Securing Infrastructure in AWS

Ryan Lewis
CLOUD ENGINEER

@ryanmurakami ryanlewis.dev

Overview

It’s between resources and their VPC

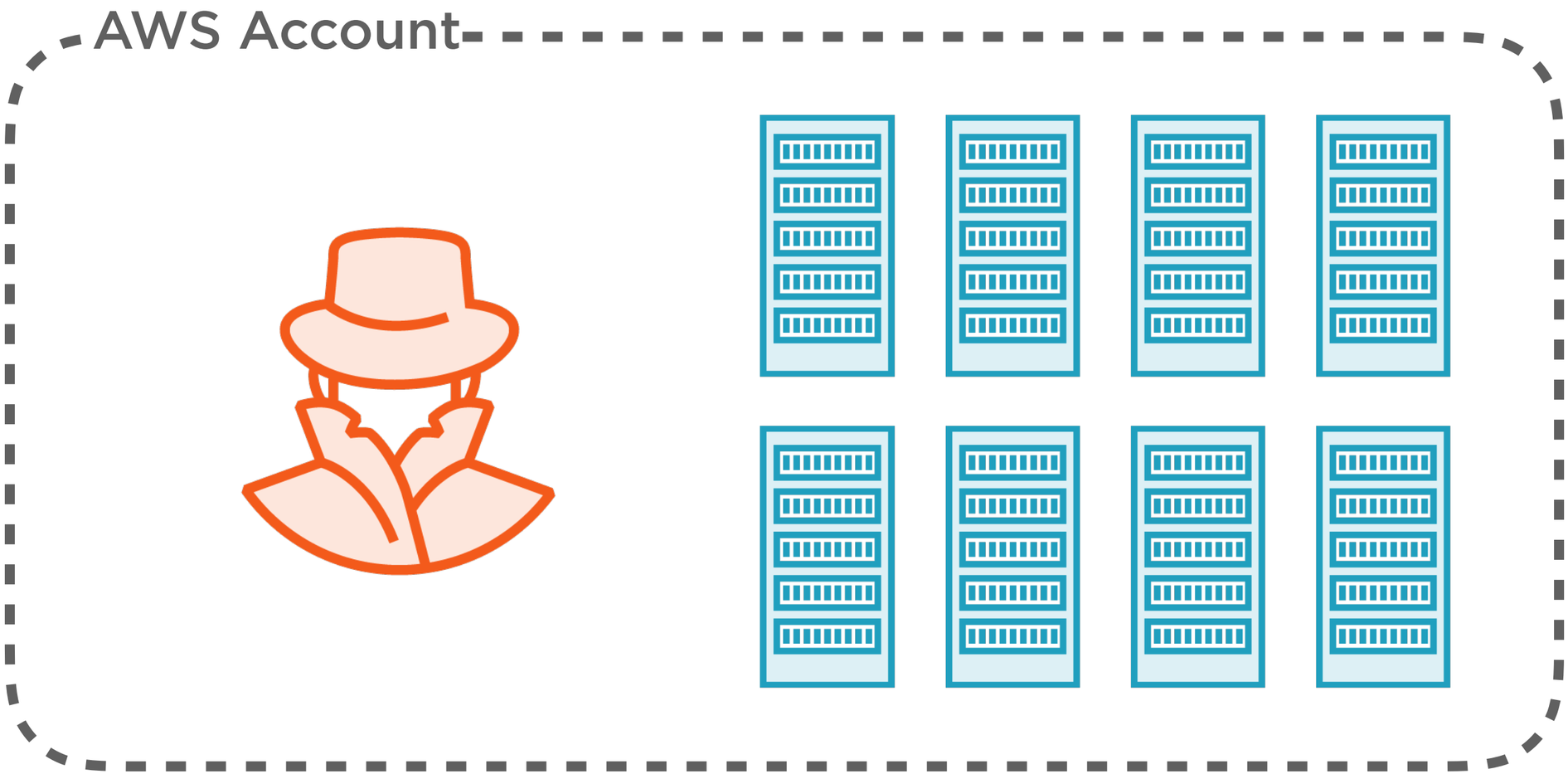
Filtering the ingresses and egresses

A VPC for every account

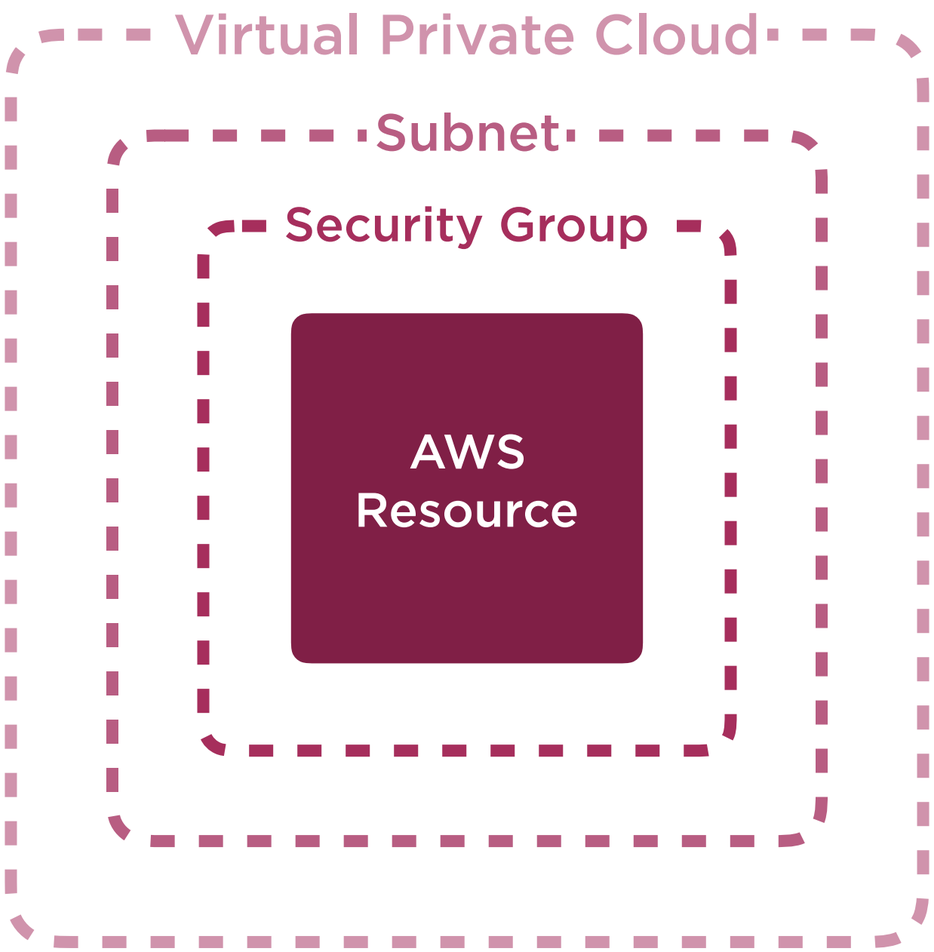
Reading VPC Flow Logs like a map

CloudTrail as Big Brother

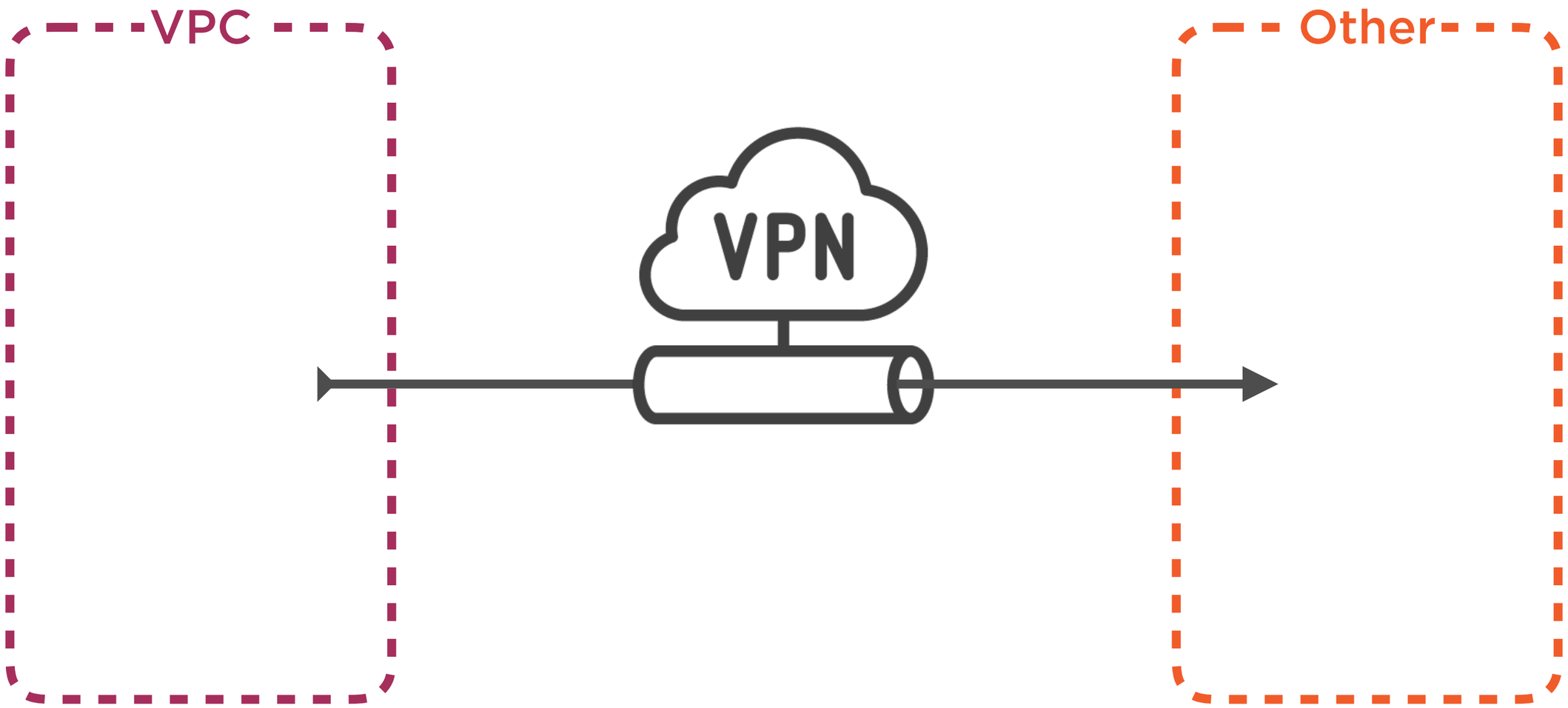
The Power of Virtual Private Cloud


AWS Account

Layered Security in AWS

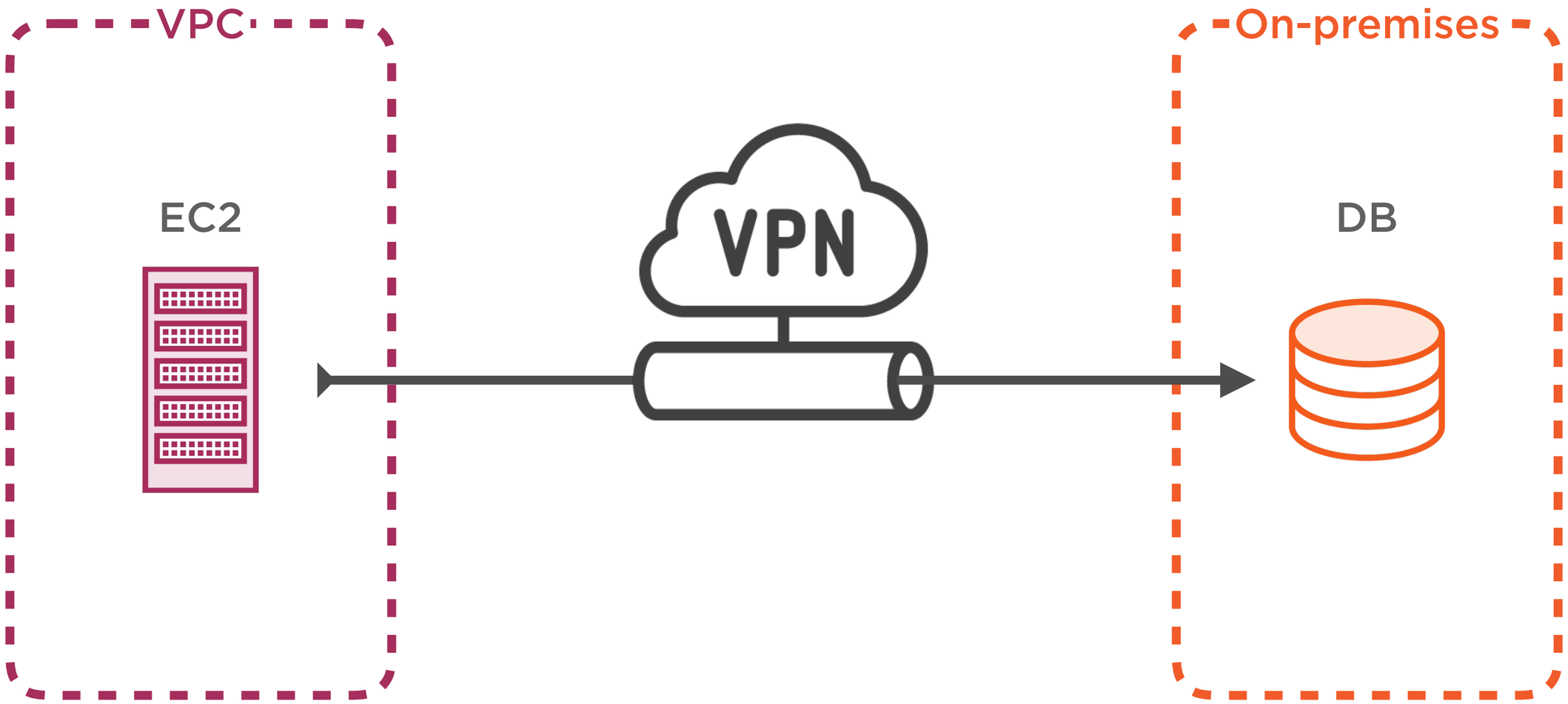


VPCs are ubiquitous across the enterprise


VPC
VPN
Other

Hybrid Cloud

Architecture design where a cloud and on-premises resources interact over a VPN connection.

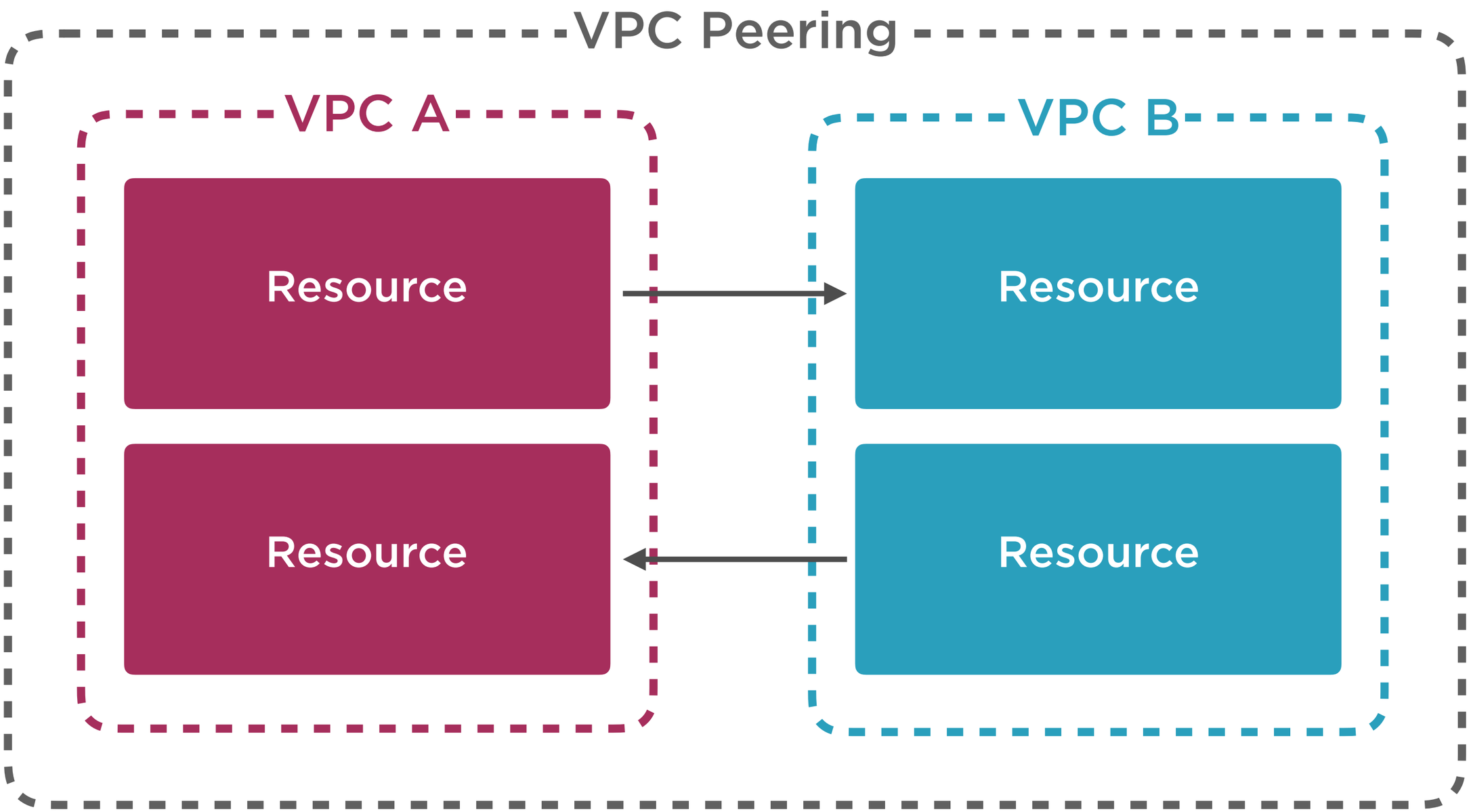

VPC
EC2
VPN
On-premises
DB

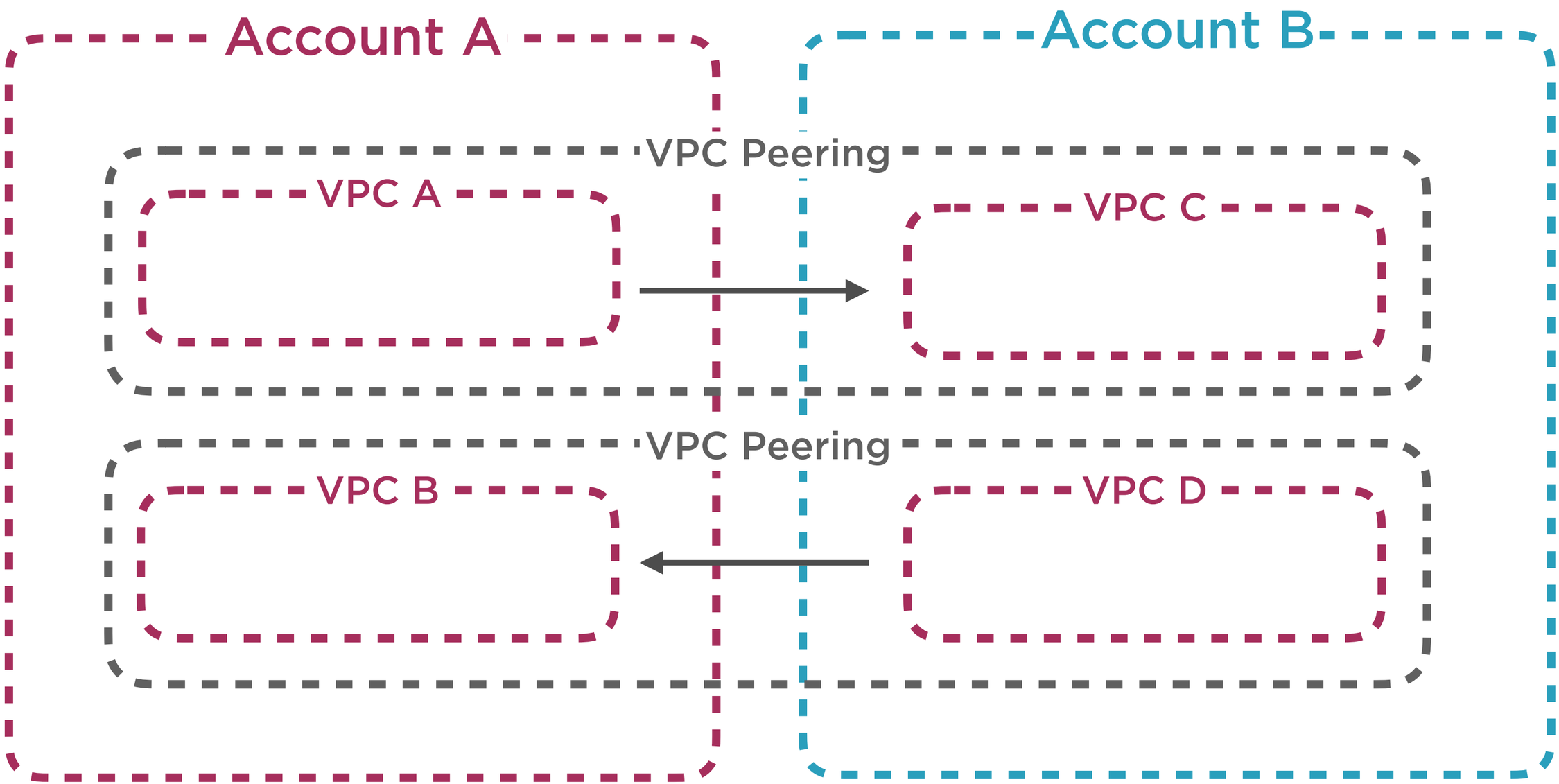
Hybrid Cloud over VPN

Faster connection speeds

No API layer to build

More secure behind firewall

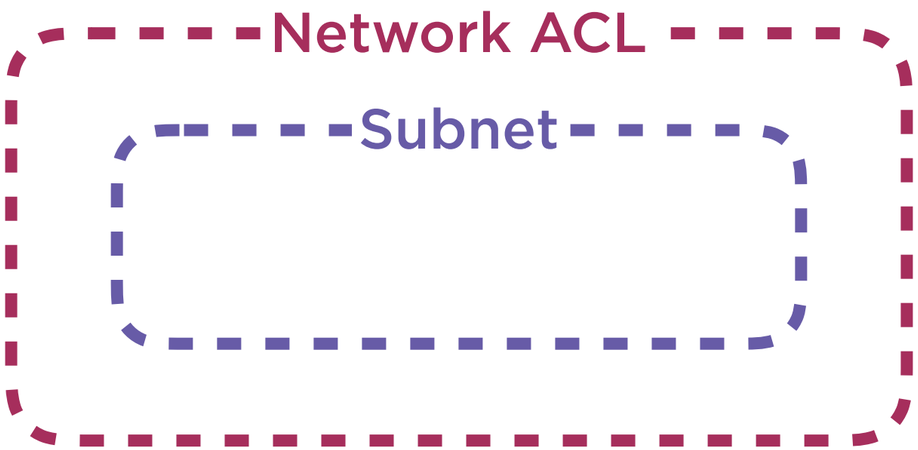

VPC Peering
VPC A
Resource
Resource
VPC B
Resource
Resource

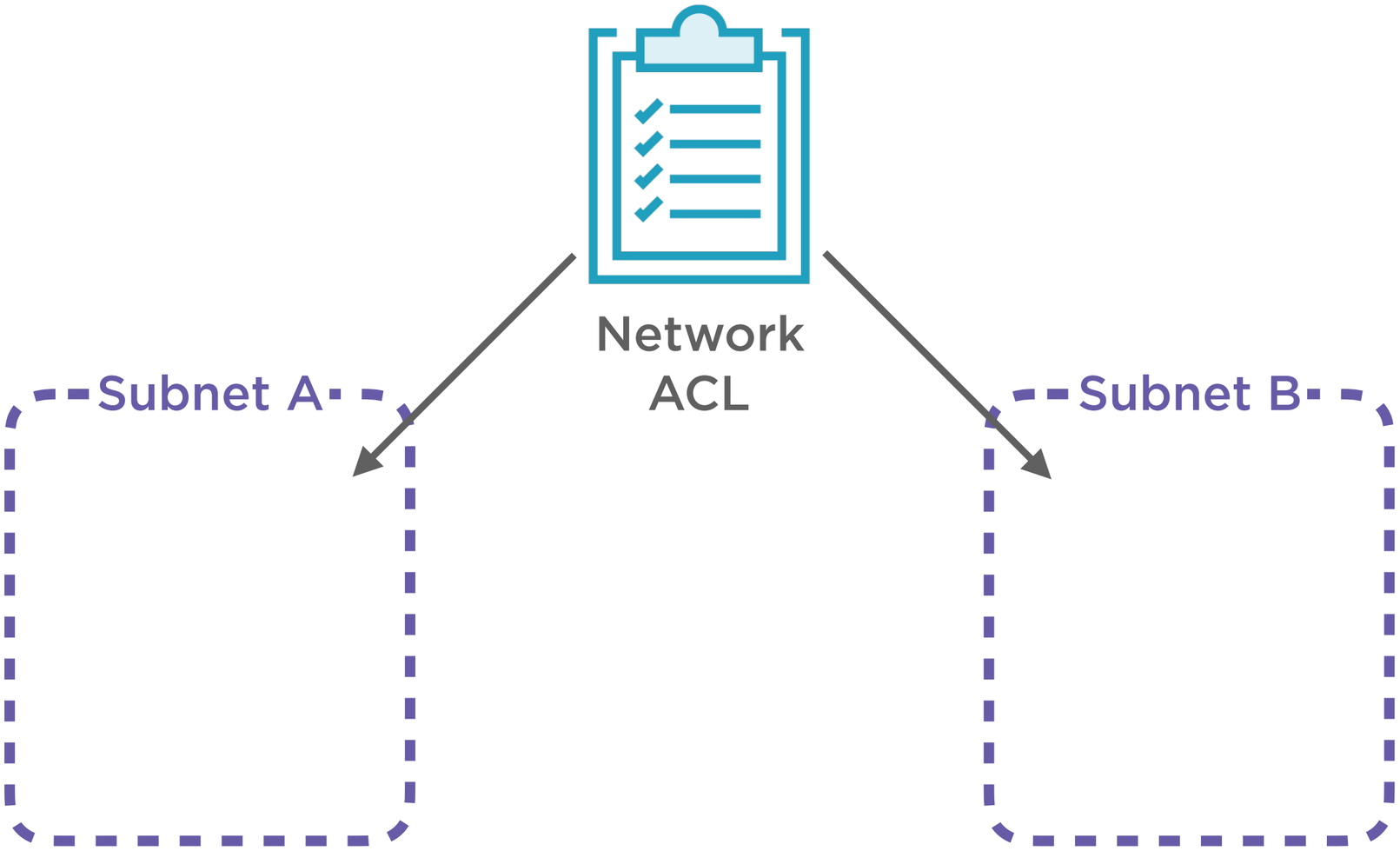

Account A
Account B
VPC Peering
VPC A
VPC C
VPC Peering
VPC B
VPC D

Ingress/Egress Filtering

Network Access Control List

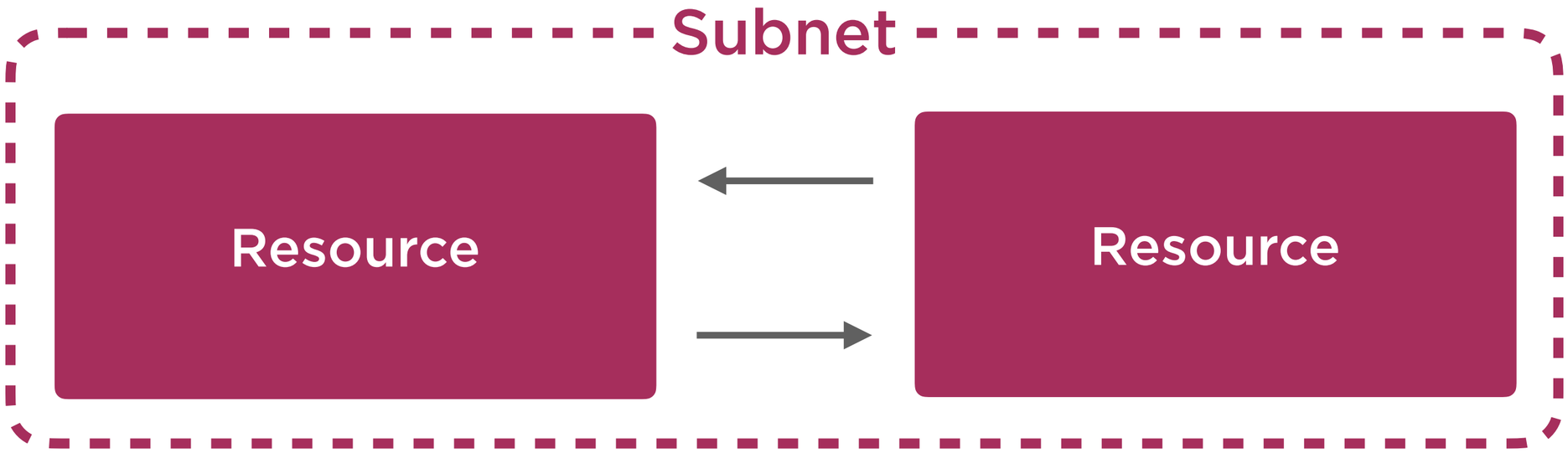
Filters traffic between subnets by IP address and port.


Network ACL
Subnet


Network
ACL
Subnet A
Subnet B

Network ACL rules have precedence over security group rules

Network ACL rules apply



Network ACL rules do not apply

Network ACL Structure

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
101	HTTPS (443)	TCP (6)	443	0.0.0.0/0	ALLOW
300	PostgreSQL (5432)	TCP (6)	5432	10.0.0.0/16	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

Rule Number

Match Criteria

Allow or Deny

Network ACLs have rules for incoming and outgoing traffic

Network ACLs are stateless, checking incoming and outgoing packets


AWS Account

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
101	HTTPS (443)	TCP (6)	443	0.0.0.0/0	ALLOW
300	PostgreSQL (5432)	TCP (6)	5432	10.0.0.0/16	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

Use outgoing Network ACL rules for egress filtering

Filter events

all 30s 5m 1h 6h 1d 1w custom

Time (UTC +00:00)	Message
2018-02-18	
04:42:44	2 180732999116 eni-da5ff2df 10.0.10.225 10.0.20.103 3000 22088 6 8 480 1518928964 1518929024 ACCEPT OK
04:42:44	2 180732999116 eni-da5ff2df 10.0.10.225 10.0.10.231 3000 41375 6 5 1974 1518928964 1518929024 ACCEPT OK
04:42:44	2 180732999116 eni-da5ff2df 5.188.87.9 10.0.10.225 46859 3489 6 1 40 1518928964 1518929024 REJECT OK
04:43:46	2 180732999116 eni-da5ff2df 5.188.11.188 10.0.10.225 54193 3509 6 1 40 1518929026 1518929084 REJECT OK
04:43:46	2 180732999116 eni-da5ff2df 77.72.82.135 10.0.10.225 53664 2473 6 1 40 1518929026 1518929084 REJECT OK
04:43:46	2 180732999116 eni-da5ff2df 10.0.20.103 10.0.10.225 22108 3000 6 3 180 1518929026 1518929084 ACCEPT OK
04:43:46	2 180732999116 eni-da5ff2df 5.188.10.10 10.0.10.225 51023 7410 6 1 40 1518929026 1518929084 REJECT OK
04:43:46	2 180732999116 eni-da5ff2df 10.0.10.225 10.0.20.103 3000 22098 6 1 60 1518929026 1518929084 ACCEPT OK
04:43:46	2 180732999116 eni-da5ff2df 5.188.10.10 10.0.10.225 51024 7410 6 1 40 1518929026 1518929084 REJECT OK
04:43:46	2 180732999116 eni-da5ff2df 185.143.223.125 10.0.10.225 45626 3406 6 1 40 1518929026 1518929084 REJECT OK
04:43:46	2 180732999116 eni-da5ff2df 10.0.10.225 10.0.20.103 3000 22108 6 8 480 1518929026 1518929084 ACCEPT OK
04:43:46	2 180732999116 eni-da5ff2df 205.209.159.124 10.0.10.225 20379 58586 6 1 52 1518929026 1518929084 REJECT OK
04:43:46	2 180732999116 eni-da5ff2df 164.52.1.46 10.0.10.225 49023 445 6 1 40 1518929026 1518929084 REJECT OK
04:43:46	2 180732999116 eni-da5ff2df 61.153.56.30 10.0.10.225 33816 22 6 1 40 1518929026 1518929084 REJECT OK
04:43:46	2 180732999116 eni-da5ff2df 14.134.100.8 10.0.10.225 31091 58586 6 1 52 1518929026 1518929084 REJECT OK
04:43:46	2 180732999116 eni-da5ff2df 104.236.145.154 10.0.10.225 49828 179 6 1 40 1518929026 1518929084 REJECT OK
04:45:04	2 180732999116 eni-da5ff2df 107.170.224.166 10.0.10.225 54143 1911 6 1 40 1518929104 1518929144 REJECT OK

Use VPC Flow Logs for auditing ingress and egress traffic

Third-party utilities can provide further filtering and security

Creating a VPC

The Bones of a VPC

VPC

Subnet x2

Route Table

Route

Internet Gateway

Internet Gateway Attachment to VPC

Subnet to Route Table Association x 2

Configuring a VPC

Principle of Least Privilege

Give a user permissions to only what they need to perform their jobs.

Ephemeral Ports

Ports on clients used to connect to servers.
Eg: Port 1786 on the client connects to port 80 on server.

Using VPC Flow Logs

VPC Flow Logs

Logs packets coming through VPC Subnets.
Aggregates packets according to a capture window.

VPC Flow Log Record Analysis

```
2 180732999 eni-da5ff2df 10.0.20.103 10.0.10.145 3000 21780 6 8 480 1518928248 151892934 ACCEPT OK
```

Use Flow Logs for analyzing traffic to your VPC and auditing access

Using CloudTrail in Your AWS Account

CloudTrail Trail

Monitor management and data events

Exports logs to S3 bucket

Can be consumed by log analysis tool

Use CloudTrail to monitor and audit the actions occurring in your account

Encrypting Data at Rest in AWS

Data at Rest

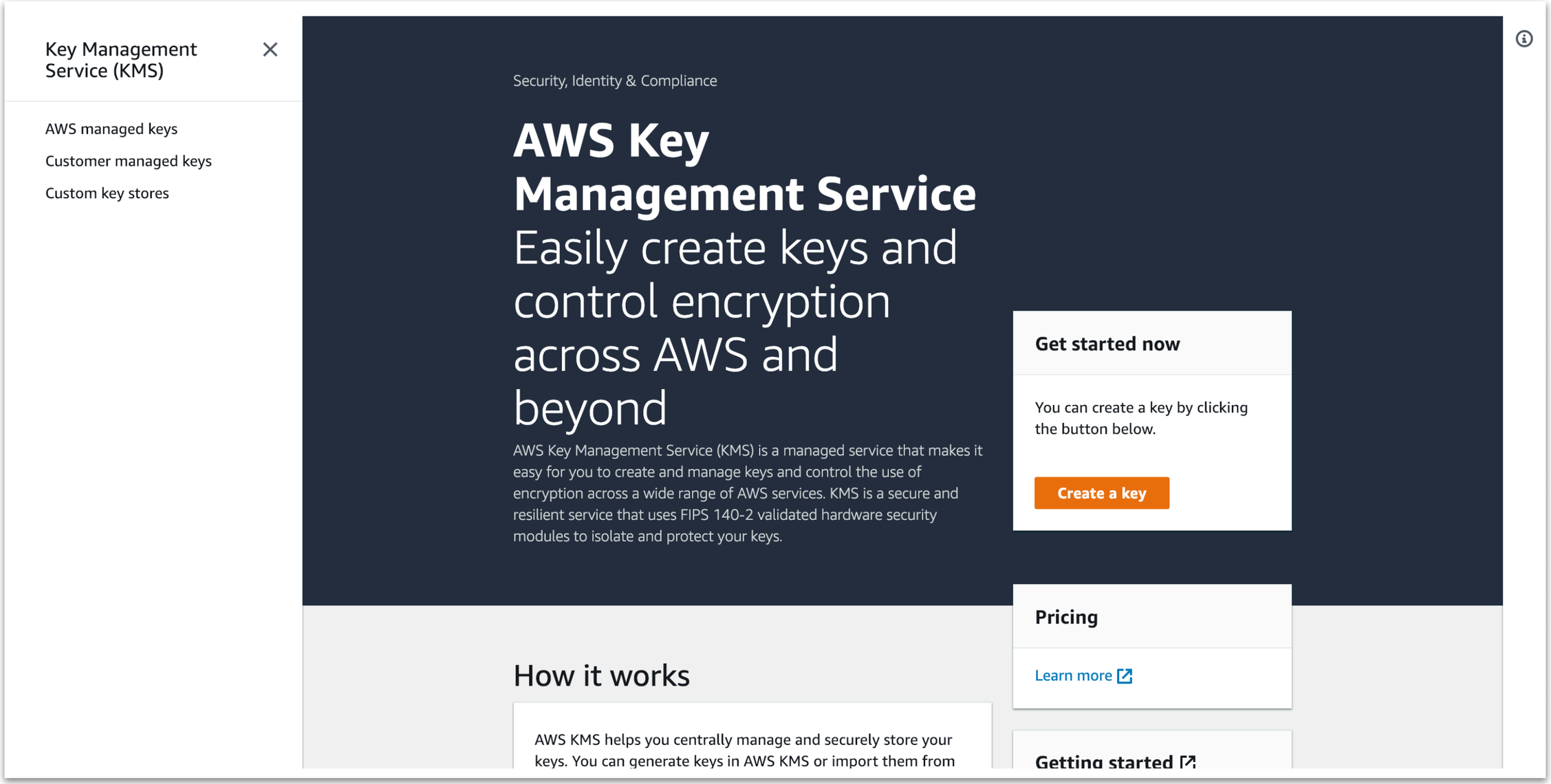
Data in Transit

Encrypting Data in Transit

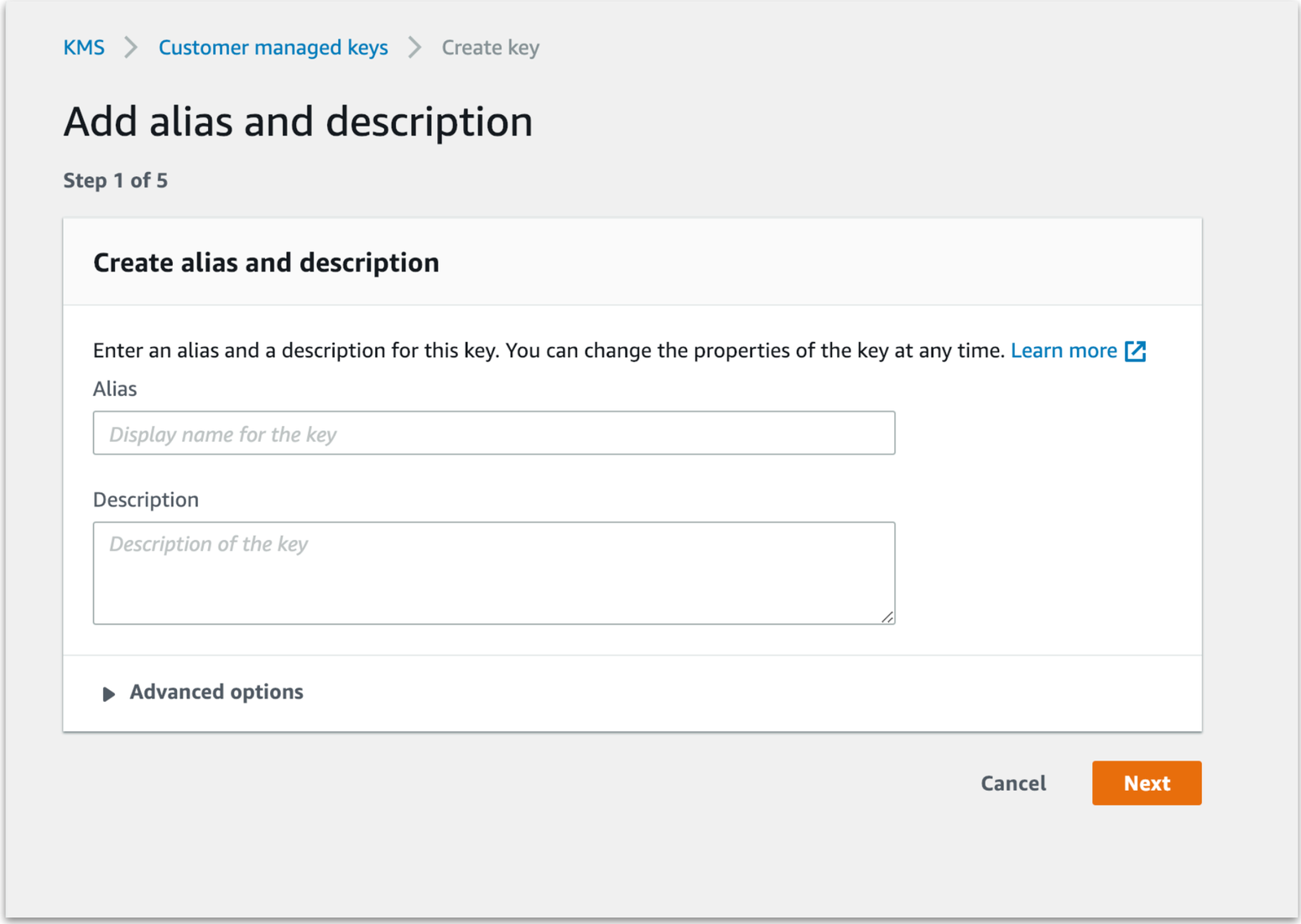
Use HTTPS connections to encrypt with SSL

Encrypt data before sending to AWS

AWS Key Management Service (KMS)



Creating a Key in KMS



AWS Services with Encryption

DynamoDB

RDS

S3

EBS

DynamoDB Default Table Configuration

Table settings

Default settings provide the fastest way to get started with your table. You can modify these default settings now or after your table has been created.

☑ **Use default settings**

- No secondary indexes.
- Provisioned capacity set to 5 reads and 5 writes.
- Basic alarms with 80% upper threshold using SNS topic "dynamodb".
- Encryption at Rest with DEFAULT encryption type **NEW!**

DynamoDB Encryption Options

Encryption At Rest

Select Encryption settings for your DynamoDB table to help protect data at rest. Learn more

- (●) **DEFAULT**

  Server-side encryption using AWS owned CMK (Customer Master Key)

- ( ) **KMS**

  Server-side encryption using AWS managed CMK (Customer Master Key)

RDS Encryption Options

Encryption

Encryption

- (●) Enable encryption Learn more
  Select to encrypt the given instance. Master key ids and aliases appear in the list after they have been created using the Key Management Service(KMS) console.
- ( ) Disable encryption

Master key Info

(default) aws/rds

Account

180732999116

KMS key ID

e0dfd092-657e-49ec-8813-9c6abe45818a

S3 Bucket Encryption Options

Default encryption

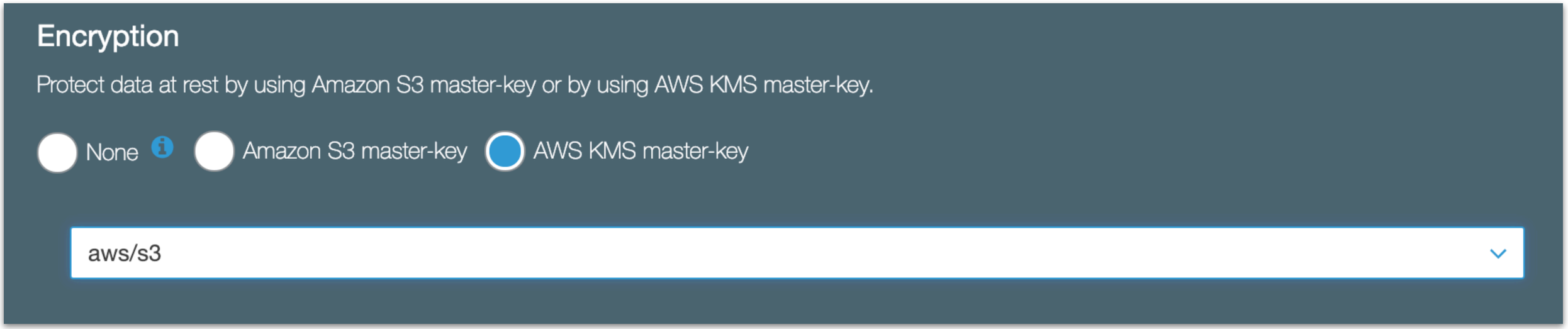
☑ Automatically encrypt objects when they are stored in S3. Learn more

○ AES-256
Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)

◉ AWS-KMS
Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

aws/s3

S3 Object Encryption Options



EBS Encryption Options

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	/dev/xvda	snap-05c184ed39d0ecd7b	8	General Purpose SSD (gp2)	100 / 3000	N/A	☑	Not Encrypted
EBS	/dev/sdb	Search (case-insensit	8	General Purpose SSD (gp2)	100 / 3000	N/A	☐	88411d00-0

Add New Volume

KMS Pricing

Customer Managed Key	$1 per month
Encrypt/Decrypt Request	$0.03/10,000 calls

First 20,000 calls per month is free

S3 Encryption Pricing Example

1 Customer Managed Key

10,000 Encrypt Requests (1 request x 10,000 objects)

2,000,000 Decrypt requests to access the objects

$1 - 1 Customer Managed Key

$5.97 - 1,990,000 requests x $0.03 / 10,000 requests

(2,010,000 requests - 20,000 free requests)

Total $6.97 / month

Conclusion

VPC and CloudTrail

The keys to securing your AWS account

Summary

VPN connecting with your peers

Filter everything with Network ACLs

CloudFormation will never die

VPC Flow Logs tell all

CloudTrail: The hardest resource to set up

Up Next

Resource Permissions

with IAM