BESA NETWORKING TRACK

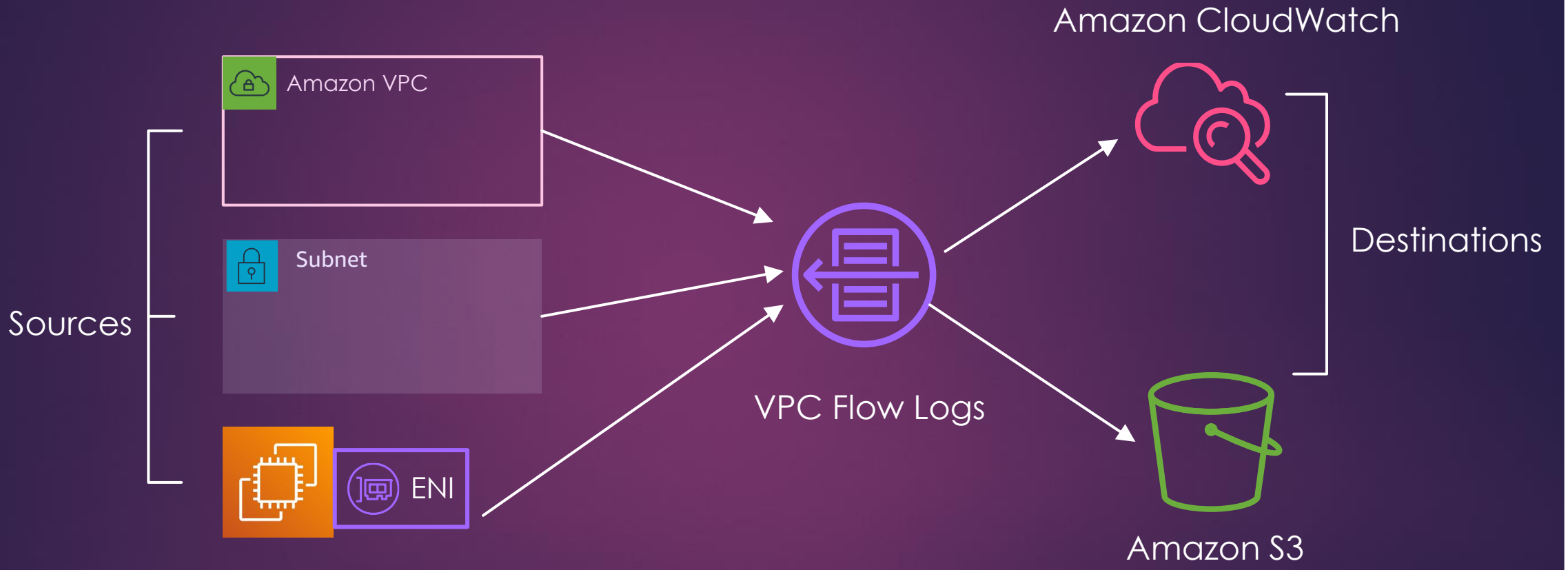
VPC FLOW LOGS
&
REACHABILITY ANALYZER

VPC FLOW LOGS

WHAT ARE A FLOW LOGS?

- FLOW LOGS RECORD INFORMATION ABOUT IP TRAFFIC FLOWING **TO** AND **FROM** NETWORK INTERFACES WITHIN THE VPC.
- ONCE THE LOGS ARE SENT TO ONE OF THE DESTINATIONS, WE CAN THEN USE THAT DATA FOR FURTHER ANALYSIS.
- TROUBLESHOOTING, CONNECTIVITY, AND SECURITY ISSUES

VPC FLOW LOGS



FEATURES OF VPC LOGS

- CAN BE CONFIGURED TO RECORD TRAFFIC PER VPC, SUBNET, OR NETWORK INTERFACE
- VIEW INFORMATION IN THE AMAZON EC2 AND AMAZON VPC CONSOLES
- FLOW LOGS ARE TURNED OFF BY DEFAULT. YOU NEED TO OPT IN
- PUBLISHED TO EITHER AMAZON S3 BUCKETS OR CLOUDWATCH LOG GROUPS
- DATA IS COLLECTED OUTSIDE THE PATH OF YOUR NETWORK TRAFFIC
- DOES NOT AFFECT NETWORK THROUGHPUT OR LATENCY

FEATURES OF VPC LOGS

- ALL SUBNETS AND NETWORK INTERFACES WITHIN A VPC WILL BE MONITORED IF THE FLOW LOGS ARE SET FOR THAT VPC.
- THE NETWORK INTERFACES INSIDE THAT SUBNET WILL BE MONITORED IF FLOW LOGS ARE ENABLED ON THE SUBNET LEVEL.
- WE WILL BE CHARGED FOR DELIVERING LOGS TO THE CLOUDWATCH LOG GROUP AND S3 BUCKET.
- FLOW LOGS RECORD 'NO DATA' AND 'SKIPPED' RECORDS
- ACCEPTED AND REJECTED TRAFFIC ARE RECORDED

VPC FLOW LOGS FIELDS

DEFAULT

Log record format

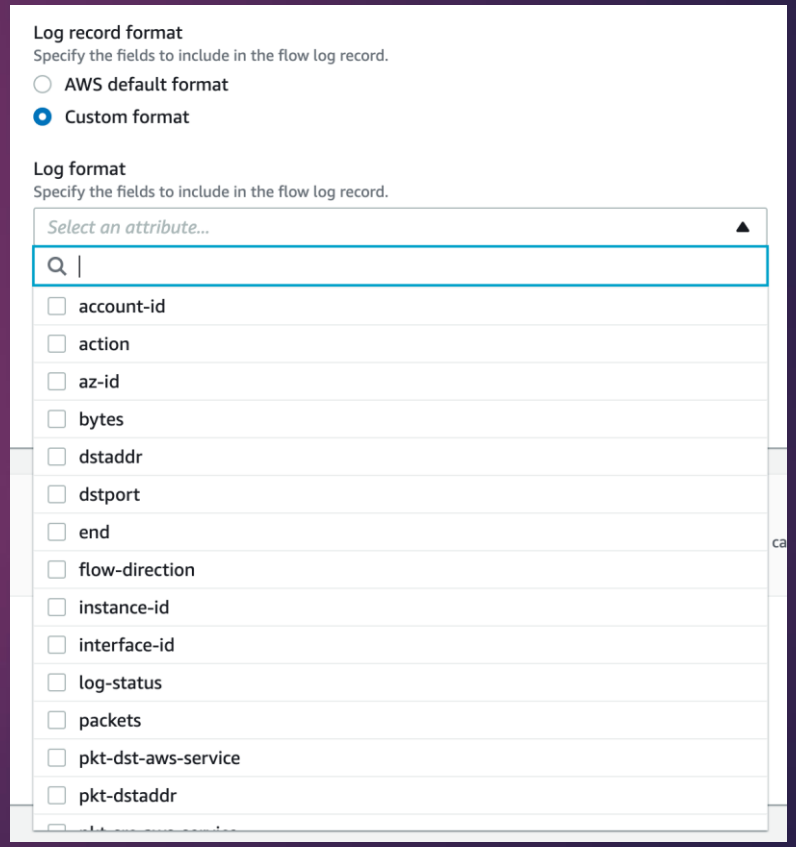
Specify the fields to include in the flow log record.

- (•) AWS default format
- ( ) Custom format

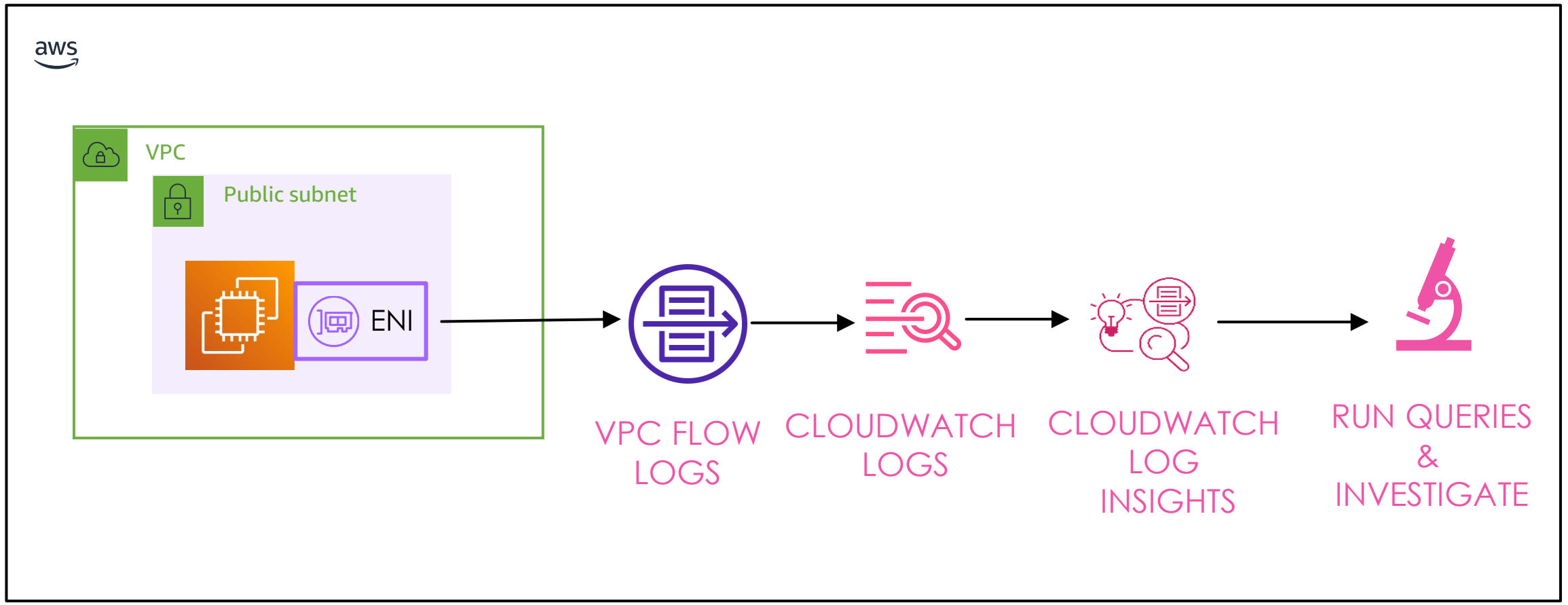
Format preview

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

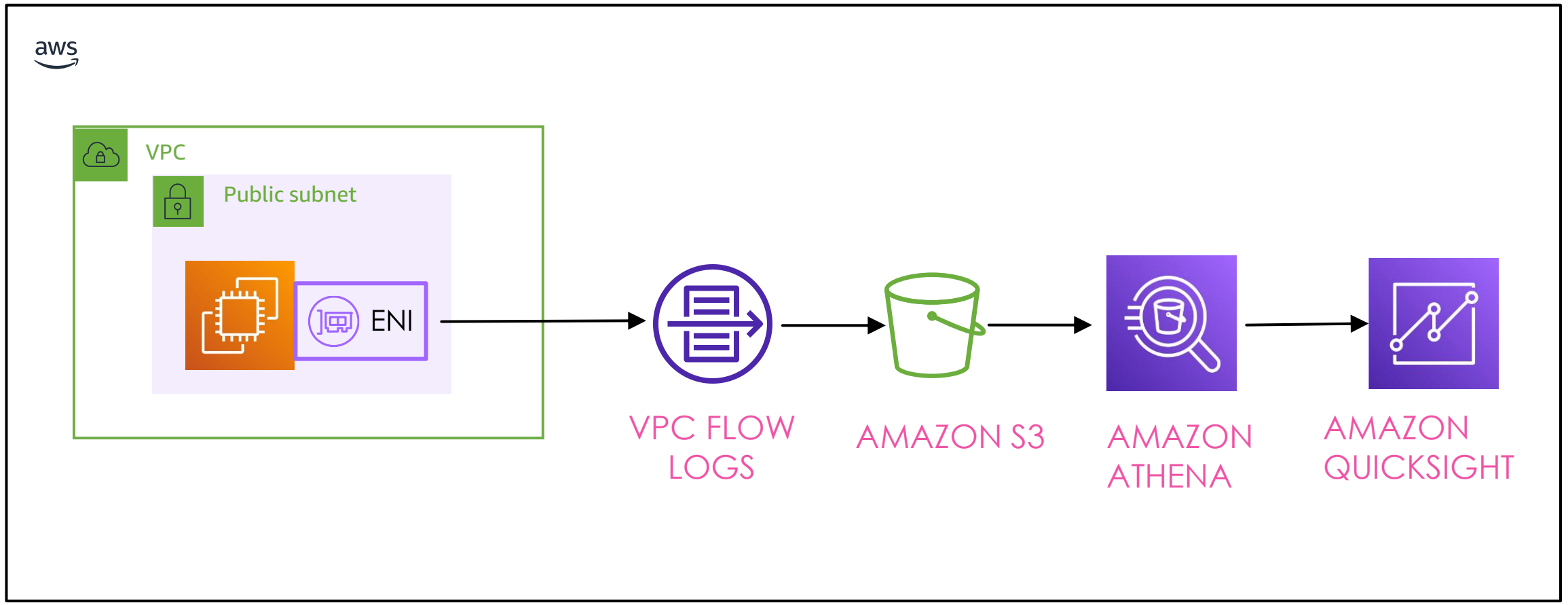
CUSTOM



TROUBLESHOOTING USING VPC FLOW LOGS: EXAMPLE



TROUBLESHOOTING USING VPC FLOW LOGS: EXAMPLE



FLOW LOG RECORD CONTENTS

VPC Flow Logs

AWS account

Elastic network interface ID

Time in Unix seconds; number of packets and bytes transferred

Action taken based on security group or network ACL

Version	2
Account ID	123456789010
Interface ID	eni-02b10a1942934552f
Source address	172.16.1.3
Destination address	172.16.32.46
Source port	36490
Destination port	443
Protocol	6
Packets	78
Bytes	5040
Start	1960245064
End	1960245070
Action	ACCEPT
Log status	OK

FLOW LOG EXAMPLE RECORDS

IN THIS EXAMPLE, SSH TRAFFIC (DESTINATION PORT 22, TCP PROTOCOL) TO NETWORK INTERFACE ENI-1235B8CA123456789 IN ACCOUNT 123456789010 WAS ALLOWED.

2 123456789010 eni-1235b8ca123456789 172.31.16.139 172.31.16.21 20641 22 6 20 4249 1418530010 1418530070 ACCEPT OK

IN THIS EXAMPLE, RDP TRAFFIC (DESTINATION PORT 3389, TCP PROTOCOL) TO NETWORK INTERFACE ENI-1235B8CA123456789 IN ACCOUNT 123456789010 WAS REJECTED.

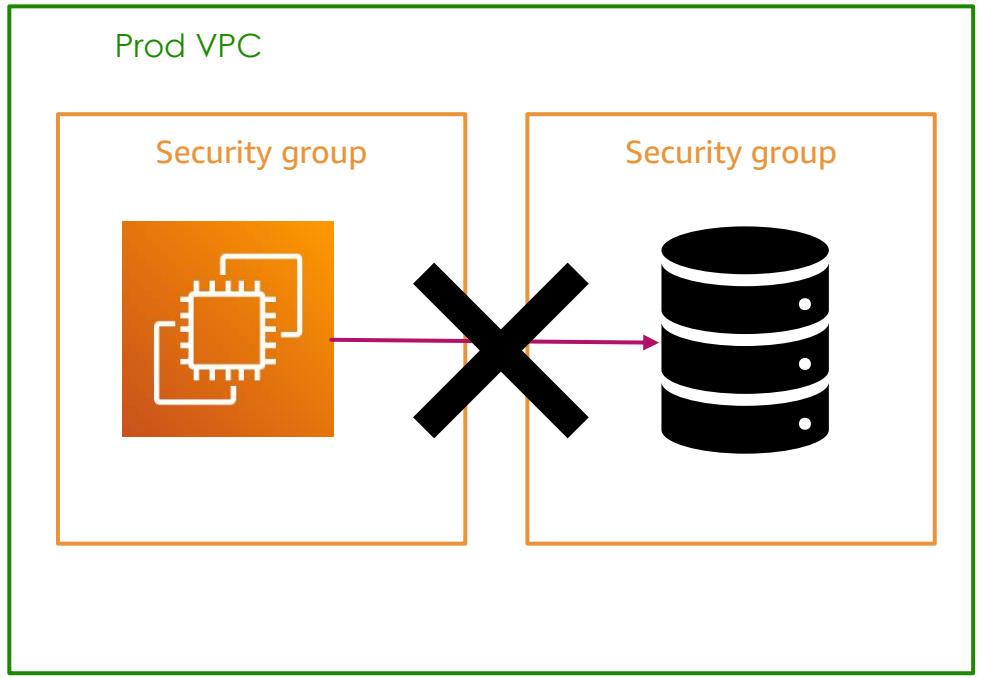
2 123456789010 eni-1235b8ca123456789 172.31.9.69 172.31.9.12 49761 3389 6 20 4249 1418530010 1418530070 REJECT OK

IN THIS EXAMPLE, NO DATA WAS RECORDED DURING THE AGGREGATION INTERVAL.

2 123456789010 eni-1235b8ca123456789 - - - - - - - 1431280876 1431280934 - NODATA

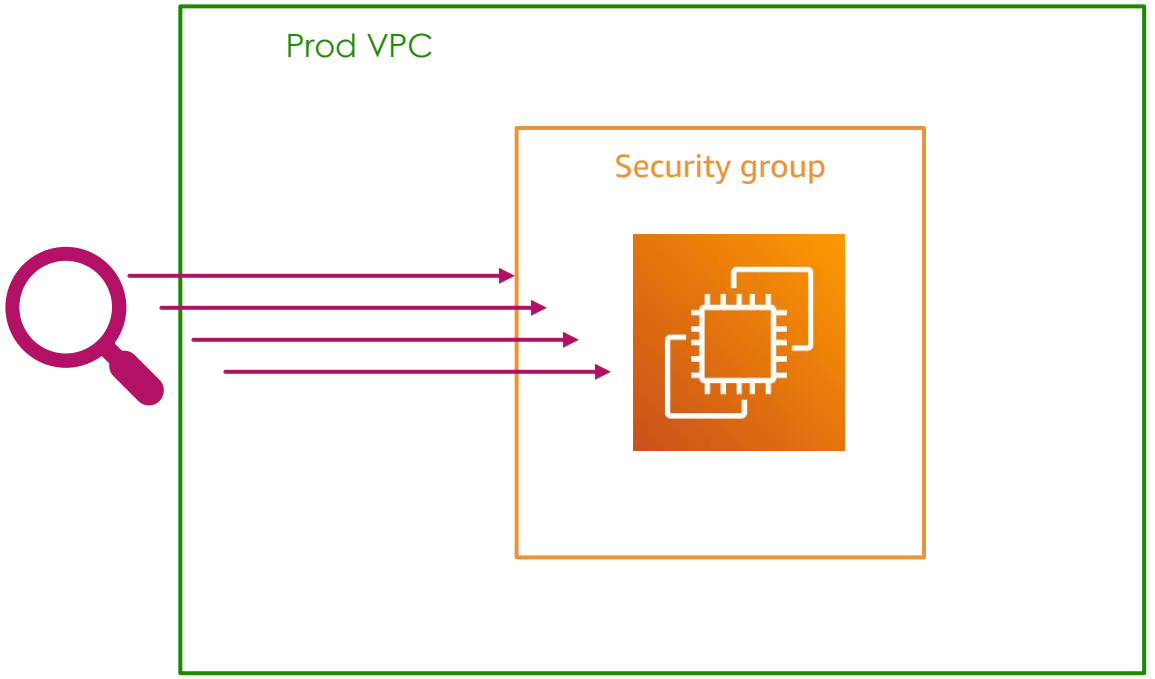
USECASE #1

Diagnose overly restrictive security group rules.



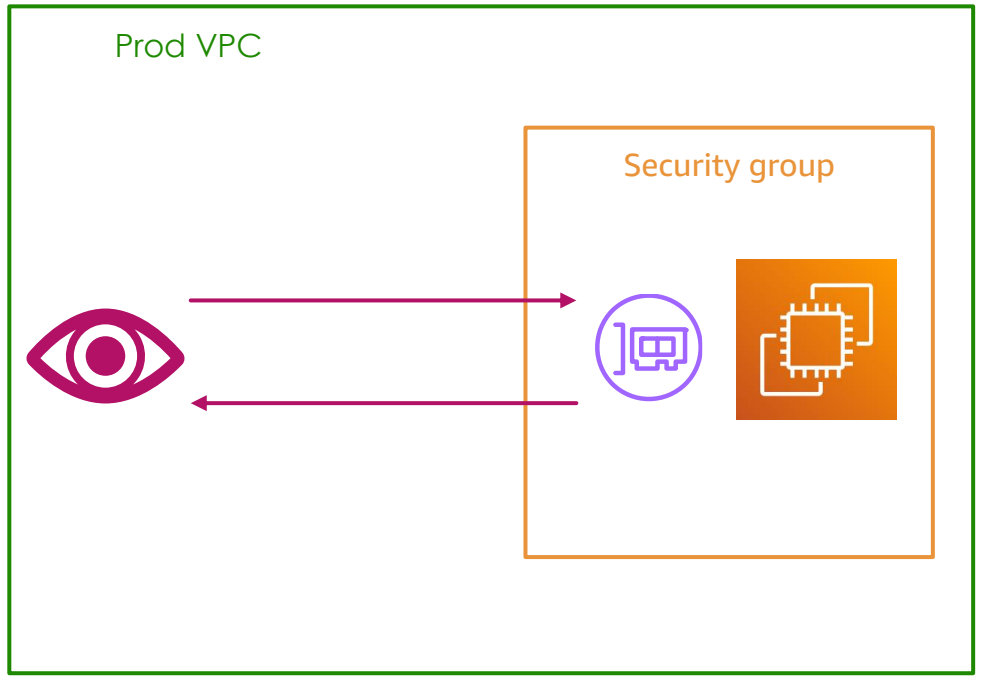
USECASE #2

Monitor the traffic that is reaching your instance



USECASE #3

Determine the direction of the traffic to and from the network interfaces



SOME LIMITATIONS OF VPC LOGS

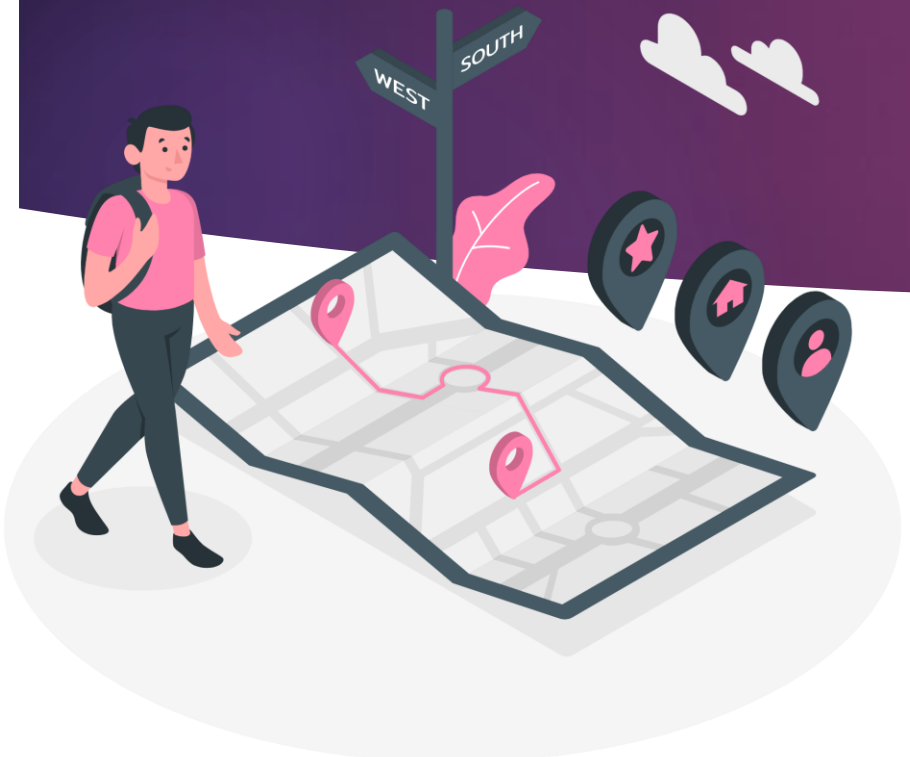
YOU CAN'T ENABLE FLOW LOGS FOR VPCS THAT ARE PEERED WITH YOUR VPC UNLESS THE PEER VPC IS IN YOUR ACCOUNT.

AFTER YOU CREATE A FLOW LOG, YOU CANNOT CHANGE ITS CONFIGURATION OR THE FLOW LOG RECORD FORMAT. NEW FLOW LOG CAN BE CREATED AFTER DELETING OLD ONE

IF TRAFFIC IS SENT TO OR SENT FROM A NETWORK INTERFACE, THE 'SRDADDR' AND 'DSTADDR' FIELDS IN THE FLOW LOG ALWAYS DISPLAY THE PRIMARY PRIVATE IPV4 ADDRESS, REGARDLESS OF THE PACKET SOURCE OR DESTINATION.

TO CAPTURE THE PACKET SOURCE OR DESTINATION, CREATE A FLOW LOG WITH THE 'PKT-SRDADDR' AND 'PKT-DSTADDR'

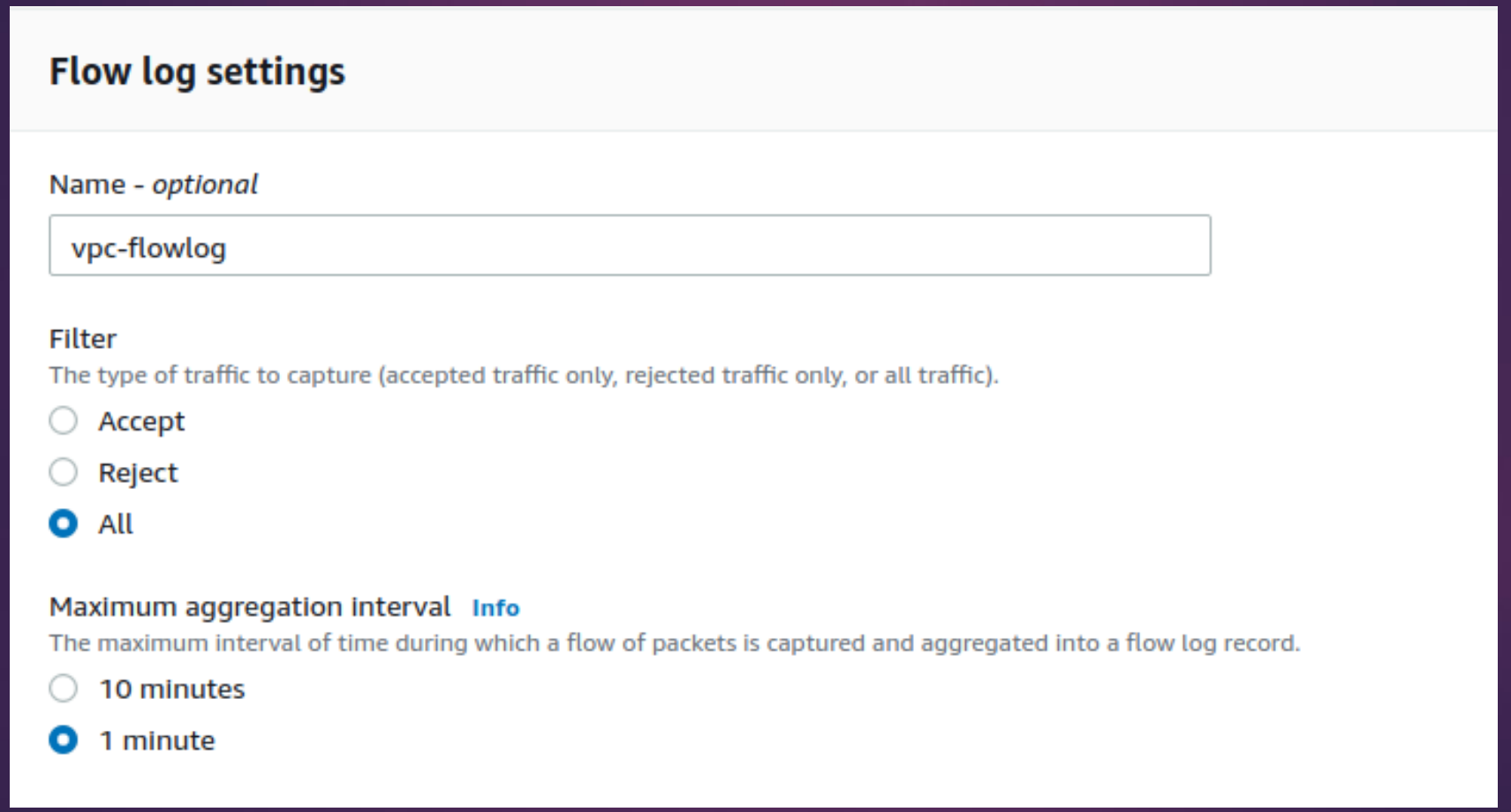
VPC FLOW LOGS
DEMO Time….How does this really work???



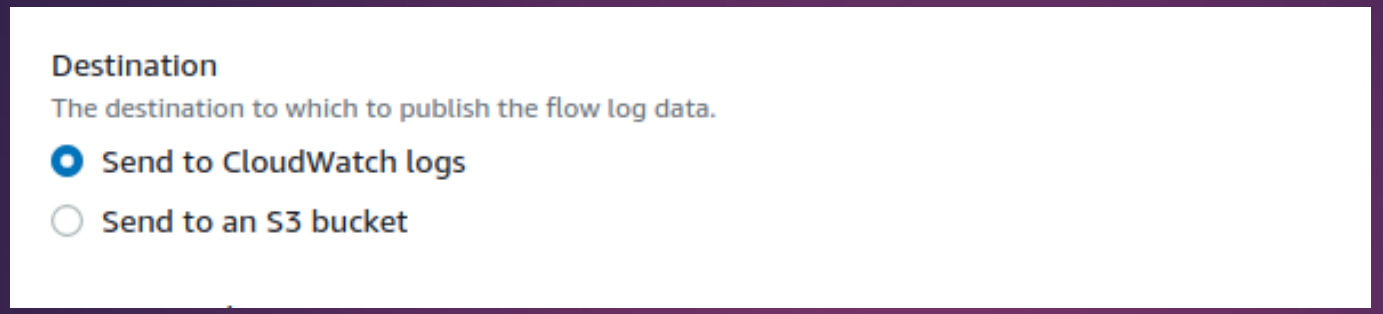
STEPS TO CREATE VPC FLOW LOG

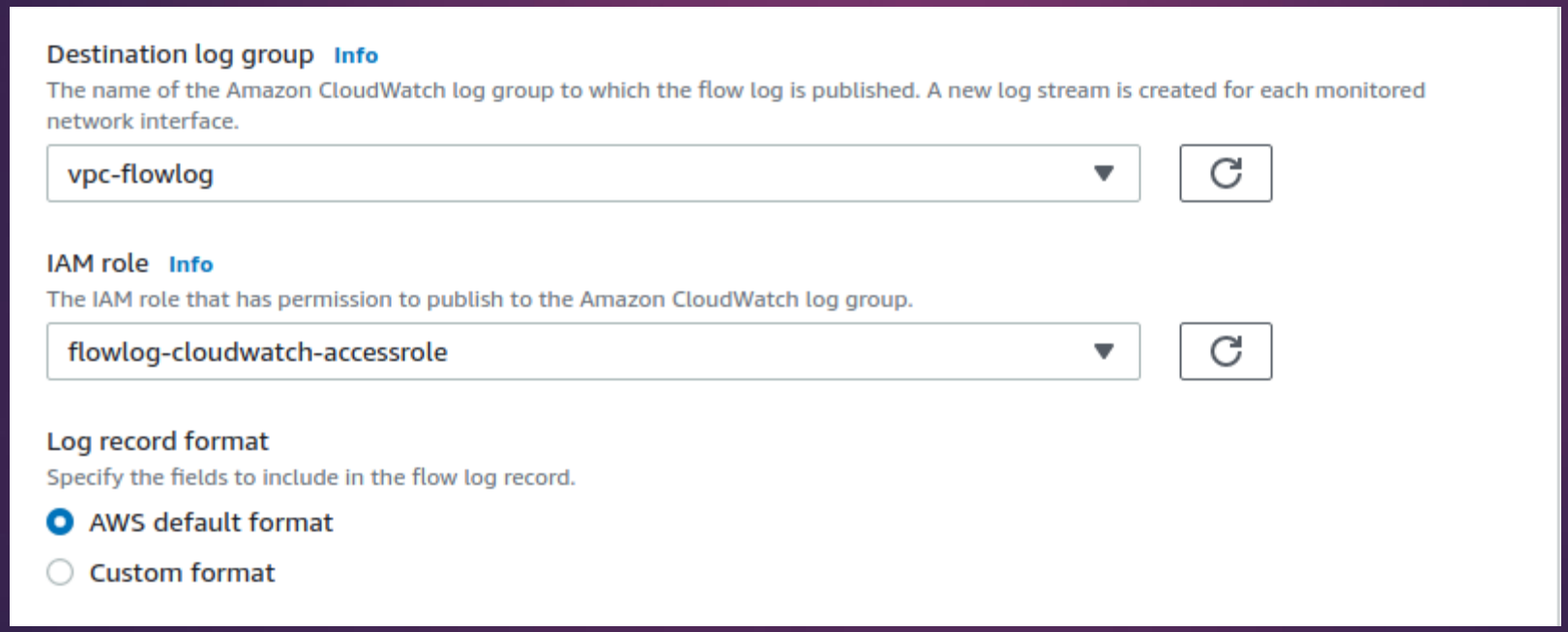
1. TO CREATE A FLOW LOG FOR A VPC, OPEN VPC CONSOLE
2. IN THE NAVIGATION PANE, CHOOSE YOUR VPCS
3. SELECT THE VPC FOR WHICH YOU WANT TO CREATE VPC FLOW LOG, UNDER ACTIONS, CLICK CREATE FLOW LOG
4. UNDER THE FLOW LOG SETTING, PROVIDE A NAME FOR THE FLOW LOG.
5. FOR FILTER, IT WILL ASK FOR THE TYPE OF TRAFFIC THAT NEEDS TO BE RECORDED.
6. CHOOSE ALL TO LOG REJECTED AND ACCEPTED TRAFFIC.
7. FOR THE MAXIMUM AGGREGATION INTERVAL, CHOOSE THE MAXIMUM PERIOD OF TIME DURING WHICH A FLOW LOG IS CAPTURED AND AGGREGATED INTO ONE FLOW LOGS RECORD.

STEPS TO CREATE VPC FLOW LOG



STEPS TO CREATE VPC FLOW LOG



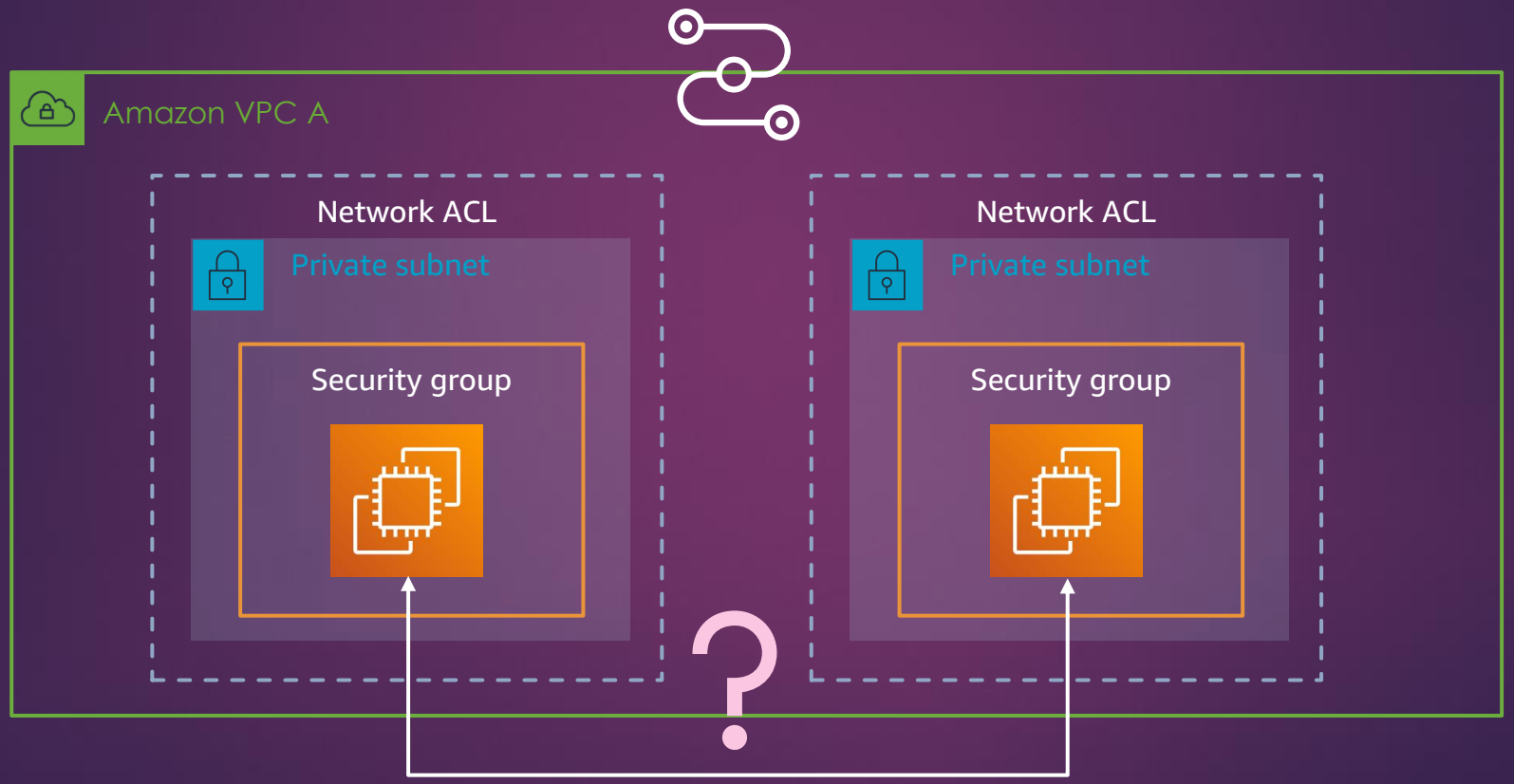


REACHABILITY ANALYZER

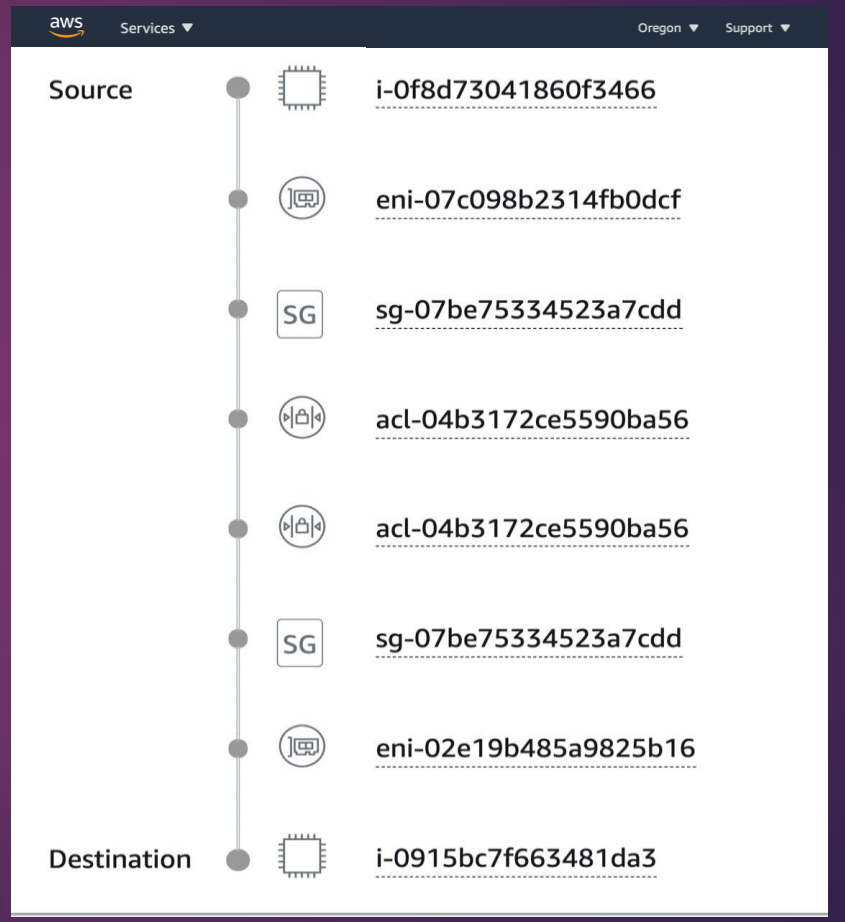
WHAT IS REACHABILITY ANALYZER?

- AN ANALYSIS TOOL THAT ENABLES YOU TO PERFORM CONNECTIVITY TESTING BETWEEN A SOURCE RESOURCE AND A DESTINATION RESOURCE IN YOUR VIRTUAL PRIVATE CLOUDS (VPCS)
- WHEN THE DESTINATION IS REACHABLE, REACHABILITY ANALYZER PRODUCES HOP-BY-HOP DETAILS OF THE VIRTUAL NETWORK PATH BETWEEN THE SOURCE AND THE DESTINATION
- WHEN THE DESTINATION IS NOT REACHABLE, REACHABILITY ANALYZER IDENTIFIES THE BLOCKING COMPONENT

FOR EXAMPLE - PATHS CAN BE BLOCKED BY CONFIGURATION ISSUES IN A SECURITY GROUP, NETWORK ACL OR ROUTE TABLE



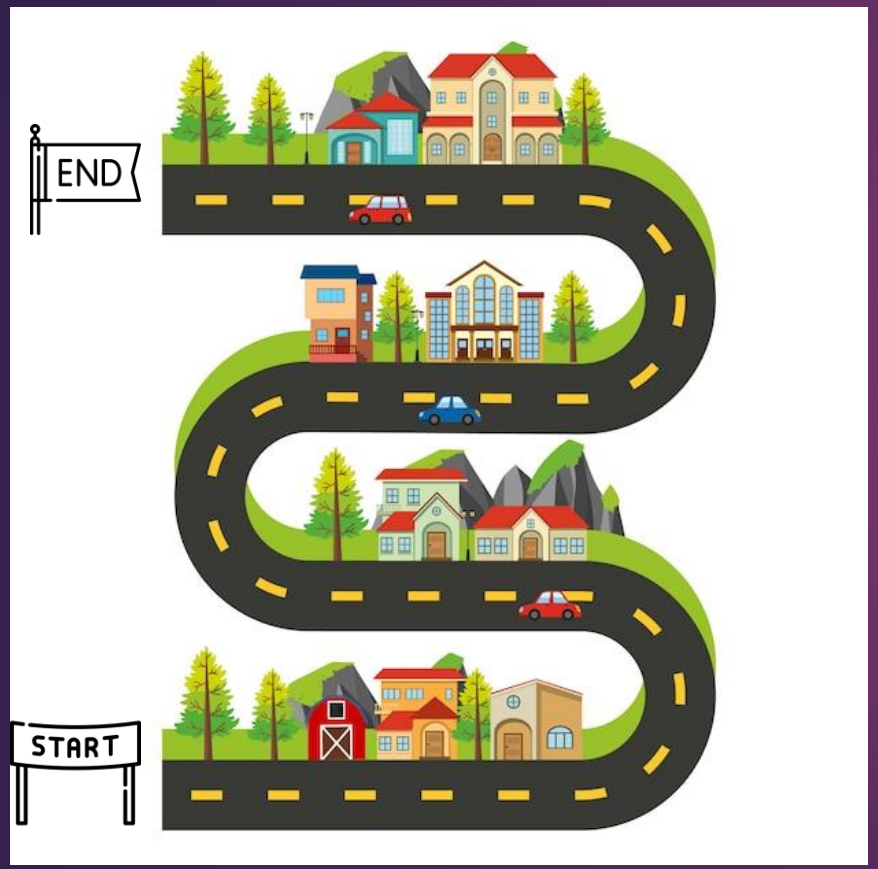
EXAMPLE – TRACING IF DESTINATION IS ‘REACHABLE’ FROM SOURCE



REACHABILITY ANALYZER

DEMO Time….How does this really work???

STEPS TO CREATE AND ANALYZE PATH



Create and analyze path Info

You can specify a network path providing a source, destination, protocol, and optionally packet headers. VPC Reachability Analyzer determines network reachability for your specified network path when you run the analysis. If your network path is reachable, we display details of the components of the network path. If the path is not reachable, we identify the blocking components. You are charged each time you analyze a path. Learn more

Path configuration

Name tag - *optional*

Creates a tag with a key of 'Name' and a value that you specify.

path-01

Path Source

Source type

Choose source type

Source

Source

▶ **Additional packet header configurations at source - *optional***

Path destination

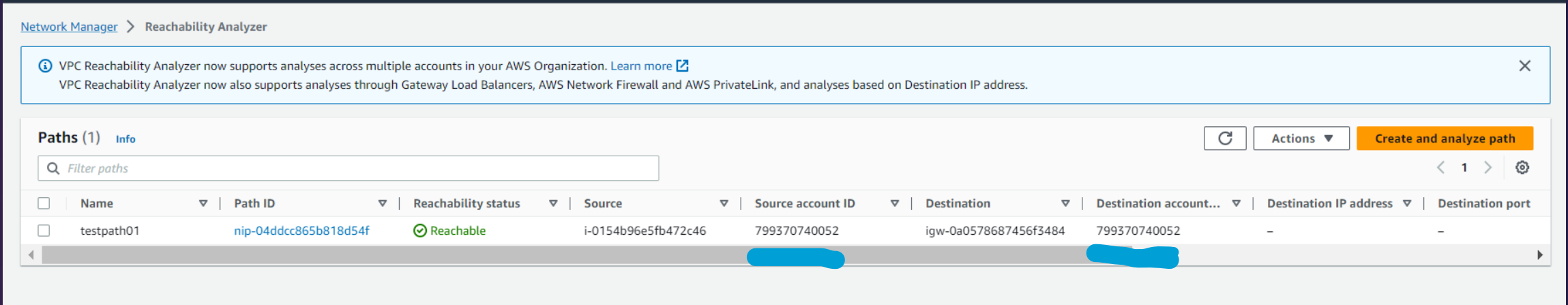
Destination type

Choose destination type

Destination

Destination

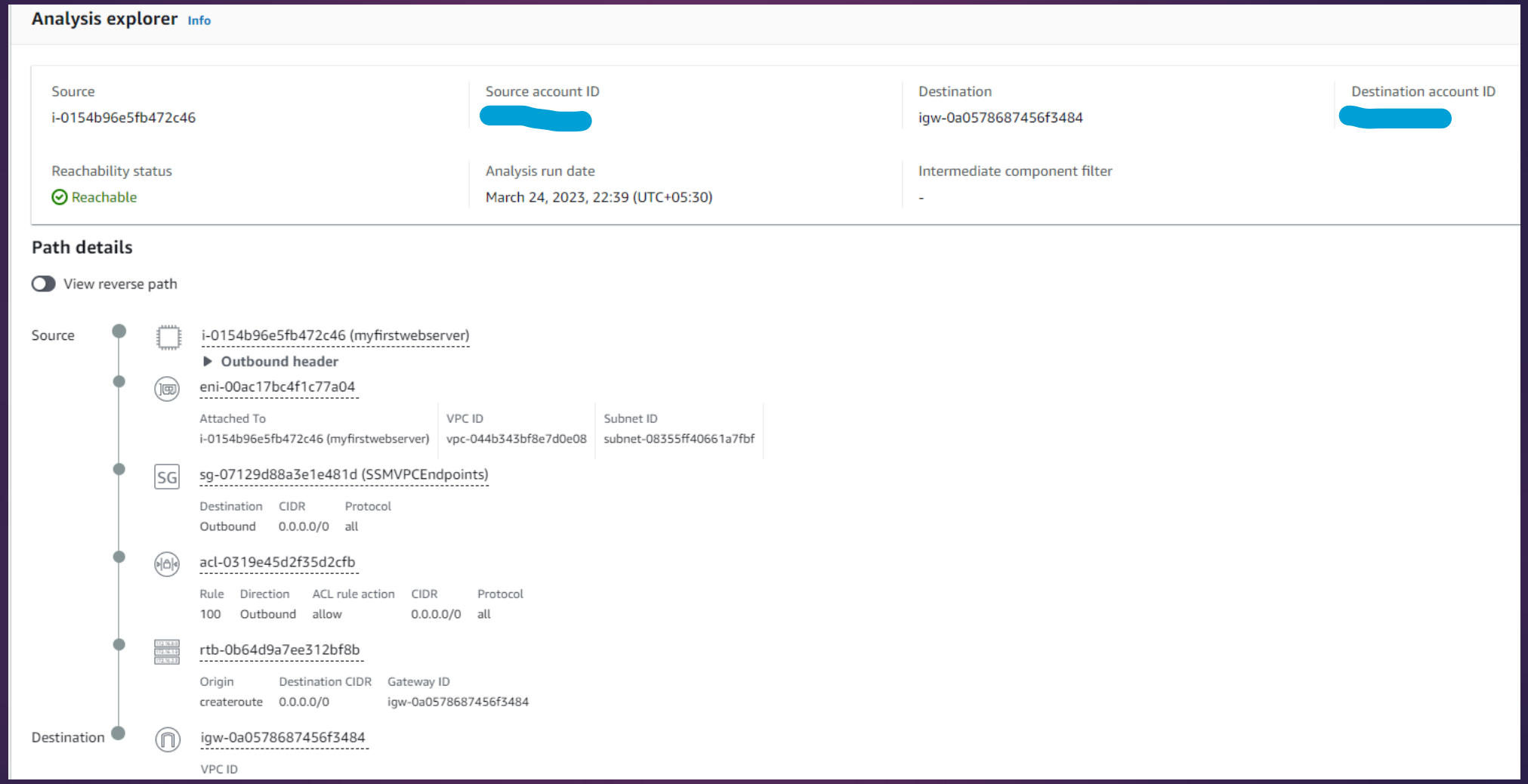
REACHABILITY STATUS



USE CASES

- TROUBLESHOOT CONNECTIVITY ISSUES CAUSED BY NETWORK MISCONFIGURATION.
- VERIFY THAT YOUR NETWORK CONFIGURATION MATCHES YOUR INTENDED CONNECTIVITY.

ANALYSIS EXPLORER



Analysis explorer Info

Source	Source account ID	Destination	Destination account ID
i-0154b96e5fb472c46	[redacted]	igw-0a0578687456f3484	[redacted]

Reachability status	Analysis run date	Intermediate component filter
Reachable	March 24, 2023, 22:39 (UTC+05:30)	-

Path details

View reverse path

Source

i-0154b96e5fb472c46 (myfirstwebserver)

▶ **Outbound header**

eni-00ac17bc4f1c77a04

Attached To	VPC ID	Subnet ID
i-0154b96e5fb472c46 (myfirstwebserver)	vpc-044b343bf8e7d0e08	subnet-08355ff40661a7fbf

sg-07129d88a3e1e481d (SSMVPCEndpoints)

Destination	CIDR	Protocol
Outbound	0.0.0.0/0	all

acl-0319e45d2f35d2cfb

Rule	Direction	ACL rule action	CIDR	Protocol
100	Outbound	allow	0.0.0.0/0	all

rtb-0b64d9a7ee312bf8b

Origin	Destination CIDR	Gateway ID
createroute	0.0.0.0/0	igw-0a0578687456f3484

Destination

igw-0a0578687456f3484

VPC ID

BESA NETWORKING TRACK

THANK YOU