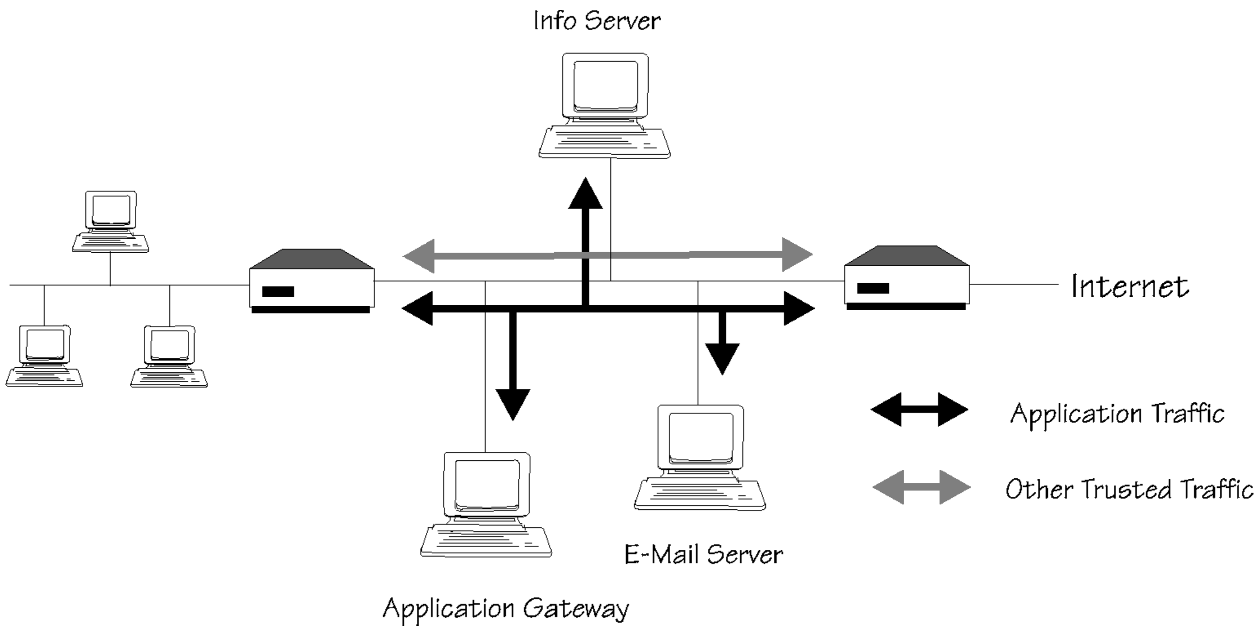


Screened Subnet Firewall

The screened subnet firewall is a variation of the dual-homed gateway and screened host firewalls. It can be used to locate each component of the firewall on a separate system, thereby achieving greater throughput and flexibility, although at some cost to simplicity. But, each component system of the firewall needs to implement only a specific task, making the systems less complex to configure.

In figure , two routers are used to create an inner, *screened* subnet. This subnet (sometimes referred to in other literature as the ``DMZ") houses the application gateway, however it could also house information servers, modem pools, and other systems that require carefully-controlled access. The router shown as the connection point to the Internet would route traffic according to the following rules:

- application traffic from the application gateway to Internet systems gets routed,
- e-mail traffic from the e-mail server to Internet sites gets routed,
- application traffic from Internet sites to the application gateway gets routed,
- e-mail traffic from Internet sites to the e-mail server gets routed,
- ftp, gopher, etc., traffic from Internet sites to the information server gets routed, and
- all other traffic gets rejected.

The outer router restricts Internet access to specific systems on the screened subnet, and blocks all other traffic to the Internet originating from systems that should not be originating connections (such as the modem pool, the information server, and site systems). The router would be used as well to block packets such as NFS, NIS, or any other vulnerable protocols that do not need to pass to or from hosts on the screened subnet.

The inner router passes traffic to and from systems on the screened subnet according to the following rules:

- application traffic from the application gateway to site systems gets routed,
- e-mail traffic from the e-mail server to site systems gets routed,
- application traffic to the application gateway from site systems get routed,
- e-mail traffic from site systems to the e-mail server gets routed,
- ftp, gopher, etc., traffic from site systems to the information server gets routed,
- all other traffic gets rejected.
- Thus, no site system is directly reachable from the Internet and vice versa, as with the dual-homed gateway firewall. A big difference, though, is that the routers are used to direct traffic to specific systems, thereby eliminating the need for the application gateway to be dual-homed. Greater throughput can be achieved, then, if a router is used as the gateway to the protected subnet. Consequently, the screened subnet firewall may be more appropriate for sites with large amounts of traffic or sites that need very high-speed traffic.
- The two routers provide redundancy in that an attacker would have to subvert *both* routers to reach site systems directly. The application gateway, e-mail server, and information server could be set up such that they would be the only systems ``known'' from the Internet; no other system name need be known or used in a DNS database that would be accessible to outside systems. The application gateway can house advanced authentication software to authenticate all inbound connections. It is, obviously, more involved to configure, however the use of separate systems for application gateways and packet filters keeps the configuration more simple and manageable.
- The screened subnet firewall, like the screened host firewall, can be made more flexible by permitting certain ``trusted'' services to pass between the Internet and the site systems. However, this flexibility may open the door to exceptions to the policy, thus weakening the effect of the firewall. In many ways, the dual-homed gateway firewall is more desireable because the policy cannot be weakened (because the dual-homed gateway cannot pass services for which there is no proxy). However, where throughput and flexibility are important, the screened subnet firewall may be more preferable.
- As an alternative to passing services directly between the Internet and site systems, one could locate the systems that need these services directly on the screened subnet. For example, a site that does not permit X Windows or NFS traffic between Internet and site systems, but needs to anyway, could locate the systems that need the access on the screened subnet. The systems could still maintain access to site systems by connecting to the application gateway and reconfiguring the inner router as necessary. This is not a perfect solution, but an option for sites that require a high degree of security.
- There are two disadvantages to the screened subnet firewall. First, the firewall can be made to pass ``trusted'' services around the application gateway(s), thereby subverting the policy. This is true also with the screened host firewall, however the screened subnet firewall provides a location to house systems that need direct access to those services.

With the screened host firewall, the ``trusted'' services that get passed around the application gateway end up being in contact with site systems. The second disadvantage is that more emphasis is placed on the routers for providing security. As noted, packet filtering routers are sometimes quite complex to configure and mistakes could open the entire site to security holes.

Different Types of Firewalls

September 12, 2012 by wing 1 Comment

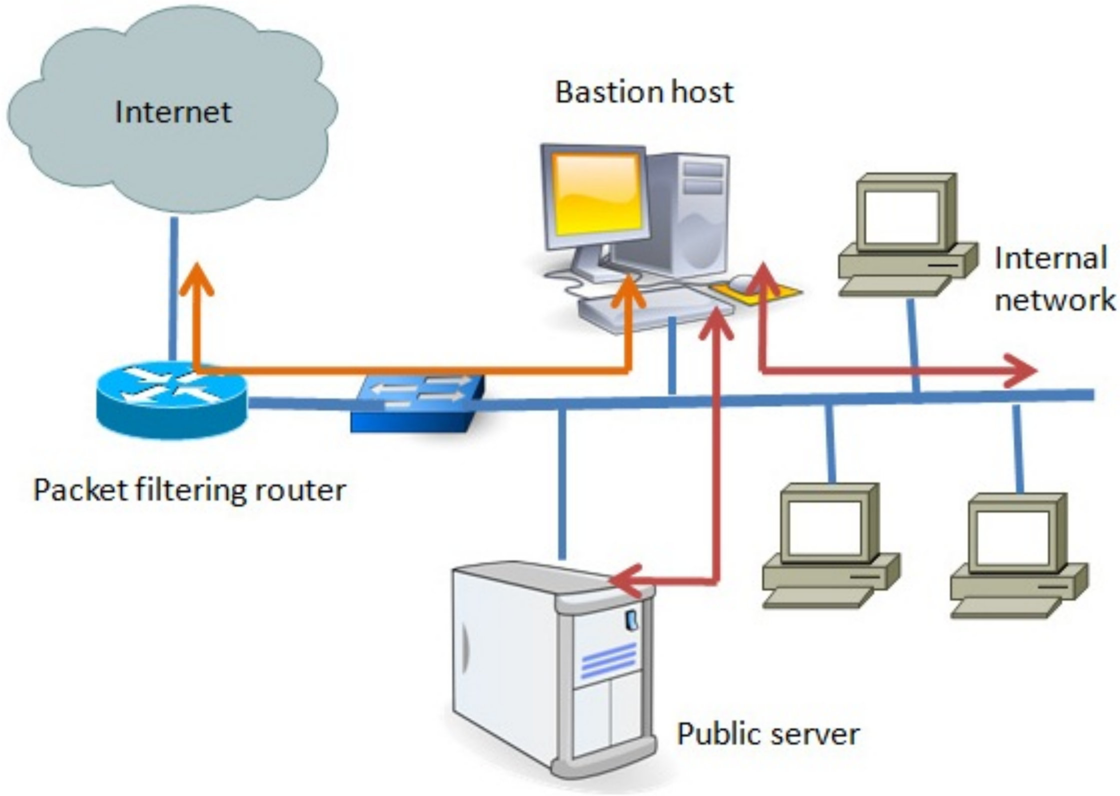
There are several types of firewalls that work on different layers of the OSI model. Depending on the kind of service and security you need for your network, you need to choose the right type of firewall. The following are the list of seven different types firewalls that are widely used for network security.

- Screened host firewalls
- Screened subnet firewalls
- Packet filter firewalls
- Stateful inspection firewalls
- Hybrid firewalls
- Proxy server firewalls
- Application level (gateway) firewalls

Screened host firewalls:

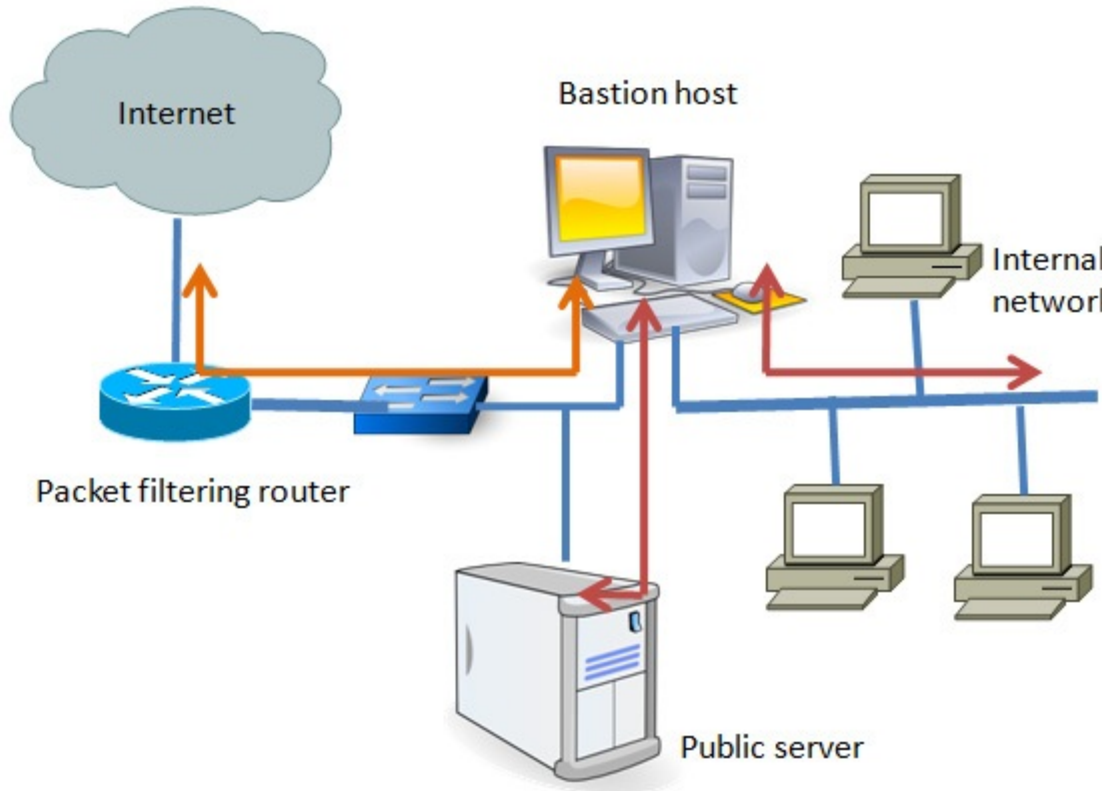
There are two types of screened host-one is **single homed bastion host and the other one is dual homed bastion host**. In case of single homed bastion host the firewall system consists of a packet filtering router and a bastion host. A bastion host is basically a single computer with high security configuration, which has the following characteristics:

- Traffic from the Internet can only reach the bastion host; they cannot reach the internal network.
- Traffic having the IP address of the bastion host can only go to the Internet. No traffic from the internal network can go to the Internet.



Screened host firewall (single-homed bastion host)

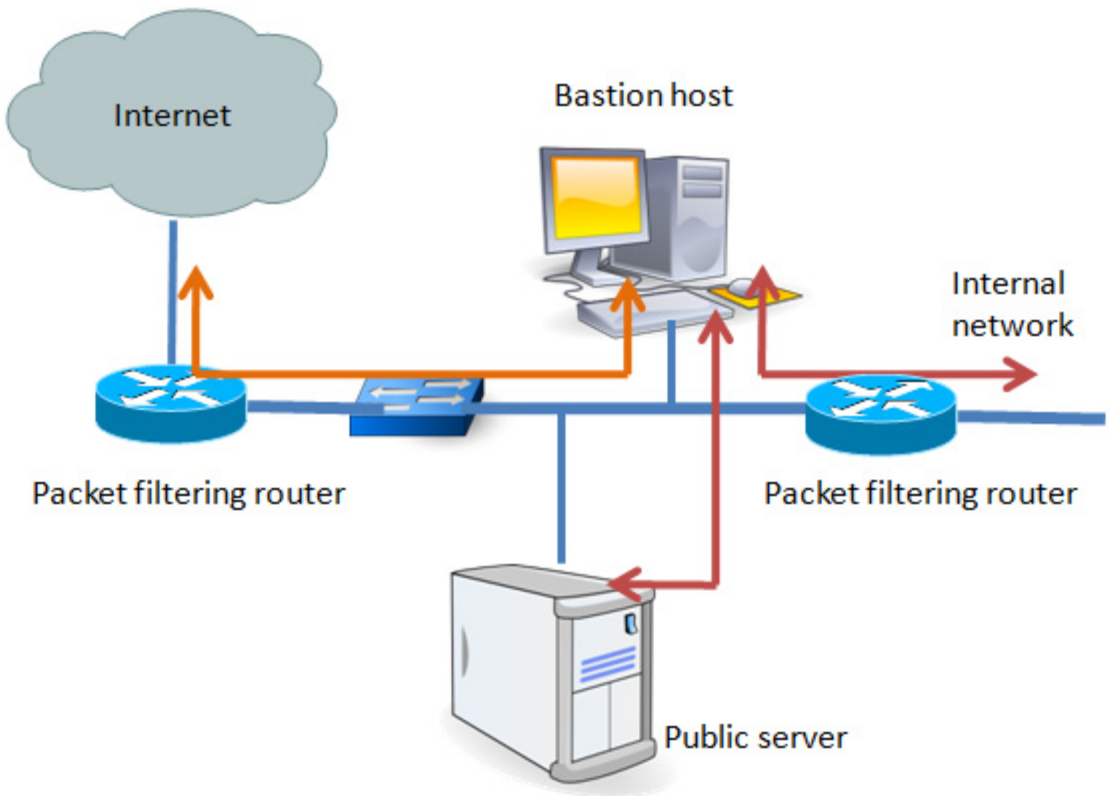
This type of configuration can have a web server placed in between the router and the bastion host in order to allow the public to access the server from the Internet. The main problem with the single homed bastion host is that if the packet filter route gets compromised then the entire network will be compromised. To eliminate this drawback we can use the **dual homed bastion host** firewall system, where a bastion host has two network cards- one is used for internal connection and the second one is used for connection with the router. In this case, even if, the router got compromised, the internal network will remain unaffected since it is in the separate network zone.



Screened host firewall (Dual-homed bastion host)

Screened subnet firewalls

This is one of the most secured firewall configurations. In this configuration, two packet filtering routers are used and the bastion host is positioned in between the two routers. In a typical case, both the Internet and the internal users have access to the screened subnet, but the traffic flow between the two subnets (one is from bastion host to the internal network and the other is the sub-network between the two routers) is blocked.



Screened subnet firewall

Packet filtering firewalls

This type of firewall is the most common and easy to deploy in a small-sized network. A router functions as a firewall by examining every packet passing through the network. Based on access control list, the router either forward or drop packets. Normally, the IP address of the source and destination, port number and type of traffic are taken into account when the router processes each data packet. Since a router cannot check packet in the application layer, this type of firewall cannot defend attacks that use application layers vulnerabilities. They also fail to fight against spoofing attacks. You can use this configuration if you need higher network speed and do need limited login and authentication capacity.

Stateful inspection

Stateful inspection firewall works at the **network layer in the OSI model**. It monitors both the header and contents of the traffic. The main difference between the packet filtering and the stateful inspection is that it the later one analyzes not only the packet headers but also inspects the state of the packets along with providing proxy services. Stateful inspection firewalls maintain a state table and a set of instructions to inspect each packet and store the information based on the type of traffic. It also monitors each TCP connection and remembers which ports are being used by that connection. If there is any port not required by the connection, then that port get closed.

Hybrid firewalls

They function almost the same way the stateful inspection type firewalls work, which means they can work both in network and in application level. Normally, in a hybrid system some hosts reside inside the firewall while the others reside outside of the firewall. To communicate with the machine outside the central network IPsec tunnels are used. An example where this type of configuration is suitable is a major site connected with its branch sites via VPN. One distinct feature of this configuration is the firewall administration at the major site distribute the security policy to its branch site so as a uniform security is maintained throughout the organization.

Proxy server firewalls

Proxy allows users to run specific service (FTP, TELNET, HTTP etc.) or type of connection by enforcing authentication, filtering and logging. For specific service there will be a specific proxy. For example, if you want to allow only HTTP connection to the Internet for your internal network users, then you must allow only HTTP proxy, nothing else. Users who need to go to Internet create a virtual circuit with the proxy server and the proxy server sends the request to connect to a specific site on behalf of that particular user. Proxy server changes the IP of the request so as the Internet or the outside world can see only the IP of the proxy server. Thus **proxy server hides the internal network behind it.** When a proxy receives the data from the Internet it sends the data back to its intended internal user via the virtual circuit. The main advantage of using proxy is that it is fully aware of the type of data it handles and can give protection to it. One disadvantage of proxy is that if there is an update of protocol that is used by the Internet, then the proxy software also needs to be updated to allow a specific service related to that protocol.

An Analysis of Fragmentation Attacks
Jason Anderson
March 15, 2001

Introduction

Fragmentation is the term given to the process of breaking down an IP datagram into smaller packets to be transmitted over different types of network media and then reassembling them at the other end. This process is an integral part of the IP protocol and is covered in depth in RFC 791.

This paper will give a brief description of fragmentation, describe some common fragmentation attacks and look at some of the measures used to prevent them. It will also discuss some of the problems fragmentation attacks have on two widely used commercial firewall and IDS packages.

IP Fragmentation

So what is fragmentation and is it always bad?

Well the answer to this question is a definite no. As discussed earlier fragmentation is an integral part of the IP protocol and without it the Internet could not operate, as we know it today.

Fragmentation is necessary in order for traffic, which is being sent across different types of network media to arrive successfully at its intended destination. The reason for this is that different types of network media and protocols have different rules involving the maximum size allowed for datagrams on its network segment. This is known as the maximum transmission unit or MTU.

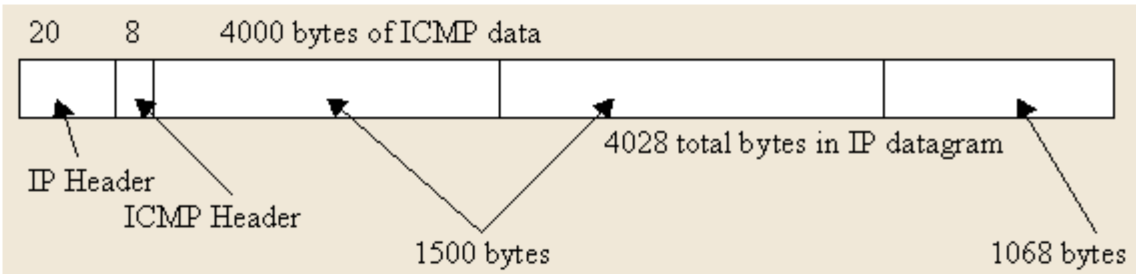
So in order to transmit a datagram across a network segment which has a MTU smaller than that of the packet to be transmitted fragmentation is required.

In order for a fragmented packet to be successfully reassembled at the destination each fragment must obey the following rules:

- Must share a common fragment identification number. Also known as fragment Id.
- Each fragment must say what its place or offset is in the original unfragmented packet.
- Each fragment must tell the length of the data carried in the fragment.
- Finally the fragment must know whether more fragments follow this one.

All of this information will be contained in the IP header. The header will be placed in an IP datagram followed by an encapsulated fragment (TCP/IP for Firewalls and Intrusion Detection Course notes SANS Darling Harbour).

The following diagram shows the breakdown of an IP fragment, which displays the elements as stated above.



Ethernet MTU = 1500

Original 4028 byte fragment broken into 3 fragments of 1500 bytes or less.

Diagram: (TCP/IP for Firewalls and Intrusion Detection Course notes SANS Darling Harbour P4-8).

The following is the TCP dump output of the same fragmented datagram displaying how the various components above are displayed.

ping.com > myhost.com: icmp: echo request (frag 21223:1480@0+)

ping.com > myhost.com: (frag 21223:1480@1480+)

ping.com > myhost.com: (frag 21223:1048@2960)

notes:

- 21223 is the fragment Id
- 1480 in the first two fragments and 1048 in the last fragment shows the number of data bytes in the current fragment
- The last number of each fragment shows the fragment offset
- The + sign in the first two fragments indicate that more fragments follow

TCP dump: (TCP/IP for Firewalls and Intrusion Detection Course notes SANS Darling Harbour P4-16).

Types of Fragmentation Attacks

There are numerous ways in which attackers have used fragmentation to infiltrate and cause a denial of service to networks, some of these are discussed below.

Ping O' Death Fragmentation Attack

The Ping O' Death fragmentation attack is a denial of service attack, which utilises a ping system utility to create an IP packet, which exceeds the maximum allowable size for an IP datagram of 65535 bytes.

This attack uses many small fragmented ICMP packets which when reassembled at the destination exceed the maximum allowable size for an IP datagram. This can cause the victim host to crash, hang or even reboot.

This attack has however been around for quite sometime and all operating system vendors should have fixes in place to rectify this problem. It is however essential to ensure that you have the latest patches installed for your operating system.

The Tiny Fragment Attack

This attack uses small fragments to force some of the TCP header information into the next fragment. This may produce a case whereby the TCP flags field is forced into the second fragment and filters that attempt to drop connection requests will be unable to test these flags in the first octet thereby ignoring them in subsequent fragments.

This attack can be used to circumvent user-defined filtering rules. The attacker hopes that a filtering router will examine only the first fragment and allow all other fragments to pass.

This attack can be prevented at the router by enforcing rules, which govern the minimum size of the first fragment. This first fragment should be made large enough to ensure it contains all the necessary header information.

The Teardrop Attack

This is also a denial of service attack that can cause the victim host to hang crash or reboot, as was the Ping O' Death attack.

The teardrop attack utilises the weakness of the IP protocol reassembly process. The teardrop attack is a UDP attack, which uses overlapping offset fields in an attempt to bring down the victim host.

This type of attack has also been around for some time and most operating system vendors have patches available to guard against this sort of malicious activity.

The Overlapping Fragment Attack

Another variation on the teardrop attack that also uses overlapping fragments is the Overlapping Fragment Attack. This attack however is not a denial of service attack but it is used in an attempt to bypass firewalls to gain access to the victim host.

This attack can be used to overwrite part of the TCP header information of the first fragment, which contained data that was allowed to pass through the firewall, with malicious data in subsequent fragments. A common example of this is to overwrite the destination port number to change the type of service i.e. change from port 80 (HTTP) to port 23 (Telnet) which would not be allowed to pass the router in normal circumstances.

Ensuring a minimum fragment offset is specified in the router's IP filtering code can prevent this attack.

The Unnamed Attack

This attack is yet another variation on the teardrop attack that attempts to cause a denial of service to the victim host. This time however the fragments are not overlapping but are created in such a way that there is a gap created in the fragments.

This is done by manipulating the offset values to ensure there are parts of the fragment, which have been skipped. Some operating systems may behave unreliably when this exploit is used upon them.

Some Known Vulnerabilities in Checkpoint Firewall-1 and ISS Real Secure

Fragmentation attacks have been used as a tool by attackers to infiltrate and cause a denial of service to networks for some time now. Many commercially available software packages have experienced vulnerabilities when faced with some of the attacks listed previously. Two well-known packages that have been susceptible to these attacks are Checkpoint Firewall-1 and Internet Security Systems (ISS) RealSecure Intrusion detection system.

Checkpoint Firewall-1 Vulnerabilities

Checkpoint Firewall-1 is one of the more widely used firewall products on the market. By doing a search on the Internet for Checkpoint Firewall-1 vulnerabilities I came across several vulnerabilities which are related to fragmentation. These are detailed below.

IP Fragment-driven Denial of Service Vulnerability

This vulnerability was discovered by Lance Spitzner (lance@spitzner.net) and has been confirmed by Checkpoint. Testing by Checkpoint has confirmed that versions 4.0 and 4.1 of Firewall-1 are affected. Earlier versions of the product were not tested.

This vulnerability exploits the way Firewall-1 handles fragmented packets. Firewall-1 is a Statefull Inspection firewall and for security reasons it reassembles all IP fragments of a datagram prior to inspection against the security policy. This is done in order to guard against attacks such as the Overlapping Fragment attack as discussed in an earlier section of this paper.

In order to identify and audit attacks such as The Ping O' Death Checkpoint added a mechanism to Firewall-1 to log certain events that occur during the fragment reassembly process. This however can cause a possible denial of service to the firewall. As Firewall-1 reassembles the entire packet before sending it on it is possible to send a number of incomplete fragments to the firewall which can never be reassembled. This will cause the logging mechanism to consume all host CPU resources on the Firewall-1 gateway hence rendering the firewall inoperable.

This vulnerability has been addressed in version 4.1 service pack 2(SP2) and version 4.0 service pack 7(SP7). The logging mechanism has been modified in these service packs to consume minimal CPU cycles.

As an interim fix however it is possible to disable the console logging by entering the following command on the Firewall-1 module command line:

$FWDIR/bin/fw ctl debug –buf

Further information on this vulnerability can be found at the following site:

http://www.checkpoint.com/techsupport/alerts/ipfrag_dos.html

One-way Connection Enforcement Bypass

Sites allowing protocols employing unidirectional data flow connections (such as FTP and RSH STDERR) are susceptible to this vulnerability.

This vulnerability made it possible to bypass Firewall-1's normal directionality check by using specially fragmented TCP connection requests or by closing and reopening one-way TCP connections in conjunction with certain complex multi-connection protocols.

This vulnerability has been addressed in version 4.1 service pack 2(SP2) and version 4.0 service pack 7(SP7). These service packs feature tighter control of directionality checks which will prevent malicious back-channel communication.

Further information on this vulnerability can be found at the following sites:

http://www.checkpoint.com/techsupport/alerts/one_way.html

http://neworder.box.sk/showme.php3?id=2622

Internet Security Systems (ISS) RealSecure Intrusion Detection System Vulnerability

ISS RealSecure is one of the more widely used Intrusion Detection System products on the market. By doing a search on the Internet for RealSecure vulnerabilities I came across the following vulnerability which are relates to fragmentation. A description of this vulnerability is detailed below.

RealSecure RSKill Denial of Service Vulnerability

This vulnerability was discovered by the Modulo Security Labs Team and has been confirmed by ISS. This vulnerability affects version 3.2 of RealSecure.

This vulnerability uses IP fragmentation to cause a denial of service to the RealSecure engine causing it to crash.

A failure in the treatment of fragmented packets with the SYN flag set causes the immediate failure in the RealSecure engine, disabling the intrusion detection.

On the Solaris version of RealSecure the engine service file ('network_engine') is disabled, causing a core dump memory file creation. The event is immediately reported through the RealSecure console.

On the NT version, the engine ('network_engine.exe') has a different bug. The service after crashing, restarts immediately, generating a Windows NT Application Log event. A large and continuous stream of these fragmented packets (SYN Flood) take the processor load up to 100% thus rendering the RealSecure engine inoperable and unable to detect any other attacks.

In order to rectify this vulnerability you will need to apply the 3.2.2 patch, available from Internet Security Systems Customer Support (support@iss.net).

Further information on this vulnerability can be found at the following sites:

http://xforce.iss.net/static/5133.php

http://www.securityfocus.com/archive/1/77548

Conclusion

As you can see fragmentation is a necessary part of the IP protocol but it has also been used extensively by attackers to circumvent and bring down firewalls and intrusion detection systems.

Although most of the attacks described in this paper have been around for some time they still can cause problems if your systems are not updated to the latest versions of patches and service packs.

References

TCP/IP for Firewalls and Intrusion Detection Course notes SANS Darling Harbour.

Northcutt Stephen. Network Intrusion Detection – An Analyst's Handbook, 1999, New Riders Publishing.

Ptacek, Thomas. Newsham, Timothy. "Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection". January 1998.
URL: http://secinf.nrt/info/ids/idspaper/idspaper.html

Unknown. "RFC791 Internet Protocol DARPA Internet Program Specification" September 1981.
URL: http://www.rfc-editor.org/rfc/rfc791.txt

Merkow, Mark. "E-Commerce Security Technologies – Part One". 02 December 1999.
URL: http://ecommerce.internet.com/outlook/article/0,1467,7761_253601_2,00.html

Spitzner, Lance. "Understanding the FW-1 State Table". 29 November 2000.
URL: http://www.enteract.com/~lspitz/fwtable.html

Fucs, de Miranda. "RealSecure Vulnerable to a DoS (Fragmented SYN)". 30 August 2000.
URL: http://neworder.box.sk/showme.php3?id=2627

Unknown. "RealSecure RSKill Denial of Service". August 2000.
URL: http://xforce.iss.net/static/5133.php

Unknown. "IP Fragment-driven Denial of Service Vulnerability". 31 January 2001.
URL: http://www.checkpoint.com/techsupport/alerts/ipfrag_dos.html

Unknown. "Potential Security Issues in VPN-1/FireWall-1". 31 January 2001.
URL: http://www.checkpoint.com/techsupport/alerts/list_vun.html

Unknown. "Common Vulnerabilities and Exposures". 22 January 2001.
URL: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0804