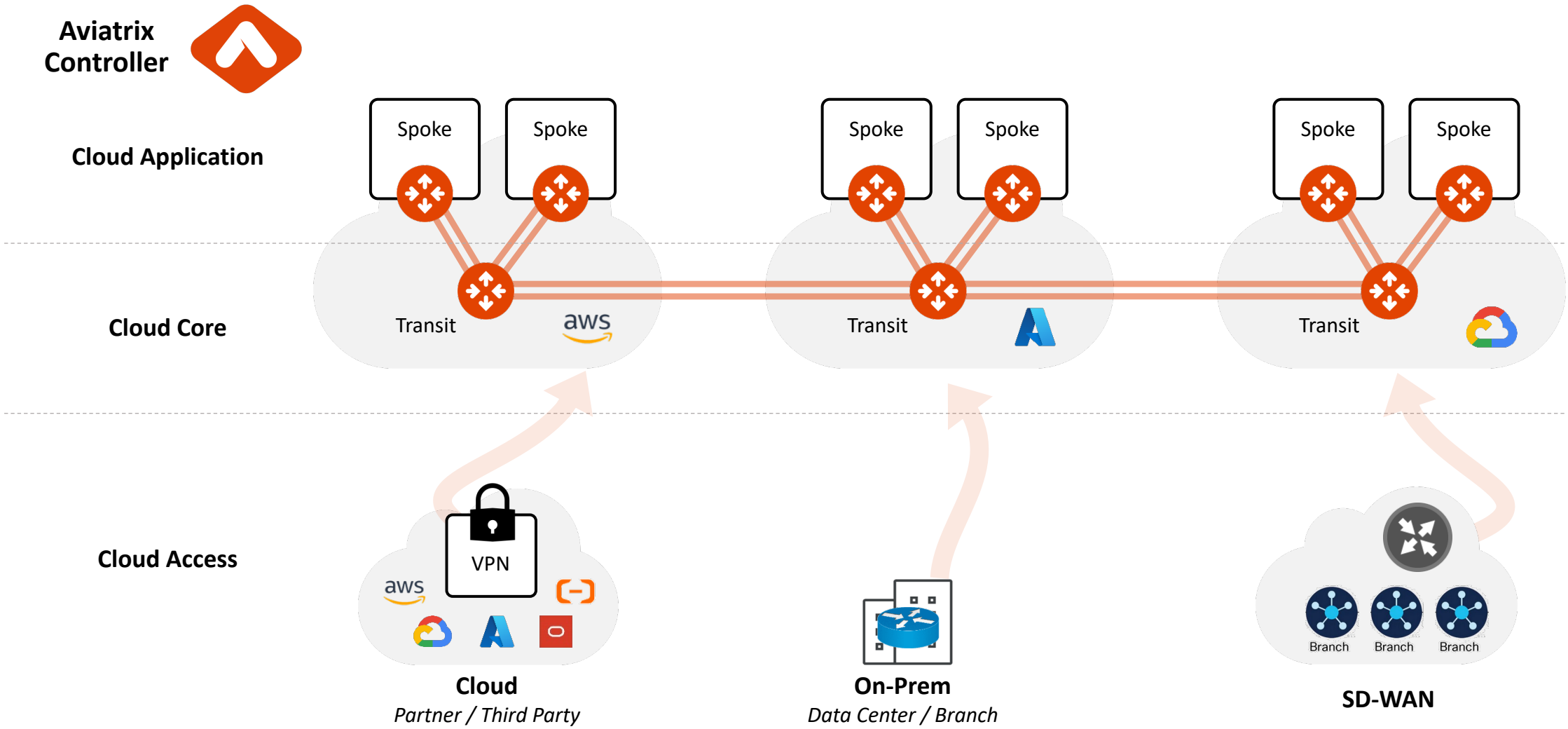
aviatrix

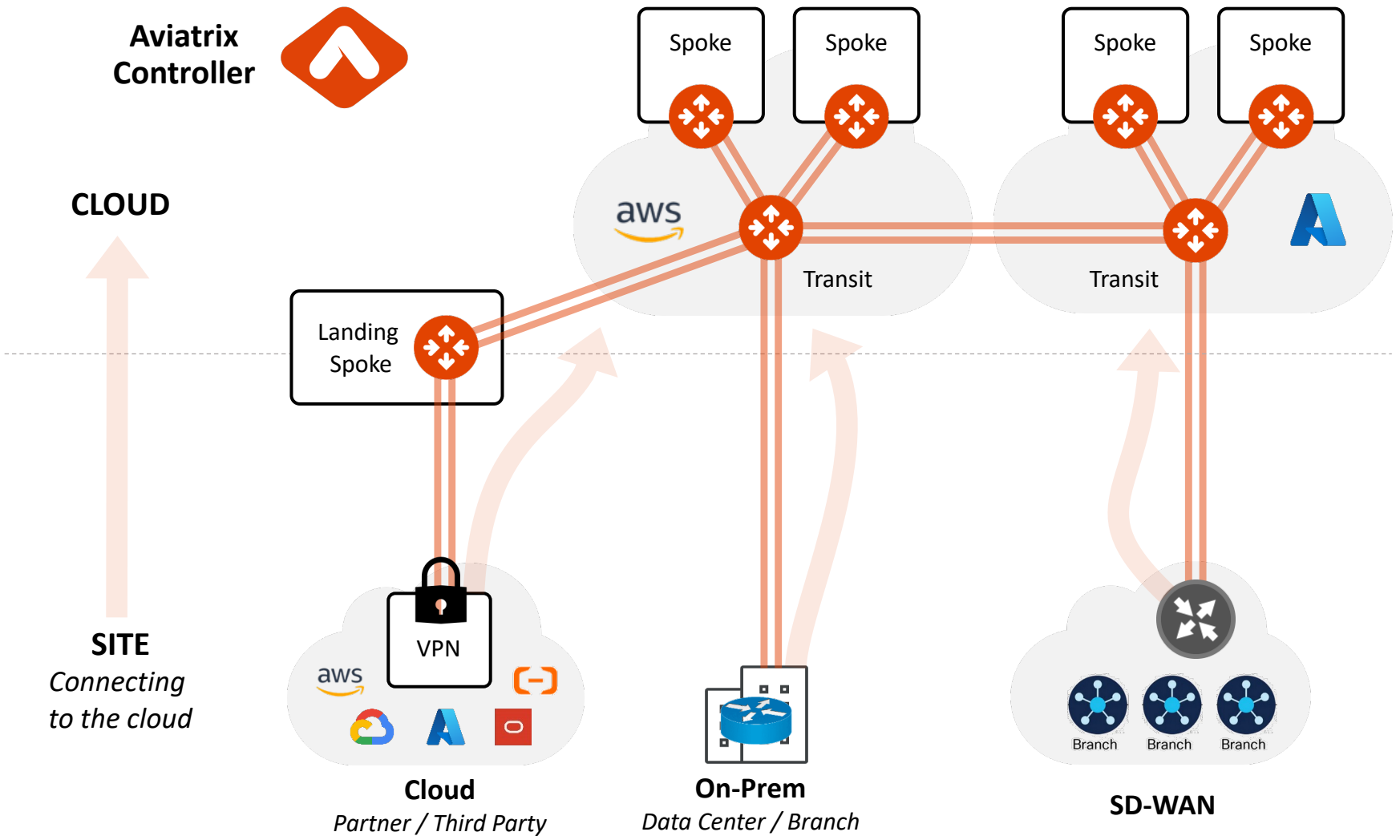
Site2Cloud

Aviatrix Multicloud Network Architecture



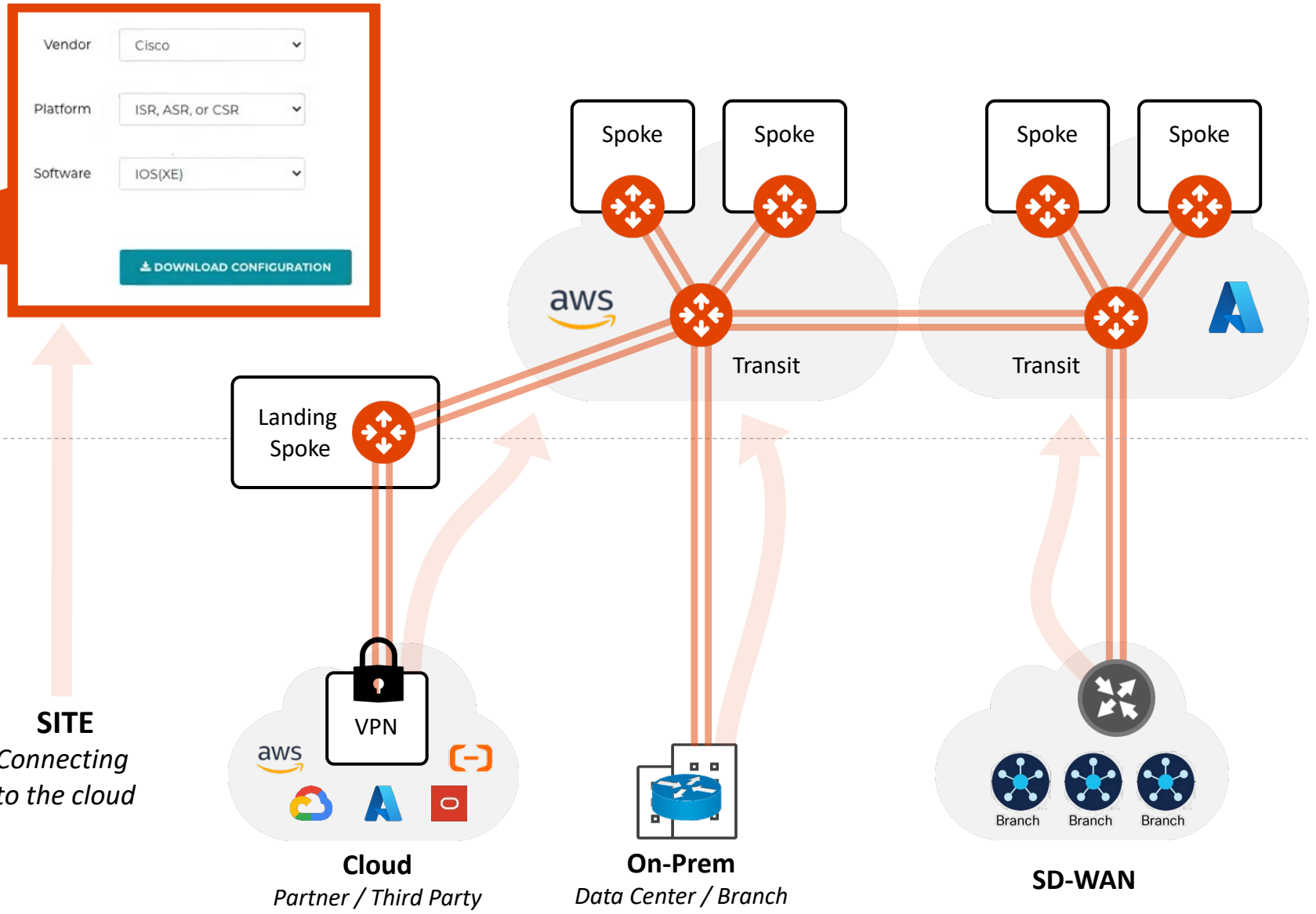
Site2Cloud Introduction

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



Site2Cloud Solution

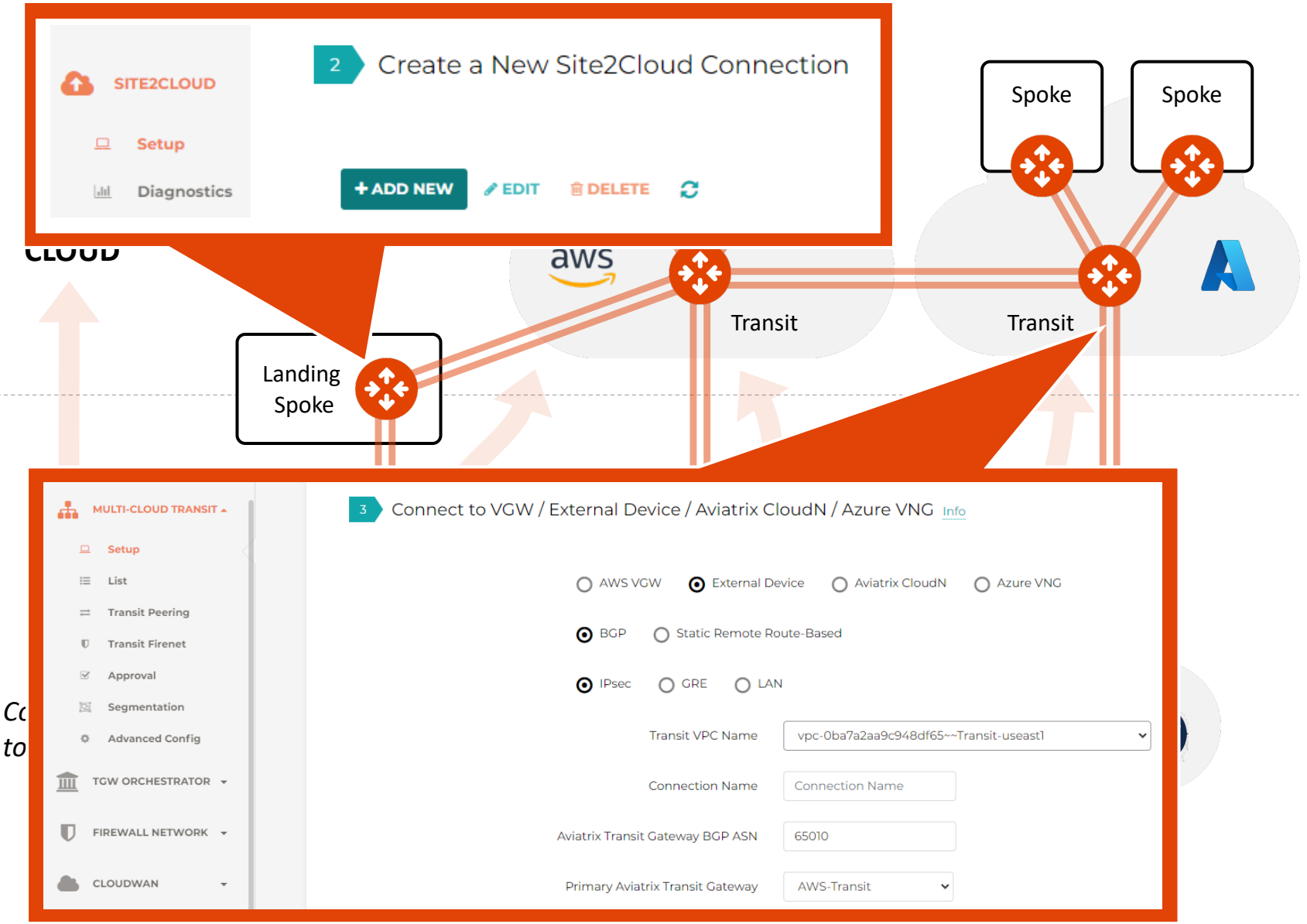
- Easy to use and template driven
- Built-in diagnostic tools
- Solves Overlapping IPs Challenges



aviatrix

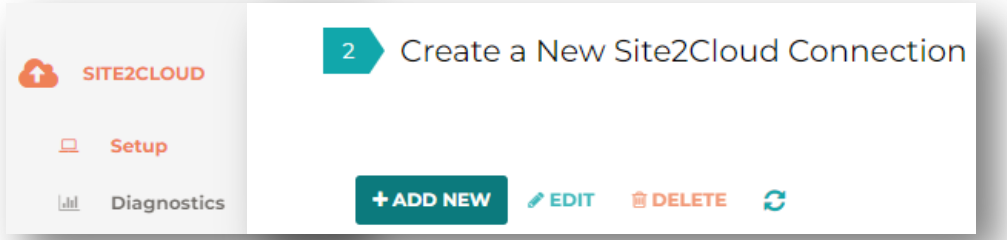
Site2Cloud Landing Options

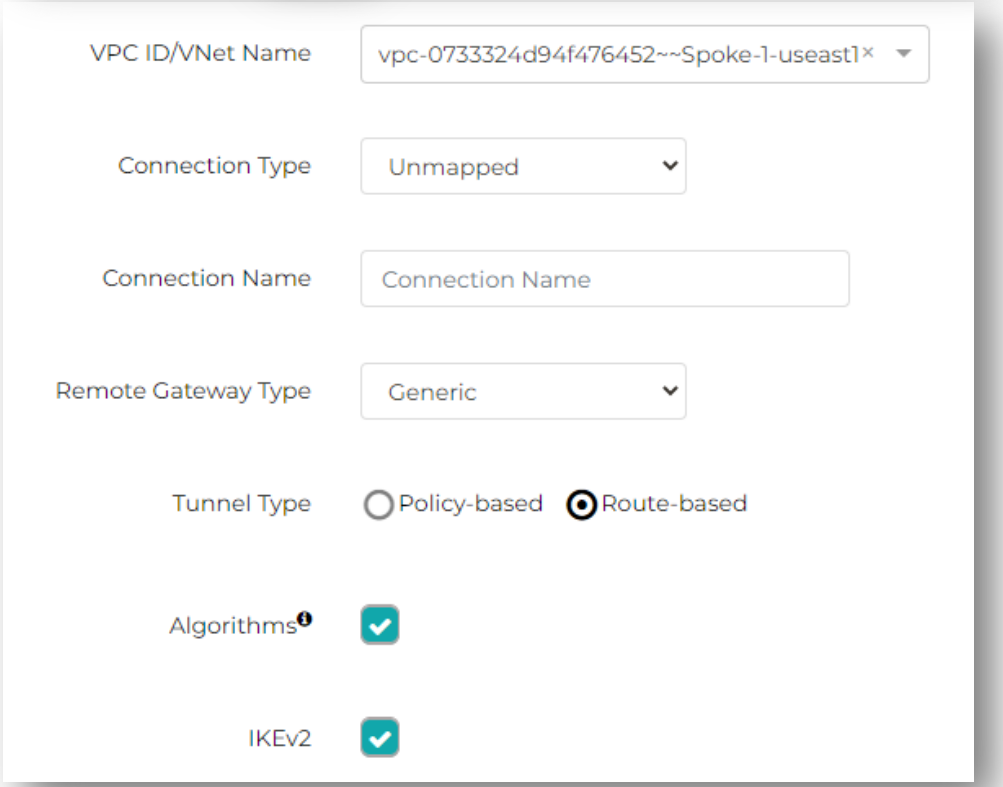
- Landing on Transit
  - Extend Core
  - SD-WAN
- Landing on Spoke
  - Scale
  - Partners
  - Complex Overlapping IP

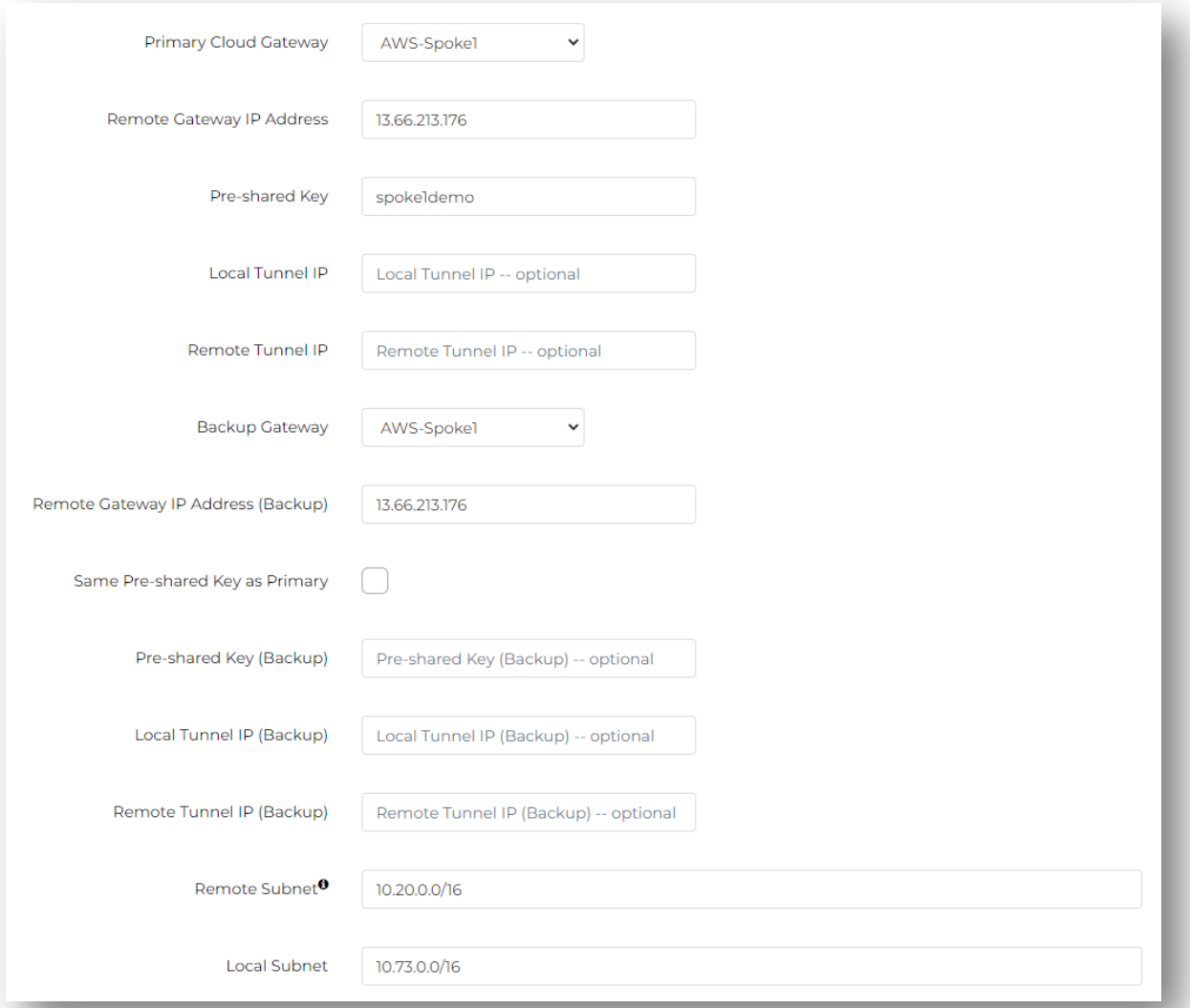


aviatrix

Site2Cloud – Spoke GWs



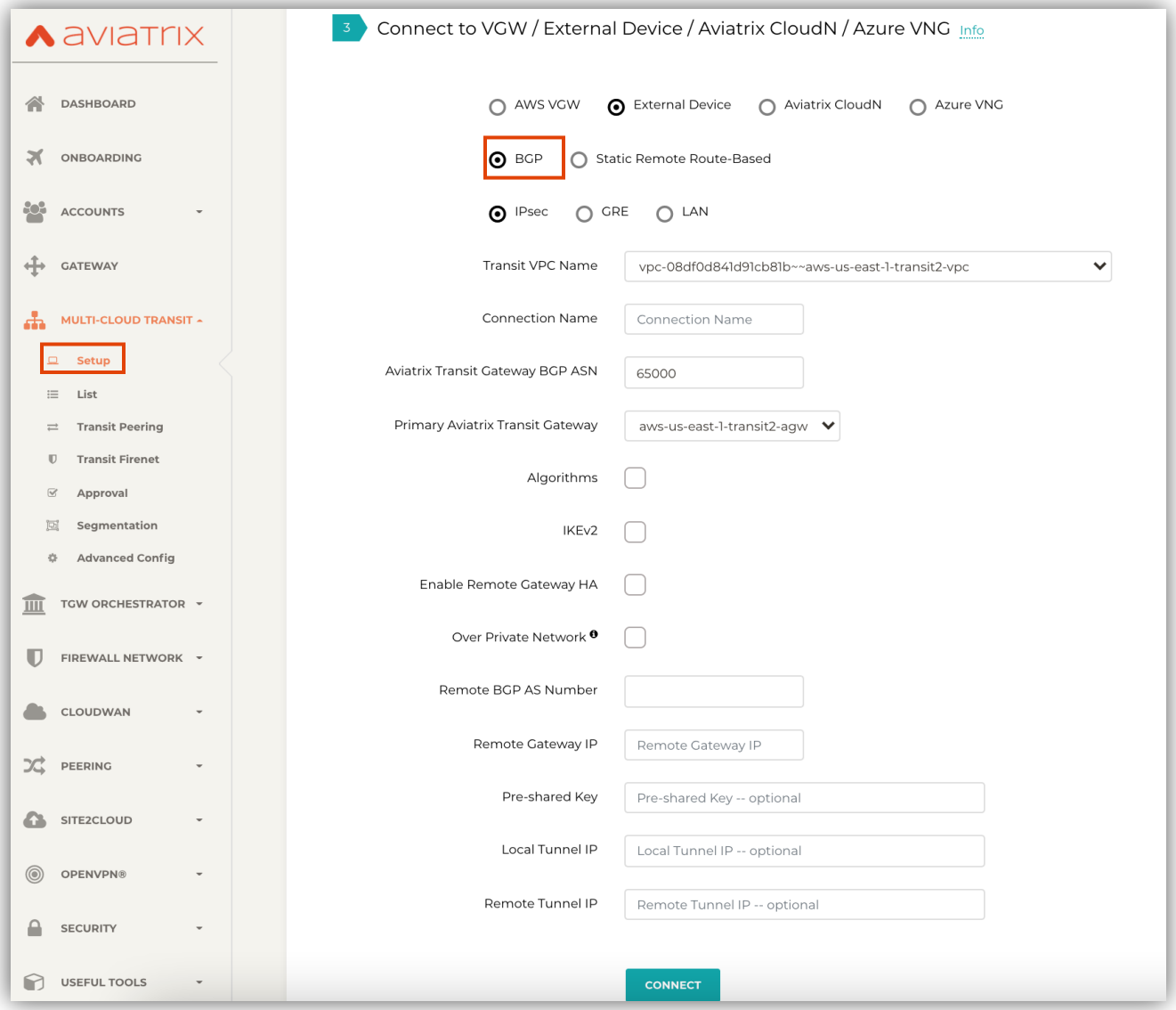




Site2Cloud – Transit Gateways

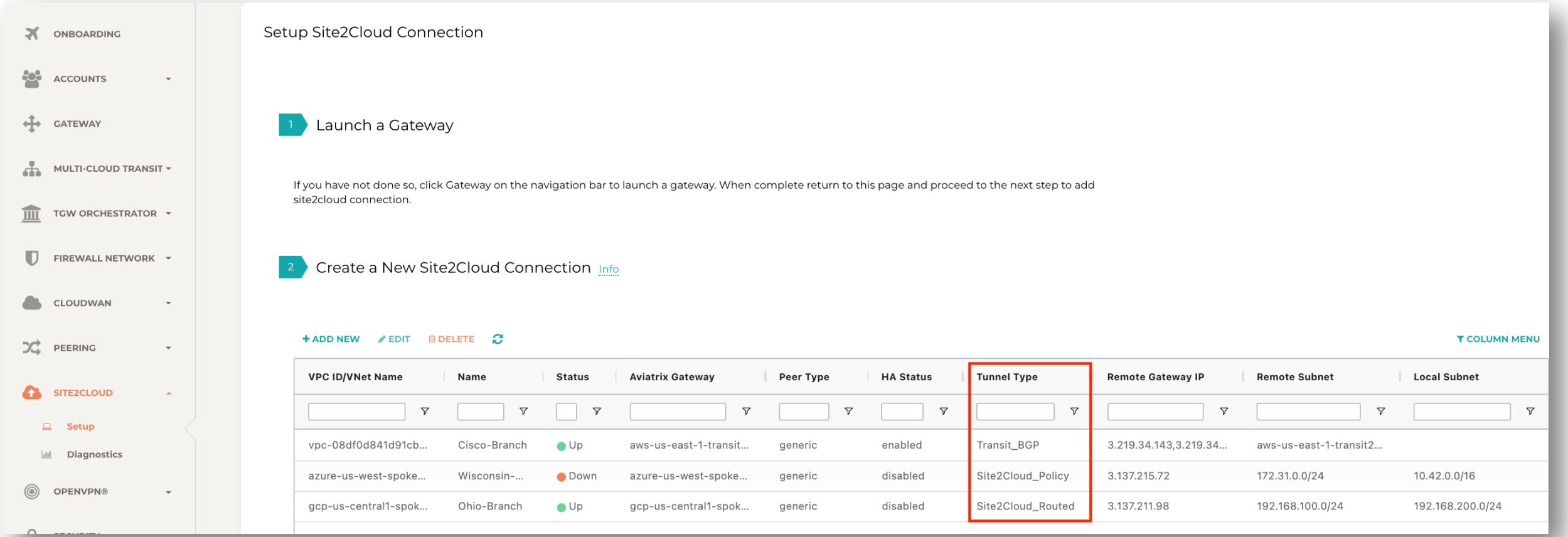
- Site2Cloud tunnels can also be built using the Aviatrix **Multi-Cloud Transit Setup** workflow

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



Site2Cloud Connection Types

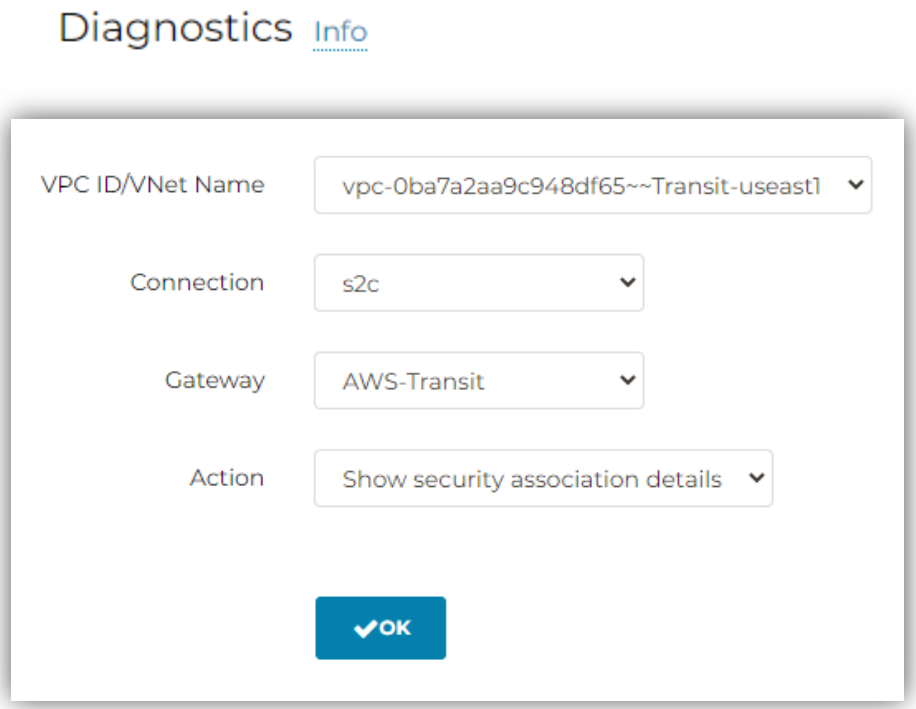
Verification



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



Monitoring – SPI

Cisco IOS Output

```
CiscoRouter#sh crypto ipsec sa interface tu1


interface: Tunnel1
    Crypto map tag: Tunnel1-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: Tunnel1-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: Tunnel1-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  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
```

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:

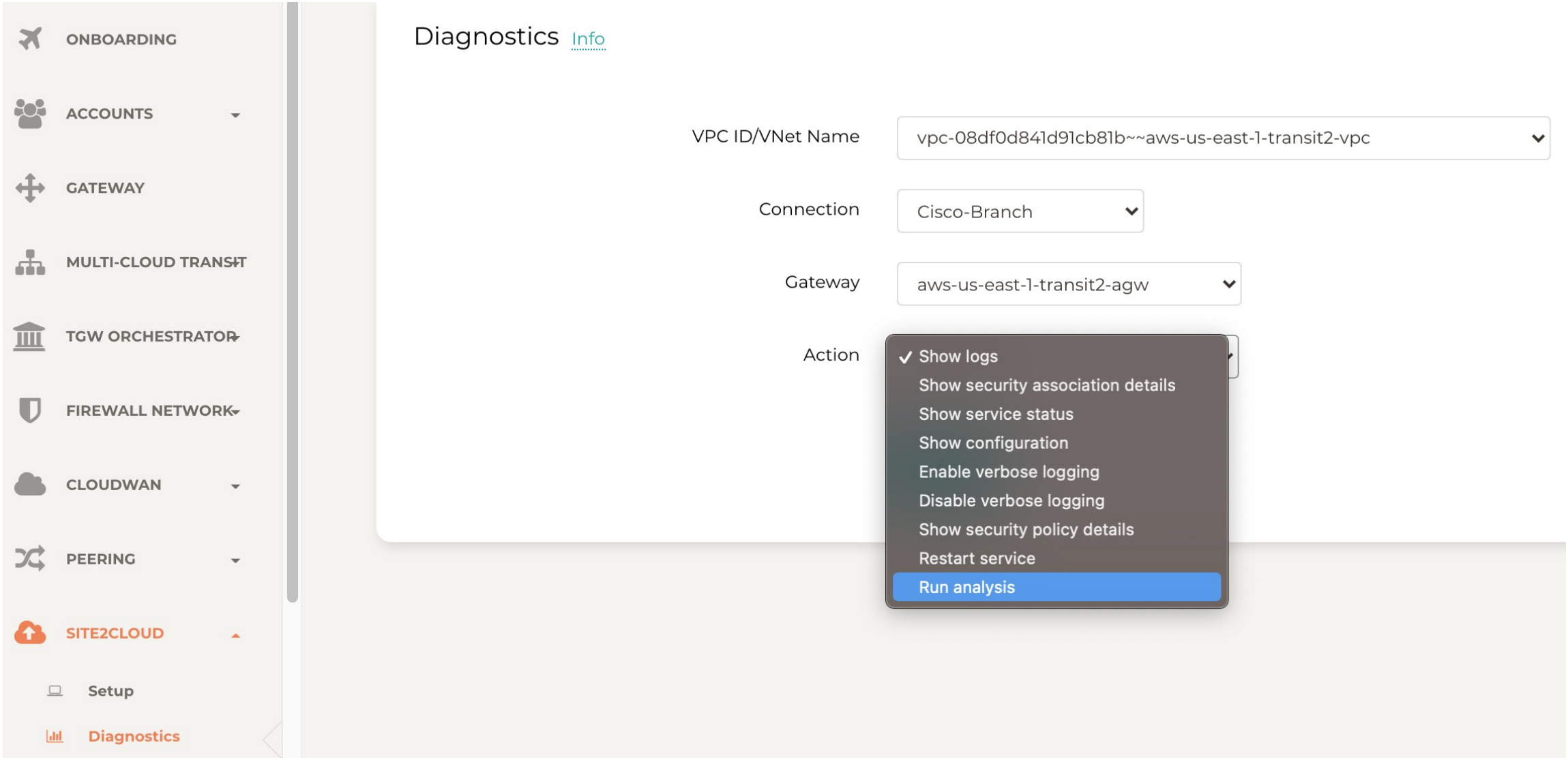
1. **Confirm Layer 3 connectivity**
   - Public IP reachable? Is there an ISP (BGP) issue?
   - If ping is disabled, check packet capture on remote public IP for ISAKMP packets
2. **Confirm SG/NSG allowed for outbound**
   - UDP 500 (ISAKMP)
   - UDP 4500 (ESP, which is encrypted traffic)
3. **Confirm 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



Diagnostics – Run analysis

Diagnostics Info

VPC ID/VNet Name: vpc-08df0d841d91cb81b~~aws-us-east-1-transit2-vpc

Connection: Cisco-Branch

Gateway: aws-us-east-1-transit2-agw

Action: Run analysis

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
500	udp	0.0.0.0/0
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: vpc-08df0d841d91cb81b~~aws-us-east-1-transit2-vpc

Connection: Cisco-Branch

Gateway: aws-us-east-1-transit2-agw

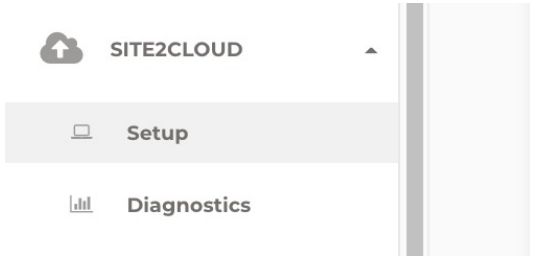
Action: Show logs

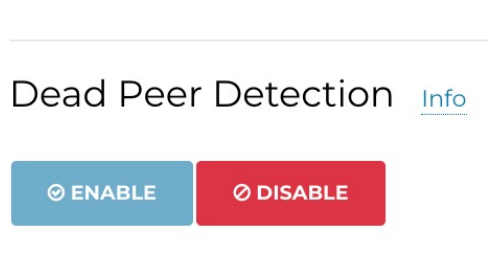
OK

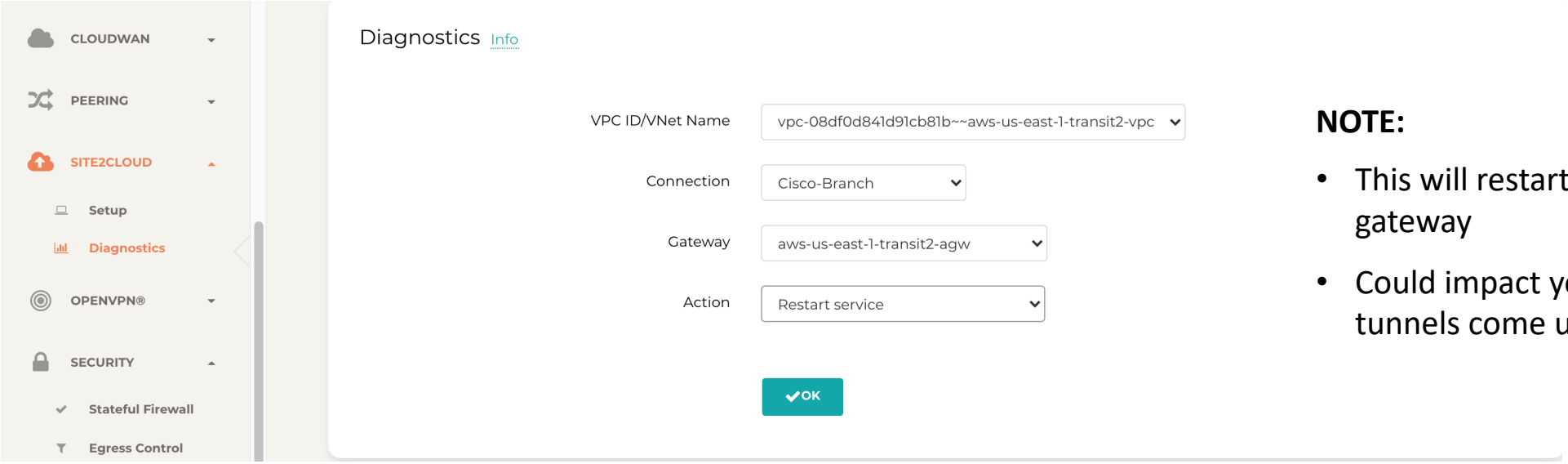
```
2021-01-20T03:26:46.605451+00:00 GW-aws-us-east-1-transit2-agw-52.203.177.219 racoon: INFO: KA remove: 10.20.0.184[4500]->3.219.34.143[4500]
2021-01-20T03:26:46.605408+00:00 GW-aws-us-east-1-transit2-agw-52.203.177.219 racoon: INFO: ISAKMP-SA deleted 10.20.0.184[4500]-3.219.34.143[4500] spi:832e88904855e6bf:37953dd95fcd745f
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:37953dd95fcd745f
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(0x3604fbc)
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(0x2fc9759d)
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(0x2fc9759d)
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(0x6bdae9e7)
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:832e889007ff7c6f:b9c6abea0d0ed9ab
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:832e889007ff7c6f:b9c6abea0d0ed9ab
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(0x6bdae9e7)
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





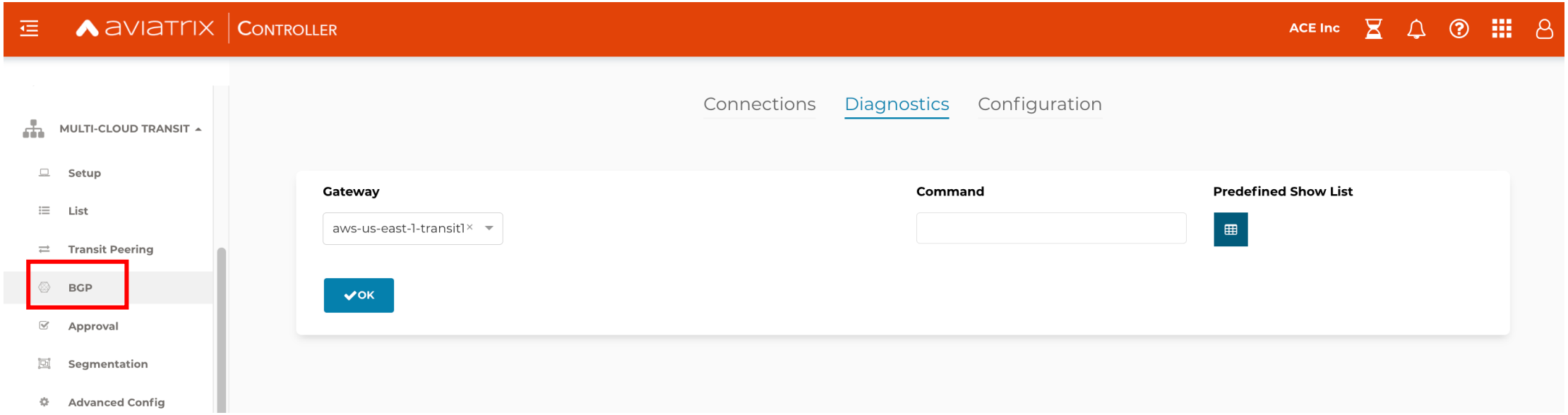


NOTE:

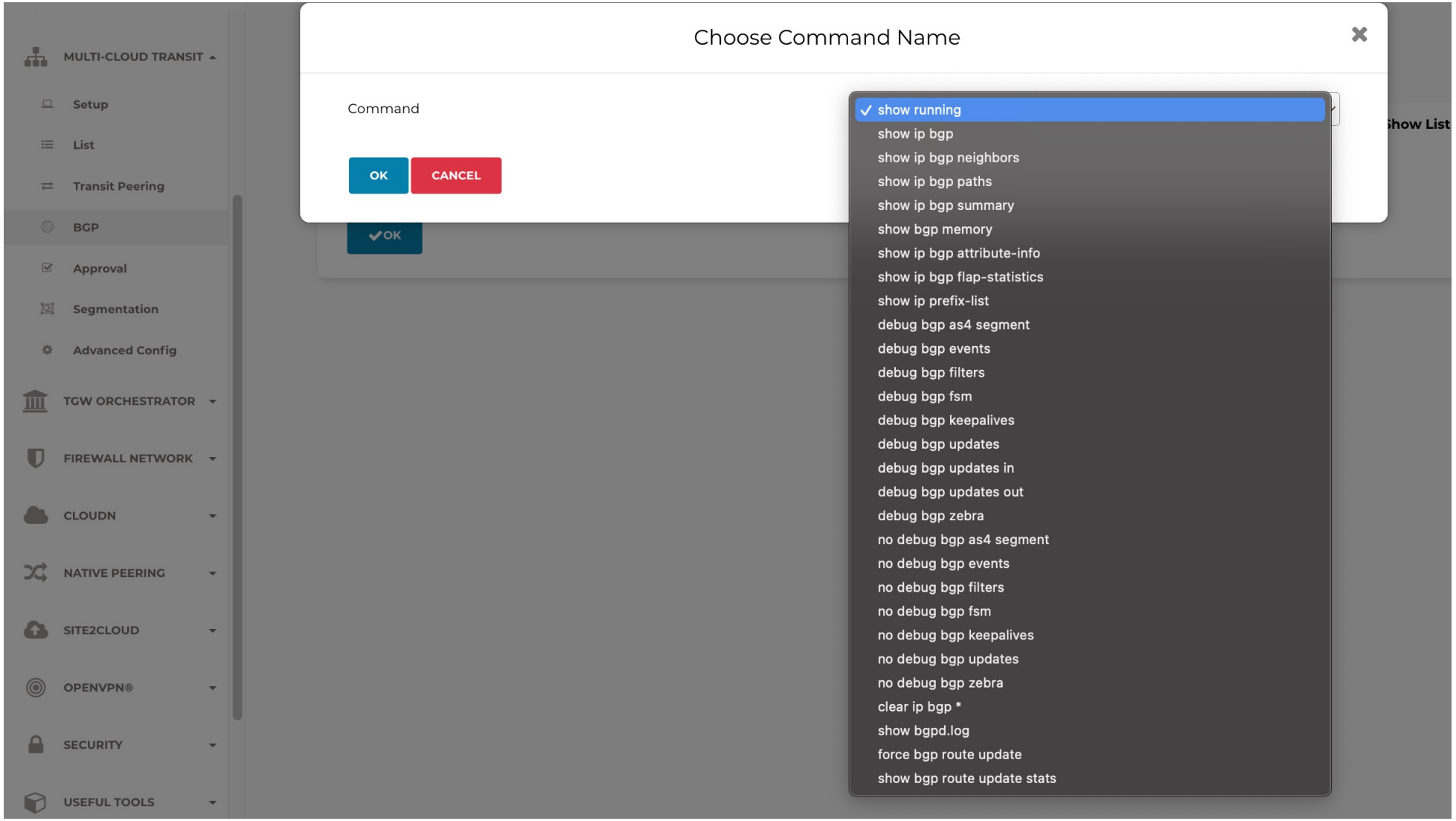
- This will restart all tunnels on this gateway
- Could impact your service till the tunnels come up

BGP Troubleshooting

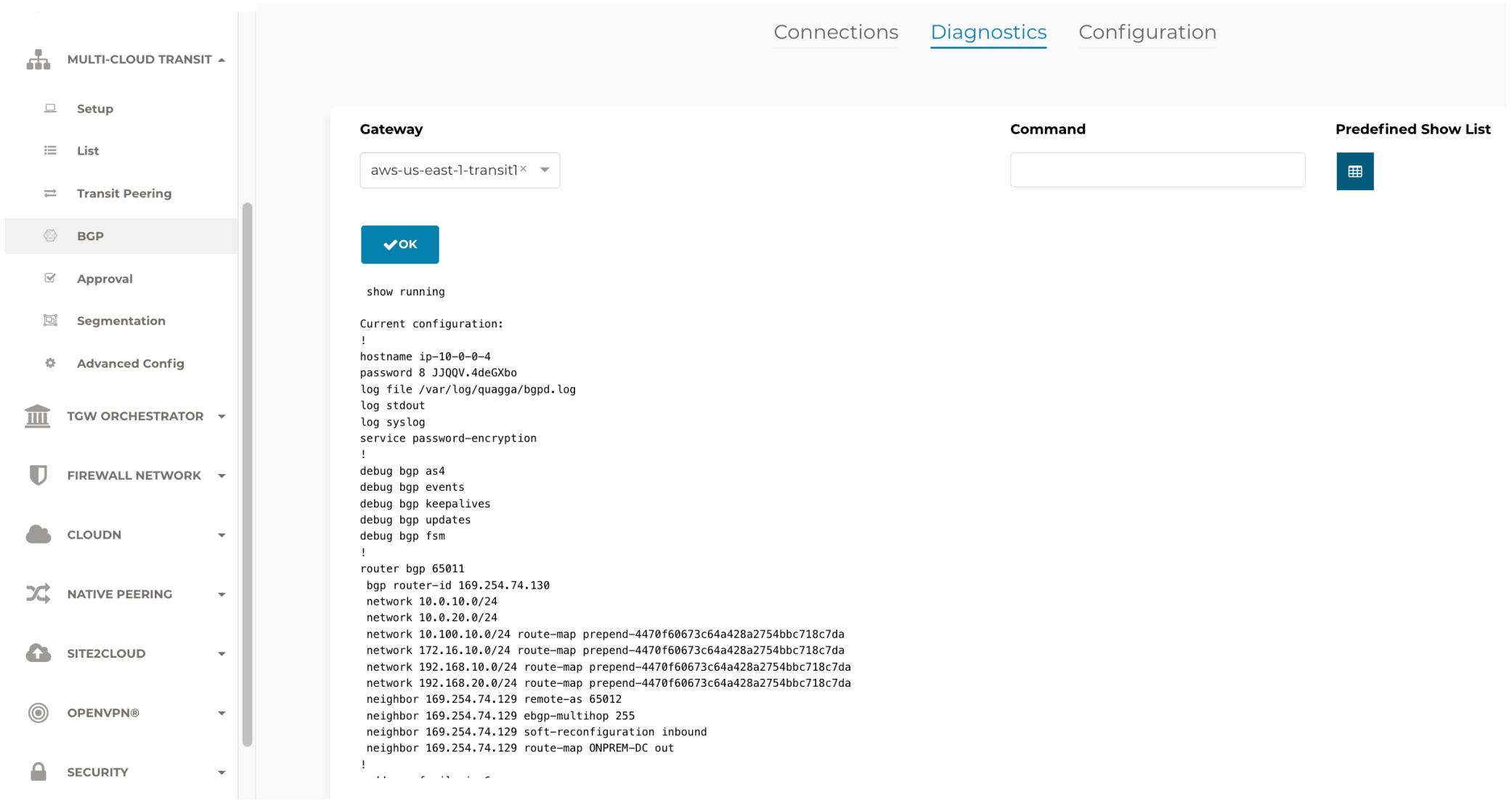
- **PATH:** Controller > MULTI-CLOUD TRANSIT > BGP > Diagnostics



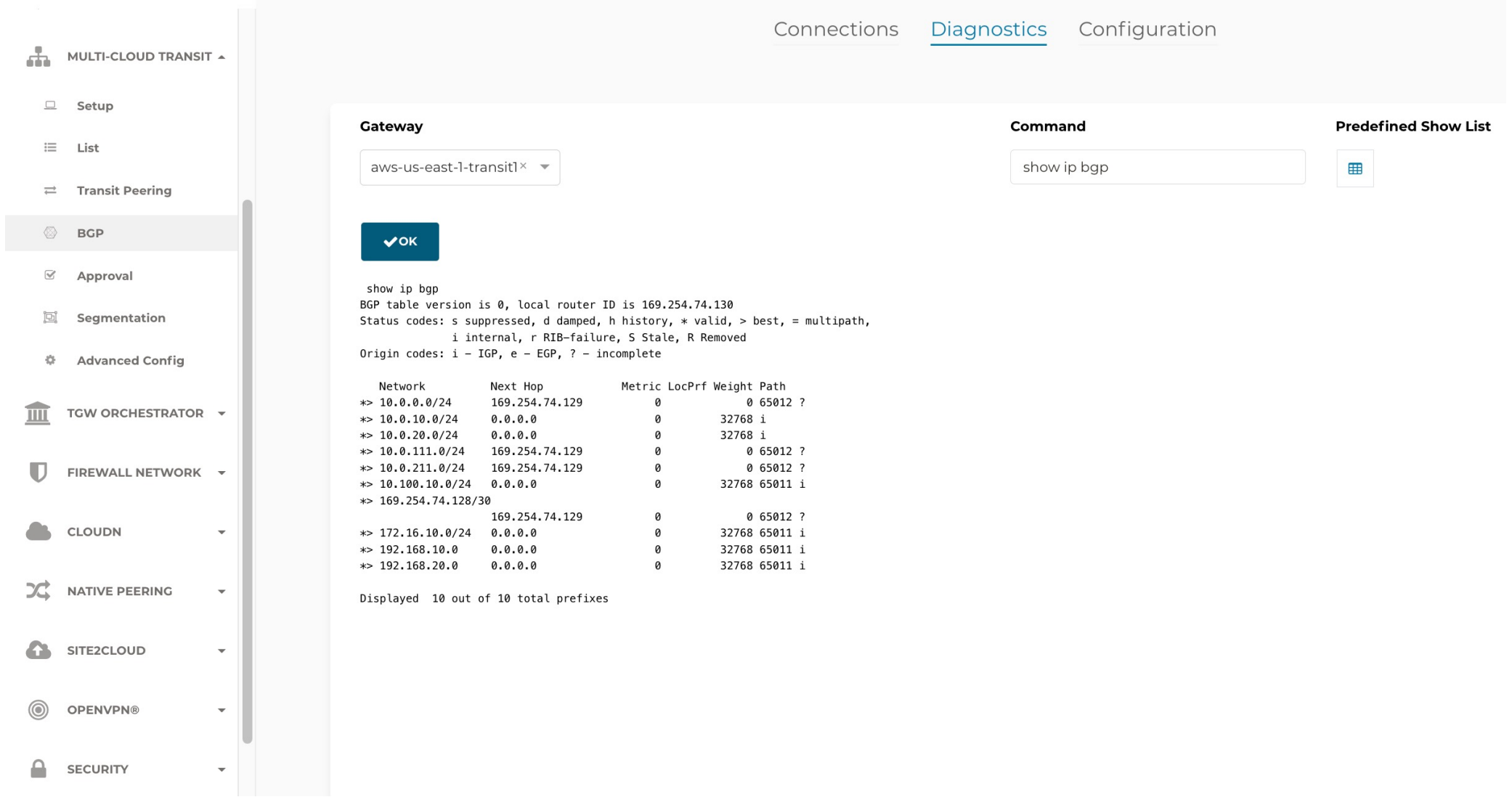
BGP Troubleshooting – List of commands



BGP Troubleshooting – show running



BGP Troubleshooting – show ip bgp



Edge

Introducing Aviatrix Edge

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

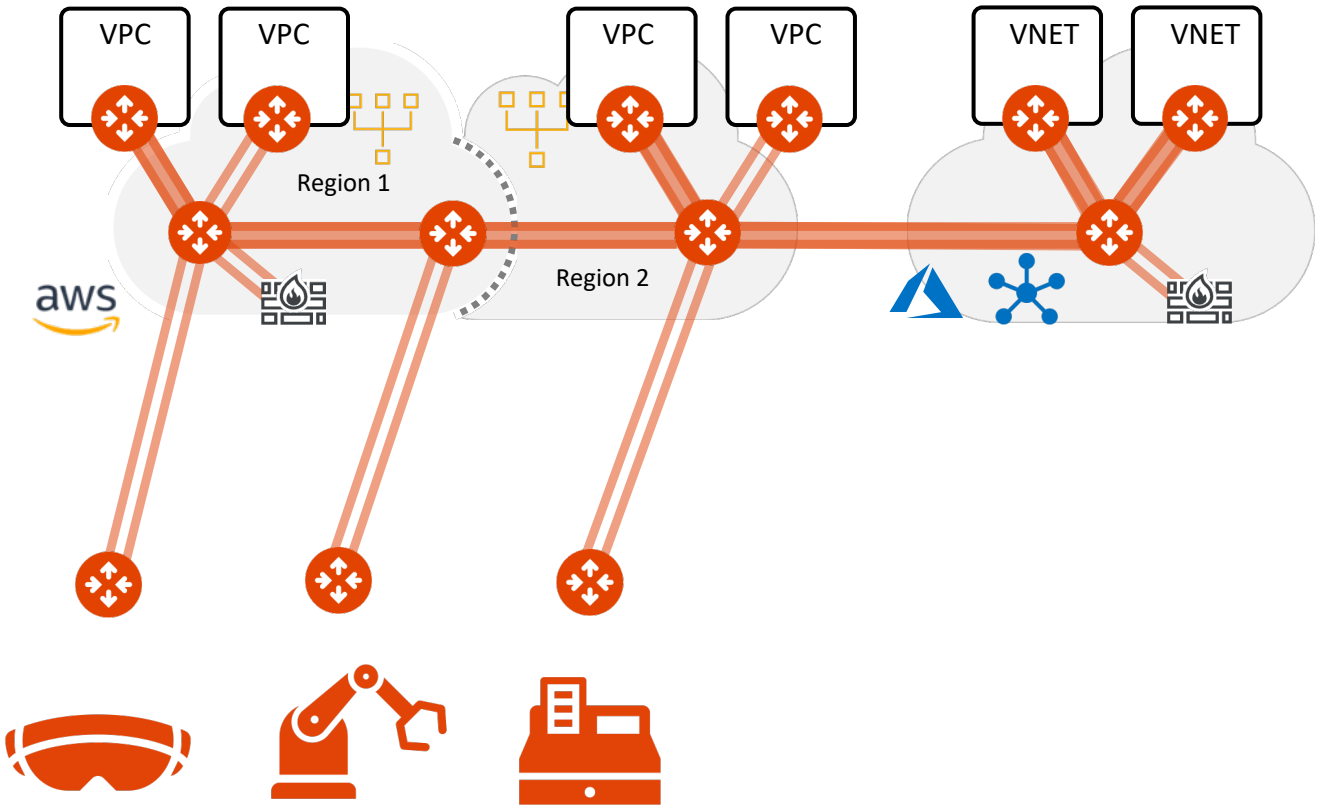
Aviatrix software in multiple form factors providing consistent network, security, and visibility to the edge.
Edge locations appear and behave as another VPC/VNET with spoke and transit capabilities.

Cloud Out Architecture

Simplified Edge Management

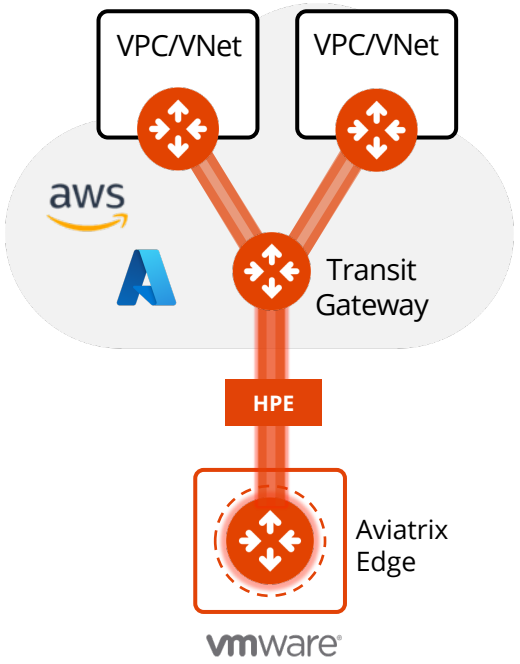
Consistent Secure Edge

Simplified Edge On-boarding

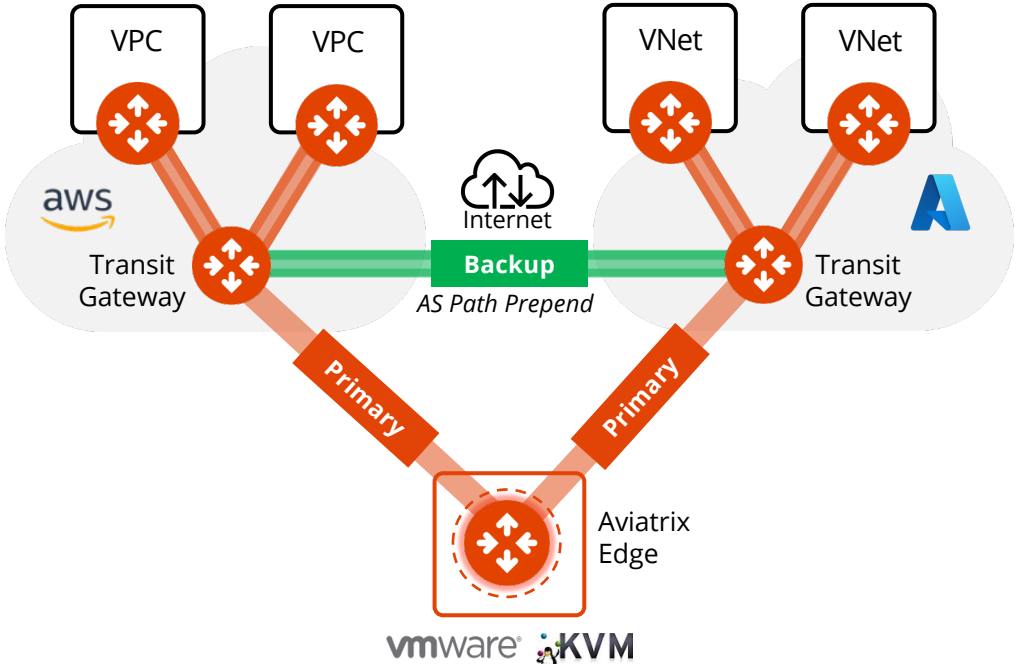


Aviatrix Edge Use Cases

Extend the Aviatrix Platform to the Edge

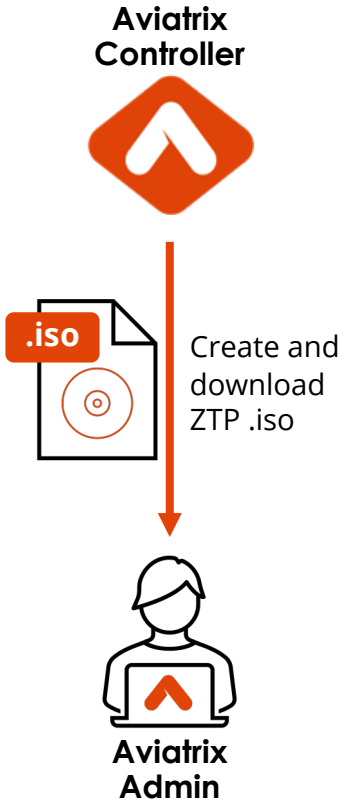


Multi-Cloud Connectivity via Aviatrix Edge

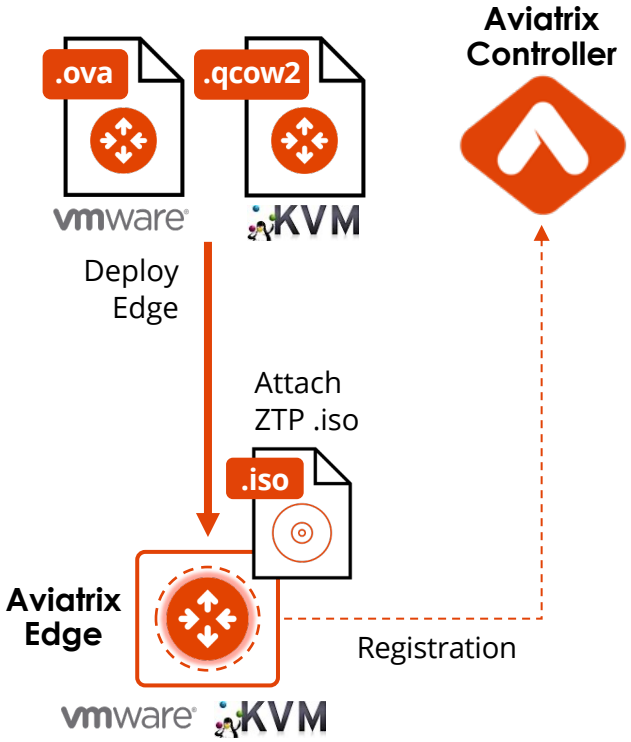


Edge 2.0 Deployment Workflow - Demo

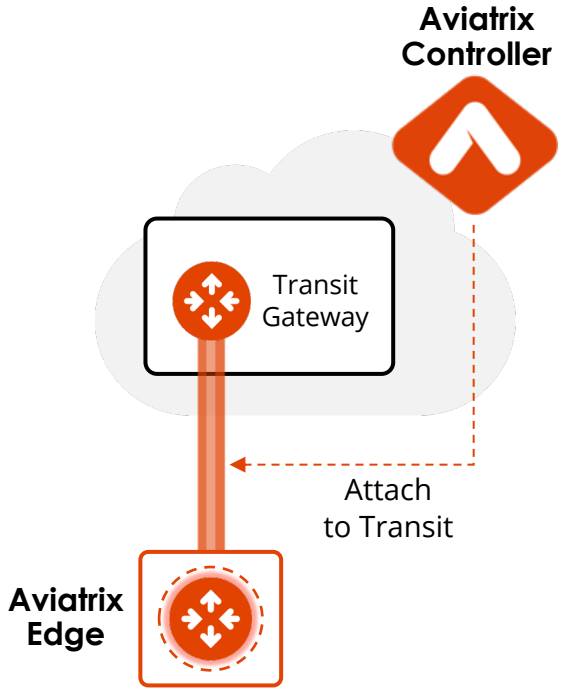
1 Create ZTP for Edge



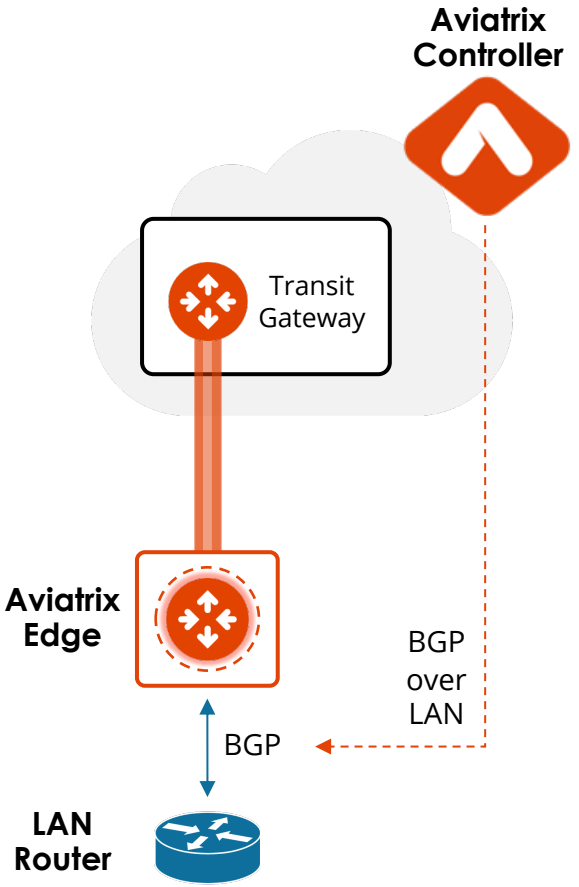
2 Deploy Edge virtual machine and attach ZTP .iso



3 Attach Edge to Transit



4 Connect Edge to External Device (LAN Router)

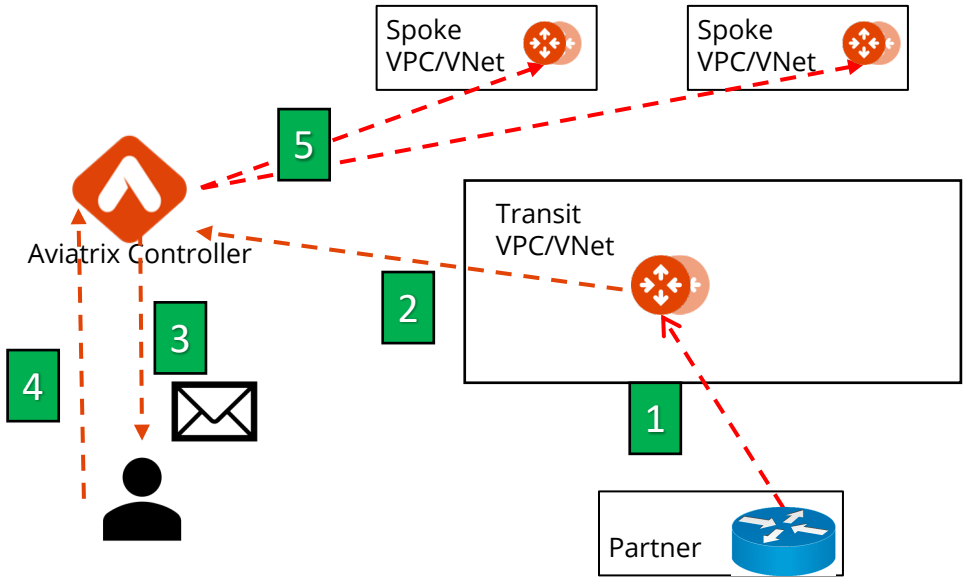


BGP Route Approval

BGP Route Approval

- Can explicitly approve any BGP-learned route from Partner or on-prem into the cloud network
- Prevents unwanted advertisement of routes such as 0/0

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



From Aviatrix Controller: Route Approval Request

N ⊗ no-reply@aviatrix.com <no-reply@aviatrix.com>
To: ⊗ Umair Hoodbhoy

Number of Events: 1.

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

Request approval for new learned CIDR(s):

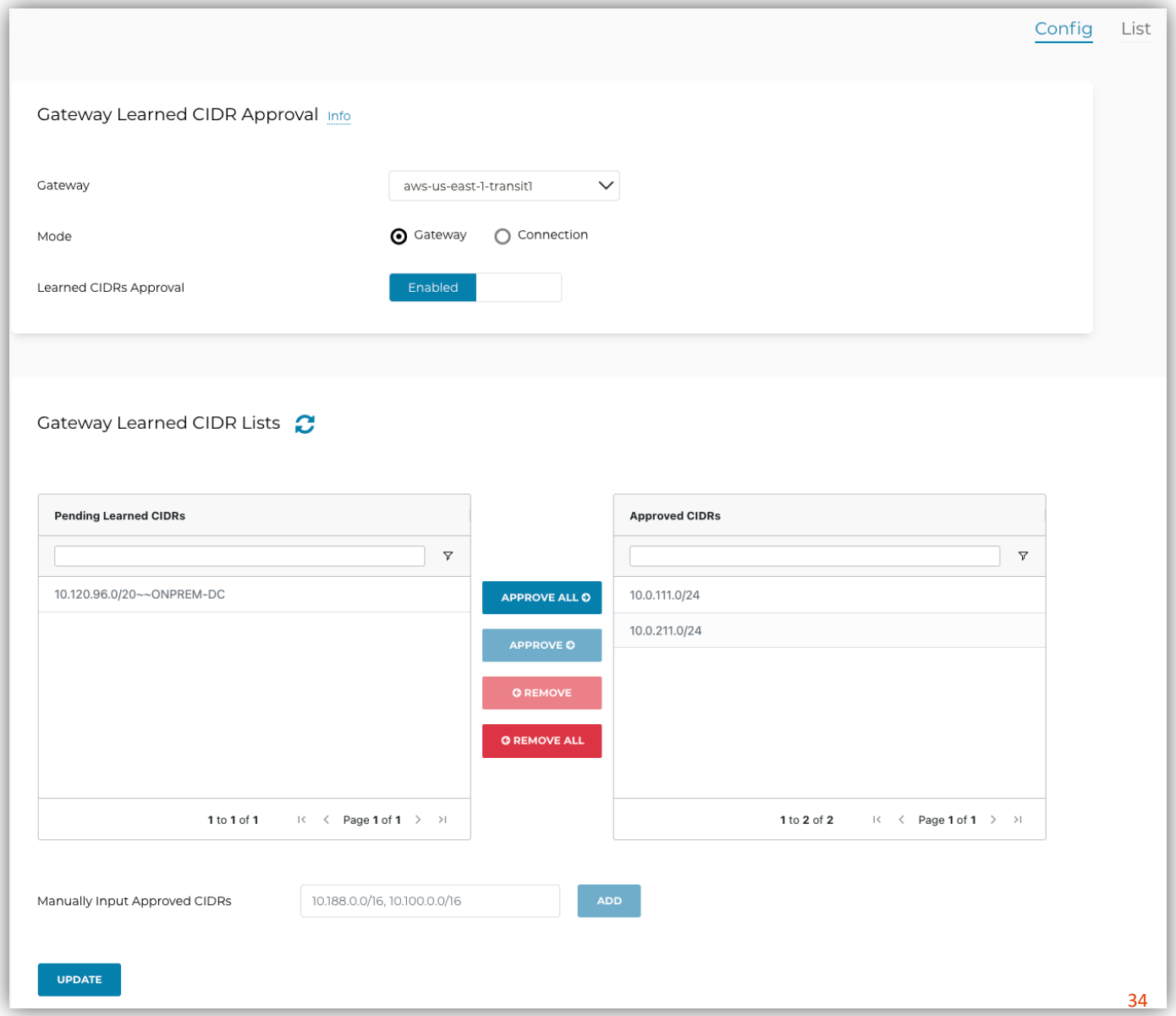
Gateway: aws-us-east-1-transit1, Connection: ONPREM-DC, CIDRs(1): 10.120.96.0/20

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

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

BGP Route Approval – Config

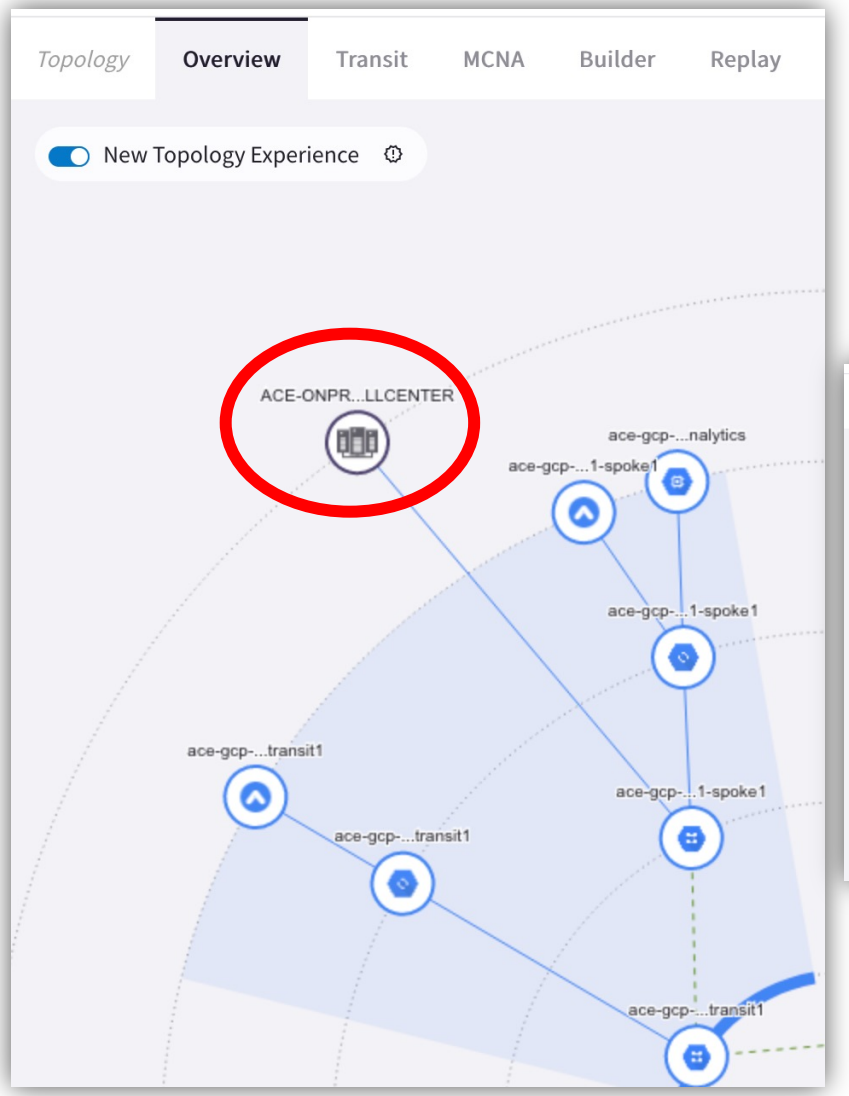
- **PATH:** Controller > MULTI-CLOUD TRANSIT > Approval > Config

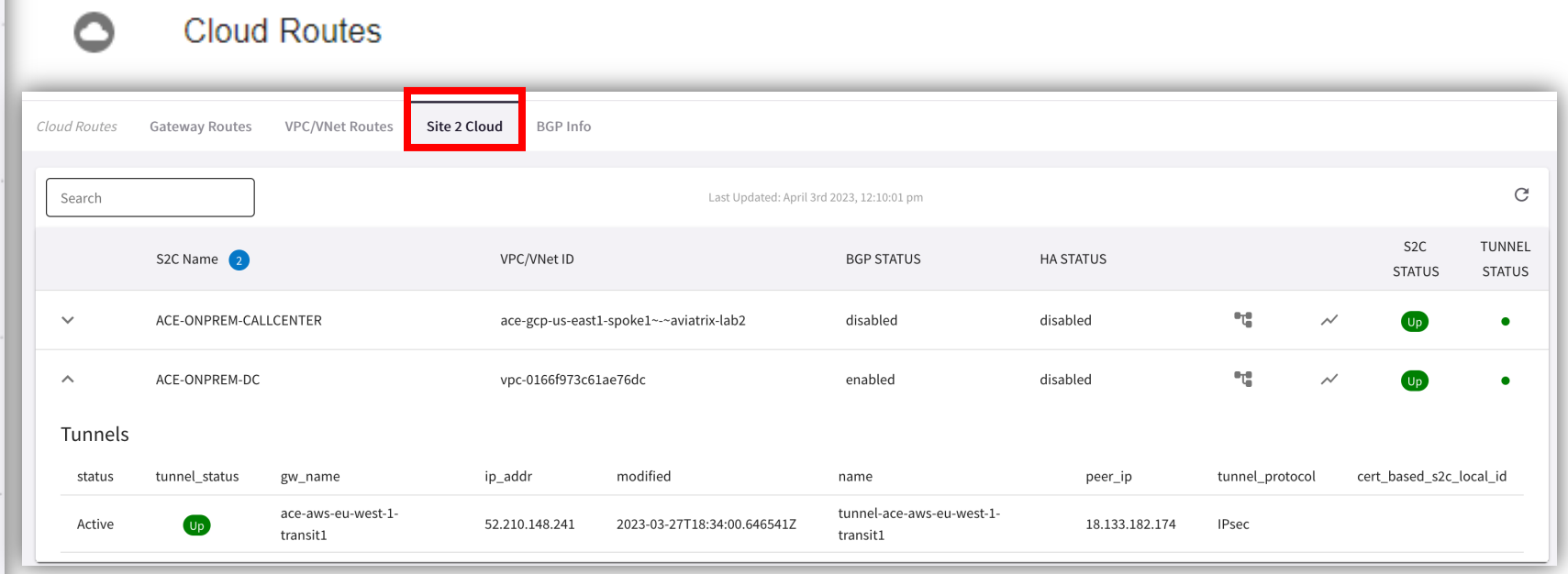


Site2Cloud & CoPilot

Site2Cloud Visibility via CoPilot

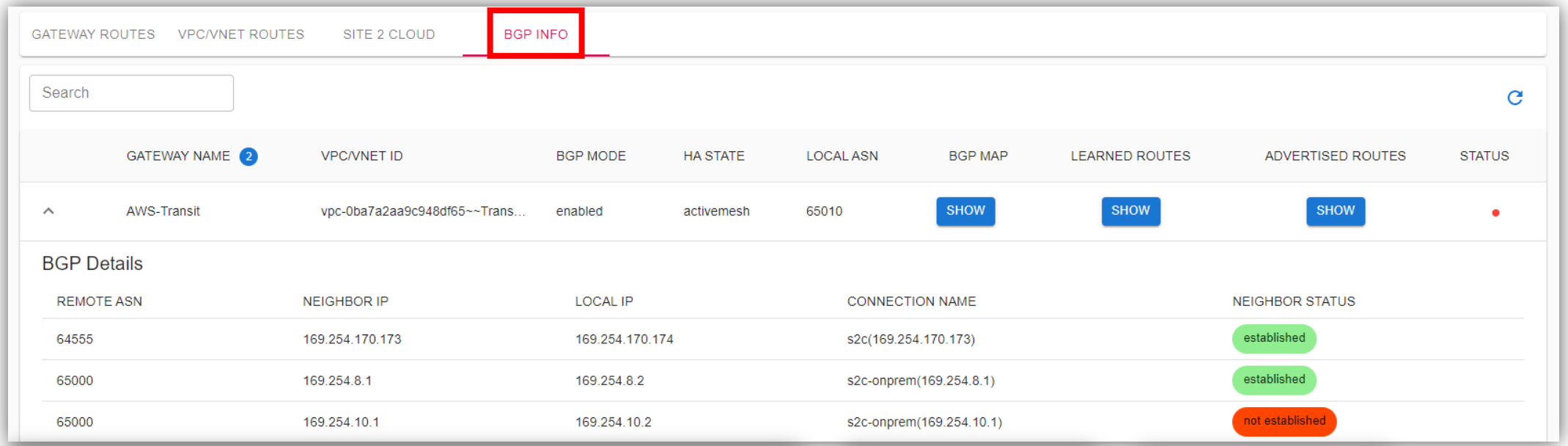
- **PATH:** COPILOT > Troubleshoot > Cloud Routes > **Site 2 Cloud**

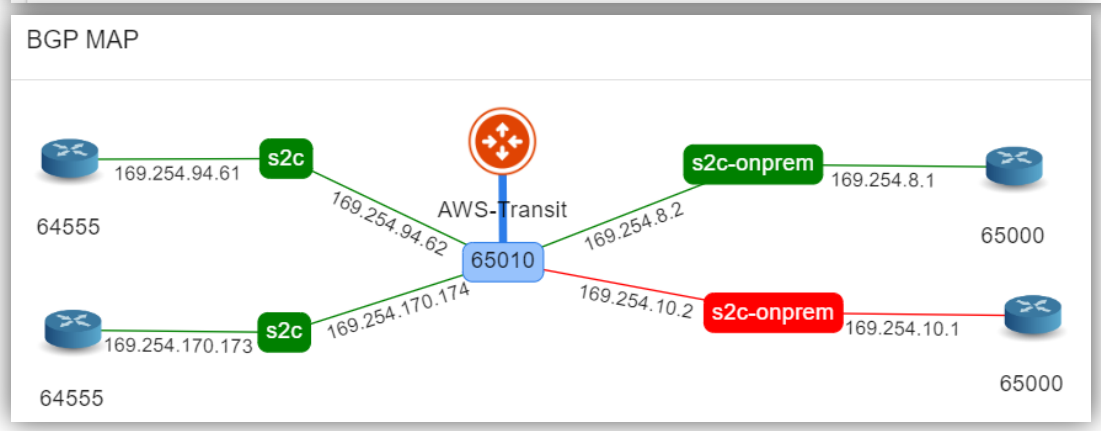


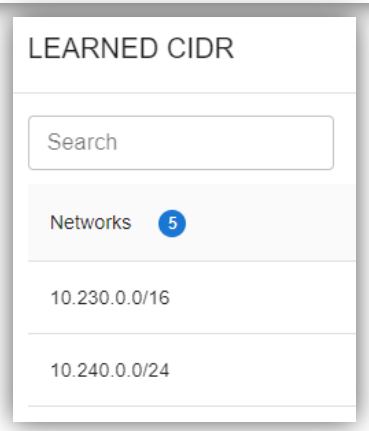


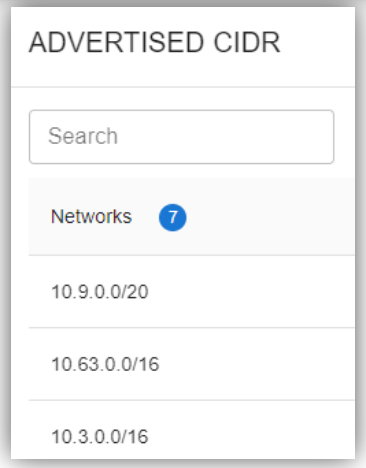
Site2Cloud BGP via CoPilot

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



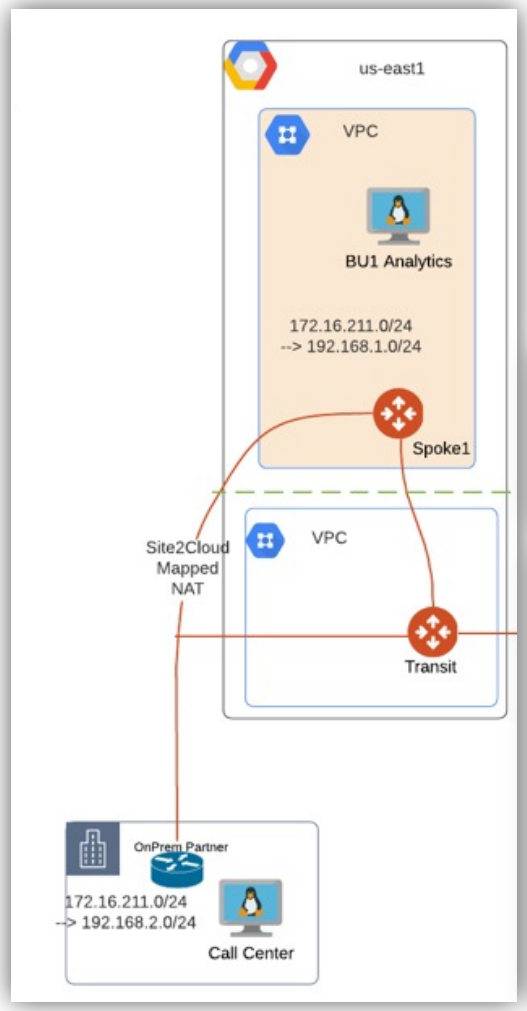


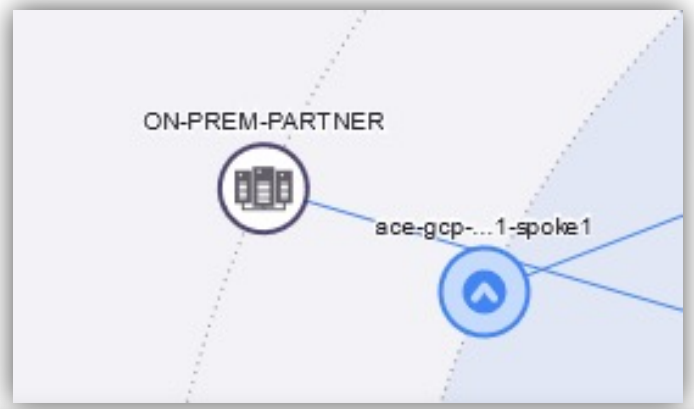


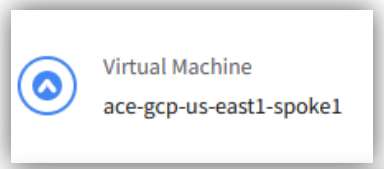


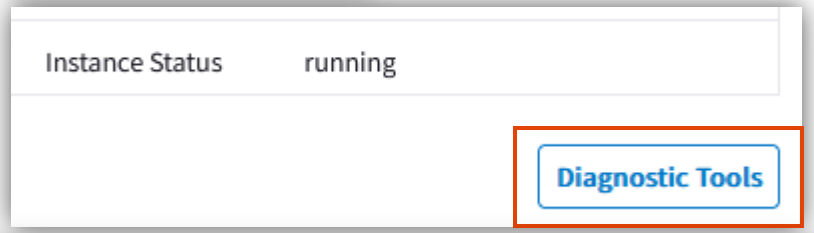
Site2Cloud Sessions via CoPilot

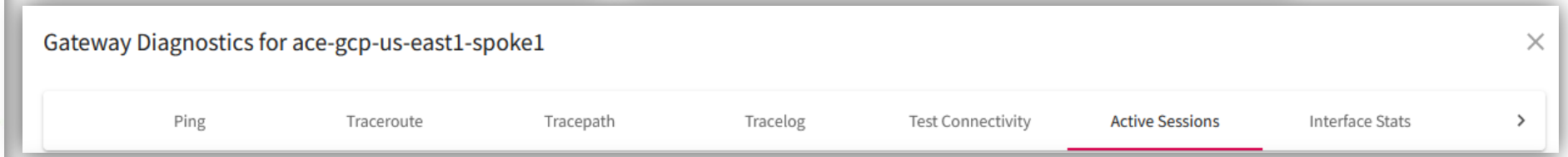
- **PATH:** COPILOT > Cloud Topology > Topology > select the concerned Gateway > **Diagnostic Tools**

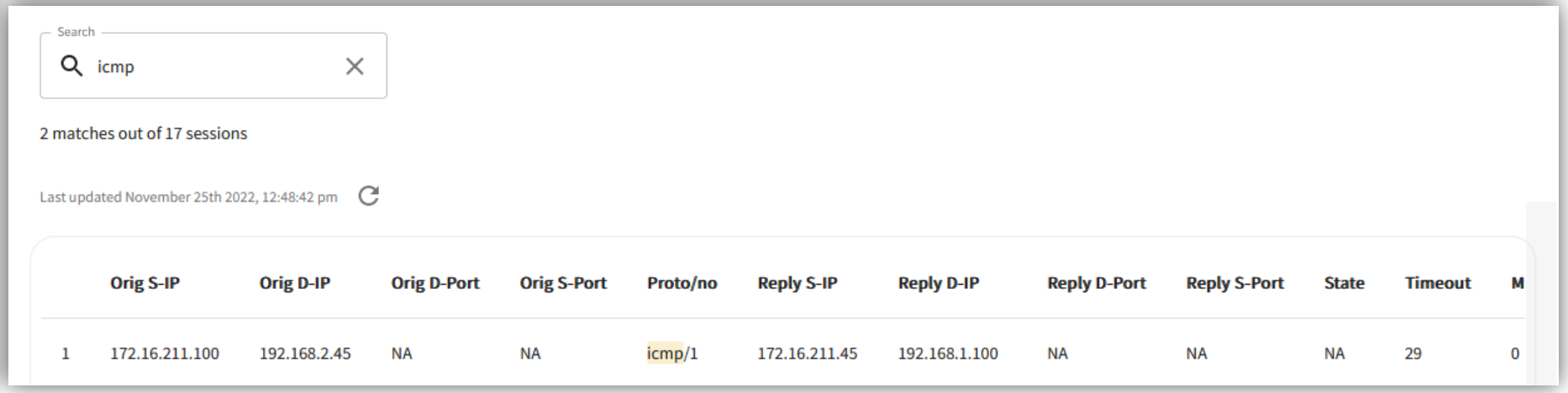












aviatrix

Next: Lab 6 Site2Cloud