IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 11, November 2021

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

| Volume 10, Issue 11, November 2021 ||

| DOI:10.15680/IJIRSET.2021.1011081|

Software-Defined Wide-Area Network (SD-WAN) Implementation in Service Provider Network

Bhagyashri Jadhav Dr. V. R. Gosavi, Ms. Manju D. Pawar

P.G. Student, Department of Electronics and Telecommunication Engineering, Maharashtra Institute of Technology, Aurangabad, India

Assistant Professor, Department of Electronics and Telecommunication Engineering, Maharashtra Institute of Technology, Aurangabad, India

ABSTRACT: This paper gives us comprehensive performance analysis of software defined wide area network SDWAN and MPLS network. We have analysis these two on basis of network performance check and network security in the network with the help of graphical view and CLI command line interface. Results obtain in these testing shows how service provider can befit from SDWAN services with increasing network security and additional benefits obtain from SDWAN.The main objective of this thesis was to develop an understanding of the nature of SDWAN technology. The SDWAN technology is described briefly, and a network scenario is illustrated to examine the different communication protocols.

KEYWORDS: software-defined wide-area network, Internet Protocol, Multiprotocol Label Switching, Virtual Private Network, Border gateway protocol, Transmission Control Protocol

I. INTRODUCTION

A software-defined wide-area network (SD-WAN) uses software-defined network technology such as communicating over the Internet using encryption between an organization's locations. If standard tunnel setup and configuration messages are supported by all of the network hardware vendors, SD-WAN simplifies the management and operation of a WAN by decoupling the networking hardware from its control mechanism. This concept is similar to how software-defined networking implements virtualization technology to improve data centre management and operation. In practice, proprietary protocols like Cisco IoS are used to set up and manage an SD-WAN, meaning no decoupling of the hardware and its control mechanism A key application of SD-WAN is to allow companies to build higherperformance WANs using lower-cost and commercially available Internet access, enabling businesses to partially or wholly replace more expensive private WAN connection technologies such as MPLS. However, since the SD-WAN traffic is carried over the Internet, there are no end-to-end performance guarantees. Carriers MPLS VPN WAN services are not carried as Internet traffic, but rather over carefully-controlled carrier capacity, and do come with an end-to-end performance guarantee.

SD-WAN is a disruptive and a transformative technology approach to designing and deploying enterprise WANs. It leverages principles of software defined networking and network functions virtualization for enabling the enterprise transformation to a hybrid wan network. The goal is to create a framework for helping enterprise make a seamless transition to hybrid networking. Tata Communications has chosen versa as the vendor of choice for providing SDWAN based services. The SDWAN solution architecture consist of a central infrastructure that controls and orchestrates the policies deployed at all the enterprise CPEs from a central location.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

| Volume 10, Issue 11, November 2021 ||

| DOI:10.15680/IJIRSET.2021.1011081|

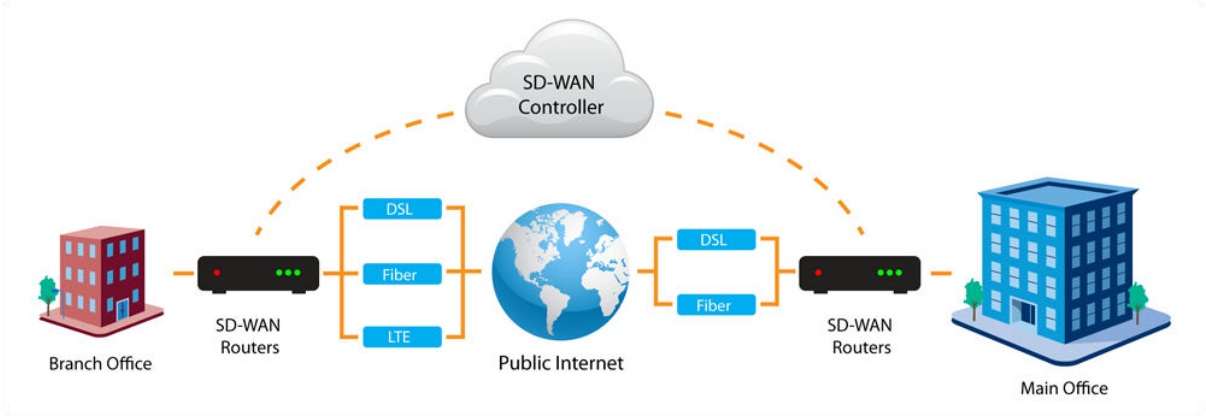

Figure1. SDWAN setup

As one can recognize from the diagram above, the enterprise WAN network is transitioning from a single private network to a hybrid combination of multiple networks with varying characteristics. This is resulting in skyrocketing complexities in the enterprise wan edge, given the stringent application requirements, and the underlying vagaries of the individual networks that form the enterprise wan network. The WAN edge should now become more and more intelligent and this results in increased complexity. The SDWAN vendors have tried to capture this requirement and are focusing their innovation in enabling the hybrid transformation. They have customized the various underlying network protocols such as BGP, OSPF, IPSec etc., and have written extensions for catering to the requirements of hybrid networking.

II. VERSA SD-WAN ARCHITECTURE

Versa SDWAN architecture consists of different components each with different functions which are connected to form a SDWAN ecosystem. The Versa SDWAN Architecture consists of the following building blocks.

- Versa Director
- Versa Controller
- Versa Analytics Nodes
- SDWAN CPE

A. Versa Director

Versa Director is the centralized orchestrator that manages and controls the CPE that are called as Flex VNFs. The key features of the Versa Director are listed below.

- Centralized Policy Management & Enforcement
- Network Overlay Support
- Role Based Access Control
- Service Orchestration
- Rest APIs
- Various Subscription plans for customers
- Hierarchical Multi-tenancy
- Operations & Management
- Device Monitoring
- Security Monitoring

Multiple sites or branches that use a similar set of configurations are templatizedusing the Versa Director Templating engine. Templates can then be used to build a generic configuration that can be applied to one or more FlexVNF CPEs. Versa Director also automates the discovery of a new branch deployment and configuration via pre-provisioned templates. The versa director also serves as a platform for converting the complex protocol and network level configurations into a standard set of generic rules using a combination of variable and fixed protocol parameter configuration. The per site parameters can then be fed separately via specific site parameter list.

B. Versa Controller

Versa Controller provides a control plane entry point for the branch nodes. The Controller authenticates the branch FlexVNF CPEs using specific parameters as part of the IKE exchange. The secure channel established using IKE

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

| Volume 10, Issue 11, November 2021 ||

| DOI:10.15680/IJIRSET.2021.1011081|

provides transport between branch node and all core nodes including the SDWAN Controller, SDWAN Director and Versa Analytics. Versa Controller serves as a Contact point for the overlay WAN network. Versa Controller also enables secure IPSec connectivity between branches without the overhead of maintaining a mesh of IKE-based connectivity per branch. The Versa Controller uses a custom route reflector to provide route and Security Association information to the branch nodes in the network group.

C. Versa Analytics

SDWAN Analytics analyses logs, events and provides reports, analytics and orchestration capabilities. It supports historical and real-time data reporting for Application usage based on total sessions, volume, bandwidth, Application performance based on latency, jitter, packet loss and Branch-to-branch access circuit performance. Analytics data can be filtered by branch, site, and application type and application category. SDWAN Analytics works in conjunction with the SDWAN Controller to report application usage and performance across branches and to the data centre. Analytics data may be leveraged by the SDWAN controller to dynamically enforce policies or modify routing when application SLAs or performance requirements are not met.

D. Versa CPE

Versa CPE is the actual branch node. The Versa CPE establishes contact with the SDWAN controller over secure channel. When the Versa CPE boots up it contacts the controller using a custom IKE protocol, and this results in the production of a data plane tunnel that is dynamically setup with the Controller. Once this is setup, the CPE then sets up custom extensions of BGP protocol with the Versa Controller. The BGP extensions provide the IPSec SAs, routes, topology and other SDWAN metrics for setting up the SDWAN Overlay in accordance with the enterprise policies. Once the overlay is setup based on enterprise application policies various applications can be mapped to the various overlays based on the SLA requirements and the real-time performance of the overlay.

III. SYSTEM DEVELOPMENT

Versa industry-leading SD-WAN offers an extensive list of capabilities including sub-second packet steering across multiple WAN interface, packet loss reduction through services such as FEC, packet replication, and poor performing link avoidance**.**Versa SD-WAN also acts as a DNS Proxy with SD-WAN Traffic steering, MP-BGP route exchange with SDN controller, Stateful high-availability, link aggregation, hierarchical QoS, per tunnel QoS, and overlay encapsulation options (VXLAN, IPSec).Versa secure SD-WAN technology differentiates from pure play SD-WAN vendors by implementing capabilities that enable a seamless SASE architecture. This includes visibility into traffic traversing the network between users, applications, and devices regardless of their location.

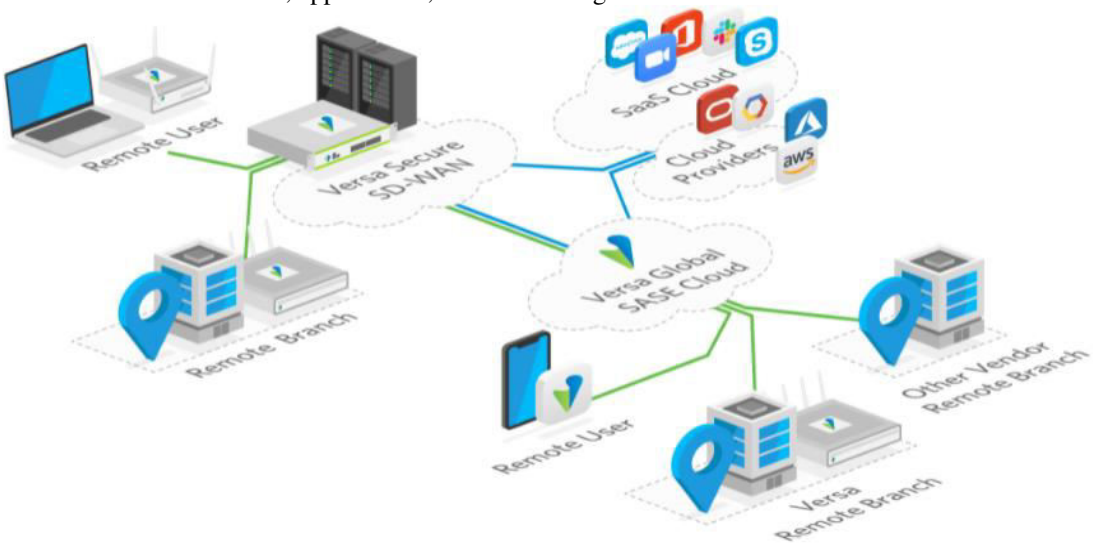

Figure 2. Overview of SDWAN

A. SDWAN Infrastructure Design:

For hosting the SDWAN Command Center (Versa Director, Versa Controller and Versa Analytics), we have identified two locations in India to have redundancy. Chennai is identified as Primary site and Mumbai is identified as Backup site. Both Primary and Backup VMs will be hosted in the IZO Private Cloud. The Versa infrastructure at Chennai and

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

| Volume 10, Issue 11, November 2021 ||

| DOI:10.15680/IJIRSET.2021.1011081|

Mumbai will communicate each other over GVPN network. We will have separate VMs hosted in the IZO Private Cloud for each of the components in the SDWAN centralized infrastructure. These separate components are connected behind the Threat Management System which comprises of firewall, IDS, IPS, etc. for security protection of the infrastructure. This will be connected to the GVPN and ILL cloud for accessing the SDWAN edge nodes, which can be part of different customer networks.

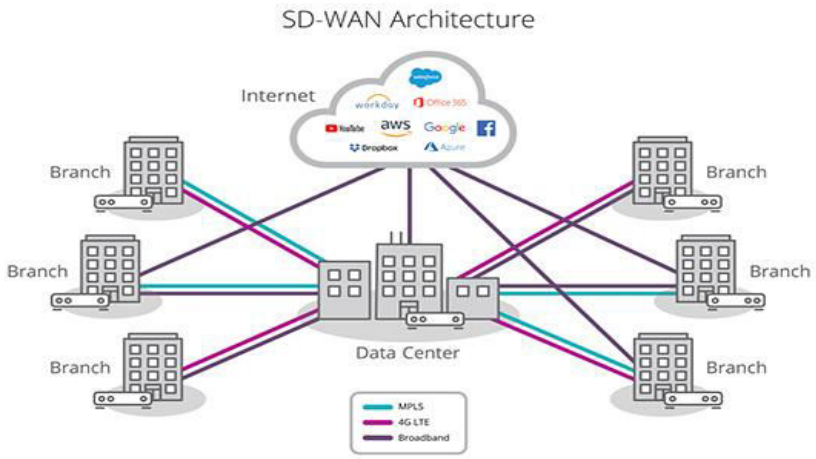

Figure 3.SDWAN Infrastructure Design

B. SDWAN Traffic Flow

This section focuses on the basic SDWAN traffic flow and various use cases with traffic flows in different scenarios.The SDWAN deployment consists of various deployment models and there are different traffic flow scenarios for each deployment model. The below sections describe the various scenarios in detail.

- As you note from the diagram above a typical enterprise network will consist of a combination of Versa CPEs and Cisco CPEs.
- All Versa CPEs will automatically setup an IKE connection to the centralized SDWAN Controller.
- This dynamic IKE session will give rise to a dynamic data plane tunnel in both the versa CPE and the Controller.
- The Versa CPE will then setup a BGP Session with Versa proprietary extensions with the controller.
- This BGP session will then download the topology, encryption and other overlay parameters depending on the policies setup in the orchestrator.
- This will in turn result in overlay data plane sessions between the versa CPEs.
- The traffic between Versa CPEs in the same cloud will pass directly, while the traffic between the Versa CPEs in the different cloud [between VPN and ILL] will passthrough as Versa HUB site or a Versa Service Gateway depending on a particular customer solution. This has been highlighted in the subsequent sections.
- Versa Controller which is the control plane for all the versa branch nodes, act like a Route Reflector, to which all the branch nodes advertise its routes, overlay parameters and in turn the controller advertises the routes and route updates to all the branches.
- Based on the connectivity topology, there is also an IPSec tunnel between the branches through which the communication between the branches will happen directly in a secure mode. The Versa CPEs also setup SLA measurement sessions between the overlay tunnels depending on the topology.

IV. TRADITIONAL IP BASED MPLS NETWORK

Multiprotocol Label Switching is a protocol that integrates Layer 2 information regarding network links (For example, bandwidth, latency, utilization) into layer 3 (IP) within the network which helps to improve and simplify the exchange of IP packets.

The basic concept of MPLS is to speed up the delivery of packets by assigning the packets to the particular FEC just once. Here LERs mark the packets with the same destination with labels. These labels' values are distributed to the other LSRs using Label Distribution Protocol (LDP), Resource Reservation Protocol (RSPP), Constraint-Based Routed LDP (CRLDP) and Multiprotocol BGP by Label Edge Routers (LSRs).N Before packets enter into the MPLS domain network; Label Edge Routers (LSRs) classify IP packets into Forwarding Equivalence Class (FEC). FEC is identified

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

| Volume 10, Issue 11, November 2021 ||

| DOI:10.15680/IJIRSET.2021.1011081|

by the fixed short length value known as a label. Then Ingress LSRs assign MPLS headers to the IP packets. After the MPLS is assigned, the packets are routed through the predetermined Label Switch Path (LSP) by intermediate LSR. Subsequent routers use this label to forward the packets. Therefore, packet classification is not necessary for subsequent routers. The FEC table present in the routers helps to identify the incoming packet label. After the packets label is identified, it is replaced with the outgoing label and transferred to the next LSR. Due to the fixed length of the label, the forwarding operation is much faster than IP forwarding that requires the longest prefix match of destination IP address. When the packet reaches thedestination router, i.e., Egress LSR, the label is removed and forwarded as an IP packet to the destination address.

A. MPLS header

The MPLS header consists of 32 bits. The first 20 bits are specified as label bits. The middle Experimental 3 bits are used to define a class of service (COS) by Cisco. The Bottom of Stack (BOS) bit is used to determine the last label in the packet. The bit 1 means the last label. And the last 8 bits are used as time to live (TTL).

Figure 4. MPLS header

B. Label Stacking

The MPLS router sometimes needs more than one label on top of the packet to travel through the MPLS network that is done by packing the labels into the stack. The first label is called top label, and the last one is called bottom label. There might be a number of labels in between the first and the bottom. The graphical view of the label stack is shown in below fig.

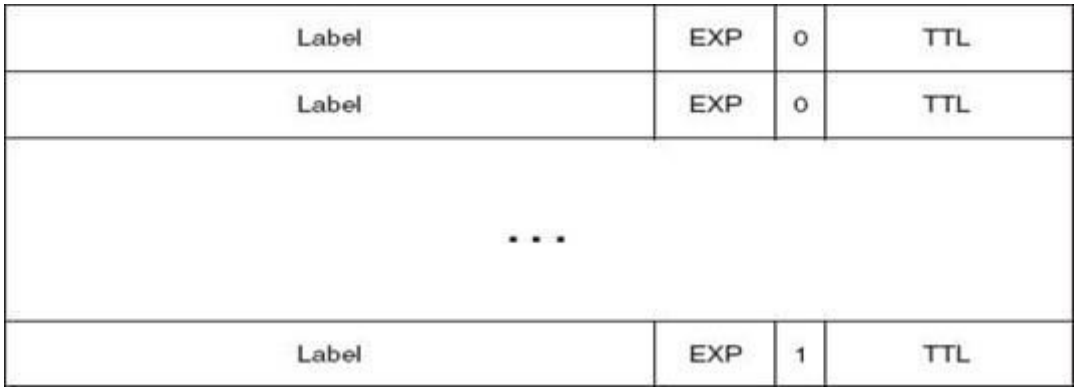

Figure 5. Label Stacks [5]

C. Control Plane and Forwarding Plane

Control Plane and Forwarding Plane are the part of router architecture. Control Plane collects the information that is used to forward the incoming packets. While Forwarding Plane decides how to switch the incoming packets after being received at inbound interface. You need to write an introductory sentence here

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

| Volume 10, Issue 11, November 2021 ||

| DOI:10.15680/IJIRSET.2021.1011081|

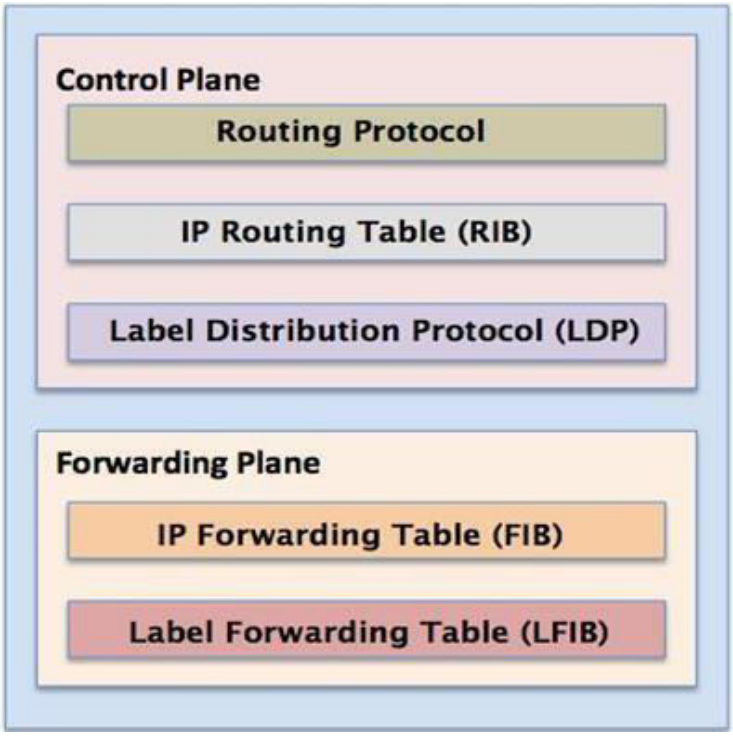

Figure 6. Control Plane and Forwarding Plane

- Control Plane
  The Control Plane exchanges routing information and labels with the adjacent routers. Routing Information is advertised to any of the routers in the MPLS domain whereas label binding information is advertised to only adjacent routers by link-state routing protocols. It consists of two types of protocols namely routing protocols (e.g., RIP, EIGRP, OSPF, and BGP) and label exchange information protocols (e.g., LDP, TDP, RSVP, etc.).
- Data Plane
  Data Plane has a forwarding plane that is based on the information attached to labels. There are two types of tables, namely LIB and LFIB. Label Forwarding Information Base (LFIB) is used by the data plane to forward the labelled packets. The Local Information Base (LIB) table contains all the local labels and the mapping of the labels which is received from the adjacent routers. The information in LFIB and label value is used by the MPLS-enabled routers to make forwarding decisions.

V. PERFORMANCE ANALYSIS OF SYSTEM

Software defined WAN was first implemented through Versa Director and MPLS also implemented, and explained command output in command line interface CLI mode on putty software. This chapter discusses the results that are obtained after the end of studying SDWAN and MPLS networks. Now in this section we will explain performance results of SDWAN network are better than MPLS network. There are several reasons for SDWAN's market momentum, but the considerations are that SDWAN provides enterprise customers with a programmable, evaluable and lower -cost alternative to multiprotocol label switching (MPLS). While for communication service providers CSP's SDWAN enables new revenue streams and empowers service differentiation in a mature enterprise marketplace. SDWAN also allows CSP's to target new market segments, including on-net and off-net customers in new geographic market where traditional cost structures have thwarted network deployments.

However, SDWAN is still very much an emerging technology, which means that multiple implementation and monetization questions remain outstanding. Accordingly, the purpose of this paper is to detail the technical factors that must be addressed to achieve a successful SDWAN implementation. Areas relevant to the discussion include security, orchestration, integration, network management and their linkage to customer requirements. Ping is a basic Internet program that allows a user to verify that a particular IP address exists and can accept requests.Our focus of this paper is to analyse network behaviour in congestion with different traffic flows. We test SDWAN networkand MPLS based network on the basis of two factors network performance check and Network Security.

A. SDWAN business, technical drivers and network performance check

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

| Volume 10, Issue 11, November 2021 ||

| DOI:10.15680/IJIRSET.2021.1011081|

As noted, SDWAN's flexible, programmable design methodology represents a strong value proposition, enabling a cogent mix of technical and business drivers. Thesedrivers in many respects generically embody the criteria that CSP's have defined for accessing successful cloud deployments. They are multi-layer, address security requirements of cloud connections, rapid deployment requirements, application enablement, as well as supporting the introduction of lower-cost self-care operational model. Consequently, as shown in below figure, CSP input confirms that SDWAN is strongly aligned with the criteria for cloud success on many levels. The top two drivers –opex and capex reduction –are not surprising; as they pragmatically reflect an industry-wide consensus that bandwidth growth will demand new business and technical models to most effective monetize the cloud.

Since SDWAN supports the ability to offload traffic to the internet, the cycle of capex- heavy core capacity upgrades is reduced or eliminated. Similarly, SDWAN can significantly reduce opex by leveraging programmability traits to enable zero-touch provisioning, which eliminates truck rolls by using customer self-care portals, centralized policy management and real time analytics.

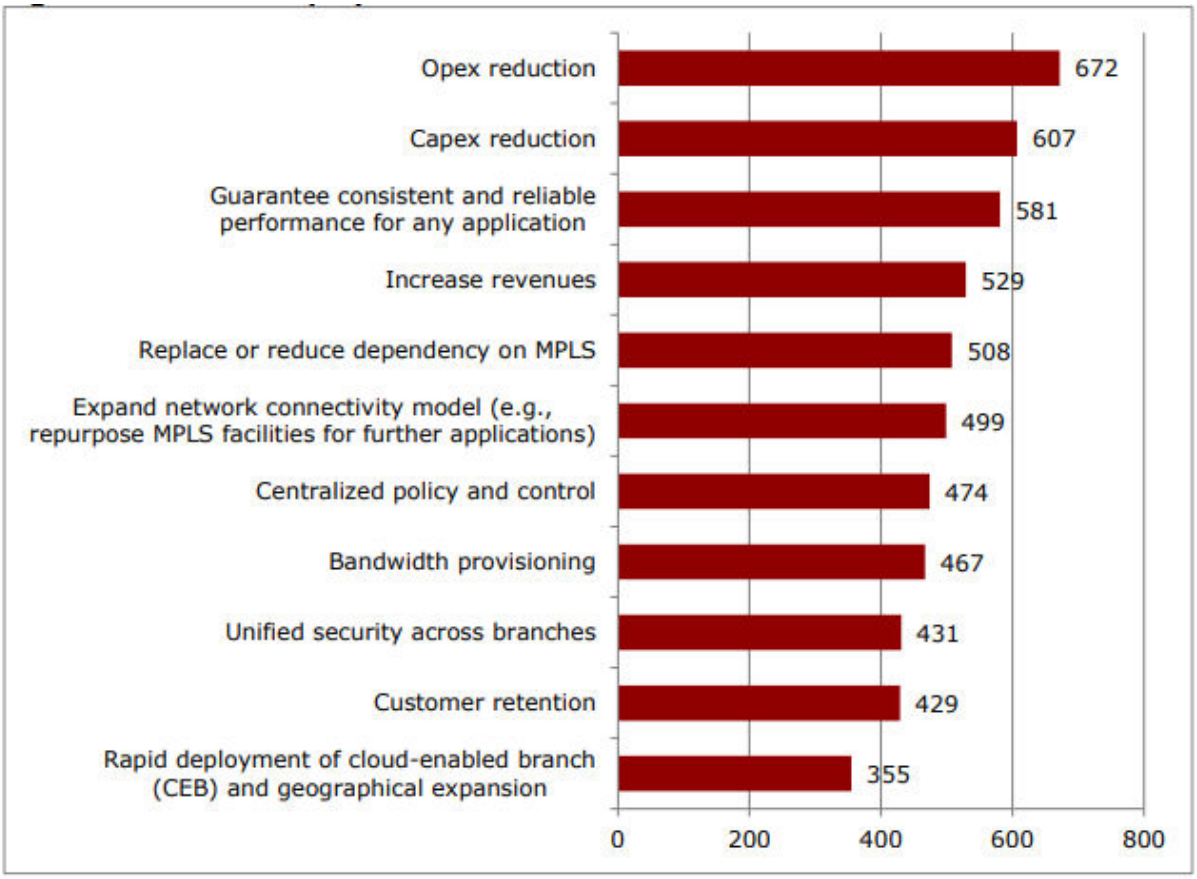

Figure 7. SDWAN deployment drivers

In addition to these two drivers, CSPs also rank other factors highly. For example, the third place ranking of "Guarantee consistent and reliable performance for any application" is a strong endorsement that, with SDWAN, enterprises can still achieve the benefits of MPLS for those applications requiring it, but also leverage dedicated internet access DIA or standard broadband for internet traffic and cloud applications.

One such use case is virtual customer premises equipment vCPE, which is also driven by the need to achieve service innovation at lower price points, without sacrificing business continuity and carrier-grade reliability. Thus is many cases vCPE and SDWAN initiatives are happening simultaneously, to enable CSPs to leverage the power of the distributed model and maximize investment return. However, the scoring of other features highlighted in the figure shows that strategic and adjacent key attributes are also driving SDWAN deployment. These include.

- Replace or reduce dependency on MPLS
- Centralized policy and control

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

| Volume 10, Issue 11, November 2021 ||

| DOI:10.15680/IJIRSET.2021.1011081|

- Unified Security across branches

B Network Security

In order to shed additional light on the relationship between SD-WAN and security, this section of the white paper considers SD-WAN security requirements on a more granularlevel, as well as the opportunities for CSPs to leverage security to achieve market differentiation.As a starting point, it's important to clarify that security is not simply an SD-WAN issue, but rather a crucial topic that must be addressed for any NFV-based cloud implementation. For example, as shown in Figure 10, in the context of the importance of various virtualized network functions (VNFS), CSPS identify security services as their top priority.

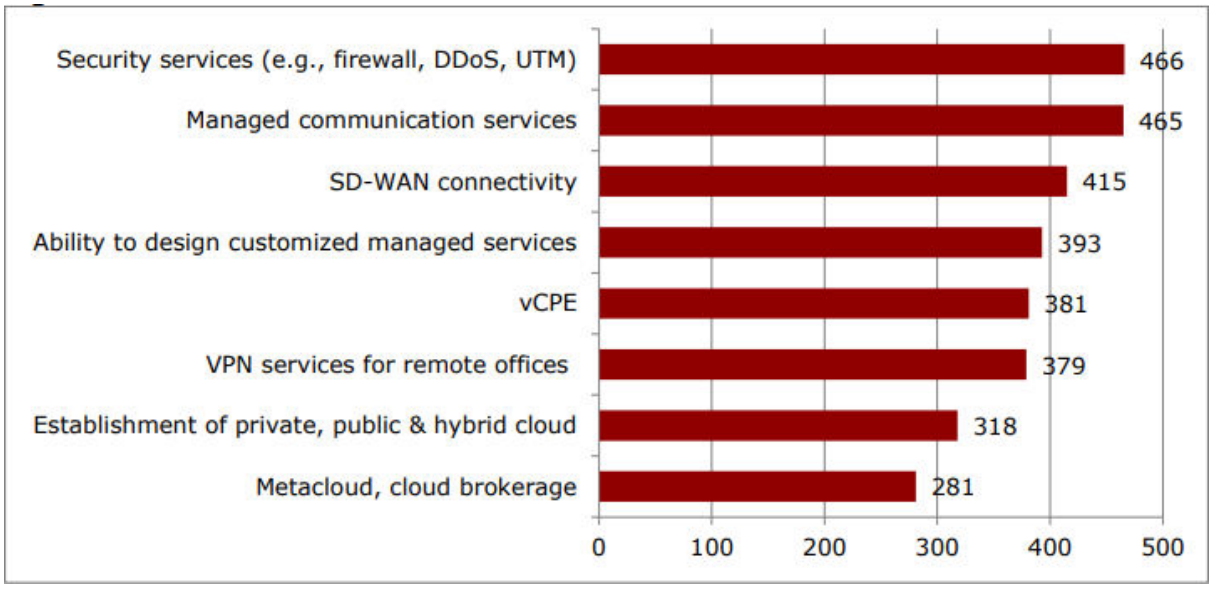

Figure 8 Network Security

The top four inputs reinforce the strong level of interplay between virtualization and security services from the perspective of both service differentiation and network requirements. Stated another way, the responses show that SD-WAN is redefining both network design and the managed services delivery model.There are several factors to consider here.

First, while security is a well-documented factor for all VNFA,SD-WAN introduces new security demands. One of the leading factors is that MPLS security is very different from securing the SD-WAN. For example, MPLS networks do not typically support encryption, since the network is provisioned to emulate a private network connection, and is therefore assumed to be secure.

In contrast, as a purely software-based implementation, SD-WAN require encryption to ensure secure access. Thus, several new technical requirements are introduced, since SD WAN connects some branch offices directly to the Internet. This includes integrating security policies into software while simultaneously maintaining the programmability and automation that SD-WAN delivers.

VI. CONCLUSION

The main objective of the paper is implementation of software defined wide area network.

The rise to prominence of SD-WAN can be attributed to several factors. First and foremost, as documented, SD-WAN empowers CSPS to achieve service differentiation on all network layers: the service layer, the orchestration layer, the policy control and analytics layer, the OSS layer and even the NFVI layer. In addition, SD-WAN's ability to deliver a programmable template that is capable of meeting future service requirements is a chief consideration.Given these traits, SD-WAN will continue to represent a strong value proposition, ensuring that future waves of service innovation and differentiation can be achieved holistically, on all network layers, irrespective of how these layers are redefined in the future.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

| Volume 10, Issue 11, November 2021 ||

| DOI:10.15680/IJIRSET.2021.1011081|

In this paper we have explained performance results of SDWAN network are better than MPLS network.This analysis is made by focusing on the SDWAN statistics: Network performance check, Network security. We have identified the challenges in SDWAN network and MPLS network. During our research, we have also examined the SDWAN architecture and found out that this architecture is scalable and flexible enough to provide well-organized packet transmission, load balancing, consistency, data security, network isolation from other networks and end-to-end controlled connectivity with QoS guaranteed.

A. Advantages

1. Improves performance:
2. Boosts security.
3. Enables cloud usage
4. Reduces costs

B Future Scope

SD-WAN has gained strong market momentum due to its ability to elegantly extend the software-defined model to many network layers- thus enabling CSPS to achieve service differentiation on multiple layers, as well. This is unlikely to change as SD-WAN matures and the issues previously noted, such as interoperability, OSS Sintegration and orchestration, diminish in impact. Still, given that the software world is by nature extremely fluid, SD-WAN requirements will continue to evalve in response to service requirements.Accordingly, this section considers the factors that will have a major impact on shaping future SD-WAN deployments. These include:

- Resiliency& Performance
- NFVI & Hybrid Network Requirements
- Extending Policy Control & Analytics

REFERENCES

[1] K.-T. Foerster, S. Schmid, and S. Vissicchio, “Survey of consistent software-defined network updates,” IEEE Communications Surveys & Tutorials, 2018.

[2] X. Zuo, Y. Cui, M. Wang, T. Wang, and X. Wang, “Low-latency networking: Architecture, techniques, and opportunities,” IEEE Internet Computing, 2018.

[3] F. Bannour, S. Souihi, and A. Mellouk, “Distributed sdn control: Survey, taxonomy, and challenges,” IEEE Communications Surveys & Tutorials, 2018.

[4] O. Michel and E. Keller, “Sdn in wide-area networks: A survey,” in IEEE Fourth International Conference on Software Defined Systems (2017).

[5] J. Jiang, V. Sekar, I. Stoica, and H. Zhang, “Unleashing the potential of data-driven networking,” in Springer International Conference on Communication Systems and Networks (2017).

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details