GOVT.POLYTECHNIC BAGEPALLI

NAME : ULLAS B A

REG NO : 136CS21055

PROGRAM : 3RD YEAR CSE

COURSE NAME : CYBERSECURITY

SEMINAR ON : VPN

Content

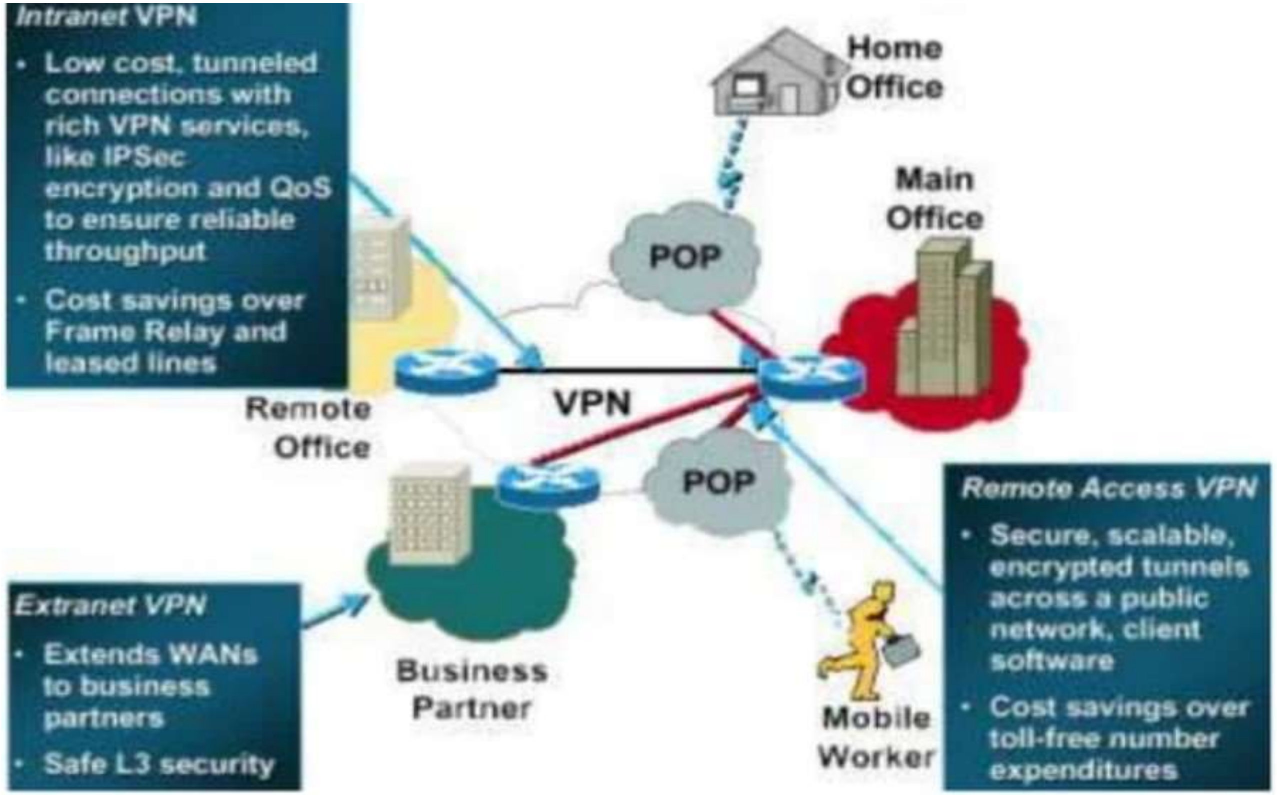
- What is VPN
- Types of VPN’s
- How does it works ?
- Protocols
- Security: firewall
- VPN devices
- Advantages
- Disadvantages
- Features
- conclusion

What is VPN ?

- A virtual private network, or VPN is an encrypted connection over the internet from a device to a network .The encrypted connection helps ensure that sensitive data is safety transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely

Types of VPN’s

- Remote-Access VPN
- Site-to-site VPN(**intranet-based**)
- Site-to-site VPN(**extranet-based**)



Intranet VPN

- Low cost, tunneled connections with rich VPN services, like IPSec encryption and QoS to ensure reliable throughput
- Cost savings over Frame Relay and leased lines

Extranet VPN

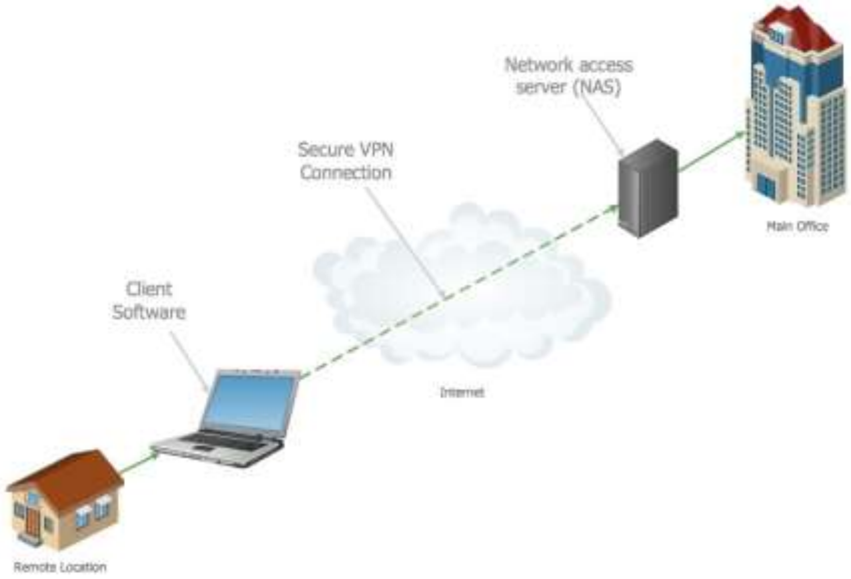
- Extends WANs to business partners
- Safe L3 security

Remote Access VPN

- Secure, scalable, encrypted tunnels across a public network, client software
- Cost savings over toll-free number expenditures

Remote-Access VPN

- A remote access VPN is for home or travelling users who need to access their central LAN from a remote location.
- They dial their ISP and connect over the internet to the LAN.
- This is made possible by installing a client software program on the remote user's Laptop or PC that deals with the encryption and decryption of the VPN traffic between itself and the VPN gateway on the central LAN.



SITE-TO-SITE VPN

- **Intranet-based –** if a company has one or more remote locations that they wish to join in a single privet network , they can cereate an intranet VPN to connect LAN to LAN.
- **Extranet-based –** when a company has a close relationship with another company (for example, a partner, supplier or customer) they can build an extranet VPN that connects LAN to LAN, and that allows all of the various companies to work in a shared environment.

Protocals used in VPN

- PPTP – Poin-to-point tunneling protocol.
- L2tp – layers to tunneling protocol.
- IPSec – Internet protocol security.
- SSL – is not used as much as the ones above.
- Encryption.

VPN Security: Firewall

A well-designed VPN uses several methods for keeping your connection and data secure:

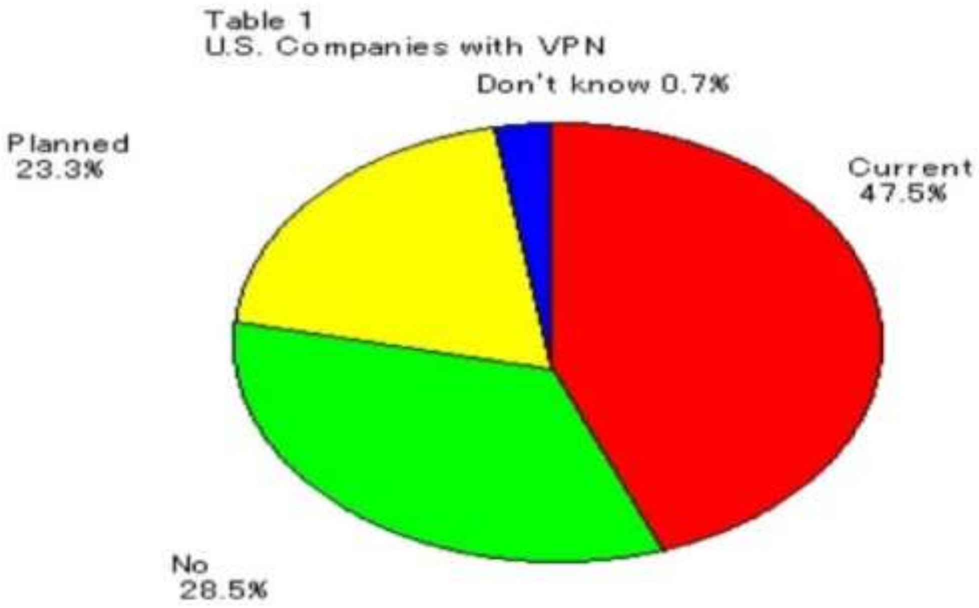
- **Firewalls**
- **Encryption**
- **IPSec**
- **AAA Server**
- You can set firewalls to restrict the number of open ports, what type of packets are passed through and which protocols are allowed through.

VPN DEVICES

- Hardware
- Firewall
- Software

VPN Features

- **security –** tunneling support between sites with at least 128bit encryption of the data.
- **Scalability –** extra users and bandwidth can be added easily to adapt to new requiremens.
- **Services –** quality of service features, including bandwidth, management and traffic shaping, are important to avoid congestion.
- **Management –** reports on user activity, management of user policies and monitoring of the VPN as a whole.



VPN Advantages

- Multiple telephone lines and banks of modems at the central site are not required.
- A reduction in the overall telecommunication infrastructure – as the IPS provides the bulk of the network.
- Reduced cost of management, maintenance of equipment and technical support.
- Simplifies network topology by eliminating modem pools and a private network infrastructure.
- VPN functionality is already present in some IT equipments.

VPN Disadvantages

- If the IPS are internet connection is down, So is the VPN .
- The central site must have a permanent internet connection so that remote clients and other sites can connect at anytime
- VPNs may provide each user with less bandwidth thana dedicated line solution
- Existing firewall ,proxies ,routers and hubs may not support VPN transmissions.

Thank you….!