NATIONAL SECURITY AGENCY
Enterprise Firewall Types

Enterprise firewalls are placed on the perimeter of a network to enforce a security policy by allowing or denying certain network traffic. The three types of enterprise firewalls (ordered by increasing complexity) are:

1) Packet Filtering
2) Stateful Packet Filtering
3) Application Proxies

Packet Filtering

A packet filter only examines traffic based on the packet header. The header includes such fields as the source and destination IP addresses, the source and destination ports, and the network protocol used.

Packet filtering is usually employed on perimeter routers in the form of access control lists (ACLs) and is very fast and effective. It can be tedious to configure since rules must be defined for each protocol, range of addresses, and direction of flow. For example, consider the case where host A wants to talk to host B on TCP port 23. Both the desired rule and its reciprocal rule must be entered into the ACL:

Rule Descriptors	In-Flow	OutFlow
Source IP	A	B
Destination IP	B	A
Source port	Any	23/TCP
Destination port	23/TCP	Any
Decision	Allow	Allow

Stateful Packet Filtering

Like packet filtering, a stateful packet filter works at the network and transport layers (on the OSI model) by examining the packet header. Unlike packet filtering, if the flow is allowed, a stateful packet filter keeps track of information about the connection's state and enters it into a state table. Entries include source and destination IP addresses, the firewall's network interfaces, source and destination ports, protocol, ACK and SEQ numbers, etc.

Example State Table	
Rule Descriptions	**Flow**
Source IP	A
Destination IP	B
Source port	61582
Destination port	23
ACK	481399856
SEQ	36910463
Firewall interface	eth0

This concept of state allows the rules to be more concise than in packet filtering since reciprocating rules are systematically inferred and not manually entered.

System performance is increased because packets entering the firewall are first compared to the state table, not to the ACL. If a packet is part of an established connection, then it is allowed. If the packet cannot be associated with an established connection, then a complete check against the ACL rules is performed.

Many stateful packet filters can alter banner information to obfuscate a server that is being protected. Some stateful packet filters have the ability to look into the application layer data and make additional filtering decisions. An example of this is to allow HTTP GET messages but not HTTP POST messages. Stateful packet filters are limited in their protocol knowledge and lack the ability to filter on encrypted traffic.

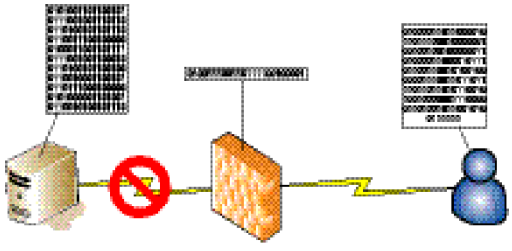
Examples of stateful packet filters include the Cisco PIX and the NetScreen firewalls.

Application Proxies

An application proxy is the most sophisticated firewall type. In addition to the features of both packet filters and stateful packet filters, application proxies contain both a server and a client process for each protocol they support. They will establish two completely separate sessions: one from the client to firewall, and another from the firewall to server. In this way, they establish a proxy that inspects and rewrites all packets for that protocol, preventing direct contact between the client and server. Since the connection is proxied through the firewall, another advantage is the ability to read encrypted sessions.

In theory, the proxy will have a complete understanding of how the protocol functions and be able to enforce compliance to established standards. For protocols where a proxy does not exist, a generic proxy can be created that allows a protocol to traverse the firewall. Although these generic proxies don't offer as much protection as an application-aware proxy, they do have the capability for robust logging.

In comparison to packet filters and stateful packet filters, application proxy performance is slower due to the complexity of filtering through all the application data. They are also more susceptible to overflow attacks because they are more complex and have a larger code base.



Sample Firewall Architecture

Conclusion

The line between stateful packet filters and application proxies is beginning to fade, while pure packet filtering has predominantly moved to the perimeter router. The best type of firewall is the one that gives a balance of security and functionality appropriate to established security policy.

No firewall will keep the network 100% safe; do not depend on one device to secure a network. Adopt a "defense in depth" strategy: deploy multiple defense mechanisms between adversaries and their targets including both *protection* and *detection* methods.