

# Moving Towards Advance Security in Networking via SD-WAN

Pooja Rathod<sup>1</sup> Anuj Patel<sup>2</sup> Jigisha Trivedi<sup>3</sup> Kaushal Patel<sup>4</sup> Poonam Sahibani<sup>5</sup>

<sup>1,2,3,4,5</sup>Sardar Patel College of Engineering, India

**Abstract** — In the era of digital transformation most of organization move to the SD-WAN technology for direct connectivity through internet from branch to branch services for cloud and SaaS (Software as a service) applications. SD-WAN (Software Define Wide Area Network) is an emerging technology which combined SDN and WAN together to get better result of network. SD-WAN will able to transfer our business-critical application through high bandwidth and other non-important traffic from low-bandwidth line. Therefor security is the users main concern for their network performance. In this report, the major approaches focused on the basic knowledge of SD-WAN and Research on security needed for SD-WAN.

**Keywords:** SD-WAN - Software Define Wide Area Network, Security, Software as a Service

## I. INTRODUCTION

### A. SDN (Software Defined Networking):

Software defined networking is rise up and effectively discussed as one of the most assuring technologies to make virtually and programmable that simplifies network operations and reduce costs. SDN is the new networking technology which concede centralized, programmable control plane and data plan abstraction, where data and control plane are separated. Network provider need more intelligent control system to directly arrange the behaviour of hundreds of routers and switches. SDN is based on Control Plane and Data Plane.

### B. WAN:

Wide Area Network will cover a broad area which may span across territory and even a whole country. Generally, telecommunication networks are used this technology. WAN provide the connectivity between multiple LANs or MANs and WAN are very expensive network because it will equipped with high speed backbone.

### C. SD-WAN:

Software-Defined Wide Area Network (SD-WAN) is a new armature way to design a Wide Area Network. The network configuration and applications are unique from underlying networking services. As a result, the services will be reconfigured, remove or added without impacting the network. By using of SD-WAN the cost is reduce. MPLS services are very costly because it will use a private leased line between branches for transferring the data. SD-WAN will use the public internet instead of MPLS line. Underlying network services are separated by SD-WAN from applications at high-level. SD-WAN adapts the technologies like intelligent routing algorithms, and others. SD-WAN connects with SaaS application, mobile users and cloud datacentres. SD-WAN routers are placed at the edge of local network and connects to a network services. SD-WAN requires two internet connections. SD-WAN brings the satisfaction to organization in terms of cost saving, availability, agility and performance. SD-WAN makes the

network smart to route the traffic. SD-WAN uses PBR (Policy Based Routing) algorithms and set of preconfigured rules for dynamically selection of tunnels. It is also responsible for balancing the traffic across the network. If there is degradation or outage in one line the SD-wan should moves to alternate line and restores them on initial paths on based on configured policies. SD-WAN were helps us to alignment of WAN to our Business priorities. We can divide our traffic by their priorities, like ad-hoc groups can use 4G/LTE, Small branch office where MPLS lines are not available will be connected with one line. VoIP traffic will be transferred through high bandwidth MPLS lines.

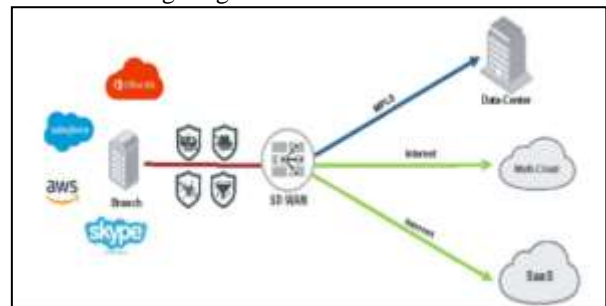


Fig. 1: Software-Defined WAN

## II. ANALYSIS

In today's Hybrid network many vendors like Fortinet, Cisco, Silver Peak, VMware, etc. are claim to provide Secure SD-WAN but it provide security up to traffic protection. Organization still need to protect data against advance security threats, malware infection and data exfiltration which requires advance security technologies like NGFW (Next Generation Firewall), SWG (Secure Web Gateway), and advance threat protection.

## III. IMPLEMENTATION DETAILS

As we know the objective of the project is providing the security for SD-WAN. First we have to learn the network security tool (firewall) because firewall is the only tool which monitor and control the traffic passing from private network to internet or vice versa.

The workflow of an SD-WAN (Software-Defined Wide Area Network) involves the dynamic and intelligent management of network traffic to optimize performance, enhance security, and ensure efficient utilization of available network resources.

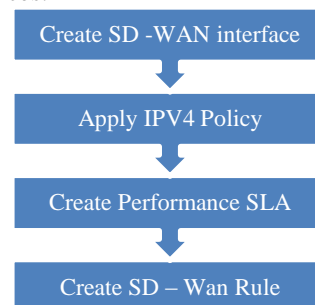


Fig. 2: SD-WAN Workflow

#### IV. TOOLS AND TECHNOLOGY

##### A. Firewall:

It is a Network Security System which has prearranged set of rules for ingress and egress traffic to control and monitor it. Firewalls gives the protection against unauthorized access of untrusted party in Private network. It can be placed in between public network and private network. There are mainly three types of Firewalls used by companies and organizations to protect their data and devices for ruinous elements far from network. Stateful inspection, Packet Filters, and Proxy server Firewalls are the types of it. Let us know this types in deep.

##### B. Stateful Inspection:

It is also known as Dynamic packet filtering. This is the smart and fast firewall which analysing the packet header and observe the packets by adding proxy server to avoid unauthorized traffic in network. It examines the traffic flows end-to-end by using its powerful architecture. This firewalls works at the Network layer of the OSI model and it is more secure than basic packet filtering firewalls.

##### C. Packet Filters:

This firewall examines the incoming and outgoing packets to control the network access. It will be comparing the packets with pre-established set of rules like packet type, allowed IP, port number, etc. This technique is use for only small and simple networks. This type of firewall cannot prevent from all type attacks. It will not give security against spoofing attacks.

##### D. Proxy Server Firewall:

This firewall is also called as application level gateways. It can filter the messages at application layer so it is most secure type of firewall. It gives the security by masking your IP address and limit traffic types. The protocol they support give the complete and protocol awareness security analysis. It improves the performance of the network and provide the best internet experience.

#### V. NGFW (NEXT GENERATION FIREWALL)

A Next-Generation Firewall (NGFW) is an advanced network security solution that combines traditional firewall capabilities with additional features such as intrusion prevention, application awareness and control, and advanced threat protection. NGFWs are designed to provide a more comprehensive and integrated approach to security compared to traditional firewalls. NGFWs are crucial components of modern cybersecurity strategies, providing enhanced protection against a wide range of cyber threats. They play a vital role in securing networks by combining multiple security technologies into a single, integrated solution.

Interface	Gateway	Cost
ARTEL_BRI(part1)	30.30.30.1	0
ARTEL_BRI(part2)	30.30.30.1	0
WAN_INTERNET_ARTEL(iswd1)	192.79.250.57	0
TATA_KL(iswd2)	1498.188.253	0

Fig. 3: SD-WAN Interfaces Member

#### VI. PROPOSED MODEL

SD-WAN uses the PBR (Policy Based Routing) algorithm for transferring and receiving the traffic. The algorithm will be explaining in detail. As we know that the objective of the project (Secure SD-WAN) is providing the security for Software-Defined WAN. To achieve this as per Gartner research there are four different options for securing SD-WAN:

- SD-WAN with Embedded Firewall
- Firewall with Embedded SD-WAN
- SD-WAN with 3rd party firewall
- SD-WAN with cloud based security

This key options are used to designing and operating the Software-Defined WAN, there are many vendors which evolve with range of security capabilities. All vendors are focuses more on Layer 3 security, or firewall functions. Now we will see all four options one-by-one in detail in next section.

##### A. SD-WAN with Embedded Firewall:

This firewall is same as a stateful firewall which you can see at branch offices. It will use for smaller branch office which has noncritical activities. As we see it was used by smaller branches the relative cost is less than other system. It vendors for this types are Citrix, CloudGenix, Silver Peak, VeloCloud.as use for larger branch and which has more critical activities. The cost is probably high. The vendors which provides this types of security is barracuda network, cisco Meraki, Fortinet. The security in this architecture is very high.

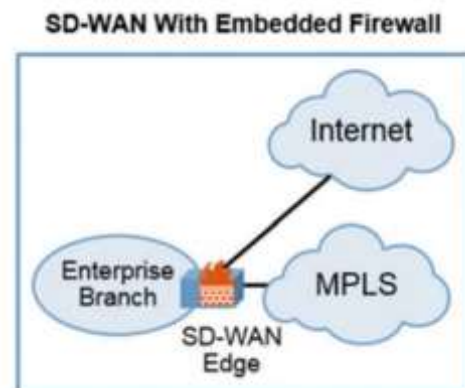


Fig. 4: Firewall with Embedded SD-WAN

### B. SD-WAN with Third-Party Firewall:

Combining a firewall with embedded Software-Defined Wide Area Network (SD-WAN) capabilities is a strategy that many organizations adopt to enhance both their network security and optimize their wide area network connectivity. When considering a firewall with embedded SD-WAN, it's essential to evaluate the specific features and capabilities of the solution to ensure it aligns with the organization's security and network optimization requirements. This integrated approach can contribute to a more efficient and secure network infrastructure.

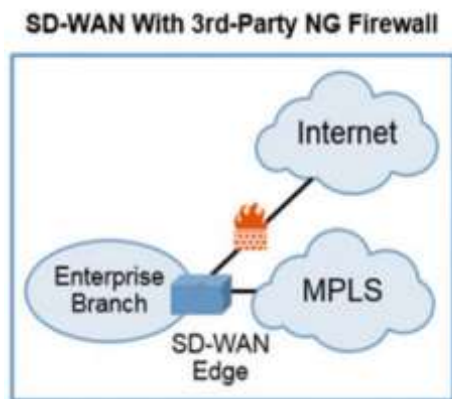


Fig. 5: SD-WAN with 3rd Party firewall

### C. SD-WAN with Cloud Based Security:

The integration of SD-WAN (Software-Defined Wide Area Network) with cloud-based security services is a powerful combination that addresses the needs of modern distributed and cloud-centric networks. It was use for small remote branch office with noncritical activities. The cost is half of the other architectures. Security level is better than stateful firewalls. The sample vendors are Symantec, Zsc

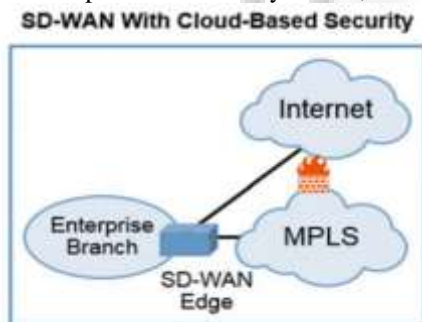


Fig. 6: SD-WAN with cloud-based security

## VII. CONCLUSION

Traditional Networks will use the MPLS technology for connecting their branches to each other which are too costly. This technology was replaced by the emerging SDN technology merging with WAN. By using SD-WAN we can transfer our traffic through the public internet 4G/LTE, so all the traffic is passing via insecure channel. SD-WAN will reduce the cost. By using this we can monitor and control the traffic from one placed and also provide the feature like we can send our high bandwidth usage application to high bandwidth with low latency and expensive line and low bandwidth application from low bandwidth with High latency and less-expensive line.

By using SD-WAN we can reduce the cost and increase the network operations but security is the main concern. We have include the advanced security features like Intrusion prevention, SSL- inspection, anti-malware and much more. At last we can conclude that SD-WAN will provide by many vendors but it need some advanced security features for better network performance and provide the Secure SD-WAN to the organization.

## REFERENCES

- [1] Shin, M. K., Nam, K. H., & Kim, H. J. (2012, October). Software-defined networking (SDN): A reference architecture and open APIs. In 2012 International Conference on ICT Convergence (ICTC) (pp. 360-361). IEEE.
- [2] Christensson, P. (2006). WAN Definition. Retrieved 2019, Nov 21, from <https://techterms.com>
- [3] Michel, O., & Keller, E. (2017, May). SDN in wide-area networks: A survey. In 2017 Fourth International Conference on Software Defined Systems (SDS) (pp. 37-42). IEEE.
- [4] Glenda, M. (2017). Secure SD-WAN: Integrated NGFW Security with WAN Transformation. Gartner.
- [5] Singh, Naresh. "Fortinet Secure SD-WAN: Best-of-Breed NGFW and SD-WAN in a Single Offering." Gartner, November 12, 2018.
- [6] FORTINET. "Upgrade Branch Infrastructures with Fortinet Secure SD-WAN." FORTINET, March 22, 2019. <https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-fortinet-sd-wan.pdf>
- [7] Sezer, Sakir, Sandra Scott-Hayward, Pushpinder Chouhan, Barbara Fraser, David Lake, Jim Finnegan, Niel Viljoen, Marc Miller, and Navneet Rao. "Are We Ready for SDN? Implementation Challenges for Software-Defined Networks." IEEE Communications Magazine 51, <https://doi.org/10.1109/MCOM.2013.6553676>
- [8] Chen, L., Qiu, M., & Xiong, J. (2015, November). An sdn-based fabric for flexible data-center networks. In 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing (pp. 121-126). IEEE.