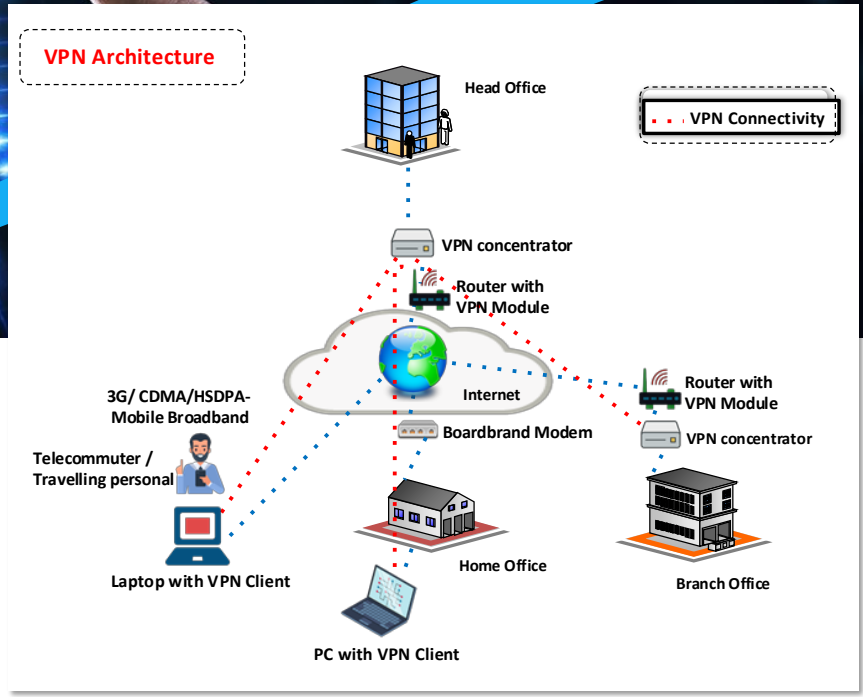
Module Flow

1. Understand Different Types of Network Segmentation
2. Understand Different Types of Firewalls and their Role
3. Understand Different Types of IDS/IPS and their Role
4. Understand Different Types of Honeypots
5. Understand Different Types of Proxy Servers and their Benefits
6. **Discuss Fundamentals of VPN and its importance in Network Security**
7. Discuss Security Incident and Event Management (SIEM)
8. Discuss User Behavior Analytics (UBA)
9. Understand Various Antivirus/Anti-malware Software

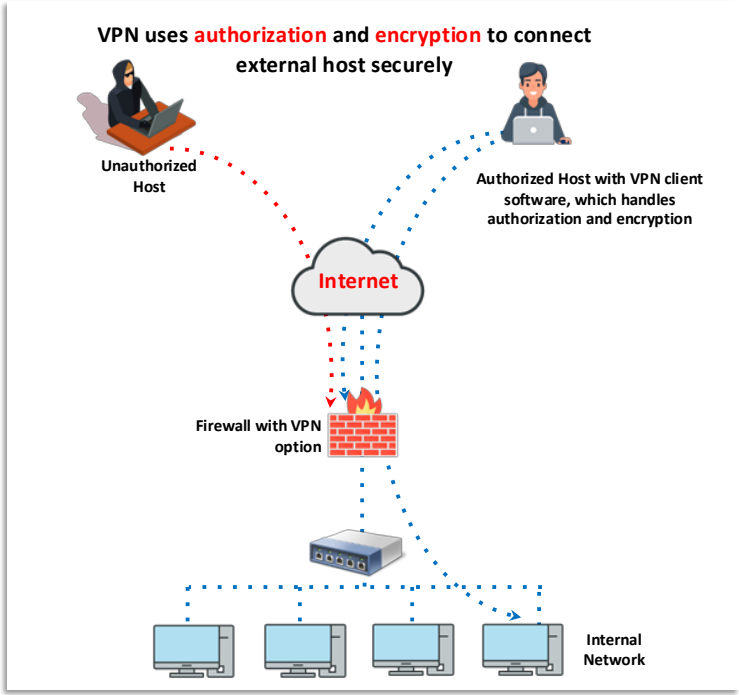
What is a VPN?

- VPNs are used to **securely communicate** with different computers over insecure channels
- A VPN use the Internet and ensures secure communication to distant offices or users within the **enterprise's network**



How VPN Works

- A client willing to connect to a company's network initially connects to the Internet
- Then, the client initiates a **VPN connection** with the company's server
- Before establishing a connection, end points must be **authenticated** through passwords, biometrics, personal data, or any combination of these
- Once the connection is established, the client can **securely access** the company's network



Why Establish VPN?

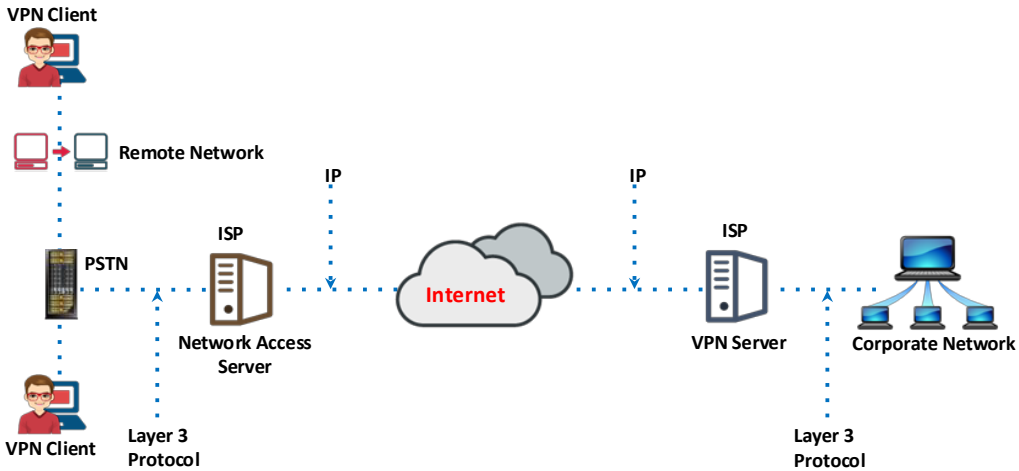
A well-designed VPN provides the following benefits:

- ✓ Extend **geographic connectivity**
- ✓ Reduce **operational costs** versus traditional WANs
- ✓ Reduce **transit times** and traveling costs for remote users
- ✓ Improve **productivity**
- ✓ Simplify **network topology**
- ✓ Provide **global networking** opportunities

VPN Components

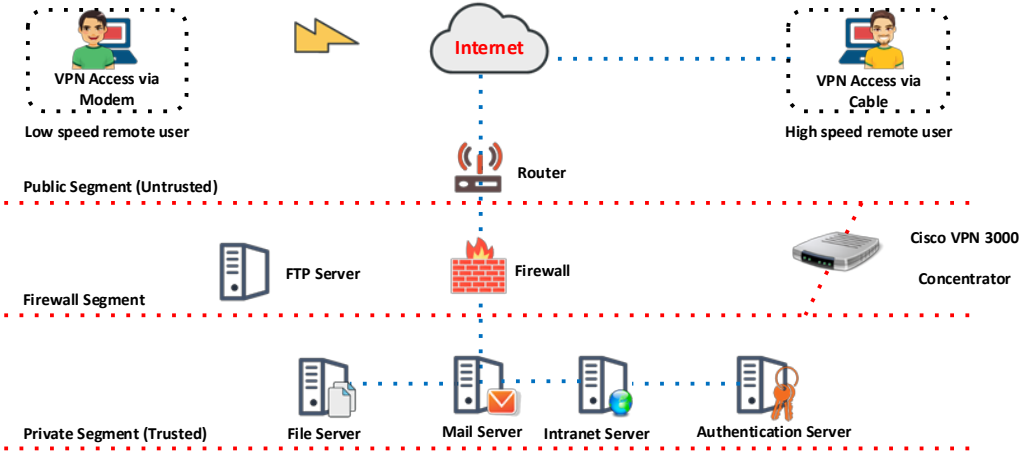
VPN Components

- ✓ VPN client
- ✓ Network access server (NAS)
- ✓ Tunnel Terminating Device (or VPN server)
- ✓ VPN protocol



VPN Concentrators

- A VPN Concentrator is a network device used to create **secure VPN connections**
- It acts as a VPN router which is generally used to create a remote access or **site-to-site** VPN
- It uses tunnelling protocols to **negotiate security** parameters, create and manage tunnels, encapsulate, transmit, or receive packets through the tunnel, and de-encapsulate them



Functions of a VPN Concentrator

- A VPN Concentrator functions as a **bi-directional** tunnel endpoint

The VPN Concentrator functions are:

01 Encrypts and decrypts data

02 Authenticates users

03 Manages data transfer across the tunnel

04 Negotiates tunnel parameters

05 Manages security keys

06 Establishes Tunnels

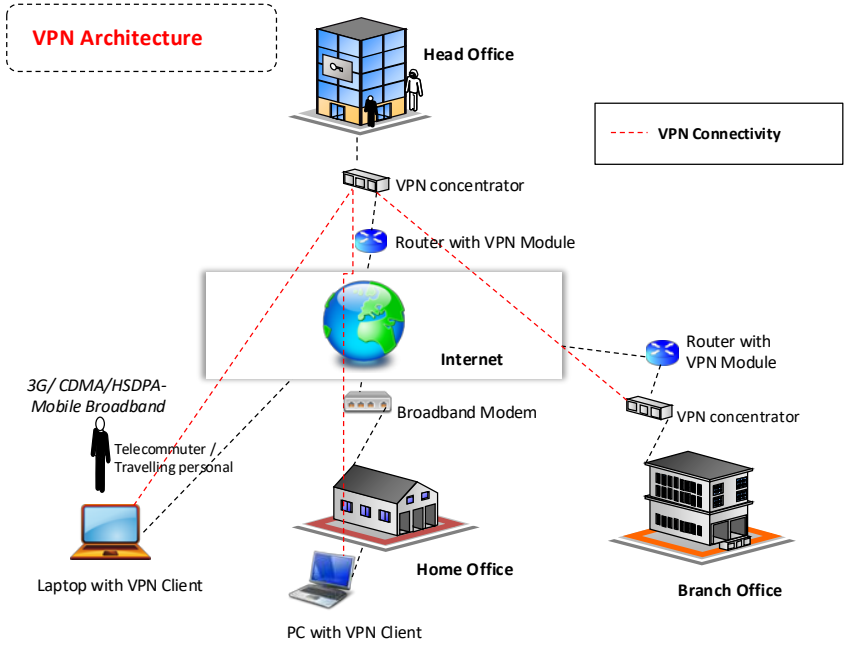
07 Assigns user addresses

08 Manages inbound and outbound data transfers as a tunnel endpoint or router

VPN Types and Categories

Client-to-Site (Remote-access) VPNs

- Remote-Access VPNs allow **individual hosts** or clients, such as telecommuters and mobile users to establish secure connections to a company's network over the Internet
- Each host contains VPN client software or uses a **web-based** client
- The VPN **encrypts** the data packets that are forwarded over the Internet to the VPN gateway at the edge of the target network, with the software installed on the client's machine
- A **VPN Gateway** receives the packets and then closes the connection to the VPN after transfer is complete

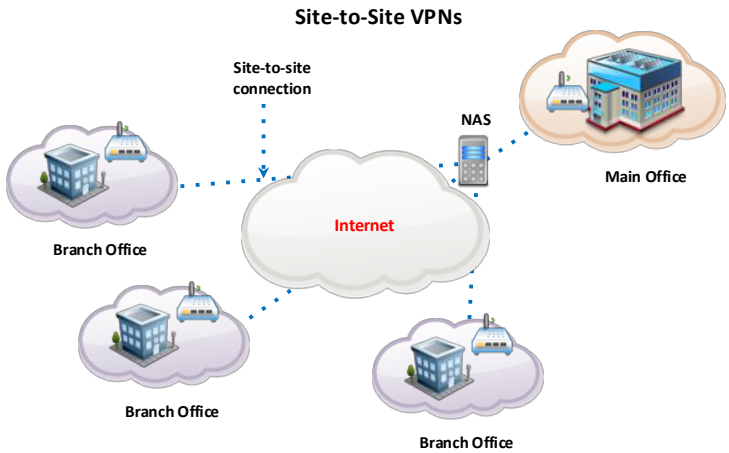


Site-to-Site VPNs

Site-to-site VPN is classified in two types:

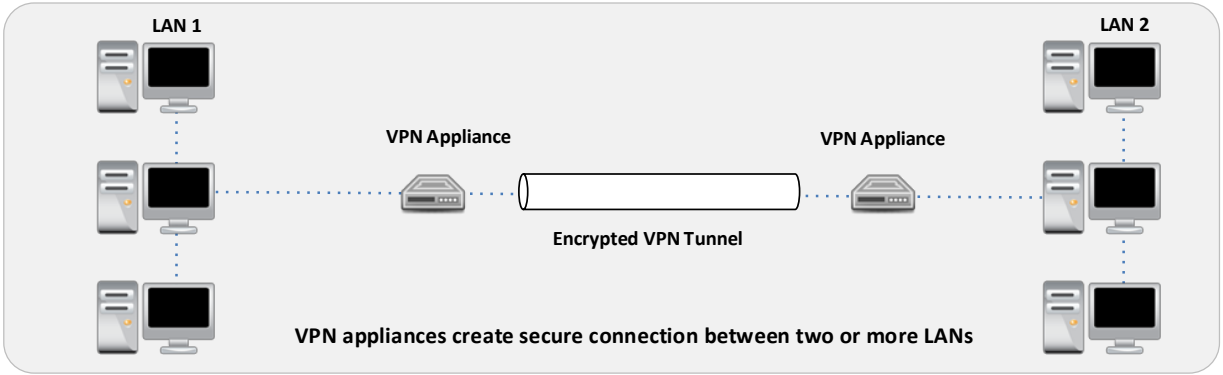
- **Intranet-based**: VPN connectivity is between sites of a **single organization**
- **Extranet-based**: VPN connectivity is between **different organizations** such as business partners, business, and its clients

- Site-to-site VPN extends the **company's network**, allows access of an organization's network resources from different locations
- It connects a **branch** or remote office network to the **company's headquarters** network
- Also known as **LAN-to-LAN** or L2L VPNs



Hardware VPNs

- A dedicated hardware VPN appliance is used to connect **routers** and **gateways** to ensure communication over an insecure channel
- It is designed to serve as a VPN endpoint and can connect to multiple LANs



Hardware VPN Products

Manufacturer	Product Name	Web Site
Cisco Systems	VPN 3000 series concentrators, VPN 3002 Hardware Clients, 7600 series routers, and Web VPN Services Module	*https://www.cisco.com*
SonicWALL	SonicWALL PRO 5060,4060,3060,2040,1260	*https://www.sonicwall.com*
Juniper Networks	NetScreen 5000, 500,200, and ISG series	*https://www.juniper.net*
WatchGuard	WatchGuard Firebox X series	*https://www.watchguard.com*

Software VPNs

- VPN software is **installed** and **configured** on routers, servers and firewalls or as a gateway that functions as a VPN

Advantages

- **No extra devices** need to be installed
- It is an **easy and low-cost way** to deploy a VPN and does not change the target network

Disadvantages

- **Extra processing** burden to devices on which it is installed
- It is **less secure** and prone to attacks

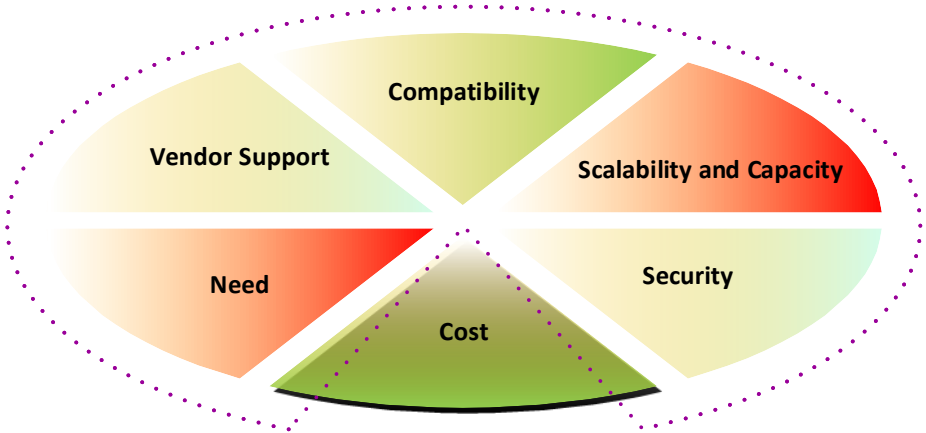
Software VPN Products

Manufacturer	Product Name	Web Site
CheckPoint	VPN-1 VSX,VPN-1 Pro, VPN-1 Edge, Firewall-1	*https://www.checkpoint.com*
NETGEAR	ProSafe VPN	*https://www.netgear.com*
Cisco Systems	Cisco AnyConnect Secure Mobility Client	*https://www.cisco.com*

Selecting an Appropriate VPN

- Choose the **best possible VPN solution** for your enterprise

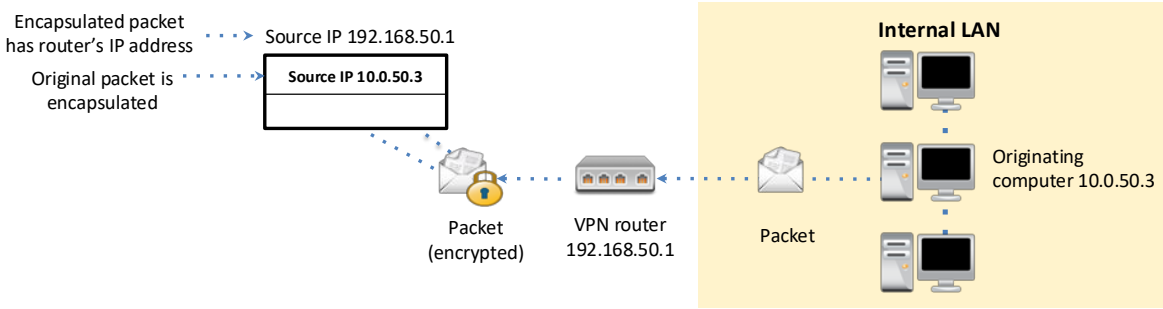
Choose the type of VPN solution based on



VPN Core Functionality: Encapsulation

- Packets over a VPN are **enclosed** within another packet (encapsulation) which has a different IP source and destination
- Concealing the source and destination of the packets protects the **integrity** of the data sent
- The most common VPN encapsulation protocols:
  - Point-to-Point Tunneling Protocol (PPTP)
  - Layer 2 Tunneling Protocol (L2TP)
  - Secure Shell (SSH)
  - Socket Secure (SOCKS)

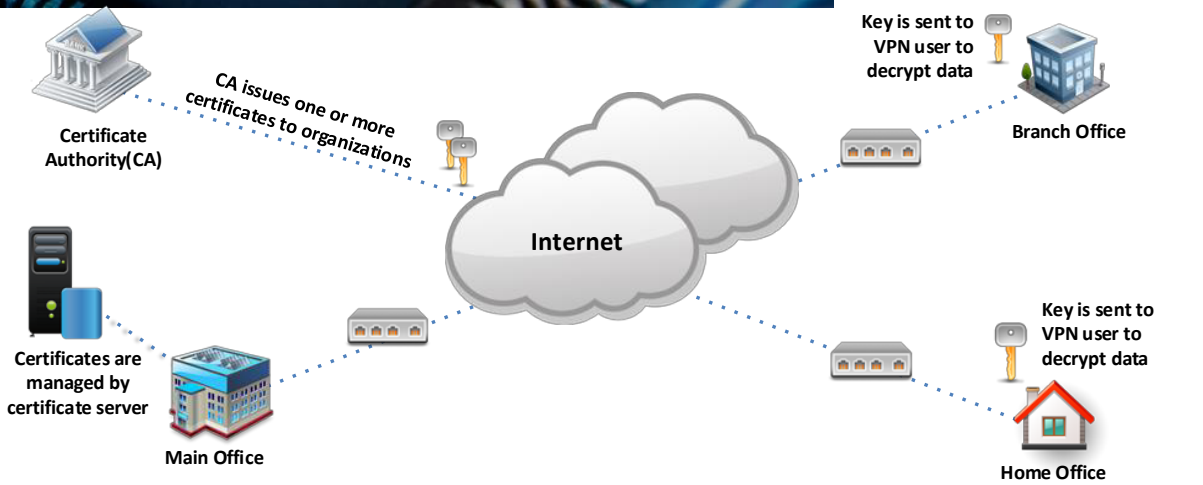
Encapsulating data to conceal source and destination information



VPN Core Functionality: Encryption

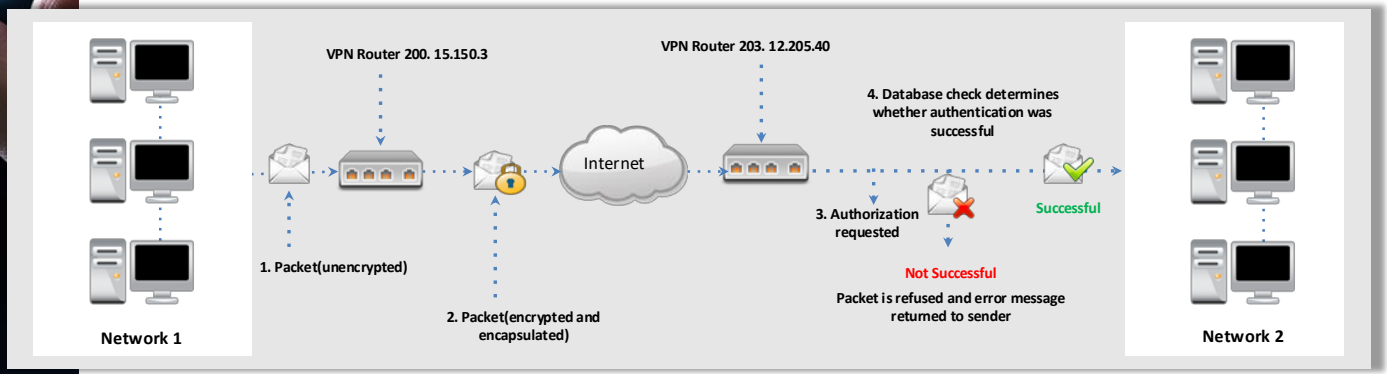
- Packets sent over a VPN are **encrypted** to maintain the confidentiality of the information
- Packets are read by decrypting with the **encryption key** from the sender

- **Common VPN Encryption Technologies**
  - Triple Data Encryption Standard (3DES)
  - Secure Sockets Layer (SSL)
  - Open VPN



VPN Core Functionality: Authentication

- Users are **authenticated** to access the VPN and its resources
- It uses **digital certificates** to authenticate users
- Common user authentication techniques for a VPN
  - IPSec
  - MS-CHAP
  - Kerberos



VPN Technologies

01 Trusted VPNs

- Were used before the **Internet** became **universal**
- Companies leased circuits from a communications provider and used them the same way as **physical cables** in a private LAN
- Organization`s know and control the pathway for their transmission
- A customer trusted communication provider maintains the integrity and security but not the encryption, these are called Trusted VPNs
- Technologies such as **ATM** circuits, **frame-relay** circuits, Multiprotocol Label Switching (MPLS) are used to implement trusted VPNs

Secure VPNs 02

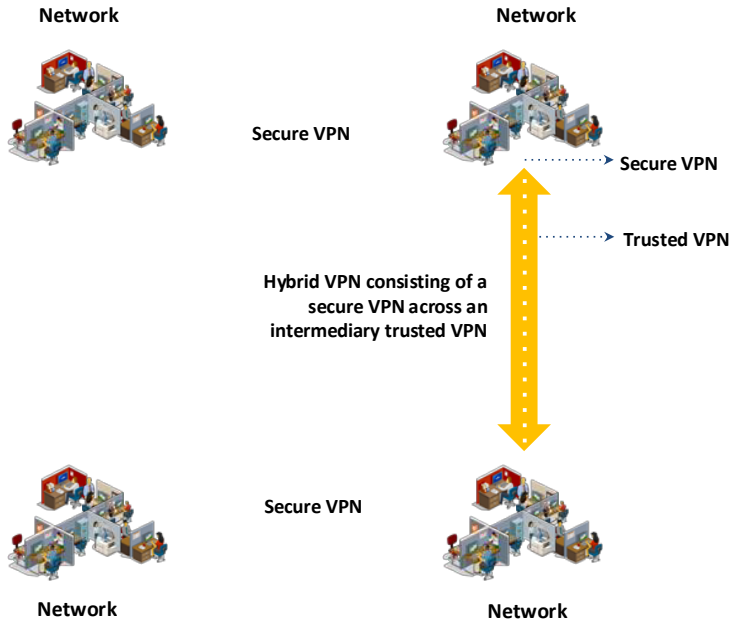
- Used when the **Internet** became a corporate **communications medium**
- Vendors created a protocol which encrypts the traffic at the originating computer and decrypts at the receiving computer
- The **encrypted** traffic acts as a tunnel between two networks, even if an attacker sees the traffic will not be able to read it
- Secure VPNs are networks constructed using encryption
- They protect the **confidentiality** and **integrity** of the data, but do not ensure the transmission path

VPN Technologies (Cont'd)

03

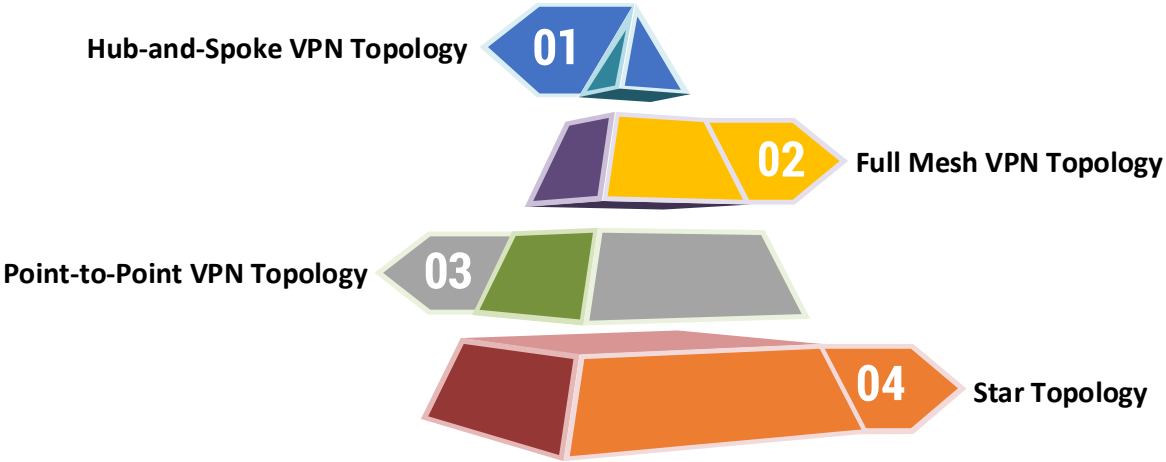
Hybrid VPNs

- A secure VPN is part of a trusted VPN, creating a hybrid VPN
- The secure part of a hybrid VPN is administered by the **customer** or the **provider**, who has provided the trusted part of the hybrid VPN



VPN Topologies

- A VPN topology specifies how the **peers** and **networks** within a VPN are connected
- Some VPN topologies include

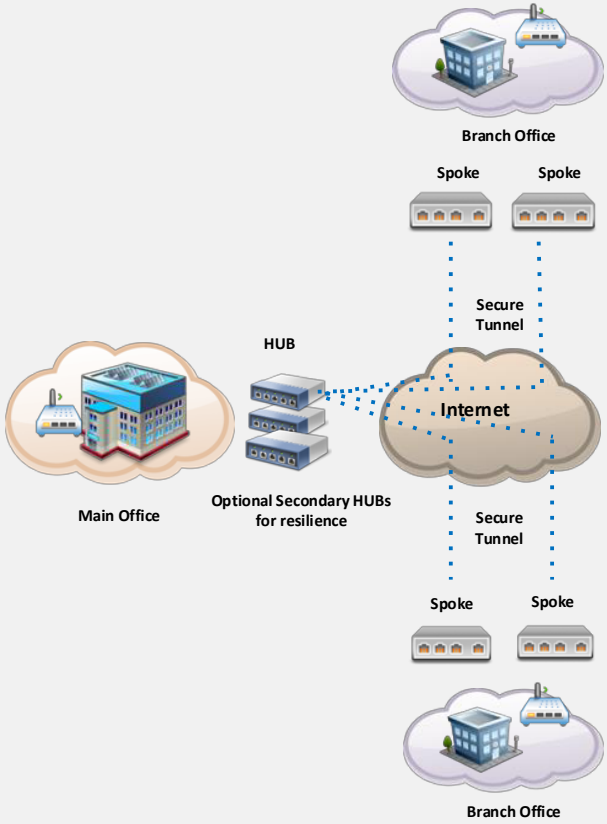


Hub-and-Spoke VPN Topology

Each individual spoke connected to the remote office is communicated securely with the **central device** (hub)

A separate and secure tunnel is **established** between the hub and each individual spoke

A **persistent connection** is established between an organization's main office and their branch offices using a third-party network or the Internet



Point-to-Point VPN Topology

1

Unlike the Hub-and-Spoke topology, offices at different locations can directly communicate with each other without any **IPsec failover**

2

This topology treats two end points as two **peer devices** participating in communication

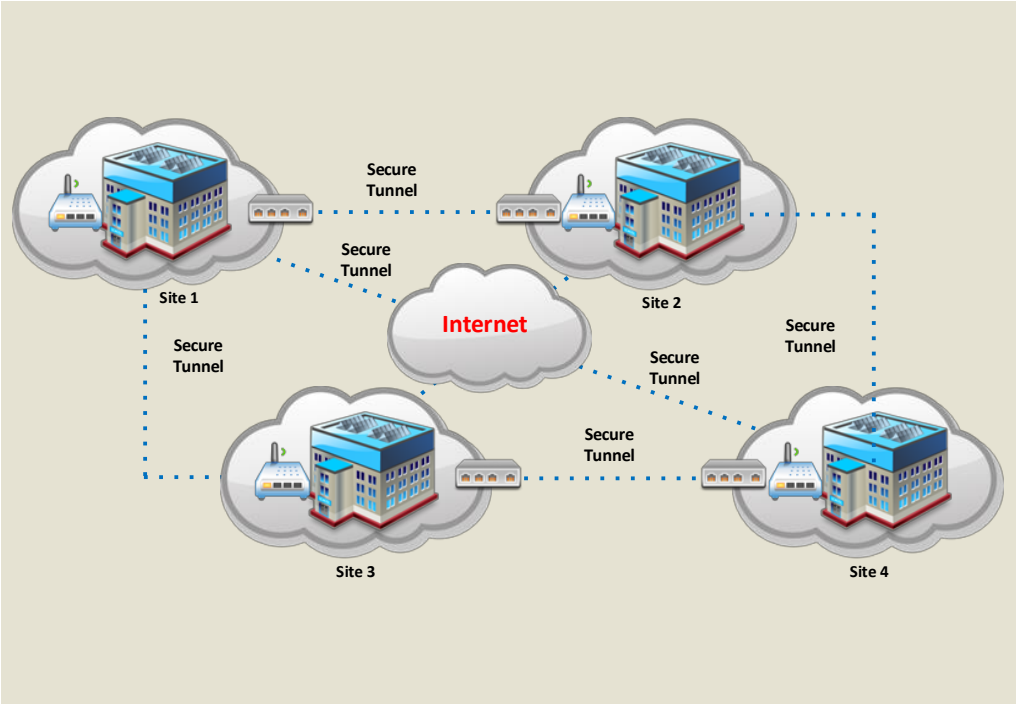
3

Only Regular IPsec or IPsec/GRE is assigned for the tunnel, as any of the **peer devices** can initiate the communication

Point-to-point VPN Topology

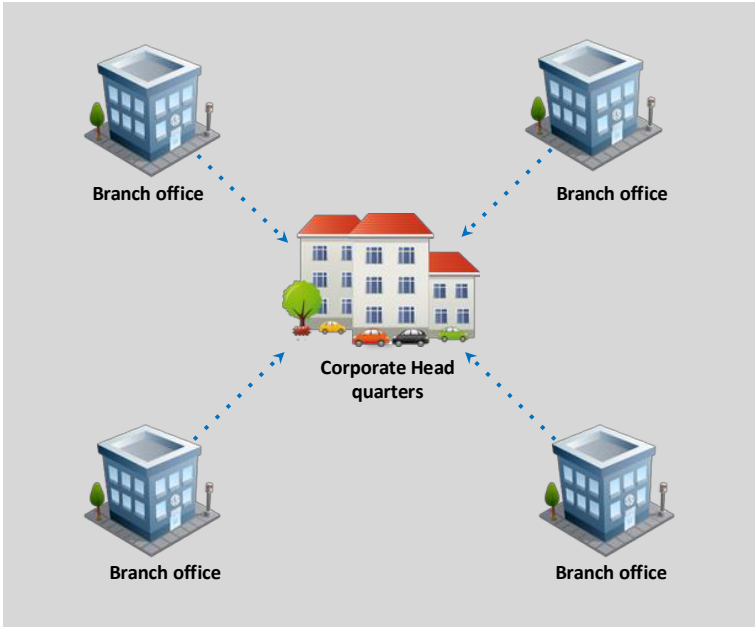
Full Mesh VPN Topology

- This topology is suitable for complicated networks where all **peers communicate** with one another
- Device to device communication in a network takes place with a unique IPsec tunnel
- A peer-to-peer connection is established between each device, preventing a **bottleneck** at the VPN gateway and saving encryption/decryption overhead
- This topology is reliable and offers **redundancy**



Star Topology

- This topology allows remote branches to **securely communicate** with corporate headquarters
- **Interconnection** between branches is not allowed
- Deployed in a bank network, preventing one branch from compromising another branch
- Attackers must first **compromise** the central network before being able to compromise a second branch
- New sites can be **added** easily and only the central sites needs to be updated
- The central site plays a major role in this **topology**. If it fails, all connections go down



VPN Security Risks

01 VPN Fingerprinting

02 Insecure Storage of Authentication Credentials

03 Username Enumeration Vulnerabilities

04 Offline Password Cracking

05 Man-in-the-Middle Attacks

06 Lack of Account Lockout

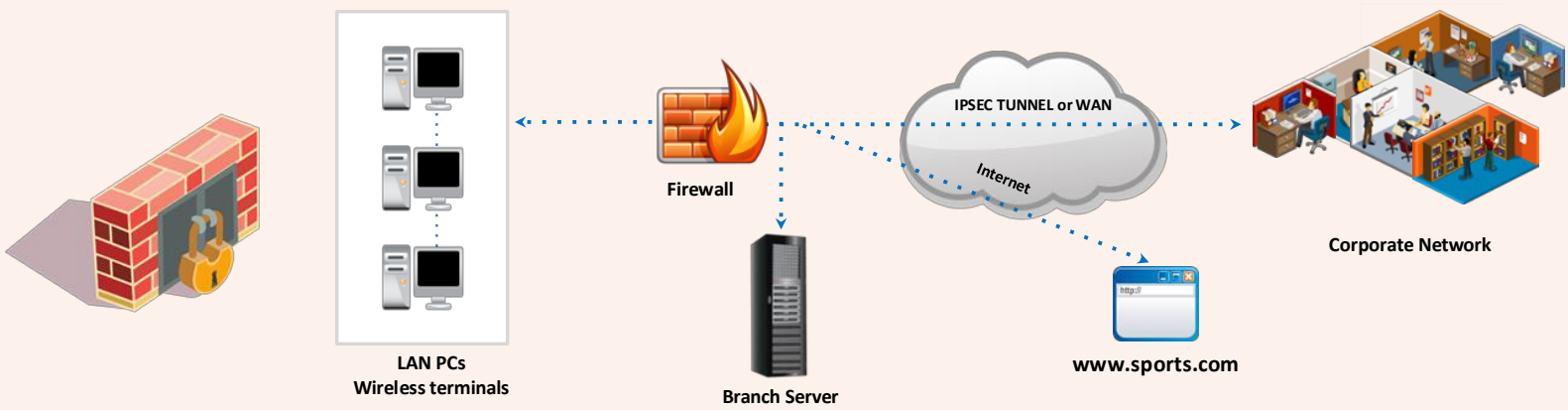
07 Poor Default Configurations

08 Poor Guidance and Documentation

VPN Security

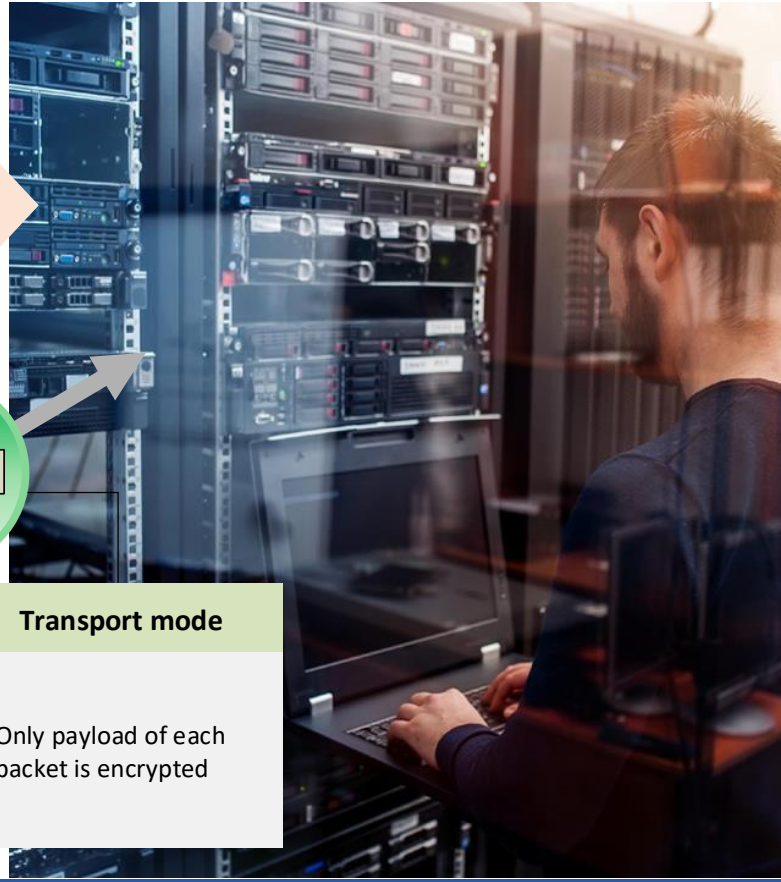
Firewalls

- Firewalls establish a protection barrier between the VPN and the Internet
- Before implementing a VPN, ensure that a **good firewall** is in place
- Firewalls should be configured to restrict open **ports**, the types of **packets** and **protocols** that traffic is allowed to pass through to the VPN



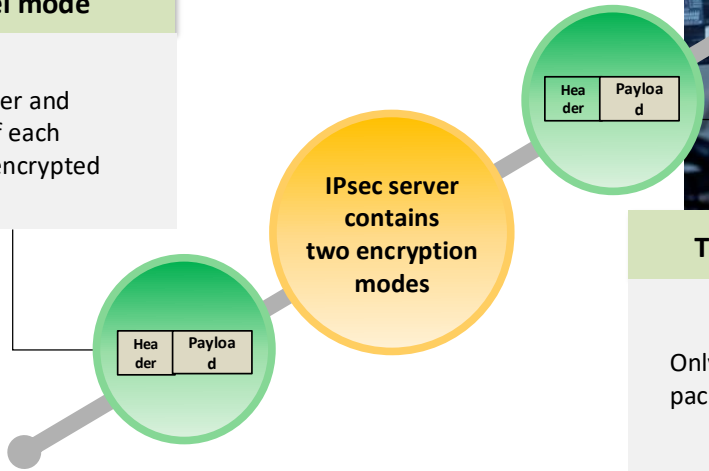
IPsec Server

- The IPsec server enhances VPN security through the use of strong **encryption algorithms** and authentication



Tunnel mode

Both header and payload of each packet is encrypted



Transport mode

Only payload of each packet is encrypted

AAA Server

❑ The AAA server is used to establish secure access in a **remote-access** VPN environment

AAA server performs the following types of checks

Authentication

- Who are you ?

Authorization

- What are you allowed to do?

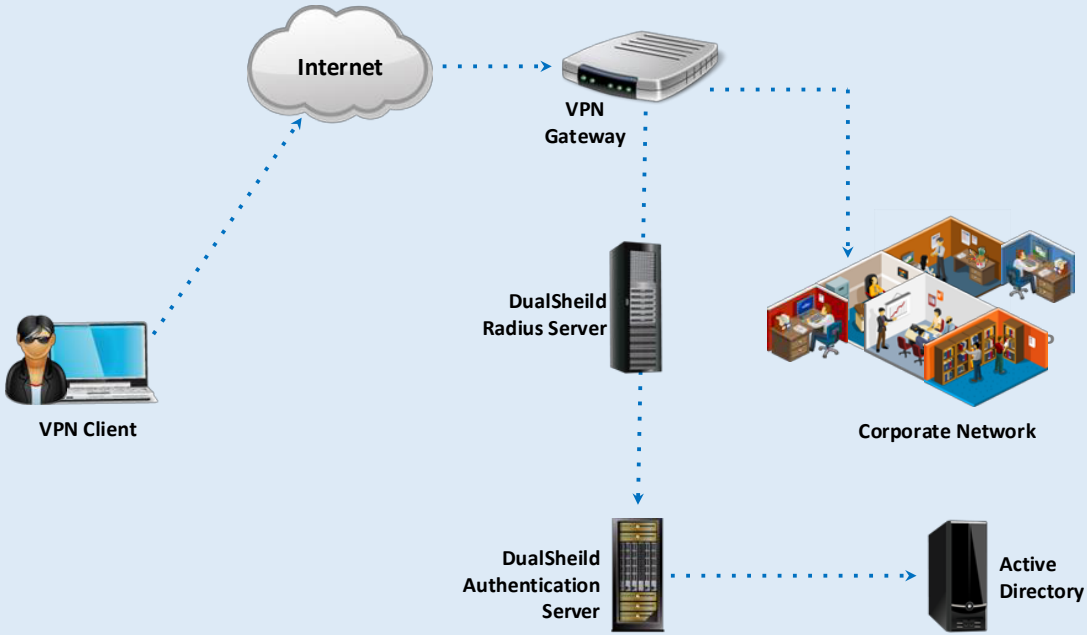
Accounting

- What do you actually do?

Remote Access Dial-In User Service

1. Remote Access Dial-In User Service (**RADIUS**) is the simplest way to use centralized authentication in VPNs
2. RADIUS is a **software application** that runs on a server and has access to all users in the domain
3. In a VPN environment, RADIUS manages both the user authentication and authorization. This reduces the total cost of ownership by managing the credentials from a **central location**
4. When a user attempts to connect the VPN server contacts the RADIUS server who then authenticates the user through a **Windows domain** using both a username and a password (typically a Windows domain controller)
5. If the username and password are correct and they have "**dial-in**" access granted they will be allowed to access the VPN
6. The VPN equipment must securely communicate with the RADIUS server and verify the user meets certain set conditions, before granting **permission** to access the network

Remote Access Dial-In User Service (Cont'd)



Connection to VPN: SSH and PPP

- PPP and SSH are **integrated in kernels** that use VPN
- VPNs using PPP and SSH work well with **dynamic IP addresses**

Configuring Network Connection

While configuring **multiple tunnels** to the computer, ensure that **IP address** of every tunnel is unique

Client and server contain **PPP processes** to communicate

PPP processes communicate using **SSH connection**

Connection to VPN: SSL and PPP

- **Point-to-point protocol** over a secure socket layer connection
- **Secure Socket Layer**
  - Built-in support for host authentication through digital certificates
- Establishing a **network connection**
  - Initial handshake for secure communication
  - "**Hello**" messages establish:
    - **SSL Version**, support for Cipher suites, and some random data
  - Key is determined separately from handshake
  - Data transferred over the link

Connection to VPN: Concentrator

Concentrator

- Expert mechanism that allows connections from **VPN peers**
- Validates its clients
- Insists on **security policies** of VPN
- Reduces operating cost of **VPN administration** and encryption from gateways, local hosts

Configuring Network Connection

- **Configure** the concentrator
- Set up **client software**
- To use VPN, client should use client software