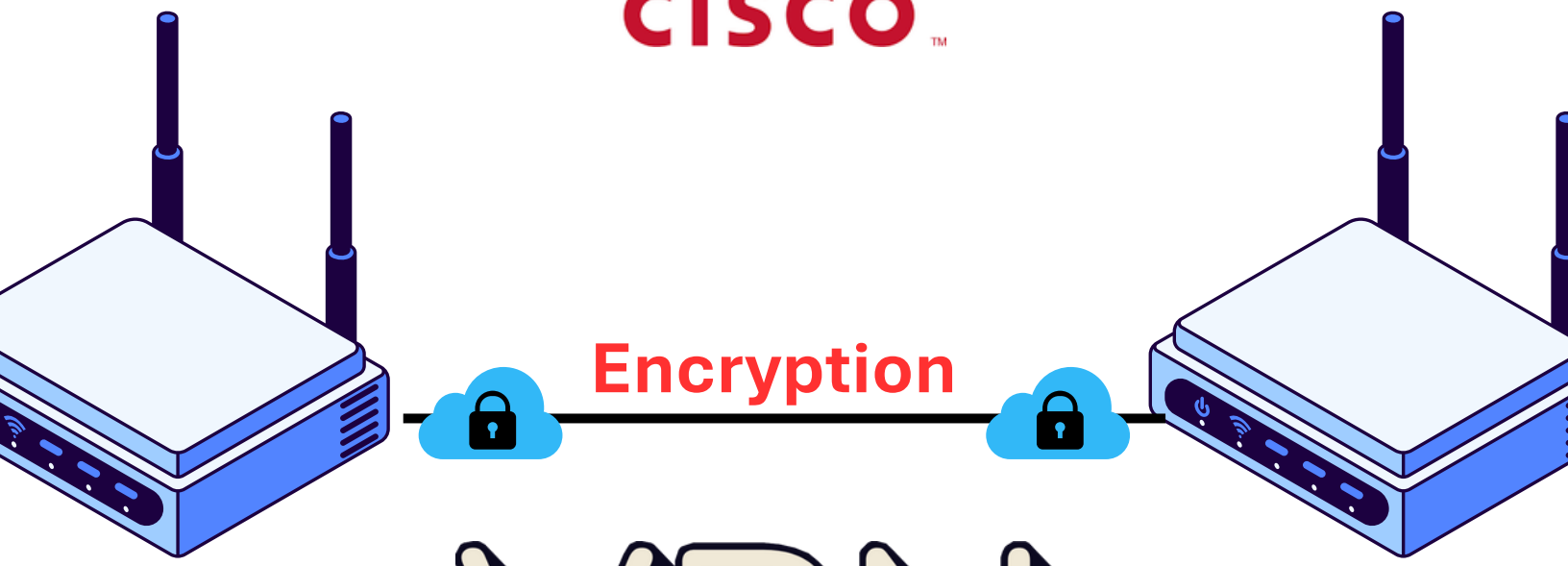
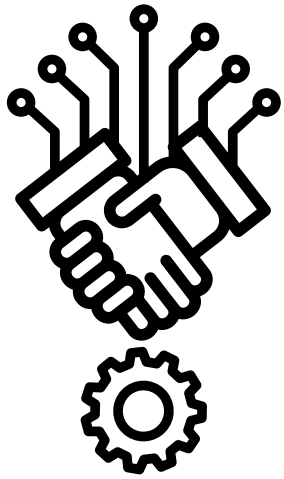


Virtual Private Network (VPN): Key Concepts & Summary Notes



Chapter 1 - VPN CONCEPT

What is VPN

What is VPN (Virtual Private Network)?

A VPN creates a secure, encrypted connection over the internet between a user and a private network.

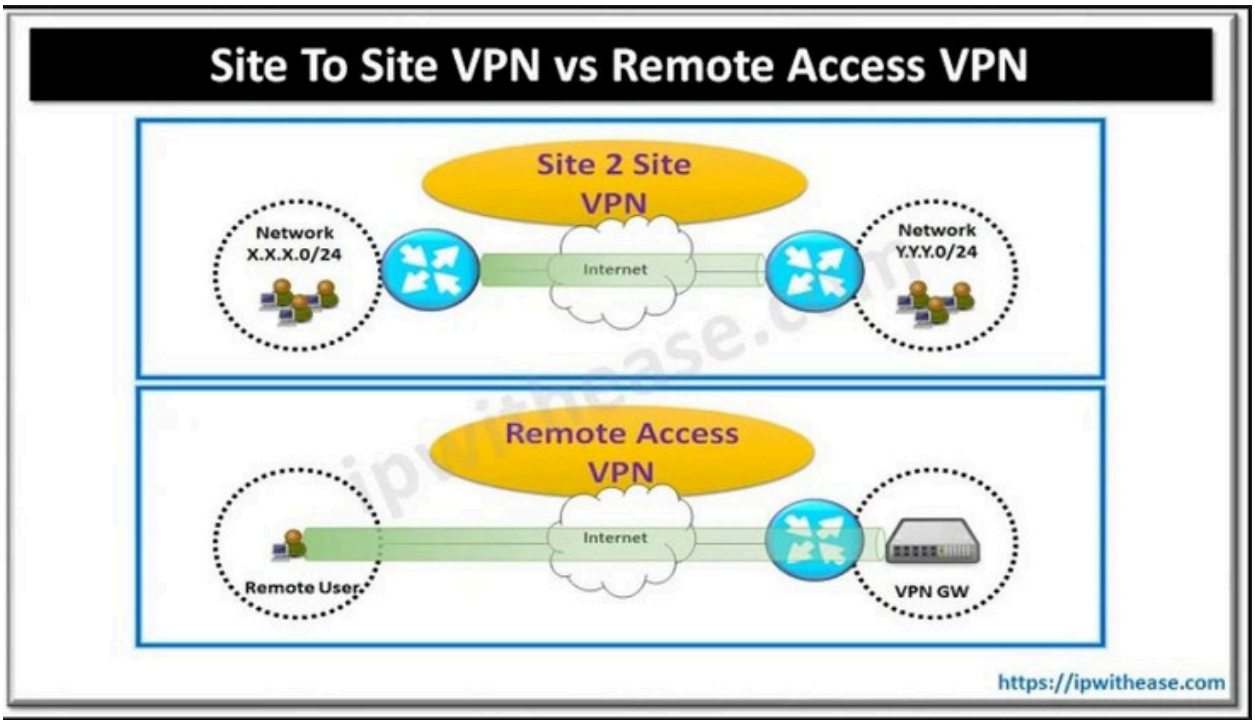
Why we use VPN:

- To protect data over public networks
- To access internal resources remotely
- To bypass geo-restrictions or censorship

Types of VPN:

1. Remote Access VPN:
   Connects individual users to a private network securely from anywhere.
   Example: An employee connects to their company's network from home.

2. Site-to-Site VPN:
   Connects two networks (offices) over the internet.
   Example: A company's UAE and India branches securely share resources.



Currently Used Protocols:

- OpenVPN – Secure, widely used, open-source
- IKEv2/IPSec – Fast, stable (great for mobile)
- WireGuard – Lightweight, modern, very fast
- L2TP/IPSec – Still in use, but less preferred
- SSTP – Works well on Windows (Microsoft-developed)
- SSL VPN – Still in use

Obsolete or Insecure Protocols:

- PPTP – Fast but outdated and insecure
- IPSec (alone) – Not commonly used standalone
- L2F (Layer 2 Forwarding) – Obsolete

Key Ways to Secure a VPN Connection:

1. Use secure protocols like OpenVPN, WireGuard, or IKEv2/IPSec
2. Enable strong encryption (e.g., AES-256)
3. Use multi-factor authentication (MFA)
4. Keep VPN software updated
5. Configure firewall and access controls

What is Encryption and Certificates

Encryption

Encryption is the process of converting plaintext (readable data) into ciphertext (unreadable data) to protect it from unauthorized access. It ensures that even if someone intercepts the data, they cannot read it without the proper decryption key.

Two Types of Encryption:

1. Symmetric Encryption

Definition: A type of encryption where the same key is used for both encryption and decryption.
Example Algorithms: AES (Advanced Encryption Standard), DES (Data Encryption Standard).
Use: Typically used for encrypting large volumes of data because it is faster than asymmetric encryption.
Key Management: Both the sender and receiver must securely exchange and store the same key.

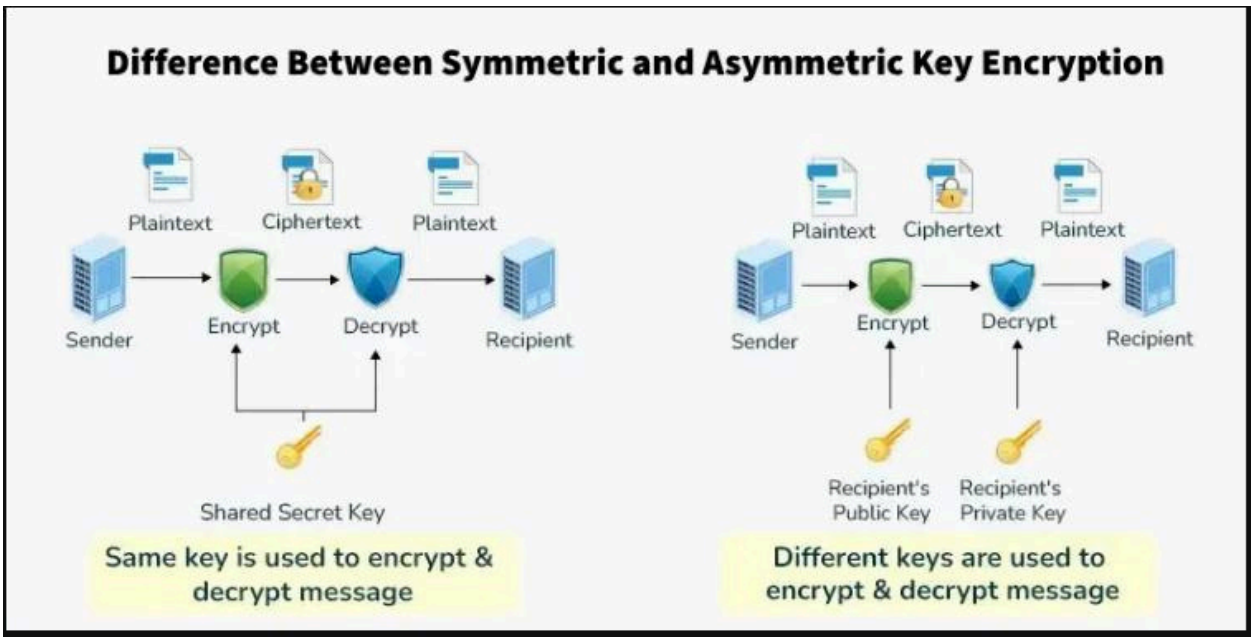
2. Asymmetric Encryption

Definition: A type of encryption that uses a pair of keys: a public key for encryption and a private key for decryption.

Example Algorithms: RSA, ECC (Elliptic Curve Cryptography).

Use: Used for secure communication, key exchange, and digital signatures. It is slower than symmetric encryption but provides better security for key distribution.

Key Management: The public key is shared openly, while the private key is kept secret by the recipient. Only the private key can decrypt data encrypted with the public key.



What is PKI

.PKI is a system that helps keep online communication secure and trustworthy.

Why is it used?

- To prove identity (like showing an ID card online)
- To keep data safe (by locking it with encryption)
- To make sure messages aren't changed (integrity)

How it works (simple steps):

1. You create a public key and private key.
2. A trusted company called a Certificate Authority (CA) checks who you are and gives you a digital certificate (like a digital ID card with your public key).
3. When you send data, others can check your identity and encrypt messages using your public key.
4. Only your private key (which only you have) can open it.
5. If your certificate gets stolen or misused, the CA can revoke (cancel) it.

Key Parts of PKI:

- Public key: Shared with others to encrypt messages.
- Private key: Kept secret, used to decrypt messages.
- Certificate Authority (CA): Like a trusted online passport office.
- Digital Certificate: A digital ID that proves you are genuine.

It's thefoundation for secure things like HTTPS websites, VPNs, and email encryption.

Hashing and Encryption

What it does:

- Converts data into unreadable form (ciphertext) to protect it from unauthorized access.
- Can be reversed (decrypted) using the right key.

Used for:

- Confidentiality – Only the intended receiver can read the data.
- Secure communication and data protection.

Examples of Encryption Protocols:

Protocol	Purpose
TLS/SSL	Secures web traffic (HTTPS)
IPsec	Used in VPNs for secure IP communication
OpenVPN	Open-source VPN protocol with strong encryption
SSH	Secure login to remote systems
S/MIME	Secures emails with encryption
BitLocker	Encrypts entire disks in Windows
AES	Symmetric encryption used widely (Advance Encryption Standard)
RSA	Asymmetric encryption (for key exchange, signatures) (Rivest-Shamir-Adleman)

HASHING

What it does:

- Converts data into a fixed-length hash value.
- One-way process – cannot be decrypted.
- Even a small change in input gives a completely different hash.

Used for:

- Integrity checking – Making sure data hasn't been changed.
- Password storage – Storing only the hash, not the password.
- Digital signatures – Verifying authenticity and data integrity.

Examples of Hashing Algorithms:

Algorithm	Purpose
MD5	Fast but outdated (not secure) (Message Digest 5)
SHA-1	Better than MD5, but still weak now (Secure Hash Algorithm)
SHA-256	Secure and widely used in modern systems
SHA-3	Latest in the SHA family, highly secure
HMAC-SHA256	Used in authentication protocols (e.g., API security)
bcrypt	Secure password hashing with salt
PBKDF2	Key derivation function (used for passwords)
Argon2	Modern and secure password hashing

Authentication and Radius Server

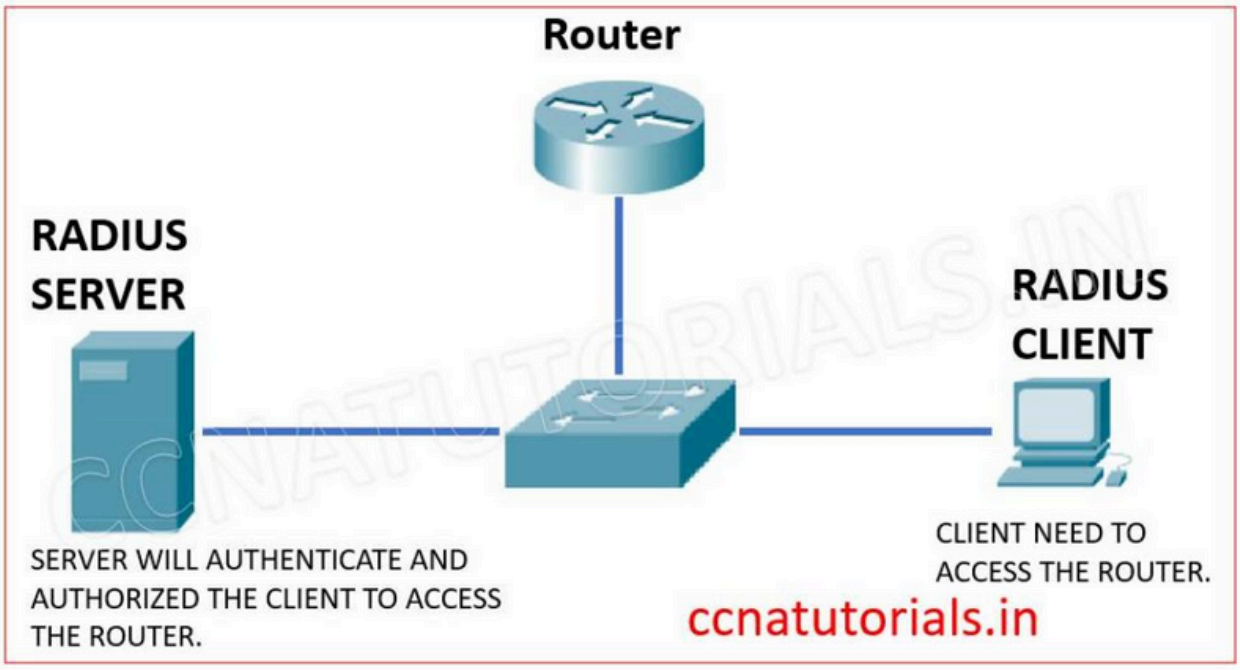
What is Authentication in VPN?

It’s the process of verifying a user's identity before allowing VPN access — usually using a username/password, certificate, or 2FA.

 What is RADIUS Server?

RADIUS (Remote Authentication Dial-In User Service) is a central server that handles:

- Authentication – Verifies user credentials
- Authorization – Checks access rights
- Accounting – Logs connection details



How It Works with VPN:

1. User tries to connect to VPN.
2. VPN server sends login info to RADIUS.
3. RADIUS checks credentials (e.g., via Active Directory).
4. If valid, user is connected; if not, access is denied.

Why Use RADIUS?

- Centralized control
- Secure and scalable
- Supports AD, 2FA, and logging

Two Factor Authentication

Two-Factor Authentication (2FA) in VPN means adding an extra layer of security when logging in.

It requires two things:

1. Something you know (like a password)

2. Something you have (like a code from your phone or an authenticator app)

Evenif someone steals your password, they can’t access the VPN without the second factor.

Simple,secure, and smarter!

Chapter 2 - VPN PROTOCOLS

PPTP AND L2TP

PPTP (Point-to-Point Tunneling Protocol)?

PPTP is one of the oldest VPN protocols, developed by Microsoft. It creates a secure connection (tunnel) over the internet to allow remote access to a private network.

Advantages of PPTP:

• Easy to set up – Built into most operating systems (Windows, macOS, Linux).

• Fast performance – Low encryption overhead makes it quick.

Low resource usage – Doesn't require powerful hardware.

Disadvantages of PPTP:

• Weak security – Uses outdated encryption (MS-CHAPv2), vulnerable to attacks.

- Blocked by firewalls – Uses TCP port 1723 and GRE protocol, which can be easily blocked.
- Obsolete – Not recommended today due to multiple known vulnerabilities.

PPTP VPN can be set up on a Windows Server, but it's not recommended today due to security vulnerabilities.

You can set it up using:

Remote Access (Role)

- This is the primary role to enable VPN services.

Routing and Remote Access Services (RRAS)

- Part of the Remote Access role. It provides the actual functionality for VPN (including PPTP).

L2TP (Layer 2 Tunneling Protocol)?

.L2TP is a VPN tunneling protocol that doesn't provide encryption by itself — it is usually combined with IPsec (Internet Protocol Security) to provide confidentiality, integrity, and encryption.

Advantages of L2TP/IPsec:

- Strong Security: Uses IPsec for encryption and authentication.
- OS Support: Built into most operating systems (Windows, macOS, Linux, iOS, Android).
- Supports NAT traversal: Can work behind NAT routers.
- Dual-layer protection: L2TP handles tunneling, IPsec handles encryption — more secure than PPTP.

Disadvantages of L2TP/IPsec:

- Harder to configure than PPTP (needs certificates or pre-shared keys).
- Slightly slower than PPTP due to double encapsulation (L2TP + IPsec).
- Sometimes blocked by firewalls (uses UDP ports 500, 4500, and ESP protocol).
- Requires proper certificate/key management for full security.

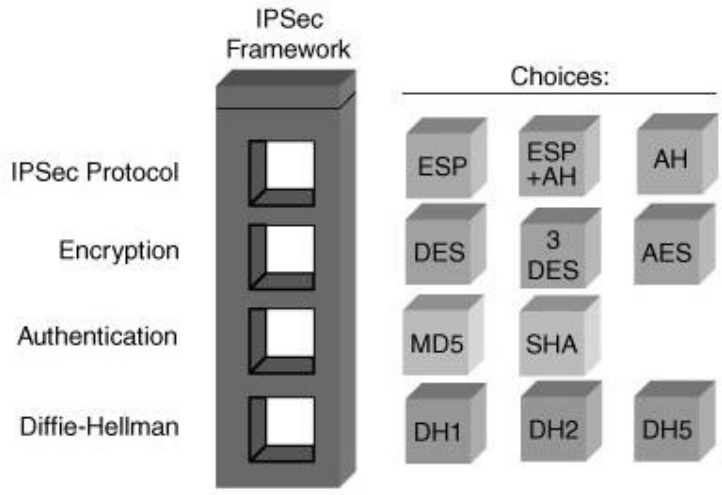
L2TP/IPsec can absolutely be implemented on a Windows Server, just like PPTP — and it's a more secure option.

IPSec

.IPSec is not a single protocol —It is a framework with several protocols that work together to provide secure, encrypted communication over IP networks.

- Encryption – to keep data private
- Authentication – to verify who's sending/receiving the data

- Integrity checks – to ensure data isn't altered in transit



Used in:

- VPNs (like L2TP/IPsec)
- Site-to-site tunnels
- Secure remote access

What is IKE

IKE (Internet Key Exchange) is a protocol used in IPsec to set up a secure and authenticated communication channel between two devices.

IKE operates in two phases, and together they are called the IKE negotiation process.

Here's how it works:

- IKE Phase 1:
  Creates a secure, encrypted communication channel between peers (called the IKE SA).

- IKE Phase 2:
  Negotiates the IPsec SAs — which define how the actual data (user traffic) will be encrypted and protected.

Final step:

Once Phase 2 is complete, the devices can securely send/receive data over the IPsec tunnel, using the keys and policies agreed during this phase.

Tunnel Mode and Transport Mode in firewalls and VPNs (especially with IPsec):

1. Tunnel Mode

Used for site-to-site VPNs (between two networks or firewalls)

- Entire IP packet is encrypted, including the original IP header
- A new IP header is added to route the encrypted packet
- Best for network-to-network or gateway-to-gateway communication

Example: Connecting two office networks securely over the internet

2. Transport Mode

Used for end-to-end communication (e.g., PC to server)

- Only the data (payload) of the IP packet is encrypted
- The original IP header stays intact
- Best for host-to-host communication (internal, secure networks)

Example: Encrypting data between a client and a server in the same network

What is SSL VPN?

SSL VPN is a type of VPN that uses SSL/TLS encryption (the same tech used in HTTPS websites) to provide secure remote access to internal network resources over the internet.

Accessible through a web browser — no dedicated VPN client required in many cases.

How it works:

- User connects via web browser (or client app like FortiClient or AnyConnect if needed)
- SSL/TLS encrypts the data between user and company network
- User is authenticated (often with username/password or 2FA)
- Access is granted to apps, files, or full network based on permissions

Types of SSL VPN:

1. Clientless SSL VPN
    - Access via web browser
    - Used for web apps, emails, internal portals
    - No software installation required

2. Full Tunnel SSL VPN (Client-based)
    - Requires VPN client (e.g., FortiClient, Cisco AnyConnect)
    - Provides access to the entire internal network
    - Encrypts all traffic, not just web

Advantages:

- Works from anywhere, even behind firewalls
- Often clientless (browser-based)
- Easy to set up for users
- Uses standard HTTPS port (443), so rarely blocked

Disadvantages:

- Limited functionality in clientless mode (web-based only)
- May require VPN client for full access
- Performance can vary depending on encryption and bandwidth

What is OPEN VPN?

OpenVPN is an open-source VPN protocol and software that allows secure point-to-point or site-to-site connections using SSL/TLS encryption.

It's highly secure, flexible, and widely supported across platforms (Windows, macOS, Linux, Android, iOS, routers, etc.).

How OpenVPN Works:

- Uses SSL/TLS for key exchange (like HTTPS websites).
- Supports both UDP (faster) and TCP (more reliable) transport protocols.
- After secure tunnel setup, all traffic is encrypted and tunneled through OpenVPN server.
- Clients use OpenVPN software or apps to connect (e.g., OpenVPN Connect).

Advantages of OpenVPN:

- Strong encryption (AES, TLS) – very secure
- Free and open source
- Cross-platform support
- Customizable and flexible – works with firewalls, proxies
- Can use TCP or UDP – suits different network types

Disadvantages of OpenVPN:

- Needs configuration – more complex setup than PPTP or L2TP
- Slightly slower than WireGuard or IKEv2 on some networks
- Requires client software on devices

What is WireGuard VPN?

devicesWireGuard is a modern, lightweight, open-source VPN protocol designed for simplicity, speed, and strong security. It's built directly into the Linux kernel and is also available for Windows, macOS, Android, and iOS.

How It Works:

- Uses public-key cryptography for authentication (like SSH).
- Establishes a point-to-point encrypted tunnel.
- Uses UDP and modern encryption (ChaCha20, Poly1305).
- Quick handshake, minimal codebase (~4,000 lines), making it efficient and easier to audit.

Advantages:

- High speed and low latency
- Lightweight and simple configuration
- Strong encryption and modern cryptographic standards
- Cross-platform and integrated into Linux kernel
- Fast reconnection – ideal for mobile/roaming users

Disadvantages:

- No built-in support for dynamic IPs or user authentication (must be handled externally)
- Still relatively new — not as mature as IPSec/OpenVPN
- Limited support for advanced networking features (e.g., complex routing)

Key Points:

- Suitable for both enterprise and personal use
- Great for site-to-site or client-to-site VPN
- Being adopted in many cloud and DevOps environments.

Thanks for your time!

Keep learning, andkeep growing!....