

Transparent, Bridging Firewall Devices

Matthew Tanase 2003-10-15

Introduction

There are many tools we use as network and security professionals to build a secure network. Routers, virtual private networks, intrusion detection systems and vulnerability scanners are regularly employed to tackle this challenging task. Many would agree that the foundation of such a defense is the firewall. While the traditional implementation of a firewall as a router works well in most situations, another version can strengthen existing configurations or succeed where its brethren fail. In this article we will examine the concept of a bridging or transparent firewall which sits in-line with the network it protects.

Background

Due to its fundamental and crucial roles in network security, there is little doubt that most of us work with firewalls everyday. As we all know, these devices inspect and filter traffic before making a decision on what to do with a packet. Normally, they have two interfaces - an internal and an external. The external connection sits downstream from a router connected to the Internet. The internal interface usually leads to a local router or private network. Each interface, or network card, has a layer 3 presence or IP address. An incoming packet from the Internet would reach the external interface, where the firewall would handle the packet according to its ruleset. Next the TTL would be decremented, the packet modified accordingly (i.e. NAT) and routed to its destination or next hop. It's easy to think of many firewalls as simple routers with sophisticated filtering techniques. Conversely, routers have simple filtering capabilities.

While this firewall approach is suitable for many situations, it does have some drawbacks.

1. It's not easy to simply 'add' a firewall to a network. The internal and external interfaces require IP addresses and create subnetting issues. The internal hosts need to be configured to see the firewall as the gateway. Additionally, surrounding routers need to recognize the firewall as a hop to the internal network. In short, the potential for several configuration problems or update requirements exist before the device is put in place.
2. Overhead. There is a lot of processing required for each packet: inspection, modification, routing. This in turn either raises hardware costs or hurts performance.

3. Everyone knows it's there. A firewall makes no effort to masquerade itself from the outside world. With a little investigation and the proper enumeration techniques, it's trivial to identify a device that is acting as a firewall. And even if the device itself is extremely secure, the mere fact that it exists and is reachable via the network makes it vulnerable. The software type and version might be revealed based on probing responses. Denial of service floods are very common since they are often the only possible attack against a secure device, such as a firewall. And there's the possibility of mapping the ruleset using firewalking and knowledge of the filtering device.

Such issues are not deal breakers, but headaches for administrators and engineers. So what, if anything, can be done to alleviate some of these shortcomings? Let's take a look.

Transparent firewalls

Since the fundamental task of a firewall is to filter packets, the weak point in its traditional behavior is the fact that it also must route packets after a decision is made. Can the model be simplified? Of course it can, and the answer comes by stepping down a layer in the OSI model. Instead of the device handling packets at layer 3 (network), what if it merely inspected frames and moved them to the proper interface? Sound familiar? This type of device would continue to filter packets, but operate at layer 2 (data link), like a bridge. Such a device has come to be known by several names: a transparent, in-line, shadow, stealth or bridging firewall.

Why a bridge? Unlike a router, which makes packet decisions, a bridge merely moves frames from one interface to the other. It's a much simpler networking device. Before we look at why this might be helpful, let's see why it can be done. Some of the same operating systems that include advanced routing capabilities, such as Linux and OpenBSD, also include bridging capabilities. Data comes in one interface, goes right over to the other and vice versa. Right in the middle of this process however, we can perform the core task of a firewall -- filtering.

What benefits come with the design of a bridging firewall?

1. Zero configuration. From a networking standpoint, there are virtually no changes. How can this be? Easy, the bridging firewall is plugged in-line with the network it is protecting. This means you can put it between two routers, or a router and a switch. You could even put it in front of a single machine. While it might be placed exactly where it should be if it were acting as a gateway or router, it's not. Remember, it merely moves

frames after inspecting them between interfaces. This means that there's no need to make any changes to your existing network. It is completely transparent. No subnetting headaches or configuration updates are required with this device.

2. Performance. Because they are simpler devices, there's less processing overhead. This cost cutting either boosts the capabilities of the machines or allows for deeper examination of the data.
3. Stealth. A key aspect of this device is the fact that it operates at layer 2 of the OSI model. This means the network interfaces have no IP addresses. Such a feature carries more weight than merely ease of configuration. Without an IP address, this device is unreachable and invisible to the outside world. If it cannot be reached, how can anyone attack it? No network probes, denial of service floods or firewalking on this machine. Your attackers won't even know it's in place, silently inspecting everything they send.

With the benefits and strengths of a bridging firewall in mind, let's examine the situations such a device can excel in.

Using transparent firewalls

Bridging devices are most useful in complex environments that require a rapid or new firewall deployment. Using a traditional firewall would require dealing with the mandatory routing changes. As mentioned above, configurations changes to hosts, neighboring routers and the firewall itself will be necessary. In a large or complex network, this will be a difficult, time-consuming task. The use of a bridging firewall reduces both the configuration and deployment time -- a definite plus for any business with limited IT resources.

A transparent, bridging firewall can also be advantageous for companies with several satellite offices or for smaller organizations. Branch and smaller networks often consist of a single WAN connection (T1, business DSL, ISDN) and one simple router. A bridging firewall can be configured by an in-house IT team and shipped to the satellite locations. Since the setups at these offices are often the same, it's likely that one design can be used for many of the networks. The device can be plugged in with zero deployment time at each location. It's a great solution to the challenging task of securing smaller corporate networks. Similarly, smaller companies without a dedicated IT staff can use a consultant to assist in the design and deployment of the firewall. The minimal configuration changes and installation time keep costs down.

Bridging devices can also be used for additional applications. Since the overhead is minimal, we can add an intrusion detection system (IDS) to the machines. The combination of security and networking devices is a hot topic for our community. It's an obvious step, since the devices all analyze the same packets. Right now, you could run an IDS such as Snort on the bridging machine in addition to the firewall. Ultimately, it makes more sense to have a single application processing (bridge or router), filtering (firewall) and analyzing (IDS) the packets. A quick glance at the products emerging from many of the major firewall and IDS vendors will confirm that this is the direction such tools are heading in. Another application to consider using on a bridging device is a sniffer. For many different reasons, it's often necessary to audit and examine the types of packets flowing in and out of a network. An in-line, bridging device is a great place for gathering such data, since it's an invisible gateway for the network. The device can be deployed and removed for analysis with no disruptions, and it becomes a fast and accurate window into our traffic using a simple device.

Getting a Bridging Firewall

Having reviewed these devices and their potential applications, I'm sure some of you would consider using one on your network. Where can you get one? The answer depends on several variables.

The more advanced users and do-it-yourselfers among us should build the device themselves. This can be accomplished with minimal hardware and an open source BSD or Linux package. Both packages have excellent firewalling capabilities. FreeBSD and OpenBSD have bridging features built into the OS. There is an open source project for adding bridging software to Linux. After installing your desired OS and configuring it to act as a bridge, it's simply a matter of designing the desired firewall ruleset -- something you have probably done several times before. A custom setup such as this provides maximum performance and flexibility for a great price -- free!

For those who are already sold on the benefits of a transparent firewall but do want to build such a device themselves, consider a commercial software package. Many of the major firewall vendors already offer enterprise-caliber variants of such devices. For a price, you get excellent setup and configuration features in addition to vendor reliability and support.

If, like many people, you'd like to explore the use of a bridging device on your network, I'd recommend a package such as Hogwash. This open source project, described as an "in-line

packet scrubber" provides a good introduction to such technologies. While it's probably not going to replace your current firewall, it's definitely a great application for testing an in-line device. It's also much easier to setup than building a device from the ground up.

Conclusion

Transparent/bridging firewalls are excellent security tools when used in the right situation. The rapid deployment capabilities and minimal configuration changes make them valuable alternatives to traditional routing firewalls. Such benefits, combined with deep packet analysis and filtering possibilities, are why many claim this is the future of the firewall industry. Soon, we will be managing in-line devices that handle the routing, filtering and analysis of packets for very large networks, reducing the complexity, deployment time and management headaches of the multiple machines required today.

Matt Tanase is President of [Qaddisin](#). His company provides nationwide security consulting services. Additionally, he produces [The Security Blog](#), a weblog dedicated to network security.

View [more articles](#) by Matthew Tanase on SecurityFocus.

Relevant Links

<http://hogwash.sourceforge.net> - homepage for the Hogwash project

<http://www.linux.org> - information center for Linux OS

<http://www.openbsd.org/faq/faq6.html#Bridge> - the OpenBSD FAQ on bridging

<http://www.freebsd.org/.../network-bridging.html> - the FreeBSD FAQ on bridging

<http://bridge.sourceforge.net> - resource for Linux bridging

<http://www.netfilter.org> - Linux OS firewall features

<http://bridge.sourceforge.net/docs/Firewalling%20for%20Free.pdf> - "Firewalling for Free", an

article on bridging firewalls

[Privacy Statement](#)

Copyright 2006, SecurityFocus