
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

NET205

Observing and diagnosing your network with AWS

Sohaib Tahir

Principal Solutions Architect, Worldwide Public Sector
Amazon Web Services

Riggs Goodman III

Global Tech Lead, Networking Partner Segments
Amazon Web Services

What you will learn in this session

Understanding of network observability

Network collection and monitoring

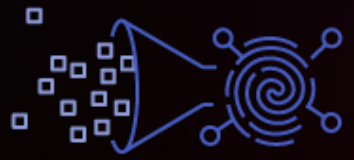
Network analysis and troubleshooting

Overview of network observability

What are customers looking for?

Architect for availability and scale

Understand and optimize costs

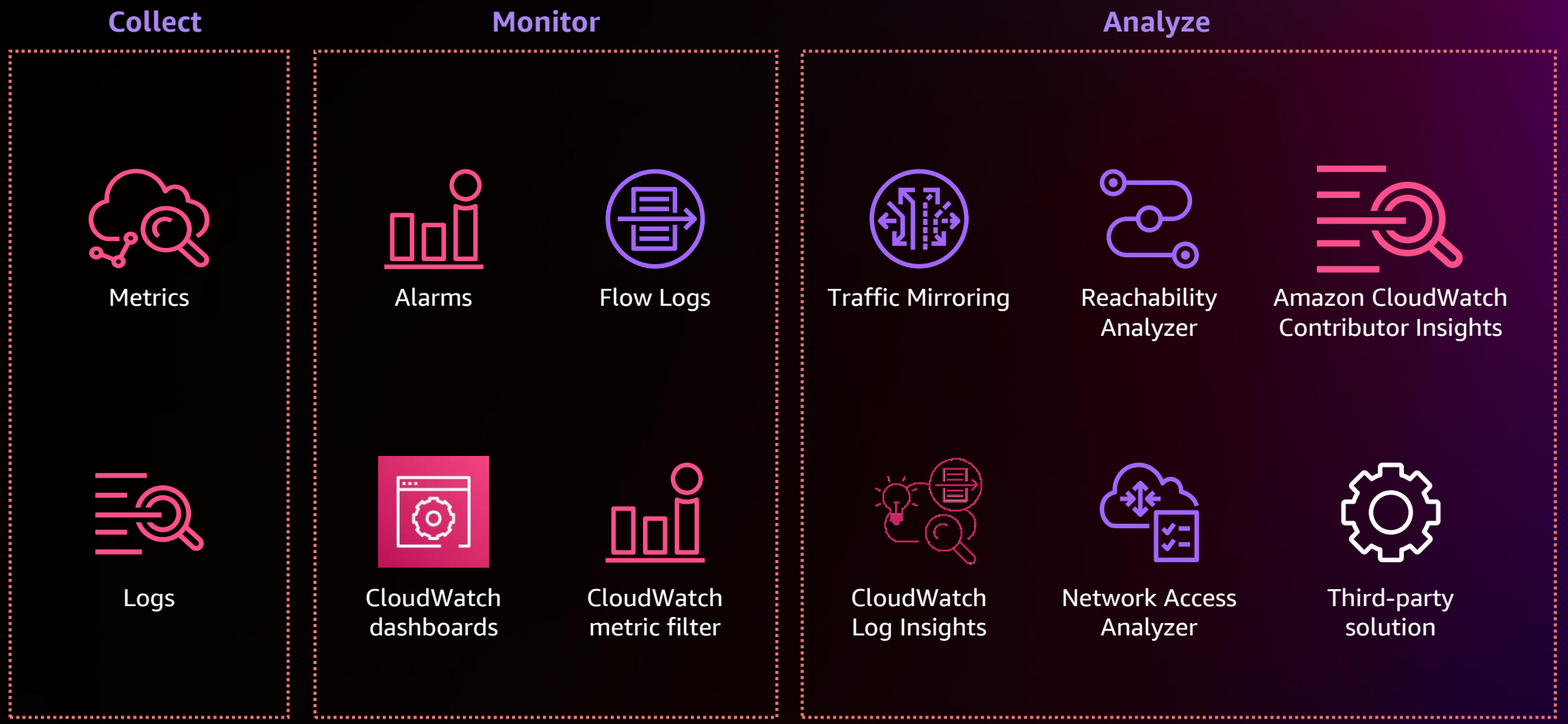


Govern network security

Identify anomalous traffic patterns

Troubleshoot network connectivity and performance

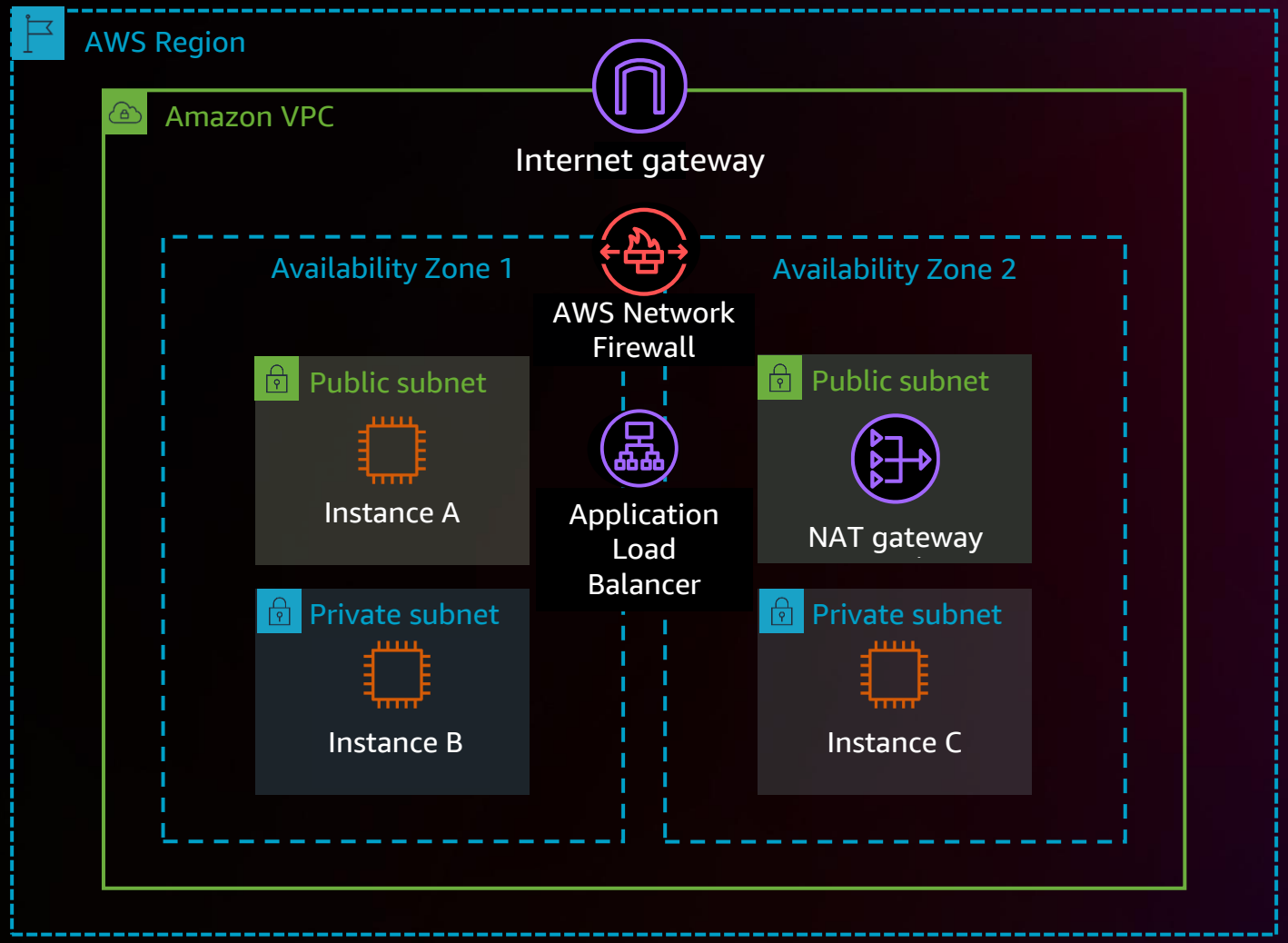
Overview of network observability



Network monitoring

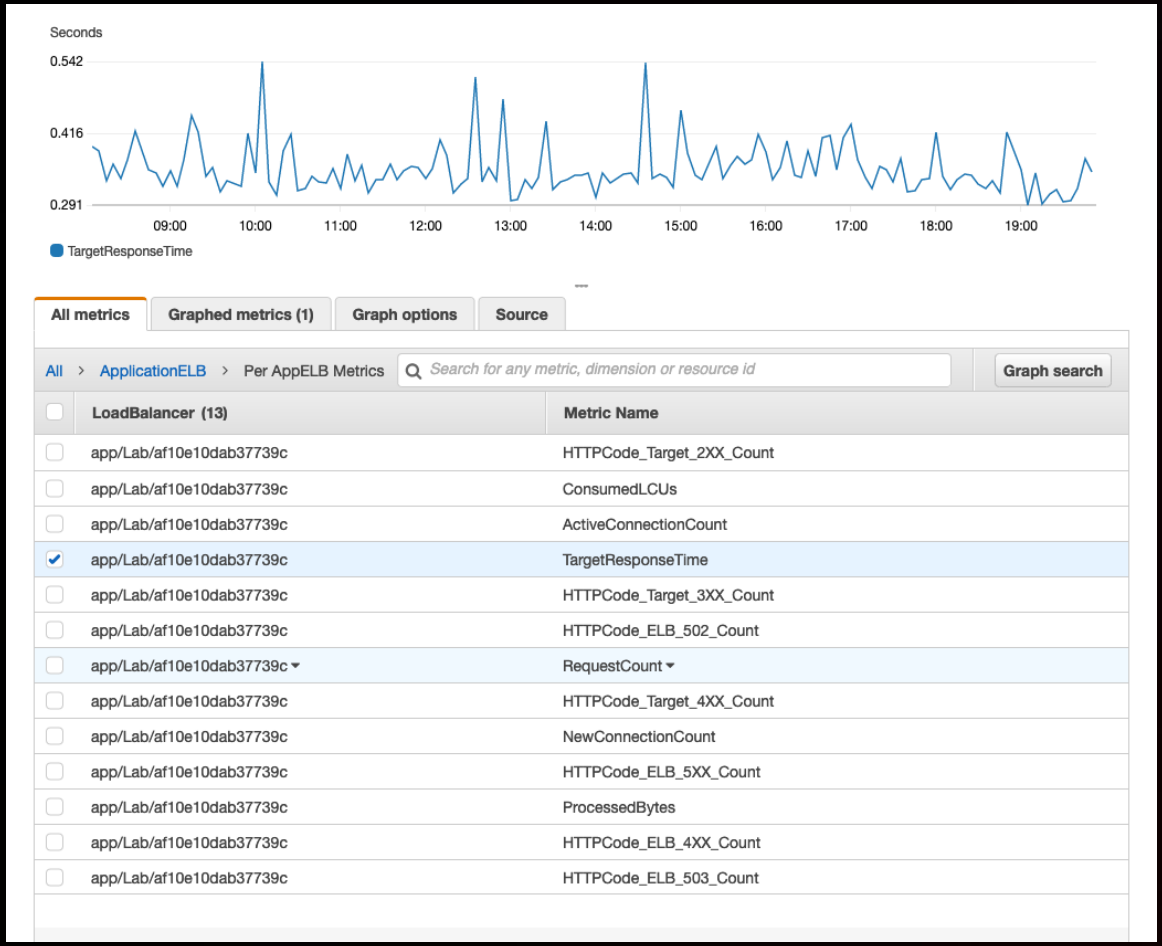
Network monitoring

MONITORING 3-TIER WEB APPLICATION



CloudWatch metrics

BUILT-IN AND CUSTOM METRICS



- Amazon CloudWatch collects default metrics from more than 100 AWS services, including Elastic Load Balancing (ELB), Amazon EC2, AWS Transit Gateway, Amazon VPC (NAT gateways), Amazon Route 53, AWS Network Firewall, AWS Direct Connect, AWS VPN, and so on
- No action is required on your part
- Publish custom metrics to CloudWatch

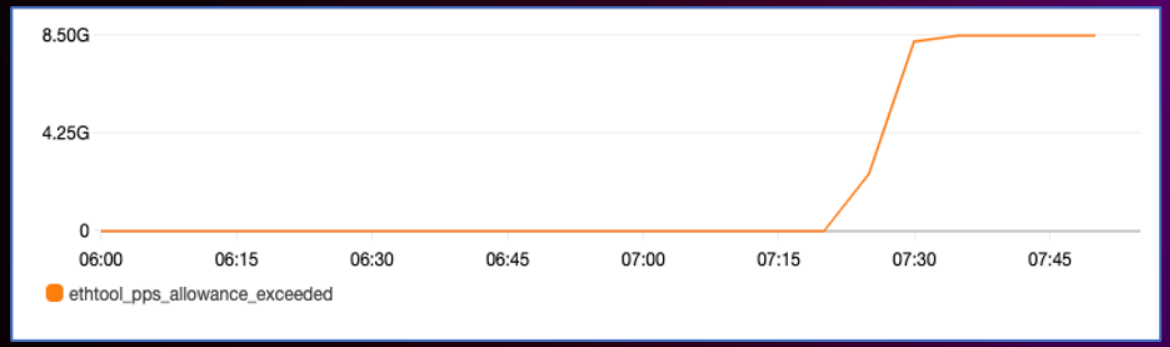
Amazon EC2 metrics

INSTANCE-LEVEL NETWORK PERFORMANCE METRICS

Amazon EC2 provides instance-level network metrics via CloudWatch

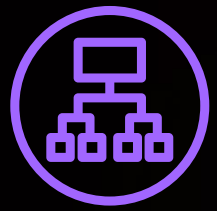
With Elastic Network Adapter (ENA), gain insights into traffic drops when network allowances are exceeded

- Instance bandwidth capability
- Packet-per-second (PPS) performance
- Connections tracked
- Link-local service access



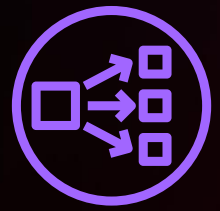
Elastic Load Balancing (ELB)

CLOUDWATCH METRICS



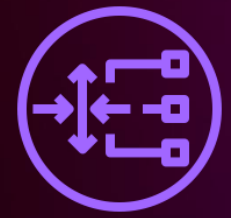
Application
Load Balancer

Connections
Load balancer capacity units (LCUs)
Header details
HTTP counts
Error codes
Bytes



Network
Load Balancer

Flows
LCUs
Healthy hosts
Bytes
Packets per second
Resets
TLS

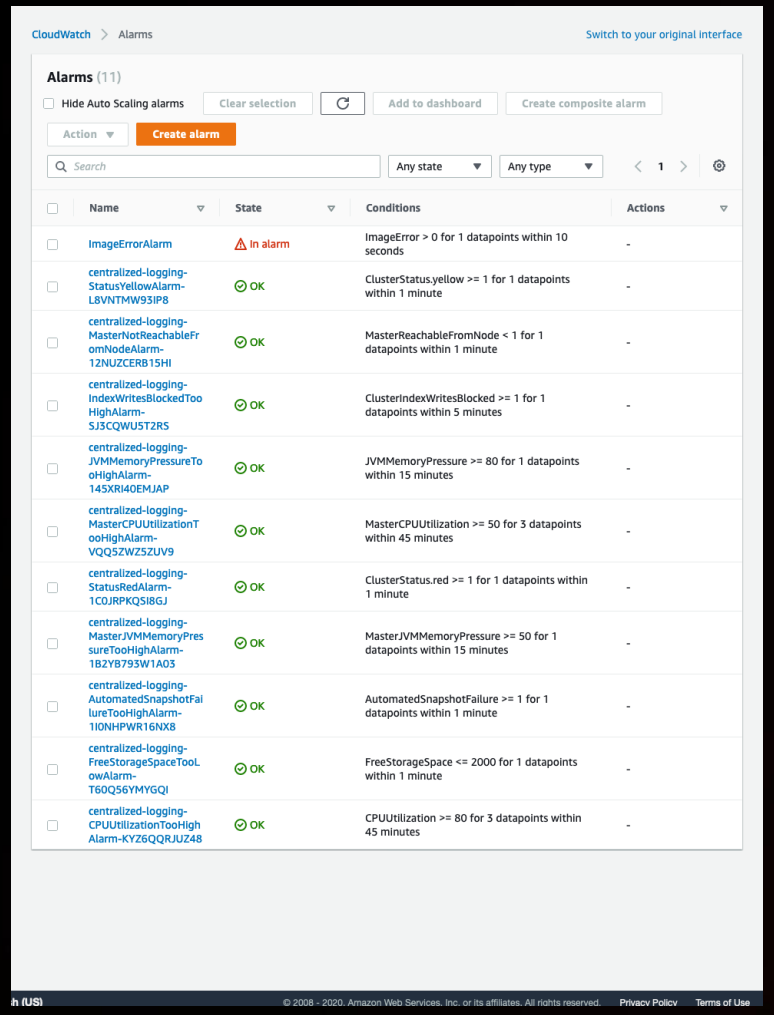


Gateway
Load Balancer

Flows
LCUs
Healthy hosts
Bytes

CloudWatch alarms

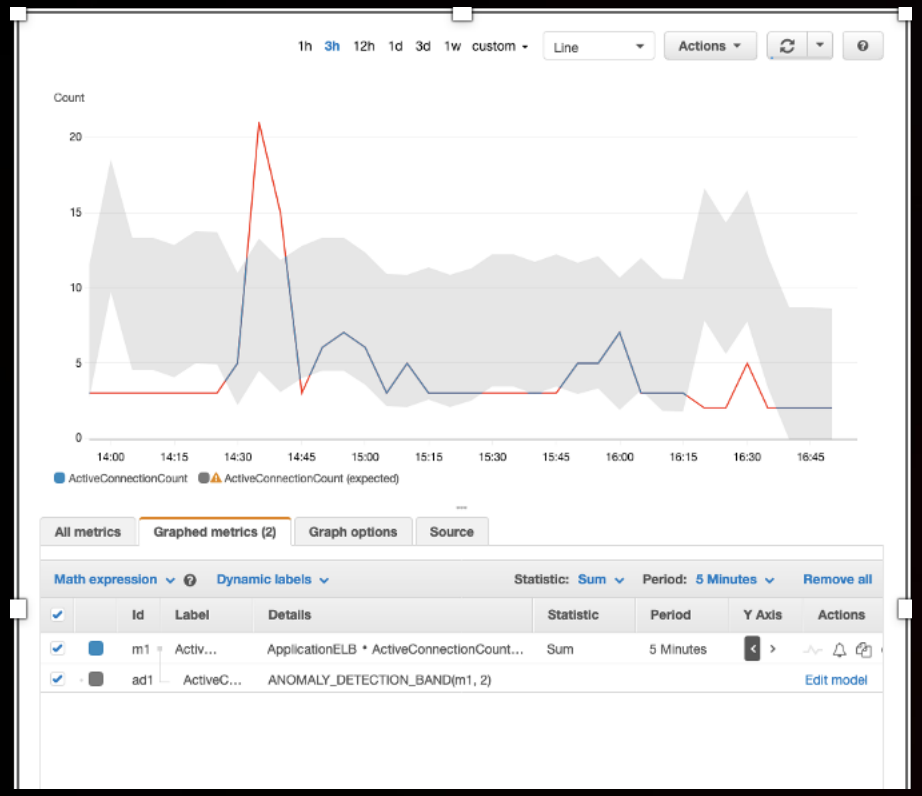
HIGH-RESOLUTION ALARMS



Amazon CloudWatch alarms allow you to set a threshold on metrics and invoke an action

- Watch a single metric or the result of a math expression
- Perform actions based on the value of metrics
  - Send a notification to an Amazon SNS topic
  - Amazon EC2 Auto Scaling action
  - EC2 action (stop, terminate, reboot, or recover)
- Add alarms to dashboards to visualize them

CloudWatch anomaly detection



- CloudWatch anomaly detection applies statistical and machine learning algorithms to the metric's past data to create a model of the metric's expected values
- Choose when to invoke an alarm – when the metric value is above the band of expected values, below the band, or both
- Anomaly detection algorithms account for the seasonality and trend changes of metrics

Network logs

ELASTIC LOAD BALANCING (ELB) ACCESS LOGS

- ELB provides access logs
- Log contains information such as the request time, the client's IP address, latencies, request paths, and server responses
- Analyze traffic patterns and troubleshoot issues
- Store access logs in Amazon S3 bucket

Example HTTP Entry

The following is an example log entry for an HTTP listener (port 80 to port 80):

```
http 2018-07-02T22:23:00.186641Z app/my-loadbalancer/50dc6c495c0c9188
192.168.131.39:2817 10.0.0.1:80 0.000 0.001 0.000 200 200 34 366
"GET http://www.example.com:80/ HTTP/1.1" "curl/7.46.0" - -
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067
"Root=1-58337262-36d228ad5d99923122bbe354" "-" "-"
0 2018-07-02T22:22:48.364000Z "forward" "-" "-" "10.0.0.1:80" "200" "-" "-"
```

Example HTTPS Entry

The following is an example log entry for an HTTPS listener (port 443 to port 80):

```
https 2018-07-02T22:23:00.186641Z app/my-loadbalancer/50dc6c495c0c9188
192.168.131.39:2817 10.0.0.1:80 0.086 0.048 0.037 200 200 0 57
"GET https://www.example.com:443/ HTTP/1.1" "curl/7.46.0" ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067
"Root=1-58337281-1d84f3d73c47ec4e58577259" "www.example.com" "arn:aws:acm:us-east-2:123456789012:certificate/12345678-12
1 2018-07-02T22:22:48.364000Z "authenticate,forward" "-" "-" "10.0.0.1:80" "200" "-" "-"
```

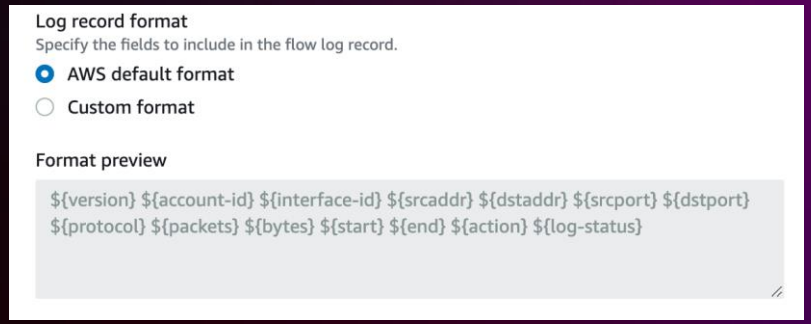
Example HTTP/2 Entry

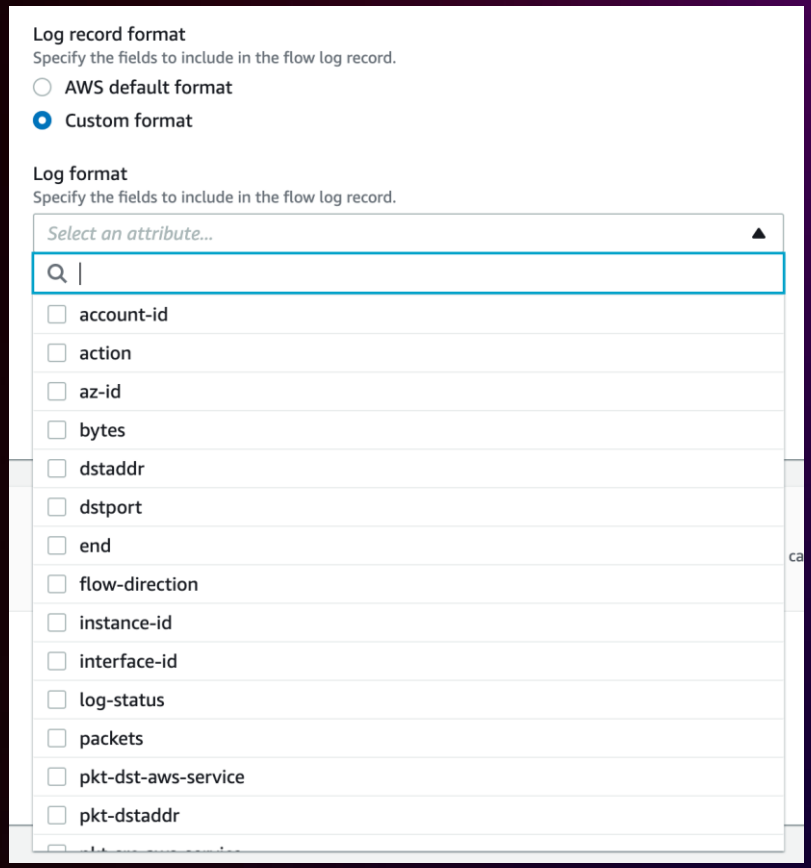
The following is an example log entry for an HTTP/2 stream.

```
h2 2018-07-02T22:23:00.186641Z app/my-loadbalancer/50dc6c495c0c9188
10.0.1.252:48160 10.0.0.66:9000 0.000 0.002 0.000 200 200 5 257
"GET https://10.0.2.105:773/ HTTP/2.0" "curl/7.46.0" ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067
"Root=1-58337327-72bd00b0343d75b906739c42" "-" "-"
1 2018-07-02T22:22:48.364000Z "redirect" "https://example.com:80/" "-" "10.0.0.66:9000" "200" "-" "-"
```

Flow logs

- Supported for Amazon VPC and AWS Transit Gateway
- Capture non-real-time metadata information about the IP traffic for your VPC and transit gateway
- Provides better visibility of network traffic patterns; monitor network security and troubleshoot issues
- Flow log data can be published to Amazon CloudWatch Logs, Amazon S3, and Amazon Kinesis Data Firehose





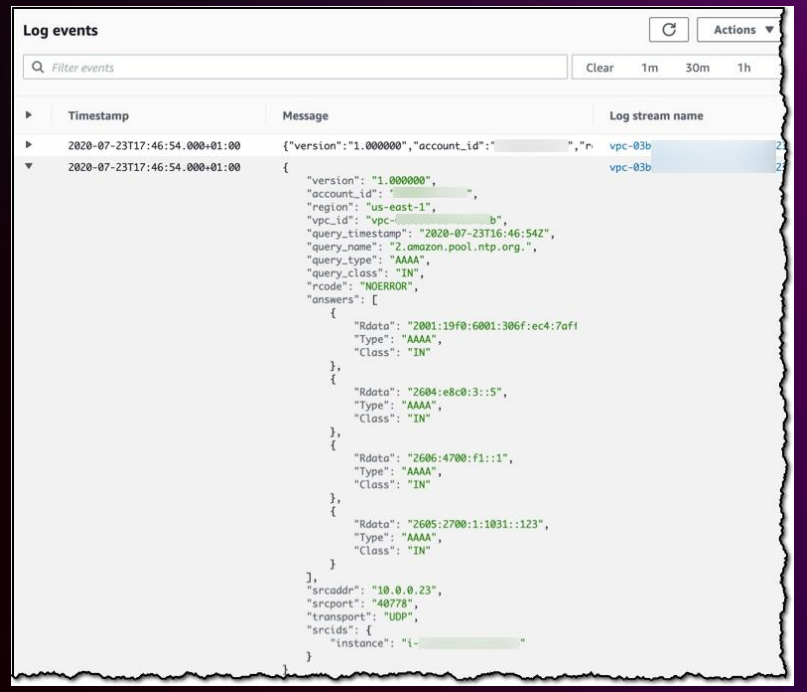
Route 53 query logs

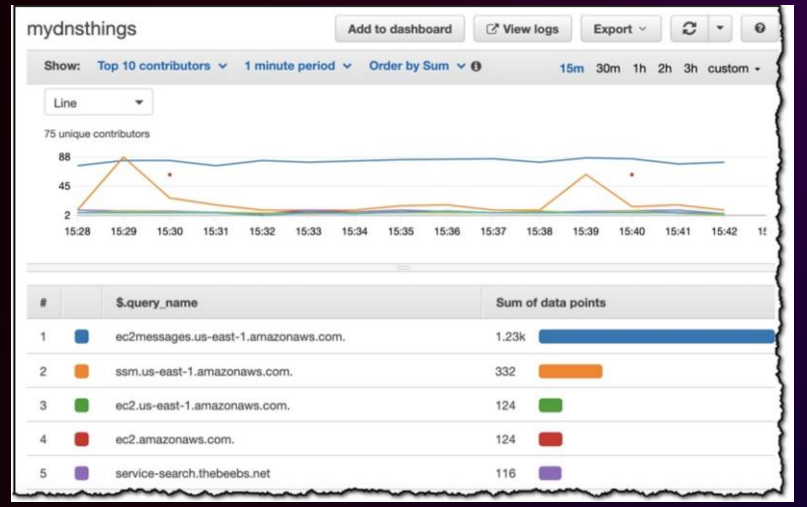
Public DNS query logs

- Log information about the public DNS queries that Route 53 receives
- Publish public DNS query logs to Amazon CloudWatch Logs and use tools like Contributor Insights

Resolver query logs

- Queries that originate in Amazon VPCs, use inbound Resolver endpoint, outbound Resolver endpoint, and Route 53 Resolver DNS Firewall
- Ship query logs to CloudWatch Logs, Amazon S3, and Kinesis Data Firehose delivery stream

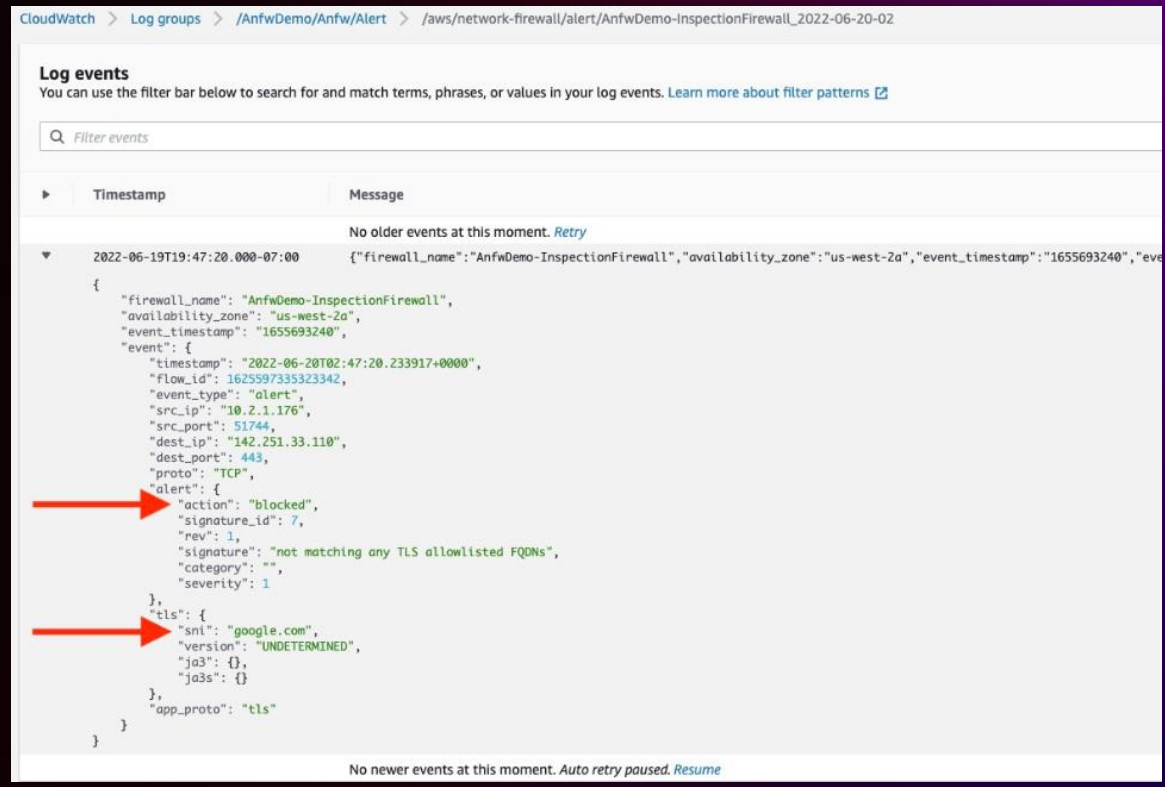




Network logs

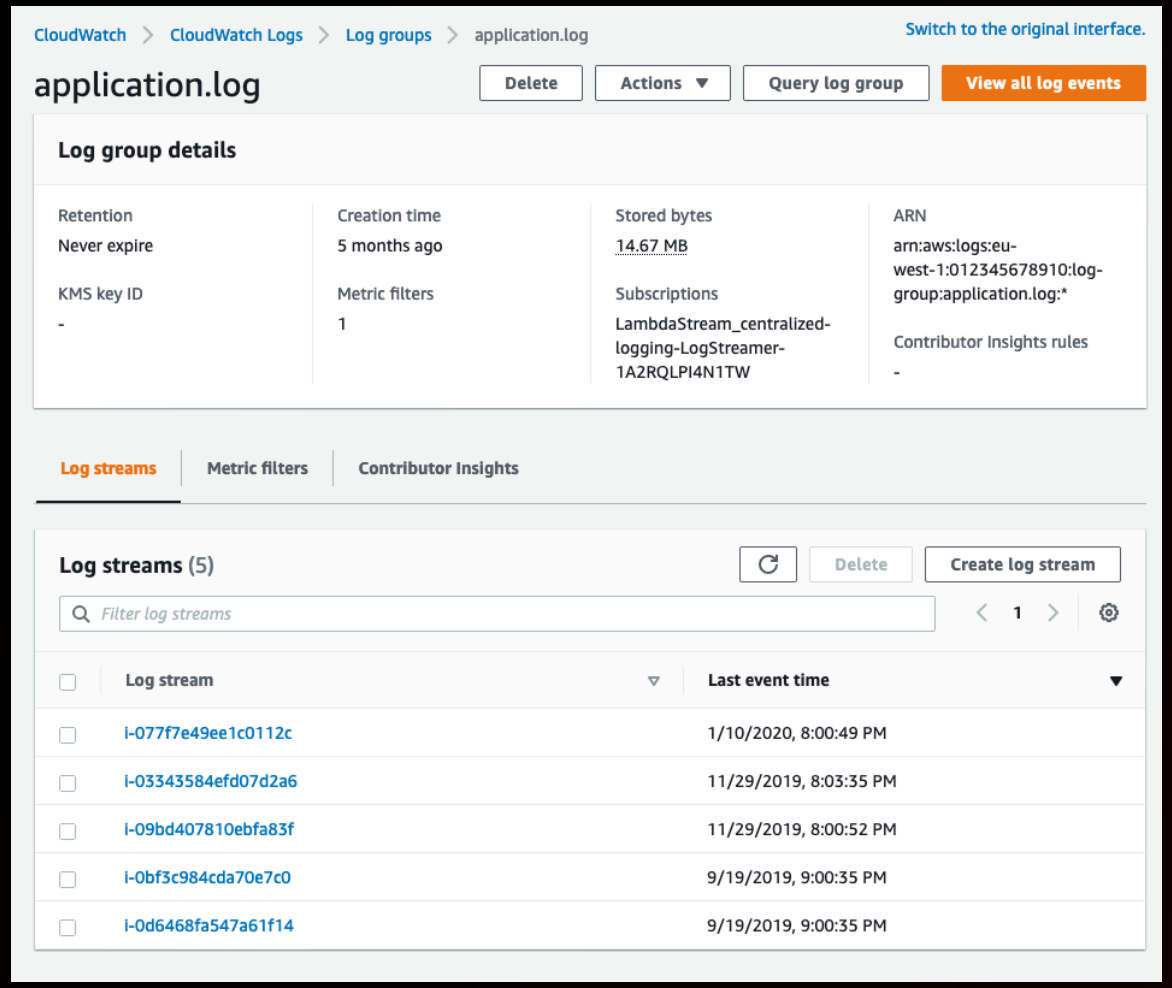
AWS NETWORK FIREWALL

- AWS Network Firewall provides flow logs and alert logs for firewall stateful engine
- Network Firewall also provides metrics on the number of packets passed, dropped, received, etc.
- Network Firewall logs can be sent to CloudWatch Logs, Kinesis Data Firehose, or Amazon S3



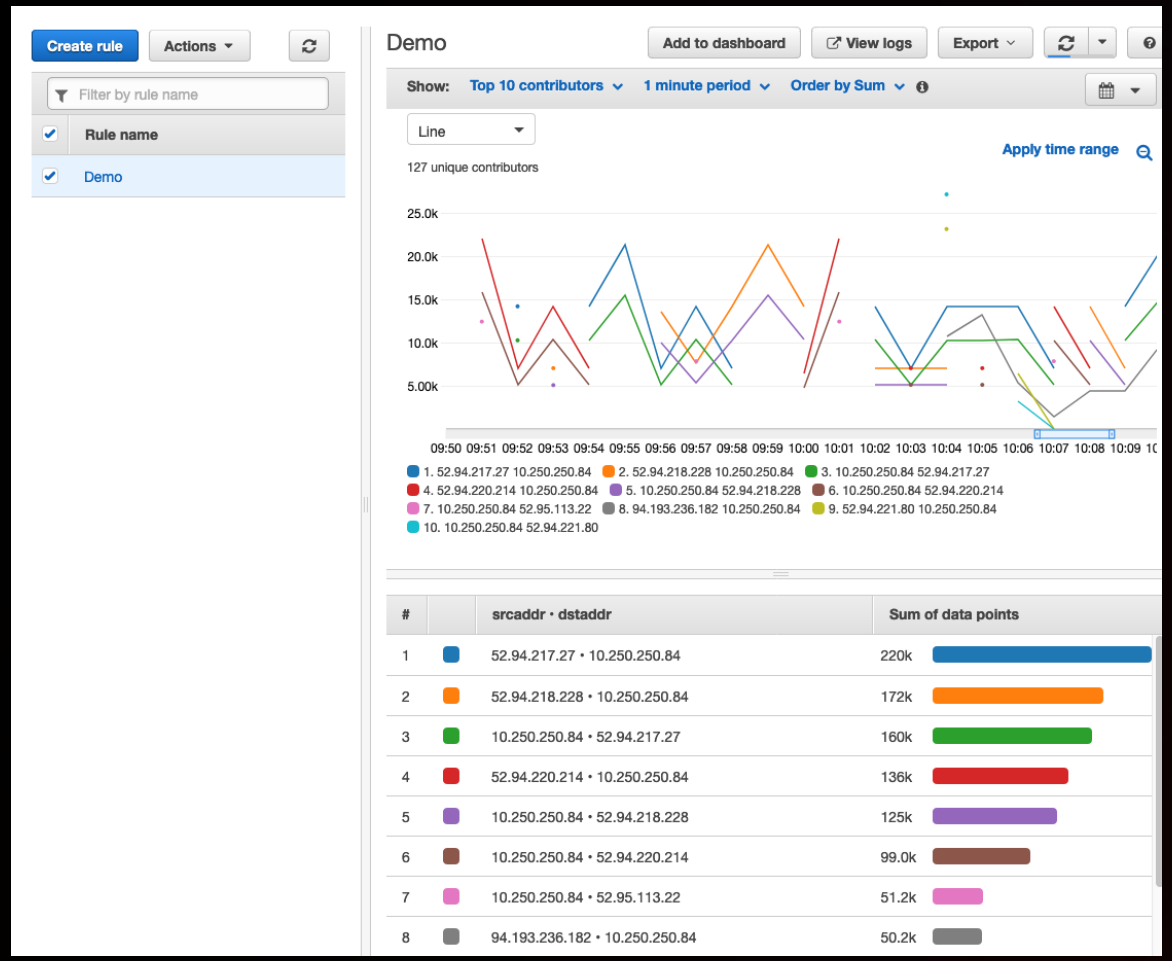
Network logs

CLOUDWATCH LOGS – EASILY COLLECT AND STORE LOGS



- Centralize the logs from all of your systems
- Search and filter logs in one place
- Archive logs for long-term retention
- Query, sort, and visualize log data in dashboards

CloudWatch Contributor Insights

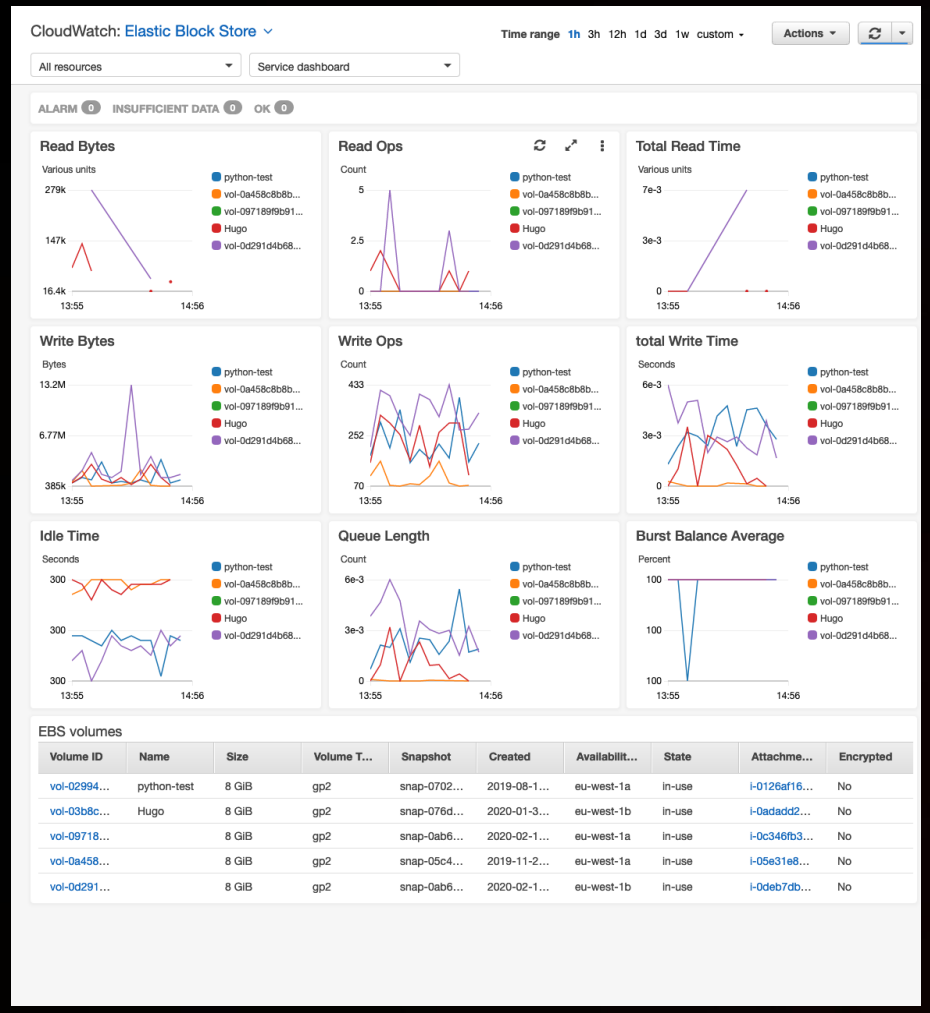


Analyzes time-series data to provide a view of the top contributors influencing system performance

- Runs continuously without needing user intervention
- Understand who or what is impacting your system
- Evaluate patterns in structured log events
- Display on CloudWatch dashboards
- Add to CloudWatch alarms

CloudWatch dashboards

UNIFIED OPERATIONAL VIEW WITH DASHBOARDS



- Create reusable graphs and visualize your cloud resources and applications in a unified view
- Include metrics, alarms, logs, and contributor insights in your dashboard
- Create cross-account cross-Region dashboards for network infrastructure and applications
- Share dashboards with team members to help respond to operational events

Bringing it all together

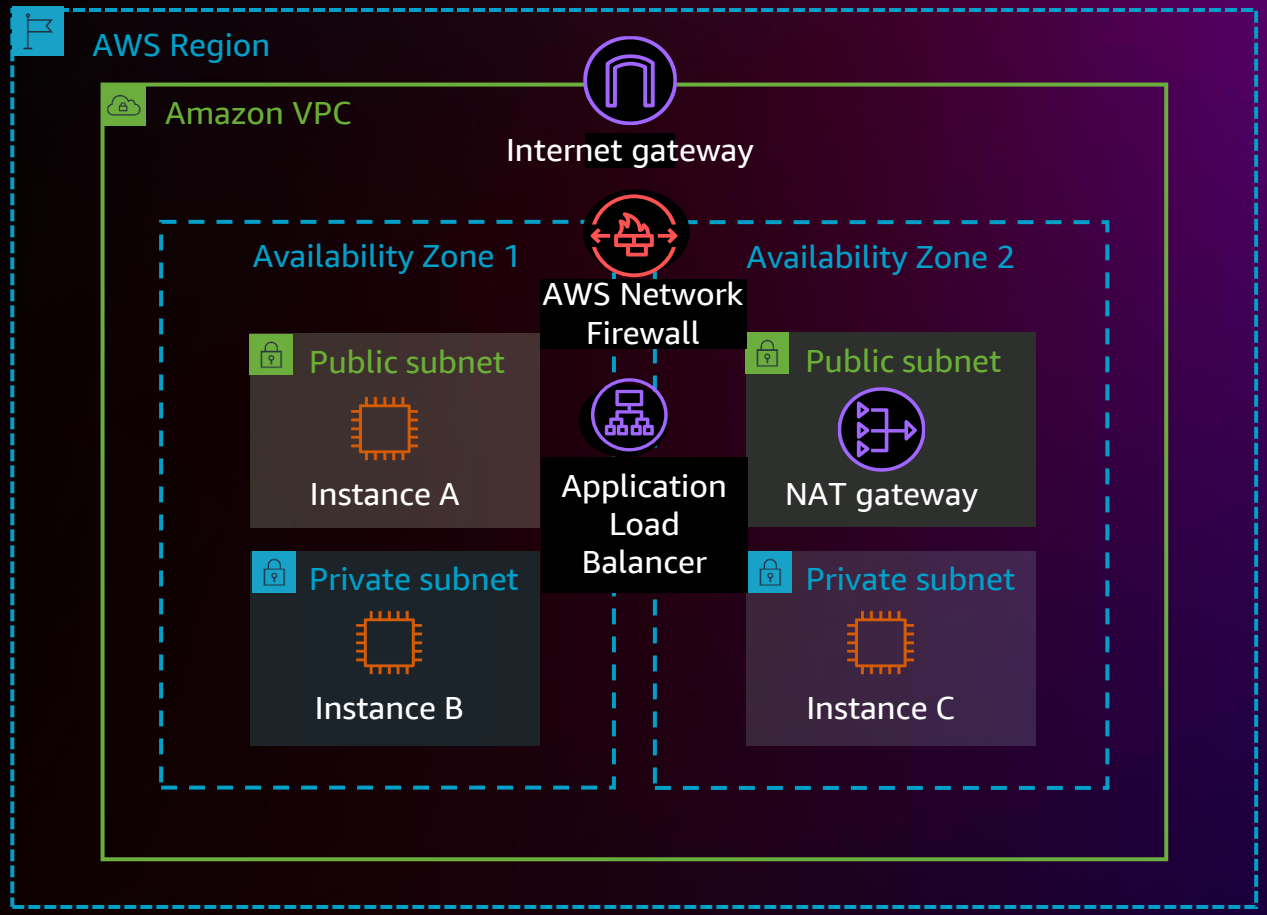
MONITORING 3-TIER WEB APPLICATIONS

Metrics and alarms

- Identify CloudWatch metrics that help instrument your workload performance and align with your monitoring goals
- Create alarms for AWS Network Firewall, Application Load Balancer, Amazon EC2, and NAT gateway metrics
- Add metrics and alarms to CloudWatch dashboard

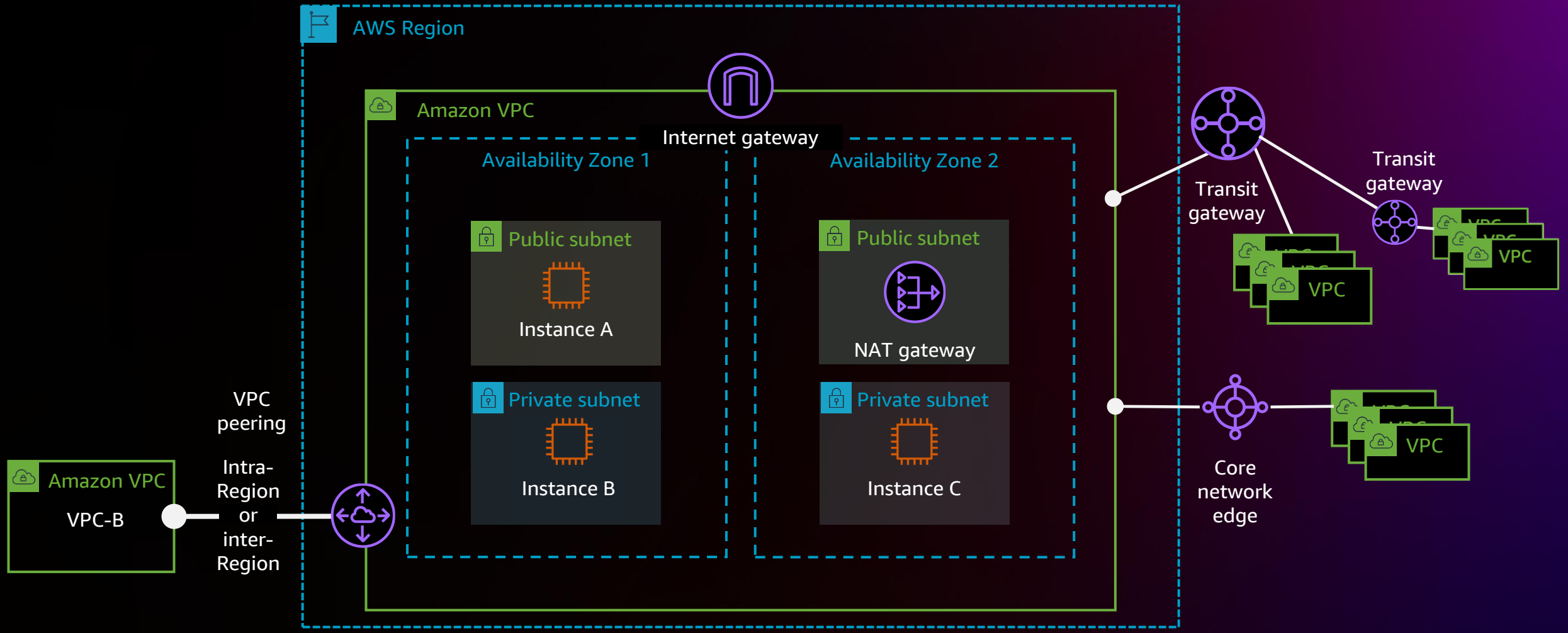
Logs and dashboard

- Enable logs for AWS Network Firewall, Application Load Balancer, Amazon VPC, and Route 53
- Push application logs to CloudWatch logs
- Use CloudWatch Contributor Insights to identify top talkers
- Add logs and insights to CloudWatch dashboard

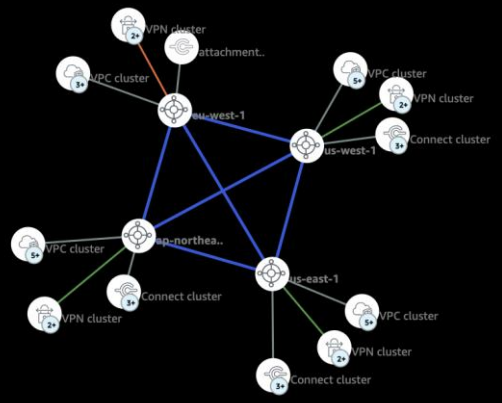


Network monitoring

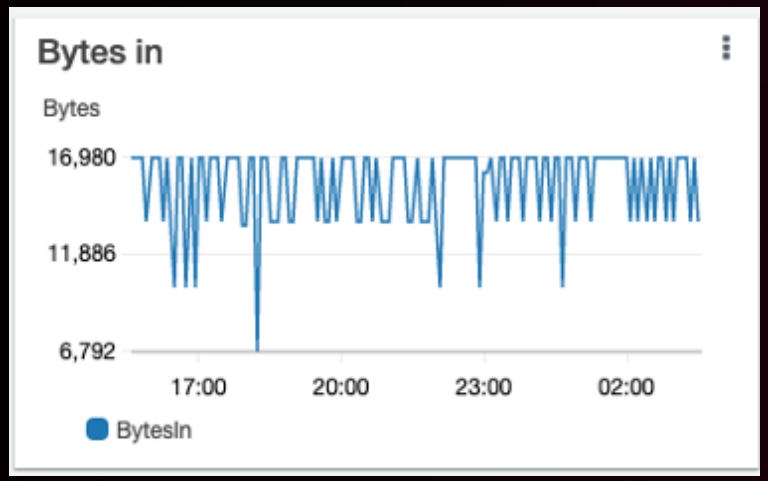
MONITORING NETWORKS ACROSS YOUR ORGANIZATION AND REGIONS



AWS Network Manager



Topologies

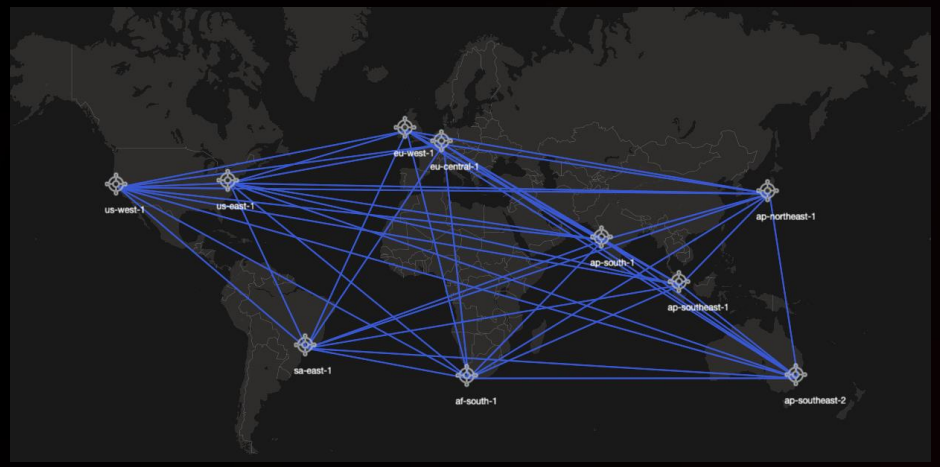


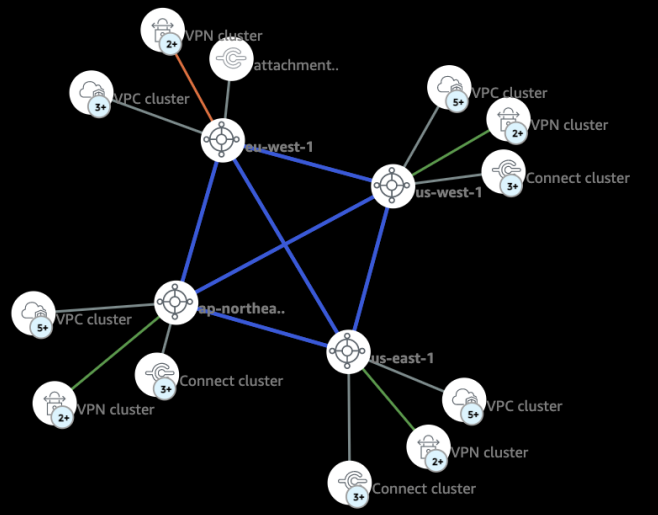
Metrics

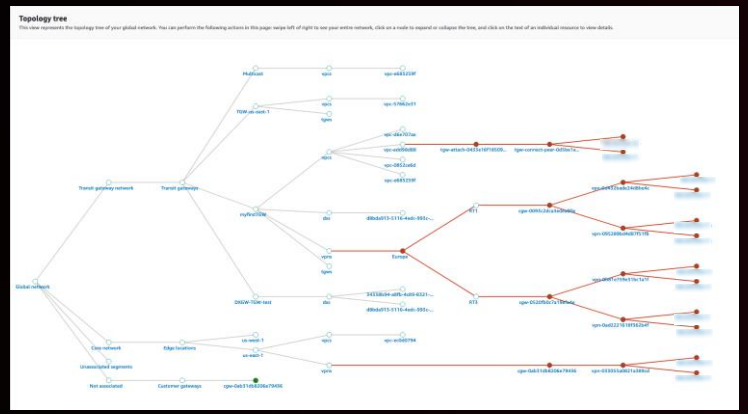
Events

AWS Network Manager

TOPOLOGY AND DASHBOARD







Dashboard

- Physical locations
- Devices and links
- Supports AWS Cloud WAN and Transit Gateway

Topology graph

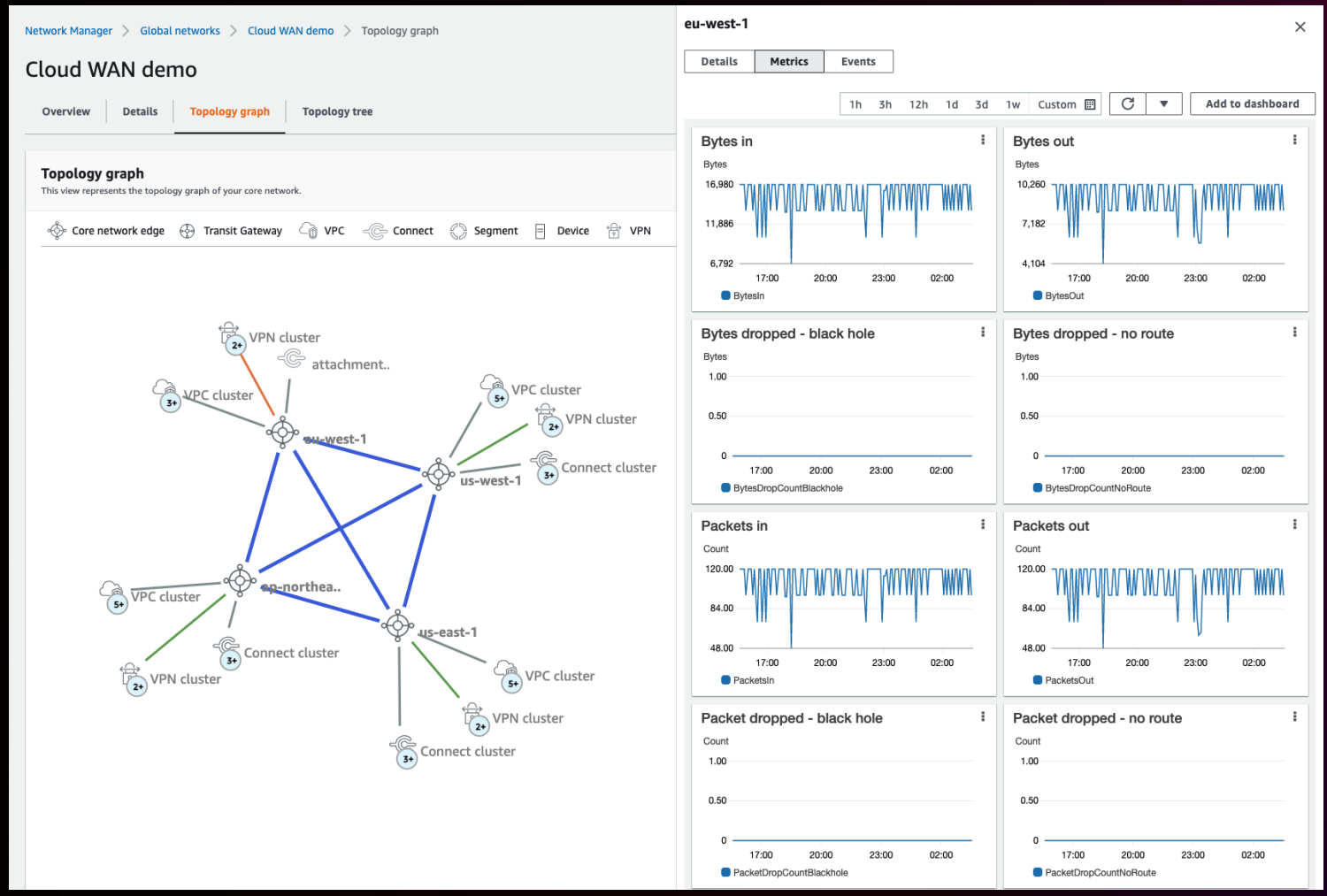
- AWS Regions
- Attachments
- Cross-Region peering
- Segments (optional)

Topology tree

- Logical diagram

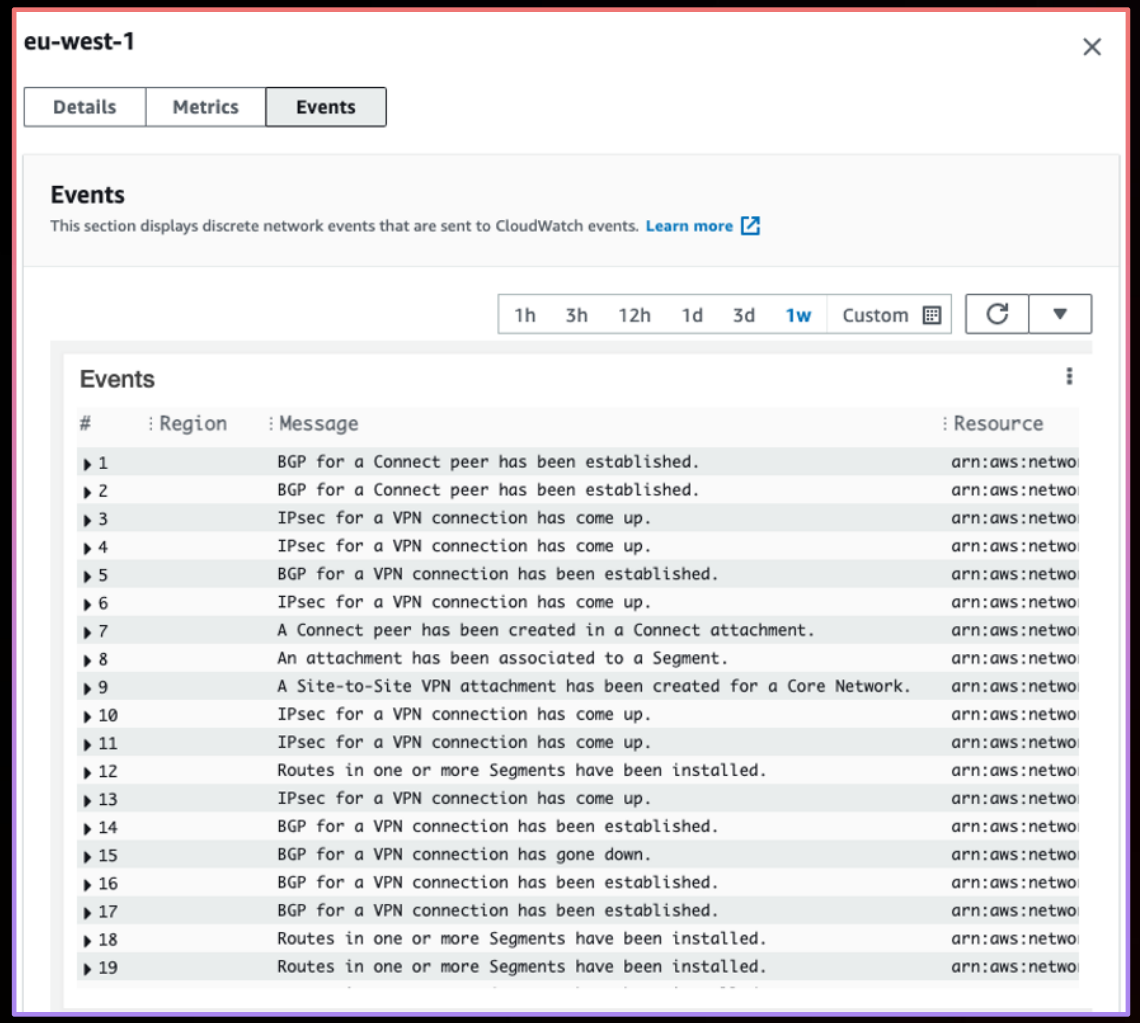
AWS Network Manager

METRICS



AWS Network Manager

EVENTS

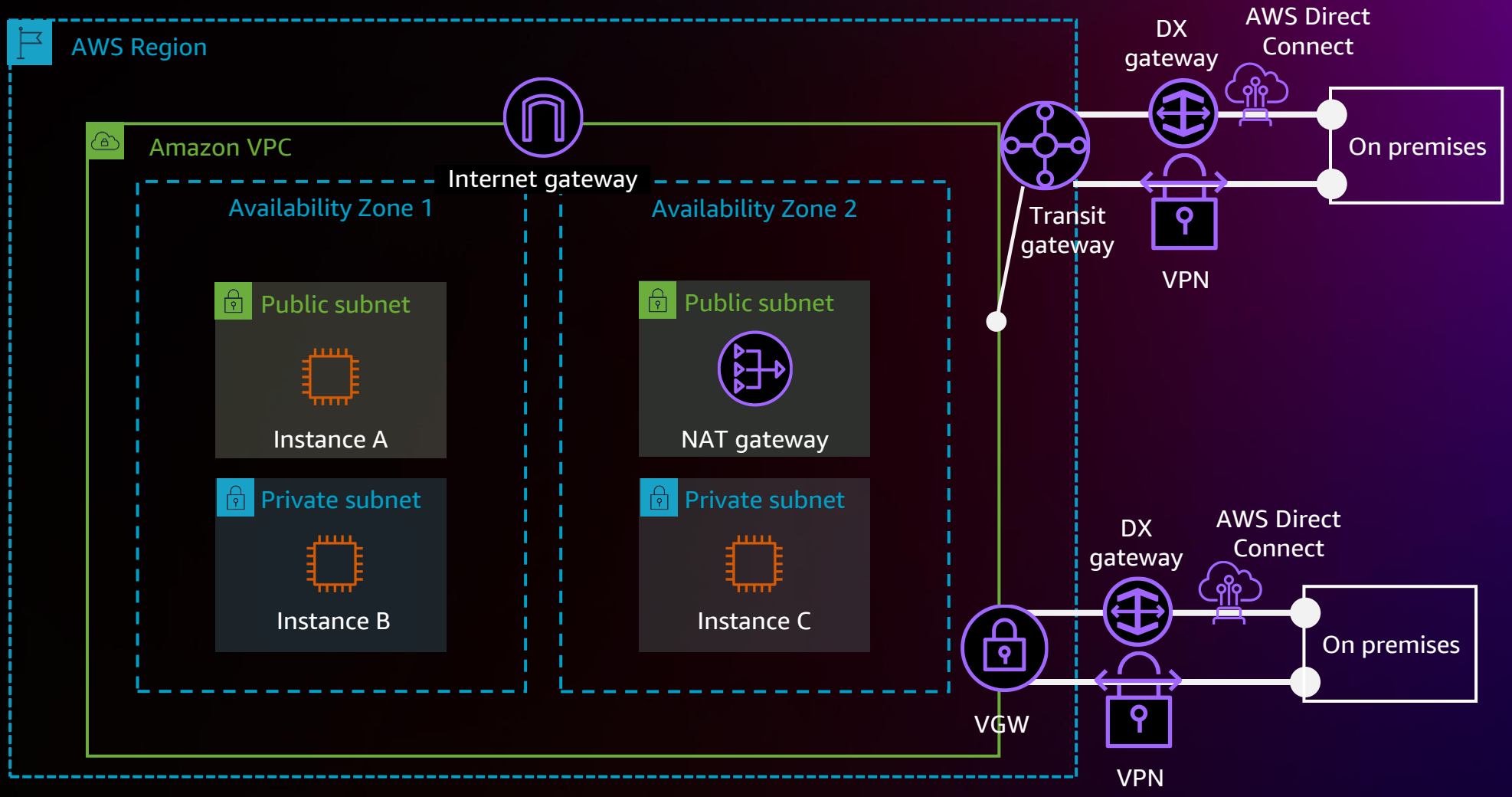


- Network events
- Topology changes
- Policy changes
- Attachment events
  - Approvals
  - Tag changes
- Route changes
  - Peering
  - BGP updates (attributes, etc.)

Changes available in Amazon EventBridge

Network monitoring

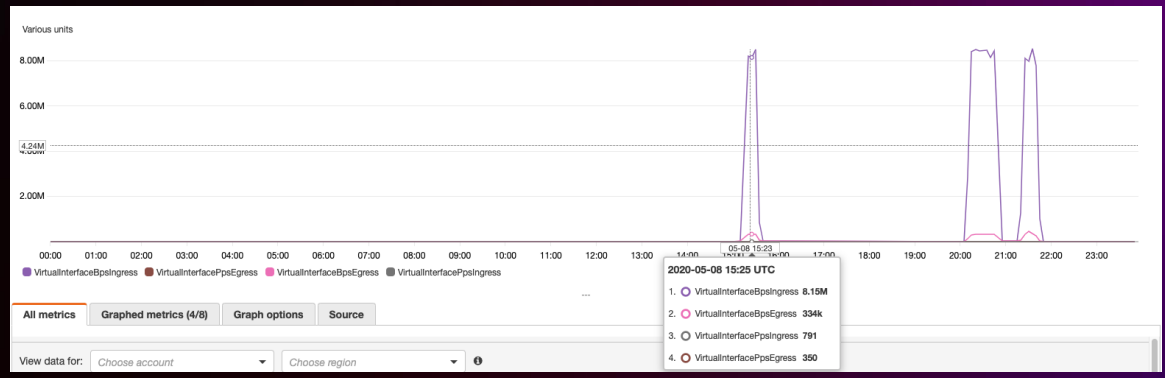
HYBRID CONNECTIVITY

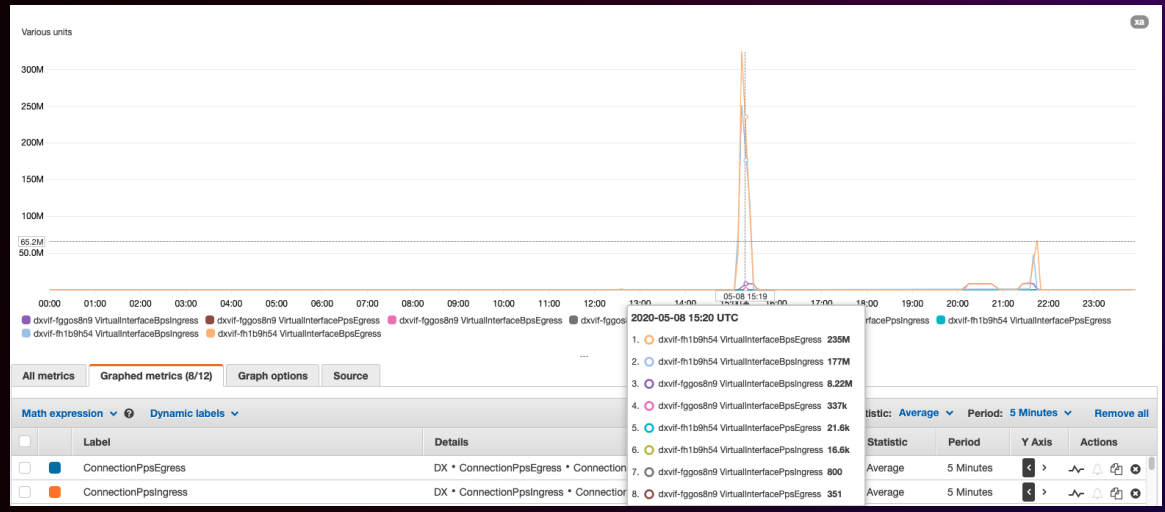


AWS Site-to-Site VPN and AWS Direct Connect

METRICS

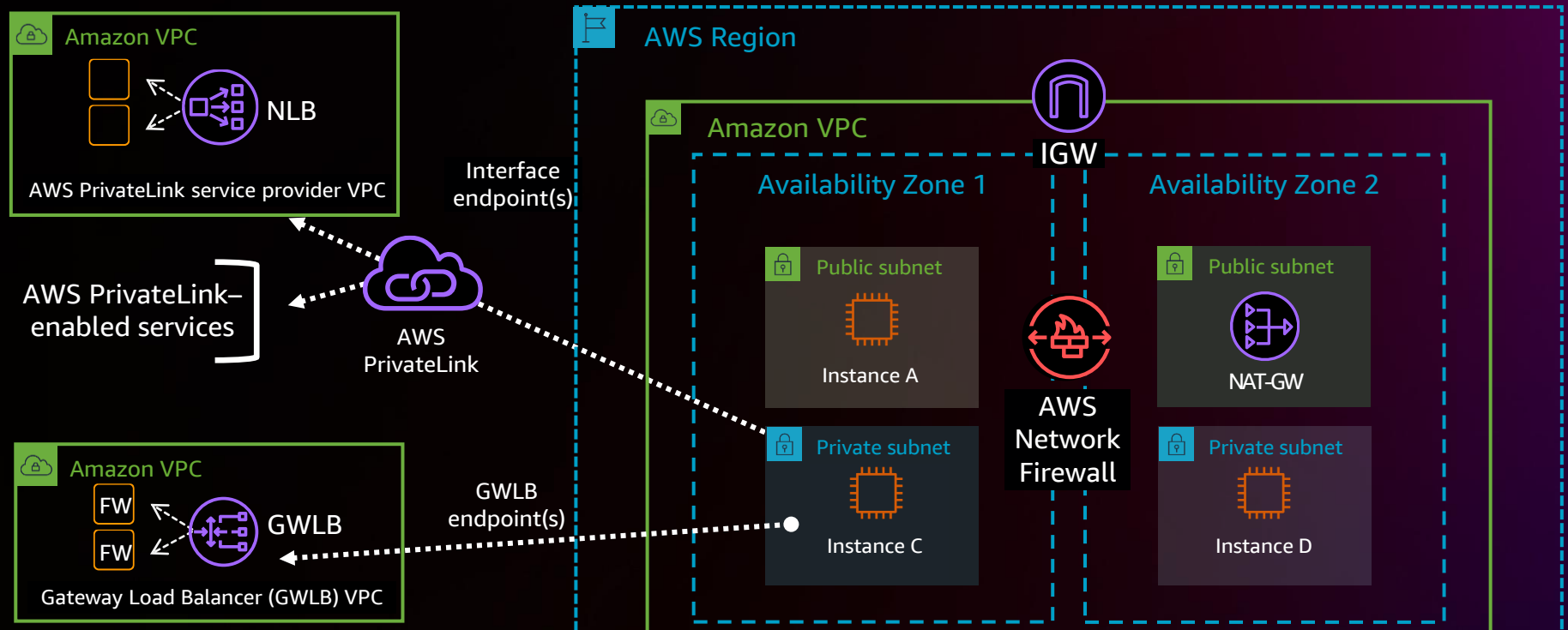
- AWS Site-to-Site VPN and AWS Direct Connect provide CloudWatch metrics for monitoring connection state and bandwidth
- AWS Direct Connect provides metrics to monitor both physical and virtual interfaces (VIFs)
- AWS Site-to-Site VPN logs provide details about IPSec, IKE, and DPD protocols





Network monitoring

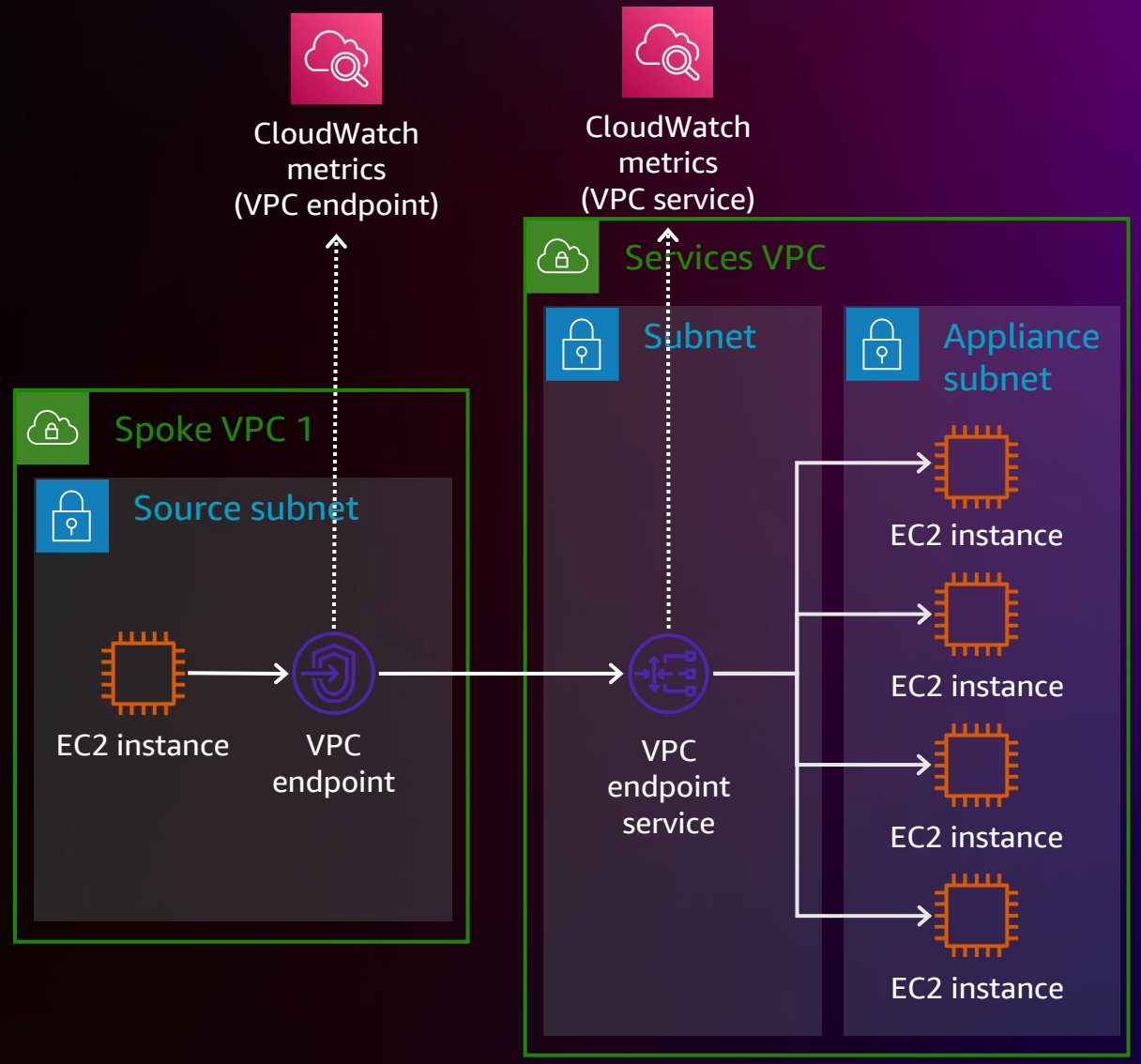
ENDPOINT SERVICES



AWS PrivateLink and Gateway Load Balancer

METRICS

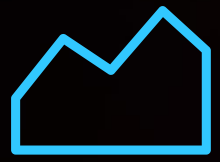
- Metrics for interface endpoints, Gateway Load Balancer endpoints, and endpoint services
- Metrics include New/Active Connections, Bytes Processed, Packets Dropped, and RST Packets Received
- ELB publishes data points for Gateway Load Balancers and targets



Network monitoring best practices

Define KPIs

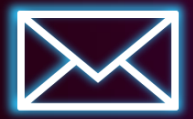
Resources to be monitored



Monitoring frequency

Monitoring tools

Monitoring team



Escalation path

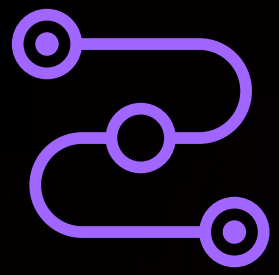
Automation

Network analysis and troubleshooting

How do I analyze network configuration across my VPCs and from the internet?

Analyzing network configurations

TROUBLESHOOT AND VALIDATE NETWORK CONFIGURATIONS



VPC Reachability Analyzer

Connectivity testing between a source resource and a destination resource

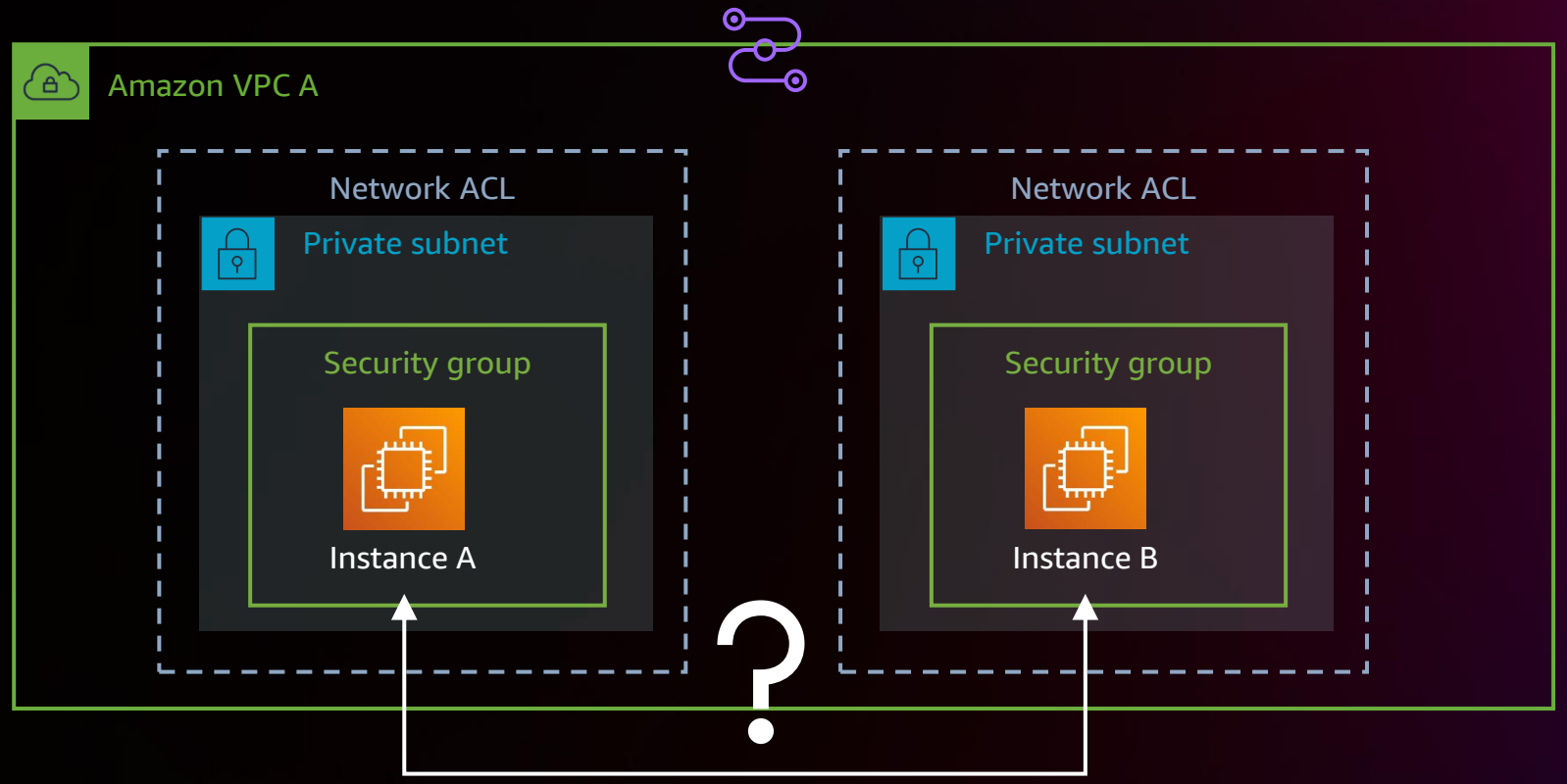
Transit Gateway Route Analyzer

Perform an analysis of the routes in your transit gateway route tables

Network Access Analyzer

Identifies unintended network access to your resources on AWS

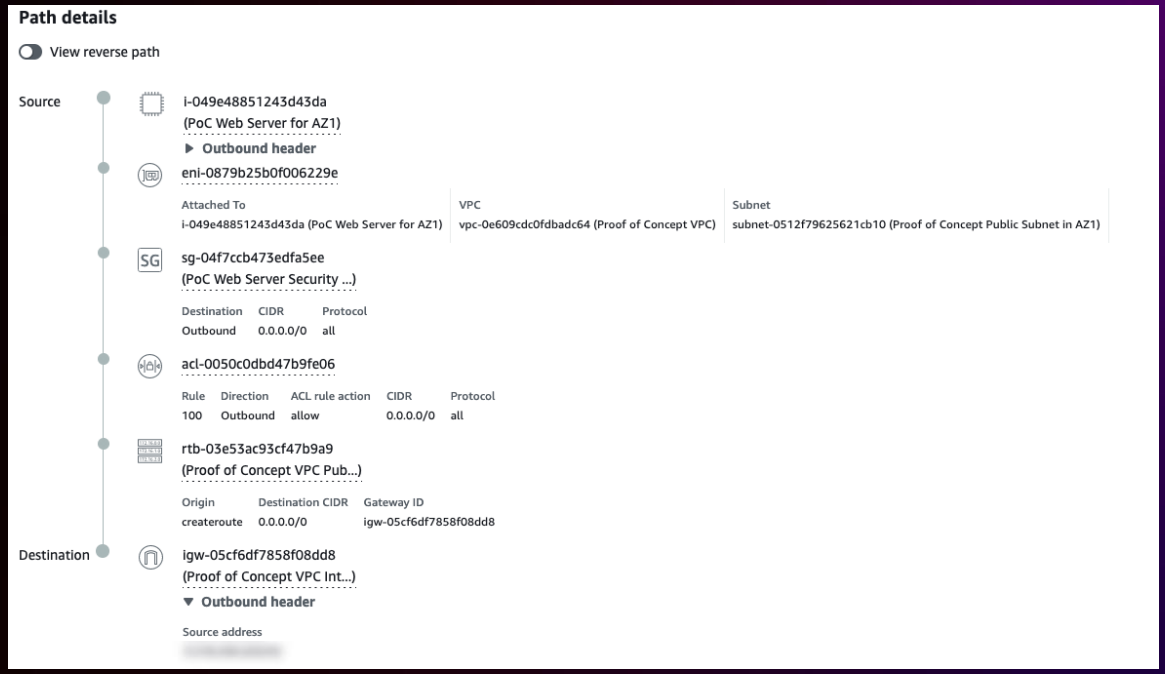
VPC Reachability Analyzer



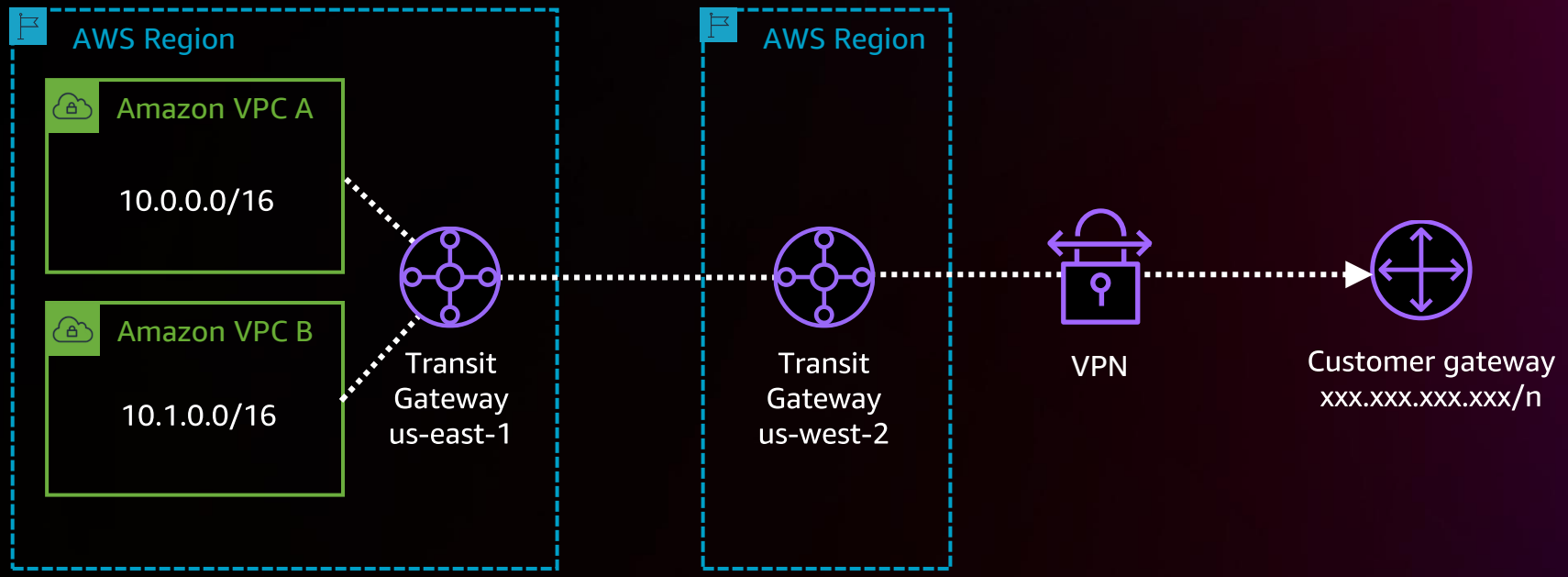
How can I verify connectivity between a source resource and a destination resource?

VPC Reachability Analyzer

- Connectivity testing between a source resource and a destination resource in your VPCs
- Produces hop-by-hop details of the virtual network path between the source and the destination
- When the destination is not reachable, VPC Reachability Analyzer identifies the blocking component
- Does not send any real packets but utilizes automated reasoning



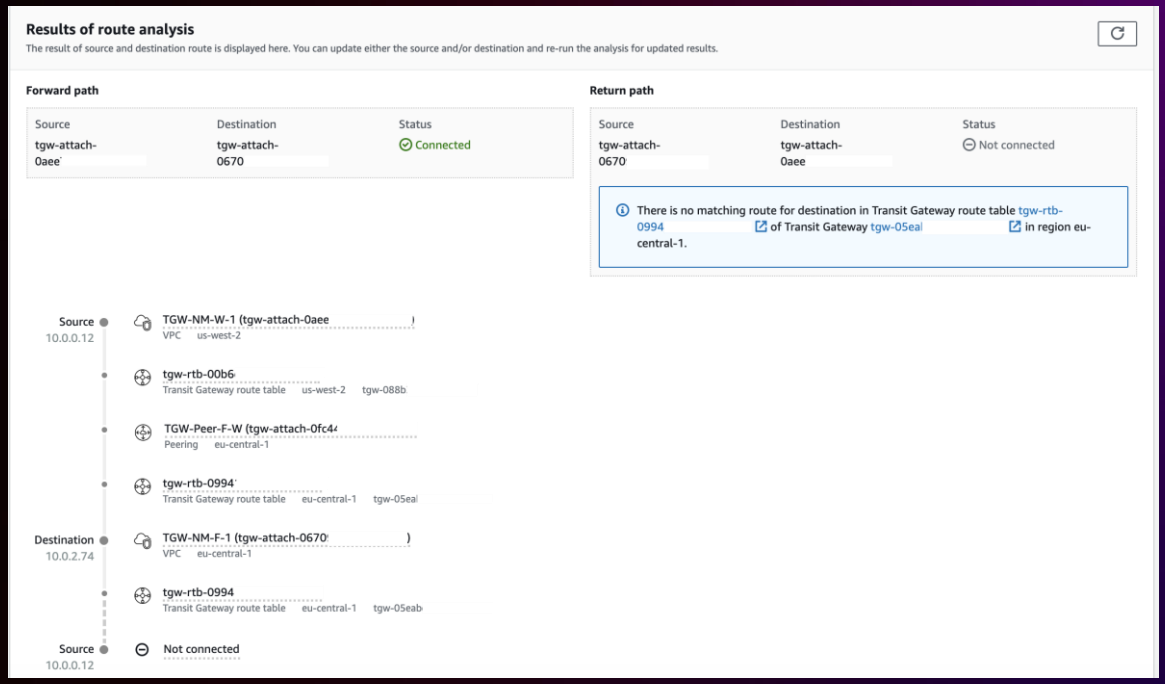
Transit Gateway Route Analyzer



How can I perform an analysis of the routes in my transit gateway route tables to verify connectivity?

Transit Gateway Route Analyzer

- Verify that the transit gateway route table configuration will work as expected before you start sending traffic
- Validate your existing route configuration
- Diagnose route-related issues that are causing traffic disruption in your global network



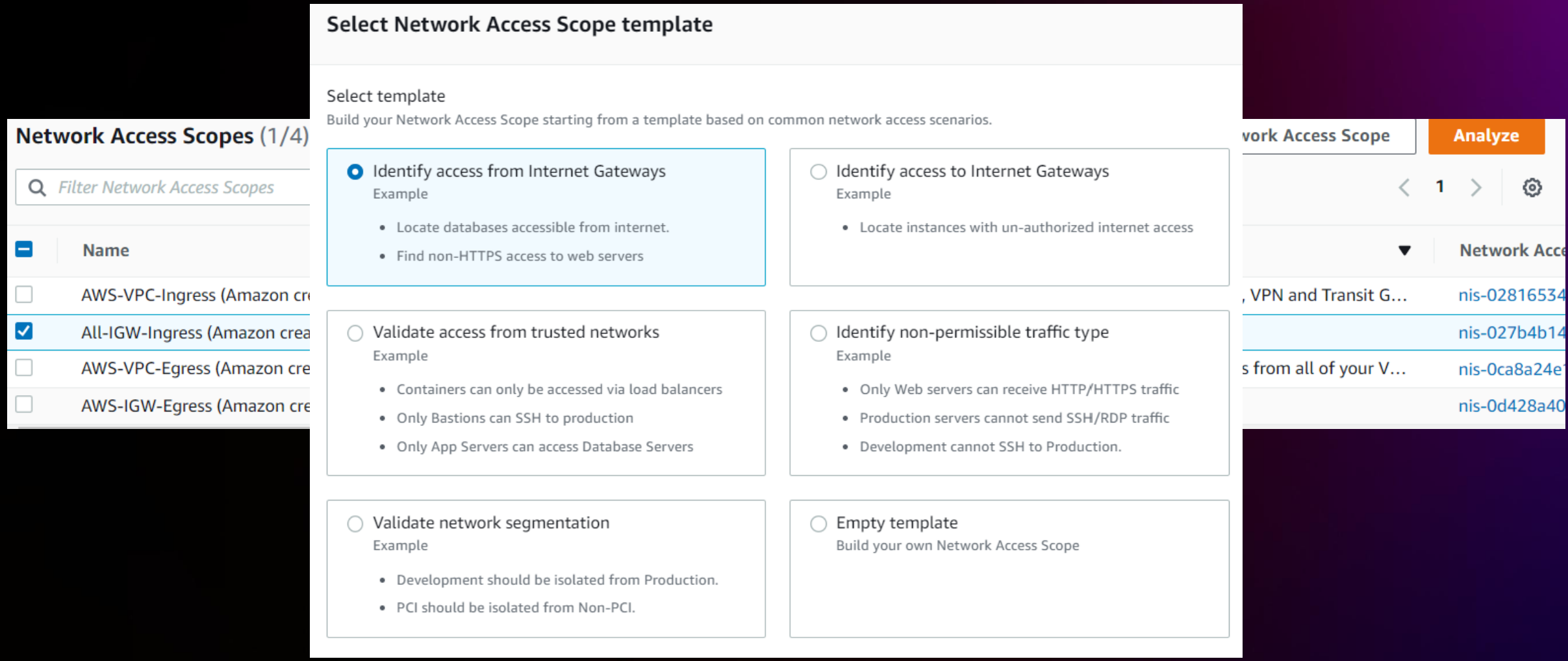
How can Network Access Analyzer help?

Network Access Analyzer can help you verify the following sample requirements utilizing automated reasoning

- Network segmentation
- Internet accessibility
- Trusted network paths
- Trusted network access

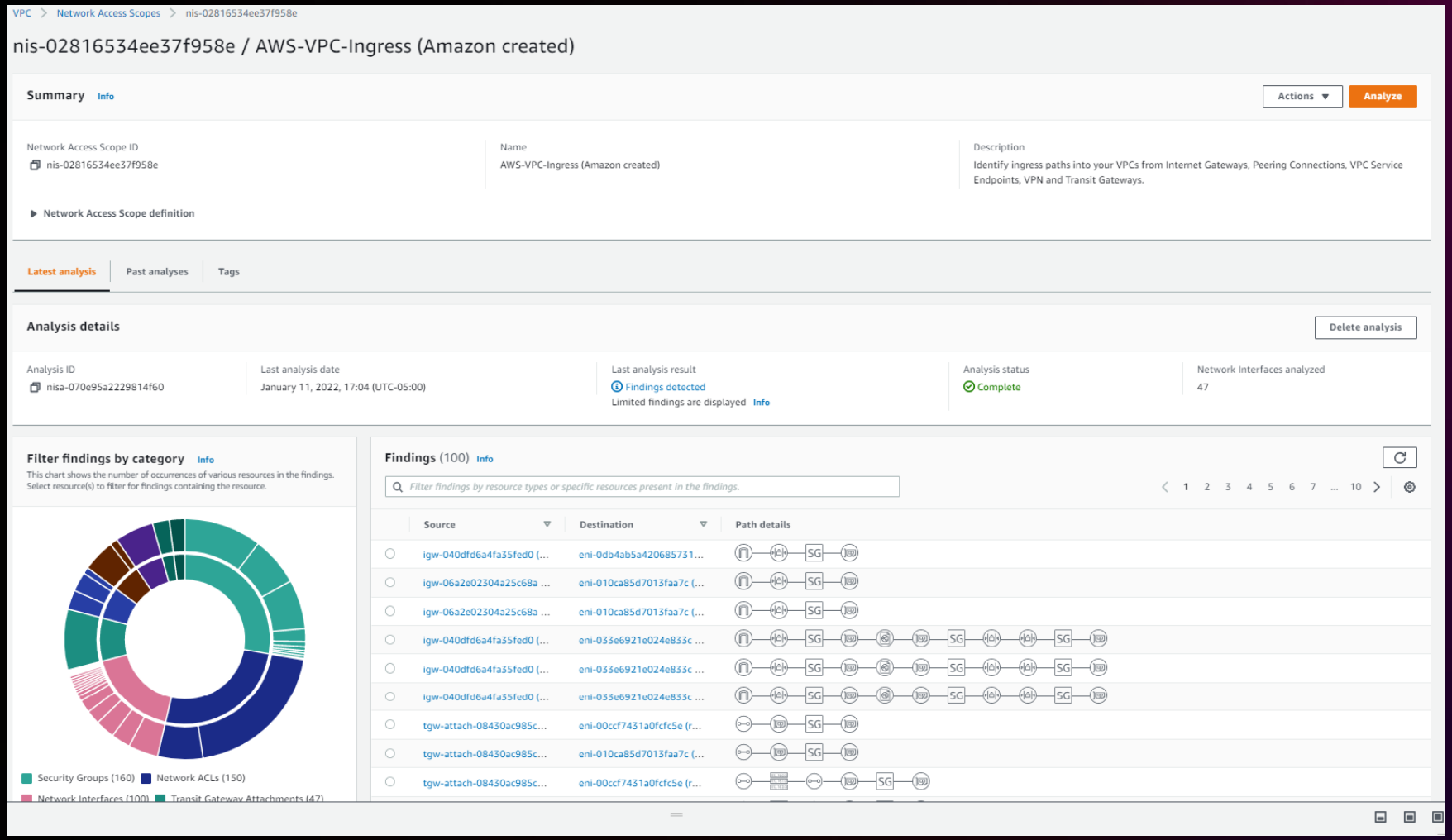
How Network Access Analyzer works

DEFINE YOUR REQUIREMENTS



How Network Access Analyzer works

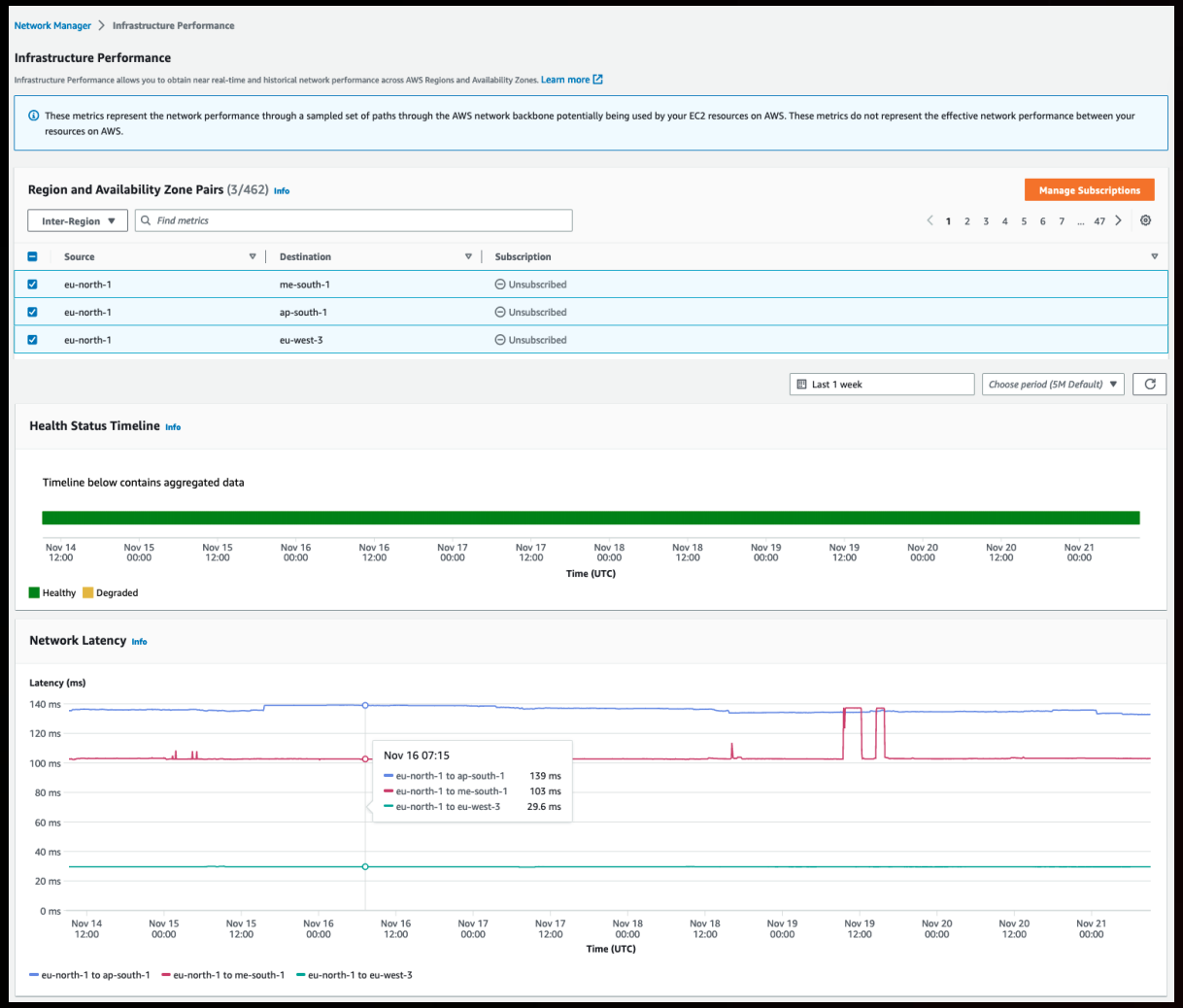
RUN ANALYSIS AND REVIEW FINDINGS



How can I identify network performance issues on AWS or out on the internet?

AWS Network Manager

MONITORING AWS GLOBAL NETWORK PERFORMANCE



Metrics for AWS global network

Aggregate round-trip latency* between AWS Regions, Availability Zones, and within Availability Zones

What you can do with this data

- Monitor latency of AWS global network using console or CloudWatch
- Understand the health status of AWS global network between Regions and Availability Zones
- Plan Region expansion

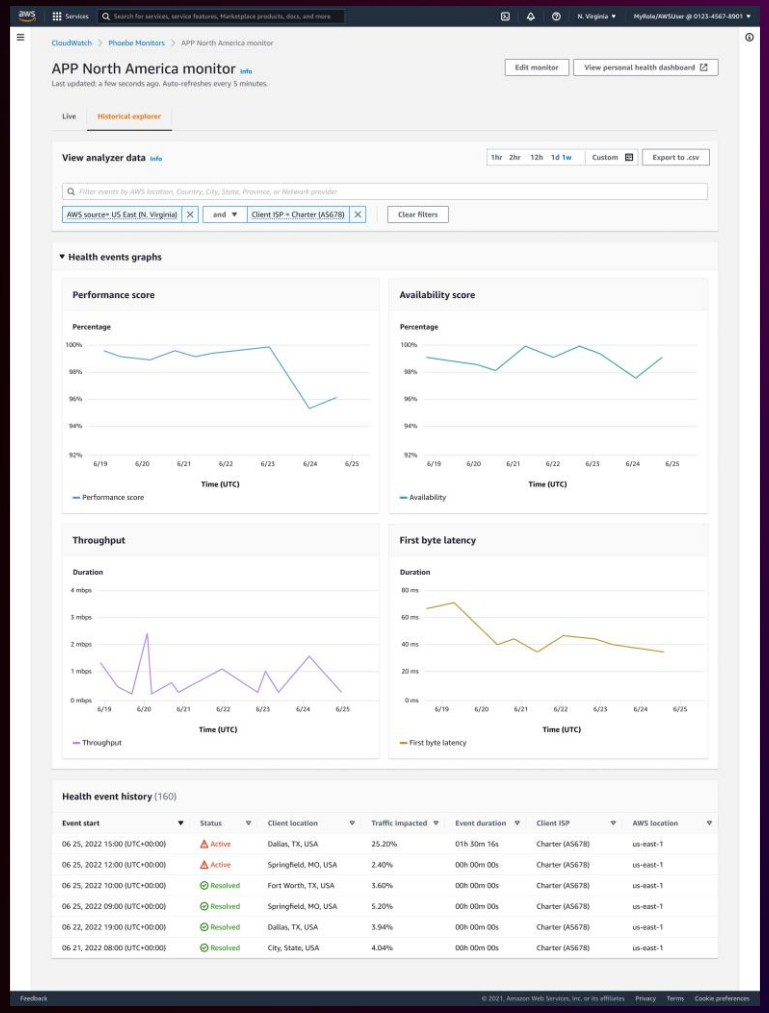
* Median (P50) round-trip latency aggregated across measurements from AWS Global Network. These measurements are not specific to your AWS resources.

Amazon CloudWatch Internet Monitor

Preview

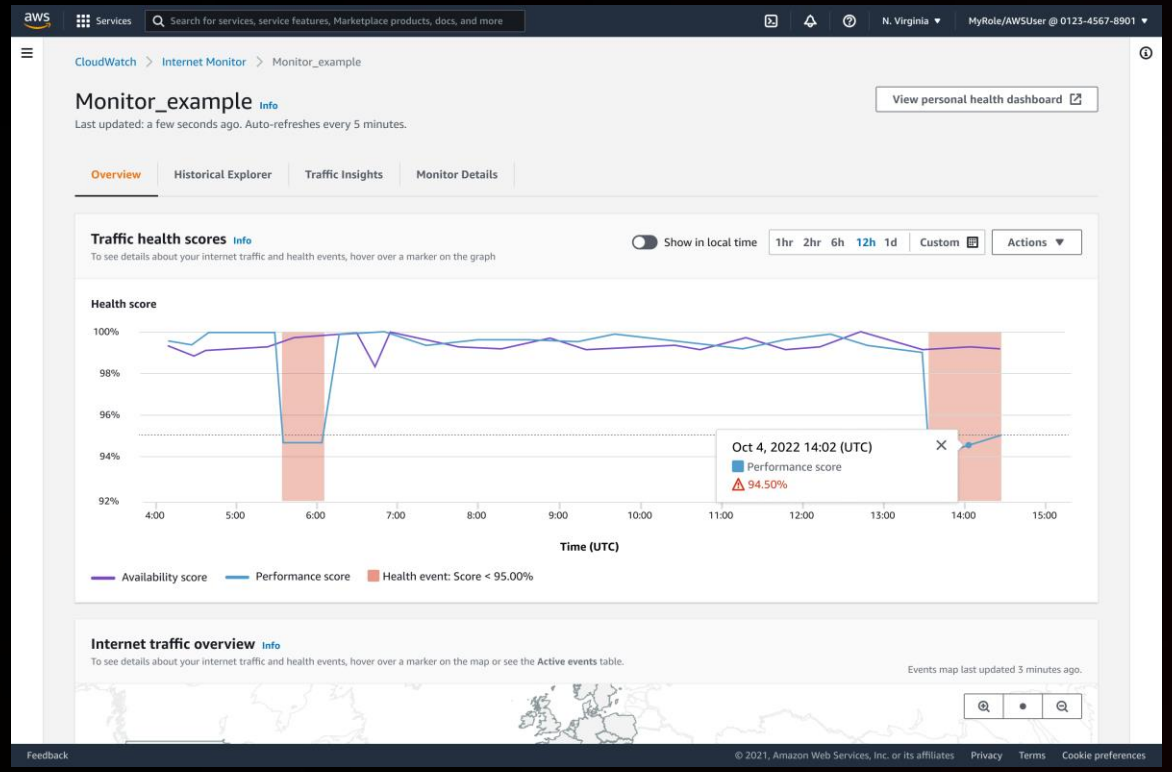
OVERVIEW

- Internet Monitor publishes measurements for your internet-facing traffic to CloudWatch
- Measurements include availability and performance scores, route-trip times (RTT), bytes transferred, and number of clients (for Amazon WorkSpaces)
- These are all measured between pairs of end-user locations and service locations



Amazon CloudWatch Internet Monitor

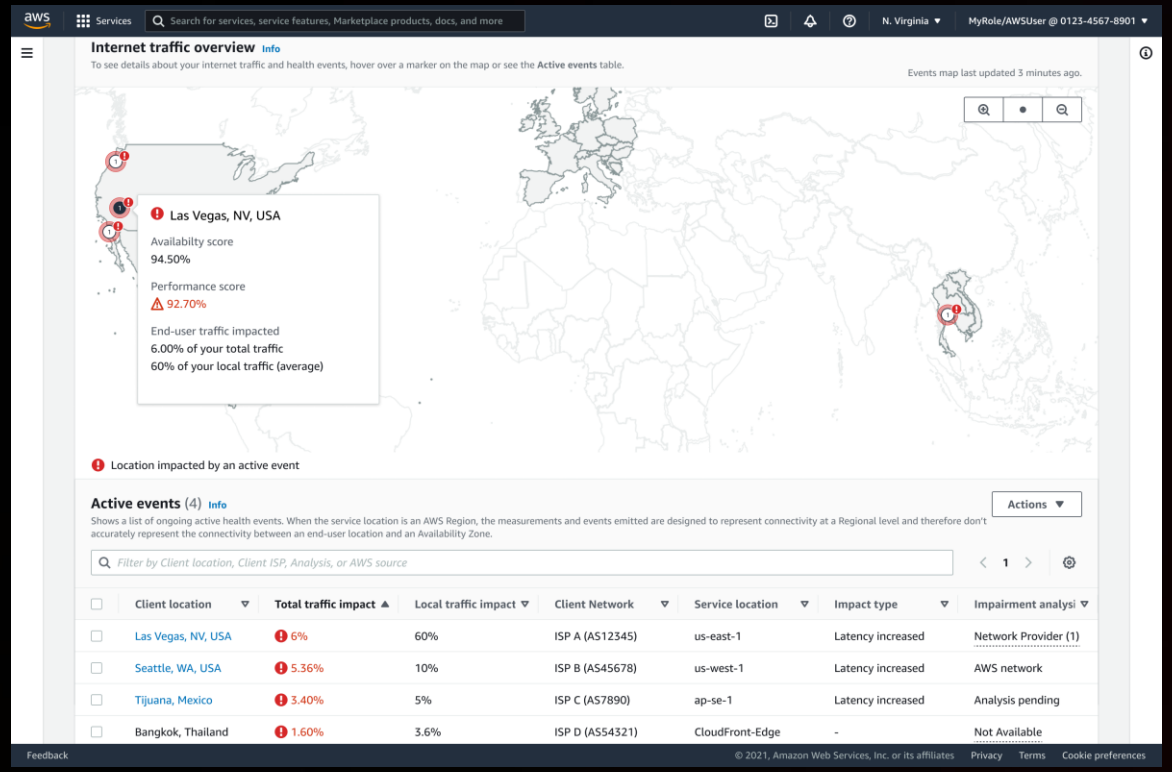
HEALTH SCORE



- Using historical data and applying statistical analysis, Internet Monitor can detect when the performance and availability of your application has dropped
- Availability score represents the percentage of traffic that is not seeing an availability drop
- Performance score represents the percentage of traffic that is not seeing a performance drop

Amazon CloudWatch Internet Monitor

WORLD MAP AND ACTIVE EVENTS

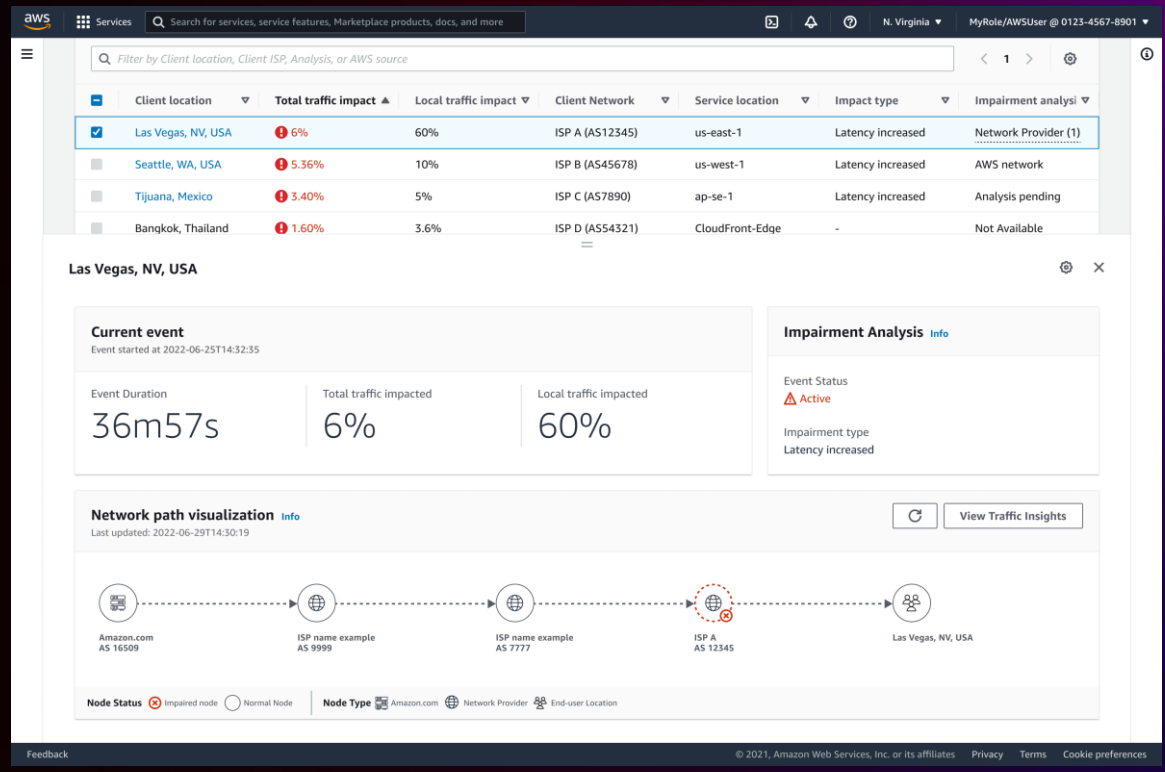


- CloudWatch Internet Monitor world map view shows the overall event status across all monitored locations
- Provides additional details about current events and highlights other events that are happening globally, sorted by total impacted traffic

Amazon CloudWatch Internet Monitor

CURRENT EVENT AND PATH VISUALIZER

- Current event details provide the duration of the event, the amount of traffic impacted, and analysis of the impairment
- Path visualizer provides details on the network path and where within the path is having the network issue

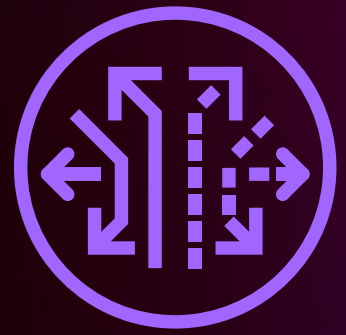


How can I capture flows and packets to understand the traffic flowing across my network?

Traffic visibility options

VPC Flow Logs

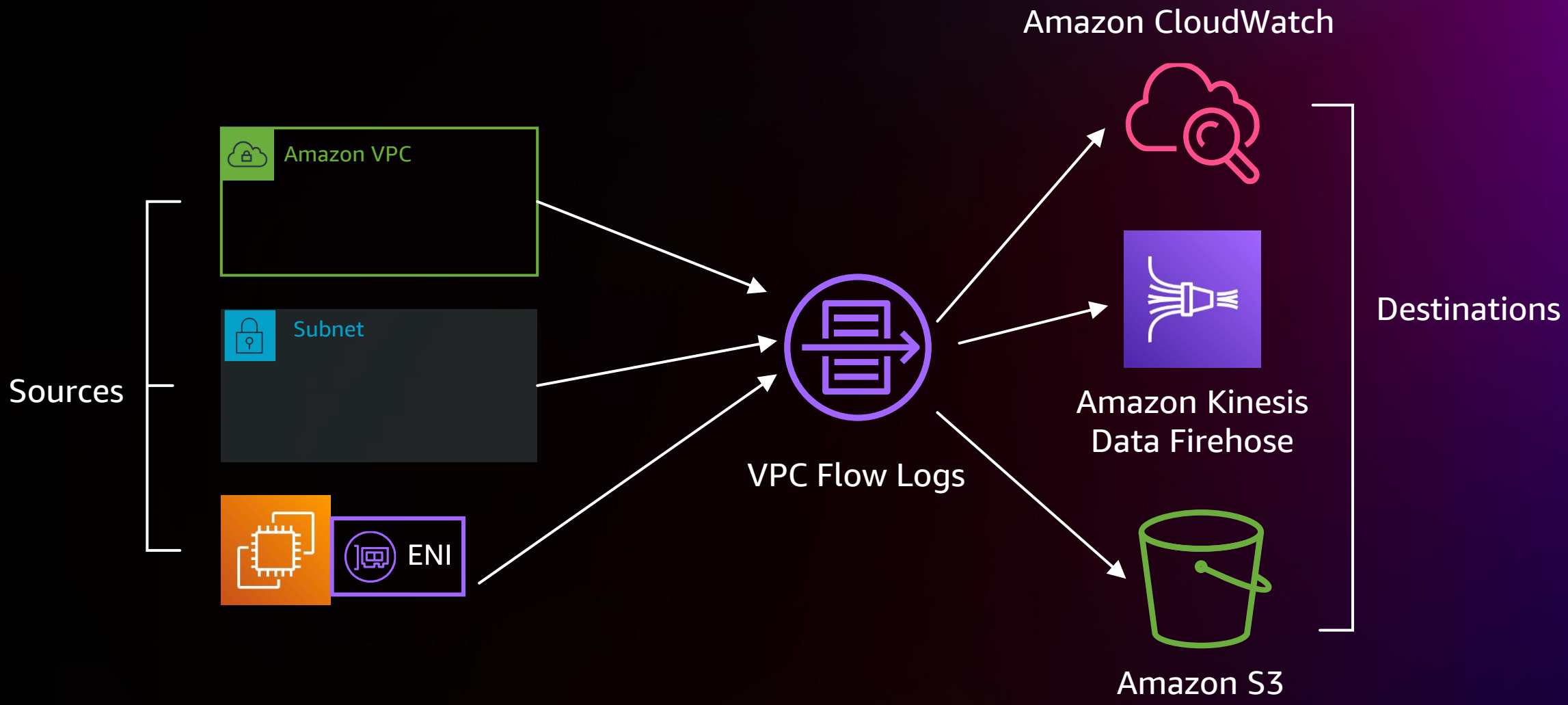
Collect and store metadata information



Traffic Mirroring

Copies network traffic, including payload

VPC Flow Logs



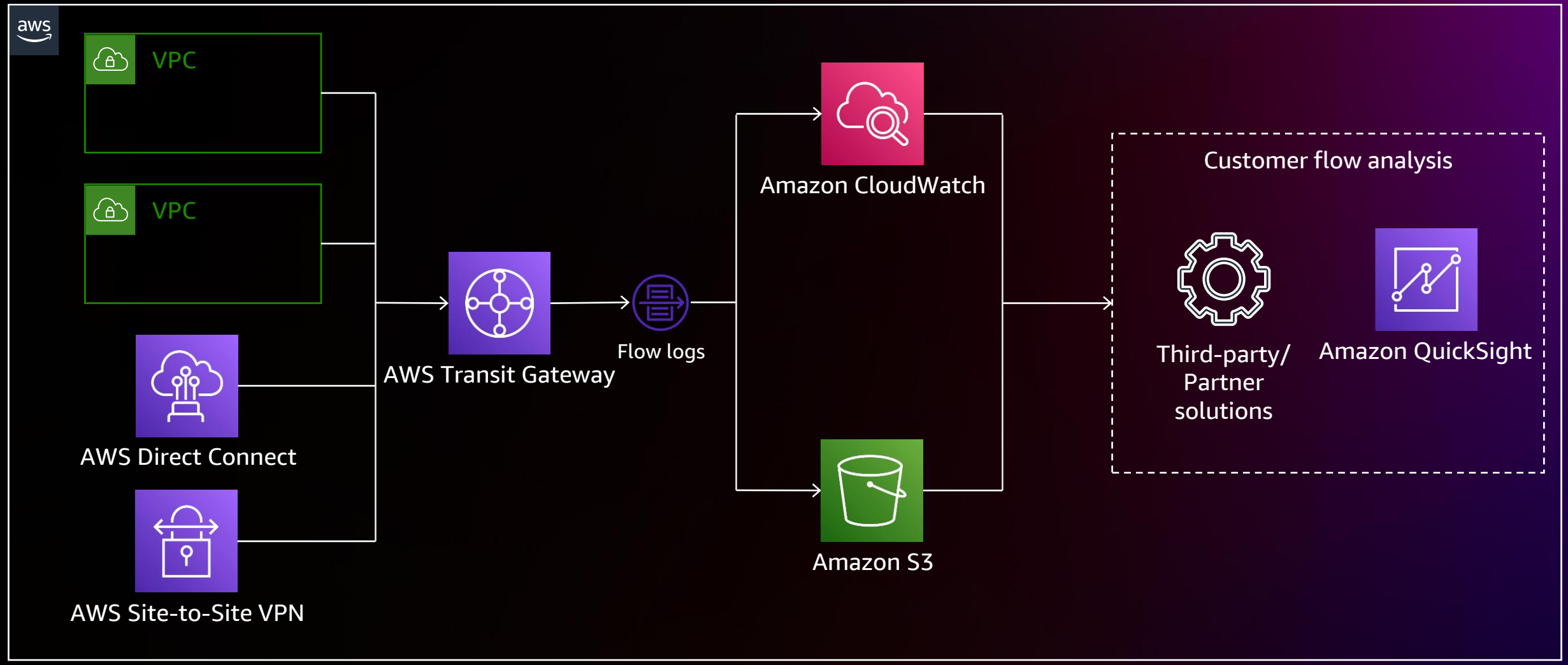
VPC Flow Logs

FIELDS AND COMMON USE CASES

- Diagnosing overly restrictive security group rules
- Monitoring the traffic that is reaching your instance
- Determining the direction of the traffic to and from the network interfaces

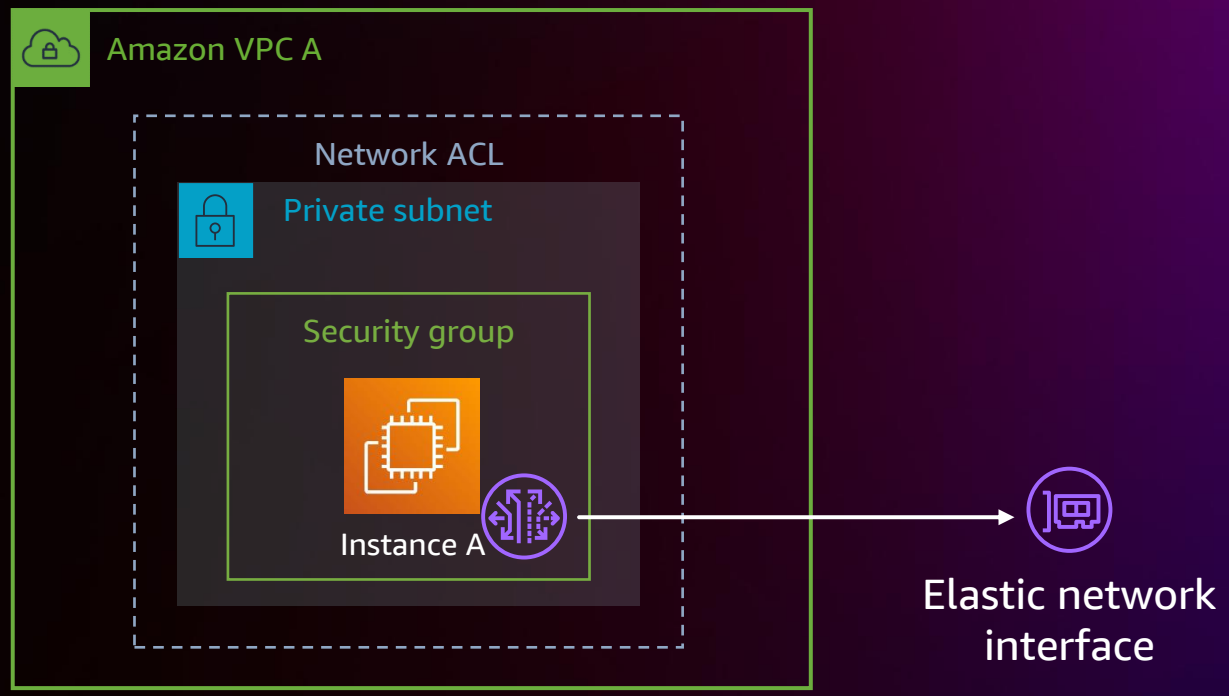
Version	2
Account ID	XXXXXXXX1234
Interface ID	eni-04b10a1942977452f
Source Address	xxx.xxx.xxx.xxx
Destination Address	xxx.xxx.xxx.xxx
Source Port	36490
Destination Port	443
Protocol	6
Packets	77
Bytes	5040
Start	1560385064
End	1560385070
Action	ACCEPT
Log Status	OK

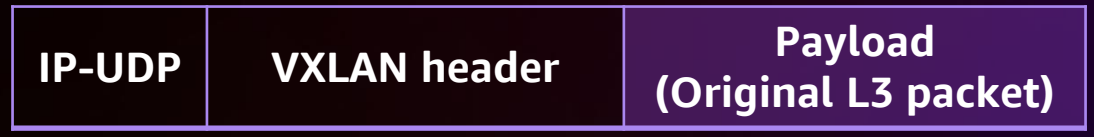
VPC Flow Logs for Transit Gateway



Traffic Mirroring with Amazon VPC

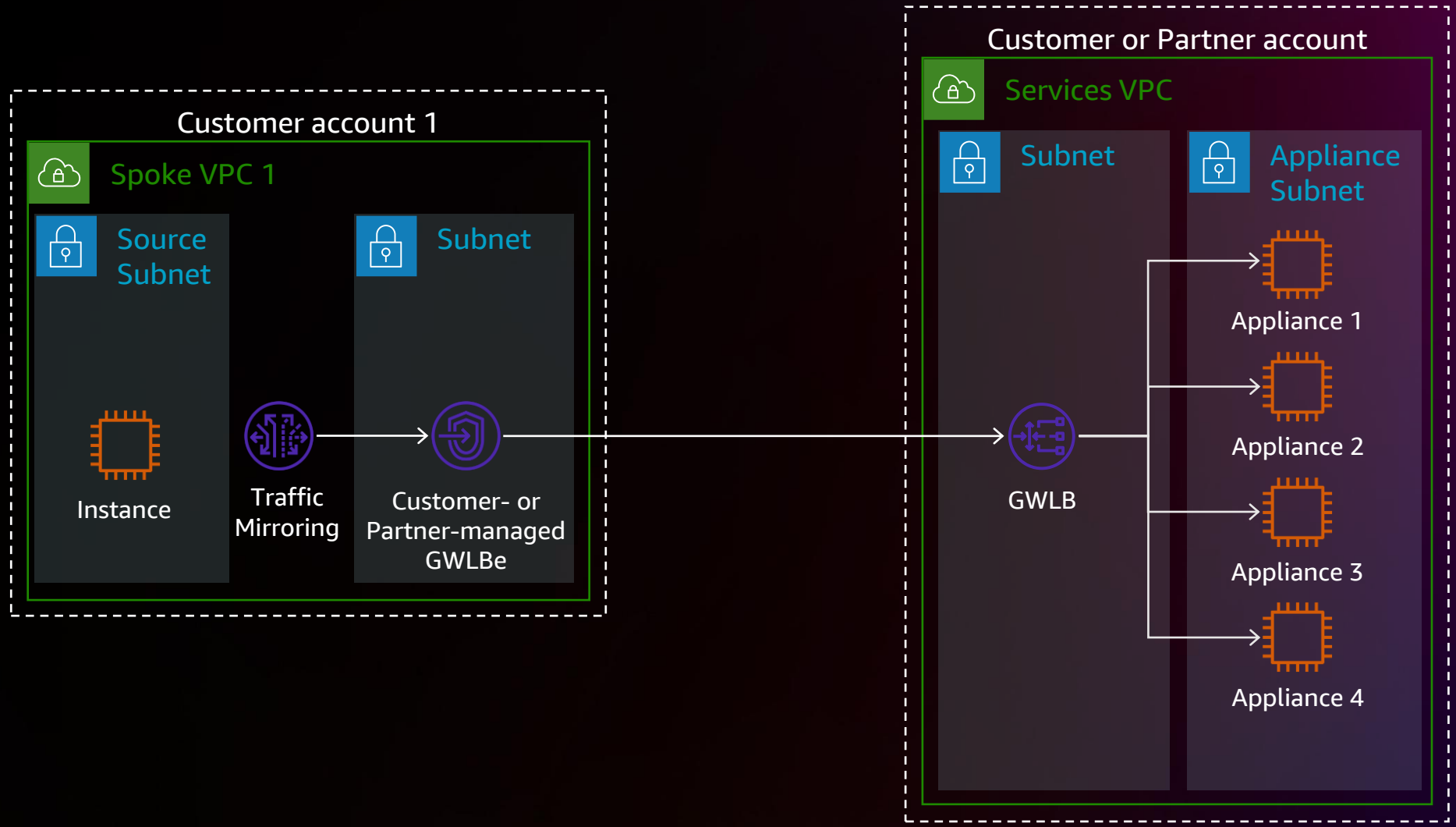
- Copy network traffic from an elastic interface of an Amazon EC2 instance, a Network Load Balancer, or a Gateway Load Balancer
- Send the traffic to out-of-band security and monitoring appliances for content inspection, threat monitoring, or troubleshooting
- Identify the block component when the destination is not reachable



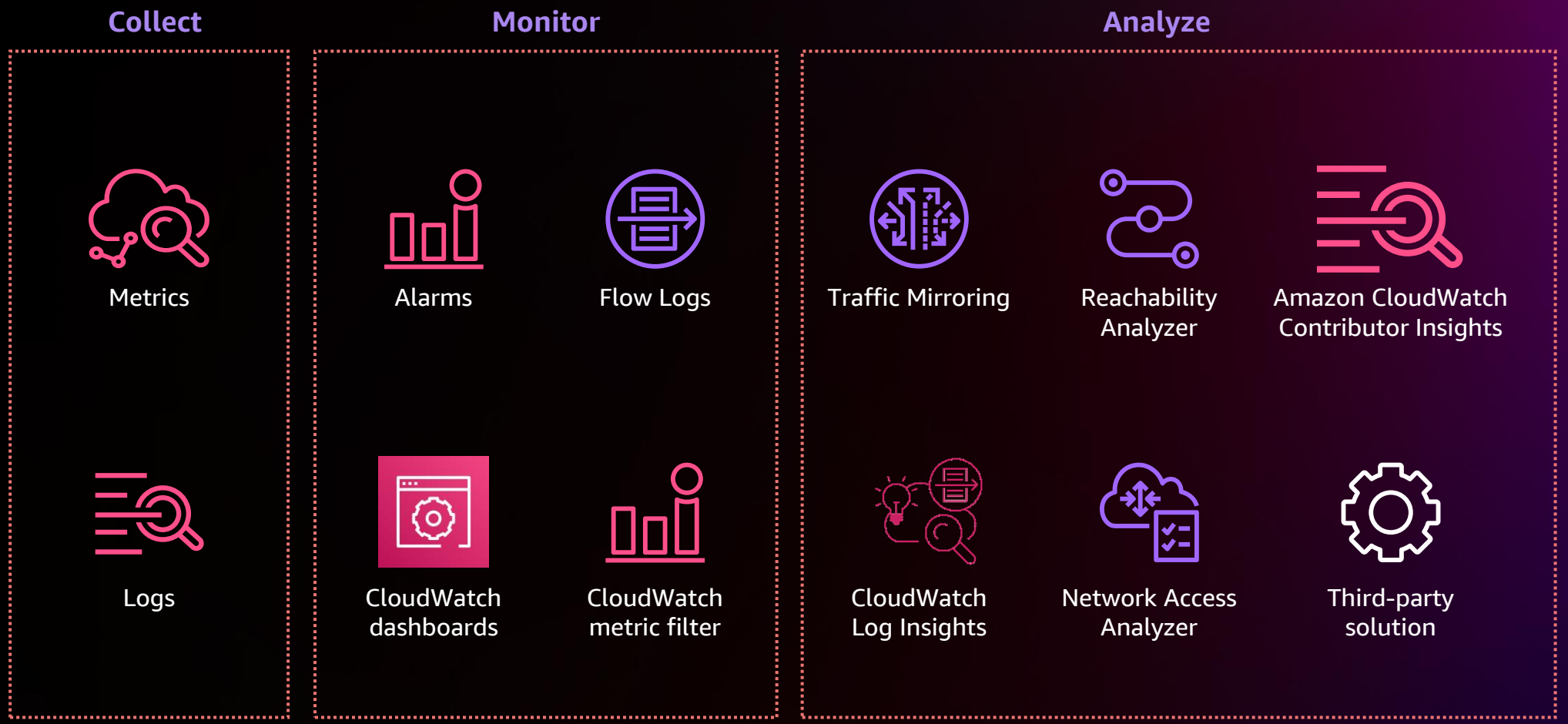


Traffic Mirroring

GATEWAY LOAD BALANCER ENDPOINT (GWLBE) AS A TARGET



Summary of network observability



Thank you!

Sohaib Tahir
sohaibt@amazon.com

Riggs Goodman III
goriggs@amazon.com

Please complete the session survey in the **mobile app**