Firewall Design Principles

Software Engineering 4C03

Dr. Krishnan

Stephen Woodall,
April 6th, 2004

Firewall Design Principles

Stephen Woodall

Introduction

A network security domain is a contiguous region of a network that operates under a single, uniform security policy. Whenever domains intersect, there is a potential need for security to control traffic allowed into the network. Firewall technology can be used to filter this traffic. The most common boundary where firewalls are applied is between an organization's internal network and the internet. This report will provide readers with a resource for understanding firewall design principles used in network security.

Firewall Interaction with the OSI and TCP/IP Network Models

Network Firewalls operate at different layers of the OSI and TCP/IP network models. The lowest layer at which a firewall can operate is the third level which is the network layer for the OSI model and the Internet Protocol layer for TCP/IP. At this layer a firewall can determine if a packet is from a trusted source but cannot grant or deny access based on what it contains. Firewalls that operate at the highest layer, which is the application layer, know a large amount of information including the source and the packet contents. Therefore, they can be much more selective in granting access. This may give the impression that firewalls functioning at a higher layer must be better, which is not necessarily the case. The lower the layer the packet is intercepted the more secure the system. If the intruder cannot get past the third layer, it is impossible to gain control of the operating system. [1]

Firewalls fall into four broad categories: packet filters, circuit level gateways, application level gateways and stateful multilayer inspection firewalls. Packet filtering firewalls operate at the network level of the OSI model or the IP layer of TCP/IP. In a packet filtering firewall, each packet is compared to a set of rules before it is forwarded. The firewall can drop the packet, forward it, or send a message to the source. Circuit level gateways operate at the session layer of the OSI model, or the TCP layer of TCP/IP. Circuit level gateways examine each connection setup to ensure that it follows legitimate TCP handshaking. Application level gateways or proxies operate at the application layer. Packets received or leaving cannot access services for which there is no proxy. Stateful multilayer inspection firewalls combine aspects of the other three types of firewalls. They filter packets at the network layer, determine whether packets are valid at the session layer, and assess the contents of packets at the application layer. [2] Diagrams of how Firewalls Interact with the OSI and TCP/IP Network Models can be found in Appendix A.

Firewall Architectures

After deciding the security requirements for the network the first step in designing a firewall is deciding on a basic architecture. There are two classes of firewall architectures, single layer and multiple layer. In a single layer architecture, one host is allocated all firewall functions. This method is usually chosen when either cost is a key factor or if there are only two networks to connect. The advantage to this architecture is any changes to the firewall need only to be done at a single host.

The biggest disadvantage of the single layer approach it provides single entry point. If this entry point is breached, the entire network becomes vulnerable to an intruder.

In a multiple layer architecture the firewall functions are distributed among two or more hosts normally connected in series. This method is more difficult to design and manage, it is also more costly, but can provide significantly greater security by diversifying the firewall defense. A common design approach for this type of architecture using two firewall hosts with a demilitarized network (DMZ) between them separating the Internet and the internal network. Using this setup traffic between the internal network and the Internet must pass through two firewalls and the DMZ. [3] An example of this architecture can be found in Appendix B.

Firewall Types

After the security requirements are established, a basic architecture is selected then Firewall functions can be chosen to meet these needs. The following is a detailed discussion of the 4 firewall categories:

Packet Filtering Firewalls

The first generation of firewall architectures appeared around 1985 and came out of Cisco's IOS software division. These are called packet filter firewalls.[4] Packet Filtering is usually performed by a router as part of a firewall. A normal router decides where to direct the data, a packet filtering router decides if it should forward the data at all. Packet Filtering rules can be set on the following: physical network interface the packet arrives on; source or destination IP address, the type of transport layer (TCP, UDP, ICMP), or the transport layer source or destination ports. Packet filtering firewalls are low cost, have only a small effect on the network performance, and do not require client computers to be configured in any particular way. However, packet filtering firewalls are not considered to be very secure on their own because they do not understand application layer protocols. Therefore, they cannot make content-based decisions on the packets, which makes them less secure than application layer and circuit level firewalls. Another disadvantage of Packet filtering firewalls are they are stateless and do not retain the state of a connection. They also have very little or no logging capability which makes it hard to detect if the network is under attack. Testing the grant and deny rules is also difficult which may leave the network vulnerable or incorrectly configured. [5]

Circuit Level Gateways

Around 1989-1990, Dave Presotto and Howard Trickey of AT&T Bell Labs pioneered the second generation of firewall architectures with research in circuit relays which were called circuit level gateways.[4] Circuit level gateways are used for TCP connections to observe handshaking between packets to ensure a requested session is legitimate. Normally, it would store the following information: a unique session identifier, the state of the connection (i.e., handshake established or closing), sequencing information, source or destination IP address, and the physical network interface through which the packet arrives or departs. The firewall then checks to see if the sending host has permission to send to the destination, and that the receiving host has permission to receive from the sender. If the connection is acceptable, all packets are routed through the firewall with no more security tests. The advantages of circuit level gateways is that they are usually faster than application layer firewalls because they perform less evaluations and they can also protect a network by blocking connections between specific Internet sources and internal hosts. The main disadvantages to circuit level gateways are that they cannot restrict access to protocol subsets other than TCP and similarly to packet filtering, testing the grant and deny rules can be difficult which may leave the network vulnerable or incorrectly configured. [6]

Application Level Gateways

The third generation of firewall architectures called Application level gateways was independently researched and developed during the late 1980s and early 1990s mainly by Gene Spafford of Purdue University, Marcus Ranum, and Bill Cheswick of AT&T Bell Laboratories.[4] Application level gateways or proxy firewalls are software applications with two primary modes (proxy server or proxy client). When a user on a trusted network wants to connect to a service on an untrusted network such as the Internet, the request is directed to the proxy server on the firewall. The proxy server pretends to be the real server on the Internet. It checks the request and decides whether to permit or deny the request based on a set of rules. If the request is approved, the server passes the request to the proxy client, which contacts the real server on the Internet. Connections from the Internet are made to the proxy client, which then passes them on to the proxy server for delivery to the real client. This method ensures that all incoming connections are always made with the proxy client, while outgoing connections are always made with the proxy server. Therefore, there is no direct connection between the trusted and untrusted networks. The main advantages are that application level gateways can set rules based on high-level protocols, maintain state information about the communications passing through the firewall server, and can keep detailed activity records. The main disadvantages are its complex filtering and access control decisions can require significant computing resources which can cause performance delays and its vulnerability to operating system and application level bugs. [7]

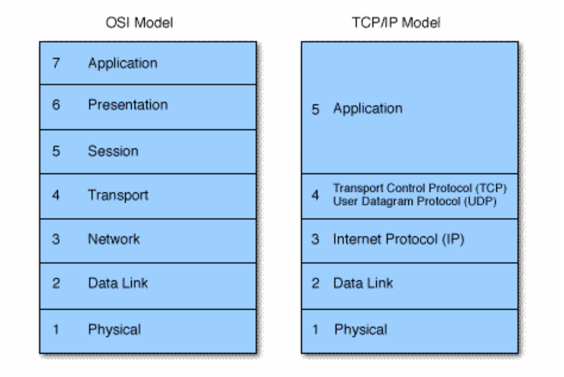
Stateful Multilayer Inspection Firewalls

Check Point Software released the first commercial product based on this fourth generation architecture in 1994 called stateful multilayer inspection firewalls.[4] Stateful multilayer inspection firewalls provide the best security of the four firewall types by monitoring the data being communicated at application socket or port layer as well as the protocol and address level to verify that the request is functioning as expected. An example is if during an FTP session the port numbers being used or an IP address were to change, the firewall would not permit the connection to continue. Another advantage is when a specific session is complete, any ports that were being used are closed. Stateful inspection systems can dynamically open and close ports for each session which differs from basic packet filtering that leaves ports in a constant opened or closed state. The main disadvantage to stateful multilayer inspection firewalls is that they can be costly because they require the purchase of additional hardware and/or software that is not normally packaged with a network device. [8, 9]

Conclusion

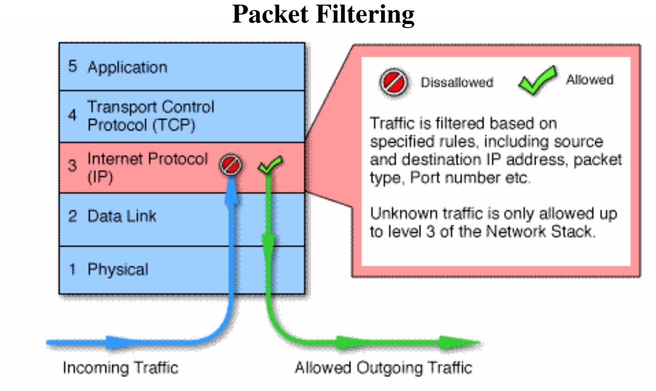
There are no specific rules that can be applied when designing a firewall because there are too many factors to consider. There are general guidelines that will help if followed. Start by denying all access to the network by default. In other words, start with a gateway that routes no traffic. Determine the inbound access policy and then specify the outbound access policy. Once the inbound and outbound policies have been specified, an architecture with appropriate firewall functions can be chosen that fits within the budget. External resources may be needed if the complexity of the firewall needed to satisfy the security requirements are too great for the in-house expertise. A costly firewall that is complex and not administrated properly can be less effective then a straightforward firewall costing many times less. [10]

Appendix A - Firewall Interaction with the OSI and TCP/IP Network Models



OSI Model	TCP/IP Model
7 Application	5 Application
6 Presentation	
5 Session	
4 Transport	4 Transport Control Protocol (TCP) User Datagram Protocol (UDP)
3 Network	3 Internet Protocol (IP)
2 Data Link	2 Data Link
1 Physical	1 Physical

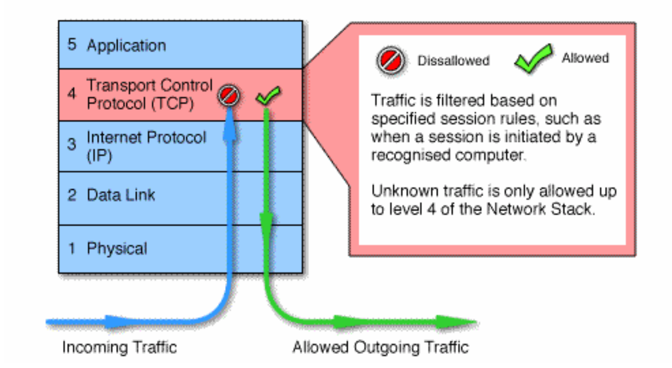
Packet Filtering



Traffic is filtered based on specified rules, including source and destination IP address, packet type, Port number etc.

Unknown traffic is only allowed up to level 3 of the Network Stack.

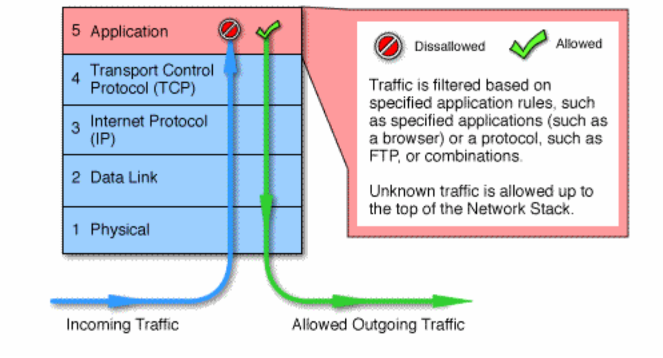
Circuit Level Gateways



Traffic is filtered based on specified session rules, such as when a session is initiated by a recognised computer.

Unknown traffic is only allowed up to level 4 of the Network Stack.

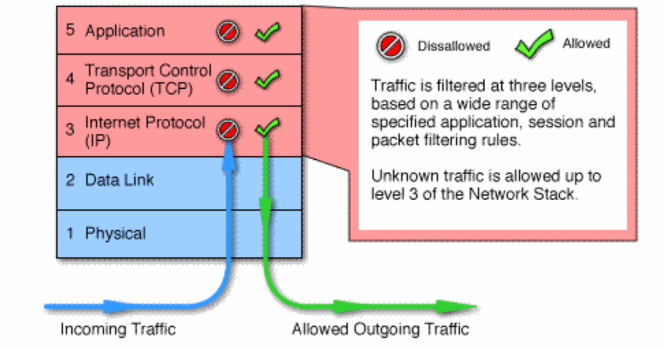
Application Level Gateways



Traffic is filtered based on specified application rules, such as specified applications (such as a browser) or a protocol, such as FTP, or combinations.

Unknown traffic is allowed up to the top of the Network Stack.

Stateful Multilayer Inspection

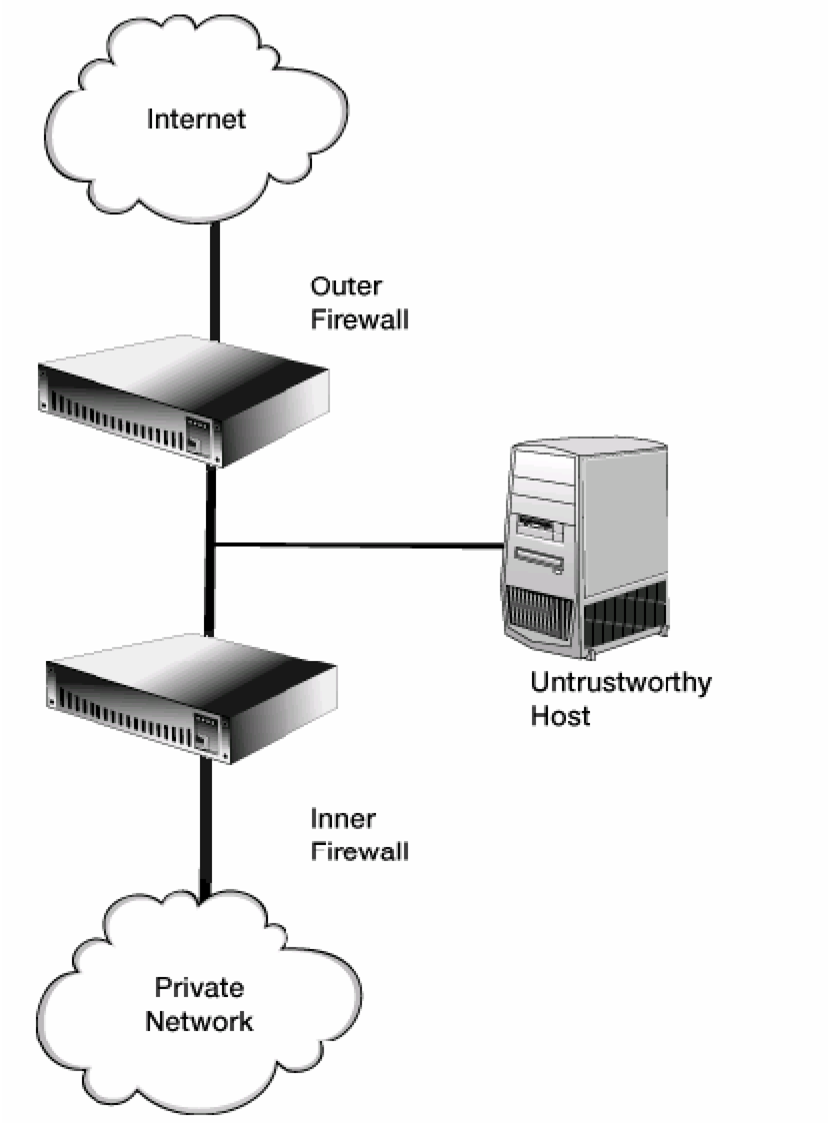


Traffic is filtered at three levels, based on a wide range of specified application, session and packet filtering rules.

Unknown traffic is allowed up to level 3 of the Network Stack.

Vicomsoft, 2003. *Firewall White Paper-What different types of firewalls are there?* http://www.firewall-software.com/firewall_faqs/types_of_firewall.html

Appendix B – Dual Firewall with DMZ Network Architecture



Carnegie Mellon University, 1999. *Design the firewall system?*
http://www.cert.org/security-improvement/graphics/sim008f1-7.gif

References:

[1] Vicomsoft, 2003. *Firewall White Paper -OSI & TCP/IP Network Models*. [Available] http://www.firewall-software.com/firewall_faqs/firewall_network_models.html (March, 25, 2004)
[2] Vicomsoft, 2003. *Firewall White Paper-What different types of firewalls are there?* [Available] http://www.firewall-software.com/firewall_faqs/types_of_firewall.html (March, 25, 2004)
[3] Carnegie Mellon University, 1999. *Design the firewall system?* [Available] http://www.cert.org/security-improvement/practices/p053.html (March, 25, 2004)
[4] ITsecurity.com, 2002. *History of the Firewall* [Available] http://www.itsecurity.com/dictionary/dictionary.htm (March, 26, 2004)
[5] ITsecurity.com, 2002. *Packet Filtering* [Available] http://www.itsecurity.com/dictionary/packfilt.htm (March, 26, 2004)
[6] ITsecurity.com, 2002. *Circuit Level Gateway* [Available] http://www.itsecurity.com/dictionary/circgate.htm (March, 26, 2004)
http://www.itsecurity.com/dictionary/circgate.htm
[7] ITsecurity.com, 2002. *Application Level Gateway* [Available] http://www.itsecurity.com/dictionary/packfilt.htm (March, 26, 2004)
[8] ComTest Technologies, 2000. *Network Security: Firewalls* [Available] http://www.comtest.com/tutorials/firewalls.html (March, 26, 2004)
[9] University of Georgia, 2003. *Firewall Technology* [Available] http://www.infosec.uga.edu/firewall.html (March, 26, 2004)
[10] Vicomsoft, 2003. *Firewall White Paper-What How o I Implement Firewall Security?* [Available] http://www.firewall-software.com/firewall_faqs/implement_firewallsecurity.html (March, 25, 2004)