Packet Filtering is one of the core services provided by firewalls. Packets can be filtered (permitted or denied) based on a wide range of criteria:

• Source address

• Destination address

• Protocol Type (IP, TCP, UDP, ICMP, ESP, etc.)

• Source Port

• Destination Port

Packet filtering is implemented as a rule-list:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Number | Action | Protocol | Source Add | Source Port | Destination Add | Destination Port |
| 1 | Deny | TCP | Any | Any | 172.16.1.5 | 666 |
| 2 | Permit | IP | Any | Any | 172.16.1.5 | Any |
| 3 | Permit | TCP | Any | Any | 172.16.1.1 | 443 |
| 4 | Permit | TCP | Any | Any | 172.16.1.1 | 80 |
| 5 | Permit | TCP | Any | Any | 172.16.1.10 | 25 |
| 6 | Deny | TCP | 66.1.1.5 | Any | 172.16.1.10 | 110 |
| 7 | Permit | TCP | Any | Any | 172.16.1.10 | 110 |

The order of the rule-list is a critical consideration. The rule-list is always parsed from top-to-bottom. Thus, more specific rules should always be placed near the top of the rule-list, otherwise they may be negated by a previous, more encompassing rule.

Also, an implicit ‘deny any’ rule usually exists at the bottom of a rule-list, which often can’t be removed. Thus, rule-lists that contain only deny statements will prevent all traffic.