## Introduction to Network Security:-

Network Security protects your network and data from breaches, intrusions and other threats. This is a vast and overarching term that describes hardware and software solutions as well as processes or rules and configurations relating to network use, accessibility, and overall threat protection.

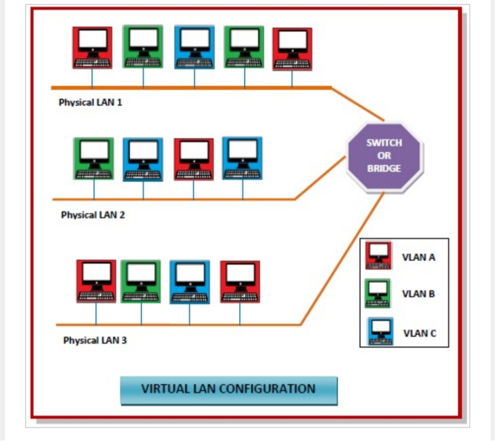
Network Security involves access control, virus and antivirus software, application security, network analytics, types of network-related security (endpoint, web, wireless), firewalls, VPN encryption and more.

Benefits of Network Security

Network Security is vital in protecting client data and information, keeping shared data secure and ensuring reliable access and network performance as well as protection from cyber threats. A well designed network security solution reduces overhead expenses and safeguards organizations from costly losses that occur from a data breach or other security incident. Ensuring legitimate access to systems, applications and data enables business operations and delivery of services and products to customers.

#VLAN :-

Virtual Local Area Networks or Virtual LANs (VLANs) are a logical group of computers that appear to be on the same LAN irrespective of the configuration of the underlying physical network. Network administrators partition the networks to match the functional requirements of the VLANs so that each VLAN comprise of a subset of ports on a single or multiple switches or bridges. This allows computers and devices in a VLAN to communicate in the simulated environment as if it is a separate LAN.



Features of VLANs

- A VLAN forms sub-network grouping together devices on separate physical LANs.
- VLAN's help the network manager to segment LANs logically into different broadcast domains.
- VLANs function at layer 2, i.e. Data Link Layer of the OSI model.

- There may be one or more network bridges or switches to form multiple, independent VLANs.
- Using VLANs, network administrators can easily partition a single switched network into multiple networks depending upon the functional and security requirements of their systems.
- VLANs eliminate the requirement to run new cables or reconfiguring physical connections in the present network infrastructure.
- VLANs help large organizations to re-partition devices aiming improved traffic management.
- VLANs also provide better security management allowing partitioning of devices according to their security criteria and also by ensuring a higher degree of control connected devices.
- VLANs are more flexible than physical LANs since they are formed by logical connections. This aids is quicker and cheaper reconfiguration of devices when the logical partitioning needs to be changed

Types of VLANs

- Protocol VLAN − Here, the traffic is handled based on the protocol used. A switch or bridge segregates, forwards or discards frames the come to it based upon the traffics protocol.
- Port-based VLAN − This is also called static VLAN. Here, the network administrator assigns the ports on the switch / bridge to form a virtual network.
- Dynamic VLAN − Here, the network administrator simply defines network membership according to device characteristics.

##VPN :-

VPN stands for the virtual private network. A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet. A Virtual Private Network is a way to extend a private network using a public network such as the internet. The name only suggests that it is a Virtual “private network” i.e. user can be part of a local network sitting at a remote location. It makes use of tunneling protocols to establish a secure connection.

VPN connections are used in two important ways −

- To establish WAN connections using VPN technology between two distant networks that may be thousands of miles apart, but where each has some way of accessing the internet.

- To establish remote access connections that enable remote users to access a private network through a public network like the internet.

Types of VPNs

The types of VPNs are as follows −

- Router VPN

The first type uses a router with added VPN capabilities. A VPN router cannot only handle normal routine duties, but it can also be configured to form VPNs over the internet to other similar routers located in remote networks.

- Firewall VPN

The second type of VPN is one built into a firewall device. Firewall VPN can be used both to support remote users and also to provide VPN links.

- Network Operating System

The third type of VPNs include those offered as part of a network operating system like Windows NT, Windows 2000, and Netware 5. These VPNs are commonly used to support remote access, and they are generally the least expensive to purchase and install.

## Firewall:-

A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization’s previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet. A firewall’s main purpose is to allow non-threatening traffic in and to keep dangerous traffic out.

Types of Firewalls

- Packet filtering

A small amount of data is analyzed and distributed according to the filter’s standards.

- Proxy service

Network security system that protects while filtering messages at the application layer.

- Stateful inspection

Dynamic packet filtering that monitors active connections to determine which network packets to allow through the Firewall.

- Next Generation Firewall (NGFW)

Deep packet inspection Firewall with application-level inspection.

## IPS :-

An intrusion prevention system (IPS) is a network security and threat prevention tool. The idea behind intrusion prevention is to create a preemptive approach to network security so potential threats can be identified and responded to swiftly. Intrusion prevention systems are thereby used to examine network traffic flows in order to find malicious software and to prevent vulnerability exploits.

An IPS is used to identify malicious activity, record detected threats, report detected threats and take preventative action to stop a threat from doing damage. An IPS tool can be used to continually monitor a network in real time.

The following are three common approaches for an IPS tool to protect networks:

- signature-based detection in which the IPS tool uses previously defined attack signatures of known network threats to detect threats and take action;
- anomaly-based detection in which the IPS searches for unexpected network behavior and blocks access to the host if an anomaly is detected; and
- policy-based detection in which the IPS first requires administrators to make security policies -- when an event occurs that breaks a defined security policy, an alert is sent to system administrators.

Types of intrusion prevention systems

Three types of intrusion prevention systems appear commonly. These types are the following:

- network behavior analysis (NBA), which analyzes network behavior for abnormal traffic flow -- commonly used for detecting DDoS attacks;
- network-based intrusion prevention system (NIPS), which analyzes a network to look for suspicious traffic -- typically surrounding protocols;
- host-based intrusion prevention system (HIPS), which are installed in a single host and used to analyze suspicious activity in one specific host.

## Proxy Servers

A proxy server is a computer system or router that functions as a relay between client and server. It helps prevent an attacker from invading a private network and is one of several tools used to build a firewall.

The word proxy means "to act on behalf of another," and a proxy server acts on behalf of the user. All requests to the Internet go to the proxy server first, which evaluates the request and forwards it to the Internet. Likewise, responses come back to the proxy server and then to the user.

Types Of Proxy Server

1. **Reverse Proxy Server:** The job of a reverse proxy server to listen to the request made by the client and redirect to the particular web server which is present on different servers.
   Example – Listen for TCP port 80 website connections which are normally placed in a demilitarized zone (DMZ) zone for publicly accessible services but it also protects the true identity of the host. Moreover, it is transparent to external users as external users will not be able to identify the actual number of internal servers.

2. Web Proxy Server: Web Proxy forwards the HTTP requests, only URL is passed instead of a path. The request is sent to particular the proxy server responds. Examples, Apache, HAP Proxy.

3. Anonymous Proxy Server: This type of proxy server does not make an original IP address instead these servers are detectable still provides rational anonymity to the client device.

4. Highly Anonymity Proxy: This proxy server does not allow the original IP address and it as a proxy server to be detected.

5. Transparent Proxy: This type of proxy server is unable to provide any anonymity to the client, instead, the original IP address can be easily detected using this proxy. But it is put into use to act as a cache for the websites. A transparent proxy when combined with gateway results in a proxy server where the connection requests are sent by the client , then IP are redirected.
6. CGI Proxy: CGI proxy server developed to make the websites more accessible. It accepts the requests to target URLs using a web form and after processing its result will be returned to the web browser. It is less popular due to some privacy policies like VPNs but it still receives a lot of requests also.
7. Suffix Proxy: Suffix proxy server basically appends the name of the proxy to the URL. This type of proxy doesn't preserve any higher level of anonymity. It is used for bypassing the web filters. It is easy to use and can be easily implemented but is used less due to the more number of web filter present in it.
8. Distorting Proxy: Proxy servers are preferred to generate an incorrect original IP address of clients once being detected as a proxy server. To maintain the confidentiality of the Client IP address HTTP headers are used.
9. Tor Onion Proxy: This server aims at online anonymity to the user's personal information. It is used to route the traffic through various networks present worldwide to arise difficulty in tracking the users' address and prevent the attack of any anonymous activities. It makes it difficult for any person who is trying to track the original address.
10. 12P Anonymous Proxy: It uses encryption to hide all the communications at various levels. This encrypted data is then relayed through various network routers present at different locations and thus I2P is a fully distributed proxy. This software is free of cost and open source to use, It also resists the censorship.
11. DNS Proxy: DNS proxy take requests in the form of DNS queries and forward them to the Domain server where it can also be cached, moreover flow of request can also be redirected.