Different ways of connecting branch office

Ella Parviainen

Haaga-Helia University of Applied Sciences

Bachelor's Thesis

2021

Bachelor of Business Administration

Abstract

Author
Ella Parviainen

Degree
Bachelor of Business Administration

Thesis title
Different ways of connecting branch office

Number of pages
36

Secure connections have a central role in business. In order to perform safe business, the daily data communications need to be in place and established securely to have a smooth working experience. A secure site-to-site connection is essential for communication in a workplace. Emerging technologies need to function together with the ones that are already in use.

This thesis examines three different ways of creating a site-to-site connection. The connection methods studied are IPSec, MPLS and SD-WAN. The functionalities of these three options are explored to find out the requirements for each connection method from a technical point-of-view. These connection methods are then compared to find out the differences and practicalities.

A model connection was designed for the target organization. The implementation was designed using IPSec VPN to find out the specific requirements for this type of VPN connection. The IPSec model was designed for the target organization by using EVE-NG and Palo Alto NGFW. The result is a proposed model for IPSec VPN implementation, which can be utilized with SD-WAN in further network development.

The following conclusion was made based on the research of this thesis. The suitable model for an organization's network connection depends on the needs and requirements of the specific organization. Network requirements, organization's needs, devices, technologies, security, knowledge of staff and business needs need to be considered when a network topology is designed. All changes to a network have to be designed securely and properly. A backup connection for a network always needs to be in place to secure business continuity.

Keywords
IPSec, VPN, MPLS, SD-WAN, branch office

Table of contents

1 Introduction

1.1 Background

Security has a great role in business as it has an impact on every aspect in a company. Every business has a strategy, and this strategy must also involve security. Companies need to design their network connection so that it’s secure and enables safe and efficient business. To ensure business continuity, office network connection needs to be easy to maintain and support the business delivery. Technical aspects, including the devices and connection establishment need to be taken into account. Creating a functional VPN site-to-site connection involves careful planning so that it supports the daily needs of work life.

This thesis covers three different ways of connecting a branch office with VPN solutions: IPSec, MPLS VPN and SD-WAN. These solutions are examined to find out the mechanisms and how they are used when connecting a branch office to another corporate site. The aim is to compare these solutions and choose the method for a site-to-site VPN connection that meets the needs of the target organization.

To increase network security, general guidelines on security services must be followed. When it comes to network security, expenses, cost-benefit, controllability, and scalability are aspects that need to be considered when designing organizational network topology. Creating a corporate network site-to-site connection has an impact on delivered services as it supports the organization with creating more efficient business services.

After performing an internship on the target organization of this thesis, I gained more personal interest on network security. An opportunity to explore the possibilities of different VPN solutions, specifically IPSec protocols, in an organizational environment was introduced. The subject of this thesis stems from an organizational need to have a better understanding of VPN mechanisms and resources to connect a branch office to main network site in a different country. This thesis introduces three different ways how a branch office can be connected. An IPSec based solution is then proposed and it is discussed on how it can be used with a SD-WAN environment in the future.

1.2 Objective

The objective of this thesis is to examine the resources that are needed for different VPN connection solutions to work within an organizational environment to establish a secure site-to-site VPN connection. In this thesis, the focus will be on IPSec VPN and what opportunities it has to offer.

1.3 Research questions

The aim of this research is to answer these following questions:

1. What are the mechanisms needed to create a site-to-site VPN connection?
2. What should be considered as a solution for securing VPN connections for this specific organization?
3. Why should SD-WAN based network solutions be considered?

This research examines what needs to be in place for IPSec VPN, MPLS VPN, as well as SD-WAN, to work as a site-to-site VPN solution in an organization. An IPSec VPN model will also be implemented, and it will be tested on a virtual environment to see in practice how it could be used in an organizational environment in the future, together with SD-WAN based network environment.

1.4 Delimitation

MPLS-based SD-WAN architecture will not be covered in this thesis as focus is on IPSec-based VPN. Transport mode will not be covered in this thesis, as the focus will be on tunnel mode-based solution, site-to-site connection.

1.5 Key concepts

AH	Authentication Header; provides authentication and integration in IPSec (Snader 2005)
BGP	Border Gateway Protocol; routing protocol for Internet traffic (Networklessons.com 2021d)
Customer Edge	Communication end on the customer side in MPLS, attached to provider edge (Techopedia Inc. 2021)
DMVPN	Dynamic multipoint virtual private network (Tizazu, Berhe & Kim 2017, 1)
ESP	Encapsulating Security Payload; protocol that encrypts IP traffic (Snader 2005)
EVE-NG	Platform for creating proof of concepts and test environments for corporate networking (EVE-NG 2021a)

Hub-and-spoke Network model where every location is connected through a central location, a hub (The Geography of Transport systems 2021)

IKE Internet Key Exchange; establishes the IPSec tunnel (Networklessons.com 2021a)

IPSec Security protocols for securing IP traffic (Zheng & Zhang 2009, 1)

LDP Label Distribution Protocol; protocol for MPLS label distribution within network (Lucek & Minei 2011, chapter 1.3.1)

Label Switching Path A mesh of tunnels between Provider Edge routers in MPLS network to be able to transport packets (Lucek & Minei 2011, chapter 1.3)

mGRE Generic routing protocol that forwards static unicast, multicast and broadcast traffic (Bahnasse & Kamoun 2015, 1)

MPLS Multiprotocol Label Switching; method for tunneling IP datagrams with labels (Snader 2005, chapter 4.7)

NAT Network Address Translation: method which translates internal IP addresses to public IP addresses to ensure privacy in network (Javvin Technologies 2004, 27)

NHRP Next Hop Resolution Protocol; protocol for determining the public IP addresses in packet routing (Networklessons.com 2021b)

Provider Edge Communication end on the provider side in MPLS network (Techopedia Inc. 2021)

RSVP protocol Resource Reservation Protocol; protocol for label distributing in MPLS (Lucek & Minei 2011, chapter 1.3)

SASE Secure Access Service Edge: cloud-based architecture that combines networking and security (Cato Networks 2021, 3)

SDN Software-Defined Networking

SD-WAN Software-Defined Wide Area Network; next-generation network architecture (Yang, Cui, Li, Liu & Xu 2019, 1-2)

Site-to-site connection A network connection established between two endpoints (Techopedia Inc. 2021)

TCP/IP Transmission Control Protocol/Internet Protocol suite that provides communication for devices across the Internet by delivering data and routing packets (Snader 2005, chapter 2.1)

Tunnel mode Method for securing IP packets in IPSec (Firewall.cx 2018)

VPN Virtual Private Network; secured network that simulates private network functionality (Snader 2005, chapter 5.1)

WAN Wide Area Network; a combination of networks (Cisco 2021)

2 IPSec VPN

This chapter introduces the concept of IPSec VPN. IPSec provides security to Internet Protocol (IP) traffic by encapsulating IP packets at the network layer. (Snader 2005, chapter 9.1) Virtual Private Network (VPN) is a way of building a private network with tunneling, in which the tunnels are encrypted and authenticated. In other words, the aim is to create an illusion of a private network when using the public network. (Snader 2005, chapter 5.1)

2.1 Introduction to TCP/IP

Transmission Control Protocol/Internet Protocol, TCP/IP, is a set of protocols that handles routing of the data packets on the Internet. These protocols provide data delivery, routing, name resolution and network control messaging. TCP/IP stack makes connection across devices on the Internet possible. The four network layers are application, transport, network, and link layer. IP is located in the network layer (2nd layer.) (Snader 2005, 2.1-2.2) Structure of the TCP/IP stack is illustrated in Figure 1.

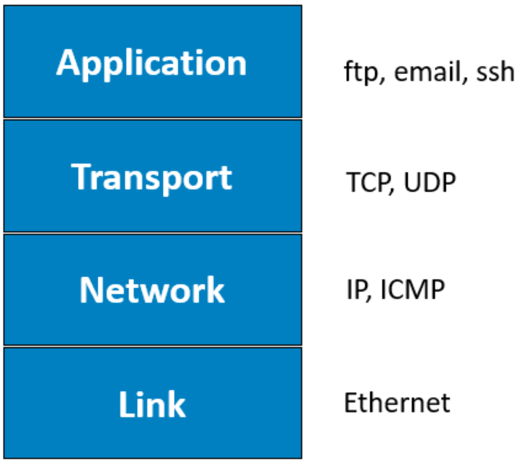

Figure 1. Layers of TCP/IP stack (adapted from Snader 2005, figure 2.1)

2.2 IPSec fundamentals

IP Security (IPSec) is a framework for securing IP traffic. (Networklessons.com 2021a) It is a security protocol that operates on the network layer by providing data authentication and access control. (Zheng & al. 2009, 1) IPSec can be thought to consist of three protocols: Authentication Header (AH), Encapsulating Security Payload (ESP) and Internet Key

Exchange (IKE). The main reason for the design of IPSec tunnels was to respond to latency issues as there was delay on packet delivery between the source and the destination. (Cisco 2019, 2)

2.3 IPSec modes

IPSec can be used in two modes: transport and tunnel mode. These two modes are explained briefly to point out their differences. This thesis will focus on tunnel mode and how it can be implemented with IPSec between two office sites.

2.3.1 Transport mode

Transport mode is not covered in this thesis. However, the concept of transport mode is summarized in this chapter as it’s used in different situations than tunnel mode. Transport mode is used for connection between hosts when the endpoints are two specific hosts, in other words, a host-to-host connection. Transport mode VPNs protect the data in the transport layer in the datagram. (Snader 2005, chapter 10.3, 11, 12.4)

2.3.2 Tunnel mode

Tunnel mode is generally used for establishing a VPN connection between two networks or a host and a network. (Snader 2005, chapter 12.5) This thesis focuses on the usage of tunnel mode as it is generally deployed between two networks in site-to-site connections. The main difference between tunnel and transport mode is that transport mode uses the original IP header. In tunnel mode, a new IP header is used. The difference of tunnel mode and transport mode AH header can be seen in Figure 2.

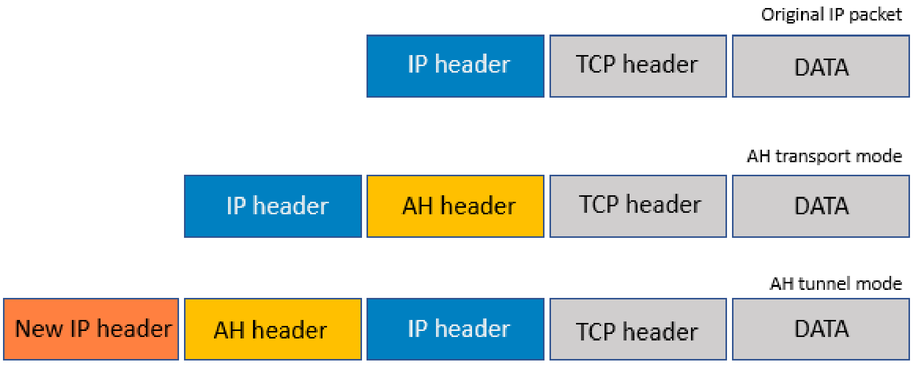

Figure 2. Difference between tunnel mode and transport mode in AH header (adapted from Networklessons.com 2021)

2.4 IPSec header

As mentioned in chapter 2.1, IPSec is a combination of three protocols. One of them is the Authentication Header (AH) that is an IP protocol that provides data integrity, in which authentication and integration are provided by cryptographic MAC over payload and an IP header. AH header consists of the next header field, the payload length, and the reserved field. (Snader 2005, chapter 9 & 11) Figure 3 shows the structure of the Authentication Header in tunnel mode.

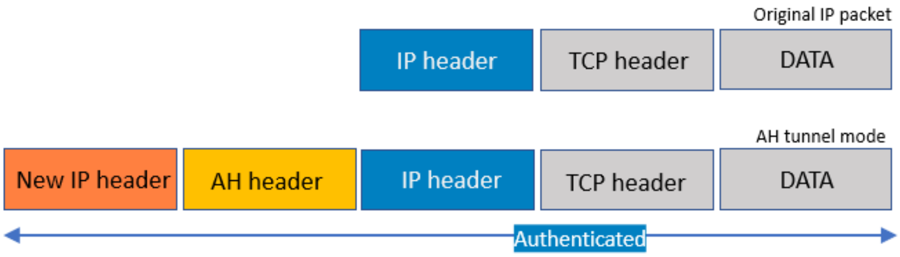

Figure 3. Authentication Header in tunnel mode (adapted from Networklessons.com 2021a)

Encapsulation Security Payload (ESP) is a protocol that provides authentication and data integrity by encrypting IP traffic. It is almost identical to the AH protocol, except placement of data authentication in packets is different. AH and ESP both protect against replay attacks as they include a sequence number in protocol headers. However, ESP also provides IPSec confidentiality due to its encryption methods. ESP should always be authenticated so it is secured from cut-and-paste attacks, and therefore authentication function is included in ESP. However, sometimes AH can be secure enough itself since it provides endpoint authentication and when confidentiality is not required. (Snader 2005, chapter 9, 11 & 12) ESP usage in site-to-site VPN that operates in tunnel mode is illustrated in Figure 4.

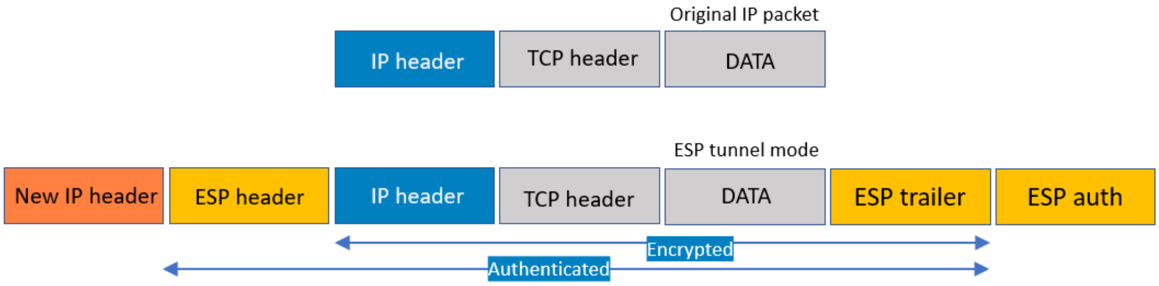

Figure 4. ESP in tunnel mode (adapted from Networklessons.com 2021a)

2.5 IPSec tunnel establishment

The third part of IPSec is the Internet Key Exchange (IKE) protocol. Internet Key Exchange handles IPSec key management as it negotiates security associations by exchanging encryption key information. It also encrypts and authenticates the VPN connection. (Snader 2005, chapter 13.1)

IPSec tunnel is established in two phases. (Snader 2005, chapter 13.1) IKE phase 1 tunnel establishes the session. Encryption and authentication are negotiated in phase 1 and Internet Security Association and Key Management Protocol (ISAKMP) tunnel is established. Phase 1 involves encryption, authentication, and hashing. It is used for management traffic and for creation of IKE phase 2 tunnel. (Networklessons.com 2021a)

After IKE phase 2 - or the IPSec tunnel establishment - that tunnel can be used for protection of user data, that will be sent through IKE phase 2 tunnel. Encryption of the traffic is then created with AH and ESP protocols. (Networklessons.com 2021a) Illustration of IPSec IKE tunnel can be seen in Figure 5.

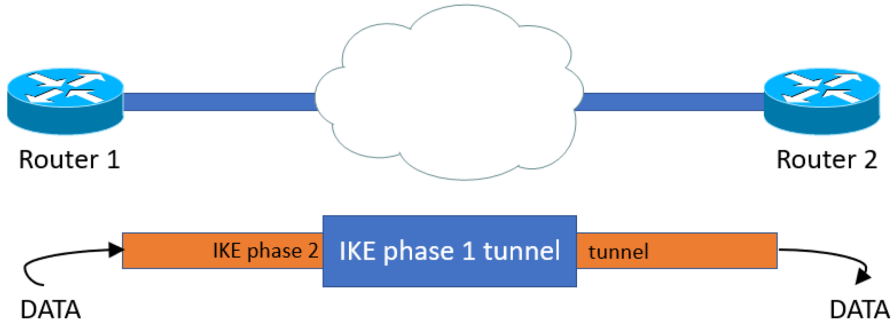

Figure 5. IKE tunnel (adapted from Networklessons.com 2021a)

2.6 DMVPN

Dynamic Multipoint Virtual Private Network (DMVPN) is a routing technique for building VPN networks with multiple sites without the need of static configuration of devices. Encryption of DMVPN can be done with IPSec. It is a hub-and-spoke network that allows the spokes to communicate directly without traffic going through a hub. Multipoint GRE (mGRE) creates tunnels that allow traffic to have multiple destinations. If direct tunnels to offices are needed, mGRE will configure them automatically. (Networklesson.com 2021b) This is illustrated in Figure 6.

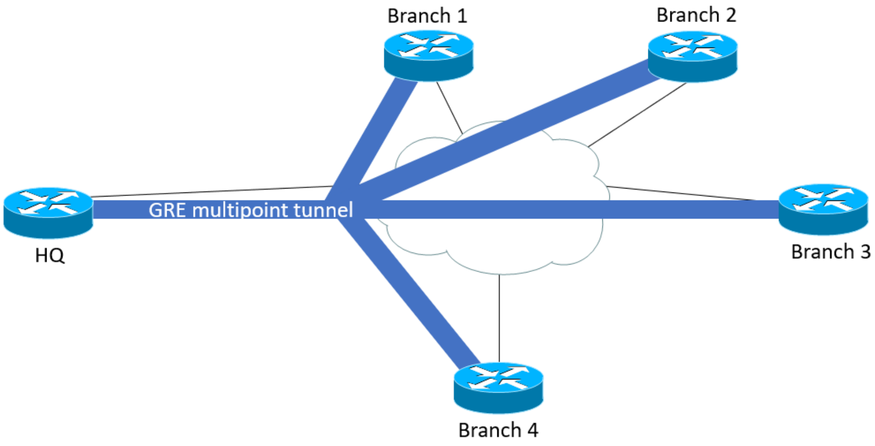

Figure 6. DMVPN GRE multipoint tunnel (adapted from Networklessons.com 2021b)

As seen in Figure 6, Multipoint GRE tunnels allow headquarters to connect to four branch offices. There is one tunnel interface for every router from headquarters. If a direct connection between branch 2 and branch 3 would be needed, a direct GRE tunnel is built between the branches. This is shown in Figure 7.

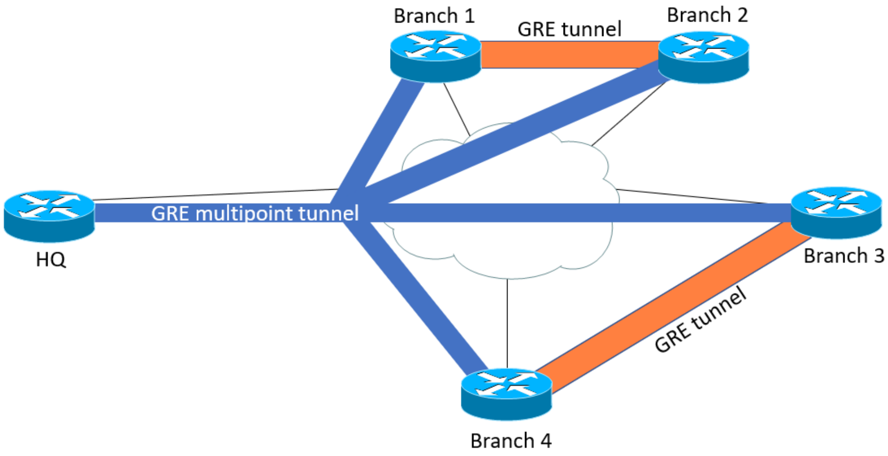

Figure 7. GRE tunnels for direct connection between branches. (Adapted from Networklessons.com 2021b)

DMVPN supports hub-and-spoke and spoke-to-spoke models. It offers the same routing protocols as legacy networks, including network topology information and change notifications on links. When configured, corporate private IP addressing must be considered. (Tizazu, Berhe & Kim 2017, 2) Next Hop Resolution Protocol (NHRP) provides help for routers to determine the public IP addresses to be able to route packets. (Networklessons.com 2021b)

For example, router A needs to determine the public IP address to be able to route the traffic to branch office router B. Router A will work as a NHRP server and the other router(s) will work as NHRP client(s). NHRP client registers with the NHRP server by reporting its public IP address. NHRP servers keeps track of the addresses in cache and when traffic routing is needed, a router will request NHRP server for the public IP addresses of the other routers (Networklessons.com 2021b).

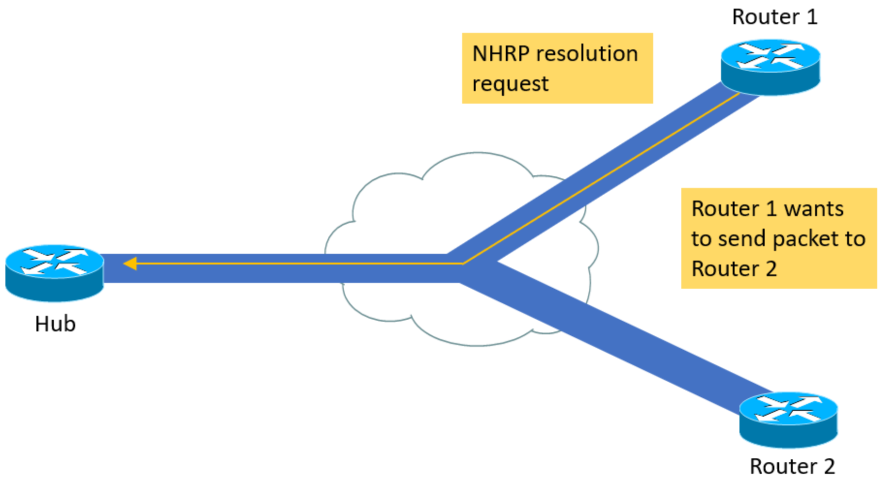

Figure 8. NHRP resolution request for public IP address (adapted from Networklessons.com 2021b)

Router 1 wants to send an IP packet to Router 2. Router 1 needs the public IP address to reach Router 2. Router 1 creates a NHRP resolution request to Hub to get the public IP address information, which can be seen in Figure 8. Hub collects the information of IP addresses in cache. Hub replies with a NHRP request reply (Figure 9) and gives public IP address to Router 1. Router 1 receives the address and is now able to send IP packet to Router 2 (Figure 10).

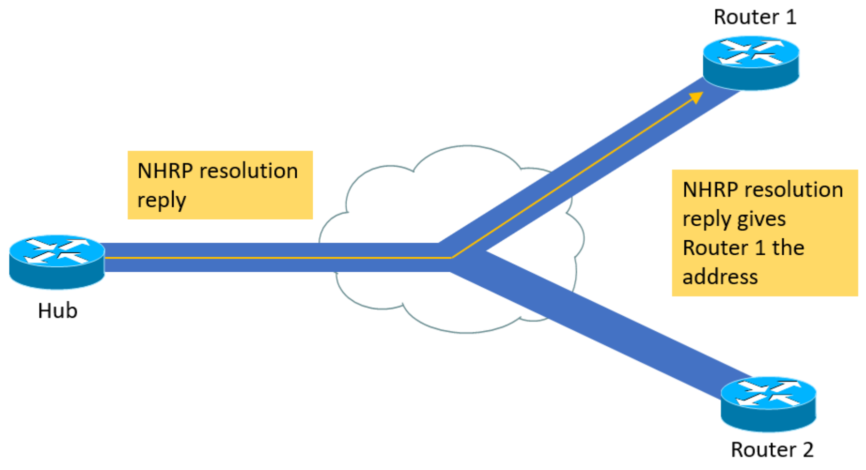

Figure 9. NHRP resolution reply (adapted from Networklessons.com 2021b)

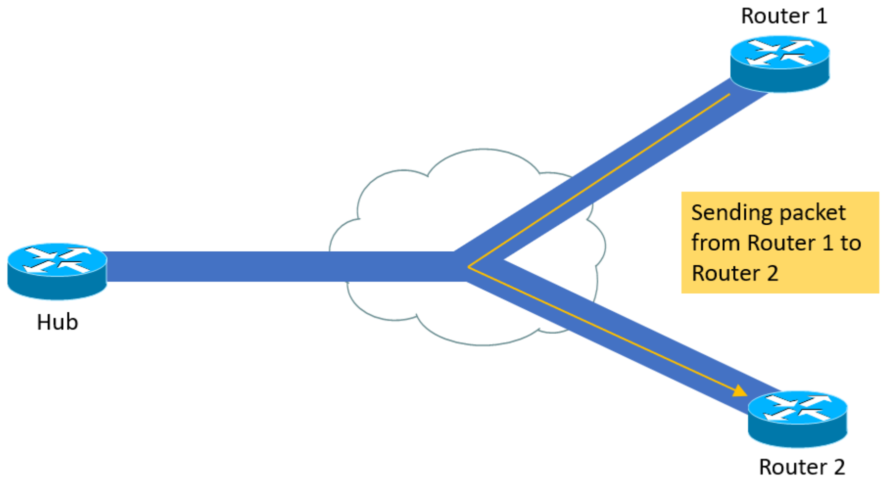

Figure 10. Sending an IP packet after NHRP resolution reply (adapted from Networklessons.com 2021b)

DMVPN builds a dynamic tunnel where each spoke establishes an IPSec tunnel into the hub. A second hub router is then used, which allows high availability for services. DMVPN enables IPSec VPN to scale better, which reduces latency and enhances performance for site-to-site communications. (Tizazu, Berhe & Kim 2017, 1)

2.7 IPSec usage

IPSec can be used between two routers to establish a site-to-site VPN connection. It can also be used between a firewall and a host for remote VPN connection. (Networklessons.com 2021a) The purpose of dynamic IPSec tunnels is to reduce latency and jitter. The packets pass through a shorter physical distance and fewer network devices, each of which can have an impact on delay in packet delivery. However, congestion levels and number of elements in the network have an impact on latency as well. That is why the extent of the performance benefits with IPSec tunnels depends on the local network topology that is deployed within the company and between the sites. (Cisco 2019, 2, 8)

3 MPLS VPN

This chapter introduces the MPLS fundamentals as well as its usage with VPN. Multiprotocol Label Switching (MPLS) is a network technology that has been used for several years. It is different from IP forwarding since it uses labels that are inserted to the packet instead of using a routing table. MPLS supports multiple protocols, such as IP. (Towards Datascience 2021)

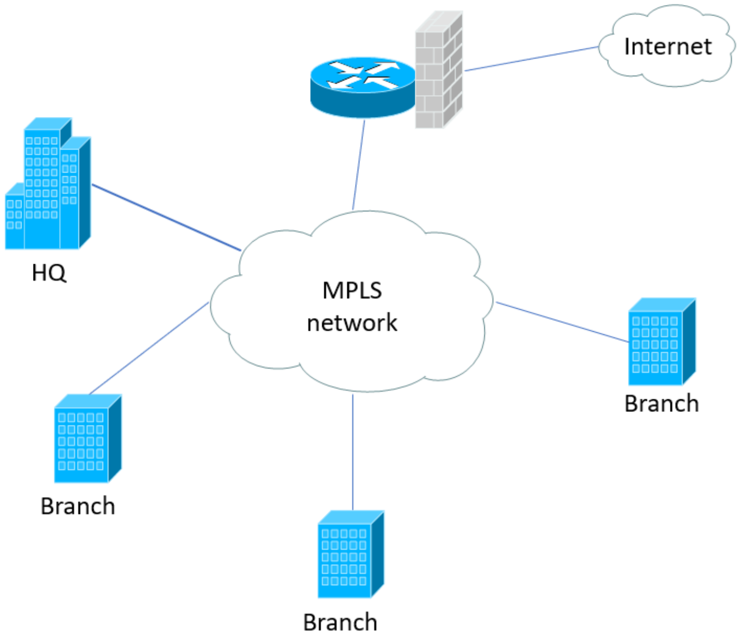

Figure 11. MPLS network (adapted from Networklessons.com 2021a)

As illustrated in Figure 11, MPLS network architecture involves MPLS connections to the main site and branches. Through the main site, branch offices get connectivity to the Internet through a router and a firewall. Remote home office connection is established in the same manner through main site connections.

3.1 BGP

Border Gateway Protocol (BGP) is a routing protocol used for Internet traffic. (Networklessons.com 2021d) Service Provider devices need to use BGP in order to be able to route traffic. The network is built with Customer Edge and Provider Edge that exchange prefixes. Therefore, all devices need to use BGP to forward packets within the network. However, all devices do not need to have that forwarding information. By building a GRE tunnel between Provider Edge routers, only these PE devices know where the traffic needs to be routed. This allows a BGP free core network. (Networklessons.com 2021c) An MPLS network with GRE tunnel core is illustrated in Figure 12.

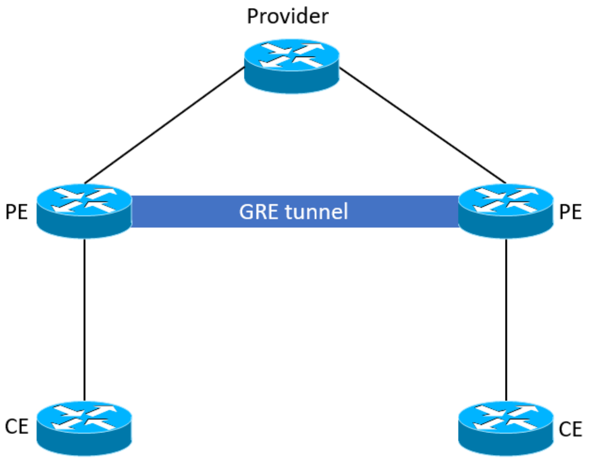

Figure 12. An MPLS network with GRE tunnel (adapted from Networklessons.com 2021c)

As can be seen in Figure 12, there are two customer edge routers as well as two provider edge routers. There is a GRE tunnel between the provider edge routers to provide the routing information for the network traffic. These PE routers are then connected to the Provider where the traffic is maintained.

3.2 MPLS header

Data has one or more MPLS headers applied when moving within a network. MPLS header structure consists of the following fields: label value, traffic class (TC), bottom of stack bit (S-bit) and time-to-live (TTL) field. MPLS packet forwarding is based on the label value field and is used as an index in MPLS forwarding table. Traffic class (TC) can then be used to determine where a packet should be placed. It is used by Provider (P) routers and Provider Edge (PE) routers. S-bit is situated in the MPLS header at the bottom of the stack and the TTL field is used for example in path-tracing and for avoiding forwarding loops. The structure of the MPLS header can be viewed in Figure 13. (Lucek & Minei 2011, chapter 1.3.1)

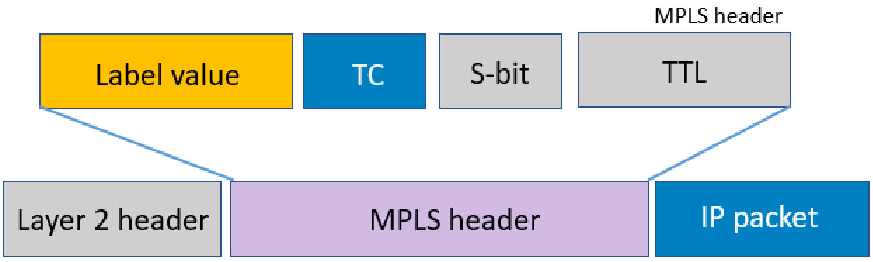

Figure 13. MPLS header structure (adapted from Towards Data science 2021)

Packets that arrive to the network have at least one MPLS header that is applied by the ingress Provider Edge (PE) router. The ingress PE router then identifies the egress PE to which the packet hast to be sent. The value of the label corresponds to the Provider (P) router where the packet is located at. Then, the next router looks up the label value and defines the output label that is used for the next part in the Provider router. By swapping labels, the packet is transported from ingress to egress Provider Edge. (Lucek & Minei 2011, chapter 1.3.1)

When public IP traffic is transported in the network, use of a one MPLS label is sufficient, but in other cases, multiple MPLS headers are needed. That is because Provider Edges in a network are working with multiple services, such as layer 2 and layer VPN. Therefore, the egress PE needs to know to which instance of the specific service the packet belongs to. This can be achieved with the MPLS header that is applied with ingress PE. Ingress Provider Edge learns which labels to use by using RSVP or LDP signaling protocols. (Lucek & Minei 2011, chapter 1.3.1)

An overview of an MPLS network is illustrated in Figure 14.

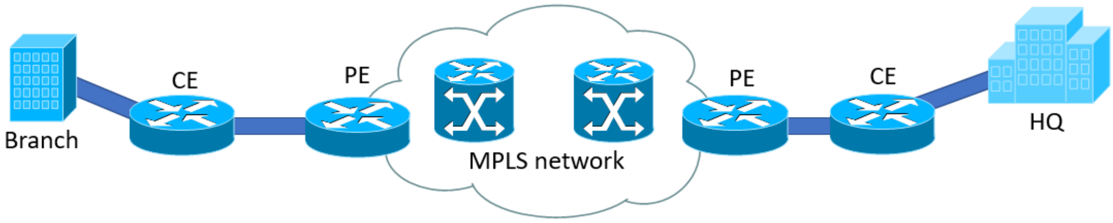

Figure 14. An MPLS network overview (adapted from Kolhar, Abualhaj & Rizwan 2016, 236)

MPLS handles the traffic routing by using labels in the Provider Network. Provider Edges (PE) 1 and 2 transport the traffic to the Customer Edges (CE) within the Provider Network.

3.3 MPLS functionality

The MPLS VPN can be accessed through a customer edge (CE) router that is connected to a provider edge (PE) router. With MPLS VPN, the same IP addresses can be used in different networks. Communication between two customer networks that share the same address needs to be distinguished. Network Address Translation (NAT) is not necessary with MPLS as the traffic is tunneled. (Snader 2005, chapter 4)

MPLS finds the destination router by using its label-switching paths. The destination router then applies a label based on that information and delivers the packet via routing. (Mitchell 2018, 4) MPLS allows multiple protocols to be tunneled, such as IP, IPv6, and Ethernet traffic. (Networklessons.com 2021c)

MPLS network can be used to tunnel several traffic types through the core of the network. (Lucek & Minei 2011, chapter 1.3) MPLS operates between layer 2 and layer 3 which is why it can sometimes be referred to as layer 2.5 protocol. It can be used in online services, such as VoIP (Voice over IP), because it offers reliability. With MPLS, network traffic can be prioritized. (Mitchell 2018, 4-5) For example, if some traffic is of higher priority, it can be set to a lower number to indicate a higher priority.

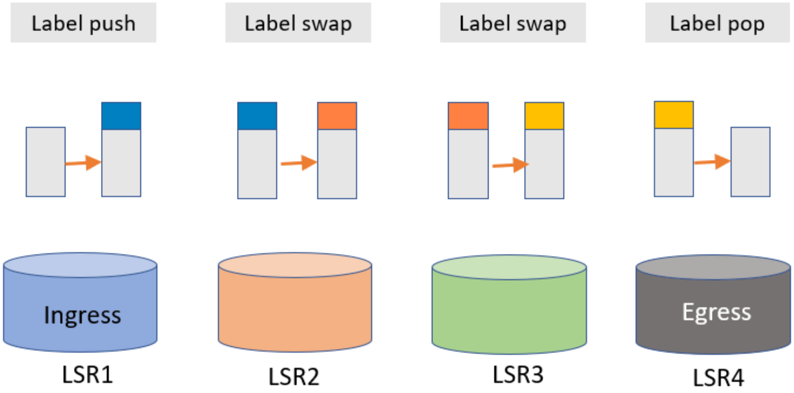

Figure 15. MPLS label switching (adapted from Towards Data science 2021)

MPLS operates by switching labels, which is illustrated in Figure 15. A mesh of tunnels is built between the routers so they can have access to the network. (Lucek & Minei 2011, chapter 1.3) First the label is pushed at the ingress point, which serves as a receiving end for IP packets. (Towards Datascience 2021) Ingress router determines the class that the packet belongs to. Packets that are put to the same class are forwarded to the same egress path. They are then forwarded with the same MPLS label to the next router. (Lucek & Minei 2011, chapter 1.3) The egress router is at the end of the MPLS network and pops the label of the incoming packet and forwards it as an IP packet. These ingress and egress routers are also known as edge routers. (Towards Datascience 2021)

4 Software-Defined Networking

This chapter introduces the key concepts of Software-Defined Networking. SD-WAN functionalities and its place in a corporate network are discussed. This chapter touches the topic of the possibilities of SD-WAN deployment in a corporate network.

4.1 About Software-Defined Networking

Software-Defined Networking is a network architecture for creating a flexible and manageable network. (Cisco 2021) The aim of Software-Defined Networking (SDN) is to cut down costs by virtualization, automation and making networks simpler with network customization. There are three key principles connected to SDN: separation of physical and virtual layers, connection from physical to logical aspect, and automation of processes that are carried over the network. (Pujolle 2020, chapter 2.1)

Five domains, which are network, storage, computing, security, and management & control are necessary to have within a company to form a functional system. These five domains can be put in a cloud environment that are distributed into datacenters. (Pujolle 2020, chapter 2.1) This creates a software-defined network that is easily manageable.

4.2 SDN architecture

The general SDN architecture consists of three layers: data, control, and application layer. Separation of data and control to their own layers allows network management to have more flexibility. (Yang & al. 2019, 2) Standardization for SDN has been made by the Open Networking Foundation. They proposed general guidelines for SDN architecture which can be seen in Figure 16.

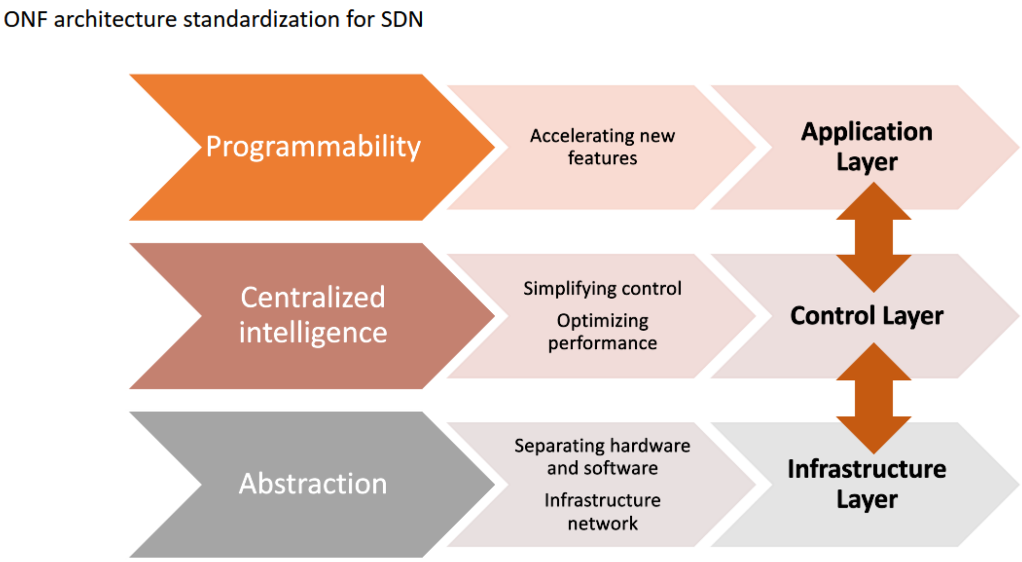

Figure 16. ONF architecture standardization for Software-Defined Network (adapted from Pujolle 2020, chapter 2.2, figure 2.5).

The bottom layer, abstraction, includes infrastructure and a logical layer that are separated from each other. Abstraction involves data transport, protocols and algorithms that enable the transportation of IP packets. The second layer, control layer, involves effective data control. This layer also includes configuration of network such as firewalls, authentication servers and other operational aspects. The top layer, application layer, includes applications that are needed by clients, storage, computation, and security. From this layer programmability information is delivered to the control layer where software networks and applications communicate. (Pujolle 2020, chapter 2.2)

4.3 Software-Defined Wide Area Networking

Software-Defined Wide-Area Networking, SD-WAN, is a next-generation architecture for wide area network, which transfers data over long-distance (Yang & al. 2019, 1-2), for example from Europe to another continent. SD-WAN offers new viewpoints on building network. Enterprise networks are one example of WAN that is critical to information security. SD-WAN simplifies connections site-to-site, such as branch offices in enterprise networks by providing flexibility and centralized control (Yang & al. 2019, 1-2).

The key elements of SD-WAN are that it provides controlled applications by host, bringing Quality of Experience (QoE), as well as centrally defined network policy without the need of having to manually configure each device. (Yang & al. 2019, 1) SDN allows management of data centers which is needed while the number of virtual machines is increasing rapidly. An SDN application called network virtualization provides scalability for data centers. By virtualizing, service providers can manage end-to-end services on virtual network and allow hardware to be implemented as software. (Mitchell 2018, 13) This would reduce the need of having to configure new devices on-site, creating a coherent information environment. It allows network management to be more simplified and quickens the pace of network upgrades. (Yang & al. 2019, 1) SD-WAN can also work well with the Internet of Things (IoT) as it works as a backbone to IoT and provides support for automatic systems that would not be impacted by packet loss. (Mitchell 2018, 22)

4.4 WAN usage and corporate network

SD-WAN network involves branch office site that is connected to the corporate data center. To be able to connect these two, the WAN connection, the Internet and the MPLS services would need to be connected within cloud services to be able to manage the branch sites over IP and MPLS traffic. This can be seen in Figure 17.

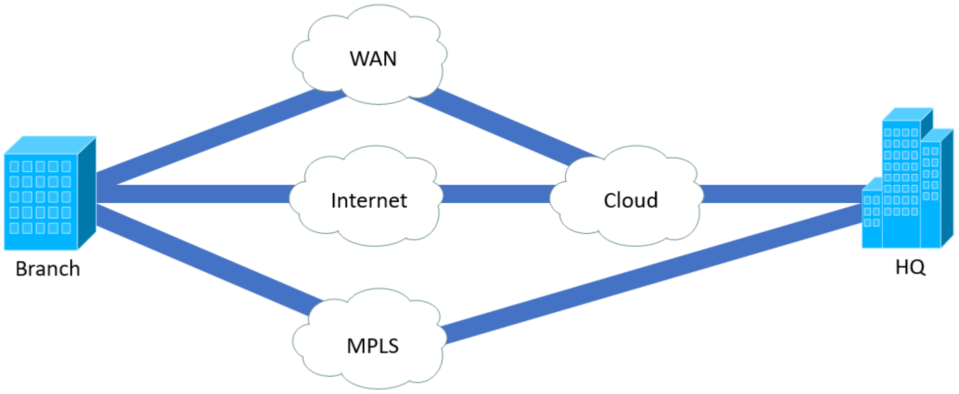

Figure 17. Basic SD-WAN corporate network architecture (adapted from Juniper Networks 2021)

To perform upgrades on network devices, configuration has to be done manually. As network entities tend to be large, they require planning and preliminary work when an update is needed as network devices and requirements change rapidly. Having to perform these manual changes result in configuration errors (Yang & al. 2019, 2). Managing network to respond to the growing world of IT is a huge challenge. As data grow fast, manual approaches are not enough to keep up with the pace. 95 % of changes made to network are still made manually which results in operational costs. Increasing automation through SD-

WAN-based solutions keeps the business up to date and increases efficiency and service quality. (Cisco 2020, 26)

Bandwidth on wide area networks is expensive, and while traffic volume on the Internet increases, operators have to increase bandwidth capacity as well in order to meet the requirements that transmission needs. WANs act as a valuable resource but despite that WANs are often over-provisioned due to trying to avoid link failures and handle traffic peaks. (Yang & al. 2019, 3). Improvements in broadband-speed result in consumption and use of content using higher bandwidth. Large multimedia files require fast download speeds, so it is essential that this is considered when supporting cloud services. (Cisco 2020, 15) Since WAN data traffic travels long distance through physical links, in which failures occur and therefore performance decreases. Low network latency is necessary for cloud environments to be able to secure interaction, which is something a legacy WAN solution is unable to offer. As businesses have multiple locations and branch offices as well, delivering business solutions effortlessly from each location is critical to the company to perform business.

Because constant network management is needed for digital business models, SDNs work as a solution for increasing flexibility and programmability to keep up with the changing business needs. Network is made more adaptable due to data and control layer being separated. As the amount of hybrid cloud – private and public cloud combined – as well as need for bandwidth, increases in corporate environments, WAN traffic becomes more based on software and hybrid cloud. (Cisco 2020, 26-27)

4.5 SD-WAN advantages

SD-WAN reduces costs as its gateway is based on the cloud so manual network upgrades or redesigns are not needed. What is more, provisioning is improved as configuration is simplified and more rapid. Automated provisioning is also possible with SD-WAN, which results in faster branch deployment as deployment is managed through a centralized management branch. SD-WAN that is secured with IPSec can get increased security when segmenting is done. This increases network security as damage can be limited to one specific area only and the system will make an alert about the problem. (Mitchell 2018, 19-20)

Software-Defined Security gives additional security to SD-WAN by serving it via software instead of hardware, allowing corporations to have layered security service for branch offices. Security costs are also reduced. SD-security is separated from physical devices as it is managed in control layer where the authentication process is located. For example, web gateways and next-generation firewalls can be maintained with SD-security. SD-security is centrally managed and integrated into security services through provisioning. The main advantage is its rapid adaptability to maintain a security environment while reducing risks with deploying multiple systems in different infrastructure environments. (Mitchell 2018, 19-21)

4.6 Network Edge

Edge computing is a framework where computing is distributed so that applications are brought closer to data sources and users. In SD-WAN, Edge computing aims to lower the cost of data transport by bringing computing, storage, and networking closer to users and devices. As data is located close to its source, latency decreases, and it allows business to be performed faster. (IBM 2021) SD-WAN connects the corporate edge to the datacenter, allowing the management of the network to be more focused on branches. Before, branch offices have been defined as remote offices without their own datacenters, but nowadays enterprises are moving to a more location-based management. As the amount of edge connected devices increases, corporations need to manage their endpoints to maintain business. Before adding endpoints to increase computing capabilities, the overall infrastructure needs to be in place, so it is easy to manage and serves edge computing in the best way possible. (Cisco 2020, 2, 27-28)

4.6.1 Secure Access Service Edge

Secure Access Service Edge (SASE) combines security and networking that is globally distributed and supports edges, such as WAN and cloud. It involves cloud-based architecture with capabilities of elasticity and adaptability. It works on a cloud platform globally and allows connectivity to edge through points of presence. Network optimization and threat prevention are also components of the cloud. Edge implementation can be done with SD-WAN where multiple Internet links are inserted to overcome link failure. (Cato Networks 2021, 3-4)

4.7 SD-WAN challenges

As with any business solution that updates the whole environment, deployment of SD-WAN across the whole company can be challenging and take time, as every aspect with connections and network security needs to be considered. What is more, one-off investment can be expensive but in the long run the cost-benefit will result in a more profitable solution for the company: it can be thought of as an investment.

5 Connecting a branch office

Both MPLS and IPSec protocols can be used together with SD-WAN environments based on the needs of the organization. Need for a separate network connection for the company's branch office was adapted to the design of the network architecture in this thesis. IPSec would be the base for the site network connectivity, while the adaptation to SD-WAN based network would be kept in mind while designing the network topology for the branch office.

Connecting a branch office with a new technique can take time and effort as it requires planning components so that they are compatible with each other and allow connectivity continuously.

5.1 Comparison between different models

A comparison of key elements of MPLS, IPSec and SD-WAN based network solutions can be seen in Table 1.

	MPLS	**IPSec**	**SD-WAN**
Cost	Standard	Lower	Involves investments to create efficient environment
Scalability	Private network that scales based on network needs	Tunnel scalability is limited	Adjustable connection quality
Functionality	Based on labels and tagging	Internet-based connection, tunnel establishment	Customized software configuration
Performance	Effective and low congestion	Enhanced performance with optimized network topology	Centralized monitoring, connection quality adjusting between forwarding and control planes
Security/Management	Built-in privacy	Running in public network, tunnels	Centralized solutions, separate control plane

Table 1. MPLS, IPSec and SD-WAN features (adapted from Mitchell 2018 2017, 15)

As corporations expand their branches, scalability can be a problem as reservation for new IP addresses and configuration of devices is needed. (Bahnasse & Kamoun 2015, 1) IPSec tunnel scalability is limited to some extent, but IPSec fits to small and medium-sized companies. Lower cost of IPSec maintenance and less investments on hardware can be reasons why IPsec would be suitable choice.

Scalability comes to question when the network needs to scale to a multinational company, which has a lot of traffic across continents daily. IPSec is suitable for site-to-site connections since it has good performance when the network topology is optimized. A solution that involves SD-WAN should be considered when connecting multiple offices together. SD-WAN offers security as well as flexibility as it is adaptable and scales according to the scope of the network. MPLS and IPsec can both be deployed in SD-WAN as it combines management and infrastructure on different layers. When a future network upgrade to SD-WAN architecture is planned, the transition from MPLS or IPSec-based network takes design, time, and improvements. At the same time, it improves management and configuration.

As networking technologies evolve constantly, security plays a great role in routing as well. Security-wise, data protection is not included in MPLS which is why encryption should be considered when connecting routers to the network (Mitchell 2018, 7). However, data can be inserted into an IP-based tunnel from any device that has connectivity to network, which something to keep in mind when having an IPSec based network connection. However, IPSec handles the connection establishment in the IKE tunnel where data is encrypted and transported. If that is done the appropriate way, IPSec would be a suitable choice for securing network connection.

MPLS offers protection for data spoofing as data can be injected to MPLS tunnel only at the head end of the tunnel. (Lucek & Minei 2011, chapter 1.3) MPLS is a secure protocol itself since it creates a private network that is not connected to the Internet directly. As IPSec runs over Internet since it’s securing IP traffic, it is therefore exposed to Internet-based threats. Network configuration needs to be done carefully since faults on configuration on critical servers could have critical effects and damage on the corporate image. The IPSec Authentication header takes care of authentication and integrity, while ESP handles the encryption of the traffic, making IPSec generally a secure protocol for VPN connections.

Implemented with SD-WAN, the method used for deployment of IPSec secure tunnels can have an impact on how the network scales (Cisco 2019), since IPSec scales best to small and medium-sized corporate connections, such as site-to-site.

MPLS functionality is based on labels and tagging and its therefore different from the functionality of IPSec since it does not transport traffic based on routing tables. Implementation of functions requires different kind of expertise and therefore the best technical solution for a network depends on the resources of the company.

Bandwidth cost is higher on MPLS compared to IPSec. Manual network configuration is also present with MPLS and the provider is responsible for dynamic data routing in its MPLS cloud. What is more, if routing is dynamic on MPLS, then static and dynamic routing should still be able to cooperate in MPLS traffic. (Mitchell 2018 2017, 6) Since MPLS is using customer and provider edge, these two need to be in place for the connection to work.

With IPSec, the tunnel establishment with SD-WAN should be involved in the planning of the SD-WAN system. As IPSec uses IKE protocol for tunnel establishment it should be considered that if all peers of a device in SD-WAN wanted to create a tunnel at the same time, IKE would take time to negotiate the key exchange. These types of latency issues could be compromised with the SD-WAN control channel in all devices that are part of the SD-WAN system. (Cisco 2019) Since SD-WAN separates the control from the rest of the architecture it allows flexibility on the rest of the system.

5.2 Connection method for the target company

Because the target company has a need for site-to-site VPN connection, IPSec was a suitable choice for this need as the set of IPSec protocols use encryption and key exchange to ensure a secure connection for network traffic. IPSec provides confidentiality, integrity and authentication since AH and ESP provide integrity by encrypting traffic on the IP header. IPSec costs are also lower than for example a SD-WAN based architecture since it does not require investments.

6 IPSec VPN implementation

This chapter explains the IPSec VPN implementation process within the target company. In the end, adaptability with IPSec and SD-WAN is discussed briefly.

6.1 Objective

The objective of the implementation is to explain the implementation process of creating a VPN site-to-site connection using IPSec and what needs to be taken into account when designing a corporate network. This chapter also examines how an IPSec VPN can be used with an SD-WAN implementation and how it can be utilized in the future when a network is designed.

6.2 Test environment

An Oracle VM VirtualBox was used to be able to configure EVE-NG machine (community edition). A virtual testing environment was then constructed with Emulated Virtual Environment (EVE-NG) to be able to test elements and configurations of an IPSec VPN connection.

6.2.1 EVE-NG test lab

EVE-NG is a platform tool for creating proof of concepts and test environments for networking and security (EVE-NG 2021a). EVE-NG simulates the functionalities of a real corporate network, without affecting the actual network. The EVE-NG test environment allows the exploration of the mechanisms of IPSec and how they would work in practice. The deployment of a virtual IPSec environment can be thought to be similar to an actual network that would be used in production.

In this thesis, EVE-NG was used to design and explore the functionalities of a corporate IPSec VPN connection and to see what needs to be put in place for it to be brought into use as a site-to-site connection.

6.2.2 Palo Alto NGFW

Palo Alto is a framework that offers a selection of networking and security solutions. (Palo Alto 2021) In this thesis, Palo Alto's Next-Generation Firewall (NGFW) was used for setting up the firewall rules, for example for inbound and outbound traffic by allowing or denying traffic.

The Palo Alto firewall consists of two main planes: data, and management. The management plane involves administrative tasks, such as configuration and performs cloud lookups for URL and DNS security. Data plane is responsible for processing flows and performing security features for example by scanning ongoing sessions. Data plane also maintains IPSec VPN connections. (Piens 2020, chapter 1)

Palo Alto was used together with EVE-NG to define the access rules of users. Palo Alto allows the administrator to allow or deny firewall rules based on needs, such as specific users having access to a certain interface. The connection was a virtualized version of a corporate network as it simulates a real office network, but it doesn't have an impact on the actual network performance or traffic.

6.3 Deployment process

The objective was to design a corporate network VPN connection between branch office in Finland and an office in another country. Network security was considered when designing the network topology. As network traffic routes through another country to the office in Finland, the connection between these two countries is in key role for creating a connection as there should be a connection available to the rest of the corporate network as well.

As deployment of SD-WAN involves several steps, any changes to system should be designed and documented in detail and the update process should be started with low priority components, so that the effect on the whole network system can be minimized in case of any errors or problems occurring during or after update process, such as missing information or device being unavailable or unreachable. The most critical components should involve a plan on how, when, and why they are updated and describe the relations between network systems and their functionality. It will help to gain a better understanding of the whole concept and the scope of the updates.

In this thesis, the target company's specific requirements and business needs for IPSec VPN network connection were analyzed based on the current network infrastructure and by interviewing coworkers about the structure of the network. Upcoming projects were also discussed to find out what possible changes there would be within the company in network and connections in the future. A need for creating a connection that is established from the local site and more independent from the rest of the corporation was the key element in the design of the network.

The design of the IPsec VPN was made in virtualized environment which simulates network functionality without affecting the actual network that is in use. The machines can be configured by adding IP addresses and gateway information to the devices.

The ability to have a manageable and adaptable network environment that is independent from the main site was considered while designing the IPSec network model in this thesis. It would allow the corporation to have more independence in general as it would not need to rely on another site's connection stability. To be able to have an independent network connection would make the daily communication easier within the company as well as the connection more convenient to maintain. Performing updates and upgrades would be easier as it would be handled on-site. The encryption provided by IKE tunnel in IPSec creates a secure environment for Internet traffic within the company. The cost of IPSec is also lower than for example with SD-WAN and since traffic operates over IP, need for physical devices is lower. This also saves costs as need for device upgrades decreases.

6.4 IPSec model design

Based on the research and the target organization's requirements, an outline for suggested IPSec VPN model for the site-to-site connection was designed. The implementation process included planning and designing as well as understanding of the network as there is vital traffic transporting in the office network and across the company to the other office sites. An illustration of the IPSec model for the site-to-site connection is illustrated in Figure 18.

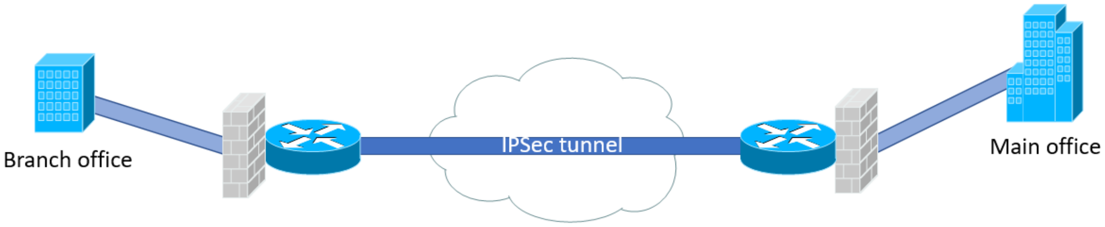

Figure 18. IPSec VPN office network for target organization

Traffic routes from the main office to internet. There is an IPSec tunnel between two routers as well as firewall to secure, deny and allow traffic. Firewall management is configured in Palo Alto. The tunnel ends at a router which is connected to the branch office. A site-to-site connection is established with the IPSec tunnel. The branch office has direct access to Internet since it’s connected to a router that is directly connected to Internet. There are firewalls on each end to make the connection more secure.

Technical details on IPSec IKE tunnel establishment can be found in chapter 2.5.

6.4.1 Challenges

While organizational environments can be quite vast and involve a lot of infrastructure, hardware and software, a lot of matters related to network topology, security, and overall performance need to be considered while implementing a new network topology, not to mention that the Quality of Service remaining stable during and after the change of network structure. A rollback plan should always be developed before taking any action upon network changes within the company. Security wise, a backup and copy of the configuration of a network structure should be in place so that a previous version is easily available for restoring in case errors emerge during update process.

The number of devices and business aspects also have an impact on how the network should be designed and therefore there is a lot of planning involved when designing new network topology. Connections should be available and up all the time or with brief interruptions. A backup connection needs to be designed as well in case of network errors or outages. It is important to ensure that all of the traffic is secured appropriately.

6.4.2 Adaptability with SD-WAN

When it comes to SD-WAN, there is a separate control plane for management of configurations and policies for the network topology. Whether it would be the need of having to add a new device when a new employee is starting in the company or to increase the number of servers for a specific business use, the management of devices is performed mainly on the control plane, where all the devices in the network are handled. The updates and upgrades for servers, routers and other devices could be performed through the control plane window, and on-site configuration would not be necessary.

Adaptability with SD-WAN was kept in mind when the model for the IPSec VPN was designed. For example, this IPSec implementation could be used as a second option for traffic if the main network implementation were designed based on SD-WAN. It could serve as a backup network connection if there were any problems occurring with traffic or connections. If any problems with the connection establishment were noticed, the backup connection would take control and switch the traffic to be routed the alternative way. The backup connection would be configured so that when a regular network connection would not be available, the system would alarm about errors in connection and then move to a VPN tunnel that would route the traffic to the backup connection temporarily.

7 Discussion

This thesis focused on the ways of how to connect a branch office to the main site of a company. Three different methods, MPLS, IPSec and SD-WAN, were discussed, and their functionalities explained. These three ways to build an office network were compared and IPSec-based site-to-site connection functionalities were explored to find out the requirements for an IPSec VPN connection.

Network architecture design takes lots of planning and the design should be responding to the needs of the company. Overall, there is a place for each of these models that were introduced in this thesis. IPSec, MPLS and SD-WAN are all suitable for office networks and it depends on the network requirements which model suits the enterprise best.

In this thesis, IPSec functionality was examined to find out the general and technical requirements of its use. IPSec is mainly suitable for small- and medium-sized companies, but it is also appropriate for branch office connections since it's a secure solution for transporting traffic over the Internet. IPSec costs are lower compared to other methods which gives the company the advantage to direct resources to other projects and improvements. As IP runs over the Internet, IPSec upgrades do not require large amount of hardware updates. IPSec requires some technical requirements to be deployed but after it is in place the configuration and maintenance of the system is convenient.

Since the world of IT is evolving constantly, networking technologies need to keep up with the pace in order to respond to the needs and to perform efficient business. IPSec has been used for decades, but it is still used and can be included in the modern development of the office infrastructure and network. SD-WAN is a current technology that will gain ground more and more and become part of every corporate network infrastructure in the future. Elements of SD-WAN, such as Network Edge and separation of control plane gives an opportunity to have more flexibility within the network and allows it to be customizable. By adding elements from both IPSec and Software-Defined WAN solutions, a secure and manageable office network that scales according to the company needs is possible.

7.1 Learning outcomes

This thesis introduced the topics of IPSec, MPLS and SD-WAN and it was interesting to learn about these three network connection methods. The thesis process gave a lot of insight on how academic research is conducted. In general, the research process went on smoothly. Finding relevant information related to this thesis was sometimes a bit hard as there was a lot of material and technical documentation on the subjects. General understanding of the concepts took time since the topic of the thesis was somewhat broad. Time management of the project was quite challenging, since in the beginning it was hard to determine how much time the writing process would take. As the writing process went on, it became easier to determine the timeline of the project because the outline of the thesis became clearer. My technical vocabulary has broadened along the writing process since reading the literature on the topics required a good understanding of the vocabulary. In general, the thesis was a great project to work on and gives a good overview on the topics discussed. It gives me useful insight for the future, whether I will be working with networks or security related tasks.

References

Ali, E., Manel, M. & Habib, Y. 2017. An Efficient MPLS-Based Source Routing Scheme in Software-Defined Wide Area Networks (SD-WAN). ACS 14th International Conference on Computer Systems and Applications. Accessed: 22 June 2021.

Bahnasse, A. & Kamoun, N. 2015. Study and Analysis of a Dynamic Routing Protocols' Scalability over a Dynamic Multi-point Virtual Private Network. International Journal of Computer Applications, 123, 2. pp. 1-x. Accessed: 2 July 2021.

Cato Networks 2021. The Network for the Digital Business Starts with the Secure Access Service Edge (SASE). Cato Networks. Accessed: 10 August 2021.

Cisco 2019. The Role of Dynamic IPsec Tunnels in Modern SD-WAN Networks. URL: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/white-paper-c11-743108.html. Accessed: 3 September 2021.

Cisco 2020. Cisco Annual Internet Report (2018–2023). URL: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html. Accessed: 22 June 2021.

Cisco 2021. What Is a WAN? Wide-Area Network. URL: https://www.cisco.com/c/en/us/products/switches/what-is-a-wan-wide-area-network.html. Accessed: 18 October 2021.

EVE-NG 2021a. URL: https://www.eve-ng.net/. Accessed: 7 July 2021.

Eve-NG 2021b. Commercial Cookbook. EVE-NG. 2021. Accessed: 26 July 2021.

Firewall.cx 2018. Understanding VPN IPSec Tunnel Mode and IPSec Transport Mode - What's the Difference? URL: https://www.firewall.cx/networking-topics/protocols/870-ipsec-modes.html. Accessed: 18 October 2021.

IBM 2021. What is Edge Computing? URL: https://www.ibm.com/cloud/what-is-edge-computing. Accessed: 23 June 2021.

Javvin Technologies 2004. Network Protocols Handbook. 2nd Edition. Javvin Technologies. USA. Accessed: 11 August 2021.

Kolhar, M. Abualhaj, M. & Rizwan, F. 2016. QoS Design Consideration for Enterprise and Provider's Network at Ingress and Egress Router for VoIP Protocols. International Journal of Electrical and Computer Engineering. 6, 1, pp. 236. Accessed: 23 September 2021.

Lucek, J. & Minei, I. 2011. MPLS-Enabled Applications: Emerging Developments and New Technologies, Third Edition. Wiley. Accessed: 18 August 2021.

Mitchell, D. 2018. From MPLS to Software-Defined Wide Area Network. East Carolina University, USA. Accessed: 5 July 2021.

Networklessons.com 2021a. IPSec (Internet Protocol Security). URL: https://networklessons.com/cisco/ccie-routing-switching/ipsec-internet-protocol-security. Accessed: 10 September 2021.

Networklessons.com 2021b. Introduction to DMVPN. URL: https://networklessons.com/cisco/ccie-routing-switching/introduction-to-dmvpn. Accessed: 14 September 2021.

Networklessons.com 2021c. Introduction to MPLS. URL: https://networklessons.com/cisco/ccie-routing-switching/introduction-to-mpls. Accessed: 14 September 2021.

Palo Alto 2021. URL: https://www.paloaltonetworks.com/. Accessed: 26 July 2021.

Piens, T. 2020. Mastering Palo Alto Networks. Packt Publishing. URL: https://learning.oreilly.com/library/view/mastering-palo-alto/9781789956375/. Accessed: 12 August 2021.

Pujolle, Guy. 2020. Software Networks. Wiley-ISTE. London. URL: https://learning.oreilly.com/library/view/software-networks-2nd/9781786304582/. Accessed: 21 June 2021.

Snader, J. 2005. VPNs Illustrated: Tunnels, VPNs, and IPSec. Addison-Wesley Professional. URL: https://learning.oreilly.com/library/view/vpns-illustrated-tunnels/032124544X/. Accessed: 15 June 2021.

Techopedia Inc. 2021. Dictionary. URL: https://www.techopedia.com/definition/16492/customer-edge-router-ce-router. Accessed: 18 October 2021.

The Geography of Transport Systems 2021. Point-to-Point versus Hub-and-Spoke Networks. URL: https://transportgeography.org/contents/chapter2/geography-of-transportation-networks/point-to-point-versus-hub-and-spoke-network/. Accessed: 12 October 2021.

Tizazu, G., Berhe, A., & Kim, K. 2017. Dynamic Routing Influence on Secure Enterprise Network Based on DMVPN. Accessed: 30 June 2021.

Towards Datascience 2021. https://towardsdatascience.com/multiprotocol-label-switching-mpls-explained-aac04f3c6e94. Accessed: 6 October 2021.

Yang, Z., Cui, Y., Li, B., Liu, Y. & Xu, Y. 2019. Software-Defined Wide Area Network (SD-WAN): Architecture, Advances and Opportunities. Department of Computer Science and Technology, Tsinghua University. Beijing, China. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8847124. Accessed: 22 June 2021.