Secure VPN Configuration and Management
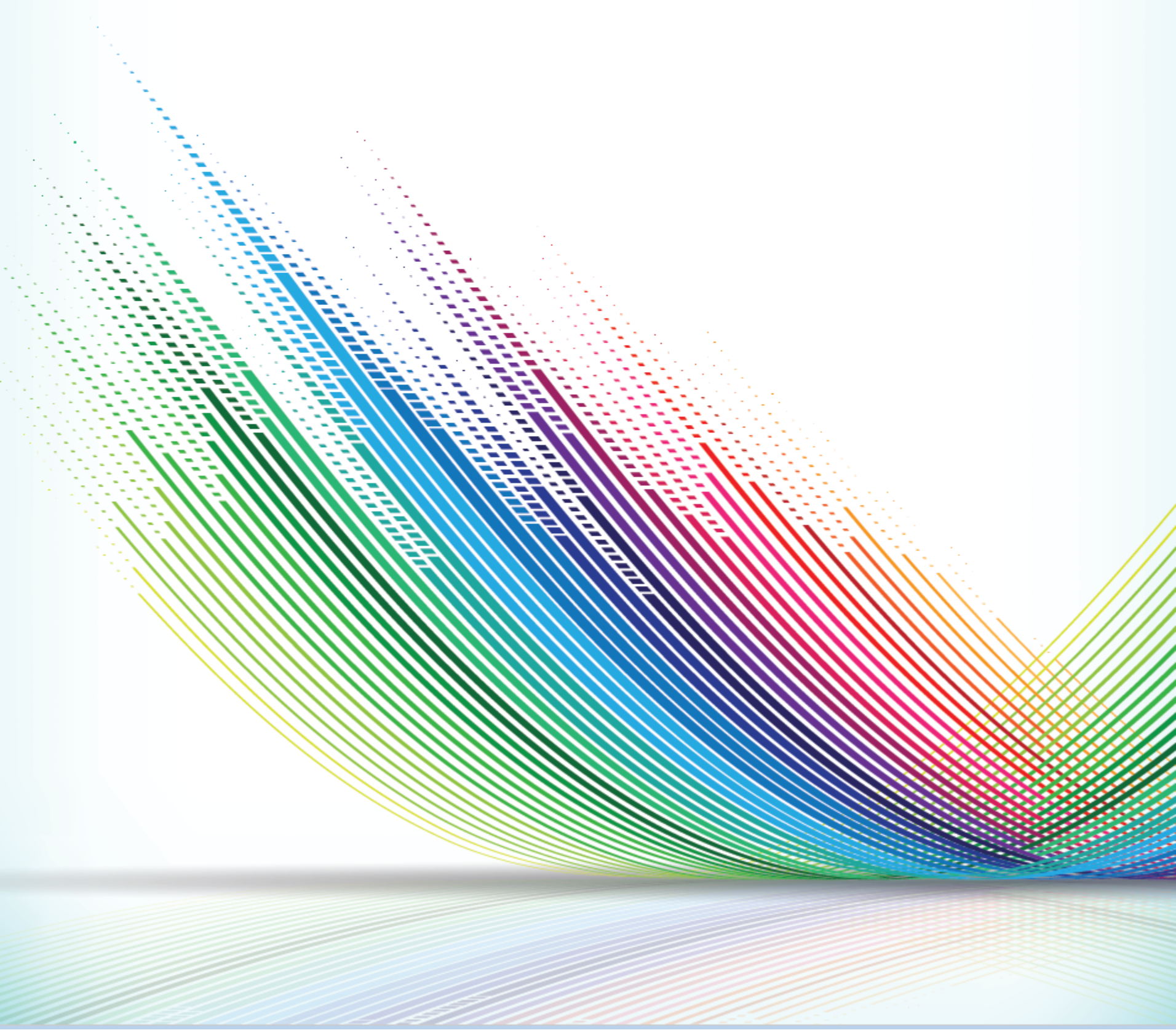
Module 09

Secure VPN Configuration and Management

Module 09

C|N D

Certified | Network Defender

Certified Network Defender

Module 09: Secure VPN Configuration and Management

Exam 312-38

Module Objectives

- Understand how a Virtual Private Network (VPN) functions
- Understand the importance for establishing a VPN
- Describe VPN components
- Describe the implementation for VPN concentrators and functions
- Explain the different VPN technologies

- Discuss the process for selecting the correct VPN technology for your needs
- Explain the core VPN functions
- Explain VPN topology implementation
- Discuss VPN security concerns
- Discuss VPN security and performance

Implementing a VPN for an organization is another important task network administrators must do to ensure the security for an organization's network especially when communicating over a public network.

This module focuses on the implementation and configuration of a VPN in an organization. The discussion ranges from the concepts of understanding what a VPN is to the configuration best practices for VPNs.

Understanding a Virtual Private Network (VPN)

- A VPN is used to **securely communicate** with different computers over unsecure channels

- A VPN uses the Internet and ensures secure communication to distant offices or users within their **enterprise's network**

VPN Architecture

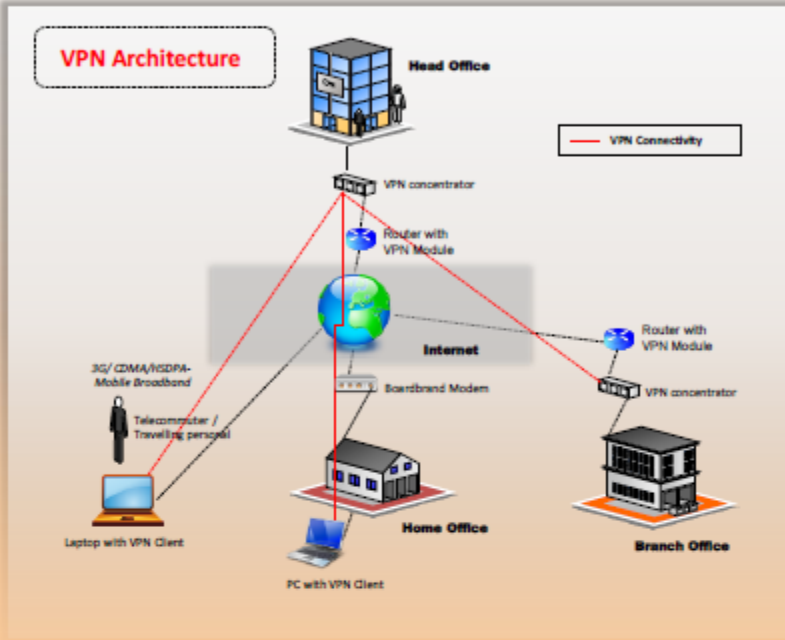Most of the organization has their offices located at different locations around the world. There is a need of establishing a remote connection between these offices as a result. Previously, remote access was established through leased lines with the help of dial-up telephone links such as ISDN, DSL, cable modem, satellite, and mobile broadband. However, establishing remote connections with these leased lines is quite expensive and the costs rise when the distance between the offices increases.

To overcome the drawback of traditional remote access technologies, organizations are adopting Virtual Private Networks (VPNs) to provide remote access to their employees and distant offices.

Virtual private network (VPN) offers an attractive solution for network administrators to connect their organization's network securely over the Internet. VPN is used to connect distant offices or individual users to their organization's network over secure channel.

VPN uses a tunneling process to transport the encrypted data over the internet. IPSec is the common protocol used in VPN at the IP level. VPN ensures the data integrity check by using a message digest and ensures data transmission is not tampered with. VPN guarantees the quality of service (QoS) through service level agreements (SLA's) with the service provider.

- **Typical features of VPN:**

  - Establishes a connection between the remote system and a LAN across an intermediary network such as the Internet.

  - VPNs allow cheap long distance connections over the Internet since both endpoints require a local Internet link which serves as a free long-distance carrier.

  - VPN uses tunneling or encapsulation protocols.

  - VPNs use encryption to provide a secured connection to a remote network over the Internet and protect your communication.

  - They provide virtual access to the physical network as if you are physically located in the office.

- **Advantages of VPNs:**

  - VPNs are inexpensive.

  - They provide the framework for corporate intranets and extranets.

  - Ensures secured transfer of data.

  - VPN allows you to access both web applications and websites in complete anonymity.

- **Disadvantages of VPNs:**

  - Designing and the implementing the VPN is a complex issue, it requires experts for configuring.

  - Reliability depends on the service provider that you choose.

- **VPN Architecture:**

  A certain set of protocols and standards need to be followed while establishing a VPN architecture. Network administrators should decide the scope, implementation and deployment of the VPN along with continuous network monitoring in order to ensure the security of a VPN. They should be continuously aware of the overall architecture and scope of the VPN.

- **Protocols used in deploying a VPN:**

  For deploying the virtual private networks, there are two primary options IPsec and SSL. Each protocol has its own unique advantages and utilized depending on the requirement of the user or the organization's IT processes.

- **IPsec VPN:**

  IPsec-based VPN is the most commonly used deployment solution by most of organizations. It is a set of protocols and standards developed by the internet engineering task force (IETF) for secure communication on the IP layer. It ensures the security of each packet in communication by encrypting and authenticating them. IPsec connections are

established using VPN client software which is pre-installed and it mainly focuses on the company managed desktops.

- **Advantages:**
  - ○ IPsec VPNs can support all IP-based applications to an IPsec VPN product.
  - ○ It offers tremendous versatility and customizability through modification of the VPN client software.
  - ○ Organizations can control the VPN client functions by using the API's in IPsec client software.
  - ○ Ensures secure exchange of IP packets between remote networks or hosts and an IPsec gateway located at the edge of your private network.

  The three basic applications when using IPsec VPN's (associated with business requirements) are:

- **Remote-Access VPNs:** These allow individual users, such as telecommuters, to connect to a corporate network. This application creates an L2TP/PPTP session. IPSec encryption protects this L2TP/PPTP session.

- **Intranet VPNs:** This helps connect branch offices to the corporate headquarters, creating a transparent Intranet.

- **Extranet VPNs:** This allows companies to connect with their business partners (for example, suppliers, customers, and joint ventures).

- **SSL VPN (web-based):**

  SSL-based VPNs provide remote-access connectivity using a Web browser and its native SSL encryption irrespective of the location. SSL doesn't require any special client software to be pre-installed and is capable of any type of connectivity. The connectivity ranges from company-managed desktops and non-company-managed desktops, such as employee-owned PCs, contractor or business partner desktops. It helps in reducing the desktop software maintenance as it downloads the software dynamically whenever there is need.

  - **Advantages:**
    - ○ It offers additional features like easy connectivity from non-company-managed desktops, little or no desktop software maintenance.
    - ○ It provides accessibility of the SSL library and access to port 443 TCP.
    - ○ It will work wherever someone can gain access to HTTPS websites such as Internet Banking, Secure Webmail or Intranet sites.

How VPN Works?

- Client willing to connect to a company's network initially connects to the internet

- Client initiates a **VPN connection** with the company's server

- Before establishing a connection, Endpoints 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

VPN uses **authorization** and **encryption** to connect external host securely

Unauthorized Host

Authorized Host
with VPN client software
Which handles authorization
and encryption

Internet

Firewall with VPN option

Internal Network

A VPN enables a secured connection over the Internet from a public network to a private network placed at a far-off site. All the network traffic in a VPN is encrypted and passes through a virtual secure tunnel, placed between the client and VPN server.

All the packets passing through a VPN is encrypted or decrypted with respect to inbound or outbound traffic. The packets are encrypted at the client side and the packets are decrypted at VPN server. For example, when a client with a VPN connection enabled, browses Youtube.com. This outbound traffic is encrypted at the client side. The encrypted data is then sent to nearest VPN server and passes it to the gateway server. Here, the data is decrypted and sent to the server hosting Youtube.com. When Youtube.com sends a reply request, the VPN server performs the reverse process on the outbound traffic.

A VPN keeps a close look on any unsecure networks. It creates a new IP address for the encrypted packet concealing the real IP address which disables attackers from finding the real IP address of the packets sent.

Why Establish VPN?

CND Certified Network Defender

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
- ✓ Provide telecommuter support
- ✓ Faster Return On Investment (ROI) than with a traditional WAN

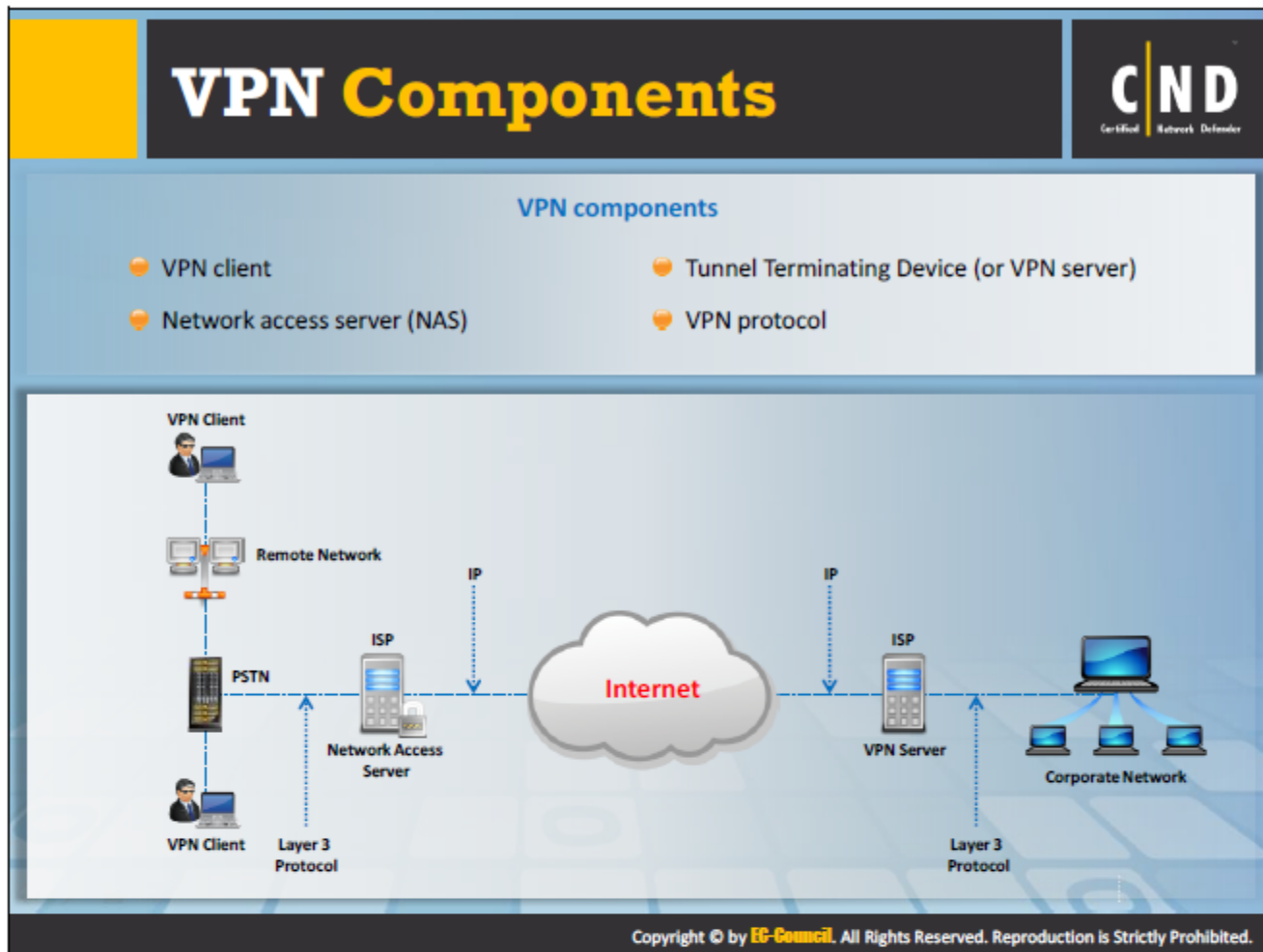The easy accessibility of sensitive data over the Internet poses a serious security threat to organizations. Attackers easily exploit and gain access to sensitive information if it traverses on an unsecured public network such as the Internet. A VPN ensures reliable communication through an encrypted tunnel, preventing attackers from gaining access to organization information. A well designed and implemented VPN can provide the following benefits:

- Enables a secured connection across multiple geographical locations.

- Saves time and expenditure for employees as it allows the sharing of information between a corporate office and its regional office.

- Enhances the level of output for remote users.

- Improves the security of data by concealing the IP address from attackers.

- Handles multiple connections simultaneously and provides the same quality of service for each connection.

- Ability to provide a secured connection to larger enterprises.

- Implementation of a VPN increases the bandwidth and efficiency of the network.

- Less maintenance cost.

This encrypted traffic proves beneficial when the user connects its system to Wi-Fi hotspots at public places. The encryption makes it difficult for eavesdroppers in the network to identify the encrypted data.

A VPN allows users to access the servers across the world making it easy for them to access all types of content. Users do not have to face restrictions like geo-blocking while browsing. A VPN allows the user to stay anonymous without sharing their device information in the network. By hiding this data, a VPN restricts websites from spying or monitoring the user. To avoid excessive monitoring from third party websites or attackers, users should install a VPN for safe browsing.

VPN Components

VPN components

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

The VPN architecture consists of four main components:

- VPN client: A computer that initiates a secure remote connection to a VPN server.

- Network access server (NAS): It is also called a media gateway or a remote-access server (RAS). It is responsible for setting up and maintaining each tunnel in a remote-access VPN. Users need to connect to the NAS to use a VPN.

- Tunnel terminating device (or VPN server): A computer that accepts VPN connections from VPN clients.

- VPN protocol: It includes VPN specific protocols used to manage tunnels and encapsulate private data. It includes the use of PPTP and L2TP protocols along with IPsec.

The following diagram shows the use of various VPN components in a remote access VPN:
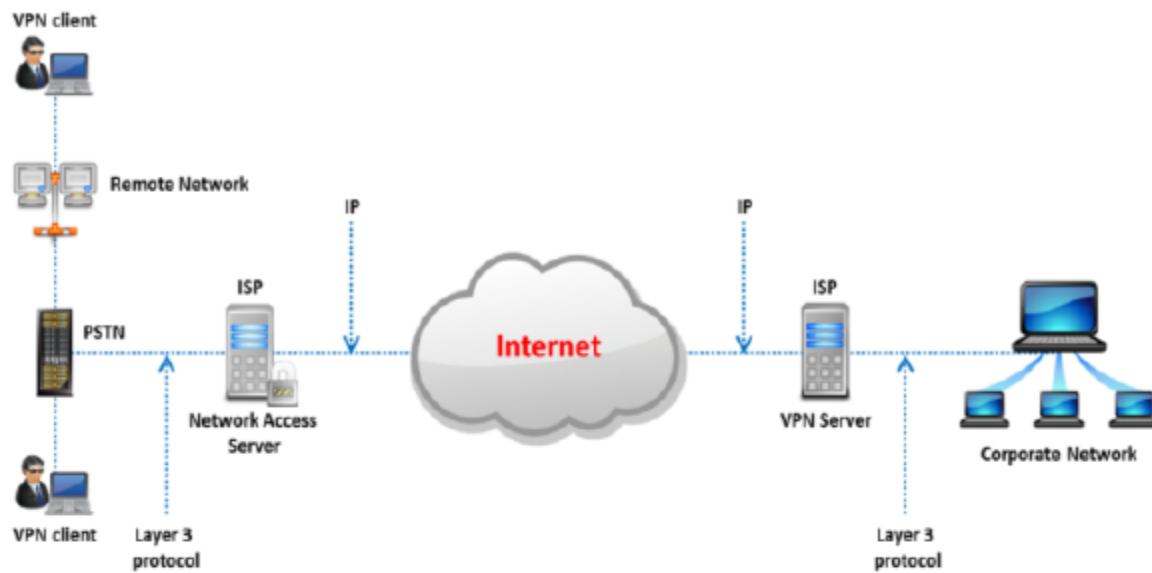

FIGURE 9.1 VPN components in a remote access VPN

A typical remote access VPN connection is established as follows:

- The remote user propagates a PPP connection with an ISP's NAS through a PSTN.

- The packets sent by the user are sent to the tunnel connecting NAS and VPN server after authenticating the user.

- The packet is encapsulated before placing it in the tunnel.

- The location of the VPN server depends on the model used for the VPN implementation.

- The VPN server accepts the packet from the tunnel, de-encapsulates and sends it to the final destination.

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

VPN concentrators normally enhance the security of the connections made through a VPN. These are generally used when a single device needs to handle a large number of VPN tunnels. They are best used for developing a remote-access VPN and site-to-site VPN.

VPN concentrators implement security of the tunnels using tunneling protocols. These protocols manage the following:

- Manage the flow of packets through the tunnel.

- Encapsulation and de-encapsulation of packets.

- Manage the creation of tunnels.

A VPN concentrator works in two ways:

- Receives plain packets at one end, encapsulates at the other end and forwards the packet to the final destination.

- Receives encapsulated packets at one end, de-encapsulates at the other end and forwards the packet to the final destination.
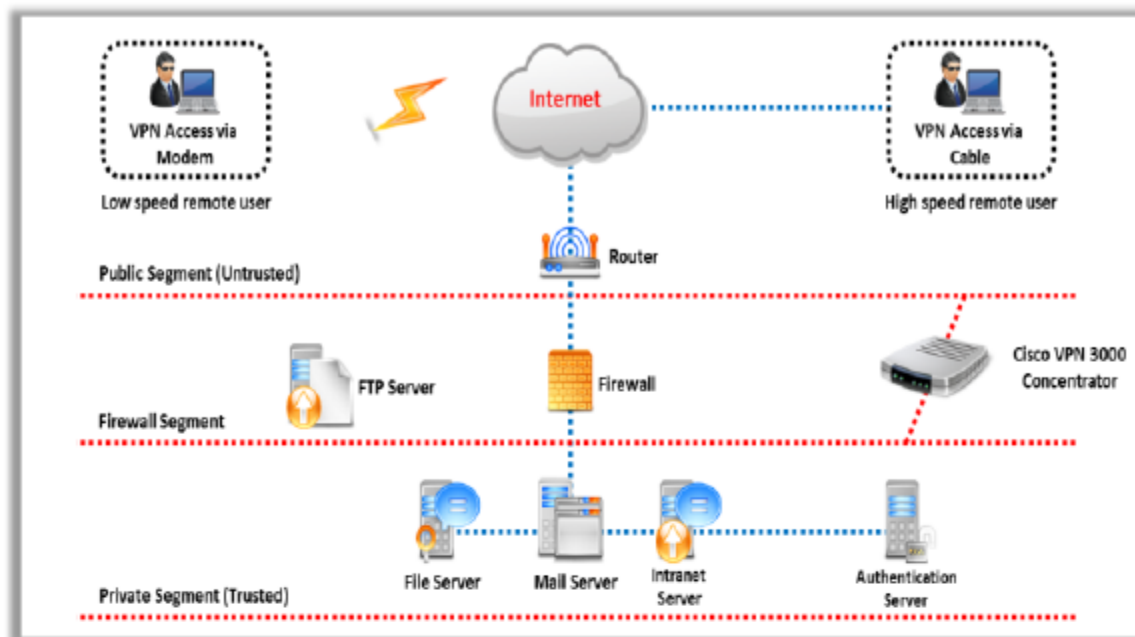
FIGURE 9.2: VPN concentrator

In the figure, the VPN concentrator is placed in parallel with the firewall supporting remote users who have both a slow and a fast Internet speed. If the VPN is placed behind the firewall, the implementation requires additional configuration changes and is vendor dependent.

VPN concentrators provide a high level of security for SSL and IPsec VPN architecture. A normal VPN tunnel requires IPsec to be implemented on the network layer of the OSI model. A major benefit of using a VPN concentrator is that the client is considered to be present outside the network and can access the network as if it is connected.

Functions of a VPN Concentrator

CND
Certified | Network Defender

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

The VPN Concentrator functions are:

Manages security keys
5

Encrypts and decrypts data
1

Manages data transfer across the tunnel
3

Assigns user addresses
7

8

2
Authenticates users

4
Negotiates tunnel parameters

6
Establishes Tunnels

Manages data transfer inbound and outbound as a tunnel endpoint or router

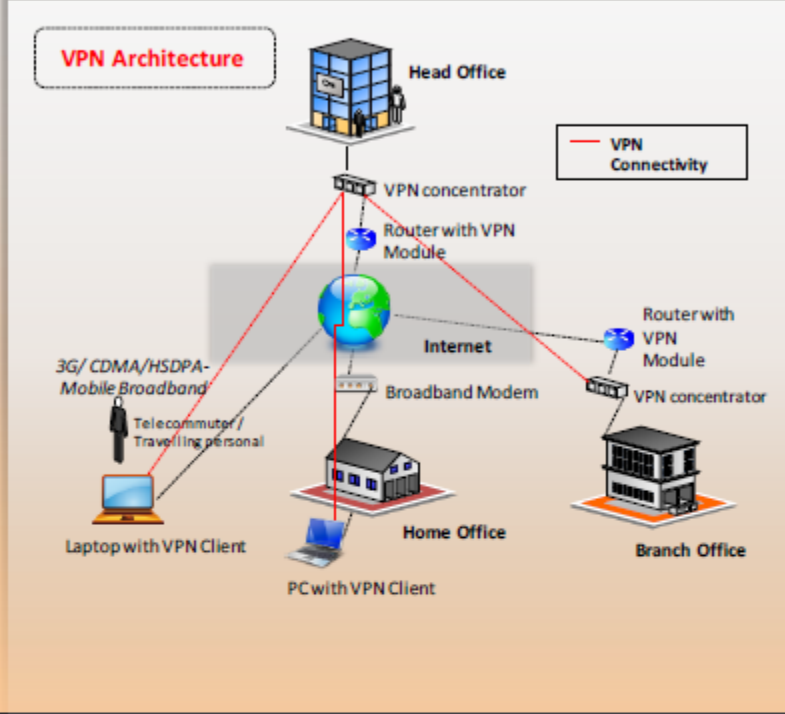A VPN concentrator adds more security controls to the router, improving the security of the communication. The functions of a VPN concentrator are as follows:

- **Data encryption and encapsulation:** The VPN concentrator encrypts the data and encapsulates it into an IPsec packet. Being bi-directional, it initially encapsulates the plain packets it receives and later expands them at the end of the tunnel before sending them to the destination.

- **Managing tunnels:** By adding the features of advanced data and network security, a VPN concentrator has the ability to create and manage large VPN tunnels. These tunnels ensure the data integrity among the systems.

- **User Authentication:** A VPN concentrator authenticates users at either the computer level or at the user level. Authentication at the computer level takes place using the Layer Two Tunneling Protocol (L2TP) protocol whereas authentication at the user level takes place using the Point-to-Point Tunneling Protocol (PPTP).

- **Traffic handler:** A VPN concentrator routes the tunneled and non-tunneled traffic depending on the server configuration. It simultaneously handles traffic of a corporate network as well as Internet resources.

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

Remote-access VPNs are used mainly to connect individual hosts to a private network. This allows the users to access the information provided in the private network. An older name for a remote-access VPN is a virtual private dial-network (VPDN) in which a dial-up configuration is required for the connection to a server.

Every host using remote-access needs to have the VPN client software installed, that wraps and encrypts the data before the host sends any traffic over the Internet to a VPN gateway. After reaching the gateway, the data is unwrapped, decrypted and passed over to the final destination in a private network. The gateway performs the reverse process in order to send the data packets back to the user. The remote-access VPN consists of two types of components:

- **Network access server (NAS) or remote-access server (RAS)**: NAS is required while users are accessing a VPN. A separate authentication process is involved while authenticating users accessing a VPN

- **Client software**: Users accessing a VPN from their own network need to install software that helps create and manage the VPN connection

VPN client software and a VPN gateway are required for the hosts supporting a remote-access VPN. Most of the VPN gateways support only IPSec while maintaining VPN services.

Advantages

- Minimizes the connection cost for the users.

- Encapsulation and encryption of data packets provides an added security layer. This hides the IP address of the packets and prevents the attackers from accessing the packets.

- Handle large number of users. The VPN provides the same service even if more users are added to VPN network.

- Sharing of files from a remote location.

Disadvantages

- Computers without any anti-virus installed pose a threat to the VPN connection.

- Implementing many VPN connections simultaneously may affect the bandwidth of the network.

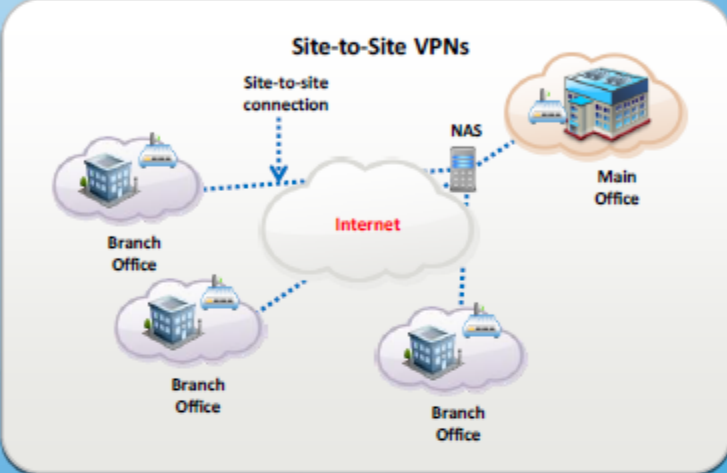- Time consuming accessing files, applications over the Internet.

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

Site-to-Site VPNs

The site-to-site VPN helps connects all the networks together. For example, the branch offices of an organization can be connected to the main campus through a site-to-site VPN. The main differentiation between a remote and a site-to-site VPN is that site-to-site VPNs do not require the need of any client software. The entire traffic is sent through a VPN gateway that encapsulates and encrypts the data packets passing through it.

In a site-to-site VPN, the outbound traffic is passed through a tunnel to the VPN gateway. The data packets in the outbound traffic are encapsulated and encrypted at the gateway and is passed to the tunnel over the Internet. The traffic is sent to the nearest gateway in the target location. The nearest gateway decrypts and de-encapsulates the data packets and they are then forwarded to the final destination.

A site-to-site VPN consists of two types:

Intranet-based

Creates an intranet VPN in order to connect each individual LAN to a single WAN.
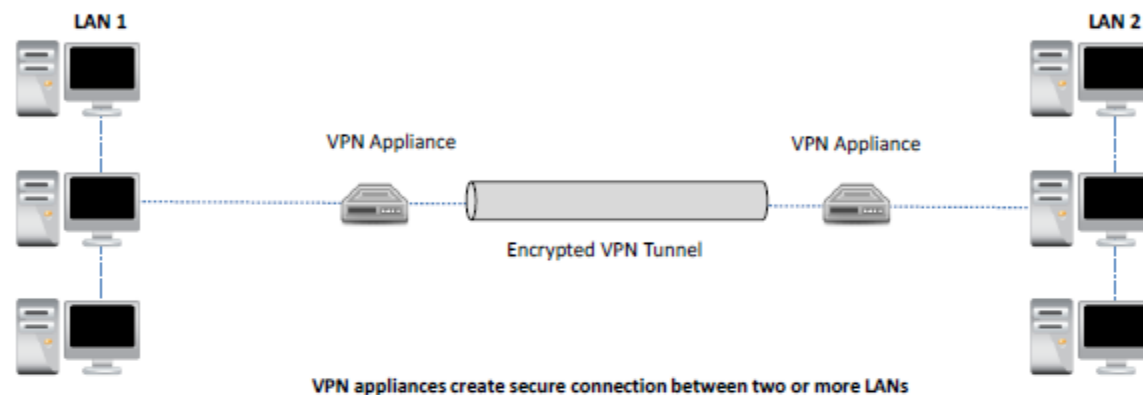
Extranet-based

Extranet VPN connects each single LAN of an organization. The extranet VPN configuration prevents any access to an intranet VPN.

Hardware VPNs

CND

- 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

- **Advantage**:

  It is more **secure**, as the hardware device's main function is to manage VPN connections
- **Disadvantage**:

  It is more **expensive** and changes the network design

LAN 1

LAN 2

VPN Appliance

VPN Appliance

Encrypted VPN Tunnel

VPN appliances create secure connection between two or more LANs

Hardware VPN Products

CND

Manufacturer	Product Name	Web Site
Cisco Systems	VPN 3000 series concentrators, VPN 3002 Hardware Clients, 7600 series routers, and Web VPN Services Module	www.cisco.com
SonicWALL	SonicWALL PRO 5060,4060,3060,2040,1260	www.sonicwall.com
Juniper Networks	NetScreen 5000, 500,200, ISG series, and Secure Access 6000/4000 series	www.juniper.net
WatchGuard	WatchGuard Firebox X series	www.watchguard.com

Hardware-based VPNs are separate devices that consist of individual processors and hardware firewalls. They easily manage authentication and encryption of the data packets. The main advantage of using a hardware-based VPN is that they provide more protection than the software variant.

Advantage

- Provides load balancing especially for large client loads.

Disadvantage

- It is more expensive than software VPN.

- More useful for large business organizations than for smaller ones.

- Less scalability.

Software VPNs

C|ND
Certified Network Defender

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

Advantage:

- **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

Disadvantage:

- **Extra processing** burden to devices on which it is installed

- It is **less secure** and prone to attacks

Software VPN Products

C|ND
Certified Network Defender

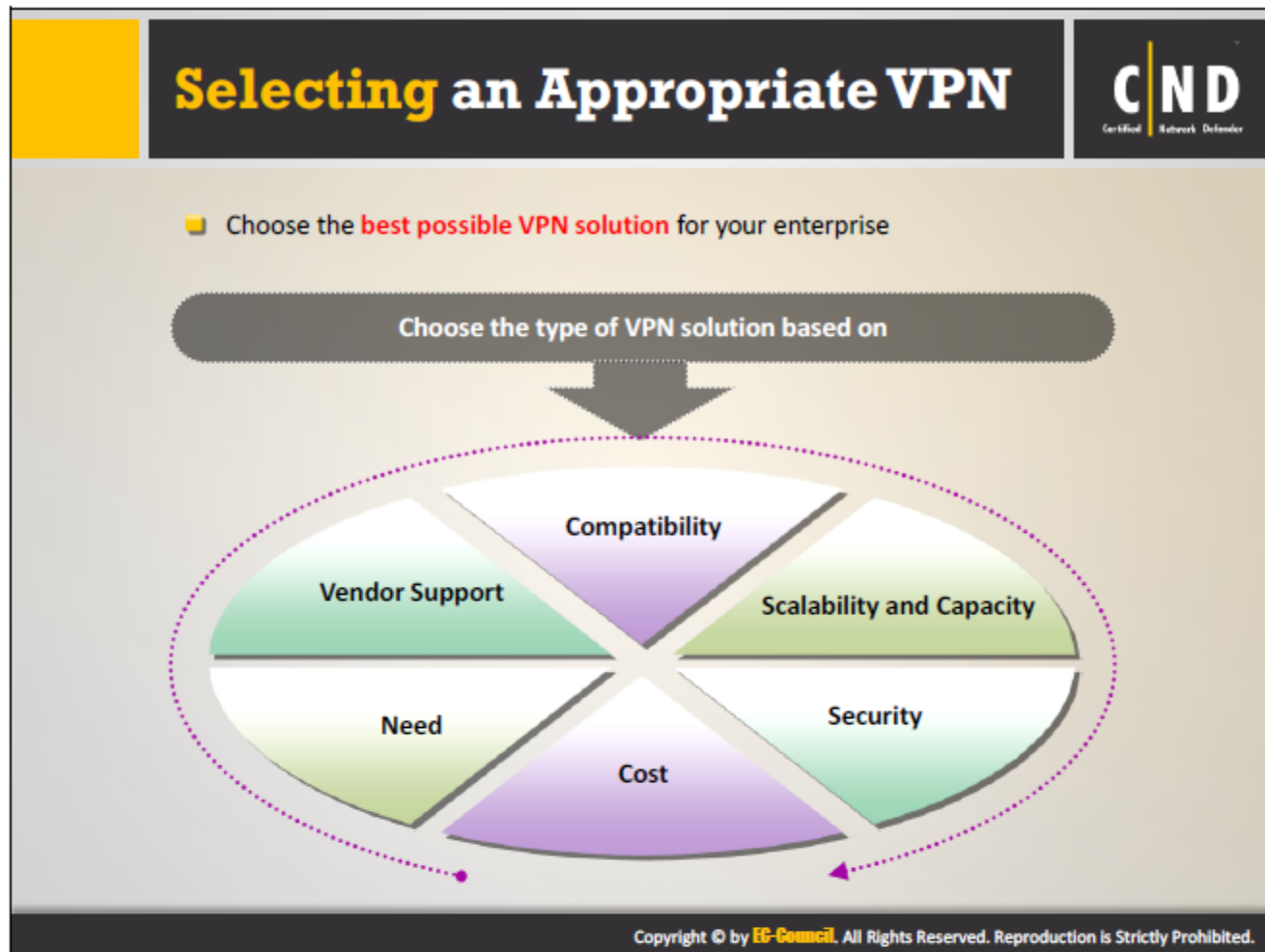| Manufacturer	Product Name	Web Site
CheckPoint	VPN-1 VSX,VPN-1 Pro, VPN-1 Edge, Firewall-1	www.checkpoint.com
NETGEAR	ProSafe VPN	www.netgear.com
Symantec Corporation	Symantec Enterprise Firewall, Norton Personal Firewall for Macintosh	www.symantec.com

Software-based VPNs are best suited for network traffic management and when the same party does not manage the VPN end points. Traffic management is performed using a tunneling process depending on the protocol and address of the traffic. Hardware encryption accelerators are used in order to improve the performance of the network.

Advantages

- Minimizes the cost of an additional hardware purchase.

- It is easy to deploy and does not change the target network.

- More scalability.

Disadvantage

- Increased processing tasks for devices implementing the VPN.

- Security is an issue and is prone to more attacks as they need to share the server with other servers and operating systems.

Selecting an Appropriate VPN

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

Choose the type of VPN solution based on

- Compatibility
- Vendor Support
- Scalability and Capacity
- Need
- Security
- Cost

The selection of an appropriate VPN depends on many factors such as cost, protocols, technical issues etc. The following are a few factors to consider while selecting a VPN:

- **Compatibility**: The organization should consider the compatibility of the selected VPN within the organization's network and determine whether it is possible to adopt the selected VPN. Selecting and implementing a VPN which is not compatible, will add an extra expense on the company's expenditure and cause security issues.

- **Scalability**: Increasing the number of employees working for an organization is a common trend. As the number of employees increases, the configured VPN also needs to accommodate the extra number of employees at the same time. The inability to handle the increasing number of users adversely affects the performance of the network. The organization must select a VPN that can handle any number of users at any time without affecting the performance of the network.

- **Security**: Security is an important factor while selecting a VPN. Two major criteria in selecting a VPN are:

  - **Authentication**: Organizations need to select an appropriate authentication method depending on the type of network on which the VPN is implemented.

  - **Encryption**: Organizations should be highly alert regarding the encryption process for the selected VPN. Some VPNs do not provide direct encryption, allowing attackers to get information from the network.
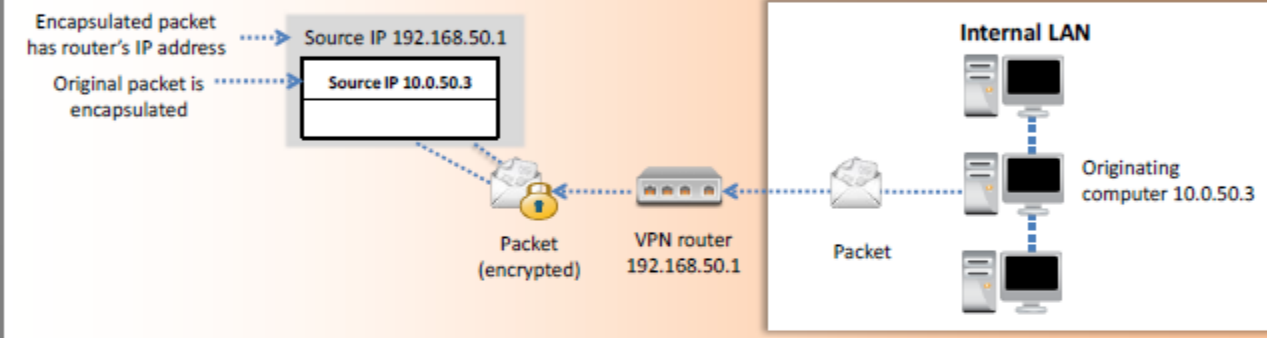
- **Capacity**: Organizations need to foresee the number of users joining the organization in the future and then select the VPN accordingly.

- **Cost**: An organization should consider cost as a factor while selecting VPNs.

- **Need**: The need for a VPN depends on the requirements of an organization. Whether remote employees need access to the network or there are encrypted traffic rules. Each organization is different and it these differences which will decide the appropriate VPN choice.

- **Vendor Support**: Two different factors in vendor support are as follows:

  - Number of servers present and their location: The VPN is selected according to the location of the vendor server and the activities performed.

  - Does the vendor limit connections, use bandwidth throttling or restrict service? VPNs that control bandwidth, reduce Internet speeds or limits them in any way are not used in an organization. Also, care should be taken while dealing with the protocols and services running in the network. The organization needs to decide on whether the existing services and protocols running are actually needed by the organization or not.

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

Encapsulated packet has router's IP address ····> Source IP 192.168.50.1

Original packet is encapsulated ····> Source IP 10.0.50.3

Packet (encrypted)

VPN router 192.168.50.1

Packet

Internal LAN

Originating computer 10.0.50.3

Encapsulation is the method in which protocols have separate functions to communicate among each other by hiding the data. Data vulnerability increases if the data does not pass through a secure channel. When data is transmitted through using VPN Tunneling it is encapsulated making it secure. It relies on various technologies and protocols such as GRE, IPsec, L2F, PPTP and L2TP.

The VPN tunnel acts as a path between the source and the destination. To send the encapsulated data securely, it is necessary to establish the tunnel. All the data packets travelling through the tunnel are encapsulated at the source point and de-encapsulated at the destination point. To send the data to the destination point, a tunnel data protocol is created. The information in the data packet is called a payload. The tunnel data protocol encapsulates the payload within the header containing the routing information. Once the server receives the payload it discards the header, de-encapsulates the payload and sends it to the destination.

All data packets transmitted through a VPN network are encapsulated using a VPN base or a carrier protocol. The encapsulated data packet is then sent through the tunnel which is later de-encapsulated at the receiver's end.

For example, TCP/IP packet encapsulated with an ATM frame, hides the TCP/IP packet within the ATM frame. Upon receiving the ATM frame, the encapsulated packet de-encapsulates in order to remove the TCP/IP packet from within.

The main goal is to provide an extra layer of security to each packet travelling across the Internet. These protocols define the way packets are sent and received by the ISP.

Types of VPN Tunneling

- **Voluntary Tunneling:** In voluntary tunneling, the client machine sets up a virtual connection to the target tunnel server. Voluntary tunneling can be setup only when there is an existing connection between the client and the server.

- **Compulsory Tunneling:** In compulsory tunneling, the client machine is not the tunnel end-point. A remote access server configures and creates the tunnel. The dial-up access server acts as the tunnel end-point.

Advantages of VPN Tunneling

VPN Tunneling allows the deployment of a VPN in a public network. It is a cost effective method, as a dedicated network is not required.

VPN encapsulation protocols are:

- Point to point Tunneling protocol (PPTP): This protocol lets multiprotocol to be encrypted and encapsulates the IP header that is directed across the Internet. Used in both remote and site-to-site VPN connections. PPTP manages the tunneling using a TCP connection and encapsulates PPP frames in IP datagrams.

- Layer 2 tunneling protocol (L2TP): Permits multiprotocol to be encrypted and sent across any medium supporting point-to-point delivery. L2TP is installed using the TCP/IP protocol. Encapsulation uses L2TP and consists of two layers:

  - L2TP encapsulation: The PPP frame is encapsulated using a L2TP header and an UDP header.

  - IPsec encapsulation: The L2TP message after the first layer is encapsulated using IPsec encapsulating security payload header, IPsec authentication trailer and a final IP header.

- Secure shell (SSH): A connection-oriented service that uses a public key cryptography in order to authenticate a remote user. Includes two types of features:

  - Port forwarding

  - Secure Tunneling

- Socket secures (SOCKS): Enables clients to communicate with Internet servers through firewalls. SOCKS are employed on proxy servers.

VPN Core Functionality: Encryption

- Packets sent over a VPN are **encrypted** to maintain the confidentially of the information
- Packets are read by decrypting with the **public keys** from the sender
- **Common VPN Encryption Technologies**
  - Triple Data Encryption Standard (3DES)
  - Secure Sockets Layer (SSL)

Certificate Authority(CA)

CA issues one or more certificates to organizations

Internet

Key is sent to VPN user to decrypt data

Branch Office

Certificates are managed by certificate server

Main Office

Key is sent to VPN user to decrypt data

Home Office

A VPN uses encryption to provide an additional layer of security to data transmitted over the VPN. Encryption plays an important role when sensitive data is carried over the Internet in an organization. All data that enters the VPN tunnel is encrypted and decrypts as soon as it reaches the end of the tunnel. An encryption key is used in the process helping the process of encryption and decryption. Encryption disables monitoring, logging or tampering of the data in an organization.

Encryption helps secure the data passing through the network. The sender encrypts the data passing through the network and the receiver decrypts the data. It requires no encryption on the communication link between a dial-up client and the internal service provider, as the process of encryption takes place between the VPN client and the VPN server.

In VPN encryption, both the sender and the receiver need to have a common encryption key that is sent along with the data. If a packet travelling through the VPN connection does not have the keys associated to it, then it is of no use to the computer. There are many mechanisms to determine the length of the encryption key. The encryption of messages using the same key enables easy interpretation of the encrypted data. The administrator can always select the encryption keys used for a connection.

In end-to-end encryption, the encryption occurs between the client application and the server. IPsec is used with an end-to end connection, once a remote access connection is made. IPsec works as follows:

- Encryption of an encapsulated packet using an encryption key. The key is known only to the sender and the receiver.

- An encapsulation header, a sub-protocol, conceals the sensitive information of the packets including: sender identity.
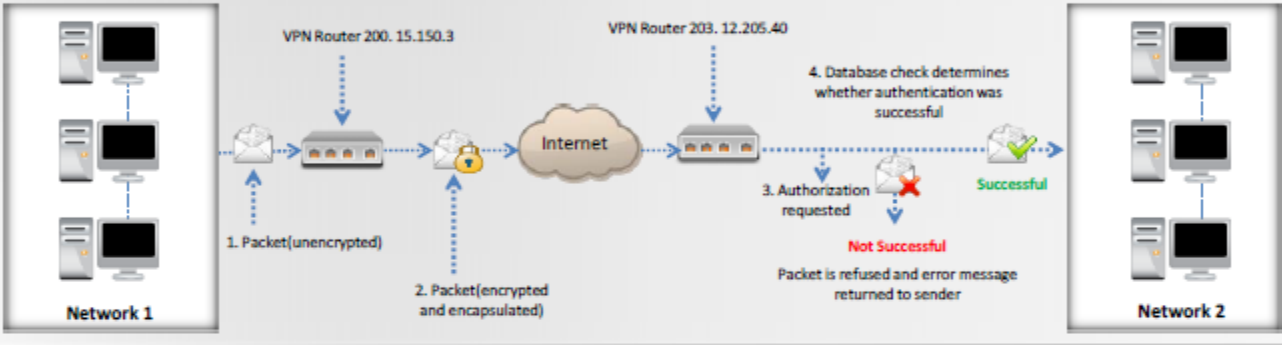
VPN encryption technologies

- Triple DES algorithm: A 64-bit block of data that processes each block three times with a 56-bit key. 3DES prevents the chances of breaking the encryption key.

- Secure Socket Layer (SSL): A secure technology that enables communication between the server and the client. SSL technology enables the secure transaction of credit card numbers, login credentials etc. over the internet.

- Open VPN: It is an open source VPN and works with the SSL protocol.

VPN Core Functionality: Authentication

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

Authentication is an integral part of VPN technology, as the hosts receiving a VPN communication need to ensure the authenticity of the hosts initiating and sending the VPN connections. A VPN employs three kinds of authentication:

- **User authentication:** The VPN deploys the mutual authentication concept. The VPN server authenticates the VPN client to check whether the client has the permission to connect. Also, the VPN client can authenticate a VPN server for proper permissions.

- **Computer authentication with L2TP/IPSec:** Remote-access computers are authenticated for proper permissions using IPsec and L2TP/IPsec.

- **Data authentication and Integrity:** All L2TP/IPsec packets sent are included with a cryptographic checksum based on the encryption key. Only the sender and the receiver know this checksum. This is to ensure the data sent is not manipulated during transit.

Authentication techniques used in VPN

- **IPsec Family**

    - **Internet Protocol Security (IPsec):** All application traffic is secured using the IP network. IPsec conducts session authentication and data packet authentication for any two securely connected entities. IPsec ensures a secured connection between two networks or remote networks to a main network.

- **Layer2 Tunneling protocol (L2TP):** This protocol initiates a connection between two L2TP connections. L2TP is always combined with the IPsec protocol in order to confirm security.

- **Kerberos**

  Kerberos consists of a record of clients and their private keys. Only the client and Kerberos know the details of the private key. Kerberos generates session keys that encrypt messages between two clients.

- **PAP**

  Password Authentication Protocol uses a clear text authentication mechanism for authenticating users. The PAP sends a username and password as per the NAS request. The NAS receives the username and password in clear text form, which means the NAS receives the details in an unencrypted form. This makes it easy for attackers establishing a connection with the NAS to acquire all the information.

- **SPAP (Shiva Password Authentication Protocol)**

  A reversible encryption mechanism that is more secure than PAP. SPAP plays its role when a Shiva client is attempting to access a server. However, this authentication mechanism is less secure than CHAP or MS- CHAP.

- **CHAP (Challenge Handshake Authentication Protocol)**

  The CHAP protocol is more secure than PAP. It uses an encryption authentication technique which transmits a password representation instead of an actual password during the authentication process. The sever sends a challenge message to the client to authenticate users. Users respond with a hash value created using a hash algorithm. The server then compares this hash value with its own calculation of the hash. If it matches, then authentication is acknowledged. The remote client creates a hash of the session ID, challenge and the password. It uses the MD-5 one way hashing algorithm.

- **MS-CHAP**

  The Microsoft Challenge Handshake Authentication Protocol uses a remote access server to send a session identifier and a challenge string to the remote access client. The client in turn sends an encrypted form of the identifier and challenge string to the server. This encrypted form is irreversible.

- **EAP (Extensible Authentication Protocol)**

  With EAP, the data for authentication is compared against an authentication database server. The EAP authentication protocol allows new plug-ins to be added at the client and server.

VPN Technologies

CND
Certified | Network Defender

1. 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

- Organizations 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

2. Secure VPNs

- 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

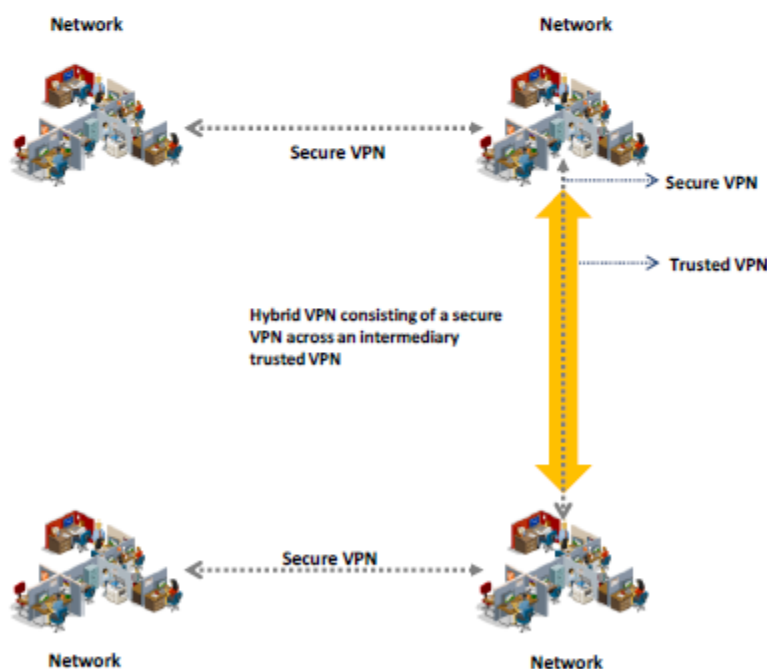- They protect the **confidentiality** and **integrity** of the data, but do not ensure the transmission path

VPN Technologies (Cont'd)

CND
Certified | Network Defender

3. 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

Hybrid VPN consisting of a secure VPN across an intermediary trusted VPN

VPN technology enables organizations to connect mobile and remote users with network access and also to connect separate branches of the same organization to a single network.

Common technologies used to deploy VPNs for secure data transmission are:

Trusted VPN

Even before the popularity of the Internet, service providers provided customers with specific circuits that could not be used by anyone else. This gave customers privacy and the ability to have their own IP addresses and policies. In order to provide security measures and avoid sniffing of the data, VPN providers are entrusted to maintain circuit integrity. This type of VPN is called a trusted VPN. The technologies used for implementing trusted VPNs over an Internet Protocol network are: Asynchronous Transfer Mode (ATM) circuits, frame relay circuits and MLPS.

ATM and frame relay operates at layer 2 of the OSI model and MLPS operates in between the data link layer and network layer. The requirements for a trusted VPN are:

- Any changes in the path of a VPN can be made only by a trusted VPN.

- All routing and addressing methods need to be described before creating a trusted VPN.

- Only a VPN provider can inject, change, or delete the data in the path of a VPN.

Secure VPN

The main goal behind implementing a secure VPN is to ensure complete security of the data in transit. In a secure VPN, all the data packets sent through the tunnel undergoes an encryption process at one end of the tunnel and decryption process at the other end of the tunnel. This prevents any attempt from the attacker to achieve data in transit. The main requirements for secure VPNs are:

- All the data packets in the traffic are encrypted and authenticated prior to sending to the client.

- The client and server need to be in a mutual understanding before initiating the connection between each other.

- Confirm the security of the connection from unauthorized users.

Hybrid VPN

Hybrid VPNs are those with trusted VPNs as part of the secure VPNs. They implement different network components of an organization at the same time in order to confirm security at very low costs. A network administrator takes extra time in differentiating between the data transfer among the secured VPNs that are part of the trusted VPNs. The main requirements for hybrid VPNs are:

- There should be a clear differentiation between the trusted VPN and the secure VPN.
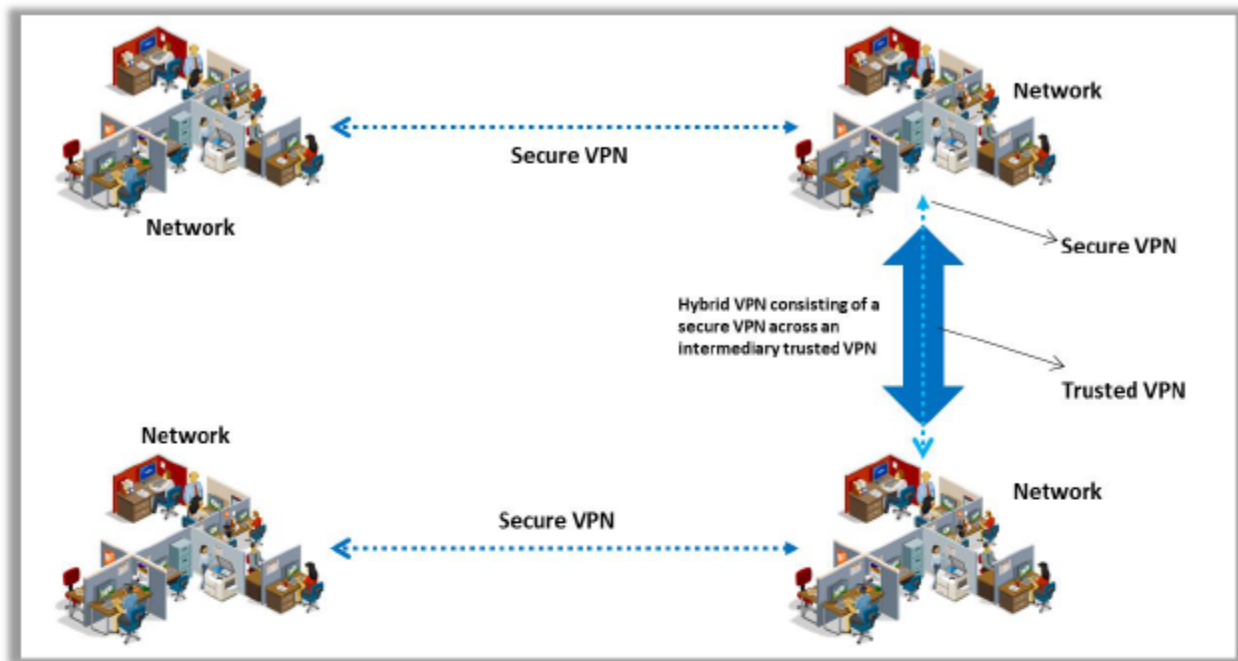
FIGURE 9.3: Hybrid VPN

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

Point-to-Point VPN Topology

1 2 3 4

Full Mesh VPN Topology

Star Topology

A VPN topology mainly deals with the specifications of how nodes in a network are connected and how they communicate with the other nodes. A VPN enables companies in a different network to communicate with each other and allows data sharing. VPN topologies enable the organization to design the way they can communicate with other networks. The different VPN topologies are:

- Hub-and-Spoke
- Point-to-Point
- Full Mesh
- Star

It is important to note that the selection of topologies depends on the requirements of the organization. For example, a Star topology is best suited in environments where the company needs to share information with another company located in a different network. A Mesh topology is best suited for an intranet.

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

- Remote offices **exchange** numerous amounts of data

- This topology is commonly used in organizations with **strict hierarchical** structures (banks, governments, retail stores, international organizations, etc.)

In hub-and-spoke technology, the main organization is considered the hub and its remote offices are considered the spokes. The spokes access the VPN through the hub. This topology is mainly used in banking and international organizations. The hub controls two types of communication:

- Communication between a spoke and a hub

- Communication between the spokes

This topology is used to represent an intranet VPN connecting an organization's main office to its regional offices. The hubs facilitate the sharing of numerous amounts of data. There are separate tunnels for data transfer between the hub and the spoke. All the data transfers happen through the hub. The hub-and–spoke topology can become a multilevel topology depending on the growth of the network.

In a multi-site network, the central hub controls the data transfer or is considered as the gateway for the remote sites to communicate with each other. For example, a cell phone tower in an area is the hub and all the mobile devices in and around the cell phone tower are the spokes. The network administrators need to always maintain a thorough study of the hub-and-spoke technology in their network.

Advantages

- Less expensive and easy to repair when one of the spokes doesn't work.

- Bonded circuits in between the hub and the spoke increase the flexibility of the network.

- Offers better security as each device in the network is separated from the other through one single connection to the hub.

- These provide high performance, centralization, and simplicity.

Disadvantages

- Any issue in the hub can affect the connection between the hub and spoke and the connection between the different spokes.
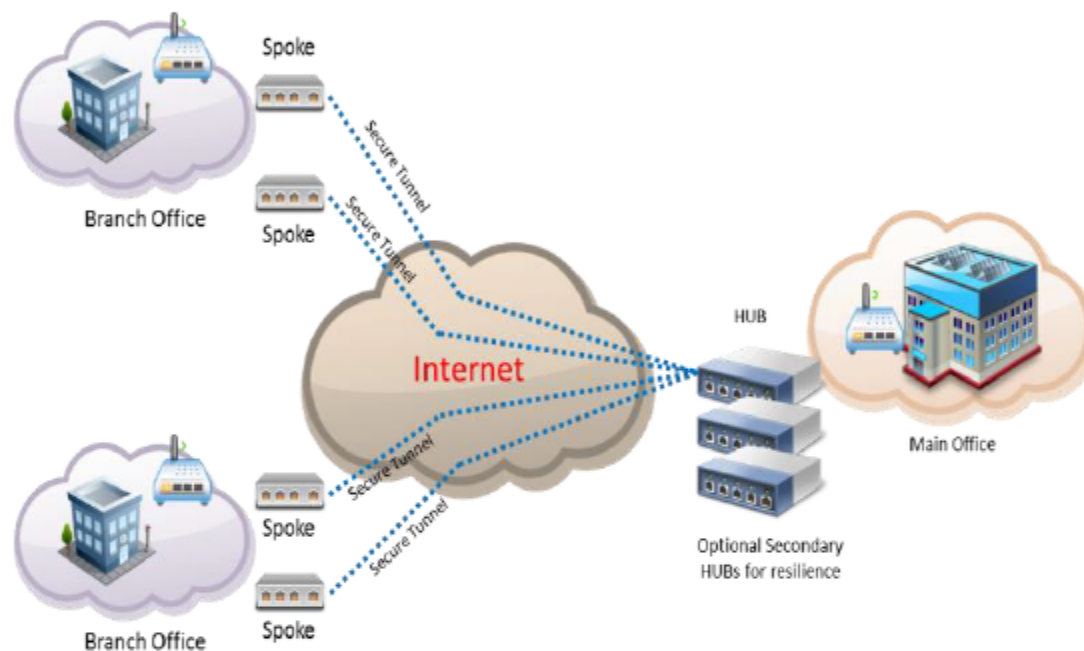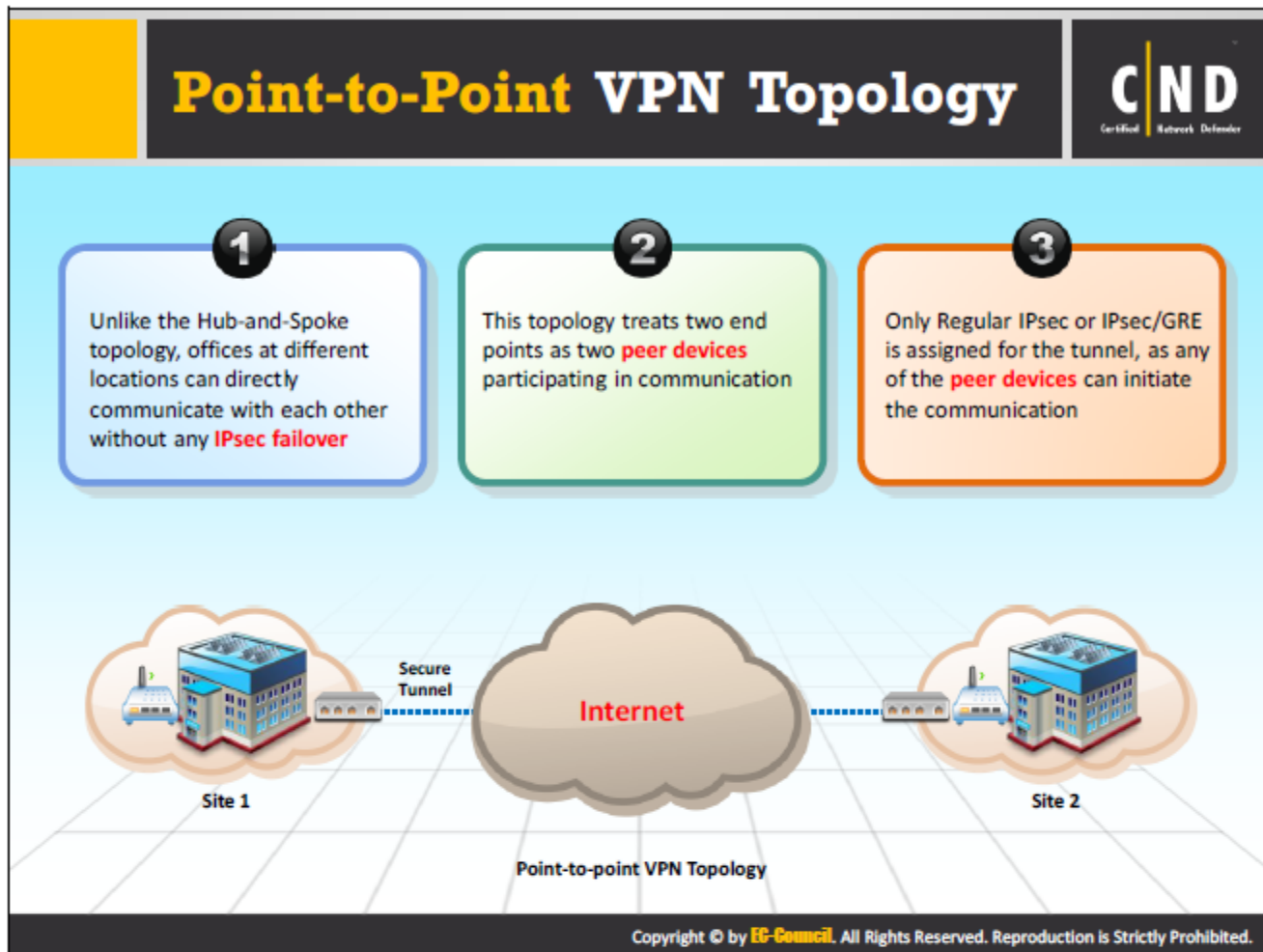

FIGURE 9.4: Hub and Spoke VPN topology

The figure clearly explains the process of the hub-and-spoke topology. In the figure, each spoke at the branch offices makes a secured connection with the hub at the main office. These secured connections are made across the Internet. The main office can have more than one hub at a time, only one hub is used to connect to each spoke. The other hubs are kept as backup hubs for flexibility.

This topology works well, if the traffic is between the hub and spoke rather than between the spokes or the remote sites. This is because, traffic between two spokes needs to go through the hub first and then forwarded to the respective spoke. This increases the chance of a bottleneck at the hub due to more spoke-to-spoke connections. All IPsec technologies can be used in this topology.

If the hub faces any issue in the connection, IPsec failover transfers the connection to a backup hub, used by all spokes. It is possible to configure multiple hubs as a main hub.

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

Site 1 — Secure Tunnel — Internet — Site 2

Point-to-point VPN Topology

In a point-to-point topology, any two end points are considered as peer devices which can communicate with each other. Any of the devices can be used to initiate the connection. The IPsec technology assigned can be either IPsec or IPsec/GRE.

Commonly configured as a regular IPsec point-to-point VPN also known as an extranet. This is where a connection is established between a device in a regularly managed network and an unmanaged device in the service provider's network.
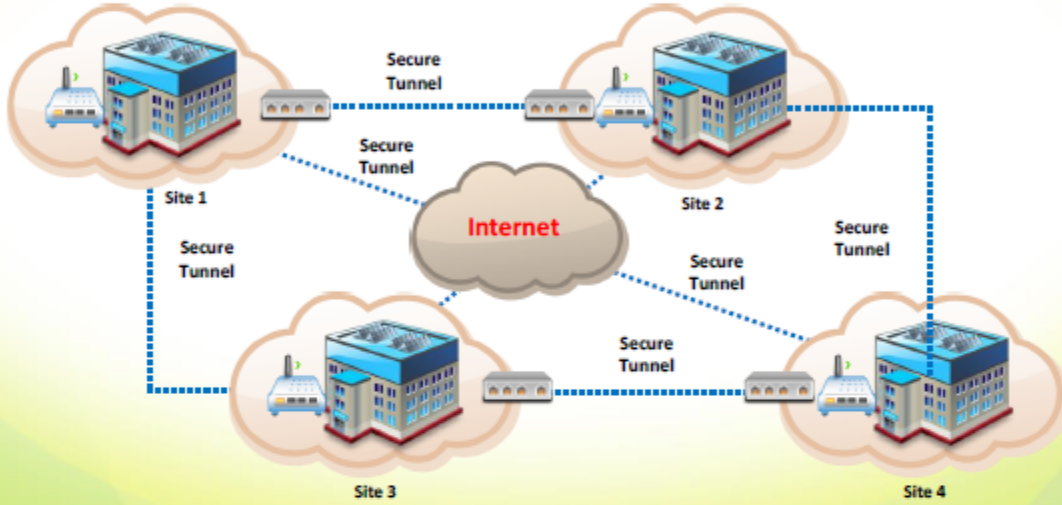
The major features of point-to-point topology are as follows:

- Easy routing of data as it needs to pass through only one router.

- Optimal routing between the customer sites.

- Introduces encryption and authentication to confirm the integrity of packets in transit.

- Uses a tunneling process in order to capture data packets with normal IP packets for forwarding over IP-based networks.

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**

In a fully meshed VPN network, all peers can communicate with each other, making it a complex network. This topology allows all the devices in a network to communicate directly with each other through an IPsec channel. This reduces the chance of any holdup at the gateway and reduces the overhead of encryption and decryption of the device. A fully meshed VPN can implement normal IPsec, IPsec/GRE and GET VPN technologies.

Advantages

- Any failure on one of the devices does not affect the entire network.
- Very reliable.
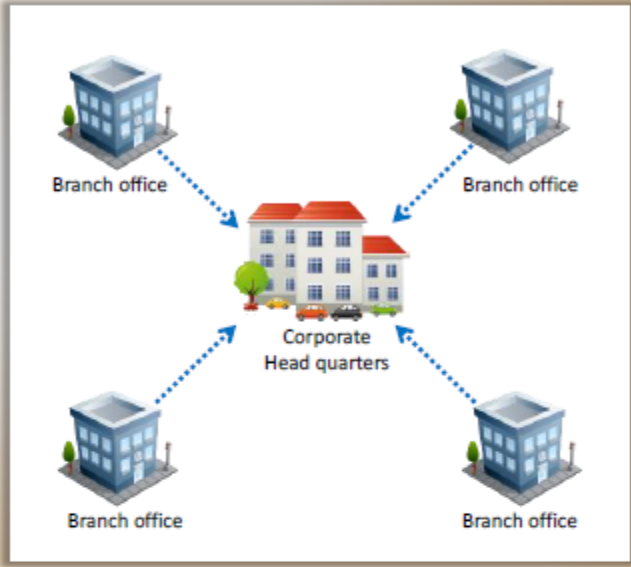- Prevents any sort of block at the gateway.

Disadvantages

- Increases the number of devices connected to the network making it difficult to manage.
- Possible chances of redundancy in network connections.

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

This is the most commonly used topology in almost all organizations. Here, all the remote offices communicate with the corporate office but at the same time deny communication between the remote offices. Each device on the network is connected to a central hub that manages the traffic through the network.
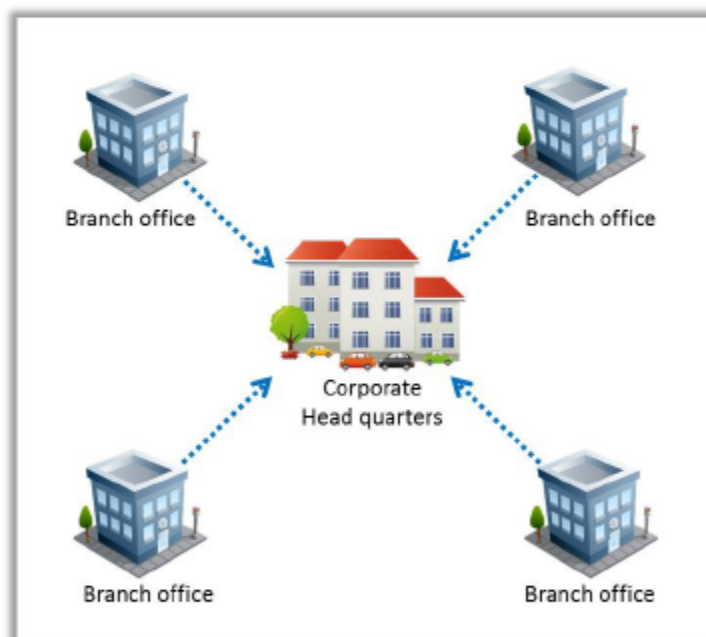

FIGURE 9.5: Star topology

In the figure, all the branch offices can communicate with each other through the corporate headquarters. But in this topology, no two branch offices can initiate a separate communication as these are allowed only through the corporate network.

Advantages

- Most suitable for a financial infrastructure as the compromise on one system does not compromise another branch without detection.

- Any attack on the branch offices can be performed through the main branch. Any manipulation in the network can be easily detected by the network administrator.

- Easy to add and remove new branch offices to the main office without affecting the neighboring sites. But, it is mandatory to update the main site regarding the new addition or removal of the sites.

Disadvantages

- Any failure in the central site affects the communication of all other sites.

- No two sites can communicate with each other directly.

- Adding more sites to the network can actually affect the capacity of the main site.

VPN Concerns: VPN Fingerprinting

CND
Certified | Network Defender

→ An attacker can use **UDP backoff** fingerprinting or Vendor ID fingerprinting for VPN server fingerprinting

→ This gives a potential attacker useful information

→ A VPN server may expose sensitive information such as type of device, **software version** details, etc. during VPN fingerprinting

→ **Ike-scan** is used to fingerprint the VPN server vendor and the version number of the IPsec VPNs

→ The Ike-scan uses its own **retransmission strategy** to deal with lost packets in order to fingerprint the VPN server

A VPN transmits data using various protocols such as TCP, IP, UDPC, IPsec, etc. Among these UDP is not a reliable transport layer protocol and completely depends on the application to provide the reliability. The main technique UDP uses for reliability is retransmission with backoff which allows the application to replace any lost packets.

Because of certain vulnerabilities in transmission protocols, several VPN servers are prone to fingerprinting. For example, UDP needs backoff and with this, the attacker could fingerprint the VPN or Vendor ID.

The VPN fingerprinting technique allows the attacker to access useful information such as the type of connections implemented, devices used and operating systems deployed. Some systems, such as Cisco PIX or Nortel Contivity, potentially reveal crucial data like the general type of devices deployed for building the network, while other systems display the software version details.

Attackers also trace out the IKE (Internet Key Exchange) scan to fingerprint the VPN server vendor and the version number of IPsec VPNs. The IKE-scan uses its own retransmission strategy to deal with lost packets and this helps attackers to fingerprint the VPN server. The IKE-scan log can find similar patterns to determine which IKE implementation a specific host has deployed.

VPN Concerns: Insecure Storage of Authentication Credentials

- VPN clients may store VPN authentication credentials in insecure places, where attackers can get easy access to these credentials
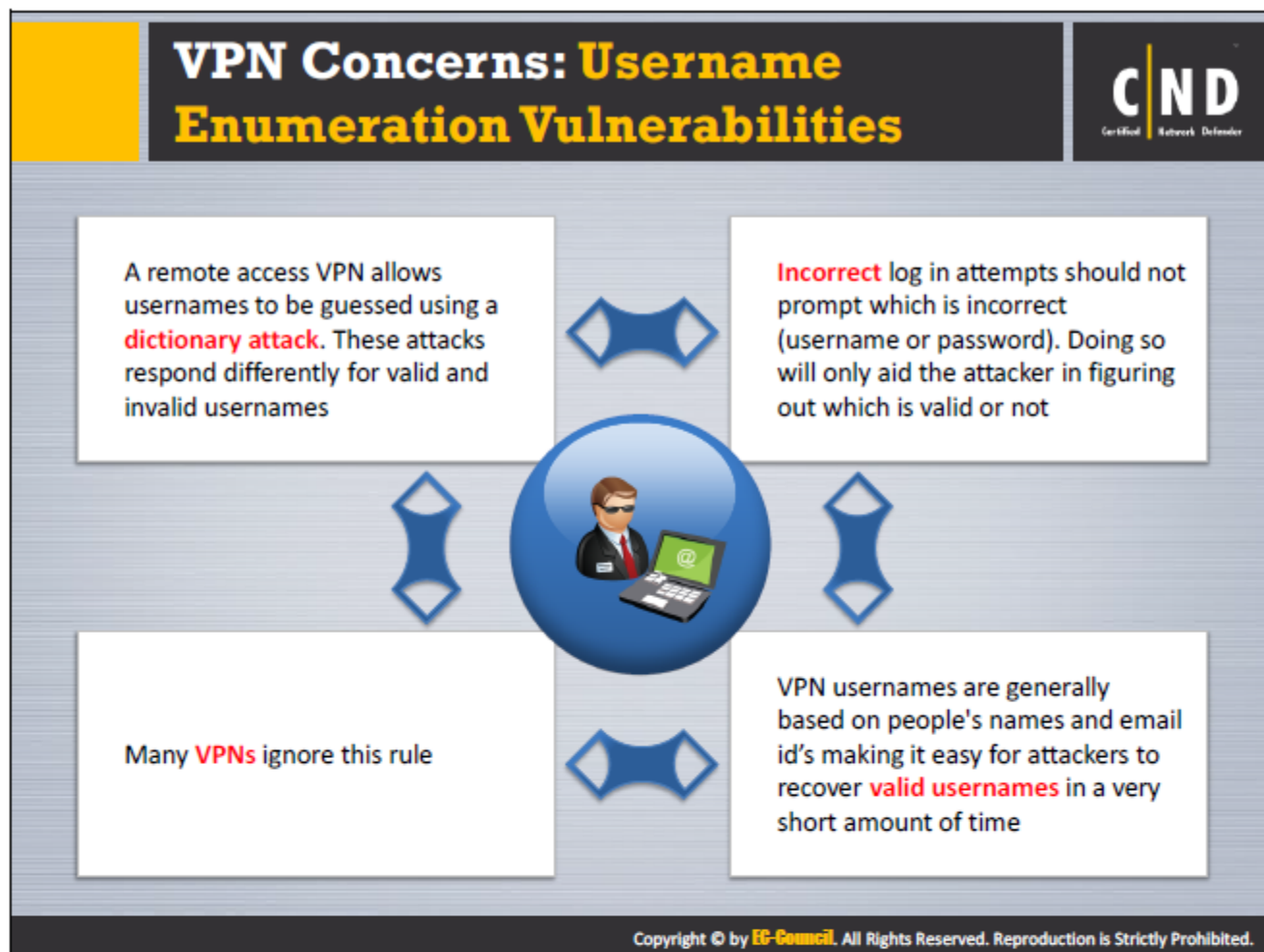- This makes it easier for an attacker to steal the credentials, increasing the security risk

Credentials can be at risk of being stolen, when a VPN client:

I Stores the Username Unencrypted in a File or the Registry	**III** Stores the Plain-Text Password in Memory
II Stores the Password in a Scrambled Form	**IV** Uses Weak Registry or File Permissions for Stored Credentials

There are certain security issues if the credentials are not stored and protected appropriately. These security issues are due to an insecure method of storing the authentication credentials by VPN clients. Common VPN issues with authentication and credentials:

- **Storing the username unencrypted in a file or a registry:** Attackers can easily perform an offline attack on the authentication process, if the credentials are stored in an encrypted format. This is possible if and only if the VPN is using the IKE aggressive mode.

- **Storing the password in a scrambled form**: If an attacker succeeds in gaining access to the client computer, they can easily gain the password. Even though the password is in a scrambled form, there is no key required to decrypt it. This provides for the attacker to implement a decryption algorithm to crack the VPN encryption.

- **Storing the plain-text in memory**: Passwords stored in plain-text are always susceptible to attack. Any user with access to the client machine can initiate the VPN client to dump the process memory using a tool known as pmdump. This tool will get access to the credentials.

- **Weak registry or file permissions for stored credentials**: Passwords are easy to get if they are not stored in a secure location and assigned with strict permissions.

VPN Concerns: Username Enumeration Vulnerabilities

A remote access VPN allows usernames to be guessed using a **dictionary attack**. These attacks respond differently for valid and invalid usernames

Incorrect log in attempts should not prompt which is incorrect (username or password). Doing so will only aid the attacker in figuring out which is valid or not

Many **VPNs** ignore this rule

VPN usernames are generally based on people's names and email id's making it easy for attackers to recover **valid usernames** in a very short amount of time

Many remote-access VPN use the IKE aggressive mode with a pre-shared key authentication method. The client sends an IKE packet to the VPN server which responds using another IKE packet. These packets contain several payloads, including the identity payload sent by the client and hash payload sent by the server. The identity payload contains the username and the hash payload contains the password. Certain flaws identified in the flow of packets are as follows:

- Few VPN servers only respond to valid usernames.

- Few VPN servers respond with an error to incorrect usernames.

- Few VPN servers respond to valid and invalid usernames. The hash payload process uses invalid usernames with null passwords.

In all the above instances, the attacker confirms the difference between the valid and invalid username from their computational differences. An attacker guesses the correct password using the IKE aggressive mode can easily uncover the hash from the VPN server. This hash can be used with a brute-force-attack in order to gain the password.

Identifying all the possible types of attacks which can occur on the login page, account registration and password changes will help prevent username enumeration vulnerabilities.

VPN Concerns: Offline Password Cracking

VPN passwords are **prone** to offline password cracking attempts

An attacker can perform an **offline** dictionary attack to crack the password of a VPN client

Offline password cracking activities are neither **logged** in the VPN server log or **triggers** an account lockout

Offline password cracking is one of the most common flaws of a VPN. An attacker can perform an offline password crack by gaining access to the password hashes. Once the attacker gets the user credentials, they can easily gain the hash access from the VPN server.

When the VPN server gives a response to the client, it consists of the contents like key exchange, identity, header, and hash. The server responding with the hash query from the client is called a hash responder. Since the responses are not in an encrypted form, an attacker gets the access to the hash responder and uses a pre-shared key to perform the attack. The attack is offline and as a result the VPN log server does not create any log entry. The attack goes unnoticed by the administrator.

Simple passwords and using simple words have increased the frequency of passwords being cracked. To prevent password cracking in the network, implement hash functions like MD5 and SHA.

VPN Concerns: Man-in-the-Middle Attacks

CND
Certified Network Defender

This attack is possible when the VPN system uses an insecure authentication protocol like IKE

Malicious attacker intercepts communication between the client and the VPN server, obtaining the client authentication to the server and using the credentials to authentication to the VPN server

This will breach the security of the VPN server

Attackers may use insecure authentication protocols such as IKE to perform Man-in-the–Middle attacks on a VPN. An attacker intercepts the communication in between the client and the server and obtains the client authentication to the server. The attacker then utilizes these authentication credentials to login and access the VPN server, allowing for complete control over the VPN Server.

Man-in-the-Middle attacks occur during data transfer through the VPN and allows an attacker to intercept, insert, delete, and modify messages, reflect messages back to the sender, replay old messages and redirect messages.

VPN Concerns: Lack of Account Lockout

CND
Certified | Network Defender

Some VPN Client implementations do not permit **locking** a user's account after a set number of incorrect login attempts ①

This allows an attacker to make multiple login attempts through **brute force guessing** ②

Check if your **VPN client** supports account lockout and ensure it is turned on in the configuration ③

The main aim of using the account lockout feature is to restrict the number of login attempts to a certain limit and if anyone goes on trying login beyond the limit, the account will automatically get locked out. This feature prevents you from password cracking attacks such as brute force, dictionary attacks etc. However, there are a few VPNs that do not provide an account lockout feature and this enables users to perform login attempts repeatedly. Attackers can take advantage of the lack of an account lockout feature to gain account credentials and it reduces the security of the account details.

VPN Concerns: Poor Default Configurations

A major security threat to a VPN is the selection of a **weak authentication** mechanism, typically IKE aggressive mode with a pre-shared key by default

Ensure you use a **certificate** based authentication mechanism

Even if the default security mode is certificate based and very strong, certain **default configurations** will allow an end user to switch to a less secure method

All authentication and encryption modes should be made **unavailable** except only the strongest

Almost all organizations have an automated configuration set-up. However, if the organization remains with the default configuration for the VPN, attackers may exploit these default configurations to compromise the security of the VPN. The organization can go for a better and secure configuration management solution.

There are certain default configurations that allow an end user to switch to a less secure method like IKE, even in the presence of stronger certificates. It is mandatory to restrict all weak authentication and encryption modes. Normally, the end user does not attempt to change the default configurations of the system thinking the vendors provided the correct and secure configuration for the system. The default configurations support many ciphers and modes, ESP and AH. These may include both strong and weak ciphers. An attacker with access to the client machine can prompt the end user to use the weaker cipher which will make things easier for them. The end user may not notice the cipher and configuration was changed because the VPN still functions normally.

The selection of weak authentication mechanisms such as IKE aggressive mode with a pre-shred key allows attackers to gain authentication credentials. It must be ensured that mechanisms selected for protecting VPNs have a certificate based authentication mechanism enabled.

Common default configuration flaws

VPN vendors usually provide a default password, which users fail to change. The default passwords are known and it makes it easy for attackers to enter the network and get access to the systems.

- Users may change the configuration setting of the VPN without prior knowledge of the setting.

VPN Concerns: Poor Guidance and Documentation

- A VPN implementation does not provide any important directions and/or documentation for which configuration is best to use

Situations where this guidance is required:

Choosing an appropriate **encryption algorithm** to prevent weak ciphers being cracked

Choosing an appropriate **authentication key mechanism** to prevent offline password cracking

Choosing an appropriate **protocol** for secure and encrypted communication to prevent MITM attacks

There are instances where the end user is not aware of the correct configuration for the VPN. Improper guidance and documentation regarding the VPN implementation can lead the customers making mistakes while using a VPN. Poor guidance can lead to security vulnerabilities in the configuration and implementation of a VPN. An incorrect implementation provides a way for attackers to gain access to the VPN. The following are situations where this guidance is required:

- Using weak ciphers like export-grade or single DES which can be cracked easily.

- While using the weak key authentication such as pre-shared key with IKE aggressive mode, which sends the username and vulnerable offline password to crack if a valid username is identified.

- Choosing AH protocol which does not encrypt VPN traffic.

Users are not provided any warning message when the implementation is incorrect. Making it very difficult for the user to know the risks and dangers associated with the improper configuration.
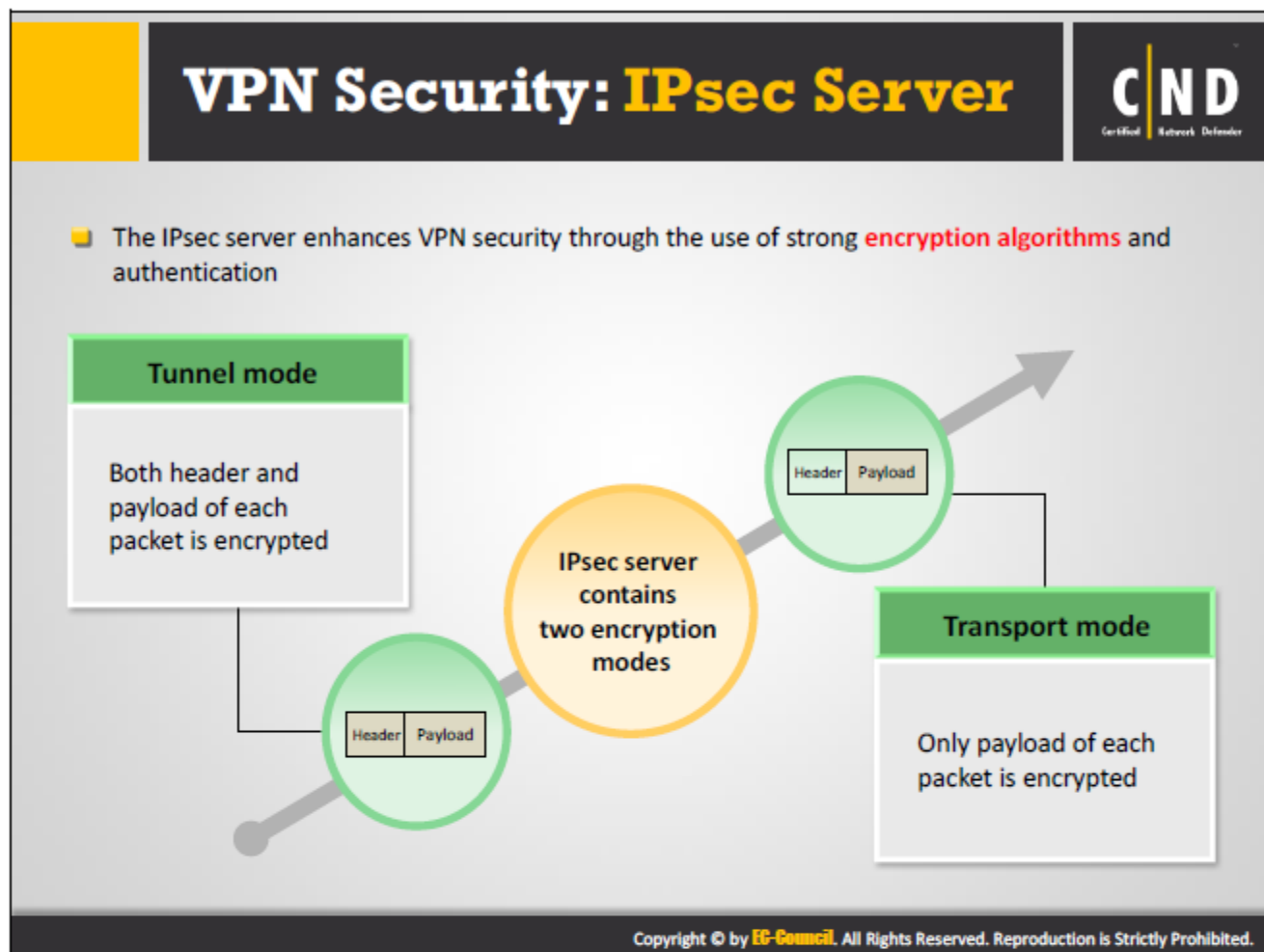
VPN Security: Firewalls

- 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
- Firewalls are also used to terminate VPN sessions

LAN PCs
Wireless terminals

Firewall

Branch Server

IPSEC TUNNEL or WAN

Internet

www.sports.com

Corporate Network

A firewall can allow or deny the flow of data through the network. These generally help in protecting the network from attackers. Firewalls can be used in two ways with a VPN:

- The VPN server is attached to the Internet and the firewall is located between the VPN server and intranet.

  - Here, packet filters are added in order to allow only VPN traffic to and from the IP address of the VPN server.

- Firewall is attached to the Internet and the VPN server is located between the firewall and intranet.

  - Here, the firewall has input and output filters on the Internet interface in order to maintain traffic and passage of traffic to the VPN server.

VPN Security: 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

IPsec server contains two encryption modes

Transport mode

Only payload of each packet is encrypted

The IPsec server consists of two types of encryption modes:
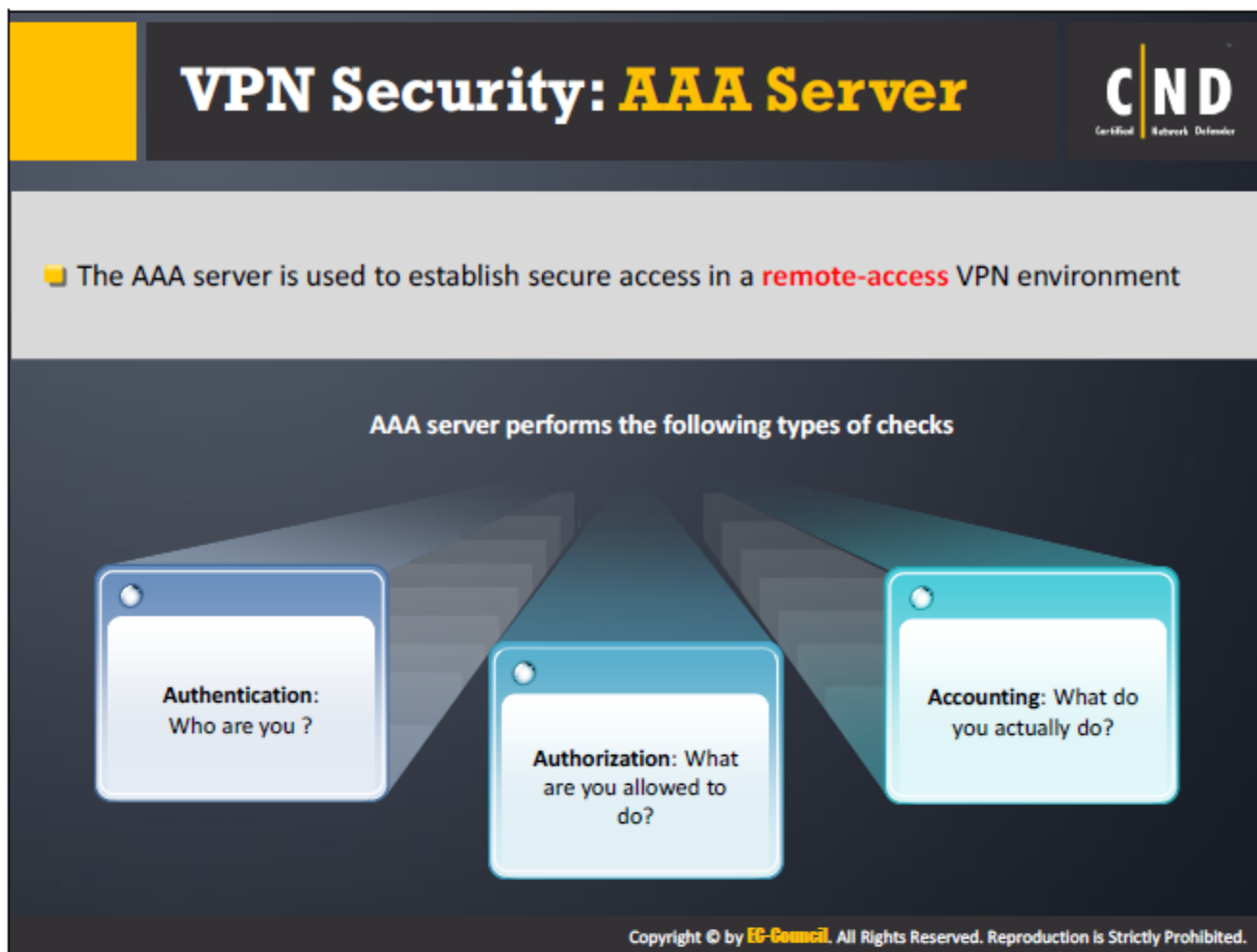
Transport mode

This is the default mode for an IPsec server. These are generally used for end-to-end communication between a server and a client. In transport mode, IPsec encrypts the IP payload through an Authentication header (AH) or Encapsulating Security Payload (ESP) header. The IP payloads can be TCP segments (containing TCP header and TCP segment data), UDP message (containing a UDP header and a message data) and ICMP messages (containing ICMP header and ICMP message data).

AH does not generally encrypt the data an only provides authentication, integrity and anti-replay protection. In an AH, it is possible to read the data but it denies all kinds of changes on the data.

Tunnel mode

In tunnel mode, IPsec encrypts both the IP payload and the header to protect an entire IP packet by encapsulating it with an AH or ESP header and an additional IP header. This mode is useful for protecting traffic between different networks and is primarily used for interoperability with gateways.

Tunnel mode of IPsec is generally implemented in configurations such as gateway-to-gateway, server-to-gateway and server-to-server. The IPsec tunnel mode is useful in protecting traffic while it is passing through untrusted networks.

VPN Security: 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?

Authentication, Authorization and Accounting (AAA) provides additional secure access in a remote-access environment. An AAA server provides users an extra layer of protection and control when compared to an ACL alone. The access control list (ACL) enables outside users to access TELNET present in the DMZ network. AAA gives permits to only a few users for accessing the application after proper authorization and authentication has occurred. This can be implemented using:

- Who you are (authentication) by verifying the user credentials such as username and password

- What you are allowed to do (authorization) is verified in order to offer access controls such as management commands, network access and VPN access

- What do you actually do (accounting), refers to what type of traffic the users access through the VPN. This option tracks traffic that passes through the VPN and records all user activity

The authentication protocols used for an AAA server are:

- RADIUS
- TACACS+
- RSA SecurID
- Windows NT
- Kerberos
- LDAP

VPN Security – Radius

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

VPN Security – Radius (Cont'd)

Internet

VPN Gateway

VPN Client

DualSheild Radius Server

DualSheild Authentication Server

Corporate Network

Active Directory

RADIUS is a client/server protocol which authenticates and authorizes dial-in-users to access the system or device. RADIUS maintains profiles in their databases enabling the remote servers to share the data enabling a centralized administration of data. Companies using a VPN network implements RADIUS for data authentication.

In RADIUS, the VPN server interacts with the RADIUS server once the user attempts a connection. The RADIUS server authenticates the user using their credentials. The user is granted access if and only if the user provides the correct credentials and has dial-in access. The RADIUS server sends a RADIUS message to the RADIUS client in response to the request for authentication.

The RADIUS messages are sent as user datagram protocol (UDP) messages and the UDP payload of a RADIUS packet can include only one RADIUS message.

Various RADIUS message types are:

- Access-request: Sent by the RADIUS client to request authentication.

- Access-accept: Sent by the RADIUS server in response to the access-request message.

- Access-reject: Sent by access-server to the RADIUS client informing them the connection request is rejected.

- Access-challenge: Sent by the RADIUS server to the RADIUS client in response to the access-request from the client.

- Accounting–request: Sent by the RADIUS client to request the information for a permitted connection.

- Accounting–response: Sent by the RADIUS server in response to the accounting-request message from the RADIUS client.
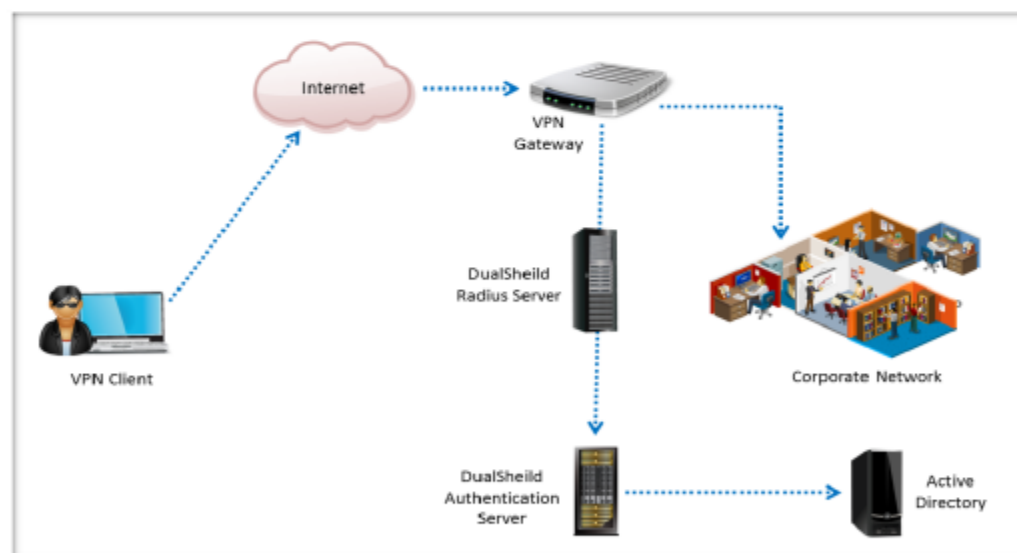

FIGURE 9.6: RADIUS

A RADIUS message consists of a RADIUS header and RADIUS attributes. The RADIUS attributes provide information regarding the number of connection attempts, username, password, service requested by the user, etc. Each has a separate RADIUS attribute and they share information between RADIUS servers, RADIUS clients and RADIUS proxies.

The RADIUS components are:

- Access clients

- Access servers

- RADIUS proxies

- RADIUS servers

- User account databases

Improving VPN Speed

Factors that could influence Internet speed while using a VPN service and the techniques to improve the speed of a VPN are:

VPN Server Location	Configure the VPN server located in your area to **avoid** the losing the Internet connection
VPN Server Load	VPN servers with many connected users tend to cause **delay** and **loss** in Internet speed. Use a paid VPN service as they have plenty of free space to accommodate new subscribers
Reliable provider	Select a **dependable** VPN provider which has a very low packet data loss. Ensure the loss is at a minimum
Configure Firewall Settings to Optimize VPN Speed	Set up and configure the correct **firewall** on the system to allow the VPN service to flow smoothly
Processor Speed	Make sure your computers have fast CPU's, this will provide better system speed, capacity and a stable Internet connection
Security Protocol Type	Use L2TP/IPsec and PPTP VPN protocols since they use **128-bit encryption**
Choose a Stable ISP	The better the Internet connection, the **faster** the VPN service

Many people using a VPN connection are concerned about the speed of the VPN affecting their internet connection. Factors influencing VPN speeds are:

VPN Server Location

A VPN server at distance would take lots of time for the data packet to move back and forth through, use a VPN Server located near your area to avoid any loss of Internet bandwidth. This will help in improving the VPN speed.

VPN Server Load

A VPN server with many connections causes a delay and loss. To avoid this, use a paid VPN service since they have plenty of free space to accommodate new subscribers.

Reliable Provider

A good and reliable VPN provider offers a zero percent data packet loss for their VPN services. For better performance select a dependable virtual private network provider which has a minimum amount of packet data loss.

Configure Firewall Settings to Optimize VPN Speed

Generally, system firewall settings affect the CPU speed and that affects the VPN and Internet speed. To increase the VPN speed, set up the correct firewall on the system to allow the VPN service to flow smoothly.

Processor Speed

In order to avoid losses in bandwidth and connection, furnish your computer with a faster and better CPU or processor to have better system speed, capacity, and a stable internet connection.

Security Protocol Type

The VPN speed depends upon the level of security encryption. A VPN solution provider offers basic VPN security protocols like OpenVPN, SSTP, L2TP/IPsec and PPTP. To get a good and a stable Internet connection, opt for L2TP/IPsec and PPTP VPN protocols as they use 128-bit encryption.

Choose a Stable ISP

The speed of an Internet connection depends on the ISP limitation, which in turn influences the speed of the connection for the VPN subscription. The higher the Internet connection limit, the faster is VPN service.

Choose a Wired Connection

Wired connections increase the speed and minimizes the latency. Wireless connections use a shared connection between the devices affecting the speed of the VPN.

Choose a Proper Device

Certain devices are incapable of handling overhead due to the encryption of a VPN tunnel. These devices are best used with a better processor.

Quality of Service (QoS) in VPNs

- The Quality of Service (QoS) in VPNs acts as a **resource reservation control** mechanism for a VPN
- It offers better management and use of network resources

QoS manages network features like :

Bandwidth: Denotes data transfer rate

Delay: Denotes time required to send data from the source to the destination

Jitter: Denotes variation in delay

Packet loss: Denotes network packets loss/drop due to a large amount of traffic

The two VPN models providing QoS:

Pipe Model: QoS guarantees the traffic from one Customer Edge (CE) to another

Hose Model: A customer's CE router sends to and receives from other CE routers on the same VPN

Quality of Service in VPNs is an end-to-end mechanism that provides different services to different applications, users or data flows according to business requirements. Service providers provide a quality service by defining the service level agreement (SLA) which further describes the QoS factors. QoS is required in a VPN as different applications have different requirements and it is mandatory to provide all required services so the VPN functions properly. Factors that affect the QoS:

- **Bandwidth**: Determines the data limit applicable during a data transmission

- **Delay**: Total time required to transmit data from the source location to the destination

- **Jitter**: Variation in latencies for packets in a given data stream

- **Packet loss**: Loss or ID ordering of data packets in a stream

- **Throughput:** Number of bytes received per second at the destination

- **Network Address Translation (NAT)**: The presence of Network Address Translation (NAT) or proxy devices between the client and the gateway can affect the connectivity in an undesirable manner. The connectivity always needs a client configuration prior to the implementation of the tunnel.

- **Goodput (Packets)**: The ratio on the number of data packets sent versus the total number of packets transmitted in the network.

- **Goodput (Bytes)**: The ratio of bytes of data sent versus the total number of bytes transmitted in the network.

- **Data Dropped**: Data lost or dropped at the destination may be due to improper access to the medium.

A SSL (Secure Socket Layer) VPN is used to provide remote user with access to web applications, client/server applications, and internal network connections. It provides a secure way for mobile users to access network resources. Deployment considerations of SSL VPNs include:

SSL VPN is categorized into:

- **SSL portal VPN**: Allows secure access of network devices by enabling a single SSL connection to a web site. Portal refers to the website that permits the user to access other services.

- **SSL tunnel VPN**: Enables web browsers to access multiple network services, applications and protocols. This is facilitated by a tunnel under the SSL. The SSL tunnel allows a web browser to access services that cannot be accessed by SSL portals.

SLAs for a VPN

- A SLA is an **agreement** between an ISP and their subscribers. Can also be between peer ISPs. SLAs specify the service criteria (traffic profile, network behavior and payment/billing)
- Specifies the **penalties** a service provider will pay if they fail to meet the committed goals

Challenges and issues providers and subscribers can face due to a SLA:

- The challenge for subscribers is to use service management tools to confirm the provider is meeting all the criteria of the SLA

- If a subscriber uses one SLA to bind more than one provider, especially if the VPN uses multiple providers, the SLA must address the provider interconnection and end-to-end service performance

- The challenge for the provider is to honor multiple SLAs from many service providers

A service level agreement (SLA) is a contract between the ISP, its subscribers and between any peer ISP's. The SLA specifies traffic profile, network behavior, payment/billing etc., and the penalties given for not following or meeting the prescribed criteria. The SLA can be fixed through a phone call, fax or using bandwidth brokers (BBs). Bandwidth brokers are agents allocating resources and controlling traffic of the administrative domain. These brokers keep a mutual agreement between each of the neighboring domains. The SLA can be either static or dynamic. Static agreements are defined with the initialization of the service and changes frequently. These agreements are negotiated by human interaction whereas negotiating dynamic agreements require an automated protocol between the BBs.

Providers and subscribers face certain challenges and technical issues using SLAs:

- The challenge for subscribers is to devise and operate service measurement tools showing an indication of what extent the SLA is honored by the provider.

- When subscribers use a SLA to bind more than one provider, when the subscriber's VPN spans multiple provider domains, the SLA must also encompass provider interconnection and the end-to-end service performance.

- The challenge for the provider is to honor multiple SLAs from many service providers.

VPN Service Providers

A VPN service provides a level of security to hide your IP address, geographic location, and protecting your data while online

✓ **Private Internet Access**
https://www.privateinternetaccess.com

✓ **TunnelBear**
https://www.tunnelbear.com

✓ **TorGuard**
https://torguard.net

✓ **PrivateTunnel**
https://www.privatetunnel.com

✓ **IPVanish VPN**
https://www.ipvanish.com

✓ **VPNReactor**
http://www.vpnreactor.com

✓ **CyberGhost VPN**
http://www.cyberghostvpn.com/en_us

✓ **proXPN's VPN**
https://proxpn.com

✓ **Hotspot Shield VPN**
http://www.hotspotshield.com

✓ **VyprVPN**
http://www.goldenfrog.com/vyprvpn

Some of the VPN service providers are listed below:

Private Internet Access

https://www.privateinternetaccess.com

The service provider offers services to protect your privacy, identity and to Unblock Censorship Filters i.e. unrestricted access even when the user is in another country.

TorGuard

https://torguard.net

TorGuard VPN is a privacy tool that transforms the blocked traffic as HTTPS traffic to overcome censorship anywhere in the world.

IPVanish VPN

https://www.ipvanish.com

IPVanish VPN offers features such as:

- It provides faster and more stable speeds.
- It protects from cyber threats and unsecured Wi-Fi hotspots.

CyberGhost VPN

http://www.cyberghostvpn.com

CyberGhost VPN offers features such as:

- Simple & secure access to content from all over the world

- Unblocks the content

- Protect users from hackers, cyber scams, bank-account theft and phishing e-mail fraud

Hotspot Shield VPN

http://www.hotspotshield.com

Some of the benefits of Using Hotspot Shield VPN are listed below:

- Protects privacy

- Bypass VPN Internet censorship

- Secures the Internet

- Enables Wi-Fi security

- Protects devices from malware

TunnelBear

https://www.tunnelbear.com

Some of the features of TunnelBear:

- Secures user data and hides IP addresses.

- Provides access to censored content.

- Blocks online web-site tracking.

PrivateTunnel

https://www.privatetunnel.com

- Secures user communications

- Protects user privacy.

- Stops malware and malicious attacks.

- Allow access to the content from anywhere.

VPNReactor

http://www.vpnreactor.com

VPNReactor maps off the ISP assigned IP address with a mysterious IP. It provides encrypted untraceable connections between the network and the Internet. It works on all platforms such as Windows, Mac OSX, IPhone.

proXPN's VPN

https://proxpn.com

Some of the benefits of proXPN:

- Unlimited VPN speed

- Access to favorite sites anywhere

- Open all available ports

- Provides PPTP connectivity

- Support for mobile devices

VyprVPN

http://www.goldenfrog.com

- NAT firewall for additional security.

- When the user connects to VyprVPN, user ISP encounters only encrypted traffic. The result is faster, unrestricted Internet speeds.

- Multiple Protocols such as L2TP, PPTP for Encryption.

Auditing and Testing the VPN

After a VPN is installed, the VPN client must be tested on every computer, using a VPN step-by-step scenario

Remote user is **issued** VPN client software and certificate

If IPsec is used, verify the IPsec policies on the remote user's machine and the **VPN gateway** are identical

If problems arise when connecting to the gateway, instruct the user to write down or report all error messages, to correctly **diagnose** the problem

01 | 02 | 03 | 04 | 05 | 06

Guide the user in installing the **software** and storing the certificate

Have the user start the VPN software and **connect** to the gateway

When the connection is established, the remote user should **authenticate** by entering the username and password when prompted

VPN testing can provide the administrator with an idea on the weaknesses in the implementation. The auditing of a VPN mainly concentrates on the standards, guidelines and procedures. VPN audits depend on other types of security audits such as a configuration audit, network security audit, server security audit etc.

After a VPN is installed, the VPN client must be tested on each computer using a VPN step-by-step scenario:

- Remote user is issued the VPN client software and certificate.

- Guide the user to install the software and store the certificate successfully.

- If IPsec is being used, verify the IPsec policies on the remote user's machine and the VPN gateway are identical.

- Have the user start the VPN software and connect to the gateway.

- If problems arise while connecting to the gateway, ask the user to write down or report all error messages to correctly diagnose the problem.

- Once the connection is established, the remote user should authenticate entering their username and password when prompted.

Testing VPN File Transfer

After testing the client, check the VPN to ensure files are transferred at **acceptable rates** and that all parts of the VPN are online when needed

I	When a remote user connects to your network, they connect to the server via a web browser
II	User then enters credentials to access the server
III	Select the files to be transferred
IV	Copy files from the corporate network to the remote user and vice versa
V	Track the time the file transfer takes
VI	Open the transferred files to make sure if they are transferred completely and working correctly
VII	The remote user disconnected from the corporate network after the file

To ensure a successful file transfer between the VPN host and the client are at an acceptable rate, all the VPN ports and other VPN components are to be checked for their online availability such as VPN gateway, Tunnel, etc.

Steps involved in checking the VPN file transfer between the host and the client are:

- Remote user should need a web browser to connect to the network.

- User should enter credentials to access the server. Then the user is to be authenticated and given access to the server contents if found genuine.

- User has to select the required files from a list of folders that are to be transferred to his system.

- Copy the files from the corporate network to the client system in the specified user location or directory and vice versa.

- Track the file transfer time either download or uploading of file.

- Open the transferred files in the client system to ensure they are transferred successfully and in a working state.

- Remote user is to be disconnected from the corporate network after the file transfer is complete.

Best Security Practices for VPN Configuration

CND
Certified Network Defender

📙 Ensure that your VPN service is configured to enforce requirements defined in the security policy

Recommended practices for a VPN deployment are:

1 **Deploy** VPN termination devices on dedicated network segments

2 Provide secure **access control** for VPN traffic

3 Use **dedicated** devices for VPN termination

4 Provide additional or **complementary authentication** to standard usernames and passwords

5 Enable an auditing feature to have a detailed **audit trail** for access, authentication, and use

6 Limit rules or **configurations** to designated users

7 Use **updated software** versions

8 Audit logs and **authentication records** on a daily basis

Recommendations for VPN Connections

CND
Certified Network Defender

✓ Provide a **dedicated firewall** for every VPN connection/server

✓ The VPN should follow **federal information processing standards** (FIPS), approved encryption and integrity protection algorithms

✓ VPN traffic should be **filtered** and inspected by internal firewalls

✓ VPN should provide **flexible and secure** communication between the remote connections and the organization's server

✓ Use **digital certifications** and device authentication methods for VPN connections

✓ Use symmetric and asymmetric forms of **cryptography** in the VPN

✓ Implement **strong application** level security on each application level

✓ Provide secure **data transmission** and information transfer between the networks

Recommendations for VPN Connections (Cont'd)

C|ND
Certified Network Defender

✓ **Configure** user authentication, access and restriction to the VPN network

✓ Manage and configure **IPsec gateways** to protect communication between networks

✓ Design **packet filters** with restrictions on limiting network traffic for additional protection

✓ Set rules and **time limits** for termination and disconnection of idle connections

✓ Define the **communication** channel for packet filters between the remote and main office

✓ Maintain a list of **authorized users** and regularly check for unauthorized access points

✗ Strictly **restrict and specify** the type of communication permitted between packet filters

✓ Deploy and plan **SSL VPN** connections according to the requirements of the organization
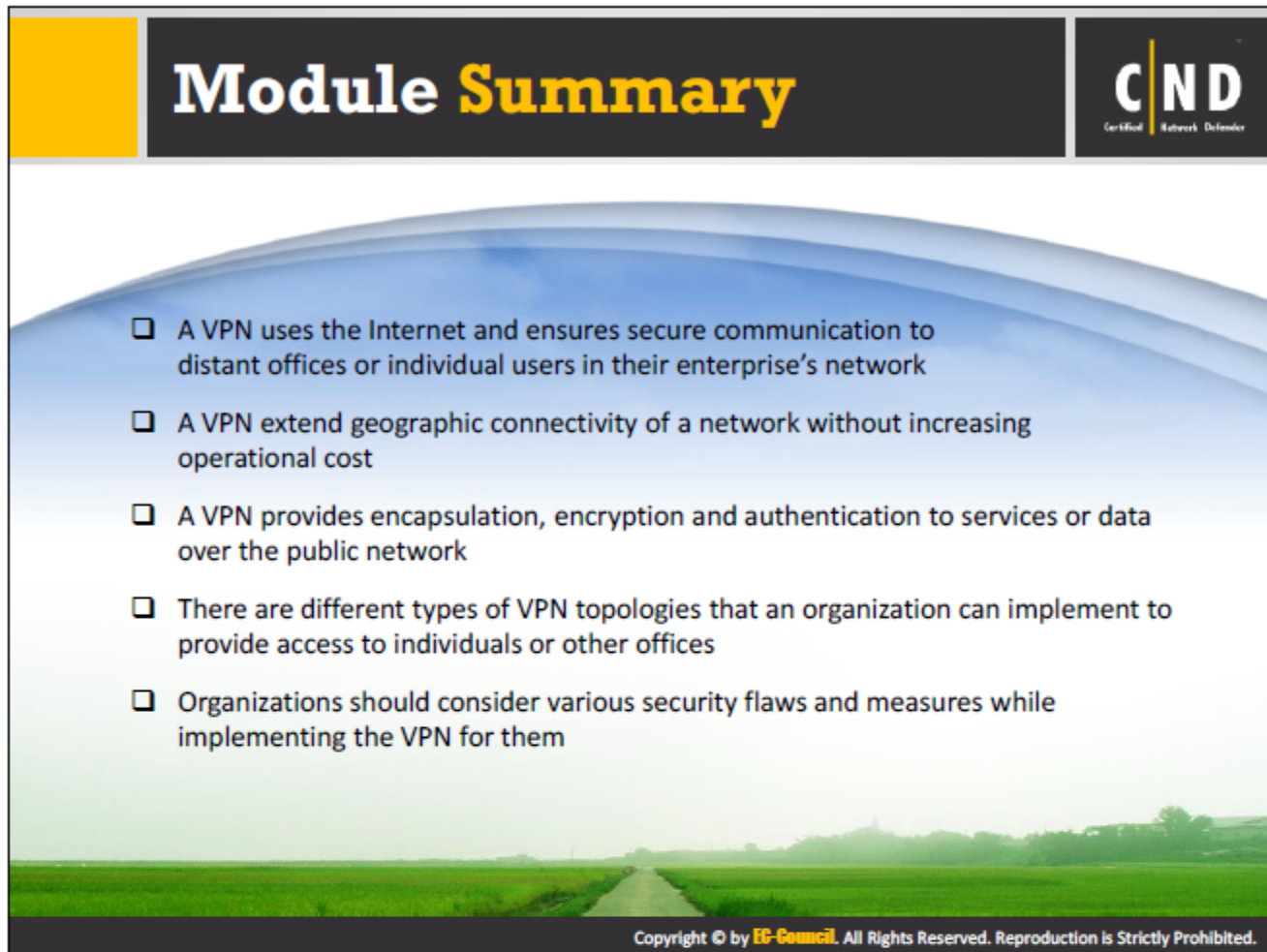
Recommendations for VPN Connections (Cont'd)

C|ND
Certified Network Defender

✓ Develop **secure remote** access to the organization's resources through a SSL VPN

✓ Provide control over all exit and entry points to ensure **network integrity** is protected

✓ **Integrate a SSL VPN** with intrusion prevention and detection techniques

✓ Provide and **restrict access** of security controls and resources to limited groups

✓ Deploy a SSL VPN with predefined **endpoint security** and access point control features

✓ SSL VPN implementation should support the overall technical, management and operational **controls** of an organization

✓ Select a SSL VPN that supports high **scalability** and availability features

✓ **Maintain** an updating, monitoring and securing process for the SSL VPN solution

Module Summary

CND
Certified | Network Defender

- ❏ A VPN uses the Internet and ensures secure communication to distant offices or individual users in their enterprise's network

- ❏ A VPN extend geographic connectivity of a network without increasing operational cost

- ❏ A VPN provides encapsulation, encryption and authentication to services or data over the public network

- ❏ There are different types of VPN topologies that an organization can implement to provide access to individuals or other offices

- ❏ Organizations should consider various security flaws and measures while implementing the VPN for them

In this module, you have learned the need of establishing a VPN, different VPN components, VPN topologies and technologies. You have also learned the various security flaws that exist due to improper/insecure configuration and implementation of a VPN. The module guides you on configuring and implementing VPN security through various security techniques, best practices and recommendations. With this module, you will able to select the appropriate VPN topology and technology based on your organization's need and will able to configure it securely.