Chapter 4

Network security

4.1 firewalls

4.2 security topologies-security zones

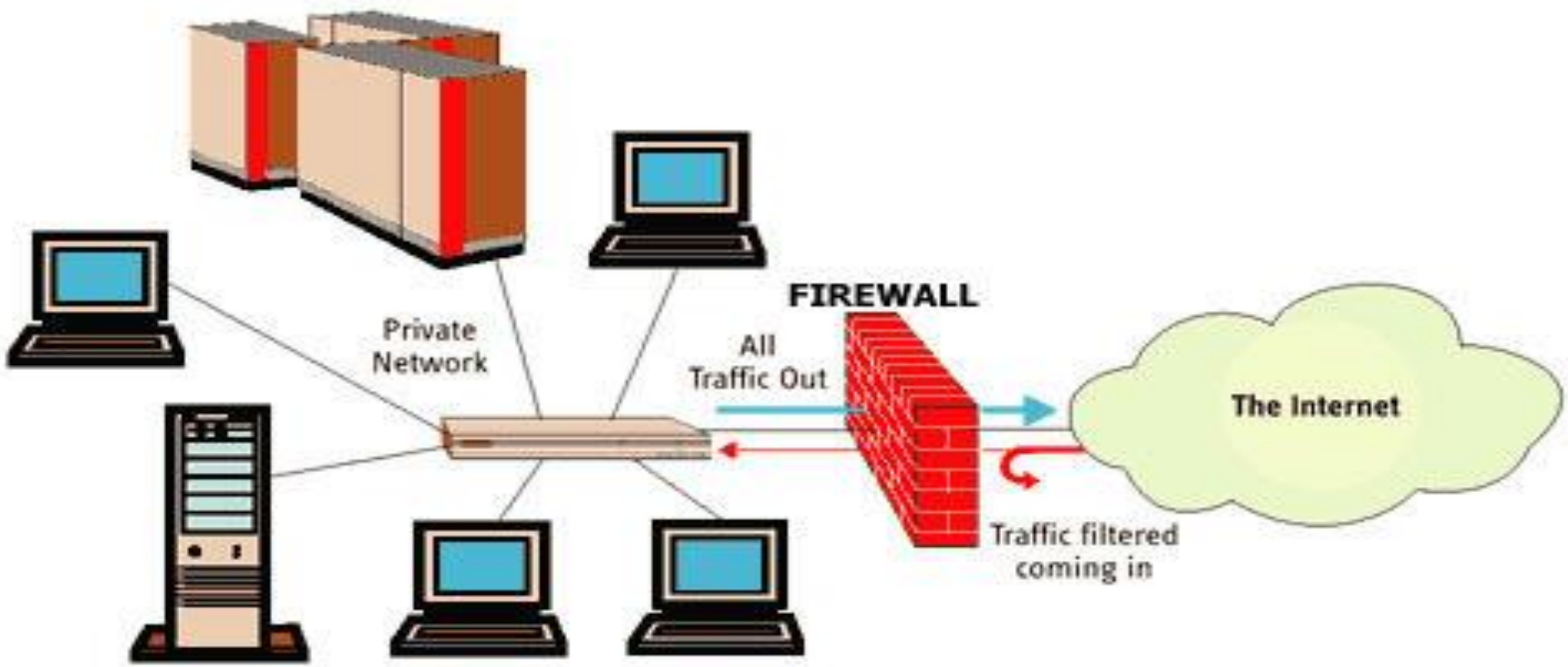
4.3 IP security

4.4 Email security

FIREWALL

- It is a network security designed for controlling or monitoring the incoming and outgoing network traffic based on some predefined rules.
- Its typically acts as a barrier between a trusted internal network and untrusted external network, such as the Internet.
- It is used for prevent from attacks.

FIREWALL


Private
Network
FIREWALL
All
Traffic Out
The Internet
Traffic filtered
coming in

TYPES OF FIREWALL

- **TYPES OF FIREWALL**
- 1) Packet filters
- 2) Circuit level gateways
- 3) Application level gateways
- **Packet filters**
- It is a firewall technique used to control network access by monitoring outgoing and incoming packets and allowing them to pass or stop based on the source and destination Internet Protocol (IP) addresses, protocols and ports .

Packet-filtering

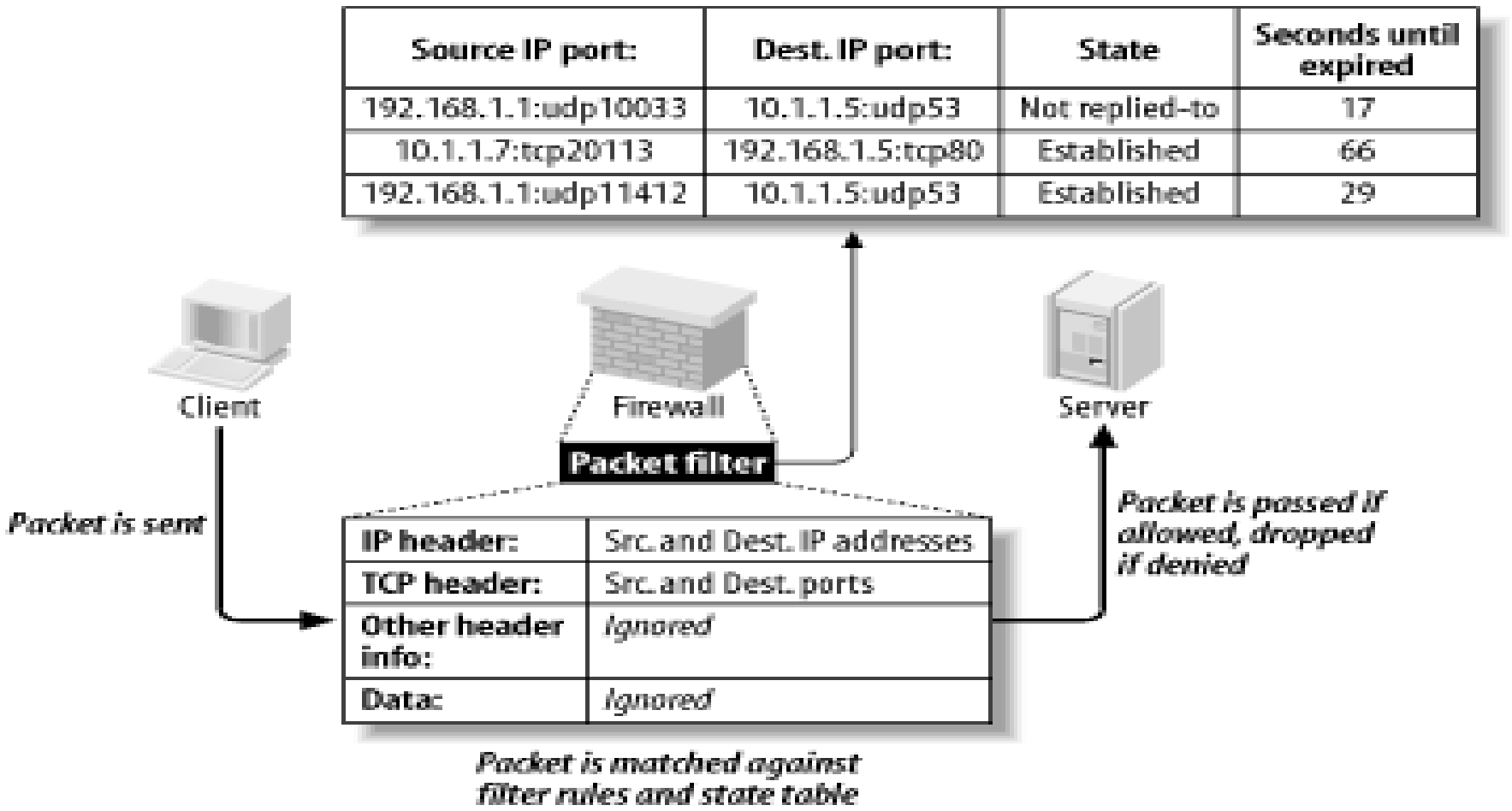
- It is also known as static filtering.
- During network communication, when a node transmits a packet that is filtered and matched with predefined rules and policies. Once matched, then a packet is either accepted or denied.
- Packet filtering firewall works at Network Layer of OSI model or IP Layer of TCP/IP.

❑**Packet-filtering firewalls have two main advantages**:

- They can process packets at very fast speeds.
- They easily can match on most fields in Layer 3 packets and Layer 4 segment headers, providing a lot of flexibility in implementing security policies.

❑**Packet-filtering firewalls have these disadvantages:**

- Complex to configure.
- Cannot prevent application-layer attacks.
- Susceptible to certain types of TCP/IP protocol attacks.
- Do not support user authentication of connections.
- Having limited logging capabilities.

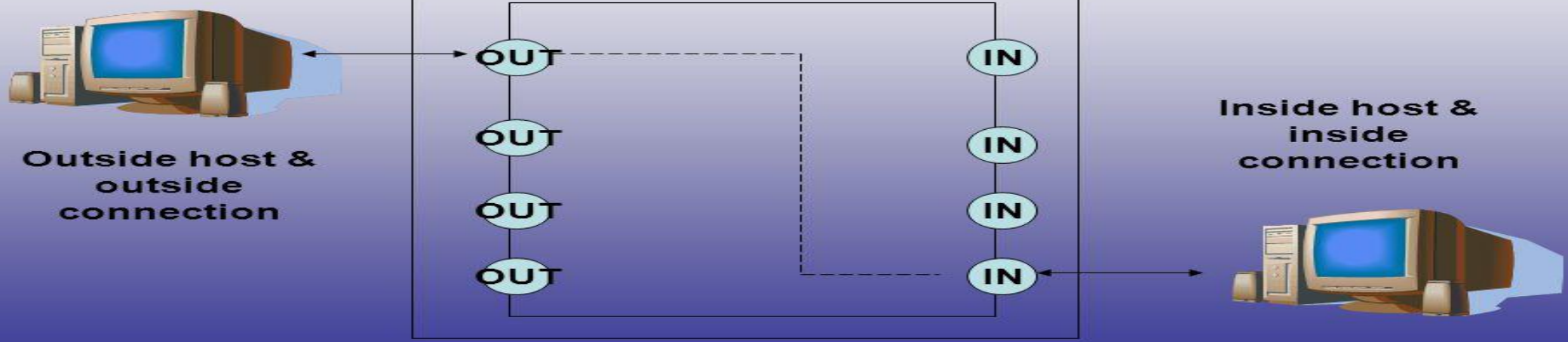

Source IP port:
Dest. IP port:
State
Seconds until expired
192.168.1.1:udp10033
10.1.1.5:udp53
Not replied-to
17
10.1.1.7:tcp20113
192.168.1.5:tcp80
Established
66
192.168.1.1:udp11412
10.1.1.5:udp53
Established
29
Client
Firewall
Server
Packet filter
Packet is sent
Packet is passed if allowed, dropped if denied
IP header:
Src. and Dest. IP addresses
TCP header:
Src. and Dest. ports
Other header info:
Ignored
Data:
Ignored
Packet is matched against filter rules and state table

Circuit level gateways

- A circuit-level gateway is a firewall that provides User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) connection security, and works between an OSI network model's transport and application layers such as the session layer.
- Monitors TCP handshaking between packets

Circuit Level Gateway

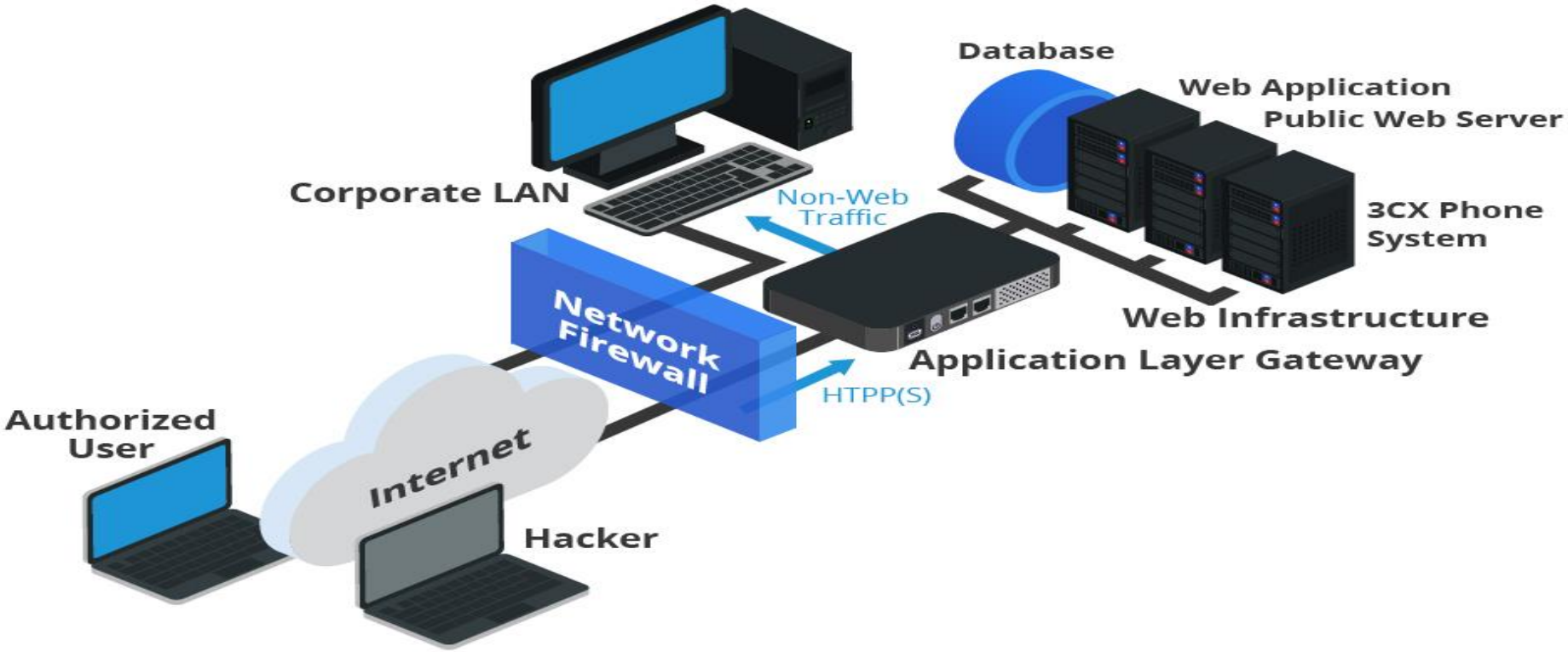
- Circuit Level Gateway.



Application Level Gateways

- **It** is also known as a proxy server
- Check data / payload
- **Working:**
- An internal user contacts the application gateways using a TCP/IP application ,such as HTTP or TELNET .
- The application gateways asks the user about the remote host with which the user wants to setup a connection for actual communication (its DNS and IP address).
- The application gateway also asks for the user id and the password required to access the services of the application gateway.

CONTD…


Database
Web Application
Public Web Server
Corporate LAN
Non-Web
Traffic
3CX Phone
System
Network
Firewall
Web Infrastructure
Application Layer Gateway
HTPP(S)
Authorized
User
Internet
Hacker

KERBEROS

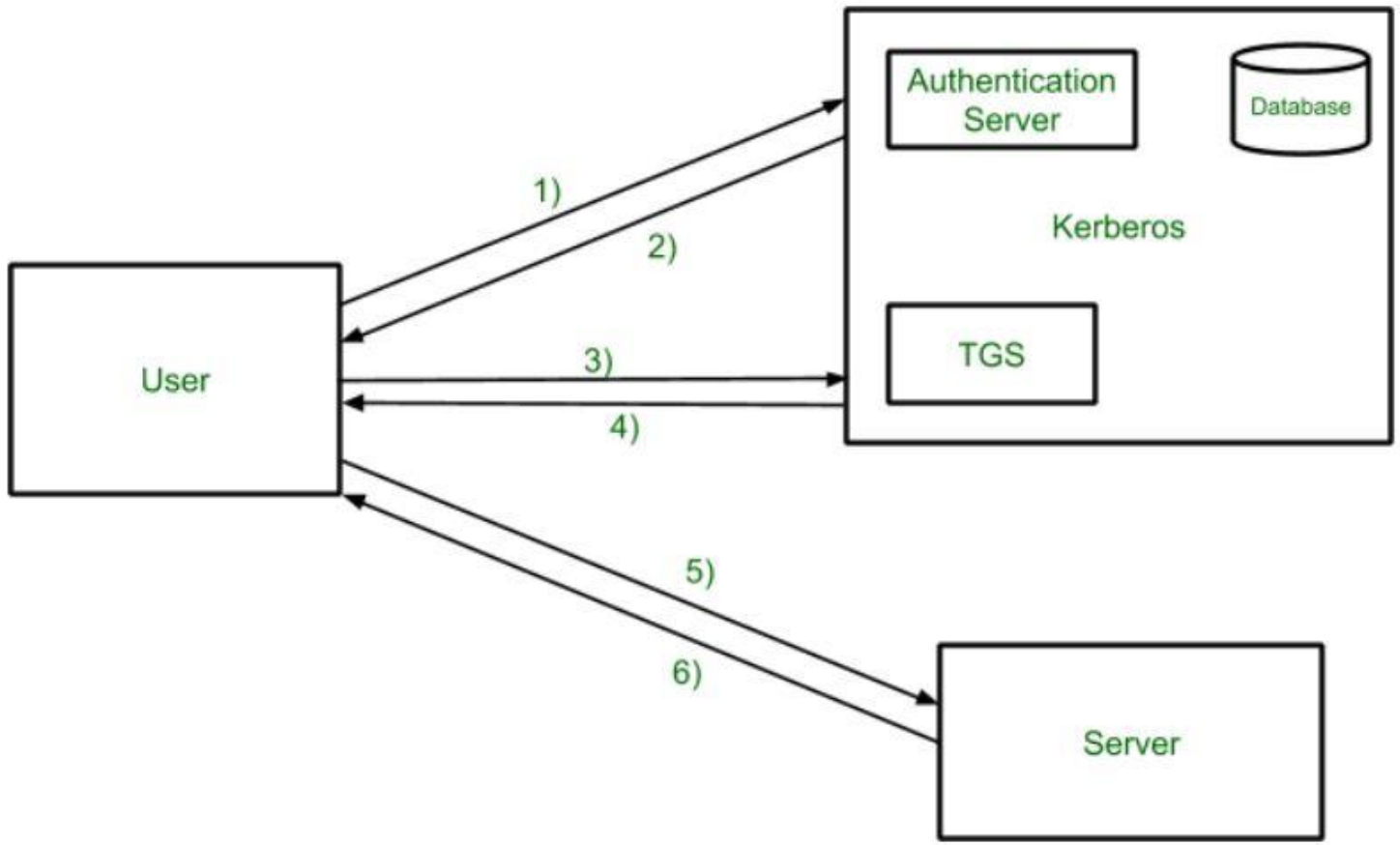
KERBEROS AUTHENTICATION

- It is a computer n/w validation convention which deals with the premise of "Ticket" to allow nodes to communicate over a non secure n/w to prove their identity to one another in a secure manner .

1.Client server model

2.Symmetric key model

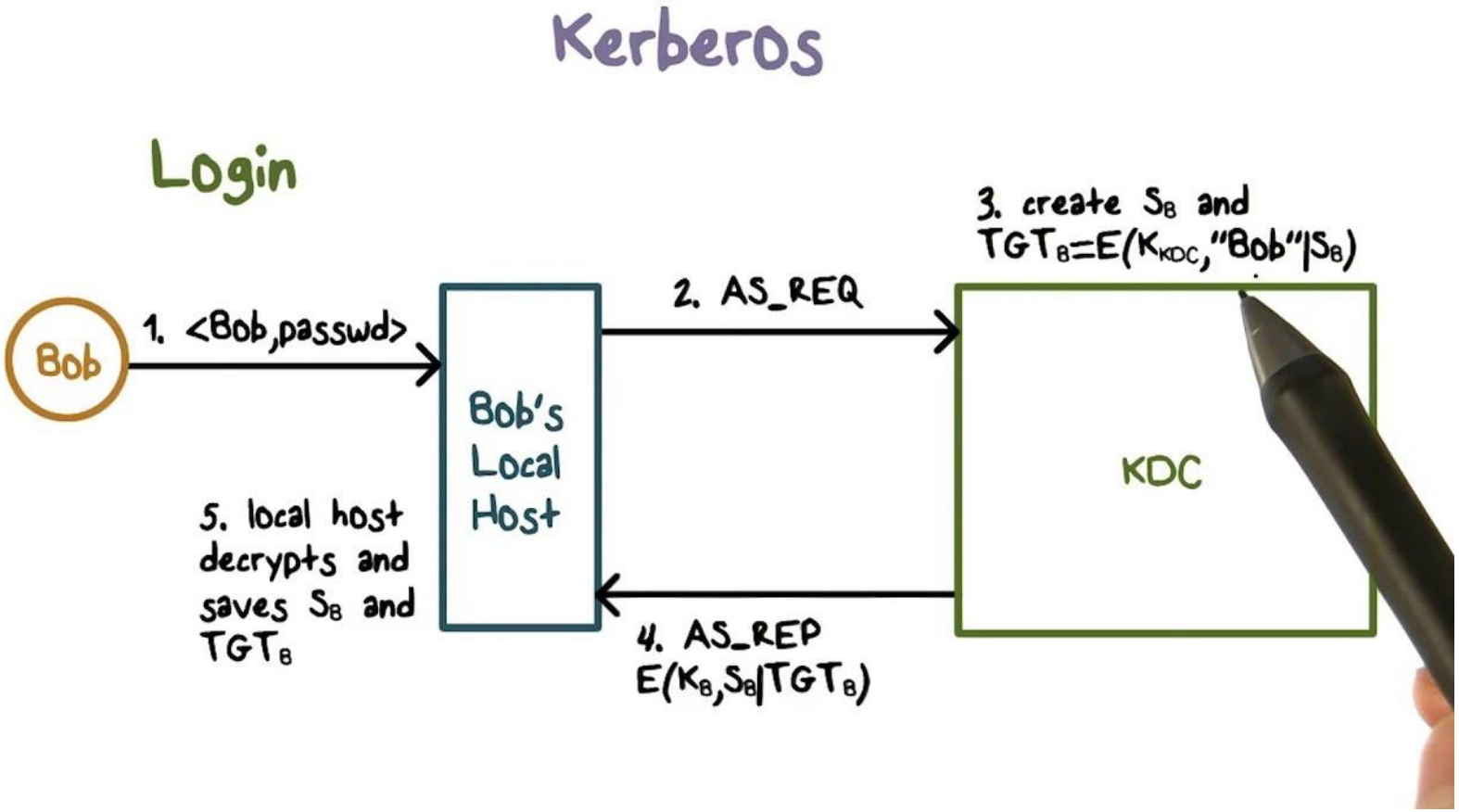
3.Key distribution centre


Authentication Server
Database
Kerberos
TGS
User
1)
2)
3)
4)
5)
6)
Server

- **Step-1:**
- first User login from any workstation and request services on host. Thus user request for ticket-granting-service.
- **Step-2:**
- Authentication Server(AS) verifies user's access right using database and then gives ticket-granting-ticket and session key. Results are encrypted using Password of user(using symmetric key that the AS shares with TGS).
- **Step-3:**
- Decryption of message is done using the password then send the ticket to Ticket Granting Server. The Ticket contain authenticators like user name and network address.

- **Step-4**
- Ticket Granting Server decrypts the ticket send by User and authenticator verifies the request then creates the ticket for requesting services from the Server.
- **Step-5:**
- User send the Ticket and Authenticator to the Server.
- **Step-6:**
- Server verifies the Ticket and authenticators then generate the access to the service. After this User can access the services.

CONTD...


Kerberos
Login
Bob
1. <Bob,passwd>
Bob's Local Host
2. AS_REQ
3. create S_B and $TGT_B = E(K_{KDC}, "Bob" | S_B)$
KDC
4. AS_REP $E(K_B, S_B | TGT_B)$
5. local host decrypts and saves S_B and TGT_B

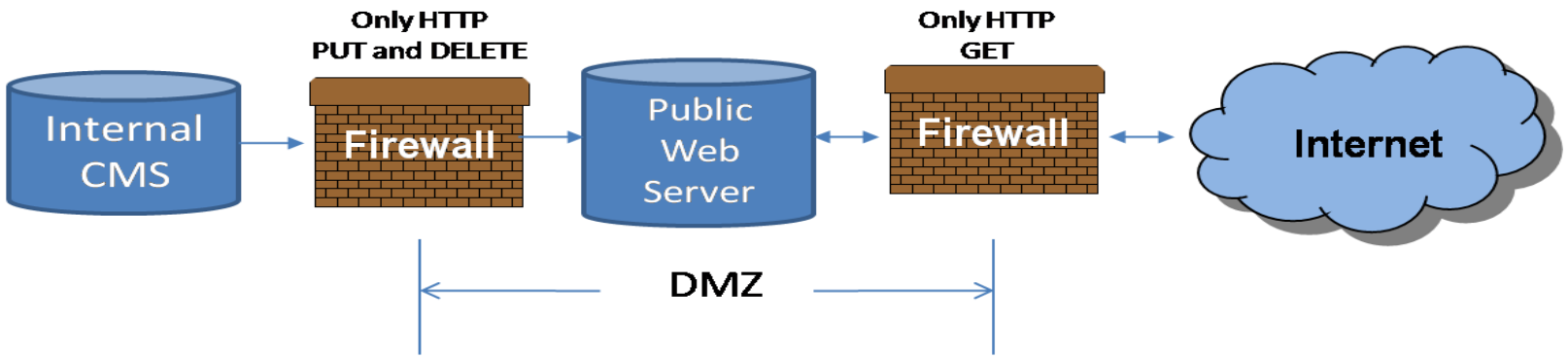
SECURITY TOPOLOGIES

- **SECURITY TOPOLOGIES**
- DMZ
- Internet Zone
- Intranet Zone
- VLAN

- **DMZ**
- This is a zone where services are placed to allow outside users from the internet and internal users to access them .
- Any devices placed within the DMZ are accessible from both the internet and the internal network.

DMZ

- It prevents outside users to from getting direct access to a server that has company data .Any systems placed in the DMZ must be configured to the highest level of security possible.



Contd…

- **Internet zone:**
- It is a worldwide /global system of interconnected computer networks .
- 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 in the form of email, web pages, files, multi-media and just about anything else that exists in digital form.
- **Intranet zone:**
- Intranet is a system in which multiple PCs are networked to be connected to each other
- PCs in intranet are not available to the world outside of the internet.

Contd..

VLAN

- It stands for virtual local area networks
- It’s a groups of hosts with a common set of requirement that communication as if they were attached to the same broad cast domain ,regardless of their physical location .

It allowed the networks admin to implement access and security policies to particular group of users

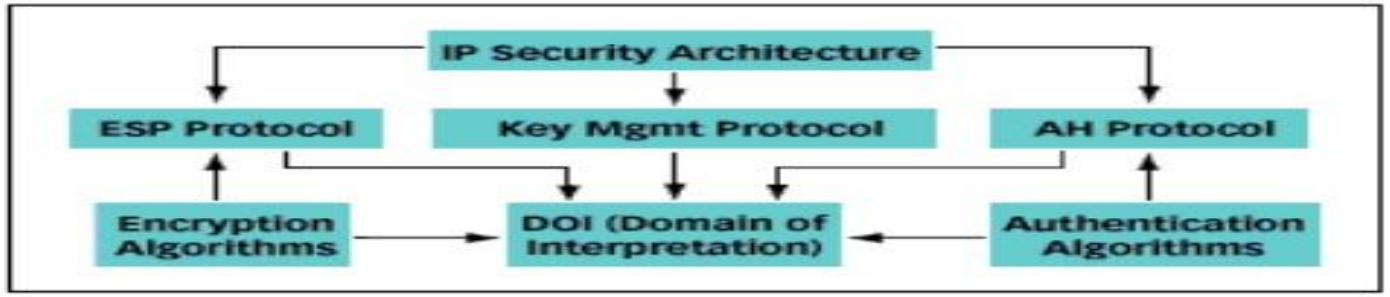
BENEFITS :

1.Broadcast control
2.Security
3.Cost reduction

IP-SECURITY-OVERVIEW

- **IP-SECURITY-OVERVIEW:**
- It is a technology that enables the network to securely send or transmit their data through an untrusted or shared network infrastructure.
-

IPSEC ARCHITECTURE



Internet Protocol Security (IPsec)

- Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.
- IPsec uses the following protocols to perform various functions:
  1. Authentication Headers (AH) provide connectionless integrity and data origin authentication for IP datagrams and provides protection against replay attacks.
  - 2. Encapsulating Security Payloads (ESP) provide confidentiality, data-origin authentication, connectionless integrity, an anti-replay service, and limited traffic-flow confidentiality

- 3. Security Associations (SA) provide the bundle of algorithms and data that provide the parameters necessary for AH and/or ESP operations

EMAIL SECURITY

EMAIL SECURITY

- Security of email transmission: Today email perhaps the most widely used application on the internet .though it was very much concern about the security of email message.
- An email message is considered to be made up of two portions

1. Content
2. Header

SECURITY OF EMAIL TRANSMISSION

- **SECURITY OF EMAIL TRANSMISSION**

- SSL encrypts messages/attachments, but only in transport between SSL/TLS enabled mail servers. So, your SSL email will be secure between your laptop or smartphone and Yale's email servers, but if the message then travels outside the Yale environment to unsecured (nonSSL) email systems (like a Gmail address, for instance), your message is no longer secure and is not protected by SSL.

- **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→ 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.

TUNNELING

- In computer networks, a **tunneling protocol** is a communications protocolthat allows for the movement of data from one network to another.
- It involves allowing private network communications to be sent across a public network (such as the Internet) through a process called encapsulation.
- Because tunneling involves repackaging the traffic data into a different form, perhaps with encryption as standard, it can hide the nature of the traffic that is run through a tunnel.

- The tunneling protocol works by using the data portion of a packet (the payload) to carry the packets that actually provide the service.
- Tunneling uses a layered protocol model such as those of the OSI or TCP/IP protocol suite, but usually violates the layering when using the payload to carry a service not normally provided by the network.
- Typically, the delivery protocol operates at an equal or higher level in the layered model than the payload protocol.

Spam and malicious code

- Spam is any kind of unwanted, unsolicited digital communication, often an email, that gets sent out in bulk.
- Spam is a huge waste of time and resources. The Internet service providers (ISP) carry and store the data. When hackers can’t steal data bandwidth from the ISPs, they steal it from individual users, hacking computers and enslaving them in a zombie botnet.
- Software providers invest resources creating email applications that try to filter most of the spam out. Consumers waste time sifting through whatever makes it past the spam filters.

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.