

VPN Technologies

Reading

20 minutes

✓ Status Incomplete

Introduction

The **Virtual Private Network (VPN)** describes a method to establish a secure, encrypted network connection between two different networks on a public network. This process makes it challenging for third parties to track your activities and information and steal your data. The VPN encryption works in real-time.

Reading

VPN Types

1. **Remote Access VPN** allows users to connect to a network and access its services and resources remotely. The connection is secure and private and takes place over the Internet.

This VPN is beneficial for both corporate and home users. A corporate employee can use a VPN to connect to their company's private network and remotely access files and resources.

Home or private users use VPN services primarily to bypass regional internet restrictions, and access blocked websites. Users looking for more security online also use VPN services to enhance their Internet privacy.

2. **Site-to-Site VPN** is also called a "router-to-router" VPN and is primarily used at the enterprise level. Companies use this technology to connect headquarters to offices in different geographic locations. When multiple offices of the same company in the exact geographic location are combined, it is called an **Intranet-based VPN**. When companies use this type of VPN to connect to another company's office, it is called an **Extranet-based VPN**. Site-to-site VPN creates a virtual bridge between networks in remote offices, connecting them through the Internet to maintain secure and private communication.
3. **Secure Sockets Layer (SSL) VPN** is used for employees to remotely access company systems in a secure and controlled environment, reducing the risk of virtual invasions.

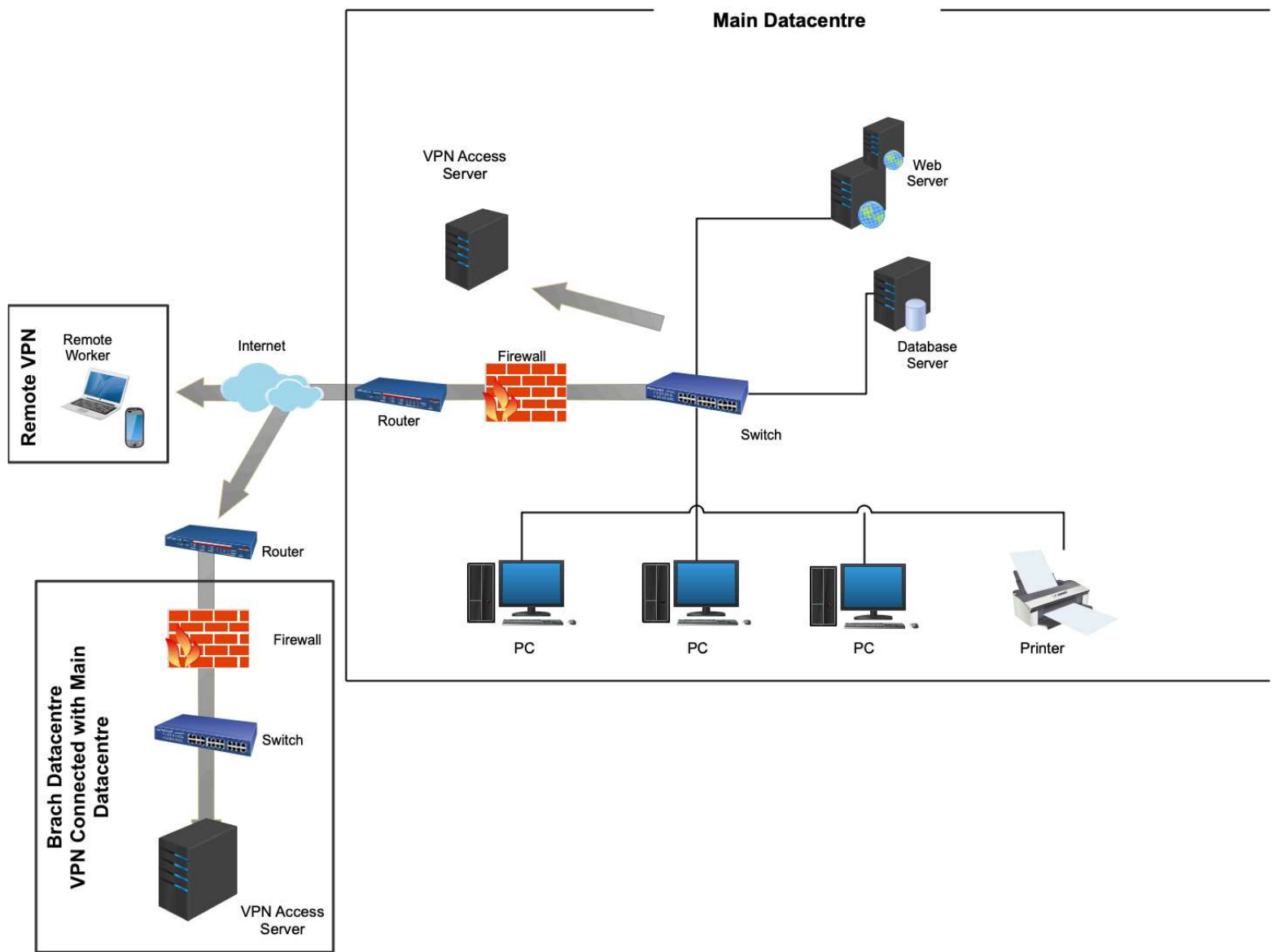
VPN Protocol Types

The VPN types are based on different security protocols. Each of these protocols offers additional features and security levels.

- **IPSec - Internet Protocol Security** is used to secure Internet communication over an IP network. It authenticates the session and encrypts all packets during the entire connection. The IPSec uses two operation modes to ensure data transfer between two different networks:
 - The **Transport mode** which encrypts the message in the data packet.
 - The **Tunnel mode** which encrypts the entire data packet. When a device connects to a VPN, it establishes an encrypted "tunnel" between the device and the VPN server.
- **Layer 2 Tunneling Protocol (L2TP)** is often combined with another VPN security protocol, such as IPSec, to create a highly secure VPN connection. L2TP creates a tunnel between two L2TP connection points, and the IPSec protocol encrypts the data and handles the secure communication in the tunnel.
- **Point-to-Point Tunneling Protocol (PPTP)** creates a tunnel and wraps the data packet. It uses a **point-to-point protocol (PPP)** to encrypt the data across the connection. PPTP is one of the most used VPN protocols. Besides Windows, PPTP is also supported on Mac and Linux.
- **Secure Sockets Layer (SSL)** and *Transport Layer Security (TLS)* create a VPN connection where the browser acts as a client and restricts access to specific applications. Online shopping sites and service providers use SSL and TLS protocols. Web browsers easily switch to SSL, and no action is required from the user. SSL connections have HTTPS at the beginning of the URL.
- **OpenVPN** is a valuable open-source VPN for creating point-to-point and site-to-site connections. It uses a custom security protocol based on **SSL** and **TLS** protocol.
- **Secure Shell (SSH)** creates the VPN tunnel through which the data transfer takes place and ensures that the tunnel is encrypted. An *SSH* client makes SSH connections, and data is transferred from a local port to the remote server through this tunnel.

In the image below, you can see a simple topology with two examples of VPN implementation:

1. Site-to-site VPN to connect a branch to the main data centre.
2. SSL VPN for a remote user connected to the main data centre.



✓ Mark Completed



Previous
Firewall Technologies

Next
Firewalls and VPNs



How well did this activity help you to understand the content?














Let us know how we're doing



> Lectures (1)

✓ Work (13)

7 hrs

 <u>Frame Makeup By Protocol Headers</u>	✓
 <u>Intro to Wireshark Filtering and Analysis</u>	✓
 <u>IP Lab</u>	✓
 <u>ARP Lab</u>	✓
 <u>TCP Lab</u>	✓
 <u>Network Administration pt 1 Quiz</u>	✓
 <u>What is a VLAN?</u>	✓
 <u>Network Segmentation</u>	✓
 <u>Network Segmentation</u>	✓
 <u>Group Share and Feedback</u>	✓
 <u>Firewall Technologies</u>	✓
 <u>VPN Technologies</u>	
 <u>Firewalls and VPNs</u>	

[W01D3 Schedule »](#)