

# Creating VPC Flow Logs



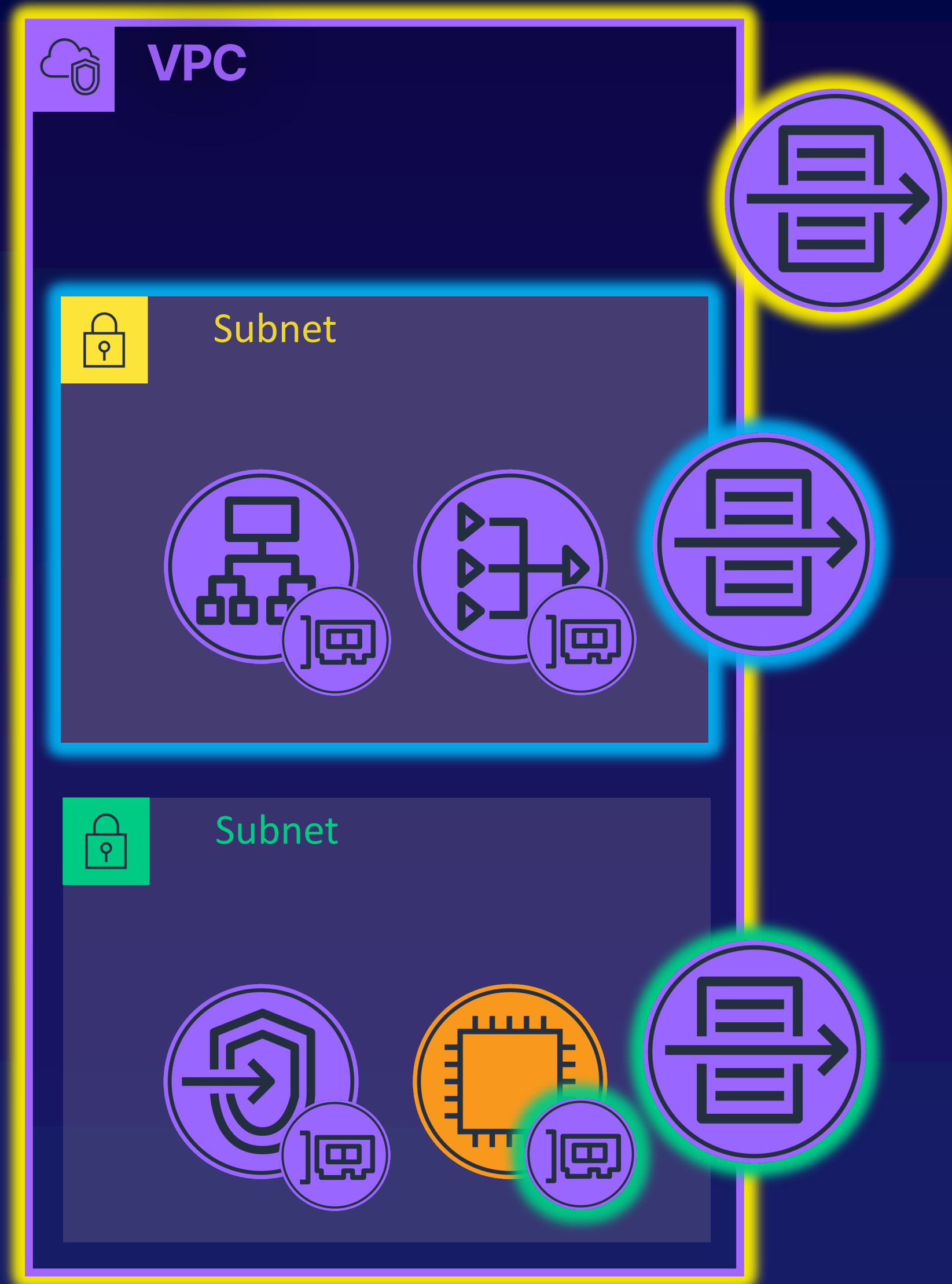
**Steven Moran**  
TRAINING ARCHITECT

# VPC Flow Logs Overview

*Capture information about IP traffic sessions processed by elastic network interfaces in your VPC.*

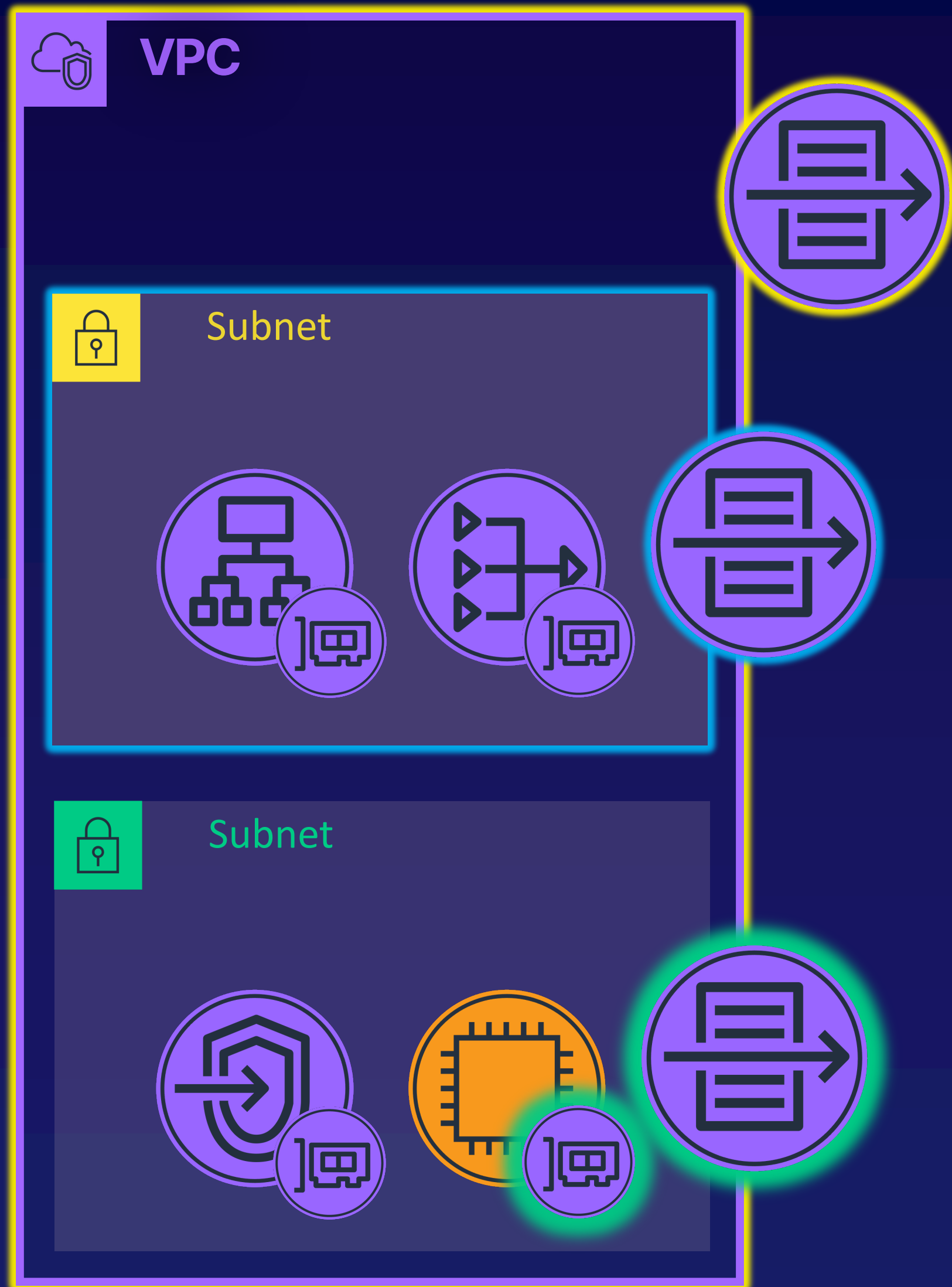


# VPC Flow Logs Overview



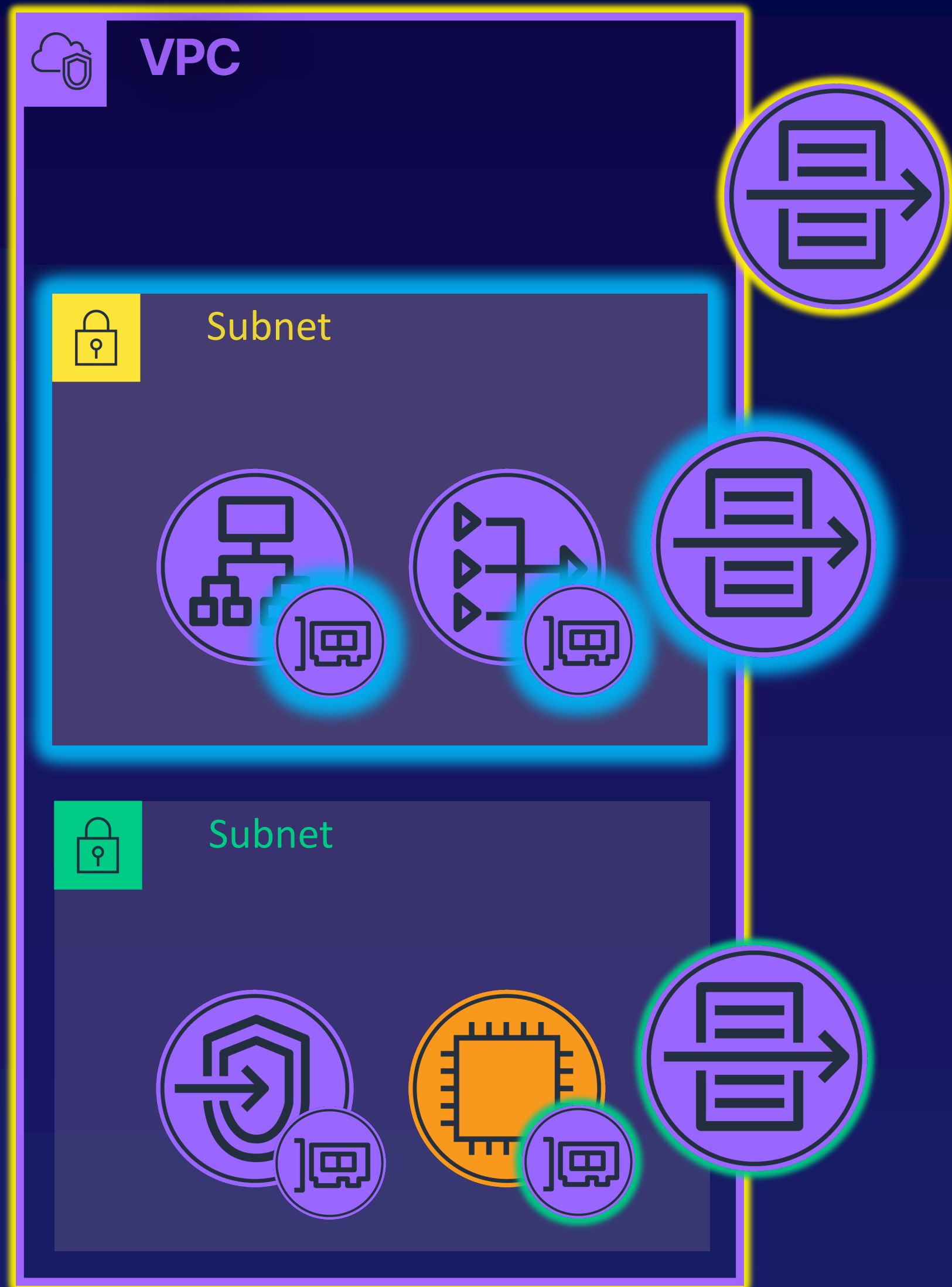
- Flow logs may be defined for:
  - VPCs
  - Subnets
  - ENIs
- Flow log definitions apply to all ENIs within scope.

# VPC Flow Logs Overview



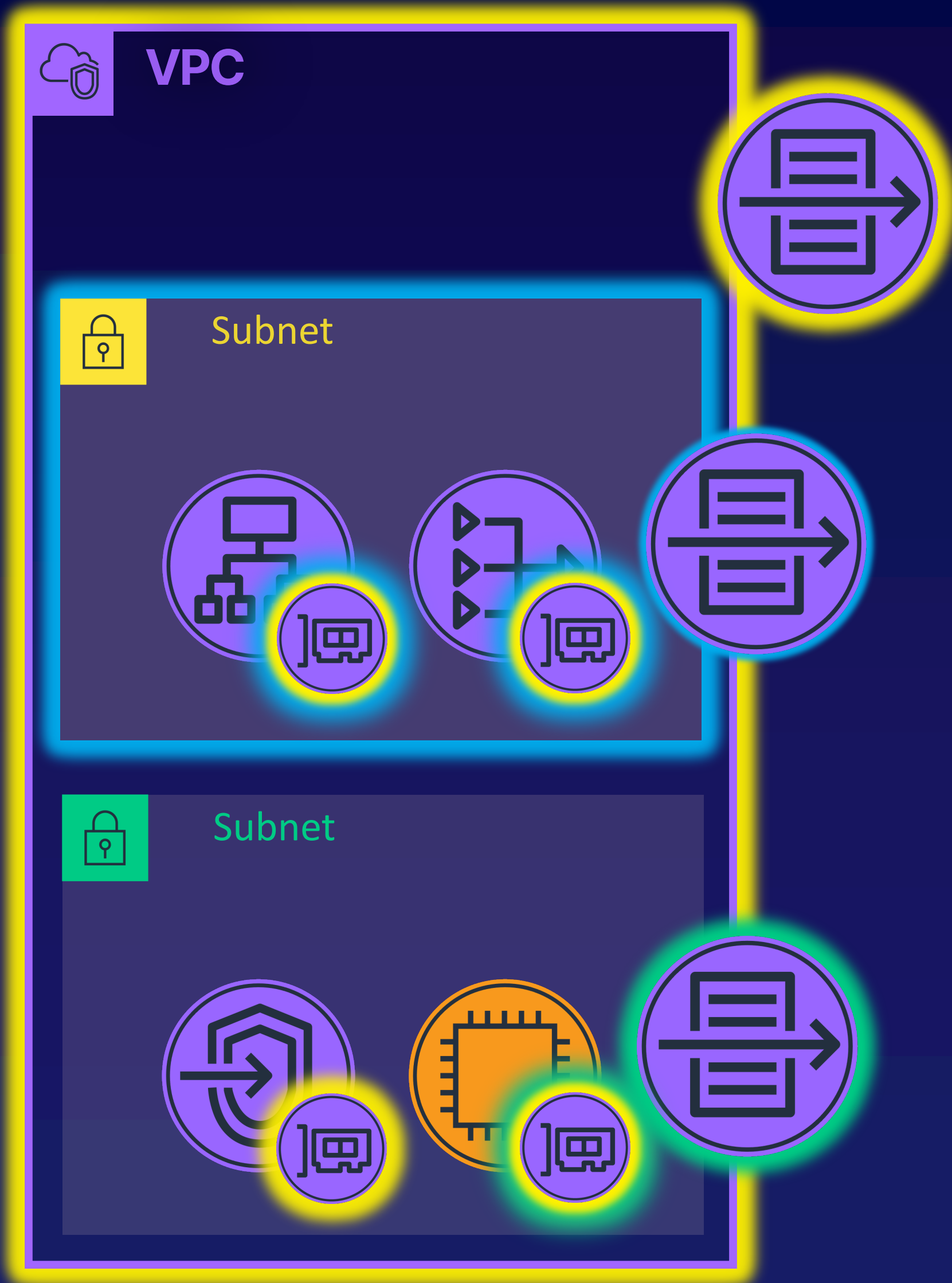
- Flow logs may be defined for:
  - VPCs
  - Subnets
  - ENIs
- Flow log definitions apply to all ENIs within scope.

# VPC Flow Logs Overview



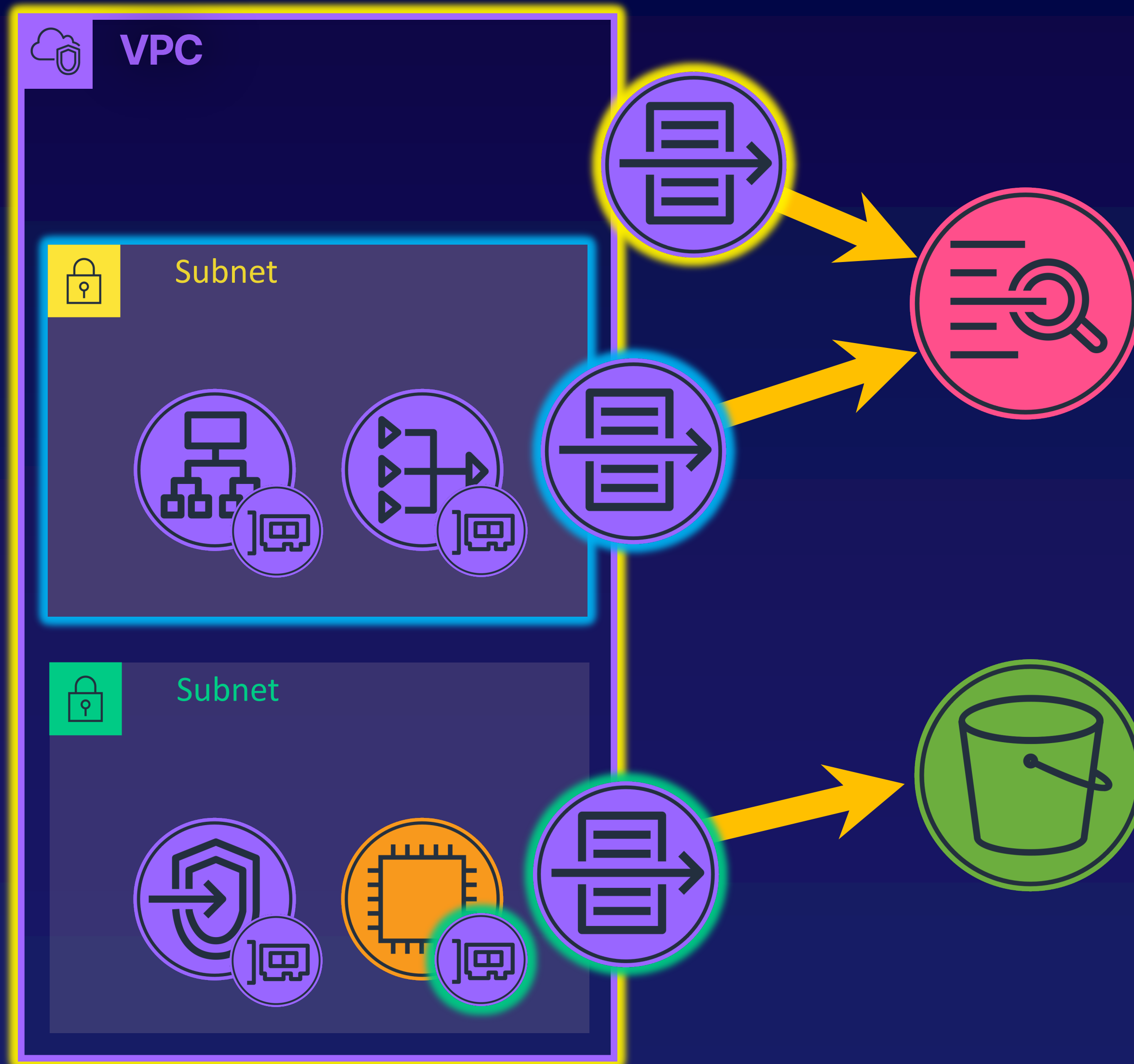
- Flow logs may be defined for:
  - VPCs
  - Subnets
  - ENIs
- Flow log definitions apply to all ENIs within scope.

# VPC Flow Logs Overview



- Flow logs may be defined for:
  - VPCs
  - Subnets
  - ENIs
- Flow log definitions apply to all ENIs within scope.
- Traffic will be logged separately for each definition.

# VPC Flow Logs Overview



- Flow log data may be sent to:
  - CloudWatch log group
    - 1 log stream per ENI
  - S3 bucket
    - 1 log file object per-publication

- Data reporting is not real-time.
  - Data aggregated over one- or ten-minute interval.
  - 5-10 minutes for publication to target.
- Definitions cannot be modified after creation.
- May not record “original” or “correct” IP addresses.



# Limitations

- Does not capture all IP traffic
  - EC2 DNS requests to Route 53
    - Requests to your own DNS servers are logged.
  - Amazon Windows license activation
  - Instance metadata
  - Amazon Time Sync Service
  - DHCP traffic
  - Default VPC router
  - Endpoint services
- Does not capture application data.



# Creating Flow Logs

The screenshot illustrates the AWS console interface for creating flow logs. It is divided into three main sections, each highlighted with an orange border:

- Your VPCs (1/2) Info:** A table listing VPCs. The 'AdvNetSpec' VPC (ID: vpc-0952ac2e3cf2e50ba) is selected. Below the table, the 'vpc-0952ac2e3cf2e50ba / AdvNetSpec' page has tabs for 'Details', 'CIDRs', 'Flow logs', and 'Tags'. The 'Flow logs' tab is highlighted with a purple box.
- Subnets (1/10) Info:** A table listing subnets. The 'public-a' subnet (ID: subnet-0748270603829f793) is selected. Below the table, the 'subnet-0748270603829f793 / public-a' page has tabs for 'Details', 'Flow logs', 'Route table', and 'Network ACL'. The 'Flow logs' tab is highlighted with a purple box.
- Network interfaces (1/4) Info:** A table listing network interfaces. The 'PrivateMetaWeb' interface (ID: eni-04e7cfa1265d008d2) is selected. Below the table, the 'Network interface: eni-04e7cfa1265d008d2 (PrivateMetaWeb)' page has tabs for 'Details', 'Flow logs', and 'Tags'. The 'Flow logs' tab is highlighted with a purple box.

At the bottom right, a 'Create flow log' button is visible, along with a table for configuring the flow log, including a 'Destination name' dropdown.

# Creating Flow Logs

**Your VPCs (1/2)** [Info](#)

1

<input type="checkbox"/>	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR (Network border)
<input checked="" type="checkbox"/>	AdvNetSpec	vpc-0952ac2e3cf2e50ba	<span style="color: green;">✔ Available</span>	10.10.0.0/16	–

vpc-0952ac2e3cf2e50ba / AdvNetSpec

Details
Flow logs
Tags

**Flow logs** [Info](#)

1

<input type="checkbox"/>	Name	Flow log ID	Filter	Destination type	Destination name
<input type="checkbox"/>					

VPC > Your VPCs > Create flow log

## 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
AdvNetSpec	vpc-0952ac2e3cf2e50ba	Available

### Flow log settings

Name - *optional*

#### 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.

- Send to CloudWatch Logs  
 Send to an Amazon S3 bucket

#### Destination log group [Info](#)

The name of the Amazon CloudWatch log group to which the flow log is published. A new log stream is created for each monitored network interface.

#### IAM role [Info](#)

The IAM role that has permission to publish to the Amazon CloudWatch log group.

The IAM role must have permission to publish to the CloudWatch log group. [Set up permissions](#)

#### 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}
  
```

### Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - <i>optional</i>	
<input type="text" value="Name"/>	<input type="text" value="AllVPCTraffic"/>	<input type="button" value="Remove"/>

You can add 49 more tags.

# Creating Flow Logs

VPC > Your VPCs > Create flow log

Create flow log Info

### Flow log settings

Name - *optional*

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

The IAM role must have permission to publish to the CloudWatch log group. [Set up permissions](#)

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)
```

[Copy](#)

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key: Name

Value - optional: AllVPCTraffic

[Remove](#)

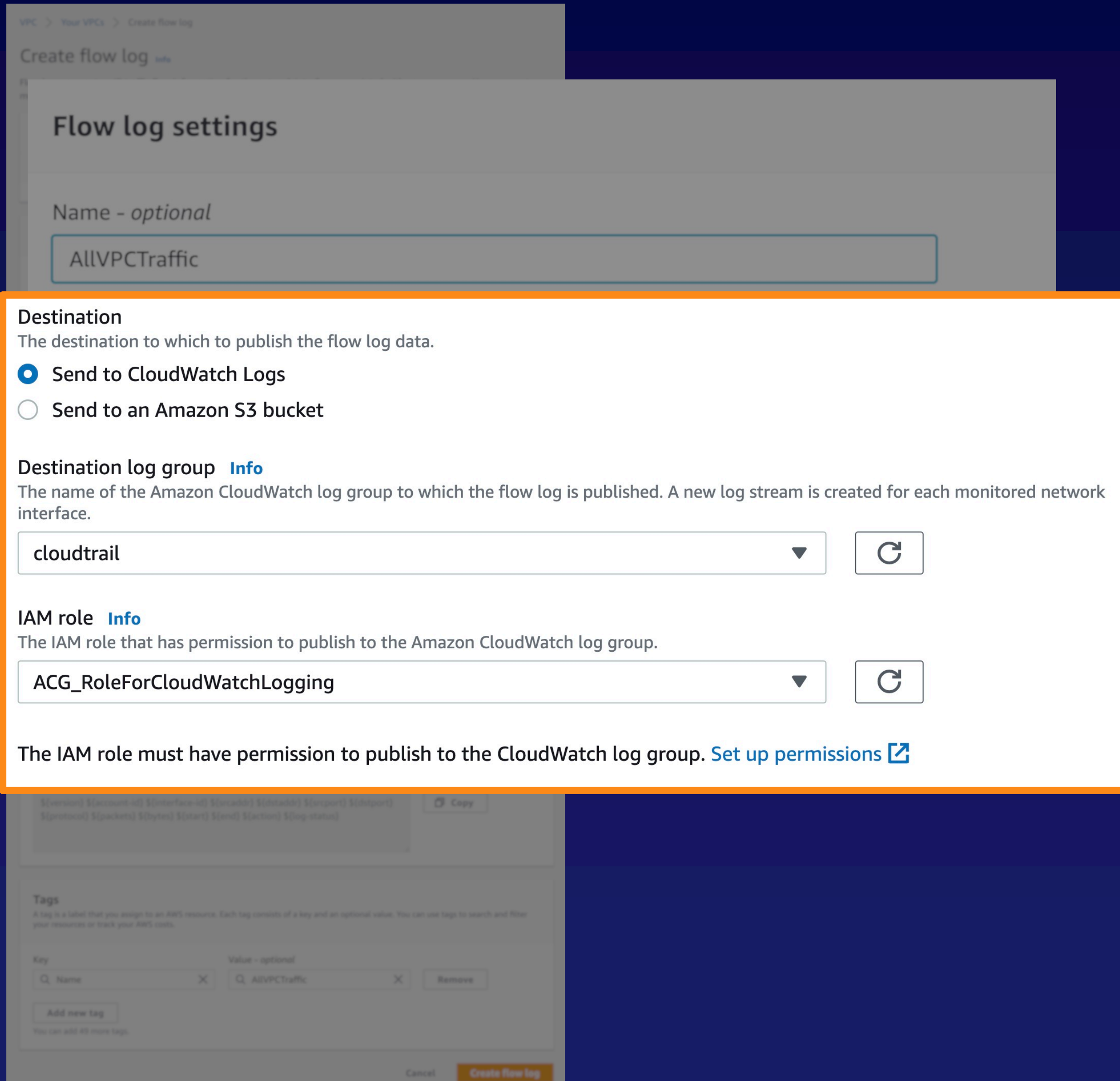
[Add new tag](#)

You can add 49 more tags.

[Cancel](#) [Create flow log](#)

- Name
- Filter
- Maximum aggregation interval

# Creating Flow Logs



**Flow log settings**

Name - optional

AllVPCTraffic

**Destination**  
The destination to which to publish the flow log data.

Send to CloudWatch Logs

Send to an Amazon S3 bucket

**Destination log group** [Info](#)  
The name of the Amazon CloudWatch log group to which the flow log is published. A new log stream is created for each monitored network interface.

cloudtrail

**IAM role** [Info](#)  
The IAM role that has permission to publish to the Amazon CloudWatch log group.

ACG\_RoleForCloudWatchLogging

The IAM role must have permission to publish to the CloudWatch log group. [Set up permissions](#)

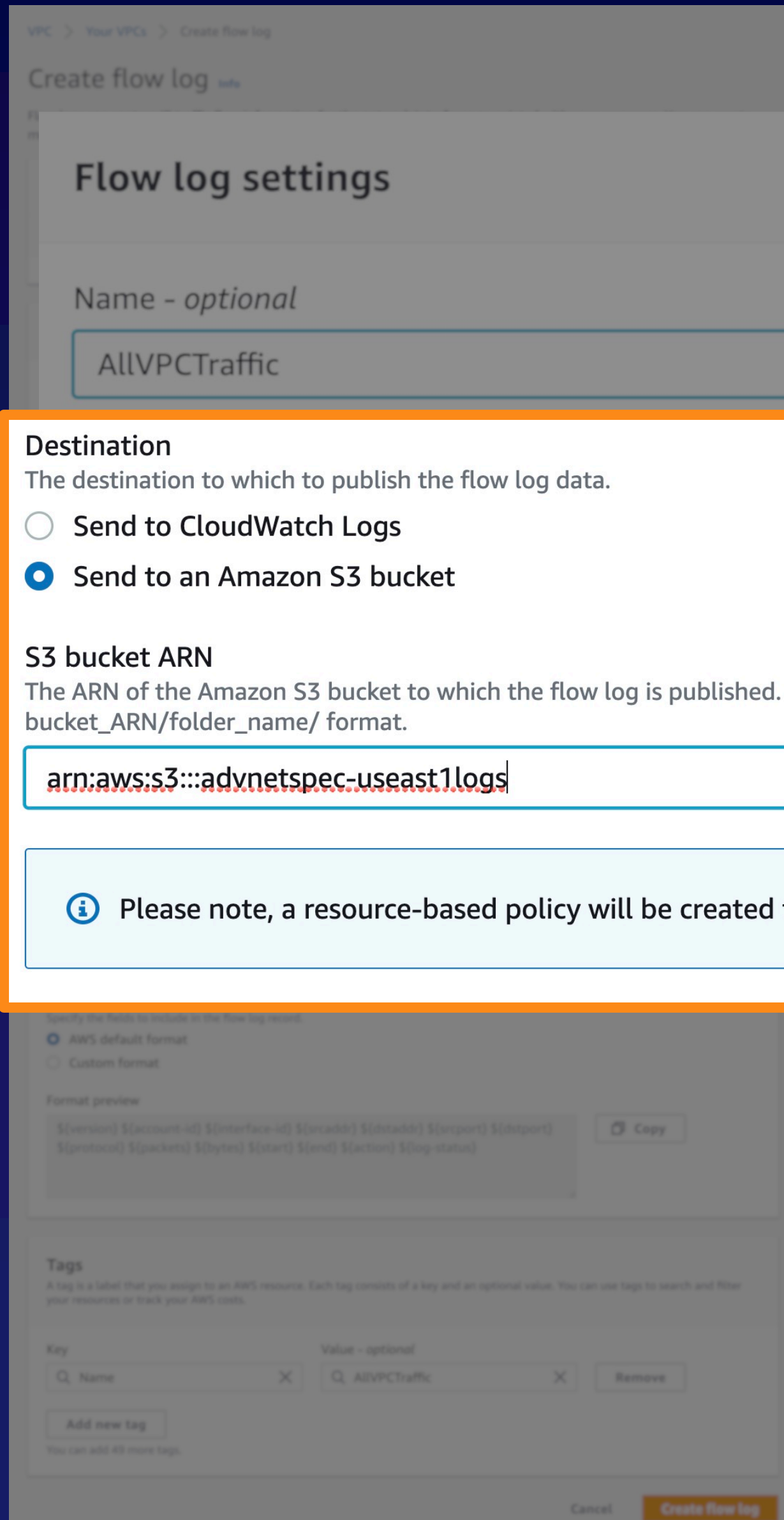
**Tags**  
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key: Name Value - optional: AllVPCTraffic

Cancel Create flow log

- Name
- Filter
- Maximum aggregation interval
- Destination
  - CloudWatch log group
    - Requires IAM role

# Creating Flow Logs



Flow log settings

Name - optional

AllVPCTraffic

**Destination**  
The destination to which to publish the flow log data.

Send to CloudWatch Logs

Send to an Amazon S3 bucket

**S3 bucket ARN**  
The ARN of the Amazon S3 bucket to which the flow log is published. You can specify a specific folder in the bucket using the bucket\_ARN/folder\_name/ format.

arn:aws:s3:::advnetspec-useast1logs

**Please note, a resource-based policy will be created for you and attached to the target bucket.**

Specify the fields to include in the flow log record.

AWS default format

Custom format

Format preview

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key: Name Value - optional: AllVPCTraffic

Add new tag

You can add 40 more tags.

Cancel Create flow log

- Name
- Filter
- Maximum aggregation interval
- Destination
  - CloudWatch log group
    - Requires IAM role
  - S3 bucket
    - Creates bucket policy

# Creating Flow Logs

Create flow log

### Flow log settings

Name - optional

Destination  
The destination to which to publish the flow log data.

Send to CloudWatch Logs

Send to an Amazon S3 bucket

S3 bucket ARN  
The ARN of the Amazon S3 bucket to which the flow log is published. You can specify a specific folder in the bucket using the bucket\_ARN/folder\_name/ format.

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}

```

- Name
- Filter
- Maximum aggregation interval
- Destination
  - CloudWatch log group
    - Requires IAM role
  - S3 bucket
    - Creates bucket policy
- Log record format

# Log Record Fields

- AWS default format

```
2 <accountID> eni-0215590d2fe2d370a 52.94.228.178 10.10.1.194 443 42024 6 24 7151 1622752466 1622752585 ACCEPT OK
```

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

# Log Record Fields

- AWS default format

2 <accountID> eni-0215590d2fe2d370a 52.94.228.178 10.10.1.194 443 42024 6 24 7151 1622752466 1622752585 ACCEPT OK

- version

- Highest field-version used in record
- AWS default format is version 2

- dstaddr
- srcport
- dstport

- protocol
- packets
- bytes
- start
- end
- action
- log-status

# Log Record Fields

- AWS default format

```
2 <accountID> eni-0215590d2fe2d370a 52.94.228.178 10.10.1.194 443 42024 6 24 7151 1622752466 1622752585 ACCEPT OK
```

- version

- protocol

- account-id

- interface-id

- srcaddr

- dstaddr

- srcport

- dstport

- IP address & ports of the source and destination of link-local traffic.
- May be local or remote depending on direction of traffic flow
- Traffic to/from ENIs always show primary private IP address.

# Log Record Fields

- AWS default format

```
2 <accountID> eni-0215590d2fe2d370a 52.94.228.178 10.10.1.194 443 42024 6 24 7151 1622752466 1622752585 ACCEPT OK
```

- version
- account-id
- interface-id
- start
- end
- action
- dstport
- protocol
- packets
- bytes
- start
- end
- log-status

- Unix time when first and last packet of aggregated data was received.

# Log Record Fields

- AWS default format

```
2 <accountID> eni-0215590d2fe2d370a 52.94.228.178 10.10.1.194 443 42024 6 24 7151 1622752466 1622752585 ACCEPT OK
```

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

- Traffic flow ACCEPT-ed or REJECT-ed by SGs and/or NACLs.

# Log Record Fields

- AWS default format

```
2 <accountID> eni-0215590d2fe2d370a 52.94.228.178 10.10.1.194 443 42024 6 24 7151 1622752466 1622752585 ACCEPT OK
```

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

- OK
- NODATA
- SKIPDATA

# Log Record Fields

- Version 3
  - vpc-id
  - subnet-id
  - instance-id
  - tcp-flags
  - type
  - pkt-srcaddr
  - pkt-dstaddr

# Log Record Fields

- Version 3
  - vpc-id
  - subnet-id
  - instance-id
  - tcp-flags
  - type
    - IPv4, IPv6, or EFA
  - pkt-srcaddr
  - pkt-dstaddr

# Log Record Fields

- Version 3
  - vpc-id
  - subnet-id
  - instance-id
  - tcp-flags
  - type
  - pkt-srcaddr
  - pkt-dstaddr

- *Original* IP address of traffic source or destination

# Log Record Fields

- Version 3
  - vpc-id
  - subnet-id
  - instance-id
  - tcp-flags
  - type
  - pkt-srcaddr
  - pkt-dstaddr
- Version 4
  - region
  - az-id
  - sublocation-type
  - sublocation-id

# Log Record Fields

- Version 3

- vpc-id

- s

- in

- to

- type

- pkt-srcaddr

- pkt-dstaddr

- AWS sublocation type that traffic comes from
  - localzone
  - outpost
  - wavelength
  - -

- Version 4

- region

- az-id

- **sublocation-type**

- sublocation-id

# Log Record Fields

- Version 3
  - vpc-id
  - subnet-id
  - instance-id
  - tcp-flags
  - type
  - pkt-srcaddr
  - pkt-dstaddr
- Version 4
  - region
  - az-id
  - sublocation-type
  - sublocation-id
- Version 5
  - pkt-src-aws-service
  - pkt-dst-aws-service
  - flow-direction
  - traffic-path

# Log Record Fields

- Version 3

- vpc-id
- subnet-id
- instance-id
- tcp-flags
- type
- pkt-srcaddr
- pkt-dstaddr

- Name of traffic source/destination AWS service

- Version 4

- region
- az-id
- sublocation-type
- sublocation-id

- Version 5

- pkt-src-aws-service
- pkt-dst-aws-service
- flow-direction
- traffic-path

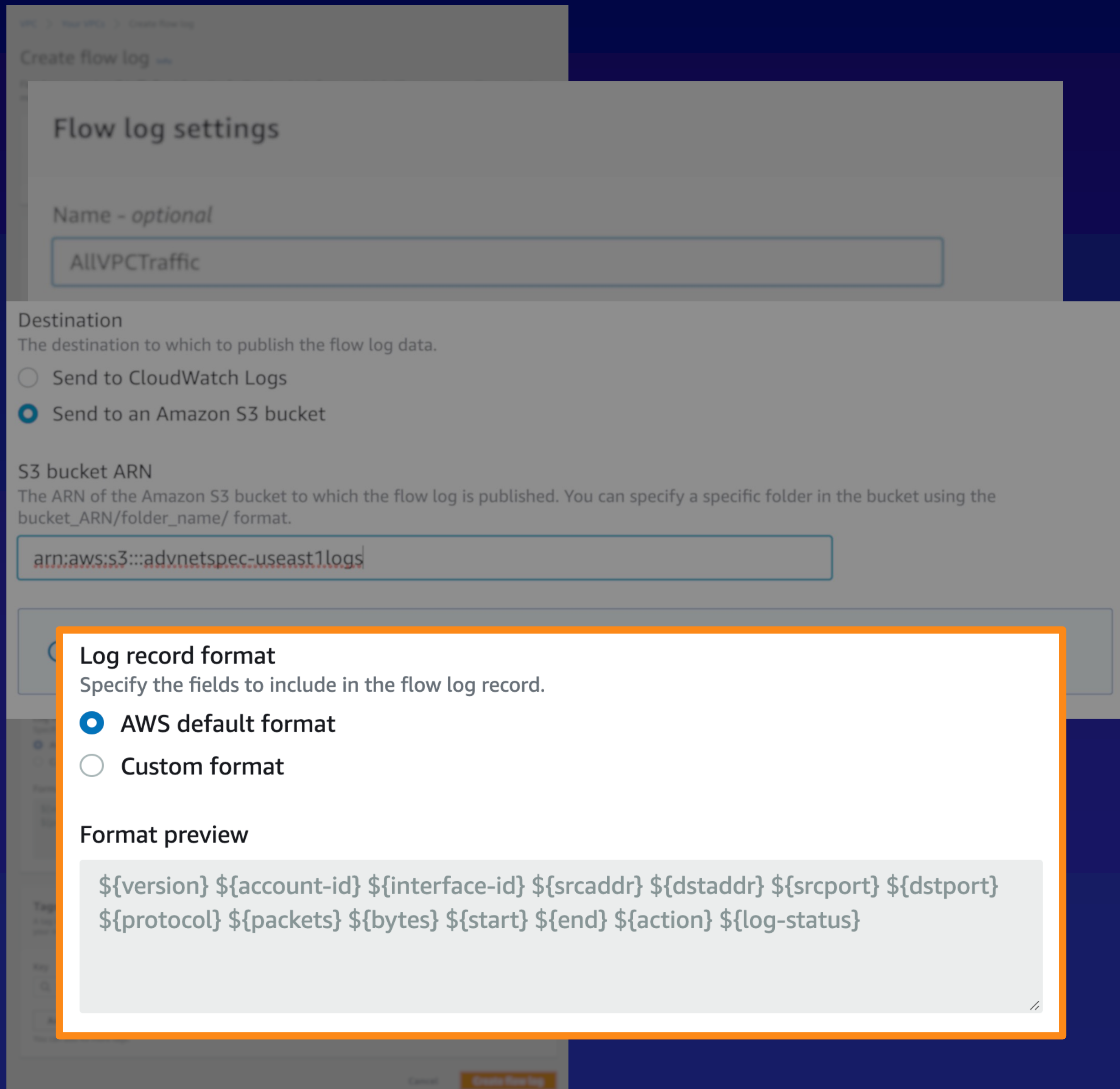
# Log Record Fields

- Version 3
    - vpc-id
    - subnet-id
    - instance-id
    - tcp-flags
    - type
    - pkt-srcaddr
    - pkt-dstaddr
  - Version 4
    - region
    - az-id
    - sublocation-type
    - sublocation-id
  - Version 5
    - pkt-src-aws-service
    - pkt-dst-aws-service
    - **flow-direction**
    - traffic-path
- Whether traffic is ingress or egress

# Log Record Fields

- Version 3
    - vpc-id
    - subnet-id
    - instance-id
    - tcp-flags
    - type
    - p
    - p
  - Version 4
    - region
    - az-id
    - sublocation-type
    - sublocation-id
  - Version 5
    - pkt-src-aws-service
    - pkt-dst-aws-service
    - flow-direction
    - traffic-path
- AWS object-type egress traffic is sent to

# Creating Flow Logs



Create flow log

### Flow log settings

Name - optional

Destination

The destination to which to publish the flow log data.

Send to CloudWatch Logs

Send to an Amazon S3 bucket

S3 bucket ARN

The ARN of the Amazon S3 bucket to which the flow log is published. You can specify a specific folder in the bucket using the bucket\_ARN/folder\_name/ format.

#### 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}
```

- Name
- Filter
- Maximum aggregation interval
- Destination
  - CloudWatch log group
    - Requires IAM role
  - S3 bucket
    - Creates bucket policy
- Log record format

# Creating Flow Logs

## 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...

## Format preview

## 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}
```

- Name
- Filter
- Maximum aggregation interval
- Destination
  - CloudWatch log group
    - Requires IAM role
  - S3 bucket
    - Creates bucket policy
- Log record format

# Creating Flow Logs

Select an attribute...

- account-id
- action
- az-id
- bytes
- dstaddr
- dstport
- end
- flow-direction
- instance-id
- interface-id
- log-status
- packets
- pkt-dst-aws-service
- pkt-dstaddr
- pkt-src-aws-service
- pkt-srcaddr
- protocol
- region
- srcaddr
- srcport
- start
- sublocation-id
- sublocation-type
- subnet-id
- tcp-flags
- traffic-path
- type
- version
- vpc-id

- Name
- Filter
- Maximum aggregation interval
- Destination
  - CloudWatch log group
    - Requires IAM role
  - S3 bucket
    - Creates bucket policy
- Log record format

# Creating Flow Logs

## 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...

interface-id ✕ flow-direction ✕ action ✕ srcaddr ✕ srcport ✕

pkt-srcaddr ✕ dstaddr ✕ dstport ✕ pkt-dstaddr ✕

protocol ✕ start ✕ end ✕ traffic-path ✕

Clear all

## Format preview

```

${interface-id} ${flow-direction} ${action} ${srcaddr} ${srcport} ${pkt-srcaddr}
${dstaddr} ${dstport} ${pkt-dstaddr} ${protocol} ${start} ${end} ${traffic-path}
  
```

```

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

- Name
- Filter
- Maximum aggregation interval
- Destination
  - CloudWatch log group
    - Requires IAM role
  - S3 bucket
    - Creates bucket policy
- Log record format

# Creating Flow Logs

### Your VPCs (1/2) [Info](#)

[Refresh](#) [Actions](#) [Create VPC](#)

< 1 > [Settings](#)

<input type="checkbox"/>	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR (Network border group)
<input checked="" type="checkbox"/>	AdvNetSpec	vpc-0952ac2e3cf2e50ba	Available	10.10.0.0/16	-

vpc-0952ac2e3cf2e50ba / AdvNetSpec

[Details](#) | [CIDRs](#) | [Flow logs](#) | [Tags](#)

---

### Flow logs (1/2) [Info](#)

[Refresh](#) [Actions](#) [Create flow log](#)

< 1 > [Settings](#)

<input type="checkbox"/>	Name	Flow log ID	Filter	Destination t...	Destination name	Maximum aggregation interval
<input type="checkbox"/>	AllVPCTraffic_CW	fl-049035da00cc7525a	ALL	cloud-watch-logs	<a href="#">cloudtrail</a>	10 minutes
<input checked="" type="checkbox"/>	AllVPCTraffic_S3	fl-03e168a35d16de857	ALL	s3	<a href="#">advnetspec-useast1logs</a>	10 minutes

# Creating Flow Logs

### Subnets (1/10) [Info](#)

Filter subnets

<input type="checkbox"/>	Name	Subnet ID
<input type="checkbox"/>	-	subnet-a48b5195
<input checked="" type="checkbox"/>	public-a	subnet-0748270603829f793
<input type="checkbox"/>	private-b	subnet-0a81335232d8477bb

subnet-0748270603829f793 / public-a

Details **Flow logs** Route table Network ACL

### Flow logs (2)

Filter flow logs

<input type="checkbox"/>	Name	Flow log ID
<input type="checkbox"/>	AllVPCTraffic_CW	fl-049035da00cc7525a
<input type="checkbox"/>	AllVPCTraffic_S3	fl-03e168a35d16de857

### Network interfaces (1/4) [Info](#)

Filter network interfaces

<input type="checkbox"/>	Name	Network interface ID
<input checked="" type="checkbox"/>	PrivateMetaWeb	eni-04e7cfa1265d008d2

Network interface: eni-04e7cfa1265d008d2 (PrivateMetaWeb)

Details **Flow logs** Tags

### Flow logs (2)

Filter flow logs

<input type="checkbox"/>	Name	Flow log ID
<input type="checkbox"/>	AllVPCTraffic_CW	fl-049035da00cc7525a
<input type="checkbox"/>	AllVPCTraffic_S3	fl-03e168a35d16de857

VPC flow logs capture information about IP traffic sessions processed by ENIs in your VPCs.

---

Log records may be sent to CloudWatch logs or stored in S3 buckets.

---

Customize fields recorded in logs using AWS-provided fields.

---

Do not record application-level data.

---

Log data is not published in real-time.