GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

A Comparison of Packet Filtering Vs Application Level Firewall Technology
Ernest Romanofski

A firewall serves as a primary defense against external threats to an organization's computer network system. The firewall is usually a combination of hardware and software used to implement an organization's security policy governing network traffic. This network traffic is between two or more networks, one of which is under the organization's control. Two objectives common to all firewall systems is to allow the flow of network traffic that has been determined to be consistent with the organization's security policy and to minimize the amount and usefulness of information about the organization's computer network system that is disclosed to those outside the firewall. A firewall is a barrier to keep destructive forces away from an organization's computer system. The organization's computer system could be directly accessible to anyone on the Internet if a firewall is not in place.

Without a firewall an organization will not be able to prevent many forms of undesirable access to their computer systems and information assets. The undesirable access could lead to loss of confidential business information; loss of availability of mission critical services; exposure of system infrastructure to those who might attack the system, and vandalism of public information services such as the organization's Web site. Firewall technology provides the organization with one of the most effective tools available to manage network risk by providing access control mechanisms that can implement complex security policies.

Firewalls are customizable so that filters can be added or removed based on several conditions. The firewall administrator can control how an organization's employees connect to Internet sites and whether files are allowed to leave the organization via the Internet. A firewall can give the organization tremendous control over how employees use the Internet. For example, a security rule could be implemented to allow only one computer within the organization to be able to receive public FTP traffic.

A firewall can be as simple as a router that filters packets or as complex as a multi-computer, multi-router solution that combines packet filtering and application level proxy services. An organization's network security policy must contain procedures to safeguard the network and its contents against damage or loss. A network security policy identifies network resources and threats, defines network use and responsibilities, and details action plans to follow when policy is violated. The network security policy needs to be strategically enforced at defensible boundaries within the organization's network. These strategic boundaries are called perimeter networks.

To establish an organization's perimeter networks, the system administrator must designate the computers that are to be protected and define the network security mechanisms that protect them. To establish a successful network security perimeter, the firewall sever must be the gateway for all communications between trusted networks within the organization's control and untrusted external networks such as the Internet. The firewall server defines the point of focus or choke point through which all communications between the internal and external networks pass.

Packet Filter Firewall

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

A packet filter firewall analyzes network traffic at the transport protocol layer. Each IP network packet is examined to see if it matches one of a set of rules defining what data flows are allowed. The rules determine whether communication is allowed based upon the information contained within the Internet and transport layer headers and the direction that the packet is headed. Packet filters enable the administrator to permit or prohibit the transfer of data based on the following controls: the physical network interface that the packet arrives on; the source IP address the data is coming from; the destination IP address the data is going to; the type of transport layer; the transport layer source port, and the transport layer destination port.

The packet filter architecture performs an analysis for one or more network protocols using a very limited rule set. The packets coming into the trusted network are compared against defined rules composed from a limited rule set for one or more protocols such as IP, TCP, or ICMP. Packets are either accepted and passed to the network stack for delivery or are denied access. If a packet satisfies all of the packet filter rules, the packet either moves up the network stack for future processing or gets forwarded to the network host. The rule set is maintained in the TCP/IP kernel. The rule set is used since packet filters do not generally understand the application layer protocols used in the communication packets. The rule set contains an associated action that will be applied to any packets matching the criteria established in the rule set. The rule set contains a deny list and a permit list which are maintained in the kernel. A network packet must first pass a check of both the deny and permit lists if it is to be routed to its proper destination. The packet must not be expressly denied and it must be expressly permitted.

Command sets that allow the checking of the source and destination port numbers on the TCP and UDP transport layer protocols are typically implemented by packet filters. The check is to determine if an applicable permit or deny rule exists for that specific port and protocol combination. It is difficult for packet filters to apply any security policy checking to the ICMP protocol layer since ICMP does not utilize port numbers for its communication protocol. To effectively apply the security policy to ICMP, the packet filter must maintain state tables to ensure that an ICMP reply message was recently requested from an internal host.

Packet filters generally do not understand how to process state information in the high level protocols such as FTP because the packet filters are implemented in the network layer. An administrator can permit certain types of connections to be made to specific computers while prohibiting other types of connections to those computers by using a packet filter that includes the TCP/UDP port filtering capability. In the general algorithm for complete network packet inspection if no matching rule is found the network packet is dropped; if a matching rule that permits the communication is found then peer to peer communication is allowed, or if a matching rule is found that denies the communication the network packet is dropped.

Packet filtering is the least secure firewall technology because it does not inspect the network packet's application layer data and does not track the state of connections. Packet filtering allows access through the firewall with a minimal amount of scrutiny. If the checks of the rules succeed the network packet is allowed to be routed through the firewall as defined by the rules in the firewall's routing table. Packet filters often use a process called network address translation to readdress network packets of outgoing traffic. This readdressing process makes the outgoing

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

traffic appear to have originated from a different host rather than the internal host. The network readdress translation hides the topology and addressing schemes of trusted networks from untrusted networks.

Packet filtering firewall technology has several advantages. It is the fastest firewall technology since it performs fewer evaluations and does less processing than other technologies. It is often implemented in hardware components such as IP routers. By prohibiting connections between specific Internet sources and internal computers, a single rule in packet filtering can help protect an entire network. Packet filters do not require client computers to be specifically configured since the packet filter does all the work. Packet filter firewalls can be used to shield internal IP addresses from external users when used in conjunction with network address translation.

While the packet filtering firewall technology is the fastest technology it does have several disadvantages. Packet filter firewalls are less secure than application level firewalls because the packet filtering firewalls do not understand application layer protocols. Packet filtering firewalls cannot restrict access to protocol subsets for even the most basic services such as the PUT and GET commands in FTP. Packet filters do not inspect the payload of the packet. Decisions are not made based on the contents of the packet. The packet filter may allow dangerous forms of permissible traffic to pass through the firewall. An e-mail attachment that contains a virus could pass through the firewall if SMTP/POP connections are allowed. Packet filters are stateless since they do not keep application level information or information about a session. Packet filters have limited abilities to manipulate information within a packet. Packet filters do not offer higher level features such as HTTP object caching, URL filtering and authentication since packet filters do not understand the protocols being used and cannot discern one from another. Packet filters are not able to restrict the information that is passed from internal computers to services on the firewall server. Therefore intruders can potentially access the services on the firewall server. Packet filters have little or no audit event generation and alerting mechanisms. It can be difficult to test accept and deny rules of packet filters because of the complexity of supporting most non-trivial network services.

Packet filtering firewall technology has been improved by the addition of dynamic packet filtering. Dynamic packet filtering is useful in providing limited support for the UDP transport protocol. The firewall associates all UDP packets that enter the trusted network with a virtual connection. If a response packet is generated and sent back to the original requester, then a virtual connection is established and the packet is allowed to pass through the firewall server. In dynamic packet filtering architecture all incoming packets are compared against defined rules contained in a limited command set for one or more low level protocols. The rules determine if the packet is denied or accepted and passed on to the network stack. Each packet is then associated with additional state information based on information contained within the packet. Based on a combination of the data contained within the network packet and the state information, dynamic rules are added or removed from the packet filter. If a packet satisfies all of the packet filter rules it either propagates up the network stack for future processing or gets forwarded to the network host. The propagation route is based on whether the packet is destined for the firewall or a remote host. The packets then move from kernel space to application space. Once in application space all network packets associated with an authenticated session are processed by an application running on the firewall host. In addition to the advantages outlined

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

for packet filtering, dynamic packet filtering adds the advantage of not allowing unsolicited UDP packets into the trusted network. If a UDP request packet originated from the trusted network and is delivered to an untrusted host, the firewall server will allow what appears to be a response packet to be delivered to the originating host. For the response packet to be allowed back in it must contain a destination address that matches the original source address, a transport layer destination port that matches the original source port and the same transport layer protocol type.

Application Level Firewall

An application level firewall evaluates network packets for valid data at the application layer before allowing a connection. The firewall examines the data in all network packets at the application layer and maintains complete connection state and sequencing information. Other security items such as user password and service requests that appear in the application layer data can be validated by the firewall. Specialized application software and proxy services are included in most application layer firewalls. Proxy services manage traffic through a firewall for a specific service such as HTTP or FTP. Proxy services can provide increased access control, detailed checks for valid data, and generate audit records about the traffic they transfer because the proxy services are specific to the protocol that they are designed to forward.

An application level firewall analyzes the complete command set for a single protocol in application space. When an incoming network packet is received it moves up the hardened network stack until it reaches the highest protocol layer found in the packet. After the network stack finishes processing the packet, its data is passed from kernel space to application space then to the proxy server that is listening on a specific TCP or UDP port. Next the proxy service processes the data it has received. The data is compared to the acceptable command set rules, as well as to host and user permission rules. The proxy determines whether to accept or deny the packet based on the results of the rules comparison. Based on how it was configured, the proxy may also perform other functions such as URL filtering, data modification, authentication logging, and HTTP object caching. A proxy service consists of the proxy server, proxy client and protocol analysis modes of operation.

A proxy server and a proxy client are two components that are typically implemented as a single executable for each application proxy. A proxy server acts as the end server for all connection requests originated on a trusted network by a real client. Rather than allowing users to communicate directly with the other servers on the Internet, all communication between the internal users on the trusted network and the Internet passes through the proxy server. When the internal user wants to connect to an external service such as FTP or Telnet they send a request to the proxy server for the connection. The proxy server decides whether to permit or deny the request based on an evaluation of a set of rules that is managed for the individual network service. Proxy servers only allow those packets through that comply with the protocol definitions because the servers understand the protocol of the service they are evaluating. The proxy client is the component that talks to the server on the external network on behalf of the real client on the trusted network. The proxy server evaluates a real client's request for a service against the policy rules defined for that proxy and determines whether to approve the request. The proxy server forwards the request to the proxy client if the request is approved. The proxy client contacts the real server on the external network on behalf of the client. The proxy client relays requests from

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

the proxy server to the real server and relays responses from the real server to the proxy server. Then the proxy server relays the requests and responses between the proxy client and the real client.

Proxy services never allow direct connection between the real client on the trusted network and the real server on the external network. Proxy services force all network packets to be examined and filtered for suitability. All communication between the real user and the real service are handled by the proxy service. The proxy service is transparent to the user on the trusted network and the real service on the external network.

Proxy services are implemented on the top of the firewall host's network stack and operate only in the application space of the operating system. Proxy services are slower than packet filtering because each packet in a session is subjected to an examination process. Each network packet must pass through the low-level protocols in the kernel before being passed up the stack to application space. Once in the application space the proxies perform a thorough inspection of the packet headers and packet data. After inspection and acceptance the packet must travel back down to the kernel, and then back down the stack for distribution. Additional checks can be performed by application level firewalls to ensure that a network packet has not been spoofed. Application level firewalls can often perform network address translation.

Application level firewall technology using proxy services has several advantages. Proxy services enforce high level protocols such as HTTP and FTP. Information about the communications passing through the firewall server is maintained by the proxy service. Proxy services can permit access to certain network services, while denying access to others. Packet data can be processed and manipulated by proxy services. Internal IP addresses are shielded from the external world because proxy services do not allow direct communications between external server and internal computers. Administrators are able to monitor attempts to violate the firewall's security policies using the audit records that proxy services can generate.

Although application level firewalls provide increased security over a packet filtering firewall there are some disadvantages to using an application level firewall. Application level firewalls are slower since inbound data is processed by the application and by its proxy. A new proxy usually must be written for each protocol that is to pass through the firewall. This can cause the number of available network services and their scalability to be limited. Proxy services are vulnerable to operating system and application level bugs. Most application level firewalls require extensive support from the operating system to run correctly. The firewalls need support from TCP/IP, Win32, Winsock, NDIS, and the standard C library. The security of the firewall server can be effected by problems in these operating system components.

When determining which firewall technology to use the system administrator needs to evaluate several opposing aspects. There is a trade off between performance and security. The performance and security trade off is based on how far up the network stack the packet must travel, as well as what level of security checks are being performed on each packet. Generally packet filter firewalls provide the highest level of performance, followed by dynamic packet filtering and then application level firewalls. The level of security checks normally follows a reverse order of performance because as network packets pass through more protocol layers, they

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

are inspected in more detail. Therefore, application level firewalls are considered more secure than dynamic packet filtering firewalls, which are more secure than packet filtering firewalls. In an application level firewall all the network packets are sent up one network stack and down a different stack resulting in two separate network sessions. This makes application level firewalls generally the slowest firewall technology. The processing time required for network packet movement is greater with application level firewalls because these firewalls implement the broadest set of security checks. Application level firewalls are considered to generally provide the best security. When implementing a firewall solution an organization needs to evaluate the advantages and disadvantages of each firewall technology and apply the best solution to meet the organization's security requirements.

References

Tyson, Jeff "How Firewalls Work" 2001
URL: http://www.howstuffworks.com/firewall.htm

Unknown "Configure Firewall Packet Filtering" July 1, 1999.
URL: http://www.cert.org/security-improvements/practices/p058.html

Unknown "Application Proxy vs. Stateful Inspection Firewall Technology" June 1, 2000
URL: http://www.firetower.com/applicationproxy.html

McGibbon, Stephan M. "Firewalls and Internet Security" 2000
URL: http://secinf.net/fw/steph/

Unknown "Design the Firewall System" July 1, 1999
URL: http://www.cert.org/security-improvements/practices/p053.html

Unknown "Securing Your Network with the Cisco Centri Firewall" 2000
URL: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch3.htm

© SANS Institute 2000 - 2002 Author retains full rights.