Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Proxies and Packet Filters in Plain English

The term firewall, in computer jargon, has the same connotation as it would in relation to your house or car. It provides protection against anything that has the ability to destroy your property. In relation to your car and house it protects against fires and in networking it provides protection against attacks on your network or computer. Network firewalls can serve several purposes. They act as a gateway providing access for your network to multiple networks or to the Internet. They can also block traffic flowing to...

Copyright SANS Institute
Author Retains Full Rights

AD

Proxies and Packet Filters in Plain English

The term firewall, in computer jargon, has the same connotation as it would in relation to your house or car. It provides protection against anything that has the ability to destroy your property. In relation to your car and house it protects against fires and in networking it provides protection against attacks on your network or computer. Network firewalls can serve several purposes. They act as a gateway providing access for your network to multiple networks or to the Internet. They can also block traffic flowing to and from the network. They have the ability to choose what is and what is not allowed to flow in and out of the network. The firewall's ability to decide what is and what is not allowed are configurations that are setup by the system administrator as policies or rules. These policies define what traffic the firewall will or will not allow to enter the network. They also define what is allowed to or not allowed to leave the network. These policies are the heart of a firewall.

The task of setting up the information allowed to flow from the network is easier because you have access to the internal network. The information that flows from the network is generated by services/protocols such as: Email (both POP and SMTP), web (WWW), FTP, etc. These services/protocols accomplish this by using ports. Ports are holes in the firewall that the services/protocols utilize to perform the above tasks. An example of this would be port 80 for WWW. When you go to a website your machine will try to connect to the site on port 80. The remote site has a server that is listening on this port and will respond with the web page that you desire. They help to improve security because the port has to be open for the information to leave the network. When it comes to setting up rules and regulations governing traffic from the "outside" world the setup can prove to be a little more difficult to establish because you are not in control of the machines outside of your firewall.

Firewalls are setup to monitor Internet traffic. It would only be able to stop someone from entering your network. This helps because not everyone from the "outside" world would be granted access by the firewall to enter the internal network. This provides another line of protection as well. For example, if someone tries to enter the network, the firewall logs the attempt. This informs the system administrator that someone tried to connect to the network. This demonstrates the firewall's system of auditing and logging connections for the network. It can provide specific information such as the origin of the connection attempt. The only problem is the breakdown of the firewall, when careless operators use the network. The firewall is useless if a user on the network is not cautious regarding the secrecy of their passwords and logins. The firewall is worthless because the "outsider" was given legal access to the network with no means of being able to stop or monitor them. They also have access to the information that can be transferred to diskettes, CD-ROM's and printouts. The firewall having no ability of monitoring this activity would be useless.

Viruses are another major concern on a network. There are some newer firewalls that proclaim that they can detect viruses before they reach your network. This is not a promised feature of firewalls since viruses come in so many forms. The best

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

protection against viruses is to have virus-scanning software on the end users' machines. The firewall would have too much to look for since there are so many viruses that can span across several operating systems or platforms. This could also slow down your firewall by making also investigate files as they enter your system. The most a firewall should be used to investigate viruses is to have the firewall send the files/traffic to a content server that can scan for viruses. Most of today's firewalls allow for plug-in like features that will work with major virus manufacturers. You can simple tell the firewall to send E-mails or FTP files to one specific server which can scan the content for viruses. This also takes the risk of having the firewall itself get infected.

Firewalls can be broken down into two categories: IP packet filters (Network Level) and proxy servers (Application Level). There are also three parts or "zones" when referring to network protection. The first zone is referred to as the Red Zone which is insecure by all practical purposes. This zone has no means of protecting the network from the "outside" world. The only security in this zone comes from the machine itself or disconnection from the network. The latter can actually provide a possibility for the average user connecting to the Internet via an ISP. The second zone is referred to as the Yellow Zone. The Yellow Zone, the first part of a firewall, is referred to as the IP packet filter (Network Level). The packet filter firewalls provide protection on the networking level. These firewalls are setup to make decisions about the source address, destination address, and ports in the individual IP packets. This form of firewall serves the purpose of establishing a checkpoint to and from the network. The packet filter is setup to determine which IP addresses, both internal and external, are allowed to pass through the network. There is also a set of rules that decide which ports are allowed to have traffic. Whenever a packet tries to enter or leave the network it is checked according to the firewall's rules. If the packet is headed from an allowed IP address toward an allowed port, it is granted access. When something is allowed to connect to a network it is referred to as trusted or known. An example, a network that is connected to the Internet with a running packet filter allows connections to port 25 (SMTP) from a known host (mail.mindspring.com) (port_numbers). When someone from Earthlink tries to send E-mail to our network it is permitted to be delivered because the connection is coming from a known/trusted host. In this instance the known host is mail.mindspring.com and the allowed port is 25. If someone from PSI tried to send E-mail to our network, it would be denied. The reasoning is due to the unfamiliarity of the host even though the port is allowed. Both of these conditions must be meant before the packet is allowed to pass through the firewall because the port must be a valid port and the host must be trusted. This type of firewall generally only affects the users outside of the network. Most of the time, users on the network will not notice the packet filter. The biggest drawback to using a packet filter is that it does not provide much in the logging arena. The final zone, referred to as the Green Zone, is the second part of a firewall called a proxy server (Application Level Firewall). This zone is "completely" secure. The Green Zone is neither one extreme nor the other because it processes requests for the internal network and for the external network.

A proxy server is more of a stopping point in between the two networks. This greatly differs from the packet filter (Network Level) firewall. The packet filter (Network

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Level) firewall watches the information as it goes from the “outside” world onto the internal network. The proxy server (Application Level Firewall) actually stops the information and inspects it before letting it access the internal network. In this case, there is no direct connection between the internal network and the “outside” world. A proxy server does not look at the information on a network level. It does things differently because most users need to authenticate to the proxy in order to be able to pass information. When a client on the network makes a request to the Internet, the proxy receives that request. The originating IP address, of the request, is changed to the same IP address as that of the proxy server. It then forwards this request to the intended destination or Internet site. Any response that is received gets sent to the proxy server which in turn forwards the response to the client on the network. This is a major boost in security for the network because there is no direct route to the network machines. All communication must be made with the proxy server, who will then inspect and forward all the information to the proper host.

Proxy servers are setup with one of two different types of architectures. The first one is referred to as a single-homed host. There is only one network card in the proxy server in this type of architecture. It is then the responsibility of the Internet router to forward requests to the proxy server and block all other information to the network. The second type of architecture, a dual-homed or multi-homed host, contains two network cards which alone can not route information. The combination of the two network cards and the proxy server allow information from the internal network to communicate with the Internet and vice versa. Requests that come from the internal network are sent to one network card. The information that comes from the Internet is sent to the other network card. Since there is no routing setup between the network cards, neither connection has a direct route to each other. The proxy server decides what to send and where to send it at this time.

The added bonus that the proxy server provides for a firewall is connection logging when the information passes through the firewall they alone do not do their own logging. The connections first access the proxy which logs everything that is going to and from the Internet. The connections from the “outside” world are logged because they need to be authenticated before being granted entrance. The internal traffic is also logged to insure that staff are completing their job duties. It can alleviate people slowing down the speed of the network by visiting “useless” sites. This is accomplished by tracking which sites they have been to and verbally tell them to stop or restricting their access.

A proxy server also provides convenience to the network. A major role of a proxy server is that it caches Internet web sites just like a web browser caches HTML pages and images. It can speed up the network in two ways. The first way is traffic is reduced on the internal network’s Internet connection because users have the opportunity to utilize the cached copy of a web site instead of direct Internet connections. The next time someone else visits the web site the proxy server does not need to use the Internet connection because the information is already available on the internal network. It also saves the time it takes the information to reach your machine because the Internet site

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

might have been cached by someone else previously on the internal network. A financial benefit of a proxy server is that it provides Internet access to many clients under one account. The machines on the internal network do not have any direct connection to the Internet so they only need to maintain one Internet IP address which makes DNS configuration easier to manage.

A proxy server uses something called Network Address Translation (NAT). This is how users on the internal network can be hidden from the outside. The way NAT works is when a machine behind the firewall attempts a connection somewhere, the proxy receives the request. The proxy then changes the source address of the packet to that of the proxy. The destination is kept the same and the request is made. When a response is received back it is done in the reverse manner. The source address of the response is kept the same and the destination address is changed to that of the internal requesting machine. This is how the internal machines are hidden from the outside.

NAT also helps organizations with growth planning for their network. Multiple users and IP addresses can be hidden behind one single IP Address or multiple addresses using NAT. A packet level firewall does not use this setup. If we had a network using a packet filter with 100 users, then we would need at least 100 IP Addresses. Every machine on the network will have its own public IP address. This becomes costly to a company of only 100 people. This can also be an inconvenience for the system administrators. If you are leasing these 100 IP Addresses from an ISP and they decide to renumber your network, you now have to change 100 machines. If you decide to grow your network then you will need to purchase additional IP Addresses. This could put you on a different network as well.

The proxy server alleviates all of these concerns. Continuing with our same example of the 100-user network, we only need a minimum of one IP Address. We then use any of the private address schemes stated in RFC 1918 (http://www.isi.edu/in-notes/rfc1918.txt). These IP Addresses are not used on the Internet. They are reserved for internal networks. We can setup our network with 10.20.20.* network. This means that we have at least 253 IP Addresses for the internal network. We can assign whatever IP Addresses that we like. All the users that would contact the Internet from this network would be hidden behind one single IP Address that is the proxy server. We no longer have concerns about renumbering. If our site is renumbered for some reason, it only affects one IP Address. Only the proxy server itself is renumbered. The other machines on the internal network use their same IP Addresses as before. If the network continues to grow we can still use one public IP and renumber the internal machines to be on a larger network. We can have as much as one entire class A network behind one public IP.

Another good ability that a firewall has is separating your networks. You do not have to put all of your internal machines on the same network behind the firewall. It is in fact best to create what is called a DMZ (De-Militarized Zone) behind your firewall. A DMZ is used to place machines that can be accessed from the outside. This lowers the risk on your internal network. The internal network now has no connectivity from the

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

outside in. When someone tries to initiate a connection from the outside world to your internal network, the traffic is stopped. The machines in your DMZ can now be reached by the outside world. This allows you to still provide protection to your servers in the DMZ but at the same time allows outsiders to reach the services needed from these machines.

There are also drawbacks to using a firewall/proxy server. The first hurdle would be the setup and planning of the firewall/proxy server. The setup and planning is the toughest part because it requires a lot of time and effort to be designed to specifically fit the needs of your internal network. The administrator needs to make sure that they configure correct services and hosts to access the firewall/proxy. You must also design a security policy and a means of implementing it. You should always create a security policy that is both secure and is agreed upon by management. A good security policy will allow you to continue to do business but in a more secure manner.

There are a number of different firewalls out there today. The ones mentioned in this document are but a few. It is best for your organization to first investigate which type of firewall would be best suited for your environment. You should also stay as up to date as possible with the latest trends and vulnerabilities in the firewall software you choose.

© SANS Institute 2001, Author retains full rights.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

References

Elton, Peter. “Linux as a Proxy Server” *Linux Journal*.
http://www.ssc.com/lj/issue44/2408.html.

NEC USA “Introduction to SOCKS”
http://www.socks.nec.com/introduction.html.

Grennan, Mark. “Firewalling and Proxy Server HOWTO”.
http://www.linuxdoc.org/HOWTO/Firewall-HOWTO.html

IANA “Port Numbers”
http://www.iana.org/assignments/port-numbers

Curtin, Matt and Marcus J. Ranum. “Internet Firewalls Frequently Asked
http://www.interhack.net/pubs/fwfaq/

Wack, John. “Packet Filtering Firewall”.
http://security.tsu.ru/info/fw/800-10/e/node55.html

Elron Software, “Elron Firewall Tech Note”.
http://nsupport.elronsoftware.com/support/fwweb.nsf/d43e687e1ccbf9f58525656e0006de25/5dba4a1c72329f4d8525651e005fe02b?OpenDocument

Vicomsoft. “Network Address Translation FAQ”.
http://www.vicomsoft.com/index.html?page=http://www.vicomsoft.com/knowledge/reference/nat.html*track=internal

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 21st, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced