UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Fakulti Teknologi Maklumat dan Komunikasi

Network Security Administration and Management

BITS 3353

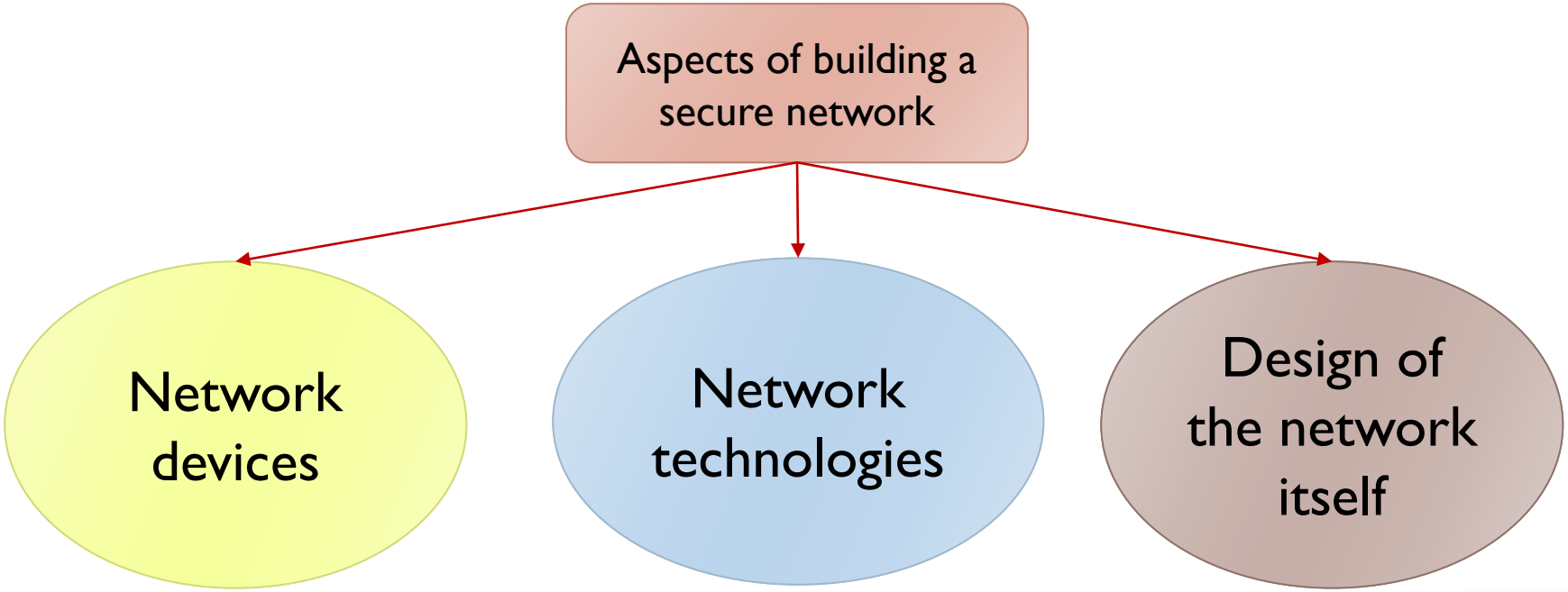
Lecture 8: Network Security

Objectives

- List the different types of network security devices and explain how they can be used
- Define network address translation and network access control
- Explain how to enhance security through network design

Security Through Network Devices

- Not all applications designed, written with security in mind
- Network must provide protection
- Networks with weak security invite attackers

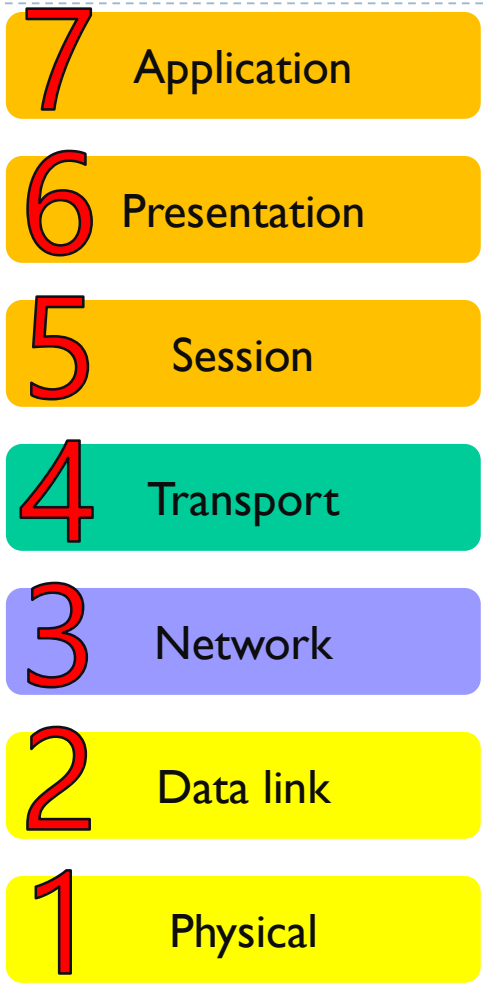


Standard Network Devices

Security features found in network hardware
–Provide basic level of security

Open systems interconnection (OSI) model
–Network devices classified based on function
–Standards released in 1978, revised in 1983, still used today
–Illustrates:
•How network device prepares data for delivery
•How data is handled once received

OSI model breaks networking steps into seven layers
–Each layer has different networking tasks
–Each layer cooperates with adjacent layers



Layer number	Layer name	Description	Function
Layer 7	Application Layer	The top layer, Application, provides the user interface to allow network services	Provides services for user applications
Layer 6	Presentation Layer	The Presentation Layer is concerned with how the data is represented and formatted for the user	Is used for translation, compression, and encryption
Layer 5	Session Layer	This layer has the responsibility of permitting the two parties on the network to hold ongoing communications across the network	Allows devices to establish and manage sessions
Layer 4	Transport Layer	The Transport Layer is responsible for ensuring that error-free data is given to the user	Provides connection establishment, management, and termination as well as acknowledgments and retransmissions
Layer 3	Network Layer	The Network Layer picks the route the packet is to take, and handles the addressing of the packets for delivery	Makes logical addressing, routing, fragmentation, and reassembly available
Layer 2	Data Link Layer	The Data Link Layer is responsible for dividing the data into packets; some additional duties of the Data Link Layer include error detection and correction (for example, if the data is not received properly, the Data Link Layer would request that it be retransmitted)	Performs physical addressing, data framing, error detection, and handling
Layer 1	Physical Layer	The job of this layer is to send the signal to the network or receive the signal from the network	Involved with encoding and signaling, data transmission, and reception

OSI reference model

Standard Network Devices

HUB

- Connect multiple Ethernet devices together:

•To function as a single network segment

- Use twisted-pair copper or fiber-optic cables
- Work at Layer 1 of the OSI model
- Do not read data passing through them
- Ignorant of data source and destination
- Rarely used today because of inherent security vulnerability

SWITCH

- Network switch connects network segments
- Operate at Data Link Layer (Layer 2)
- Determine which device is connected to each port
- Can forward frames sent to that specific device

•Or broadcast to all devices

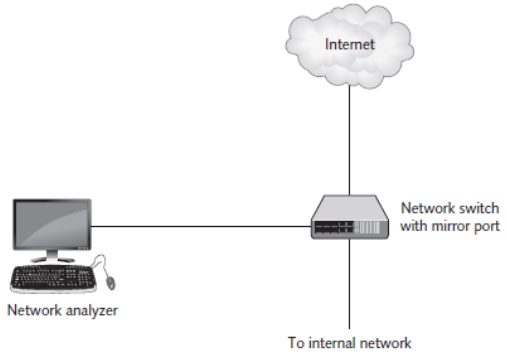
- Use MAC address to identify devices
- Provide better security than hubs

Standard Network Devices

- Network administrator should be able to monitor network traffic
  - –Helps identify and troubleshoot network problems

Traffic Monitoring Method

Port mirroring



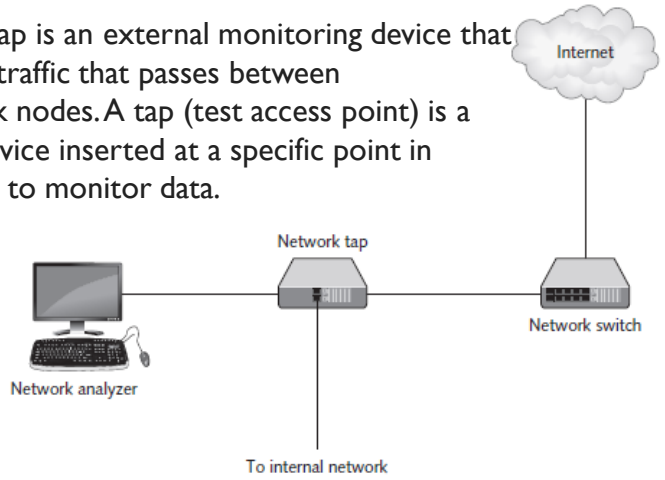
Port mirroring is a method of copying and sending network packets transmitted as input from a port to another port of a monitoring computer/switch/device. It is a network monitoring technique implemented on network switches and similar devices

Network tap

(test access point)

Separate device installed between 2 network devices

A network tap is an external monitoring device that mirrors the traffic that passes between two network nodes. A tap (test access point) is a hardware device inserted at a specific point in the network to monitor data.



Standard Network Devices

Type of attack	Description	Security defense
MAC flooding	An attacker can overflow the switch's address table with fake MAC addresses, forcing it to act like a hub, sending packets to all devices	Use a switch that can close ports with too many MAC addresses
MAC address impersonation	If two devices have the same MAC address, a switch may send frames to each device; an attacker can change the MAC address on their device to match the target device's MAC address	Configure the switch so that only one port can be assigned per MAC address
ARP poisoning	The attacker sends a forged ARP packet to the source device, substituting the attacker's computer MAC address	Use an ARP detection appliance
Port mirroring	An attacker connects his device to the switch's mirror port	Secure the switch in a locked room
Network tap	A network tap is connected to the network to intercept frames	Keep network connections secure by restricting physical access

Protecting the switch

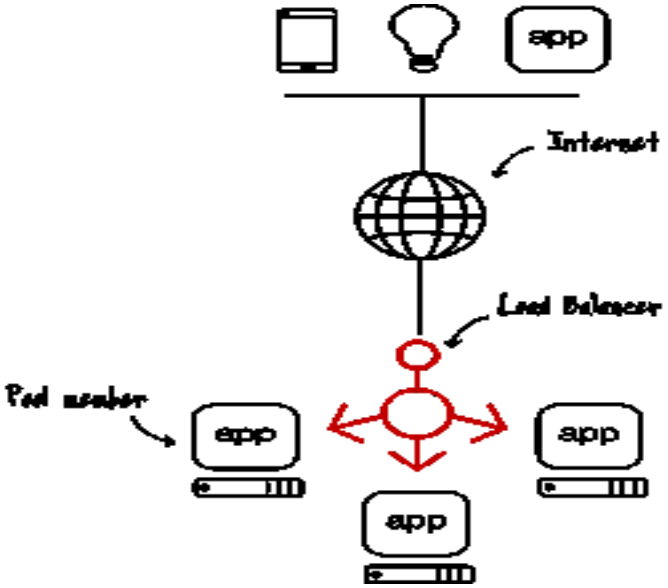
Standard Network Devices

ROUTERS

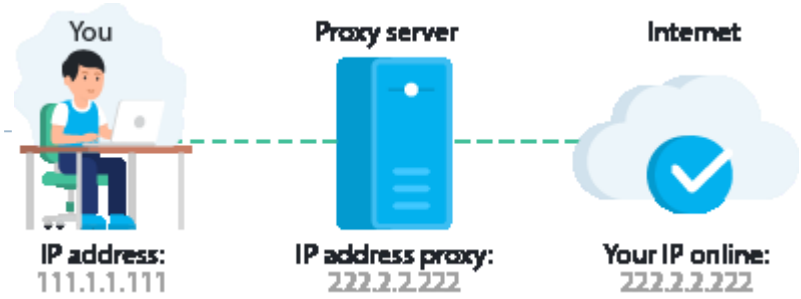
- Forward packets across computer networks
- Operate at Network Layer (Layer 3)
- Can be set to filter out specific types of network traffic

LOAD BALANCER

- Load balancer lets you evenly distribute network traffic to prevent failure caused by overloading a particular resource.
- Load-balancing technology provides these advantages:
  - The probability of overloading a single server is reduced.
  - Each networked computer can benefit from having optimized bandwidth.
  - Network downtime can be reduced.



PROXY SERVER



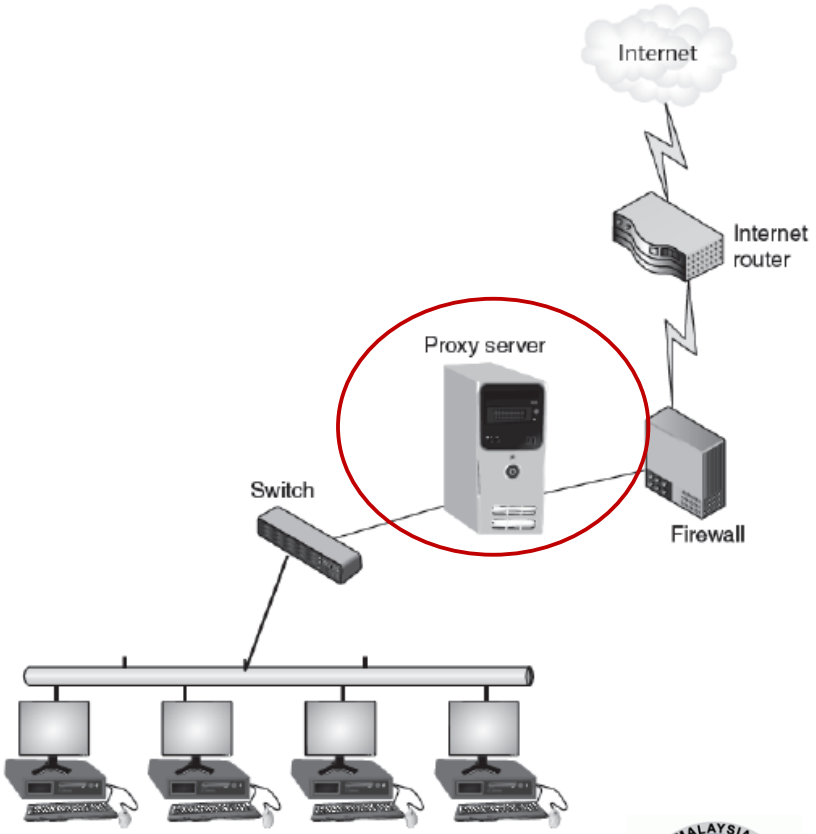
- A proxy server is a or an application
- program that intercepts user requests from the internal secure network and then processes that request on behalf of the user.

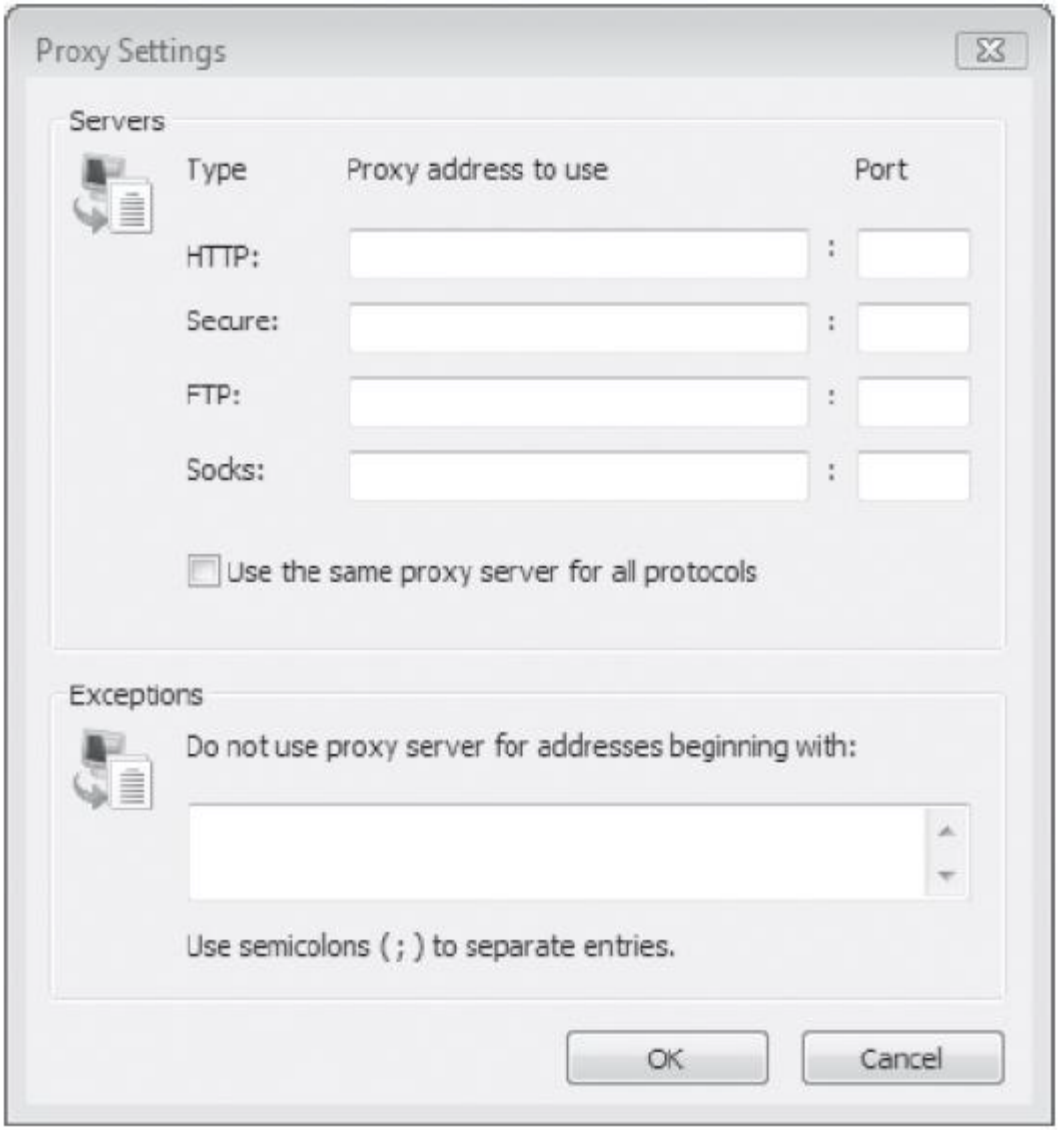
- Without a proxy server, your data travels along the following route:

When you type a website into your address bar and press enter, the information goes from your computer through your internet service provider's (ISP) router first. Then it continues to the server of the site you requested. The site's reply is sent back along the same route.

- If you use a proxy server, the path from your computer to the website is a little different.

The user (meaning you) connects to the proxy server, for example with a computer, laptop or smartphone. The proxy server sends your request on to its destination on the internet. The rest of the web won't be able to see your IP address, but the IP of the proxy.





Configuring access to proxy servers

Proxy server advantages

- Improved management
  - -Block specific Web pages or sites
- Stronger security
  - -Intercept malware
  - -Hide client system's IP address from the open Internet

Network Security Hardware

- Specifically designed security hardware devices

WHY? Greater protection than standard networking devices

FIREWALLS

SPAM FILTERS

VPN

IDS

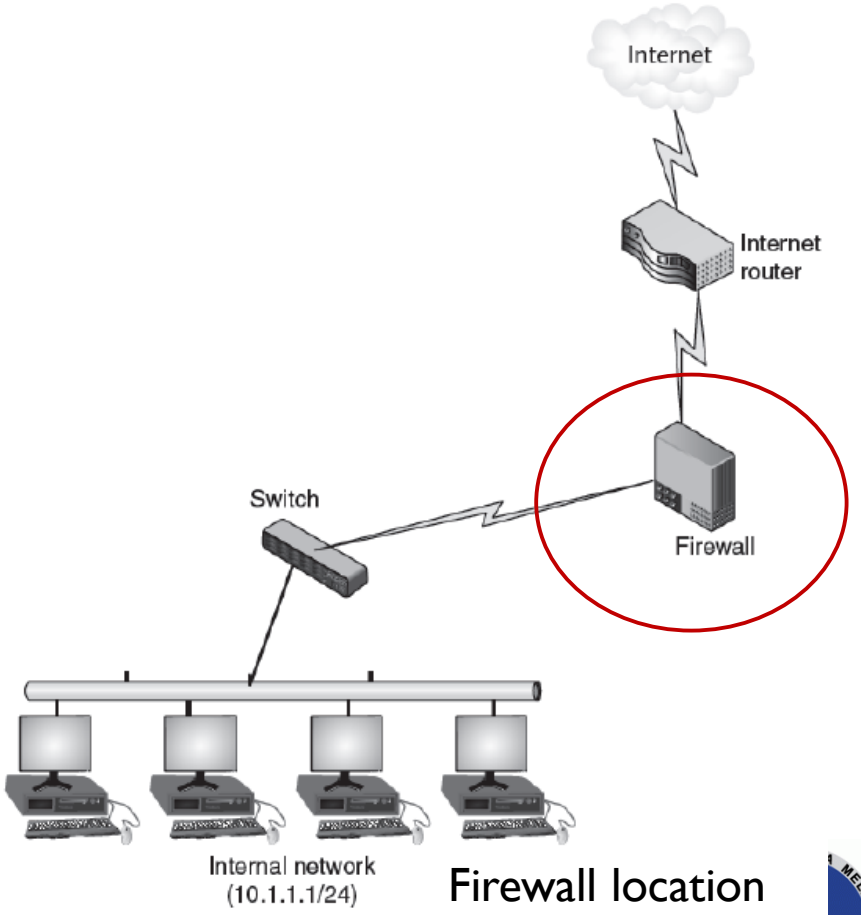
INTERNET CONTENT FILTER

WEB SECURITY GATEWAYS

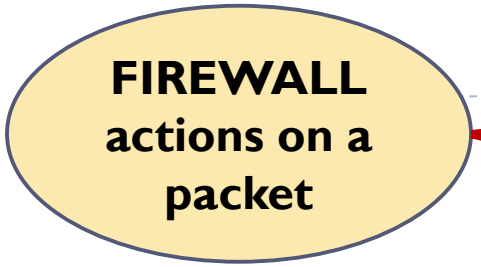
Network Security Hardware

FIREWALLS

- Firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
- A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet
- Can either accept or deny packet entry
- Usually located outside network security perimeter



Firewall location

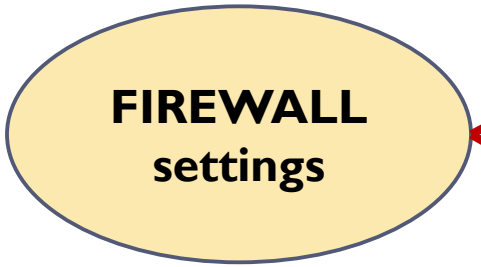


Allow

Drop

Reject

Ask

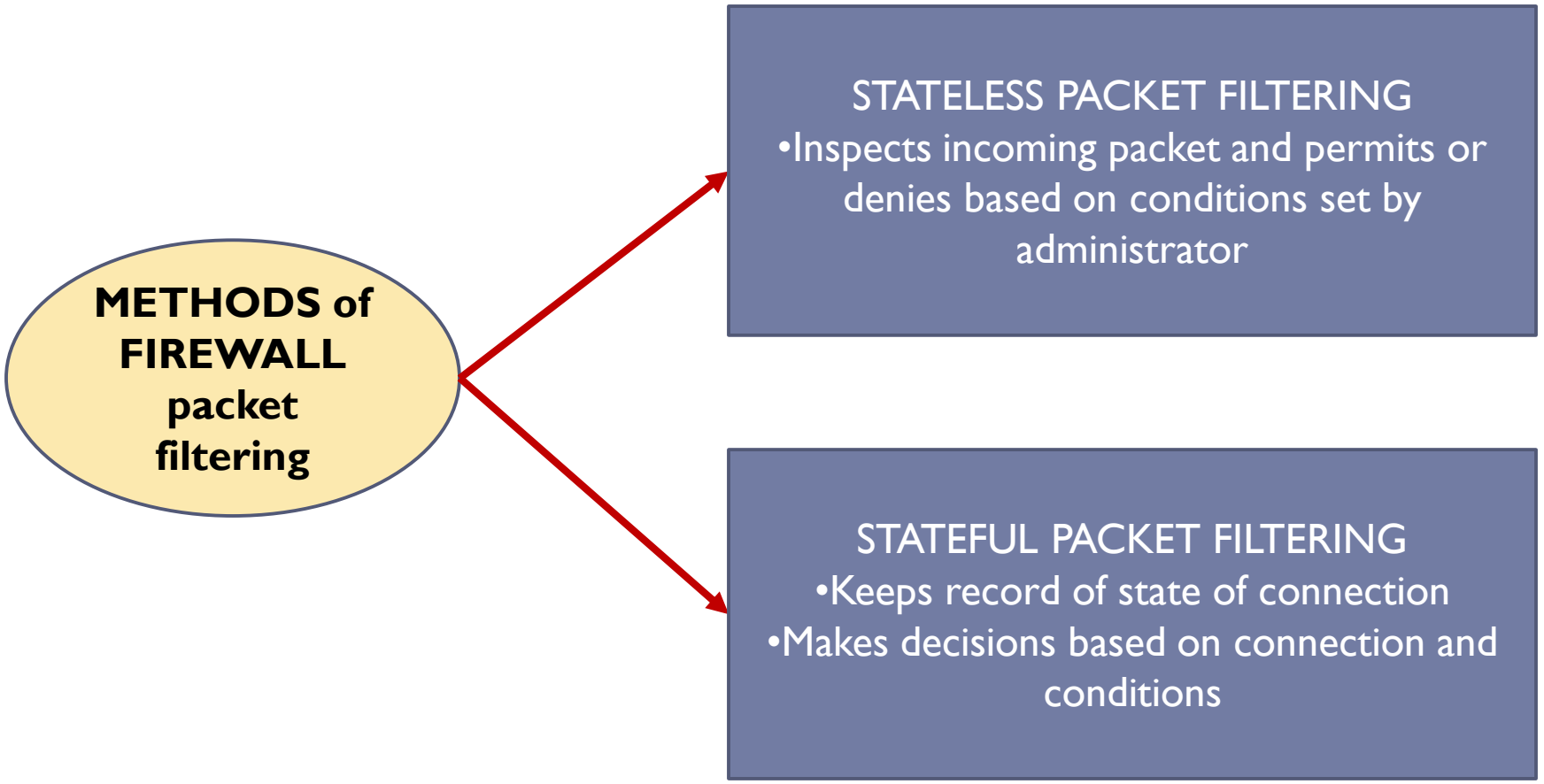


Rule-based firewall settings

–Set of individual instructions to control actions

Application-Aware firewall

–identifying the applications that send packets through the firewall and then make decisions about the application


METHODS of FIREWALL packet filtering
STATELESS PACKET FILTERING
•Inspects incoming packet and permits or denies based on conditions set by administrator
STATEFUL PACKET FILTERING
•Keeps record of state of connection
•Makes decisions based on connection and conditions

Network Security Hardware

SPAM FILTERS

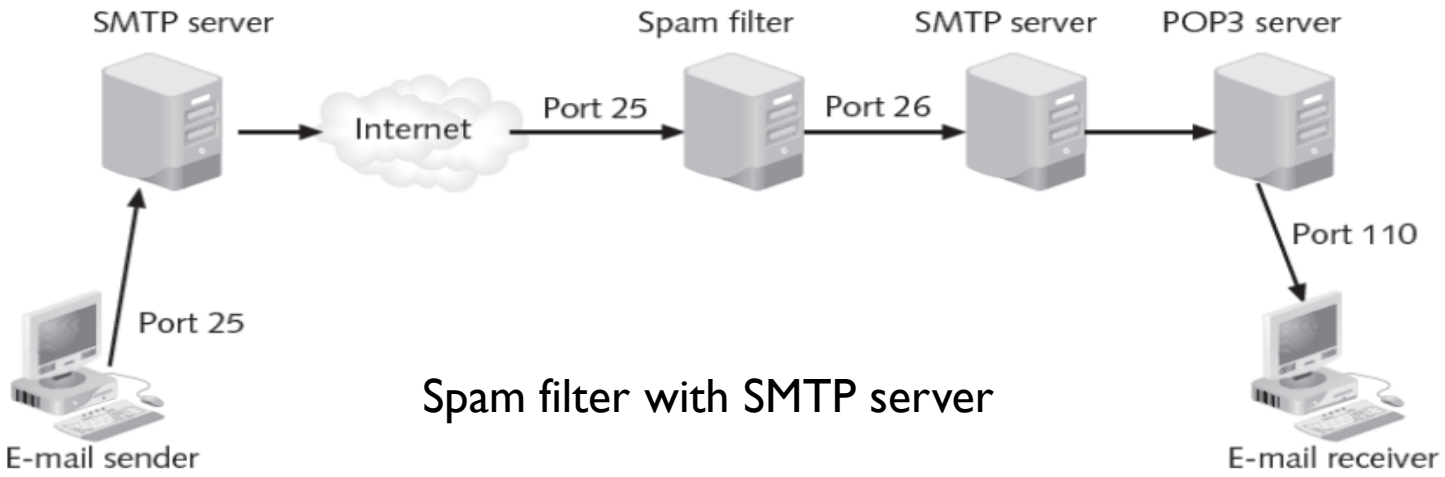
➢ Spam filters block spam before it reaches the host

Email systems use two protocols

Simple Mail Transfer Protocol (SMTP)
•Handles outgoing mail

Post Office Protocol (POP)
•Handles incoming mail

Spam filters installed with the SMTP server
–Filter configured to listen on port 25
–Pass non-spam e-mail to SMTP server listening on another port
–Method prevents SMTP server from notifying spammer of failed message delivery



Spam filter with SMTP server

Network Security Hardware

SPAM FILTERS

2

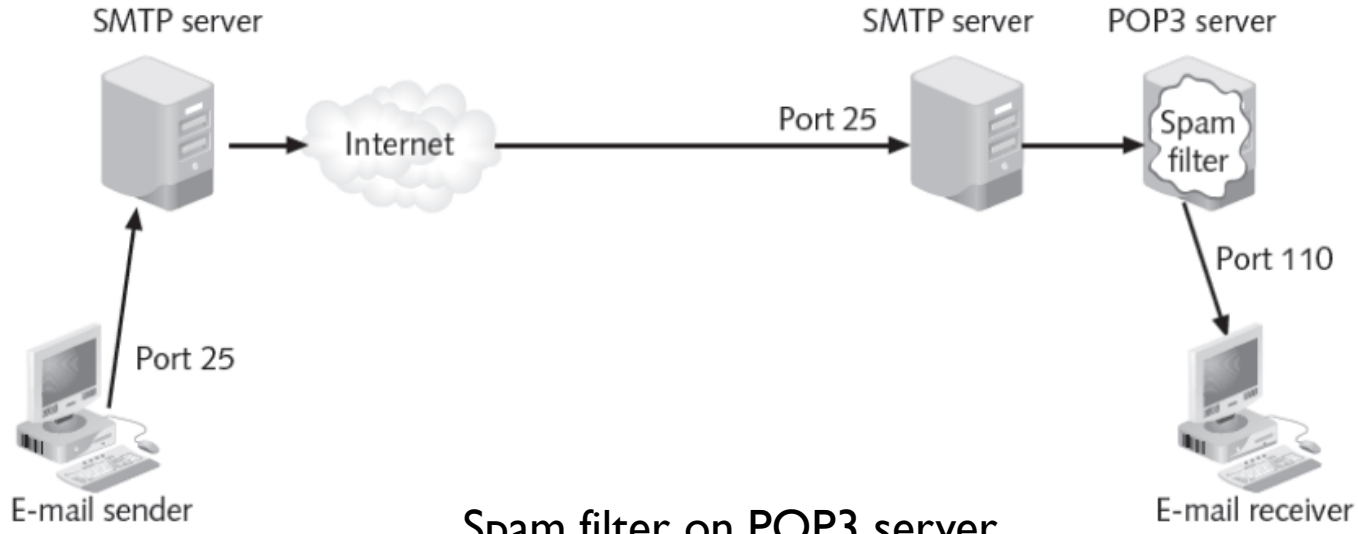
Spam filters installed on the POP3 server

-Filter configured to listen on port 100

–All spam must first pass through SMTP server and be delivered to user's mailbox

–Can result in increased costs

•Storage, transmission, backup, deletion



Spam filter on POP3 server

Network Security Hardware

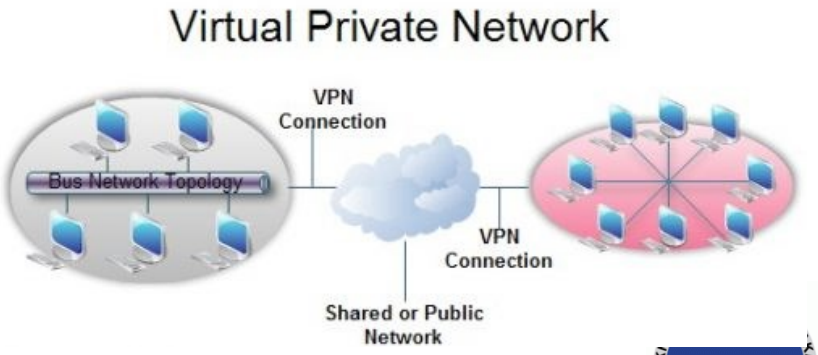
VIRTUAL PRIVATE NETWORK (VPN)

- **Virtual private network** (**VPN**) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.
- VPN technology was developed to allow remote users and branch offices to access corporate applications and resources. To ensure security, the private network connection is established using an encrypted layered tunneling protocol and VPN users use authentication methods, including passwords or certificates, to gain access to the VPN.

TYPES OF VPNs

Remote-access
- User to LAN connection

Site-to-site
- Multiple sites can connect to other sites over the Internet



Network Security Hardware

INTERNET CONTENT FILTERS

- Monitor Internet traffic
- Block access to preselected Web sites and files
- Unapproved sites identified by URL or matching keywords

Feature	Description
URL and content filtering	Network administrators can block access to specific Web sites or allow only specific Web sites to be accessed, while all others are blocked; blocking can be based on keywords, URL patterns, or lists of prohibited sites
Malware filtering	Filters can assess if a Web page contains any malicious elements or exhibits any malicious behavior, and then flag questionable pages with a warning message
Prohibit file downloads	Executable programs (.exe), audio or video files (.mp3, .avi, .mpg), and archive files (.zip, .rar) can be blocked
Profiles	Content-specific Web sites, such as adult, hacking, and virus-infected Web sites, can be blocked
Detailed reporting	Administrators can monitor Internet traffic and identify users who attempt to foil the filters

Internet content filter features

Network Security Hardware

WEB SECURITY GATEWAYS

- Can block malicious content in real time
- Block content through application level filtering

Examples of blocked Web traffic
- Cookies
- Adware, spyware
- Peer to peer file sharing
- Script exploits

MONITORING METHOD

ANOMALY-BASED MONITORING

- Compares current detected behavior with baseline

SIGNATURE-BASED MONITORING

- Looks for well-known attack signature patterns

BEHAVIOR-BASED MONITORING

- Detects abnormal actions by processes or programs
- •Alerts user who decides whether to allow or block activity

HEURISTIC MONITORING

- Uses experience-based techniques

Monitoring methodology	Trap application scanning ports?	Comments
Anomaly-based monitoring	Depends	Only if this application had tried to scan previously and a baseline had been established
Signature-based monitoring	Depends	Only if a signature of scanning by this application had been previously created
Behavior-based monitoring	Depends	Only if this action by the application is different from other applications
Heuristic monitoring	Yes	IDS is triggered if any application tries to scan multiple ports

Methodology comparisons to trap port-scanning application

Network Security Hardware

INTRUSION DETECTION AND PREVENTION

HOST INTRUSION DETECTION SYSTEM (HIDS)

- Software-based application that can detect attack as it occurs
- Installed on each system needing protection
- Monitors system calls and file system access
- Can recognize unauthorized Registry modification
- Monitors all input and output communications
  - Detects anomalous activity

NETWORK INTRUSION DETECTION SYSTEM (NIDS)

- Watches for attacks on the network
- NIDS sensors installed on firewalls and routers:
  - Gather information and report back to central device
- Passive NIDS will sound an alarm
- Active NIDS will sound alarm and take action
  - Actions may include filtering out intruder's IP address or terminating TCP session

Security Through Network Technologies: Network Address Translation

- Internet routers normally drop packet with a private address

Network address translation (NAT)

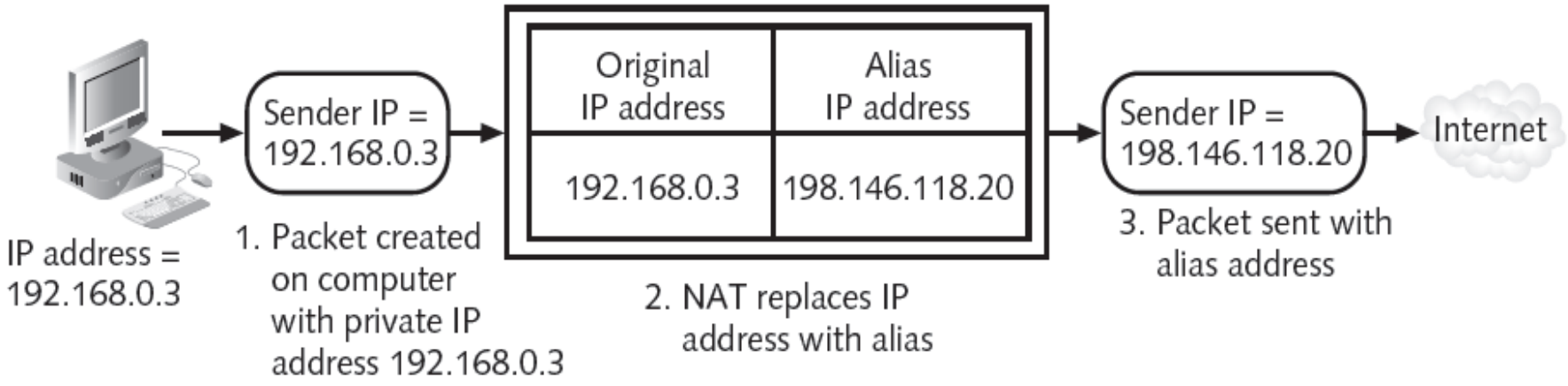
–Allows private IP addresses to be used on the public Internet
–Replaces private IP address with public address

Port address translation (PAT)

–Variation of NAT
•Outgoing packets given same IP address but different TCP port number

NAT Advantages

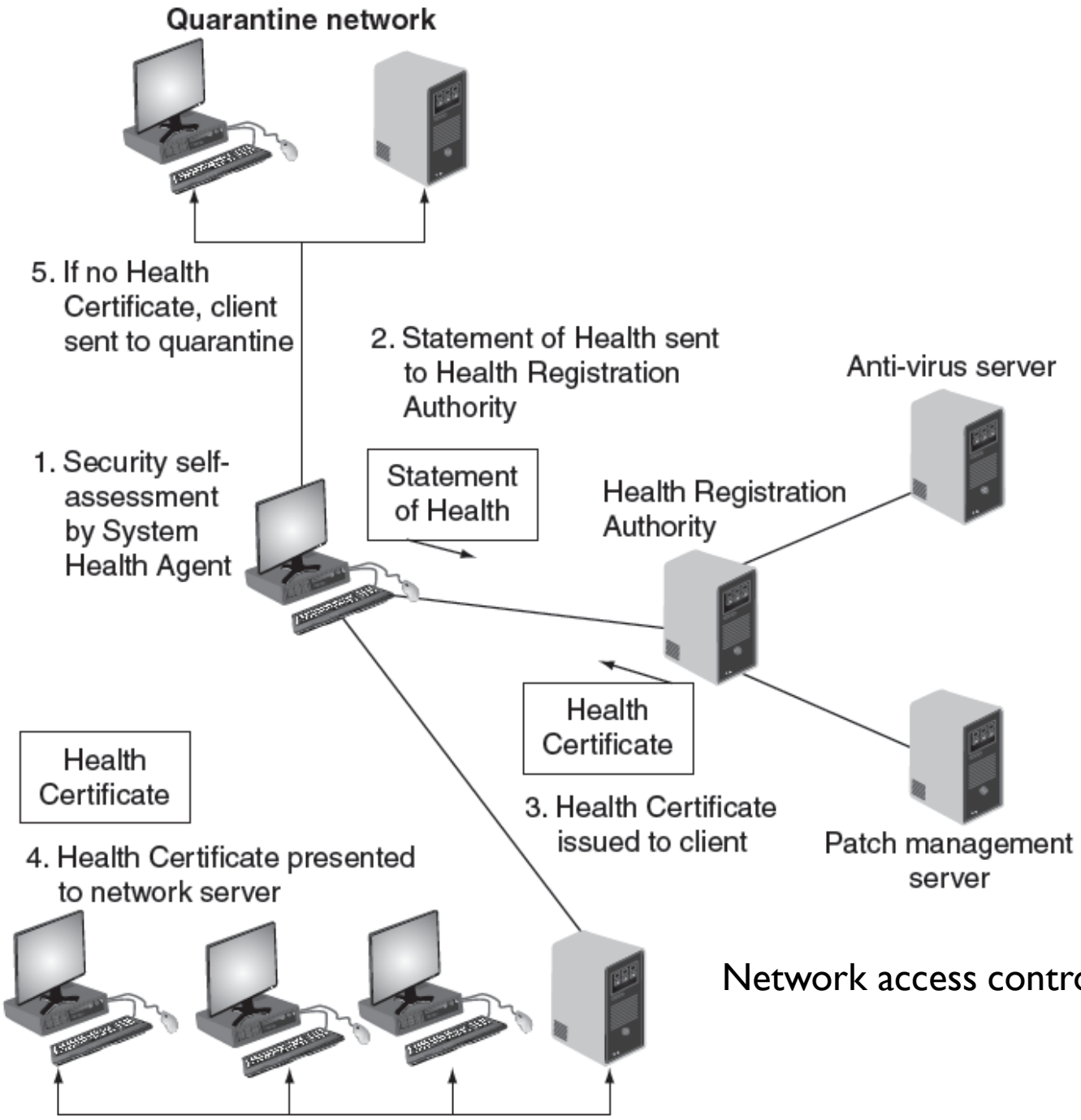
–Masks IP addresses of internal devices
–Allows multiple devices to share smaller number of public IP addresses



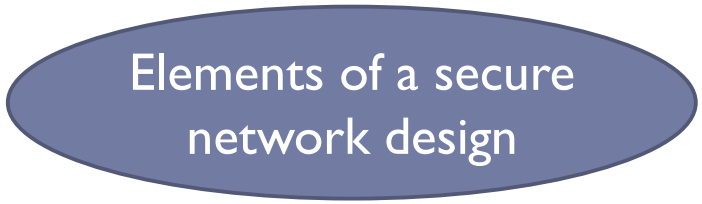
Network address translation (NAT)

Security Through Network Technologies: Network Access Control (NAC)

- Examines current state of system or network device:
  -Before allowing network connection
- Device must meet set of criteria
  -If not met, NAC allows connection to quarantine network until deficiencies corrected



Network access control framework



Demilitarized zones

Virtual LANs

Subnetting

Remote Access

Demilitarized zones

- Separate network located outside secure network perimeter
- Untrusted outside users can access DMZ but not secure network

Demilitarized zones

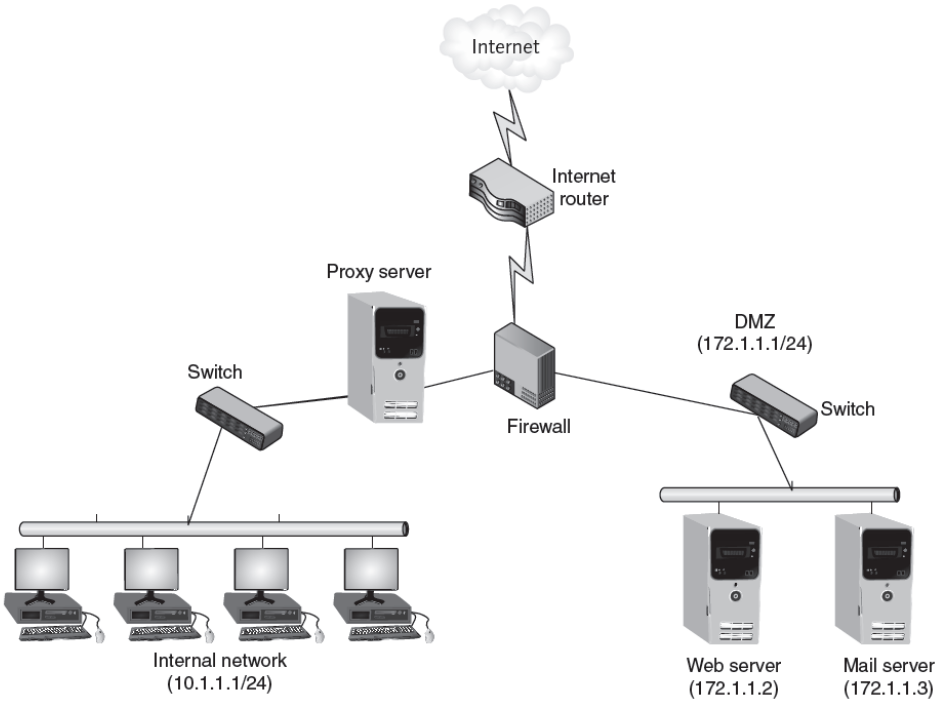


Figure 1: DMZ with one firewall

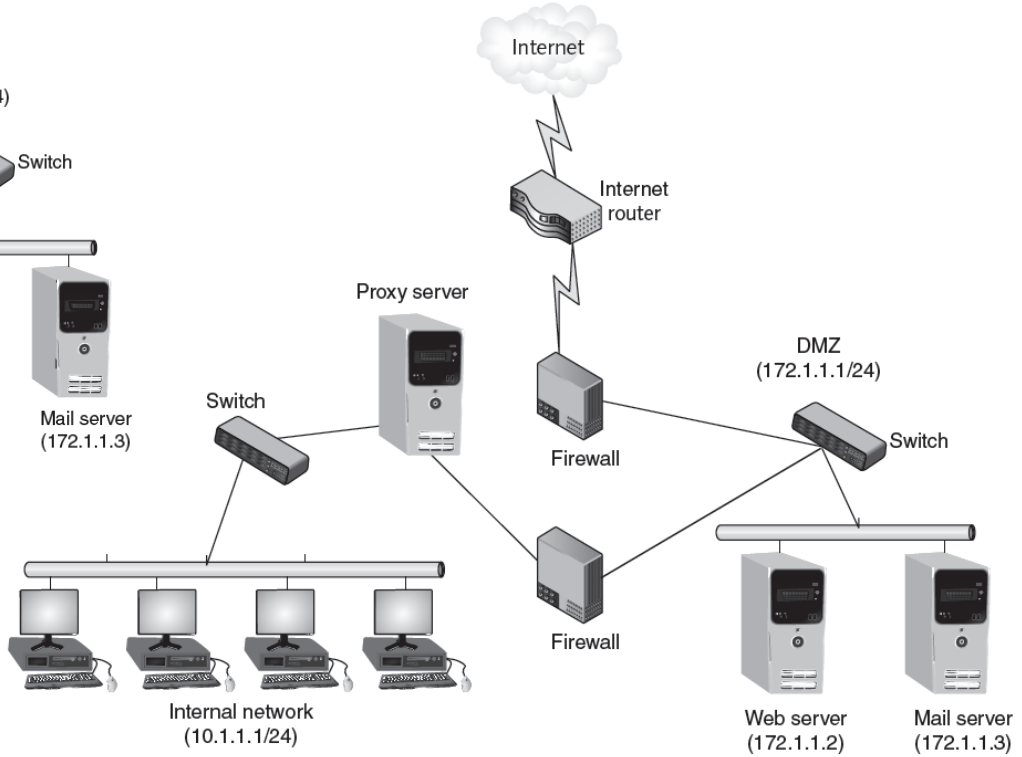


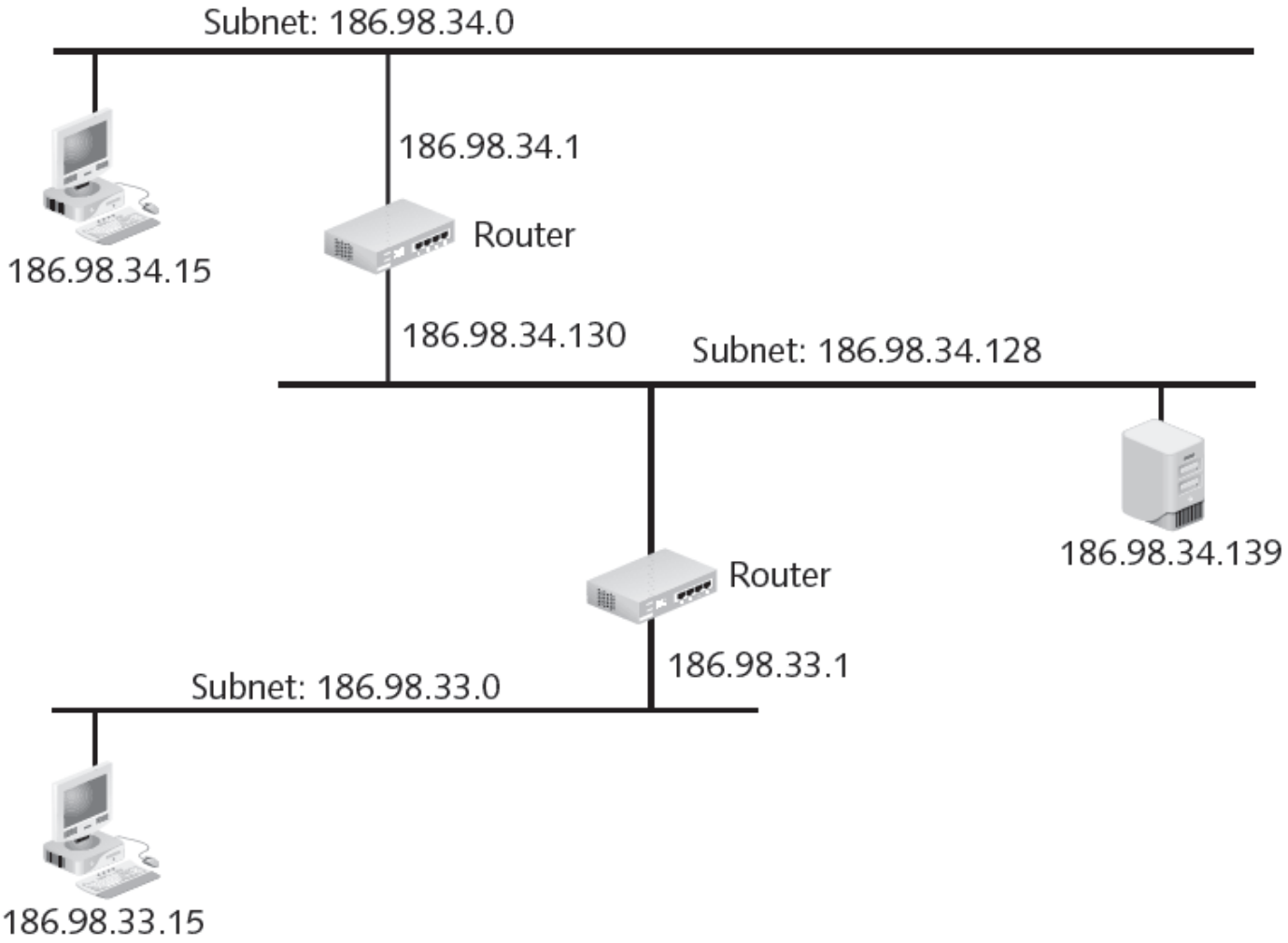
Figure 2: DMZ with two firewalls

Elements of a secure network design

Subnetting

- Dividing a network into two or more networks
- Network administrators can utilize network security tools to make it easier to regulate who has access in and out of a particular subnetwork.
- Subnet addresses are instantly recognizable so that the source of potential security issues can be quickly addressed.

Subnetting


Subnet: 186.98.34.0
186.98.34.1
Router
186.98.34.15
186.98.34.130
Subnet: 186.98.34.128
186.98.34.139
Router
186.98.33.1
Subnet: 186.98.33.0
186.98.33.15

Subnetting

Advantage	Explanation
Decreased network traffic	Broadcasts to network hosts are generally limited to individual subnets
Flexibility	The number of subnets and hosts on each subnet can be customized for each organization and easily changed as necessary
Improved troubleshooting	Tracing a problem on a subnet is faster and easier than on a single large network
Improved utilization of addresses	Because networks can be subdivided, it generally reduces the number of wasted IP addresses
Minimal impact on external routers	Because only routers within the organization are concerned with routing between subnets, routers outside the organization do not have to be updated to reflect changes
Reflection of physical network	Hosts can be grouped together into subnets that more accurately reflect the way they are organized in the physical network

Advantages of subnetting

Virtual LANs

- Allow scattered users to be logically grouped together:
  - Even if attached to different switches
- Reduce network traffic and provide a degree of security similar to subnetting
- Can isolate sensitive data to VLAN members
- Prevent direct communication between servers, which can bypass firewall or IDS inspection.

Remote Access

- Working away from the office commonplace today
- Strong security for remote workers must be maintained
- Remote access provides remote users with the same access and functionality as local users through a VPN or dial-up connection

Summary

- Standard network security devices provide a degree of security
  - –Hubs, switches, router, load balancer
- Hardware devices specifically designed for security give higher protection level
  - –Hardware-based firewall, Web application firewall
- Proxy server intercepts and processes user requests
- Virtual private network uses unsecured public network and encryption to provide security
- Intrusion detection system designed to detect attack as it occurs
- Network technologies can help secure a network
  - –Network address translation
  - –Network access control
- Methods for designing a secure network
  - –Demilitarized zones - Subnetting
  - –Virtual LANs - Remote Access