الجمهورية الجزائرية الديمقراطية الشعبية

PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA

وزارة التعليم العالي و البحث العلمي

MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH

وزارة البريد والمواصلات السلكية واللاسلكية

MINISTRY OF POST AND TELECOMMUNICATIONS

المدرسة الوطنية العليا للإتصالات وتكنولوجيات الإعلام والإتصال

THE HIGHER NATIONAL SCHOOL OF TELECOMMUNICATIONS AND INFORMATION AND COMMUNICATION TECHNOLOGIES (ENSTTIC)

Final Year Project

For the fulfilment of the requirements for the degree of State Engineer in:

Telecommunications and IP Networks

Presented by: Chihabeddine MERABET & Yasser RAMLIA

"Implementing SD-WAN over Traditional WAN for Enterprises"

Defended before the jury composed of:

- President: Mr. Djalal ZIANI KERARTI (Associate Professor at ENSTTIC)
- Examiner: Ms. Chifaa TABET HELLEL (Associate Professor at ENSTTIC)
- Supervisor: Ms. Sarra MAMECHAOUI (Associate Professor at ENSTTIC)

Promotion: IGE 45

Academic Year: 2024/2025

Dedication

“

أولا الحمد لله على كل شيء، فهو من منحني القوة والصبر والشغف لأواصل مسيرتي الدراسية من بدايتها حتى نهايتها

I dedicate this thesis to you, my dear parents — my father and mother — whose unwavering support, endless sacrifices, and unconditional love have always been my greatest source of motivation. For that, I am eternally grateful.

To my younger sisters, Raounek and Takoua, and my little brother, Abderrahmene — your futures are dear to my heart. May you find success and fulfilment in every path you choose. Your constant presence, support, and inspiration have played a pivotal role in my accomplishments, and I am deeply indebted to you.

Sincere thanks go to my project partner, Yasser, for your diligent work, commitment, and dedication to our shared endeavour. Your contributions have been invaluable, and I am profoundly grateful.

To Horizon Club and all its members — with whom I shared five unforgettable years — thank you. Horizon gave me far more than I could ever give back: knowledge, personal growth, true friendship, and a collection of memories I will always treasure.

To all the professors and staff of ENSTTIC — your guidance, dedication, and support throughout these years have been instrumental to my academic and personal growth. Thank you.

To the friends I made along the way — Mehdi, Yassine, Abdessamed, and many others — thank you for the companionship, laughter, and shared experiences that made this journey more meaningful.

And finally, to the people of Gaza — may peace prevail, suffering end, and justice and dignity be restored.

”

Thank you for believing in me - Chihabeddine MERABET -

“

First and foremost, I thank Allah for granting me the strength, patience, and perseverance throughout these years.

To my dear parents, your unconditional love, support, and guidance have been my greatest source of strength. Your sacrifices and encouragement have brought me to where I am today, and for that, I am eternally grateful.

To my father, who once walked the halls of this very institution it has been both a privilege and a deep source of inspiration to follow your path. I carry forward the legacy you began with pride and gratitude.

To my sister and little brother, as your eldest sibling, it has been a joy and an honor to grow alongside you. Your innocence, energy, and affection have always brought light to my days and reminded me of my purpose. Thank you for being my inspiration and for giving me strength through your smiles.

To my project partner Chihab Thank you for being the source of inspiration, knowledge, and motivation throughout this journey. Your profound insights, expertise, and guidance have significantly shaped this thesis.

To my professors, thank you for your invaluable guidance, mentorship, and the knowledge you have generously shared. Your support has played a crucial role in shaping both my academic and personal growth.

To my friends, A heartfelt thank you for your love, appreciation, and constant encouragement. Your presence made this journey more joyful and meaningful.

This incredible chapter at ENSTTIC draws to a close, marking not an end, but the beginning of an even greater adventure.

”

With utmost gratitude – Yasser RAMLIA –

Acknowledgement

“

First, we would like to express our sincere gratitude to our supervisor, Ms. Sarra MAMECHAOUI, for her invaluable guidance, continuous support, and insightful feedback throughout the development of this project. Her availability and readiness to assist whenever needed played a crucial role in the successful completion of this work.

We would also like to thank the esteemed members of the jury, Mr. Djalal ZIANI KERARTI and Ms. Chifaa TABET HELLEL, for accepting to evaluate our work and for their constructive remarks and observations, which greatly enriched this final project.

We are especially thankful to Mr. Adel BENSALEM for his valuable help and guidance throughout the project. His technical support and advice were instrumental in overcoming many challenges and in achieving our objectives.

Our heartfelt thanks go to all the professors who have contributed to our academic journey. Their dedication and knowledge have shaped our understanding and prepared us for this final step.

We are also deeply grateful to our families for their unwavering encouragement, patience, and emotional support during all stages of our studies. Their belief in us has been our greatest source of strength.

Finally, We extend our thanks to our friends and classmates who have shared this academic path with us. Their support, discussions, and collaboration made this experience all the more meaningful.

”

Abstract

In the context of digital transformation, enterprises increasingly rely on cloud services, remote collaboration, and distributed infrastructures. Traditional WAN architectures based on technologies like leased lines and MPLS often struggle to meet modern demands for agility, scalability, and cost-efficiency. Software-Defined Wide Area Network (SD-WAN) emerges as a strategic solution by separating the control and data planes, enabling centralized management, application-aware routing, and reduced operational complexity.

This final year project investigates SD-WAN as a modern alternative to traditional WANs, focusing on its architecture, deployment models, and integrated security capabilities. Cisco Catalyst SD-WAN was selected for implementation due to its modular design and robust enterprise features. A virtual lab environment was developed to simulate a multi-branch enterprise network, including controller bootstrap, certificate-based authentication, edge device onboarding, and policy enforcement.

The project demonstrates the practical benefits of SD-WAN in terms of scalability, security, and performance optimization. The outcomes provide a concrete methodology for enterprises aiming to adopt SD-WAN to enhance their network flexibility and management efficiency.

***Keywords**: WAN, MPLS, SDN, SD-WAN, Cisco Catalyst SD-WAN, GNS3*

الملخص

في سياق التحول الرقمي، تعتمد المؤسسات بشكل متزايد على الخدمات السحابية، العمل عن بُعد، والبنى التحتية الموزعة. تواجه الشبكات التقليدية المعتمدة على تقنيات مثل "الخطوط المؤجرة" (Leased lines) و "تبديل تسمية متعدد البروتوكولات" (MPLS) صعوبات في تلبية المتطلبات الحديثة من حيث المرونة، قابلية التوسع، والكفاءة من حيث التكلفة. تظهر "شبكة الاتصال الواسعة النطاق المحدّدة البرمجيات" (SD-WAN) كحل استراتيجي من خلال فصل طبقة التحكم عن طبقة البيانات، مما يتيح إدارة مركزية وتقليلاً لتعقيد العمليات.

يبحث هذا المشروع في (SD-WAN) كبديل حديث للشبكات التقليدية، مع التركيز على بنيته، نماذج التطبيق، والقدرات الأمنية المدمجة. تم اختيار "سيسكو كاتاليست للشبكة الواسعة المعرفة برمجياً" للتطبيق بفضل تصميمه وميزاته القوية التي تستهدف الشركات. تم تطوير بيئة افتراضية لمحاكاة شبكة مؤسسة متعددة الفروع.

يُظهر المشروع الفوائد العملية لـ(SD-WAN) من حيث قابلية التوسع، الأمان، وتحسين الأداء. وتقدم النتائج منهجية ملموسة للمؤسسات التي تهدف إلى اعتماد (SD-WAN) لتعزيز مرونة الشبكة وكفاءة إدارتها.

***الكلمات المفتاحية:** WAN, MPLS, SDN, SD-WAN, Cisco Catalyst SD-WAN, GNS3*

Résumé

Dans le contexte de la transformation numérique, les entreprises s'appuient de plus en plus sur les services en nuage, la collaboration à distance et des infrastructures distribuées. Les architectures de réseau étendu (WAN) traditionnelles, basées sur des technologies telles que les lignes louées et la commutation d'étiquettes multiprotocole (MPLS), peinent souvent à répondre aux exigences actuelles en matière d'agilité, de scalabilité et de rentabilité. Le réseau étendu défini par logiciel (SD-WAN) s'impose comme une solution stratégique en séparant le plan de contrôle du plan de données, permettant ainsi une gestion centralisée, un routage intelligent selon les applications et une réduction de la complexité opérationnelle.

Ce projet de fin d'études explore le réseau étendu défini par logiciel (SD-WAN) comme une alternative moderne aux réseaux étendus traditionnels, en mettant l'accent sur son architecture, ses modèles de déploiement et ses capacités de sécurité intégrées. La solution Cisco Catalyst réseau étendu défini par logiciel a été choisie pour sa conception modulaire et ses fonctionnalités avancées destinées aux environnements d'entreprise. Un laboratoire virtuel a été mis en place afin de simuler un réseau d'entreprise multi-sites, comprenant le démarrage initial (bootstrap) des contrôleurs, l'authentification par certificats, l'enregistrement des équipements périphériques (onboarding) et l'application des politiques de sécurité.

Le projet met en évidence les avantages pratiques du réseau étendu défini par logiciel (SD-WAN) en matière de scalabilité, de sécurité et d'optimisation des performances. Les résultats obtenus fournissent une méthodologie concrète pour les entreprises souhaitant adopter le SD-WAN afin d'améliorer la flexibilité et l'efficacité de la gestion de leur réseau.

Mots clés *: Réseau étendu, MPLS, SDN, SD-WAN, Cisco Catalyst SD-WAN, GNS3*

Table of Content

List of Tables and Figures

List of Tables

List of Figures

List of Acronyms

WAN – Wide Area Network
MPLS – Multiprotocol Label Switching
SDN – Software-Defined Networking
SD-WAN – Software-Defined Wide Area Network
ISP – Internet Service Provider
QoS – Quality of Service
LSR – Label Switch Router
LSP – Label Switched Path
LDP – Label Distribution Protocol
VPN – Virtual Private Network
TE – Traffic Engineering
PE – Provider Edge
P – Provider (Core Router)
CE – Customer Edge
API – Application Programming Interface
O&M – Operations and Maintenance
DIY – Do It Yourself
POC – Proof of Concept
MSP – Managed Service Provider
ZTP – Zero-Touch Provisioning
OMP – Overlay Management Protocol
NETCONF – Network Configuration Protocol
SSHD – Secure Shell Daemon
DTLS – Datagram Transport Layer Security
DIA – Direct Internet Access
TLOC – Transport Locator
IPS – Intrusion Prevention System
IDS – Intrusion Detection System
IPsec – Internet Protocol Security
CSR – Certificate Signing Request

General Introduction

In today's digital era, enterprises are increasingly reliant on distributed computing, cloud-based services, and geographically dispersed teams. To support this transformation, Wide Area Networks (WANs) have become the backbone for enabling secure and efficient connectivity between branch offices, data centres, and cloud applications. Traditionally, enterprise WANs have been built upon technologies such as leased lines and Multiprotocol Label Switching (MPLS), which, while reliable, often lack the agility, scalability, and cost-efficiency demanded by modern business needs.

The emergence of Software-Defined Wide Area Network (SD-WAN) technology represents a paradigm shift in enterprise networking. By decoupling the network control and data planes, SD-WAN introduces centralized orchestration and application-aware routing, while significantly reducing operational complexity and infrastructure costs. These capabilities make SD-WAN a suitable solution for enterprises seeking to optimize performance, enhance security, and streamline connectivity across hybrid multi-cloud environments.

This final year project aims to explore and implement SD-WAN as a modern alternative to traditional WAN infrastructures. After presenting the evolution of WAN technologies and the limitations of legacy MPLS-based architectures, the project focuses on the design and deployment of a Cisco Catalyst SD-WAN solution in a simulated enterprise environment.

Chapter 1 presents an introduction to WAN technologies, where we explored the principles of traditional architectures such as MPLS, identified their limitations, and introduced Software-Defined Networking (SDN) as a foundational concept leading to SD-WAN. The chapter also outlines the benefits of SD-WAN, common deployment models, step-by-step implementation strategies, and the key challenges involved in migrating from MPLS to SD-WAN.

Chapter 2 is dedicated to a comparative study of available SD-WAN solutions, culminating in the selection of Cisco Catalyst SD-WAN for our implementation. This chapter details the solution's architecture, components (including vManage, vSmart, vBond, and WAN Edge), its policy-driven control mechanisms, and integrated security capabilities such as segmentation, IPS/IDS, and application-aware policies.

Chapter 3 focuses on the practical implementation of Cisco Catalyst SD-WAN in a simulated environment using GNS3. We successfully deployed all control plane elements and WAN Edge devices, onboarded them into the SD-WAN fabric, tested network reachability using advanced diagnostics, and applied security policies to validate end-to-end protection.

Having established the critical need for modern WAN solutions in today's digital landscape, we now turn our attention to examining the technological evolution that has shaped enterprise networking. Chapter 1 provides a comprehensive foundation by exploring the journey from traditional WAN architectures to the emergence of Software-Defined networking paradigms.

Chapter One:
Evolution of Wide Area Network (WAN) technologies

Contents:

Introduction

Wide Area Network (WAN) plays a crucial role in connecting geographically dispersed branches and data centres, enabling communication, remote monitoring and resource sharing across enterprise sites. However, traditional WAN architectures, primarily based on legacy technologies such as leased lines and Multi-Protocol Label Switching (MPLS), are increasingly proving inadequate in meeting modern performance, flexibility, and cost-efficiency requirements.

This chapter provides an overview of the evolution of WAN technologies. It explores the functionality of MPLS. To establish a foundation for understanding Software-Defined solutions, the chapter introduces Software-Defined Networking (SDN). Building upon this, the concept of Software-Defined Wide Area Networking (SD-WAN) is presented in detail, including its architecture, components, advantages, and the reasons for its growing adoption as a superior alternative to traditional WAN models. Finally, the chapter addresses the aspects of migrating from legacy WAN infrastructures to SD-WAN in enterprise contexts. This includes common migration strategies, deployment models, and the challenges organizations may face during the transition.

1. Introduction to Wide Area Network (WAN)

1.1. Definition of Wide Area Network (WAN)

A Wide Area Network (WAN) is a telecommunication network that connects geographically dispersed locations including cities, countries, and even continents, by connecting smaller networks. This is unlike Local Area Networks (LAN) that operate within a limited area such as a building or campus. This WAN can be either public (using the internet) or private (using leased lines and secure communication channels) [1].

WAN plays a crucial role in modern enterprises by connecting branch offices, data centres, and cloud services together, facilitating communication and resource sharing across global locations. WAN ensures that organizations with dispersed operations can still maintain a unified and efficient computer network [2].

Today's IT organizations tend to deploy their infrastructures geographically over a WAN to increase productivity, support global collaboration and minimize costs. WAN ensures that branch offices and remote workers can access shared applications, databases, and even cloud services. Traditional LAN-oriented infrastructures are insufficient to support global collaboration with high application performance and scalability [3].

1.2. Purpose of Wide Area Network (WAN)

Wide-area networks (WAN) are the backbone of the enterprise today. If WAN connections didn't exist, organizations would be isolated in restricted areas or specific geographic regions. With the digitization of resources, companies use WANs to do the following:

- Communication:
  WANs allow communication between branches, sharing voice and data information.

- Resource Sharing:
  WAN enables resource sharing between branches of an organization by connecting geographically dispersed locations through a centralized network infrastructure.

- Data Backup and Disaster Recovery:
  It ensures business continuity through remote data storage and backups by storing copies of it in secure, off-site locations. These remote backups ensure that data can be quickly recovered.

- Connecting to applications running in the cloud:
  This connectivity supports greater flexibility, remote work, and collaboration across teams and locations.

1.3. Evolution of Wide Area Network (WAN) technologies

As businesses expand across multiple locations, enterprises cannot build their own global network infrastructure, so they rely on third-party service providers for connectivity.

The following are some common types of connections used in WAN [4]:

- Leased lines:
  A leased line is a direct network connection that an enterprise rents from Internet Service Providers (ISP). It can connect two LAN endpoints together. Leased lines are not necessarily physical lines. They may be virtual connections that the service providers implement over other network infrastructure.

- Multiprotocol Label Switching (MPLS):
  Multiprotocol Label Switching (MPLS) is a technique that routes data traffic based on predetermined labels. It attempts to route critical data traffic across shorter or faster network paths, improving network performance and Quality of Service (QoS). It works between OSI layers 2 and 3. Entreprises use it to create a unified network across existing infrastructure.

- Software-defined WAN (SD-WAN):
  Software-Defined Wide-Area Network (SD-WAN) is an evolution of MPLS technology. It abstracts the MPLS functions into a software layer. SD-WAN can reduce networking costs and provide greater flexibility than a fixed connection.

2. Multiprotocol Label Switching (MPLS)

2.1. Definition of Multiprotocol Label Switching (MPLS)

Multiprotocol Label Switching (MPLS) has been around for several years. It is a popular networking technology that uses labels attached to packets to forward them through the network.

The MPLS labels are advertised between routers so that they can build a label-to-label mapping. These labels are attached to the IP packets, enabling the routers to forward the traffic by looking at the label and not the destination IP address. The packets are forwarded by label switching instead of by IP switching [5].

2.2. Label Switching

Label Switching replaces traditional IP routing. Instead of routers making hop-by-hop forwarding decisions based on IP addresses, MPLS routers use short, fixed-length labels to determine the path. These labels are pre-assigned and exchanged between routers [5].

MPLS Label:

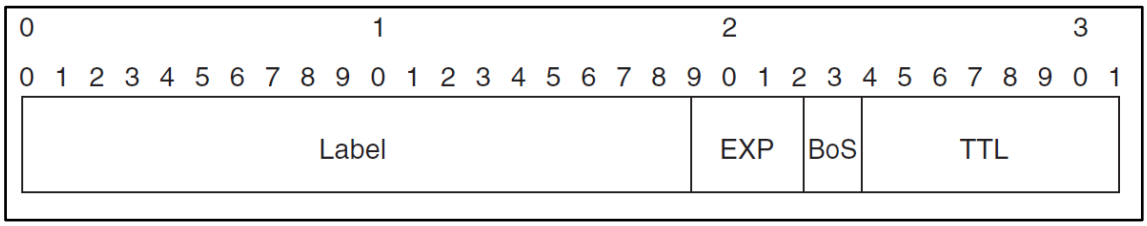

Figure 1: Syntax of MPLS Label [5]

One MPLS label is a field of 32 bits. Illustrated in Figure 1:

- The first 20 bits are the label value. This value can be between 0 and 2^{20}–1, or 1048575. However, the first 16 values are exempted from normal use.
- Bits 20 to 22 are the three experimental (EXP) bits. These bits are used solely for quality of service (QoS).
- Bit 23 is the Bottom of Stack (BoS) bit. It is 0, unless this is the bottom label in the stack. If so, the BoS bit is set to 1.
- Bits 24 to 31 are the eight bits used for Time To Live (TTL). It is simply decreased by 1 at each hop, and its main function is to avoid a packet being stuck in a routing loop.

Label Stacking

The stack is the collection of labels that are found on top of the packet. The stack can consist of just one label, or it might have more. Figure 2 represents Label Stacking concept:

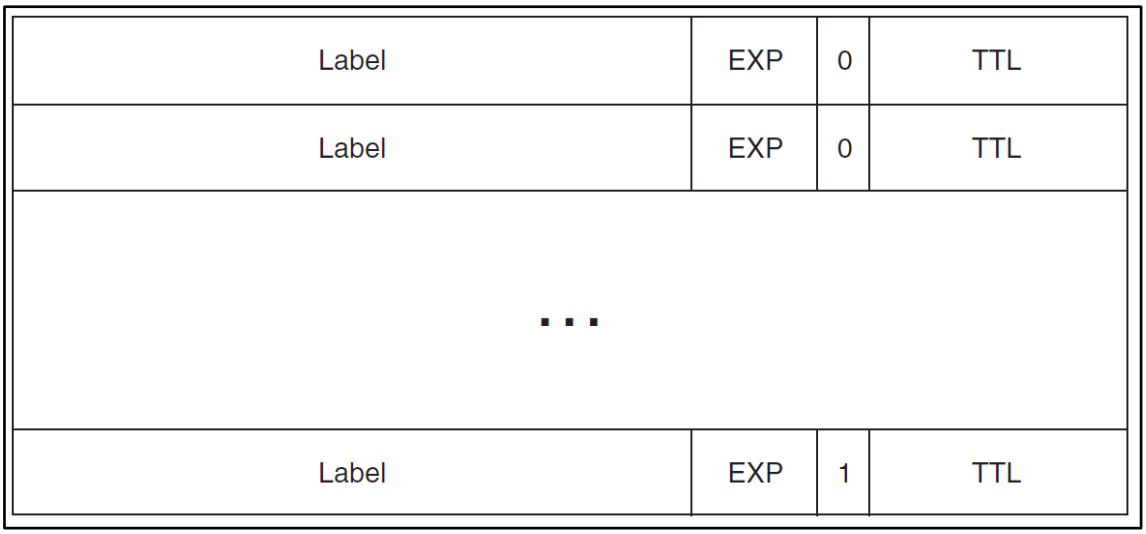

Figure 2: Label Stack [5]

MPLS-capable routers might need more than one label on top of the packet to route that packet through the MPLS network. This is done by packing the labels into a stack. The first label in the stack is called the top label, and the last label is called the bottom label. In between, you can have any number of labels. The BoS bit is 0 for all the labels, except the bottom label. For the bottom label, the BoS bit is set to 1.

Some MPLS applications actually need more than one label in the label stack to forward the labelled packets, such as MPLS VPN and MPLS Traffic Engineering [5].

Encoding of MPLS

The label stack sits in front of the Layer 3 packet, before the header of the transported protocol, but after the Layer 2 header. It ls represented in Figure 3:

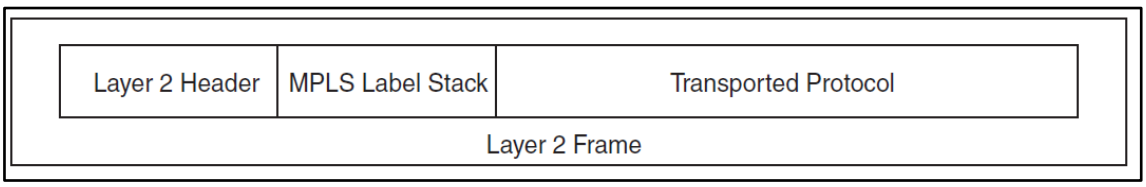

Figure 3: Encapsulation for Labelled Packet [5]

Label Switch Router

A label switch router (LSR) is a router that supports MPLS. It is capable of understanding MPLS labels and of receiving and transmitting a labelled packet on a data link. Three kinds of LSR exist in an MPLS network:

- Ingress LSR: First router in the MPLS path, receives a packet that is not labelled yet, inserts a label (stack) in front of the packet, and send it on a data link.

- Egress LSR: receives labelled packets, removes the label(s), and send them on a data link. Ingress and egress LSR are edge LSR.
- Intermediate LSR: A router in the middle of the MPLS path, receives an incoming labelled packet, perform an operation on it, switch the packet, and send the packet on the correct data link.

An LSR can do the three operations: pop, push, or swap. Bellow in Figure 4.

- Push is to add one or more labels onto the received packet. If the received packet is already labelled, the LSR pushes one or more labels onto the label stack and switches out the packet. If the packet is not labelled yet, the LSR creates a label stack and pushes it onto the packet.
- Swap replaces an existing label with a new one (performed by intermediate LSR).
- Pop is to remove one or more labels from the top of the label stack.

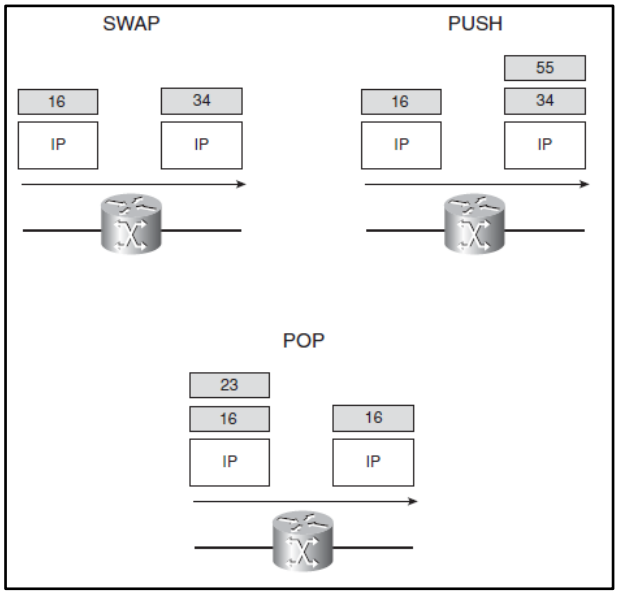

Figure 4: Operations on Labels [5]

Ingress and egress LSR are referred to as provider edge (PE) routers. Intermediate LSR are referred to as provider (P) routers [5].

Label Switched Path

A label switched path (LSP) is a sequence of LSRs that switch a labelled packet through an MPLS network or part of an MPLS network. Basically, the LSP is the path through the MPLS network or a part of it that packets take. The first LSR of an LSP is the ingress LSR for that LSP, where the last LSR of the LSP is the egress LSR. All the LSRs in between the ingress and egress LSR are the intermediate LSRs [5]. As it is shown in Figure 5:

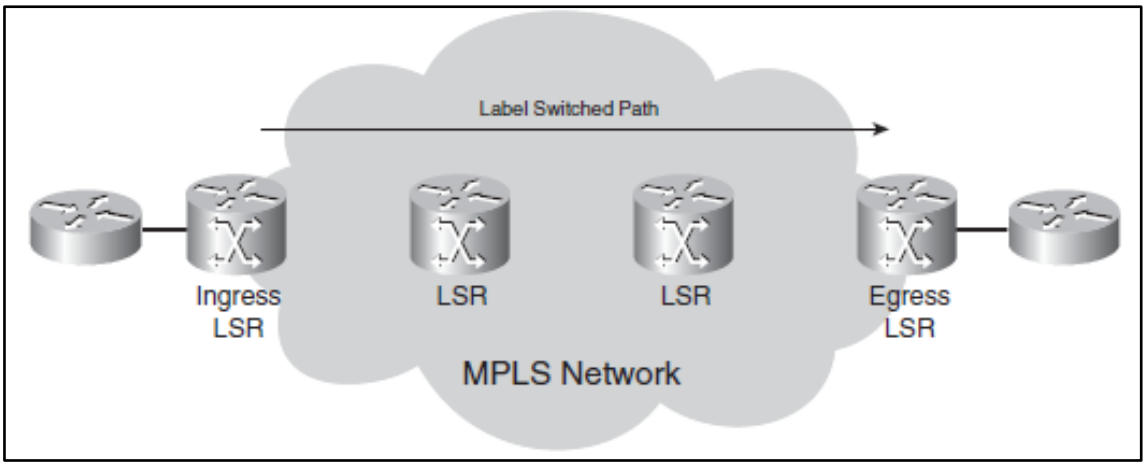

Figure 5: An LSP Through an MPLS Network [5]

2.3. Label Distribution Protocol (LDP)

LDP is a protocol that automatically generates and exchanges labels between routers. Each router will locally generate labels for its prefixes and will then advertise the label values to its neighbours.

LDP first establishes a neighbour adjacency before it exchanges label information.

First, LSR sends UDP multicast hello packets to discover other neighbours. Once two routers decide to become neighbours, they build the neighbour adjacency using a TCP connection. This connection is then used for the exchange of label information. Normally, a loopback interface is used for the neighbour adjacency.

LDP will only form a single neighbour adjacency, no matter how many interfaces two LSRs have in between.

There are two types of LDP adjacencies:

- Local adjacency: established by exchanging Link Hello messages between two LSRs.
- Remote adjacency: established by exchanging Target Hello messages between two LSRs.

Two LDP peers establish LDP sessions and exchange Label Mapping messages over the session so that they establish an LSP. LDP sessions are classified into the two types: Local LDP sessions created over a local adjacency, and Remote LDP sessions created over a remote adjacency [6].

2.4. MPLS Virtual Private Network (VPN)

MPLS VPN, or MPLS Virtual Private Networks, are the most popular and widespread implementation of MPLS technology. MPLS VPN can provide scalability and divide the network into separate smaller networks, which is often necessary in the larger enterprise networks.

A VPN emulates a private network over a common infrastructure, ensuring that multiple customer networks remain isolated from one another while enabling interconnectivity between different locations of the same organization [5]. Figure 6 highlights the architecture of an MPLS VPN.

MPLS VPN relies on specific router roles:

- Customer Edge (CE) Router: A router located at the customer's premises that connects to the service provider's MPLS network. CE routers do not need to run MPLS.
- Provider Edge (PE) Router: A router at the service provider's network edge that connects to CE routers. PE routers maintain VPN routing tables and use MPLS labels to forward customer traffic.
- Provider (P) Router: A core network router that does not directly connect to customers but facilitates label switching within the MPLS backbone.

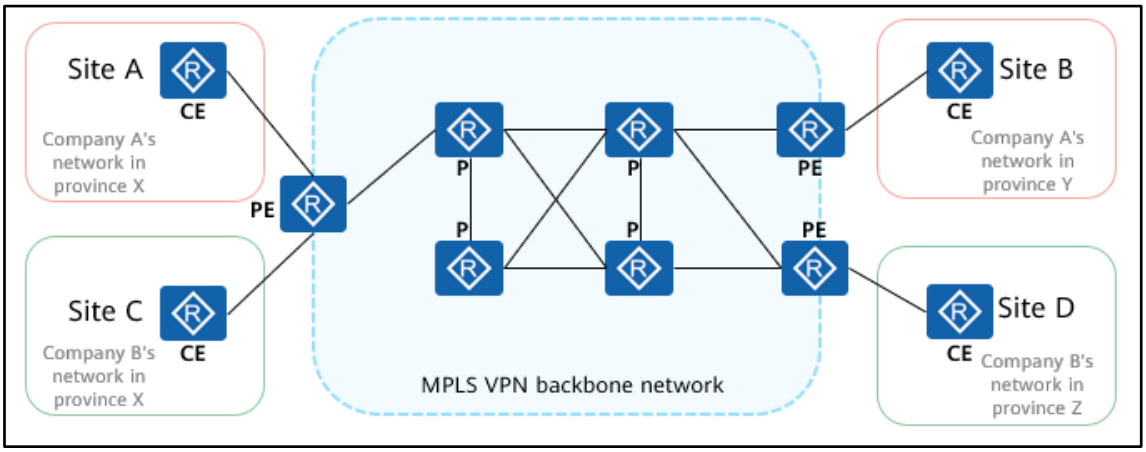

Figure 6 :MPLS VPN Schematic Overview [9]

2.5. Benefits of Multiprotocol Label Switching (MPLS)

MPLS enables enterprises and service providers to build scalable, high-performance, and reliable networks. Unlike traditional IP-based routing, MPLS efficiently manages traffic flows, ensuring better control and flexibility [5][7].

MPLS provides the following major benefits:

- Scalable support for Virtual Private Networks (VPNs):
  MPLS enables VPN services to be supported in service provider networks, thereby greatly accelerating Internet growth and reducing complexity while maintaining strong security.

- Traffic Engineering (TE):
  Allows network administrators to prioritize and control traffic flows, reduce congestion, and optimize bandwidth usage efficiently.

- Quality of Service (QoS):
  QoS is a means to prioritize important traffic over less important traffic and make sure it is delivered. An example where QoS is needed is VoIP traffic. VoIP traffic needs to be delivered to the destination within a certain time to the destination, or it becomes obsolete. Therefore, QoS should prioritize the VoIP traffic to ensure that it is delivered within a certain time constraint.

- High reliability:
  Routing based on labels over a private network ensures that packets will be reliably delivered to their destination. In addition, MPLS supports Service Level Agreements (SLAs) that guarantee uptime, fast recovery from failures, and network performance assurance.

- High performance and low latency:
  Dedicated MPLS paths ensure efficiency and a good user experience. It is also essential for real-time communication, like voice, video and mission-critical information.

2.6. Limitations of Multiprotocol Label Switching (MPLS)

While MPLS offers high performance and reliability, it also has several drawbacks, most notably [8]:

- Expensive deployment and maintenance:
  MPLS networks that rely on dedicated private WAN connections tend to be expensive. Deployments and upgrades of the required private connection can also turn into a resource-intensive processes. MPLS networks are costly to scale and maintain, especially as organizations expand their operations globally. Each new office or remote site requires additional MPLS lines, which come with high provisioning costs and long lead times.

- Inefficient for cloud & SaaS applications:
  As organizations continue to migrate their applications to the cloud, the traditional MPLS architecture becomes less effective. MPLS was not designed with cloud-first strategies in mind. MPLS cannot be extended to the cloud since it requires its own dedicated infrastructure. Therefore, it is not a good fit for remote users or for connecting to SaaS applications. It can also cause cloud and SaaS application access delays, resulting in poor user service.

- Bottlenecks in network performance:
  Traditional MPLS networks are designed for point-to-point connections, routing all traffic through centralized data centres. As businesses adopt cloud-based applications, this architecture creates a significant bottleneck. This leads to increased latency and degraded user experience.

- Inefficient for remote applications:
  MPLS does not have a centralized operations centre for reconfiguring locations or deploying new ones, and does not enable quick scalability. MPLS networks, designed primarily for static office locations, struggle to efficiently support the dynamic nature of remote access. VPN connections often add another layer of complexity and latency, further exacerbating performance issues for remote users who need reliable and fast access to cloud applications and corporate data.

3. Introduction to Software-Defined Networking (SDN)

3.1. Definition of Software-Defined Networking (SDN)

Software-Defined Networking (SDN) is an approach to networking that uses software-based controllers or Application Programming Interfaces (API) to communicate with underlying hardware infrastructure and direct traffic on a network.

This model differs from that of traditional networks, which use dedicated hardware devices (i.e., routers and switches) to control network traffic. SDN can create and control a virtual network or control a traditional hardware via software.

While network virtualization allows organizations to segment different virtual networks within a single physical network, or connect devices on different physical networks to create a single virtual network, software-defined networking enables a new way of controlling the routing of data packets through a centralized server [10].

3.2. Concept of Software-Defined Networking (SDN)

SDN separates the network into control and forwarding functions, enabling the network control to become directly programmable and allows the underlying infrastructure to be abstracted from applications and network services.

3.2.1. SDN Control Plane

The control plane is responsible for making network-wide decisions and instructing the data plane on how to forward packets [11].

- Centralized - Hierarchical – Distributed:
  - Initial SDN control plane proposals focused on a centralized solution, where a single control entity has a global view of the network. While this simplifies the implementation of the control logic, it has scalability limitations as the size and dynamics of the network increase. To overcome these limitations, several approaches have been proposed, hierarchical and fully distributed approaches.
  - In hierarchical solutions, distributed controllers operate on a partitioned network view, while decisions that require network-wide knowledge are taken by a logically centralized root controller.
  - In distributed approaches, controllers operate on their local view or they may exchange synchronization messages to enhance their knowledge. Distributed solutions are more suitable for supporting adaptive SDN applications.
- Controller Placement:
  A key issue when designing a distributed SDN control plane is to decide on the number and placement of control entities, especially in the context of large networks.

3.2.2. SDN Data Plane

In SDN, the data plane is responsible for processing data-carrying packets using a set of rules specified by the control plane. The data plane may be implemented in physical hardware switches or in software implementations [11]:

- Hardware Switch-based SDNs:
  This approach implements the data plane processing inside a physical device.

- Software Switch-Based SDNs:
  Some physical switches may implement SDN support using software on the device, such as Open vSwitch. Hypervisors may likewise use software implementations to support SDN protocols in the virtual switches used to support their virtual machines.

- Host-Based SDNs:
  Host-based SDNs deploy the SDN agent inside the operating system of the communicating endpoints.

3.3. Architecture of Software-Defined Networking (SDN)

SDN refers to a network architecture where data forwarding plane is controlled by a remote-control plane, which previously operated as a single unit. With this separation, innovative ideas have been proposed and the infrastructure network architecture gains a new direction of network evolution [12].

The SDN architecture (illustrated in Figure 7) is composed of three main layers, each with distinct responsibilities:

3.3.1. Infrastructure Layer (Data Plane)

The lowest layer is an infrastructure layer, also called the data plane, it consists of hardware networking devices which are interconnected with each other for exchanging information, and it is solely responsible for forwarding data packets regardless of network architecture.

The Data Plane generally consists of data forwarding elements, such as Ethernet switches, packet switches, routers, etc., these elements take an active part in data packet forwarding.

3.3.2. Controller Layer (Control Plane)

The middle layer is a controller layer, also called a control plane, this plane is separated from the network core devices and is responsible for unified controlling action. A single SDN controller is responsible for controlling entire data flows of an underlying infrastructure network centrally. SDN controller acts as an operating system for the network (NOS).

3.3.3. Application Layer (Management Plane)

A topmost layer is an application layer, also called management plane, this layer is responsible for management and data-forwarding-related tasks (e.g. data traffic monitoring, mobility management, routing, security, load balancer, etc.).

3.3.4. Communication Interfaces in SDN

- Southbound API:
  In SDN architecture, southbound API are used as a communication protocol between control plane and data plane of the network. These southbound APIs can be an open source or proprietary, the most common open-source example is OpenFlow.
- Northbound API:
  The northbound API in SDN architecture is used to communicate between the SDN controller and applications running over the network. These upper layers use northbound interfaces such as RESTful API

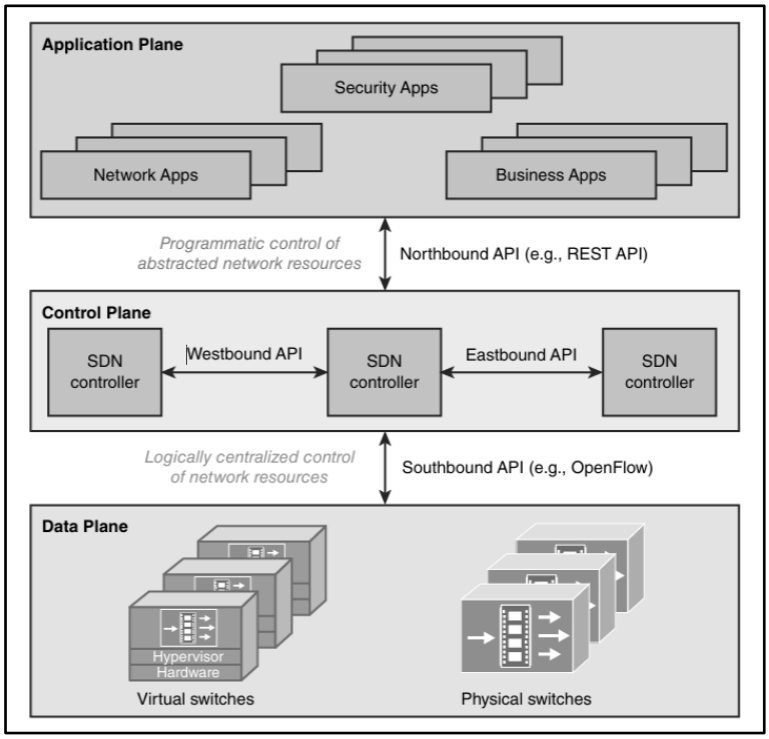

Figure 7: Software-Defined Architecture [20]

3.4. Benefits of Software-Defined Networking (SDN)

SDN adapts the network to ever-changing business needs, and significantly reduces operations and management complexity.

The benefits that enterprises and carriers can achieve through an SDN architecture include [11]:

- Centralized control of multi-vendor environments:

SDN controller can control any network device from any vendor, including switches, routers, and virtual switches. Rather than having to manage groups of devices from individual vendors, administrators can use SDN control software.

- Reduced complexity through automation:
  Instead of manually programming multiple vendor-specific hardware devices, developers can control the flow of traffic over a network simply by programming an open-standard, software-based controller. Networking administrators also have more flexibility in choosing networking equipment, since they can choose a single protocol to communicate with any number of hardware devices through a central controller.

- Increased network reliability and security:
  A software-defined network delivers visibility into the entire network, providing a more holistic view of security threats. With the proliferation of smart devices that connect to the internet, SDN offers clear advantages over traditional networking. Operators can create separate zones for devices that require different levels of security, or immediately quarantine compromised devices so that they cannot infect the rest of the network.

4. Software Defined Wide Area Network (SD-WAN)

4.1. Definition of Software Defined Wide Area Network (SD-WAN)

A Software-Defined Wide Area Network (SD-WAN) is a networking technology that enhances WAN performance. SD-WAN provides secure, reliable, and scalable connectivity across various locations while centralizing management and visibility over the network.

SD-WAN is abstracted from the underlying hardware network and enables a secure virtualized overlay independent of the underlying network. This overlay and abstraction enable SD-WAN to carry the application traffic independent of the physical network. That means SD-WAN can work over multiple links no matter if they are MPLS, LTE or Broadband internet.

4.2. Functionality of Software Defined Wide Area Network (SD-WAN)

SD-WAN architecture splits the network into control and forwarding planes. The control plane is located centrally (often at an organization's headquarters) to enhance network oversight and response. This way, administrators can write rules and policies to deploy across an entire network at once.

4.2.1. Components of Software Defined Wide Area Network (SD-WAN)

The architectural components of a software-defined wide area network include multiple interlocking pieces that collectively create an intelligent, dynamic, and efficient network management system [13]. Figure 8 presents the key components of SD-WAN architecture.

- SD-WAN Edge:
  The SD-WAN edge is essentially the network's frontier where the endpoints reside. These endpoints could be anything from a branch office to a remote data centre or a cloud platform. Each edge can connect to one or more WAN links, such as traditional private lines, MPLS private lines, and Internet links. Edges can provide a wide range of functions, such as application identification, application-based traffic steering, QoS, WAN acceleration, and security.

- SD-WAN Orchestrator:
  The SD-WAN Orchestrator serves as the network's virtual manager. It is responsible for overseeing traffic flow, applying policies and protocols set by network operators. This component provides a centralized platform for operational control, reducing manual intervention and increasing network efficiency.

- SD-WAN Controller:
  The SD-WAN Controller serves as the network's administrative hub, responsible for centralizing network management. It provides operators with a single-pane view of the network, enabling them to set policies for the orchestrator to execute.

- SD-WAN Gateways:
  An SD-WAN gateway is a device that can connect to an SD-WAN overlay network and multiple legacy VPNs. To enable communication between a legacy network (MPLS VPN) and an SD-WAN overlay network, an SD-WAN gateway can function as an intermediate device.

- Overlay Network:
  The overlay network is the virtual WAN architecture that manages the flow of data between different sites, while abstracting the underlying physical network infrastructure. This is what allows SD-WAN to operate more efficiently on optimized traditional, physical infrastructures.

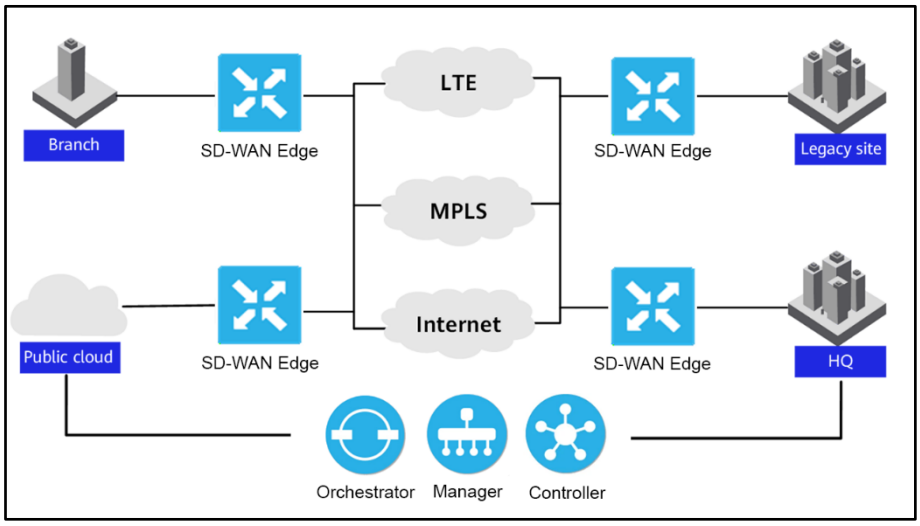

Figure 8: SD-WAN Architecture

4.2.2. Architecture of Software Defined Wide Area Network (SD-WAN)

The logical architecture of the SD-WAN solution consists of the network layer, control layer, and service layer. Each layer provides different functions and contains several core components [13][15].

4.2.2.1. Network Layer:

The network layer can be divided into a physical (underlay) network and a virtual (overlay) network.

- A physical network refers to a WAN created and maintained by carriers. Examples of such a network include a private line network, MPLS network, and the Internet.
- A Virtual network where service policies are deployed on the overlay networks in order to decouple complex services from complex WAN interconnection.

The network layer of SD-WAN is mainly constructed using two types of network elements (NEs), namely, edge and gateway.

4.2.2.2. Control Layer:

The SDN controller functions like a brain of the SD-WAN solution. It provides three functions: network orchestration, control, and management. These functions are described as follows:

- Network orchestration:
  The orchestration component of the SDN controller is responsible for service-oriented network orchestration and automated configuration provisioning. Service orchestration in SD-WAN can be classified into two categories. One category is related to enterprise WAN networking, such as SD-WAN site creation, WAN link creation, VPN creation, and VPN topology definition. The other category is related to network policies, such as application identification, application-based traffic steering, QoS, and WAN optimization policies.

- Network control:
  The control component of the SDN controller is responsible for centralized control of the network layer in SD-WAN and implements on-demand interconnections of enterprise WANs based on user intents. Compared with the distributed control mode of legacy networks, the centralized control mode separates the control plane from the forwarding plane, simplifying enterprise WAN O&M, minimizing network configuration errors, and optimizing enterprise WAN O&M efficiency.

- Network management:
  The management component of the SD-WAN controller implements management and O&M of enterprise WANs. For example, the component collects alarms and logs of SD-WAN NEs; collects and analyses performance statistics of links, applications, and networks; and intuitively presents a multidimensional display of O&M information such as network topologies, faults, and performance.

4.2.2.3. Service Layer:

The service layer of SD-WAN interconnects with the controller to present and provision SD-WAN services through service interfaces. Typically, there are two types of service interfaces. One type lies in the in-house portal, this in-house portal can be directly deployed and used by enterprise customers. The other type comes to the northbound open API. That is, the SD-WAN controller can be integrated with third-party service orchestration systems belonging to carriers or enterprises. The third parties can customize the portal and service provisioning process according to their requirements for service functions and display style.

4.3. Key features and benefits of SD-WAN

SD-WAN technology is important as it enhances network performance across wide area networks and offers better performance, increased security, and flexibility. SD-WANs optimize data flow based on current network conditions, application needs, and pre-defined policies, allowing greater control without sacrificing performance or incurring high costs. The key benefit of SD-WAN technology is that it can identify the best possible routes for traffic, and this simplification improves overall speed and service quality [14].

4.3.1. Features of Software Defined Wide Area Network (SD-WAN)

- Better application experience:
  SD-WAN allows remote sites to connect more easily to networks, data centres, and/or multiple-clouds with lower latency, better performance, and more reliable connectivity. When users demand more of their applications and infrastructure at unprecedented agility and scale, an appealing user experience can be make-or-break.

- Efficient operations:
  As network infrastructures have evolved, the sprawl of point products used for networking and security increases complexity. SD-WAN uses automation to make connectivity a simpler process across mixed environments, including on-premises, hybrid, and cloud. SD-WAN enables centralized orchestration, zero-touch provisioning, and analytics along with deep integrations of cloud on-ramps to accelerate cloud connectivity.

- Enhanced security posture:
  An SD-WAN solution needs to have integrated security. Otherwise, it's just another connectivity option that unfortunately becomes an attack vector. When properly implemented, secure SD-WAN enables private, secure and direct internet access. It's critical that an SD-WAN solution can ensure consistent security at all edges, from flexible WAN edges to the cloud edge.

4.3.2. Benefits of Software Defined Wide Area Network (SD-WAN)

SD-WAN offers an alternative to traditional WAN architectures, delivering significant advantages in performance, security, and cost-efficiency. By intelligently routing traffic across a mix of connections like broadband internet, MPLS, and LTE, SD-WAN optimizes network resources. This translates to faster application performance, improved productivity, and greater business agility. Some of its key benefits are [13]:

- Improved network performance:
  SD-WAN prioritizes business-critical applications, ensuring optimal performance and minimal latency. It dynamically adjusts traffic flows based on real-time network conditions, maximizing bandwidth utilization. This results in a smoother and more responsive experience for users, regardless of their location.

- Enhanced security:
  SD-WAN incorporates advanced security features like next-generation firewalls, intrusion prevention systems, and secure web gateways. It enables secure segmentation of the network, isolating sensitive data and applications from potential threats. This comprehensive approach strengthens the security posture and protects against evolving cyberattacks.

- Cost efficiency:
  SD-WAN reduces reliance on expensive MPLS circuits by leveraging cost-effective broadband internet connections. It optimizes bandwidth utilization, minimizing the need for costly upgrades. This leads to significant cost savings without compromising performance or security.

- Centralized management:
  SD-WAN provides centralized control and visibility over the entire network, simplifying management and configuration. Administrators can easily define and enforce policies, monitor performance, and troubleshoot issues from a single interface. This streamlines operations and reduces the burden on IT staff.

- Scalability and flexibility:
  SD-WAN allows businesses to easily scale their network up or down as needed, accommodating growth and changing demands. It supports a wide range of connectivity options, providing flexibility to adapt to different environments and requirements. This ensures the network can evolve with the business, supporting new initiatives and enabling digital transformation.

- Full Visibility
  SD-WAN architecture provides a holistic view of the network, allowing operators to monitor and manage network activities efficiently.

- Analytics and Troubleshooting
  The architecture provides valuable insights into network performance and application issues, improving troubleshooting and reducing response time to network outages.

4.4. Comparison between SD-WAN and Traditional WAN (MPLS)

SD-WAN evolved from MPLS technology. In many ways, SD-WAN can be seen as a software abstraction of MPLS technology that's applicable to wider scenarios: It brings secure, private connectivity that's agnostic to all kinds of links and providers and is cloud-aware. While MPLS handled failure scenarios with backup links, SD-WAN handles them with real-time traffic steering based on centralized policy. Also, since SD-WAN unifies the entire WAN backbone, it delivers comprehensive analytics across the network globally. This wasn't possible before, because of disparate pieces of infrastructure and policy.

This table offers detailed comparison between SD-WAN and Traditional WAN (MPLS)[17]:

	SD-WAN	**Traditional WAN (MPLS)**
Cost	Consolidated services greatly reduce TCO	Expensive to build and maintain
Approach	Software Defined WAN provides a software defined approach of managing Wide Area Network.	Traditional WAN provides a conventional approach of managing Wide Area Network.
Flexibility	It provides a better flexibility in WAN management	It fails to provide a better flexibility in WAN management
Configuration time	New configuration and scale up takes very low time	New configuration and scale up takes very high time
Automatic configuration	In SD WAN network configuration is done automatically without requiring human intervention	In traditional network configuration is done by skilled resources means requires human intervention.
Speed connectivity	It provides low cost and high-speed connectivity.	It does not provide low cost and high-speed connectivity
Performance	It provides high performance for the application in cloud as it directly accesses applications hosted in cloud.	It provides low performance for the application in cloud as it connects to intermediate hub then to cloud
Data centres limitation	In Software Defined WAN, Data centres are not limited based on underlying hardware that comprises the network	In traditional WAN, Data centres are limited in their capacity to deal with incoming connections to multiple cloud platforms
Complexity	Software Defined WAN simplifies the complexity associated with management, configuration and infrastructure arrangement of WANs.	Traditional WAN increases the complexity associated with management, configuration and infrastructure arrangement of WAN
Security features	SD WAN solutions provide secure VPN than traditional WAN and also integrates additional features like firewall, Wan Optimization, SWG etc.	Traditional WAN solutions may not provide secure VPN like SD WAN and also fails to fully integrate additional features like firewall, Wan Optimization, SWG etc.
Data security	SD WAN provides a secured data traffic through end-to-end encryption over a virtual private network (VPN) connection also integrates additional security features.	Traditional WAN is secure over an MPLS connection as packets that are sent are private as well as packet loss is avoided

Table 1: Comparison between SD-WAN and Traditional WAN (MPLS)

5. Migrating from MPLS to SD-WAN

5.1. SD-WAN implementation

The benefits of software-defined WAN make many organizations interested in adopting it, but the implementation process can seem daunting. Enterprises can use this seven-step process as a guide to deploy a successful SD-WAN implementation.

5.1.1. SD-WAN implementation steps

The seven steps of an SD-WAN implementation [20]:

- Step 1. Collect requirements
  Collecting requirements is always the first step to implement an SD-WAN architecture.

- Step 2. Identify site profiles
  Use the functional requirements specification to identify connectivity requirements, application traffic flows, quality of service (QoS), quality of experience, bandwidth and security.

- Step 3. Select proof-of-concept sites
  Identify proof-of-concept (POC) sites. by selecting a few of the most important site types for the POC. Once those are identified, the next step is to determine the circuit characteristics of the sites to order the corresponding test circuits. The lead time for procuring circuits is normally long, so teams should place circuit orders for the sites as soon as they know which links to order.

- Step 4. Evaluate products
  Begin evaluation of potential products, referring to industry resources for potential vendors, and begin assembling selection criteria. The market changes quickly, with new product features releasing periodically. Competition is fierce, but expect that features are comparable across vendors, with some proprietary variations. Functions like Secure Access Service Edge are becoming commonplace.

- Step 5. Choosing deployment model
  Next, determine the types of available offerings: DIY, co-managed with a managed service provider or fully outsourced to an MSP. The selection depends on the resources teams can muster for the evaluation and implementation. For example, a global enterprise may find it useful to partner with an MSP who has established relationships with ISPs in foreign countries.

- Step 6. Test the proof of concept
  Begin hands-on evaluation with the POC in the lab. This step can happen while waiting for circuits and can cover as many products as necessary, although network teams should likely limit it to the top two or three candidates. Be sure to evaluate performance using traffic generators and monitoring functions.

- Step 7. Determine the SD-WAN model
  Determine the appropriate deployment model. Vendors either offer preferred models or provide choices to customers. This step validates the implementation and the deployment model in the production environment. It should result in few surprises, other than perhaps finding a forgotten application or two. Include at least one of each type of critical production site in this step to verify that the product satisfies the most stringent requirements.

5.1.2. SD-WAN implementation techniques

Different SD-WAN implementations result in varying architectures. Three primary types are common [17]:

- On-Premises SD-WAN:
  In this architecture, the SD-WAN hardware resides on-site. Network operators have direct, secure access and control over the network and hardware, offering enhanced security for sensitive information.

- Cloud-Enabled SD-WAN:
  This form of SD-WAN architecture connects to a virtual cloud gateway over the internet, enhancing network accessibility and facilitating better integration and performance with cloud-native applications.

- Cloud-Enabled with Backbone SD-WAN:
  This architecture gives organizations an extra layer of security by connecting the network to a nearby point of presence (PoP), like a data centre. It allows traffic to shift from the public internet to a private connection, enhancing network security and providing a fallback in case of connection failures.

5.2. SD-WAN deployment

5.2.1. SD-WAN deployment model

SD-WAN deployment models are primarily determined by the organization's network and business requirements. An organization may opt for one of three deployment models [18]:

- Do-it-yourself (DIY)

  The organization purchases the SD-WAN solution directly from a vendor and manages all aspects of deployment and system management internally.

- Fully Managed

  The organization delegates the entirety of the SD-WAN deployment and management process to a Managed Service Provider (MSP).

- Co-managed or Hybrid

  Here, the organization retains control over certain aspects of the SD-WAN management while outsourcing the remainder to an MSP.

The choice between these models primarily depends on the organization's size and the capabilities of its IT team.

5.2.2. SD-WAN deployment form factors

The SD-WAN architecture includes various form factors [17]:

- Physical Appliance: A device installed on-premises at locations such as branch offices or data centres.
- Virtual: A virtual machine set up on universal customer premises equipment or servers at branch locations.
- Cloud: This version of SD-WAN is operated using software situated in a cloud environment.

5.3. Migration challenges for Entreprises

Migrating from traditional MPLS to SD-WAN is a transformative step for organizations, enhancing flexibility, cost-effectiveness, and overall network management. However, like any significant shift in infrastructure, migration can present its unique challenges. Let’s delve into these challenges with a balance of technical depth and clarity [19].

5.3.1. Infrastructure Assessment and Compatibility

- Legacy Hardware
  Legacy hardware, often deeply embedded in an organization’s network infrastructure, can pose significant hurdles when considering a migration to SD-WAN.

- Interoperability
  SD-WAN solutions may not always play well with existing network equipment. For example, an existing WAN optimization controller, tailored to enhance MPLS performance, might not be compatible with SD-WAN’s dynamic traffic routing mechanisms. Similarly, traditional firewalls, configured for static MPLS paths, could struggle with SD-WAN’s fluctuating traffic patterns. This misalignment can result in inefficient traffic flow, dropped connections, or even security vulnerabilities.

- Bandwidth Considerations
  Variable Bandwidth: Unlike MPLS, which offers guaranteed bandwidth, SD-WAN utilizes public internet, which can have varying congestion levels, potentially affecting performance.
  Application Performance: Ensuring that critical applications receive the necessary bandwidth and priority is crucial. This requires an accurate assessment of application traffic and crafting appropriate SD-WAN policies.

- Security Concerns
  Public Internet Exposure: Shifting to SD-WAN, which predominantly uses the public internet, can expose traffic to more threats. Integrating next-gen firewalls, secure web gateways, and other advanced security features is vital.
  End-to-End Encryption: MPLS inherently trusts the core network, while SD-WAN treats every segment as untrusted, demanding robust encryption across the board. Ensuring encryption doesn't impede performance is a challenge.

5.3.2. Deployment & Configuration Complexity

- Zero-Touch Provisioning (ZTP)
  At its core, ZTP is a mechanism that automates configuring devices in a network without manual intervention. For instance, when a new branch office is set up, ZTP can allow for routers, switches, and other equipment to be provisioned automatically. However, the catch is in the setup. Implementing ZTP demands a robust initial configuration and a deep understanding of the underlying infrastructure.

- Policy Configuration
  While powerful, the dynamic path selection feature of SD-WAN necessitates careful policy configurations for diverse traffic types. For instance, a company might prioritize video conferencing traffic over regular file transfers to ensure smooth meetings. This requires network administrators to create nuanced policies, considering the criticality and bandwidth requirements of various applications, which can be a meticulous and intricate task.

- Skillset & Training
  New Technology Curve: IT teams familiar with MPLS may need extensive training on SD-WAN technologies and strategies, impacting rollout timelines.
  Vendor Variance: With many SD-WAN vendors in the market, each with its nuances, training must be specific to the chosen solution.

5.3.3. Operational Concerns

- Monitoring & Reporting
  Unlike the more predictable and static paths of MPLS, the dynamic essence of SD-WAN means that paths might change in real-time based on various network conditions like latency, jitter, or packet loss. This dynamic behaviour necessitates advanced monitoring solutions. For example, in a global corporation with branches across continents, SD-WAN might shift from one internet connection to another during heavy data transfers. While this ensures optimal performance, it also means that IT teams need to have detailed visibility and alerts for these shifts.

- Failover & High Availability
  SD-WAN's architecture inherently supports failover, ensuring that if one connection path fails, the traffic is rerouted to another available path. However, the real challenge is guaranteeing this transition is seamless, especially during peak traffic. Consider a financial institution executing high-frequency trades; even a minor hiccup during a path switch can lead to significant financial implications.

- Vendor Lock-in
  Choosing a single vendor solution can sometimes lead to limitations in flexibility and future scaling. Organizations should be mindful of this and consider interoperability with other systems and potential future changes in their needs.

Conclusion

The evolution of Wide Area Network (WAN) technologies reflects the growing demands of modern enterprise environments. Traditional WAN solutions, such as those based on MPLS, have served organizations for many years but face limitations in cost, flexibility, and adaptability, particularly in the context of cloud-centric and distributed applications.

This chapter has provided a comprehensive overview of WAN development, from its foundational role and the operation of MPLS networks, to the emergence of Software-Defined Networking (SDN) and Software-Defined Wide Area Network (SDWAN) which offer numerous benefits including centralized management, application-aware routing, enhanced security, and cost optimization.

Furthermore, we explored the key steps and models involved in migrating from legacy WAN architectures to SD-WAN, highlighting both key opportunities and the challenges enterprises may encounter during the transition.

Building upon our understanding of WAN evolution and the fundamental principles of SD-WAN technology, we now focus on the practical implementation landscape. Chapter 2 delves into the comparative analysis of available SD-WAN solutions, with particular emphasis on Cisco Catalyst SD-WAN's architecture, components, and operational capabilities that make it a leading choice for enterprise deployments.

Chapter Two:
Architecture and Operation of the Cisco SD-WAN Solution

Contents:

Introduction

Building on the foundational concepts introduced in the previous chapter. This chapter begins with a general overview of existing SD-WAN solutions, highlighting the technological principles they share and the key differentiators between vendor offerings. It then shifts focus to Cisco Catalyst SD-WAN, presenting its architecture and components. The chapter also explores how Cisco SD-WAN uses policy-based management to optimize traffic, while its integrated security features protect distributed networks.

By the end of this chapter, Cisco Catalyst SD-WAN is explored in depth, highlighting its architectural strengths and demonstrating how it enforces centralized control over enterprise sites, making them more scalable and secure.

1. Overview of SD-WAN Solutions

With numerous solutions available in the market and a vast ecosystem of vendors, SD-WAN provides an opportunity for companies to simplify their WAN architecture.

Different SD-WAN solutions align themselves in various ways with different enterprise priorities. Some SD-WAN solutions offer included end-to-end VPN options as standard where others work well with IoT items. Other SD-WAN offerings are designed to provide high-quality voice and video performance or outstanding connections to SaaS platforms [22].

Gartner, a research organization, publishes an annual report titled “2024 Gartner® Magic Quadrant™ for SD-WAN”. It provides a detailed analysis and review of the various vendors in the WAN-Edge market. Figure 9 shows the graph for “2024 Gartner® Magic Quadrant™ for SD-WAN” released by Gartner in September 2024.

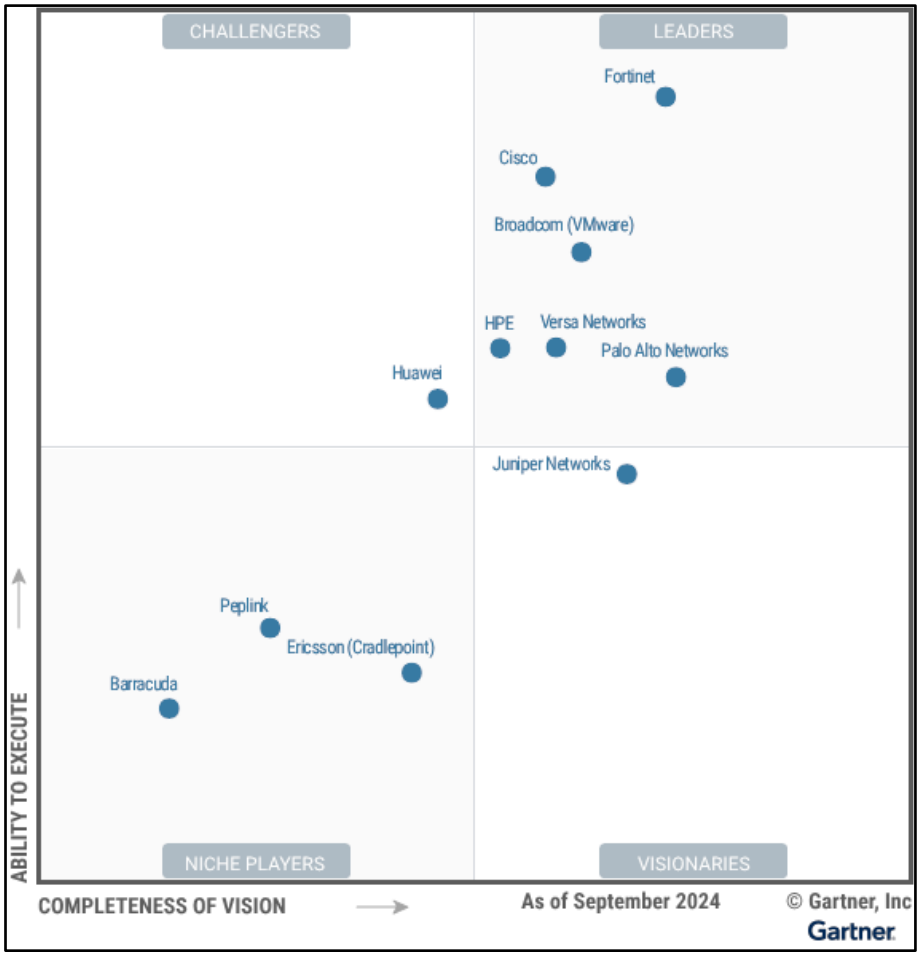

Figure 9: 2024 Gartner® Magic Quadrant™ for SD-WAN [23]

1.1. Fortinet Secure SD-WAN

The Fortinet Secure SD-WAN solution is comprised of multiple components. Overall, the components that make up the Fortinet Secure SD-WAN solution are: FortiGate, FortiManager, FortiAnalyzer, and FortiDeploy.

FortiGate runs FortiOS, the core of the Secure SD-WAN solution. FortiManager drives orchestration and management. FortiAnalyzer and FortiDeploy help the whole solution come together, delivering a solution that is unmatched by other vendors [24].

1.2. Cisco Catalyst SD-WAN

Cisco emerged as a leader in Gartner's magic quadrant 2024. Cisco offers two SD-WAN solutions, one is Cisco Catalyst SD-WAN, and the second is Cisco Meraki SD-WAN.

The more popular and mainstream SDWAN solution is Cisco Catalyst SD-WAN powered by Viptela solution which includes vSmart Controller, vManage, vBond Orchestrator and vEdgeCloud router.

1.3. VMware VeloCloud SD-WAN

VMware VeloCloud SD-WAN is a cloud network service solution. VMware SD-WAN solution offers VMware SD-WAN Edge, VMware SD-WAN gateways, and VMware SD-WAN orchestrator and controllers.

VMware SD-WAN Edge is an enterprise-class appliance providing secure and optimized connectivity to applications anywhere, on and off the cloud.

VMware Gateways optimize data paths to all applications, branches, and data centers, along with the ability to deliver network services to and from the cloud.

VMware Orchestrator is a cloud-hosted or on-premises central management tool. Its web-based user interface provides simplified configuration, provisioning, monitoring, fault management, logging, and reporting functions [25].

1.4. Versa Secure SD-WAN

Versa Secure SD-WAN is an advanced, innovative networking platform. the Versa SD-WAN service separates network services from physical infrastructure, thus enabling organizations to control WANs with high efficiency while not necessarily focusing on the physical layer.

Versa SD-WAN comprises several key components, VOS (Versa Operating System) is an operating system that offers multiple functionalities that are much needed for the SD-WAN solution.

VSAC (Versa Software-Defined WAN Controller) is a cloud-based component that allows remote users and devices to have secure access to the network. Versa SD-WAN Appliances is the Edge physical hardware [26].

1.5. HPE Aruba Networking EdgeConnect SD-WAN

The HPE Aruba Networking EdgeConnect SD-WAN platform enables enterprises to improve application performance and reduce the cost and complexity of building a WAN by leveraging broadband internet to connect users to applications. Three components comprise the HPE Aruba Networking EdgeConnect SD-WAN platform:

HPE Aruba Networking EdgeConnect SD-WAN are defined as physical or virtual SD-WAN appliances and are deployed in branch offices.

HPE Aruba Networking EdgeConnect SD-WAN Orchestrator, included with the EdgeConnect SD-WAN platform, provides high level of visibility into both legacy and cloud applications, and centrally assigns policies based on business intent to secure and control all WAN traffic.

HPE Aruba Networking EdgeConnect WAN Optimization is an optional performance pack that combines WAN optimization technologies with EdgeConnect SD-WAN to create a single, unified WAN edge platform [27].

SD-WAN comparison chart

Vendors	Cisco Catalyst SD-WAN	Fortinet Secure SD-WAN	Versa Secure SD-WAN	VMware VeloCloud SD-WAN	HPE Aruba Networking EdgeConnect SD-WAN
Supports traditional routing and SD-WAN	✅ Available (SD-WAN available with existing infrastructure)	✅ Available (SD-WAN available with existing infrastructure)	✅ Available (SD-WAN available with existing infrastructure)	⚠ Limited (No smooth migration)	✅ Available (Supports traditional routing, firewall, and SDWAN)
Purpose-built SDWAN Architecture	✅ Available (Dedicated control, data, and management plane components)	⛔ Not Available (Legacy firewall-based Architecture)	✅ Available (Dedicated control, data, and management plane components)	✅ Available (Dedicated control, data, and management plane components)	⛔ Not Available (Integrated control plane and data plane within each firewall)
Remote branch security services	✅ Available (Includes enterprise firewall with application-awareness, IDS/IPS, URL filtering)	✅ Available (Features with IPS/IDS, application control)	✅ Available (Features with IPS/IDS, application control)	⚠ Limited (Performance impact unknown)	⚠ Limited (Lacks security integrations in the SDWAN console)
Encrypted traffic Analysis	✅ Available (Detects malware by matching encrypted SHA)	✅ Available (Provides TLS/SSL traffic Encryption)	✅ Available (Provides TLS/SSL traffic Encryption)	⛔ Not Available (Cannot detect encrypted Malware)	⛔ Not Available (Cannot detect encrypted Malware)
Security insights	✅ Available (Better visibility and control through security insights)	✅ Available (Provides security insights with event logging on a security-centric dashboard)	✅ Available (Dashboard display for applications analytics, URL filtering, stateful Firewall)	⚠ Limited (Basic monitoring insights with no security monitoring dashboard)	⚠ Limited (Limited security insights with no security monitoring dashboard)
SaaS connectivity	✅ Available (SaaS applications based on performance metrics and best path selection)	⚠ Limited (Basic SaaS optimization)	⚠ Limited (Basic SaaS optimization)	⚠ Limited (SaaS optimization based on manual application rule creation)	✅ Available (SaaS applications based on performance metrics and best path selection)
Data centre Integration	✅ Available Data Centre integration	⛔ Not Available (No data centre Integration)	⛔ Not Available (No data centre Integration)	✅ Available Data Centre integration	⛔ Not Available (No data centre Integration)
Analytics and visibility	✅ Available (Advanced visibility and analytics into network and app performance)	⚠ Limited (Visibility and analytics into network and app performance)	⚠ Limited (Visibility and analytics into network and app performance)	⚠ Limited (Basic visibility and analytics into network and app performance)	⚠ Limited (Basic SD-WAN visibility with Aruba Unity Orchestrator)

Table 2: SD-WAN comparison chart [28]

Table 2 highlights that Cisco Catalyst SD-WAN offers the most comprehensive and balanced solution, with strong support for traditional routing, a purpose-built SD-WAN architecture, integrated security, advanced analytics, and seamless cloud and data centre connectivity. Fortinet and Versa provide solid security-focused SD-WAN solutions, but lack full architectural separation or integration features. VMware VeloCloud delivers a scalable SD-WAN core but falls short in security and visibility. Aruba EdgeConnect, while supporting core SD-WAN functions, is more limited in architecture and security analytics. Ultimately, Cisco stands out as the most complete enterprise-grade SD-WAN platform among the evaluated vendors. Figure 10 shows this solutions logos:

Figure 10: SD-WAN solution leaders

Why we choose Cisco Catalyst SD-WAN

In the context of this project, we chose to implement Cisco Catalyst SD-WAN over other available solutions and various open-source alternatives. This choice is motivated by several technical and practical considerations that align with enterprise needs and educational goals.

Firstly, Cisco Catalyst SD-WAN offers a well-structured, modular architecture that simplifies deployment and management. Its user-friendly interface, centralized vManage dashboard, and rich monitoring capabilities provide greater visibility and control over the network infrastructure, which is essential for enterprise environments.

Secondly, Cisco's solution is less complex to implement compared to other commercial solutions, making it more accessible for lab-based environments and educational simulations. This aspect is particularly important for practical learning and aligns with the requirements of Cisco Certified Internetwork Expert (CCIE) certification tracks, which often involve Catalyst SD-WAN technologies in their lab exams.

Moreover, Cisco Catalyst SD-WAN integrates a wide range of built-in features, including advanced security policies, firewall services, encryption mechanisms, and application-aware routing, all of which are crucial for securing and optimizing enterprise connectivity. In contrast, many open-source SD-WAN solutions lack these features and typically require additional manual configurations or third-party tools to achieve equivalent functionality.

Lastly, Cisco's extensive documentation, community support, and virtualized infrastructure make it a highly lab-friendly and scalable solution, suitable for both real-world deployment and academic experimentation.

For these reasons, Cisco Catalyst SD-WAN was selected as the ideal solution for this implementation project.

2. Cisco Catalyst SD-WAN Solution

The Cisco Catalyst SD-WAN is a Software-Defined WAN (SD-WAN) solution. It is an enterprise-grade SD-WAN architecture overlay that enables digital and cloud transformation for enterprise. The solution fully integrates routing, security, centralized policy and orchestration into large-scale networks and addresses the problems and challenges of common WAN deployments [29].

Cisco Catalyst SD-WAN forms a software overlay that runs over standard network transport services, including the public Internet, MPLS, and LTE. The overlay network also supports next-generation software services, such as cloud applications [30].

3. Cisco Catalyst SD-WAN Components

Cisco Catalyst SD-WAN is a distributed architecture that provides a clear separation between the management plane, control plane, and data plane. Figure 11 summarise Cisco Catalyst components and the interconnection between them.

3.1. Cisco vManage

In the management plane, Cisco vManage represents the user interface of the solution. Network administrators and operators perform configuration, onboarding, policy creation, provisioning, troubleshooting, and monitoring. vManage offers both a single-tenant dashboard and a multitenant dashboard for a variety of customer and service provider deployments.

Cisco vManage is used to store certificate credentials, and to create and store configurations for all Cisco edge network components. As these components come online in the network, they request their certificates and configurations from vManage. When vManage receives these requests, it pushes the certificates and configurations to the vEdge devices. For Cloud routers, vManage can also sign certificates and generate bootstrap configurations, and it can decommission the devices.

Cisco vManage communicates with vEdge devices and controllers using a secure channel Datagram Transport Layer Security (DTLS) tunnel. Within this secure channel, it communicates with the devices or controllers using the NETCONF protocol, within an SSH session [30].

The vmanage-admin account is created during the initial device or controller setup. vManage uses this secure channel for monitoring, configuring, and managing each of the following:

- Cisco SD-WAN vEdge devices
- Cisco SD-WAN Validator (vBond Orchestrator)
- Cisco SD-WAN Controller (vSmart)

vManage is also highly scalable, depending on the needs of the environment. When vManage is clustered, redundancy can be provided, with multiple clusters deployed regionally or globally. A single cluster is made up of three or more vManage NMSs. A vManage cluster can manage up to 6,000 WAN Edges, with each cluster node handling 2,000 WAN Edges.

3.2. Cisco vSmart

The component that provides control plane functionality is vSmart. vSmart is the brain of the SD-WAN network. vSmart is highly scalable and can handle up to 5,400 connections per vSmart server with up to 20 vSmarts in a single deployment. A WAN Edge can connect to up to three vSmarts at a time but only needs connectivity to one to get policy information [31].

Traditional link-state and distance-vector protocols, such as OSPF and IS-IS, rely on distributed computation and limited network visibility, leading to potential inefficiencies. In contrast, Cisco SD-WAN centralizes routing intelligence within vSmart controllers, enabling globally optimized routing decisions [31].

The Cisco vSmart Controller oversees the control plane of the Cisco Catalyst SD-WAN overlay network, establishing, adjusting, and maintaining the connections that form the Cisco Catalyst SD-WAN network.

The major components of the Cisco vSmart Controller are [30]:

- Control plane connections: Each Cisco vSmart Controller establishes and maintains a control plane connection with each edge router in the overlay network. Each connection, which runs as a DTLS tunnel, is established after device authentication succeeds, and it carries the encrypted payload between the Cisco vSmart Controller and the vEdge router. This payload consists of route information necessary for the Cisco vSmart Controller to determine the network topology, and then to calculate the best routes to network destinations and distribute this route information to the Edge routers.
- OMP (Overlay Management Protocol): The OMP protocol is a routing protocol similar to BGP that manages the Cisco Catalyst SD-WAN overlay network. OMP runs inside DTLS control plane connections and carries the routes, next hops, keys, and policy information needed to establish and maintain the overlay network.
- Authentication: The Cisco vSmart Controller has pre-installed credentials that allow it to authenticate every new edge router that comes online. These credentials ensure that only authenticated devices are allowed access to the network.
- Netconf and CLI: Netconf is a standards-based protocol used by Cisco vManage to provision a Cisco vSmart Controller. In addition, each Cisco vSmart Controller provides local CLI access and AAA.

3.3. Cisco vBond

Cisco vBond is a Validator -previously called Orchestrator-, It coordinates the initial onboarding of Cisco SD-WAN Controllers and vEdge routers. During the onboarding processes, the Cisco vBond authenticates and validates the devices wishing to join the overlay network.

Cisco vBond is the only Cisco vEdge device that is located in a public address space. This design allows the vBond to communicate with Cisco SD-WAN Controllers and vEdge routers that are located behind NAT devices, and it allows the vBond to solve any NAT-traversal issues of these Cisco vEdge devices.

The major components of the Cisco SD-WAN Validator are:

- Control plane connection: Each vBond has a persistent control plane connection in the form of a DTLS tunnel with each Cisco Catalyst SD-WAN Controller and vEdge routers.
- NAT traversal: vBond facilitates the initial orchestration between edge routers and Cisco SD-WAN Controllers when one or both of them are behind NAT devices. Standard peer-to-peer techniques are used to facilitate this orchestration.
- Load balancing: In a domain with multiple Cisco SD-WAN Controllers, vBond automatically performs load balancing of vEdge routers across the Cisco SD-WAN Controllers when routers come online.

To provide redundancy for the Cisco vBond, multiple vBonds can be created in the network and point all edge routers. Each vBond maintains a permanent DTLS connection with each Cisco Catalyst SD-WAN Controller in the network. If one vBond becomes unavailable, the others are automatically and immediately able to sustain the functioning of the overlay network. In a domain with multiple Cisco SD-WAN Controllers, the vBond pairs a vEdge router with one of the Cisco SD-WAN Controllers to provide load balancing [30].

3.4. Cisco vEdge

Cisco vEdge is an edge router, whether a hardware or software device, it is responsible for the data traffic sent across the network.

The components of vEdge router are [30]:

- DTLS control plane connection: Each vEdge router has one permanent DTLS connection to each Cisco SD-WAN Controller. This permanent connection is established after device authentication succeeds, and it carries encrypted payload between the edge router and the Cisco SD-WAN Controller. This payload consists of route information necessary for the Cisco SD-WAN Controller to determine the network topology, and then to calculate the best routes to network destinations and distribute this route information to the edge routers.
- OMP (Overlay Management Protocol): OMP runs inside the DTLS connection and carries the routes, next hops, keys, and policy information needed to establish and maintain the overlay network. OMP runs between the edge router and the Cisco SD-WAN Controller and carries only control information.
- Protocols: vEdge router supports standard protocols, including OSPF, BGP, VRRP, and BFD.
- Routing Information Base (RIB): Each vEdge router has multiple route tables that are populated automatically with direct interface routes, static routes, and dynamic routes learned via BGP and OSPF. Route policies can affect which routes are stored in the RIB.
- Netconf and CLI: Netconf is a standards-based protocol used by vManage to provision a vEdge router. In addition, each edge router provides local CLI access and AAA.

Direct Internet Access (DIA):

Direct Internet Access (DIA) improves internet experience for branch users by eliminating latency in backhauling traffic to a central site. It reduces bandwidth consumption at the central site, which thereby also reduces WAN costs.

The Cisco SD-WAN DIA solution is secure and easy to implement. DIA is configured for specific applications and keeps business critical applications on premium WAN links, DIA can be enabled for internet browsing and SaaS applications, whereas business critical or latency sensitive applications such as voice. An essential feature of the Cisco SD-WAN solution is the ability to segment users. Segmentation is useful in keeping employees and guests separate. Cisco SD-WAN allows DIA to be configured for a VPN segment, allowing control of internet access on a per VPN segment basis [32].

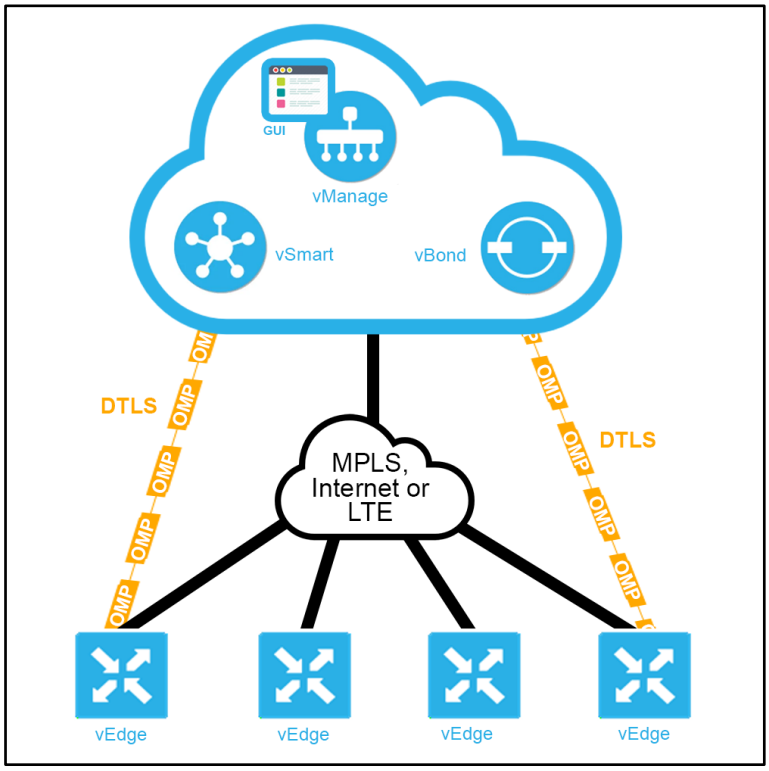

Figure 11: Cisco Catalyst SD-WAN components

4. Overlay Management Protocol (OMP)

Within the Cisco SD-WAN solution, the routing protocol selected is the Overlay Management Protocol (OMP), It runs between the vSmart controllers and WAN Edge routers where control plane information, such as route prefixes, next-hop routes, crypto keys, and policy information, is exchanged over a secure connection. If no policy is defined, the default behaviour of OMP is to allow a full mesh topology, where each WAN Edge router can connect directly to other WAN Edge routers.

OMP is enabled by default and doesn't need to be explicitly enabled. As components in the fabric learn about their respective control elements, they will automatically initiate control connections to them. With this information, reachability can be achieved, which ultimately allows for the orchestration of the topology. Figure 12 show OMP and its DTLS Tunnels between vSmart and vEdge sites.

Cisco Catalyst SD-WAN control plane architecture uses three types of OMP routes [30] [31] [32]:

- OMP routes: Prefixes that are learned at the local site. The prefixes are redistributed into OMP so that they can be carried across the overlay. OMP routes advertise attributes including transport location (TLOC) information, which is similar to a BGP next-hop IP address for the route, and other attributes such as origin, originator, preference, site ID, tag, and VPN.

- TLOC routes: The logical tunnel termination points on the WAN Edge routers that connect into a transport network. A TLOC route is uniquely identified and represented by a three-tuple, consisting of system IP address, link color, and encapsulation.
- Service routes: represent services (such as firewall, IPS, application optimization, etc.) that are connected to the WAN Edge local-site network and are available for other sites. In addition, these routes also include VPNs. VPN labels are sent in this update type to tell the vSmart controllers which VPNs are serviced at a remote site.

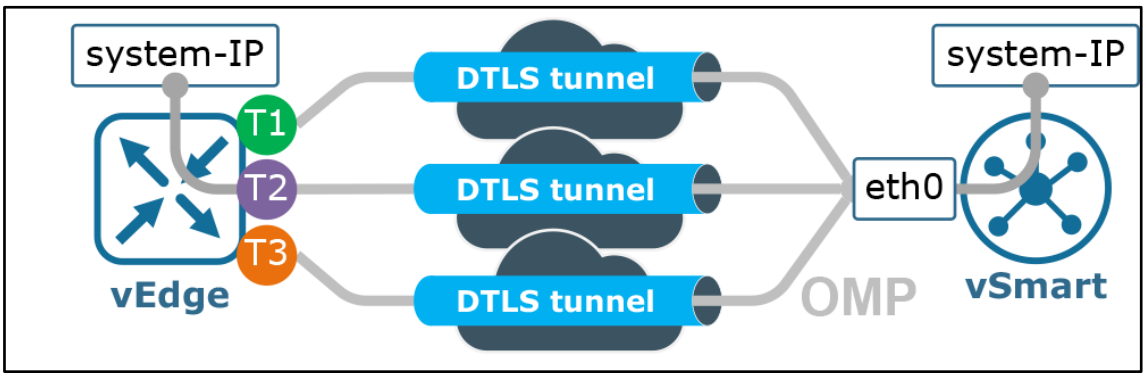

Figure 12: OMP peering over DTLS [33]

5. Cisco SDWAN policies

Cisco SD-WAN policies are the mechanism through which administrators can encode their intent into the network fabric. Policies are the way that network administrators configure the Cisco SD-WAN fabric in order to meet their business intentions.

Network administrators use several different types of policies (shown in Figure 13) in order to meet their business objectives. Policies can be classified as either centralized policies or localized policies. Generally speaking, centralized policies control routing information and data that is forwarded across the Cisco SD-WAN fabric. Localized policies control routing and traffic forwarding at the perimeter of the Cisco SD-WAN fabric were WAN Edge routers interface with traditional routers [31].

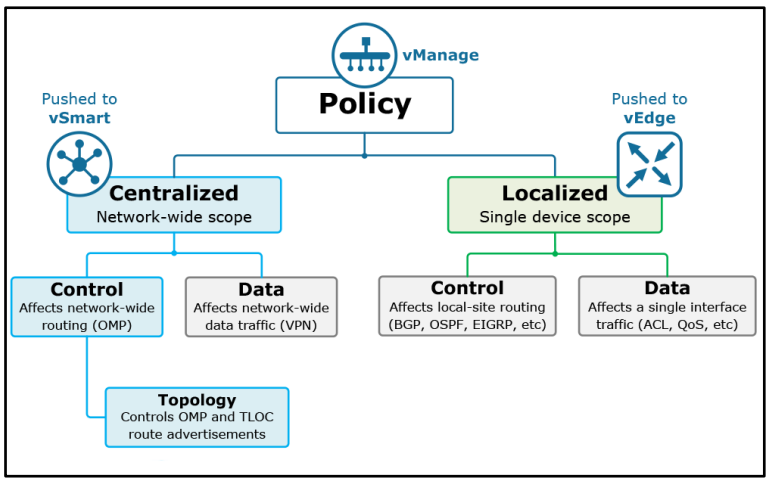

Figure 13: Cisco SD-WAN policies types [33]

5.1. Centralised Policies

Centralized policies can be further classified as either control policies (called topology policies in the vManage GUI) or data policies (called traffic policies in the vManage GUI). Control policies are used to manipulate the structure of the Cisco SD-WAN fabric by altering the control plane information exchanged by the Overlay Management Protocol (OMP). Data policies are used to manipulate the data plane directly by altering the forwarding of traffic through the Cisco SD-WAN fabric [31].

- **Centralized Control Policy:**
  Control policies are used to manipulate the propagation of routing information in the control plane, including manipulating or filtering OMP routes and Transport Locator (TLOC) routes.
  Control policies are used for applications such as preferring one site over another for a specific destination (or default routing) and limiting which sites can build tunnels directly across the fabric. Inbound control policy affects the OMP route information coming from vEdge routers before it is stored in the vSmart controllers' database. And an outbound one affects the OMP route advertisements from the controllers toward the WAN edge devices [31][32].

- **Centralized Data Policy:**
  While control policies are used to manipulate the control plane, centralized data policies directly affect the forwarding of traffic in the data plane.
  Centralized data policies are a flexible and powerful form of policy-based routing and are commonly used to accomplish Direct Internet Access for specific applications, network service insertion, and data plane manipulations such as packet duplication and Forward Error Correction (FEC) [31][33].

- **Centralized Control vs. Data Policies:**
  - Control policies act on the OMP routing advertisements to/from the vSmart controller while data policies act on application traffic that goes through WAN edge routers.
  - Control policies are executed on vSmart, and only the results are advertised to vEdges in the form of OMP updates. On the other hand, data policies are sent to WAN edge routers and executed locally in memory [33].

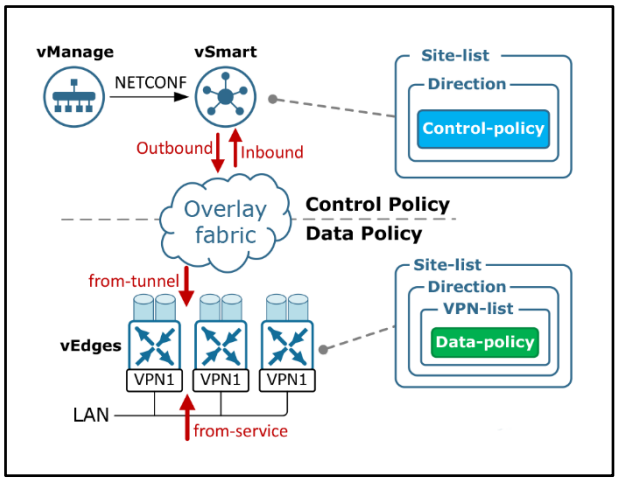

Figure 14: Control and Data policies [33]

5.2. Localised Policies

Similar to centralized policies, localized policies can be used to manipulate both the control plane and the data plane. There are two main types of localized policy: traditional localized policy and security policy. Traditional localized policies include route policy, quality of service, and access control lists (ACLs). The security policy feature set supports use cases such as compliance, guest access, Direct Cloud Access (DCA), and Direct Internet Access (DIA).

Localized policies that affect the control plane, called route policies, can be used to filter or manipulate routes exchanged or learned outside of the SD-WAN fabric via protocols such as BGP, OSPF, and EIGRP. Route policies can also be used to filter routes as they are redistributed from one protocol to another—including into and out of OMP. Route policies are the only way to impact the control plane with localized policy [31].

Localized policies that affect the data plane include the following:

- Quality of Service: Quality of Service (QoS) can be configured on the WAN Edge routers to perform queueing, shaping, policing, congestion avoidance, and congestion management.
- Access Control Lists (ACL): can be created with the localized policy to filter traffic at the interface level. ACLs can also be used to mark or remark traffic for QoS purposes.
- Security Policy: Security policies were first introduced in version 18.2 with the Zone-Based Firewall (ZBFW) feature set and have continued to expand in functionality in subsequent releases. As of version 19.2, the Security Policy feature set currently supports Application-Aware ZBFW, Intrusion Prevention, URL Filtering, Advanced Malware Protection (AMP), and DNS Security. These features are used to affect traffic in the data plane.

6. Cisco SD-WAN Security

Cisco SD-WAN architecture provides strong security for control plane, data plane, and management plane operations. To enable the SD-WAN branches to have Direct Internet Access (DIA) without dependency on another device or solution for security, strong threat defence mechanisms are built into the WAN Edge router. This ensures the protection of user traffic at branch networks from internet threats, and it also improves the application performance, allowing traffic to securely use DIA when that is the optimal path [31].

The following are some of the threat defence features which are available on the WAN Edge router:

- Application-Aware Enterprise Firewall.
- Intrusion Protection & Detection (IPS/IDS).
- URL filtering.

6.1. Application-Aware Enterprise Firewall

Application-Aware Enterprise Firewall is a proper firewall provides protection of stateful TCP sessions, enables logging, and ensures that a zero-trust domain is implemented between segments in the network.

Cisco SD-WAN takes an integrated approach and has implemented a robust Application-Aware Enterprise Firewall directly into the SD-WAN code. The Cisco SD-WAN firewall provides stateful inspection, zone-based policies, and segment awareness [31].

Zone configuration consists of the following components:

- Source zone is a grouping of VPNs where the data traffic flows originate.
- Destination zone is a grouping of VPNs where the data traffic flows terminate.
- Firewall policy is a localized security policy that defines the conditions that the originating data traffic flow must match to allow the flow to continue to the destination zone.
- Zone pair is a container that associates a source zone with a destination zone and that applies a firewall policy to the traffic that flows between the two zones.

Through the help of Cisco vManage, implementing a firewall policy at the branch is relatively straightforward. No matter how the firewall policy is configured, it must eventually be tied to an overall security policy, which is then attached to the branch WAN Edge router template.

6.2. Intrusion Detection and Prevention Systems (IDS/IPS)

Intrusion detection and prevention (IDS/IPS) is another important key to branch security and a component of the Cisco SD-WAN security suite. An IDS/IPS can inspect traffic in real time in order to detect and prevent cyberattacks by comparing the application behaviour against a known database of threat signatures. Once detected, an IDS/IPS can notify the network operator through syslog events and dashboard alerts as well as stop the attack by blocking the threatening traffic flow.

IDS/IPS is enabled through the use of Cisco operating system IOS-XE application service container technology. Cisco SD-WAN IDS/IPS runs Snort, the most widely deployed intrusion prevention engine (IPS) in the world, and leverages dynamic signature updates published by Cisco Talos.

The Cisco Talos Intelligence Group is one of the largest commercial threat intelligence teams in the world and is composed of world-class researchers, analysts, and engineers. These teams create accurate, rapid, and actionable threat intelligence for Cisco customers, products, and services. With Talos, the IDS/IPS system can provide real-time traffic analysis to reliably protect the branch from thousands of threats on a daily basis. Cisco vManage connects to the Talos signature database and downloads the signatures Then pushes them down into the branch vEdge routers without user intervention. Signatures are a set of rules that an IDS and an IPS use to detect typical intrusive activity.

The two methods for signature update include automatic IPS signature update via vManage and manual IPS signature update using CLI commands available on the WAN Edge device. When a new signature package is updated, the Snort engine will restart and traffic may be interrupted or bypass inspection for a short period [31].

6.3. URL Filtering

URL Filtering is another Cisco SD-WAN security function that leverages the Snort engine for inspection of HTTP and HTTPS payloads, in order to provide comprehensive web security at the branch. The URL Filtering engine enforces acceptable use controls to block or allow websites. An

administrator can choose to permit or deny websites based on 82 different categories, the site's web reputation score, and a dynamically updated URL database. Custom black and white lists can also be created with customized end-user notifications, in order to bypass the URL Filtering engine for websites that are internal or trusted [31]. Illustrated in Figure 15.

When an end user requests access to a particular website through their web browser, the URL Filtering engine inspects the web traffic and first queries any custom URL lists:

- If the URL matches an entry in the whitelist, access is granted with no further inspection or processing.
- If the URL matches an entry in the blacklist, access is denied with no further inspection. When access is denied, the user can be redirected to a block page with a customizable message or can also be redirected to a custom URL.

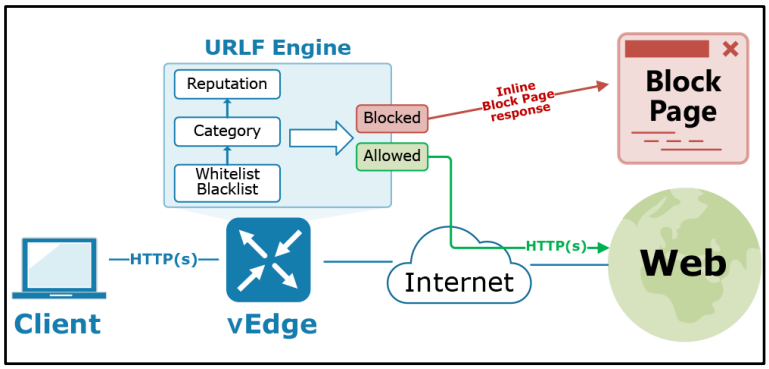

Figure 15: URL Filtering [33]

Conclusion

The Cisco Catalyst SD-WAN solution represents a significant advancement in wide area networking. This chapter has provided an in-depth look at Cisco Catalyst SD-WAN, detailing its architecture, key components, and the crucial role of the Overlay Management Protocol (OMP) in enabling efficient and secure communication across the network.

We have also examined how Cisco leverages policy-based management to optimize traffic flows and enforce quality of service, while integrating robust security features such as Application-aware firewalls, IDS/IPS and URL filtering. Together, these elements form a powerful framework for building agile, scalable, and secure enterprise networks.

With a thorough understanding of Cisco Catalyst SD-WAN's theoretical framework and architectural advantages established, we now transition to the practical validation of these concepts. Chapter 3 presents the hands-on implementation and testing of the solution in a simulated enterprise environment, demonstrating the real-world applicability of the technologies and methodologies discussed in the previous chapters.

Chapter Three:
Cisco Catalyst SD-WAN implementation

Contents:

Introduction

In this chapter, we present the practical implementation of Cisco Catalyst SD-WAN within a virtualized lab environment using GNS3. This phase of our project aims to simulate and validate the deployment of a Software-Defined Wide Area Network for a typical enterprise with geographically distributed branch sites. The objective is to design, configure, and test a scalable SD-WAN architecture that enhances network performance, centralizes management, and integrates advanced security features.

This chapter serves as a comprehensive account of the end-to-end implementation, from topology design to testing and securing the SD-WAN deployment. The results underscore the operational viability of Cisco Catalyst SD-WAN as a modern solution for enterprise networking.

1. Objectives of the Lab

The objective of this lab is to implement Cisco Catalyst SD-WAN solution using GNS3, simulating a real-world enterprise network environment. Specifically, this lab aims to:

- Design an enterprise SD-WAN Topology: Develop a virtual network topology that integrates Cisco SD-WAN components, including vManage, vBond, vSmart controllers, and WAN Edge devices (vEdgeCloud routers).
- Perform Bootstrap Configuration: Execute the initial configuration for SD-WAN controllers (vManage, vBond, and vSmart), ensuring secure inter-controller communication and proper system initialization.
- Certificate Installation and Authentication: Install and authenticate digital certificates on the SD-WAN controllers and Edge devices to establish trusted and secure communication within the SD-WAN fabric.
- WAN Edge Device Configuration and Activation: Configure WAN Edge devices, perform their bootstrap process, install their certificates, and activate them using the device chassis ID and authorization token to ensure valid integration into the SD-WAN fabric.
- Inter-Site Connectivity Verification: Validate the SD-WAN deployment by ensuring successful routing and end-to-end reachability between different sites through ping tests.
- Security Policy Implementation: Apply an Intrusion Prevention and URL filtering security policies on one of the Edge devices, showcasing the capability of SD-WAN to enforce advanced security controls, monitoring and content filtering at the network edge.

By accomplishing these objectives, this lab demonstrates the practical deployment and validation of Cisco Catalyst SD-WAN technology, from initial design and configuration to security policy enforcement.

2. Lab Hardware and Software Environment

2.1. Physical Hosts Configuration

To implement and test our Cisco Catalyst SD-WAN solution, we deployed a local lab environment consisting of three main components: a physical server to host the GNS3 VM and SD-WAN appliances, a personal computer for accessing the vManage dashboard and remote CLI access, and a 4G LTE modem to interconnect the server and PC via a private network. Below in Table 3 are the detailed specifications of each device used in the setup:

Device	Specification	
Server	Model	HP ProLiant DL380p Gen8
	Processor	Intel Xeon E5-2609 @ 2.40GHz, 4 Cores / 4 Logical Processors
	Installed RAM	32 GB (4 × 8GB) SAMSUNG PC3L-10600R DDR3-1333
	Network Interface	Broadcom NetXtreme Gigabit Ethernet
	Storage	4 × HP Logical Volume SCSI Disk Devices (4 × 256 GB)
	Operating System	Windows 10 Pro, Version 22H2
	BIOS	HP P70
PC	Processor	Intel Core i5-8250U @ 1.60GHz 1.80GHz
	Installed RAM	12 GB
	Operating System	Windows 10 Pro
Modem	Model	Huawei E5172As-22

Table 3: Detailed specification of Lab devices

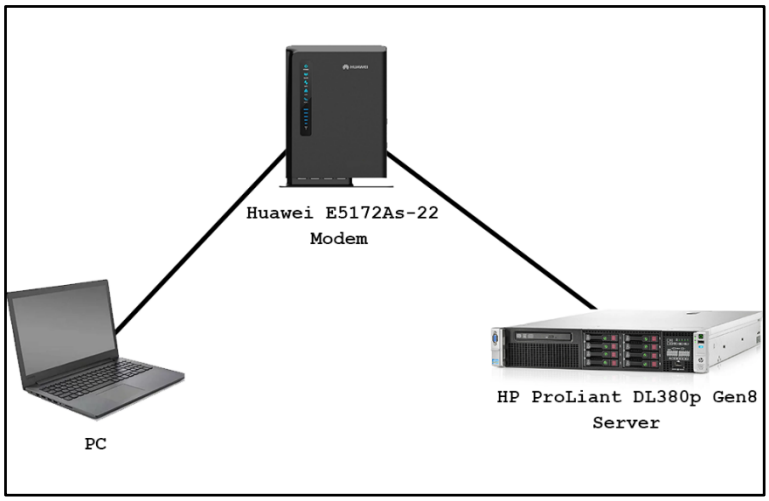

Figure 16 : Physical hosts network topology

2.2. Virtualization Environment

2.2.1. Graphical Network Simulator 3 (GNS3)

GNS3 is a free and open-source network emulator software widely used by network engineers to emulate, configure, test, and troubleshoot both virtual and physical network environments. In this lab environment, we utilized GNS3 version 2.2.54, which comprises two main components, both components were installed on the server:

GNS3 Desktop, serving as the graphical user interface (GUI) and used to design the SD-WAN lab topology and to deploy and configure virtual appliances (vManage, vSmart, vBond, and vEdge…) running within the GNS3 VM.

The GNS3 VM was installed on VMware Workstation Pro 17 with 30 GB of RAM and allocated a single processor with 4 cores, ensuring sufficient computational resources to run multiple Cisco Catalyst SD-WAN controllers and edge devices concurrently. Network connectivity for the GNS3 VM was configured using a bridged network adapter, enabling it to obtain an IP address within the same subnet as the host server via DHCP.

2.2.2. VMware Workstation Pro 17

VMware Workstation Pro 17 is the latest version of VMware's flagship virtual machine software. It allows you to create, configure, and run multiple virtual machines (VMs) on a single physical computer.

In our SD-WAN lab implementation, VMware Workstation Pro 17 was employed as the hypervisor platform to host the GNS3 VM, which is essential for running resource-intensive network functions within the GNS3 environment. The choice of VMware Workstation over other virtualization solutions was motivated by its high stability, integration with GNS3, and robust performance under load.

2.2.3. Cisco Catalyst SD-WAN 19.2.0

In this project, we deployed Cisco Catalyst SD-WAN version 19.2.0, which includes the core software components required to build a secure and scalable SD-WAN fabric. The solution is composed of four primary virtual appliances: vManage 19.2.0, vBond Orchestrator 19.2.0, vSmart Controller 19.2.097, and vEdgeCloud Router 19.2.0. These virtualized network functions (VNFs) were instantiated within the GNS3 VM environment, hosted on a VMware Workstation Pro 17 platform.

Each appliance was allocated system resources based on Cisco's recommended minimum requirements and the constraints of the lab environment:

- vManage: allocated 20 GB of RAM, 1 vCPU, and 30 GB of virtual storage to support the graphical user interface, policy engine, and centralized configuration management functions.
- vBond Orchestrator: allocated 2 GB of RAM and 1 vCPU; it does not require persistent storage for basic functionality.
- vSmart Controller: allocated 4 GB of RAM and 1 vCPU, with no dedicated storage requirements.

- vEdgeCloud: allocated 2 GB of RAM and 1 vCPU, also without storage needs in this configuration.

2.2.4. Support Tools

- Solar-PuTTY: A lightweight and feature-rich SSH client used for remote access and command-line configuration of the SD-WAN components and network devices.
- Wireshark: An advanced network traffic analyser utilized to is used to capture traffic and analyse Packets including IPv4, Datagram Transport Layer Security (DTLS), and Overlay Management Protocol (OMP).

3. Network Topology

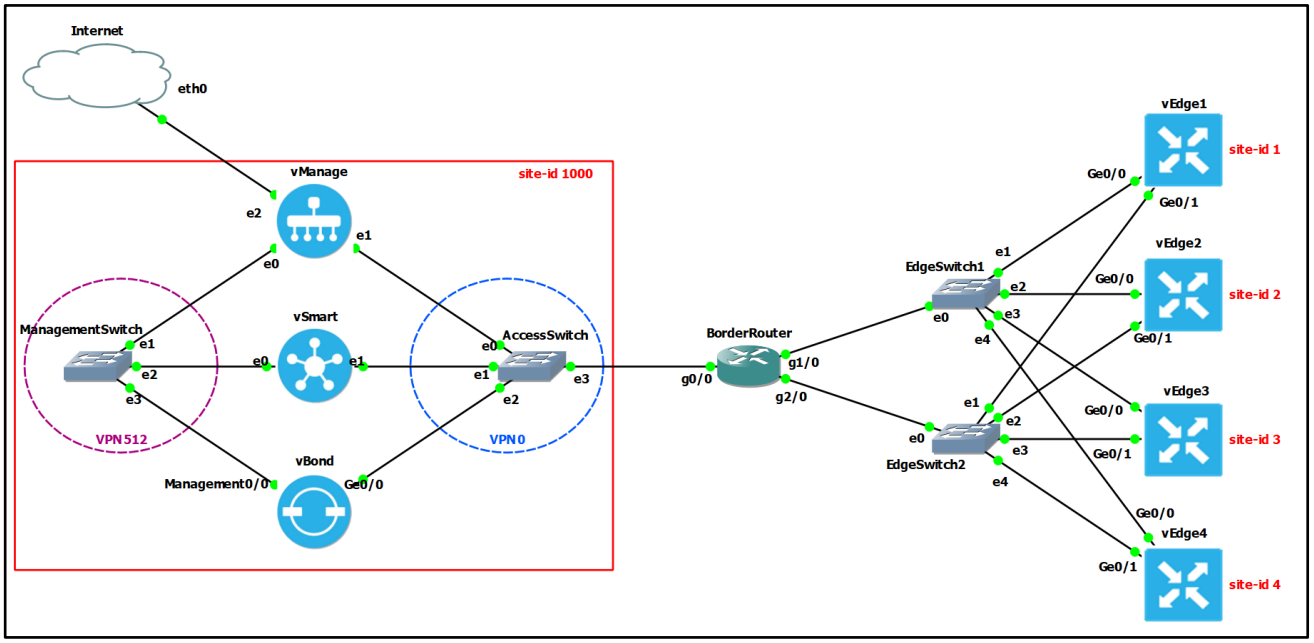

Figure 17: Cisco SD-WAN Lab Topology in GNS3

Figure 17 show Cisco Catalyst SD-WAN Lab topology created in GNS3. The topology is divided into two main segments: the centralized Controller Site (Site ID 1000) and four Branch Sites (Site IDs 1–4).

3.1. Controller Site (site-id 1000)

This site hosts the Cisco Catalyst SD-WAN control plane components and is logically segmented into two virtual networks:

- VPN 512 (Management Plane): Interconnects the controllers and allows out-of-band management through a Management Switch.

- VPN 0 (Transport/Data Plane): Facilitates communication between controllers and edge devices via the Access Switch and Border Router.

vManage interfaces:

- eth0: Connected to VPN 512 via the Management Switch
- eth1: Connected to VPN 0 via the Access Switch
- eth2: Connected directly to the Internet (via physical modem) it acquires an IP address via DHCP. This interface enables access to the vManage GUI from the physical PC.

vSmart interfaces:

- eth0: Connected to VPN 512 (management) via the Management Switch.
- eth1: Connected to VPN 0 (control traffic) via the Access Switch.

vBond interfaces:

- Management0/0: Connected to VPN 512 for initial device registration and management.
- Ge0/0: Connected to VPN 0 to facilitate overlay network orchestration and WAN Edge onboarding.

3.2. Branch Sites (Site IDs 1–4)

Each site contains a vEdgeCloud device configured with a unique site-id and dual interfaces (Ge0/0, Ge0/1) for redundancy and traffic distribution. These devices are connected through two Layer 2 switches (EdgeSwitch1 and EdgeSwitch2) to a Border Router, which links them back to the Controller Site.

- vEdge1: site-id 1
- vEdge2: site-id 2
- vEdge3: site-id 3
- vEdge4: site-id 4

4. Controllers Bootstrap configuration

4.1. vManage:

In this lab environment, vManage is assigned the system IP address 1.1.1.1, which uniquely identifies the vManage within the SD-WAN fabric, and it is situated in Site ID 1000. The lab's organizational name, configured across all components, is designated as “ether-net”.

To enable control-plane connectivity, the vBond Orchestrator’s IP address 10.10.1.3 was configured within vManage. This setup facilitates the establishment of secure control connections between vManage and vBond, essential for authenticating WAN edge devices and orchestrating overlay tunnels.

For operational consistency, clock synchronization across all SD-WAN components is configured by setting the timezone to Africa/Algiers, aligning with the geographic location of the controller site in Algiers.

The vManage interface configuration is as follows:

- eth0 (Management Plane - VPN 512):
  - Connected to the Management Switch, part of the 172.16.1.0/24 subnet.
  - Configured with the static IP address 172.16.1.1/24.
  - Provides out-of-band management access to vManage, vSmart, and vBond components.
- eth1 (Transport/Data Plane - VPN 0):
  - Connected to the Access Switch, part of the 10.10.1.0/24 subnet.
  - Configured with the static IP address 10.10.1.1/24.
  - This interface establishes control connections with SD-WAN edge devices.
  - Configured with a tunnel-interface, enabling the creation of secure IPsec tunnels between controllers and edge routers.
  - Tunnel services is configured to allow essential protocols and services (HTTP, ICMP…) and enabling advanced management protocols such as NETCONF for network configuration automation and SSHD (Secure Shell Daemon) for remote CLI management.
- eth2 (Internet Access):
  - Directly connected to the physical modem for external network access and GUI management via physical PCs.
  - Configured as a DHCP client, automatically obtaining an IP address from the modem's DHCP pool.
  - This interface serves dual purposes: providing internet connectivity and enabling GUI access from external workstations without interfering with the SD-WAN fabric's internal routing.

For efficient routing, a default route was configured pointing towards the Border Router with the gateway IP address 10.10.1.254. This ensures forwarding any traffic destined for the edge devices.

4.2. vBond:

In this lab setup, the system IP for the vBond is configured as 1.1.1.3, and it resides in Site ID 1000. The vBond appliance used here is originally a vEdge router, reconfigured to function as a vBond through the vbond command, where its local interface IP (10.10.1.3) was specified and the local designation was set, transforming it from a vEdge to a vBond.

The timezone for vBond is configured as Africa/Algiers, and the GPS location is set to Algiers.

The vBond interface configurations are as follows:

- Management0/0 (Management Plane - VPN 512):
  - Connected to the Management Switch within the 172.16.1.0/24 management subnet.
  - Configured with the static IP address 172.16.1.3/24.
- Ge0/0 (Transport/Data Plane - VPN 0):
  - Connected to the Access Switch within the 10.10.1.0/24 transport subnet.
  - Configured with the static IP address 10.10.1.3/24.
  - Configured with a tunnel-interface to establish secure IPsec tunnels, ensuring data confidentiality and integrity between control components and edge devices.
  - Support protocols and management services, including HTTP, ICMP. NETCONF is configured for network automation, and SSHD for secure remote CLI access.

- IPsec encapsulation is configured, providing encryption for control-plane communications over the network infrastructures.

Default route was configured pointing towards the Border Router with the gateway IP address 10.10.1.254. This ensures forwarding any traffic destined for the edge devices.

4.3. vSmart:

In this lab implementation, the system IP for the vSmart is configured as 1.1.1.2 and is situated in Site ID 1000. The timezone is configured as Africa/Algiers and the GPS location is set to Algiers.

The vSmart interface configuration comprises two key connections:

- eth0 (Management Plane - VPN 512):
  - This interface is connected to the Management Switch within the 172.16.1.0/24 subnet.
  - Configured with the IP address 172.16.1.2/24.
- eth1 (Transport/Data Plane - VPN 0):
  - This interface connects to the Access Switch within the 10.10.1.0/24 subnet.
  - Configured with the IP address 10.10.1.2/24.
  - The tunnel-interface under VPN 0 is configured to encrypt communication and to ensure data confidentiality and integrity.
  - Services and management protocols are permitted under the tunnel interface, including HTTP, ICMP, NETCONF for network programmability, and SSHD for secure CLI access.

Default route was configured pointing towards the Border Router with the gateway IP address 10.10.1.254. This ensures forwarding any traffic destined for the edge devices.

vManage web GUI

We used a web browser to access the vManage GUI by entering the URL https://192.168.1.5:8443. 192.168.1.5 is the IP address of eth2. The default login credentials used are admin/admin.

After logging in, Organization Name was set to “ether-net”, and the vBond address was assigned the IP address 10.1.1.3 in the **Administration > Settings** page.

Next, vBond orchestrator is added with its IP address 10.10.1.3 and vSmart controller with IP address 10.10.1.2. in **Configuration > Devices > Controllers > Add Controller**.

5. Controller Certificate installation and Authentication

In the Cisco SD-WAN architecture, controllers cannot become operational unless their identity is authenticated through a chain of trust. This identity validation process ensures that only authorized and trusted devices can join the SD-WAN fabric while maintaining operational flexibility. Each controller must have a root certificate signed by a trusted Certification Authority (CA).

5.1. Generating private key and self-signed certificate

Within the vManage vshell (Linux shell) environment, we generated two essential cryptographic files: **SDWAN.key** and **SDWAN.pem**, utilizing the OpenSSL toolkit, which is used for generating cryptographic keys and certificates.

- Generating the Private Key: **SDWAN.key**

```
vManage:~$ openssl genrsa -out SDWAN.key 2048
```

This command generates a 2048-bit RSA private key, saved as SDWAN.key. The RSA key is the foundation of the public-private key pair used for cryptographic operations. This key remains securely stored on vManage and is used to sign certificates and authenticate encrypted sessions within the SD-WAN fabric.

- Creating the Self-Signed Certificate: **SDWAN.pem**

```
vManage:~$ openssl req -x509 -new -nodes -key SDWAN.key -sha256 -days 2000 -subj "/C=DZ/ST=ORAN/L=ENSTTIC/O=ether-net/CN=SD-WAN" -out SDWAN.pem
```

This command generates a self-signed X.509 certificate, saved as SDWAN.pem, which binds the public key to an identity defined by the distinguished name (DN). The certificate is valid for 2000 days and is used to establish trust within the SD-WAN overlay.

  - **req -x509**: Generates a self-signed X.509 certificate instead of a certificate signing request (CSR).
  - -**new -nodes**: Creates a new certificate without password protection on the private key.
  - -**key SDWAN.key**: Uses the previously generated RSA private key to sign the certificate.
  - -**sha256**: Utilizes the SHA-256 hashing algorithm for enhanced cryptographic security.
  - **-days 2000**: Sets the certificate validity period to 2000 days (~5.5 years), ensuring long-term operational continuity.
  - **-subj "/C=DZ/ST=ORAN/L=ENSTTIC/O=ether-net/CN=SD-WAN"**: Defines the subject DN, which contains attributes: country (C), state (ST), locality (L), organization (O), and common name (CN). These attributes identify the certificate holder.
  - **-out SDWAN.pem**: Specifies the output filename for the generated certificate.

Purpose of SDWAN.key and SDWAN.pem

- **SDWAN.key**: The private key used to sign certificates, authenticate encrypted sessions, and establish secure control connections within the SD-WAN fabric.
- **SDWAN.pem**: The self-signed certificate containing the public key, used to authenticate vManage to other SD-WAN components and ensure trust in control-plane communications.

Once the SDWAN.key (private key) and SDWAN.pem (self-signed certificate) were generated on vManage, these cryptographic artifacts were securely copied to the vBond and vSmart controllers

Within the vManage GUI, we navigated to: **Administration > Settings,** under the Controller Certificate Authorization section, the default setting is Cisco Automated. We changed the certificate signing mode to Enterprise Root Certificate. This selection configures the SD-WAN system to use a local Certificate Authority (CA) (represented by the SDWAN.pem certificate) for signing and authorizing device certificates. To implement this, we pasted the contents of the SDWAN.pem file into the provided input field for the Enterprise Root Certificate.

To confirm that the root certificate chain was correctly propagated and synchronized across the SD-WAN infrastructure, we accessed the vManage RESTful API:

https://192.168.1.5/dataservice/system/device/sync/rootcertchain

The response is

```
{"syncRootCertChain":"done"}
```

5.2. Certificates installation

- **Generating Certificate Signing Requests (CSRs)**
  Within the vManage GUI, we navigated to: **Configuration > Certificates > Controllers** Here, we initiated the CSR (Certificate Signing Request) generation for each controller (vManage, vBond, vSmart). Upon successful generation, the status for each controller is updated to "CSR Generated", indicating readiness for certificate signing.

- **Preparing CSRs for Signing**
  For each controller, we copy the CSR content from the GUI then we create a .csr file locally on each controller using vim command in vshell and copy the CSR content into it.

- **Signing CSRs with the Enterprise Root CA**
  Using the OpenSSL toolkit in vManage vshell mode, we sign each CSR with the previously generated **SDWAN.pem** and **SDWAN.key**

  ```
  vManage:~$ openssl x509 -req -in vManage.csr -CA SDWAN.pem -CAkey
  SDWAN.key -CAcreateserial -out vManage.crt -days 2000 -sha256
  ```

  This command is executed for each controller's CSR, producing unique signed certificates (vManage, vBond.crt and vSmart.crt).

- **Installing the Signed Certificates**
  With the .crt files ready, we return to the vManage GUI under: **Configuration > Certificates > Controllers > Install Certificate.** For each controller: we copy .crt contents, and paste it into the installation field.

At this stage, all controllers are fully operational, equipped with valid certificates, and have successfully established secure control plane connections with one another, ensuring a stable and authenticated SD-WAN environment.

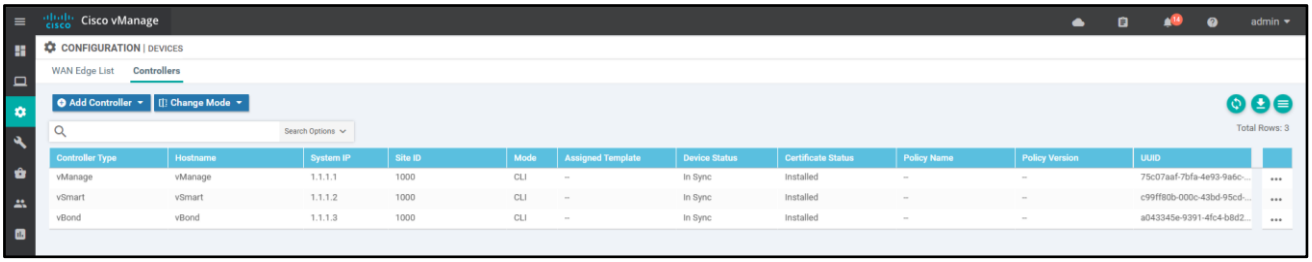

Figure 18: vManage, vSmart and vBond installed

6. vEdge Onboarding and Certification

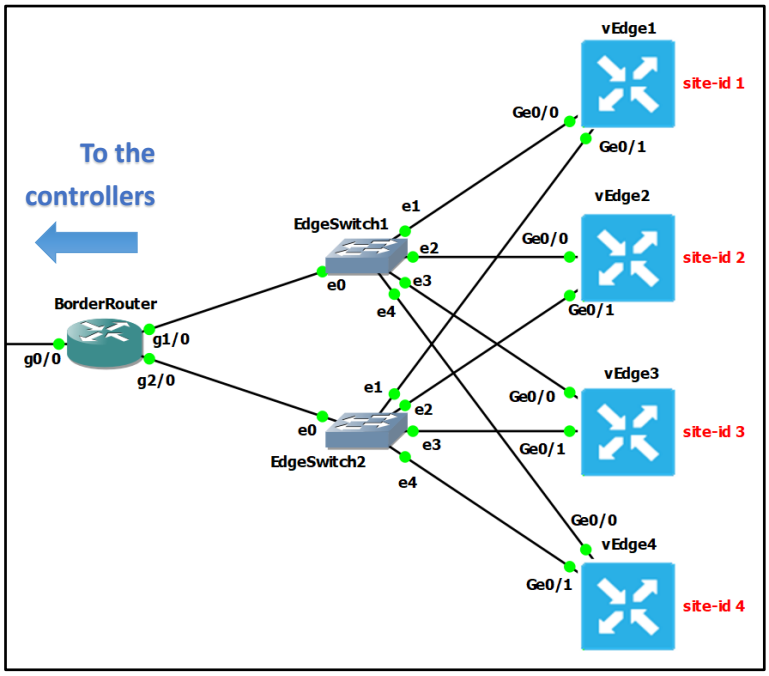

Figure 19: Edge sites topology

The Border Router serves as the primary gateway to external networks and is connected to two EdgeSwitches to provide high availability and redundancy. Specifically, the Border Router is connected via:

- Interface g1/0, which is associated with the 172.19.0.0/16 subnet, linking it to EdgeSwitch1.
- Interface g2/0, which operates in the 172.18.0.0/16 subnet, connecting it to EdgeSwitch2.

These EdgeSwitches function as distribution-layer devices, aggregating the network traffic from the vEdge routers deployed at multiple sites. Each EdgeSwitch provides physical and logical connectivity to all deployed vEdge devices, thereby ensuring resilient and load-balanced paths for the SD-WAN fabric.

Each vEdge router is configured with:

- Interface Ge0/0, which connects to EdgeSwitch1 within the 172.19.0.0/16 subnet.
- Interface Ge0/1, which connects to EdgeSwitch2 in the 172.18.0.0/16 subnet.

The vEdges are identified by their respective site-ids and assigned IP addresses, as detailed in Table 4.

Site ID	vEdge Router	Interface	Address IP
site-id 1	vEdge1	Ge0/0	172.19.0.11 /16
		Ge0/1	172.18.0.11 /16
site-id 2	vEdge2	Ge0/0	172.19.0.22 /16
		Ge0/1	172.18.0.22 /16
site-id 3	vEdge3	Ge0/0	172.19.0.33 /16
		Ge0/1	172.18.0.33 /16
site-id 4	vEdge4	Ge0/0	172.19.0.44 /16
		Ge0/1	172.18.0.44 /16

Table 4 : vEdges sites and IP addresses

6.1. vEdges Bootstrap configuration:

Each vEdge was assigned a unique hostname (vEdge1, vEdge2, vEdge3, vEdge4). Furthermore, each vEdge was configured with a unique system IP address (vEdge1: 2.2.2.1 through vEdge4: 2.2.2.4) to uniquely identify each router within the SD-WAN domain.

Consistent with the control plane components, the organization name was set to "ether-net" on all vEdges. Additionally, the vBond orchestrator IP was specified as 10.10.1.3, enabling each vEdge to establish secure control connections with the orchestrator.

To maintain accurate time synchronization across the network, the clock timezone was set to Africa/Algiers, and GPS coordinates were specified for each vEdge's physical location:

- Site 1: Oran
- Site 2: Constantine
- Site 3: Sétif
- Site 4: Tlemcen

Each vEdge router's transport interface (specifically Ge0/0) was configured as a tunnel interface, enabling secure IPsec tunnels with SD-WAN controllers. Under this tunnel configuration, we permitted all services (including HTTP, ICMP, and others) and explicitly allowed both NETCONF and SSHD.

To enable proper communication with the control plane (vManage, vBond, and vSmart) and external networks, a default route was configured on each vEdge pointing to 172.19.0.1, which represents the IP address of the border router.

6.2. vEdge onboarding and certification

6.2.1. Uploading WAN Edge List:

In order to onboard WAN Edge devices (vEdges) into the Cisco Catalyst SD-WAN environment, we utilized the WAN Edge List feature available in vManage.

The procedure began by navigating to the vManage Dashboard under **Configuration > Devices > WAN Edge List**. Here, we selected Upload WAN Edge List, which allows the uploading of a pre-generated serial file (**serialFile.viptela**). This file, with the ".viptela" extension, contains unique serial numbers and device identifiers of the WAN Edge devices and is obtained from the Cisco Plug and Play (PnP) portal. The PnP portal, linked to a Cisco Smart Account, acts as a centralized platform for managing and pre-authorizing devices before deployment, ensuring compliance with enterprise security policies.

Upon uploading the **serialFile.viptela** to vManage, we selected the "Validate the uploaded WAN Edge List and send it to controllers" option. This validation step is critical to ensuring the integrity and authenticity of the list before it is distributed to all control components (vManage, vBond, vSmart). It also verifies that the uploaded list matches the serial numbers of the physical or virtual vEdges intended for deployment.

Verification of the successfully uploaded and validated WAN Edge List can be performed through:

- Graphical Interface: Navigate to **Configuration > Devices > WAN Edge List** on the vManage dashboard to review the list of valid devices.
- CLI Verification: Execute the following commands:
  - `show control valid-vedges` on vManage and vSmart, which lists all validated and authorized WAN Edge devices.
  - `show orchestrator valid-vedges` on vBond, which confirms the orchestrator's list of validated edge devices.

6.2.2. Installing Edge Certificate:

We employed a structured process involving enterprise root certificate installation and bootstrap configuration.

First, we copied the SDWAN.pem enterprise root certificate (generated and exported from the vManage controller) into each vEdge device. This was done using the vim command in vshell mode on the vEdge appliance. After placing the certificate, we transitioned from vshell mode back to the standard vEdge CLI prompt.

At this stage, it was essential to remove any default root certificate chains installed on the vEdge to prevent conflicts and ensure exclusive use of the enterprise certificate. We accomplished this by issuing the following command:

```
vEdge# request root-cert-chain uninstall
```

This action removed the existing default root certificates, clearing the way for installing the newly prepared enterprise certificate. Subsequently, we executed:

```
vEdge# request root-cert-chain install /home/admin/SDWAN.pem
```

This command installed the enterprise root certificate on the vEdge, ensuring that the device's trust model aligned with the organization's certificate authority.

6.2.3. Edge activation:

Next, we navigated to the vManage Dashboard under **Configuration > Devices > WAN Edge List** and selected an unused vEdge entry from the uploaded list. By clicking Generate Bootstrap Configuration, vManage generated and downloaded a bootstrap configuration file. This file contained vital onboarding information, including:

- Chassis Number (unique device identifier)
- One-Time Password (OTP) token
- Organization Name
- vBond Orchestrator IP Address

Using this information, we activated the vEdge by executing the following command in its CLI:

```
vEdge# request vedge-cloud activate chassis-number [chassis number]
token [otp]
```

This command securely initiated the onboarding process, establishing a control connection with the vBond orchestrator and validating the device's authenticity.

After a short period, the vEdge was successfully onboarded and integrated into the SD-WAN fabric. We verified the onboarding and control connection establishment by executing:

- `show control connections` Displays all active control connections to vSmart, vBond, and vManage, confirming the vEdge's connectivity.
- `show control local-properties` Shows the status of the local certificate, verifying that the enterprise certificate is installed and that the vEdge's identity has been validated by vBond (serial number replaced the OTP token).

Finally, the vEdge devices appeared in the vManage dashboard as active and reachable, signaling successful onboarding and integration into the SD-WAN infrastructure.

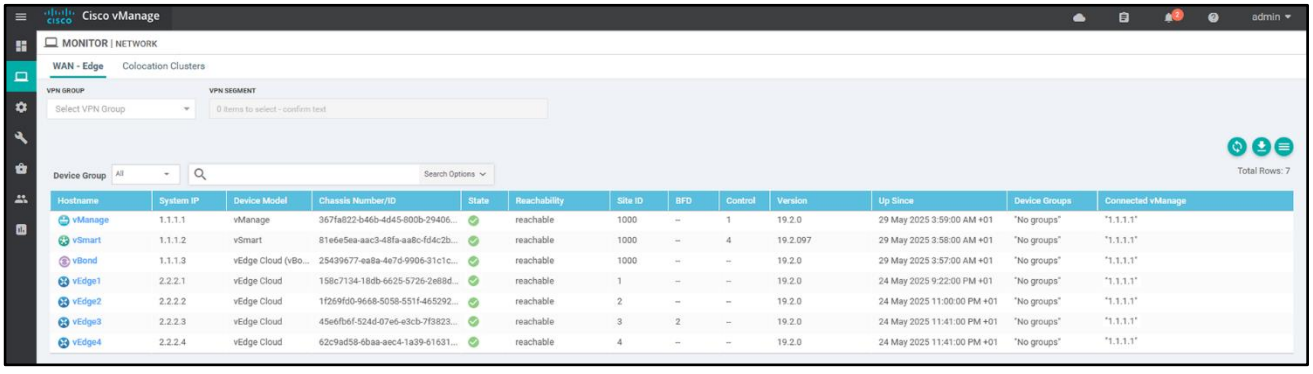

Figure 20: All Controllers and Edge devices are installed

7. vManage Dashboard Exploration

- Main Dashboard

  Upon accessing the Cisco vManage GUI through the vManage eth2 IP address, this interface is accessible via HTTPS. Users authenticate using default administrative credentials (username: admin, password: admin). Upon successful authentication, the vManage Dashboard is displayed. Key elements of the dashboard include:

  - Component Status Overview: show Cisco Catalyst SD-WAN components (vManage, vSmart, vBond and vEdge), including the number of this components.
  - Recent Reboot Metrics: Displays the number of vManage reboots within the last 24 hours and a number of warnings or invalid certificates.
  - Control Status: Visualizes the current control connection health of WAN Edge devices, categorizing them as having full control, partial control, or no control status.
  - Site Health: Summarizes the operational health of SD-WAN sites, indicating the number of sites with full WAN connectivity, partial WAN connectivity, or no WAN connectivity.
  - WAN Edge Inventory: Details the total number of WAN Edge devices imported into the WAN Edge List. It classifies devices based on their deployment status (deployed, staging).

  Additional Widgets: The vManage dashboard offers a modular set of informational widgets, such as Transport Health and Transport interface Distribution.

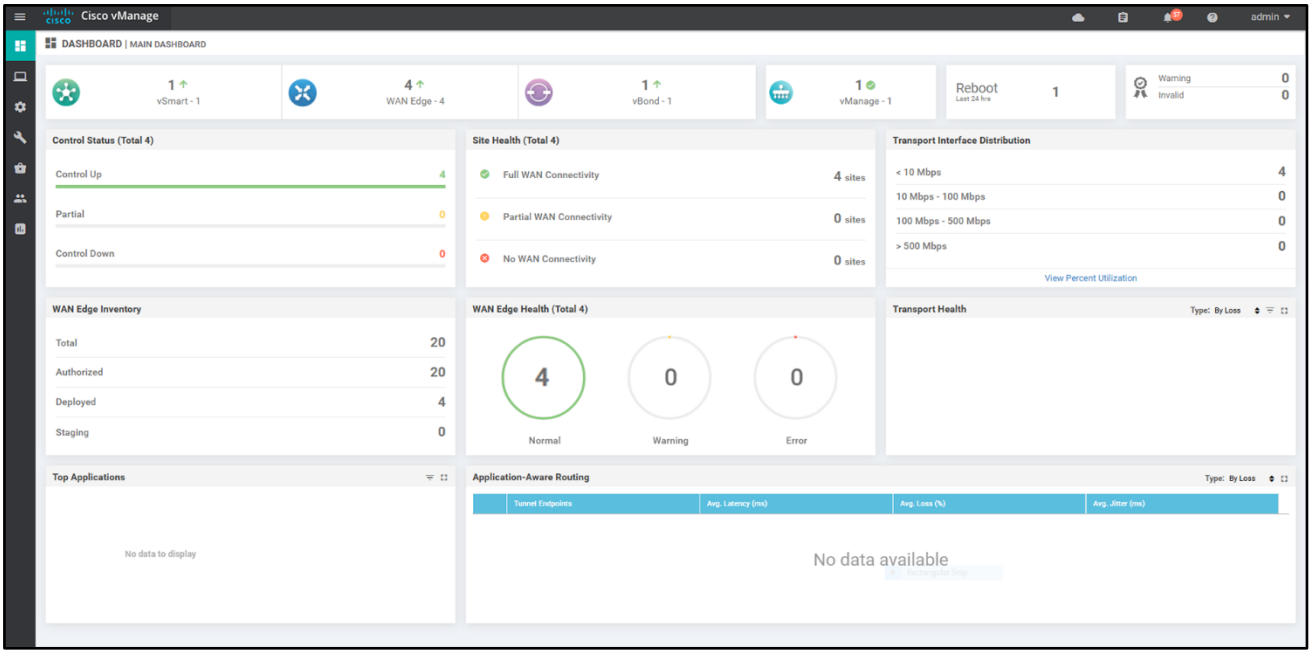

Figure 21: vManage Dashboard

- Geography

  Within the Geography page, the system provides a dynamic and interactive geographic visualization of the SD-WAN fabric's deployed components, including controllers (vManage, vBond, vSmart) and WAN Edge devices. This visualization is implemented using the OpenStreetMap API.

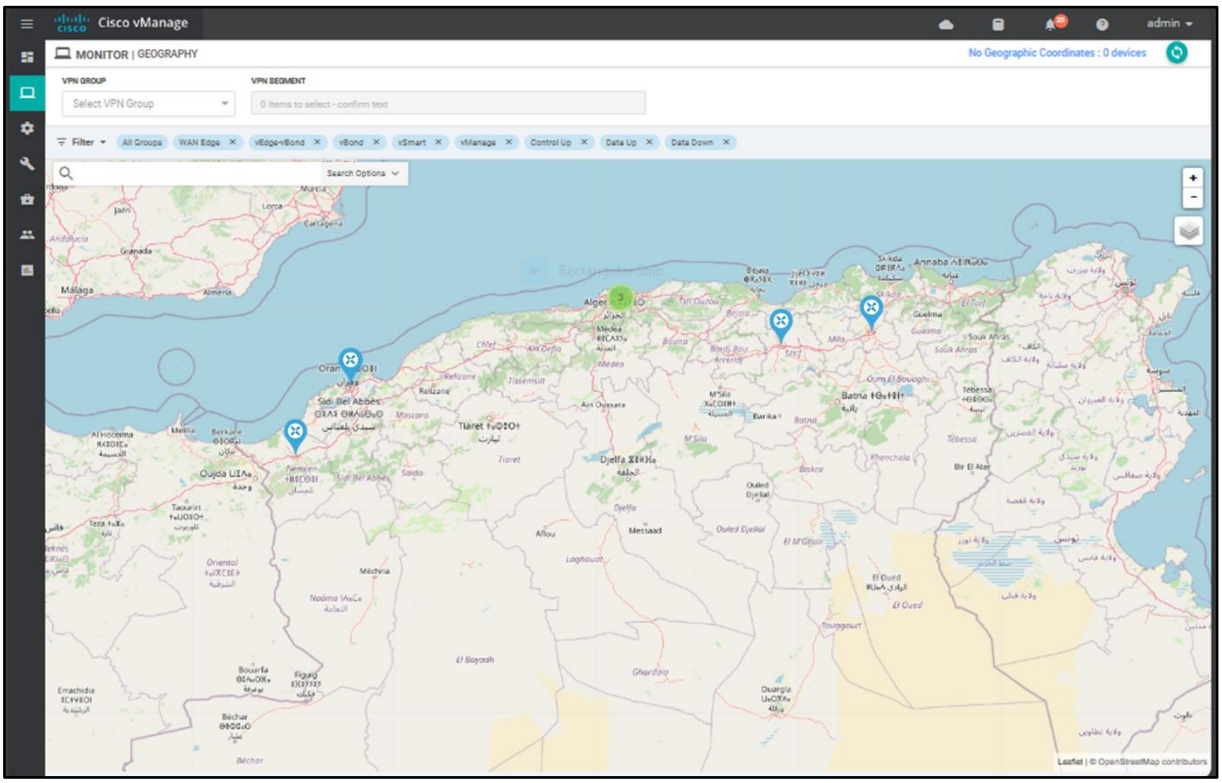

Figure 22: Location of control and Edge sites in vManage GUI

- Network

  The Network page in Cisco vManage provides a centralized view of all SD-WAN components, including controllers and WAN Edge devices. Key details include Chassis ID, Site ID, Software Version, Reachability Status, Up Since, and System IP.

  This page is essential for network inventory management and real-time monitoring. By selecting a device, administrators can access advanced settings such as interface configurations, routing policies, control connections, and software upgrades.

- Alarms

  The Alarms page in Cisco vManage provides a centralized interface for monitoring network alerts. Alarms are categorized by severity into four levels: Critical, Major, Medium, and Minor. This page enables network administrators to rapidly identify and prioritize issues, ensuring the resilience, security, and stability of the SD-WAN infrastructure.

- Events

  The Events page in Cisco vManage provides a comprehensive log of network events, categorized by severity into three levels: Critical, Major, and Minor. These events capture key operational activities, including user logins and logouts, file uploads, root certificate modifications, and control

connection changes. This detailed event logging supports auditing, compliance, and proactive incident management to ensure the integrity and security of the SD-WAN environment.

- Logs
  The Logs page in Cisco vManage provides a system log of vManage activities, including SSH sessions, root certificate modifications, file uploads, and user actions. This log data is essential for system monitoring, troubleshooting, and forensic analysis, ensuring transparency and accountability in the management of the SD-WAN infrastructure.

- SSH Terminal
  In the Tools menu, the SSH Terminal functionality enables secure remote management and control of all SD-WAN components. This interface facilitates direct command-line access to each network element, allowing for advanced configuration, troubleshooting, and monitoring within the software-defined WAN environment.

- Software Update
  The **Maintenance > Software Update** interface provides a centralized platform for performing software upgrades on SD-WAN components, including WAN Edge devices, Controllers, and the vManage network management system. This capability ensures that all elements operate with the latest firmware and software versions, thereby maintaining system stability, security, and feature compatibility across the SD-WAN infrastructure.

- Manage Users
  The **Administration > Manage Users** module enables comprehensive user account management, including the creation, modification, and deletion of user profiles. Additionally, users can be assigned to predefined or custom user groups. By default, three user groups are provided:

    - Basic: Grants view-only access limited to the main dashboard, restricting interaction with system settings.
    - Operator: Provides full read-only access across the SD-WAN environment, allowing monitoring without modification privileges.
    - NetAdmin: Offers full administrative privileges with unrestricted read and write access to all system components and configurations.

  Furthermore, administrators can define custom user groups with tailored permissions, enabling control over feature access and operational capabilities within the SD-WAN management platform.

- Monitor devices
  The **Monitor > Network > Devices** provides comprehensive visibility and control over the operational status and performance of network devices. Key functionalities include:

    - Device Interface Monitoring:
      Displays the operational state of each device's network interfaces, including assigned IP addresses, associated VPNs, and real-time statistics on transmitted and received packet counts.

- Device Control Connections:
  Visualizes the control-plane connections established between each Edge device and the network controllers (vManage, vSmart, and vBond), presenting a detailed topology of the control architecture for each component.

- Device System Status:
  Provides critical system health metrics, such as real-time and historical (up to 7 days) CPU and memory utilization, temperature readings, power supply status, fan performance, and records of system reboots and crash events.

- Device Troubleshooting Tools:
  Supports advanced diagnostic capabilities, including connectivity testing with customizable ping parameters and traceroute analysis. The interface also displays the device bring-up status and enables traffic verification through tunnel health checks, application route visualization, and simulated traffic flows using protocols such as ICMP, HTTPS, and custom application traffic (e.g., LinkedIn).

- Device Real-Time Information:
  Provides a live snapshot of essential device attributes, including hostname, last update timestamp, GPS location, timezone, site identifier, and the associated vBond IP address.

8. Edge sites connectivity:

8.1. Test Reachability of the Edge sites:

After the successful onboarding of all controllers (vManage, vSmart, and vBond) and Edge devices (vEdges), we conducted a reachability test to validate the inter-site connectivity. This was accomplished using the advanced ping tool available in the **Monitor > Network > Troubleshooting > Ping** section of Cisco vManage. Specifically, from vEdge1, an ICMP ping was initiated towards vEdge2 within VPN 0 utilizing the interface ge0/0. The results demonstrated successful reachability, confirming operational connectivity between Site 1 and Site 2.

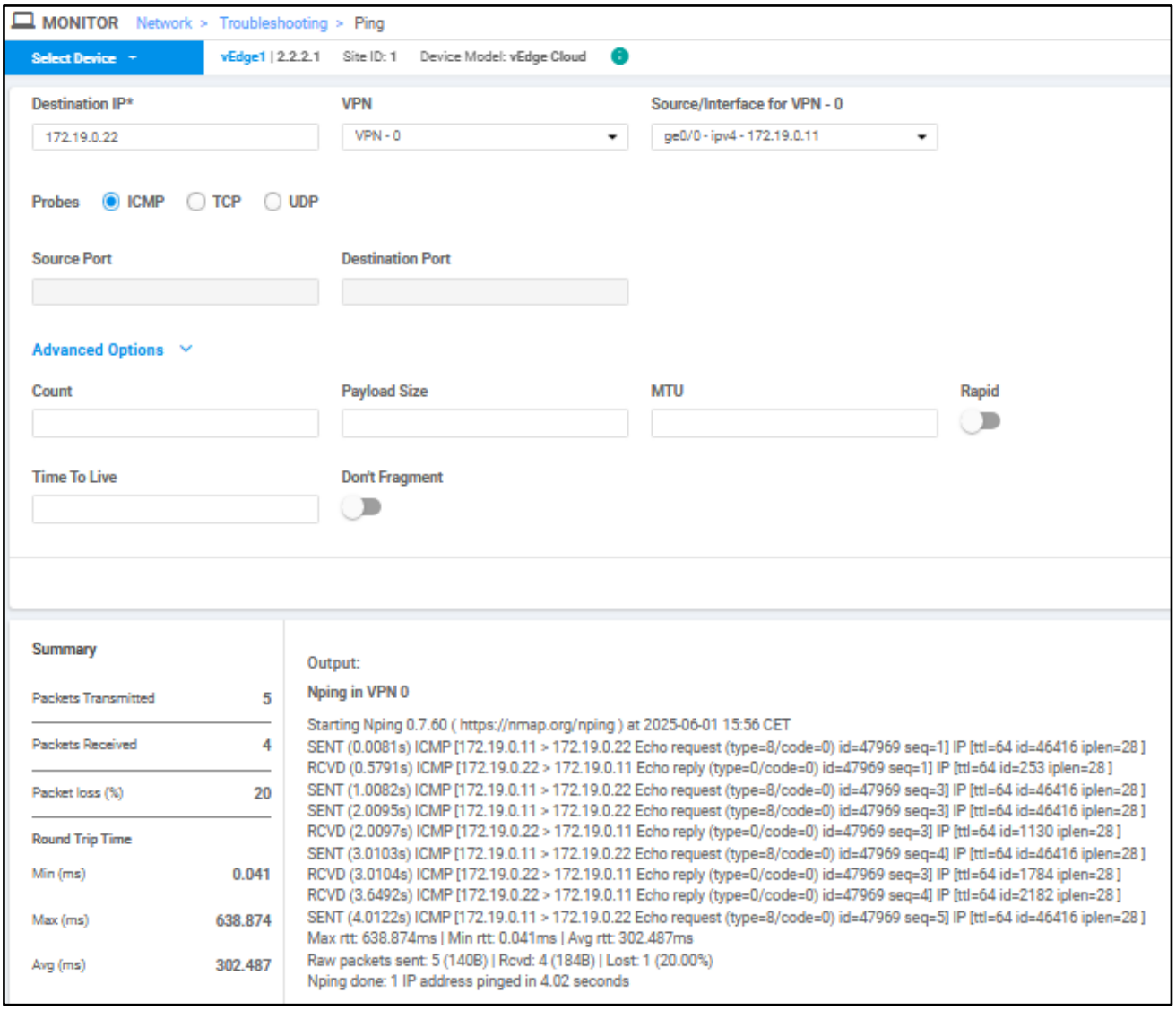

Figure 23: Ping between vEdge1 and vEdge2

8.2. Analysing DTLS packet using Wireshark:

We conducted a Wireshark packet capture on the eth1 interface of the vSmart controller. Upon inspection of the captured traffic, multiple protocols were observed, including standard network management and diagnostic protocols such as ARP (Address Resolution Protocol) and ICMP (Internet Control Message Protocol). However, the most significant protocol identified was DTLSv1.2 (Datagram Transport Layer Security, version 1.2), which is used by OMP to secure control-plane communications over UDP.

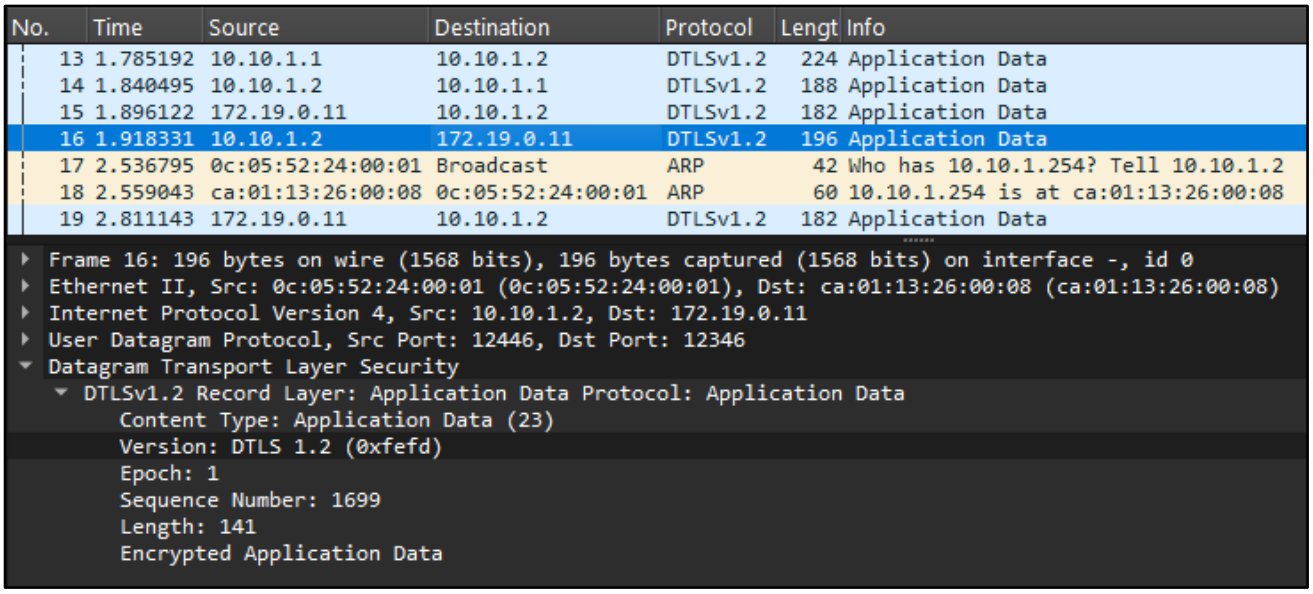

Figure 24: Analysing DTLSv1.2 packet using Wireshark

A notable observation in the capture is as follows:

- Packet No. 16:
  - Protocol: DTLSv1.2
  - Source IP: 10.10.1.2 (vSmart)
  - Destination IP: 172.19.0.11 (vEdge1)
  - Packet Size: 196 bytes
  - Details: The packet encapsulates a DTLS Application Data payload within the IPv4 packet structure. This payload contains encrypted OMP control messages between vSmart and vEdge.
- Packet No. 19:
  - Protocol: DTLSv1.2
  - Source IP: 172.19.0.11 (vEdge1)
  - Destination IP: 10.10.1.2 (vSmart)
  - Packet Size: 182 bytes
  - Details: This packet represents the response from vEdge1 to vSmart, continuing the bidirectional OMP control-plane communication secured via DTLSv1.2.

8.3. Simulating LinkedIn flow in vEdge Router:

The Simulate Flow feature available in the **Monitor > Network > Troubleshooting > Simulate Flow** section of the Cisco vManage GUI was utilized to emulate traffic flows across the SD-WAN fabric. In this simulation, we used a LinkedIn flow originating from a PC located in Site 1, destined for the vManage system within VPN 0. The simulation output provided details such as the specific routing path, the number of next hops, and the intermediate forwarding nodes encountered along the path (from the PC, traversing through the vEdge1 router, and into at the vManage controller). The results verified proper path and route resolution, affirming that the data plane is fully operational and capable of supporting real-time application flows between the edge sites and the centralized management components.

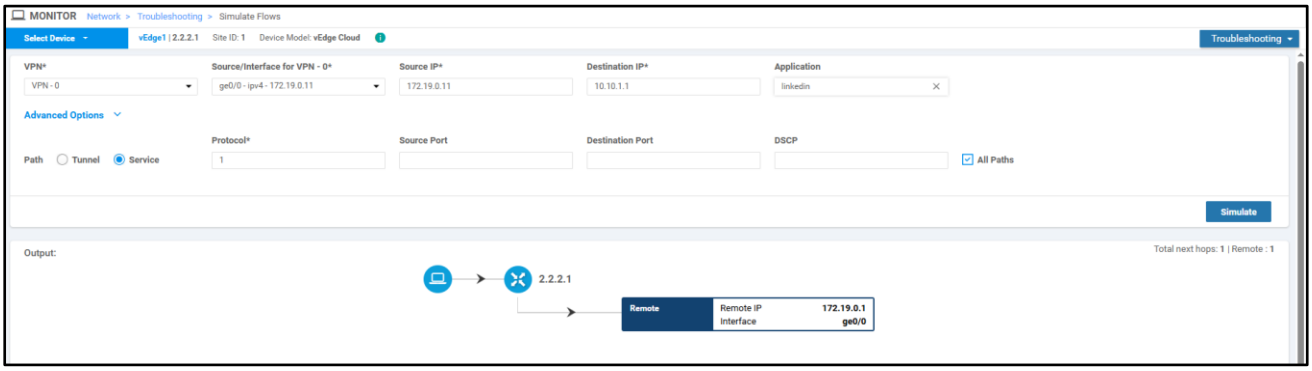

Figure 25: LinkedIn flow simulation in vEdge1

9. Applying Security Policy

In the **Settings > Security** section of vManage GUI, it is possible to define and implement various security policies. The platform provides four pre-configured security policy templates to streamline deployment:

- Compliance: Integrates Application Firewall with Intrusion Prevention System (IPS).
- Guest Access: Combines Application Firewall with URL Filtering for controlled external guest access.
- Direct Cloud Access: Encompasses Application Firewall, IPS, Advanced Malware Protection (AMP), and DNS Security for secure cloud interactions.
- Direct Internet Access: Extends the coverage of Direct Cloud Access by incorporating URL Filtering to further enhance security for direct internet traffic.

For the purpose of this lab implementation, a Custom Security Policy was created to demonstrate granular control over security components.

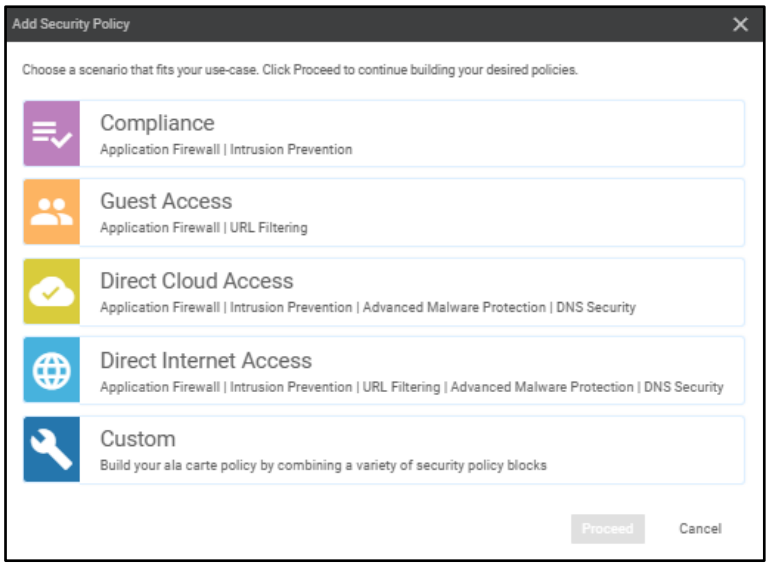

Figure 26: Security policies templates

9.1. Intrusion Prevention Policy Configuration:

We created new Intrusion Prevention Policy in VPN 0 to secure the transport domain responsible for direct internet access.

The signature set was configured to the default profile. Inspection Mode was set to Prevention, ensuring that identified threats are not only detected but actively blocked in real time. The Alert Level Logging parameter was set to Error, prioritizing the logging of significant intrusion events.

The policy was labelled IPS, denoting its role in proactive threat mitigation.

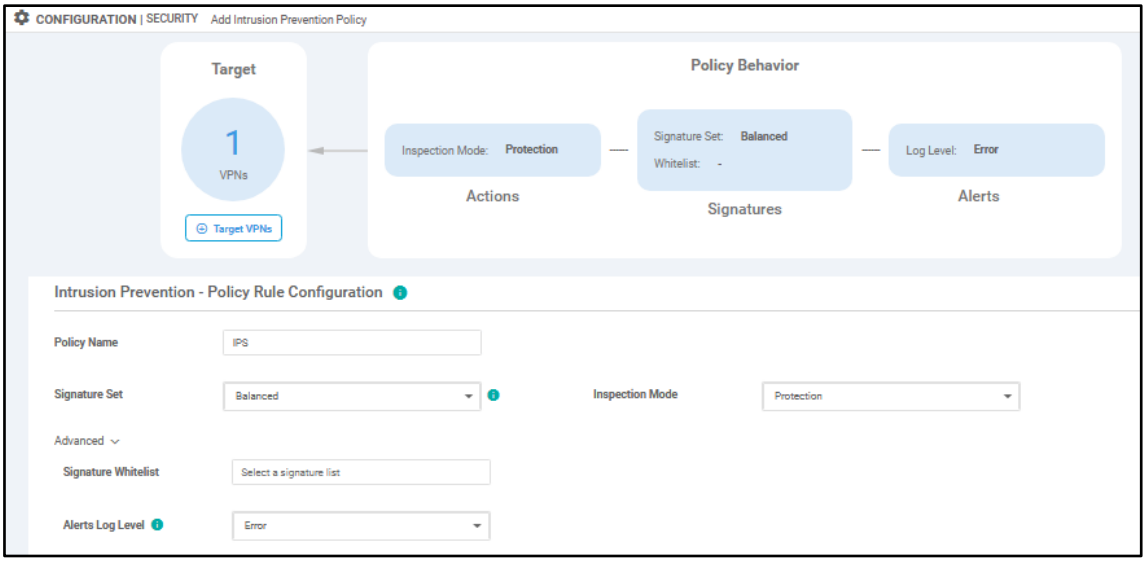

Figure 27: Adding Intrusion Prevention Policy

9.2. URL Filtering Policy Configuration:

A new URL Filtering Policy was created and similarly applied to VPN 0.

We selected some web categories for blocking, namely:

- Confirmed Spam Sources
- Hacking
- Malware Sites
- Botnets
- Keyloggers and Monitoring
- Spam URLs
- Spyware and Adware

Web Reputation Level was configured to Moderate Risk. The Block Page Content was customized to present end users with the message: “This page is blocked by the network administrator”. This policy was designated as URL_Filtering.

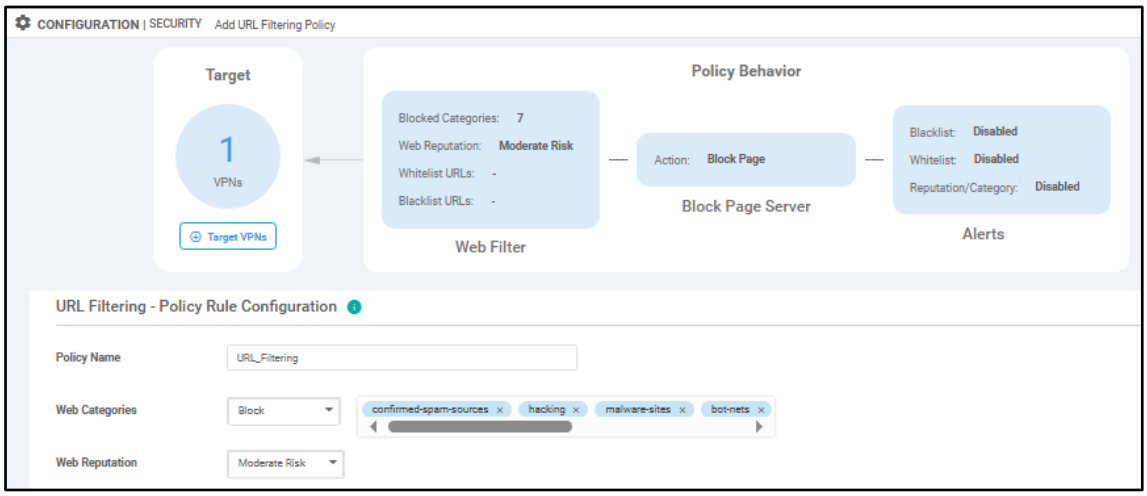

Figure 28: Adding URL Filtering policy

We named the final security policy encapsulating both the IPS and URL_Filtering modules: IPS_and_URL_Filtering

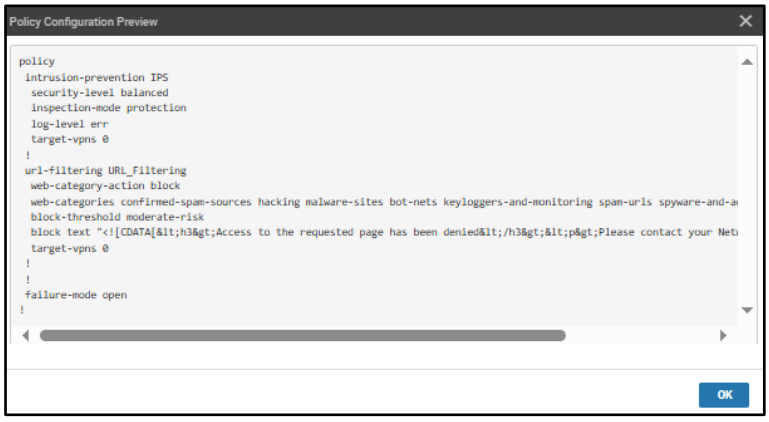

Figure 29: Security policy configuration preview

Conclusion

The implementation of the Cisco Catalyst SD-WAN version 19.2.0 has provided valuable insights into the deployment, operation, and capabilities of a modern Software-Defined WAN architecture. This lab demonstrated the effectiveness of Cisco's centralized SD-WAN control model in simplifying network management across distributed sites while ensuring scalability, flexibility, and security.

The deployment showed the integration of core SD-WAN components and highlighted the platform's advanced capabilities in real-time monitoring, and secure overlay establishment using Overlay Management Protocol (OMP). Moreover, the integration of customizable security policies, such as Intrusion Prevention System (IPS) and URL filtering, showcased the platform's built-in security mechanisms that protect enterprise traffic at the WAN edge without requiring additional infrastructure.

Overall, the Cisco Catalyst SD-WAN solution proves to be a comprehensive and efficient approach for building intelligent, secure, and application-aware enterprise WANs, aligning with modern networking requirements and digital transformation initiatives.

General Conclusion

The rapid digital transformation and increasing reliance on cloud services have pushed traditional WAN architectures to their limits. While MPLS-based solutions have served enterprises reliably for decades, they often fall short in addressing today's needs for scalability, flexibility, security, and cost-efficiency. In response to these limitations, Software-Defined Wide Area Network (SD-WAN) has emerged as a disruptive technology that redefines enterprise connectivity by introducing centralized control, application-aware routing, and seamless integration with diverse transport links.

This project provided a comprehensive study of WAN technologies, tracing the evolution from legacy infrastructures to modern, software-driven approaches. Through an in-depth comparison between MPLS and SD-WAN, we identified key benefits of SD-WAN, such as simplified management, enhanced performance, and improved security through integrated features.

A particular emphasis was placed on the Cisco Catalyst SD-WAN solution, chosen for its compatibility with real-world enterprise needs. In a simulated lab environment, we successfully designed and implemented a complete SD-WAN topology with multiple branch sites and a centralized control plane. The project involved bootstrapping controllers, onboarding edge devices, certificate management, testing inter-site connectivity, analysing control traffic, and applying custom security policies.

This implementation not only validates the operational advantages of SD-WAN but also highlights its feasibility as a scalable and secure alternative to traditional WANs. As enterprises continue to embrace cloud-first strategies and decentralized workforces, SD-WAN stands out as a strategic enabler of agile, resilient, and intelligent network infrastructures. This project thus contributes both academically and practically to the understanding and adoption of SD-WAN technologies in modern enterprise contexts.

Appendix

Bootstrap configuration of vManage

```
vManage# show running-config
system
 host-name             vManage
 gps-location latitude 3.153752
 gps-location longitude 36.724293
 system-ip             1.1.1.1
 site-id               1000
 admin-tech-on-failure
 sp-organization-name  ether-net
 organization-name     ether-net
 clock timezone Africa/Algiers
 vbond 10.10.1.3
vpn 0
 interface eth1
  ip address 10.10.1.1/24
  tunnel-interface
   allow-service all
   allow-service dhcp
   allow-service dns
   allow-service icmp
   allow-service sshd
   allow-service netconf
   no allow-service ntp
   no allow-service stun
   allow-service https
  !
  no shutdown
 !
 interface eth2
  ip dhcp-client
  no shutdown
 !
 ip route 0.0.0.0/0 10.10.1.254
!
vpn 512
 interface eth0
  ip address 172.16.1.1/24
  no shutdown
 !
!
```

Figure 30: Bootstrap configuration of vManage

Bootstrap configuration of vBond

```
vBond# show running-config
system
 host-name               vBond
 gps-location latitude 3.153752
 gps-location longitude 36.724293
 system-ip               1.1.1.3
 site-id                 1000
 admin-tech-on-failure
 no route-consistency-check
 organization-name       ether-net
 clock timezone Africa/Algiers
 vbond 10.10.1.3 local
vpn 0
 interface ge0/0
  ip address 10.10.1.3/24
  ipv6 dhcp-client
  tunnel-interface
   encapsulation ipsec
   allow-service all
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   allow-service sshd
   allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
  !
  no shutdown
 !
 ip route 0.0.0.0/0 10.10.1.254
!
vpn 512
 interface eth0
  ip address 172.16.1.3/24
  no shutdown
 !
!
```

Figure 31: Bootstrap configuration of vBond

Bootstrap configuration of vSmart

```
vSmart# show running-config
system
 host-name             vSmart
 gps-location latitude 3.153752
 gps-location longitude 36.724293
 system-ip             1.1.1.2
 site-id               1000
 admin-tech-on-failure
 organization-name     ether-net
 clock timezone Africa/Algiers
 vbond 10.10.1.3
vpn 0
 interface eth1
  ip address 10.10.1.2/24
  tunnel-interface
   allow-service all
   allow-service dhcp
   allow-service dns
   allow-service icmp
   allow-service sshd
   allow-service netconf
   no allow-service ntp
   no allow-service stun
  !
  no shutdown
 !
 ip route 0.0.0.0/0 10.10.1.254
!
vpn 512
 interface eth0
  ip address 172.16.1.2/24
  no shutdown
 !
!
```

Figure 32: Bootstrap configuration of vSmart

Configuration of BorderRouter

```
interface GigabitEthernet0/0
 ip address 10.10.1.254 255.255.255.0
 media-type gbic
 speed 1000
 duplex full
 negotiation auto
!
interface GigabitEthernet1/0
 ip address 172.19.0.1 255.255.0.0
 negotiation auto
!
interface GigabitEthernet2/0
 ip address 172.18.0.1 255.255.0.0
 negotiation auto
```

Figure 33: BorderRouter configuration

Bootstrap configuration of vEdge1

```
vEdge1# show running-config
system
 host-name               vEdge1
 gps-location latitude 35.696966
 gps-location longitude -0.615798
 system-ip               2.2.2.1
 site-id                 1
 admin-tech-on-failure
 no route-consistency-check
 organization-name       ether-net
 clock timezone Africa/Algiers
 vbond 10.10.1.3
vpn 0
 interface ge0/0
  ip address 172.19.0.11/16
  ipv6 dhcp-client
  tunnel-interface
   encapsulation ipsec
   allow-service all
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   allow-service sshd
   allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
  !
  no shutdown
 !
 interface ge0/1
  ip address 172.18.0.11/16
  no shutdown
 !
 ip route 0.0.0.0/0 172.19.0.1
!
```

Figure 34: Bootstrap configuration of vEdge1

Bootstrap configuration of vEdge2

```
vEdge2# show running-config
system
 host-name               vEdge2
 gps-location latitude 36.362752
 gps-location longitude 6.606578
 system-ip               2.2.2.2
 site-id                 2
 admin-tech-on-failure
 no route-consistency-check
 organization-name       ether-net
 clock timezone Africa/Algiers
 vbond 10.10.1.3
vpn 0
 interface ge0/0
  ip address 172.19.0.22/16
  ipv6 dhcp-client
  tunnel-interface
   encapsulation ipsec
   allow-service all
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   allow-service sshd
   allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
  !
  no shutdown
 !
 interface ge0/1
  ip address 172.18.0.22/16
  no shutdown
 !
 ip route 0.0.0.0/0 172.19.0.1
!
```

Figure 35: Bootstrap configuration of vEdge2

Bootstrap configuration of vEdge3

```
vEdge3# show running-config
system
 host-name               vEdge3
 gps-location latitude 36.179521
 gps-location longitude 5.40633
 system-ip               2.2.2.3
 site-id                 3
 admin-tech-on-failure
 no route-consistency-check
 organization-name       ether-net
 clock timezone Africa/Algiers
 vbond 10.10.1.3
vpn 0
 interface ge0/0
  ip address 172.19.0.33/16
  ipv6 dhcp-client
  tunnel-interface
   encapsulation ipsec
   allow-service all
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   allow-service sshd
   allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
  !
  no shutdown
 !
 interface ge0/1
  ip address 172.18.0.33/16
  no shutdown
 !
 ip route 0.0.0.0/0 172.19.0.1
```

Figure 36: Bootstrap configuration of vEdge3

Bootstrap configuration of vEdge4

```
vEdge4# show running-config
system
 host-name               vEdge4
 gps-location latitude 34.881994
 gps-location longitude -1.321166
 system-ip               2.2.2.4
 site-id                 4
 admin-tech-on-failure
 no route-consistency-check
 organization-name       ether-net
 clock timezone Africa/Algiers
 vbond 10.10.1.3
vpn 0
 interface ge0/0
  ip address 172.19.0.44/16
  ipv6 dhcp-client
  tunnel-interface
   encapsulation ipsec
   allow-service all
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   allow-service sshd
   allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
  !
  no shutdown
 !
 interface ge0/1
  ip address 172.18.0.44/16
  no shutdown
 !
 ip route 0.0.0.0/0 172.19.0.1
```

Figure 37: Bootstrap configuration of vEdge 4

Private key and self-signed certificate (SDWAN.key and SDWAN.pem)

```
vManage:~$ cat SDWAN.key
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA1Azf3sFb1naRb65xnmtdF+uveY0xAgIb61FoNFaQPtdQM+w4
c+0TV7Pjb5BaIiFCyKv6NqfcgQMWb7OGWXZZjbIYfOTAdcNp5hui7IFIN6hYa9tR
1H8H95ZiVc409qVCoXENd7ZPhB+eHGR+Sr8/Biolk9k9ffdFbCdwSXp0B/jhTGkh
7DhoW7wJOT/7Svob4ALNj9ExpLluwuFaRQesaeEV9JdLTVu4WfFOqMW0x1kv/rDP
9LNyY3Vz5gCQ5LPR7xAQT7+wdcjw6WctNXvbRjYwLF5HqPFjkDFuCF4SIAPDX4LD
VqMy4tYZjSBz7avYMEEDj53+qBypopsu+8P8DwIDAQABAoIBAEXKnvwv48woZiG9
5oNfjtpKpgx5ngGtNAc1Wfiv7PXh4/HS85mkE9Ovz1Fuz1ugWty1TbsjcH29yGqn
Sba0LzFlxo2EtJuN35Lu0abJvj0jWUbWfo5T6QliI6deISx0pAOCtA4MoQs5ZM6v
fKmZXGLpCEkrHQQSmHTKXjiw5vOgKxRuAurGpgI/Cb1yRGb20JV1TfTDRP2r1vQ6
RhY6EpNe98i3QzPoDljVe4vIrZOhJVwW4E+WIVwLfsnruYhluto0UlQx3M7C+J0o
ppxfg5GWWc/xXBD+sEqhDz1AwQoEy17Vp+gsW7aLV2ObmjkBAkso7nGrzXsvkMRF
JU/ApYECgYEA5bnaj4SutVvtlteZtW4ZAoCPJYBklG99F4ekZYzZmVJ3YQpsTG0y
Vib9xq4S5ig0nfRiIZEZlYyHxjSZLbVpGzYZ4vLOE2IGVlaG7r+yfMm9OywMreSz
X+YZZPdwmG2S8b9IoWHp0Vy8SQGlijunM7fJq6PZSdi4L9ViI3oPP68CgYEA7E1+
dmLFn//RV8RSoG1lvrgiIMKrSCX2kj1uWSSzv/74NT0ppMHh6NKnVPpW+j76Hhh/
W46C/jYUHzt/aloM432bJAdGoF6Cc3RDrfyP2xc2ek2LQcVBA3uN0X6vo0xZ65MQ
layb5r8/CNZDOokItbOOU0LtL/fNuYlcWKn2waECgYA1iGHOH/U2ff2XsRY4mTdq
xdqVup21mWVlHk7I+1GZ0QXQr0UdajTYrq1kpxvwVl4skM6FkDKODvl0zr0DUcr0
dF8D6+Dp02X2qKM476MAQWK/bzxlKW5DYrN4O9EZNC+R9iIOsipyh1G5EZEp7UzB
WIq+XKg99Sq2utrruX3kMQKBgQDHkJrg+IHWooH2EYOGoV1wOKn56O4mvIkE8ISl
HG4CFB8jN0hYMLXNnzpadiHGrjEmAaJtfGn8r0dHKURuWSbRaV8AinSHM8oQH3yZ
D9eePHhxydN19FT3z/zxlIBY9T5ryYQUI/Z2ZcWifPHCGcEVU1M71iXigPFpZCxt
ZP1UgQKBgQCciRNBpkuk9c3M44ifEy2NZiM5H399E1YkPwjHbn/0iyWGV8uE2L0x
uPQxjKA/0cJwkUIPK42Ceeq+HAX2JSOG4fTv35nMSJcxAp5uXCEST6HnPOA0F6x7
maX2etfZ3n017FURcrSujegEUgsiNE2EGTAcHRH+1vRWyw2SOjDqHg==
-----END RSA PRIVATE KEY-----
```

Figure 39: Private key SDWAN.key

```
vManage:~$ cat SDWAN.pem
-----BEGIN CERTIFICATE-----
MIIDcTCCAlmgAwIBAgIJAO/jHWl23/JhMA0GCSqGSIb3DQEBCwUAME8xCzAJBgNV
BAYTAlVLMQswCQYDVQQIDAJMRDELMAkGA1UEBwwCTEQxFTATBgNVBAoMDFNELVdB
Ti1ET0FOSDEPMA0GA1UEAwwGU0QtV0FOMB4XDTI1MDUyNDAzNDAyMVoXDTMwMTEx
NDAzNDAyMVowTzELMAkGA1UEBhMCVUsxCzAJBgNVBAgMAkxEMQswCQYDVQQHDAJM
RDEVMBMGA1UECgwMU0QtV0FOLURPQU5IMQ8wDQYDVQQDDAZTRC1XQU4wggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDpF6t+7R22thp48ohHhG8dGHX9r6k2
CoA0rfb8xkoZJWqDMQbcrDDYoh4RRAJFR3iAzpodBxFt54IGiIHMvpqjv2wu1fLu
momVAoztEoGe2dJ1NBBIhNoszk5hTJhIF8hRVHKkFhH5kwfdyB+cUR4b+TJnWj2u
jOF6CjEiejY3Fe5ab+EsCCz+EKLroet7WDynbVS5RRcvv4zYu4u2YdY/sElSrH6h
aMHN474EIHLLRZsGoPAT/KGeJ8hTLPYFGJtXBgFnODGoIzQJkbqiK39H1s34Yd+S
GEbx++sn9BBt5mMV8+EEpEEU91n8J9wlc1B3pKj+VOq183MxVC620AvtAgMBAAGj
UDBOMB0GA1UdDgQWBBStHDEZDbCOvETy1o/84U2LZ/4NwzAfBgNVHSMEGDAWgBSt
HDEZDbCOvETy1o/84U2LZ/4NwzAMBgNVHRMEBTADAQH/MA0GCSqGSIb3DQEBCwUA
A4IBAQAcoztXTFTYrU60UE3M6V3Wq60RZlPQOOvFe9SU7+LjjbrGjr2XXQkux4Qx
rUduCIEgAAa3gOZL4XvTjl/iHtL7b3VInfYTLEPUjtpeTs7Mdb3y7Nyo+PcTmU9u
gd9v4nzOzDndQ4SfMVrbCHYAgOqHYLgFsDP6CCLO5LgVbv8QviPUmhDn5Q+yO9bY
y/ppksuFyJ/LmSyLU2mqYS24w5LzAbOpVuMgUGZe+Bw5JMct5RteoF14R1CcI11o
r5ksQwxOn1DmJbPWEc8Hfyar1qETfNj3En0VmZVfwsSZdAYNUaymJ7sStZ7Wrs+L
q4r1ba8+Q9n+Q4X5eJZu3qksLu1F
-----END CERTIFICATE-----
```

Figure 38: Self-signed certficate SDWAN.pem

vManage Certificate

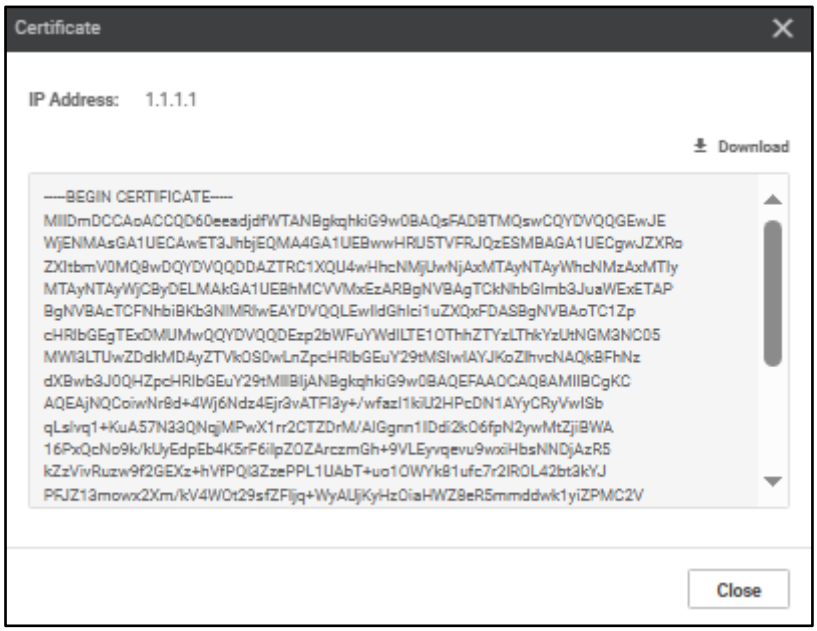

Figure 40: vManage certificate

vBond Certificate

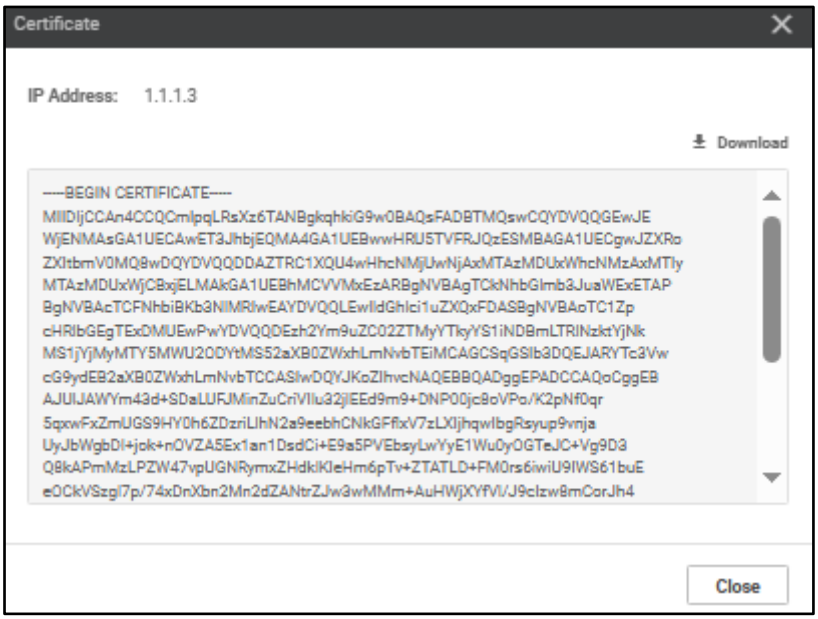

Figure 41: vBond certificate

vSmart Certificate

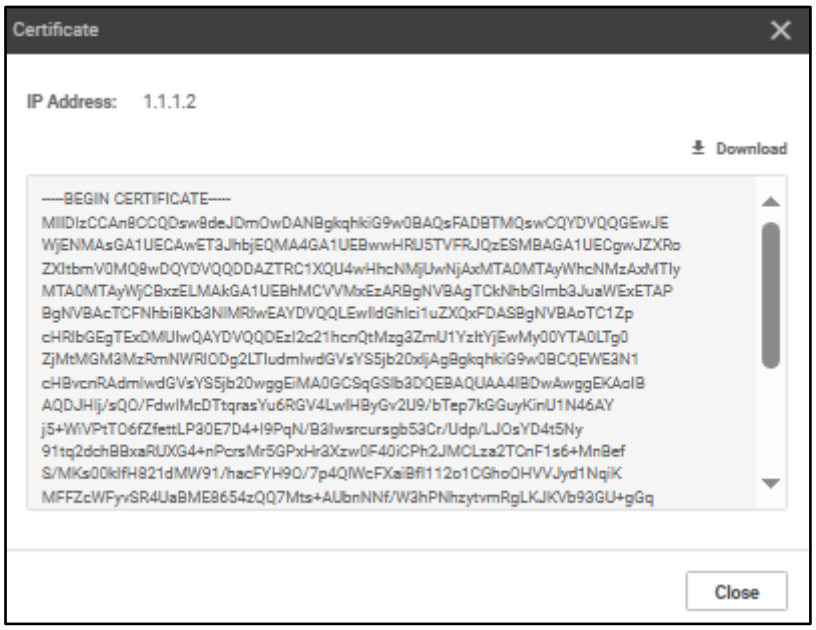

Figure 42: vSmart certificate

WAN Edge List

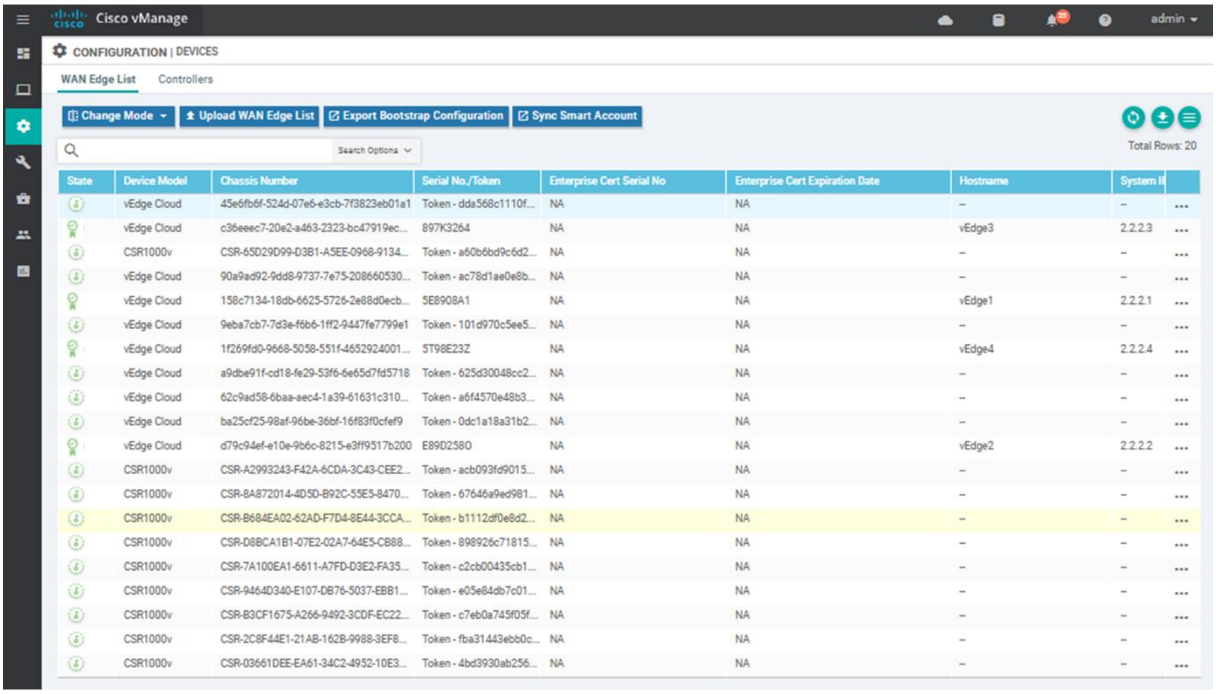

Figure 43: WAN Edge list

vBond Orchestrator Control connections

```
vBond# show orchestrator connections
                                                                                       PEER                      PEER
         PEER     PEER     PEER             SITE        DOMAIN      PEER             PRIVATE  PEER             PUBLIC
         ORGANIZATION
INSTANCE TYPE     PROTOCOL SYSTEM IP        ID          ID          PRIVATE IP       PORT     PUBLIC IP        PORT    REMOTE COLOR     STATE
         NAME                    UPTIME
---------------------------------------------------------------------------------------------------------------------------------------------------
------------------------------------------------
0        vedge    dtls     2.2.2.1          1           1           172.19.0.11      12346    172.19.0.11      12346   default          up
         ether-net               0:00:24:18
0        vedge    dtls     2.2.2.2          2           1           172.19.0.22      12366    172.19.0.22      12366   default          up
         ether-net               0:00:01:41
0        vedge    dtls     2.2.2.3          3           1           172.19.0.33      12366    172.19.0.33      12366   default          up
         ether-net               0:00:00:30
0        vedge    dtls     2.2.2.4          4           1           172.19.0.44      12346    172.19.0.44      12346   default          up
         ether-net               0:00:00:18
0        vsmart   dtls     1.1.1.2          1000        1           10.10.1.2        12346    10.10.1.2        12346   default          up
         ether-net               0:00:24:32
0        vsmart   dtls     1.1.1.2          1000        1           10.10.1.2        12446    10.10.1.2        12446   default          up
         ether-net               0:00:24:31
0        vmanage  dtls     1.1.1.1          1000        0           10.10.1.1        12346    10.10.1.1        12346   default          up
         ether-net               0:00:17:20
0        vmanage  dtls     1.1.1.1          1000        0           10.10.1.1        12446    10.10.1.1        12446   default          up
         ether-net               0:00:17:19
```

Figure 44: vBond orchestrator control connection

Local properties vEdge1

```
vEdge1# show control local-properties
personality                     vedge
sp-organization-name            ether-net
organization-name               ether-net
root-ca-chain-status            Installed

certificate-status              Installed
certificate-validity            Valid
certificate-not-valid-before    May 27 01:42:05 2025 GMT
certificate-not-valid-after     May 25 01:42:05 2035 GMT

dns-name                        10.10.1.3
site-id                         1
domain-id                       1
protocol                        dtls
tls-port                        0
system-ip                       2.2.2.1
chassis-num/unique-id           45E6FB6F-524D-07E6-E3CB-7F3823EB01A1
serial-num                      E976D3D5
token                           Invalid
keygen-interval                 1:00:00:00
retry-interval                  0:00:00:16
no-activity-exp-interval        0:00:00:20
dns-cache-ttl                   0:00:02:00
port-hopped                     FALSE
time-since-last-port-hop        0:00:00:00
pairwise-keying                 Disabled
embargo-check                   success
number-vbond-peers              1
```

Figure 45: vEdge1 local properties

References:

[1] GlobalYo, Exploring the Benefits and Functionality of Wide Area Networks (WAN), https://www.globalyo.com/blog/exploring-the-benefits-and-functionality-of-wide-area-networks-wan/.

[2] Behrouz A. Forouzan, Data Communications and Networking, McGraw-Hill Education, 5th edition, ISBN: 978-0073374226, 2013.

[3] Y. Zhang, N. Ansari, M. Wu, and H. Yu, "On Wide Area Network Optimization", IEEE Communications Surveys and Tutorials, N°4, Vol. 14, pp. 1090–1113, 2012.

[4] Amazon Web Services (AWS), What is a Wide-Area Network (WAN)?, https://aws.amazon.com/what-is/wan/#:~:text=A%20wide%2Darea%20network%20(WAN,area%2C%20or%20even%20the%20world.

[5] Luc De Ghein, MPLS Fundamentals, Cisco Press, ISBN: 978-1587051963, 2004.

[6] NetworkLessons.com, MPLS LDP (Label Distribution Protocol), https://networklessons.com/mpls/mpls-ldp-label-distribution-protocol.

[7] Cato Networks, Pros and Cons of MPLS, https://www.catonetworks.com/blog/pros-and-cons-of-mpls/.

[8] CommandLink, What Are the Challenges of Traditional MPLS Networks in Modern IT Infrastructure?, https://www.commandlink.com/what-are-the-challenges-of-traditional-mpls-networks-in-modern-it-infrastructure/. .

[9] Huawei, MPLS VPN, https://info.support.huawei.com/hedex/api/pages/EDOC1100331435/AEM10132/04/resources/dc/dc_fd_mpls_1009.html.

[10] VMware, Software-Defined Networking (SDN), https://www.vmware.com/topics/software-defined-networking.

[11] Carlos Fernandez and Jose L. Muñoz, Software Defined Networking (SDN) with OpenFlow 1.3, Open vSwitch and Ryu, UPC Telematics Department,

[12] Idris Z. Bholebawa and Upena D. Dalal, "Performance Analysis of SDN/OpenFlow Controllers: POX Versus Floodlight", Wireless Personal Communications, N°1, Vol. 102, pp. 1–15, 2018, DOI: 10.1007/s11277-017-4939-z.

[13] Cheng Sheng, Jie Bai, and Qi Sun, Software-Defined Wide Area Network Architectures and Technologies, CRC Press, ISBN: 978-0367695774, 2021.

[14] Dan Pitt, SD-WAN For Dummies, 2nd VMware Special Edition, John Wiley & Sons, ISBN: 978-1119516084, 2018.

[15] VirtualArmour, What is SD-WAN? A Comprehensive Guide to Software-Defined Networking, https://virtualarmour.com/sd-wan-guide/

[16] GeeksforGeeks, Difference Between Traditional WAN and SD-WAN, https://www.geeksforgeeks.org/difference-between-traditional-wan-and-sd-wan/.

[17] Palo Alto Networks, What Is SD-WAN Architecture?, https://www.paloaltonetworks.com/cyberpedia/sd-wan-architecture.

[18] Fortinet, What is SD-WAN Architecture?, https://www.fortinet.com/resources/cyberglossary/sd-wan-architecture

[19] Portnox, MPLS to SD-WAN Migration: Everything You Need to Know, https://www.portnox.com/blog/network-security/mpls-to-sd-wan-migration-everything-you-need-to-know/.

[20] Terry Slattery, 7 steps of an SD-WAN implementation, TechTarget, https://www.techtarget.com/searchnetworking/tip/7-steps-of-an-SD-WAN-implementation.

[21] William Stallings, Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud, Pearson Education, ISBN: 9780134175393, 2015.

[22] STL Partners, 8 Leading SD-WAN Providers: A Comprehensive Analysis, https://stlpartners.com/articles/network-innovation/sd-wan-providers/.

[23] Fortinet, 2024 Gartner® Magic Quadrant™ for SD-WAN, https://global.fortinet.com/lp-en-ap-2024-gartner-mq-sdwan

[24] Fortinet, Fortinet Secure SD-WAN Reference Architecture, April 3, 2019.

[25] VMware, VeloCloud SD-WAN Edge Platform Specifications.

[26] PyNet Labs, Versa SD-WAN Components and Their Features, https://www.pynetlabs.com/versa-sd-wan-components/.

[27] Hewlett Packard Enterprise, HPE Aruba Networking EdgeConnect SD-WAN.

[28] Cisco, SD-WAN Competitive Comparison, https://www.cisco.com/site/us/en/products/networking/sdwan-routers/sdwan-competitive-comparison.html.

[29] Cisco, Cisco SD-WAN: Application-Aware Routing Deployment Guide, July 2020.

[30] Cisco, Cisco Catalyst SD-WAN Getting Started Guide, https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book.html.

[31] J. Gooley, D. Yanch, D. Schuemann, and J. Curran, Cisco Software-Defined Wide Area Networks: Designing, Deploying and Securing Your Next Generation WAN with Cisco SD-WAN, Cisco Press, ISBN: 978-0-13-653317-7, 2020.

[32] Cisco, Cisco SD-WAN: Cloud Scale Architecture.

[33] NetworkAcademy.io, Cisco SD-WAN Deep-Dive, https://www.networkacademy.io/ccie-enterprise/sdwan.