(16M)

Chapter-8

Network security

Page No.
Date : / /

(1) Properties of secure communication. (1+1+1) ④ ②

(Q) Explain desirable properties of secure communication.

When two people want to communicate securely over the computer network, certainly sender wants only the receiver to be able to understand a message that sender has sent. Sender and receiver also wants to sure that ~~person~~ the content of their message has not been altered in transit.

Considering these requirements, we can identify the following desirable properties for secure communication.

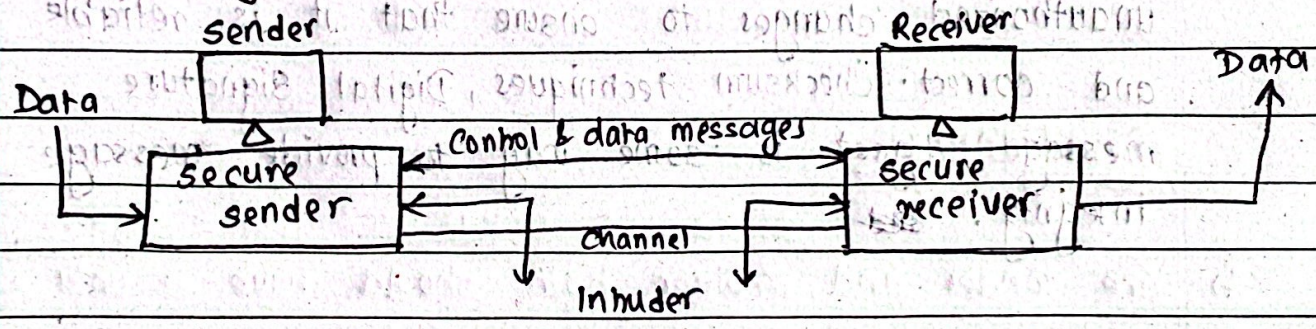


Fig:- Sender, receiver and intruder

(1) Confidentiality

Only the sender and intended receiver should be able to understand the content of transmitted message. It is necessary that the message should be encrypted so that data can't be understood by other than the receiver.

Page No.
Date : / /

(2) Authentication

Both the sender and receiver should be able to confirm the identity of the other party involved in the communication to confirm that the other party is who or what he/she claim to be.

(3) Non-repudiation

It is the ability to prove that the sender actually sent the data.

(4) Message Integrity and Non-reliability

Integrity means that data is protected from unauthorized changes to ensure that it is reliable and correct. Checksum techniques, Digital Signature message digest is some way to provide message integrity.

(5) Access control & availability

Some user may be legalized to access resources while others are not.

Availability guarantees that systems, applications and data are available to users when they need them. The most common attack that impacts availability is denial of service in which the attacker interrupts access to information, system, devices or other network resources.

Page No.
Date : / /

* Cryptography (1) (2)

→ Cryptography refers to the tools and techniques used to make messages secure for communication between the participants and make messages immune to attacks by hackers.

[M]
plain text → Encryption → cipher text → Decryption → plain text
M'

sender → Receiver

* Symmetric key cryptography (1) (4)

In symmetric key cryptography, both sender and receiver share a single secret key for encryption and decryption. The cipher text has almost the same size as the original message and built on a secret or some random unpredictable data.

The strength mostly depends on the key length and encryption of large files is faster and efficient.

Page No.
Date : / /

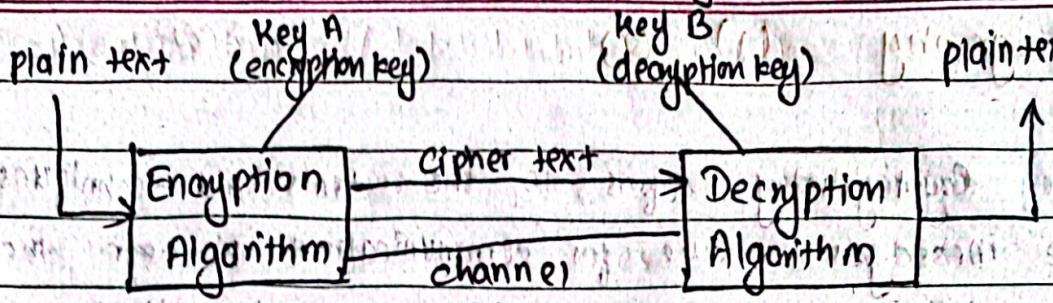


Fig:- Symmetric key cryptography principle

Advantages

- It takes less time to encrypt a message using the symmetric key algorithm.
- It is effective to use for long messages.

Disadvantages

- The sender and receiver both should have a unique symmetric key. Therefore, a large numbers of user increases.
- The distibution ~~bet~~ of keys between two users can be difficult.

Page No.
Date: / /

* Difference between symmetric and Asymmetric key system. (1+1+1) (3)

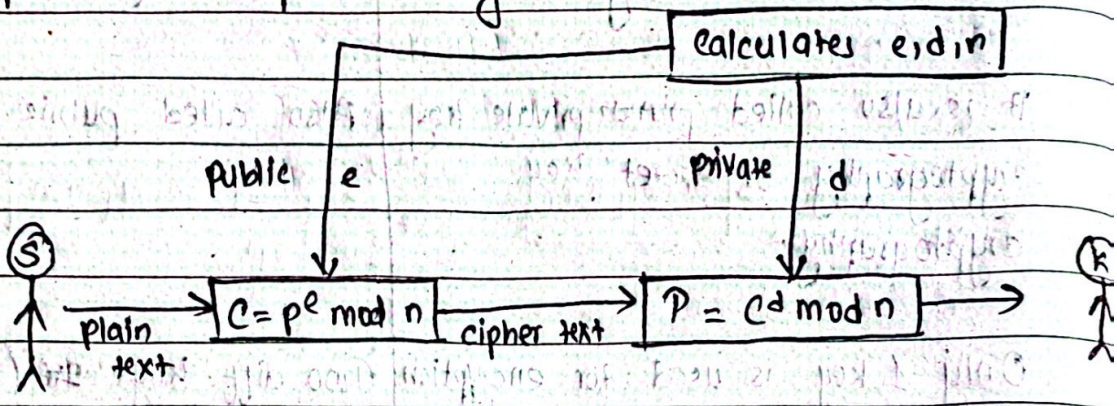
→

	Symmetric key system (Secret key)	Asymmetric key system (Public key)
(1)	It is also called ~~primo~~ private key cryptography or secret key cryptography.	Also called public key cryptograph
(2)	Only 1 key is used for encryption & decryption.	Two diff. keys ~~are~~ (public & private) keys are used for en&de.
(3)	Symmetric key algorithms are faster in execution.	Slower in execution.
(4)	less complex and less computational power is required.	more complex & more computational power needed.
(5)	Used for transfer of bulk data because it executes faster.	Used for secretly exchanging the secret key.
(6)	Sharing the key in bet: sender & receiver is not safe.	No problem of key sharing because of private key concept.
(7)	Commonly used symmetric key algos → DES, AES, RCY, 2DES, 3DES	Algos → RSA, Deffie ~~He~~ Hellman, DSA, etc.

Page No.
Date : / /

* RSA algorithm (1+1+1+1) (4)

RSA algorithm is the most common public key encryption algorithm which uses two numbers, e and d as public and private keys.



Algorithm

Steps to select private and public keys:

1. Choose two prime numbers say p and q.
2. Calculate $n = p \times q$, n is modulus for encryption and decryption.
3. Calculate $\phi(n) = (p-1) \times (q-1)$
4. Choose random integer 'e'; $1 \leq e < \phi(n)$ and coprime of $\phi(n)$.
5. Calculate 'd' as, $e \times d = 1 \bmod \phi(n)$
   or, $d = e^{-1} \bmod \phi n$

Page No.
Date : / /

Now, (e,n) are announced to the public and d and ϕ are kept secret.

Encryption

1. Take receiver's public key (n,e).
2. Represent plain text by a positive integer, say m such that $1 \leq m < n$.
3. Compute cipher text $c = m^e \bmod n$.
4. Send cipher text to receiver.

Decryption

1. Use private key (d,n) to compute plain text message, m,

$$\boxed{m = c^d \bmod n}$$

2. Extract plaintext from message representative m.

Page No.
Date : / /

* Deffi Helman Algorithm (1)

→

This is a key exchange algorithm used for securely establishing a shared secret over an insecure channel.

Algorithm

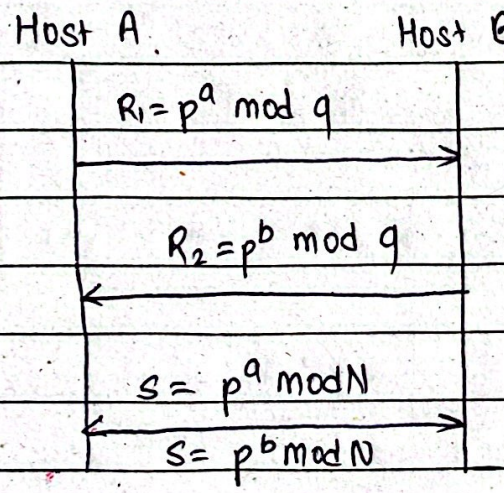
(1) A chooses a large random number a and calculates $A_1 = p^a \bmod q$

(2) A sends R_1 to B. Note that A doesnot send the value of a; A only sends R_1.

(3) B chooses another large number y and calculate $R_2 = p^b \bmod q$.

(4) B sends R_2 to A. Again, note that B doesnot send the value of b but only sends R_2.

(5) A calculate $S = (R_2)^a \bmod N$. B also calculates $S = (R_1)^b \bmod N$. And S is secret key.



Page No.
Date : / /

Example,

$q = 13$ $\quad$ $p = 6$

$a = 3$ $\quad$ $b = 10$

$R_1 = 6^3 \bmod 13$

$= 8$

$R_2 = 6^{10} \bmod 13$

$= 4$

$S = R_2^{\,q} \bmod 13$

$= 4^3 \bmod 13$

$= 12$

$S = R_1^{\,b} \bmod 13$

$= 8^{10} \bmod 13$

$= 12$

Page No.
Date : / /

* Digital signatures (1+1+1+1)

Digital signature is a mathematical technique used to validate the authenticity of person.

eg:- Internet banking user/password, Email password etc.

Digital signatures should be done in such a way that, they are:

a) Verifiable:

It must be possible to prove that a document signed by an individual was indeed signed by that individual. The signature must be verifiable.

b) Non forgeable and Non repudiable

The signature cannot be forged and a signer cannot later ~~repudio~~ deny having signed the document.

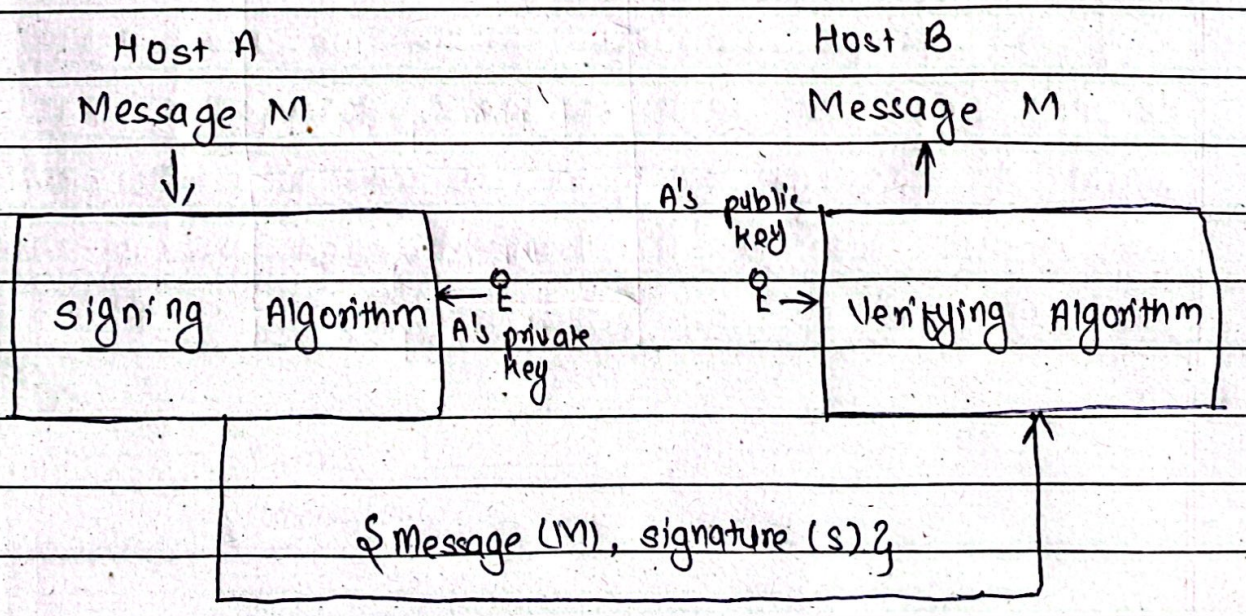


Fig:- Digital signature process

Page No.
Date : / /

Algorithm in digital signature

1) key generation

key validates user (id/password, otp etc)

2) Signing Algorithm

Task we have done ~~with~~ ~~our~~ will validate with our key.

3) Signature verifying algorithm

It verifys our signature.

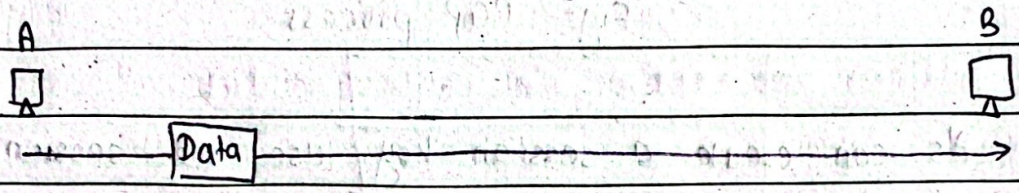
Page No.
Date : / /

* Securing E-mail (PGP) (1+1)

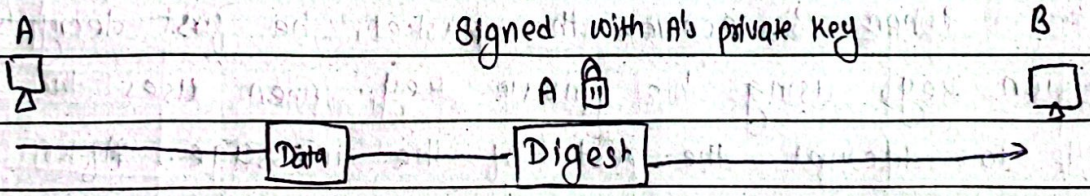
Q) What is PGP. How can PGP secure email communication?

Pretty Good Privacy (PGP) is a high quality encryption software used to encrypt and decrypt the email.

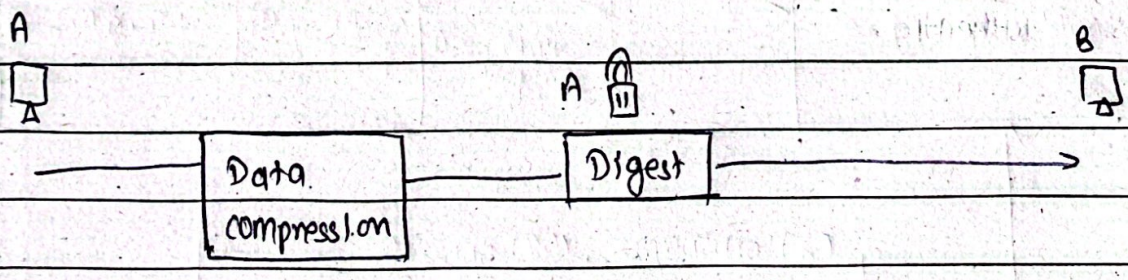
It uses latest technique of encryption including public key cryptography and digital signature.



The simplest scenario is to send the email message in plaintext. For authentication, A signs the message. A creates a digest of the message and signs it with A's private key.



For further improvement, to make the packet more compact, the message is compressed.



Page No.
Date : / /

Confidentiality in an email system can be achieved using conventional encryption with one-time session key as shown below:

- A's private key
- B's public key
- B's private key
- A's public key

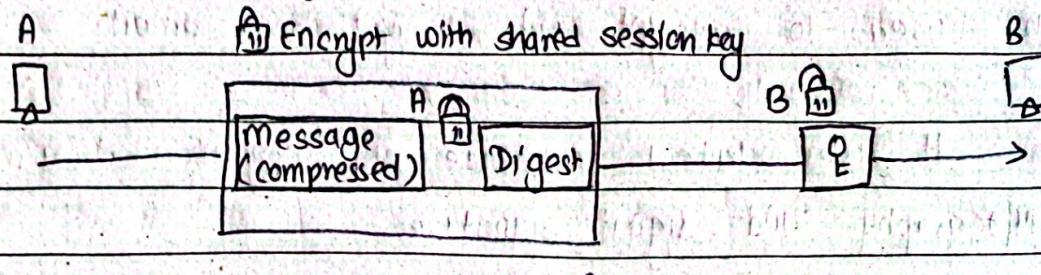


Fig:- PGP process

A's can create a session key, use the session key to encrypt the message and digest and send the key itself with the message. However, to protect session key, A encrypt it with B's ~~privat~~ public key.

When B receives the packet, he first decrypts the session key, using his private key. Then uses the session key to decrypt the rest of the message. After decompressing the rest of the message, B creates a digest of message & checks to see if it is equal to the digest sent by A. If it is, then the message is authentic.

Page No.
Date : / /

* Secure Socket layer (SSL) (1+1)

SSL is designed to provide security and compression services to data generated from the application layer. SSL can receive data from the application layer protocol, the received data is compressed, signed and encrypted. The data is then passed to a reliable transport-layer protocol.

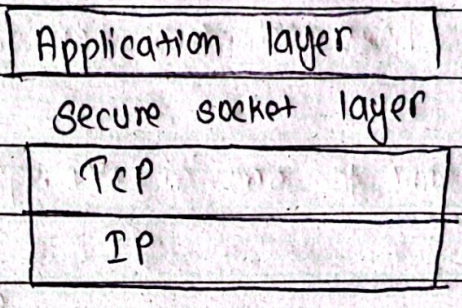
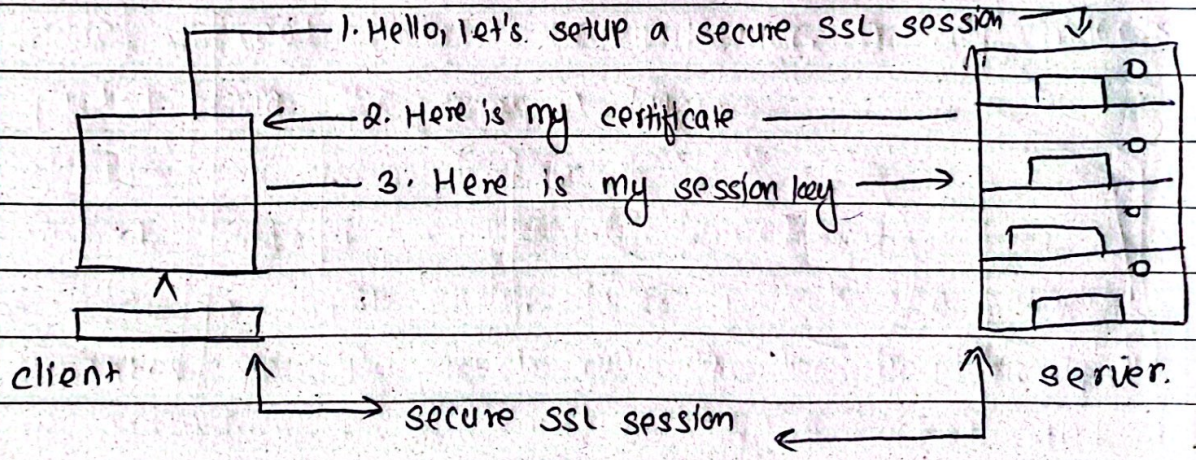


Fig:- SSL Layer



Page No.
Date : / /

* IP sec (IP security) (4+1)

At the network layer, security is applied between two hosts, two routers or host and a router. The purpose of IPsec is to protect those applications that used the service of the network layer directly such as routing protocols.

The protocol offers authentication and privacy servi at the IP layer, and can be used with both IPV4 and IPV6.

IPsec operates in one of two modes

a) Transport mode

In transport mode, IPsec protects what is delivere from the transport layer to the network layer. The transport mode doesnot protect the IP header, it only protects the packet from the transport layer.

b) Tunnel mode

In tunnel mode, IPsec protects the entire IP packet It takes an IP packet including the header, applies IPsec security methods to the entire packet and then adds a new IP header.

IPsec (defines two protocols: Authentication Header (AH) protocol & Encapsulating Security Payload (ESP) protocol.

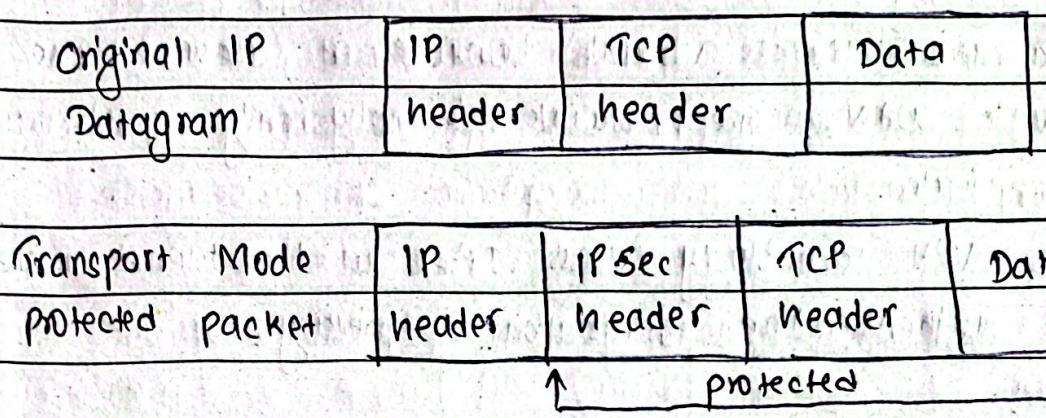


Fig: IPsec in transport mode

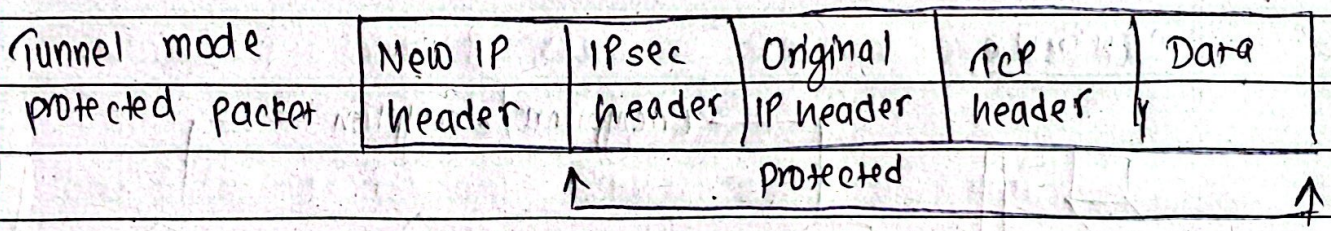


Fig:- IPsec in tunnel mode

Page No.
Date : / /

* VPN (Virtual Private Network) (1+1+1)

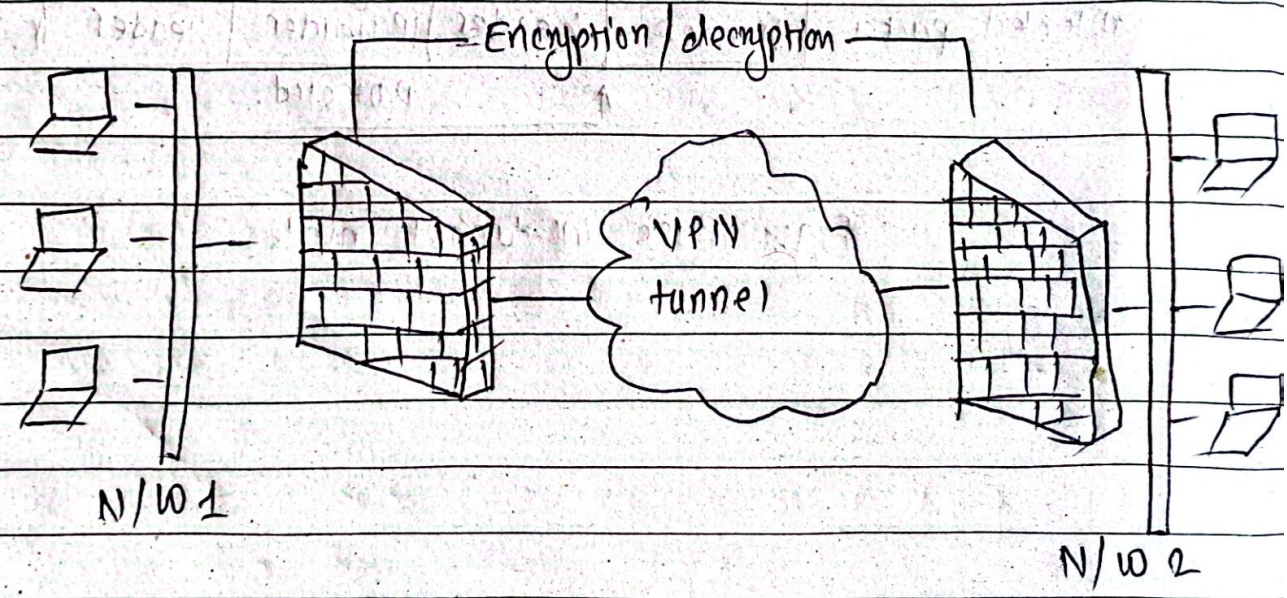
VPN creates a network that is private but virtual. It is private because it guarentees privacy inside the organization. It is virtual because it doesnot use real private WANs; the network is physically public but virtually private.

VPN technology uses IPsec in the tunnel mode to provide authentication, integration & privacy.

→ VPN offers high amount of security.

→ Allows users to remotely access a private N/w

Architecture

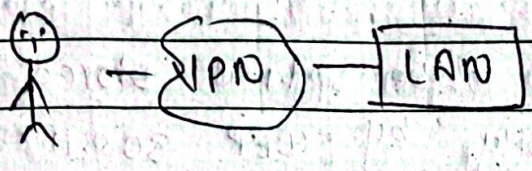


Page No.
Date : / /

Types of VPN protocal

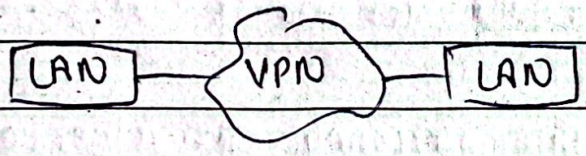
1) Point to point Tunneling protocol (PPTP)

- It is basic security protocol which is used for VPN which is used in Windows NT system.
- It supports connectivity between user and a LAN.



2) Layer 2 Tunneling Protocol (L2TP)

- It is advanced version of PPTP.
- It supports both user to LAN and LAN to LAN.



Page No.
Date : / /

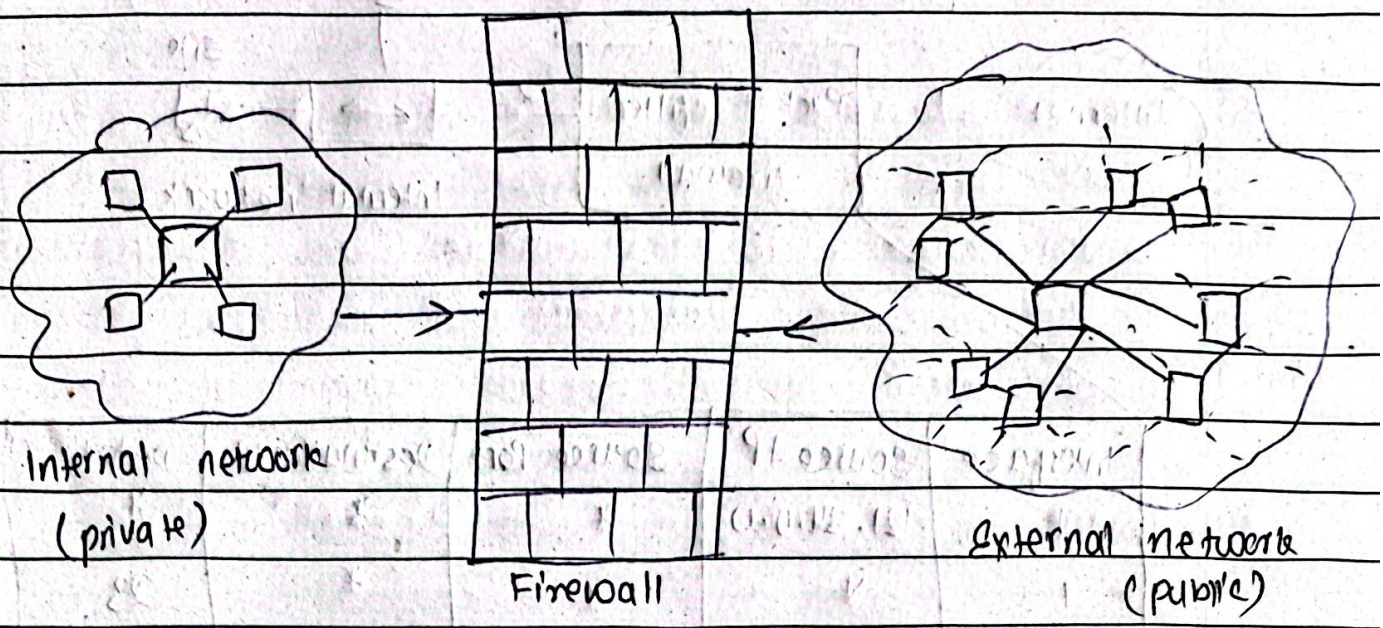
* Firewalls (1+1+1+1+1+1+1+1+1+1)

Firewall is a system which monitor and control incoming and outgoing traffic based on predefined rules. Firewall is a security system intended to protect an organization's network against external threats such as hackers coming from another network. An organization places a firewall at its connection to external networks. A firewall partitions the Internet into two regions refered to informally as the inside & outside.

Firewall acts like a barrier. A firewall is a combination of hardware & software that isolates an organization's internal network from the internet allowing specific connections to pass & blocking others.

Organizations employ firewalls for the following reason

- To prevent intruders from interfering with the daily operation of internal network, denial of service attack, SYN FIN attack.
- To prevent intruders from deleting or modifying information stored within the internal network.
- To prevent intruders from ~~deleting~~ obtaining secret information.
- Allow only authorized access to inside network.



Types

1) Packet filter firewall

Packet filter ~~firewall~~ is the first generation firewall which is essentially a router that has been programmed to filter out certain IP addresses or TCP port numbers. It works on Network and Transport layer. These types of routers are relatively simple in ~~desing~~ design & also act very quickly, but are little too simple to provide a high level of security.

It can block @ IP address, full Network, service (http, ftp etc)