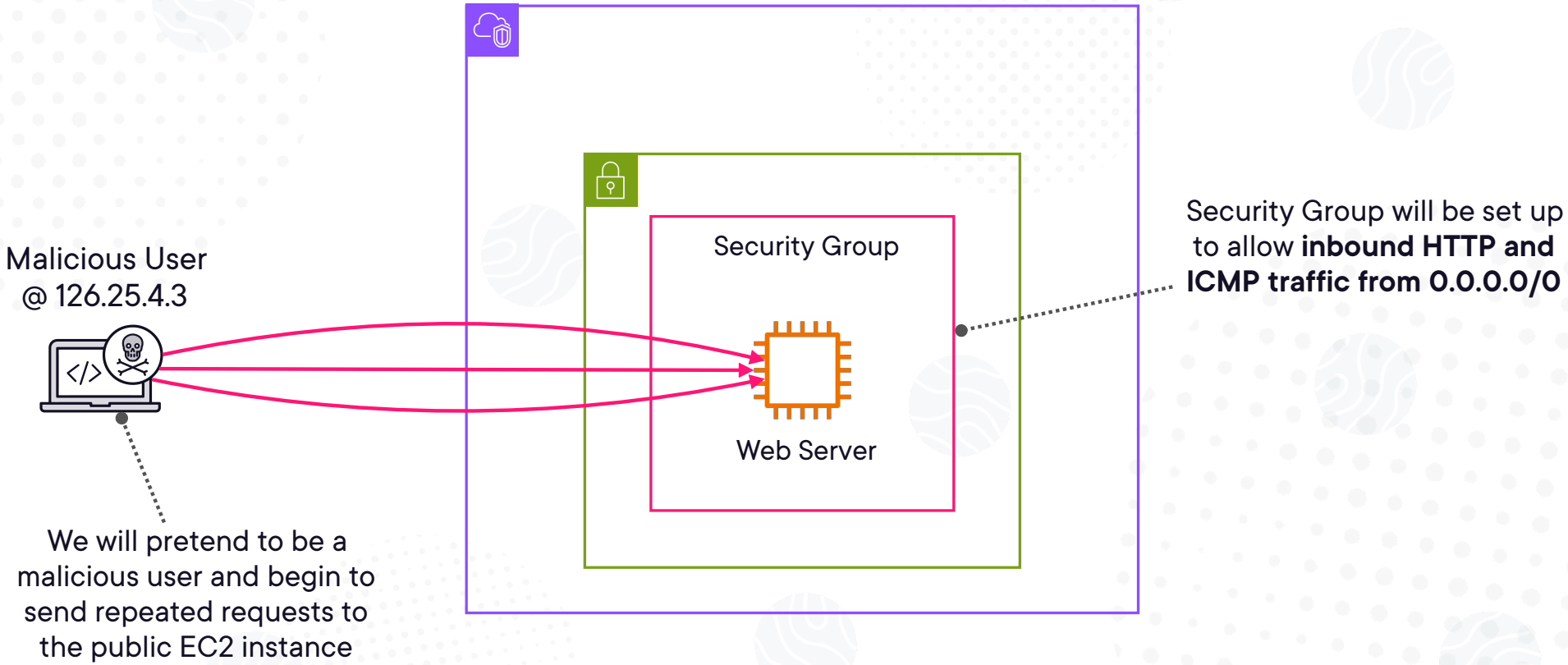
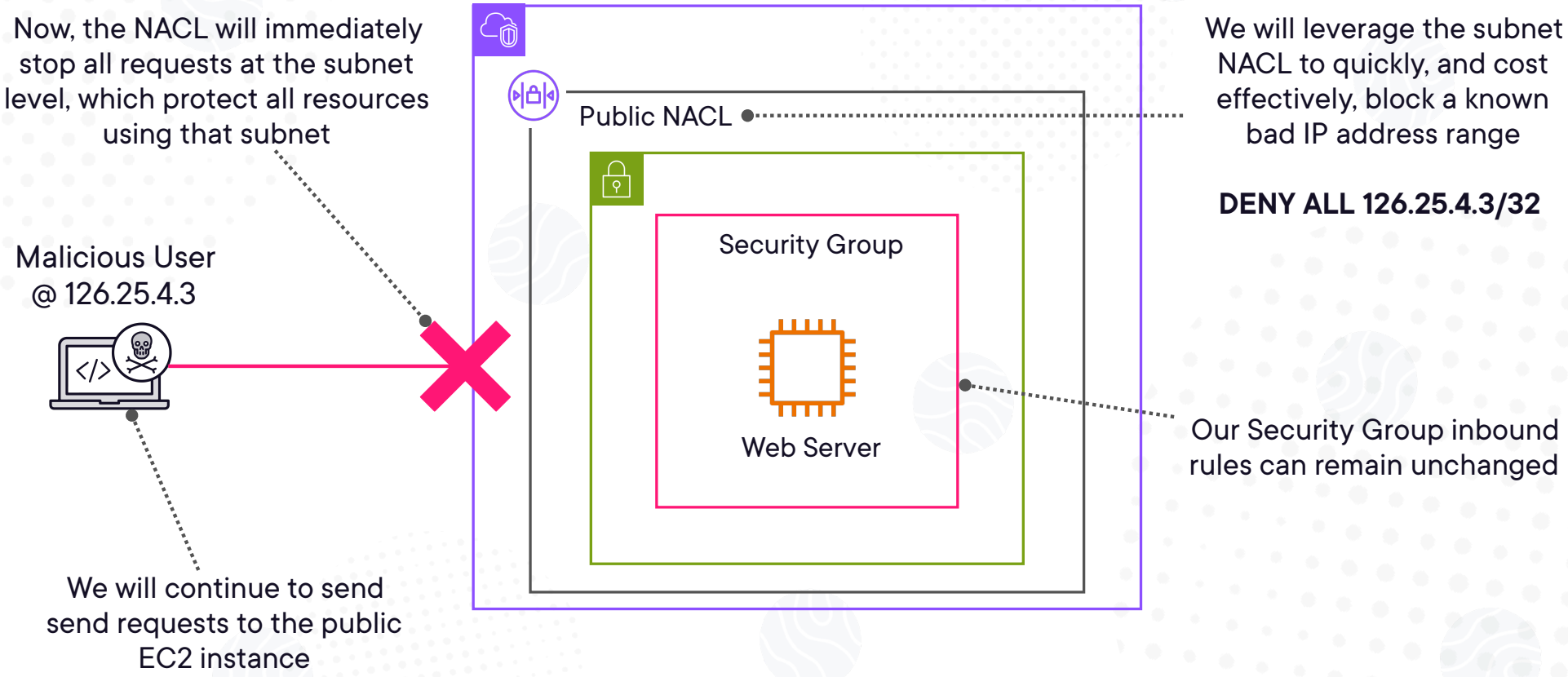
# Advanced VPC Concepts: Miscellaneous Features and Scenarios

**Andru Estes**
Principal Author
andru-estes

# Demo: Blocking Bad IPs Quickly via NACLs



# Demo: Blocking Bad IPs Quickly via NACLs

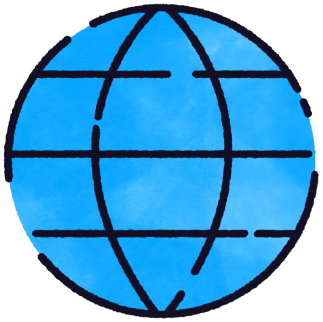


# Logging VPC Traffic with VPC Flow Logs

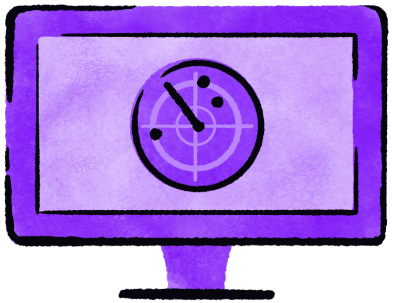

# VPC Flow Logs

VPC feature that enables you to capture IP traffic information about any traffic going to and coming from network interfaces in your VPC

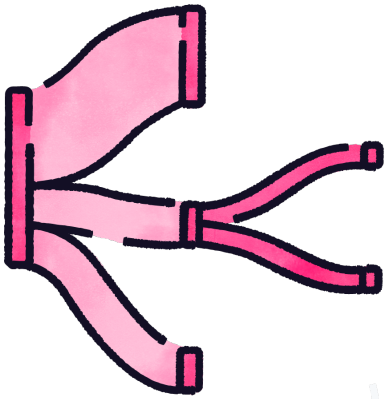
# VPC Flow Logs Source Options



Entire VPC



VPC Subnet



Specific ENI

# VPC Flow Logs Concepts

These are collected and do not affect network throughput or latency

Also supports ELBs, RDS, Redshift, NAT Gateways, Transit Gateway


Use Case 1: Diagnosing security group rules for denied traffic


Use Case 2: Monitoring the traffic that is connecting to your instance


Use Case 3: Determining the direction of traffic flow to and from ENIs

# VPC Flow Logs Destination Options

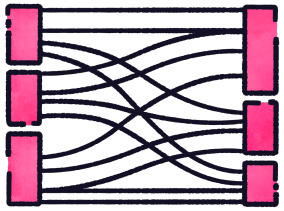
After configuring your VPC Flow Logs source, you must choose the destination where you want your logs to be sent. There are currently three options.

## Amazon CloudWatch Logs

Send VPC Flow Logs to a log group to perform operations on or monitor

## Amazon S3

Store the logs within a secure bucket for cheap, long-term storage for compliance



## Amazon Data Firehose

Send logs to an autoscaling delivery stream to perform analytics or transform

# VPC Flow Logs Record Example - Default Format

**Flow log records represent a network flow in your VPC, and they include a 5-tuple capture of information by default.**
**Each record captures information within an aggregation interval, also called a capture window.**

2 123456789010 eni-1235a6bc789101112 165.222.10.30 10.0.0.24 21234 443 6 20 4249 1418530010 1418530070 REJECT OK

# VPC Flow Logs Record Example - Default Format

Flow log records represent a network flow in your VPC, and they include a 5-tuple capture of information by default.
Each record captures information within an aggregation interval, also called a capture window.

2 123456789010 eni-1235a6bc789101112 165.222.10.30 10.0.0.24 21234 443 6 20 4249 1418530010 1418530070 REJECT OK

The version of the Flow Logs (default is 2)

# VPC Flow Logs Record Example - Default Format

Flow log records represent a network flow in your VPC, and they include a 5-tuple capture of information by default.
Each record captures information within an aggregation interval, also called a capture window.

2 123456789010 eni-1235a6bc789101112 165.222.10.30 10.0.0.24 21234 443 6 20 4249 1418530010 1418530070 REJECT OK



The AWS account ID

# VPC Flow Logs Record Example - Default Format

Flow log records represent a network flow in your VPC, and they include a 5-tuple capture of information by default.
Each record captures information within an aggregation interval, also called a capture window.

2 123456789010 eni-1235a6bc789101112 165.222.10.30 10.0.0.24 21234 443 6 20 4249 1418530010 1418530070 REJECT OK

The interface IDs being recorded

Use this to identify which network resource traffic is being sent to, or being sent from.

# VPC Flow Logs Record Example - Default Format

Flow log records represent a network flow in your VPC, and they include a 5-tuple capture of information by default.
Each record captures information within an aggregation interval, also called a capture window.

2 123456789010 eni-1235a6bc789101112 **165.222.10.30** 10.0.0.24 21234 443 6 20 4249 1418530010 1418530070 REJECT OK



**The source IP address making the traffic call**

Use this to identify and isolate problems related to the problematic IP addresses

# VPC Flow Logs Record Example - Default Format

Flow log records represent a network flow in your VPC, and they include a 5-tuple capture of information by default.
Each record captures information within an aggregation interval, also called a capture window.

2 123456789010 eni-1235a6bc789101112 165.222.10.30 **10.0.0.24** 21234 443 6 20 4249 1418530010 1418530070 REJECT OK

**Destination IP address for where the traffic is going**

Use this to identify and isolate problems related to the problematic IP addresses

# VPC Flow Logs Record Example - Default Format

Flow log records represent a network flow in your VPC, and they include a 5-tuple capture of information by default.
Each record captures information within an aggregation interval, also called a capture window.

2 123456789010 eni-1235a6bc789101112 165.222.10.30 10.0.0.24 21234 443 6 20 4249 1418530010 1418530070 REJECT OK



The source port of the network call

Use this to identify and isolate problems related to the ports being allowed or denied for both inbound and outbound traffic!

# VPC Flow Logs Record Example - Default Format

Flow log records represent a network flow in your VPC, and they include a 5-tuple capture of information by default.
Each record captures information within an aggregation interval, also called a capture window.

2 123456789010 eni-1235a6bc789101112 165.222.10.30 10.0.0.24 21234 443 6 20 4249 1418530010 1418530070 REJECT OK

The destination port of the network call

Use this to identify and isolate problems related to the ports being allowed or denied for both inbound and outbound traffic!

# VPC Flow Logs Record Example - Default Format

Flow log records represent a network flow in your VPC, and they include a 5-tuple capture of information by default.
Each record captures information within an aggregation interval, also called a capture window.

2 123456789010 eni-1235a6bc789101112 165.222.10.30 10.0.0.24 21234 443 6 20 4249 1418530010 1418530070 REJECT OK



The protocol of the network call (TCP = 6)

Use this to quickly identify and isolate problems related to the wrong protocol being allowed or denied.

# VPC Flow Logs Record Example - Default Format

Flow log records represent a network flow in your VPC, and they include a 5-tuple capture of information by default.
Each record captures information within an aggregation interval, also called a capture window.

2 123456789010 eni-1235a6bc789101112 165.222.10.30 10.0.0.24 21234 443 6 20 4249 1418530010 1418530070 REJECT OK

Number of packets transferred

# VPC Flow Logs Record Example - Default Format

Flow log records represent a network flow in your VPC, and they include a 5-tuple capture of information by default.
Each record captures information within an aggregation interval, also called a capture window.

2 123456789010 eni-1235a6bc789101112 165.222.10.30 10.0.0.24 21234 443 6 20 **4249** 1418530010 1418530070 REJECT OK



Number of bytes transferred

# VPC Flow Logs Record Example - Default Format

Flow log records represent a network flow in your VPC, and they include a 5-tuple capture of information by default.
Each record captures information within an aggregation interval, also called a capture window.

2 123456789010 eni-1235a6bc789101112 165.222.10.30 10.0.0.24 21234 443 6 20 4249 **1418530010** 1418530070 REJECT OK

Start time (Epoch)

# VPC Flow Logs Record Example - Default Format

Flow log records represent a network flow in your VPC, and they include a 5-tuple capture of information by default.
Each record captures information within an aggregation interval, also called a capture window.

2 123456789010 eni-1235a6bc789101112 165.222.10.30 10.0.0.24 21234 443 6 20 4249 1418530010 **1418530070** REJECT OK



**End time (Epoch)**

# VPC Flow Logs Record Example - Default Format

**Flow log records represent a network flow in your VPC, and they include a 5-tuple capture of information by default.**
**Each record captures information within an aggregation interval, also called a capture window.**

2 123456789010 eni-1235a6bc789101112 165.222.10.30 10.0.0.24 21234 443 6 20 4249 1418530010 1418530070 **REJECT** OK

**The action associated with the traffic**

**Use this to quickly identify successes or failures and isolate problems.**

**Action can be:**
- ACCEPT
- REJECT

# VPC Flow Logs Record Example - Default Format

**Flow log records represent a network flow in your VPC, and they include a 5-tuple capture of information by default.**
**Each record captures information within an aggregation interval, also called a capture window.**

2 123456789010 eni-1235a6bc789101112 165.222.10.30 10.0.0.24 21234 443 6 20 4249 1418530010 1418530070 REJECT **OK**

**Log status for the flow log**

**Status can be:**
- OK
- NODATA
- SKIPDATA

# VPC Flow Logs Record Example - Default Format

**Flow log records represent a network flow in your VPC, and they include a 5-tuple capture of information by default.**
**Each record captures information within an aggregation interval, also called a capture window.**

2 123456789010 eni-1235a6bc789101112 165.222.10.30 10.0.0.24 21234 443 6 20 4249 1418530010 1418530070 REJECT OK

**Make sure you know how to read this syntax! Here are the official field names for review *(in the correct order)*:**

version, account-id, interface-id, srcaddr, dstaddr, srcport, dstport, protocol, packets, bytes, start, end, action, status

# Analyzing VPC Flow Logs

You can use an AWS-managed analytics service called Amazon Athena to query the logs

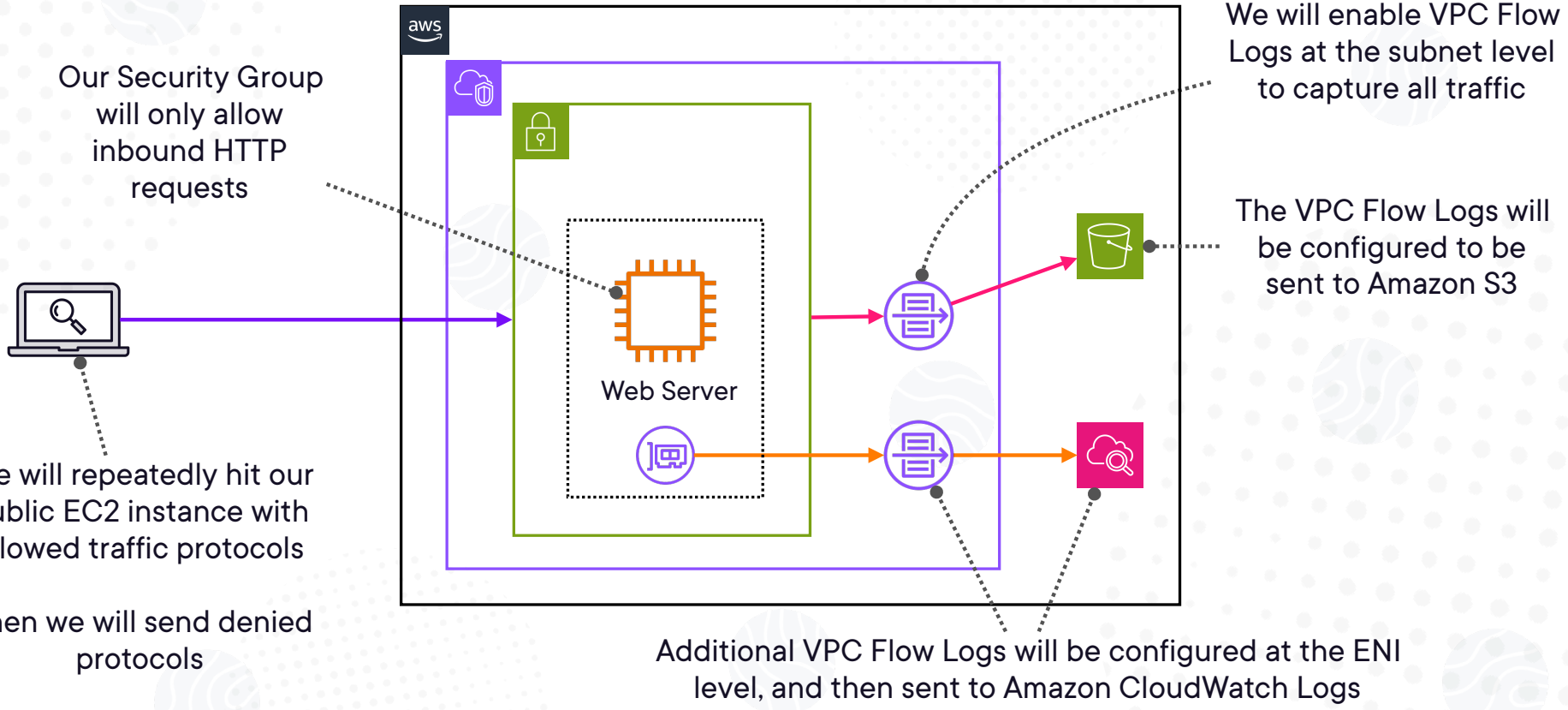
Works on logs stored in your Amazon S3 buckets

Works on logs stored in Amazon CloudWatch Logs

# Exam Pro Tip #1: If you need to monitor IP traffic, think VPC Flow Logs.

# Exam Pro Tip #2: This feature is NOT the same thing as packet inspection.

# Demo: Setting up VPC Flow Logs



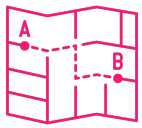
# Capturing Traffic with VPC Traffic Mirroring

# VPC Traffic Mirroring

VPC feature that allows you to copy network traffic from an ENI and then send that traffic to an out-of-band security or monitoring appliance for inspection

# VPC Traffic Mirroring Concepts


You set up a source (*ENI to watch*), filter, target (*destination*), and session




**Destinations**: ENI, Gateway Load Balancer, or a Network Load Balancer

Capability to filter traffic and truncate packets for better data extractions

Supports same VPC, Intra-Region peered VPC, or TGW-attached VPC

Source and targets do **not** have to be in the same AWS account

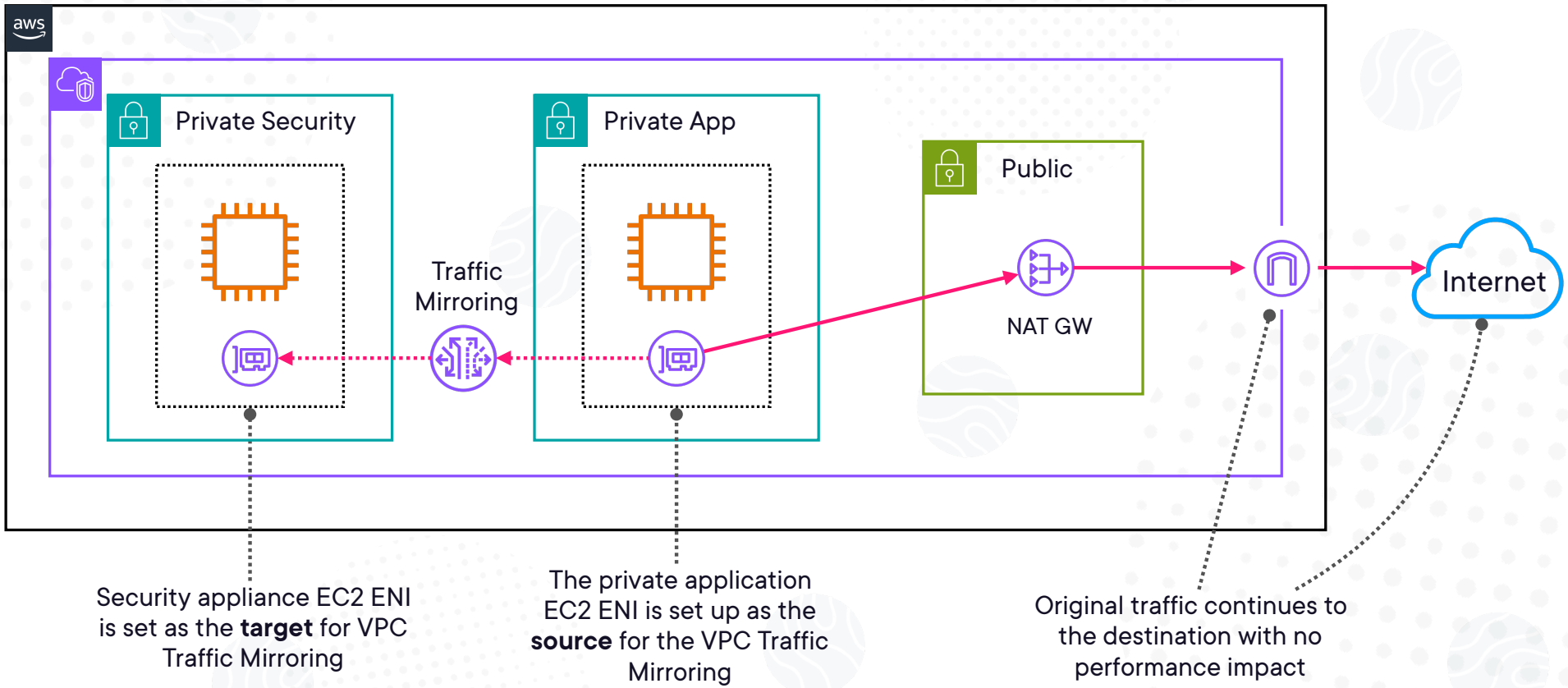
# VPC Traffic Mirroring Use Cases

Content Inspection

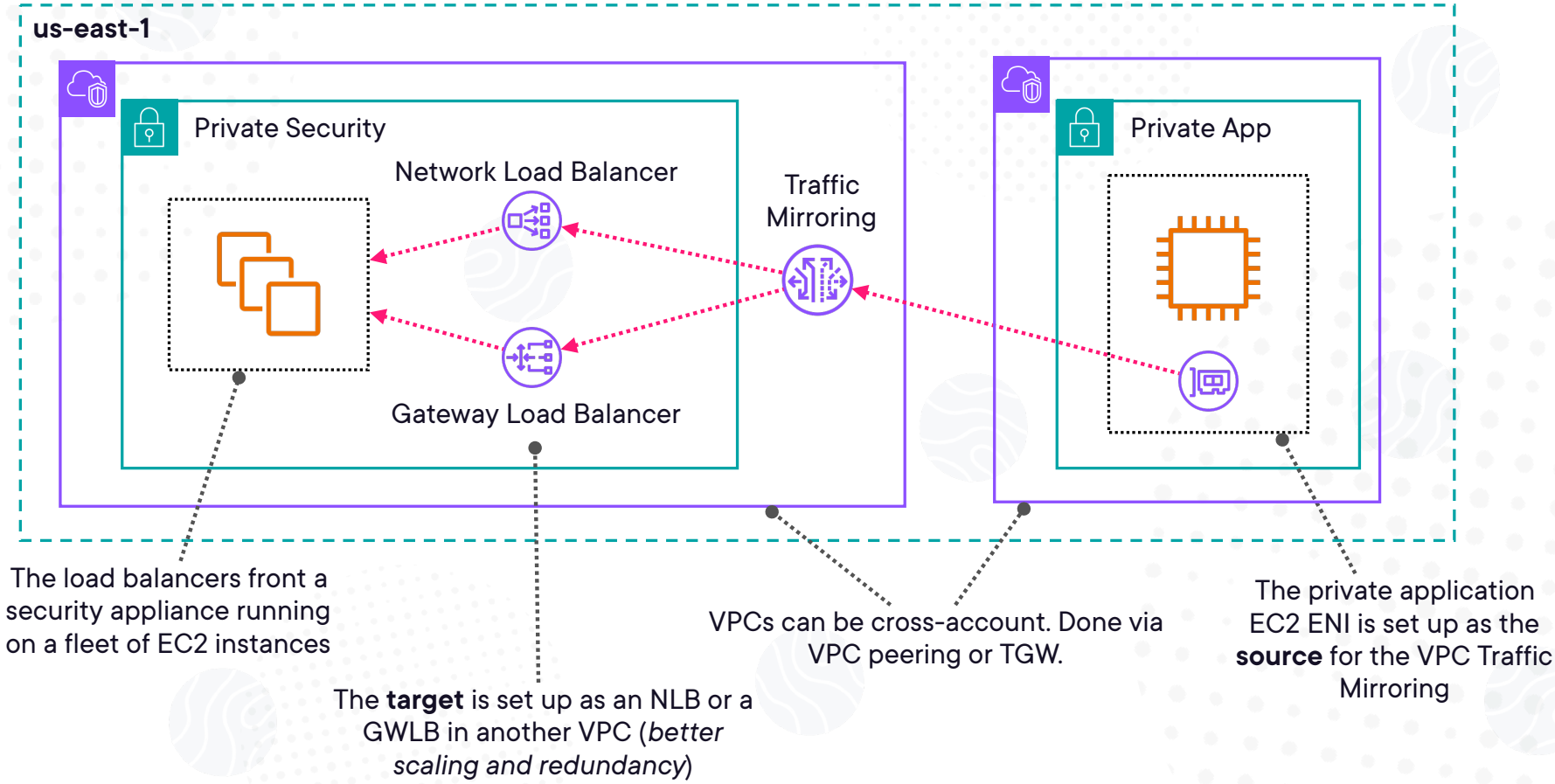
Threat Monitoring

Troubleshooting

# Example Supported Architecture - Same VPC



# Example Supported Architecture - Intra-Region VPC



# IPv6 Egress-only Internet Gateways

# Egress-only Internet Gateways Concepts

Internet gateway that is only useable by resources with IPv6 addresses


It works like a NAT Gateway, but it is only for your IPv6 resources

Allows outbound for IPv6 to the internet, and prevents inbound initiation

No charge for egress-only internet gateways (*but remember data transfers*)

To use these, they require updates to your VPC route tables

# Exam Pro Tips

IPv4 and IPv6 routing is handled via different route rules within route tables

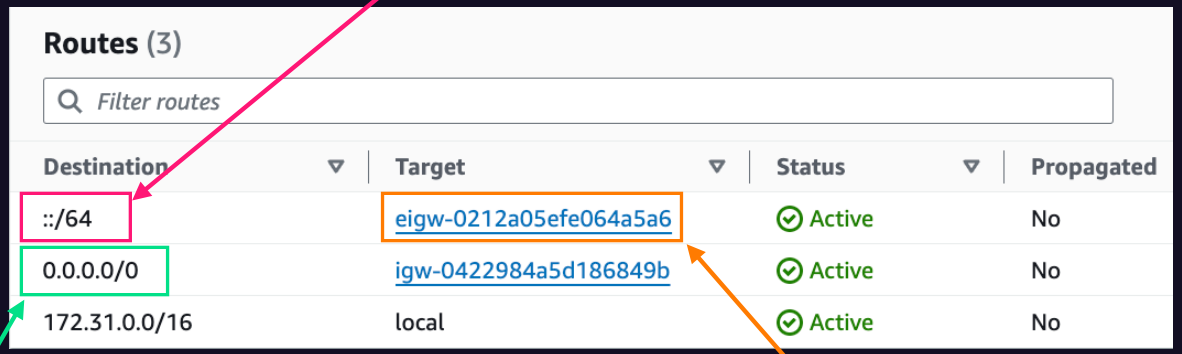
Dual-stack resources can use either NAT Gateways or Egress-only Internet Gateways

You attach your Egress-only Internet Gateway to a VPC just like a normal IGW

# Example Route Table

**Remember you must update your route tables to leverage your Egress-only Internet Gateway (EIGW)!**

The syntax for all IPv6 traffic




Notice IPv4 traffic has its own route rule

The target references the attached EIGW

# Module Summary and Exam Tips

# You can leverage NACLs to quickly block suspected malicious IP address ranges!

# This is the quickest and most cost-effective method.

# VPC Flow Logs Exam Tips

**These capture IP traffic information within your VPC network flows**

**Be familiar with the default version fields**

**These are not meant for packet inspections**

**Remember the supported sources:**

- ENI
- Subnet
- Entire VPC

**Remember the supported destinations:**

- Amazon S3
- Amazon CloudWatch Logs
- Kinesis Data Firehose (*can be cross-account*)

# Common Ports to Know for VPC Flow Logs

Review these ports, as you should be familiar with them to properly analyze your VPC Flow Logs.

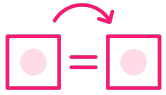
- HTTP: 80
- HTTPS: 443
- SSH: 22
- FTP: 21
- Telnet: 23
- SMTP: 25 (*Standard Port*)
- SMTP: 587 (*Default Port for SMTP with TLS*)
- DNS: 53
- RDP: 3389
- MySQL: 3306
- PostgreSQL: 5432
- Microsoft SQL Server: 1433
- Redis: 6379
- LDAP: 389

# VPC Traffic Mirroring Exam Tips

Feature that allows you to copy network traffic from an ENI and send that traffic to an out-of-band security or monitoring appliance for inspection

Remember that you set up a source (*ENI*), optional filters, a target (*ENI, NLB, or GWLB*), and a session

**Use Cases**: Content inspection, threat monitoring, and troubleshooting

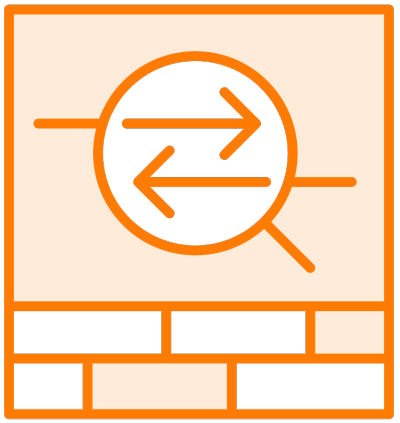


Same VPC, Intra-Region peered VPC, or TGW-attached VPC, and the VPC Traffic Mirroring target can be in a different AWS account

# Egress-only Internet Gateways Exam Tips


**IPv6**

These only work for resources that have IPv6 addresses assigned



**Outbound Only**

Similar to a NAT Gateway where outbound traffic is allowed, but traffic cannot be initiated coming in