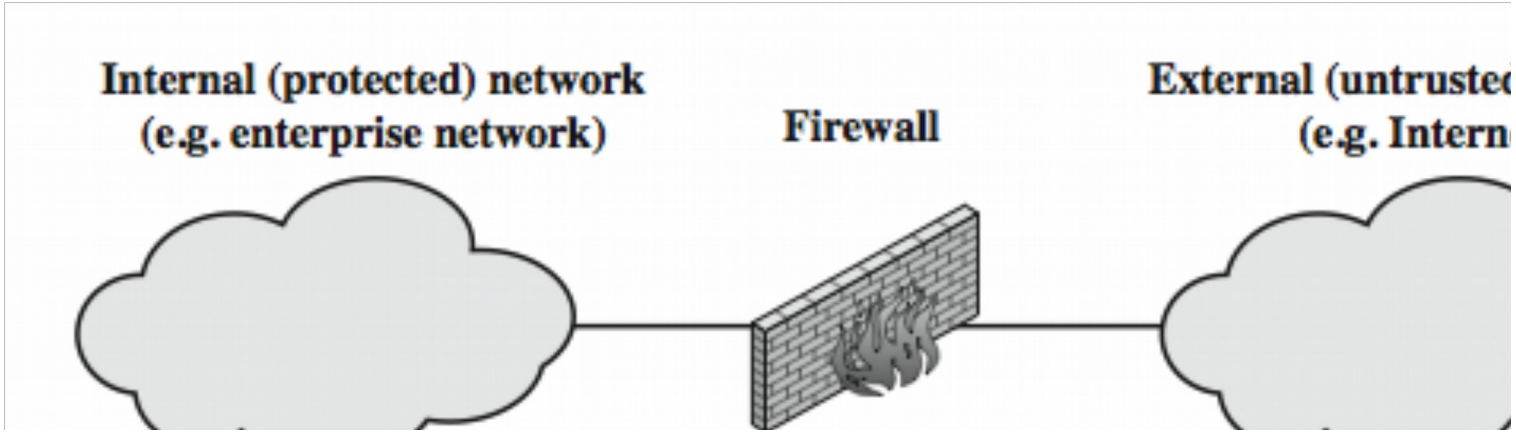
Module 5

Network Security and Applications

Firewalls

- It is a single point of defense between two networks
- It can be simply a router or a multi-computer or multi router solution
- It can be a router or a group of routers and computers to enforce access control between two networks

Firewalls


Internal (protected) network
(e.g. enterprise network)
Firewall
External (untruste
(e.g. Intern

Limitations

It cannot protect from attacks bypassing it

- e.g. trusted organisations, trusted services)

It cannot protect against internal threats

- eg disgruntled employees

It cannot protect against access via WLAN

- if improperly secured against external use

It cannot protect against malware imported via laptops, pendrives or other storage devices which are already infected

Types of Firewall

1. Packet Filters
2. Circuit Level Firewalls
3. Application Layer Firewalls
4. Dynamic packet filters
5. Stateful Inspection firewall
6. Guard
7. Personal Filrewall

Packet Filters

- It works at the network layer
- Each packet is examined to see if it matches one of the set of rules
- These rules specify the allowable data flow and also the direction of data flow
- The actions taken are: accept, reject and drop

Packet Filters

- The following factors are matched
  - Physical network interface at which the packet arrives on
  - Address from which the data is coming from
  - Address to which the data is going to
  - Type of transport layer protocol (TCP,UDP)
  - Transport layer source port
  - Transport layer destination port

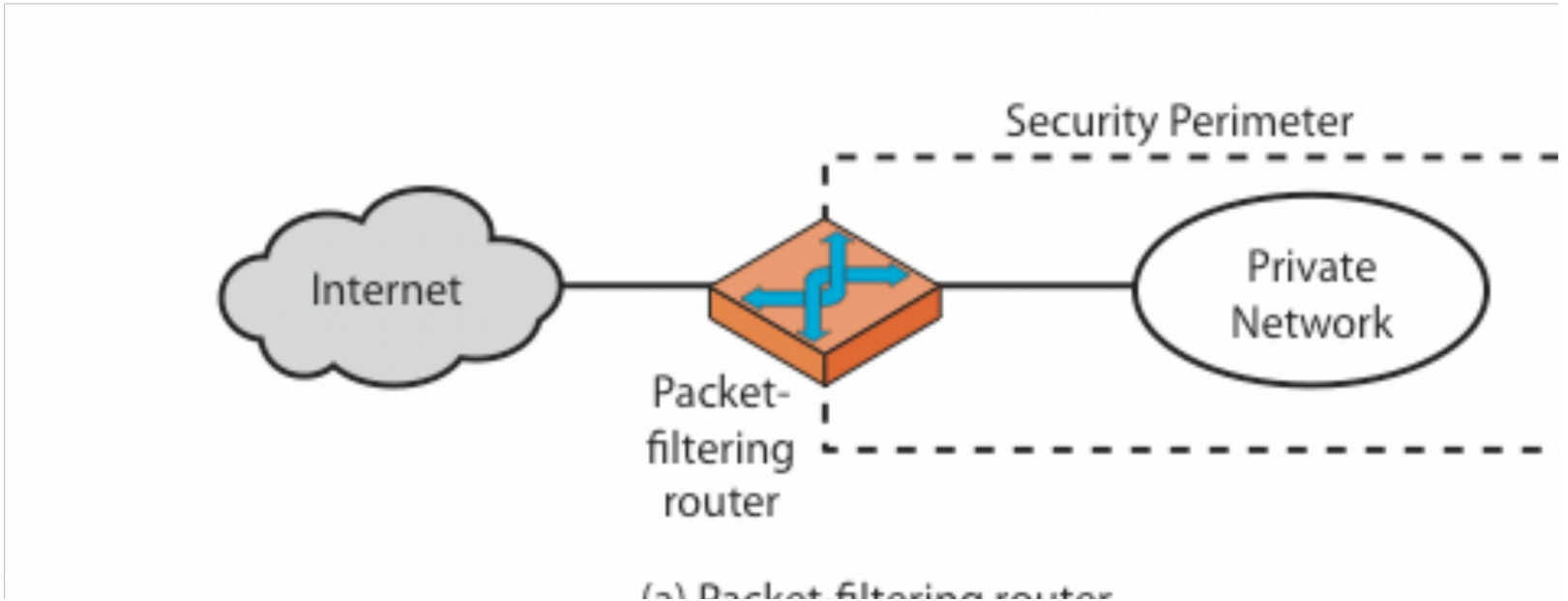
Packet Filters

- Advantages
  - Faster than other techniques
  - Less complicated because a single rule controls denying or allowing the packet
  - Do not require client computers to be configured specially
  - Shield the internal IP address from the external world

Packet Filters

- Disdvantages
  - Doesn’t understand application layer protocols and hence can’t restrict access to FTP services such as PUT and GET commands
  - They are stateless and hence not suitable for Application Layer protocols
  - No audit mechanism and alert generation mechanism

Packet Filters



(a) Packet-filtering router

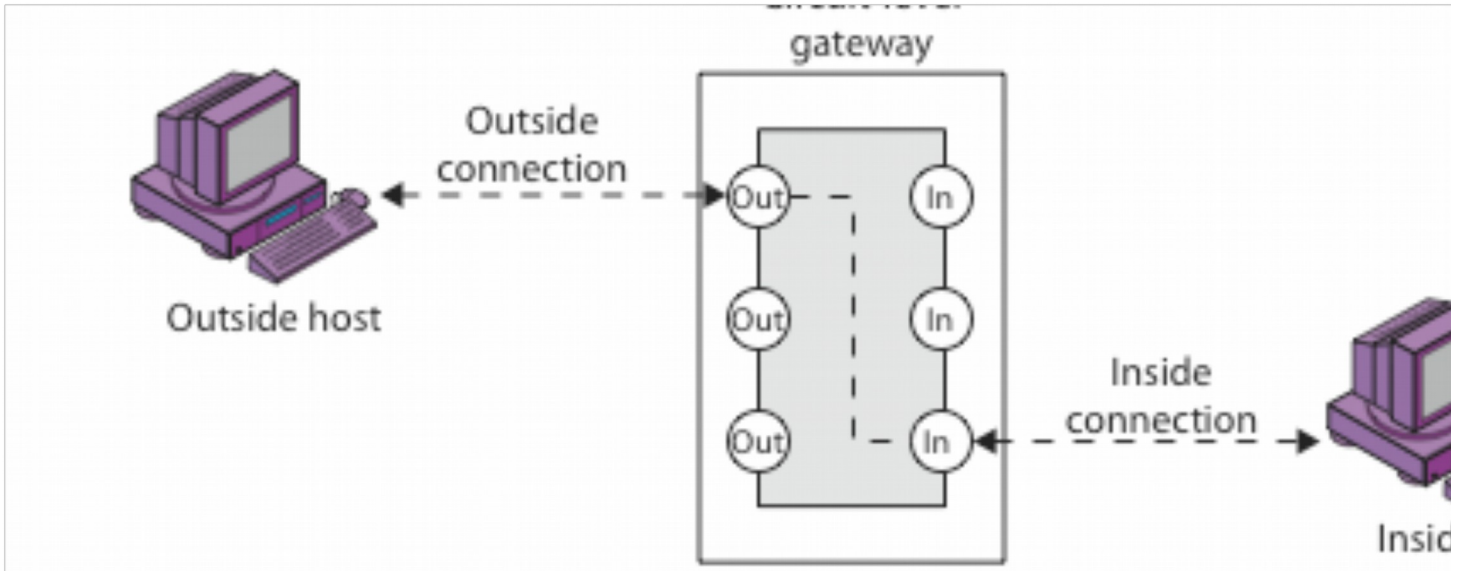
Circuit Level Filters

- It operates at the transport and session layers of OSI model
- It validates TCP, UDP sessions before opening a connection or circuit
- When a session is established, the firewall maintains a table of valid connections and lets the data pass through when the session information matches entry in the table
- The table entry is deleted and the circuit is closed once the session is terminated

Circuit Level Filters

- When a connection is setup, the circuit level firewall stores the following information :
  - A unique session identifier for the connection
  - State of the connection(handshake,established, closing)
  - Sequencing Information
  - Source IP address
  - Destination IP address
  - Physical network interface through which the data arrives
  - Physical network interface through which the packet goes out

Circuit Level Filters



Circuit Level Filters

- Advantages
  - Faster than Application Layer Firewall
  - More secured than packet filter firewall
  - Maintain limited state information of the protocols
  - Protect against spoofing attacks
  - Shields the internal IP address from external networks by Network Address Translation(NAT)

Circuit Level Filters

- Disdvantages
  - Can’t restrict access to protocol subsets other than TCP
  - Limited audit event generation capabilities
  - Can’t perform security checks on higher level protocols

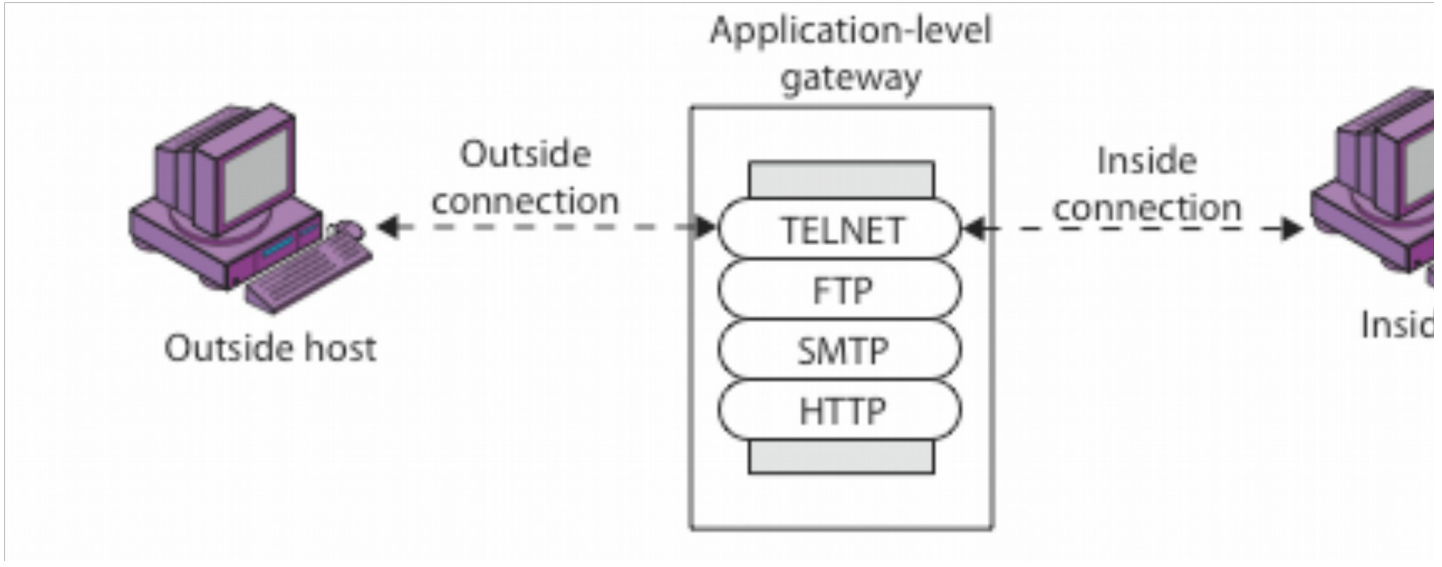
Application Level Filters

- It evaluates network packets for valid data at the Application Layer before allowing a connection
- It uses special purpose programs called proxy services
- The proxy services manage data transfer through a firewall for a specific service such as FTP or http
- The proxy services do not allow direct connection between a real service and the user
- A proxy service has two components:
  - Proxy server
  - Proxy client

Application Level Filters

- When a real client wants to access a service like FTP, the request is sent to the proxy server (because the user's default gateway is set to proxy server)
- The proxy server evaluates the request and decides to deny or allow it depending on a set of rules that are managed for network service
- Once the packet is allowed by the proxy server, it is sent to the proxy client who contacts the actual server providing that service
- The proxy client relays back the information sent by the actual server to the proxy server who decides whether to send the information to the client or not

Application Level Filters



Application Level Filters

- Advantages
  - Enforce and understand high level protocols like HTTP, FTP
  - Maintain information about the communication passing through the firewall sever
  - Can be used to deny access to certain network services while allowing others
  - Shields internal IP address by not allowing direct communication between external servers and internal systems

Application Level Filters

- Advantages
  - Transparent between user and external network
  - Capable of manipulating packet data
  - Provides features like HTTP object caching, URL filtering and user authentication
  - Generates auditing records, allowing administrators to monitor threats to the firewall

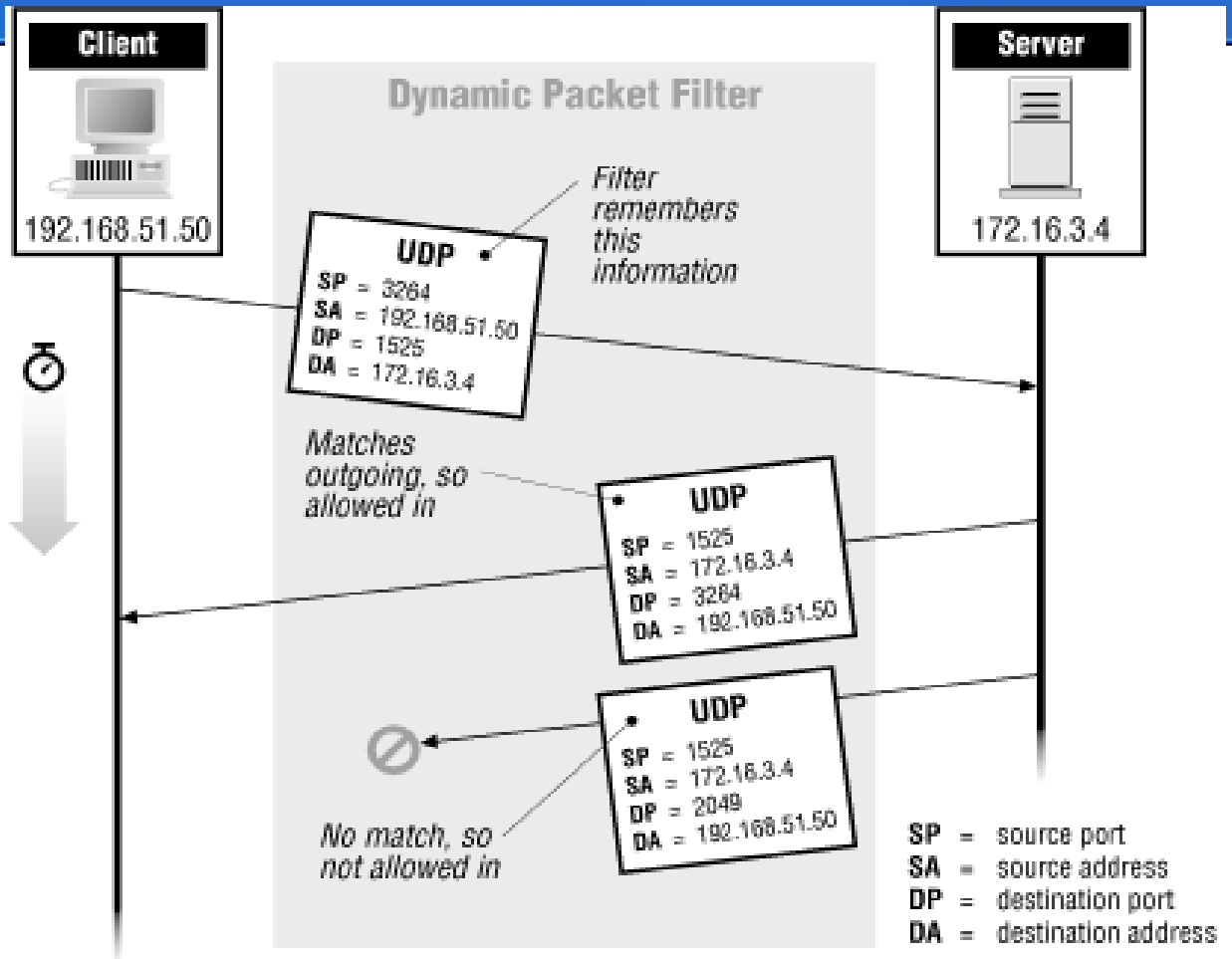
Application Level Filters

- Disdvantages
  - Require replacing the native network stack on firewall server
  - Do not allow network servers to run firewall servers because proxy servers use the same ports
  - Slow in nature which leads to performance degradation
  - Not scalable
  - Proxy services require modifications to client procedures
  - Relies on OS support and thus are vulnerable to bugs

Dynamic Level Filters

- It allows modifications of security rules dynamically
- It is suitable for providing limited support for UDP
- It is most suitable for application layer protocols like DNS
- This protocol associates all UDP packets that goes from the internal network to the external network and vice versa with a virtual connection
- The information corresponding to a virtual connection is remembered for a small unit of time

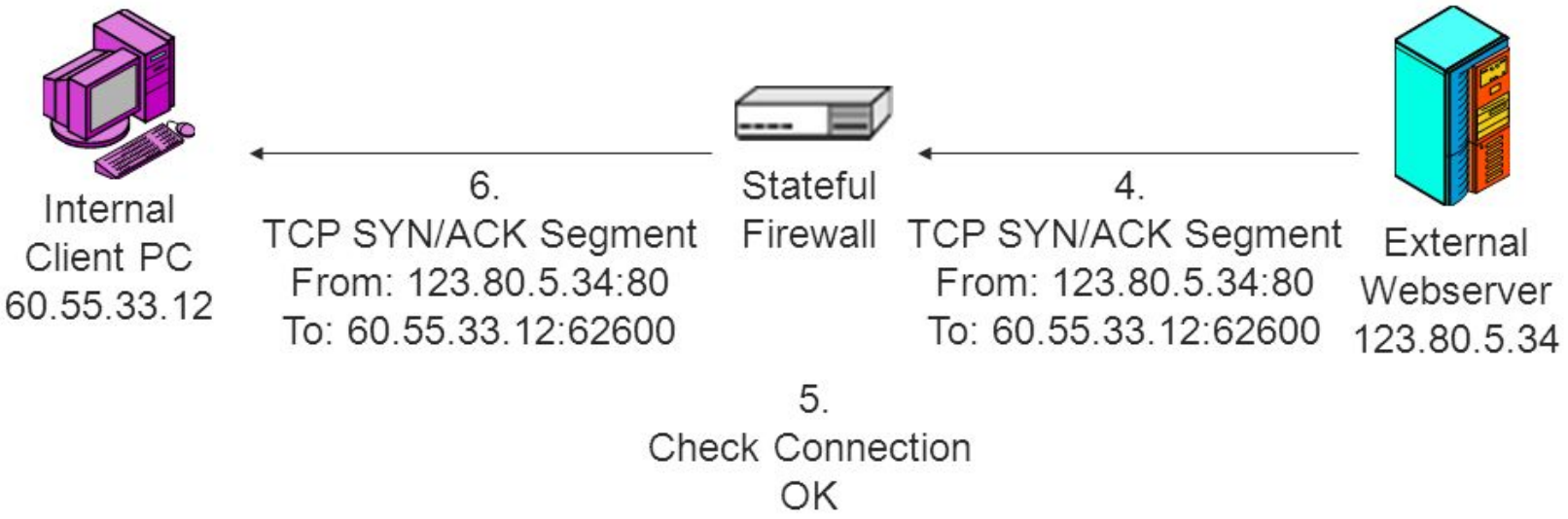
Dynamic Level Filters



Stateful Inspection Firewall

- It maintains state information from one packet to another in the input stream
- It tracks the sequence of packets as well as the conditions from one packet to another

Stateful Inspection Firewall



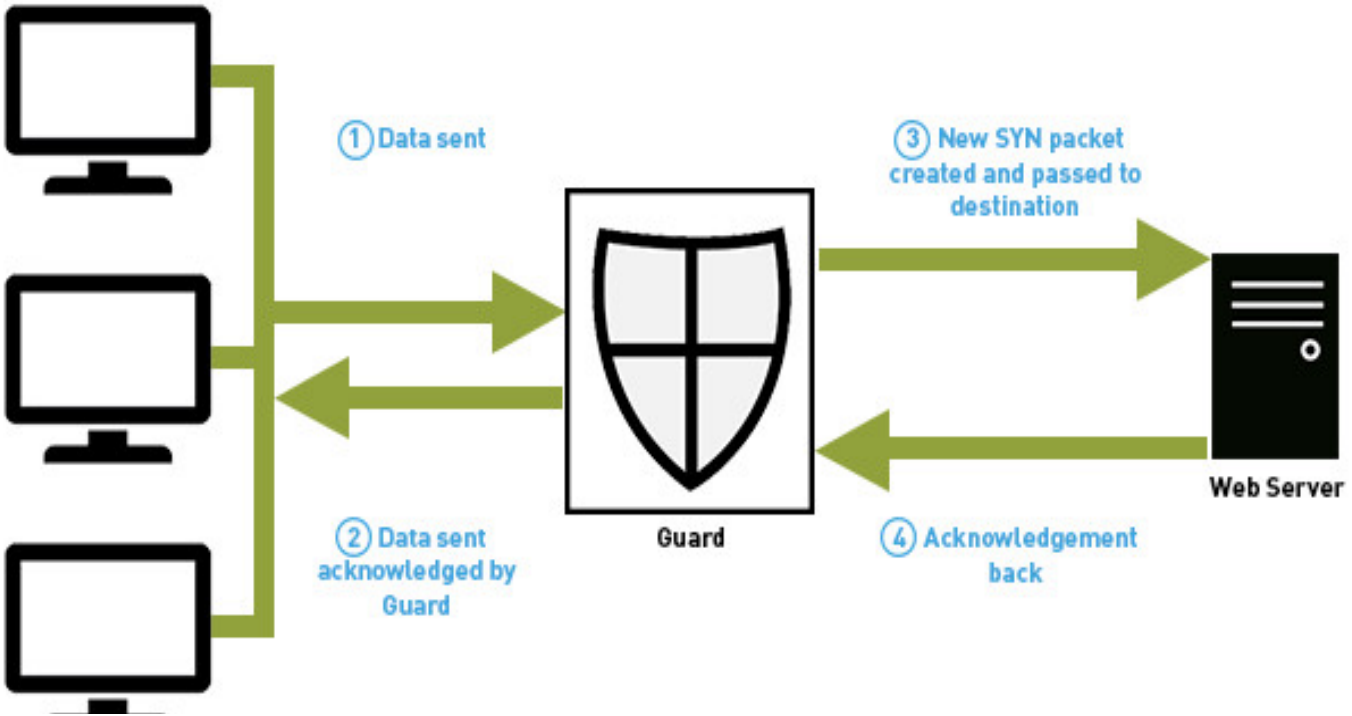
Connection Table

Type	Internal IP	Internal Port	External IP	External Port	Status
TCP	60.55.33.12	62600	123.80.5.34	80	OK

Guard

- It receives protocol data units , interprets them and passes them through the same or different protocol data units that achieve either the same result or a modified result
- It decides what services to perform on behalf of the user
- It is similar to the proxy services but more complex in nature

Guard


1 Data sent
3 New SYN packet created and passed to destination
Web Server
Guard
2 Data sent acknowledged by Guard
4 Acknowledgement back

Personal Firewall

- It is an application program that runs on a workstation to block unwanted network traffic
- It is configured to enforce some policy
- This policy is defined by the user which includes permitting downloads only from trusted sites, restricting data sharing only to secured websites
- It includes generation of access logs

Personal Firewall