Site2Cloud (S2C) and Edge

ACE Solutions Architecture Team

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

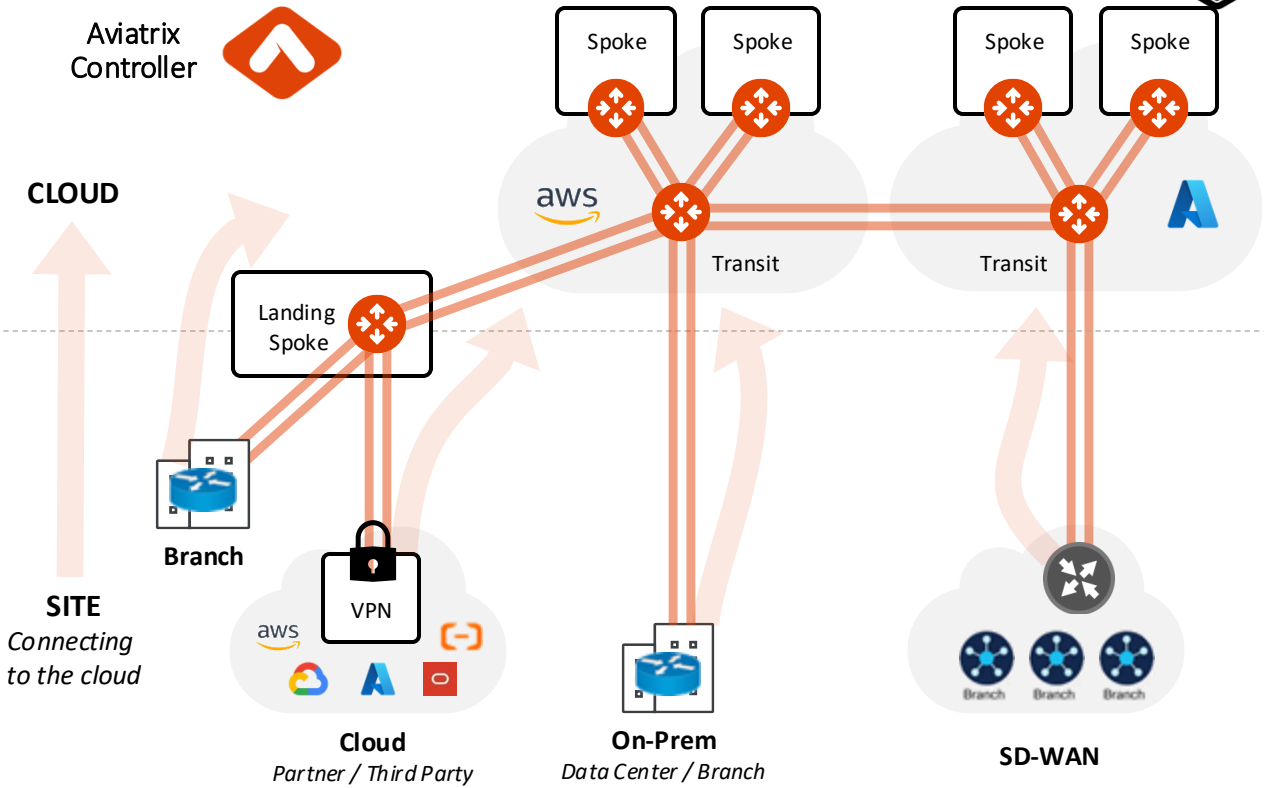
Other Services to Connect to External Networks

SD-WAN Integration

Overview

What is Site2Cloud?

- Connection from Public Cloud to:
  - On-Prem DC
  - 3rd Party Appliances, SD-WAN
  - Branch
  - Clouds Native Constructs (VPCs/VNets/VCNs)

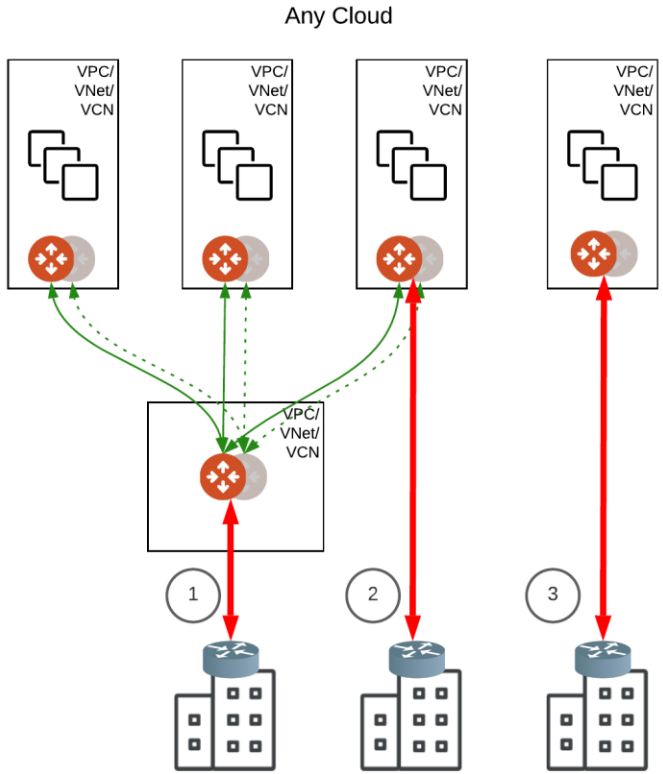


Site2Cloud Landing Options

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

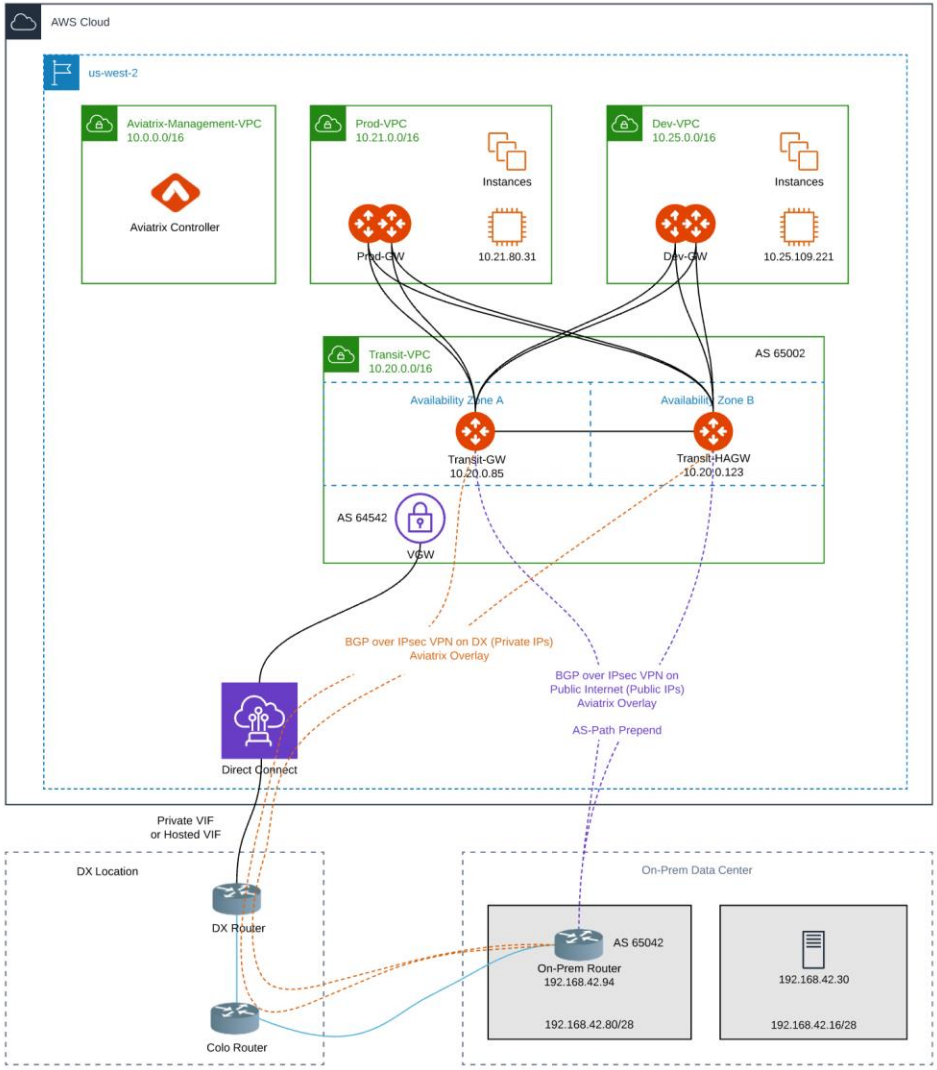


Use Cases

High Speed DC Connectivity with Backup VPN

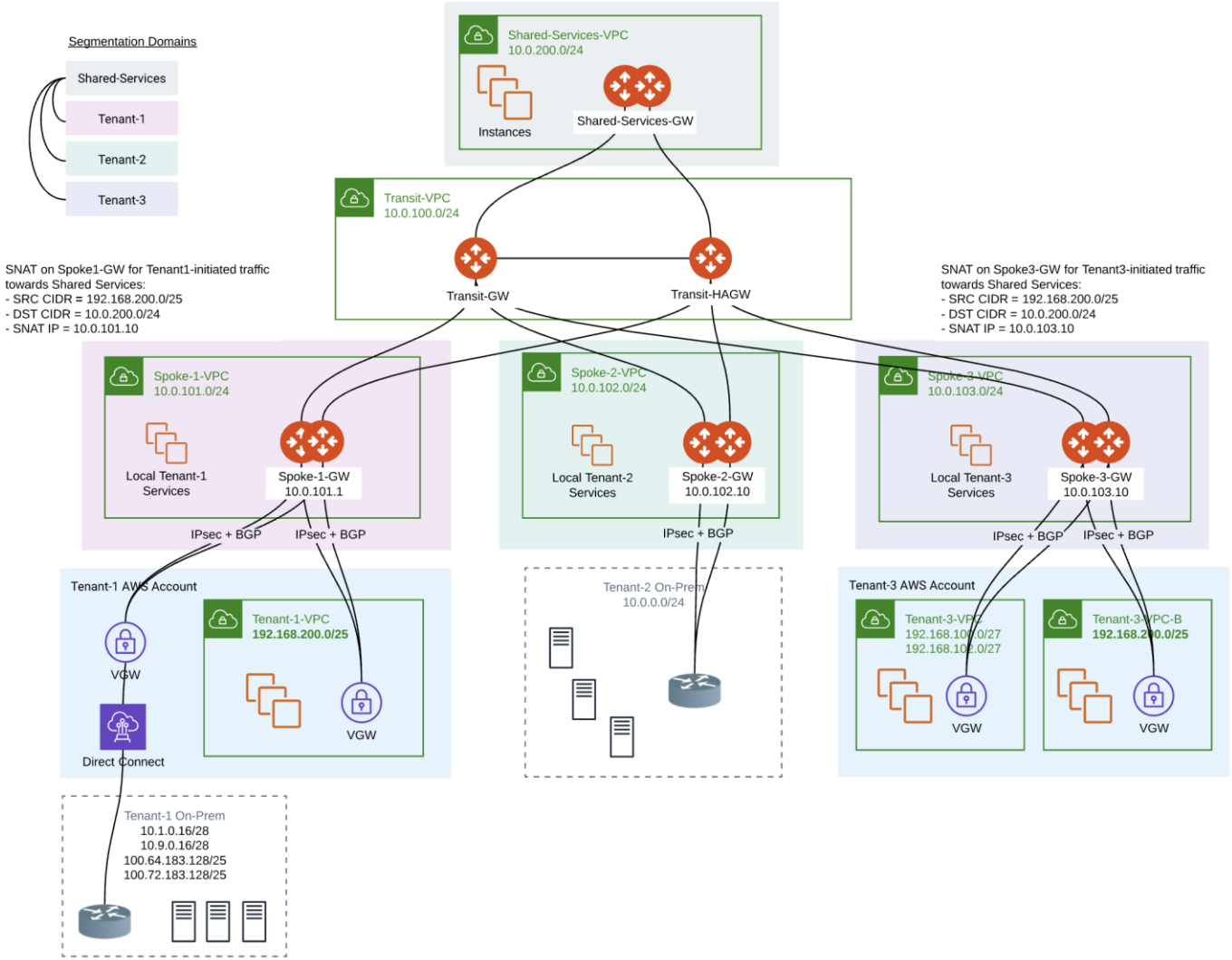
High Speed DC Connectivity with Backup VPN

- 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



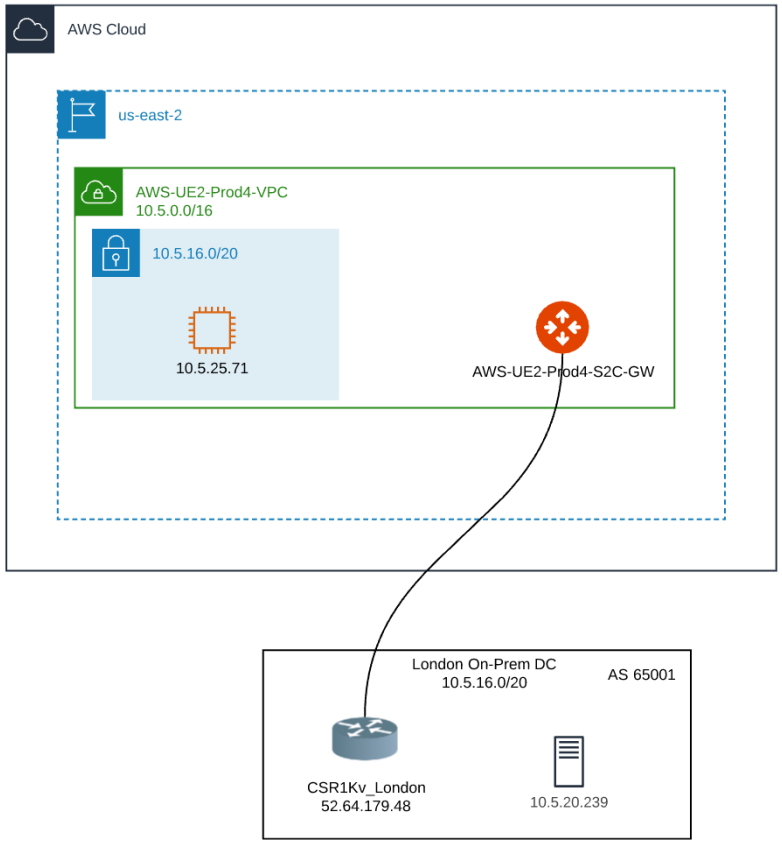
Segmentation and NAT Support

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



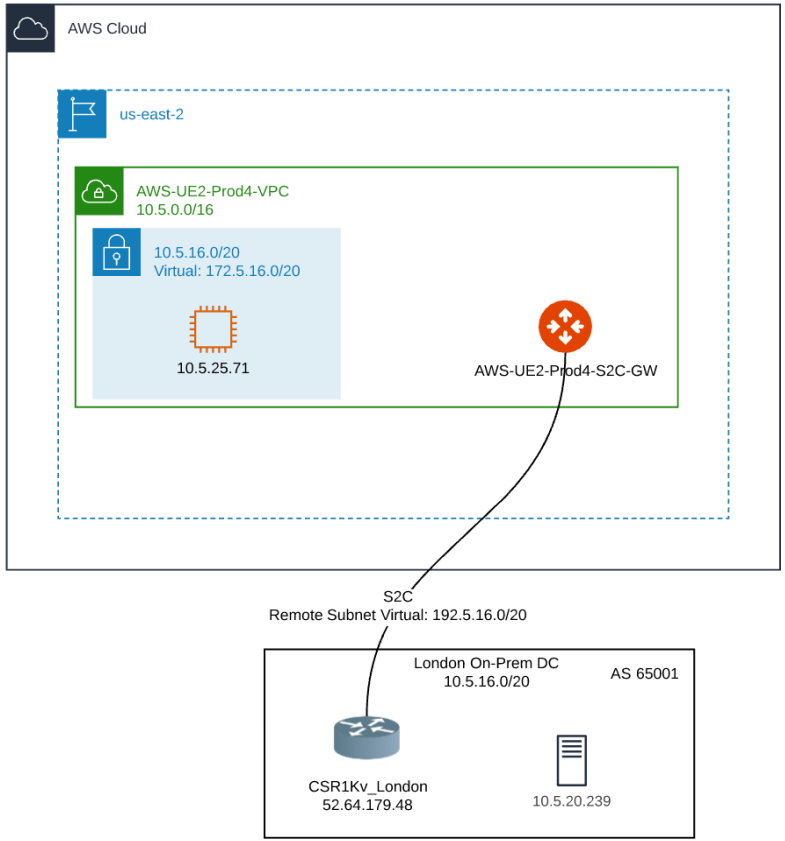
Requirements

- 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



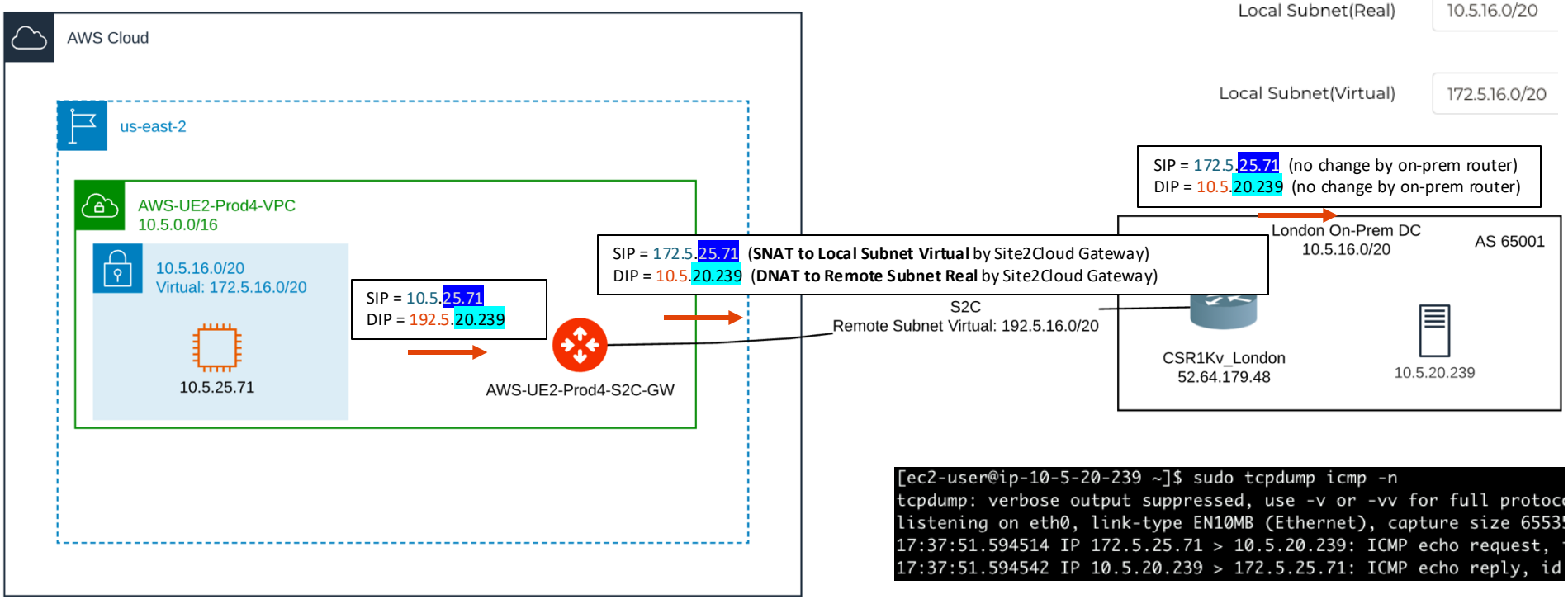
Solution – Mapped NAT with Route-Based Site2Cloud

- 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
- It works with both Route-based and Policy-based IPsec



Packet Walk

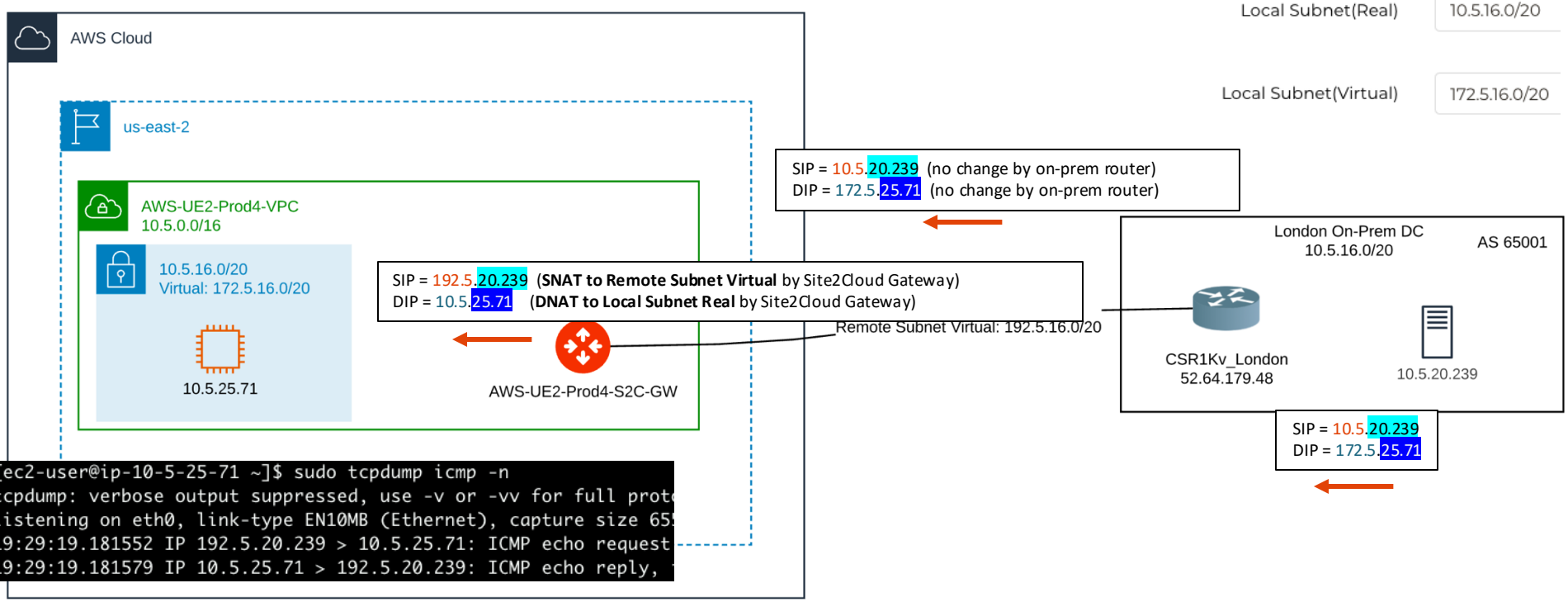
Remote Subnet (Real)	10.5.16.0/20
Remote Subnet (Virtual)	192.5.16.0/20
Local Subnet(Real)	10.5.16.0/20
Local Subnet(Virtual)	172.5.16.0/20




```
[ec2-user@ip-10-5-20-239 ~]$ sudo tcpdump icmp -n
tcpdump: verbose output suppressed, use -v or -vv for full protoc
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



Download the External Connection Configuration

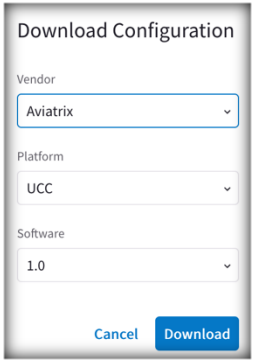
Automatic External Connection Template

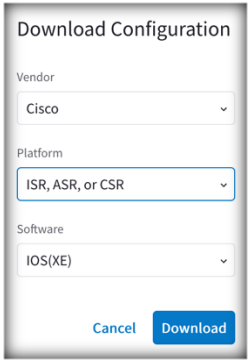
A ***remote site configuration template*** can be generated from the CoPilot.

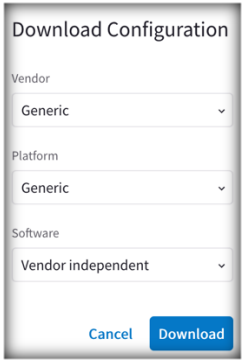
- This template file contains the *gateway public IP address*, *VPC/VNet CIDR*, *pre-shared secret* and *encryption algorithm*.
- You can import the information to your remote router/firewall configuration.

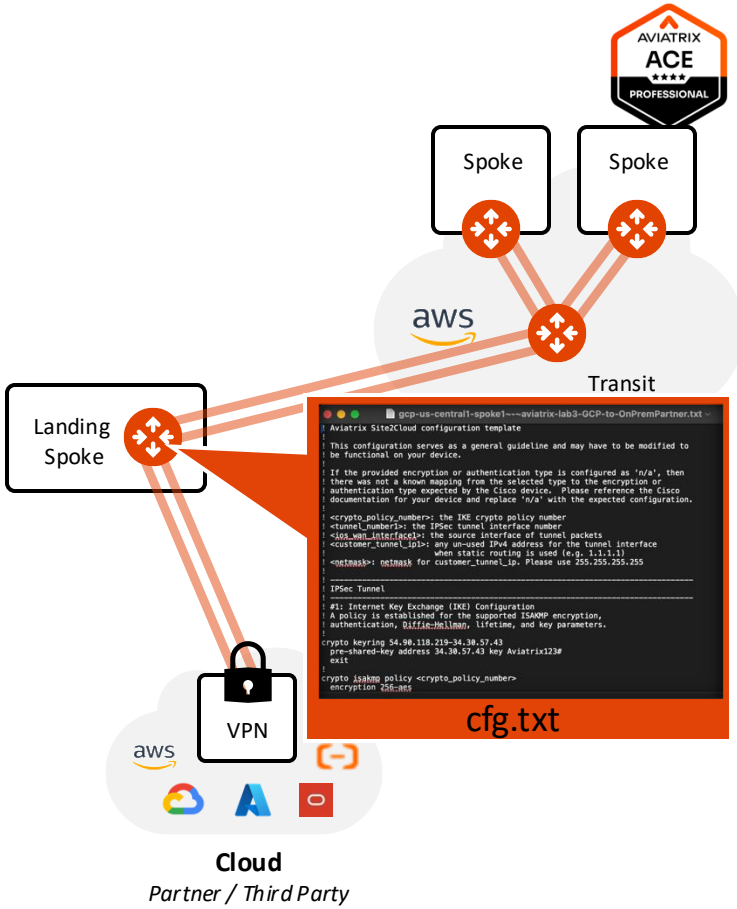
Vendor: **Platform:**

- Aviatrix → UCC
- Cisco → ASA 5500 Series / ISR, ASR or CSR
- Generic → Generic









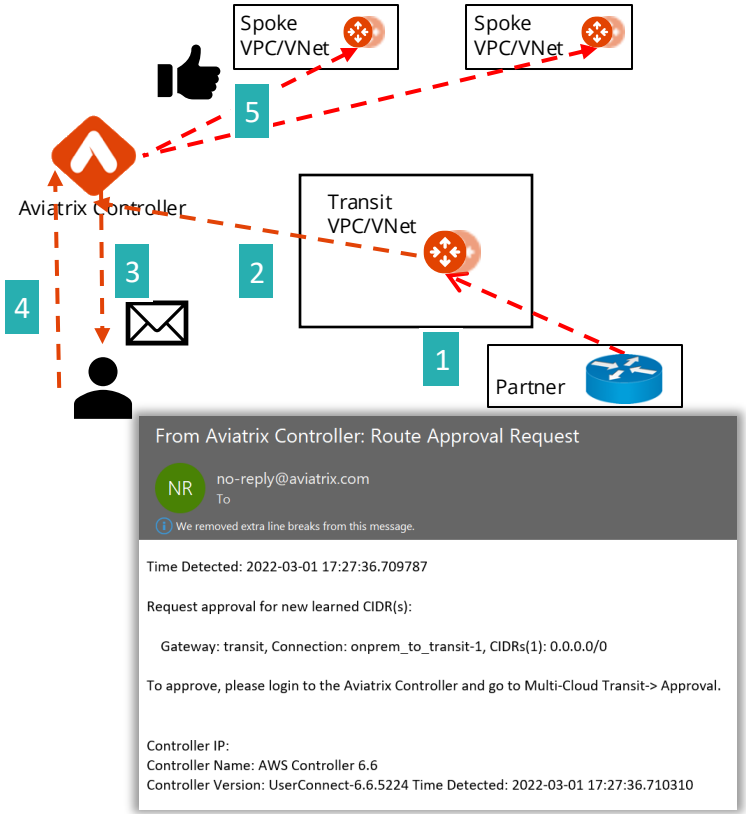
Route Approval

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



Aviatrix Edge

Introducing Aviatrix Edge

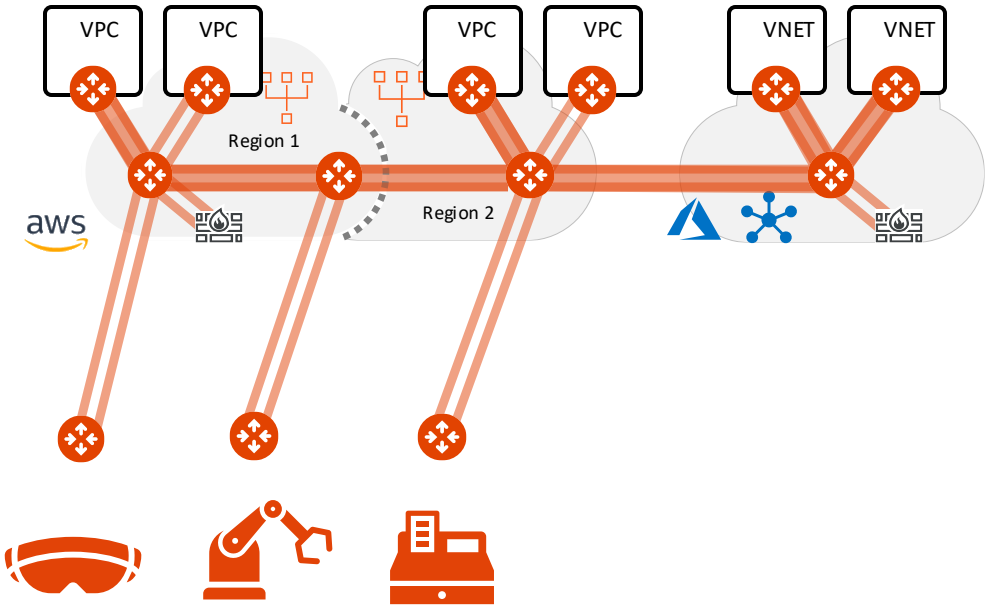
The only multi-cloud native platform with enterprise-grade visibility and control for public cloud and the edge
Aviatrix software in multiple form factors providing consistent network, security, and visibility to the edge.
Edge locations appear and behave as another VPC/VNET with spoke and transit capabilities.

Cloud Out Architecture

Simplified Edge Management

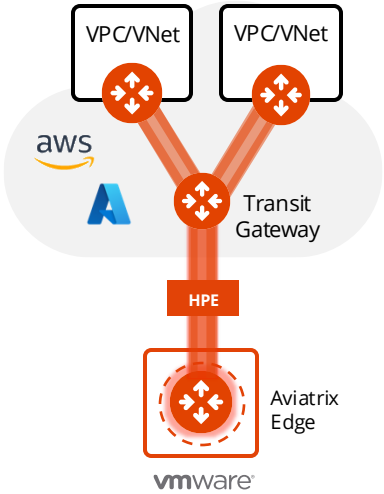
Consistent Secure Edge

Simplified Edge On-boarding

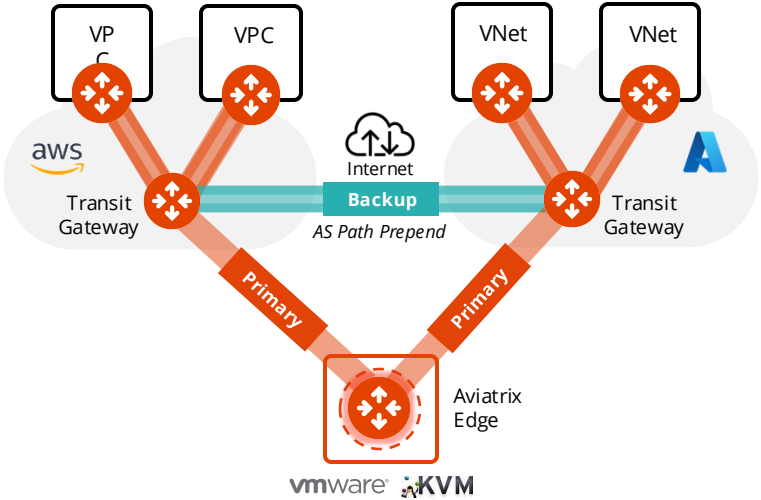


Aviatrix Edge Use Cases

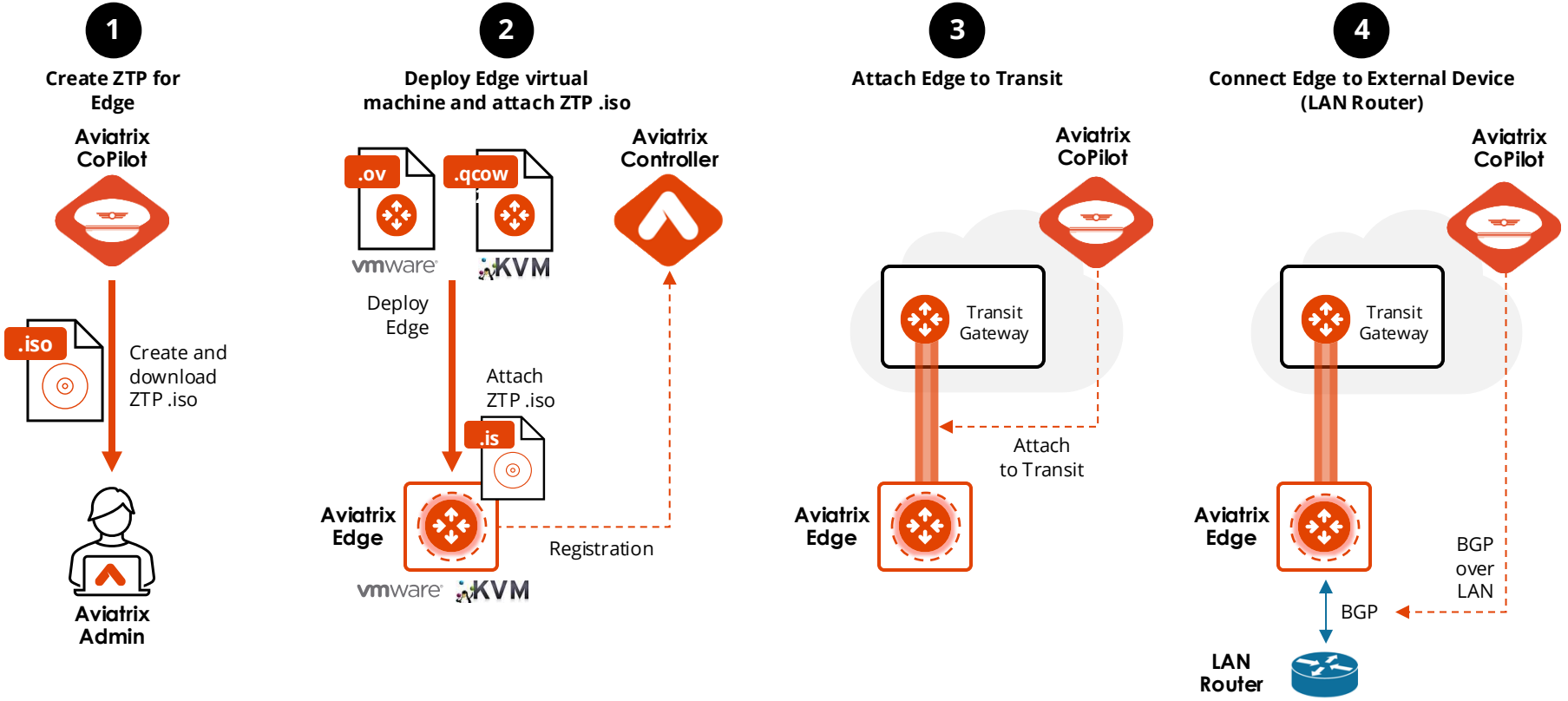
Extend the Aviatrix Platform to the Edge



Multi-Cloud Connectivity via Aviatrix Edge



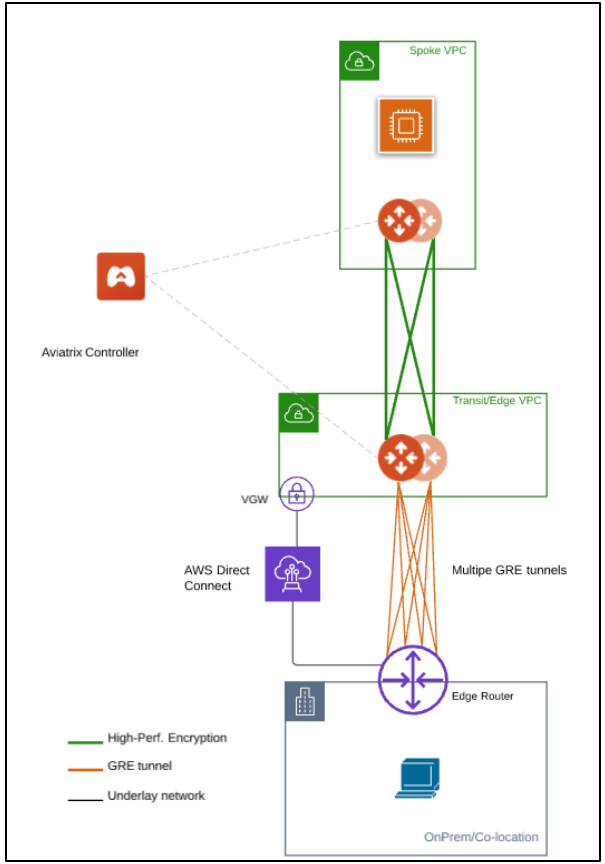
Edge 2.0 Deployment Workflow

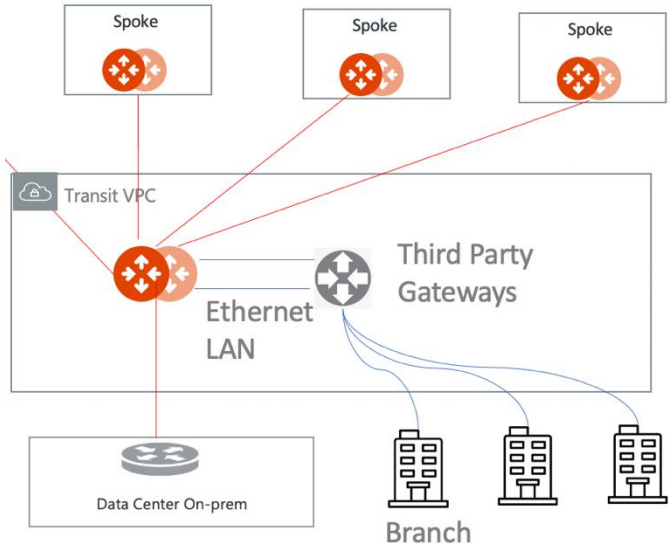


Other Services to Connect to External Networks

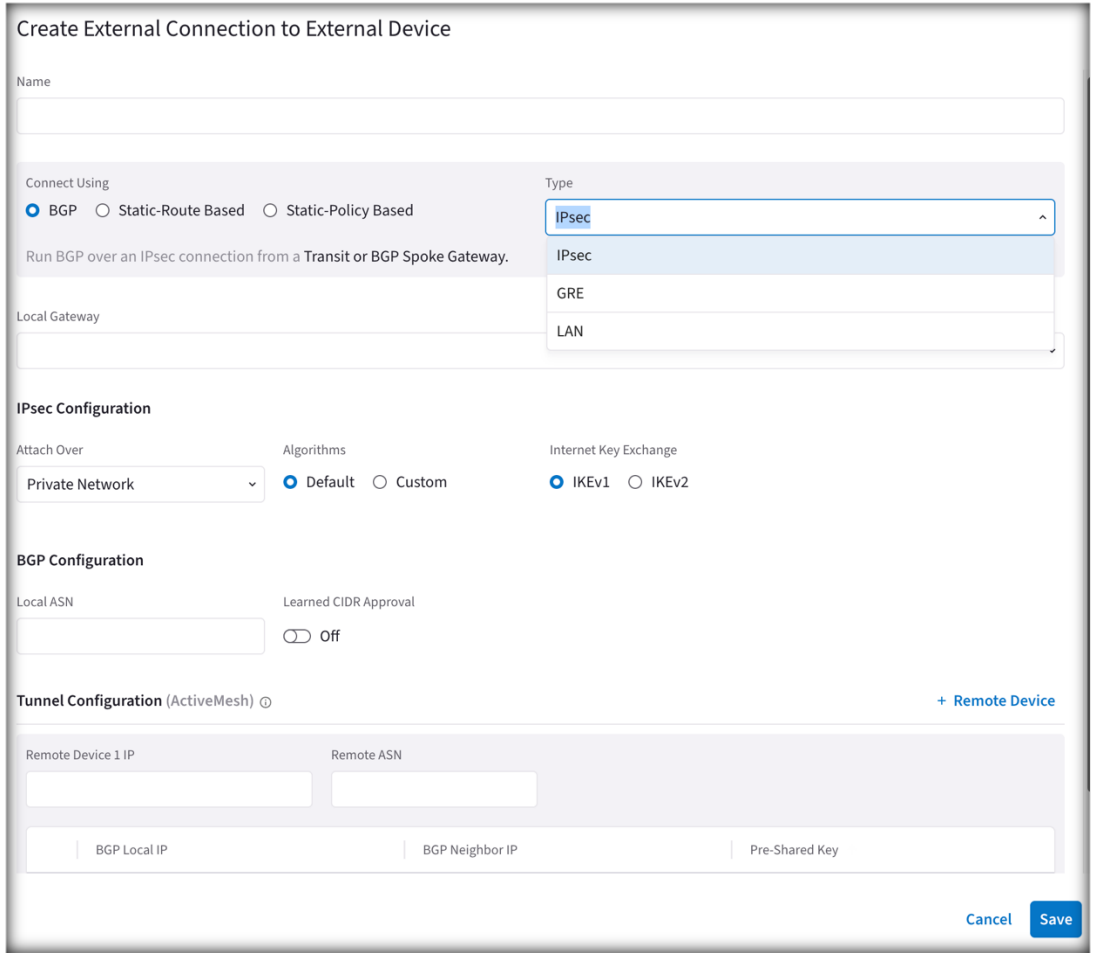
Connections to External Device

- **IPsec** (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)





Configuration – CoPilot > Networking > Connectivity > + External Connection

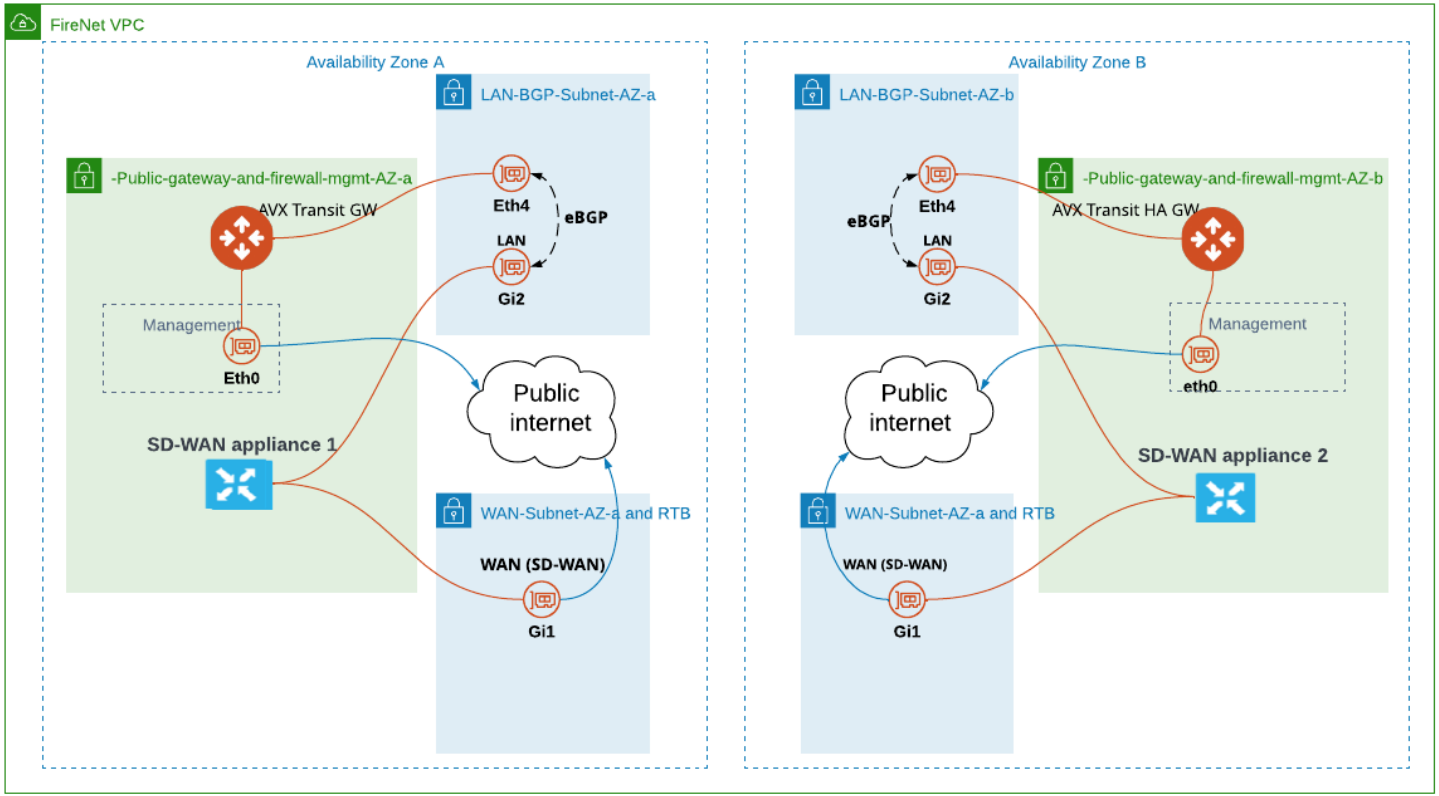


SD-WAN Integration

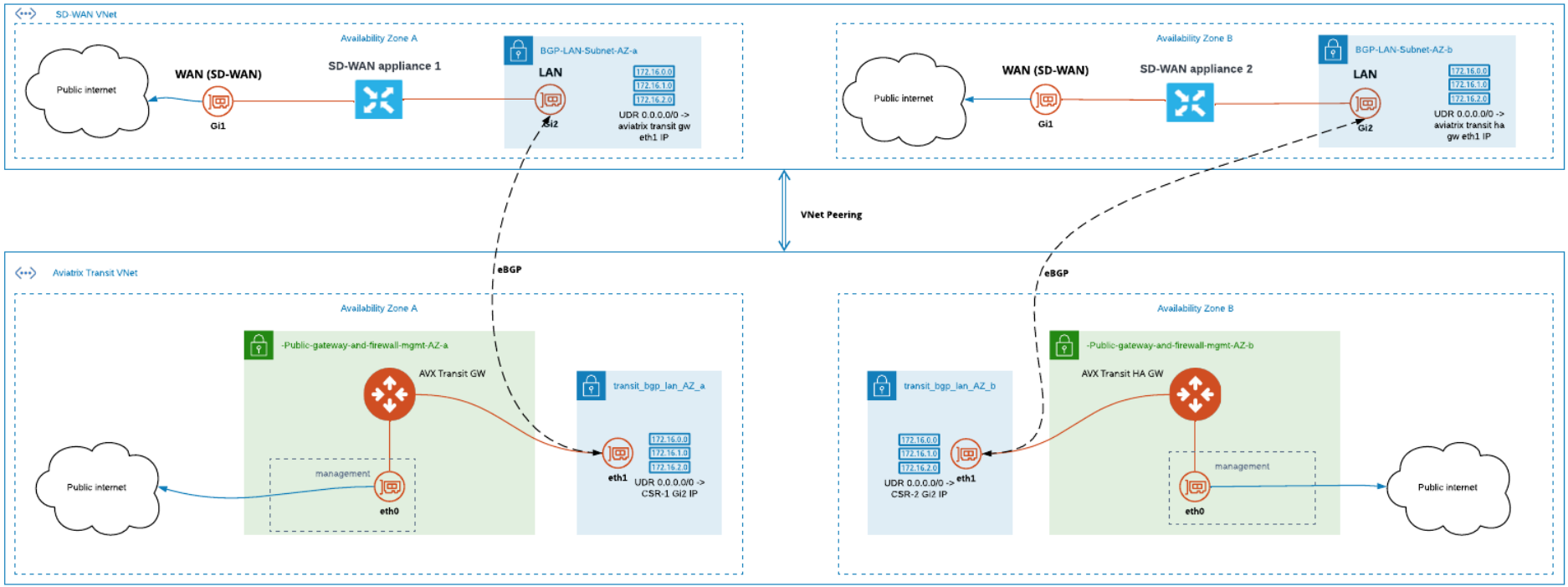
Solution – SD-WAN integration with Aviatrix

- 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: User VPN