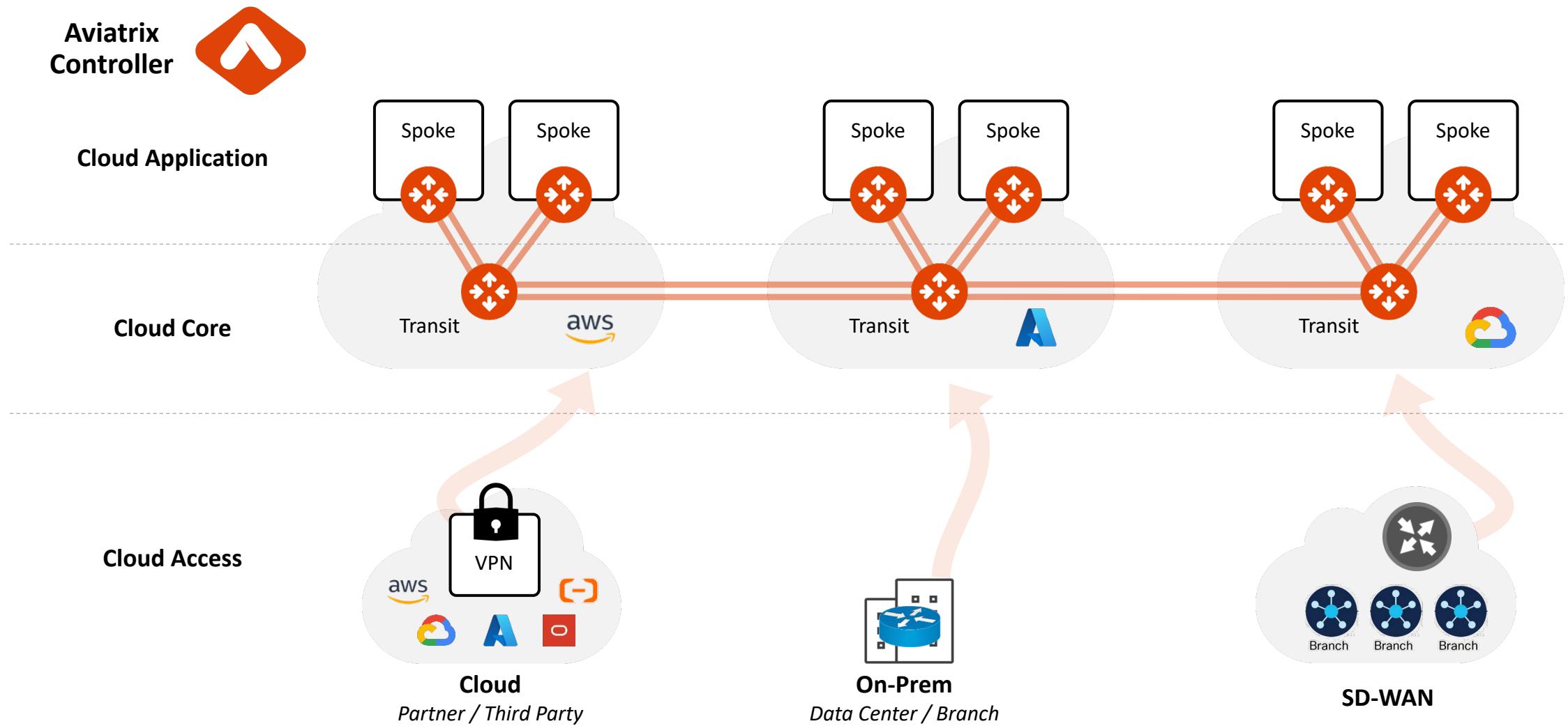




## Site2Cloud

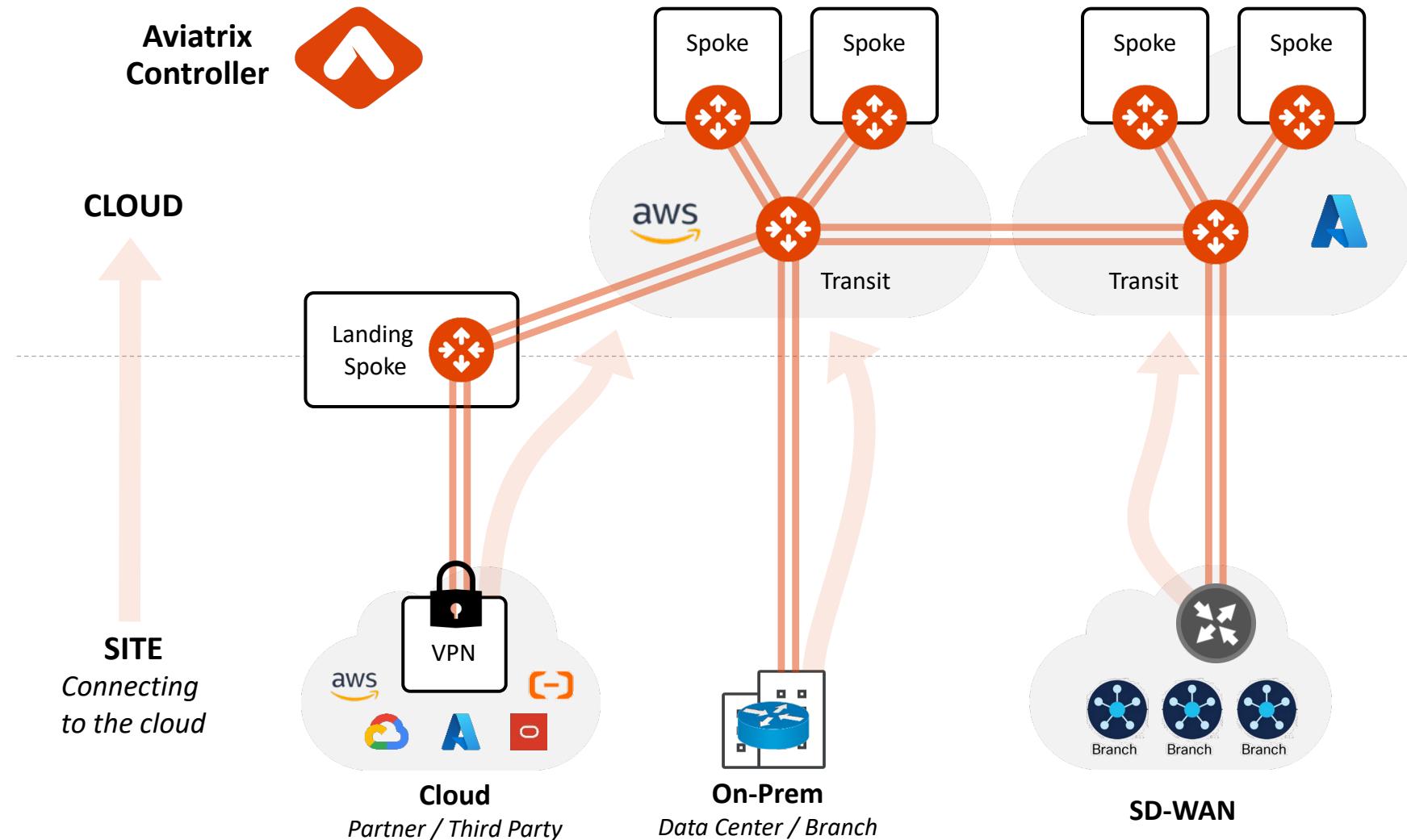


# Aviatrix Multicloud Network Architecture



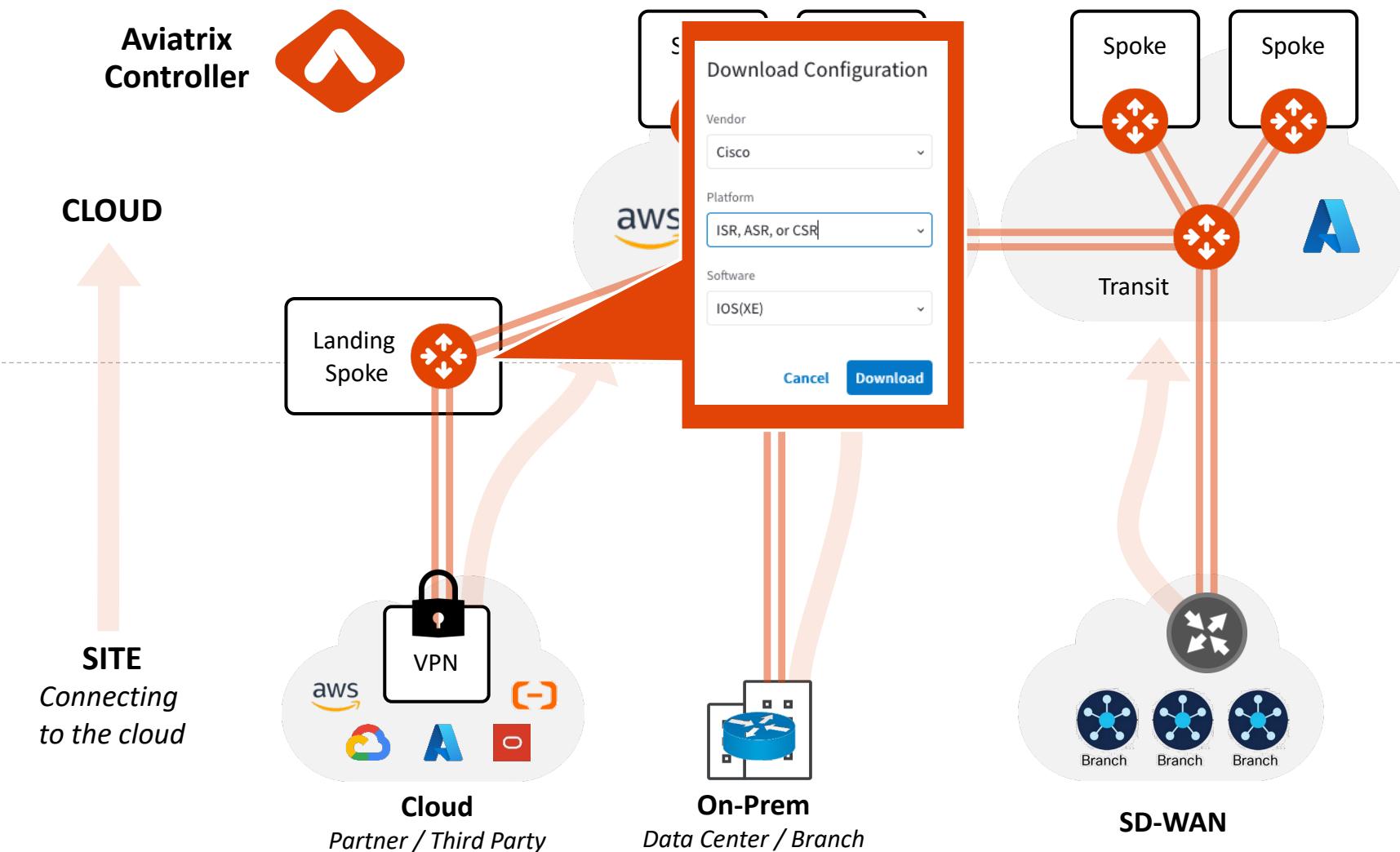
# Site2Cloud Introduction

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



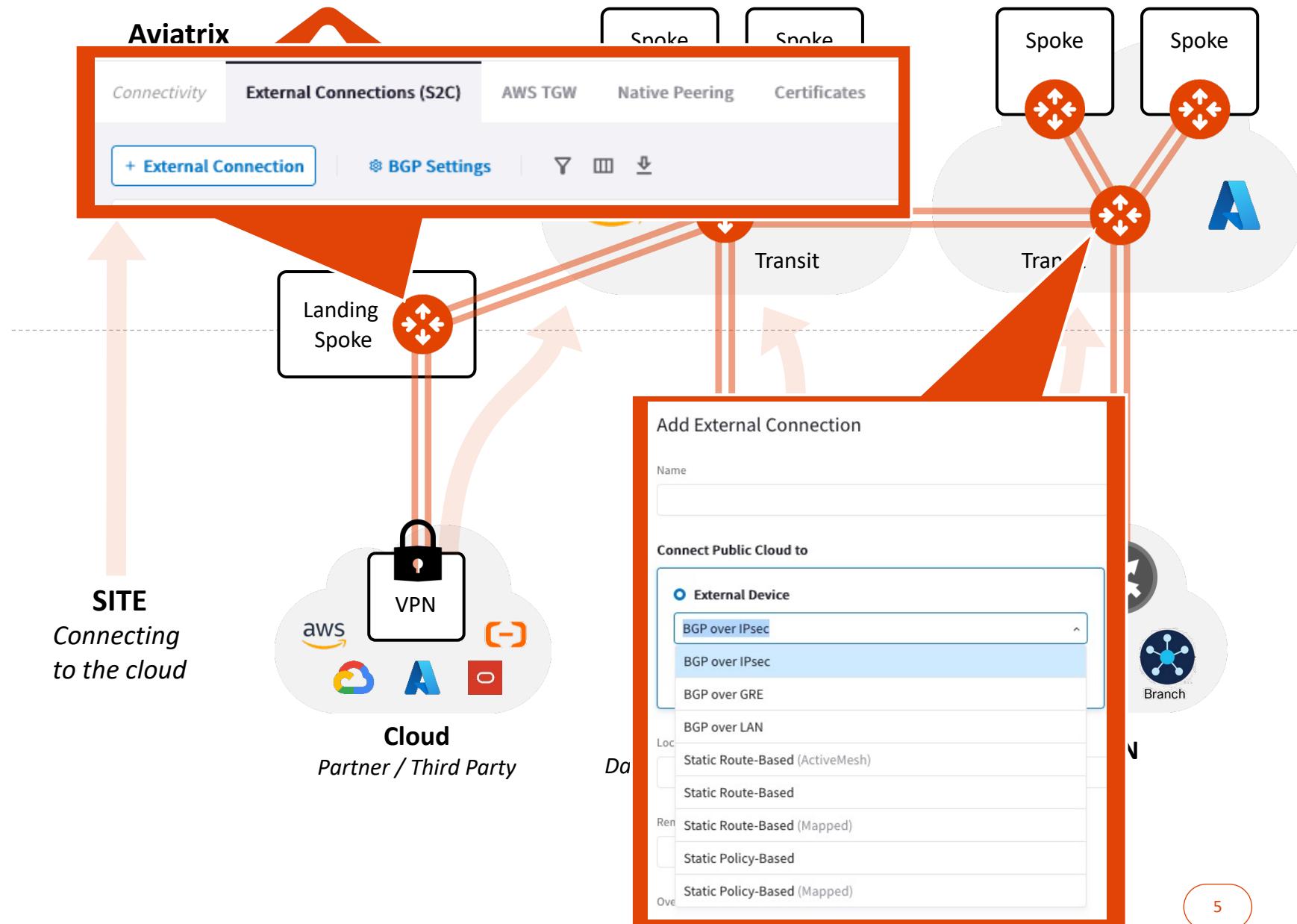
# Site2Cloud Solution

- 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

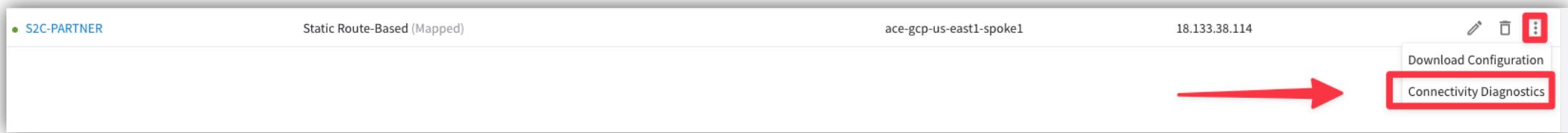
Connection

Connectivity	External Connections (S2C)	AWS TGW	Native Peering	Certificates
	<a href="#">+ External Connection</a>			
	<a href="#">BGP Settings</a>			
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	

- 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



- 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](https://en.wikipedia.org/wiki/Security_Parameter_Index)

A screenshot of the 'Connectivity Diagnostics Tools' interface. The title is 'Connectivity Diagnostics Tools: S2C-PARTNER'. On the left, there's a sidebar titled 'Tools' with options: 'Gateway Instance' (dropdown), 'Logs' (selected), 'Security Association Details', 'IPsec Service', 'Configuration', 'Security Policy Details', 'Analysis', and 'Reset Connection'. To the right of the sidebar is a main area titled 'Logs' with a 'Verbose Logging' section containing 'Enable' and 'Disable' buttons. Below this is a 'Run' button. In the center, there's a small illustration of a person standing next to a set of three toggle switches. At the bottom, the text 'Select Gateway and Tool from the left to begin' is displayed.

# 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)
```

## Aviatrix Controller output of SITE2CLOUD > Diagnostics > 'show 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 96ecdab9 87f9a01b ebe59b21 0cc0481b e1faaeb4 bd569f76 ad9e792e c9c5668b
    A: hmac-sha256 00460de3 70ad81af 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 17:57:25 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

# Monitoring – ‘Current’ number is increasing

Aviatrix Controller output of SITE2CLOUD > Diagnostics > ‘show security association details’

## First time

```
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 ebe59b21 0cc0481b e1faaeb4
        bd569f76 ad9e792e c9c5668b
        A: hmac-sha256 00460de3 70ad81af 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
```

Aviatrix Controller output of SITE2CLOUD > Diagnostics > ‘show security association details’

## Second time

```
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 ebe59b21 0cc0481b e1faaeb4
        bd569f76 ad9e792e c9c5668b
        A: hmac-sha256 00460de3 70ad81af 91eed15a 0cf33b21
        172b8abe 2d9bea7f 4e9822b0 9362006f
            seq=0x00000000 replay=0 flags=0x00000000 state=mature
            created: Nov 30 17:57:14 2020           current: Nov 30
        18:41:49 2020
            diff: 2675(s) hard: 3600(s) soft: 2880(s)
            last: Nov 30 17:57:26 2020 hard: 0(s)   soft: 0(s)
            current: 27012 (bytes)           hard: 0 (bytes)
            soft: 0 (bytes)
            allocated: 548                  hard: 0       soft: 0
            sadb_seq=5 pid=27784 refcnt=0
```

‘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)
  - 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](https://docs.aviatrix.com/HowTos/site2cloud_faq.html)

# Diagnostics - Run Analysis

Connectivity Diagnostics Tools: S2C-PARTNER

The screenshot shows a web-based interface for connectivity diagnostics. On the left, a sidebar titled "Tools" lists several options: "Gateway Instance" (set to "ace-gcp-us-east1-sp ..."), "Logs", "Security Association Details", "IPsec Service", "Configuration", "Security Policy Details", and "Analysis". The "Analysis" button is highlighted with a red box. Below the sidebar, there's a "Reset Connection" button. The main area is titled "Analysis" and shows the status "Connection S2C-PARTNER is UP." A "Run" button is located in the top right corner of this area, also highlighted with a red box. At the bottom right of the main area is a "Close" button.

Last Run: Nov 3, 2023 3:58 PM

Run

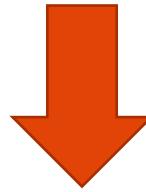
Analysis

Connection S2C-PARTNER is UP.

Close

# Analysis – On-prem router is down

On-prem router is **down**



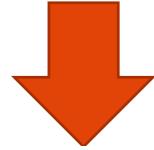
Tunnel analysis for connection London-S2C:

Tunnel AWS-UE2-Prod4-S2C-GW<-->52.64.179.48: 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 Groups associated with i-06b88aa0bf47944		
Ports	Protocol	Source
80	tcp	0.0.0.0/0
22	tcp	0.0.0.0/0
N/A	icmpv6	::/0
4500	udp	0.0.0.0/0
<u>500</u>	<u>udp</u>	<u>0.0.0.0/0</u>
3389	tcp	0.0.0.0/0
179	tcp	0.0.0.0/0
N/A	icmp	0.0.0.0/0



Tunnel analysis for connection London-S2C:

Tunnel AWS-UE2-Prod4-S2C-GW<-->52.64.179.48: 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

On-Prem Cisco IOS config:

```
crypto keyring 52.64.179.48-3.128.2.253  
  pre-shared-key address 3.128.2.253 key WRONG
```



Tunnel analysis for connection London-S2C:

Tunnel AWS-UE2-Prod4-S2C-GW<-->52.64.179.48: ISAKMP Phase 1 SA is not established. Possible reasons:

1. Peer gateway not reachable over UDP port 4500,
2. Pre-shared key mismatch.

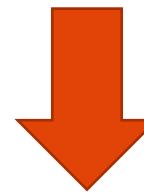
# Analysis – DH Group mismatch

## Connection Detail

```
IKE Version: 1
Connection Type: mapped
DPD config: enable
BGP status: disabled
Insane mode: disabled
Load balancing: undefined
Real Local Subnet: 10.5.16.0/20
Virtual Local Subnet: 172.5.16.0/20
Real Remote Subnet: 10.5.16.0/20
Virtual Remote Subnet: 192.5.16.0/20
Phase 1 Authentication: SHA-256
Phase 2 Authentication: HMAC-SHA-256
Phase 1 DH Groups: 14
Phase 2 DH Groups: 14
Phase 1 Encryption: AES-256-CBC
Phase 2 Encryption: AES-256-CBC
Tunnel Type: Site2Cloud_Routed
```

On-Prem Cisco IOS config:

```
crypto isakmp policy 1
    encryption aes 256
    hash sha256
    authentication pre-share
    group 2
    lifetime 28800
```



Tunnel analysis for connection London-S2C:

Tunnel AWS-UE2-Prod4-S2C-GW<-->52.64.179.48: ISAKMP Phase 1 SA is not established. Possible reasons:  
1. Encryption/Authentication algorithm mismatch,  
2. DH group number mismatch.

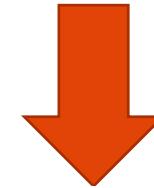
# Analysis – Encryption algorithm mismatch

## Connection Detail

```
IKE Version: 1
Connection Type: mapped
DPD config: enable
BGP status: disabled
Insane mode: disabled
Load balancing: undefined
Real Local Subnet: 10.5.16.0/20
Virtual Local Subnet: 172.5.16.0/20
Real Remote Subnet: 10.5.16.0/20
Virtual Remote Subnet: 192.5.16.0/20
Phase 1 Authentication: SHA-256
Phase 2 Authentication: HMAC-SHA-256
Phase 1 DH Groups: 14
Phase 2 DH Groups: 14
Phase 1 Encryption: AES-256-CBC
Phase 2 Encryption: AES-256-CBC
Tunnel Type: Site2Cloud_Routed
```

On-Prem Cisco IOS config:

```
crypto ipsec transform-set 52.64.179.48-3.128.2.253 esp-aes esp-sha-hmac
mode tunnel
```



Tunnel analysis for connection London-S2C:

Tunnel AWS-UE2-Prod4-S2C-GW<-->52.64.179.48: 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 blue box)

Verbose Logging: Enable (highlighted with blue box)

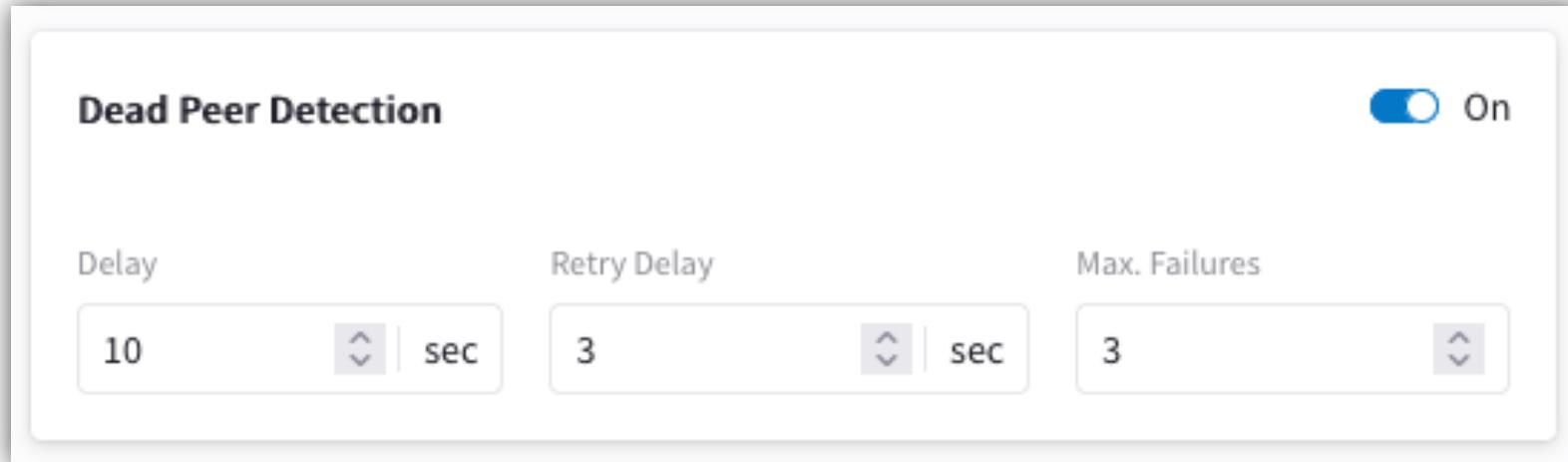
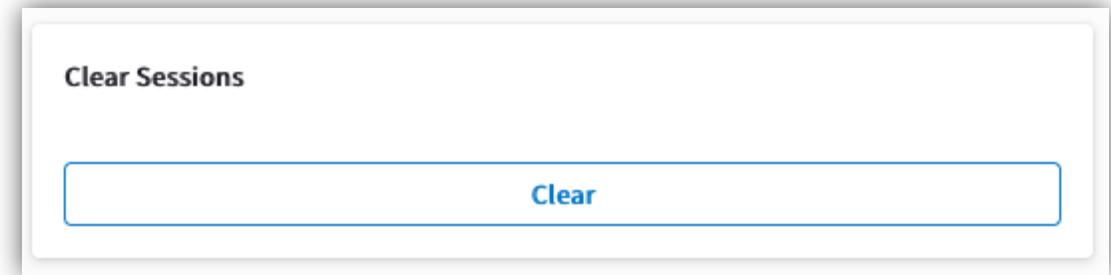
Logs

```
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 SITE2CLOUD > Setup
  - Restart the VPN service from SITE2CLOUD > 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 '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 over the second connection (S2C-PARTNER), with 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... x

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

The screenshot shows a web-based interface for BGP troubleshooting. At the top, it says 'BGP Diagnostics Tools: ACE-ONPREM-DC'. On the left, there's a sidebar with 'Tools' and 'Gateway Instance' set to 'ace-aws-eu-west...'. Below that is a 'BGP Command' section. In the center, there's a large input field labeled 'Command' containing '|'. A dropdown menu lists various BGP-related commands. To the right of the input field is a large black rectangular area. At the bottom right of the interface is a 'Close' button.

# 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 Run

Last Run: Nov 3, 2023 4:16 PM

Command show ip bgp ×

**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

A large, solid orange shape curves from the top left towards the bottom right, creating a dynamic background element.

# 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



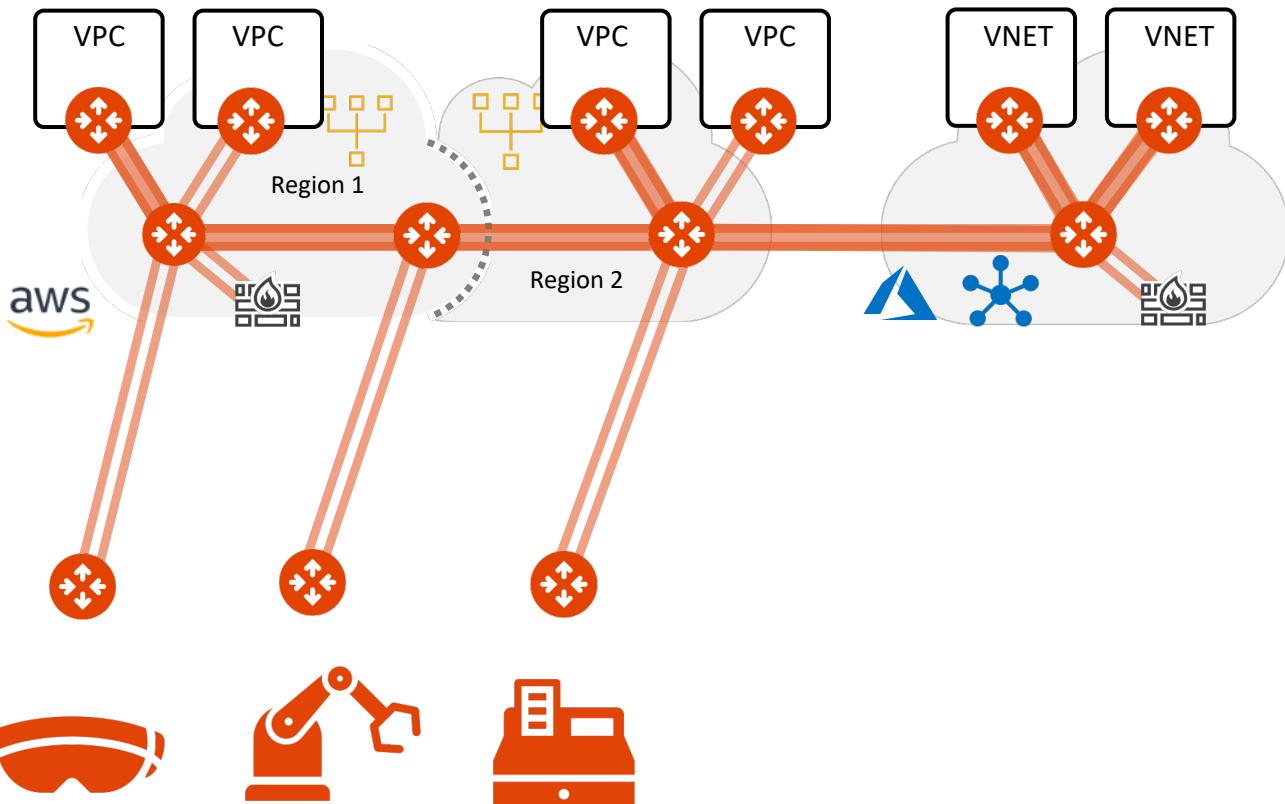
## Simplified Edge Management



## Consistent Secure Edge

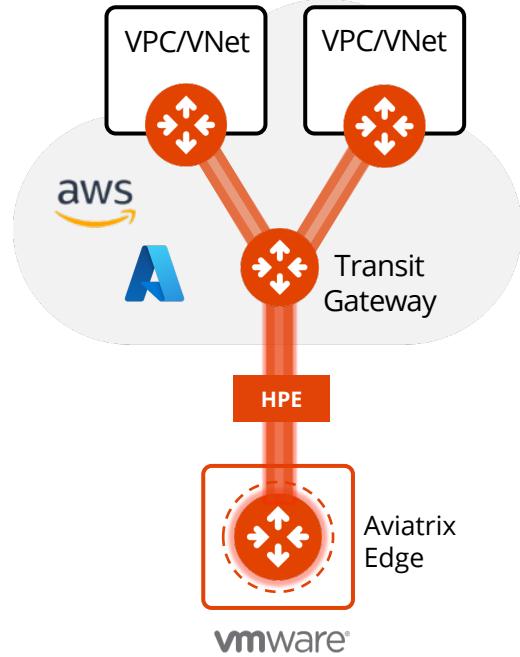


## Simplified Edge On-boarding

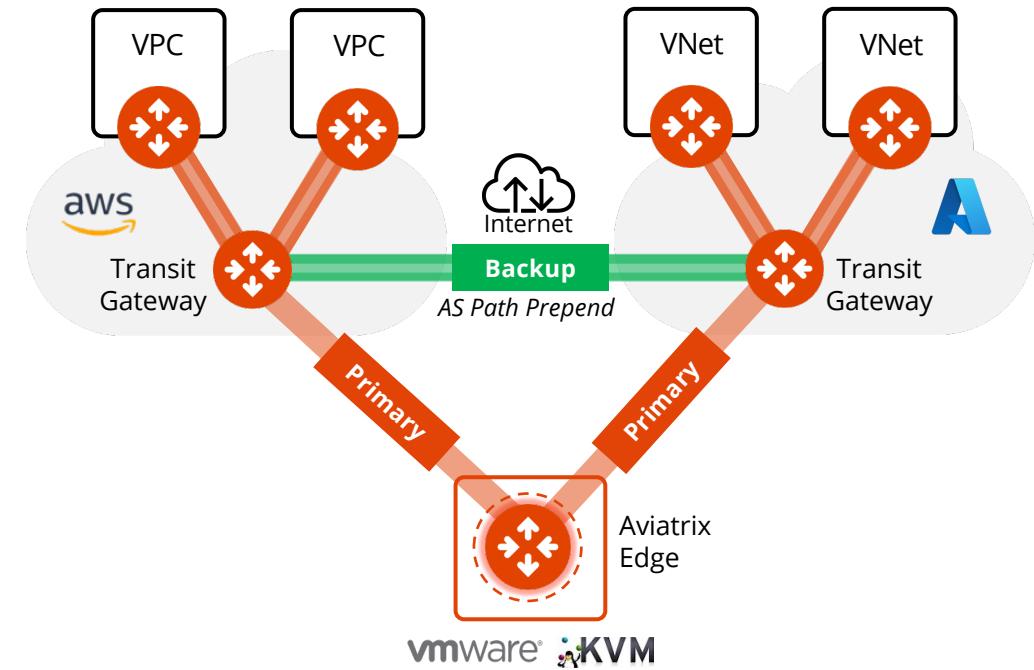


# Aviatrix Edge Use Cases

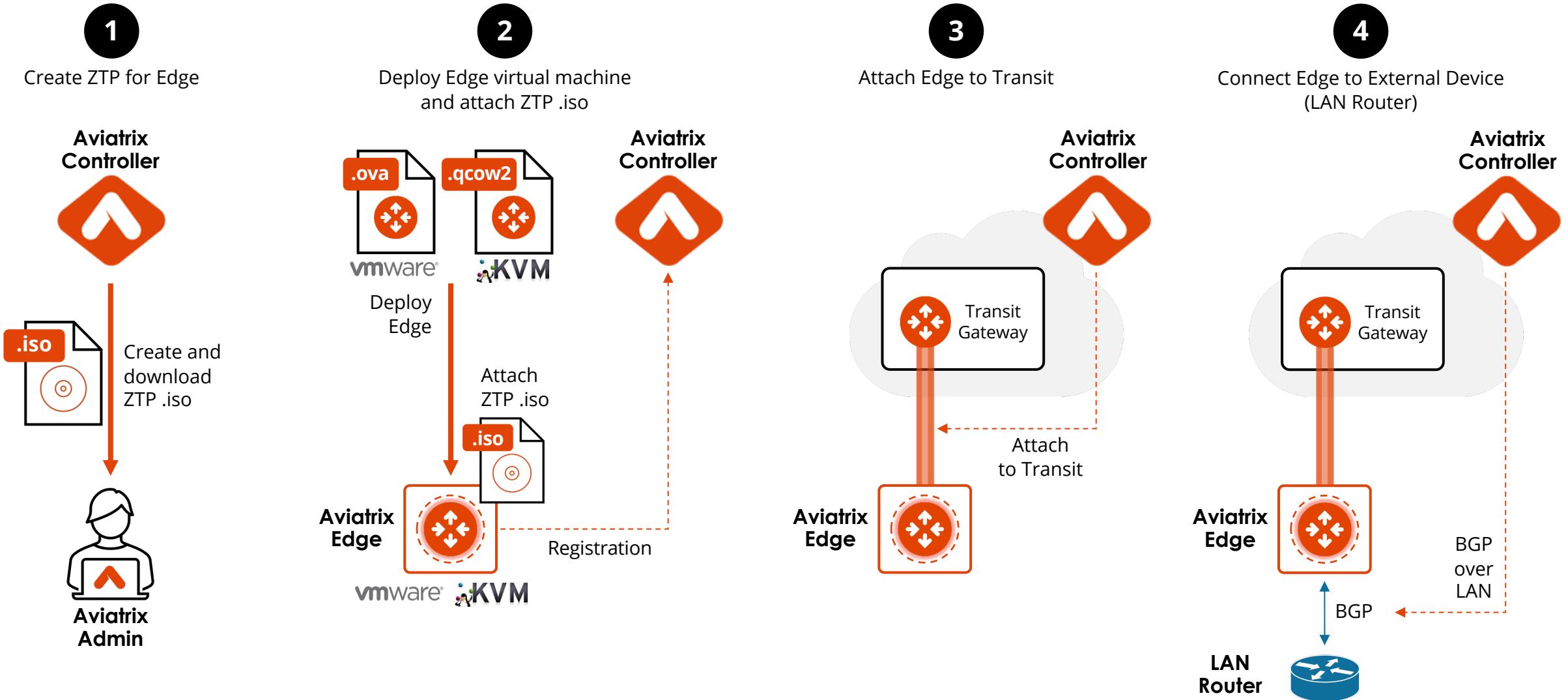
## Extend the Aviatrix Platform to the Edge



## Multi-Cloud Connectivity via Aviatrix Edge



# Edge 2.0 Deployment Workflow - Demo

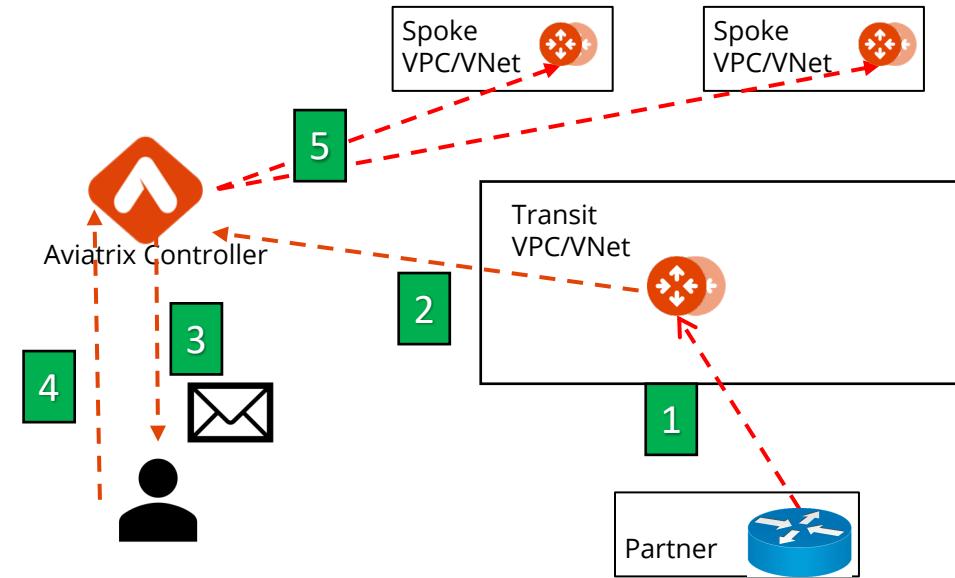


# BGP Route Approval

# 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  
From: 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

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

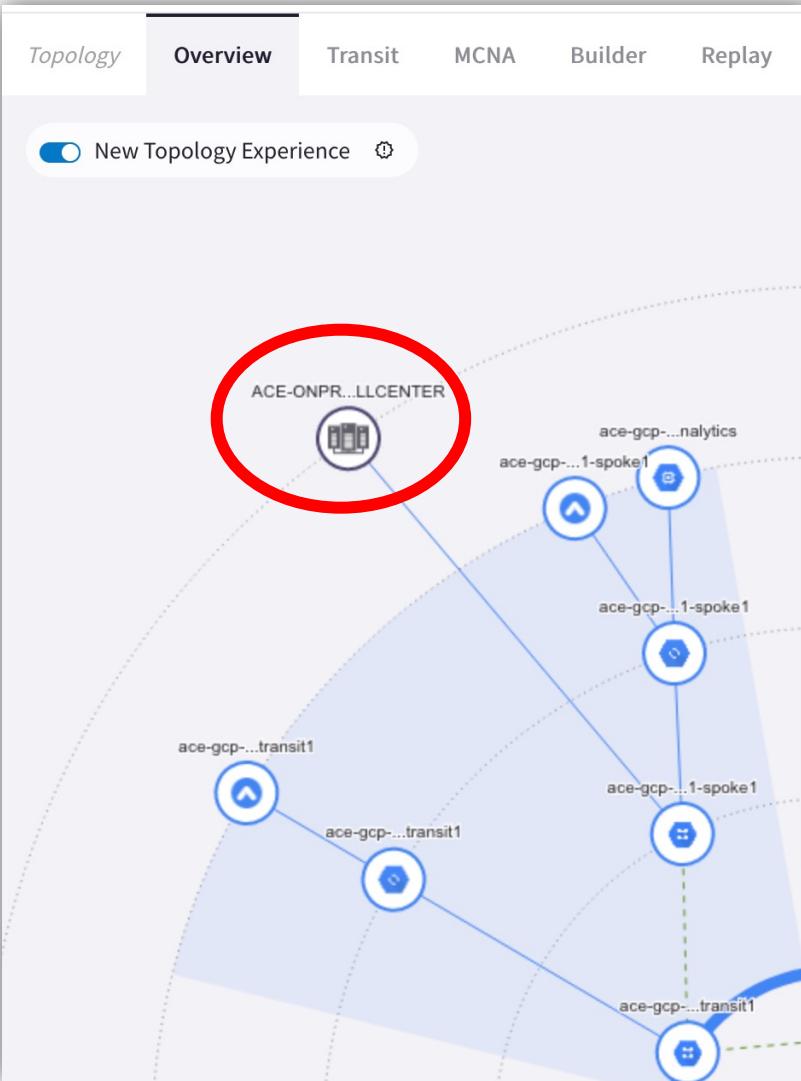
ace-aws-eu-west-1-transit1 eu-west-1a subnet-0557b31d4673c3aca Up

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

# Site2Cloud & CoPilot

# Site2Cloud Visibility via CoPilot

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



### Cloud Routes

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	

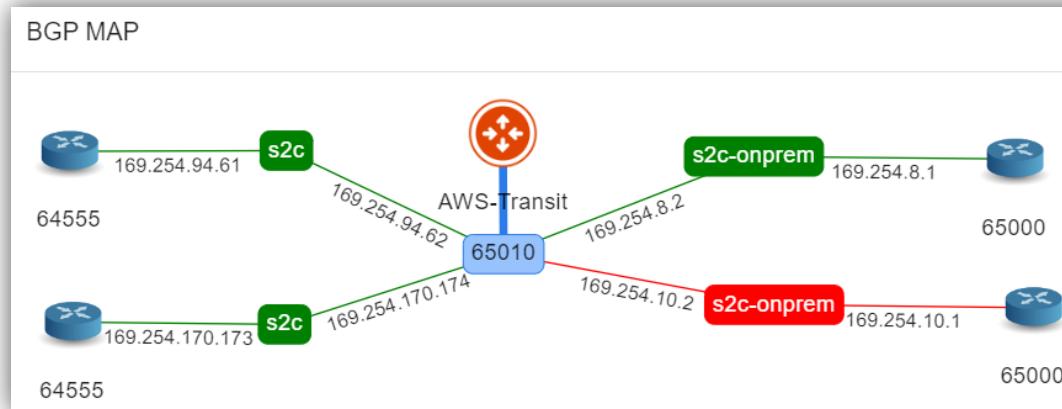
# Site2Cloud BGP via CoPilot

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

Cloud Routes   Gateway Routes   VPC/VNet Routes   External Connections   **BGP Info**

Y   □   ↓

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/	Enabled	activemesh	65011	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		Established



LEARNED CIDR

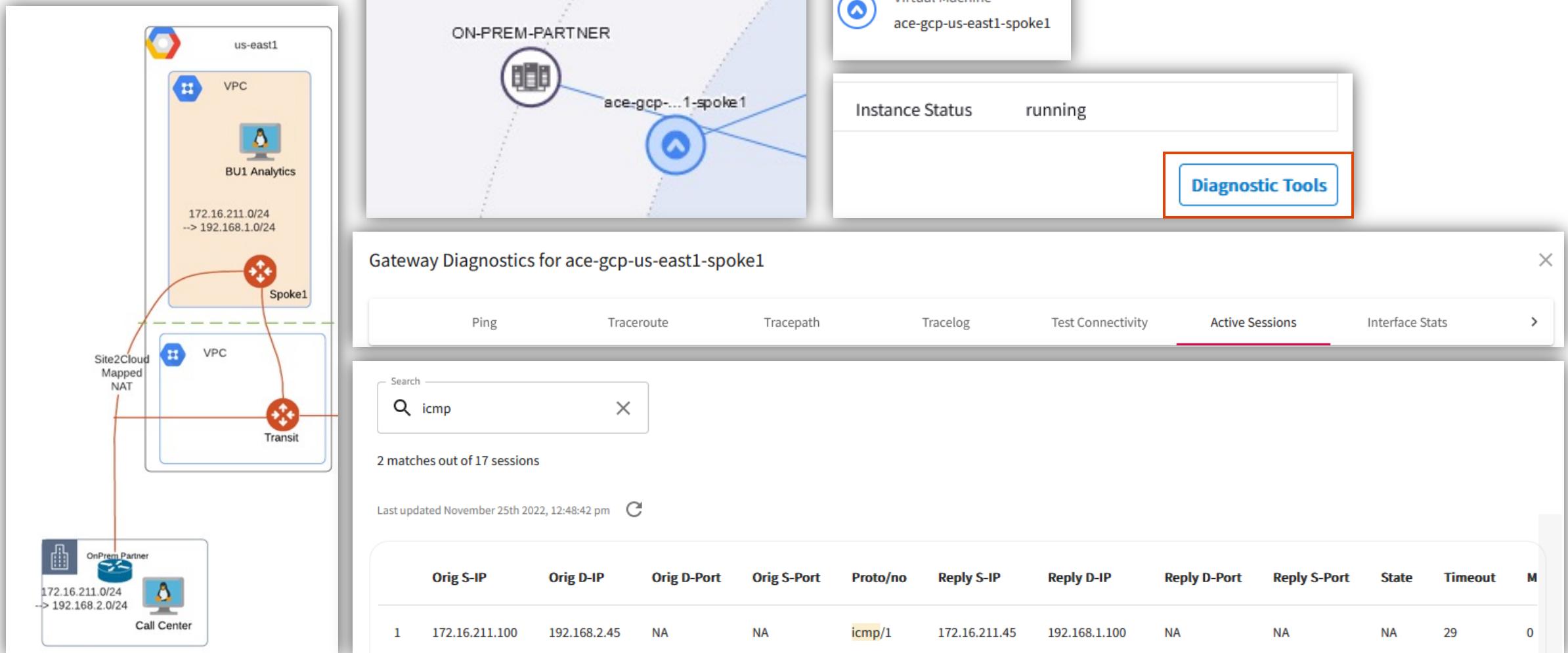
Search
Networks 5
10.230.0.0/16
10.240.0.0/24

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





---

Next: Lab 3 Site2Cloud