Government Polytechnic Ahmedabad
Program: Diploma in Computer Engg
Computer and Network Security
(3350704-C304)
UNIT_4

NETWORK SECURITY

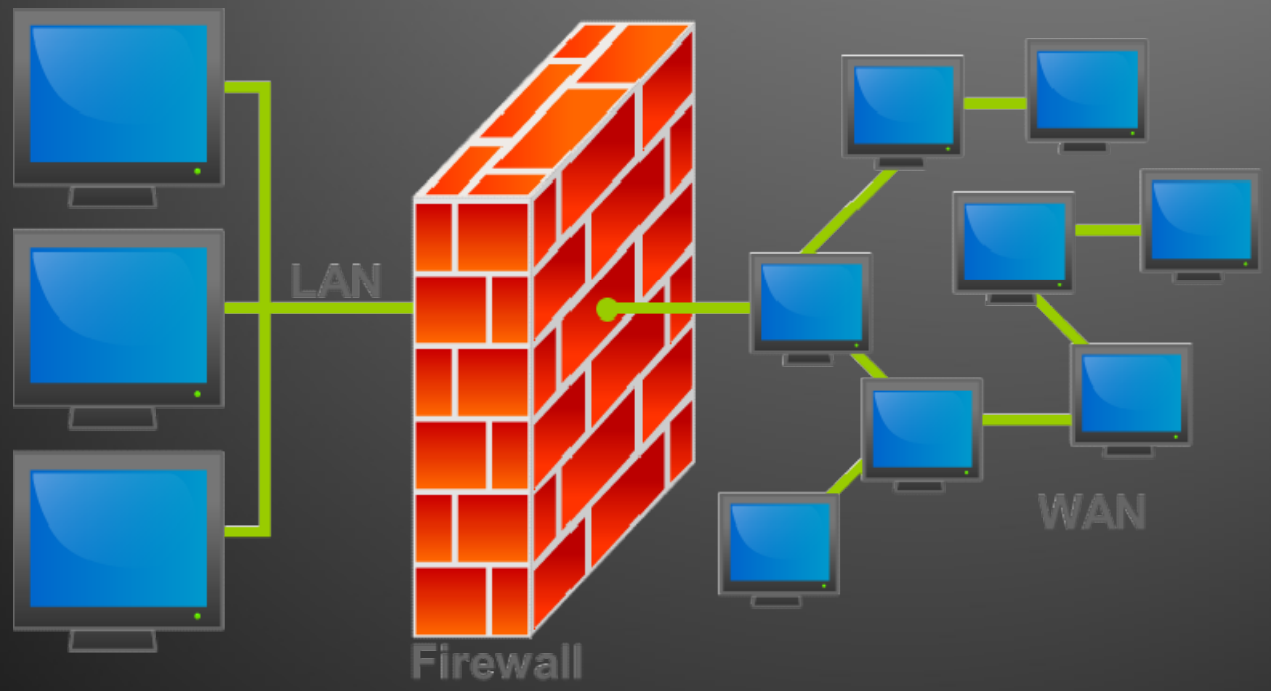
4.1 FIRE WALL

- A firewall is a device (or software feature) designed to control the flow of traffic into and out-of a network.
- In general, firewalls are installed to prevent attacks.
- Firewalls can be either hardware or software
- It provides following facilities:
  1) Block incoming network traffic
  2) Block out going network traffic
  3) Make internal resources available
  4) Allow connections to internal networks
  5) Report on Network traffic & firewall activities

Cont..

- A firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules.
- Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.

FIRE WALL



TYPES OF FIREWALL

1) Packet filters
2) Circuit level gateways
3) Application level gateways
4) Stateful multilayer inspection firewalls

1) PACKET FILTERS

- On the Internet, packet filtering is the process of passing or blocking packets at a network interface based on source and destination addresses, ports, or protocols.
- The process is used in conjunction with packet mangling and Network Address Translation (NAT).
- Packet filtering is often part of a firewall program for protecting a local network from unwanted intrusion.
- Packet filtering firewall works at Network Layer of OSI model or IP Layer of TCP/IP

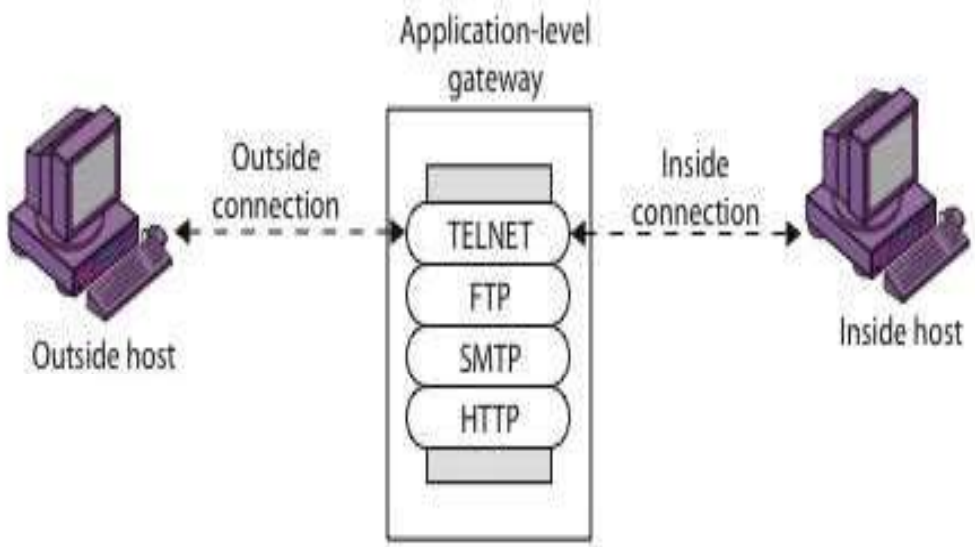
2) CIRCUIT LEVEL GATEWAYS

- It works at Session Layer of OSI model or TCP Layer of TCP/IP
- Monitors TCP handshaking between packets.
- Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.
- It is useful for hiding information about protected networks

3) APPLICATION LEVEL GATEWAYS

- Also called Proxies, similar to circuit-level gateway except that they are application specific.
- It works at Application Layer of OSI model
- It has full access to protocol
  - user requests service from proxy
  - proxy validates request as legal
  - then actions request and returns result to user
- Need separate proxies for each service
  - E.g., SMTP (E-Mail)
  - NNTP (Net news)
  - DNS (Domain Name System)
  - NTP (Network Time Protocol)
  - custom services generally not supported

APPLICATION LEVEL GATEWAYS



(b) Application-level gateway

4) STATEFUL MULTILAYER INSPECTION FIREWALLS

- It combines the aspects of the other three types of firewall.
- They filter packets at Network Layer, determine whether session packets are legitimate and evaluate contents of packet at the application layer.
- It allows direct connection between client & host.
- It offer
  - high level of security,
  - good performance,
  - transparency to end users.

KERBEROS AUTHENTICATION

- Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography.
- It has the following characteristics:
- It is secure: it never sends a password unless it is encrypted.
- Only a single login is required per session. Credentials defined at login are then passed between resources without the need for additional logins.
- The concept depends on a trusted third party – a Key Distribution Center (KDC). The KDC is aware of all systems in the network and is trusted by all of them.
- It performs mutual authentication, where a client proves its identity to a server and a server proves its identity to the client.

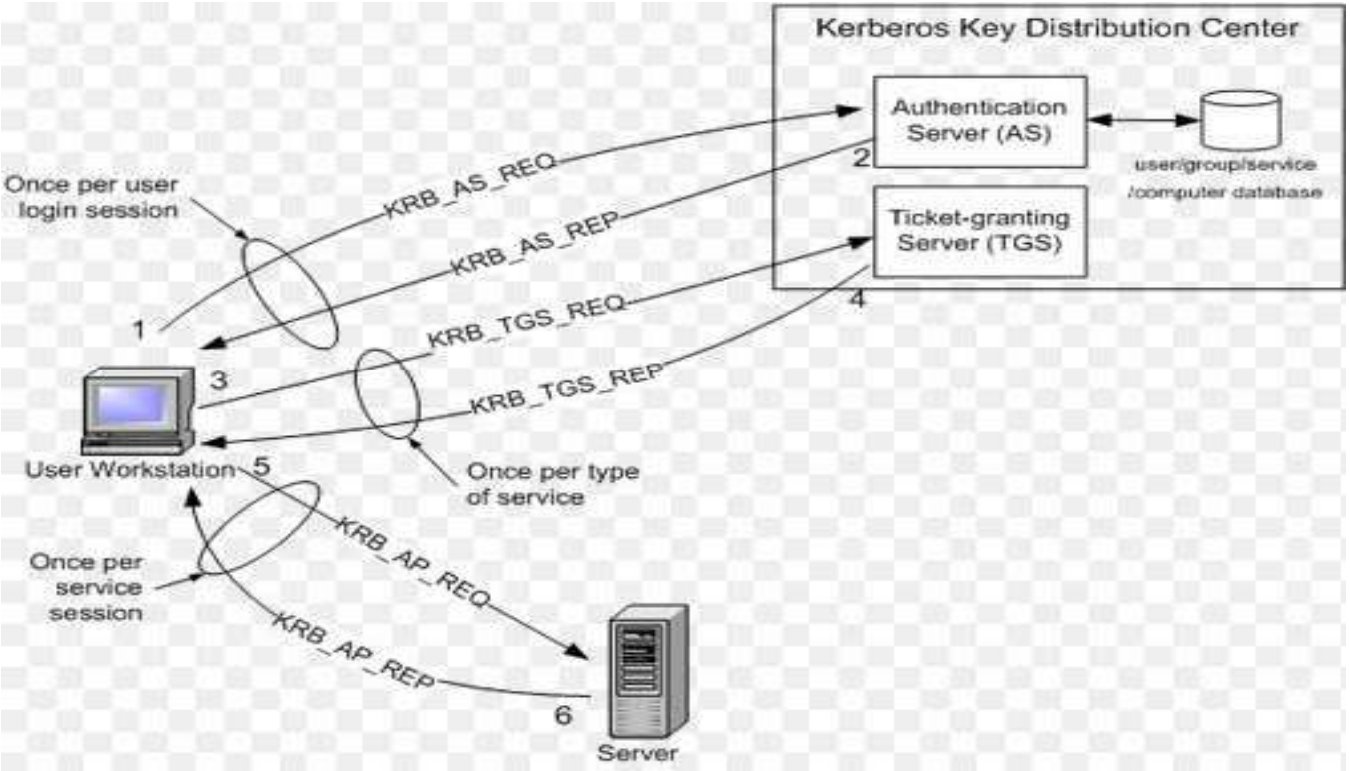
KERBEROS AUTHENTICATION

- Ticket-Granting Server (TGS): A client that wishes to use a service has to receive a ticket – a time-limited cryptographic message – giving it access to the server.
- Authentication Server (AS) :to verify clients
- Steps:

Step 1: The user logs on to the workstation and requests service on the host. The workstation sends a message to the Authorization Server requesting a ticket granting ticket (TGT).

Step 2: The Authorization Server verifies the user's access rights in the user database and creates a TGT and session key. The Authorization Sever encrypts the results using a key derived from the user's password and sends a message back to the user workstation.

KERBEROS AUTHENTICATION



KERBEROS AUTHENTICATION

Step 3: When the user wants access to a service, the workstation client application sends a request to the Ticket Granting Service containing the client name, realm name and a timestamp. The user proves his identity by sending an authenticator encrypted with the session key received in Step 2.

Step 4: The TGS decrypts the ticket and authenticator, verifies the request, and creates a ticket for the requested server. The ticket contains the client name and optionally the client IP address. It also contains the realm name and ticket lifespan. The TGS returns the ticket to the user workstation. The returned message contains two copies of a server session key – one encrypted with the client password, and one encrypted by the service password.

KERBEROS AUTHENTICATION

Step 5: The client application now sends a service request to the server containing the ticket received in Step 4 and an authenticator. The service authenticates the request by decrypting the session key. The server verifies that the ticket and authenticator match, and then grants access to the service. This step as described does not include the authorization performed by the Intel AMT device, as described later.

Step 6: If mutual authentication is required, then the server will reply with a server authentication message.

4.2 SECURITY TOPOLOGIES- SECURITY ZONES

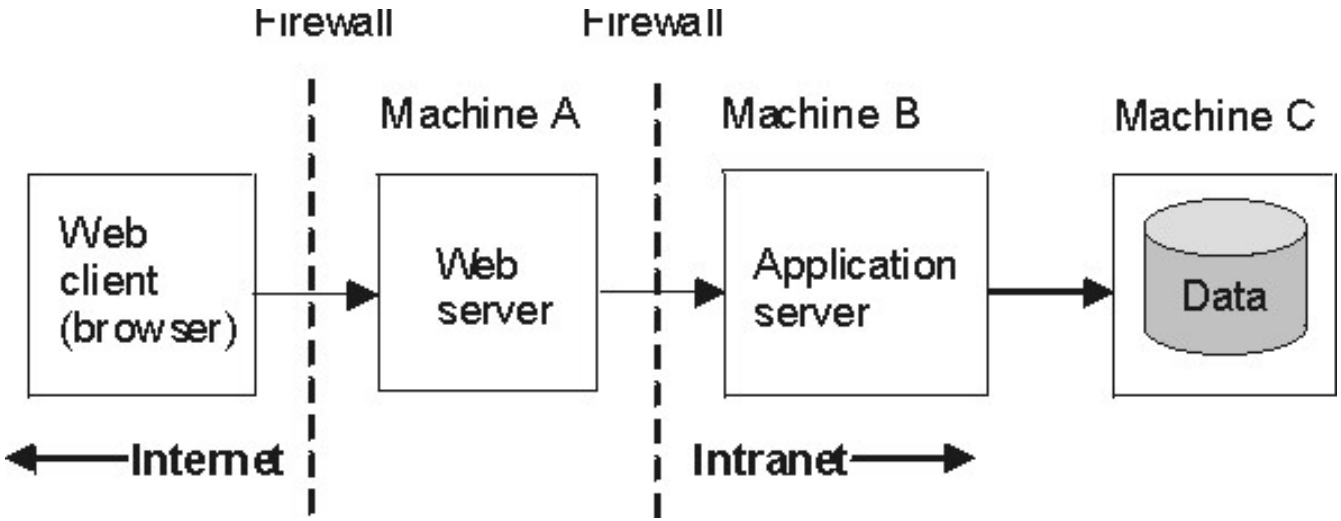
1) DMZ
2) Internet Zone
3) Intranet Zone

DMZ–DEMILITARIZED ZONE

- DMZ means - what is essentially a buffer between the internet and the internal network.
- It is separated by an *outer firewall* on the internet facing side of the DMZ and an *inner firewall* on the internal network side of the DMZ.
- Any devices placed within the DMZ are accessible from both the internet and the internal network.
- There is no communication, however, from the internet directly though the DMZ to the internal network.
- Any systems placed in the DMZ must be configured to the highest level of security possible .
- These systems should always be considered to be compromised and must never be given direct and unrestricted access to the inner network.
- Servers placed in the DMZ are: web, ftp, email and remote access servers.

DMZ–Demilitarized Zone

- A typical DMZ configuration includes:
  - Outer firewall b/t the Internet and the Web Server processing the requests originating on the company Web site.
  - Inner firewall b/t the Web Server and the appl. Server to which it is forwarding requests. Date resides behind this.



INTERNET ZONE

- The internet is the name given to the entire public network which provides the infrastructure for the transfer of data between remote points.
- Such data can take the form of email, web pages, files, multi-media and just about anything else that exists in digital form.
- Every computer in internet is identified by IP Address.
- A Special computer DNS is used to give name to the IP address.

INTRANET ZONE:

- An intranet can be described as a mini-internet build within the safety of a secure networking environment.
- Intranets are typically used to provide internal corporate web sites for employee only access. Because the intranet servers have internal, private IP addresses and reside behind firewalls they are generally not accessible to the outside world.
- If external access is needed to an intranet this is best achieved through the implementation of a Virtual Private Network (VPN).

Extranet

- An extranet is an extension of a selected portion of a company's intranet to external partners.
- This allows a business to share information with customers, suppliers, partners, and other trusted groups while using a common set of Internet protocols to facilitate operations.
- Extranets can use public networks to extend their reach beyond a company's own internal network, and some form of security, typically VPN, is used to secure this channel.

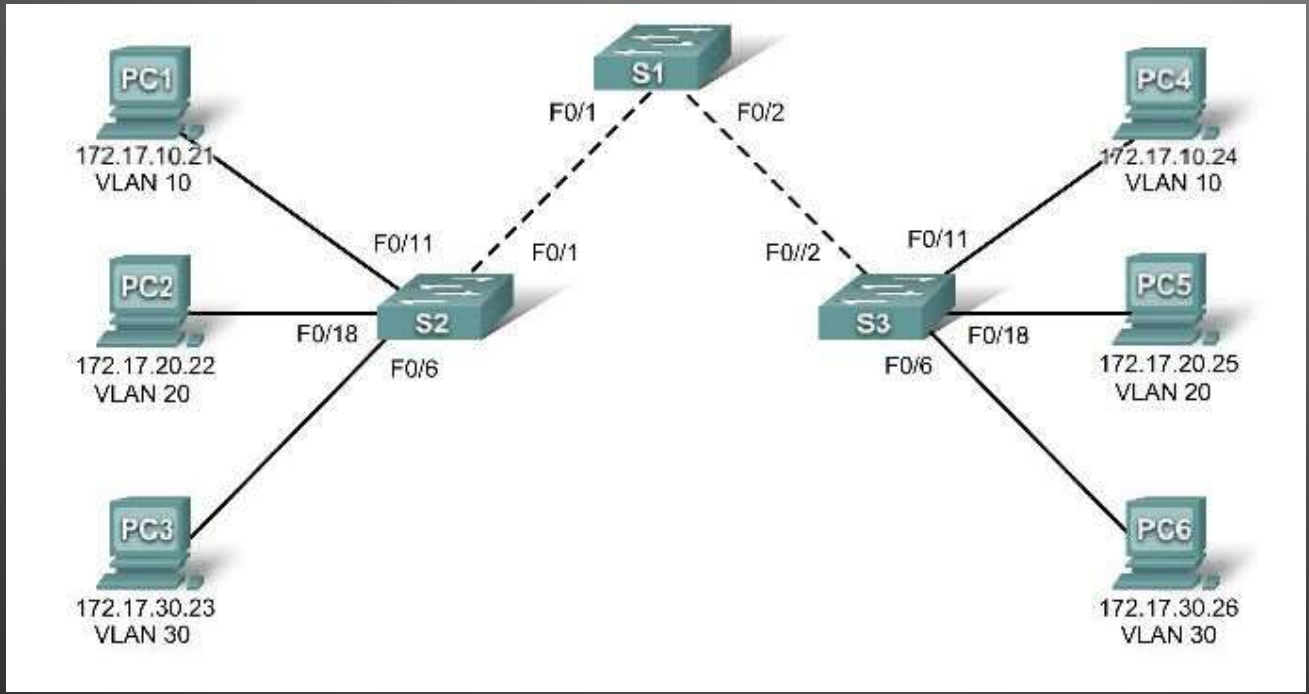
Cont…

- The use of the term extranet implies both privacy and security. Privacy is required for many communications, and security is needed to prevent unauthorized use and events from occurring.
- Proper firewall management, remote access, encryption, authentication, and secure tunnels across public networks are all methods used to ensure privacy and security for extranets.

VLAN

- Virtual local area networks
  - A way of dividing a single physical network switch among multiple network segments or broadcast domains.
  - Ability to configure multiple LANs on a single switch
- Trunk – allows switches to share many VLANs over a single physical link
- Routers needed to make different VLANs talk

VLAN

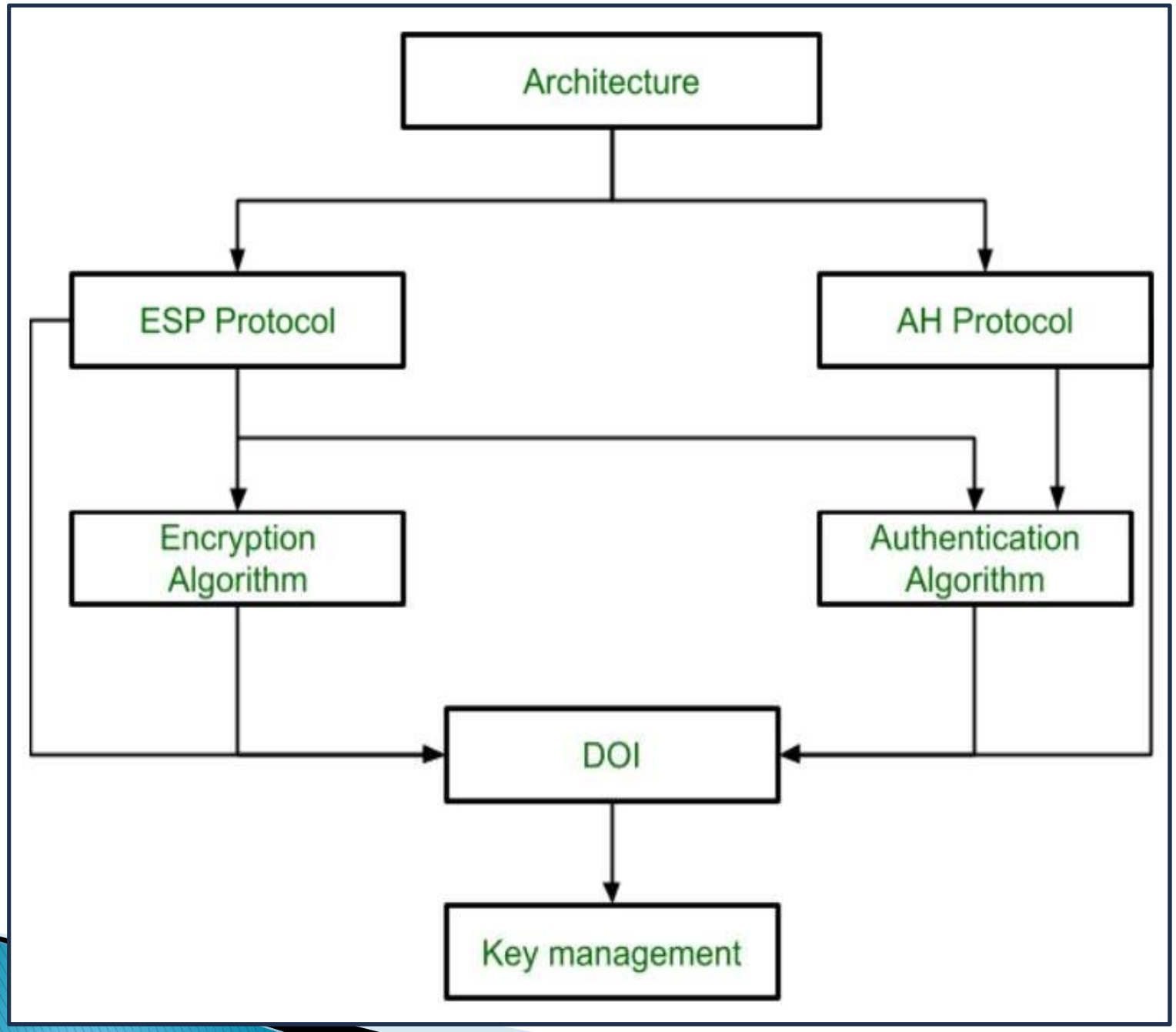

PC1
172.17.10.21
VLAN 10
PC2
172.17.20.22
VLAN 20
PC3
172.17.30.23
VLAN 30
S1
F0/1
F0/2
F0/11
F0/1
F0/18
S2
F0/6
F0//2
F0/11
S3
F0/18
F0/6
PC4
172.17.10.24
VLAN 10
PC5
172.17.20.25
VLAN 20
PC6
172.17.30.26
VLAN 30

IP Security

- Internet Protocol Security is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network. It is used in virtual private networks.
- It also defines the encrypted, decrypted and authenticated packets. The protocols needed for secure key exchange and key management are defined in it.
- IPsec is developed to ensure the integrity, confidentiality and authentication of data communications over an IP network.

IPsec Architecture

- IPSec architecture uses two protocols to secure the traffic or data flow. These protocols are ESP (Encapsulation Security Payload) and AH (Authentication Header). IPSec Architecture include protocols, algorithms, DOI, and Key Management.
- All these components are very important in order to provide the three main services:
- Confidentiality
- Authentication
- Integrity


Architecture
ESP Protocol
AH Protocol
Encryption Algorithm
Authentication Algorithm
DOI
Key management

- 1. Architecture:
  Architecture or IP Security Architecture covers the general concepts, definitions, protocols, algorithms and security requirements of IP Security technology.
- 2. ESP Protocol:
  ESP(Encapsulation Security Payload) provide the confidentiality service. Encapsulation Security Payload is implemented in either two ways:
  - ESP with optional Authentication.
  - ESP with Authentication.
- 3. Encryption algorithm:
  Encryption algorithm is the document that describes various encryption algorithm used for Encapsulation Security Payload.

4. AH Protocol:
AH (Authentication Header) Protocol provides both Authentication and Integrity service. Authentication Header is implemented in one way only: Authentication along with Integrity.

5. Authentication Algorithm:
Authentication Algorithm contains the set of the documents that describe authentication algorithm used for AH and for the authentication option of ESP.

6. DOI (Domain of Interpretation):
DOI is the identifier which support both AH and ESP protocols. It contains values needed for documentation related to each other.

7. Key Management:
Key Management contains the document that describes how the keys are exchanged between sender and receiver.

Modes of IPsec

The IPsec protocols AH and ESP can be implemented in a host-to-host transport mode, as well as in a network tunneling mode.

- Transport mode

In transport mode, only the payload of the IP packet is usually encrypted or authenticated. The transport and application layers are always secured by a hash, so they cannot be modified in any way, for example by translating the port numbers.

- Tunnel mode

In tunnel mode, the entire IP packet is encrypted and authenticated. It is then encapsulated into a new IP packet with a new IP header.

Email Security

- Email security is the term for any procedure that protects email content and accounts against unauthorized access.
- 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:

1. Strong passwords
2. Password rotations
3. Spam filters
4. Desktop-based anti-virus/anti-spam applications

Follow essential security measures to keep email safe and secure

1. The Best Email Security, Use strong passwords that are unique.
2. Watch out for phishing emails.
3. Use spam filters and anti-virus software.
4. Do not let employees use company email addresses for private messages.
5. Always report spam mails.
6. Double-check the recipient, every time - especially on mailing lists.
7. Never open attachments or click on links in email messages from unknown senders.
8. Avoid accessing company email from public Wi-Fi connections.

SPAM AND MALICIOUS CODE

1. Spam : It is irrelevant or unsolicited messages sent over the Internet, typically to a large number of users, for the purposes of advertising, phishing, spreading malware, etc.
2. Malicious code: Malicious code is the term used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system. Malicious code is an application security threat that cannot be efficiently controlled by conventional antivirus software alone.

EMAIL ENCRYPTION

- **Email encryption involves encrypting**, or disguising, the content of **email messages** in order to protect potentially sensitive information from being read by anyone other than intended recipients.
- **Steps:**
- Encrypt all outgoing messages
- On the Tools menu, click Trust Center, and then click E-mail Security.
- Under Encrypted e-mail, select the Encrypt contents and attachments for outgoing messages check box.
- To change additional settings, such as choosing a specific certificate to use, click Settings.
- Click OK twice.

What is Malware ?

- Malware is the collective name for a number of malicious software variants, including viruses , Ransomware and spyware. Shorthand for malicious software, malware typically consists of code developed by cyber attackers, designed to cause extensive damage to data and systems or to gain unauthorized access to a network. Malware is typically delivered in the form of a link or file over email and requires the user to click on the link or open the file to execute the malware. Malware has actually been a threat to individuals and organizations since the early 1970s when the Creeper virus first appeared. Since then, the world has been under attack from hundreds of thousands of different malware variants, all with
- the intent of causing the most disruption and damage as possible.

What Can Malware Do ?

- Malware delivers its payload in a number of different ways. From demanding a ransom to stealing sensitive personal data, cybercriminals are becoming more and more sophisticated in their methods. The following is a list of some of the more common malware types and definitions.

- **Types of Malware:**

1. **Virus**
   Possibly the most common type of malware, viruses attach their malicious code to clean code and wait for an unsuspecting user or an automated process to execute them. Like a biological virus, they can spread quickly and widely, causing damage to the core functionality of systems, corrupting files and locking users out of their computers. They are usually contained within an executable file.
2. **Worms**
   Worms get their name from the way they infect systems. Starting from one infected machine, they weave their way through the network, connecting to consecutive machines in order to continue the spread of infection. This type of malware can infect entire networks of devices very quickly.
3. **Spyware**
   Spyware, as its name suggests, is designed to spy on what a user is doing. Hiding in the background on a computer, this type of malware will collect information without the user knowing, such as credit card details, passwords and other sensitive information.
4. **Trojans**
   Just like Greek soldiers hid in a giant horse to deliver their attack, this type of malware hides within or disguises itself as legitimate software. Acting discretely, it will breach security by creating backdoors that give other malware variants easy access.
5. **Ransomware**
   Also known as scareware, ransomware comes with a heavy price. Able to lockdown networks and lock out users until a ransom is paid, ransomware has targeted some of the biggest organizations in the world today — with expensive results.

How Does Malware Spread ?

Each type of malware has its own unique way of causing havoc, and most rely on user action of some kind. Some strains are delivered over email via a link or executable file. Others are delivered via instant messaging or social media. Even mobile phones are vulnerable to attack. It is essential that organizations are aware of all vulnerabilities so they can lay down an effective line of defense.

How to Protect Against Malware ?

Now that you understand a little more about malware and the different flavors it comes in, let's talk about protection. There are actually two areas to consider where protection is concerned: protective tools and user vigilance. The first is often the easiest to implement, simply because you can often set and forget best-in-class protective software that manages and updates itself. Users, on the other hand, can be prone to temptation ("check out this cool website!") or easily led by other emotions such as fear ("install this antivirus software immediately"). Education is key to ensure users are aware of the risk of malware and what they can do to prevent an attack.

Virus: A computer virus, much like a flu virus, is designed to spread from host to host and has the ability to replicate itself. Similarly, in the same way that flu viruses cannot reproduce without a host cell, computer viruses cannot reproduce and spread without programming such as a file or document. In more technical terms, a computer virus is a type of malicious code or program written to alter the way a computer operates and is designed to spread from one computer to another. A virus operates by inserting or attaching itself to a legitimate program or document that supports macros in order to execute its code. In the process, a virus has the potential to cause unexpected or damaging effects, such as harming the system software by corrupting or destroying data.

Types of viruses:

1. **File infector viruses** – A virus that attached itself to an executable program. It is also called a parasitic virus which typically infects file with .exe or .com extensions. Some file infectors can overwrite host files and others can damage your hard drive's formatting.
2. **Boot sector viruses** – These viruses are once common back when computers are booted from floppy disks. Today, these viruses are found distributed in forms of physical media such as external hard drives or USB. If the computer is infected with a boot sector virus, it automatically loads into the memory enabling control of your computer.
3. **Multi-partite viruses** – A type of virus that is very infectious and can easily spread on your computer system. It can infect multiple parts of a system including memory, files, and boot sector which makes it difficult to contain.
4. **Macro viruses** – This type of virus is commonly found in programs such as Microsoft Word or Excel. These viruses are usually stored as part of a document and can spread when the files are transmitted to other computers, often through email attachments.

5. **Master boot record viruses** – A boot sector virus is a type of virus that infects the boot sector of floppy disks or the Master Boot Record (MBR) of hard disks (some infect the boot sector of the hard disk instead of the MBR). The infected code runs when the system is booted from an infected disk, but once loaded it will infect other floppy disks when accessed in the infected computer. While boot sector viruses infect at a BIOS level, they use DOS commands to spread to other floppy disks. For this reason, they started to fade from the scene after the appearance of Windows 95 (which made little use of DOS instructions). Today, there are programs known as 'boot kits' that write their code to the MBR as a means of loading early in the boot process and then concealing the actions of malware running under Windows. However, they are not designed to infect removable media.

logic bomb :

- A logic bomb, sometimes referred to as slag code, is a string of malicious code used to cause harm to a network when the programmed conditions are met.
- The term comes from the idea that a logic bomb “explodes” when it is triggered by a specific event. Events could include a certain date or time, a particular record being deleted from a system or the launching of an infected software application.
- The level of destruction caused by a logic bomb can vary greatly and the set of conditions able to set one off is unlimited.
- Common malicious actions that logic bombs are able to commit include data corruption file deletion or hard Drive clearing.
- Unlike other forms of malware that break into a secure system, logic bomb attacks tend to be cyber sabotage from a person within an organization who has access to sensitive data.
- One way that employees might exact revenge on a company if they believe they might be fired is to create a logic bomb that they diffuse each day, and that they alone are the only ones capable of putting off.
- That way, once they are no longer with the organization, the attack can begin, either instantly or after a pre-determined time period.

How logic bombs work :

- Logic bombs are secretly inserted into a computer network through the use of malicious code. The code can be inserted into the computer's existing software or into other forms of malware such as viruses worms or trojan horses. It then lies dormant, and typically undetectable, until the trigger occurs. Triggers can be categorized as positive or negative. Logic bombs with positive triggers happen after a condition is met, such as the date of a major company event. Negative triggers initiate a logic bomb when a condition is not met, such as an employee fails to enter the diffuse code by a certain time. Either way, when the conditions become true, the logic bomb will go off and inflict its programmed damage.