SCSA 1502

COMPUTER NETWORKS AND DESIGN

Unit III- VPNS, INTRANETS & EXTRANETS

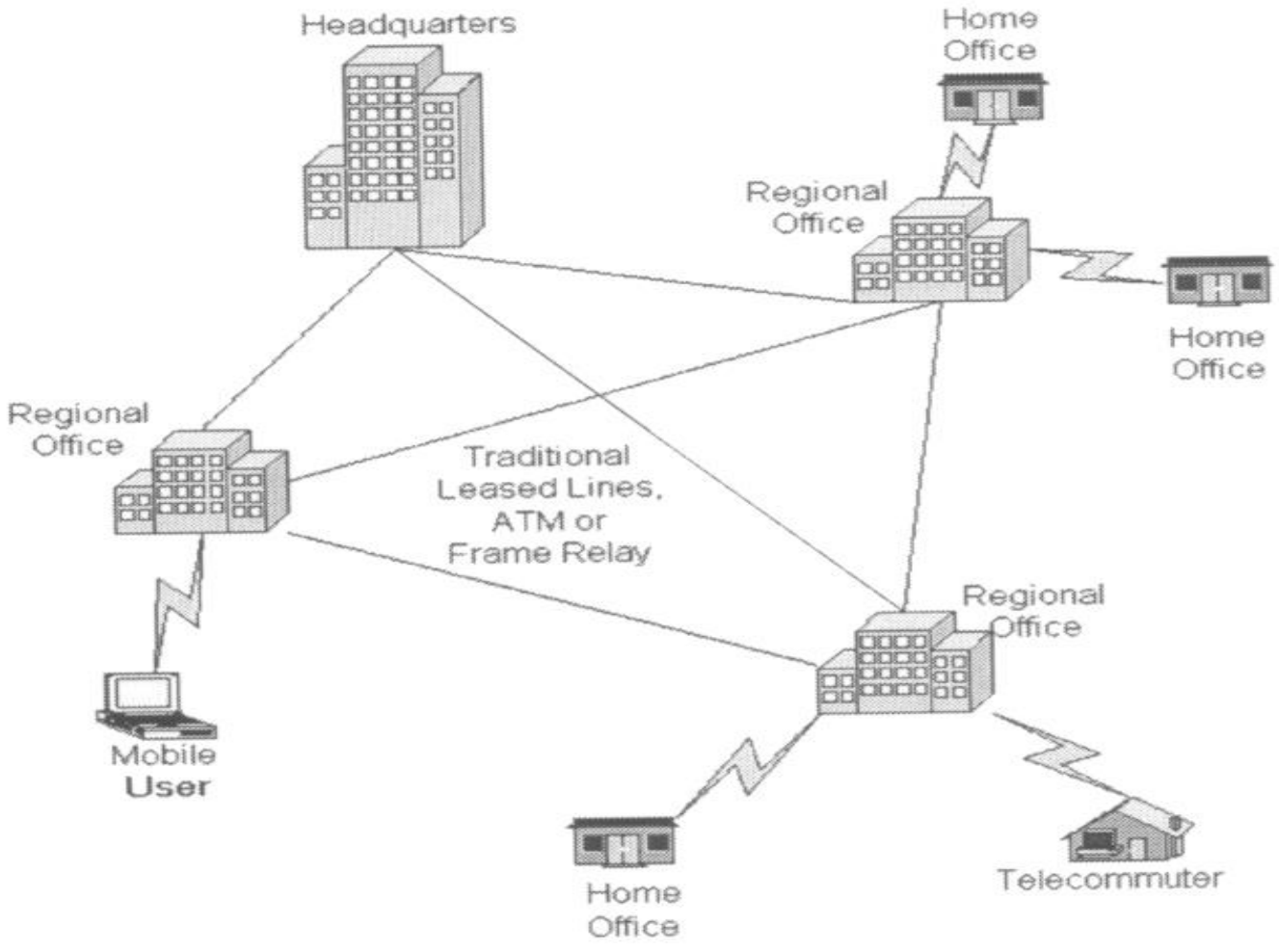
VPNS, INTRANETS AND EXTRANETS

UNIT 3

Virtual Network management and planning – VPNs for small businesses – Secure remote access in VPNs – IPSec VPNs – Integrating data centers with Intranets – Implementing and supporting Extranets.

Virtual Private Network - Introduction

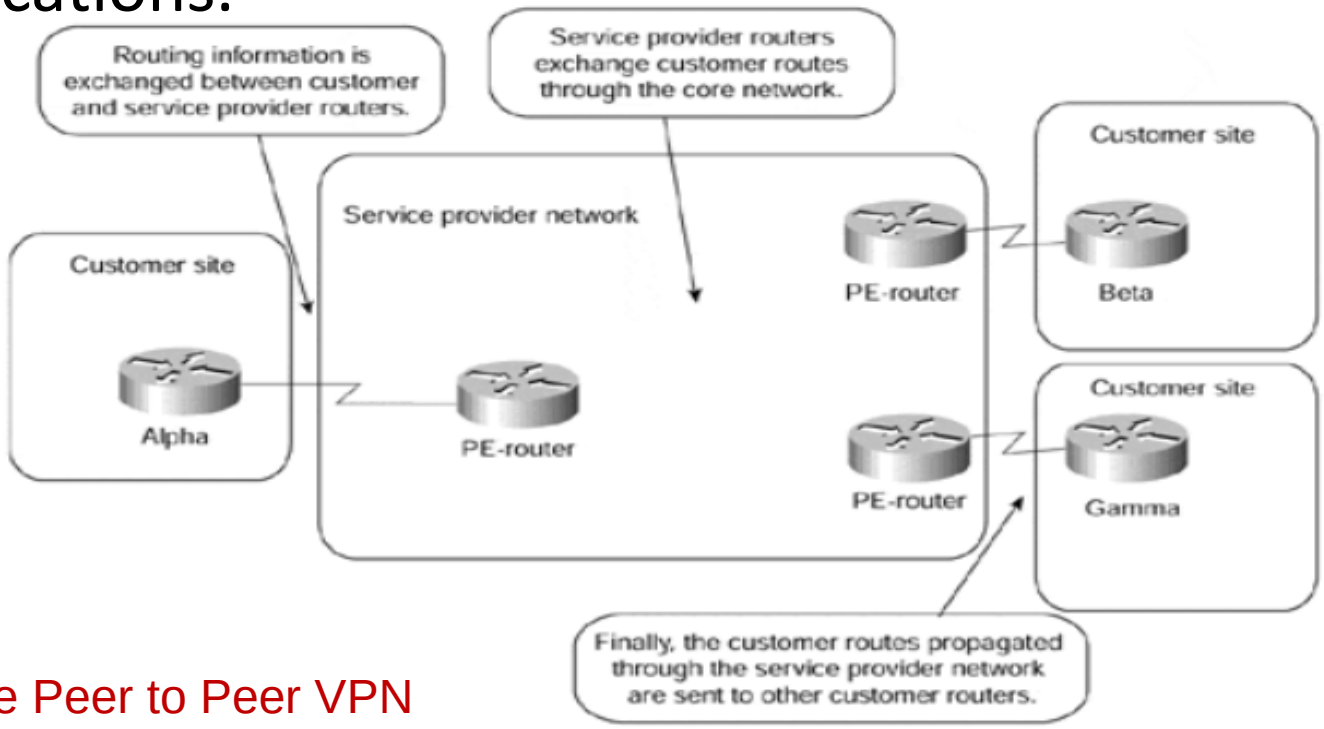
Traditional Connectivity:



[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.



Sample Peer to Peer VPN

VPN – Introduction

- A virtual private network extends a private network across a public network
- Enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.
- A VPN is a secure, point-to-point connection between two network end points

VPN – Introduction Contd.,

- A VPN establishes an encrypted channel that keeps a user's identity and access credentials, as well as any data transferred, inaccessible to hackers.
- A VPN is a **service that both encrypts your data and hides your IP address by bouncing your network activity through a secure chain to another server miles away**.
- This obscures your online identity, even on public Wi-Fi networks, so you can browse the internet safely, securely and anonymously.

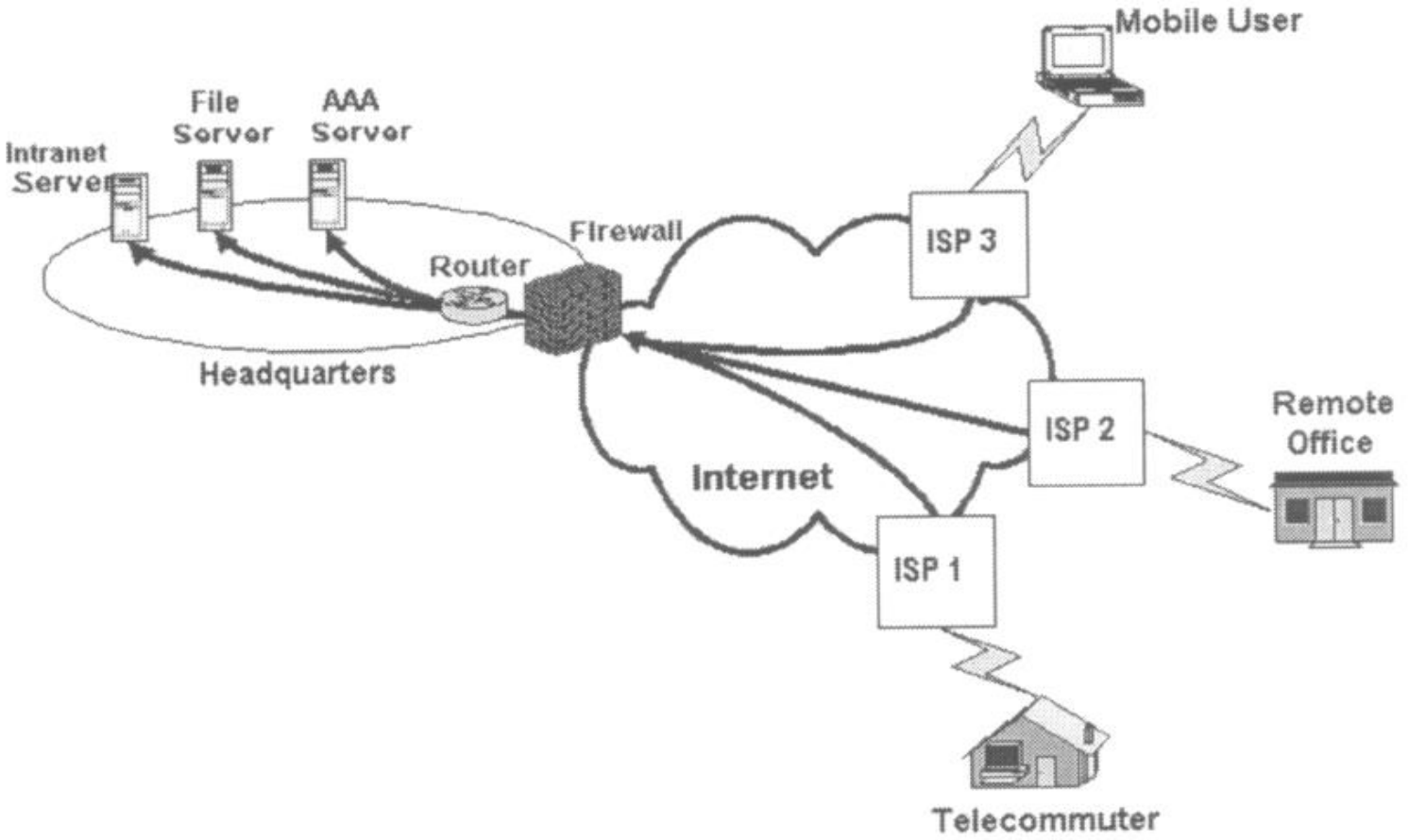
VPN – Introduction Contd.,

- Using a virtual private network (VPN) is usually a good idea, especially if you frequent public Wi-Fi.
- By encrypting your Wi-Fi connection, a VPN protects your communications from invasive eyes
- Plays a vital role in your overall digital defense. But using a **free VPN is a no good, very bad idea**.

Private Networks & VPN's

- 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



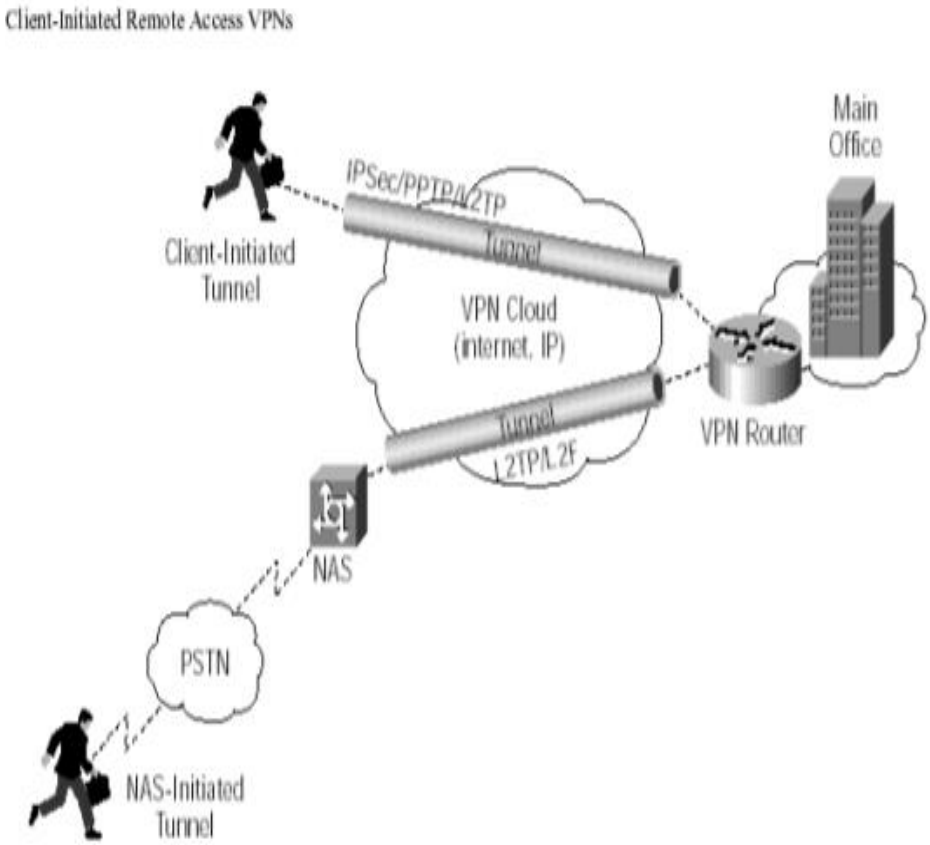
(From Gartner Consulting)

Remote Access VPN

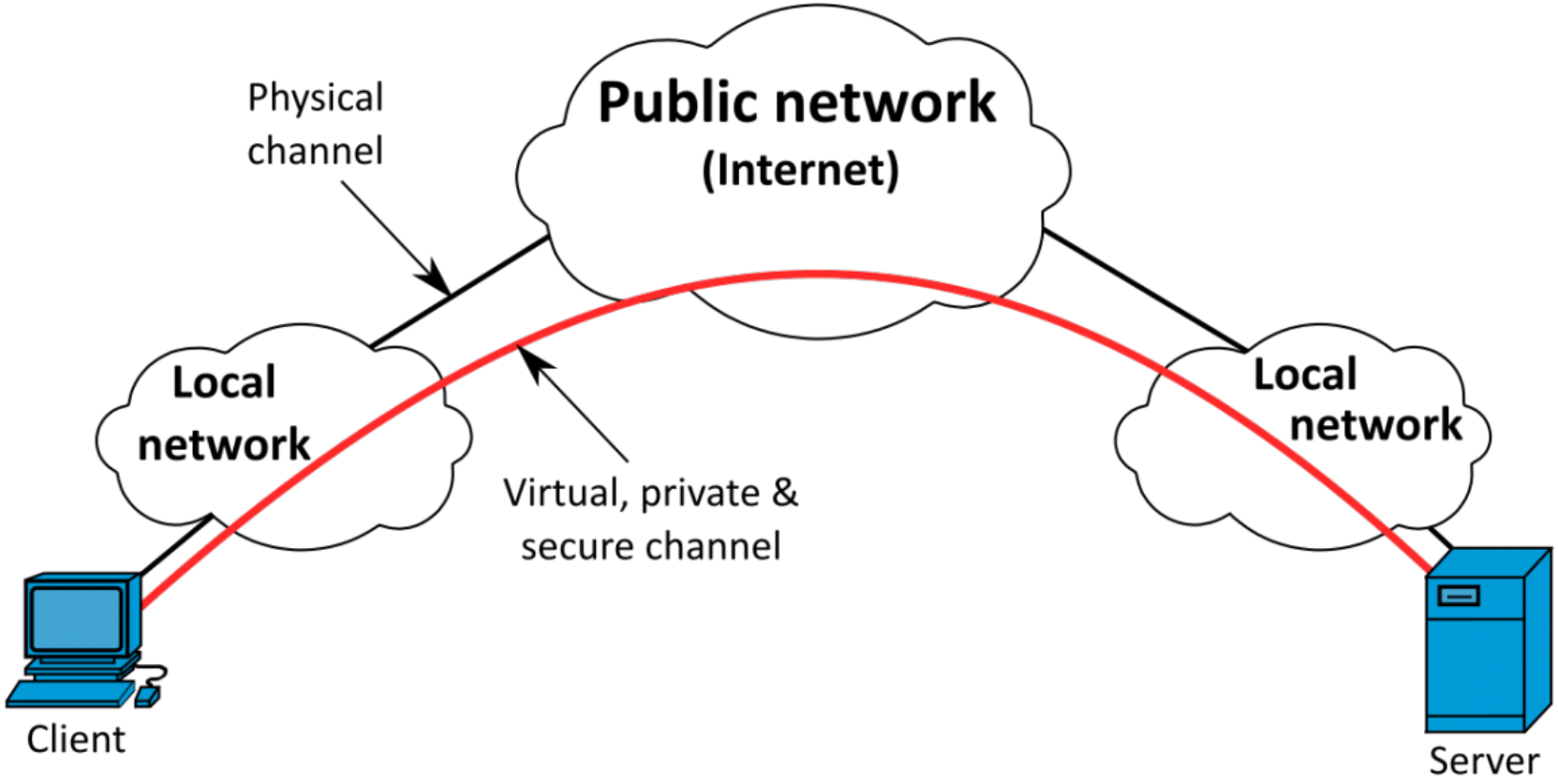
A **remote-access VPN** allows individual users to establish secure connections with a remote computer network.

There are two components required in a remote-access VPN. The first is a **network access server**(NAS).

The other required component of remote-access VPNs is client software



VPN – Schematic Representation



VPN - 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.

VPN - Four Critical Functions

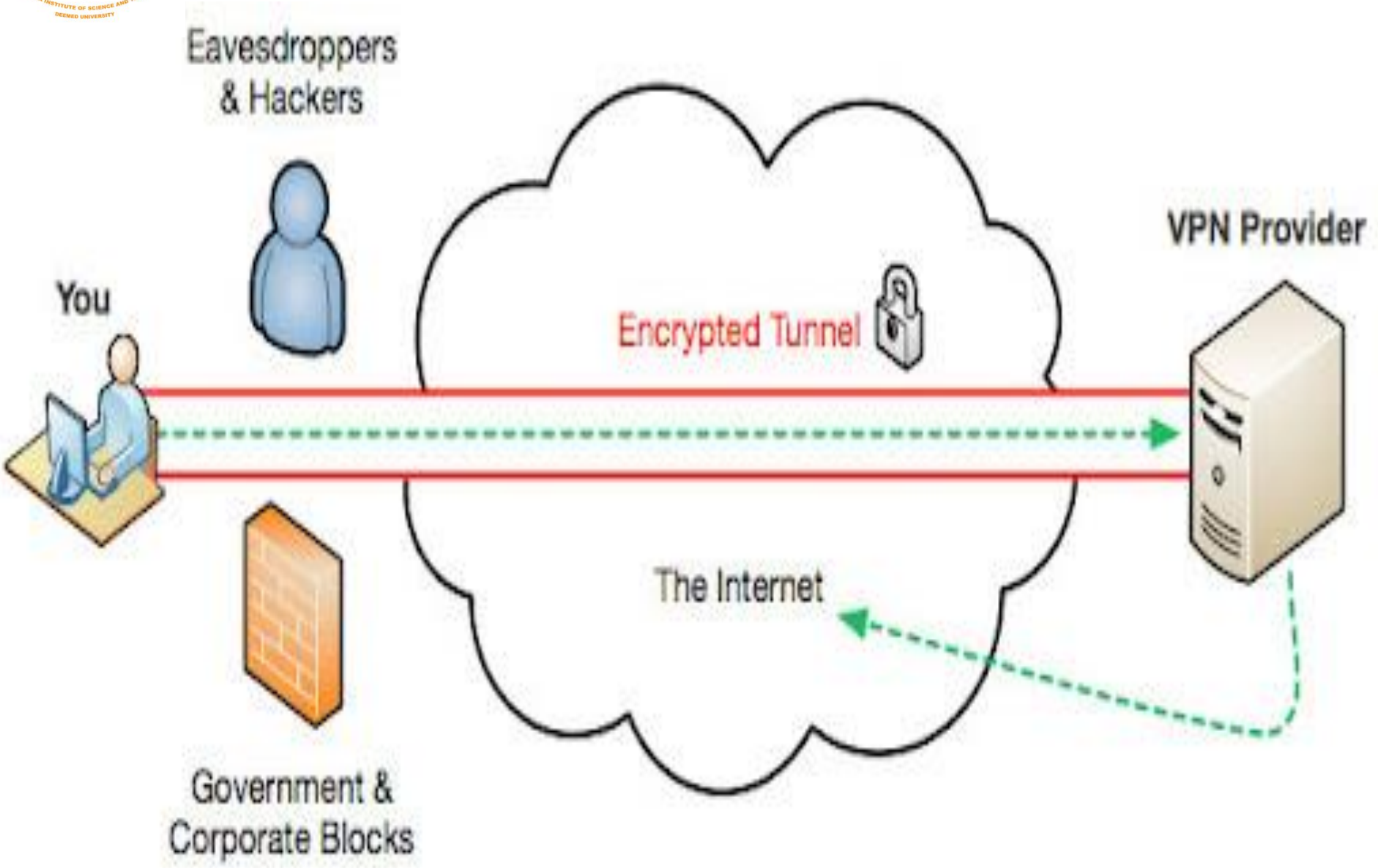
- Authentication – validates that the data was sent from the sender.
- Access control – limiting unauthorized users from accessing the network.
- Confidentiality – preventing the data to be read or copied as the data is being transported.
- Data Integrity – ensuring that the data has not been altered

VPN - **Encryption**

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

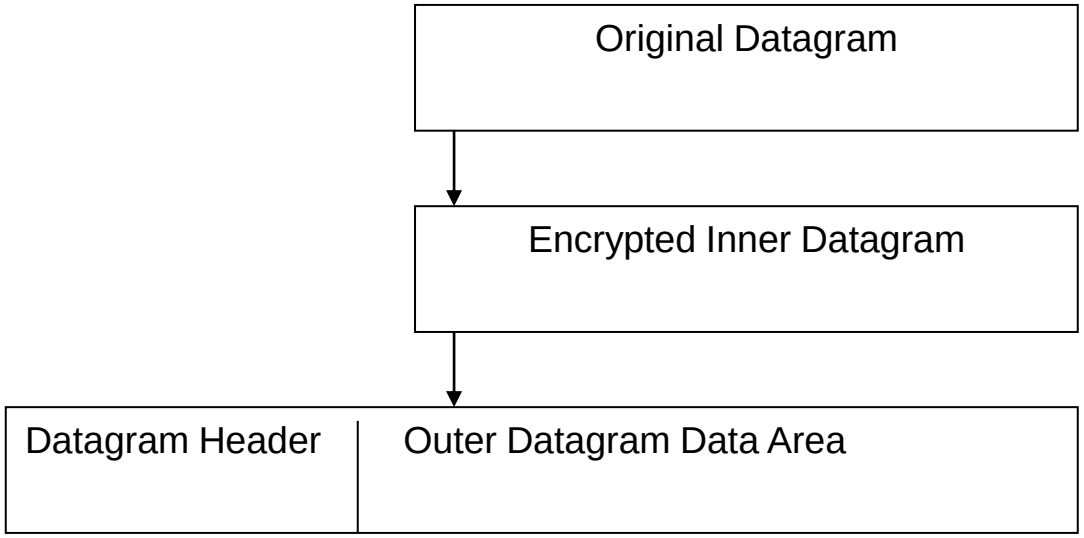
VPN - **Encryption**

- VPNs work by funneling all of **your internet traffic** through an encrypted pipe to the VPN server, making it more difficult for anyone on the internet to see which sites you are visiting or which apps you are using.


Eavesdroppers
& Hackers
You
Encrypted Tunnel
VPN Provider
The Internet
Government &
Corporate Blocks

VPN - Tunneling

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



Two types of end points:

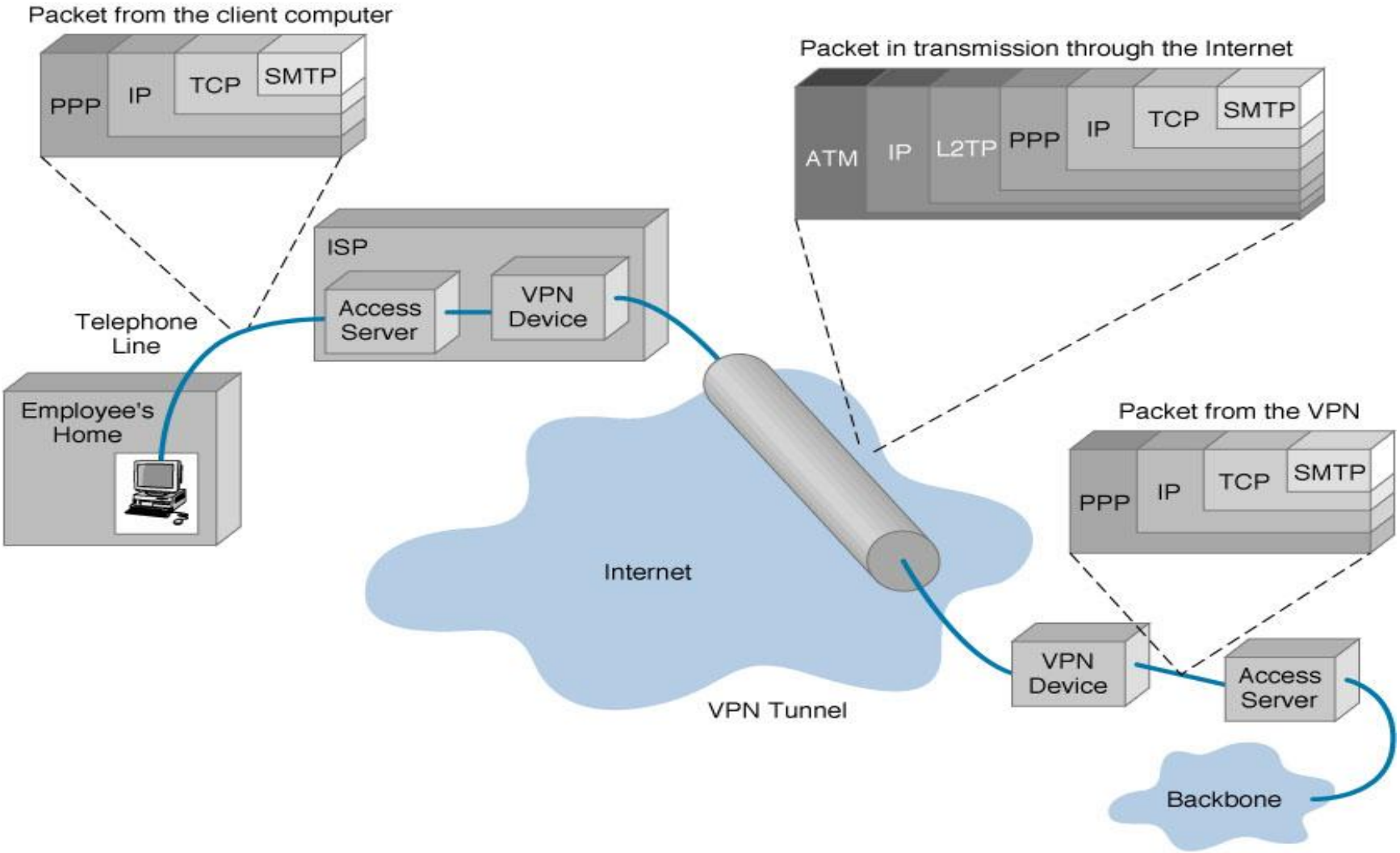
- ❑ Remote Access
- ❑ Site-to-Site

Data Encapsulation [From Comer]

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

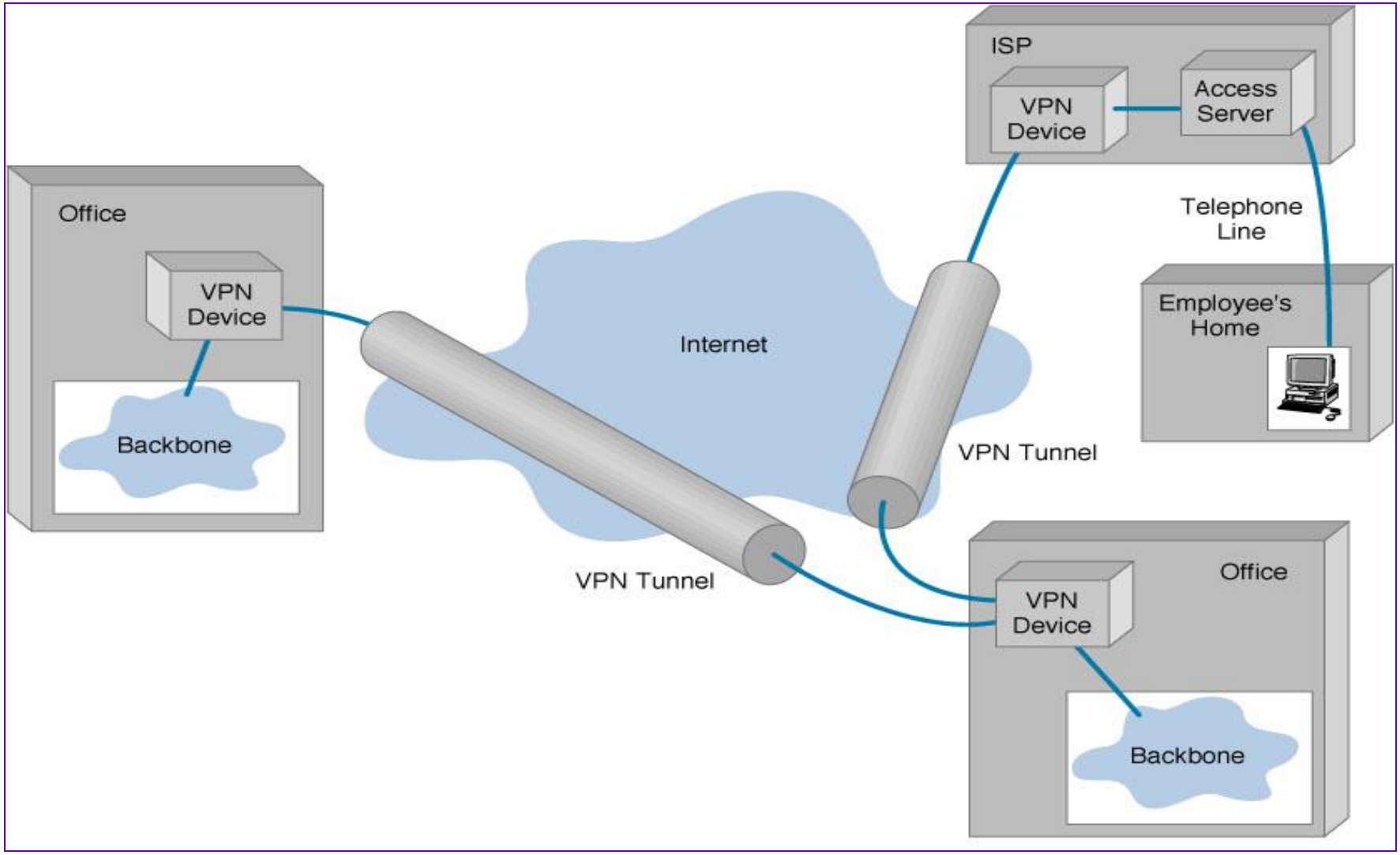


VPN - Types of Implementations

- What does “implementation” mean in VPNs?

- 3 types
  - Intranet – Within an organization
  - Extranet – Outside an organization
  - Remote Access – Employee to Business

VPN - Basic Architecture



VPN - Device Types

- 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

VPN - Device Types

Device Types: *Firewall*

- More security?

Pros

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

Cons

- Still relatively costly

VPN - Device Types

Device Types: *Software*

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

Pros

- Flexible
- Low relative cost

Cons

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

VPN

Advantages VS. Disadvantages

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**

VPN

Advantages VS. Disadvantages

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

VPN Advantages

- : **Scalability**
  - Flexibility of growth
  - Efficiency with broadband technology

- **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

- **Security** -- The VPN should protect data while it's traveling on the public network. If intruders attempt to capture the data, they should be unable to read or use it.

- **Reliability** -- Employees and remote offices should be able to connect to the VPN with no trouble at any time (unless hours are restricted), and the VPN should provide the same quality of connection for each user even when it is handling its maximum number of simultaneous connections.

VPN Disadvantages

VPNs require detailed understanding of network security issues and careful installation / configuration to ensure sufficient protection on a public network like the Internet.

The reliability and performance of an Internet-based VPN is not under an organization's direct control. Instead, the solution relies on an ISP and their quality of service.

VPN products and solutions from different vendors have not always been compatible due to issues with VPN technology standards. Attempting to mix and match equipment may cause technical problems, and using equipment from one provider may not give as great a cost savings.

VPN Applications in Industries

- **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

VPN Characteristics

- **Cheaper than WANs**
  - dedicated leased lines are very expensive
- **Easier to establish than WANs**
  - ISPs will usually help make the initial IP connection
  - hours for VPNs vs. weeks for WANs
- **Slower than LANs**
  - encryption/decryption takes time
  - typical LANS are 10-100 Mbps
    - endpoints connected by VPM may go through many router hops
      - minimize by using same ISP for everything
  - dial in users are going to be typically 56Kbps
- **Less reliable than WANs**
  - with WANs routers are under your control and performance is negotiated with provider, not so with VPN you only control initial IP connection
- **Less secure than isolated LANs or WANs**
  - because Internet is used hackers can find you
  - VPN protocol is one more thing to be attacked

Future of VPN

- 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.

Intranet, Extranet and Internet

- **Intranet** is shared content accessed by members within a single organization.
- **Extranet** is shared content accessed by groups through cross-enterprise boundaries.
- **Internet** is global communication accessed through the Web.

Intranet, Extranet & Internet – Continued.,

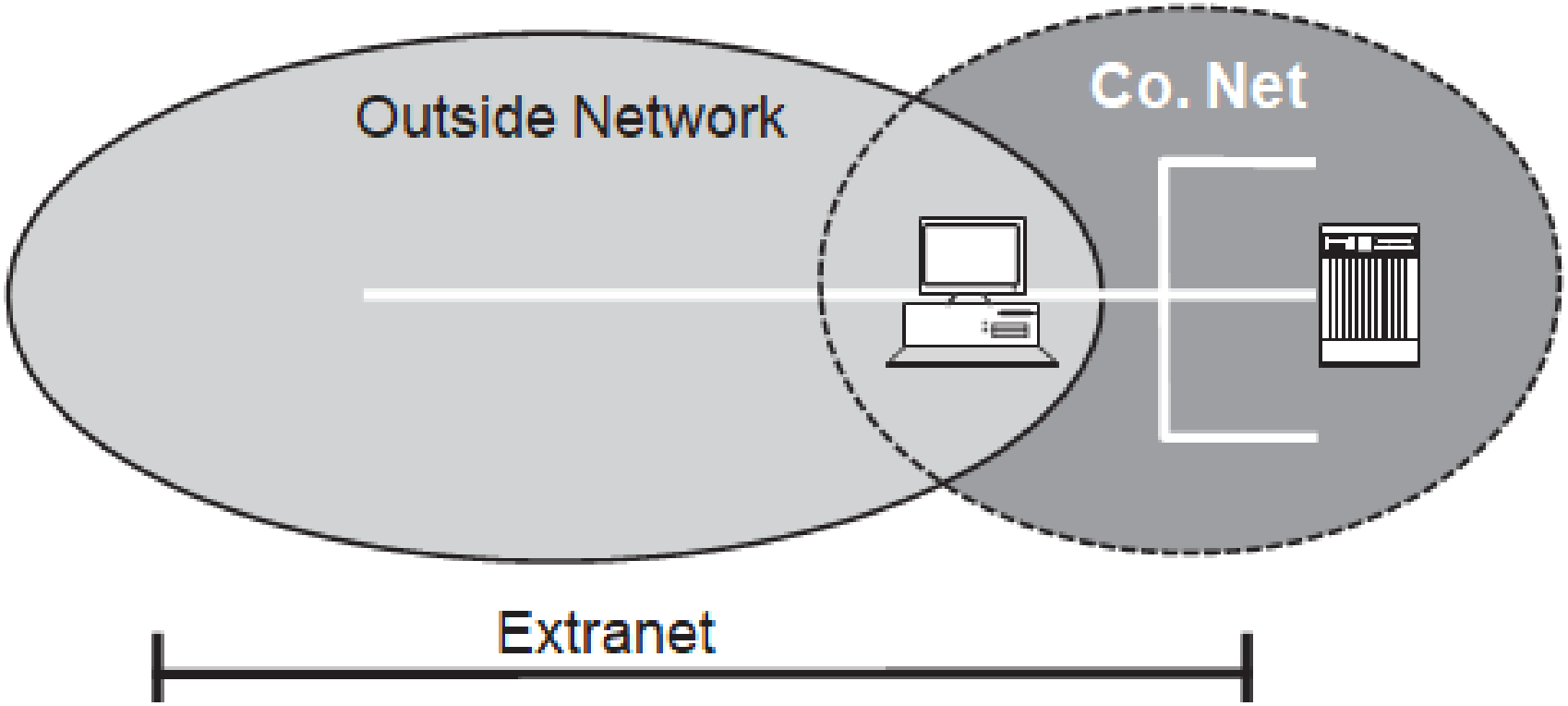
- Intranet VPNs **provides site to site internal connectivity within the company**. The collection of all internal company sites, connected in this way, is often referred to as the company's Intranet.
- Intranet VPNs provides the same level of connectivity and reliability as a fully private network.

Intranet, Extranet & Internet – Continued.,

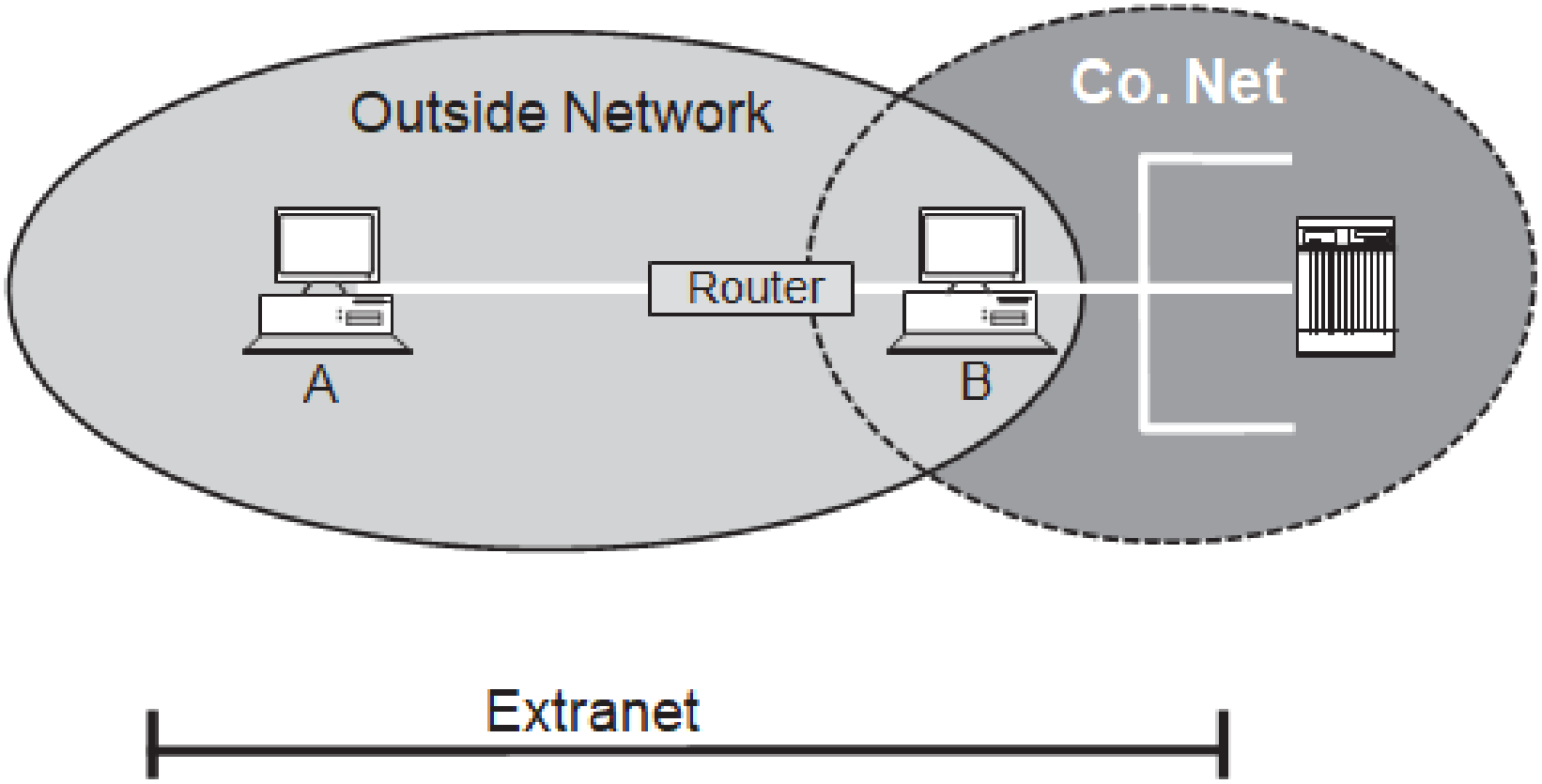
- An extranet VPN links **outside customers, suppliers, partners**, or communities of interest to an enterprise customer's network over a shared infrastructure using dedicated connections

- Extranet VPNs differ from intranet VPNs in that they allow access to users outside the enterprise.

Extranet Venn diagram

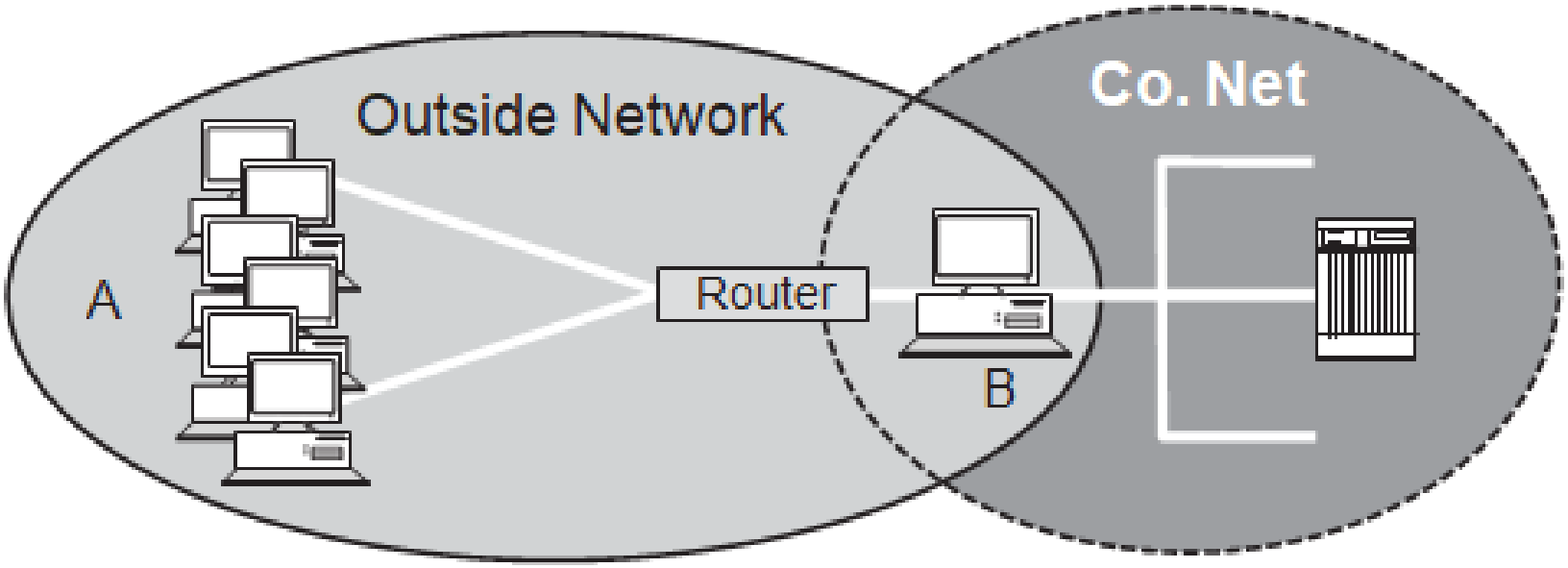


EXTRANET ARCHITECTURES

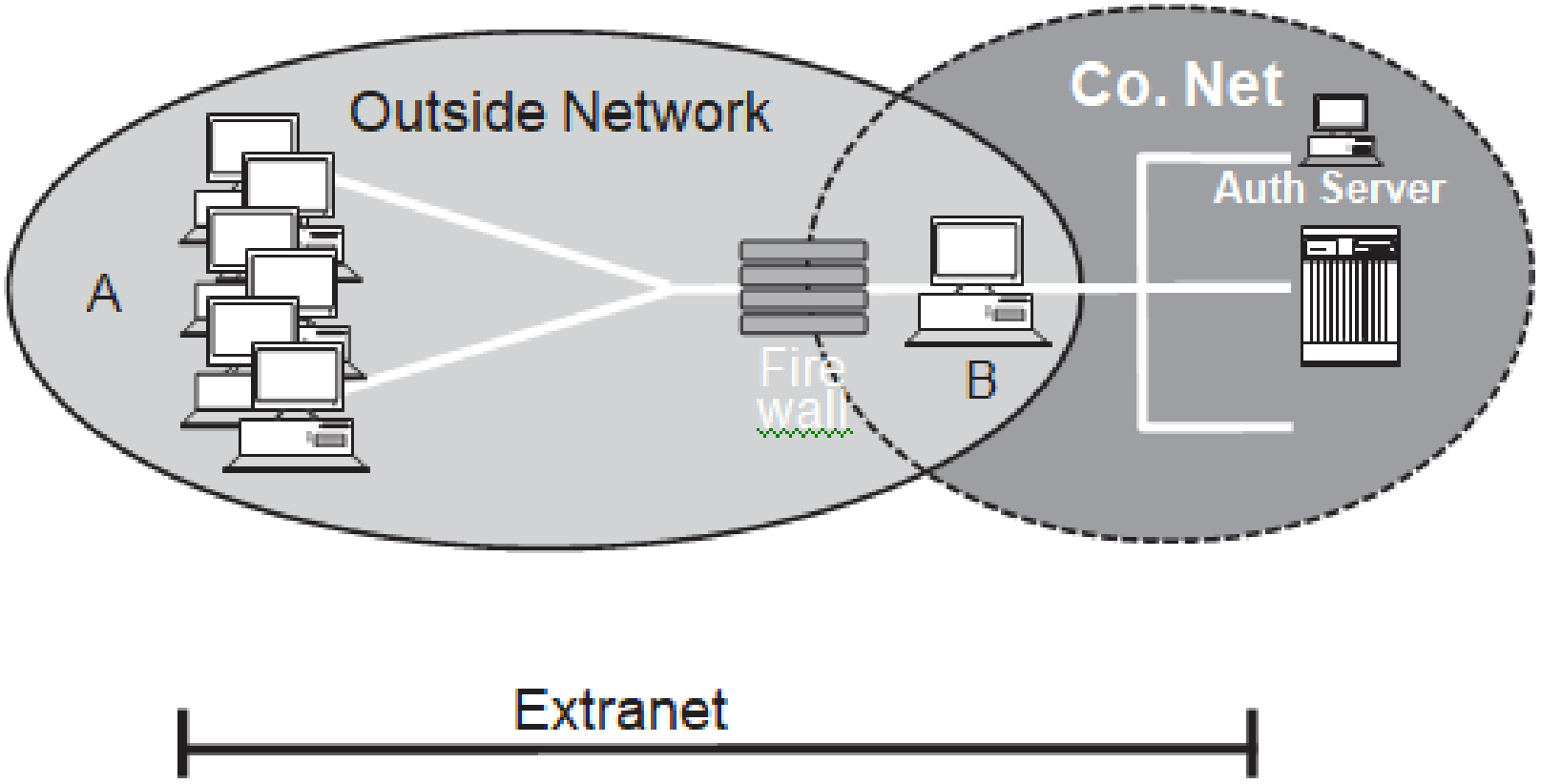


Basic extranet with router

More realistic extranet



Extranet using an application layer gateway firewall



Extranet using an application layer gateway firewall

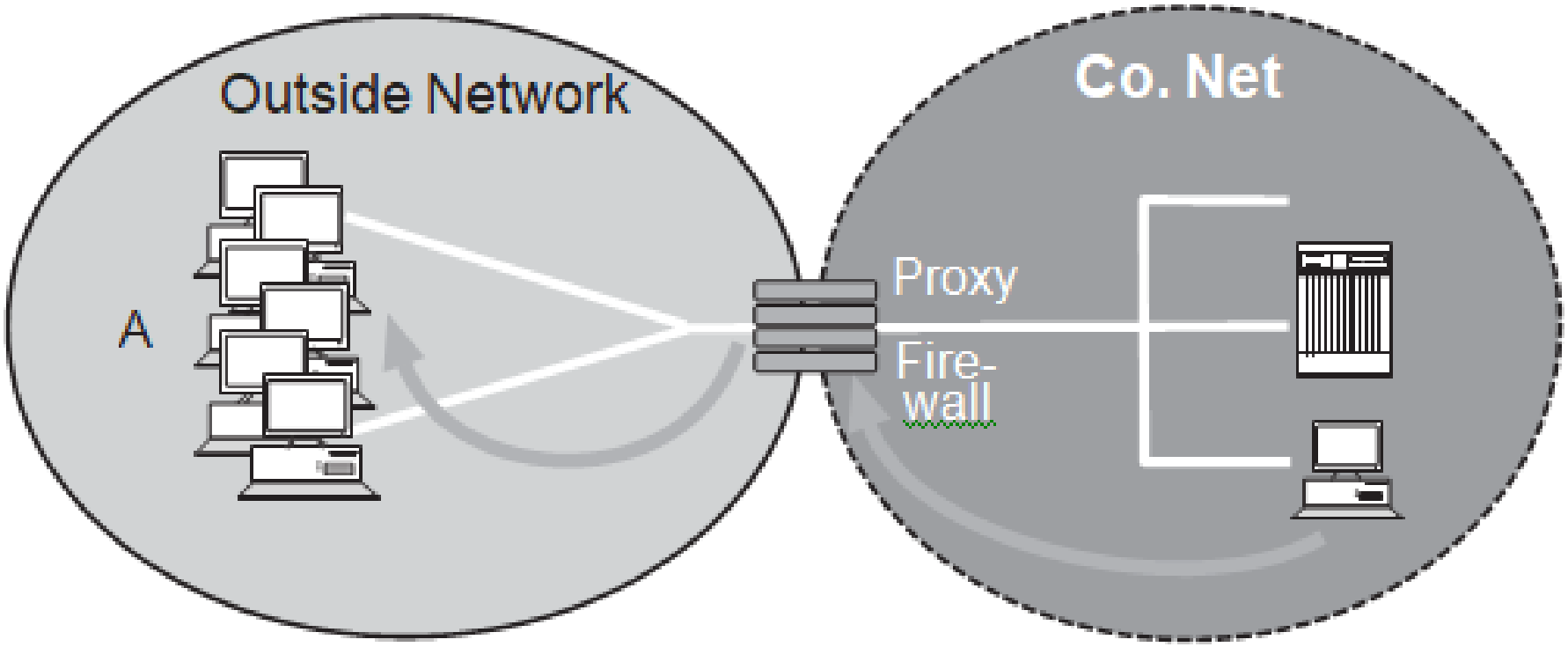
- These software tools have the ability to not only perform router type functions with access control rules, but also provide user authentication services on a per user basis

- In addition to supporting access control by IP address and user, some gateways have the further capability to restrict access by specific TCP/IP service port, such as Port 80, HTTP, so the extranet users can only access the internal resource on the specific application port and not expose the internal machine to any greater vulnerability than necessary.

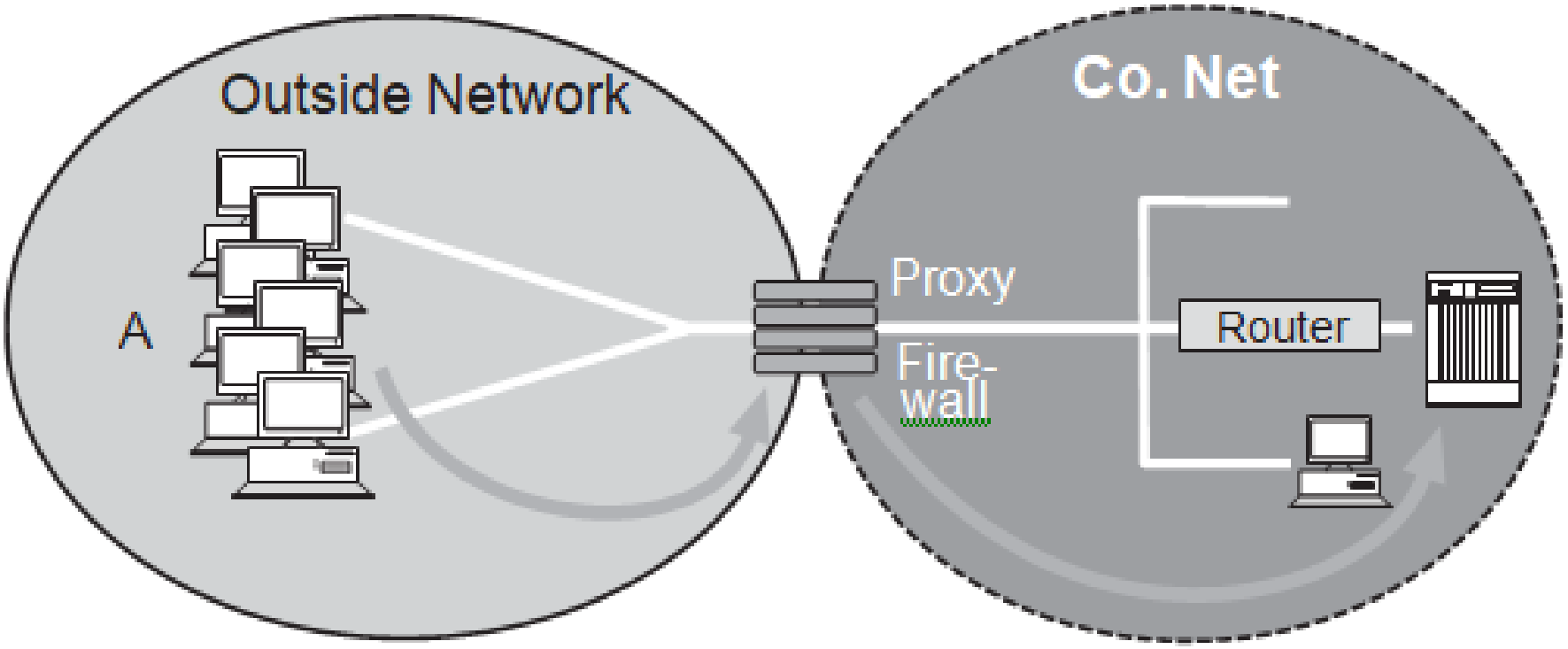
Proxy mechanism

- from an outside network to a portion of an internal company network.
- Normally, a proxy performs control and address translation for access from an intranet to the external Internet.
- These types of proxies normally reside on the firewall, and all user access to the Internet is directed through the proxy.
- The proxy has the ability to exert access control over who in the intranet is allowed external access, as well as where they can go on the Internet.
- The proxy also provides address translation such that the access packet going

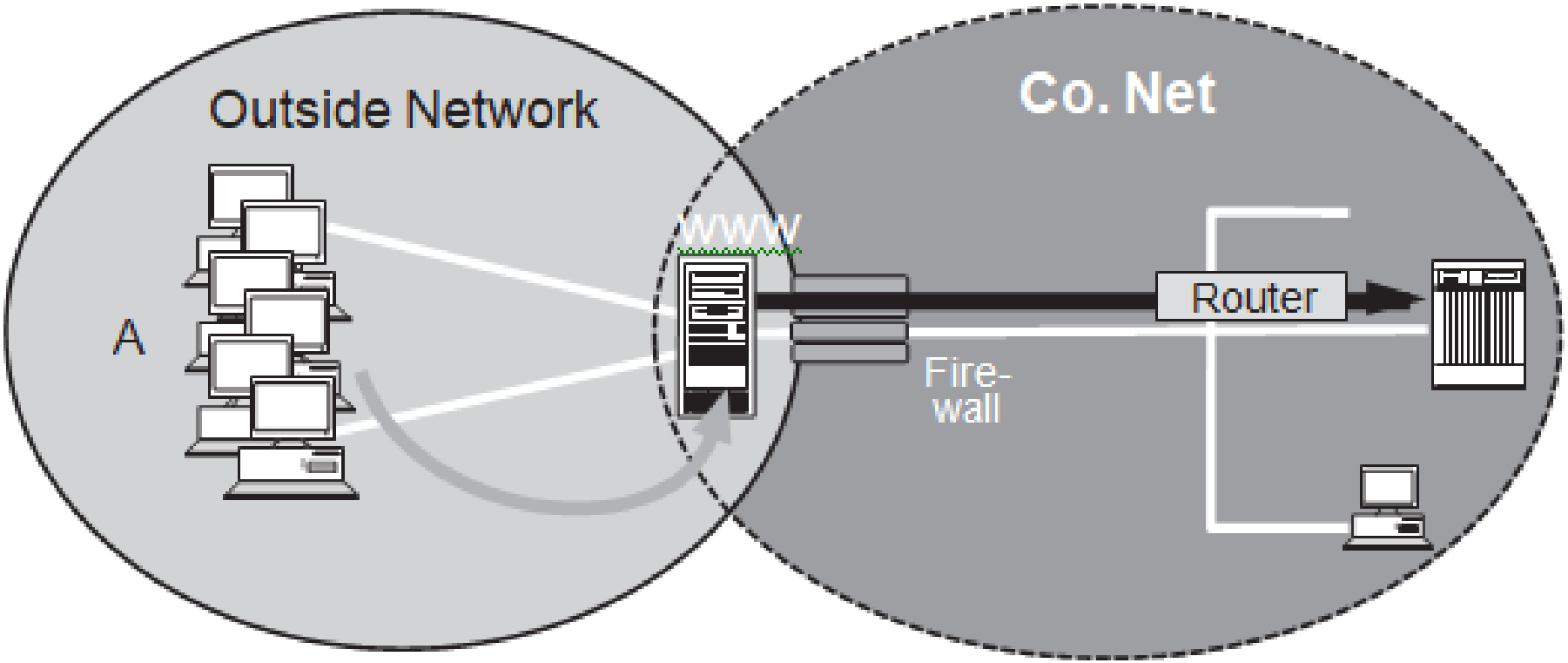
Outbound proxy architecture



Reverse proxy extranet architecture



Extranet with authenticating Web server



External Users Access Path

External Server Access Path

- **Is a VPN illegal?**

If you do something illegal through a virtual private network (VPN) connection, your local country's laws still apply. However, simply having and using a VPN is completely legal.

- **Why would someone need to use a VPN?**
- **A VPN allows you to use the Internet from a country that has more progressive digital policies. This way, you can visit websites that are blocked in your own country. Since they encrypt website traffic, your identity remains protected.**

VPN FAQ

What is private Internet?

When you work with a VPN service, all of your internet traffic is routed and encrypted via an intermediary server. As a result, the internet connection is more secure, anonymous and private. Other advantages include watching geo-blocked content from streaming sites like Netflix.

VPN FAQ

- **Is a VPN good or bad?**

  A VPN has many benefits including accessing geoblocked websites, getting better prices during online shopping and protecting your privacy and important data. However, a VPN can also slow your connection, have a monthly fee and there's an increase in anti-VPN software. Really, if you'll use a VPN, it's a great thing.

VPN FAQ

Can you be tracked if you use a VPN?

No, a VPN ensures that no one can track your IP address and website traffic and conceals your data via encryption.

Intranet, Extranet & Internet – Continued.,

- VPNs can be divided into three main categories – **remote access, intranet-based site-to-site, and extranet-based site-to-site**.

- Individual users are most likely to encounter remote access VPNs, whereas big businesses often implement site-to-site VPNs for corporate purposes.

Intranet, Extranet & Internet
VPN – Continued.,

- A VPN connection **establishes a secure connection between you and the internet**.
- Via the VPN, all your data traffic is routed through an encrypted virtual tunnel.
- This disguises your IP address when you use the internet, making its location invisible to everyone.
- A VPN connection is also secure against external attacks.

VPN – Security

- A **VPN can help secure that critical connection**.
- VPNs are good for when you're out and about, using Wi-Fi networks that aren't your own.
- A VPN can also help protect your privacy at home, and it may also let you access streaming content that would be otherwise unavailable.
- **VPNs can be hacked**, but it's hard to do so.

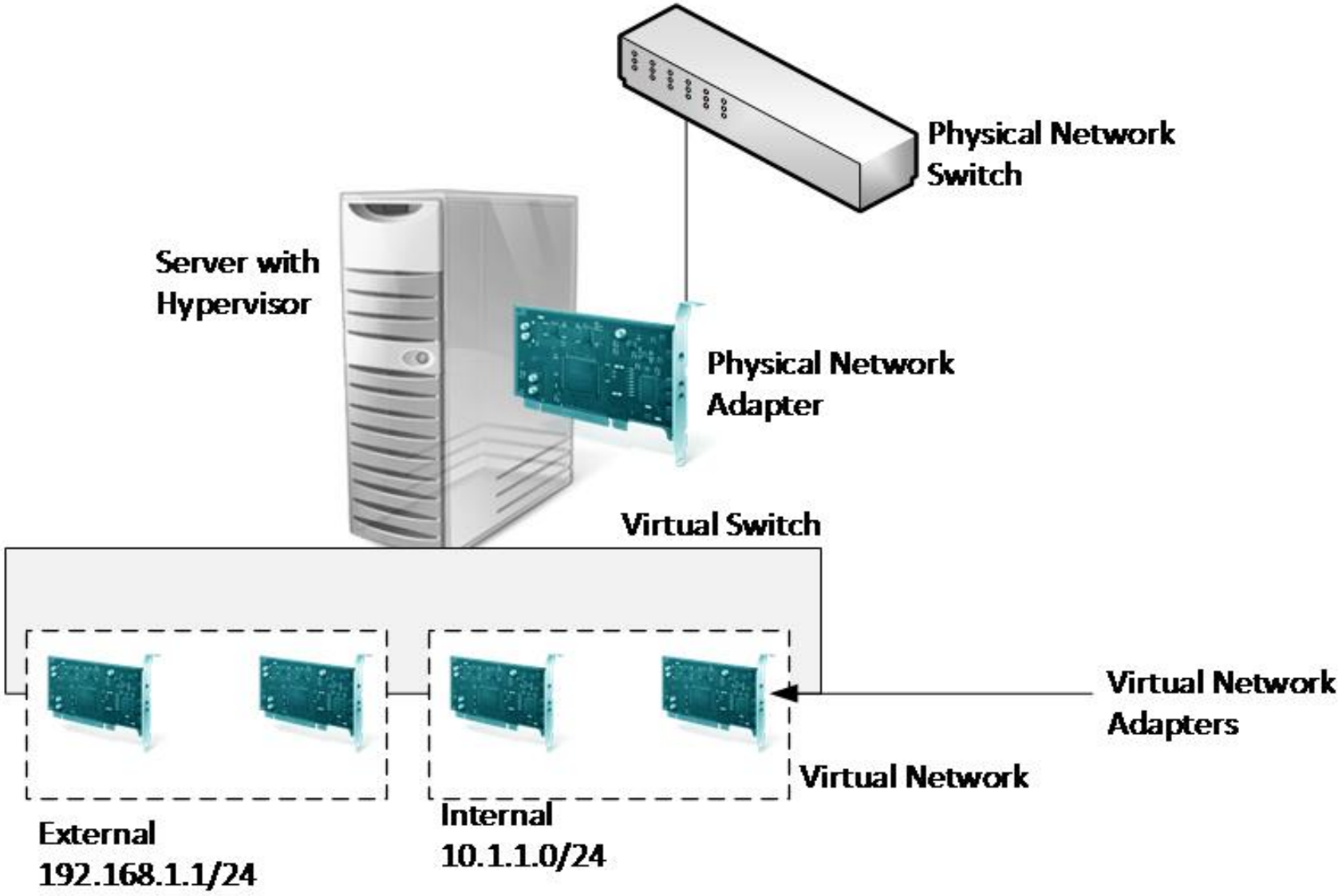
The chances of being hacked without a VPN are significantly greater than being hacked with VPN

VPN services

The best free VPN services you can download today:

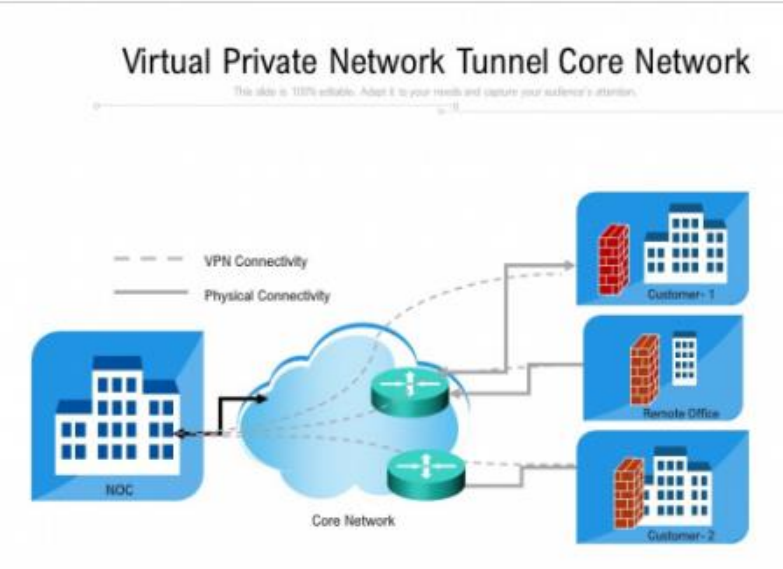
- **ProtonVPN (Free):** Truly secure with unlimited data – the best free VPN. ...
- **Windscribe:** Generous on data, and has good security.
- **Hotspot Shield Free VPN:** Decent free VPN with generous data allowances.
- **TunnelBear Free VPN:** Great identity protection for free.
- **Speedify:** Super secure speed

VPN – Structure



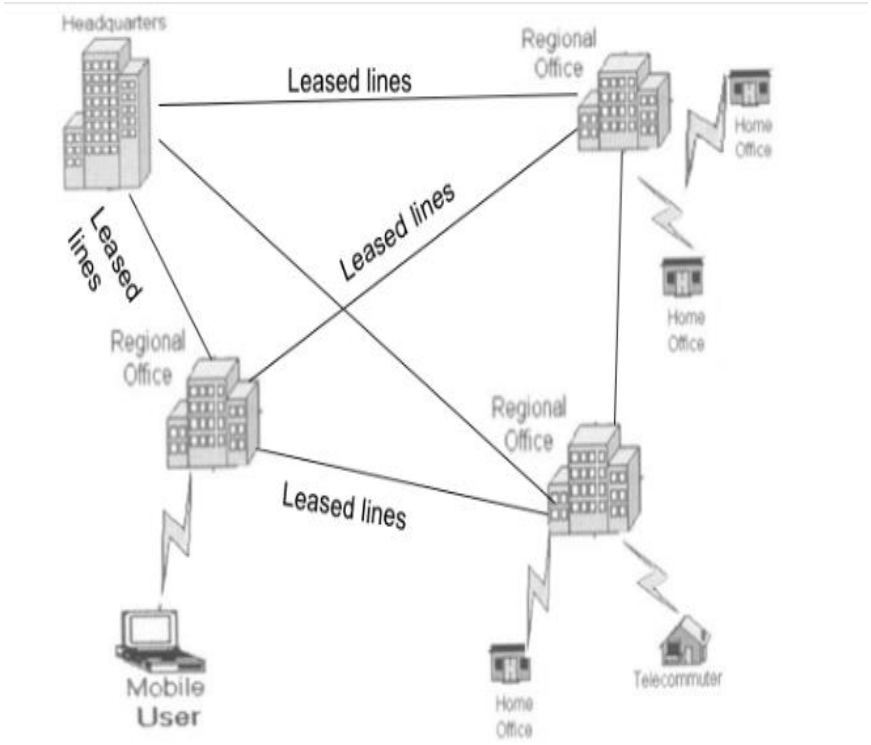
Virtual Network Management

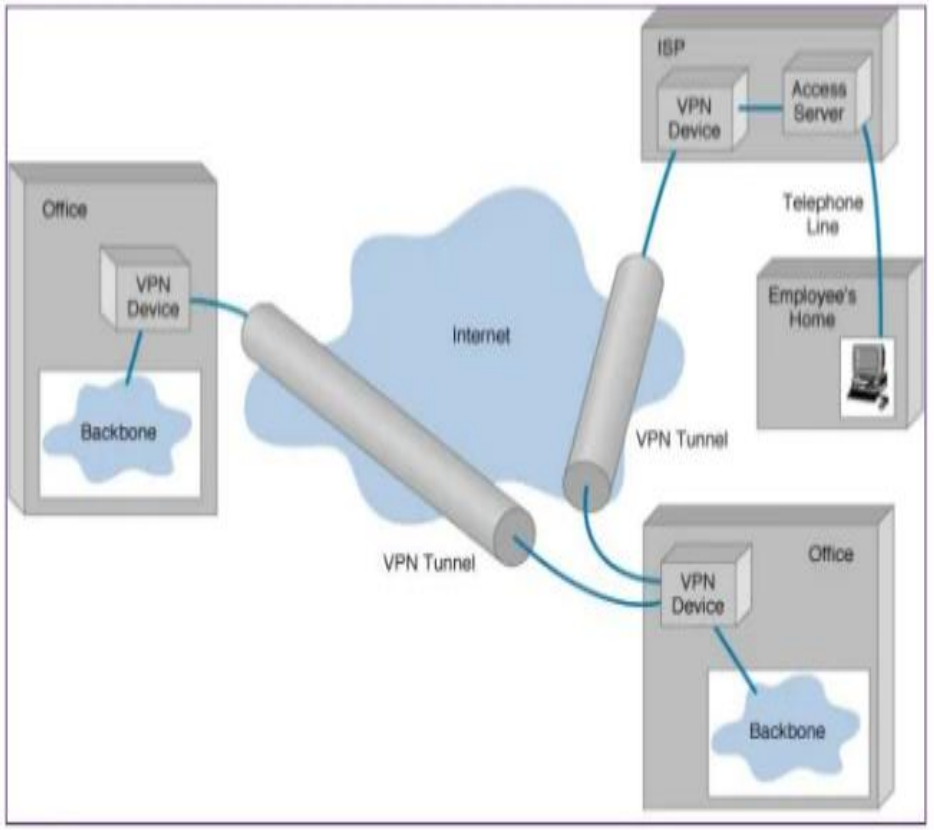
- Virtual Network is a managed system level object representing the Virtual LAN connectivity across the logical partitions



VPNs for small businesses

Conventional Systems Vs VPNs

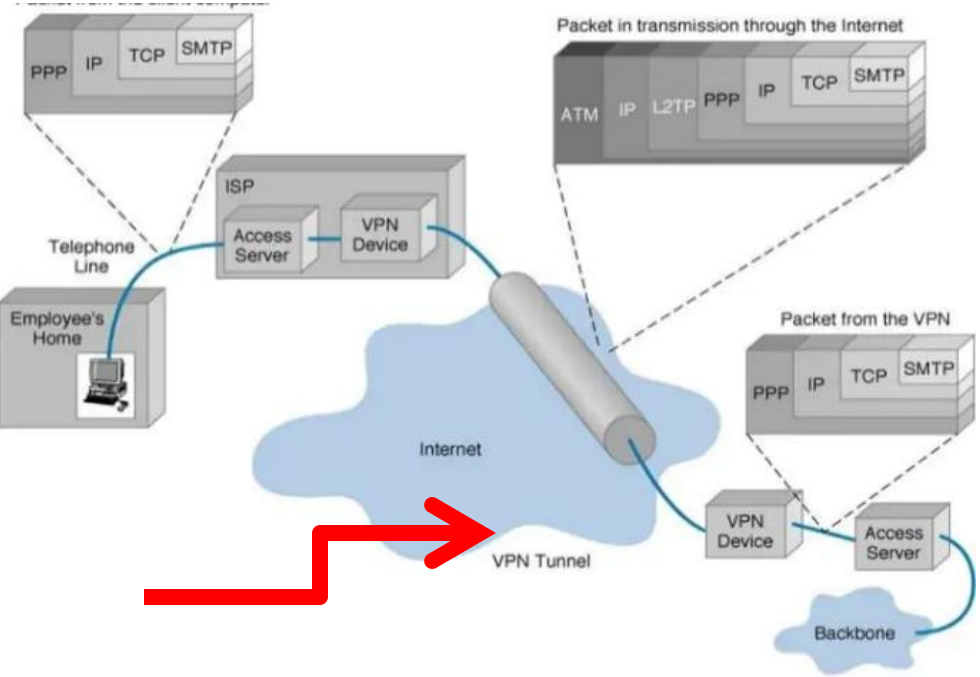




Requirements of VPN

- **TUNNELING.**
- **ENCRYPTION.**
- **ENCAPSULATION.**
- **AUTHENTICATION.**
- **FIREWALL.**

- Virtual private network technology is based on the idea of tunneling.
- VPN tunneling involves establishing and maintaining a logical network connection .
- Tunneling is the process of placing an entire packet within another packet before it's transported over the Internet.
- That outer packet protects the contents from public view and ensures that the packet moves within a virtual tunnel.



Types of Tunneling

1. **Voluntary.**
2. **compulsory.**

Voluntary - Compulsory

- In voluntary tunneling, the VPN client manages connection setup.
- The client first makes a connection to the carrier network provider (an ISP in the case of Internet VPNs).
- Then, the VPN client application creates the tunnel to a VPN server over this live connection.

- 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 set up in just one step compared to the two-step procedure

- Compulsory tunneling hides the details of VPN server connectivity from the VPN clients and effectively transfers management control over the tunnels from clients to the ISP.
- In return, service providers must take on the additional burden of installing and maintaining FEP devices.

Continued.,

- Point-to-Point Tunneling Protocol (PPTP)
- Layer Two Tunneling Protocol (L2TP)
- Internet Protocol Security (IPsec)

- It's the most widely supported VPN method among Windows users and it was created by Microsoft in association with other technology companies.
- compared to other methods, PPTP is faster and it is also available for Linux and Mac users. .
- Voluntary tunneling method.

IPsec is actually a collection of multiple related protocols.

It can be used as a complete VPN protocol solution or simply as the encryption scheme within L2TP or PPTP.

IPsec exists at the network layer (Layer Three of the OSI model.

L2TP (**L**ayer **2** **T**unneling **P**rotocol) it's another tunneling protocol that supports VPNs.

The difference between PPTP and L2TP is that the second one provides not only d*ata confidentiality but also data integrity*.

L2TP was developed by Microsoft and Cisco as a combination between PPTP and L2F(Layer 2 Forwarding).

Continued.,

What is Encryption?

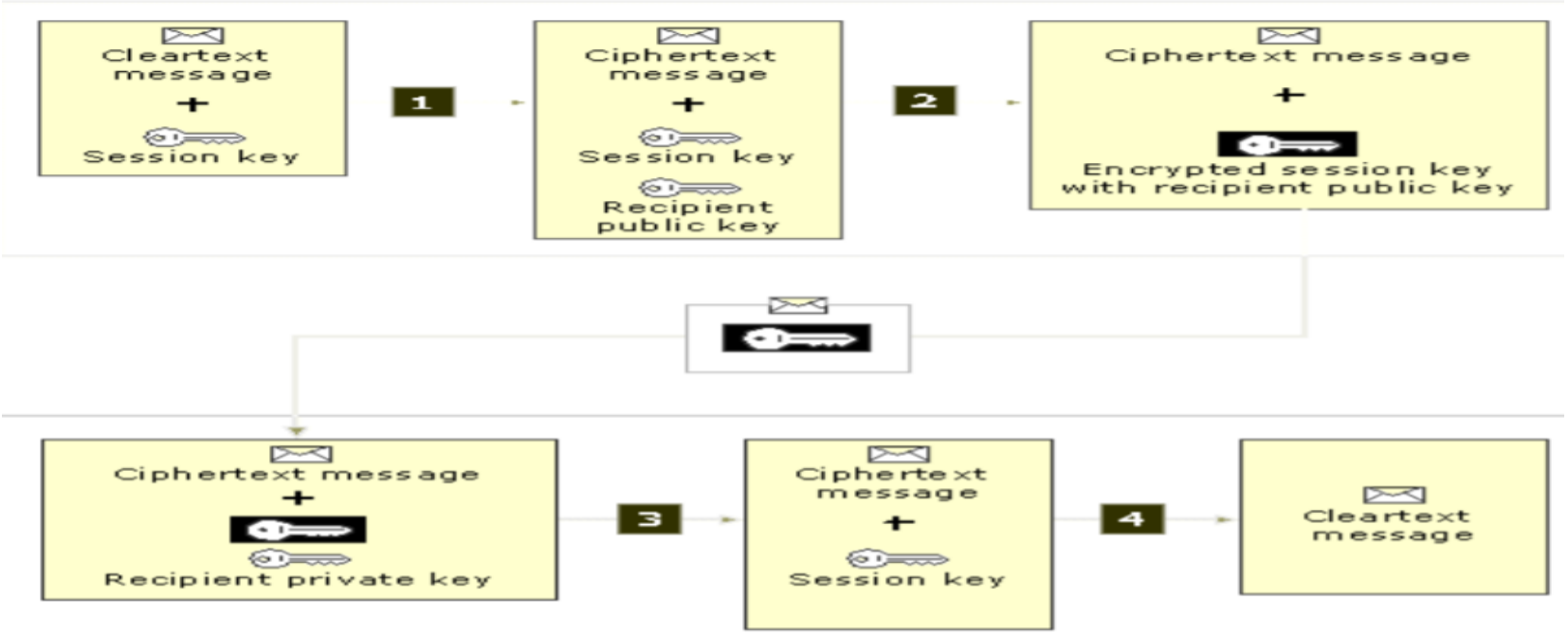
- Encryption is the process of encoding data so that only a computer with the right decoder will be able to read and use it.
- The VPN client at each end of the tunnel encrypt the data entering the tunnel and decrypt it at the other end .

Types of Encryption

There are most two common forms of encryption

- 1 . symmetric-key encryption
- 2 . public-key Encryption

Process of Encryption



Authentication

- Authentication process determine if the sender is the authorized person and if the data has been redirect or corrupted .

- There are 2 levels of Authentication.

  - Computer-Level Authentication
  - User-level Authentication

Firewall provides network security and business continuity .

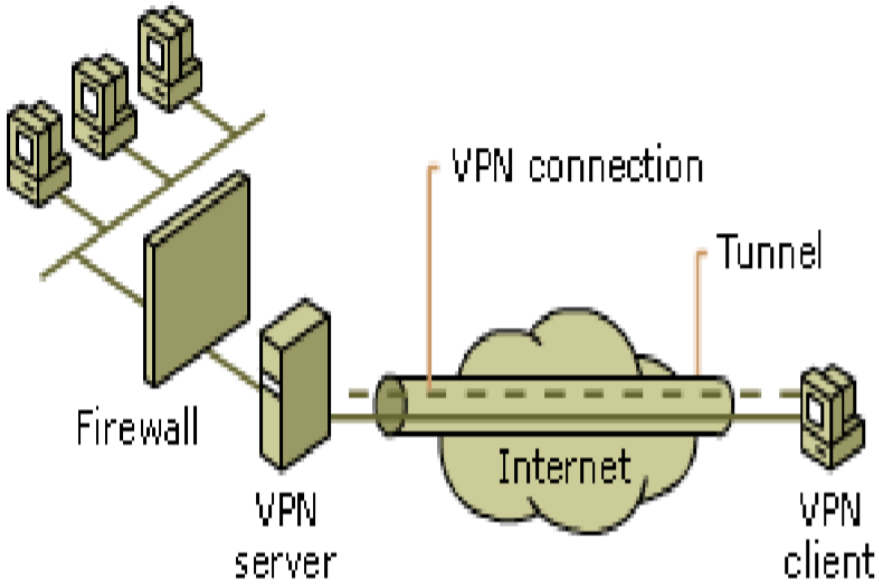
It prevents attacks, and secures your data communications with multiple parallel Virtual Private Network (VPN) connections.

There are two approaches to using a firewall with a VPN server:

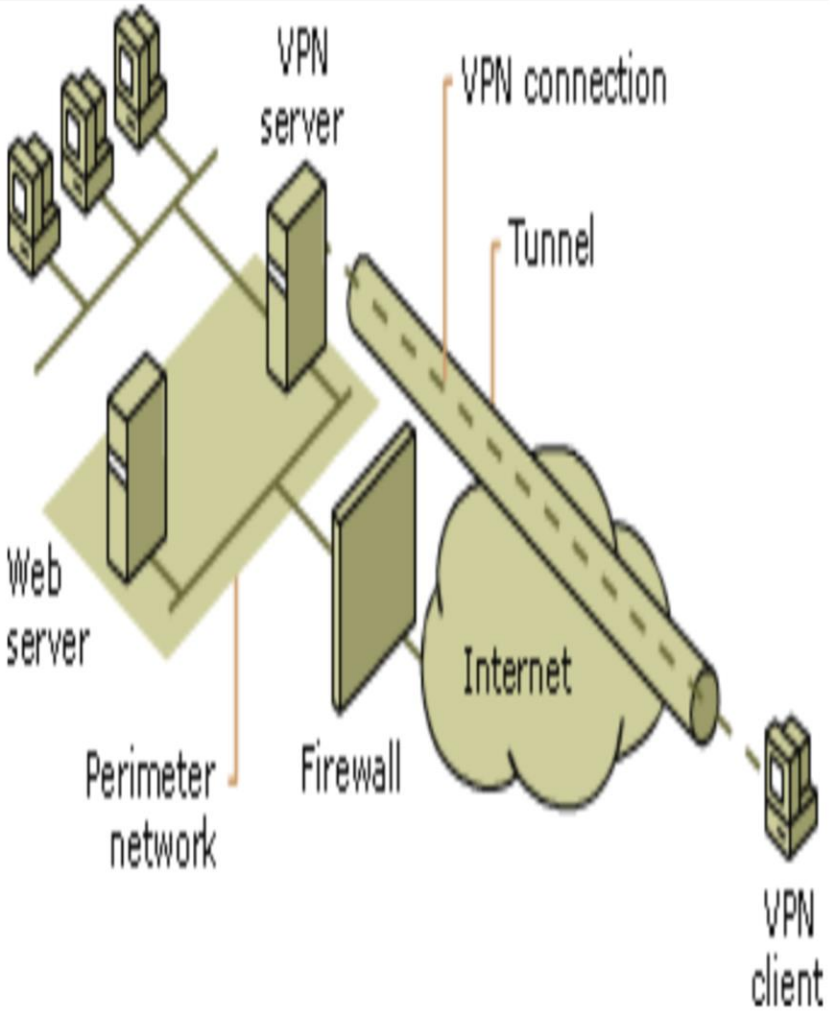
VPN server in front of the firewall..

VPN server behind the firewall..

VPN server in front of the firewall.



VPN server behind the firewall

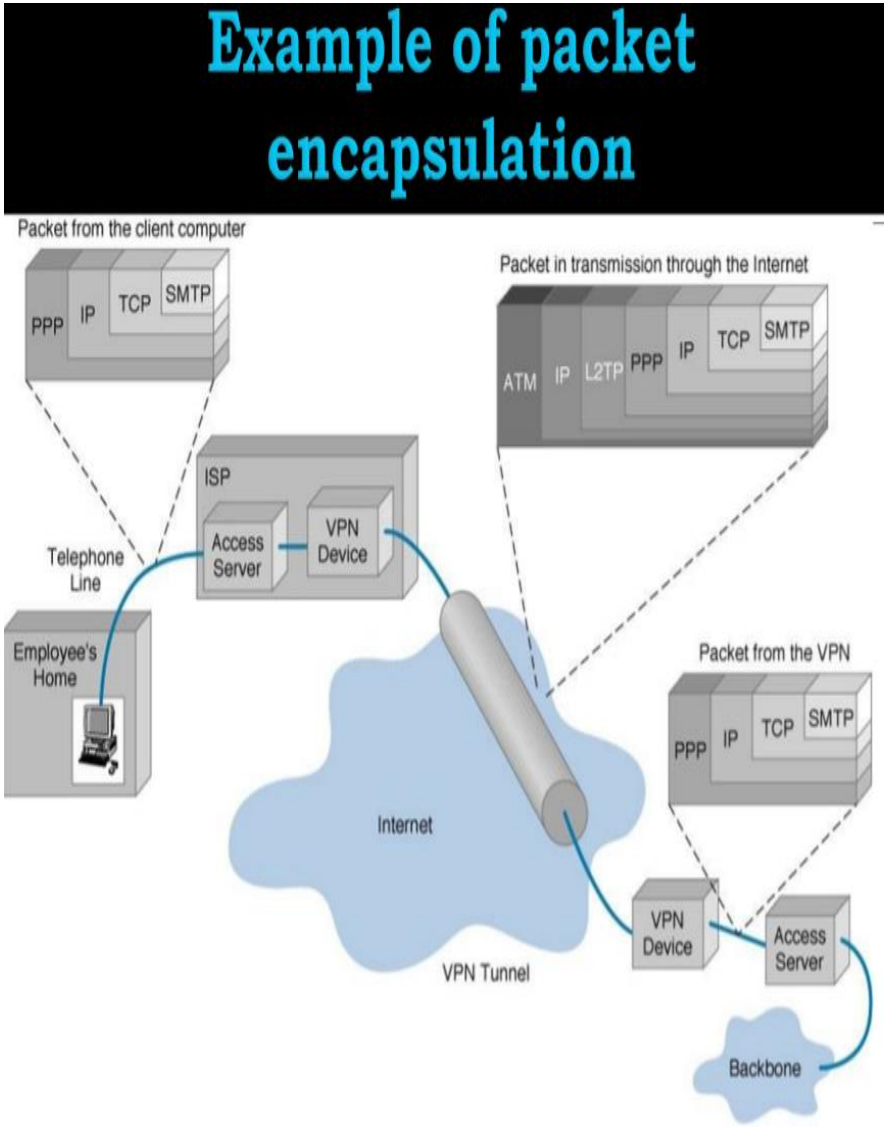


Encapsulation of Data

- For data encapsulation, VPN relies on either of the following technologies like GRE , IPSec, L2F,PPTP and L2TP .
- In which IPsec and PPTP are more popular.

Types of VPN

- Remote access VPN
- Intranet VPN
- Extranet VPN

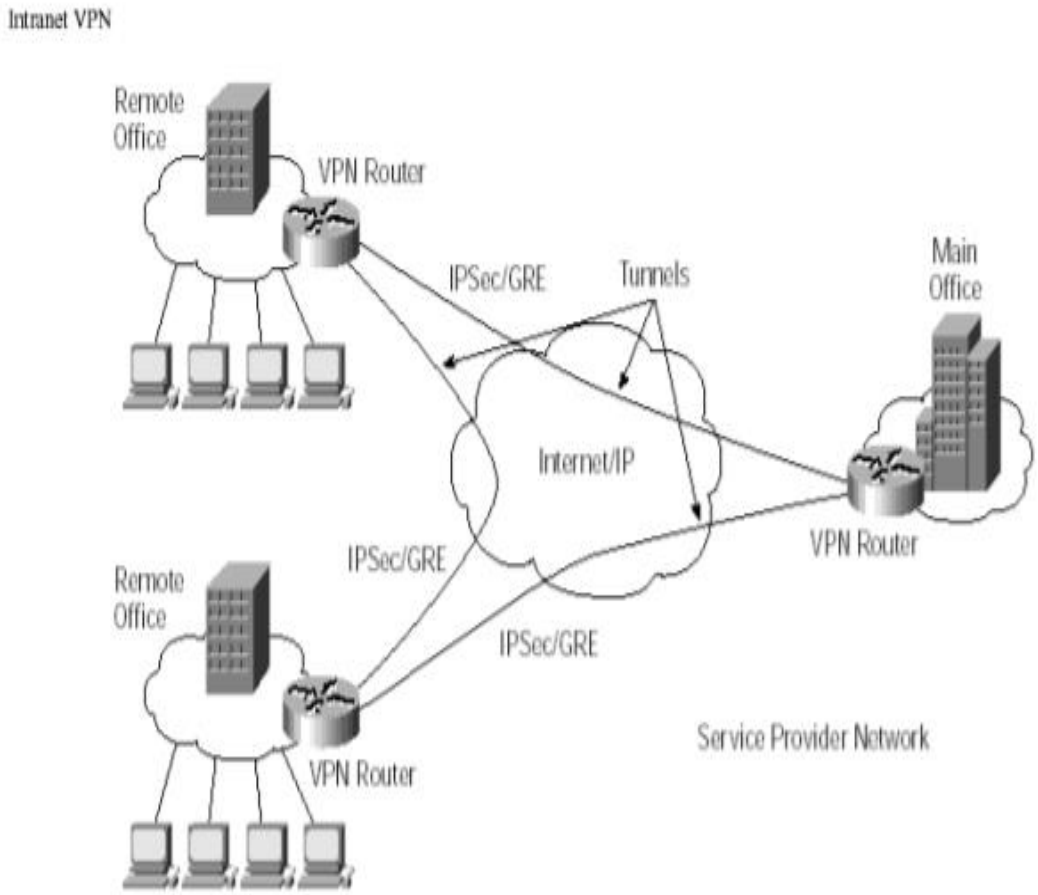


Intranet VPN

Intranet VPNs link corporate headquarters, remote offices, and branch offices over a shared infrastructure using dedicated connections.

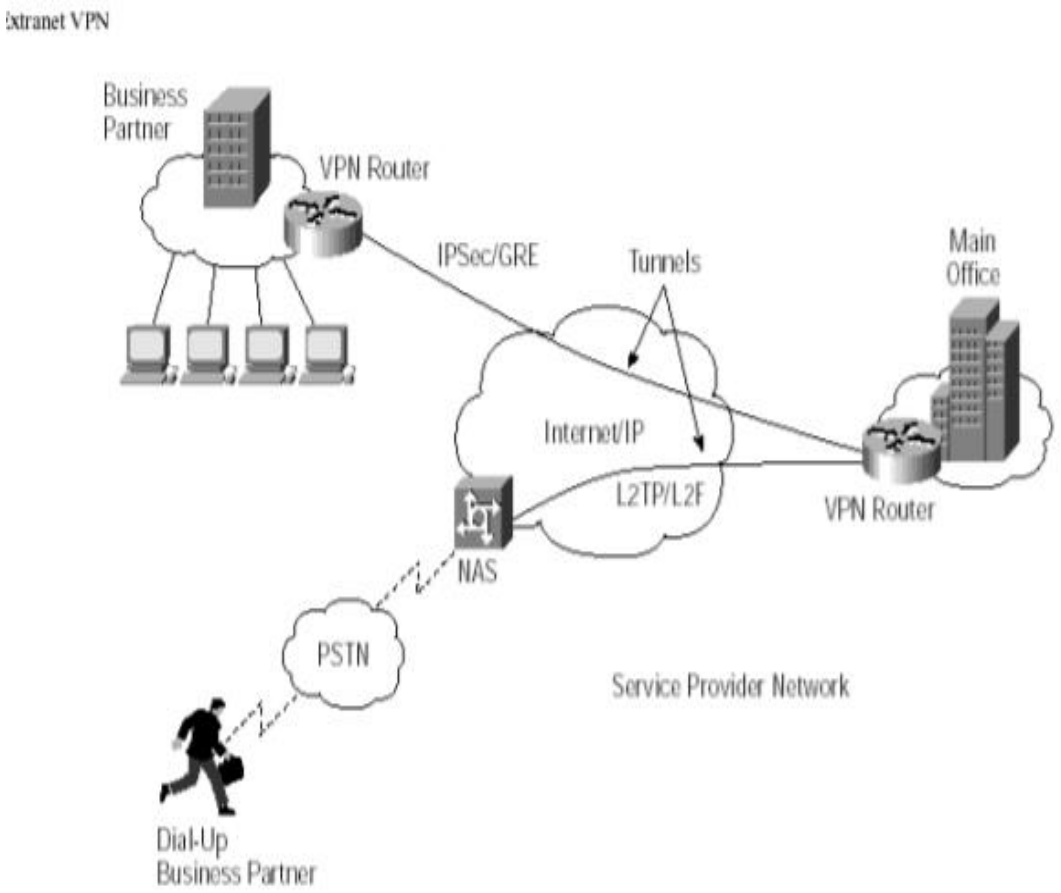
The benefits of an intranet VPN are as follows:

- Reduces WAN bandwidth costs
- Connect new sites easily



Extranet VPN

Extranet VPNs link customers, suppliers, partners, or communities of interest to a corporate intranet over a shared infrastructure using dedicated connections. In this example, the VPN is often an alternative to fax, snail mail, or EDI. The extranet VPN facilitates e-commerce.




SIST
JUSTICE PEACE REVOLUTION
SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY
DEEMED UNIVERSITY

Thank you