

Basic Firewall Theory

A firewall is the wall in a car that protects you from harm when the engine catches fire. At least, that's the definition that confused my mother when I told her I was writing this chapter. In networking, a firewall is a device that prevents certain types of traffic from entering or leaving your network. Usually, the danger comes from attackers attempting to gain access to your network from the Internet, but not always. Firewalls are often deployed when networks are connected to other entities that are not trusted, such as partner companies.

A firewall can be a standalone appliance, software running on a server or router, or a module integrated into a larger device, like a Cisco 6500 switch. These days, a firewall's functionality is often included in other devices, such as the ubiquitous cable-modem/router/firewall/wireless access point devices in many homes.

Modern firewalls can serve multiple functions, even when they're not part of combination devices. VPN services are often supported on firewalls. A firewall running as an application on a server may share the server with other functions such as DNS or mail, though generally, a firewall should restrict its activities to security-related tasks. The Cisco Adaptive Security Appliance (ASA) is a firewall that is bundled with other security features like VPN and IDS/IPS.

Best Practices

One of the things I tell my clients over and over is:

Security is a balance between convenience and paranoia.

We all want security. If I told you that I could guarantee the security of your family, wouldn't you jump at the chance? But what if I told you that to achieve this goal, I needed to put steel plates over all the windows in your home, replace the garage door with a brick wall, and change the front door to one made of cast iron? You might reconsider—it wouldn't be very convenient, would it? Companies also often want a

high level of security, but like you, they may not be willing to give up too many conveniences to achieve it.

A while ago, I was working as a consultant in Manhattan for a large firm that was having security problems. We gave them some options that we knew had worked for other organizations. These were the responses we received:

One-time password key fobs

“We don’t want that—the key fobs are a pain, and it takes too long to log in.”

VPN

“We like the idea, but can you make it so we don’t have to enter any passwords?”

Putting the email server inside the firewall

“Will we have to enter more than one password? Because if we do, forget it.”

Password rotation

“No way—we don’t want to ever have to change our passwords!”

Needless to say, the meeting was a bit of a challenge. The clients wanted security, and they got very excited when we said we could offer them the same level of network security that the big banks used. But the minute they realized what was involved in implementing that level of security, they balked—they balked at the idea of any inconvenience.

More often than not, companies do come to an understanding that they need a certain level of security, even if some conveniences must be sacrificed for its sake. Sadly, for many companies, this happens only after their existing security has been compromised. Others may be forced into compliance by regulations like Sarbanes-Oxley and PCI.

If you find yourself designing a security solution, you should follow these best practices:

Simple is good

This rule applies to all of networking, but it is especially relevant for security rules. When you are designing security rules and configuring firewalls, keep it simple. Make your rules easy to read and understand. Where applicable, use names instead of numbers. If your firewall has 60,000 rules in it, I’d be willing to bet you’ve got holes. And yes, there are plenty of firewalls out there with tens of thousands of rules.

Monitor the logs

You must log your firewall status messages to a server, and you must look at these messages on a regular basis. If you have a firewall in place and you’re not examining the logs, you are living with a false sense of security. Someone could be attacking your network right now and you’d have no idea. I’ve worked on sites that kept buying more Internet bandwidth, amazed at how much they needed. When I examined their firewall logs, I discovered that the main bandwidth consumers were warez sites that hackers had installed on their internal FTP servers. Because no one looked at the logs, no one knew there was a problem.

Deny everything; permit what you need

This is a very simple rule, but it's amazing how often it's ignored. As a best practice, this has got to be the one with the biggest benefit.

In practical terms, blocking all traffic in both directions is often viewed as too troublesome. This rule should always be followed to the letter on inbound firewalls—nothing should ever be allowed inbound unless there is a valid, documented business need for it. Restricting all outbound traffic except that which is needed is also the right thing to do, but it can be an administrative hassle. Here is a prime example of convenience outweighing security. On the plus side, if you implement this rule, you'll know that peer-to-peer file sharing services probably won't work, and you'll have a better handle on what's going on when users complain that their newly installed instant messenger clients don't work. The downside is that unless you have a documented security statement, you'll spend a lot of time arguing with people about what's allowed and what's not.

The default behavior of many firewalls, including the Cisco PIX and ASA, is to allow all outbound traffic. Restricting outbound traffic may be a good idea based on your environment and corporate culture, though I've found that most small and medium-size companies don't want the hassle. Additionally, many smaller companies don't have strict Internet usage policies, which can make enforcing outbound restrictions a challenge.

Everything that's not yours belongs outside the firewall

This is another simple rule that junior engineers often miss. Anything from another party that touches your network should be controlled by a firewall. Network links to other companies, including credit card verification services, should never be allowed without a firewall.

The corollary to this rule is that everything of yours should be inside the firewall (or in the DMZ, as described in the next section). The only devices that are regularly placed in such a way that the firewall cannot monitor them are VPN concentrators. VPN concentrators are often placed in parallel with firewalls. Everything else should be segregated with the firewall. Segregation can be accomplished with one or more DMZs.



Firewalls get blamed for everything. It seems to be a law of corporate culture to blame the firewall the minute anything doesn't work. I believe there are two reasons for this. First, we naturally blame what we don't understand. Second, a firewall is designed to prevent traffic from flowing. When traffic isn't flowing, it makes sense to blame the firewall.

The DMZ

Firewalls often have what is commonly called a *DMZ*. DMZ stands for demilitarized zone, which of course has nothing to do with computing. This is a military/political

term referring to a zone created between opposing forces in which no military activity is allowed. For example, a demilitarized zone was created between North and South Korea.



Using military nomenclature is common in the computing world. From demilitarized zones to Trojan horses to network warriors, we seem to love to militarize what we do, if only in name.

In the network security realm, a DMZ is a network that is neither inside nor outside the firewall. The idea is that this third network can be accessed from inside (and probably outside) the firewall, but security rules will prohibit devices in the DMZ from connecting to devices on the inside. A DMZ is less secure than the inside network, but more secure than the outside network.

A common DMZ scenario is shown in [Figure 27-1](#). The Internet is located on the outside interface. The users are on the inside interface. Any servers that need to be accessible from the Internet are located in the DMZ network.

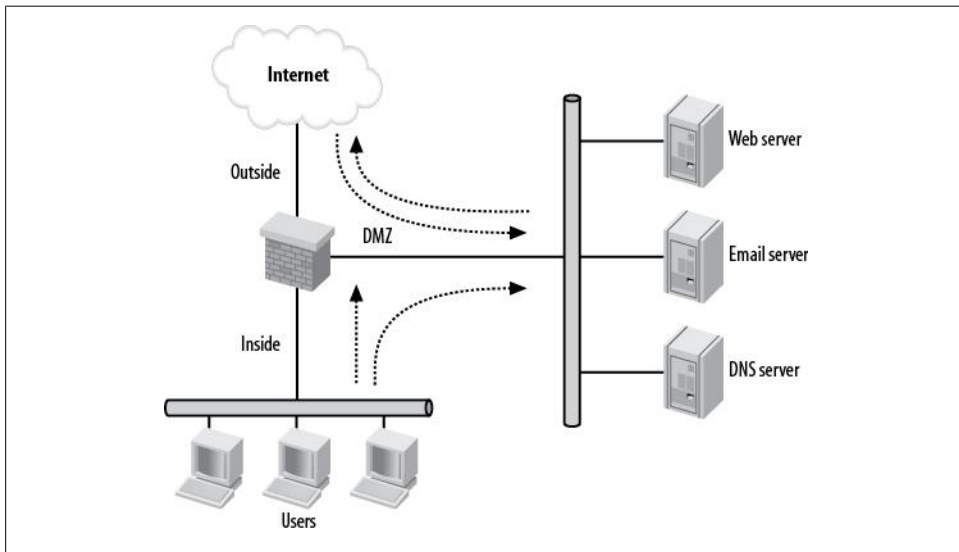


Figure 27-1. Simple DMZ network

In this network, the firewall should be configured as follows:

Inside network

The inside network can initiate connections to any other network, but no other network can initiate connections to it.

Outside network

The outside network cannot initiate connections to the inside network. The outside network can initiate connections to the DMZ.

DMZ

The DMZ can initiate connections to the outside network, but not to the inside network. Any other network can initiate connections into the DMZ.

One of the main benefits of this type of design is isolation. Should the email server come under attack and become compromised, the attacker will not have access to the users on the inside network. However, in this design, the attacker *will* have access to the other servers in the DMZ because they're on the same physical network. (The servers can be further isolated with Cisco Ethernet switch features such as private VLANs, port ACLs, and VLAN maps; see [Chapter 25](#) for more information.)

Servers in a DMZ should be locked down with security measures as if they were on the Internet. Rules on the firewall should be configured to allow services only as needed to the DMZ. For example:

Email server

POP, IMAP, and SMTP (TCP ports 110, 143, and 25) should be allowed. All other ports should not be permitted from the Internet.

Web server

HTTP and HTTPS (TCP ports 80 and 443) should be allowed. All other ports should be denied from the Internet.

DNS server

Only DNS (UDP port 53, and, possibly, TCP port 53) should be allowed from the Internet. All other ports should be denied.

Ideally, only the protocols needed to manage and maintain the servers should be allowed from the managing hosts inside to the DMZ.

Another DMZ Example

Another common DMZ implementation involves connectivity to a third party, such as a vendor or supplier. [Figure 27-2](#) shows a simple network where a vendor is connected by a T1 to a router in the DMZ. Examples of vendors might include a credit card processing service or a supplier that allows your users to access its database. Some companies even outsource their email system to a third party, in which case the vendor's email server may be accessed through such a design.

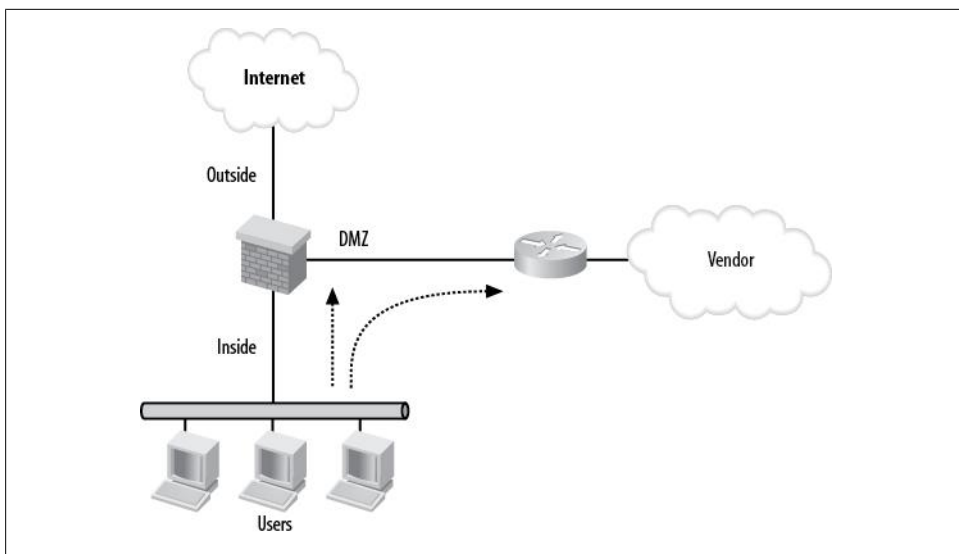


Figure 27-2. DMZ connecting to a vendor

In a network like this, the firewall should be configured as follows:

Inside network

The inside network can initiate connections to any other network, but no other network can initiate connections to it.

Outside network

The outside network cannot initiate connections to the inside network or to the DMZ. The inside network can initiate connections to the outside network, but the DMZ cannot.

DMZ

The DMZ cannot initiate connections to any network. Only the inside network can initiate connections to the DMZ.

Multiple DMZ Example

The real world is not always as neat and orderly as my drawings would have you believe. The examples I've shown are valid, but larger companies have more complicated networks. Sometimes a single DMZ is not enough.

Figure 27-3 shows a network with multiple DMZs. The design is a combination of the first two examples. Outside is the Internet, and inside are the users. DMZ-1 is a connection to a vendor. DMZ-2 is where the Internet servers reside. The security rules are essentially the same as those outlined in the preceding section, but we must now also consider whether DMZ-1 should be allowed to initiate connections to DMZ-2 and vice versa. In this case, the answer is no.

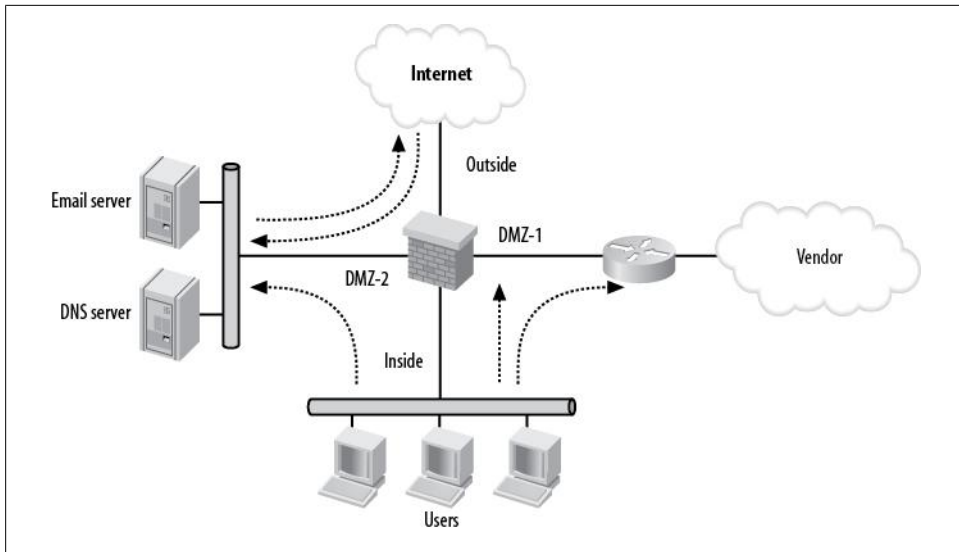


Figure 27-3. Multiple DMZs

The firewall should be configured as follows:

Inside network

The inside network can initiate connections to any other network, but no other network can initiate connections to it.

Outside network

The outside network cannot initiate connections to the inside network or to DMZ-1. The outside network can initiate connections to DMZ-2.

DMZ-1

DMZ-1 cannot initiate connections to any other network. Only the inside network can initiate connections into DMZ-1.

DMZ-2

DMZ-2 can initiate connections only to the outside network. The outside network and the inside network can initiate connections to DMZ-2.

Alternate Designs

The Internet is not always the outside interface of a firewall. Many companies have links to other companies (parent companies, sister companies, partner companies, etc.). In each case, even if the companies are related, separating the main company from the others with a firewall is an excellent practice to adopt.

Figure 27-4 shows a simplified layout where Your Company's Network is connected to three other external entities. Firewall A is protecting Your Company from the Internet, Firewall B is protecting Your Company from the parent company, and Firewall C is protecting Your Company from the sister company.

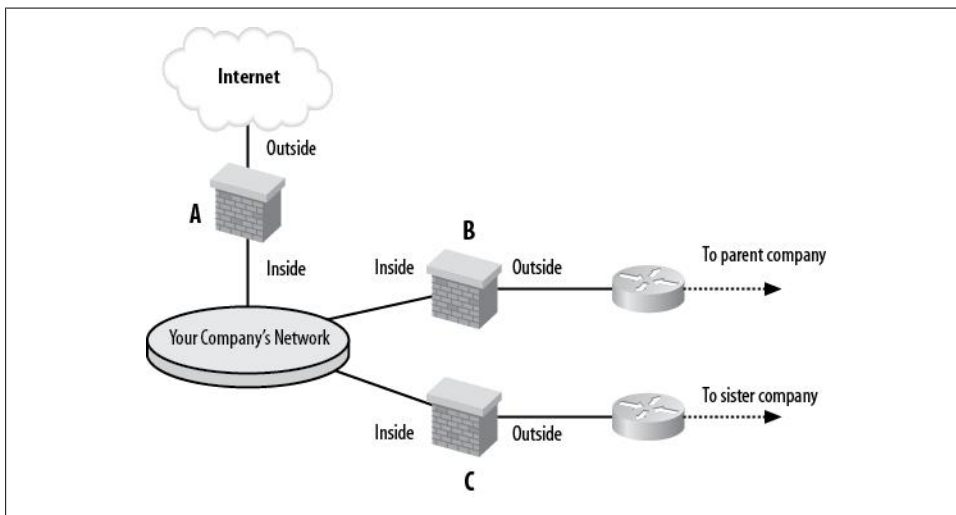


Figure 27-4. Multiple firewall example

Each firewall has an inside and an outside interface. While each of the firewalls' inside interfaces are connected to the same network, the outside interfaces are all connected to different networks.

Firewalls are also often used in multitiered architectures like those found in ecommerce websites. A common practice is to have firewalls not only at the point where the website connects to the Internet, but between the layers as well. Figure 27-5 shows such a network.

In a layered design like this, one firewall's inside network is the next firewall's outside network. There are four firewalls connected to the balancing layer. The top two, a failover pair, connect the balancing layer to the Internet layer. To these firewalls, the balancing layer is the inside network. The bottom two firewalls (another failover pair) connect the balancing layer to the web layer. To these firewalls, the balancing layer is the outside network.

Firewalls are another building block in your arsenal of networking devices. While there are some common design rules that should be followed, such as the ones I've outlined here, the needs of your business will ultimately dictate how you deploy your firewalls.

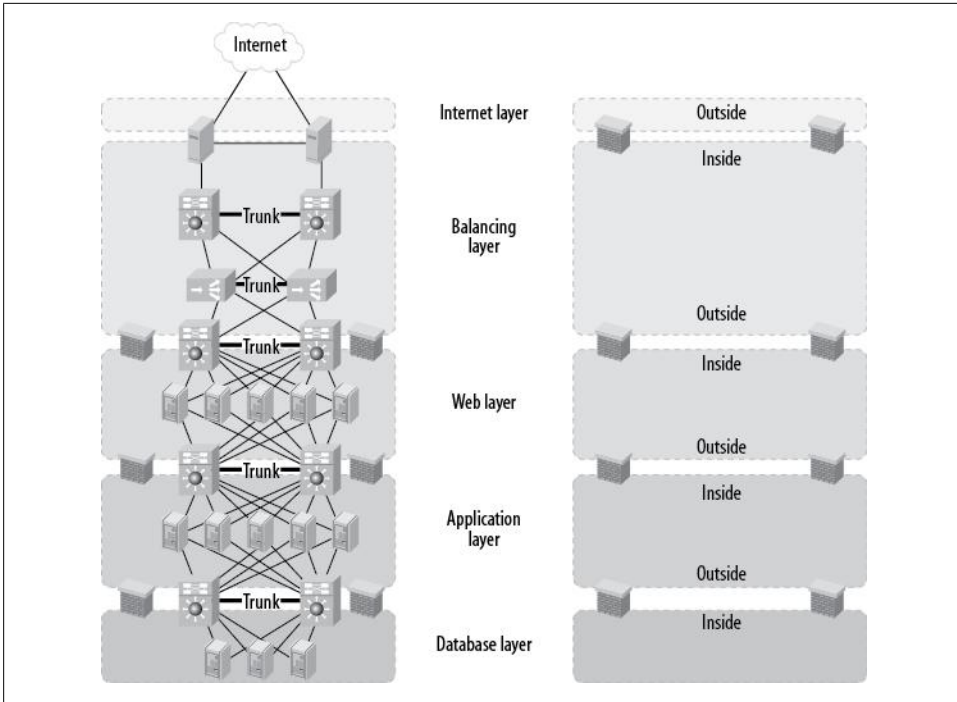


Figure 27-5. Ecommerce website