Virtual Private Network (VPN)



A Comprehensive Guide to VPN

CODELIVLY
LEARN CYBERSECURITY

Table of Content

1.History of VPN 3

1.1 Why We Need VPN: 3

1.2 Who Created VPN? 3

1.3 Purpose and First Use: 3

1.4 Problem VPN Solves: 3

2. Introduction 4

3. Explanation..……..……3

3.1 Encryption 5

3.2 Tunneling Protocol 6

3.3 IP Address Masking 7

3.4 Authentication Mechanism 7

3.5 VPN Server 8

3.6 Kill Switch 9

3.7 Split Tunneling 10

3.8 VPN Client Software 10

3.9 VPN Gateway 11

4. How VPN Works: 12

5. Technical Workflow and VPN Protocols 13

6. Key VPN Protocols: 13

7. Advantages of VPN 15

8. Disadvantages and Flaws of VPN 15

9. Key Features of VPN 16

10. Popular VPN Examples 16

10.1 Open-Source VPNs: 16

10.2 Paid VPNs: 16

11. Conclusion 17

12. References: 17

History of VPN

Why We Need VPN:

In the early days of the internet, network communications were unencrypted, making sensitive data vulnerable to interception. The need for a secure and private means of transmitting data became apparent as businesses and individuals required privacy from hackers, government surveillance, and online threats.

Who Created VPN?

VPN technology was first conceptualized by Microsoft engineers in 1996. **Gurdeep Singh-Pall**, a Microsoft employee, created the first VPN protocol called **PPTP (Point-to-Point Tunneling Protocol)**, which allowed secure and private data transmissions over the internet.

Purpose and First Use:

VPN was initially designed to enable employees to securely connect to corporate networks from remote locations. The early adopters of VPNs were corporations that needed to ensure that their sensitive business data remained private when accessed by employees from outside the office.

Problem VPN Solves:

The key issue VPNs address is the need for secure, encrypted data communication over public networks. This was particularly important for remote workers and those accessing sensitive systems, preventing man-in-the-middle (MitM) attacks and unauthorized access.

Introduction

A **Virtual Private Network (VPN)** is a technology that allows users to create a secure, encrypted connection over a less secure network, typically the internet. VPNs were developed to enable users to safely and privately transmit data across public networks as if they were directly connected to a private network. It offers users **anonymity and security** by masking their IP address and encrypting the data sent over the network.

VPNs have become widely popular in both **corporate and personal use**. Businesses use VPNs to allow **remote employees** to securely access company resources, while individual users often utilize VPNs to protect their online privacy, secure data on public Wi-Fi, and bypass geographic restrictions on content.



Explanation:

A VPN extends a private network across a public network. It allows users to send and receive data securely as if they were connected to a private network, even though they are using a public network. VPNs work by creating a virtual encrypted tunnel between the user's device and the VPN server, making their IP address anonymous and encrypting their online activities.

Key Components of VPN:

A VPN comprises several key components that work together to ensure secure, private, and anonymous internet access. These components provide the core functionality of VPN services,

allowing users to protect their data, hide their online activities, and securely connect to private networks.

1. Encryption

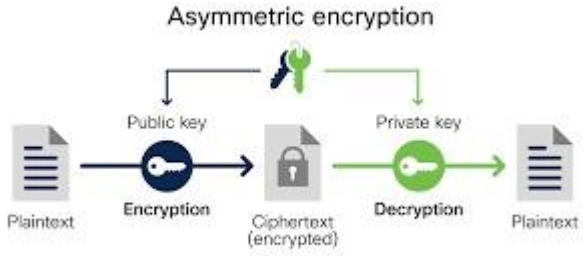
Encryption is one of the most critical components of a VPN. It scrambles the user's data into an unreadable format, ensuring that even if the data is intercepted, it cannot be deciphered by unauthorized parties. Only the VPN server and client (the user) have the keys to decrypt the data.

Example:

When accessing a website over a public Wi-Fi network without a VPN, data like your browsing history, passwords, and personal details could be intercepted by attackers using packet sniffers. However, with a VPN enabled, all data between your device and the VPN server is encrypted, making it impossible for attackers to read or misuse the information.

Types of Encryption Used in VPNs:

- **AES-256 (Advanced Encryption Standard)**: The most widely used encryption standard for VPNs, offering a high level of security.
- **RSA (Rivest-Shamir-Adleman)**: An encryption algorithm that is commonly used for secure key exchange between the client and the VPN server.



source:image

2. Tunneling Protocol

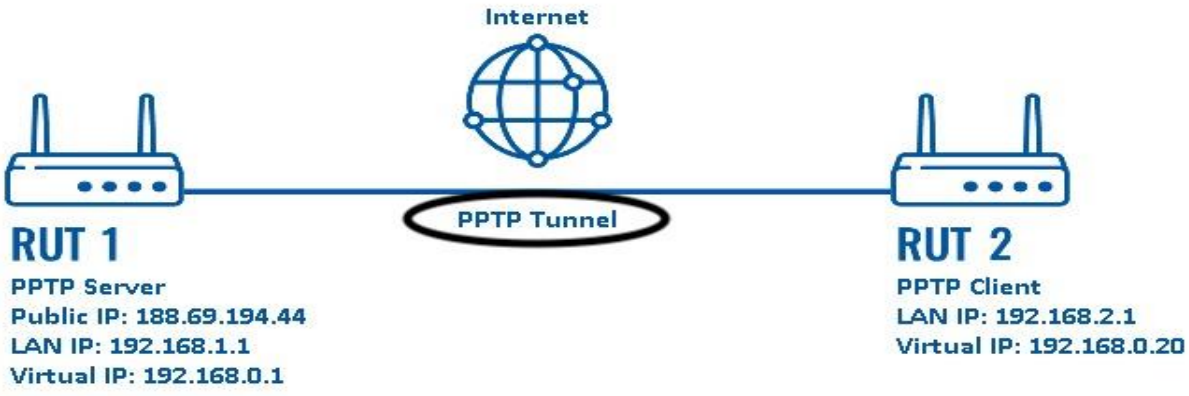
Tunneling Protocols define how data is transferred between the VPN client and server. These protocols create a "tunnel" for secure communication and govern the encryption and security levels of the connection. VPN protocols impact the speed, security, and stability of the connection.

Example:

- **OpenVPN** is a widely used open-source VPN protocol known for its strong security and flexibility. It supports a variety of encryption methods and is compatible with most devices and platforms.
- **IKEv2 (Internet Key Exchange version 2)** is another protocol that is especially good for mobile devices due to its ability to quickly reconnect when switching between networks, such as from Wi-Fi to mobile data.

Common VPN Protocols:

- **PPTP** (Point-to-Point Tunneling Protocol): One of the earliest VPN protocols, easy to set up but offers weak security.
- **L2TP/IPSec (Layer 2 Tunneling Protocol/Internet Protocol Security)**: Combines encryption with tunneling, providing strong security but may result in slower speeds.
- **WireGuard**: A modern protocol known for its speed, security, and simplicity compared to older protocols like OpenVPN.

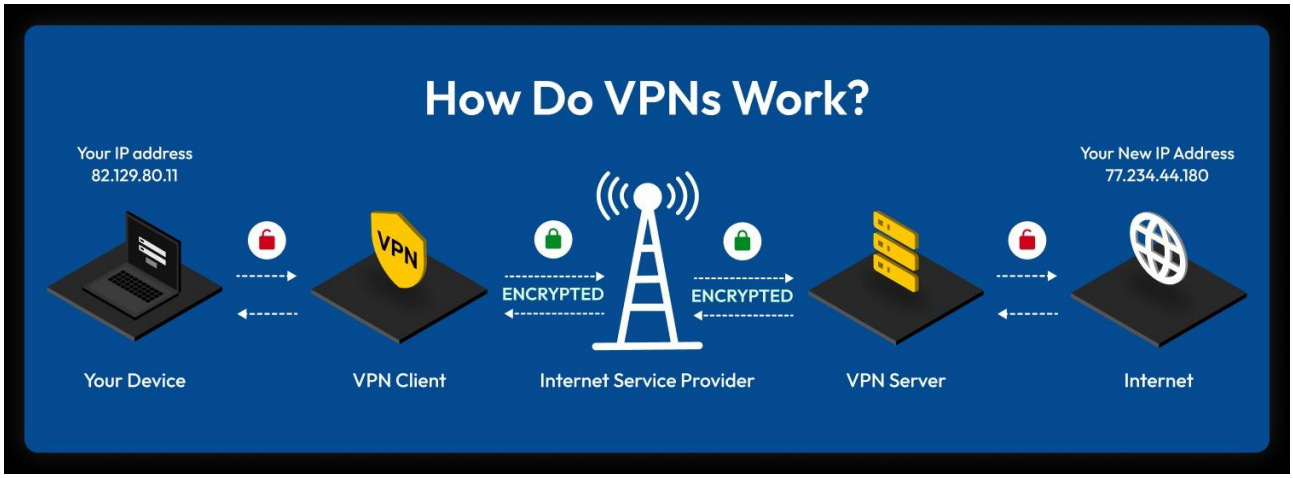


3. IP Address Masking

VPNs hide the user's real IP address by replacing it with the IP address of the VPN server. This process is known as **IP masking**, which protects the user's location and identity from being tracked or logged by websites, ISPs, or other entities. By using different VPN servers, users can appear to be browsing from any geographic location.

Example:

When connected to a VPN server in another country (e.g., connecting to a server in the USA from Europe), websites and services see the IP address of the VPN server instead of the user's actual IP address. This can allow users to bypass geo-restrictions on services like Netflix, which offers different content based on location.



4. Authentication Mechanism

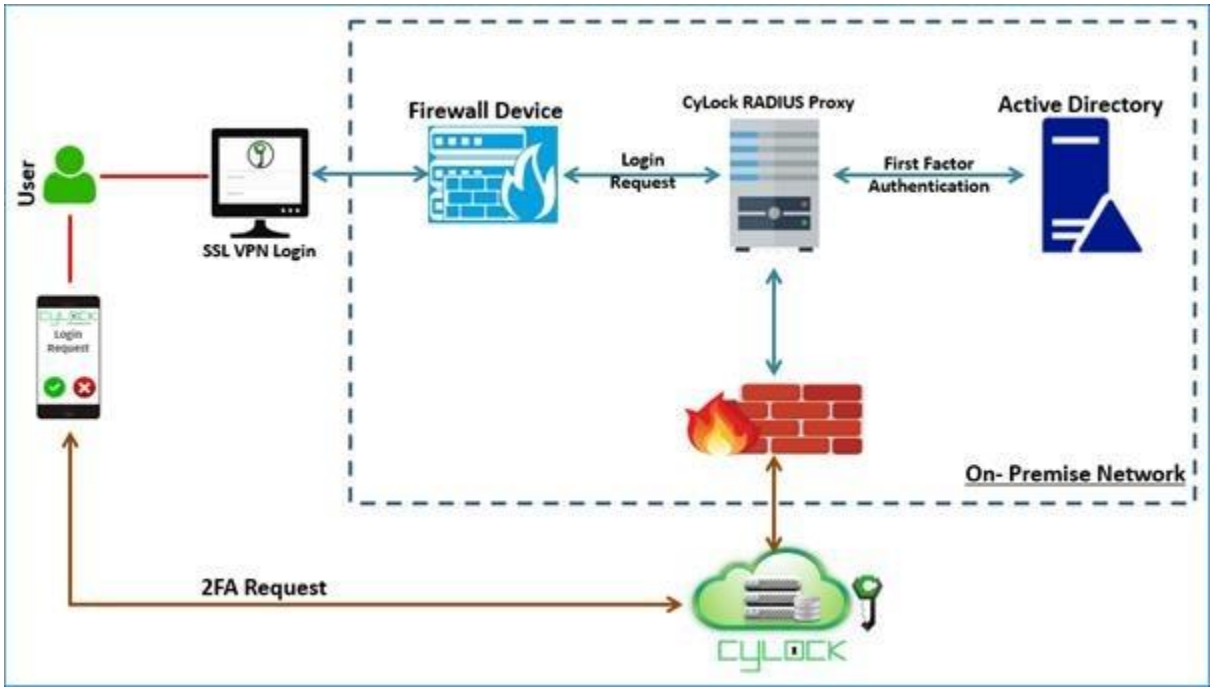
Authentication is the process by which the VPN verifies the identity of the user and ensures that they have permission to access the network. Authentication mechanisms protect VPNs from unauthorized access and help establish a secure connection between the user and the VPN server.

Example:

When a user connects to a corporate VPN, they typically need to provide credentials like a username and password. In more secure setups, two-factor authentication (2FA) might be required, where the user provides a one-time password (OTP) sent to their phone in addition to their regular password.

Common Authentication Methods:

- **Pre-shared Key (PSK)**: A secret key shared between the VPN client and server.
- **Certificates**: Public and private key pairs used to authenticate and secure communications.
- **Multi-Factor Authentication (MFA)**: An extra layer of security requiring additional forms of identification (e.g., OTP or biometric data) along with a password.



5. VPN Server

The **VPN server** is the central component that handles the user's connection. It serves as the intermediary between the user's device and the internet, encrypting outgoing traffic and decrypting incoming traffic. The VPN server also assigns an IP address to the user and routes their internet traffic through its own network.