CSF3404 Cyber Security

Chapter 5
Implementing Network Security

Lecturer:
Waheed Ghanem
Fakhrul Adli bin Mohd Zaki
Aalim Rozli

Faculty of Ocean Engineering Technology and Informatics,
Universiti Malaysia Terengganu

Configure Security Parameters on Network Devices and Technologies

UMT
We lead

- Configure security parameters on the network devices and technologies.

- Understanding the devices and technologies that make the network function.

- How the network devices and technologies operate.

- Manage security settings for specific devices that are used within a network.

Network Components

- **Device:** Any piece of hardware such as a computer, server, printer, or smartphone.
- **Media:** Connects devices to the network and carries the data between devices.
- **Network adapter:** Hardware that translates the data between the network and a device.
- **Network operating system:** Software that controls network traffic and access to network resources.
- **Protocol:** Software that controls network communications using a set of rules.

Network Devices

- Different types of internetwork devices provide different levels of connectivity and security between network interconnections and network segments.

- **Router:**
  - A device that connects multiple networks that use the same protocol.
  - Determine the most efficient path for data to take.
  - Filter network traffic based on other criteria.
  - Most routers will not forward broadcast network traffic.
- **Switch:**
  - Has multiple network ports and combines multiple physical network segments into a single logical network.
  - It controls network traffic on the logical network by creating dedicated or switched.
  - Standard switches generally forward broadcast to all ports on the switch.
  - Some switches can perform routing functions based on protocol addresses.

Network Devices

- **Proxy server:**
  - Isolate internal networks from the Internet by downloading and storing Internet files on behalf of internal clients.
  - Generates a completely new request packet using itself as the source.
  - Providing security.
  - Improve client response time.
  - Reduce Internet traffic by providing frequently used pages to clients from a local source.
  - A proxy server can also include Network Address Translation (NAT) and firewall functionality.
- **Firewall:**
  - Any software or hardware device that protects a system or network by blocking unwanted network traffic.
  - Firewalls generally are configured to stop suspicious or unsolicited incoming traffic.
  - The types of traffic blocked are configured using predefined rule sets.
  - Information about the incoming or outgoing connections can be saved to a log.
  - Used for network monitoring or hardening purposes.

Network Devices

- **Firewall:** There are three common types of firewalls:
  - **Host or personal firewalls** are installed on a single computer and are used to secure most home computers.
  - **Network-based firewalls** are dedicated hardware/software combinations that protect all the computers on a network behind the firewall.
  - **Web application-based firewalls** are specifically deployed to secure an organization's web-based applications and transactions from attackers.
- **Load balancer:**
  - A network device that performs load balancing as its primary function.
  - Is the practice of spreading out the work among the devices in a network.
  - More resources are available and data is processed faster.
  - All the devices in the network perform more efficiently.
  - A dedicated program or hardware device is used to provide the balancing service.
- **All-in-one security appliance:**
  - A single network security device is used to perform a number of security functions to secure a network.
  - Most devices will contain firewall, intrusion prevention, load balancing, filtering, and reporting functionalities.

Multifunction Network Devices

- Is any piece of network hardware that is meant to perform more than one networking task without having to be reconfigured.

- Is a combination switch, router, Dynamic Host Configuration Protocol (DHCP) server, and firewall that is installed in many small offices or home networks.

Application Aware Devices

- Is a network device that manages the information of any applications that interface with it.
- This information includes the state of applications and the resources they require.
- To more efficiently designate resources across a network.
- Examples of application-aware devices include firewalls, intrusion detection systems, intrusion prevention systems, and proxies.

Router Discovery Protocols

- The language that routers use to communicate with each other.
- **Routing Information Protocol (RIP):**
  - Is a simple distance-vector protocol.
  - Is easy to configure and works well inside simple autonomous systems.
  - Is best deployed in small networks with only a few routers in an environment that does not change much.
  - Most equipment that supports RIP costs less than equipment that supports more complicated routing protocols.
- **RIPv2:**

  RIPv2 enhances RIP by supporting the following features:
  - **Next Hop Addressing:** Includes Internet Protocol (IP) address information in routing tables for every router in a given path.
  - **Authentication:** Enables password authentication and the use of a key.
  - **Subnet mask:** Supports more subnets and hosts on an internetwork by supporting Variable Length Subnet Masks (VLSMs).
  - **Multicast packet:** Decreases the workload of non–RIPv2 hosts by communicating only with RIPv2 routers.
  - RIPv2 packets use **224.0.0.9** as their **IP multicast address**.

Router Discovery Protocols

- **Interior Gateway Routing Protocol (IGRP):**
  - This is a distance-vector routing protocol developed by Cisco as an improvement over RIP and RIPv2.
  - It was designated as a protocol best deployed on interior routers within an autonomous system (AS).
- **Enhanced Interior Gateway Routing Protocol (EIGRP):**
  - This is a proprietary routing protocol developed by Cisco and is considered a hybrid protocol.
  - It includes features that support **VLSM** and classful and classless subnet masks.
  - Reduce convergence times and improve network stability during changes.

Network Analysis Tools

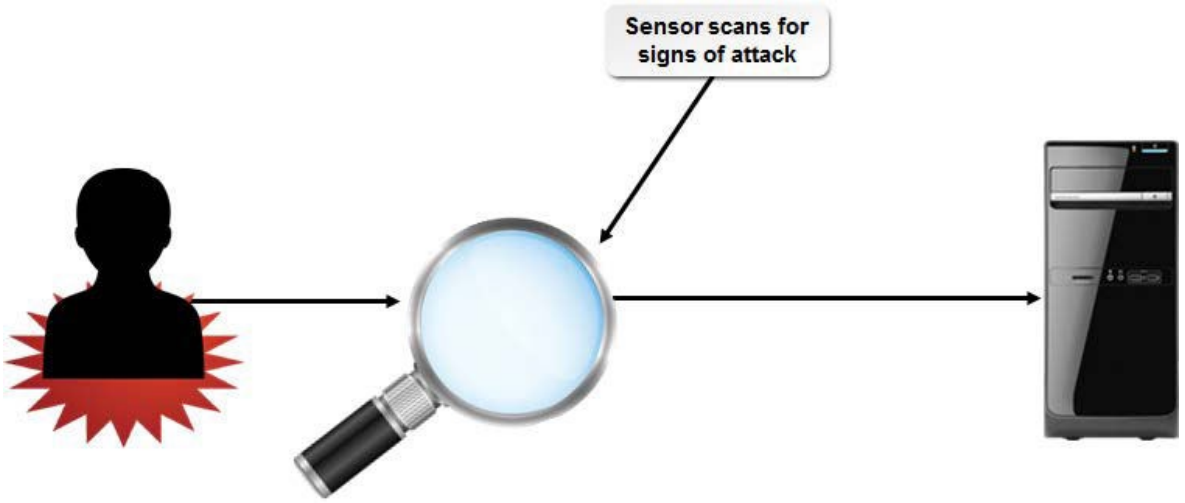
- **Sniffer:**
  - A device or program that monitors network communications on the network wire or across a wireless network and captures data.
  - Used to gather information passed through a network.
  - To selectively record specific types of transactions based on devices, protocols, or applications used.

- **Protocol analyzer:**
  - Also known **as a network analyzer**.
  - It is a type of diagnostic software.
  - It can examine and display data packets that are being transmitted over a network.
  - Protocol analyzers can gather all the information passed through a network.
  - Selectively record certain types of transactions based on various filtering mechanisms.
  - It is possible to gather information on all or just part of the network.
  - Traffic can be captured on one wireless channel at a time.

Intrusion Detection System

- IDS is a detection control system that scans, audits, and monitors the security infrastructure for signs of attacks in progress.
- IDS software can also analyze data and alert security administrators to potential infrastructure problems.
- An IDS can comprise a variety of hardware sensors, intrusion detection software, and IDS management software.
- An IDS can be set up to use host-based detection.
- It monitors a computer system for unexpected behavior or drastic changes to the system's state.

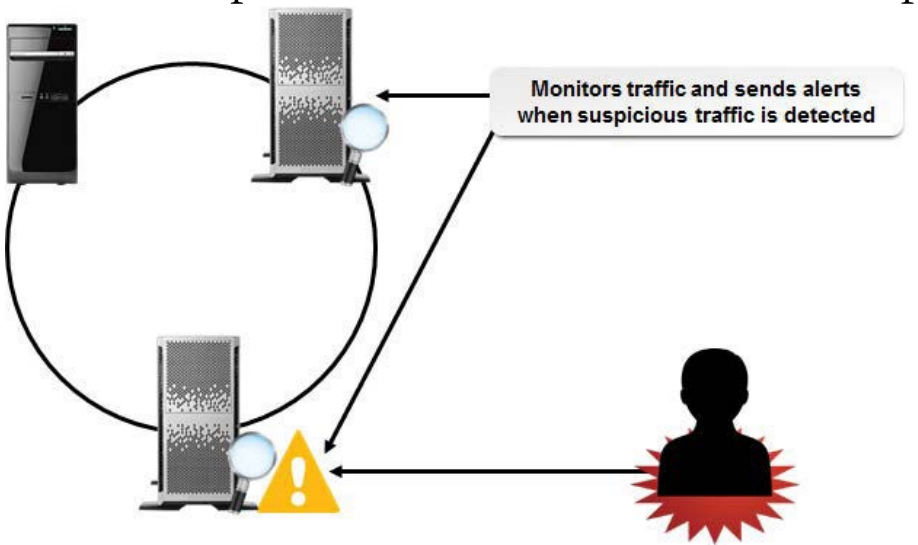
An IDS scanning for signs of an intrusion



Network Intrusion Detection System

- Is a type of IDS that primarily uses passive hardware sensors to monitor traffic on a specific segment of the network.
- It cannot analyze encrypted packets.
- It can sniff traffic and send alerts about anomalies or concerns.
- It is rogue machine detection.
- A rogue machine is any unknown or unrecognized device that is connected to a network, often with malicious intent.
- By using various techniques to scan for suspicious behavior, an NIDS can spot a rogue machine.

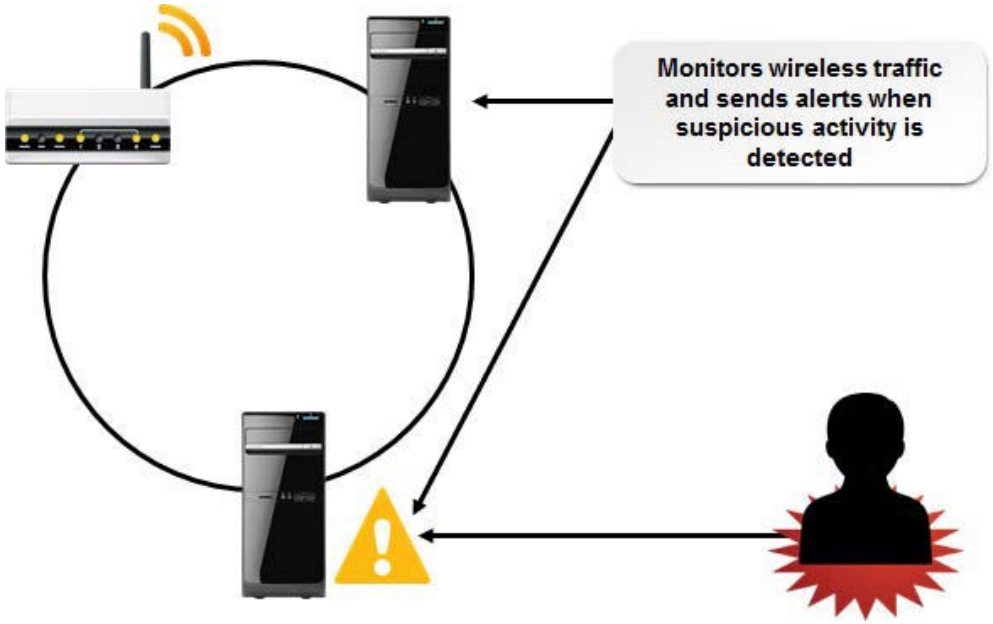
A NIDS Scanning for Suspicious Activity on a Network



Wireless IDS

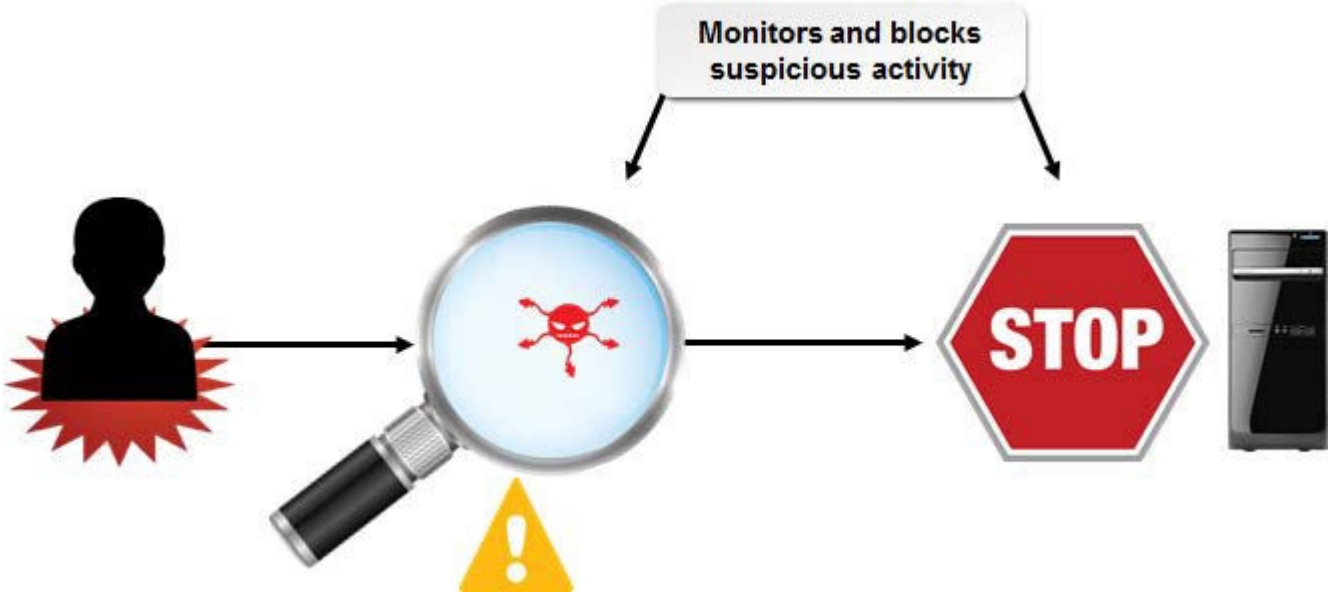
- Is a type of NIDS that scans the radio frequency spectrum for possible threats to the wireless network.
- Primarily rogue access points.
- A WIDS usually compares the Media Access Control (MAC) address of a device that acts as an access point to known addresses.
- If it doesn't find a match, it gives out an alert.
- MAC address spoofing can complicate the efficacy of a WIDS.

A Wireless IDS



Intrusion Prevention System

- An IPS has the monitoring capability of an IDS.
- Actively works to block any detected threats.
- To take the extra steps necessary to prevent an intrusion into a system.

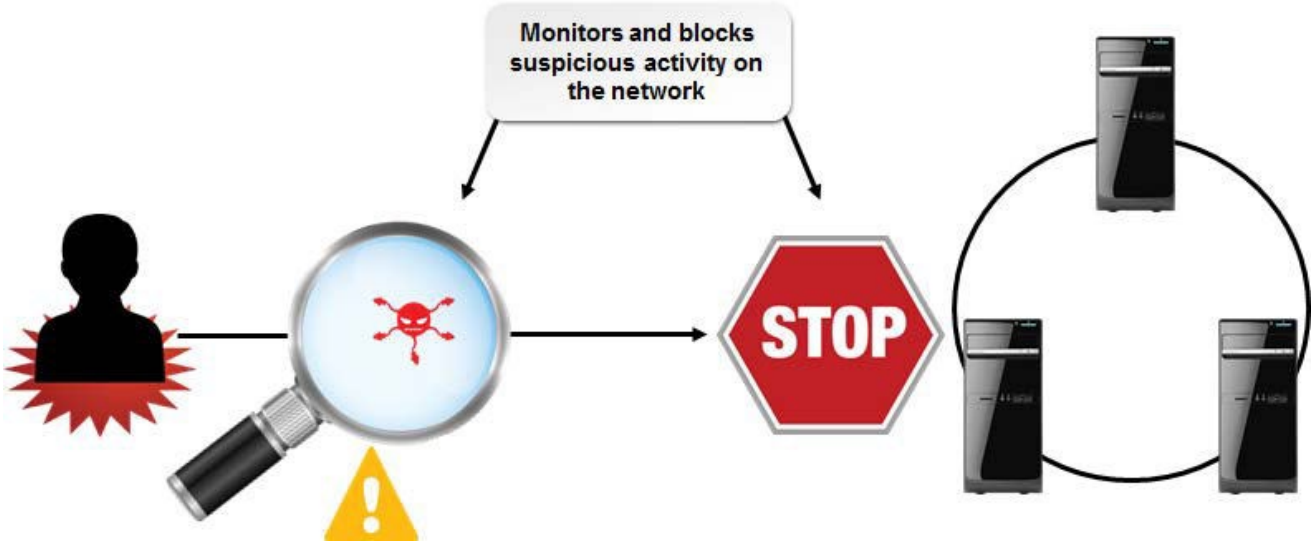


An IPS Blocking an Intrusion Attempt

Network Intrusion Prevention System

- A (NIPS) monitors the suspicious network and system traffic and reacts in real-time to block it.
- Blocking may involve dropping unwanted data packets or resetting the connection.
- It can regulate traffic according to specific content.
- It examines packets as they travel through the IPS.
- This is in contrast to the way a firewall behaves, which blocks IP addresses or entire ports.

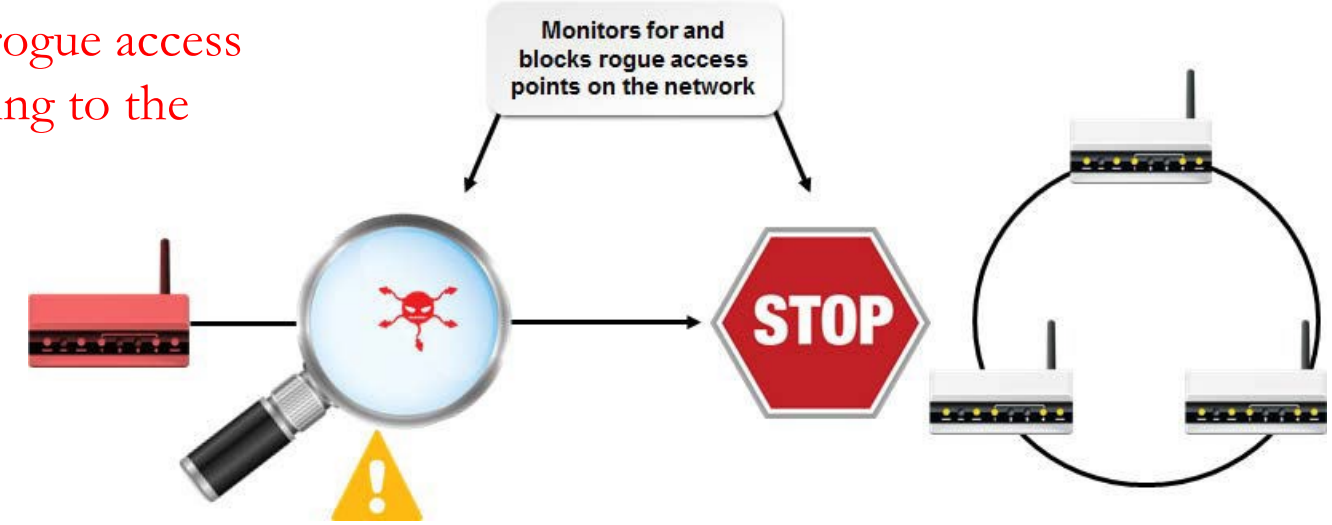
A NIPS Blocking Suspicious Activity on a Network



Wireless IPS

- Is a type of NIPS that scans the radio frequency spectrum for possible threats to the wireless network.
- Primarily rogue access points.
- It can actively block this malicious traffic.
- It can drop undesired packets in real-time as they come in through the network.

A WIPS blocking a rogue access point from attaching to the network



Types of Network Monitoring Systems

- Various methods of network monitoring:
  - **Behavior-based monitoring:**
    - Detects changes in normal operating data sequences and identifies abnormal sequences.
    - They have no performance baseline or acceptable traffic pattern defined.
    - Initially, It will report all traffic as a threat.
    - Over time, it learns which traffic is allowed and which is not with the assistance of an administrator.
  - **Signature-based monitoring:**
    - It uses a predefined set of rules provided by a software vendor to identify traffic that is unacceptable.
  - **Anomaly-based monitoring:**
    - It uses a database of unacceptable traffic patterns identified by analyzing traffic flows.
    - It is dynamic and creates a performance baseline of acceptable traffic flows during its implementation process.
  - **Heuristic monitoring:**
    - It is set up using known best practices and characteristics in order to identify and fix issues within the network.

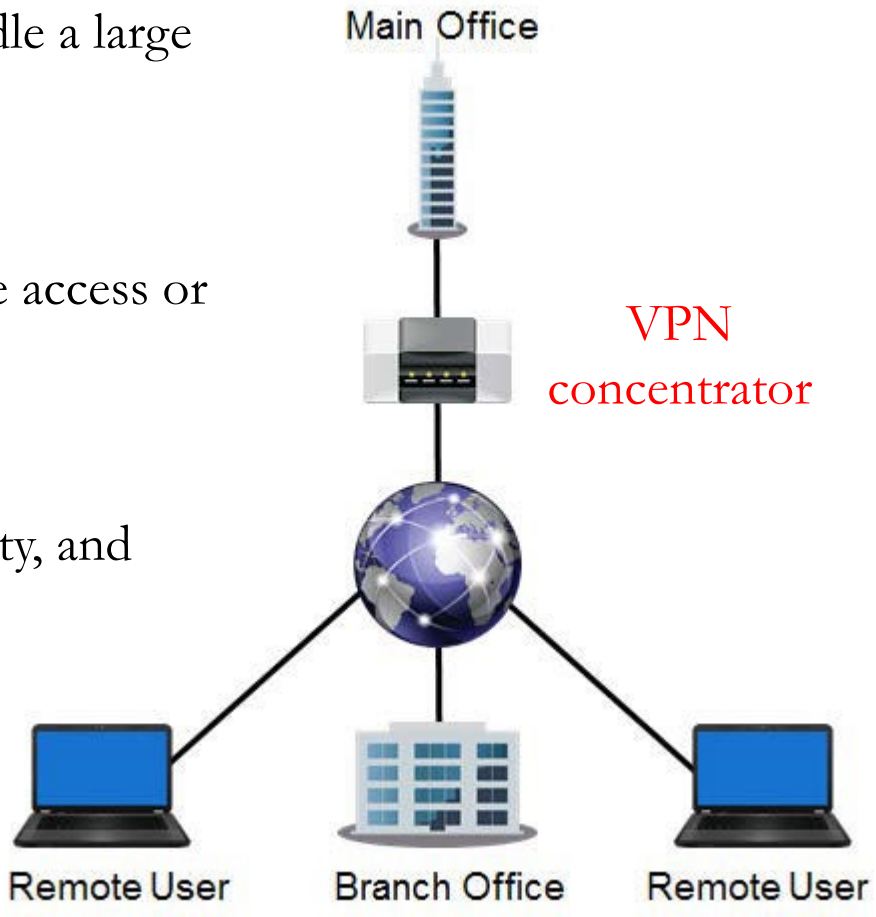
Virtual Private Network

- A VPN is a private network that is configured by tunneling through a public network, such as the Internet.
- VPNs provide secure connections between endpoints, such as routers, clients, or servers.
- It uses tunneling to encapsulate and encrypt data.
- Special VPN protocols are required to provide the VPN tunneling, security, and data encryption services

Using a VPN to tunnel through the Internet
and access a private server

VPN Concentrator

- It is a single device that incorporates advanced encryption and authentication methods in order to handle a large number of VPN tunnels.
- It is geared specifically toward secure remote access or site-to-site VPNs.
- It provides high performance, high availability, and impressive scalability.



Web Security Gateways

- It is a utility used primarily to intentionally block internal Internet access to a predefined list of websites or categories of websites.
- The utility is configured by administrators to deny access to a specified list of Uniform Resource Locators (URLs).
- This type of software can also be used for tracking and reporting a business' Internet usage and activity.
- It can provide a number of functions, including
  - URL filtering, which is based on blacklist settings;
  - Malware inspection, which is used to identify infected packets;
  - Content inspection, which is used to scan the contents of a packet for abnormalit

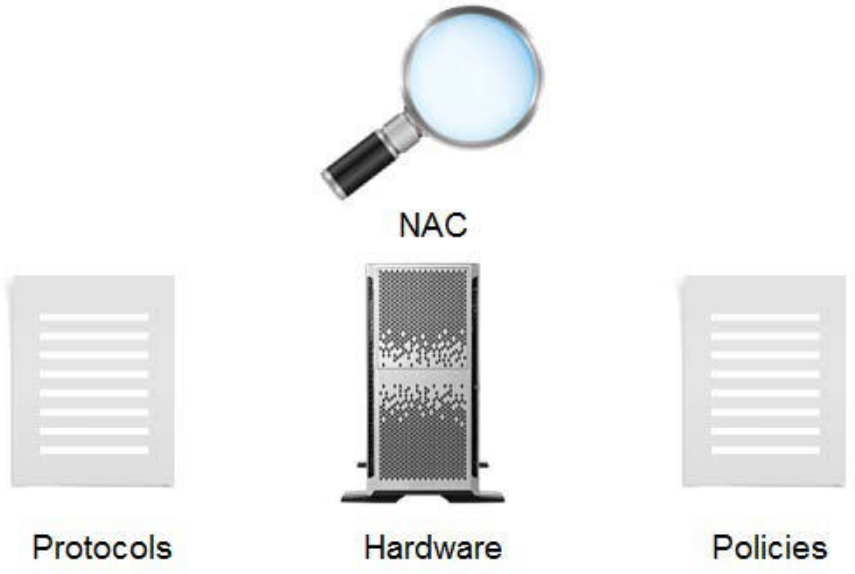
Network Design Elements and Components

- Many factors can go into properly setting up and securing a network from common threats and vulnerabilities.

- But understanding;
  - How the design elements and components work within that network enables you to easily manage and make the necessary security-related adjustments.

Network Access Control

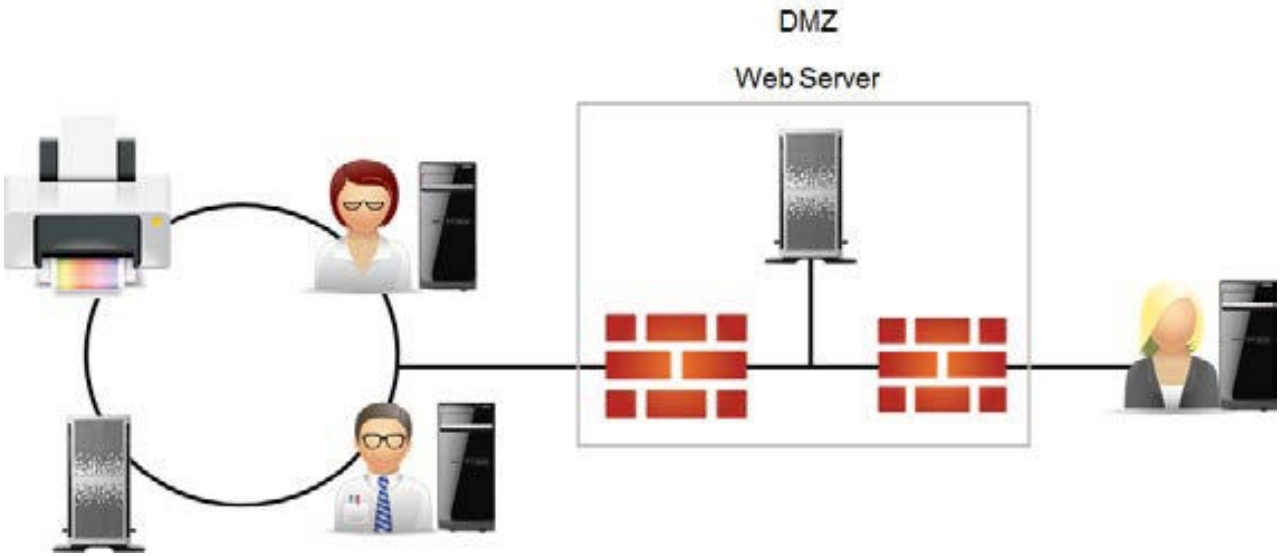
- Is a general term for the collected protocols, policies, and hardware that govern access on device network interconnections.
- NAC provides an additional security layer that scans systems for conformance and allows or quarantines updates to meet policy standards.
- Security professionals will deploy a NAC policy according to an organization's needs based on three main elements:
  - ✓ Authentication method
  - ✓ Endpoint vulnerability assessment
  - ✓ Network security enforcement



- Security professionals must determine where NAC will be deployed within their network structure.

Demilitarized Zone

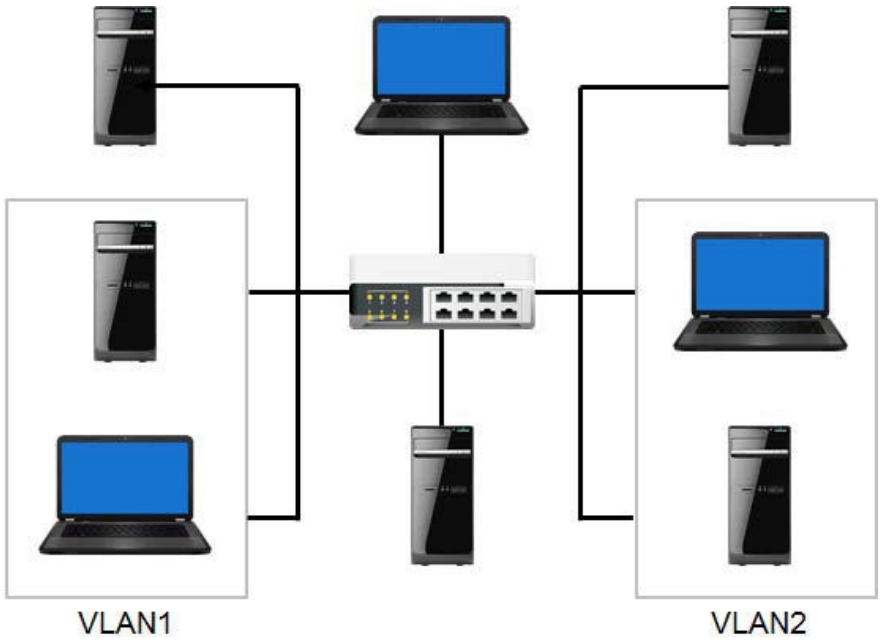
- A DMZ is a small section of a private network that is located between two firewalls and made available for public access.
- A DMZ enables external clients to access data on private systems, such as web servers, without compromising the security of the internal network as a whole.
- The external firewall enables public clients to access the service.
- The internal firewall prevents them from connecting to protected internal hosts.



Virtual Local Area Network

- A VLAN is a point-to-point logical network that is created by grouping selected hosts together, regardless of their physical location.
- A VLAN uses a switch or router that controls the groups of hosts that receive network broadcasts.
- VLANs can provide network security by enabling administrators to segment groups of hosts within the larger physical network.

A switch segmenting hosts on a VLAN



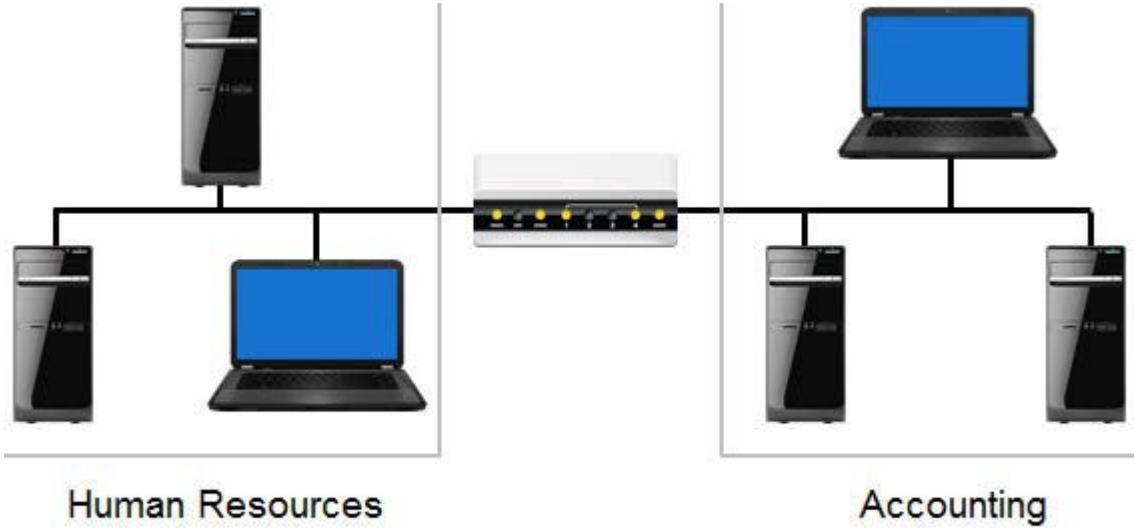
VLAN Vulnerabilities

- Give attackers the opportunity to redirect packets from one VLAN to another and to capture those packets and the data they contain.
- Some VLAN switch configurations can also be open to other attacks such as Denial of Service (DoS), traffic flooding, and MAC address spoofing.
- Correctly configuring a VLAN implementation can eliminate these types of attacks.

Subnetting

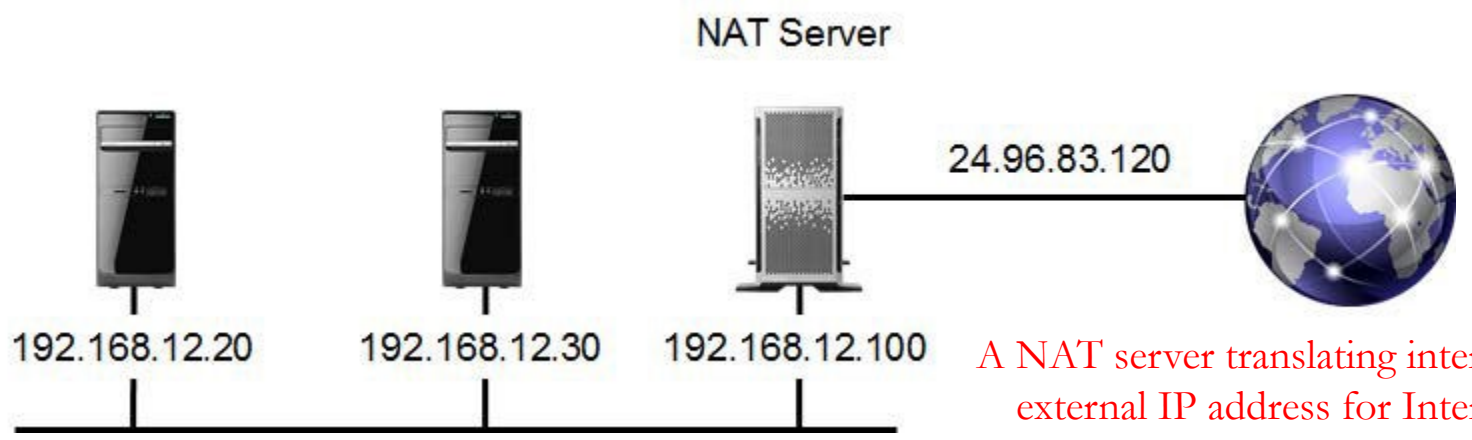
- Is a network design element that is used to divide a large network into smaller logical networks.
- Each node is configured with an IP address and a subnet address in order to segment a network into subnetworks and to create a routing structure.
- Create logical groups of network devices based on an addressing scheme.
  - ✓ Data flow and security measures can be managed more easily on a smaller scale than on a large network.

A subnet that divides a network based on different departments in a company



Network Address Translation

- Is a simple form of Internet security that conceals internal addressing schemes from the public Internet.
- A router is configured with a single public IP address on its external interface and a private one.
- Non-routable address on its internal interface.
- A NAT service translates between the two addressing schemes.
- Packets sent to the Internet from internal hosts all appear as if they came from a single IP address.
- Preventing external hosts from identifying and connecting directly to internal systems.



A NAT server translating internal IP addresses to an external IP address for Internet communication

Remote Access

- It is the ability to connect to network systems and services from an offsite or remote location.

- It is a method that enables authorized users to access and use systems and services through a secure Internet connection.

- Remote access is often most secure when users are able to connect through a VPN.

An employee accessing company data through a remote connection

Telephony

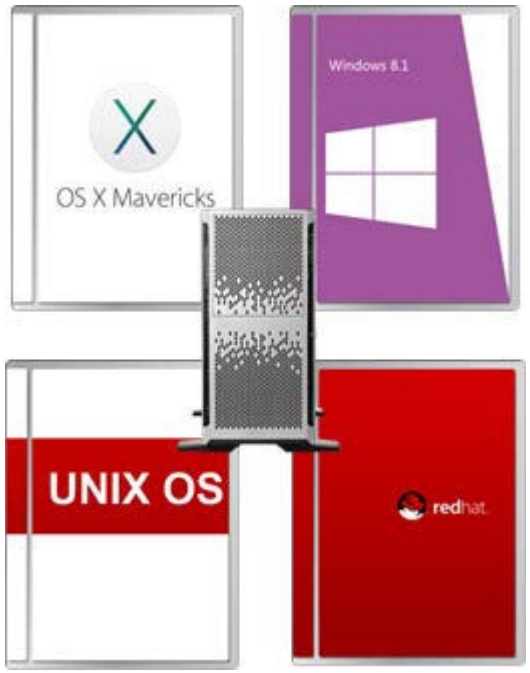
- Telephony provides voice communications through devices over a distance.

- Modern networks are designed to handle more than just the traditional networking components.

- Common telephony components include:
  - ✓ Voice over Internet Protocol (VoIP) implementations, in which voice traffic is transmitted over the IP network.
  - ✓ Private branch exchange implementations.
  - ✓ Computer telephony integration (CTI), which incorporates telephone, email, web, and computing infrastructures.

Virtualization

- Virtualization technology separates computing software from the hardware it runs on via an additional software layer.
- This enables a great deal of additional flexibility and increases hardware utilization by running multiple operating systems on a single computer.
- Virtualization allows hardware resources in an organization to be pooled and leveraged as part of a virtual infrastructure.
- Increasing available processing and storage capacity.
- Virtualization has many uses in the modern IT environment:
  - ✓ Running multiple operating systems on one computer.
  - ✓ Separating software applications within a single operating system to prevent conflicts.
  - ✓ Increasing utilization of processing and storage resources throughout the organization by creating a virtual infrastructure.



Running multiple operating systems on one computer

Cloud Computing

- Cloud computing is a method of computing that involves real-time communication over large networks to provide the resources, software, data, and media needs of a user, business, or organization.
- This method of computing usually relies on the Internet to provide computing capabilities that a single machine cannot.
- It refers to the resources that are available on a particular network.
- This could include business websites, consumer websites, storage services, IT-related services, file editing applications, and social networking websites.
- Can access and manage your data and applications from any computer anywhere in the world.
- The storage method and location are hidden.

A user accessing various resources from a cloud computing architecture over the Internet

Cloud Computing Deployment Models

- **Private:**
  - Private cloud services are usually distributed by a single company or other business entity over a private network.
- **Public:**
  - Public cloud computing is done over the Internet by organizations that offer their services to general consumers.
- **Community:**
  - When multiple organizations share ownership of a cloud service, they are deployed as a community cloud.
  - To pool resources for a common concern.
- **Hybrid:**
  - Hybrid cloud computing combines two or more deployment methods into one entity.
  - It offers computing services to the general public.

Cloud Computing Service Types

- **Software:**
  - ✓ Software as a Service (**SaaS**) refers to using the cloud to provide applications to users.
  - ✓ Examples include Microsoft® Office 365™, Salesforce®, and Gmail™.
- **Platform:**
  - ✓ Platform as a Service (**PaaS**) refers to using the cloud to provide virtual systems, such as operating systems, to customers.
  - ✓ Examples include Oracle® Database, Microsoft Windows Azure™ SQL Database, and Google App Engine™.
- **Infrastructure:**
  - ✓ Infrastructure as a Service (**IaaS**) refers to using the cloud to provide access to any or all infrastructure needs a client may have.
  - ✓ Examples include Amazon® Elastic Compute Cloud®, Microsoft Windows Azure Virtual Machines, and OpenStack™.

Open Systems Interconnection model

- It is a way to abstract how a network is structured based on how it communicates with other elements in the network, similar to the Transmission Control Protocol/Internet Protocol (TCP/IP) model.
- These elements are divided into seven discrete layers with a specific order.
    1. Physical
    2. Data link
    3. Network
    4. Transport
    5. Session
    6. Presentation
    7. Application
- The main purpose of the OSI model is to encourage seamless and consistent communication between different types of network products and services.

Open Systems Interconnection model

1. **Physical:**
   - Defines connections physical transmission media
2. **Data link:**
   - Provides a link between two directly connected nodes, as well as detecting and fixing errors in the physical layer.
3. **Network:**
   - Provides the protocols for transferring data from one node to another in a system with multiple nodes with unique addresses (a network).
4. **Transport:**
   - Controls the reliability of data transmission between nodes on a network for the benefit of the higher layers.
5. **Session:**
   - Controls the connections between computers through check pointing so that connections, when terminated, may be recovered
6. **Presentation:**
   - Transforms data into a format that can be understood by the programs in the application layer above it.
7. **Application:**
   - Allows client interaction with software by identifying resource and communication requirements.

Internet Protocol

1. Transmission Control Protocol/Internet Protocol (TCP/IP)
   - ✓ It is a routable network protocol suite that enables computers to communicate over all types of networks.
   - ✓ TCP/IP is the native protocol of the Internet and is required for Internet connectivity.
2. IP version 4 (IPv4)
   - ✓ It uses a 32-bit number assigned to a computer on a TCP/IP network.
   - ✓ Some of the bits in the address represent the network segment; the other bits represent the computer.
   - ✓ The 32-bit IPv4 address is usually separated by dots into four 8-bit octets, 10101100.00010000.11110000.00000001.
   - ✓ Each octet is converted to a single decimal value.
3. IP version 6 (IPv6)
   - ✓ It increases the available pool of IP addresses by implementing a 128-bit binary address space.
   - ✓ IPv6 is separated by colons into eight groups of four hexadecimal digits: 2001:0db8:85a3:0000:0000:8a2e:0370:7334.
4. Dynamic Host Configuration Protocol (DHCP):
   - ✓ It is used to automatically assign IP addressing information to IP network computers.
   - ✓ Most IP systems obtain addressing information dynamically from a central DHCP server.
   - ✓ A router configured to provide DHCP functions.

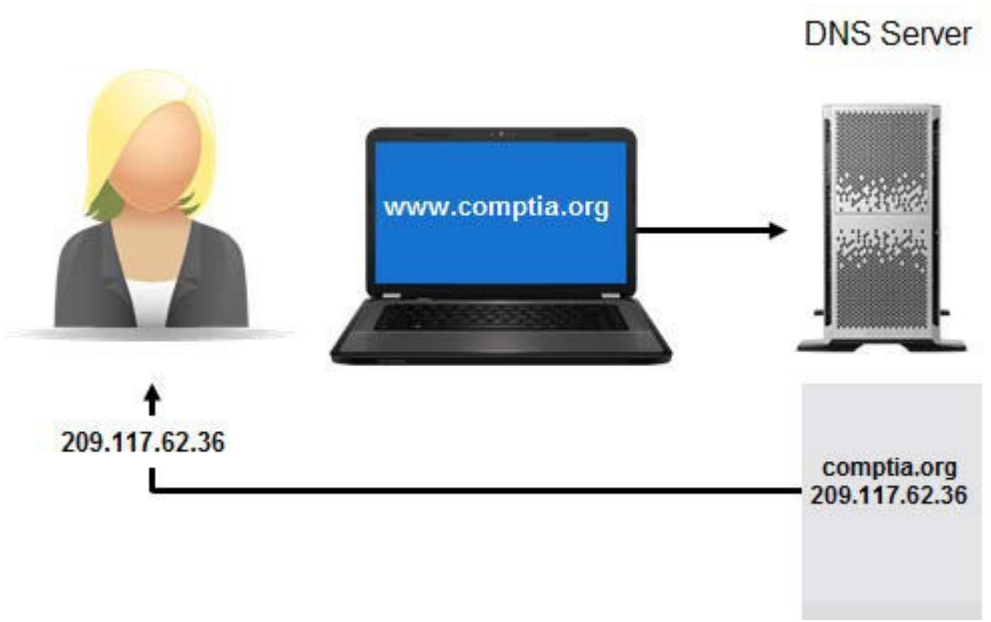
Domain Name System

1. DSN is the primary name resolution service on the Internet and private IP networks.

2. DNS is a hierarchical system of databases that map computer names to their associated IP addresses.

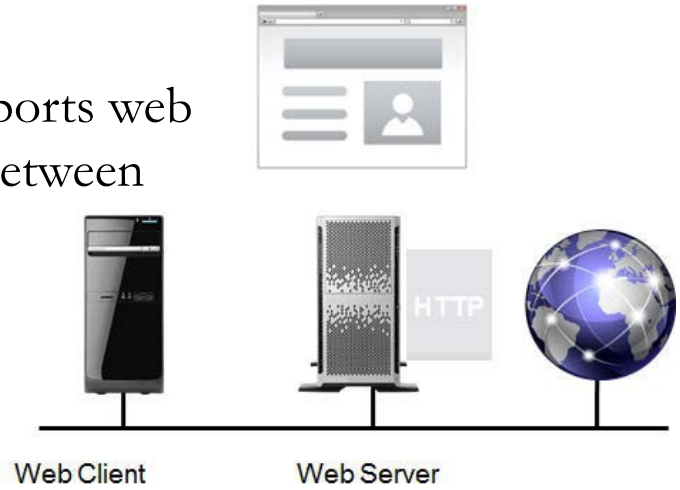
3. DNS servers store, maintain, and update databases and respond to DNS client name resolution requests to translate human-intelligible host names to IP addresses.

4. The DNS servers on the Internet work together to provide global name resolution for all Internet hosts.



Hypertext Transfer Protocol

- HTTP is the TCP/IP protocol that enables clients to connect to and interact with websites.
- HTTP is responsible for transferring the data on web pages between systems.
- HTTP defines how messages are formatted and transmitted.
- What actions web servers and the client's browser should take in response to different commands.
- HTTPS is a secure version of HTTP that supports web commerce by providing a secure connection between a web browser and a server.
- HTTPS uses SSL/TLS to encrypt data.



HTTP translating a client request to access Internet resources using a web browser

Web Server Security

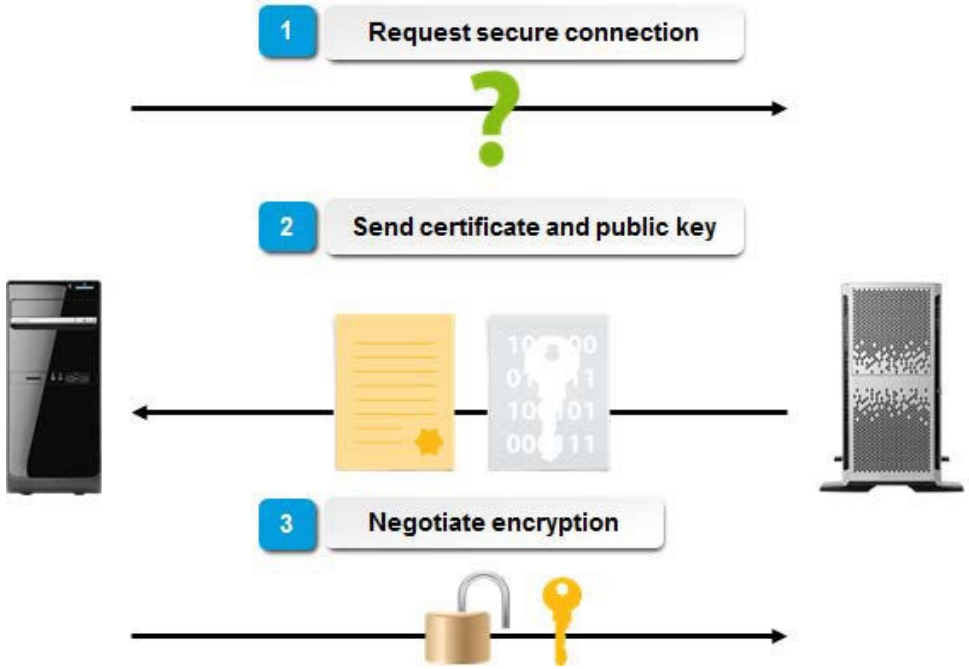
UMT
We lead

- Hackers primarily try to break into the web servers of organizations.
- If the web server is breached.
  - Then the hacker gets direct access to all the sensitive data stored on the web servers.
- Securing web servers remains one of the toughest challenges security administrators face.
- To effectively secure web servers:
  - Remove unnecessary services running in the background.
  - Avoid remote access to web servers.
  - Store web applications, website logs that contain user information, and other related files on another, secured, drive.
  - Install security patches regularly.
  - Delete or disable unused user accounts.
  - Use the appropriate security tools.
  - Use port scanners to scan the web servers regularly.

Secure Sockets Layer & Transport Layer Security

- SSL & TSL are security protocols that combine digital certificates for authentication with public key data encryption.
- These protocols protect sensitive communication by using a secure, encrypted, and authenticated channel over a TCP/IP connection.
- A web client that supports SSL or TLS can connect securely to an SSL or TLS enabled server.
- SSL/TLS is a server-driven process.

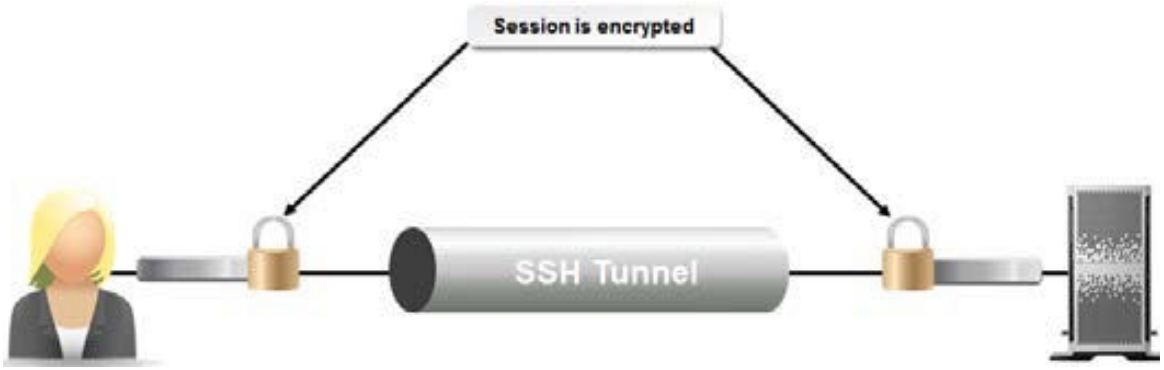
- **TLS vs. SSL**
  - SSL is a predecessor of TLS.
  - The latest versions of TLS are more secure than SSL.
  - Very few websites currently implement them.



An SSL/TLS handshake securing a web browsing session

Secure Shell

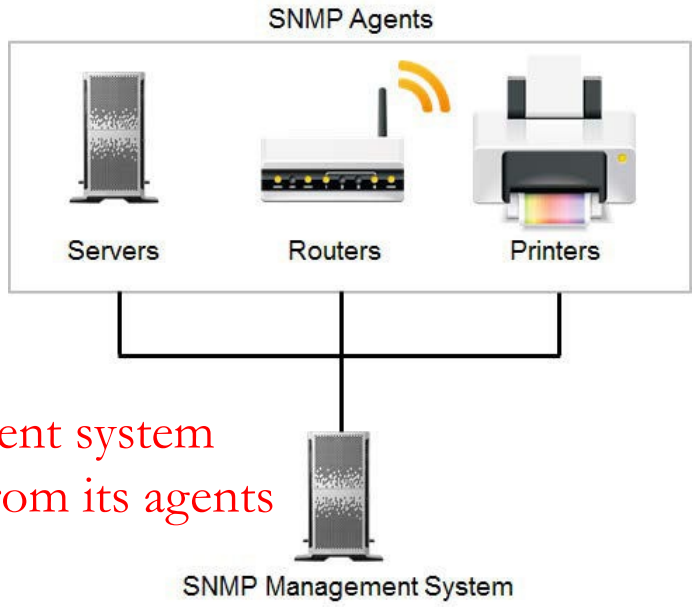
- SSH is a protocol used for secure remote login and secure transfer of data.
- SSH consists of a server and a client.
- Most SSH clients also implement login terminal-emulation software to open secure terminal sessions on remote servers.
- SSH is the preferred protocol for working with File Transfer Protocol.
- Microsoft Windows does not offer native support for SSH.



Using an SSH tunnel to
remotely access a web server

Simple Network Management Protocol

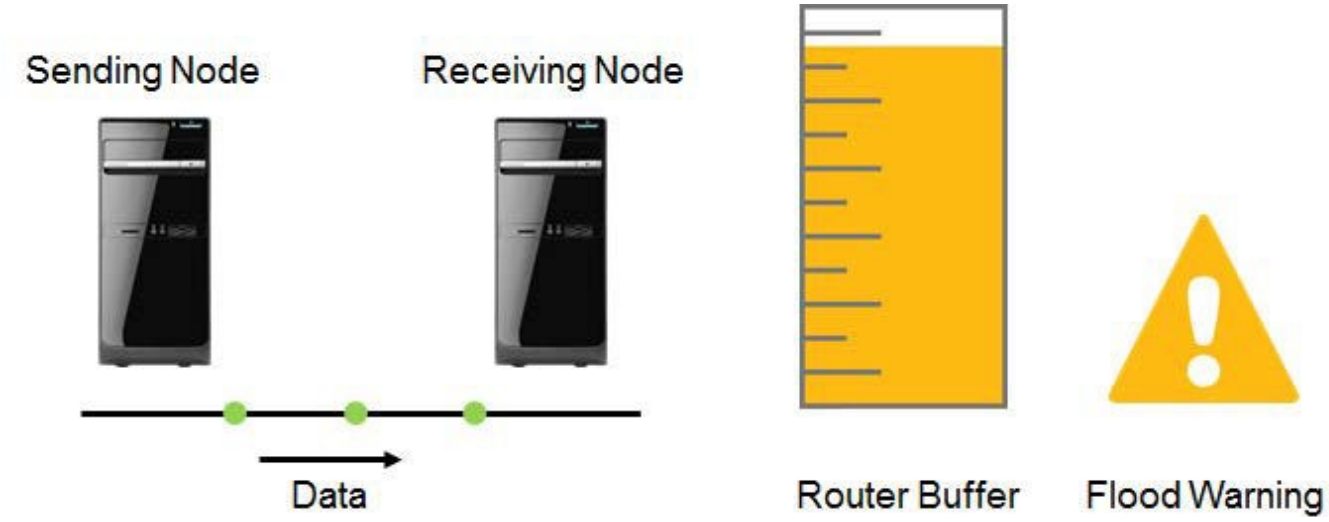
- SNMP is a service used to collect information from network devices for diagnostic and maintenance purposes.
- SNMP includes two components:
  - Management systems.
  - Agent software: which is installed on network devices such as servers, routers, and printers.
- The agents send information to an SNMP manager.
- The SNMP manager can then notify an administrator of problems and it run a corrective program or script, store the information for later review.
- Ask the agent about a specific network device.



An SNMP management system receiving information from its agents

Internet Control Message Protocol

- ICMP is an IP network service that reports on connections between two hosts.
- It is often used for simple functions, such as the ping command that checks for a response from a particular target host.
- Attackers can use redirected ICMP packets in two ways:
  - To flood a router and cause a DoS attack by consuming resources (Smurf attack).
  - To reconfigure routing tables by using forged packets.



A Smurf attack flooding nodes on a network using ICMP

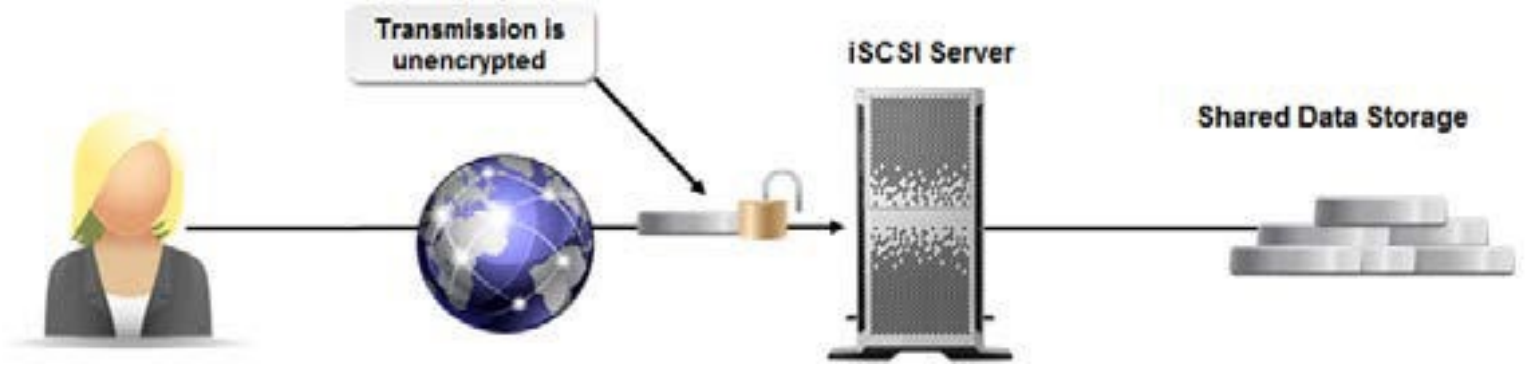
Internet Protocol Security

- IPSec is a set of open, non-proprietary standards that you can use to secure data as it travels across the network or the Internet.
- IPSec uses an array of protocols and services to provide data authenticity and integrity, anti-replay protection, non-repudiation, and protection against eavesdropping and sniffing.
- IPSec operates at the Network layer of the TCP/IP model, so the protocol is not application dependent.

IPSec policy securing a connection between two computers

Internet Small Computer System Interface

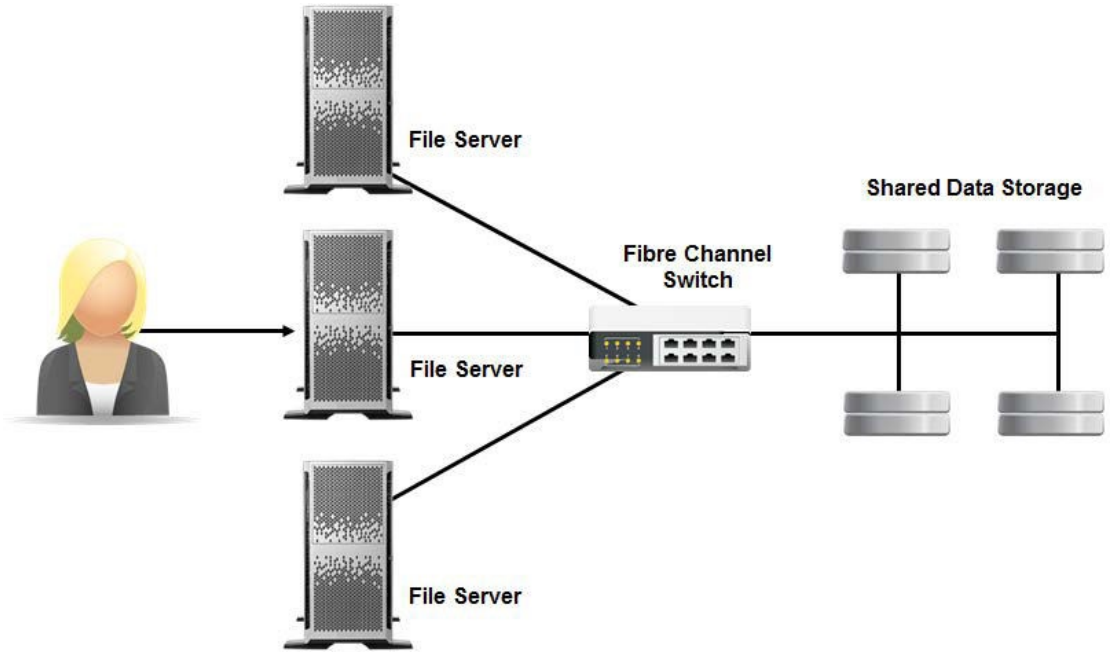
- iSCSI is a protocol implementing links between data storage networks using IP.
- This protocol is designed to extend across wide area networks without needing any new infrastructure.
- Users can enter commands and remotely manage data servers from great distances, and iSCSI can centralize data storage.
- The information is not bound to individual servers.
- An iSCSI does not inherently provide encryption during transmission.



A client connecting to iSCSI storage facilities over the Internet

Fibre Channel

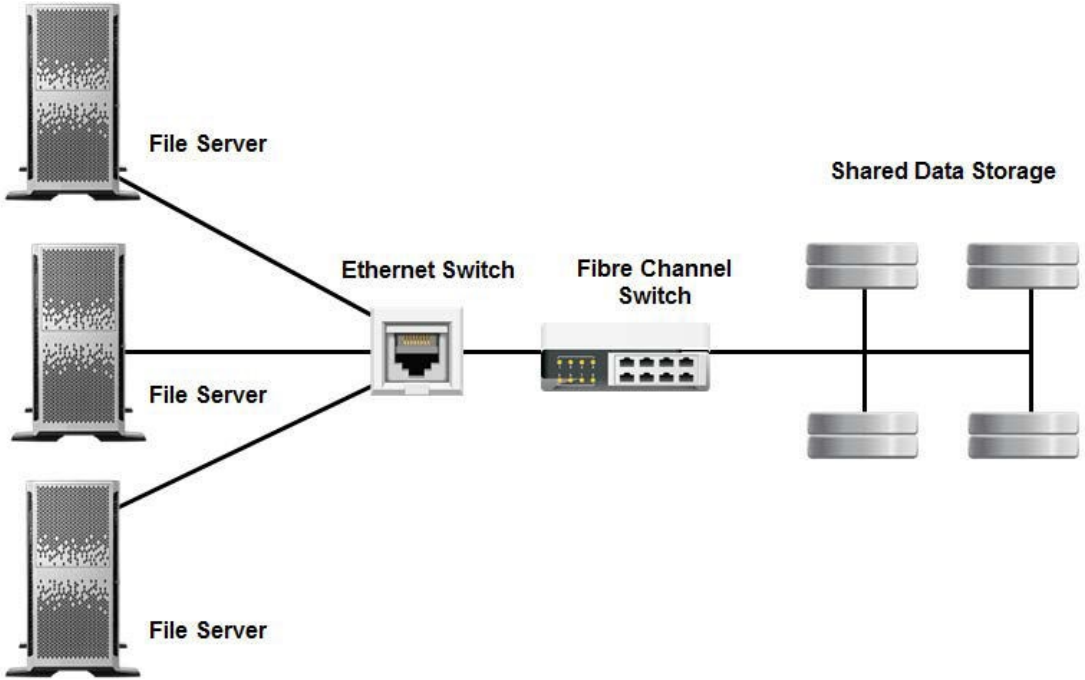
- Fibre Channel is a protocol designed to link data storage across a network and provide remote access over large distances.
- Fibre Channel requires installing special-purpose cabling in place of existing infrastructure.
- Fibre Channel is a more expensive option.
- It provides greater performance and reliability.
- Implementing security controls like encryption and authentication is difficult on Fiber Channel.



Accessing data storage through Fibre Channel

Fibre Channel over Ethernet

- FCoE allows traditional Fibre Channel protocols to use high-speed Ethernet networks to transmit and store data.
- This protocol decreases the infrastructure cost of cabling.
- It reduces the amount of physical hardware required such as network interface cards and switches required.
- Power and cooling costs may be reduced.
- FCoE is subject to much of the same security pitfalls as traditional Fibre Channel.
- Should not be considered a viable alternative as far as security is concerned.



Fibre Channel implemented over Ethernet

Telnet

- Telnet is a network protocol that allows a client to initiate remote command access to a host over TCP/IP.
- The client runs a Telnet program that can establish a connection with a remote server.
- Grant the client a virtual terminal into the server.
- Telnet is not recommended today, as it leads to major security vulnerabilities.
- The Telnet protocol is not encrypted. Man-in-the-middle attacks are also relatively easy.
- Telnet does not require any sort of authentication between client and host.

Network Basic Input Output System

UMT
We lead

- NetBIOS is an interface that allows applications to properly communicate over different computers in a network.

- NetBIOS has three basic functions:
  - ✓ Communication over sessions
  - ✓ Connectionless communication using datagrams
  - ✓ Name registration

- Attackers can exploit NetBIOS by obtaining information about a system, including registered name, IP addresses, and operating system/applications used.

- To harden NetBIOS against an attack, you should implement strong password policies, limit root access on a network share, and disable null session capability.

File Transfer Protocols

- File Transfer Protocol:
  - ✓ This protocol enables the transfer of files between a user's workstation and a remote host.
- Simple File Transfer Protocol:
  - ✓ This protocol was an early unsecured file transfer protocol that has since been declared obsolete
- Trivial File Transfer Protocol:
  - ✓ This is a very limited protocol used primarily as an automated process of configuring boot files between machines
- FTP over SSH:
  - ✓ It is a secure version of FTP that uses an SSH tunnel as an encryption method to transfer, access, and manage files.
- Secure Copy Protocol:
  - ✓ This protocol uses SSH to securely transfer computer files between a local and a remote host, or between two remote hosts.
- File Transfer Protocol Secure:
  - ✓ Combines the use of FTP with additional support for SSL/TLS.

Ports and Port Ranges

- A port is the endpoint of a logical connection.
- Client computers connect to specific server programs through a designated port.
- All ports are assigned a number in a range from 0 to 65,535.
- The Internet Assigned Numbers Authority (IANA) separates port numbers into three blocks:
  - ✓ Well-known ports ➔ which are preassigned to system processes by IANA;
  - ✓ Registered ports ➔ which are available to user processes and are listed as a convenience by IANA;
  - ✓ Dynamic ports ➔ which are assigned by a client operating system as needed when there is a request for service.

Rule-Based Management

- It is the use of operational rules or restrictions to govern the security of an organization's infrastructure.
- Rules are incorporated into organizational policies that get disseminated throughout an organization.
- **Example**:
  - A company that uses a **security policy** to determine how employees can access the **Internet** and other **network resources**.

Network Administration Security Methods

- Flood guard
  - It is a tool to protect resources from flooding attacks.
  - It applies appropriate mitigation techniques.
- Loop protection
  - Apply the appropriate configurations to the router.
  - Verify that the appropriate manufacturer's configurations are applied as well.
- Port security
  - Disabling unnecessary services.
  - Closing ports that are by default open or have limited functionality.
  - Regularly applying the appropriate patches.
  - Hiding responses from ports that indicate their status and allow access to pre-configured connections only.
- Secure router configuration
  - Properly secured.
  - Prevent routing loops.
- MAC limiting
  - It is the technique of defining how many different MAC addresses may connect to a network device.

Network Administration Security Methods

- MAC filtering
  - It is the technique of allowing or denying devices with certain MAC addresses to connect to a network.
- Network separation
  - Splitting your network into two or more logically separated networks.
  - It helps separate critical network functions from lower-priority functions.
- VLAN management
  - VLAN configurations can be very complicated.
  - Its security measures can be implemented and managed quickly.
  - Most organizations will keep track of VLAN configurations using diagrams and documentation.
- Implicit deny
  - Use the principle of implicit deny so that the firewall blocks any traffic it does not recognize.
- Log analysis
  - It helps detect any unauthorized intrusion attempts on the network.

Unified Threat Management

- UTM refers to a system that centralizes various security techniques ➔ firewall, anti-malware, network intrusion prevention, URL filtering, content inspection, malware inspection, etc. ➔ into a **single appliance.**

- It is a single console through which a security administrator can monitor and manage various defense settings.

Unified threat management combining the functionality of various security techniques into one device

Guidelines for Applying Network Security Administration Principles

- Manage the network devices to ensure that configurations conform with your security policies.
- Maintain documentation about all current server configurations.
- Establish and document baselines that suit your organization.
- Update antivirus software regularly.
- Configure the required network services only.
- Disable unused interfaces and unused application service ports.
- Have a good backup strategy and disaster recovery plan (DRP) in place.
- Apply security updates and patches regularly.
- Ensure that sensitive data is well encrypted.
- Regularly check event logs for unusual activities.
- Monitor network activities on a regular basis.

Secure Wireless Traffic

- Wireless networking has become a standard in most networks because of the mobility it gives to network users and the simplicity of connecting components to a LAN.

- This very simplicity creates security problems because any attacker with physical access and a laptop with a wireless network adapter can attach to your wireless LAN, and once an attacker is on your network, you're vulnerable.

Wireless Antenna Types

- Wireless networking signals can be amplified using a variety of different antenna types.
- The two main categories of antennas are **directional** and **omni-directional**.
  - **Omni-directional** antennas send and receive radio waves from all directions.
    - **Rubber duck:**
      - It is a small omnidirectional antenna that is usually sealed in a rubber jacket.
      - It is ideal for mobility. It is often used in walkie-talkies or two-way radios, as well as short-range wireless networking.
  - **Directional** antennas transmit signals to a specific point.
    - **Ceiling dome:**
      - It is installed on ceilings and is commonly used to cover rooms in a building with a wireless signal.
    - **Yagi:**
      - A directional antenna is used primarily in radio. It is used in long-distance wireless networking to extend the range of hotspots.
    - **Parabolic:**
      - A very precise directional antenna. It is used often in satellite dishes.
    - **Backfire:**
      - A small directional antenna. It is used in wireless networks to efficiently target a specific physical area without overextending coverage.
    - **Cantenna**:
      - This is a homemade directional antenna that can extend wireless networks or help to discover them.

Wireless Protocol (802.11 Standards)

- There are various 802.11 standards that you may encounter in networking implementations.
- **802.11:**
  - A family of specifications developed by the IEEE for wireless LAN communications between wireless devices or between wireless devices and a base station.
  - It specifies wireless data transfer rates of up to 2 megabits per second (Mbps) in the 2.4 gigahertz (GHz) frequency band.
- **802.11a:**
  - It is a fast and secure wireless protocol but relatively expensive.
  - 802.11a supports speeds up to 54 Mbps in the 5 GHz frequency band with a limited range of only 60 feet.
- **802.11b:**
  - 802.11b is the least expensive wireless network protocol.
  - 802.11b provides for an 11 Mbps transfer rate in the 2.4 GHz frequency.
  - 802.11b has a range of up to 1,000 feet in an open area and a range of 200 to 400 feet in an enclosed space.
- **802.11g:**
  - 802.11g provides for a 54 Mbps transfer rate in the 2.4 GHz band.
  - It is compatible with 802.11b and may operate at a much faster speed.

Wireless Protocol (802.11 Standards)

- There are various 802.11 standards that you may encounter in networking implementations.
- **802.11n:**
  - 802.11n supports speeds up to 600 Mbps in the 2.4 GHz or 5 GHz ranges..
- **802.11ac:**
  - A specification that improves on 802.11n by adding wider channels in the 5 GHz band to increase data throughput to a total of 1300 Mbps.

Wireless Security Protocols

- The following table describes security protocols often used in wireless networking:
  - Wired Equivalent Privacy (WEP)
    - Provides 64-bit, 128-bit, and 256-bit encryption using the Rivest Cipher 4(RC4) algorithm for wireless communication that uses the 802.11a and 802.11b protocols.
    - WEP was extremely vulnerable With a 24-bit IV size to an IV attack that would be able to predict the IV value.
  - Wireless Transport Layer Security (WTLS)
    - It is a security layer of the Wireless Application Protocol (WAP).
    - It uses public-key cryptography for mutual authentication and data encryption.
    - WTLS is meant to provide secure WAP communications.
    - If it is improperly configured or implemented, then it can expose wireless devices to attacks that include email forgery and sniffing data.
  - **802.1x**
    - It is used to provide a port-based authentication mechanism over a LAN or wireless LAN.
    - 802.1x uses the 802.11a and 802.11b protocols for wireless communications.
    - 802.1x uses the Extensible Authentication Protocol (EAP) to provide user authentication against a directory service.

Wireless Security Protocols

- The following table describes security protocols often used in wireless networking:
  - **Wi-Fi Protected Access (WPA/WPA2)**
    - WPA was introduced during the development of the 802.11i IEEE standard and WPA2 implemented all the mandatory components of the standard.
    - It provides for dynamic reassignment of keys to prevent the key attack vulnerabilities of WEP.
  - **EAP**
    - A framework that allows clients and servers to authenticate with each other.
    - EAP does not specify which authentication method should be used.
    - It enables the choice of a wide range of current authentication methods.
    - It allows for the implementation of future authentication methods. EAP is often utilized in wireless networks and wired implementations
    - Two common EAP implementations are:
      - Protected Extensible Authentication Protocol (PEAP), which is an open standard developed by a coalition made up of Cisco Systems, Microsoft, and RSA Security.
      - Lightweight Extensible Authentication Protocol (LEAP), which is Cisco Systems' proprietary EAP implementation.

Thank you