Network Security :-

1. What is Network Security ?

"Network Security" refers to any activity designed to protect the usability and integrity of your network and data. It includes both hardware and software technologies. It targets a variety of threats and stops them from entering or spreading on your network.

2. How does Network Security works ?

Network security combines multiple layers of defenses at the edge and in the network. Authorized users gain access to network resources, but malicious actors are blocked from carrying out exploits and threats.

- ➢ Authorization of access to data in a network.
- ➢ Network security covers a variety of computer networks, both public and private.
- ➢ Combines multiple layers of defenses at the edge and in the network.
- ➢ Each network security layer implements policies and controls.
- ➢ Protect proprietary information from attack.

3. How do Network Security benefits ?

Every organization that wants to deliver the services that customers and employees demand must protect its network. Network security also helps you protect proprietary information from attack. Ultimately it protects your reputation.

➔ Risk Mitigation :
One of the most important tasks for any business in today’s technological environment is risk mitigation. This ensures a minimum risk level for virus and malware infection, spyware infection, and hacker attacks.

➔ Increased Network Performance :
The performance of computer networks is a vital issue for any company; downtime and lag cost money in more ways than one. A managed network security services provider can help you ensure that your network is always performing at peak efficiency levels.

➔ Less Stress for Management Staff :
Managing a network is definitely not easy, and the difficulty goes up as the network increases.A managed network security service provider can simplify the process.

➔ Faster and More Proactive Resolution of Problems :
Taking a more proactive stance has its benefits; it can help to pinpoint issues before they cause problems with network performance, uptime and stability.

➔ Centralized updates :
It is very important that the anti-virus software is timely updated. A network security system which is centralized offers this advantage of timely updates without even the knowledge of the individuals.

➔ Levels of access :
The security software gives different levels of access to different users. The authentication of the user is followed by the authorization technique where it is checked whether the user is authorized to access certain resource.

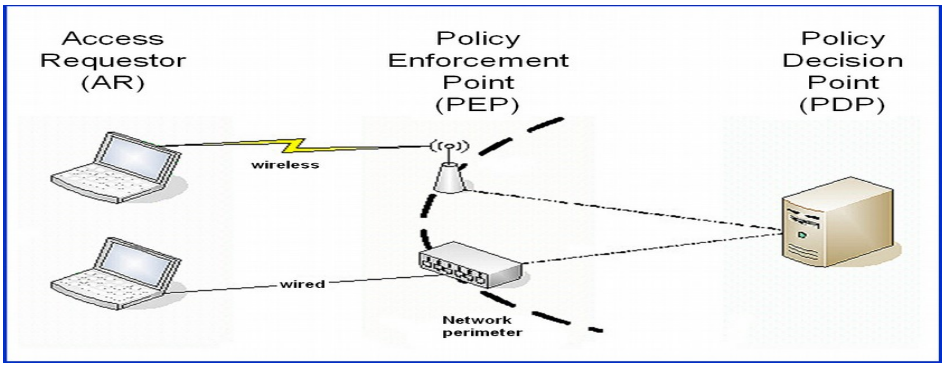
➔ Centrally controlled :
Unlike the desktop security software, the network security software is controlled by a central user called network administrator. While the former is prone to worms and virus attacks, the latter can prevent the hackers before they damage anything.

- **Lower Costs :**
  Using a managed security service is more cost-effective than paying IT consultants on an hourly basis, or keeping a full-time staff. Lower expenditures mean a better bottom line, and more ability to pass those savings on to your customers.

4. Types of Network Security

4.1 Network Access control
4.2 Anti-Virus and Anti-Malware software
4.3 Application security
4.4 Behavioral analytics
4.5 Data loss prevention
4.6 Email security
4.7 Network Segmentation Security
4.8 Security information and event management (SIEM)
4.9 VPN
4.10 Intrusion Detection System (IDS) and Intrusion Prevention Systems (IPS)
4.11 Firewalls/UTM

4.1 Network Access Control :



Network Access Control (NAC) is a computer networking solution that uses a set of protocols to define and implement a policy that describes how to secure access to network nodes by devices when they initially attempt to access the network.

- Prevents unauthorized network access to protect your information assets.
- Helps proactively mitigate network threats such as viruses, worms, and spyware.

- ➔ Addresses vulnerabilities on user machines through periodic evaluation and remediation.
- ➔ Brings you significant cost savings by automatically tracking, repairing, and updating client machines.
- ➔ Recognizes and categorizes users and their devices before malicious code can cause damage.
- ➔ Evaluates security policy compliance based on user type, device type, and operating system.
- ➔ Enforces security policies by blocking, isolating, and repairing noncompliant machines in a quarantine area without needing administrator attention.
- ➔ Applies posture assessment and remediation services to a variety of devices, operating systems, and device access methods including LAN, WLAN, WAN, and VPN.
- ➔ Enforces policies for all operating scenarios without requiring separate products or additional modules.
- ➔ Supports seamless single sign-on through an agent with automated remediation.
- ➔ Provides clientless web authentication for guest users.

4.2 Anti-Virus and Anti-Malware software:

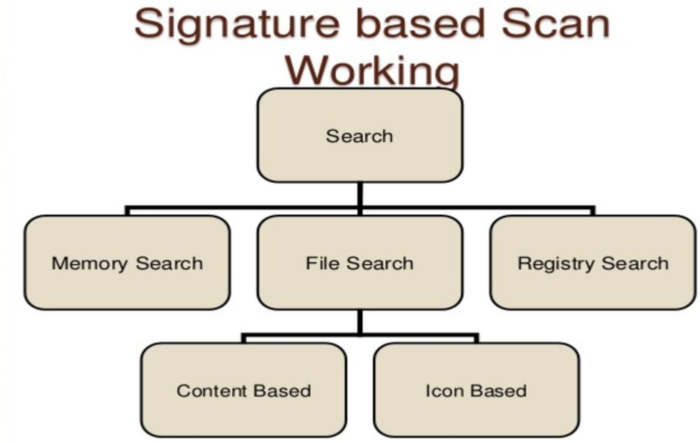
An anti-virus software program is a computer program that can be used to scan files to identify and eliminate computer viruses and other malicious software (malware).

How Anti-Virus Works:

- ➔ Signature-based detection
- ➔ Heuristic-based detection
- ➔ Behavioural-based detection

- ➔ Sandbox detection
- ➔ Data mining techniques
- ➔ Cloud antivirus detection

Signature - based detection :-



Signature-based detection checks all the executable files and validates it with the known list of viruses and other types of malware, or it checks if the unknown executable files shows any misbehaviour as a sign of unknown viruses. Files, programs and applications are basically scanned when they in use.

Heuristic - based detection :-

Antivirus programs use heuristics, by running susceptible programs or applications with suspicious code on it, within a runtime virtual environment. This keeps the vulnerable code from infecting the real world environment. Heuristic technology is deployed in most of the antivirus programs. This helps the antivirus software to detect new or a variant or an altered version of malware, even in the absence of the latest virus definitions.

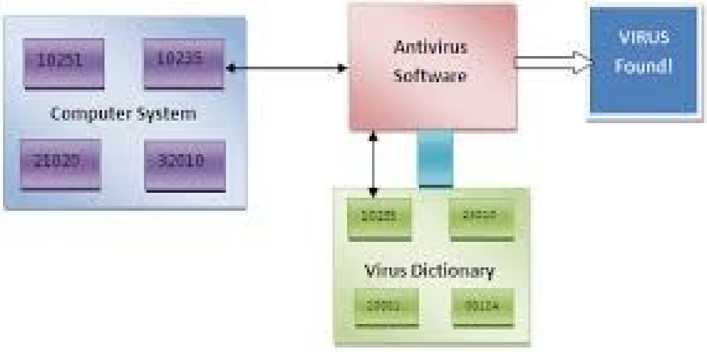
Behavioural - based detection :-

This type of detection is used in Intrusion Detection mechanism. This concentrates more in detecting the characteristics of the malware during execution. This mechanism detects malware only while the malware performs malware actions.Behavior blocking software integrates with the operating system of a host computer and monitors program behavior in real-time for malicious actions. The behavior blocking software then blocks potentially malicious actions before they have a chance to affect the system.

Monitored behaviors can include:

i. Attempts to open, view, delete, and/or modify files.
ii. Attempts to format disk drives and other unrecoverable disk operations.
iii. Modifications to the logic of executable files, scripts of macros.
iv. Modification of critical system settings, such as start-up settings.
v. Scripting of e-mail and instant messaging clients to send executable content.
vi. Initiation of network communications.

Sandbox **detection** :-

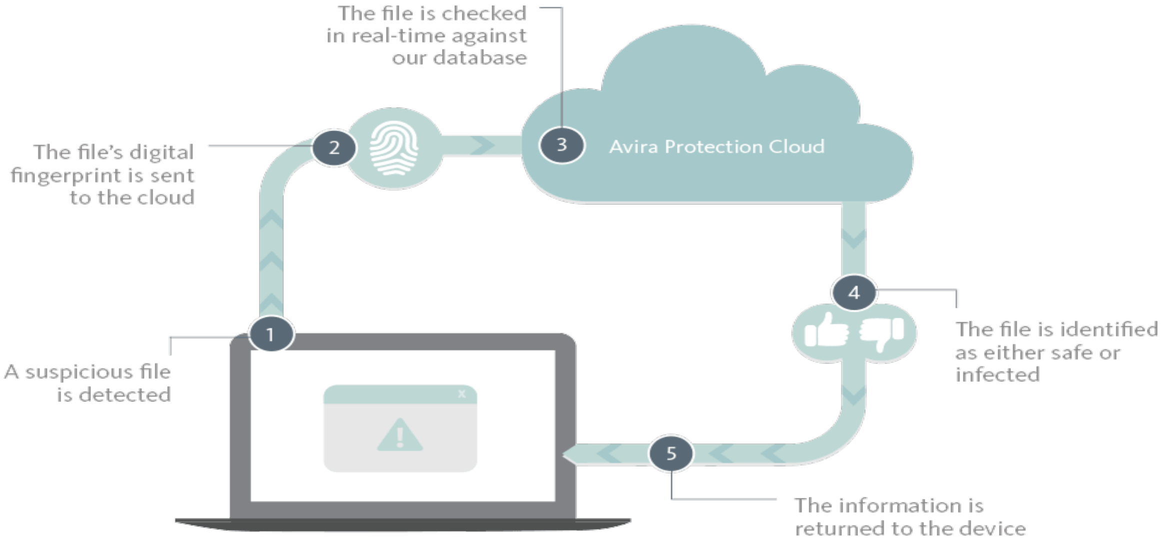


Signature based Antivirus

It executes any applications in the virtual environment to track what kind of actions it performs. Verifying the actions of the program that are logged in, the antivirus software can identify if the program is malicious or not. Sophisticated, targeted malware, designed to evade detection, will be detected and blocked when detonated in your sandbox.

Cloud antivirus detection :-

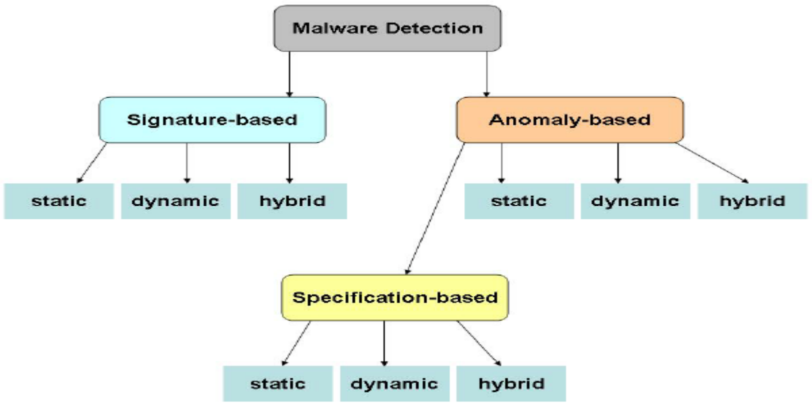
e.g. Avira Anti-Virus Protection Cloud


The file is checked in real-time against our database
The file's digital fingerprint is sent to the cloud
2
3
Avira Protection Cloud
4
The file is identified as either safe or infected
1
A suspicious file is detected
5
The information is returned to the device

Cloud antivirus detection is a type of antivirus protection that uses a small client on the computer that collects information and processes all of the forms of virus detection mentioned in the cloud. By running all detection in the cloud, the computer requires little processing compared to a full antivirus program running on the computer but does always need an Internet connection.

Cloud antivirus software is split into two parts a small "agent" that runs on your computer, and the antivirus "engine" that exists on a server, somewhere on the Internet.

How Anti-Malware Works:



Malware is bad software, plain and simple. It’s code that was created for the purpose of doing something sinister to your computer. Most of the time, it infiltrates a person’s system without their knowledge.
Types of malware were typically named not for what they do but how they attack the machine. Other types of malware include viruses, which infect legitimate files, backdoors, which can open programs and steal data from your computer, and rootkits, which can spy and collect passwords.

Definitions :-

Many programs scan for malware using a database of known malware definitions (also called signatures). These definitions tell what the malware does and how to recognize it. If the anti-malware program detects a file that matches the definition, it’ll flag it as potential malware. This is a good way to remove known threats, but it does require regular updates to make sure the program doesn’t miss out on newly developed malware.

Heuristics :-

Another way anti-malware (AM) detects bad software is a form of analysis called heuristics. An alternative to database scanning, heuristic analysis allows anti-malware programs to detect threats that were not previously discovered. Heuristics identifies malware by behaviors and characteristics, instead of comparing against a list of known malware.

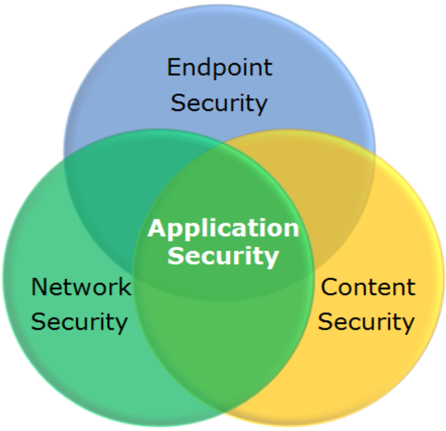
Sandboxing :-

A third way anti-malware software can find malware is by running a program it suspects to be malicious in a sandbox, which is a protected space on the computer. The program believes it has full access to the computer when, in fact, it is running in an enclosed space while theantimalware monitors its behavior. If it demonstrates malicious behavior, the anti-malware will terminate it. Otherwise, the programis allowed to execute outside the sandbox. However, some forms of malware are smart enough to know when they're running in a sandbox and will stay on their best behavior until they're allowed free access to the computer.

Removal :-

Anti-malware doesn't just flag malware and be on its way. Once malware has been found on a system, it needs to be removed. Many threats can be deleted by the anti-malware program as soon as they are detected. However, some malware is designed to cause further damage to your computer if it is removed. If your anti-malware suspects this is the case, it will usually quarantine the file in a safe area of your computer's storage. Basically, the anti-malware puts the malware in a timeout. Quarantining a malicious file prevents it from causing harm, and allows you to remove the file manually without damaging your computer.

4.3 Application security :



Application security encompasses measures taken throughout the code's life-cycle to prevent gaps in the security policy of an application or the underlying system (vulnerabilities) through flaws in the design, development, deployment, upgrade, or maintenance or database of the application.

Applications are links between the data and the user (or another application). The software performs user administration, then a multi-factor authentication method is expected to be in place to access this information. Based on classification of the data being processed by the application, suitable authentication, authorization, and protection of data in storage or transit should be designed for the application in addition to carrying out secure coding.

To protect the software and related sensitive data, a measurement should be taken during each phase of the SDLC (Software Development Life Cycle).
This measurement broadly divides issues into pre and post-deployment phases of development.
Again, **software security deals with the pre-deployment issues**, and **application security takes care of post-deployment issues**.

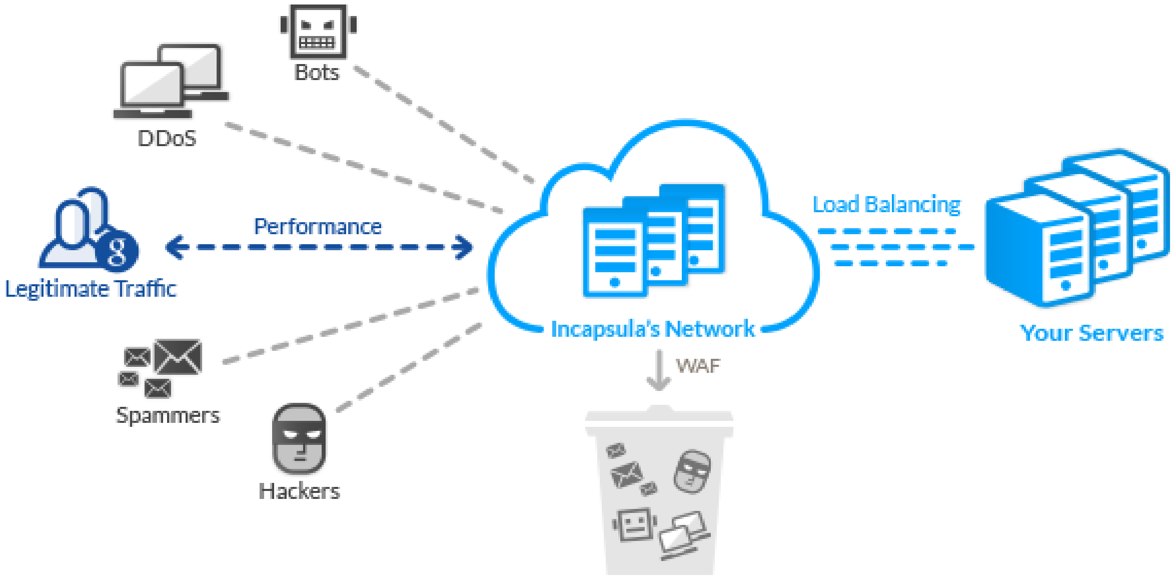
Software security (pre-deployment) activities include :

- ➔ Secure software design.
- ➔ Development of secure coding guidelines for developers to follow.
- ➔ Development of secure configuration procedures and standards for the deployment phase.
- ➔ Secure coding that follows established guidelines.
- ➔ Validation of user input and implementation of a suitable encoding strategy.
- ➔ User authentication.
- ➔ User session management.
- ➔ Function level access control.
- ➔ Use of strong cryptography to secure data at rest and in transit.
- ➔ Validation of third-party components.
- ➔ Arrest of any flaws in software design/architecture.

Application security (post-deployment) activities include :

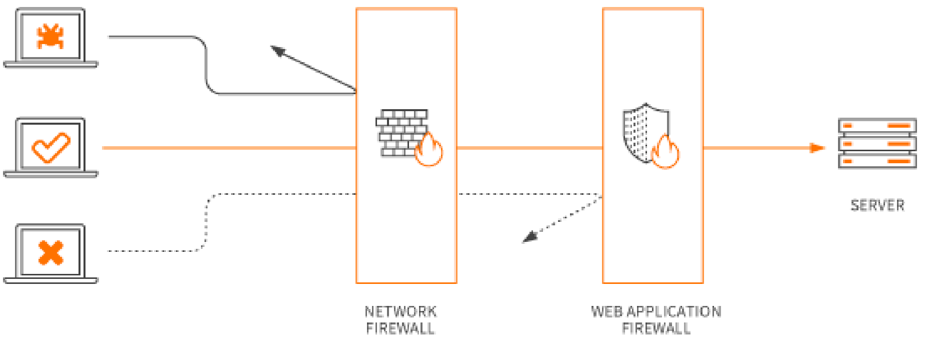
- ➔ Post deployment security tests.
- ➔ Capture of flaws in software environment configuration.
- ➔ Malicious code detection (implemented by the developer to create backdoor, time bomb).
- ➔ Patch/upgrade.
- ➔ IP filtering.
- ➔ Lock down executables.
- ➔ Monitoring of programs at runtime to enforce the software use policy.

Web Application Security :-



Web applications are most often client-server based applications in which the browser acts as client, sending requests and receiving responses from the server to present the information to the user. Therefore, web application security concerns are about client-side issues, server-side protections, and the protection of data at rest and in transit.
Client-side issues are more difficult to fix unless precautions are thought of while designing the user interface.
Server-side components can be protected by implementing countermeasures during the design and coding phases of application development. This requires that secure system/server software is installed.

WEB Application firewall (WAF):



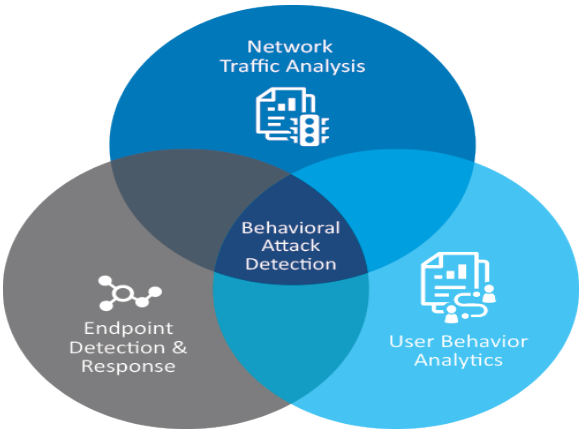
WAFs are designed to protect web applications/servers from web-based attacks that IPSs cannot prevent. In the same regards as an IPS, WAFs can be network or host based.

WAF configured as in-line and monitor traffic to and from web applications/servers. Basically, the difference is in the level of ability to analyze the Layer 7 web application logic. A WAF can be either network-based or host-based and is typically deployed through a proxy and placed in front of one or more Web applications. It monitors traffic before it reaches the Web application, analyzing all requests using a rule base to filter out potentially harmful traffic or traffic patterns. Web application firewalls are a common security control used by enterprises to protect Web applications against zero-day exploits, impersonation and known vulnerabilities and attackers.

Mobile application security :

Mobile systems such as smart phones and tablets that use varied operating systems and security designs are more prevalent than web applications.
These devices, and the applications running on these devices, may pose tremendous risks for the sensitive data they store. Business emails and personal contacts may be exposed to untrusted networks. These applications also interact with many supporting
services. Devices can be stolen. Malware can be installed. Mobile apps can be reverse engineered to access sensitive corporate data.

4.4 Behavioral analytics :



Behavioural analysis is a technique that uses profiles of known behaviour and expected usage patterns to spot anomalies, which may be a sign of an imminent cyber attack or an on-going infection.
Behavioural analysis can call upon a number of techniques, depending on the product used, these include:

➔ **Security intelligence and threat knowledge:** There is much information out there about the type of attacks being perpetrated and how they are being initiated. Security companies build up profiles of attack vectors and malware instances and use these to predict next moves and identify incoming threats.

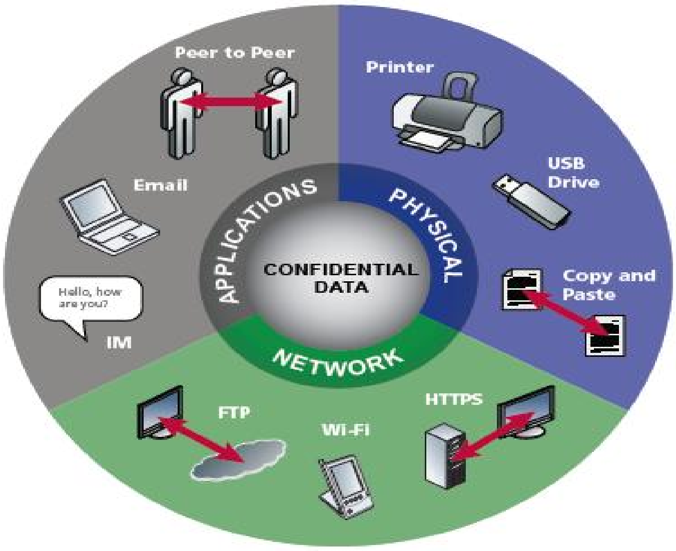
➔ **Profile analysis:** To understand and determine any changes in behaviour, need to understand the behaviour first. Behavioural analysis works by analysing normal behavioural patterns.

➔ **Monitoring, analysis and detection:** This involves understanding baseline of expected behaviour on a network. Using the profile analysis information as a basis for monitoring and detection of potential cyber attacks. Traffic behaviour is one area that can give a lot of information and allow early detection of anomalies. It can also help in the fight against Botnets, which are typically difficult to detect.

User behavior analytics (UBA) is the tracking, collecting and assessing of user data and activities using monitoring systems.

UBA technologies analyze historical data logs including network and authentication logs collected and stored in log management and SIEM systems to identify patterns of traffic caused by user behaviors, both normal and malicious. While UBA systems don't take action based on their findings, they are intended to provide security teams with actionable insights.
Machine learning algorithms allow UBA systems to eliminate false positives and provide clearer and more accurate actionable risk intelligence.

4.5 Data loss prevention :



Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer.
Generally, DLP software products classify and protect confidential and critical information to prevent end users from accidentally or maliciously sharing data that could put the organization at risk. Data loss prevention software and tools monitor and control endpoint activities, plus filter data streams on corporate networks and protect data as it moves.

Reason behind adopting Data Loss Prevention Software : Insider threats and tightened state privacy laws that include strict data protection and access control requirements are two factors that have led to increased DLP adoption. As employees, partners, and contractors create, manipulate, and share data, they work on and off the network, on corporate and personal devices, and in the cloud.

Email is an especially important consideration of data loss prevention strategy because so much sensitive data and information is shared through email today. Business-critical communication also relies on email, which poses a threat to organizations if employees fail to follow corporate policies for handling sensitive/confidential data.

The technological means employed for dealing with data leakage incidents can be divided into categories :

- ➔ Standard Security Measures.
- ➔ Advanced/Intelligent Security Measures.
- ➔ Designated DLP Systems.

➔ **Standard Security Measures :**

Standard security measures, such as firewalls, intrusion detection systems (IDSs) and antivirus software, are commonly available products that guard computers against outsider and insider attacks. The use of a firewall, for example, prevents the access of outsiders to the internal network and an intrusion detection system detects intrusion attempts by outsiders.

➔ **Advanced/Intelligent Security Measures :**

Advanced security measures employ machine learning and temporal reasoning algorithms for detecting abnormal access to data (e.g., databases or information retrieval systems) or abnormal email exchange, honeypots for detecting authorized personnel with malicious intentions and activity-based verification (e.g., recognition of keystroke dynamics) and user activity monitoring for detecting abnormal data access.

➔ **Designated DLP Systems :**

Designated DLP solutions detect and prevent unauthorized attempts to copy or send sensitive data, intentionally or unintentionally, mainly by personnel who are authorized to access the sensitive information. In order to classify certain information as sensitive, these solutions use mechanisms, such as exact data matching, structured data fingerprinting, statistical methods, rule and regular expression matching, published lexicons, conceptual definitions and keywords.

DLP reference data in one of three states :

- Data in Motion (Network).
- Data at rest (Storage).
- Data in use (Endpoints).

Data in motion can be leaked via:

- SMTP
- FTP
- HTTP/HTTPS etc...

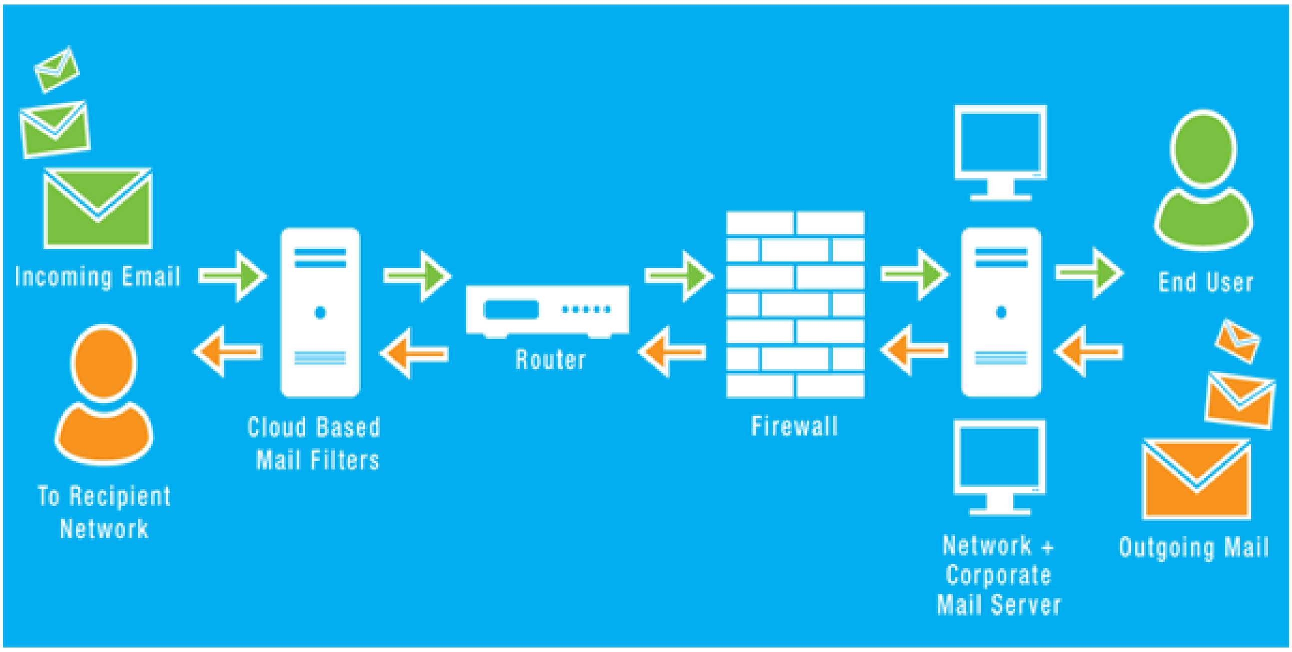
Data at rest could :

- Reside at wrong place.
- Be accessed by wrong person.
- Be owned by wrong person. Etc...

Data in use at endpoints can be leaked via:

- USB
- E-mails
- Web Mails
- HTTP/HTTPS
- FTP etc ...

4.6 Email security :



Email security describes various techniques for keeping sensitive information in email communication and accounts secure against unauthorized access, loss, or compromise. Email is a popular medium for the spread of malware, spam, and phishing attacks, using deceptive messages to entice recipients to divulge sensitive information, open attachments or click on hyperlinks that install malware on the victim's device. Email is also a common entry vector for attackers looking to gain a foothold in an enterprise network and breach valuable company data.

Email security is a broad term that encompasses multiple techniques used to secure an email service. From an individual/end user standpoint, proactive email security measures include:

- ➔ Strong passwords
- ➔ Password rotations
- ➔ Spam filters
- ➔ Desktop-based anti-virus/anti-spam applications

The Need for Email Security:

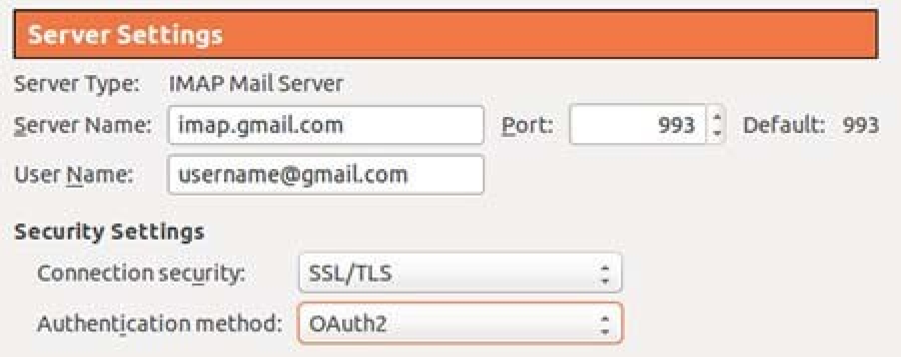
Malware sent via email messages can be quite destructive. Phishing emails sent to employees often contain malware in attachments designed to look like legitimate documents or include hyperlinks that lead to websites that serve malware. Opening an email attachment or clicking on a link in an email can be all that it takes for accounts or devices to become compromised.

Phishing emails can also be used to trick recipients into sharing sensitive information, often by posing as a legitimate business or trusted contacts.Phishing emails aimed at stealing information typically will ask recipients to confirm their login information, passwords, social security number, bank account numbers, and even credit card information.

Enterprise Email Security Best Practices :

- ➔ Engage employees in ongoing security education around email security risks and how to avoid falling victim to phishing attacks over email.
- ➔ Require employees to use strong passwords and mandate password changes periodically.
- ➔ Utilize email encryption to protect both email content and attachments.
- ➔ Implement security best practices for BYOD if your company allows employees to access corporate email on personal devices.
- ➔ Ensure that webmail applications are able to secure logins and use encryption.
- ➔ Implement scanners and other tools to scan messages and block emails containing malware or other malicious files before they reach your end users.
- ➔ Implement a data protection solution to identify sensitive data and prevent it from being lost via email.
- ➔ Always use TLS :

TLS stands for Transport Layer Security, and it ensures your connection to a website is encrypted as well as verifying the integrity of the server you are connecting to. TLS is also used to encrypt your connection to an email server and connections between email servers. While using an external email client, such as Outlook, Apple Mail, or Thunderbird, always make sure your emails are fetched over an encrypted channel.



Server Settings

Server Type: IMAP Mail Server

Server Name: imap.gmail.com Port: 993 Default: 993

User Name: username@gmail.com

Security Settings

Connection security: SSL/TLS

Authentication method: OAuth2

End User Email Security Best Practices :

- ➔ Never open attachments or click on links in email messages from unknown senders.
- ➔ Change passwords often and use best practices for creating strong passwords.
- ➔ Never share passwords with anyone, including co-workers.
- ➔ Try to send as little sensitive information as possible via email, and send sensitive information only to recipients who require it.
- ➔ Use spam filters and anti-virus software.
- ➔ When working remotely or on a personal device, use VPN software to access corporate email.
- ➔ Avoid accessing company email from public wi-fi connections.

Protocols using for e-mail Communication:

- ➔ **Simple Mail Transfer Protocol (SMTP):**

Text based commands for forwarding email between UA MSA (mail submission agent) MSA, MDA (mail delivery agent)

- ➔ **Internet Message Access Protocol (IMAP):**

Supports several clients can be connected to the same mailbox IMAP over SSL (IMAPS)

- ➔ **Post Office Protocol (POP3):**

Another popular mail retrieval protocol. Client connects, gets email, deletes messages on server One client can connect at a time POP3 over SSL (POP3S)

Security Services over Email :

- ➔ **Privacy :** No one should read message except recipient
- ➔ **Authentication:** Recipient should know exactly who the sender is
- ➔ **Integrity:** Recipient should be able to tell whether message was altered in transit
- ➔ **Non repudiation:** Recipient can prove that the sender really sent it
- ➔ **Proof of submission:** Erification to the sender that the mailer got it
- ➔ **Proof of delivery:** Verification to sender that the recipient got it
- ➔ **Message flow confidentiality:** Eavesdropper cannot determine the sender's ID

- **Anonimity:** Ability to send so recipient does not know sender
- **Containment:** Ability to keep secure messages from "leaking" out of a region
- **Audit:** Logging of events having relevance to security
- **Accounting:** Maintain usage statistics (might charge for service)
- **Self destruct:** Message is destroyed on delivery
- **Message sequence integrity:** Sequence of messages have arrived in order, without loss

Common Threats :

- **Malware :** Increasingly, attackers are taking advantage of e-mail to deliver a variety of attacks to organizations through the use of malware, or "malicious software," that include viruses, worms, Trojan horses, and spyware. These attacks, if successful, may give the malicious entity control over workstations and servers, which can then be exploited to change privileges, gain access to sensitive information, monitor users' activities, and perform other malicious actions.

- **Spam and phishing** : Unsolicited commercial e-mail, commonly referred to as spam, is the sending of unwanted bulk commercial e-mail messages. Such messages can disrupt user productivity, utilize IT resources excessively, and be used as a distribution mechanism for malware. Related to spam is phishing, which refers to the use of deceptive computer-based means to trick individuals into responding to the e-mail and disclosing sensitive information.

- **Social engineering :** Rather than hack into a system, an attacker can use e-mail to gather sensitive information from an organization's users or get users to perform actions that further an attack. A common social engineering attack is e-mail spoofing, in which one person or program successfully masquerades as another by falsifying the sender information shown in e-mails to hide the true origin.

- **Entities with malicious intent :** Malicious entities may gain unauthorized access to resources elsewhere in the organization's network via a successful attack on a mail server.

- **Unintentional acts by authorized users :** Not all security threats are intentional. Authorized users may inadvertently send proprietary or other sensitive information via e-mail, exposing the organization to embarrassment or legal action.

Security Safeguards :

- **Implement Management Controls :** Management security controls-such as organization-wide information security policies and procedures, risk assessments, configuration management and change control, and contingency planning-are essential to the effective operation and maintenance of a secure e-mail system and the supporting network infrastructure.

- **Carefully Plan the System Implementation :** The most critical aspect of deploying a secure e-mail system is careful planning before installation, configuration, and deployment. As is often said, security should be considered from the initial planning stage.

- **Secure the Mail Server Application :** Securing the mail server application generally includes patching and upgrading the mail server; configuring the mail server user authentication and access and resource controls; configuring, protecting, and analyzing log files; and periodically testing the security of the mail server application.

- **Secure the Mail Client :** Securely installing, configuring, and using mail client applications generally includes patching and upgrading the mail client applications; configuring the mail client security features (e.g., disable automatic opening of messages); enabling antivirus, antispam, and antiphishing features; configuring mailbox authentication and access; and securing the client’s host operating system.

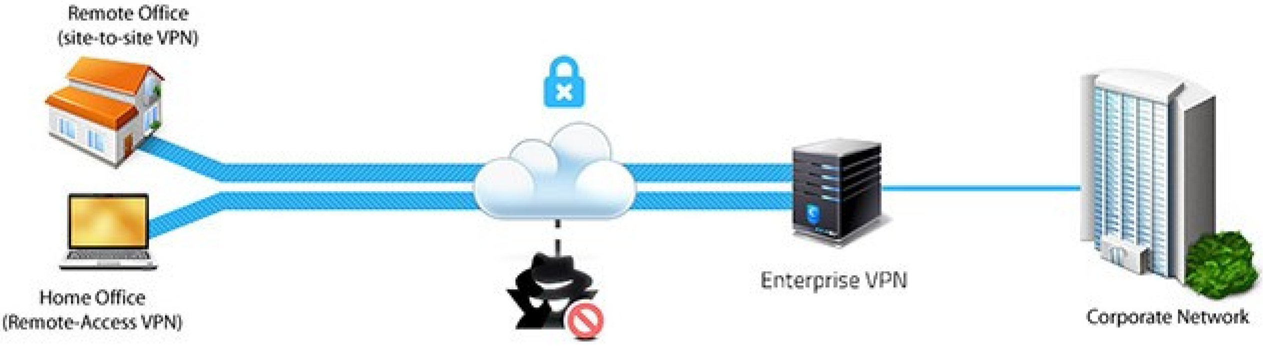
- **Secure the Transmission :** A related control to protect the confidentiality and integrity of the message is to deploy a secure e-mail solution such as leveraging PKI technology to encrypt and sign the message. Digital rights management and data leakage prevention systems can be used to prevent the accidental leakage and exfiltration of sensitive information.

- **Secure the Supporting Operating Environment :** While the mail server and mail clients are the two primary components of an e-mail system, the supporting network infrastructure is essential to its secure operations. Many times, the network infrastructure, including such components as firewalls, routers, and intrusion detection and prevention systems, will provide the first layer of defense between untrusted networks and a mail server.

4.7 Network Segmentation Security :

Network segmentation in computer networking is the act or profession of splitting a computer network into subnetworks, each being a network segment. Advantages of such splitting are primarily for boosting performance and improving security.

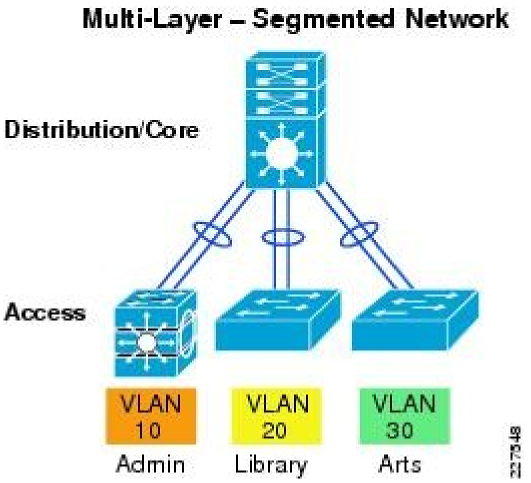
Network segmentation is providing a critical network security defense against increasingly sophisticated cyber-threats. The firewall was the singular line of defense against cyber-threats. Tempting intellectual property and data assets lay on the other side of the firewall once the network perimeter was breached. The attacks often originated from insiders, third parties or partners with valid credentials to access the network.



Advantages Of Network Security :

- **Reduced congestion:** Improved performance is achieved, because on a segmented network there are fewer hosts per subnetwork, thus minimizing local traffic.
- **Improved security:** Broadcasts will be contained to local network. Internal network structure will not be visible from outside.

- **Containing network problems:** Limiting the effect of local failures on other parts of network.
- **Controlling visitor access:** Visitor access to the network can be controlled by implementing VLANs to segregate the network.
- **Unauthorized Access:** A cyber-criminal gains unauthorized access to a network, segmentation or "zoning" can provide effective controls to limit further movement across the network.
- **Seperate VLAN's:** Departments should access via their own VLAN to their application servers because of the confidential nature of the information they process and store.



Effective network segmentation classifides to just five basic steps:

- **Understand the business and organizational drivers :** To know what to protect, need to understand what front-end components, such as point-of-sale terminals and back-end components, support the core functions of the enterprise. Then, identify which assets, data and personnel are critical to ensure continuity of the business.

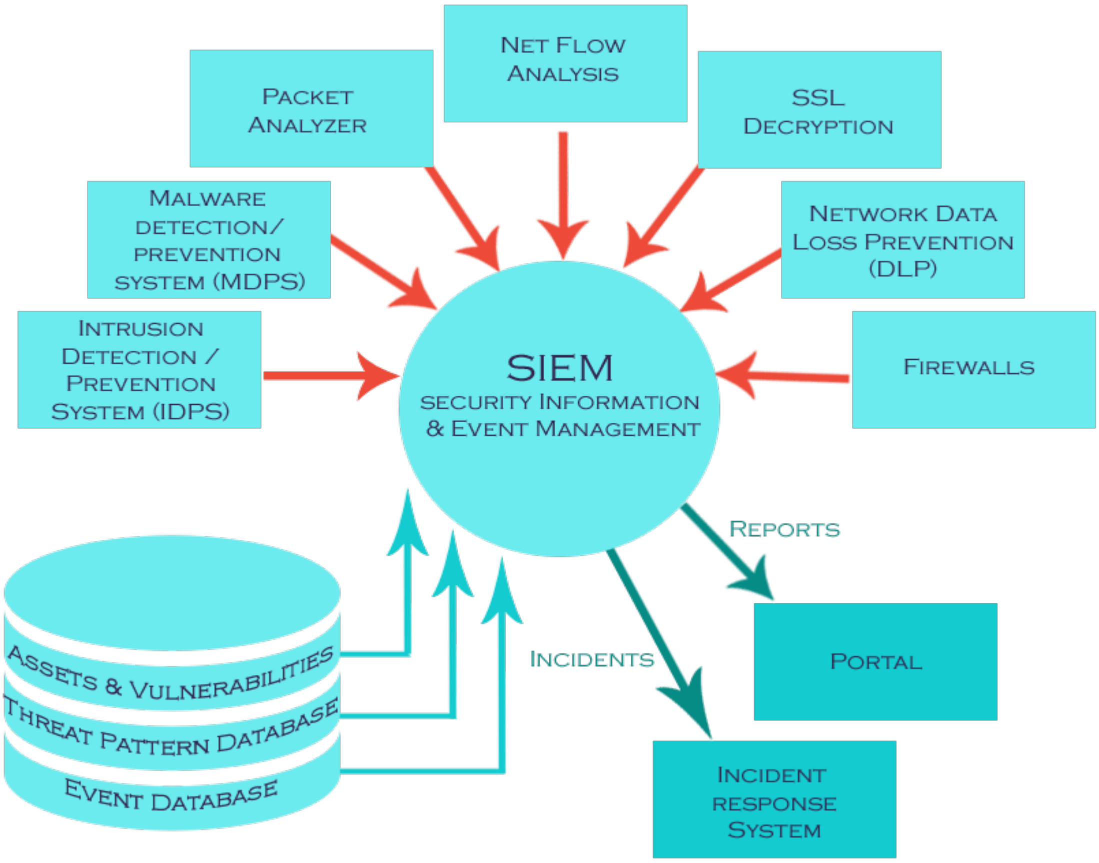
- **Create the plan :** Isolate and protect the most important components. Group related items together, for example all your Windows servers, into one virtual LAN (VLAN). Other asset groups might include infrastructure (routers, switches, VPNs and VoIP) in one VLAN and security assets (IDS, firewalls, web filters and scanners) in another.

- ➔ **Determine who can access what data :** Who needs to administer the routers or switches and Servers ? Who needs access to the human resources or financial systems? Who should able to remotely control the security cameras? If there is no business need, there should be no access.

- ➔ **Implement segmentation :** Network segmentation is a significant, long-term project, but each step along the way increases security.

- ➔ **Maintain :** The network access policy, defined in firewalls, routers and related devices, changes constantly to cater to new business requirements. Ensuring that new changes do not violate your segmentation strategy requires a good degree of visibility and automation (this visibility is also useful to avoid outages or business disruption resulting from misconfiguration).

4.8 Security Information and Event Management (SIEM):



Security Information and Event Management (SIEM) is an approach to security management that seeks to provide a holistic view of an organization’s information technology (IT) security. SIEM combines SIM

(security information management) and SEM (security event management) functions into one security management system provides real-time analysis of security alerts generated by network hardware and applications.
SIEM system collects logs and other security-related documentation for analysis.
And it’s work by deploying multiple collection agents in a hierarchical manner to gather security-related events from end-user devices, servers, network equipment and even specialized security equipment like firewalls, antivirus or intrusion prevention systems. The collectors forward events to a centralized management console, which performs inspections and flags anomalies.

SIEM Capabilities :

- ➔ **Data aggregation:** Log management aggregates data from many sources, including network, security, servers, databases, applications, providing the ability to consolidate monitored data to help avoid missing crucial events.

- ➔ **Correlation:** looks for common attributes, and links events together into meaningful bundles. This technology provides the ability to perform a variety of correlation techniques to integrate different sources, in order to turn data into useful information. Correlation is typically a function of the Security Event Management portion of a full SIEM solution.

- ➔ **Alerting:** the automated analysis of correlated events and production of alerts, to notify recipients of immediate issues. Alerting can be to a dashboard, or sent via third party channels such as email.

- ➔ **Dashboards:** Tools can take event data and turn it into informational charts to assist in seeing patterns, or identifying activity that is not forming a standard pattern.

- ➔ **Compliance:** Applications can be employed to automate the gathering of compliance data, producing reports that adapt to existing security, governance and auditing processes.

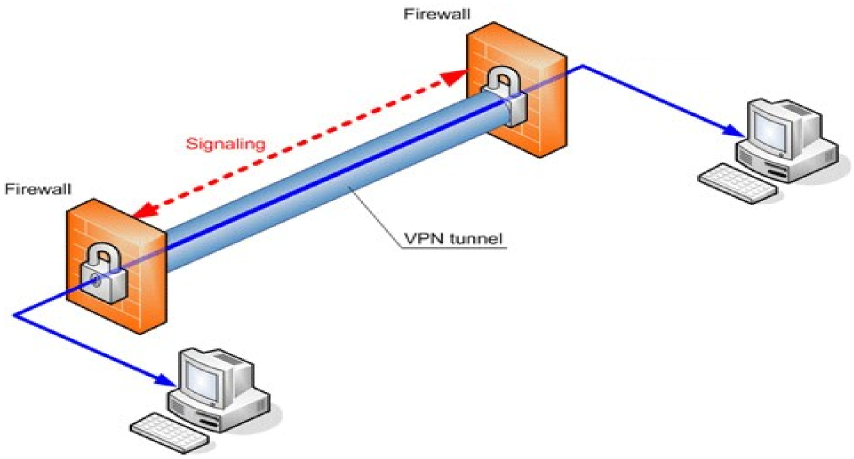
- **Retention:** Employing long-term storage of historical data to facilitate correlation of data over time, and to provide the retention necessary for compliance requirements. Long term log data retention is critical in forensic investigations as it is unlikely that discovery of a network breach will be at the time of the breach occurring.

- **Forensic analysis:** The ability to search across logs on different nodes and time periods based on specific criteria. This mitigates having to aggregate log information in your head or having to search through thousands and thousands of logs.

Why SIEM Necessary ?

- Rise in data breaches due to internal & external threats.
- Attackers are smart and traditional security tools just don't suffice.
- Mitigate sophisticated cyber-attacks.
- Manage increasing volumes of logs frommultiple sources.
- Meet straigent compliance requirements.

4.9 VPN (Virtual Private Network) :



A **VPN** or **Virtual Private Network** is a network connection that enables you to create a secure connection over the public Internet to private networks at a remote location. With a VPN, all network traffic (data, voice, and video) goes through a secure virtual tunnel between the host device (client) and the VPN provider’s servers, and is encrypted. VPN technology uses a combination of features such as encryption, tunneling protocols, data encapsulation, and certified connections to provide with a secure connection to private networks and to protect identity.

Types of VPNs :

- ➔ **Site-to-site VPNs :** are used in the corporate environment. A site-to-site VPN ensures the safe encrypted connection of two or more local area networks (LANs) of the same company or of different companies. It means two geographically separated offices are virtually bridged together into a single LAN and users can access data throughout this network.

- ➔ **Remote Access VPNs:** Connect an individual computer to a private network. This type of VPN can be divided again into two groups:

- ➔ **Corporate VPNs :** Corporate VPNs allow business travelers and telecommuters to connect to their company networks and remotely access resources and services on the networks. When a user connects his/her device to the company's VPN, the VPN thinks that the user's computer is on the same local network as the VPN.

- ➔ **Personal VPNs :** Personal VPNs provide consumers with the same private and secure connection as the corporate VPNs. However, personal VPNs are not used to connect to private networks to access private resources.

Benefits of Masking IP Address :

A VPN masks your IP address, giving you much greater privacy for your online activities. Unshielded, this IP address the unique address for each device on the internet can be misused to reveal your identity, location, ISP, and even the specifics of your online activity.
When you use a VPN, your IP address is masked so you can surf the web anonymously. Thus, no one can find out where you connect from or what you do online by exchanging your IP address with the VPN server's IP address, you can virtually connect from a geographic location that is different from where you are physically located.

VPN Hardware and Software :

VPN is a client-server technology that is made up of hardware and software components on both the client (user) side and the server side. As

VPNs have progressed from a corporate tool into today's personal VPN, the installation requires no additional hardware on the user side other than the computer or device for accessing the internet.

Client (your computer) :

- ➔ The hardware is the personal computer, smart phone or tablet.
- ➔ The software is the VPN client app running on your device

VPN Server :

- ➔ The hardware are server computers and traffic routers.
- ➔ The software controls the traffic routing and communication between the servers and the client (your computer).

VPN systems may be classified by :

- ➔ **Security at the packet level :** VPN security begins at the data packet level the basic building block of online communication. Each data packet is encrypted, packaged in multiple envelopes, and treated as a certified letter. Taken together, these steps ensure data is secure even against deep data packet analysis and potential eavesdropping anywhere between the two connected computers.

- ➔ **Encryption :** All traffic between the two computers is encrypted and isolated in a secure tunnel, shutting out ISPs from eavesdropping and logging your web activity. Encryption for devices connected to a VPN includes VOIP communication, Skype, emails anything that uses an online connection gives more comprehensive protection than a proxy server.

- ➔ **Envelope Strategy :** VPNs use various tunneling protocols to encapsulate data packets for secure transit. Tunneling protocols essentially place the individual data packets – open postcards with the names of the sender and recipient and the data payload into new sealed envelopes marked with the IP address of the VPN. Each envelope contains and conceals the earlier message envelopes. In addition to the layered envelopes, the original message within is also encrypted.

- ➔ **Point-to-point Communication :** When a VPN tunnel connection is opened up, it authenticates sender identity and the integrity of the sent messages. Similar to a registered letter providing point-to-point communication, it ensures that no unauthorized people can intercept the message and that data packets are not tampered.

- ➔ **Layered connection:** The OSI layer they present to the connecting network, such as Layer 2 circuits or Layer 3 network connectivity.

- ➔ **Topology of connections:** The type of topology of connections, such as site-to-site or network-to-network

VPN Security Protocols :

- ➔ **Internet Protocol Security (IPsec):** IPsec uses encryption, encapsulating an IP packet inside an IPsec packet. De-encapsulation happens at the end of the tunnel, where the original IP packet is decrypted and forwarded to its intended destination.

- ➔ **Transport Layer Security (SSL/TLS):** Can tunnel an entire network's traffic or secure an individual connection. An SSL VPN can connect from locations where IPsec runs into trouble with Network Address Translation and firewall rules.

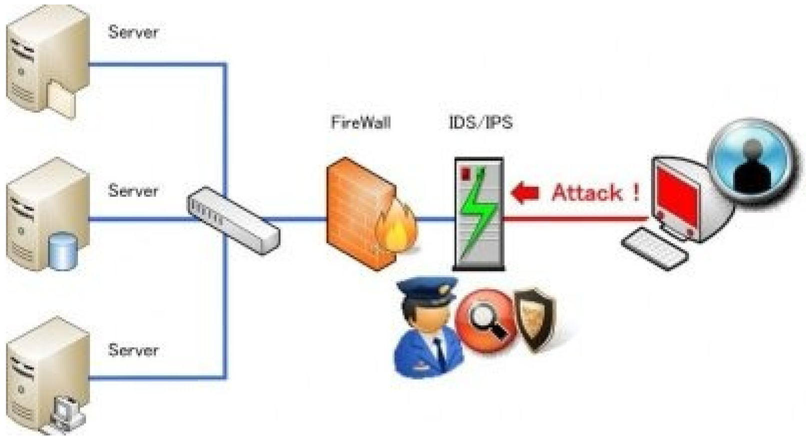
- ➔ **Datagram Transport Layer Security (DTLS):** Used in Cisco AnyConnect VPN and in OpenConnect VPN to solve the issues SSL/TLS has with tunneling over UDP.

- ➔ **Microsoft Point-to-Point Encryption (MPPE):** Works with the Point-to-Point Tunneling Protocol and in several compatible implementations on other platforms.

- ➔ **Microsoft Secure Socket Tunneling Protocol (SSTP):** tunnels Point-to-Point Protocol (PPP) or Layer 2 Tunneling Protocol traffic through an SSL 3.0 channel. (SSTP was introduced in Windows Server 2008 and in Windows Vista Service Pack 1.)

- ➔ **Secure Shell (SSH) VPN:** OpenSSH offers VPN tunneling (distinct from port forwarding) to secure remote connections to a network or to inter-network links. OpenSSH server provides a limited number of concurrent tunnels. The VPN feature itself does not support personal authentication.

4.10 Intrusion Detection System (IDS) and Intrusion Prevention Systems (IPS) :



What is IDS & IPS :

Intrusion detection is the process of monitoring the events occurring in your network and analyzing them for signs of possible incidents, violations, or imminent threats to your security policies. Intrusion prevention is the process of performing intrusion detection and then stopping the detected incidents. These security measures are available as intrusion detection systems (IDS) and intrusion prevention systems (IPS), which become part of network to detect and stop potential incidents.

What an IDS & IPS do :

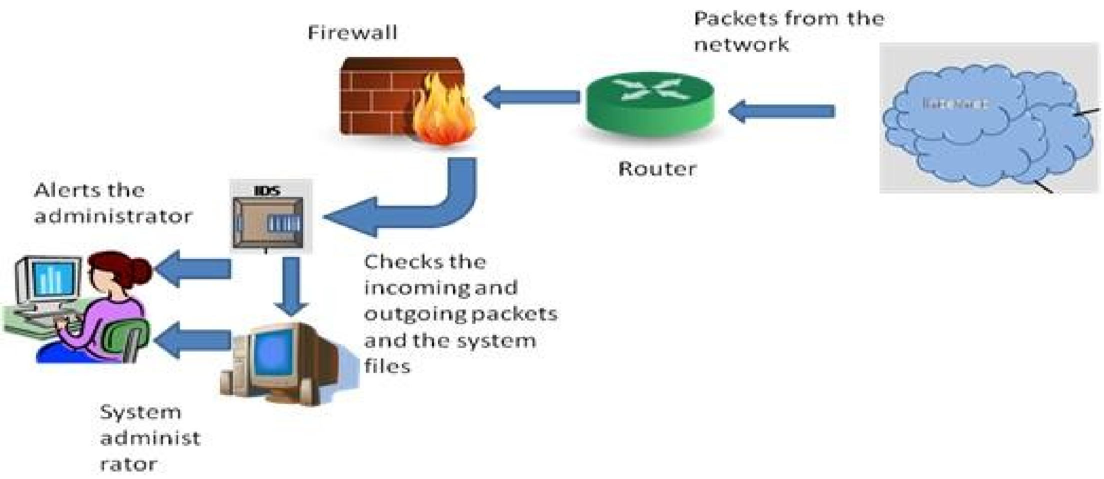
Intrusion detection systems (IDS) and intrusion prevention systems (IPS) constantly watch your network, identifying possible incidents and logging information about them, stopping the incidents, and reporting them to security administrators.IDS/IPS have become a necessary addition to the security infrastructure of most organizations, precisely because they can stop attackers while they are gathering information about your network.

Intrusion Detection System (IDS):

An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity, policy violations or detecting vulnerability exploits against a target application or computer.

How does IDS works?

Any detected activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system combines outputs from multiple sources, and uses alarm filtering techniques to distinguish malicious activity from false alarms.



The three IDS detection methodologies are typically used to detect incidents.

- ➔ **Signature-Based Detection:** Compares signatures against observed events to identify possible incidents. This is the simplest detection method because it compares only the current unit of activity (such as a packet or a log entry, to a list of signatures) using string comparison operations.

- ➔ **Anomaly-Based Detection:** Compares definitions of what is considered normal activity with observed events in order to identify significant deviations. This detection method can be very effective at spotting previously unknown threats.

- **Stateful Protocol Analysis:** compares predetermined profiles of generally accepted definitions for protocol activity for each protocol state against observed events in order to identify deviations.

NIDS & HIDS:

A system that monitors important operating system files is an example of a **HIDS** (Host-based Intrusion Detection Systems), while a system that analyzes incoming network traffic is an example of a **NIDS** (Network Intrusion Detection Systems).

Network Intrusion Detection Systems (NIDS):

Network intrusion detection systems (NIDS) are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. It performs an analysis of passing traffic on the entire subnet, and matches the traffic that is passed on the subnets to the library of known attacks. Once an attack is identified, or abnormal behavior is sensed, the alert can be sent to the administrator. NID Systems are also capable of comparing signatures for similar packets to link and drop harmful detected packets which have a signature matching the records in the NIDS.

Two types of NIDS On-Line NIDS & Off-Line NIDS:

- On-line NIDS deals with the network in real time. It analyses the Ethernet packets and applies some rules, to decide if it is an attack or not.
- Off-line NIDS deals with stored data and passes it through some processes to decide if it is an attack or not.

Host Intrusion Detection Systems (NIDS):

Host intrusion detection systems (HIDS) run on individual hosts or devices on the network. A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator if suspicious activity is detected. It takes a snapshot of existing system files and matches it to the previous snapshot. If the critical system files were modified or deleted, an alert is sent to the administrator to investigate.

Detection method :

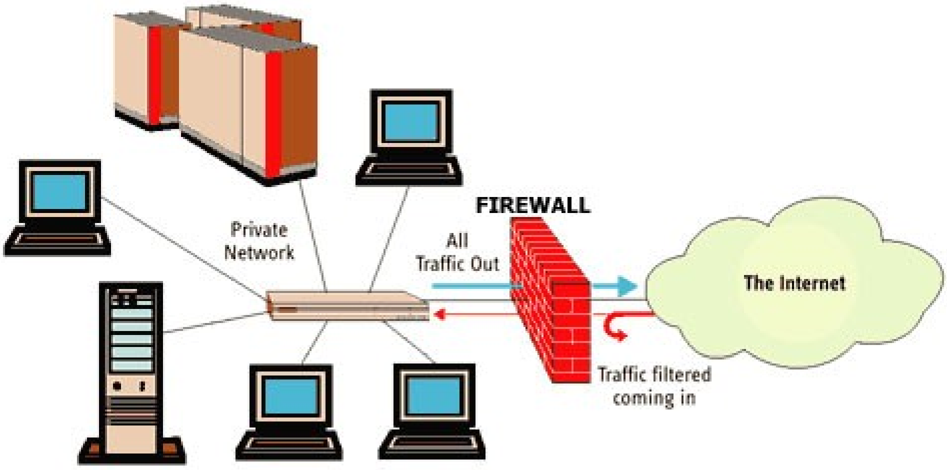
- **Signature-based:** Signature-based IDS refers to the detection of attacks by looking for specific patterns, such as byte sequences in network traffic, or known malicious instruction sequences used by malware.

- **Anomaly-based:** Anomaly-based intrusion detection systems were primarily introduced to detect unknown attacks. The basic approach is to use machine learning to create a model of trustworthy activity, and then compare new behavior against this model. Although this approach enables the detection of previously unknown attacks.

- **Rule based:** A knowledge base programmed as rules will decide the output alongside an inference engine. If the defined rules for example all match, a certain assumption can be determined in which an action may take place. This assumption is the power of the inference engine.
  e.g. If more traffic was leaving the company than usual, as well as coming from a certain server, the inference engine may assume, the server could be compromised by a hacker.

4.11 Firewalls/UTM :

Firewall :



A firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. Firewall typically establishes a barrier between a trusted, secure internal network and another outside network.

The main purpose of a firewall is to separate a secure area from a less secure area and to control communications between the two. Firewalls can perform a variety of other functions, but are chiefly responsible for controlling inbound and outbound communications on anything from a single machine to an entire network.
Network layer or packet filters: Network layer firewalls, also called packet filters, operate at a relatively low level of the TCP/IP protocol stack, not allowing packets to pass through the firewall unless they match the established rule set.

Types of Firewall:
There are two types of firewall : Hardware and Software Firewalls.

- ➔ **Hardware Firewall :**

SONICWALL
WatchGuard
paloalto NETWORKS
FORTINET
Juniper NETWORKS
STONESOFT Real World Business Security
CISCO
Check Point SOFTWARE TECHNOLOGIES LTD.

Can be purchased as a stand-alone product but are also typically found in broadband routers, and should be considered an important part of your system and network set-up. Most hardware firewalls will have a minimum of four network ports to connect other computers, but for larger networks, business networking firewall solutions are available.

Software Firewalls :

Software firewalls are installed on your computer (like any software) and you can customize it; allowing you some control over its function and protection features. A software firewall will protect your computer from outside attempts to control or gain access your computer.

Firewalls are often categorized as : Network Firewalls and Host-based Firewalls.

- **Network firewalls:** filter traffic between two or more networks; they are either software appliances running on general purpose hardware, or hardware-based firewall computer appliances. Network-based firewalls are positioned on the gateway computers of LANs, WANs and intranets.

- **Host-based firewalls:** provide a layer of software on one host that controls network traffic in and out of that single machine. Firewall appliances may also offer other functionality to the internal network they protect, such as acting as a DHCP or VPN server for that network. The host-based firewall may be a daemon or service as a part of the operating system or an agent application such as endpoint security or protection.

Network layer firewalls generally fall into two sub-categories: **Stateful** and **Stateless**:

- **Stateful :** Stateful firewalls maintain context about active sessions, and use that "state information" to speed packet processing. Any existing network connection can be described by several properties, including source and destination IP address, UDP or TCP ports, and the current stage of the connection's lifetime (including session initiation, handshaking, data transfer, or completion connection). If a packet does not match an existing connection, it will be evaluated according to the ruleset for new connections. If a packet matches an existing connection based on comparison with the firewall's state table, it will be allowed to pass without further processing.

- ➔ **Stateless :** Stateless firewalls require less memory, and can be faster for simple filters that require less time to filter than to look up a session. They may also be necessary for filtering stateless network protocols that have no concept of a session. However, they cannot make more complex decisions based on what stage communications between hosts have reached.

Firewall are often classifides as below :

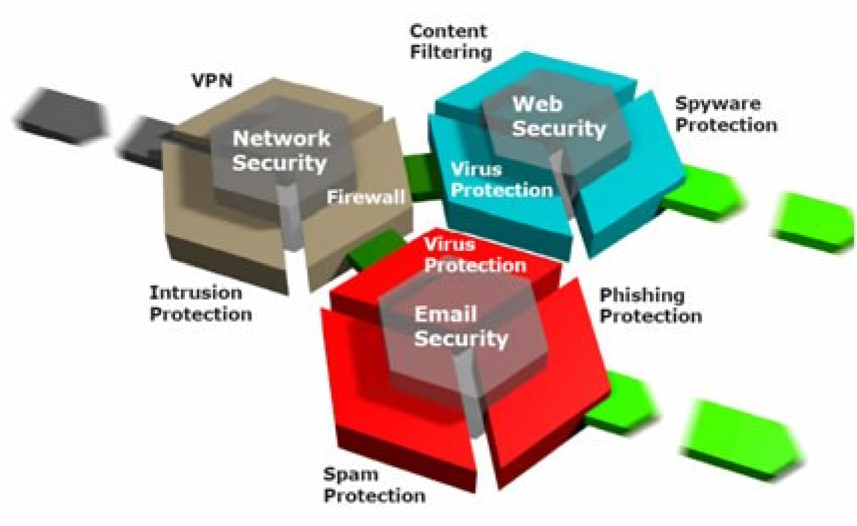
- ➔ **Application-Layer Firewall :** Application-layer firewalls work on the application level of the TCP/IP stack (i.e., all browser traffic HTTP,HTTPS, or all telnet or FTP traffic), and may intercept all packets traveling to or from an application. They block other packets (usually dropping them without acknowledgment to the sender).Application firewalls accomplish their function by filter the connections between the application layer and the lower layers of the OSI model. Also application firewalls further filter connections by examining the process ID of data packets against a rule set for the local process involved in the data transmission.

- ➔ **Proxies Firewall :** A proxy server is a gateway from one network to another for a specific network application, in the sense that it functions as a proxy on behalf of the network user. A proxy firewall prevents direct connections between either sides of the firewall; both sides are forced to conduct the session through the proxy, which can block or allow traffic based on its rule set. A proxy service must be run for each type of Internet application the firewall will support, such as an HTTP proxy for Web services.

- ➔ **Network Address Translation :** Firewalls often have network address translation (NAT) functionality, and the hosts protected behind a firewall commonly have addresses in the "private address range.Firewalls often have such functionality to hide the true address of protected hosts. Originally, the NAT function was developed to address the limited number of IPv4 routable addresses that could be used or assigned to companies or individuals as well as reduce both the amount and therefore cost of obtaining enough public addresses for every computer in an organization. Although NAT on its own is not considered a security feature, hiding the addresses of protected devices has become an often used defense against network reconnaissance.

➔ **Next-generation firewalls :** Next-generation firewalls (NGFWs) were created in response to the evolving sophistication of applications and malware. Application and malware developers have largely outwitted the long-standing port-based classification of traffic by building port evasion techniques into their programs. NGFWs act as a platform for network security policy enforcement and network traffic inspection.

UTM (Unified Threat Management) :



Essential Components of Unified Threat Management Security Solutions:

➔ **Application Control :** Application control is a next gen firewall feature that identifies and controls the applications that generate more traffic in the organizational network.

➔ **Intrusion Prevention System (IPS) :** IPS identifies the attacks that originate beyond and inside the network perimeter and protects the internal network. It offers a wide range of features including predefined/ custom signature and packet logging to detect and block malicious activities on the internal network.

- **Spam Filter :** Anti-spam technologies are an integral part of UTM systems. They detect threats by various techniques including blocking spammed IP's and spammed emails, conducting DNS look ups, IP comparison etc.

- **Antivirus filter :** Antivirus filter in UTM screens all files in a database for virus signatures and infected file patterns and provide multi layered protection against malware attacks.

- **Data Loss Prevention System (DLP) :** DLP systems incorporated in the UTM systems prevent intentional or unintentional leakage of data to and fro the organization. The filtering scans in DLP systems helps in allowing, blocking or archiving the content based on the text strings and pattern matches with the DLP data base.

Features of Unified Threat Management Solutions :

- Firewall to keep the unwanted traffic away from the organizational network.
- Online gateway security which covers virus scanning, malware scanning, checking of phishing mails with malicious attachments.
- Integrated approach which improves attack identification and reduce false positives.
- Network Intrusion Prevention system to prevent attacks on unpatched systems.
- Remote access security.
- Auto updating of latest security/ antivirus updates or features Minimal human intervention required.
- Secure wireless capabilities.
- Internal Vulnerability Scanning.
- Web Content Filtering.
- Web & Email Anti-Virus.
- Virtual Private Networking.

5. Referrence :

➔ http://www.cisco.com/c/en/us/products/security/what-is-network-security.html

➔ https://www.tutorialspoint.com/information_security_cyber_law/network_security.htm

➔ https://en.wikipedia.org

➔ https://blog.malwarebytes.com/101/2015/12/how-does-anti-malware-work/

➔ https://digitalguardian.com

➔ http://www.computerhope.com