VPN : Virtual Private Network

→ VPN extend private N/w across the public N/w and enable user to send and recieve data across shared (or) public N/w as if computer devices where directly connected to private N/w

→ It create by establishing a virtual point to point connection through use of dedicated circuit (or) ~~are~~ with tunneling protocol over existing N/w

VPN Server :

→ An switched virtual N/w. Network management software participant operation as well as configuration and reporting middleware component known as virtual Network server

Services :

→ Directory service
→ Security service
→ Connection management service
→ Bandwidth service
→ virtual routing service

VPN Security Model

- → Confidentiality
- → Authentication
- → Integrity

Types

- → Remote access
- → site to site
- → extranet based site to site
  - ↓
  - Connecting outside the n/w

VPN Protocol :

- → it determine exactly how data is routed through a connection
- → protocol have different specification based on benifits and decided circumstances to main
- → Two main approaches
  - 1. 2 protocol is used — for data, for security
  - 2. 1 protocol is used

→ PPTP → point to point tunneling protocol

IPsec/L2TP → Layer 2 tunneling protocol

OpenVPN

SSTP → Secure Socket Tunneling protocol

IKEv2 → Internet Key exchange version 2

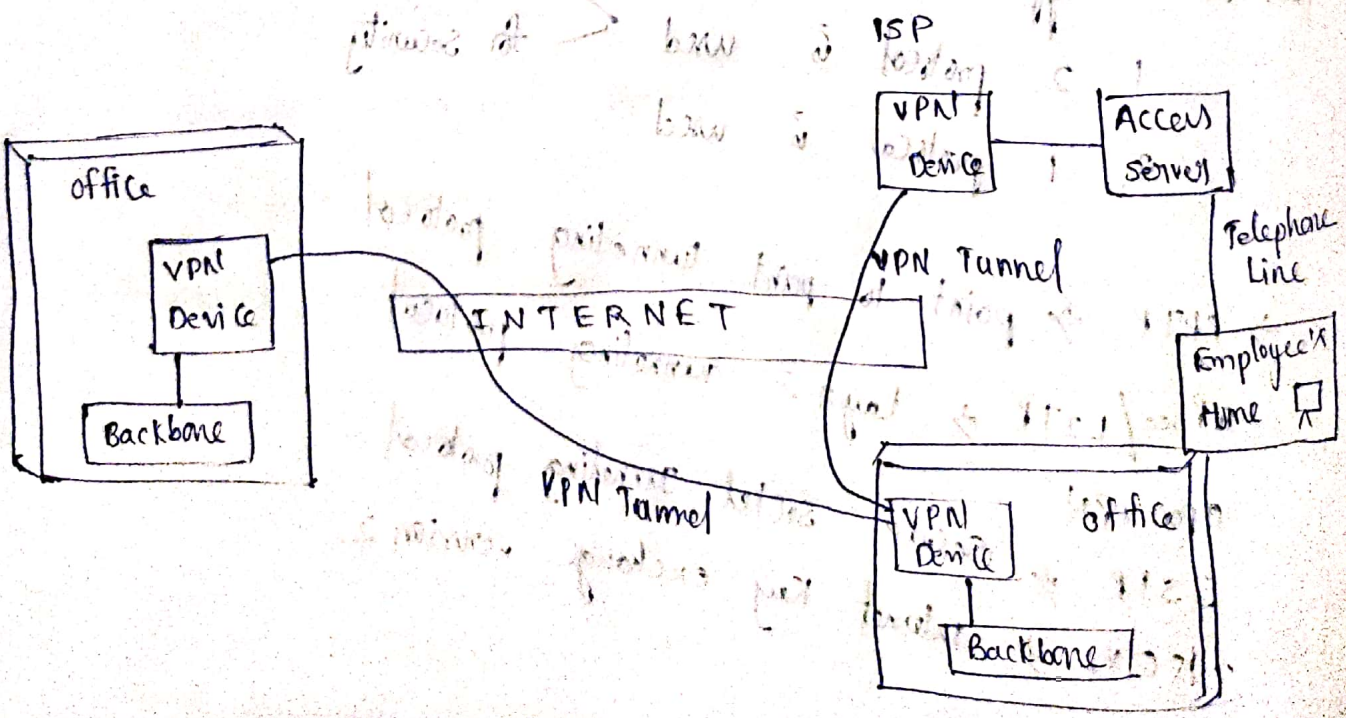
VPN Benifits

- high hide user IP address and Browsing history
- Secure Connection with encryption
- Paving geo blocked Content
- Making more difficult for advertiser to target adds to individual

Challenges

- Not all devices made supports VPN
- VPN donot protect against every threads
- Paid VPN are more trusted and secure
- A VPN Makes low Internet speed

VPN Architecture



Features of extranet

1. Data Security :

→ Sharing Confidential data is of utmost priority and the extranet provides a safe environment for data sharing between the organizations

2. Faster communication :

→ Extranet allows to connect multiple organizations and escalate the communication b/w them.

3. Flexibility :

→ Extranet provides a flexible and scalable environment to work on for everyone involved, which also increases the productivity of the organization.

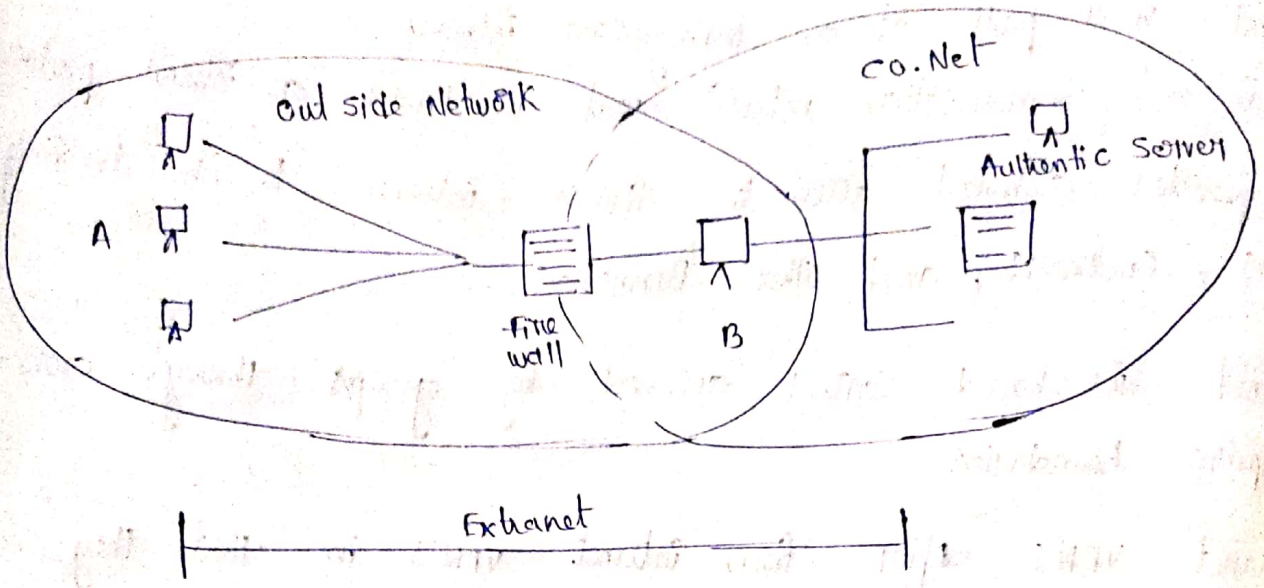
4. cost :

→ it may decrease the cost of paperwork and travel to some extent.

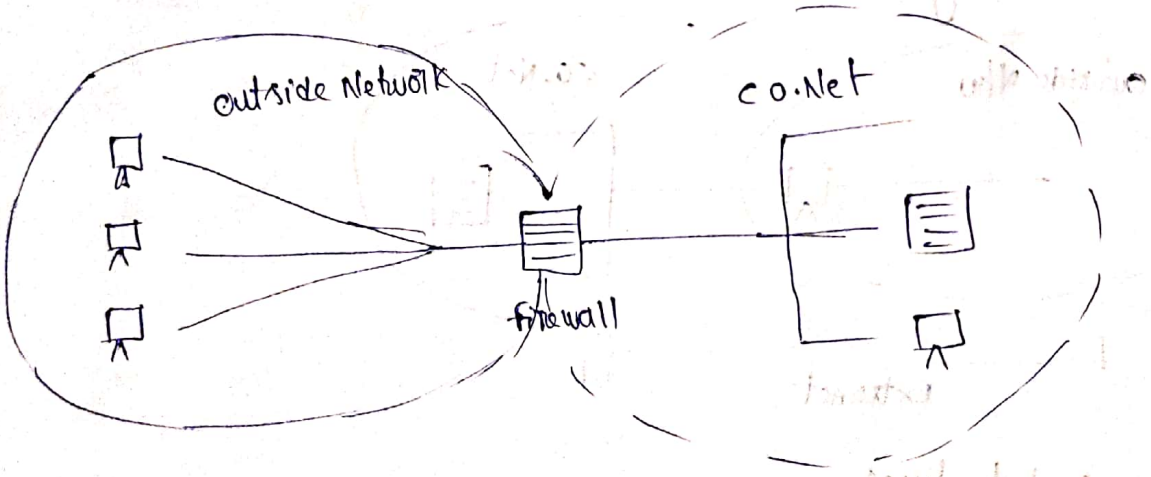
5. Authentication :

→ It provides authentication mechanisms like username and password. Therefore, only authorized users can access the network.

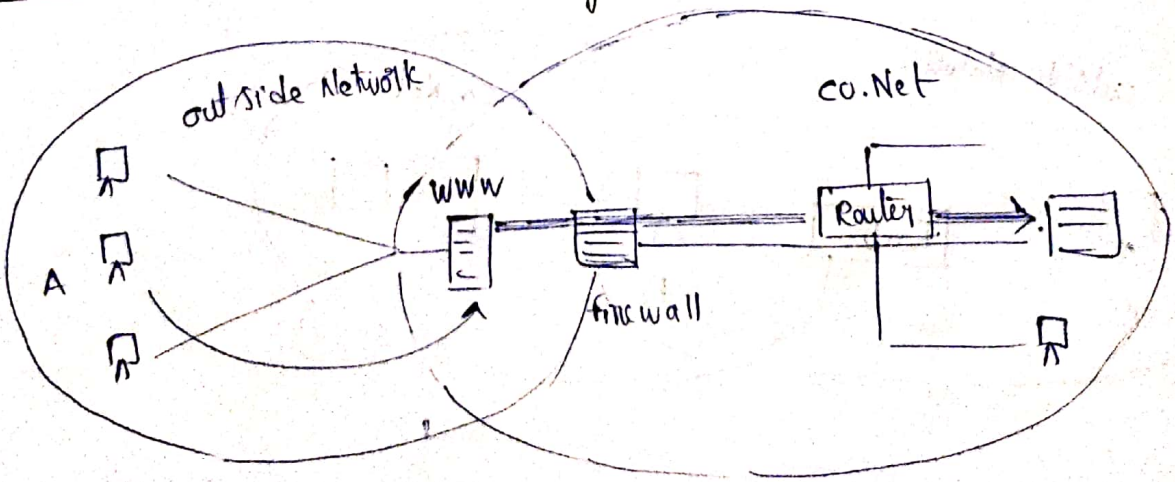
3. Extranet using an application layer gateway -firewall



4. outbound proxy architecture



5. Extranet with authenticating web server



Advantages

- Security
- Data
- Network sharing
- communication

Disadvantages

- complex security
- Hosting
- Expensive
- limited.

1. IP Security (IPSec)

- The IP Security (IPSec) is an Internet Engineering Task Force (IETF) standard
- IP security is a security N/w protocol suite that authentication and encryption of secure encrypted communication b/w two computers over internet
- IP security can protect data b/w a pair of host and pair of security gateway b/w security gateway and host

Uses of IP security

- To encrypt application layer data
- To provide security for routers sending routing data across the public internet.
- To provide authentication without encryption, like to authenticate that the data originates from a known sender.
- To protect N/w data by setting up circuit using IPSec tunneling in which all data is being sent b/w the two endpoints is encrypted, as with a VPN connection.

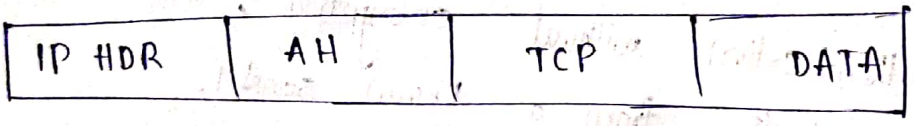
Components of IP Security

1. Encapsulating Security payload (ESP)

* it provides data integrity, encryption, authentication and anti replay, it also provides authentication for payload.

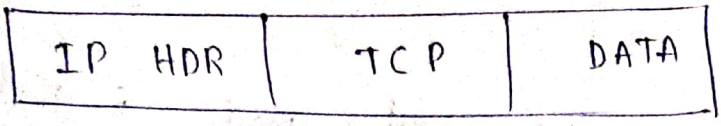
2. Authentication Header (AH)

* it also provides data integrity, authentication and anti replay and it does not encryption.
* the anti replay protection, protects against unauthorized transmission of packets.
* it does not protect data's confidentiality.

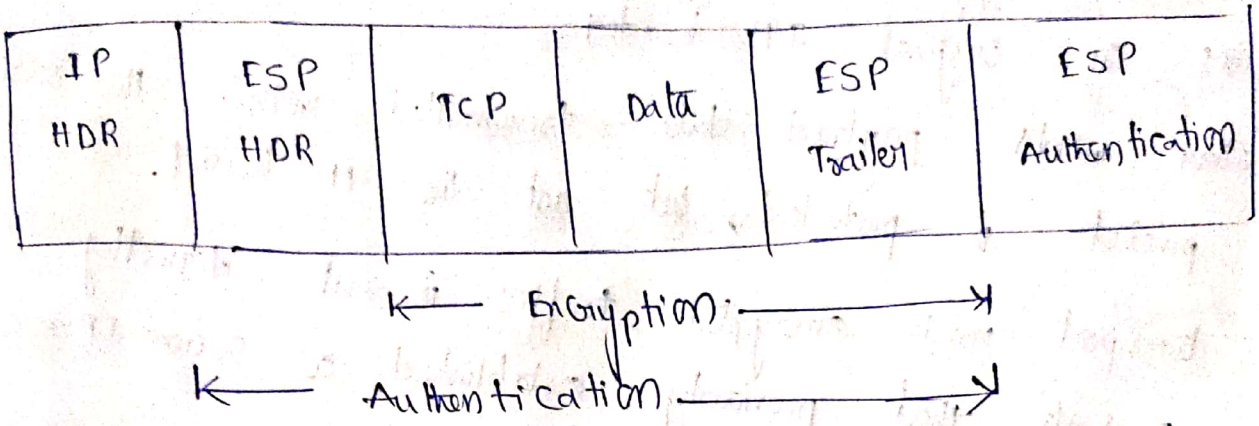


3. Internet Key Exchange (IKE)

* it is a n/w security protocol designed to dynamically exchange encryption keys and find a way over security association (SA) b/w two devices.
* the Security Association (SA) establishes shared security attributes b/w 2 network entities to support secure communication.



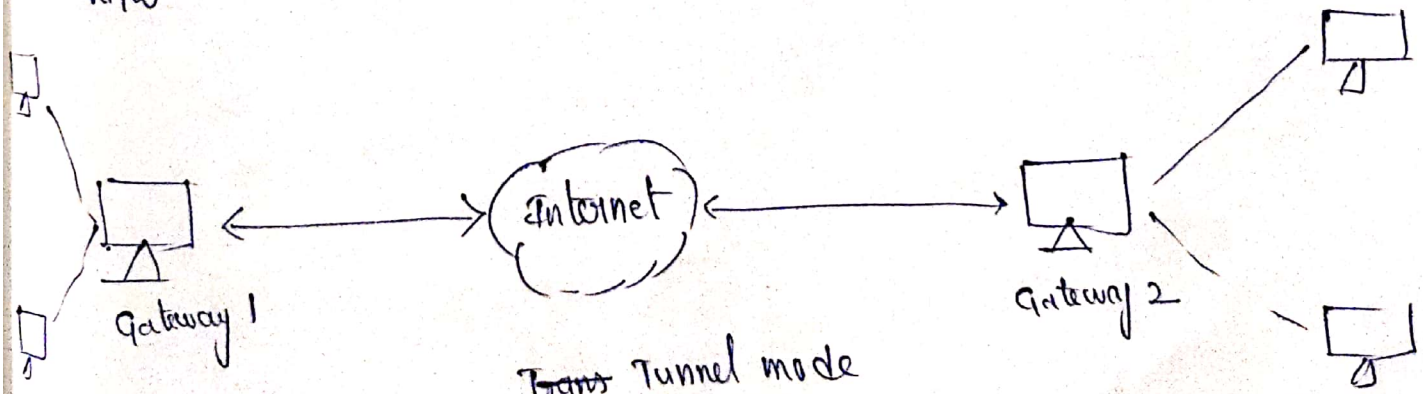
original packet



Modes of IPSec

1. Tunnel Mode

- In tunnel mode, the entire original IP packet is encapsulated to become the payload of a new IP packet.
- Additionally, a new IP header is added on top of the original IP packet.
- tunnel mode is useful for protecting traffic b/w different N/w



Trans Tunnel mode

2. Transport Mode

→ The main difference in transport mode is that it retains the original IP header.

→ In other words, payload data transmitted within the original IP packet is protected, but not the IP header.

→ In transport mode, encrypted traffic is sent directly b/w 2 hosts that previously established a secure IPsec tunnel.