Aditya Arunkumar Vishwakarma. International Journal of Engineering Research and Applications
www.ijera.com
ISSN: 2248-9622, Vol. 11, Issue 5, (Series-VI) May 2021, pp. 14-17

RESEARCH ARTICLE OPEN ACCESS

SD-WAN gateway to the future

Aditya Arunkumar Vishwakarma
D. G. Ruparel College of Science, Matunga West, Mumbai 400 016

ABSTRACT
In today's new world, many things are moving over cloud and other such services. However, how these services work or are made is known only to a few people. To break this barrier, everyone must know 'what is cloud computing, cloud storage, data management, network architecture, Clients and Providers, etc.' To understand this soon enough, one needs to know about SD-WAN technology first. How it deals with various things and how a vast network is managed through it (an interface or GUI and CLI altogether).
Keywords - Cloud, Cloud Computing, SD-WAN, Interface, GUI and CLI.

Date of Submission: 15-05-2021 Date of Acceptance: 31-05-2021

I. INTRODUCTION

Cisco SD-WAN is a secure, cloud-scale architecture that is open, programmable, and scalable. Through the Cisco vManage console, you can quickly establish an SD-WAN overlay fabric to connect data centres, branches, campuses, and colocation facilities to improve network speed, security, and efficiency.
Software defined WAN
Centralized reachability, security & application policies. SD-WAN is powered by the points mentioned in the earlier sentence.

- Single extensible control plane
- Operates over DTLS/ TLS secure tunnel
- Dramatically reduces complexity & increases overall solution scale

The SD-WAN vision is built on this centralized Routing intelligence. SD WAN Fabric essentially makes all service side routers (LAN) learn routes & forward it to centralized controller, which then reflects the route to other routers over the networks control plane. The best part is the data traffic does not flow to the controller. Controllers are only involved in control plane communications.

To understand SD-WAN, we need to look at the main reason for which it was built and the history of network architecture.

History:

In olden times Branches had different services each being distributed to one another. So, to access a service one branch had to connect to different other branches. Later, companies started using DLLs or Dedicated leased lines. They provided QOS, full coverage & security etc. However, they were costly. Normal people could not afford a leased line. So, several network experts created VPN- Virtual Private Network. This was cheap and connection was made between two branches.

There are many types of VPN e.g. MPLS based VPN, IPSEC based VPN etc. These were alternates for DLLs.
However, MPLS was costly too. If MPLS went down e.g. for 2-3 hours in rarest cases then internet connectivity was used as an alternative backup.
For e.g.
A company has 100 branches, each branch has its own data center with servers. Configuration on all of them would significantly increase management costs. Also servers in data center get outdated with time as they cannot run new / latest software.

Hence, cloud computing came into existence. As cloud computing does not require servers, management and other expenses are reduced. To access the internet each branch does not have to go to data centers first and then internet.

If each branch has its own net connection, then the delay latency drop etc will be reduced and brought to the necessary latency ie. 100-120 needed for QOS.

However, each branch needs security features. One cannot go to every router and write configurations.

So, SDN started to simplify WAN, Basically, it separated the brain (control plane) from the body (data plane).

II. PARTS OF SD-WAN

The three basic parts of SD-WAN architecture are:

1. vSmart
2. vManage
3. vEdge routers

The brain was moved to a centralized location known as vSmart. vSmart automatically configures the data. If 2 vSmart are used, brain redundancy takes place which is good. Now to MANAGE and MONITOR multiple vSmarts another application known as VMANAGE is used. It can monitor multiple kinds of vSmart.

The separation of data plane & control plane reduced maintenance costs.
vManage can use rest of API.
Router – more than one vSmart copies of brain
For 1 vSmart not more than 1 router can be used.
vManage- multiple vSmart configurations can be monitored and managed at once.

Hence, this was the foundation for SD-WAN and the reason it was built was to put everything over the cloud and to reduce the work of writing too many configurations over each and every device.
It also reduced management cost and the need for data centres to be updated every now and then was stopped.

Devices:
The entire Cisco SD-WAN routing portfolio includes:
Viptela OS Routers

1. **vEdge-100:** five fixed 10/100/1000 Mbps ports. Comes in three different flavors:
   - **vEdge 100b:** Ethernet only
   - **vEdge 100m:** Ethernet and integrated 2G/3G/4G modem
2. **vEdge-1000:** 8 ports of fixed GE SFP
3. **vEdge-2000:** 2 Pluggable Interface Modules
4. **vEdge-5000:** 4 Network Interface Modules
5. **ISR 1100-4G:** 4 GE WAN ports
6. **ISR 1100**-4GLTE: 4 GE WAN ports, 4G LTE (CAT4)
7. **ISR 1100-6G:** 6 GE WAN ports (4 GE and 2 SFP)
8. IOS XE SD-WAN Routers
   - **ISR & ASR Series:** With IOS XE SD-WAN software image, SD-WAN capability can be enabled on select ISR 1000 series, ISR 4000 series and ASR 1000 series routers.
   - **ENCS:** With IOS XE SD-WAN software image, SD-WAN capability can be enabled on select ENCS 5000 series platforms.
   - **vEdge Cloud** and **CSR** 1000V are the cloud elements of the SD-WAN solution.

vEdge router functionalities: All of vEdge Routers offer the same software functionality. The key differences between the platforms are in respect to throughput, redundancy in hardware components and port density. Some models of vEdge-100 routers offer additional functionality in the form of Power over Ethernet.

vSmart: Centralized controllers, called Cisco vSmart Controllers, oversee the control plane of the Cisco SD-WAN fabric, efficiently managing provisioning, maintenance, and security for the entire SEN overlay network. They perform the function of transferring/uploading the configurations as stated by the user on the vManage or the GUI.

SD-WAN can be configured with CLI or GUI (vManage) where CLI is used by experienced architects and GUI is for newer folks who do not have much idea or are new to CLI and CLI commands.

So, one must begin with GUI only for a better understanding. This applies to absolutely everyone, to know what the features of SD-WAN are.

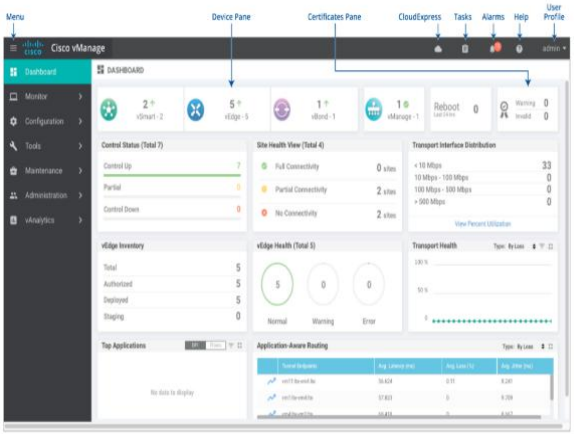

Fig. (GUI/Cisco vManage interface)

The above figure is the GUI dashboard for keeping each and every device, commands, interfaces, etc. in check to avoid failures.

The CLI counterpart uses commands only. Hence, if one does not know commands, he/she can make use of the GUI interface.

vBond Orchestrator: Another device, called the Cisco vBond Orchestrator, automatically authenticates all other Cisco vEdge devices when they join the SEN overlay network.

Now moving on to control plane and data plane:
Control Plane:
1. Facilitates fabric discovery
2. Dissimilates control plane info between vEdge.
3. Dramatically reduces control plane complexity.
4. Distributes data plane & app- aware routing policies to vEdge routers.
5. Implements control plane policies

Data Plane:
1. The main part of a vEdge router.
2. Path of forwarding configurations. – virtual Data forwarding
3. Implement policies
4. Application aware routing
5. Physical or virtual form factor (100 mb, 1 GB, 10 GB, 20 GB +)
6. Based on Cisco or Viptela
7. Provides secure data plane with remote vEdge routers
8. Establishes secure control plane with vSmart controllers (OMP)
9. Implements data plane & application aware routing policies.
10. Exports performance statistics
11. Uses traditional routing protocols e.g. VRRP
12. Supports zero-touch deployment

That being said, let's talk about the vSmart.
vSmart controls the brain (control plane of vEdge routers (single centralized location) and forwards all the necessary configs to data plane at once. If vSmarts go down, SD-WAN network will be paralyzed as it performs major functions in the network.

Deployment option for every device (vEdge, vSmart, vManage)

On Premise – vEdge	vEdge- Hosted
ESXi or KVM Physical server	AWS / Azure

Cisco SD WAN can build secure overlay fabric on any kind of public or private transport (MPLS, Internet, 4G/ZTE, satellite, Ptop & so on).
Coming on to IPsec tunnels and TLOCS
A secure IPsec tunnel is built on the overlay fabric using TLOCS between end points. IP address can change when we work with DHCP & this change of address can impact the identification on end pts, so to overcome this, SD WAN uses system IP, color, Encapsulation to identify end points.

A TLOC is a Transport Locator, which is analogous to a LISP RLOC, or Routing Locator. Both abstract the router itself in favor of location-based mapping. RLOCs represent the routing location and not an endpoint. This is different than traditional routing, where a router would be identified by its physical address on each interface.

- System-IP: This address is similar to an OSPF or BGP Router-ID and does not need to be routable or reachable.
- Transport Color: The color is used to differentiate different transports, i.e. MPLS, Internet, and LTE (mobile data). In cases where transport types are duplicated but should still be treated differently from each other (such as two different Internet providers) the colors could be arbitrary, such as Silver and Gold. Part of this color information includes the details needed for data plane tunnel setup such as interface IPs, ports (for NAT-T) and some fabric information.
- Encapsulation Type: This is important for the advertising of data plane connectivity. The choices are IPSec or GRE, and for obvious reasons a GRE TLOC will not establish a data plane tunnel with an IPSec one.

Combining all three pieces of information creates a TLOC. An SD-WAN router with connectivity to three different transports (and colors) would have three TLOCs. Exchanging these TLOCs allows the arbitrary (or full-mesh) topology of the SD-WAN fabric to be built.

TLOCS are advertised as TLOC routes in OMP messages sent between vEdge & vSmart. vSmart distributes these TLOC to other vEdges in the overlay network. In the absence of control policies on vSmart these TLOCS are sent to all other in the network however this distribution can be controlled with policies configured on vSmart. Once these TLOCs are advertised to vEdges, then these vEdges can create an IPSEC tunnel between themselves. By default vEdges can create a full mesh network between them.

TLOCS and Colors
The specificator that is used is categorized as private or public.
Private colors (MPLS private 1-6, metro – Ethernet)
All others are public
(Red, blue --- public, Ethernet)
Private v/s public color is highly significant. The color setting applies to the following

Colors
Based on the color settings on both sides, vEdges know when to use public or private IP address when establishing IPSEC tunnels.

If private colors are used on both sides, a private IPP & port ate used to establish a tunnel.
If there is a mix of private & public colors, a public IP & port are used. When a tunnel is established between -2- public colors, public addressing as a tunnel source & destination is used.
If a private / public color is removed then it can talk to the routes of the same color. By default, the color is default.

III. SOME REQUIRED INFORMATION FOR SD-WAN ENTHUSIASTS:

There are many complicated commands in SD-WAN. One such command is as under:
'show policy zbfw filter-statistics'
This command is for filtering the statistics on a vEdge.
Note: This command will come in use in the further stages of SD-WAN configuration.
There are many such commands in configuring SD-WAN. Hence some people find it easy to do configurations on GUI even if it takes a lot of time because no one can remember such commands except some experienced people who have vast knowledge on this stuff. That being said, this tells us how vast the configurations are in SD-WAN though it is a new technology.

IV. CONCLUSION:

Lastly, these are some basic things one needs to keep in mind while trying out the configurations/ GUIs for SD-WAN.

1. The interface
2. Basic knowledge about the devices which will be used
3. Basic information about TLOCS, OMPS, and various other routing protocols
4. The commands (what they mean in certain case)
5. And make this architecture after knowing what it will be used for.

That said, SD-WAN is a freshly created technology not known to many people out there. This paper aims to give basic knowledge to people who plan to study SD-WAN or practice this in labs. This will give some necessary knowledge one needs to master this technology.

REFERENCES:

[1]. https://sdwan-docs.cisco.com/Product_Documentation/vManage_Help/Release_18.2/Dashboard/Dashboard
[2]. https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-07-vedge-routers-data-sheet-cte-en.html
[3]. https://sdwan-docs.cisco.com/Product_Documentation
[4]. https://www.cisco.com/c/en_in/solutions/enterprise-networks/sd-wan/index.html
[5]. https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/system-overview.html