

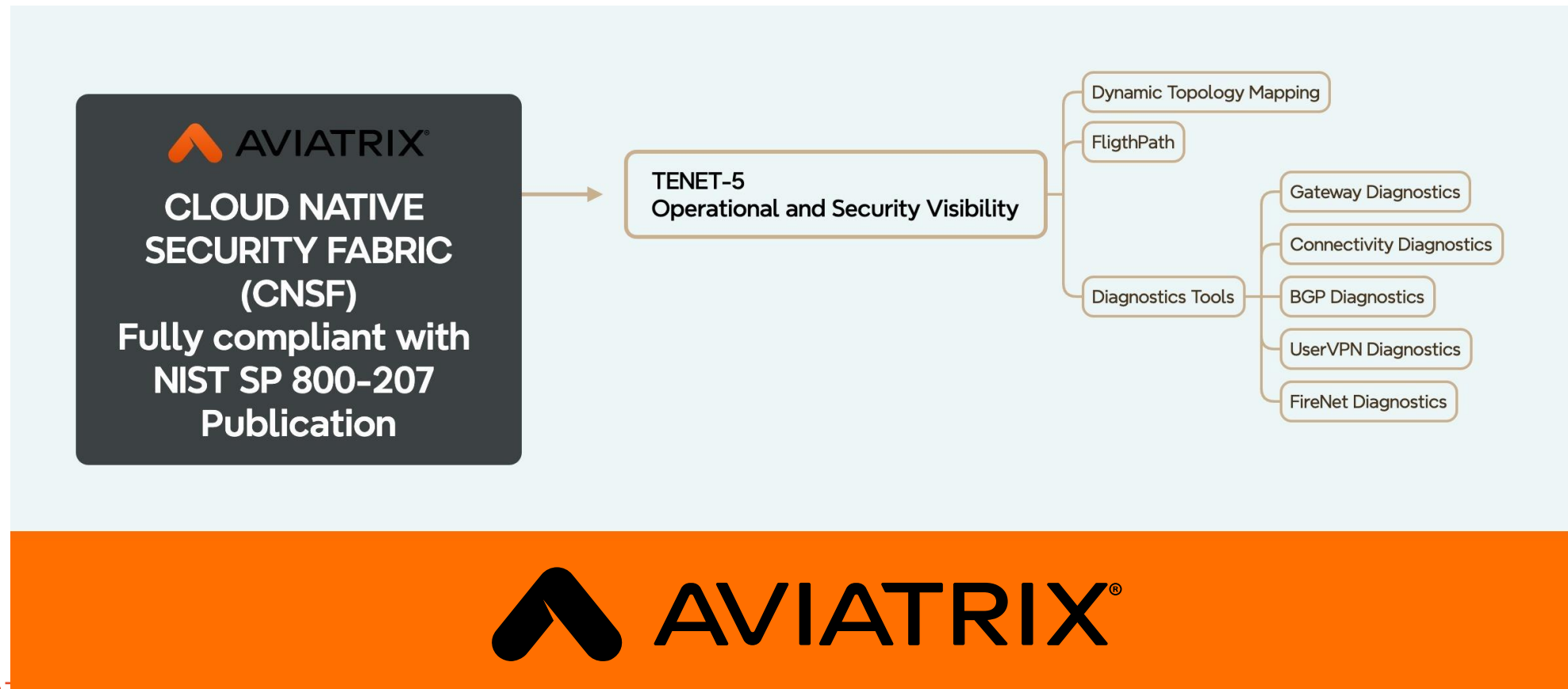


Tenet-5: Operational and Security Visibility

Security and Operational Visibility

Tenet from NIST Publication 800-207 - Zero Trust Architecture (ZTA)

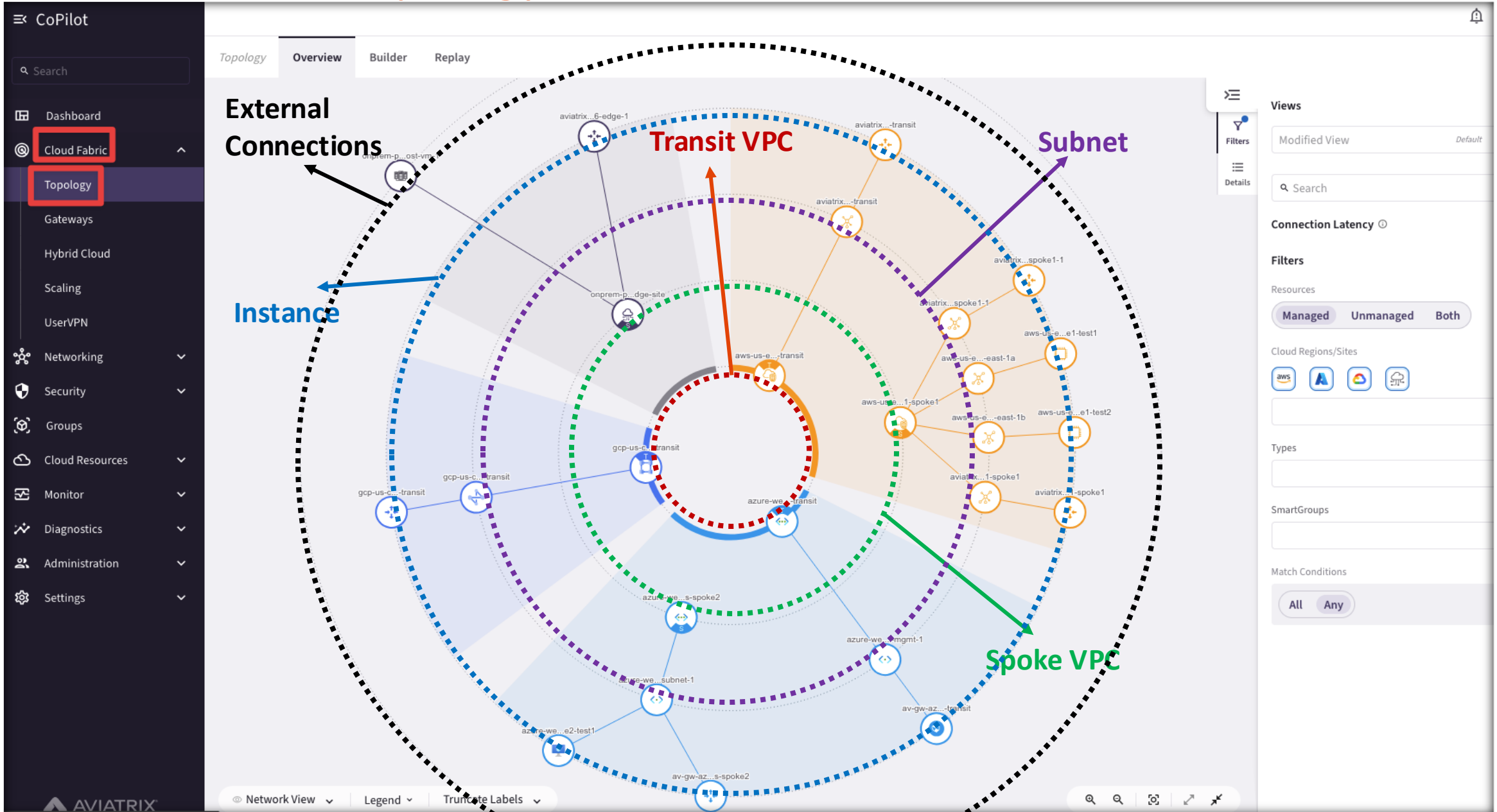
As mentioned in Section 3.4.1, all traffic is inspected and logged on the network and analyzed to identify and react to potential attacks against the enterprise. However, as also mentioned, some (possibly the majority) of the traffic on the enterprise network may be opaque to layer 3 network





Dynamic Topology

Cloud Fabric – Topology: Circles



Network ACL: ✓ Pass

ACL ID: [acl-0744968facc89e164](#)

Direction	Protocol	Port	CIDR	Allow/Deny
Outbound	ALL	ALL	0.0.0.0/0	allow
Inbound	ALL	ALL	0.0.0.0/0	allow
Outbound	ALL	ALL	0.0.0.0/0	deny
Inbound	ALL	ALL	0.0.0.0/0	deny

Security Groups:

Group Name: accounting-aws-spoke-prod ([sg-06a88d2c8afc084e3](#))

Inbound Rules				
Type	Protocol	Port Range	Source	Description
All traffic	ALL	ALL	10.1.4.0/24	
https	tcp	443	54.148.104.116/32	
Outbound Rules				
Type	Protocol	Port Range	Destination	Description
All traffic	ALL	ALL	0.0.0.0/0	

Group Name: None ([None](#))

- ❑ You can run a report in CoPilot for two instances using **Diagnostics > AppIQ > FlightPath**.

When selecting the source and destination instances to run the report against, you can specify two managed resources or one managed resource and one external resource.

Diagnostics Tools – Gateway Diagnostics



CoPilot

Search

Dashboard

Cloud Fabric

Networking

Security

Groups

Cloud Resources

Monitor

Diagnostics

Diagnostic Tools

Cloud Routes

Administration

Settings

Diagnostics Tools

Gateway Diagnostics

Connectivity Diagnostics

BGP Diagnostics

Controller Diagnostics

UserVPN Diagnostics

FireNet Diagnostics

Tools

Gateway Instance

aws-us-east-2-spoke1

Ping

Packet Capture

Traceroute

Tracepath

Connectivity

Active Sessions

Interface Stats

Services

Diagnostics

Tracelog

Traceroute

Interface

Use Route Table

Destination (IP / Host Name)

10.0.12.40

tracert to 10.0.12.40 (10.0.12.40), 30 hops max, 60 byte packets

1 10.0.10.142 (10.0.10.142) 0.286 ms 0.304 ms 0.284 ms

2 10.0.21.136 (10.0.21.136) 11.917 ms 11.889 ms 11.873 ms

3 10.0.13.140 (10.0.13.140) 12.364 ms 12.400 ms 12.379 ms

4 10.0.12.40 (10.0.12.40) 12.665 ms 12.932 ms 12.963 ms

Copy to Clipboard

Aviatrix

Diagnostics Tools – BGP Diagnostics



CoPilot

Search

Dashboard

Cloud Fabric

Networking

Security

Groups

Cloud Resources

Monitor

Diagnostics

AppIQ

Diagnostics Tools

Cloud Routes

Administration

Settings

Diagnostic Tools

Gateway Diagnostics

Connectivity Diagnostics

BGP Diagnostics

Controller Diagnostics

UserVPN Diagnostics

FireNet Diagnostics

Tools

Gateway Instance

onprem-pod96-edge-1

BGP Command

BGP Command

Command

show ip bgp

Last Run: Jul 24, 2025 6:39 AM

Run

Copy to Clipboard

```
Hello, this is FRRouting (version 9.1).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

onprem-pod96-edge-1# terminal length 0
onprem-pod96-edge-1# show ip bgp
BGP table version is 225, local router ID is 10.40.251.2, vrf id 0
Default local pref 100, local AS 64581
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

   Network        Next Hop         Metric LocPrf Weight Path
*> 10.40.1.0/28    10.40.251.1       0         7         0 64900 ?
*> 10.40.1.16/28   10.40.251.1       0         7         0 64900 ?
*> 10.40.1.32/28   10.40.251.1       0         7         0 64900 ?
*> 10.40.1.48/28   10.40.251.1       0         7         0 64900 ?
*> 10.40.1.64/28   10.40.251.1       0         7         0 64900 ?
*> 10.40.1.80/28   10.40.251.1       0         7         0 64900 ?
*> 10.40.1.96/28   10.40.251.1       0         7         0 64900 ?
*> 10.40.1.112/28  10.40.251.1       0         7         0 64900 ?
*> 10.40.1.128/28  10.40.251.1       0         7         0 64900 ?
*> 10.40.1.144/28  10.40.251.1       0         7         0 64900 ?
*> 10.40.1.160/28  10.40.251.1       0         7         0 64900 ?
*> 10.40.1.176/28  10.40.251.1       0         7         0 64900 ?
*> 10.40.1.192/28  10.40.251.1       0         7         0 64900 ?
*> 10.40.1.208/28  10.40.251.1       0         7         0 64900 ?
*> 10.40.1.224/28  10.40.251.1       0         7         0 64900 ?
*> 10.40.1.240/28  10.40.251.1       0         7         0 64900 ?
*> 10.40.2.0/28    10.40.251.1       0         7         0 64900 ?
*> 10.40.2.16/28   10.40.251.1       0         7         0 64900 ?
*> 10.40.2.32/28   10.40.251.1       0         7         0 64900 ?
*> 10.40.2.48/28   10.40.251.1       0         7         0 64900 ?
*> 10.40.2.64/28   10.40.251.1       0         7         0 64900 ?
*> 10.40.2.80/28   10.40.251.1       0         7         0 64900 ?
```

Diagnostics Tools – Controller Diagnostics



CoPilot

Search

Dashboard

Cloud Fabric

Networking

Security

Groups

Cloud Resources

Monitor

Diagnostics

AppIQ

Diagnostics Tools

Cloud Routes

Administration

Settings

Diagnostics Tools

Gateway Diagnostics

Connectivity Diagnostics

BGP Diagnostics

Controller Diagnostics

UserVPN Diagnostics

FireNet Diagnostics

Tools

Ping

Services

Command Log

Event Log

Diagnostics

Configuration Bundle

Event Log

Search

Refresh

2025-07-24T04:37:59.603912 GATEWAY-CREATED: gwname: gcp-us-central1-spoke1

2025-07-24T04:37:59.349212 GATEWAY-INITIALIZED: gwname: gcp-us-central1-spoke1

2025-07-24T04:37:38.814590 GATEWAY-CREATED: gwname: aws-us-east-2-transit

2025-07-24T04:37:37.053696 GATEWAY-INITIALIZED: gwname: aws-us-east-2-transit

2025-07-24T04:37:05.008054 GATEWAY-CREATED: gwname: azure-west-us-spoke1

2025-07-24T04:36:59.240538 GATEWAY-INITIALIZED: gwname: azure-west-us-spoke1

2025-07-24T04:36:36.237278 GATEWAY-CREATED: gwname: aws-us-east-2-spoke1

2025-07-24T04:36:36.008779 GATEWAY-INITIALIZED: gwname: aws-us-east-2-spoke1

2025-07-23T19:48:51.959532 TUNNEL-CREATED: conn_name: onprem-pod96-edge-1-to-onprem-pod96-host-vm-1, gw_name: onprem-pod96-edge-1, peer: 10.40.251.1

2025-07-23T19:45:43.456424 GATEWAY-CREATED: gwname: azure-west-us-transit

2025-07-23T19:45:18.005727 GATEWAY-INITIALIZED: gwname: azure-west-us-transit

2025-07-23T19:45:08.020290 GATEWAY-CREATED: gwname: aws-us-east-1-spoke1-1

2025-07-23T19:45:06.533176 GATEWAY-INITIALIZED: gwname: aws-us-east-1-spoke1-1

2025-07-23T19:44:27.570068 GATEWAY-CREATED: gwname: aws-us-east-1-transit

2025-07-23T19:44:26.328614 GATEWAY-INITIALIZED: gwname: aws-us-east-1-transit

2025-07-23T19:44:03.618553 GATEWAY-CREATED: gwname: onprem-pod96-edge-1

2025-07-23T19:43:33.880793 GATEWAY-CREATED: gwname: gcp-us-central1-transit

2025-07-23T19:43:33.634298 GATEWAY-INITIALIZED: gwname: gcp-us-central1-transit

2025-07-23T19:42:39.145253 GATEWAY-CREATED: gwname: azure-west-us-spoke2

2025-07-23T19:42:31.159612 GATEWAY-INITIALIZED: gwname: azure-west-us-spoke2

2025-07-23T19:39:00.062168 GATEWAY-CREATED: gwname: aws-us-east-1-spoke1

2025-07-23T19:38:58.359706 GATEWAY-INITIALIZED: gwname: aws-us-east-1-spoke1

2025-07-23T19:31:54.848210 ACCOUNT-CREATED:

2025-07-23T19:31:51.766476 ACCOUNT-CREATED:

2025-07-23T19:31:32.113071 GATEWAY-INITIALIZED: gwname: onprem-pod96-edge-1

2025-07-23T19:24:56.252203 ACCOUNT-CREATED:

2025-07-23T19:23:29.910459 ACCOUNT-CREATED:

Copy to Clipboard

AVIATRIX

Diagnostics Tools – UserVPN Diagnostics



CoPilot

Search

Dashboard

Cloud Fabric

Networking

Security

Groups

Cloud Resources

Monitor

Diagnostics

AppIQ

Diagnostic Tools

Cloud Routes

Administration

Settings

Diagnostic Tools

Gateway Diagnostics

Connectivity Diagnostics

BGP Diagnostics

Controller Diagnostics

UserVPN Diagnostics

FireNet Diagnostics

Tools

Diagnostics

Session History

ELB Status

Session History

User's Name

Start Time

End Time

Jul 24, 2025 08:09 AM

Jul 24, 2025 08:09 AM

Destination IPs

Gateways

Run

Diagnostics Tools – FireNet Diagnostics



☰ CoPilot

🔍 Search

🏠 Dashboard

🌐 Cloud Fabric

🔗 Networking

🛡️ Security

👤 Groups

☁️ Cloud Resources

📊 Monitor

🔧 Diagnostics

AppIQ

Diagnostic Tools

Cloud Routes

👥 Administration

⚙️ Settings

Diagnostic Tools

Gateway Diagnostics

Connectivity Diagnostics

BGP Diagnostics

Controller Diagnostics

UserVPN Diagnostics

FireNet Diagnostics

Tools

Gateway Instance

azure-west-us-transit

Diagnostics

Diagnostics

Last Run: Jul 24, 2025 8:13 AM

Run

Copy to Clipboard

```
{
  "diagnostics_results": {
    "dmz_info": {
      "inspection": "yes",
      "egress": "no",
      "tgw": null,
      "domain": null,
      "all_spoke_list": [],
      "inspecting_spoke_list": [],
      "management_access": "no"
    },
    "azure-west-us-transit": {
      "System Time": {
        "Status": "Ok",
        "Offset with Controller": "0.49s"
      },
      "SSH": {
        "service": "Up",
        "port": {
          "22": "Up"
        }
      },
      "HTTPS": {
        "service": "Up",
        "port": {
          "443": [
            "up",
            "reachable"
          ]
        }
      },
      "certs": {
        "ip": "20.253.160.185",
        "is_enabled": true,
        "gwfqdn": "2d2466896d6344538ed08d06fdb6c55b.aviatrixnetwork.com",
        "cacrt": "/usr/local/share/ca-certificates/ca.crt",
        "svid_info": [
          "subject=C = US, O = SPIRE, CN = 2d2466896d6344538ed08d06fdb6c55b",
          "issuer=C = US, O = Aviatrix Systems SPIRE, CN = 17666843-0007-4191-98ae-d5e7e1e6d7b7",
          "notBefore=Jul 23 19:45:43 2025 GMT",
          "notAfter=Jul 24 19:45:53 2025 GMT"
        ]
      }
    }
  }
}
```



**Next: Tenet-6 Audit, Logs, Reporting
and Alerts**