

# 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

## Collect



Metrics



Logs

## Monitor



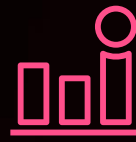
Alarms



Flow Logs

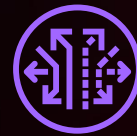


CloudWatch dashboards



CloudWatch metric filter

## Analyze



Traffic Mirroring



Reachability Analyzer



Amazon CloudWatch Contributor Insights



CloudWatch Log Insights



Network Access Analyzer



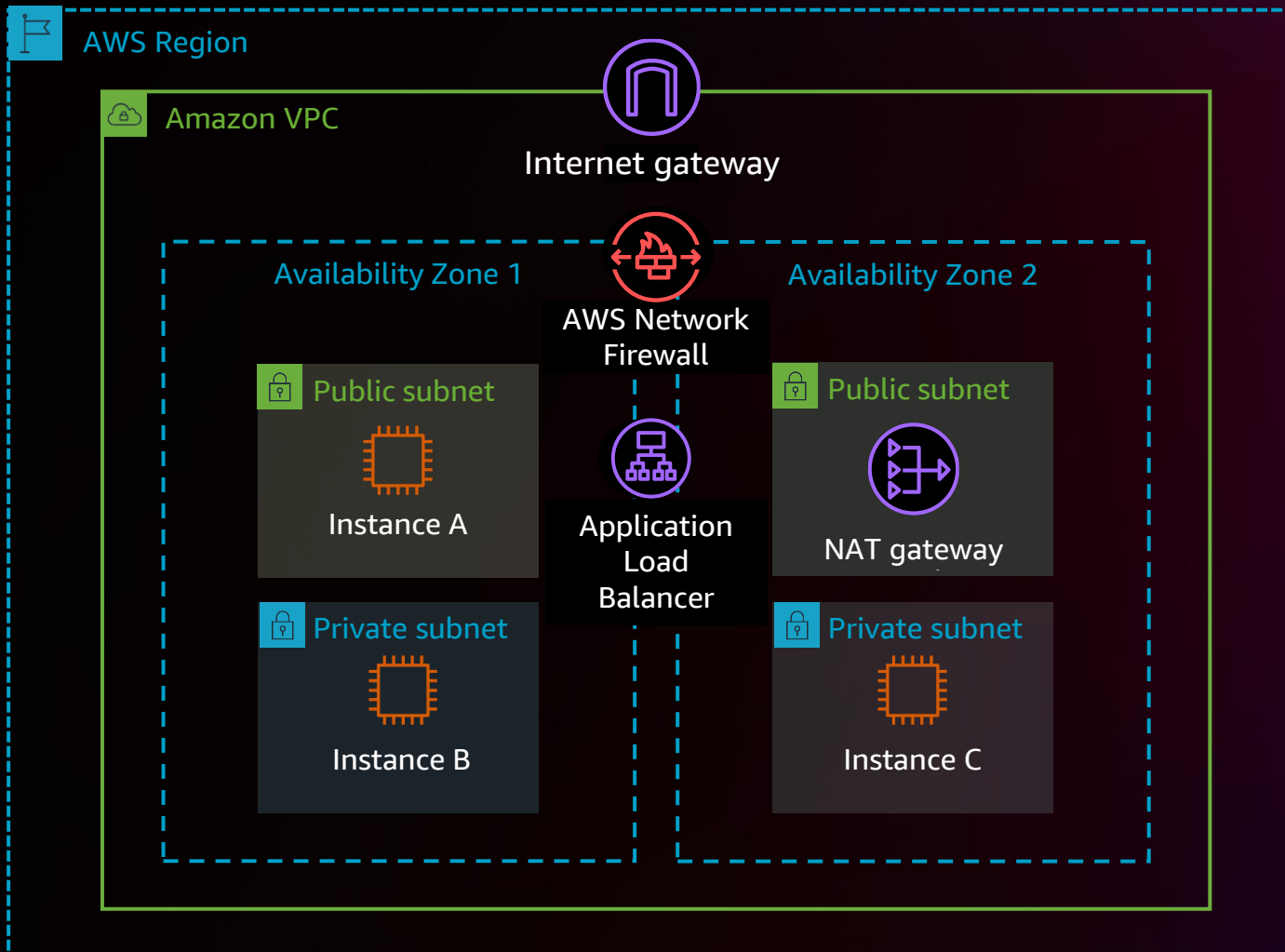
Third-party solution

# Network monitoring



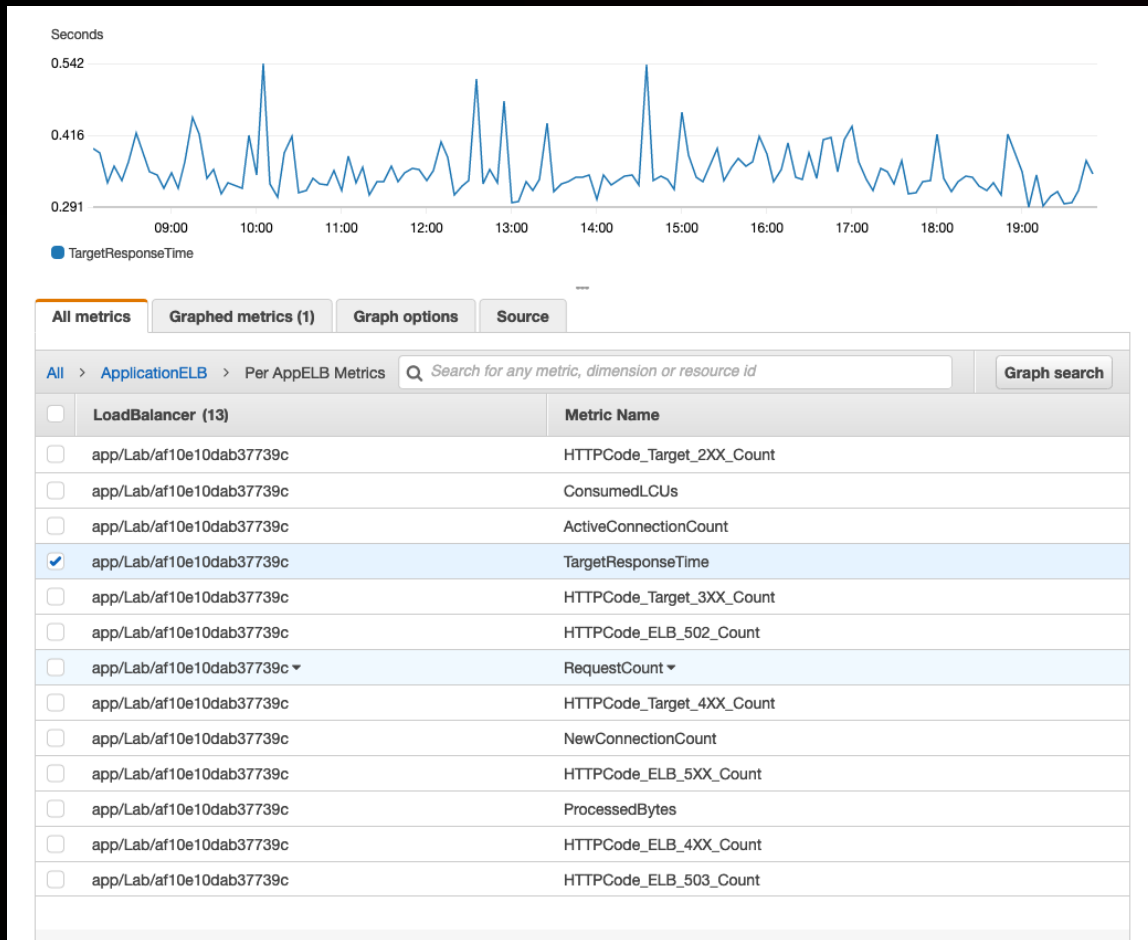
# Network monitoring

## 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

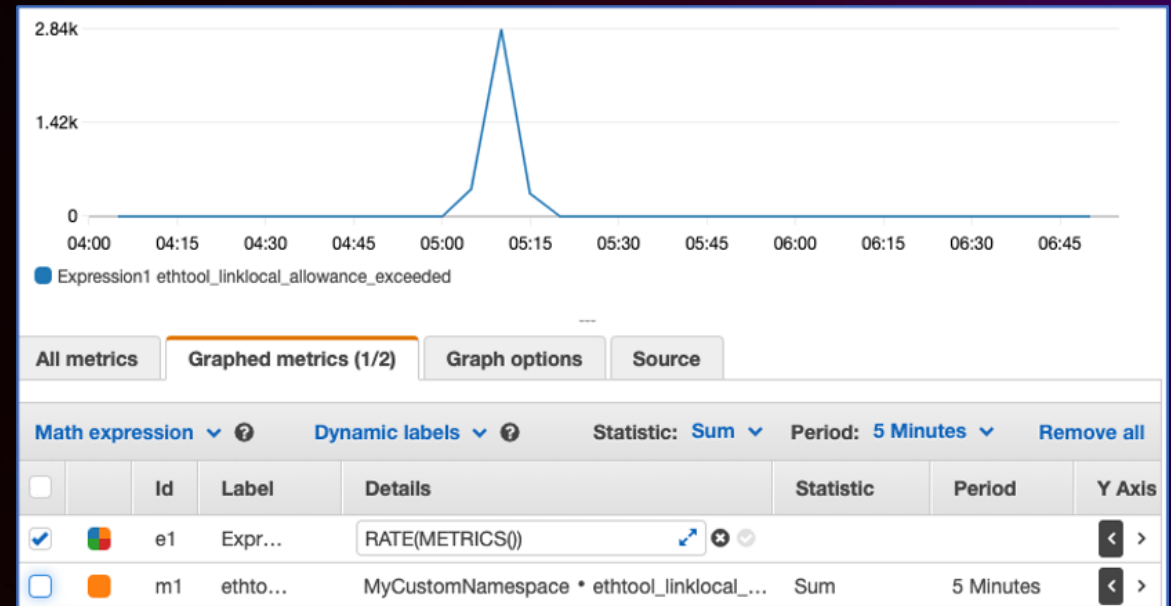
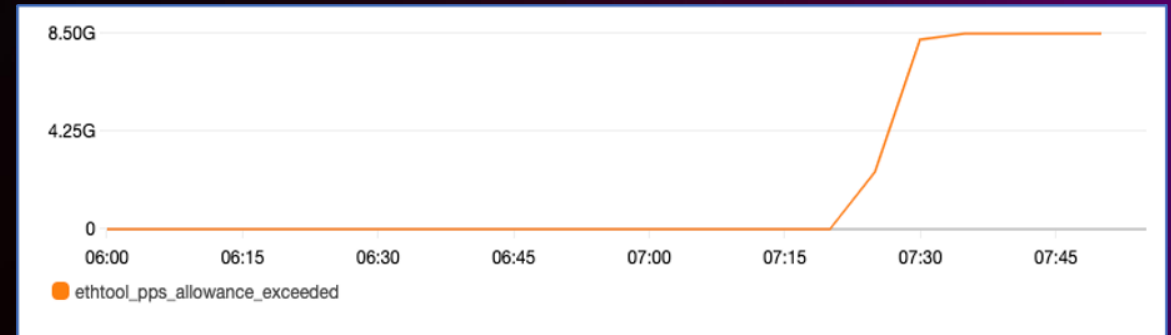
# Amazon EC2 metrics

## INSTANCE-LEVEL NETWORK PERFORMANCE METRICS

Amazon EC2 provides instance-level network metrics via CloudWatch

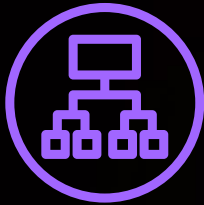
With Elastic Network Adapter (ENA), gain insights into traffic drops when network allowances are exceeded

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



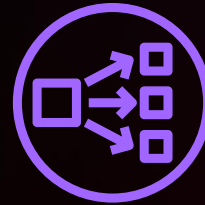
# Elastic Load Balancing (ELB)

CLOUDWATCH METRICS



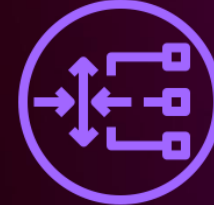
Application  
Load Balancer

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

CloudWatch > Alarms Switch to your original interface

Alarms (11)

Hide Auto Scaling alarms

Action

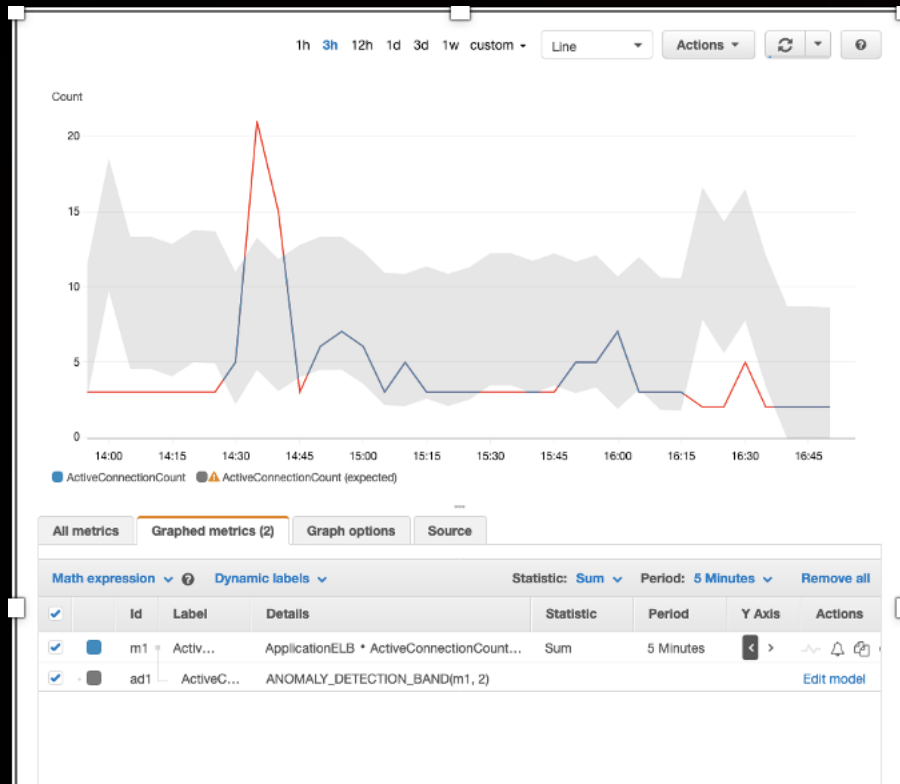
< 1 > ⌕

<input type="checkbox"/>	Name	State	Conditions	Actions
<input type="checkbox"/>	ImageErrorAlarm	<span style="color: red;">⚠ In alarm</span>	ImageError > 0 for 1 datapoints within 10 seconds	-
<input type="checkbox"/>	centralized-logging-StatusYellowAlarm-L8VNTMWS5IP8	<span style="color: green;">✔ OK</span>	ClusterStatus.yellow >= 1 for 1 datapoints within 1 minute	-
<input type="checkbox"/>	centralized-logging-MasterNotReachableFromNodeAlarm-12NUZCERB15HI	<span style="color: green;">✔ OK</span>	MasterReachableFromNode < 1 for 1 datapoints within 1 minute	-
<input type="checkbox"/>	centralized-logging-IndexWritesBlockedTooHighAlarm-SJ3CQWU5T2RS	<span style="color: green;">✔ OK</span>	ClusterIndexWritesBlocked >= 1 for 1 datapoints within 5 minutes	-
<input type="checkbox"/>	centralized-logging-JVMMemoryPressureTooHighAlarm-145XR140EMJAP	<span style="color: green;">✔ OK</span>	JVMMemoryPressure >= 80 for 1 datapoints within 15 minutes	-
<input type="checkbox"/>	centralized-logging-MasterCPUUtilizationTooHighAlarm-VQQ5ZWZ5ZUV9	<span style="color: green;">✔ OK</span>	MasterCPUUtilization >= 50 for 3 datapoints within 45 minutes	-
<input type="checkbox"/>	centralized-logging-StatusRedAlarm-1COJRPKQ5IBGJ	<span style="color: green;">✔ OK</span>	ClusterStatus.red >= 1 for 1 datapoints within 1 minute	-
<input type="checkbox"/>	centralized-logging-MasterJVMMemoryPressureTooHighAlarm-1B2YB793W1A03	<span style="color: green;">✔ OK</span>	MasterJVMMemoryPressure >= 50 for 1 datapoints within 15 minutes	-
<input type="checkbox"/>	centralized-logging-AutomatedSnapshotFailureTooHighAlarm-110NHPWR16NX8	<span style="color: green;">✔ OK</span>	AutomatedSnapshotFailure >= 1 for 1 datapoints within 1 minute	-
<input type="checkbox"/>	centralized-logging-FreeStorageSpaceTooLowAlarm-T60Q56YMYGQI	<span style="color: green;">✔ OK</span>	FreeStorageSpace <= 2000 for 1 datapoints within 1 minute	-
<input type="checkbox"/>	centralized-logging-CPUUtilizationTooHighAlarm-KY26QQRJU248	<span style="color: green;">✔ OK</span>	CPUUtilization >= 80 for 3 datapoints within 45 minutes	-

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

**Log record format**  
Specify the fields to include in the flow log record.

AWS default format  
 Custom format

**Format preview**

```
#{version} #{account-id} #{interface-id} #{srcaddr} #{dstaddr} #{srcport} #{dstport}
#{protocol} #{packets} #{bytes} #{start} #{end} #{action} #{log-status}
```

**Log record format**  
Specify the fields to include in the flow log record.

AWS default format  
 Custom format

**Log format**  
Specify the fields to include in the flow log record.

Select an attribute... ▲

Q |

- account-id
- action
- az-id
- bytes
- dstaddr
- dstport
- end
- flow-direction
- instance-id
- interface-id
- log-status
- packets
- pkt-dst-aws-service
- pkt-dstaddr

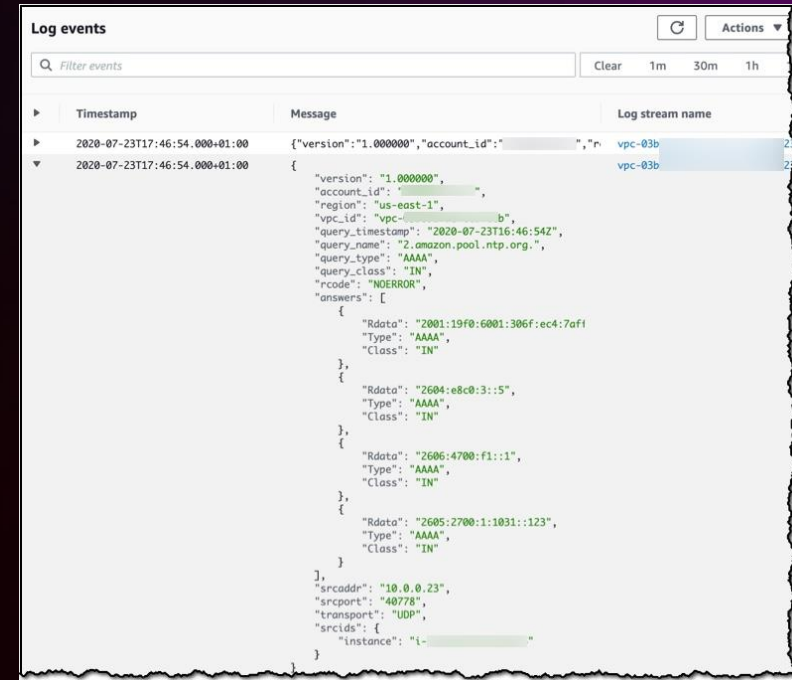
# Route 53 query logs

## 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



The screenshot shows the AWS CloudWatch Logs console. The 'Log events' view displays a single log event with the following message:

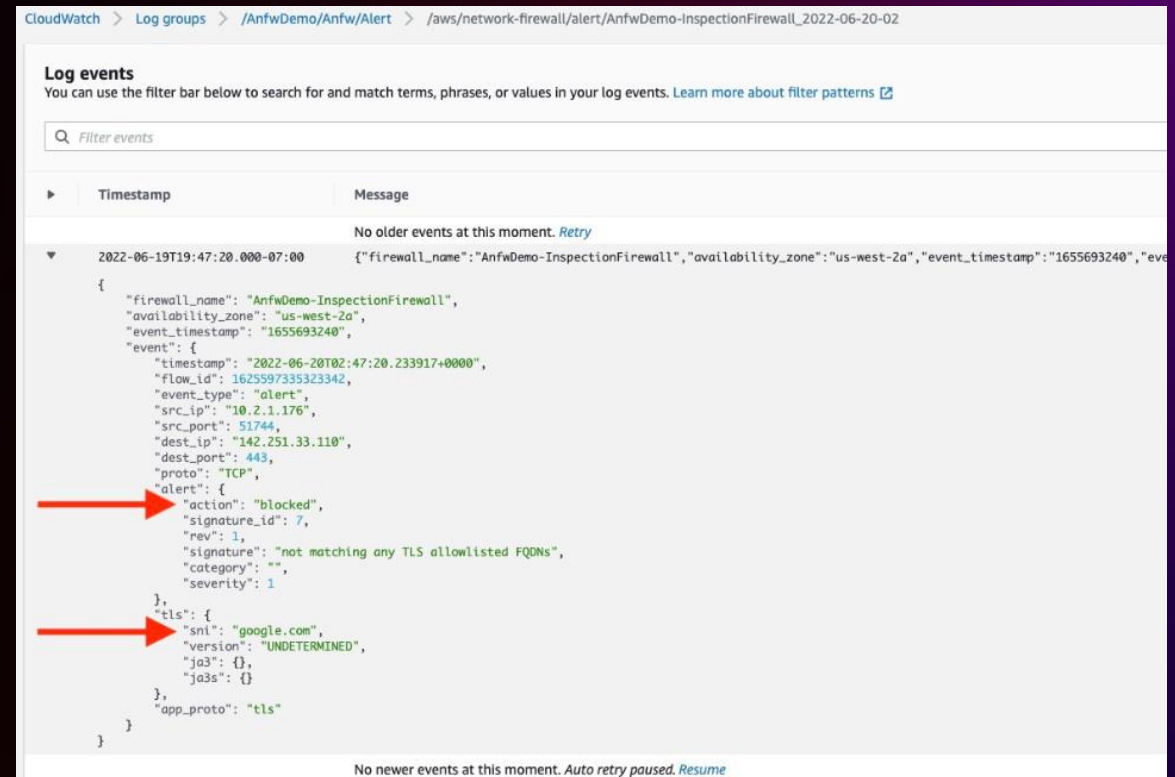
```
{ "version": "1.000000", "account_id": "...", "region": "us-east-1", "vpc_id": "vpc-...", "query_timestamp": "2020-07-23T16:46:54Z", "query_name": "2.amazon.pool.ntp.org.", "query_type": "AAAA", "query_class": "IN", "rcode": "NOERROR", "answers": [ { "Rdata": "2001:19f0:6001:306f:ec4:7af1", "Type": "AAAA", "Class": "IN" }, { "Rdata": "2604:e8c0:3::5", "Type": "AAAA", "Class": "IN" }, { "Rdata": "2606:4700:f1::1", "Type": "AAAA", "Class": "IN" }, { "Rdata": "2605:2700:1:1031::123", "Type": "AAAA", "Class": "IN" } ], "srcaddr": "10.0.0.23", "srcport": "40778", "transport": "UDP", "srcids": { "instance": "i-..." } }
```



# 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



```
CloudWatch > Log groups > /AnfwDemo/Anfw/Alert > /aws/network-firewall/alert/AnfwDemo-InspectionFirewall_2022-06-20-02

Log events
You can use the filter bar below to search for and match terms, phrases, or values in your log events. Learn more about filter patterns

Filter events

Timestamp      Message
No older events at this moment. Retry

2022-06-19T19:47:20.000-07:00  {"firewall_name": "AnfwDemo-InspectionFirewall", "availability_zone": "us-west-2a", "event_timestamp": "1655693240", "event": {
  "timestamp": "2022-06-20T02:47:20.233917+0000",
  "flow_id": "162559735323342",
  "event_type": "alert",
  "src_ip": "10.2.1.176",
  "src_port": "51744",
  "dest_ip": "142.251.33.110",
  "dest_port": "443",
  "proto": "TCP",
  "alert": {
    "action": "blocked",
    "signature_id": 7,
    "rev": 1,
    "signature": "not matching any TLS allowlisted FQDNs",
    "category": "",
    "severity": 1
  },
  "tls": {
    "sni": "google.com",
    "version": "UNDETERMINED",
    "ja3": {},
    "ja3s": {}
  },
  "app_proto": "tls"
}
}

No newer events at this moment. Auto retry paused. Resume
```

# Network logs

CLOUDWATCH LOGS – EASILY COLLECT AND STORE LOGS

The screenshot displays the AWS CloudWatch Logs console for a log group named 'application.log'. The breadcrumb navigation shows 'CloudWatch > CloudWatch Logs > Log groups > application.log'. There are buttons for 'Delete', 'Actions', 'Query log group', and 'View all log events'. The 'Log group details' section includes:

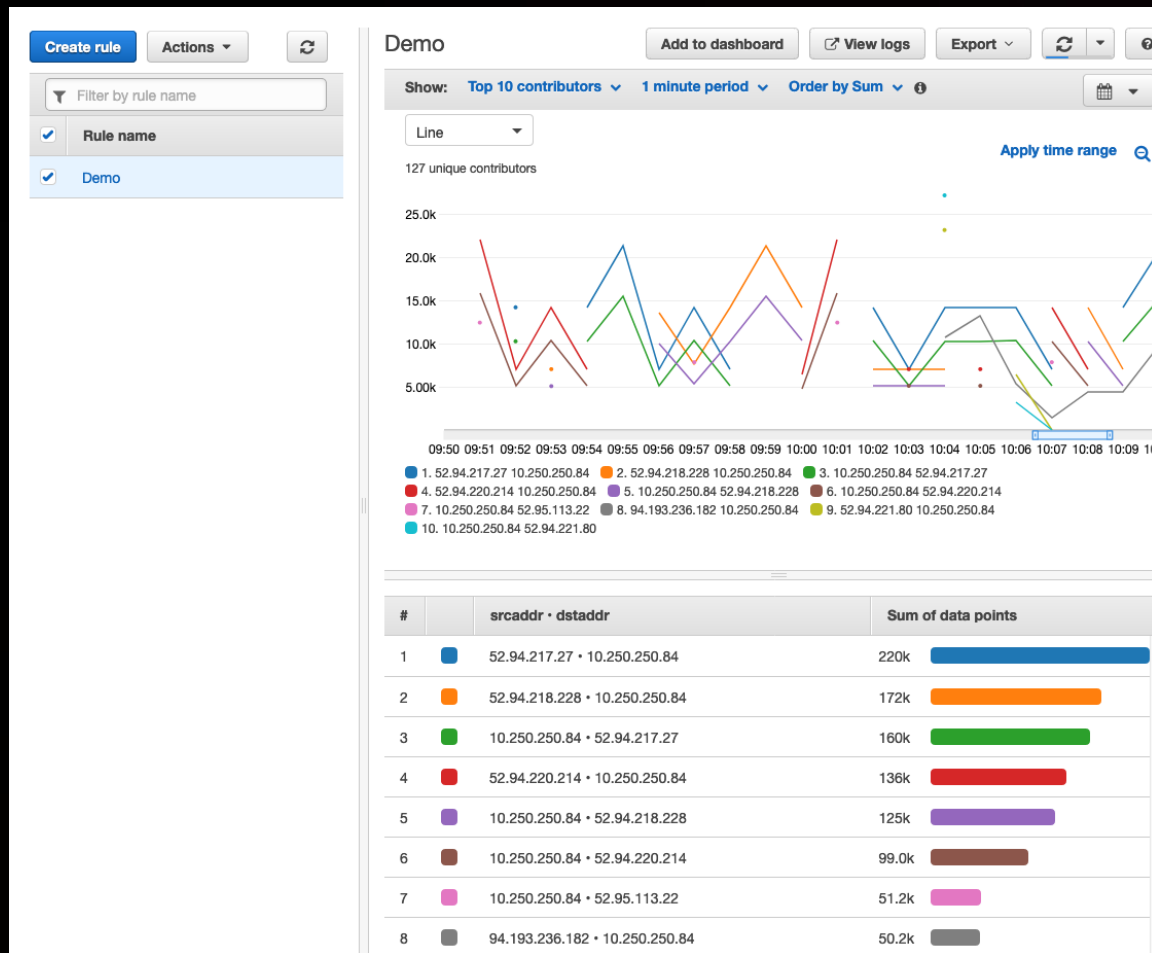
Retention Never expire	Creation time 5 months ago	Stored bytes 14.67 MB	ARN arn:aws:logs:eu-west-1:012345678910:log-group:application.log:*
KMS key ID -	Metric filters 1	Subscriptions LambdaStream_centralized-logging-LogStreamer-1A2RQLPI4N1TW	Contributor Insights rules -

Below the details are tabs for 'Log streams', 'Metric filters', and 'Contributor Insights'. The 'Log streams (5)' section includes a search bar, a refresh button, a 'Delete' button, and a 'Create log stream' button. A table lists the log streams with their IDs and last event times:

Log stream	Last event time
<a href="#">I-077f7e49ee1c0112c</a>	1/10/2020, 8:00:49 PM
<a href="#">I-03343584efd07d2a6</a>	11/29/2019, 8:03:35 PM
<a href="#">I-09bd407810ebfa83f</a>	11/29/2019, 8:00:52 PM
<a href="#">I-Obf3c984cda70e7c0</a>	9/19/2019, 9:00:35 PM
<a href="#">I-Od6468fa547a61f14</a>	9/19/2019, 9:00:35 PM

- 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

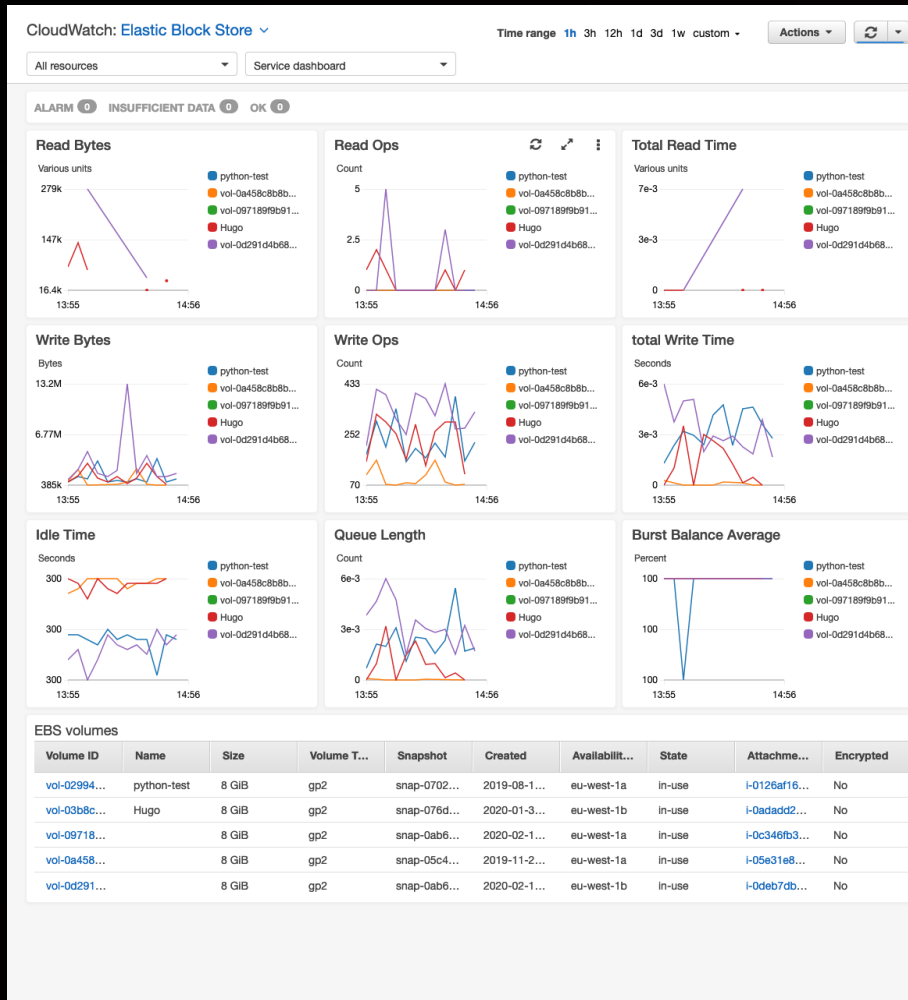


Analyzes time-series data to provide a view of the top contributors influencing system performance

- 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



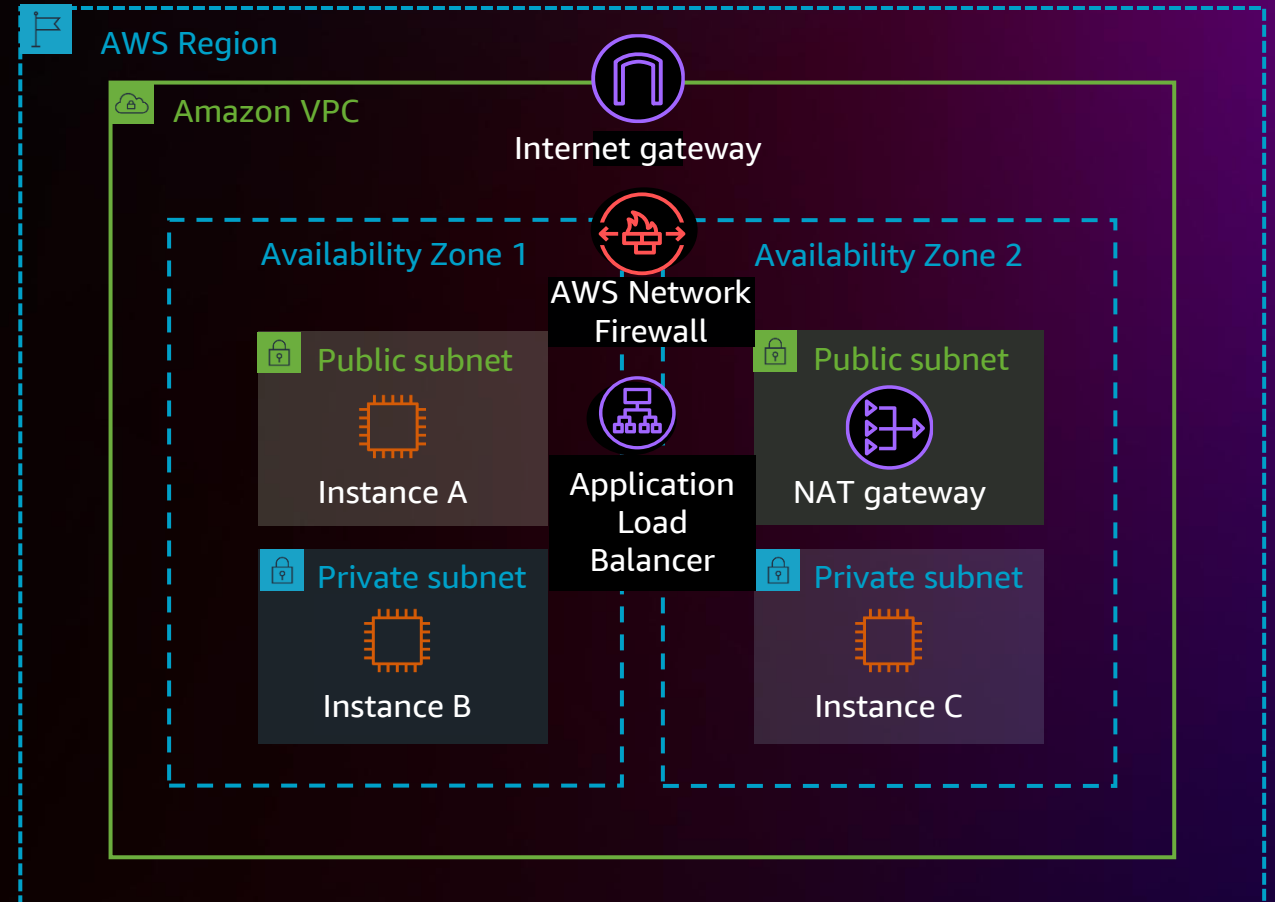
### Metrics and alarms

- 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



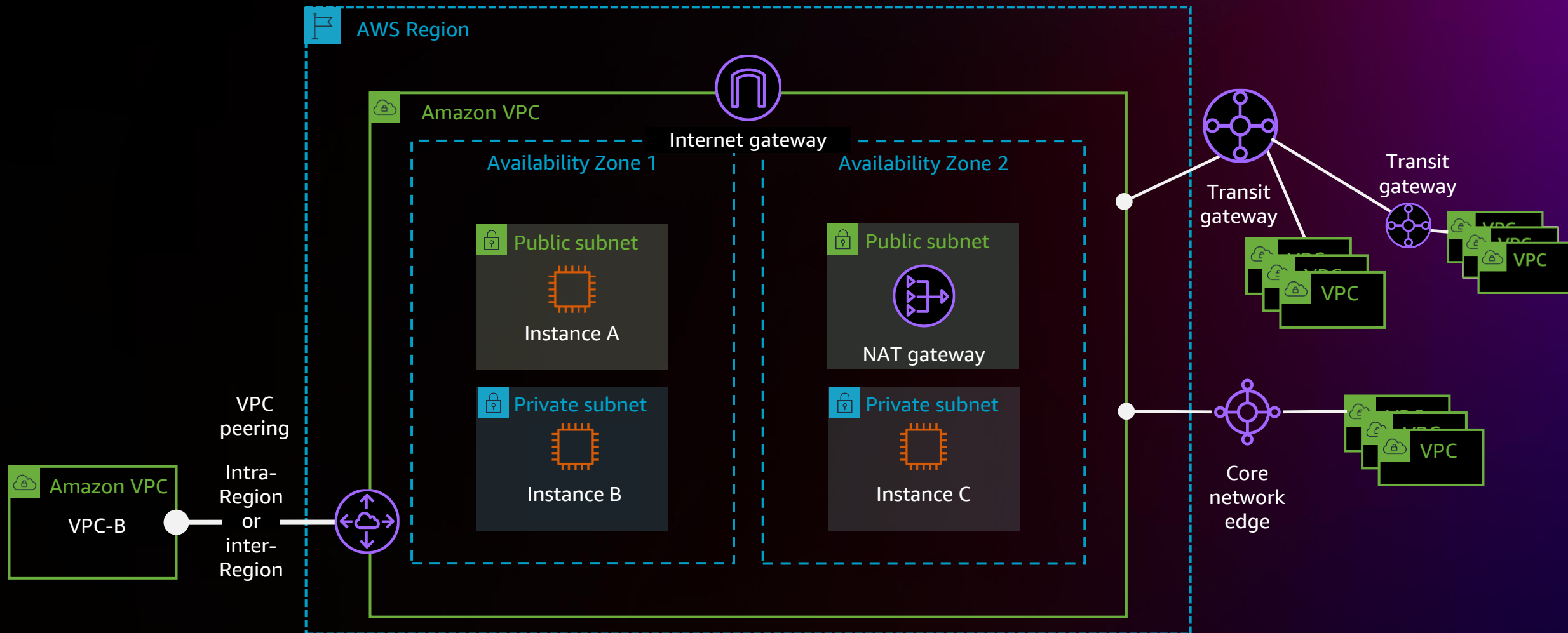
### Logs and dashboard

- 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

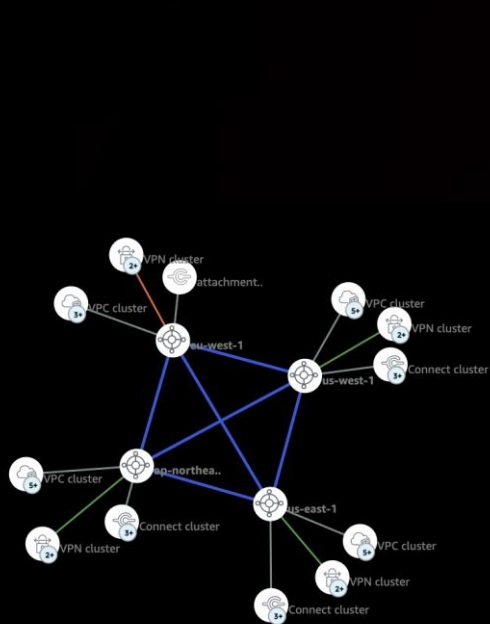


# Network monitoring

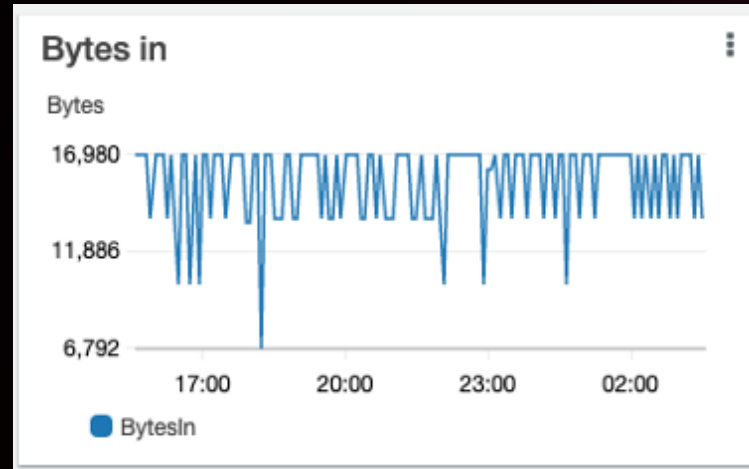
MONITORING NETWORKS ACROSS YOUR ORGANIZATION AND REGIONS



# AWS Network Manager



Topologies



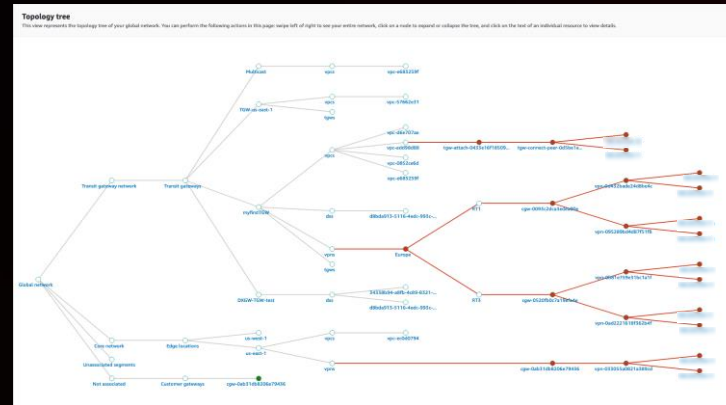
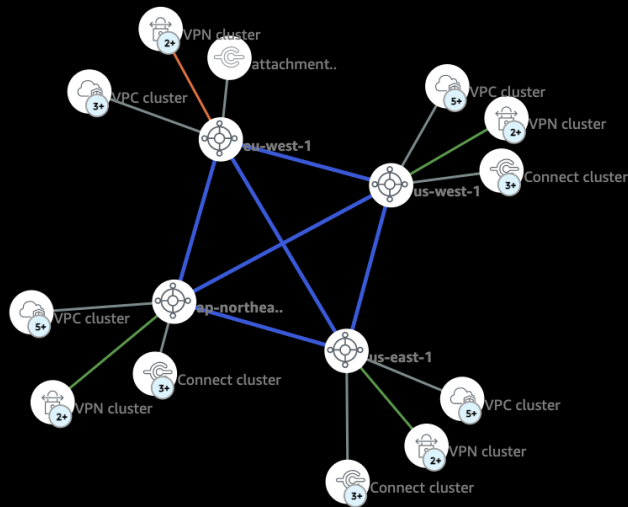
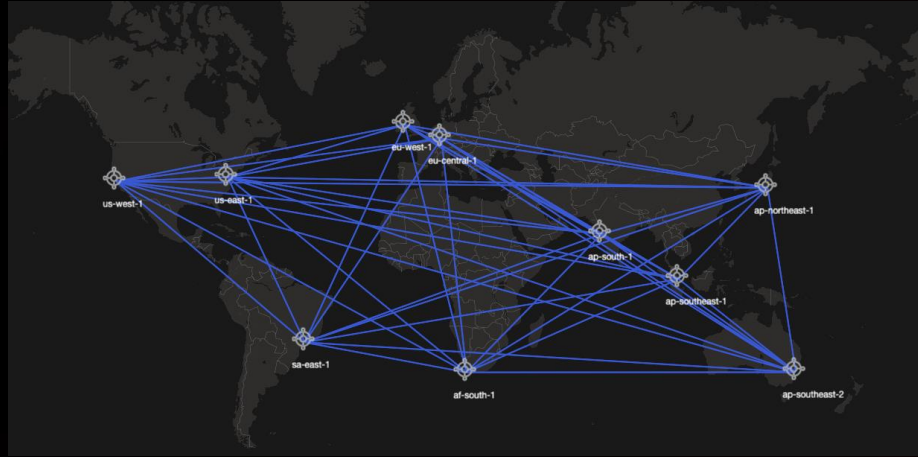
Metrics

#	Region	Message	Resource
▶1		BGP for a Connect peer has been established.	arn:aws:netwo
▶2		BGP for a Connect peer has been established.	arn:aws:netwo
▶3		IPsec for a VPN connection has come up.	arn:aws:netwo
▶4		IPsec for a VPN connection has come up.	arn:aws:netwo
▶5		BGP for a VPN connection has been established.	arn:aws:netwo
▶6		IPsec for a VPN connection has come up.	arn:aws:netwo
▶7		A Connect peer has been created in a Connect attachment.	arn:aws:netwo
▶8		An attachment has been associated to a Segment.	arn:aws:netwo
▶9		A Site-to-Site VPN attachment has been created for a Core Network.	arn:aws:netwo
▶10		IPsec for a VPN connection has come up.	arn:aws:netwo
▶11		IPsec for a VPN connection has come up.	arn:aws:netwo
▶12		Routes in one or more Segments have been installed.	arn:aws:netwo
▶13		IPsec for a VPN connection has come up.	arn:aws:netwo
▶14		BGP for a VPN connection has been established.	arn:aws:netwo
▶15		BGP for a VPN connection has gone down.	arn:aws:netwo
▶16		BGP for a VPN connection has been established.	arn:aws:netwo
▶17		BGP for a VPN connection has been established.	arn:aws:netwo
▶18		Routes in one or more Segments have been installed.	arn:aws:netwo
▶19		Routes in one or more Segments have been installed.	arn:aws:netwo

Events

# AWS Network Manager

## TOPOLOGY AND DASHBOARD



## Dashboard

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

## Topology graph

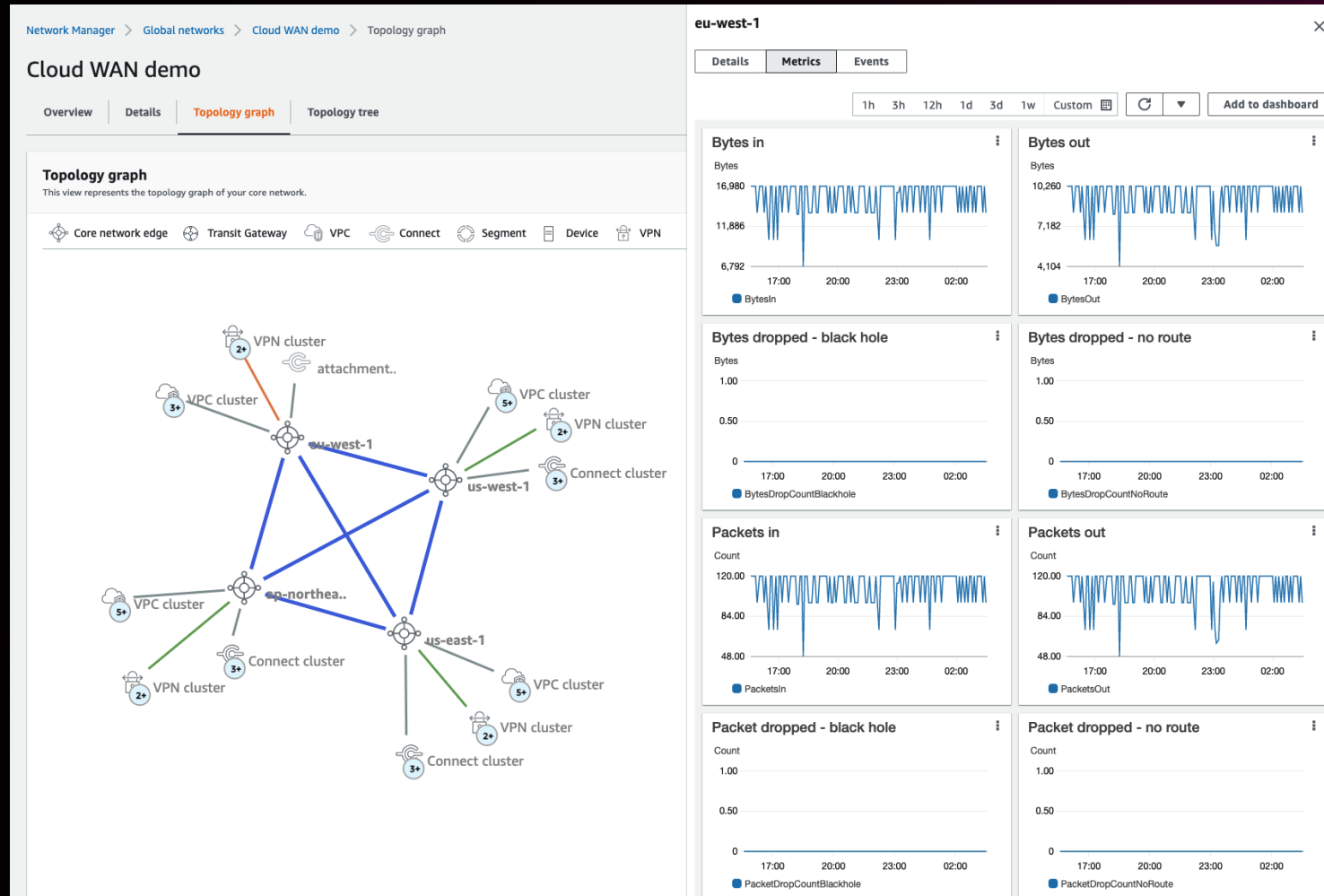
- AWS Regions
- Attachments
- Cross-Region peering
- Segments (optional)

## Topology tree

- Logical diagram

# AWS Network Manager

## METRICS



# AWS Network Manager

## EVENTS

eu-west-1

Details Metrics Events

Events

This section displays discrete network events that are sent to CloudWatch events. [Learn more](#)

1h 3h 12h 1d 3d 1w Custom

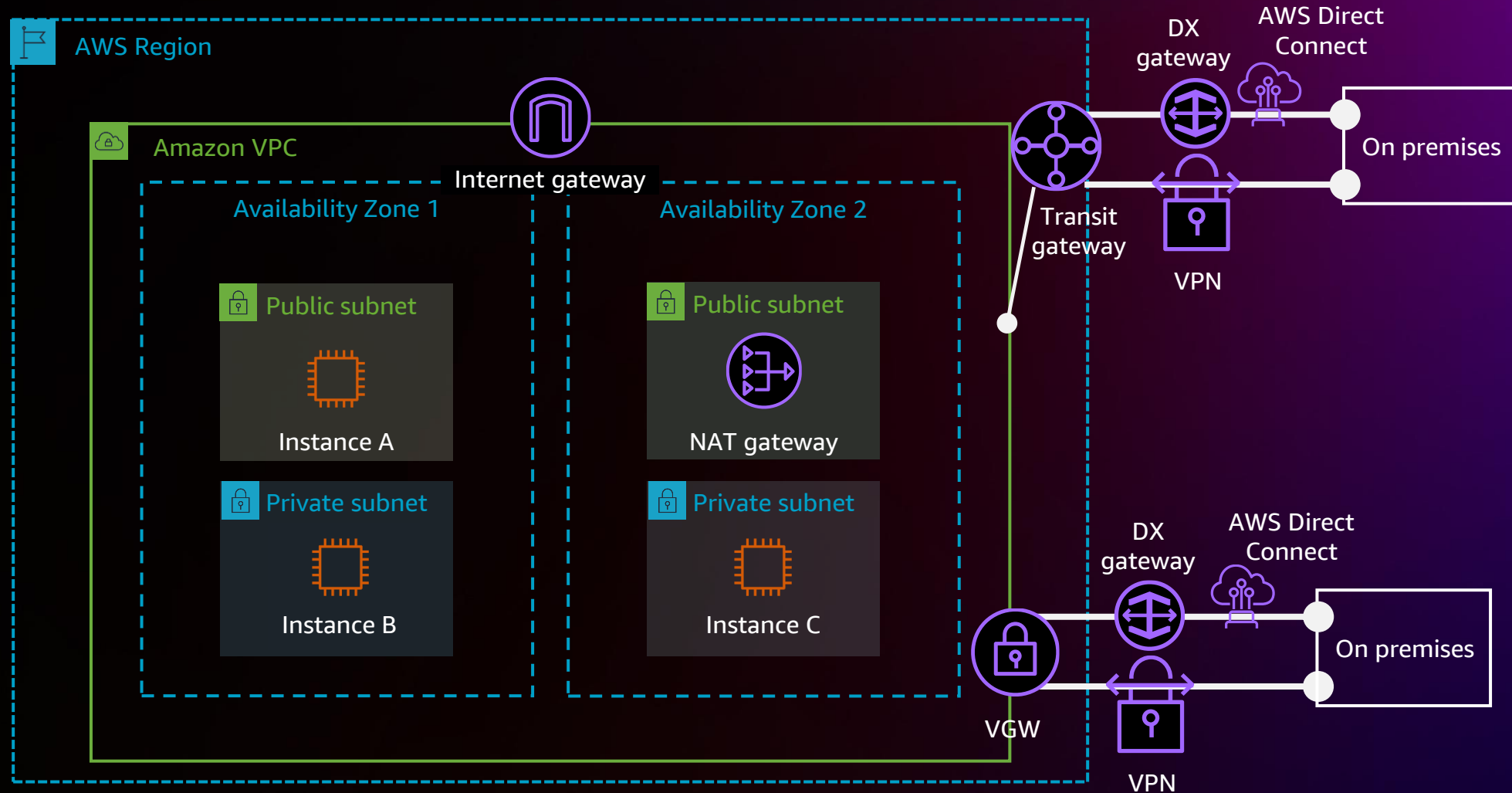
#	Region	Message	Resource
1		BGP for a Connect peer has been established.	arn:aws:netwo
2		BGP for a Connect peer has been established.	arn:aws:netwo
3		IPsec for a VPN connection has come up.	arn:aws:netwo
4		IPsec for a VPN connection has come up.	arn:aws:netwo
5		BGP for a VPN connection has been established.	arn:aws:netwo
6		IPsec for a VPN connection has come up.	arn:aws:netwo
7		A Connect peer has been created in a Connect attachment.	arn:aws:netwo
8		An attachment has been associated to a Segment.	arn:aws:netwo
9		A Site-to-Site VPN attachment has been created for a Core Network.	arn:aws:netwo
10		IPsec for a VPN connection has come up.	arn:aws:netwo
11		IPsec for a VPN connection has come up.	arn:aws:netwo
12		Routes in one or more Segments have been installed.	arn:aws:netwo
13		IPsec for a VPN connection has come up.	arn:aws:netwo
14		BGP for a VPN connection has been established.	arn:aws:netwo
15		BGP for a VPN connection has gone down.	arn:aws:netwo
16		BGP for a VPN connection has been established.	arn:aws:netwo
17		BGP for a VPN connection has been established.	arn:aws:netwo
18		Routes in one or more Segments have been installed.	arn:aws:netwo
19		Routes in one or more Segments have been installed.	arn:aws:netwo

- 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

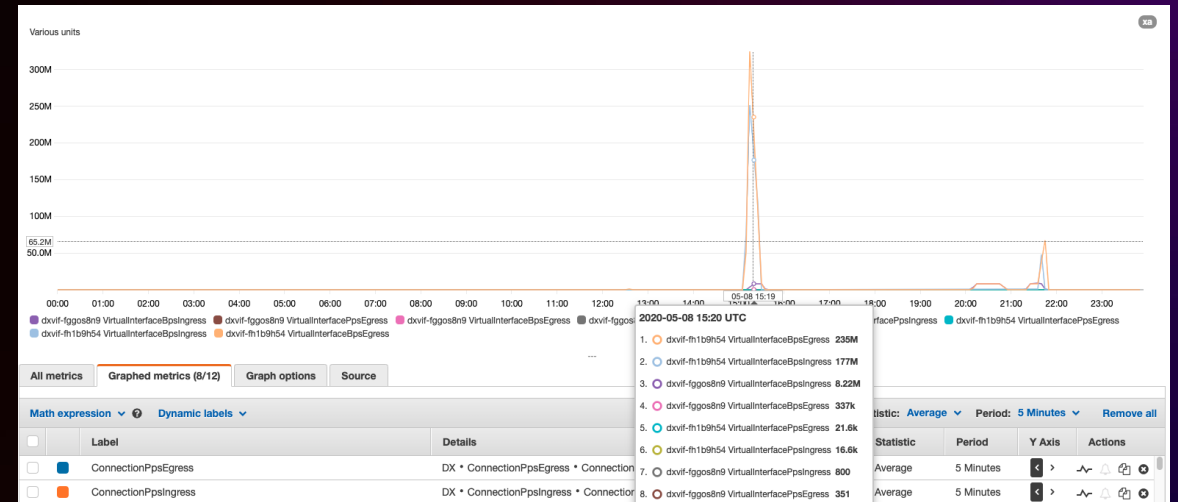
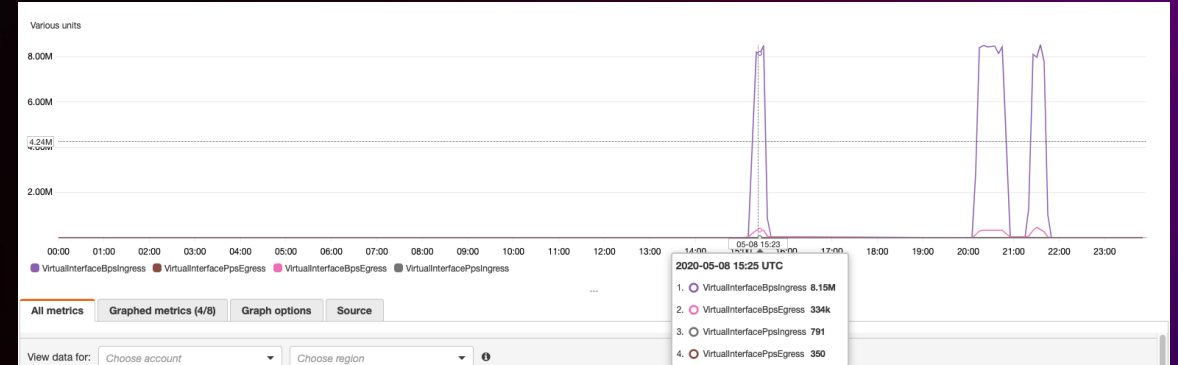
HYBRID CONNECTIVITY



# AWS Site-to-Site VPN and AWS Direct Connect

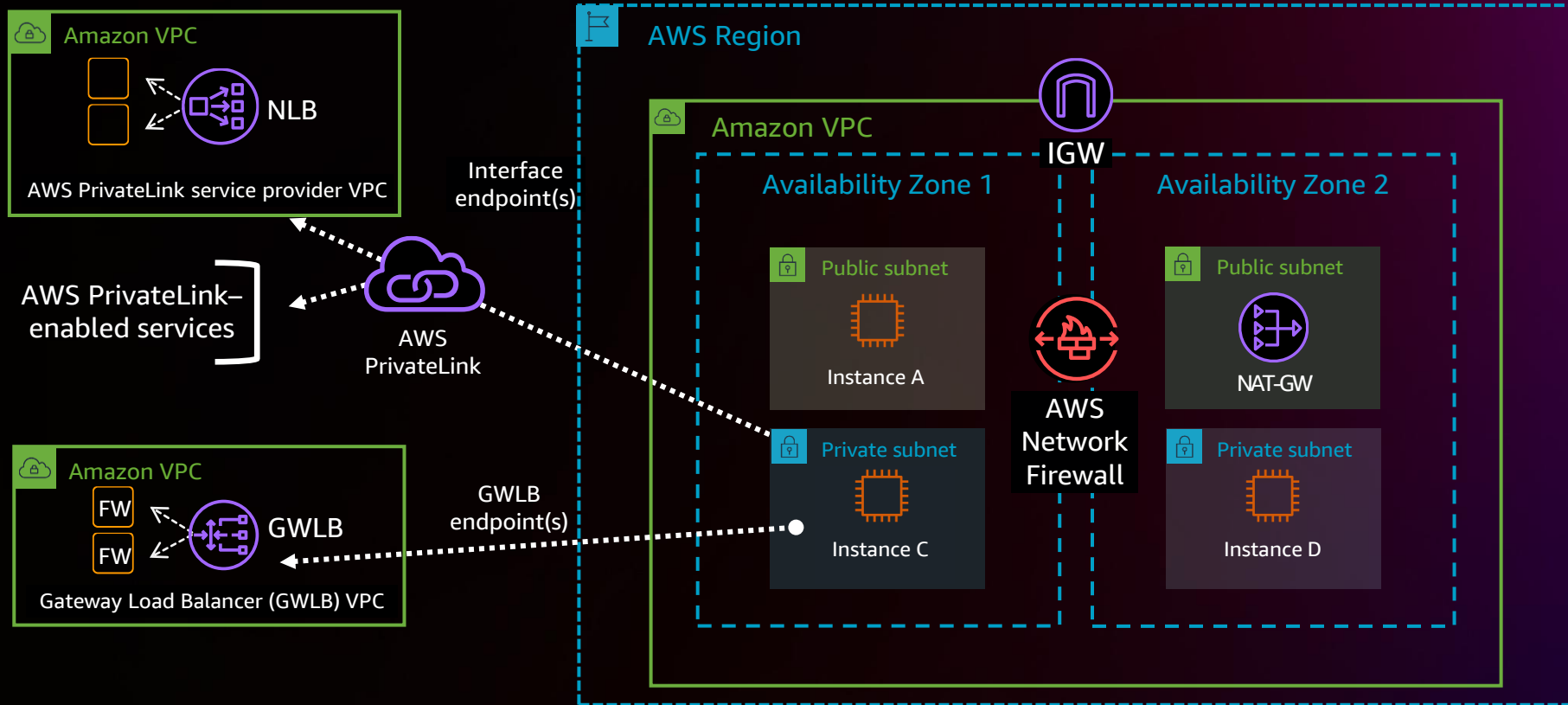
## METRICS

- 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

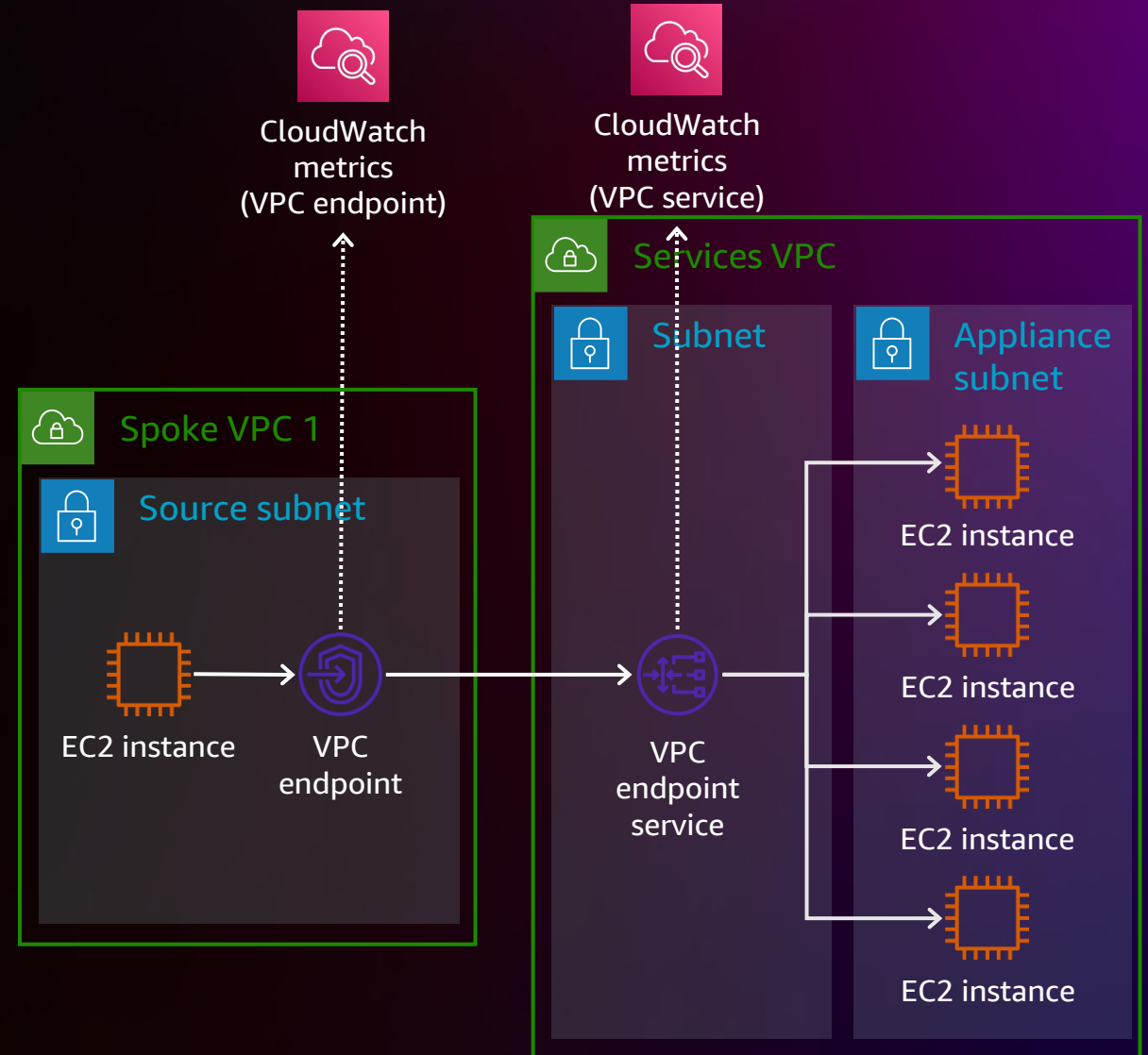
## ENDPOINT SERVICES



# 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



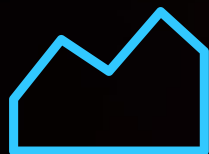
# Network monitoring best practices



Define KPIs



Resources to  
be monitored



Monitoring  
frequency



Monitoring tools



Monitoring team



Escalation  
path



Automation

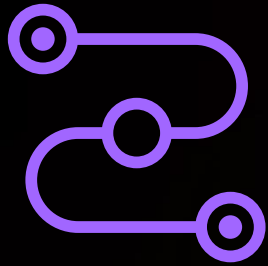
# Network analysis and troubleshooting



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

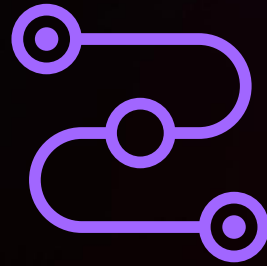
# Analyzing network configurations

TROUBLESHOOT AND VALIDATE NETWORK CONFIGURATIONS



## VPC Reachability Analyzer

Connectivity testing between a source resource and a destination resource



## Transit Gateway Route Analyzer

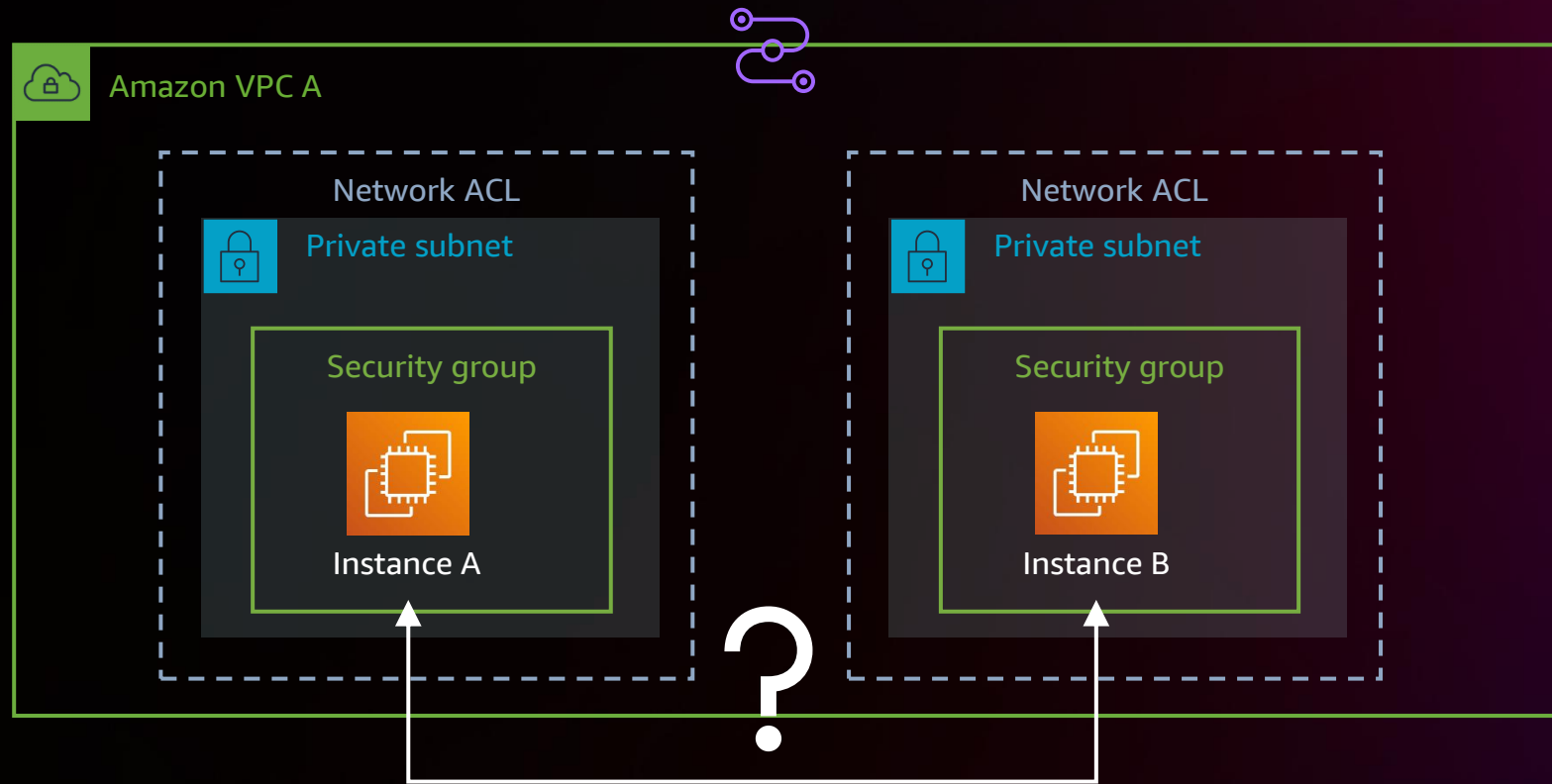
Perform an analysis of the routes in your transit gateway route tables



## Network Access Analyzer

Identifies unintended network access to your resources on AWS

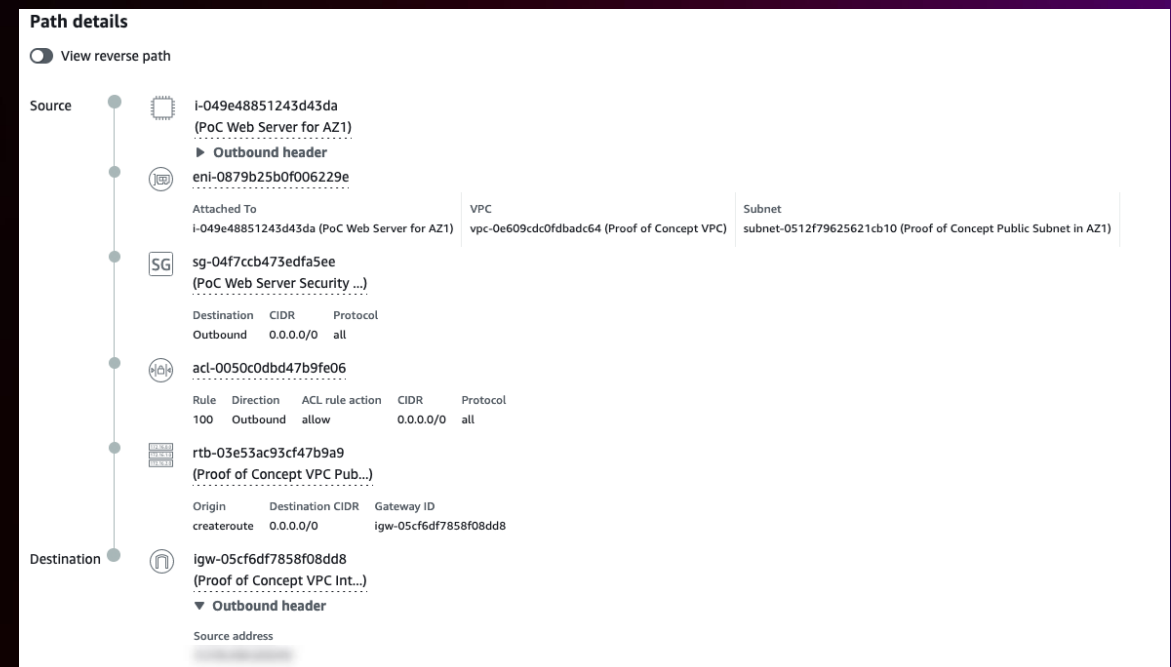
# VPC Reachability Analyzer



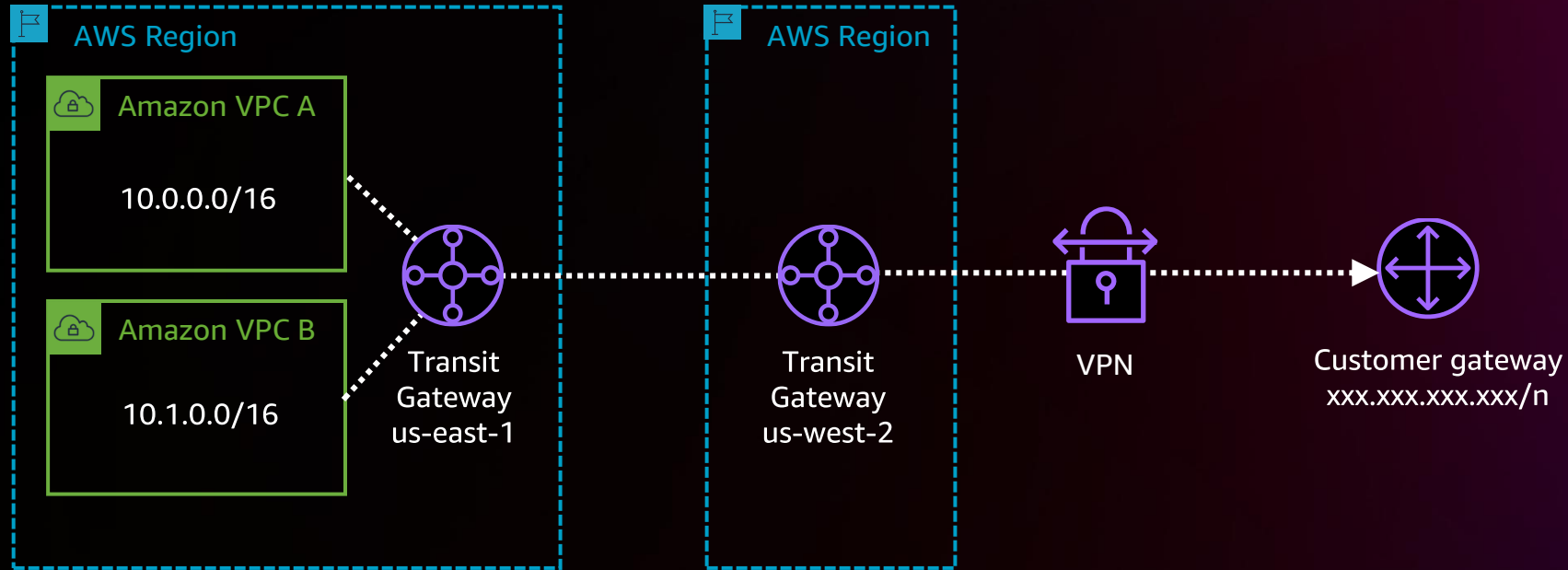
How can I verify connectivity between a source resource and a destination resource?

# 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

The screenshot displays the 'Results of route analysis' interface. It includes a summary table for both forward and return paths, a detailed path diagram, and a warning message.

**Results of route analysis**  
The result of source and destination route is displayed here. You can update either the source and/or destination and re-run the analysis for updated results.

Forward path		
Source	Destination	Status
tgw-attach-0aee	tgw-attach-0670	Connected

Return path		
Source	Destination	Status
tgw-attach-0670	tgw-attach-0aee	Not connected

**Warning:** There is no matching route for destination in Transit Gateway route table tgw-rtb-0994 of Transit Gateway tgw-05eal in region eu-central-1.

**Path Diagram:**

- Source:** 10.0.0.12
- Forward Path:** TGW-NM-W-1 (tgw-attach-0aee) VPC us-west-2 → tgw-rtb-00b6 Transit Gateway route table us-west-2 tgw-088b → TGW-Peer-F-W (tgw-attach-0f4) Peering eu-central-1 → tgw-rtb-0994 Transit Gateway route table eu-central-1 tgw-05eal
- Destination:** 10.0.2.74
- Return Path:** TGW-NM-F-1 (tgw-attach-0670) VPC eu-central-1 → tgw-rtb-0994 Transit Gateway route table eu-central-1 tgw-05eal
- Final Status:** Not connected

# 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

### Network Access Scopes (1/4)

Filter Network Access Scopes

	Name
<input type="checkbox"/>	AWS-VPC-Ingress (Amazon cre
<input checked="" type="checkbox"/>	All-IGW-Ingress (Amazon crea
<input type="checkbox"/>	AWS-VPC-Egress (Amazon cre
<input type="checkbox"/>	AWS-IGW-Egress (Amazon cre

### Select Network Access Scope template

#### Select template

Build your Network Access Scope starting from a template based on common network access scenarios.

Identify access from Internet Gateways

Example

- Locate databases accessible from internet.
- Find non-HTTPS access to web servers

Identify access to Internet Gateways

Example

- Locate instances with un-authorized internet access

Validate access from trusted networks

Example

- Containers can only be accessed via load balancers
- Only Bastions can SSH to production
- Only App Servers can access Database Servers

Identify non-permissible traffic type

Example

- Only Web servers can receive HTTP/HTTPS traffic
- Production servers cannot send SSH/RDP traffic
- Development cannot SSH to Production.

Validate network segmentation

Example

- Development should be isolated from Production.
- PCI should be isolated from Non-PCI.

Empty template

Build your own Network Access Scope

Network Access Scope

Analyze

< 1 > ⚙

Network Access

, VPN and Transit G...	nis-02816534
	nis-027b4b14
s from all of your V...	nis-0ca8a24e
	nis-0d428a40



# How Network Access Analyzer works

RUN ANALYSIS AND REVIEW FINDINGS

VPC > Network Access Scopes > nis-02816534ee37f958e

## nis-02816534ee37f958e / AWS-VPC-Ingress (Amazon created)

Summary [Info](#) Actions ▾ Analyze

Network Access Scope ID: nis-02816534ee37f958e | Name: AWS-VPC-Ingress (Amazon created) | Description: Identify ingress paths into your VPCs from Internet Gateways, Peering Connections, VPC Service Endpoints, VPN and Transit Gateways.

▶ Network Access Scope definition


Latest analysis | Past analyses | Tags

### Analysis details Delete analysis

Analysis ID: nisa-070e95a2229814f60 | Last analysis date: January 11, 2022, 17:04 (UTC-05:00) | Last analysis result: Findings detected (Limited findings are displayed [Info](#)) | Analysis status: Complete | Network Interfaces analyzed: 47

#### Filter findings by category [Info](#)

This chart shows the number of occurrences of various resources in the findings. Select resource(s) to filter for findings containing the resource.



- Security Groups (160)
- Network ACLs (150)
- Network Interfaces (100)
- Transit Gateway Attachments (47)

#### Findings (100) [Info](#)

Filter findings by resource types or specific resources present in the findings.

Source	Destination	Path details
igw-040dfd6a4fa35fed0 (...)	eni-0db4ab5a420685731...	Internet Gateway -> Network Interface
igw-06a2e02304a25c68a (...)	eni-010ca85d7013faa7c (...)	Internet Gateway -> Network Interface
igw-06a2e02304a25c68a (...)	eni-010ca85d7013faa7c (...)	Internet Gateway -> Network Interface
igw-040dfd6a4fa35fed0 (...)	eni-033e6921e024e833c (...)	Internet Gateway -> Network Interface -> Security Group -> Network Interface
igw-040dfd6a4fa35fed0 (...)	eni-033e6921e024e833c (...)	Internet Gateway -> Network Interface -> Security Group -> Network Interface -> Security Group -> Network Interface
igw-040dfd6a4fa35fed0 (...)	eni-033e6921e024e833c (...)	Internet Gateway -> Network Interface -> Security Group -> Network Interface -> Security Group -> Network Interface -> Security Group -> Network Interface
tgw-attach-08430ac985c...	eni-00ccf7431a0fcfc5e (r...	Transit Gateway Attachment -> Network Interface
tgw-attach-08430ac985c...	eni-010ca85d7013faa7c (...)	Transit Gateway Attachment -> Network Interface
tgw-attach-08430ac985c...	eni-00ccf7431a0fcfc5e (r...	Transit Gateway Attachment -> Network Interface -> Security Group -> Network Interface

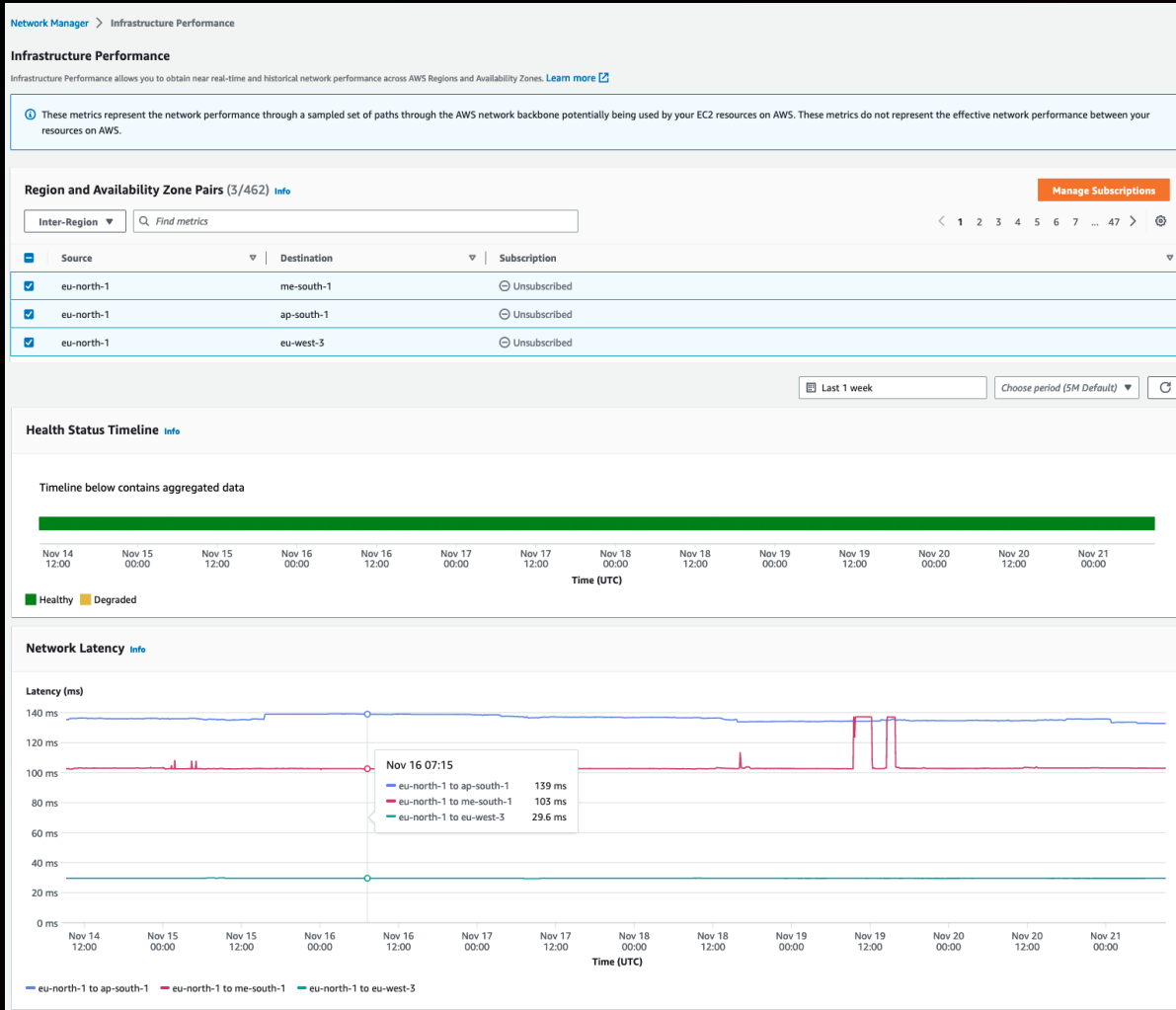


# How can I identify network performance issues on AWS or out on the internet?



# 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.

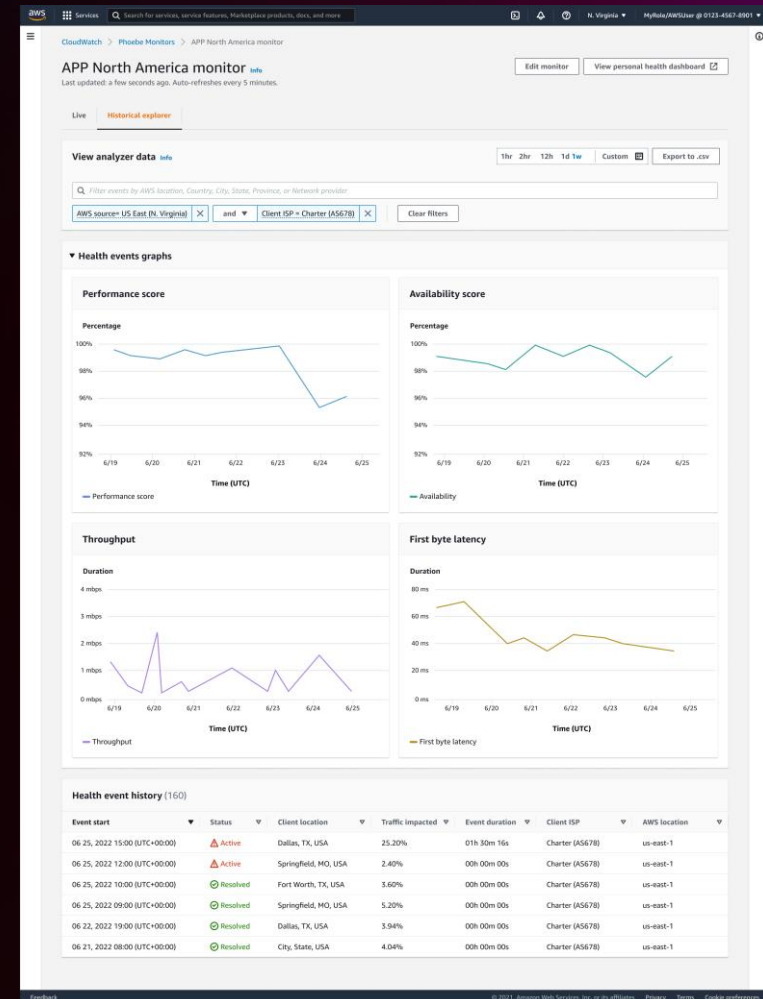


# Amazon CloudWatch Internet Monitor

Preview

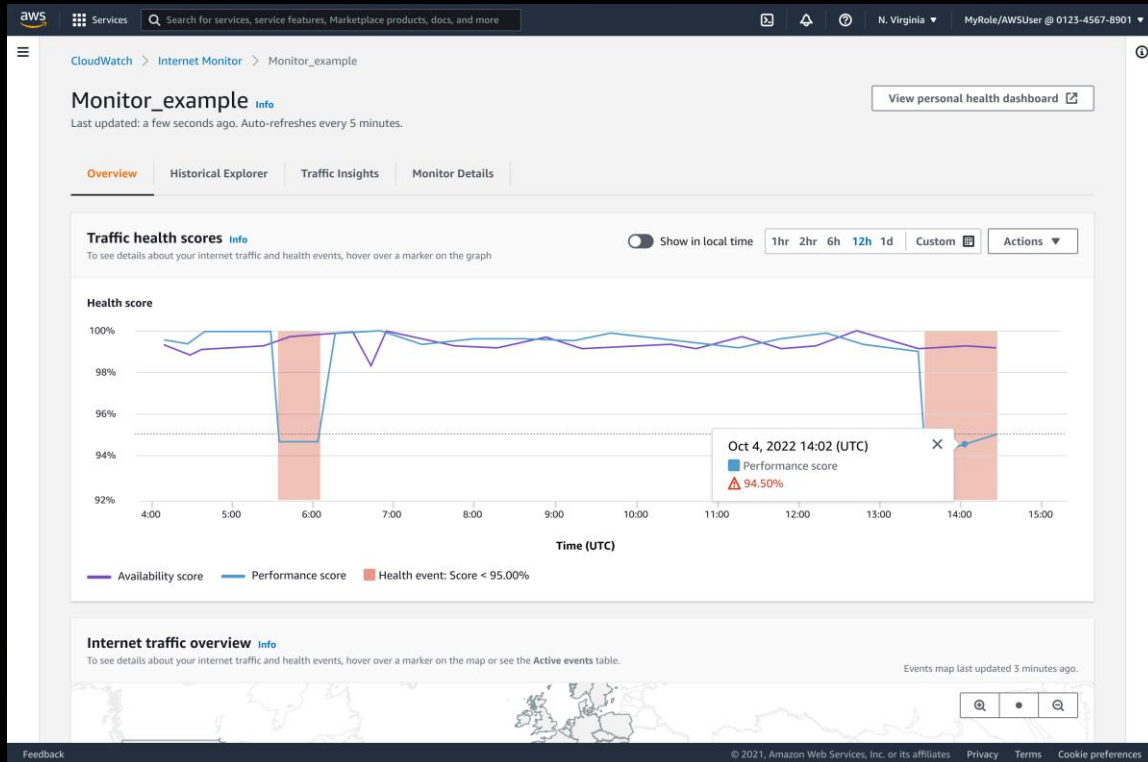
## OVERVIEW

- 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

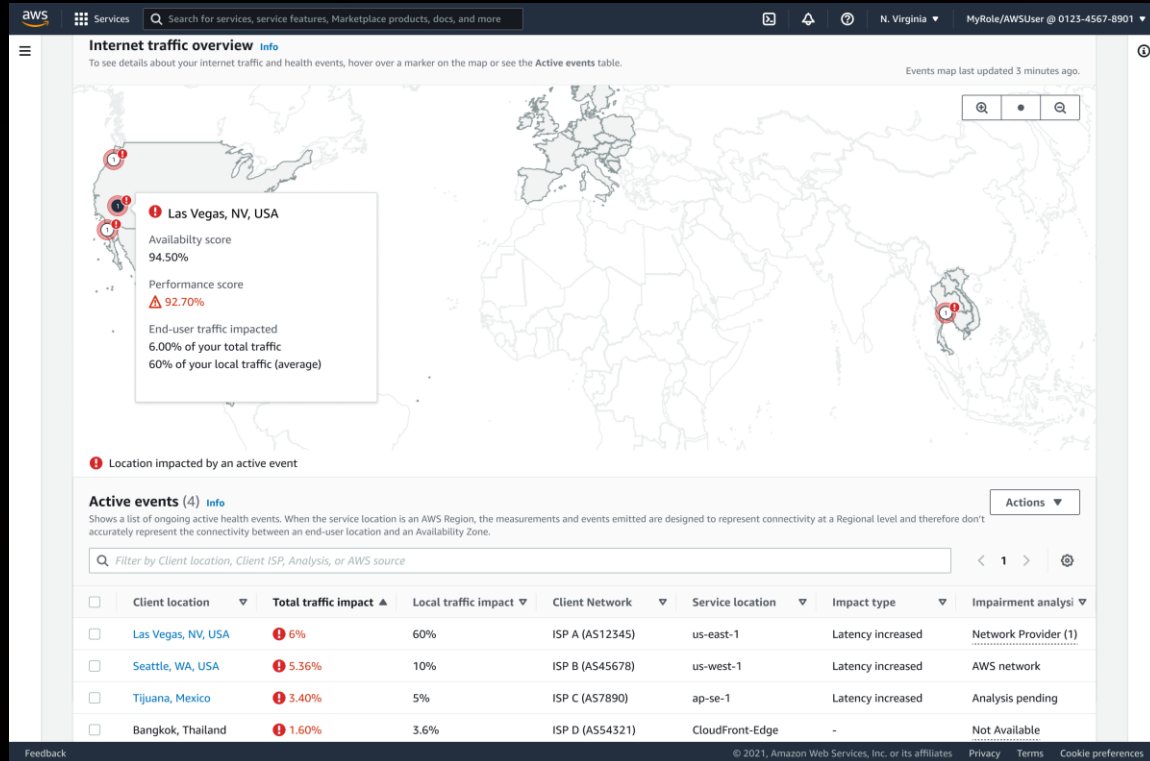
## HEALTH SCORE



- 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

The screenshot displays the Amazon CloudWatch Internet Monitor interface. At the top, there is a search bar and navigation options. Below this is a table listing various client locations and their associated traffic impact and impairment analysis.

Client location	Total traffic impact	Local traffic impact	Client Network	Service location	Impact type	Impairment analysis
Las Vegas, NV, USA	6%	60%	ISP A (AS12345)	us-east-1	Latency increased	Network Provider (1)
Seattle, WA, USA	5.36%	10%	ISP B (AS45678)	us-west-1	Latency increased	AWS network
Tijuana, Mexico	3.40%	5%	ISP C (AS7890)	ap-se-1	Latency increased	Analysis pending
Bangkok, Thailand	1.60%	3.6%	ISP D (AS54321)	CloudFront-Edge	-	Not Available

Below the table, the interface shows details for the selected event in Las Vegas, NV, USA. The 'Current event' section indicates the event started at 2022-06-25T14:32:35. Key metrics include an event duration of 36m57s, 6% total traffic impacted, and 60% local traffic impacted. The 'Impairment Analysis' section shows the event status as 'Active' and the impairment type as 'Latency increased'.

The 'Network path visualization' section shows a sequence of nodes: Amazon.com (AS 16509), ISP name example (AS 9999), ISP name example (AS 7777), ISP A (AS 12345), and Las Vegas, NV, USA. The ISP A node is highlighted with a red dashed circle, indicating it is the source of the impairment. A legend at the bottom identifies node status (impaired vs. normal) and node types (Amazon.com, Network Provider, End-user Location).

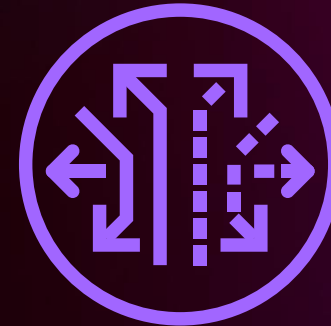
**How can I capture flows  
and packets to understand  
the traffic flowing across  
my network?**

# Traffic visibility options



**VPC Flow Logs**

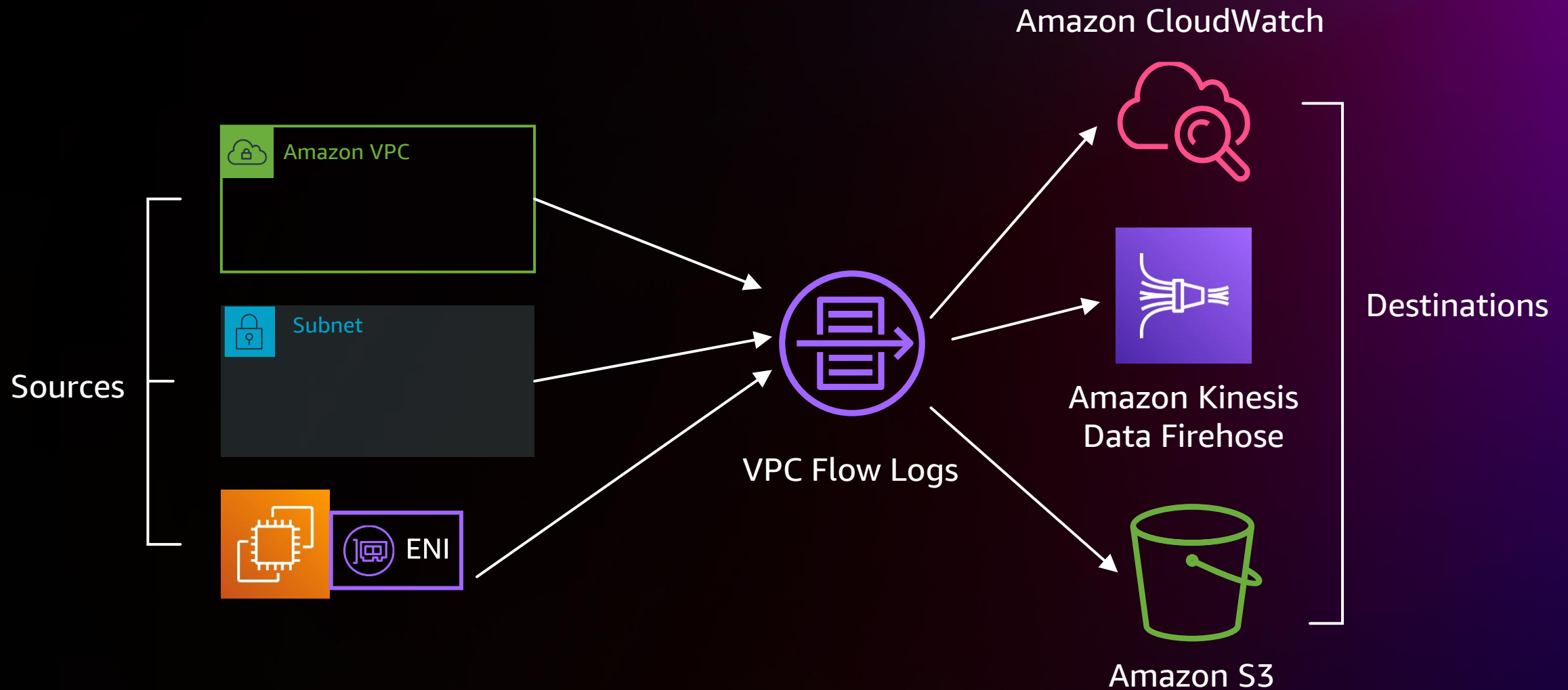
Collect and store metadata information



**Traffic Mirroring**

Copies network traffic,  
including payload

# VPC Flow Logs



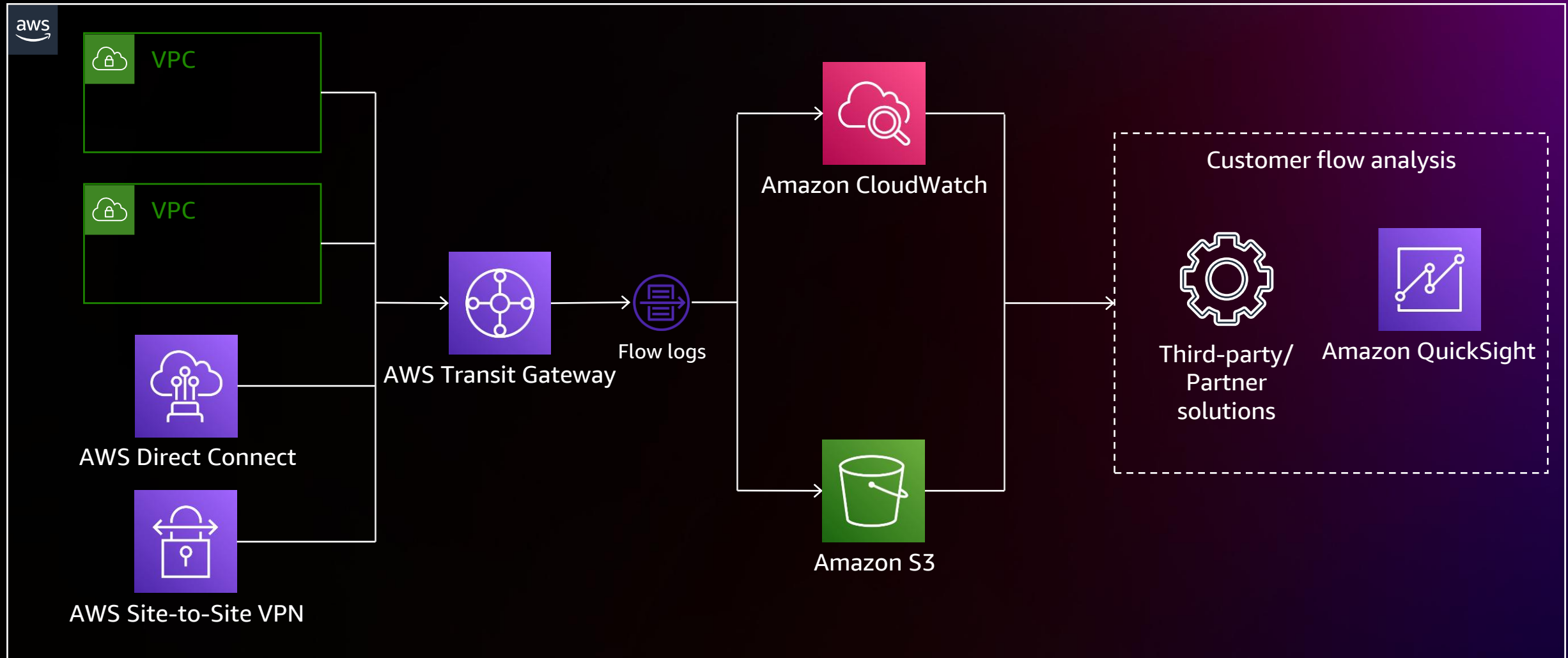
# VPC Flow Logs

## 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

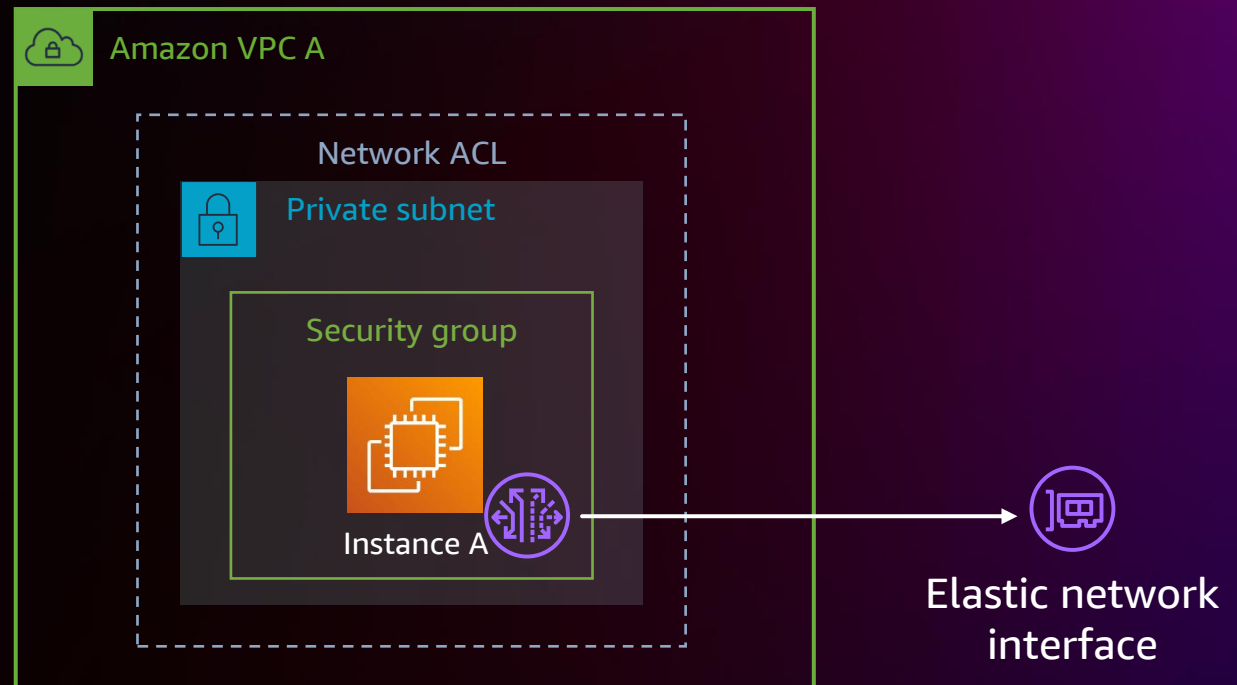
Version	2
Account ID	XXXXXXXX1234
Interface ID	eni-04b10a1942977452f
Source Address	xxx.xxx.xxx.xxx
Destination Address	xxx.xxx.xxx.xxx
Source Port	36490
Destination Port	443
Protocol	6
Packets	77
Bytes	5040
Start	1560385064
End	1560385070
Action	ACCEPT
Log Status	OK

# VPC Flow Logs for Transit Gateway



# Traffic Mirroring with Amazon VPC

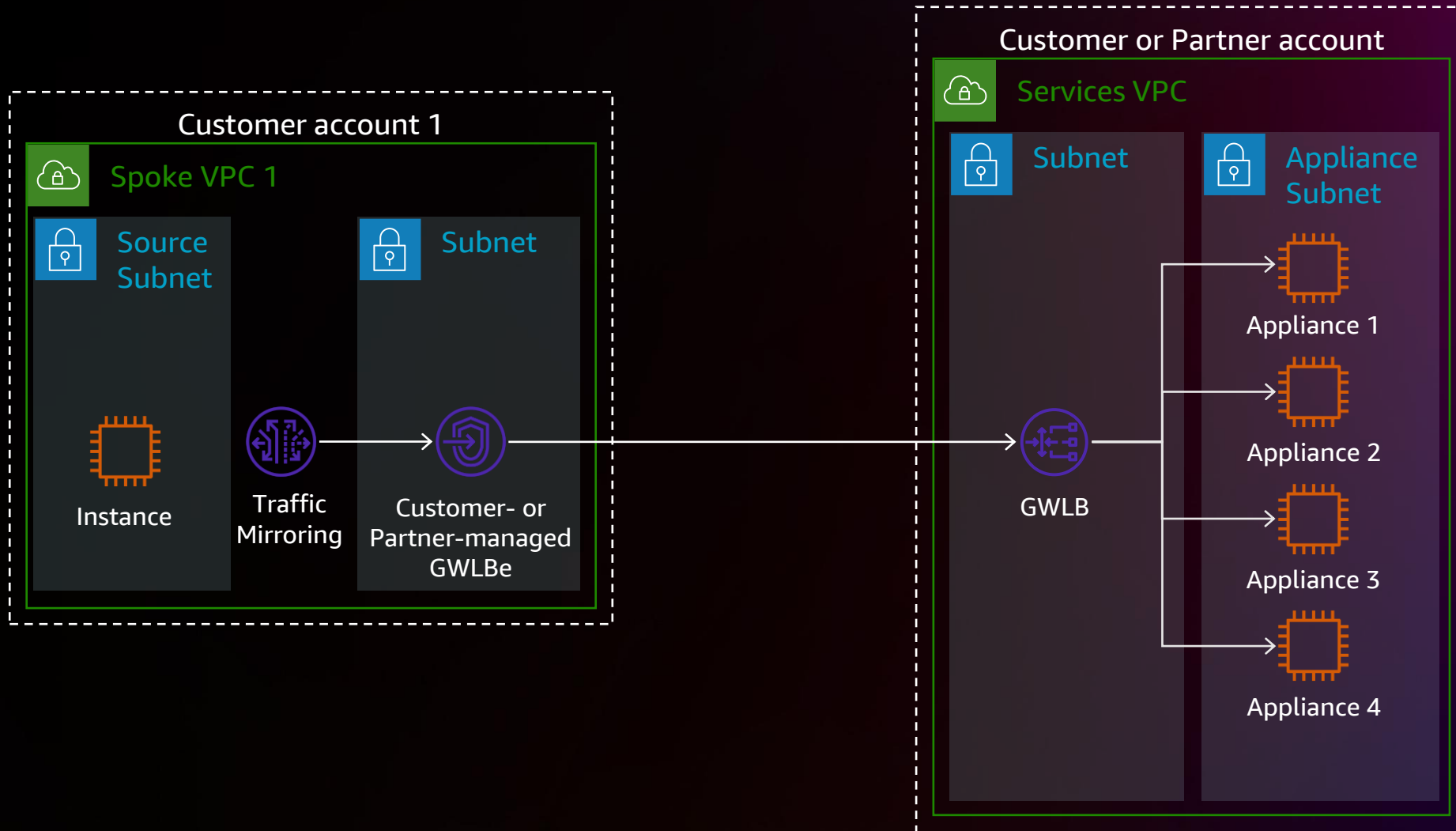
- Copy network traffic from an elastic interface of an Amazon EC2 instance, a Network Load Balancer, or a Gateway Load Balancer
- Send the traffic to out-of-band security and monitoring appliances for content inspection, threat monitoring, or troubleshooting
- Identify the block component when the destination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



IP-UDP	VXLAN header	Payload (Original L3 packet)
--------	--------------	---------------------------------

# Traffic Mirroring

GATEWAY LOAD BALANCER ENDPOINT (GWLBE) AS A TARGET



# Summary of network observability

## Collect



Metrics



Logs

## Monitor



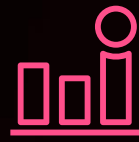
Alarms



Flow Logs

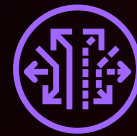


CloudWatch dashboards

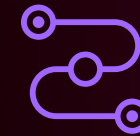


CloudWatch metric filter

## Analyze



Traffic Mirroring



Reachability Analyzer



Amazon CloudWatch Contributor Insights



CloudWatch Log Insights



Network Access Analyzer



Third-party solution

# Thank you!

Sohaib Tahir

sohaibt@amazon.com

Riggs Goodman III

goriggs@amazon.com



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

