**STATEFUL FIREWALL**

* Remembers information between states, context-sensitive, more powerful than stateless.
* It is also referred to as static packet filtering, static filtering, or packet filtering.
* Easy to implement and we do not need a specialized IOS version to run it.
* Applications that use random port number would have trouble in operation.

Common static filter packets based on one or more of the following

* Source ip address or port number
* Destination IP address or port number
* Protocol number

**STATELESS FIREWALL (AKA dynamic packeting)**

* Important is preventing TCP based attack.
* Allows internal ports to have conversation with the outside hosts
* Outside hosts would not be allowed to start conversation with the inside hosts.
* Would accomplish this by keeping session table.

STATE TABLE

* Would have source and destination IP address and port numbers
* TCP and UDP flag settings
* TCP sequencing information

**TCP 3 WAY HANDSHAKE**

* Clients initiate communication with SYN packet.
* Recipient replies with SYN-ACK
* Clients replies with ACK

Not remember information between states, context-free, less powerful than stateful

As we move up in the OSI stack it tends to be more stateful as we go lower it would be stateless.

Table

Description automatically generated with medium confidence

**MIDDLEMAN BETWEEN THE INTERNAL USERS AND OUTSIDE DESTINATIONS :PROXY SERVER**

* Inside users attempts to connect to outside destination.
* The proxy server receives that attempt, holds it, and then itself attempts to connect to the destination
* The proxy server connects, gets the info the inside user wanted ( a web page ) and then presents that information to the inside user.
* Proxy server allows to tie down network access, since proxy server works to the application layer.