Lecture 23: Firewalls

- Introduce several types of firewalls
- Discuss their advantages and disadvantages
- Compare their performances
- Demonstrate their applications

What is a Digital Firewall?

- A digital firewall is a system of **hardware and software components** designed to restrict access between or among networks, most often between the Internet and a private Internet.
- 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 a Firewall can do

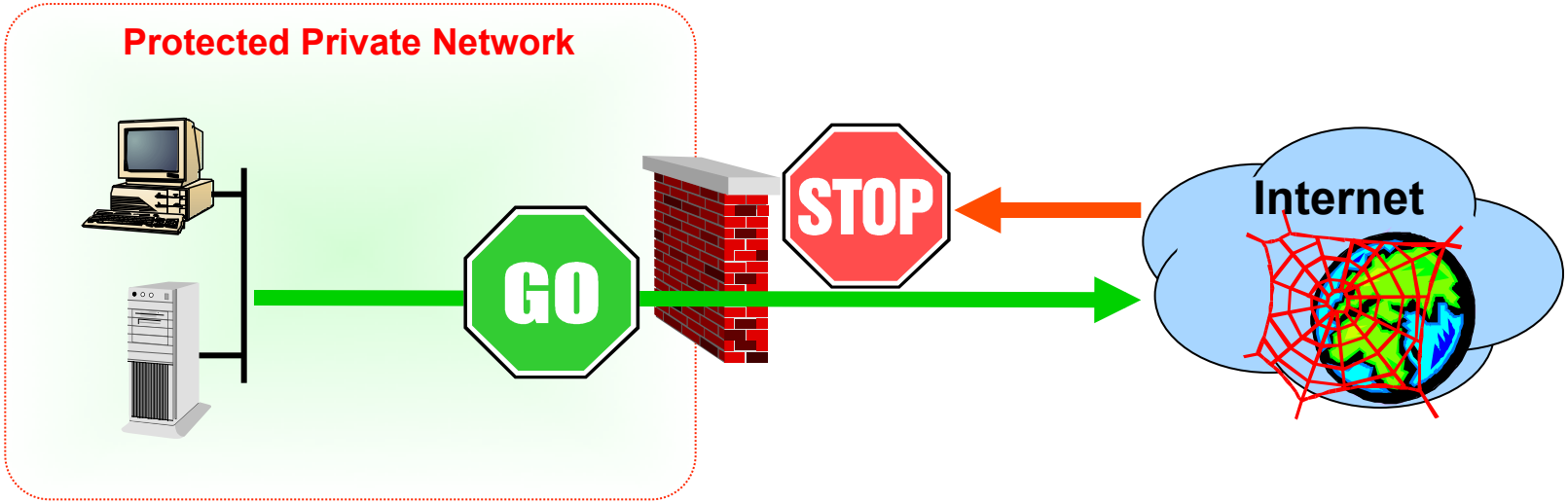
- Implement security policies at a single point
- Monitor security-related events (audit, log)
- Provide strong authentication for access control purpose

What a Firewall cannot do

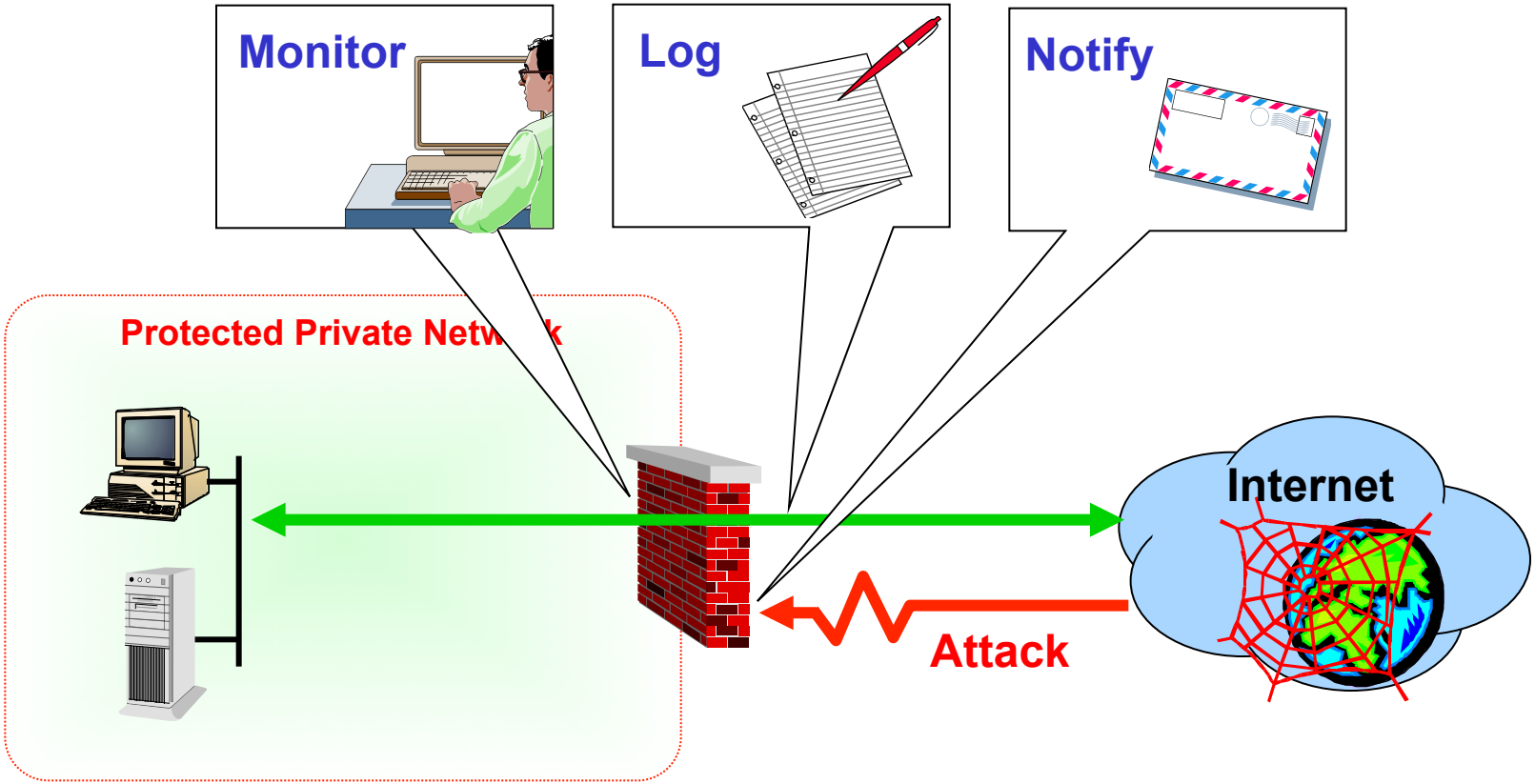
- Protect against attacks that bypass the firewall
  - Dial-out from internal host to an ISP
- Protect against internal threats
  - disgruntled employee
  - Insider cooperates with an external attacker
- Protect against the transfer of virus-infected programs or files

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)
- Dynamic packet filtering firewalls
  - a combination of the three above

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

Filtering Types

- Packet filtering
  - Packets are treated individually
  - No state information is memorized
- Session filtering or dynamic packet filtering
  - Packets are grouped into connections
  - Packets in a connection are detected
  - State information is memorized

Packet Filtering

- Decisions made on per-packet basis
- No state information saved
- Works at the network level of the OSI model
- Applies packet filters based on access rules defined by the following parameters:
  - Source address
  - Destination address
  - Application or protocol/next header (TCP, UDP, etc)
  - Source port number
  - Destination port number

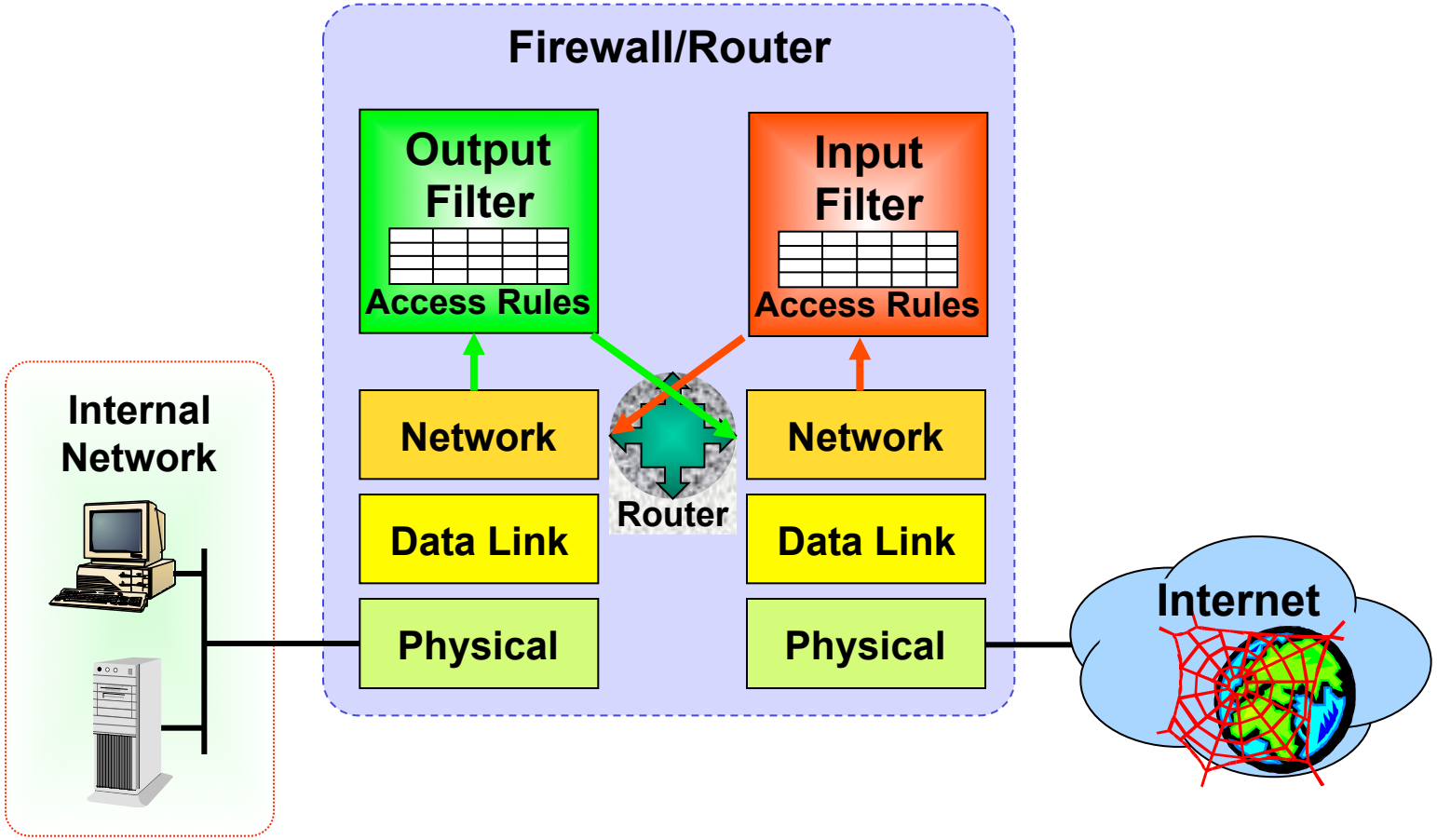
Packet Filtering Policy Example

	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

- Advantages:
  - Simple, low cost, fast, transparent to user
- Disadvantages:
  - 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
  - It is easy to accidentally configure a packet filtering firewall to allow traffic types, sources, and destinations that should be denied based on an organization's policy
    - due to the small number of variables used for decision

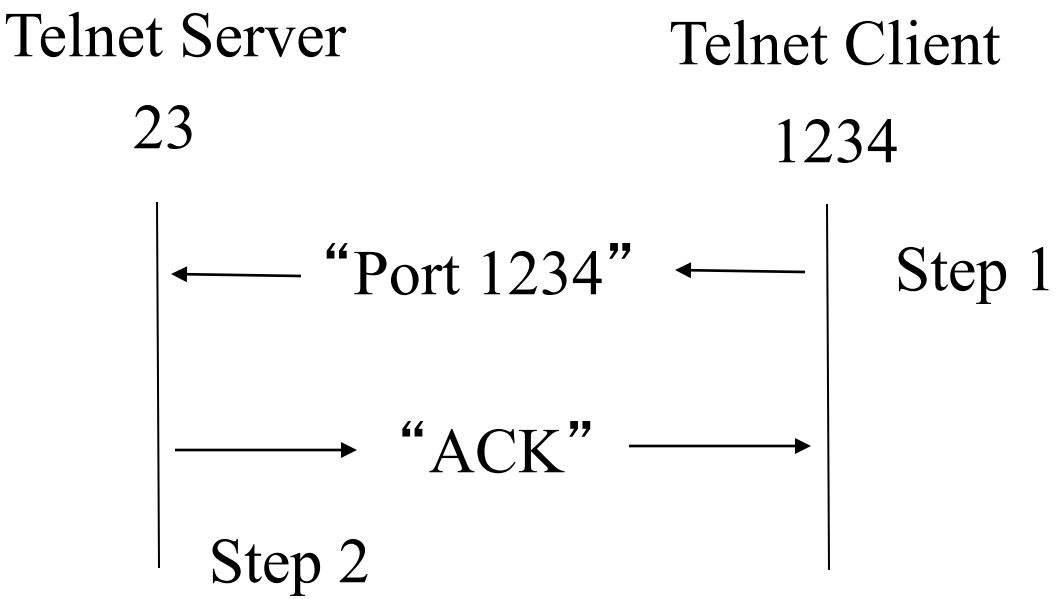
Session Filtering

- Traditional packet filters do not examine higher layer context
  - ie matching return packets with outgoing flow
- Dynamic packet filtering examines data at all levels
- They examine each IP packet in context
  - Keep track of client-server connection
  - Check each packet validly belongs to one
- Hence are more able to detect bogus packets out of context

Session Filtering

- Packet decision made in the context of a connection
- If packet is a new connection, check again policy
- If packet is part of an existing connection, match it up in the state table and update table.
  - A connection table is maintained

Example of Session Establishment



(1) The Client opens channel to the Server, tells 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 that uses TCP creates 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 less than 1024 are the well-known port numbers and are assigned permanently to particular applic.

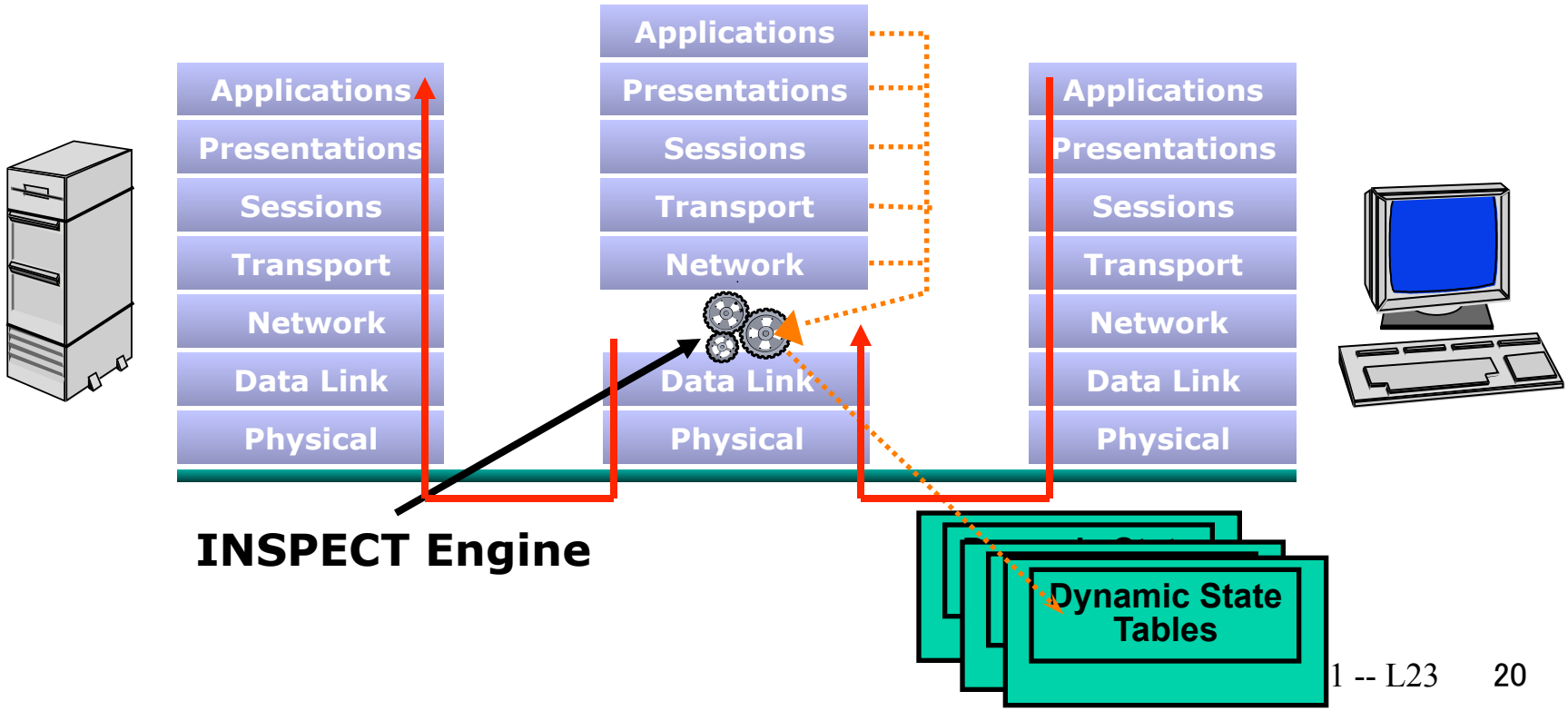
Using ACK in Session Filtering

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

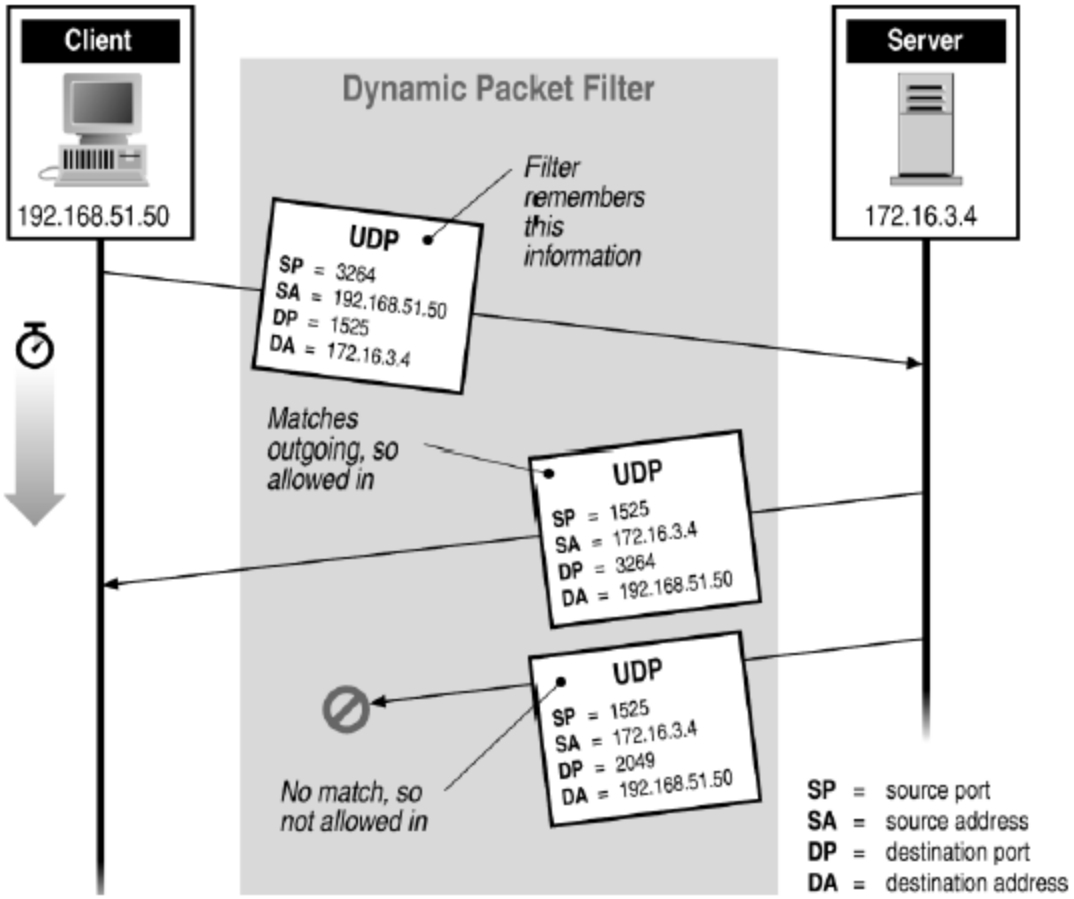
- The ACK signifies that the packet is part of an ongoing conversation
- Packets without the ACK are connection establishment messages

Dynamic Packet Filtering Firewalls

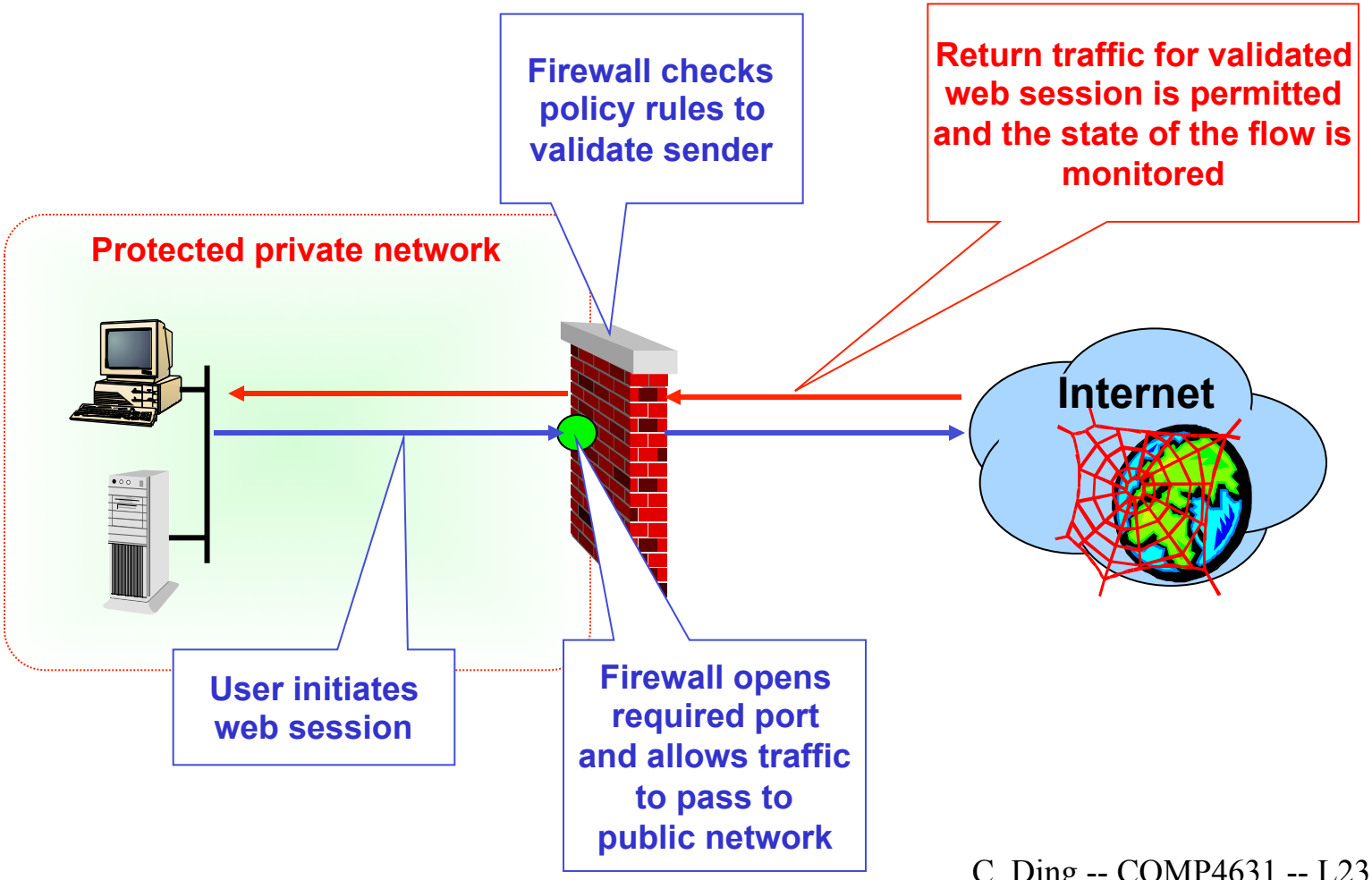
- Packets inspected between data link layer and network layer
- State tables are created to maintain connection context



Dynamic Packet Filtering Firewalls Example



Dynamic Packet Filtering Implementation



Dynamic Packet Filtering Strengths

- Monitors the state of all data flows
- Transparent to users
- Low CPU overheads
  - For the second and later packets belong to the same connection, no table look-up of the policy database is done.

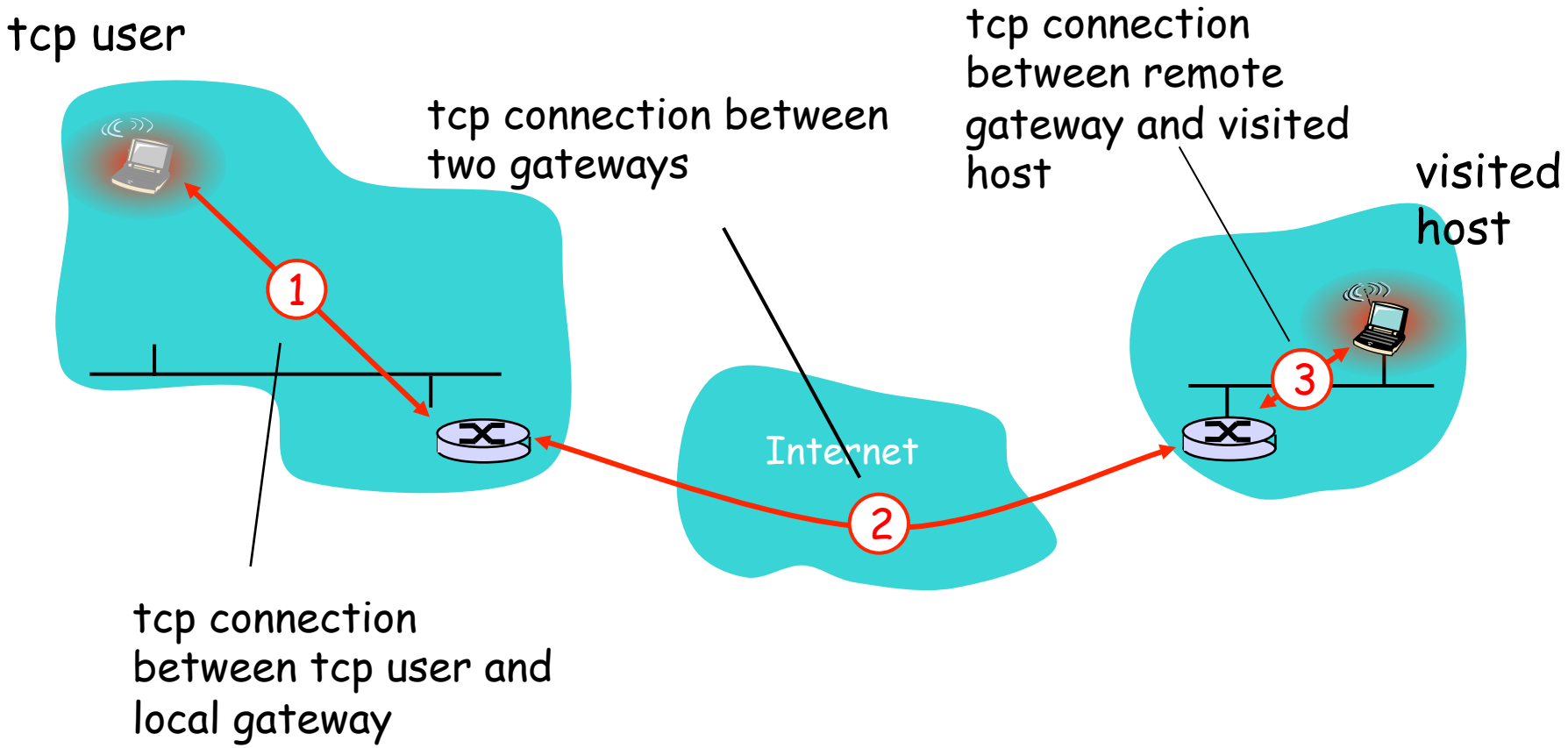
Designing the Physical Firewall

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

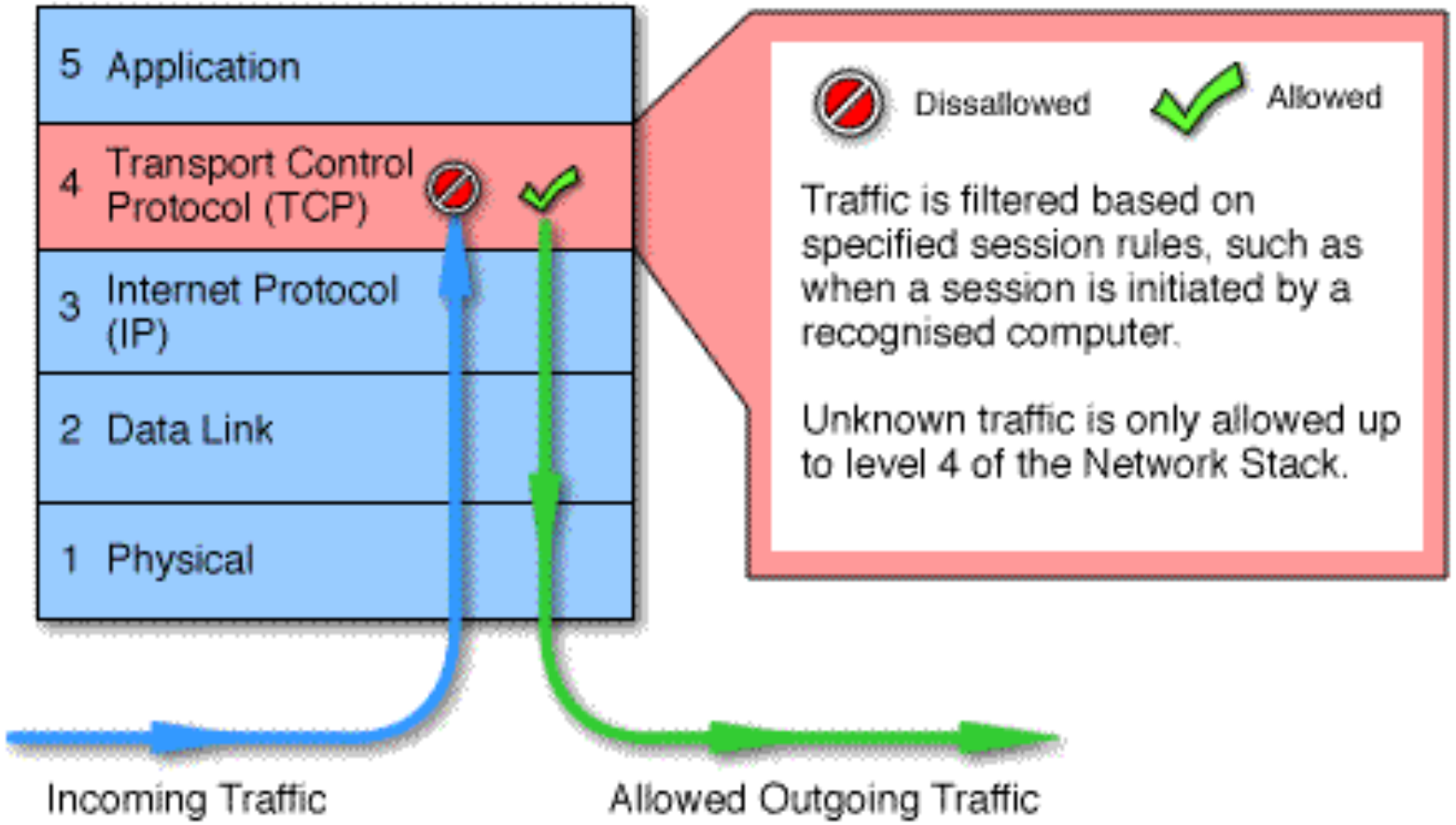
Circuit Level Gateways

- Circuit level gateways work at the **session layer** of the OSI model, or the **TCP layer** of TCP/IP
- Monitor TCP handshaking between packets to determine whether a requested session is legitimate.
- 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



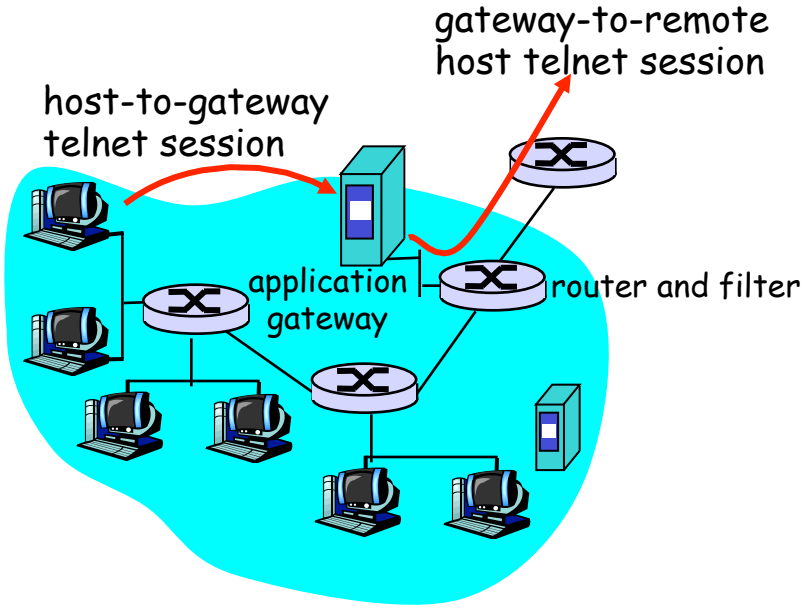
Circuit Level Gateways



Application Gateways

- Similar to 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

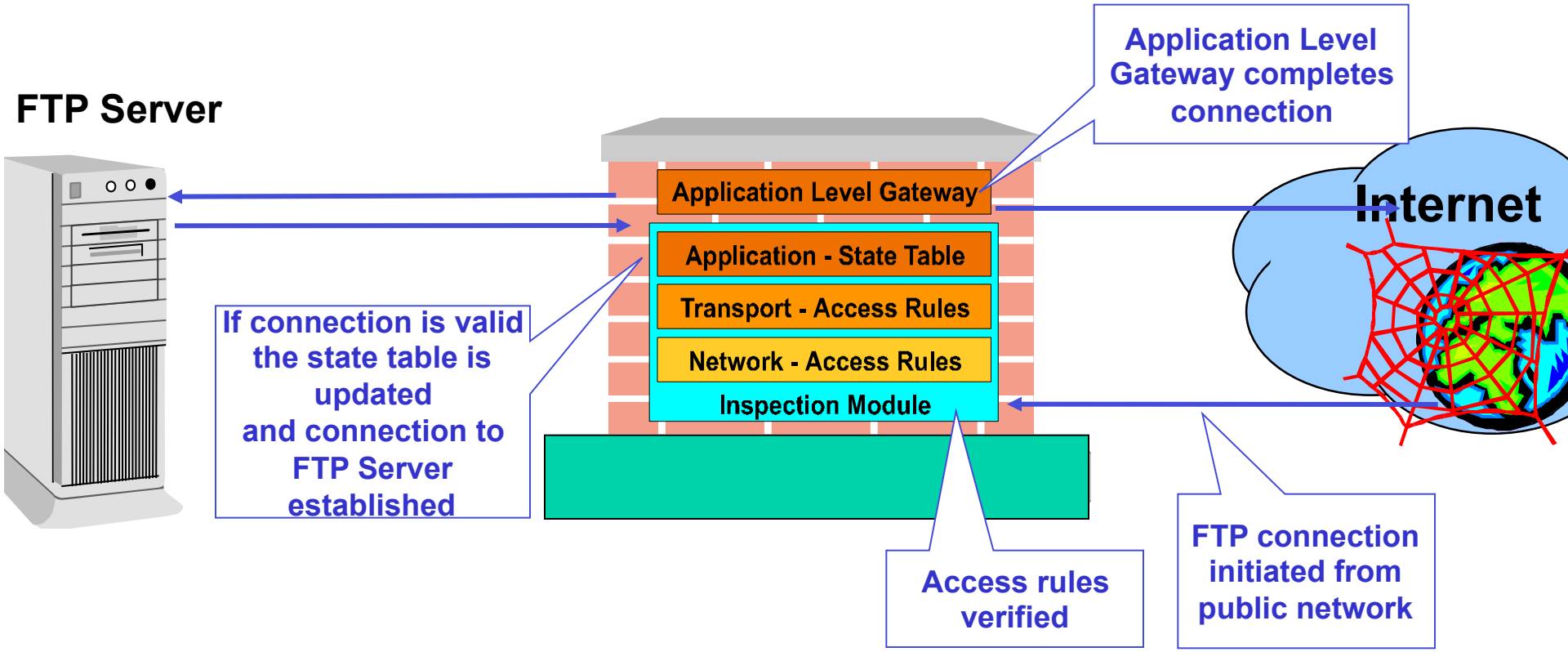
Application Gateways



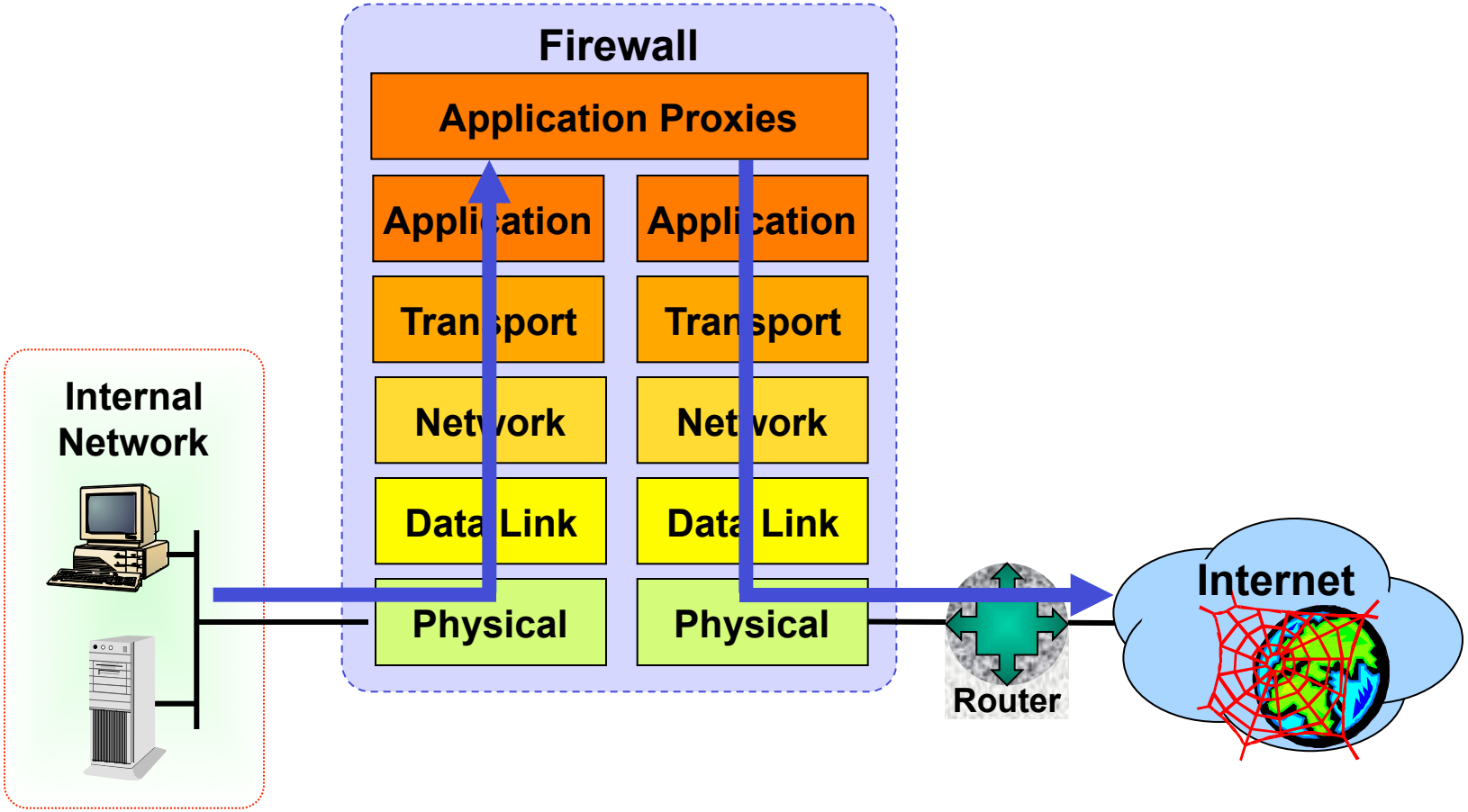
- It filters packets on application data as well as on IP/TCP/UDP fields.
- Example: It allows selected internal users to telnet outside.

1. Require all telnet users to telnet through gateway.
2. For authorized users, gateway sets up telnet connection to dest host. Gateway relays data between 2 connections
3. Router filter blocks all telnet connections not originating from gateway.

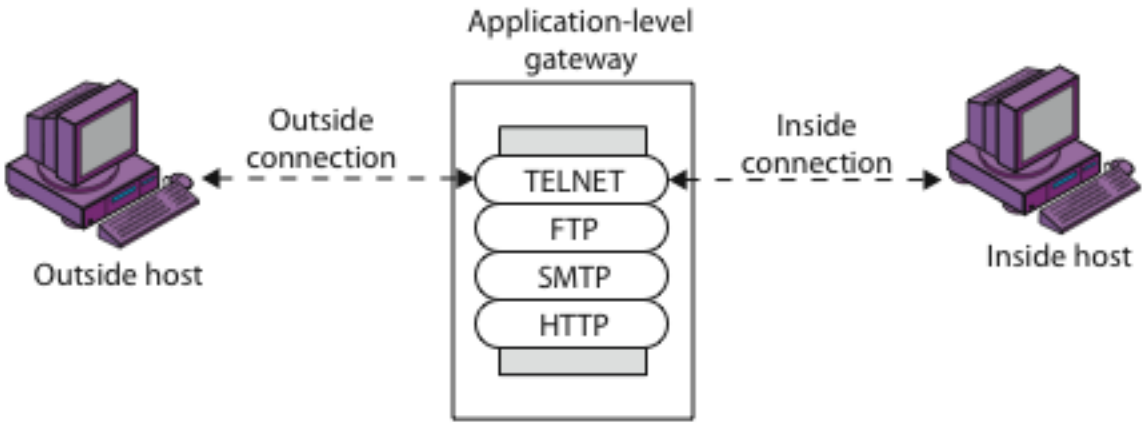
Application Gateway Example



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.

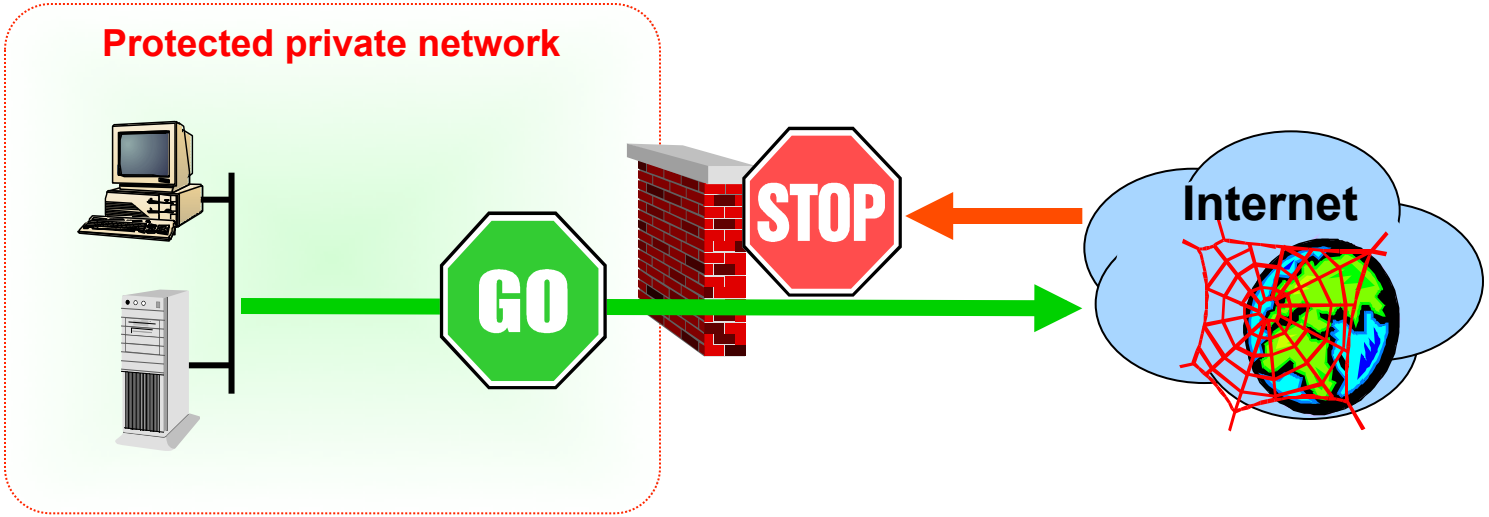
Application Gateway Weaknesses

- 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.
- Requires high performance host computer
- Expensive

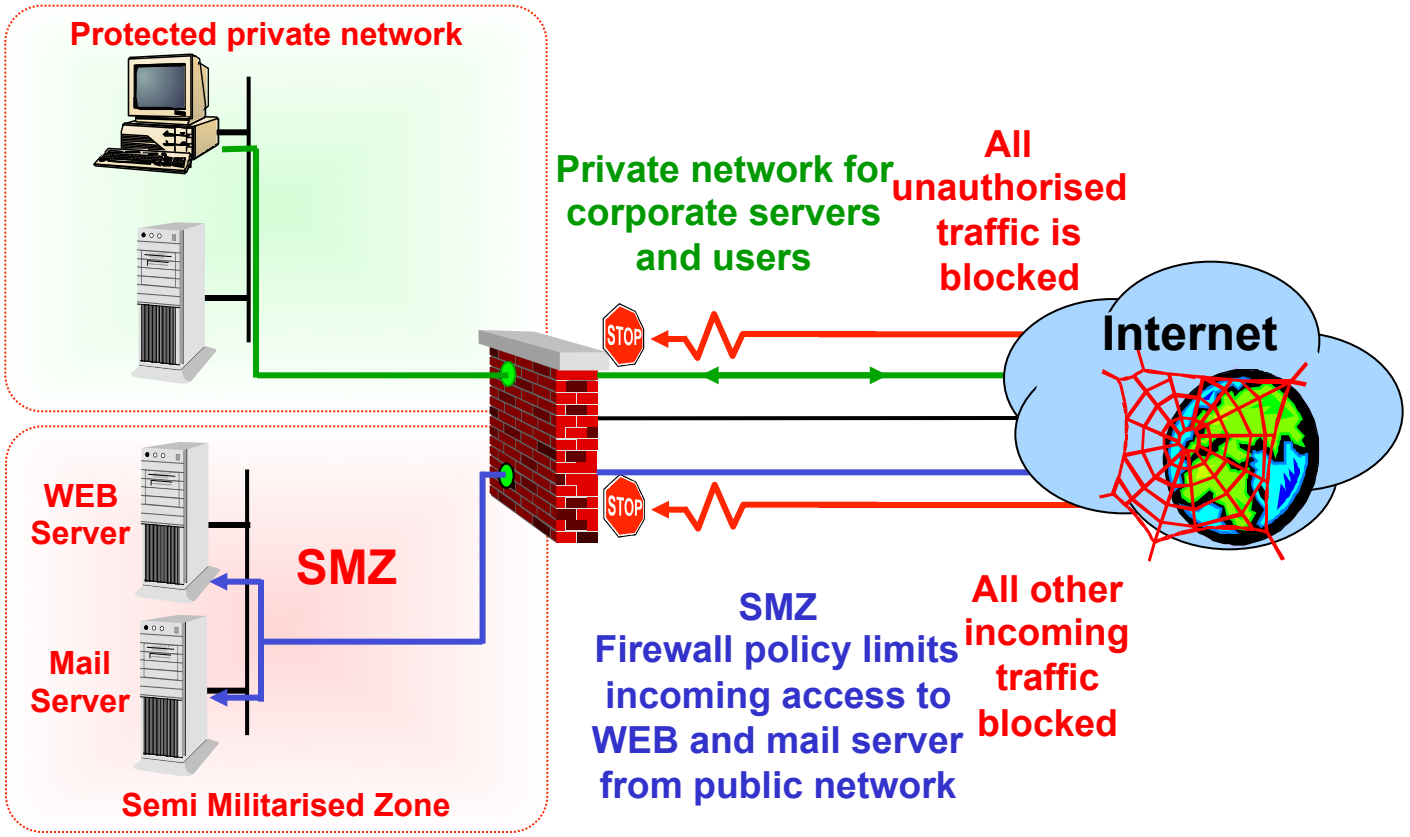
Network Configuration Examples

Protected Private Network

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



Semi-Militarised Zone



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.