International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 06 | June 2020 www.irjet.net p-ISSN: 2395-0072

Automation of Software Defined - Wide Area Network and it's Use Cases

R Preetham Kumar[1], Saba Farheen N S[2]

[1]*Dept. of Electronics and Communication Engineering, R V College, Karnataka, India*
[2]*Professor, Dept. of Electronics and Communication Engineering, R V College, Karnataka, India*

Abstract - *Software Defined - Wide Area Network (SD-WAN) uses software to control and manage the connectivity and services between data centers and remote branches or cloud instances. This paper aims to develop and deploy an SD-WAN architecture at various organizations by making use of the Juniper's Junos Operating System (OS). This paper proposes a very basic design of SD-WAN architecture which includes three Linux devices and two security (SRX devices from Juniper Networks) boxes. The major features of SD-WAN like Public Key Infrastructure Daemon (PKID), In-Service Software Upgrade (ISSU) and Zero Touch Provisioning (ZTP) are also being automated and tested by using the toby tool developed by Juniper Networks which supports ROBOT framework for testing. SD-WAN improves security and reduces threats. It streamlines branch Wide Area Network (WAN) architecture and reduces WAN cost by up to 90 percent. In addition to this based on the region and location where WAN is being deployed the internet bandwidth requirement gets reduced by a factor of 70 percent when compared to MPLS bandwidth.*

Key Words: **Public Key Infrastructure Daemon (PKID), Multiprotocol Label Switching (MPLS), In-Service Software Upgrade (ISSU), Long Term Evolution (LTE), Zero Touch Provisioning (ZTP).**

1.INTRODUCTION

SD-WAN is a novel structural approach which would sever as an alternative to WAN where applications and the network configurations are secluded from the given networking services like Internet access or private data services. A simple SD-WAN network is shown in Fig. 1, has a centrally enforced security and application flow policy which would manage and secure all MPLS, broadband, and 4G/LTE wireless links. With zero touch provisioning (ZTP), one can simply ship the gateway device to the required site for automatic SD-WAN access. The task of setting up policies per site, per tenant, and per department becomes quick and simple with the aid of an intuitive User Interface (UI) and automated workflows.

Application Quality of Experience (AppQoE) aims to improve the user experience at the application level by constantly monitoring the class-of -service parameters and System Level Agreements (SLA) compliance of application traffic to ensure that the application data is sent over the available SLA-compliant link.

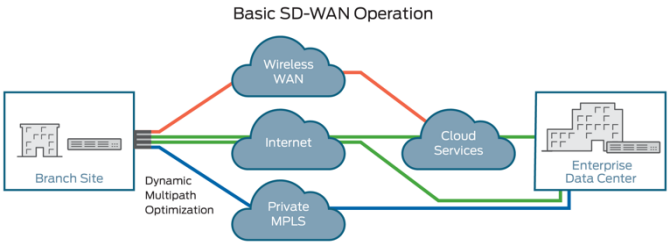

Fig -1: Sample SD-WAN Network

SD-WANs logical and physical architectures and made quick study of the delegate advances made to improve it. [1] motivates the discoveries made by rising methods, that includes machine learning for networking and network function virtualization, alongside with new transport conventions. As SD-WAN is viewed as the cutting-edge technology structure of wide area network, examination of this paper assists with using the software-define wide area network. [3] evaluated the efficiency of the PKI protocol in regard to the reloading of certificates. Author ran a few tests while testing so as to measure the quantity of certificates that can be reloaded from the PKI at different velocities. The outcomes of result demonstrate that the from start to finish inertness between a vehicle and the PKI is non-immaterial, as speed expands, the quantity of effectively reloaded certificates diminishes. Works incorporate a presentation assessment and examination with the mix of a Hardware Security Module that quickens cryptographic activities and diminishes the start to finish inertness, and the protocols under a blocked G5 network. IPsec-gateway cluster system is [7] proposed by improving and broadening the Inter Key Exchange, IKEv2 protocol. A structured standby IPsec-gateway Selection algorithm along with switch SA strategy for Encapsulates Security Payload and a suitable re-transmission approach were employed to improvise IKEv2. This mechanism can deploy IPsec-gateways in different network segments and prevent Encapsulating Security payload (ESP) loss when IPsec-gateway performs switching. Simulations show that this mechanism can improve the availability and scalability of IPsec gateway cluster.

2. SD-WAN Architecture

A SD-WAN deployment offers an adaptable and automated approach to route traffic from site to site. A basic SD-WAN architecture is shown in a Fig. 2 which includes a few simple elements such as:

- A Controller.
- Multiple overlay tunnels.
- Multiple location/sites.

- Multiple inter connections between sites forming an underlay network.

The SD-WAN controller, worked and used by Contrail Service Orchestration (CSO), goes about as an adaptation layer and gives an interface in a manner permitting only the administrator to arrange and deal with the devices at the locales.

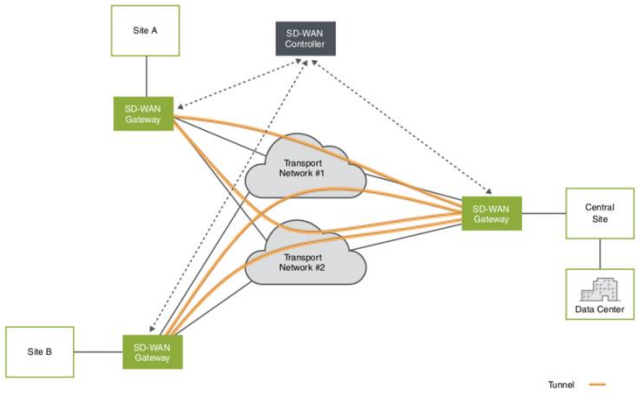

Fig -2: SD-WAN Architecture

2.1 Architectural Elements

Some of the architectural elements that required to design SD-WAN are:

1. Spoke Devices

A spoke device is named after a CPE device which is located at an Enterprise customer's branch site in a SD-WAN model. These devices sometimes can act as a Gateway Router (GWR), which provides a greater link connectivity from the many branch sites to other sites in the network model and to the Internet also. Spoke devices are of two kinds in SD-WAN model: on-premise spoke and cloud spoke.

Even in on-premise spoke devices they defined two more devices, they are specific SRX Series Services Gateways or NFX Network Services devices.

2. Hub Devices (SD-WAN Gateway)

The deployment topologies such as dynamic mesh and hub-and-spoke are the two types of deployments in SD-WAN model. Every site in a dynamic mesh deployment has a distributed CPE device interfaced with different locales and the gateway device. There could be a one hub device and more than one spoke device in a hub-and-spoke deployment.

From spoke devices to a hub device which act as a SD-WAN gateway has its own Internet Protocol (IP), ending MPLS/Generic Routing Encapsulation (GRE) and IPsec tunnels. The SD-VPN gateway which is a kind of hub device also works as an IPsec concentrator.

A service provider environment can also provide cloud hub. The service provider who provides cloud hub also have hub device inside the service provider's network. These devices are normally shared between each other, which gives hub functionalities to different clients.

3. Underlay (Physical) Network

The condition of physical connection between spoke and hub devices are remembered by underlay network in SD-WAN. The client sections do not have any consciousness of the underlay network, it basically gives reachability between on-premise spoke devices.

Fig. 3 shows the condition of physical connection between spoke and hub devices are remembered by underlay network in SD-WAN. The client sections do not have any consciousness of the underlay network, it basically gives reachability between on-premise spoke devices.

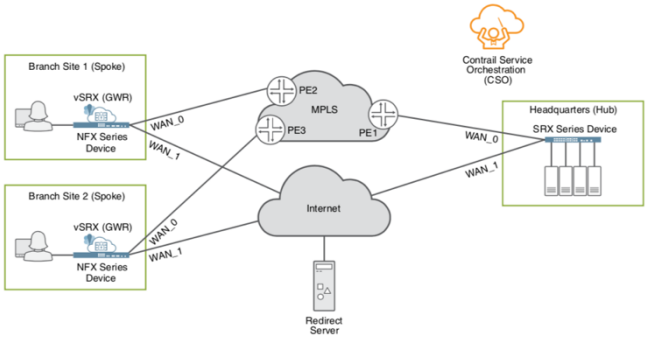

Fig -3: SD-WAN Underlay Network

4. Overlay (Tunnels) Network

The condition of logical connection between spoke and hub devices are remembered by overlay network in SD-WAN. The client sections do have some consciousness of the overlay network, and it basically gives shipping client traffic between sites.

An overlay arrangement is shown in Fig. 4. for a hub-and-spoke condition. Each port in a spoke has two passages to convey traffic towards the hub point: one through the private MPLS cloud and another over the Internet.

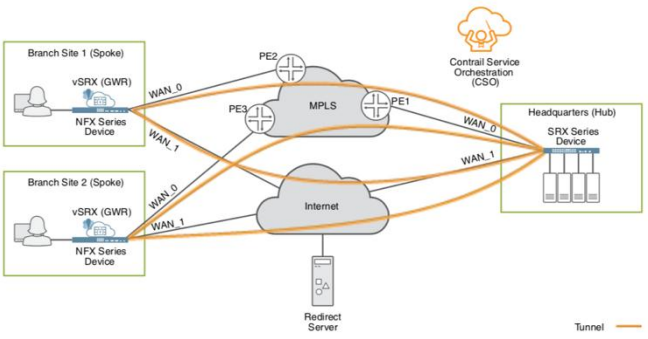

Fig -4: SD-WAN Overlay Network

2.2 System Development

The prominent features of SD-WAN that could be helpful for an organization are being described in this section. Also

describes the path switch process which occurs in the routers with help of CoS, up-gradation of image from lower version to higher version without any disruption of traffic and the services provided by SD-WAN called ZTP.

1. Digital Certificates with PKI

A public key infrastructure (PKI) bolsters the distribution and ID of public encryption keys, empowering clients to both safely trade information over systems such as the Internet and verifying the identity of the other parties.

A digital certificate is an electronic way to confirm one's ID through a confided in outsource software, known as a Certificate Authority (CA). A self-signed certificate is utilized by some organizations to witness one's identity. If autonomous Certificate Authority of any organization claims to have a Certificate Authority server then in that case, they can create their own CA. In the event that they utilize an independent CA or standalone CA, they should contact CAs organization for the addresses of their CA and CRL servers and for the data they require while submitting individual certificate demands. At the point when they utilize their own CA, they decide this data themselves. The PKI gives an infrastructure to digital certificate the executives.

2. Class of Service

Typically, when the network encounters congestion and delay, a portion of the packets must be dropped. Junos OS class of administration (CoS) empowers clients to separate traffic into classes and set different degrees of throughput and packets misfortune when congestion occurs. They can have a more noteworthy authority over the packet drop since they themselves can design rules as per their necessities.

In planning CoS applications, one should cautiously consider the administration needs, and should altogether plan and structure the CoS arrangement to guarantee consistency and interoperability over all stages in a CoS area. Because CoS is implemented in hardware rather than in software, one can experiment with and deploy CoS features without affecting packet forwarding and switching performance.

3. Unified In-Service Software Upgrade

The ISSU feature will enable client to upgrade new version of image over the older version Junos OS images with no disturbance on the control plane and with minimal interruption of traffic.

Unified ISSU exploits the advantage of the redundancy provided by dual Routing Engines and works in conjunction with the graceful Routing Engine switchover feature and the Non-Stop Active Routing (NSR) feature. Unified ISSU provides the following advantages

- Operating costs are reduced while delivering higher service level.
- Network downtime is eliminated during software upgrades.
- Allows quick usage of new features.

4. Zero Touch Provisioning

Zero Touch Provisioning (ZTP) will enable one to configure and provision devices automatically, and thus reduces the manual intervention required for adding devices to the network. In Juniper ZTP is directed by CSO team, the ZTP offers following benefits:

- Simplified, faster and automated deployment of configurations.
- Auto generated configurations that are more accurate.
- Faster scaling of the network as one need not manually apply configurations on each device in the network.

3. Design of SD-WAN Topology

The construction of a simple basic SD-WAN network requires three Linux devices such as a client, a server and an intermediate Linux and two SRX hardware devices a spoke and a hub.

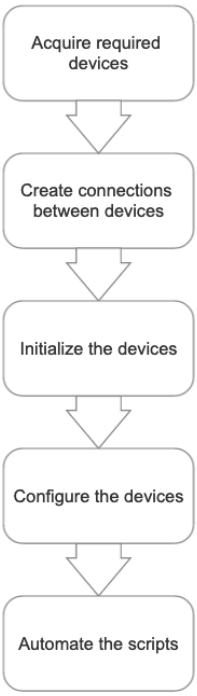

Fig -5: Flow-Diagram of automation

Testing the hardware devices becomes very important as these devices would be working on high amount of traffic. Thus, the features that are required for the SD-WAN testing are written through the Toby tool which extends its support to handle high amount of data transfer without any issues. The scripts are automated using ROBOT framework

which gets reflected in the hardware devices. The flow diagram describing the methodology is as shown in Fig. 5

Construction of topology that is required to automate the test cases is shown in Fig. 6. The topology consists of three Linux devices, one SRX security device and one vSRX. The links between them are built through Lab Resource Manager (LRM). LRM is where the lab will have these devices and those are connected to each other through virtual LAN (VLAN). For the formation of these links one should execute a pswitch command like "pswitch -l device1-name device1-link device2-name device2-link".

Fig -6: Design Topology

The three Linux devices can be named as Client, Server and intermediate Linux(h0). Linux devices are used to generate and facilitate traffic flow between them. Security box which is near the client is called as a spoke. It is basically platform independent, but this project employs SRX345 platform. Other security box which is near the server is called hub1. These devices will have all the required configurations. Scripts are automated on these devices to have required SD-WAN features. In real world, client can be any enterprise, Internet Service Provider or a small organization.

4. Results and Discussions

Automation helps to create processes which are progressively productive, adaptable, solid, and supportable. This chapter briefs about the steps being followed to automate the different features of SD-WAN using the toby tool. Results such as PKID behavior during certificate loading and after device reboot, CoS shaping verification, ISSU image upgrade and Zero Touch Provisioning are described. Description of each case includes its importance, the flow of script, and its usefulness for the users.

4.1 PKID behavior during certificate loading and after device reboot

Digital certificates play an important role when the data is being encrypted and decrypted. Fig. 7 illustrates the PKID behaviour during certificate loading and after the device reboot. Initially, the base configuration of all the protocols are to be pushed on to the device. Then the certificates are to be loaded on to the Design Under Test (DUT) unit. These certificates would be used to perform encryption and decryption of data at the client and server end. Once the certificates are loaded one should check the status of all the tunnels (Ethernet, LTE and DSL) are up.

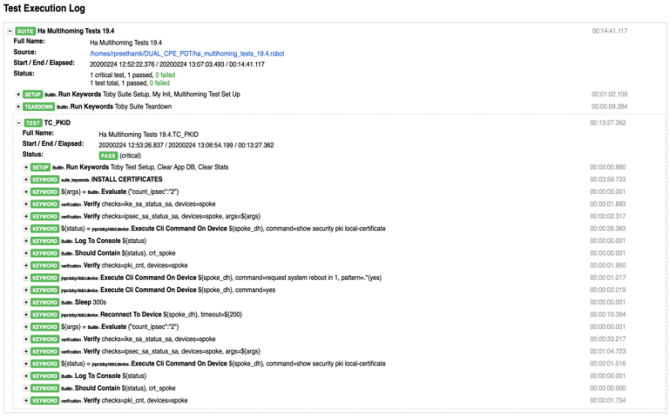

Fig -7: PKID behaviour during certificate loading and after device reboot

When the device gets rebooted the number of certificates would be compared with the stage before PKID behaviour was initiated to reconfirm that the device does not lose any of its digital certificates. If the device loses even one of the certificates, then the decryption of data would not be possible. In case of any failure, during the certificates loading process one should file a problem report so that the certificate team would help in providing the access to the lost ones.

4.2 CoS shaping verification

In order to perform the CoS shaping verification process, link with stable bandwidth needs to be used and the path would be switched accordingly as shown in Fig. 8. Initially, the base configuration of all the protocols are to be pushed on to the device. The traffic gets generated from both the client and the server end, and in turn flows through the spoke device choosing the path or tunnel with higher bandwidth (Ethernet, LTE and DSL). The device unceasingly analyzes the best path among all the links and continues to send traffic on it. Thus, the device acts in an intelligent way in order to choose the best path and switches the link accordingly. This feature helps the devices to have high end functionalities and makes it is so adaptable that different platforms can be used on it without any issue.

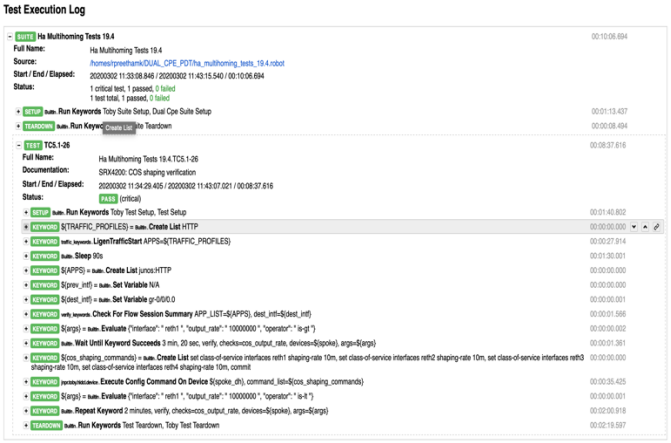

Fig -8: CoS Shaping Verification

4.3 ISSU image upgrade

The ISSU image up-gradation process is as shown in Fig. 9, wherein the base configuration of all the protocols needs to be pushed on to the Design Under Test (DUT) unit. The DUT consist of two devices one acting as a master and other as slave. The command to upgrade the image gets executed in the master wherein the image gets copied onto the slave from the master followed by which the slave would undergo up gradation and reboot. Once the status of slave is up the liabilities of slave and master are inter changed. The process of copying image is carried out even for the second time so that the new image is loaded onto both the devices. To verify the proper functionality of the device status of all the links needs to be checked along with the flow of traffic on these links. A failure of upgrade could only happen due to insufficient space or when one tries this feature with an older version.

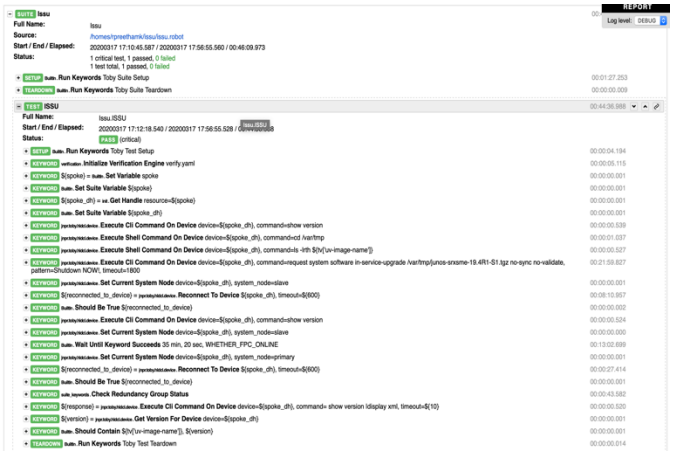

Fig -9: ISSU image upgrade

4.4 Zero Touch Provisioning

ZTP accelerates image up-gradation service on all the devices owned by an organization without any manual intervention there by considerably reducing the time taken when compared to manual upgrade. Fig. 10 illustrates the process of ZTP which starts with the creation of list of tasks being assigned to each of the devices owned by an enterprise. Communication between the enterprise and DUT is established through the phone home server feature of the device. The enterprise activates the device to apply stage-1 configuration thereby changing the status of device from expected to active, which indicates that the DUT is authenticated but not yet operational. Once the device gets authenticated the enterprise automatically triggers a job to push the provisioning and stage-2 (optional) configurations. The state of DUT gets changed from Active

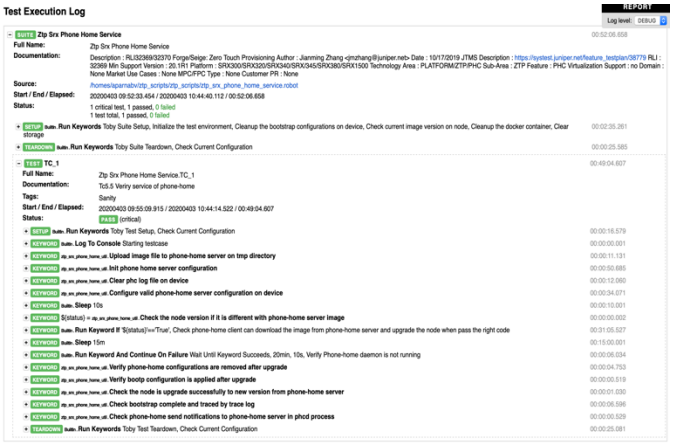

Fig -10: Zero Touch Provisioning

Provisioned, which indicates that the DTU is fully functional.

5. CONCLUSIONS

SD-WAN is a wide-area network having a virtualized overlay network abstracting the software from the hardware.

PKI provides recovery key for an encrypted storage device, can secure local networks for instance and work with physical identity cards to store digital certificates which will ensures the users privacy. CoS allows to perform switching to the best path without losing any traffic in any instance and provides best possible way for the data to reach from source to destination with the help of preconfigured policies. Images upgrades are very essentially for devices to work. So ISSU image upgrade can provide image upgrades without stopping the functioning of device and ultimately upgrades image into it without interruption of traffic. The ZTP feature is very famous in the internet world where it could configure and upgrade enterprise or service provider devices (100 to 1000 devices) in the least time when compared to days and months.

REFERENCES

1. Z. Yang, Y. Cui, B. Li, Y. Liu, and Y. Xu, “Software-defined wide area network (sd-wan): Architecture, advances and opportunities,” in 2019 28th International Conference on Computer Communication and Networks (ICCCN), IEEE, 2019, pp. 1–9.

2. S ̌eremet and S. C ̌au ̌sevi ́c, “Advancing ip/impls with software defined network in wide area network,” in 2019 International Workshop on Fiber Optics in Access Networks (FOAN), IEEE, 2019, pp. 56–61.

3. F. Haidar, A. Kaiser, B. Lonc, and P. Urien, “C-its pki protocol: Performance evaluation in a real environment,” in 2019 15th Annual Conference on Wireless On-demand Network Systems and Services (WONS), IEEE, 2019, pp. 52–55.

4. P. Karla, S. I. Saffer, V. P. Gurupur, and S. C. Suh, "Identification of class of services in the internet and a proposed approach to traffic prioritization at layer 3," in 2012 Proceedings of IEEE Southeastcon, IEEE, 2012, pp. 1–5.
5. M. Wajahat, B. Balasubramanian, A. Gandhi, G. Jung, and S. P. Narayanan, "A model-driven graybox approach to rehoming service chains," in 2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS), IEEE, 2018, pp. 116–122.
6. Y. Demchenko, S. Filiposka, M. de Vos, D. Regvart, T. Karaliotas, P. Grosso, and C. de Laat, "Zerotouch provisioning (ztp) model and infrastructure components for multi-provider cloud services provisioning," in 2016 IEEE International Conference on Cloud Engineering Workshop (IC2EW), IEEE, 2016, pp. 184–189.
7. O. Jebbar, F. Khendek, and M. Toeroe, "Upgrade of highly available systems: Formal methods at the rescue," in 2017 IEEE International Conference on Information Reuse and Integration (IRI), IEEE, 2017, pp. 270–274.
8. P. S. Rao, K. Santosh, and T. Ramesh, "Priority based traffic balancing routing protocol for wdm optical networks," in 2017 International conference on Microelectronic Devices, Circuits and Systems (ICMDCS), IEEE, 2017, pp. 1–4.