



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

ACCA5034

Data Security and Compliance

Week 7 : Security Technology: Firewalls, and VPNs

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk

Learning Objective(s) and Key Concepts

Learning Objective(s)

- Explain the various approaches to firewall implementation.
- Describe virtual private networks (VPNs) and discuss the technology that enables them.

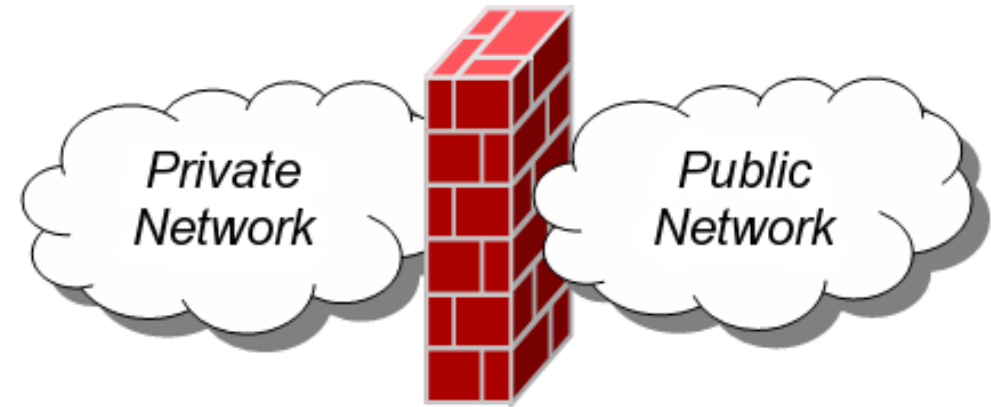
Key Concepts

We look at:

- Firewalls
- Firewall Types
- Firewall policies
- VPNs
- VPN Types

Firewalls

- A **firewall** is an integrated collection of security measures designed to prevent unauthorised electronic access to a networked computer system.
- A network firewall is similar to firewalls in building construction, because in both cases they are intended to isolate one "network" or "compartment" from another.



Firewall Technologies

- In information security, a firewall is the combination of hardware and software that filters or prevents specific information from moving between the untrusted network (outside) and the trusted network (inside).
- May be the following:
 - Separate computer system.
 - Software service running on existing router or server.
 - Separate network containing supporting devices.

Firewalls Processing Modes

- Packet filtering by data packet header information.
- Application-layer proxy by higher layer protocols and can include cache services.
- MAC layer firewalls by MAC address.
- Hybrids by a combination of the above.

Firewall Types

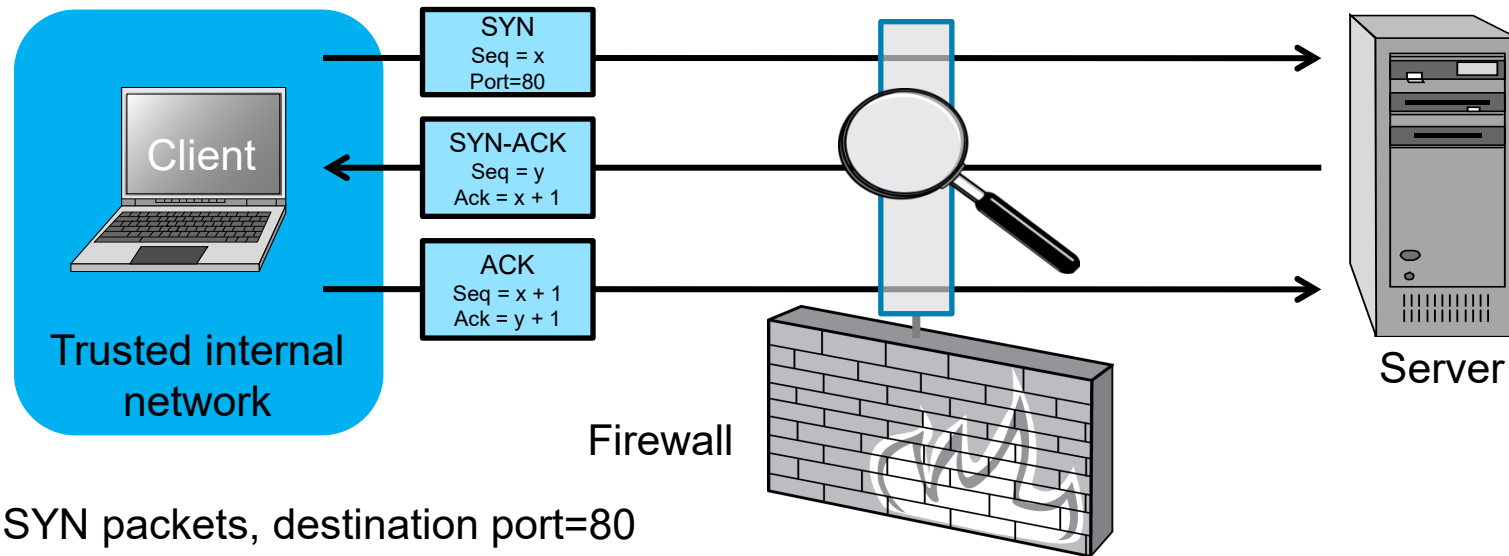
- **packet filters (stateless)**
 - If a packet matches the packet filter's set of rules, the packet filter will drop or accept it
- **"stateful" filters**
 - it maintains records of all connections passing through it and can determine if a packet is either the start of a new connection, a part of an existing connection, or is an invalid packet.
- **application layer**
 - It works like a proxy it can “understand” certain applications and protocols.
 - It may inspect the contents of the traffic, blocking what it views as inappropriate content (i.e. websites, viruses, vulnerabilities, ...)

Packet-Filtering Firewalls

- Packet-filtering firewalls examine the header information of data packets.
- Most often based on the combination of the following:
 - IP source and destination address.
 - Direction (inbound or outbound).
 - Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) source and destination port requests.
- Simple firewall models enforce rules designed to prohibit packets with certain addresses or partial addresses from passing through device.

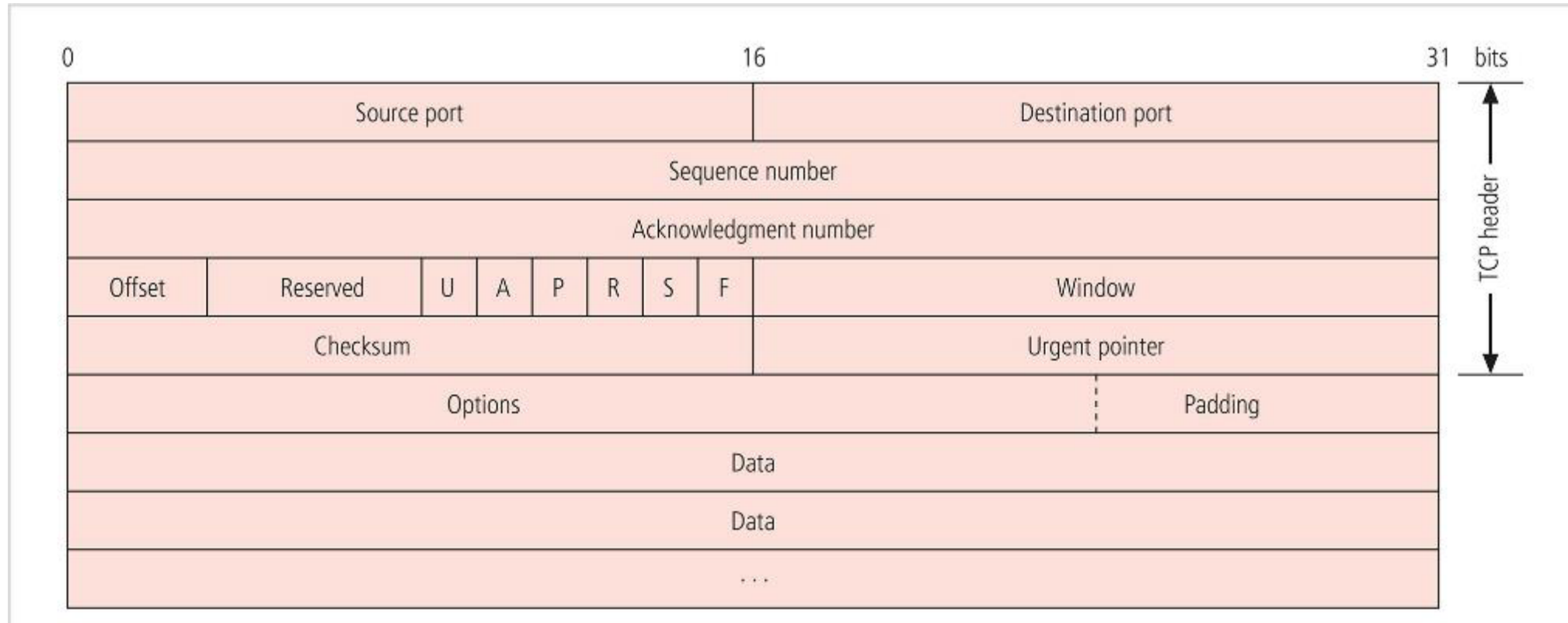
Stateless Firewalls

- A stateless firewall doesn't maintain any remembered context (or "state") with respect to the packets it is processing. Instead, it treats each packet attempting to travel through it in isolation without considering packets that it has processed previously.

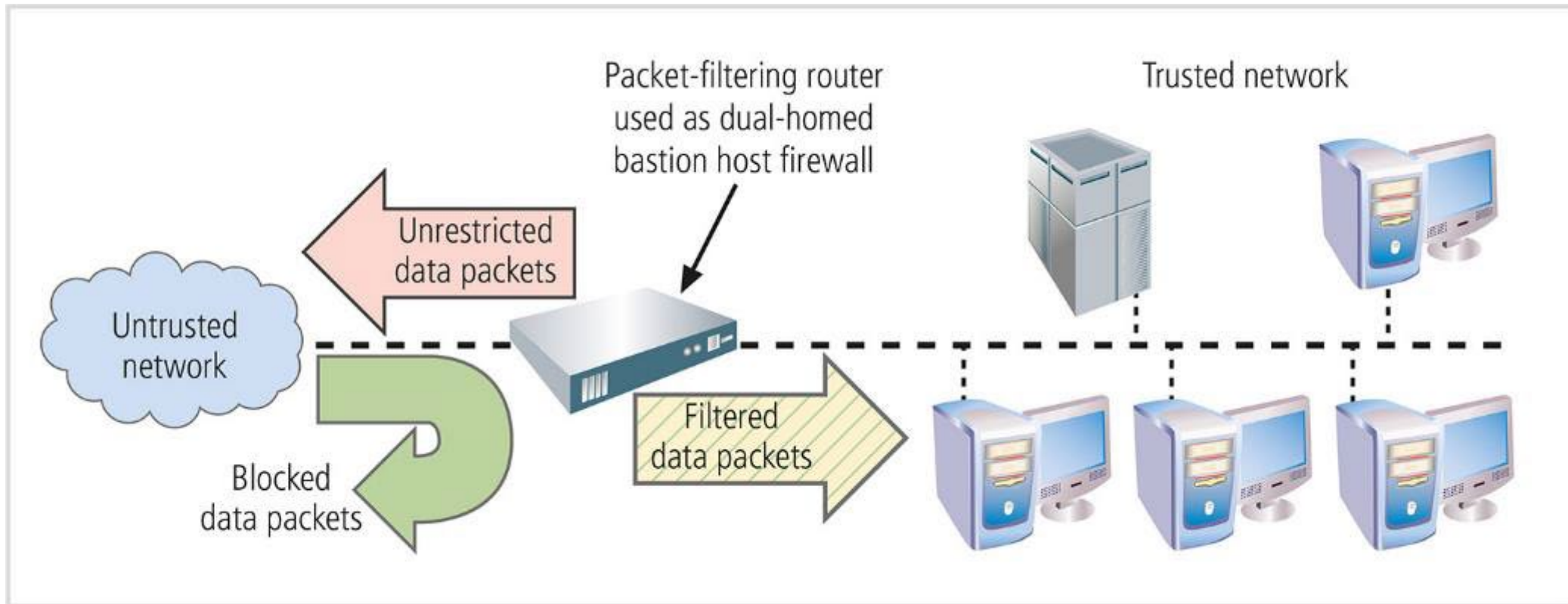


Allow outbound SYN packets, destination port=80
Allow inbound SYN-ACK packets, source port=80

TCP Packet



Packet filtering router



Packet-Filtering Firewalls

- Three subsets of packet-filtering firewalls are as follows:
 - Static filtering requires that filtering rules be developed and installed within the firewall.
 - Dynamic filtering allows firewall to react to an emergent event and update or create rules to deal with that event.
 - Stateful packet inspection (SPI) are firewalls that keep track of each network connection between internal and external systems using a state table.

Application Layer Proxy Firewall

- A device capable of functioning both as a firewall and an application layer proxy server.
- Since proxy servers are often placed in unsecured areas of the network (e.g., DMZ), they are exposed to higher levels of risk from less trusted networks.
- Additional filtering routers can be implemented behind the proxy firewall, further protecting internal systems.

MAC Layer Firewalls

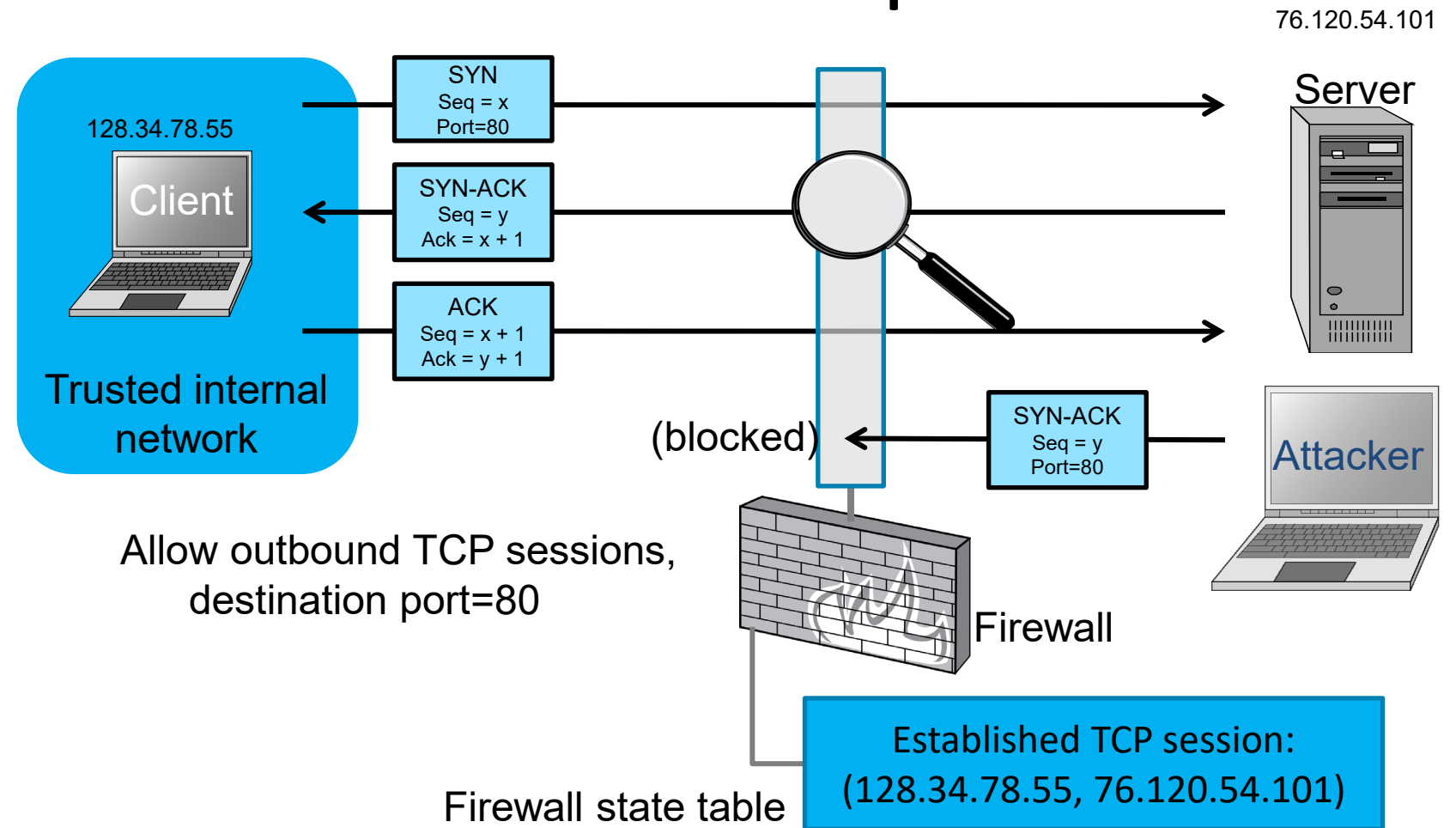
- Designed to operate at the media access control sublayer of a network's data link layer.
- Make filtering decisions based on specific host computer's identity.
- MAC addresses of specific host computers are linked to access control list (ACL) entries that identify specific types of packets that can be sent to each host. All other traffic is blocked.

Statefull Firewalls (SPI)

- **Stateful firewalls** can tell when packets are part of legitimate sessions originating within a trusted network.
- Stateful firewalls maintain tables containing information on each active connection, including the IP addresses, ports, and sequence numbers of packets.
- Using these tables, stateful firewalls can allow only inbound TCP packets that are in response to a connection initiated from within the internal network.

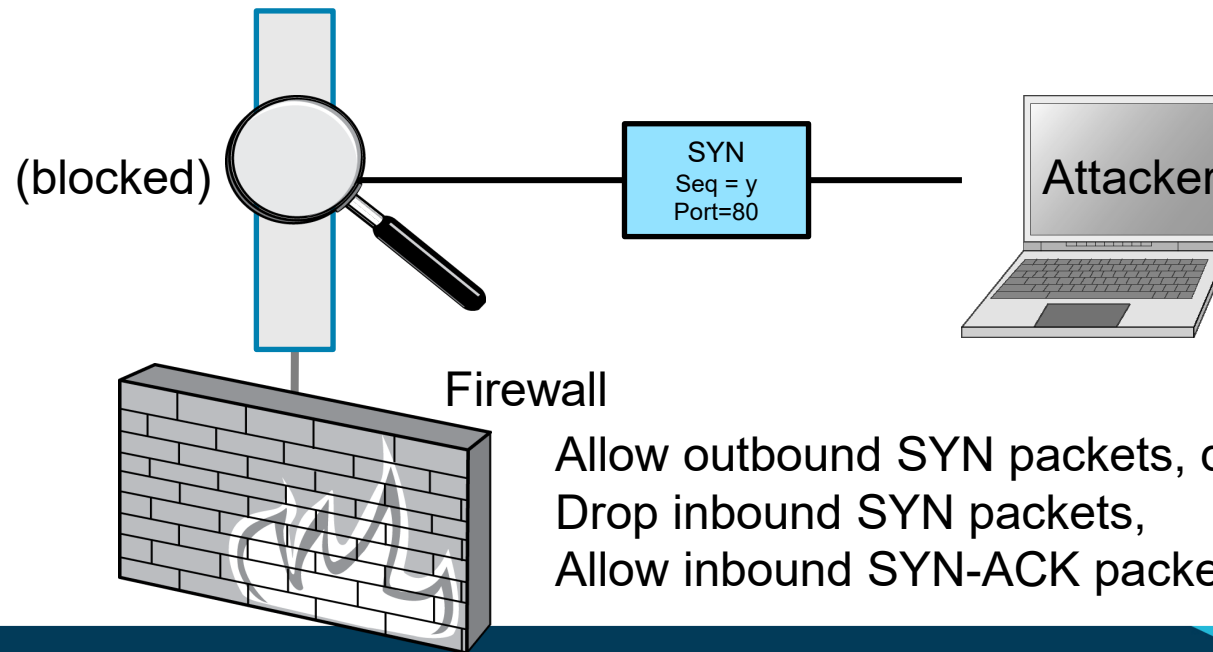
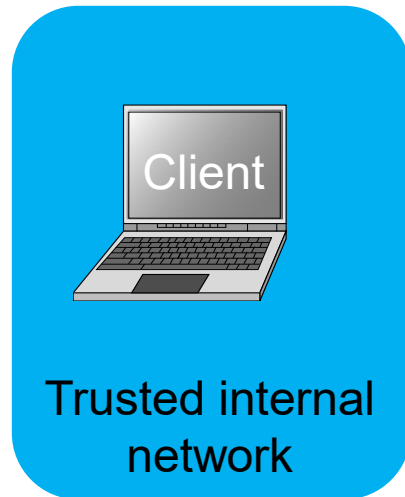
Statefull Firewall Example

Allow only
requested TCP
connections



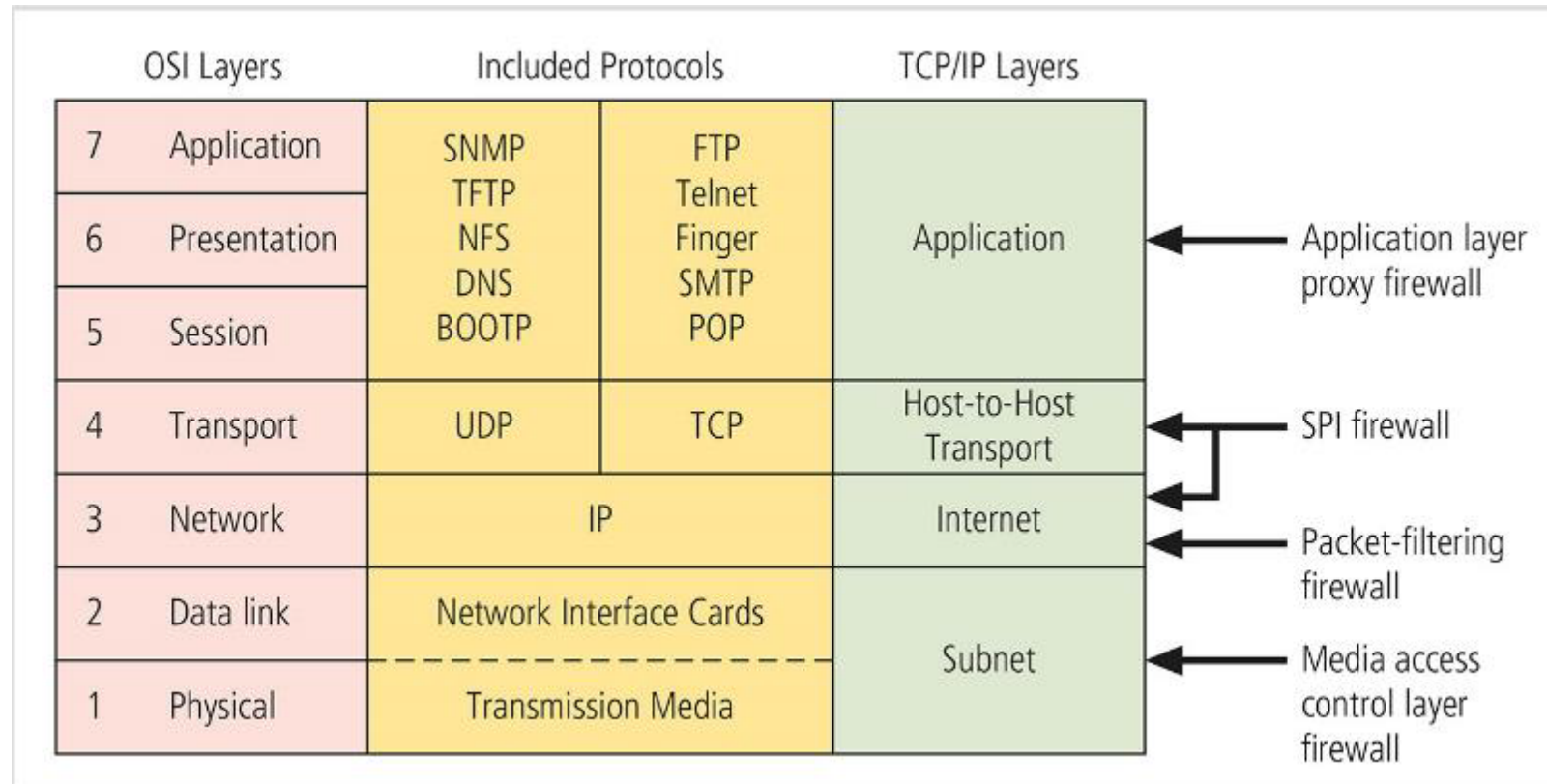
Stateless Restrictions

- Stateless firewalls may have to be fairly restrictive in order to prevent most attacks.



Allow outbound SYN packets, destination port=80
Drop inbound SYN packets,
Allow inbound SYN-ACK packets, source port=80

Firewall Types and Protocol Levels



Hybrid Firewalls

- Combine elements of other types of firewalls, that is, elements of packet filtering and proxy services, or of packet filtering and circuit gateways.
- Alternately, may consist of two separate firewall devices, each a separate firewall system, but connected to work in tandem.
- Enables an organization to make security improvement without completely replacing existing firewalls.
- Include the Next Generation Firewall (NGFW) and Unified Threat Management (UTM) devices.

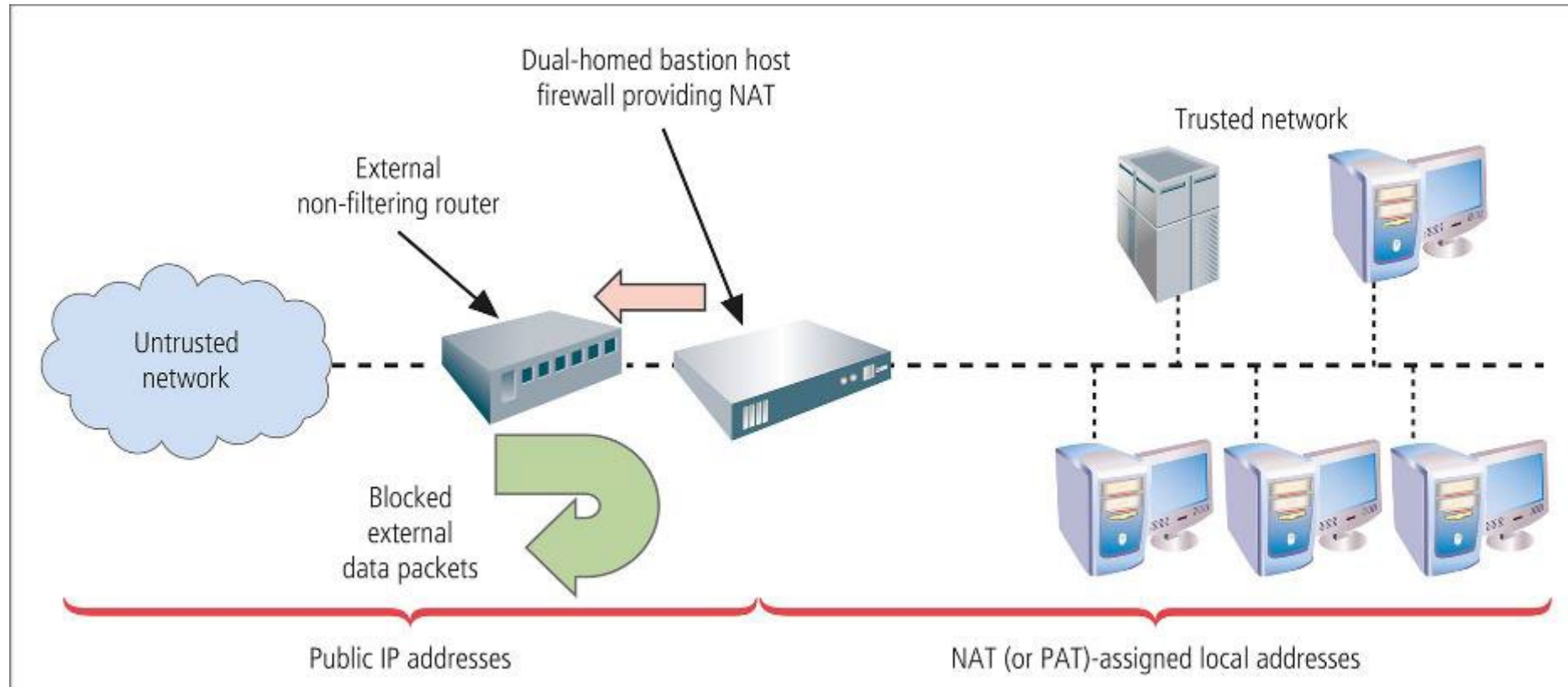
Firewall Architectures

- Firewall devices can be configured in several network connection architectures.
- Best configuration depends on three factors:
 - Objectives of the network.
 - Organization's ability to develop and implement architectures.
 - Budget available for function.
- Four common architectural implementations of firewalls: Single Bastion Hosts, Screened Host and Screened Subnet (with demilitarized zone (DMZ)).

Single Bastion Hosts

- Commonly referred to as sacrificial host as it stands as sole defender on the network perimeter.
- Usually implemented as a dual-homed host, which contains two network interface cards (NICs), one connected to external network, one connected to internal network.
- Implementation of this architecture often makes use of network address translation (NAT), creating another barrier to intrusion from external attackers.

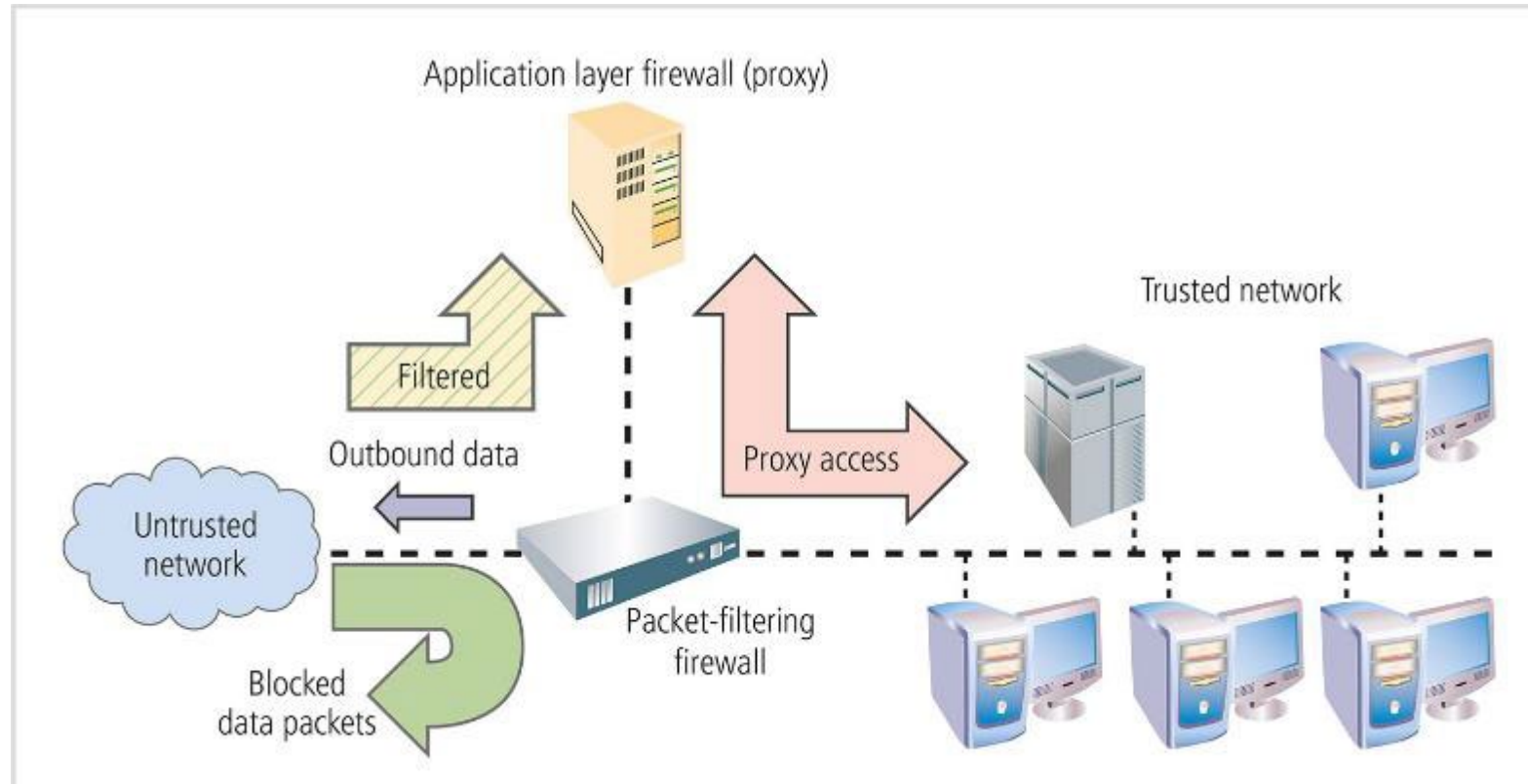
Dual-Homed Bastion Host Firewall Architecture



Screened Host Architecture

- Combines packet-filtering router with separate, dedicated firewall such as an application proxy server.
- Allows router to prescreen packets to minimize traffic/load on internal proxy.
- Requires external attack to compromise two separate systems before attack can access internal data.

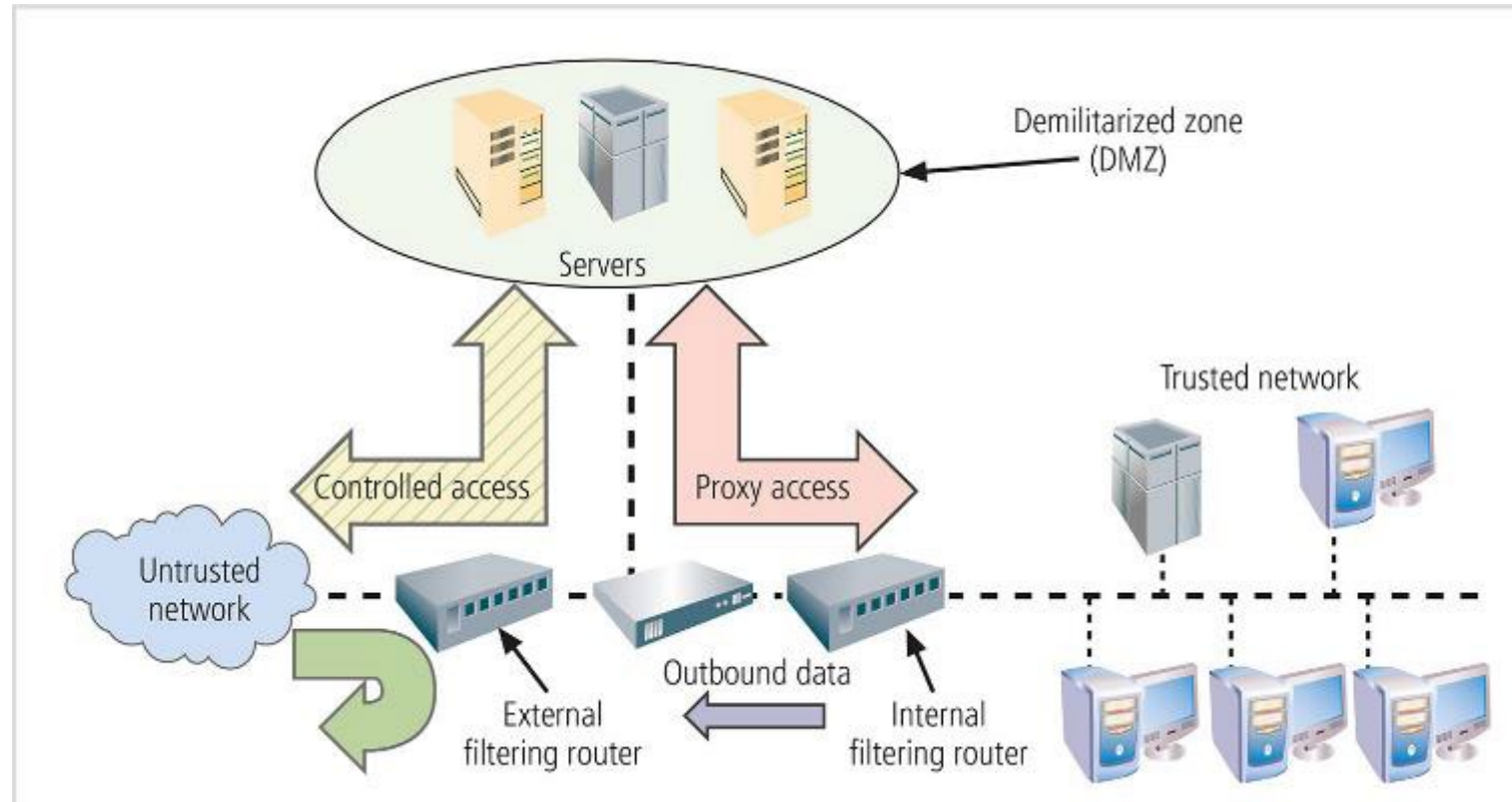
Screened Host Firewall Architecture



Screened Subnet Architecture (with DMZ)

- The dominant architecture used today.
- Commonly consists of two or more internal firewalls behind packet-filtering router with each protecting a trusted network:
 - Connections from outside or untrusted network are routed through external filtering router.
 - Connections from outside or untrusted network are routed into and out of routing firewall to separate the network segment known as DMZ.
 - Connections into trusted internal network are allowed only from DMZ bastion host servers.

Screened Subnet Firewall Architecture with DMZ

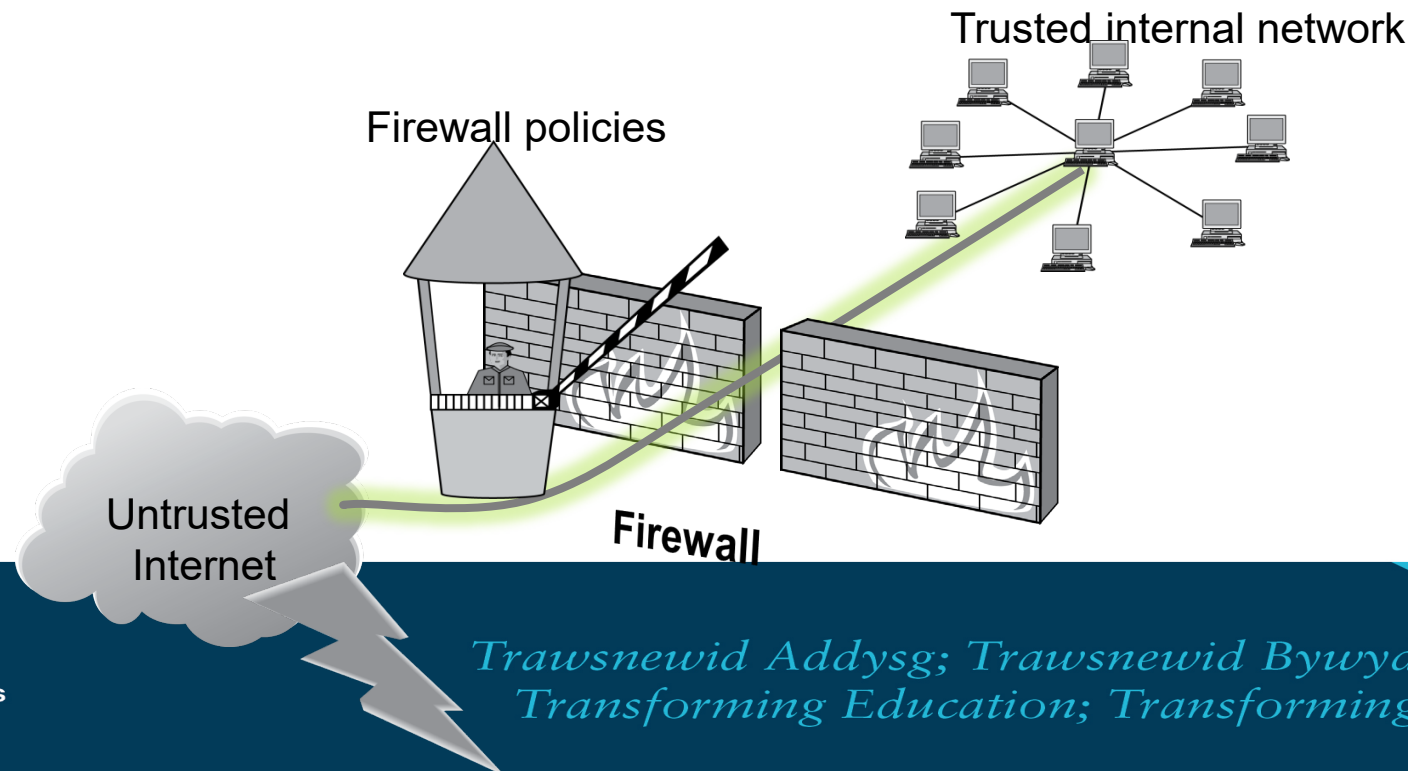


Best Practices for Firewalls

- All traffic from the trusted network is allowed out.
- Firewall device is never directly accessed from the public network.
- Simple Mail Transport Protocol (SMTP) data are allowed to pass through firewall but must go to SMTP server.
- Internet Control Message Protocol (ICMP) data are denied.
- Telnet access to internal servers should be blocked from the public network.
- When Web services are offered outside the firewall, HTTP traffic should be blocked from reaching internal networks using a DMZ or proxy access.
- All data not verifiably authentic should be denied.

Firewall Policies

- To protect private networks and individual machines from the dangers of the greater Internet, a firewall can be employed to filter incoming or outgoing traffic based on a predefined set of rules called **firewall policies**.



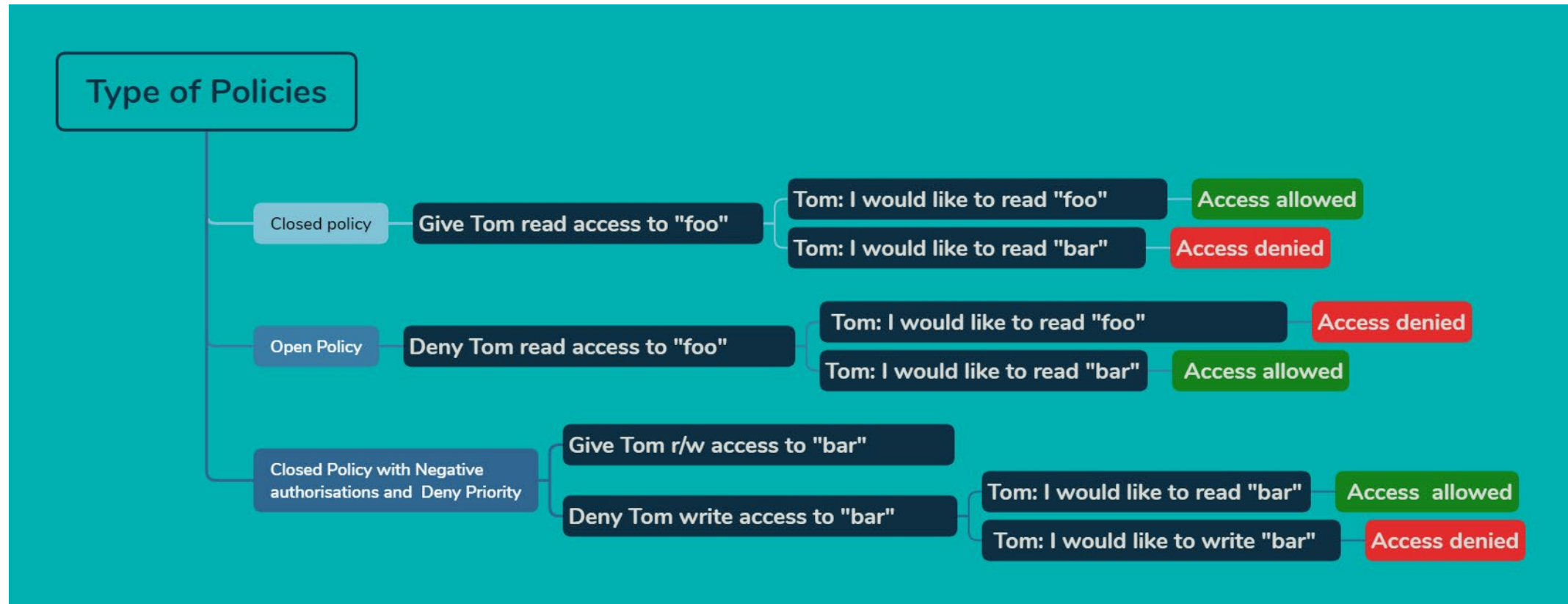
Policy Actions

- Packets flowing through a firewall can have one of three outcomes:
 - **Accepted:** permitted through the firewall
 - **Dropped:** not allowed through with no indication of failure
 - **Rejected:** not allowed through, accompanied by an attempt to inform the source that the packet was rejected
- Policies used by the firewall to handle packets are based on several properties of the packets being inspected, including the protocol used, such as:
 - TCP or UDP
 - the source and destination IP addresses
 - the source and destination ports
 - the application-level payload of the packet (e.g., whether it contains a virus).

Blacklists and White Lists

- There are two fundamental approaches to creating firewall policies (or rulesets) to effectively minimize vulnerability to the outside world while maintaining the desired functionality for the machines in the trusted internal network (or individual computer).
- **Blacklist Approach**
 - Allows all traffic except what is explicitly blocked.
 - More flexible but less secure, as it assumes all threats can be identified.
- **Whitelist Approach**
 - Blocks all traffic unless explicitly allowed.
 - More secure but requires careful rule management..

Type of policies



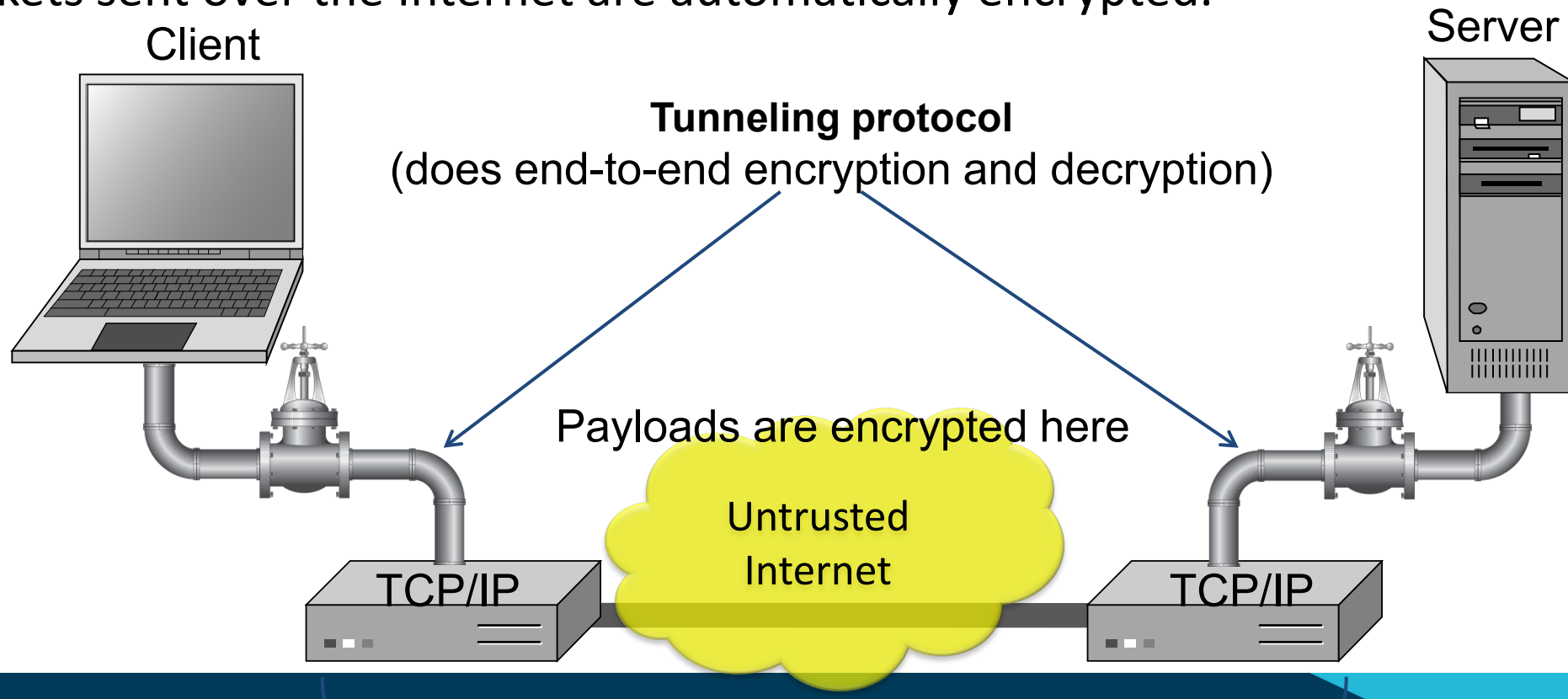
VPN

Tunnels

- The contents of TCP packets are not normally encrypted, so if someone is eavesdropping on a TCP connection, he can often see the complete contents of the payloads in this session.
- One way to prevent such eavesdropping without changing the software performing the communication is to use a **tunneling protocol**.
- In such a protocol, the communication between a client and server is automatically encrypted, so that useful eavesdropping is infeasible.

Tunneling Prevents Eavesdropping

- Packets sent over the Internet are automatically encrypted.



IPSec

- IPSec defines a set of protocols to provide confidentiality and authenticity for IP packets
- Each protocol can operate in one of two modes, **transport mode** or **tunnel mode**.
 - In **transport mode**, additional IPsec header information is inserted before the data of the original packet, and only the payload of the packet is encrypted or authenticated.
 - In **tunnel mode**, a new packet is constructed with IPsec header information, and the entire original packet, including its header, is encapsulated as the payload of the new packet.

Virtual Private Networking (VPN)

- **Virtual private networking (VPN)** is a technology that allows private networks to be safely extended over long physical distances by making use of a public network, such as the Internet, as a means of transport.
- VPN provides guarantees of data confidentiality, integrity, and authentication, despite the use of an untrusted network for transmission.
- There are two primary types of VPNs, **remote access VPN** and **site-to-site VPN**.

Types of VPNs

- **Remote access** VPNs allow authorized clients to access a private network that is referred to as an **intranet**.
 - For example, an organization may wish to allow employees access to the company network remotely but make it appear as though they are local to their system and even the Internet itself.
 - To accomplish this, the organization sets up a VPN endpoint, known as a **network access server, or NAS**. Clients typically install VPN client software on their machines, which handle negotiating a connection to the NAS and facilitating communication.
- **Site-to-site** VPN solutions are designed to provide a secure bridge between two or more physically distant networks.
 - Before VPN, organizations wishing to safely bridge their private networks purchased expensive leased lines to directly connect their intranets with cabling.

References

- Slides are devised from the recommended books:
 - Whitman & Mattord, Principles of Information Security, 6th Edition
 - Chapter 7: Security Technology: Access Controls, Firewalls, and VPNs
- Some of the slides are devised from my own notes



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Any Questions?

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk