An Introduction to Firewalls

22/4/2025

What is a digital firewall?

- A digital firewall is a system of **hardware and software components** designed to restrict access between two networks, most often between the Internet and a private network.
- The firewall is part of an overall security policy that creates a perimeter defense designed to protect the information resources of the organization.

A physical firewall

1. What is the firewall composed of?
2. What are the hardware and software components of this firewall?
3. What is the defence perimeter?

What can a firewall do?

- Implement security policies at a single point
- Monitor security-related events (audit, log)
- Provide strong authentication for access control purpose

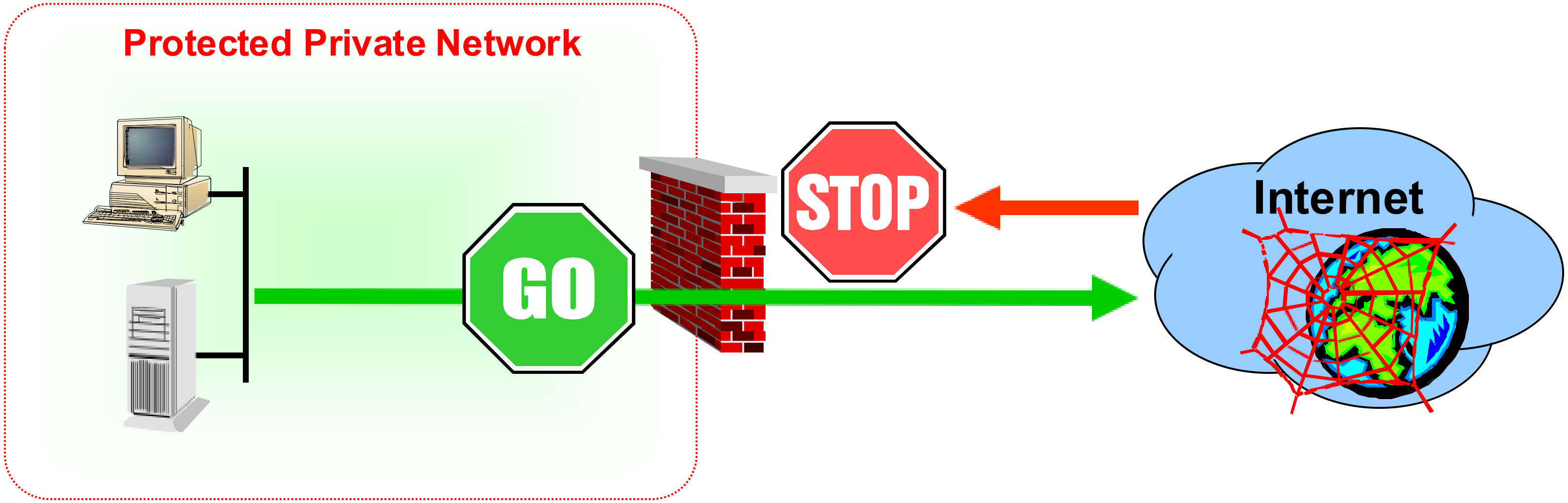
What cannot a firewall do?

- ❒ Protect against attacks that bypass the firewall
  - ❍ Dial-out from internal host to an ISP, as such a connection does not go through the firewall
- ❒ Protect against internal threats
  - ❍ disgruntled employee
  - ❍ Insider cooperates with an external attacker
- ❒ Protect against the transfer of virus-infected programs or files

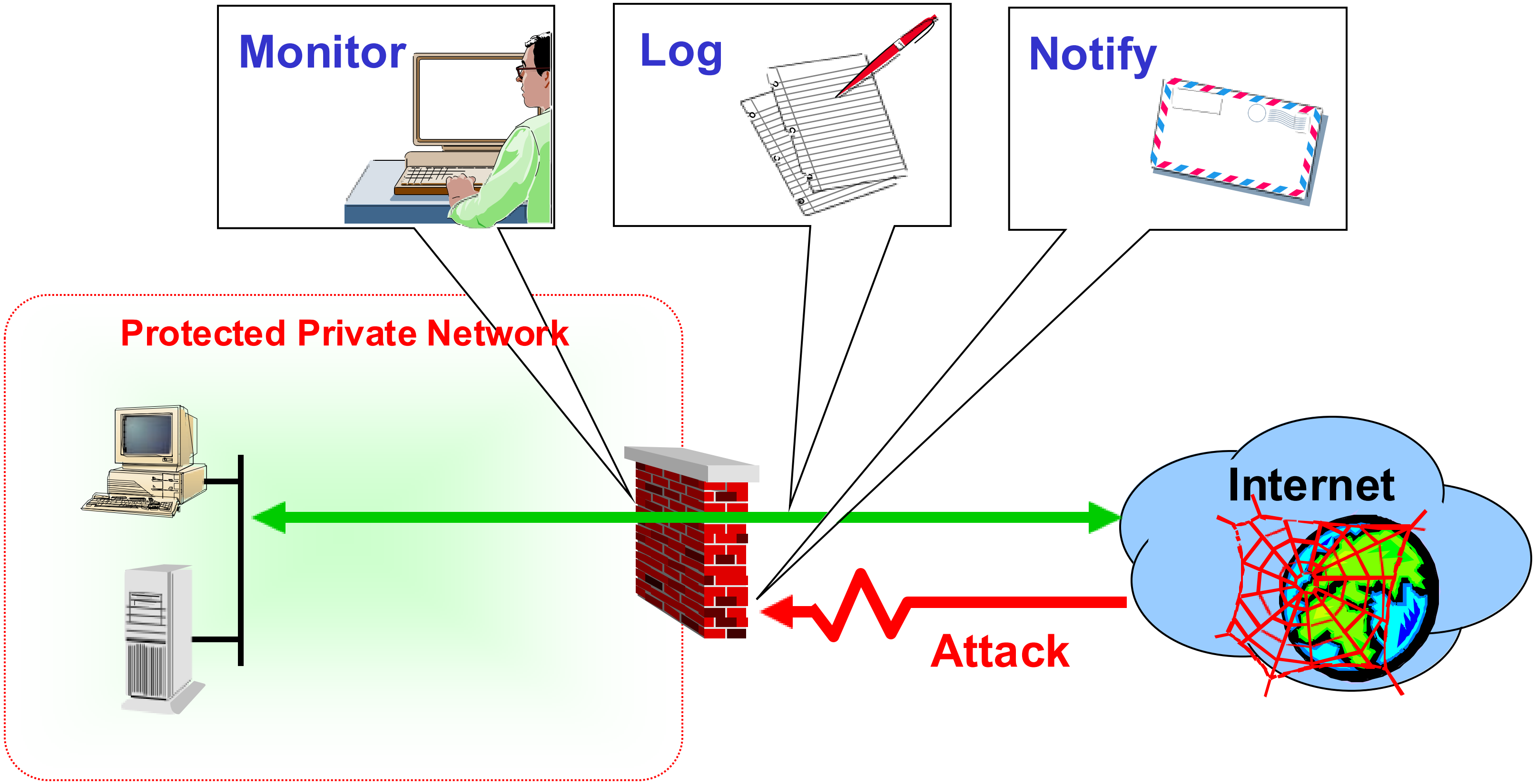
Firewall - typical layout

A firewall denies or permits access

based on policies and rules



Watching for attacks



Firewall technologies

They may be classified into four categories:

- Packet filtering firewalls
- Circuit level gateways
- Application gateways (or proxy servers)
- Session filtering firewalls

  a combination of the three above

- These technologies operate at different levels of detail, providing varying degrees of network access protection.

Packet Filtering and Session Filtering Firewalls

Filtering types

- Packet filtering
  - Packets are treated individually
  - No connection state information is memorized
- Session filtering (also called dynamic packet filtering)
  - Packets are grouped into connections
  - Packets in a connection are detected
  - Connection state information is memorized

Packet filtering

- With packet filtering decisions are made on per-packet basis
- No connection state information is saved
- It works at the network level of the OSI model
- It applies packet filters based on access rules defined by the following parameters:
  - Source address
  - Destination address
  - Protocol in the next header (TCP, UDP, etc)
  - Source port number
  - Destination port number

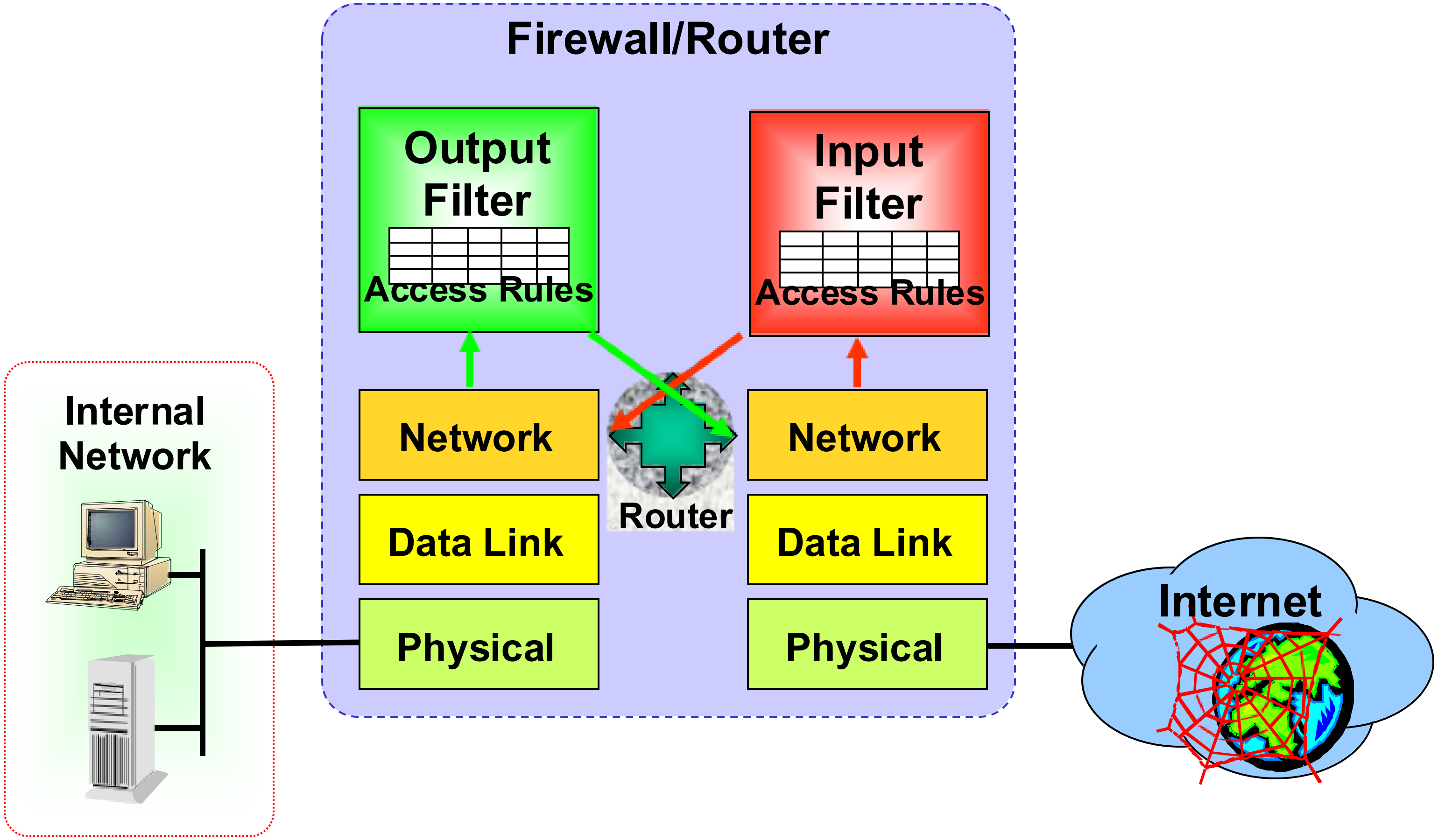
Packet filtering policy example

	My host		Other host		
action	name	port	name	port	comments
block	*	*	microsoft.com	*	Block everything from MS
allow	My-gateway	25	*	*	Allow incoming mail

Packet filtering policy example

Rule	Direction	Source Address	Destination Address	Protocol	# Source Port	# Destin. Port	Action
1	Out	*	10.56.199*	*	*	*	Drop
2	Out	10.56*	10.122*	TCP	*	23 (Telnet)	Pass
3	In	10.122*	10.56.199*	TCP	23 (Telnet)	*	Pass
4	In & Out	*	10.56.199*	TCP	*	25 (Mail)	Pass
5	In	*	*	TCP	*	513 (rlogin)	Drop
6	In	201.32.4.76	*	*	*	*	Drop
7	Out	*	*	TCP	*	20 (FTP)	Pass
8	In	*	10.56.199*	TCP	*	20 (FTP)	Drop

Packet filtering firewalls



Packet filtering firewalls

- Strengths:
  - Simple, low cost, fast, transparent to user
- Weaknesses:
  - They cannot prevent attacks that employ application-specific vulnerabilities or functions
    - because they do not examine upper-layer data.
  - Most packet filter firewalls do not support advanced authentication schemes
    - due to the lack of upper-layer functionality
  - Such a firewall may not be able to capture all access control policies of an organization
    - due to the small number of variables used for decision

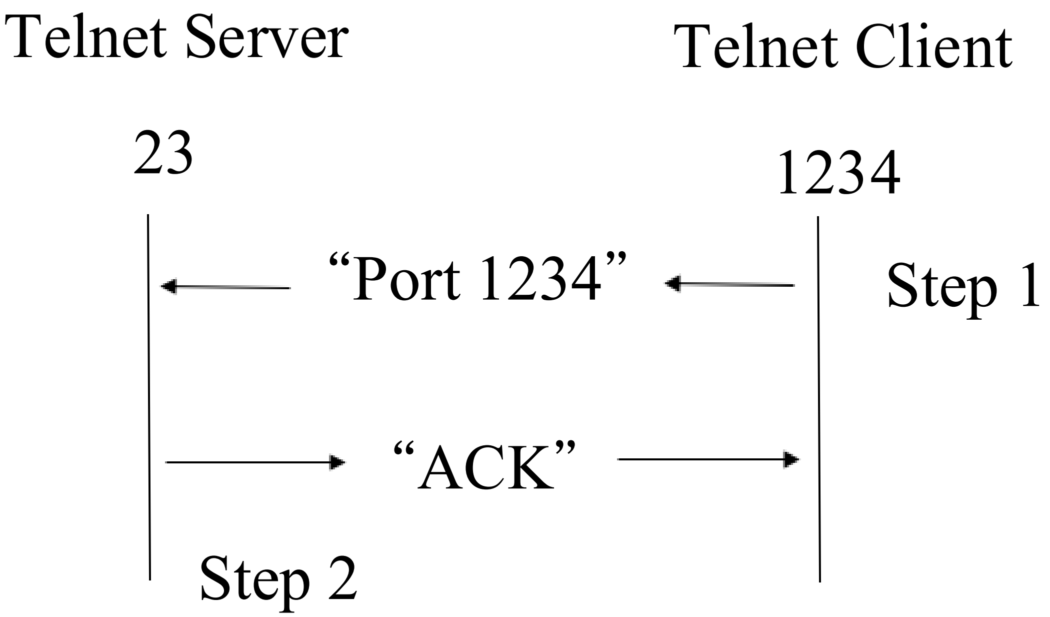
Session filtering

- Traditional packet filtering does not examine higher layer context.
- Session filtering (i.e., dynamic packet filtering) examines data at all levels.
- Session filtering examines each IP packet in context.
  - It keeps track of client-server connections.
  - It checks if a packet belongs to one existing connection.
- Hence, session filtering is more able to detect bogus packets out of context.

Session filtering

- Packet decision is made in the context of a connection.
  - A connection state table is maintained.
- If a packet is a new connection, it checks the security policy.
  - If the policy is yes, a new connection is saved in the connection state table
- If a packet belongs to an existing connection, it matches it up in the connection state table and updates the connection state table.

Example of connection establishment



Telnet Server

Telnet Client

23

1234

"Port 1234"

Step 1

"ACK"

Step 2

(1) The Client opens channel to the Server, sends its port number. The ACK bit is not set while establishing the connection but will be set on the remaining packets.

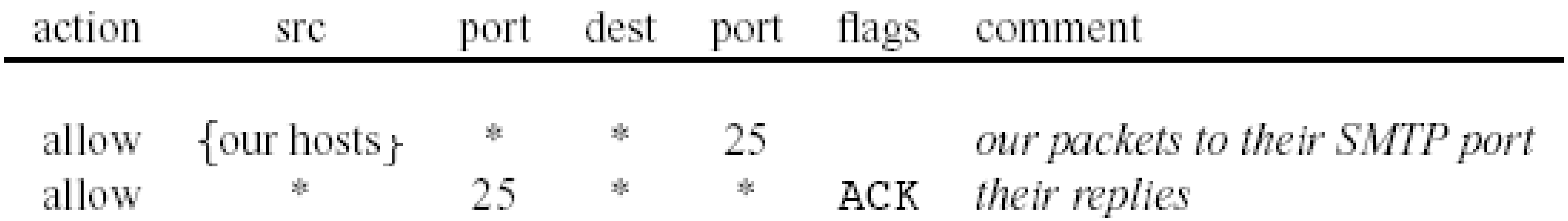
(2) Server acknowledges.

Example of connection state table

Source address	Source port	Destination Address	Destination port	Connection State
192.168.1.100	1030	210.9.88.29	80	established
192.168.1.102	1031	216.32.42.123	25	established

- In general, when an application uses TCP to create a session with a remote host, it creates a TCP connection in which the TCP port number for the remote (server) application is a number less than 1024 and the TCP port number for the local (client) application is a number between 1024 and 16383.
- The numbers < 1024 are the well-known port numbers and are assigned permanently to specific applications.

Using ACK in session filtering

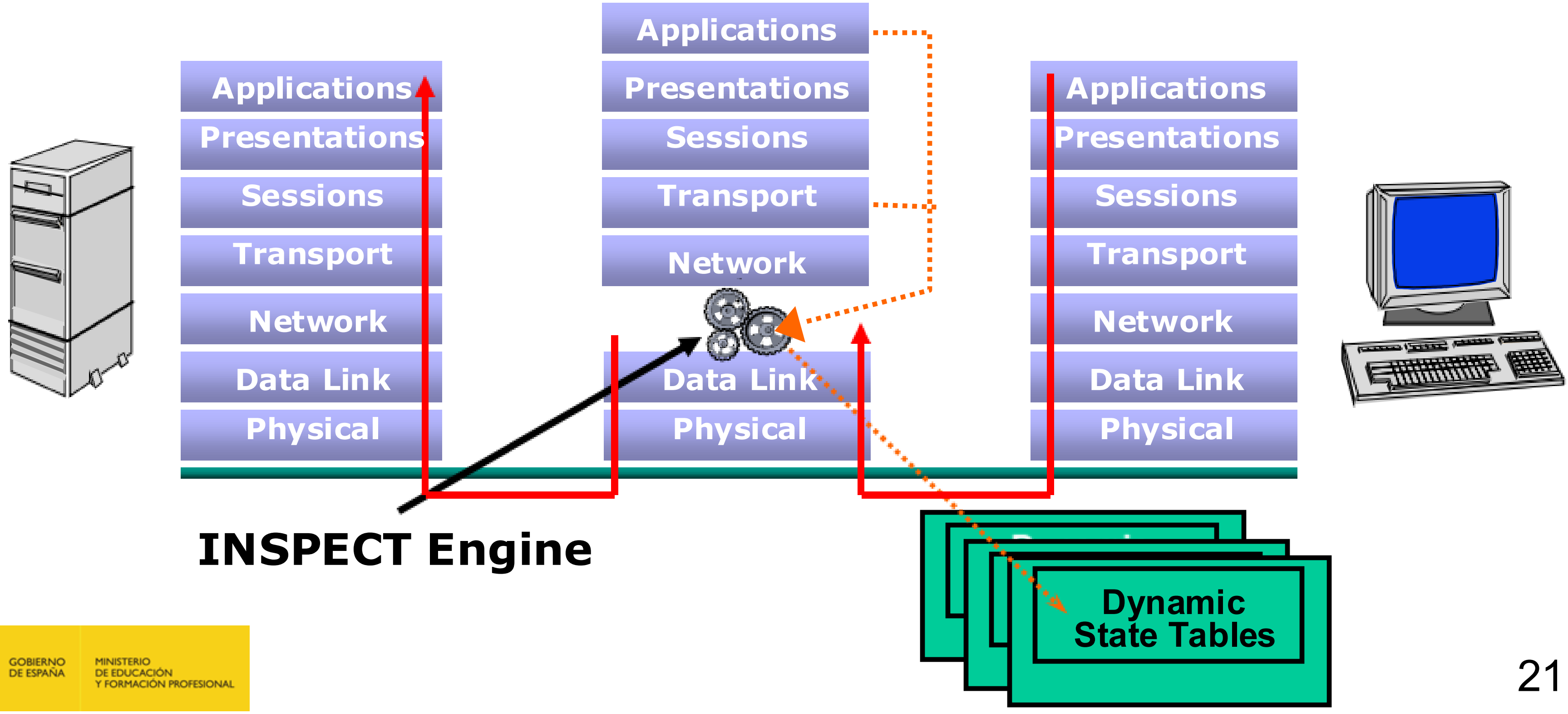


action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	25		*our packets to their SMTP port*
allow	*	25	*	*	ACK	*their replies*

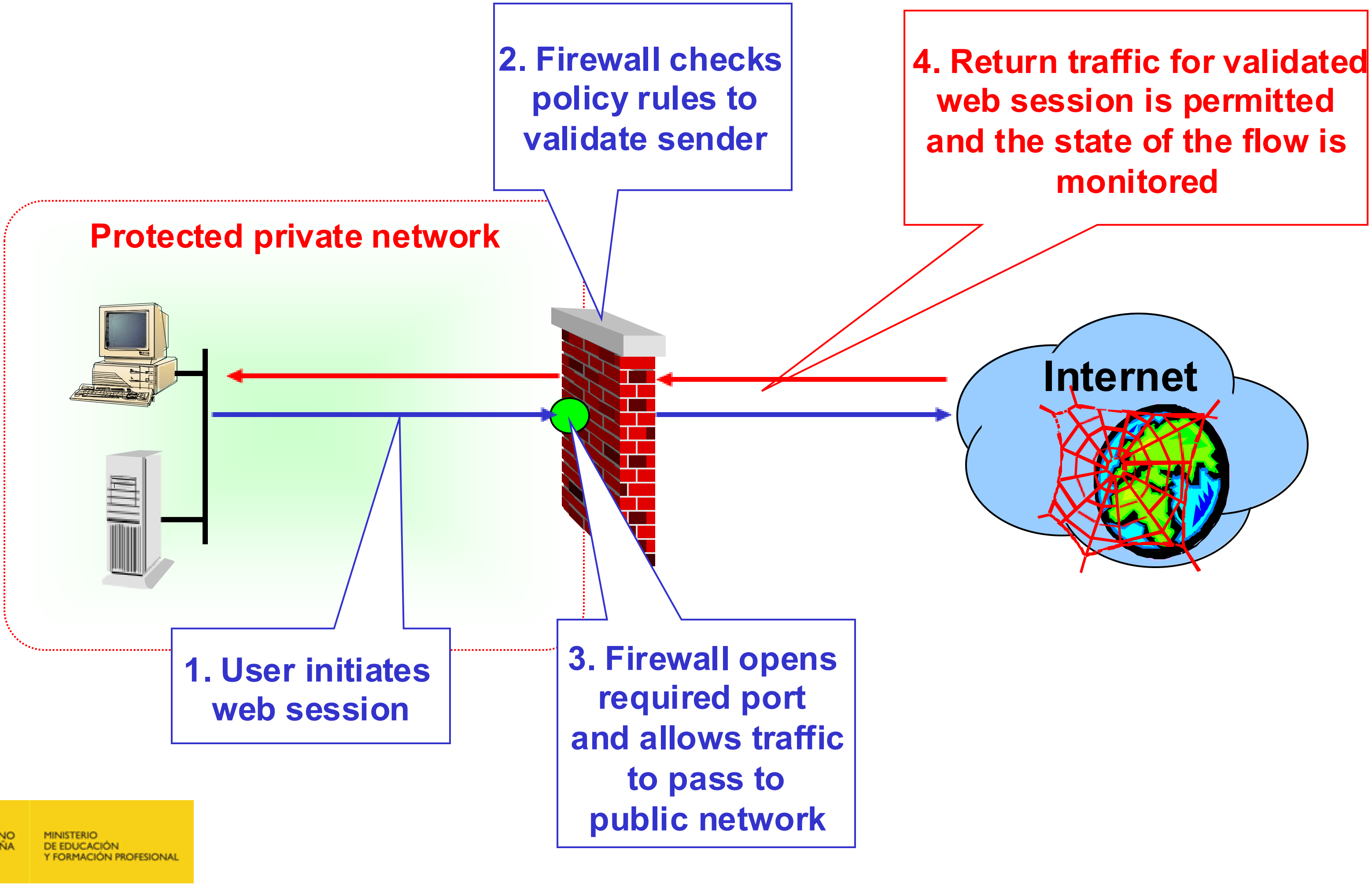
- The ACK signifies that the packet is part of an ongoing conversation
- Packets without the ACK are connection establishment messages

Session filtering firewalls

- Packets are inspected between data link layer and the application layer
- State tables are created to maintain connection context



Session filtering implementation



1. User initiates web session

2. Firewall checks policy rules to validate sender

3. Firewall opens required port and allows traffic to pass to public network

4. Return traffic for validated web session is permitted and the state of the flow is monitored

Session filtering strengths

- It monitors the state of all data flows
- It is transparent to users
- It has low CPU overheads
  - For the second and later packets belonging to the same connection, no table look-up of the policy database is done.

Designing a physical firewall

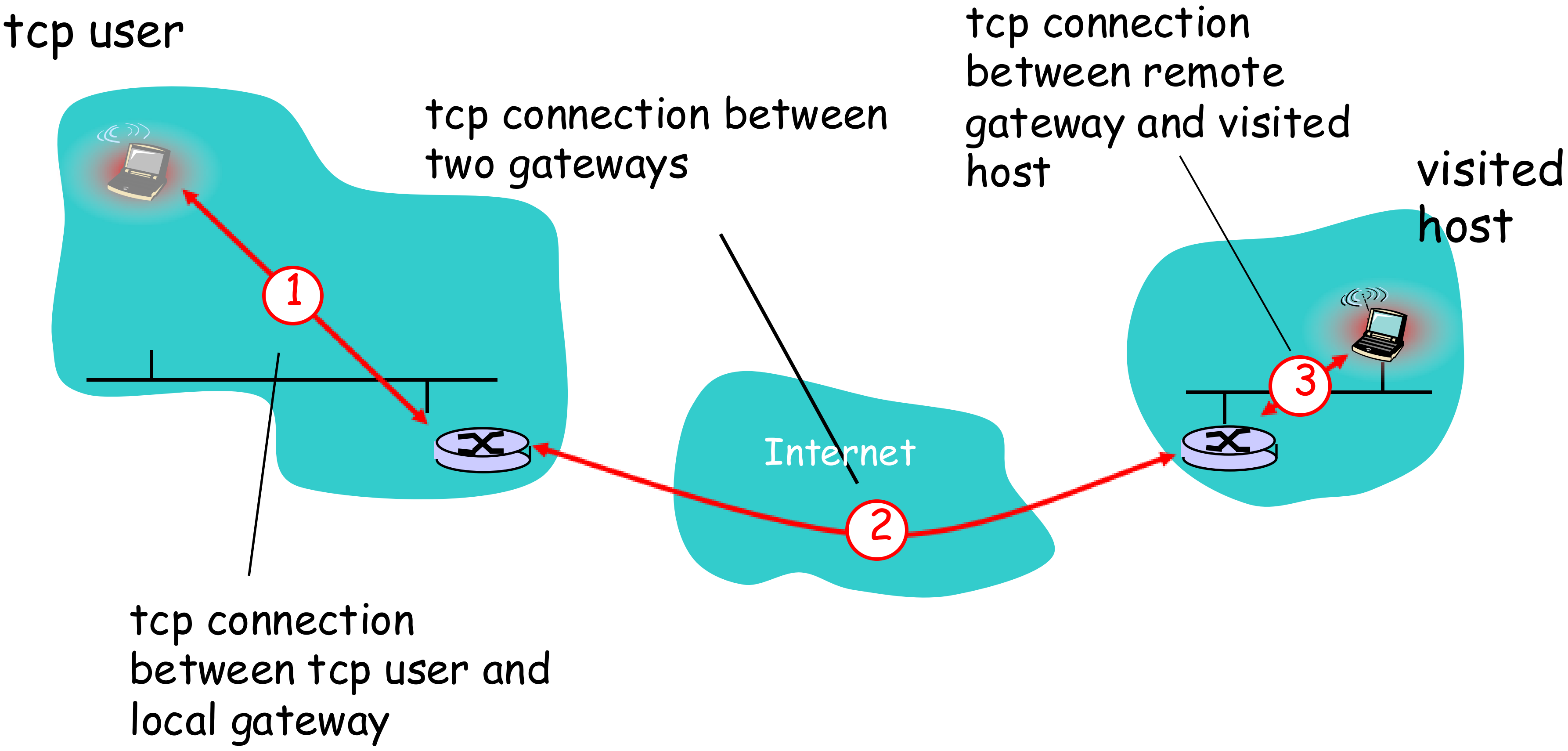
1. How do you design it into a packet filtering firewall?
2. How do you design it into a session filtering firewall?

Circuit Level Gateways

Circuit level gateways

- Circuit level gateways work at the **session layer** of the OSI model, or the **TCP layer** of TCP/IP.
- They monitor TCP handshaking between packets to determine whether a requested session is legitimate.
- They do not permit an end-to-end TCP connection.
  - Rather, the gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outside host.
  - Once the two connections are established, the gateway typically relays TCP segments from one to the other without examining the contents.

Circuit level gateway example



tcp user

tcp connection between two gateways

tcp connection between remote gateway and visited host

visited host

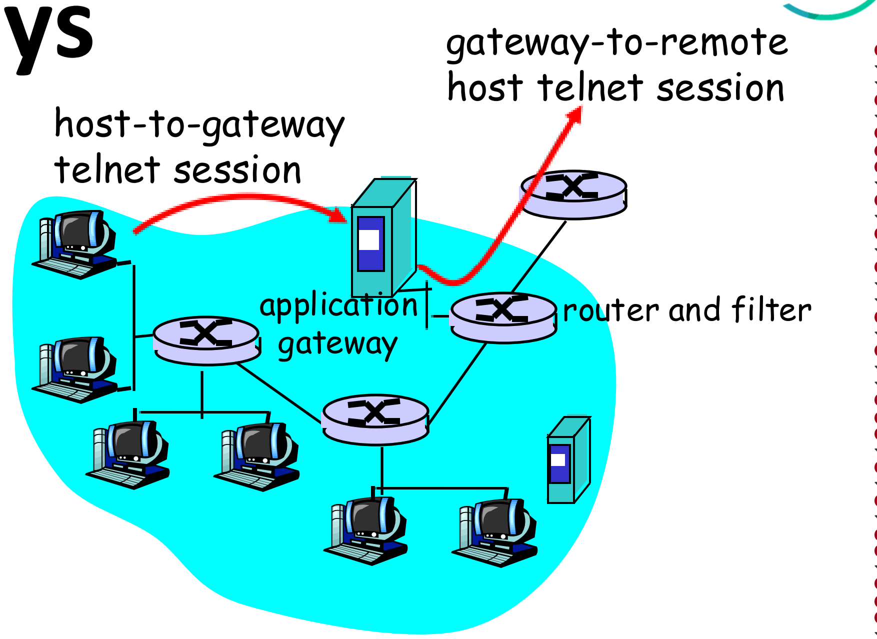
tcp connection between tcp user and local gateway

Application Gateways (Proxy Servers)

Application gateways

- They are similar as circuit-level gateways except that they are application specific (i.e., tailored to a specific application program).
- Every connection between two networks is made via an application program called a "**proxy”**.
- Connection state is maintained and updated.
- Proxies are application or protocol specific.
- Only protocols that have specific proxies configured are allowed through the firewall; all other traffic is rejected.
  - E.g., a gateway that is configured to be a web proxy will not allow any ftp, gopher, telnet or other traffic through

Application gateways



gateway-to-remote host telnet session

host-to-gateway telnet session

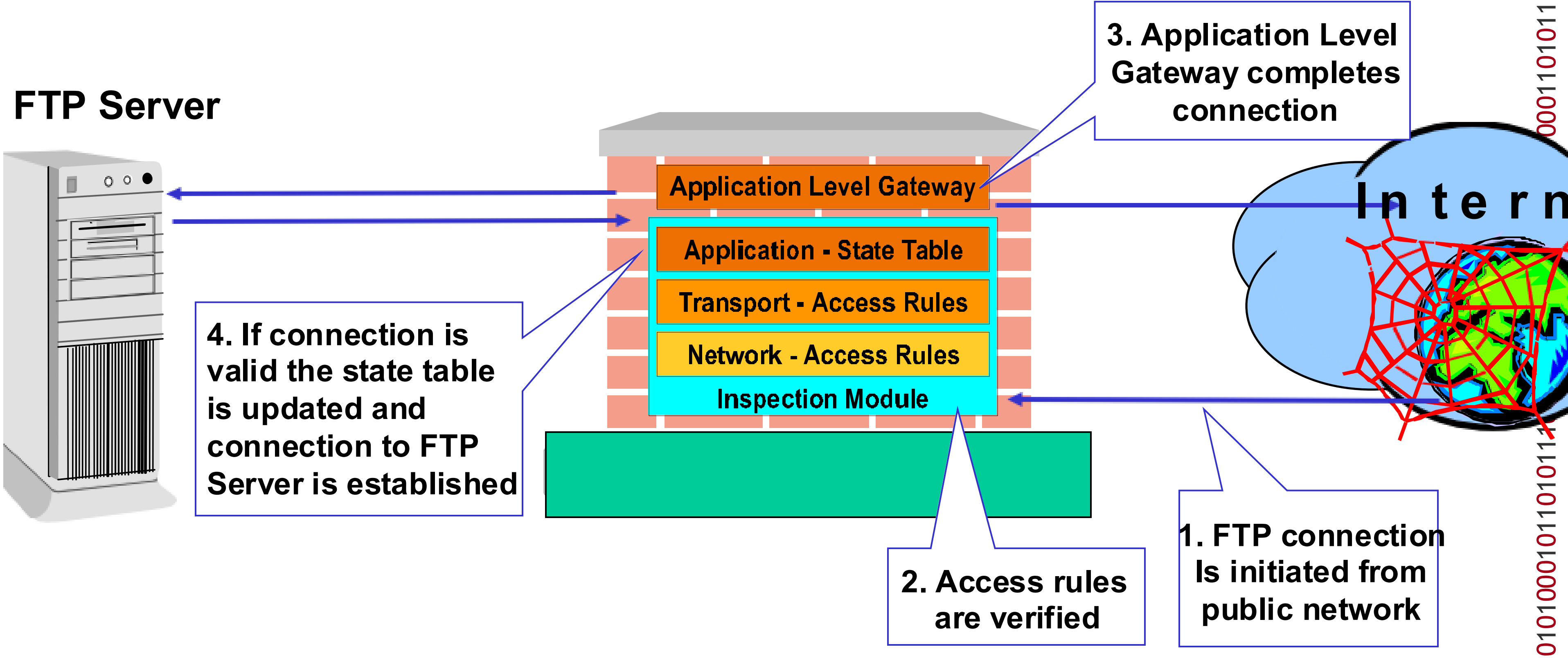
application gateway

router and filter

- It filters packets on application data as well as on IP/TCP/UDP fields.
- Example: It allows selected internal users to telnet outside.

1. Require all telnet users to telnet through gateway.
2. For authorized users, gateway sets up telnet connection to destination host. Gateway relays data between 2 connections
3. Routers and filters block all telnet connections not originating from gateway.

Application gateway example



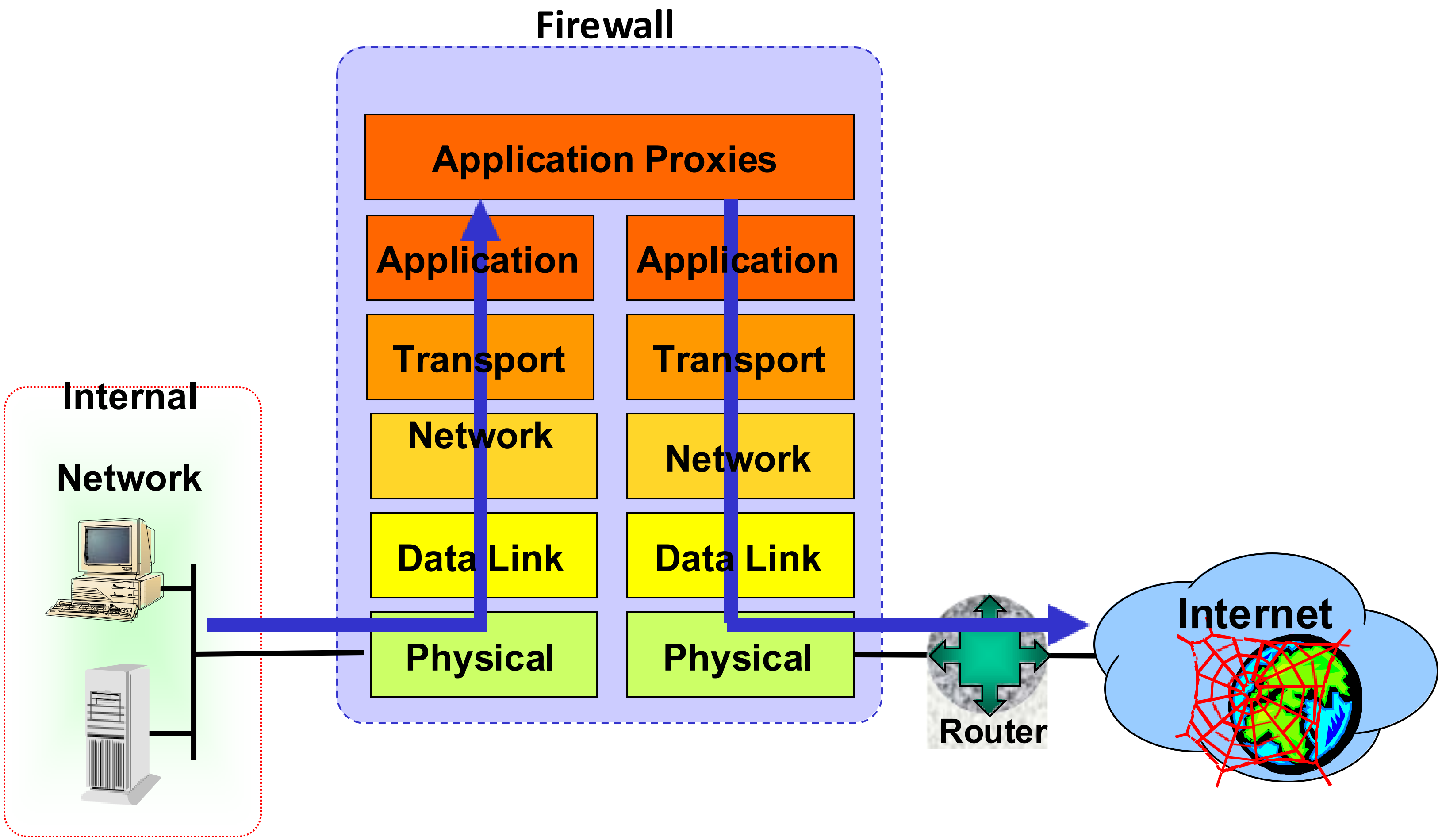
1. FTP connection Is initiated from public network

2. Access rules are verified

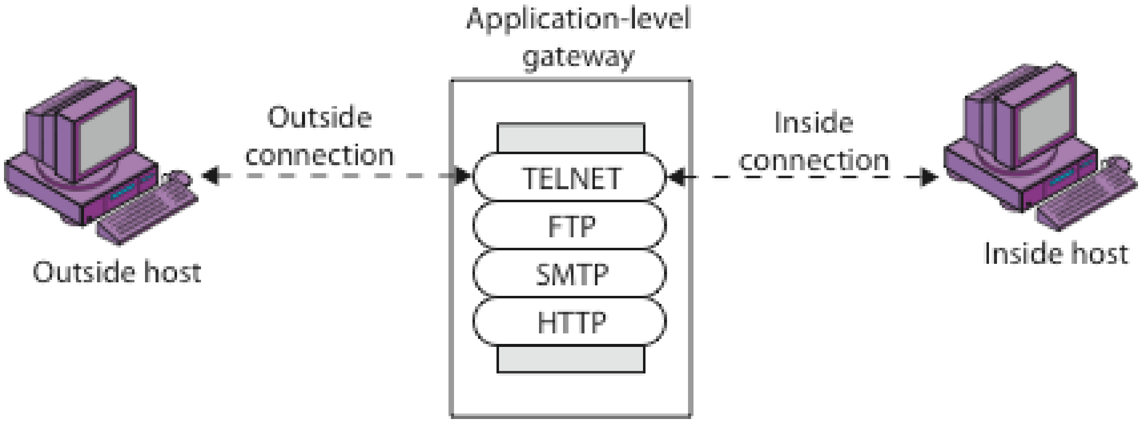
3. Application Level Gateway completes connection

4. If connection is valid the state table is updated and connection to FTP Server is established

Application gateways



Application gateways



(b) Application-level gateway

Application gateway strengths

- More secure than packet filtering firewalls
  - Rather than trying to deal with the numerous possible combinations that are to be allowed and forbidden at the TCP and IP level, the application gateway need only scrutinize a few allowable applications.
- It is easy to log and audit all incoming traffic at the application level.

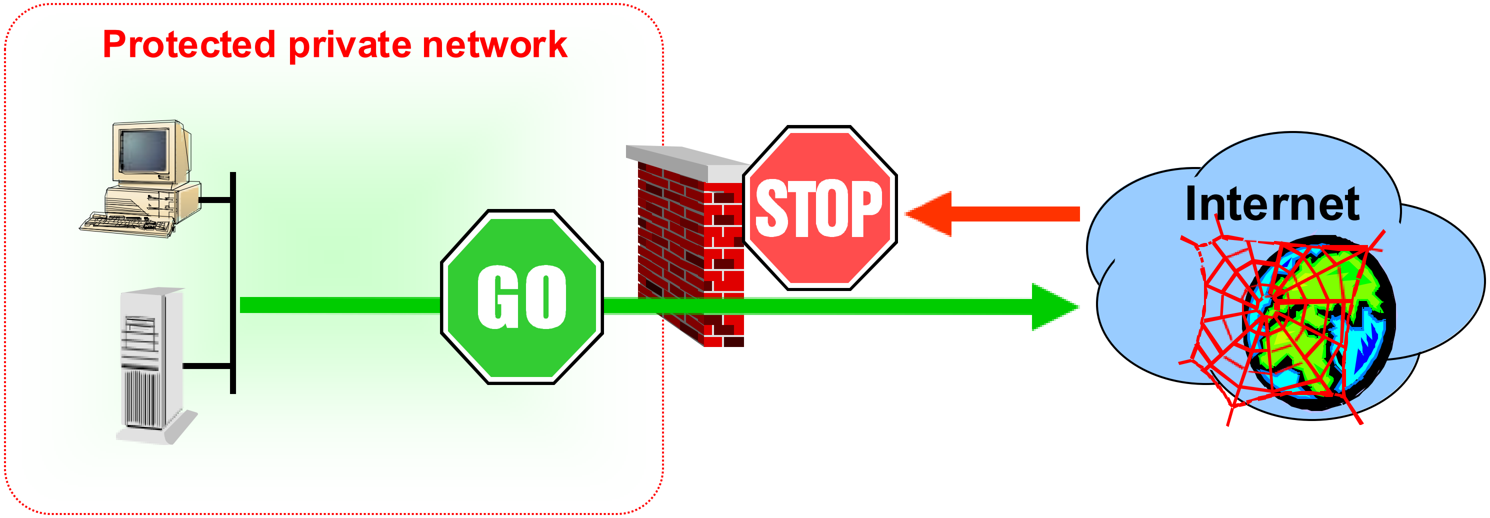
Application gateway weaknesses

- They are very CPU intensive.
  - There are two spliced connections between the end users, with the gateway at the splice point, and the gateway must examine and forward all traffic in both directions.
- They require high performance host computers.
- They are expensive.

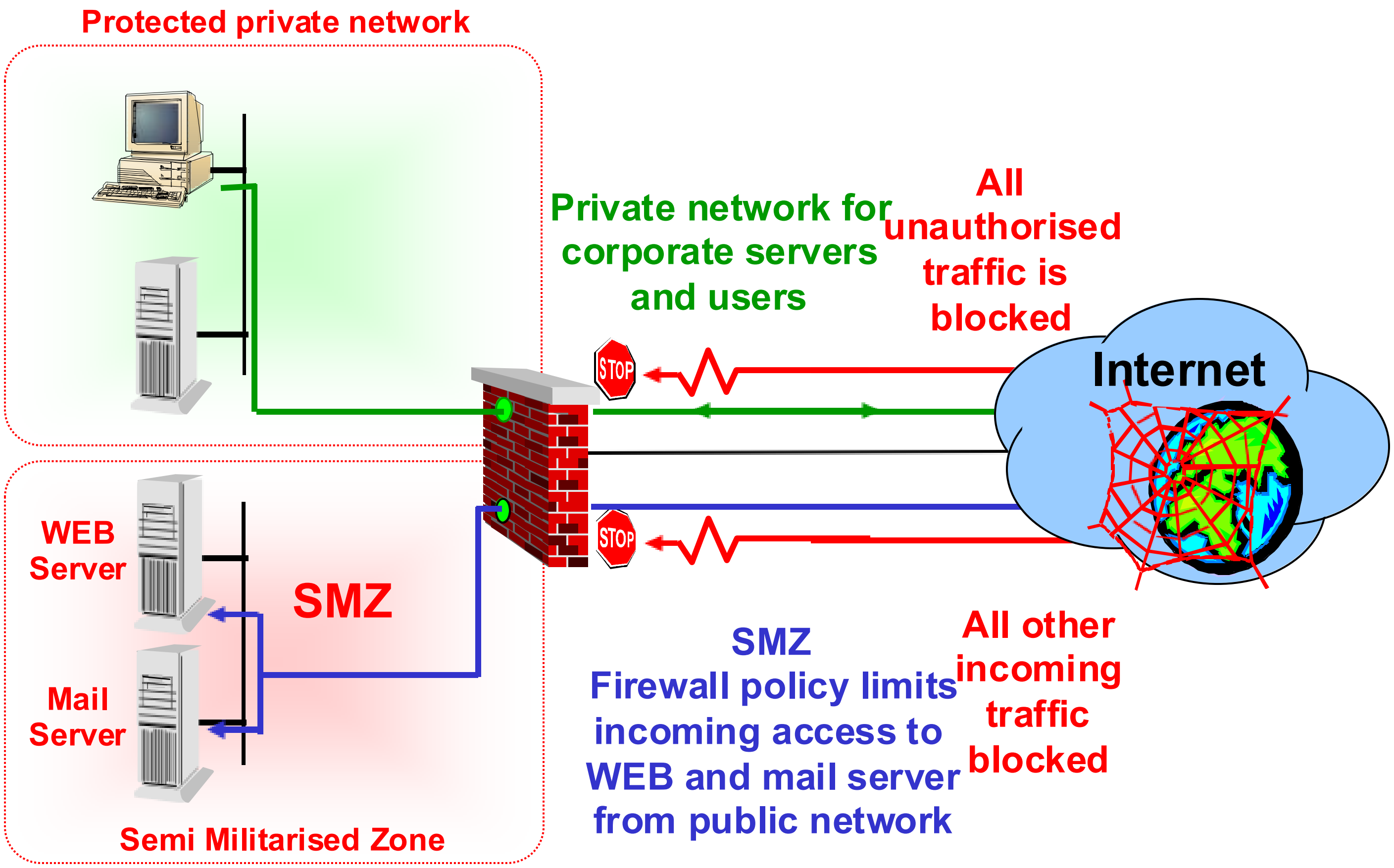
Network Configuration Examples

Protected private network

- Allow all access from private network to the Internet
- Restrict all access from the Internet to the private network



Semi-militarised zone


Protected private network
Private network for corporate servers and users
All unauthorised traffic is blocked
STOP
Internet
STOP
WEB Server
SMZ
Mail Server
Semi Militarised Zone
SMZ Firewall policy limits incoming access to WEB and mail server from public network
All other incoming traffic blocked

Concluding remarks

- All that a firewall can do is to control network activities between OSI levels 2 and 7.
- They cannot keep out data carried inside applications, such as viruses within email messages:
  - there are just too many ways of encoding data to be able to filter out this kind of threat.
- Although firewalls provide a high level of security in today's private networks to the outside world, we still need the assistance of other related security components in order to guarantee proper network security.