Tenet-5: Operational and Security Visibility

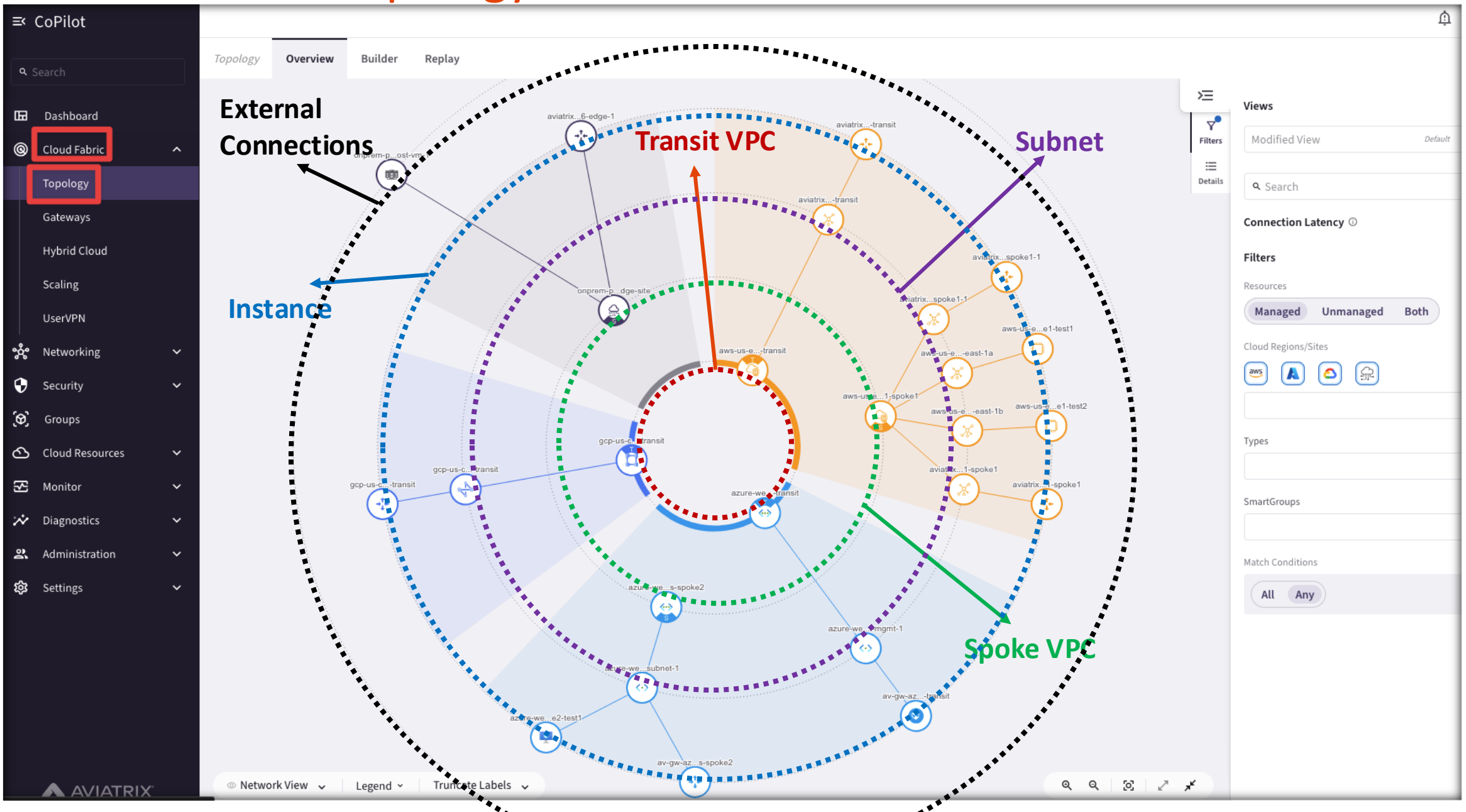
Security and Operational Visibility

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

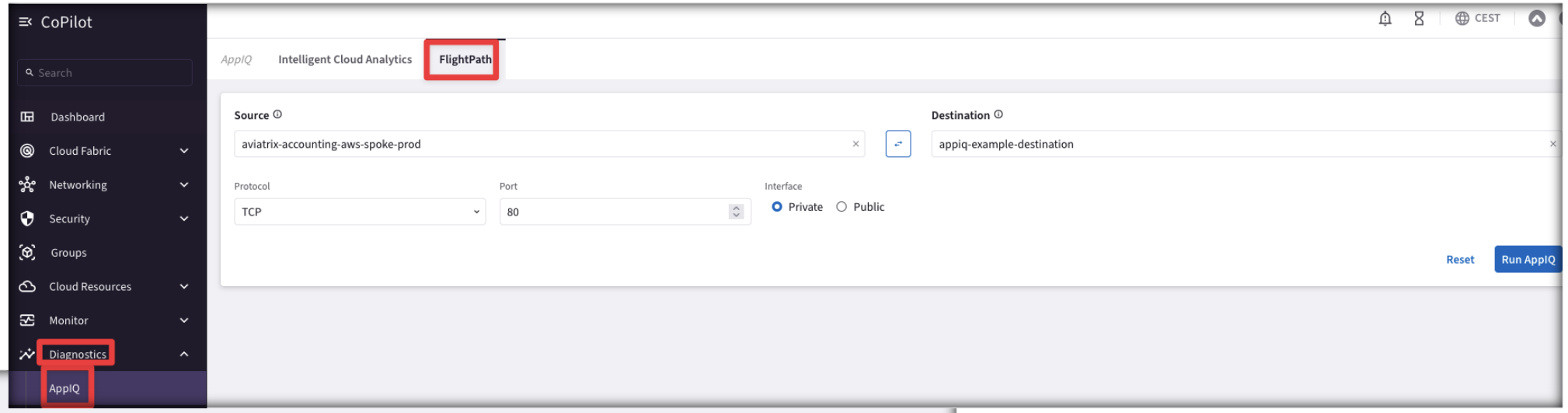
As mentioned in Section 3.4.1, all traffic is inspected and logged on the network and analyzed to identify and react to potential attacks against the enterprise. However, as also mentioned, some (possibly the majority) of the traffic on the enterprise network may be opaque to layer 3 network

Dynamic Topology

Cloud Fabric – Topology: Circles



FlightPath



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)

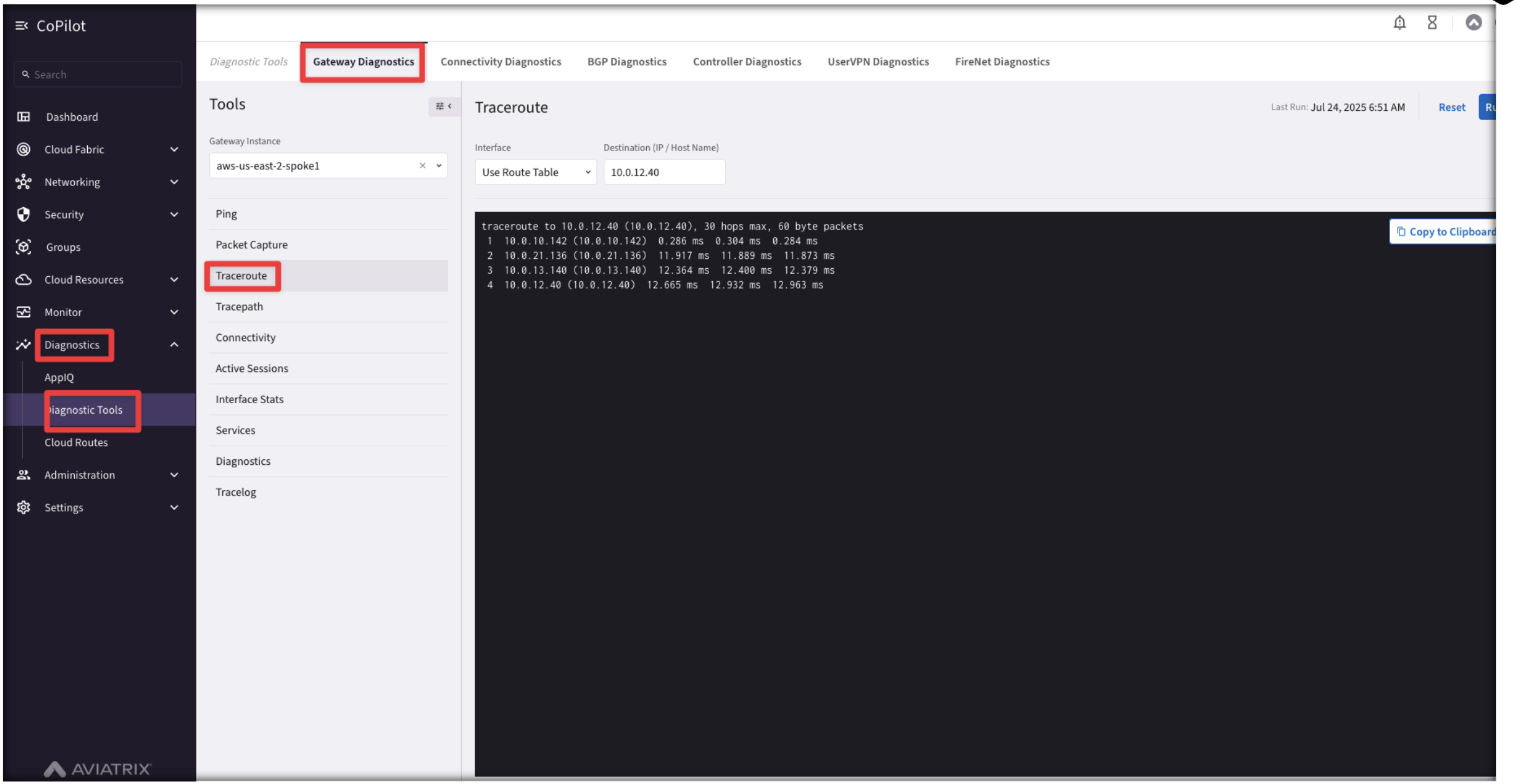
Inbound Rules				
Type	Protocol	Port Range	Source	Description
All traffic	ALL	ALL	10.1.4.0/24	
https	tcp	443	54.148.104.116/32	
Outbound Rules				
Type	Protocol	Port Range	Destination	Description
All traffic	ALL	ALL	0.0.0.0/0	

Group Name: None (None)

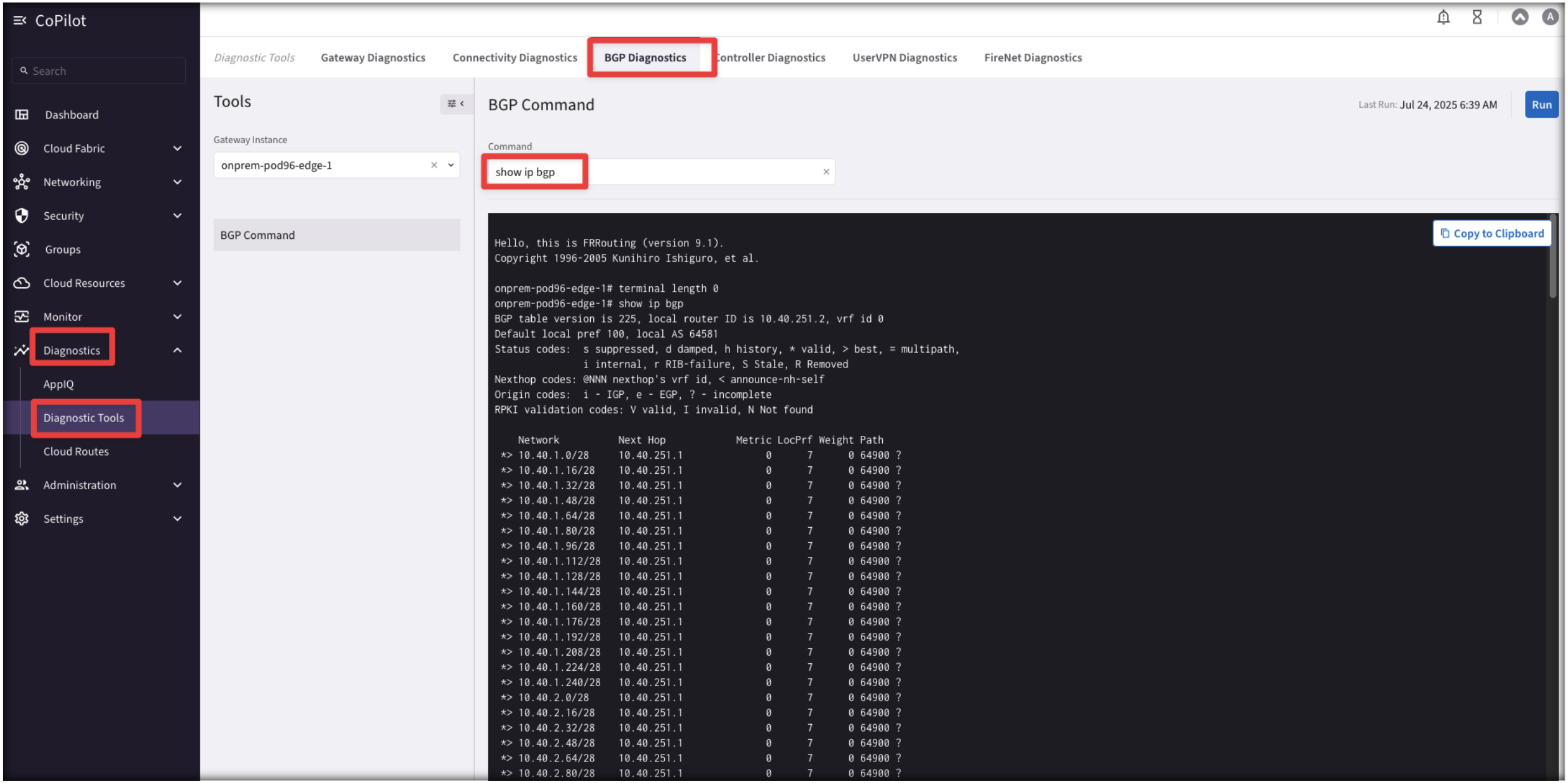
- You can run a report in CoPilot for two instances using **Diagnostics > AppIQ > FlightPath**.

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.

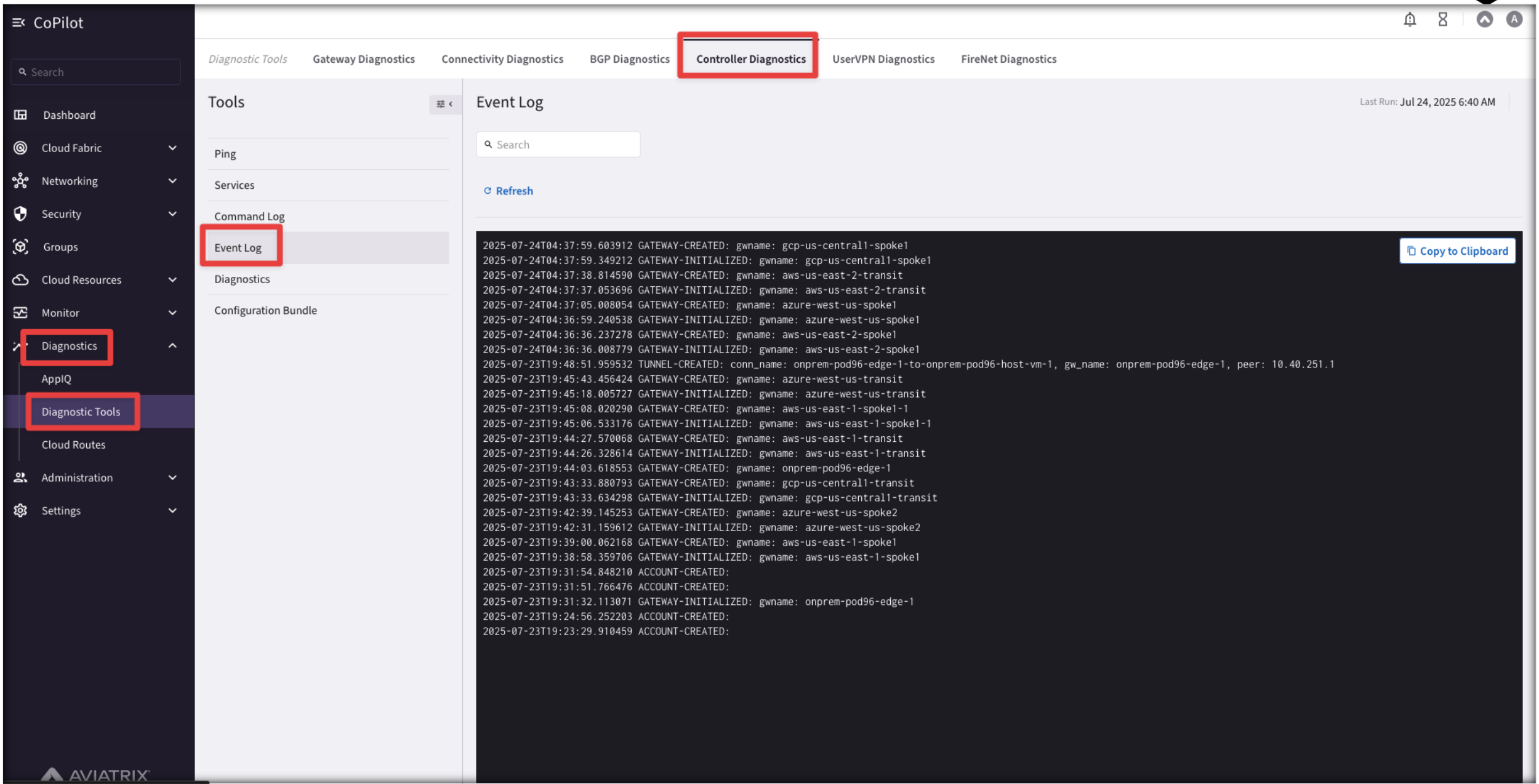
Diagnostics Tools – Gateway Diagnostics



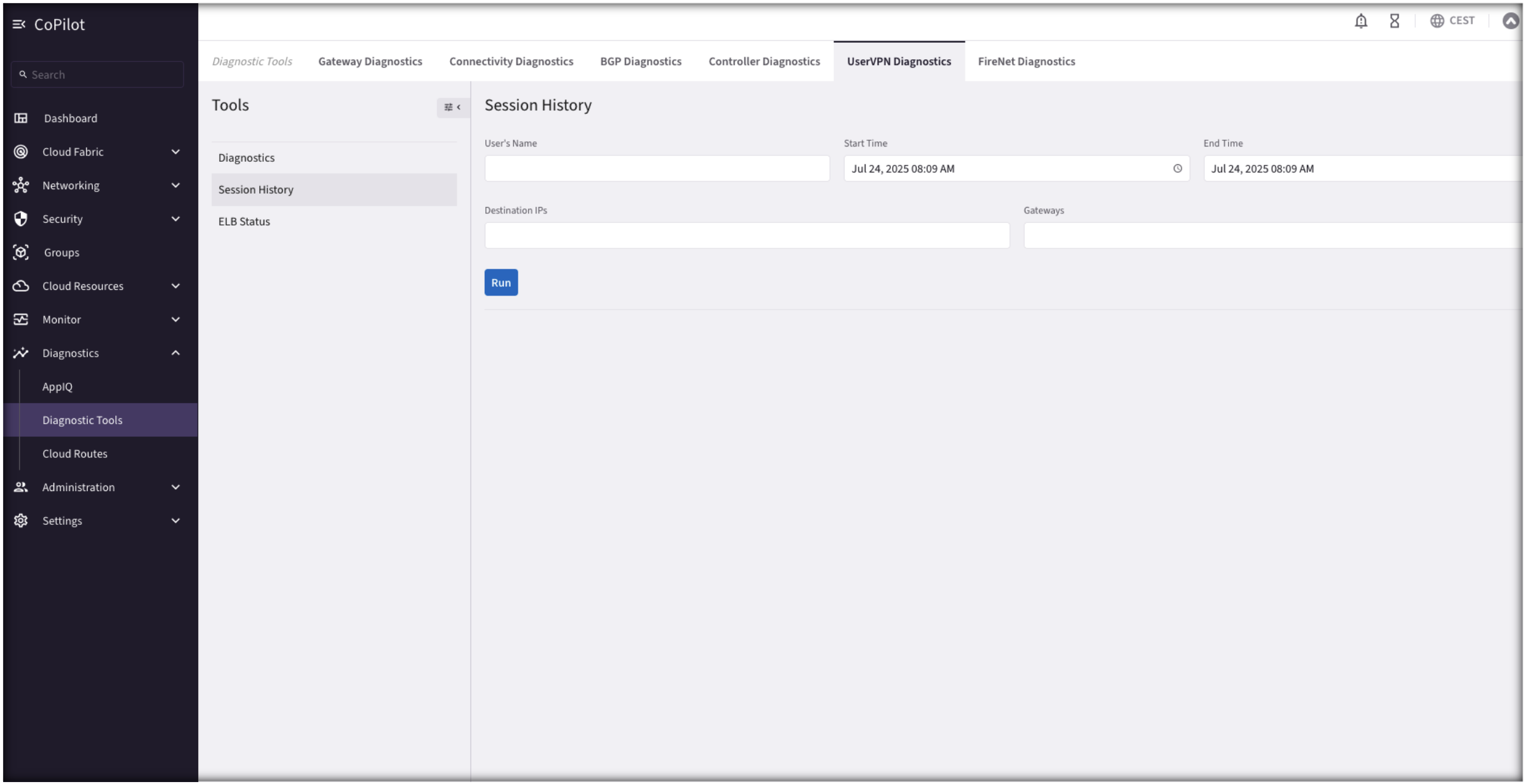
Diagnostics Tools – BGP Diagnostics



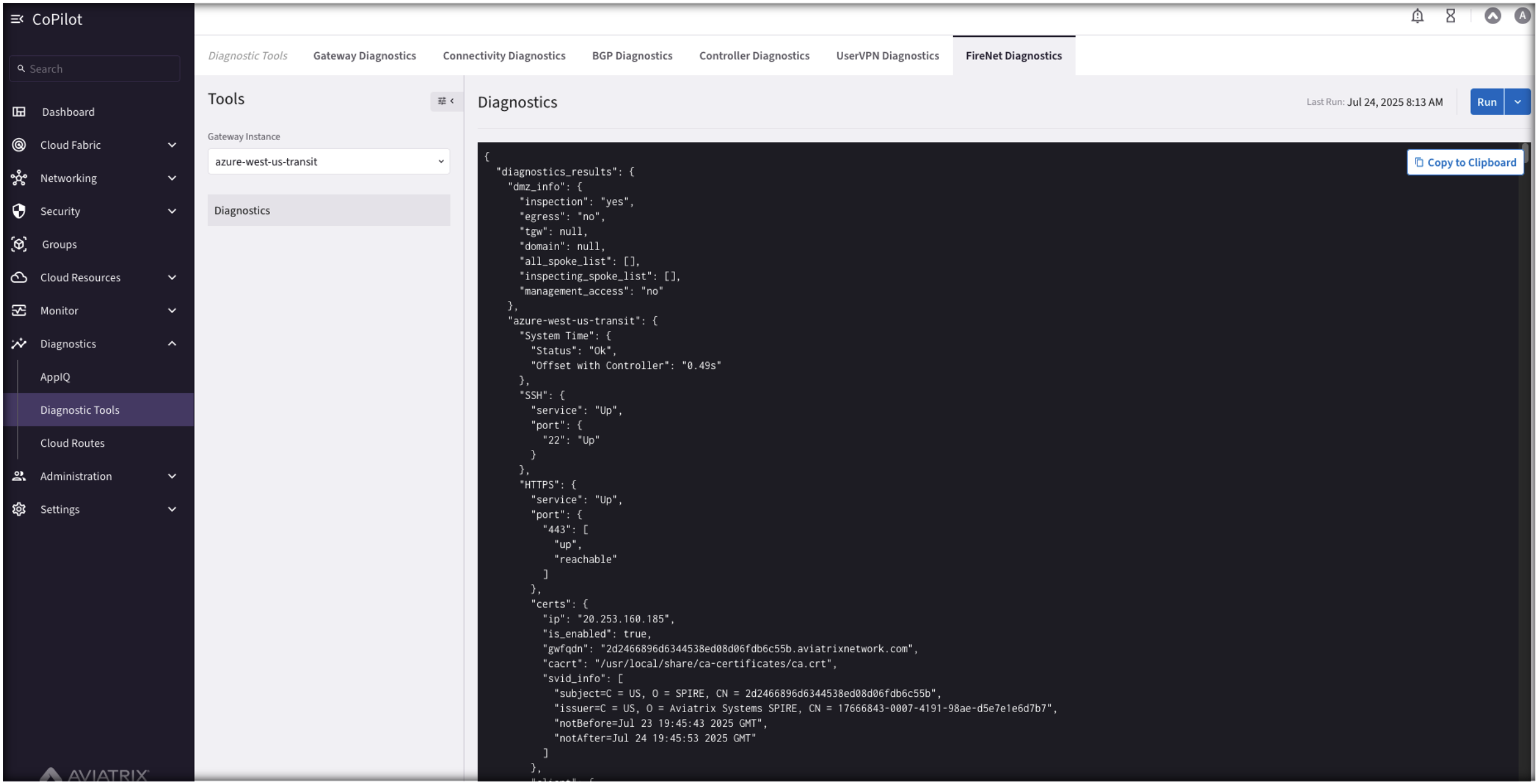
Diagnostics Tools – Controller Diagnostics



Diagnostics Tools – UserVPN Diagnostics



Diagnostics Tools – FireNet Diagnostics



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