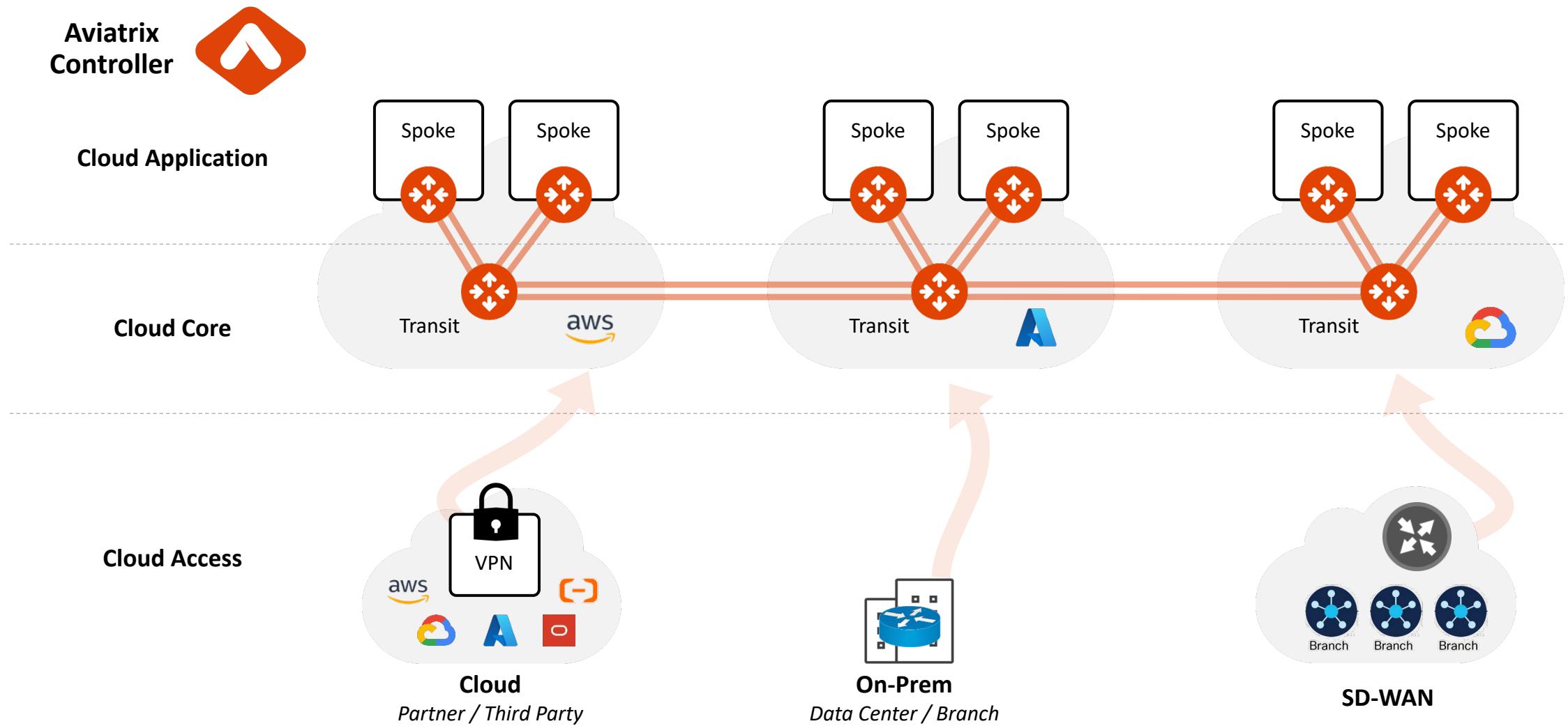




Site2Cloud

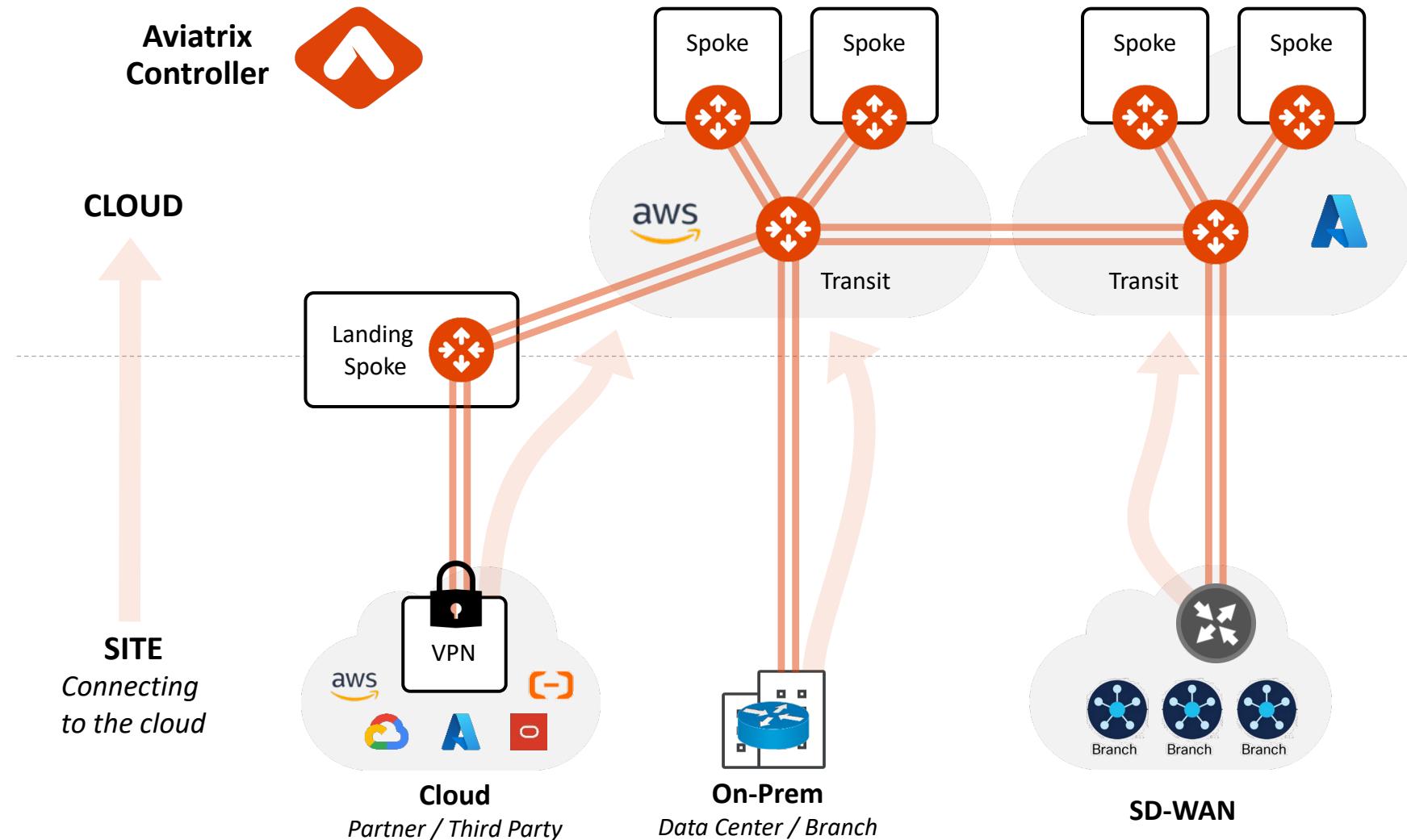


Aviatrix Multicloud Network Architecture



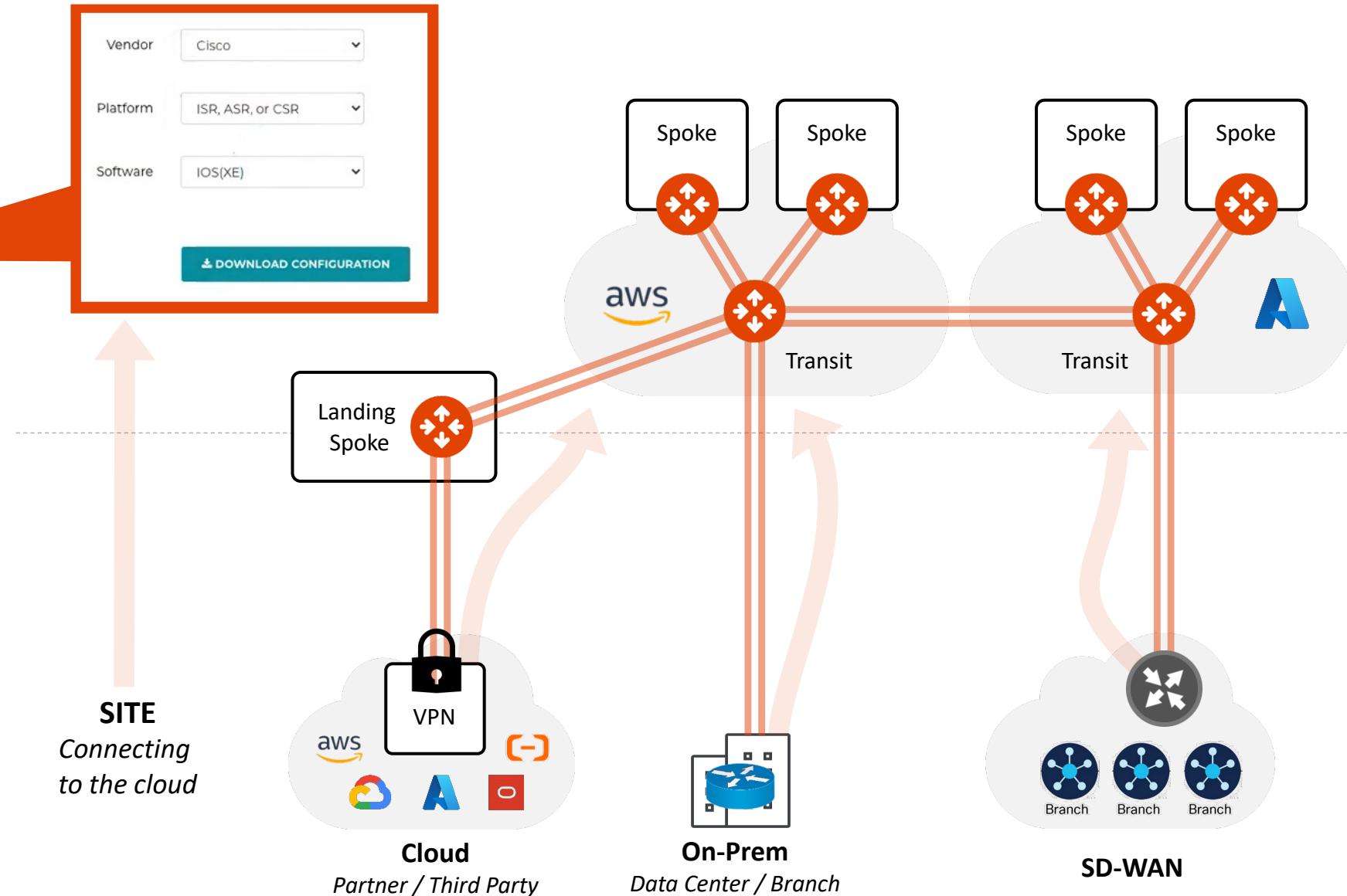
Site2Cloud Introduction

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



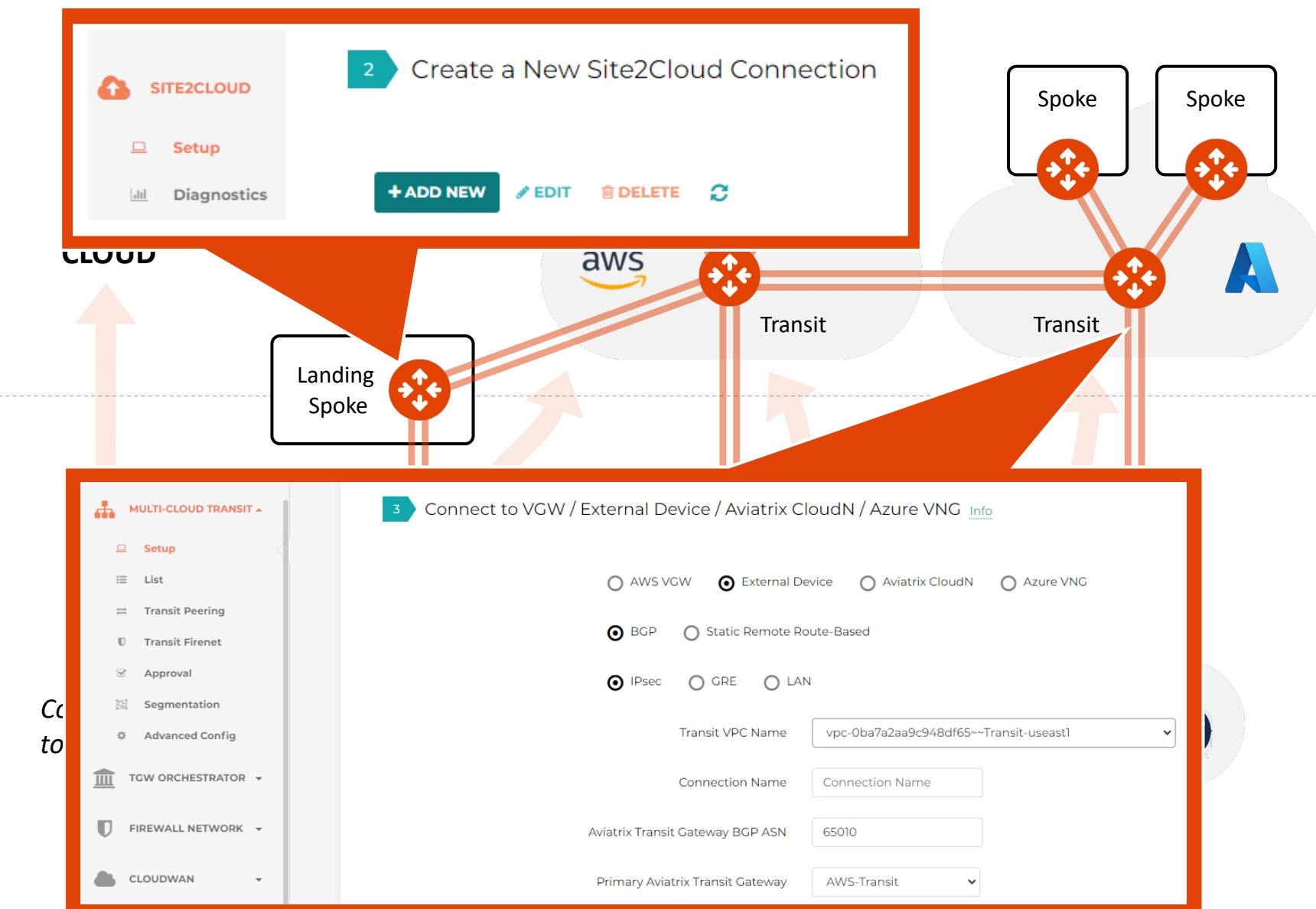
Site2Cloud Solution

- 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



Site2Cloud – Spoke GWs

2 Create a New Site2Cloud Connection

SITE2CLOUD

Setup

Diagnostics

+ADD NEW EDIT DELETE

VPC ID/VNet Name: vpc-0733324d94f476452~~Spoke-1-useast1x

Connection Type: Unmapped

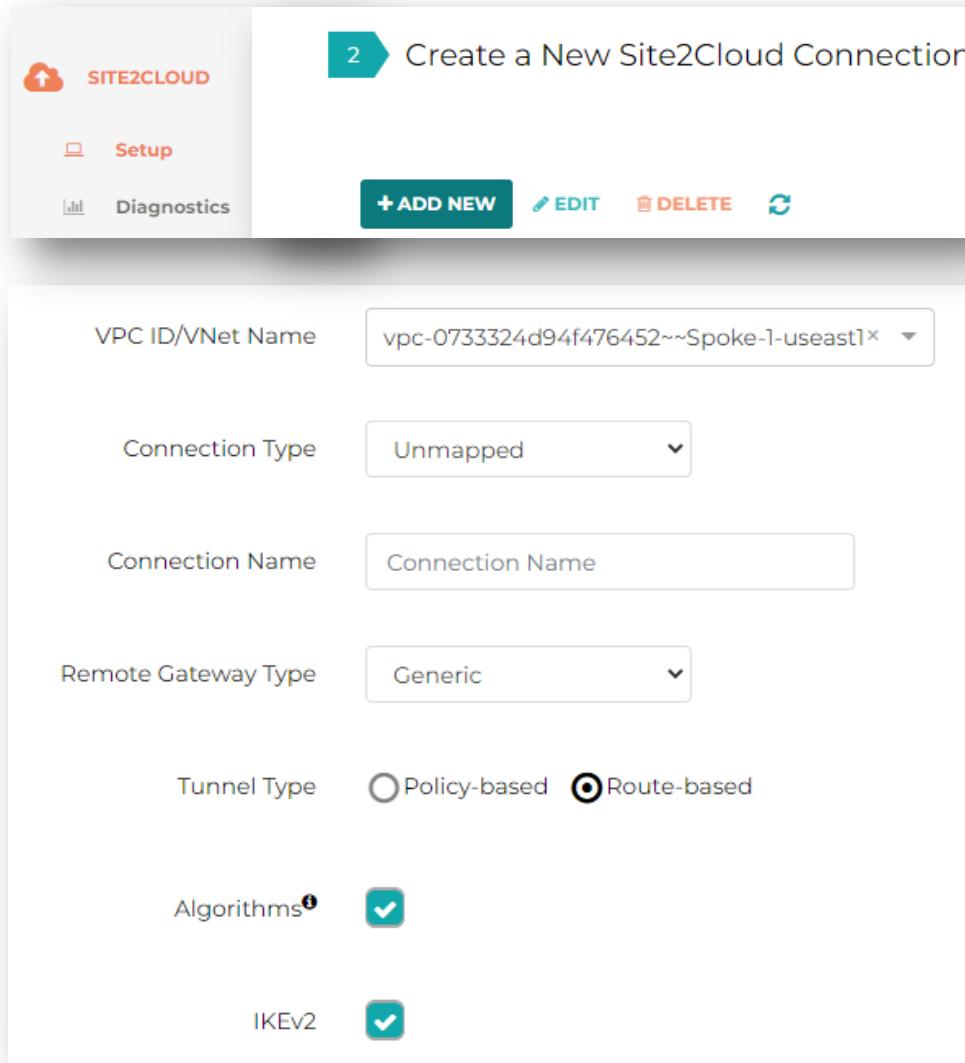
Connection Name: Connection Name

Remote Gateway Type: Generic

Tunnel Type: Policy-based Route-based

Algorithms:

IKEv2:



Primary Cloud Gateway: AWS-Spoke1

Remote Gateway IP Address: 13.66.213.176

Pre-shared Key: spoke1demo

Local Tunnel IP: Local Tunnel IP -- optional

Remote Tunnel IP: Remote Tunnel IP -- optional

Backup Gateway: AWS-Spoke1

Remote Gateway IP Address (Backup): 13.66.213.176

Same Pre-shared Key as Primary:

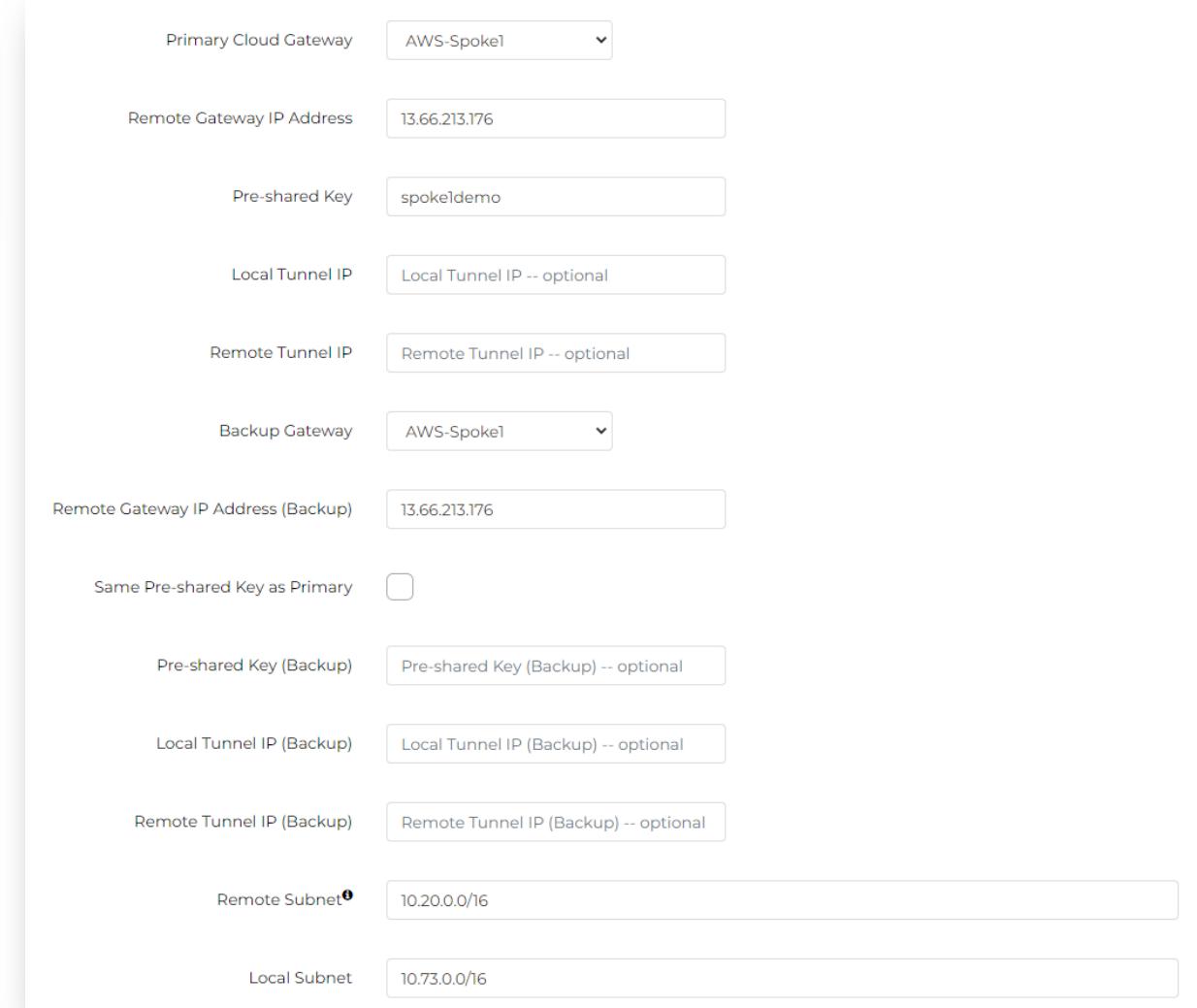
Pre-shared Key (Backup): Pre-shared Key (Backup) -- optional

Local Tunnel IP (Backup): Local Tunnel IP (Backup) -- optional

Remote Tunnel IP (Backup): Remote Tunnel IP (Backup) -- optional

Remote Subnet: 10.20.0.0/16

Local Subnet: 10.73.0.0/16



Site2Cloud – Transit Gateways

- Site2Cloud tunnels can also be built using the Aviatrix **Multi-Cloud Transit Setup** workflow
- **BGP** is supported on Site2Cloud tunnels to either Transit Gateway or Spoke Gateway

The screenshot shows the Aviatrix Multi-Cloud Transit Setup interface. On the left, a sidebar lists various cloud services: DASHBOARD, ONBOARDING, ACCOUNTS, GATEWAY, MULTI-CLOUD TRANSIT (with 'Setup' selected), TGW ORCHESTRATOR, FIREWALL NETWORK, CLOUDWAN, PEERING, SITE2CLOUD, OPENVPN®, SECURITY, and USEFUL TOOLS. The 'MULTI-CLOUD TRANSIT' section is expanded, showing sub-options: List, Transit Peering, Transit Firenet, Approval, Segmentation, and Advanced Config. On the right, a configuration form titled 'Connect to VGW / External Device / Aviatrix CloudN / Azure VNG' is displayed. It includes a legend with radio buttons for AWS VGW, External Device, Aviatrix CloudN, and Azure VNG. The 'BGP' option is selected and highlighted with a red box. Below the legend are fields for 'Transit VPC Name' (set to 'vpc-08df0d841d91cb81b~aws-us-east-1-transit2-vpc'), 'Connection Name' (empty), 'Aviatrix Transit Gateway BGP ASN' (set to '65000'), 'Primary Aviatrix Transit Gateway' (set to 'aws-us-east-1-transit2-agw'), 'Algorithms' (unchecked), 'IKEv2' (unchecked), 'Enable Remote Gateway HA' (unchecked), 'Over Private Network' (unchecked), 'Remote BGP AS Number' (empty), 'Remote Gateway IP' (empty), 'Pre-shared Key' (empty), 'Local Tunnel IP' (empty), and 'Remote Tunnel IP' (empty). A large blue 'CONNECT' button is at the bottom right.

Site2Cloud Connection Types

Verification

ONBOARDING

ACCOUNTS

GATEWAY

MULTI-CLOUD TRANSIT

TGW ORCHESTRATOR

FIREWALL NETWORK

CLOUDWAN

PEERING

SITE2CLOUD

- Setup
- Diagnostics

OPENVPN®

Setup Site2Cloud Connection

1 Launch a Gateway

If you have not done so, click Gateway on the navigation bar to launch a gateway. When complete return to this page and proceed to the next step to add site2cloud connection.

2 Create a New Site2Cloud Connection [Info](#)

+ ADD NEW EDIT DELETE

T COLUMN MENU

VPC ID/VNet Name	Name	Status	Aviatrix Gateway	Peer Type	HA Status	Tunnel Type	Remote Gateway IP	Remote Subnet	Local Subnet
vpc-08df0d841d91cb...	Cisco-Branch	Up	aws-us-east-1-transit...	generic	enabled	Transit_BGP	3.219.34.143,3.219.34...	aws-us-east-1-transit2...	
azure-us-west-spoke...	Wisconsin-...	Down	azure-us-west-spoke...	generic	disabled	Site2Cloud_Policy	3.137.215.72	172.31.0.0/24	10.42.0.0/16
gcp-us-central1-spok...	Ohio-Branch	Up	gcp-us-central1-spok...	generic	disabled	Site2Cloud_Routed	3.137.211.98	192.168.100.0/24	192.168.200.0/24

Monitoring & Troubleshooting Site2Cloud

Monitoring

- Tunnel is operational? ‘Current’ number is increasing on both ends
 - Controller > SITE2CLOUD > Diagnostics > ‘show security association details’
 - 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

Diagnostics [Info](#)

VPC ID/VNet Name: vpc-0ba7a2aa9c948df65~Transit-useast1

Connection: s2c

Gateway: AWS-Transit

Action: Show security association details

OK

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

Diagnostics

The screenshot shows the Aviatrix Diagnostics interface. On the left, a sidebar lists navigation options: ONBOARDING, ACCOUNTS, GATEWAY, MULTI-CLOUD TRANSIT, TGW ORCHESTRATOR, FIREWALL NETWORK, CLOUDWAN, PEERING, and SITE2CLOUD. Under SITE2CLOUD, there are two sub-options: Setup and Diagnostics, with Diagnostics being the active tab. The main area is titled "Diagnostics" with an "Info" link. It contains three dropdown menus: "VPC ID/VNet Name" set to "vpc-08df0d841d91cb81b~~aws-us-east-1-transit2-vpc", "Connection" set to "Cisco-Branch", and "Gateway" set to "aws-us-east-1-transit2-agw". A "Action" dropdown menu is open, listing several options: "Show logs" (selected), "Show security association details", "Show service status", "Show configuration", "Enable verbose logging", "Disable verbose logging", "Show security policy details", "Restart service", and "Run analysis". The "Run analysis" button is highlighted with a blue background.

VPC ID/VNet Name

Connection

Gateway

Action

- ✓ Show logs
- Show security association details
- Show service status
- Show configuration
- Enable verbose logging
- Disable verbose logging
- Show security policy details
- Restart service

Run analysis

Diagnostics – Run analysis

Diagnostics [Info](#)

VPC ID/VNet Name

Connection

Gateway

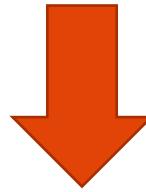
Action

✓OK

Connection Cisco-Branch is UP.

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.

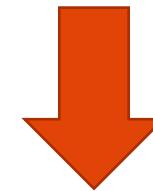
Analysis – DH Group mismatch

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

Diagnostics [Info](#)

VPC ID/VNet Name

Connection

Gateway

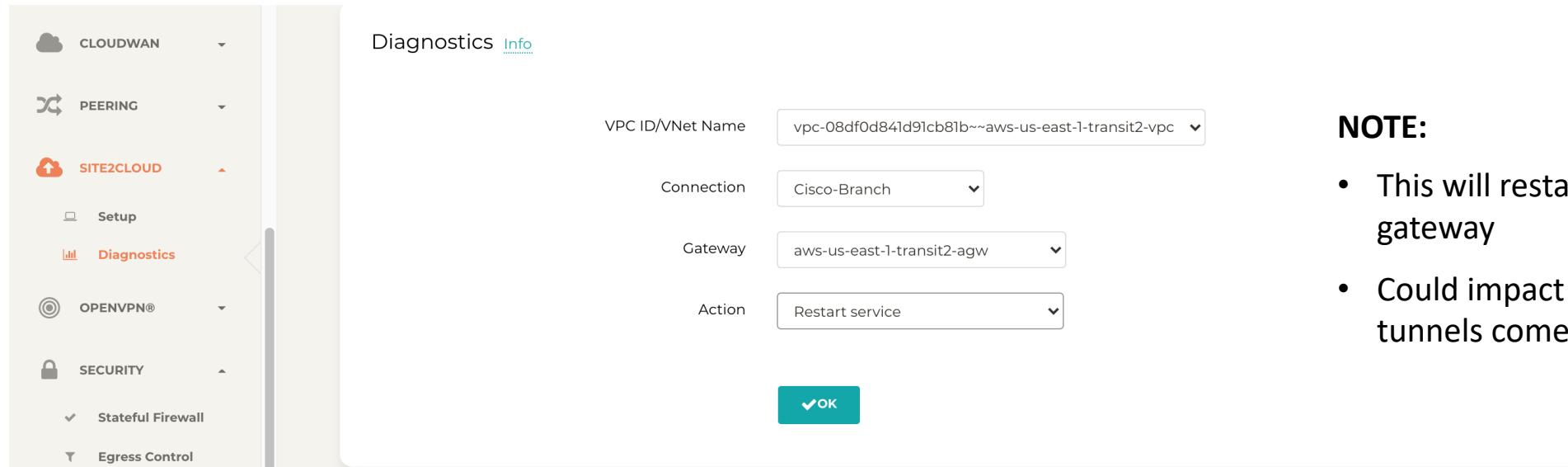
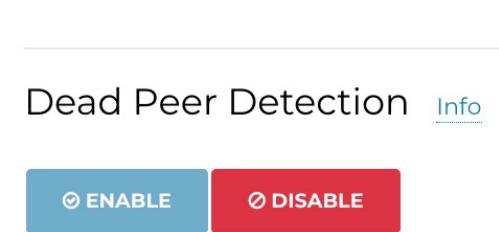
Action

✓OK

```
2021-01-20T03:26:46.605451+00:00 GW-aws-us-east-1-transit2-agw-52.203.177.219 racoon: INFO: KA remove: 10.20.0.184[4500]->3.219.34.143[4500]
2021-01-20T03:26:46.605408+00:00 GW-aws-us-east-1-transit2-agw-52.203.177.219 racoon: INFO: ISAKMP-SA deleted 10.20.0.184[4500]-3.219.34.143[4500] spi=832e88904855e6bf:37953dd95fc745f
2021-01-20T03:26:46.605299+00:00 GW-aws-us-east-1-transit2-agw-52.203.177.219 racoon: INFO: ISAKMP-SA expired 10.20.0.184[4500]-3.219.34.143[4500] spi=832e88904855e6bf:37953dd95fc745f
2021-01-20T03:10:14.387335+00:00 GW-aws-us-east-1-transit2-agw-52.203.177.219 racoon: INFO: IPsec-SA expired: ESP/Tunnel 3.219.34.143[4500]->10.20.0.184[4500] spi=232458848(0xddb0a60)
2021-01-20T03:00:01.800701+00:00 GW-aws-us-east-1-transit2-agw-52.203.177.219 racoon: INFO: IPsec-SA established: ESP/Tunnel 10.20.0.184[4500]->3.219.34.143[4500] spi=3835126865(0xe4976451)
2021-01-20T03:00:01.800616+00:00 GW-aws-us-east-1-transit2-agw-52.203.177.219 racoon: INFO: IPsec-SA established: ESP/Tunnel 10.20.0.184[4500]->3.219.34.143[4500] spi=56643516(0x3604fb)
2021-01-20T03:00:01.776433+00:00 GW-aws-us-east-1-transit2-agw-52.203.177.219 racoon: INFO: respond new phase 2 negotiation: 10.20.0.184[4500]<=>3.219.34.143[4500]
2021-01-20T02:58:14.387377+00:00 GW-aws-us-east-1-transit2-agw-52.203.177.219 racoon: INFO: IPsec-SA expired: ESP/Tunnel 10.20.0.184[4500]->3.219.34.143[4500] spi=801731997(0xfc9759d)
2021-01-20T02:58:14.387282+00:00 GW-aws-us-east-1-transit2-agw-52.203.177.219 racoon: INFO: IPsec-SA expired: ESP/Tunnel 3.219.34.143[4500]->10.20.0.184[4500] spi=232458848(0xddb0a60)
2021-01-20T02:19:41.683772+00:00 GW-aws-us-east-1-transit2-agw-52.203.177.219 racoon: INFO: IPsec-SA expired: ESP/Tunnel 3.219.34.143[4500]->10.20.0.184[4500] spi=94876720(0x5a7b430)
2021-01-20T02:10:14.387200+00:00 GW-aws-us-east-1-transit2-agw-52.203.177.219 racoon: INFO: IPsec-SA established: ESP/Tunnel 10.20.0.184[4500]->3.219.34.143[4500] spi=801731997(0xfc9759d)
2021-01-20T02:10:14.387096+00:00 GW-aws-us-east-1-transit2-agw-52.203.177.219 racoon: INFO: IPsec-SA established: ESP/Tunnel 10.20.0.184[4500]->3.219.34.143[4500] spi=232458848(0xddb0a60)
2021-01-20T02:10:14.363432+00:00 GW-aws-us-east-1-transit2-agw-52.203.177.219 racoon: INFO: respond new phase 2 negotiation: 10.20.0.184[4500]<=>3.219.34.143[4500]
2021-01-20T02:07:41.683847+00:00 GW-aws-us-east-1-transit2-agw-52.203.177.219 racoon: INFO: IPsec-SA expired: ESP/Tunnel 10.20.0.184[4500]->3.219.34.143[4500] spi=1809508839(0x6bd9e9e7)
2021-01-20T02:07:41.683743+00:00 GW-aws-us-east-1-transit2-agw-52.203.177.219 racoon: INFO: IPsec-SA expired: ESP/Tunnel 3.219.34.143[4500]->10.20.0.184[4500] spi=94876720(0x5a7b430)
2021-01-20T01:26:31.520923+00:00 GW-aws-us-east-1-transit2-agw-52.203.177.219 racoon: INFO: KA remove: 10.20.0.184[4500]->3.219.34.143[4500]
2021-01-20T01:26:31.520876+00:00 GW-aws-us-east-1-transit2-agw-52.203.177.219 racoon: INFO: ISAKMP-SA deleted 10.20.0.184[4500]-3.219.34.143[4500] spi=832e889007ff7c6fb9c6abea0d0ed9ab
2021-01-20T01:26:31.520715+00:00 GW-aws-us-east-1-transit2-agw-52.203.177.219 racoon: INFO: ISAKMP-SA expired 10.20.0.184[4500]-3.219.34.143[4500] spi=832e889007ff7c6fb9c6abea0d0ed9ab
2021-01-20T01:19:41.683639+00:00 GW-aws-us-east-1-transit2-agw-52.203.177.219 racoon: INFO: IPsec-SA established: ESP/Tunnel 10.20.0.184[4500]->3.219.34.143[4500] spi=1809508839(0x6bd9e9e7)
2021-01-20T01:19:41.683545+00:00 GW-aws-us-east-1-transit2-agw-52.203.177.219 racoon: INFO: IPsec-SA established: ESP/Tunnel 10.20.0.184[4500]->3.219.34.143[4500] spi=94876720(0x5a7b430)
2021-01-20T01:19:41.641426+00:00 GW-aws-us-east-1-transit2-agw-52.203.177.219 racoon: INFO: respond new phase 2 negotiation: 10.20.0.184[4500]<=>3.219.34.143[4500]
```

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:

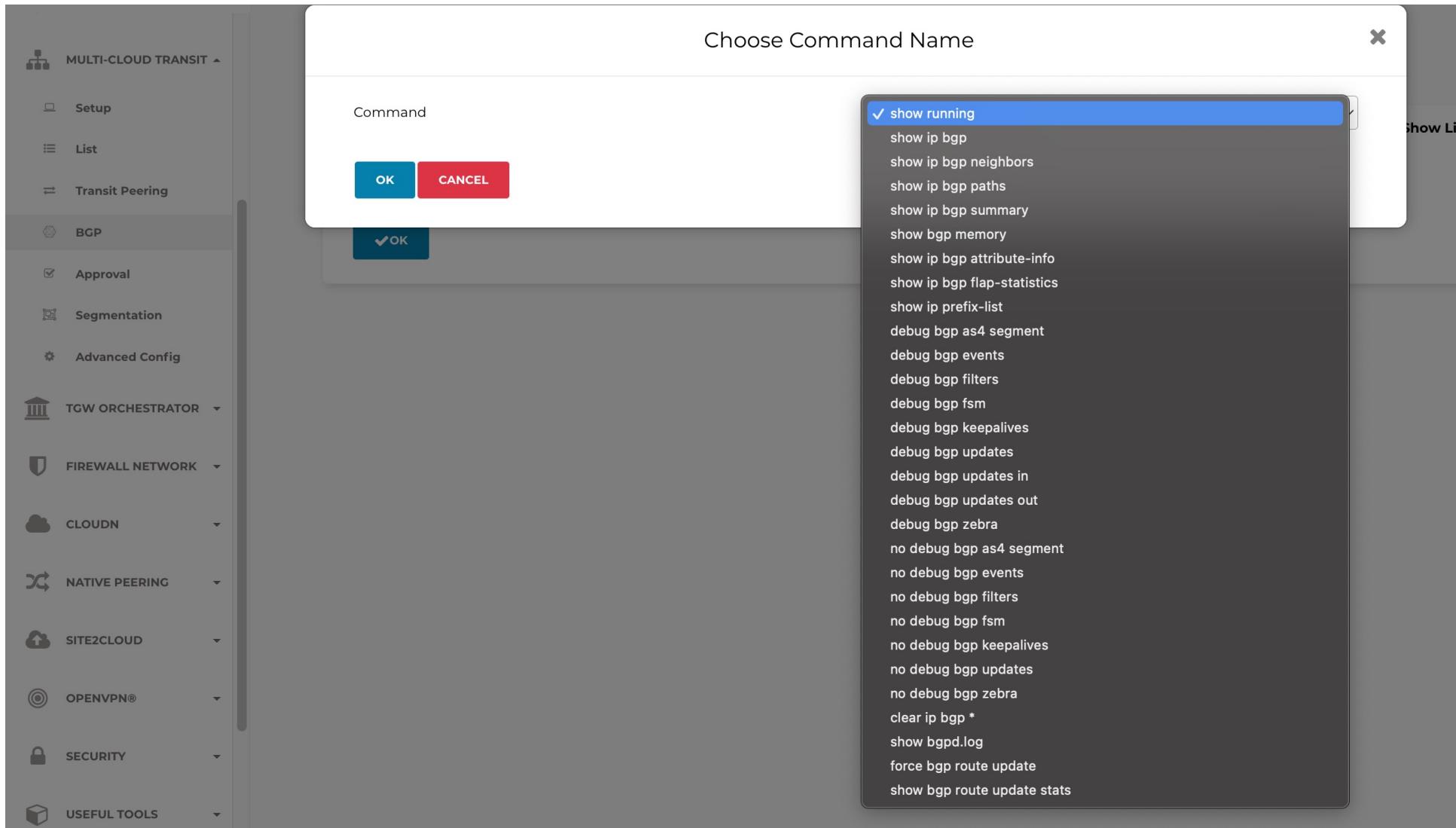
- This will restart all tunnels on this gateway
- Could impact your service till the tunnels come up

BGP Troubleshooting

- **PATH:** Controller > MULTI-CLOUD TRANSIT > BGP > Diagnostics

The screenshot shows the Aviatrix Controller web interface. The top navigation bar includes the Aviatrix logo, the word "CONTROLLER", and various status icons (ACE Inc, clock, bell, question mark, grid, and refresh). The left sidebar under "MULTI-CLOUD TRANSIT" has several sections: "Setup", "List", "Transit Peering", "BGP" (which is highlighted with a red box), "Approval", "Segmentation", and "Advanced Config". The main content area has tabs for "Connections", "Diagnostics" (which is selected and underlined), and "Configuration". A central panel titled "Gateway" shows "aws-us-east-1-transit1" in a dropdown menu and a blue "OK" button below it. To the right of the gateway panel are sections for "Command" (with an empty input field) and "Predefined Show List" (with a grid icon).

BGP Troubleshooting – List of commands



BGP Troubleshooting – show running

The screenshot shows the Aviatrix Cloud Transit interface. The left sidebar has sections for Multi-Cloud Transit, TGW Orchestrator, Firewall Network, CloudN, Native Peering, Site2Cloud, OpenVPN®, and Security. Under Multi-Cloud Transit, the BGP section is selected. The main area shows a Gateway named "aws-us-east-1-transit1". A command box contains "show running". The output is as follows:

```
✓OK  
show running  
Current configuration:  
!  
hostname ip-10-0-0-4  
password 8 JJQQV.4deGXbo  
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 10.0.10.0/24  
network 10.0.20.0/24  
network 10.100.10.0/24 route-map prepend-4470f60673c64a428a2754bbc718c7da  
network 172.16.10.0/24 route-map prepend-4470f60673c64a428a2754bbc718c7da  
network 192.168.10.0/24 route-map prepend-4470f60673c64a428a2754bbc718c7da  
network 192.168.20.0/24 route-map prepend-4470f60673c64a428a2754bbc718c7da  
neighbor 169.254.74.129 remote-as 65012  
neighbor 169.254.74.129 ebgp-multihop 255  
neighbor 169.254.74.129 soft-reconfiguration inbound  
neighbor 169.254.74.129 route-map ONPREM-DC out  
!
```

BGP Troubleshooting – show ip bgp

The screenshot shows the Aviatrix Cloud Control Platform interface. The left sidebar lists various network components: MULTI-CLOUD TRANSIT, TGW ORCHESTRATOR, FIREWALL NETWORK, CLOUDN, NATIVE PEERING, SITE2CLOUD, OPENVPN®, and SECURITY. The MULTI-CLOUD TRANSIT section is expanded, showing sub-options like Setup, List, Transit Peering, and BGP (which is selected). The main content area has tabs for Connections, Diagnostics (underlined), and Configuration. In the Diagnostics tab, there's a Gateway dropdown set to "aws-us-east-1-transit1", a Command input field containing "show ip bgp", and a Predefined Show List button. A large central window displays the output of the "show ip bgp" command:

```
✓OK  
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  
*> 10.0.0.0/24    169.254.74.129      0        0 65012 ?  
*> 10.0.10.0/24   0.0.0.0            0        32768 i  
*> 10.0.20.0/24   0.0.0.0            0        32768 i  
*> 10.0.111.0/24  169.254.74.129      0        0 65012 ?  
*> 10.0.211.0/24  169.254.74.129      0        0 65012 ?  
*> 10.100.10.0/24 0.0.0.0            0        32768 65011 i  
*> 169.254.74.128/30  
                  169.254.74.129      0        0 65012 ?  
*> 172.16.10.0/24 0.0.0.0            0        32768 65011 i  
*> 192.168.10.0   0.0.0.0            0        32768 65011 i  
*> 192.168.20.0   0.0.0.0            0        32768 65011 i  
  
Displayed 10 out of 10 total prefixes
```

A large, solid orange shape is positioned on the left side of the slide, curving from the top-left towards the center. It covers approximately one-third of the slide's width.

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



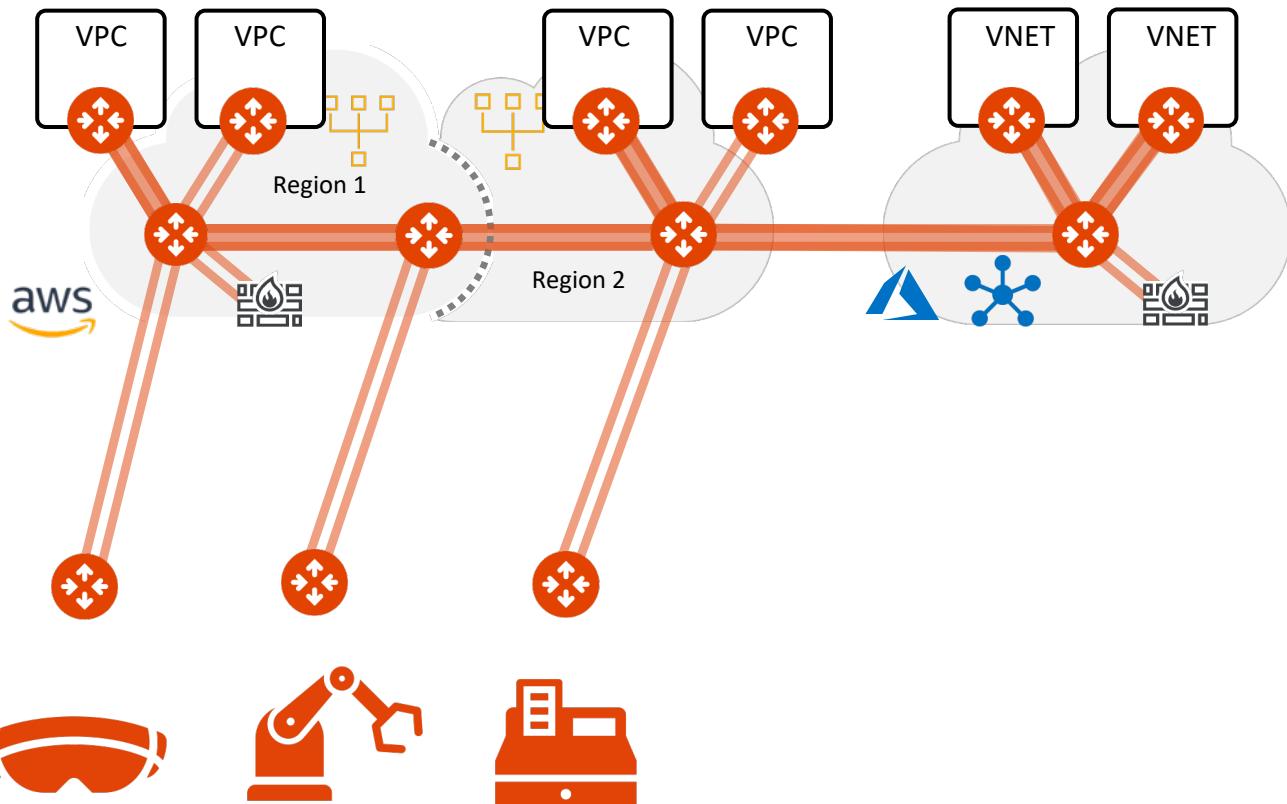
Simplified Edge Management



Consistent Secure Edge

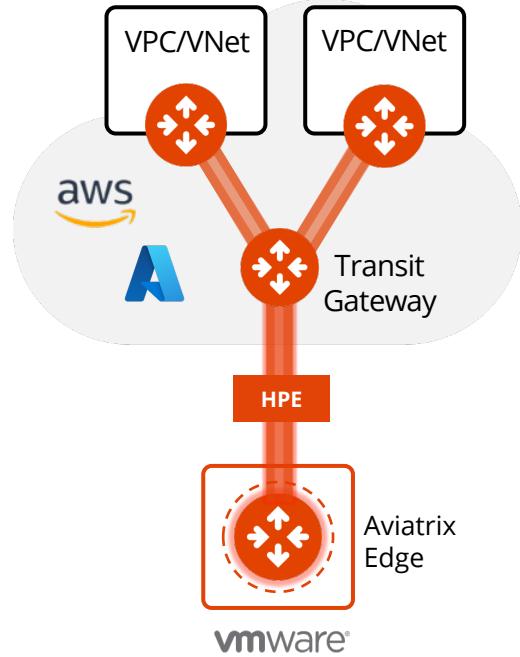


Simplified Edge On-boarding

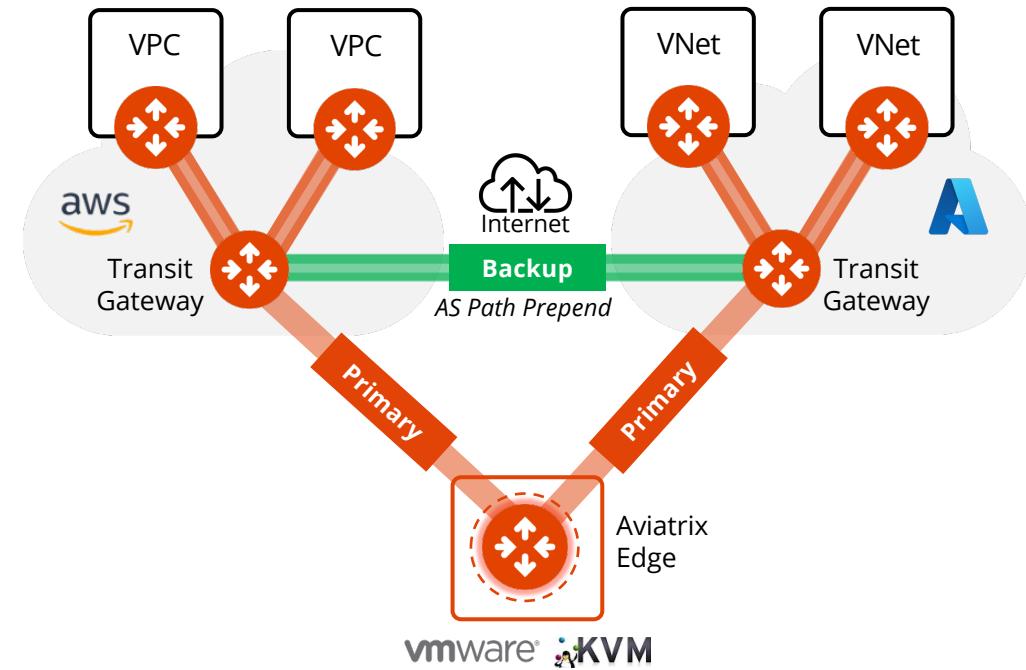


Aviatrix Edge Use Cases

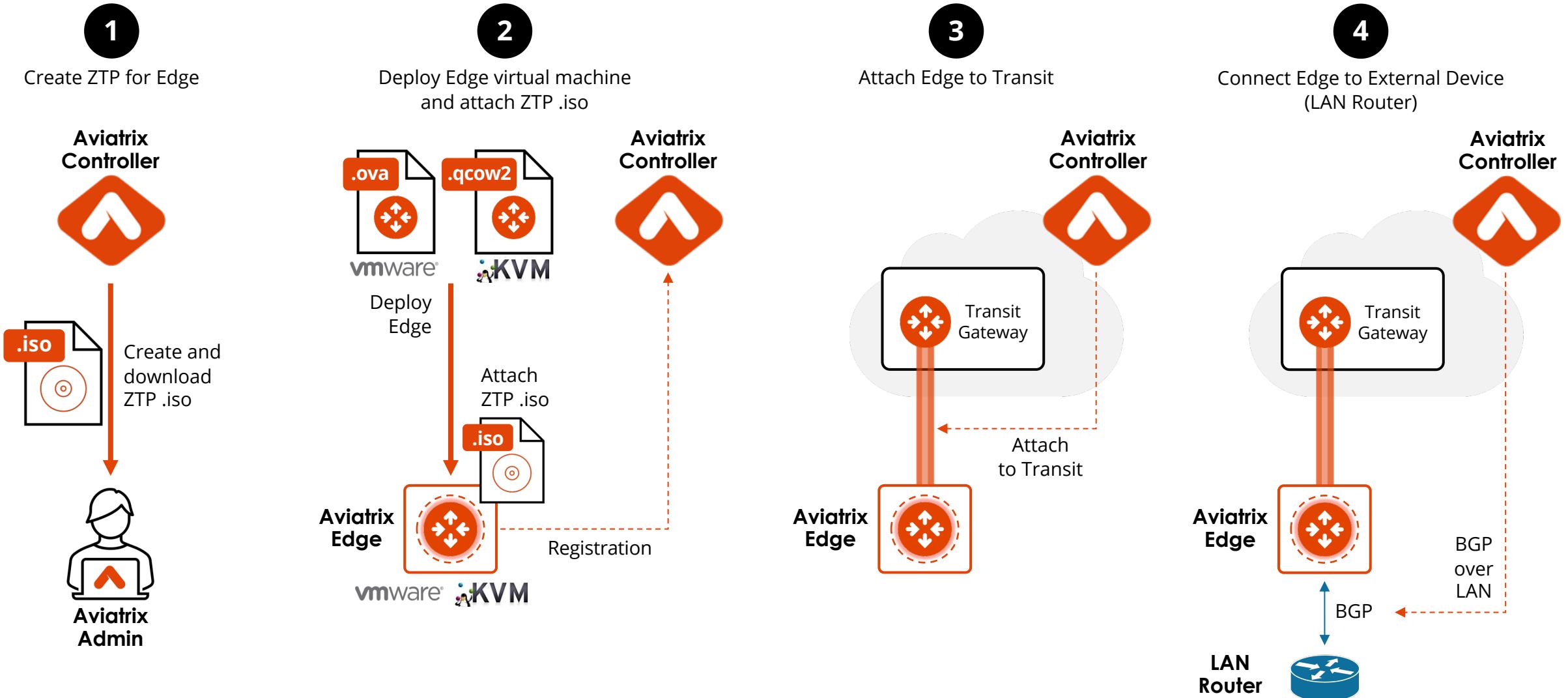
Extend the Aviatrix Platform to the Edge



Multi-Cloud Connectivity via Aviatrix Edge



Edge 2.0 Deployment Workflow - Demo

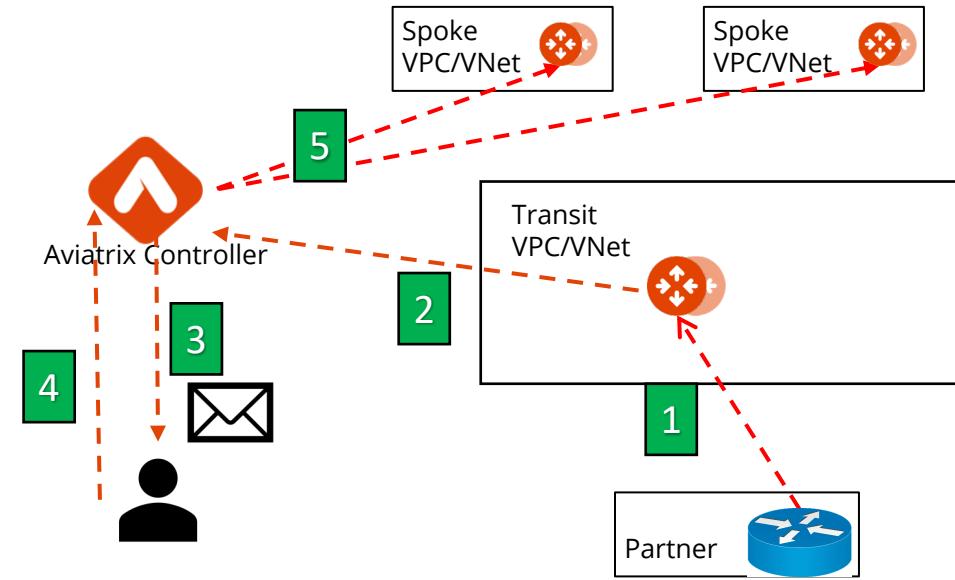


BGP Route Approval

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

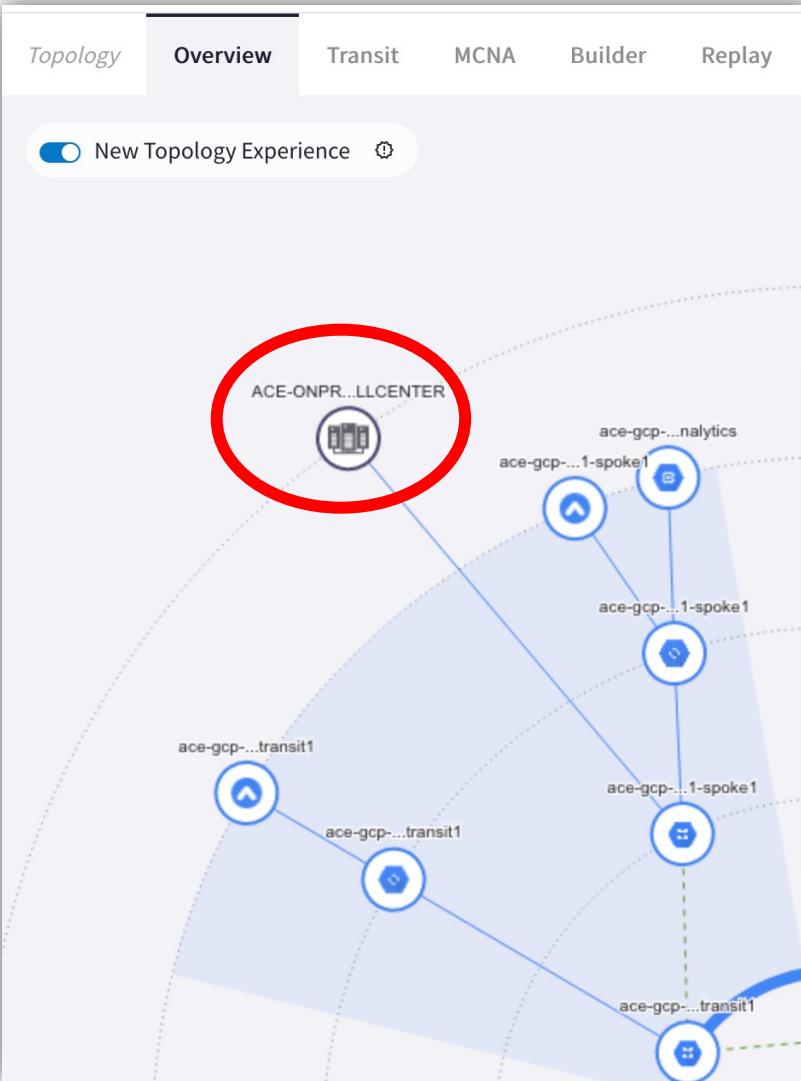
- **PATH:** Controller > MULTI-CLOUD TRANSIT > Approval > Config

The screenshot shows the Aviatrix BGP Route Approval configuration page. At the top right are 'Config' and 'List' buttons. The main section is titled 'Gateway Learned CIDR Approval' with an 'Info' link. It includes a 'Gateway' dropdown set to 'aws-us-east-1-transit1', a 'Mode' radio button group where 'Gateway' is selected, and a 'Learned CIDRs Approval' dropdown set to 'Enabled'. Below this is a 'Gateway Learned CIDR Lists' section with two tables: 'Pending Learned CIDRs' (containing one entry: '10.120.96.0/20 ~ ONPREM-DC') and 'Approved CIDRs' (containing two entries: '10.0.111.0/24' and '10.0.211.0/24'). Between the tables are four buttons: 'APPROVE ALL' (blue), 'APPROVE' (light blue), 'REMOVE' (red), and 'REMOVE ALL' (dark red). At the bottom are 'Manually Input Approved CIDRs' input fields containing '10.188.0.0/16, 10.100.0.0/16' and an 'ADD' button, along with an 'UPDATE' button.

Site2Cloud & CoPilot

Site2Cloud Visibility via CoPilot

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



Cloud Routes

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

GATEWAY ROUTES VPC/VNET ROUTES SITE 2 CLOUD **BGP INFO**

Search C

GATEWAY NAME	VPC/VNET ID	BGP MODE	HA STATE	LOCAL ASN	BGP MAP	LEARNED ROUTES	ADVERTISED ROUTES	STATUS
AWS-Transit	vpc-0ba7a2aa9c948df65~~Trans...	enabled	activemesh	65010	SHOW	SHOW	SHOW	●

BGP Details

REMOTE ASN	NEIGHBOR IP	LOCAL IP	CONNECTION NAME	NEIGHBOR STATUS
64555	169.254.170.173	169.254.170.174	s2c(169.254.170.173)	established
65000	169.254.8.1	169.254.8.2	s2c-onprem(169.254.8.1)	established
65000	169.254.10.1	169.254.10.2	s2c-onprem(169.254.10.1)	not established

BGP MAP

The BGP Map displays the network topology. At the center is the AWS-Transit gateway (65010). It has two green connections labeled 's2c' to on-premises routers with IP addresses 169.254.94.61 and 169.254.170.173, both with ASN 64555. It also has two red connections labeled 's2c-onprem' to on-premises routers with IP addresses 169.254.8.1 and 169.254.10.1, both with ASN 65000.

LEARNED CIDR

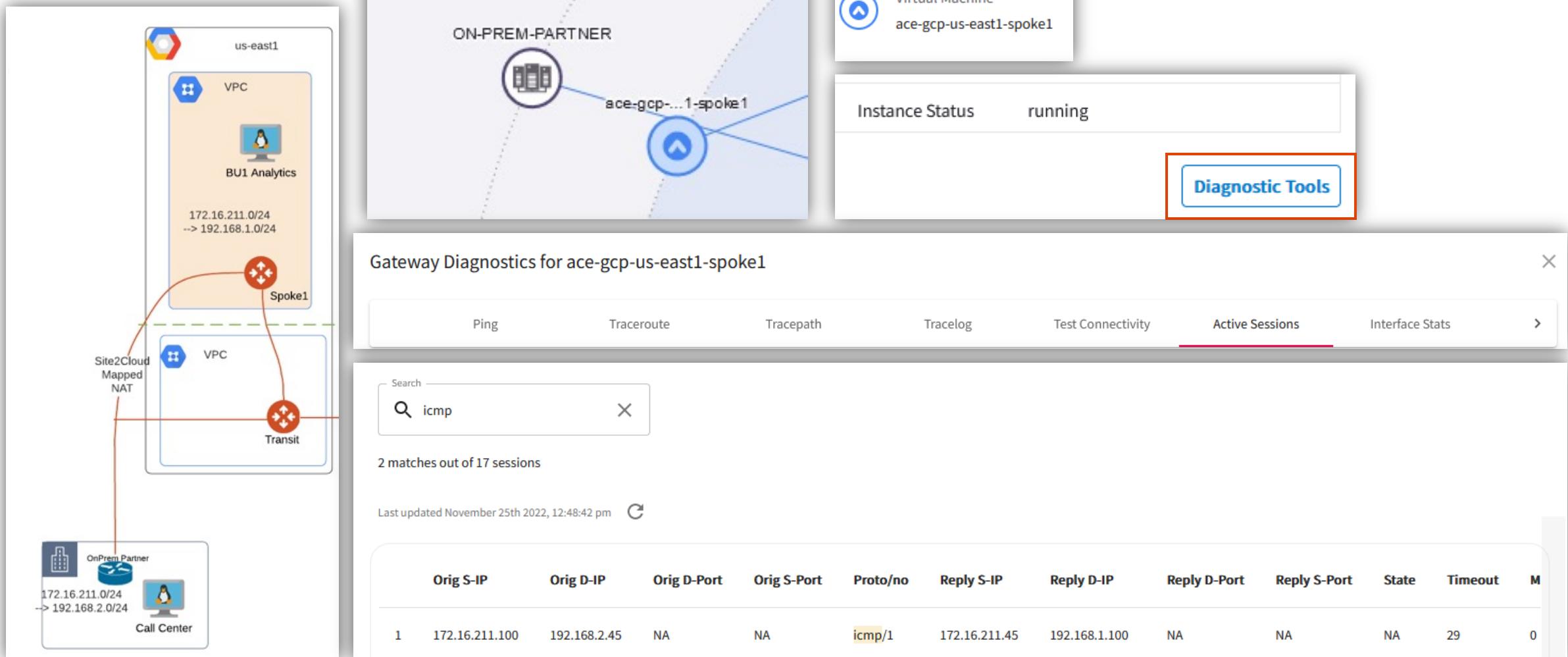
Networks
10.230.0.0/16
10.240.0.0/24

ADVERTISED CIDR

Networks
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 6 Site2Cloud