Name: Kanchan Chopde

CSC 5372 Principles of Cyber Security

Winter 2024

Assignment 2

- **What are the differences between the LAN, WAN, and DMZ?**

LAN (Local Area Network): A LAN is a network that connects computers and devices within a limited area, such as a home, office, or school.

Characteristics:

- Typically private and secure.
- Used for internal communication and resource sharing.
- Controlled by the organization or individual owning the network.
- Devices within a LAN can communicate directly without going through external networks.

WAN (Wide Area Network):A WAN is a network that connects multiple LANs over a large geographic area, often using public infrastructure like the internet.

Characteristics:

- Spans large distances, potentially across cities or countries.
- Utilizes public or private networks to connect geographically dispersed locations.
- Enables communication between different LANs and remote users.
- May involve leased lines, satellites, or internet connections.

DMZ (Demilitarized Zone): A DMZ is a separate network segment that acts as a buffer between the LAN and external untrusted networks like the internet.

Characteristics:

- Provides an additional layer of security by isolating external-facing servers from the internal network.
- Hosts services like web servers, email servers, or FTP servers that need to be accessible from the internet.
- Subject to more stringent security measures than the LAN to protect against external threats.

While a LAN is a local network for internal communication, a WAN connects multiple LANs over larger distances. On the other hand, a DMZ serves as an isolated zone between the internal LAN and external networks, hosting services that require external access while maintaining security by segregating them from the internal

network. Each network type serves distinct purposes in ensuring efficient communication and security within an organization's overall network infrastructure.

- **What functions are performed by the DC?**

Controls Active Directory administration privileges and limit domain user accounts: The domain controller ensures every computer connected to a network is authorized before granting access rights to sensitive files. It carefully reviews user accounts and provides administrative privileges and access to only those who need them to perform their job functions. It also ensures user accounts are protected with robust passwords.

Avoids "operator error" data breaches: The data controller provides network-wide security policies, such as those that require users to set a unique and robust password.

Manages the network centrally: Managing and configuring devices individually is a time-consuming task. A domain controller can save cost and time to set login and security parameters for devices from a centralized server. Additionally, domain controllers allow automatically installing network printers on your system as soon as they join your domain. You can centrally manage, pause, command, or restart printing devices on your network.

Allows sharing of resources: Domain controllers enable sharing of resources as all the devices are connected centrally. You can set login-specific access privileges and access any computer or device. This helps reduce the cost required to purchase new printers, computers, and more.

Prevents unauthorized user access: Domain controllers have set security controls to prevent user accounts from accessing the network with too many failed login attempts. It can disable user accounts immediately when an employee leaves an organization, require login credentials for locked screens, and restrict USB access based on user permissions and access rights.

- **What operations does the PF-Sense node perform?**

The PF-Sense node performs various operations related to high availability and network security. Some operations include:

1. High Availability Configuration: Setting up state synchronization using pfsync on both primary and secondary nodes.Configuring synchronization of states, interfaces, and custom filter host IDs.Establishing configuration synchronization (XMLRPC) between nodes for seamless failover.

2. CARP (Common Address Redundancy Protocol): Using CARP for redundant IP addresses to ensure continuous connectivity during failover.Sharing a CARP type Virtual IP address (VIP) across cluster nodes, with one node as the master receiving traffic for the IP address.
3. State Table Synchronization: Exchanging active connection state information between nodes using the pfsync protocol for seamless failover
4. Configuration Synchronization: Enabling configuration synchronization using XMLRPC to maintain identical firewall settings between nodes
5. Network Security:Implementing security best practices such as setting secure passwords, limiting access to key-based authentication, and changing default ports for SSH access.

- **Please diagnose in detail what happens when the user makes a call to the website. Please include the path the traffic takes, including the ports and hosts involved.**

When a user makes a call to a website, several steps occur in the process, involving multiple hosts, ports, and network components. Here is a detailed diagnosis of what happens during this interaction:

User Initiates Request: The user enters the website's URL in their web browser and hits Enter. The browser sends an HTTP request to the website's domain name.

DNS Resolution: The request is first sent to a Domain Name System (DNS) server to resolve the domain name to an IP address. The DNS server responds with the IP address of the website.

Establishing Connection: The browser initiates a TCP connection to the web server hosting the website. The connection typically uses port 80 for HTTP or port 443 for HTTPS.

Request Processing: The web server receives the request and processes it. It may interact with application servers, databases, or other resources to generate the content requested.

Response Generation: The web server generates an HTTP response containing the requested content. This response is sent back to the user's browser over the established TCP connection.

Data Transmission: Data packets containing the website's content travel through various network devices like routers and switches. Each device forwards packets based on routing tables and destination IP addresses.

Firewall Inspection: Traffic may pass through firewalls that inspect packets for security purposes. Firewalls can filter traffic based on rules, allowing or blocking specific types of data.

Load Balancing (if applicable): In cases where load balancing is implemented, requests may be distributed across multiple servers for better performance and reliability.

Content Delivery Network (CDN): If the website uses a CDN, content may be cached on servers closer to the user for faster delivery.

Response Display: The user's browser receives the response and renders the website content for display. Images, scripts, and other resources may be fetched from different hosts or CDNs specified in the webpage.

- **What are the differences (and why) between the two PF-Sense nodes?**

In the given Infrastructure in labs, there are 2 pf-sense nodes.
pfSense with LAN, WAN, and Datacenter:

Functionality: pfSense offers features like unified threat management, load balancing, multi-WAN support, and more for network security and routing.

pfSense can be used to filter traffic between your network and the internet, blocking unwanted traffic and protecting your devices from attack.

pfSense with LAN, WAN, DMZ, Office, VPN:

Configuration: Setting up pfSense with LAN, WAN, DMZ, Office, and VPN involves defining different zones for specific purposes like internal LAN, external WAN, isolated DMZ for public-facing servers, office network for internal users, and VPN for secure remote access.

NAT and Routing: Proper NAT configuration is essential to allow access between these zones while maintaining security measures. Port forwarding and static routes may be required to enable communication between the different network segments.

- **Please explain the OSI model in detail.**

Open System Interconnection (OSI) Model consists of 7 layers. It tells us about communication duties of a system without taking into consideration their internal structure and technology. Each layer in OSI model has some assigned duty which enables communication from one open system to another.

7 Layers are:

Physical layer:

The Physical Layer defines the physical characteristics of the network such as connections, voltage levels and timing.

Data Link layer:

The Data Link layer formats the message into a data frame and adds a header containing the hardware destination and source address to it. This header is responsible for finding the next destination device on a local network.

This layer is subdivide into 2 sub-layers:

logical link control (LLC) and

media access control (MAC).

The LLC functions include:
Managing frames to upper and lower layers
Error Control
Flow control

The MAC sublayer carries the physical address of each device on the network. This address is more commonly called a device's MAC address. MAC address is a 48 bits address which is burned into the NIC card on the device by its manufacturer.

Network layer:

This layer provides logical addresses which routers will use to determine the path to the destination. In most cases, the logic addresses here means the IP addresses (including source & destination IP addresses).

Transport layer:

This layer maintains flow control of data and provides for error checking and recovery of data between the devices. The most common example of Transport layer is Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

Session layer:

Layer 5 establishes, maintains, and ends communication with the receiving device.

Presentation layer:

This layer ensures the presentation of data, that the communications passing through are in the appropriate form for the recipient. In general, it acts as a translator of the network. For example, you want to send an email and the Presentation will format your data into email format. Or you want to send photos to your friend, the Presentation layer will format your data into GIF, JPG or PNG... format.

Application Layer:

This is the closest layer to the end user. It provides the interface between the applications we use and the underlying layers. Telnet, FTP, email client (SMTP), HyperText Transfer Protocol (HTTP) are examples of Application layer.