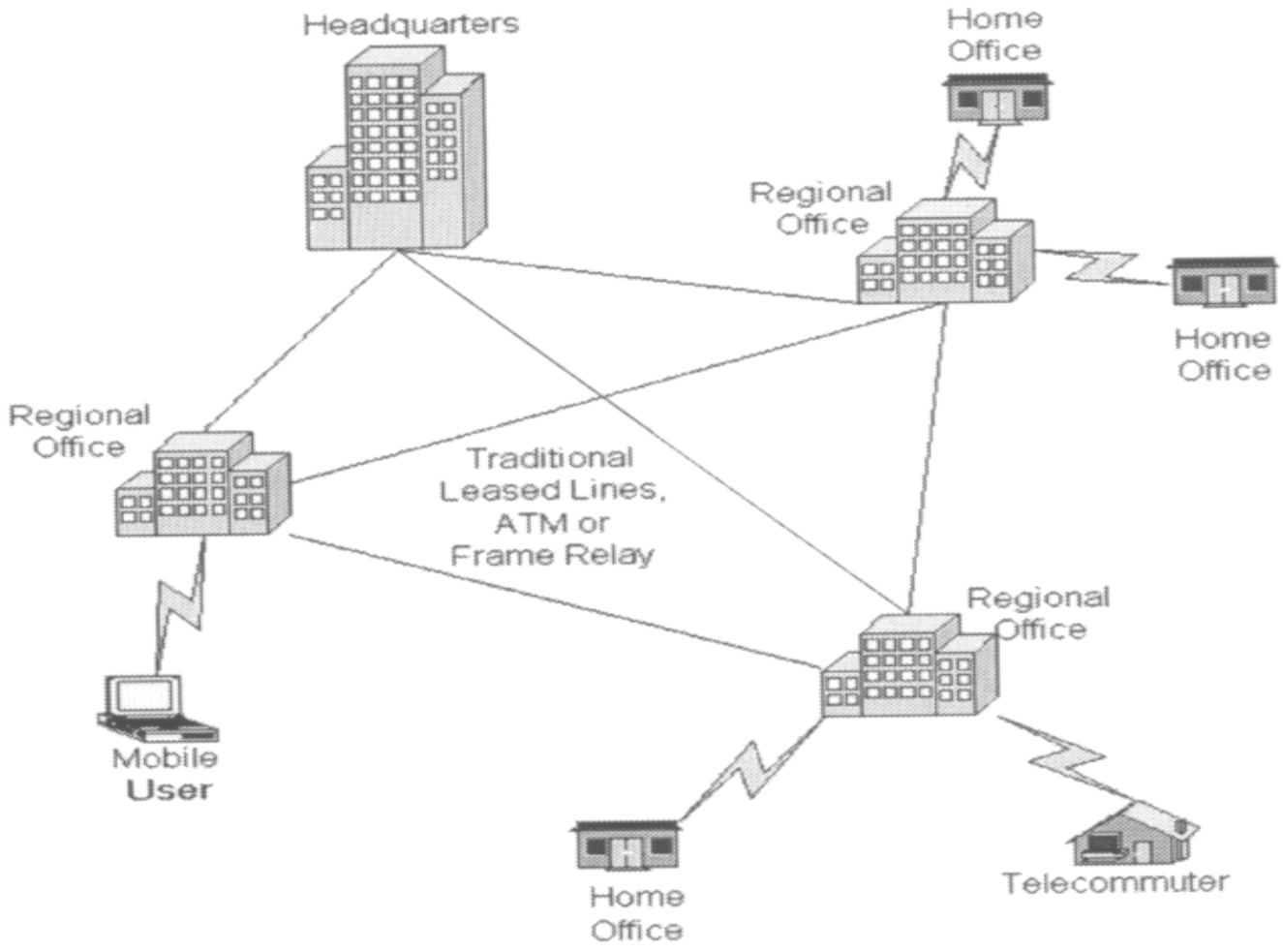
VIRTUAL PRIVATE NETWORKS (VPN)

Niti gupta

Traditional Connectivity



[From Gartner Consulting]

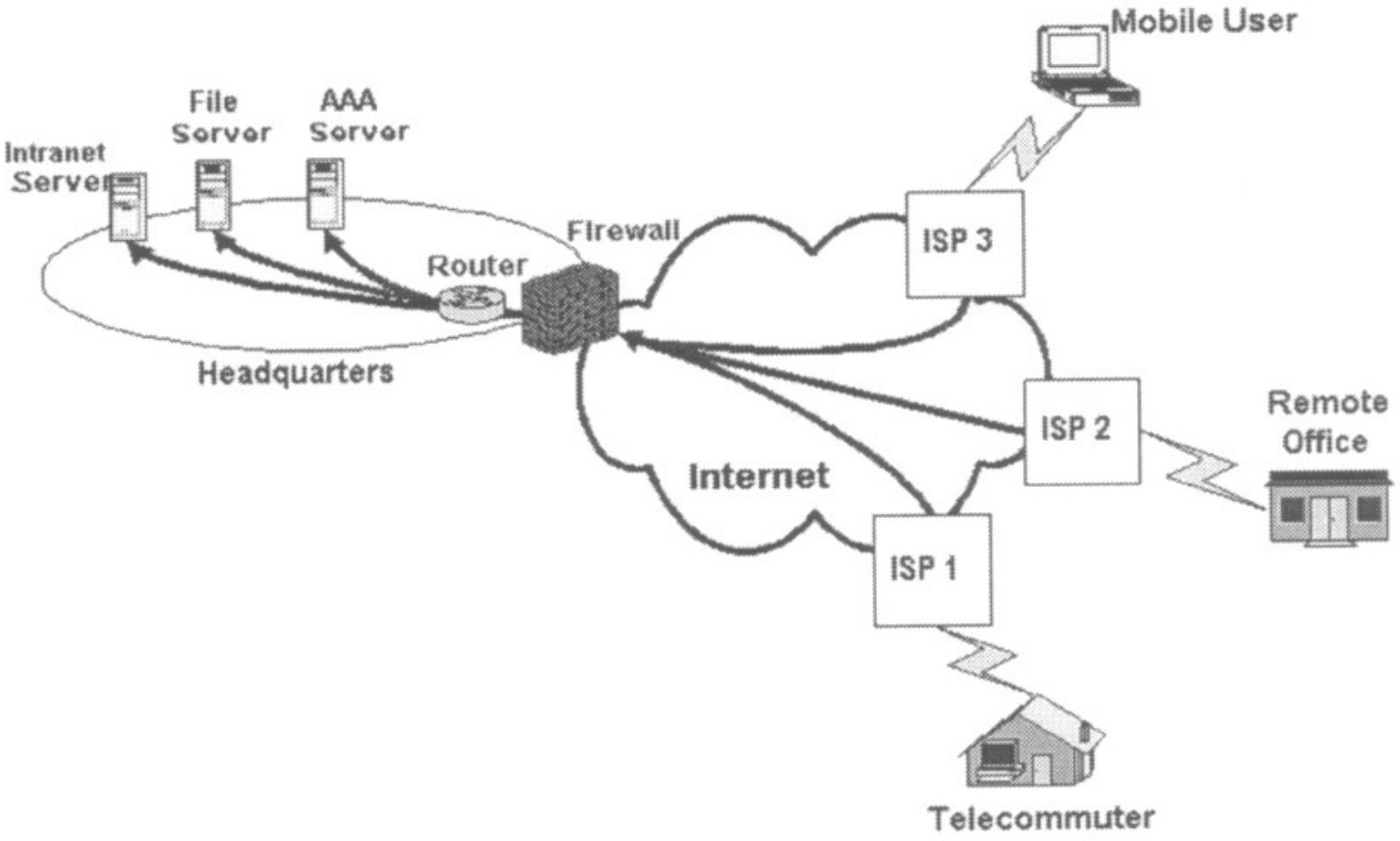
What is VPN?

- Virtual Private Network is a type of private network that uses public telecommunication, such as the Internet, instead of leased lines to communicate.
- Became popular as more employees worked in remote locations.
- Terminologies to understand how VPNs work.

Private Networks vs. Virtual Private Networks

- Employees can access the network (Intranet) from remote locations.
- Secured networks.
- The Internet is used as the backbone for VPNs
- Saves cost tremendously from reduction of equipment and maintenance costs.
- Scalability

Remote Access Virtual Private Network



Brief Overview of How it Works

- ✓ Two connections – one is made to the Internet and the second is made to the VPN.
- ✓ Datagrams – contains data, destination and source information.
- ✓ Firewalls – VPNs allow authorized users to pass through the firewalls.
- ✓ Protocols – protocols create the VPN tunnels.

Four Critical Functions

- Authentication – validates that the data was sent from the sender.
- Access control – limiting unauthorized users from accessing the network.
- Confidentiality – preventing the data to be read or copied as the data is being transported.
- Data Integrity – ensuring that the data has not been altered

Encryption

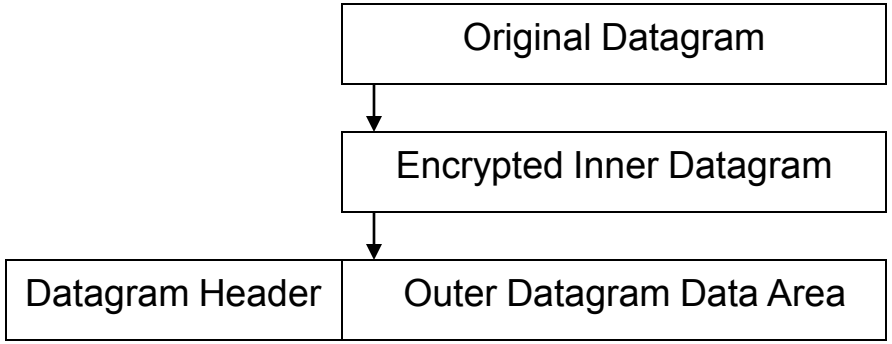
- Encryption -- is a method of “scrambling” data before transmitting it onto the Internet.
- Public Key Encryption Technique
- Digital signature – for authentication

Tunneling with VPN

- Tunneling is the process of placing an entire data packet within another packet (which provides the routing information) and sending it over the internet. The path through which the packets travel is called tunnel. For a tunnel to be established, both the tunnel client and the tunnel server must be using the same tunneling protocol.

Tunneling

A virtual point-to-point connection made through a public network. It transports encapsulated datagrams.



Data Encapsulation [From Comer]

Two types of end points:

- Remote Access
- Site-to-Site

Types of VPN Tunneling

- VPN supports two types of tunneling:

1. Voluntary and
2. Compulsory

Both types of tunneling are commonly used

In **voluntary tunneling** the VPN client manages connection setup. The client first make the connection to the carrier network protocol (an ISP). Then the VPN clients application creates the tunnel to a VPN server over this live connection.

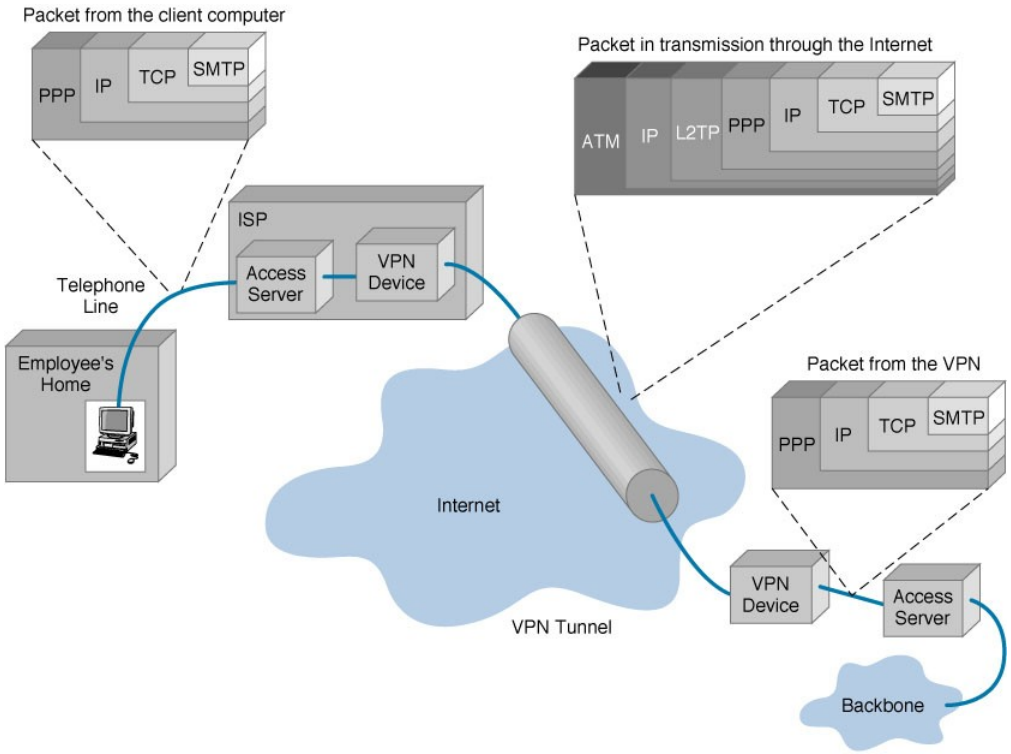
Types of VPN Tunneling

- In **compulsory tunneling**, the carrier network provider manages VPN connection setup. When the client first makes an ordinary connection to the carrier, the carrier in turn immediately brokers a VPN connection between that client and a VPN server. From the client point of view, VPN connections are setup in just one step compared to the two step procedure required for voluntary tunnels.

Four Protocols used in VPN

- PPTP -- Point-to-Point Tunneling Protocol
- L2TP -- Layer 2 Tunneling Protocol
- IPsec -- Internet Protocol Security
- SOCKS – is not used as much as the ones above

VPN Encapsulation of Packets

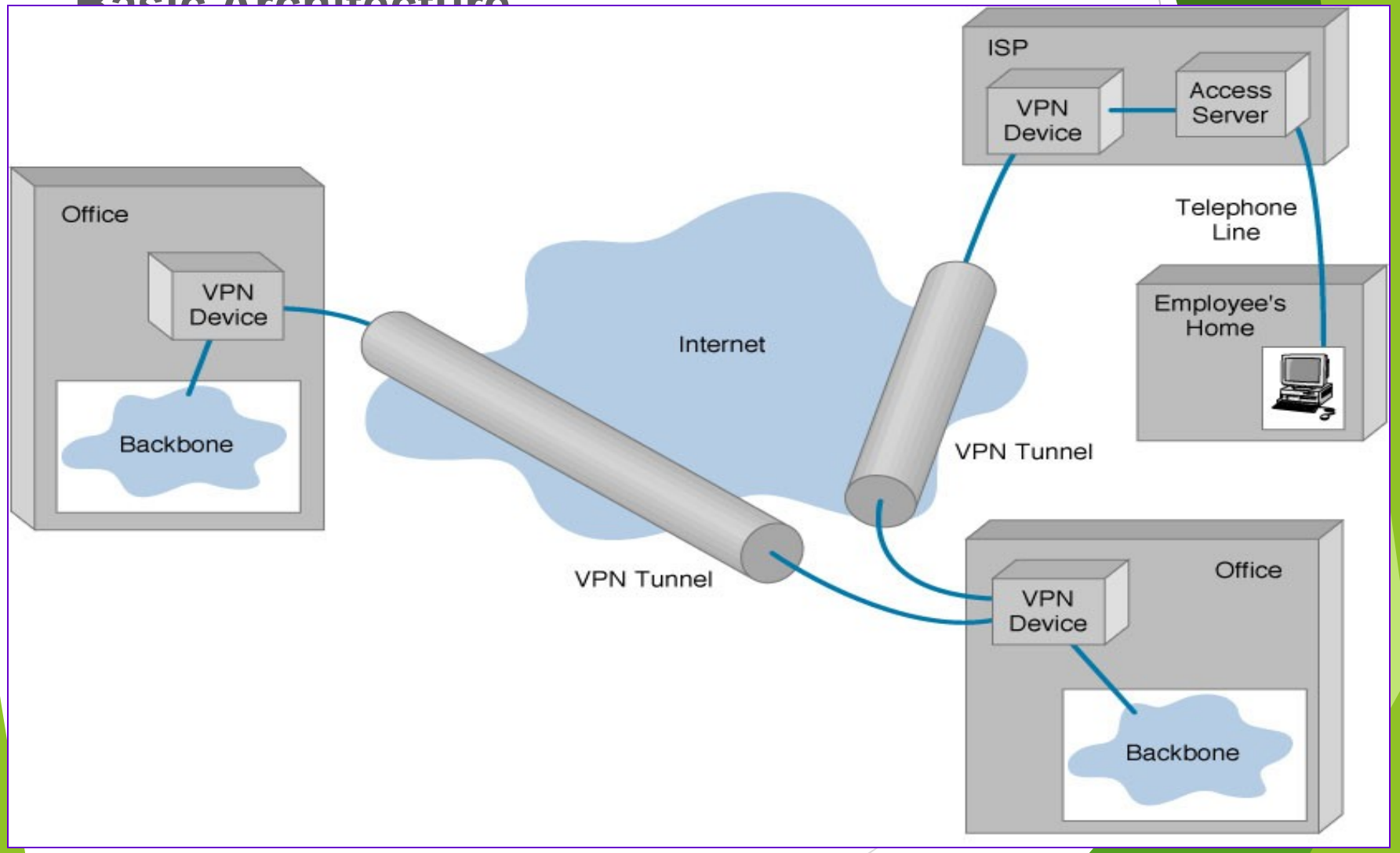


Types of Implementations

- What does “implementation” mean in VPNs?
- 3 types
  - Intranet – Within an organization
  - Extranet – Outside an organization
  - Remote Access – Employee to Business

Virtual Private Networks (VPN)

Basic Architecture



Device Types

- What it means
- 3 types
  - Hardware
  - Firewall
  - Software

Device Types: Hardware

- Usually a VPN type of router

Pros

- Highest network throughput
- Plug and Play
- Dual-purpose

Cons

- Cost
- Lack of flexibility

Device Types: Firewall

- More security?

Pros

- "Harden" Operating System
- Tri-purpose
- Cost-effective

Cons

- Still relatively costly

Device Types: Software

- Ideal for 2 end points not in same org.
- Great when different firewalls implemented

Pros

- Flexible
- Low relative cost

Cons

- Lack of efficiency
- More labor training required
- Lower productivity; higher labor costs

Advantages VS. Disadvantages

Advantages: Cost Savings

- Eliminating the need for expensive long-distance leased lines
- Reducing the long-distance telephone charges for remote access.
- Transferring the support burden to the service providers
- Operational costs

- Cisco VPN Savings Calculator

Advantages: Scalability

- Flexibility of growth
- Efficiency with broadband technology

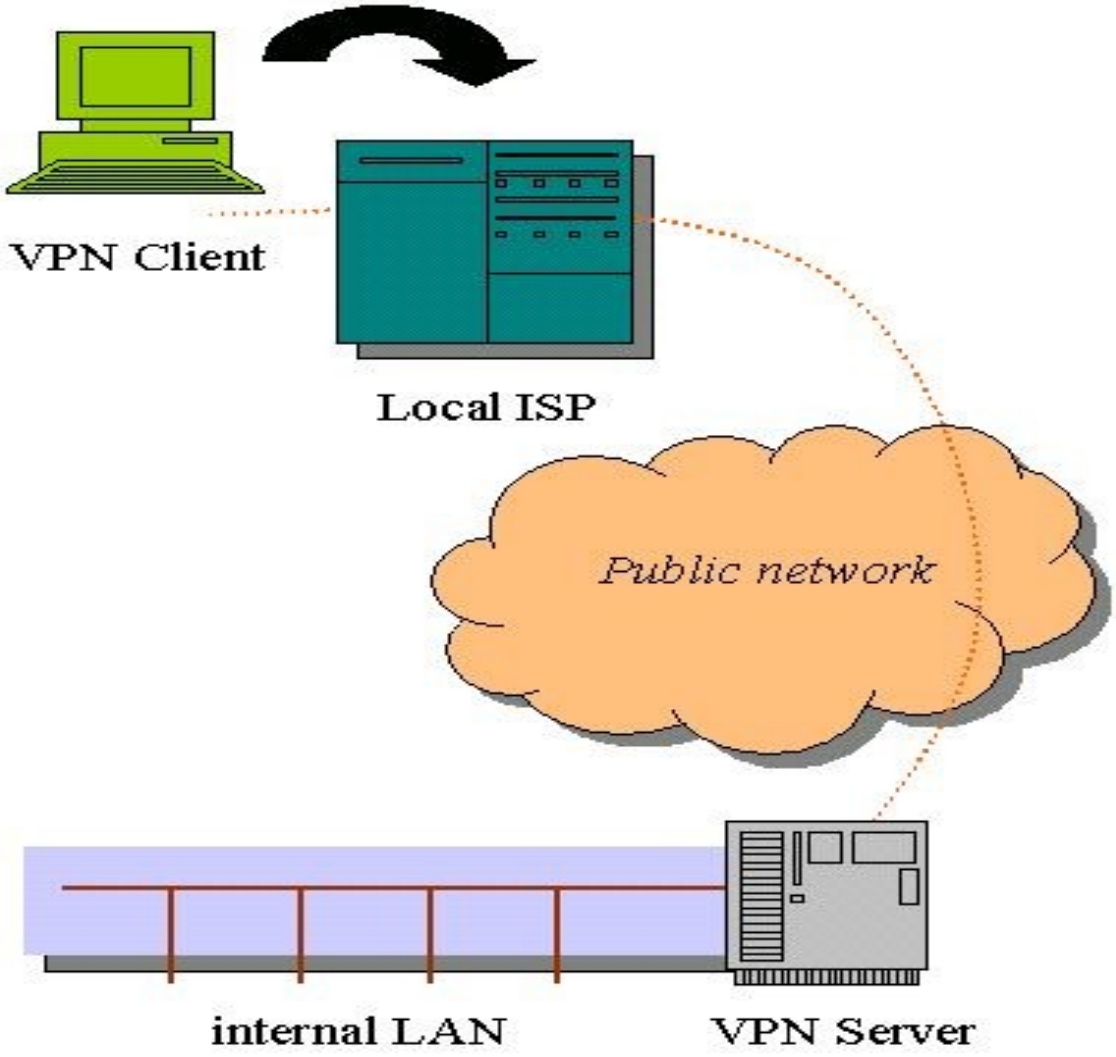
Disadvantages

- VPNs require an in-depth understanding of public network security issues and proper deployment of precautions
- Availability and performance depends on factors largely outside of their control
- Immature standards
- VPNs need to accommodate protocols other than IP and existing internal network technology

Applications: Site-to-Site VPNs

- Large-scale encryption between multiple fixed sites such as remote offices and central offices
- Network traffic is sent over the branch office Internet connection
- This saves the company hardware and management expenses

Site-to-Site VPNs



Applications: Remote Access

- Encrypted connections between mobile or remote users and their corporate networks
- Remote user can make a local call to an ISP, as opposed to a long distance call to the corporate remote access server.
- Ideal for a telecommuter or mobile sales people.
- VPN allows mobile workers & telecommuters to take advantage of broadband connectivity.
  i.e. DSL, Cable

Industries That May Use a VPN

- **Healthcare:** enables the transferring of confidential patient information within the medical facilities & health care provider
- **Manufacturing**: allow suppliers to view inventory & allow clients to purchase online safely
- **Retail:** able to securely transfer sales data or customer info between stores & the headquarters
- **Banking/Financial:** enables account information to be transferred safely within departments & branches
- **General Business:** communication between remote employees can be securely exchanged

Some Businesses using a VPN

- CVS Pharmaceutical Corporation upgraded their frame relay network to an IP VPN
- ITW Foilmark secured remote location orders, running reports, & internet/intranet communications w/ a 168-bit encryption by switching to OpenReach VPN
- Bacardi & Co. Implemented a 21-

Where Do We See VPNs Going in the Future?

- VPNs are continually being enhanced.

  Example: Equant NV

- As the VPN market becomes larger, more applications will be created along with more VPN providers and new VPN types.
- Networks are expected to converge to create an integrated VPN
- Improved protocols are expected, which will also improve VPNs.

Security concerns in VPN

- SSL VPNs serve as gateways into corporate infrastructure and as such, security is a critical component of any SSL VPN offering. So important are the security-related capabilities of SSL VPN products that the differences in the security features set across products often determine which SSL VPN an enterprise will choose to deploy.

SSL VPN security falls into three categories:

Security concerns in VPN

- **Authentication and Authorization:**

Users gain access to valuable information and systems through the SSL VPN. Because of this, it is critical to ensure that only authorized users access resources through the SSL VPN and that individual users access only those resources that they are supposed to access.

Contd..

- **Endpoint Security:**

Endpoint security is sometimes known as Client-Side Security or Browser-Side Security. It refers to technology implemented to prevent any security-related problems occurring on devices used to access resources via the SSL VPN. It is important to realize that as opposed to earlier remote-access technologies, SSL VPN technology allows access from machines not known to be secure and as such, the endpoint concerns are different from the endpoint issues present in older

Contd…

- **Server-Side Security:**

Server-Side security, sometimes known as Network Security, refers to protecting internal corporate resources including the SSL VPN server itself from falling victim to any form of compromise.

Authentication mechanism in VPN

- Tunnel endpoints must authenticate before secure VPN tunnels can establish.
- User-created remote access VPNs may use passwords, biometrics, two-factor authentication or other cryptographic methods.
- Network-to-network tunnels often use passwords or digital certificates, as they permanently store the key to allow the tunnel to establish automatically and without intervention from the user

Password

- A **password** is a secret word or string of characters that is used for authentication, to prove identity or gain access to a resource (example: an access code is a type of password). The password should be kept secret from those not allowed access.

Biometrics

- **Biometrics** consists of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. In computer science, in particular, biometrics is used as a form of identity access management and access control. It is also used to identify individuals in groups that are under surveillance.

Two-factor authentications

- **Two-factor authentication** (TFA or 2FA) means using two independent means of evidence to assert an entity's identity to another entity. Two-factor authentication is commonly found in electronic computer authentication, where basic authentication is the process of a requesting entity presenting some evidence of its identity to a second entity.

Types of two-factor authentication

- **Tokens:** One form of 'something you have' is the smart card and USB tokens. Differences between the smart card and USB token are diminishing; both technologies include a microcontroller, an OS, a security application, and a secured storage area.
- **Wireless Tokens:** A new quality of tokens has been developed to ease the authentication process without keying character sequences and with automatic pairing of authentication factors. Presumed the bearer of the authentication factors prepares himself in good separation from other similar entities, the achieved pairing status may be maintained for all the daytime and especially during worktime without repetition of the pairing process. Then the problem of lost laptop or left phone may be prevented by automatic alarm in case of unwanted access of arms length.

Contd…

- **Virtual Token**

Virtual tokens are a new concept in multi-factor authentication first introduced in 2005 by security company, Sestus. Virtual tokens reduce the costs normally associated with implementation and maintenance of multi-factor solutions by utilizing the user's existing internet device as the "something the user has" factor. Also, since the user's internet device is communicating directly with the authenticating website, the solution does not suffer from man-in-the-middle attacks and other forms of online fraud

Contd…

- **Magnetic Cards**

Magnetic cards (credit cards, debit cards, ATM cards, gift cards, etc) combined with secure, encrypting card readers provide a possible solution for two-factor/strong authentication.

Contd…

- **SMS One Time Password**

SMS One time password uses information sent in an SMS to the user as part of the login process. One scenario is where a user either registers (or updates) their contact information on a website. During this time the user is also asked to enter his or her regularly used telephone numbers (home, mobile, work, etc). The next time the user logs in to the website, they must enter their username and password; if they enter the correct information, the user then chooses the phone number at which they can be contacted immediately from their previously registered phone numbers.

Contd…

- **Mobile Signature**

Mobile signatures are digital signatures created on a SIM card securely on a mobile device by a user's private key. In such a system text to be signed is securely sent to the SIM card on a mobile phone. The SIM then displays the text to the end-user who checks it before entering a PIN code to create a signature which is then sent back to the service provider

Contd…

- **Digital Certificates**

Digital Client certificates are a PKI solution for enabling the enhanced user identification and access controls needed to protect sensitive online information. Digital certificates can also be stored and transported on smart cards or USB tokens for use when traveling. Each certificate can only be used to authenticate one particular user because only that user's computer has the corresponding and unique private key needed to complete the authentication process. Client certificates are delivered electronically, however, deployment and support of digital certificates have proven problematic

Assignment-3

1. Explain model of cryptographic system? What are the different concepts in cryptography
2. What do you understand by public key cryptography?
3. What are digital signature? Explain requirement of digital signature system.
4. Define firewall. Explain types of firewalls.
5. Explain network security. What are the different types of network attacks?
6. What are intrusion detection systems? Describe types of intrusion detection system.
7. What do you understand by VPN? Explain various types of VPN protocols and explain types of VPN.
8. What is the use of tunneling with VPN? What are the security concerns in VPN ?