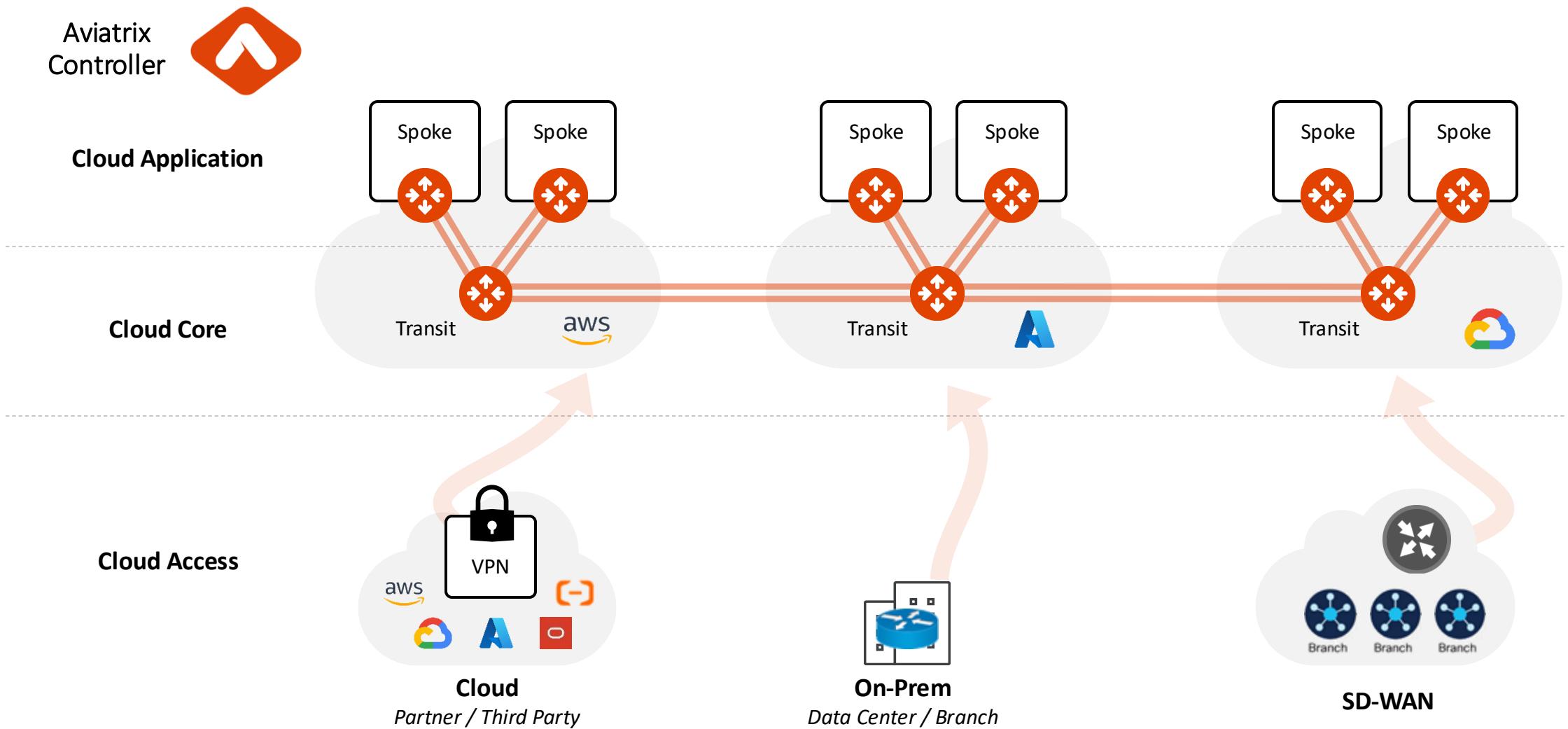




Site2Cloud

ACE Team

Aviatrix Multicloud Network Architecture

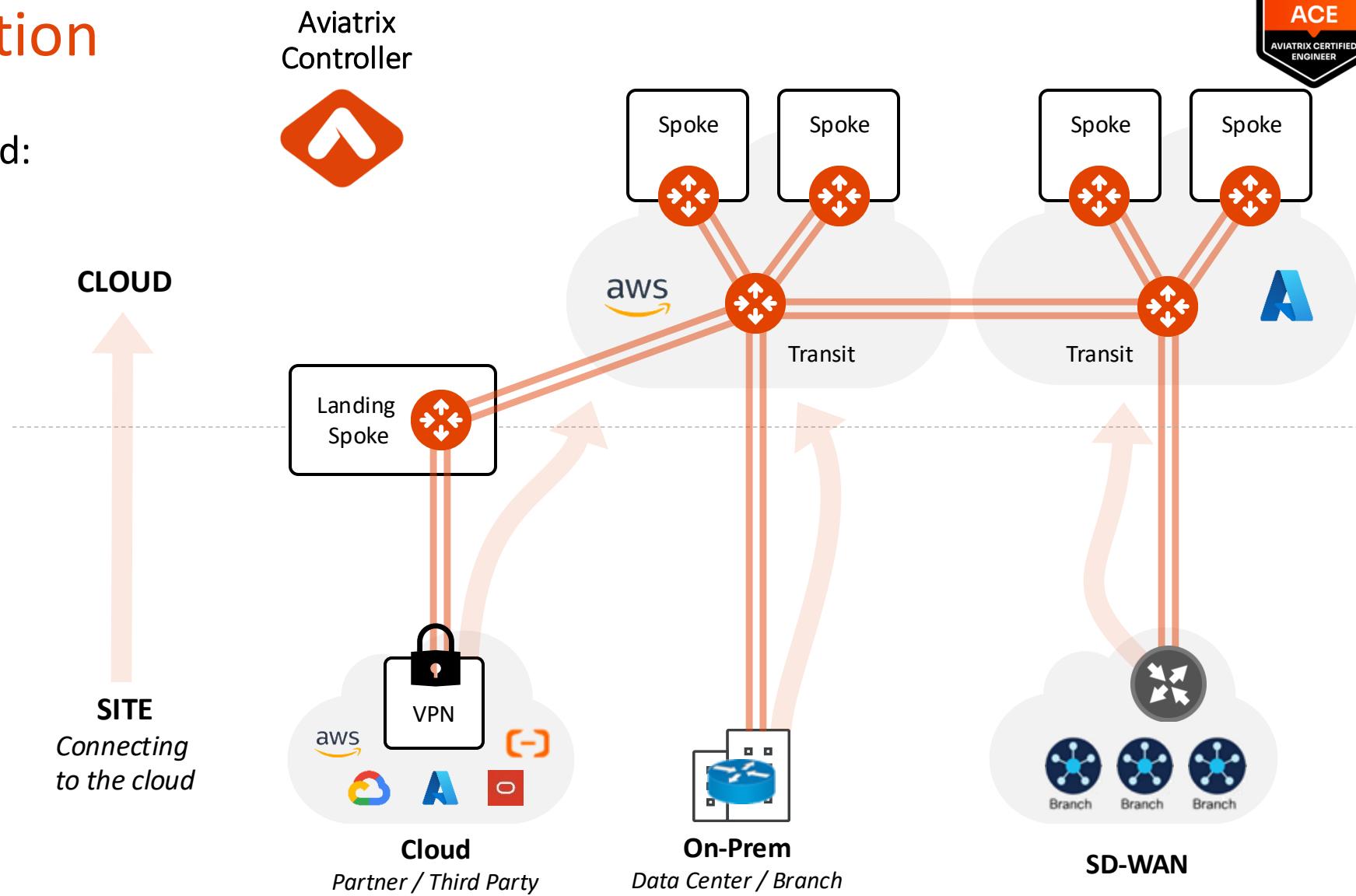


Site2Cloud Introduction



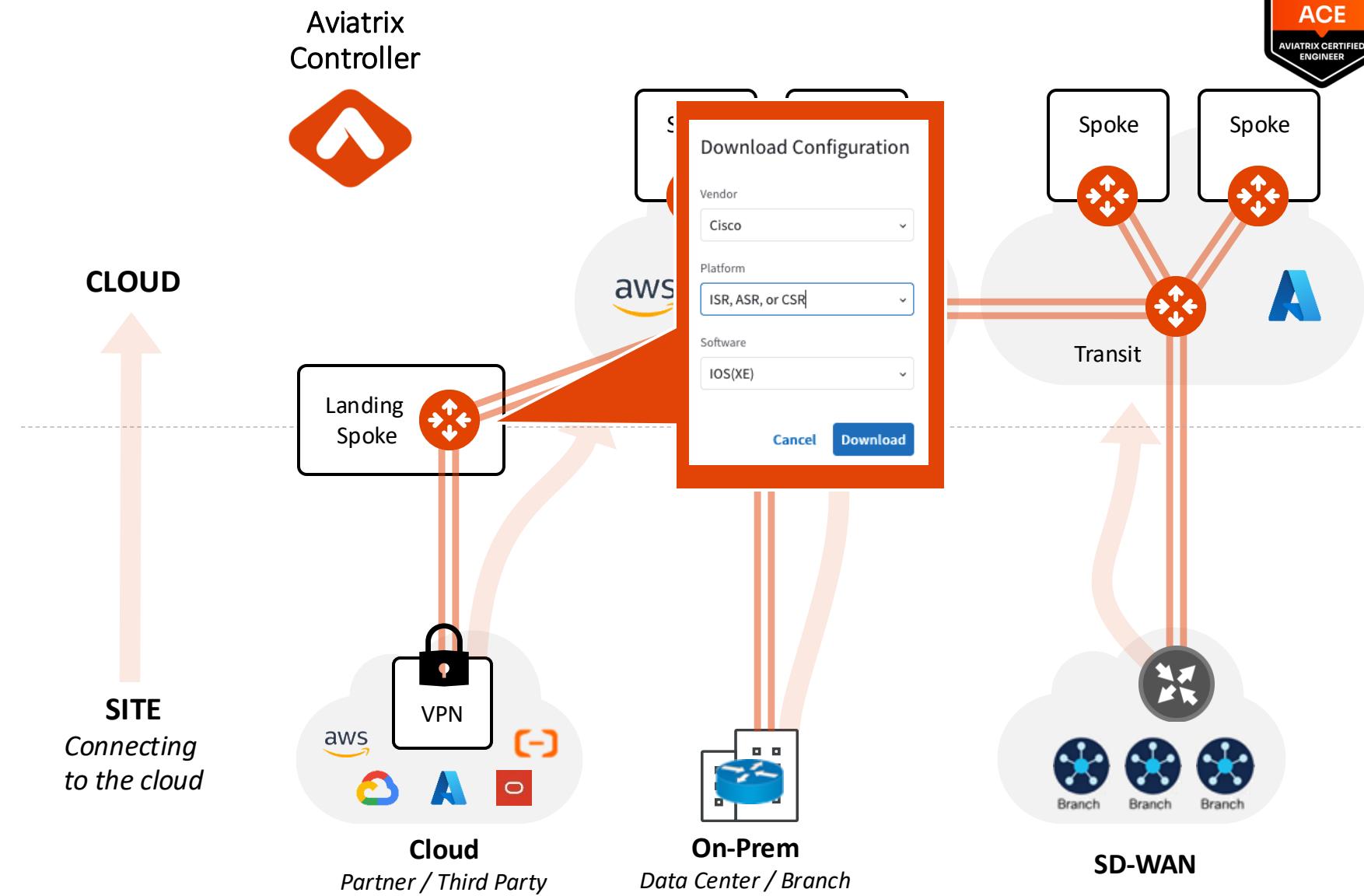
IPsec connection to Public Cloud:

- 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



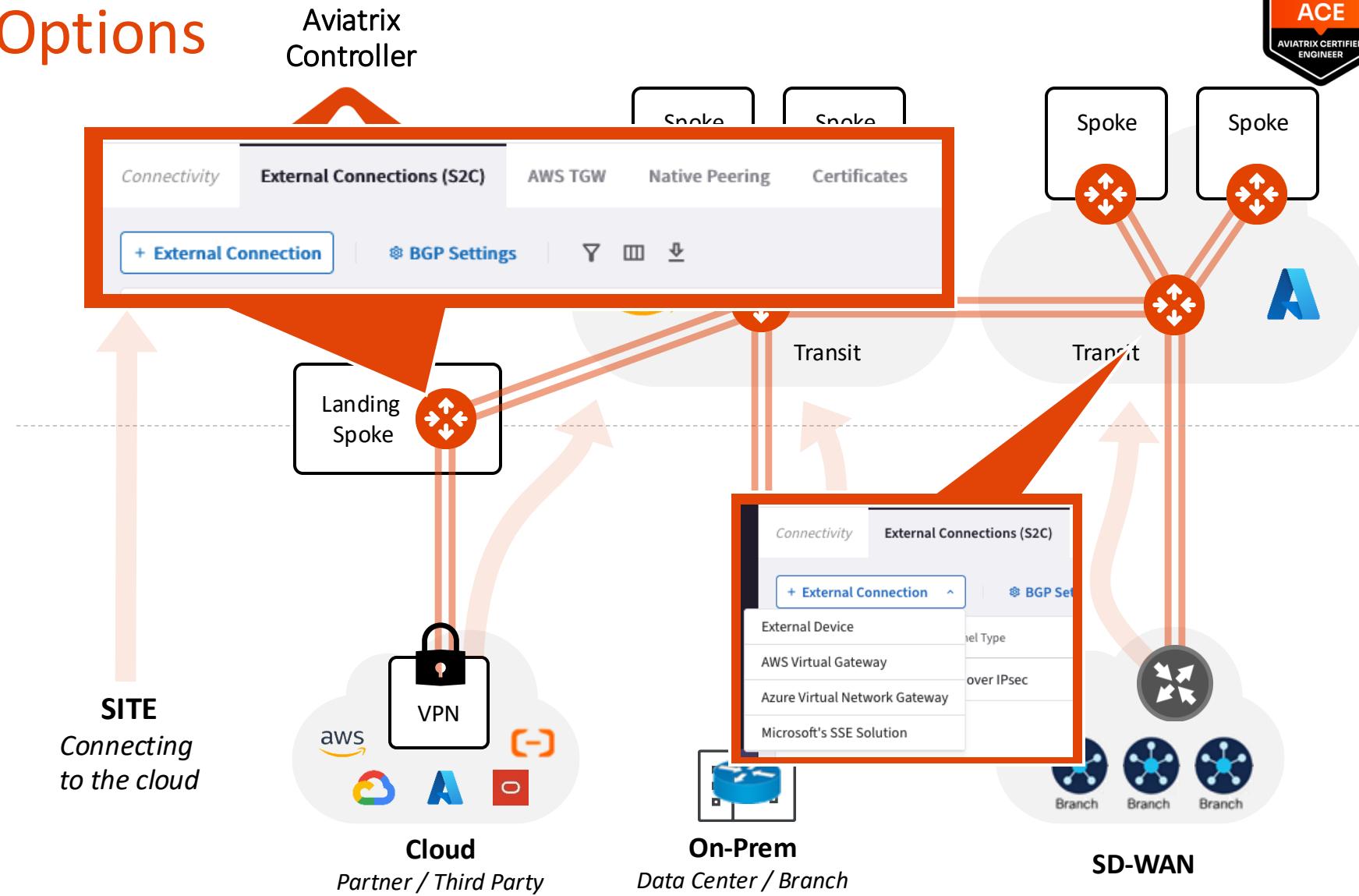
Site2Cloud Landing Options

- **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



Create External Connection to External Device

Name: S2C-PARTNER

Connect Using: BGP Static-Route Based Static-Policy Based

Type: Mapped

Custom Mapped: Off

Connect overlapping networks between the cloud and on-premises from a Transit, Spoke, or Specialty Gateway.

Local Gateway: ace-gcp-us-east1-spoke1 | Real Local Subnet CIDR(s): 172.16.211.0/24 | Virtual Local Subnet CIDR(s): 192.168.1.0/24

Remote Gateway Type: Generic | Real Remote Subnet CIDR(s): 172.16.211.0/24 | Virtual Remote Subnet CIDR(s): 192.168.2.0/24

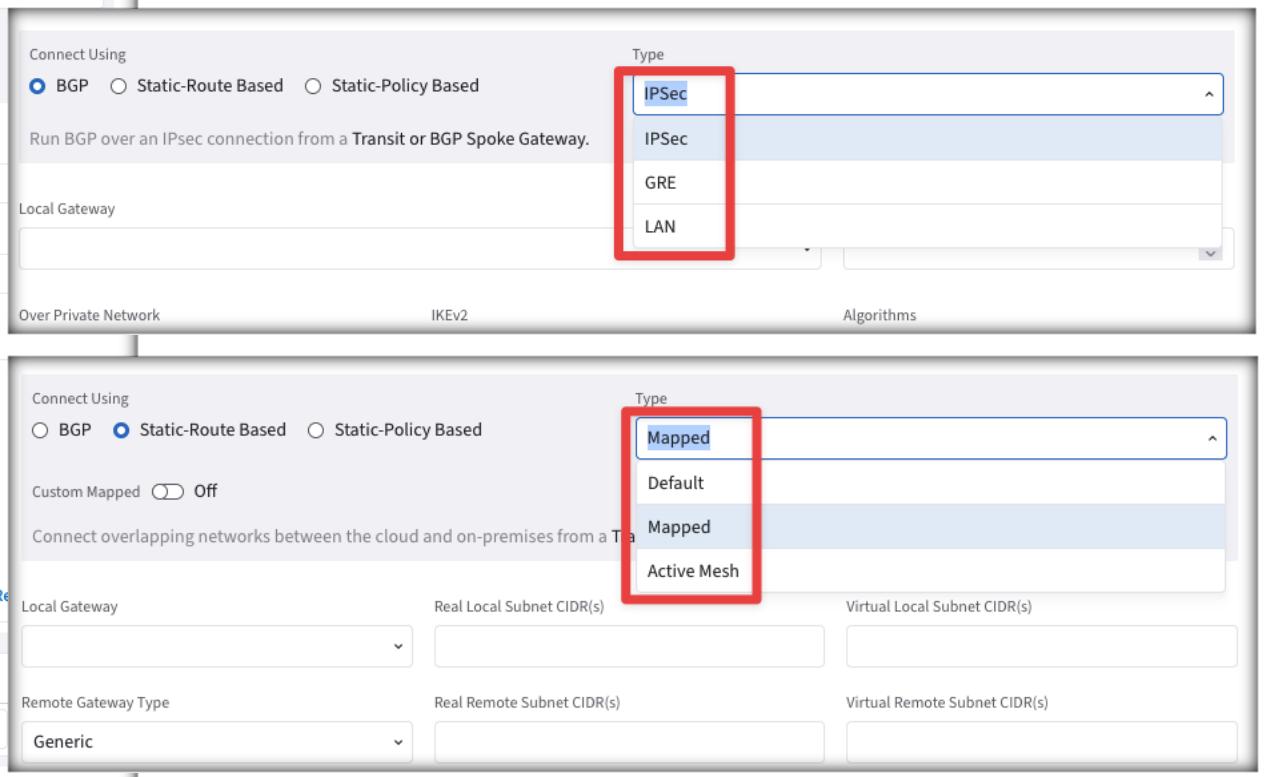
Advanced Settings

Authentication Method: PSK Certificate

Over Private Network: Off | IKEv2: On | Algorithms: Default

Tunnel Configuration

| Remote Gateway IP | Local Gateway Instance | Local Tunnel IP | Remote Tunnel IP | Pre-Shared Key |
|-------------------|------------------------|-----------------|------------------|----------------|
| 18.130.247.103 | ace-gcp-us-e ... | 169.254.0.1/30 | 169.254.0.1/30 | ***** |



BGP over IPsec: The 'Type' dropdown is set to 'IPSec' (highlighted with a red box). Other options shown are 'GRE' and 'LAN'.

Static Route-Based Mapped: The 'Type' dropdown is set to 'Mapped' (highlighted with a red box). Other options shown are 'Default', 'Mapped', and 'Active Mesh'.

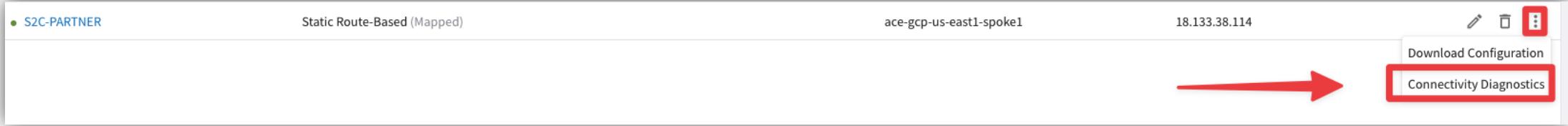
Active Mesh: The 'Type' dropdown is set to 'Active Mesh' (highlighted with a red box).

Buttons at the bottom: Cancel, Save

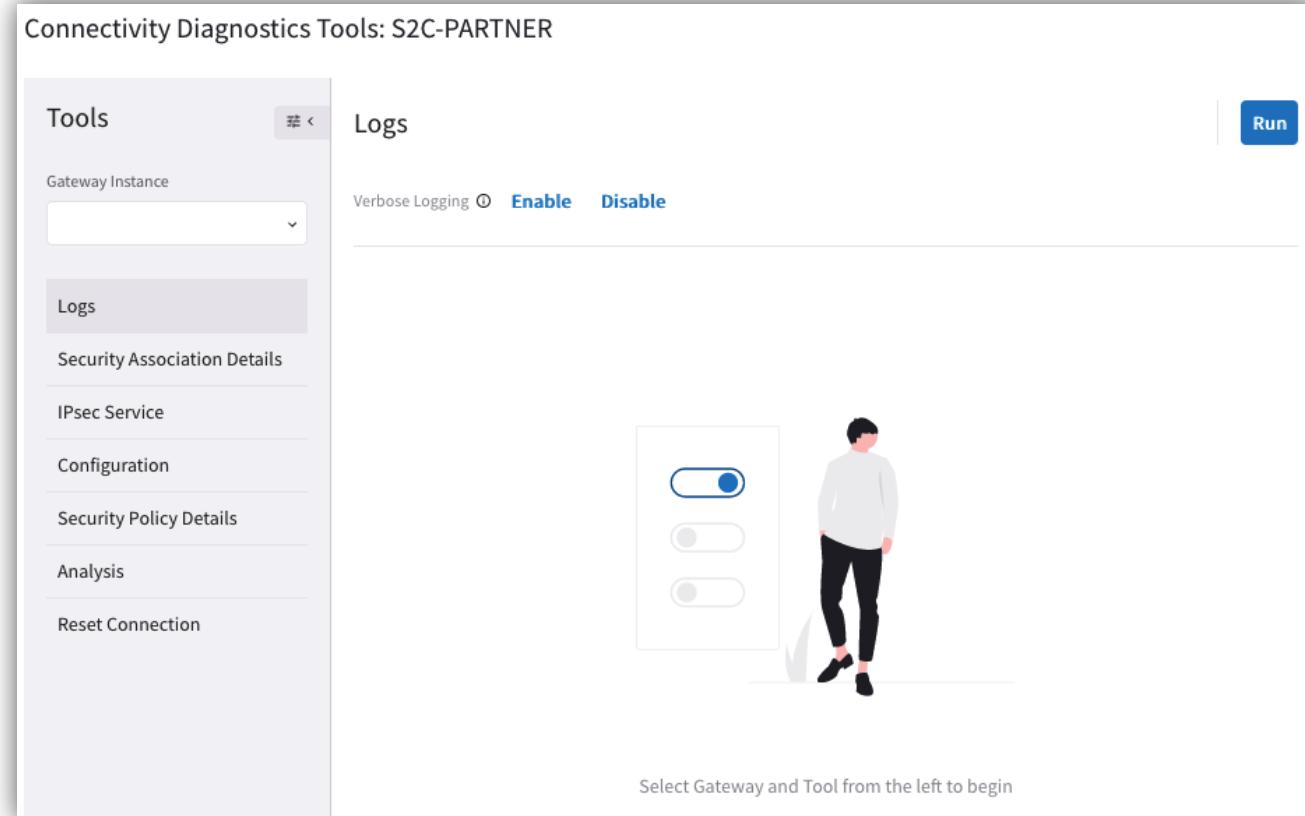


Monitoring & Troubleshooting Site2Cloud

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



The screenshot shows the 'Connectivity Diagnostics Tools' interface for 'S2C-PARTNER'. On the left, a sidebar titled 'Tools' lists options: Gateway Instance (dropdown), Logs (selected), Security Association Details, IPsec Service, Configuration, Security Policy Details, Analysis, and Reset Connection. To the right, the 'Logs' section is displayed with a heading 'Logs'. It includes a 'Verbose Logging' toggle switch set to 'Enable' (blue), and buttons for 'Run' and 'Disable'. Below the logs, there's a small illustration of a person standing next to a large switch-like interface with three toggle switches, one of which is blue. At the bottom, the text 'Select Gateway and Tool from the left to begin' is visible.

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

Last Run: Jan 30, 2024 11:52 PM | Run

Tools

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

Security Association Details

| Local IP | Local Port | Remote IP | Remote Port | Protocol | SPI | Encryption | Hash | Diff |
|--------------|------------|---------------|-------------|----------|------------|------------|-------------|-------------------------------------|
| 172.16.211.2 | 4500 | 34.139.73.146 | 4500 | esp-udp | 978561465 | aes-cbc | hmac-sha256 | 1581(s) hard: 3960(s) soft: 3454(s) |
| 172.16.211.2 | 4500 | 34.139.73.146 | 4500 | esp-udp | 3249923436 | aes-cbc | hmac-sha256 | 1581(s) hard: 3960(s) soft: 3253(s) |

Details for SPI 978561465:

```
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 2cd6fb1be 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 e122cc7d 4668d2c 9361341c 2d698735 60778402 6dbc2d0 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

Monitoring – ‘Current’ number is increasing



Aviatrix CoPilot outcome – First Time

Aviatrix CoPilot outcome – Second Time

Connectivity Diagnostics Tools: s2c-partner

- Tools
- Gateway Instance
- Logs
- Security Association Details**
- IPsec Service
- Configuration
- Security Policy Details
- Analysis
- Reset Connection

Security Association Details

Last Run: Jan 31, 2024 12:02 AM

Run

```
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 2cd6f5be 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 23:02:58 2024
    diff: 2185(s) hard: 3960(s) soft: 3454(s)
    last: Jan 30 22:33:03 2024 hard: 0(s) soft: 0(s)
    current: 1008(bytes) hard: 0(bytes) soft: 0(bytes)
    allocated: 12 hard: 0 soft: 0
    sadb_seq=3 pid=5199 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 e122cc7 f4668d2c 9361341c 2d698735 60778402 6dbcb2d0 4c2e0ffd
    A: hmac-sha256 c9536926 532f504e 5fdcc950 d1594047 2687cecb d9e74556 e798354f
```

Connectivity Diagnostics Tools: s2c-partner

- Tools
- Gateway Instance
- Logs
- Security Association Details**
- IPsec Service
- Configuration
- Security Policy Details
- Analysis
- Reset Connection

Security Association Details

Last Run: Jan 31, 2024 12:04 AM

Run

```
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 2cd6f5be 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 23:04:49 2024
    diff: 2296(s) hard: 3960(s) soft: 3454(s)
    last: Jan 30 22:33:03 2024 hard: 0(s) soft: 0(s)
    current: 1428(bytes) hard: 0(bytes) soft: 0(bytes)
    allocated: 17 hard: 0 soft: 0
    sadb_seq=3 pid=5464 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 e122cc7 f4668d2c 9361341c 2d698735 60778402 6dbcb2d0 4c2e0ffd
    A: hmac-sha256 c9536926 532f504e 5fdcc950 d1594047 2687cecb d9e74556 e798354f
```

‘Current’ number is increasing



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 – for ESP)
 - UDP 4500 (NAT- Traversal)
- 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 Analysis Last Run: Nov 3, 2023 3:58 PM Run

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

Logs

Security Association Details

IPsec Service

Configuration

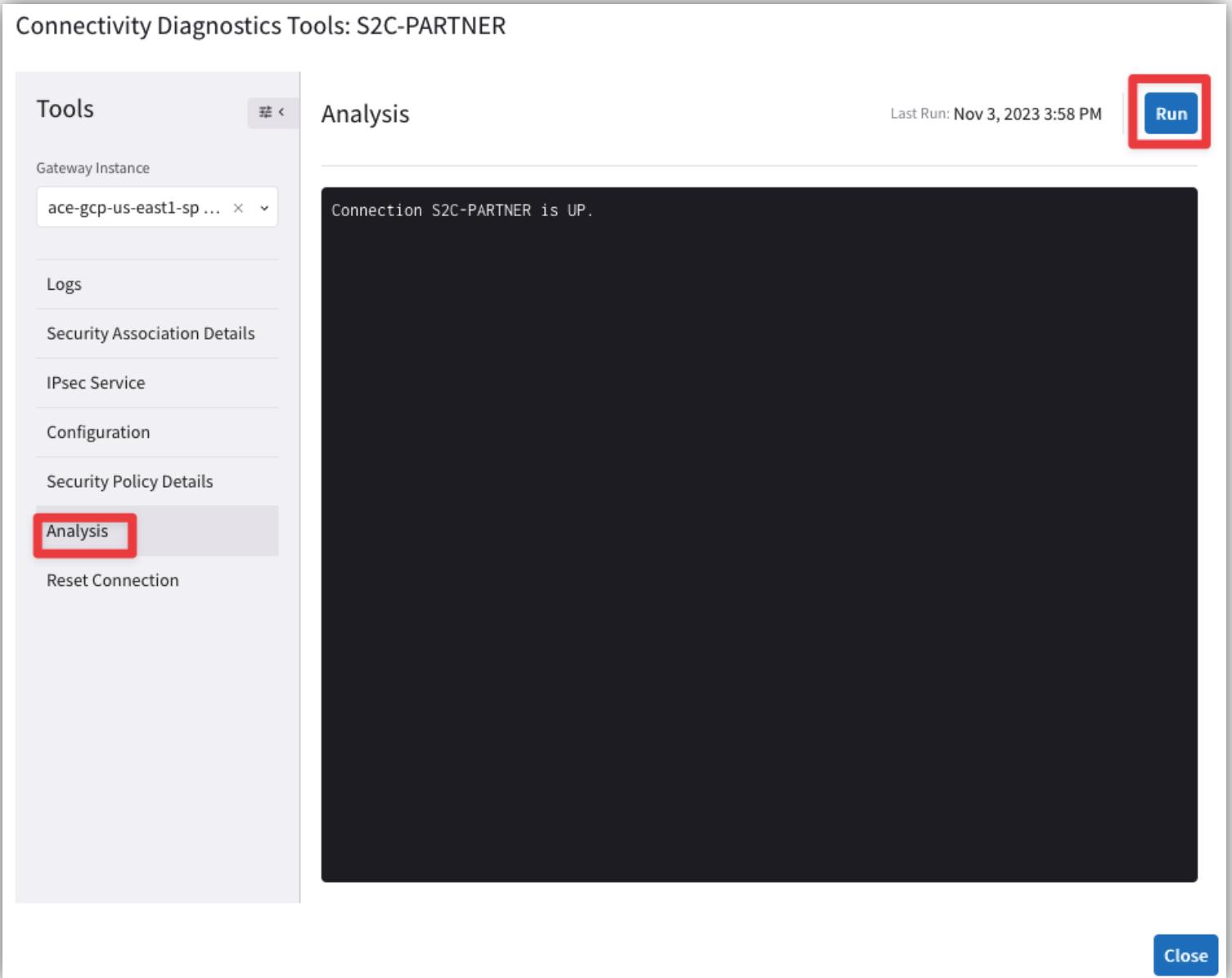
Security Policy Details

Analysis

Reset Connection

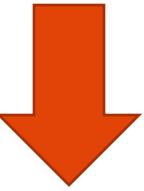
Connection S2C-PARTNER is UP.

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](#)

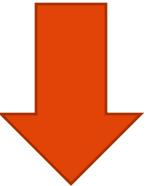
Tunnel analysis for connection s2c-partner:

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**

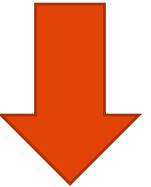
Tunnel analysis for connection s2c-partner:

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"
            ],
        }
    }
}

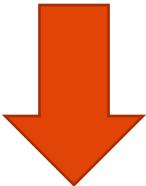
```

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**
- Security Association Details
- IPsec Service
- Configuration
- Security Policy Details
- Analysis
- Reset Connection

Last Run: Nov 3, 2023 3:57 PM

Run

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

```

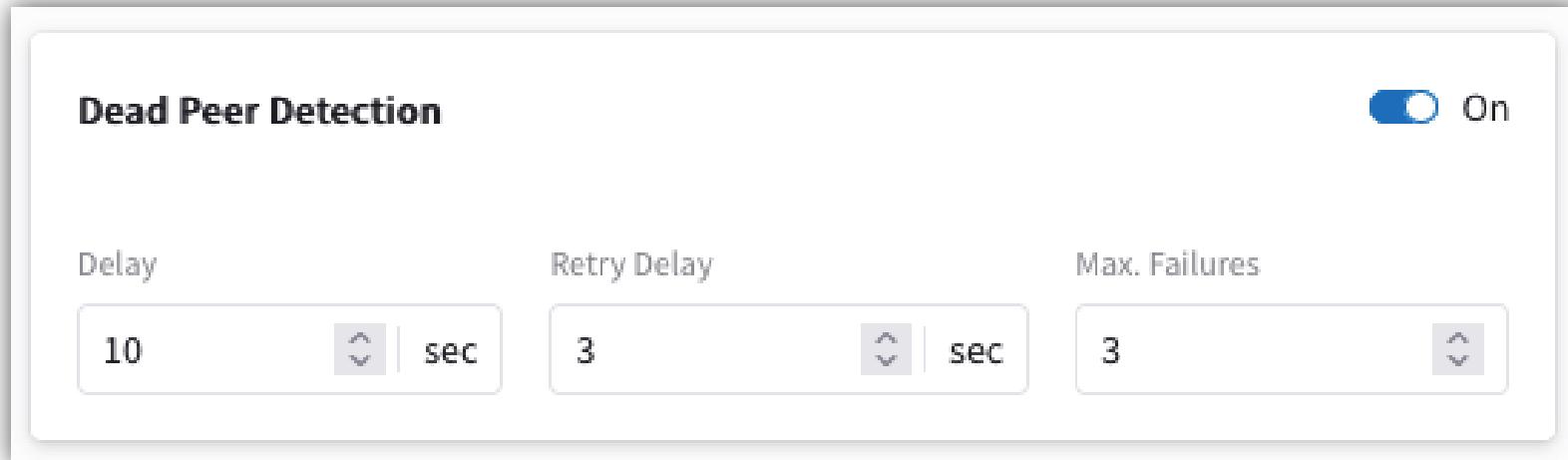
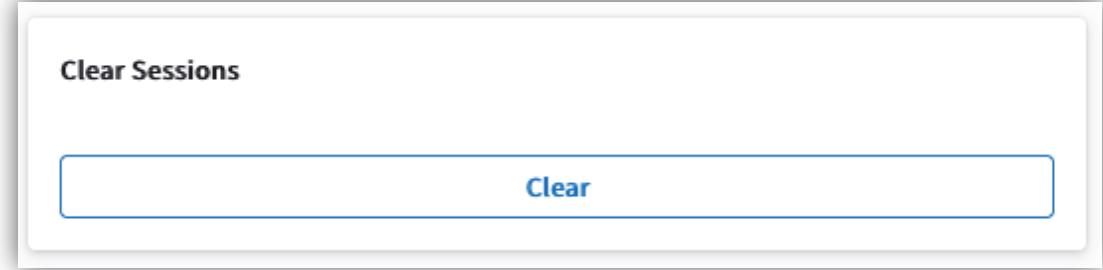
2023-11-03T14:15:58.182653+00:00 GW-ace-gcp-us-east1-spoke1-35.237.68.55 charon: 213[IKE]
<gw-172_16_211_2-18_133_38_114|8> outbound CHILD_SA net-0_0_0_0-0_0_0{54} established
with SPIs cbdd1cf6_i c535c2d4_o and TS 0.0.0.0/0 === 0.0.0.0/0
2023-11-03T14:15:58.181406+00:00 GW-ace-gcp-us-east1-spoke1-35.237.68.55 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

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**

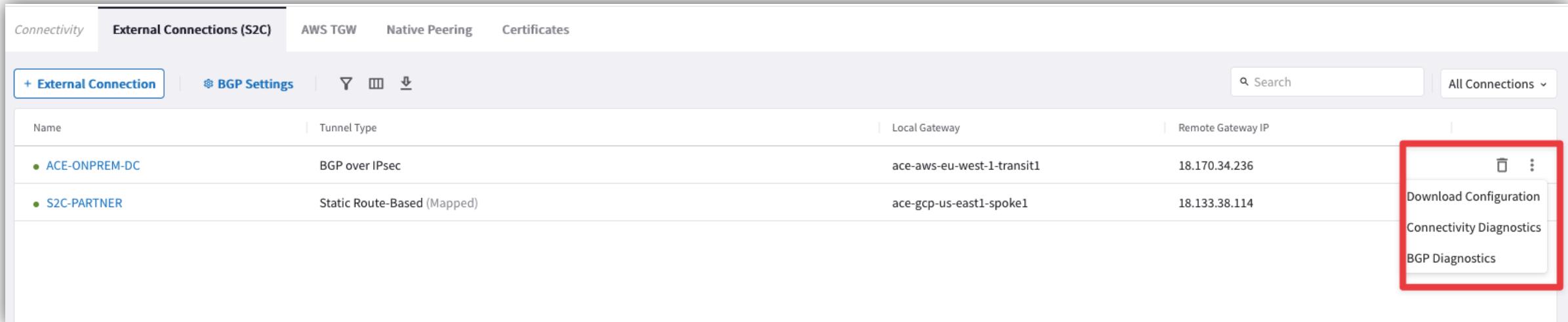


NOTE:

- 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



The screenshot shows the Aviatrix CoPilot interface with the following details:

- Navigation:** Connectivity, External Connections (S2C) (selected), AWS TGW, Native Peering, Certificates.
- Toolbar:** + External Connection, BGP Settings, Filter icons, Search, All Connections.
- Table Headers:** Name, Tunnel Type, Local Gateway, Remote Gateway IP.
- Table Data:**

| 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 |
- Context Menu (highlighted by a red box):**
 - 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

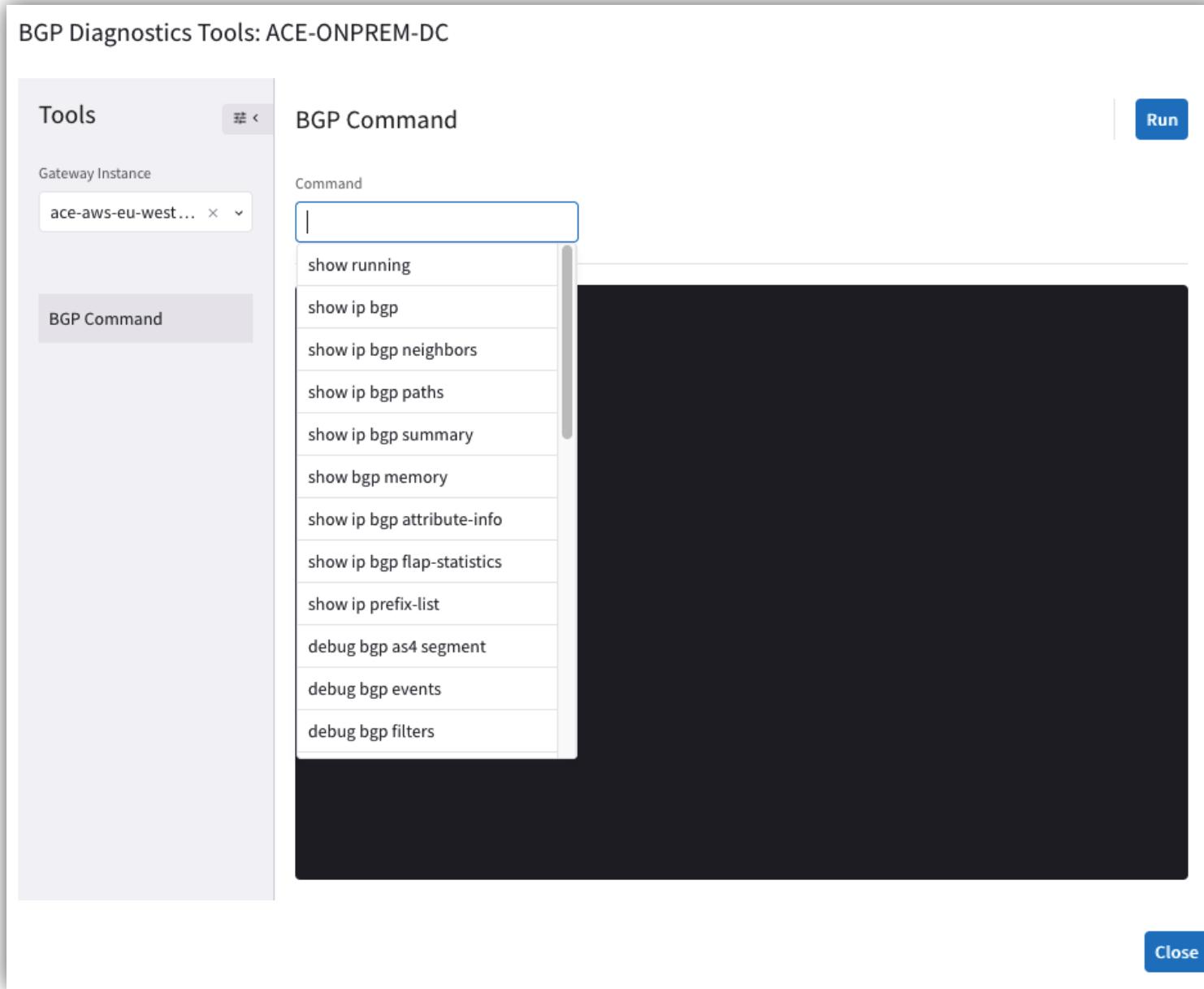
BGP Command

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 ✖

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

BGP Command: show ip bgp ✖

Last Run: Nov 3, 2023 4:16 PM Run

BGP Command

```
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       65012 ?
*> 10.0.111.0/24    169.254.74.129          0       65012 ?
*> 10.0.211.0/24    169.254.74.129          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



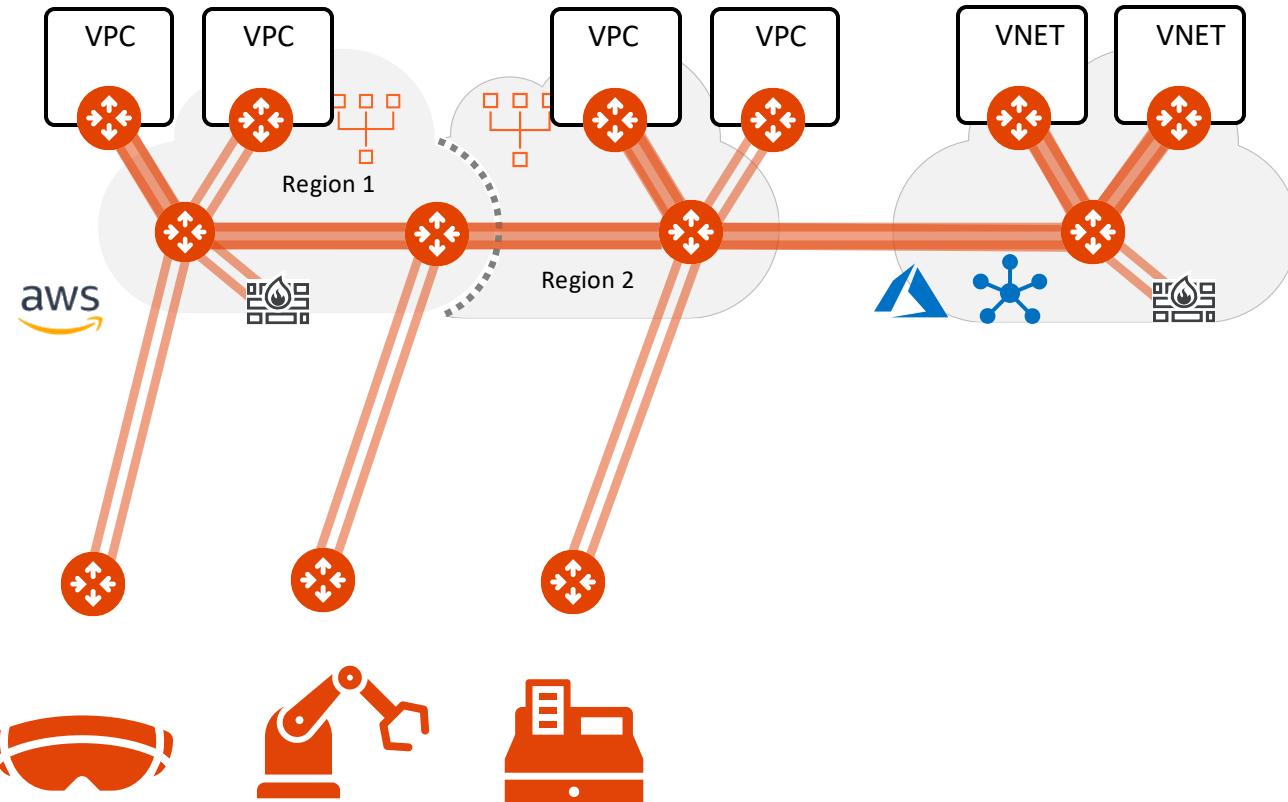
Simplified Edge Management



Consistent Secure Edge

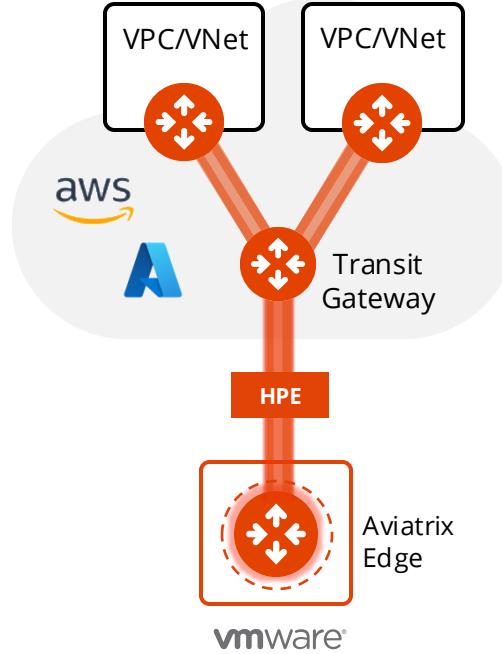


Simplified Edge On-boarding

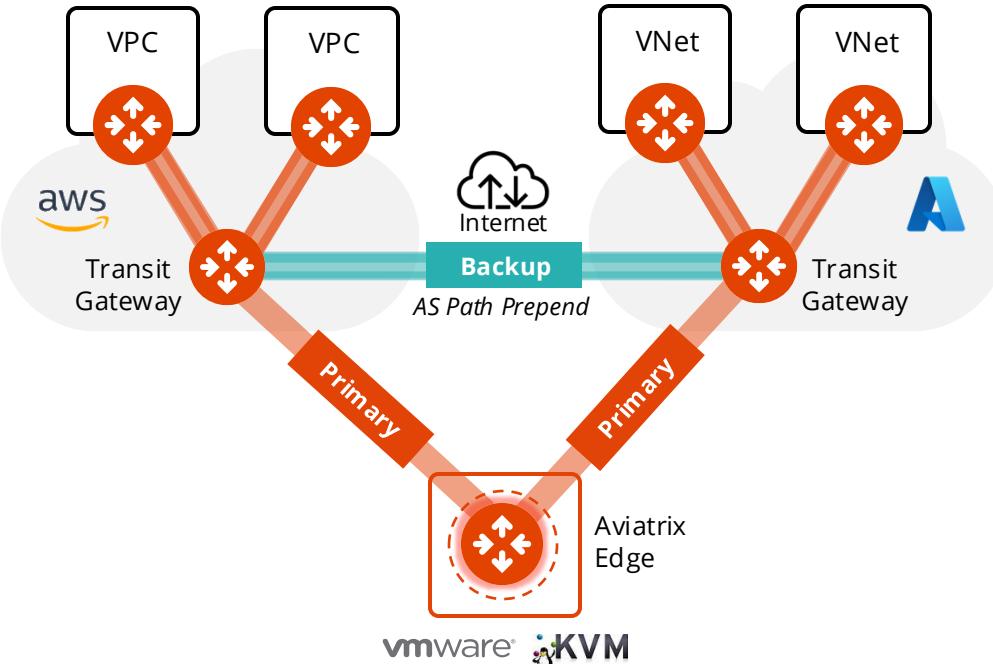


Aviatrix Edge Use Cases

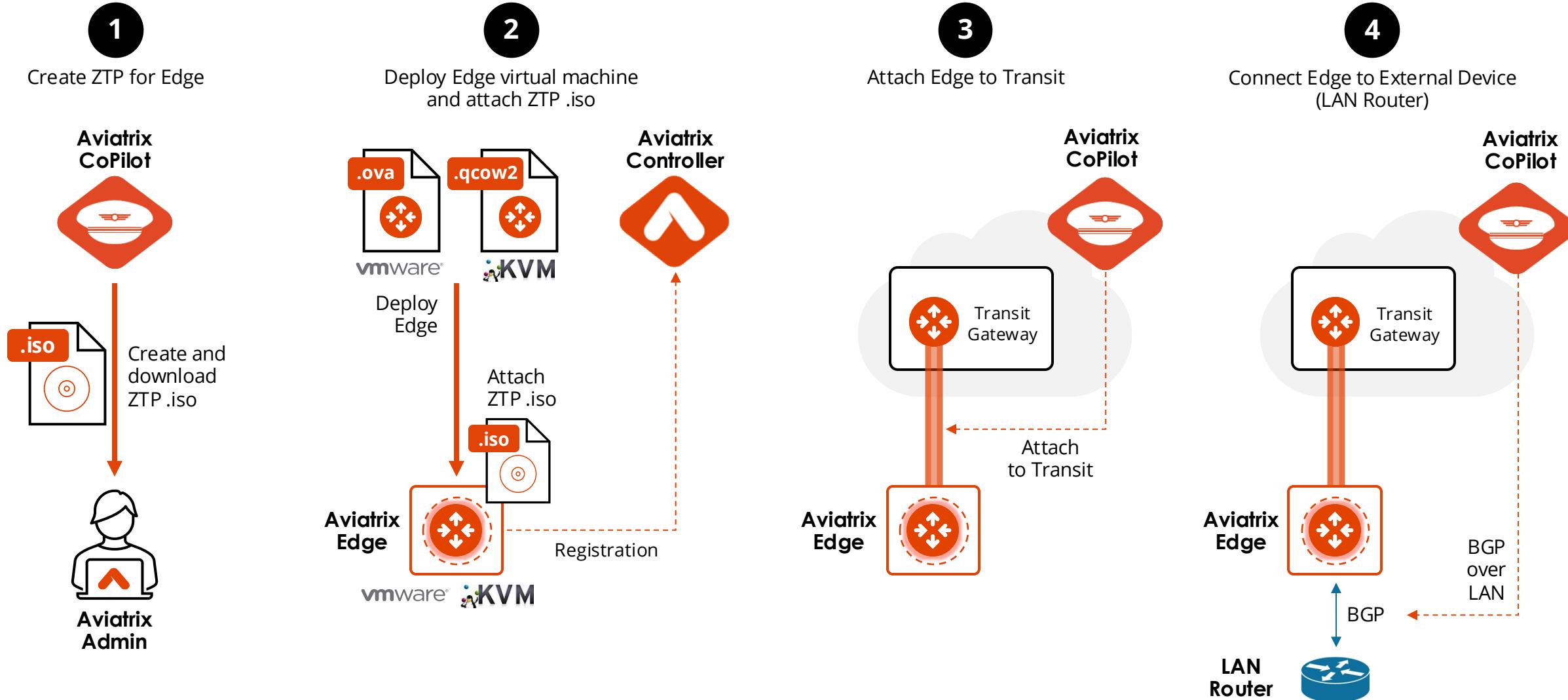
Extend the Aviatrix Platform to the Edge



Multi-Cloud Connectivity via Aviatrix Edge



Edge 2.0 Deployment Workflow - Demo

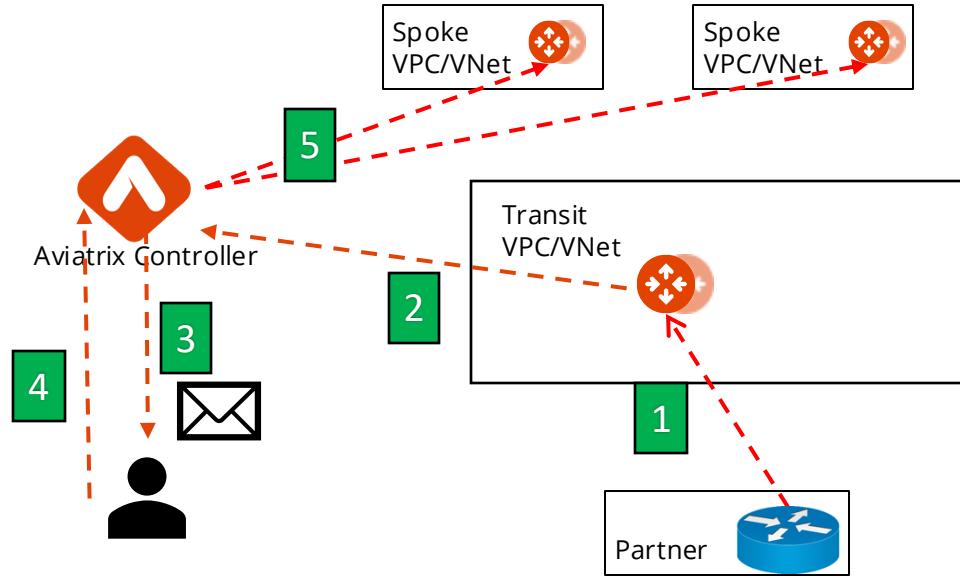




BGP Route Approval

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

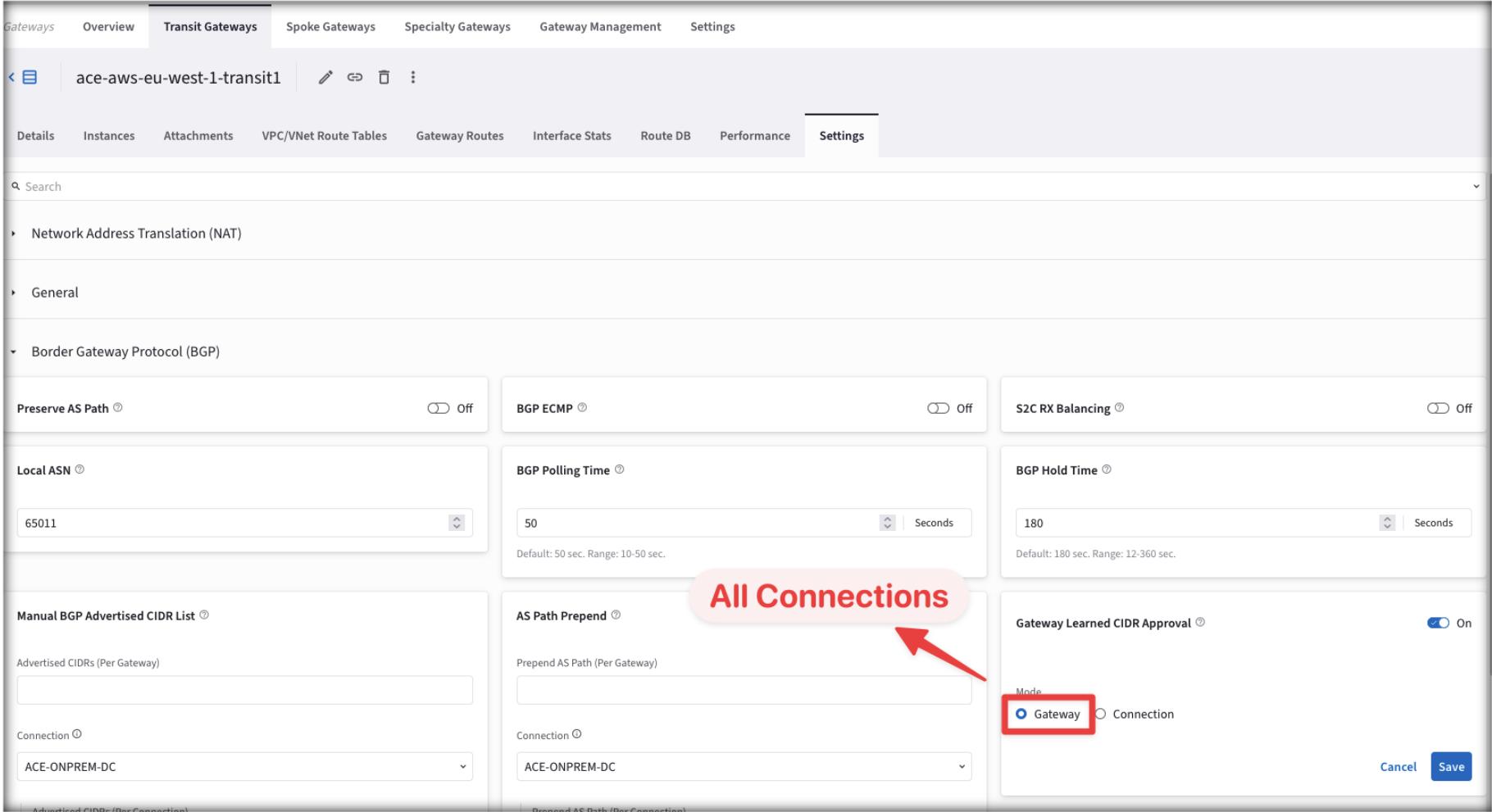
 no-reply@aviatrix.com <no-reply@aviatrix.com>
 To: Umair Hoodbhoy
 Number of Events: 1.

 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 – Activation

- **PATH:** CoPilot > Cloud Fabric > Gateways > select the relevant Gateway > Settings > Border Gateway Protocol (BGP)



The screenshot shows the Aviatrix CoPilot interface for managing gateways. The top navigation bar includes tabs for Gateways, Overview, Transit Gateways (which is selected), Spoke Gateways, Specialty Gateways, Gateway Management, and Settings. Below the navigation is a breadcrumb trail showing the path: ace-aws-eu-west-1-transit1. The main content area has a tab bar with Details, Instances, Attachments, VPC/VNet Route Tables, Gateway Routes, Interface Stats, Route DB, Performance, and Settings (which is selected). A search bar is present above the configuration sections.

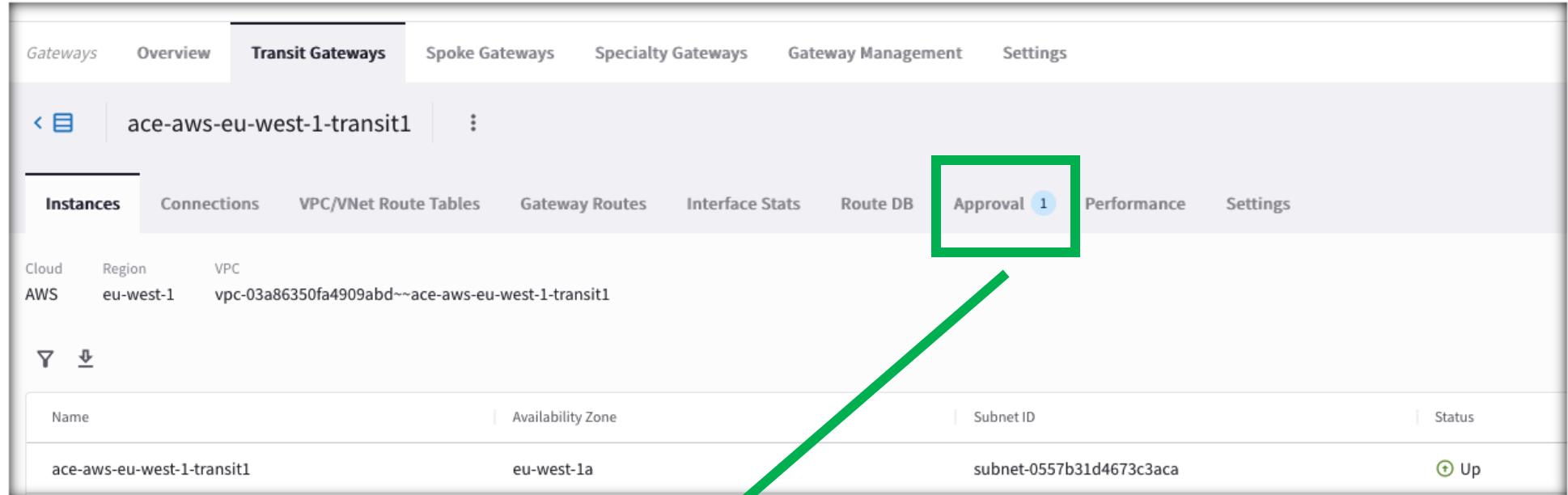
Border Gateway Protocol (BGP) Configuration:

- Preserve AS Path:** Off
- BGP ECMP:** Off
- S2C RX Balancing:** Off
- Local ASN:** 65011
- BGP Polling Time:** 50 Seconds (Default: 50 sec. Range: 10-50 sec.)
- BGP Hold Time:** 180 Seconds (Default: 180 sec. Range: 12-360 sec.)
- Manual BGP Advertised CIDR List:** (Empty field)
- AS Path Prepend:** (Empty field)
- Gateway Learned CIDR Approval:**
 - Mode:** **Gateway** (highlighted with a red box)
 - Connection

A red callout bubble with the text "All Connections" points to the "AS Path Prepend" section. A red arrow points from the "All Connections" callout to the "AS Path Prepend" input field.

BGP Route Approval – Verification

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



Gateways Overview Transit Gateways Spoke Gateways Specialty Gateways Gateway Management Settings

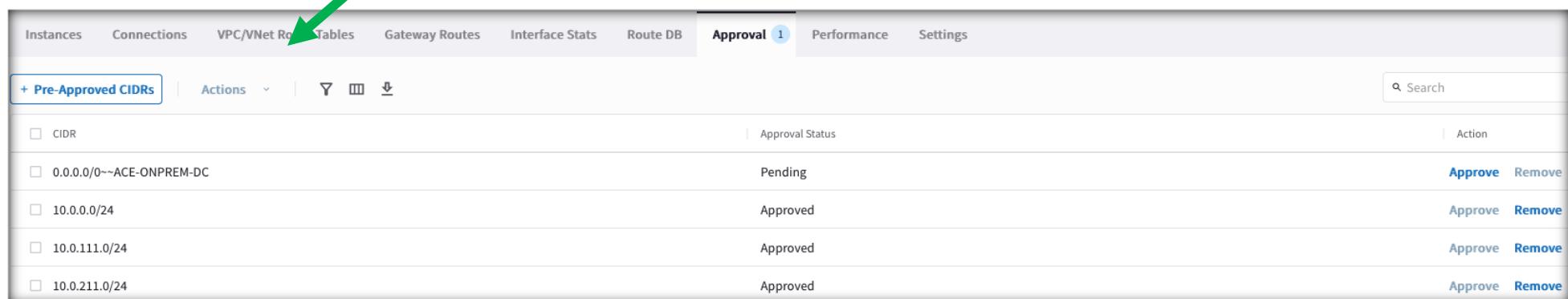
ace-aws-eu-west-1-transit1

Instances Connections VPC/VNet Route Tables Gateway Routes Interface Stats Route DB Approval 1 Performance Settings

Cloud Region VPC
AWS eu-west-1 vpc-03a86350fa4909abd~~ace-aws-eu-west-1-transit1

Name Availability Zone Subnet ID Status

ace-aws-eu-west-1-transit1 eu-west-1a subnet-0557b31d4673c3aca Up



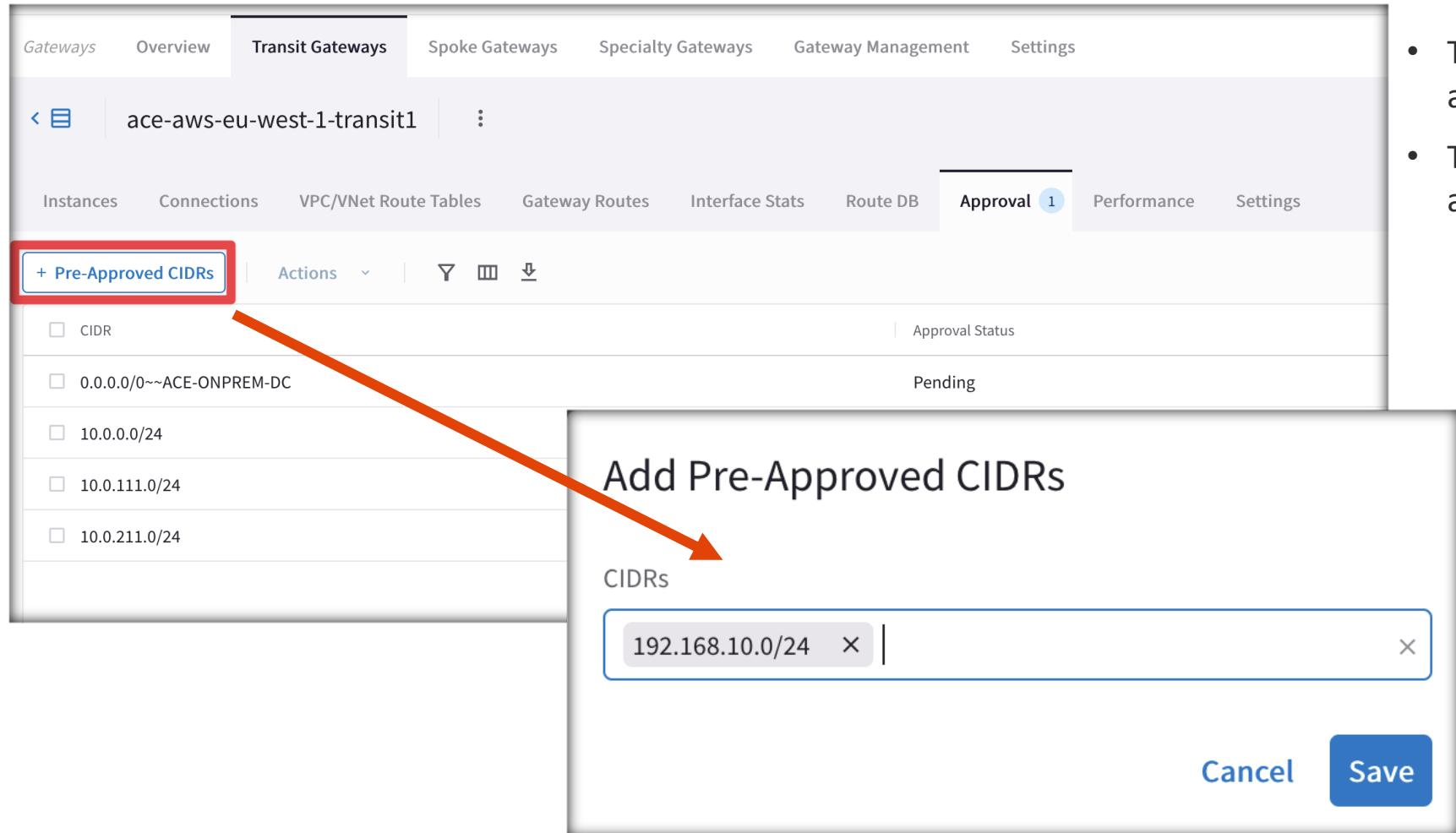
Instances Connections VPC/VNet Route Tables Gateway Routes Interface Stats Route DB Approval 1 Performance Settings

+ Pre-Approved CIDRs Actions

| 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 1 pending item), Performance, and Settings. A prominent red box highlights the 'Approval' tab. On the left, there's a sidebar with a '+ Pre-Approved CIDRs' button, which is also highlighted with a red box and has a red arrow pointing to it from the main interface. The main pane displays a table with columns for CIDR and Approval Status (Pending). The table lists several entries, with the first one being '0.0.0.0/0~ACE-ONPREM-DC'. A modal dialog box is overlaid on the interface, titled 'Add Pre-Approved CIDRs'. It contains a text input field labeled 'CIDRs' containing the value '192.168.10.0/24'. At the bottom of the dialog 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



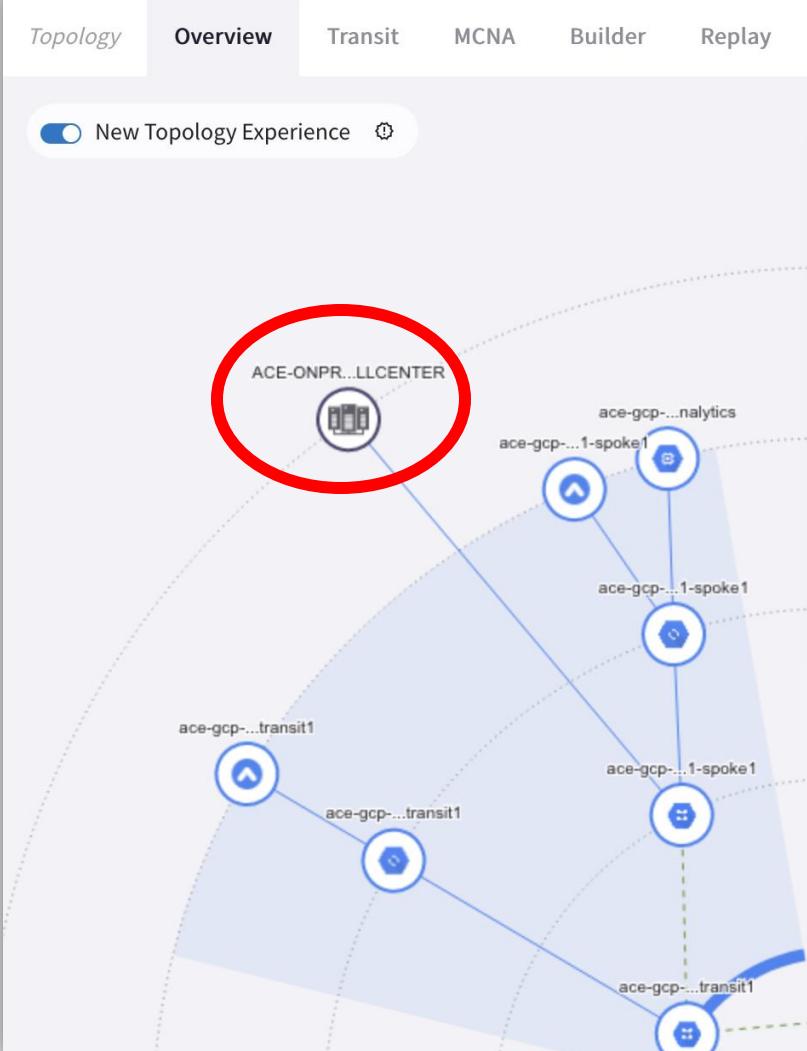
Site2Cloud & CoPilot

Site2Cloud Visibility via CoPilot

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

Topology

New Topology Experience ?



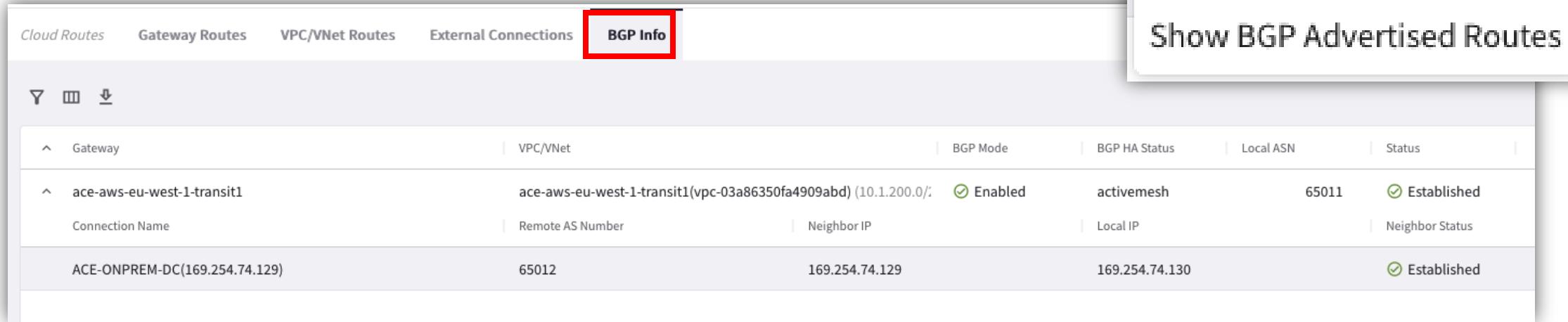
Cloud Routes

| Cloud Routes | Gateway Routes | VPC/VNet Routes | Site 2 Cloud | BGP Info |
|-----------------------|--|----------------------------|---|-----------------------------------|
| Search | | | Last Updated: April 3rd 2023, 12:10:01 pm | |
| S2C Name | VPC/VNet ID | BGP STATUS | HA STATUS | S2C STATUS |
| ACE-ONPREM-CALLCENTER | ace-gcp-us-east1-spoke1~~aviatrix-lab2 | disabled | disabled | Up ✓ |
| ACE-ONPREM-DC | vpc-0166f973c61ae76dc | enabled | disabled | Up ✓ |
| Tunnels | | | | |
| status | tunnel_status | gw_name | ip_addr | modified |
| Active | Up | 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 |

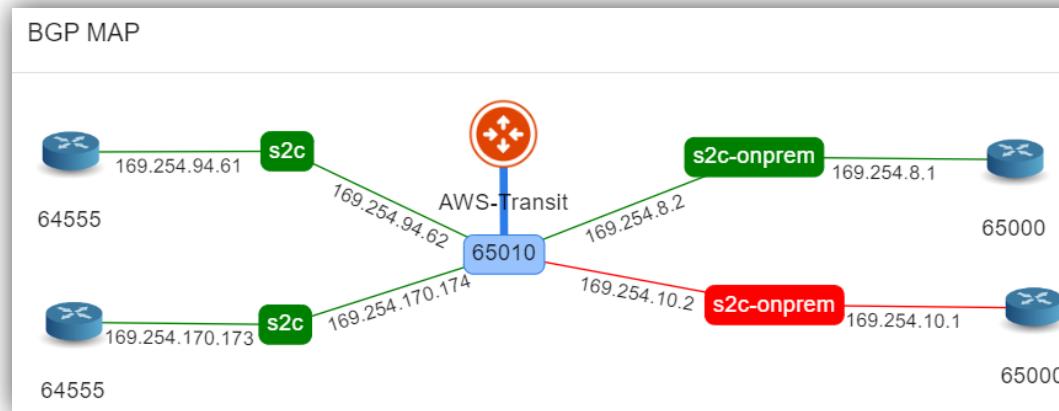
| Cloud Routes | Gateway Routes | VPC/VNet Routes | External Connections | BGP Info |
|--|--|----------------------|----------------------|-----------------------|
| Y ☰ ▼ | | | | |
| ^ Name | VPC/VNet | BGP Status | Status | Tunnel Status |
| ACE-ONPREM-DC | ace-aws-eu-west-1-transit1(vpc-04804a29e22b93c0) | Enabled | Up | Up |
| Tunnel Name | Gateway | IP Address | Peer IP Addr... | Tunnel Proto... |
| tunnel-ace-aws-eu-west-1-tran... | ace-aws-eu-west-1-transit1 | 52.51.35.139 | 35.178.41.7 | IPsec |
| | | | | Up |
| | | | | Active |
| | | | | Jan 29, 2024 12:19 PM |

Site2Cloud BGP via CoPilot

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



| Gateway | VPC/VNet | BGP Mode | BGP HA Status | Local ASN | Status |
|-------------------------------|--|---|----------------|-----------|---|
| ace-aws-eu-west-1-transit1 | ace-aws-eu-west-1-transit1(vpc-03a86350fa4909abd) (10.1.200.0/ | <input checked="" type="checkbox"/> Enabled | activemesh | 65011 | <input checked="" type="checkbox"/> Established |
| Connection Name | Remote AS Number | Neighbor IP | Local IP | | Neighbor Status |
| ACE-ONPREM-DC(169.254.74.129) | 65012 | 169.254.74.129 | 169.254.74.130 | | <input checked="" type="checkbox"/> Established |



LEARNED CIDR

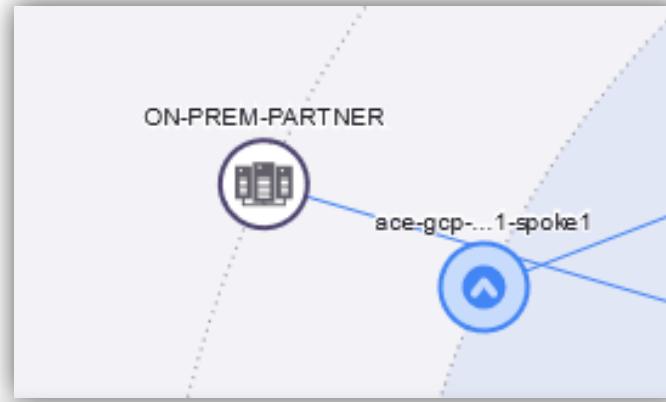
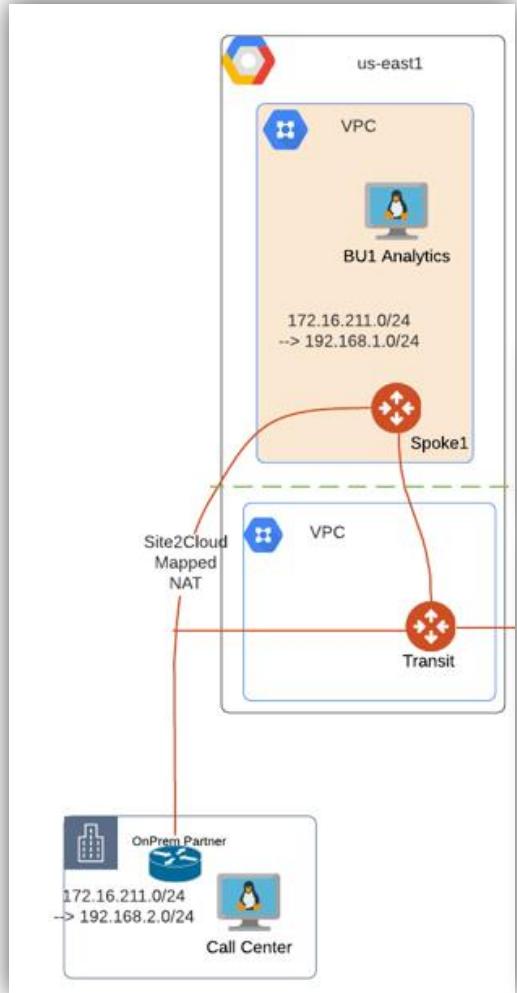
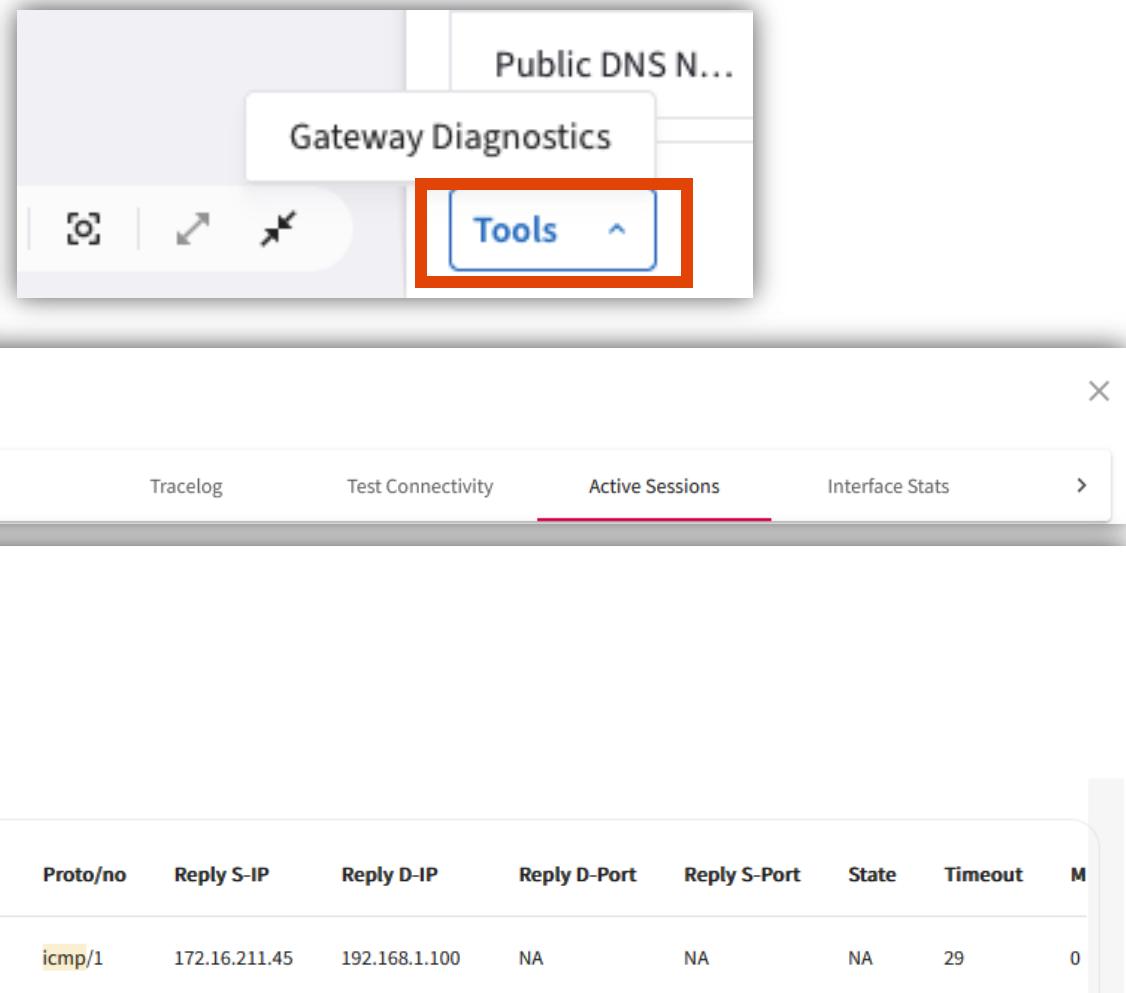
| Search |
|---------------|
| Networks 5 |
| 10.230.0.0/16 |
| 10.240.0.0/24 |

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 Fabric > Topology > select the relevant Gateway > Diagnostic Tools

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

Active Sessions

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