Linking OpenStack Workloads to the Public Cloud Using SD-WAN

Shannon McFarland - CCIE #5245

Distinguished Engineer - Cisco Office of the Cloud CTO

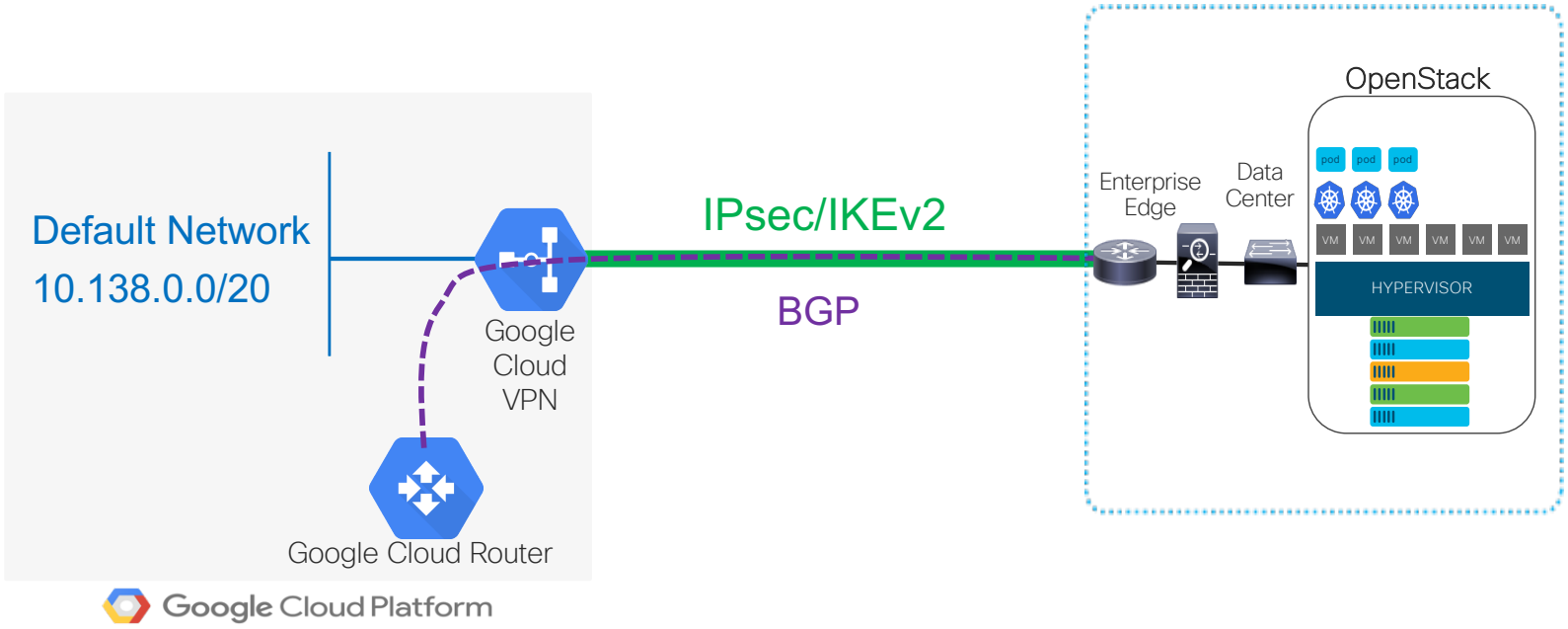
@eyepv6

Agenda

- Hybrid/Multicloud Options
- SD-WAN Overview
- Cisco SD-WAN Cloud onRamp (CoR) - Linking OpenStack to the Public Cloud
- Summary

Hybrid/Multicloud Networking Options

Cloud Service Provider – Native IPsec VPN Service



Virtual Routers

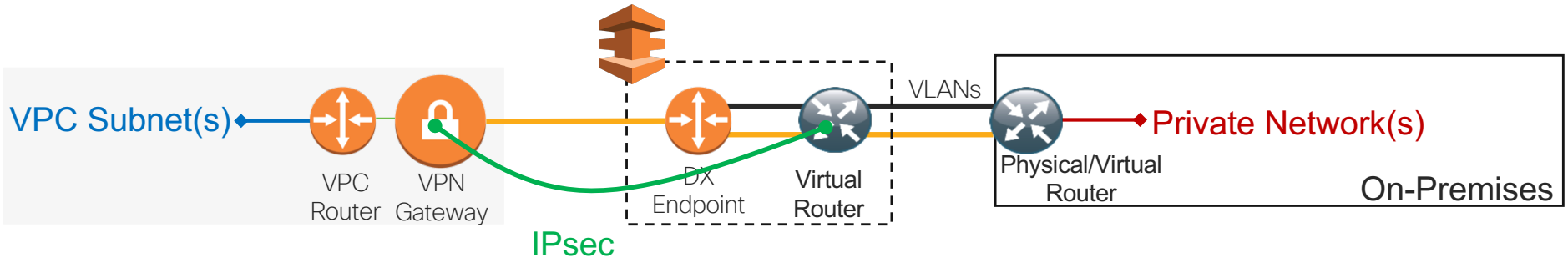
Per-VPC Virtual Router

Transit VPC: Virtual Router + CSP VPN

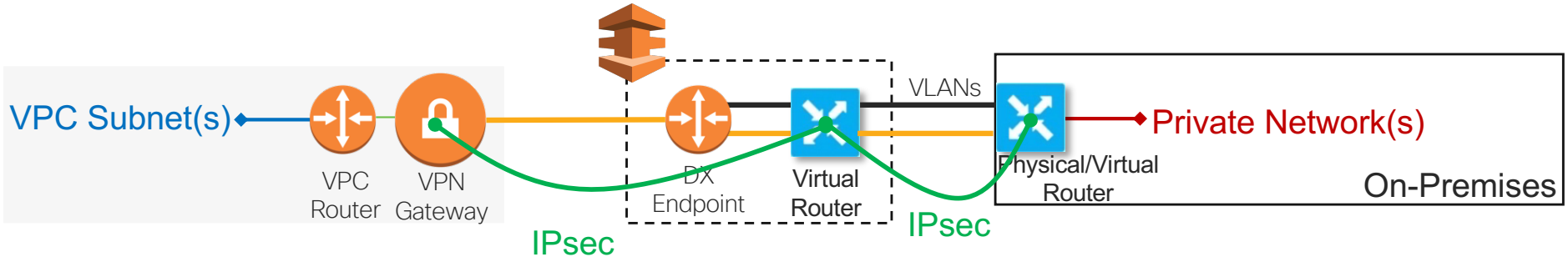
Transit VPC: Virtual Router + Per-VPC Virtual Router

Colocation – With or Without VPN

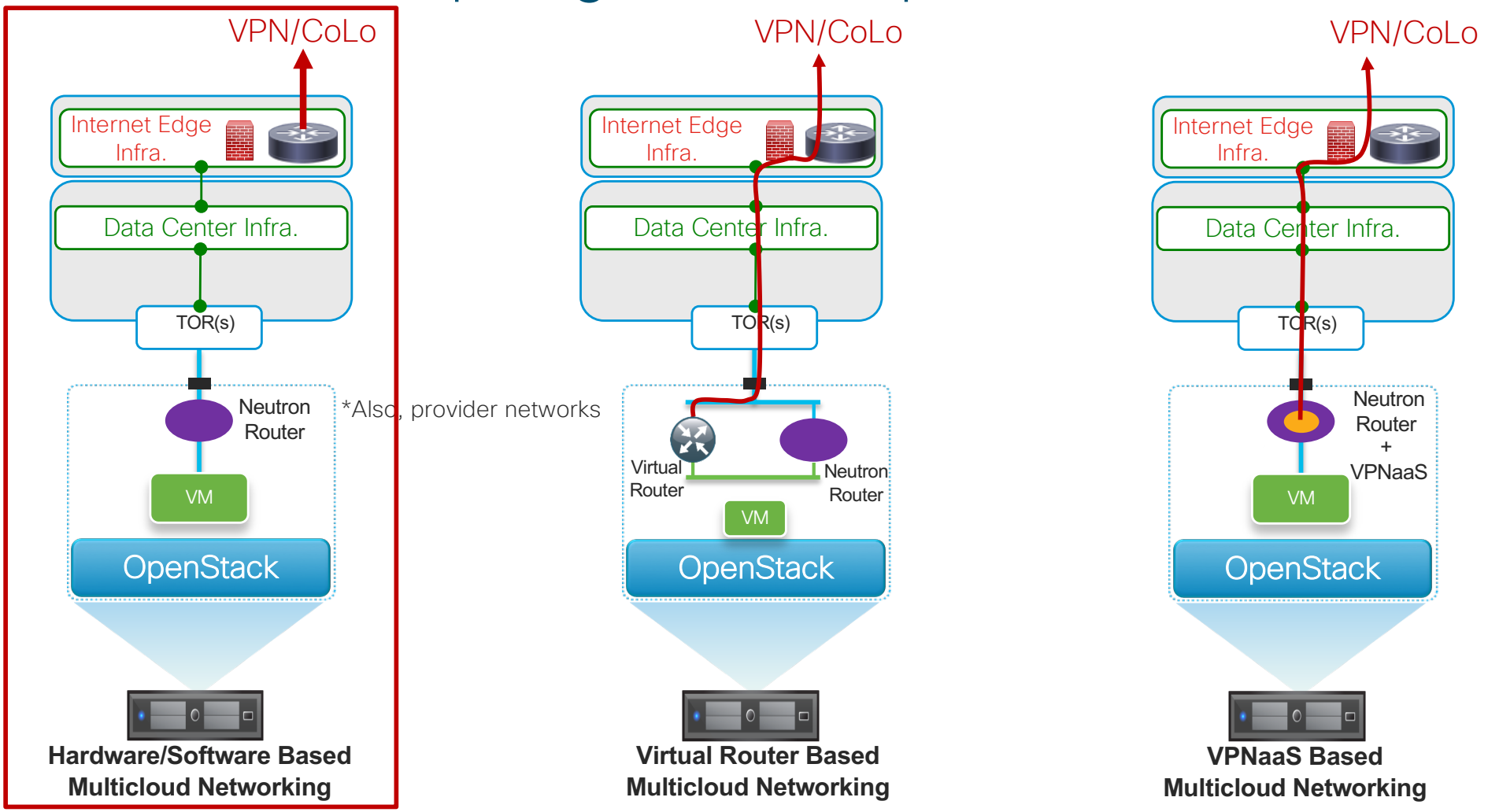
Cisco Routers or Firewalls + Some Combo of Colocation/peering



Cisco SD-WAN + Some Combo of Colocation/peering



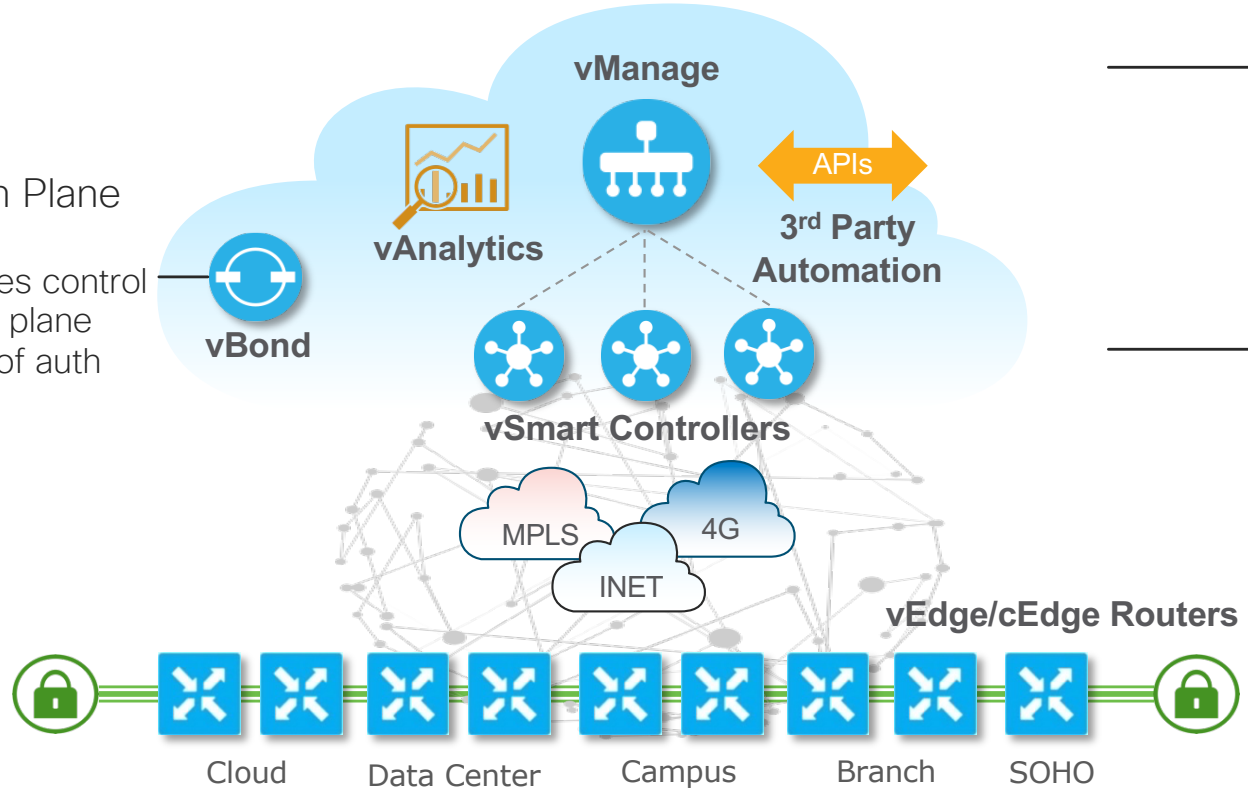
Multicloud Topologies With OpenStack



SD-WAN Overview

Cisco SD-WAN Architecture

Orchestration Plane
- vBond
- Orchestrates control and mgmt. plane
- First point of auth



Management Plane
- vManage
- UI
- Policies, templates
- Monitoring

Control Plane
- vSmart
- Fabric discovery
- Control plane policies

Data Plane
- vEdge/cEdge

We Can Do This The Easy Way or Hard Way

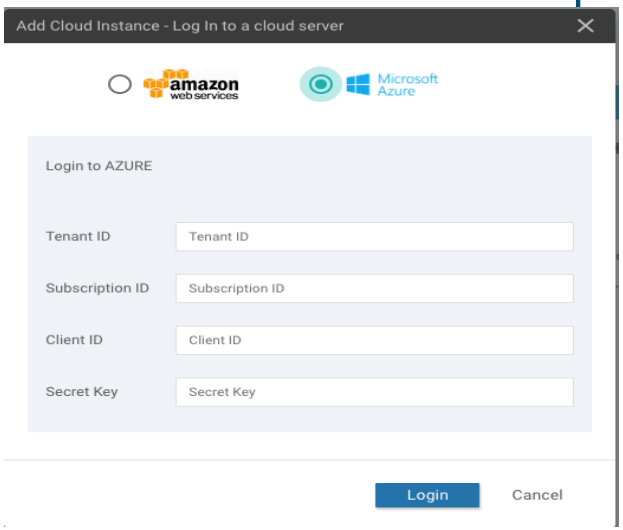
I'll explain the hard stuff, but..

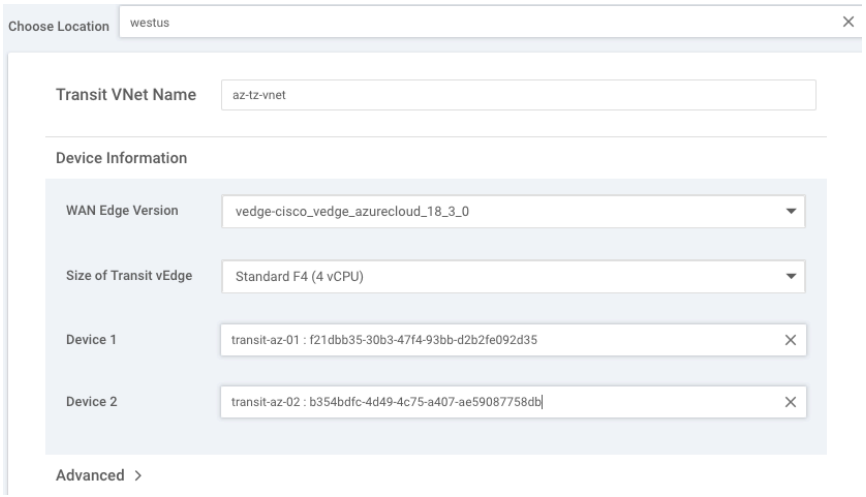
1) Design it
2) Deploy the Control Plane
3) Deploy the On-Premises Data Plane (to include connections to OpenStack)
4) Create/Gather your Public Cloud Credentials/Roles
5) Deploy the Transit VNet/VPCs via Cloud onRamp
6) Map the application/host VNet/VPCs to the Transit
7) Deploy Policy(s) that Meets Your Requirements
8) Have a Nice Day! ☺

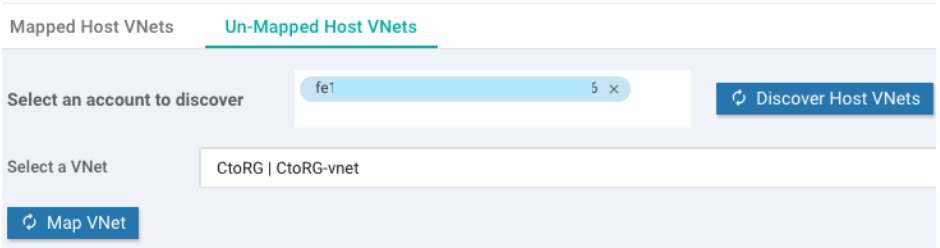
We will talk about these two

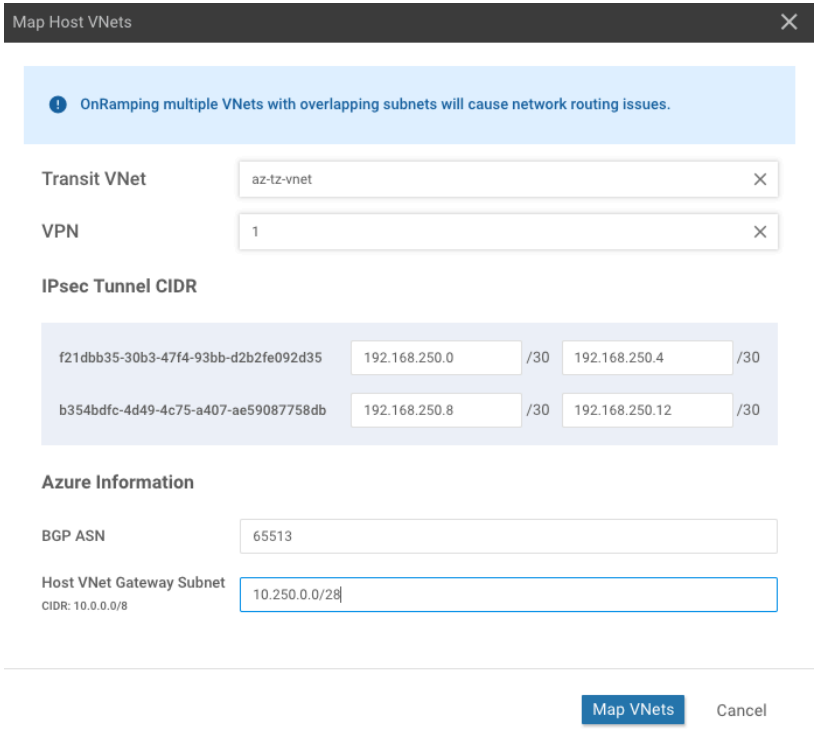
Cisco SD-WAN Cloud onRamp for IaaS – Azure

Cloud OnRamp IaaS for Azure

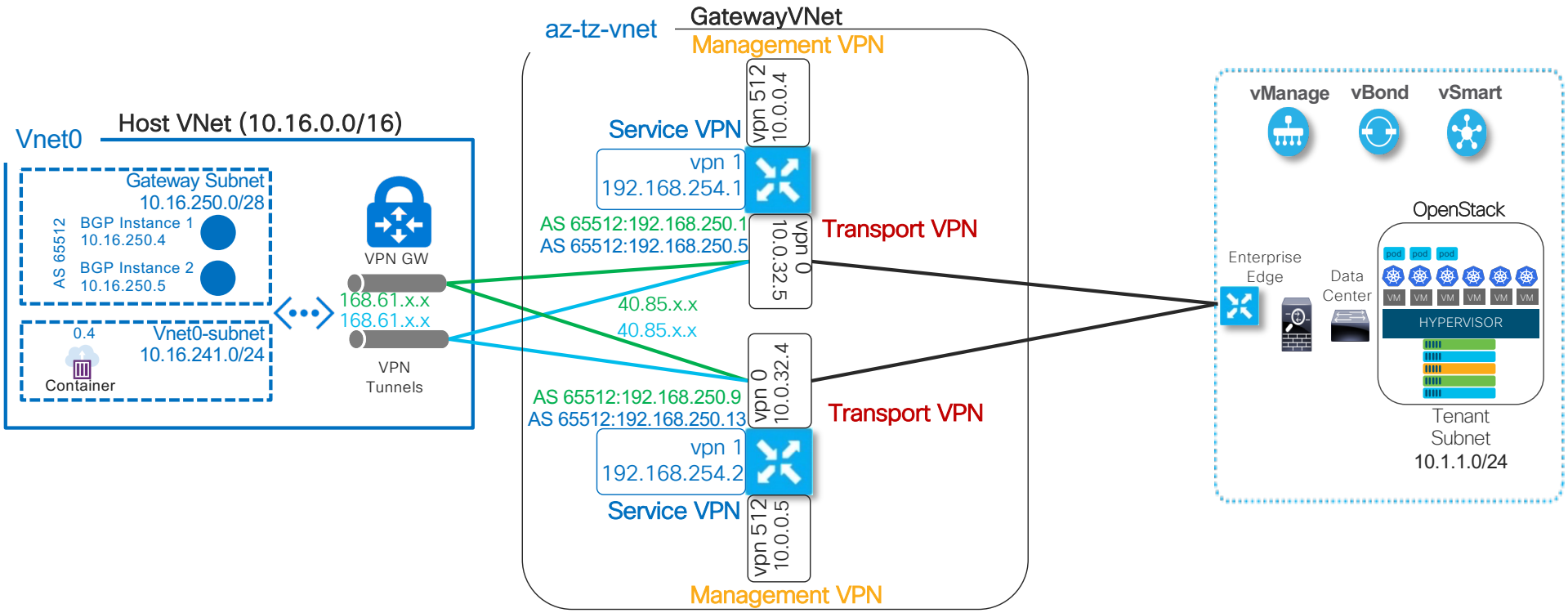








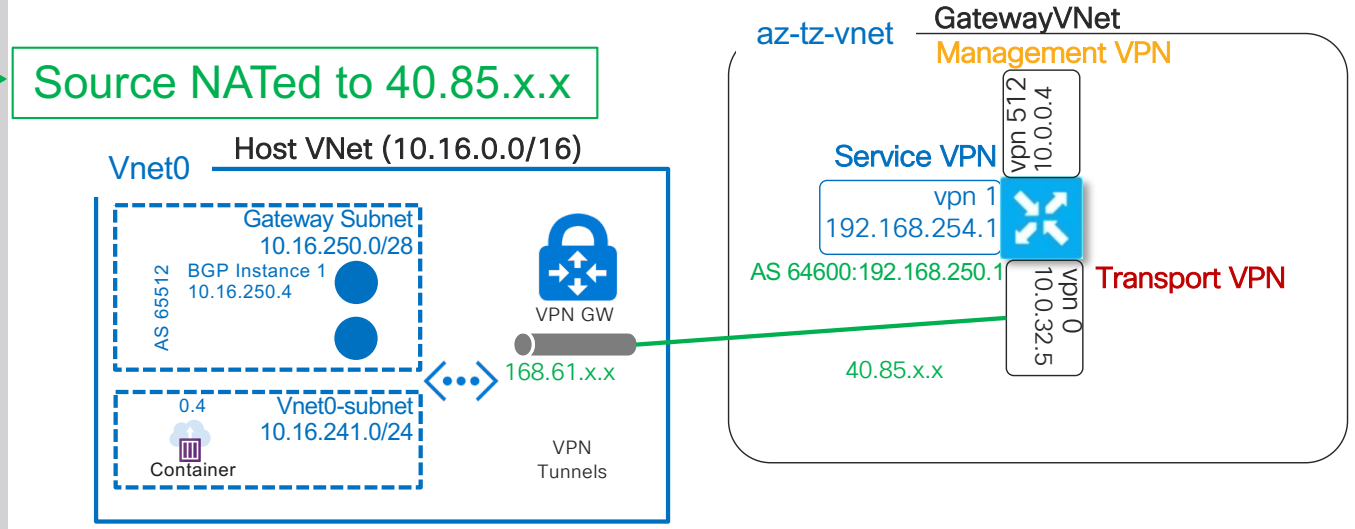
Cisco SD-WAN CoR for Azure



Azure – Host VNet –to- Transit VNet Mapping - IPsec

vEdge-Cloud – Transit VNet

```
interface ipsec9
 ip address 192.168.250.1/30
 tunnel-source       10.0.32.5
 tunnel-destination 168.61.x.x
 ike
  version      2
  rekey        28800
  cipher-suite aes128-cbc-sha1
  group        2
  authentication-type
   pre-shared-key
    pre-shared-secret <PSK_HERE>
   !
  !
 !
 ipsec
  rekey                    3600
  replay-window            512
  cipher-suite             aes256-cbc-sha1
  perfect-forward-secrecy none
```

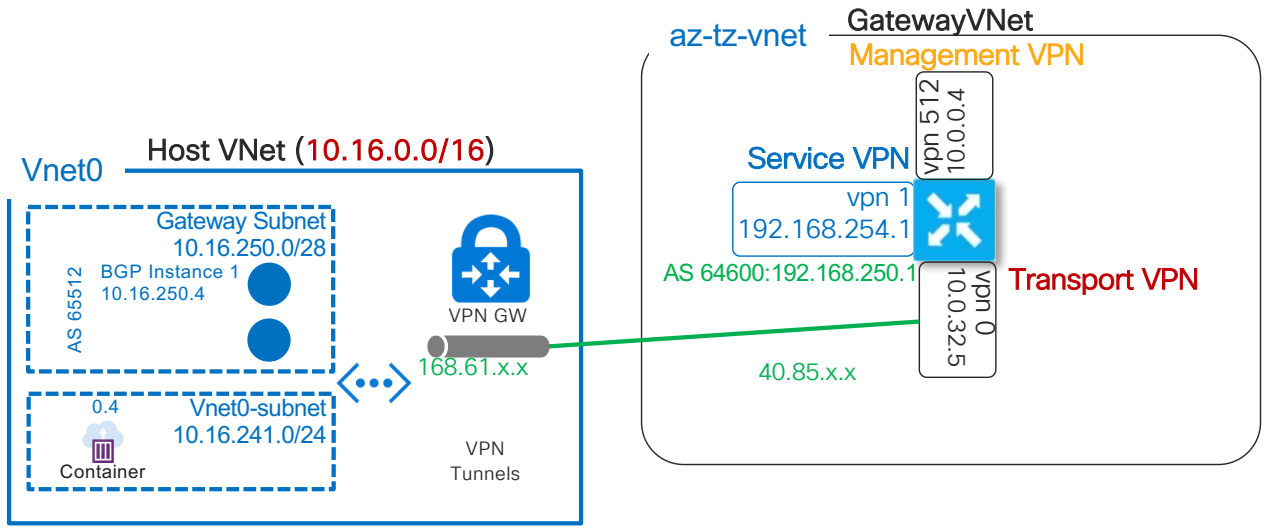


NAME	STATUS	PEER 1	PEER 2	IP ADDRESS 1	IP ADDRESS 2
COR_Vnet0_vpnConnection_vedge1_vng_ip_1	Connected	COR_Vnet0_Virtual_Network_Gateway	COR_Vnet0_LNG_vedge1	168.61.	40.85.
COR_Vnet0_vpnConnection_vedge2_vng_ip_2	Connected	COR_Vnet0_Virtual_Network_Gateway	COR_Vnet0_LNG_vedge2	168.61.	40.85.

Azure – Host Vnet –to- Transit VNet Mapping - BGP

vEdge-Cloud – Transit VNet

```
vpn 1
 router
  bgp 64600
   timers
    holdtime 30
   !
   address-family ipv4-unicast
    network 0.0.0.0/0
   !
   neighbor 10.16.250.4
    no shutdown
    remote-as      65512
    update-source ipsec9
    ebgp-multihop 2
```




```
# az network vnet-gateway list-advertised-routes --name COR_Vnet0_Virtual_Network_Gateway --peer 192.168.250.1 --output yaml
value:
- asPath: '65512'
  localAddress: 10.16.250.4
  network: 10.16.0.0/16
  nextHop: 10.16.250.4
  origin: Igp
  sourcePeer: null
```

Advertised

Received

```
transit-az-01# show ip route
OUTPUT OMITTED...

                                                PROTOCOL  NEXTHOP     NEXTHOP          NEXTHOP
VPN     PREFIX            PROTOCOL              SUB TYPE  IF NAME     ADDR             VPN      TLOC IP     COLOR            ENCAP   STATUS
-------------------------------------------------------------------------------------------------------------------------------------------
1       10.16.0.0/16      bgp                   i         -           10.16.250.4      -        -           -                -       F,S,R
```

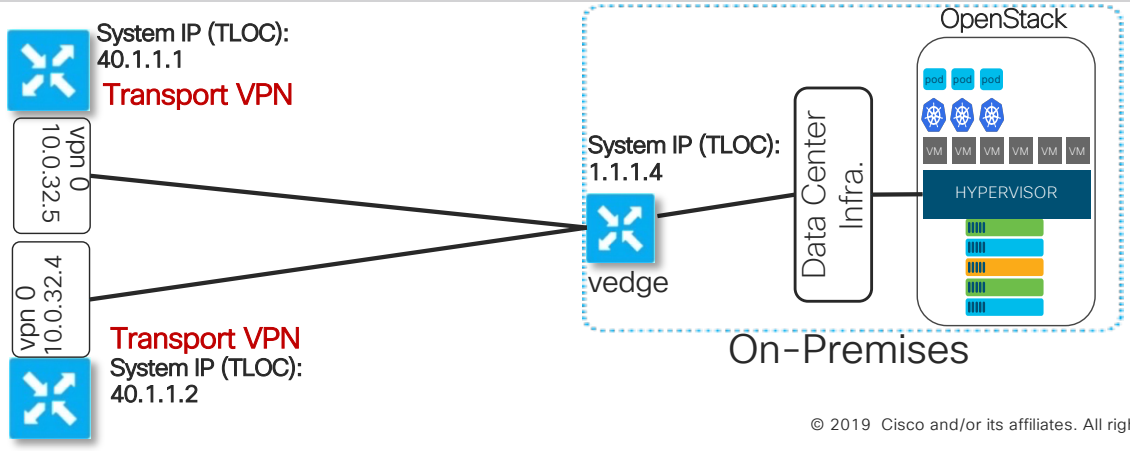
Transit VNet –to- On-Premises - IPsec

Transit VNet vEdge - IPsec

```
transit-az-01## show ipsec outbound-connections
OUTPUT SUMMARIZED...

SOURCE            SOURCE  DEST                          DEST                                    REMOTE            REMOTE            AUTHENTICATION
IP                PORT    IP                            PORT    SPI     TUNNEL MTU  TLOC ADDRESS  TLOC COLOR        USED
-------------------------------------------------------------------------------------------------------------------------------------------
10.0.32.5         12386   <ON_PREMISES_vEDGE_PUBLIC_IP>  12426   275     1441        1.1.1.4       public-internet   AH_SHA1_HMAC
```

On-Premises vEdge - IPsec

```
vedge-01# show ipsec outbound-connections
OUTPUT SUMMARIZED...

SOURCE                          SOURCE  DEST                 DEST                                    REMOTE            REMOTE            AUTHENTICATION
IP                              PORT    IP                   PORT    SPI     TUNNEL MTU  TLOC ADDRESS  TLOC COLOR        USED
-------------------------------------------------------------------------------------------------------------------------------------------
<ON_PREMISES_vEDGE_PUBLIC_IP>   12426   <TRANSIT-vEDGE-EIP>  12386   286     1441        40.1.1.1      default           AH_SHA1_HMAC
<ON_PREMISES_vEDGE_PUBLIC_IP>   12426   <TRANSIT-vEDGE-EIP>  12386   259     1441        40.1.1.2      default           AH_SHA1_HMAC
```



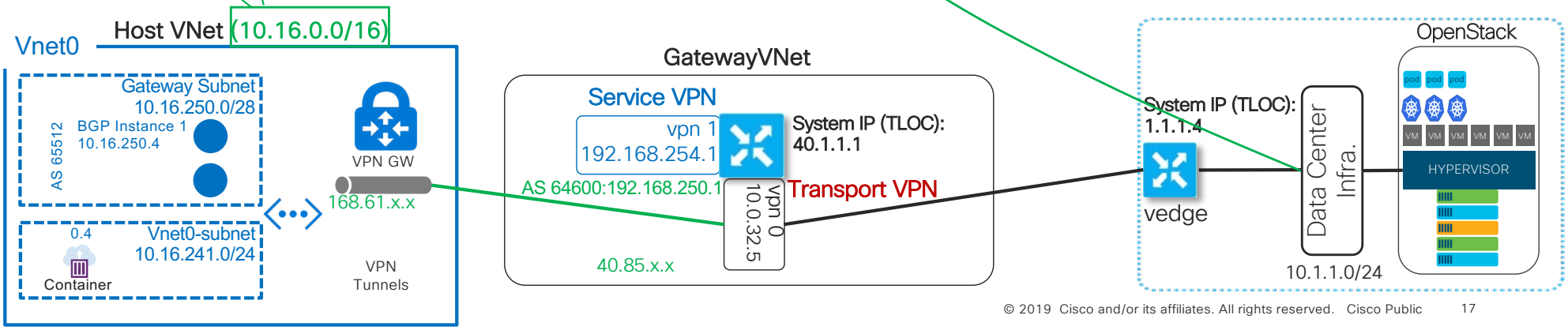
Transit VNet –to- On-Premises - BGP/OMP

Transit VNet vEdge - BGP/OMP

```
transit-az-01# show ip route
OUTPUT SUMMARIZED...

VPN     PREFIX              PROTOCOL    PROTOCOL  NEXTHOP    NEXTHOP      NEXTHOP  TLOC IP     COLOR            ENCAP   STATUS
                                        SUB TYPE  IF NAME    ADDR         VPN
-------------------------------------------------------------------------------------------------------------------------------
1       10.1.1.0/24         omp         -         -          -            -        1.1.1.4    public-internet  ipsec   F,S
1       10.16.0.0/16        bgp         i         -          10.16.250.4  -        -          -                -       F,S,R
```

On-Premises vEdge - Connected/OMP

```
vedge-01# show ip route
OUTPUT SUMMARIZED...

VPN     PREFIX              PROTOCOL    PROTOCOL  NEXTHOP    NEXTHOP      NEXTHOP  TLOC IP     COLOR            ENCAP   STATUS
                                        SUB TYPE  IF NAME    ADDR         VPN
-------------------------------------------------------------------------------------------------------------------------------
1       10.1.1.0/24         connected   -         ge0/1      -            -        -          -                -       F,S
1       10.16.0.0/16        omp         -         -          -            -        40.1.1.1   default          ipsec   F,S
1       10.16.0.0/16        omp         -         -          -            -        40.1.1.2   default          ipsec   F,S
```



Verify Routing and Reachability

... Output summarized

On an on-premises OpenStack VM, ping the container that is running in the public cloud (10.16.241.4)

```
[centos@os-vm1 ~]$ ping 10.16.241.4
PING 10.16.241.4 (10.16.241.4): 56 data bytes
64 bytes from 10.16.241.4: seq=1 ttl=61 time=5.069 ms
64 bytes from 10.16.241.4: seq=2 ttl=61 time=4.446 ms
```

On the on-premises OpenStack VM, wget to the Azure Container Instance (10.16.241.4)

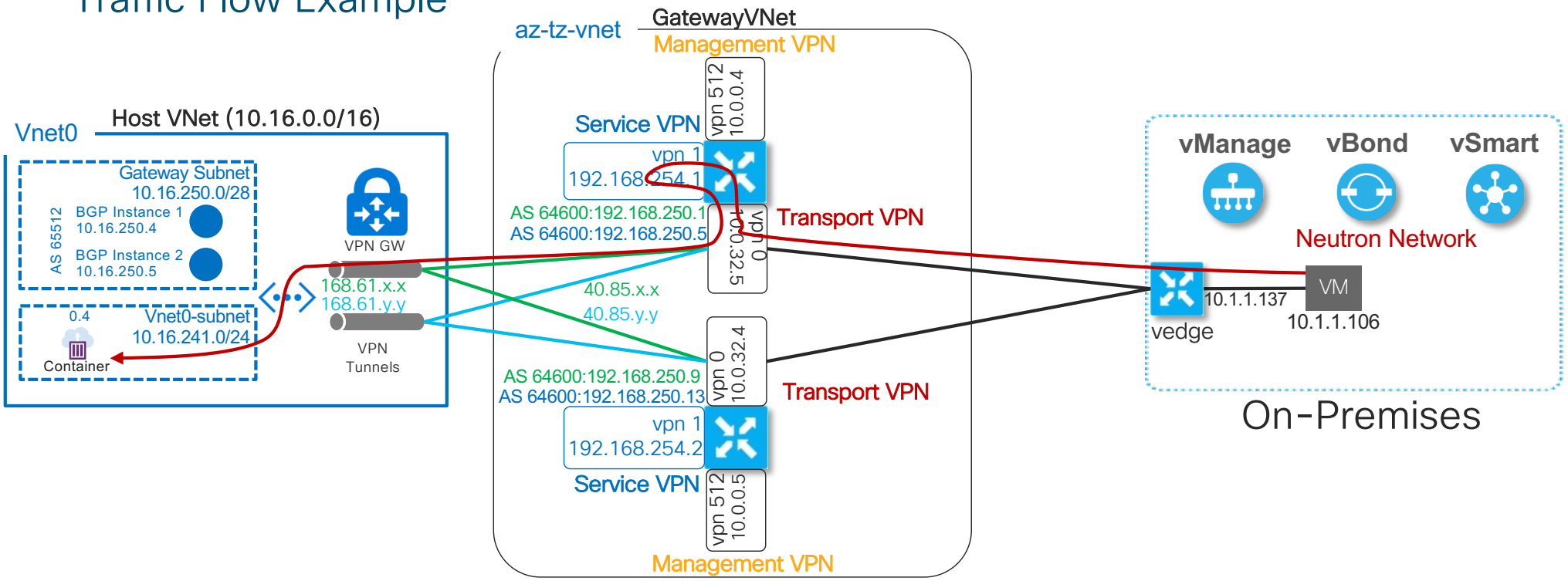
```
[centos@os-vm1 ~]$ wget -O - http://10.16.241.4
Connecting to 10.16.241.4 (10.16.241.4:80)
<html>
<head>
  <title>Welcome to Azure Container Instances!</title>
```

From the public cloud container watch the connection log from the on-premises OpenStack VM **(10.1.1.106)**

```
# az container attach --resource-group CtoRG -n appcontainer
Container 'appcontainer' is in state 'Running'...
(count: 1) (last timestamp: 2019-03-26 18:18:20+00:00) pulling image "microsoft/aci-helloworld"
(count: 1) (last timestamp: 2019-03-26 18:18:26+00:00) Successfully pulled image "microsoft/aci-helloworld"
(count: 1) (last timestamp: 2019-03-26 18:18:29+00:00) Created container
(count: 1) (last timestamp: 2019-03-26 18:18:29+00:00) Started container

Start streaming logs:
listening on port 80
::ffff:10.1.1.106 - - [26/Mar/2019:20:48:44 +0000] "GET / HTTP/1.1" 200 1663 "-" "Wget"
::ffff:10.1.1.106 - - [26/Mar/2019:20:48:56 +0000] "GET / HTTP/1.1" 200 1663 "-" "Wget"
::ffff:10.1.1.106 - - [26/Mar/2019:21:09:24 +0000] "GET / HTTP/1.1" 200 1663 "-" "Wget"
```

Cisco SD-WAN CoR for Azure

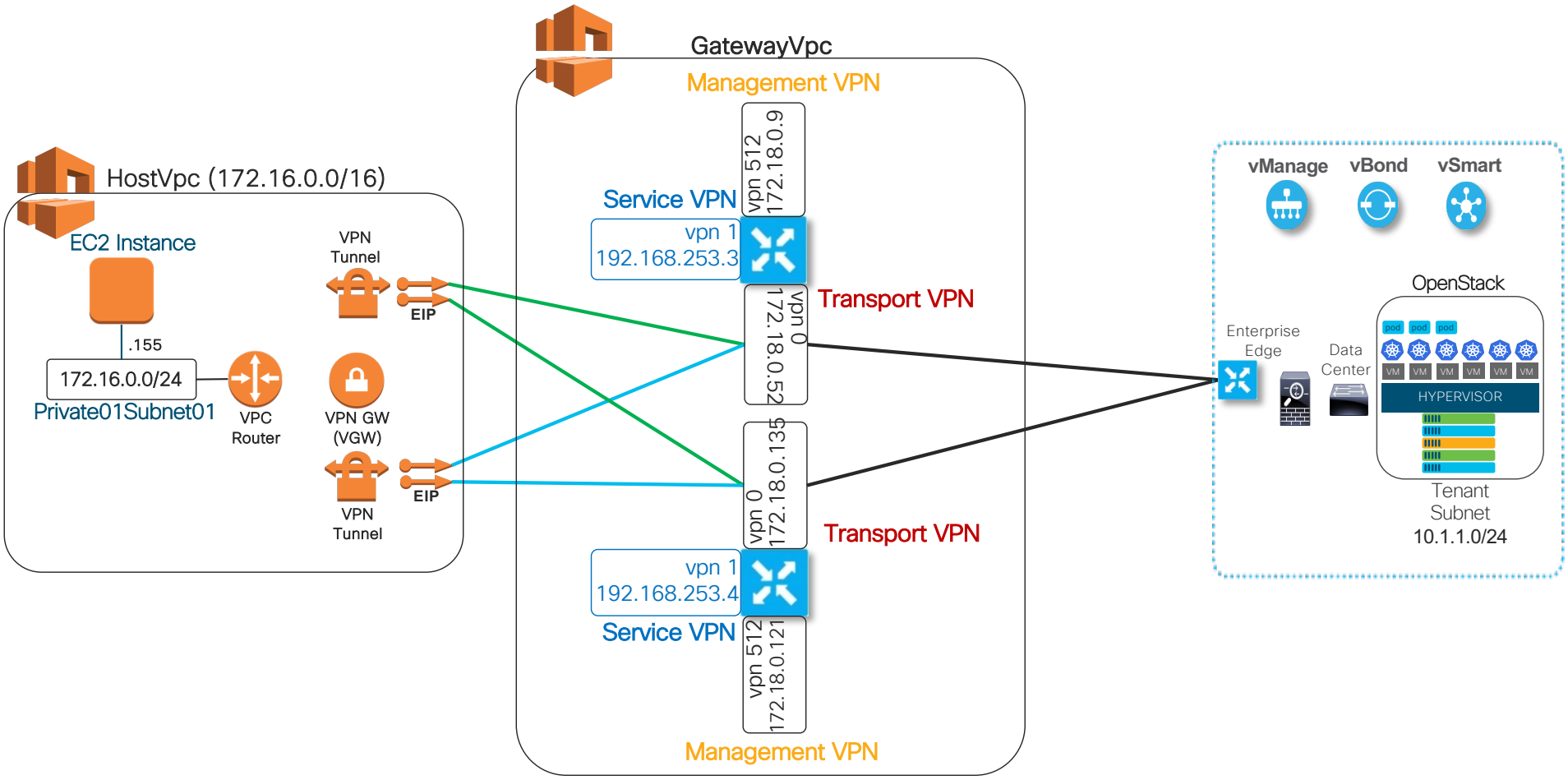
Traffic Flow Example




```
[centos@os-vm1 ~]$ traceroute 10.16.241.4 -n
traceroute to 10.16.241.4 (10.16.241.4), 30 hops max, 46 byte packets
 1  10.1.1.137  0.153 ms  0.202 ms  0.173 ms
 2  192.168.254.1  2.453 ms  2.535 ms  2.566 ms
 3  168.61.17.148  4.272 ms  3.467 ms  3.287 ms
 4  10.16.241.4  5.123 ms  4.123 ms  4.206 ms
```

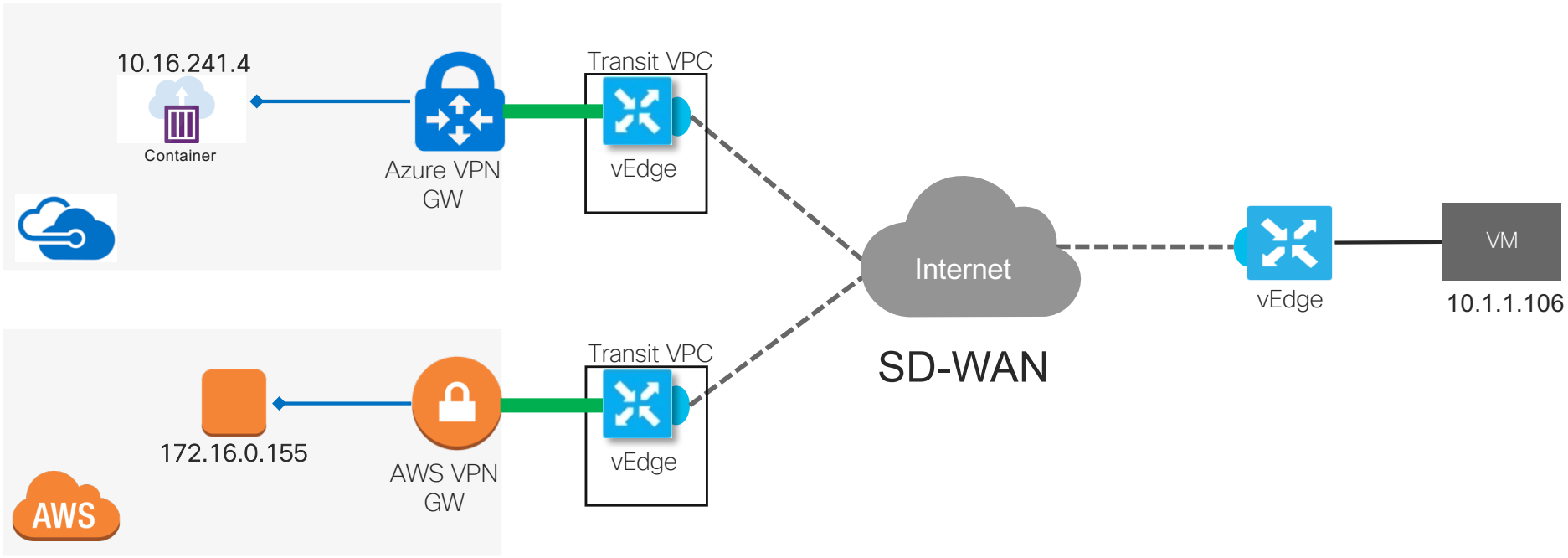
Cisco SD-WAN Cloud onRamp for IaaS – AWS

Cisco SD-WAN CoR for AWS



Link Them Altogether

Cisco SD-WAN and Multicloud



SD-WAN Multicloud Routing

Transit VNet vEdge - BGP

```
transit-az-01# show ip route
OUTPUT SUMMARIZED...
```

VPN	PREFIX	PROTOCOL	PROTOCOL SUB TYPE	NEXTHOP IF NAME	NEXTHOP ADDR	NEXTHOP VPN	TLOC IP	COLOR	ENCAP	STATUS
1	10.1.1.0/24	omp	-	-	-	-	1.1.1.4	public-internet	ipsec	F,S
1	10.16.0.0/16	bgp	i	-	10.16.250.4	-	-	-	-	F,S,R
1	172.16.0.0/16	omp	-	-	-	-	50.1.1.1	default	ipsec	F,S

Transit VPC vEdge - BGP

```
transit-aws-01# show ip route
OUTPUT SUMMARIZED...
```

VPN	PREFIX	PROTOCOL	PROTOCOL SUB TYPE	NEXTHOP IF NAME	NEXTHOP ADDR	NEXTHOP VPN	TLOC IP	COLOR	ENCAP	STATUS
1	10.1.1.0/24	omp	-	-	-	-	1.1.1.4	public-internet	ipsec	F,S
1	10.16.0.0/16	omp	-	-	-	-	40.1.1.1	default	ipsec	F,S
1	172.16.0.0/16	bgp	e	ipsec2	169.254.9.241	-	-	-	-	F,S

On-Premises vEdge - IPsec

```
vedge-01# show ip route
OUTPUT SUMMARIZED...
```

VPN	PREFIX	PROTOCOL	PROTOCOL SUB TYPE	NEXTHOP IF NAME	NEXTHOP ADDR	NEXTHOP VPN	TLOC IP	COLOR	ENCAP	STATUS
1	10.1.1.0/24	connected	-	ge0/1	-	-	-	-	-	F,S
1	10.16.0.0/16	omp	-	-	-	-	40.1.1.1	default	ipsec	F,S
1	172.16.0.0/16	omp	-	-	-	-	50.1.1.1	default	ipsec	F,S

Policies & Routing

Internet Exit Routing Considerations (1)

- By default, Cloud onRamp reconfigures the VPC/VNet route tables so that all traffic traverses the transit vEdges - Great for Enterprise InfoSec policies

Azure Route Table **Before** CoR:

```
PS Azure:\> Get-AzureRmEffectiveRouteTable -NetworkInterfaceName corvm444 -ResourceGroupName CtoRG | Format-Table

Name State  Source  AddressPrefix    NextHopType NextHopIpAddress
---- -----  ------  -------------    ----------- ----------------
     Active Default {10.16.0.0/16}   VnetLocal   {}
     Active Default {0.0.0.0/0}      Internet    {}
     Active Default {10.0.0.0/8}     None        {}
     Active Default {100.64.0.0/10}  None        {}
     Active Default {192.168.0.0/16} None        {}
```

Azure Route Table **After** CoR:

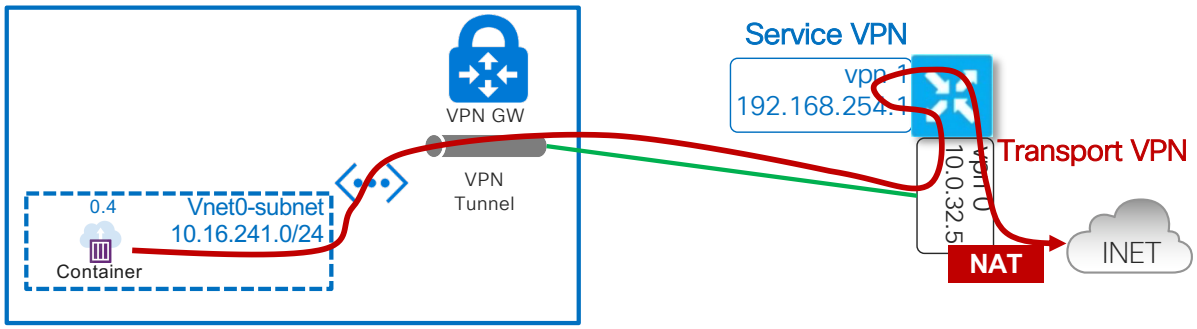
```
PS Azure:\> Get-AzureRmEffectiveRouteTable -NetworkInterfaceName corvm444 -ResourceGroupName CtoRG | Format-Table

Name State  Source                AddressPrefix        NextHopType           NextHopIpAddress
---- -----  ------                -------------        -----------           ----------------
     Active Default               {10.16.0.0/16}       VnetLocal             {}
     Active VirtualNetworkGateway {192.168.250.1/32}   VirtualNetworkGateway {10.16.250.4}
     Active VirtualNetworkGateway {192.168.250.9/32}   VirtualNetworkGateway {10.16.250.5}
     Active VirtualNetworkGateway {0.0.0.0/0}          VirtualNetworkGateway {10.16.250.4}
     Active VirtualNetworkGateway {0.0.0.0/0}          VirtualNetworkGateway {10.16.250.5}
```

Internet Exit Routing Considerations (2)

- If you want to have specific traffic or all non-on-premises traffic leave the transit vEdges directly:
  - https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.4/07Policy_Applications/04Using_a_vEdge_Router_as_a_NAT_Device/Configuring_Local_Internet_Exit
    - Perform NAT on a WAN/Transport VPN (e.g., VPN 0) for specific or all destinations not found in the transit routing table
    - Create a Data Policy to do NAT per-VPN for specific or all destinations not found in the transit routing table

Transit vEdge

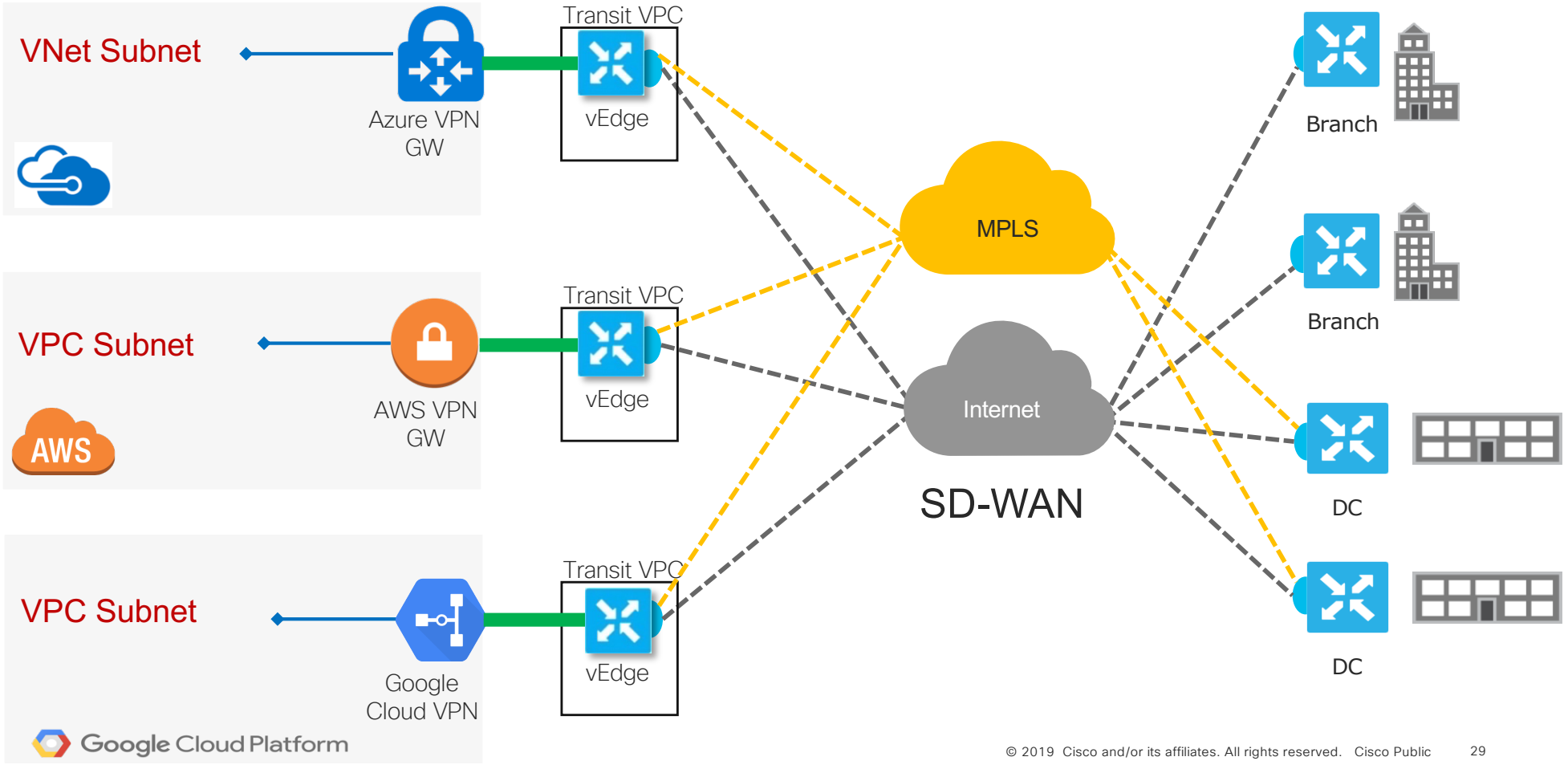
```
vpn 0
 interface ge0/0
  nat
!
vpn 1
 ip route 0.0.0.0/0 null0
 ip route x.x.x.x/32 vpn 0
```




```
transit-az-01# show ip route
                                                PROTOCOL  NEXTHOP     NEXTHOP   NEXTHOP
VPN    PREFIX              PROTOCOL             SUB TYPE  IF NAME     ADDR      VPN      TLOC IP    COLOR     ENCAP   STATUS
-------------------------------------------------------------------------------------------------------------------------------
1      x.x.x.x/32          nat                  -         ge0/0       -         0        -          -         -       F,S
```

Summary

Cisco SD-WAN and Multicloud



Reference

Cisco SD-WAN

Public Cloud Support

- Cisco SD-WAN (vEdge) on AWS: https://sdwan-docs.cisco.com/Product_Documentation/Getting_Started/Viptela_Overlay_Network_Bringup/07Deploy_the_vEdge_Routers/01Create_vEdge_Cloud_VM_Instance_on_AWS
- AWS Marketplace: https://aws.amazon.com/marketplace/pp/B07BZ53FJT
- Cisco SD-WAN on Microsoft Azure: https://sdwan-docs.cisco.com/Product_Documentation/Getting_Started/Viptela_Overlay_Network_Bringup/07Deploy_the_vEdge_Routers/02Create_vEdge_Cloud_VM_Instance_on_Azure
- Microsoft Azure Marketplace: https://azuremarketplace.microsoft.com/en-us/marketplace/apps/cisco.cisco_cloud_vedge_4_nics?tab=Overview
- Brand New SD-WAN Design/Deployment Guides: https://www.cisco.com/c/en/us/solutions/design-zone/networking-design-guides/branch-wan-edge.html

Summary

- There are many options for linking on-premises OpenStack workloads to other clouds
  - Leverage external components to do the work - Usually true when OpenStack operators don't 'own' the network design
  - Leverage external components to do the work and integrate with OpenStack - Ideal situation where you get automation from OpenStack and a solid external design/scale - Can we say "plugins?"
  - Deploy native appliances/services inside OpenStack to do the work
- SD-WAN greatly simplifies the deployment and operation of a hybrid cloud
  - Zero-touch provisioning of infrastructure
  - Dynamic policy deployment feeds the 'where, when, how, what' of the design
  - Leverage built-in features such as WAN optimization, transport failover, health-checking, application monitoring, etc.


CISCO