Site2Cloud (S2C)

WWW.AVIATRIX.COM

Solutions Engineering

Agenda

- Site2Cloud Overview
- Site2Cloud Use Cases
    1. High Speed DC Connectivity with Backup VPN
    2. Shared Services Multi-Tenant Architecture (aka SaaS Provider)
    3. Overlapping IP Space Scenarios
- Other Services to Connect to External Networks
- SD-WAN Integration

aviatrix

Overview

What is Site2Cloud?

- Connection from Public Cloud to:
  - On-Prem DC
  - 3rd Party Appliances, SD-WAN
  - Branch
  - Clouds Native Constructs (VPCs/VNets/VCNs)
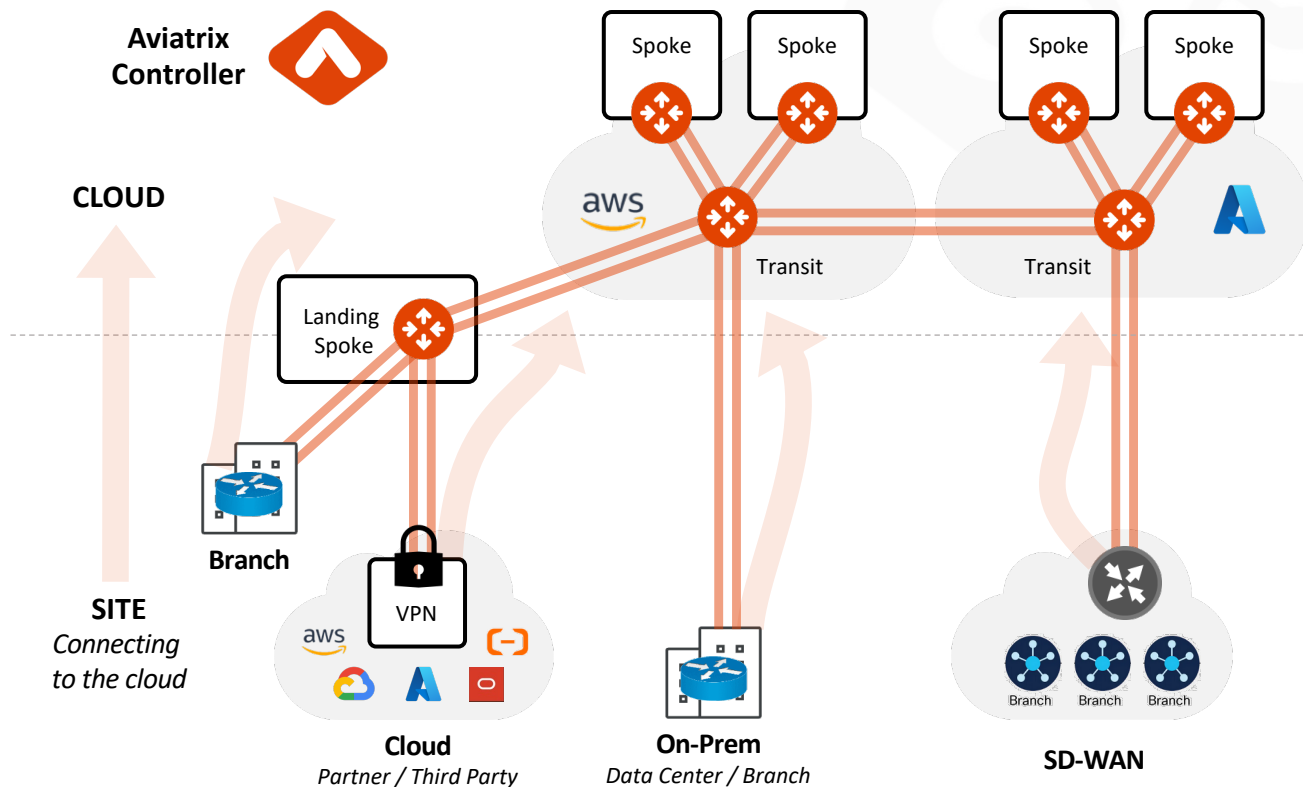
Site2Cloud Landing Options
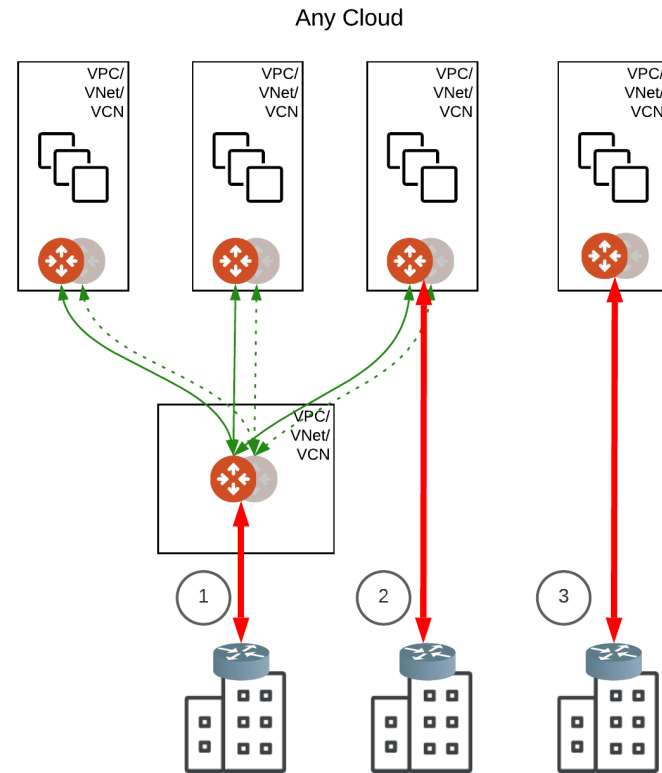
1. **Transit Gateway**
   - Route redistribution to other connected networks (automatic or upon approval)
   - Basic NAT support
   - BGP support
   - Segmentation support for external connections
   - Active/Active or Active/Standby

2. **Spoke Gateway**
   - Option to easily redistribute routes to other networks
   - Advanced NAT support (Mapped NAT)
   - BGP supported as of 6.6
   - Active/Standby or Active/Active

3. **"Standalone" Gateway (with Second Gateway)**
   - Advanced NAT support
   - No support for BGP
   - Active/Active or Active/Standby

Any Cloud

Use Cases

High Speed DC Connectivity with Backup VPN

High Speed DC Connectivity with Backup VPN

- Connecting on-prem data centers to the cloud via route-based Site2Cloud + BGP control plane, landing on Transit gateways

- Primary Site2Cloud is using private IPs to leverage the DX underlay

- Backup Site2Cloud is using public IPs to use the public Internet as underlay

- On both connections, ECMP can be enabled for Active/Active high performance or disabled (typically if on-prem has stateful firewalls)

- On-prem router is performing AS-path prepend on VPN routes advertised to Aviatrix transit over the VPN connection, to force Transit gateways to send traffic via the DX connection

- Additionally, on-prem router would use Weight or Local Pref, etc., to send traffic to the DX connection

- If DX connection goes down, traffic would automatically failover to Backup connection

- Branch connectivity is following a similar BGP-based Site2Cloud to Transit gateways, but it is typically only via VPN over the public Internet
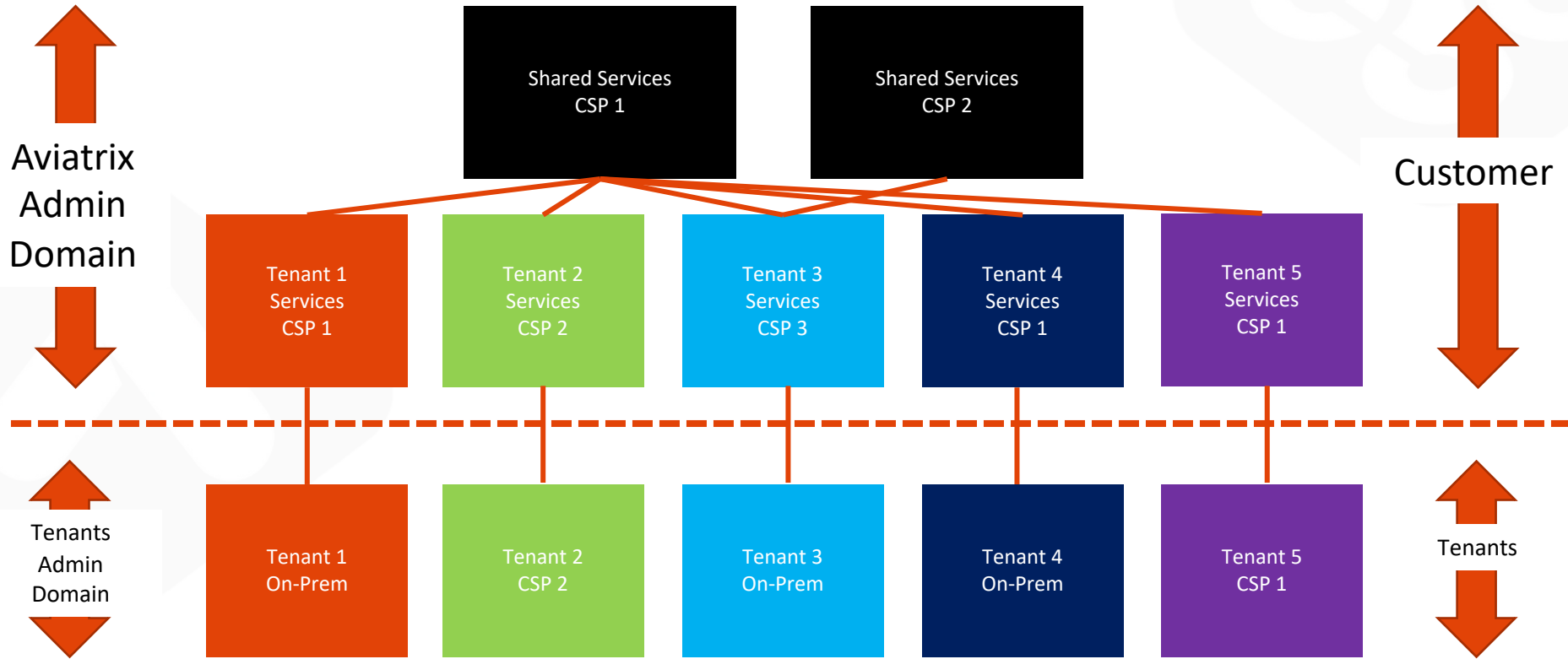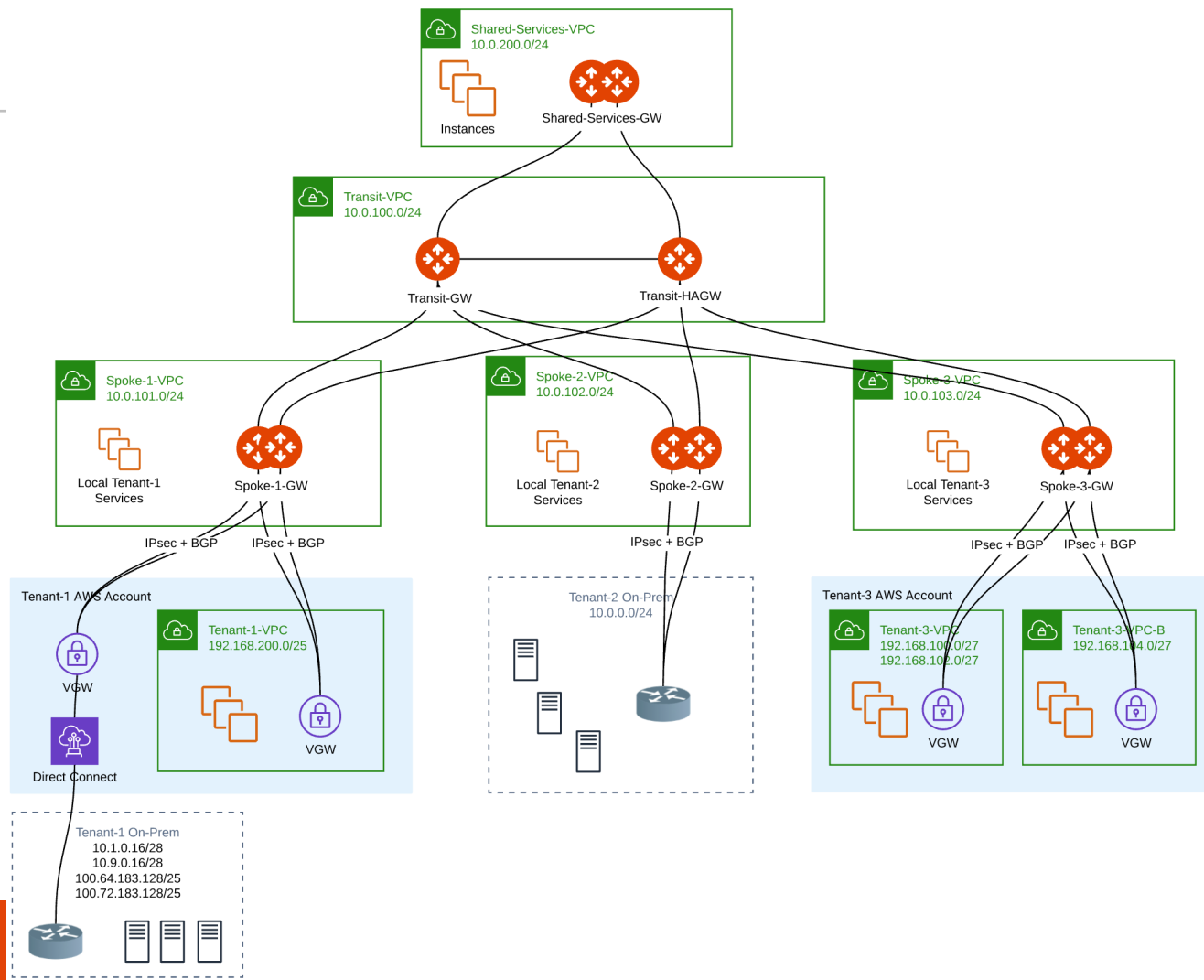

aviatrix
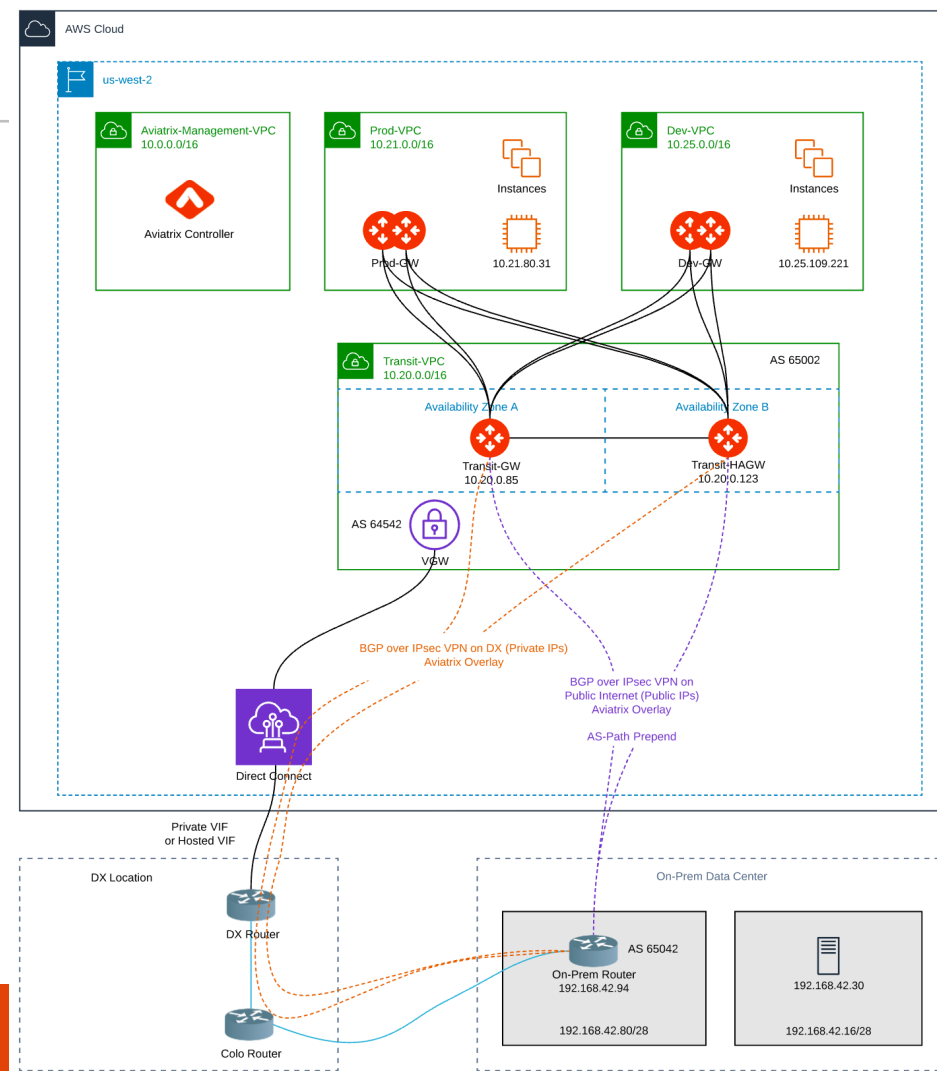
SaaS High-Level Architecture

Requirements and Solution

1. Connect a large number of tenants (1000+)
   - Distribute the tenants across Spoke gateways, for horizontal scaling and blast radius minimization
2. Provide both dedicated tenant services, and shared services
   - Host shared services in common Spoke VPCs
   - Host dedicated services in tenant-specific Spoke VPCs
3. Onboard the tenants with BGP: dynamic control plane that fits their operational model
   - Terminate BGP on the tenant Spoke gateways
4. Handle overlapping IPs across tenants, and between tenants and shared services
   - Use NAT on the tenant Spoke gateways
5. Maintain isolation across tenants
   - Use segmentation domains on the tenant Spoke gateways
6. Provide the highest throughput to tenant services
   - Horizontal scaling
   - Tenant services are directly hosted in the Spoke VPC where BGP terminates
   - They're directly accessed by tenants, without the Transit layer being a bottleneck
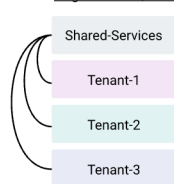
Typical Architecture
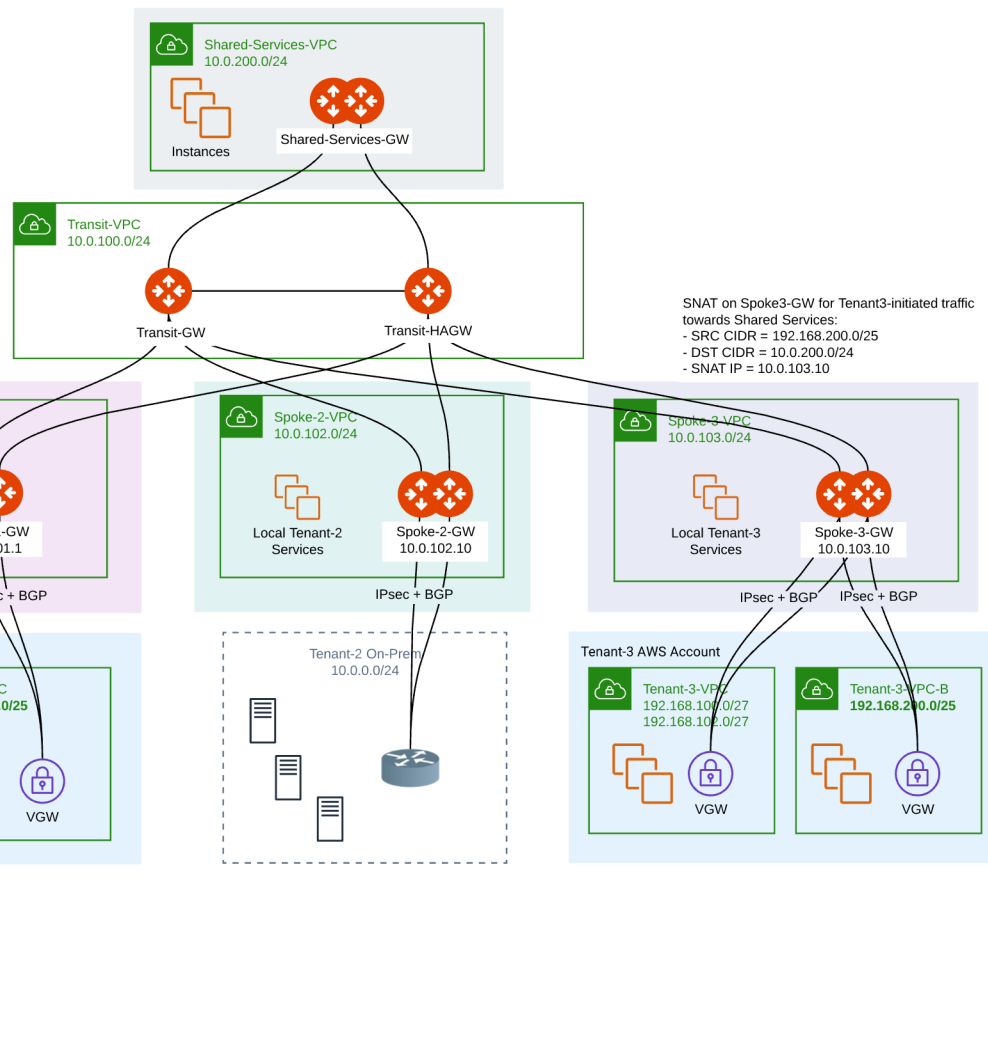
Segmentation and NAT Support

- SaaS Providers Aviatrix Validated Design https://aviatrix.com/resources/design-guides/aviatrix-validated-design-saas-providers-infrastructure

Segmentation Domains

- Shared-Services
- Tenant-1
- Tenant-2
- Tenant-3

Shared-Services-VPC 10.0.200.0/24
Instances
Shared-Services-GW

Transit-VPC 10.0.100.0/24
Transit-GW
Transit-HAGW

SNAT on Spoke1-GW for Tenant1-initiated traffic towards Shared Services:
- SRC CIDR = 192.168.200.0/25
- DST CIDR = 10.0.200.0/24
- SNAT IP = 10.0.101.10

SNAT on Spoke3-GW for Tenant3-initiated traffic towards Shared Services:
- SRC CIDR = 192.168.200.0/25
- DST CIDR = 10.0.200.0/24
- SNAT IP = 10.0.103.10

Spoke-1-VPC 10.0.101.0/24
Local Tenant-1 Services
Spoke-1-GW 10.0.101.1
IPsec + BGP   IPsec + BGP

Spoke-2-VPC 10.0.102.0/24
Local Tenant-2 Services
Spoke-2-GW 10.0.102.10
IPsec + BGP

Spoke-3-VPC 10.0.103.0/24
Local Tenant-3 Services
Spoke-3-GW 10.0.103.10
IPsec + BGP   IPsec + BGP

Tenant-1 AWS Account
VGW
Direct Connect
Tenant-1-VPC 192.168.200.0/25
VGW

Tenant-2 On-Prem 10.0.0.0/24

Tenant-3 AWS Account
Tenant-3-VPC 192.168.100.0/27 192.168.101.0/27
VGW
Tenant-3-VPC-B 192.168.200.0/25
VGW

Tenant-1 On-Prem
10.1.0.16/28
10.9.0.16/28
100.64.183.128/25
100.72.183.128/25

Use Cases

Overlapping IP Space Scenarios

SaaS Provider Scenario

- Tenants could be on-prem or in their own cloud environment, separate from the customer cloud environment
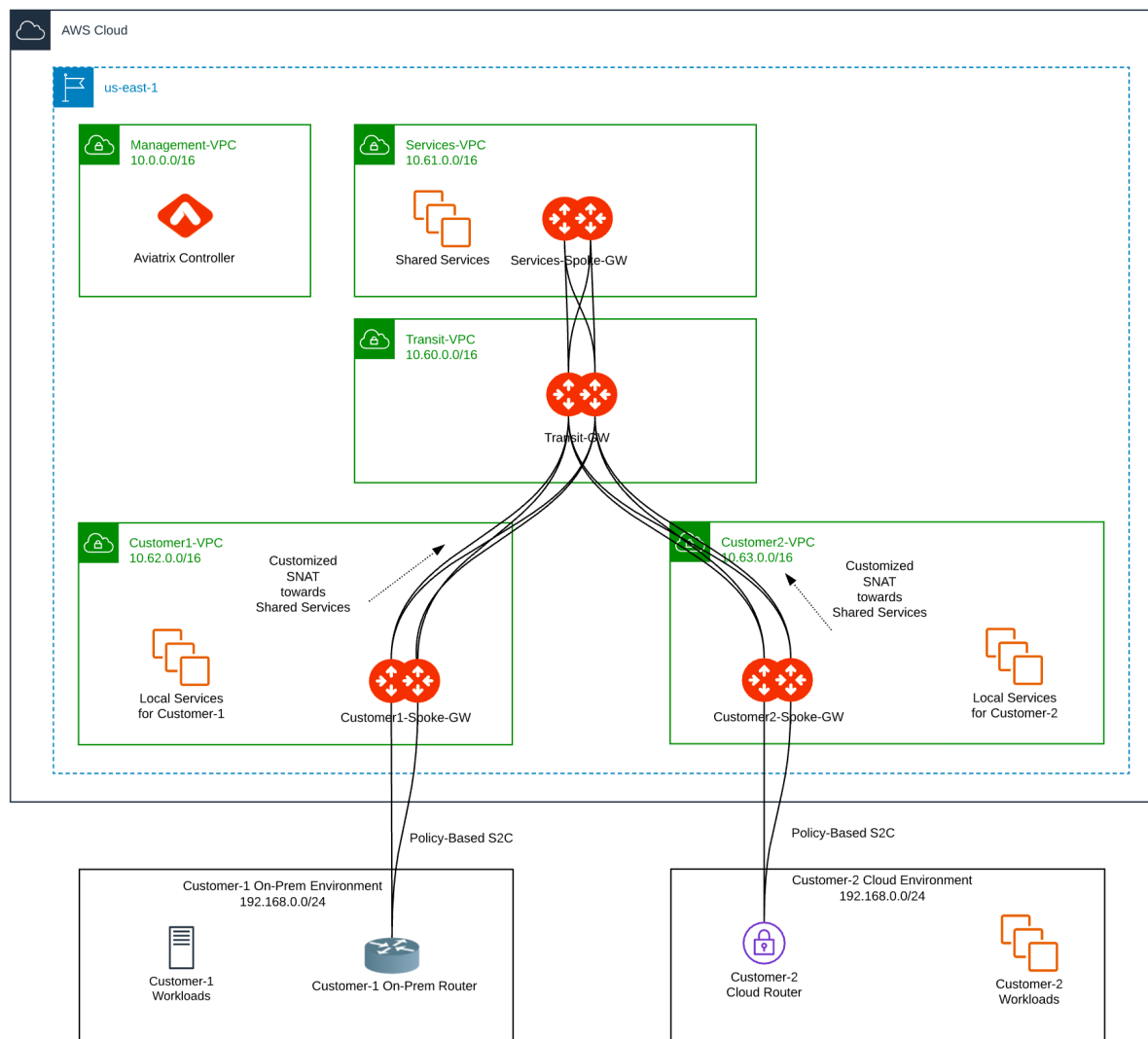
- Tenants are onboarded via policy-based or route-based Site2Cloud with static routing, landing on ActiveMesh spoke gateways

- They land in their own VPCs to handle overlapping IP scenarios and provide them local services

- Customized SNAT is used to uniquely differentiate incoming overlapping tenant traffic when communicating with shared services

AWS Cloud

us-east-1

Management-VPC
10.0.0.0/16

Aviatrix Controller

Services-VPC
10.61.0.0/16

Shared Services   Services-Spoke-GW

Transit-VPC
10.60.0.0/16

Transit-GW

Customer1-VPC
10.62.0.0/16

Customized
SNAT
towards
Shared Services

Local Services
for Customer-1

Customer1-Spoke-GW

Customer2-VPC
10.63.0.0/16

Customized
SNAT
towards
Shared Services

Customer2-Spoke-GW

Local Services
for Customer-2

Policy-Based S2C

Policy-Based S2C

Customer-1 On-Prem Environment
192.168.0.0/24

Customer-1
Workloads

Customer-1 On-Prem Router

Customer-2 Cloud Environment
192.168.0.0/24

Customer-2
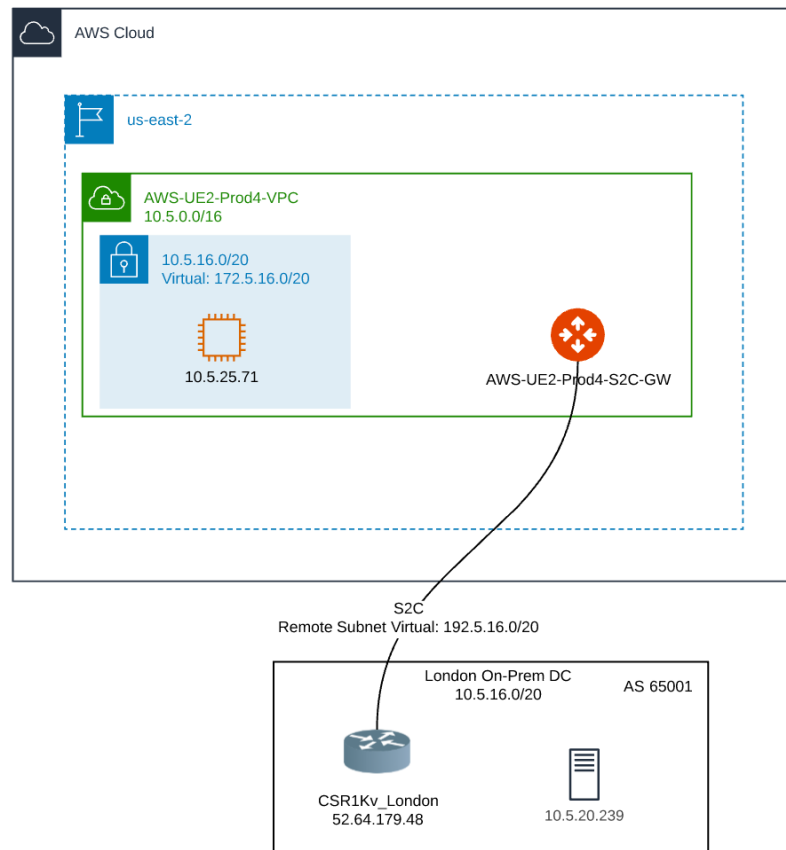Cloud Router

Customer-2
Workloads

Requirements

- Need to connect overlapping networks between the cloud and on-prem

- Don't want the on-prem router to implement any NAT

  - Keep it simple with no on-prem dependency

  - Many on-prem routers have no NAT, or very limited NAT

- The host information must be preserved

  - No NAT overload requirement anywhere

- The configuration must be simple and scalable
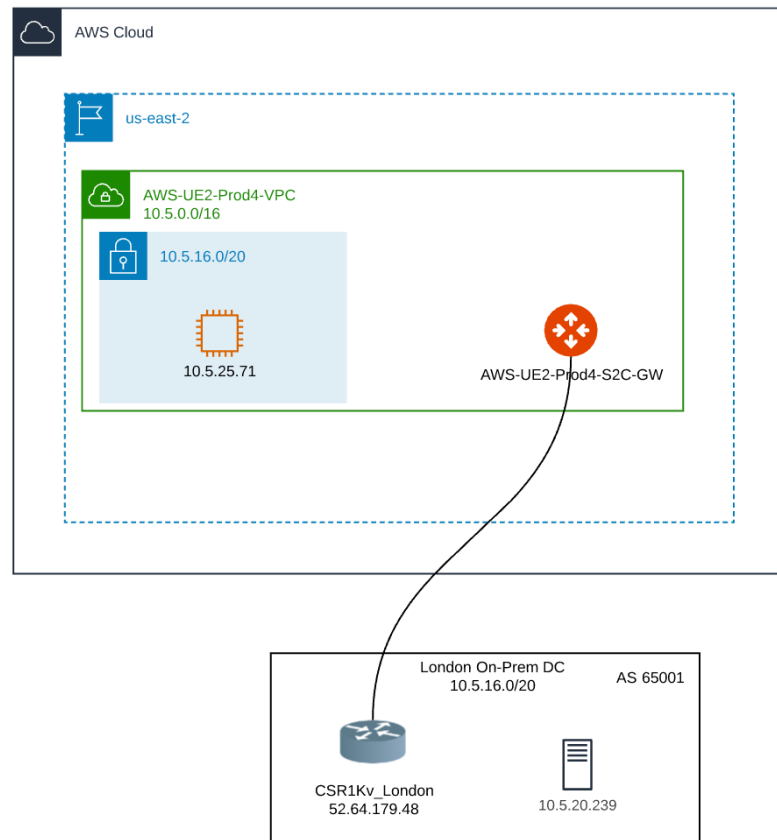
Solution – Mapped NAT with Route-Based Site2Cloud

- Virtual subnets, which are defined to be unique (not necessarily RFC1918), are used for communication between overlapping VPC and on-prem

- The Site2Cloud Gateway NATs between real subnets and virtual subnets, while preserving the host information in the IP

- There is no need for any on-prem NAT operations

- The configuration is extremely simple, and it does not require individual /32 NAT rules

- Route-based IPsec is required

AWS Cloud

us-east-2

AWS-UE2-Prod4-VPC
10.5.0.0/16

10.5.16.0/20
Virtual: 172.5.16.0/20

10.5.25.71

AWS-UE2-Prod4-S2C-GW

S2C
Remote Subnet Virtual: 192.5.16.0/20

London On-Prem DC
10.5.16.0/20   AS 65001

CSR1Kv_London
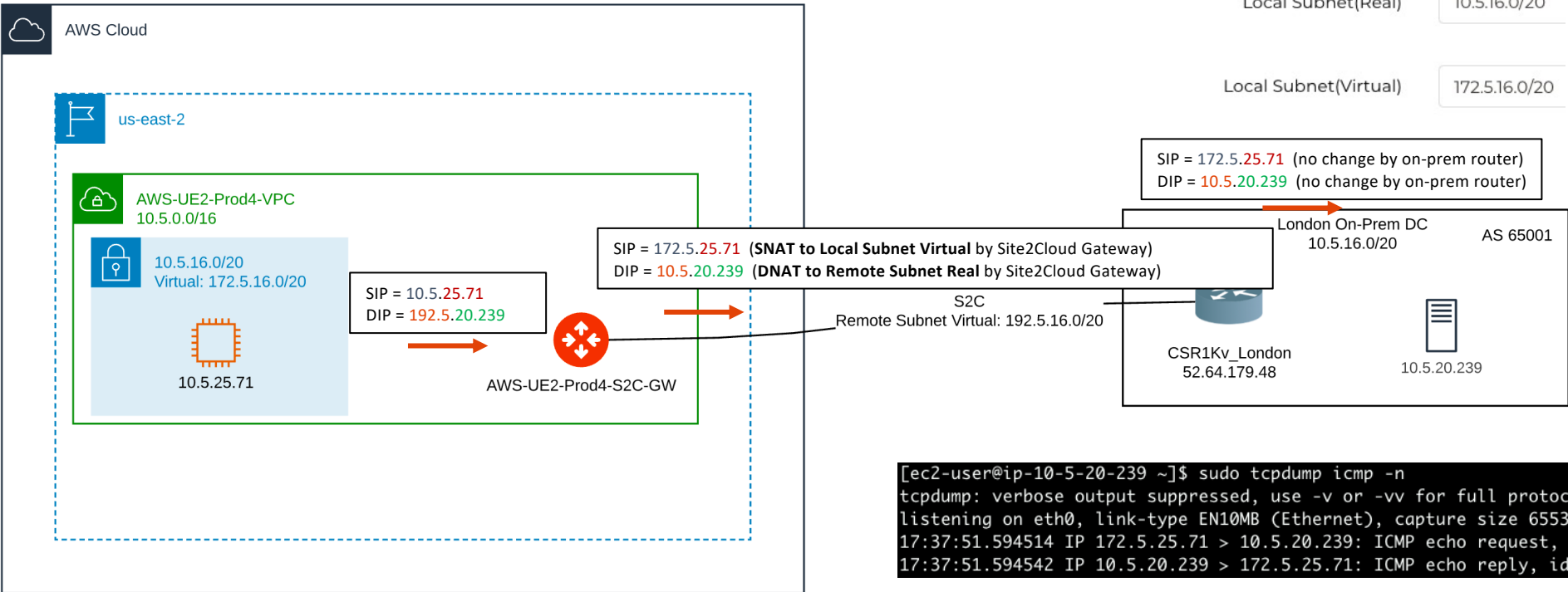52.64.179.48

10.5.20.239

aviatrix

Packet Walk

Remote Subnet (Real) — 10.5.16.0/20

Remote Subnet (Virtual) — 192.5.16.0/20

Local Subnet(Real) — 10.5.16.0/20
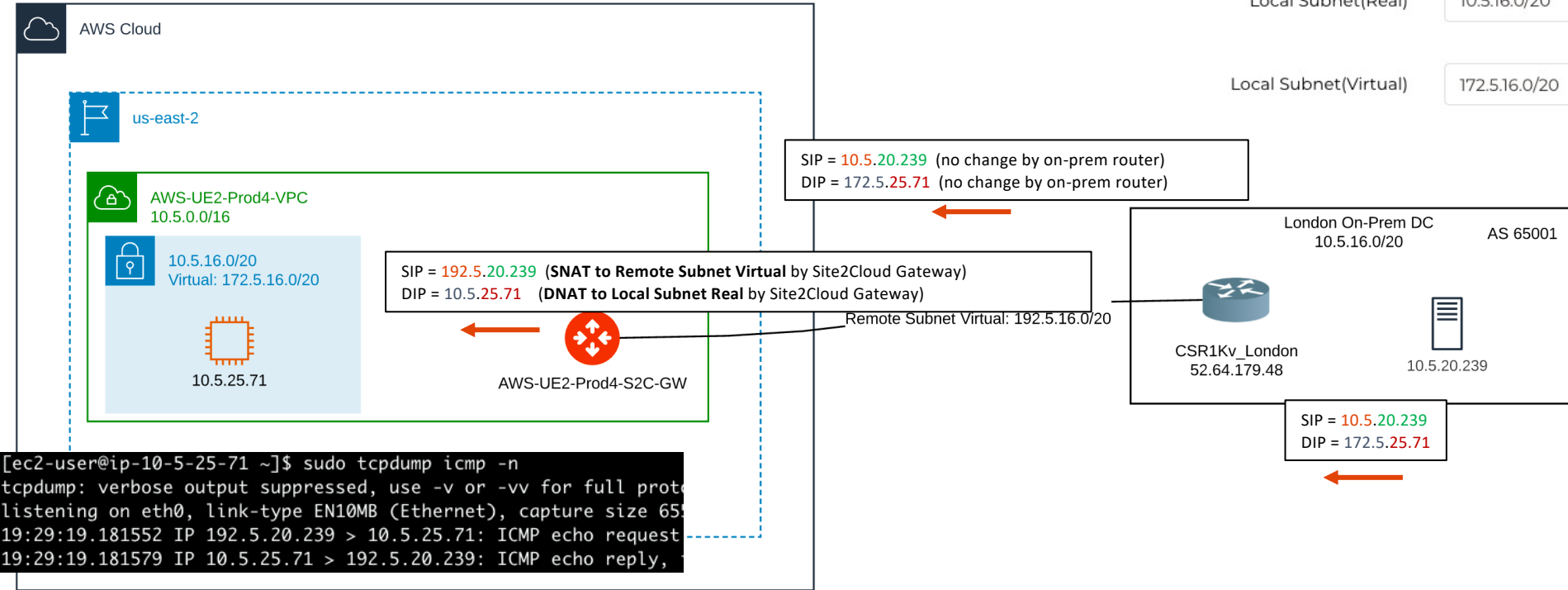
Local Subnet(Virtual) — 172.5.16.0/20

AWS Cloud

us-east-2

AWS-UE2-Prod4-VPC
10.5.0.0/16

10.5.16.0/20
Virtual: 172.5.16.0/20

10.5.25.71

SIP = 10.5.25.71
DIP = 192.5.20.239

AWS-UE2-Prod4-S2C-GW

SIP = 172.5.25.71 (**SNAT to Local Subnet Virtual** by Site2Cloud Gateway)
DIP = 10.5.20.239 (**DNAT to Remote Subnet Real** by Site2Cloud Gateway)

S2C
Remote Subnet Virtual: 192.5.16.0/20

SIP = 172.5.25.71 (no change by on-prem router)
DIP = 10.5.20.239 (no change by on-prem router)

London On-Prem DC
10.5.16.0/20   AS 65001

CSR1Kv_London
52.64.179.48

10.5.20.239

```
[ec2-user@ip-10-5-20-239 ~]$ sudo tcpdump icmp -n
tcpdump: verbose output suppressed, use -v or -vv for full protoco
listening on eth0, link-type EN10MB (Ethernet), capture size 6553
17:37:51.594514 IP 172.5.25.71 > 10.5.20.239: ICMP echo request,
17:37:51.594542 IP 10.5.20.239 > 172.5.25.71: ICMP echo reply, id
```

Packet Walk – Return Traffic

Remote Subnet (Real)	10.5.16.0/20
Remote Subnet (Virtual)	192.5.16.0/20
Local Subnet(Real)	10.5.16.0/20
Local Subnet(Virtual)	172.5.16.0/20

AWS Cloud

us-east-2

AWS-UE2-Prod4-VPC
10.5.0.0/16

10.5.16.0/20
Virtual: 172.5.16.0/20

10.5.25.71

AWS-UE2-Prod4-S2C-GW

SIP = 192.5.20.239 (**SNAT to Remote Subnet Virtual** by Site2Cloud Gateway)
DIP = 10.5.25.71   (**DNAT to Local Subnet Real** by Site2Cloud Gateway)

Remote Subnet Virtual: 192.5.16.0/20

SIP = 10.5.20.239 (no change by on-prem router)
DIP = 172.5.25.71 (no change by on-prem router)

London On-Prem DC
10.5.16.0/20   AS 65001

CSR1Kv_London
52.64.179.48   10.5.20.239

SIP = 10.5.20.239
DIP = 172.5.25.71

```
[ec2-user@ip-10-5-25-71 ~]$ sudo tcpdump icmp -n
tcpdump: verbose output suppressed, use -v or -vv for full proto
listening on eth0, link-type EN10MB (Ethernet), capture size 65!
19:29:19.181552 IP 192.5.20.239 > 10.5.25.71: ICMP echo request
19:29:19.181579 IP 10.5.25.71 > 192.5.20.239: ICMP echo reply, 1
```

aviatrix

Overlapping IP Use Cases for Site2Cloud – Reference

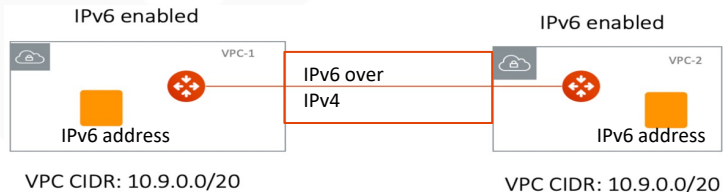## Overlapping CIDRs Within Cloud(s) or Directly to a VPC

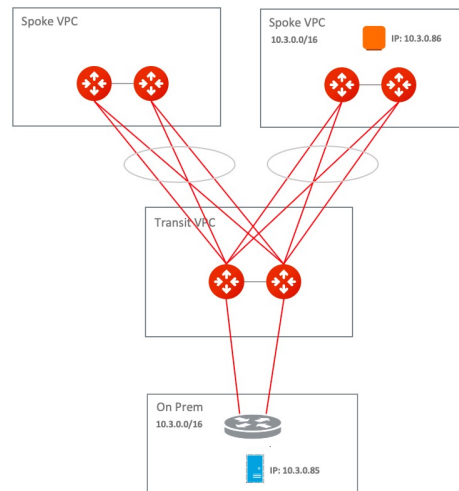https://docs.aviatrix.com/HowTos/connect_overlap_cidrs.html

instance-1: 10.17.4.179

Instance-2: 10.17.7.81

gateway-1: 52.10.222.115

gateway-2: 54.71.250.58

IPSEC encryption

VPC-1: 10.17.0.0/20

(On-prem): 10.17.0.0/20
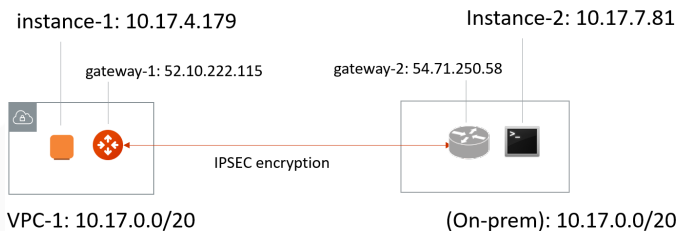
Use IPv6 to Connect Overlapping VPC CIDRs

https://docs.aviatrix.com/HowTos/ipv6_peering.html

IPv6 enabled

IPv6 enabled

VPC-1

VPC-2

IPv6 over IPv4

IPv6 address

IPv6 address

VPC CIDR: 10.9.0.0/20

VPC CIDR: 10.9.0.0/20

Requirement: EC2 instances can communicate with each other with IPv6

Aviatrix ActiveMesh with Customized SNAT and DNAT on Spoke Gateway

https://docs.aviatrix.com/HowTos/transit_solution_activemesh_spoke_snat_dnat_rfc1918.html

Spoke VPC

Spoke VPC
10.3.0.0/16   IP: 10.3.0.86

Transit VPC

On Prem
10.3.0.0/16

IP: 10.3.0.85

Other Overlapping IP CIDR Solutions

https://docs.aviatrix.com/HowTos/overlapping_network_solutions.html

Route Approval

BGP Route Approval

- Can explicitly approve any BGP-learned route from Partner or on-prem into the cloud network
- Prevents unwanted advertisement of routes such as 0/0 from Partner

1. New routes arrive at Transit Gateway
2. Transit Gateway reports new routes to Controller
3. Controller notifies admin via email
4. Admin logs in to Controller to approve
5. If approved, Controller programs the new routes to Spoke VPCs

- **Note:**
  - Route Approval completely blocks a BGP prefix to even be considered by control plane
  - Prefixes blocked are not even programmed in the Gateway route table

Spoke VPC/VNet
Spoke VPC/VNet
Aviatrix Controller
Transit VPC/VNet
Partner

From Aviatrix Controller: Route Approval Request

NR no-reply@aviatrix.com
To
ⓘ We removed extra line breaks from this message.

Time Detected: 2022-03-01 17:27:36.709787

Request approval for new learned CIDR(s):

Gateway: transit, Connection: onprem_to_transit-1, CIDRs(1): 0.0.0.0/0

To approve, please login to the Aviatrix Controller and go to Multi-Cloud Transit-> Approval.

Controller IP:
Controller Name: AWS Controller 6.6
Controller Version: UserConnect-6.6.5224 Time Detected: 2022-03-01 17:27:36.710310

Aviatrix Edge

Introducing Aviatrix Edge

The only multi-cloud native platform with enterprise-grade visibility and control for public cloud and the edge
Aviatrix software in multiple form factors providing consistent network, security, and visibility to the edge.
Edge locations appear and behave as another VPC/VNET with spoke and transit capabilities.
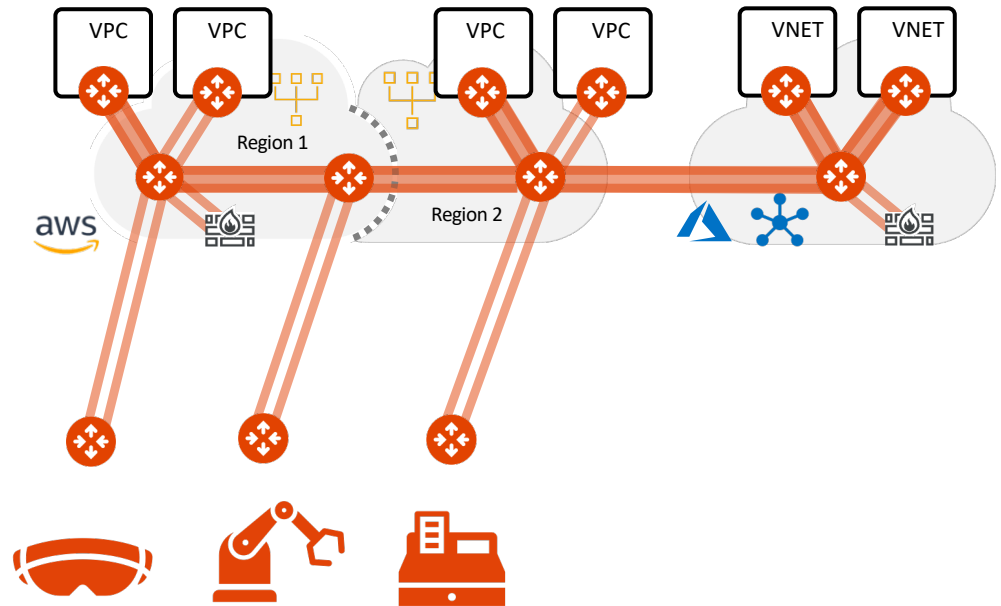
Cloud Out Architecture
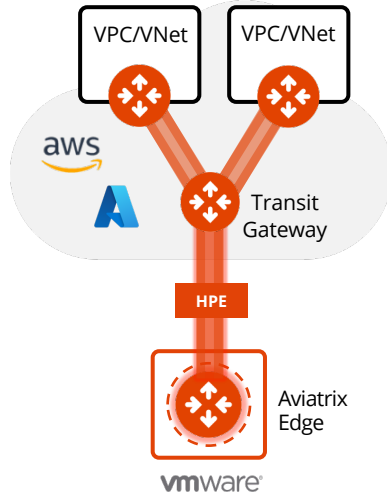
Simplified Edge Management
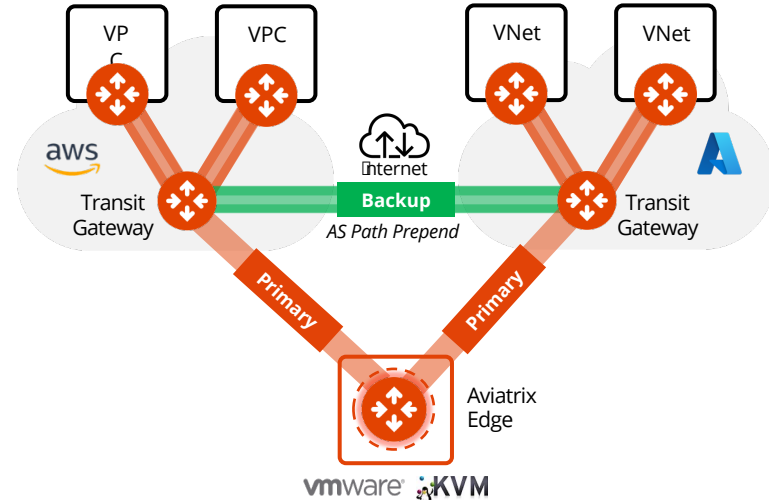
Consistent Secure Edge

Simplified Edge On-boarding

Aviatrix Edge Use Cases

Extend the Aviatrix Platform to the Edge

Multi-Cloud Connectivity via Aviatrix Edge

Edge 2.0 Deployment Workflow - Demo

1 Create ZTP for Edge

Aviatrix Controller

Create and download ZTP .iso

Aviatrix Admin

2 Deploy Edge virtual machine and attach ZTP .iso

.ov — vmware
.qcow — KVM

Aviatrix Controller

Deploy Edge

Attach ZTP .iso

Aviatrix Edge

vmware KVM

Registration

3 Attach Edge to Transit

Aviatrix Controller

Transit Gateway

Attach to Transit

Aviatrix Edge

4 Connect Edge to External Device (LAN Router)

Aviatrix Controller

Transit Gateway

Aviatrix Edge

BGP over LAN

BGP

LAN Router

Other Services to Connect to External Networks

Connections to External Device

- I**Psec** (discussed already)

- **BGP over GRE** (AWS only)

  - Extends Aviatrix overlay to external networks without encryption, and without IPsec speed limitations

  - Useful for AWS DX

- **BGP over LAN**

  - Route exchange without any tunneling protocol

  - High-performance, widely compatible SD-WAN integration

 - Integrates with GCP Network Connectivity Center (NCC)
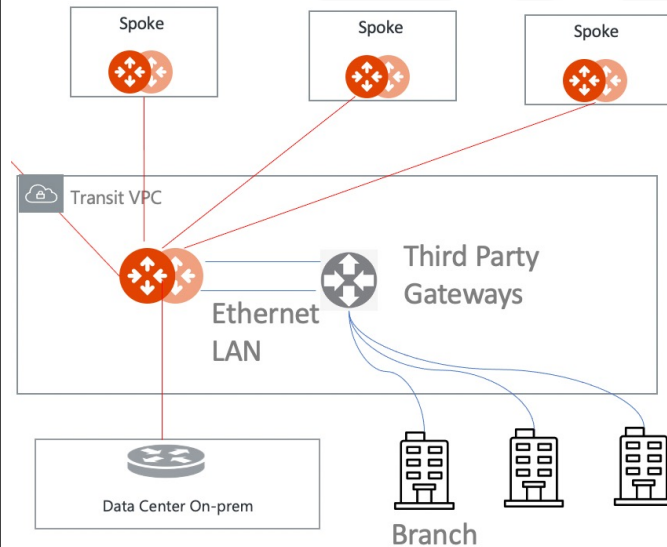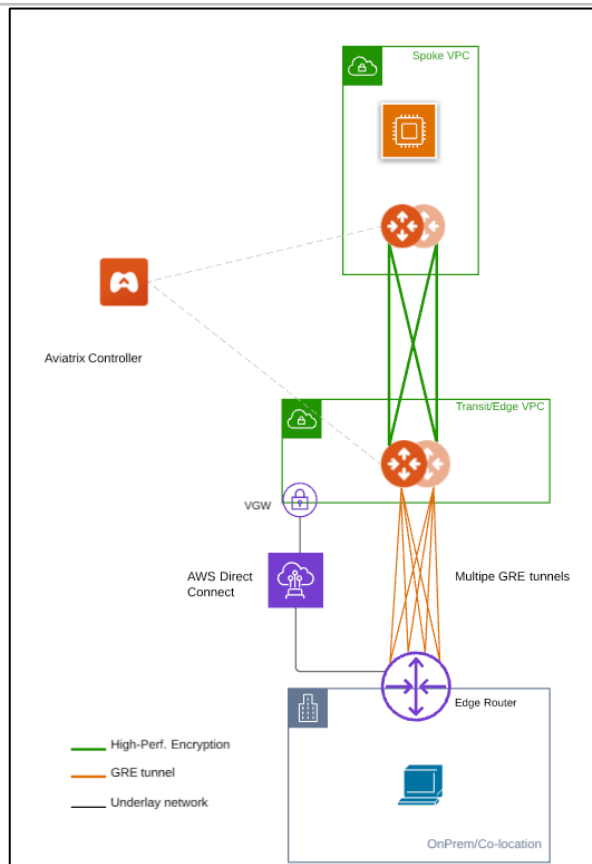
SD-WAN Integration

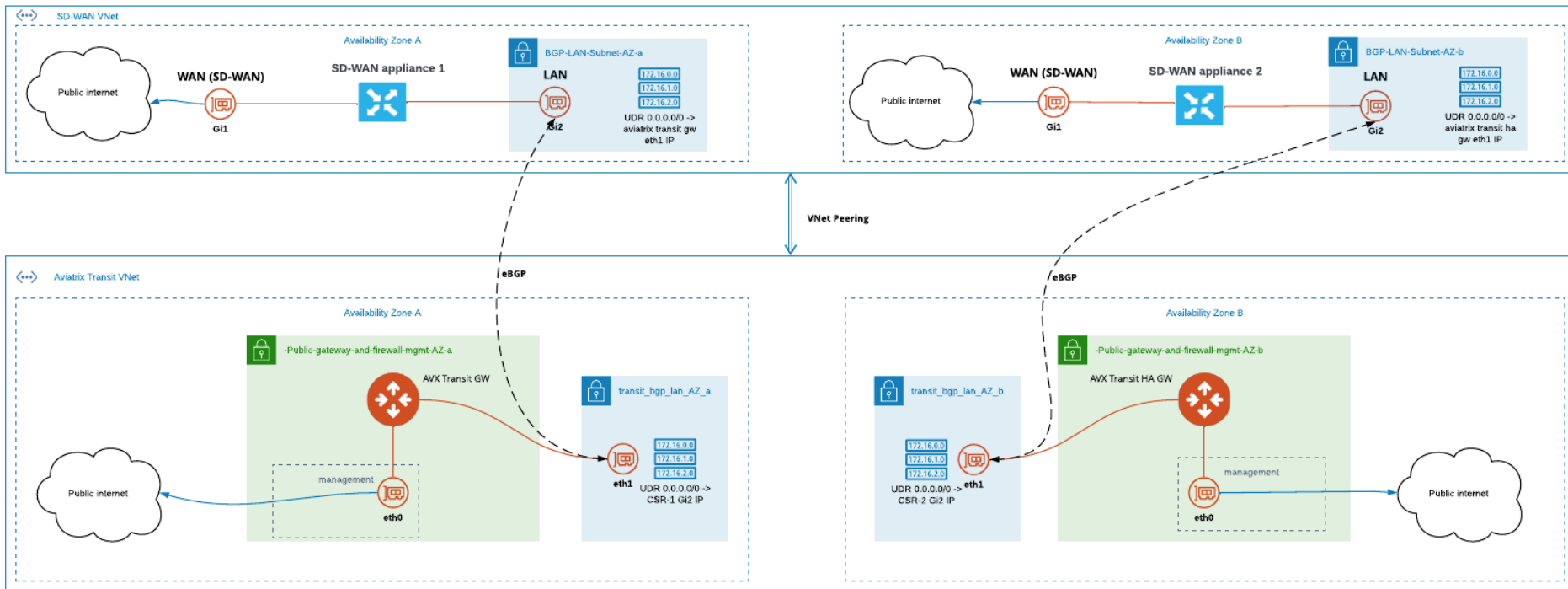# Solution – SD-WAN integration with Aviatrix

- BGP based integration with SD-WAN cloud instances
  - BGP over IPsec
  - BGP over LAN
  - BGP over GRE
- Service chaining by inspecting traffic with Next Gen Firewalls
- Advanced Traffic Engineering and Filtering options
- All other Aviatrix benefits apply

BGP over LAN in AWS
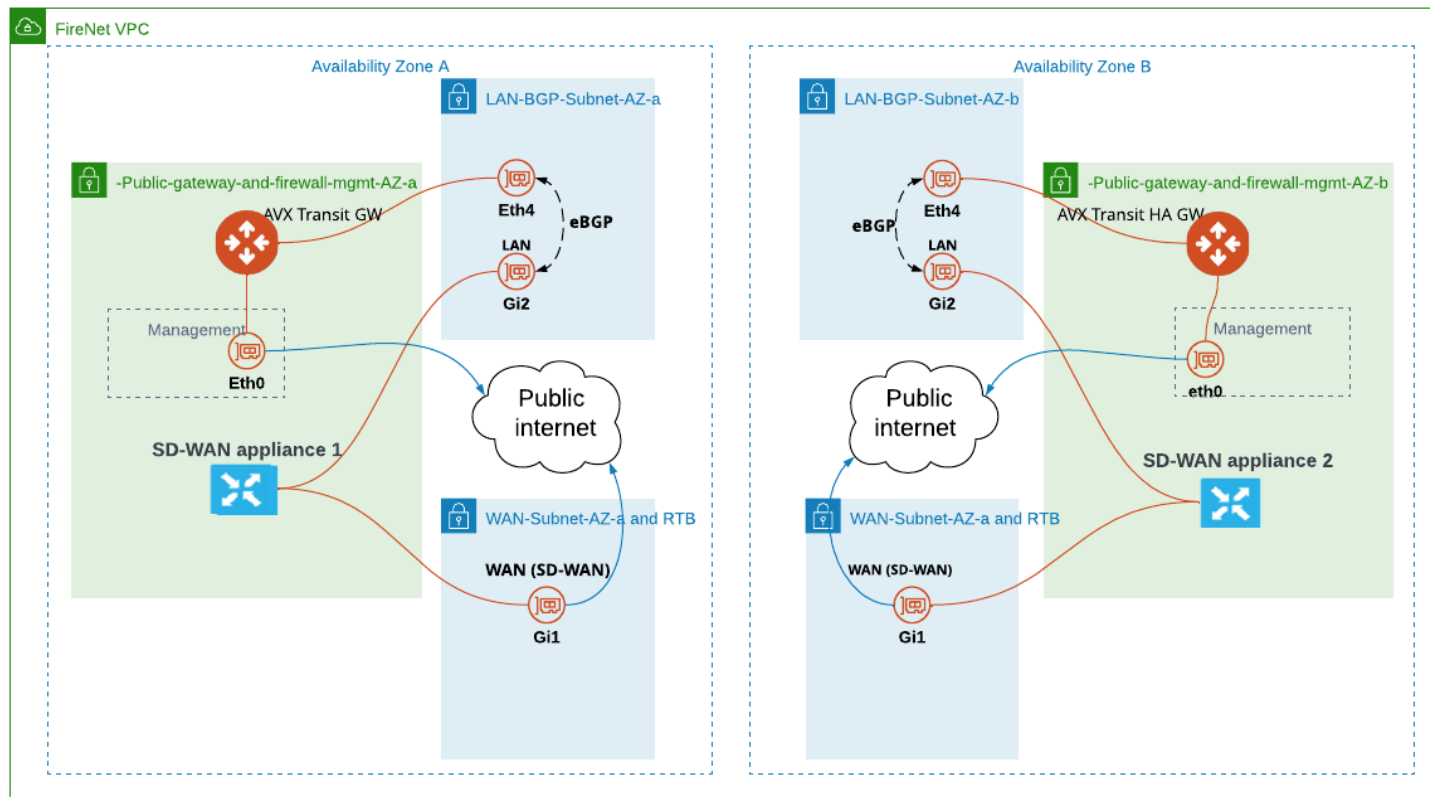
BGP over LAN in Azure

Next: Lab 8 – Site2Cloud