



## A ROOKIE'S GUIDE TO DEFENSIVE BLOCKS

When it comes to security, there's no room for error, but many IT pros still end up learning on the job. Here's a 'Firewalls 101' playbook. BY MICHAEL J. DEMARIA

Imagine you park your car in the garage and the engine ignites. If you have a firewall or buffer zone between the toasted car and your house, you're safe—in theory anyway. Same is true with your network. The Internet is a hotbed of hostility, with would-be attackers constantly scanning for exploitable systems. Firewalls and DMZs (demilitarized zones) let you control network traffic so your users get Internet access but attackers are stymied—again, in theory anyway.

The rub is that your firewalls and demilitarized zones must be set up correctly. Sounds simple, and if you're an experienced administrator, it may be. But not everyone charged with guarding a network has these skills. It's with less experienced admins in mind that we present this primer. If you've moved beyond the basics, see previous articles at [www.nwc.com/1214/1214ws1.html](http://www.nwc.com/1214/1214ws1.html), [www.nwc.com/1223/1223f1.html](http://www.nwc.com/1223/1223f1.html) and [www.nwc.com/1310/1310f2.html](http://www.nwc.com/1310/1310f2.html).

### BABY, LET ME IN

Rule No. 1: Firewalls are all about access control. You create a set of rules defining which ports to keep open, which to disallow, and any IP addresses or entire networks to block. A firewall on the edge of your network is effective only if it is configured correctly. And don't forget in-house traffic—firewalls are not just for Internet connections; they should be used to control access from one part of your internal network to another. You never know: That innocent intern at the front desk could be trying to attack your payroll system.

There are three types of firewalls, each with advantages and disadvantages in terms of security and performance:

- » **Packet-filter firewalls.** The simplest firewall is a packet filter. Packet-filter firewalls often are embedded in routers, broadband modems, NAT boxes, advanced switches, traffic shapers and other gear. That's because packet-filter firewalls are simple for vendors to develop, devour few CPUs and have a modest memory overhead. Packet filters inspect traffic one packet at a time with no knowledge of

previous packets; each packet is matched against your rule set. Most commonly, rules are based on source address and port or destination address and port. Some packet-filter firewalls allow for looking at TCP flags, such as SYN packets, but this can get ugly fast, especially if you have to do it by hand. Packet-filter firewalls are useful for filtering out specific traffic types. For example, if you never want SNMP or NetBIOS packets to traverse your border router, use a packet filter.

Packet filters have some major security weaknesses, however. They're susceptible to IP spoofing. They can't see TCP sequencing numbers. And perhaps worst of all, they can't determine if a connection was made from inside or outside. Someone on the outside could send packets with a common source port of 53 (DNS) or 80 (HTTP) and effectively scan the entire internal network.

- » **Stateful packet-filter firewalls.** Stateful packet filters are packet filters that overdosed on Jolt. These firewalls maintain a table that stores the state information of every connection and thus can see when a connection is initiated, handshaking and ending. This is much better than a packet filter from a security standpoint because the firewall can protect against out-of-sequence packets and spoofed TCP connections. Attackers also can't pass packets that falsely appear to be from an existing connection. You could make a single rule to reject all incoming SYN connections and not have to worry much about people scanning or connecting to your network through common spoofing methods.

The downside is that stateful firewalls require lots of CPUs and memory, and as the number of connections grows, so do the processing requirements. When you test stateful firewalls, measuring packets per second alone is not adequate.



## Glossary

### SYN packets:

Initiate the process of establishing TCP connections, which must be made before other packets can be sent.

### Stateful devices:

Monitor all details of sessions in which they are involved. For example, a stateful firewall goes beyond examining an individual packet's header and looks at the entire TCP session.

## WORKSHOP

Instead, you need to look at simultaneous connections on networks with many users or on high-traffic Web sites. A firewall that performs well with a few users may not scale to several thousand.

» **Proxy firewalls.** The proxy is generally the most secure type of firewall because it enforces protocol, though performance is an issue. There are two types of proxy firewalls, application specific (as in protocol, such as HTTP or SMTP) and generic. Generic proxies protect against IP attacks, such as fragmentations and spoofs, but offer no security benefit over stateful packet filters for protocol attacks.

In a proxy, the client and server do not have a direct channel. To the server, the proxy acts as a client, and to

the client, the proxy acts as a server—the proxy is the middleman, passing messages between the two.

Application-specific proxies can inspect traffic, some even at Layer 7, and can check for valid HTTP in Web connections and try to detect exploits, such as buffer overflows. But not all proxies are equally intelligent. Typically, they work only at the protocol level, not all the way into the application layer, and if a proxy is checking only protocol syntax, destructive data payloads could get through. Proxy firewalls also are limited in protocol support; they're usually specialized. Performance is another big concern: Some organizations may want one or more specialized proxies to handle HTTP or FTP traffic and to protect the borders with a stateful firewall.

### CRIMINAL INTENT

Sometimes the job of firewall administration will fall to an engineer who, though good at setting up routers and switches, doesn't have the devious mind-set needed to ferret out the holes in a network. He or she may be confident after installing a firewall and blocking incoming SYN connections. But is the network secure? Not by a long shot. You should limit outbound connections to approved protocols and ports because, for example, some DDoS (distributed denial of service) zombies and other Trojans phone home by connecting to IRC (Internet Relay Chat) servers. If your firewall allows only outgoing HTTP, SMTP and DNS, these Trojans won't cause damage (see "Fireproofing Against DoS Attacks," at [www.nwc.com/1225/1225f3.html](http://www.nwc.com/1225/1225f3.html)).

Be aware, however, that a lot of traffic—legitimate and illegitimate—is running over Port 80. For example, WebDAV (Web-based Distributed Authoring and Versioning) is a protocol that, among other things, lets you mount hard drives remotely. When Apple says WebDAV support is built into the new version of Mac OS X, one of the features touted is that it can work through firewalls.

Another security flaw is having a hole in the network that lets users bypass the firewall. Big offenders here are devices that have modems to allow dial-in administration. Some organizations consider attaching a modem to a computer on the LAN such a security risk that it's punishable by immediate termination. While it may be convenient to dial into a network-monitoring

## SHUNNING THE FIREWALL LEAPERS

Firewalls are a start, but what happens if your antivirus, content-filtering or intrusion-detection systems discover an anomaly or attack attempt? You'll want to ban the attacker from accessing any part of your network. This is where you can take advantage of products that let you shun attackers.

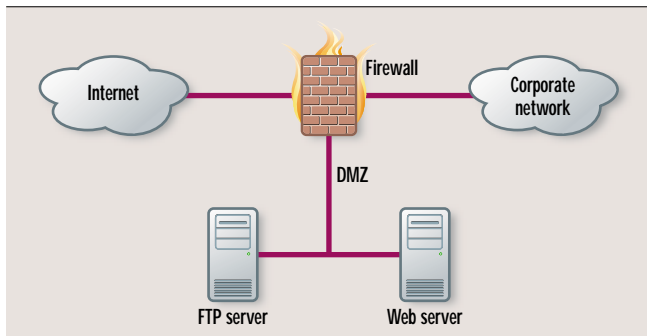
Some IDSs can force rules into the firewall to ban an IP address or entire network, cutting the attacker off. You can do this manually by inserting a *deny x.x.x.x* rule whenever you discover an anomaly. Having an IDS do that for you makes the shunning take effect as soon as an attack is discovered. Shunning capabilities are vendor-dependent. For example, Check Point Software Technologies firewalls can integrate with IDSs that adhere to the OPSEC (Open Platform for Secure Enterprise Connectivity) standard. Check Point created OPSEC to expand its firewalls' capabilities and allow other products to permit or deny traffic. For a guide to IDSs, see [www.nwc.com/1217/1217f2.html](http://www.nwc.com/1217/1217f2.html).

Devices such as ForeScout Technologies' ActiveScout and Tip-

pingPoint Technologies' UnityOne will block traffic to and from internal hosts based on attack signatures. These are not firewalls but active shunning devices that work with your firewall and IDS.

Shunning can have a downside, however; it can lead to a DoS (denial of service) attack. For example, say your IDS shuns when it receives a certain UDP packet. An attacker could conceivably create several thousand spoofed UDP packets sent from every IP address AOL owns. If you're not watching, one person can block your organization from all AOL users—a significant number of Internet users. You need to define carefully what events trigger a shun and for how long. Port and page scans are often innocuous; actively trying to run an exploit like an IIS overflow is not. Dial-up ISPs rotate IP addresses often, and an IP previously used by an attacker may no longer be suspect. Also, attackers coming from behind NAT (Network Address Translation) or NAPT (Network Address Port Translation) boxes can cause entire organizations to be shut out.

## SETTING UP A DMZ



box to see why the corporate Internet connection is down, an attacker could gain access to the LAN if he or she can guess the passwords. This is why you should deploy internal firewalls—the biggest threat to your network likely will come from the inside, be it an outsider with a modem or an untrustworthy employee.

Network-based firewalls also are ineffective when dealing with hostile code. A network firewall by itself can't determine if the traffic passing through it is legitimate or dangerous. But personal firewalls, which shim themselves into the IP stack of an operating system, can monitor traffic closely. Unlike hardware firewalls, personal firewalls have no physical separation between public and private interfaces. The personal firewall software intercepts packets before they are sent out via the network interface and before passing incoming packets up the stack to the application (see "No Desktop Is an Island," at [www.nwc.com/1223/1223f4.html](http://www.nwc.com/1223/1223f4.html)).

There are Trojans whose sole purpose is to capture keystrokes and e-mail them to attackers or broadcast them to IRC channels. Not all Trojan traffic waits for incoming connections

either—some initiate contact with an outside host, even using normal traffic such as HTTP. One advantage of personal firewalls here is that they can look at which application is sending the data, and the better products let you set access rules based not only on ports but on applications. You can, for example, let only Microsoft Internet Explorer and Netscape send data through Port 80. Remember, though, that personal firewalls cannot remove Trojans, and viruses are still a threat, so you need to run antivirus software as well (see "How Trojan Viruses Work: A New Wrinkle," at [www.nwc.com/1223/1223f45.html](http://www.nwc.com/1223/1223f45.html)).

**HALT! WHO GOES THERE?** Say you have a public Web server connected directly to your LAN, and incoming connections are blocked to all machines except the Web server. Sounds good—unless someone takes advantage of an exploit on the server. The attacker then has access to your LAN.

This is where a DMZ comes into play. In the military, a DMZ is a buffer between two warring parties to prevent further incursions or attacks. A DMZ in the IT sense is a

neutral zone protecting a host or network that is assumed vulnerable. You have the public network (the Internet), a private network that you want to protect and a DMZ network, which is reachable from the Internet. Firewalls with DMZ capabilities have a third network interface for this purpose. You can have several DMZs, depending on the features and number of interfaces on your firewall. By restricting traffic in and out of the DMZ, you make it difficult to hop through the firewall.

The theory is that you never want an external user making a direct connection to private internal resources, so the DMZ is a semipublic zone. The DMZ should have only tightly controlled connections to the corporate LAN so if your Web server is violated, the attackers can't reach corporate records.

Sometimes this hard separation is nearly impossible. You may have a Web server that needs to communicate with a back-end database that sits on the LAN. This opens up a way to communicate from the Internet through the DMZ to the LAN. Never assume an attacker won't be able to figure out how your network is laid out. Terminate all remote users in the DMZ, limit access to those areas to which the users need entry rights. All remote users are external users, which means you shouldn't trust them. Also, make sure all hosts in the DMZ are hardened and locked down. Make applications as secure as possi-

ble; the default settings are not necessarily good enough. Finally, check the logs often to detect trends or attacks; DMZs don't make getting into your network impossible, just more difficult.

For more information, see our Survivor's Guide security section, at [www.nwc.com/1226/1226f2.html](http://www.nwc.com/1226/1226f2.html). Remember that securing your network is not a fire-and-forget-it process. Attackers are staying up nights devising ways around your defenses. As Irish orator John Philpot Curran has been paraphrased, "Eternal vigilance is the price of liberty." We'll add, "And of security." **NC**

*Michael J. DeMaria is an associate technology editor based at NETWORK COMPUTING's Syracuse University's Real-World Labs®. Send your comments on this article to him at [mdemaria@nwc.com](mailto:mdemaria@nwc.com).*

## WEB LINKS

» **"Appshield Inspects and Protects Your Web Apps From HTTP to Z"**

(NETWORK COMPUTING, April 15, 2002)  
[www.nwc.com/1308/1308sp1.html](http://www.nwc.com/1308/1308sp1.html)

» **"Seeing to the Health of the Body Corporate"** (NETWORK COMPUTING, April 1, 2002)

[www.nwc.com/1307/1307colmoskowitz.html](http://www.nwc.com/1307/1307colmoskowitz.html)

» **"Simple Measures Cut Viruses Off at the Pass"** (InternetWeek, Sept. 17, 2001)

[www.internetweek.com/enterprise/enterprise091701.htm](http://www.internetweek.com/enterprise/enterprise091701.htm)