

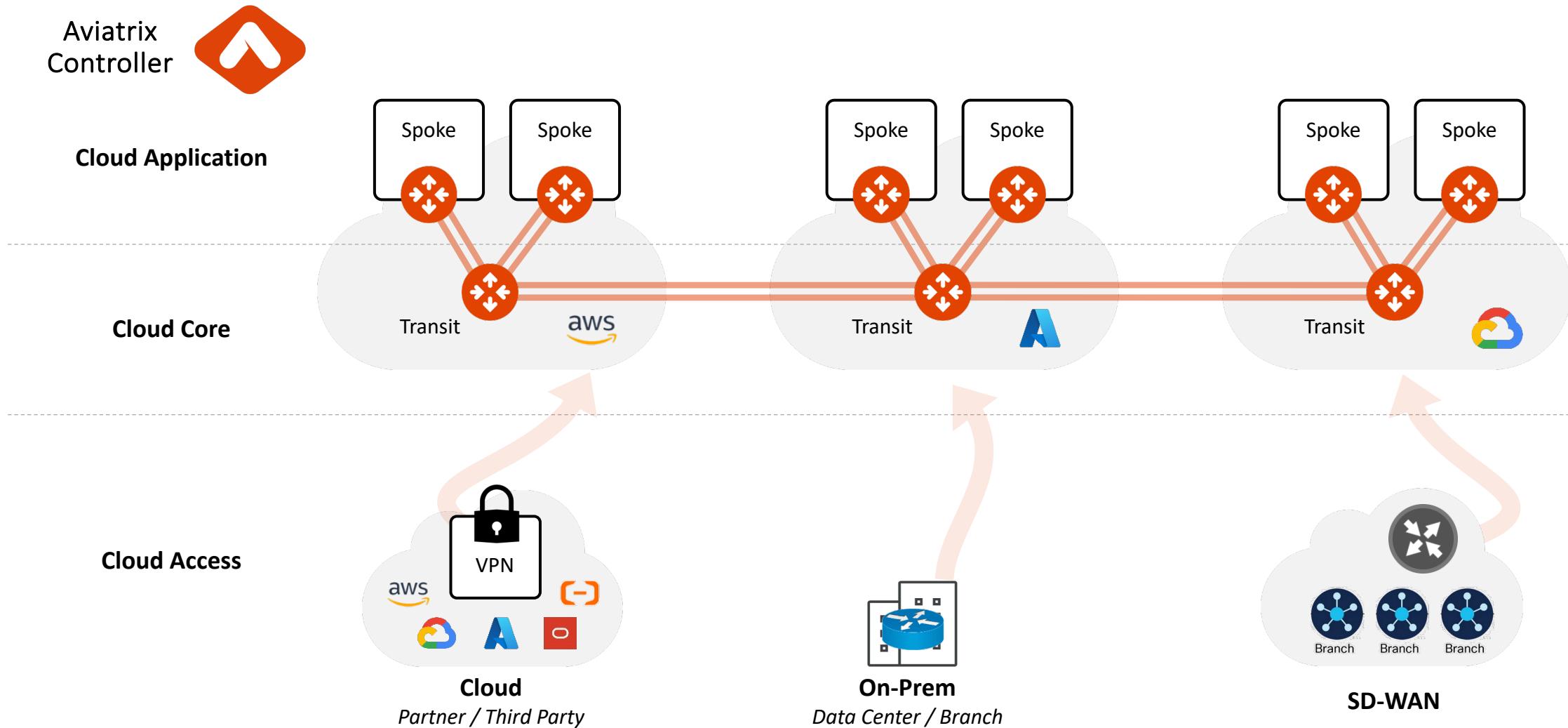


Site2Cloud

ACE Solutions Architecture Team



Aviatrix Multicloud Network Architecture

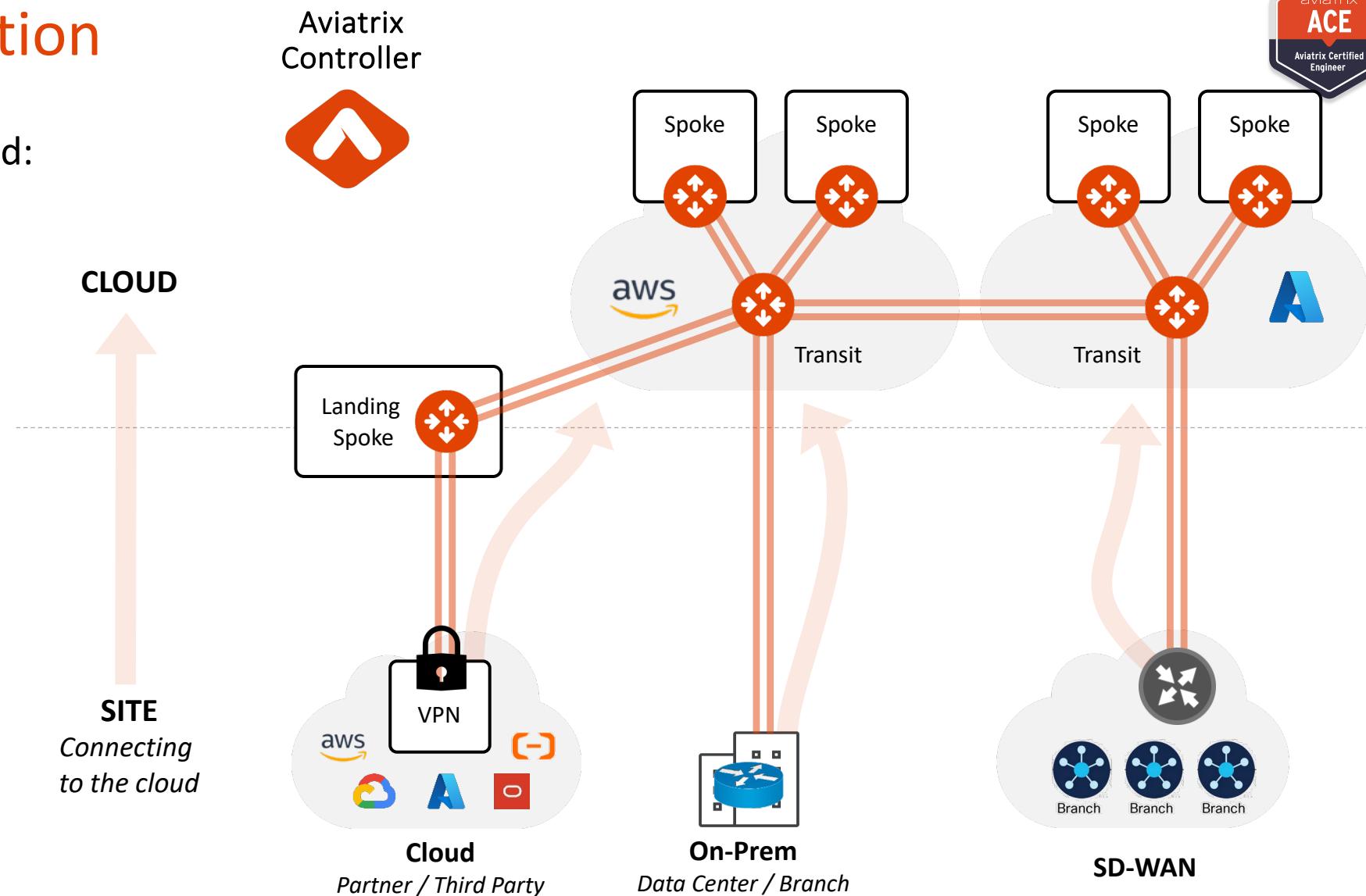


Site2Cloud Introduction



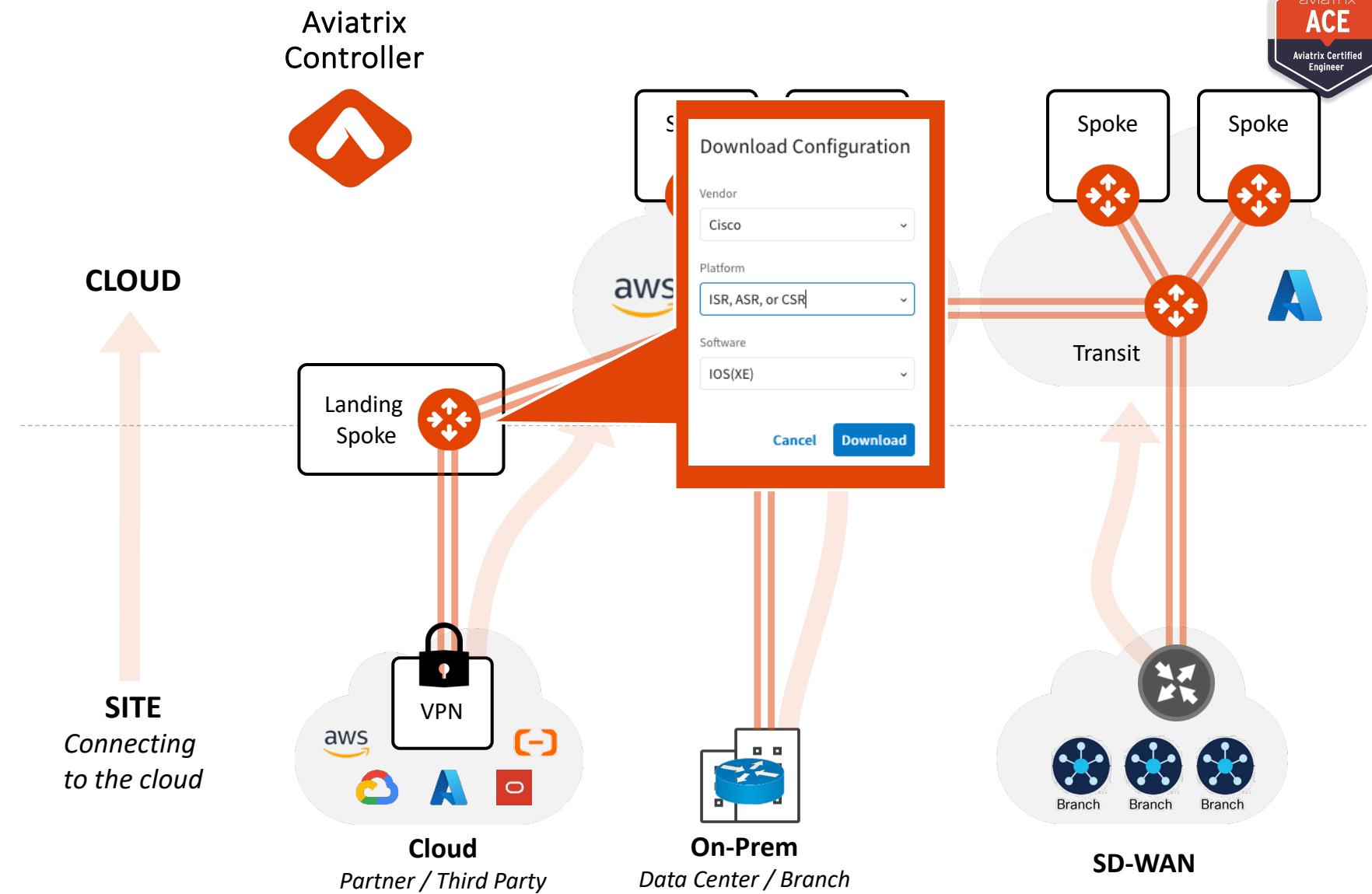
IPsec connection to Public Cloud:

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



Site2Cloud Solution

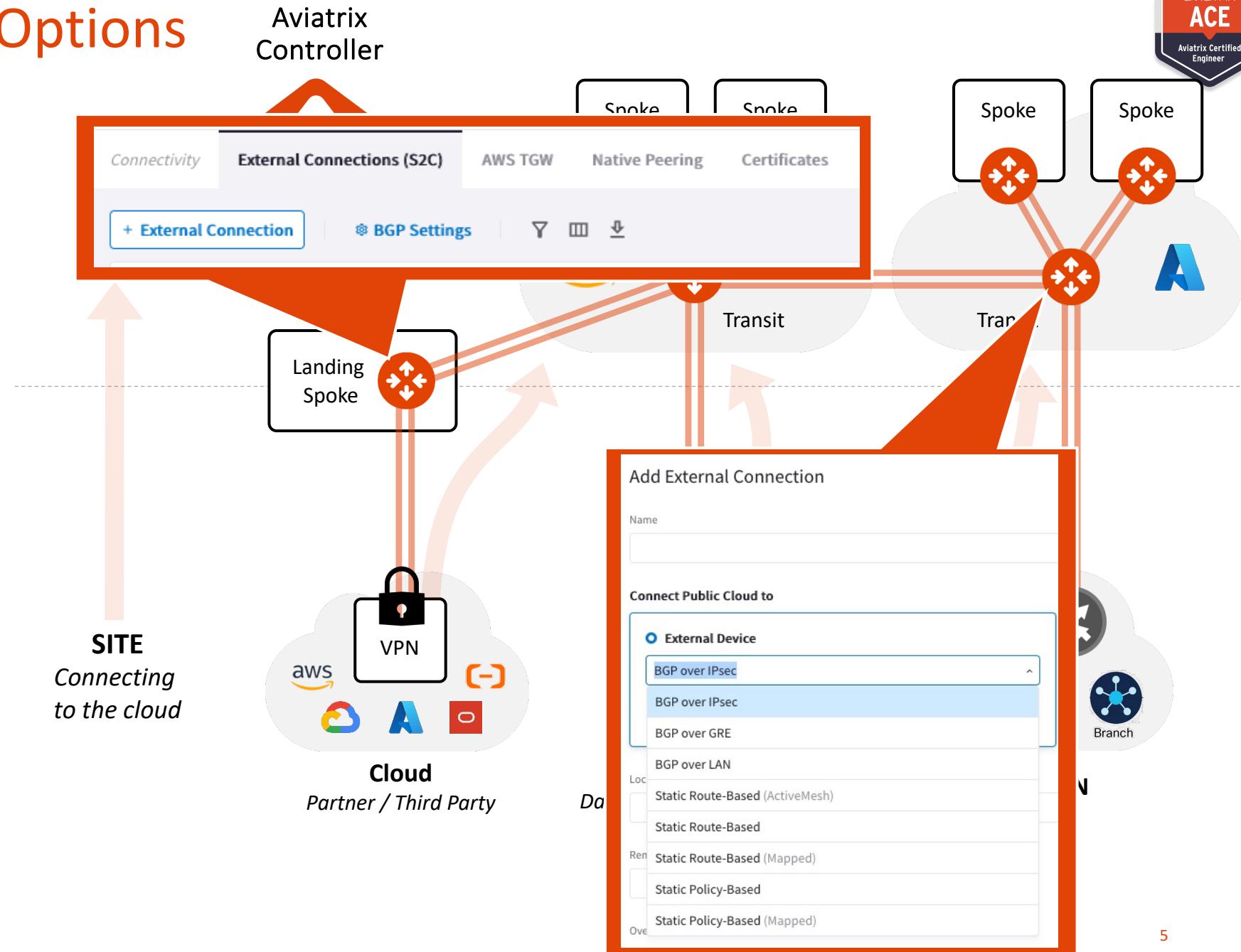
- Easy to use and template-driven
- Built-in diagnostic tools
- Solves Overlapping IPs Challenges



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

Add External Connection

ACE-Branch

Connect Public Cloud to

External Device

Static Route-Based (Mapped)

Connect overlapping networks between the cloud and on-prem from Spoke / Regular Gateway.

Custom Mapped Off

Local Gateway: ace-aws-eu-west-1-spoke2

Real Local Subnet CIDR(s): 172.16.10.0/24

Virtual Local Subnet CIDR(s): 192.168.10.0/24

Remote Gateway Type: Generic

Real Remote Subnet CIDR(s): 172.16.10.0/24

Virtual Remote Subnet CIDR(s): 192.168.20.0/24

Advanced Settings

Authentication Method: PSK Certificate

Pre-Shared Key Optional

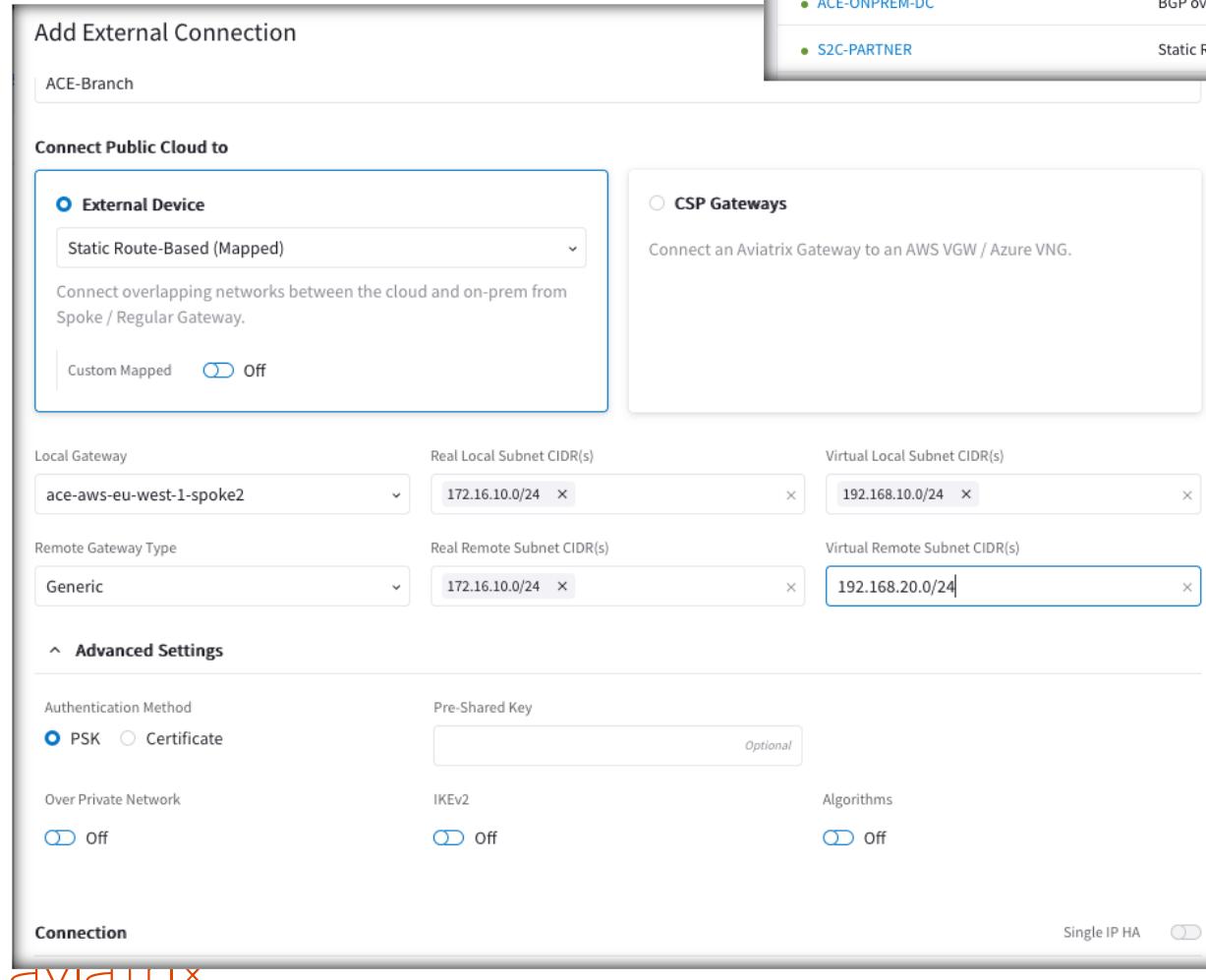
Over Private Network Off

IKEv2 Off

Algorithms off

Single IP HA

Connection

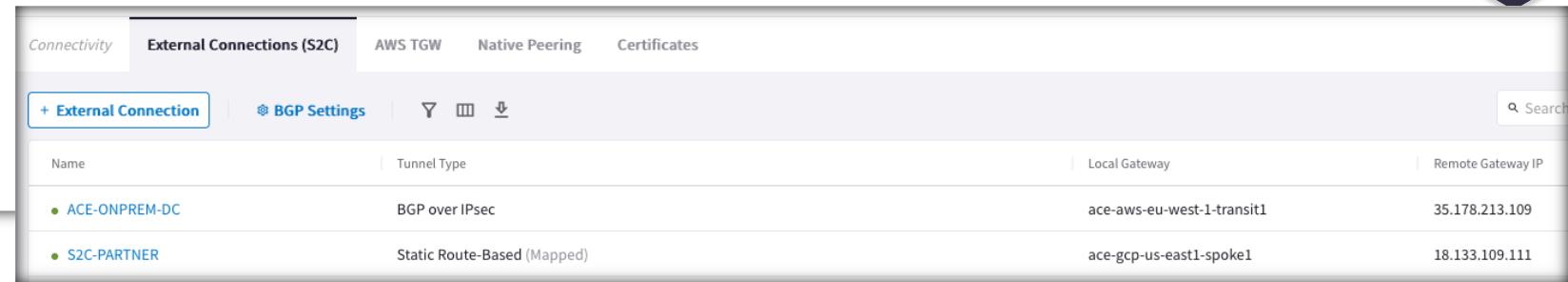


Connectivity **External Connections (S2C)** AWS TGW Native Peering Certificates

+ External Connection ⚙ BGP Settings Y □ ▾

| Name | Tunnel Type | Local Gateway | Remote Gateway IP |
|---------------|-----------------------------|----------------------------|-------------------|
| ACE-ONPREM-DC | BGP over IPsec | ace-aws-eu-west-1-transit1 | 35.178.213.109 |
| S2C-PARTNER | Static Route-Based (Mapped) | ace-gcp-us-east1-spoke1 | 18.133.109.111 |

Search



External Device

BGP over IPsec

BGP over GRE

BGP over LAN

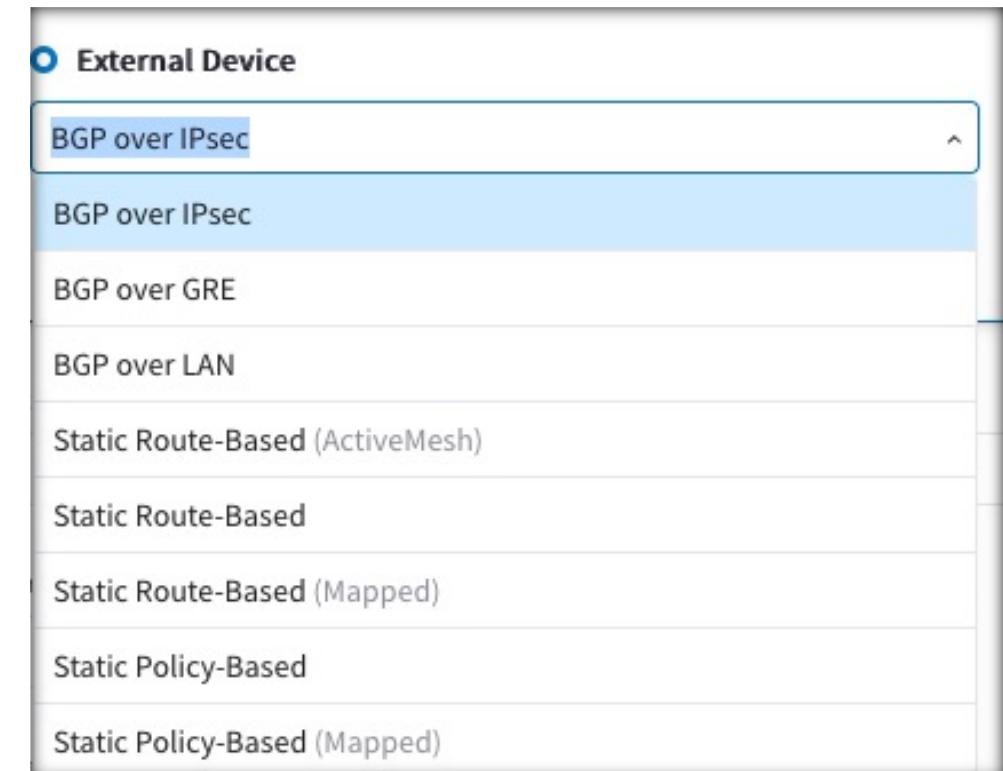
Static Route-Based (ActiveMesh)

Static Route-Based

Static Route-Based (Mapped)

Static Policy-Based

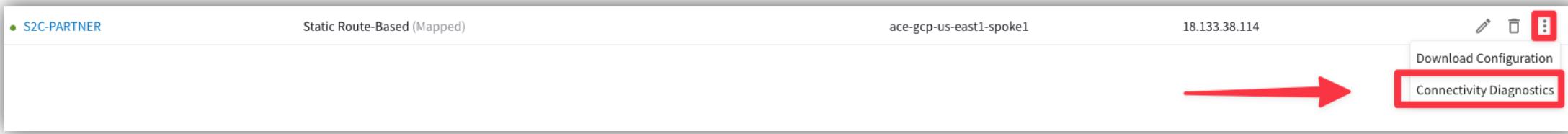
Static Policy-Based (Mapped)





Monitoring & Troubleshooting Site2Cloud

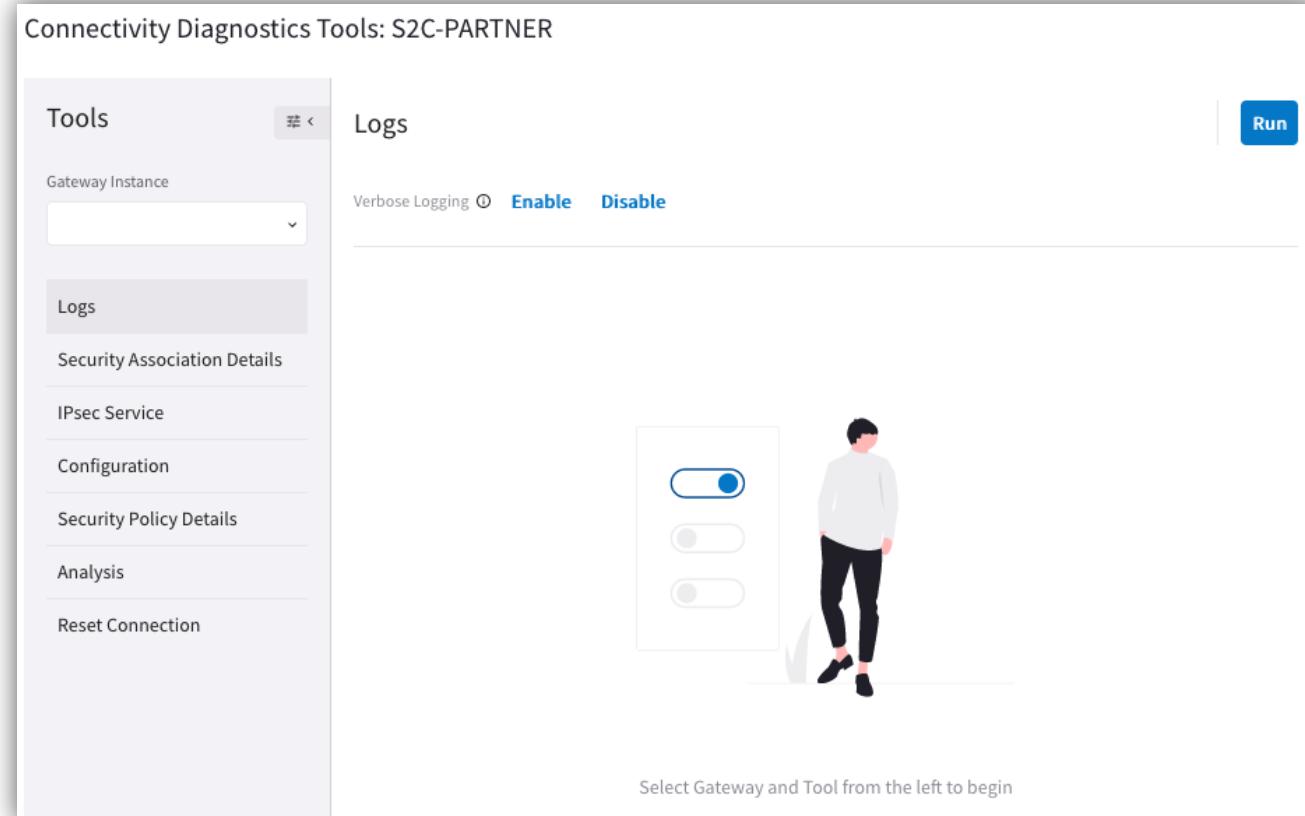
Connectivity Diagnostics



S2C-PARTNER Static Route-Based (Mapped) ace-gcp-us-east1-spoke1 18.133.38.114

Download Configuration
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



Connectivity Diagnostics Tools: S2C-PARTNER

Tools

Gateway Instance

Logs

Security Association Details

IPsec Service

Configuration

Security Policy Details

Analysis

Reset Connection

Logs

Verbose Logging Enable Disable

Run

Select Gateway and Tool from the left to begin

Monitoring – SPI

Cisco IOS Output

```
CiscoRouter#sh crypto ipsec sa interface tunl1

interface: Tunnell
  Crypto map tag: Tunnell-head-0, local addr 10.120.112.22
  <SNIP>
  local crypto endpt.: 10.120.112.22, remote crypto endpt.: 52.203.177.219
  plaintext mtu 1422, path mtu 1500, ip mtu 1500, ip mtu idb
GigabitEthernet1
  current outbound spi: 0x6011AE9(100735721)
  PFS (Y/N): Y, DH group: group14

  inbound esp sas:
    spi: 0xB1CDC56E(2983052654)
      transform: esp-256-aes esp-sha256-hmac ,
      in use settings ={Tunnel UDP-Encaps, }
      conn id: 5229, flow_id: CSR:3229, sibling_flags FFFFFFFF80004048,
  crypto map: Tunnell-head-0
    sa timing: remaining key lifetime (k/sec): (4608000/677)
    IV size: 16 bytes
    replay detection support: Y
    Status: ACTIVE(ACTIVE)
    spi: 0x5F054D46(1594182982)
      transform: esp-256-aes esp-sha256-hmac ,
      in use settings ={Tunnel UDP-Encaps, }
      conn id: 5235, flow_id: CSR:3235, sibling_flags FFFFFFFF80000048,
  crypto map: Tunnell-head-0
    sa timing: remaining key lifetime (k/sec): (4607944/727)
    IV size: 16 bytes
    replay detection support: Y
    Status: ACTIVE(ACTIVE)
```

CoPilot > Diagnostic Tools > Connectivity Diagnostics > ‘Security Association Details’

```
10.20.0.184[4500] 3.219.34.143[4500]
  esp-udp mode=tunnel spi=1594182982 (0x5f054d46) reqid=0(0x00000000)
  E: aes-cbc 96ecdab8 87f9a01b abe59b21 0cc0481b elfaaeb4 bd569f76 ad9e792e c9c5668b
  A: hmac-sha256 00460de3 70ad31af 91eed15a 0cf33b21 172b8abe 2d9bea7f 4e9822b0 9362006f
  seq=0x00000000 replay=0 flags=0x00000000 state=mature
  created: Nov 30 17:57:14 2020 current: Nov 30 18:27:42 2020
  diff: 1828(s) hard: 3600(s) soft: 2880(s)
  last: Nov 30 17:57:26 2020 hard: 0(s) soft: 0(s)
  current: 18437(bytes) hard: 0(bytes) soft: 0(bytes)
  allocated: 374 hard: 0 soft: 0
  sadb_seq=5 pid=26586 refcnt=0
```

SPI matches on both ends

The screenshot shows the CoPilot interface with the 'Connectivity Diagnostics' tab selected. In the 'Tools' section, 'Gateway Instance' is set to 'ace-aws-eu-west-1-t...' and 'Connection' is set to 'ACE-ONPREM-DC'. The 'Security Association Details' table lists a single entry with the following details:

| Local IP | Remote IP | Protocol | spi | reqid | Transform | Created | Current |
|--------------------|-------------------|----------|------------------------------------|---------------------|---------------------------|----------------------|----------------------|
| 10.1.201.188[4500] | 35.178.41.7[4500] | esp-udp | spi=1594182982 (0x5f054d46) | reqid=0(0x00000000) | E: aes-cbc A: hmac-sha256 | Nov 30 17:57:14 2020 | Nov 30 18:27:42 2020 |

Below the table, a note states: "Last Run: Jan 30, 2024 12:59 PM" and there is a 'Run' button.

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

Connectivity Diagnostics Tools: s2c-partner

Tools

- Gateway Instance ace-gcp-us-east1-sp ...
- Logs
- Security Association Details**
- IPsec Service
- Configuration
- Security Policy Details
- Analysis
- Reset Connection

Security Association Details

Last Run: Jan 30, 2024 11:52 PM

```
172.16.211.2[4500] 3.11.235.99[4500]
  esp-udp mode=tunnel spi=978561465(0x3a53a9b9) reqid=2(0x00000002)
  E: aes-cbc bf319f33 0c38a8ee 78955df1 1ba02557 7b7f1e87 dd4dd120 e8414390 4462d2e0
  A: hmac-sha256 2cd6f1be a83d8b44 d5c4519c e232fb62 dfbe355f 5a567a52 f0c7f9c7
b46958c8
  seq=0x00000000 replay=0 flags=0x00000000 state=mature
  created: Jan 30 22:26:33 2024 current: Jan 30 22:52:54 2024
  diff: 1581(s) hard: 3960(s) soft: 3454(s)
  last: Jan 30 22:33:03 2024 hard: 0(s) soft: 0(s)
  current: 672(bytes) hard: 0(bytes) soft: 0(bytes)
  allocated: 8 hard: 0 soft: 0
  sadb_seq=1 pid=3662 refcnt=0
  3.11.235.99[4500] 172.16.211.2[4500]
  esp-udp mode=tunnel spi=3249923436(0xc1b5e56c) reqid=2(0x00000002)
  E: aes-cbc cd182749 e122cccd 9361341c 2d698735 60778402 6dbcb2d0 4c2e0ffd
  A: hmac-sha256 c9536926 532f504e 5fdcc950 d1594047 2687cecb d9e74556 e798354f
d8c93b98
  seq=0x00000000 replay=0 flags=0x00000000 state=mature
  created: Jan 30 22:26:33 2024 current: Jan 30 22:52:54 2024
  diff: 1581(s) hard: 3960(s) soft: 3253(s)
  last: Jan 30 22:33:03 2024 hard: 0(s) soft: 0(s)
  current: 672(bytes) hard: 0(bytes) soft: 0(bytes)
  allocated: 8 hard: 0 soft: 0
  sadb_seq=2 pid=3662 refcnt=0
```

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

Connectivity Diagnostics Tools: S2C-PARTNER

Tools

Gateway Instance
ace-gcp-us-east1-sp ... ×

Logs

Security Association Details

IPsec Service

Configuration

Security Policy Details

Analysis

Reset Connection

Last Run: Nov 3, 2023 3:58 PM

Run

Connection S2C-PARTNER is UP.

Close



Analysis – On-prem router is down

On-prem router is **down...**



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 – 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:

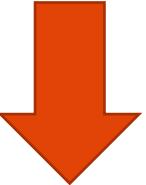
Tunnel ace-gcp-us-east1-spoke1<-->3.11.235.99: ISAKMP Phase 1 SA is not established. Possible reasons:

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](#)

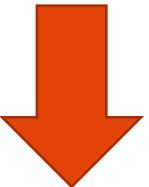
Tunnel analysis for connection s2c-partner:

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

Configuration

Last Run: Jan 31, 2024 12:09 AM | Run

```

        "id": "3.11.235.99"
    },
    "children": {
        "net-0_0_0_0-0_0_0_0_0": {
            "local_ts": [
                "0.0.0.0/0",
                "::/0"
            ],
            "remote_ts": [
                "0.0.0.0/0",
                "::/0"
            ],
            "rekey_time": 3600,
            "esp_proposals": [
                "aes256-sha256-modp2048"
            ],
        }
    }
}

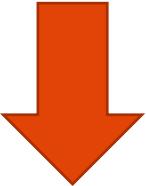
```

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#

```



Analysis

Last Run: Jan 31, 2024 12:24 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

```

Diagnostics – show logs

Connectivity Diagnostics Tools: S2C-PARTNER

Tools

Gateway Instance: ace-gcp-us-east1-sp ...

- Logs** (highlighted with red box)
- Security Association Details
- IPsec Service
- Configuration
- Security Policy Details
- Analysis
- Reset Connection

Last Run: Nov 3, 2023 3:57 PM

Run (highlighted with red box)

Verbose Logging: **Enable** **Disable**

```

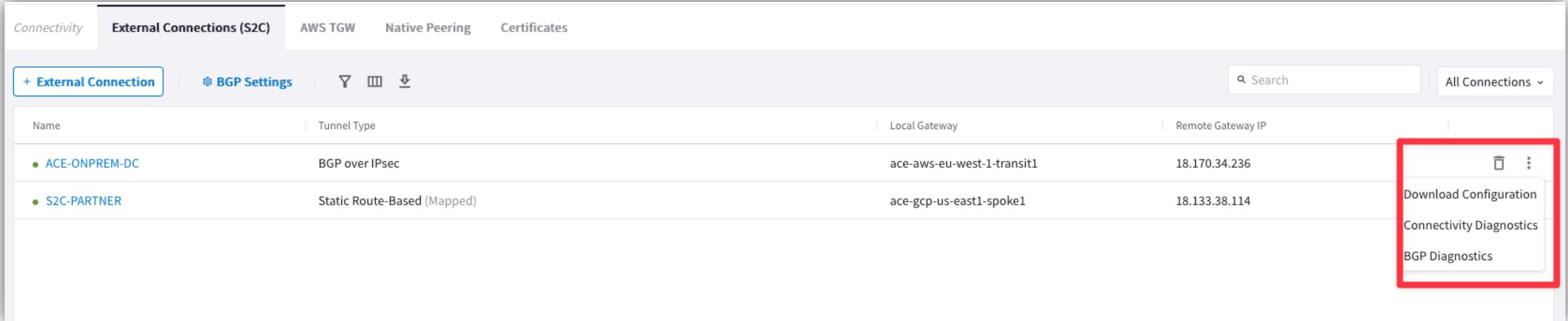
2023-11-03T14:15:58.182653+00:00 GW-ace-gcp-us-east1-spoke1-35.237.68.55 charon: 213[IKE]
<gw-172_16_211_2-18_133_38_114|8> outbound CHILD_SA net-0_0_0_0-0_0_0{54} established
with SPIs cbdd1cf6_i c535c2d4_o and TS 0.0.0.0/0 === 0.0.0.0/0
2023-11-03T14:15:58.181406+00:00 GW-ace-gcp-us-east1-spoke1-35.237.68.55 charon: 213[IKE]
<gw-172_16_211_2-18_133_38_114|8> CHILD_SA closed
2023-11-03T14:15:58.181000+00:00 GW-ace-gcp-us-east1-spoke1-35.237.68.55 charon: 213[IKE]
<gw-172_16_211_2-18_133_38_114|8> sending DELETE for ESP CHILD_SA with SPI cf004751
2023-11-03T14:15:58.180647+00:00 GW-ace-gcp-us-east1-spoke1-35.237.68.55 charon: 213[IKE]
<gw-172_16_211_2-18_133_38_114|8> closing CHILD_SA net-0_0_0_0-0_0_0{52} with SPIs
cf004751_i (2268 bytes) b44433dd_o (2268 bytes) and TS 0.0.0.0/0 === 0.0.0.0/0
2023-11-03T14:15:58.180039+00:00 GW-ace-gcp-us-east1-spoke1-35.237.68.55 charon: 213[IKE]
<gw-172_16_211_2-18_133_38_114|8> received DELETE for ESP CHILD_SA with SPI b44433dd
2023-11-03T14:15:58.072201+00:00 GW-ace-gcp-us-east1-spoke1-35.237.68.55 charon: 212[ENC]
<gw-172_16_211_2-18_133_38_114|8> generating CREATE_CHILD_SA response 1004 [ SA No KE TSi
TSr ]
2023-11-03T14:15:58.071101+00:00 GW-ace-gcp-us-east1-spoke1-35.237.68.55 charon: 212[IKE]
<gw-172_16_211_2-18_133_38_114|8> inbound CHILD_SA net-0_0_0_0-0_0_0{54} established
with SPIs cbdd1cf6_i c535c2d4_o and TS 0.0.0.0/0 === 0.0.0.0/0
2023-11-03T14:15:58.063697+00:00 GW-ace-gcp-us-east1-spoke1-35.237.68.55 charon: 212[ENC]
<gw-172_16_211_2-18_133_38_114|8> parsed CREATE_CHILD_SA request 1004 [ N(REKEY_SA) SA No KE
TSi TSr ]
2023-11-03T13:21:11.679741+00:00 GW-ace-gcp-us-east1-spoke1-35.237.68.55 charon: 105[IKE]
<gw-172_16_211_2-18_133_38_114|8> outbound CHILD_SA net-0_0_0_0-0_0_0{52} established
with SPIs cf004751_i b44433dd_o and TS 0.0.0.0/0 === 0.0.0.0/0
2023-11-03T13:21:11.678766+00:00 GW-ace-gcp-us-east1-spoke1-35.237.68.55 charon: 105[IKE]
<gw-172_16_211_2-18_133_38_114|8> CHILD_SA closed

```

Close

BGP Troubleshooting

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



The screenshot shows the Aviatrix CoPilot interface with the 'External Connections (S2C)' tab selected. The table lists two connections:

| Name | Tunnel Type | Local Gateway | Remote Gateway IP |
|---------------|-----------------------------|----------------------------|-------------------|
| ACE-ONPREM-DC | BGP over IPsec | ace-aws-eu-west-1-transit1 | 18.170.34.236 |
| S2C-PARTNER | Static Route-Based (Mapped) | ace-gcp-us-east1-spoke1 | 18.133.38.114 |

A context menu is open for the 'ACE-ONPREM-DC' connection, with the following options:

- Download Configuration
- Connectivity Diagnostics
- BGP Diagnostics

BGP Troubleshooting – List of commands

BGP Diagnostics Tools: ACE-ONPREM-DC

Tools

Gateway Instance

ace-aws-eu-west... ×

BGP Command

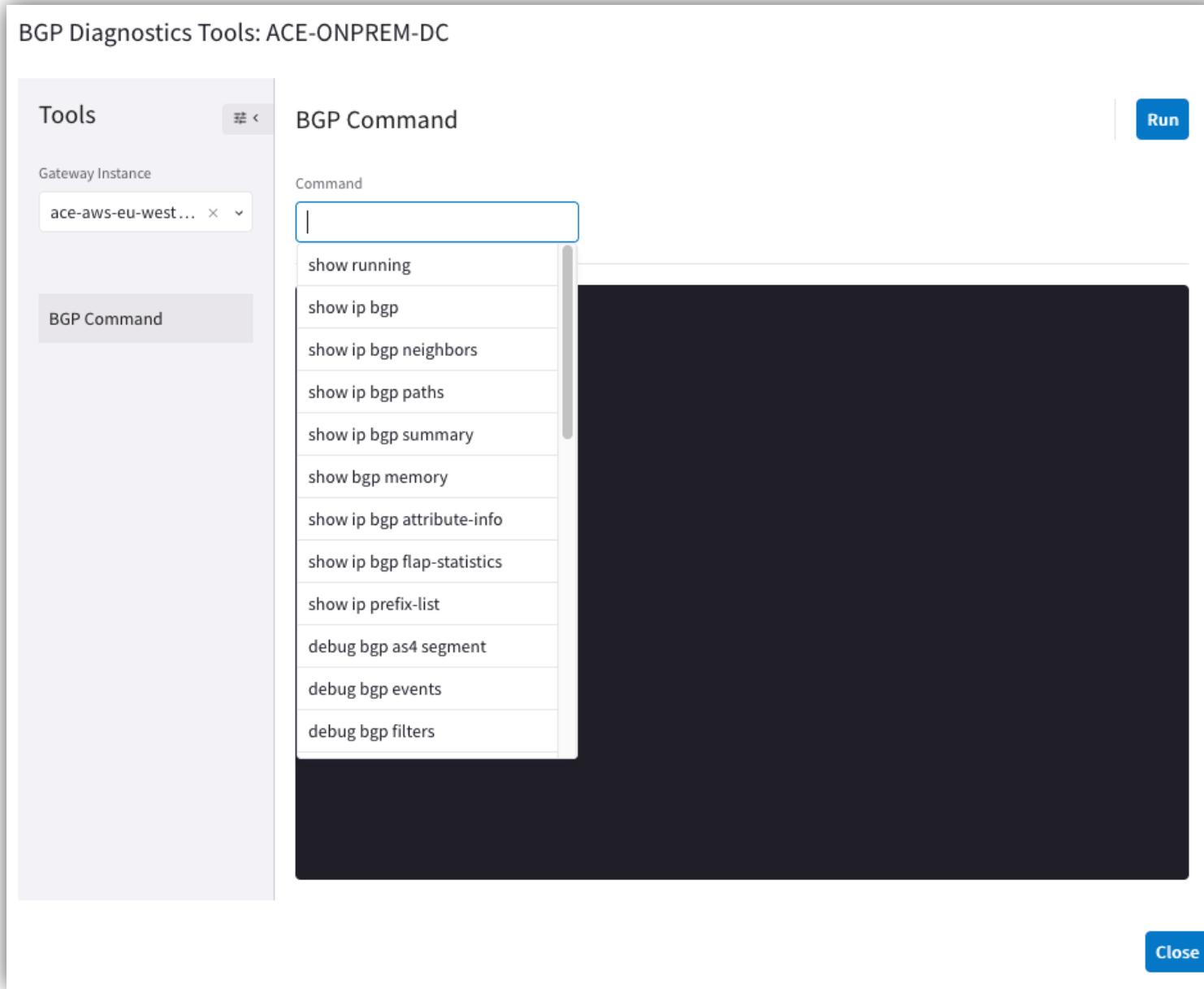
BGP Command

Command

- show running
- show ip bgp
- show ip bgp neighbors
- show ip bgp paths
- show ip bgp summary
- show bgp memory
- show ip bgp attribute-info
- show ip bgp flap-statistics
- show ip prefix-list
- debug bgp as4 segment
- debug bgp events
- debug bgp filters

Run

Close



BGP Troubleshooting – show running

BGP Diagnostics Tools: ACE-ONPREM-DC

Tools < BGP Command Last Run: Nov 3, 2023 4:15 PM Run

Gateway Instance: ace-aws-eu-west... x

Command: show running

BGP Command

```
show running

Current configuration:
!
hostname ip-10-1-201-175
password 8 9vYpDhy25C4YA
log file /var/log/quagga/bgpd.log
log stdout
log syslog
service password-encryption
!
debug bgp as4
debug bgp events
debug bgp keepalives
debug bgp updates
debug bgp fsm
!
router bgp 65011
bgp router-id 169.254.74.130
network 10.1.211.0/24
network 10.1.212.0/24
network 172.16.211.0/24 route-map prepend-8ffc7ca367064962aa7f9286e8463c0e
network 192.168.211.0/24 route-map prepend-8ffc7ca367064962aa7f9286e8463c0e
network 192.168.212.0/24 route-map prepend-8ffc7ca367064962aa7f9286e8463c0e
neighbor 169.254.74.129 remote-as 65012
```

Close

BGP Troubleshooting – show ip bgp

BGP Diagnostics Tools: ACE-ONPREM-DC

Tools < BGP Command Last Run: Nov 3, 2023 4:16 PM Run

Gateway Instance: ace-aws-eu-west... x

Command: **show ip bgp**

show ip bgp
BGP table version is 0, local router ID is 169.254.74.130
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

| Network | Next Hop | Metric | LocPrf | Weight | Path |
|----------------------|----------------|--------|--------|--------|---------|
| *> 0.0.0.0 | 169.254.74.129 | | 0 | 65012 | i |
| *> 10.0.0.0/24 | 169.254.74.129 | 0 | | 0 | 65012 ? |
| *> 10.0.111.0/24 | 169.254.74.129 | 0 | | 0 | 65012 ? |
| *> 10.0.211.0/24 | 169.254.74.129 | 0 | | 0 | 65012 ? |
| *> 10.1.211.0/24 | 0.0.0.0 | 0 | | 32768 | i |
| *> 10.1.212.0/24 | 0.0.0.0 | 0 | | 32768 | i |
| *> 169.254.74.128/30 | | | | | |
| | 169.254.74.129 | 0 | | 0 | 65012 ? |
| *> 172.16.211.0/24 | 0.0.0.0 | 0 | | 32768 | 65011 i |
| *> 192.168.211.0 | 0.0.0.0 | 0 | | 32768 | 65011 i |
| *> 192.168.212.0 | 0.0.0.0 | 0 | | 32768 | 65011 i |

Displayed 10 out of 10 total prefixes

Close



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



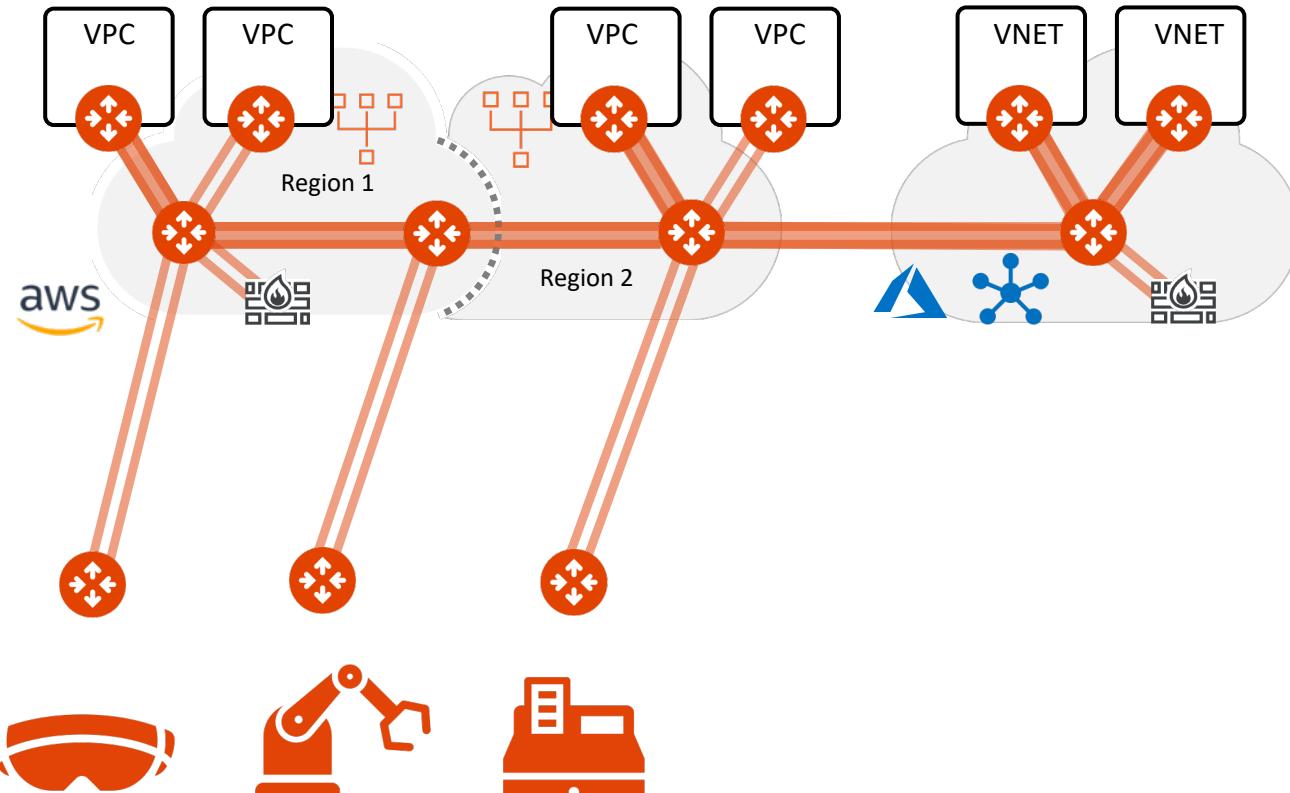
Simplified Edge Management



Consistent Secure Edge

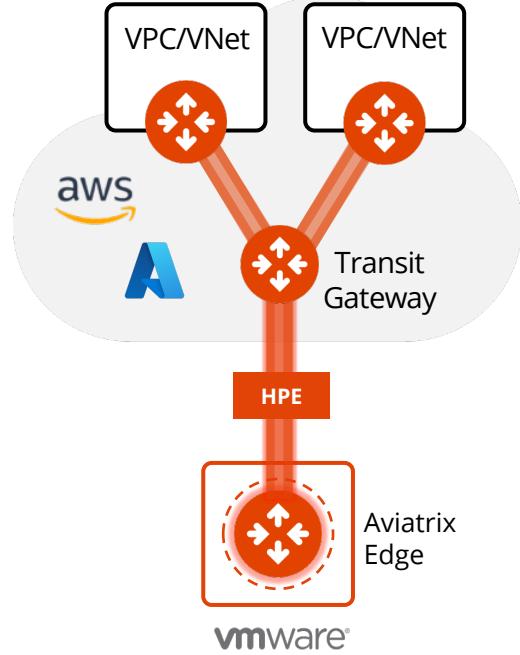


Simplified Edge On-boarding

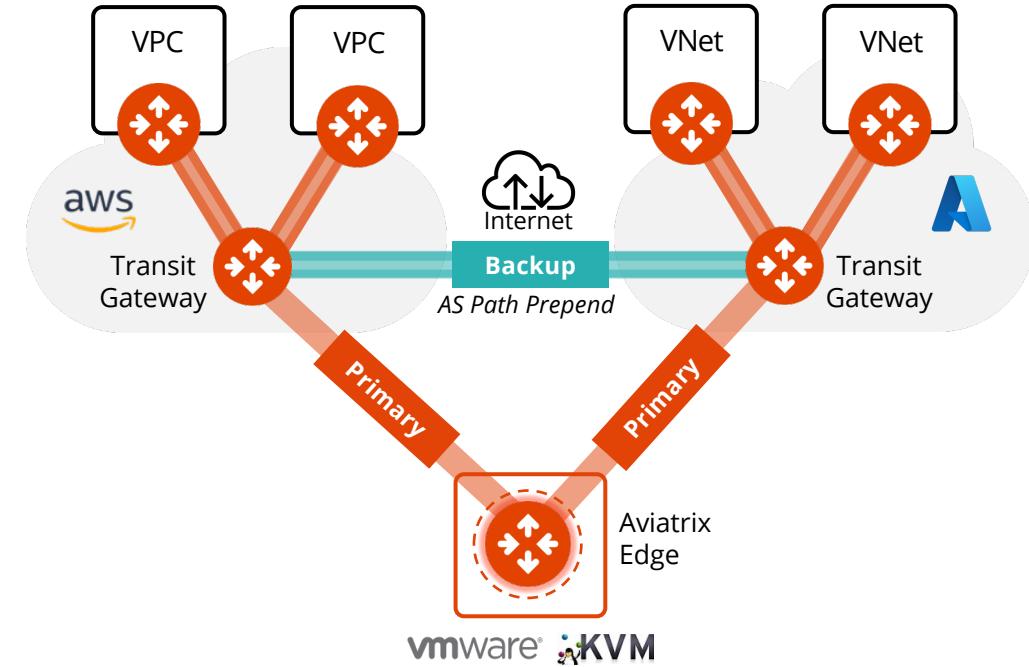


Aviatrix Edge Use Cases

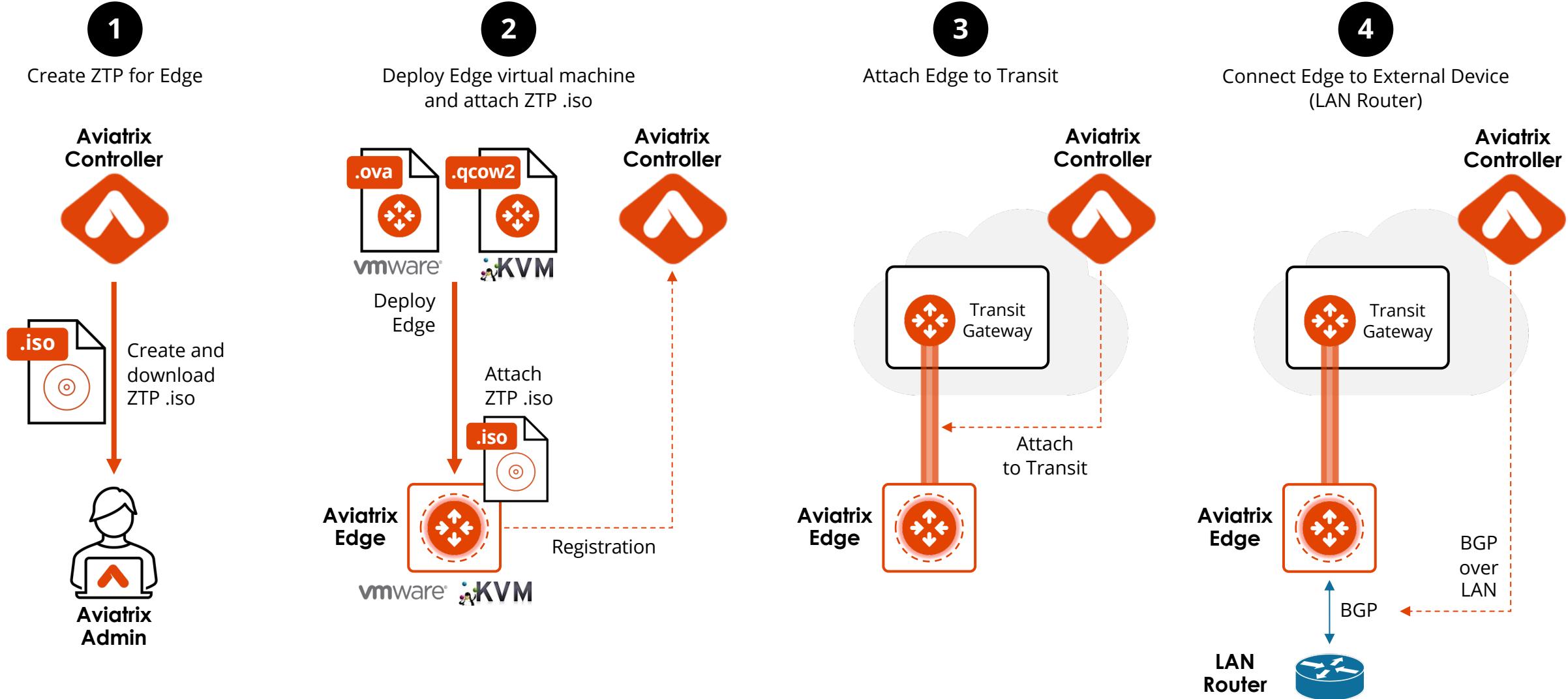
Extend the Aviatrix Platform to the Edge



Multi-Cloud Connectivity via Aviatrix Edge



Edge 2.0 Deployment Workflow - Demo



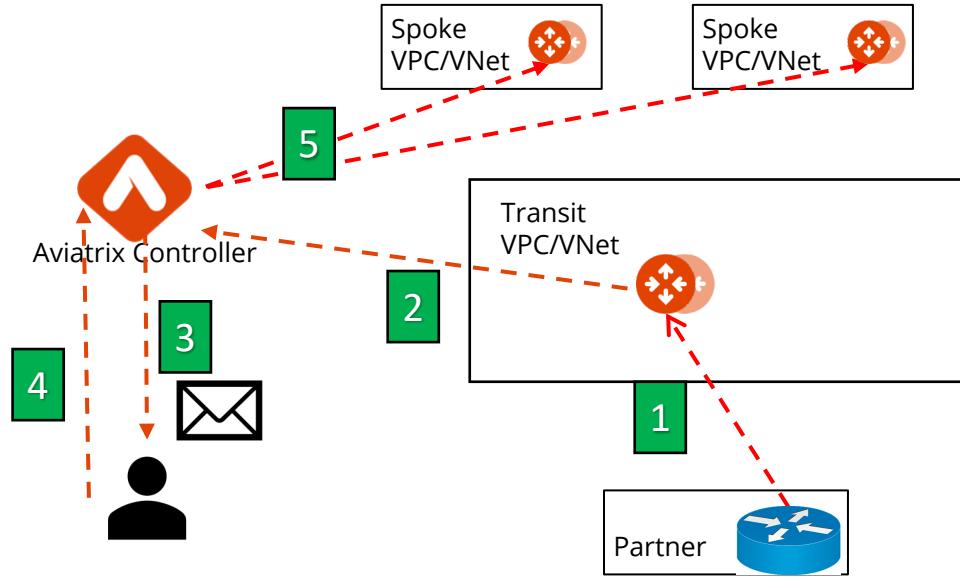


BGP Route Approval

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

 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):

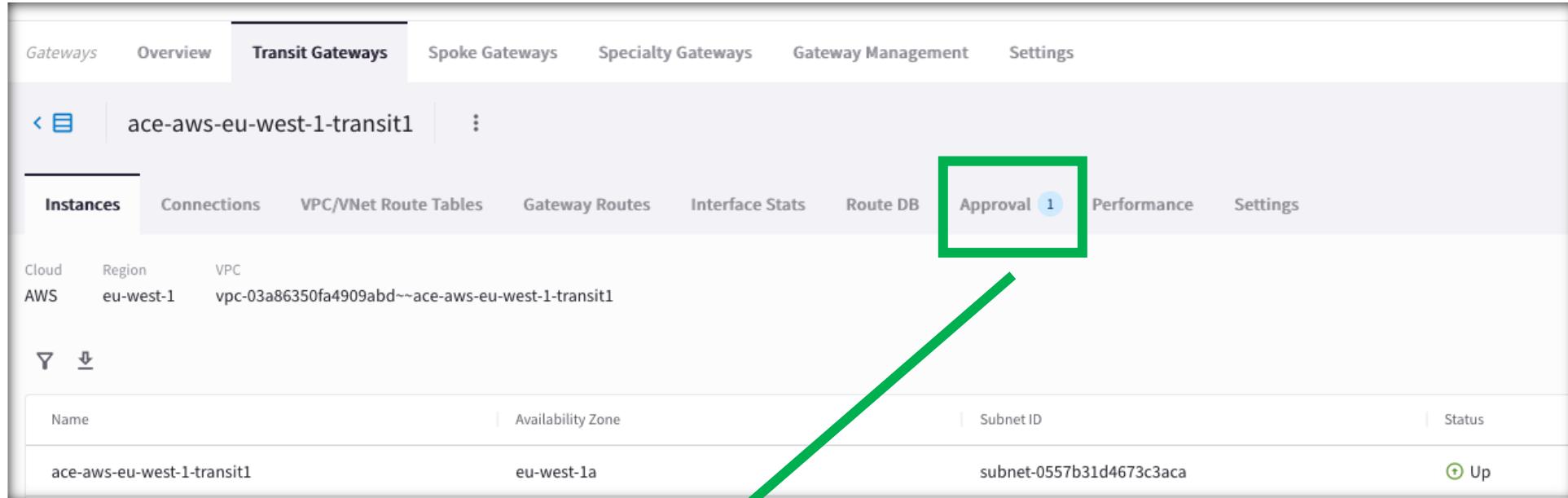
Gateway: aws-us-east-1-transit1, Connection: ONPREM-DC, CIDRs(1): 10.120.96.0/20

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

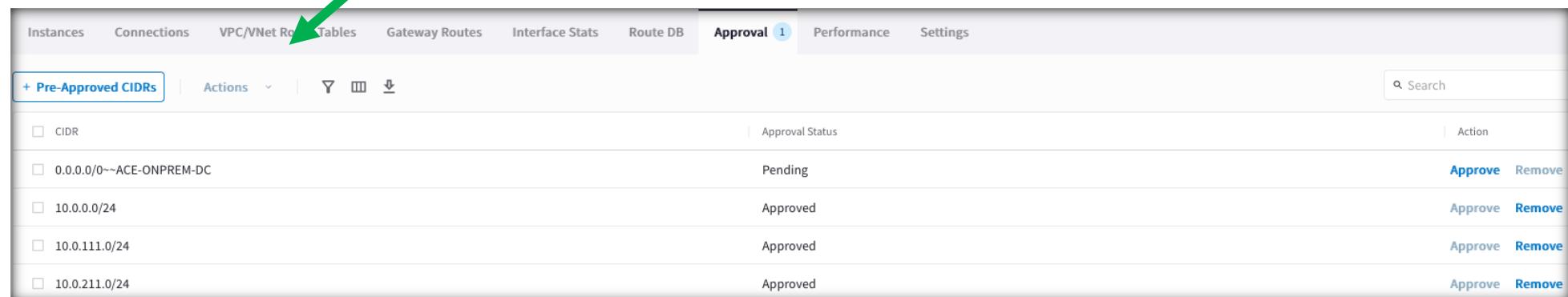
BGP Route Approval – Config

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



The screenshot shows the 'Transit Gateways' section of the CoPilot interface. A specific gateway, 'ace-aws-eu-west-1-transit1', is selected. The 'Approval' tab is highlighted with a green box and a green arrow points from it to the 'Tables' tab in the second screenshot.

| Name | Availability Zone | Subnet ID | Status |
|----------------------------|-------------------|--------------------------|--------|
| ace-aws-eu-west-1-transit1 | eu-west-1a | subnet-0557b31d4673c3aca | Up |

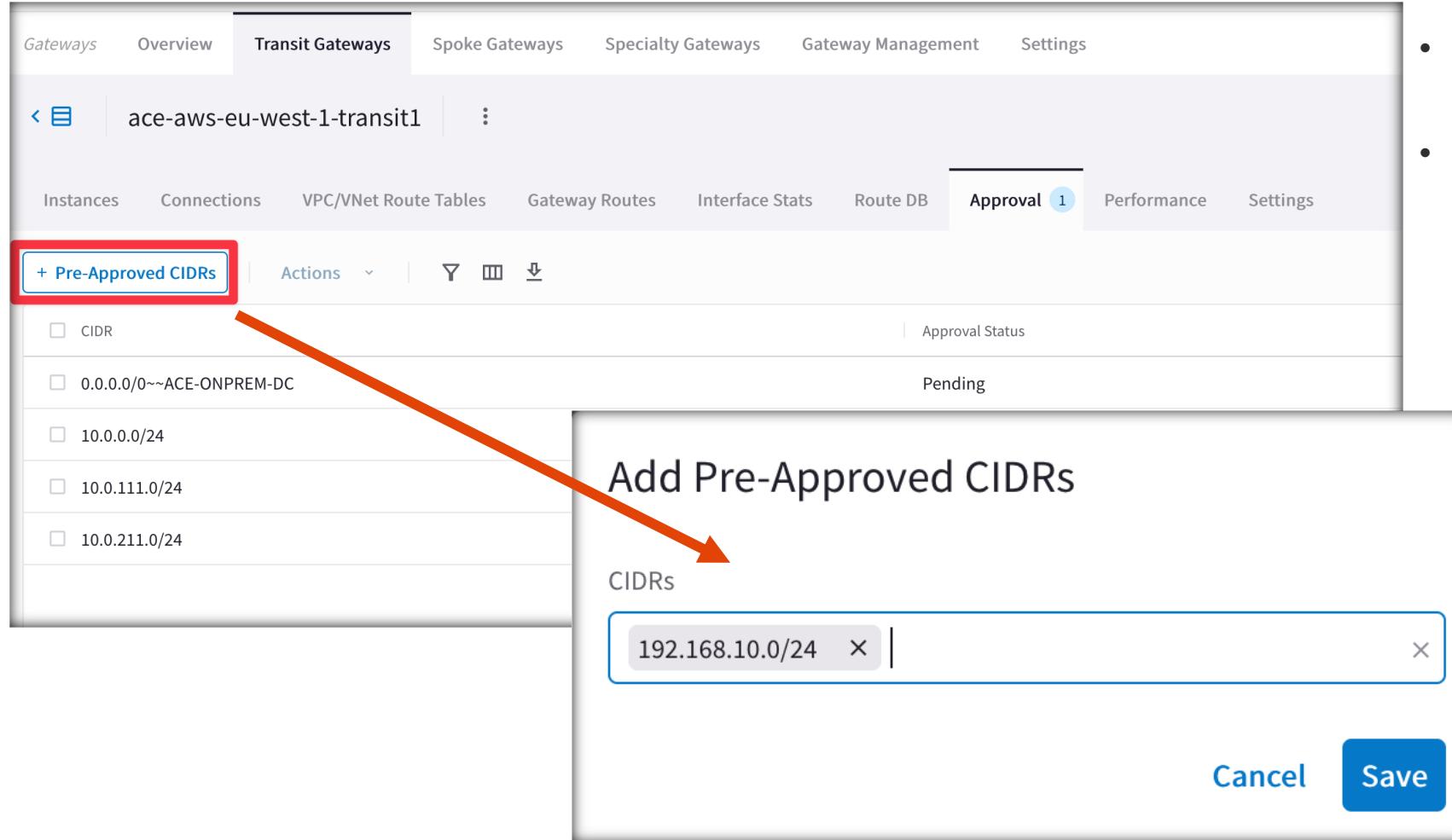


The 'Tables' tab displays a list of pre-approved CIDRs. Each row includes a checkbox, the CIDR range, its current approval status, and buttons for 'Approve' and 'Remove'.

| CIDR | Approval Status | Action |
|-------------------------|-----------------|----------------|
| 0.0.0.0/0~ACE-ONPREM-DC | Pending | Approve Remove |
| 10.0.0.0/24 | Approved | Approve Remove |
| 10.0.111.0/24 | Approved | Approve Remove |
| 10.0.211.0/24 | Approved | Approve Remove |

BGP Route Approval – Config – Pre-Approved CIDRs

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



The screenshot shows the Aviatrix CoPilot interface for managing gateways. The top navigation bar includes tabs for Gateways, Overview, Transit Gateways (selected), Spoke Gateways, Specialty Gateways, Gateway Management, and Settings. Below the navigation is a breadcrumb path: 'ace-aws-eu-west-1-transit1'. The main content area has tabs for Instances, Connections, VPC/VNet Route Tables, Gateway Routes, Interface Stats, Route DB, Approval (with a notification count of 1), Performance, and Settings. The Approval tab is active. On the left, there's a sidebar with a '+ Pre-Approved CIDRs' button, which is highlighted with a red box. A large red arrow points from this button to a modal dialog titled 'Add Pre-Approved CIDRs'. The modal contains a text input field labeled 'CIDRs' containing the value '192.168.10.0/24'. At the bottom of the modal are 'Cancel' and 'Save' buttons.

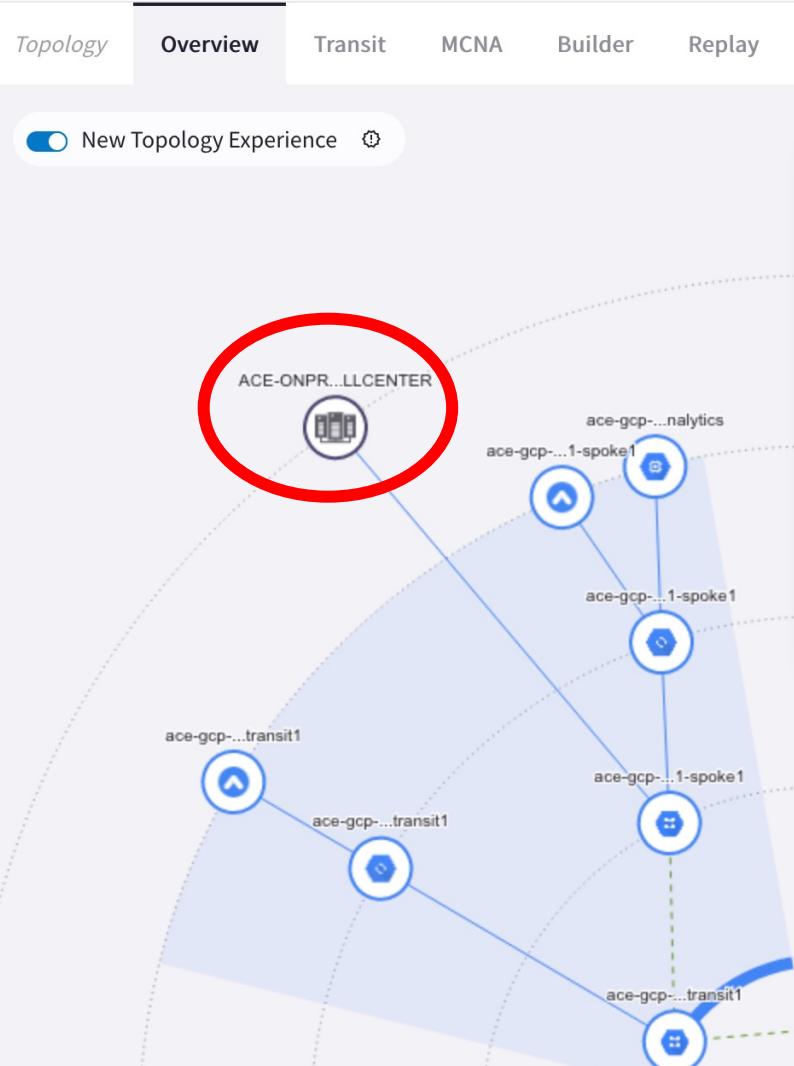
- This feature allows to pre-approving CIDRs advertised by external networks.
- The CIDRs will be propagated without the administrator logs into the CoPilot



Site2Cloud & CoPilot

Site2Cloud Visibility via CoPilot

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



Cloud Routes

- [Cloud Routes](#)
- [Gateway Routes](#)
- [VPC/VNet Routes](#)
- Site 2 Cloud**
- [BGP Info](#)

Last Updated: April 3rd 2023, 12:10:01 pm

| S2C Name | VPC/VNet ID | BGP STATUS | HA STATUS | S2C STATUS | TUNNEL STATUS |
|-----------------------|--|------------|-----------|------------|---------------|
| ACE-ONPREM-CALLCENTER | ace-gcp-us-east1-spoke1~~aviatrix-lab2 | disabled | disabled | | |
| ACE-ONPREM-DC | vpc-0166f973c61ae76dc | enabled | disabled | | |

Tunnels

| status | tunnel_status | gw_name | ip_addr | modified | name | peer_ip | tunnel_protocol | cert_based_s2c_local_id |
|--------|---------------|----------------------------|----------------|-----------------------------|-----------------------------------|----------------|-----------------|-------------------------|
| Active | | ace-aws-eu-west-1-transit1 | 52.210.148.241 | 2023-03-27T18:34:00.646541Z | tunnel-ace-aws-eu-west-1-transit1 | 18.133.182.174 | IPsec | |

[Cloud Routes](#)

[Gateway Routes](#)

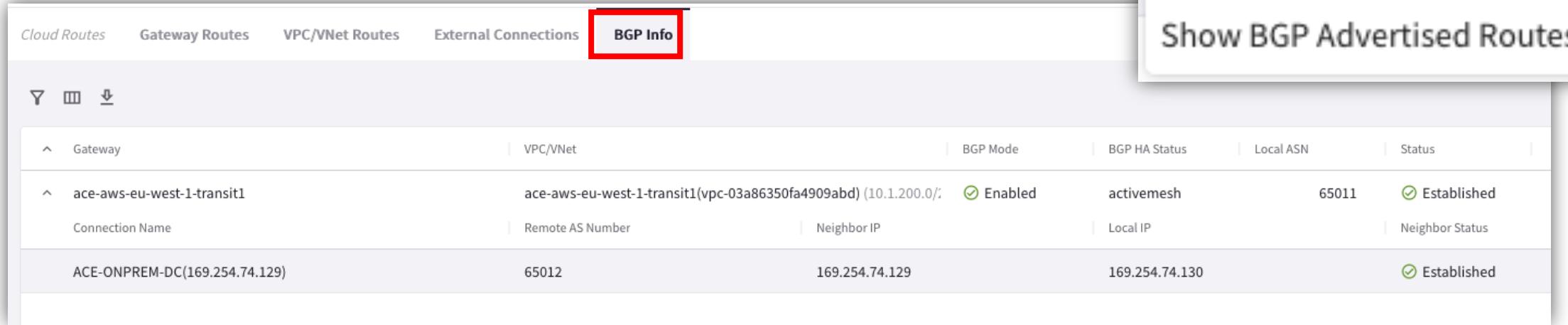
[VPC/VNet Routes](#)

External Connections

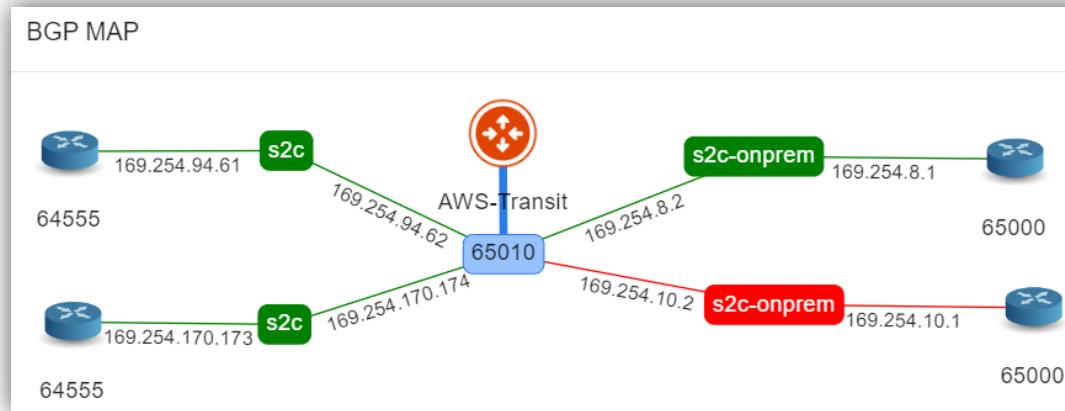
[BGP Info](#)

Site2Cloud BGP via CoPilot

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



| Cloud Routes | Gateway Routes | VPC/VNet Routes | External Connections | BGP Info |
|-------------------------------|--|-----------------|----------------------|----------------|
| Gateway | VPC/VNet | | | |
| ace-aws-eu-west-1-transit1 | ace-aws-eu-west-1-transit1(vpc-03a86350fa4909abd) (10.1.200.0/ | | | Enabled |
| Connection Name | Remote AS Number | | Neighbor IP | Local IP |
| ACE-ONPREM-DC(169.254.74.129) | 65012 | | 169.254.74.129 | 169.254.74.130 |
| | | | | Established |



LEARNED CIDR

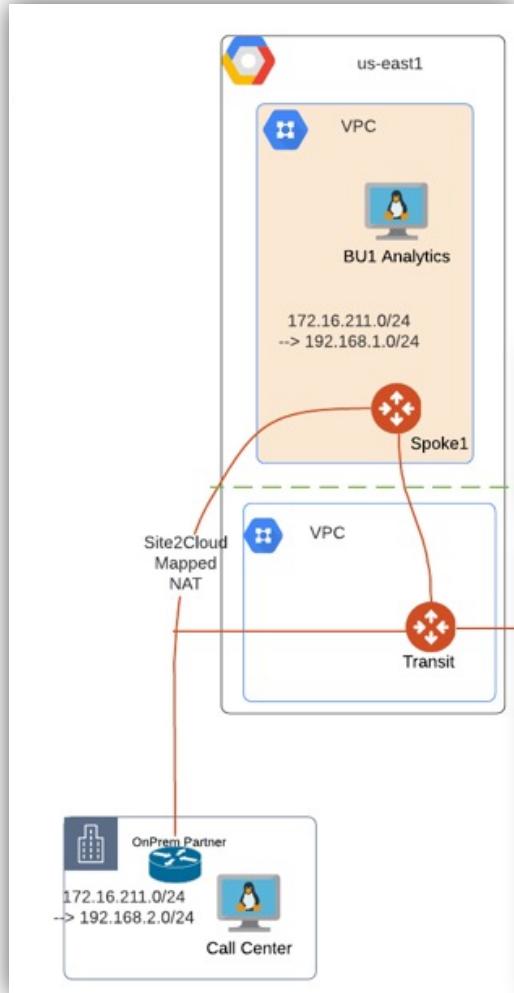
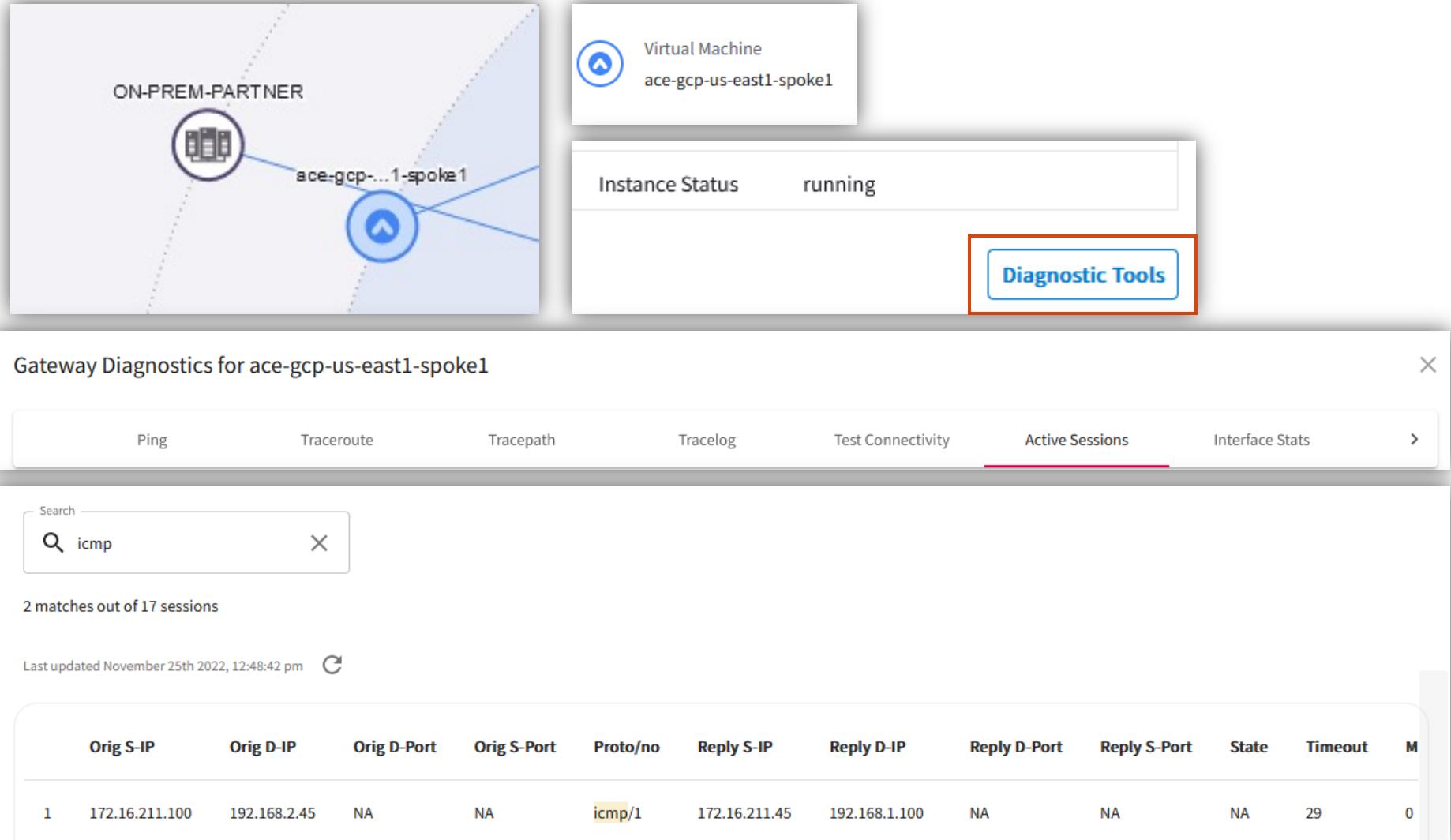
| Search |
|---------------|
| Networks 5 |
| 10.230.0.0/16 |
| 10.240.0.0/24 |

ADVERTISED CIDR

| Search |
|--------------|
| Networks 7 |
| 10.9.0.0/20 |
| 10.63.0.0/16 |
| 10.3.0.0/16 |

Site2Cloud Sessions via CoPilot

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

The screenshot shows the "Gateway Diagnostics" interface for the gateway "ace-gcp-us-east1-spoke1". The interface includes a map view with nodes "ON-PREM-PARTNER" and "ace-gcp-us-east1-spoke1" connected by a line. To the right, a card displays the "Virtual Machine" details: "ace-gcp-us-east1-spoke1" with "Instance Status" set to "running". A red box highlights the "Diagnostic Tools" button.

Gateway Diagnostics for ace-gcp-us-east1-spoke1

Ping Traceroute Tracepath Tracelog Test Connectivity Active Sessions Interface Stats

Search: icmp

2 matches out of 17 sessions

Last updated November 25th 2022, 12:48:42 pm

| Orig S-IP | Orig D-IP | Orig D-Port | Orig S-Port | Proto/no | Reply S-IP | Reply D-IP | Reply D-Port | Reply S-Port | State | Timeout | M |
|------------------|--------------|-------------|-------------|----------|---------------|---------------|--------------|--------------|-------|---------|---|
| 1 172.16.211.100 | 192.168.2.45 | NA | NA | icmp/1 | 172.16.211.45 | 192.168.1.100 | NA | NA | NA | 29 | 0 |



Next: Lab 6 Site2Cloud