Top 10 Threats to SME Data Security

(and what to do about them)

October 2008

By Scott Pinzon, CISSP
Information Security Analyst, WatchGuard Technologies

Technical Editor: Corey Nachreiner, CISSP
Senior Network Security Analyst, WatchGuard Technologies

Introduction

The mass media that covers IT often fixates on network security issues that are sensational, yet rare. If you follow IT issues too, you've probably seen the extensive reporting of a virus or a worm that refers to a notorious celebrity – even if in reality it is low-risk, and slow-spreading.

Sometimes the mainstream reporting on network security isn't even factual. In the second half of 2008, both Fox News[1] and the Sunday *Glasgow Herald*[2] reported on cases they touted as "the worst cyberheist ever." In each case, the subjects of the story denied the reported version. When objective observers asked for proof of the media claims, no further evidence was presented.

The upshot of all this sloppy reporting is that it's difficult to find reality-based, accurate reporting on what the network security threat really is today for the average business.

Since 1999, the WatchGuard® LiveSecurity® team (the folks who provide expert guidance and support for WatchGuard customers) has monitored emerging network security threats daily, with a special focus on issues that affect small to medium-sized enterprises (SMEs). When we spot an issue that could negatively impact SMEs, we alert our subscribers with email broadcasts. Because our subscribers are over-worked, time-constrained IT professionals, we alert only when we know an attack is not merely feasible, but likely. This

[1] FoxNews.com, October 10, 2008, "World Bank Under Cyber Siege in 'Unprecedented Crisis'," http://www.foxnews.com/story/0,2933,435681,00.html.
[2] Market Watch, August 24, 2008, "Best Western Responds to Sunday Herald Story Claiming Security Breach," http://www.marketwatch.com/news/story/best-western-responds-sunday-herald/story.aspx?guid={A87F9682-AC67-4803-A135-B6ACF42C0956}&dist=hppr.

emphasis on business context and practicality makes the LiveSecurity service nearly unique. Our approach is constantly refined by input from our tens of thousands of subscribers, field trips to customer sites, focus groups, and security-over-beer bull sessions.

As a result, we've developed a seasoned and practical perspective that differs from typical IT reporting. We've formed carefully considered conclusions on what types of data compromises most often occur in the real world. This paper lists the top 10 most common vectors of data compromise from our experience as security analysts for SMEs. We also suggest practical techniques and defenses to counter each vector.

If you are an experienced IT director or CSO, you should find few surprises here. Most of these topics are well-known in the trenches. But we consider them under-reported, for the simple reason that "normal" is not sexy. An average mistake or common misconfiguration does not often build into a fascinating headline that acts as a click magnet for online ad revenue. But if you're an administrator concerned about hardening your network against common problems, this is a more useful list than, say, "the top data breaches of all time."

We dedicate these observations and advice to helping you reach your Internet safety goals – so that you don't find your organization as the subject of the next sensationalized (and possibly exaggerated) data security headline.

Assumptions

Last year, WatchGuard passed the milestone of 500,000 security appliances installed. The majority of these installations occurred at businesses having between 20 and 1,000 networked users. When we describe common vulnerabilities and compromises, we have a particular network environment in mind. Generally speaking, we view a "typical" SME network as having the following qualities:

- **Average complexity**. Fewer than 3,000 networked devices
- **Predominantly Windows OS**. Most of the computers within one release earlier or later than XP SP2; Vista in the minority; a few Linux or Unix servers; up to 20% of users on Mac OS X
- **Many Microsoft business applications**. Heavy use of the Microsoft Office suite and Internet Explorer; Exchange server; SBS. Alternate software might be present, but does not dominate (for example, the IT staff might use Firefox but most users do not).
- **Public-facing web site**. Whether self-hosted or staged by an ISP, the organization has a web site, and the site accepts input from the public (e.g., in sales order forms or Web 2.0 features such as forum comments).
- **Porous perimeter**. What was formerly the network boundary is now amended to accept connections from business partners, remote laptops, kiosks, smart phones, and other mobile devices. Most of these connections are encrypted.
- **Wireless end users**. Whether at company headquarters or out on the road (probably both), many of the organization's end users connect via Wi-Fi.
- **Remote offices and telecommuters**. We assume this typical SME is not entirely officed in one building. The SME has at least a couple of permanent branch offices and many remote workers, such as a geographically dispersed sales force with employees connecting to HQ from home.
- **Understaffed IT department**. For various reasons, the IT team is at least one head count short of fully staffed, and as a result, much of the work is done in reactive mode.

In our minds, this is North America's typical small-to-medium enterprise network.

Top 10 Threats

While we feel confident that our list of threats reflects reality, our attempt to rank them by how frequently they occur is subjective. We believe that Threat # 1 happens far more often than Threat # 10, but the exact ranking is not really the point. Our goal was to identify the most common data security failures so that an IT staff can address them explicitly and intentionally.

In some of these ten items, we use the word "reckless." We intend the word as defined in the dictionary: "utterly unconcerned about the consequences of some action; without caution; careless."[3] Today, the Internet must always be considered a hostile environment. To visit it carelessly is like visiting the toughest neighborhood in a big city after dark, flashing a roll of cash, and paying no attention to your surroundings. In short: unless you exercise caution, you're asking for trouble.

We list at least three mitigations or countermeasures for each threat. In the interest of saving your time, we tried not to repeat countermeasures. We could reasonably prescribe for the majority of these threats any of the following partial solutions:

- Monitor your logs regularly
- Install software patches promptly
- Train your users in security

If a particular countermeasure seems highly feasible in your particular environment, feel free to apply it across the board.

In hopes that this list helps you encourage your users to more thoughtful and cautious network usage, here are the threats our subscribers experience most often – and tips on defending your network against them.

Threat #10: Insider attacks

Verizon's Intrusion Response Team investigated 500 intrusions in 4 years and could attribute 18% of the breaches to corrupt insiders. Of that 18%, about half arose from the IT staff itself.[4] (This indicates that senior management would do well to keep an eye on the IT staff.)

In our experience, insider attacks occur less frequently in SMEs than in major corporations. We attribute this to environmental constraints. If an SME CIO is disciplined and diligent, poor practices are much easier to log, notice, and correct on a small network than in a network with tens of thousands of users. There is also more likelihood in SMEs that every employee knows every other employee. It's harder to bury suspicious activities in a crowd when your co-workers are friends (or at least, not strangers). Plus, if corrupt people make up *n* percent of the global population, in raw numbers, a smaller user population contains fewer corrupt people.[5]

The flip side of this coin, though, is that a smaller staff more often entrusts sensitive duties to a single person, with no one co-responsible to provide checks and balances. A sensational illustration of the problem of entrusting too much to a single person played out in July 2008 when Terry Childs, a disgruntled contractor for the City of San Francisco, locked the City out of its own new multi-million dollar fiber WAN network.[6] He

---

[3] From dictionary.com, http://dictionary.reference.com/browse/reckless.
[4] Summarized at http://www.infosectoday.com/Articles/2008_Data_Breach_Investigations_Report.htm. For a PDF of the report, visit http://www.verizonbusiness.com/resources/security/databreachreport.pdf.
[5] For example, if we stipulate that 2% of all employees are corrupt enough to sell or abuse company data, a company of 10,000 employees has 200 potential traitors, while a company of 100 employees has only 2.
[6] "S.F. officials locked out of computer network," http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/07/14/BAOS11P1M5.DTL .

could do so because no one else on staff fully understood the network architecture. Resolving the situation cost the city at least $200,000 in contractor fees and paid overtime, and could add up to much more in the long run.[7]

Mitigating Inside Attacks

Implement the principle of dual control. Even if your key IT gal has earned your complete trust, can your company's work continue tomorrow if she gets hit by a bus? Implementing dual control means that for every key resource, you have a fallback. For example, you might choose to have one technician primarily responsible for configuring your Web, FTP, DNS, and SMTP servers. But at the very least, login credentials for those servers must be known or available to another person. Honest people tend to stay honest if they know that another observer could drop in at any time.

Formalize your hiring. If you're still hiring on the friend-of-a-friend method, perhaps it's time to step up to professional processes for hiring, including doing basic background checks. Depending on the type of data that resides in your network, criminal and credit checks might be appropriate, too. Always check the applicant's references – that practice is essentially free.

Reduce opportunity for mischief. Many insider compromises occur opportunistically. Promote the policy of locking computers into password-protected screensaver mode when leaving a desk unattended. Remind your users not to share their passwords with co-workers (middle-managers trying to empower their staffs typically are the worst at password overshare). Use firewalls internally to subdivide your network; for example, you can cordon off sensitive network segments such as R&D or HR to their own contained segments. Consider rearranging floor plans and furniture so that workspaces are open to more lines of sight, reducing chances for sneakiness. Resuscitate any security awareness campaigns that may have fallen by the wayside.

Threat # 9: Lack of contingency planning

Businesses that pride themselves on being nimble and responsive oftentimes achieve that speed by abandoning standardization, mature processes, and contingency planning. Many SMEs have found that a merely bad data failure or compromise turns disastrous when there is no Business Continuity Plan, Disaster Recovery Plan, Intrusion Response Policy, up-to-date backup system *from which you can actually restore*, or off-site storage. Each of these is considered a standard, base-requirement business practice, yet many SMEs treat them as "luxuries" and "overhead." Though such practices don't improve the bottom line immediately, your bottom line will experience much worse punishment if you procrastinate on contingency preparation until it's too late.

Mitigation for lack of planning

Policy development has a reputation for being painful, but it doesn't have to be that bad – nor all that expensive. Certainly if you have budget for it, hire an expert to help you develop sound information assurance methodologies. If you don't have much money to work with, leverage the good work others have done and modify it to fit your organization. These resources can help show you the way:

- "Producing Your Network Security Policy"
  http://www.watchguard.com/press/whitepapers.asp
  A common-sense approach that makes policy easier to draft, maintain, and enforce, using in-house expertise

[7] "Tab for lockup of San Francisco's WAN may reach $1M,"
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=326239.

- The SANS Security Policy Project
  http://www.sans.org/resources/policies/
  Free resources, including sample policies and policy templates; deployment guidelines

- Internet Security Policy: A Technical Guide
  http://www.rxn.com/services/faq/internet/ISPTG.html
  Developed by Barbara Guttman and Robert Bagwill for the US National Institute of Standards and Technology (NIST), this classic paper still applies

Threat # 8: Poor configuration leading to compromise

Inexperienced or underfunded SMEs often install routers, switches, and other networking gear without involving anyone who understands the security ramifications of each device. In this scenario, an amateur networking guy is just happy to get everything successfully sending data traffic back and forth. It doesn't occur to him that he should change the manufacturer's default username and password login credentials.

Hackers keep long, diligently maintained lists of default logins to virtually every networking device, from the most expensive switch to the cheapest printer.[8] If the configuration hasn't been changed from its default, anyone capable of doing a basic Internet search could feasibly log into your network resources and take control.

Network settings must be chosen with diligence and care. On one hand, most vendors ship their products with wide-open default settings, in order to minimize calls for technical support. Even if you've bought very powerful network security gear, those powerful defenses might not be turned on by default. On the other hand, mucking about with settings you don't fully understand could turn *off* defenses, or put the device in an unsafe listening state. A lot of networking equipment uses terminology that is difficult to understand, or labels that improperly communicate what an option does. In Verizon Business's report on the causes of 500 real-world data breaches, 62% could be attributed to significant internal errors that caused or directly contributed to the breach.[9] In short: configure, but configure with care.

Mitigation for poor configuration choices

Always change the default username and password when installing networked devices. This requires no expertise and has no downside (unless you forget the password). Your password should be at least 15 characters long; using a favorite phrase from a movie, song, or scripture works well. The login credentials should be recorded and stored in a password vault that at least one other administrator can access.

Perform an automated audit scan. If you can afford it, hiring a penetration-testing organization to audit your network is a sound idea. But if you can't afford to hire consultants, you probably *can* afford a one-time, automated scan of your network. And if even *that* surpasses your budget, get your hands on a free tool such as Nessus[10] or Nmap[11] and find out what is connected to your network. There are many, many vulnerability management products on the market at all price points. Regular use of one or more of them should be part of your network maintenance routine.

---

[8] One example, maintained by a German hacker collective, can be found at http://www.phenoelit-us.org/dpl/dpl.html. Many such password lists exist.
[9] Verizon Business RISK Team, "2008 Data Breach Investigations Report," www.verizonbusiness.com/resources/security/databreachreport.pdf.For a snappy summary, see http://www.infosectoday.com/Articles/2008_Data_Breach_Investigations_Report.htm.
[10] Nessus is vulnerability scanning software, and may or may not be free to you, depending on how you use it. For more information, start with the Wikipedia entry: http://en.wikipedia.org/wiki/Nessus_(software).
[11] Nmap, short for "network mapper," is available as a free download: http://nmap.org/.

Have a consultant check you out. If you can tell you're in over your head when you try to configure a device, get expert help. Your ISP can probably recommend qualified consultants. So can your WatchGuard reseller.

Select solutions that are easy to use. When you add to your network, take advantage of free trials and hands-on demos. All SMEs love a bargain, but give extra consideration to products that make tasks understandable and easy. Getting a great price for gear you can't understand is a false economy.

Threat # 7: Reckless use of hotel networks and kiosks

Virtually every business has at least one or two (if not a hundred) road warriors attending industry events, visiting prospective customers, and meeting with clients. These employees most often work from laptop computers.

Hotel networks are notoriously lousy with worms, viruses, spyware and malware, and are often run with poor security practices overall.[12] Public kiosks make a convenient place for an attacker to leave a keylogger, just to see what falls into his net. Laptops that don't have up-to-date personal firewall software, anti-virus, and anti-spyware can get compromised at kiosks. Then, the next time the employee attaches to the headquarters network, a smart attacker can use that compromised laptop as the first stepping-stone to penetrate your entire network.

Adding to the risk: in a survey commissioned by Fiberlink, one in four road warriors admitted to altering security settings or purposely delaying security updates on a laptop in order to get their work done.[13]

Traditional defenses can be rendered useless when the user literally carries the laptop around the gateway firewall, and connects from inside the Trusted zone.

Mitigating reckless use of hotel networks

Make sure your road warriors have comprehensive defenses on their computers. Any device that's going to roam the wild and then return to your network should have on board, at minimum, anti-virus, anti-spyware/malware, and a personal firewall. Make sure that these all updated regularly.

Set and enforce a policy forbidding employees from turning off defenses. Workers used to shifting for themselves on the road often conclude, accurately or inaccurately, that laptop defenses are preventing them from doing their jobs. Many workers then disable the defenses. That practice might "solve" a short-term problem, but it also puts their computers at much greater risk. If you have IT personnel on call, your policy should be that workers are never to turn off defenses unless they call and receive authorization from you. Many popular anti-virus solutions can be configured so that they cannot be turned off, even by a user with local administrator privileges; check for such capabilities in your current solution.

Install client integrity checks at headquarters. You can find a wide variety of products designed to check the integrity and security health of remote clients requesting access to your servers. Different products filter by differing criteria. For example, you can reject connection requests unless they come from trusted MAC or IP addresses. Other types of products will check that the requesting client is running the latest versions of anti-virus, anti-spyware, firewall, and so on. When trying to select an endpoint integrity product,

---

[12] A recent study of 147 hotels by Cornell University found inadequate security practices at many of them. 20% of the hotels still used hubs in their networks and did not encrypt traffic, meaning, any guest of the hotel with a packet sniffer could see whatever hotel network activity and web surfing any other guest on the same subnet was doing. For more, see the Web Admin Blog entry "Consider Your Hotel Network Hostile," (http://www.webadminblog.com/index.php/2008/09/15/consider-your-hotel-networks-hostile/) and Cornell's report, "Hotel Network Security: A Study of Computer Networks in U.S. Hotels," available at http://www.hotelschool.cornell.edu/research/chr/pubs/reports/abstract-14928.html.

[13] Fiberlink commissioned Kelton Research, who surveyed 333 IT professionals on line. The results were written up in a white paper, available from Fiberlink: http://www.fiberlink.com/fiberlink/en-US/knowledge/whitepapers/Kelton_Research_Results.html.

investigate how it performs remediation: if the product determines that an attempted connection does not meet integrity checks, what does it do? Ideally, if the problem is outdated defenses on the client, your integrity-checking solution should fix the problem automatically.

Threat # 6: Reckless use of Wi-Fi hotspots

Public wireless hotspots carry all the same risks as hotel networks -- and then some. Attackers commonly put up an unsecured wireless access point which broadcasts itself as "Free Public Wi-Fi." Then they wait for a connection-starved road warrior to connect. With a packet sniffer enabled, the attacker can see everything the employee types, including logins. This attack is particularly nefarious because the attacker pulls the data out of the air, leaving *absolutely no trace* of compromise on the victim computer.

The breadth and scope of wireless attacks is quite wide. For example, attackers can simply sit in the parking lot of any retail establishment that offers a public Wi-Fi hotspot; fire up a wireless packet sniffer; and record everything that goes by, in real time. But in another wireless attack known as sidejacking,[14] an attacker can capture the session ID provided to your employee when she logs onto her web mail account. Depending on the web mail site's settings, the attacker could replay the session ID as much as *six months later* and read your employee's web mail.

Mitigating reckless use of Wi-Fi

Teach users to always choose encrypted connections. If a road warrior is using a company-authorized computer to connect back to your network, have the user connect via a Virtual Private Network (VPN). This encrypts the data stream, so that even though eavesdroppers can still listen in wirelessly, what they receive is gibberish. In public hotspots, users should always select an encrypted connection where possible. You can tell which networks are encrypted because they require a password, and the user interface will usually show which encryption method is in use: WEP, WPA2, etc. In public spaces, this offers only scant protection, since the public can learn the network password. However, it stops the most casual wireless wardrivers.

Encourage users to select reputable hotspots. When you're on the road and desperate for an Internet connection, you can find yourself in some pretty sketchy venues.[15] Who knows what security practices they follow at Gung Lee's Smoke/Lotto/Manicure and Internet Café? Speaking very generally, a Wi-Fi hotspot at a global franchise such as McDonald's[16] or Starbucks[17] will have been built with customer safety in mind, and the store cares about its business reputation. Teach your staff to select known and quality hotspots whenever possible.

Teach users to prefer wired connections. Recent advances in cracking wireless encryption algorithms have dramatically decreased the amount of time attackers require to decrypt wireless transmissions.[18] These recent innovations have led some security experts to recommend, when data is truly sensitive, not to trust wireless connections at all. Even on a wired connection, data is still more secure using a VPN.

For further mitigation against public W-Fi threats, follow the tips under Threat # 7, "Mitigating reckless use of hotel networks."

---

[14] For details, see our video, "What is a sidejacking attack?" at http://www.youtube.com/watch?v=nFNFa-48lpI

[15] Or doing odd things such as holding your laptop out the window to find the wireless signal. *CIO*, August 20, 2008, "20 Crazy Things People Do to Get Wi-Fi Connections," http://www.cio.com/article/445070/_Crazy_Things_People_Do_to_Get_Wi_Fi_Connections?page=1.

[16] McDonald's statement of wireless policy: http://www.mcdonalds.com/wireless/general_info.html.

[17] Details of Starbucks' wireless offering: http://www.starbucks.com/retail/wireless.asp.

[18] *The Register*, October 10 2008, "Turbo-charged wireless hacks threaten networks," http://www.theregister.co.uk/2008/10/10/graphics_card_wireless_hacking/.

Threat #5: Data lost on a portable device

Much sensitive data is compromised every year when workers accidentally leave a smart phone in a taxi, a USB stick in a hotel room, or a laptop on a commuter train. Does this happen often? The British government lost 747 laptops in four years.[19]

Setting aside employee negligence, sometimes devices are stolen: In Australia, 200,000 phones are stolen per year, or roughly one every three minutes.[20] In the UK, 2 million mobile phones are stolen per year, or, one every twelve seconds.[21]

In short, when the topic is data stored on small devices, it's wiser for administrators to stop thinking about what they'll do "if that device ever gets lost…" and instead, think, "*when* it gets lost…"

Mitigating data lost on portable devices

Teach users to proactively defend physical gear. Most robberies are opportunistic. Typical scenario: Alice's smart phone is in her purse. She's sitting in a coffee house and she decides her coffee needs more cream. She guesses it will be safe to leave her purse unattended during the few seconds it takes to cross to the counter where the cream is. The moment Alice stands and turns her back, a fleet-footed thief can silently snag the purse and flee. Even if Alice had the disposition and stamina to give chase, how could she, in business clothes and pumps? Most robberies can be prevented by refusing to put the device at risk, even briefly.

Company policy should require mobile devices to be password-protected. Most mobile devices offer the option of encrypting all user data on the device, and/or requiring a password in order to access the data. Users typically view such measures as drags on their productivity, and disable them. Your policy should require the use of available security measures, and detail serious consequences for employees caught ignoring the policy. Functionally, this is unenforceable. But a percentage of true believers will follow the policy. And it means you're covered and have the right to act if a flagrant abuse of the policy comes to light.

Manage mobile devices centrally. As technological reinforcement of the policy described above, consider investing in servers and software that centrally manage mobile devices. RIM's Blackberry Enterprise Server can help you ensure transmissions are encrypted; and if an employee notifies you of a lost phone, you can remotely wipe data from the lost Blackberry. You can also centrally enforce password access and password length on the devices, lock out Bluetooth connections, and more. For devices that run Windows Mobile 5.0, use the Messaging and Security Features pack and ActiveSync to enable device-wipe features. Even the risky iPhone can beef up its security a bit, though not centrally.[22] These steps go a long way toward minimizing the negative impacts of lost devices.

Invest in encrypted USB flash drives. USB thumb drives, similar in size to an AA battery, are wildly popular and frequently lost. If you authorize company use of USB flash drives, spend the extra money to get the encrypted kind. Compared to a data breach, it's cheap insurance. Such drives[23] keep all their contents strongly

---

[19] Asiaone, July 19, 2008, "British ministry admits loss of 747 laptops, secret data files," http://www.asiaone.com/Digital/News/Story/A1Story20080719-77633.html.

[20] Decoder, August 2008, "Mobile Phone Theft. What can be done?", http://www.decoder.com.au/2008/08/06/mobile-phone-theft-what-can-be-done/.

[21] CNET Australia, May 10, 2007, "Lost mobile phones: a survival guide," http://www.cnet.com.au/mobilephones/phones/0,239025953,339276173,00.htm.

[22] For details, refer to "Six Essential Apple iPhone Security Tips," CIO, October 7, 2008; http://www.cio.com/article/453280/Six_Essential_Apple_iPhone_Security_Tips?page=1.

[23] For example, the Kingston Data Traveler Elite Privacy Edition flash drive encrypts all its contents with 128-bit AES and requires a password to decrypt them. Brute force attacks fail, because after 25 consecutive failed password attempts, the drive destroys the data it contains. http://www.engadget.com/2006/03/16/kingston-data-traveler-elite-privacy-edition-co-self-destructing/.

encrypted. The legitimate user merely has to enter a password to go about business as usual. But if the device is lost or stolen and an attacker tries to guess the password, a number of consecutive wrong login attempts triggers data destruction. Many security professionals speak highly of Ironkey products, and a search on "secure USB flash drive" will show you many additional options.

Train your users in data security. Viewing your user community as willful laggards becomes a self-fulfilling prophecy. Instead, equip them to handle portable data with savvy. According to a survey from the Computing Technology Industry Association (CompTIA), when organizations instituted training for remote workers, 92% of these organizations said the number of major security breaches were reduced.[24]

Threat #4: Web server compromise

Almost every SME today has a web site, and almost every web site has application code customized uniquely for the organization that runs the site. The most common botnet attack today is against web sites; and the fatal flaw in most web sites is poorly-written custom application code. Attackers have compromised hundreds of thousands of servers in a single stroke with automated SQL injection attacks.[25] Legitimate sites are then caused to serve malware, thus unwittingly spreading the bot master's empire. Legitimate sites that have suffered these attacks and wound up serving malware to their customers include those of Snapple, the City of San Francisco,[26] Sony Playstation,[27] and the British government.[28]

Mitigating web server compromise

Audit your web app code. If (for instance) a web form has a field where a visitor is intended to supply a phone number, the web application should be written to discard excess characters. If the code is not written in this way, an attacker can submit an entire executable script of thousands of characters in a field that need accept only 14 characters. Web app code should also fail shut when handling errors; in other words, if the program doesn't know what to do with data or a command, it should reject it, not process it. These are just two examples of the security issues that commonly go wrong for the SME that is too frugal or too rushed to audit web site code.

Input validation is the fancy term for making sure your web apps will not accept malicious data or commands from the Internet. Allowing for your budget, seek the best code auditing solution you can afford (whether a team of experts or an automated tool), with emphasis on finding out whether your code does proper input validation.

Don't trust your web server. Any web server that the public can access should not reside within the Trusted segments of your network. Keep such web servers in the "DMZ," and minimize the number and type of connections from the server to more trusted internal resources.

Use a firewall that can filter HTTP and HTTPS traffic. If your firewall performs little more than stateful packet-filtering, it is focused primarily on packet headers rather than packet payloads. That's similar to hiring someone to inspect your mail for letter-bombs, but he only examines the outside of the envelopes. Seek a gateway solution that can catch malicious HTTP traffic. It should be able to inspect content, not just headers, by examining traffic both heuristically and against a list of "known bad" signatures.

---

[24] *CIO*, May 21, 2008, "Mobile-Related Security Threats on the Rise," http://www.cio.com/article/364113/Mobile_Related_Security_Threats_On_the_Rise.
[25] A botnet called Asprox provides an example of this. For details, see Secureworks' analysis from May 2008: http://www.secureworks.com/research/threats/danmecasprox/?threat=danmecasprox
[26] http://securitywatch.eweek.com/exploits_and_attacks/huge_volumes_of_bigtime_sites_hacked_via_asprox_attacks.html
[27] http://blogs.zdnet.com/security/?p=1394&tag=rbxccnbzd1.
[28] http://security.itproportal.com/articles/2008/07/24/super-malware-asprox-takes-uk-storm-targets-government-websites/

Threat #3: Reckless web surfing by employees

As recently as five years ago, the average person could discern when he or she was surfing to a shady area of the Internet. You usually didn't get infected with malware unless you visited a porn site, a gambling site, or some sort of low-rent, illicit web page. No more. A 2006 study by the University of Washington[29] found that the sites that spread the most malware were (in order)

1. Celebrity fan sites (such as the type that give breathless updates on the follies of Paris Hilton and Britney Spears)
2. Casual gaming sites (where you can play checkers or Battleship against a stranger)
3. Porn sites (coming in at a surprising third place)

Employees who surf to non-business-related sites end up inviting malware into the corporate network. The unhappy payoff can include bot clients, trojans, spyware, keyloggers, spambots – pretty much the entire gamut of malware.

Since the UW's 2006 study, social networking sites such as MySpace and Facebook have taken the lead as veritable cesspools of spam, trojans, and spyware – not to mention crash-prone apps and, with video involved, avalanches of non-business-related, bandwidth-hogging traffic[30]. Click-happy users mean no harm, but they cause it anyway.

Mitigating reckless web surfing

Gather data on your company's current web habits. The computers and Internet connection at your company headquarters are often more robust than the equipment your employees have at home. As a result, they usually prefer your network over their own for shopping, paying bills online, and more. Employees often consider this a soft benefit of working for you.

But you might be surprised at the unreasonable lengths some employees go to. If you have not looked at outbound HTTP traffic in your logs, you should. Clients following our advice have discovered that employees surf porn at lunch; run their own small business sites from the company's network; download pirate software via company servers; and more. Get some empirical evidence of how much cyberslacking is occurring within your user community; then you can respond appropriately, based on facts.

Adopt a stricter policy. Because the amount of hostile traffic on the Internet has climbed dramatically in the last three years, liberal web policies need to be reconsidered. The data you gather on current web traffic might provide good reason to override your employee's protests and implement new, safer policies. Depending on what's appropriate to your business environment, consider revising your Acceptable Use Policy to rope off entire swaths of the Web. Think big and take back your network: if you'll be safer implementing "no sports, no celebrity sites, no political blogs, no [fill in the blank];" consider banning anything that doesn't support your institutional mission.

Implement web content filtering. You can put technological enforcement behind your new tough policy using web filtering software such as the WebBlocker service from WatchGuard. Web filtering solutions maintain databases (updated daily) of blocked URLs in scores of categories. More categories mean more nuance. If, for example, you run a medical clinic, you might need to allow access to some sports sites related to injuries your patients sustain; but with URL filtering, you can still block Fantasy Football and the NFL.

---

[29] University of Washington News, February 2006, "Spyware poses a significant threat on the Net," http://www.uwnews.org/article.asp?articleID=22331.
[30] WatchGuard Blogs, October 2008, "Brace your users for anti-social networking," http://blogs.watchguard.com/2008/10/brace-your-users-for-anti-social.html.

As with many of these Top Threats, security awareness training is part of the mitigation. Consider making it mandatory for every employee to view a training video such as our free "Spyware: Think Before You Click"[31].

Threat #2: Malicious HTML email

The vast majority of attackers who choose email as their primary vector have stopped sending emails with malicious attachments. (That's so 2003!) The most common email attack now arrives as an HTML email that links to a malicious, booby-trapped site. One wrong click can trigger a drive-by download.[32] The hazards are the same as in Threat # 3, "Reckless web surfing;" but the attacker uses a slightly different vector to get the victim to his malicious website.

Mitigating malicious HTML email

Implement aggressive spam filtering. Take advantage of the plethora of excellent spam filtering products, and layer different approaches. You can filter spam at the desktop of the recipient; at your mail server; and at the gateway to your network. You can do it via Bayesian filters, character strings, regular expressions, and recurrent pattern detection. Ask a trusted advisor to help you craft the combination of defenses that is best for you. Since more than 80% of all emails are spam,[33] we recommend solutions that drop unwanted email at your gateway, before the spam burdens your mail server. That frees up more server resources for handling legitimate email.

Implement an outbound web proxy. Some administrators set up their LAN so that all HTTP requests and responses get re-directed to a web proxy server. This technique provides a single choke-point where all web traffic can be monitored for appropriateness. The web proxy won't catch an inbound malicious email, but if a user on your network clicks a link in that HTML email, doing so generates an HTTP request that the web proxy can catch. This provides two advantages. First, the majority of malware is not very sophisticated, and simply won't work if a web proxy interrupts the HTML request – the link won't know how to "phone home." Second, the proxy provides an excellent opportunity to scan or filter HTTP and stop questionable traffic. If the user's HTTP request never makes it to the attacker's booby-trapped web site, the trap is never sprung, and your user and your network do not become the victim.

Raise user awareness about email security. Malicious email grows increasingly deceptive year after year. The days are gone when you can count on recognizing spam because it is spelled poorly. Users must be made aware that criminals might send them email. Users also need examples of what dangerous emails look like. Implement periodic training and reminders. For starters, try showing our free security awareness video, "Bud Has Mail."[34]

Threat #1: Automated exploit of a known vulnerability

Verizon's *2008 Data Breach Investigations Report* compiles factual evidence from more than 500 data breaches, occurring over the course of four years. Verizon's RISK Team was able to verify that 73% of the breaches occurred from external sources (as opposed to insider betrayal, or sloppiness on the part of a business partner).

In all but rare cases, the typical SME will not be the target of a focused, purposeful attack by a malicious hacker or criminal collective. Most of the threat to a typical small business comes from the tides of automated attacks scanning the Internet daily. The Open Web Application Security Project (OWASP) characterizes such attacks as

---

[31] Available from Google Video at http://video.google.com/videoplay?docid=-4094518401580008932.
[32] If this term is unfamiliar to you, see our video, "What Is a Drive-by Download?" at http://video.google.com/videoplay?docid=-3351512772400238297&ei=DubvSOTxOpH8qAPUtJH4Dw&q=Corey+Nachreiner.
[33] CommTouch Year-End Email Threat Report, http://www.commtouch.com/Site/News_Events/pr_content.asp?news_id=983&cat_id=1.
[34] Preview and free download available at http://www.watchguard.com/budhasmail.

"non-targeted,"[35] because they attempt to compromise any computers having security holes the attacker knows how to exploit. The vast majority of automated attacks on the Internet try to exploit holes in Windows.

Microsoft provides patches every month, but short-staffed SMEs may fail to install the patches. Installing patches can be daunting. Sometimes the patch itself introduces new problems to the network, so all patches must be tested before they are deployed. Yet, patching is essential.

Consider these contrasting statistics. There are botnets right now successfully exploiting flaws that Microsoft patched *four years ago*.[36] On the other hand, in Verizon's investigations of 500 data breaches, there were zero cases of an attacker exploiting a vulnerability within 30 days of it being announced and patched. So statistically speaking, if you can patch a known vulnerability within 30 days of the vendor publishing the patch, you are likely to head off attacks.

Negligent SMEs commonly get victimized if they don't install Windows patches during the same month the patch is published. But your network contains much more than Microsoft products. Your patching routine needs to extend systematically to all the applications and OS components on your network.

Mitigating automated exploits

Invest in patch management. For any LAN larger than a simple home network, it's risky to patch on an ad hoc basis. Patch management software will help you scan your network, identify missing patches and software updates, and distribute patches from a central console, greatly increasing your chance of having your entire network up to date. For a Windows-based LAN, the most applauded patch management software comes from Shavlik[37]. However, if you search on "patch management software," you can find solutions at all price points.

Build an inexpensive test network. Some vendors offer rock-solid patches and updates; others (especially those with complex products), issue patches where the cure is worse than the disease. Even reputable companies can slip up. Therefore, we recommend installing a patch on a test system and seeing how it behaves before deploying it throughout your network. If you don't have a test network now, the next time you replace outmoded desktop computers and servers, hang onto them and dedicate them to being your test network. Alternatively, if you have one spare computer that is robust, you can affordably set up a "test network" on it by using virtualization products to install virtual servers and virtual PCs. You can search on "virtualization products" to learn more about products from VMware, Microsoft, Citrix, and many, many others.

Keep an eye on the vendor forums that mean the most to you. Any software application or networking device that is critical to your ability to stay in business should be represented on the short list of websites you check every day. User communities, official blogs, and support forums are often the first to report on new vulnerabilities. Problems caused by faulty patches generally come to light within two days of the patch or upgrade release as relevant forums light up with urgent discussions. By watching them, you can learn when the majority of users deem it wise to upgrade.

Emphasize thoroughness over speed. "Patch promptly" has been preached so much that some organizations turn patching into a fire drill. You don't need to work your staff overtime or rush them. It's more important to verify that patches or updates are stable and that they don't break any custom applications your organization runs. You want to make sure you patch every vulnerability you can, so take a systematic approach. As long as you plan the work and work the plan, the odds are you will get to your security holes before hackers do, and without overlooking an obscure yet important upgrade.

---

[35] The highly respected OWASP lists "non-target specific" attacks as the number one threat agent on their wiki: http://www.owasp.org/index.php/Category:Threat_Agent .
[36] For substantiating details for this claim, search the Web for bots by name. Examples include Rxbot (aka Rbot), Gaobot, and SDbot.
[37] Shavlik Netchk has enjoyed wide support from networking professionals for years; for details, see http://www.shavlik.com/netchk-protect.aspx .

Minimize what's installed on your network. Most end users have no concept of ongoing maintenance, or of the unintended side-effects possible when applications interact. The more applications and software utilities you have on your network, the more opportunities you create for attackers to find a weak spot. Seek to standardize as much as possible on a single corporate hard drive image with a set suite of apps, tools, and defenses. For example, if workers can get their needs met with Windows Media Player, there's extra risk but no extra upside to also allowing Quicktime, WinAmp, RealPlayer, and DivX on your network. When departments ask for exceptions, require a business justification. In essence, this tip is saying *do* put all your eggs in one basket – but then guard that basket!

Consider alternatives to "hole-y" software. Certain software applications attract attackers, in part because of their popularity; in part, because they have known vulnerabilities. If these oft-attacked packages are not vitally integrated into your network environment, consider replacing them with less attacked or more secure alternatives. For example, Internet Explorer has long been a favorite target of mass exploits. Consider switching your standard corporate browser to Mozilla Firefox, running the plug-in called NoScript. If your users are just as happy with Mac OS X as they are Windows, currently there are far fewer trojans and attacks for OS X. Switching might be a viable alternative for you.

However, don't fall for security by obscurity. Today's attackers follow the money. If today's "safe" software gains enough market share to lure attackers, it might become the next big target. If you switch a common application for a less common one, it should be because the less-common app has genuine security advantages, not because attackers haven't focused on it yet.

Conclusion

To recap, we believe that realistically, the top ten threats to SMEs are:

10. Insider attacks

9. Lack of contingency planning

8. Poor network configuration leading to compromise

7. Reckless use of hotel networks and kiosks

6. Reckless use of Wi-Fi hot spots

5. Data lost on a portable device

4. Web server compromise

3. Reckless web surfing by employees

2. Malicious HTML email

1. Automated exploit of a known vulnerability

All of these attack vectors are well-known to security professionals. Mature processes, techniques, and technologies are available to help you defend against them. Although on some days it might feel like the bad guys are winning, through diligence and persistent effort, you can harden your network against attacks. Thousands of network administrators run for years at a time without any compromises or intrusions. We hope this paper contributes to your being counted among those savvy administrators. For business decision makers, XTM offers an ideal cache of reliable security and superior TCO. XTM allows businesses to utilize mobility, consumer technologies, Web 2.0, and other new business applications in a highly secure manner.

For more information

In addition to the countermeasures we've suggested above, a diligent network administrator might want to examine the range of security solutions that WatchGuard Technologies offers. Our Extensible Threat Management (XTM) gateway security appliances go a long way to solving nine of the ten threats listed herein. (Sadly, our appliances cannot stop your employees from losing portable devices.) But our solutions *can* help you secure your wireless network, check the integrity of clients requesting access to your network, filter spam, proxy web services, minimize insider threats, create VPNs, and much more. For details, visit www.watchguard.com or talk to your WatchGuard reseller.

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. All products are backed by LiveSecurity Service, a ground-breaking support and maintenance program. 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.

WatchGuard Extensible Threat Management

An Overview of XTM

July 2008

Abstract

Unified threat management (UTM) spawned a new era of IT security. The promise of these integrated security appliances proved to be an exceptional and efficient way of securing commercial networks. However, businesses today face an inflection point, dictated by changing market trends and new technologies that demand more of today's UTM. Hence the need is for eXtensible threat management (XTM) solutions, the next generation of UTM appliances. XTM is predicated upon the substantive expansion of three elements: more security, greater networking capabilities, and more management flexibility. This paper provides an overview of these issues and the WatchGuard® Technologies perspective on "extensibility" and XTM.

Unified Threat Management (UTM)

Originally coined in 2003 by IDC analyst, Charles Kolodgy, the term *unified threat management (UTM)* represented a ground-breaking concept in having disparate security functions – firewall, intrusion detection/intrusion prevention (IDS/IDP) and gateway anti-virus (AV) – reside in a single, integrated network security appliance.

WatchGuard Technologies, a pioneer of firewall technology since 1996, was an early innovator of UTM solutions, and was one of the first to lead the industry with high performance UTM offerings. By January, 2008, WatchGuard offerings had far exceeded the foundational elements of UTM (firewall, IDS/IPS and gateway AV) to include a host of new security and network connectivity features, such as web-based content filtering and spam blocking, as well as both IPSec and SSL VPN capabilities.

UTM appliances quickly became a network security favorite for SMB, mid-market (SME), and enterprise branch office environments. UTM devices gained substantial ground in education, healthcare, and retail segments because they helped to address regulatory mandates, such as the Children's Internet Protection Act (CIPA), Health Insurance Portability and Accounting Act (HIPAA), and Payment Card Industry Data Security Standard (PCI DSS).

As the demand for UTM grew, so too did the industry and the number of respective solutions. By 2007, the UTM market had grown approximately 35 percent year-over-year, to reach $1.216 billion. By 2008, industry analysts estimate that sales of UTM appliances will surpass traditional firewall/VPN solutions. By 2010, sales of UTM devices are expected to exceed $2.5 billion.

WatchGuard confirms that analyst reports are on target, and that the UTM market continues to grow at a record pace. In particular, WatchGuard sees accelerated UTM market growth as appliances expand into new geographic regions around the world and move upstream into more enterprise and distributed environments. What is unclear right now is whether the current state of UTM offerings in the market is sufficient to fully meet future business demand and IT expectations.

Trends Affecting UTM

Clearly, UTM has moved from a concept to a business and network security reality. The growth and acceptance of UTM is undeniable. However, there are factors to suggest that UTM, in its current state, will not be sufficient to tackle the next generation of looming security threats, nor capable enough to meet the needs of savvy businesses that leverage new forms of technologies to be more productive and efficient.

New Threats

Threats are changing. The next generation of security threats will present unparalleled challenges and risks. The "black hat" community is not the band of miscreants that it used to be. What was once done to gain notoriety and underground fame among fellow hackers has now turned into big business, similar to organized crime syndicates. Data is valuable, and gaining control of web sites, servers, and personal computers can be lucrative.

WatchGuard sees the next generation of security threats to be more sophisticated and less conspicuous. Security threats are taking on new forms, morphing common annoyances such as spam email and mutating them into hybrid spam/phishing/malware payload-delivery vehicles. The traditional attacks on network ports and data networking protocols will change to attacks that exploit holes directly at the application layer.

Threats are becoming more stealthy and concealed, as well. Typically, when a threat reaches a broad enough audience, a "signature" can be developed to counter and neutralize the threat. Today, the writers of these attacks have learned that low profile attacks keep threats "under the radar," and hence, avoid detection and the eventual signature that will wipe them out. Likewise, other attackers have developed automated repackaging malware applications so that the malware changes every few minutes – effectively staying ahead of any anti-virus vendors' ability to produce a signature.

Changing Business Dynamics

Business is changing. Several factors are all converging to change the way businesses operate. Leading this, WatchGuard sees business mobility, the "millennial" generation, the "consumerization" of IT, Web 2.0+, and new technologies, such as virtualization and Software as a Service (SaaS), all creating new dynamics for network security and data protection.

Mobility, mobile workers, and remote office technologies accelerate business opportunities, but at the same time, create new venues for security risks. According to a recent survey conducted by Stanford University and Hong Kong University of Science and Technology, "92 percent of Fortune 500 respondents agreed that uncoordinated mobility initiatives lead to security risks and high integration costs. But 93 percent reported that mobility can provide a significant competitive advantage."[1] The traditional desktop is being redefined by mobile devices and mobile applications. As this happens, IT staff must address the inherent security risks that accompany this trend.

Likewise, the next generation of workers, the "millennials", mirrors the benefits and risks associated with mobility. The millennial generation is instrumental in adopting new technologies, particularly, IM, peer-to-peer, and social networking tools, yet shows lackluster awareness and even disdain towards the risks that go with these technologies. In a recent blog post titled, "IT Risk and the Millennials," Samir Kapuria talks about what could turn out to be one of the most pressing issues for IT. Kapuria points out, CIOs are trying to figure out how to cope with this generation.

[1] "The Mobility Manifesto: What enterprise mobility means and how to make the most of it" – Nokia Corporation

> "Millennials are used to freely downloading software from the Internet, such as Skype; using applications like Facebook; and bringing their iPods and laptops into the office—all of it blurring the lines between personal and work life."[2]

New Technologies

Relative to this is the "consumerization" of IT and Web 2.0 technologies. Designed to foster more collaboration, greater efficiencies, the sharing of information, and more productivity, the IT landscape of "consumerized' technologies (iPhones/iPods, USB drives), and Web 2.0 applications (mash ups, peer-to-peer and social networks) is also creating new security and information leakage concerns. It has been noted that some consumer-oriented applications, such as Facebook or LinkedIn,` are being used as contact managers or even as CRM substitutes. Businesses that rush out and adopt these new tools may also find themselves in uncharted security waters.

For example, the media recently reported on a popular online consumer game, World of Warcraft, and how malware associated with the game is stealing user passwords and account data. For a consumer, that is a serious threat. By analogy, if one applies this type of scenario to something like Second Life, which quickly morphed from a game into a business-to-business[3] vehicle for corporate events, sales, training, marketing, and demand generation, then we see how deleterious this type of malware could be if it could capture corporate passwords and corporate data. Bottom line is businesses have yet to experience the risks associated with consumer technologies and Web 2.0 applications in the work environment.

New business technologies are shaping security profiles. This ranges from VoIP to Virtualization. For example, virtualization is the general term used to describe the abstraction of IT resources. Virtualization hides the physical characteristics of computing resources from their users, be they applications or end users.[4] This includes making a single physical resource (such as a server, an operating system, an application, or storage device) appear to function as multiple virtual resources; it can also include making multiple physical resources (such as storage devices or servers) appear as a single virtual resource.[5] As businesses adopt virtualization, they must understand the security risks associated with it.

Software as a Service (SaaS) presents similar security challenges for IT staff. With industry heavyweights, such as Cisco, Google, and Microsoft, pushing for more IT services to be "in the cloud," questions arise of

---

[2] https://forums.symantec.com/syment/blog/article?message.uid=306119
[3] Using Second Life as a Business-to-Business Tool, Information Week (April 26, 2007) http://www.informationweek.com/blog/main/archives/2007/04/using_second_li_2.html
[4] Electronic Commerce: A Managerial Perspective, Turban, E., (2008)
[5] "The Pros and Cons of Virtualization," Business Trends Quarterly, Mann, Andi (April 21, 2008); "Virtualization 101," Enterprise Management Associates (EMA), Mann, Andi (Oct. 29, 2007)

who controls the data, how is it protected, which laws and regulations apply, how is it audited, and what recourse is available should something happen? Assuming that SaaS is an inevitable reality, businesses will need XTM solutions to ensure secure connectivity to the cloud, as well as to protect the integrity of applications and data interactions.

Likewise, as businesses deploy new technologies, they must address protection in new ways. For example, mobility and data in motion is changing the concept of how to secure the network perimeter. Protecting the end point device will be subjacent to protecting users and data as they move through networking, web, and messaging platforms.

Lastly, businesses and IT administrators will have to do more with fewer resources. A recent Goldman Sachs report stated that security budgets are down from previous forecasts. As global economic issues create turbulent markets, companies are expected to react by reducing IT expenditures.

All of these factors – the next generation of threats, changing business dynamics (i.e. mobility, "millennials," consumerization of IT, and Web 2.0 applications), and new business technologies – dictate how network security will operate in the future. WatchGuard believes that the UTM industry is at an inflection point, and that the current state of UTM appliances is insufficient to fully address these factors. Therefore, what business and technical decision makers will need is the next generation of UTM – XTM, or extensible threat management solutions.

Extensible Threat Management (XTM)

Extensible threat management (XTM) is the next generation of unified threat management (UTM), integrated network security appliances. As stated by IDC analyst, Charles Kolodgy, in SC Magazine (May 2, 2008):

> "IDC believes that UTM will remain the primary security solution for distributed environments, but within the enterprise it will evolve into an eXtensible Threat Management (XTM) platform. XTM platforms will take security appliances beyond traditional boundaries by vastly expanding security features, networking capabilities and management flexibility. Future XTM appliances should provide automated processes – such as logging, reputation-based protections, event correlation, network access control and vulnerability management. Adding to the networking capabilities will be management of network bandwidth, traffic shaping, throughput, latency and other features, including unified communications."

Based on this definition, WatchGuard foresees XTM as an extension of the UTM category. XTM will expand on what UTM has delivered, but will include additional substantive developments in three core areas:

- More security features
- Greater networking capabilities
- More management flexibility

WatchGuard Extensibility

Extensibility means having the ability to extend or add on to. This is what WatchGuard is innovating with its UTM family of security and connectivity solutions. The vision is to provide XTM solutions that deliver extensibility. WatchGuard's extensible components are:

- Extensible protection
- Extensible management
- Extensible choice
- Extensible ownership

Protection

Extensible protection derives from the unique WatchGuard approach to network security. WatchGuard utilizes a security scheme built upon its "intelligent layered security" architecture that incorporates myriad security technologies, including application proxy technology to defend against spyware, malware, viruses, outside attacks and other harmful events. This approach of extensible protection guards against port and protocol-specific threats, as well proactively protecting businesses at the application layer, thus creating an "application aware" defense posture.

Management

Extensible management addresses the need to incorporate more network and management capabilities. This includes integration of networking technologies, such as WAN optimization, active/active failover for high availability (HA), and management software that allows one-touch control over hundreds of WatchGuard XTM appliances. As well, extensible management includes having open, standards-based management hooks, thus allowing businesses to leverage and utilize existing management suites, such as HP OpenView, to seamlessly manage their XTM appliances as part of one console.

Choice

Extensible choice speaks to providing complete device flexibility. This means that WatchGuard XTM appliances will have the ability to be configured for optimal deployment in any kind of network or business environment. As well, this means administrators will have the ability to pick and choose security services that best meet their organization's needs. For example, a school administrator may only want firewall and web-content filtering on their XTM, while a business may opt for all security services, minus gateway AV, for their WatchGuard XTM deployment.

Ownership

Extensible ownership revolves around growth-oriented options that yield superior total cost of ownership (TCO) and return on investment (ROI). WatchGuard XTM solutions will continue to support a software upgradeable path, which allows users to upgrade security services, subscriptions and capabilities on the fly, without ever having to swap out hardware. Not only does this extend the life of the appliance, but gives owners more flexibility in determining how they utilize their security investment. As well, WatchGuard is working to ensure XTM appliances have the greatest degree of network systems interoperability. This way, regardless of the network topology mix (Cisco, Juniper or Extreme), WatchGuard XTM appliances will provide maximum interoperability.

The Business and Technical Cases for XTM

For business decision makers, XTM offers an ideal cache of reliable security and superior TCO. XTM allows businesses to utilize mobility, consumer technologies, Web 2.0, and other new business applications in a highly secure manner.

Because of the inherent flexibility found in XTM, these solutions will help businesses address the needs of regulatory compliance and future changes that are bound to come.

With greater networking and security capabilities, XTM solutions also eliminate the costly need to purchase and manage multiple routing and stand-alone security appliances. For example, small businesses that currently purchase low-end routers and then supplement them with firewall devices will be able to use a single XTM device for both routing and security. Likewise, instead of utilizing separate appliances, such as a spam firewall, web application filter, and IDS/IDP solution, with XTM businesses can utilize all of these services in one device. This makes the cost of XTM acquisition, as well as the cost of management, much lower than traditional best-of-breed, stand-alone appliances.

For technical decision makers, XTM offers greater management, real-time user control and superior security. As the network perimeter changes and users pass through network, web and messaging platforms, administrators will look to XTM appliances to provide “common reputation services” so that regardless of the device or location, the user and data are always protected. XTM will offer administrators new capabilities in “policy migration” as well. This way, as older appliances such as firewalls are replaced, newer devices can extend and enforce existing security policies.

Finally, technical decision makers who are not security experts will be able to rest assured, knowing that their networks are highly protected with proactive, XTM-based security. The intelligent layered security architecture from WatchGuard offers an unmatched array of security technologies, designed to protect against unknown, “zero day” threats.

Conclusion

XTM is the next generation of UTM, and it is predicated upon the substantive expansion of three foundational elements: more security, greater networking capabilities, and more management flexibility. From this foundation, WatchGuard adds to extensibility by offering: extensible protection, extensible management, extensible choice, and extensible ownership. Although the changing landscape of business dynamics and technology developments has created new efficiencies and accelerated business opportunities, these carry with them new forms of sophisticated threats and risks. The current state of UTM will not be enough to address these changes, hence the need for the next generation of UTM – WatchGuard XTM solutions.

For more information about WatchGuard XTM security solutions, visit us at www.watchguard.com, or contact your reseller.

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 unified threat management (UTM) solutions provides the best combination of strong, reliable, multi-layered security with the best ease of use in its class. Our newest product line – the WatchGuard SSL – makes secure remote access easy and affordable, regardless of the size of your network. All products are backed by LiveSecurity Service, a ground-breaking support and maintenance program. 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.

Part. No. WGPE66567_072408

MEETING PCI DSS MERCHANT REQUIREMENTS WITH A WATCHGUARD® FIREBOX®

FEBRUARY 2008

Introduction

Over the past few years there have been several high profile security breaches that have resulted in the loss of credit information and individual account data for millions of credit card users, including:

- June 2005 – a hacker infiltrates the network of CardSystems Solutions Inc. and accesses potentially 40 million credit card numbers retained by a company that processed payment data for MasterCard International Inc. and other companies.[1]
- January 2007 – an unauthorized intrusion into the computer systems that process and store information related to customer transactions of the TJX Companies, Inc., results in the theft of at least 45.7 million credit and debit card numbers.[2, 3]

The goal of the Payment Card Industry Data Security Standard (PCI DSS) is to create a framework for good security practice around the handling of cardholder data. A PCI-compliant operating environment is one in which the cardholder data exists (i.e., it does NOT refer to the whole corporate network), and PCI DSS defines the requirements for how access to this data must be controlled, monitored, logged, and audited.

---

[1] *40M credit cards hacked; Breach at third party payment processor affects 22 million Visa cards and 14 million MasterCards*, July 27, 2005, Jeanne Sahadi, CNN/Money.
[2] *Retailer TJX reports massive data breach Credit, Debit data stolen. Extent of breach still unknown*, January 17, 2007, Paul F. Roberts, Info
[3] *TJX breach involved 45.7m cards, company reports*, March 28, 2007, Jenn Abelson, The Boston Globe

The objective of this white paper is to clearly outline how firewall deployment impacts meeting PCI DSS standards a for a PCI DSS merchant. Tables include a description of each PCI DSS standard and then show how the WatchGuard Firebox family of appliances achieves these requirements.

Please note that the steps required for a company to achieve PCI DSS compliance vary based on that company's architecture; it is not possible to identify a single, "generic" network solution and Firebox configuration for achieving PCI DSS compliance.

PCI DSS Overview

The potential for loss from security breaches prior to the recent high profile incidents was well recognized by each of the major credit card vendors, who responded by creating their own information security programs:

- Visa Card Information Security Program
- MasterCard Site Data Protection
- American Express Data Security Operating Policy
- Discover Information and Compliance
- JCB Data Security Program

Each company's intentions were roughly similar: to create an additional level of protection for customers by ensuring that merchants meet minimum levels of security when they store, process, and transmit cardholder data.

In 2004, the credit card companies came together and the Payment Card Industry Security Standards Council was formed to align their individual policies and create the Payment Card Industry Data Security Standard (PCI DSS) in December 2004. In September, 2006, the PCI standard was updated to version 1.1 to provide clarification and minor revisions to version 1.0.[4]

The goal of PCI DSS is to create a framework for good security practice around the handling of cardholder data. It does *not* define the security requirements for your whole IT infrastructure

PCI DSS applies to every organization that processes credit or debit card information, including merchants and third-party service providers that store, process, or transmit credit/debit card data. Any company involved in processing, storing, or transmitting credit card numbers ***must*** be compliant with the standard or risk losing the ability to process credit card payments, as well as risk being fined for violations up to $100,000 per incident. It's not enough to simply make a statement confirming compliance; merchants and financial institutions must have their compliance status validated by outside vendors who are a certified PCI DSS Qualified Security Assessor (QSA).

Merchants and Merchant Levels

For PCI DSS, a merchant is defined as any company that accepts credit or debit cards in exchange for goods or services. Merchants are categorized into one of four levels, based on the transaction volume. The higher the transaction volume a company has, the greater the impact of a security breach is likely to be, warranting tighter security requirements. As a result, the higher the credit card transaction volume a merchant organization has, the more stringent the requirements are for achieving PCI DSS compliance.

For Level 1 merchant organizations, compliance is achieved by undergoing an annual on-site security audit, quarterly network scans and validation by a qualified security assessor (QSA) and approved scanning vendor (ASV). Level 2 and 3 merchants must comply with the PCI DSS Self Assessment Questionnaire and undergo a

[4] http://en.wikipedia.org/wiki/PCI_DSS

quarterly network scan, which must be validated by both the merchant and an ASV. For Level 4 merchant, it is recommended that the organization comply with the PCI DSS Self Assessment Questionnaire and to have an annual network scan. Note that for a Level 4 merchant, if a breach has been reported or found, VISA reserves the right to move the Level 4 merchant to a Level 1. If so, the Level 4 merchant must abide by the Level 1 validation requirements. Hence, Level 4 merchants are strongly encouraged to consider the PCI DSS-recommended actions as mandatory.

PCI DSS Merchant Levels

Level	Description
1	• Any merchant processing over 6,000,000 transaction per year • Any merchant that has been involved in a hack or attack that caused a data disclosure • Any merchant that PCI determines should be at Level 1 to minimize risk to cardholder data
2	Any merchant processing 1,000,000 to 6,000,000 transactions per year
3	Any merchant processing 20,000 to 1,000,000 e-commerce transactions per year
4	• Any merchant processing fewer than 20,000 e-commerce transactions per year • All other merchants, regardless of acceptance channel, processing up to 1 million transactions per year

Fines Associated with Non-Compliance

ALL of the deadlines for meeting PCI DSS have passed, which means that **ANY** merchant that does not comply with the standard is at risk of being fined. Visa USA has announced that it will start fining banks that process merchant transactions (which will pass the costs on to the merchant) between $5,000 and $25,000 per month if their Level 1 or 2 merchants have not demonstrated compliance. In addition, the fines of $10,000 per month may already be assessed today for prohibited data storage by a Level 1 or Level 2 merchant.

Companies that are not yet compliant will be fined up to $500,000 by the card brand companies if compromised, not including any civil liabilities (which typically dwarf this amount). Any company still in business and needing to continue transaction after such a compromise will automatically "restart" at Level 1 status, making future achievement of compliance significantly more expensive.

PCI DSS Compliance and Requirements Overview

In order to achieve PCI DSS compliance, a merchant must demonstrate 100% conformance with the requirements of the standard, but being compliant today does not mean indefinite compliance. To ensure that a PCI-compliant merchant is able to incorporate new technologies and to respond to new ways of hacking personal data, there are continuing auditing responsibilities that must be undertaken to retain PCI DSS compliance.

There are 12 requirements that must be satisfied in order to achieve compliance, addressing the technologies, policies, and procedures that must be in place. The requirements are organized into six main control objectives**:**

- **Build and Maintain a Secure Network**
    - Requirement 1: Install and maintain a firewall configuration to protect cardholder data
    - Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

- **Protect Cardholder Data**
  - Requirement 3: Protect stored cardholder data
  - Requirement 4: Encrypt transmission of cardholder data across open, public networks
- **Maintain a Vulnerability Management Program**
  - Requirement 5: Use and regularly update anti-virus software
  - Requirement 6: Develop and maintain secure systems and applications
- **Implement Strong Access Control Measures**
  - Requirement 7: Restrict access to cardholder data by business need-to-know
  - Requirement 8: Assign a unique ID to each person with computer access
  - Requirement 9: Restrict physical access to cardholder data
- **Regularly Monitor and Test Networks**
  - Requirement 10: Track and monitor all access to network resources and cardholder data
  - Requirement 11: Regularly test security systems and processes
- **Maintain an Information Security Policy**
  - Requirement 12: Maintain a policy that addresses information security

Breeding a "Culture of Security"

Take the PCI DSS conformance out of the equation for a moment and ask yourself, "Do we have a culture of security within our organization?" What this means is:

1) Do we educate and train each other on best security practices for our business?
2) Do we have a security policy that is up-to-date, that people are aware of, and do we have a way to review it, change it as needed, and to enforce it?
3) Do we have the controls – be they policy-driven, technical, or whatever – to be able to make sure that we stay compliant within the policy that we've created?

If you have those factors, you have a security culture – and when you have a security culture, regardless of the regulatory or industry compliance standards you have to meet, you're going to have a sound framework from which you can adapt to them.[5]

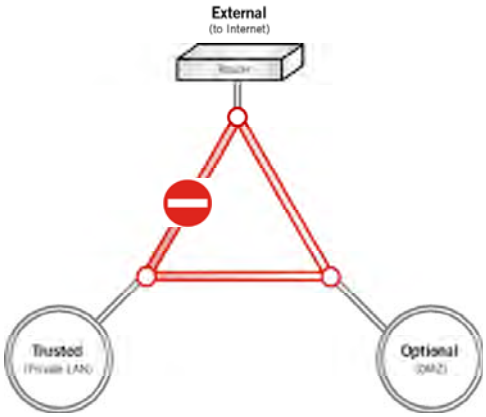
There's No Such Thing as "Certified PCI DSS Compliant"

Where firewalls are concerned, there is no product that is going to be "certified PCI DSS compliant." It's just a myth. Any network firewall, and by extension a unified threat management (UTM) appliance that combines a network firewall with other features (such as anti-virus and intrusion prevention services), can be a part of *becoming* compliant, but it's only going to cover a certain portion of the compliance requirements.

For companies seeking PCI DSS compliance, it is important to design a network with appropriate physical and logical boundaries to segregate the PCI-compliant operating environment. The PCI DSS monitoring scope must also be made manageable. To this end, the strong segregation capability available with the application proxy technology of the WatchGuard® Firebox® X family of UTM appliances is ideally suited to meeting these requirements.

[5] *Cutting through Compliance Clutter*, February 2008, WatchGuard Radio Free Security interview Chris Squier, CISSP.

Zoned Networks



All Firebox appliances support the zoned network architecture for creating a Demilitarized Zone (DMZ), as required by PCI DSS. In this architecture, only the servers contained within the DMZ are accessible from the Internet, and the cardholder data is contained within the Trusted network zone. As required by PCI DSS, WatchGuard application proxy technology provides detailed control over the traffic that passes between network zones. This enables administrators to block all traffic by default and to define which traffic is allowed to pass from one zone to the next, including protocols, ports, content (e.g., MIME types, file types, and URLs) and verbs (e.g., HTTP GET). Via this architecture, communication between the Trusted zone and the Internet can be completely prohibited, and those between the Trusted and DMZ zones can be strictly limited to traffic that meets the PCI DSS and corporate communication requirements.

Beyond supporting the required network architectures, there are strong logging, monitoring, and auditing component required by PCI DSS, all of which are supported by WatchGuard Firebox appliances. In addition, the security subscriptions available for all WatchGuard Firebox appliances – including Gateway AntiVirus/ Intrusion Protection Service, WebBlocker, and spamBlocker – are a perfect complement to PCI DSS standards.

Compliance with the PCI DSS standards can only be achieved via a combination of PCI DSS operating environment network architecture (including firewall deployment) and security practices, procedures, and policies. Compliance can only be granted via independent assessment by a Qualified Security Assessor (QSA). As a result, it is not possible to define a single recipe for achieving compliance.

PCI DSS Requirements Impacted by Firebox Deployment

The tables below list PCI DSS requirements that a Firebox deployment addresses. This is not a complete set of the PCI DSS requirements; those that cannot be addressed by a Firebox deployment have not been included. The comments explain how a WatchGuard Firebox appliance complements each requirement.

Note: PCI DSS Requirement sections 3, 7, 9 and 12 are not included in these tables as they do not affect a network firewall deployment.

1. Install and maintain a firewall configuration to protect cardholder data

Req #	Requirement Details	Comments
1.2	Build a firewall configuration that denies all traffic from "untrusted" networks and hosts, except for protocols necessary for the cardholder data environment.	The Firebox proxy architecture is ideal for meeting this requirement. The proxy architecture provides detailed granular control over which protocols, ports, and content are allowed through the firewall. This is achieved by blocking all traffic by default and defining a proxy policy that allows only approved traffic to pass into the PCI DSS operating environment. The Firebox IPS and AV services can also be used to scan the allowed traffic to monitor for threats from malware or unauthorized intrusion attempts.
1.3	Build a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks. This firewall configuration should include items 1.3.1 through 1.3.8 below.	Using a zoned network architecture such as the one described in the Introduction, WatchGuard Firebox family of firewalls can be configured so that traffic from the Internet into the public-facing servers in the DMZ, and from the DMZ into the Trusted zone is restricted to only approved traffic types.

1.3.1	Restricting inbound Internet traffic to Internet protocol (IP) addresses within the DMZ (ingress filters)	Using the zoned network architecture described above, Firebox appliances can be configured so that the only IP addresses that are accessible from the Internet are contained within the DMZ. The same configuration can be used to ensure that none of the IP addresses in the Trusted zone are visible or accessible from the Internet.
1.3.2	Not allowing internal addresses to pass from the Internet into the DMZ	This requirement refers to blocking any traffic from the Internet that has an RFC1918 IP address (i.e. IP addresses in any of the following ranges 10.0.0.0/32, 172.16.0.0/20 or 192.168.0.0/16) from entering the DMZ. Fireboxes can be configured to ensure that communication coming from the Internet from any RFC1918 IP address is blocked.
1.3.3	Implementing stateful inspection, also known as dynamic packet filtering (that is, only ”established” connections are allowed into the network)	The objective of this requirement is to ensure that only traffic that is part of a legitimately established TCP/IP connection passes through the firewall, which is a basic approach to detecting and preventing malicious intrusion attempts. Firebox appliances include stateful inspection firewalls and other technologies, such as Protocol Anomaly Detection and Intrusion Prevention Services that can be used to meet or exceed the objectives of this requirement.
1.3.5	Restricting inbound and outbound traffic to that which is necessary for the cardholder data environment	The Firebox proxy architecture provides detailed granular control over which protocols, ports and content are allowed through the firewall. The Firebox IPS and AV services can also be used to scan the allowed traffic to monitor for threats from malware or unauthorized intrusion attempts.
1.3.6	Securing and synchronizing router configuration files. For example, running configuration files (for normal functioning of the routers), and start-up configuration files (when machines are re-booted) should have the same secure configuration	This requirement only affects a Firebox if used as primary router. If this is the case, then the WatchGuard System Manager may be used to define and deploy a synchronized configuration to each Firebox.
1.3.7	Denying all other inbound and outbound traffic not specifically allowed	The Firebox proxy architecture is uniquely able to fulfill the objectives of this requirement by creating detailed policies that define only the traffic that is allowed into and out of the network. All other traffic is blocked.
1.3.8	Installing perimeter firewalls between any wireless networks and the cardholder data environment, and configuring these firewalls to deny any traffic from the wireless environment or from controlling any traffic (if such traffic is necessary for business purposes)	If a Firebox X Edge appliance is used as the wireless access point, the wireless network can be isolated from both the DMZ and Trusted network zones.
1.4	Prohibit direct public access between external networks and any system component that stores cardholder data (for example, databases, logs, trace files).	The requirements in section 1.4 relate specifically to the use of zoned network architecture to segregate cardholder data so as to ensure that it cannot be accessed directly via the Internet. WatchGuard Firebox appliances support network zones, and they can be configured to create a DMZ for all public-facing servers and a Trusted zone where the cardholder data resides. They can also be configured to ensure that no traffic can pass from the Internet into the Trusted zone, or vice versa. All traffic to and from the Internet therefore has to go via the public servers in the DMZ, with the Firebox configured to ensure that all traffic from the Trusted zone to the Internet is blocked, ensuring that all external traffic comes from the IP addresses in the DMZ.
1.4.1	Implement a DMZ to filter and screen all traffic and to prohibit direct routes for inbound and outbound Internet traffic	
1.4.2	Restrict outbound traffic from payment card applications to IP addresses within the DMZ.	
1.5	Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet. Use technologies that implement RFC 1918 address space, such as port address translation (PAT) or network address translation (NAT).	Network Address Translation (NAT) is a standard feature in all Firebox appliances.

2. Do not use vendor-supplied defaults for system passwords and other security parameters

The "system" referred to in this requirement is the whole PCI DSS environment and it encompasses databases, endpoints, network infrastructure, etc. The idea is to essentially ensure that it is not possible for a system to be compromised by anyone who is able to identify the system components and try the default passwords for the devices used. Password management for Firebox appliances is easily achieved via the management interface.

2.2.2	Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function)	Firebox appliances' proxy architecture provides detailed granular control over which protocols, ports, and content are allowed passage through the firewall. This is achieved by blocking all traffic by default and defining a proxy for those specific protocols that are allowed. The Firebox IPS and AV services can also provide security for those protocols that are allowed.
2.3	Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS (transport layer security) for web-based management and other non-console administrative access.	All management communications with Firebox appliances are done via a secure encryption-based protocol.

4. Encrypt transmission of cardholder data across open, public networks

4.1	Use strong cryptography and security protocols such as secure sockets layer (SSL) / transport layer security (TLS) and Internet protocol security (IPSec) to safeguard sensitive cardholder data during transmission over open, public networks. Examples of open, public networks that are in scope of the PCI DSS are the Internet, Wi-Fi (IEEE 802.11x), global system for mobile communications (GSM), and general packet radio service (GPRS).	All e-Series Firebox appliances running Version 10 firmware support IPSec and SSL VPN communication.
4.1.1	For wireless networks transmitting cardholder data, encrypt the transmissions by using Wi-Fi protected access (WPA or WPA2) technology, IPSec VPN, or SSL/TLS. Never rely exclusively on wired equivalency privacy (WEP) to protect confidentiality and access to wireless LAN. If WEP is used, do the following: • Use with a minimum 104-bit encryption key and 24 bit-initialization value • Use ONLY in conjunction with Wi-Fi protected access (WPA or WPA2) technology, VPN, or SSL/TLS • Rotate shared WEP keys quarterly (or automatically if the technology permits) • Rotate shared WEP keys whenever there are changes in personnel with access to keys • Restrict access based on media access code (MAC) address	Wireless networks are inherently insecure, but there are some circumstances where they cannot be avoided. In these cases, the standard requires that the wireless operating environment be physically segregated from the wired environment and appropriately firewalled. When a Wi-Fi solution must be used, the Firebox X Edge supports WPA2 and can be combined with either an IPSec or SSL VPN to achieve the objectives of this requirement.

5. Use and regularly update anti-virus software or programs

5.1.1	Ensure that anti-virus programs are capable of detecting, removing, and protecting against other forms of malicious software, including spyware and adware	All Firebox appliances provide Gateway AntiVirus support that serve to reduce the ingress of malware into the network, helping to meet the objectives of this requirement.
5.2	Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.	All Firebox appliances provide automatic updates of the Gateway AntiVirus signature database, helping to meet the objectives of this requirement. In addition, the appliance Logs are updated whenever traffic is denied by the Gateway AntiVirus and whenever the signature sets are updated.

6. Develop and maintain secure systems and applications

6.1	Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.	WatchGuard LiveSecurity® Service gives you access to updates and enhancements for Firebox products, including minor software patches and new software versions.
6.2	Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update standards to address new vulnerability issues.	WatchGuard LiveSecurity Service Rapid Response Team, a dedicated group of network security experts, monitors the Internet to identify emerging threats, then delivers LiveSecurity Service alerts that describe what can be done to address each new menace.
6.6	Ensure that all web-facing applications are protected against known attacks by applying either of the following methods: • Having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security • Installing an application layer firewall in front of web-facing applications Note: This method is considered a best practice until June 30, 2008, after which it becomes a requirement	This requirement specifically addresses the potential vulnerabilities in applications accessible from the Internet and it refers specifically to the use of web application firewalls to provide a robust mechanism to mitigate application vulnerabilities (e.g., SQL injection, cross site scripting). In combination with a web application firewall, Fireboxes provide an additional layer of protection. The HTTP proxy is a high-performance content filter that examines web traffic to identify suspicious content, which can be a virus, spyware, or other type of intrusion. It can also protect your web server from attacks from the external network.

8. Assign a unique ID to each person with computer access

8.2	In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users: • Password • Token devices (e.g., SecureID®, certificates, or public key) • Biometric	Firebox appliances support authentication via Active Directory, which streamlines authentication, saving time and eliminating hassles.
8.3	Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial- in service (RADIUS) or terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSec) with individual certificates.	Firebox appliances support two-factor authentication, including RADIUS, SecureID, and individual VPN certificates.
8.4	Encrypt all passwords during transmission and storage on all system components.	All management communications with Firebox appliances are done via a secure encryption-based protocol, and Firebox appliances store their password information in an encrypted format.

10. Track and monitor all access to network resources and cardholder data

One of the gray areas of the standard, DSS Requirement 10 should be treated carefully – if misinterpreted, it can have the most significant impact on the effort and costs required to achieve compliance. The basic objective is to ensure that all access to stored cardholder data is logged, but the extended objective is also to ensure that any configuration changes to the network components used to access and/or isolate the stored data are also logged. All log data should be stored and periodically monitored to identify any potential or actual security breaches (either via routine audit/test or actual attack). In the case of a compromise, this data is essential for tracing the cause and identifying the network vulnerability so that it may be remedied.

A PCI-compliant environment should be designed with the appropriate physical and logical boundaries to segregate the PCI-compliant operating environment and to make PCI DSS monitoring scope manageable. Trapping all that can be logged is NOT the point of the monitoring requirement; protection of cardholder data is paramount, and therefore should be the focus of all logging activity.

Practical monitoring of the network for all but the smallest organization is best done using something like a Security Information Management (SIM) solution. These solutions will continually analyze the data logs from the various network components and use data correlation techniques to attempt to identify and alert the system administrator of any security breaches. Key aspects of a PCI DSS-compliant environment to enable meaningful monitoring are:

- Consistent time stamping amongst network equipment for data correlation
- Identity management solution (e.g., Microsoft Active Directory)
- Event management storage (including firewall data, that must be configured to send data to the SIM)

Firewalls are considered to be an infrastructure component, i.e., a carrier and/or handler of cardholder data. As such, they need to be configured to send logs to the SIM. Exactly what data must be logged is not defined in the standard, and this should be determined as a tradeoff between security and business criteria. At the highest level, firewalls need to be able to provide the following:

- Ability to send logs to the SIM, most typically via SNMP
- Compatibility with the chosen identity management solution
- IDS, IPS and antivirus solutions – the actions of which must also be logged
- Wireless networks require special attention as they are fundamentally insecure. Every precaution must be taken to secure against wireless hacks.

10.1	Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	Pertains to being able to trace each login activity to an individual. Per comments above, it is best to use an Active Directory type solution for tracking identity and logging access. All Firebox appliances support authentication via Active Directory.
10.2	Implement automated audit trails for all system components to reconstruct the events listed in 10.2.1 through 10.2.7	When reading the PCI DSS specification to understand the impact on a firewall deployment, it is easy to believe that all of the logging requirements pertain to the firewall also. In reality, these requirements are requirements for the whole PCI DSS operating environment, and if it is possible to capture and log this information elsewhere, then it is not necessary for this information to be logged at the firewall.
10.2.1	All individual user accesses to cardholder data	
10.2.2	All actions taken by any individual with root or administrative privileges	
10.2.3	Access to all audit trails	
10.2.4	Invalid logical access attempts	
10.2.5	Use of identification and authentication mechanisms	
10.2.6	Initialization of the audit logs	
10.2.7	Creation and deletion of system-level objects	
10.3	Record at least the following audit trail entries for all system components for events listed in 10.3.1 through 10.3.6	For a firewall deployment, this requirement pertains to ensuring that any configuration changes to the network components used to access and/or isolate the stored data are logged. All Firebox appliances will log user login and configuration changes, including the user name and IP address of the machine from which the login was initiated.
10.3.1	User identification	
10.3.2	Type of event	
10.3.3	Date and time	
10.3.4	Success or failure indication	
10.3.5	Origination of event	
10.3.6	Identity or name of affected data, system component, or resource	

10.4	Synchronize all critical system clocks and times.	All Fireboxes support NTP synchronization.
10.5	Secure audit trails so they cannot be altered.	This can be achieved in by either configuring the Firebox to send log data to a SIM via SNMP, or by using the Firebox logs in their raw form. If the Firebox logs are used, then the Log server must be on a secure machine (interaction with the Firebox is secure). Firebox appliances also support sending log data to syslog servers, but this is not recommended as this is not a secure solution.
10.5.4	Copy logs for wireless networks onto a log server on the internal LAN.	If Firebox X Edge wireless access points are used, this is achievable by using WatchGuard Log server.
10.6	Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS). Note: Log harvesting, parsing, and alerting tools may be used to achieve compliance with Requirement 10.6.	WatchGuard Log Viewer can be used to search Firebox appliance logs sent to the WatchGuard Log server for specific event types.

11. Regularly test security systems and processes

11.4	Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up-to-date.	Firebox Intrusion Prevention Service (IPS) security subscription can be used to address this requirement. While it is not recommended that the Firebox IPS solution be the only IPS system deployed in the network, use of the Firebox IPS is a great complement to addressing this requirement.

Summary

Any company that accepts credit or debit cards in exchange for goods or services must already be compliant with the PCI DSS requirements. As of June 30, 2008 all web-facing applications must also be protected by a web application firewall.

The keys to achieving PCI DSS compliance are:

- Fostering a culture of security within the organization
- Designing, deploying, and maintaining a secure networking infrastructure, a necessary component of which is a firewall.

While the notion of a “PCI DSS-compliant”firewall is a myth, application proxy-based firewalls are particularly well suited to meeting the requirements of the standard.

In particular, the PCI DSS standard requires a zoned network architecture where all traffic into the trusted portion of the network is blocked by default so that only the specific protocols, ports, and content allowed by the corporation’s security policy are allowed to pass into the Trusted zone. Implementing and securing this type of network architecture is exactly what an application proxy-based firewall is ideally suited for.

Compliance with the PCI DSS standards cannot be achieved by the deployment of a single network component. It can only be achieved via a combination of PCI DSS operating environment network architecture (including firewall deployment) and security practices, procedures, and policies. As a result, it is not possible to define a single recipe for achieving compliance.

The WatchGuard Firebox X family of UTM products is ideally suited to building and maintaining a PCI DSS-compliant network environment thanks to the strong segregation capability available with the built-in application proxy technology. For more information about our powerful network security solutions, visit us at www.watchguard.com or contact your reseller.

WatchGuard provides a useful, no-nonsense guide to establishing a strong network security policy. For your free copy, visit www.watchguard.com/infocenter/whitepapers/security_policy.asp.

References

1. www.pcicomplianceguide.org
2. PCI Compliance: Understand and Implement Effective PCI Data Security Standard Compliance, June 2007, Tony Bradley, et al
3. *Payment Card Industry (PCI) Data Security Standard, Version 1.1*, September 2006, PCI Security Standards Council (www.pcisecuritystandards.org)
4. *Cutting Through Compliance Clutter*, February 2008, WatchGuard Radio Free Security interviews Chris Squier, CISSP

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 unified threat management (UTM) solutions provides the best combination of strong, reliable, multi-layered security with the best ease of use in its class. All products are backed by LiveSecurity Service, a ground-breaking support and maintenance program. 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.

Part. No. WGAG66504_011209

TRUE ZERO DAY PROTECTION

The Only Defense Against Evolving Security Threats

March 2008

Abstract

Zero day attacks are a growing threat to corporate networks, because they pass undetected through conventional signature-based defenses. Many, if not most, systems are vulnerable to these attacks. The actual number of infections is staggering, and dealing with them burdens IT departments and impacts corporate bottom lines. The corporate losses are the criminals' gains, as compromised systems feed an underground cyber-economy worth millions and millions of dollars. Rather than relying solely on signatures, businesses need a security strategy that also includes protection from zero day attacks. This white paper explains the mechanisms of zero day threats and shows how the WatchGuard approach of combining application proxy firewall and intelligent layered security provides fundamentally stronger protection for business networks.

Introduction

A corporate user clicks on a link in an email, taking him to a web site. The site serves up a deliberately corrupted media file that contains a snippet of program code. Within seconds, the user's computer is taken over by a criminal and is sending spam emails all over the Internet.

This is just one example of a zero day attack. A zero day attack is an attempt to exploit a vulnerability in computer software or equipment, before that vulnerability has been disclosed and a specific preventive measure exists. Zero day protection, therefore, is the ability to block such a threat, even though the exact mechanisms of the attack are unknown.

"Black hat" hackers are becoming incredibly sophisticated at finding new vulnerabilities and exploiting them before the security community can react. It can take less than a second to compromise a single machine. A zero day worm that exploits a previously undiscovered but widely prevalent security hole can propagate across hundreds of thousands of Internet-connected machines within a few hours. Consider the following examples:

> **Code-Red worm, July 19, 2001.** More than 359,000 computers were infected in less than 14 hours. At the peak of the outbreak, more than 2,000 new hosts were infected each minute.[1]
>
> **SQL Slammer, July 25, 2003.** At least 75,000 machines were infected, 90 percent of them within the first ten minutes.[2]
>
> **Storm Worm, January 2007.** Storm spawned a "botnet" of remotely controlled zombie machines, each capable of spreading constantly mutating infections to others through various means. In effect, each variant represented a new zero day attack. By year's end, one source estimated the botnet's size at over 1.8 million infected computers worldwide.[3] The Storm botnet remains a highly active, virulent, and worrisome threat.

True zero day protection has to work from day zero, hour zero, minute zero.

Conventional Defenses and the Zero Day Threat

Most security vendors build their detection strategies around signatures, which are essentially the "fingerprints" of the computer code used to launch an attack. While signatures are a useful element of defense, *any scheme that relies on signatures alone cannot claim to offer true zero day protection.*

The moment an exploit has been released into the wild, security companies that rely on signatures are in a race to obtain samples, build a signature, then test, package, and distribute it. The time from the first attack until the end users have installed the protective signature is termed the "window of vulnerability."

In the best-case scenario, creating and testing a signature can take hours. Fully closing the window by installing the signature can take days, and depends ultimately on the vigilance of end users. However:

- The most virulent Internet worms spread in minutes, not hours or days
- Malware authors have learned how to make their code self-mutating, requiring constant development of new signatures
- Criminals have learned that if their efforts fly under the radar, they can delay discovery of the vulnerability and avoid signature-based security entirely

The Computer Security Institute, which publishes an annual report on the state of network security, concluded in its report for 2007 that given the evolving state of malware, reliance on signatures was leaving defenses "increasingly permeable."[4]

Zero Day Threats: The Harsh Realities

The popular image of a hacker is a teenager, holed up in his bedroom at his parents' home, launching attacks so he can brag about them to his online hacker buddies. Sorry to say, the black hats have grown up. They are organized gangs. They hide behind an array of ever-changing Internet addresses to elude detection, and many work out of foreign countries.

Means, Motive … and Plentiful Opportunities

The potential for zero day attacks lurks everywhere. The National Vulnerability Database, sponsored by the Department of Homeland Security's National Cyber Security Division, listed more than 29,000 Common Vulnerabilities and Exposures (CVEs) as of January 2008. This database is a comprehensive library of vulnerabilities uncovered by "white hat" security researchers. On average, there are 15 new CVEs added per day.[5]

From web browsers and media players to office applications and corporate databases, nearly every type of application has been revealed to have some vulnerability. How do the black hats take advantage of them to compromise machines? Here are some common avenues:

- **Tricking users into opening executable files** masquerading as other file types, sent via email or instant messaging
- **Directing users to visit web sites** that spread infections (drive-by downloads)
- **Sending carefully crafted documents** that contain executable code, taking advantage of application vulnerabilities that allow the code to run (buffer overflow attacks)

For the small to medium-size enterprise (SME), one new hacker technique is especially alarming – the use of personal information, often found on social networking sites, to target individuals within the organization. Vulnerabilities in common office applications allow attackers to send infected documents, seemingly of business value, with enough insider information to prompt the target to open them. In one survey, 32% of respondents said they had experienced a targeted attack directed at their industry or their organization.[6]

Quantifying the Risk

Compromised machines aren't just theoretical. They're a reality. The Microsoft Spyware Removal tool removed malware from more than 8 million computers during the first half of 2007. The infection rate had more than doubled compared to 2006.[7]

ShadowServer, an all-volunteer group of security professionals, tracks botnet activity. As of January 2008, they were tracking more than 2,000 command-and-control servers controlling more than 200,000 zombie machines owned by unsuspecting users.[8] Symantec reported that during the first half of 2007, more than 5 million distinct computers became bot-infected at some point.[9]

No business, regardless of size, is immune. A 2007 survey of security practitioners representing organizations of every size revealed that:[10]

- 52% reported virus incidents
- 25% experienced denial-of-service (DoS) attacks
- 21% uncovered bots within the organization
- 13% detected system penetration
- 10% reporting password sniffing
- 10% suffered web site defacement
- 06% encountered an exploit of their organization's DNS server

This survey was skewed to a population that is more security conscious than the norm. It is likely that the numbers are even higher at organizations that adopt a "see no evil, hear no evil" approach.

Costs and Impacts

The expense in time required to clean infected machines is immense. There are no automated tools or documented steps for cleanup after a zero day attack. Especially when hackers use rootkit techniques, which bury the evidence of their work deep within the operating system, the smartest course is usually to reinstall the operating system and restore files from the last successful backup.

In the meantime, workplace productivity suffers. In one survey, over a six-month period more than one in four users reported their productivity was impacted by an infection, with productivity declines between 21 and 32 percent.

Even more alarming, those users on average waited more than 18 working hours to have the infection repaired.[11] The legal liability for companies harboring infected machines on their networks is an emerging area of law. It is a special concern when those machines contain or access confidential data.

What Do the Black Hats Want?

An entire underground economy has risen around compromised machines. Access to "owned" servers, services for launching "phishing" schemes, rental botnets for spam runs, and malware creation services are all advertised for a fee. These in turn support a marketplace for stolen identities, compromised bank accounts, and credit card numbers. One study tracked activity on an underground server and found more than $1.5 million in transactions over a 24-hour period in one trading channel alone.

To service this underground economy, the hacker is usually not after the data on the computer, but the computer itself and the ability to control it. It could be used as a platform for launching attacks on other, higher-value computers. Or more likely, the aim is to add the computer to a botnet, as a tool for all kinds of criminal schemes.

Hackers have become incredibly sophisticated at hiding their tracks, and typically the only visible sign that a machine has been compromised is a slight slowdown. If the exploit is successful, a hacker can have control of the machine in milliseconds. Typically, the first step after gaining control is to patch the machine's vulnerabilities to improve its security posture. The hacker isn't doing the victim any favors; simply securing ownership by locking out the competition.

Mounting an Effective Defense

Zero day attacks that routinely bypass signature-based detection are especially valuable to the criminal hacker. WatchGuard firewalls enforce security in an entirely different way. Signatures are a secondary element of a multi-layered defense. The twin pillars of WatchGuard's zero day protection strategy are:

- Application proxy firewall
- Multi-faceted detection strategy termed *intelligent layered security*

Understanding how these defenses work separately and in concert is the key to understanding how true zero day protection can be achieved.

Application Proxy Firewall

WatchGuard was an industry pioneer in implementing application proxy technology in a firewall appliance. Even though there are hundreds and hundreds of firewall vendors, WatchGuard remains one of the handful that use an application proxy.

The Traditional Approach: Packet-Based Firewalls

The first firewalls were deployed at large enterprises that needed to handle large amounts of traffic. These first firewalls were packet filters. Packet filters do not process packets as intensively as an application proxy, so they are simpler to design and inherently faster. Despite advances in hardware and processing speed, well-known firewall vendors still rely on their legacy packet-based designs.

To understand a packet filter, consider a packet: a set of data bytes, assembled into a compact bundle for routing over the Internet. Each packet begins with a header that contains information about the contents including:

- Internet address of the sender
- Internet address of the recipient
- Protocol being used
- For most protocols, a port number that the receiving computer uses to direct the packet to the correct application

A packet filter firewall looks at the information in the header. It checks the source, destination, protocol, and port number and if the combination is allowed, it forwards the packet. Most home routers contain packet filter firewalls.

Stepping Up Security: Stateful Inspection and Signatures

A stateful inspection firewall is a packet-based firewall that doesn't just look at the packets individually, but understands what a correct sequence of packets should look like. It understands the state of each connection, and drops packets that are out of logical sequence. Most business-class firewalls are of the stateful inspection type.

For added protection that looks at the data within each packet, some firewall vendors depend on signatures alone. This reactive approach is flawed in dealing with zero day attacks because:

- A signature is written after the exploit is known, which could take anywhere from hours to weeks, or perhaps never if the exploit is uncommon
- Until a signature is applied, systems are highly vulnerable as there is no secondary defense; security is only as strong as the last signature update
- Many end users take an “if it ain’t broke, don’t fix it” approach to critical network components such as firewalls, and do not patch and update them regularly

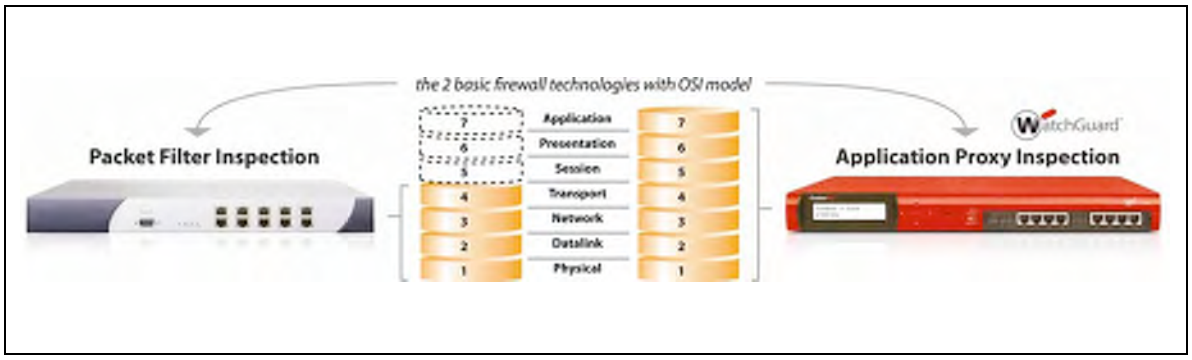
Taking a Deeper Look: Application Proxy Firewall

While packet filters look for bad things and filter them out, application proxy firewalls take the opposite approach. They are designed to recognize good traffic, allow it, and block everything else. This approach blocks whole classes of attacks. As one simple example, a number of FTP servers have vulnerabilities associated with the DELE (delete) command, which could lead to outside control of the machine. The WatchGuard application proxy does not recognize use of the DELE command as legitimate traffic – in fact, it protected against those attacks years before specific vulnerabilities were even known.

To obtain this level of protection, an application proxy firewall doesn't simply look at the packet as it flies by. It disassembles the packet, rebuilds and re-sends it. It is called a “proxy” because it handles the connections on behalf of the source and destination machines. At the endpoints, the session proceeds as though each machine is communicating directly with the other. In fact, each is communicating with the firewall.

An application proxy is more processor-intensive than a packet-based firewall. Delivering the benefit of an application proxy with full-speed network performance calls for more than brute-force processing. It requires strategic design. (See *Intelligent Layered Security*, next section.)

The critical security difference between a packet-based and application proxy firewall is easily understood by looking at the seven-layer OSI model. The OSI model is fundamental to modern networking, and governs how data is packaged. A packet inspection firewall can only take action based on the first three layers of the model. A stateful inspection firewall adds the transport layer. An application proxy firewall has the capability to inspect all seven layers and take action based on the topmost application layer, where most zero day threats reside.



An application proxy makes decisions based on information that packet-based firewalls do not even consider. This includes checks such as:

- Is the packet formatted properly for this protocol?
- Does it contain unknown types of content that could be malicious (.exe files, .scr files, other executable types – even if they have been renamed)?
- Does it contain non-ASCII characters?
- Does it contain dangerous commands?
- Is the amount of data too long for this protocol?
- Does the pattern suggest a potential attacker looking for information about internal systems?

Most significantly, the WatchGuard proxy checks for and validates compliance with Internet standards for the protocol being used (RFC compliance). Whole classes of vulnerabilities, such as buffer overflow attacks, violate standards in some way and the application proxy eliminates the need for many signature checks by enforcing compliance.

The WatchGuard proxy's understanding of applications and protocols is so thorough that if a packet contains benign abnormalities that aren't a security concern, it can rebuild the packet to proper specification before sending it on.

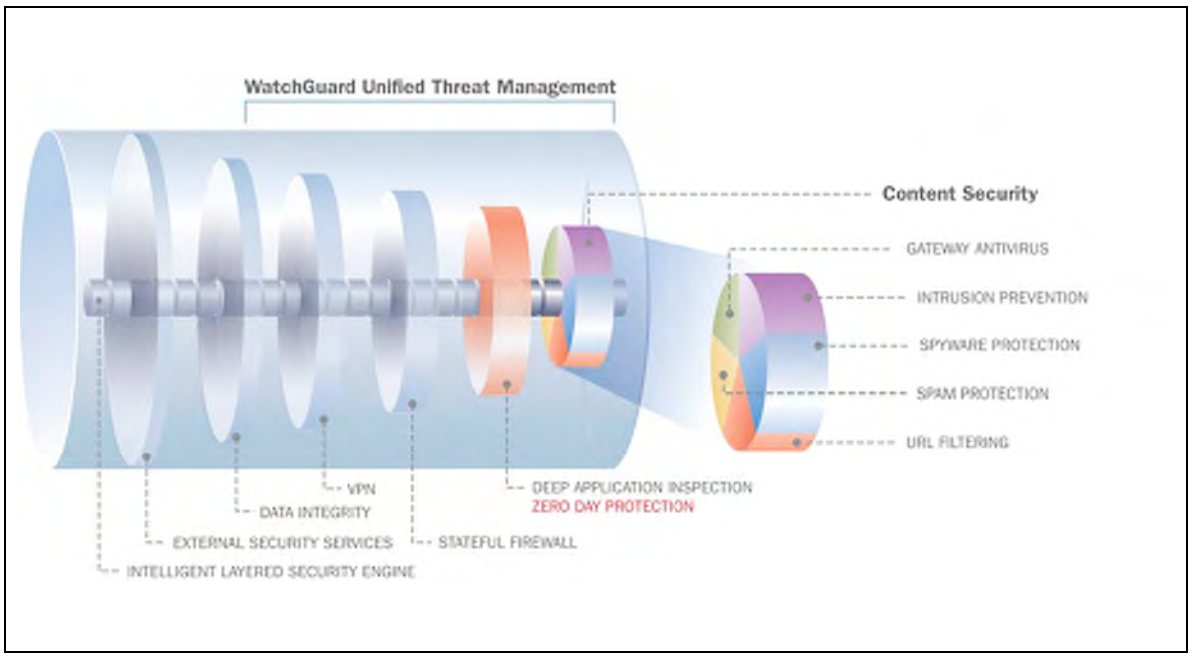
Intelligent Layered Security

Typically, packet-based firewalls check for simple anomalies in the headers or connection, test against a set of signatures, and forward the packet. With a WatchGuard firewall, each connection and packet goes through a series of checks, beginning with the simplest checks first, working from the bottom to the top of the seven-layer OSI model. Any check can strip or modify pieces of the packet, or deny or drop it to eliminate the need for further processing. For the few malicious packets that can survive the gauntlet, signatures at the application layer mop them up.

The intelligent layered security approach allows a WatchGuard firewall to deliver the full zero day protection of an application proxy, with limited impact on network performance. Depending on the port and protocol, only a few checks are needed for most packets. Just a small percentage call for the full scrutiny of layer-seven inspection, augmented by WatchGuard signatures.

The WatchGuard signatures capture specific threats carefully crafted by the black hats to masquerade as benign traffic. For traffic leaving the network, signatures are used mainly to detect and block traffic from machines infected with spyware or bot software, sending rogue instant messages, or participating in peer-to-peer file sharing. For traffic coming into the network, the signatures mainly protect against specific threats aimed at servers that can't be detected by the proxy, such as cross-site scripting or SQL injection.

Most of the other broad classes of threats are effectively trapped without signatures by the first six layers below.



For maximum security, any layer can place the incoming Internet address in the firewall's blocklist – a "penalty box" for misbehaving connections. With this autoblock capability enabled, a WatchGuard firewall drops all further packets from that address for a period of time. This adds

an especially effective element for enforcing zero day security, since few hacking attempts – even previously unknown ones – can proceed without triggering suspicion at some level.

In addition, all firewalls must leave some ports open. These open ports allow access to universal services such as web or email. An attacker probing the open ports for vulnerable servers and services is one of the first signs of an intrusion. A WatchGuard firewall set to autoblock not only denies the probe, but might also send back a response that reports the target doesn't exist. In fact, white hats typically find it difficult or impossible to do a penetration test or security audit of a network protected by a well-configured WatchGuard firewall.

Out on the Border

Think of a packet passing through a firewall as a vehicle at a border crossing. A packet inspection firewall can ask the driver where he's coming from, where he's going, and what he's going to do when he gets there. A stateful inspection firewall does a little more – it can also consider the flow of the conversation, and whether something doesn't seem quite right. If the firewall applies signatures, it can look inside the car, and compare what it sees against a list of contents deemed illegal.

A WatchGuard application proxy firewall with intelligent layered security conducts the same conversation. Then it opens the glove box, pops open the hood, and looks under the seats. It looks for loose screws or false panels. At any point along the way, if it finds anything suspicious, it halts the inspection and denies entry. If necessary, it disassembles parts of the car, tearing it completely apart if it has to. Then, if everything is legal, it puts the car back together and sends it on its way, running better than ever before. All in much, much less than the blink of an eye.

Meeting the Zero Day Challenge

Security is a balancing act between access and security. The most secure network is one that no one can access. At the other extreme, unlimited access is a strategy for disaster. Striking the right balance is a task for IT personnel who understand their organization's needs for effective defense, weighed against the needs of their users.

This is the only approach that can rise to the challenge of the today's hackers. They are incredibly resourceful, technically skilled, and handsomely rewarded for their efforts. They are constantly refining their techniques, and their attacks are swifter and stealthier than even before. A conventional reactive security stance, based on packet filters and signatures, is powerless against the new generation of sophisticated zero day attacks.

Thwarting zero day attacks calls for a proactive security posture that detects and blocks attacks at multiple levels, looks deep into the application layer when necessary, and allows only known good traffic to pass. A firewall that meets those requirements is not only highly protective right out of the gate, but can also be tuned to achieve zero day protection while balancing organizational needs for security and access.

WatchGuard firewalls deliver that protection. For more information about WatchGuard security solutions, visit us at www.watchguard.com, or contact your reseller.

[1] Cooperative Association for Internet Data Analysis (www.caida.org), "The Spread of the Code-Red Worm (CRv2)"
[2] Cooperative Association for Internet Data Analysis (www.caida.org), "The Spread of the Sapphire/Slammer Worm"
[3] MessageLabs Intelligence: 2007 Annual Security Report, p. 12
[4] Computer Security Institute, *2007 CSI Computer Crime and Security Survey*, p. 3
[5] Current statistics are at http://nvd.nist.gov
[6] Computer Security Institute, *2007 CSI Computer Crime and Security Survey*, p. 2
[7] *Microsoft Security Intelligence Report, January through June 2007, Key Findings Summary*, p. 7-8
[8] Current statistics are at http://www.shadowserver.org
[9] *Symantec Internet Security Threat Report: Trends for January-June 07*, p. 15
[10] Computer Security Institute, *2007 CSI Computer Crime and Security Survey*, p. 13
[11] Computing Technology Industry Association, *Summary: Making the Case for Managed Services – The Business Impacts of IT Problems at SMBs*

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 unified threat management (UTM) solutions provides the best combination of strong, reliable, multi-layered security with the best ease of use in its class. Our newest product line – the WatchGuard SSL – makes secure remote access easy and affordable, regardless of the size of your network. All products are backed by LiveSecurity Service, a ground-breaking support and maintenance program. 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.

Part. No. WGCE66521_032608

WATCHGUARD AND UNIFIED THREAT MANAGEMENT:

A Business Overview

AUGUST 2007

DYNAMIC THREAT ENVIRONMENT

Keeping corporate networks safe is more challenging every year, and network security has become one of the most critical issues facing businesses today. New and ever-changing threats appear with alarming regularity, and no organization is immune from risk.

Every time a new and more sophisticated threat presents itself, it changes the very definition of what a "secure network" really is. According to the IBM Internet Security Systems X-Force Research and Development Team, more than 7,247 new Internet security vulnerabilities were discovered in 2006, and 88.4% of those could be exploited remotely.

When a network is breached by intruders, a Denial of Service (DoS) attack, or a malicious virus, the entire organization becomes vulnerable. This can leave a company's operational resources, customer data, proprietary tools and technologies, and intellectual capital in danger of being stolen, misused, or vandalized by third parties. Network attacks can take many forms, including:

Network Intrusion - In an intrusion scenario, a hacker with no access privileges attempts to penetrate a network remotely for malicious purposes.

DoS/DDoS Attacks - In a DoS attack, targeted systems or networks are rendered unusable, often by monopolizing system resources. A Distributed Denial of Service (DDoS) involves many computer systems - possibly hundreds - all sending traffic to a few specific targets.

Viruses and Worms - A virus is a computer program that infects other programs with copies of itself, but which is transferred from system to system by some outside mechanism such as e-mail. A virus executes and does its damage when the program it has infected executes. This is distinct from a worm, which is a computer program that is capable of repeatedly copying itself to other computer systems. Worms can carry viral code.

Adware and Spyware - Adware is a software application which installs itself, often without the user's permission, and displays advertising banners while the program is running. They may appear as pop-up windows or as a bar that appears on a computer screen. It may also change browser properties such as the home page. Spyware is similar to adware but often does not reveal its presence by pop-ups or other means. It uses code to track a user's personal information and pass it on to third parties without the user's authorization or knowledge.

Rootkits - A rootkit embeds itself into an operating system and intercepts commands that other programs use to perform basic functions, like accessing files on the computer's hard drive. It hides between the operating system and the programs that rely on it, controlling what those programs can see and do.

DNS Poisoning - Domain Name System (DNS) servers are duped into re-directing traffic originally heading to a benign destination to a malicious Web site instead.

A network can also become vulnerable every time a business experiences growth and change. As networks become more complex and are expected to do more to support and drive business objectives, a simple firewall is not capable of providing the security your network needs. This is where Unified Threat Management (UTM) solutions can be the right solution.

WHAT IS UNIFIED THREAT MANAGEMENT?

Unified Threat Management is the name for an emerging trend in the appliance security market. Unified Threat Management appliances are an evolution of traditional firewall and VPN appliances into a product that has many additional capabilities such as: URL filtering, spam blocking, spyware protection, intrusion prevention, gateway antivirus, and a centralized management, monitoring, and logging function. These functions were traditionally handled by multiple systems.

WHY UNIFIED THREAT MANAGEMENT?

Unified Threat Management Solutions are Cost-effective

Integrating multiple security capabilities into a single appliance mean that you can purchase and use fewer appliances, eliminating the cost of building layered security with separately purchased solutions.

Stops Attacks at the Network Gateway to Keep Your Business Moving

The multi-functional security approach offered by UTM appliances lets you avert catastrophe by blocking a broad range of network threats before they have the opportunity to enter your network. For example, malicious code will not have the opportunity to disable security at the desktop or server level. Your business-critical files and applications remain available to keep your staff on the job.

Easy to Set Up and Use

Separate security systems means different management consoles to configure each system. Because the management paradigms of these systems are typically very different, it can be very time consuming to make sure the different security policies on each system work together and provide adequate protection. In addition, log information from each system will be stored in different formats in different locations, making detection and analysis of security events difficult.

Whether you are an IT expert or a security novice, a UTM solution with centralized management, monitoring and logging provides indispensable ease of use for configuring and managing your security. A UTM solution makes it easy to build coherent security policies, simplifies administration tasks such as log file management, auditing, and compliance reporting, and lowers operational costs when compared with the complexity of setting up separate security systems to defend against various specific threats.

UNIFIED THREAT MANAGEMENT AND ZERO DAY PROTECTION

Most UTMs in the market today rely on signature- (or pattern-) based technologies to deliver key security functions such as URL filtering, spam blocking, spyware protection, intrusion prevention, and gateway antivirus.

Signatures are only Part of the Solution

Signature-based solutions, for years the mainstay of every network security arsenal, use a database of known signature files to identify and block malicious traffic before it enters a network. They provide protection against threats such as trojans, buffer overflows, arbitrary execution of malicious SQL code, instant messaging and peer-to-peer usage (such as Napster, Gnutella, and Kazaa), and policy violations.

Once an exploit threat has been unleashed and identified however, it can take anywhere from a few hours to a few weeks for corresponding signature files to become available for download. This security "downtime" creates a window of vulnerability during which networks are open to attack:

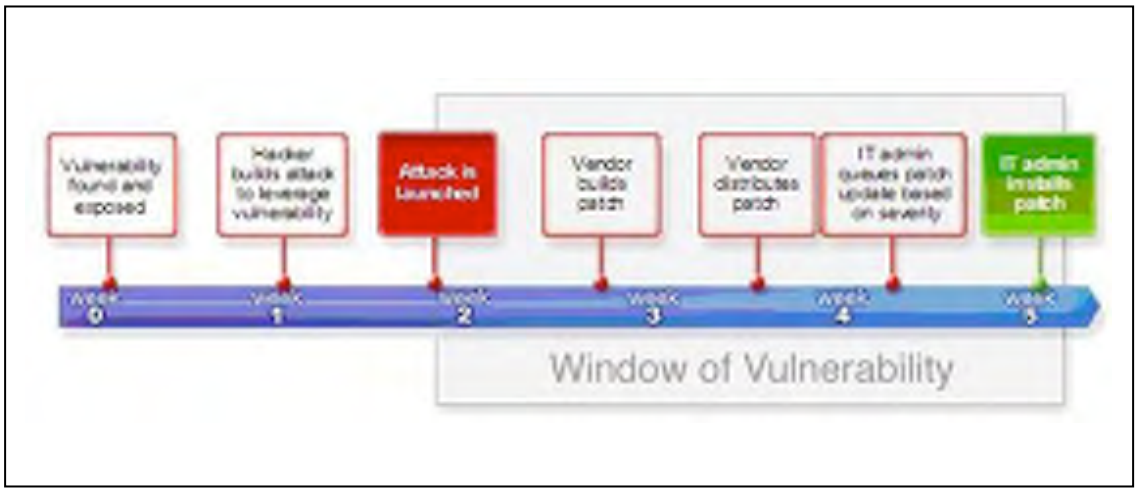


Figure 1: Attack Lifecycle and the Window of Vulnerability

In today's dynamic threat environment, with hundreds of new threats released every year, and worms able to propagate across the world in a few minutes, signatures are often not available soon enough. Protection mechanisms which can defend against new and unknown threats without requiring new signatures or configuration changes are required. This type of protective mechanism is known as Zero Day protection.

WATCHGUARD UNIFIED THREAT MANAGEMENT

Zero Day Protection

Although hundreds of new attacks are developed each year, the majority of these attacks fall into a few major classes. WatchGuard® Intelligent Layered Security offers Zero Day protection, as it is designed to protect against these major classes of attacks, and in many cases can offer protection against a brand new attack without requiring any updates or configuration changes.

Intelligent Layered Security

The Intelligent Layered Security (ILS) engine at the heart of the WatchGuard family of UTM appliances provides powerful protection for growing enterprises, defending against both known and unknown attacks and giving maximum protection while minimizing impact on network performance.

Intelligent Layered Security performs proactive, in-depth diagnostic searches of the data stream and cooperatively shares information on suspicious traffic among its layers. Zero Day protection is provided through three key mechanisms:

- **Protocol Anomaly Detection -** Internet standards for data traffic are enforced to detect and block non-conforming traffic and isolate threats
- **Behavioral Analysis -** Hosts exhibiting suspicious behaviors are identified and stopped
- **Pattern Matching -** High-risk file types known to propagate viruses or attacks are flagged and deleted before they enter your network

Data flows smoothly while traffic is scanned, and viruses, worms, spyware, trojans, and other malicious attacks are proactively blocked at the edge of your network.

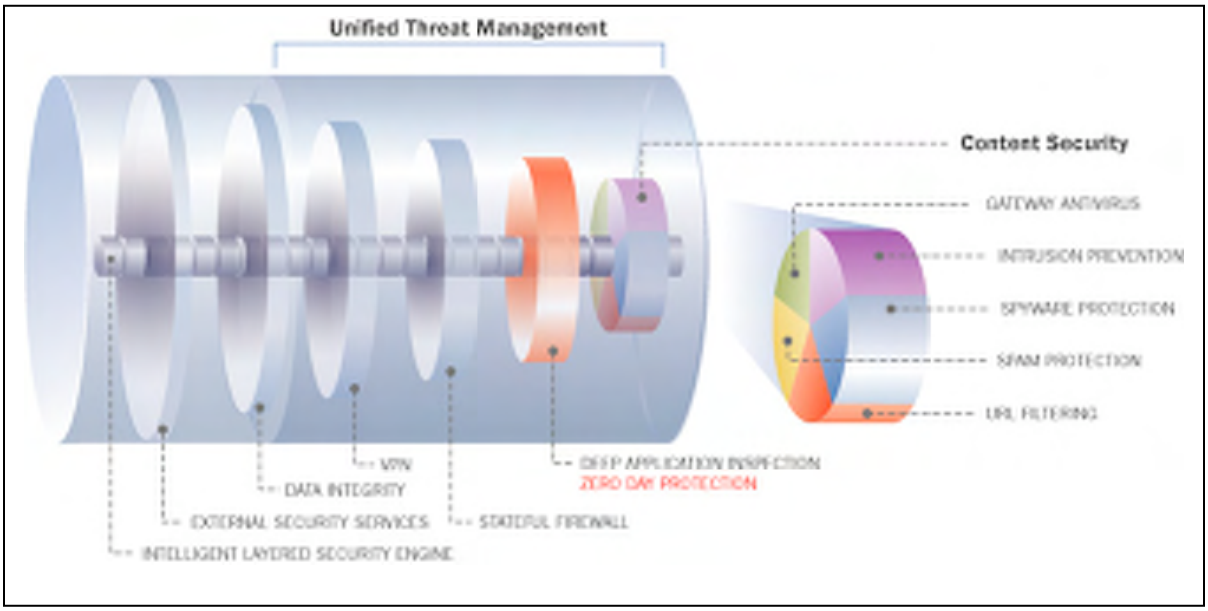


Figure 2: Intelligent Layered Security Architecture and UTM

The WatchGuard ILS architecture consists of six security layers working cooperatively with one another to dynamically detect, block, and report on malicious traffic while passing benign traffic through as efficiently as possible. Each layer performs different security functions:

1. **External security services** provide technologies that extend network protection beyond the firewall

2. **Data integrity** validates the data packet integrity and packet protocol conformance

3. **Virtual Private Networking** (VPN) ensures secure and private external communication

4. **Stateful firewall** restricts traffic to the sources, destinations, and ports allowed by the security policy

5. **Deep application inspection** ensures conformance with application layer protocol standards, rejects dangerous files by pattern or file type, blocks dangerous commands, and modifies data to prevent leakage of critical system information

6. **Content security** analyzes and regulates traffic for appropriate content; examples of this include signature-based technologies, spam blocking services, and URL-based content filtering

More details about the WatchGuard ILS architecture and its Zero Day protection capabilities can be found in our whitepaper titled *Introducing the WatchGuard Intelligent Layered Security Architecture: Better Security for the Growing Enterprise*.

Unified Threat Management Services

WatchGuard offers a number of security services which are designed to augment the Zero Day protection capabilities of ILS. The services currently offered are gateway antivirus, intrusion prevention, anti-spam, URL filtering, and spyware protection.

Gateway Antivirus and Intrusion Prevention Service

This service combines two key capabilities; let's look at each one in turn.

Gateway AntiVirus Capabilities

Identifies and blocks worms, spyware, and trojans within e-mail attachments, therefore blocking threats from entering your network and executing dangerous payloads. The integration of Gateway AntiVirus (AV) with other security layers in ILS provides some important benefits, namely:

- **Efficiency -** The Gateway AV service only scans files not blocked by the ILS pattern matching capabilities, greatly reducing the number of files which need to be scanned
- **More granular control -** Gateway AV finds viruses in file types which you may choose to allow into your network such as .zip, .doc, etc.

The WatchGuard antivirus database contains thousands of virus, spyware, worm, and Trojan signatures, including both Wildlist and "zoo" viruses. A broad range of compression/decompression algorithms is supported, including ZIP, RAR 2.0, TAR, GZIP, ARC, and CAB files. Signature delivery is automatic, and signature update checks can be programmed for any desired interval. The targeted threat response time is 8 hours, which is significantly better than industry average.

Intrusion Prevention Capabilities

WatchGuard Intrusion Prevention Service (IPS) provides in-line protection from attacks that comply with protocol standards but carry malicious content. It is a signature-based service designed to protect against a broad range of attacks including cross-site scripting, buffer overflows, and SQL injections.

The IPS can selectively block IM services, such as AIM, Yahoo, IRC, and MSN Messenger. This protects against IM-based security threats, including exploits which allow the attacker to gain control of a machine running an IM client, and infections by viruses transferred in files over IM.

Peer-to-Peer (P2P) applications such as Napster, GNUtella, Kazaa, Morpheus, BitTorrent, eDonkey2000, and Phatbot can also be blocked. Peer-to-Peer presents two problems. First, it uses up valuable bandwidth that is better used for business purposes. Second, it is a well-known vector for transmitting spyware (Kazaa in particular). By blocking P2P, we solve both of these problems.

The IPS can also detect and block outbound spyware communication to malicious hosts, preventing sensitive data from being sent out by spyware programs. This activity can be logged or alerted on so that the system administrator can identify and remediate infected machines.

The WatchGuard proprietary intrusion prevention engine integrates tightly with other ILS, functions, reducing false positives and speeding execution while producing comprehensive log information.

Anti-Spam Service

Spam accounts for more than 63% of all e-mail today, and represents a major problem for most companies. The WatchGuard spamBlocker service utilizes Commtouch® Recurrent Pattern Detection (RPD™) technology for real-time anti-spam detection that provides powerful protection from spam attacks. Rather than evaluating keywords and content, this technology analyzes large volumes of Internet traffic in real time to identify the repetitive components, or DNA, of each outbreak as soon as they emerge. Close to 500 million messages per day are sampled, and advanced algorithms detect, identify, and classify new outbreaks - typically within 1-2 minutes. These algorithms are also capable of distinguishing solicited bulk e-mail from spam. spamBlocker utilizes this technology to give you up-to-the-minute protection from spam attacks by comparing suspected spam directly with the Commtouch® Detection Center (which has approximately 20,000,000 spam classifications) in real time. This technology provides four key benefits:

- **Extremely fast response** to new outbreaks
- **Near zero false positives** make it the best service in the industry at distinguishing legitimate communication from spam attacks
- **High spam detection rate** protects networks from 97% of unwanted e-mails
- **Language agnostic** to block spam regardless of the language, content, or format of the message

URL Filtering Service

The WatchGuard WebBlocker URL filtering capability enables you to configure not only who gets Web access and who doesn't, but also what type of Web access is available. Using an intuitive set of controls, you can quickly select which categories of Web pages users get access to, and what time of day they get access. WebBlocker utilizes site database and engines from the global Web-filtering leader, SurfControl™, to ensure the most accurate categorization and complete coverage. WebBlocker uses numerous categories to help you block content you don't want to allow on your network. For example, blocking pornography can assist in enforcing company policy on sexual harassment in the workplace, and blocking sports content may increase workplace productivity. With the WebBlocker customizable exceptions lists, per-person authentication, and

provision for different access policies depending on the time of day, you'll be able to efficiently enforce IT policies.

WebBlocker will also help keep your network and end users secure from viruses, worms, and spyware by preventing users from reaching sites that are known distribution points for malicious applications.

Spyware Protection

While spyware protection is not currently a separate service, anti-spyware technology is built into the Gateway Anti-Virus/Intrusion Prevention Service (GAV/IPS), and also into WebBlocker. Anti-spyware technology in ILS is made up of three parts:

- Blocking of URLs which contain spyware (WebBlocker)
- Detection and blocking of spyware downloads and drive-by installs (GAV/IPS)
- Detection and blocking of outbound spyware communication to malicious hosts (IPS)

For maximum protection, the Gateway AV/IPS and the WebBlocker services are required.

PROTECTING YOURSELF AGAINST A SOPHISTICATED ENEMY

The evolution of traditional network security practices into comprehensive UTM solutions brings with it a level of protection never before available to corporate networks. As sophisticated network threats appear with increasing frequency, this integrated, layered security approach, including ILS, signature-based services, and URL-based filtering, provides the strongest one-stop protection for any growing network infrastructure.

For more information about WatchGuard Security Solutions, visit us at www.watchguard.com, or contact your reseller.

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 unified threat management (UTM) solutions provides the best combination of strong, reliable, multi-layered security with the best ease of use in its class. All products are backed by LiveSecurity® Service, a ground-breaking support and maintenance program. 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.

Part. No. WGCE6628 092007

PRODUCING YOUR NETWORK SECURITY POLICY

JULY 2007

Frederick M. Avolio
Avolio Consulting

Steve Fallin
D. Scott Pinzon, CISSP, NSA-IAM
Watchguard Technologies, Inc.

Executive Summary

Network security experts agree that well-run corporations need a written security policy. The policy sets appropriate expectations regarding the use and administration of corporate IT assets. However, the conventional w isdom holds that composing and maintaining these documents bog down in a morass of bureaucratic inefficiency and pointless wrangling, which never ends and produces nothing useful.

This paper lays out a common-sense approach to writing corporate security policies that makes them easier to draft, maintain, and enforce. Our "question and answer" approach requires no outside consultants. Instead, you can use your in-house knowledge and resources to yield a brief, usable, and – most importantly – understandable policy document, in a reasonable amount of time. To help you generate such a policy, this paper clears away some misconceptions about the purpose of network security; details the process of writing the policy; then explains how to keep refining the drafted policy.

Introduction

It is the rare organization that is happy with its security policy. Many will admit to not even having one. But, security policies are like noses: everyone has one. Every organization follows either a formal or an informal security policy, even if it is what we jokingly refer to as the Primordial Network Security Policy: “Allow anyone in here to get out, for anything, but keep people out there from getting in."

Realistically, many security policies are ineffective. Sometimes an organization gets lucky and has a security policy that is pretty good – but not usually. To be effective, a security policy (and, let’s reset that right now to “security policies,” because we are talking about a set of policies) should be consistent, relevant, and useable. The goal of this white paper is to help you create such documents.

Armed with this paper, your small- or medium-sized enterprise (SME) can either create your first computer network security policy, or beef up what you already have. This paper covers policy but not procedures. Computer and network security policies define proper and improper behavior; they spell out what is permitted and what is denied. Procedures detail the methods to support and enforce the policies, and usually describe specific steps to take in regular system administration. For example, your policy might state, "Server administrators must adhere to the company's operating system configuration standards." A separate procedures document would specify what all those settings are.

This paper will help you set policy. First, we correct some misconceptions to help you understand what your real goals are. Then we describe the process for writing your policy, and end with some thoughts on what to do after completing your initial draft.

Four Common Misconceptions

1. "The goal of network security is to secure the network" (or "the computers"). Securing the network is easy, but it's not your goal. Your real goal — and a more difficult job — is securing the business.

   The goal of network security is to support the network and computer business requirements, using methods that reduce risk. Security policies describe what you must secure, and the ways you secure them, to support your business or mission. Firewalls, intrusion detection systems

(IDS), anti-virus (AV), backup and restore strategies, locked doors, and system administration checklists are all some of the things you might use. Security policies provide the blueprint for using them: the what, how, why, when, and by whom.

2. "Security policies must be long and complex." In fact, just the opposite is true. We believe the well-known security axiom, “Complexity and security are inversely proportional.” Complex systems are usually less secure than simple systems. Complex policies are usually ignored; simple policies might live.

   A good security policy is really a set of documents, each addressing a specific need. By breaking your overall policy into smaller pieces, each managed separately, you greatly simplify the process of creating effective, consistent, relevant, and useable documents. This is not to say that the entire set of security policies will or should be just a few pages. But each individual element — each policy — should be usable by the target audience. “Usable” does not mean merely "understandable,” or even “readable” and “memorable.” It also has to take into account your corporate culture. So keep it real. Don't write academic tomes (unless that is your corporate culture). Write something your target audience can read and understand, in the amount of time their duties permit them.

3. "Security policies have to be nearly perfect, or 100% complete." No. Good enough security now is better than perfect security never.

   For some reason organizations treat security as something sacred, when this is exactly the area where practicality should reign. There is not one right way to write a security policy. You are also allowed to modify it later. General George S. Patton said, “A good plan, violently executed right now, is far better than a perfect plan executed next week.” That is not to say that your goal should be to produce something shoddy or incomplete and call it “whole.” But it is perfectly fine to build security policies in parts, refining each part separately in the ongoing process of security policy development. Some parts will seem fully baked before other parts do. That's OK. That's how the process works.

4. "Security policies only have to be written once." Until there are no more bad guys in the world and everyone agrees to mind his or her own business, the process of managing a security policy never ends.

   The threats your organization faces will change over time. As the threats to your business change, so too will your company’s business requirements. The vulnerabilities will change as well, and so will the risks you are willing to take to do business, and so will the tools you use to reduce or counter those risks. Because of all this, the security policy process is never really done. It only lies dormant for a time.

If you're willing to believe the truths of the previous four paragraphs, then press on. We will next discuss:

- The general structure of the security policy
- The process of putting the policy documents together
- What documents you should create
- What they should say
- How and when to review and revise them

The Process

The first step in writing your policies is to gather a team. Writing a set of security policies is usually a top-down process, but it does not have to be, and may combine bottom-up and top-down approaches. Your policy development team should be made up of people who work with your network and the Internet, but come from different functional areas of the company. Each manager in your company has a unique view of the company's needs and risks. You need people who know something about the technology, but also some who know about business. Include some people from the trenches, too. There is nothing less useful than a painstakingly documented security policy that, when implemented, makes the shipping department unable to track packages, or blocks the sales reps from network resources they need from the road.

However, don't let the process of forming the committee halt all progress. Remember, well begun is half done; you can start developing the drafts with just a few knowledgeable IT staffers.

Before writing any policies, scope out your business requirements. What regulations apply to your industry (GLBA, HIPAA, Sarbanes-Oxley, ISO17799, new state or local laws, etc.)? Get familiar with penalties for any non-compliance, as this will help you prioritize your policies and gauge the proper level of discipline for employees who do not adhere to policy. To consider other business issues, ask yourself:

- What services are required for your business, and how might you provide them securely?
- How much do employees depend on Internet access, use of email and availability of intranet services?
- Do your users need remote access to the internal network?
- Is there a business requirement for everyone to have access to the Web?
- Do customers access your data (technical support, order status, etc.) via the Internet?

It takes discipline to ask repeatedly, "Is there a business requirement?" for every service. But the business requirements are the most important drivers of your security policies. Business drivers help you distinguish between what the organization really needs, as opposed to what a few employees want. If you have trouble getting started, look at what you are already doing and ask, “Why are we doing that?” The answer will kick-start your response to the questions above.

Policy Creation

In this section we will interactively start to draft your policies, beginning with the Root Security Policy and then working through a few of the others. Each policy sets out the definitive answer to a set of key questions.

The Root Security Policy

The first document you’ll draft is the “Root Security Policy.” This is also the easiest to write, as it is the framework which points to the other policy documents.

As you draft a Root Security Policy, you will also enumerate the initial list of subordinate policies that you should produce next.

Your list will be specific to your organization, but will probably include the following subordinate policies:

- **Computer Acceptable Use.** A general document covering all computer use by employees and contractors, including desktop, mobile, home PCs, and servers.
- **Password.** A description of the requirements for password protecting computer systems, the rules for choosing passwords, and how the password policy is enforced.

- **Email.** This policy covers the use of email sent from any company email address and received at any company computer system.

- **Web.** A specification of what browsers may be used, how they should be configured, and any restrictions on which sites employees can visit.

- **Mobile Computing and Portable Storage.** A description of who owns the mobile computing and portable storage on your network, how they are supported, and what specific devices (if any) are authorized for use on the company network.

- **Remote Access.** A policy stating who can access what information from which locations under what circumstances.

- **Internet.** A description of your Internet-facing gateway configuration, stating what is allowed in and out, and why.

- **Wireless.** A specification stating how wireless access will be managed on your network; how access points will be plugged in, secured, and maintained; who is allowed to use them; and under what circumstances.

- **Servers.** A statement of the company standards for servers, what services are enabled or disabled by default, and important distinctions between production, test, and development environments.

- **Incident Response Plan.** No policy is complete until it also specifies what to do when defenses fail: what is considered a security incident; who gets called; who is authorized to shut things down if needed; who is responsible for enforcing applicable local laws; who speaks for the company.

The Root Security Policy will also specify numerous easy-to-describe items, such as:

- **The company name.** Does this policy apply to your whole company, or a distinct division, office, or locale?

- **The purpose of the policy.** What is it for? What do you hope to gain by creating a policy?

- **The individuals or organizations responsible for the policy.** Who is responsible for overall network security? The head of the IT department? The information systems security officer? Some other executive? (Tip: In the drafting phase, you are allowed to write "To Be Determined.") Eventually, you will also want a "Site Security Committee," a small group of managers and technical people representing various user groups in the organization, including the HR department. This committee is responsible for maintaining the policy so that it is current and relevant.

- **The scope of the policies.** Make sure that you state what geographies, organizations, and assets you are covering. State explicitly which geographies, organizations, and assets the policy does not cover, as well.

The Root Security Policy should also briefly describe:

- **Penalties for breaking policy.** Determining this will probably require talking to upper management and the Human Resources department, but will almost always include words such as, "disciplinary action up to and including termination of employment."

- **Who enforces the policy.** All managers and supervisors should be responsible for the administration and enforcement of the policy.

- **Who must abide by the policy.** All employees should be responsible for adhering to the policy. Will there be exceptions? Under what circumstances? Take the time to define an exceptions process, making sure that the process calls for periodic review of the exceptions.
- **The other documents listed in the policy.** The root policy forms the framework for the rest of the document. This entry can be as simple as a bulleted list or as detailed as a bibliography.
- **How to request policy changes.** There will and should be changes as the policy matures. Specify when and how changes can be made, and who can make them.
- **How often your policies must be reviewed.** For most SMEs, a year is too long to go without a policy review. Monthly reviews are too frequent. If you are not sure what interval to specify, start with "quarterly, or as needed." ("As needed," for example, might be after a request for a change, or when the requirements or the apparent threats change.)

How many pages will all this fill up? As many as it takes, but usually no more than two to five pages (initially) for the Root Security Policy, and one or two pages for each individual sub-policy. In school, you might have gotten used to padding your documents to meet some minimum page requirement. In security policies, follow the opposite route: brevity reads like wisdom.

Acceptable Use Policies

After you have the Root Security Policy, producing the subordinate or AUP policy largely means making lists and asking questions. List the assets you must protect. For example, your list might include:

- Desktop computers
- Mobile computers
- Servers
- Routers
- Email systems
- Application data

For each asset, ask:

- Who administers the asset?
- Who uses it?
- How critical is it to the mission of your enterprise?
- How do you manage it?
- How do you protect it?

This exercise gives you a checklist of assets to cover with AUPs. All of your AUPs will answer similar, overlapping core questions, and will have the same format. Each AUP will address:

- **Objective.** What is the purpose of this particular AUP?
- **Target.** Describe the systems to which this AUP pertains.
- **Responsible parties.** To whom does the policy pertain?
- **Policy.** A detailed statement of what the policy is. What does the policy permit? What does it deny? What are the user responsibilities? What must the employee report?

As you go through the process of creating your AUPs, you must answer these questions at least. If other good questions occur to you, answer them as well (For example, according to policy, where and how is data stored? Is an employee allowed to store the sales forecast on a home computer? When and how should data be destroyed?). Some information in the AUPs will be redundant, but one of the goals is for each AUP to be somewhat self-contained.

Answer each question with a simple declarative sentence or paragraph. You want to reduce the possibility of your text being misinterpreted. Therefore, as you answer the questions, don't merely write to be understood. Try to write so that you cannot be misunderstood. Prefer specific words over vague words. Prefer active sentences over passive sentences. For example, in a passive sentence like "This policy is to be adhered to at all times," who must adhere to the policy? We can't tell. Clearer: "All IT team members must follow this policy, always."

For the balance of this guide, as we describe each AUP we'll assume that you have answered the fundamental questions above. The rest of our description will concentrate on issues unique to each AUP.

Personal Computer AUP

Questions to answer include:

- Who owns the PC? (Most of the time it's the company, but you'll need the policy to also address, for example, the home PC of a telecommuter.)
- Are there any restrictions on non-business use? (For example, may a company computer be used for games, or personal email?)
- Who is authorized to use the PC? Only the employee to whom it is issued? Any employee of the company? An employee's immediate family?
- How should the user protect the computer data? (For example, must the user encrypt files?)
- How should the user protect the computer from unauthorized access? (Passwords? Password-protected screensaver? How many minutes before the screen saver times out?)
- What software must be running on the PC? (Examples: Antivirus? Personal firewall? A spyware detector? What versions? etc.)
- Are there restrictions on software installation? (For example, is the user permitted to install anything downloaded from the Internet?)
- What special protection is required for mobile computers?
- What activities or classes of activities are prohibited?
- Will you monitor keystrokes or communications? If so, how will you notify employees of this?
- Who is responsible to back up computer data?
- How must the user protect or mark personal information on a company-owned computer?

Email

Questions to answer include:

- May employees use email accounts for non-business-related email?
- Must employees include a disclaimer when they send non-business-related email? When they post to public email forums?
- Must they (or may they) encrypt and sign messages? If so, how?

- What restrictions apply to sending email? (For example, you should generally prohibit spam, illegal transmissions, chain letters, etc.)
- What, if any, attachment types are prohibited (sending or receiving)?
- Is email subject to monitoring? If so, how will you notify employees of this fact?
- What email client software is permitted?
- May users access outside email accounts (other ISPs, Hotmail, Hushmail, etc.)? If so, under what conditions?
- May employees access web-based email accounts from company PCs? What rules govern the use of POP? IMAP?
- Who may use corporate email systems or email clients?

Web Access

Questions to answer include:

- Are there any restrictions on accessing external web sites? (To answer this, you might want to consult the web site of one of the many web filtering services. They'll list categories of objectionable material you might not have thought of, including sports sites, hate sites, gambling sites, etc.)
- May users access non-business related email accounts via the Web, using company machines?
- Do you restrict certain types of web content, such as streaming media, or content that might violate copyright laws?
- What browsers may or may not be used?
- What, if any, rules govern the use of browser add-ins or Java applets?
- Are there any required browser configurations?

Mobile Computing & Portable Storage

Questions to answer include:

- May users bring their own PDA to work? If so, are they permitted to access the company network via their PDA?
- What PDAs are supported?
- May users install software on the PDA?
- Are there restrictions on devices with wireless capabilities (see Wireless AUP)?
- May corporate data be stored on user-owned portable storage (USB jump drives, smart phones, iPods, etc.)? If so, how must it be protected?
- Should the storage device be password-locked? Should it be encrypted?
- Do you restrict the type of information you permit to be stored on portable devices?
- Is any particular software prohibited?
- Many devices use portable SD or CF memory cards. Are employees permitted to use these? What rules govern their usage? Can company data be stored on these cards? (Consider also unorthodox "storage devices" such as digital cameras, novelty devices, toys with RAM, DVDs, etc.)

Remote Access

Questions to answer include:

- Do you restrict remote access to the enterprise to just authorized users (probably—i.e., not employee's family members)?
- Is wireless access permitted? (See Wireless AUP.) Is access from Internet cafés permitted? If so, under what circumstances and with what safeguards?
- What software and hardware combinations and configurations are required for remote access?
- May users access the enterprise network from devices your IT department has not issued, or has not authorized?
- How will you authenticate (confirm the identity of) the person accessing the network?
- How is access controlled? By passwords, security tokens, VPNs, or what?
- Is remote access granted to all employees, or must they apply for it? How do they apply?
- What activities are prohibited? What activities are permitted?
- Is account activity monitored? If so, how will you notify employees of this fact?
- In what ways must a user protect the remote access account?

Internet-facing Gateway Configuration

This could apply to a router, switch, firewall, or UTM. If you have more than one, write an AUP for each one, but use the same format for each. Identify which gateway you are writing about in the Target section of each AUP.

Questions to answer include:

- How is the device accessed? What authentication is used? Are there other required safeguards for access? What protocols are permitted or denied for administrative access? (For example, "SSH required, TELNET prohibited.")
- What outgoing protocols are permitted? Which are denied? (If Trojan horse code infests your network, proper egress filtering can prevent the code from contacting its author to establish a back door into your network.)
- What incoming protocols are permitted? Which are denied? (Ingress filtering.)
- What application-level controls are in place for filtering? For example, do you filter HTTP (Web) traffic? SMTP (mail) traffic? How about Domain Name Services?
- Will you control Internet access based on protocol and target-system? For example, will the gateway permit email- or web-related protocols from the Internet to any internal machine, or just to email and web servers?
- Will you control outgoing connections to ensure that only appropriate connections are made? For example, will email-related protocols be allowed outbound only from the enterprise email server(s) and not from desktop computers? What about other services, such as DNS and NTP?

Servers

This AUP should apply to all dedicated servers used by multiple users within the enterprise that may also communicate with other servers (Internet or intranet). This is a general policy. You might have more specific ones for HTTP servers, FTP servers, email servers, etc.

Questions to answer include:

- What is the main purpose of the server?
- What information must be kept about the server (IP address, MAC address, physical location, operating system (OS) version, patch level, services offered, person responsible, etc.)?
- May individuals deploy internal servers, or is that right restricted to IT alone?
- What are the OS configuration policies that must be followed? (Usually, the answer points to another document for OS-specific procedures.)
- How is administrative access controlled?
- How is the server physically protected?
- How is the server monitored, and by whom?
- What is the back-up policy?
- Who may access the server (non-administrative access)? Who may not?
- What is the patch-control policy for the server? (This may point to another "patch control" policy or procedure document.)
- What change control procedures must be followed? (This may point to another "change control" policy or procedure document.)

Wireless Devices

The Target section of your Wireless AUP might look different than the Target section of other AUPs. You must specify if your wireless policy covers:

- All wireless devices, i.e., mobile phones, PDAs, computers (This is the most comprehensive option).
- Only those that directly connect to the enterprise network (This omits basic mobile phones.)
- Those that indirectly or occasionally connect to the enterprise network, such as PDAs, PDA/phone combinations, and devices like the Blackberry. (This omits wireless enabled laptops.)

Depending on the degree to which you use wireless technologies, it may be necessary to draft a Wireless AUP specific to each type of device (e.g., Blackberry® wireless devices, wireless enabled laptops, 802.11 capable phones).

Once you've defined the Target, questions to answer include:

- Is wireless access to your network allowed?
- Are any kinds of data or communication prohibited over wireless?
- What protection must be in place before wireless communication is authorized?
- How must the user protect the wireless device (physically and logically)?
- For wireless data, what hardware is approved, permitted, and/or required?

- For wireless data, what software is approved, permitted, and/or required?
- What rules govern wireless access points? Must they be deployed, configured, and installed by IT, or are other employees permitted such activities?
- What are the configuration requirements for wireless access points? (For example, "The password and username must be changed from the manufacturer's default.")
- Is VPN software required? Which or what kind? Who must or may install it?
- Where must wireless connections terminate on the network? In the DMZ? On a segregated VLAN?
- How must wireless connections authenticate and encrypt?
- Is wireless permitted for remote users connecting to the Internet with enterprise equipment?
- Is wireless access permitted for mobile users connecting into the enterprise network from outside the enterprise?
- What security devices and controls must be in place on authorized wireless devices?
- What configuration rules must users follow when connecting home wireless networks to enterprise assets?

Incident Response Plan (IRP)

"The best laid plans of mice and men often go awry." The sections above deal with your Acceptable Use Policy. But even with the best security devices, practices, and policies, you still might find yourself dealing with a network security intrusion or incident. Since mid-incident is the worst time to develop a plan, your next step is to formulate an Incident Response Policy.

Initial questions to answer in your IRP include:

- What do you consider a security incident? (You probably will consider web site defacement or a virus outbreak a security incident. But, is a port scan of all your Internet-facing systems a security incident? How about if they are port scanned once a day for a week? What if you discover the LAN room was left unlocked overnight?)
- If an incident occurs, who are you going to call? Everyone in the organization should know who to call. Everyone who is on the call list should know what to do with a suspected security incident.
- When must you call the police, FBI, Secret Service, or other local or federal civil authorities? Talking with a lawyer or your local FBI field office will help here.
- Which are your most important systems? Which are most difficult to recover? Which are least important or easiest to recover? If a security incident brings systems down, balancing the importance of each system against how long it takes to recover it will help you prioritize your triage efforts.

The IRP should contain contact information for everyone who must be contacted when an incident is discovered or suspected. People to consider adding to the "call list" include:

- System and network administrators
- Senior management
- Managed service providers
- Help desk
- Lawyers
- Public relations

- Law enforcement

And then from that list, answer:

- Who must be contacted immediately?
- Who can be contacted later? What are the outer boundaries of "later"?
- Who is responsible to contact whom?

Note that any mention of a security incident made to people outside your organization can have unforeseen repercussions. Your policy should state who is authorized to discuss your company's security with outsiders. All other insiders should be prohibited from divulging information, especially to the press.

Modern legislation means that every security incident can have legal implications. Even if you do not intend to prosecute anyone, the law might obligate you to disclose the incident. Consider having your IRP specify the title of the person in your company who is responsible for having functional familiarity with relevant laws in your country, state, and municipality; in other words, they know what actions the laws support and which actions they prohibit, and can advise others on what to do.

Your IRP should remind you of the steps to take during a security incident:

- The most important thing to remember: take good notes. During an incident, you will be tempted to wait until things are contained to document the event. Take the time to take good notes as events unfold, for a whole lot of reasons ranging from helping you understand the incident later, to defending your actions in court. You don't have to write down every little command you type. Write what symptoms made you take action. Document each major milestone in your response, noting each new tool used (including version numbers) and why you did what you did.
- Try to answer as many of the W's for any incident as possible: Who, What, Where, When, Why, and How.
- Make sure you're addressing the entire problem by assessing its scope. How bad is it? How many systems are affected? How certain are you that you're aware of the entire problem? (Axiom: Evil usually multi-tasks.) How bad might it become?
- Secure the systems affected. You need printed procedures for securing each system. It may be as simple as unplugging the network connection or pulling the power plug. It may require posting a guard. Seriously.
- If you plan on going to court over the incident, now is the time to call in experts. Do not touch anything else. Do not do anything else. "Computer forensics" is a specialty. Forensics requires evidence—certifiably unchanged data. Take no action that might change data.
- If you are not going to prosecute the incident, secure the vulnerabilities, if any, that led to the incident. Restore the system from a known good baseline and return it to use.

You will want to add and improve upon this rudimentary IRP. Incident response planing deserves a course of its own; this paper presents just a start. Like all security-related policies, your IRP should be tested, periodically evaluated (especially after use), and revised.

Next Steps

What a lot of work! Yet the task is feasible, isn't it?

If you go through the steps laid out in this paper, you will end up with a draft security policy. At this stage, there is danger on two fronts.

First, you might foolishly think that you are finished. This is just the starting point. You now have an imperfect blueprint. You must refine it, and then — when you are satisfied with it — you must periodically pick it up and view it again. Review with a critical eye, asking, “What is right? What is wrong? What needs to be changed? What should be completely scrapped?”

The other mistake is to think that the whole process is rubbish. If you have gone through the exercise, no matter what you ended up with, you are almost certainly further along than when you started. Even if most of what you have needs major revisions, by answering the questions you have learned a lot about what you are doing and what your enterprise needs in security policies.

In either case, take a break from the process and come back at it with a fresh perspective in two to four weeks. As you review what you’ve done in the previous round, look for areas where your answers could be misinterpreted, where your needs have changed, or where your original ideas aren’t working out. As with owning a house, part of owning a security policy is tinkering with it. Don’t be afraid to make necessary changes to meet your evolving business needs, and don’t forget to schedule your next periodic review.

Conclusion

Improving your existing security policy (even if it’s the primordial variant) need not overwhelm you. You can do it. In fact, there’s probably no one better suited. Ask questions, challenge your assumptions, write it all down, and give yourself permission to be less than perfect.

Following these simple steps will give you a great shot at producing a brief, usable, and most importantly understandable policy document in a reasonable amount of time. If no better benefits emerge, "I helped create my company's security policy" will look great on your resume.

For more information about WatchGuard security solutions, visit us at www.watchguard.com or contact your reseller.

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 unified threat management (UTM) solutions provides the best combination of strong, reliable, multi-layered security with the best ease of use in its class. All products are backed by LiveSecurity® Service, a ground-breaking support and maintenance program. 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..