Introduction to firewalls

What is a firewall?  
Security checkpoint usually between a protected and untrusted network or between a networked device and a network  
-Private network and Internet  
-Different parts of a private network  
-PC and the network it is connected to  
It filters incoming and outgoing data

Stand-alone Hardware firewall products  
CISCO ASA 6606

Integrated Broadband Router and Firewall  
CISCO 2901

Software Firewall  
Norton Internet Security

Conventional Packet-Filtering Firewalls – Makes independent decision per packet, No concept of TCP sessions or UDP flows  
Stateful Packet-Filtering Firewalls – Recognises TCP connections or UDP flows, Filters packets by connection/flow. Stateful connection table.  
Application Level Firewall – All above + Protocol checking/fidelity

Software Firewalls - Potential hazard: packets are already “on” the machine before the firewall checks them.

Packet Filtering Firewall  
(Conventional)  
Access Control List ACL  
Inspects packets independently on their own mertis  
Has no concept of TCp sessions and connections  
Is stateless (has no memory)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Rule | Source IP | Source Port | Dest IP | Dest Port | Protocol | Access | Explanation |
| A | \* | \* | 10.1.0.1 | \* | \* | Deny | Deny any access to 10.1.0.1 |
| B | \* | \* | 10.2.12.12 | \* | \* | Deny | Deny any access to 10.2.12.12 |
| C | 10.1.0.0/16 | \* | \* | 80 | TCP | Allow | Only traffic from 10.1.0.0 destined for port 80 via TCP is allowed |
| D | \* | 80 | 10.1.0.0/16 | \* | TCP | Allow |  |
| E | 10.1.0.0/16 | \* | \* | 80 | TCP | Allow |  |
| F | \* | 80 | 10.1.0.0/16 | \* | TCP | Allow |  |
| Z | \* | \* | \* | \* | \* | Deny | Clean up rule |

ACL rules can be based on many things  
Source/Dest IP  
Source/Dest Port

Stateful Firewall/ Stateful Packet Inspection  
Firewall does not always respond to the same packet in the same way  
Depends on what “state” the firewall is in  
Firewall states can be made to correspond with the status of TCP connections

Firewall allows/denies connections and filters packets based on whether they belong t allowed connection  
“Source” and “destination” now refer to connections, not individual packets  
Stateful Connection Table  
-New connection added to a dynamic list  
Separate table from main rulebase

UDP does not use connection handshake, just sends datagrams out  
Firewall could act like a packet filter for UDP but this would be less efficient since all UDP packets would need to be checked against the main rulebase  
UDP flow states: Begin when the first packet is received, ended by the firewall time-out mechanism

<action><protocol>from<source\_IP><source\_port>to<destination\_IP><destination\_port>

1. Allow anyone to access a website on the server located at 192.71.12.8
2. Allow internal users to send mail via SMTP (TCP port 25) on the mail server located at 141.241.100.10 and to retrieve mail from the same server using POP3 (TCP port 110)
3. Allow internal users to access any websites they wish except for a server located at 12.7.6.15
4. Allow external users to send mail into the network via SMTP to the mail server located at 192.71.12.15
5. Deny anything that is not explicitly allowed and to protect the firewall itself from attack.

<Deny> <TCP> from <\*><\*> to <192.71.0.1><\*>  
<Allow> <TCP> from <\*><\*> to <192.71.12.8><80>  
<Allow> <TCP> from <192.71.0.0/16><\*> to <141.241.100.10><25>  
<Allow> <TCP> from <192.71.0.0/16><\*> to <141.241.100.10><110>  
<Deny> <TCP> from <192.71.0.0/16><\*> to <12.7.6.15><80>  
<Allow> <TCP> from <192.71.0.0/16><\*> to <\*><80>  
<Allow> <TCP> from <\*><\*> to <192.71.12.15><25>  
<Deny> <\*> from <\*><\*> to <\*><\*>