of the ways that WatchGuard security appliances running the Fireware XTM operating system excel over "commodity" security:

- By empowering you to inspect encrypted traffic that today you accept blindly
- By adding security to Voice over Internet Protocol (VoIP) that others don't
- By offering greater visibility into your network through robust reporting and flexible, easy-to-use management tools

Some security appliances reflect such a strong engineering background that you have to be an engineer yourself to comprehend their mystifying user interface. In contrast, WatchGuard was started by pioneering engineers who thought carefully about what IT administrators really need. Read on to see whether you can believe all firewalls are alike – or if, perhaps, security appliances running Fireware XTM might be the Mercedes E-class of network security.

Seeing Through What Was Opaque: HTTPS Inspection

The majority of network administrators allow encrypted web traffic, such as HTTPS, to pass through perimeter defenses. Because encryption scrambles these streams into unreadable text, an administrator cannot readily see whether an HTTPS connection carries desired information or hostile code. This combination of allowed access with a cloak of stealth has made encrypted web traffic a tool that appeals to attackers.

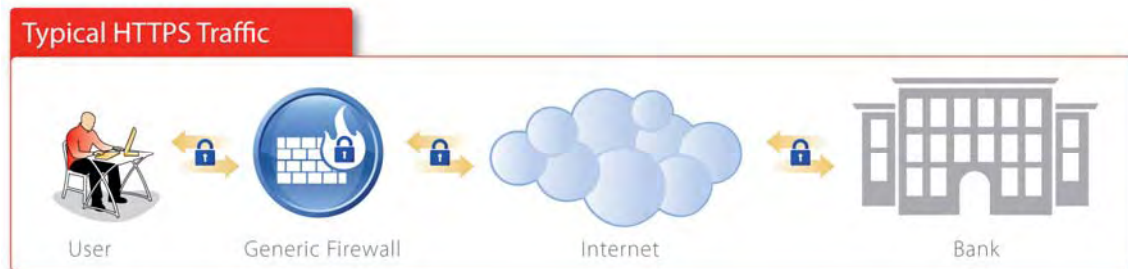


Figure 1: When a user behind a typical firewall requests encrypted data from an HTTPS website, that data – whether it's safe or dangerous – will be returned fully encrypted. Because the typical firewall does not decrypt this traffic, it enters the network regardless of its payload.

Four years ago, most attackers lacked the programming sophistication to manipulate the certificate system underlying HTTPS. Since then, attackers have cleared that technical hurdle. Abuses of HTTPS have grown rapidly, to the point where hardly a week goes by without news reports of a fraud, breach, or criminal campaign that utilizes web encryption.

Some recent examples of how criminals utilize HTTPS include the following:

- In the Anti-Phishing Work Group's report¹ summarizing phishing activity for the second half of 2008, the APWG found that only a small proportion of deceptive phishing sites had been set up from scratch by phishers. Instead, 81% of phishing sites were legitimate sites that the phishers had compromised.

Phishers routinely add an SSL certificate to deceptive sites. According to the APWG, phishers are drifting away from the old technique of putting up an impersonation site, then trying to convince visitors they are dealing with the site of a major brand. More often now, phishers offer something

¹ Found at http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey2H2008.pdf

at apparent extraordinary value (e.g., inexpensive pharmacy products) and lure visitors to phishing sites that appear to be little-known but legitimate businesses. Communicating via HTTPS makes these malicious sites look more like legitimate e-commerce retailers, with concern for the consumer's safety. In this context, then, attackers use HTTPS first as a social engineering trick to build the visitor's confidence. When a gullible user clicks through and provides payment details, the attacker has already harvested useful information. But why stop there? Now the attacker has established a network connection to the visitor, and the HTTPS hides whatever the attacker does next. The attacker can send his drive-by download of a Java exploit to the victim over a secure encrypted connection.

- **The botnet named Ghag** (a word for an Albanian dialect) functions primarily as a spambot. Its template-based engine can generate and send up to 7,000 email messages per hour, per bot. Normally, when a spambot infects your network, you can stop it from spamming by using an egress filter to block port 25 outbound (most clients on your LAN do not need to send traffic to all IP addresses everywhere over port 25 – most of your clients just need to be able to reach your mail server). However, when Ghag infects a client on your network, Ghag sidesteps your egress filtering, by using your mail server to send its spam. Ghag bots use encrypted port 443 (HTTPS) to communicate with their creator's command and control server.
- **Cimbot**, also primarily a spambot, breaks new ground in botnet stealth. The actual spambot stores itself as an encrypted file on your disk drive. Rather than self-executing, as most bot clients do, it only decrypts itself when the botmaster commands it to. Even then, rather than running as a normal Windows process, it runs only in system memory, making it difficult to detect on your computer. Cimbot can receive its commands both over port 80 (HTTP) and encrypted port 443 (HTTPS).

We cite these examples to prove one simple point: as a network administrator, you can no longer trust that HTTPS connections to your network are benign. Today, your network defenses must see what is going on under the cloak of encryption.

How WatchGuard HTTPS Inspection Works

In response to this burgeoning threat, WatchGuard designed the Firewall XTM operating system to inspect HTTPS traffic. Firewall XTM HTTPS inspection works on both incoming and outgoing traffic, and inspects not only packet headers but also payload (body content).

How does Firewall XTM see into this previously opaque threat? To explain how it works, we must consider two scenarios where encrypted web traffic is used:

- **Outbound**, in which a user behind your firewall on your Trusted network segment wants to connect to an arbitrarily-chosen HTTPS website on the Internet
- **Inbound**, in which strangers on the Internet want to connect (and input random data) to an HTTPS server that you operate

Scenario 1: Trusted user, connecting out-bound

XTM HTTPS inspection extends the much-lauded security proxy technology from WatchGuard. Conceptually, the WatchGuard XTM appliance stands in for (that is, *proxies*) both parties trying to establish an encrypted connection. It intercepts, decrypts, and inspects communications in each direction, and responds as appropriate based on security and networking logic. Thus, from the perspective of your user's machine, the WatchGuard XTM appliance seems to be the web server; and from the web server's perspective, the WatchGuard XTM appliance seems to be the requesting client.

How can this work, when encrypted connections would normally be unreadable to a perimeter device? WatchGuard software generates an encryption key certificate that is tightly associated with your specific WatchGuard XTM appliance (based on serial number, user input, and other parameters). The appliance then exports this digital certificate to your clients, who import it into their web browsers. Because you

generated and exported this certificate yourself, you can operate as your own Certificate Authority (CA) – after all, you should have no doubt authenticating your own identity. The exported certificate thus can bear more trust than a normal public SSL certificate. Its “trusted anchor” status allows any of your users to trust the XTM appliance to answer on their behalf when visiting any HTTPS site.

As an additional security measure, the XTM appliance also verifies the remote certificate, which ensures that the remote server really is what it claims to be. Now, suppose one of your users wants to see how much money she has in her checking account. When her browser goes to “bank.com” and she signs into bank.com’s secure server, your XTM appliance stands in the middle, between your user and bank.com. From bank.com’s perspective, your XTM security appliance appears to be the requesting client. Bank.com’s secure web server sends the information that your user asked for. The XTM appliance establishes its own connection to bank.com to decrypt bank.com’s traffic. Then it re-encrypts the traffic using the encryption key from the “trusted anchor” certificate, which your users implicitly trust. So your users browser will decrypt the XTM security appliance’s HTTPS response and inspect it.

The traffic is decrypted inside the firewall only to let the security logic in the HTTP proxy scan the data, perform any needed security functions, and then we re-encrypt the data before it exits the box. During the brief time that the HTTPS has been decrypted inside the firewall, it is normal HTTP. That simple truth contains vast implications. It means that now encrypted channels can enjoy every bit as much security as unencrypted channels. You can configure Fireware XTM to inspect HTTPS at any level of depth you want, balancing security needs with performance desires. You can even pass traffic to the WatchGuard HTTP proxy, enabling you to filter and block on a whole range of characteristics (e.g., based on strict interpretation of a protocol standard; based on character strings; based on regular expressions; based on denying URLs that contain .EXE; and more).

After XTM inspects the HTTPS traffic, it re-encrypts clean traffic and passes the data to its final destination on your network. Unlike inferior inspection technologies, Fireware XTM unleashes full security screening and logic on the HTTPS packet, but does not open it up to prying human eyes. In the example above, your user’s financial data remains confidential between her and her bank; yet you have strong confidence that the HTTPS stream did not contain anything you filter against.



Figure 2: When a user behind a WatchGuard Fireware XTM firewall makes the same request as in Figure 1 to receive encrypted data, the firewall is able to decrypt the HTTPS traffic into normal HTTP. It can then inspect it for anomalies, re-encrypt the data, and pass it along to the user. The user’s communication remains confidential, while the network has an additional layer of protection from encrypted threats.

Scenario 2: External user connecting in-bound

If you run your own encrypted web server, HTTPS inspection provides an indispensable layer of security. If you use your encrypted web server for e-commerce, your web form might simply request an email address or phone number, but attackers on the Internet may submit all manner of hostile code. If you maintain an encrypted server for connections from trusted business partners, be aware that Verizon’s Intrusion

Response Team has documented² that almost one-third (32%) of all breaches enter networks through compromised partners.

In either case, these attacks have particular virulence because the attacker gets to register with your site and establish a connection over a channel filled with expected, legitimate traffic, all before you have the opportunity to apply defenses. These provide more reasons to inspect HTTPS traffic carefully.

As with the “outbound” scenario, in the “inbound” scenario, once again the WatchGuard XTM appliance stands in the middle and proxies on behalf of the connecting parties. In this scenario, though, WatchGuard software does not generate the encryption key certificate used to decrypt the traffic. In this case, your internal web server already has a private SSL certificate. You export the certificate from the web server, and import it into the WatchGuard XTM appliance. Then your XTM device can respond on behalf of your web server, and pass along only traffic that is decrypted, inspected, and found clean.

This simple expedient of turning “un-inspectable” HTTPS into inspectable HTTP pays off in myriad ways. If traffic coming from a business partner utilizes unexpected or unauthorized HTTP methods (perhaps you don’t expect your partner to send OPTIONS, PUT, or DELETE commands) as encrypted traffic, it would have passed into your network. As unencrypted traffic, you can block it automatically. Perhaps your user forum provides a place for customers to post pictures, but an attacker tries to upload an executable binary. Without WatchGuard XTM HTTPS inspection, you could neither anticipate nor stop the attack. With HTTPS inspection, you can spot the illicit traffic and drop it.

HTTPS Inspection: the Bottom Line

WatchGuard’s innovative HTTPS inspection solves a longstanding problem by making opaque encrypted connections totally transparent. Very few security appliances solve this problem today. To our knowledge, as of this writing, even those few vendors who offer HTTPS inspection do not offer the ability to fully inspect the entire HTTPS packet payload the way that WatchGuard Fireware XTM can. One of our competitors decrypts HTTPS, but does not re-encrypt it after inspection. WatchGuard security appliances, designed with you in mind, provide superior security to such commodity offerings.

“Can you pwn me now?” or, VoIP Security

According to the Telecommunications Industry Association, between 2005 and 2006 the number of residential Voice over Internet Protocol (VoIP) users tripled. Between 2006 and 2007, adoption of VoIP doubled in some regions of the US. By 2007, 10 percent of US households had VoIP, with a growth trajectory predicted to exceed 18 million users in 2009.

If that seems like rapid expansion, VoIP adoption outside the US is even faster. When VoIP use had penetrated to 10% of US households, it had reached 40% of households in France. China has more VoIP phones in use than Public Switched Telephone Network (PSTN) phones.

Despite VoIP’s worldwide explosion, most of the security issues surrounding VoIP technology have not been adequately resolved.

Why you need VoIP security today

“Security and complexity are often inversely proportional,” goes the old security axiom.³ In other words, the more complicated a process is, the more it leaves room for mistakes, flaws, and insecurity. That does not bode well for VoIP. That’s because basic operations of VoIP require:

² In the 2009 Data Breach Investigations Report, <http://www.verizonbusiness.com/products/security/risk/databreach/>

- Converting an analog voice to digital signals
- Compressing those digital signals into packets the Internet can carry
- Reassembling the packets at the receiving end as audible voice
- Translating telephone numbers into IP addresses (and vice versa)
- Letting the telephone system know where to find phone users

In short, implementing VoIP introduces your network to numerous codecs,⁴ protocols, and transport methods. If complexity does not promote security, VoIP exposes substantial attack surface for malicious hackers.

“VoIP provides the kind of technical wilderness that attackers love...but Fireware XTM can help.”

VoIP and network security have always had that “inversely proportional” relationship. When administrators first tried to implement Session-Initiation Protocol (SIP) and H.323, firewalls typically broke VoIP connections. That was because these protocols initiate a connection on a known, standard port, but then they want to open other ports dynamically, as needed. It took security vendors a while to create special services that could handle the dynamic ports temporarily and close them cleanly after a session terminated. The result is that many security vendors now claim “VoIP Support!” – not because they secure VoIP in any sophisticated way, but simply because they no longer break VoIP. That is not the same as VoIP security.

In 2007, Cisco made headlines when it published a [Security Response](#) admitting that a bug in their Unified IP Phone’s implementation of Real-Time Transport Protocol (RTP) could allow a remote attacker to eavesdrop on VoIP phone calls. Six months later, the security vendor VoIPShield announced that it could document more than [100 security holes](#) in Cisco, Avaya, and Nortel VoIP products.

Since 2006, attackers have increasingly exploited security flaws in codecs. By injecting malicious code into files that your computer must decompress to use, attackers found they could execute malware on victim computers using file formats previously considered benign (such as QuickTime .MOV and Windows Media Player .WMP and .WAV files).

Given that attackers like to exploit codec flaws, VoIP provides the kind of technical wilderness that attackers love. VoIP incorporates audio, video, fax, and text, and provides numerous codec options in each of those technologies. Take audio alone: some users demand stereo sound and great audio quality, and thus prefer codecs that result in larger packets. Other, more bandwidth-sensitive, users prefer codecs that create smaller packets using a lower average bitrate, but requiring intensive processing. For reasons such as these, VoIP audio has at least [eight codecs](#) in common use.

Thus, to enjoy VoIP functionality, you must accept unregulated IP traffic from strangers, in a format that your computers must execute in order to use, mingled with traditional data packets on your LAN. Clearly, VoIP technology magnifies the risk to any network.

³ For more security axioms from Fred Avolio, who managed the team that invented the first commercial firewall, see <http://www.avolio.com/papers/axioms.html>.

⁴ Codec blends and shortens the terms “compression” and “decompression” or “coder” and “decoder,” depending on which authorities you believe.

From WatchGuard's perspective, as bad as it is that an attacker might be able to eavesdrop on a call or teleconference, there are even worse problems with VoIP. Because VoIP runs mingled with your IP network, its most serious threat is that any hole in VoIP provides a stepping-stone to **all** your network data.

But Fireware XTM can help.

How WatchGuard's VoIP Security Works

Fireware XTM comes standard with Application Layer Gateways that intercept and inspect VoIP-related protocols such as H.323 and Session Initiation Protocol (SIP). These gateway security proxies allow you to reduce your exposure to VoIP-related risk.

If you believe all firewalls are commodities, ask other security vendors if their so-called VoIP security offers the following capabilities, which come standard with WatchGuard XTM appliances.

Secure Call Setup

The H.323 protocol suite supports five audio codecs:

- G.711
- G.722
- G.723.1
- G.728
- G.729

In practice, most administrators don't use all five. In fact, you might only use the two most common codecs, G.711 and G.729. XTM VoIP security enables you to deny all connection requests compressed with codecs you don't use. Denying specific codec connections makes your network invulnerable to all attacks that exploit holes in those codecs – even attacks yet to be invented.

The Application Layer Gateway also empowers you to allow calls from a whitelist. Most likely, your VoIP implementation exists to serve you and business partners, not every possible caller in the world. If "limited audience" describes your environment, you can configure XTM VoIP to deny calls from unauthorized phone numbers or unauthorized IP addresses.

Secure Topology

Some VoIP features and responses display data that specifies what VoIP gear you use, on what versions of software (similar to the way some verbose web page errors divulge what server software hosts the web page). Fireware XTM allows you to hide your network topology with a simple click in a check box. Similarly, SIP and H.323 interchanges can divulge, in the User-Agent header, information useful to hackers. WatchGuard's VoIP security features enable you to put whatever string you want in this header, denying information to attackers, or even (if you so choose) misleading them. If your VoIP responses don't disclose your system or portray it as a different system, opportunistic hackers seeking low-hanging fruit will not bother to parse out the truth. They'll most likely switch to an easier target.

Some VoIP-related attacks involve *directory harvesting*, the attacker's attempt to gather all the phone numbers and addresses in your VoIP database or soft switch. WatchGuard VoIP security triggers whenever someone sends the SIP REGISTER command. The Application Layer Gateway then performs additional inspection to prevent directory harvesting. Too busy to find this option and turn it on? That's fine – WatchGuard's commitment to security makes this the default setting.

Secure Bandwidth

WatchGuard XTM VoIP security features also create advantages in throughput and efficient use of resources.

With the ability to deny calls compressed in certain codecs, you can standardize on the most efficient codecs, and reject calls using bandwidth-hogging formats, if you choose.

XTM's Application Layer Gateway can also enforce idle timeouts. If an existing media connection passes no data for a quiet period (a duration that you define), you can auto-terminate the connection, freeing up network resources.

In some phone-related attacks, hackers forced the victim system to make unwanted calls; for example, to expensive pay-by-the-minute toll numbers.⁵ In other attacks, hackers create a Denial of Service condition by establishing a high volume of gratuitous VoIP connections. WatchGuard XTM security helps you define a maximum number of allowable sessions and a maximum number of channels allowed per call, minimizing the damage an attacker can do with forced calls or excessive connections. Such limits also increase the likelihood that you'll spot a problem caused by an unusual volume of calls.

VoIP Security: the Bottom Line

As VoIP security emerges from its nascent state, beware of two major issues: unified implementations that blend your LAN and telephony without due regard for data security; and vendors who claim to "support" VoIP security without actually adding to your defense. For unified messaging, you need true unified threat management that filters normal Internet traffic *and* VoIP-related codecs and protocols. With the security features cited above, plus many more, XTM helps you support your organization with the telecommunication features it needs, while maintaining a level of security that steps past commodity firewalls.

Flexible Management

Despite the huge amount of attention researchers and analysts spend on dramatic "zero day" security flaws, such flaws are not the biggest threat to your network. The two biggest threats to business networks are *misconfiguration* and *inattention*.

The two biggest threats to business networks are misconfiguration and inattention.

How Management Affects Security

Owning and deploying the finest security solutions in the world will not strengthen your network security if the complexity of the products prevents you from using them properly. News headlines provide numerous examples supporting that statement:

- Maine-based Hannaford Bros. grocery chain suffered a major breach in March 2008, losing customer credit card data that has since been linked to at least 2,000 fraud cases worldwide. Hannaford CIO Bill Homa said that the cost to fix the breach would be "a big number... millions."⁶ Analysts believe the breach likely occurred because Hannaford had [misconfigured](#) a complex network-messaging tool, exposing sensitive data.⁷
- Verizon's RISK team reported in 2008 that after documenting 500 real-world intrusions across a four-year span, in 87% of the cases, the victim organizations had proper policies and controls in place *but were not following their own policies*.
- Research firm Gartner has predicted that misconfiguration will account for [70% of breaches](#) over wireless local area networks, through 2009.

⁵ For a 2009 example of such an attack, read "VoIP hackers strike Perth business,"

<http://www.zdnet.com.au/news/communications/soa/VoIP-hackers-strike-Perth-business/0,130061791,339294515,00.htm>.

⁶ "Hannaford to spend 'millions' on IT security upgrades after breach," Computerworld, April 22, 2008.

⁷ For more details on the Hannaford Bros. breach and how WatchGuard products could have prevented it, refer to our white paper, "How WatchGuard Could Have Saved Hannaford and TJX Money," available for download at <http://www.watchguard.com/infocenter/whitepapers.asp>.

- The Code Red worm was still infecting computers in 2008, even though vendors issued patches for Code Red exploits in 2001. Rbot, a bot that is at least four years old, was the most-often removed malware by Microsoft's Malicious Software Removal Tool in 2008. Both cases indicate that significant amounts of the Internet population neglect installing the software patches that stop such exploits.

Improperly configured gear undermines security. This belief propels WatchGuard's wholehearted commitment to making security appliances easy for you to use. It is also why management tools that other vendors charge a premium for, come standard in WatchGuard XTM products.

In today's stressed economic climate, many IT departments have reduced personnel. You and your remaining staff might have to fulfill responsibilities that may formerly have occupied the attentions of several more professionals. WatchGuard understands that you need your gear to work in intuitive ways, even though you have different management needs in different circumstances. If you're comparison shopping security products, check to see if other vendors include the following management features in their standard offering, as WatchGuard does.

Choice of Management Interface

All WatchGuard product families offer a choice of three different management approaches:

- Win32-based client GUI (WatchGuard System Manager)
- Web-based, clientless GUI
- Command Line Interface (CLI)

Fortinet, Cisco, and Sonicwall each offer some of these options, but none of them offer all three – and especially not in their standard product. With WatchGuard, the three management options come standard, and in addition, each of the three choices works in exactly the same way across WatchGuard Firebox and XTM product lines, from the most affordable models to the most powerful. For example, if you remotely administer a small branch office, and administer your main headquarters security appliance, you would probably use different WatchGuard appliance models, but you can still use the same techniques and menu choices.

Best-of-breed CLI Implementation

If you prefer a command line interface (CLI), you'll like the WatchGuard command line. Tricks you've learned as shortcuts in a Linux bash shell or using a Cisco OS (for example, typing "st" for "status") also work in the WatchGuard CLI. Programmed for efficiency, our command line accepts abbreviated commands, and auto-completes strings (such as expanding "conf" into "configure").

The scriptable CLI from WatchGuard accepts familiar commands, such as using the Unix Expect tool to configure or manage your appliance. The flexible scripting support provides excellent interoperability between WatchGuard products and other security devices on your network. In fact, you can even program WatchGuard appliances to respond automatically to threats that other devices on your network detect. Routers, switches, and external scanners each have different views of your network; with Fireware, you can harness the collective intelligence of all your devices to alert on spikes in traffic or to block hostile patterns.

The command line interface features a sensible approach that supports security. For example, attackers who manage to break into a network immediately attempt to disrupt or delete defenses. But the WatchGuard command line is not a shell, and provides no command for deleting the Fireware configuration file. Cisco users will also recognize the WatchGuard two-tier command mode, similar to Cisco's "enable" mode. Even when authenticated, you can only monitor WatchGuard devices and their status. To issue commands to them, you must enter Command Mode with an additional password – one more layer of security for your sensitive control center.

Our CLI's Help mode is context-sensitive. Entering a question mark at the end of a string calls up an explanation of that string or a list of relevant commands. Look at these differing responses to the ? character, depending on what came before it:

WG(config)#?	Configure commands:	bridge	local area network settings
		cluster	Firecluster
		ddns	dynamic DNS service
		debug-cli	configure debugging options
		default-packet-handling	default packet handling
WG(config)#ip ?		allowed-site	allowed IP address
		blocked-port	blocked ports
		blocked-site	blocked IP address
		dns	IP Domain Name Service Resolver
		dynamic-routing	dynamic routing configuration
WG(config)#ip i?		icmp	Internet Control Message Protocol
		ipsec	IP Security Protocol

Centralized and Remote Management

Perhaps you're not a great typist, or you just prefer a "mouse-able" interface. WatchGuard offers two choices: a rich Windows client and a graphical web interface.

You can install the Win32 client on any PC you want, thus transforming it into your WatchGuard Management Server. This client-based UI enables features such as one-touch configuration updates. You can push updates once, from one central location, and know that all corresponding WatchGuard security devices will get the same update. This eliminates the problem of re-typing configuration settings repeatedly for multiple devices, and eliminates any need to travel to various locations to install updates. The same principle applies to firmware updates and to the synchronization of license keys—they can be applied to all of your centrally-managed WatchGuard appliances as a single administrative move. What's more, these can be scheduled to take place automatically—perfect for doing updates during an off-hours maintenance window. You might find you really like using the Windows client, WatchGuard System Manager. It has been refined over years, and a robust user community swaps practical tips about it every day on our moderated user forum.

As an outstanding complement to the Win32 management client, the WatchGuard web-based, clientless user interface empowers you to control a WatchGuard appliance located anywhere in the world, from anywhere in the world. WatchGuard XTM's web-based GUI uses the latest technology to deliver an extremely rich, dynamic management environment that is light-years ahead of previous generations of web-based GUIs—such as those found on many other firewalls.

CLI, client-based GUI, and clientless web-based GUI – each has advantages to help you in your multifaceted role. Why choose one or the other when you can use all three?

Rich Reporting

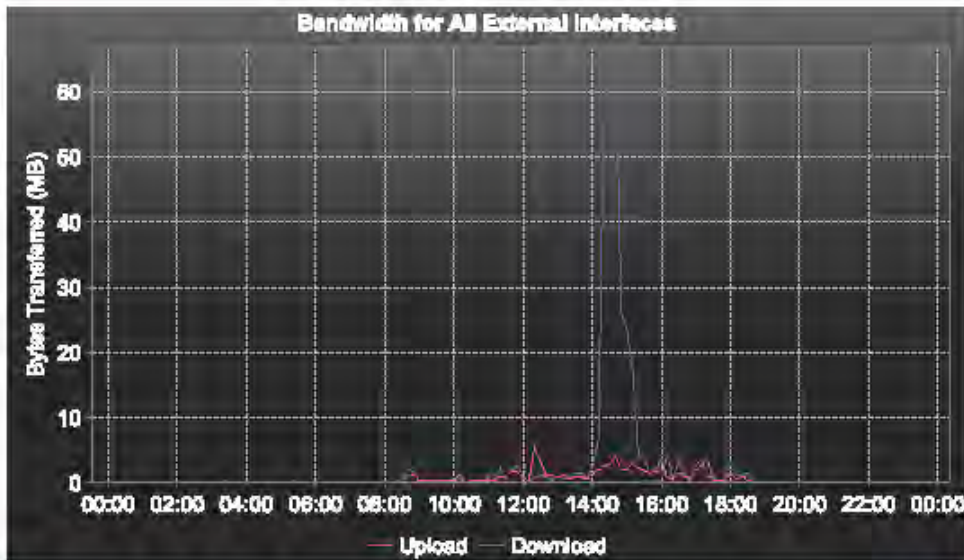
At WatchGuard, we believe a security appliance should provide you numerous ways to monitor your network. Our proven and trusted WatchGuard System Manager is already known for superb real-time, view-at-a-glance features such as HostWatch, Bandwidth Meter, and Traffic Monitor. But network security and business health intertwine. It's not enough for you to know what's going on in your network – you need to show other departments and senior management what you know. That's why Firewall XTM offers more than 40 preconfigured reports.

Bandwidth Usage for All External Interfaces

edge_00788 (203.215.153.106) 727300788245F



From	To	Number of Logs
6/16/08 12:00 AM	6/17/08 12:00 AM	130



Bandwidth Statistics for All External Interfaces

Time	Bytes Transferred			
	upload	Bytes (%)	Download	Bytes (%)
6/16/08 12:00 AM	49481	0.06%	39949	0.01%
6/16/08 12:10 AM	40140	0.05%	38473	0.01%
6/16/08 12:20 AM	51102	0.06%	52287	0.02%
6/16/08 12:30 AM	37328	0.04%	36820	0.01%
6/16/08 12:40 AM	40721	0.05%	38864	0.01%
Total	.21 MB	0.26%	.20 MB	0.06%

Figure 3: With Firewall XTM Reporting Options you can create groups of devices in WatchGuard Server Center, and create reports for device groups. Reports can be reformatted to HTML or PDF. Options menus let you customize report storage location and logo/URL used in HTML reports.

A partial list of reporting that comes standard with Fireware XTM includes:

- Packet Filter Summary by Service, by Time, and by Session
- Web Trend Summary
- Web Activity Audit
- Most Popular Domains
- URL Details by Time
- Most Active Clients
- Intrusion Prevention Summary
- VPN Tunnel Bandwidth
- Alarms
- Antivirus Service Summary by Virus
- Detail by Virus
- Proxied Traffic Summary by Proxy
- Proxied Traffic Summary by Time
- Proxied Traffic Summary by Session
- spamBlocker Summary
- SMTP Proxy Detail

Though we provide scores of preconfigured reports, that doesn't mean you have to stop there. You can use them as springboards to help you customize the exact report you want. You can even group devices and create custom reports for each group. You can output any of our reports on-demand or scheduled in advance. You can generate them as HTML or PDF, depending on your needs, and customize them with desired logos or URLs.

Flexible Management: the Bottom Line

Rival security vendors charge you a premium for features that merely parallel WatchGuard's standard management package, included with purchase. WatchGuard lets you use client-based, web, and command line interfaces, at your discretion, at any time, without restriction. All methods work the same across all our products. No standard reporting package surpasses WatchGuard's offering – in fact, as of this writing, Fortinet offers a mere *two reports* unless you purchase their expensive reporting upgrade.

Flexible, easy-to-understand, consistently performing controls mean more than convenience to you. We began this section citing a notorious break-in where the real culprit was a network tool that caused administrative confusion. Virtually all security experts agree that misconfiguration can lead to data compromise. With the management and reporting features cited above, plus many more, XTM takes the security appliance beyond the realm of commodity, offering demonstrably better security.

Conclusion: When No Means Yes

Every network administrator wants increased awareness of what traffic is doing on the network, and easier, more powerful ways to control that traffic. WatchGuard appliance models running Fireware XTM meet both those needs through features designed with you in mind.

Did this paper prove that all firewalls are *not* alike? You be the judge. Does your current firewall or security appliance:

- Inspect the full payload of HTTPS traffic, enable you to filter it in several different ways, then reassemble and re-encrypt it to send it to its destination securely?
- Not only permit VoIP traffic, but also add security by filtering unnecessary and unwanted codecs and cloaking tell-tale signs that divulge which VoIP system you use?
- Provide three different management interfaces, so that you can match your style or your need with the tool you prefer to use?

Not all firewalls are alike. Make sure you have the one that will do the most for your network. For more details on all the advantages you'll experience by using WatchGuard Fireware XTM, contact your WatchGuard reseller today or visit www.watchguard.com.

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

ABOUT WATCHGUARD

Since 1996, WatchGuard Technologies has provided reliable, easy to manage security appliances to hundreds of thousands of businesses worldwide. Our Firebox X family of extensible threat management (XTM) solutions provides the best combination of strong, reliable, multi-layered security with the best ease of use in its class. Our newest solution – the WatchGuard XTM 1050 – provides high performance and fully extensible, enterprise-grade security at an affordable price. WatchGuard is a privately owned company, headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. For more information, please visit www.watchguard.com.

No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features or functionality will be provided on an if and when available basis. ©2009 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard Logo, Firebox, Fireware are either registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other trademarks and tradenames are the property of their respective owners. Part. No. WGCE66633_072409