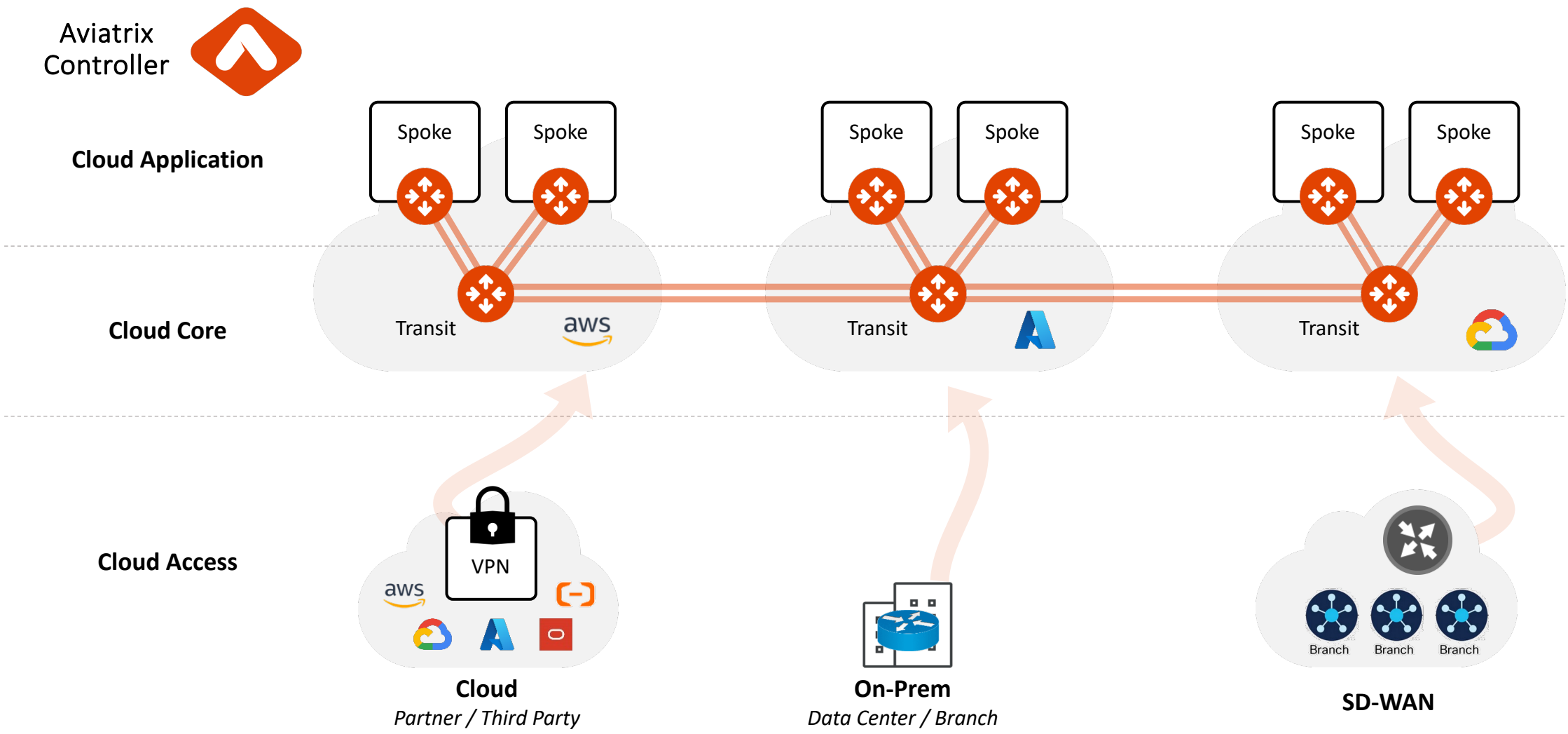
Site2Cloud

ACE Solutions Architecture Team

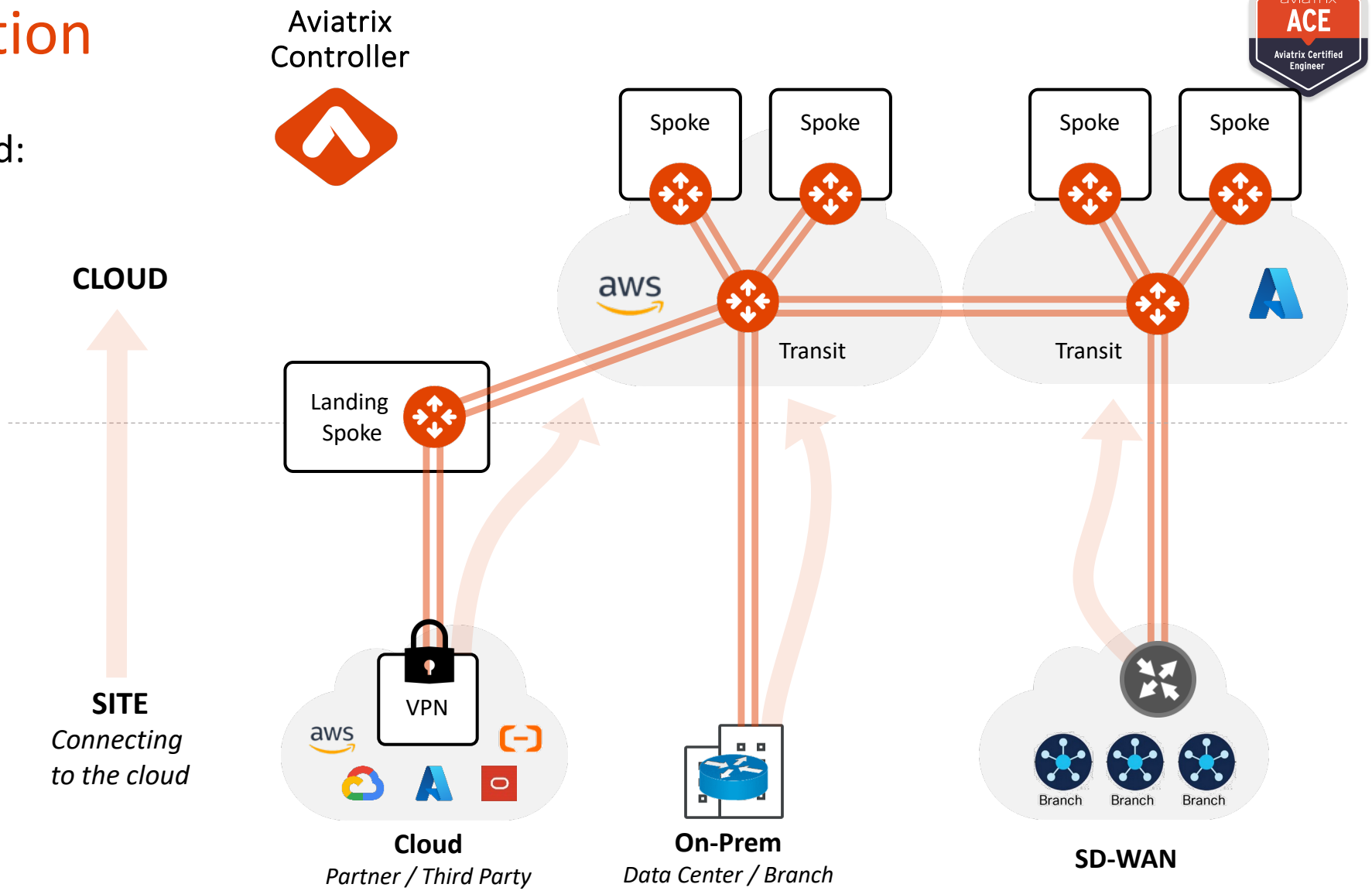
Aviatrix Multicloud Network Architecture



Site2Cloud Introduction

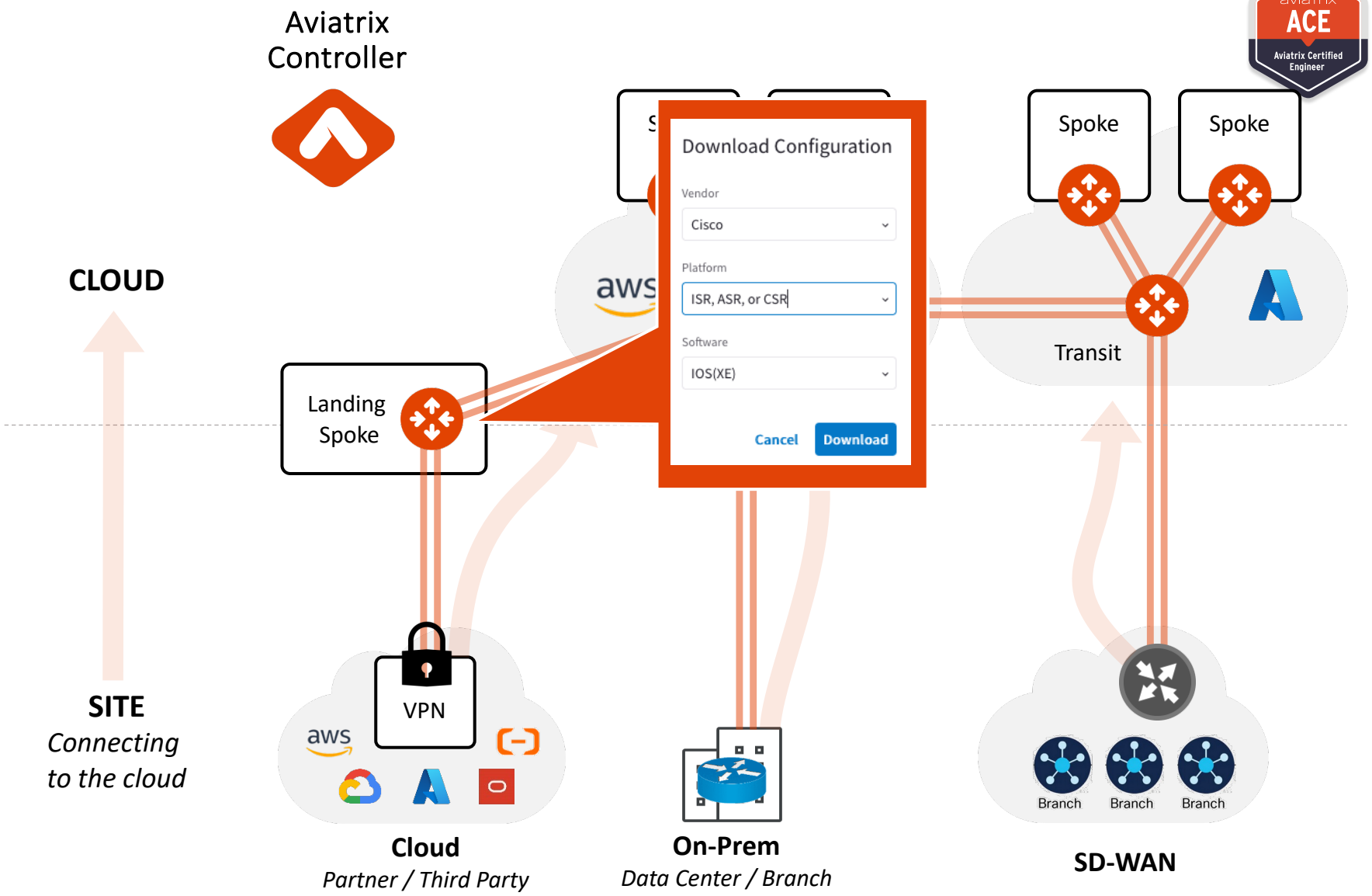
IPsec connection to Public Cloud:

- On-Prem DC
- Branch
- 3rd Party Appliances, SD-WAN
- Clouds Native Constructs (VPCs/VNets/VCNs)



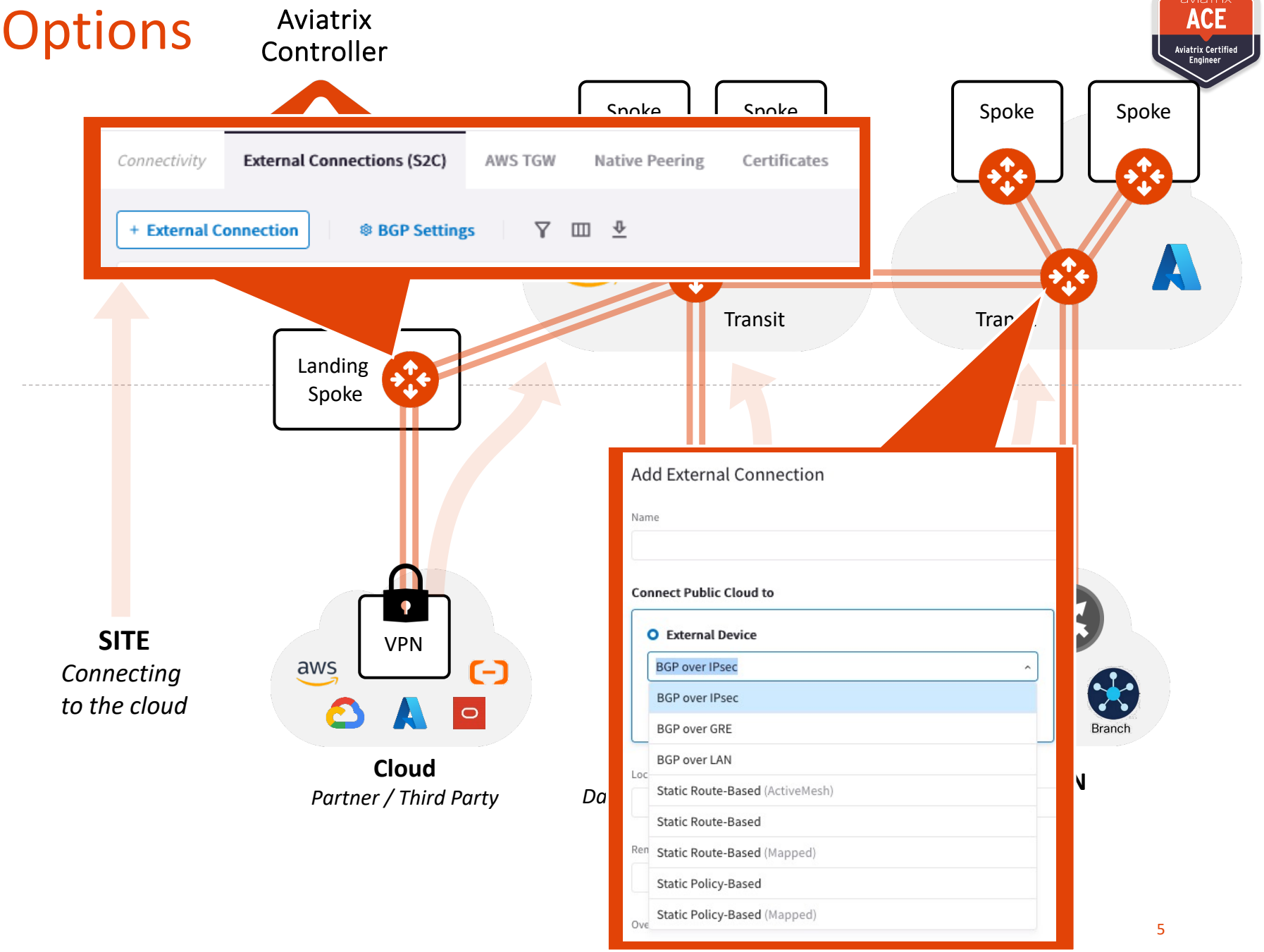
Site2Cloud Solution

- Easy to use and template-driven
- Built-in diagnostic tools
- Solves Overlapping IPs Challenges



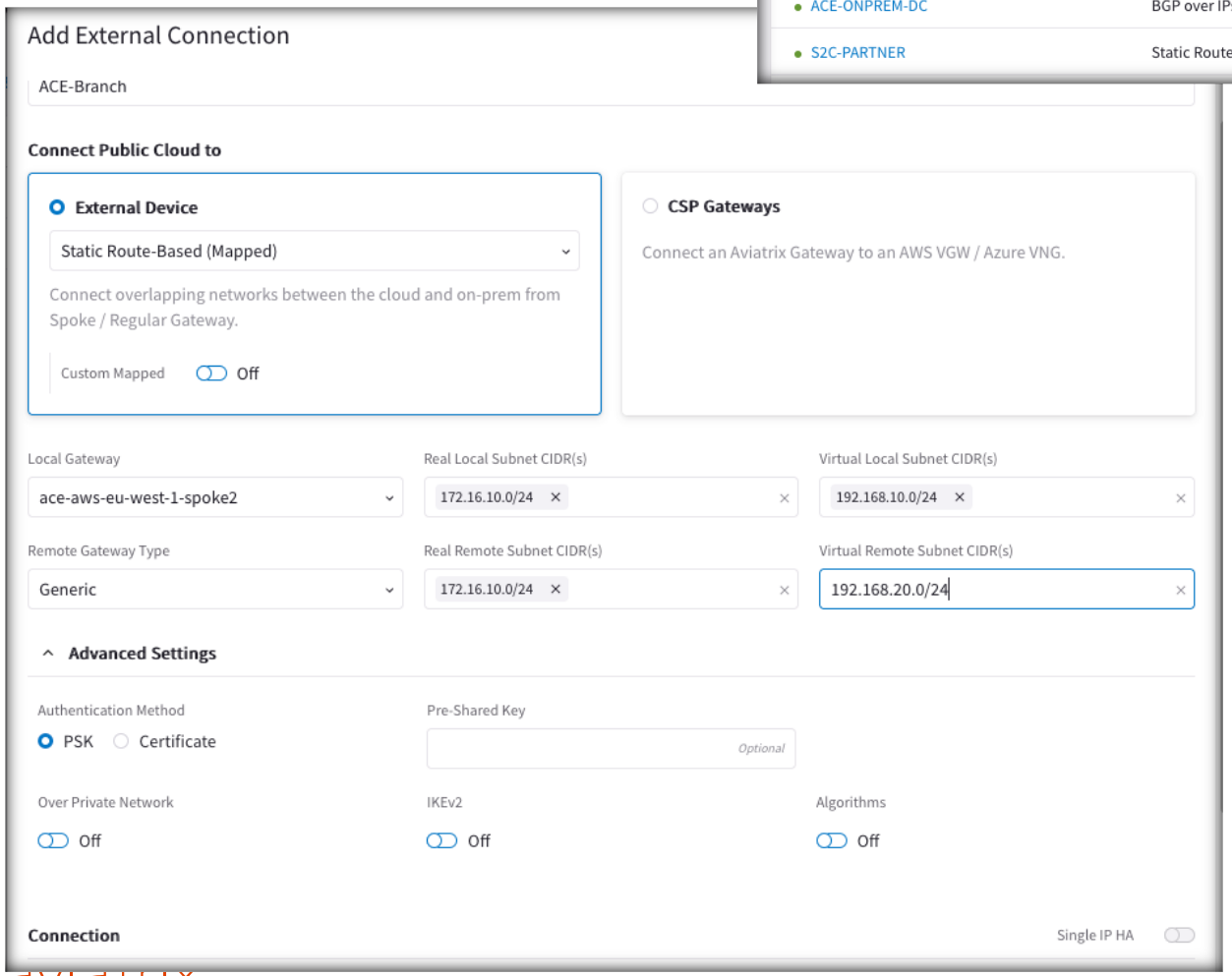
Site2Cloud Landing Options

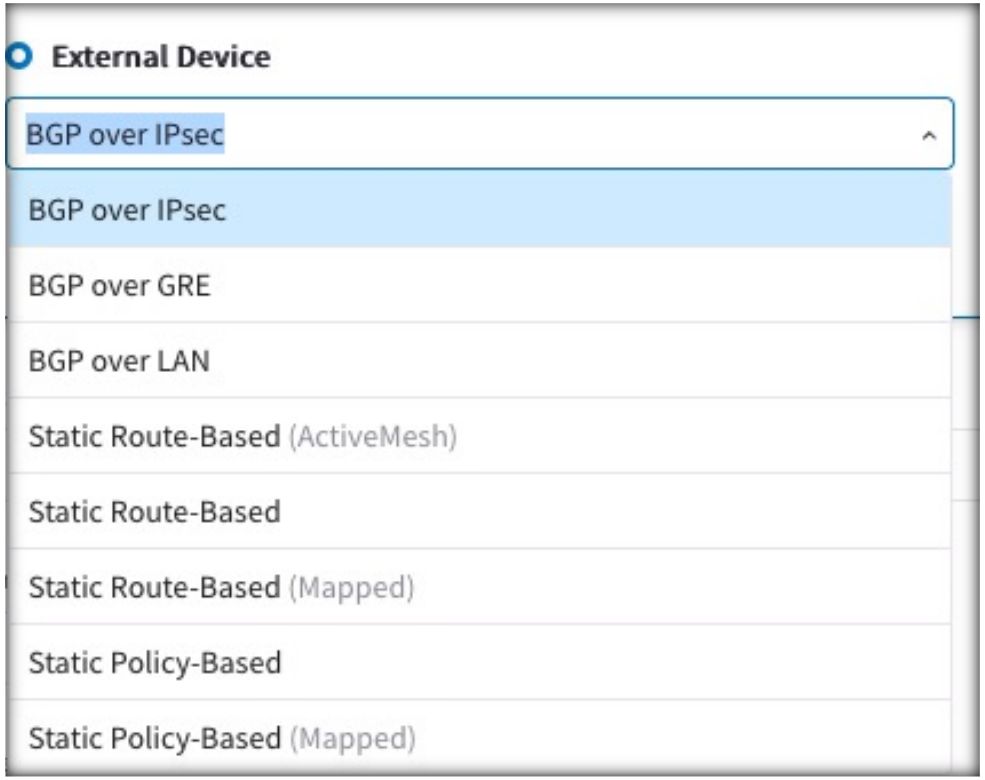
- **Landing on Transit**
  - Extend Core
  - SD-WAN
- **Landing on Spoke**
  - Scale
  - Partners
  - Complex Overlapping IP
  - Advanced NAT capabilities



Site2Cloud – Deployment

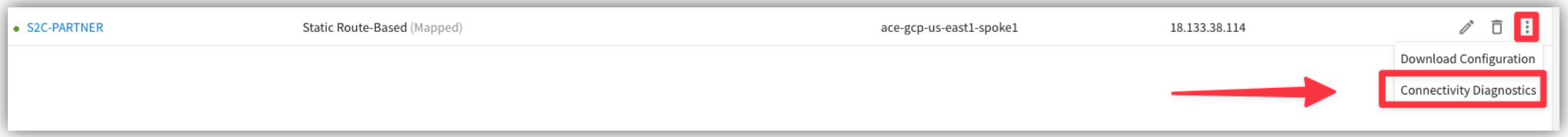
BGP is supported on Site2Cloud tunnels to either Transit Gateway or Spoke Gateway



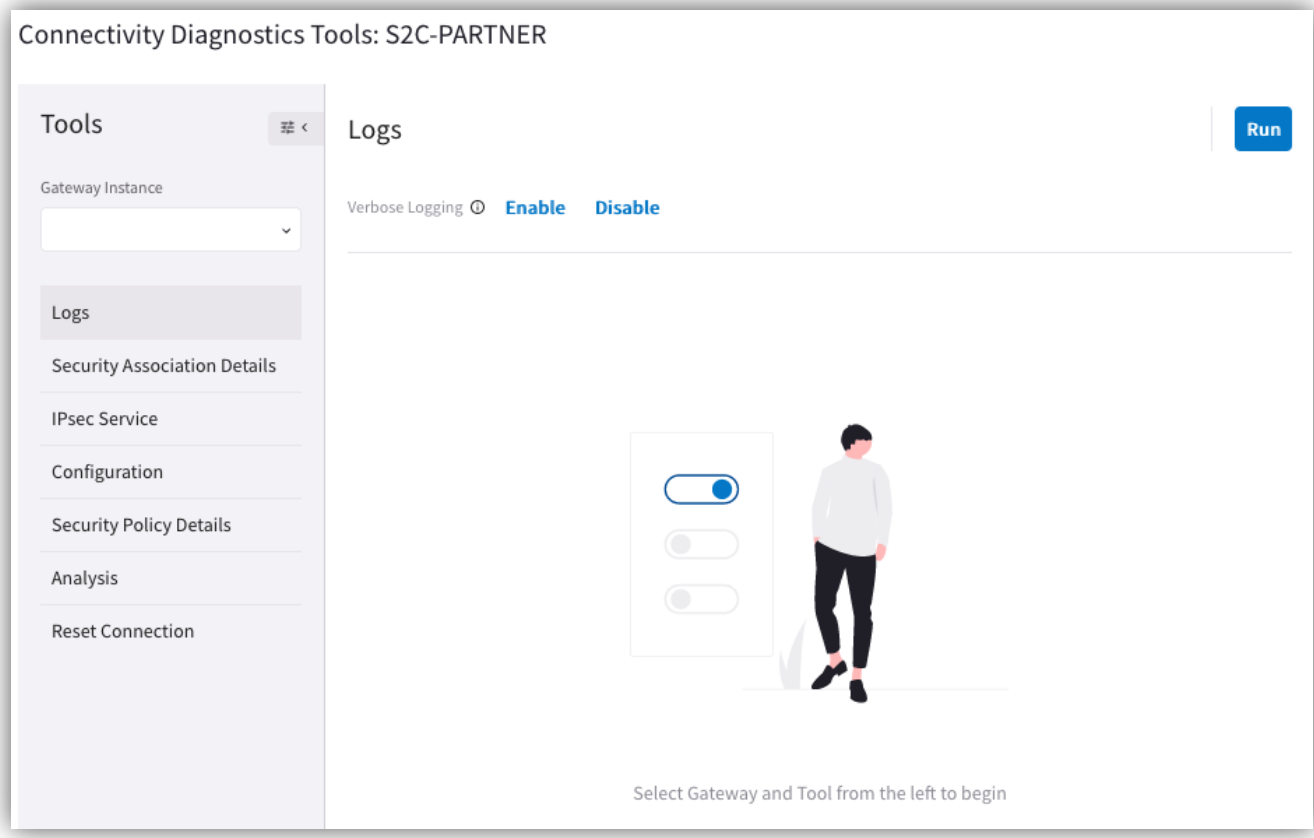


Monitoring & Troubleshooting Site2Cloud

Connectivity Diagnostics



- Tunnel is operational?
- 'Current' number is increasing on both ends
  - **CoPilot> Networking > Connectivity > External Connections (S2C) > Connectivity Diagnostics**
  - Make sure SPI (Security Parameter Index) matches on remote end
  - SPI is an identification tag added to the header while using IPsec for tunneling the IP traffic
  - SPI is required part of an IPSec Security Association (SA)
  - https://en.wikipedia.org/wiki/Security_Parameter_Index

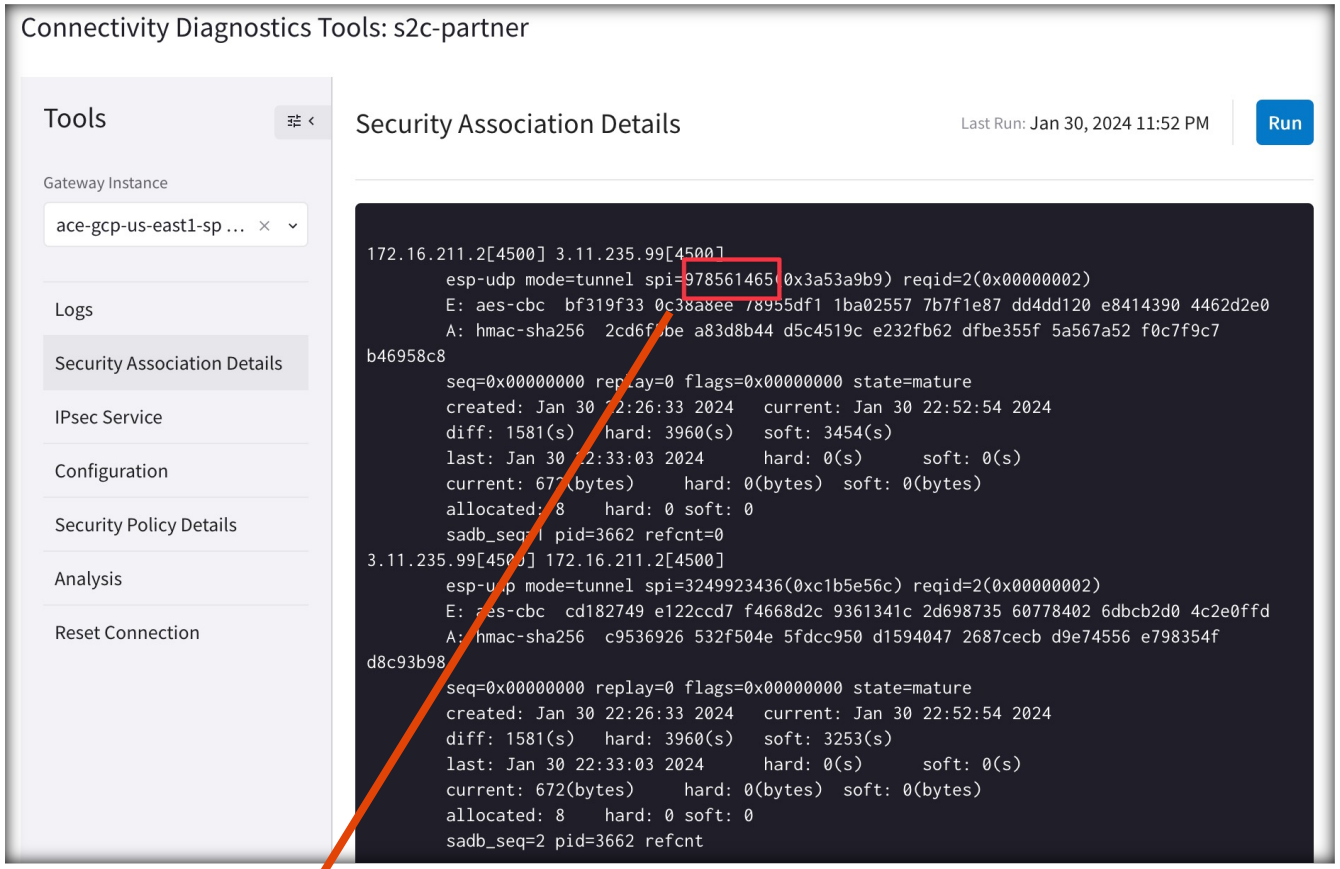


Monitoring – SPI

Cisco IOS outcome

```
OnPrem-Partner#show crypto ipsec sa interface tu1

interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 172.16.211.36

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer 34.139.73.146 port 4500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 8, #pkts encrypt: 8, #pkts digest: 8
    #pkts decaps: 8, #pkts decrypt: 8, #pkts verify: 8
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 172.16.211.36, remote crypto endpt.: 34.139.73.146
     plaintext mtu 1422, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
     current outbound spi: 0xC1B5E56C(3249923436)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x81432F90(2168663952)
        transform: esp-256-aes esp-sha256-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        conn id: 2001, flow_id: CSR:1, sibling_flags FFFFFFFF80000048, crypto map: Tunnel1-head-0
        sa timing: remaining key lifetime (sec): 2021
        Kilobyte Volume Rekey has been disabled
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
      spi: 0x3A53A9B9(978561465)
        transform: esp-256-aes esp-sha256-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        conn id: 2004, flow_id: CSR:4, sibling_flags FFFFFFFF80000048, crypto map: Tunnel1-head-0
```

Aviatrix CoPilot outcome



SPI matches on both ends

Troubleshooting

In the event of an IPsec VPN tunnel going down, follow these steps in sequence:

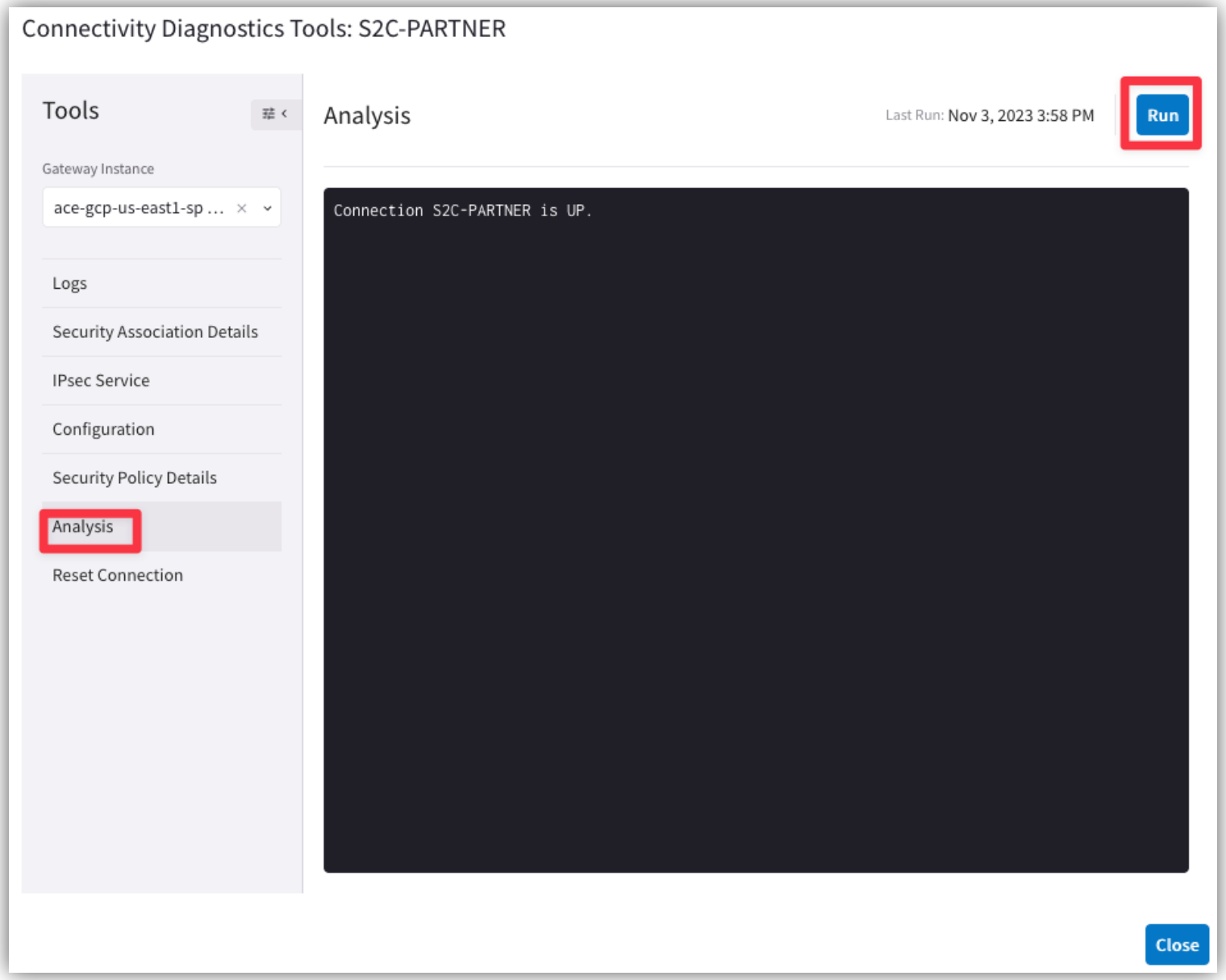
1. **Confirm Layer 3 connectivity**
   - Public IP reachable? Is there an ISP (BGP) issue?
   - If ping is disabled, check packet capture on remote public IP for ISAKMP packets
2. **Confirm SG/NSG allowed for outbound**
   - UDP 500 (ISAKMP)
   - UDP 4500 (ESP, which is encrypted traffic)
3. **Confirm whether IPsec Phase 2 or IPsec SA negotiation is stuck**
   - Restart IPsec service from SITE2CLOUD > Diagnostics
4. **Check policies outside each end of the tunnel**
   - ACL policies on remote end
   - Security Groups/NACLs on Cloud side

Supported IPsec Encryption Algorithms

Type	Value
Phase 1 Authentication	SHA-1, SHA-512, SHA-384, SHA-256
Phase 1 DH Groups	1, 2, 5, 14, 15, 16, 17, 18, 19, 20, 21
Phase 1 Encryption	AES-256-CBC, AES-256-GCM-64, AES-256-GCM-96, AES-256-GCM-128, AES-192-CBC, AES-128-CBC, AES-128-GCM-64, AES-128-GCM-96, AES-128-GCM-128, 3DES
Phase 2 Authentication	HMAC-SHA-1, HMAC-SHA-512, HMAC-SHA-384, HMAC-SHA-256, NO-AUTH
Phase 2 DH Groups	1, 2, 5, 14, 15, 16, 17, 18, 19, 20, 21
Phase 2 Encryption	AES-128-CBC, AES-192-CBC, AES-256-CBC, AES-256-GCM-64, AES-256-GCM-96, AES-256-GCM-128, AES-128-GCM-64, AES-128-GCM-96, AES-128-GCM-128, 3DES, NULL-ENCR

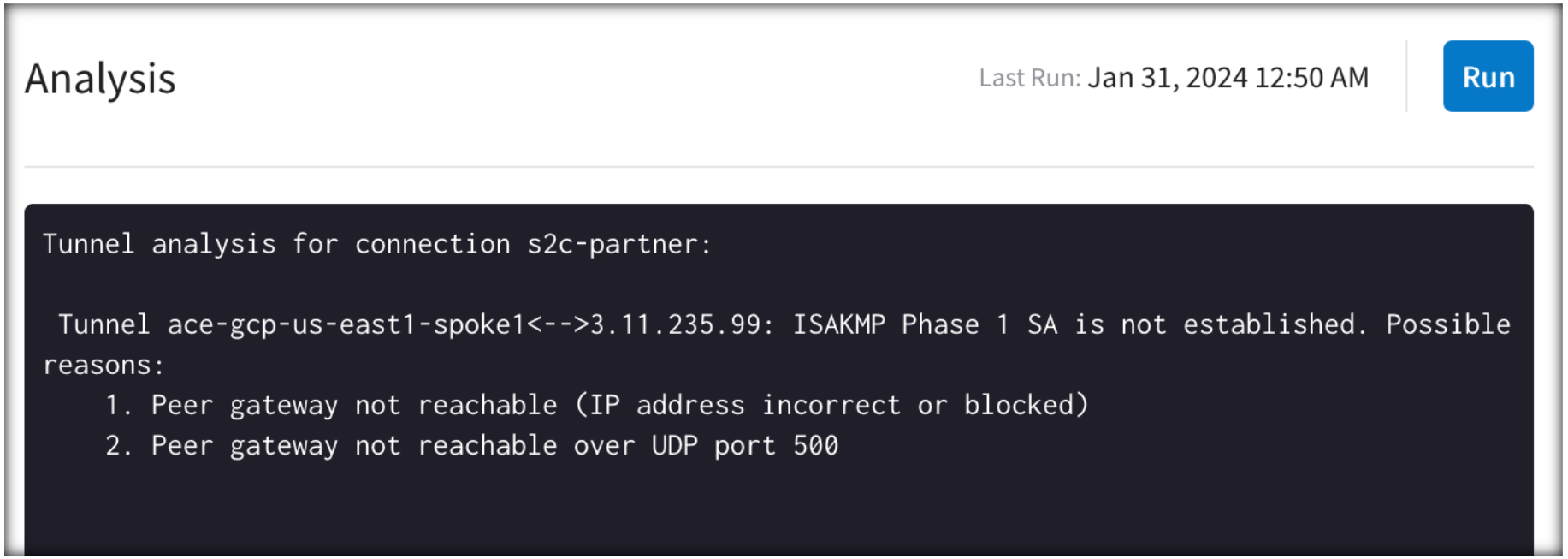
https://docs.aviatrix.com/HowTos/site2cloud_faq.html

Diagnostics - Run Analysis



Analysis – On-prem router is down

On-prem router is **down…**



Analysis – UDP port 500 is not permitted

Security group rule ID	IP version	Type	Protocol	Port range	Source
sgr-0176887910548ab41	IPv4	Custom UDP	UDP	4500	0.0.0.0/0
sgr-00e743fbe80ad493f	IPv4	All ICMP - IPv4	ICMP	All	0.0.0.0/0
sgr-0befa511b6d1e85f5	IPv4	SSH	TCP	22	0.0.0.0/0

Analysis

Last Run: Jan 31, 2024 12:50 AM

Run

```
Tunnel analysis for connection s2c-partner:

 Tunnel ace-gcp-us-east1-spoke1<-->3.11.235.99: ISAKMP Phase 1 SA is not established. Possible
reasons:
    1. Peer gateway not reachable (IP address incorrect or blocked)
    2. Peer gateway not reachable over UDP port 500
```

Analysis – Pre-shared key mismatch

```
crypto ikev2 keyring OnPrem-Aviatrix
 peer OnPrem-Aviatrix
  address 34.139.73.146
  identity address 34.139.73.146
  pre-shared-key WRONG
 !
```

Analysis

Last Run: Jan 31, 2024 1:01 AM

Run

```
Tunnel analysis for connection s2c-partner:

 Tunnel ace-gcp-us-east1-spoke1<-->3.11.235.99: ISAKMP Phase 1 SA is not established. Possible
reasons:
    1. IPSEC Phase 1 authentication method is not pre-shared key
    2. Pre-shared key mismatch
    3. IPSEC remote id mismatch
```

Analysis – DH Group mismatch

```
OnPrem-Partner#show crypto ikev2 proposal
 IKEv2 proposal: avx-s2c
      Encryption : AES-CBC-256
      Integrity  : SHA256
      PRF        : SHA256
      DH Group   : DH_GROUP_1536_MODP/Group 5
```

Analysis

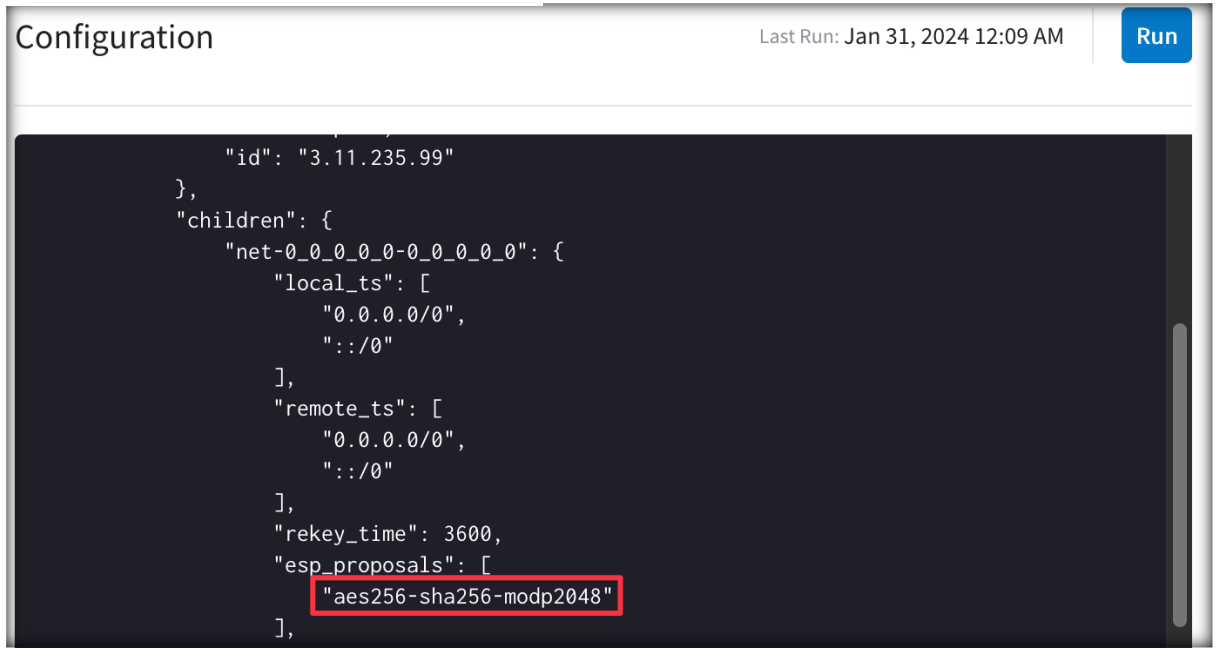
Last Run: Jan 31, 2024 1:10 AM

Run

```
Tunnel analysis for connection s2c-partner:

 Tunnel ace-gcp-us-east1-spoke1<-->3.11.235.99: IPsec Phase 2 SA is not established. Possible
reasons:
    1. Encryption/Authentication algorithm mismatch
    2. DH group number mismatch
```

Analysis – Encryption algorithm mismatch

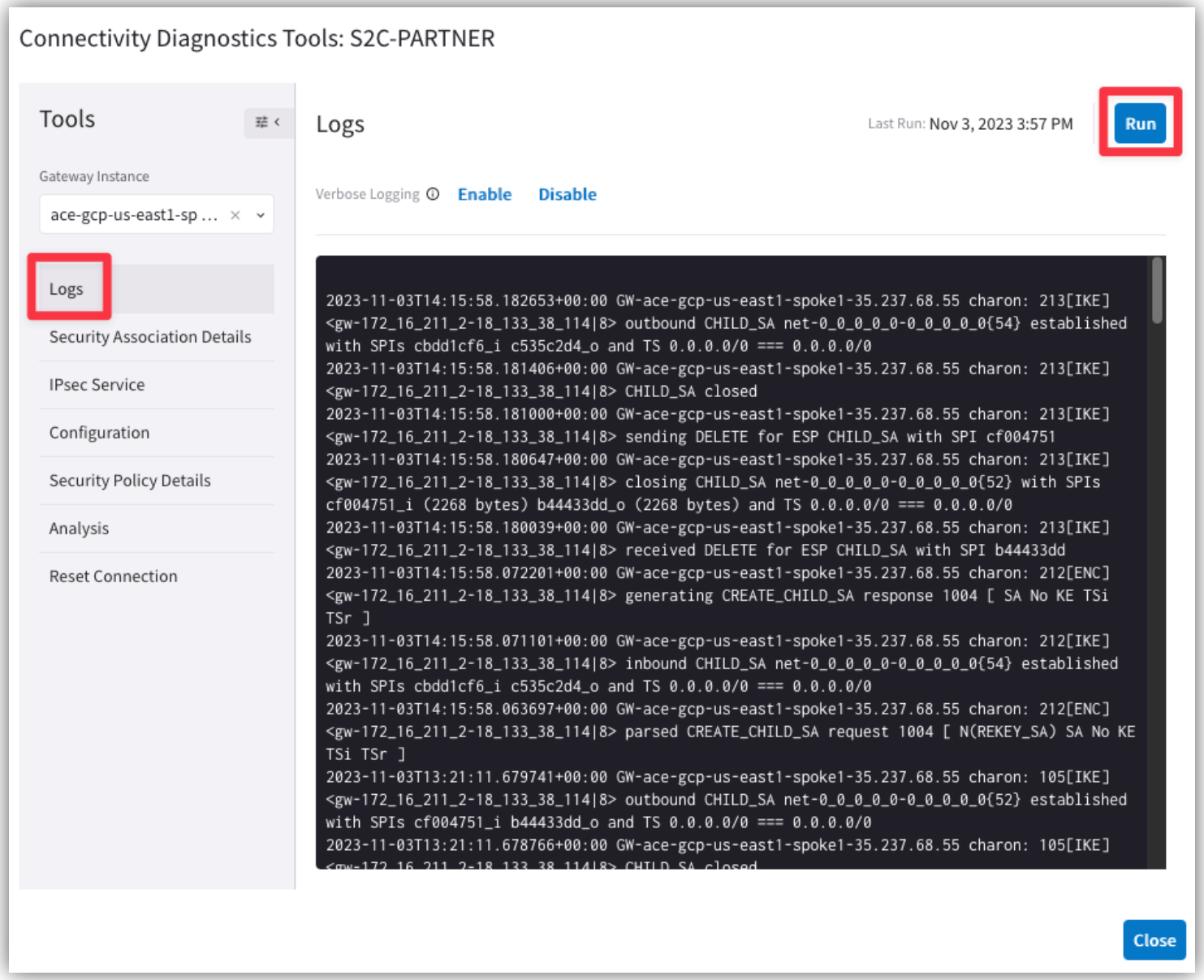
Aviatrix CoPilot outcome



Cisco IOS outcome

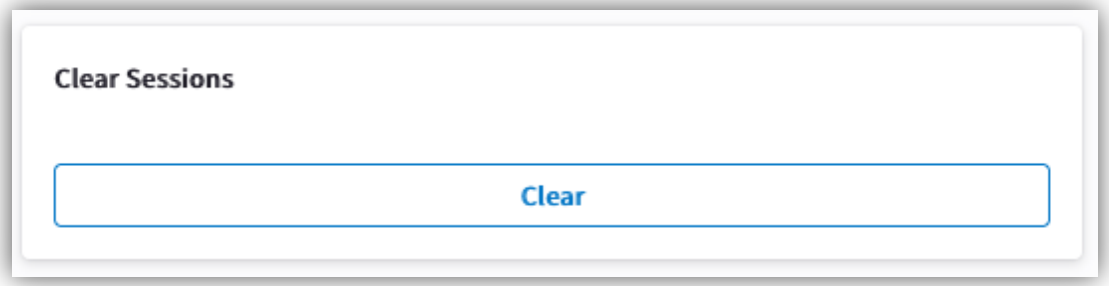
```
OnPrem-Partner#show crypto ipsec transform-set
Transform set default: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set OnPrem-Aviatrix: { esp-256-aes esp-md5-hmac  }
   will negotiate = { Tunnel,  },

OnPrem-Partner#
```

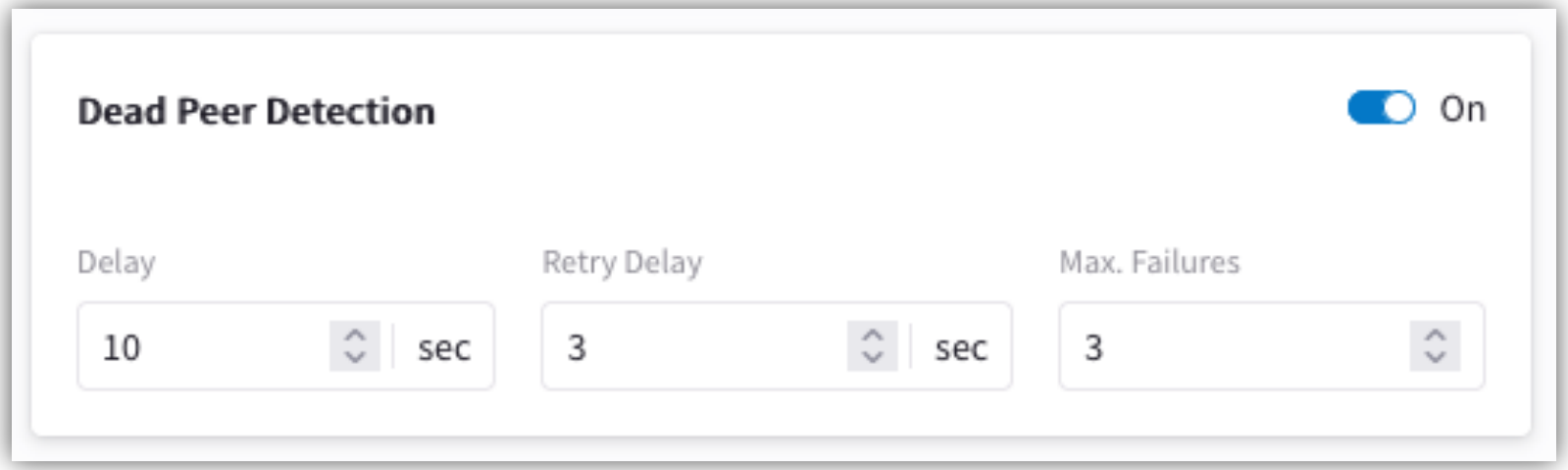
Diagnostics – show logs



Dead Peer Detection Mismatch

- Dead Peer Detection is configured on Aviatrix gateways by default as follows (can be configured):
  - interval 10 seconds
  - retry 3 times
  - max failure 3 times
- If DPD is disabled on remote end:
  - Disable it on Site2Cloud gateway from **Networking > Connectivity > S2C conn. > Settings**
  - Restart the VPN service from **Networking > Connectivity > S2C conn. > Connectivity Diagnostics**





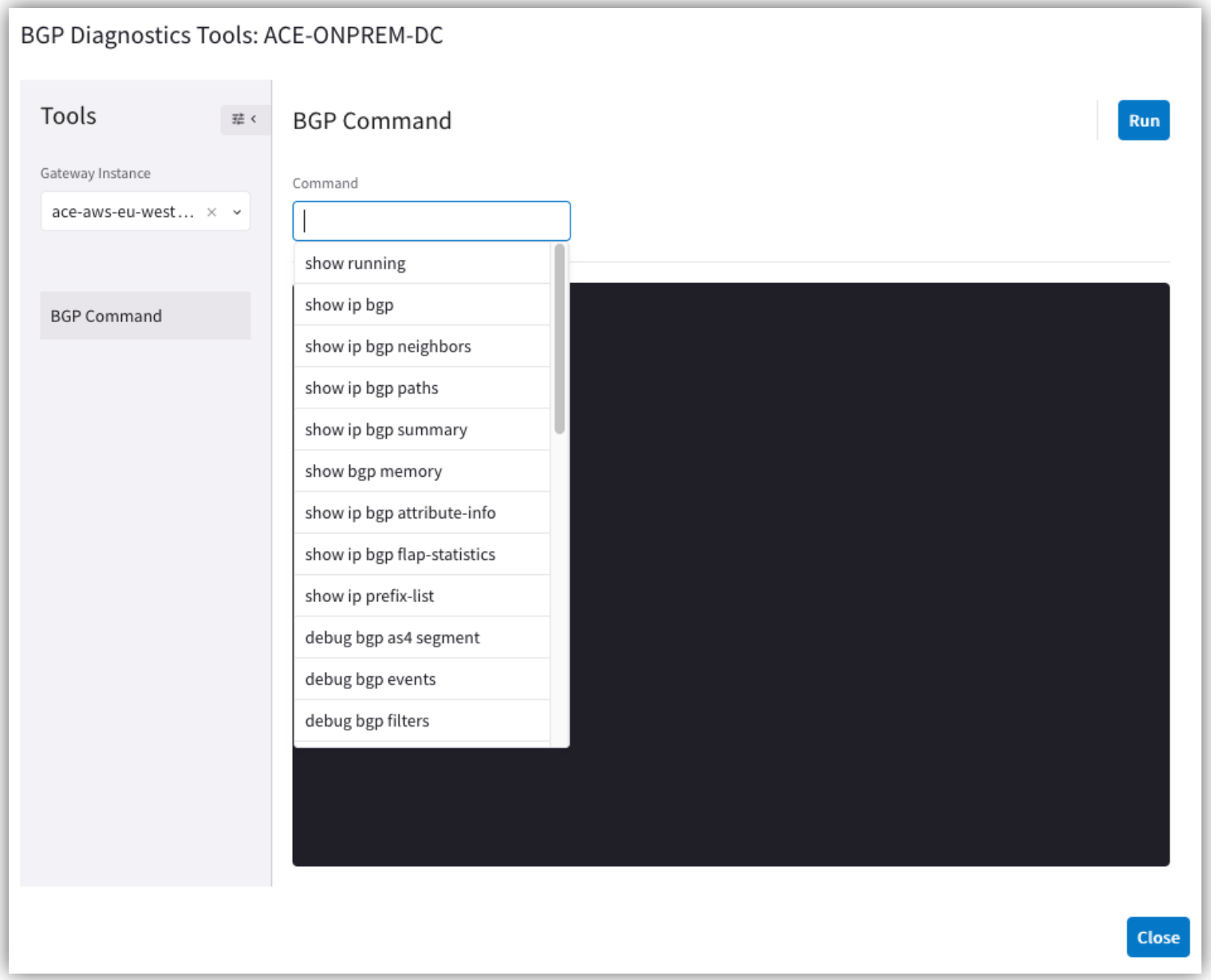
NOTE:

- This will restart all tunnels on this gateway
- Could impact your service till the tunnels come up

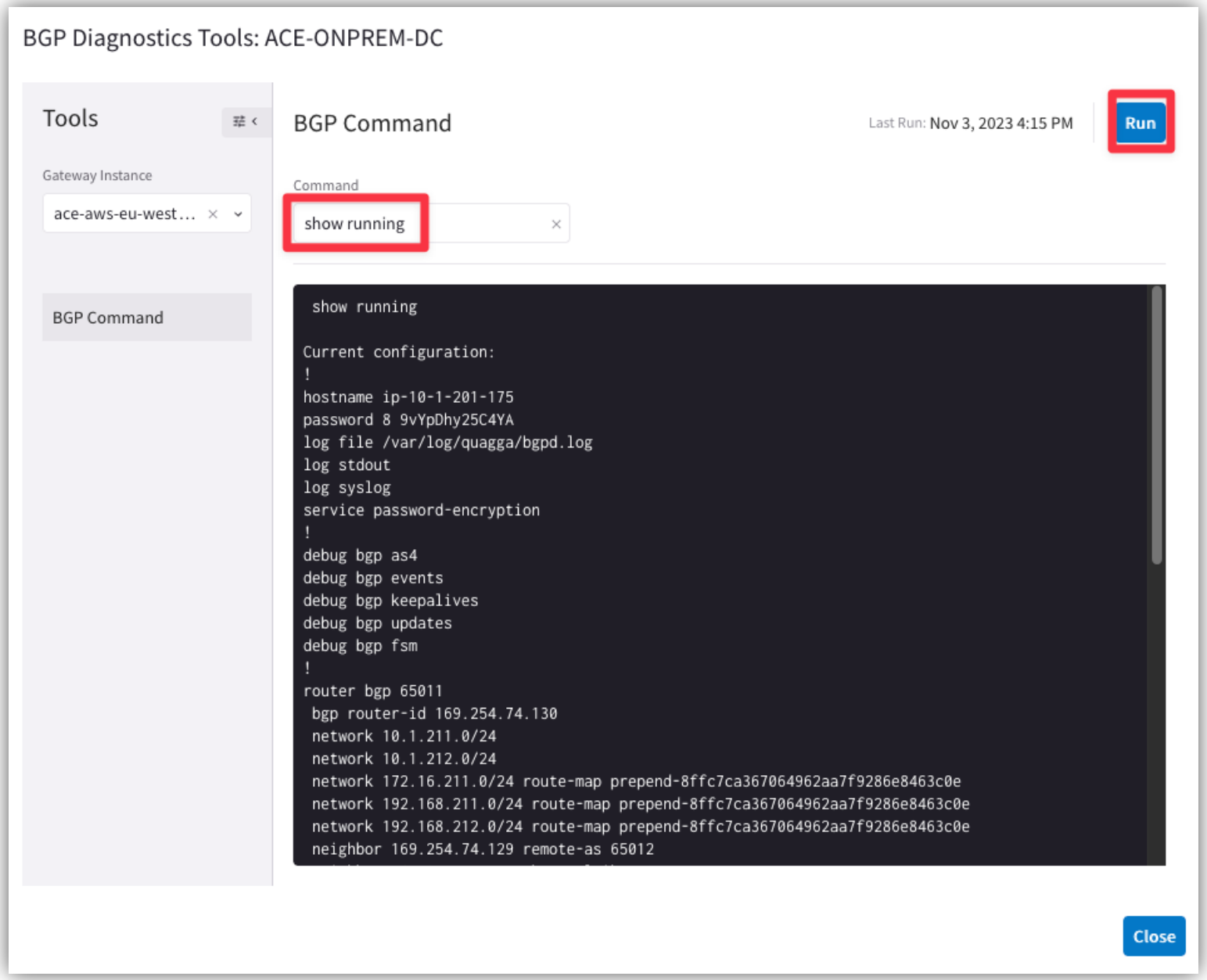
BGP Troubleshooting

- **PATH:** CoPilot> Networking > Connectivity > External Connections (S2C) > BGP Diagnostics

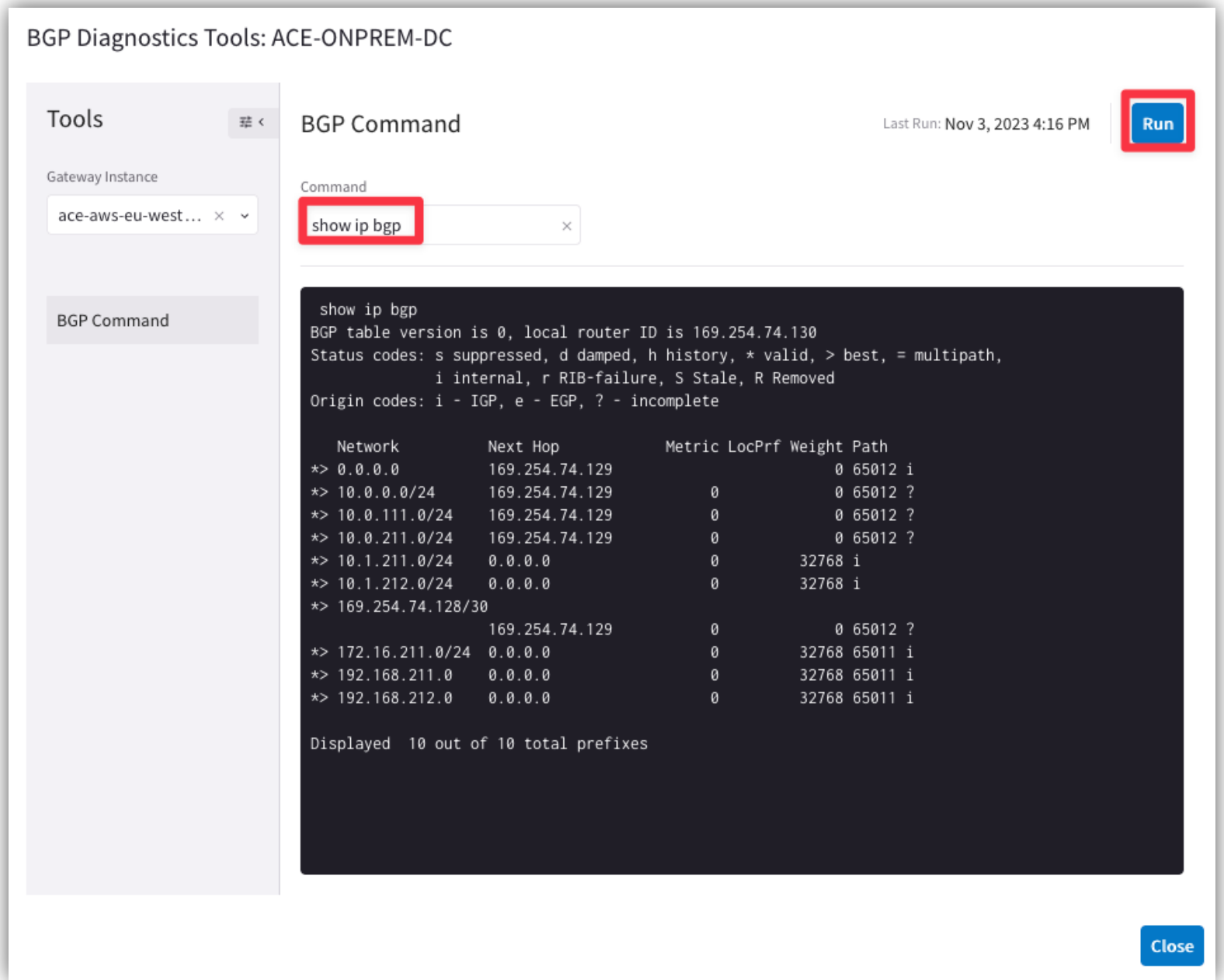
BGP Troubleshooting – List of commands



BGP Troubleshooting – show running



BGP Troubleshooting – show ip bgp



Edge

Introducing Aviatrix Edge

The only multi-cloud native platform with enterprise-grade visibility and control for public cloud and the edge

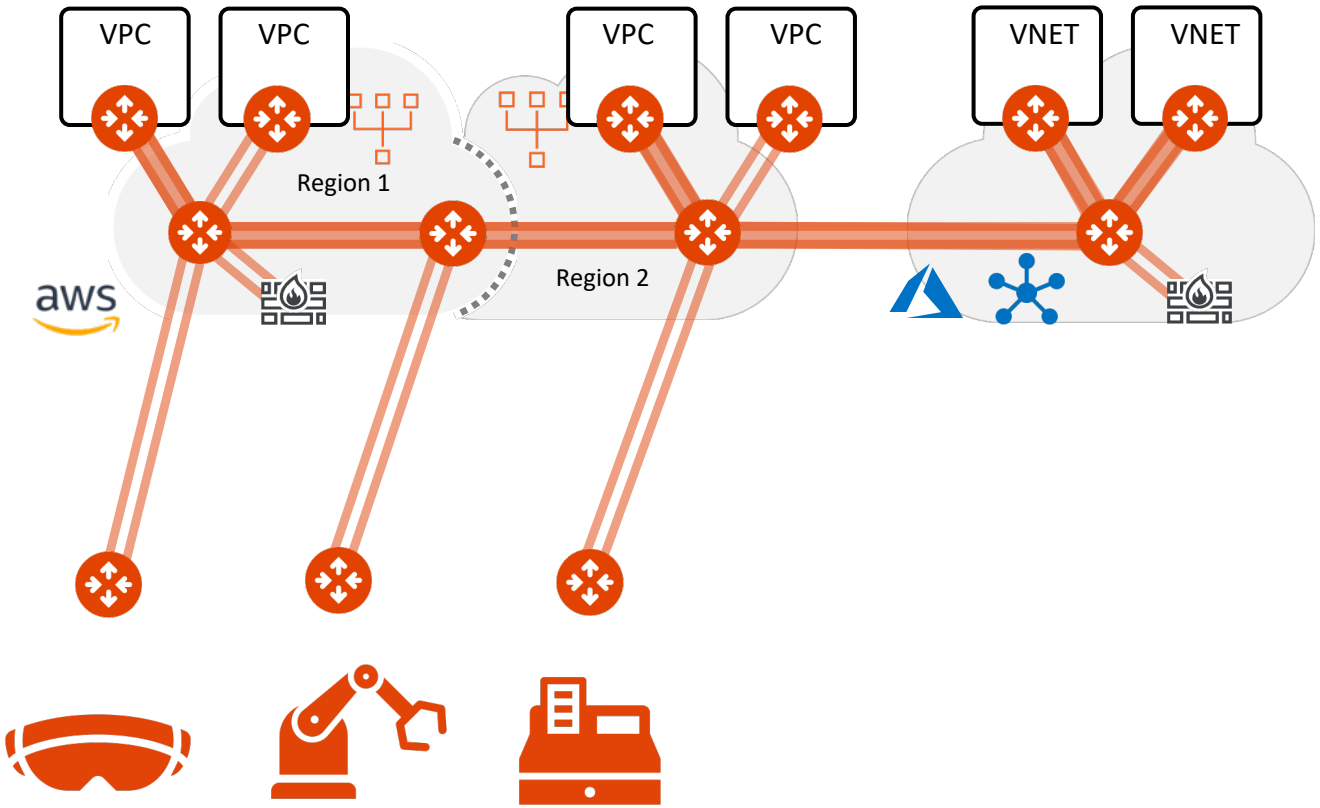
Aviatrix software in multiple form factors providing consistent network, security, and visibility to the edge.
Edge locations appear and behave as another VPC/VNET with spoke and transit capabilities.

Cloud Out Architecture

Simplified Edge Management

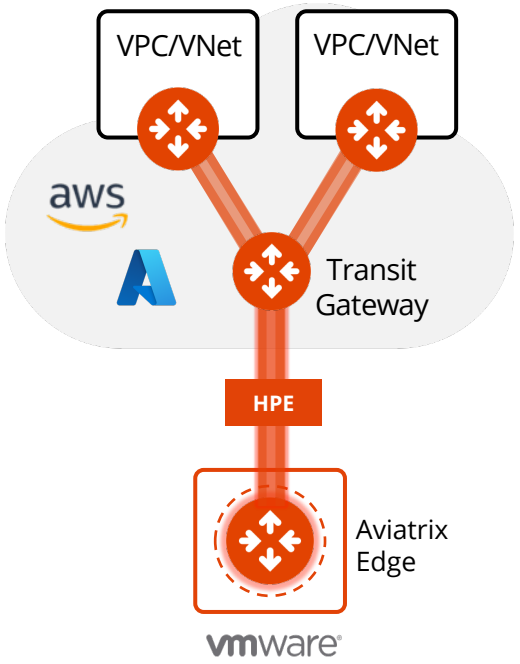
Consistent Secure Edge

Simplified Edge On-boarding

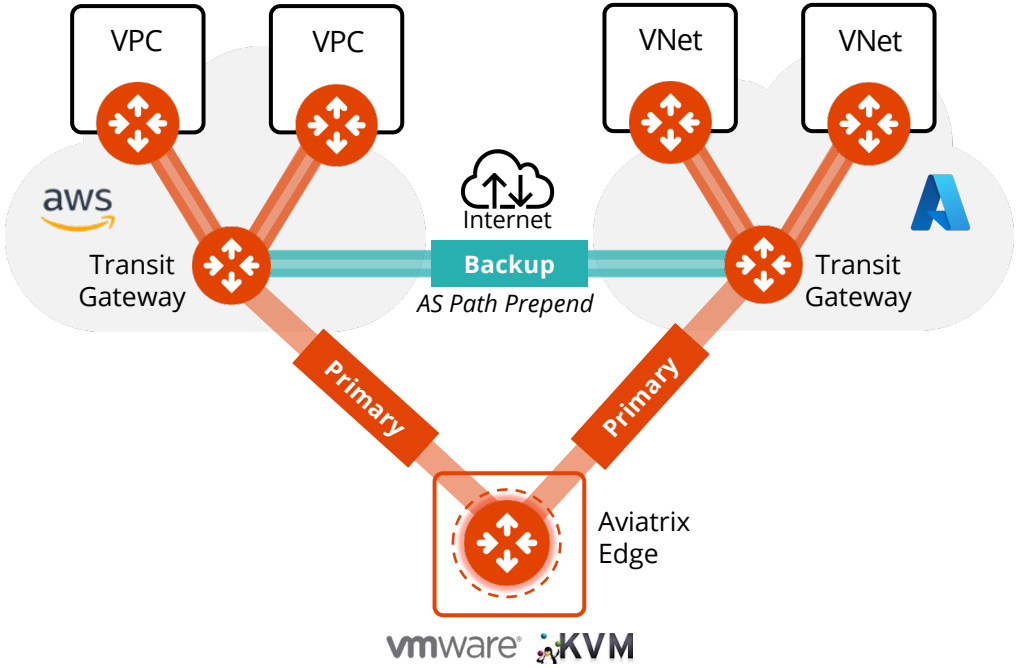


Aviatrix Edge Use Cases

Extend the Aviatrix Platform to the Edge

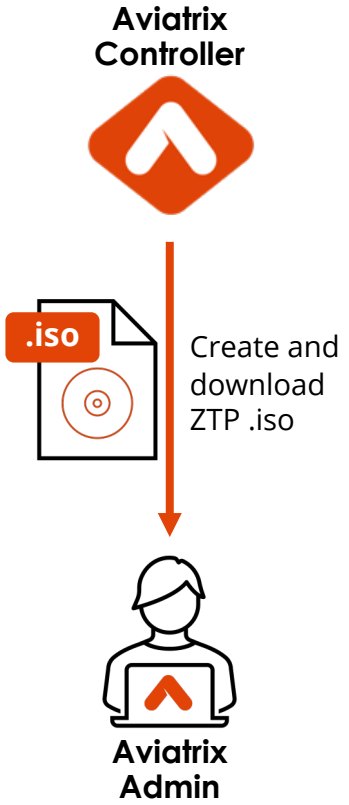


Multi-Cloud Connectivity via Aviatrix Edge

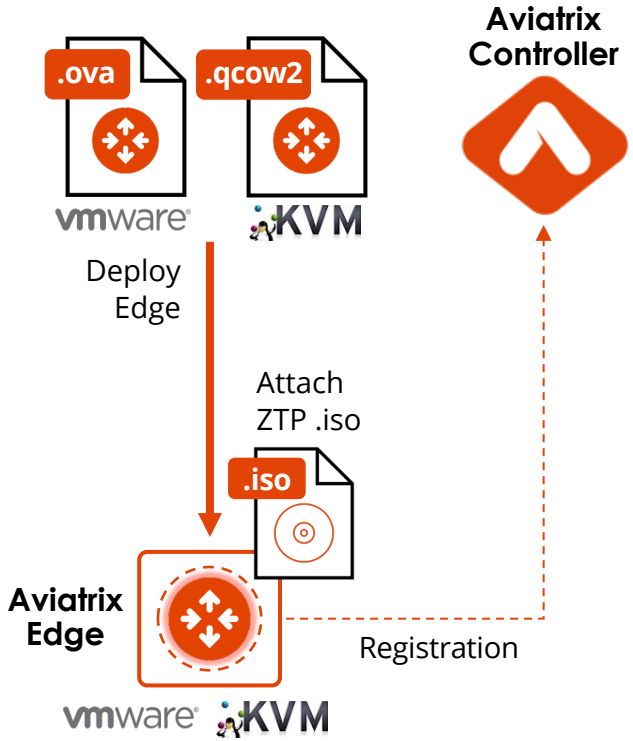


Edge 2.0 Deployment Workflow - Demo

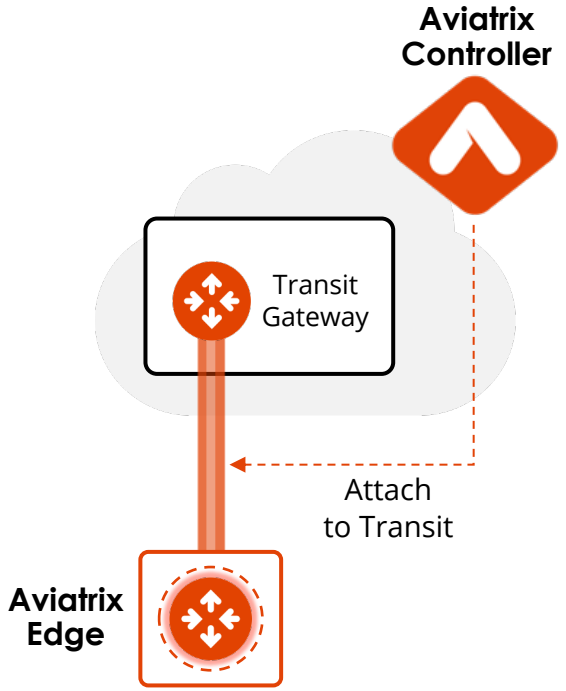
1 Create ZTP for Edge



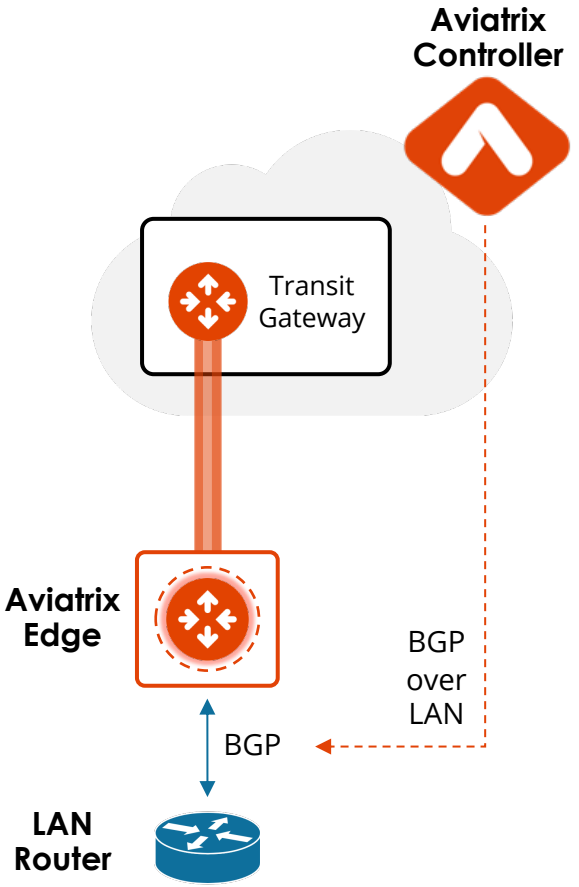
2 Deploy Edge virtual machine and attach ZTP .iso



3 Attach Edge to Transit



4 Connect Edge to External Device (LAN Router)

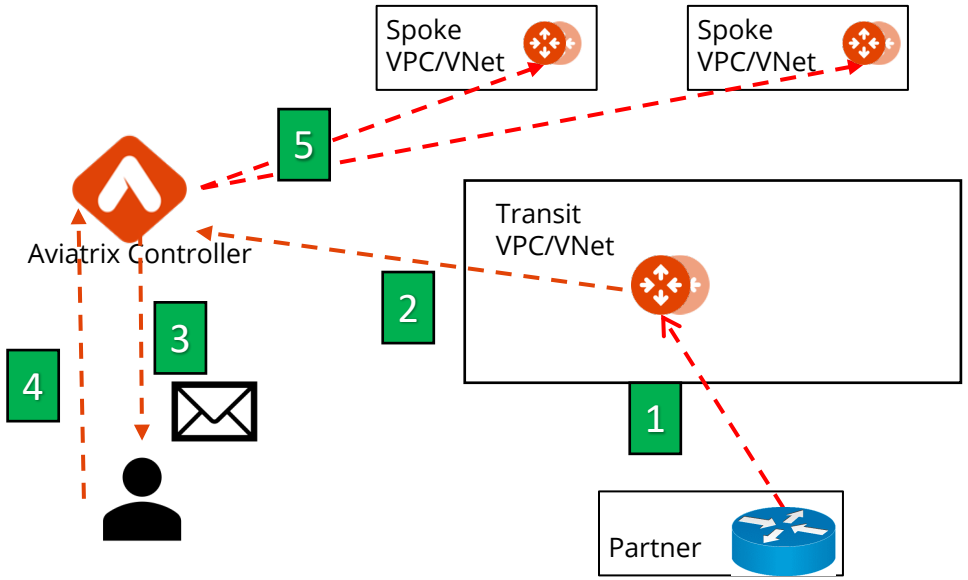


BGP Route Approval

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

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



From Aviatrix Controller: Route Approval Request

N

no-reply@aviatrix.com <no-reply@aviatrix.com>

To: Umair Hoodbhoy

Number of Events: 1.

****

Time Detected: 2022-07-21 13:55:43.288542

Request approval for new learned CIDR(s):

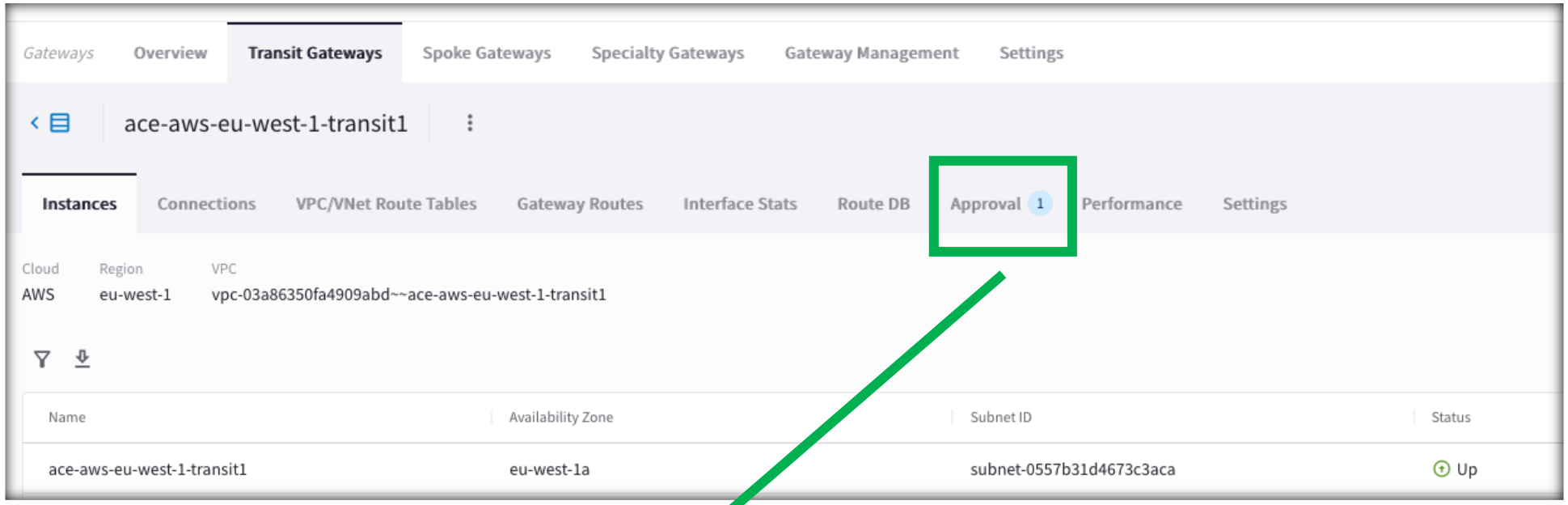
Gateway: aws-us-east-1-transit1, Connection: ONPREM-DC, CIDRs(1): 10.120.96.0/20

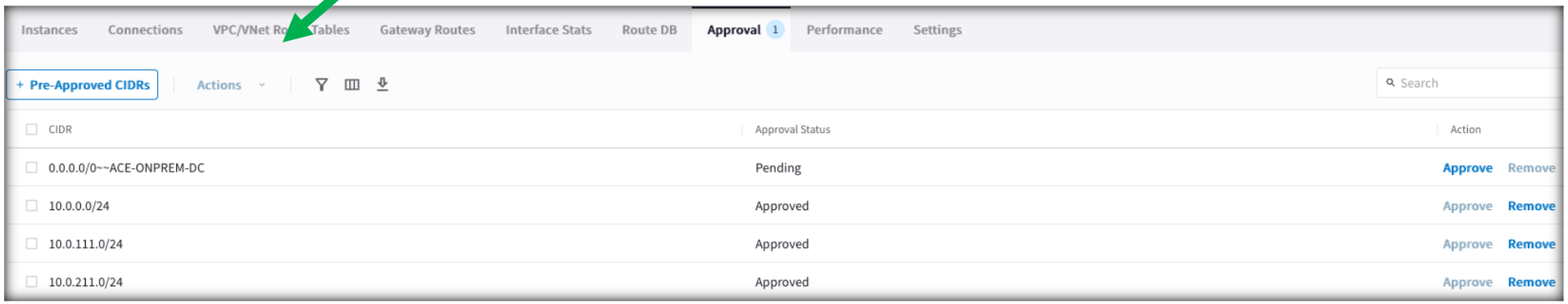
To approve, please login to the Aviatrix Controller and go to Multi-Cloud Transit-> Approval.

Controller IP: 54.163.74.31
Controller Name: ACE Inc
Controller Version: UserConnect-6.7.1324
Time Detected: 2022-07-21 13:55:43.289339

BGP Route Approval – Config

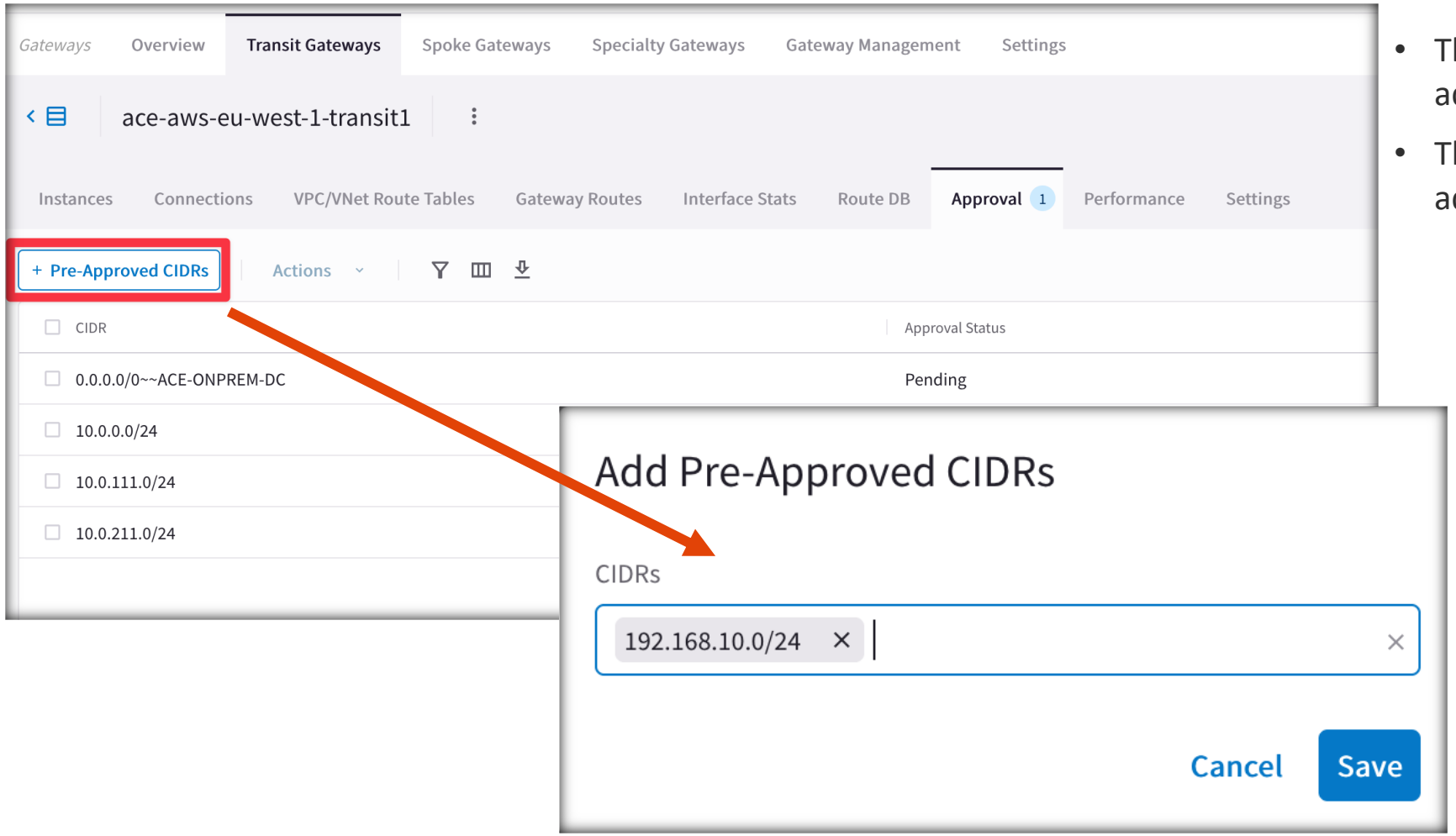
- **PATH:** CoPilot > Cloud Fabric > Gateways > select the relevant Gateway





BGP Route Approval – Config – Pre-Approved CIDRs

- **PATH:** CoPilot > Cloud Fabric > Gateways > select the relevant Gateway > Approval

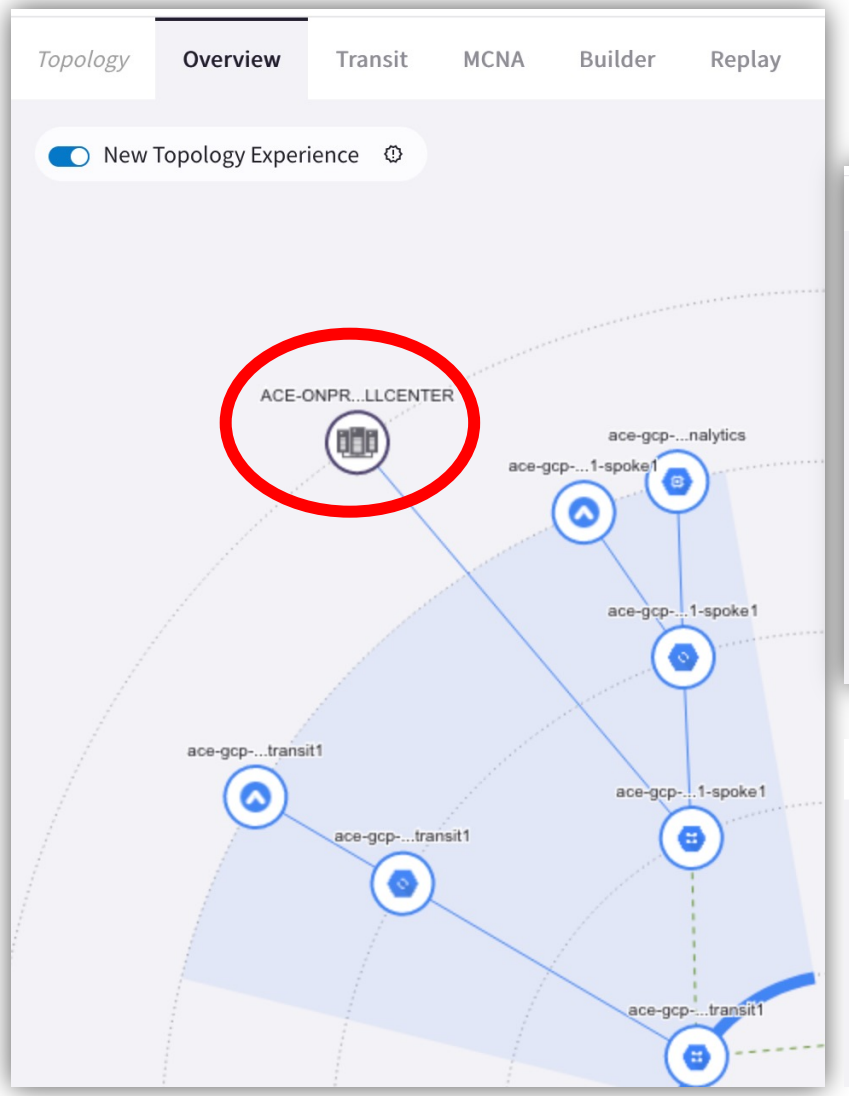


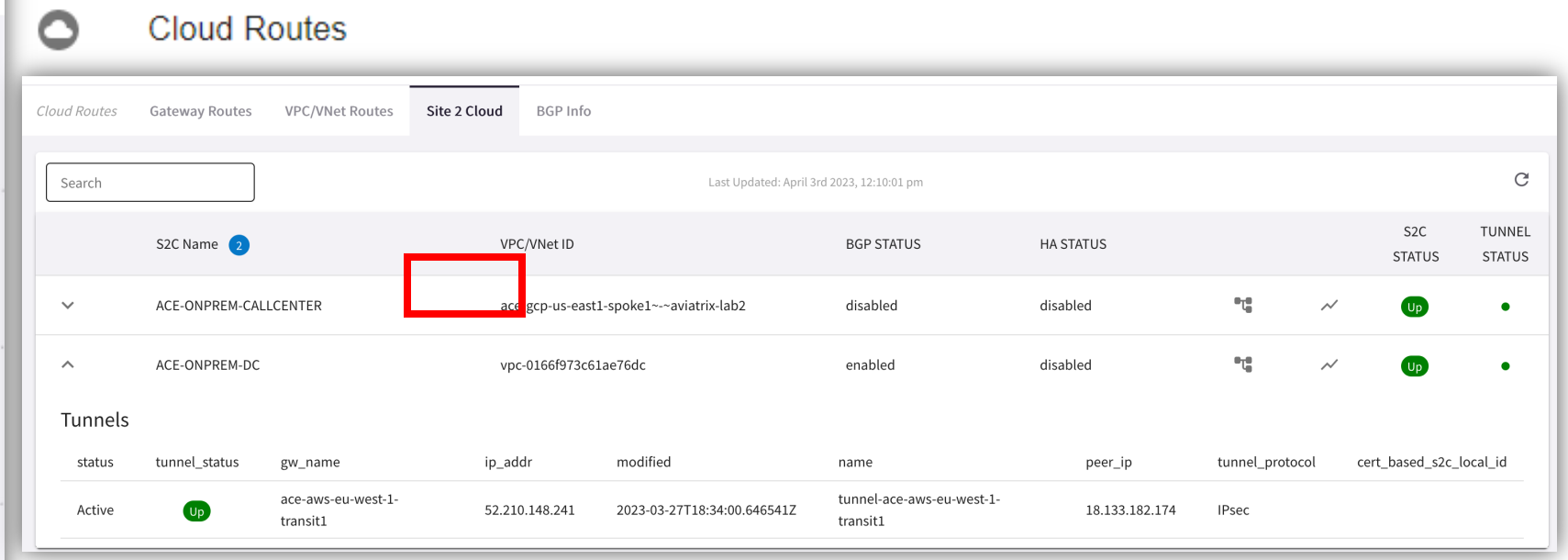
- This feature allows to pre-approving CIDRs advertised by external networks.
- The CIDRs will be propagated without the administrator logs into the CoPilot

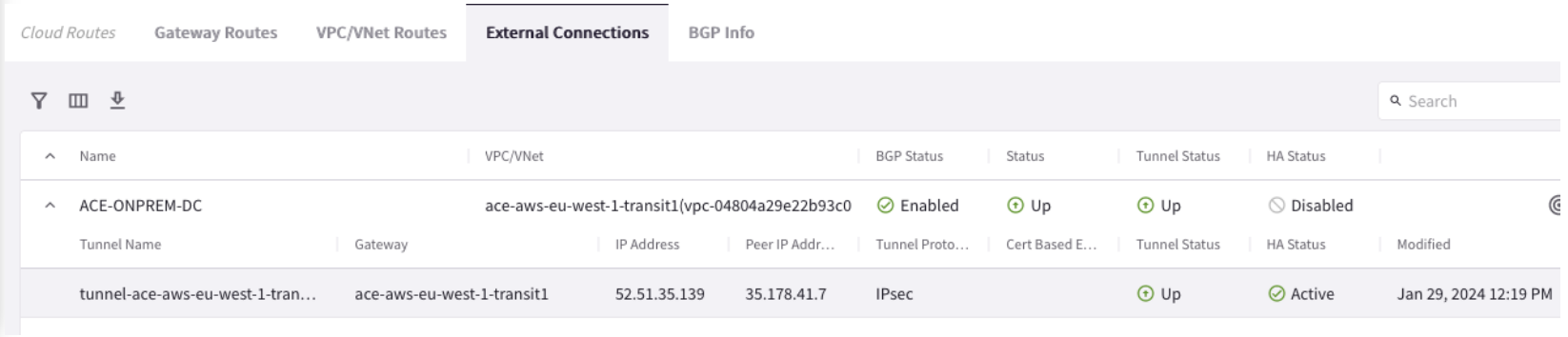
Site2Cloud & CoPilot

Site2Cloud Visibility via CoPilot

- **PATH:** COPILOT > Troubleshoot > Cloud Routes > **Site 2 Cloud**

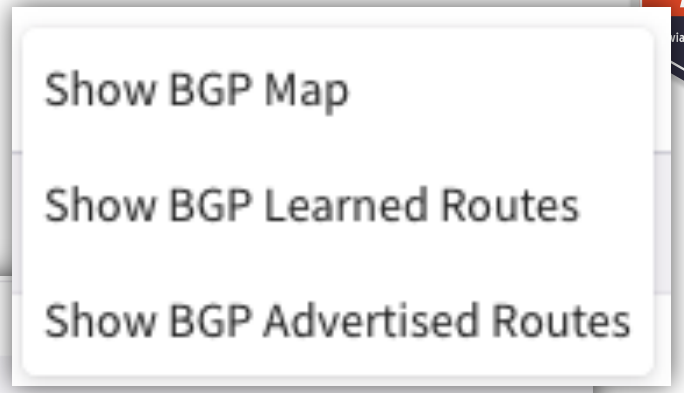


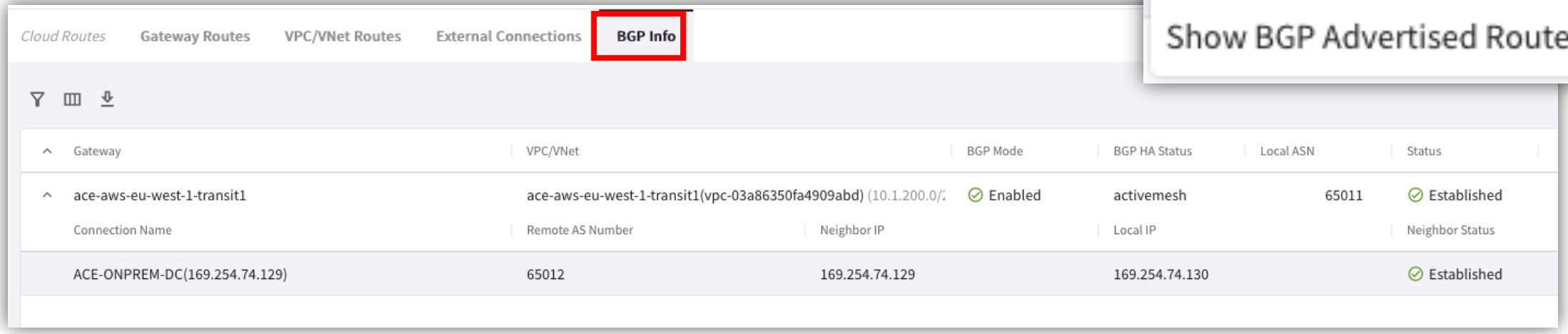


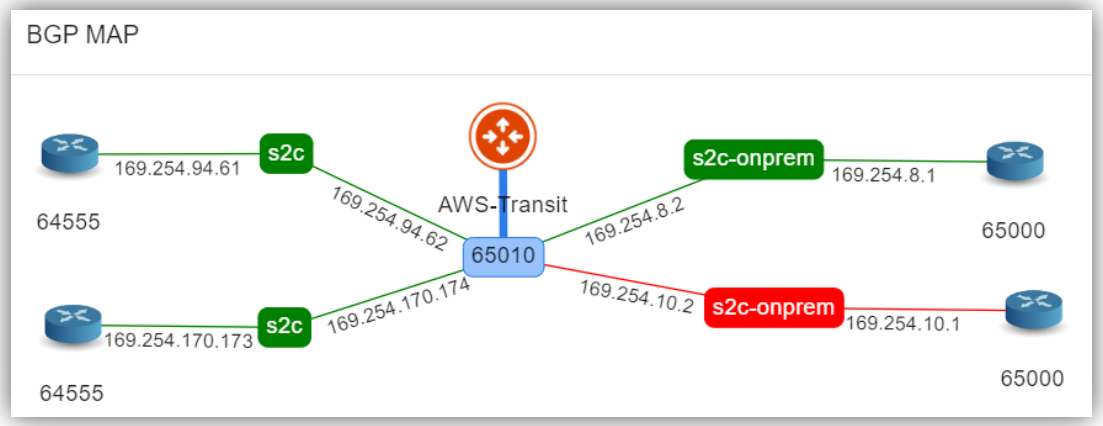


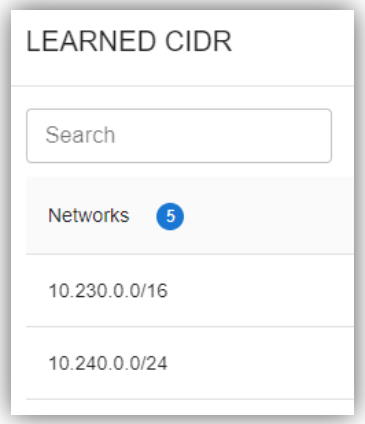
Site2Cloud BGP via CoPilot

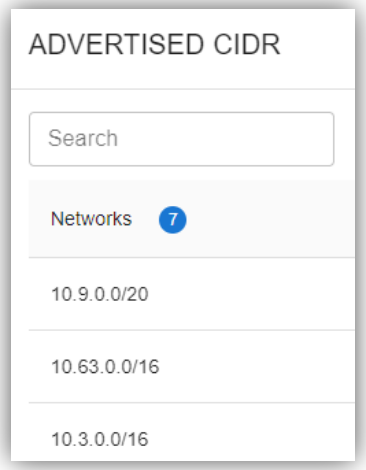
- **PATH:** COPILOT > Diagnostics > Cloud Routes > **BGP Info**





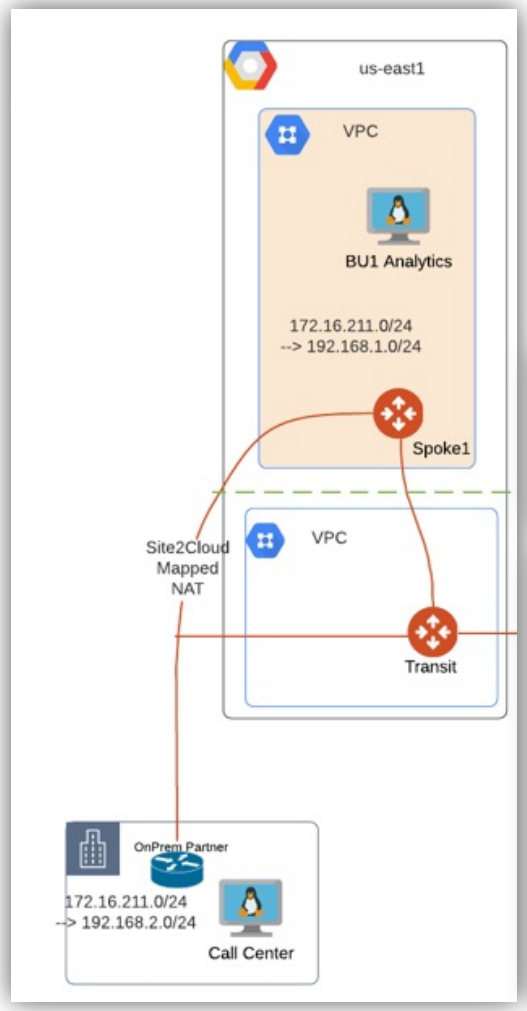


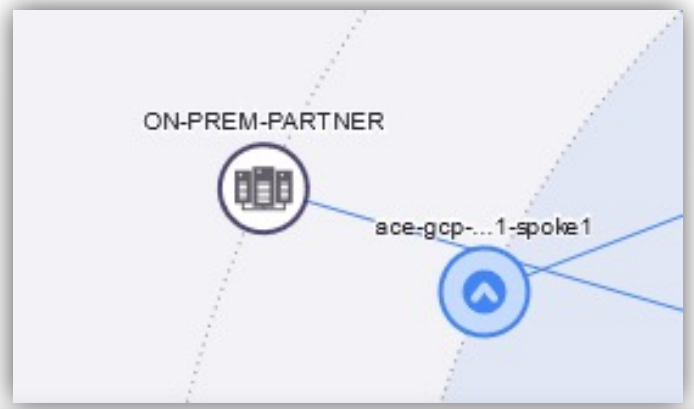


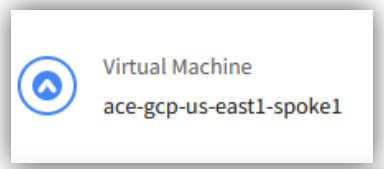


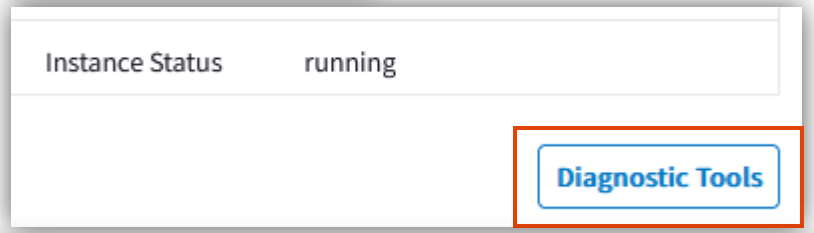
Site2Cloud Sessions via CoPilot

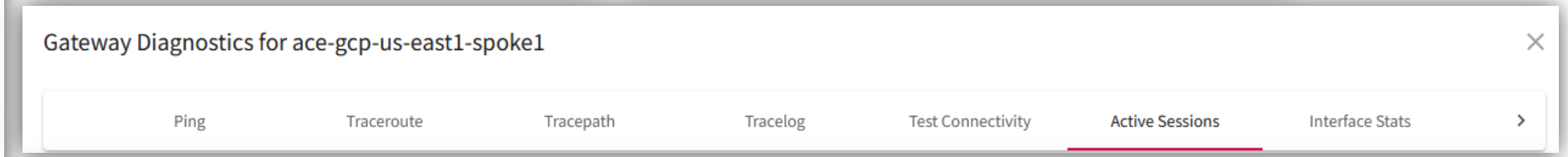
- **PATH:** COPILOT > Cloud Topology > Topology > select the concerned Gateway > **Diagnostic Tools**

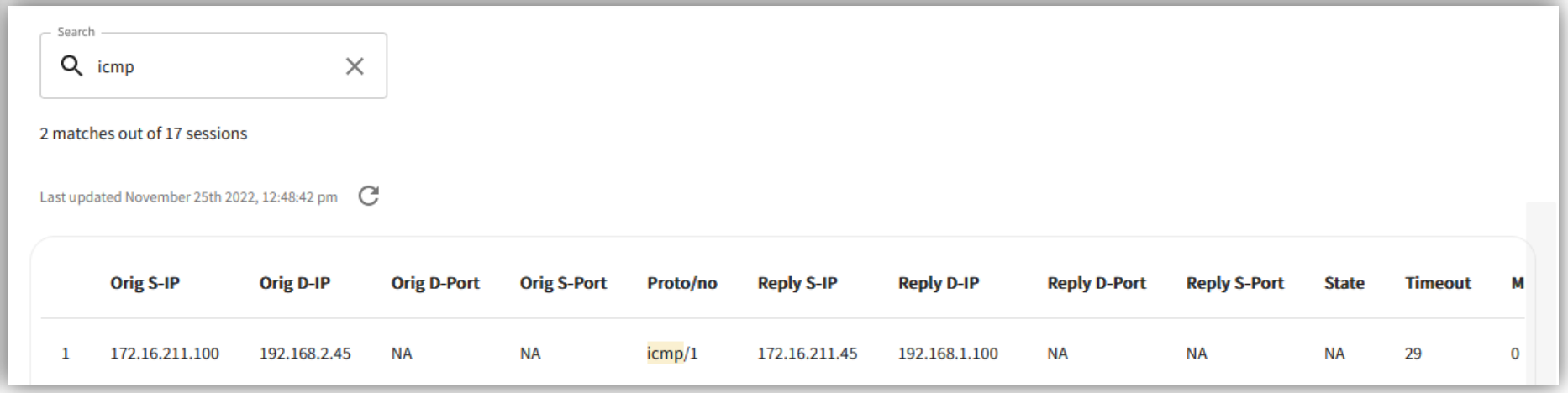












Next: Lab 6 Site2Cloud