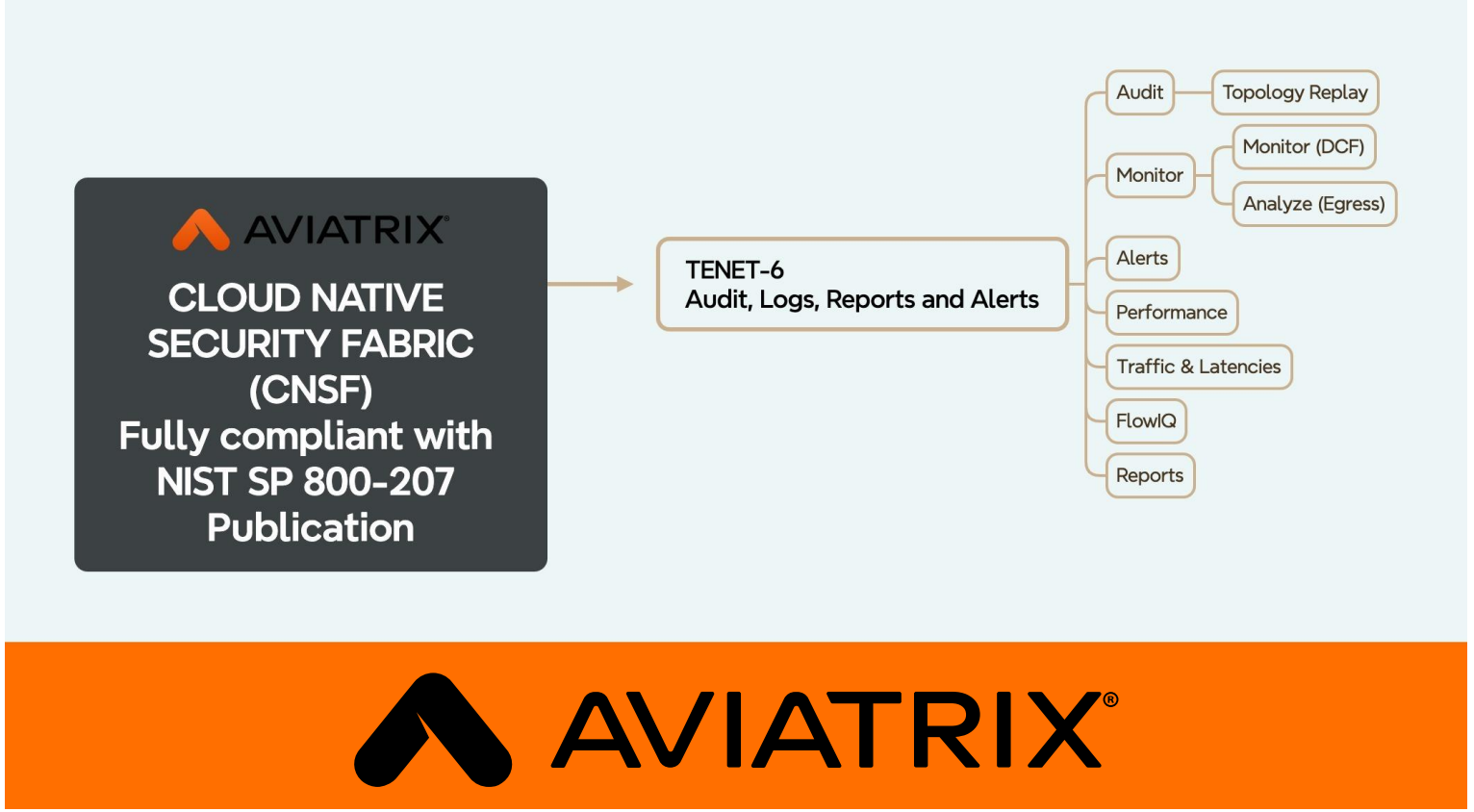
TENET-6: Audit, Logs, Reports and Alerts

Audit, Reporting and Alerts

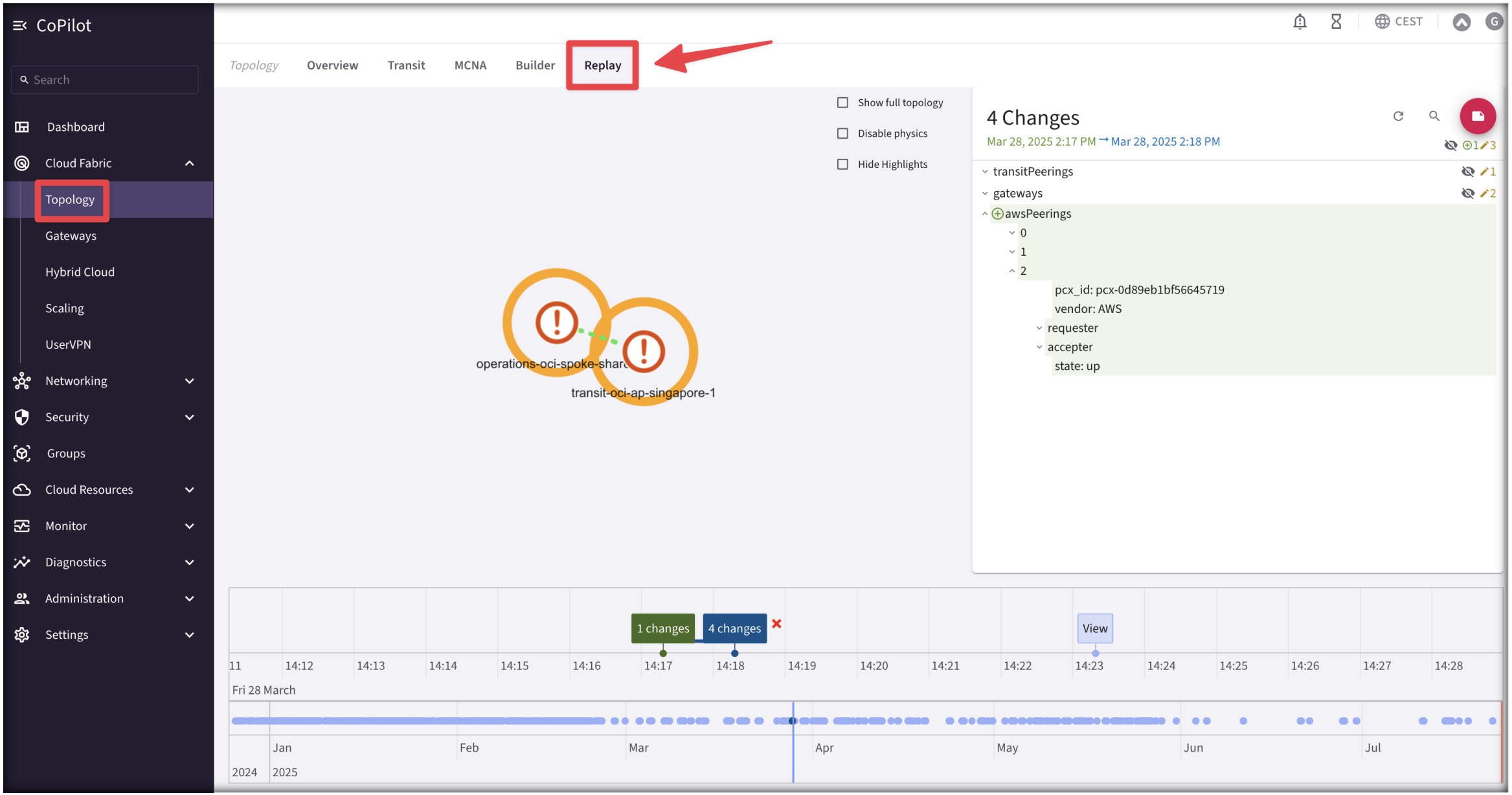
Tenet from NIST Publication 800-207 - Zero Trust Architecture (ZTA)

ZTA should allow developers and administrators sufficient flexibility to satisfy their business requirements while using logs and audit actions to identify access behavior patterns. Policy Engine (PE) and Policy Admin (PA) components must be properly configured and monitored, and any configuration changes must be logged and subject to audit.



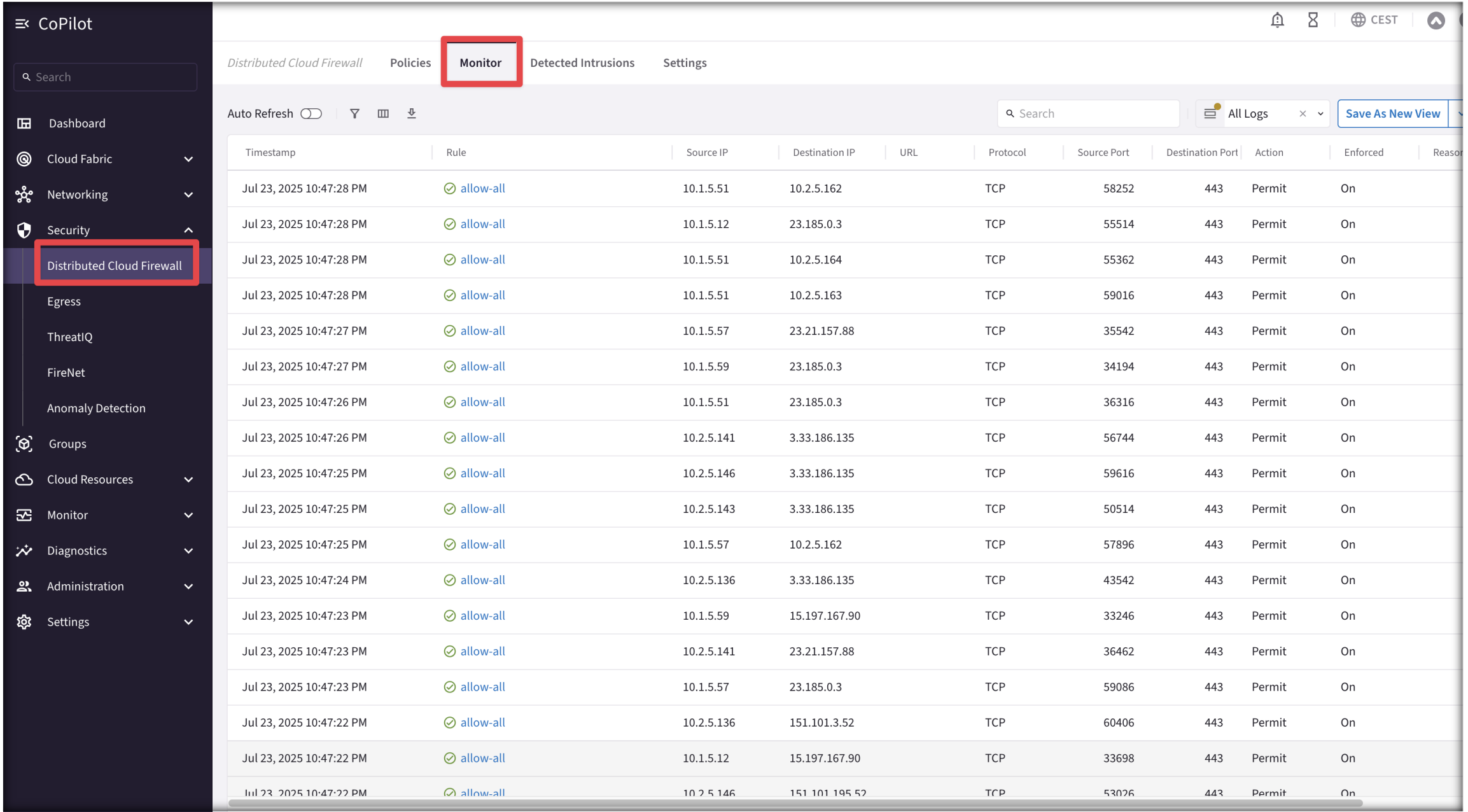
Topology Replay

Topology replay - Auditing

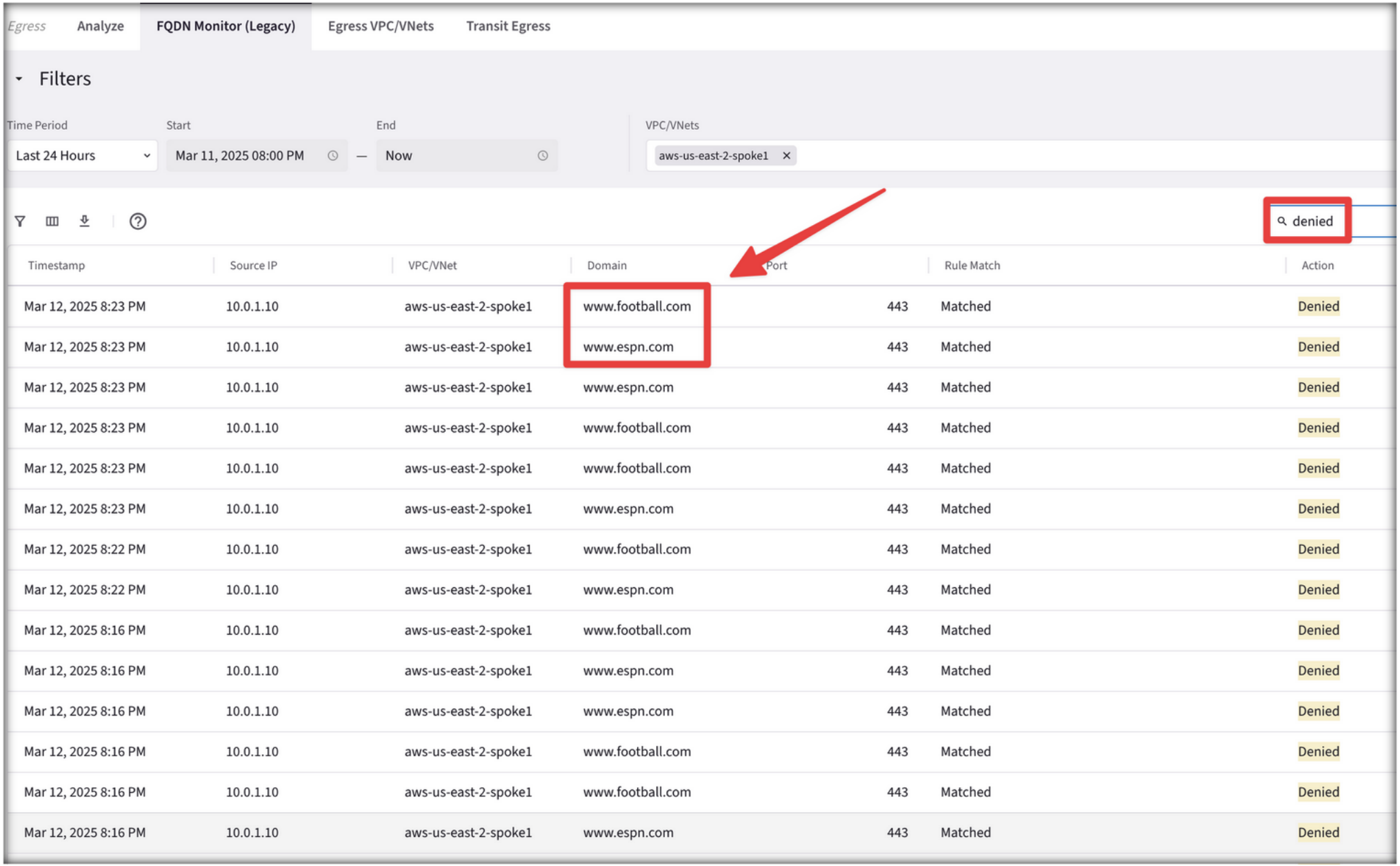


Monitor (DCF & Egress)

DCF Monitor


CoPilot
Search
Dashboard
Cloud Fabric
Networking
Security
Distributed Cloud Firewall
Egress
ThreatIQ
FireNet
Anomaly Detection
Groups
Cloud Resources
Monitor
Diagnostics
Administration
Settings
CEST
Distributed Cloud Firewall
Policies
Monitor
Detected Intrusions
Settings
Auto Refresh
Search
All Logs
Save As New View
Timestamp | Rule | Source IP | Destination IP | URL | Protocol | Source Port | Destination Port | Action | Enforced | Reason
Jul 23, 2025 10:47:28 PM | allow-all | 10.1.5.51 | 10.2.5.162 | | TCP | 58252 | 443 | Permit | On
Jul 23, 2025 10:47:28 PM | allow-all | 10.1.5.12 | 23.185.0.3 | | TCP | 55514 | 443 | Permit | On
Jul 23, 2025 10:47:28 PM | allow-all | 10.1.5.51 | 10.2.5.164 | | TCP | 55362 | 443 | Permit | On
Jul 23, 2025 10:47:28 PM | allow-all | 10.1.5.51 | 10.2.5.163 | | TCP | 59016 | 443 | Permit | On
Jul 23, 2025 10:47:27 PM | allow-all | 10.1.5.57 | 23.21.157.88 | | TCP | 35542 | 443 | Permit | On
Jul 23, 2025 10:47:27 PM | allow-all | 10.1.5.59 | 23.185.0.3 | | TCP | 34194 | 443 | Permit | On
Jul 23, 2025 10:47:26 PM | allow-all | 10.1.5.51 | 23.185.0.3 | | TCP | 36316 | 443 | Permit | On
Jul 23, 2025 10:47:26 PM | allow-all | 10.2.5.141 | 3.33.186.135 | | TCP | 56744 | 443 | Permit | On
Jul 23, 2025 10:47:25 PM | allow-all | 10.2.5.146 | 3.33.186.135 | | TCP | 59616 | 443 | Permit | On
Jul 23, 2025 10:47:25 PM | allow-all | 10.2.5.143 | 3.33.186.135 | | TCP | 50514 | 443 | Permit | On
Jul 23, 2025 10:47:25 PM | allow-all | 10.1.5.57 | 10.2.5.162 | | TCP | 57896 | 443 | Permit | On
Jul 23, 2025 10:47:24 PM | allow-all | 10.2.5.136 | 3.33.186.135 | | TCP | 43542 | 443 | Permit | On
Jul 23, 2025 10:47:23 PM | allow-all | 10.1.5.59 | 15.197.167.90 | | TCP | 33246 | 443 | Permit | On
Jul 23, 2025 10:47:23 PM | allow-all | 10.2.5.141 | 23.21.157.88 | | TCP | 36462 | 443 | Permit | On
Jul 23, 2025 10:47:23 PM | allow-all | 10.1.5.57 | 23.185.0.3 | | TCP | 59086 | 443 | Permit | On
Jul 23, 2025 10:47:22 PM | allow-all | 10.2.5.136 | 151.101.3.52 | | TCP | 60406 | 443 | Permit | On
Jul 23, 2025 10:47:22 PM | allow-all | 10.1.5.12 | 15.197.167.90 | | TCP | 33698 | 443 | Permit | On
Jul 23, 2025 10:47:22 PM | allow-all | 10.2.5.146 | 151.101.195.52 | | TCP | 53026 | 443 | Permit | On

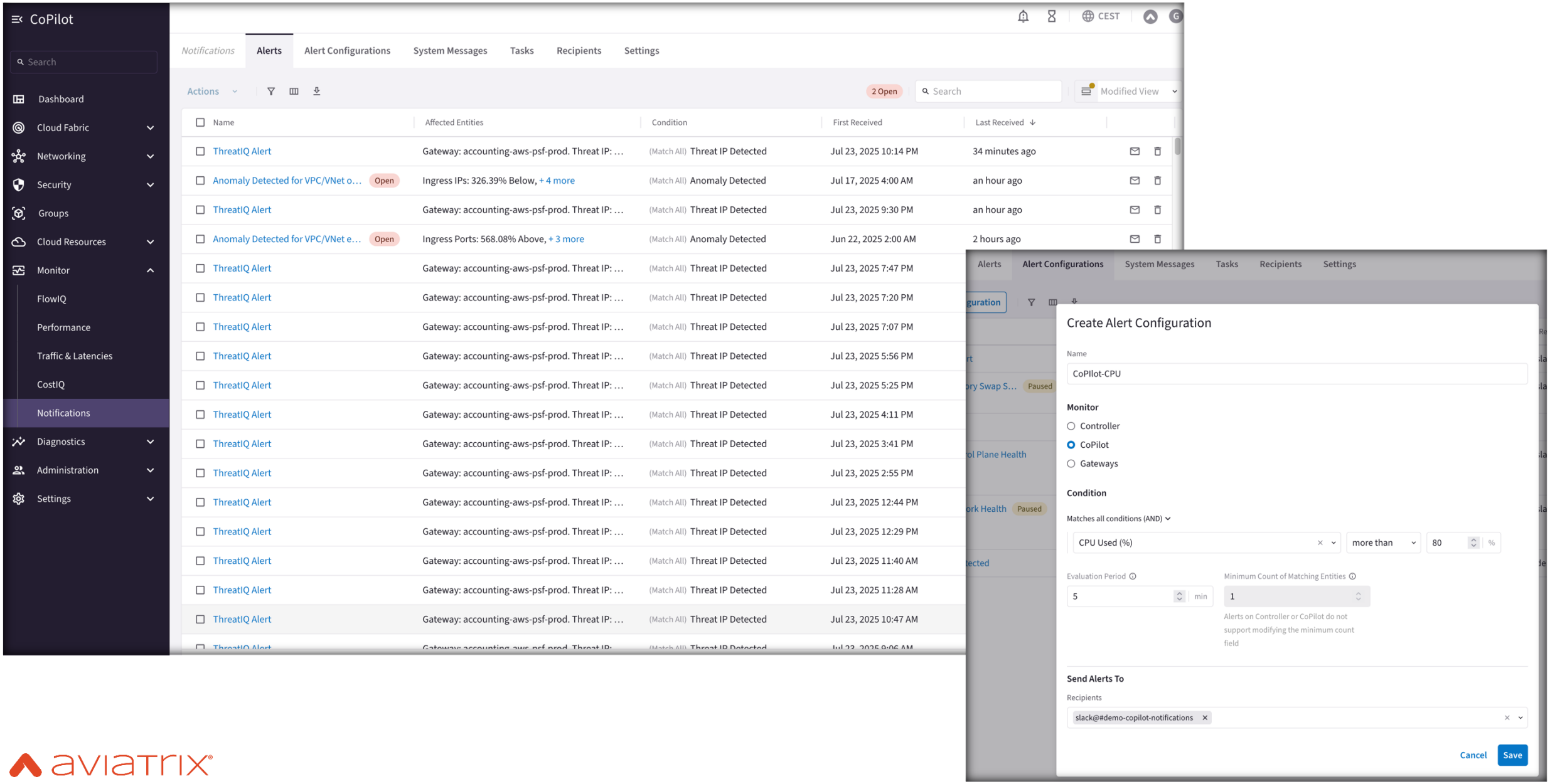
Egress Monitor



Timestamp	Source IP	VPC/VNet	Domain	Port	Rule Match	Action
Mar 12, 2025 8:23 PM	10.0.1.10	aws-us-east-2-spoke1	www.football.com	443	Matched	Denied
Mar 12, 2025 8:23 PM	10.0.1.10	aws-us-east-2-spoke1	www.espn.com	443	Matched	Denied
Mar 12, 2025 8:23 PM	10.0.1.10	aws-us-east-2-spoke1	www.espn.com	443	Matched	Denied
Mar 12, 2025 8:23 PM	10.0.1.10	aws-us-east-2-spoke1	www.football.com	443	Matched	Denied
Mar 12, 2025 8:23 PM	10.0.1.10	aws-us-east-2-spoke1	www.football.com	443	Matched	Denied
Mar 12, 2025 8:23 PM	10.0.1.10	aws-us-east-2-spoke1	www.espn.com	443	Matched	Denied
Mar 12, 2025 8:22 PM	10.0.1.10	aws-us-east-2-spoke1	www.football.com	443	Matched	Denied
Mar 12, 2025 8:22 PM	10.0.1.10	aws-us-east-2-spoke1	www.espn.com	443	Matched	Denied
Mar 12, 2025 8:16 PM	10.0.1.10	aws-us-east-2-spoke1	www.football.com	443	Matched	Denied
Mar 12, 2025 8:16 PM	10.0.1.10	aws-us-east-2-spoke1	www.espn.com	443	Matched	Denied
Mar 12, 2025 8:16 PM	10.0.1.10	aws-us-east-2-spoke1	www.espn.com	443	Matched	Denied
Mar 12, 2025 8:16 PM	10.0.1.10	aws-us-east-2-spoke1	www.football.com	443	Matched	Denied
Mar 12, 2025 8:16 PM	10.0.1.10	aws-us-east-2-spoke1	www.football.com	443	Matched	Denied
Mar 12, 2025 8:16 PM	10.0.1.10	aws-us-east-2-spoke1	www.espn.com	443	Matched	Denied

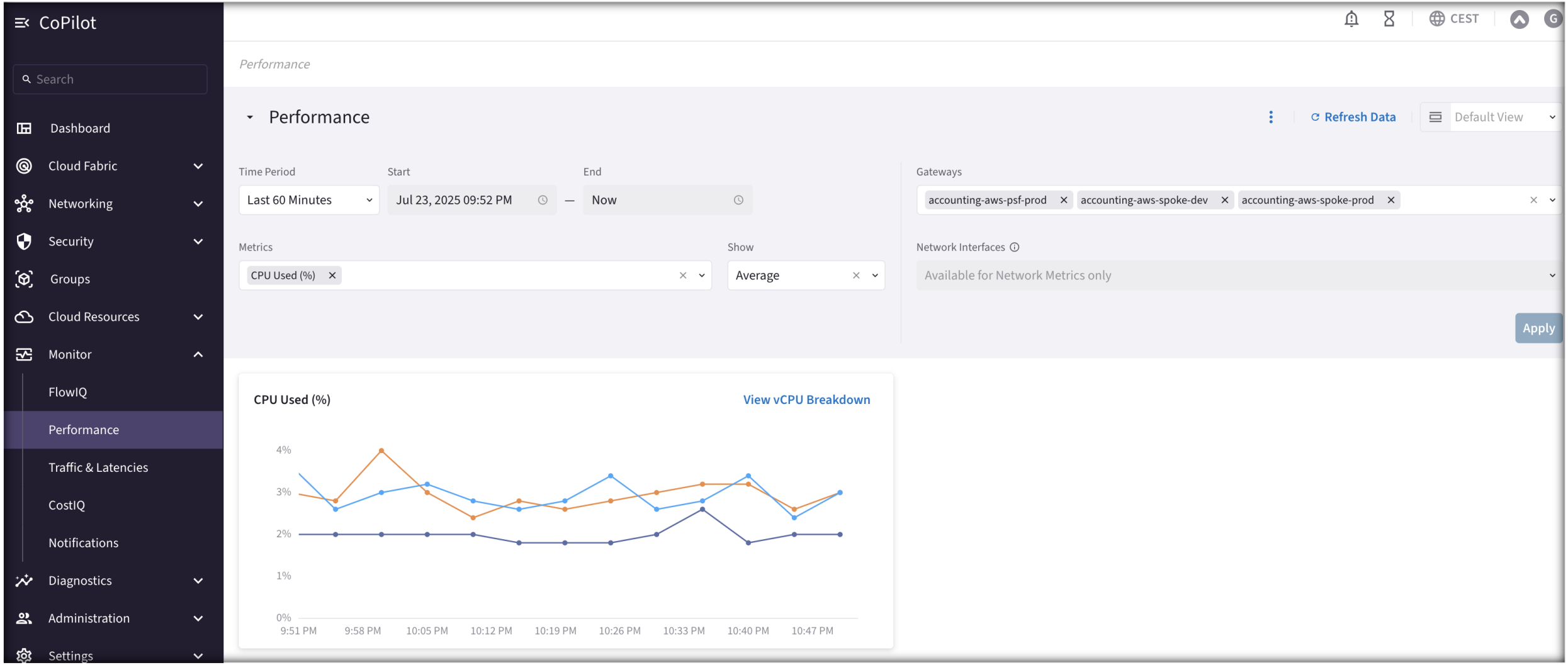
Alert

DCF Monitor


CoPilot
Search
Dashboard
Cloud Fabric
Networking
Security
Groups
Cloud Resources
Monitor
FlowIQ
Performance
Traffic & Latencies
CostIQ
Notifications
Diagnostics
Administration
Settings
CEST
Notifications
Alerts
Alert Configurations
System Messages
Tasks
Recipients
Settings
Actions
2 Open
Search
Modified View
Name
Affected Entities
Condition
First Received
Last Received
ThreatIQ Alert
Gateway: accounting-aws-psf-prod. Threat IP: …
(Match All) Threat IP Detected
Jul 23, 2025 10:14 PM
34 minutes ago
Anomaly Detected for VPC/VNet o…
Open
Ingress IPs: 326.39% Below, + 4 more
(Match All) Anomaly Detected
Jul 17, 2025 4:00 AM
an hour ago
Jul 23, 2025 9:30 PM
Anomaly Detected for VPC/VNet e…
Ingress Ports: 568.08% Above, + 3 more
Jun 22, 2025 2:00 AM
2 hours ago
Jul 23, 2025 7:47 PM
Jul 23, 2025 7:20 PM
Jul 23, 2025 7:07 PM
Jul 23, 2025 5:56 PM
Jul 23, 2025 5:25 PM
Jul 23, 2025 4:11 PM
Jul 23, 2025 3:41 PM
Jul 23, 2025 2:55 PM
Jul 23, 2025 12:44 PM
Jul 23, 2025 12:29 PM
Jul 23, 2025 11:40 AM
Jul 23, 2025 11:28 AM
Jul 23, 2025 10:47 AM
Create Alert Configuration
Name
CoPIlot-CPU
Monitor
Controller
CoPilot
Gateways
Condition
Matches all conditions (AND)
CPU Used (%)
more than
80
%
Evaluation Period
5
min
Minimum Count of Matching Entities
1
Alerts on Controller or CoPilot do not support modifying the minimum count field
Send Alerts To
Recipients
slack@#demo-copilot-notifications
Cancel
Save

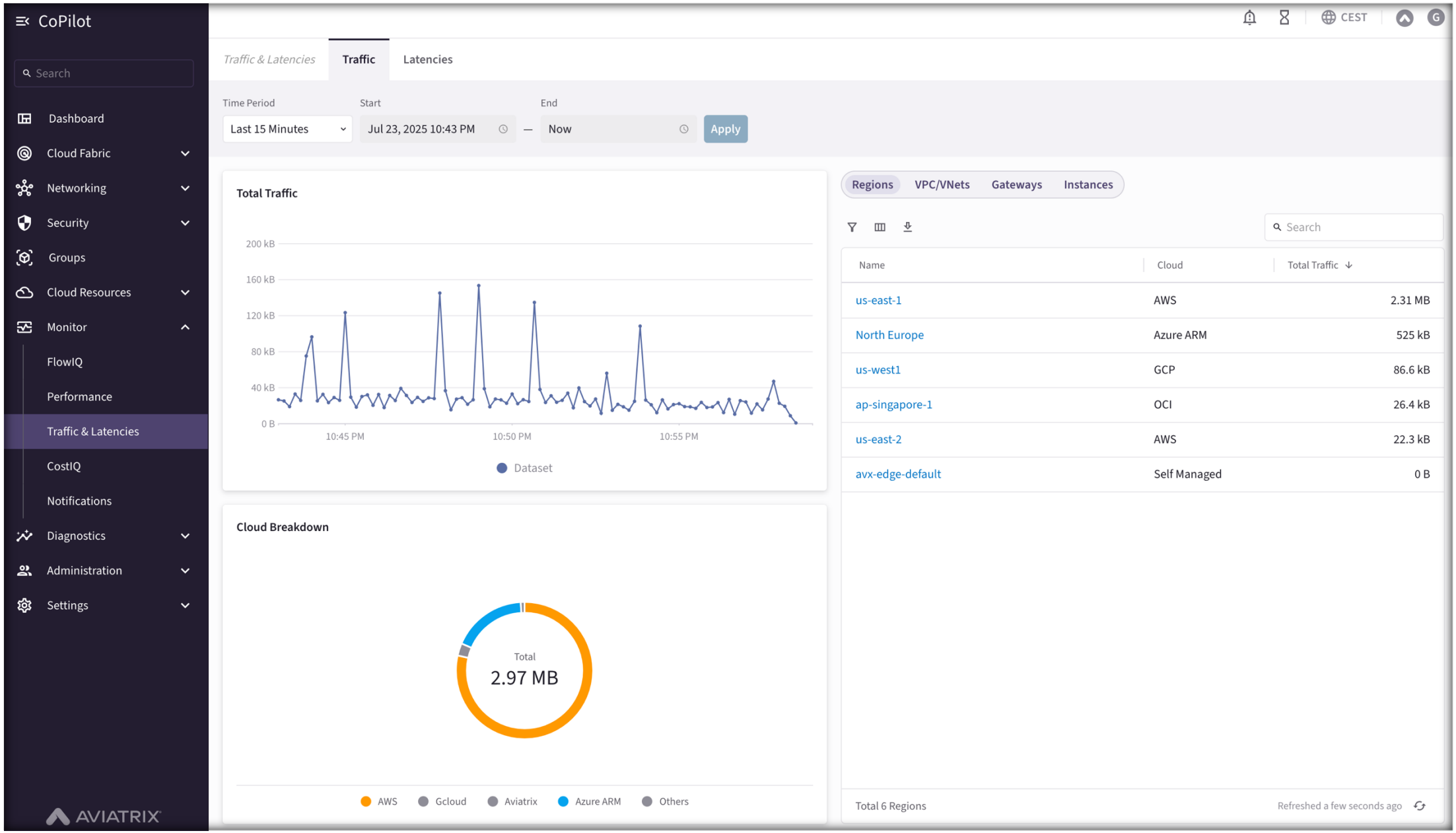
Performance

Performance – Network Metrics and System Metrics

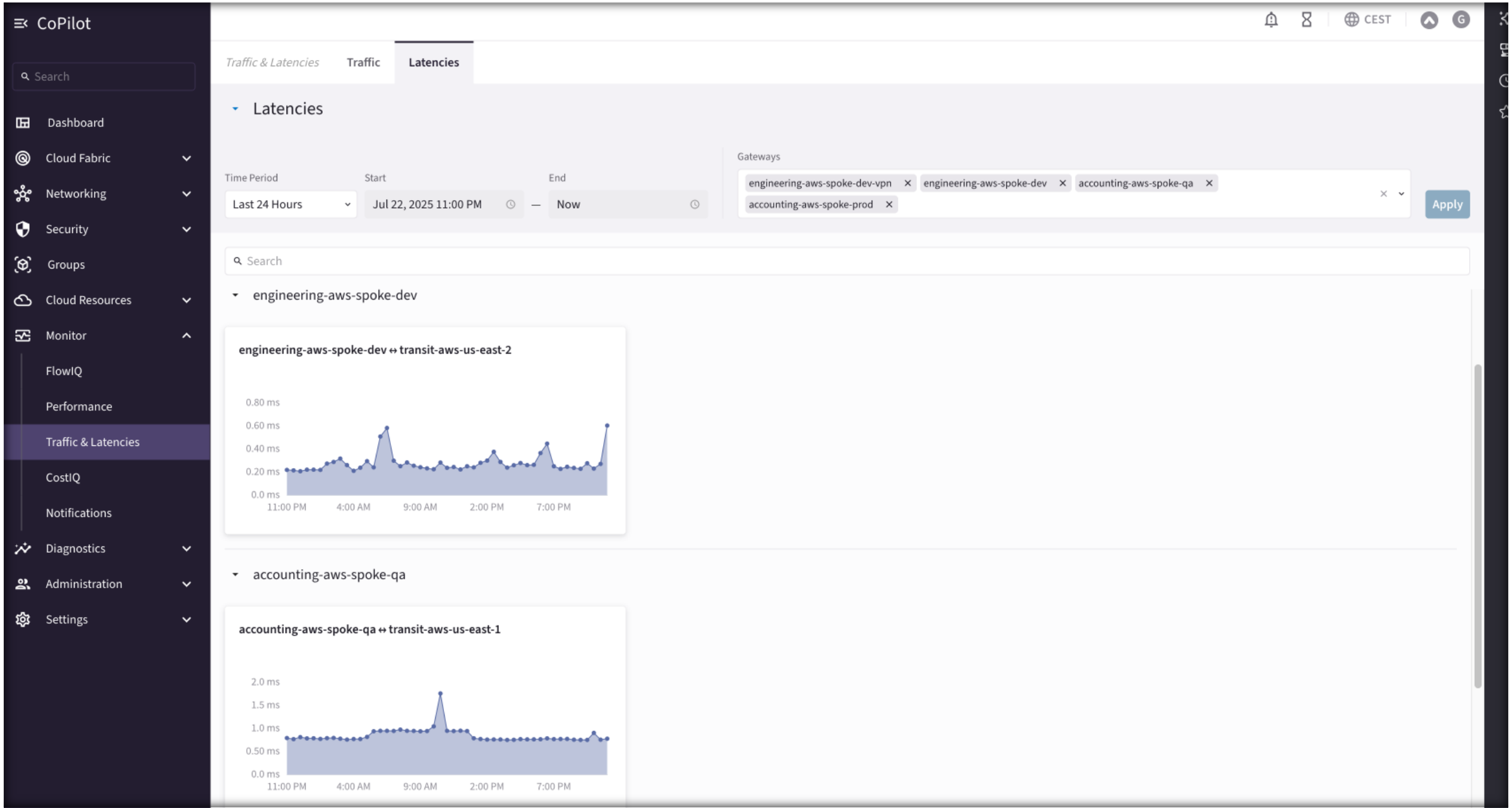


Traffic and Latencies

Traffic

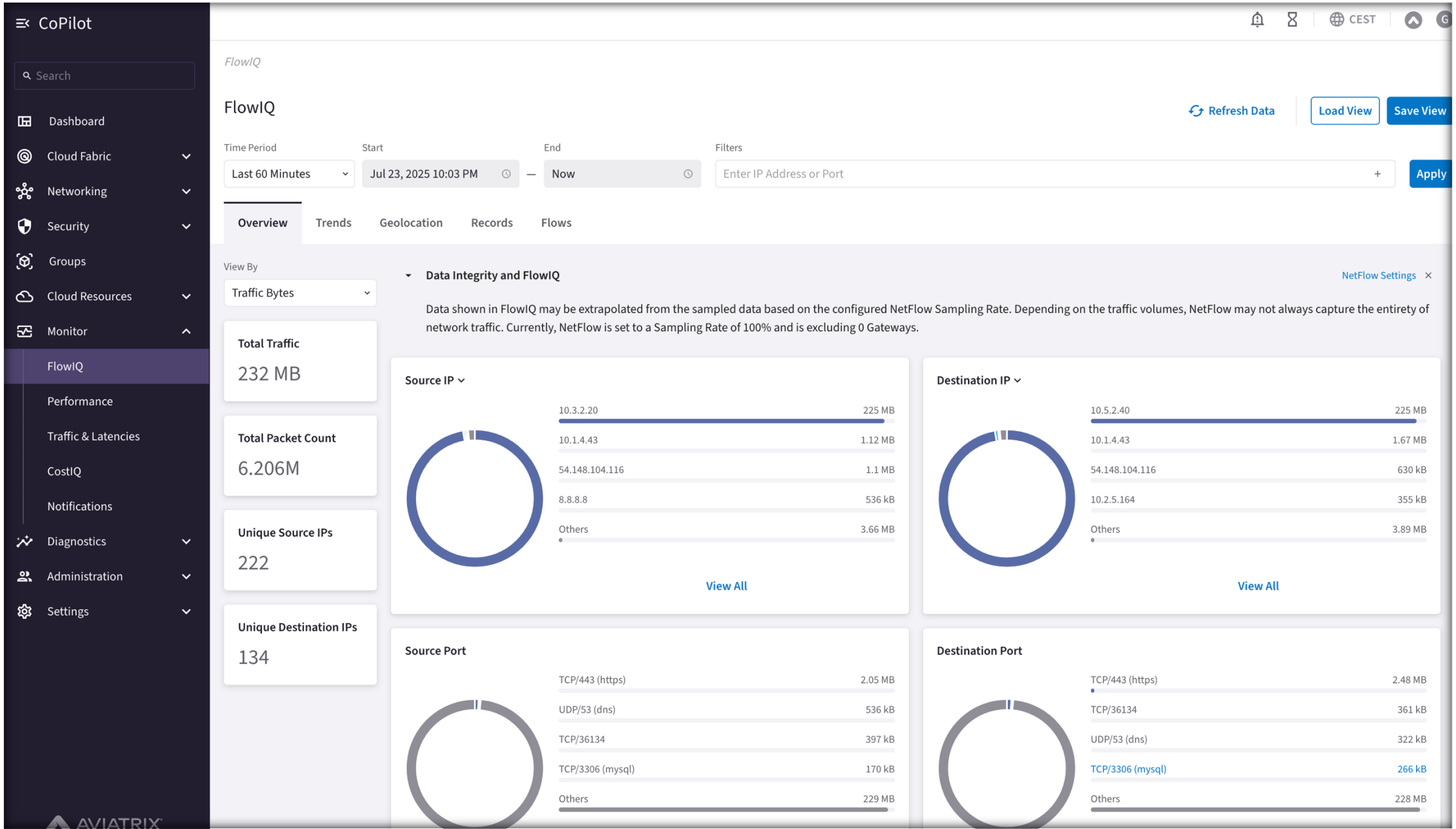

CoPilot
Search
Dashboard
Cloud Fabric
Networking
Security
Groups
Cloud Resources
Monitor
FlowIQ
Performance
Traffic & Latencies
CostIQ
Notifications
Diagnostics
Administration
Settings
AVIATRIX
CEST
Traffic & Latencies
Traffic
Latencies
Time Period
Last 15 Minutes
Start
Jul 23, 2025 10:43 PM
End
Now
Apply
Total Traffic
200 kB
160 kB
120 kB
80 kB
40 kB
0 B
10:45 PM
10:50 PM
10:55 PM
Dataset
Cloud Breakdown
Total
2.97 MB
AWS
Gcloud
Aviatrix
Azure ARM
Others
Regions
VPC/VNets
Gateways
Instances
Search
Name
Cloud
Total Traffic
us-east-1
AWS
2.31 MB
North Europe
Azure ARM
525 kB
us-west1
GCP
86.6 kB
ap-singapore-1
OCI
26.4 kB
us-east-2
AWS
22.3 kB
avx-edge-default
Self Managed
0 B
Total 6 Regions
Refreshed a few seconds ago

Latencies


CoPilot
Search
Dashboard
Cloud Fabric
Networking
Security
Groups
Cloud Resources
Monitor
FlowIQ
Performance
Traffic & Latencies
CostIQ
Notifications
Diagnostics
Administration
Settings
CEST
Traffic & Latencies
Traffic
Latencies
Latencies
Time Period
Last 24 Hours
Start
Jul 22, 2025 11:00 PM
End
Now
Gateways
engineering-aws-spoke-dev-vpn
engineering-aws-spoke-dev
accounting-aws-spoke-qa
accounting-aws-spoke-prod
Apply
Search
engineering-aws-spoke-dev
engineering-aws-spoke-dev ↔ transit-aws-us-east-2
0.80 ms
0.60 ms
0.40 ms
0.20 ms
0.0 ms
11:00 PM
4:00 AM
9:00 AM
2:00 PM
7:00 PM
accounting-aws-spoke-qa
accounting-aws-spoke-qa ↔ transit-aws-us-east-1
2.0 ms
1.5 ms
1.0 ms
0.50 ms
0.0 ms
11:00 PM
4:00 AM
9:00 AM
2:00 PM
7:00 PM

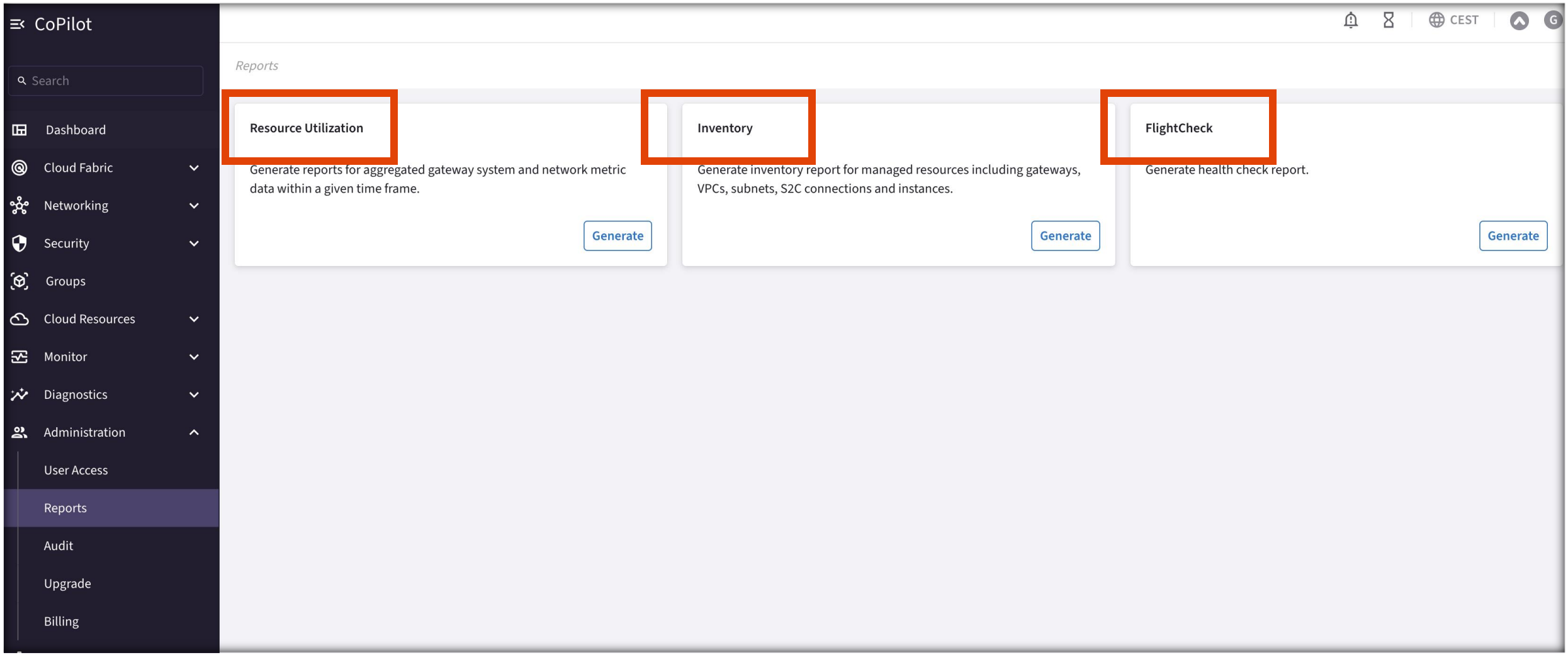
FlowIQ

FlowIQ – CoPilot, collector of Meta Data



Reports

Reports


CoPilot
Search
Dashboard
Cloud Fabric
Networking
Security
Groups
Cloud Resources
Monitor
Diagnostics
Administration
User Access
Reports
Audit
Upgrade
Billing
CEST
G
Reports
Resource Utilization
Generate reports for aggregated gateway system and network metric data within a given time frame.
Generate
Inventory
Generate inventory report for managed resources including gateways, VPCs, subnets, S2C connections and instances.
Generate
FlightCheck
Generate health check report.
Generate

Next: Tenet-7 Least Privilege Access