5-2023

A Study on Security Attributes of Software-Defined Wide Area Network

Siva Naga Lakshmi Keerthi Swamy

A Study on Security Attributes of Software-Defined Wide Area Network

by

Siva Naga Lakshmi Keerthi Swamy

A Starred Paper

Submitted to the Graduate Faculty of

St. Cloud State University

in Partial Fulfillment of the Requirements

for the Degree

Master of Science in

Information Assurance

May 2023

Starred Paper Committee:
Susantha Herath, Chaiperson
Akalanka B. Mailewa
Jieyu Wang

Abstract

For organizations to communicate important data across various branches, a reliable Wide Area Network (WAN) is important. With the increase of several factors such as usage of cloud services, WAN bandwidth demand, cost of leased lines, complexity in building/managing WAN and changing business needs led to need of next generation WAN. Software-defined wide area network (SD- WAN) is an emerging trend in today's networking world as it simplifies management of network and provides seamless integration with the cloud. Compared to Multiprotocol Label Switching (MPLS) majorly used in traditional WAN architecture, SD-WAN incurs less cost, highly secure and offers great performance. This paper will mainly focus to investigate this next-generation WAN's security attributes as security plays a crucial role in SD-WAN implementation. The goal of the paper is to analyze SD-WAN security by applying principles of CIA triad principle. Comparison of SD-WAN products offered by three different vendors in SD-WAN market with respect to its security is another important area that will be covered in this paper.

Table of Contents

Chapter Page

List of Tables

List of Figures

Figure Page

Chapter I: Introduction

Introduction

Wide Area Network is a telecommunication network, interconnecting devices across the globe. Large Organizations use WAN to connect their branch offices, data center and cloud services. This communication is most important part for business continuity. First public WANs were launched in the early 1980s. Different technologies like Asynchronous Transfer Mode (ATM), Frame Relay (FR) and Multi-Protocol Label Switching (MPLS) were used to implement WAN.

Software-defined wide area network (SD- WAN) is most prevalent modern WAN solution in recent years. This next-generation WAN is an intent-based network which resolved the problems faced by clients with traditional WAN. SD-WAN uses Software Defined Network (SDN) principle to decouple control and data plane, virtualizes major part of routing functions, uses software-controllers and open APIs to abstract the infrastructure and manage the connectivity and services. SD-WAN provides cloud-based management which simplifies management, automates the operations of WAN networks. SD-WAN is economical and provides transport independence, consequently improving application performance, more suitable for Software-as-a-service and public cloud applications. As SD-WAN connects to Internet, which is highly insecure, it is crucial to understand SD-WAN’s security equation. This paper will majorly focus on security attributes of SD-WAN with respect to CIA triad. Additionally, this paper will compare security attributes of major three vendors offering SD-WAN solution.

Problem Statement

Security attributes and strength of SD-WAN product is unclear as it is emerging technology.

Nature and Significance of the Problem

WAN is the ingress and egress point of enterprise network. Any unsecured ingress points possibly lead to security breach.SD-WAN systems create network perimeter and make connection to many like internet, extranet, WAN, and branches. This is the reason that enterprise network stakeholders need to pay utmost attention to WAN security.

There are misconceptions about SD-WAN today is that due to its encrypted traffic capabilities it is secure by default at initial deployment. But Built-in SD-WAN security features provide only base for network security. They do not provide comprehensive security solution to an enterprise network, though they are vital for mitigating risk. It is important to understand what baseline SD-WAN solution offers and to which extent SD-WAN makes the network secure. This helps to understand whether SD-WAN is secure at Internet scale. Based on which extra measures can be taken to fill in the gaps and to avoid system being vulnerable to attacks. Hence, this paper will discuss extensively about SD-WAN security attributes to get good picture of its security level in a general sense.

Objective of the Study

The objective of the study is to gain insight into security strength of SD-WAN solution. This study also aims to apply CIA triad principle to these security features

identified. Comparative analysis on three major SD-WAN products in the market is to be followed.

Study Questions/Hypotheses

Below are the study questions of this research based on which data is collected, analyzed, and interpreted:

- What are the security attributes of SD-WAN solution?
- What is the result of applying CIA triad concept to SD-WAN security attribute?
- To draw comparison between the selected SD-WAN products with respect to its security.

Definition of Terms

API – Application Programming Interface is a software interface using which how two applications can communicate with each other.

CIA Triad – It is an information security model in which Confidentiality, Integrity, and Availability together for CIA triad are the core components.

CSRF/XSRF – Cross-Site Request Forgery is a type of cyber-attack where unauthorized actions are executed on a web application.

DDOS – Distributed Denial-of-Service attack is a type of cyber-attack which floods traffic originating from different sources to targeted server, network or service to disrupt legitimate traffic.

DOS – Denial-of-Service attack is type of cyber-attack which brings down machine or network making it not accessible to legitimate users.

IaaS – Infrastructure as a Service is an application of cloud computing in which infrastructure services are rendered to customer via cloud.

ICMP – Internet Control Message Protocol is a network layer protocol that does error-reporting in case of communication problems over Internet.

IPsec – Internet Protocol Security is a network protocol suite to provide secure encrypted connections between two devices connected via Internet.

LAN – LAN is a group of devices which are connected to each other in one physical location.

LTE – Long Term Evolution is a standard for wireless data transmission for data terminals and mobile phones. It is generally used with 4G connection.

MPLS – Multiprotocol Label Switching is a networking protocol in transport layer used for forwarding data packets to destination via their physical MPLS circuits set at predetermined paths.

NMAP – Network Mapper is a network scanner utility/tool which is free and open source.

PCI DSS– Payment Card Industry Data Security Standard is a set of security policies to achieve secure credit card transactions.

SaaS – Software as a Service is also an application of cloud computing that delivers a software and the IT infrastructure and platforms associated with it to the users.

SDN – Software Defined Networking is a technology which has programmatic approach to manage network with the user of software-based controllers.

SD-WAN – Software-defined WAN is an application of Software-defined Networking to managing the WAN.

SSH – Secure Shell Protocol is a network protocol for secure remote login.

TCP – Transmission Control Protocol is a transport layer protocol which ensure reliability of packets transmitted.

VoIP – Voice Over Internet Protocol is a group of technologies which enable to make voice calls using Internet.

VPN – Virtual Private Network is a service that keeps a online connection encrypted and protected. In other words, it makes user stay private while being online.

WAN – Wide Area Network is a large network geographically distributed which interconnects multiple local area networks (LANs).

XSS – Cross-Site Scripting is type of cyber security attack where malicious scripts are injected to legitimate web pages.

Summary

This chapter has given an overview about our research on Security Attributes of SD-WAN. It provides an idea of what is the problem our research is attempting to solve and the importance of the problem. We have covered other important sections in this chapter which includes some study questions and term definitions. These study questions will be answered in the coming chapters.

Chapter II: Background and Review of Literature

Introduction

This chapter starts with a comparison between SD-WAN technology with traditional WAN technology. The advantages of SD-WAN over traditional WAN are mentioned as part of the comparison. Salient features SD-WAN technology will be discussed along with its security features. Different news articles, research papers on security of SD-WAN will be detailed in this chapter. Different researcher's work on evaluation of current SD-WAN products in market will also be mentioned in detail.

Background Related to the Problem

Traditional WANs have software deeply coupled with hardware to control the traffic. So, in almost all cases the software and hardware are available as a combined product offered by any single networking vendor. This kind of architecture was not suitable to the newly adopted cloud-based applications which include SaaS and IaaS, as it could manage this heavy traffic leading to performance issues. Traditional WAN architecture majorly used MPLS technology for networking which made use of dedicated and backup expensive circuits. Additionally, MPLS was originally built for point-to-point connectivity and cannot be used for centralized operations and this rigid in nature makes this technology not easy for scalability.

SD-WAN is a MPLS alternative which provides high performance WAN without using dedicated circuits. SD-WAN provides a virtual service by following a programmatic approach to manage enterprise networks.SD-WAN decouples data plane and control plane which were tightly couples in traditional WAN. Here, Data plane

forwards the traffic and control plane make decisions like where data should be sent.SD-WAN monitors each WAN connections performance and uses this information to manage traffic and achieve high performance. Characteristic features of SD-WAN are:

a. Centralized control - SD-WANs can be provisioned easily as it automates device provisioning. SD-WAN uses centralized controller that provisions and deploys branches in very fast way. This simplifies to manage complex networks.
b. Multi-connection, multi transport – The gateway router in SD-WAN supports hybrid WAN i.e., it supports MPLS, internet, LTE etc.
c. Dynamic path selection – Depending on network conditions, SD-WAN automatically selects WAN Link and directs traffic to it.
d. Policy based management - SD-WAN can inspect traffic (Layer 1 to Layer 7) and use granular routing policies based on customer use case. It also supports quality of service policy. For example: If a company wants best performance for VoIP and web conferences, the company can assign more priority for those kind of traffic packets.
e. Use of APIs: APIs can be used in SD-WAN to customize network and automate any kind of functionality. Ex: A company can setup an API in SD-WAN infrastructure to trouble shoot devices, real-time traffic monitoring etc.

f. Optimized cloud connectivity – SD WANs can be easily connected to several public clouds. They performance of SD-WAN with SaaS application like Salesforce, Microsoft 365

Security strength of any technology plays a vital role. Below are the security features of SD-WAN which makes it very secure:

a. Network segmentation: By segmenting network into small networks limits any attack is limited to manageable area.
b. Encrypted network traffic – SD-WAN have inbuilt 128 and 256-bit AES encryption and IPsec based VPN capabilities.
c. Single pane of glass monitoring - Increase visibility into the WAN is achieved with SD WAN's real-time, simultaneous management of network for threat and risk detection.
d. Automated key rotation: SD-WAN replace traditional manual VPN key rotation with an automated system making rotations frequently with no manual intervention and no downtime.
e. Threat intelligence: Many SD-WAN solutions have artificial intelligence and machine learning based.

Literature Related to the Problem

Various research has been done by researchers, news websites, SD-WAN vendors on security features of SD-WAN. According to Wood (2017) representing velo cloud SD-WAN product of VM Ware, he says it offers wide range of security capabilities as below:

- Segmentation.
- Secure connectivity.
- Security services insertion.
- Secure deployment. MPLS
- Visibility and compliance.

Wood (2017) quotes that “SD-WAN can drive segmentation and do it in a much more secure manner than even MPLS because MPLS doesn’t encrypt any traffic at all, whereas SD-WAN automatically encrypts all traffic”. He also mentions that “default SD-WAN solution will not necessarily be a best-of breed security solution.” Though SD-WAN uses layer 7 firewall as edge device and has application recognition capability to route traffic through different security services as part of its inbuilt security features.

An article released by Vodafone (“The top 5 SD-WAN security benefits for your business,” 2021), mentions various security benefits of SD-WAN. The article appreciates SD-WAN solution as its security is highly scalable as well as centralized as centralized controller can be used to apply security policies for entire network and is easy scalable. Additionally, this article also touches another salient CIA principle which is availability. It says that SD-WAN can be used increase availability by having variety of network connection types into WAN such as internet connection, private circuits, and mobile networks. SD-WAN avoids data loss from intrusions with its connection with cloud. SD-WAN enables to use virtual firewall to handle attacks in real time. This virtual firewall has many advantages as it can be used to restrict access to websites for set of employees or guests also it can be enabled/disabled based on its need. Segmentation

implemented in SD-WAN can be leveraged in multiple ways. Segmentation policies can be managed from a single pane of glass. Automatic adaption during any network sudden changes is also achieved. SD-WAN also can be used to prioritize different traffic by moving the prioritized traffic over MPLS link which have high bandwidth and low latency. For example, this prioritized traffic can be voice or video.

A security survey was done by heavy ready reports on SD-WAN (Hodges, 2019). In its research, it determined usage of various of SD-WAN security features by SD-WAN customers. This research in a way provides the list of wide range of security services of SD-WAN solution. It declared that SD-WAN security capabilities are growing at fast pace. Below are the key findings of this research:

a. Security services is an integral part of SD-WAN deployments.
b. SD-WAN customers are focusing on security offerings of SD-WAN solution to make decision while selecting the vendor.
c. SD-WAN is well versed in managing complicated security routing algorithms.
d. SD-WAN has capability to apply any security policy based on the application.
e. 92% of Communication service providers are planning to integrate SD-WAN security solution into their security as a service portfolio.
f. It deduced that vFirewall (40%), intrusion prevention (35%), distributed denial of service mitigation (34%) and secure SD branch (30%) are considered as most high valued services among the SD-WAN security services.

g. Among the application-focused services offered by SD-WAN application control (26%), web filtering (25%) and packet filtering (25%) were highly used in enterprise networks.

This research well explains different security offerings currently used by various existing customers of SD-WAN.

New research *("*SD-WAN security: A new era of flexibility and individual networks*,"* 2022) brings up another salient security feature of SD-WAN which is ensuring security during initial deployment. The protection mechanism used here is authentication, usually based on certificates meeting the first principle of CIA triad i.e., confidentiality. SD-WAN mainly achieves confidentiality by encryption and a VPN to secure the to and from traffic from public Internet. An optimized security solution should not provide security costing performance and CPU. This is achieved by SD-WAN by reducing the traffic that passes through the security system. This approach also makes security management easier. SD-WAN uses a split tunnel to segment traffic so that big chunk of the traffic is forwarded through firewall to go to Internet. Remaining chunk goes from one website to another website and security operations are not performed on it. SD-WAN device checks what is connects or going to connect using its control component which makes this technology to deny or restrict traffic going to website. Very importantly, SD-WAN providers have integrated their solution with cloud security providers and cloud service importers.

Another research ("The role of SD-WAN in securing the expanding network perimeter," n.d.) mentions about another major advantage of SD-WAN interims of its security offerings which is SD-WAN solution is PCI DSS complaint making SD-WAN highly secure to transmit sensitive credit card data. SD WAN's security characteristic

flexible provisioning and network segmentation can be leveraged to isolate POS systems, critical networks, and data from rest of the network.

Literature Related to the Methodology

The paper prepared by Bustamante and Avila-Pesantez (2021) uses experimental methodology to compare two SD-WAN solutions to perform analysis of their cybersecurity mechanisms to respond to common attacks. Commercial SD-WAN solution FortiGate is contrasted with open-source solution Flexiant in terms of confidentiality, integrity, and availability. Understand their mitigating capabilities against DoS attacks, TCP syn flood, ICMP flood using HPing3 and application layer attack using slowhttptest were performed was the focus in the paper. The simulation parameters form the basis of comparison between these SD-WAN products. This research paper considered different simulation parameters mentioned in Table 1.

Table 1

Simulation Parameters used in Security Evaluation

	FortiGate	**Flexiwan**
CPE	3	3
Redundant Links (MPLS/Broadband)	Yes	Yes
SSH	Yes	Yes
Web Management	Yes	Yes
HTTPS	No	No
Cloud controller	Yes	No
Release	7.0.0	4.1.3
CPE	FortiGate KVM with fortiOS	Ubuntu 18.04 with flexirouter

Different tools were used to understand the security stand. To test their security stand against brute force attack via SSH and web login using Hydra and Burp Suite were performed with 6 characters long. The results of DDOS attacks on these products is mentioned in Table 2.

Table 2

Denial of Service Attacks Results of SD-WAN Products

	FortiGate	*Flexiwan*	
	CPE (Firewall)	CPE	Controller
TCP Port	80	8080	80
TCP SYN Flood	Successful	Successful	Failed
ICMP Flood attack (HPing3) single source	Successful	Successful	Failed
Application layer attacks (slowhttptest)	Successful	Successful	Failed

Vulnerability assessments were done using NMAP And Nessus. Some analysis on IPSEC tunnel parameters to evaluate their cryptography strength such as authentication methods, encryption algorithms and hashing algorithms were done as shown in Table 3. The security tests concluded that commercial solution FortiGate

performed well though open-source solution was strong against XSS, CSRF or the northbound rest API.

Table 3

IPSEC Tunnel Parameters of SD-WAN Products

	Vendor	
	FortiGate	***Flexiwan***
IKE Version	1,2	2
Authentication Methods	Preshared Key, Certificado digital	Preshared Key
Encryption algorithm	DES-MD5, DES -SHA1 DES-SHA256, DES-SHA384, DES- SHA512	AES-CBC-128
Hashing Algorithm	MD5, SHA-256, SHA-512, SHA-384	SHA-256, SHA-128

Azhar (2021) presented a paper on Testing SD-WAN vendors for Service Providers Integration where he compared Cisco Meraki SD-WAN solution and VMware Velocloud SD-WAN solution using experimental methodology. Interestingly, Azhar focused on an important security feature, i.e., authentication and authorization of API requests which will achieved by rate limiting the requests to a defined number for a given time. As SD WAN's API interface of controller and orchestrator is located in Internet, the rate limiting of API calls works against misuse by legitimate user. Considering this security aspect, Cisco SD-WAN product Meraki is given 8 score out of 10 whereas VMware velo cloud is given 4. Velo cloud used token for authentication and

a key value pair for authorization as shown in below Figure 1. Velo cloud used cookie-based authorization besides API key token which is vulnerable to Cross site result forgery (CSRF/XSRF). Logging visibility is another security parameter which is considered while evaluating the score. Cisco Meraki provided useful logging information with respect to security such as last usage of key and one-click option to revoke a key when it is lost or compromised.

Figure 1

Cisco Meraki API Request Response Time Example

Cisco has recently released an article where it compared six SD-WAN solutions of major vendors (SD-WAN vendors comparison chart, 2022). The security parameters used for comparison were as below:

- Custom Silicon
- Segmentation
- Encrypted traffic analysis
- Threat intelligence
- Remote Office Branch Office On prem security services

Table 4 contains their key findings. Comparison of availability of a particular security feature in six SD-WAN products that are most prevalent in the market is done.

Table 4

Security Features Comparison of Different SD-WAN Products

		SD-WAN Vendors					
		Cisco	VMware	Fortinet	Silver Peak	Versa	Palo Alto
Security Features	Remote Office Branch office On prem security services	Yes	Yes (wl)	Yes	No	Yes	Yes(wl)
	Custom Silicon	Yes	Yes (wl)	Yes (wl)	No	No	No
	Segmentation	Yes	Yes (wl)	Yes (wl)	Yes(wl)	Yes	Yes (wl)
	Encrypted traffic analysis	Yes	No	Yes (wl)	No	Yes	No
	Threat intelligence	Yes	No	Yes	No	Yes	No

Note. wl stands for “with some limitations”

Cisco SD-WAN product offers many on-prem security services such as Snort IPS, threat grid sandboxing URL filtering, DNS security (Cisco product), AMP File Analysis, Talos threat intelligence, SSL. These security capabilities are integrated and made available in vmanage. Versa networks and Fortinet networks also provide similar security services. Other vendor either provide basic or no security capabilities. Cisco also offers a trusted platform chip known as custom silicon to protect device against back door and foundational attacks.

The article says this security feature ensures automated, foolproof authentication. This security feature is not provided by any other vendors in SD-WAN

market. Also, Cisco SD-WAN product has a peculiar way of performing encrypted traffic analysis. It does the analysis without decryption by matching encrypted SHA patterns which is a performance efficient process. It is seen that many other products support this. Virtual routing and forwarding based segmentation are supported by most of the vendors. This network segmentations limits the damage during occurrence of cybersecurity attack. It also plays a pivotal role in limiting access privileges to those who require it. Cisco additionally supports multi segment topologies and multi tenancy.

A recent paper (Gordeychik & Kolegov, n.d.) did an excellent evaluation of selected security SD-WAN solutions in the market and provided a summary of security issues identified. On “Silver Peak Unity EdgeConnect”, a SD-WAN product of Aruba networks a Hewlett Packard Enterprise company the evaluation resulted in multiple security issues. Few of the security issues mentioned are WEBUI /REST API leaks software versions, lack of protection against CSRF for REST API, slow HTTP attacks brought WEB UI down, using admin count user can access OS interface via CLI backdoor. The paper mentions that a search engine named Shodan detected Silver peak appliances which were using outdated and unsupported Linux 2.6.38 OS which was released in March 2011 as shown in the below Figure 2. Similarly, the researchers also evaluated “Citrix NetScaler SD-WAN”. The list of security issues on this solution included Unauthorized access to Munin web UI, multiple SQL injections, arbitrary file reading via path traversal, etc.

Figure 2

Linux Kernel Version Leakage for Silver Peak

Another research paper (Gordeychik et al., n.d.) from the writers of the above research paper along with new researcher, performed SD-WAN mass enumeration by implementing passive finger printing with Shodan and Censys search engines. They also could find out product version using active fingerprinting with Nmap and NSE engine. Figure 3 shows leakages of different SD-WAN products along with the source which was attacked.

Figure 3

SD WAN Versions Leakages

Vendor	Source	Leakage	Example
Cisco vEdge Cisco vBond Cisco vManage Cisco vSmart	SSH warning message (/etc/issue)	Product version	viptela 17.2.4
VeloCloud Network Orchestrator	HTML	UI version	<link href="/css/vco-ui.3.0.0.1509625568730.common.css">
Teloip Orchestrator API	JSON	API version	{"host":"_v5.02_Teloip Orchestrator API", …}
Fatpipe SYMPHONY SD-WAN	HTML	Product version	9.1.2r142
Versa Analytics	JavaScript	Indirect version	{ANALYTICS_PATH : "/analytics/v1.0.0/", …}
Versa FlexVNF	JavaScript	Package version	{"package-name": "versa-flexvnf-20161214-191033-494bf5c-16.1R2", …}
Riverbed SteelHead	HTML	Indirect version	<meta name="application-name" content="web3 v0.15.8" />
Citrix NetScaler SD-WAN VPX	HTML	Product version	<link href="/br_ui/rdx/core/css/rdx.css?v=9.3.1.35" rel="stylesheet" type="text/css"/>
Silver Peak Unity Orchestrator	URI	Product version	https://e.com/8.3.6.35923/webclient/php/login.html
Silver Peak Unity EdgeConnect	URI	Product version	https://e.com/8.1.4.11_66255/php/user_login.php

Summary

This chapter explained how SD-WAN emerged and how it solved problems of traditional WAN architecture. A small comparison between MPLS and SD-WAN has been discussed. Further, it talks about prominent security features of SD-WAN solution. The literature review of the problem included several research papers and articles on security attributes of SD-WAN. Later, literature review to the methodology discusses

comparison of SD-WAN product of different vendors with respect to its security features done by various researchers.

Chapter III: Methodology

Introduction

This chapter will give a plan to extensively understand security attributes of SD-WAN solution and how the CIA triad concept will be applied to the security offerings of SD-WAN solution. Also, it will give a plan to understand compare security strength of three SD-WAN products belonging to different vendors.

Questions that are attempted to provide answer in this chapter are mentioned below:

1. What are the security benefits of SD-WAN solution?
2. How does each security attribute of SD-WAN make the solution more secure?
3. Does each security attribute of SD-WAN meet CIA triad principle?
4. What are the features that were considered to make comparative analysis on SD-WAN products?
5. What is the result of comparative analysis done on top three SD-WAN products?

The above questions form the basis to search for data, collect the data, strategy, and tools to be used to perform analysis and interpret the data.

Design of the Study

To study analysis of security features in SD-WAN solution, qualitative approach is performed for evaluation of security strength in different SD-WAN products. Since, security concepts in SD-WAN is explored which is descriptive in nature, qualitative approach is selected. To perform comparative analysis mixed approach is adopted.

Some of the parameters considered for comparative analysis such as key size, number of attacks in last year, attack surface of SD-WAN product, number of well-known issues are deal with numbers and statistics. Other parameters need qualitative approach.

Q1 addresses the most important aspect of this study which is identifying security strengths in SD-WAN solution. This is found in various SD-WAN vendor produced articles in google, articles posted by various networking security websites in internet and papers written by researchers found in google scholar. The keywords used to search and collect this data was “SD-WAN security”, “security benefits of SD-WAN”. The time span used to search research papers were from 2015 to 2022.

Q2 discusses in depth about each security feature identified as part of Q1. This is found in various SD-WAN vendor produced articles in google, articles posted by various networking security websites in internet and papers written by researchers found in google scholar. The answer of Q1 can be used as keywords for get content for Q2. The time span used to search research papers were from 2015 to 2022.

Q3 applies CIA triad concept to SD-WAN product. Here to differentiate each security attribute of SD-WAN under the three principles of CIS triad, articles are collected and studies to get in depth understanding of CIA principles from study websites. Additionally, books such as “The Basics of Information Security”, “Information Security Handbook”, “Network Vulnerability assessment” taken from library were referred. Then the answers from above question, security attributes of SD-WAN will be listed under the appropriate CIA triad principle and justification will be provided for the same. It is prominent to use CIA triad concept to understand security strength of

SD-WAN as CIA triad considers the three most valuable concepts in Information Security.

Q4 was addressed by attaining information from SD WAN vendor official website regarding comparison of their product to other products in market. This gave good insights on what parameters were used for comparative analysis. Also, articles in internet and research papers on google scholar where comparative analysis was already performed between SD-WAN products were thoroughly studied and used as reference to collect required data. Top three SD-WAN vendors in the market were shortlisted to perform security evaluation for this research. They keywords used to collect this data was “comparison of SD- WAN products”, “difference in security strength of SD-WAN product”. The research papers studied were from the timespan 2020- 2022 year, since SD-WAN market merged very recently.

Q5 is addressed by visiting different SD-WAN vendor official websites and understand which security attributes listed in the answer to question 1 were being supported. Also, information in white papers produced by Engineers of those vendor companies were collected and analyzed. Discussion over e-mails with these marketing engineers of these SD WAN products also provided insights about their product. This helped in attaining good picture of each SD WAN product and their security strength. This was also investigated by studying research papers on these products by other researchers and collecting their interpreted data. The key words used were “security of top SD WAN products”, “CISCO SD-WAN security”, “VM Ware SD-WAN security”,”

Versa SD-WAN”. Since these products are launched recently into the market, recent timestamps research papers were only available in google scholar.

Data Collection

To evaluate security equation of SD-WAN solution, information gathering plays a crucial role. Internet is a great useful tool to gather data. Various sources from Internet like google scholar, technical websites, news articles, SD WAN vendor official websites were leveraged to collect all the info as mentioned in design of study. Different keywords to get information for each question mentioned in design of study. The result of a question acted as input to get the answer to another question.SD-WAN is an application of Software Defined Networking (SDN) which was introduced in 2012-2013. SD-WAN was picked up from 2015. So, all the prominent research papers on SD-WAN which discussed about its security were used to retrieve information.

Chapter IV: Data Presentation and Analysis

Introduction

This chapter provides elaborate explanation of each security feature in SD-WAN and the way it contributes to improve the security posture of SD-WAN. Further, each security feature is evaluated based on CIA triad principle. Comparative analysis of security features of top three SD-WAN vendors is discussed in depth.

Data Presentation

Security Features of SD-WAN

Below is the list of security features of SD-WAN which this paper will be discuss followed by in detail explanation of each security feature:

1. Application-Aware Firewall: SD-WAN provides application-aware firewall functionality. The firewall can identify and classify applications based on their characteristics and apply security policies accordingly. The application-aware firewall can identify and block unauthorized applications and prevent them from accessing the network.
2. Intrusion Prevention System (IPS): SD-WAN comes with an Intrusion Prevention System (IPS) that detects and blocks attacks in real-time. The IPS is designed to identify and prevent known and unknown threats, including malware, ransomware, and phishing attacks.
3. URL Filtering: SD-WAN provides URL filtering functionality, which enables administrators to block access to websites that are deemed inappropriate or

malicious. The URL filtering feature can also be used to prevent users from accessing social media sites during working hours.

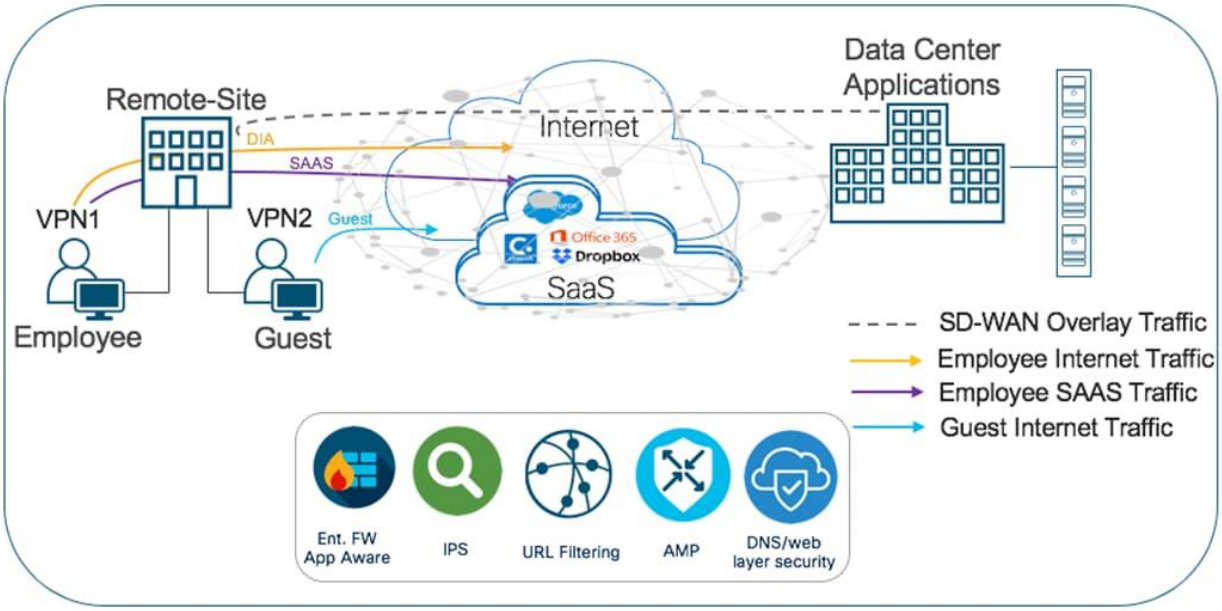
4. Anti-Virus Protection: SD-WAN provides anti-virus protection that can detect and block malware and viruses. The anti-virus protection is designed to provide real-time protection against the latest threats and can be updated automatically.
5. Virtual Private Network (VPN): SD-WAN provides Virtual Private Network (VPN) functionality that allows remote workers to access the corporate network securely. The VPN uses encrypted tunneling to provide secure access to the network and ensures that all data transmitted over the VPN is secure.
6. Multi-Factor Authentication (MFA): SD-WAN provides Multi-Factor Authentication (MFA) functionality that requires users to provide more than one form of authentication to access the network. MFA adds an extra layer of security and makes it more difficult for unauthorized users to access the network.
7. Centralized Management: SD-WAN provides centralized management, which enables administrators to manage the entire network from a single console. The centralized management feature makes it easier to enforce security policies and monitor the network for potential security threats.

8. Dynamic Path Selection: SD-WAN provides dynamic path selection, which enables the network to route traffic over the most optimal path based on the network conditions. Dynamic path selection improves network performance and reduces the risk of downtime due to network congestion.
9. Continuous Monitoring: SD-WAN provides continuous monitoring of the network and alerts administrators in real-time if any security threats are detected. The continuous monitoring feature enables administrators to respond quickly to security threats and take the necessary steps to mitigate the risks.

The figure below showcases different security features supported in a typical SD-WAN solution:

Figure 4

Security Features Supported by a Typical SD-WAN



Application-aware Firewall. Application-aware firewall (AAF) is a software-defined wide area network (SD-WAN) security feature that enhances network security by inspecting and filtering network traffic based on application layer protocols, instead of port and protocol numbers. AAF is designed to be context-aware, giving administrators the ability to control and manage application-specific policies and rules. This feature provides a more granular level of security than traditional firewalls, which only consider the network layer.

In SD-WAN, AAF is an important security feature that benefits many businesses. One of the main advantages of AAF is that it allows network administrators to set security policies based on specific applications, rather than IP addresses or ports. This means that security policies can be created based on the specific needs of each application, rather than having a one-size-fits-all approach. As a result, businesses can protect their applications against a variety of threats such as malware, ransomware, and phishing attacks.

Another important benefit of AAF is that it improves application performance by optimizing traffic flows based on application requirements. AAF can identify and prioritize different types of traffic based on application requirements, helping to reduce latency, packet loss, and jitter, which improves application performance. In addition, AAF provides real-time visibility into application traffic, allowing administrators to monitor and troubleshoot in real time. This feature enables businesses to identify and resolve performance issues quickly and efficiently, reducing the risk of outages. For example, Aruba SD-WAN solution uses deep packet inspection in its application firewall

to identify and distinguish applications based on their traffic patterns (“Advanced threat defense with Aruba SD-branch,” 2022).

Overall, AAF is an important security feature in SD-WAN that brings many benefits to businesses. By providing application-specific and contextual policies and rules, AAF improves network security and performance, and provides real-time control of application traffic.

Intrusion Prevention System. An IPS (Intrusion prevention system) is a security feature that is designed to detect and prevent cyber threats by analyzing network traffic in real-time. It does this by monitoring data packets as they move across the network and comparing them against a set of predefined rules and signatures. If the IPS detects any traffic that matches a known threat, it can take immediate action to prevent the attack from causing any damage.

An intrusion detection system (IDS) is a system that only detects attacks and generates alerts. An intrusion prevention system (IPS) is a system that can actively block malicious traffic from entering the network. This makes it a more proactive approach to network security, as it can prevent attacks before they can cause any harm.

In an SD-WAN environment, an IPS can provide critical network protection against cyber threats. SD-WANs are designed to provide more flexible and scalable network connectivity by using a combination of public and private networks, including the internet. This increased flexibility can make SD-WANs more vulnerable to cyber threats, as there are more potential entry points for attackers to exploit.

An IPS can help protect your network from cyber threats by monitoring and analyzing network traffic regardless of its source or destination. This allows us to detect and prevent cyber threats from any point in the network, including the internet. Additionally, an IPS can provide granular security controls that allow administrators to define specific policies and rules for how network traffic should be handled. An IPS can be configured to block traffic from known malicious IP addresses or prevent certain types of traffic from entering the network altogether. It can also provide alerts to notify administrators when specific types of traffic are detected, such as traffic that violates company policies or compliance regulations.

An IPS is a valuable security feature for SD-WANs and can help detect and prevent attacks before they can cause any damage. IPS can also help administrators manage network traffic more effectively, but it's important to choose an IPS solution that is designed specifically for SD-WANs and can scale to meet the needs of the network.

URL Filtering. URL filtering is a security feature that allows network administrators to block access to specific websites based on the Uniform Resource Locator (URL). SD-WAN solutions that include URL filtering functionality can help to improve security by controlling access to potentially harmful sites and preventing data breaches.

One of the primary benefits of URL filtering is that it can be used to block access to websites known to contain malware or other malicious content. By doing so, the risk of malware infection can be significantly reduced. URL filtering can also help to prevent

data breaches caused by phishing attacks, where attackers create fake websites designed to steal sensitive information from unsuspecting users.

Additionally, URL filtering can be used to enforce company policies and ensure that employees are not wasting time on non-work-related sites. By blocking access to certain sites, companies can improve productivity and prevent employees from engaging in activities that could put the company at risk.

Another advantage of URL filtering is that it can help companies comply with regulatory requirements. For example, the EU's General Data Protection Regulation (GDPR) requires companies to ensure that their websites are GDPR-compliant. By blocking access to websites that are not compliant, companies can avoid inadvertently violating the regulation.

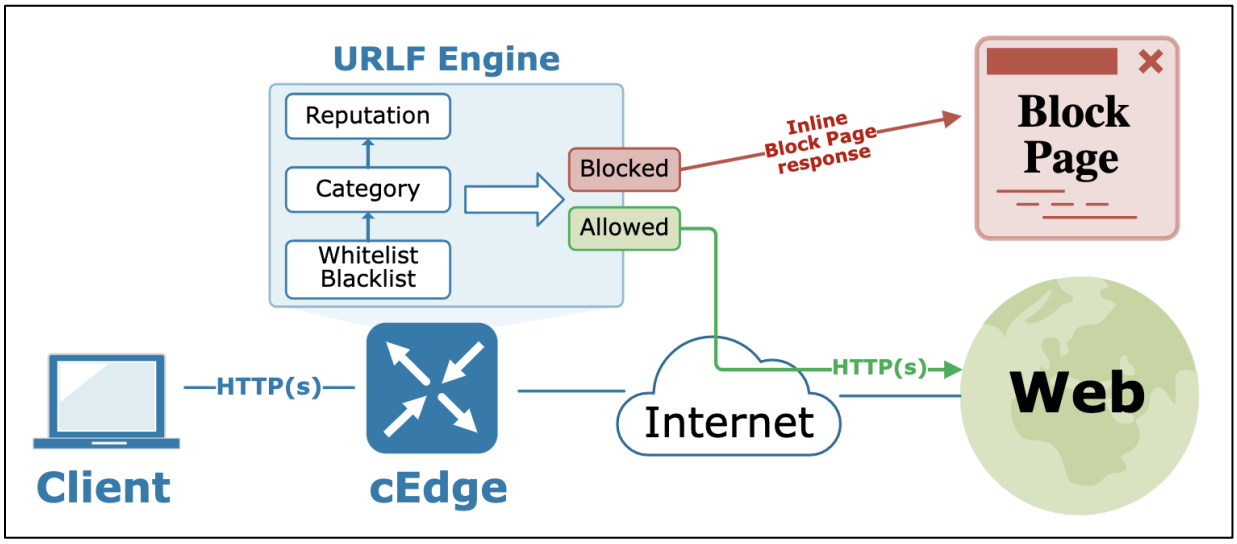
URL filtering can also be used to provide granular control over user access to websites. This means that only authorized users can access specific sites, helping to prevent data breaches caused by unauthorized access to sensitive information.
By combining URL filtering with other security features such as encryption and multi-factor authentication, SD-WAN solutions can significantly improve security and reduce the risk of data breaches and other security threats.

Cisco SD-WAN URL Filtering features enabled edge devices to inspect both plain HTTP traffic and encrypted HTTPS traffic and enforce URL based control. Either a cloud-hosted or locally hosted database is utilized by the URLF engine. Cisco’s SD-WAN Edge devices don't download the URL database locally by default. "Download URL Database on Device" option must be selected in order to enable the local database

copy. The HTTP(s) request is permitted, and no further inspection is carried out if the URL matches an entry in a whitelist that is defined by the user. The router responds with a block page or an HTTP redirect to an existing block page if the URL matches an entry in a user-defined blacklist. The requested URL falls into one of the 82 pre-defined Web categories if it does not match one of the whitelist or blacklists. Access is granted if the corresponding Web category is permitted. The request is routed to the blocked page if it is blocked.

Figure 5

URL Filtering in Cisco SD-WAN (URL Filtering, 2022)



In summary, URL filtering is an important security feature in SD-WAN solutions that can help to prevent malware infections, phishing attacks, and data breaches. By controlling access to potentially harmful sites, enforcing company policies, and complying with regulatory requirements, URL filtering can help to improve security and protect sensitive information.

Antivirus Protection. Antivirus Protection is like the immune system of your network, protecting against malware and other cyber threats. As a security feature of SD-WAN, it is one of the essential measures to safeguard network traffic and data. The antivirus protection in SD-WAN works by using specialized software that scans incoming and outgoing traffic for viruses and other malicious code. This software is installed on devices at the edge of the network, such as routers or firewalls. When malware is detected, the antivirus software takes swift action to prevent it from spreading and causing harm to the network. This can include blocking access to infected websites, quarantining infected files, and notifying network administrators of the threat.

Anti-Virus Protection is a security feature that works to stop malware and other types of malicious software from getting into a network. It works by blocking incoming traffic before it reaches the network and scanning it for known malware and viruses. A dedicated virtual machine that is connected to the SD-WAN network and runs antivirus software provides antivirus protection in SD-WAN.

The fact that anti-virus protection in SD-WAN provides a centralized security platform capable of safeguarding all network devices is the primary advantage of this type of protection (Weinberg, 2019). In conventional wide area networks (WANs), each device typically has its own anti-virus software, which can result in inconsistencies and vulnerabilities. All network devices are protected by a single antivirus solution with SD-WAN, which can be updated and managed from a single location.

Anti-virus protection in SD-WAN has the additional advantage of reducing device load. Running antivirus software on every device can slow down performance and consume a lot of resources. SD-WAN can offload the processing of anti-virus scans to a central location by deploying a dedicated virtual machine that runs antivirus software. This reduces the load on individual devices.

Cisco, Fortinet, and Palo Alto Networks are just a few of the vendors that offer SD-WAN solutions with Anti-Virus Protection features. These sellers give extensive security arrangements that consolidate hostile to infection insurance with other security elements, for example, interruption discovery and anticipation, web sifting, and firewalls.

Finally, hostile to infection assurance is a fundamental component in SD-WAN that improves the security stance of associations. It provides a centralized platform for managing and controlling WAN connections, shields all network devices from known malware and viruses, and reduces device load. SD-WAN with anti-virus protection will continue to be a popular choice for businesses looking to improve their security posture as network security threats continue to evolve. The importance of antivirus protection in SD-WAN cannot be overemphasized. Malware can cause significant damage to a network, such as theft of sensitive data, disruption of operations, and financial losses. By using antivirus protection as part of an SD-WAN solution, organizations can significantly reduce their risk of falling victim to cyber-attacks and ensure the security and integrity of their network. The Anti-Virus Protection feature is one of the features that make SD-WAN safer.

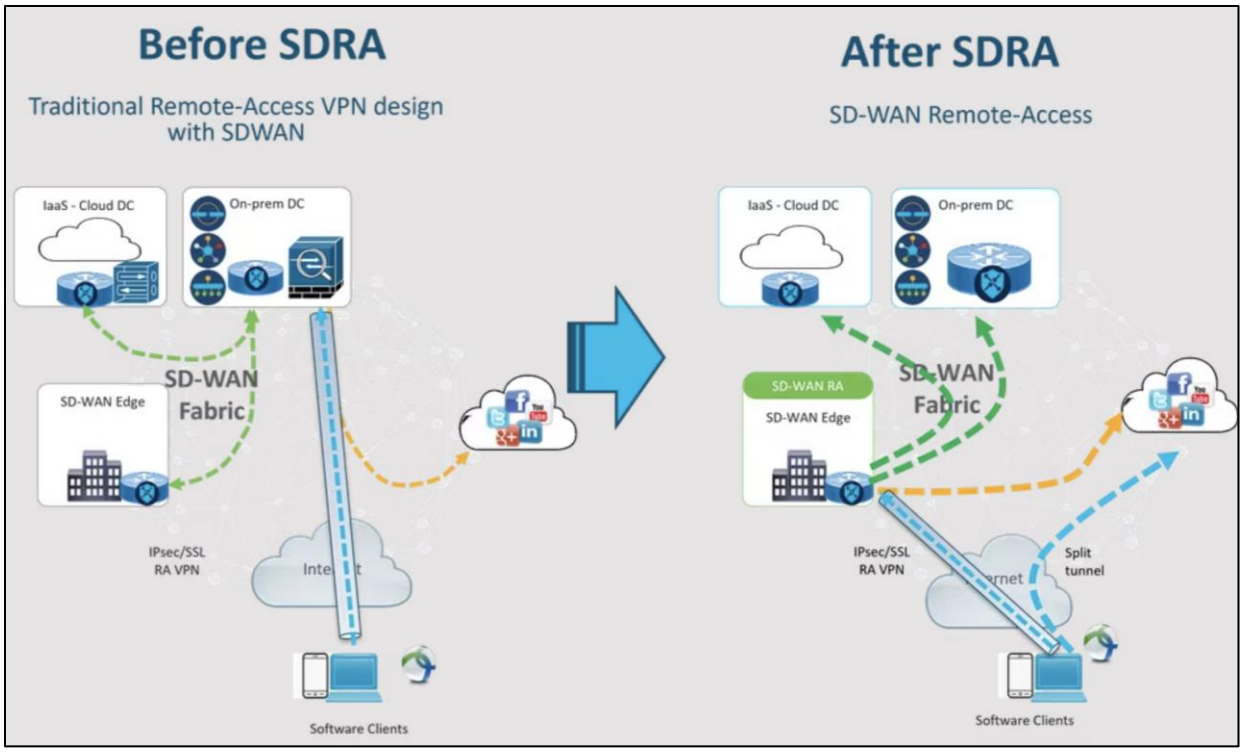
Virtual Private Networks. A virtual private network (VPN) is a safe tunnel that connects two or more devices over an unreliable network like the Internet. Encryption protocols are used to build the tunnel to keep data between the devices safe from unauthorized access or interception. There are two fundamental kinds of VPNs: VPNs for remote access and site-to-site VPNs. Remote access VPNs enable individual users to connect to a network from a remote location, whereas site-to-site VPNs are used to connect two or more networks together.

VPNs are used to secure connections between various network locations, such as branch offices and data centers, in the context of SD-WAN. This is important because traditional wide area networks are usually made to connect different locations with private, dedicated connections like MPLS circuits or leased lines. When connecting to cloud environments, these private connections can be challenging to manage and are costly. On the other hand, SD-WAN makes it possible for businesses to connect their various network locations using the Internet, which is more cost-effective and adaptable. VPNs come in handy because it can be risky to transmit sensitive data over the Internet without adequate security measures.

By utilizing VPNs to lay out secure passages between various organization areas, SD-WAN can give an elevated degree of safety for information transmissions. The encryption conventions utilized by VPNs guarantee that information communicated between the gadgets is shielded from unapproved access or capture. VPNs can also be set up to use a variety of authentication methods, like usernames and passwords or digital certificates, to make sure that only authorized users can access the network.

Figure 6

Split Tunnel Used in Cisco SD-WAN (“Configure SD-WAN remote access (SDRA) with AnyConnect and ISE server,” 2022)



The capacity of SD-WAN to support a variety of VPNs is one of its advantages. Site-to-site VPNs, remote access VPNs, and even third-party VPNs from various vendors are all supported by SD-WAN. Because of this adaptability, businesses are able to select the VPN service that best meets their requirements and budget. The capacity of SD-WAN to provide centralized management and control of the VPN infrastructure is yet another advantage. This means that rather than having to manage each connection separately, network administrators can easily configure and manage the VPN connections from a single console. Monitoring and troubleshooting VPN

connections is made simpler as a result, which can help cut down on downtime and boost network performance.

In conclusion, VPNs are an important part of SD-WAN because they make data transmissions between different network locations highly secure. VPNs protect data transmitted over the Internet from unauthorized access or interception by employing authentication and encryption protocols. SD-WAN is a cost-effective and flexible option for connecting various network locations because it supports multiple VPN types and provides centralized management and control.

Multi-Factor Authentication. Before gaining access to a system or network, users are required to provide two or more forms of authentication with the Multi-Factor Authentication (MFA) security feature. MFA is a critical component of security in SD-WAN due to the nature of the technology.

Software-based solutions like SD-WAN are susceptible to cyberattacks like malware attacks, unauthorized access, and data breaches. By adding an additional layer of protection, MFA is an efficient method for enhancing the security of SD-WAN. MFA ensures that only authorized users can access the network by requiring users to provide multiple forms of authentication. This fundamentally lessens the gamble of unapproved access and information breaks. Below table explains the most prevalent methods of authentication in MFA.

Table 5

Methods of Authentication in MFA

Factor	Description
Knowledge	Something the user knows, such as Password or PIN
Possession	Something the user has, such as security token or OPT sent to smartphone
Inherence	Something the user is, such as biometric data (finger print or facial scan)

MFA is typically used as part of the authentication process in SD-WAN for remote users who access the network outside of the corporate setting. Solutions like biometric authentication, or smart card authentication can be used to implement MFA in SD-WAN. Biometric authentication which includes facial recognition or fingerprinting make it harder for criminals to pretend to be users. To gain access to the system, a smart card with a cryptographic key must be inserted into a card reader using smart card authentication.

MFA in SD-WAN helps to protect the network from security threats like hacking, phishing, and other cyberattacks by requiring multiple forms of authentication. Additionally, it reduces the likelihood of data breaches and other security incidents by ensuring that only authorized users have access to sensitive applications and information. A hacker will not be able to access the network unless they provide the additional authentication factor, even if they are successful in obtaining a user's password.

Additionally, MFA is necessary for adhering to data security standards like the Payment Card Industry Data Security Standard (PCI DSS) and the General Data

Protection Regulation (GDPR). In order to safeguard sensitive data and prevent data breaches, these regulations require businesses to implement robust authentication measures.

In conclusion, MFA is an essential feature of SD-WAN that requires users to provide multiple forms of authentication prior to accessing the network, providing an additional level of security. SD-WAN is now a more secure option for businesses thanks to this significant reduction in the likelihood of unauthorized access and data breaches.

Centralized Management. Centralized management, or the capacity to manage and monitor the network from a single, unified interface, is one of the most important aspects of SD-WAN. In this article, we will make sense of the advantages of unified administration in SD-WAN and how it adds to making SD-WAN safer.

Network administrators can have complete visibility and control over their network from a single location thanks to centralized management in SD-WAN. This means that they won't have to physically access each device to easily configure, monitor, and troubleshoot the network. Because it enables organizations with multiple branch locations to manage all their network devices from a single location, this feature is especially useful for them because it saves time and reduces the likelihood of errors.

Table 6

Key Difference Between Centralized Management in Traditional WAN and SD-WAN

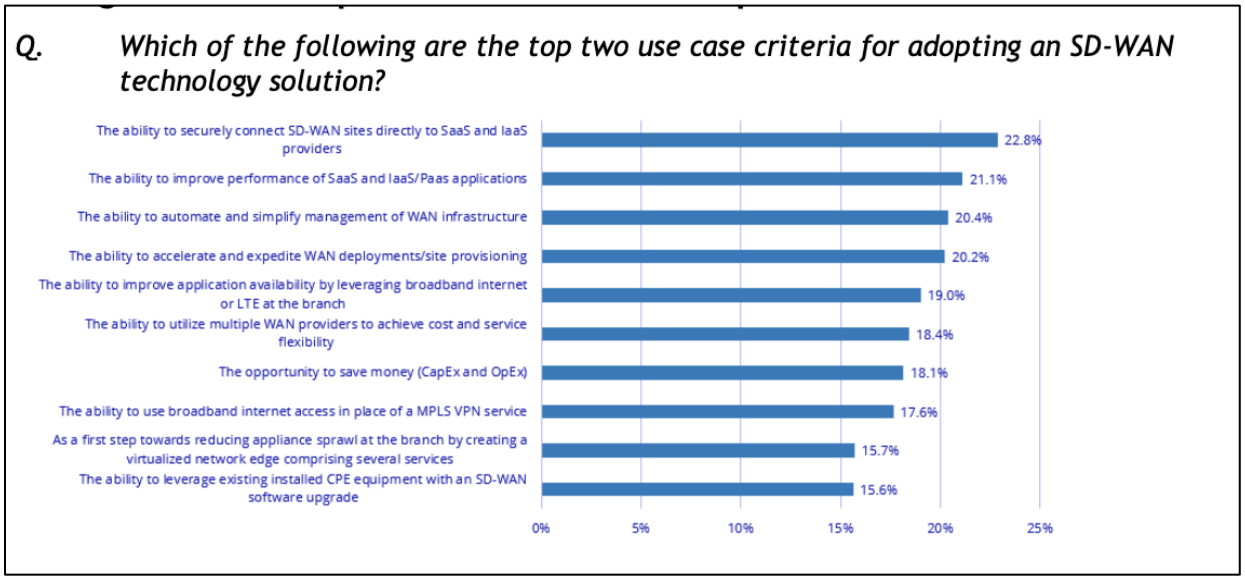
Feature	Traditional WAN	SD-WAN
Centralized Management	Requires manual configuration and management of individual devices and connections.	Offers centralized management, allowing for the configuration and management of devices and connections from a single interface.

Improved network security is one of the main advantages of centralized management in SD-WAN. Administrators are able to quickly identify and respond to potential security threats because they have complete visibility and control over the network. They can quickly identify and isolate compromised applications or devices, set security policies for the entire network, and keep an eye on network traffic for unusual activity. Additionally, centralized management can assist businesses in meeting network security regulations like the Payment Card Industry Data Security Standard (PCI DSS) and the General Data Protection Regulation (GDPR).

As per the study conducted by IDC Analyst on SD-WAN ‘s Security, Application Experience and Operational Simplicity Drive Market Growth, simplified WAN management is among the top three drivers of SD-WAN adoption.

Figure 7

Top Three Drivers for SD-WAN Adoption (IDC Technology Spotlight, 2019)



In addition, SD-WAN's centralized management makes it possible for businesses to implement a zero-trust security model, which is becoming increasingly significant in the threat landscape of today. A security model known as zero-trust security requires ongoing authentication and authorization for access to network resources and makes the assumption that no user or device can be trusted by default. Unified administration in SD-WAN empowers associations to carry out this model by giving granular command over client and gadget access, as well as the capacity to powerfully change security approaches in light of evolving conditions.

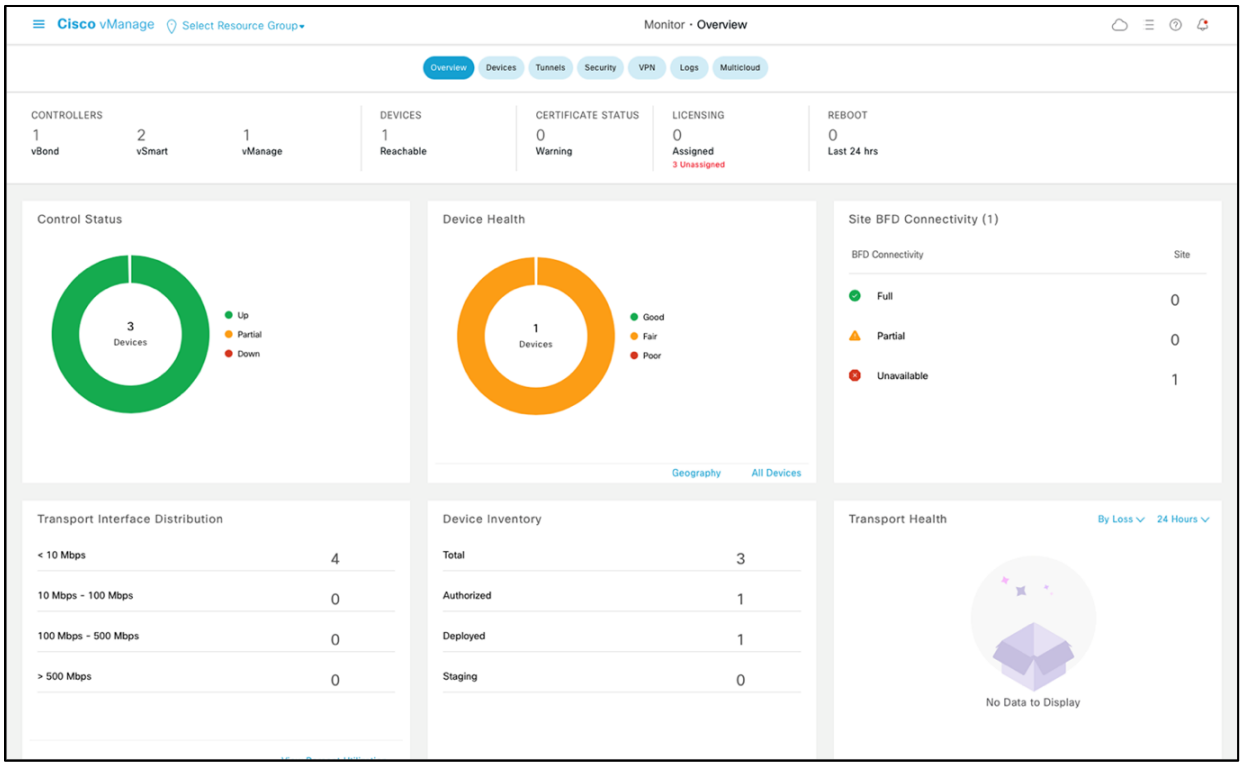
Unified administration in SD-WAN likewise gives a few different advantages, for example.

a) Management of the network simplified: Without having to access each device individually, administrators can easily configure and monitor the network with centralized management. Network management becomes more effective and efficient as a result of this time and error reduction.
b) Lower downtime: Administrators can quickly identify and resolve issues before they become major ones by monitoring the network in real time. Reliability of the network as a whole and downtime are both reduced as a result.
c) Improved adaptability: Organizations can scale their network more easily as they grow thanks to centralized management's ease of adding new network devices and locations as needed.

Cisco SD-WAN dashboard shown in Figure 8 enables to connect all of the company's data centers, core and campus locations, branches, colocation facilities, cloud infrastructure, and remote workers with the help of this dashboard. Cisco SD-WAN uses Overlay Management Protocol (OMP) to your entire network to enable this interconnection. Cisco SD-WAN improves on IT tasks with mechanized provisioning, bound together arrangements, and smoothed out administration, making changes, updates, and goals in record time by leveraging this centralized management feature and thereby enhancing network security, reliability, and functionality.

Figure 8

Cisco SD-WAN Dashboard for Centralized Management Feature (“SD-WAN solution - Cisco SD-WAN solution overview,” 2022)



Overall, centralized management is a key feature of SD-WAN that offers numerous advantages to businesses, including increased scalability, reduced downtime, improved security, and simplified network management. Central management enables administrators to quickly identify and respond to potential security threats, implement zero-trust security policies, and comply with network security regulatory requirements by providing them with complete visibility and control over the network (“Secure SD-WAN,” 2023).

Dynamic Path Selection. Software-Defined Wide Area Network has a feature called Dynamic Path Selection (DPS) that uses application and network conditions to intelligently route traffic over multiple paths, such as private circuits, LTE connections, and Internet broadband. Based on real-time performance metrics like latency, jitter, packet loss, and bandwidth availability, SD-WAN dynamically selects the most secure and efficient path for data traffic with DPS.

SD-WAN security is enhanced by a number of DPS benefits. First, DPS makes it possible for SD-WAN to automatically adjust to changes in the network and application environment. As a result, traffic is always routed over the most secure and optimal route. DPS can, for instance, automatically switch to another path without user intervention in the event that one path experiences packet loss or becomes congested, ensuring that traffic continues to flow securely and smoothly.

Second, DPS enables SD-WAN to implement advanced security policies and protocols, such as encryption, firewall, intrusion prevention, and malware detection, at the network edge, adding an additional layer of protection. Depending on the particular security requirements of each location, SD-WAN can enforce security policies and protocols on a per-application or per-branch basis with DPS. Applications that are not sensitive, like web browsing, can be routed over public broadband connections, while applications that are sensitive, like financial transactions, can be encrypted and routed over dedicated circuits.

Thirdly, DPS makes it possible for SD-WAN to connect securely cloud-based applications and services. Based on real-time network conditions, SD-WAN can use

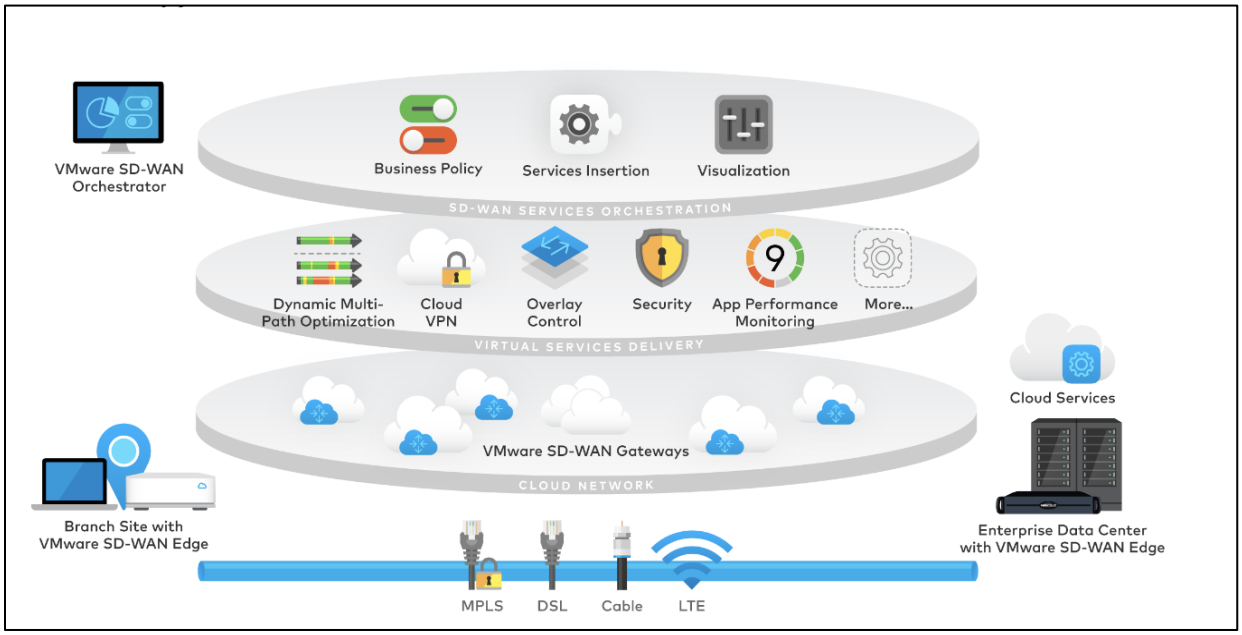
DPS to automatically route traffic to the cloud data center that is closest and most reliable and enforce security policies and protocols at the cloud edge. Without sacrificing performance or security, this ensures that traffic is always directed to cloud applications via the most secure and optimal route.

Figure 9

Dynamic Path Steering in Aruba SD-WAN (“Aruba SD-WAN dynamic path steering with service level agreements,” 2019)

Figure 10

VMware SD-WAN Shows Support for Dynamic Multi-Path Optimization



DPS makes it possible for SD-WAN to connect remote and mobile users securely, regardless of where they are or what device they are using. SD-WAN can securely connect remote and mobile users to the corporate network over any Internet connection, including public Wi-Fi, LTE, or satellite, with DPS. Without sacrificing performance or security, this makes it possible for mobile and remote employees to securely access corporate applications and data from any location.

DPS has been demonstrated in a number of studies to significantly enhance SD-WAN security and performance. SD-WAN with DPS, for instance, was found to be capable of detecting and preventing all advanced threats and malware in a study conducted by NSS Labs (NSS-Labs-SD-WAN-comparative-report-performance, 2018), while also reducing WAN latency by up to 80% and increasing application performance

by up to 40%. SD-WAN with DPS reduced WAN costs by up to 90%, increased network reliability by up to 99.99%, and increased security by allowing security policies and protocols to be enforced at the network edge.

Figure 11

Packet Delay Variation and Packet Loss (Voice and Video)

Vendor	Dynamic Path Selection	
	VoIP QoE	Video QoE
Barracuda Networks	2.56	2.32
Citrix Systems	4.33	4.52
Cradlepoint	4.16	1.19
FatPipe Networks	4.26	3.55
Forcepoint	4.39	4.04
Fortinet	4.40	4.40
Talari Networks	4.41	4.38
Versa Networks	4.37	4.53
VMware	4.39	4.46

In conclusion, SD-WAN's Dynamic Path Selection makes it possible to route data traffic over multiple paths in an intelligent and secure manner. SD-WAN can automatically adapt to changes in the network and application environment, enforce advanced security policies and protocols, provide secure connectivity to cloud-based applications and services, and extend the corporate network to users who are located far away or on the move with the help of DPS. DPS is an essential feature for any organization that relies on WAN connectivity. It is a potent tool that significantly enhances SD-WAN's security and performance.

Continuous Monitoring. Continuous monitoring, which plays a crucial role in ensuring the network's security, is one of SD-WAN's key features. Real-time monitoring of network traffic, devices, and applications to identify potential security threats on a constant basis is continuous monitoring. SD-WAN keeps an eye on the traffic on the network all the time to look for any unusual activity that could be a sign of a security threat like malware or a data breach. Because it makes it possible for businesses to quickly identify and respond to security incidents, it is an essential part of network security. The capacity to detect and prevent security threats in real time is one of the primary advantages of continuous monitoring in SD-WAN. SD-WAN relies heavily on continuous monitoring because it enables businesses to better control and monitor their entire network from a single location.

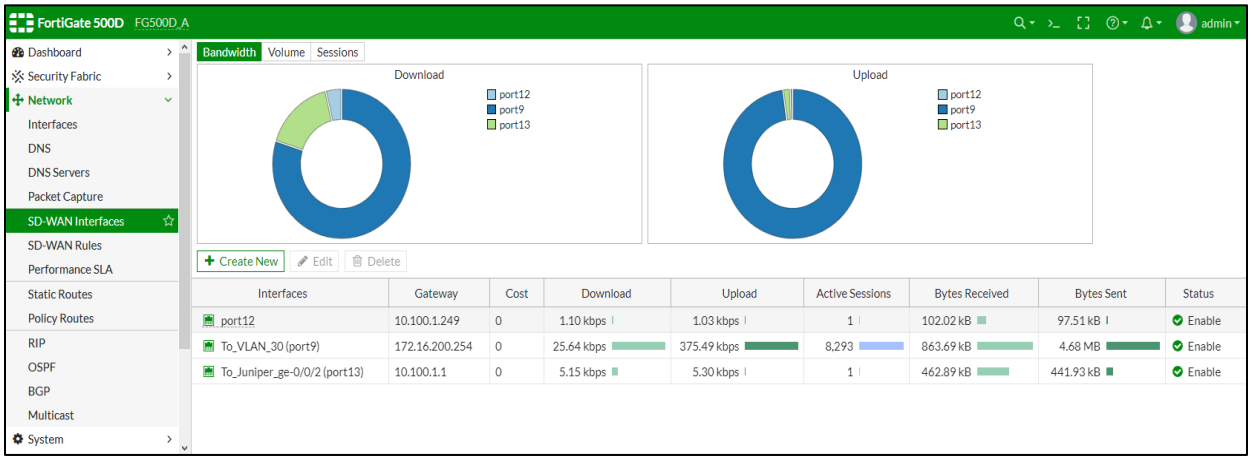
SD-WAN keeps checking the network for vulnerabilities like out-of-date software and notifies administrators so they can take the necessary steps. An organization's risk of a security breach can be significantly reduced by addressing vulnerabilities before they are used. Organizations are able to identify any potential application and network vulnerabilities through continuous monitoring.

The capacity to impose security policies across the entire network is yet another significant advantage of SD-WAN that benefits from continuous monitoring. SD-WAN makes it possible for businesses to centrally define and enforce security policies, ensuring that all applications and devices comply. Organizations can verify that these policies are being followed and identify devices or applications that are not in compliance with them through continuous monitoring.

Organizations are also able to adhere to regulatory requirements with the aid of continuous monitoring. As part of their security strategy, many regulatory frameworks, like the Payment Card Industry Data Security Standard (PCI DSS) and the General Data Protection Regulation (GDPR), require businesses to implement continuous monitoring. Organizations can guarantee that they are meeting these regulatory requirements by implementing SD-WAN with continuous monitoring. Figure shows dashboard of FortiGate SD-WAN which is used for continuous monitoring (“SD-WAN GUI and monitoring enhancements,” 2023).

Figure 12

FortiGate SD-WAN GUI for Continuous Monitoring



In conclusion, continuous monitoring is a crucial component of SD-WAN that contributes significantly to the network's security. It makes it possible for businesses to quickly identify security threats, identify vulnerabilities, enforce security policies, and comply with regulatory requirements. Organizations can significantly improve their

network security posture and lower their risk of a security breach by implementing SD-WAN with continuous monitoring.

CIA Triad and Application of CIA Triad Principle on SD-WAN's Security Features

The CIA Triad Principle is a fundamental concept of information security that deals with the three essential components of information security: confidentiality, integrity, and availability. Triads are an essential tool for designing and implementing information security measures to protect sensitive data and systems from unauthorized access, modification, or destruction.

Confidentiality is the first element of the CIA's triple principle. It deals with the protection of sensitive information from unauthorized disclosure. Confidentiality ensures that only authorized people or systems can access sensitive data. Security measures may include access control mechanisms, such as password protection, encryption, or physical security measures, such as door locks or restricting access to certain areas.

Integrity is the second element of the CIA's triple principle. It deals with protecting sensitive information from unauthorized modification or alteration. Integrity ensures that data is accurate, complete, and reliable. Integrity measures may include digital signatures, checksums, or hashes capable of detecting changes to data. Additionally, access control and audit logs can help prevent unauthorized changes to data.

Availability is the third component of the CIA's triple principle. It refers to the protection of information and data systems from unauthorized denial of service (DoS) attacks or other disruptions that may render the system unavailable. Availability ensures that authorized users can access information and data systems when needed. Available

measures may include contingency, backup, and disaster recovery plans to ensure that information systems can recover quickly from an incident.

Application-aware Firewall. The application-aware firewall security feature can be evaluated using the CIA triad principle in SD-WAN. This feature enhances security against unauthorized access and data breaches by enabling organizations to implement granular policies to control network traffic based on the application being used.

a) Confidentiality: Confidentiality is ensured by controlling access to sensitive data via application-specific policies in the context of the application-aware firewall security feature. By setting these policies to allow or deny access to particular applications, sensitive data can only be accessed by authorized individuals.
b) Integrity: The application-aware firewall security feature in SD-WAN protects data integrity by monitoring network traffic and preventing attempts to alter or alter data in transit. Data injection attacks is just one example of the types of cyberattacks that this feature protects against.
c) Availability: By allowing authorized users to access the network and the applications they require to complete their tasks while blocking unauthorized access, the application-aware firewall security feature ensures availability. Additionally, organizations can use this feature to prioritize traffic on the network and guarantee that critical applications receive priority access to network resources.

In conclusion, this feature enhances security against a variety of cyber threats and aids organizations in protecting their sensitive information by guaranteeing confidentiality, integrity, and availability.

Intrusion Prevention System. Below is the discussion whether Intrusion Prevention System meets all principles of CIA triad.

a) Confidentiality: By preventing unauthorized network access, IPS significantly contributes to maintaining confidentiality. Monitoring traffic patterns, identifying potential threats, and blocking suspicious traffic are some of the various strategies that IPS employs in order to identify and prevent attempts at unauthorized access. This helps to ensure that sensitive data is only accessible to authorized users.

    An IPS system can, for instance, spot and stop Distributed Denial of Service (DDoS) attacks, which can render a network inaccessible and compromise confidentiality (Ristic, 2019). The IPS system is able to identify and block malicious traffic, assisting in the preservation of confidential information and the availability of the network.

b) Integrity: IPS assists with keeping up with the trustworthiness of information by observing traffic designs and recognizing expected dangers. The framework can distinguish any endeavors to alter information. This aids in ensuring that data remains reliable and accurate.

    An IPS system, for instance, is able to identify and thwart SQL injection attacks, which are designed to alter database data. The IPS system is

capable of detecting the attack and blocking the malicious traffic, thereby preventing data modification.

c) Availability: By detecting and preventing attacks that can render a network inaccessible, IPS is crucial to maintaining availability. The system is able to keep track of traffic patterns, identify potential threats, and take the necessary preventative measures. This helps make sure that data is always available.

An IPS system, for instance, is capable of detecting and preventing malware attacks that could jeopardize a network's availability. The IPS system is able to identify an attack and prevent malicious traffic from entering the network, preserving its availability.

In conclusion, SD-WAN's IPS security feature is an effective security measure for protecting data transmission over the network because it adheres to each of the three CIA triad principles. The IPS system contributes to maintaining confidentiality, integrity, and availability by detecting and preventing attacks that have the potential to make a network inaccessible as well as unauthorized access, unauthorized modification, and attacks.

URL. Let us look at analysis done below to understand whether Intrusion Prevention System meets all principles of CIA triad.

a) Confidentiality: URL filtering can be used to restrict access to specific websites and content, thereby preventing unauthorized access and safeguarding data's confidentiality. URL Filtering aids in preventing employees from accidentally accessing confidential or sensitive information

by preventing access to websites that are known to be malicious or to contain harmful content. This aids in the prevention of data breaches and other security incidents that could jeopardize the data's confidentiality (“What Is URL filtering?,” n.d.).

b) Integrity: By preventing unauthorized modifications, URL filtering can also aid in maintaining the integrity of data. URL Filtering helps employees avoid downloading malware or other types of malicious software that could compromise the integrity of data by blocking access to websites that are known to be malicious or contain harmful content. This aids in ensuring that data remains reliable and accurate.

c) Availability: By limiting access to particular content and websites, URL filtering can have an effect on the availability of data. However, this can be mitigated by ensuring that employees have access to alternative resources and that only essential websites are blocked. URL Filtering contributes to ensuring that data remains accessible by preventing security incidents that could impact the availability of data by preventing access to websites that are known to be malicious or contain harmful content.

In conclusion, URL Filtering adheres to the CIA triad principle by effectively protecting data confidentiality, integrity, and availability.

Anti Virus

a) Confidentiality: By stopping malware from stealing or transmitting sensitive data, antivirus protection contributes to maintaining confidentiality. Software

that aims to harm, disrupt, or gain unauthorized access to a computer system or network is known as malware. It can steal or alter data, compromise network security, and cause system crashes or failures once it infects a system. Signature-based detection, behavioral analysis, and sandboxing are some of the methods that are utilized in anti-virus protection to identify and eliminate malware. Signature-based identification includes looking at the code of documents or applications against a data set of known malware marks. Attempts to alter system files or establish unauthorized network connections are two examples of suspicious behavior that are looked for in behavioral analysis. In order to observe the behavior of potentially malicious code and prevent it from infecting the system, sandboxing is a method that isolates it in a controlled environment. Symantec Endpoint Protection Feature (n.d.), an anti-virus software aids in safeguarding confidential network data by employing these strategies.

b) Integrity: Malware is capable of adjusting or erasing documents, scrambling information for deliver, or embedding secondary passages into the framework for future access. By identifying and eliminating malware that attempts to alter or delete files, encrypt data, or insert backdoors, antivirus protection contributes to the integrity of data. It additionally assists with forestalling unapproved admittance to information by hindering malware that endeavors to lay out unapproved network associations. Antivirus software contributes to the safety and security of the network by preserving the integrity of data.

c) Availability: System crashes, sluggish network performance, or blocking access to essential applications or data are all ways in which malware can compromise availability. By identifying and eliminating malware that has the potential to slow down network performance or cause system crashes, antivirus protection contributes to maintaining availability. By preventing malware from flooding the network with traffic, it also aids in the prevention of denial-of-service attacks. Anti-virus protection aids in ensuring that authorized users have access to the network and its resources by maintaining availability.

In conclusion, Anti-Virus Protection meets Confidentiality, Integrity, and Availability which are part of CIA triad principle.

Virtual Private Network.

a) Confidentiality: VPN guarantees secrecy by utilizing encryption to protect the information communicated between the endpoints. Secure tunneling is made possible by VPN protocols like OpenVPN, IPSec, and SSL/TLS. These protocols encrypt the data. OpenVPN, for instance, encrypts data with the OpenSSL library and offers robust encryption. IPSec gives encryption, validation, and respectability of information transmission. SSL/TLS protocols use certificates to guard against man-in-the-middle attacks and verify the authenticity of endpoints.

b) Integrity: In order to guarantee that data has not been altered during transit, VPN protocols make use of integrity checks like hash functions. A unique

checksum for the transmitted data is created using hash functions. At the receiving end, this checksum is compared to ensure that the data has not been altered. The data is rejected if the checksums do not match.

c) Availability: The idea behind availability is to make sure that authorized users can access data whenever they need it. VPNs provide a safe connection between two endpoints to guarantee availability. This association guarantees that information is accessible to the planned beneficiaries. The user does not need to take any additional actions in order to access the data because the VPN connection is established automatically.

In conclusion, the CIA triad principle is satisfied by the SD-WAN VPN security feature.

Multi-factor Authentication.

a) Confidentiality: By adding an additional layer of security to user credentials, multi-factor authentication (MFA) increases data confidentiality. An attacker will not be able to access the network or application without the additional authentication factor with MFA, even if the user's password is compromised. This ensures that only authorized users have access to sensitive data and helps to prevent unauthorized access. MFA "makes it much more difficult for an attacker to steal credentials and gain unauthorized access to systems, applications, and data," as stated in the National Institute of Standards and Technology (NIST) Digital Identity Guidelines (NIST, 2017, p. 6).

b) Integrity: By providing an additional layer of security to prevent unauthorized changes to the data, MFA also improves the integrity of the data. By requiring different types of confirmation, MFA guarantees that main approved clients can make changes to the information. This helps keep data from being altered without permission, which can hurt the data's accuracy and dependability. MFA "helps to prevent unauthorized changes to information and information systems," as stated in the NIST Digital Identity Guidelines (NIST, 2017, p. 6).

c) Availability: By adding an additional layer of protection against unauthorized denial-of-service attacks, MFA also makes data more accessible. MFA makes sure that only authorized users can access the network or application by requiring multiple forms of authentication. This aids in the prevention of unauthorized denial-of-service attacks, which have the potential to compromise the application or network's availability. MFA "helps to prevent denial-of-service attacks by making it more difficult for an attacker to authenticate," as stated in the NIST Digital Identity Guidelines NIST, 2017, p. 6). In addition, phishing attacks, which are a common way for hackers to steal user credentials, are less likely to occur thanks to MFA. Even if phishers have obtained a user's password, MFA makes it harder for them to access the network or application.

In conclusion, by enhancing data confidentiality, integrity, and availability, MFA fulfills all three CIA triad principles. MFA adds an extra layer of protection against

unauthorized modifications, access, and denial-of-service attacks. Additionally, it aids in reducing the threat of phishing attacks.

Centralized Management.

a) Confidentiality: By providing secure access control, centralized management safeguards the confidentiality of data. It prevents unauthorized access to the network and its data by utilizing authentication and encryption to ensure that only authorized personnel can access it. A fine-grained level of access control that restricts access based on job functions and responsibilities is provided by the utilization of Role-Based Access Control (RBAC). Data breaches and data loss are less likely as a result of this.

    SD-WAN merchants like Fortinet deal incorporated administration reassures that give security highlights like Identity and Access Management (IAM) and Single Sign-On (SSO), which offer extra security layers to safeguard against unapproved access to the organization. SSO solutions ensure that only authorized individuals can access the network, whereas IAM solutions provide secure access control.

b) Integrity: By providing a consistent and uniform set of security policies across the entire network, centralized management ensures the integrity of data. Consistencies in security policies that could result in data breaches or loss are eliminated by this. Cisco and other SD-WAN providers provide centralized management consoles that enable network administrators to apply security

policies to all network devices simultaneously, guaranteeing that all devices adhere to the same set of policies.

In addition, network traffic can be monitored and analyzed in real time with Centralized Management. Before they harm the network, anomalies and threats can be detected and dealt with by administrators of the network. Vendors of SD-WAN, such as VMware, provide centralized management consoles that offer analytics and visualization of network traffic in real time. This enables administrators of the network to quickly identify and resolve issues.

c) Availability: Data availability is ensured by providing network devices with high availability and redundancy through centralized management. Silver Peak and other SD-WAN providers provide centralized management consoles that allow network administrators to monitor and manage the entire network from a single location, saving time and effort. This guarantees that authorized personnel will always have access to network devices.

Additionally, Centralized Management offers capabilities for automated failover and disaster recovery, which guarantee that network services will continue to function even in the event of a network failure. Palo Alto Networks and other SD-WAN providers provide centralized management consoles with automated failover and disaster recovery capabilities to always guarantee the availability of network services.

In conclusion, the Centralized Management security feature of SD-WAN fulfills the CIA triad by offering high availability and redundancy to network devices, automated failover and disaster recovery capabilities, consistent and uniform security policies, real-time monitoring and analysis of network traffic, and secure access control for authorized personnel. These features guarantee that authorized personnel can access, secure, and have access to the network's data.

Dynamic Path Selection.

a) Availability: By employing multiple data transmission paths, the DPS feature of SD-WAN ensures that network traffic can be rerouted in the event of a network failure or congestion.

    SD-WAN's DPS feature ensures that data is transmitted over the most optimal path by dynamically selecting the best path for data transmission based on network conditions. By ensuring that data is transmitted over the most secure route and reducing the likelihood of network congestion or failure, this increases the availability of network systems.

A report by Gartner found that SD-WAN arrangements can further develop network accessibility by involving numerous ways for information transmission (“Magic quadrant for SD-WAN,” n.d.). According to the report, "SD-WAN solutions offer built-in resiliency, failover, and load-balancing capabilities that can help ensure high availability of business-critical applications." This demonstrates the DPS feature's effectiveness in increasing network system availability.

Taking everything into account, SD-WAN's DPS security satisfies the Availability in CIA triad.

Continuous Monitoring. One of the security highlights of SD-WAN is continuous monitoring. Organizations will be able to quickly identify and respond to security threats thanks to this feature, which is designed to provide visibility and monitoring of network traffic in real time. Let us investigate whether software-defined WAN's continuous monitoring security feature adheres to the CIA triad principle.

a) Confidentiality: Data confidentiality is protected by continuous monitoring. It does this by checking network traffic for unapproved access endeavors. Security personnel can be alerted to unauthorized access attempts and take action to prevent data breaches through continuous monitoring. The Ponemon Institute conducted a study that found that the average cost of a data breach in 2020 would be $3.86 million (Ponemon Institute, 2020). As a result, it is essential for businesses to safeguard the confidentiality of their data.
b) Integrity: Data integrity is also protected by continuous monitoring. It does this by looking for data tampering in network traffic. Data tampering can be detected, and security personnel alerted through continuous monitoring, allowing them to take preventative measures. Organizations can ensure that their data is accurate and not altered by ensuring the integrity of the data.
c) Availability: Data availability is also ensured by continuous monitoring. It does this by looking for network failure or congestion by monitoring network traffic.

Security personnel can be notified of network congestion or failure through continuous monitoring, allowing them to take preventative measures against data loss. Organizations can guarantee that authorized users have access to data whenever they need it by ensuring its availability.

In conclusion, software-defined WAN's security feature continuous monitoring can assist businesses in meeting the CIA triad principle. Organizations can quickly identify security threats with continuous monitoring's real-time visibility and monitoring of network traffic.

Table 7

Application of CIA Triad Principle on SD-WAN Security Feature

SD-WAN Security Feature	Confidentiality	Integrity	Availability
Application-Aware Firewall	Yes	Yes	Yes
Intrusion Prevention System	Yes	Yes	Yes
URL Filtering	Yes	Yes	Yes
Anti-Virus Protection	Yes	Yes	Yes
Virtual Private Network	Yes	Yes	Yes
Multi-Factor Authentication	Yes	Yes	Yes
Centralized Management	Yes	Yes	Yes
Dynamic Path Selection	No	No	Yes
Continuous Monitoring	Yes	Yes	Yes

Comparative Analysis on Top Three SD-WAN Products (Cisco SD-WAN, Fortinet SD-WAN and VMware SD-WAN)

Three of the most popular SD-WAN solutions on the market are Cisco SD-WAN, Fortinet SD-WAN and VMware SD-WAN. In order to assist businesses in safeguarding their applications and networks from cyber threats, these SD-WAN solutions offer a variety of security features. In this comparison, we will look at their solution's security features and determine how well they protect the network.

Firewall. Considering Cisco SD-WAN, Fortinet SD-WAN VMware SD-WAN, all incorporate an underlying firewall that gives stateful bundle review and access control list (upper leg tendon) usefulness. All solutions' firewalls can be set up to filter traffic based on the IP addresses of the source and destination, protocol type, and port number. An additional layer of security is provided by all of them to block traffic based on the type of application or URL category.

However, Cisco SD-WAN's firewall features are more advanced than VMware SD-WAN's. The application-aware firewall included in Cisco SD-WAN is capable of identifying and blocking specific applications that pose a security risk. The application-aware firewall in Cisco SD-WAN can be set up to use different policies for different applications, giving you complete control over the traffic on the network ("Cisco SD-WAN security configuration guide," 2023).

With a firewall feature set that is more robust and granular, Fortinet SD-WAN offers a security solution that is more comprehensive. Fortinet SD-WAN includes

advanced features like interruption avoidance, web separation, and antivirus security that VMware SD-WAN does not offer.

Table 8

Security Strengths of Firewall used in Each SD-WAN Product

Cisco SD-WAN firewall	**Fortinet SD-WAN firewall.**	**VMware SD-WAN firewall**
Deep packet inspection	Application control	Distributed Architecture
Intrusion prevention	Malware protection	Micro segmentation
URL filtering	SSL inspection	Cloud Integration

VPN. A VPN feature is included in all the three SD-WAN solutions, Cisco SD-WAN, Fortinet and VMware SD-WAN, allowing businesses to establish secure site-to-site connections between their remote sites and the corporate network. All three solutions use IPSec encryption to protect data transmitted over the VPN tunnel, preventing unauthorized third parties from intercepting sensitive information. Flexibility and increased security are provided by the fact that these three solutions can be set up to use various authentication methods, such as RADIUS, digital certificates, or pre-shared keys.

However, Cisco SD-WAN outperforms VMware SD-WAN and Fortinet in terms of VPN features. A secure extensible network (SEN) feature in Cisco SD-WAN enables businesses to securely connect to cloud applications and services. A secure overlay network is used by the SEN feature of Cisco SD-WAN to provide secure connectivity to cloud applications and services. This ensures that data sent to and from the cloud cannot be intercepted by unauthorized parties. Additionally, it supports Dynamic

Multipoint VPN (DMVPN), which provides a mesh-like topology for direct branch office communication and enables multiple branch offices to connect to a single hub.

Comparing VPN in Cisco SD-WAN and VPN in Fortinet SD-WAN, the two solutions differ in a few ways. For instance, Cisco SD-WAN does not have a security fabric that provides integrated security across the network, whereas Fortinet SD-WAN does. Additionally, Fortinet SD-WAN offers UTM capabilities, which provide a comprehensive security strategy that unites a number of security features into a single solution. Similar functionality is not available in Cisco SD-WAN.

Intrusion Prevention. A network intrusion detection and prevention system (IPS) is included in all the three SD-WAN solutions. To identify and block malicious traffic, the IPS in both solutions employ signature-based and behavioral-based methods. Malware, phishing, and distributed denial-of-service (DDoS) attacks are just a few of the traffic types that can be detected and blocked by the IPS in both solutions.

The open-source intrusion detection system Snort serves as the foundation for the intrusion prevention system (IPS) offered by VMware SD-WAN. The IPS uses behavioral analysis to find unknown threats and signature-based detection to find known threats. In addition, it offers a comprehensive security solution with features like threat intelligence feeds, stateful firewalling, and packet inspection. Since the IPS is spread across all SD-WAN nodes, it protects the entire network from threats.

However, Cisco SD-WAN's IPS features are more advanced than VMware SD-WAN's. Cisco SD-WAN incorporates Advanced Malware Protection (ATP) that gives an extra layer of insurance against cutting edge digital dangers. Advanced threats like

zero-day attacks and advanced malware are identified and blocked by the ATP feature in Cisco SD-WAN using machine learning and behavioral analysis. Additionally, the system includes sandboxing capabilities, which enable the execution of suspicious files in a virtual environment for malicious behavior analysis. When ATP is enabled, the IPS automatically sends any suspicious traffic to the ATP engine for further investigation. In order to help stop the spread of malware throughout the network, the ATP engine can block the traffic or quarantine the affected devices if it determines that the traffic is malicious.

Fortinet SD-WAN has a more advanced IPS system with machine learning algorithms and real-time threat intelligence feeds that are able to identify and stop emerging threats. The IPS system for Fortinet SD-WAN can also work with Fortinet's Security Fabric, a complete security solution with advanced threat detection, response, and management capabilities.

Application Visibility and Control. There is an application visibility and control (AVC) feature in Cisco SD-WAN, Fortinet SD-WN and VMware SD-WAN that enables businesses to monitor and control the performance of applications running on the network. Organizations can prioritize or block applications based on their importance or security risk using the AVC feature, which provides visibility into the applications used on the network. This is achieved by Deep packet Inspection and Dynamic Path Selection (“Application steering using SD-WAN rules,” n.d.).

Cisco SD-WAN offers more advanced AVC features than VMware SD-WAN and Fortinet SD-WAN. Cisco SD-WAN incorporates application-mindful directing, which can

naturally control traffic to the ideal way founded on application execution necessities. In Cisco SD-WAN, application-aware routing ensures that even under heavy network loads, critical applications receive the bandwidth and network resources they require to function effectively. Application aware routing is also provided by Fortinet SD-WAN.

Quality of Service. A quality of service (QoS) feature is included in Cisco SD-WAN, Fortinet SD-WAN and VMware SD-WAN to guarantee the consistent and predictable performance of critical network applications. QoS gives traffic a higher priority based on how important an application is. This makes sure that critical applications get the bandwidth and network resources they need to work well.

However, Cisco SD-WAN's QoS features are more advanced than VMware SD-WAN's. Granular QoS policies that can be set up by application, user, location, and network condition are included in Cisco SD-WAN. In Cisco SD-WAN, granular QoS policies ensure that even under heavy network loads, critical applications receive sufficient bandwidth and network resources to function effectively (“Implement QoS in Cisco SD-WAN,” 2018). Cisco SD-WAN's QoS policies can be tailored to meet an organization's specific requirements, offering maximum flexibility and traffic control. Similarly, Fortinet SD-WAN also uses deep packet inspection to prioritize critical applications, does traffic shaping, link load balancing, policy-based routing, etc.

Security Orchestration. Security orchestration features are available in both Cisco SD-WAN, Fortinet SD-WAN and VMware SD-WAN, allowing businesses to automate security procedures and policies. By automating the deployment and configuration of security policies, security orchestration makes security management

simpler, lowers the likelihood of human error, and ensures that security policies are consistently applied throughout the network.

However, Cisco SD-WAN's security orchestration features are more advanced than VMware SD-WAN's. Organizations can automate security policies based on a variety of parameters, including location, user, application, and network condition using the policy-based automation framework that is included in Cisco SD-WAN. Cisco SD-WAN's policy-based automation framework ensures that security policies are dynamically applied in response to changing network conditions, maximizing cyber threat protection.

A Security-Driven Networking strategy is used in Fortinet SD-WAN, which combines security and networking capabilities into a single platform. A security fabric that makes it possible to connect the platform to other Fortinet security products is also included. In contrast, Cisco SD-WAN provides secure connectivity to cloud applications and data centers by utilizing a cloud-first architecture. The platform from Fortinet might be better suited for businesses that need a high level of security, like those in regulated fields like finance or healthcare.

Known Vulnerabilities. Cisco SD-WAN is vulnerable to denial-of-service attacks, remote code execution, and authentication bypass. VMware SD-WAN has vulnerabilities for authentication bypass, command injection, and remote code execution. Fortinet SD-WAN has been accounted for to have weaknesses for arbitrary code execution, XSS attacks, DoS attacks, and MitM attacks (NVD – Vulnerabilities, n.d.).

Table 9

Some of Cisco SD-WAN Vulnerabilities

CVE-2021-1483	An attacker could use this vulnerability to execute arbitrary code with root privileges in the Cisco SD-WAN vContainer. The CVSS (Common Vulnerability Scoring System) score for the vulnerability is 9.8, which indicates that it is a critical vulnerability.
CVE-2020-3375	An unauthenticated attacker could use this vulnerability to execute arbitrary code with root privileges on the Cisco SD-WAN Solution. The CVSS score of 9.8 out of 10 indicates that the vulnerability is critical.
CVE-2020-3266	The Cisco SD-WAN Solution is affected by this flaw, which makes it possible for an authenticated attacker to gain access and run any code they want. The CVSS score of 8.8 out of 10 indicates that the vulnerability is of high severity.
CVE-2019-1652	This weakness influences the vManage online administration point of interaction of Cisco SD-WAN and could permit an unauthenticated aggressor to execute erratic code with root honors. The CVSS score of 9.8 out of 10 indicates that the vulnerability is critical.

Table 10

Some of VMware SD-WAN Vulnerabilities

CVE-2021-21986	This vulnerability affects VMware SD-WAN Orchestrator and could allow an attacker with network access to the administration interface to execute commands with unrestricted privileges. The CVSS (Common Vulnerability Scoring System) score for the vulnerability is 9.1, which indicates that it is a critical vulnerability.
CVE-2021-21987	An unauthenticated attacker with network access to the administration interface could use this VMware SD-WAN Orchestrator vulnerability to upload any file. A CVSS score of 8.1 out of 10 indicates that the vulnerability is of high severity.
CVE-2021-21985	An attacker with network access to the administration interface could use this VMware SD-WAN Orchestrator vulnerability to obtain sensitive information. The CVSS score of 6.5 out of 10 indicates that the vulnerability is of moderate severity.
CVE-2021-21984	An attacker with access to the local network could use this vulnerability to execute arbitrary commands with unrestricted privileges on VMware SD-WAN Edge. The CVSS score of 8.8 out of 10 indicates that the vulnerability is of high severity.

Table 11

Some of Fortinet SD-WAN Vulnerabilities

CVE-2021-32589	FortiManager and FortiAnalyzer are affected by this flaw, which makes it possible for an unauthenticated attacker to use root privileges to run arbitrary commands on the system. The CVSS (Common Vulnerability Scoring System) score for the vulnerability is 9.8, which indicates that it is a critical vulnerability.
CVE-2020-12812	FortiManager and FortiAnalyzer are affected by this flaw, which makes it possible for an adversary with system access to execute arbitrary commands with root privileges. The CVSS score of 7.2 out of 10 indicates that the vulnerability is of high severity.
CVE-2020-29016	FortiAnalyzer is affected by this flaw, which makes it possible for an unauthenticated attacker to execute arbitrary code with root privileges. The CVSS score of 9.8 out of 10 indicates that the vulnerability is critical.
CVE-2019-5591	FortiManager is affected by this flaw, which makes it possible for an adversary with system access to execute arbitrary commands with root privileges. The CVSS score of 8.8 out of 10 indicates that the vulnerability is of high severity.

Cisco SD-WAN has a feature called Trust Anchor that offers devices a secure boot procedure that safeguards their integrity. Trust Anchor gives a protected chain of trust from the equipment to the product, guaranteeing that the gadget's product is liberated from malware or other security dangers. Similar functionality does not exist in Fortinet SD-WAN.

Below is the figure which mentions whether the security feature is present in the SD-WAN product and also mentions whether the security feature is part of inbuilt solution, or it is a third-party solution.

Table 12

Security Features Supported in Top Three SD-WAN Products

Security Feature	Cisco SD-WAN	VMWare SD-WAN	Fortinet SD-WAN
Advanced Threat Protection	Yes (Integrates with third party solutions)	Yes (Integrates with third party solutions)	Yes (Built-in support for FortiGate NGFW)
Zero-Trust Security	Yes (With the help of Cisco TrustSec)	Yes (With the help of VMware NSX-T)	No
Encryption	AES-256 , SSL/TLS, DTLS	AES-256 , SSL/TLS	AES-256 , SSL/TLS
Segmentation	Application-centric	Application-centric	Network-centric
Intrusion Detection /Prevention	Yes (Snort-based IDS/IPS)	Yes (Snort-based IDS/IPS)	Yes (Built-in support for FortiGate NGFW)
Trust Anchor	Yes (Hardware-based)	Yes (Hardware-based)	No
Centralized Management	Yes (Cisco vManage)	Yes (VMware Orchestrator)	No
Firewall	Yes (Zone-based, NGFW)	Yes (Zone-based, NGFW)	Yes (Built-in support for FortiGate NGFW)
Web Filtering	Yes (Integrated with Cisco Umbrella)	No	Yes (Built-in support for FortiGate NGFW)
Anti-Virus/Malware	Yes (Integrated with third party solutions)	Yes (Integrated with third party solutions)	Yes (Built-in support for FortiGate NGFW)
IPSec VPN	Yes(Built-in)	Yes(Built-in)	Yes(Built-in)
SSL VPN	Yes(Built-in)	Yes(Built-in)	Yes(Built-in)

In general, both Fortinet SD-WAN, VMware SD-WAN and Cisco SD-WAN offer a variety of security features that can assist businesses in protecting their applications and networks from cyber threats. However, Cisco SD-WAN offers application-aware firewall, secure extensible network, advanced threat prevention, and granular QoS

policies, which VMware SD-WAN does not. Cisco SD-WAN is a better option for businesses that want a high level of security and flexibility in their SD-WAN solution because of these advanced security features when compared with VMware SD-WAN.

However, Fortinet SD-WAN provides a more complete security solution with more advanced and granular features like SSL inspection, web filtering, and an IPS system that is more advanced. Fortinet SD-WAN's security includes likewise incorporate with Fortinet's Security Texture, which can give extra security highlights like high level danger discovery, reaction, and the executives. While VMware SD-WAN is a magnificent decision for associations searching for a more rearranged and smoothed out SD-WAN arrangement, Fortinet SD-WAN is a stronger and far-reaching answer for associations with more perplexing security prerequisites.

Fortinet SD-WAN takes a more network-centric approach to security, whereas Cisco SD-WAN takes a more application-centric approach. Fortinet SD-WAN divides the network into segments based on network characteristics, whereas Cisco SD-WAN divides the network into segments based on application characteristics. Depending on the specific requirements of a given organization, this distinction may make one solution more suitable for them. The choice between these SD-WANs comes down to the specific needs and priorities of the organization.

Data Analysis

Prominent security features of SD-WAN were shortlisted and explained in detail. Example of different SD-WANs were considered to analyze and explain each security feature. Further CIA triad is applied to each security feature and analyzed whether it

meets CIA triad principle. Security features of top three SD-WAN products in the market are studied and comparative analysis is drawn. Comments on which SD-WAN product is secure than other is provided based on the comparative analysis

Summary

This chapter provides a very good understanding of SD-WAN security strength. Each security feature that is supported by SD-WAN is discussed thoroughly with required details. Elaborate explanation is provided on how each security attribute of SD-WAN makes it more secure. Each security attribute is further analyzed based on CIA triad principle in an in-depth manner. Comparison of these security features between top three SD-WAN products is made. The next chapter describes the results of the study, conclusion, and future work.

Chapter V: Results, Conclusion, and Recommendations

Introduction

This chapter will conclude the paper by providing results of SD-WAN security principles and also provide some recommendations to reader about the possible future work.

Results

All of the questions that were identified during the methodology have been found and addressed below, based on the research that was conducted throughout the study.

1. What are the security benefits of SD-WAN solution?

   This research question is answered under “Security features of SD-WAN” which is first section under “Data-presentation” in chapter IV where the security attributes that will be analyzed in this paper are listed with their definitions.

2. Explain how each security attribute of SD-WAN makes the solution more secure.

   This research question is answered under the same section “Security features of SD-WAN” in Chapter IV with each security attribute as a sub-heading example VPN, IPS, URL filtering, etc.

3. Does each security attribute of SD-WAN meet CIA triad principle?

   This is the question that this research paper mainly focuses on. This research question is answered under “CIA Triad and application of CIA triad principle

on SD-WAN's security features" which is second section under "Data-presentation" in chapter IV with each security attribute as a sub-heading.

4. What are the attributes that were considered to make comparative analysis on SD-WAN products?

   This research question is answered under "Comparative Analysis on top three SD-WAN products (Cisco SD-WAN, Fortinet SD-WAN and VMware SD-WAN)" which is third section under "Data-presentation" in chapter IV. Attributes like security orchestration, known vulnerabilities, firewall, VPN were considered as comparison parameters.

5. What is the result of comparative analysis done on top three SD-WAN products?

   This research questions provides the summary of comparative analysis is provided under the same section "Comparative Analysis on top three SD-WAN products (Cisco SD-WAN, Fortinet SD-WAN and VMware SD-WAN)" in chapter IV which tells about which SD-WAN product is more secure than other based on the analysis done.

Conclusion

This paper discusses about the new emerging WAN technology i.e., SD-WAN. A comparison is drawn between SD-WAN and traditional WAN mentioning various benefits of SD-WAN. By referring various research paper and articles, security posture of SD-WAN is discussed in length and bread of this paper. Security feature of SD-

WAN's purpose, functionality, technical details, its advantages, and application in different SD-WAN products have been discussed extensively.

In this paper, the application of CIA triad principle on each security attribute of SD-WAN is done in an elaborate manner by distinguishing functionality of each security attribute under Confidentiality, Integrity, and Availability. The current top three SD-WAN products in the market are selected to perform comparative analysis based on their security strength. Security parameters of each of this SD-WAN product is studied and a comparison is made. Few comments are made on which SD-WAN product is more secure among the three. This paper will help readers to understand SD-WAN from security point of view and provide a deep dive into each security feature of SD-WAN.

Future Work

This paper mainly focused on security offerings of SD-WAN, its benefits and comparison of SD-WAN products in market. Further research can be done to understand whether SD-WAN is a complete security solution and what are the gaps in the security of SD-WAN solution. It can be further extended to list the measures that can be taken to fill those gaps by usage of third-party devices or software. SD-WAN is an emerging technology and relatively new, which means we are going to see problems or challenges arising down the road. Solutions to overcome these problems is something that researchers can look out for.

References

Advanced threat defense with Aruba SD-branch. (2022). Aruba, A Hewlett Packard Enterprise Company. https://www.securewirelessworks.com/datasheets/TB_Advanced-Threat-Defense-with-Aruba-SD-Branch.pdf

Application steering using SD-WAN rules | *Administration guide*. (n.d.), Fortinet. https://docs.fortinet.com/document/fortigate/7.2.4/administration-guide/125874/application-steering-using-sd-wan-rules

Aruba SD-WAN dynamic path steering with service level agreements. (2019). Aruba, A Hewlett Packard Enterprise Company. https://www.arubanetworks.com/assets/tg/TB_SD-WAN-Dynamic-Path-Steering.pdf

Azhar, I. (2021, November). *Testing of SD-WAN vendors APIs for service providers integration*. https://openrepository.aut.ac.nz/. https://openrepository.aut.ac.nz/bitstream/handle/10292/14259/AzharI.pdf?sequence=3

Bustamante, J. R., & Avila-Pesantez, D. (2021, October). Comparative analysis of cybersecurity mechanisms in SD-WAN architectures: A preliminary results. In *2021 IEEE Engineering International Research Conference* (EIRCON) (pp. 1-4). IEEE.

Cisco SD-WAN security configuration guide, Cisco IOS XE release 17.x -security overview [Cisco SD-WAN]. (2023). Cisco. https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-17/security-book-xe/security-overview.html

Configure SD-WAN remote access (SDRA) with AnyConnect and ISE server. (2022, March 15). Cisco. https://www.cisco.com/c/en/us/support/docs/security/flexvpn/217697-configure-sd-wan-remote-access-sdra-wi.html

Gordeychik, S., & Kolegov, D. (n.d.). SD-WAN threat lLandscape. *Arxiv*. https://arxiv.org/pdf/1811.04583.pdf

Gordeychik, S., Kolegov, D., & Nikolaev, A. (n.d.). SD-WAN internet census. *Arxiv*. https://arxiv.org/. https://arxiv.org/pdf/1808.09027.pdf

Hodges, J. (2019). *Heavy reading's 2019 SD-WAN security survey*. A Custom Research Report Produced for Amdocs, Fortinet, Lavelle Networks, and Nuage Networks. Retrieved October 15,2022, from https://www.amdocs.com/sites/default/files/2021-06/SD-WAN-Security-Survey-Report.pdf

IDC Technology Spotlight. (2019, April). *SD-wan: Security, application experience and operational simplicity drive market growth*. https://www.vology.com/wp-content/uploads/2020/04/V-IDC-SD-WAN.pdf

Implement QoS in Cisco SD-WAN. (2018). Cisco. https://www.cisco.com/c/en/us/support/docs/routers/vedge-router/213408-implement-qos-in-cisco-sd-wan.html

Magic quadrant for SD-WAN. (n.d.). Gartner. https://www.gartner.com/en/documents/4018621

National Institute of Standards and Technology (NIST). (2017). *Security and privacy controls for information systems and organizations*. NIST Special Publication 800-53. Washington, DC: U.S. Department of Commerce.

NSS-labs-SD-WAN-comparative-report-performance. (2018). Fortinet. https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/NSS-Labs-SD-WAN-Comparative-Report-Performance.pdf

NVD - vulnerabilities. (n.d.) NIST. https://nvd.nist.gov/vuln

Ponemon Institute. (2020). *What does a data breach cost?* Digital Guardian. https://www.digitalguardian. com/blog/what-does-data-breach-cost-2020

Ristic, I. (2019). Web application security with SSL/TLS and IPS. In *Bulletproof SSL and TLS: Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications* (pp. 209-234). Apress.

SD-WAN GUI and monitoring enhancements | *New features.* (2023). Fortinet. https://docs.fortinet.com/document/fortigate/6.4.0/new-features/985780/sd-wan-gui-and-monitoring-enhancements

SD-WAN security: A new era of flexibility and individual networks. (2022, August 1). Andersen. https://andersenlab.com/blueprint/what-is-sd-wan-security

SD-WAN solution-Cisco SD-WAN solution overview. (2022). Cisco. https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-sd-wan-sol-overview-cte-en.html

SD-WAN vendors comparison chart. (2022, September 26). Cisco. https://www.cisco.com/c/en/us/products/routers/sd-wan-vendor-comparison.html

Secure SD-WAN. (2023). Fortinet. https://www.fortinet.com/products/sd-wan

Symantec endpoint protection features. (n.d.). Broadcom. https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/

endpoint-protection/all/what-is-v45096464-d43e1648/how-symantec-endpoint-protection-technologies-prot-v97539434-d43e1669.html

The role of SD-WAN in securing the expanding network perimeter. (n.d.). Comcast Business. https://business.comcast.com/community/browse-all/details/the-role-of-sd-wan-in-securing-the-expanding-network-perimeter

The top 5 SD-WAN security benefits for your business, home, vodafone. (2021, April 13). Retrieved October 16, 2022, from https://www.vodafone.com/business/workplace-security/SD-WAN-security

URL filtering (URLF). (2022). NetworkAcademy.Io. https://www.networkacademy.io/ccie-enterprise/sdwan/url-filtering-urlf

Weinberg, N. (2019, October 23). *How IT pros deal with SD-WAN security concerns*. Network World. https://www.networkworld.com/article/3447618/how-to-augment-sd-wan-security-with-intrusion-prevention-anti-virus-utm-and-more.html

What Is URL filtering? (n.d.). Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-url-filtering

Wood, M. (2017, May 25). *Building a secure SD-WAN architecture*. Retrieved October 13, 2022, from https://www.techerati.com/the-stack-archive/cloud/2017/05/25/building-a-secure-sd-wan-architecture/