An Overview of Firewalls

CIT 233

Oliver Garraux
11/14/2008

Purpose

A firewall is a device or piece of software that is used in computer networks to aid in preventing unauthorized access to network resources. They help to secure the devices attached to the network. In general, a firewall inspects and filters network traffic based on characteristics of the traffic. Many times, firewalls are placed between other network devices so traffic is forced to go through them, though there are also personal firewalls that protect just a single computer.

Background

Computer networks consist of many different components and devices that interact together. They interact by using **protocols**, which are rules that dictate how different devices should communicate. One common protocol that all devices used on a daily basis is IP (Internet Protocol), which allows network devices to communicate with other networks.

When network devices communicate, they do not do so in continuous streams of data. Instead, they are packet-switched, meaning that each communication is broken into small chunks called **packets**, which are individually delivered to their destination.

OSI Model

When an application on one device sends data, the data goes through the **OSI Model**. The OSI Model refers to different layers that the data goes through, from the application on the computer, all the way down to the physical medium that the data is actually transmitted on.

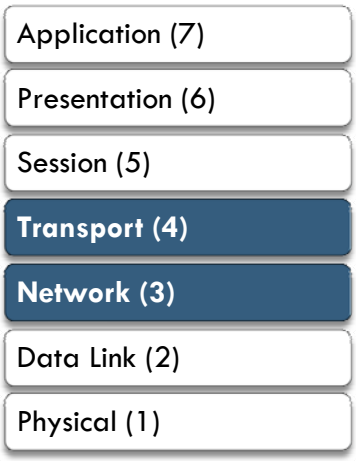

Figure 1 - Layers 3 and 4, Network and Transport respectively, are of the most importance when talking about firewalls.

There are seven layers in the OSI Model. Each of the protocols that a device uses to send or receive packets is part of one of these seven layers. For example, IP, which was mentioned above, works at Layer 3 (the network layer). The two layers that firewalls most commonly work with are the transport and network layers.

Without going into too much unnecessary detail, the network layer is responsible for getting the data to the right computer on the right network. The network layer uses IP (Internet Protocol) and **IP addresses** to accomplish this. Each packet has a source IP address (the IP address of the device sending the packet) and a destination IP address (the IP address of the device that the packet is being sent to). One caveat with the network layer is that most home and many business networks use network address translation. Network address translation, or NAT, lets multiple computers share a single IP address on the Internet by assigning them with private addresses that can only be used internally. This prevents the computers from being directly accessed from the Internet by default. How NAT works will be covered in more detail later on.

Ports and Applications

The transport layer is responsible for getting the traffic to the right application running on the destination computer. Two primary protocols are used in the transport layer: TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). Both of these protocols use **ports** for addresses. Computer applications use ports to send and receive data. Each packet has a source and a destination port. The source port is the port that the application sending data

uses; the destination port corresponds to the application that is receiving data. For example, a webserver usually listens on port 80, waiting to receive data from any web browsers that connect to it.

TCP is more common than UDP. It is a connection-oriented protocol; when a device begins communicating using TCP, a connection is established and the software on each device keeps track of what port number on one device is communicating with what port on the other device. UDP is much less common and is connectionless. This makes it somewhat less secure – the computer looks at the UDP packets it receives individually and not as a part of a connection, so it is easier for an attacker to forge them.

To expand a little more on the webserver example, when a web browser connects to a web server to access a website, it connects to port 80 by default – if the web server is using another port, the person using the web browser must explicitly specify it. The port that the web browser uses to send data *from* does not matter. The computer chooses a random port number for that. The webserver will send its response to the port that the web browser has connected from. Figure 2 illustrates an example of how this works. The web browser sends a packet, using a random port (49240) as a source port, and 80 as a destination port. The webserver then replies, using 80 as its source port, and sending the packet to port 49240 for the web browser.

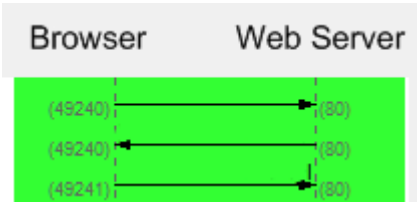

Figure 2 - A browser connects to a web server. The port numbers are in parenthesis, and each line represents a single packet, with the arrow showing where it is sent from/to.

In addition to port 80, many other port numbers have been assigned to particular protocols. Port 25 is assigned to SMTP, and is used for sending emails. Many Internet service providers use firewalls to block their subscribers' computers from connecting to any mail server on port 25 other than the ISP's. This is an effort to block people from sending spam. A table of the most common protocols and port numbers is listed below.

In particular, ports 135 to 139, and port 445 are important to pay attention to. They are used by Windows to share files, which is useful between computers on a local network, but it poses a major security risk if it is accessible from the Internet (Petri). Therefore, a firewall should be used to ensure that traffic from the Internet destined for these ports on local computers is blocked.

Table 1- Common Port Numbers

Port Number	Protocol Name	Use
21	FTP (File Transfer Protocol)	Used to transfer files
25	SMTP (Simple Mail Transfer Protocol)	Used to send emails
80	HTTP (Hypertext Transfer Protocol)	Used to access websites
110	POP3 (Post Office Protocol)	Can be used to receive emails
135-139	NetBIOS	Windows File Sharing
143	IMAP (Internet Message Application Protocol)	Another way to receive emails
443	HTTPS (Hypertext Transfer Protocol – Secure)	Encrypted version of HTTP
445	NetBIOS	Windows File Sharing
993	IMAPS (Internet Message Application Protocol – Secure)	Encrypted version of IMAP

How Firewalls Work

Rules

A firewall filters network traffic based on rules that the user configures. Either a rule can block a particular kind of network traffic, or it can allow it.

Firewalls can be operated in two different general styles. The first is **allow-by-default**. Allow-by-default permits all traffic, unless there is a rule specifically forbidding it. This is less secure, but it is less likely to accidently impact any legitimate applications.

The second style is **deny-by-default**. With deny-by-default, the firewall blocks all traffic unless there is a rule specifically permitting it. This is a more secure option because only the traffic that has been purposely allowed will be allowed through. However, it is much more likely that some legitimate traffic will be blocked, potentially causing problems.

Filtering by Traffic Characteristics

To make decisions on whether to allow or deny a particular packet, a firewall will compare the packet with each of the rules it has. A firewall's rules use characteristics of the packet to match the particular packets to which it should apply. The most common characteristics are the source and destination IP address, along with the source and destination port number. Some firewalls may use other characteristics as well, such as the domain name of the website a user is visiting, but these are more advanced features that go beyond what a traditional firewall does. It is becoming more common to see these features on devices designed for small businesses though.

On most firewalls, the first rule that matches the packet is the rule that the firewall will use. If, for example, there is a rule at the beginning of the list that blocks all packets, then all of the packets will be blocked, even if other rules further down the list would allow some of those packets through. When configuring a firewall, always pay attention to the order of the rules, because it does make a difference.

Below is an example of a few firewall rules from a Cisco router. The exact syntax of the commands is not as important as what each rule is actually doing.

```
1  permit tcp 10.1.2.0 0.0.0.255 host 192.168.1.10 eq 25
2  permit tcp 10.2.3.0 0.0.0.255 host 192.168.1.10 eq 25
3  deny tcp any host 192.168.1.10 eq 25
```

In the example above, the black text determines whether the rule is for allowing or blocking traffic, the green text represents the source IP address, the blue text represents the destination IP address, and the orange text represents the destination port number.

The first two lines in the example permit traffic from certain IP addresses (the networks 10.1.2.0 and 10.2.3.0) to connect to the mail server (on port 25 at the computer with address 192.168.1.10). The bottom line blocks all other traffic that is trying to get to the mail server. The net effect of the firewall rules is to limit access to the mail server to computers on the networks 10.1.2.0 and 10.2.3.0. The rules that permit access from certain networks are put first because the firewall evaluates the rules in order. If the deny rule was put at the top, all of the traffic would be denied because the first rule would match all of the traffic and block it.

Network Address Translation

Network address translation (NAT) is technically not just a function of a firewall. Most routers are capable of doing NAT as well. However, most firewalls (and consumer-oriented routers) will use NAT by default.

As was mentioned earlier, NAT lets a single Internet-facing IP address be shared between multiple computers on a local network by giving the computers private IP addresses. This means that the computers cannot be directly accessed from the Internet using their private IP addresses. This poses a problem when those computers need to communicate with a website, or any other Internet service. The local computers behind NAT *are* able to send packets to external IP addresses. The device performing the NAT keeps track of the outgoing connections that local computers make by using Port Address Translation (PAT). PAT keeps track of which source ports the router has sent requests out on. The router will also modify the packets that it sends out, to change the source IP address on them from the local computer's private IP address (which the web server would not be able to reach) to the Internet-facing public IP address that the router or firewall doing the NAT has. Therefore, when the web server responds, it will respond to the router/firewall. When the router or firewall sees a response on one of the connections it is tracking, it modify the packet again, this time changing the destination address from the router/firewall's Internet-facing IP address, to the local computer's private IP address. It uses PAT again to determine which internal computer it should forward the response to, based on the TCP or UDP port on the router the Internet server responded to (Cisco Systems).

One advantage of using NAT from a security perspective is that it prevents worms and other malware on the Internet from directly contacting and infecting computers on the local network. It also hides all of the local computers behind one address, which limits the amount of information a potential attacker can obtain about the local network. While NAT is not a replacement for a firewall, it is a good feature to use, with a true firewall or even with just a normal router.

Types of Firewalls

Dedicated Firewall

There are two different types of firewalls. The first is a dedicated (or hardware) firewall device. A hardware firewall acts as a device on a network. It is usually installed between two different networks, such as between a local area network and an Internet connection. It then can filter all of the traffic going between the Internet and the computers on the local network. While they are many times called hardware firewalls, the term dedicated firewall is more accurate. All "hardware" firewalls will use software, but the software will just be running on hardware dedicated to running the firewall.

One of the largest makers of dedicated firewalls is Cisco Systems. In addition to making routers and switches, Cisco makes PIX firewalls and ASA security devices. Most of Cisco's routers can act as firewalls as well, using Access Control Lists (ACL's), which are simply sets of firewall filtering rules. Cisco's PIX firewalls are traditional firewalls, though Cisco seems to be phasing them out and pushing customers more towards their new ASA series. The ASA series can do all of the traditional firewall tasks that the PIX can, but they can also handle higher-level security related tasks. ASA series devices can do antivirus filtering and work as an Intrusion Prevention System (IPS) to detect and automatically stop attacks that make it through the firewall rules (Davis, 2007). The ASA devices are a great example of where firewalls are going in the future. They are getting smarter, and will be able to work at the upper layers of the OSI model, basing filtering decisions on more than just the network and transport layer addresses. Many times these features are known as an "application firewall" because they can operate at the application layer

of the OSI model. Cisco's newer devices can be configured through a graphical interface, though knowledge of the command line interface is still beneficial.

Other business-class firewall manufacturers include Sonicwall, and Fortinet. They both offer application layer firewalls for small and medium businesses that are comparable to Cisco's ASA series devices. Manufacturers of consumer network device such as Linksys, Netgear, and Dlink all make easy to configure firewall type devices for home users. While they may lack the powerful command line interface and configurability that Cisco's and other business-grade firewalls provide, they are perfectly capable of providing security for home networks with a few desktop or notebook computers.

Many hardware firewalls, especially ones that have application firewall features, are licensed on a per-user basis. For example, some of Cisco's ASA models made for small businesses limit the number of local IP addresses they will let through. However, hardware firewalls are truly the best way to protect an entire network from attacks. Even if all of the computers on the network have software firewalls, having a dedicated firewall to protect the entire network makes it easier to stop attackers from outside the organization.

Software Firewall

The second type of firewall is a software, or personal firewall. A personal firewall is usually just a piece of software that installs on a computer. The most common software firewall for Windows systems is the Windows Firewall, which is included in Windows XP SP2 and higher. It was previously called Internet Connection Firewall, and is substantially improved in Windows XP Service Pack 2 (Microsoft Corp., 2004).

Windows Firewall can be configured from the Control Panel using the Windows Firewall applet. From the Control Panel applet, a user can define exceptions, which allow specific programs to receive connections through the firewall on particular ports. This demonstrates one of the advantages of software firewalls. Because they are running on the end user's system, they can base their filtering on more than simply characteristics of the network traffic. They can filter traffic based on the computer program that is trying to communicate as well. A second advantage of software firewalls is that they still provide protection even when the computer is connected to a public network, such as a wifi hotspot, or university's network.

Windows Firewall in Vista has several major improvements over the Windows XP SP2 version. The version in Windows XP will only filter incoming connections. In other words, it can block attempts by other computers to connect to the computer its running on, but it cannot block a program (even a malicious one) from opening a connection to another computer (Huitema, 2004). In Vista, Windows Firewall can filter outgoing connections as well (though it does not do so by default). The user interface through the Windows Firewall Control Panel applet is similar to what it was in XP. However, Vista also offers a much more powerful interface to manage the firewall through the Windows Firewall with Advanced Security MMC snapin (Bott, 2006). Inbound and outbound rules can be defined through the MMC snapin. The new interface offers more granularity in specifying the characteristics of the traffic to filter. Traffic can be filtered based on the program, source/destination port number, and source/destination IP address. It is also possible to define different profiles to use when the computer is on public and private networks.

There are many other third party software firewalls available for Windows. One of the most popular ones is ZoneAlarm. While it is widely used, ZoneAlarm has a history of causing errors in some applications, even while disabled. In the past, Sygate Personal Firewall was a very well respected firewall for Windows. Unfortunately, Symantec purchased Sygate and discontinued their consumer products in 2005 (Evers, 2005). Still, there are many third party software firewalls available for Windows. Symantec offers a personal firewall as part of their Norton 360 package, and Agnitum continues to offer their personal firewall product, Outpost (Gann, 2008). Typically,

Windows Firewall should be disabled if a third party software firewall is being used, to ensure that they do not conflict. However, running a personal firewall on end users' computers while having a dedicated firewall protecting the whole network is not only possible, but a good idea.

There are many web-based port scanners available to test a firewall after it has been installed. A port scanner is a program that tries to connect to many different ports on a computer to see which ones are being blocked by a firewall. A web-based port scanner is simply a website that will scan a computer and display which ports the firewall on that computer is or is not blocking. There are many different websites that will do this. One of the better known ones is ShieldsUP, but many others can be found by searching. Testing a firewall is helpful to make sure that it is really doing what it should be.

Conclusion

In summary, firewalls play a vital role in protecting computers and computer networks from attack. They filter network traffic based on the source and destination addresses that each packet has. The two types of addresses that most firewalls look at are the IP address (identifies a computer), and the port number (identifies an application on a computer). A firewall decides whether to allow or block a packet by evaluating a series of rules that a user has configured to see if the packet matches the characteristics that a rule specifies. A firewall may be a dedicated network device that filters network traffic for an entire network for computers, or it may be a piece of software installed to protect a single personal computer. Many times it is advantageous to use both to provide defense in depth.

Bibliography

Bott, E. (2006, January 14). *Windows Vista to include two-way firewall*. Retrieved November 9, 2008, from Ed Bott's Windows Expertise: http://www.edbott.com/weblog/?p=1219

Cisco Systems. (n.d.). *Cisco IOS Network Address Translation Overview*. Retrieved November 9, 2008, from Cisco Technology White Papers: http://www.cisco.com/en/US/technologies/tk648/tk361/tk438/technologies_white_paper09186a0080091cb9.html

Davis, D. (2007, February 01). *Cisco administration 101: Learn the difference between PIX and ASA*. Retrieved November 12, 2008, from TechRepublic: http://content.techrepublic.com.com/5100-10878_11-6155407.html

Evers, J. (2005, November 28). *CNET News*. Retrieved November 11, 2008, from Symantec scraps Sygate consumer firewall: http://news.cnet.com/Symantec-scraps-Sygate-consumer-firewall/2100-7350_3-5974230.html

Gann, R. (2008, April 23). *Agnitum Outpost Pro Security Suite 2008 Review*. Retrieved November 13, 2008, from PC World: http://www.pcworld.idg.com.au/index.php/taxid;2136212919;pid;5317;pt;1

Huitema, C. (2004, August 14). *The Windows XP/SP2 Firewall*. Retrieved November 10, 2008, from Christian Huitema: http://www.huitema.net/sp2-firewall.asp

Microsoft Corp. (2004, August 4). *Understanding Windows Firewall*. Retrieved 11 3, 2008, from Microsoft: http://www.microsoft.com/windowsxp/using/security/internet/sp2_wfintro.mspx

Petri, D. (n.d.). *What's TCP port 445 used for in Windows 2000/XP?* Retrieved November 10, 2008, from Petri IT Knowledgebase: http://www.petri.co.il/what%27s_port_445_in_w2k_xp_2003.htm