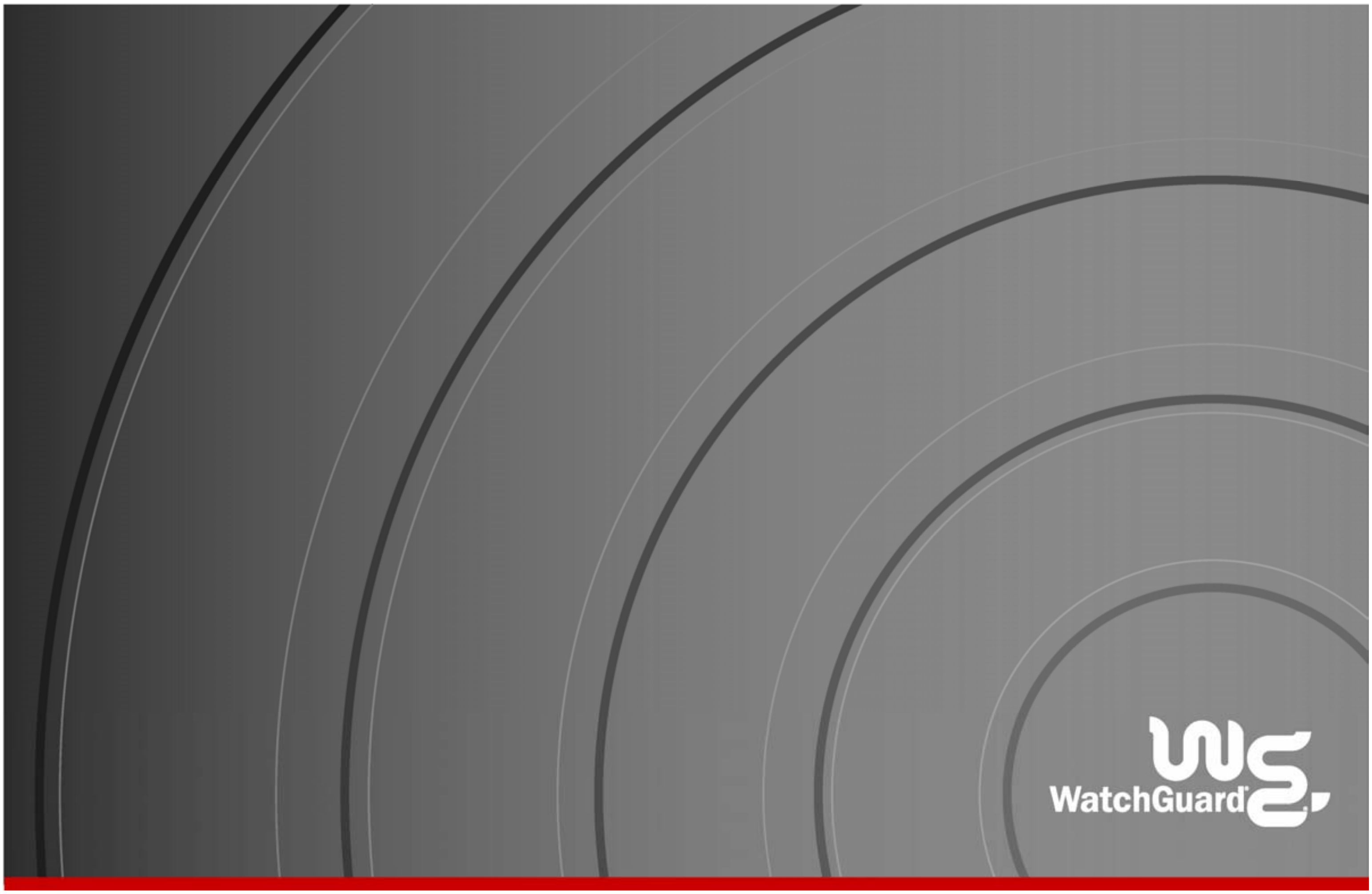

SMALL BUSINESS NETWORK SECURITY GUIDE

WHY A REAL FIREWALL PROVIDES THE BEST NETWORK PROTECTION

AUGUST 2004

SMALL BUSINESS NETWORK SECURITY GUIDE:

WHY A REAL FIREWALL PROVIDES THE BEST NETWORK PROTECTION

EXECUTIVE SUMMARY

Many small businesses mistakenly believe that a Network Address Translation (NAT) device, which allows networked computers to share a single, public IP address, provides the same network protection as a true firewall. But inexpensive NAT devices, such as routers, were designed to let traffic in to a network, and any security benefits are a side effect.

There is a similar misperception about NAT devices that advertise stateful packet inspection (SPI) functionality. These devices also leave networks vulnerable to attack and don't offer the strength of a fully-integrated firewall/VPN solution.

An integrated security solution employs a layered approach that utilizes both NAT and SPI functionality, is designed specifically for security, and maintains the convenience and flexibility of a low-end NAT device.

WatchGuard® Technologies' Firebox® X Edge line of model-upgradeable firewall/VPN endpoints provides network security for small businesses, remote offices, and telecommuters. It's built exclusively for security and is easy to manage, even for businesses with limited networking experience.

CHANGING HACKER LANDSCAPE COMPROMISES SMALLER BUSINESSES

Only a few short years ago, it was mainly large corporations that depended on Internet connectivity and had to dedicate resources to protect their networks from a small, but destructive community of elite hackers. Nowadays, the threat is much more widespread. Smaller businesses, whose Internet connectivity is often mission-critical, are now regularly attacked by a growing base of less expert hackers with one simple motivation – profit.

Hacking for profit is easy to do. Anyone with some knowledge about how computers work, and the intention to do harm, can download free programs and scripts that do the dirty work automatically. Once in, these programs take control of the compromised computer and run silently in the background, watching what the user types (for example, credit card numbers), stealing processor power, and otherwise wreaking havoc.

If you think your business isn't at risk, look at these statistics. Analysts at Gartner Group* estimate that 40 percent of all small businesses managing their own network security are now hacked every year. They further estimate that more than half of those companies don't realize it until the damage becomes obvious. The FBI reports that the average cost of a network security breach is close to $150,000. Clearly the cost to protect against the probability of attack is far less than the cost of clean up.

Industry analysts now agree: all computers need protection. The issue is: how much is enough?

*Gartner Group, 2004

BUSTING THE NAT MYTH: WHY NAT DOESN'T PROVIDE "FIREWALL-LIKE" SECURITY

Say you wanted to keep your home address private from everyone except friends and family members. If you managed to do that, would you then say, "Keeping my address private makes me completely safe. I no longer have to lock the doors or use a security device." Foolish, right? Yet many businesspeople follow that logic when concluding that a NAT device, such as a router, is a firewall.

Network Address Translation was designed specifically to allow many computers to share a single public IP address, which is the numeric identifier that represents a computer or device on a network. The functionality was developed as a simple solution to the critical shortage of unique IP addresses that came about as worldwide use of the Internet exploded.

NAT works like this: when a piece of transmitted data, called a packet, leaves your network for the Internet, a NAT device replaces all private IP source addresses with one public address. It also hides your private, unregistered network address from the public. Since the NAT box advertises its own address to the world as the source address, all replies from the Internet return to the NAT device. The device then checks an internal table for a match before opening a port and redirecting replies to the appropriate computer inside the network.

So where did the myth come from that NAT devices give the same network protection as a firewall? If an attacker initiates a connection to a network through an obscure port, the NAT device checks the table. If it finds that no one inside the network has requested information on that port, it drops the packet, providing, in this sense, a modicum of security. That's how the myth originated.

But NAT devices weren't designed for security. In fact, their main purpose is to share access to the Internet and let traffic in. Any security benefits provided are side effects. Although these devices are often advertised as providing "firewall-like security," the vendors that make them generally aren't focused on security and don't provide protection against new types of threats. With only a NAT device between a network and the Internet, all computers on that network are vulnerable.

For example, a hacker can send an "anybody there?" message, called a ping, to millions of addresses. Firewalls recognize ping and hide themselves. NAT devices, however, respond, letting the hacker know he's found a live connection and an easy way in to the network.

Interestingly, hackers have developed attacks specifically for NAT devices, including:

- Exploiting open ports. Once a NAT device opens a port by putting it in the NAT table, all traffic destined to that port is allowed through to the local computer identified in the table. Hackers use automated programs to guess which ports NAT has opened, and they keep trying until they get through.

- Taking over the server. Some NAT devices can be configured so that packets not matching anything in the NAT table are sent to a specified computer, such as a server, rather than be discarded. This lets the administrator ensure that good traffic is not lost and that computer applications that wouldn't normally work through NAT can run. But from a security perspective this isn't smart because it allows the NAT device to let everything through. Once a hacker gets control of the server, he can easily access any other computer on the same network.

- Spoof attacks. NAT devices are especially susceptible to spoofing. That's when hackers alter data packets to make it look like they're coming from a valid source. Anyone with sufficient technical knowledge, using hacking tools freely available on the Internet, can put another user's IP address in the "From" (source) field of packets. Since NAT relies on analyzing addresses, false addresses can easily compromise NAT devices.

- Default remote access. Many NAT devices leave a port open to the Internet, which is protected by a password, to allow remote administration. Hackers circulate lists of open ports and the default passwords set by the manufacturers' NAT devices. If the default password protecting the NAT device isn't changed, knowledgeable attackers can log themselves in, reconfigure the device, and take over administrative privileges.

NAT definitely has its place. It's allowed Internet usage to expand quickly, giving millions of people worldwide access to its vast resources. But it's not a security solution.

NAT DEVICES WITH SPI FUNCTIONALITY OFFER ONLY PARTIAL SECURITY

These days many NAT devices are advertised as being firewalls mainly because they include stateful packet inspection (SPI) functionality. Packet inspection means examining where each packet comes from (by IP source address), where it's going (IP destination), and what port it's using. This information helps the device determine whether to allow or deny the packet's passage through the network.

Stateful packet inspection goes a few steps further. It examines more of the packet's delivery information and its conditions, including what port the packet is using, and maintains a sense of context. For example, it examines whether there was a request for the packet and denies it if the packet is false. If the packet is forwarded to the requesting computer, SPI immediately closes the connection – similar to closing a door.

Low-end NAT devices that feature SPI functionality are not true firewalls. In addition, no standard exists for how SPI should be implemented, and the effectiveness of each vendor's solution can vary greatly. While offering more protection than a simple NAT device, NAT devices with SPI are only the beginning of the story.

AN INTEGRATED FIREWALL/VPN SOLUTION IS ROBUST AND SECURE

As safe as stateful packet inspection sounds, there is a lot more that a firewall can, and should, do. Today's firewall uses the best of NAT and SPI functionality and, most important, is designed specifically for security. It focuses on controlling the flow of traffic passing through it, including both inbound and outbound data packets, as well as information passing between separate protected networks.

The best firewall/VPN solution for small businesses uses an integrated, layered approach and provides these significant benefits:

Authenticating connections. A real firewall goes further than only checking the source IP address, destination IP address, and related port numbers to decide if traffic is valid. It also checks, for example, the sequence number of the packet for duplicates or out-of-bound values (hackers try to recycle an existing packet header with different data inside).

Controlling outbound traffic. A real firewall does more than deal with only inbound connections. Firewalls offer egress filtering – the ability to close outgoing connections. Some Trojans (programs containing malicious code) are programmed to infect a machine, then "phone home" to their creator. Egress filtering can help stop this. Similarly, egress filtering can prevent worms (self-replicating viruses) from infecting machines and using them as their next launching pad.

Securely handling special cases. True firewalls support numerous applications that require special treatment, such as Microsoft® NetMeeting and audio/video streaming, and handle them securely without special user requirements. The firewall first identifies the packets as coming from a specific application. It then rewrites and re-routes the packets compatibly with both the application and NAT.

Robust processing power. Inexpensive NAT devices typically don't include the powerful processors required for "deep packet inspection." Even NAT devices with SPI functionality will typically degrade significantly in performance if called upon to inspect each packet. Only devices designed to be a true firewall typically contain the power needed to combine security and performance.

FIREBOX® X EDGE SECURES SMALL BUSINESS NETWORKS

WatchGuard Technologies' Firebox X Edge is a line of model-upgradeable integrated firewalls that can be used as a standalone appliance or as VPN endpoints. Designed specifically for small businesses, Firebox X Edge secures small business networks, remote offices, and telecommuter workstations. It's also easy to manage, even for businesses with limited in-house networking experience.

Firebox X Edge provides the following benefits:

- "Plug-and-play" setup: Intuitive Web-based user interface and quick-start wizards make it easy to set up and configure.
- Fastest performance in its class: Designed to support all network traffic without degrading network performance.
- 10 Ethernet ports: Connects users to networked devices, including printers, fax machines, and servers, quickly and easily.
- Dynamic stateful packet inspection: Delivers commercial-grade security that protects your business and networks.
- Virtual Private Networking (VPN): Extends a secure tunnel from Firebox X Edge to safely connect telecommuters and remote offices.
- Managed desktop antivirus: Provides centrally managed desktop protection against known viruses, web attacks, and WAN failover: Enables a second Internet connection if the primary connection or provider fails.

SUMMARY

There is no question that smaller businesses need to secure their networks – including perimeter remote offices and telecommuters – from attack. Regardless of the vendor you choose, your firewall should – at the very least – control both inbound and outbound traffic.

The best overall solution for a small network is an integrated, layered approach that uses both NAT and SPI functionality. A true firewall solution controls both inbound and outbound traffic, authenticates connections, and includes powerful processors that don't degrade network performance. This type of solution is designed specifically for security, is flexible and easy to manage, and secures the network perimeter.

WatchGuard Technologies' Firebox X Edge is a line of model-upgradeable integrated firewalls that can be used as standalone devices or VPN endpoints. Designed specifically for small businesses, Firebox X Edge offers secure, reliable protection to all computers on the network, including remote office and telecommuter workstations.

ADDRESS:
505 Fifth Avenue South
Suite 500
Seattle, WA 98104

WEB:
www.watchguard.com

E-MAIL:
information@watchguard.com

U.S. SALES:
+1.800.734.9905

INTERNATIONAL SALES:
+1.206.521.8340

FAX:
+1.206.521.8342

ABOUT WATCHGUARD

WatchGuard network security solutions provide small- to mid-sized enterprises worldwide with effective, affordable network protection. Our Firebox line of extendable, integrated security appliances is designed to be fully upgradeable as an organization grows, and to deliver the industry's best combination of security, performance, intuitive interface, and value. WatchGuard Intelligent Layered Security architecture protects against emerging threats effectively and efficiently, and provides the flexibility to integrate additional security functionality and services offered through WatchGuard. Every WatchGuard product comes with an initial LiveSecurity Service subscription to help customers stay on top of security with vulnerability alerts, software updates, expert security instruction, and superior customer care.

FOR MORE INFORMATION

Please visit us on the Web at www.watchguard.com or contact your reseller for more information.

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.

Part. No WGCA66105_0804