
AWS
re:Invent

NET207

Monitoring and troubleshooting network traffic

Rithisha Padmanabh

Senior Product Manager-Tech

AWS

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Learning Objectives



Monitor your AWS network traffic

VPC Flow Logs



Gain deeper visibility into the payload

VPC Traffic Mirroring



Track network performance of EC2 instances

EC2 Instance-Level Metrics

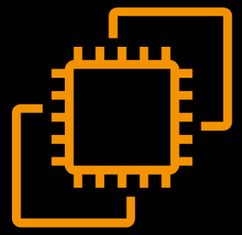


Troubleshoot network connectivity issues

VPC Reachability Analyzer

NEW

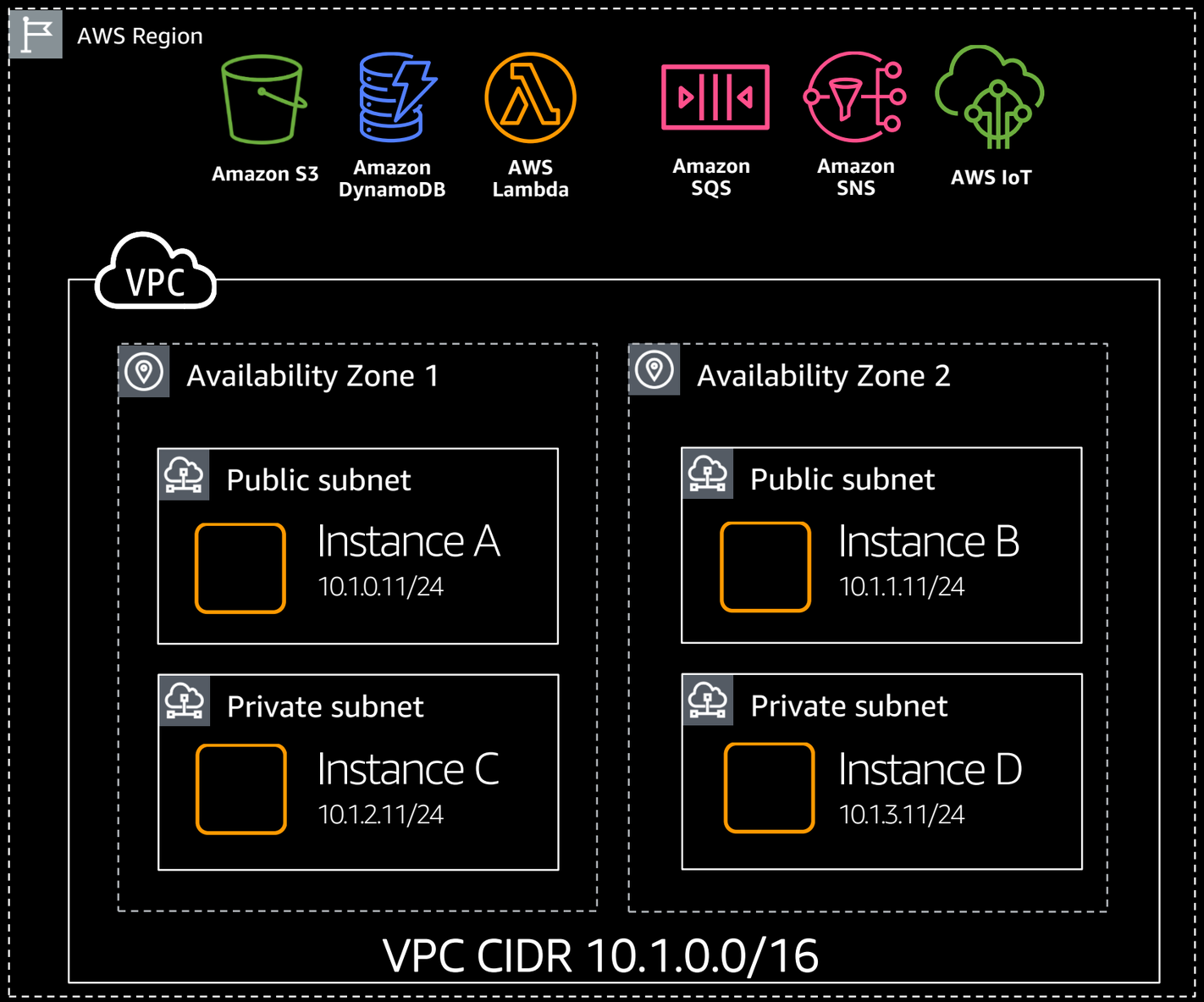
AWS Networking Recap

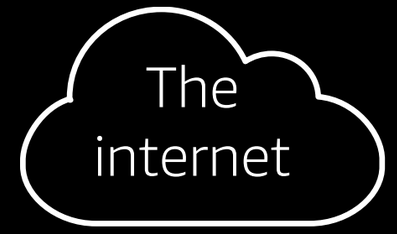


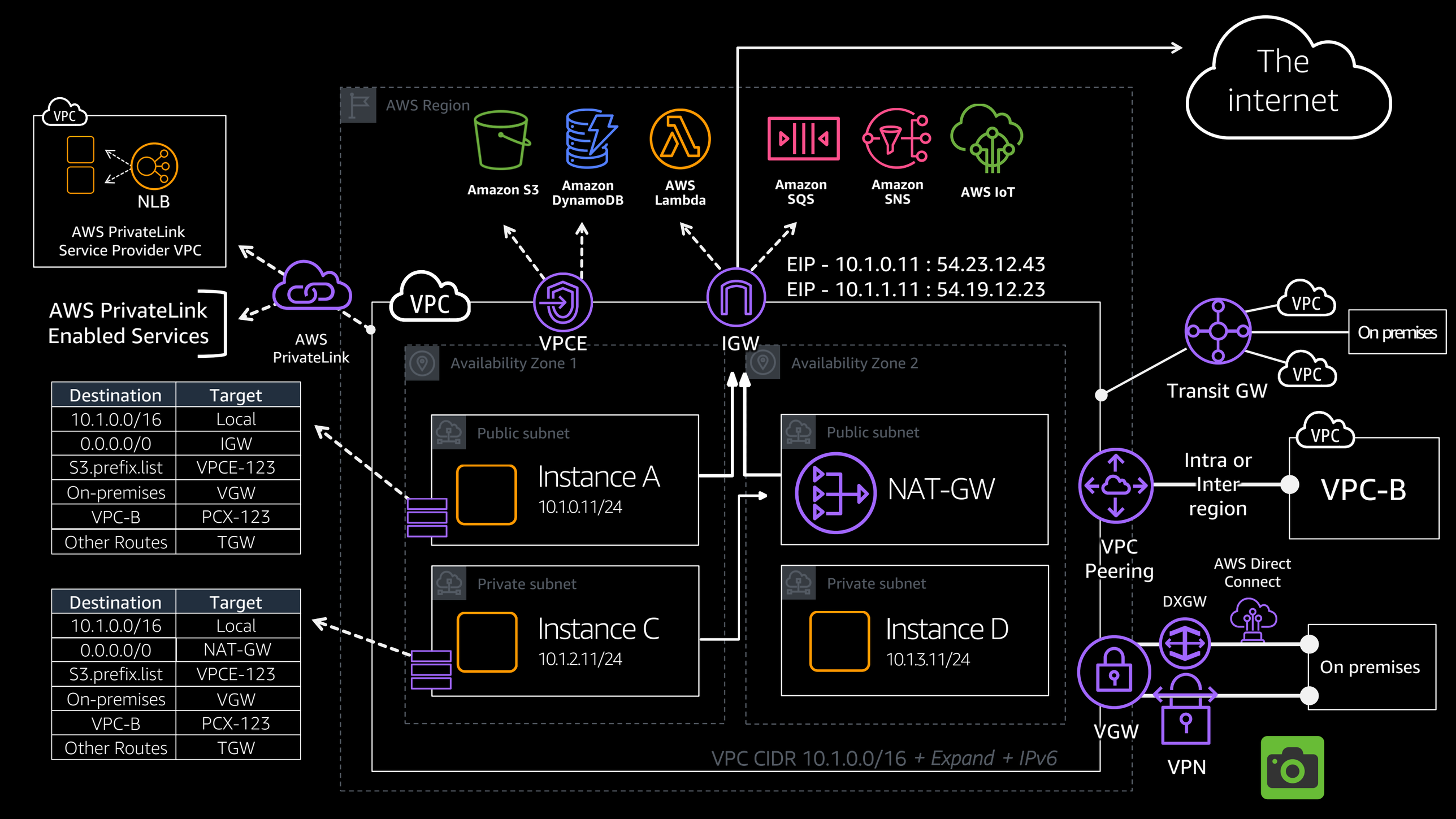
Amazon EC2



Amazon VPC






The internet
AWS Region
Amazon S3
Amazon DynamoDB
AWS Lambda
Amazon SQS
Amazon SNS
AWS IoT
VPC
NLB
AWS PrivateLink Service Provider VPC
AWS PrivateLink Enabled Services
AWS PrivateLink
VPCE
IGW
EIP - 10.1.0.11 : 54.23.12.43
EIP - 10.1.1.11 : 54.19.12.23
Availability Zone 1
Availability Zone 2
Public subnet
Instance A
10.1.0.11/24
NAT-GW
Private subnet
Instance C
10.1.2.11/24
Instance D
10.1.3.11/24
VPC CIDR 10.1.0.0/16 + Expand + IPv6
Transit GW
On premises
Intra or Inter region
VPC-B
VPC Peering
AWS Direct Connect
DXGW
VGW
VPN
Destination
Target
10.1.0.0/16
Local
0.0.0.0/0
IGW
S3.prefix.list
VPCE-123
On-premises
VGW
VPC-B
PCX-123
Other Routes
TGW
Destination
Target
10.1.0.0/16
Local
0.0.0.0/0
NAT-GW
S3.prefix.list
VPCE-123
On-premises
VGW
VPC-B
PCX-123
Other Routes
TGW

How do you get visibility into your AWS network traffic?



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

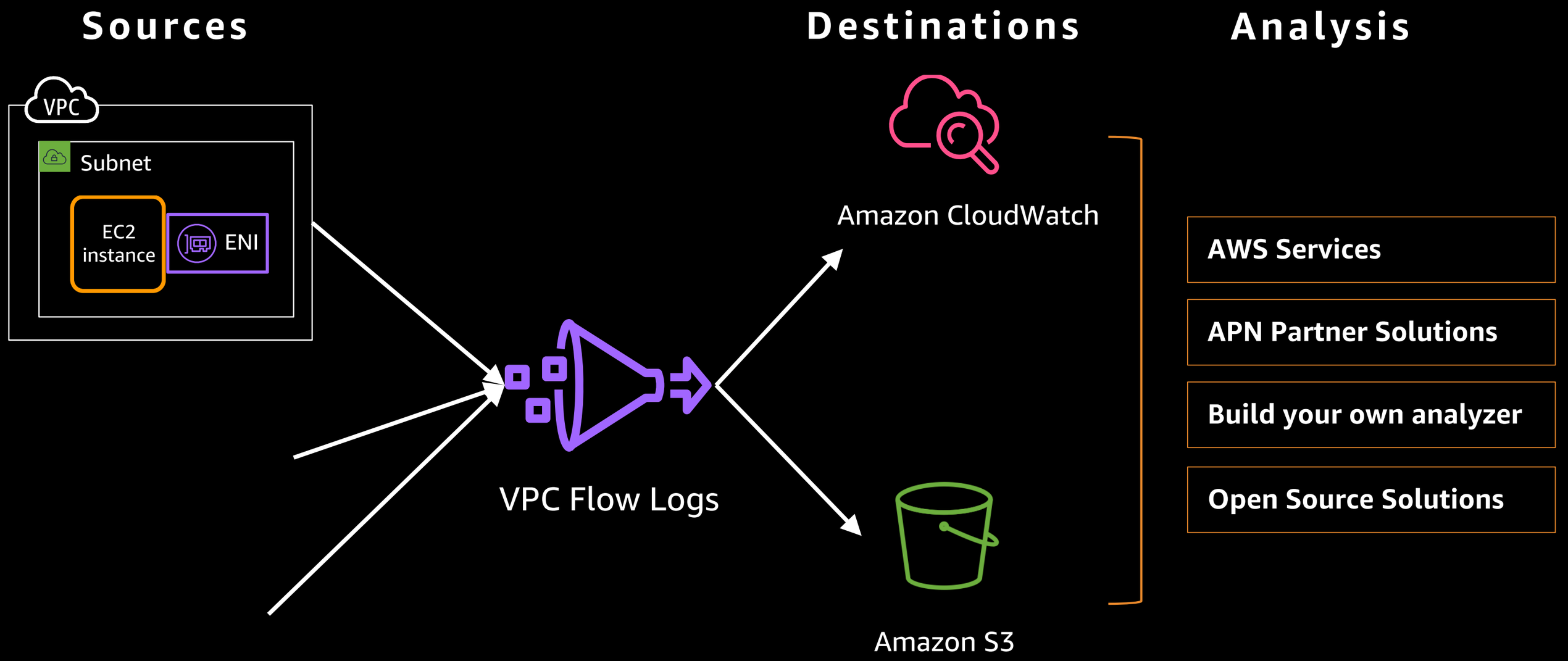
Amazon VPC Flow Logs



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Life of a VPC Flow Log



Analyze VPC Flow Logs with

AWS Services


CloudWatch Log Insights


CloudWatch Contributor Insights


Amazon Athena


Amazon QuickSight


Amazon Elasticsearch Service

AWS Partners*

splunk> sumo logic

DATADOG

CISCO STEALTHWATCH CLOUD

CHECK POINT CloudGuard

New Relic.

d10 networks

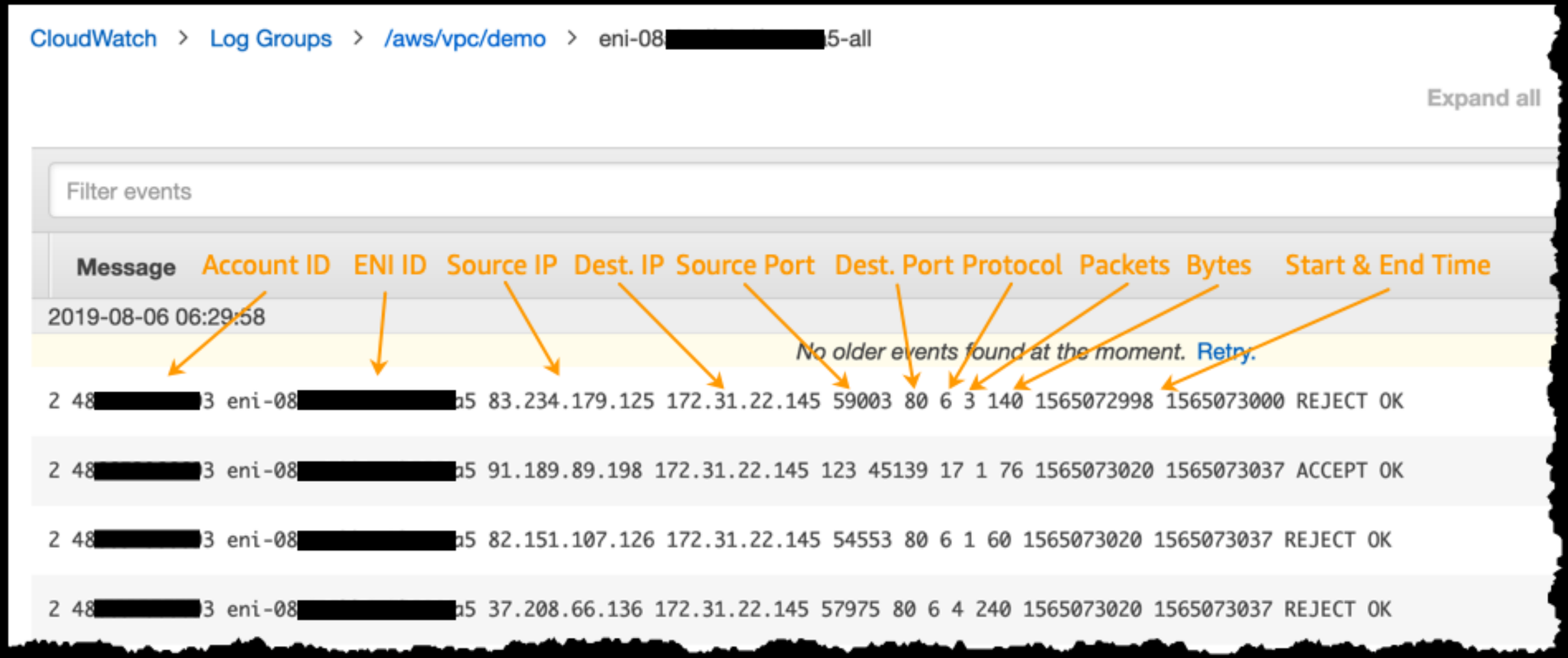
*This is not a complete list; to view all AWS Partners who offer this capability, see: https://amzn.to/3euswFI

What does a Flow Log look like?



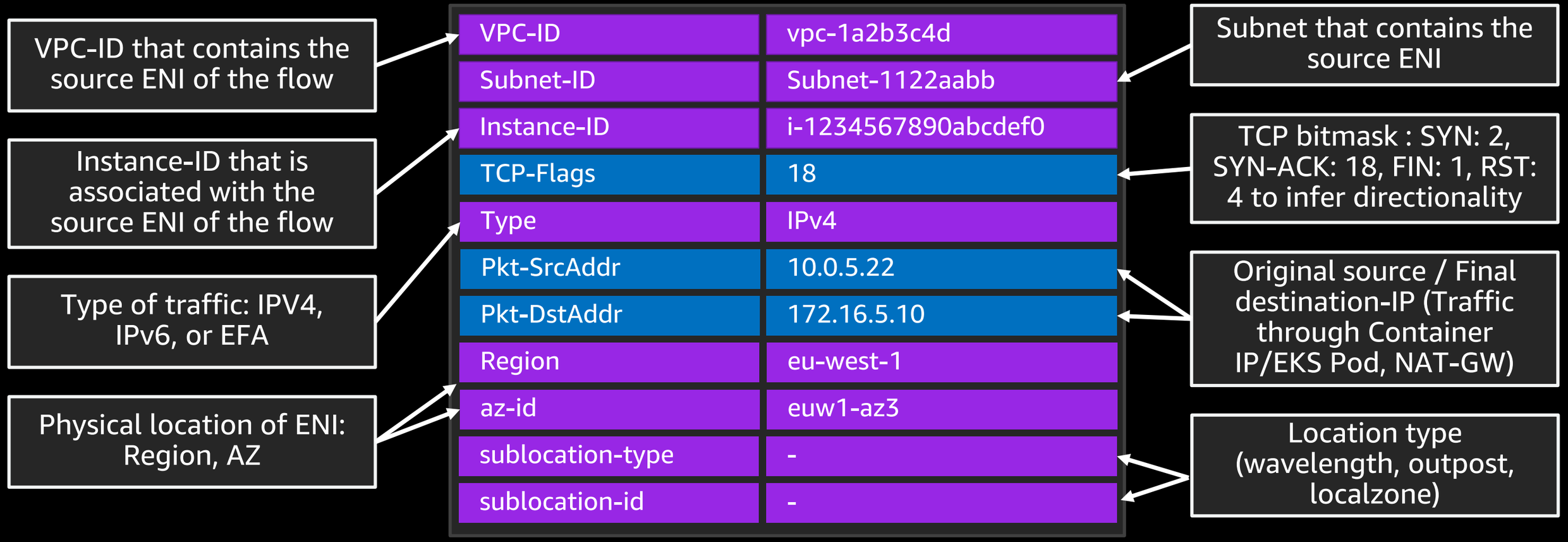
© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Flow Log Contents



Enriched Flow Log Contents

NEW



1-Minute Aggregation Intervals

NEW

Create flow log Info

Flow logs can capture IP traffic flow information for the network interfaces associated with your resources. You can create multiple flow logs to send traffic to different destinations.

Selected resources Info

Name	Resource ID	State
	vpc-d1e8beab	Available

Flow log settings

Name - *optional*

my-vpc-flow-log

Filter

The type of traffic to capture (accepted traffic only, rejected traffic only, or all traffic).

- Accept
- Reject
- All

Maximum aggregation interval Info

The maximum interval of time during which a flow of packets is captured and aggregated into a flow log record.

- 10 minutes
- 1 minute

Destination

The destination to which to publish the flow log data.



Fine-grained visibility and troubleshooting



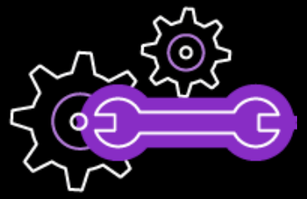
Faster threat detection and response

How are customers using VPC Flow Logs?



Visibility

Gain operational visibility into traffic patterns and application dependencies



Troubleshooting

Diagnose connectivity and configuration issues and data transfer charges



Security

Detect anomalies and prevent data leakage in a near real-time manner



Compliance

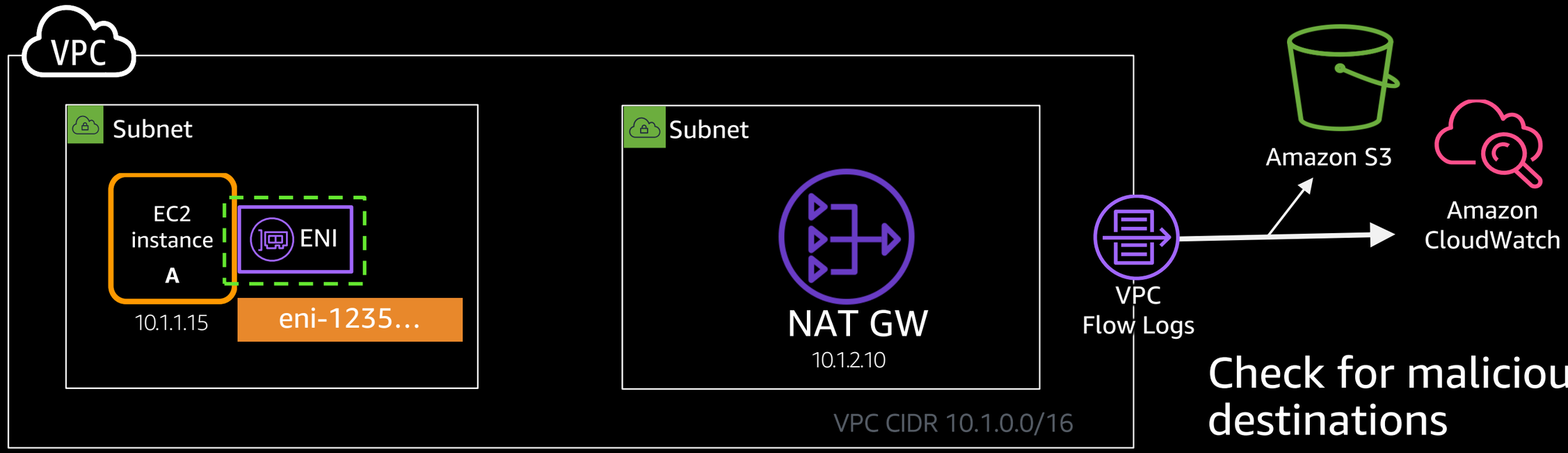
Archive for regulatory requirements and ad-hoc analysis

An example:

Consider an Amazon EC2 instance using a NAT Gateway to send traffic to an internet destination



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Check for malicious destinations

Version	…	ENI	SRC Addr	DES Addr	Pkt-SrcAddr	Pkt-DstAddr	…
3		eni-1235…	10.1.1.15	10.1.2.10	10.1.1.15	1.2.3.4	

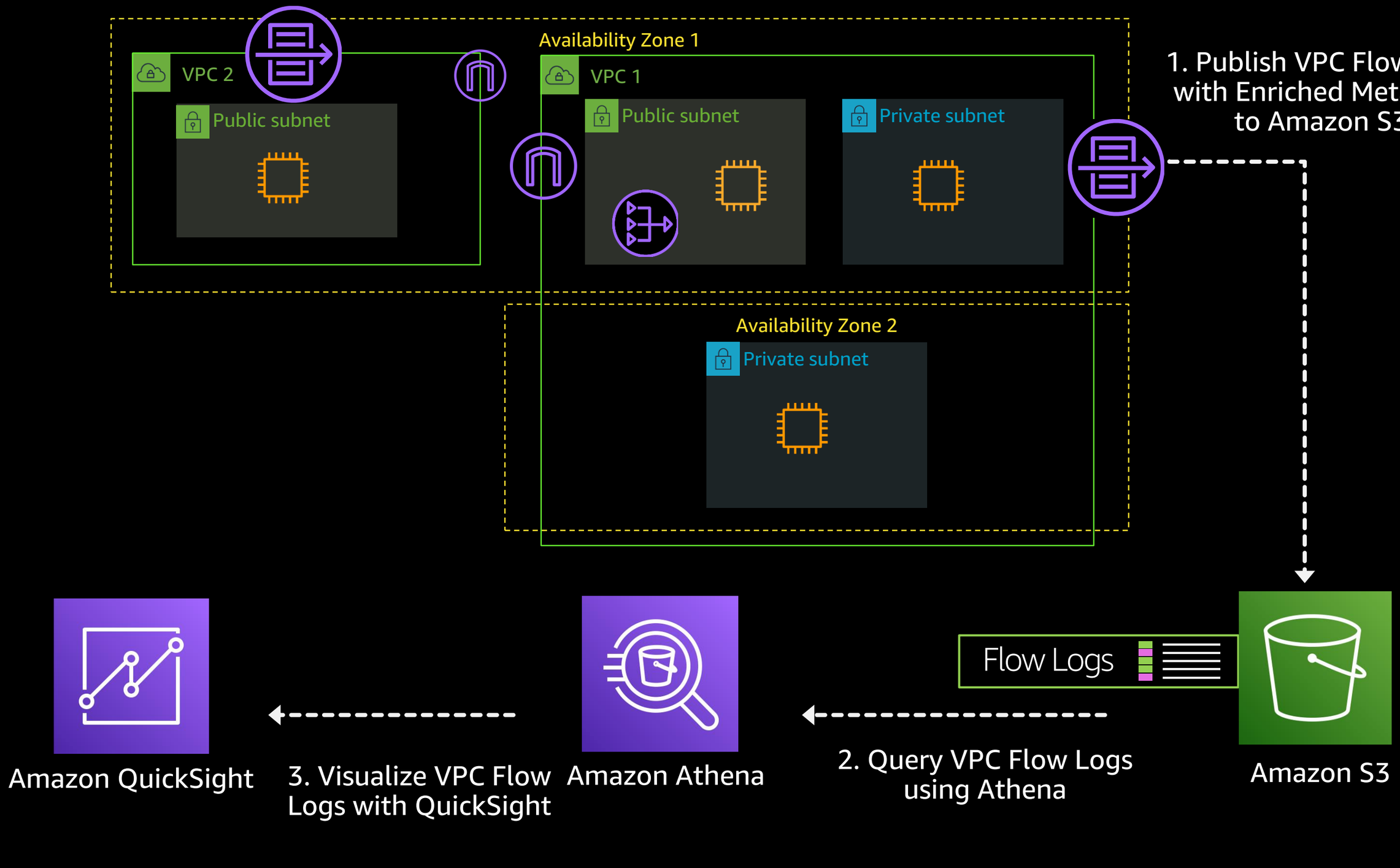
Malicious IP

VPC Flow Logs Demo Workflow



AWS re:Invent

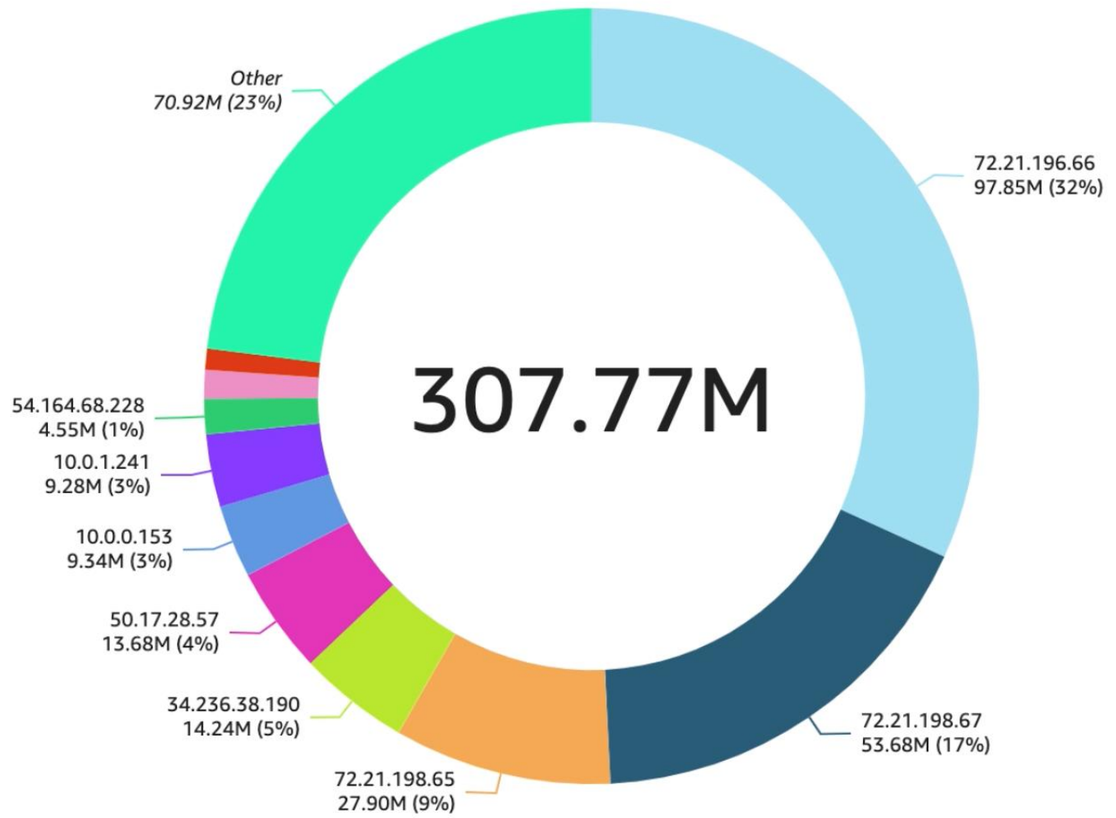
© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.


Availability Zone 1
VPC 2
Public subnet
VPC 1
Public subnet
Private subnet
1. Publish VPC Flow Logs with Enriched Metadata to Amazon S3
Availability Zone 2
Private subnet
Flow Logs
Amazon QuickSight
3. Visualize VPC Flow Logs with QuickSight
Amazon Athena
2. Query VPC Flow Logs using Athena
Amazon S3

Field wells **Group/Color** dstaddr **Value** bytes (Sum)

Sum of Bytes by Protocol | [Log Scaled] Sum of Bytes by Protocol | **Top Destinations by IP** | Top Destinations by instanceId | Top Destination by InstanceId (2) | D

Top Destination IPs by Egress traffic from Server (Sum of Bytes)



Group By: dstaddr

Size: bytes (Sum)

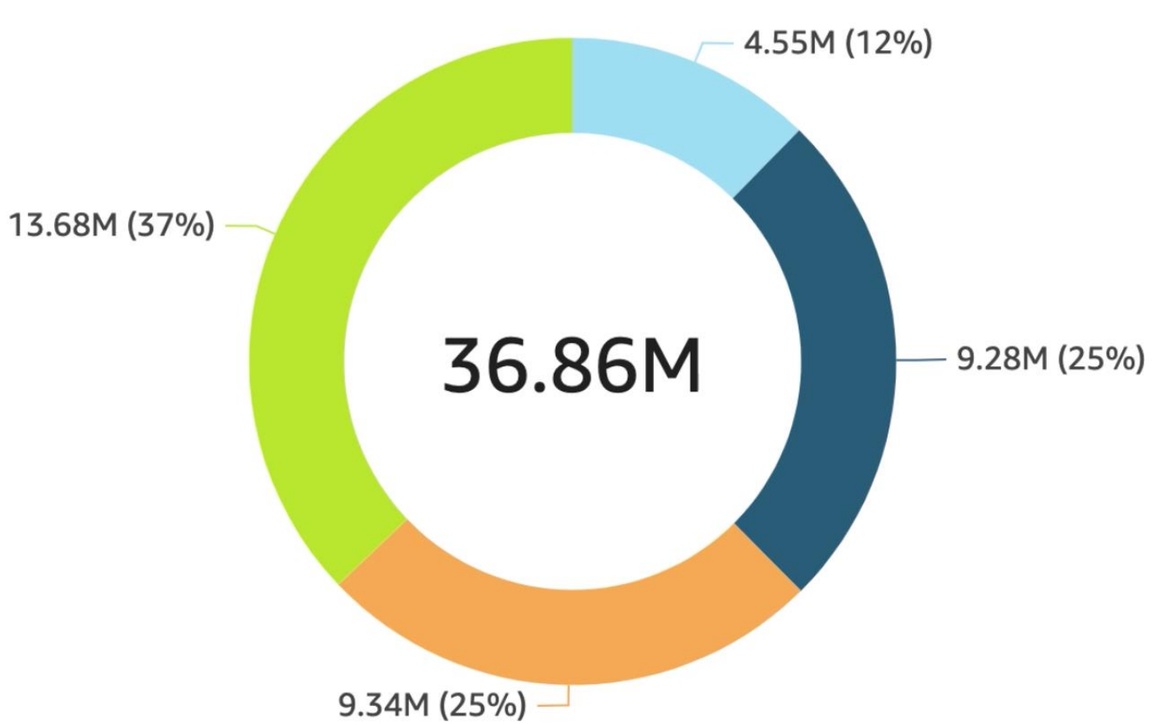
Add Undo Redo ☆ FlowLogs Summaries & Demo Autosave ON Print Share Admin...

Visualize Filter Story Parameters Actions Themes Settings

Field wells **Group/Color** dstInstanceId **Value** bytes (Sum)

Sum of Bytes by Protocol | [Log Scaled] Sum of Bytes by Protocol | Top Destinations by IP | Top Destinations by instanceId | **Top Destination by InstanceId (2)** | D

Top Destination Instances by Egress traffic from Server (Sum of Bytes)



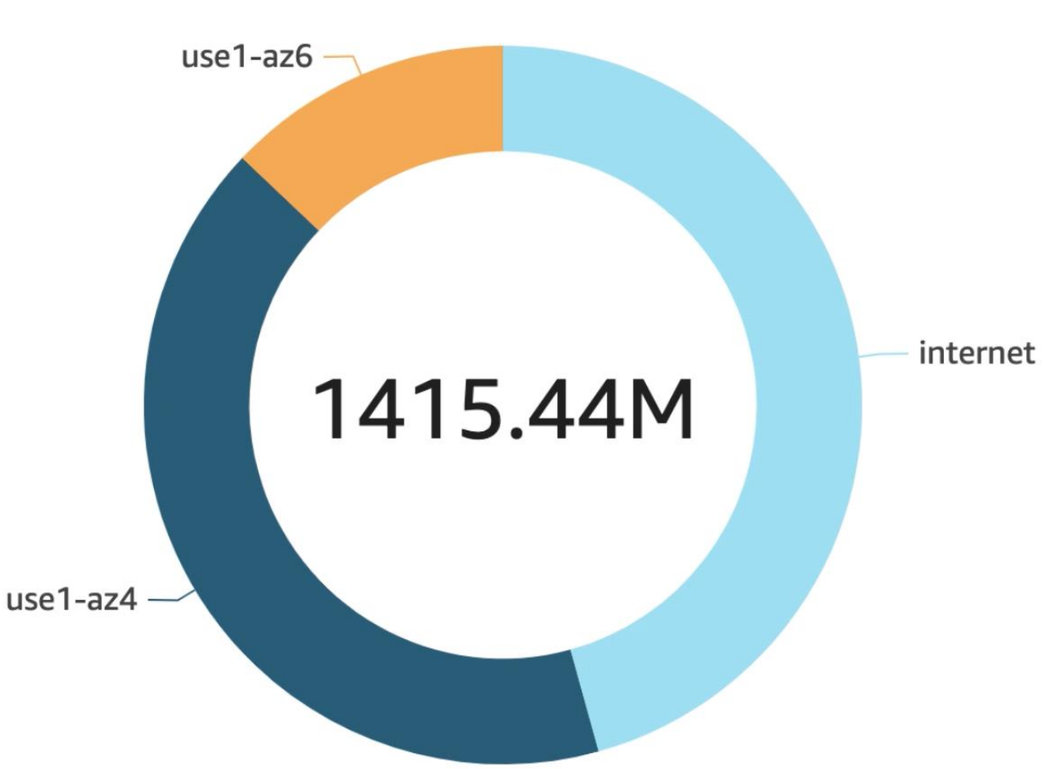
Add Undo Redo ☆ FlowLogs Summaries & Demo Autosave ON Print Share Admin...

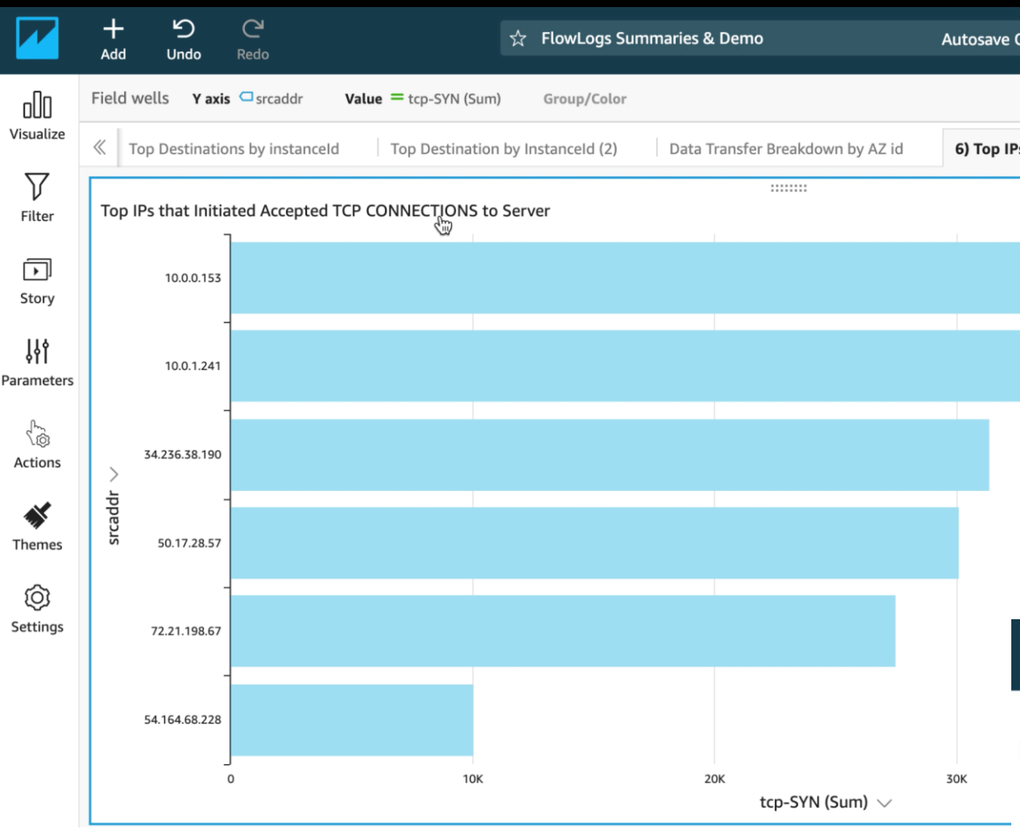
Visualize Filter Story Parameters Actions Themes Settings

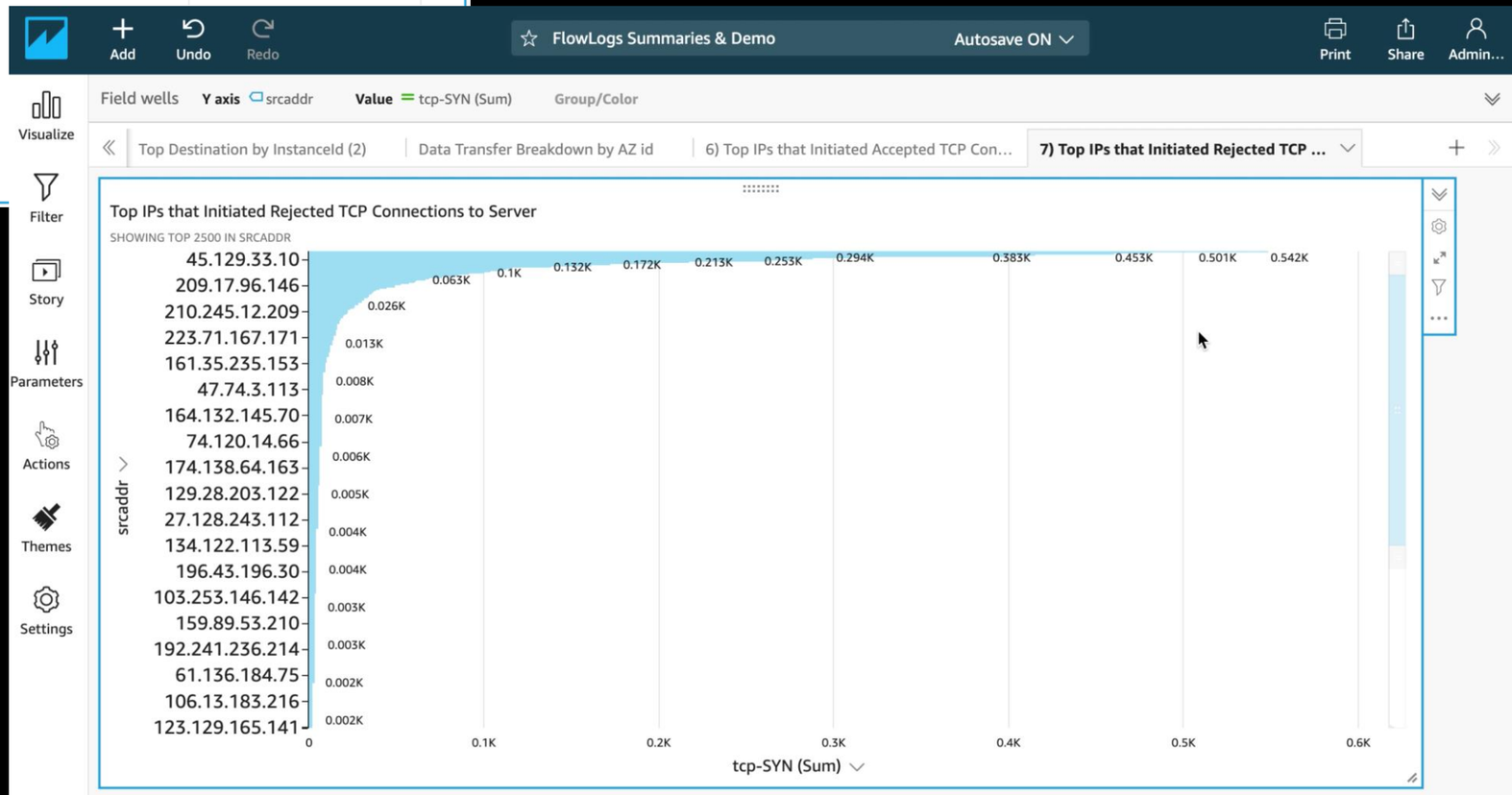
Field wells **Group/Color** az-info **Value** bytes (Sum)

Top Destinations by IP | Top Destinations by instanceId | Top Destination by InstanceId (2) | **Data Transfer Breakdown by AZ id** | 6) Top IPs that Initiated Accepted TCP

Data Transfer Breakdown by AZ id




Add
Undo
Redo
FlowLogs Summaries & Demo
Autosave ON
Print
Share
Admin...
Visualize
Filter
Story
Parameters
Actions
Themes
Settings
Field wells
Y axis srcaddr
Value tcp-SYN (Sum)
Group/Color
Top Destinations by instanceId
Top Destination by InstanceId (2)
Data Transfer Breakdown by AZ id
6) Top IPs that Initiated Accepted TCP ...
7) Top IPs that Initi
Top IPs that Initiated Accepted TCP CONNECTIONS to Server
10.0.0.153
10.0.1.241
34.236.38.190
50.17.28.57
72.21.198.67
54.164.68.228
srcaddr
0
10K
20K
30K
tcp-SYN (Sum)


Add
Undo
Redo
FlowLogs Summaries & Demo
Autosave ON
Print
Share
Admin...
Visualize
Filter
Story
Parameters
Actions
Themes
Settings
Field wells
Y axis srcaddr
Value tcp-SYN (Sum)
Group/Color
Top Destination by InstanceId (2)
Data Transfer Breakdown by AZ id
6) Top IPs that Initiated Accepted TCP Con...
7) Top IPs that Initiated Rejected TCP ...
Top IPs that Initiated Rejected TCP Connections to Server
SHOWING TOP 2500 IN SRCADDR
45.129.33.10
209.17.96.146
210.245.12.209
223.71.167.171
161.35.235.153
47.74.3.113
164.132.145.70
74.120.14.66
174.138.64.163
129.28.203.122
27.128.243.112
134.122.113.59
196.43.196.30
103.253.146.142
159.89.53.210
192.241.236.214
61.136.184.75
106.13.183.216
123.129.165.141
0.063K
0.1K
0.132K
0.172K
0.213K
0.253K
0.294K
0.383K
0.453K
0.501K
0.542K
0.026K
0.013K
0.008K
0.007K
0.006K
0.005K
0.004K
0.004K
0.003K
0.003K
0.002K
0.002K
srcaddr
0
0.1K
0.2K
0.3K
0.4K
0.5K
0.6K
tcp-SYN (Sum)

Create Table from... | create table topR... | Top Talkers

```
1 SELECT dstaddr, SUM(bytes) AS totalBytesOUT
2 FROM demo_flowlogs_vpc
3 WHERE srcaddr='10.0.4.116'
4 GROUP BY dstaddr
5 ORDER BY totalBytesOUT DESC
6 LIMIT 10
7
```

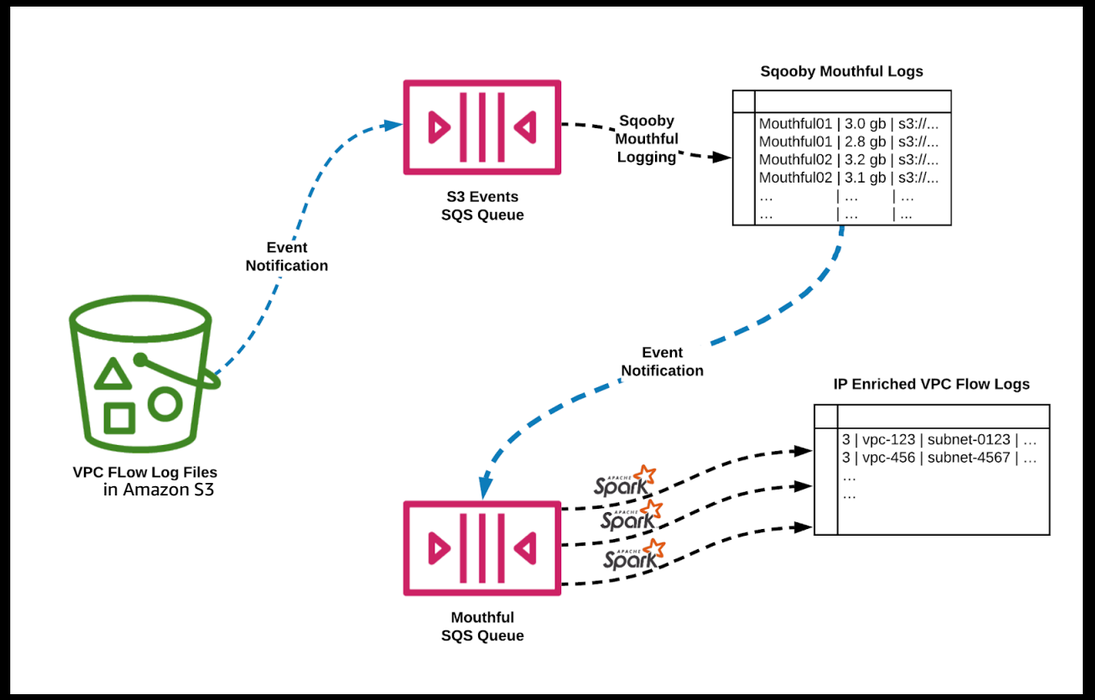
Run query | Save as | Create | (Run time: 4.77 seconds, Data scanned: 17.17 MB) | Format query | Clear

Use Ctrl + Enter to run query, Ctrl + Space to autocomplete

Results

	dstaddr	totalBytesOUT
1	72.21.196.66	97848690
2	72.21.198.67	53683541
3	72.21.198.65	27899093
4	10.0.0.153	18688374
5	10.0.1.241	18561110
6	34.236.38.190	14239055
7	50.17.28.57	13681612
8	54.164.68.228	4550563
9	112.85.42.143	3661361
10	188.166.69.54	2657812





Watch the full video here
https://bit.ly/2L7BAnt

Find the blog here
https://bit.ly/3bktsei

How do you get deeper visibility into the payload?



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

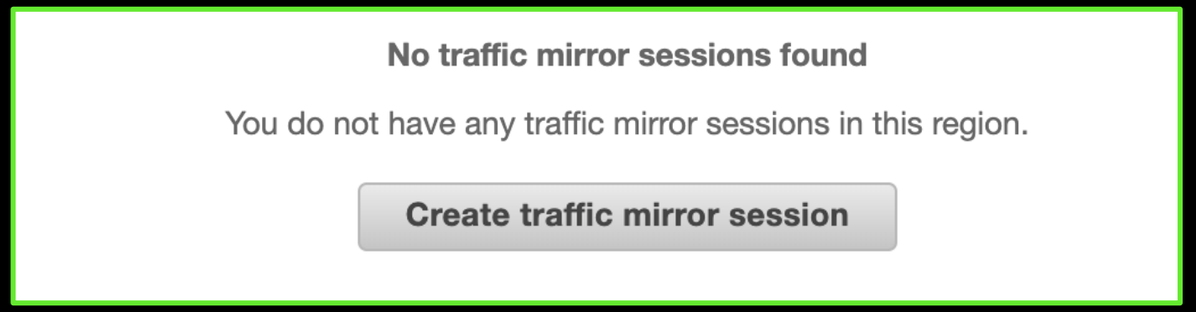
Amazon VPC Traffic Mirroring

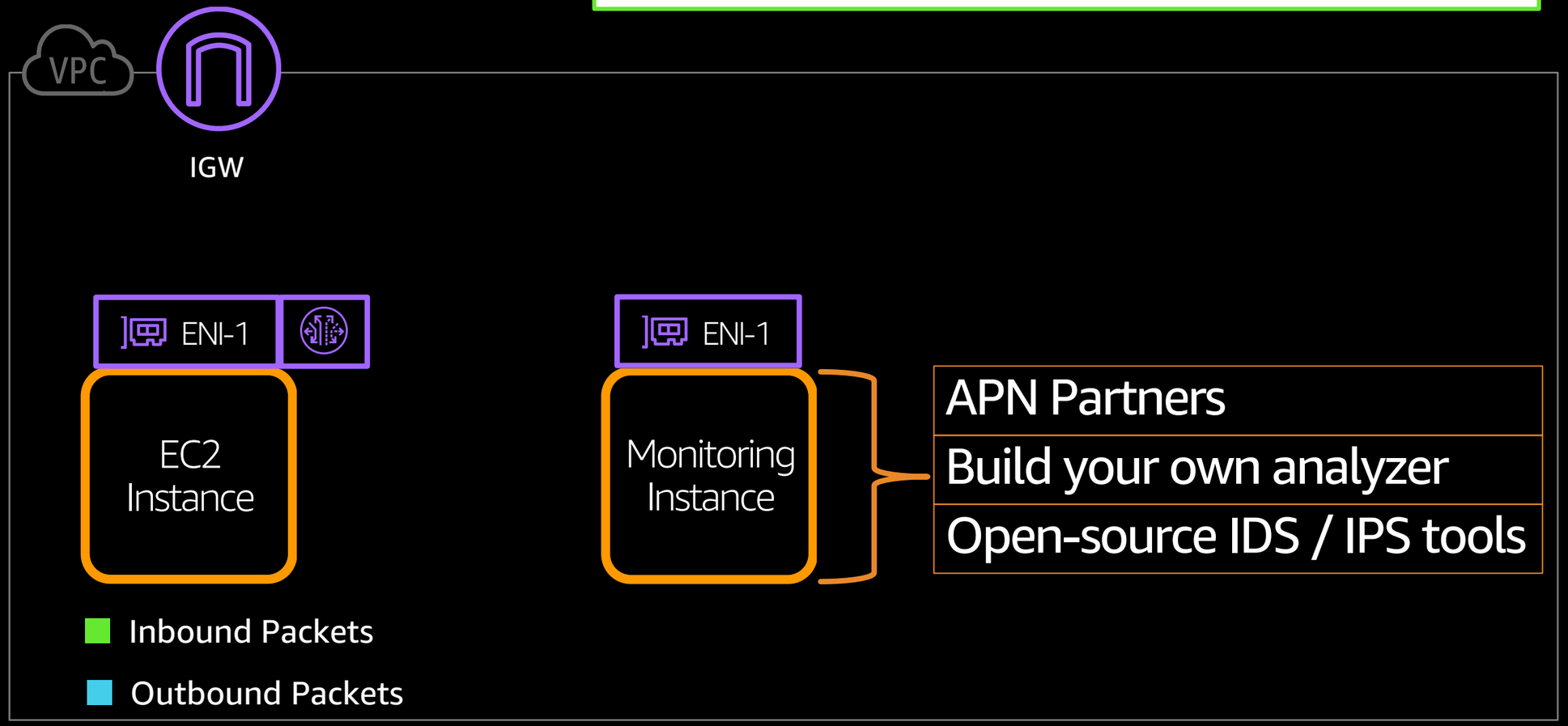


AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is Amazon VPC Traffic Mirroring?

























This list of AWS Partners is not comprehensive, but shows the range of AWS Partners offering solutions in this area



















This list of AWS Partners is not comprehensive, but shows the range of AWS Partners offering solutions in this area

VPC Traffic Mirroring: Three components



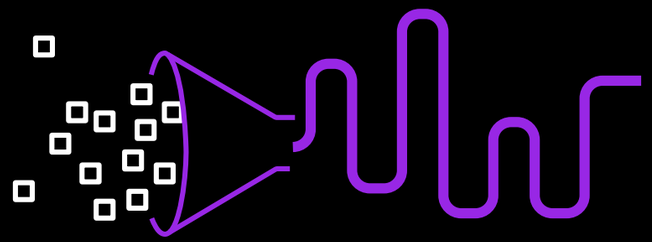
AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



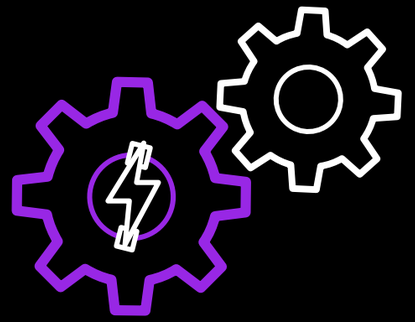
Targets

The destination for mirrored traffic



Filters

A set of rules that define the traffic that is copied in a Traffic Mirror session



Sessions

An entity that describes traffic mirroring from a source to a target using filters



VPC Traffic Mirroring Targets

THE DESTINATION FOR MIRRORED TRAFFIC

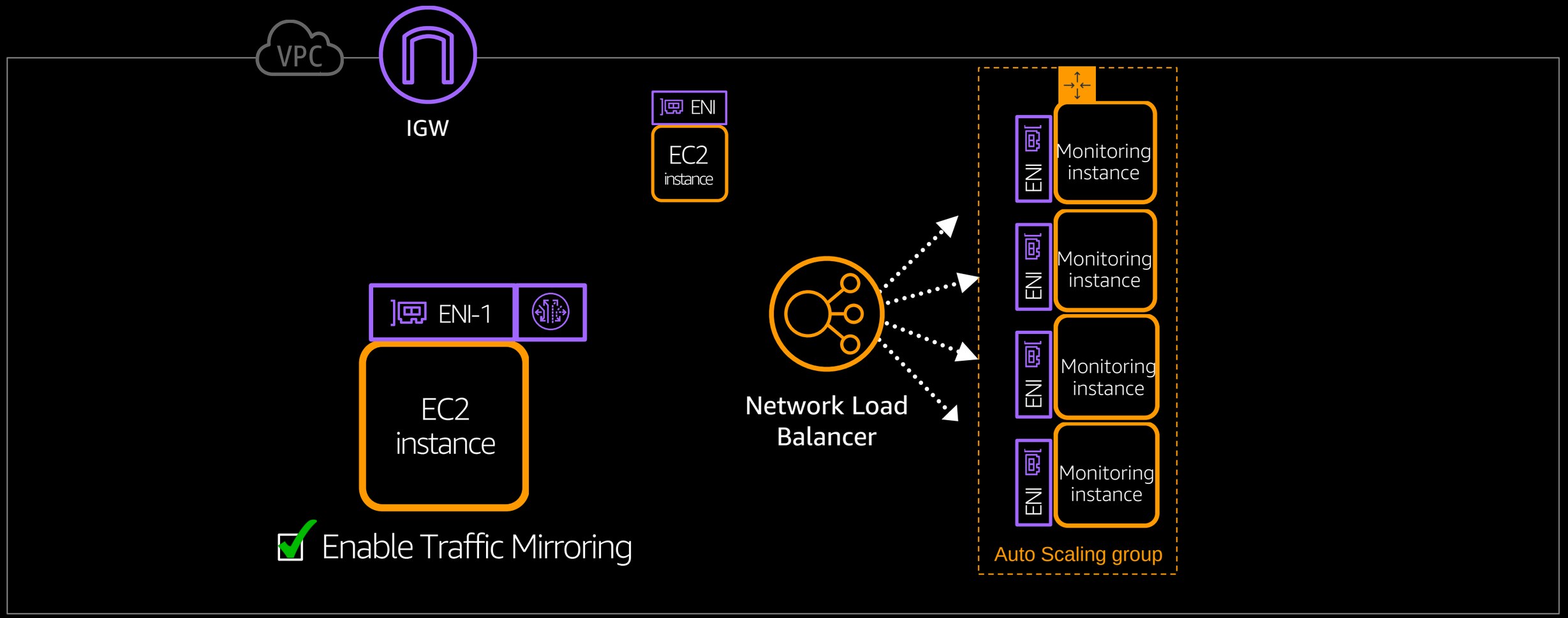


Elastic network interfaces



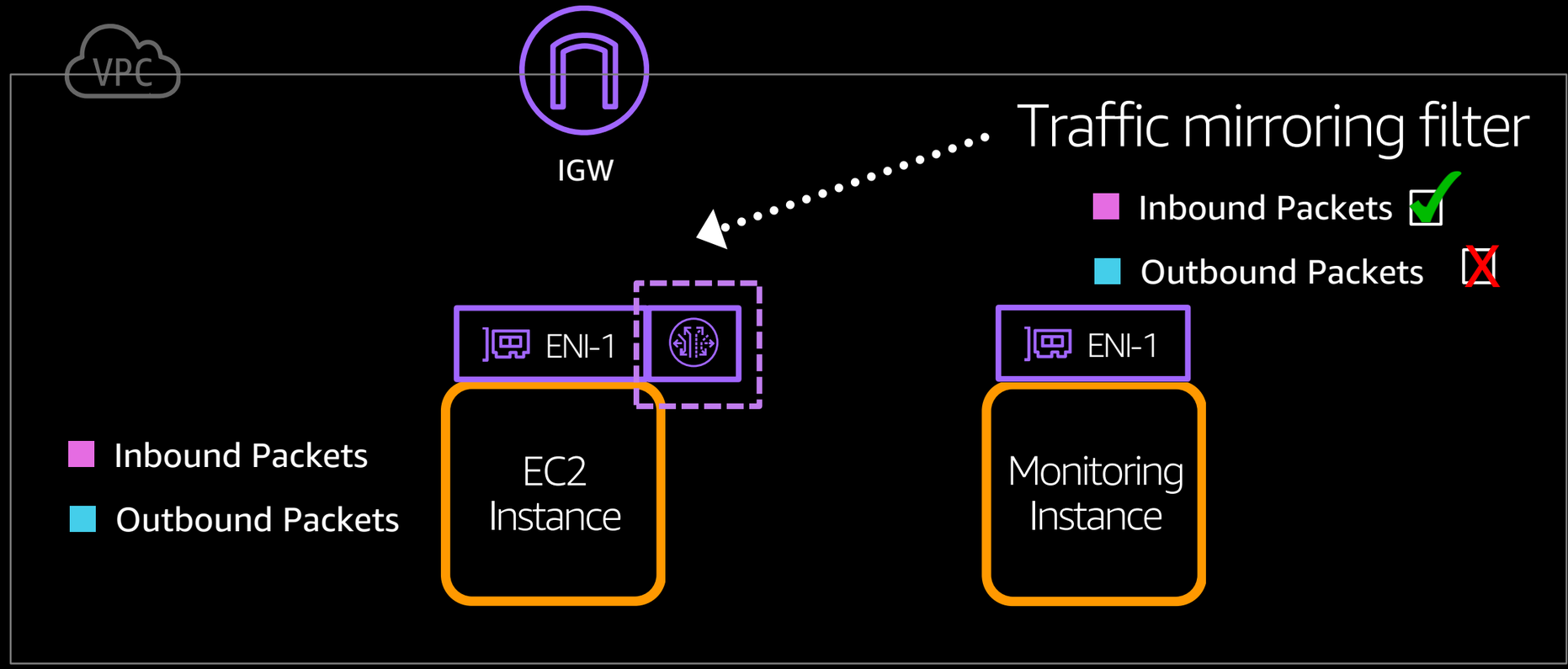
Network Load Balancers

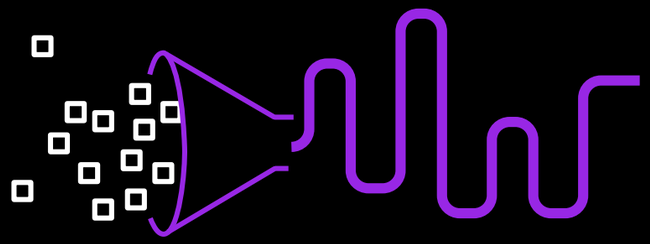
Network Load Balancer as a Target



VPC Traffic Mirroring Filters

RULES TO DEFINE TRAFFIC THAT IS MIRRORED





VPC Traffic Mirroring Filters

AN EXAMPLE

Type	Flow Direction	Protocol	Source IP	Source Port	Dest IP	Dest Port	Truncation
Option	Ingress	TCP	Source IP	Any	My server IP	80	No
	Egress	UDP	0.0.0.0/0	Range	List of CIDRs	Range	Sample (Bytes)
	Both	Any					



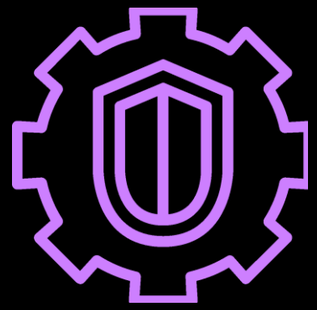
VPC Traffic Mirroring Sessions

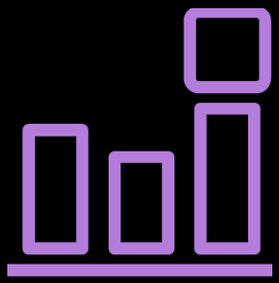
COMBINES THE SOURCE, FILTER, AND TARGET

Source	Filter	Target

Key Benefits of VPC Traffic Mirroring







Simplified native operation

Through agent-less, native mirroring capabilities

Improved security posture

Through packet capture at the elastic network interface level

Wide range of monitoring options

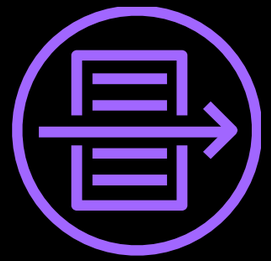
By integrating with multiple tools and APN partners

VPC Flow Logs vs. VPC Traffic Mirroring



AWS re:Invent

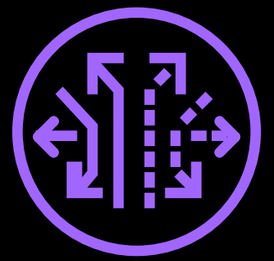
© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



VPC Flow Logs

- Logs of network flows where each record captures metadata about a specific 5-tuple

- Destination: Amazon S3 or Amazon CloudWatch Logs



VPC Traffic Mirroring

- Copies of real network packets with the ability to truncate

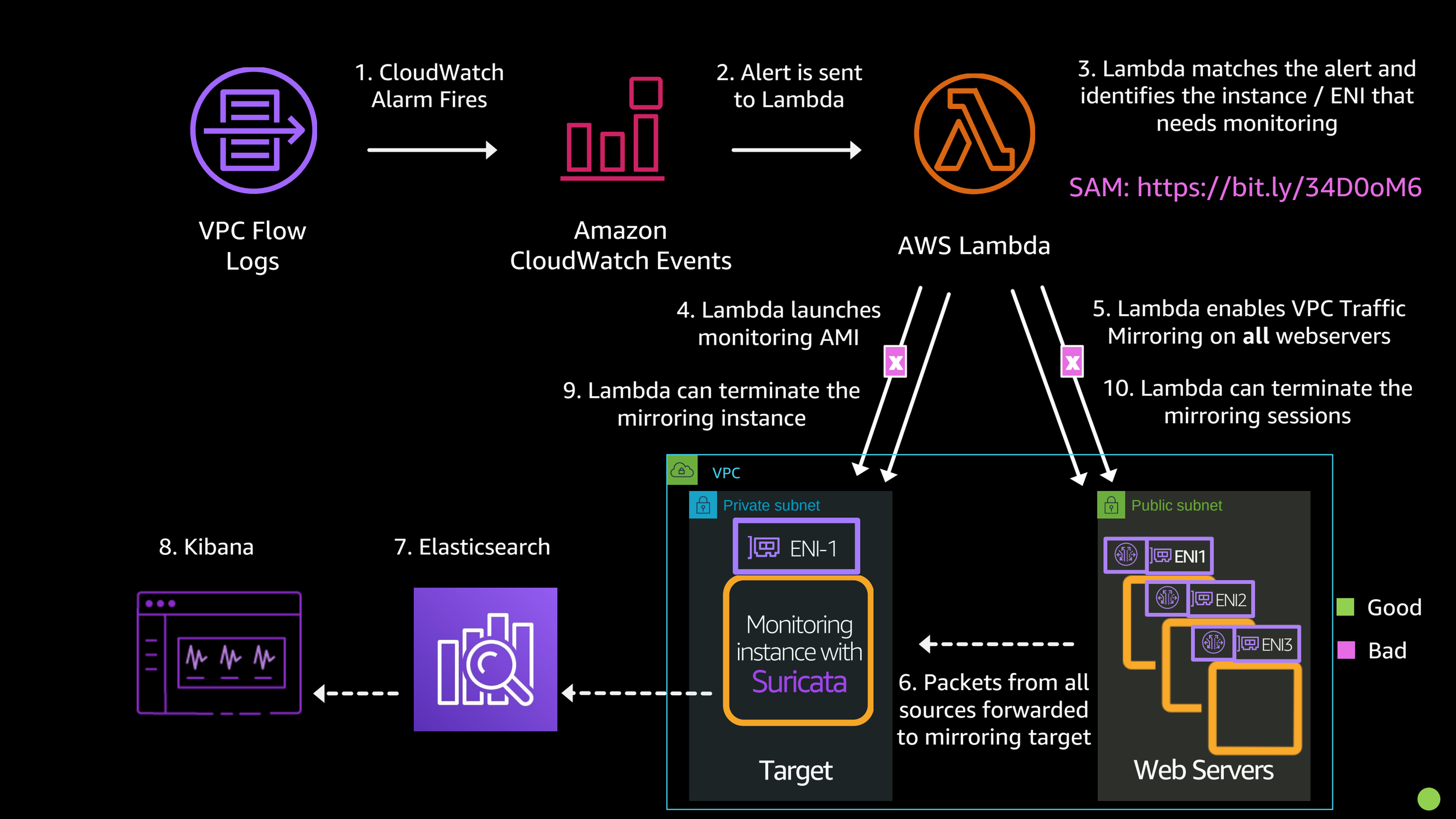
- Destination: Another elastic network interface or Network Load Balancer

VPC Traffic Mirroring Demo Workflow



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.


1. CloudWatch Alarm Fires
2. Alert is sent to Lambda
3. Lambda matches the alert and identifies the instance / ENI that needs monitoring
SAM: https://bit.ly/34D0oM6
VPC Flow Logs
Amazon CloudWatch Events
AWS Lambda
4. Lambda launches monitoring AMI
5. Lambda enables VPC Traffic Mirroring on **all** webservers
9. Lambda can terminate the mirroring instance
10. Lambda can terminate the mirroring sessions
VPC
Private subnet
ENI-1
Monitoring instance with Suricata
Target
Public subnet
ENI1
ENI2
ENI3
Web Servers
6. Packets from all sources forwarded to mirroring target
8. Kibana
7. Elasticsearch
Good
Bad

How do you monitor the network performance of your EC2 instances?

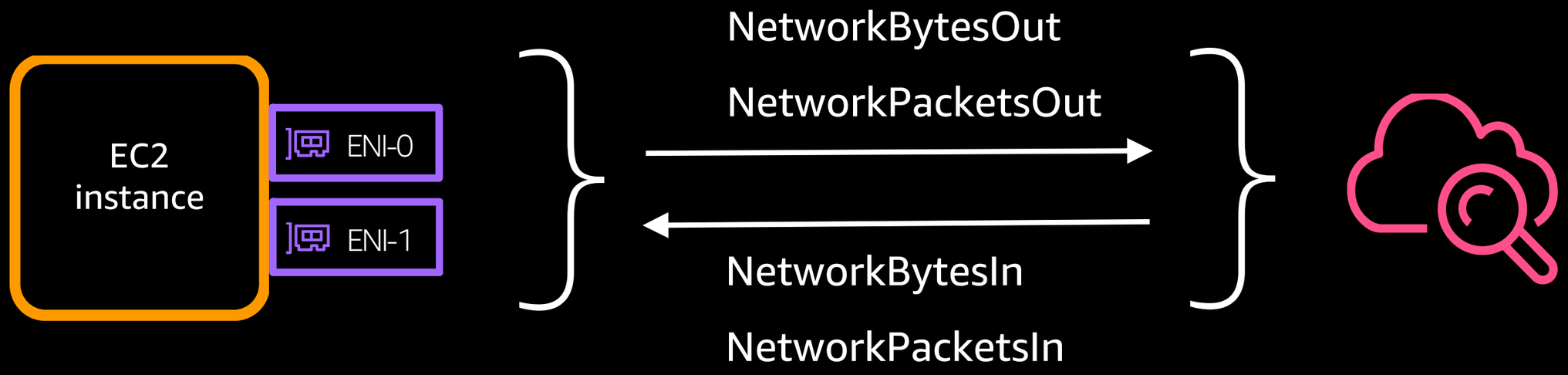


AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Network usage of EC2 instances

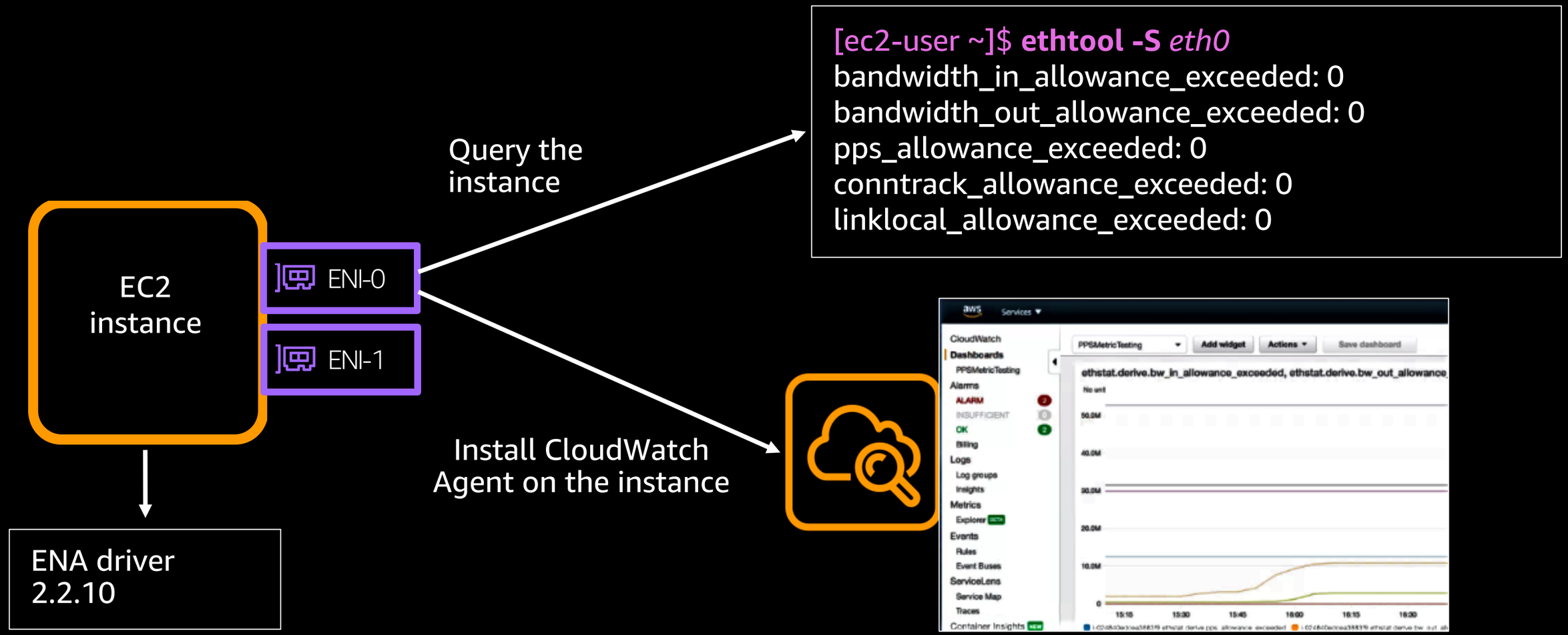
AMAZON EC2 ALLOWS YOU TO ACTIVELY MONITOR THE TRAFFIC VOLUME TO AND FROM YOUR INSTANCES



Network performance of EC2 instances

NEW

MONITOR AND TROUBLESHOOT PACKET LOSS WHEN INSTANCE ALLOWANCES ARE EXCEEDED



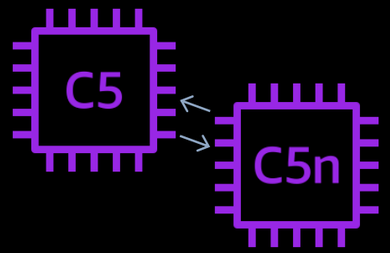
Network performance of EC2 instances

INSTANCE LEVEL NETWORK PERFORMANCE METRICS OFFER THREE ADVANTAGES



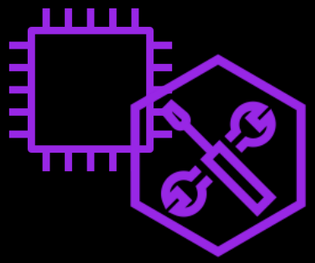
Monitor

Metrics on bytes and packets on a per-instance level give granular visibility of instance network performance



Benchmark

Using these metrics with network throughput benchmark testing helps you choose the right instance for your workload



Troubleshoot

You can troubleshoot network issues using these metrics and diagnose root cause of packet loss

You now have visibility into your network traffic! But…



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How do you know if your network is properly configured and secure?



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon VPC Reachability Analyzer



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

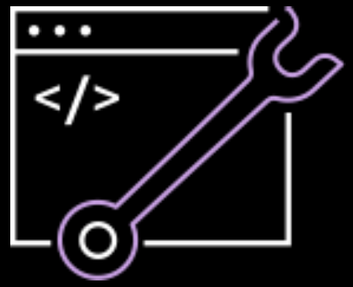
Introducing VPC Reachability Analyzer

NEW

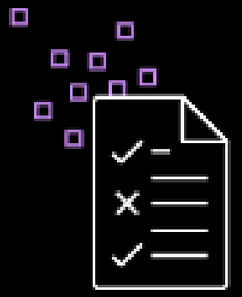
CONFIGURATION AND NETWORK REACHABILITY ANALYSIS



Troubleshoot connectivity issues



Ensure configuration matches intent



Automated validation

Use Cases in Action

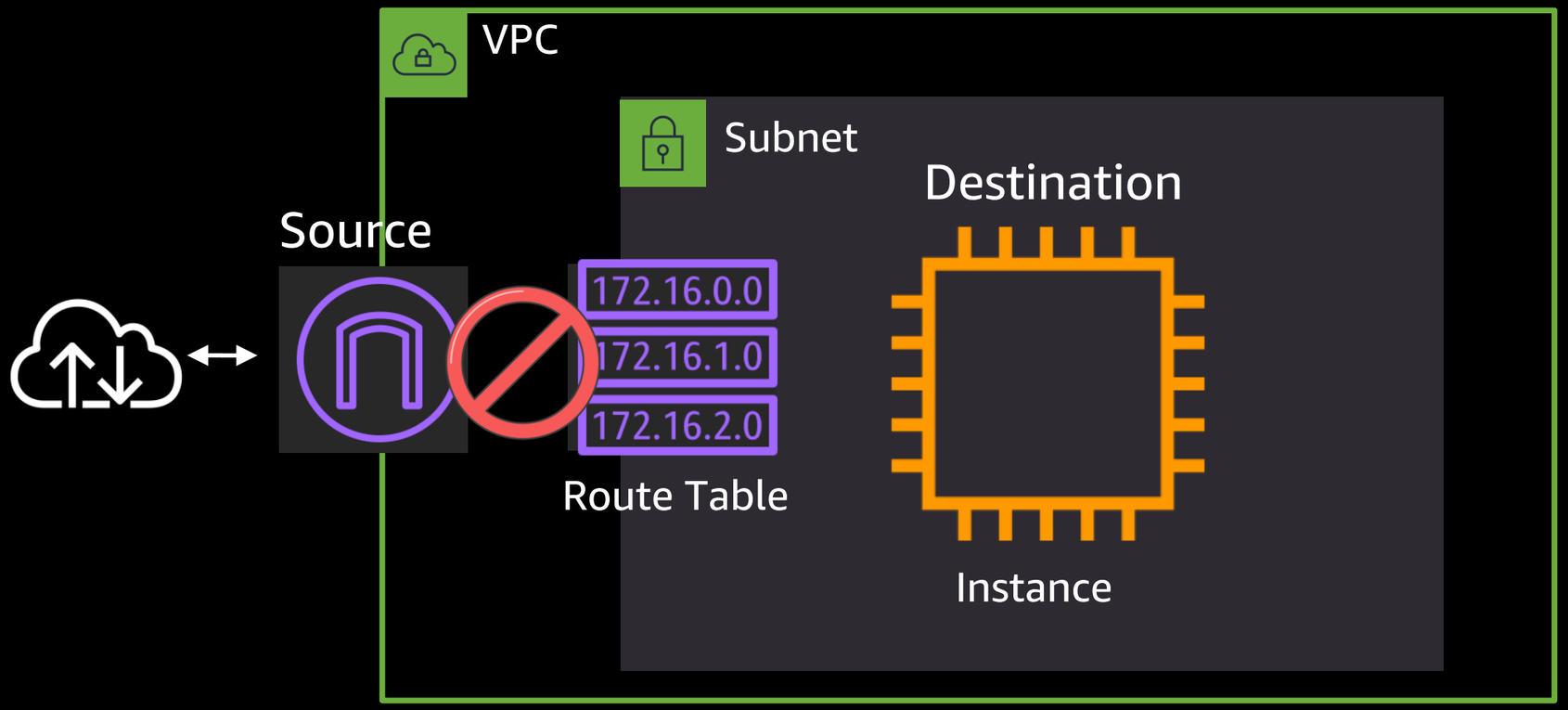


AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Troubleshooting

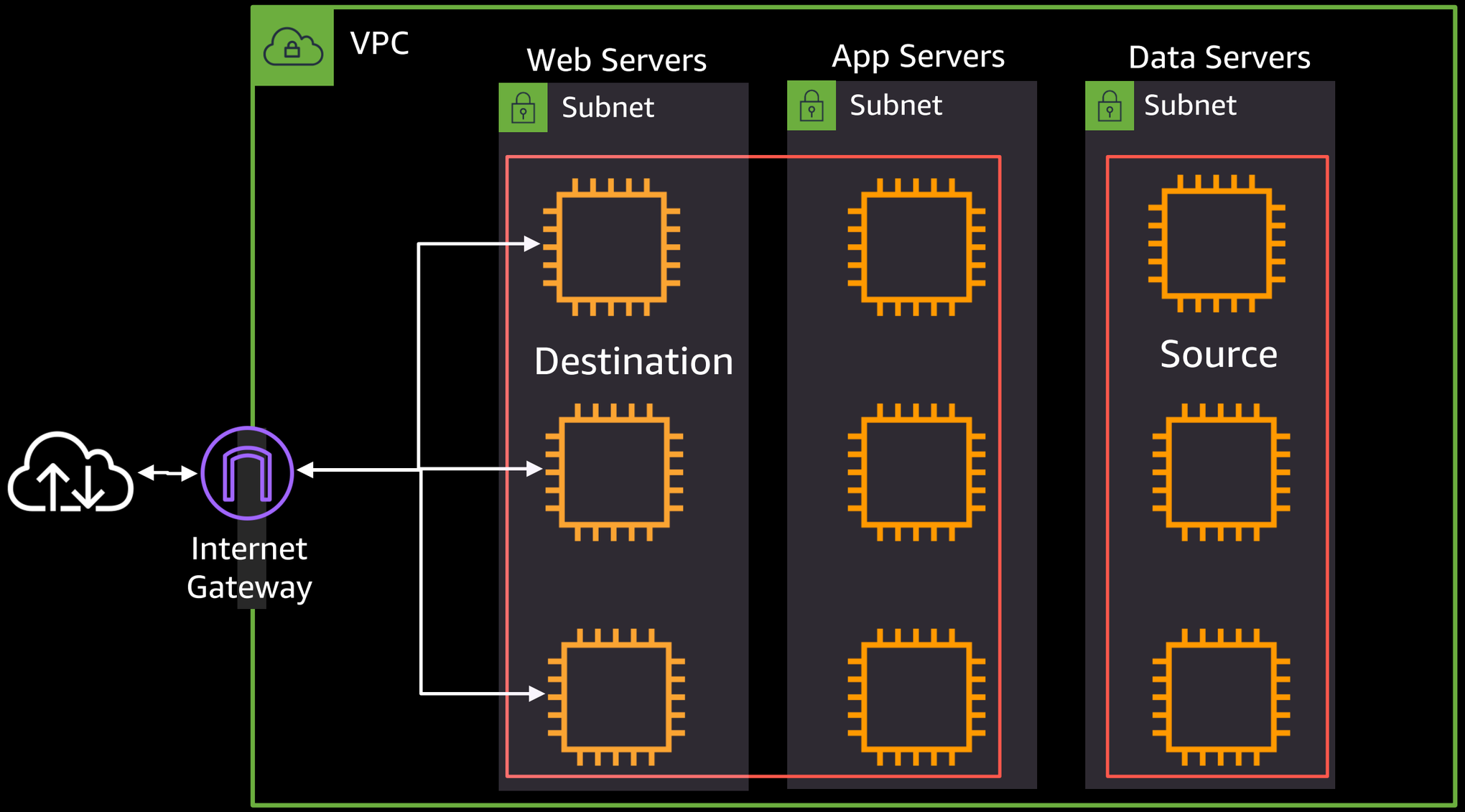
UNABLE TO SSH TO YOUR INSTANCE



Security Groups and Network ACLs, both allow traffic on port 22
Source : Instance, Destination : IGW

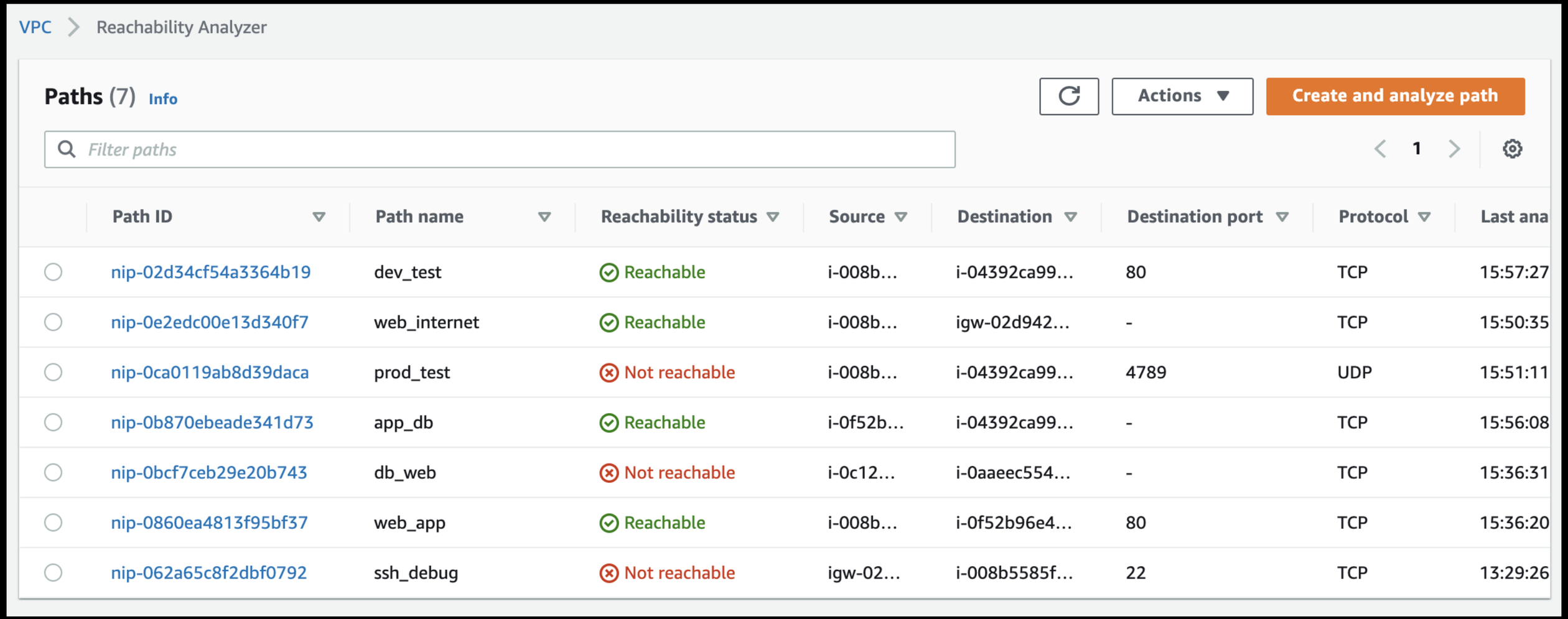
Intent Verification

INTENT: DATABASE SHOULD NOT BE CONNECTED TO WEB



Automated Validation

RUN AUTOMATED REACHABILITY ANALYSIS



List of Components Supported

- VPCs
- Network interfaces
- Subnets
- Network ACLs
- Security Groups
- Route tables

- Elastic Load Balancers
- Application Load Balancers
- Network Load Balancers
- Internet gateways
- Virtual private gateways
- Transit gateways
- VPC peering connections

Recap



Monitor your AWS network traffic

VPC Flow Logs



Gain deeper visibility into the payload

VPC Traffic Mirroring



Track network performance of EC2 instances

EC2 Instance-Level Metrics



Troubleshoot network connectivity issues

VPC Reachability Analyzer

NEW

Thank you!



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Please complete the session survey

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.