4) Computer Security Technology & Intrusion Detection

Page No. 84
Date

4.1 Firewalls:-

A firewall is a part of computer system or network that is designed to block unauthorised access while permitting authorised ~~connects~~ communications. It is a device or set of devices that is configured to permit or deny network transmissions based upon a set of rules and other criteria.

- Need of firewall:-
  1. All businesses connected to the internet need to make sure they have a firewall security solution.
  2. Protection from vulnerable services
  3. Concentrated security
  4. Controlled access to site systems.
  5. Policy enforcement
  6. It stops thieves and intruders from accessing your computer

- Limitations of firewall:-
  1. Even with the use of Proxy firewalls, it is still unable to control the content transferred across the network boundaries satisfactorily.
  2. Firewalls are extremely vulnerable table to insider attacks and covert channels
  3. They can become bottleneck of traffic.
  4. If a firewall is compromised, the protected network is extremely vulnerable.

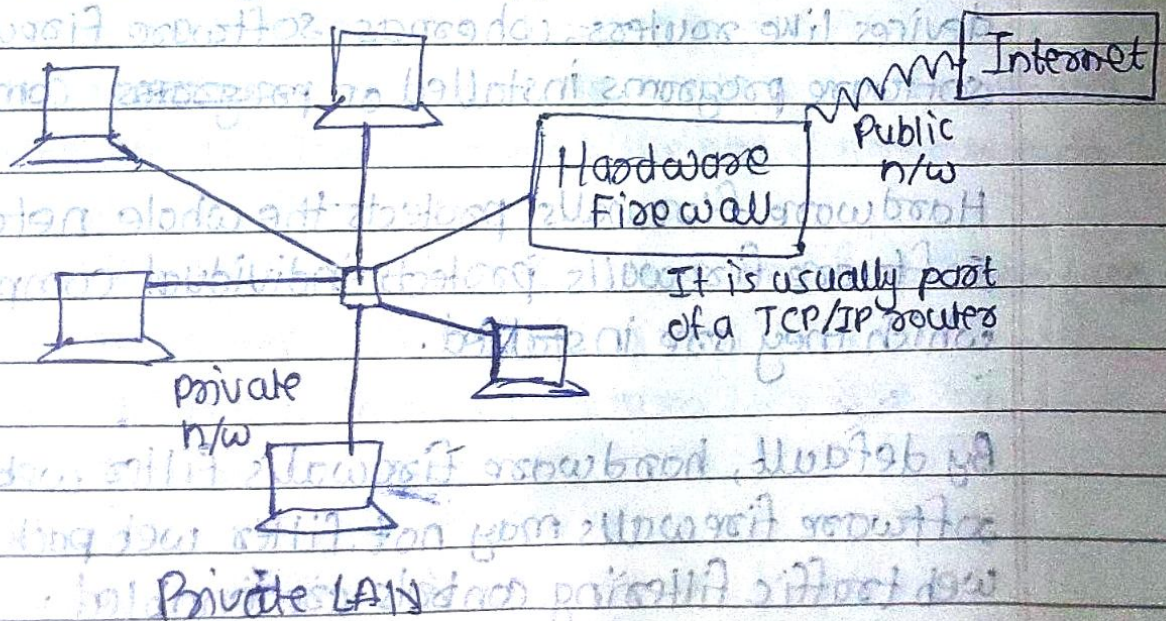
- Characteristics of firewall:
  1. All traffic from inside to outside, and vice versa, must pass through the firewall.
  2. Only authorised traffic, as defined by the local security policy, will be allowed to pass.

③ The firewall itself is immune to penetration. This implies that use of a trusted system with a secure OS.
④ Protection of wireless networks (Wi-Fi) effectively blocks intrusion attempts through wireless networks (Wi-Fi)
⑤ Access to the network and the internet : It specifies which programs installed on your computer can access the network or the Internet.
⑥ Protection of ports and protocols
⑦ Protection against intruders
⑧ It prevents certain programs from accessing the internet, if it is configured to do so.

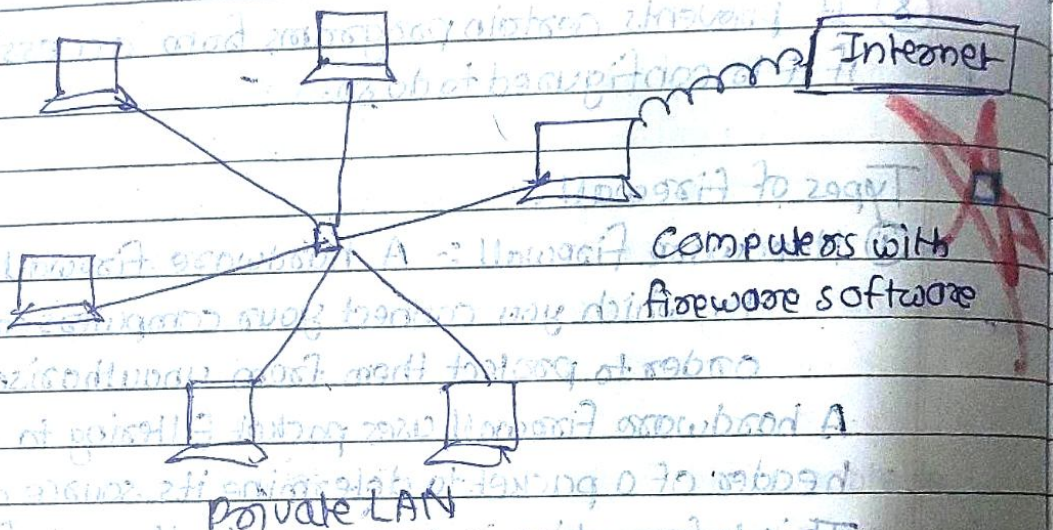
Types of Firewall :-

① Hardware firewall :- A hardware firewall is a device to which you connect your computers or network in order to protect them from unauthorised access.

A hardware firewall uses packet filtering to examine the header of a packet to determine its source and destination. This information is compared to the set of predefined or user-created rules that determine whether the packet is to be forwarded or dropped.



② Software firewall :- A software firewall is a piece of software that is installed on your computer in order to protect it from the unauthorised access. A software firewall will protect your computer from outside attempts to gain access to your computer, and, depending on your choice of software firewall, it could also provide protection against the most common Trojan programs or mail worms.



□ Difference between hardware and software firewall:
Hardware firewalls are specifically built within hardware devices like routers, whereas software firewalls are software programs installed on ~~programs~~ computers.

Hardware firewalls protects the whole network whereas Software firewalls protects individual computers on which they are installed.

By default, hardware firewalls filter web packets, while software firewalls may not filter web packets until web traffic filtering controls are enabled.

A hardware firewall can be configured to use a proxy service for filtering packets while a software firewall does not use a proxy service to filter packets.

Types of Firewall
1. Packet Filtering firewalls
2. Circuit level gateways
3. Application gateways
4. Stateful multilayer inspection firewall.

1. Packet Filtering Firewalls or Network Layer firewalls :-
These firewalls usally work at the network layer of OSI model, or IP layer of TCP/IP. They are usally part of a router. A router is a device that receives packets from one network and forwards them to another network. In packet filtering firewall, each packet is compared to set of criteria before it is forwarded. Depending upon the packet and the criteria, the firewall can drop the packet, forward it or send it to message originator.

Advantages :-
1. Because not a lot of data is analysed or logged, the use very little CPU resources and create less latency in the network
2. It is cost effective that are already the part of network to do additional duty as firewalls.
3. N/w layer firewalls tend to be very fast and tend to be very transparent to users.
4. Simple and straight forward mechanism
5. Faster in operation.

Drawbacks:
1. They don't provide password controls.
2. User's can't identify themselves.
3. The person who configures firewall protocol for the routers needs a thorough knowledge of the IP structure.
4. Remains vulnerable to spoofing source attacks.

etc.

② Application Gateways / Proxy servers :-

Application Gateways are also called proxies, are somewhat similar to circuit level gateways exped that they are application specific. They can filter packets at application layer of OSI or TCP/IP model. Incomming & Outgoing packets can't access services for which there is no proxy. They can filter packets at the application layer of OSI or TCP/IP model. In plain terms, an application level gateway is configured to be a web proxy will not allow all FTP, gopher, telnet or other traffic through. Because they filter packets at the application layer, they can filter application specific commands such as http: post, get etc;

It works like a proxy. A proxy is a process that sits between a client and the server. For a client, proxy looks like a server and for a server, Proxy looks like a client.

Advantages:
1. Since application proxies examine packets at application program level, a very fine level of security and access control may be achieved.
2. Checks traffic in greater details than packet filters.
3. No need to check each and every packet, but checks application as a whole.

④ The greatest advantage is that no direct connections are allowed through the firewall under any circumstances.
⑤ Proxies provide a high level of protection against denial of service attacks.
⑥ Easier to install, setup and operate.

Disadvantages :-

① Proxies require large amount of computing resources in the host system which can lead to performance bottlenecks or slows down network.
② Proxies must be written for specific application programs and not all applications have proxies available.
③ The software products used may be costly to procure.
④ In some cases, setup might be difficult and require administrative help.
⑤ It does not support new services easily.

③ Circuit Level Gateways :-

These firewalls work at the session layer of the OSI model, or TCP/IP layer of TCP/IP. They monitor TCP handshaking between the packets to determine whether a requested session is legitimate. Traffic is filtered based on the specified session rules. Information passed to remote computers through a circuit level gateway appears to be have originated from a gateway. This is useful for hiding information about protected network.

For every request/response, there will be two connections to be setup : one from the client machine to the firewall, and the second between the firewall to the external server and similarly in reverse way. Hence it is possible to enable / disable these services through the circuit gateways.

Advantages

1. More secure than packet filters since they work on higher level
2. Do not check individual packets in bound or outbound
3. Can hide internal network structure to external activities
4. Flexibility to enable or disable sessions or services is available
5. Less expensive as compared to application level products
6. Operation is transparent to end users.

Disadvantages :-

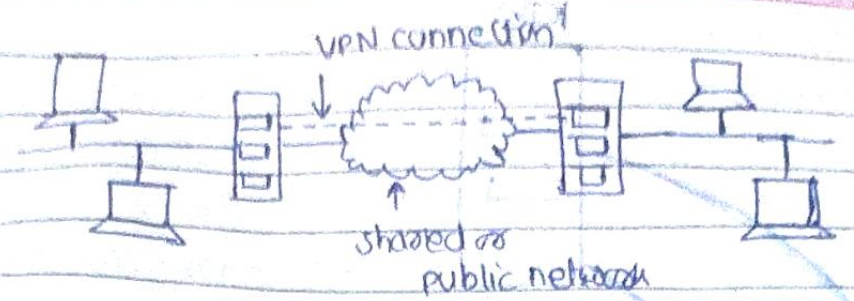
1. Less secured as compared to application gateways.
2. Breaks the client server model
3. Requires two dedicated connections ~~on the basis of their~~ to be set up for each service / response.
4. They provide very little control over what happens through the gateway.
5. Circuit levels firewalls cannot restrict access to protocol subsets other than TCP.

Implementing Firewall :-

(Read from textbook : Not imp for exam)

4.2 Virtual Private Network (VPN) :-

A virtual private network is a network that uses a public telecommunication infrastructure, such as internet, to provide remote offices or individual users with secure access to their organisation's network. Basically, a VPN is a private network that uses a public network (usually the internet to connect remote sites or users together.

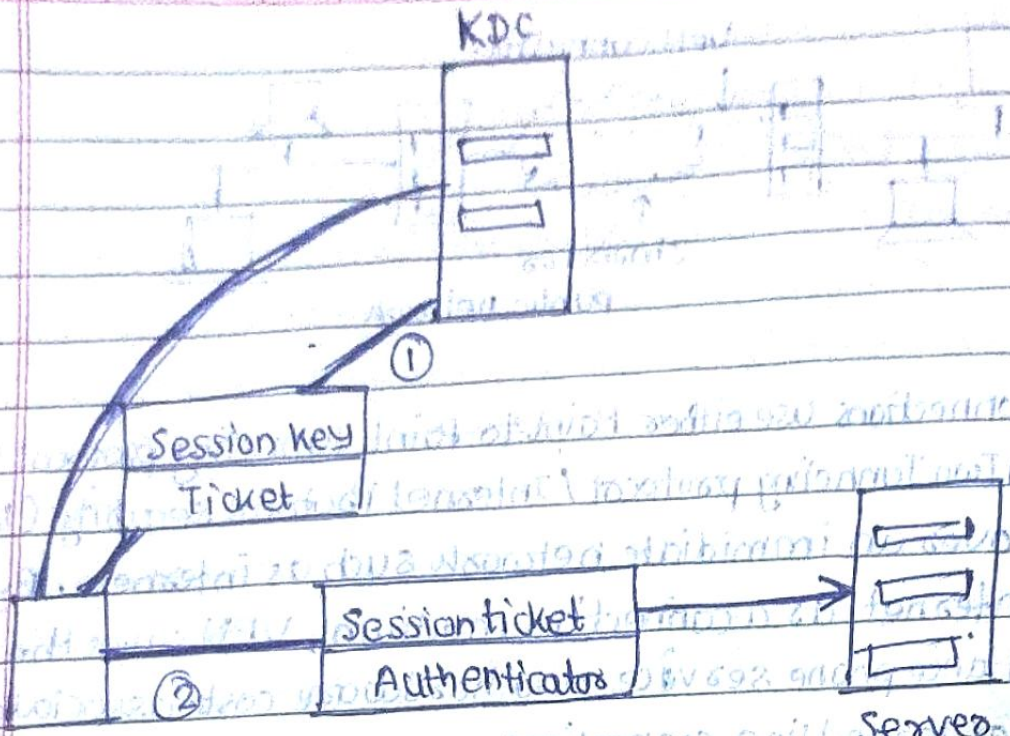


VPN connections use either Point-to-Point Tunneling protocol (PPTP) or Layer Two Tunneling protocol / Internet Protocol Security (L2TP/IPSec) over an immidiate network such as internet. By using internet as a connection medium, VPN saves the cost of long distance phone service and hardware cost associated with dial up or leased line connections.

VPNs are point to point connections across a private or public network such as the Internet. A VPN client uses special TCP/IP based protocols, called tunneling protocols, to make a virtual call to a virtual point to point connection. The remote access server answers the call, authenticates the caller and transfers data between the VPN client and the organisation's private network.

Kerberos :- Kerberos is a computer network authentication protocol, which allows nodes communicating over a non-secure network to prove their identity to one another in a secure manner. Its designers aimed primarily at a client-server model, and it provides mutual authentication - both the user and the server verify each other's identity.

In a kerberos system, there is a designated site on the network, called the kerberos server, which performs a centralized key management and administrative functions. The server maintains a database containing the secret keys of all users, generates session key when the two wish to communicate securely, and authenticates the identity of a user who requests certain network services



① A session ticket is encrypted with a server's long term key is bundled with the session key and enclosed inside a encrypted package for the client.

② Client encrypts the authenticator using session key and sends session ticket with encrypted authenticator to server

③ Server decrypts sessions ticket to obtain session key then uses the session key to decrypt the authenticator.

□ Security Topologies :- A security topology is the arrangement of hardware devices with respect to internal security requirements and needs for public access.

① Security zones :- They are the areas the network with specific security-related attributes and requirements. Security zones are a simple way to classify websites into three security categories:

(i) Browser Security : Low (Trusted sites)

This zone is for the sites that you trust and feel comfortable allowing certain security previlages. This zone contains Web sites that you can trust as safe (such as websites that are on your organisation Intranet or that come from established companies in whom you have confidence).

(ii) Browser Security : Medium (Unclassified sites)

This zone is for the sites that you have not classified or you are not sure of.

(iii) Browser Security : High (Restricted sites)

This zone is for the sites that you don't trust and want to restrict the access they have to your PC. You can protect your PC by not allowing these sites certain previliages such as ActiveX, cookies, filedownloads, etc.

(2) Demilitarized zone :- A DMZ (Demilitarized Zone) is an area of the network that sits between the Internet and organisations internal network.

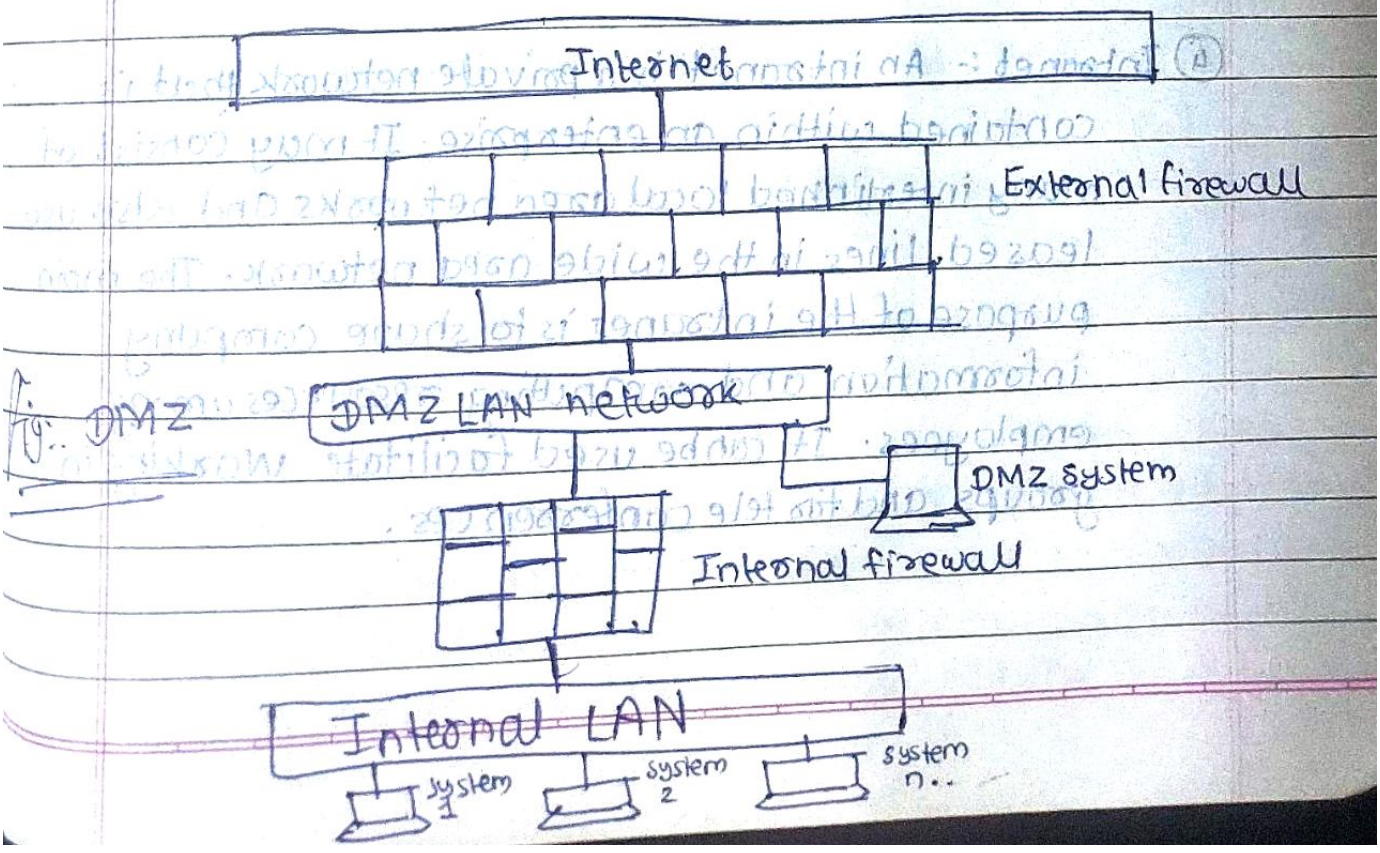


Fig:- DMZ

In computer networks, a DMZ (Demilitarized zone) is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data. A DMZ is an optional and more secure approach to a firewall and effectively acts as a proxy server as well.

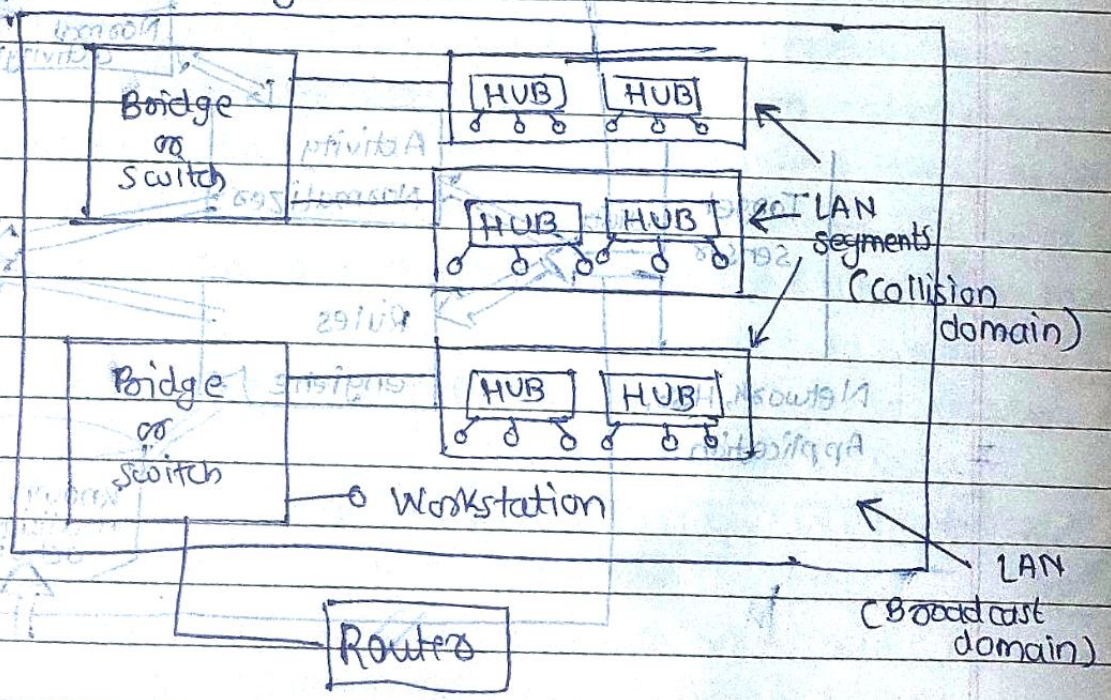
(3) Internet :- The internet is a global system of interconnected computer networks that use the standard Internet Protocol suite (TCP/IP) to serve billions of users worldwide. It is a network of networks that consist of millions of private, public, academic, business and government networks of local to a global scope that are linked by the broad array of electronic and optical networking technologies. It carries a vast array of information resources and services, most notably the inter-linked hypertext documents of the World Wide Web (WWW) and the infrastructure to support electronic mail.

(4) Intranet :- An intranet is a private network that is contained within an enterprise. It may consist of many interlinked local area networks and also use leased lines in the wide area network. The main purpose of the intranet is to share company information and computing resources among employees. It can be used facilitate working in groups and for tele conferences.

⑤ Extranet :- An extranet is a private network that uses Internet technology and the public telecommunication system to securely share a part of business information or operations with suppliers, vendors, partners, customers or other businesses. An extranet can be viewed as a part of a company's intranet that is extended to users outside the company.

⑥ Virtual Local Area Network (VLAN) :-

A Virtual Local Area Network (VLAN) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer. LAN is an abbreviation for local area network and in this context virtual refers to a physical object re created and altered by additional logic.

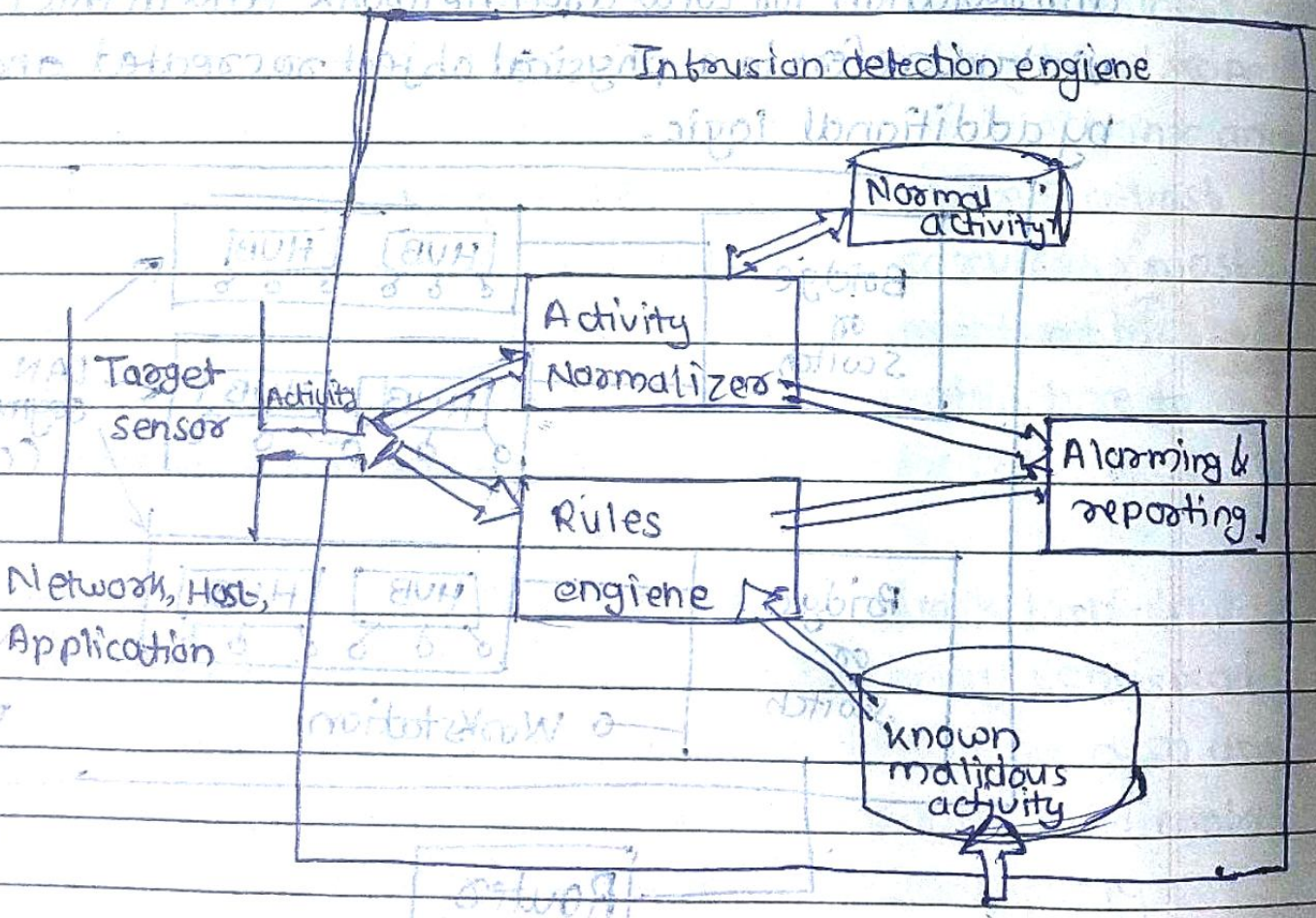


The basic reason for splitting networks into VLANs is to reduce congestion on a large LAN. A VLAN is a group of devices on one or more LANs that are configured to communicate as if they are attached to the same wire, when in fact they are located on different LAN segments.

4.3 Intrusion Detection Systems :-

An Intrusion Detection System (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. Its functions include :-

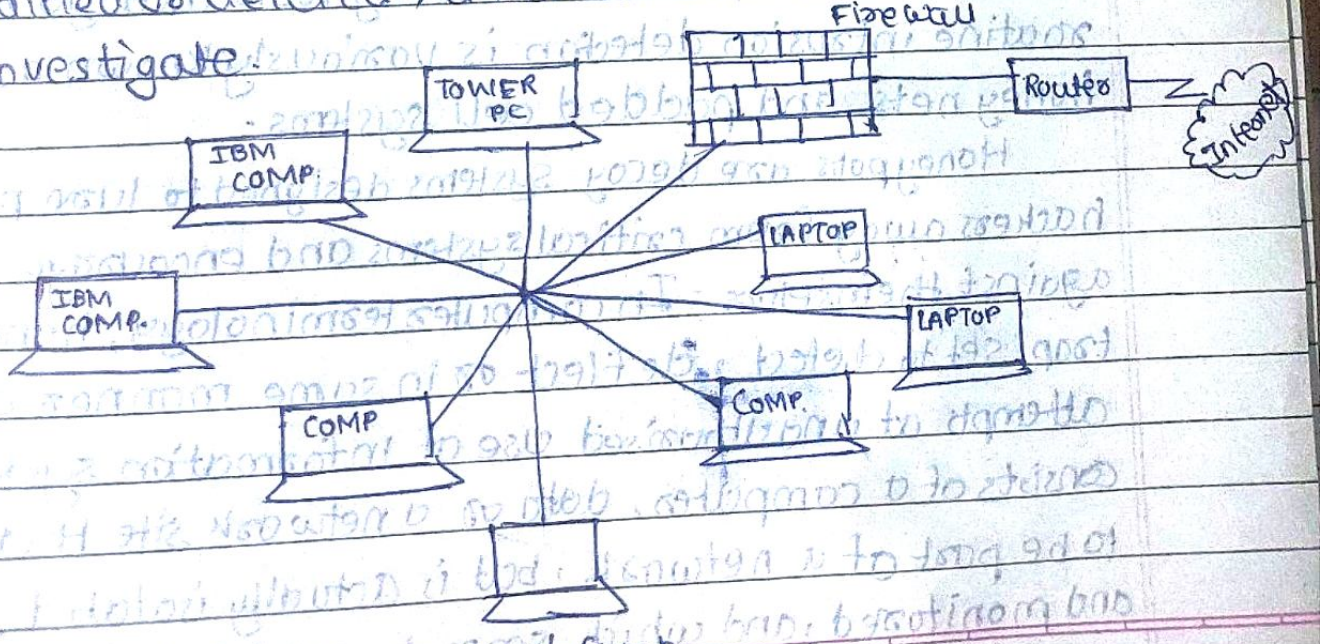
1. Monitoring and analysing both user and system activities
2. Analysing system configuration and vulnerabilities
3. Assessing system and file integrity
4. Ability to recognise patterns typical of attacks
5. Analysis of abnormal activity patterns
6. Tracking user policy violations.



① The network, host, application or target sensor provides data packets, host activity, application activity or change detections to the rules engine (misuse detector) and activity normalizer (anomaly detector).
② The rules engine searches the data for patterns from the known malicious activity database (signatures).
③ The activity normalizer performs analysis of the data, adjusting the baseline as the usage changes over time.
④ The known malicious activity database must be constantly updated with the latest patterns of malicious activity.
⑤ Both rules engine and activity normalizer in turn trigger the alarming and reporting as necessary.

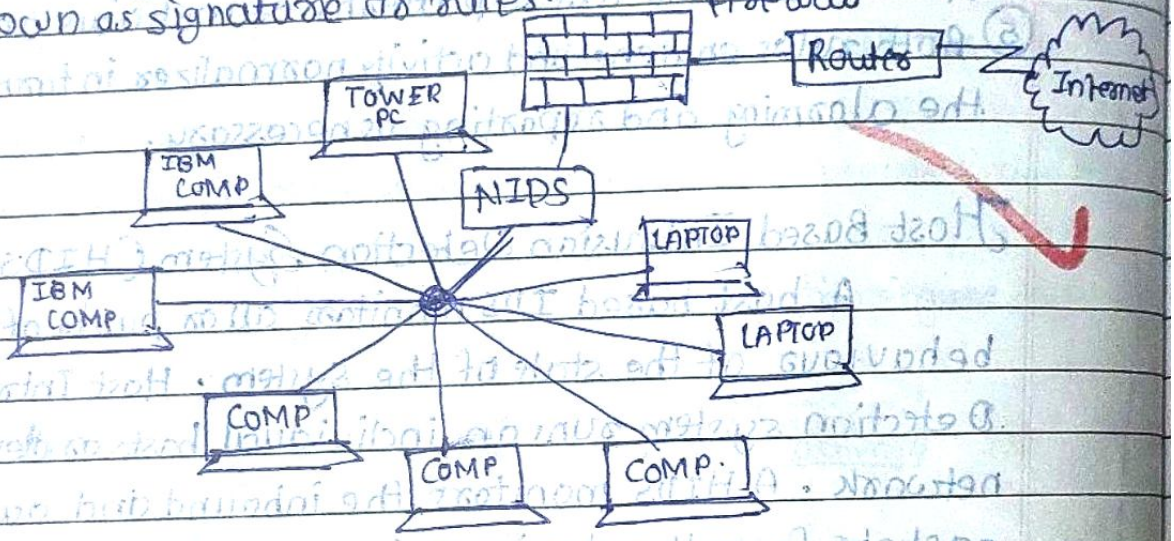
Host Based Intrusion Detection System (HIDS) :-

A host based IDS monitors all or parts of dynamic behaviour of the state of the system. Host Intrusion Detection system runs on individual hosts or devices on a 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 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 administrator to investigate.



Network Based Intrusion Detection System (NIDS):

Network Intrusion Detection System are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. It tries to detect malicious activity such as Denial of service attacks, port scans or even attempts to crack into computers by monitoring network traffic. A NIDS reads all the incomming packets and tries to find suspicious patterns known as signature or rules.



Honey Pots, Honey Nets and Padded Cell Systems:-

A class of powerful security tools that go beyond routine intrusion detection is variously known as honey pots, honey nets, and padded cell systems.

Honeypots are decoy systems designed to lure potential hackers away from critical systems and encourage attacks against themselves. In computer terminology, honey pot is a trap set to detect, deflect or in some manner counteract attempts at unauthorised use of information systems. It consists of a computer, data or a network site that appears to be part of a network, but is actually isolated, (un)protected, and monitored, and which seems to contain information or a resource of value to attackers.

When a collection of honey pots connects several honey pot systems on a subnet, it may be called a honey net.

A padded cell is a honey pot that has been protected so that it cannot be easily compromised. In other words, a padded cell is a hardened honey pot. In addition to attracting attacker with tempting data, a padded cell operates in tandem with a traditional IDS.

4.4 E-mail Security

Email is the most important single service running on the Internet. It is also the number one source of security risk. Every corporate mail server and workstation currently sending and receiving messages (email) is vulnerable to ever-growing list of attacks. The main threats to an email can be:

1. Viruses
2. Spam
3. Phishing

- Email encryption :- It refers to encryption, and often authentication, of email messages. E-mail encryption can rely on public key cryptography.

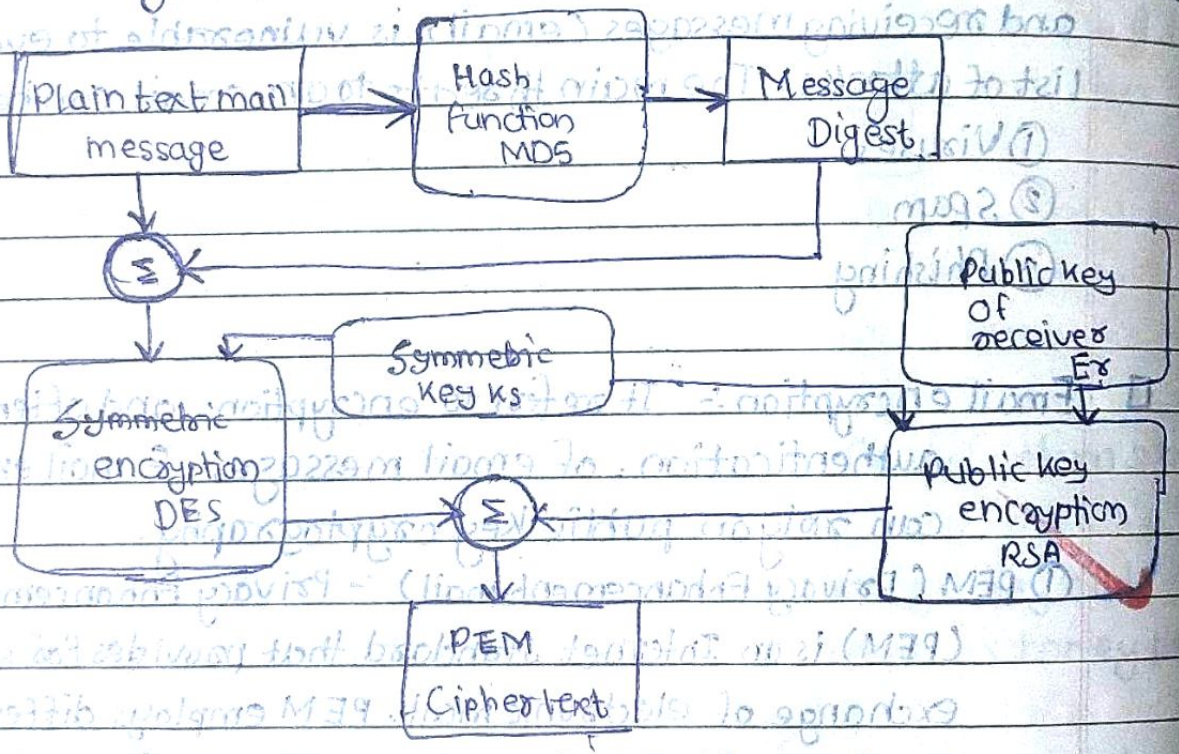
① PEM (Privacy Enhancement mail) :- Privacy Enhancement Mail (PEM) is an Internet standard that provides for secure exchange of electronic mail. PEM employs different cryptographic techniques to provide - confidientiality, sender authentication, and message integrity.

① Integrity of the message :- The message integrity allows the user to ensure that the message hasn't been modified or tampered during the transist from sender to receiver.

② Authentication of the sender :- It allows the receiver user to verify that the PEM message that they have received is truly from a person who claims to send it.

③ Confidientiality :- The objective allows a message to be kept secret from the people whom the message was not addressed.

④ Non-repudiation :- It prohibits the sender of the message to go back on the commitment of sending the message.



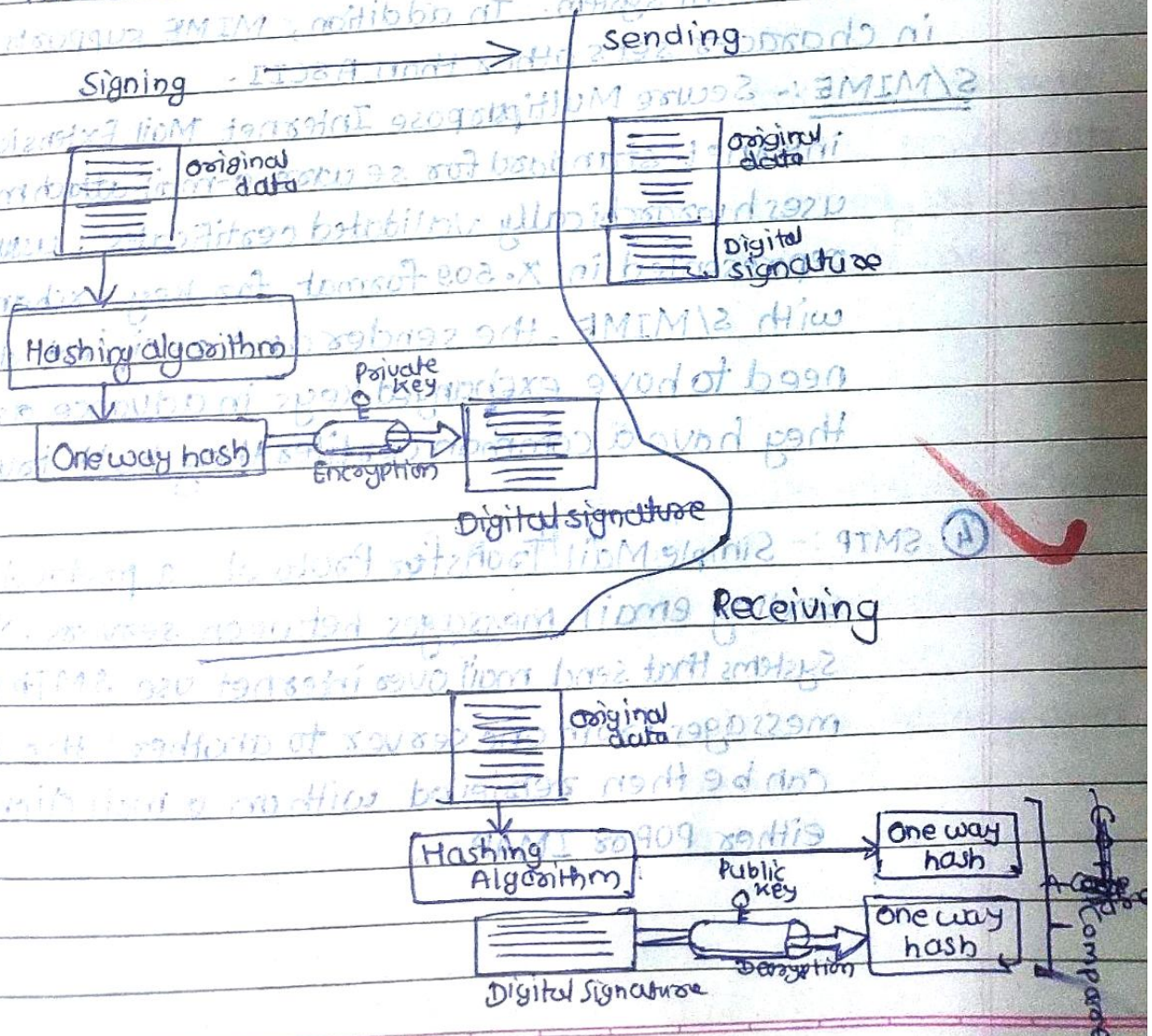
① The plain text mail message is applied with a strong hash function such as MD5 and Message Digest is generated.

② The message digest is appended with the message itself and the message digest added message is encrypted under symmetric key K's.

③ The symmetric key K's itself is encrypted using public key Cryptography, under the public key of receiver Ex. The public key is obtained using Digital Certificate with the help of PKI and CA. The encrypted message is appended with Encrypted Symmetric key and the PEM Ciphertext is formed which ensures the secure communication of the message using email.

② PGP (Preety Good Privacy):

Preety Good Privacy (PGP) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. It is often used for signing, encrypting and decrypting email to increase the security of email communications.

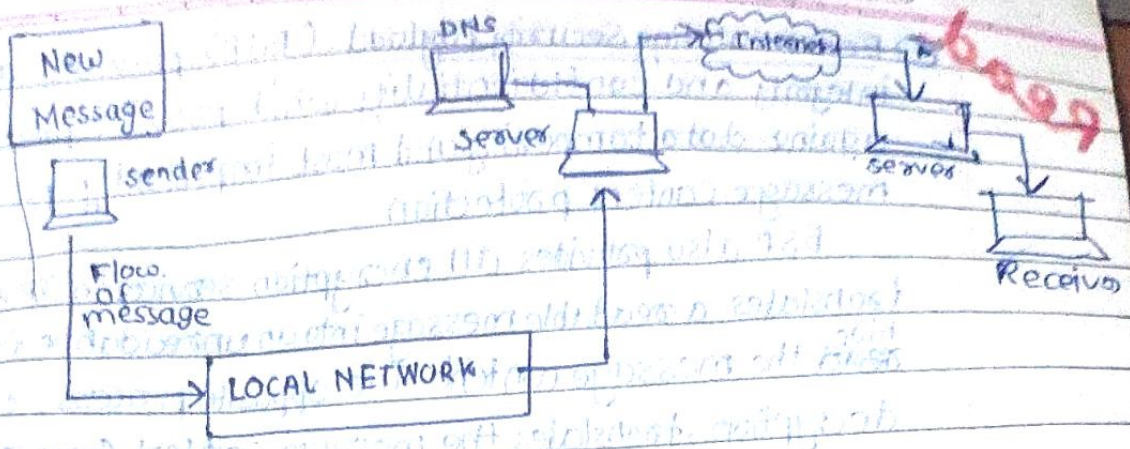


PGP creates secure e-mail at sender site. The email message is hashed to create a digest. The digest is encrypted using sender's private key. The message and the digest are encrypted using the one time secret key created by sender. The secret key is encrypted using receiver's public key and is sent together with the encrypted combination of message and digest.

(3) MIME :- Multipurpose Internet Mail Extensions. A specification for formatting non-ASCII messages so that they can be sent over the internet. Many e-mail clients now support ~~mime~~ MIME, which enables them to send and receive graphics, audio and video files via the Internet mail system. In addition, MIME supports messages in character sets other than ASCII.

S/MIME :- Secure Multipurpose Internet Mail Extensions is the internet standard for secure e-mail attachment. It uses hierarchically validated certificates, usually represented in X.509 format, for key exchange. Thus, with S/MIME, the sender and recipient do not need to have exchanged keys in advance as long as they have a common certifer they both trust.

(4) SMTP :- Simple Mail Transfer Protocol, a protocol for sending email messages between servers. Most e-mail systems that send mail over internet use SMTP to send messages from one server to another; the messages can be then retrieved with an e-mail client using either POP or IMAP.



① A message is created on the clients local network.
② The user sends the message via the Domino6 server.
③ Lotus Domino executes a TCP/IP DNS resolution and finds the target server
④ The message is transferred to the target recipients server, and then delivered to the recipient.

4.5 IP-security:- Ipsec is an Internet Engineering task force (IETF) standard suite of protocols that provide data authentication, integrity and confidentiality as data is transferred between communication points across IP networks.

IPsec components :-

① Encapsulating Security Payload (ESP) :- Provides confidentiality, authentication and integrity
② Authentication header (AH) :- Provides authentication and integrity.
③ Internet key exchange (IKE) :- Provides key management and Security Association (SA) management.

Read

① Encapsulating Security Payload (ESP) provides authentication, integrity and confidentiality which provides protection against data tampering and most importantly provide message content protection.

ESP also provides all encryption services in IPSec. Encryption translates a readable message into an unreadable format to hide the message content. The opposite process, called decryption, translates the message content from an unreadable format to readable message.

In addition, ESP has an option to perform authentication called ESP authentication. Using ESP authentication, ESP provides authentication and integrity for the payload and the not for the IP header.

Original Packet

IP HDR	TCP	DATA

Packet with IPSec ESP

IP HDR	ESP HDR	TCP	DATA	ESP Trailer	ESP Authentication

Encrypted

Authenticated

Read

② Authentication Header (AH):-

AH provides authentication and integrity, which protects against data tampering, using the same algorithms as ESP. AH also provides optional anti-replay authentication header is inserted into the packet between the IP header and any subsequent packet contents. Although AH protects the packet's origin, destination, and contents from being tampered with, the identity of the sender and receiver is known. It does not protect data confidentiality.

Original packet

IP HDR	TCP	Data

Packet with IpSec AH

IP HDR	AH	TCP	Data

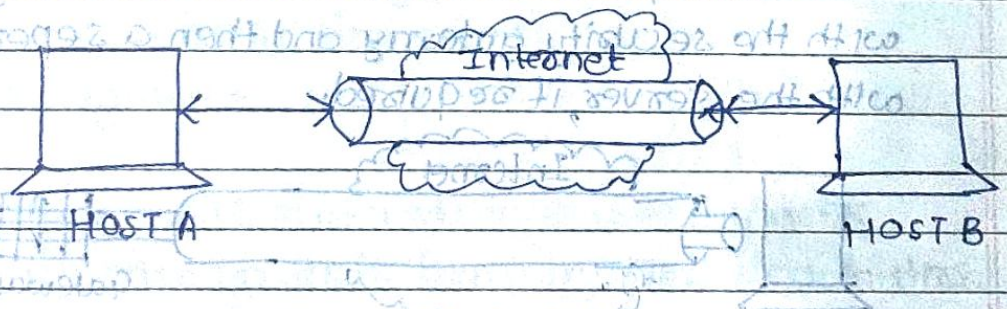
← Authenticated →

Read

③ Key Management :- IpSec uses the Internet key Exchange (IKE) protocol to facilitate and automate the SA setup and the exchange of keys between parties transferring data. Using keys ensures that only the sender and the receiver of the message can access it. IKE manages the process of key refreshing; ~~but~~ however, a user can control the key strength and the refresh frequency. Refreshing keys on a regular basis ensures data confidentiality between sender and receiver.

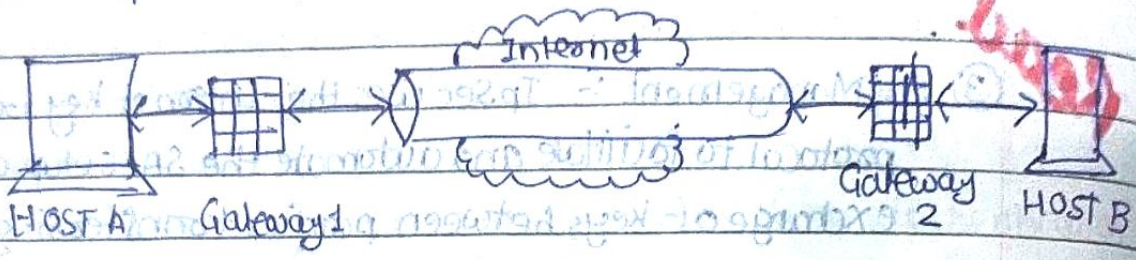
IPsec configurations :- There are four basic configurations for machine-to-machine connections using IPsec.

① The simplest is a host-to-host connection between two machines, as shown below

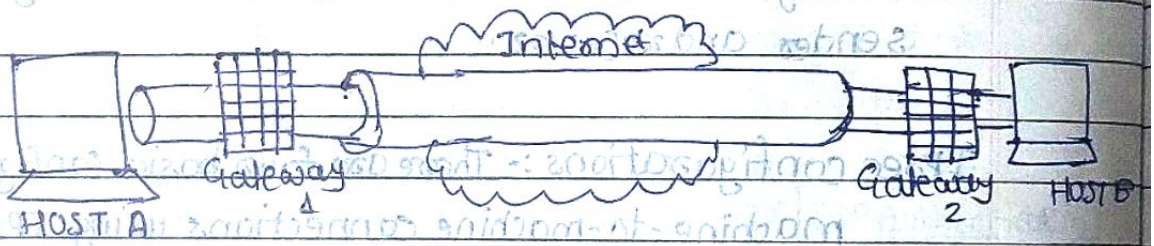


In this case, the Internet is not a part of the security association between the machines. As many options exist, both communicating parties must agree on the use of protocols that are available, and the agreement is referred to as a security association

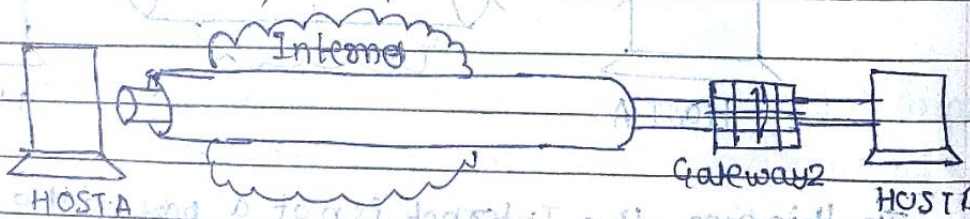
(2) The next level of implementation places two security devices in the stream, relieving the hosts of the calculation and encapsulation duties. These two gateways have a security association between them, but the network is assumed to be secure from each machine to its gateway, and no Ipsec is performed in this hop.



(3) The third case combines the first two, a seperate security association exists between the gateway devices, but additionally, a security association exists between hosts. This could be considered as tunnel inside tunnel



(4) In this case, the user establishes a security association with the security gateway and then a seperate association with the server, if required.



IP security :- Internet Protocol Security (IPsec) is a framework of open standards for helping to ensure private, secure communications over Internet Protocol (IP) networks, through the use of cryptographic security services. IPsec supports network level data integrity, data confidientiality, data origin authentication, and replay protection. Because IPsec is integrated at Internet layer (layer 3), it provides security for almost all protocols in TCP/IP suite, and because IPsec is applied ~~transparently~~ transparently to applications, there is no need to configure seperate security for each application that uses TCP/IP.

The following elements are part of the IPsec framework :-

1. A general description of security requirements and mechanisms at the network layer
2. A protocol for encryption (ESP).
3. A protocol for authentication (AH).
4. A definition for the use of cryptographic algorithms for encryption and authentication.
5. A definition of security policies and security associations between communicating peers.
6. Key management

IPsec helps provide defense-in-depth against:

1. Network based attacks from untrusted computers, attacks that can result in the denial-of-service of applications, services, or the network
2. Data corruption
3. Data theft
4. User-credential theft
5. Administrative control of servers, other computers, and the network.