iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.51475

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

SD-WAN: The Future of Networking

Naveen[1], Abhishek Sharma[2], Neha Ahlawat[3]
B.Tech, Computer Science and Engineering, PDM University

Abstract: ***Software-defined wide area network (SD-WAN) is a networking technology that enables organizations to build secure, high-performance WANs (Wide Area Networks) using software-based controls that provide simplified network management, help businesses offer seamless connectivity to their users in this current world trend of cloud technology and Edge computing. It operates in a centralized manner, allowing for the control of the entire network at once surpassing the limitations of traditional WANs. This paper discusses the SD-WAN technology, including why it was created, its benefits, the components that make up the technology, the challenges associated with its adoption, the security features it offers, and the future of SD-WAN in networking.***

Keywords: ***SD-WAN, SDN, MPLS, SASE, Template, Cloud Technology***

I. INTRODUCTION

Software-defined wide area network (SD-WAN) is one of the cutting-edge technologies, that emerged in the networking industry in around 2014 and can be also considered as a subset of Software-defined networking (SDN). SDN comes with the idea of dividing the control plane and data plane allowing for centralized control of network devices using the software. Traditionally, network devices such as switches and routers had their control plane and data plane integrated into the same hardware device.

SD-WAN takes this concept a step further by focusing specifically on wide area networks (WANs), which are used to connect geographically dispersed locations. Networking devices such as routers, firewalls, and WAN optimization devices were separate devices that performed specific functions within a network. However, with the advent of SD-WAN, these functions can be combined into a single device, providing a more streamlined and efficient approach to network management. It is an overlay network architecture that abstracts the underlying physical network and provides a logical view of the network to the applications and users.

A. Exploring Features of SD-WAN Technology

In traditional WAN (Wide Area Network) it becomes difficult to provide services in today's era of constantly evolving and advancing, and with the rise of technologies like hybrid cloud, multi-cloud, IoT services, and big data, because it uses MPLS (Multiprotocol Label Switching) circuits that don't work on the cloud-centric world. Businesses require a more flexible, scalable, and secure network infrastructure that can handle the demands of bandwidth-intensive applications. They are not designed to provide direct connectivity to these applications. This can result in poor application performance and increased latency and cause management complexity, application-performance unpredictability, and data vulnerability.

However, The SD-WAN model does not exclude the usage of MPLS. It allows businesses to use multiple types of connections, including broadband, LTE, and MPLS, to connect their various locations to the cloud or internet, which makes it flexible.

The initial deployment cost of SD-WAN may be relatively high, but it is more cost-effective compared to traditional and inflexible MPLS circuits over time. SD-WAN provides GUI (Graphical User Interface) based management for the deployment and configuration of devices. The focal point of the management interface is using of templates. Templates define and apply common configuration settings across network infrastructure or to selective sites and devices according to requirements. This reduces the effort and time to manage and also allows administrators to easily add new sites or devices to the network by applying pre-defined configuration templates, that make SD-WAN more efficient and Scalable. Graphical Interface gives the health status of the network in real-time including application performance, security information, and network topology in visual representation.

SD-WAN is designed to be programable, which is made possible by its compatibility with the APIs (Application Programming Interfaces) makes it adaptable to changing business needs, with integration with other systems and applications such as cloud services, security tools, and monitoring systems.

SD-WAN provides Zero Touch provisioning (ZTP) through its centralized management architecture, which enables the addition of new devices to the SD-WAN solution with minimal console and cabling technical requirements. This policy eliminates the need to send an expert to deploy devices, as it automatically configures them, streamlining the process and minimizing the need for on-site support.

©IJRASET: All Rights are Reserved

B. The architecture of SD-WAN

The architecture of SD-WAN is specifically designed to simplify the Wide Area Network (WAN) to meet the demands of modern times. It achieves this by decoupling the network hardware from its control mechanism.

SD-WAN architecture functions as an overlay network, meaning it is built on top of an existing underlay physical network that consists of routers and switches. The key difference is that SD-WAN introduces edge devices at each location to facilitate the control and management of the network.

SD-WAN comprises three key components

1) Edge devices
2) Controller
3) Orchestrator

a) SD-WAN Edge Devices

SD-WAN edge devices serve as endpoint devices that provide secure connectivity between branch offices and data centers or cloud environments. These devices utilize software controls to manage and route data traffic, allowing for the efficient management of multiple network connections, such as MPLS, internet, or cellular networks.

b) SD-WAN Controller

SD-WAN controllers are typically located at headquarters, data centers, or in the cloud. They serve as a centralized management platform that allows network administrators to configure and manage SD-WAN edge devices from a single location which are connected to the controller. It provides Quality of Service (QoS) policies to prioritize network traffic, manage the network topology, and handle IP address management. The SD-WAN controller is responsible for pushing down the policies to the SD-WAN edge devices.

c) SD-WAN Orchestrator

An SD-WAN Orchestrator is a tool that enables network administrators to effectively manage and monitor their SD-WAN infrastructure using a graphical user interface. It provides real-time updates on network performance, including important metrics such as bandwidth utilization, packet loss, and latency. Armed with this information, network administrators can optimize network traffic.

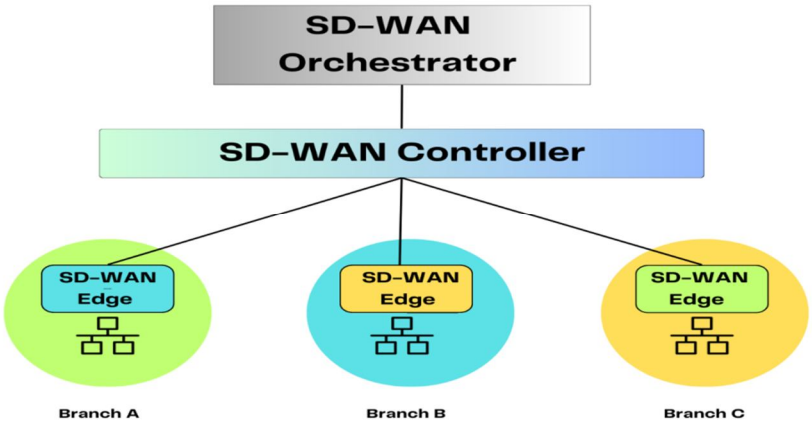


Fig. 1: SD-WAN Components

The figure shows that SD-WAN architecture comprises multiple components, including the SD-WAN Orchestrator, SD-WAN Controllers, and SD-WAN Edge Devices. SD-WAN Orchestrator is at the top, and it communicates with the SD-WAN Controllers that are deployed in the data center or cloud. The SD-WAN Controllers, communicate with the SD-WAN Edge Devices that are installed at each branch

They all communicate with the help of API; Southbound APIs are used for communication between controllers and edge devices. Northbound APIs are utilized for communication between applications and the network infrastructure. Additionally, East-West APIs are used to facilitate communication between the same entities, such as between two controllers.

C. The issue with SD-WAN Solution

SD-WAN is a highly advanced networking technology that provides numerous advantages to enterprises. but deploying and managing it requires specialized skills and expertise, making it necessary to ensure that the team tasked with such responsibilities possesses the requisite skills. Moreover, before implementing SD-WAN, it is crucial to ascertain its compatibility with the existing network infrastructure. This step is vital to avoid any conflicts that could arise between the two systems and to ensure seamless integration SD-WAN employs a centralized controller to manage network operations. This centralized architecture can pose a significant security risk. If the controller is compromised, an attacker could gain complete control over the network and potentially cause significant damage, the attacker could manipulate the traffic flow, steal sensitive data, or even bring down the entire network and the use of the public internet for data transfer makes the network vulnerable to manipulation, data theft, and potential network failure. Thus, it is essential to implement robust security measures to prevent unauthorized access and mitigate any potential security breaches. Ensuring the network's security is crucial to safeguarding sensitive data and maintaining uninterrupted network operations.

D. Ensuring Network Security with SD-WAN Technology

The use of IPsec (Internet Protocol Security), VPN (Virtual Private Network) tunnels, next-generation firewalls (NGFWs), and micro-segmentation of application traffic provides a strong foundation for SD-WAN security.

IPsec-based VPNs are a widely used solution for creating encrypted connections between two endpoints. They can also be employed to establish secure tunnels between Software-Defined Wide Area Network (SD-WAN) edge devices and remote sites, data centers, or cloud services. Although some SD-WAN solutions may use alternative VPN protocols or security mechanisms, such as Secure Sockets Layer/Transport Layer Security (SSL/TLS) or Datagram Transport Layer Security (DTLS), to encrypt traffic and secure connections over the public internet.

Integrating Next-Generation Firewall (NGFW) technology into an SD-WAN solution can significantly enhance security features. An NGFW is a specialized firewall that is designed to protect against modern cyber threats. By incorporating advanced threat detection and prevention capabilities, including intrusion prevention, anti-malware protection, and URL and web content filtering. These features enable the network to identify and block malicious traffic, protect against various forms of cyber-attacks, and ensure secure access to applications. SD-WAN solutions utilize micro-segmentation, which divides the network into smaller segments, each with its own security policy and control. network administrators can create tailored security policies based on specific applications or user groups, and apply those policies to specific network segments. By isolating each network segment from others, unauthorized access can be prevented, and lateral movement of threats can be restricted, which significantly enhances network security.

E. SASE: A Comprehensive Solution

Secure Access Service Edge (SASE) is a revolutionary network security model that was introduced in 2019. SASE integrates both networks (SD-WAN) and security-as-a-service to provide a single comprehensive solution. This new approach to network security provides organizations with a unified and simplified approach to securing their networks, regardless of their location or device type.

SASE use services into a single, cohesive set of functions. These functions include threat protection, data leak prevention (DLP), DNS, Cloud Access Security Broker (CASB), Cloud Secure Web Gateway (SWG), Zero Trust Network Access (ZTNA), Web Application and API Protection as a Service (WAAPaaS), Firewall-as-a-Service (FWaaS), Domain Name System (DNS), and Remote Browser Isolation (RBI).

SD-WAN and SASE are well-suited for edge computing, where low-latency services and real-time data processing are essential. Edge computing is critical for applications such as autonomous vehicles, healthcare monitoring, and industrial automation that require real-time processing. By leveraging SD-WAN and SASE, organizations can securely and efficiently extend their networks to the edge and ensure reliable and fast connectivity for critical applications.

F. SD-WAN in Indian Networking

During the COVID-19 pandemic, businesses in India had to adapt to remote work to ensure the safety of their employees, leading to a surge in demand for SD-WAN solutions. With the need for network connectivity and security for remote employees, SD-WAN proved to be a reliable and effective solution and the recent implementation of 5G technology in India has boosted the demand for SD-WAN solutions. In India, the SD-WAN market is expected to grow at a CAGR of 25.6% between 2020 and 2025. Globally, the SD-WAN market is projected to grow from USD 3.4 billion in 2022 to USD 13.7 billion by 2027, with a CAGR of 31.9% during the forecast period.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

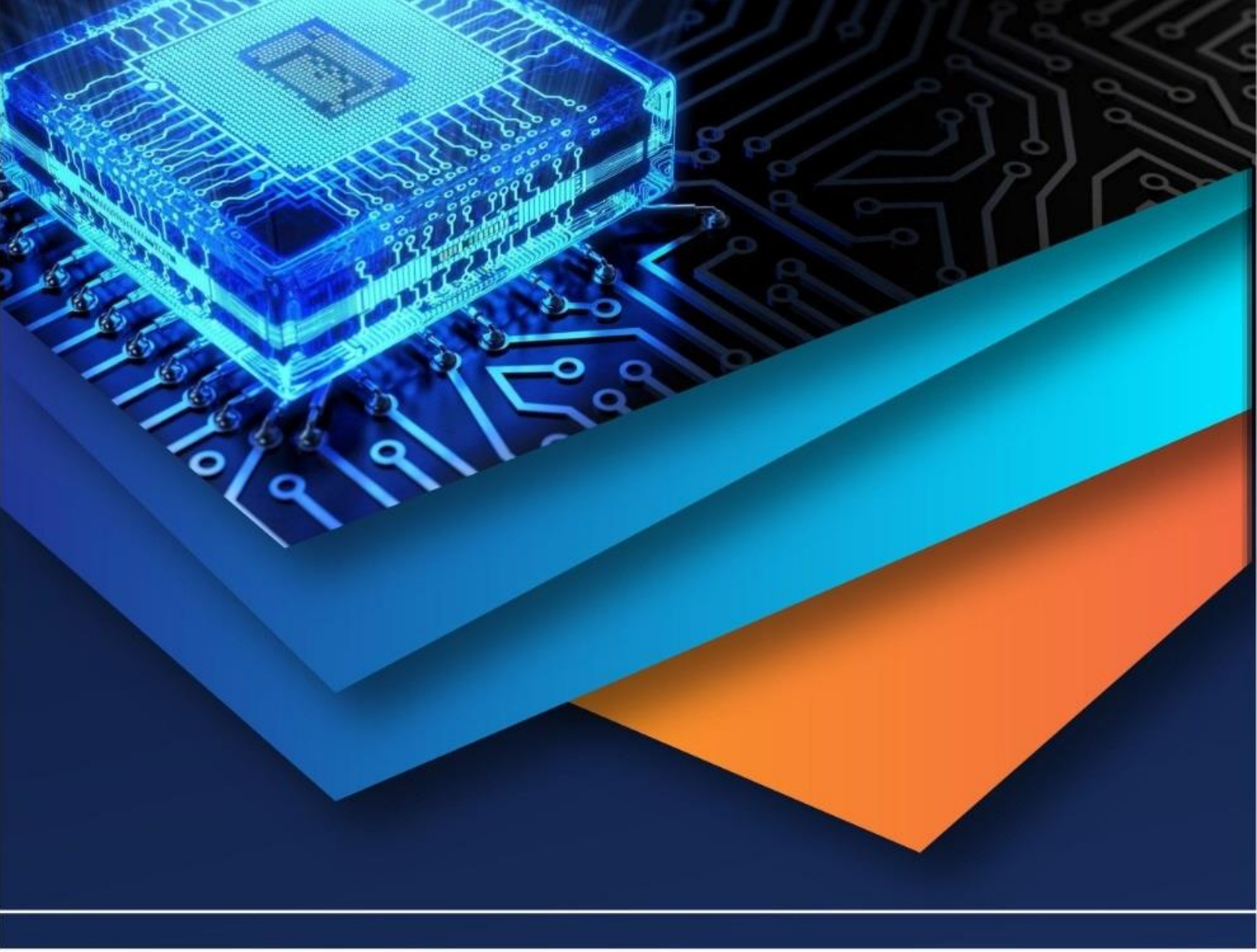
There are several SD-WAN providers available in the market, including Cato, Aryaka, VMware, Versa, Meraki, Fortinet, Forcepoint, Citrix, Barracuda, and many more. Enterprises should carefully evaluate their specific requirements and choose a provider that best meets their needs.

II. CONCLUSION

SD-WAN has great potential to enhance visibility and control over network operations and its centralized and software approach is making it more flexible, cost-efficient, scalable, and speedy. It is an ideal solution for organizations that have complex network requirements or that operate across multiple locations. SD-WAN simplifies the network between different sites but before choosing a vendor organizations should understand what kind of services they want. The challenge of efficiently transmitting data and ensuring swift and uninterrupted data flow can be effectively resolved by implementing SD-WAN technology with robust security measures.

REFERENCES

[1] Catherine Janire Mena Diaz, Laberiano Andrade-Arenas, Javier Gustavo Utrilla Arellano, Miguel Angel Cano Lengua, Analysis about Benefits of Software-Defined Wide Area Network: A New Alternative for WAN Connectivity, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 13, No. 1, 2022
[2] Fatma al deeb, Abdussalam ali ahmed , Software defined wide area network SD-WAN: Principles and architecture,4th international African conference on current studies October 2021
[3] P. Segeč, M. Moravčík, J. Uramová, J. Papán, O. Yeremenko, SD-WAN - architecture, functions and benefits, 18th International Conference on Emerging eLearning Technologies and Applications (ICETA) November 2020
[4] Sumit Badotra and Surya Narayan Panda, A Survey on Software Defined Wide Area Network, International Journal of Applied Science and Engineering 2020. 17, 1: 59-73.
[5] Raphael Horvatha, Dietmar Nedbala, Mark Stieningera, A Literature Review on Challenges and Effects of Software Defined Networking, Conference on ENTERprise Information Systems / International Conference on Project MANagement / Conference on Health and Social Care Information Systems and Technologies, CENTERIS / ProjMAN / HCist 2015 October 7-9, 2015
[6] Pooja Batra Nagpal, Sarika Chaudhary, Naman Verma, Architecture of Software Defined Wide-Area Network: A Review, GRD Journals- Global Research and Development Journal for Engineering, Vol. 5, Issue 6, May 2020.
[7] Ashok Rajendran, Security analysis of a software defined wide area network solution, Degree project in electrical engineering, second cycle, 30 credits Stockholm, Sweden 2016.
[8] What Is SD-WAN? https://www.cisco.com/c/en_in/solutions/enterprise-networks/sd-wan/what-is-sdwan.html
[9] Gartner, "The Future of Security Networks is in the Cloud" August 2019.
[10] What is a software-defined wide area network? SD-WAN's architecture, benefits and security, https://www.sdxcentral.com/networking/sd-wan/definitions/software-defined-sdn-wan/
[11] SD-WAN Benefits, https://www.catonetworks.com/sd-wan/the-way-forward-how-sd-wan-benefits-the-modern-enterprise/
[12] How SD-WAN can simplify your enterprise network, https://timesofindia.indiatimes.com/business/startups/trend-tracking/how-sd-wan-can-simplify-your-enterprise network/articleshow/90250717.cms
[13] Enabling SD-WAN and SASE – An Ideal Edge Computing Use Case, https://www.networkcomputing.com/network-security/enabling-sd-wan-and-sase-%E2%80%93-ideal-edge-computing-use-case
[14] What is SASE? A cloud service that marries SD-WAN with security, https://www.networkworld.com/article/3574014/what-is-sase-a-cloud-service-that-marries-sd-wan-with-security.html
[15] Benefits of SD-WAN such as WAN simplification, lower costs, bandwidth efficiency is driving the SD-WAN market growth., https://www.globenewswire.com/en/news-release/2023/02/14/2607662/0/en/Software-Defined-Wide-Area-Network-SD-WAN-Market-worth-13-7-billion-by-2027-Growing-at-a-CAGR-of-31-9-Report-by-MarketsandMarkets.html#:~:text=14%2C%202023%20(GLOBE%20NEWSWIRE),of%20the%20SD%2DWAN%20market.
[16] India's Growing SD-WAN Market, https://chiefit.me/indias-growing-sd-wan-market/
[17] SD-WAN Solutions in India, https://sourceforge.net/software/sd-wan/india/



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)