ADARA

SD WAN

Performance Based

Cloud Interconnections

Rev 2019

ADARA VNF AWS and Data Center deployment

Topology:

- Topology Diagram Logical View:

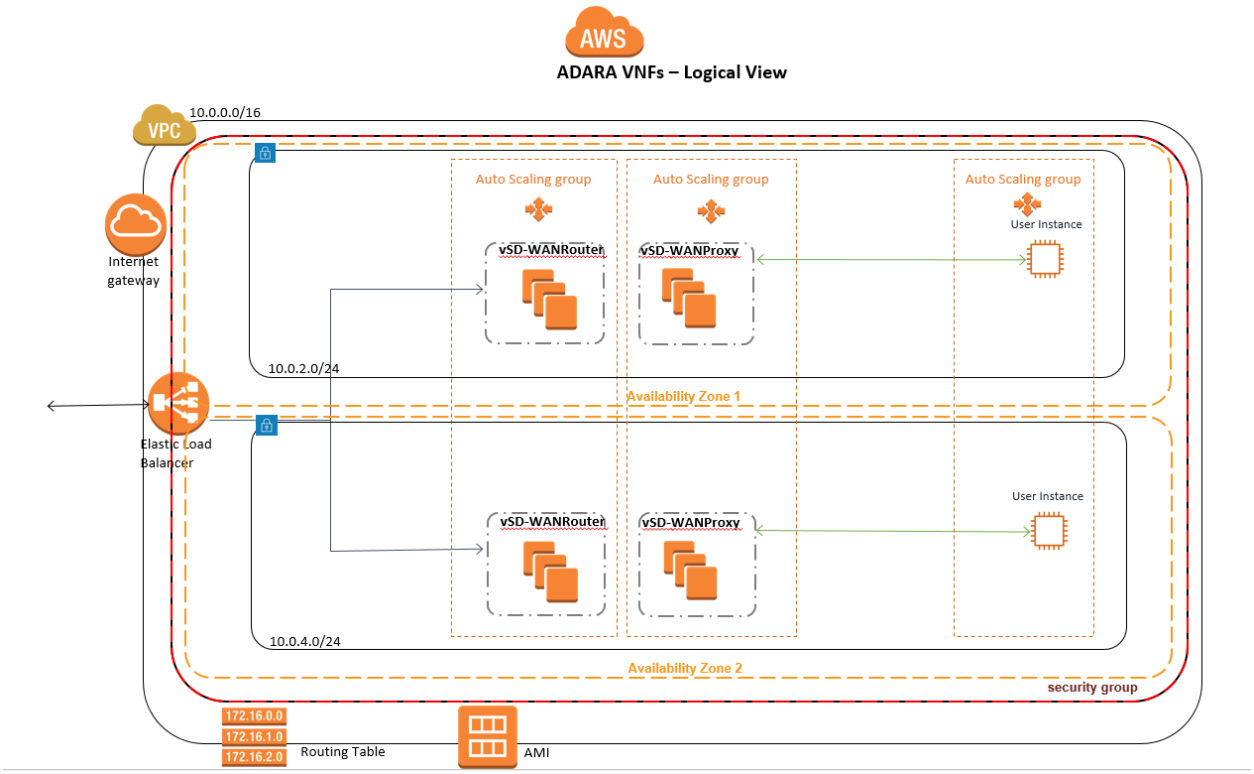


Figure 1

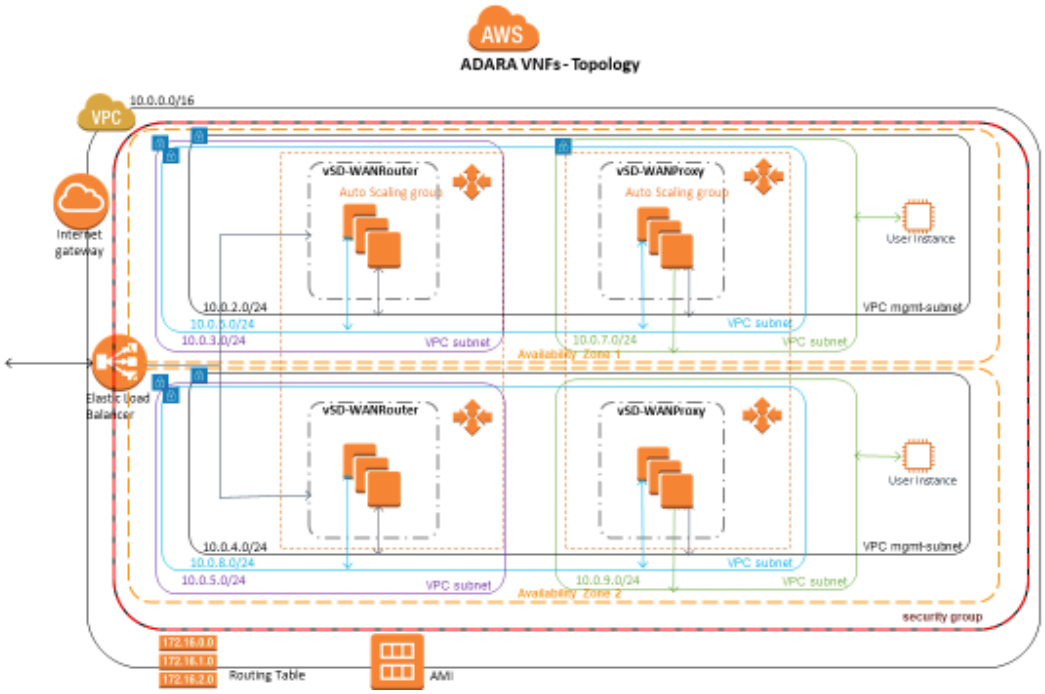
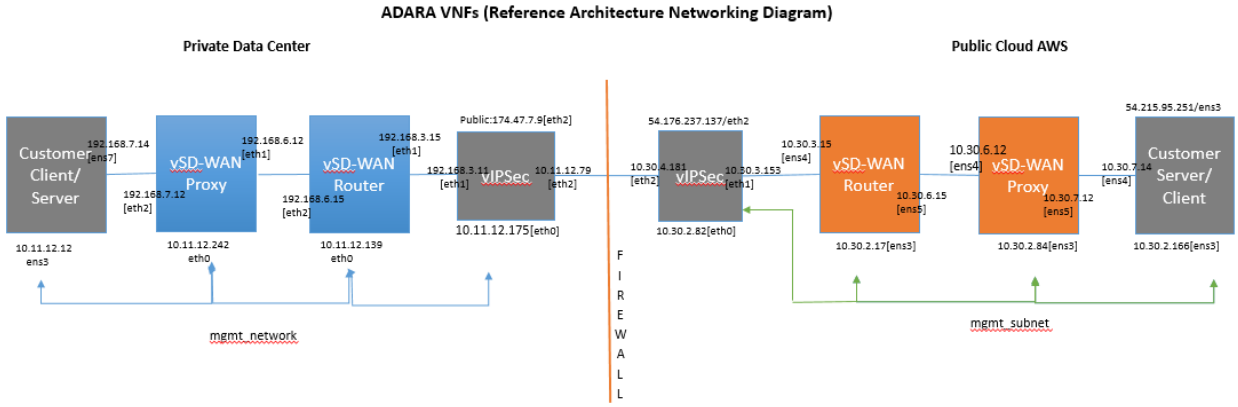

AWS
ADARA VNFs - Topology
VPC
10.0.0.0/16
Internet gateway
Elastic Load Balancer
vSD-WANRouter
Auto Scaling group
vSD-WANProxy
Auto Scaling group
User Instance
10.0.2.0/24
10.0.6.0/24
10.0.3.0/24
VPC subnet
10.0.7.0/24
VPC subnet
VPC mgmt-subnet
Availability Zone 1
vSD-WANRouter
vSD-WANProxy
User Instance
10.0.4.0/24
10.0.8.0/24
10.0.5.0/24
VPC subnet
10.0.9.0/24
VPC subnet
VPC mgmt-subnet
Availability Zone 2
security group
172.16.0.0
172.16.1.0
172.16.2.0
Routing Table
AMI

Figure 2



Note: Client/Server VMs are representatives of existing clients/servers in customer environment.

Figure 3

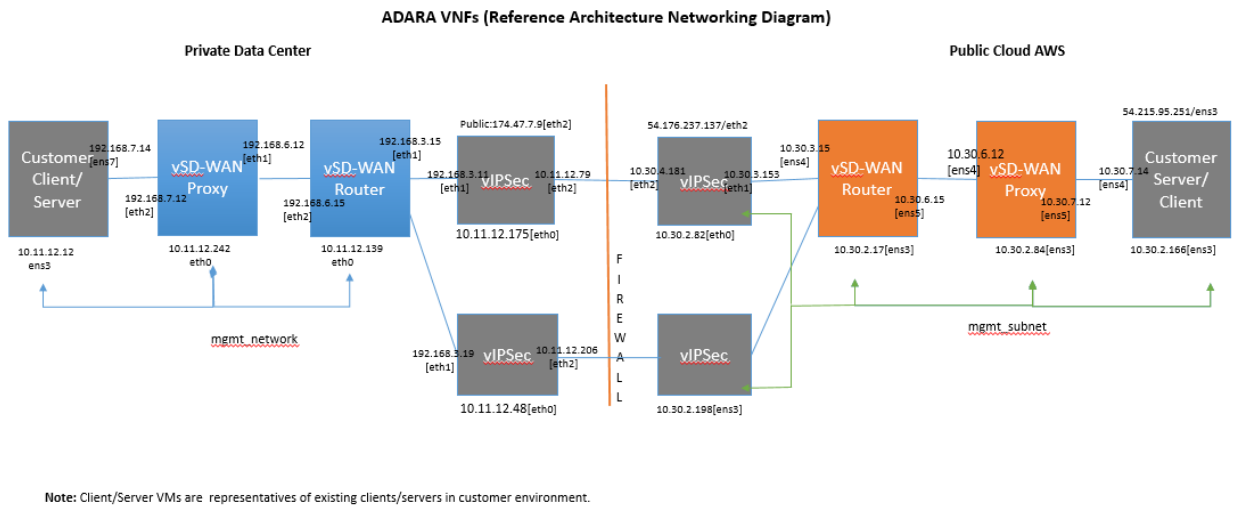


Figure 4

Deployment and Configuration on Public Cloud (AWS):

Pre-requisites:

- Account details with AWS public cloud.
- Select a Region, Availability zone, and Key Pair on AWS for the deployment.
- ADARA VNF Images for AWS
- Data Center Common Infrastructure details
- Data Center Common Services (NTP, DNS, DHCP, Default Gateway etc.)

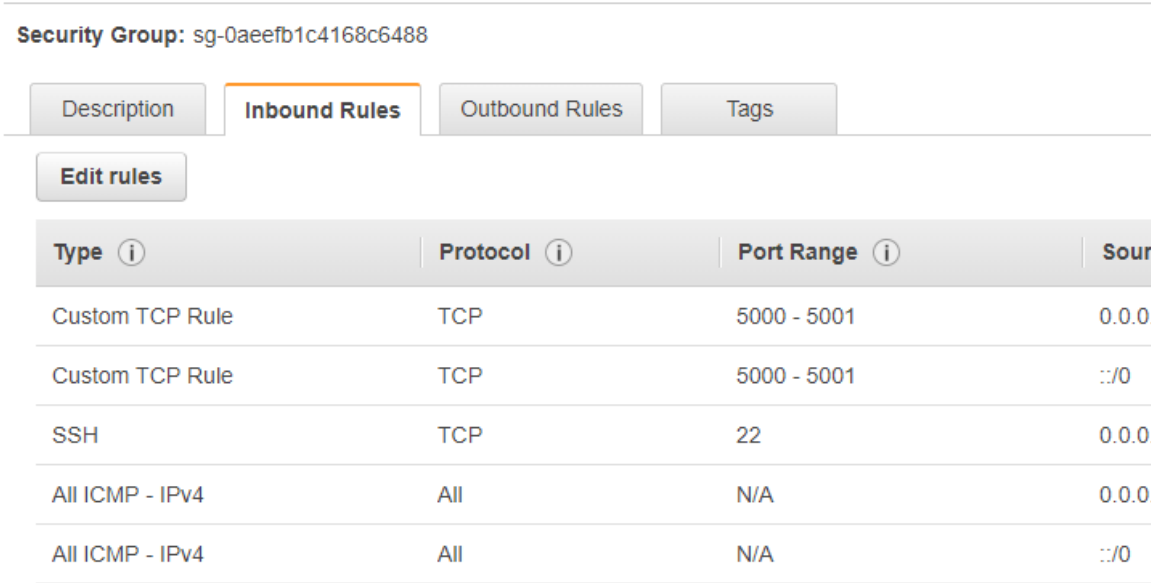
AWS: VNFs AMI image table

VNF Name	Description	VNF Image ID	Flavor	Key Pair eg.	Security Group eg.
vSD-WANProxy	Virtual SD-WAN Proxy: TCP Proxy, De-duplication Proxy	ami-0133f5826287c5f43	M4.xLarge or larger	<keyPair>	<secGroup>
vSD-WAN Router	Virtual SD-WAN Router	ami-05b90e2d4ac78ee00	M4.xLarge or larger	<keyPair>	<secGroup>

Table 1

Deployment: Below example is per RA Topology

Note: Please substitute appropriate values for your environment

- Create a VPC <VPC> or use existing:
  - <VPCName> in <Region> with CIDR <eg. 10.0.0.0/16>
  - Note down VPC_ID
- Create Key Pair:
  - Create a Key Pair <keyPair> in AWS Console for the region under EC2 Dashboard - Network & Security TAB
  - Download the key Pair and store in secure location (.pem)
  - This Key will be used to SSH to the instances
- Create 4 subnets in the <VPC> in <Region> and <AvailabilityZone> under VPC Dashboard
  - Example below for reference
  - mgmt_subnet: CIDR: 10.0.2.0/24
  - wan_to_vnf_subnet: CIDR: 10.0.3.0/24
  - vnf_subnet: CIDR: 10.0.6.0/24
  - vnf_to_server_subnet: CIDR: 10.0.7.0/24
- Create Internet Gateways: under VPC Dashboard
  - Create Internet Gateway <IGW>
  - Attach IGW to <VPC> (ensure IGW lists the VPC as attached)
- Create Security Group:
  - Create Security Group <secGroup> under Security TAB in AWS Console for <VPC>
  - Add InBound Rules
    - 

  - Add OutBound rules to allow necessary traffic
    - Type: All Traffic, Protocol: All protocols, Port Range: All, Dest: 0.0.0.0/0

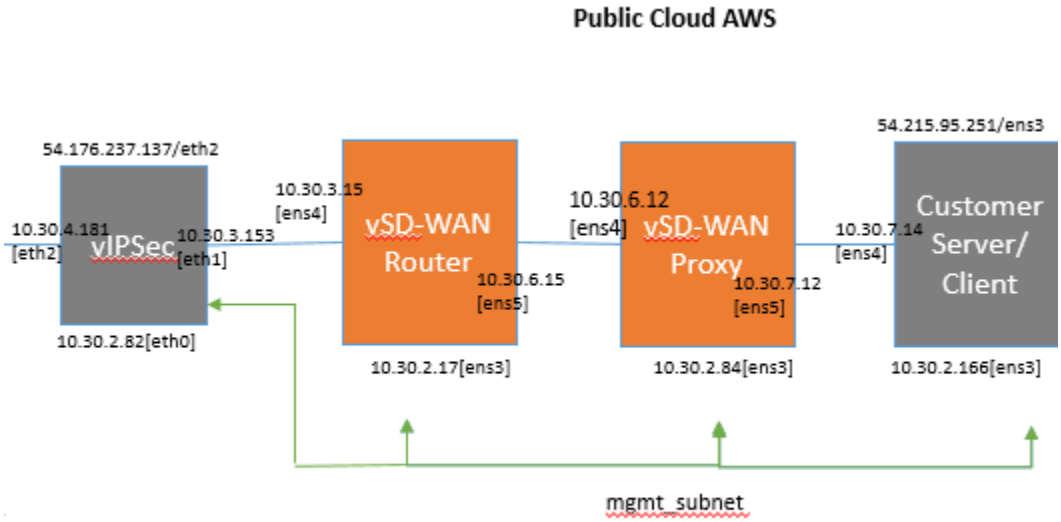
- Create or ensure Network ACL <networkACL> for <VPC>: Please refer to any specific security policies of your organization
    - Create Network ACLs under Security TAB or use existing for <VPC> in AWS Console
    - Ensure all 4 subnets are associated with <networkACL>
    - Add InBound and OutBound rules to allow necessary traffic (ICMP, TCP, SSH etc)
    - Associate the 4 subnets above under Network ACL TAB
- Create a Route Table:
    - Create a Route Table <routingTable> for <VPC>
    - Ensure all 4 subnets above are listed under the <routingTable>
    - Ensure routes for the VPC local CIDR is allowed
        - Eg. 10.0.0.0/16 (local)
    - Add route for external connectivity (as deemed necessary)
        - Eg. 0.0.0.0/0 for IGW
    - Subnet explicit Associations with the Route Table:
        - Associate subnet (ADARA vSD-WANRouter)
            - Eg. 10.0.3.0/24 to enable external connectivity to its pair in Data Center
        - Associate additional subnets which need external connectivity to this Route Table
            - Eg. if Instances need to be managed from outside and have Elastic/Public IPs
            - mgmt_network eg. 10.0.2.0/24
- Create VNF instances:
    - VNF images:
        - VNF image information in Table 1
    - VNF <vSD-WANRouter>
        - Create VNF <vSD-WANRouter> M4.XLarge or larger on the mgmt_subnet using AMI image <VNF Image>
        - Select appropriate <VNF Image>, subnets, <SecGrp> and <KeyPair> for <VPC>
        - Create additional network Interfaces on subnets and attach to the VNF per Topology
        - Disable Source/Destination for both VNFs on all network interfaces
        - Set and persist IP forwarding and unset RPF check on the VNF eg.
            - $ sysctl net.ipv4.conf.all.forwarding=1
            - $ sysctl net.ipv4.conf.all.rp_filter=0
            - ip forwarding and rp_filter settings can be made persistent via /etc/sysctl.conf file
        - Configure Routes:

        - Configure appropriate routes to the other end of the tunnel (vSD-WANRouter) in the data center
    - Download the configuration script from http://s3.amazon.aws.com/adara-public/configure_vsdwanrouter.sh
    - Run bash ./configure_vsdwanrouter.sh and follow the prompt
    - Check status and connections:
        - service --status-all | grep adara
- VNF <vSD-WANPROXY>
    - Create VNF <vWANProxy> M4.XLarge or larger on the mgmt_subnet using AMI image <VNF Image>
    - Select appropriate <VNF Image>, subnets, <SecGrp> and <KeyPair> for <VPC>
    - Create additional Network Interfaces on subnets and attach to the VNF per Topology
    - Disable Source/Destination for both VNFs on all network interfaces
    - Set and persist IP forwarding and unset RPF check on the VNF eg.
        - $ sysctl net.ipv4.conf.all.forwarding=1
        - $ sysctl net.ipv4.conf.all.rp_filter=0
        - ip forwarding and rp_filter settings can be made persistent via /etc/sysctl.conf file
    - Configure Static Route:
        - Add static routes for vSD-WANProxy pair and any clients in Data Center
        - Eg. ip route add 192.168.6.0/24 via 10.30.6.15 dev ens4
        - Ip route add 192.168.7.0/24 via 10.30.6.15 dev ens4
    - Download the configuration script from http://s3.amazon.aws.com/adara-public/configure_vsdwanrouter.sh
    - Run bash ./configure_vsdwanrouter.sh and follow the prompt
- VNF <IPSec>:
    - Please use third party IPSec VNF and configure for your environment
- Server/Client:
    - Create or use existing Server/Client on the mgmt_subnet
    - Ensure you have same security established on the Server/Client with <SecGrp> and <KeyPair> in the <VPC>
    - Establish connectivity on the Data Interface over <eg. 10.0.7.x> network
    - Disable Source/Destination for both VNFs on all network interfaces
    - Set and persist IP forwarding and unset RPF check on the VNF: eg.
        - $ sysctl net.ipv4.conf.all.forwarding=1
        - $ sysctl net.ipv4.conf.all.rp_filter=0

- ip forwarding and rp_filter settings can be made persistent via /etc/sysctl.conf file

- Configure Routes:
  - Configure appropriate route to Server IP in AWS
  - Eg. ip route add 192.168.7.0/24 via 10.30.7.12 dev ens4

- Note:
  - If VNF AMI already has the multiple network interfaces created or a single mgmt_subnet
  - If not, then use needs to create network interfaces manually and attach it to the corresponding VNF.
  - RA Topology example below:



  - Network Interfaces for VNF <vSD-WANRouter>:
    - Ensure Network Interface <eth0> on mgmt_subnet IP 10.0.2.161 UP
    - Create Network Interface <eth1> on subnet 10.0.6.15
    - Create Network Interface <eth2> on subnet 10.0.3.15
    - Attach the above Network Interfaces to vSD-WANRouter
    - Login to VNF and ensure these interfaces are persistent and UP
  - Network Interfaces for VNF <vSD-WANProxy>:
    - Ensure Network Interface <eth0> on mgmt_subnet IP 10.0.2.174 UP
    - Create Network Interface <eth1> on subnet 10.0.6.12
    - Assign IP to Network Interface <eth1>
      - Eg. Check ifconfig –a for the newly added Network Interface

        - Note: On AWS console, you may see the IF name as eth#, and once logged in to VNF you may see the IF name as ens#
        - Assign IP 10.0.6.12 to the appropriate IF and status UP
    - Create Network Interface <eth2> on subnet 10.0.7.12
    - Assign IP to Network Interface <eth2>
        - Eg. Check ifconfig –a for the newly added Network Interface
        - Note: On AWS console, you may see the IF name as eth#, and once logged in to VNF you may see the IF name as ens#
        - Assign IP 10.0.7.12 to the appropriate IF and status UP
    - Attach the above Network Interfaces to vSD-WANProxy
    - Login to VNF and ensure these interfaces are persistent and UP
        - Eg. edit /etc/network/interfaces and add the above network interface details with auto UP
- Client/Server are representatives of client/server from customer environment (requirement: Establish IP connectivity per RA topology)
    - Network Interfaces for VNF <server/client>:
    - Ensure Network Interface <eth0> on mgmt_subnet IP 10.0.2.207 UP
    - Create Network Interface <ens4> on subnet 10.0.7.14
    - Attach the above Network Interfaces to <server/client>
    - Login to Client/Server and ensure these interfaces are persistent and UP

Data Center (on-premise) VNFs

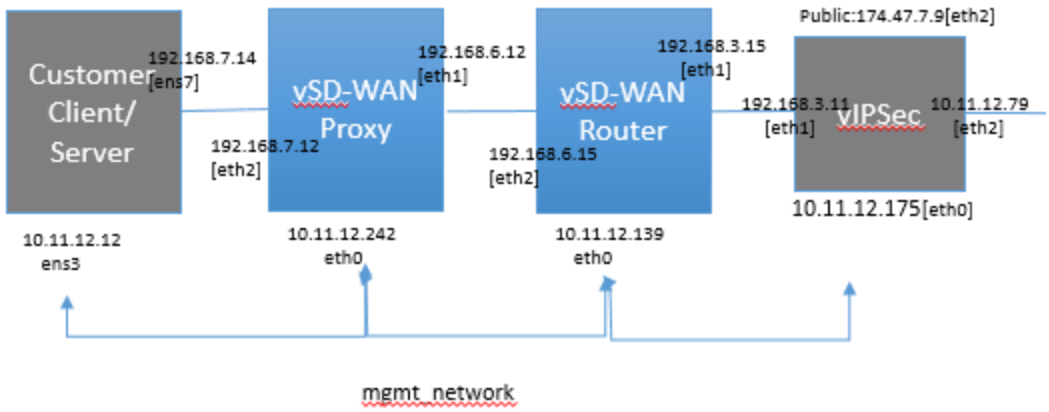
Pre-requisites:

- Hypervisor: KVM Host
- Gather DC lab details:
    - NTP, DNS, Search string, Domain string, DHCP, Default Gateway, and IP pool for the DC deployment
    - Download ADARA VNF images and verify the checksum provided
        - https://s3.amazonaws.com/adara-distro/distro/

DC: VNFs image table

VNF Name	Description	VNF Image ID	Flavor
vSD-WANProxy	Virtual SD-WAN Proxy: TCP Proxy, De-duplication Proxy	vSD-WANProxy.img	4 CPU, 16 GB Mem
vSD-WAN Router	Virtual SD-WAN Router	vSD-WAN Router.img	4 CPU, 16 GB Mem

Table 2



Note: Client/Server VMs are representatives of existing clients/servers in customer environment.

Deployment: Below example is per RA Topology

Note: Please substitute values according to your environment

- Create VNF instances:
  - VNF <vSD-WANRouter>
    - Create an instance or VNF <vSD-WANRouter> on the mgmt_subnet using image <VNF ImageName>
    - Select appropriate <subnets>, <KeyPair where applicable> for your data center
    - Set and persist IP forwarding and unset RPF check on the VNF: eg.
      - $ sysctl net.ipv4.conf.all.forwarding=1
      - $ sysctl net.ipv4.conf.all.rp_filter=0
      - ip forwarding and rp_filter settings can be made persistent via /etc/sysctl.conf file
    - Establish connectivity to vSD-WANProxy on the Data Interface over <eg. 192.168.6.x> network
    - Establish connectivity to outside on the Data Interface over <eg. 192.168.3.x> network
    - Configure Routes:

- Configure appropriate routes to the other end of the tunnel (vSD-WANRouter) in AWS
  - Download the configuration script from
  - https://s3.amazonaws.com/adara-distro/distro/configure_vsdwanrouter.sh
  - Run bash ./configure_vsdwanrouter.sh and follow the prompt
- VNF <vSD-WANProxy>
  - Create VNF <vWANProxy> on the mgmt_subnet using qcow2 image <VNF Image>
  - Select appropriate <VNF Image>, <subnets>, <KeyPair where applicable> for data center
  - Set and persist IP forwarding and unset RPF check on the VNF: eg.
    - $ sysctl net.ipv4.conf.all.forwarding=1
    - $ sysctl net.ipv4.conf.all.rp_filter=0
    - ip forwarding and rp_filter settings can be made persistent via /etc/sysctl.conf file
  - Establish connectivity to vSD-WANRouter on the Data Interface over <eg. 192.168.6.x> network
  - Establish connectivity to Client/Server on the Data Interface over <eg. 192.168.7.x> network
  - Configure Static Route:
    - Configure static route to IP of vSD-WANProxy pair in AWS
    - Eg. ip route add 10.0.6.0/24 via 192.168.6.15 dev eth1
    - Ip route add 10.0.7.0/24 via 192.168.6.15 dev eth1
  - Download the configuration script from
  - https://s3.amazonaws.com/adara-distro/distro/configure_vsdwanproxy.sh
  - Run bash ./configure_vsdwanrouter.sh and follow the prompt
- VNF < IPSec>:
  - Please use third party IPSec VNF and configure for your environment
- Server/Client:
  - Create or use existing Server/Client in the data center
  - Ensure the same security established on the Server/Client with <KeyPair where applicable> in the data center
  - Establish connectivity on the Data Interface to vSD-WANProxy over <eg. 192.168.7.x> network
  - Set and persist IP forwarding and unset RPF check on the VNF: eg.
    - $ sysctl net.ipv4.conf.all.forwarding=1
    - $ sysctl net.ipv4.conf.all.rp_filter=0
    - ip forwarding and rp_filter settings can be made persistent via /etc/sysctl.conf file
  - Configure Route:
    - Configure appropriate route to Server IP in AWS
    - Eg. ip route add 10.0.7.0/24 via 192.168.7.12 dev ens7