INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH AND INNOVATIVE STUDIES
ISSN: 2820-7157
www.ijsrisjournal.com

February 2025 Volume 5 Number 1 54-64

Received Date: December 20, 2025 Accepted Date: January 12, 2026 Published Date: February 01, 2026

Study and implementation of a high-availability site-to-site VPN

ETUMANGELE TSHITAKA Gabriel

Gombe Higher Institute of Education, Assistant Second term, gabrieletums2015@gmail.com , +243 817 851 599

Abstract

Since the early days of the Internet until today, technology has evolved enormously. Since the advent of the Internet, information exchange has become commonplace; information is exchanged between one or more people; between a user and a server; between a company and its customers/partners via the Internet. The Internet is the network of networks. It is public and unsecured. Since all individuals and companies communicate and exchange data or information, they are all exposed to threats and risks when using the Internet as a means of transmission for communication.

The implementation of a VPN is based on decryption platforms. The configuration of these platforms depends on the operating system used. Establishing a VPN connection requires knowledge of cryptography and network configuration. Several solutions exist, using proprietary and open-source platforms. VPN technology guarantees secure exchanges of sensitive information, accessible from anywhere, as long as an internet connection is available.

Keywords: Study, Implementation, VPN, Site-to-Site, High Availability, Protocol

1. VPN technologies

Nowadays, companies exchange more and more data, so traffic is enormous. They exchange data with several companies or individuals who may be their customers, partners or subsidiaries. Via the Internet, a company can exchange data from its local network () with the local networks of its partners or subsidiaries. This chapter will present VPNs, including their categories, protocols and architecture. A VPN will ultimately be chosen for implementation.

1.1. Introduction to VPNs

VPN, or Virtual Private Network, is a system that allows a direct link to be created between remote computers. The connection between the computers is managed transparently by the VPN software, creating a tunnel between them. Computers connected to the VPN are thus on the same local (virtual) network, which allows them to bypass any restrictions on the network (such as firewalls or proxies).

A virtual private network is based on a protocol called tunnelling, which is a protocol that allows data passing from one end of the VPN to the other to be secured by cryptographic algorithms. The term "tunnel" is used to symbolise the fact that between the entry and exit points of the VPN, the data is encrypted and therefore incomprehensible to anyone located between the two ends of the VPN, as if the data were passing through a tunnel. In the case of a VPN established between two machines, the element that encrypts and decrypts data on the user (client) side is called a VPN client, and the element that encrypts and decrypts data on the organisation side is called a VPN server (or more generally a remote access server).

In this way, when a user needs to access the virtual private network, their request is transmitted in plain text to the gateway system, which connects to the remote network via a public network infrastructure and then transmits the request in encrypted form. The remote computer will then provide the data to the VPN server on its local network, which will transmit the response in encrypted form. Upon receipt by the user's VPN client, the data will be decrypted and then transmitted to the user.

A VPN also generally has a gateway providing external access, which allows the apparent source IP address of its connections to be changed. This makes it more difficult for the service provider to identify and roughly locate the sending computer. However, the VPN infrastructure (usually a server) has the information needed to identify the user. This also makes it possible to bypass the geographical restrictions of certain services offered on the Internet.

1.1.1. How it works

The principle of tunnelling consists of constructing a virtual path after identifying the sender and the recipient. The source then encrypts the data and routes it along this virtual path. In order to provide easy and inexpensive access to corporate intranets or extranets, virtual private access networks simulate a private network, when in reality they use a shared access infrastructure, such as the Internet.

The data to be transmitted may be handled by a protocol other than IP. In this case, the tunnelling protocol encapsulates the data by adding a header. Tunnelling is the set of encapsulation and transmission processes.

1.1.2. VPN categories

There are three categories of VPNs, which are:

- ✓ Access VPN
- ✓ Intranet VPN
- ✓ Extranet VPN

First, the access VPN (gateway station) is used to allow mobile users to access their company's network. The user uses an Internet connection to establish a secure link.

Secondly, the Intranet VPN is used to connect two or more intranets within the same company. This type of network is particularly useful within a company with several remote sites. This technique is also used to connect company networks without involving an intranet (data sharing, resource sharing, remote server operation).

Finally, an organisation's extranet VPN can be used to communicate with its customers and partners. It then opens up its local network to them. In this case, it is necessary to have strong user authentication and a record of the various accesses. In addition, only some of the resources will be shared, which requires rigorous management of the exchange spaces.

1.1.3. VPN tunnelling protocols

There are several different types of protocols that manage point-to-point connections, such as PPP (Point-to-Point Protocol), PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol) and IPSEC (IP Security Protocol). These protocols create a tunnel through which information can pass without having to create a new access path each time, just as happens with traffic.

The following protocols will be presented below: PPP (Point-to-Point Protocol), PPTP (Point-to-Point Tunneling Protocol), L2F (Layer Two Forwarding), L2TP (Layer 2 Tunneling Protocol), SSTP (Secure Socket Tunneling Protocol), MPLS (Multi-Protocol Label Switching), IPSEC (IP Security Protocol), SSL/TLS (Secure Socket Layer), and SSH (Secure Shell) protocols are presented below.

A. PPP

The Point-to-Point Protocol (PPP) was developed in the 1980s. The PPP protocol was developed to transfer data over synchronous or asynchronous links between two points using HDLC as the encapsulation basis and an HDLC Frame Check Sequence (FCS) for error detection. This link allows full duplex and guarantees the order of packet arrival. An interesting feature of this protocol is the simultaneous multiplexing of several OSI model layer 3 protocols. This protocol encapsulates IP, IPX and NetBEUI packets in PPP frames and then transmits these encapsulated PPP packets over the point-to-point link. PPP is therefore used between a remote client and a remote access server. The PPP protocol is described in RFC 1331.

NAS (Network Access Service) is ISP equipment that supports 16 to 200 simultaneous PPP communications. The PPP client is available on all recent operating systems: example of Windows RAS (Remote Access Service).

B. PPTP

The PPTP (Point to Point Tunnelling Protocol) is a layer 2 protocol developed by Microsoft. It is an extension of the PPP protocol. This protocol encapsulates PPP frames in IP datagrams in order to transfer them over an IP network.

PPTP enables the encryption of encapsulated PPP data and its compression via the GRE (Generic Routing Encapsulation) protocol. All PPTP connections use a PPTP client and server.

C. L2F

The L2F (Layer Two Forwarding) protocol is a Layer 2 protocol developed by Cisco. This protocol is implemented in the IOS (Internetworking Operating System) operating system used in the brand's equipment. It is described in RFC 2341.

This protocol allows a remote access server to carry traffic over PPP and transfer this data to an L2F server. This L2F server decapsulates the packets and sends them over the network.

In this case, the client connects to the ISP via a standard PPP link and uses the tunnel created between the remote access server and the end router.
It should be noted that unlike PPTP and L2PT, L2F does not require a client. In addition, multiple clients can use the same tunnel. This protocol is gradually being replaced by L2TP, which is more flexible.

The L2TP (Layer Two Tunnelling Protocol) is a layer 2 protocol. It is a convergence of the PPTP and L2F protocols. It combines the advantages of both protocols. It is a recent protocol (August 1999). This protocol is recognised as the standard tunnelling protocol for dial-up access.

It uses the PPP communication protocol to extend remote network access to a site on the Internet through a tunnel. The elements on both sides of the tunnel consist of an LAC (L2TP Access Concentrator) and an LNS (L2TP Network Server). The LAC terminates the physical PPP connection at an ISP's point of presence (POP) and establishes a virtual PPP session through the tunnel to the LNS.

L2TP is a network protocol that encapsulates PPP frames to send them over IP, X25, frame relay or ATM networks. When configured to carry data over IP, L2TP can be used for tunnelling over the Internet. However, L2TP can also be implemented directly on WAN media (frame relay) without using the IP transport layer.

D. SSTP

SSTP (Secure Socket Tunneling Protocol) is a new tunnelling protocol that uses the HTTPS protocol on TCP port 443 to pass traffic through firewalls and web proxies that may block PPTP and L2TP/IPsec traffic. The SSTP protocol provides a mechanism for encapsulating PPP traffic within the SSL channel of the HTTPS protocol. The use of PPP enables support for strong authentication methods, such as EAP-TLS. The SSL protocol provides transport-level security with enhanced key negotiation, encryption, and integrity verification.

When a client attempts to establish an SSTP VPN connection, the SSTP protocol first establishes a bidirectional HTTPS layer with the SSTP server. Protocol packets transit as data payload over this HTTPS layer.

The SSTP protocol encapsulates PPP frames in IP datagrams for transmission over the network. SSTP uses a TCP connection (on port 443) for tunnel management, as well as PPP data frames. The SSTP message is encrypted with the SSL channel of the HTTPS protocol.

E. SSL

Designed by Netscape, SSL is a protocol that sits between the application layer and the transport layer to ensure confidentiality, authentication and data integrity during communications. It can be applied to applications such as HTTP, POP, FTP, etc.

F. IPSEC

IPSec (Internet Protocol Security) is a layer 3 protocol. It is widely used in the creation of virtual private networks and to secure remote access to an intranet. IPSec services are based on cryptographic mechanisms that provide a high level of security. As security is provided at the IP level, IPSec can be implemented on all network equipment and provides a single means of protection for data exchanges.

IPSec is a standard developed by an IETF working group. The first version appeared in August 1995 (RFC 1825 to 1829). A second version, which also includes a dynamic security parameter management system, was published in November 1998 (RFC 2401 to 2411).

IPSec fits into the TCP/IP protocol stack at the IP level. This has the advantage of making it usable by higher levels and, in particular, offering a single means of protection for all applications. In other words, where other systems secure applications on a case-by-case basis, IPSec secures the underlying network. This approach is not without its constraints, notably performance issues and the difficulty of accurately distinguishing between different flows.

The security services provided by IPSec are:

- ✓ Confidentiality: encryption of data and headers, configurable encryption algorithm (DES or triple DES)

- ✓ Authentication and data integrity: addition of a MAC field, configurable MAC generation method
- ✓ Replay protection: addition of a sequence number that is protected in integrity by the MAC
- ✓ Access control

The second IPSEC protocol is the AH (Authentication Header) protocol, which ensures the integrity and authentication of the origin of IP packets but not the confidentiality of the data.

The IP packet is assigned a new field that allows the authenticity of the data to be verified. This field contains a hash (MD5 or SHA-1 digest) called the "Integrity Check Value". Protection against replay (packet reinjection) is provided by a sequence number, which prevents flood attacks. The security parameters related to communication s are identified by a unique identifier (Security Parameters Index) characterising the Security Association (SA). This is a combination of the recipient's address and the protocol used.

This protocol provides the means to guarantee:

- ✓ the authentication of the packet and its sender (if the source address of the packet is that of the sender).
- ✓ The uniqueness of the packet (no replay).
- ✓ Data integrity (no deliberate or accidental alteration of the packet during transport).

Only certain fields are certified in the packet: the IP version, header/data/packet length, data (in tunnel or transport mode), flow identifier, next protocol or header, source and recipient IP address. The others are not certified because their values change during the packet's lifetime (e.g. TTL, traffic class?). For total protection of the IP packet, Tunnel mode must be used.

Finally, the third IPSEC protocol is the IKE (Internet Key Exchange) protocol. The purpose of this protocol in its first phase is to build an initial secure tunnel between the two hosts (the IKE tunnel). It is used to manage IPSec tunnels (negotiating and updating SAs), which constitute the second phase of the IKE protocol. These tunnels are used to exchange data between hosts. However, IPSec offers the option of manual authentication without using IKE.

It is a combination of several other protocols:

- ✓ ISAKMP, Internet Key Agreement and Security Management Protocol: a generic framework allowing the use of several key exchange protocols
- ✓ SKEME and Oakley, key exchange systems.

G. MPLS

In computer networks and telecommunications, Multi-Protocol Label Switching (MPLS) is a data transport mechanism based on label switching. It is a network technique whose main role is to combine the concepts of Layer 3 IP routing and Layer 2 switching mechanisms. One of the initial objectives of MPLS was to increase the speed of datagram processing across all intermediate equipment. With the introduction of gigabit routers, this objective has now taken a back seat. Since then, functionality has largely taken precedence over performance, with the following motivations in particular:

- ✓ Creation of VPNs
- ✓ Multicast routing
- ✓ Flexibility: possibility of using several types of media (ATM, FR, Ethernet, PPP, SDH).
- ✓ Differential Services (DiffServ)

MPLS clearly reigns supreme in wide area networks (WANs): 74% of companies that participated in Nemertes' 2011-2012 Computing and Communications Benchmark study have deployed MPLS/IP-VPN services.

H. SSH

SSH refers to both the cryptographic network protocol and the utilities that implement this protocol. SSH operates on a client-server model, connecting a Secure Shell client application—where the session is displayed—to an SSH server—where the session is executed.

Most operating systems, with the exception of Microsoft Windows, include SSH by default. SSH supports tunnelling, which transfers arbitrary TCP ports and X11 connections, while file transfer can be performed using the associated SFTP (Secure File Transfer Protocol) or SCP (Secure Copy Protocol) protocols. By default, an SSH server listens on the standard TCP port 22.

The SSH suite includes three utilities (slogin, ssh, and scp), which are secure versions of earlier insecure UNIX utilities (rlogin, rsh, and rcp). SSH uses public-key encryption to authenticate the remote computer and allow it to authenticate the user, if necessary.

2. Tunnelling

Tunnelling provides a private access route that only authorised users can use. This is particularly useful on public networks. Although everyone uses a public network, not everyone has the right to see what is passing through the tunnel. The data to be transferred may be frames from another protocol. Rather than sending a frame directly, it is encapsulated in another frame, which is responsible for implementing the tunnel. The additional header provides routing information so that the payload of this new packet can pass through the tunnel. Tunnelling involves the phases of encapsulation, transmission and decapsulation of data.

It establishes connections that are protected from malicious individuals seeking to infiltrate a network. Tunnelling can be applied to layers 2 or 3 of the OSI model, depending on the implementation systems. At layer 2, the PPTP and L2TP protocols encapsulate and decrypt the payload in a PPP frame and send it through an intermediate network.

2.1.1. VPN architecture

Table 1: VPN architecture

Communication layers	Security protocols
Application layer	SSH, S/MIME, PGP
Transport layer	SSL, TLS, WTLS
Network layer	IPsec, MPLS
Data link layer	PPTP, L2TP
Physical layer	Scrambling, Hopping, Quantum Communications

2.2. Types of VPN

There are several types of VPNs operating on different layers of the OSI model. These VPNs are PPTP VPN, L2TP VPN, SSTP VPN, VOIP VPN, SSH VPN, SSL VPN, IPSEC VPN, Site-to-Site VPN, and MPLS VPN. Most VPNs are based on the use of tunnels, which rely on the use of a public network, where exchanges are secure. The way it works is by encapsulating the data to be transported in the packets of the protocol creating the tunnel. PPTP VPN is easy to set up and offers basic online security with fast speeds. PPTP is integrated into a wide range of desktop and portable devices and features 128-bit encryption.

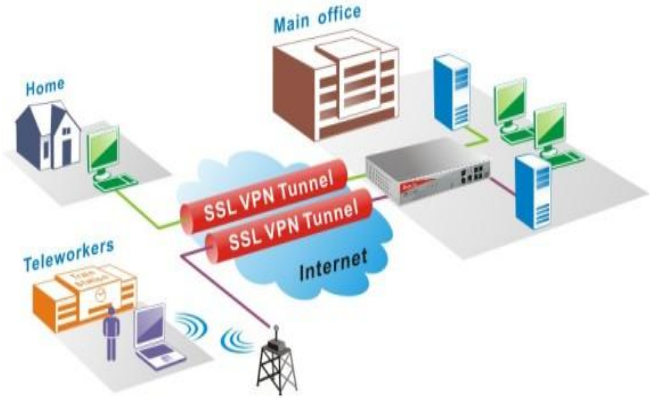

Figure 1: SSL VPN

SSTP VPN is a type of VPN tunnel that provides a mechanism for encapsulating PPP traffic over the SSL channel of the HTTPS protocol. MPLS VPN is a solution provided by specialised operators, and only sites connected by the VPN can communicate with each other.

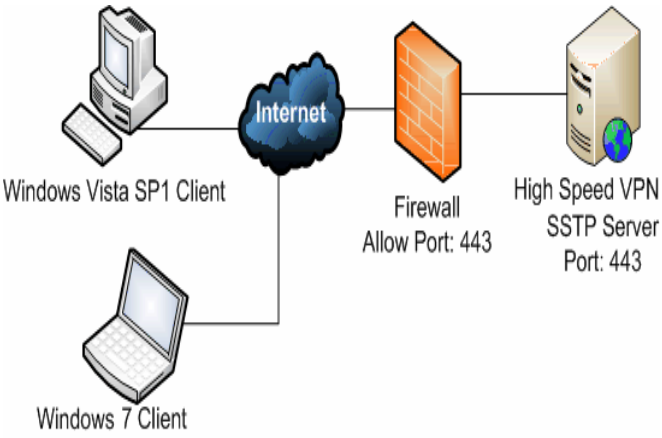

Figure 2: SSTP VPN

IPESEC VPN is the creation of a VPN based on internet connections provided by an operator. Only configured sites can communicate with each other. This requires the hosting of computer servers at each site.

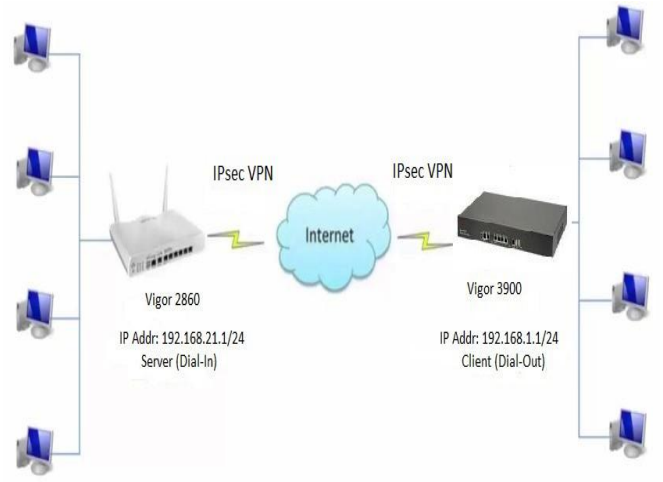

Figure 3: IPSEC VPN

Site-to-site VPNs are also known as router-to-router VPNs, and are mainly used for commercial operations. As many companies have national and international offices, a site-to-site VPN is used to connect the main office network to the rest of the offices. This type of VPN is based on an intranet.

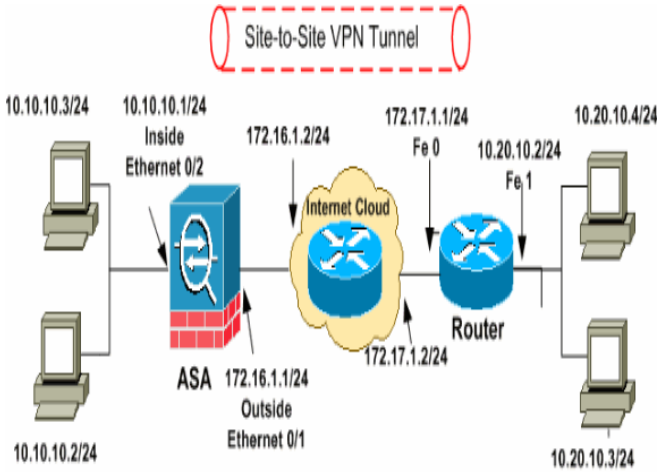

Figure 4: Site-to-site VPN

2.2.1. Comparison table between MPLS/IPSEC VPNs

Table 2: Comparison between MPLS VPN and IPSEC

	MPLS	IPSEC
Quality of service	Lower than Frame Relay and ATM networks but higher than other IP VPNs.	Low due to transfer via the public Internet domain
Security	Comparable to the security offered by existing ATM and Frame Relay networks.	Total security thanks to the combination of digital certificates and PKI for authentication, as well as a range of encryption options, including triple DES and AES.
Compatible applications	All applications, including mission-critical enterprise software requiring high quality of service and low latency, and real-time applications (video and voice over IP)	Secure remote and mobile access. IP applications, including email and Internet. Not suitable for real-time or high-priority traffic
Scope	Depends on the service provider's MPLS network	Very extensive, as it is based on Internet access
Scalability	High scalability since it does not require peer-to-peer interconnection between sites and standard deployments can support tens of thousands of VPN connections	Larger deployments require careful planning to address issues such as site-to-site interconnection and peering
Management costs	No processing required by routing	Additional processing for encryption and decryption

3. Redundancy protocols

Redundancy is the duplication of an element essential to the normal functioning of the computer system, with a view to compensating for the possible failure of this element and thus ensuring the continuity of a vital computer function.

Advantages:

- ✓ Computer networks are becoming increasingly large and logical
- ✓ LANs are no longer geographically limited
- ✓ All LANs have a gateway
- ✓ A gateway is always a router

3.1. Router redundancy

One way to eliminate a single point of failure at the default gateway is to implement a virtual router. To implement this type of router redundancy, multiple routers are configured to work together, presenting the illusion of a single router to the hosts on the LAN.

3.2. Steps for router failover

When the active router fails, the redundancy protocol assigns the active router role to the standby router. Here is the procedure in the event of an active router failure:

- ✓ The standby router stops seeing Hello messages from the forwarding router
- ✓ The standby router assumes the role of the transport router
- ✓ Since the new transport router takes over the IP address and MAC address of the virtual router, host devices experience no interruption in service.

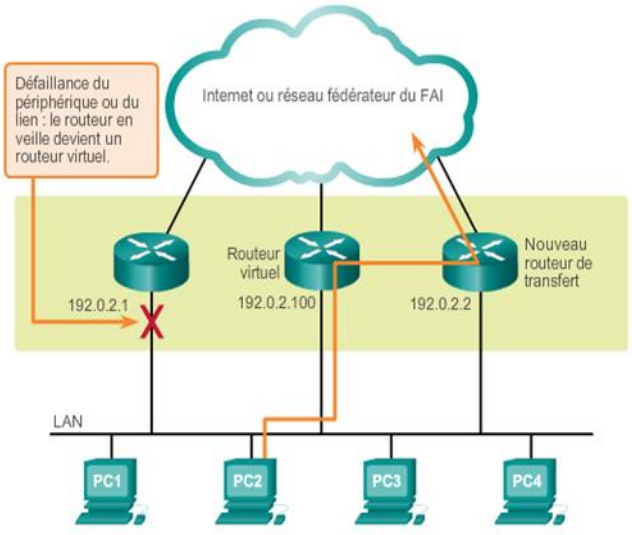

Figure 5: Steps involved in router failover

3.3. First-hop redundancy protocols

The ability of a network to perform dynamic recovery after the failure of a device acting as the default gateway is called first-***hop redundancy***.

- ❖ **HSRP Protocol**: (Hot Standby Router Protocol) Cisco's proprietary HSRP protocol, designed to enable transparent failover of an IPv4 device at the first hop.
- ❖ **VRRP Protocol**: At a time when high availability is one of the key words in networking, the VRRP (Virtual Router Redundancy Protocol) increases router availability during large data transfers within the same subnet.
- ❖ **GLBP Protocol**: The goal is always the same: to create redundancy on the gateway, using at least two routers. However, GLBP (Gateway Load Balancing Protocol) introduces a new feature***: load balancing***. This makes it possible to distribute the load between our different routers.
- ❖ **STP Protocol**: The STP (Spanning Tree Protocol) is a Layer 2 protocol that works on bridges and switches. The STP protocol specification is IEEE 802.1D. The main purpose of the STP protocol is to ensure that you do not create loops when you have redundant paths in your network. Loops are fatal for a network.

When different types of protocol are used in switches, this creates timing problems between the blocking and forwarding states. Therefore, it is recommended that you use identical types of STP protocol.

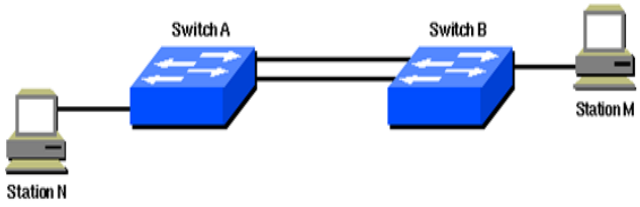

Figure 6: Redundant link between switch A and B

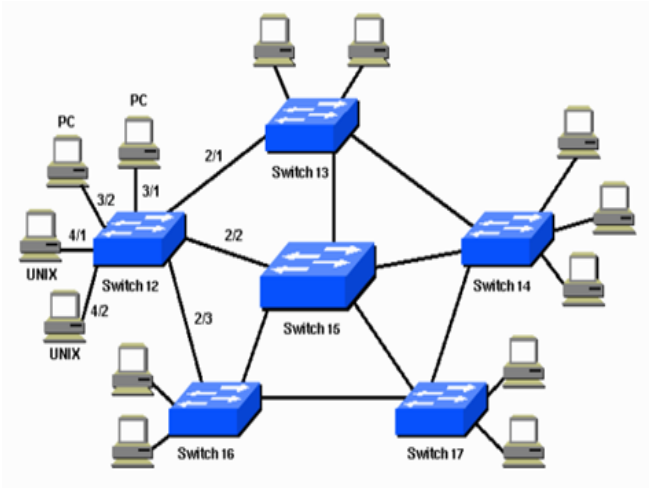

Figure 7: STP protocol network diagram

The following information applies to the scenario in the network diagram:

- ✓ Switch 15 is the primary switch.
- ✓ Switches 12, 13, 14, 16, and 17 are connected to workstations and PCs.
- ✓ The network defines the following VLANs: 1200201202203204
- ✓ The domain name for the VTP (Virtual Local Area Network Protocol) is STD-Doc.

Remember that a root switch is identified for each VLAN. After the root switch is identified, the switches adhere to the following rules:

- ✓ **STP Rule 1**: All ports on the root switch must be in forwarding mode.
- ✓ **STP Rule 2**: The root port must be placed in forwarding mode. In addition, the switches in each LAN segment communicate to determine which one is best suited to move data from that segment to the root bridge. This switch is called the designated switch.
- ✓ **Rule 3 STP**: In a single LAN segment, the port on the designated switch that connects to that LAN segment must be placed in forwarding mode.
- ✓ **STP Rule 4**: All other ports on all switches (VLAN-specific) must be placed in block mode. This rule applies only to ports connected to other bridges or switches. The STP protocol does not affect ports connected to workstations or PCs. These ports remain forwarded.

4. Setting up topologies and testing

4.1. Introduction to the Cisco Packet Tracer simulator

Packet Tracer is software developed by CISCO that allows users to build a virtual physical network and simulate the behaviour of network protocols on that network. Users build their network using equipment such as routers, switches and computers. This equipment must then be connected using various cables and fibre optics. Once all the equipment is connected, it is possible to configure the IP addresses of the available services for each piece of equipment.

4.2. Installing the Cisco Packet Tracer simulator

Get Packet Tracer 7.1.1. The download is available on the official Cisco Academy website.

https://www.netacad.com/courses/packet-tracer-download/. This requires registration. Then proceed to the download page

https://www.netacad.com/group/offerings/packet - the tracer/

1. Download Cisco Packet Tracer 7.1.1
2. Run the installer and follow the on-screen instructions to complete the installation.
3. You will be asked to log in to your Cisco Networking Academy account. If you do not have an account, you can also log in as a guest.

Figure 8: Downloading Cisco Packet Tracer

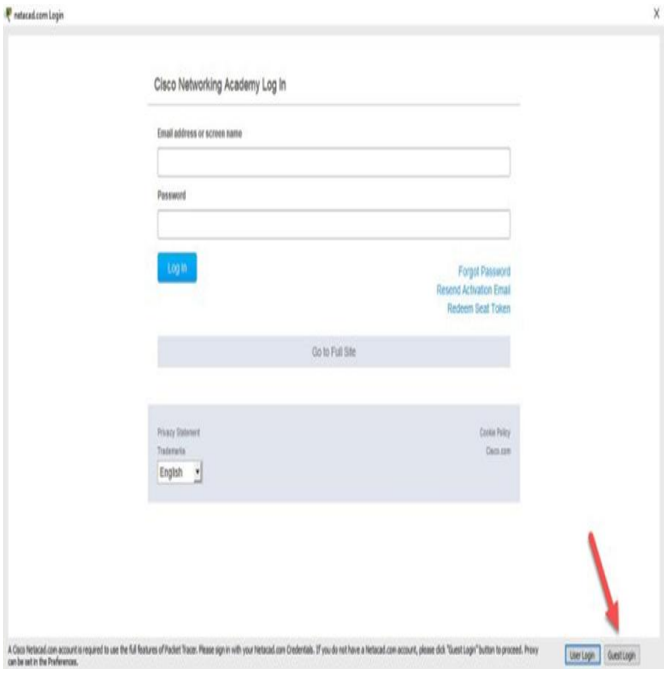

Figure 9: Accessing the Cisco Networking Academy platform

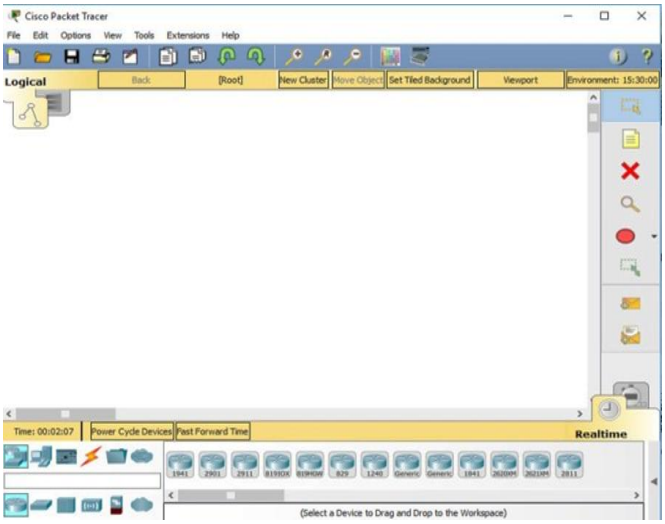

Figure 10: Packet Tracer interface

4.3. Topology equipment

- ✓ **The Router:** is a piece of computer network communication equipment designed for routing. It is responsible for transmitting packets across different networks and determining the next network node to which a data packet should be sent.
- ✓ **The Switch**: Cisco EtherSwitch modules offer businesses the ability to integrate switching and routing on a single platform. They combine Layer 3 WAN network routing with non-blocking Layer 2 switching.
- ✓ **The Firewall**: A firewall is a computer tool (hardware and/or software) designed to protect a computer or computer network from intrusions from a third-party network (particularly the Internet).

4.3.1. Topology implementation and testing

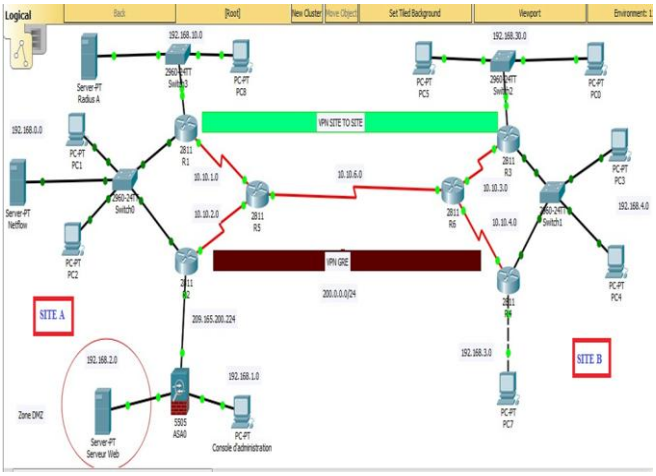

Figure 11: Implementation of a site-to-site VPN

The figure above shows the topology designed to meet the company's needs. We have therefore set up three routers at the main site, two of which provide redundancy and failover functions, and the third for the WAN connection. Switches are used to interconnect the equipment.

To enhance security, we created a VPN tunnel between the two remote sites and integrated an ASA firewall to which a demilitarised zone hosting a web server is connected.

Several IP addresses were used in the project, as shown in the following tables:

Site: A

Table 3: IP addresses for Site A

	Interfaces	Adresse IP	Adresse Masque	Passerelle
R1	F1/0	192.168.10.1	255.255.255.0	
	F0/0	192.168.0.2	255.255.255.0	
	S2/0	10.10.1.1	255.255.255.252	
R2	F0/0	192.168.0.3	255.255.255.0	
	F1/0	209.165.200.225	255.255.255.248	
	S2/0	10.10.2.1	255.255.255.252	
R5	S2/0	10.10.1.2	255.255.255.252	
	S2/2	10.10.6.1	255.255.255.252	
	S2/1	10.10.2.2	255.255.255.252	
PC1	NIC	192.168.0.4	255.255.255.0	192.168.0.1
PC2	NIC	192.168.0.5	255.255.255.0	192.168.0.1
PC8	NIC	192.168.10.2	255.255.255.0	192.168.10.1
PC6	NIC	192.168.1.2	255.255.255.0	192.168.1.1
SERVEUR RADIUS	NIC	192.168.10.3	255.255.255.0	192.168.10.1
SERVEUR Web	NIC	192.168.2.10	255.255.255.0	192.168.2.1
VPN GRE R2	TUNNEL S2/0	200.0.0.1	255.255.255.0	

Table 4: IP addresses for Site B

	Interfaces	Adresse IP	Adresse Masque	Passerelle
R3	F1/0	192.168.30.1	255.255.255.0	
	F0/0	192.168.4.2	255.255.255.0	
	S2/0	10.10.3.2	255.255.255.252	
R4	F0/0	192.168.4.3	255.255.255.0	
	F1/0	192.168.3.1	255.255.255.0	
	S2/1	10.10.4.2	255.255.255.252	
R6	S2/0	10.10.3.1	255.255.255.252	
	S2/2	10.10.6.2	255.255.255.252	
	S2/1	10.10.4.1	255.255.255.252	
PC3	NIC	192.168.4.4	255.255.255.0	192.168.4.1
PC4	NIC	192.168.4.5	255.255.255.0	192.168.4.1
PC7	NIC	192.168.3.2	255.255.255.0	192.168.3.1
PC5	NIC	192.168.30.2	255.255.255.0	192.168.30.1
VPN GRE R4	TUNNEL S2/1	200.0.0.2	255.255.255.0	

Conclusion

This work, consisting of a study and implementation of a high-availability site-to-site VPN architecture, is now complete. This vast and complex project has highlighted the importance of having a secure VPN network in a company. From security concepts to security mechanisms, a company must have a security policy that is tailored to its activities and needs.

Our VPN-based security policy has enabled us to set up a complex and extensive network on the Packet Tracer environment. This network, consisting of six (6) routers, supports three VPNs that we have developed. An IPSEC AH Transport Mode VPN, an IPSEC ESP Tunnel Mode VPN, and an IPSEC AH/ESP Transport Mode VPN. The implementation of these VPNs on our network secured the packets exchanged between the different routers and tunnels.

The IPSEC AH Transport mode VPN partially secures communication because the AH protocol encrypts only part of the packet (the header). This VPN was created with a tunnel over IPSEC to secure the data exchanged, added to an ISAKMP security policy, a GRE access list and an IPSEC profile. This VPN is used in many cases between two workstations for an end-to-end connection. With this VPN, authentication and integrity are ensured. The IPSEC ESP Tunnel mode VPN was configured between the edge routers to enhance security. It required an ISAKMP security policy and an *IPSEC transform set* to associate the peers, which are the addresses of the router interfaces when it comes to tunnelling.

We have seen that the HSRP and VRRP redundancy protocols are very similar. GLBP provides load balancing, and STP works on bridges and switches. Even if the load is not perfectly balanced, the concept is nonetheless interesting.

Thanks to today's Internet connections, VPN solutions are more than reliable and allow relatively small businesses to access advanced features. Setting up a VPN requires rigour, as it is actually a combination of three technologies (encryption, routing and firewalling). If you don't pay attention, you can quickly leave yourself open to major security breaches.

IPSEC ESP Tunnel mode VPN encrypts the entire packet, unlike ESP. IPSEC AH/ESP Transport mode VPN is a combination of the first two VPNs, as it ensures the integrity, authentication and encryption of data or packets.

Finally, a hacker sniffing the network will not be able to decrypt anything since everything is encapsulated with ESP and authenticated with AH. Data flows securely within the tunnel, but outside the tunnel (outside the access list) nothing is encrypted, and data is transmitted in clear text. The choice of VPN is therefore based on our needs and costs.

References

http://biblio.univ-antananarivo.mg/pdfs/randretsamalalaHenintsoaV_ESPA_MAST_18.pdf

https://dspace.ummto.dz/server/api/core/bitstreams/7901d846-1d1c-4d20-99b9-05de8b02f1b7/content

https://fr.slideshare.net/slideshow/mise-en-place-d-un-vpn-sitetosite-au-sein-d-une-entreprise-cas-de-la-soroubat-socit-de-routes-et-btiments/151521827

BM Lounas (2023). *Design and implementation of an automation solution for network service migration with secure remote access*. https://dspace.ummto.dz/items/01783a5f-c5ed-4c2c-ad0c-64a945b7d54e

G Anis (2016). *Implementation of a VPN solution to secure a company's network < CASE: ENIEM*. https://www.ummto.dz/dspace/bitstream/handle/ummto/12426/GaouaouiAnis.pdf?sequence=1

S Helali (2022). *Integration of network infrastructures and systems: Design, implementation, security and supervision*. https://books.google.com/books?hl=en&lr=&id=jSxVEAAAQBAJ&oi=fnd&pg=PP1&dq=VPN+Site-to-

Site+haute+disponibilit%C3%A9+architectures&ots=g_qnwnndrU&sig=Xaf3T_A7SGayOpRootQZn4iVyJQ

SM Diène (2021). *Design and implementation of a secure architecture for a multi-site enterprise network.* http://rivieresdusud.uasz.sn:8080/handle/123456789/1432

S Sonia (2014). *Implementation of a VPN Site-to-Site interconnection with ASA Cisco*. https://www.ummto.dz/dspace/bitstream/handle/ummto/12783/SaadSonia.pdf?sequence=1