EVEN 792-038: LINUX NETWORKING
SD-WAN as a Service for Hybrid Cloud
Milestone-2

Jagan Cherukuru Agribabu (jcheruk) Jayalakshmi Viswanathan (jviswan)
Sandeep Kundala (skundal) Sushmitha Natanasabapathy (snatana)

1. INTRODUCTION:

a. What is SD-WAN?

SD-WAN stands for software-defined wide-area network. It is a software-defined approach to manage the wide-area network, or WAN that connects and dynamically routes traffic across branches/sites, data centers and clouds.

b. Why SD-WAN? Why not just use traditional WAN?

Connecting with traditional WAN includes specialized equipment or fixed circuits in the past, but SD-WAN is implemented as a software-based solution or hybrid of hardware / software which provides versatility. For example, in a traditional WAN, dedicated MPLS circuits are used to ensure safety and reliable connectivity. In a cloud-centered world, this approach would no longer apply. Traditional WAN uses MPLS for efficient network traffic flow between the multiple sites. MPLS is a privately managed backbone with built-in Quality of Service (QoS). It provides end-to-end distribution and control of secure packet transmission. Providers can provide QoS by assigning priority to certain traffic in the network. But, the drawback of MPLS with traditional WAN was high cost of service, setup time and lack of centralized control.

In terms of network cost, capacity, agility and visibility, SD-WAN challenges MPLS ' pitfalls. SD-WAN provides flexibility by offering on-demand provisioning and a pay-as-you-grow model for enterprises and customers. SD-WAN minimizes the difficulty of managing infrastructure and connectivity. Enterprises can use software-based management to leverage automation to phase out expensive routing hardware and improve network efficiency (as it has greater visibility of the network).

2. RELATED WORK:

Organizations such as Cisco, VMWare and SilverPeak have developed their proprietary solutions for providing SD-WAN as a service to customers. We will discuss a few of them in this section.

a. Viptela:

Cisco has had a good history with SD WAN solutions starting with iWAN and with the acquisition of Meraki and Viptela powered SD WAN, it is a big player in this segment. Meraki powered SD WAN has simple management, orchestration and automation features and suitable for lean IT environments whereas Viptela powered SD WAN is preferred for enterprises with sophisticated environments which require advanced routing and secure segmentation. Viptela is kind of a game

changer in the movement from hardware-based networking to software defined approach with regards to WAN.

Viptela works via an overlay fabric which is carrier and transport agnostic. It is based on open architecture supports multi-cloud architecture by offering seamless public cloud expansion as well as SaaS optimization. Customers are given the freedom to deploy it on-premise or in the cloud. It is made of four primary components named vManage, vSmart Controllers, vBond Orchestrator and vEdge Routers. Except for vEdge routers, everything are software components and vEdge can be a physical device or software. vManage is the centralized network management system and is very helpful in monitoring, configuring and maintaining all the SD-WAN devices across the network.

Viptela provides an overlay on top of the services/components of the organization which results in transport independence i.e. disaggregates the service from the physical network. The vSmart controller helps in separating the control plane from the data plane and establishes control plane connection with all the vEdge routers. The vSmart controllers work in tandem with vBond orchestrator to maintain communication between the Controller and the routers. The routers now have lesser load and can perform data plane operations efficiently. The control, data and management planes scale and work independently. We intend to replicate the multi cloud support and try to make our solution cloud agnostic.

There are several features of Viptela SD WAN like zero-trust network security and segmentation, advanced filtering and security, predictable application experience using multiple hybrid links etc. which come in handy for a sophisticated enterprise environment. The major pulling factor is the vAnalytics which helps administrators collect data from SD-WAN and analyze it to identify network and bandwidth issues instantly. Consequently, it helps in gauging the performance of new and existing components of an application on the network. All these components and capabilities make Cisco SD-WAN powered by Viptela a truly stable and scalable solution.

There are a few things which can make it less desirable. The movement of using software instead of hardware can reduce the operational and maintenance costs but still there is an overhead of infrastructure change costs as the adoption is a big deviation from the traditional way. Additionally, Viptela SD-WAN requires at least 4 primary components to be up and running at all times. While the separation of functionality can be a good thing but still it adds to the operational complexity of ensuring these components to be up and running at all times.

b. VeloCloud:

The VeloCloud SD-WAN solution was built as a “transport-independent” product that is easy to implement and that permits the use of any type of physical transport connection, from MPLS to cable to cellular LTE. Their cloud resident gateways are of benefit to companies requiring a secure overlay that is transport independent, operating across any combination (public or private circuits), with secure connectivity to enterprise data centers, cloud compute and SaaS applications.

Their architecture is similar to that of Viptela in terms of their secure network overlay where separate control plane and data plane layers improve network service agility by moving intelligence from the data plane into the programmable control plane. Another key feature is virtual service delivery where services are deployed from a catalog of applications. Based on the type of service, the services are delivered at the branch, in the private data center, or in the cloud. Orchestration and analytics layer provides the control plane for forwarding traffic to and from on-premises and cloud nodes, across the multiple underlying transports and with the policy-driven insertion of distributed network services. Also it provides sub-second dynamic traffic steering, supports TCP optimization and forward-error correction for real-time applications.

In terms of routing, VeloCloud SD-WAN automatically recognizes the applications, allows prioritizing them and steers the traffic down the best performing link automatically in real-time. In the event both links were not performing as needed the VeloCloud would send the traffic down both links

VeloCloud Edge, Gateways and Orchestrator are the products included in the SD-WAN where the gateways is deployed at cloud data centers around the world. These gateways provide scalability, redundancy, and flexibility; optimize data paths to all applications, branches, and data centres and deliver network services from the cloud.

Velocloud suffers from similar disadvantages as Viptela. It requires a significant amount of investment to set up the whole infrastructure while helping reduce the operational costs moving forward.

c. Silver Peak's Unity EdgeConnect SD-WAN Edge Platform:

Silver Peak Unity is a virtual WAN overlay enabling customers to deploy all broadband or hybrid WANs using different types of connectivity like MPLS. LTE, DSL etc. It makes use of two components Unity EdgeConnect and Unity Orchestrator for designing an efficient SD-WAN application. It has almost all the features of Viptela SD-WAN and additionally has an optional Unity Boost component to optimize performance by improving latency mitigation and data reduction. They also have forward error correction feature which is essentially not present in all vendor solutions.

While the whole idea of removing expensive private MPLS with Internet using Silver Peak SD WAN to save costs looks interesting, there are question marks on the SLA from low cost ISPs. Generally, when the low cost Broadband provider suffers an outage, the SLA will not be comparable with Private based networks.

3. PROBLEM STATEMENT:

Provide solution to customer to connect their sites irrespective of the cloud environment they are deployed with value added solutions for effective routing,

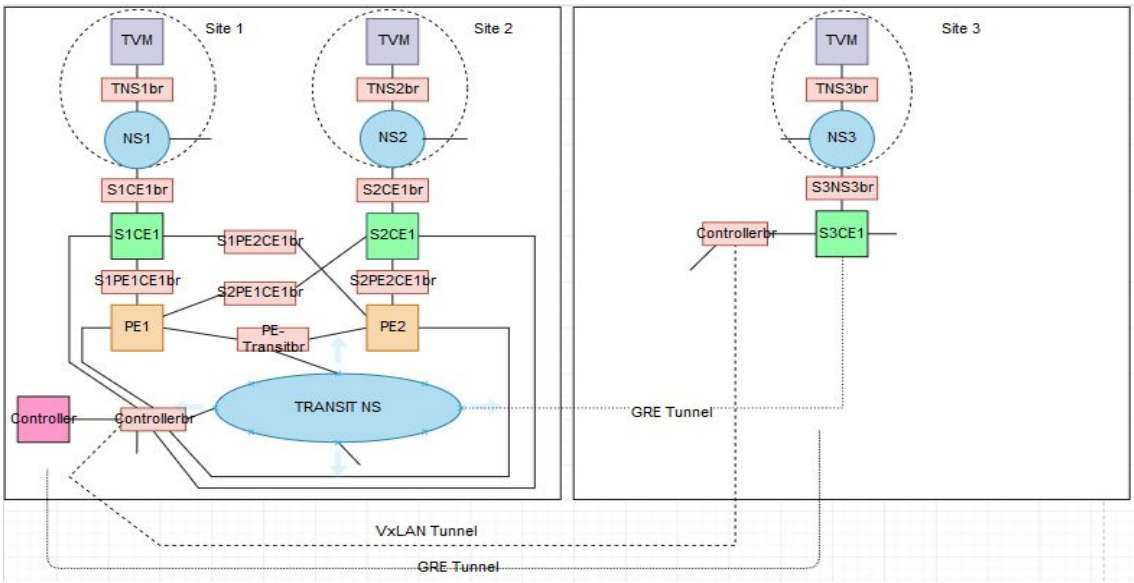
flexibility, configurability and security which improves user experience and reduces work for the network administrator.

4. ARCHITECTURE:

The customer approaches with requirement of connecting his/her sites present in different clouds in such a way that there is a significant reduction in the cost of deployment and maintenance, increases user experience and gives better value added services compared to traditional WAN solution.

First, the customer approaches that he/she wants to use the solution provided by us (let's call the solution provider as team10) and provides a list of clouds in which their sites are placed in, Tenant ID leased to the customer in the clouds (*Note that the Tenant ID should be the same in all clouds)* and number of provider edge routers required. Using this information Team10 deploys transit namespace, controller network in the clouds with controller VM in primary cloud (specifications given by the user), provider edge routers (PE) (specifications given by user) and GRE tunnel between the clouds.

Then the controller is handed over to the customer with all the instructions like the file format required for deployment of customer edge routers (CE), connection between the CE and PE and connection between the CE and site namespace. To provide connection between the CE in other cloud (not primary), a GRE tunnel is created between the transit NS and the remote CE.



5. FEATURES:

a. Functional Features:

Route optimization:

- The route taken from a network is changed dynamically from the PE and CE's CPU utilization, using policy based routing feature of linux boxes.
- The CE's and PE's are configured with separate routing tables to populate routes in each corresponding to which PE/CE the CE/PE should forward.

Flexible WAN:

- The user can attach/detach connections between CEs and PEs in the existing sites.
- The user can create new connections between the sites and PEs.

Asynchronous Data transfer:

- The delay tolerant traffic is marked and sent from the origin VM.
- PE checks the marked traffic, checks the destination CE's CPU utilization. If CE's CPU utilization is below the threshold, the PE forwards the traffic to the destination CE, else stores the packets in the memory and forwards it once the CPU utilization is below the threshold.

b. Management Features:

Security:

- Provide security to all the edge routers using IP tables to allow only the traffic from the IP addresses the tenant is using and deny everything else.

Configurability:

- Tenant can configure the addition and deletion of connections between CE and PE, can add or delete CE.
- Tenant can configure custom security rules on the CEs to allow or deny the traffic towards the site *(Note: If a site has multiple CEs the IP Table would be identical)*.

Accountability:

Logs provided to the customer which are stored on the controller:

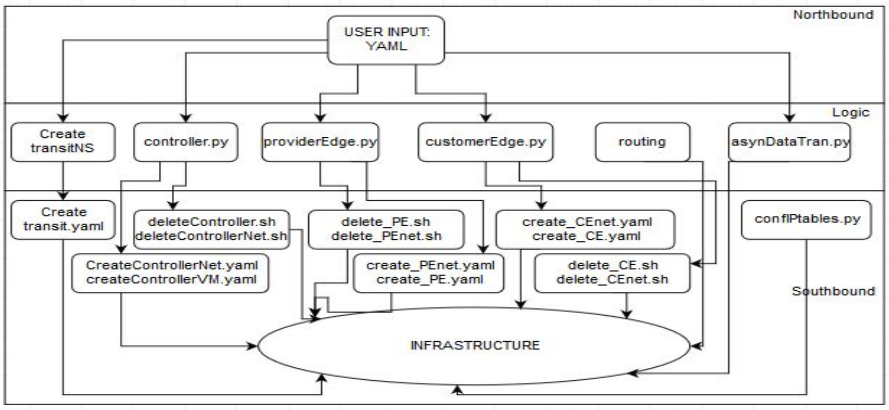
- CPU utilization of Customer and Provider Edge Routers
- Dynamic route table updates on CE.
- IPtable updates on CE, PE and controller
- Addition/deletion of sites, CE and PE

Scripts used:

Program file name	***Description***
create_transit.yaml	*Ansible playbook to create transit namespace in primary cloud for the tenant.* ***Requires:*** *transit_var.yaml*
controller.py	*Python program to create or delete management network and*

	controller VMs. ***Requires:*** *createControllerNetwork.yaml, createControllerNetwork_hyp.yaml, controllerNetConfVar.yaml, controllerNetConfVar_hyp.yaml, createControllerVM.yaml, controllerNetworkTemplate.xml.j2, controllerTemplate.xml.j2, controllerNetworkHypTemplate.xml.j2, deleteVM.sh, deleteNet.sh*
providerEdge.py	*Python program to create or delete PE router VMs and network depending upon user's input.* ***Requires:*** *create_PEnetwork.yaml, PEnet_vars.yaml, create_PE.yaml, PE_vars.yaml, deleteVM.sh, deleteNet.sh*
customerEdge.py	*Python program to create or delete CE router VMs and CE to Site network depending upon user's input.* ***Requires:*** *createCEVM.yaml, createCEVM_hyp.yaml, CE(*)ConfVar.yaml, createCENSnet.yaml, createCENSnet_hyp.yaml, CETemplate.xml.j2, CENSTemplate.xml.j2, deleteVM.sh, deleteNet.sh*
createCEPEnet.py	*Python program to create network between the CE and PE* ***Requires:*** *createCEPEnet.yaml, PE_CE(*)confVar.yaml*
deleteCEPEnet.py	*Python program to delete network between the CE and PE* ***Requires:*** *deleteNet.sh, PE_CE1confVar.yaml*
routing.py	*Python program to change routes in edge routers depending upon the CPU usage of the next hop edge routers.*
asynDataTransfer.py	*Python program to check destination CE at PE and then store or forward depending upon the CPU utilization of the destination CE.*
confIPtables.py	*Python program to change the ip table rules as per the user requirements.*

Implementation Architecture:



In the Northbound interface, the user gives respective input depending upon the function to perform i.e., to create transit namespace, to create/delete controller network, to create/delete provider edge network, to create/delete customer edge network, and after setting up the infrastructure, to configure IP table rules.

In logic layer, the respective python files are executed depending upon the input to create infrastructure, to enable dynamic routing functionality and asynchronous data transfer.

In the southbound, there are ansible scripts, python files and shell scripts to create, delete and configure the network infrastructure depending upon the input given by the user.

REFERENCES:

1. What is SD-WAN? - CISCO: https://www.cisco.com/c/en/us/solutions/enterprise-networks/sd-wan/what-is-sd-wan.html#~why-now-
2. VMWARE VeloCloud https://www.velocloud.com/sd-wan
3. Performance based routing: the gold rush for SD WAN https://www.networkworld.com/article/3387152/performance-based-routing-pbr-the-gold-rush-for-sd-wan.html
4. SD-WAN can help solve the challenges of multi cloud. https://www.networkworld.com/article/3339622/sd-wan-can-help-solve-challenges-of-multi-cloud.html
5. CISCO LIVE - Introduction to Cisco SD-WAN (Viptela) https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/LTRCRS-2015.pdf
6. Cisco Validated Design - Cisco SD WAN Design https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/CVD-SD-WAN-Design-2018OCT.pdf?oid=dsgen013910
7. Cisco- Forwarding_and_QoS_Overview https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_17.2/08Forwarding_and_QoS/01Forwarding_and_QoS_Overview