Cryptography and Network security II
Second Course

Lecture 10: **Security: Firewall/Proxy Server**

Table of contents:

Introduction

The Internet is the world's most fertile medium for spawning attacks against the networks connected to it. In security parlance the Internet is a threat multiplier, a system that multiplies the security risks already associated with networking. There are plenty of clever people consider it great sport to try to breach any security measures-the better your security, the better challenge to them. For example, computers at the U.S. Defense Department were attacked an estimated 250,000 times in 1997, according to the U.S. General Accounting Office. At the same time the lure of commercial opportunity and the temptation to mine its vast lode of information are enormous.

Firewalls

For many organizations that would like to connect to the Internet, finding the right comfort level of connectivity is their core of issue. That level of connectivity ranges from total openness to a totally closed system. The national Computer Association estimates that less than 1 percent of companies connected to the Internet have some sort of firewall protections device in place. Put another way, 99 companies in 100 are totally open. No wonder then that we read so many stories of Internet break-ins in the mass media

Firewalls types

Many people have heard or believe that a firewall prevents unauthorized and improper transit of access and information from one network to another. The choice of the term firewall is unfortunate, because it leads one to think of a sample, unreachable barrier. This notion goes beyond simplistic-it is genuinely naïve and even dangerous to think of any firewall in this way.

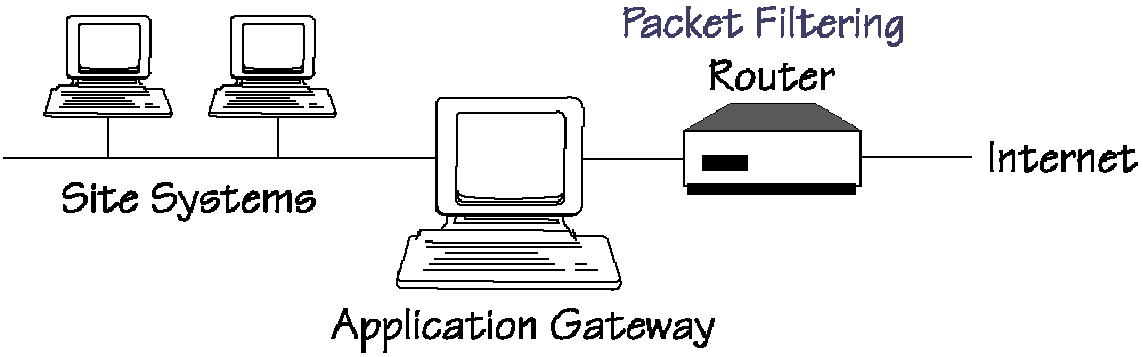
A firewall is combination of software and hardware used to keep unauthorized individuals from accessing a private LAN. Firewalls usually run on dedicated high-performance networked workstation residing outside the LAN inside the router link to the Internet.

Firewalls are successful only when they implement a predefined security plan. A properly chosen, configured, and maintained firewall can keep unwelcome guests from logging on to your network and using its applications, servers, and other resources.

Some firewall configurations have an inherent weakness. If an attacker succeeds in piercing a single firewall, notably a packet-filtering firewall, they than have total access to your system. This violates our perimeter rule in which we use increasingly stronger defenses as we approach the core

information of resource sought. We use attrition to filter out, in stages, those who do not have permission to go any higher. Indirectly we also establish security levels appropriate to our user community.

The all-or-nothing nature of a single firewall is solved by the use of several firewall devices in tandem. Dual-homed gateway firewalls, screened host firewalls, and screened subnet firewalls al have multiple barriers to eliminate the all-or-nothing aspect provided by a single firewall. Firewall components usually contain one or more of three repellent techniques: packet filtering, proxy server, and circuit sources. However, this chapter will introduce the first two techniques.



Advantages and Disadvantages of Firewall

Advantages	**Disadvantages**
Reduces the risk of security breaches	Vendor software upgrades can degrade the effectiveness of filtering
Reduces time spent coping with the result of intrusions: viruses, corrupted data, stole files	If short on Internet savvy, a conservative approach is necessary
Reduces cost to and potential disruption of the business	Desirable or convenient services can become unavailable due to the context problem in filtering
Minimizes legal and financial exposure	Complexity reduces security
Avoids the irony of implicitly sponsoring attackers by giving them access to your computing resources	Hardware, software and maintenance costs
Allows access to Internet resources and business opportunities	Software maintenance and upgrade costs
Is one answer to Internet access versus the need for privacy	Initial setup and ongoing administrative costs
If well executed, gives attackers nervous breakdowns and sends them somewhere else	Lost business due to a broken or malfunctioning firewall

Packet filter firewalls

A router usually performs packet filtering as data packets pass through the router's interfaces. The filter reads fields in Internet Protocol (IP) packets such as source and destination IP addresses and TCP/User Datagram Protocol source and destination ports. By checking these fields, the packet filter can allow passage of trusted packets or disallow passage of packets from unauthorized sources.

Packets filtering, when installed on routers, turn the routers into firewall routers. Firewall routers should do no routing, but sometimes do anyway. Packets not explicitly allowed are discarded. Filtering can take place in your own firewall router, your Internet network service provider's router connection to you, or both.

Fields alone in the TCP/IP protocol are inadequate to provide the level of resolution often needed, e.g., "allow this but not that" within an application. For instance, while it is possible or File Transfer protocol, it is not possible to allow the GET function of the FTP while disallowing the PUT function when filtering is used. The entire protocol must be allowed or not. Filtering TCP segments is difficult, but doing the same for User Datagram Protocol messages is nearly impossible because UDP offers essentially no context.

Packet filters do not copy well with FTP or Domain Name Service. For example, it is easy to falsify an outgoing message into an allowed form to get through the filter. In sum, packet-filtering firewalls are good at looking at routing information, but they cannot see into the application where the need and control possibilities are greatest. Being near
sighted at higher layers, packet-filter firewalls depend on secure implementations compound the security problem.

The work involved in setting up filter tables is complicated, and each router vender's syntax and format are different. If the tables do not cover every possible condition, then the firewall has a security hole in it. There is also a small negative effect on performance as the router does more processing of the TCP/IP headers than it would normally do.

The filter setup process has three steps:

1. Decide what you will and will not allow. This flows directly from security policy.
2. Specify the permitted packets as logical expressions.
3. Rewrite those expressions in whatever syntax your router vendor uses.

It may not be necessary to isolate your network totally from outside. It may be wiser to segregate network into that part which can communicate freely and that part which requires isolation. Because the latter be hard to specify some people simply choose to isolate their network altogether. However, the benefit of having such a mixed-access network is that the unsecured part is easier to use.

Packets filtering can be set up with standard routers, such as those from Bay Networks Inc., Cisco Systems Inc., and 3Com Corp. Experts say the bare-bones router approach to security as least desirable. They say this approach lacks the tools that create complex filtering rules and provide an audit trail to become aware of and examine suspicious events. Firewall vendors such as CheckPoint Software Technologies Ltd., in Lexington, mass., provide additional software tools to fill that gap.

Firewalls should disallow services that are not needed or those that could cause compromise. They include Network Information and File Service and the unauthenticated remote "r commands" such as rsh, rcp, and finger. Remove, block, or restrict protocols from the router that might help an attacker.

Proxy Server

Proxy servers are specialized Web servers that operate behind firewall to improve network efficiency and security. Proxy servers are implemented as software programs on a host platform. The host platform can be anything from a small PC to a complex multiprocessor configuration.

Proxy servers operate at the application level within the computer. They stop all network session and create a separate session to the desired destination if it is authorized. Then they shuttle information from the original connection to the second connection. They have more control of a session since they create and maintain the actual connection outside.

The application level gateways use the proxy applications, which are the programs that act on behalf of the user requesting service through the firewall. Proxy applications are the applications on the firewall that accept connections from the users and if the connection is allowed create a separate connection. The proxy then passes the information between two connections.

Proxy servers do not allow any packets to pass directly between the two networks. What they do, instead, is require that the original connection be made to a special purpose application -referred to as a proxy-on the firewall. The proxy application determines whether to actually establish a connection to the requested destination host on behalf of the originating host. This relaying of packets by a proxy can help prevent some application-level attacks such as the popular buffer overflow attack. This assumes, of course, that the proxy application on the firewall is hardened against such attacks and does not allow a successful attack on the firewall itself.

One limitation of a proxy server is that it requires a separate application for each network services. In other words, such a firewall requires a separate program for Telnet, FTP, electronic mail, the World Wide Web, or any other supported service. If you want to support another service through your firewall, you need to add a new proxy application. Thus if a new service is introduced on the Internet and your firewall does not have a proxy application for that service then your users will be denied access to that service. In addition, there is a limit to the number of active applications a computer can support which will restrict the total number of simultaneous connections your firewall can provide.

Some proxy servers do, however, provide a generic proxy application that allows the forwarding of any service. But these generic proxies lose much of the advantages of an application-level gateway by not being aware of the application-specific protocol they are forwarding. The result is a slower version of the packet filtering capability. A very popular generic proxy favored by homegrown firewall developers is the socks software.

Another important feature of proxy server is online auditing. This feature allows a proxy server to monitor activity and record specific events.

Advantages and Disadvantages of Proxy Server

Advantages	**Disadvantages**
Allows only services for which a proxy exists	A two-step process for client-server applications: Connect to server gateway; gateway connects as client to external server
The protocol itself can be filtered (e.g., PUT command in FTP)	May require modified clients
Hides host name and IP addresses; outsiders see only gateway	May force users to change their normal work pattern by adding steps
Excellent authentication: advanced authentication is possible from outside hosts using one-time passwords	More expensive than a packet-filtering router
Allows authentication to reside only on the gateway; internal host security becomes less important	Changes to applications require changes to the gateway; less flexible than a packet-filtering router
Superior logging capability	Requires all supported services, called proxy services

Simple filtering rules: Send all traffic to the gateway and reject the rest	Difficult to adapt to new services such as World Wide Web and Gopher
Often used for Telnet, FTP, e-mail, X-windows, plus other services	Investment value in the gateway is limited by the lifetime of the applications it runs
Gateway can check source IP addresses	
Centralizes mail collection and distribution	

The difference between Firewall and Proxy Server

A. Firewall

1. Firewall is a router (computer which is able to forward packets between two more networks) with some restriction rules applied.
2. Most of current routers can be used as an easy firewall (most of routers allow to define restrictions). It applies by example to Cisco routers, Linux systems, etc… But real firewall is more complicated. It implements mechanisms to allow dynamically opened holes for incoming connections (for FTP sessions by example) and more.
3. Firewall works on the packet level. It can apply rules on packets (by checking the source/destination IP address, source/destination port, etc…) to decide whether the packet will be forwarded or denied.
4. The client stations have to be configured to use firewall as default gateway.
5. If you disable the firewall (only the router works) all LAN station has direct and full Internet access.
6. You can imagine the firewall as a set of restrictive rules (all is enabled when these rules are inactive). So you can eliminate/change some rules to create a whole (range) of port by example.
7. Services which use low-level TCP/IP protocols (ping, trace route, etc…) will work behind firewall (if they are not disabled by firewall restrictions).

B. Proxy Server

1. Application proxy server is a computer which is able to handle requests in some communication protocols (HTTP, FTP, SOCKS,). For each used protocol appropriate proxy service must be enabled.

2. Proxy works on application protocol level. They don't work on packet level so they can't forward packets.

3. Applications on the client PC have to be configured to use proxy server to access Internet servers.

4. If you disable proxy there is no way to connect from the LAN to the Internet servers.
5. Services which use low-level TCP/IP protocols (ping, trace-route, etc…) will not work behind proxy.

Conclusion

Basically, it is good to use both firewall and proxy server, do to some state full inspection, and for specific protocols add a caching proxy. Firewalls/proxy servers are important part of a balanced organization's security architecture. They do not provide the total security solution. They act as a filter,

and, like any filter, they may still allow threats to enter organization's network. Companies masts carefully evaluate the network services they allow through the firewall/proxy server to decide what type of firewalls/proxy server is the most appropriate for their needs.

Many types of firewalls or proxy servers are in use today, which suggests that there is no one "best" firewall or proxy server. Different firewalls or proxy servers are built for different environments. To find the best firewall or proxy server for the organization it is important to map the organization's requirements to particular firewall or proxy server architecture. In addition, the appropriate firewall or proxy server for company's environment depends on several factors, including the level of expertise of firewall or proxy server administrators, the types of services company plans to support, company's budget, and the organizational needs.

High security and ease of use in a firewall or proxy server are almost mutually exclusive goals: The more robust the security, the more difficult the device is to administer. As small companies with few resources grapple with the difficulties providing security in the Internet age, they search for solutions that balance simple administration with reasonable security.

The first security purchase of any company should be a firewall or proxy server, and the low-end segment of the firewall or proxy server market -- currently a modest market -- will swell considerably during the next few years to answer small companies' and branch offices' need for turnkey solutions.

The firewall appliance includes all of the firewall hardware and software necessary to stop digital barbarians at the gate. Unlike traditional firewalls, which are notoriously difficult to administer, the firewall appliance is simple to install and administer.

Firewall appliances have yet to make a real dent in the firewall market. Firewalls have been high-end products used by experts, and the dominant players in the market cater to them. The Gartner Group estimates that about 15 percent of the enterprise network managers buying firewalls require the highest security and have dedicated specialists to administer firewalls. This segment should remain a stable percentage of the market during the next five years.