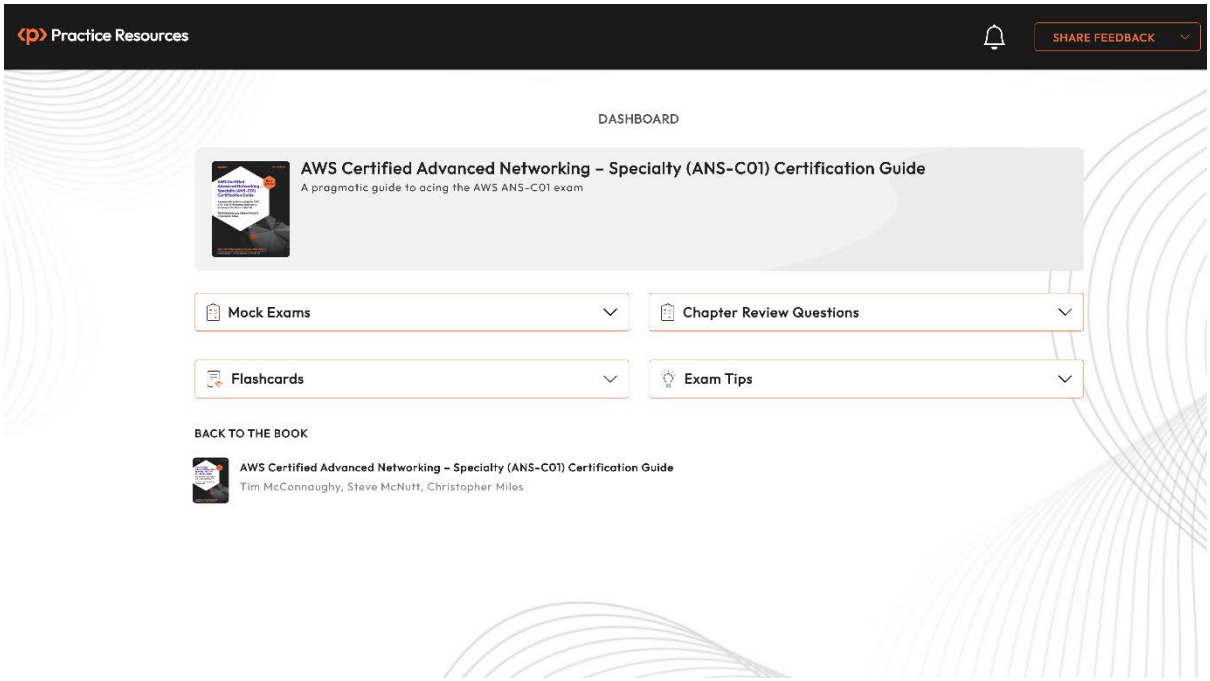
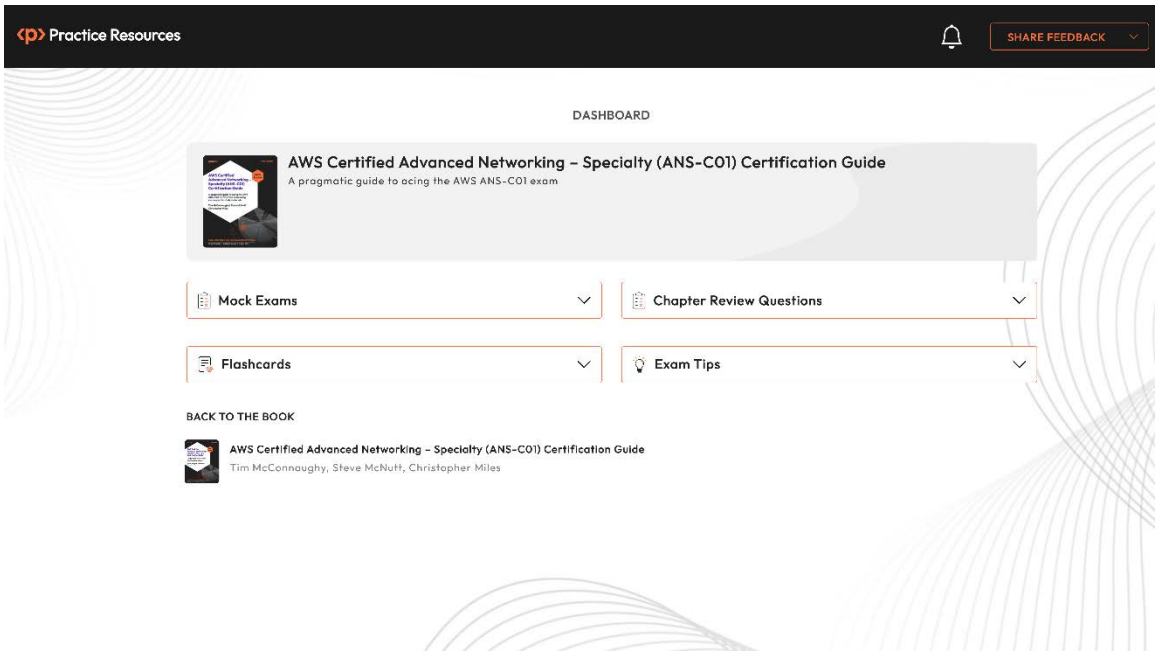
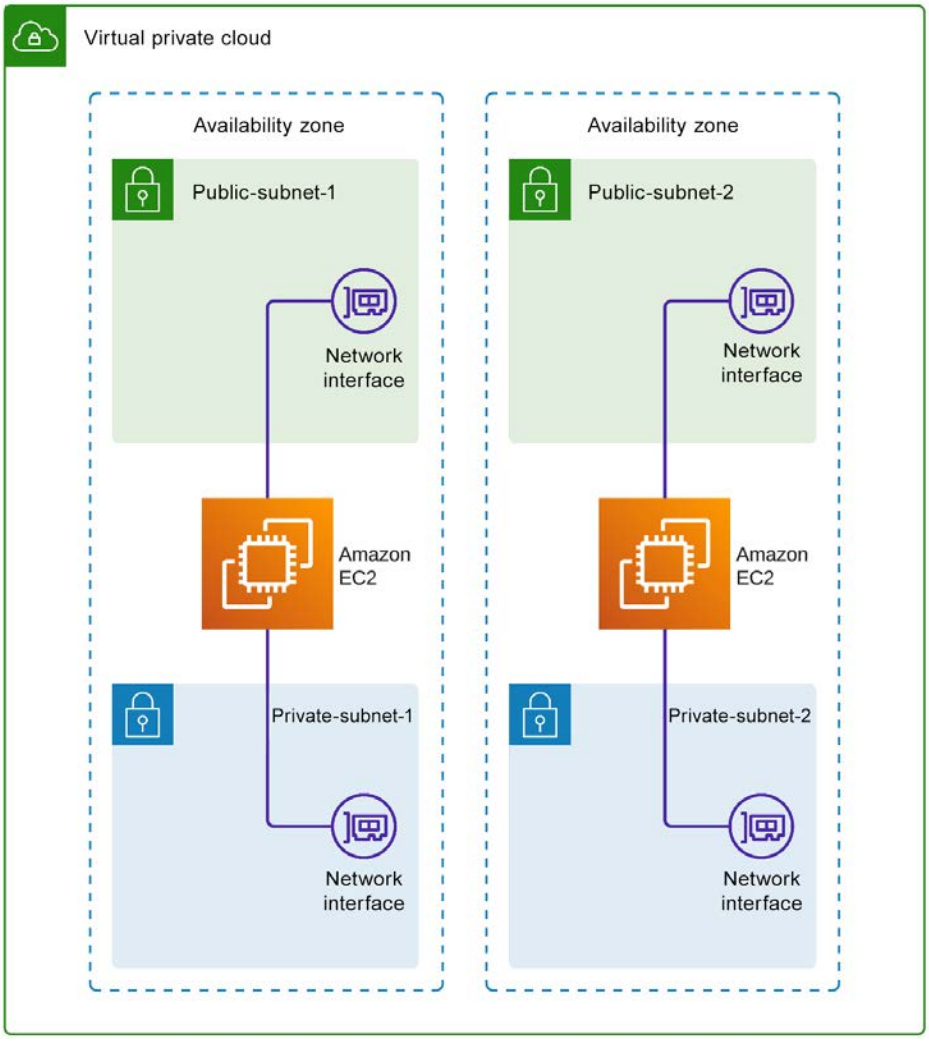
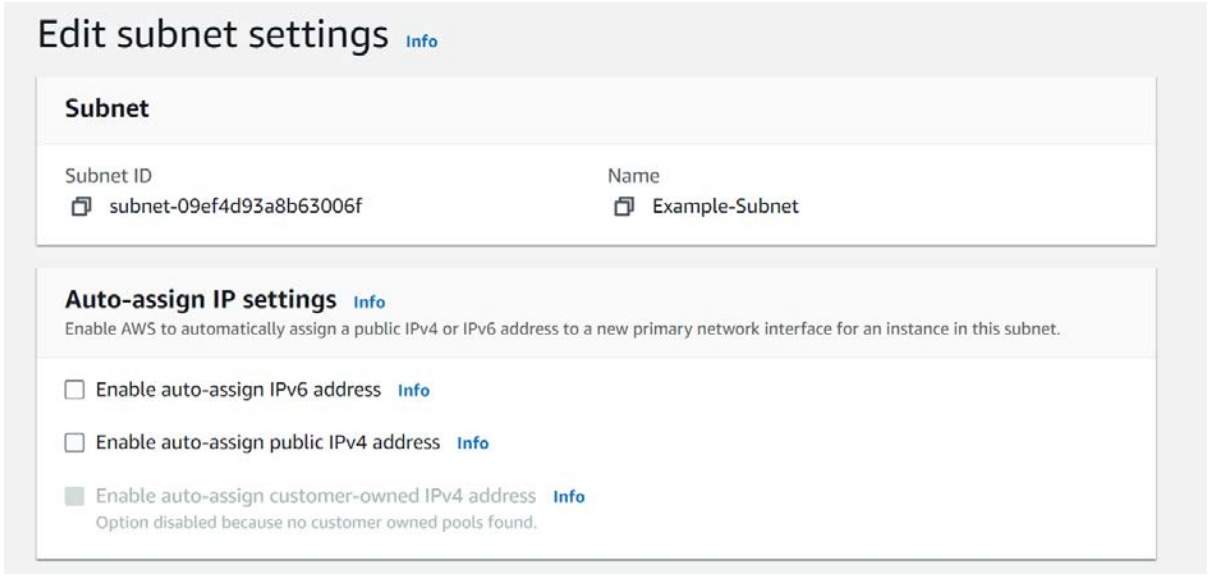
Preface:

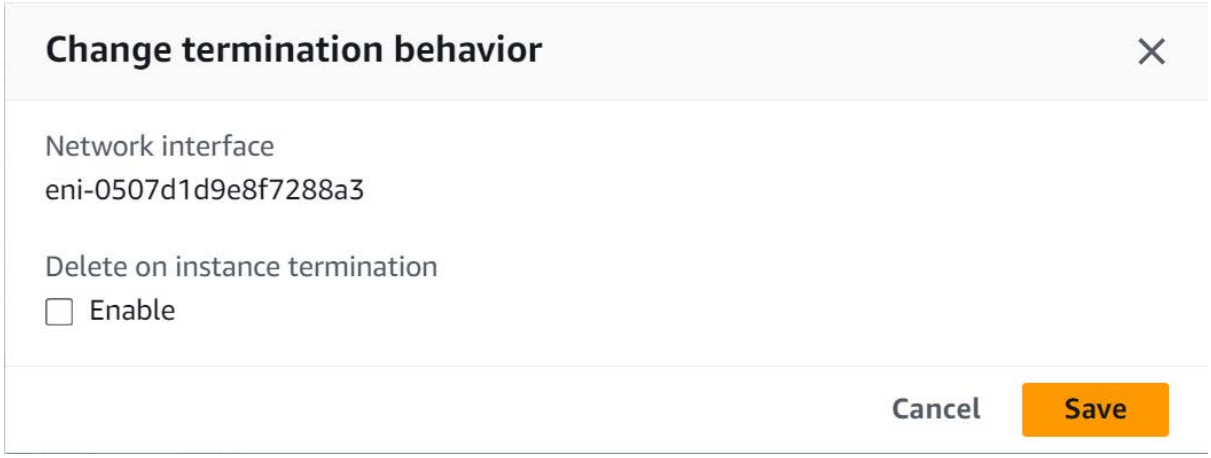

Practice Resources
SHARE FEEDBACK
DASHBOARD
AWS Certified Advanced Networking – Specialty (ANS-C01) Certification Guide
A pragmatic guide to acing the AWS ANS-C01 exam
Mock Exams
Chapter Review Questions
Flashcards
Exam Tips
BACK TO THE BOOK
AWS Certified Advanced Networking – Specialty (ANS-C01) Certification Guide
Tim McConnaughy, Steve McNutt, Christopher Miles

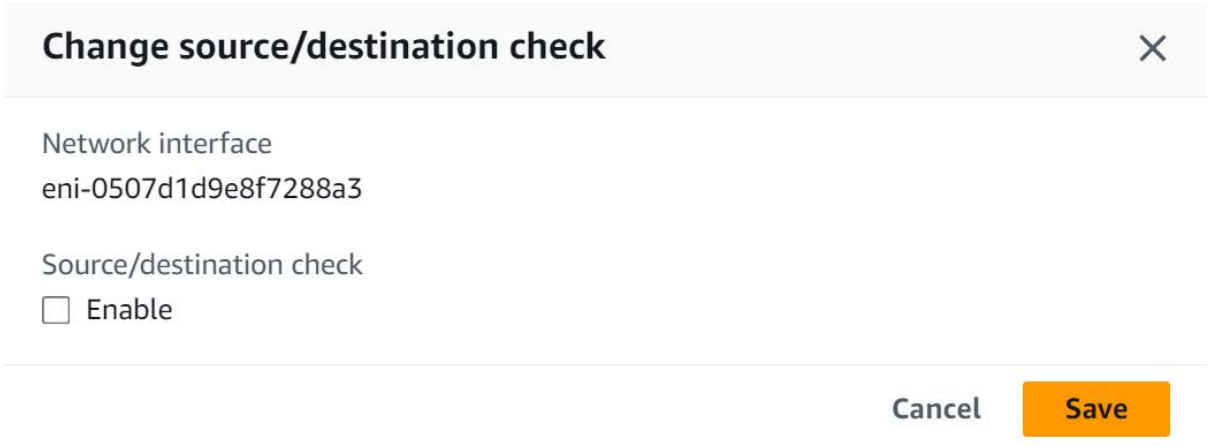
Chapter 1: Advanced VPC Networking






Edit subnet settings Info
Subnet
Subnet ID
subnet-09ef4d93a8b63006f
Name
Example-Subnet
Auto-assign IP settings Info
Enable AWS to automatically assign a public IPv4 or IPv6 address to a new primary network interface for an instance in this subnet.
Enable auto-assign IPv6 address Info
Enable auto-assign public IPv4 address Info
Enable auto-assign customer-owned IPv4 address Info
Option disabled because no customer owned pools found.


Change termination behavior
Network interface
eni-0507d1d9e8f7288a3
Delete on instance termination
Enable
Cancel
Save


Change source/destination check
Network interface
eni-0507d1d9e8f7288a3
Source/destination check
Enable
Cancel
Save

EC2 > Network interfaces > Create network interface

Create network interface

An elastic network interface is a logical networking component in a VPC that represents a virtual network card.

Details Info

Description - *optional*
A descriptive name for the network interface.

Description of your network interface

Subnet
The subnet in which to create the network interface.

Select subnet

Private IPv4 address
The private IPv4 address to assign to the network interface.

- (•) Auto-assign
- ( ) Custom

Elastic Fabric Adapter

- [ ] Enable

▼ Advanced settings

You can optionally set the IP prefix delegation

IPv4 prefix delegation
The IPv4 prefixes to assign to the network interface.

- (•) Do not assign
- ( ) Auto-assign
- ( ) Custom

Idle connection tracking timeout Info
Specifies the idle timeout duration in seconds.

TCP established timeout
432000

UDP stream timeout
180

UDP timeout
30

Tags - *optional*

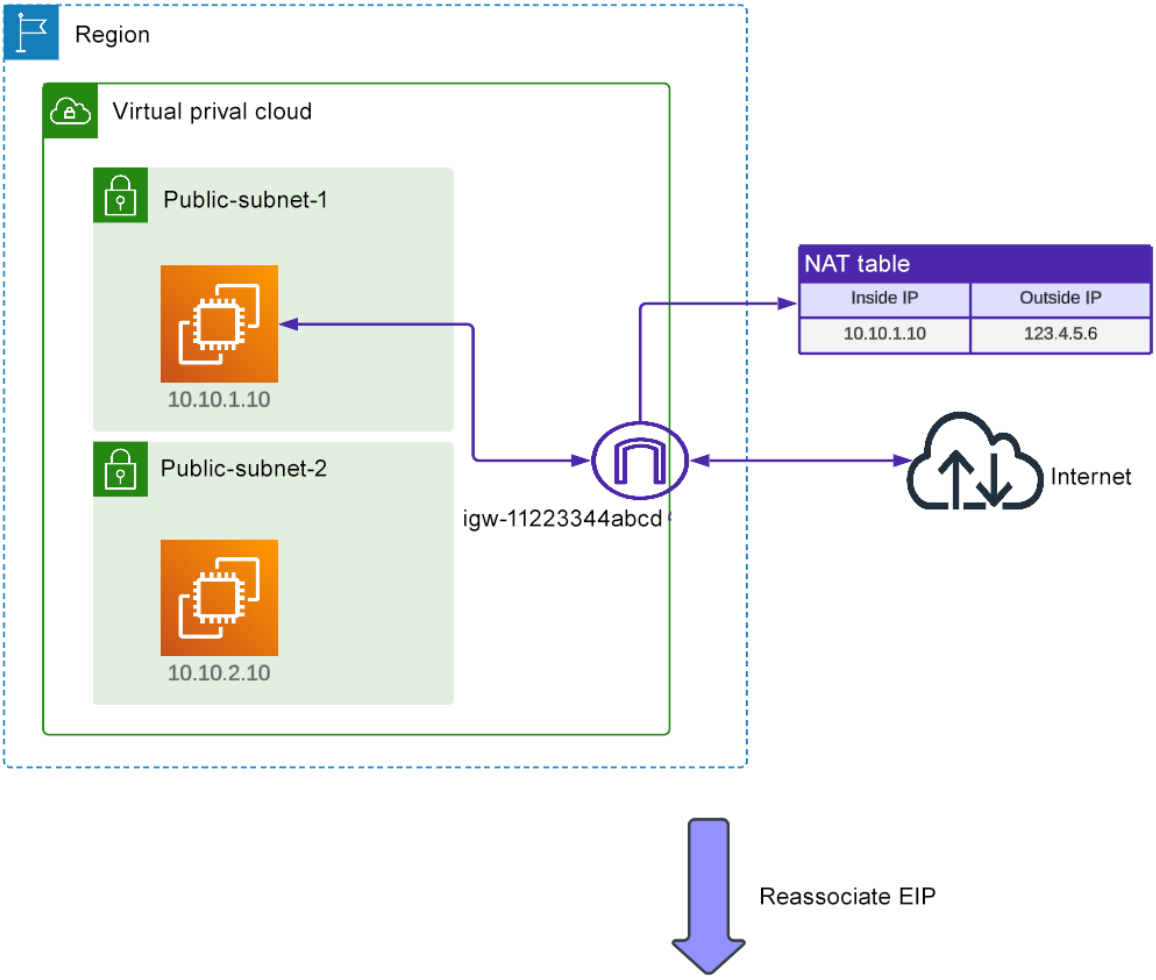
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

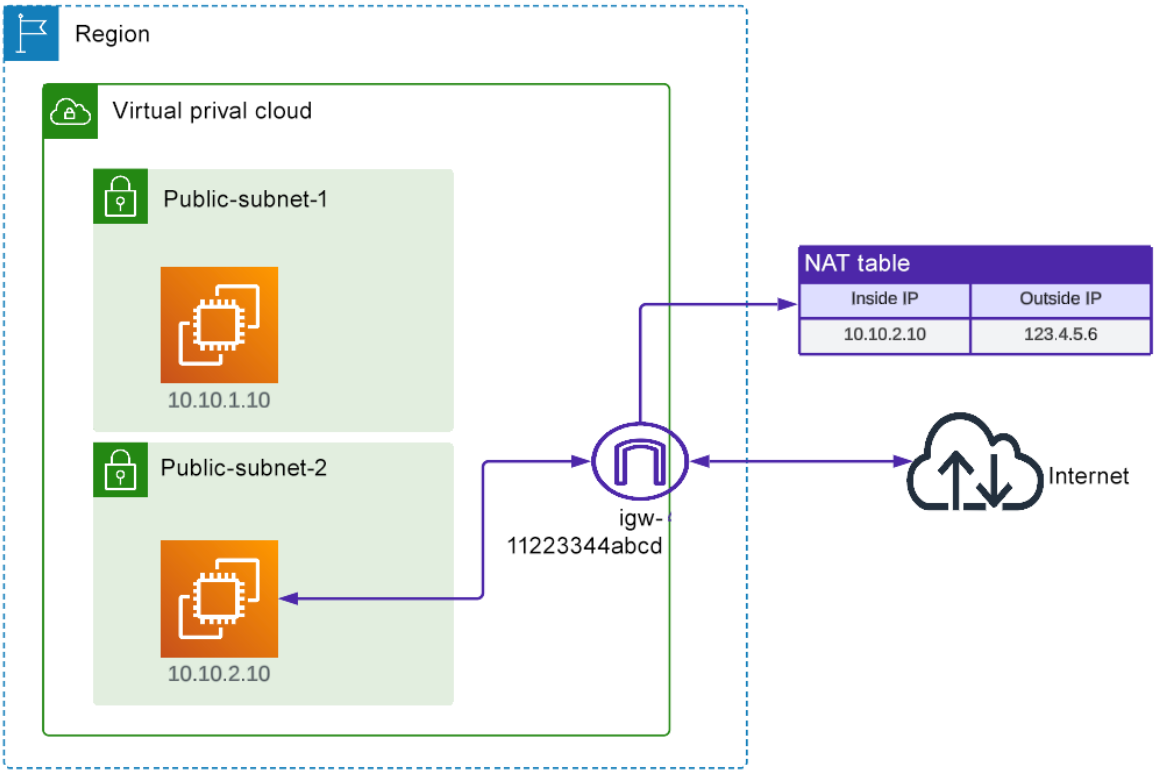
Add new tag

You can add 50 more tags

Cancel | Create network interface


Region
Virtual prival cloud
Public-subnet-1
10.10.1.10
Public-subnet-2
10.10.2.10
igw-11223344abcd
NAT table
Inside IP
Outside IP
10.10.1.10
123.4.5.6
Internet

Reassociate EIP


Region
Virtual prival cloud
Public-subnet-1
10.10.1.10
Public-subnet-2
10.10.2.10
igw-
11223344abcd
NAT table
Inside IP
Outside IP
10.10.2.10
123.4.5.6
Internet

EC2 > Elastic IP addresses > Allocate Elastic IP address

Allocate Elastic IP address Info

Elastic IP address settings Info

Public IPv4 address pool

- (•) Amazon's pool of IPv4 addresses
- ( ) Public IPv4 address that you bring to your AWS account with BYOIP. (option disabled because no pools found) Learn more
- ( ) Customer-owned pool of IPv4 addresses created from your on-premises network for use with an Outpost. (option disabled because no customer owned pools found) Learn more

Network border group Info

ap-southeast-2

Global static IP addresses

AWS Global Accelerator can provide global static IP addresses that are announced worldwide using anycast from AWS edge locations. This can help improve the availability and latency for your user traffic by using the Amazon global network. Learn more

Create accelerator

Tags - *optional*

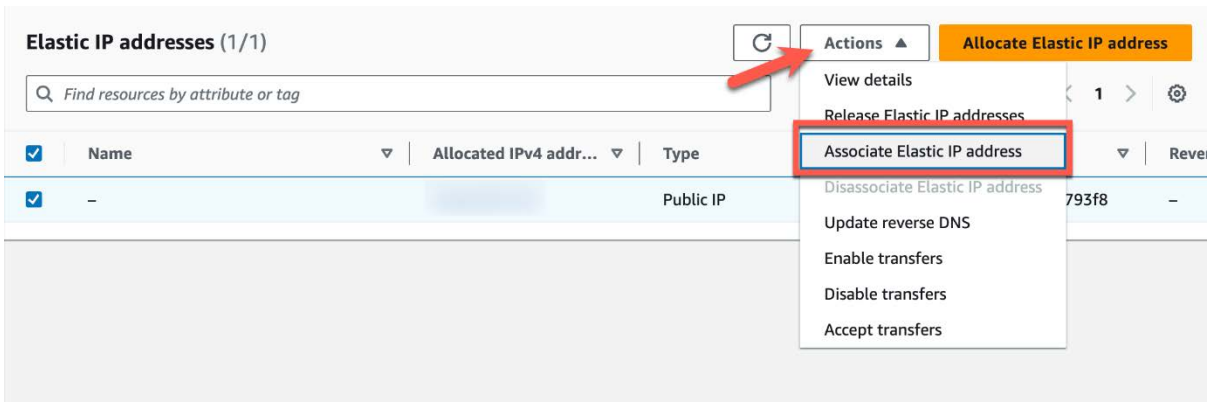
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

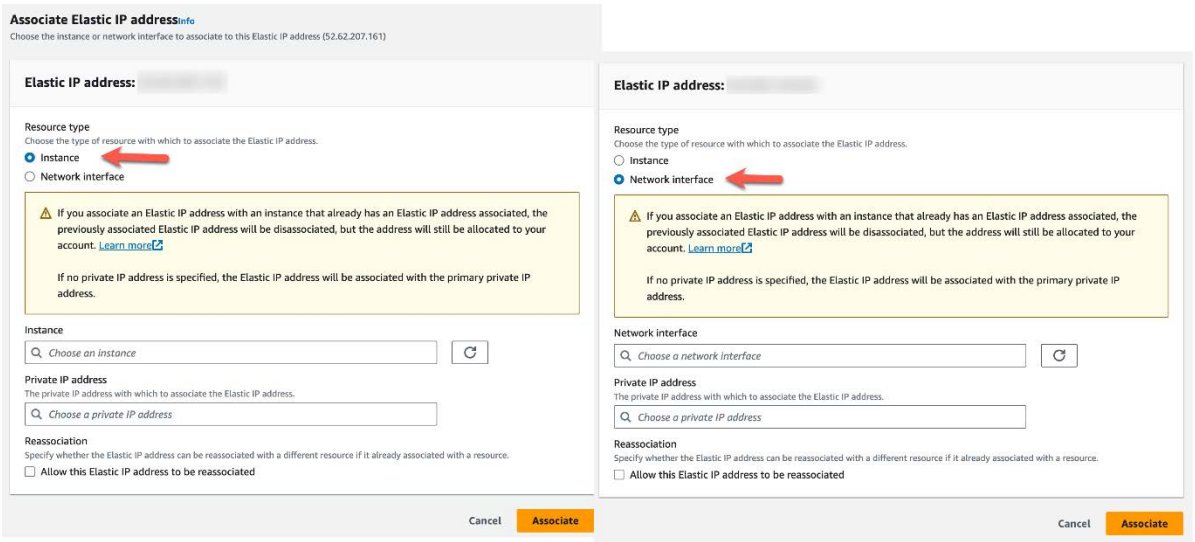
No tags associated with the resource.

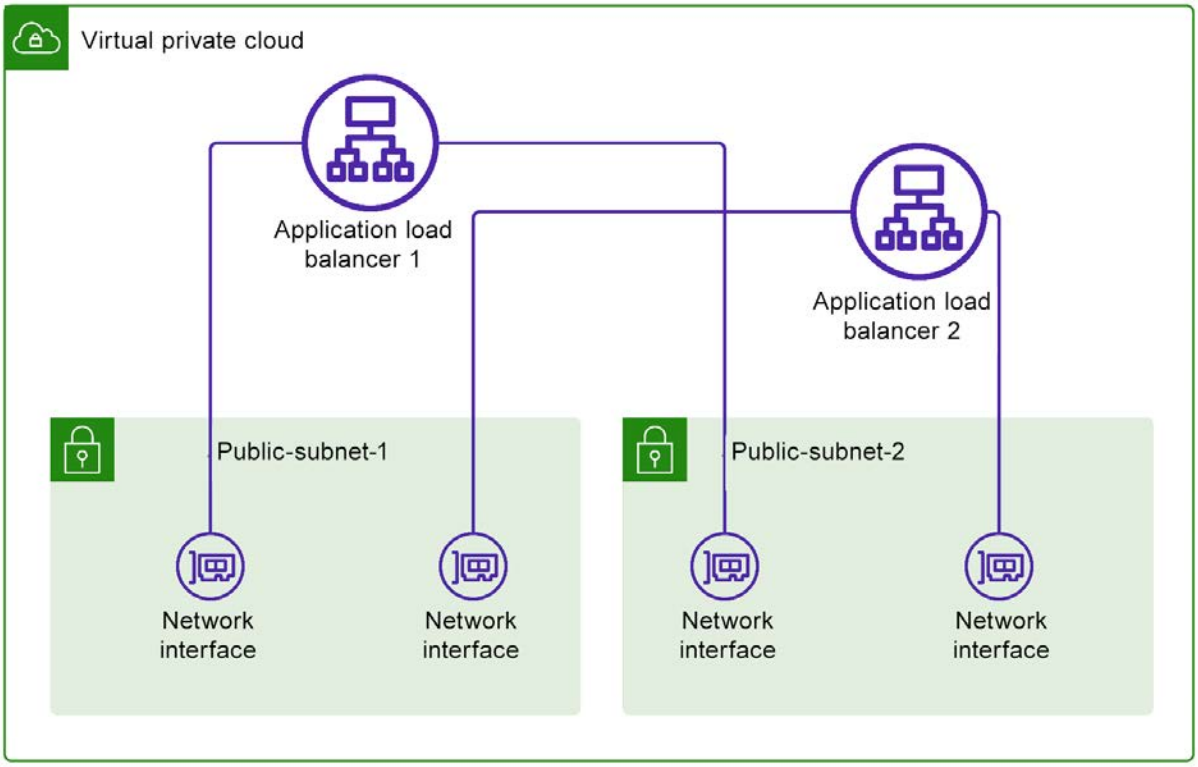
Add new tag

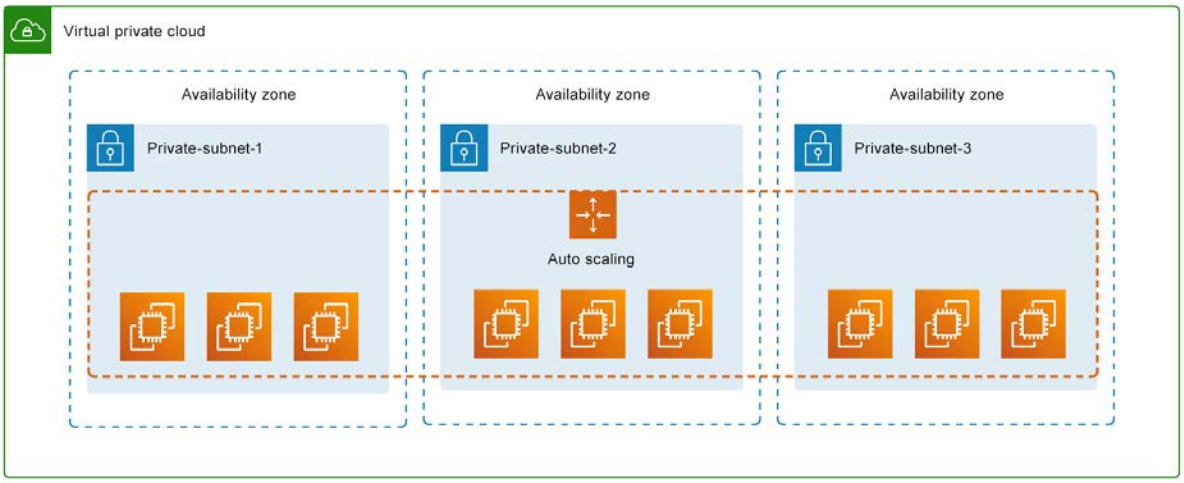
You can add up to 50 more tag

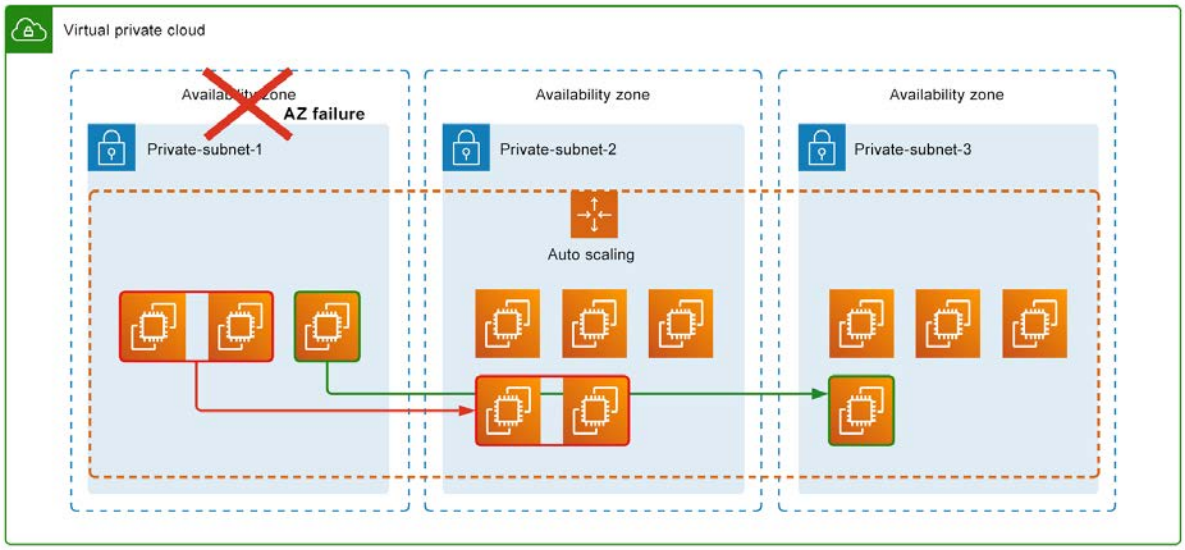
Cancel Allocate

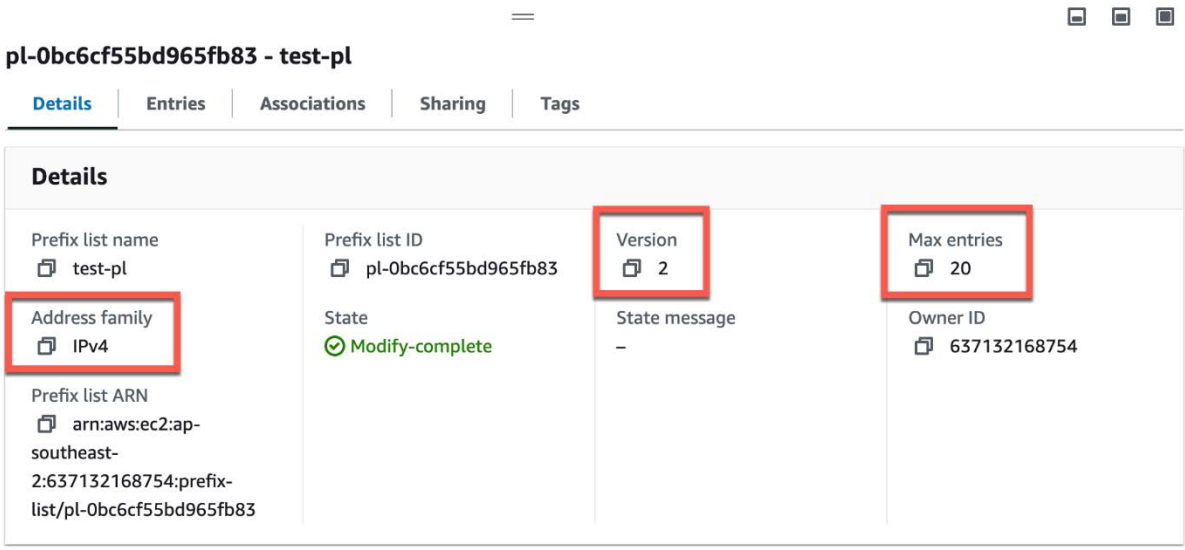


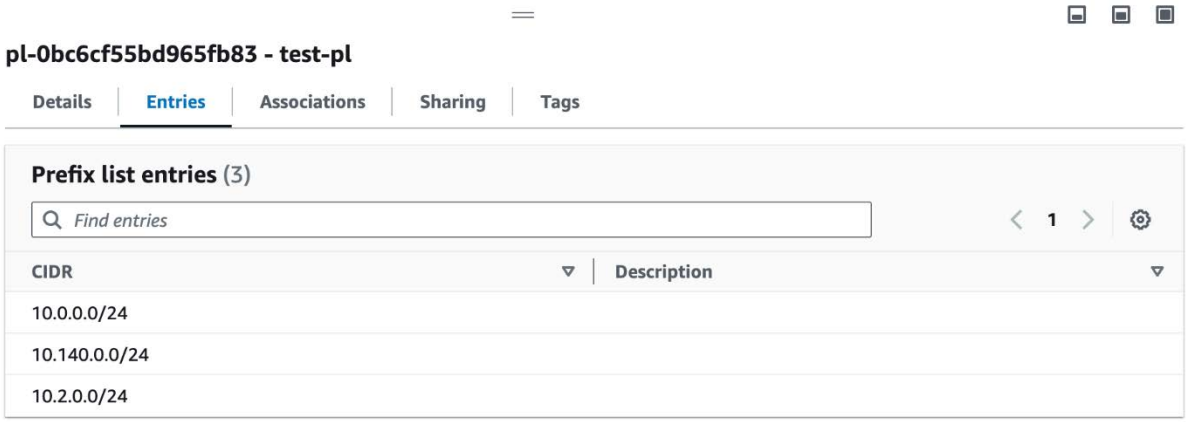

Associate Elastic IP address Info
Choose the instance or network interface to associate to this Elastic IP address (52.62.207.161)
Elastic IP address:
Resource type
Choose the type of resource with which to associate the Elastic IP address.
Instance
Network interface
If you associate an Elastic IP address with an instance that already has an Elastic IP address associated, the previously associated Elastic IP address will be disassociated, but the address will still be allocated to your account. Learn more
If no private IP address is specified, the Elastic IP address will be associated with the primary private IP address.
Instance
Choose an instance
Private IP address
The private IP address with which to associate the Elastic IP address.
Choose a private IP address
Reassociation
Specify whether the Elastic IP address can be reassociated with a different resource if it already associated with a resource.
Allow this Elastic IP address to be reassociated
Cancel
Associate
Elastic IP address:
Resource type
Choose the type of resource with which to associate the Elastic IP address.
Instance
Network interface
If you associate an Elastic IP address with an instance that already has an Elastic IP address associated, the previously associated Elastic IP address will be disassociated, but the address will still be allocated to your account. Learn more
If no private IP address is specified, the Elastic IP address will be associated with the primary private IP address.
Network interface
Choose a network interface
Private IP address
The private IP address with which to associate the Elastic IP address.
Choose a private IP address
Reassociation
Specify whether the Elastic IP address can be reassociated with a different resource if it already associated with a resource.
Allow this Elastic IP address to be reassociated
Cancel
Associate


Virtual private cloud
Application load balancer 1
Application load balancer 2
Public-subnet-1
Public-subnet-2
Network interface
Network interface
Network interface
Network interface


Virtual private cloud
Availability zone
Private-subnet-1
Availability zone
Private-subnet-2
Auto scaling
Availability zone
Private-subnet-3


Virtual private cloud
AZ failure
Private-subnet-1
Availability zone
Private-subnet-2
Auto scaling
Availability zone
Private-subnet-3


pl-0bc6cf55bd965fb83 - test-pl
Details
Entries
Associations
Sharing
Tags
Details
Prefix list name
test-pl
Prefix list ID
pl-0bc6cf55bd965fb83
Version
2
Max entries
20
Address family
IPv4
State
Modify-complete
State message
–
Owner ID
637132168754
Prefix list ARN
arn:aws:ec2:ap-southeast-2:637132168754:prefix-list/pl-0bc6cf55bd965fb83


pl-0bc6cf55bd965fb83 - test-pl
Details
Entries
Associations
Sharing
Tags
Prefix list entries (3)
Find entries
1
CIDR
Description
10.0.0.0/24
10.140.0.0/24
10.2.0.0/24

VPC > Managed prefix lists > Create prefix list

Create prefix list Info

Create a prefix list to easily refer to CIDR blocks.

Prefix list name Info

Name of your prefix list

Max entries Info

Max number of entries for this prefix list

Address family Info

Address family cannot be changed after the prefix list is created.

- (•) IPv4
- ( ) IPv6

Prefix list entries Info

Each entry consists of a CIDR block and, optionally, a description for the CIDR block.

Specify Max entries above, then choose Add new entry to add a prefix list entry.

Add new entry

Tags - *optional*

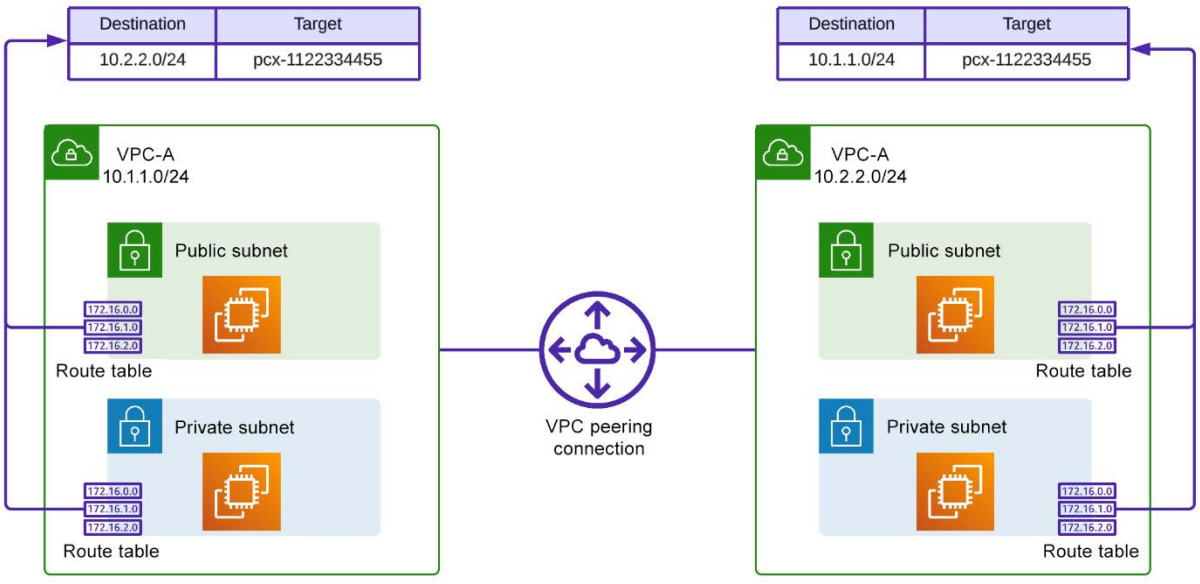
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

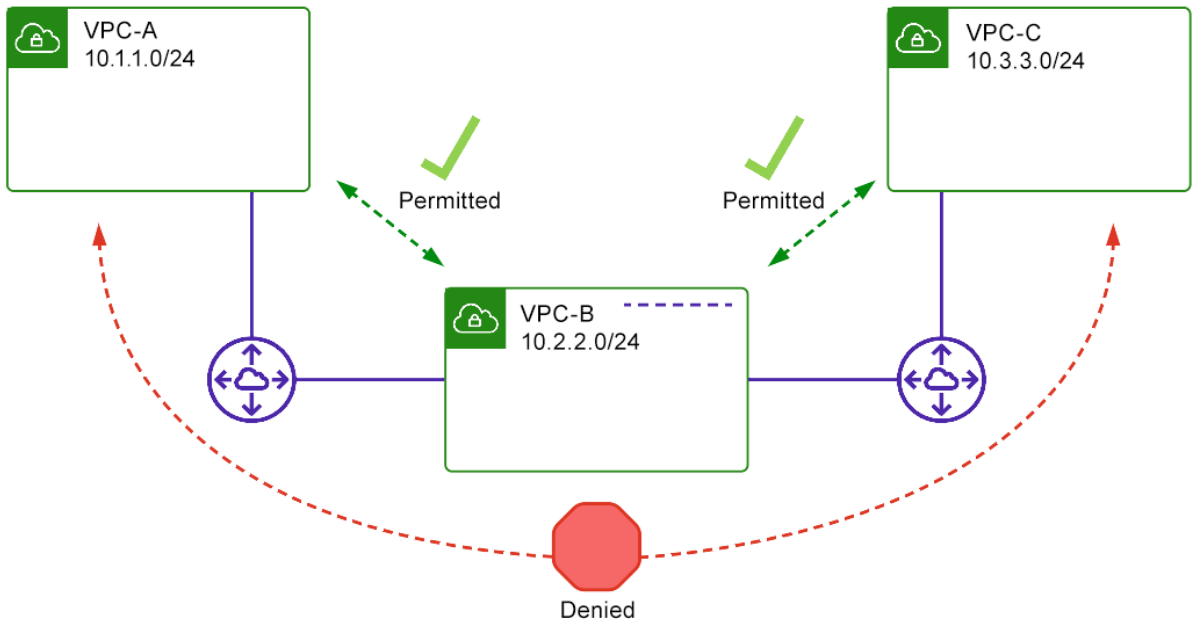
No tags associated with the resource.

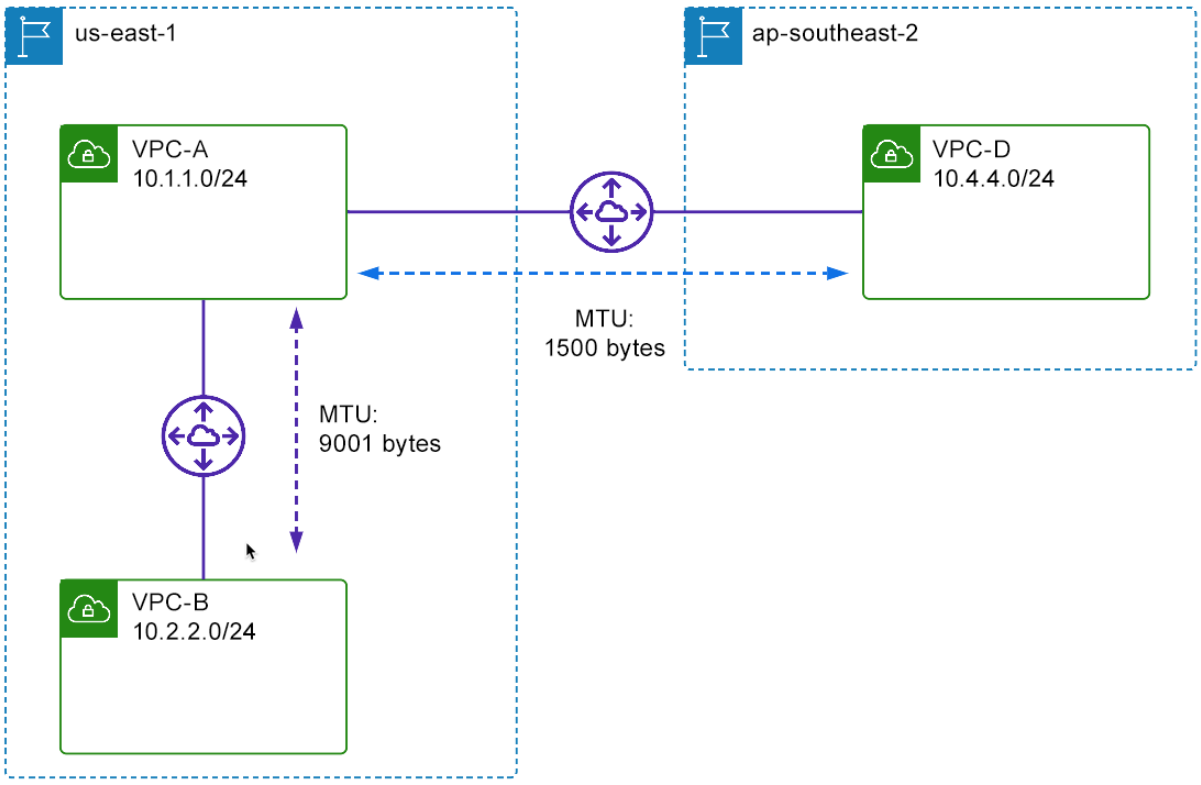
Add new tag

You can add 50 more tags.

Cancel | Create prefix list




VPC-A
10.1.1.0/24
VPC-C
10.3.3.0/24
Permitted
Permitted
VPC-B
10.2.2.0/24
Denied


us-east-1
ap-southeast-2
VPC-A
10.1.1.0/24
VPC-D
10.4.4.0/24
MTU:
1500 bytes
MTU:
9001 bytes
VPC-B
10.2.2.0/24

VPC > Peering connections > Create peering connection

Create peering connection

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately.

Info

Peering connection settings

Name - *optional*

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

my-pc-01

Select a local VPC to peer with

VPC ID (Requester)

Select a VPC

Select another VPC to peer with

Account

- (•) My account
- ( ) Another account

Region

- (•) This Region (ap-southeast-2)
- ( ) Another Region

VPC ID (Accepter)

Select a VPC

Tags

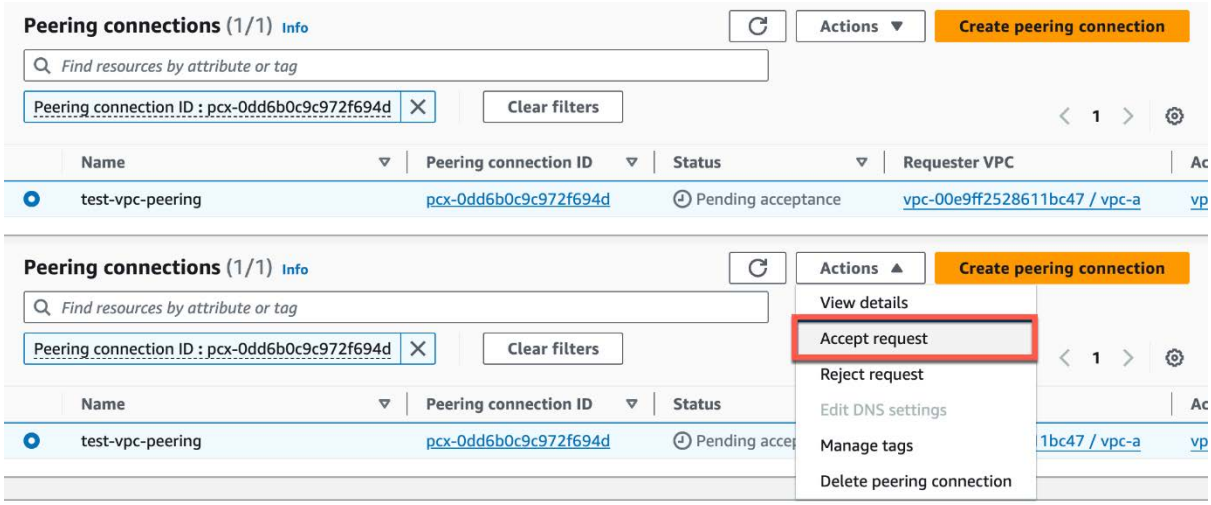
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

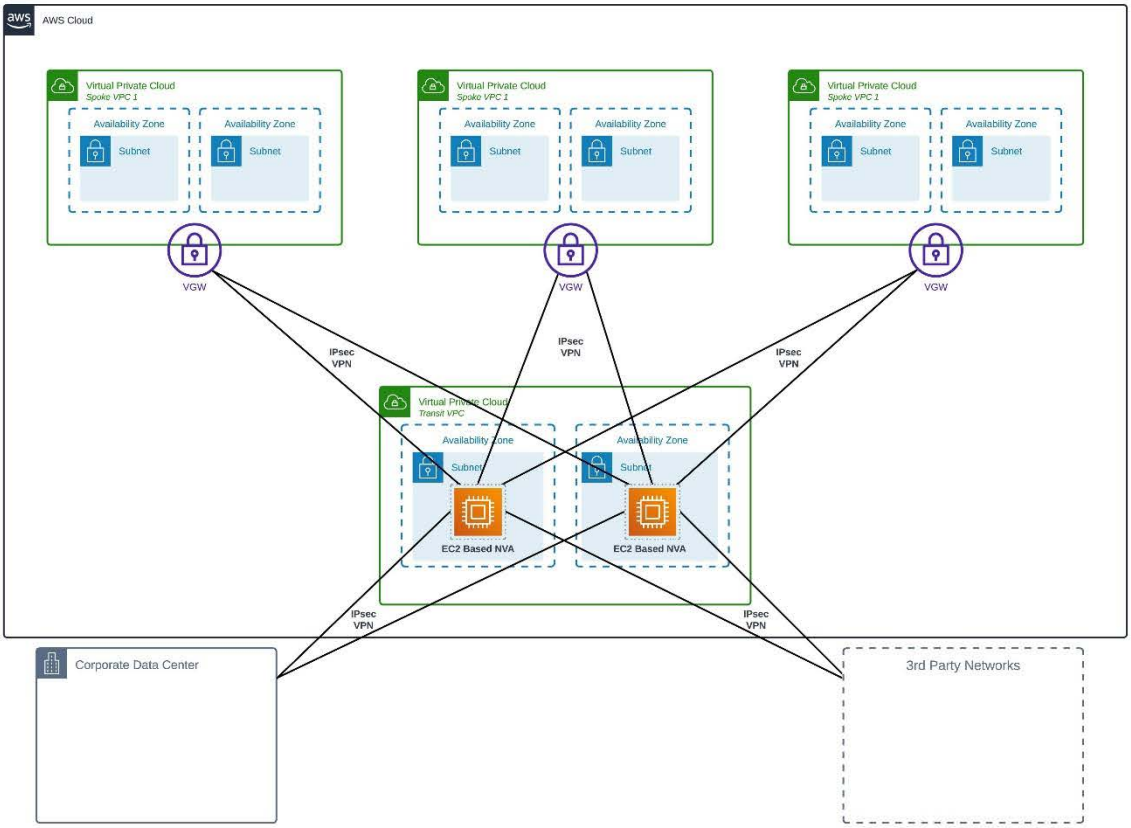
Add new tag

You can add 50 more tags.

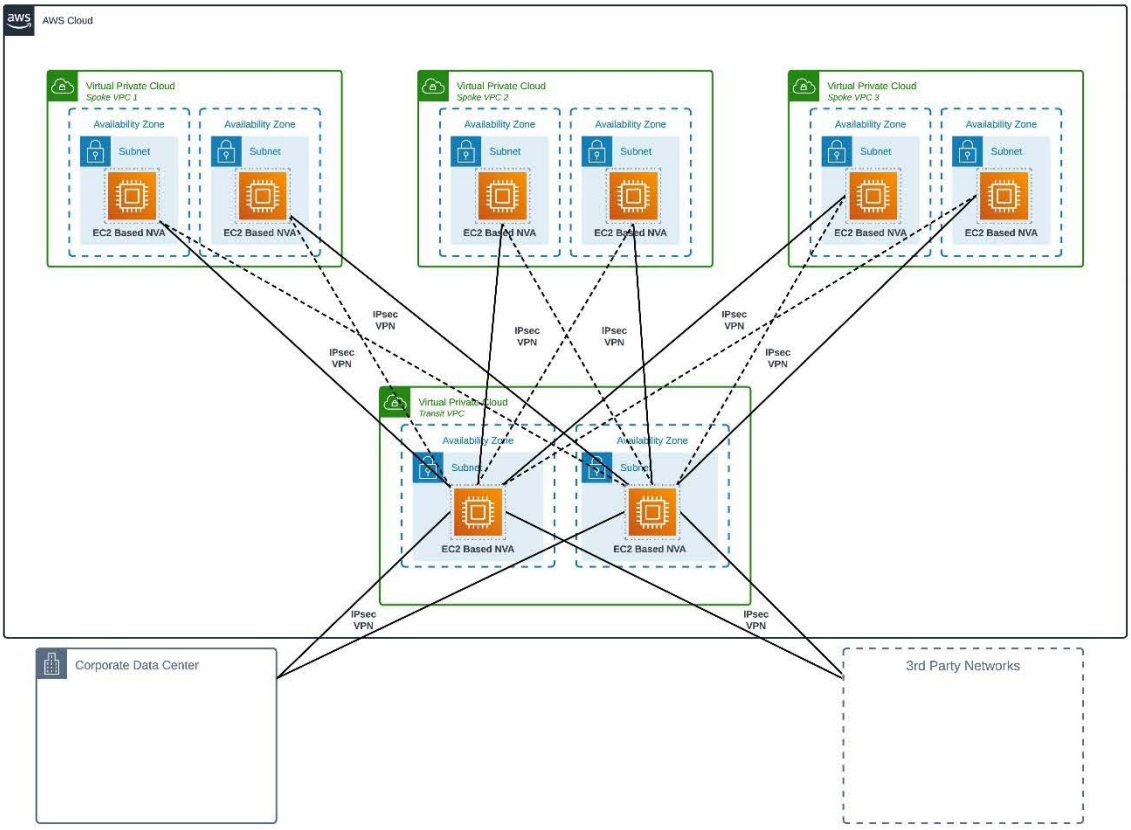
Cancel | Create peering connection

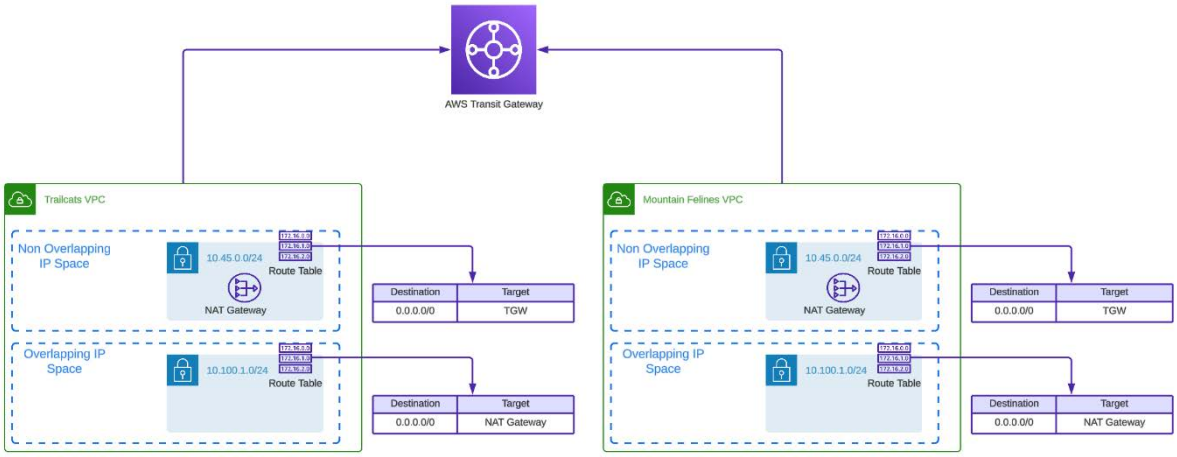

Peering connections (1/1) Info
Actions
Create peering connection
Find resources by attribute or tag
Peering connection ID : pcx-0dd6b0c9c972f694d
Clear filters
1
Name
Peering connection ID
Status
Requester VPC
test-vpc-peering
pcx-0dd6b0c9c972f694d
Pending acceptance
vpc-00e9ff2528611bc47 / vpc-a
Peering connections (1/1) Info
Actions
Create peering connection
Find resources by attribute or tag
Peering connection ID : pcx-0dd6b0c9c972f694d
Clear filters
1
Name
Peering connection ID
Status
test-vpc-peering
pcx-0dd6b0c9c972f694d
1bc47 / vpc-a
View details
Accept request
Reject request
Edit DNS settings
Manage tags
Delete peering connection

Option 1:

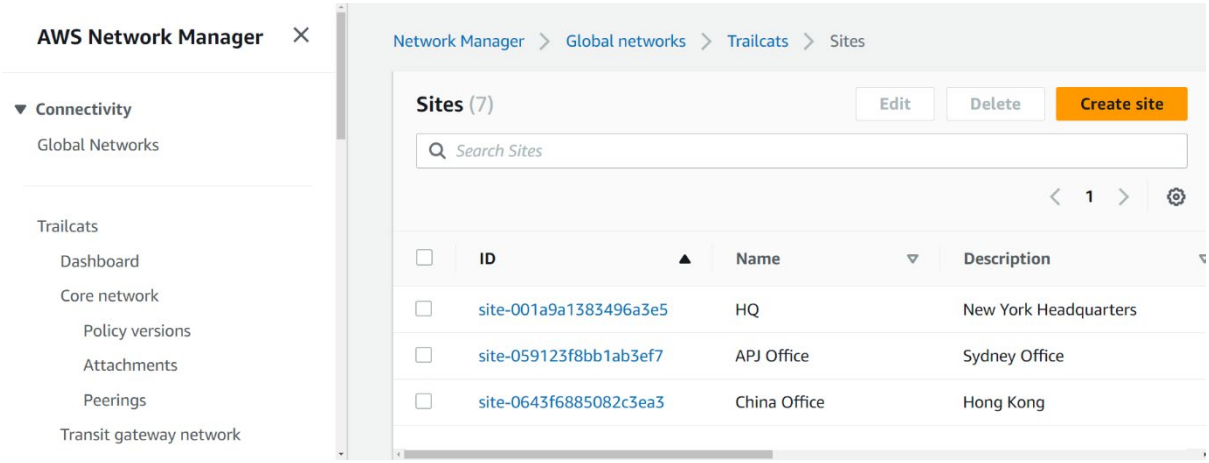


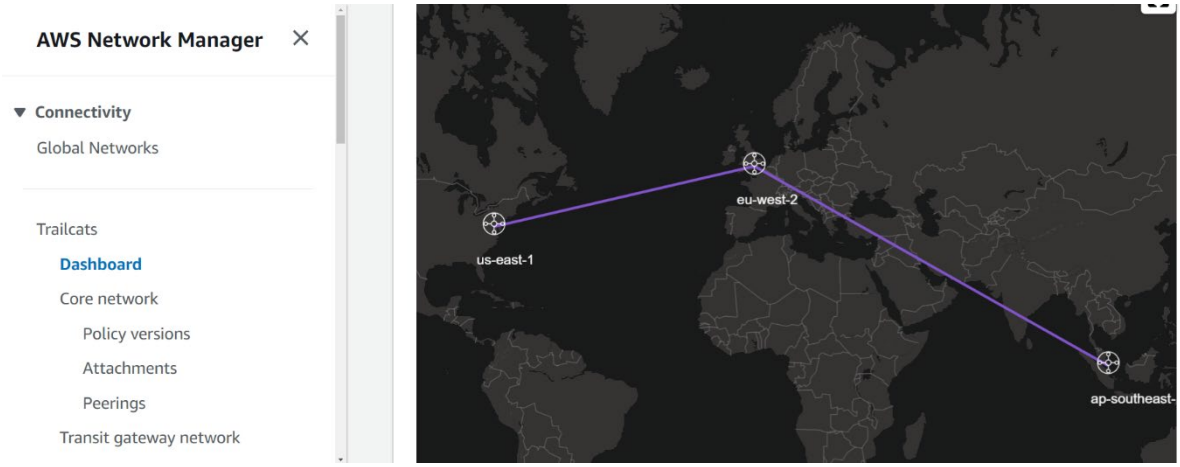
Option 2:

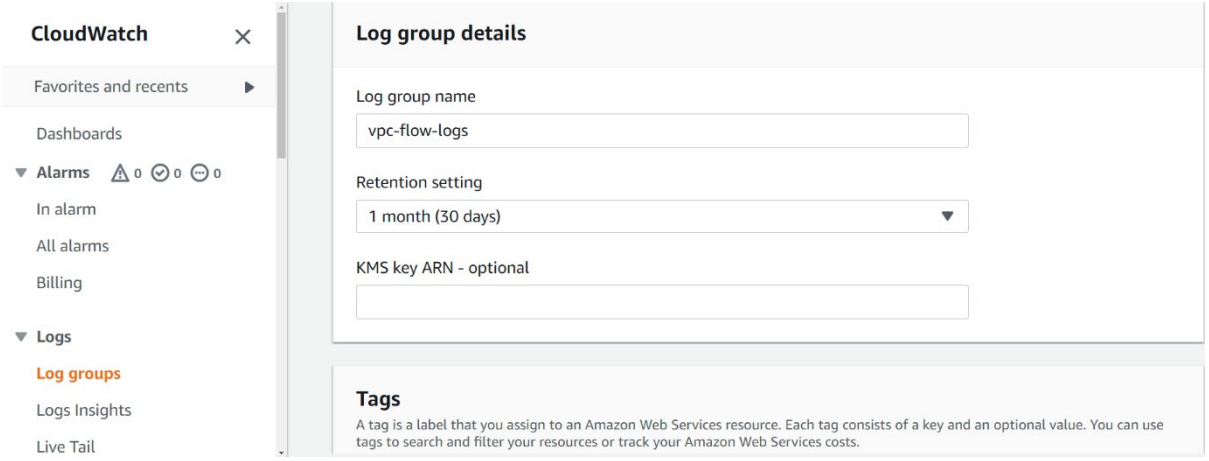



AWS Transit Gateway
Trailcats VPC
Non Overlapping IP Space
10.45.0.0/24
Route Table
NAT Gateway
Overlapping IP Space
10.100.1.0/24
Route Table
Destination
Target
0.0.0.0/0
TGW
Destination
Target
0.0.0.0/0
NAT Gateway
Mountain Felines VPC
Non Overlapping IP Space
10.45.0.0/24
Route Table
NAT Gateway
Overlapping IP Space
10.100.1.0/24
Route Table
Destination
Target
0.0.0.0/0
TGW
Destination
Target
0.0.0.0/0
NAT Gateway

Chapter 2: VPC Traffic and Performance Monitoring







Amazon S3

Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

Create bucket Info

Buckets are containers for data stored in S3. Learn more

General configuration

Bucket name

vpc-flow-logs-bucket-app1-randomstringofcharacters

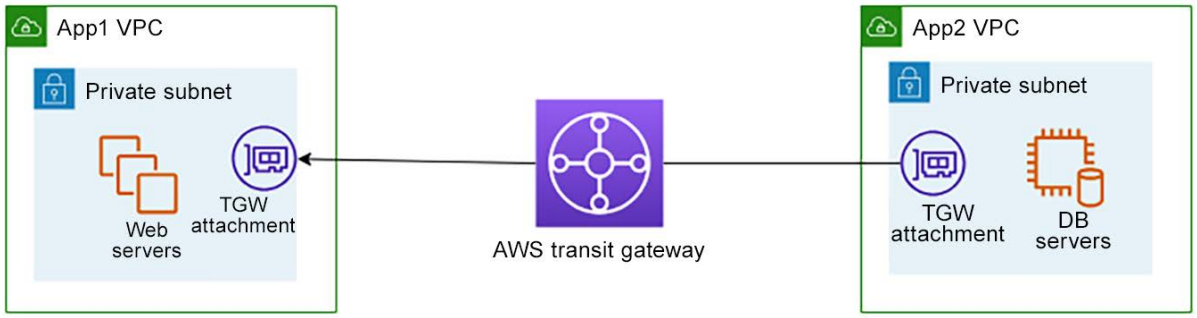
Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming

AWS Region

US East (N. Virginia) us-east-1

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.



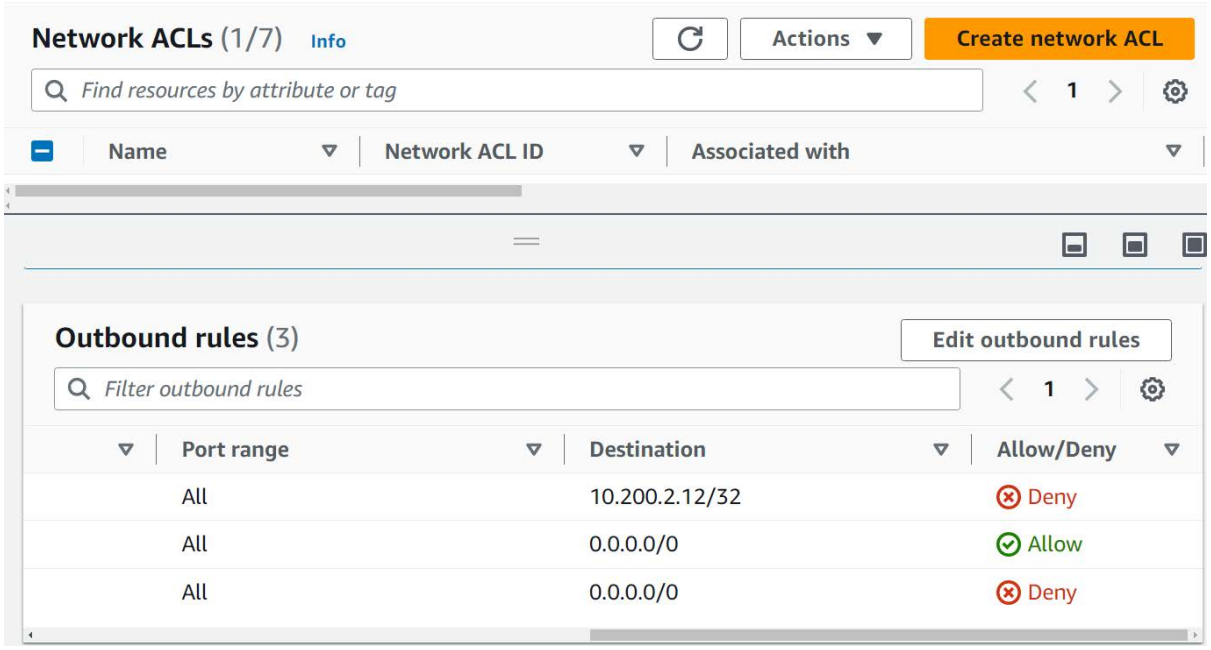
Log events

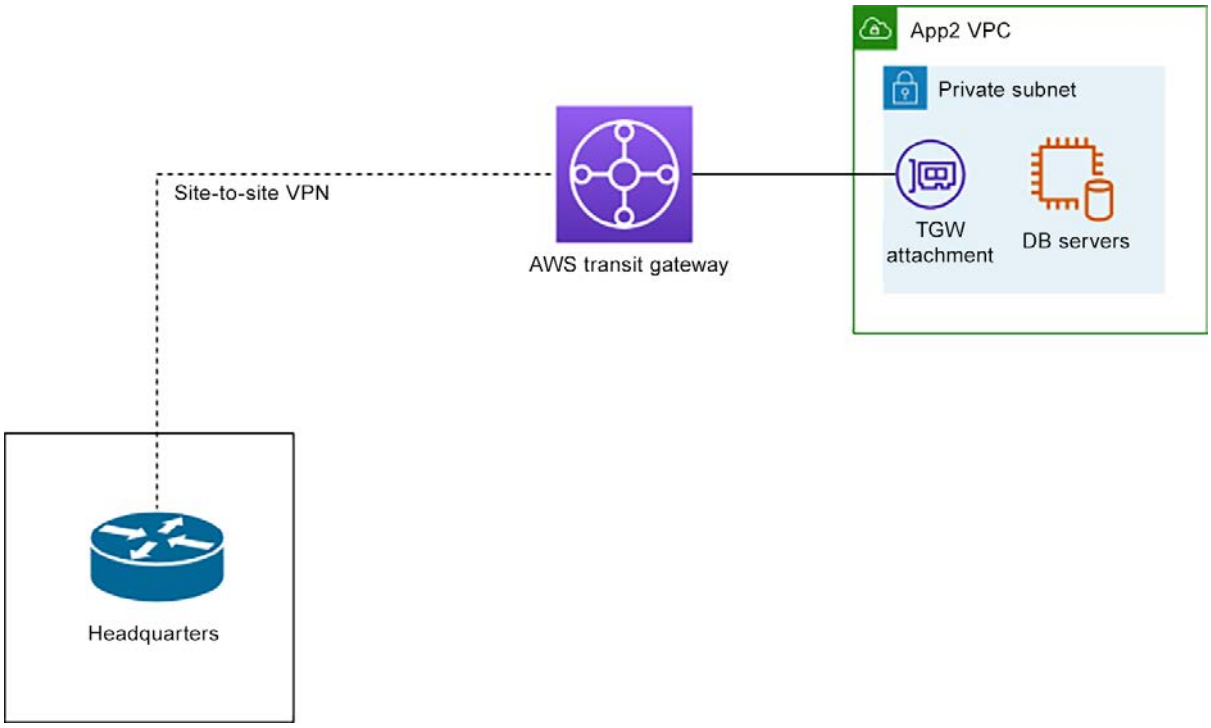
You can use the filter bar below to search for and match terms, phrases, or values in your log events. Learn more about filter patterns

Actions | Start tailing | Create metric filter

10.200.2.12 | Clear | 1m | 30m | 1h | 12h | Custom | Display

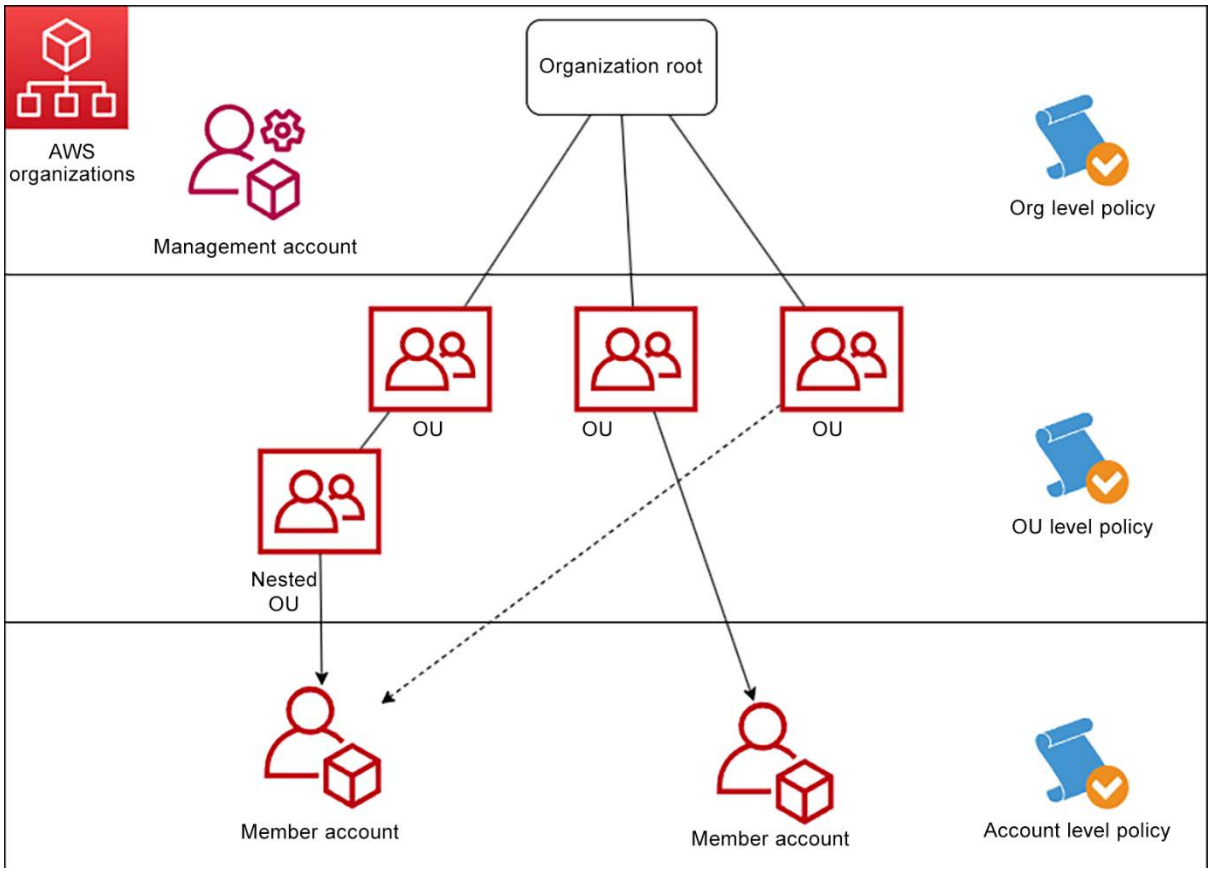
Timestamp	Message
2023-08-05T13:36:29.000-04:00	2 [redacted] eni-068b5ed779598f382 10.200.1.36 10.200.2.…
	2 [redacted] eni-068b5ed779598f382 10.200.1.36 10.200.2.12 0 0 1 55 4620 1691256989 1691257049 REJECT OK
2023-08-05T13:37:30.000-04:00	2 [redacted] eni-068b5ed779598f382 10.200.1.36 10.200.2.…
	2 [redacted] eni-068b5ed779598f382 10.200.1.36 10.200.2.12 0 0 1 58 4872 1691257050 1691257109 REJECT OK

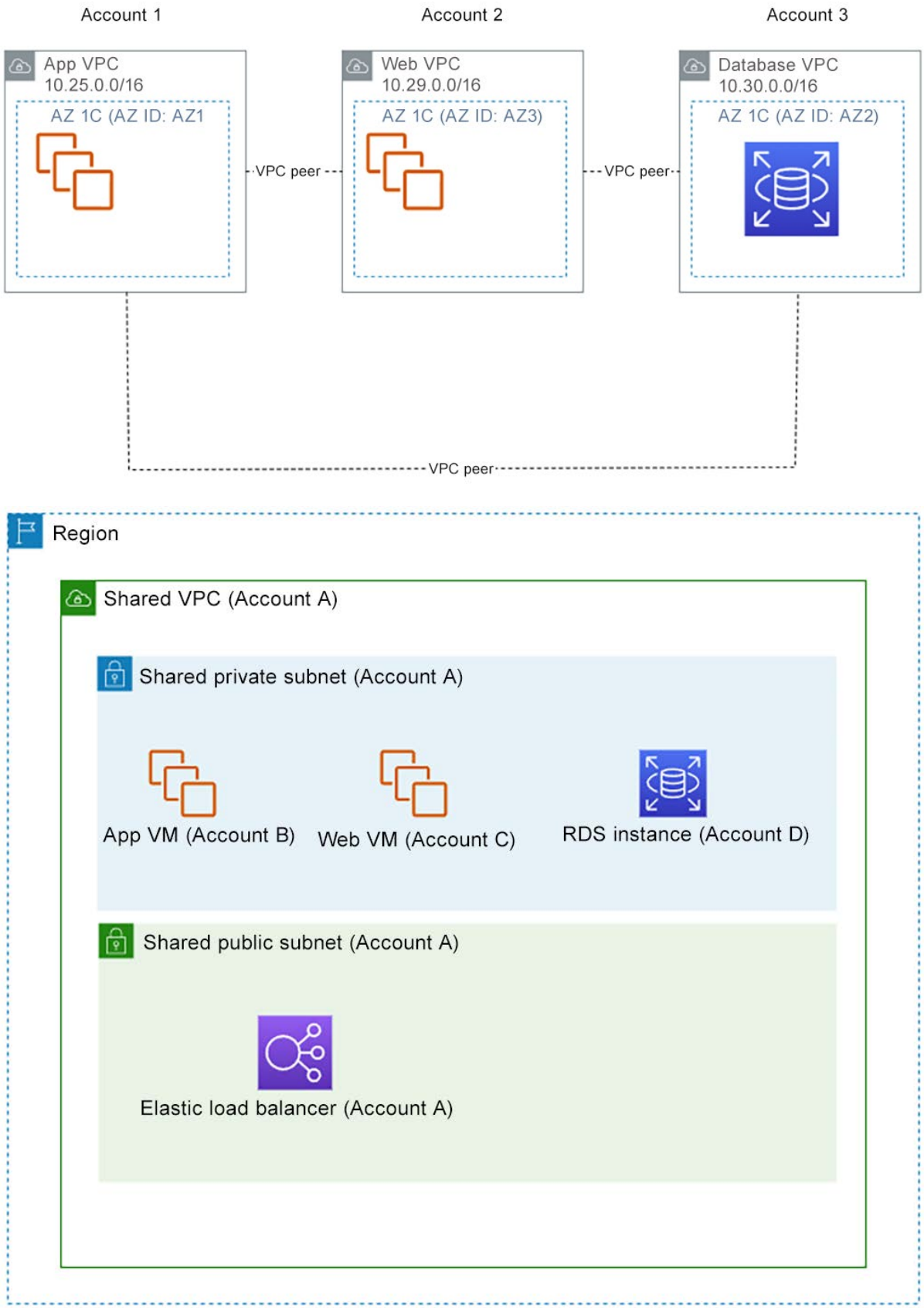


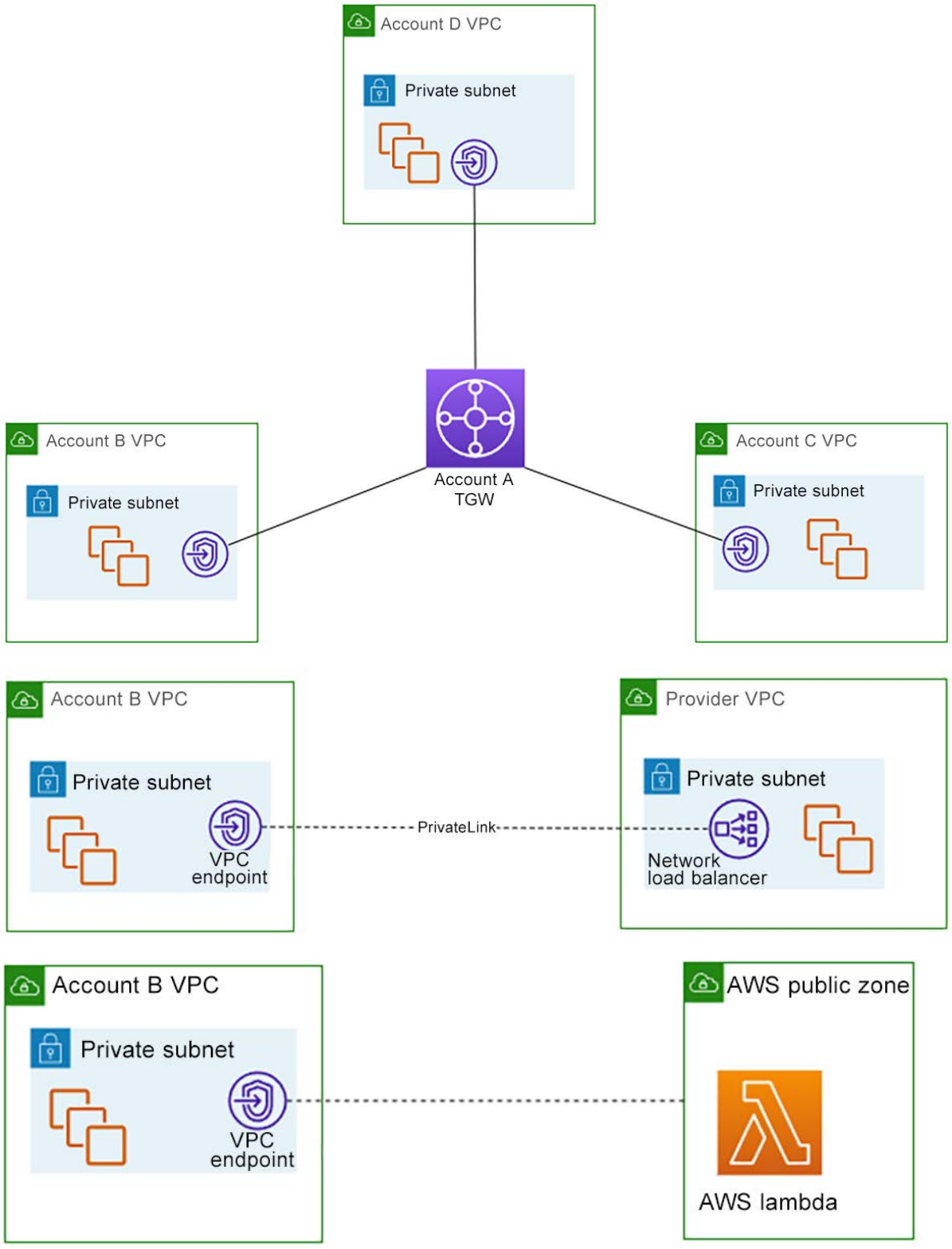


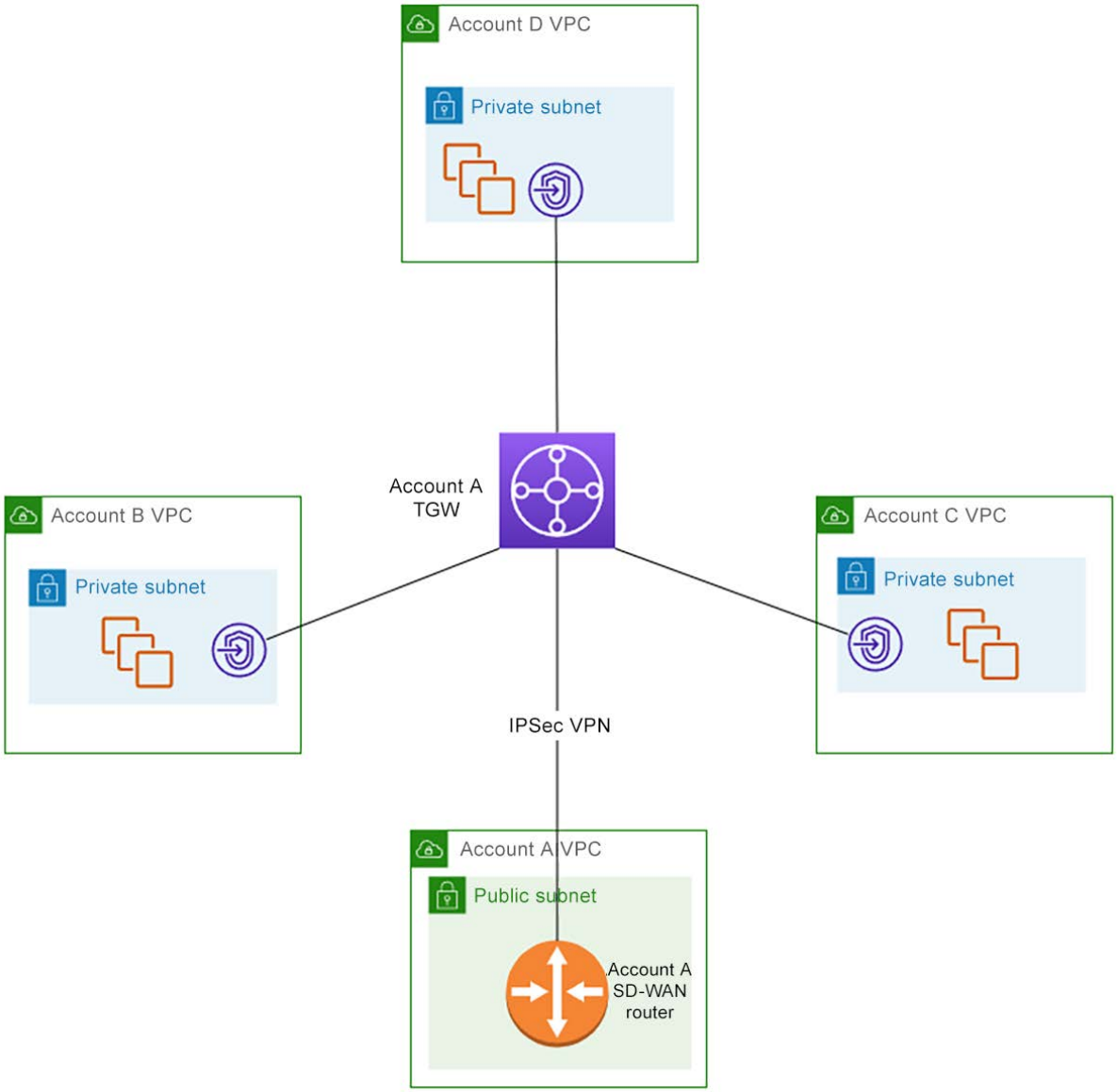
Outside IP Header (Public) 20 bytes	ESP Header 8 bytes	Original IP Header (Private) 20 bytes	Original Payload (variable)	ESP Trailer (variable, usually around 20-22)

Chapter 3: Networking Across Multiple AWS Accounts

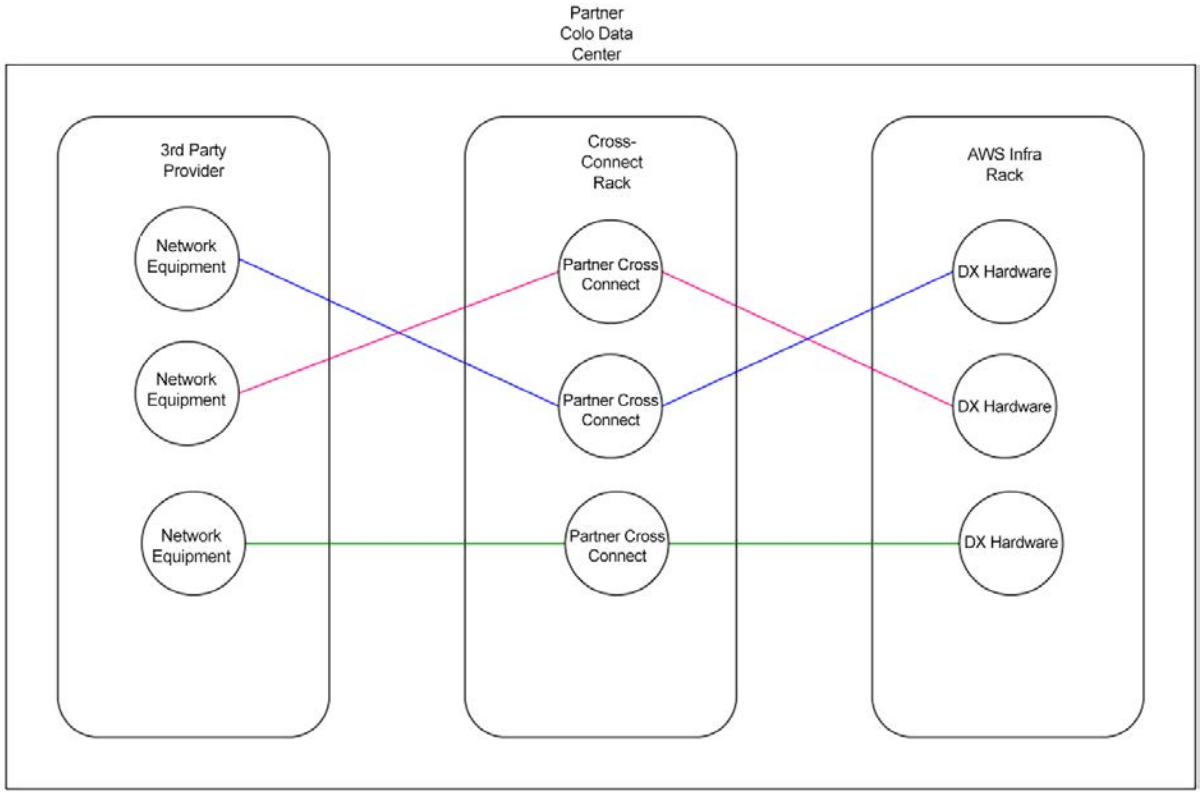


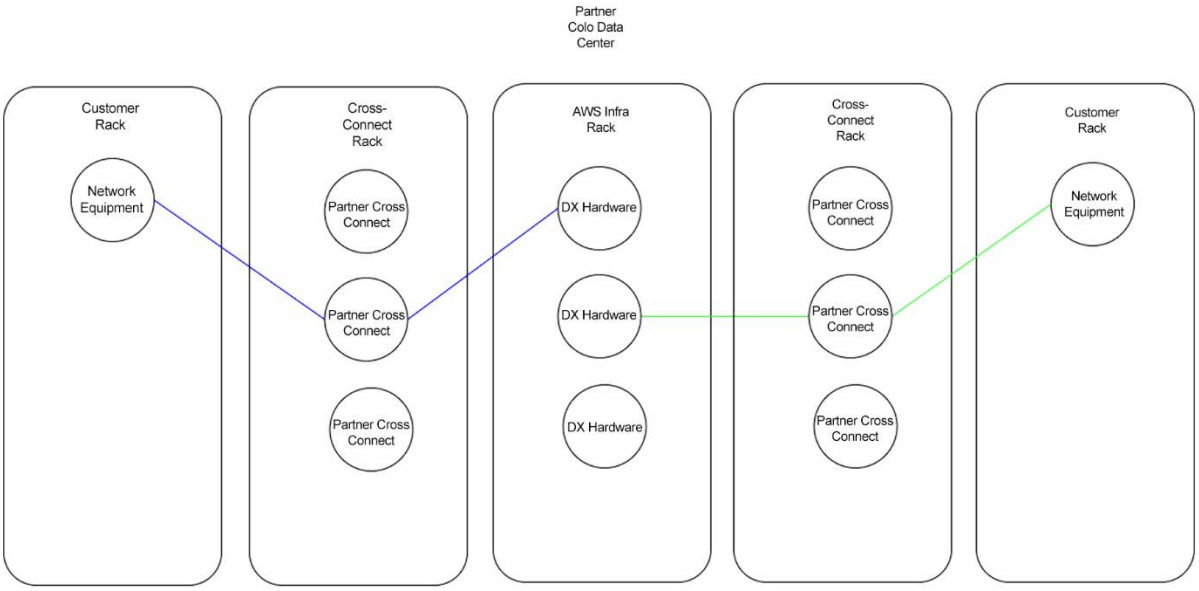

Account 1
Account 2
Account 3
App VPC
10.25.0.0/16
AZ 1C (AZ ID: AZ1
Web VPC
10.29.0.0/16
AZ 1C (AZ ID: AZ3)
Database VPC
10.30.0.0/16
AZ 1C (AZ ID: AZ2)
VPC peer
VPC peer
VPC peer
Region
Shared VPC (Account A)
Shared private subnet (Account A)
App VM (Account B)
Web VM (Account C)
RDS instance (Account D)
Shared public subnet (Account A)
Elastic load balancer (Account A)

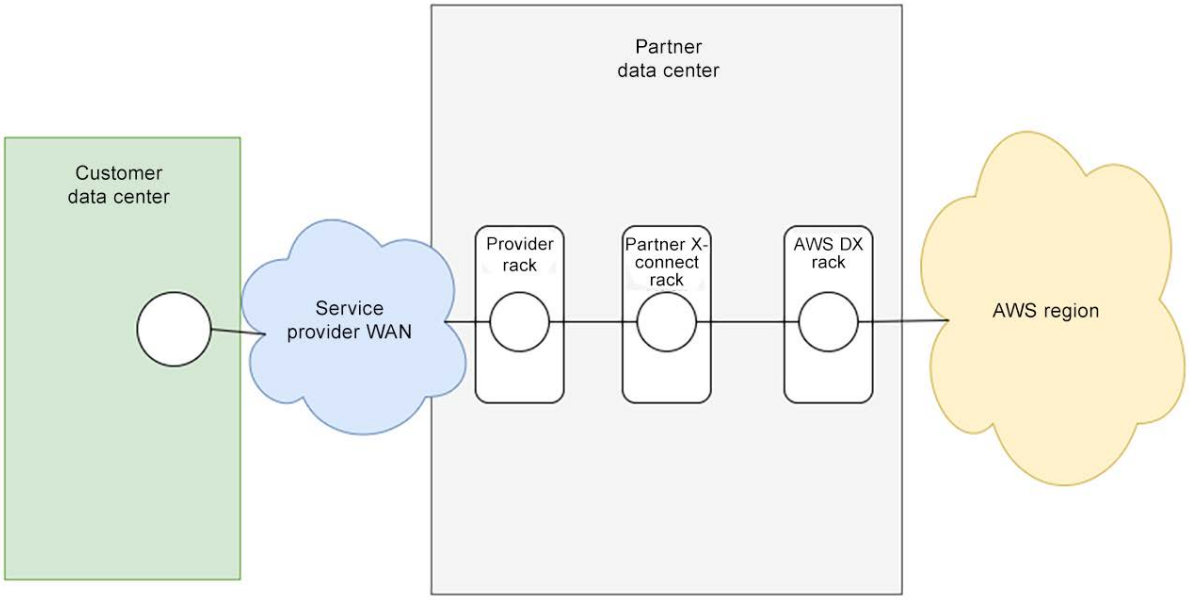

Account D VPC
Private subnet
Account A
TGW
Account B VPC
Private subnet
Account C VPC
Private subnet
Account B VPC
Private subnet
VPC
endpoint
PrivateLink
Provider VPC
Private subnet
Network
load balancer
Account B VPC
Private subnet
VPC
endpoint
AWS public zone
AWS lambda


Account D VPC
Private subnet
Account A
TGW
Account B VPC
Private subnet
Account C VPC
Private subnet
IPSec VPN
Account A VPC
Public subnet
Account A
SD-WAN
router

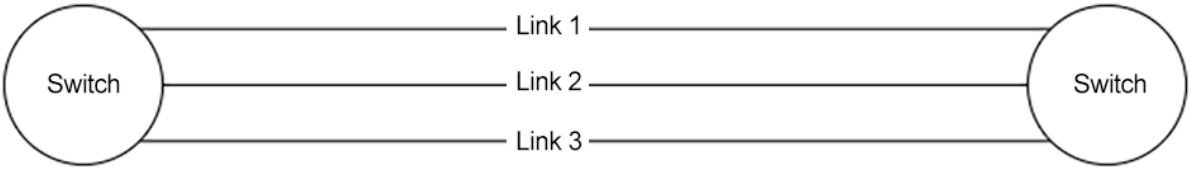
Chapter 4: AWS Direct Connect





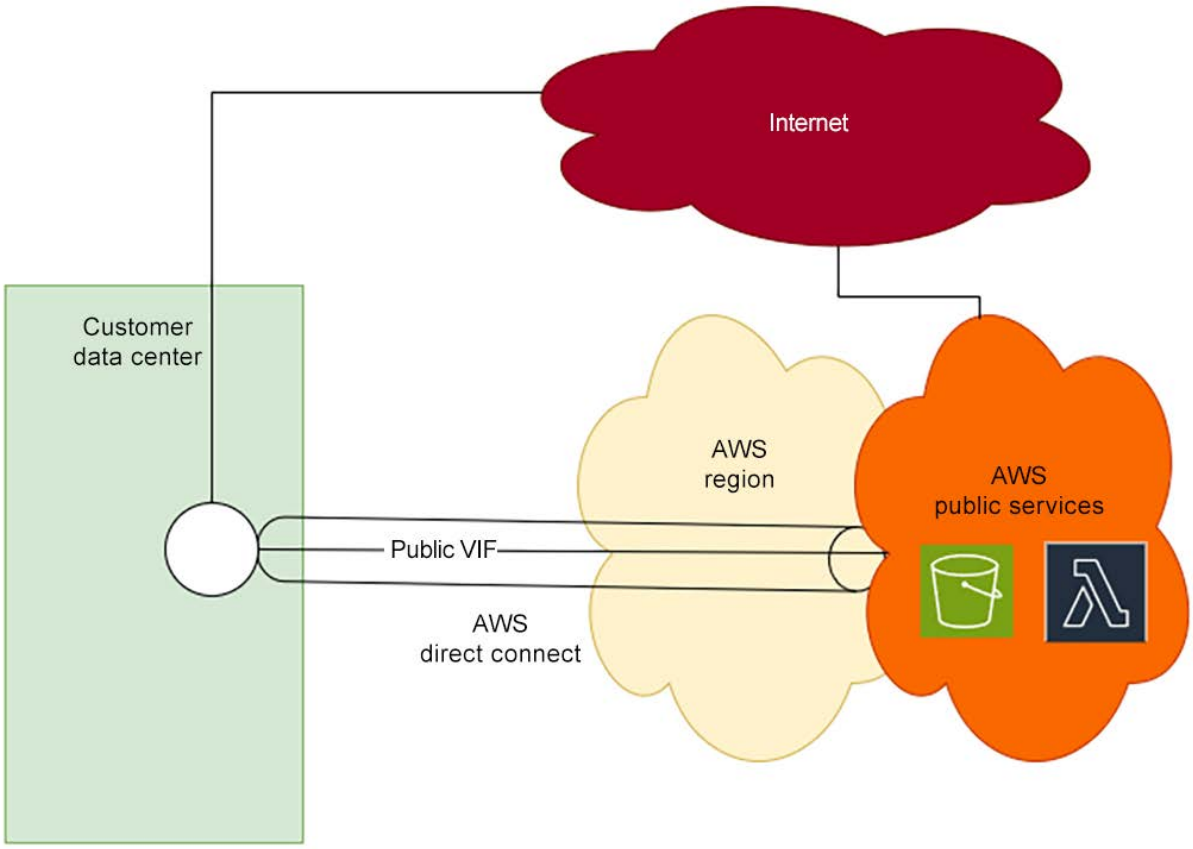


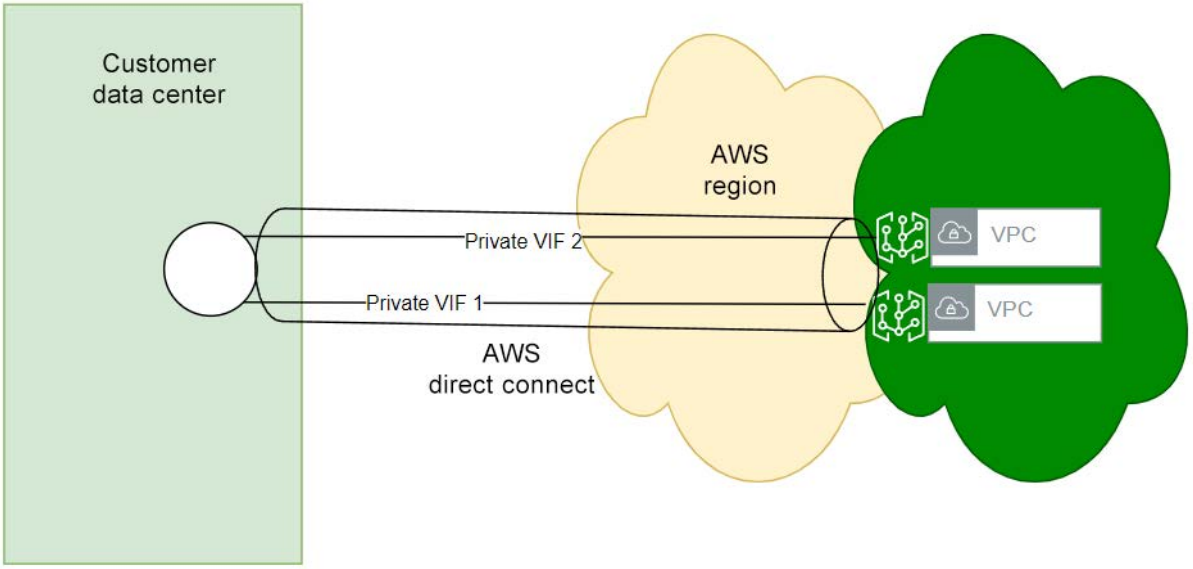
Physical
Cabling

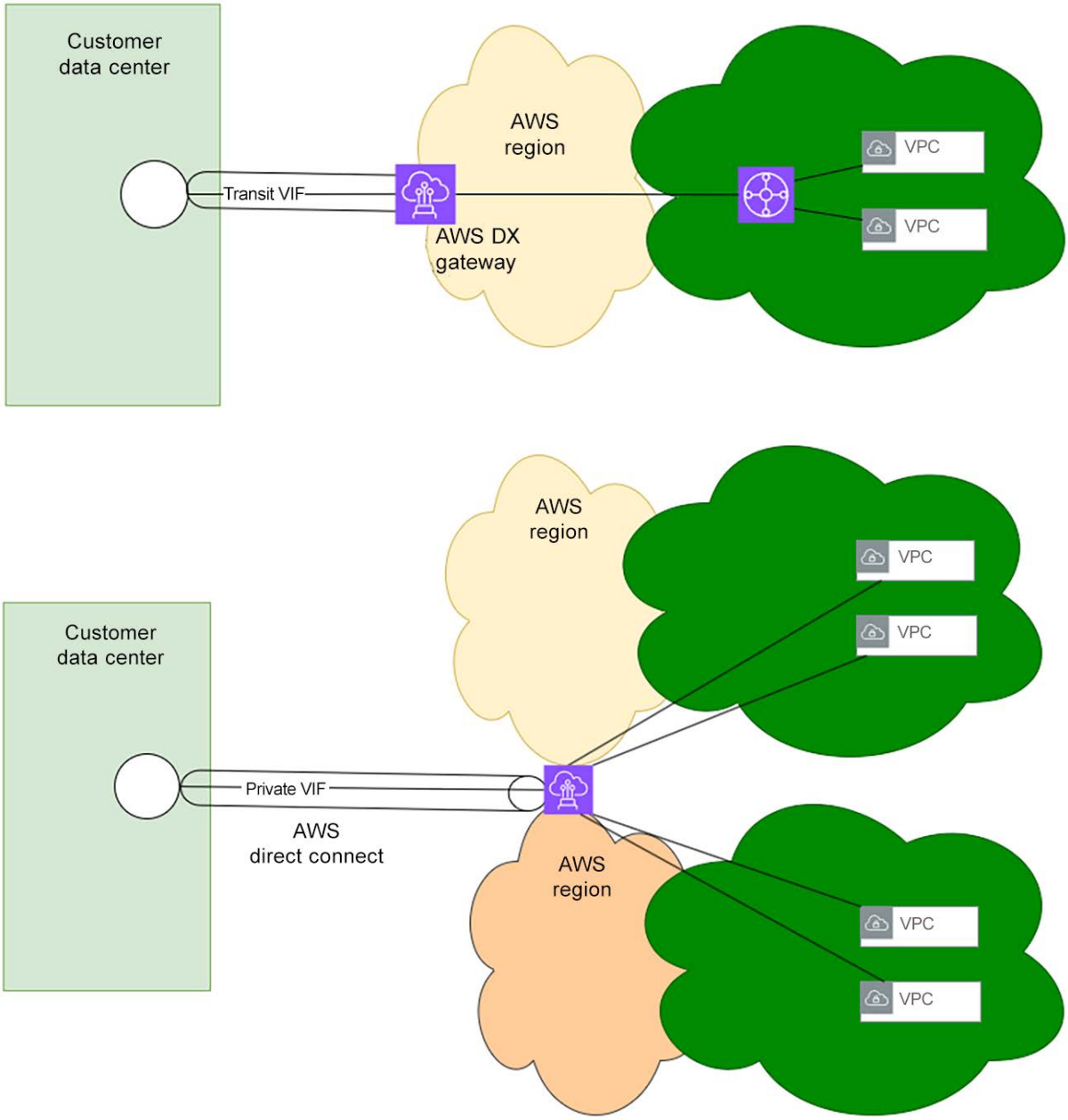


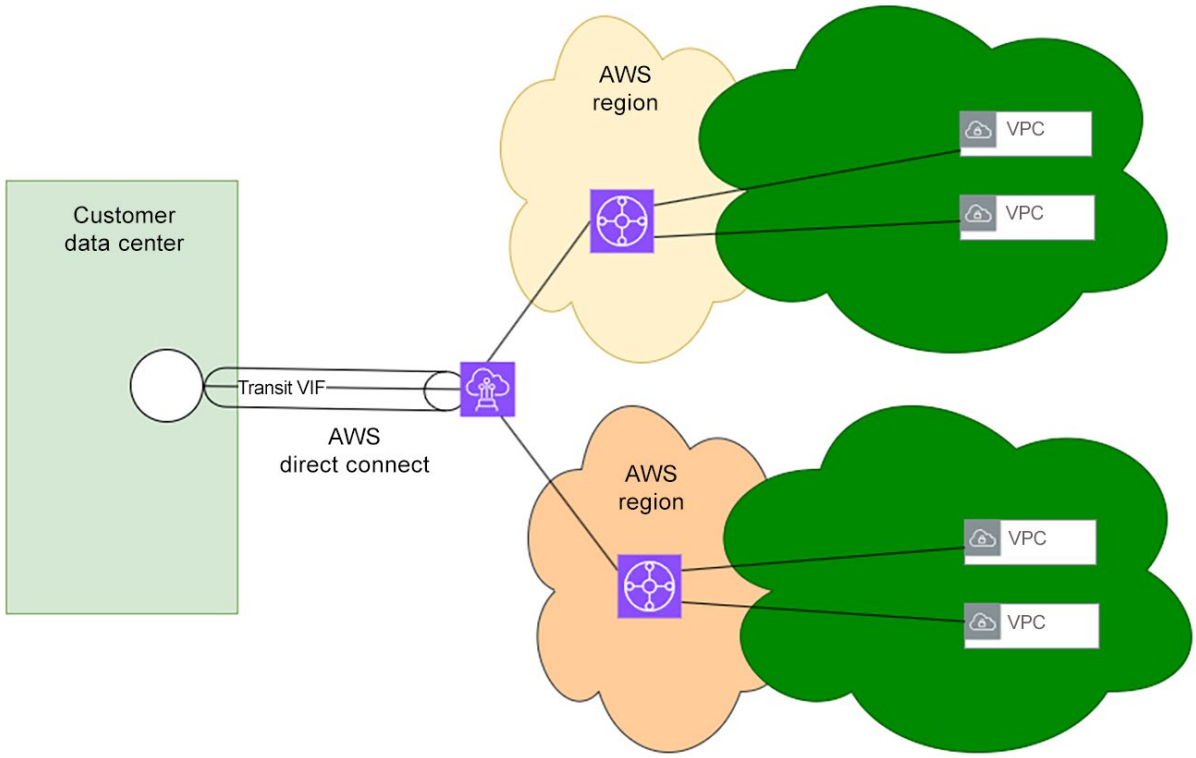
Logical
Cabling

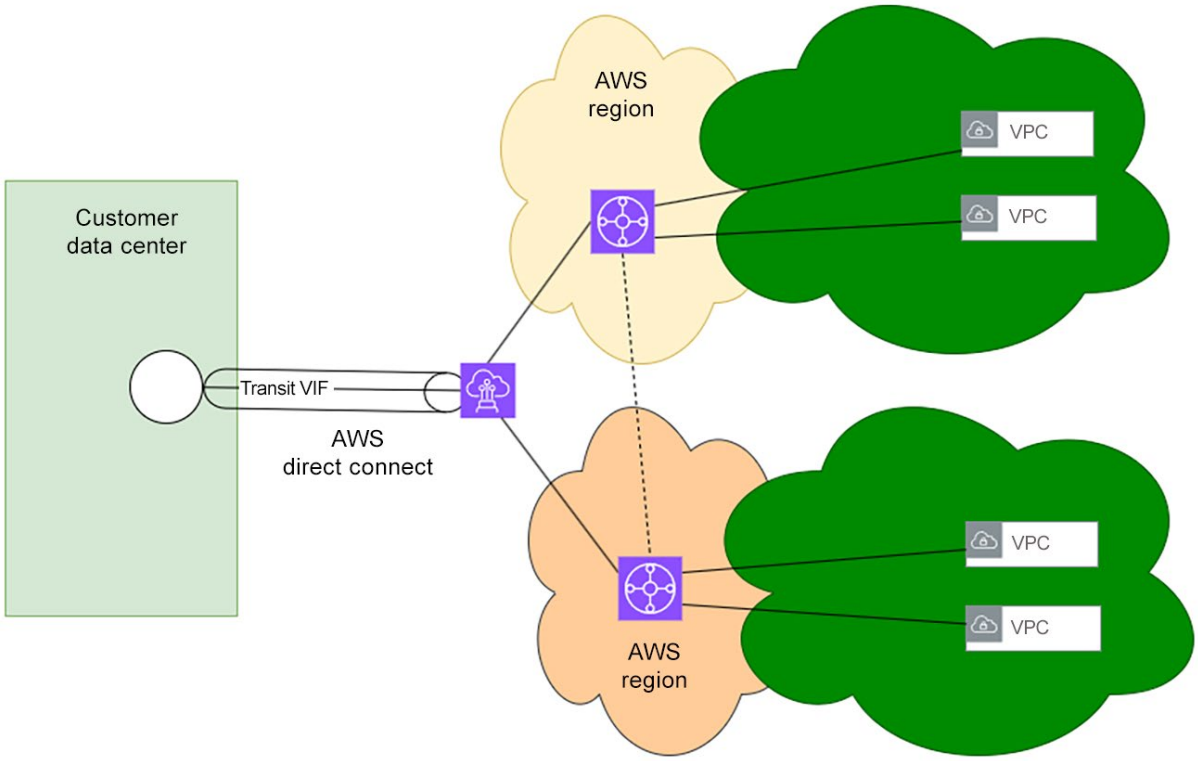
Ethernet frame
headers

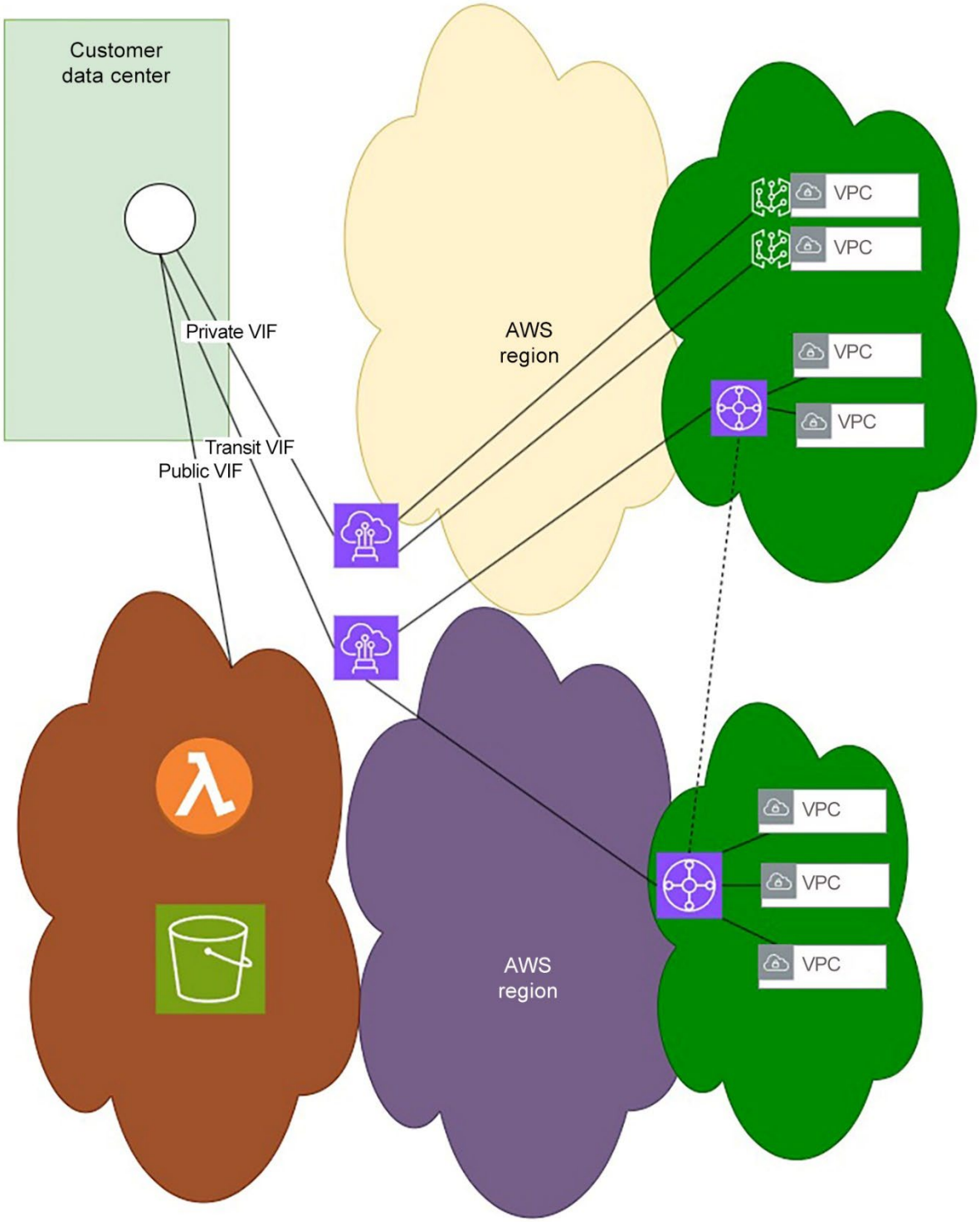

Internet
Customer
data center
AWS
region
AWS
public services
Public VIF
AWS
direct connect

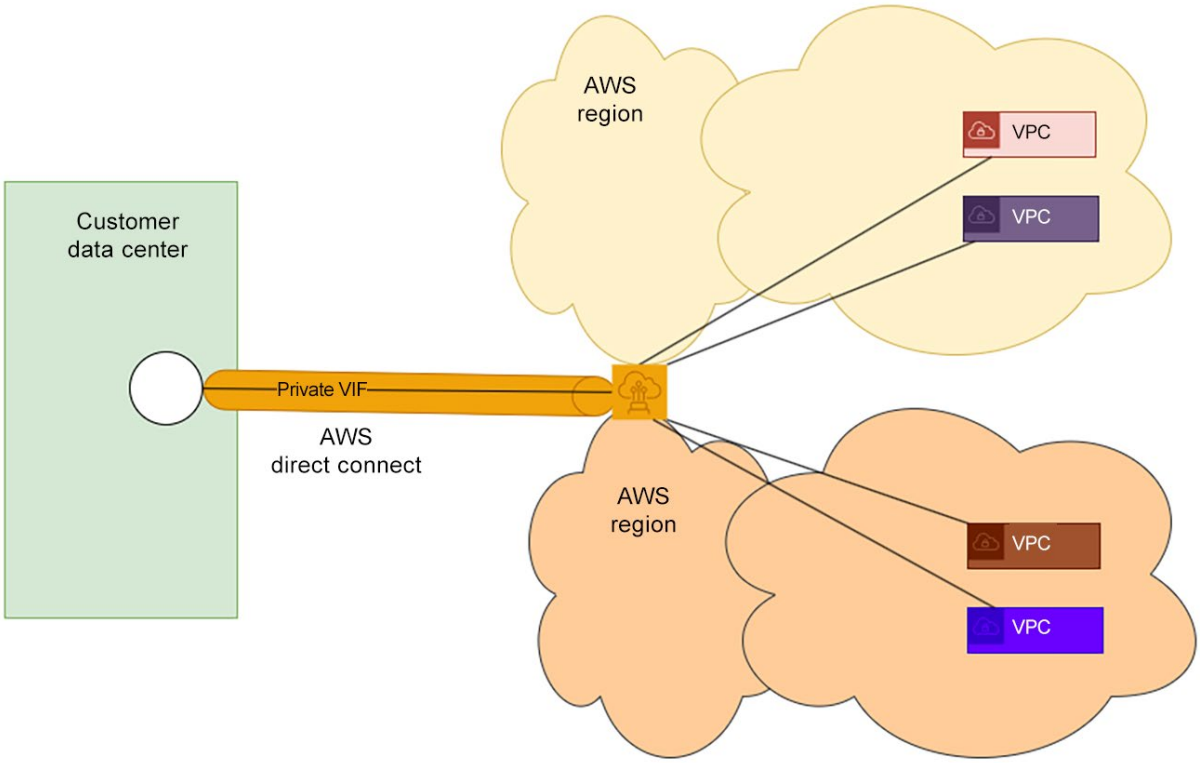

Customer
data center
AWS
region
Private VIF 2
Private VIF 1
VPC
VPC
AWS
direct connect

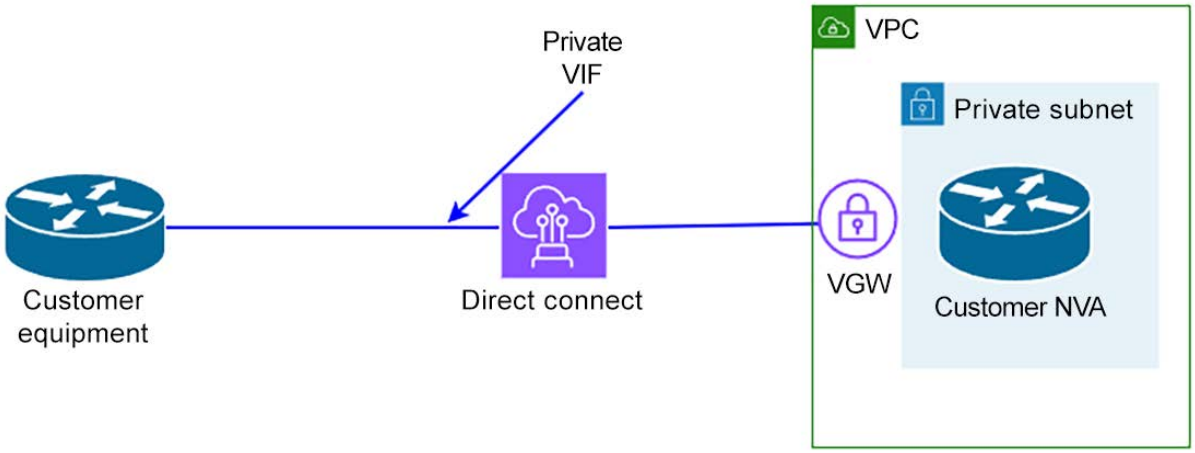

Customer
data center
Transit VIF
AWS
region
AWS DX
gateway
VPC
VPC
AWS
region
VPC
VPC
Customer
data center
Private VIF
AWS
direct connect
AWS
region
VPC
VPC

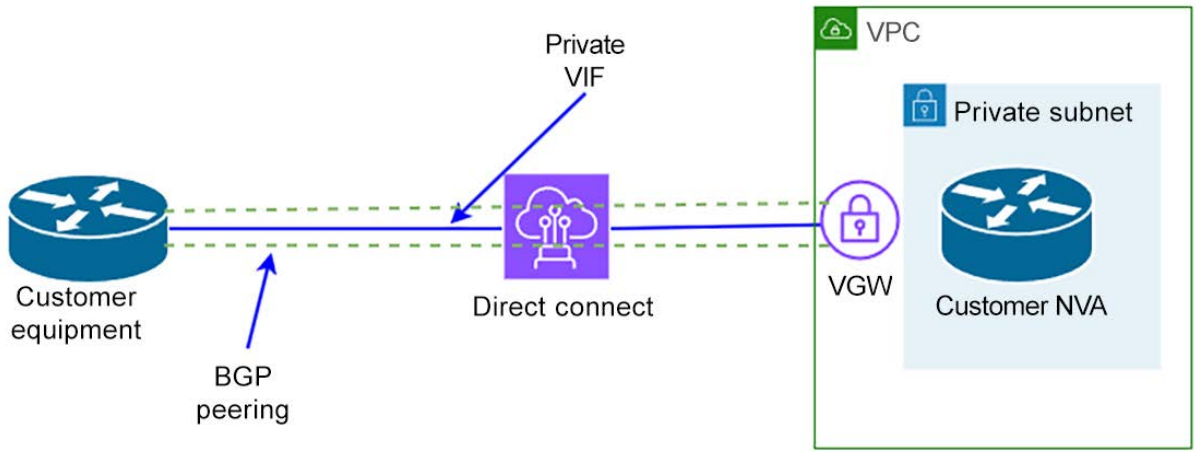

AWS
region
VPC
VPC
Customer
data center
Transit VIF
AWS
direct connect
AWS
region
VPC
VPC

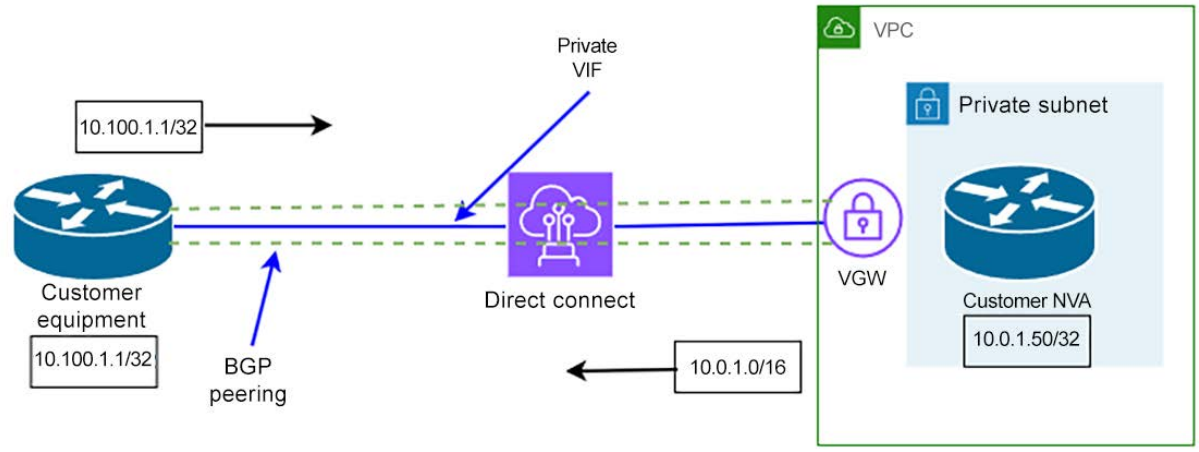

AWS
region
VPC
VPC
Customer
data center
Transit VIF
AWS
direct connect
VPC
VPC
AWS
region

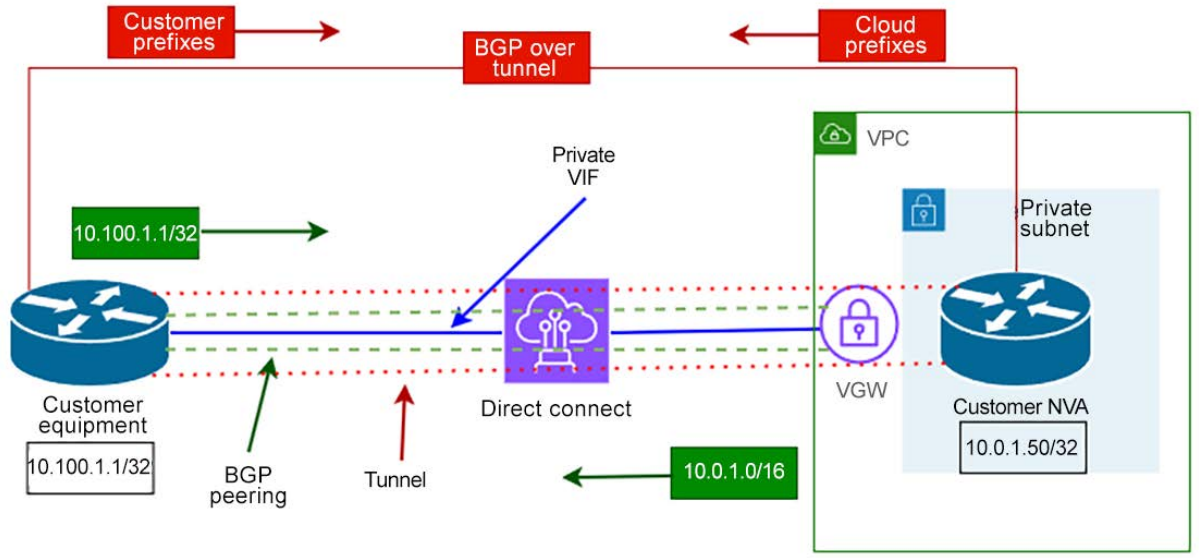

Customer
data center
Private VIF
Transit VIF
Public VIF
AWS
region
VPC
VPC
VPC
VPC
AWS
region
VPC
VPC
VPC

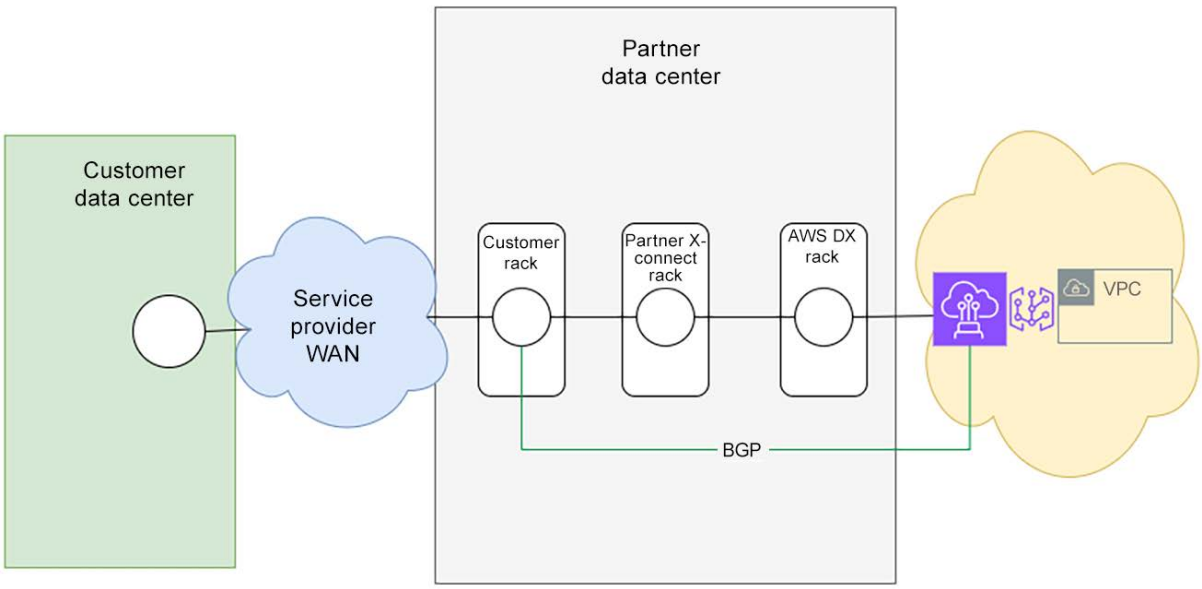

AWS
region
VPC
VPC
Customer
data center
Private VIF
AWS
direct connect
AWS
region
VPC
VPC

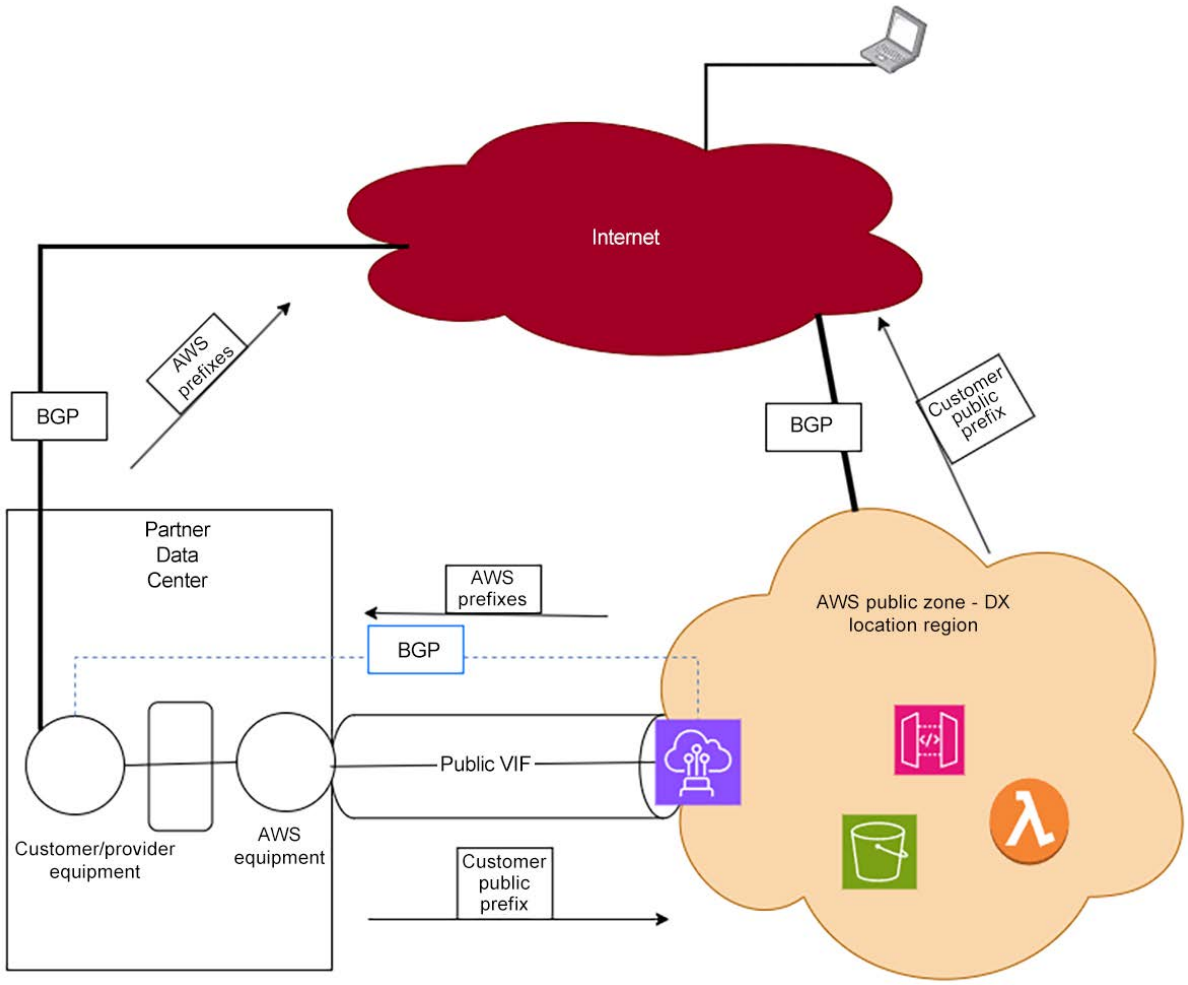

Private
VIF
VPC
Private subnet
Customer
equipment
Direct connect
VGW
Customer NVA

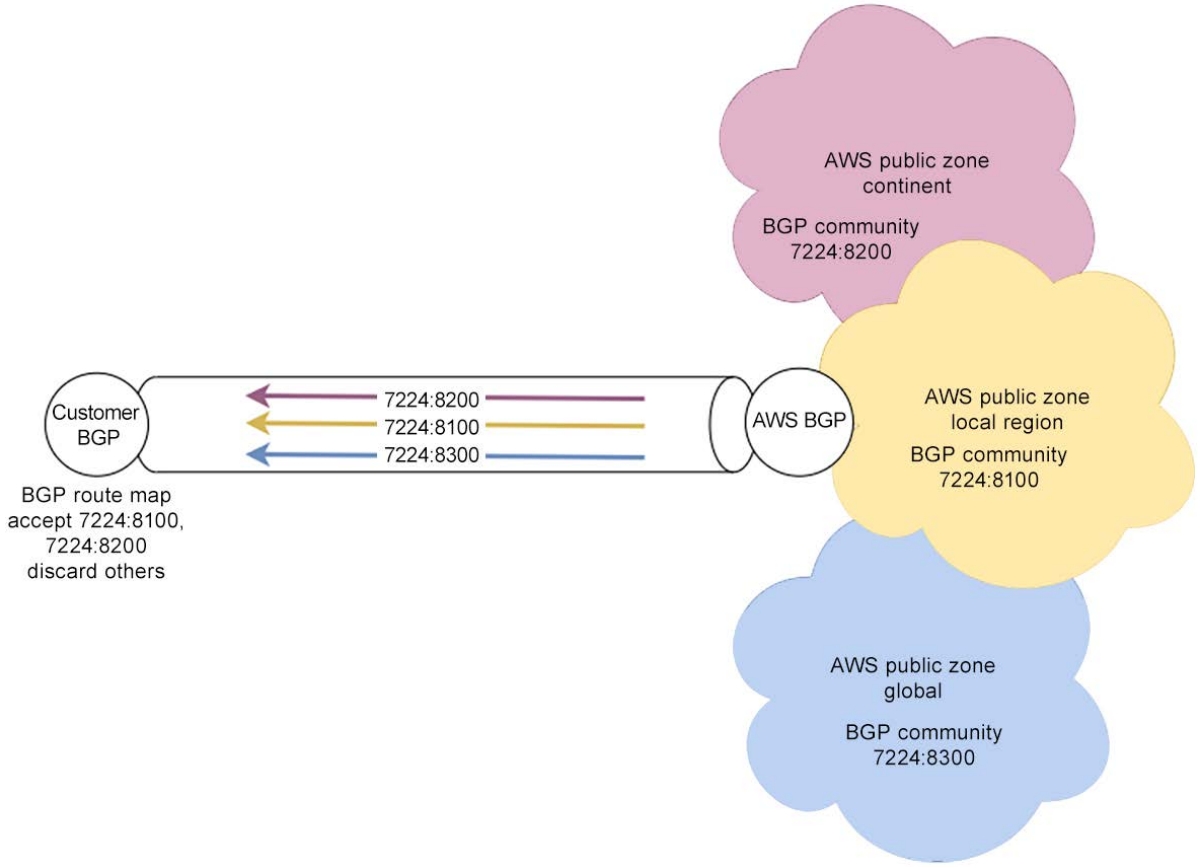

Private
VIF
VPC
Private subnet
Customer
equipment
Direct connect
VGW
Customer NVA
BGP
peering

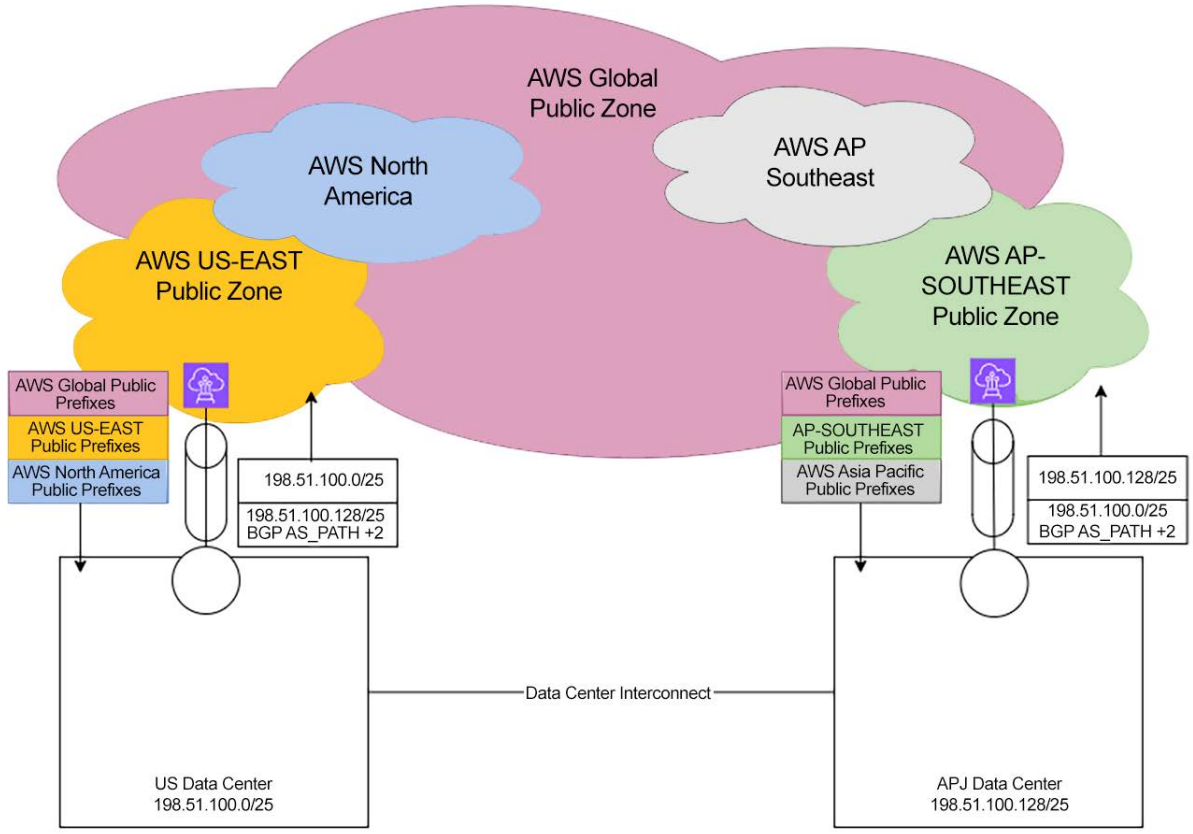

VPC
Private subnet
Private VIF
10.100.1.1/32
Customer equipment
10.100.1.1/32
BGP peering
Direct connect
VGW
Customer NVA
10.0.1.50/32
10.0.1.0/16

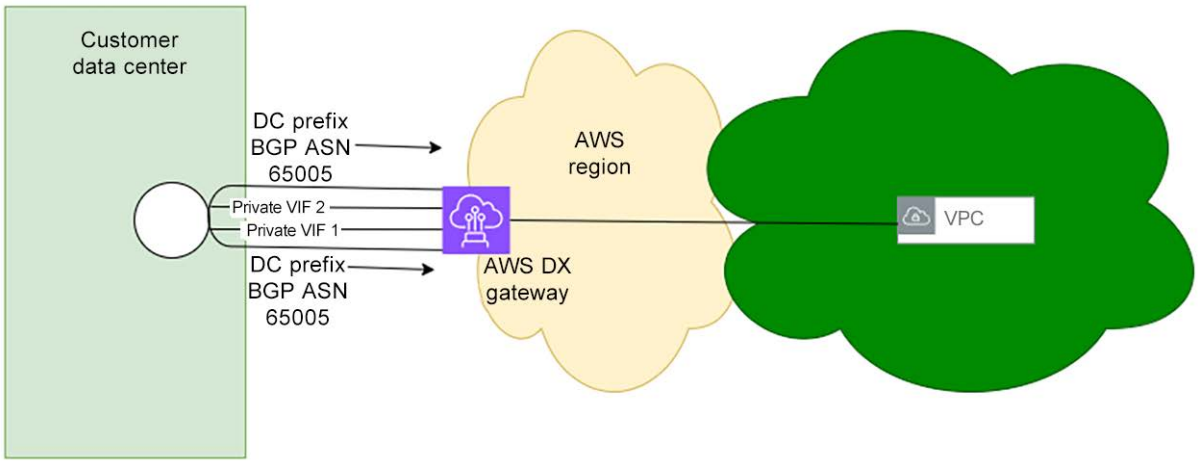

Customer prefixes
BGP over tunnel
Cloud prefixes
VPC
Private subnet
Private VIF
10.100.1.1/32
Customer equipment
10.100.1.1/32
BGP peering
Tunnel
Direct connect
VGW
Customer NVA
10.0.1.50/32
10.0.1.0/16


Partner data center
Customer data center
Service provider WAN
Customer rack
Partner X-connect rack
AWS DX rack
VPC
BGP

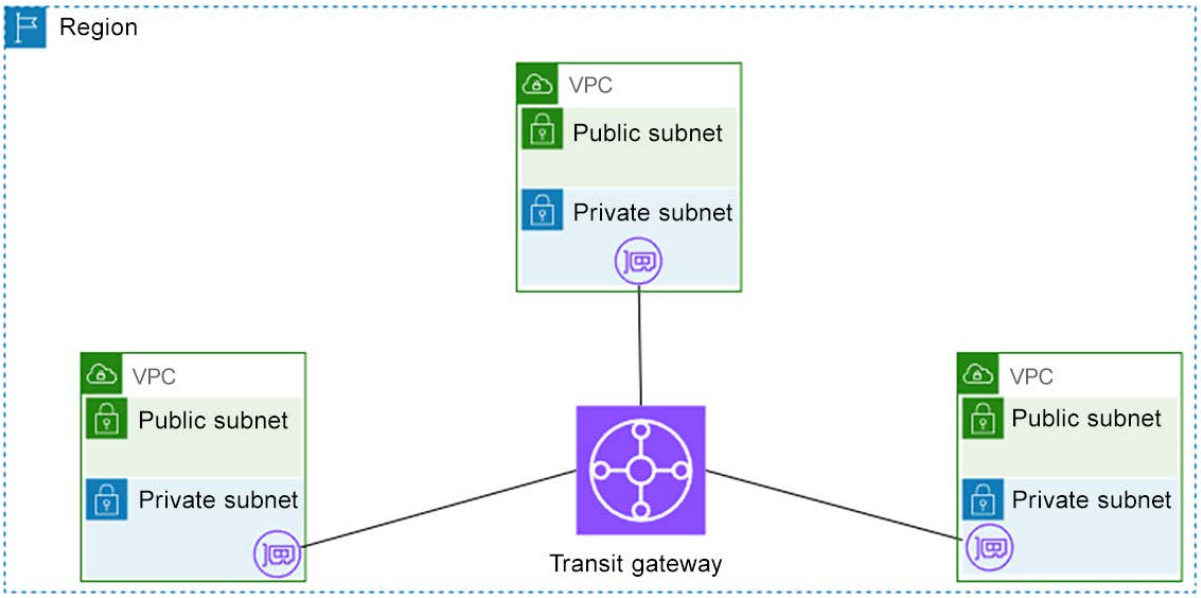

Internet
AWS prefixes
BGP
BGP
Customer public prefix
Partner Data Center
AWS prefixes
BGP
AWS public zone - DX location region
Public VIF
Customer/provider equipment
AWS equipment
Customer public prefix

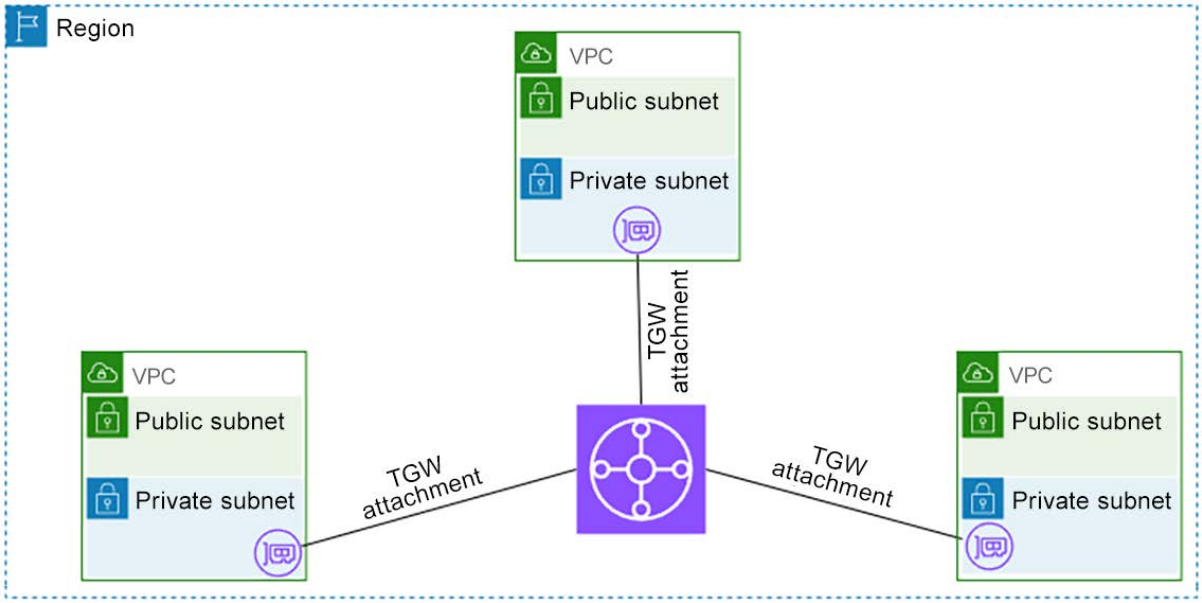

AWS public zone
continent
BGP community
7224:8200
AWS public zone
local region
BGP community
7224:8100
AWS public zone
global
BGP community
7224:8300
Customer
BGP
7224:8200
7224:8100
7224:8300
AWS BGP
BGP route map
accept 7224:8100,
7224:8200
discard others

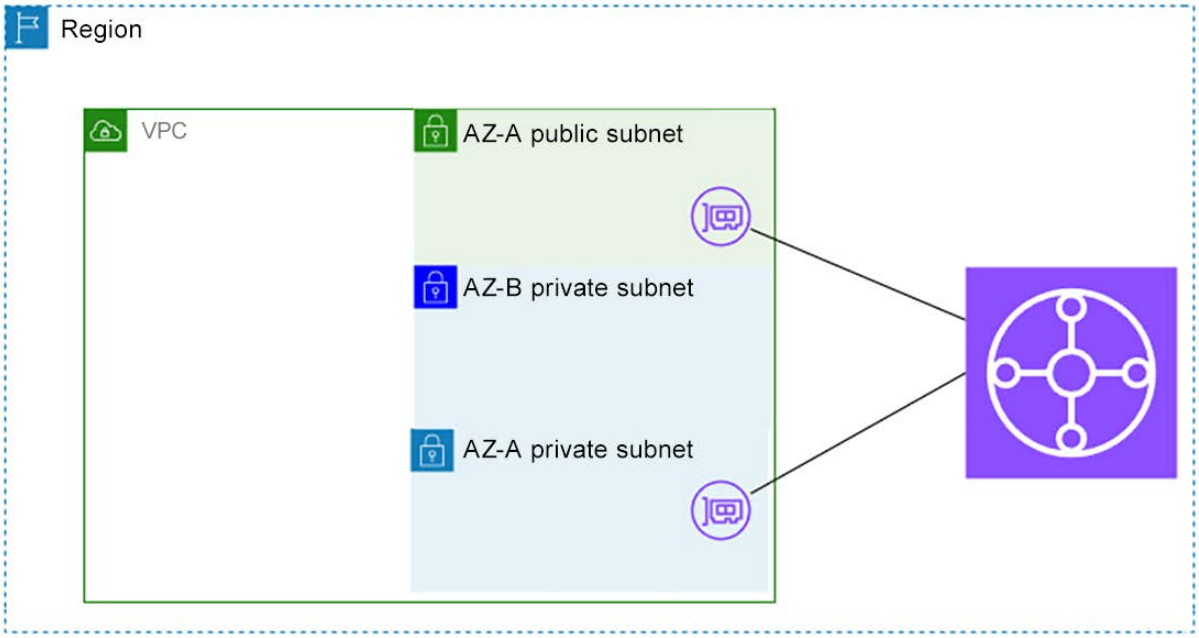

AWS Global
Public Zone
AWS North
America
AWS AP
Southeast
AWS US-EAST
Public Zone
AWS AP-
SOUTHEAST
Public Zone
AWS Global Public
Prefixes
AWS US-EAST
Public Prefixes
AWS North America
Public Prefixes
198.51.100.0/25
198.51.100.128/25
BGP AS_PATH +2
AWS Global Public
Prefixes
AP-SOUTHEAST
Public Prefixes
AWS Asia Pacific
Public Prefixes
198.51.100.128/25
198.51.100.0/25
BGP AS_PATH +2
Data Center Interconnect
US Data Center
198.51.100.0/25
APJ Data Center
198.51.100.128/25

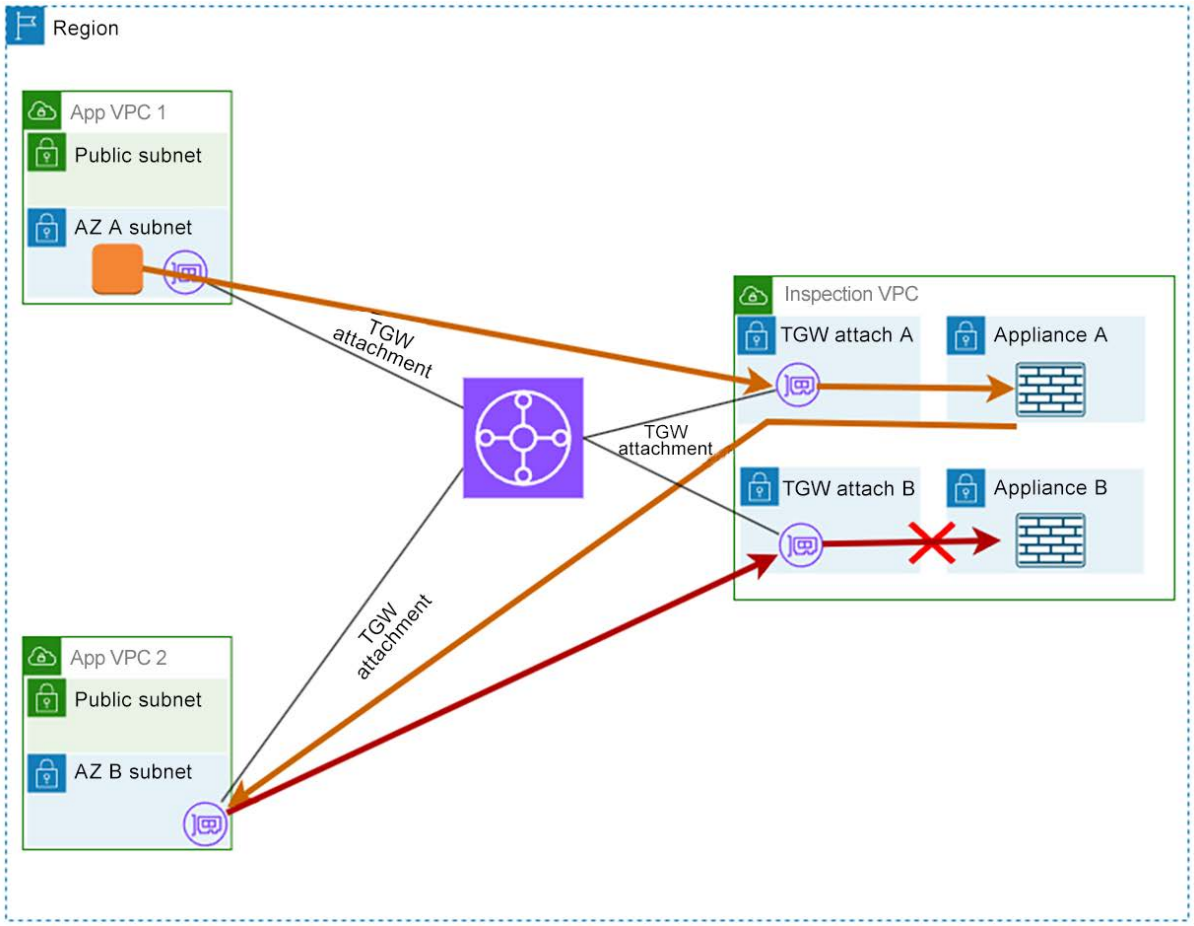

Customer
data center
DC prefix
BGP ASN
65005
Private VIF 2
Private VIF 1
DC prefix
BGP ASN
65005
AWS
region
AWS DX
gateway
VPC

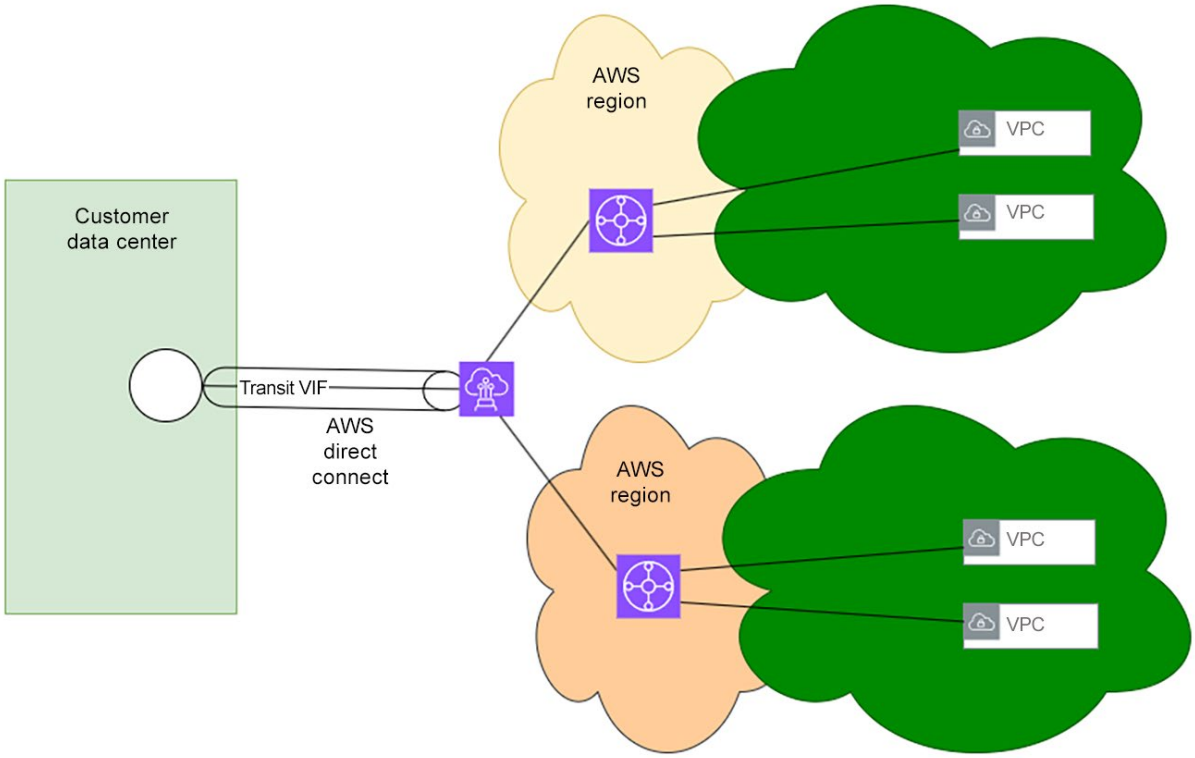
Chapter 5: Hybrid Networking with AWS Transit Gateway

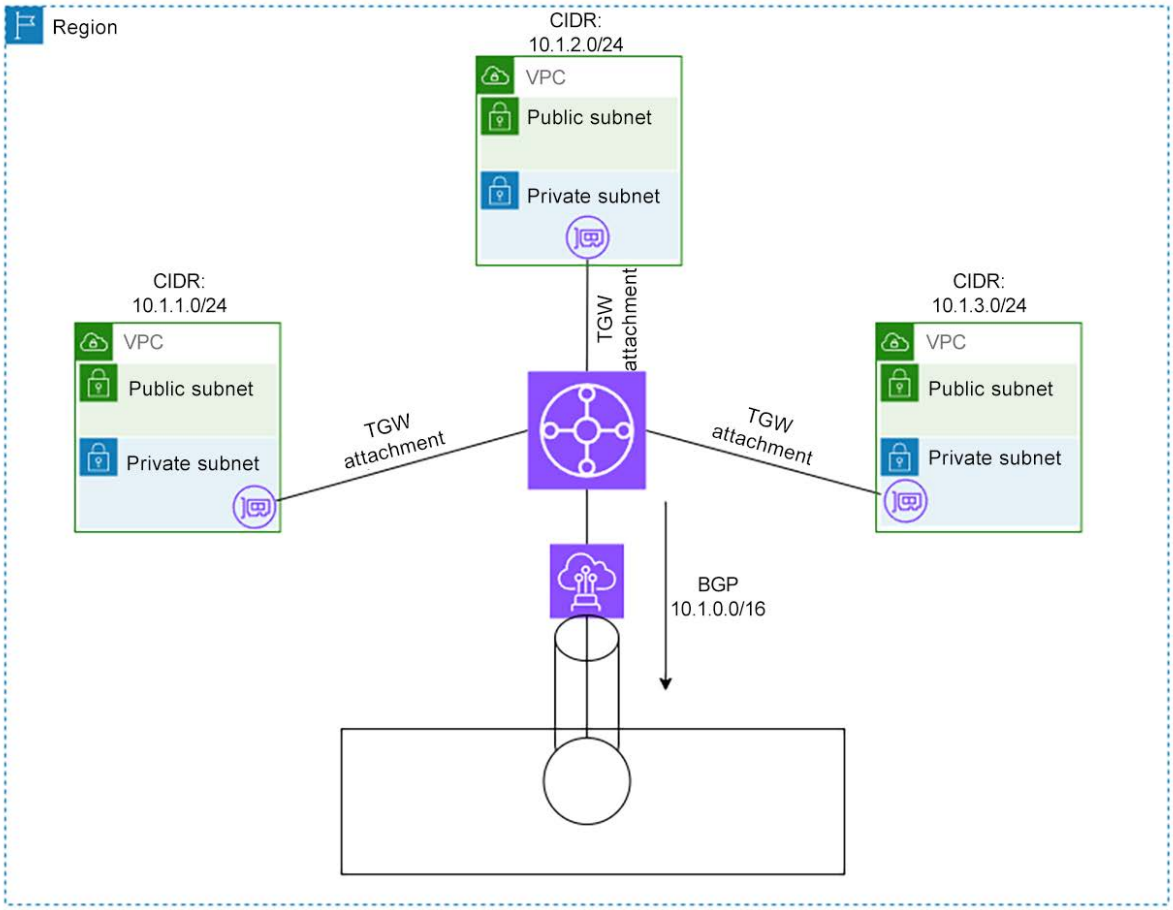


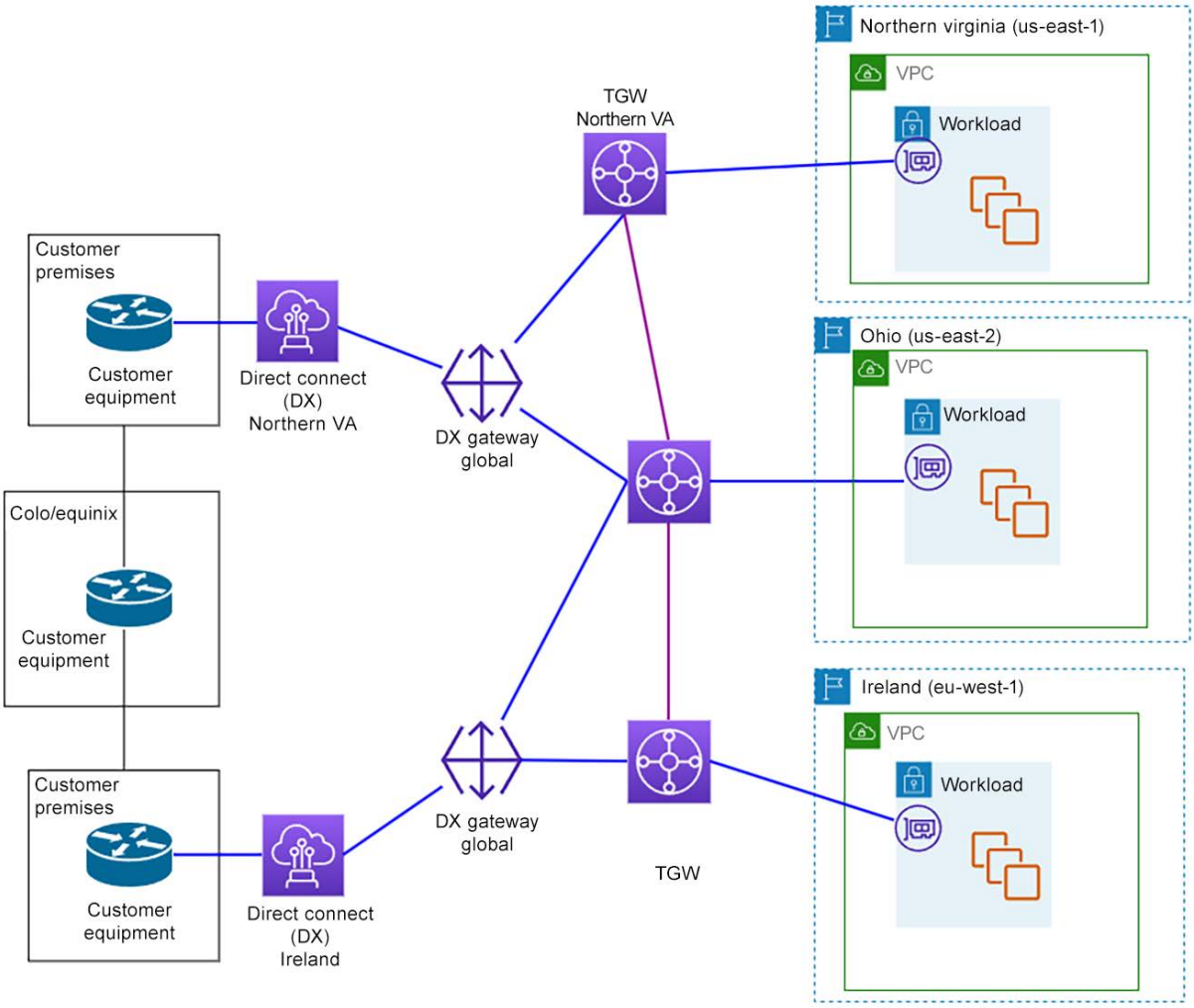


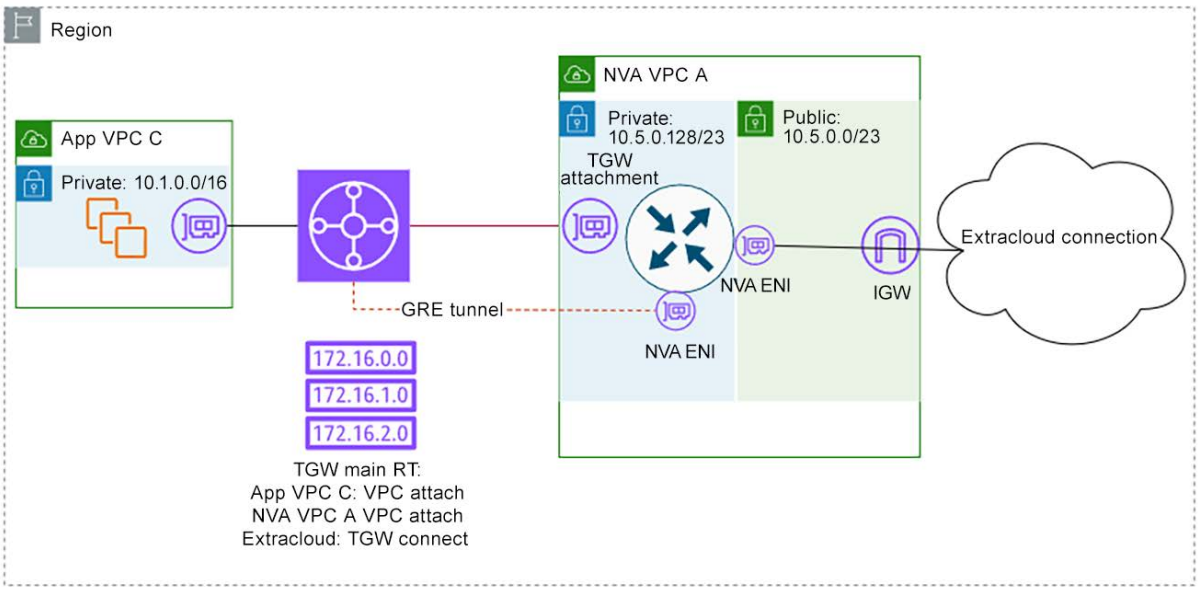

Region
VPC
AZ-A public subnet
AZ-B private subnet
AZ-A private subnet

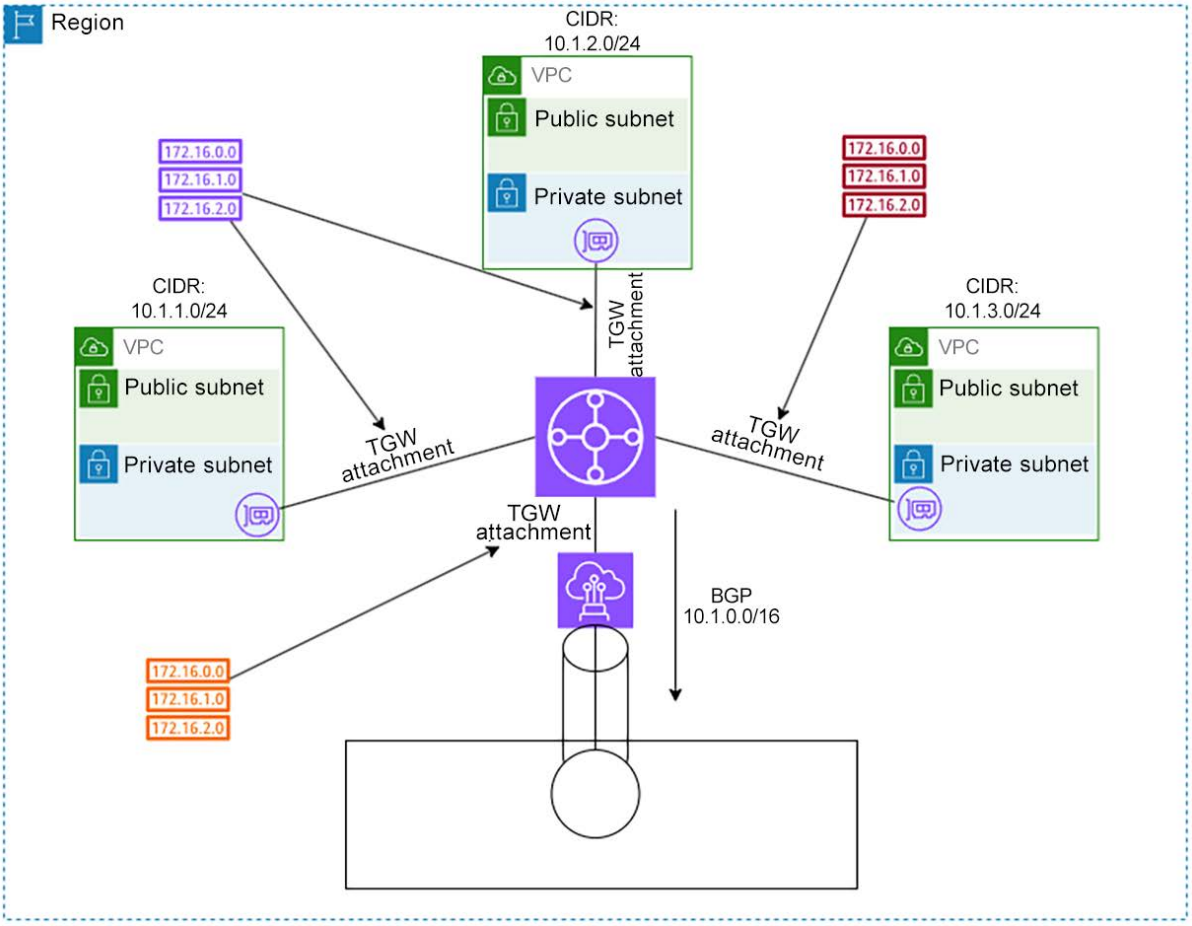

Region
App VPC 1
Public subnet
AZ A subnet
TGW attachment
Inspection VPC
TGW attach A
Appliance A
TGW attachment
TGW attach B
Appliance B
TGW attachment
App VPC 2
Public subnet
AZ B subnet

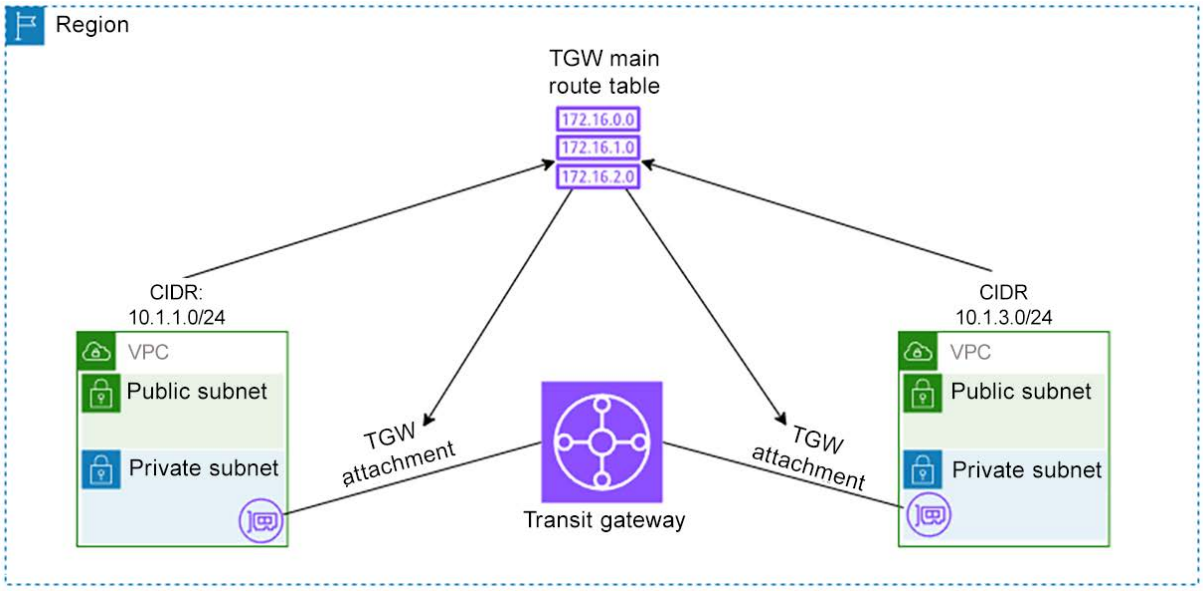

AWS
region
VPC
VPC
Customer
data center
Transit VIF
AWS
direct
connect
AWS
region
VPC
VPC

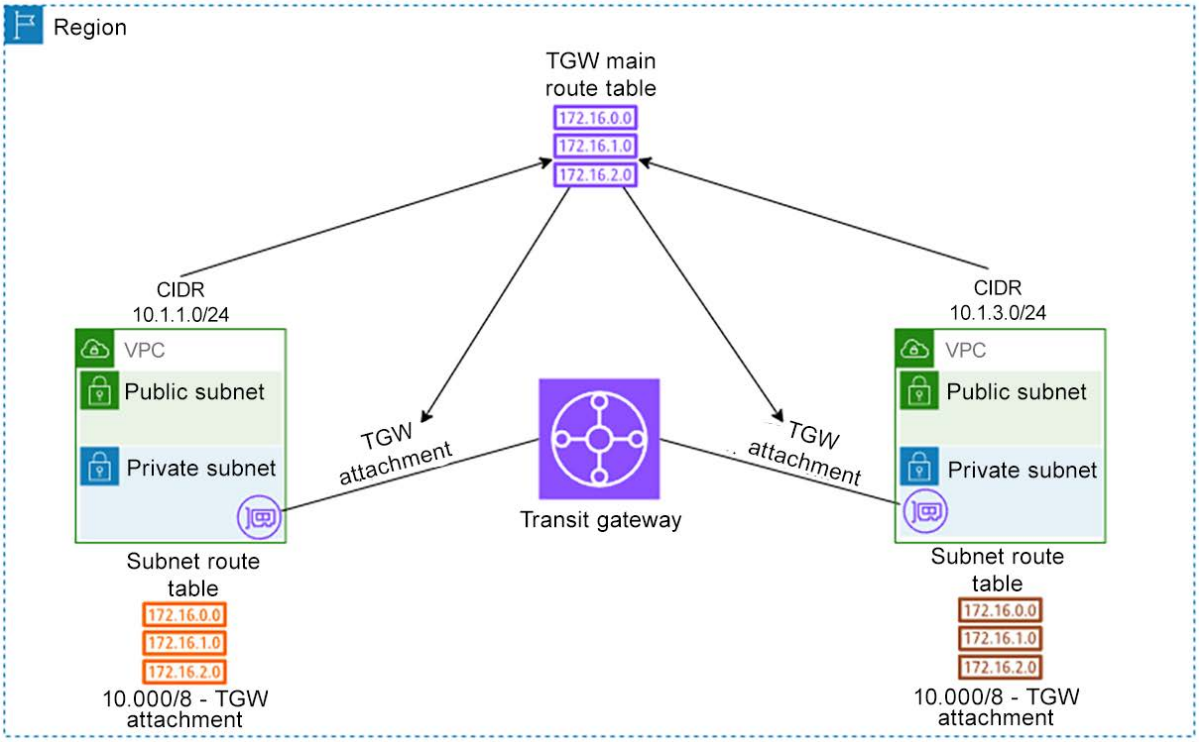

Region
CIDR:
10.1.2.0/24
VPC
Public subnet
Private subnet
CIDR:
10.1.1.0/24
VPC
Public subnet
Private subnet
TGW
attachment
CIDR:
10.1.3.0/24
VPC
Public subnet
Private subnet
TGW
attachment
TGW
attachment
BGP
10.1.0.0/16

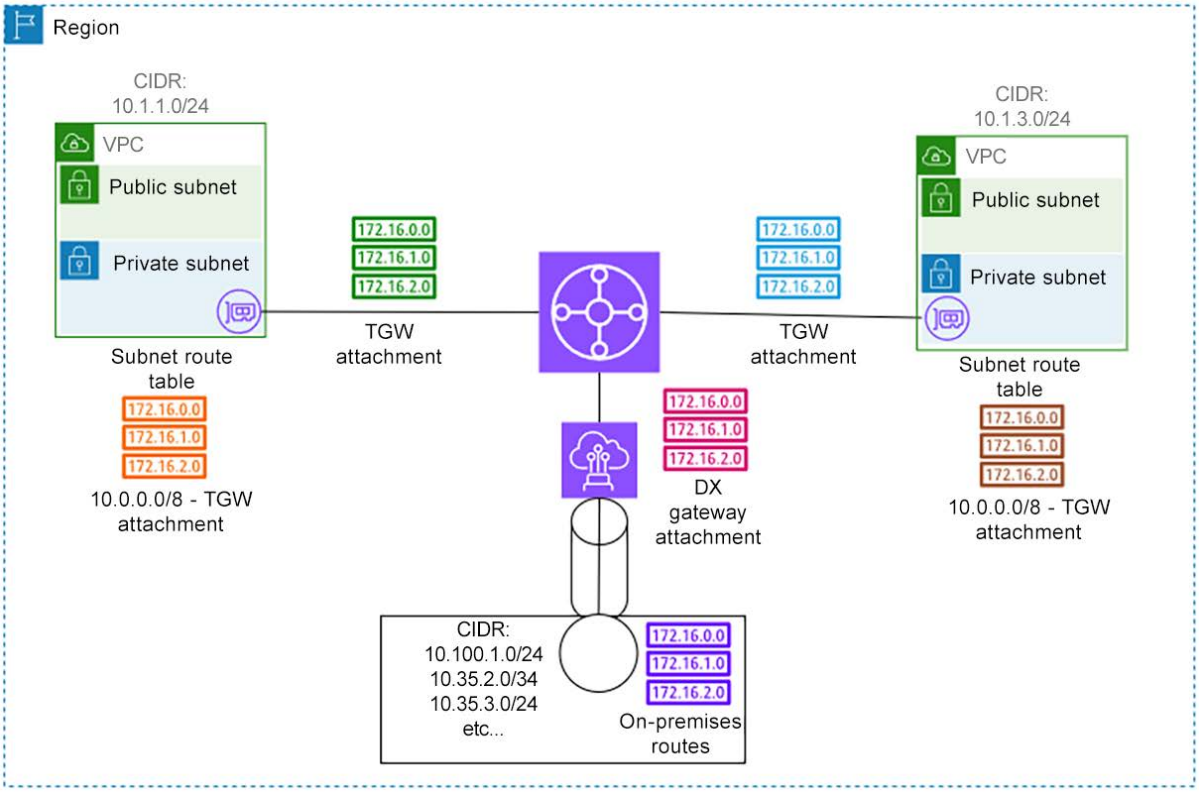

Northern virginia (us-east-1)
VPC
Workload
TGW
Northern VA
Customer
premises
Customer
equipment
Direct connect
(DX)
Northern VA
DX gateway
global
Ohio (us-east-2)
VPC
Workload
Colo/equinix
Customer
equipment
Ireland (eu-west-1)
VPC
Workload
Customer
premises
Customer
equipment
DX gateway
global
TGW
Direct connect
(DX)
Ireland

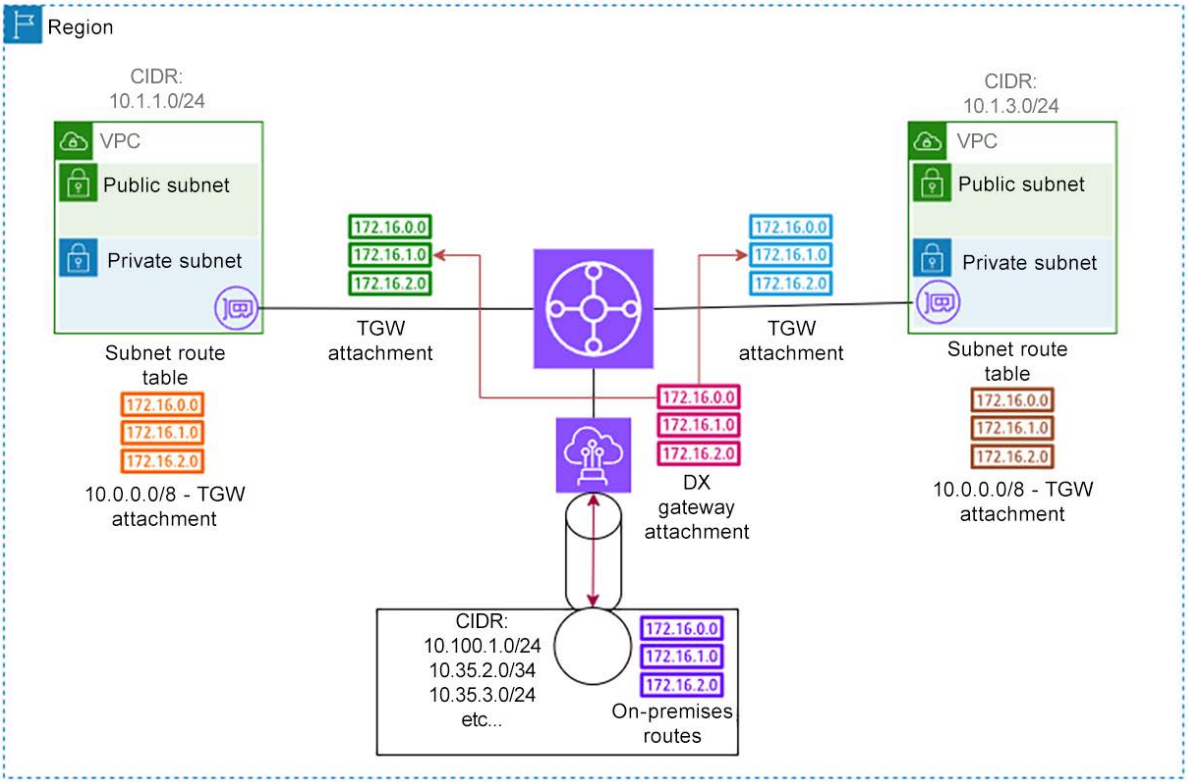

Region
NVA VPC A
Private:
10.5.0.128/23
Public:
10.5.0.0/23
TGW
attachment
App VPC C
Private: 10.1.0.0/16
Extracloud connection
NVA ENI
IGW
GRE tunnel
NVA ENI
172.16.0.0
172.16.1.0
172.16.2.0
TGW main RT:
App VPC C: VPC attach
NVA VPC A VPC attach
Extracloud: TGW connect

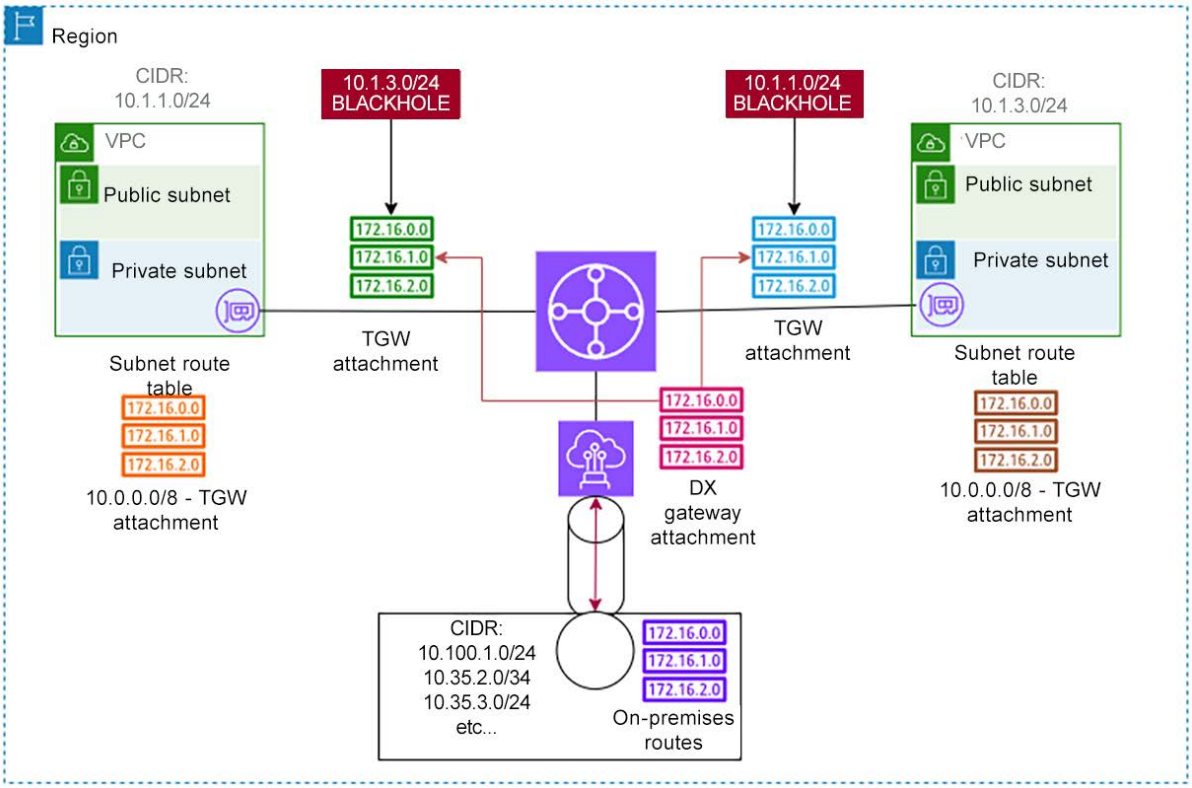

Region
CIDR:
10.1.2.0/24
VPC
Public subnet
Private subnet
172.16.0.0
172.16.1.0
172.16.2.0
CIDR:
10.1.1.0/24
VPC
Public subnet
Private subnet
TGW attachment
TGW attachment
TGW attachment
TGW attachment
CIDR:
10.1.3.0/24
VPC
Public subnet
Private subnet
BGP
10.1.0.0/16
172.16.0.0
172.16.1.0
172.16.2.0

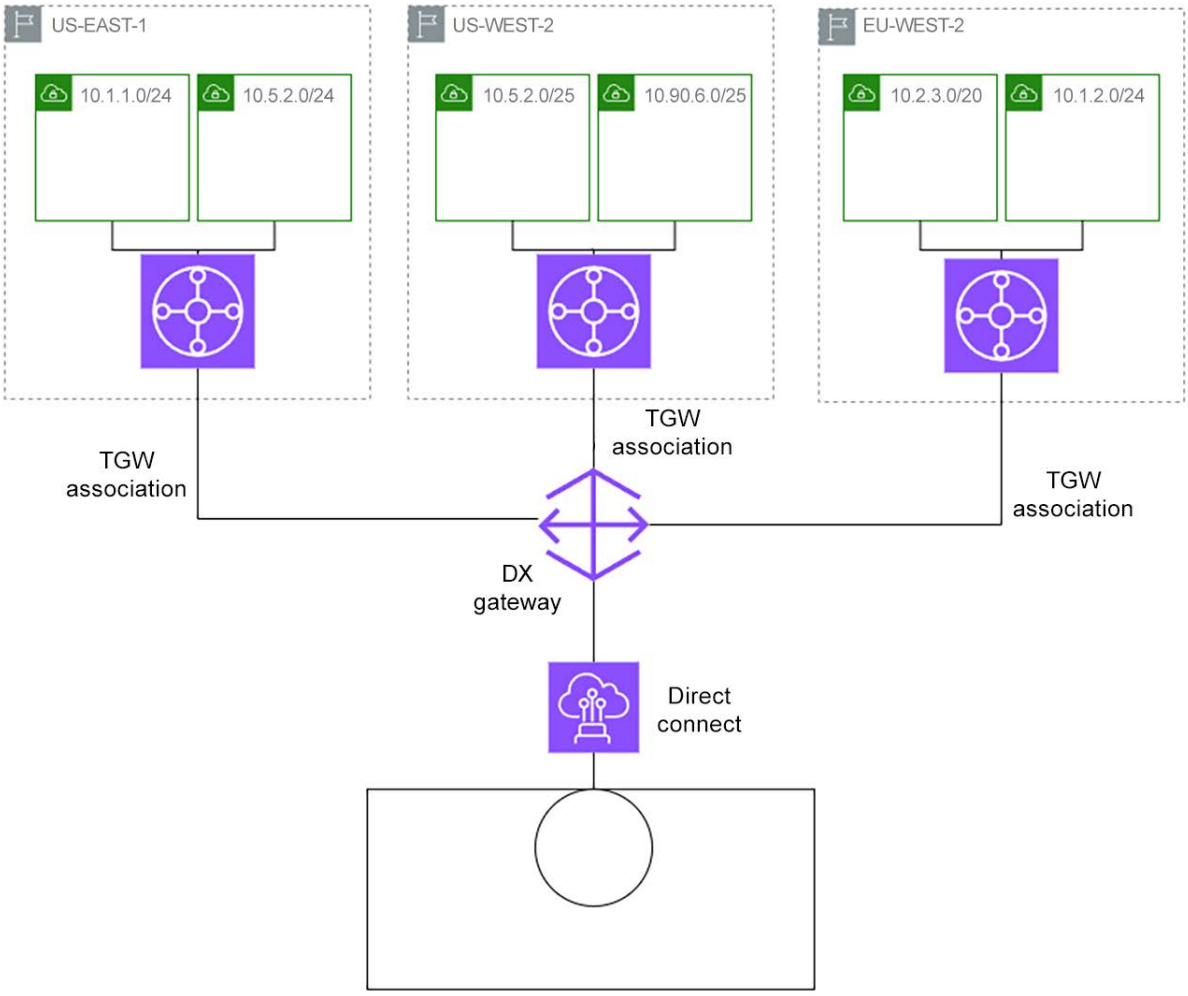

Region
TGW main
route table
172.16.0.0
172.16.1.0
172.16.2.0
CIDR:
10.1.1.0/24
VPC
Public subnet
Private subnet
TGW attachment
Transit gateway
TGW attachment
CIDR
10.1.3.0/24
VPC
Public subnet
Private subnet

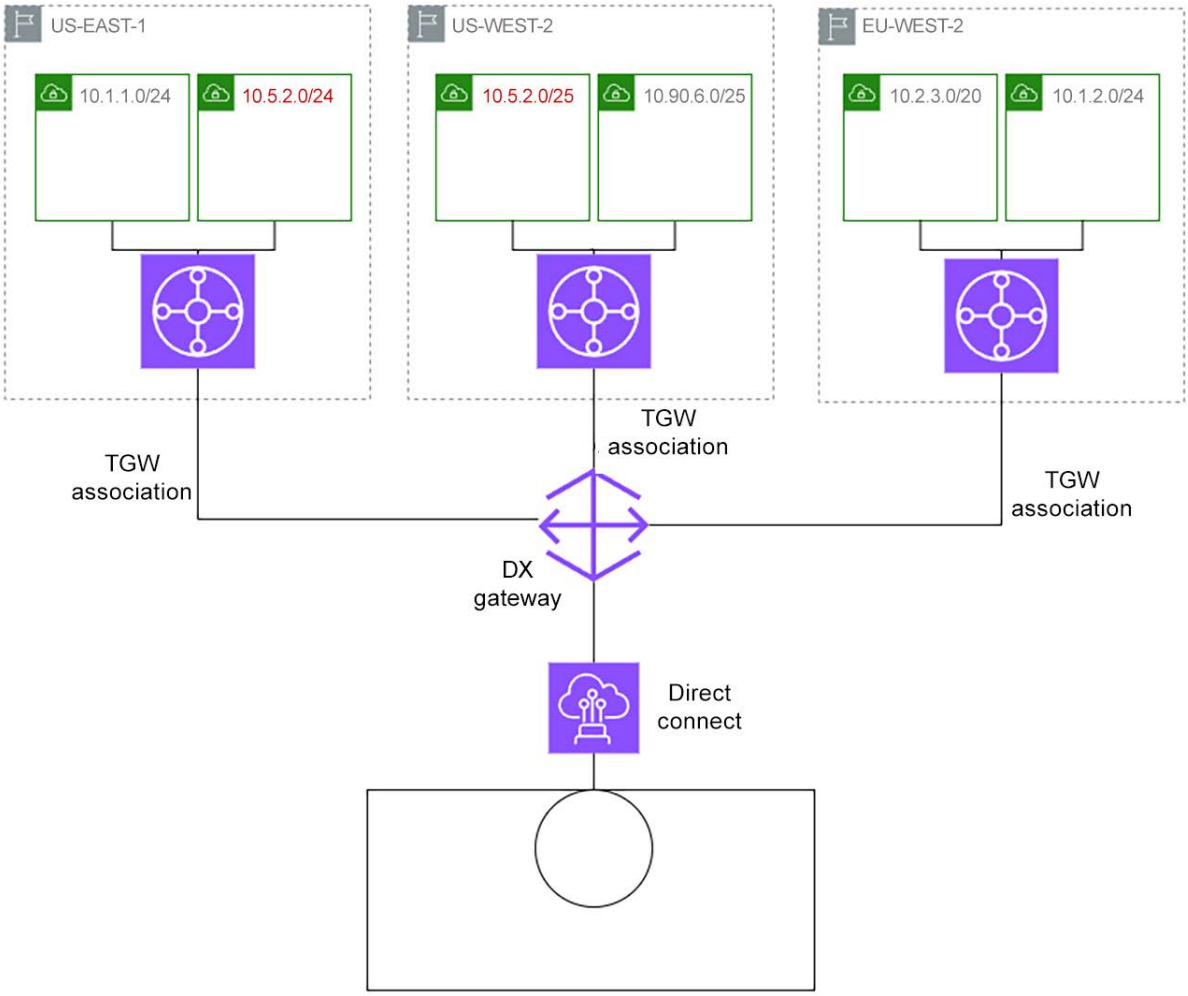

Region
TGW main route table
172.16.0.0
172.16.1.0
172.16.2.0
CIDR 10.1.1.0/24
CIDR 10.1.3.0/24
VPC
Public subnet
Private subnet
TGW attachment
TGW attachment
Transit gateway
Subnet route table
172.16.0.0
172.16.1.0
172.16.2.0
10.000/8 - TGW attachment

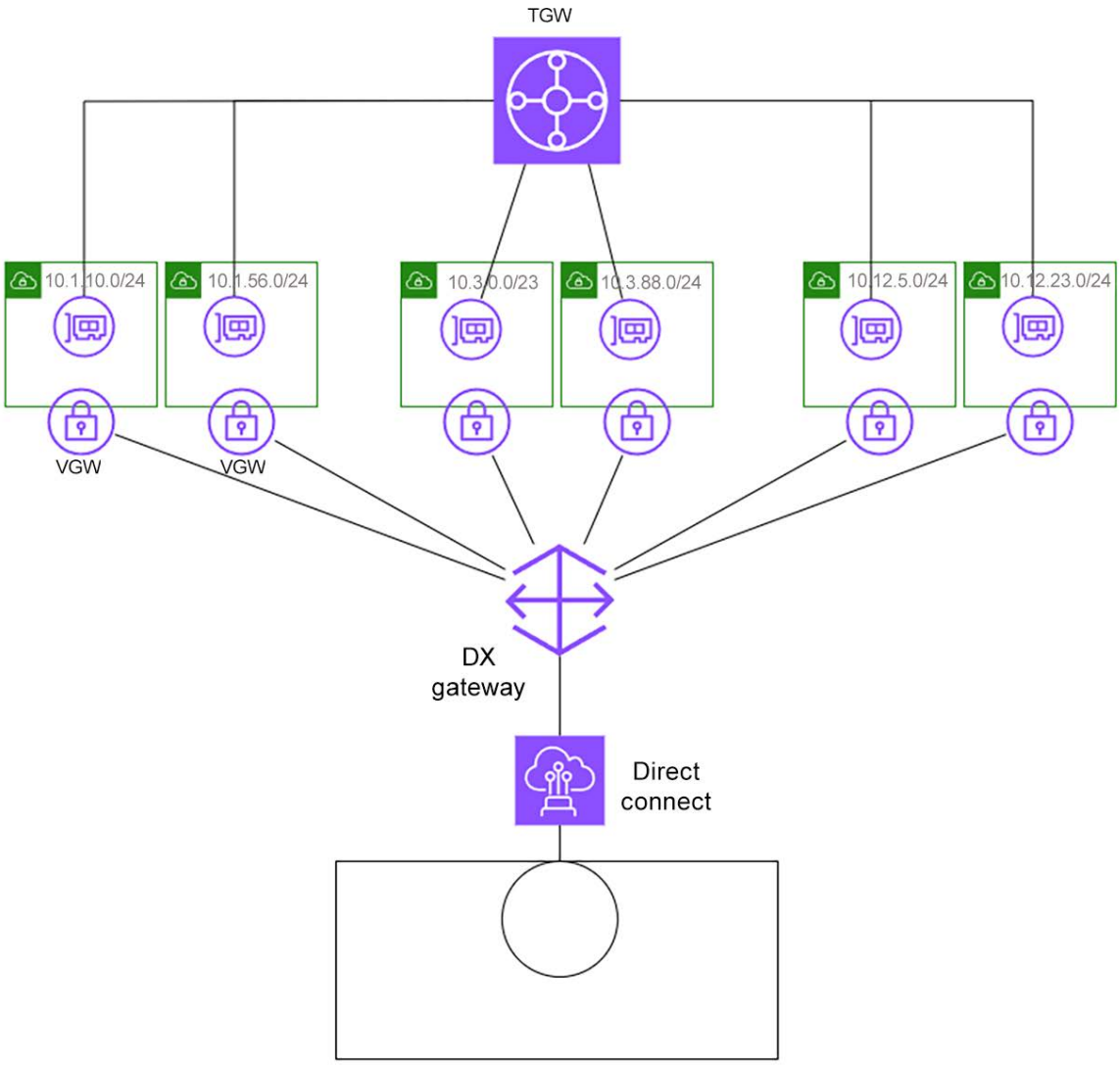

Region
CIDR: 10.1.1.0/24
CIDR: 10.1.3.0/24
VPC
Public subnet
Private subnet
172.16.0.0
172.16.1.0
172.16.2.0
TGW attachment
TGW attachment
Subnet route table
10.0.0.0/8 - TGW attachment
DX gateway attachment
CIDR: 10.100.1.0/24 10.35.2.0/34 10.35.3.0/24 etc...
On-premises routes

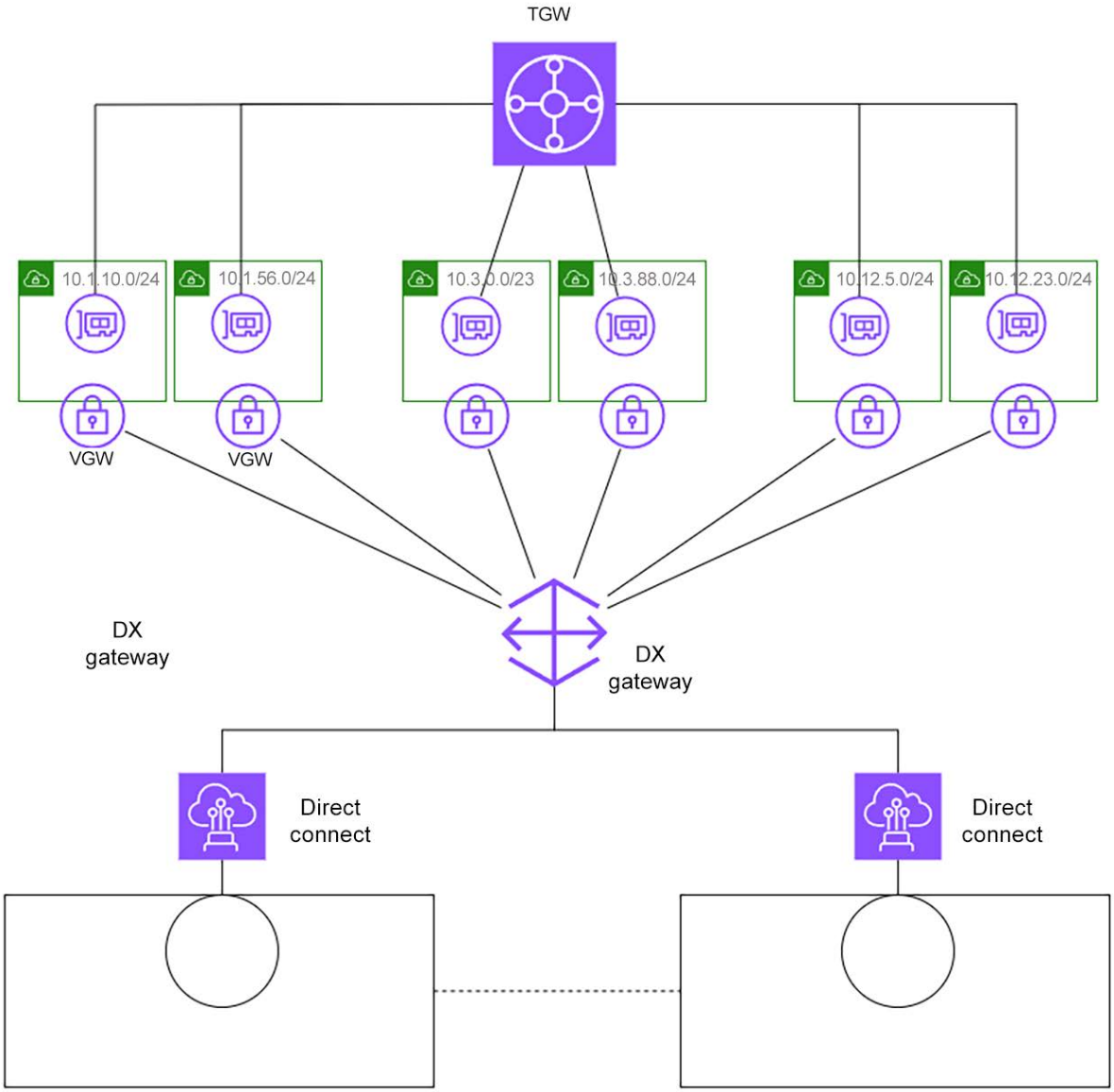

Region
CIDR:
10.1.1.0/24
VPC
Public subnet
Private subnet
Subnet route table
172.16.0.0
172.16.1.0
172.16.2.0
10.0.0.0/8 - TGW attachment
TGW attachment
DX gateway attachment
CIDR:
10.1.3.0/24
VPC
Public subnet
Private subnet
Subnet route table
10.0.0.0/8 - TGW attachment
CIDR:
10.100.1.0/24
10.35.2.0/34
10.35.3.0/24
etc...
On-premises routes

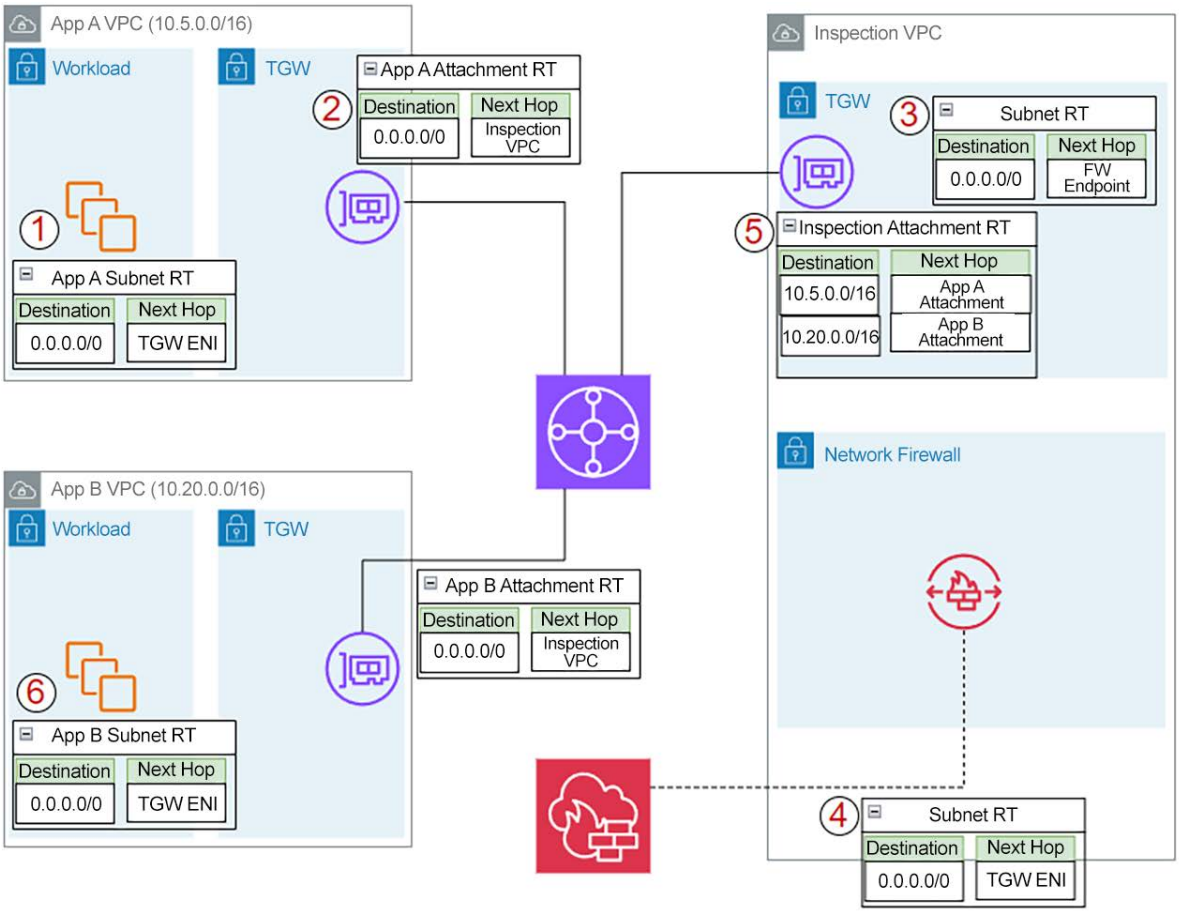

Region
CIDR:
10.1.1.0/24
10.1.3.0/24 BLACKHOLE
10.1.1.0/24 BLACKHOLE
CIDR:
10.1.3.0/24
VPC
Public subnet
Private subnet
Subnet route table
172.16.0.0
172.16.1.0
172.16.2.0
10.0.0.0/8 - TGW attachment
TGW attachment
DX gateway attachment
CIDR:
10.100.1.0/24
10.35.2.0/34
10.35.3.0/24
etc...
On-premises routes

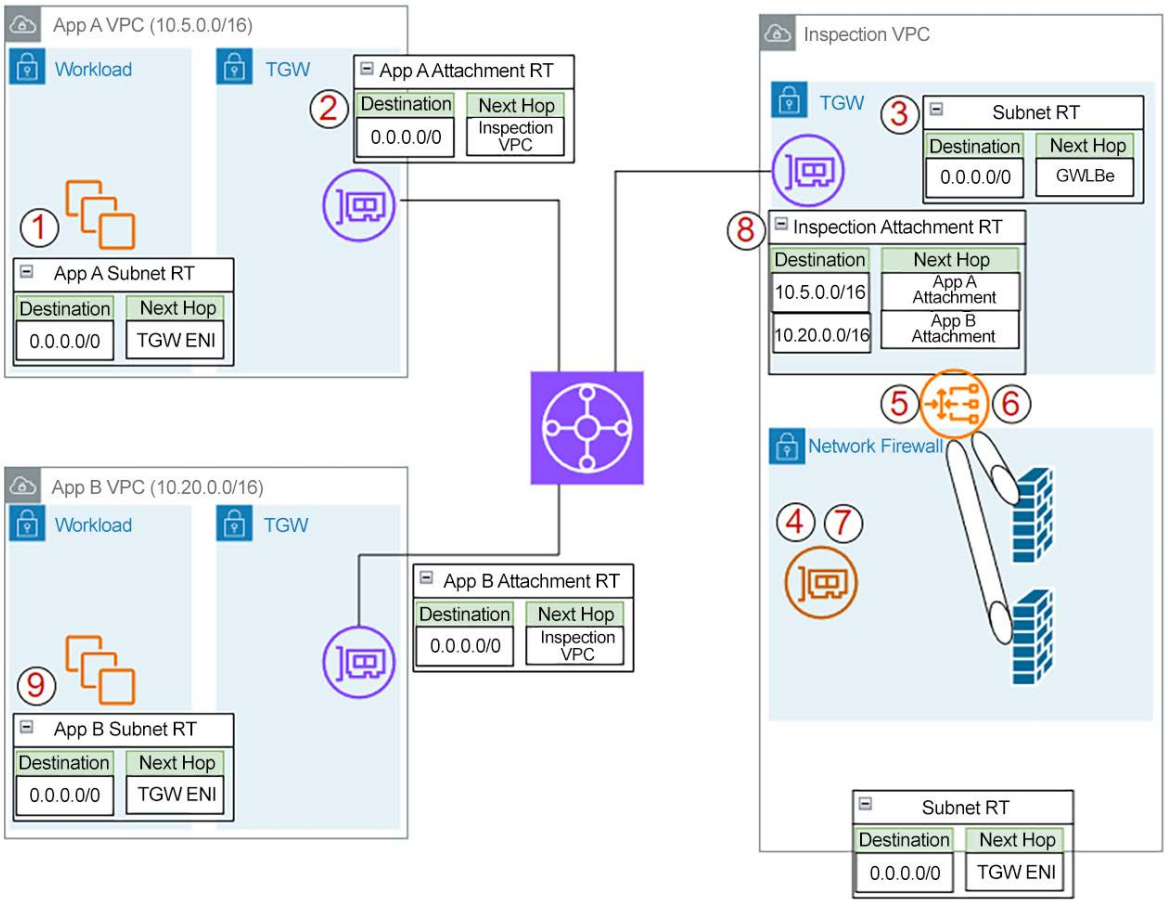

US-EAST-1
10.1.1.0/24
10.5.2.0/24
US-WEST-2
10.5.2.0/25
10.90.6.0/25
EU-WEST-2
10.2.3.0/20
10.1.2.0/24
TGW association
TGW association
TGW association
DX gateway
Direct connect


US-EAST-1
10.1.1.0/24
10.5.2.0/24
US-WEST-2
10.5.2.0/25
10.90.6.0/25
EU-WEST-2
10.2.3.0/20
10.1.2.0/24
TGW association
TGW association
TGW association
DX gateway
Direct connect

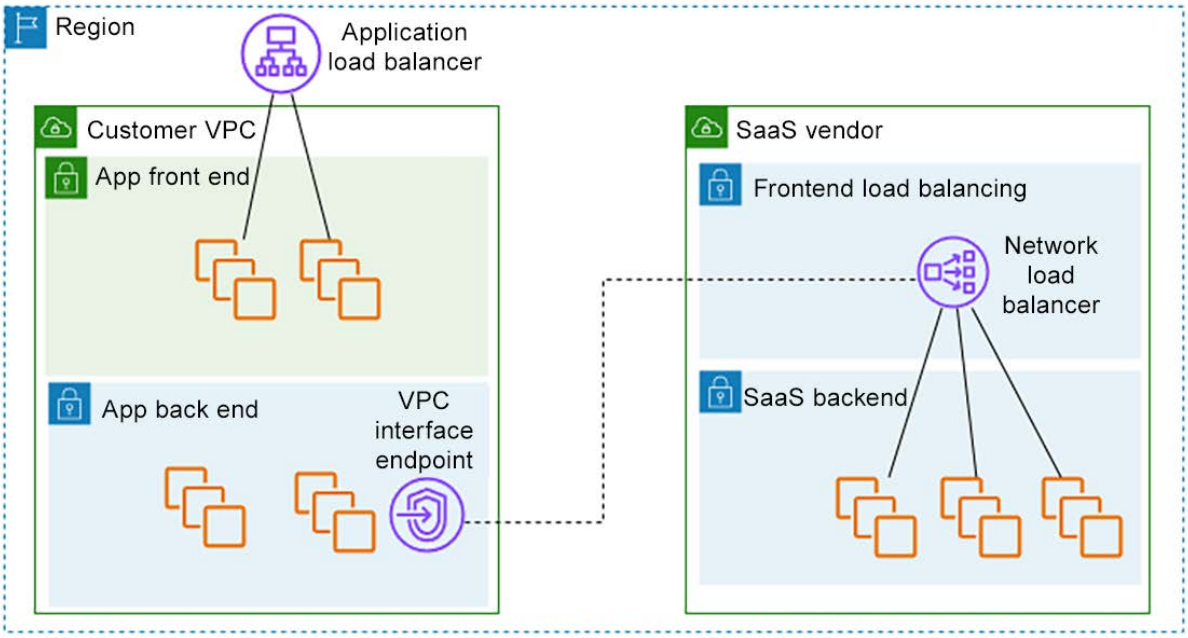

TGW
10.1.10.0/24
10.1.56.0/24
10.3.0.0/23
10.3.88.0/24
10.12.5.0/24
10.12.23.0/24
VGW
VGW
DX
gateway
Direct
connect

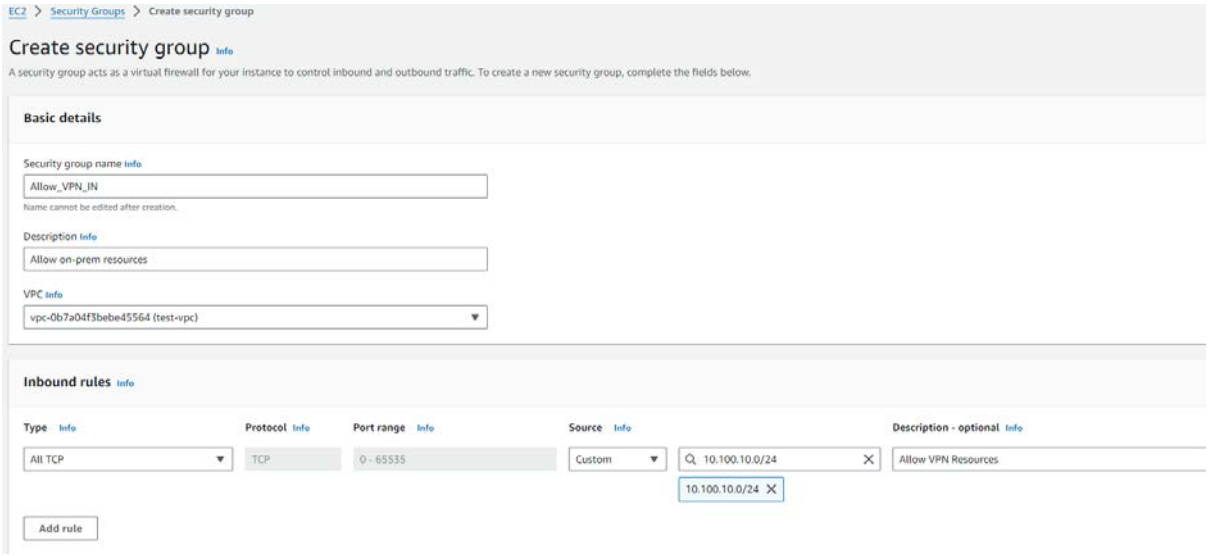

TGW
10.1.10.0/24
10.1.56.0/24
10.3.0.0/23
10.3.88.0/24
10.12.5.0/24
10.12.23.0/24
VGW
VGW
DX
gateway
DX
gateway
Direct
connect
Direct
connect


App A VPC (10.5.0.0/16)
Workload
TGW
App A Attachment RT
Destination
Next Hop
0.0.0.0/0
Inspection VPC
1
App A Subnet RT
Destination
Next Hop
0.0.0.0/0
TGW ENI
Inspection VPC
TGW
3
Subnet RT
Destination
Next Hop
0.0.0.0/0
FW Endpoint
5
Inspection Attachment RT
Destination
Next Hop
10.5.0.0/16
App A Attachment
10.20.0.0/16
App B Attachment
Network Firewall
App B VPC (10.20.0.0/16)
Workload
TGW
App B Attachment RT
Destination
Next Hop
0.0.0.0/0
Inspection VPC
6
App B Subnet RT
Destination
Next Hop
0.0.0.0/0
TGW ENI
4
Subnet RT
Destination
Next Hop
0.0.0.0/0
TGW ENI


App A VPC (10.5.0.0/16)
Workload
TGW
App A Attachment RT
Destination
Next Hop
0.0.0.0/0
Inspection VPC
1
App A Subnet RT
Destination
Next Hop
0.0.0.0/0
TGW ENI
Inspection VPC
TGW
3
Subnet RT
Destination
Next Hop
0.0.0.0/0
GWLBe
8
Inspection Attachment RT
Destination
Next Hop
10.5.0.0/16
App A Attachment
10.20.0.0/16
App B Attachment
5
6
Network Firewall
4
7
App B VPC (10.20.0.0/16)
Workload
TGW
App B Attachment RT
Destination
Next Hop
0.0.0.0/0
Inspection VPC
9
App B Subnet RT
Destination
Next Hop
0.0.0.0/0
TGW ENI
Subnet RT
Destination
Next Hop
0.0.0.0/0
TGW ENI

Chapter 6: Connecting Third-Party Networks to AWS





Create VPN connection Info

Select the resources and additional configuration options that you want to use for the site-to-site VPN connection.

Details

Name tag - *optional*

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

s2svpn

Value must be 256 characters or less in length.

Target gateway type Info

- (•) Virtual private gateway
- ( ) Transit gateway
- ( ) Not associated

Virtual private gateway

vgw-0ae6a6267b8dec93e ▼

Customer gateway Info

- (•) Existing
- ( ) New

Customer gateway ID

cgw-0b40ae5dfaf938e29 ▼

Routing options Info

- (•) Dynamic (requires BGP)
- ( ) Static

Local IPv4 network CIDR - *optional*

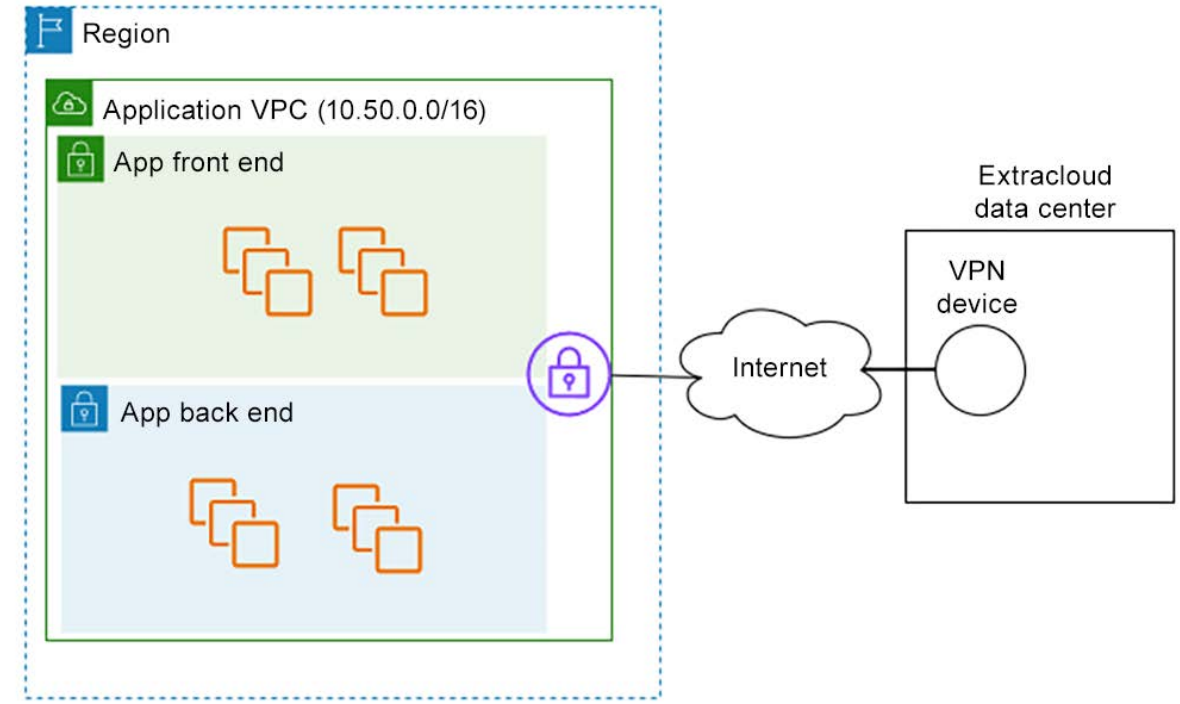
The IPv4 CIDR range on the customer gateway (on-premises) side that is allowed to communicate over the VPN tunnels. The default is 0.0.0.0/0.

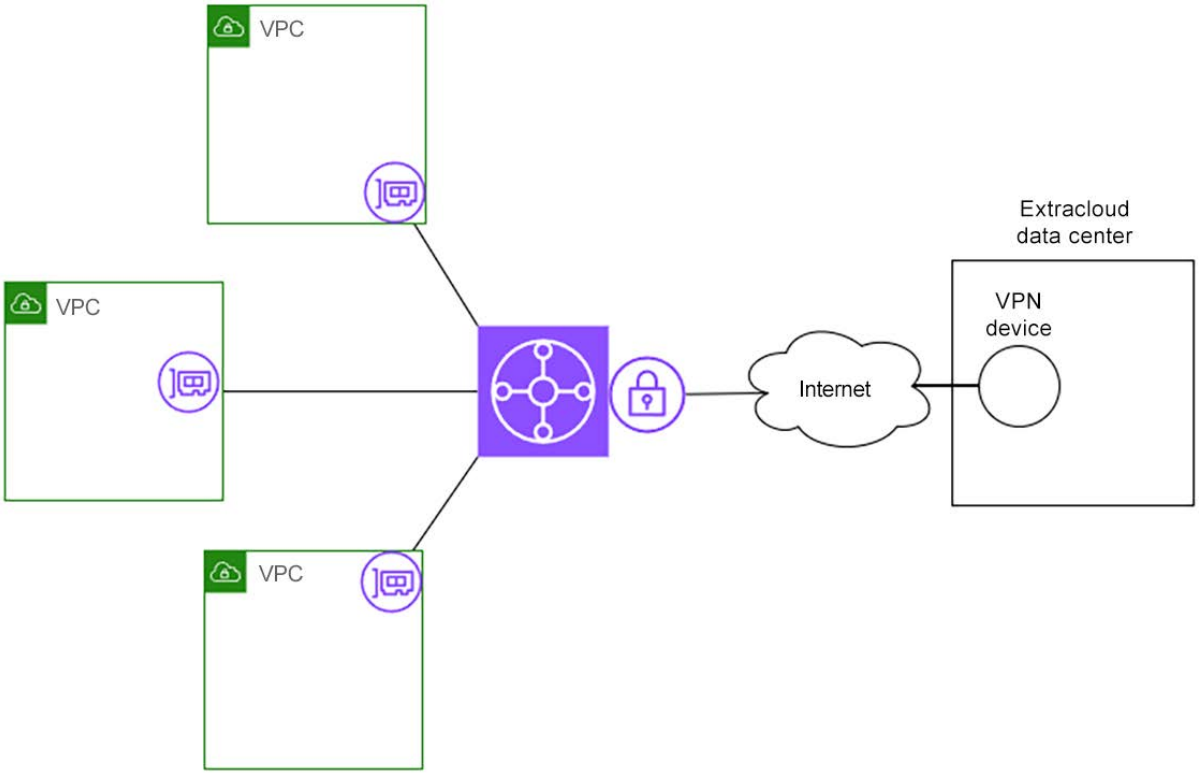
🔍 *0.0.0.0/0*

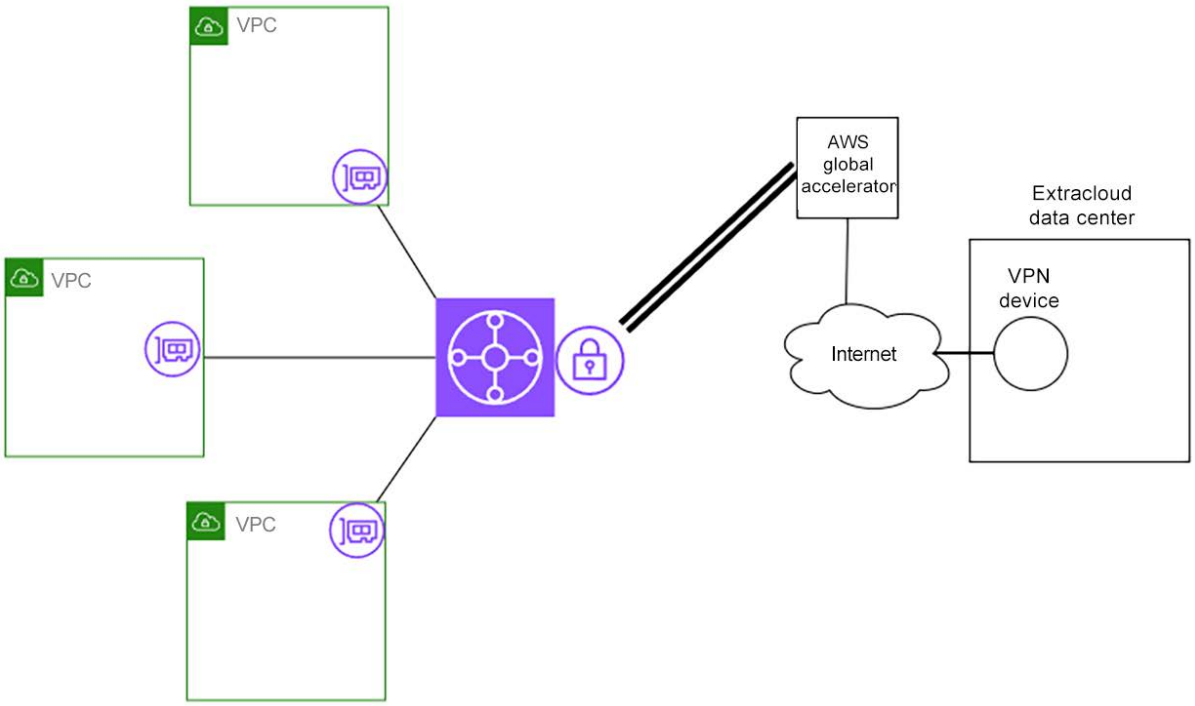
Remote IPv4 network CIDR - *optional*

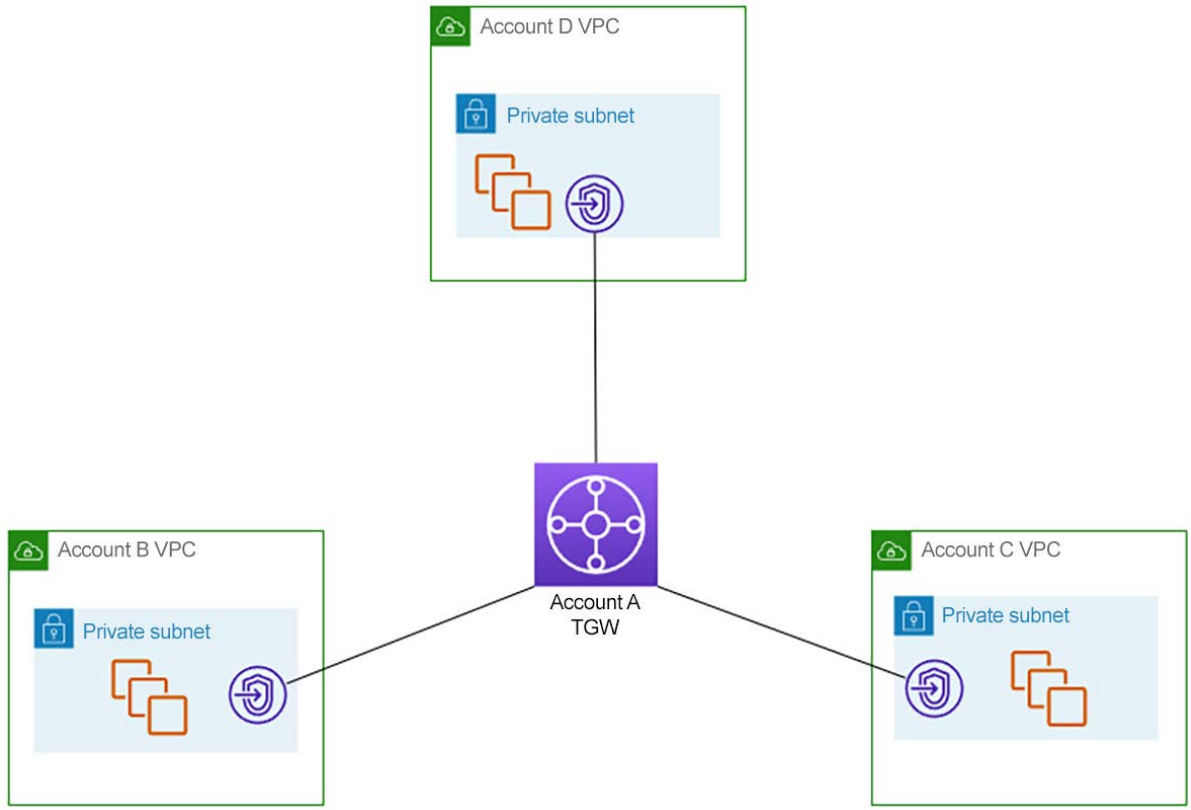
The IPv4 CIDR range on the AWS side that is allowed to communicate over the VPN tunnels. The default is 0.0.0.0/0.

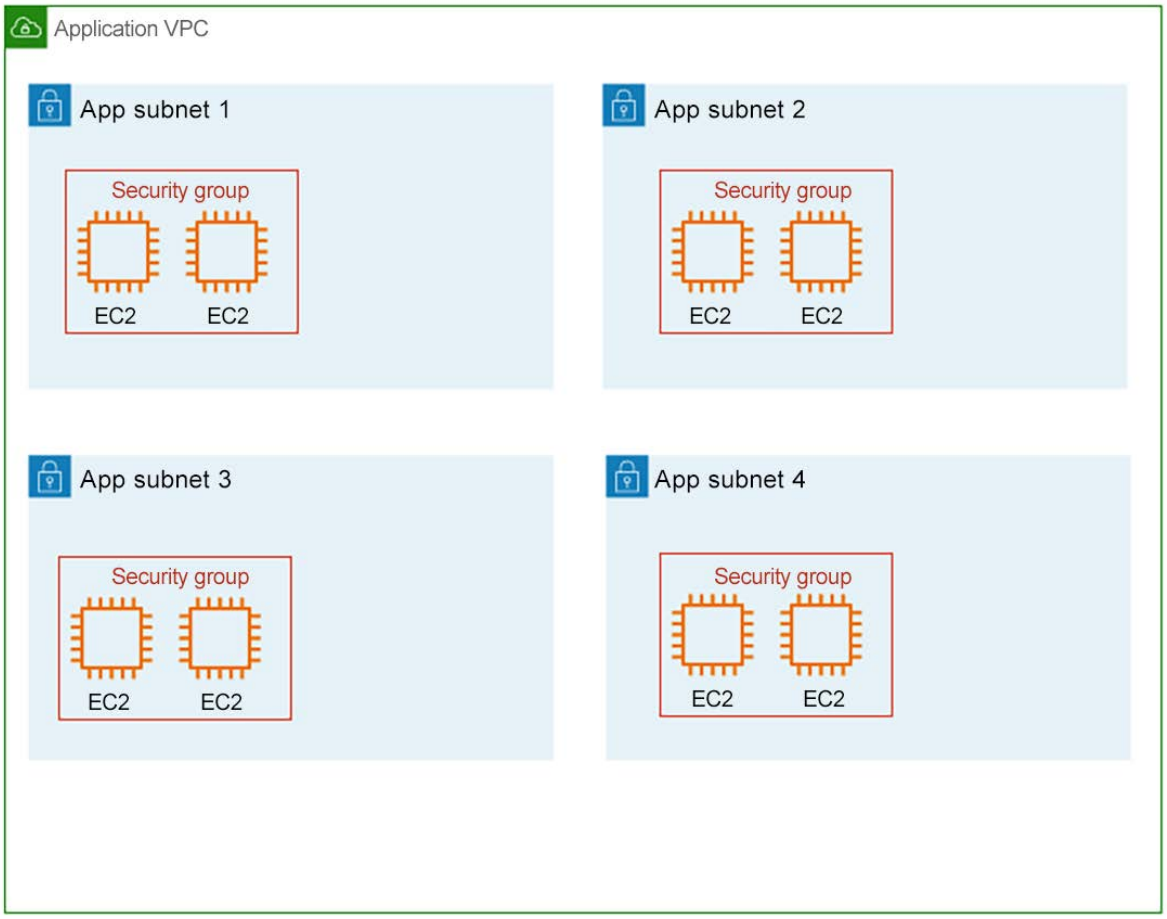
🔍 *0.0.0.0/0*

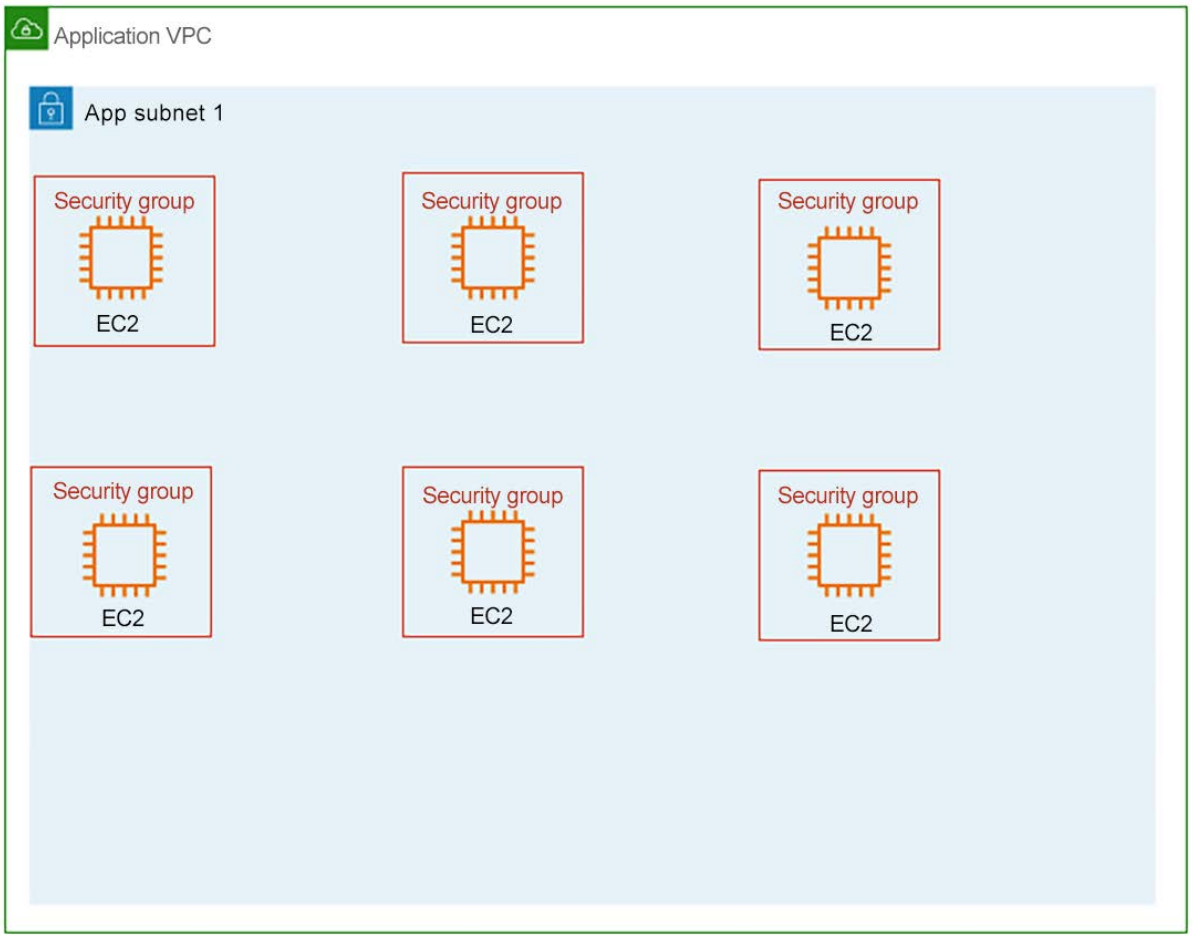

Region
Application VPC (10.50.0.0/16)
App front end
App back end
Extracloud
data center
VPN
device
Internet

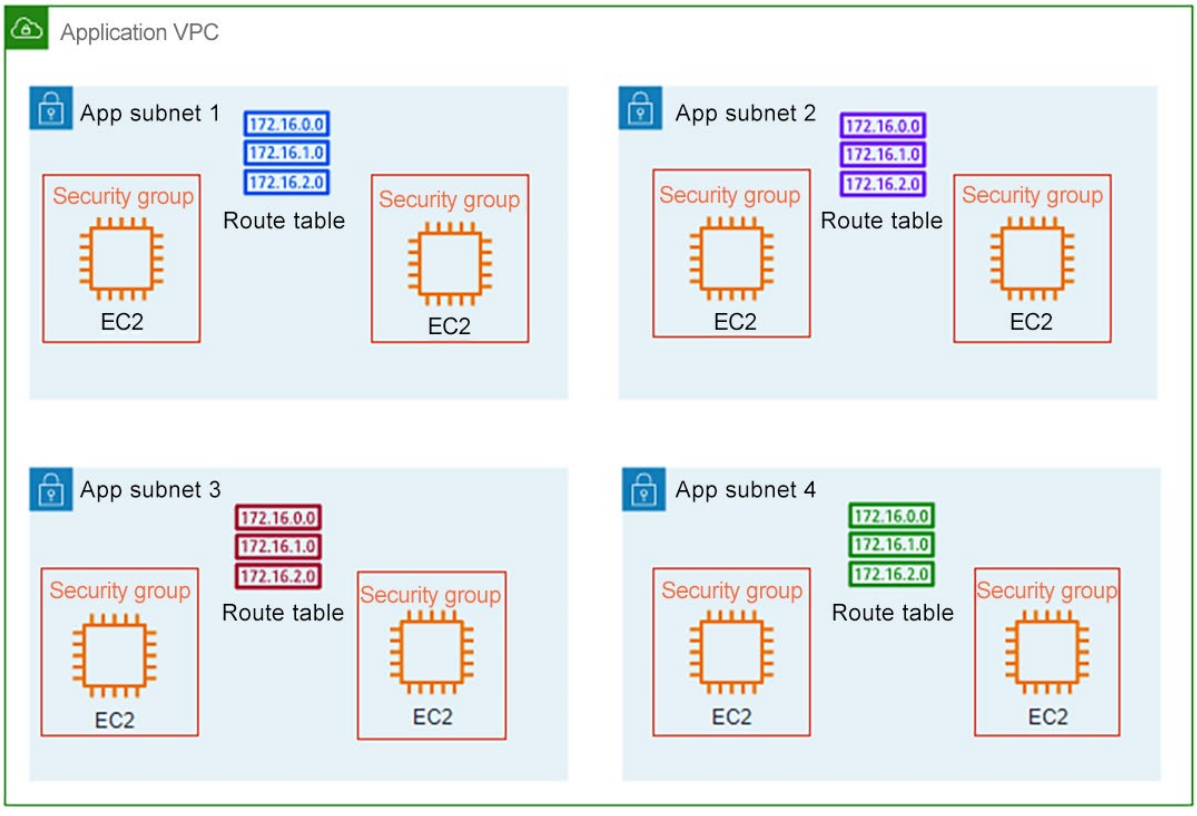

VPC
VPC
VPC
Extracloud
data center
VPN
device
Internet

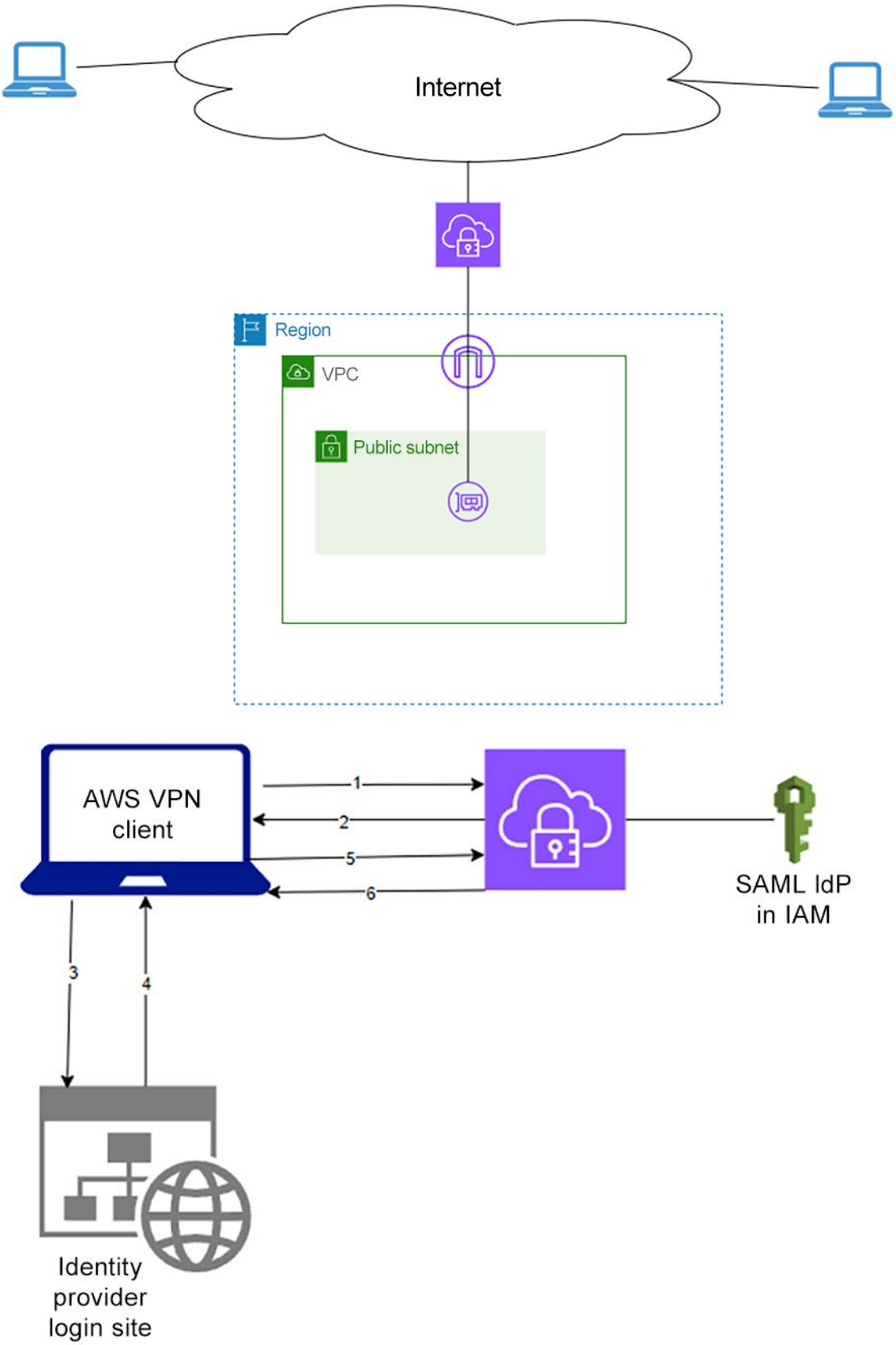

VPC
VPC
VPC
AWS
global
accelerator
Extracloud
data center
VPN
device
Internet

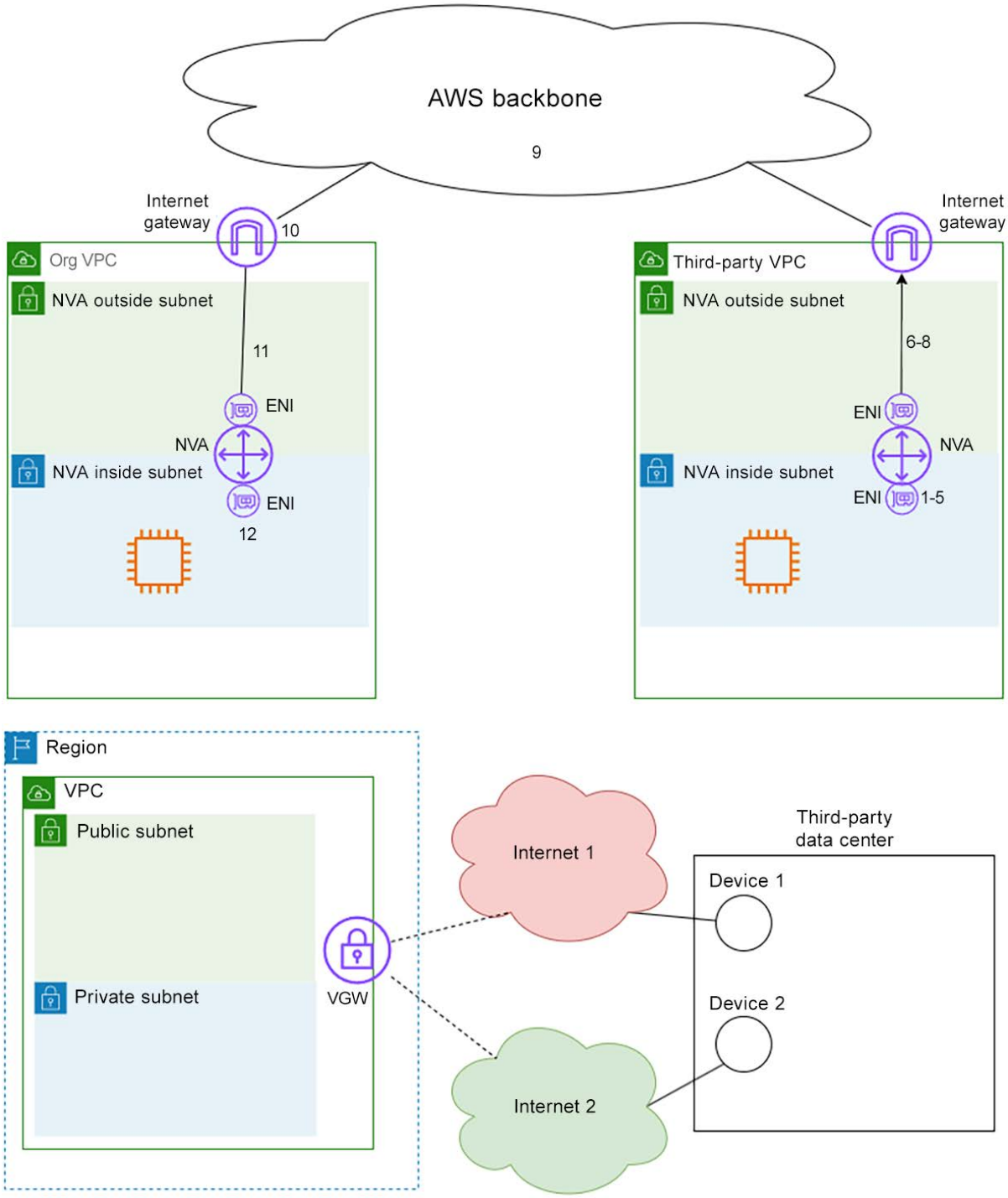

Account D VPC
Private subnet
Account A
TGW
Account B VPC
Private subnet
Account C VPC
Private subnet

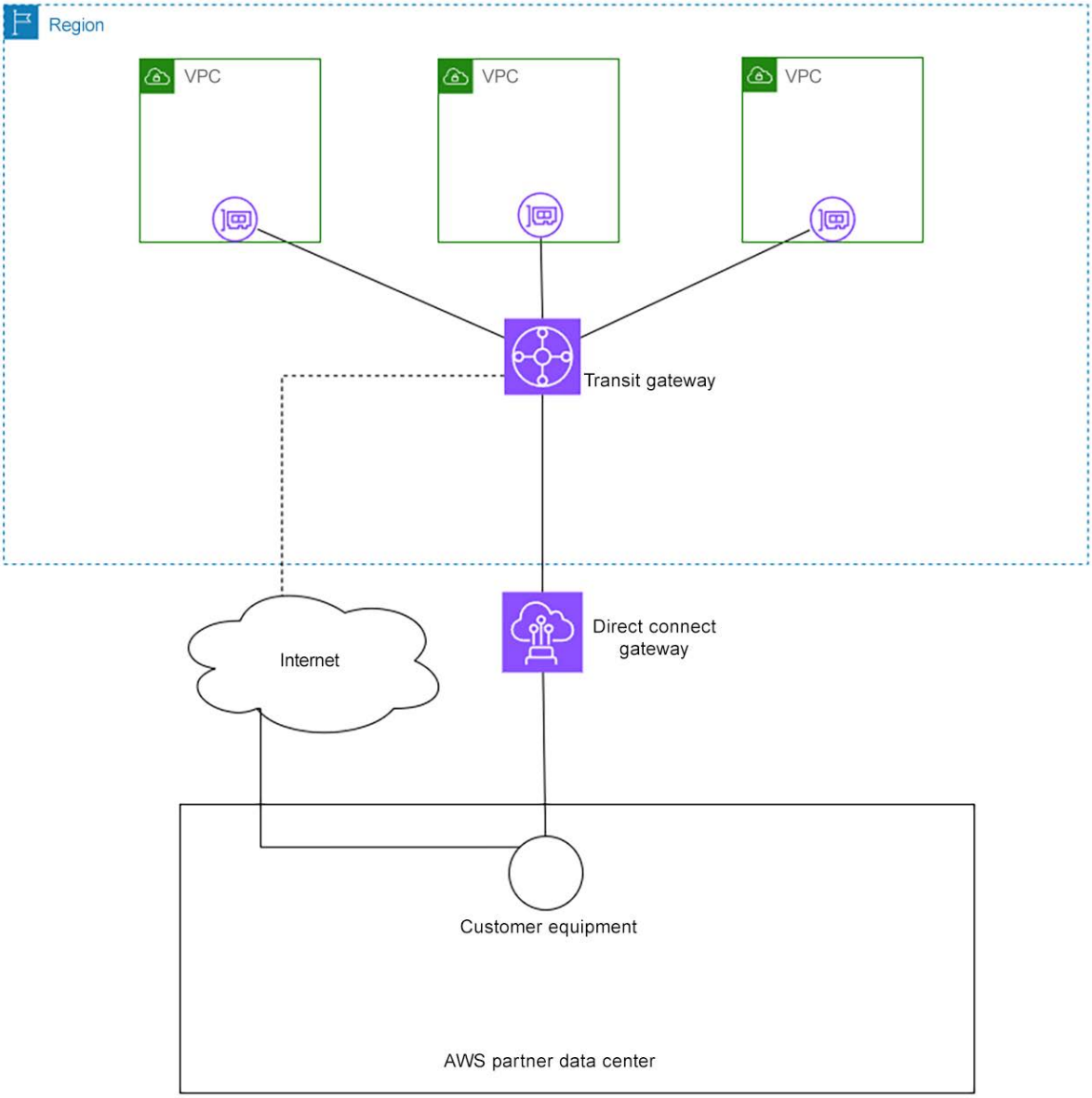

Application VPC
App subnet 1
Security group
EC2
EC2
App subnet 2
Security group
EC2
EC2
App subnet 3
Security group
EC2
EC2
App subnet 4
Security group
EC2
EC2

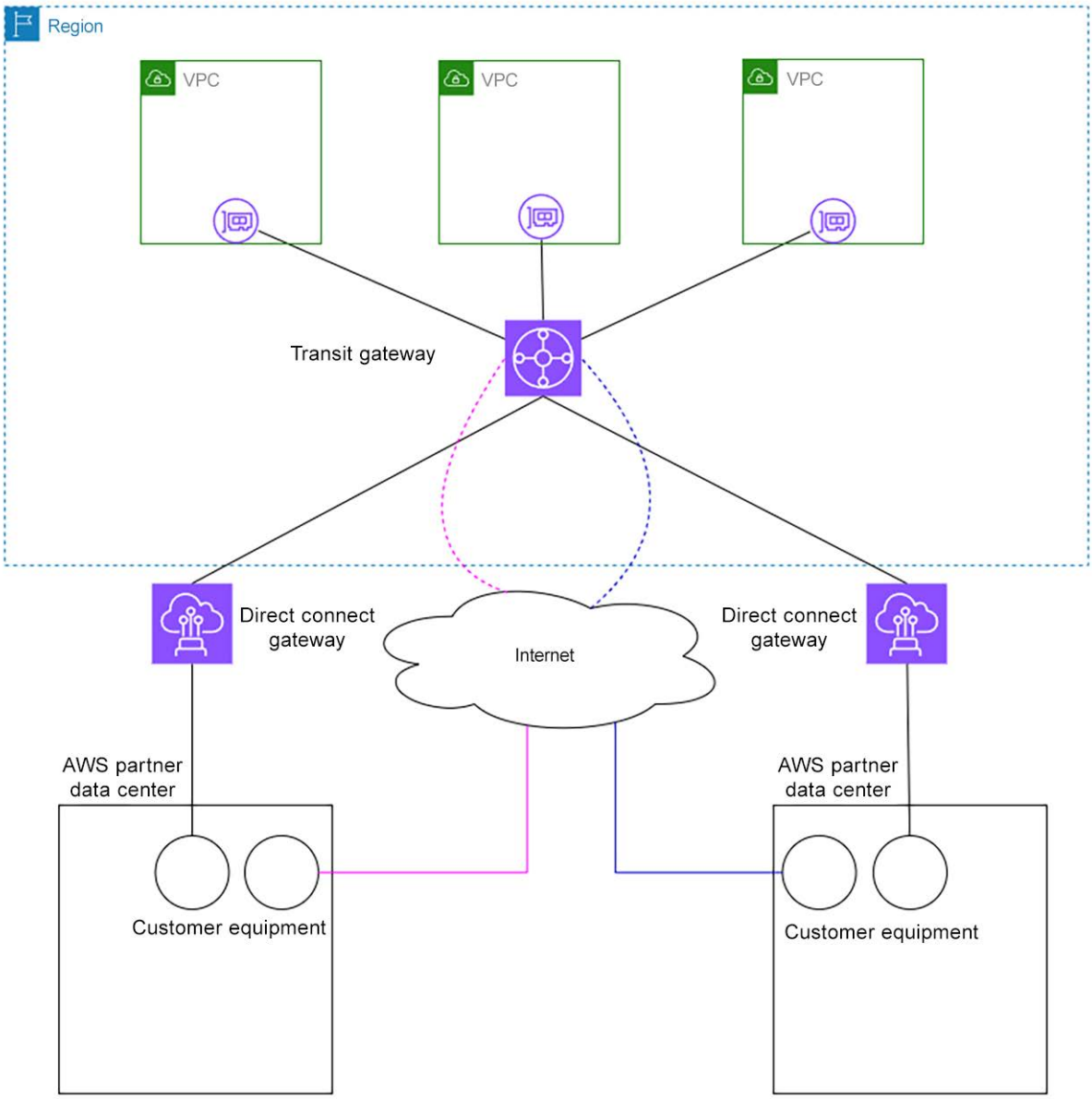

Application VPC
App subnet 1
Security group
EC2
Security group
EC2
Security group
EC2
Security group
EC2
Security group
EC2
Security group
EC2

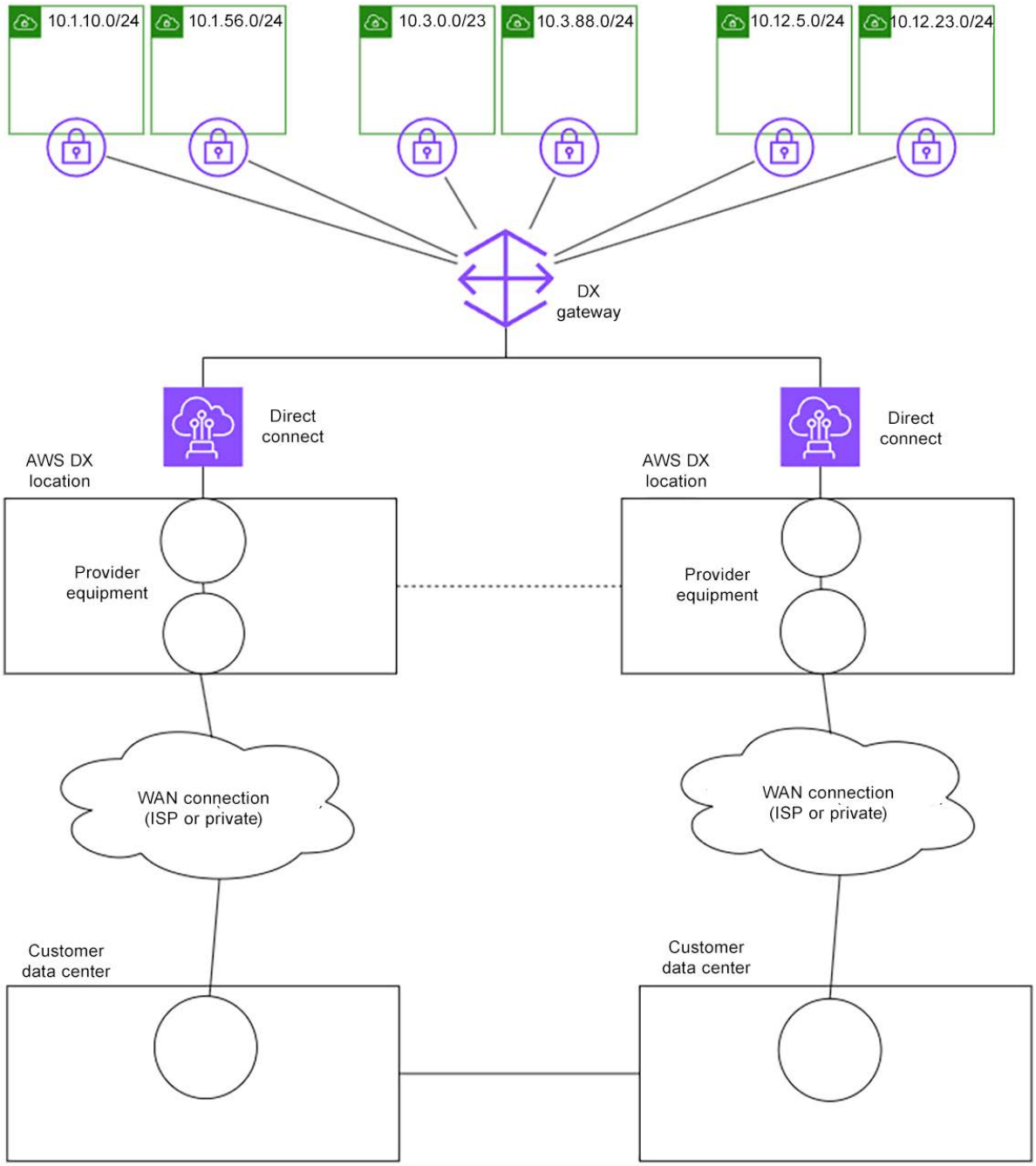

Application VPC
App subnet 1
172.16.0.0
172.16.1.0
172.16.2.0
Route table
Security group
EC2
Security group
EC2
App subnet 2
172.16.0.0
172.16.1.0
172.16.2.0
Route table
Security group
EC2
Security group
EC2
App subnet 3
172.16.0.0
172.16.1.0
172.16.2.0
Route table
Security group
EC2
Security group
EC2
App subnet 4
172.16.0.0
172.16.1.0
172.16.2.0
Route table
Security group
EC2
Security group
EC2

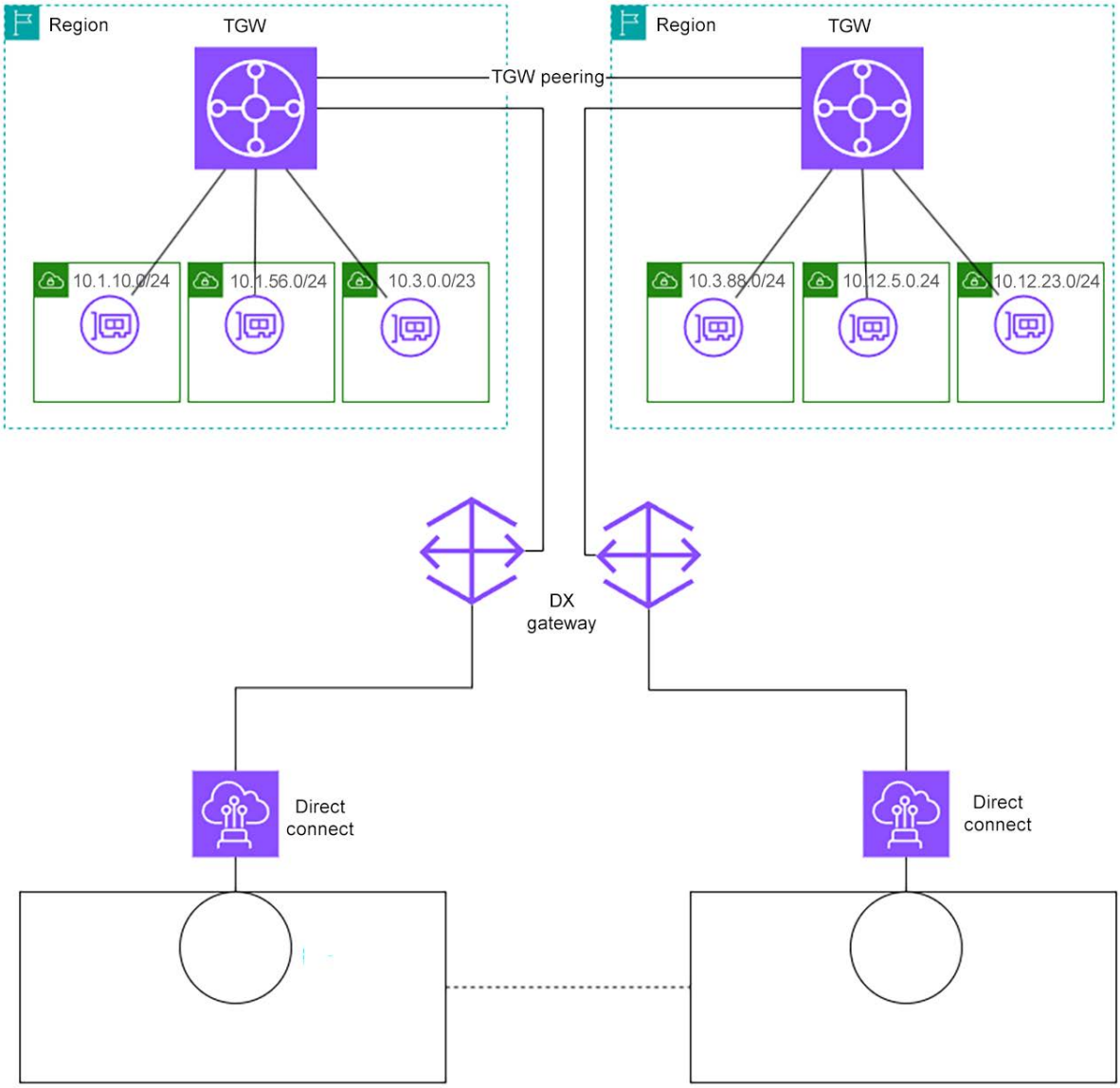

Internet
Region
VPC
Public subnet
AWS VPN client
1
2
5
6
SAML IdP in IAM
3
4
Identity provider login site

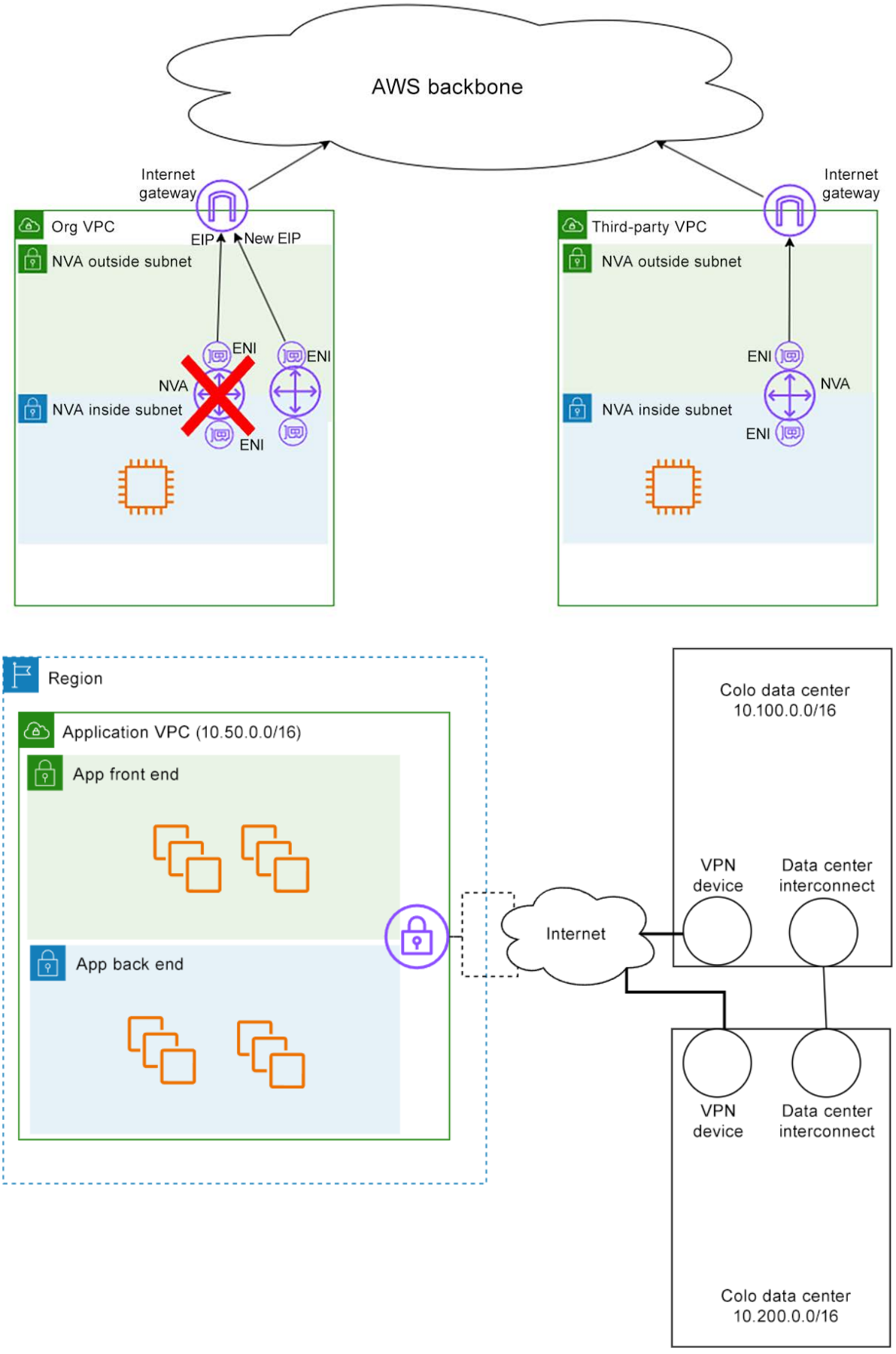

AWS backbone
9
Internet gateway
10
Org VPC
NVA outside subnet
11
ENI
NVA
NVA inside subnet
ENI
12
Internet gateway
Third-party VPC
NVA outside subnet
6-8
ENI
NVA
NVA inside subnet
ENI
1-5
Region
VPC
Public subnet
Private subnet
VGW
Internet 1
Internet 2
Third-party data center
Device 1
Device 2

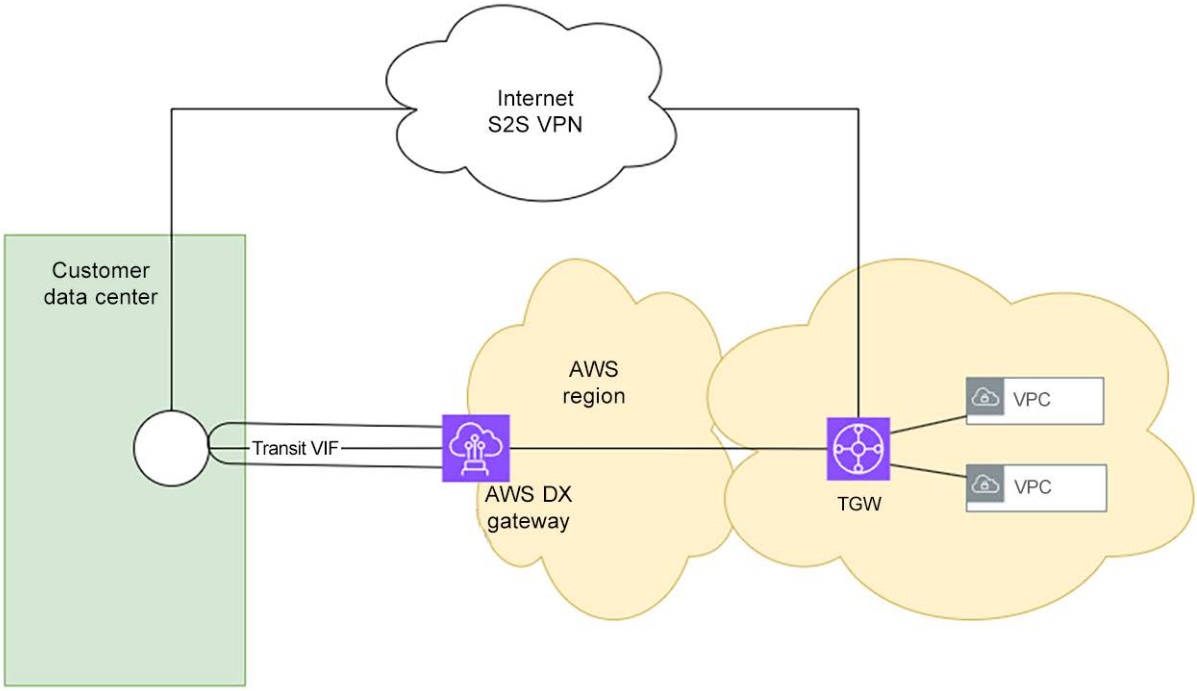

Region
VPC
VPC
VPC
Transit gateway
Internet
Direct connect
gateway
Customer equipment
AWS partner data center

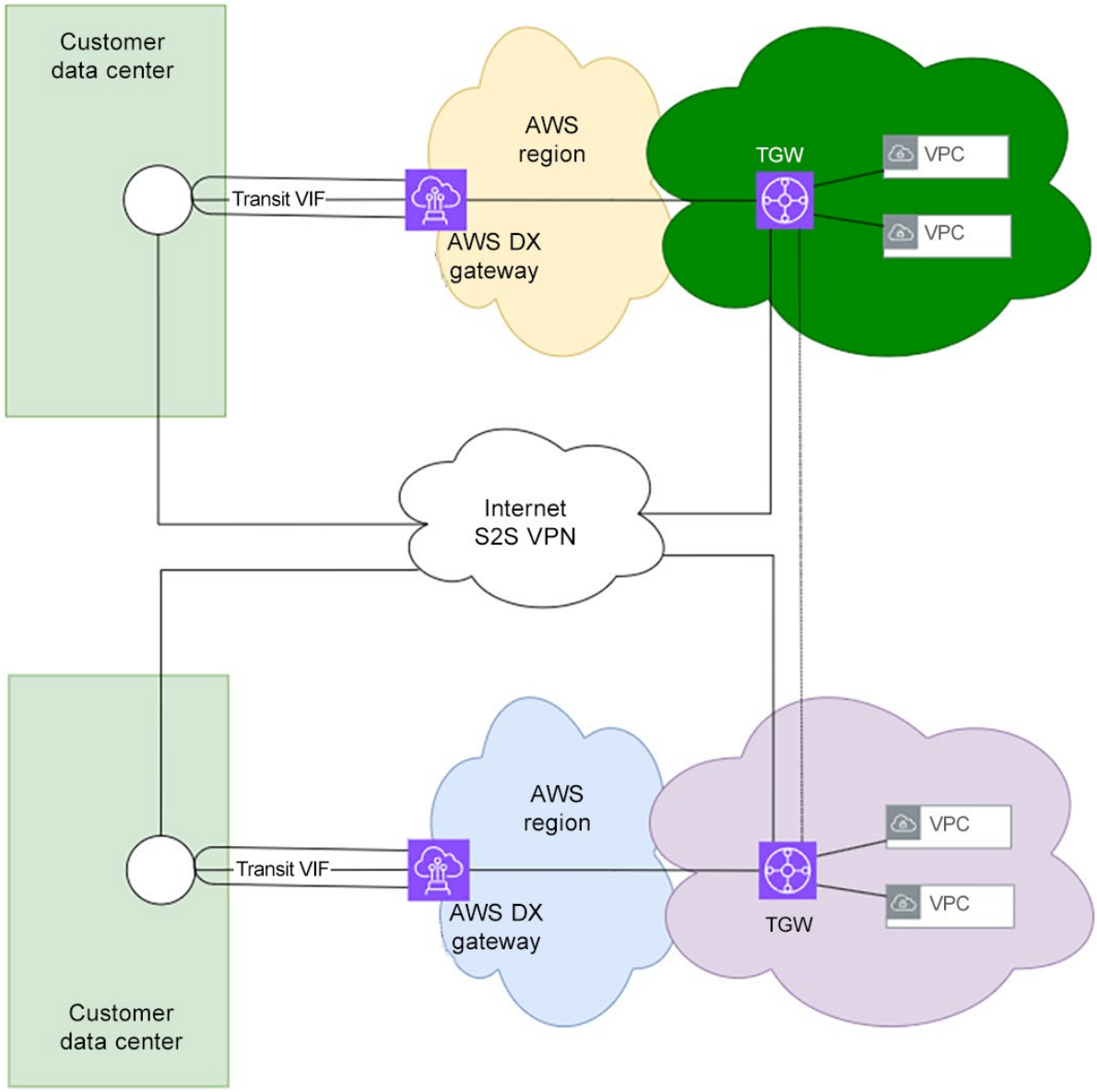

Region
VPC
VPC
VPC
Transit gateway
Direct connect gateway
Internet
Direct connect gateway
AWS partner data center
AWS partner data center
Customer equipment
Customer equipment

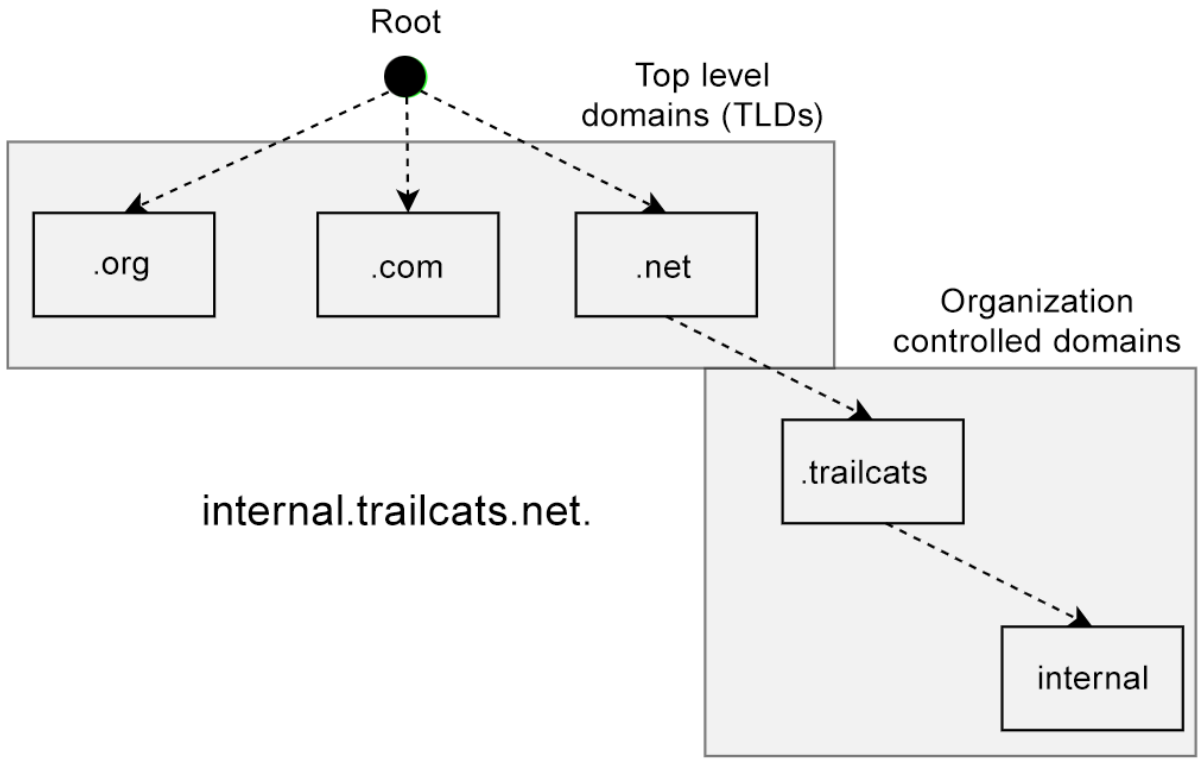

10.1.10.0/24
10.1.56.0/24
10.3.0.0/23
10.3.88.0/24
10.12.5.0/24
10.12.23.0/24
DX gateway
Direct connect
Direct connect
AWS DX location
AWS DX location
Provider equipment
Provider equipment
WAN connection (ISP or private)
WAN connection (ISP or private)
Customer data center
Customer data center


Region
TGW
TGW peering
Region
TGW
10.1.10.0/24
10.1.56.0/24
10.3.0.0/23
10.3.88.0/24
10.12.5.0.24
10.12.23.0/24
DX
gateway
Direct
connect
Direct
connect


AWS backbone
Internet gateway
Org VPC
EIP
New EIP
NVA outside subnet
ENI
ENI
NVA
NVA inside subnet
ENI
Internet gateway
Third-party VPC
NVA outside subnet
ENI
NVA
NVA inside subnet
ENI
Region
Application VPC (10.50.0.0/16)
App front end
App back end
Internet
Colo data center
10.100.0.0/16
VPN device
Data center interconnect
VPN device
Data center interconnect
Colo data center
10.200.0.0/16

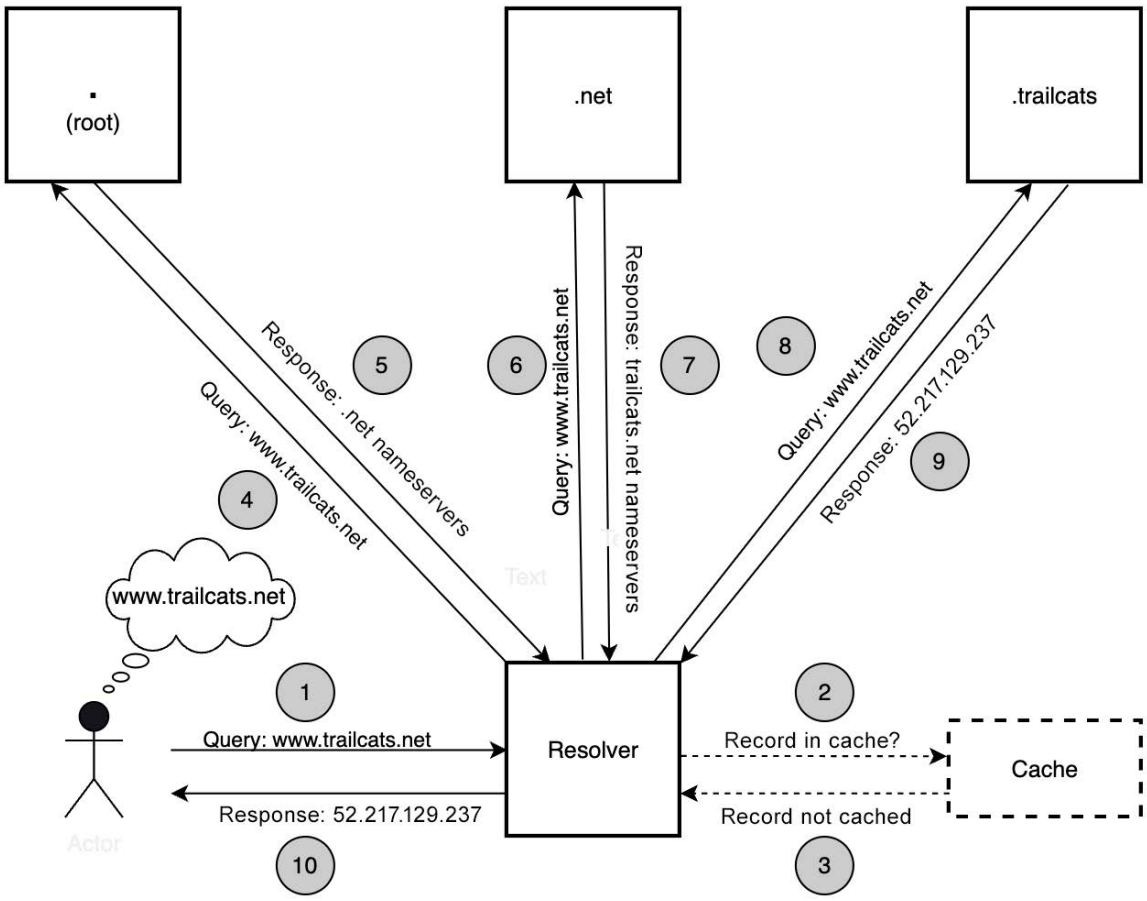

Internet
S2S VPN
Customer
data center
AWS
region
Transit VIF
AWS DX
gateway
TGW
VPC
VPC


Customer
data center
AWS
region
TGW
VPC
VPC
Transit VIF
AWS DX
gateway
Internet
S2S VPN
AWS
region
VPC
VPC
Transit VIF
AWS DX
gateway
TGW
Customer
data center



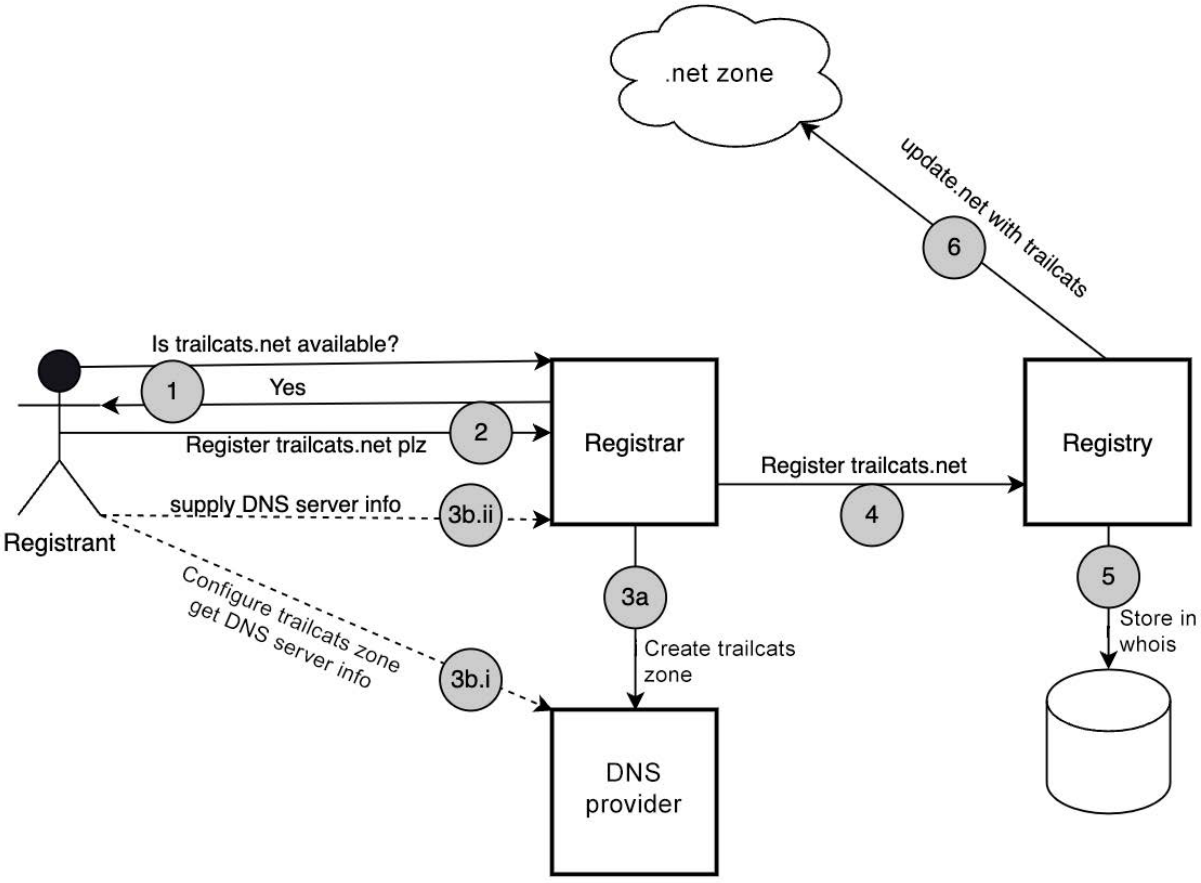

```
~ dig . ns

; <<>> DiG 9.10.6 <<>> . ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61832
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       518400  IN      NS      a.root-servers.net.
.                       518400  IN      NS      b.root-servers.net.
.                       518400  IN      NS      c.root-servers.net.
.                       518400  IN      NS      d.root-servers.net.
.                       518400  IN      NS      e.root-servers.net.
.                       518400  IN      NS      f.root-servers.net.
.                       518400  IN      NS      g.root-servers.net.
.                       518400  IN      NS      h.root-servers.net.
.                       518400  IN      NS      i.root-servers.net.
.                       518400  IN      NS      j.root-servers.net.
.                       518400  IN      NS      k.root-servers.net.
.                       518400  IN      NS      l.root-servers.net.
.                       518400  IN      NS      m.root-servers.net.
```

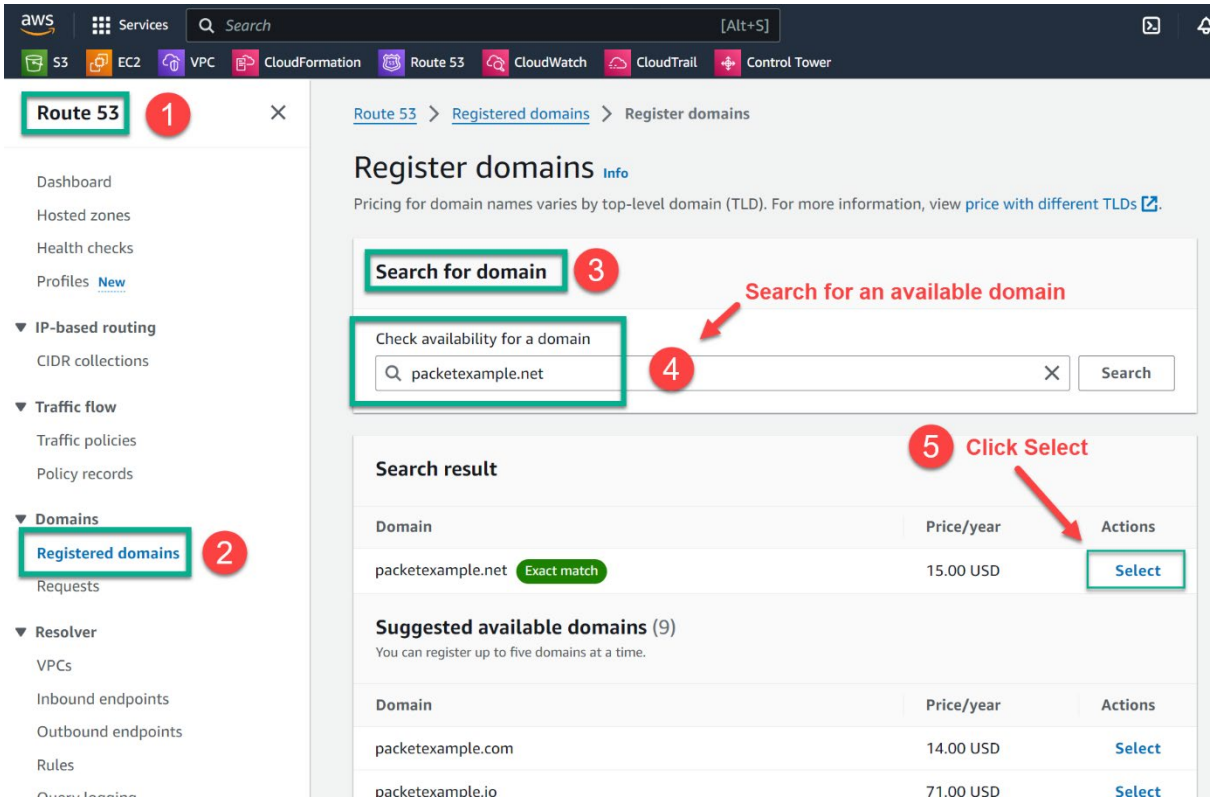
```
~ dig org. ns

; <<>> DiG 9.10.6 <<>> org. ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31410
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;org.                           IN      NS

;; ANSWER SECTION:
org.                    3531    IN      NS      a0.org.afilias-nst.info.
org.                    3531    IN      NS      a2.org.afilias-nst.info.
org.                    3531    IN      NS      b0.org.afilias-nst.org.
org.                    3531    IN      NS      b2.org.afilias-nst.org.
org.                    3531    IN      NS      c0.org.afilias-nst.info.
org.                    3531    IN      NS      d0.org.afilias-nst.org.
```

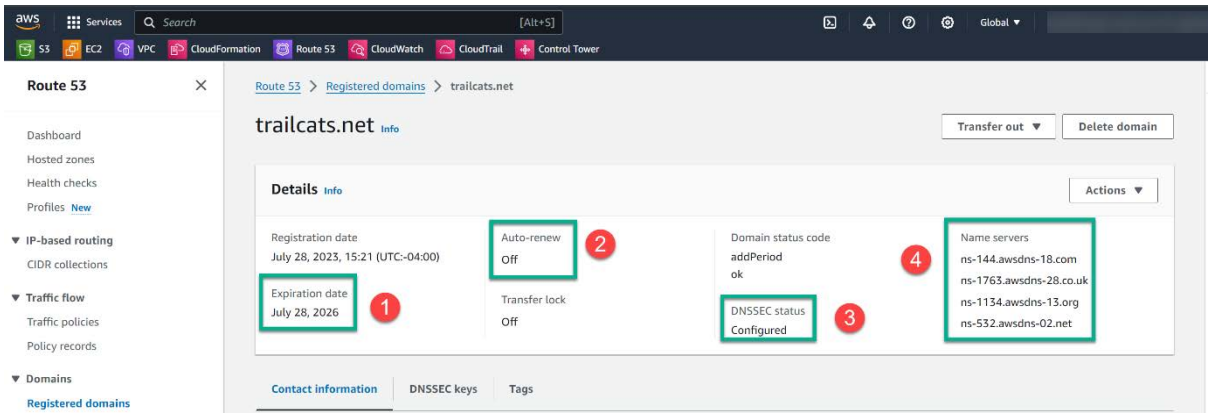


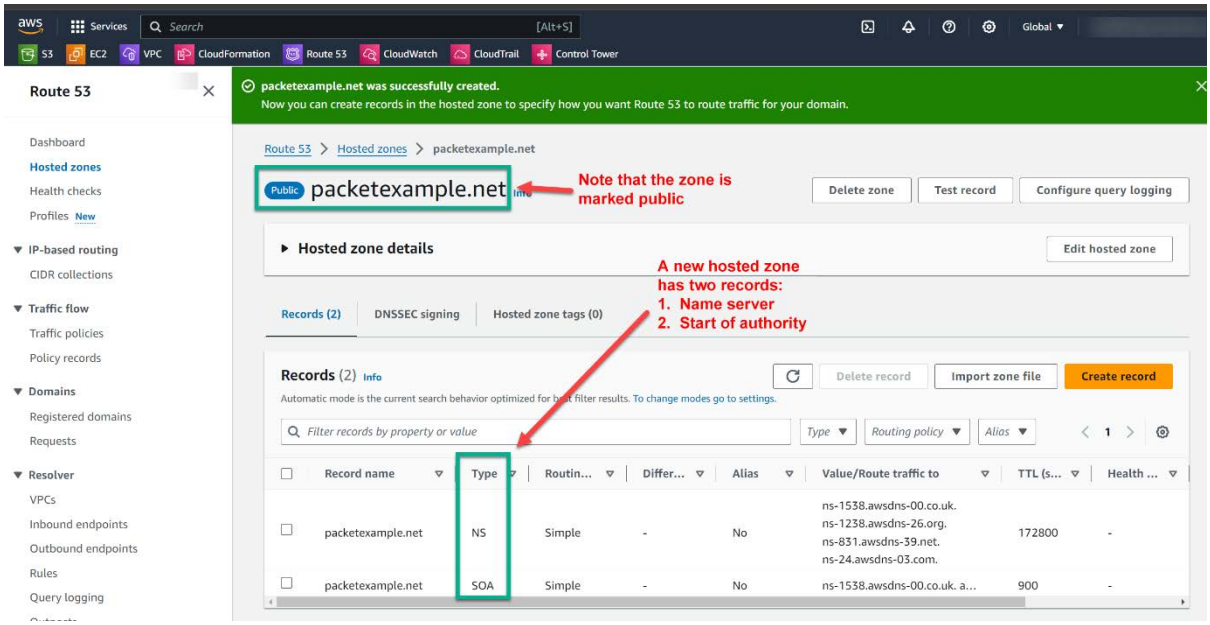
```
~/books/ANS-C01  main  dig NS trailcats.net

; <<>> DiG 9.10.6 <<>> NS trailcats.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32442
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;trailcats.net.                 IN      NS

;; ANSWER SECTION:
trailcats.net.          172209  IN      NS      ns-144.awsdns-18.com.
trailcats.net.          172209  IN      NS      ns-532.awsdns-02.net.
trailcats.net.          172209  IN      NS      ns-1134.awsdns-13.org.
trailcats.net.          172209  IN      NS      ns-1763.awsdns-28.co.uk.
```

```
trailcats.net.          5       IN      RRSIG A 13 2 5 20230807020300
20230807000255 53358 trailcats.net.
/3R7jV2730SRAhPkjJ/0p0CTwHxOlxHmALkKczEM9b1eZqI+fC+9bFKs
2PNKYMXr85ZL65ZfIf3/BiNFexgnMQ==
```

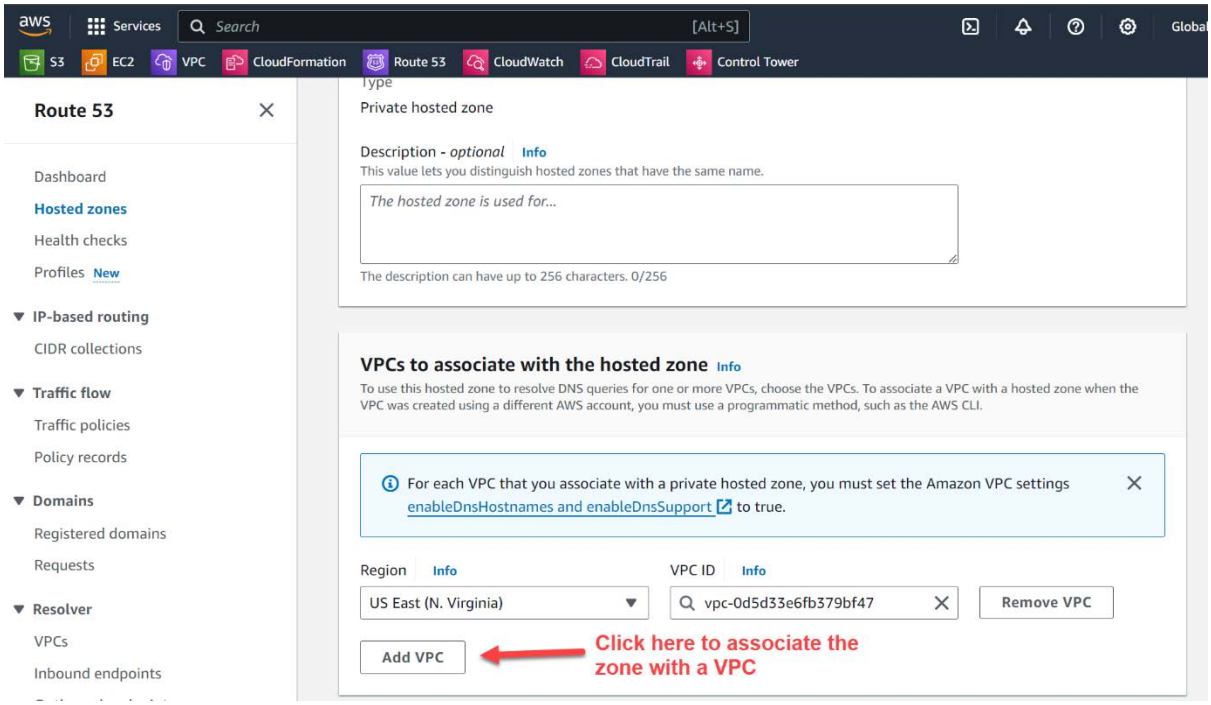


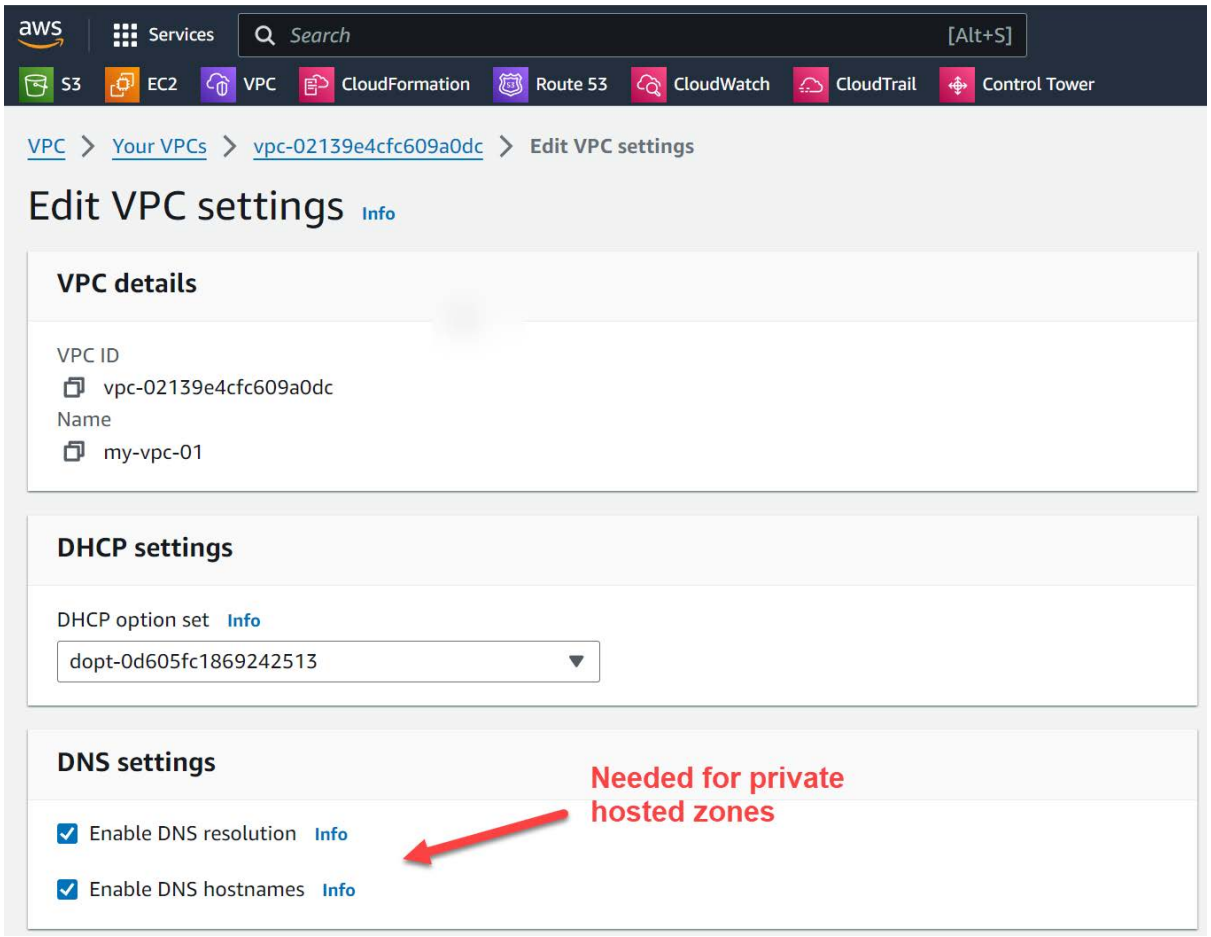

aws
Services
Search
[Alt+S]
S3
EC2
VPC
CloudFormation
Route 53
CloudWatch
CloudTrail
Control Tower
Route 53
1
Dashboard
Hosted zones
Health checks
Profiles New
IP-based routing
CIDR collections
Traffic flow
Traffic policies
Policy records
Domains
Registered domains
2
Requests
Resolver
VPCs
Inbound endpoints
Outbound endpoints
Rules
Route 53 > Registered domains > Register domains
Register domains Info
Pricing for domain names varies by top-level domain (TLD). For more information, view price with different TLDs.
Search for domain
3
Search for an available domain
Check availability for a domain
packetexample.net
4
Search
5
Click Select
Search result
Domain
Price/year
Actions
packetexample.net
Exact match
15.00 USD
Select
Suggested available domains (9)
You can register up to five domains at a time.
Domain
Price/year
Actions
packetexample.com
14.00 USD
Select
packetexample.io
71.00 USD
Select

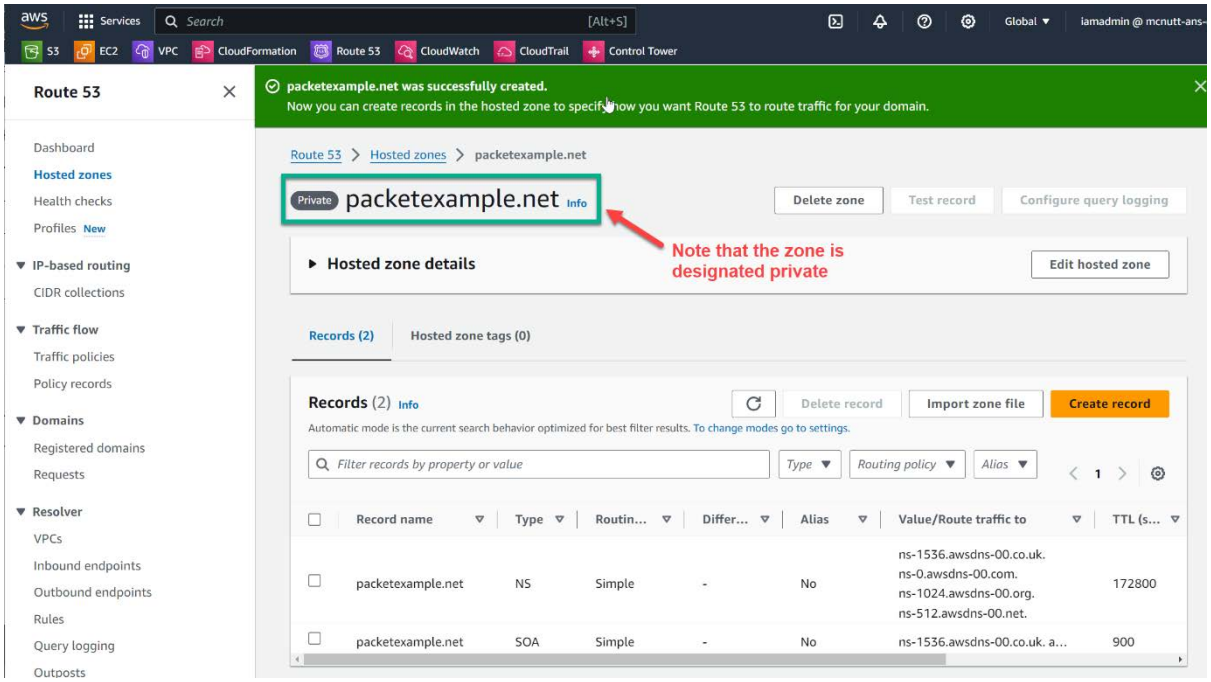

aws
Services
Search
[Alt+S]
Global
S3
EC2
VPC
CloudFormation
Route 53
CloudWatch
CloudTrail
Control Tower
Route 53
Dashboard
Hosted zones
Health checks
Profiles New
IP-based routing
CIDR collections
Traffic flow
Traffic policies
Policy records
Domains
Registered domains
Route 53 > Registered domains > trailcats.net
trailcats.net Info
Transfer out
Delete domain
Details Info
Actions
Registration date
July 28, 2023, 15:21 (UTC-04:00)
Expiration date
July 28, 2026
1
Auto-renew
Off
2
Transfer lock
Off
Domain status code
addPeriod
ok
4
DNSSEC status
Configured
3
Name servers
ns-144.awsdns-18.com
ns-1763.awsdns-28.co.uk
ns-1134.awsdns-13.org
ns-532.awsdns-02.net
Contact information
DNSSEC keys
Tags

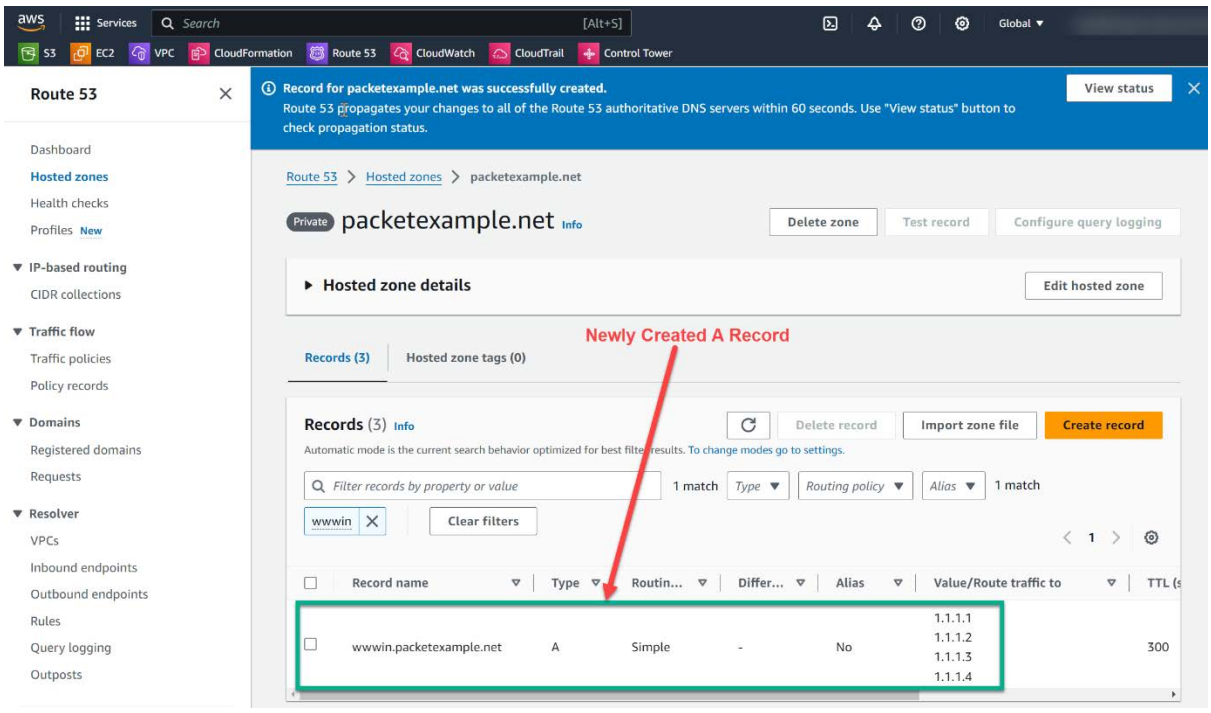


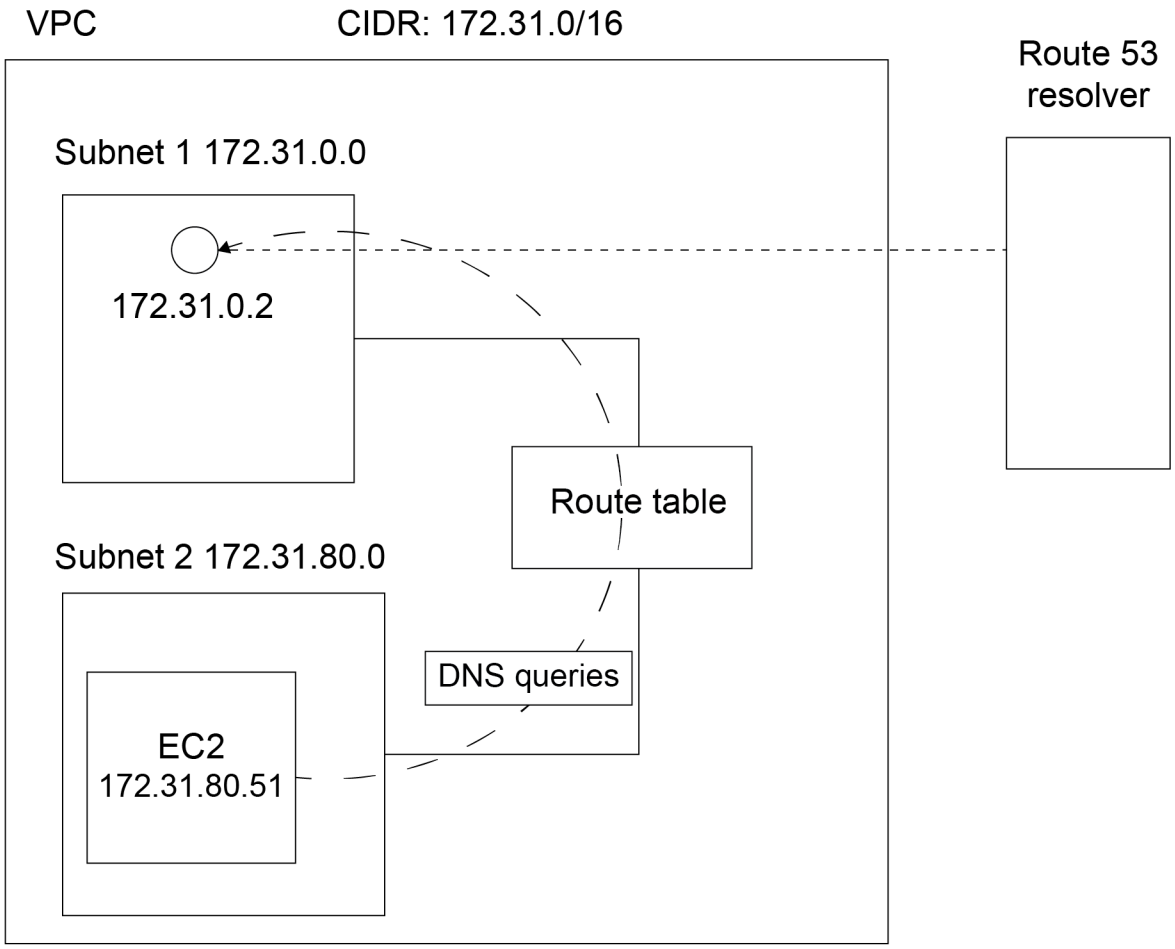

```
~ dig ns net. +short
a.gtld-servers.net.
b.gtld-servers.net.
c.gtld-servers.net.
d.gtld-servers.net.
e.gtld-servers.net.
f.gtld-servers.net.
g.gtld-servers.net.
h.gtld-servers.net.
i.gtld-servers.net.
j.gtld-servers.net.
k.gtld-servers.net.
l.gtld-servers.net.
m.gtld-servers.net.
~ dig @a.gtld-servers.net. ns trailcats.net. +short
ns-144.awsdns-18.com.
ns-532.awsdns-02.net.
ns-1134.awsdns-13.org.
ns-1763.awsdns-28.co.uk.
```

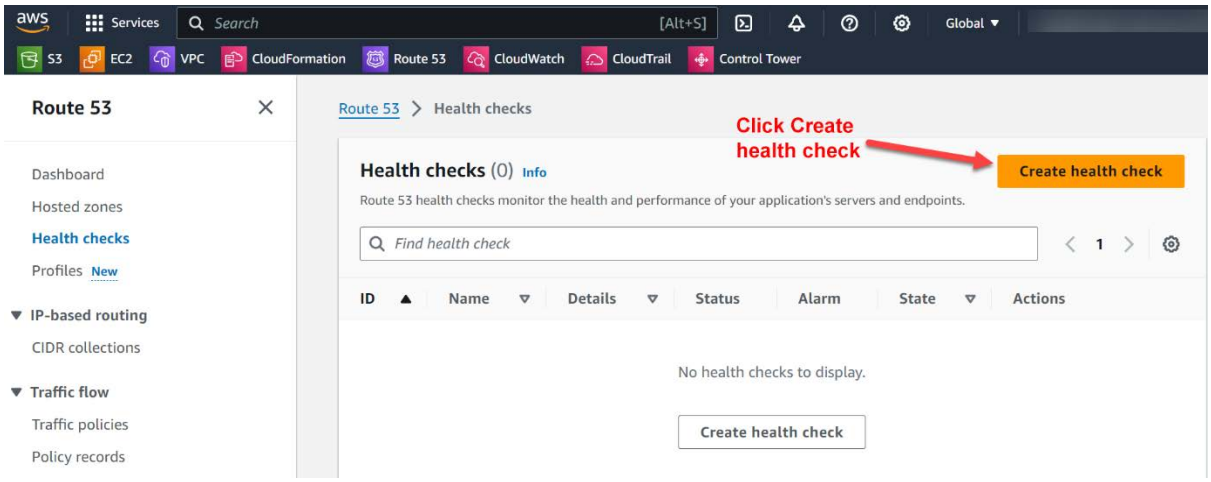

Route 53
Dashboard
Hosted zones
Health checks
Profiles New
IP-based routing
CIDR collections
Traffic flow
Traffic policies
Policy records
Domains
Registered domains
Requests
Resolver
VPCs
Inbound endpoints
Private hosted zone
Description - optional Info
This value lets you distinguish hosted zones that have the same name.
The hosted zone is used for...
The description can have up to 256 characters. 0/256
VPCs to associate with the hosted zone Info
To use this hosted zone to resolve DNS queries for one or more VPCs, choose the VPCs. To associate a VPC with a hosted zone when the VPC was created using a different AWS account, you must use a programmatic method, such as the AWS CLI.
For each VPC that you associate with a private hosted zone, you must set the Amazon VPC settings enableDnsHostnames and enableDnsSupport to true.
Region Info
US East (N. Virginia)
VPC ID Info
vpc-0d5d33e6fb379bf47
Remove VPC
Add VPC
Click here to associate the zone with a VPC


VPC > Your VPCs > vpc-02139e4cfc609a0dc > Edit VPC settings
Edit VPC settings Info
VPC details
VPC ID
vpc-02139e4cfc609a0dc
Name
my-vpc-01
DHCP settings
DHCP option set Info
dopt-0d605fc1869242513
DNS settings
Enable DNS resolution Info
Enable DNS hostnames Info
Needed for private hosted zones


Route 53
packetexample.net was successfully created.
Now you can create records in the hosted zone to specify how you want Route 53 to route traffic for your domain.
Route 53 > Hosted zones > packetexample.net
Private packetexample.net Info
Delete zone
Test record
Configure query logging
Note that the zone is designated private
Hosted zone details
Edit hosted zone
Records (2)
Hosted zone tags (0)
Records (2) Info
Delete record
Import zone file
Create record
Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.
Filter records by property or value
Type
Routing policy
Alias
Record name
Type
Routin...
Differ...
Alias
Value/Route traffic to
TTL (s...
packetexample.net
NS
Simple
-
No
ns-1536.awsdns-00.co.uk.
ns-0.awsdns-00.com.
ns-1024.awsdns-00.org.
ns-512.awsdns-00.net.
172800
packetexample.net
SOA
Simple
-
No
ns-1536.awsdns-00.co.uk. a...
900

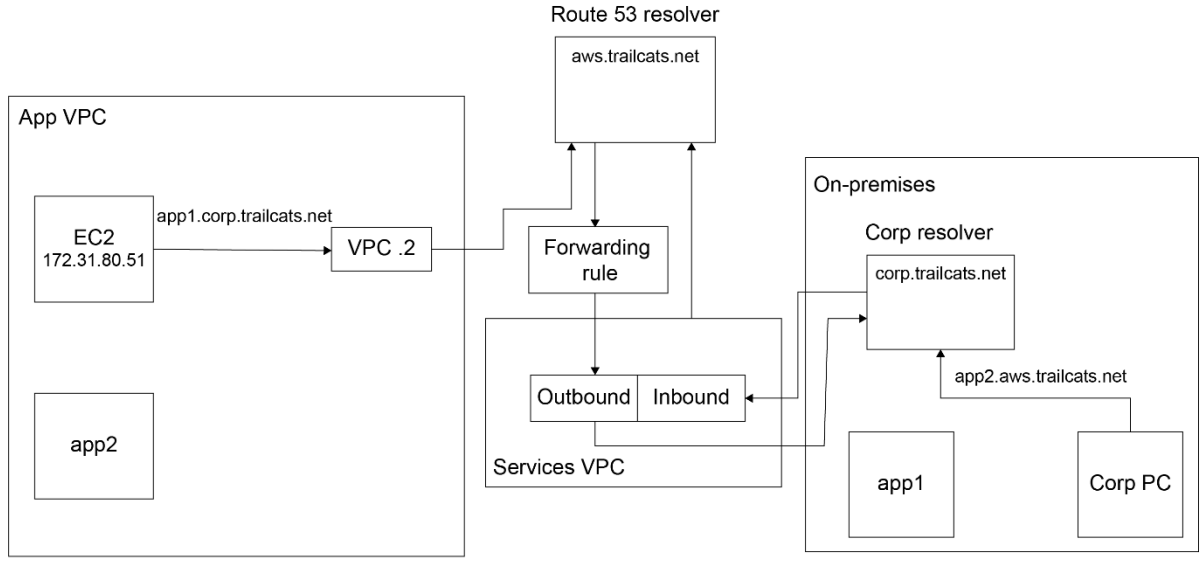

Route 53
Record for packetexample.net was successfully created.
Route 53 propagates your changes to all of the Route 53 authoritative DNS servers within 60 seconds. Use "View status" button to check propagation status.
View status
Route 53 > Hosted zones > packetexample.net
Private packetexample.net Info
Delete zone
Test record
Configure query logging
Hosted zone details
Edit hosted zone
Newly Created A Record
Records (3)
Hosted zone tags (0)
Records (3) Info
Delete record
Import zone file
Create record
Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.
Filter records by property or value
1 match
Type
Routing policy
Alias
1 match
wwwin
Clear filters
Record name
Type
Routin...
Differ...
Alias
Value/Route traffic to
TTL (s
wwwin.packetexample.net
A
Simple
-
No
1.1.1.1
1.1.1.2
1.1.1.3
1.1.1.4
300

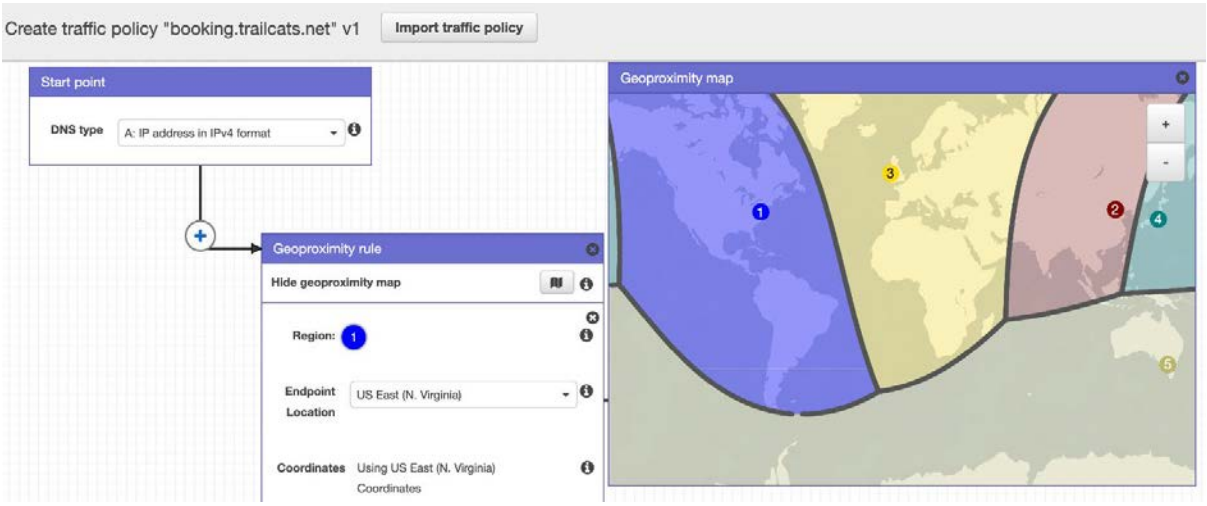

VPC
CIDR: 172.31.0/16
Route 53 resolver
Subnet 1 172.31.0.0
172.31.0.2
Route table
Subnet 2 172.31.80.0
DNS queries
EC2
172.31.80.51

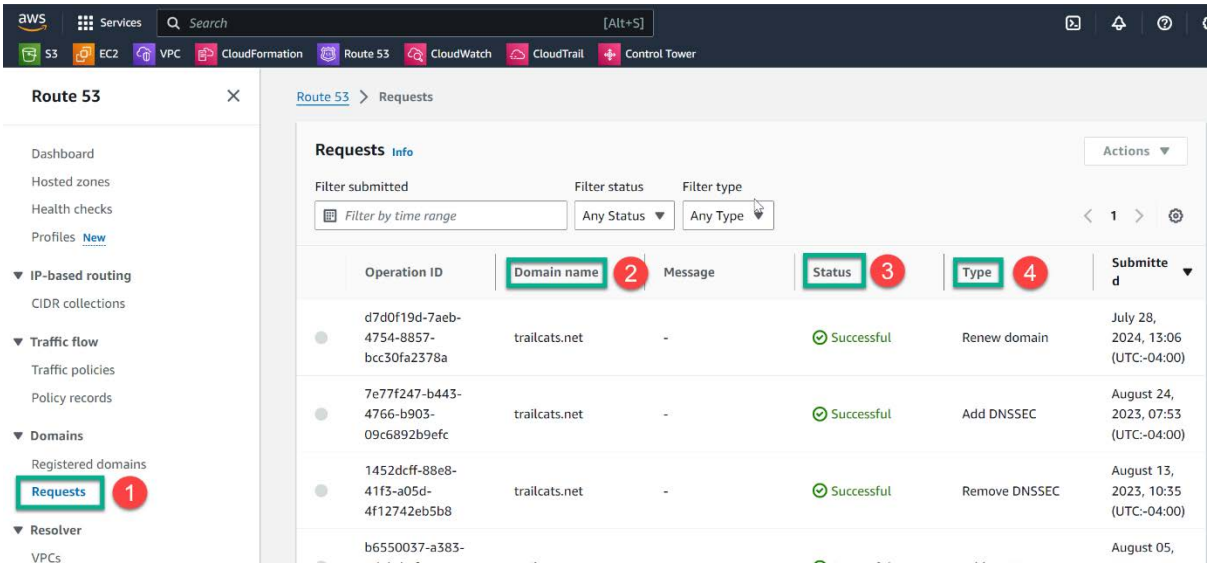

aws
Services
Search
[Alt+S]
Global
S3
EC2
VPC
CloudFormation
Route 53
CloudWatch
CloudTrail
Control Tower
Route 53
Dashboard
Hosted zones
Health checks
Profiles New
IP-based routing
CIDR collections
Traffic flow
Traffic policies
Policy records
Route 53 > Health checks
Click Create health check
Health checks (0) Info
Route 53 health checks monitor the health and performance of your application's servers and endpoints.
Create health check
Find health check
1
ID
Name
Details
Status
Alarm
State
Actions
No health checks to display.
Create health check

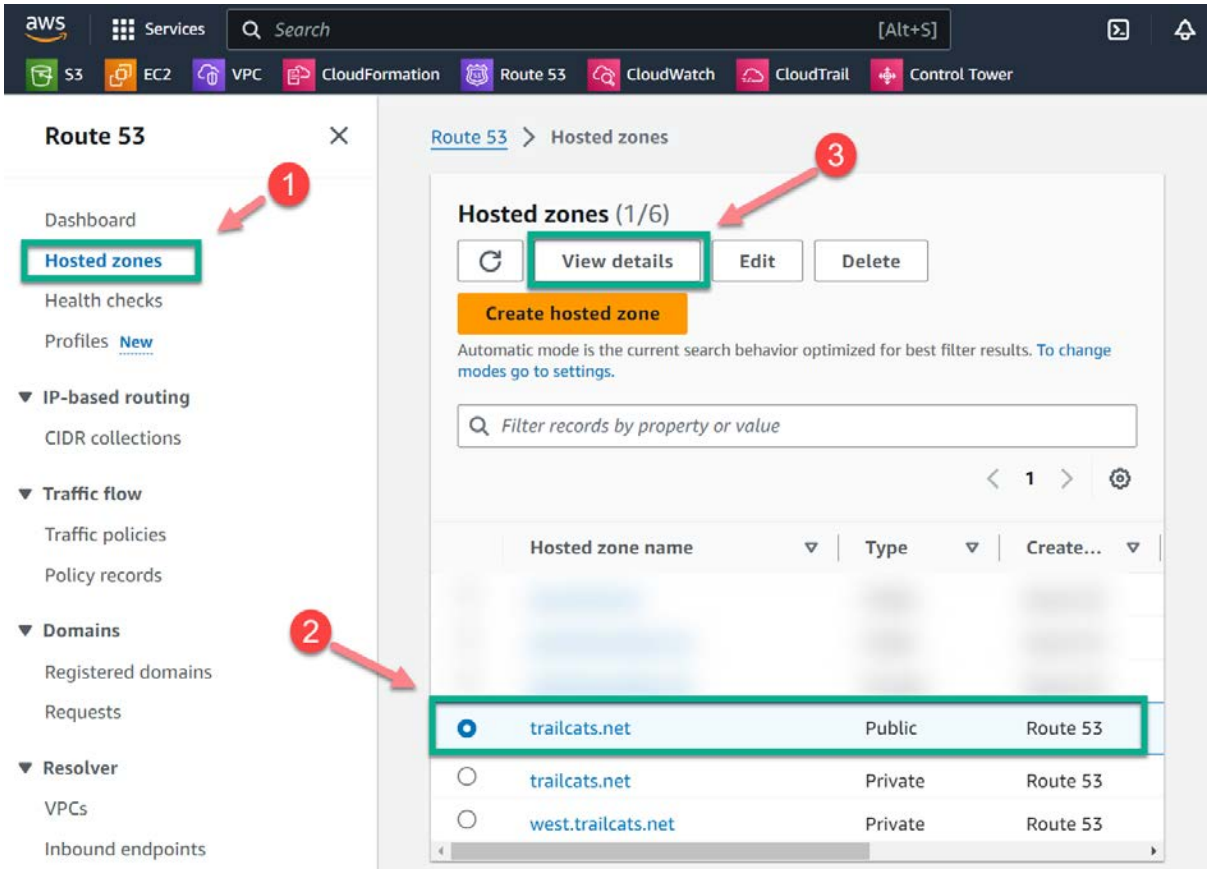

aws
Services
Search
[Alt+S]
Global
iamadmin @ mcnutt-ans-c01-general
S3
EC2
VPC
CloudFormation
Route 53
CloudWatch
CloudTrail
Control Tower
Create health check
Step 1: Configure health check
Step 2: Get notified when health check fails
Configure health check
Route 53 health checks let you track the health status of your resources, such as web servers or mail servers, and take action when an outage occurs.
Name
Trailcats TCP
What to monitor
Endpoint
Status of other health checks (calculated health check)
State of CloudWatch alarm
Monitor an endpoint
Multiple Route 53 health checkers will try to establish a TCP connection with the following resource to determine whether it's healthy. Learn more
Specify endpoint by
IP address
Domain name
Protocol
TCP
Simple TCP check
Domain name *
trailcats
Port *
80
Advanced configuration
URL
tcp://trailcats:80/
Health check type
Basic - no additional options selected (View Pricing)
Monitor an endpoint
Multiple Route 53 health checkers will try to establish a TCP connection with the following resource to determine whether it's healthy.
Learn more
Specify endpoint by
IP address
Domain name
Protocol
HTTP
Domain name *
trailcats.net
Port *
80
Path
/
Cat-on-a-leash1.jpg
Test to see if resources on server is available
Advanced configuration
Request interval
Standard (30 seconds)
Fast (10 seconds)
Failure threshold *
3
String matching
No
Yes
Latency graphs
Invert health check status
Disable health check
By default, disabled health checks are considered healthy. Learn more
Health checker regions
Customize
Use recommended
US East (N. Virginia)
US West (N. California)
US West (Oregon)
Select regions
10-second checks are an upcharge

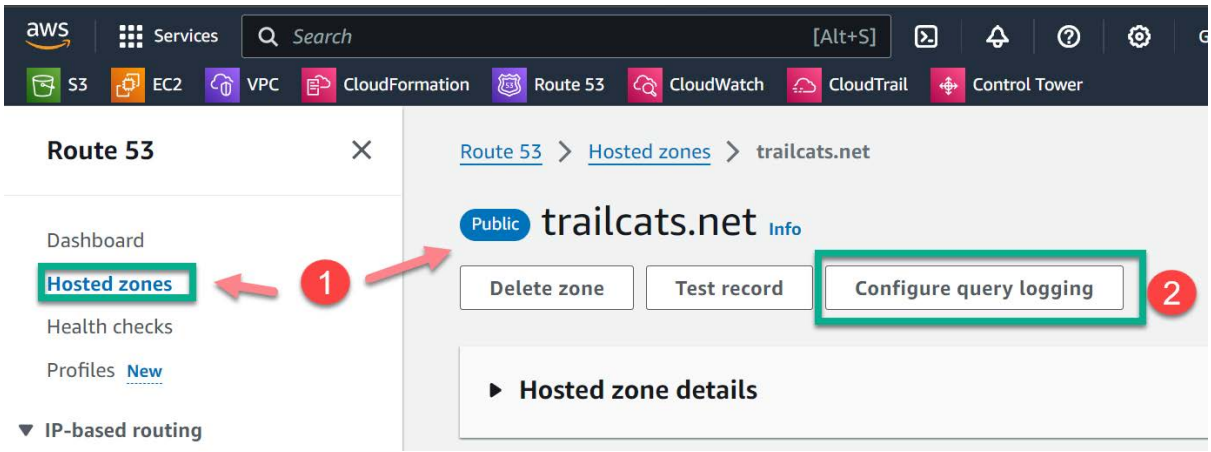
Chapter 8: AWS Route 53: Advanced

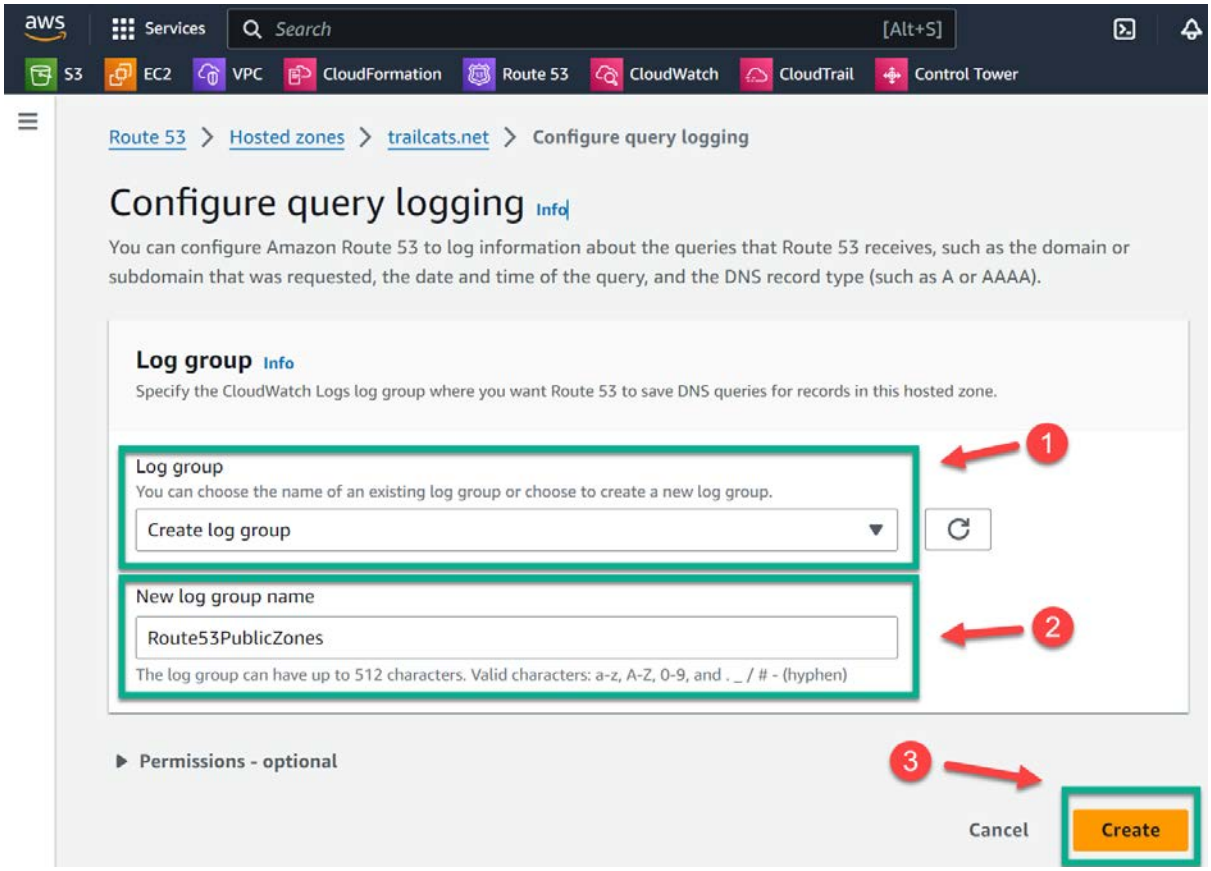


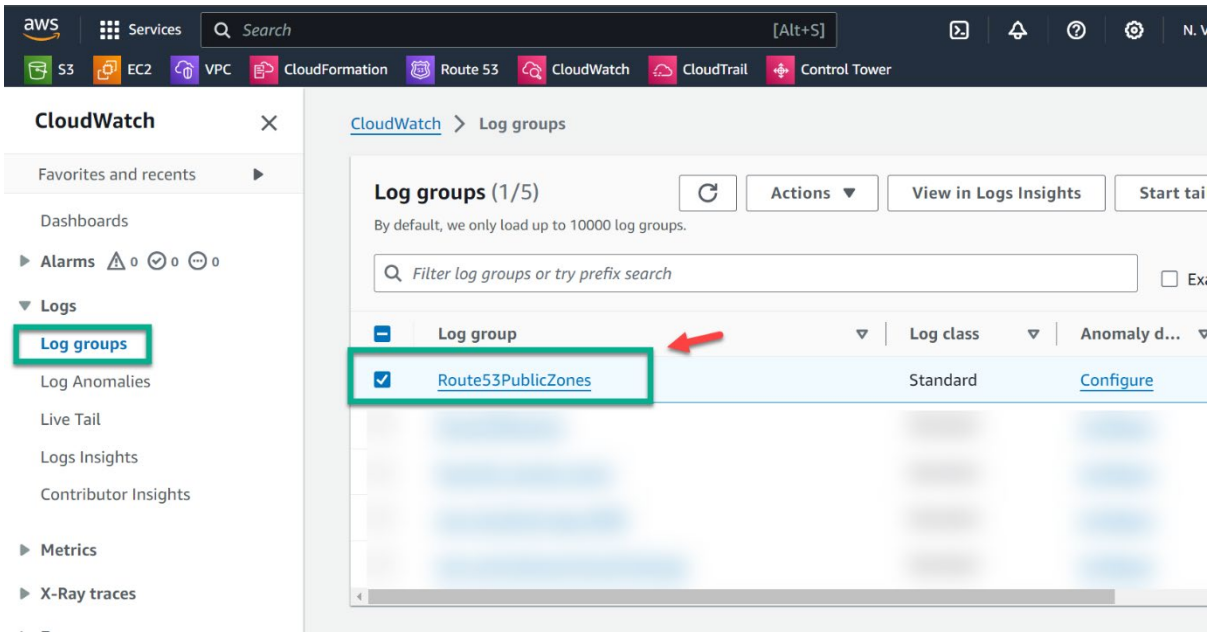


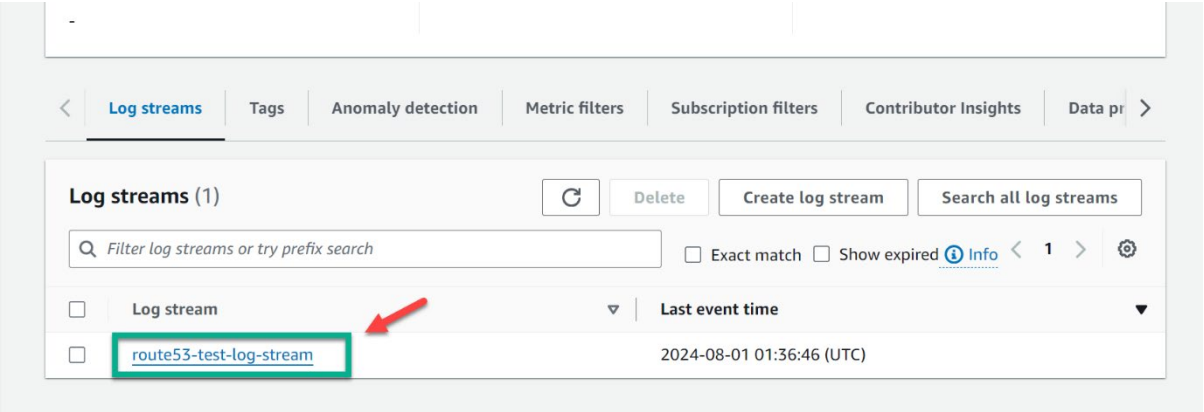


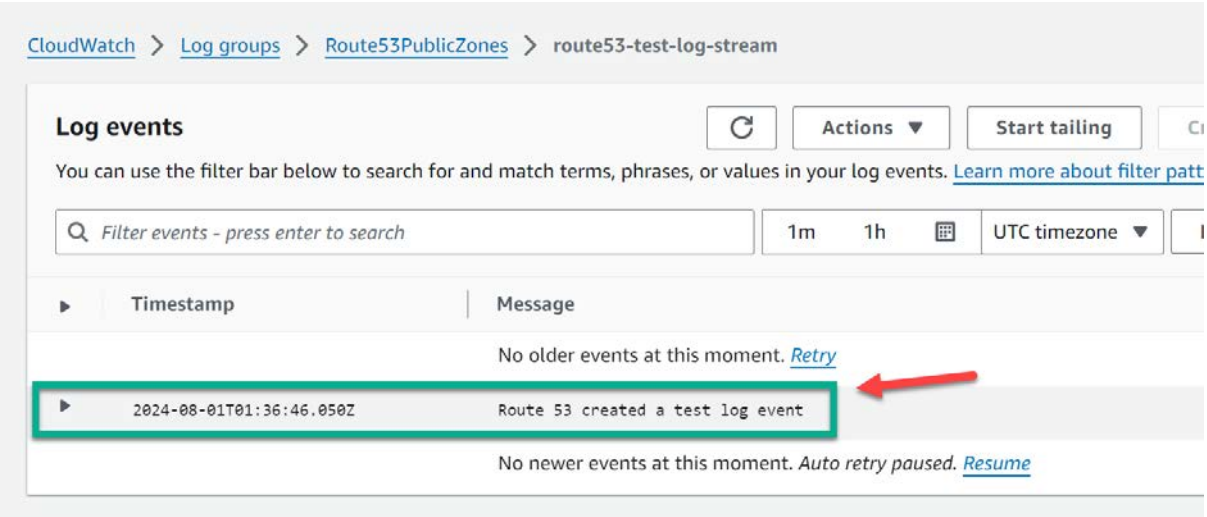

aws
Services
Search
[Alt+S]
S3
EC2
VPC
CloudFormation
Route 53
CloudWatch
CloudTrail
Control Tower
Route 53
Dashboard
Hosted zones
Health checks
Profiles New
IP-based routing
CIDR collections
Traffic flow
Traffic policies
Policy records
Domains
Registered domains
Requests
Resolver
VPCs
Inbound endpoints
Route 53 > Hosted zones
Hosted zones (1/6)
View details
Edit
Delete
Create hosted zone
Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.
Filter records by property or value
Hosted zone name
Type
Create...
trailcats.net
Public
Route 53
trailcats.net
Private
Route 53
west.trailcats.net
Private
Route 53
1
2
3

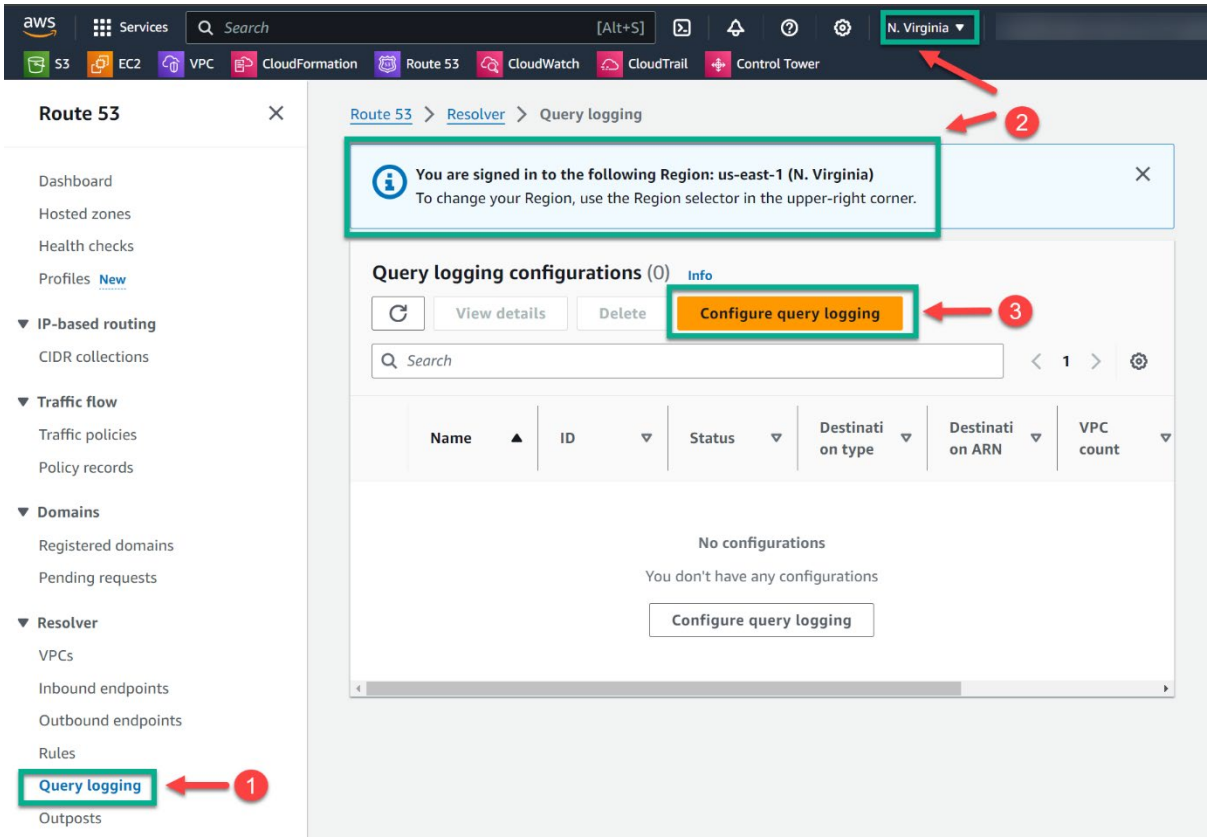

aws
Services
Search
[Alt+S]
S3
EC2
VPC
CloudFormation
Route 53
CloudWatch
CloudTrail
Control Tower
Route 53
Dashboard
Hosted zones
Health checks
Profiles New
IP-based routing
Route 53 > Hosted zones > trailcats.net
Public
trailcats.net
Info
Delete zone
Test record
Configure query logging
Hosted zone details
1
2

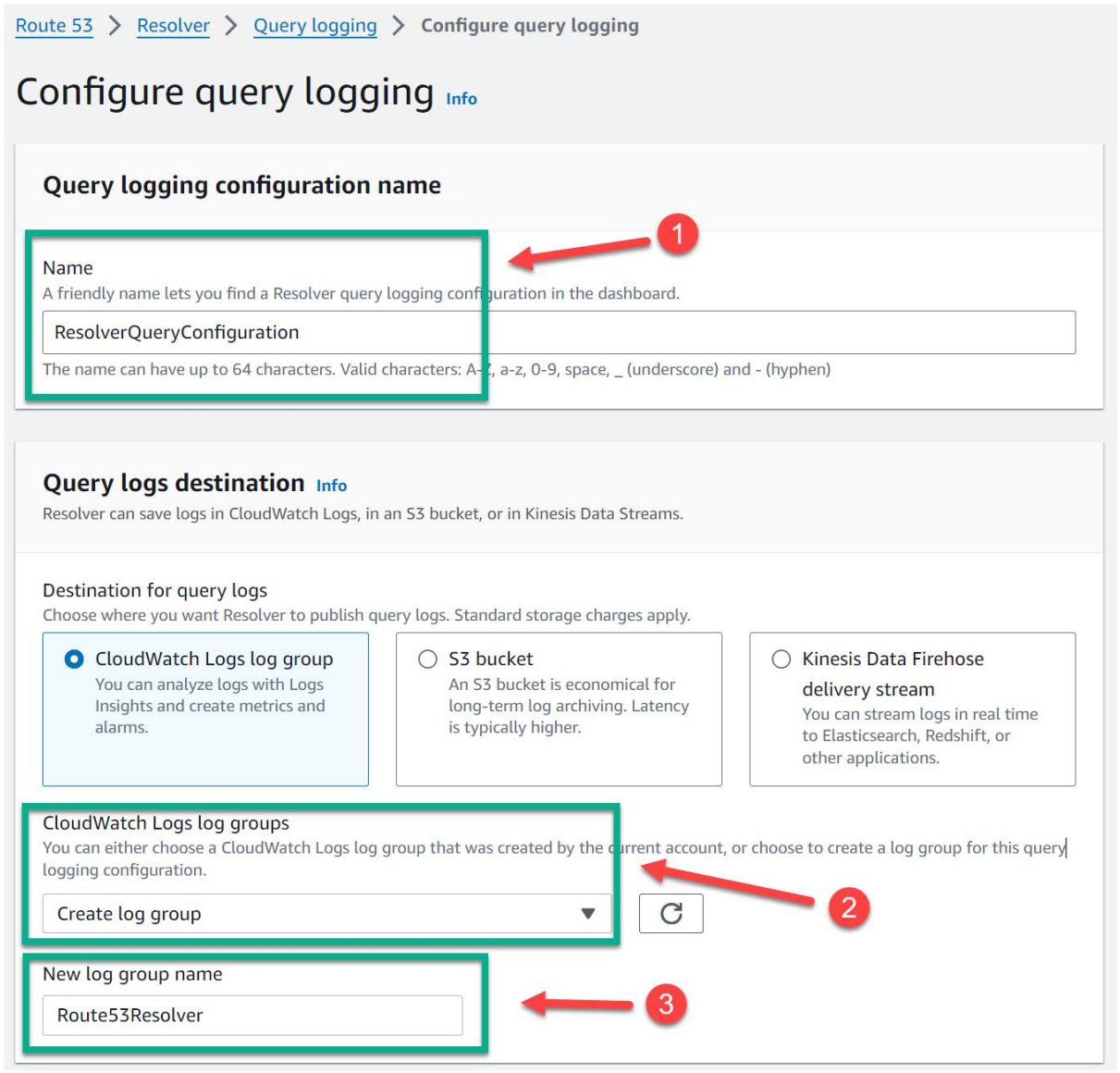

aws
Services
Search
[Alt+S]
S3
EC2
VPC
CloudFormation
Route 53
CloudWatch
CloudTrail
Control Tower
Route 53 > Hosted zones > trailcats.net > Configure query logging
Configure query logging Info
You can configure Amazon Route 53 to log information about the queries that Route 53 receives, such as the domain or subdomain that was requested, the date and time of the query, and the DNS record type (such as A or AAAA).
Log group Info
Specify the CloudWatch Logs log group where you want Route 53 to save DNS queries for records in this hosted zone.
Log group
You can choose the name of an existing log group or choose to create a new log group.
Create log group
1
New log group name
Route53PublicZones
The log group can have up to 512 characters. Valid characters: a-z, A-Z, 0-9, and . _ / # - (hyphen)
2
Permissions - optional
3
Cancel
Create


aws
Services
Search
[Alt+S]
S3
EC2
VPC
CloudFormation
Route 53
CloudWatch
CloudTrail
Control Tower
CloudWatch
Favorites and recents
Dashboards
Alarms 0 0 0
Logs
Log groups
Log Anomalies
Live Tail
Logs Insights
Contributor Insights
Metrics
X-Ray traces
CloudWatch > Log groups
Log groups (1/5)
Actions
View in Logs Insights
By default, we only load up to 10000 log groups.
Filter log groups or try prefix search
Log group
Log class
Anomaly d...
Route53PublicZones
Standard
Configure


Log streams
Tags
Anomaly detection
Metric filters
Subscription filters
Contributor Insights
Log streams (1)
Delete
Create log stream
Search all log streams
Filter log streams or try prefix search
Exact match
Show expired
Info
Log stream
Last event time
route53-test-log-stream
2024-08-01 01:36:46 (UTC)


CloudWatch
Log groups
Route53PublicZones
route53-test-log-stream
Log events
Actions
Start tailing
You can use the filter bar below to search for and match terms, phrases, or values in your log events.
Filter events - press enter to search
1m
1h
UTC timezone
Timestamp
Message
No older events at this moment. Retry
2024-08-01T01:36:46.050Z
Route 53 created a test log event
No newer events at this moment. Auto retry paused. Resume


Services
Search
[Alt+S]
N. Virginia
S3
EC2
VPC
CloudFormation
Route 53
CloudWatch
CloudTrail
Control Tower
Route 53
Dashboard
Hosted zones
Health checks
Profiles New
IP-based routing
CIDR collections
Traffic flow
Traffic policies
Policy records
Domains
Registered domains
Pending requests
Resolver
VPCs
Inbound endpoints
Outbound endpoints
Rules
Query logging
Outposts
1
Route 53 > Resolver > Query logging
2
You are signed in to the following Region: us-east-1 (N. Virginia)
To change your Region, use the Region selector in the upper-right corner.
Query logging configurations (0) Info
View details
Delete
Configure query logging
3
Search
Name
ID
Status
Destination type
Destination ARN
VPC count
No configurations
You don't have any configurations
Configure query logging


Route 53 > Resolver > Query logging > Configure query logging
Configure query logging Info
Query logging configuration name
Name
A friendly name lets you find a Resolver query logging configuration in the dashboard.
ResolverQueryConfiguration
The name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, space, _ (underscore) and - (hyphen)
1
Query logs destination Info
Resolver can save logs in CloudWatch Logs, in an S3 bucket, or in Kinesis Data Streams.
Destination for query logs
Choose where you want Resolver to publish query logs. Standard storage charges apply.
CloudWatch Logs log group
You can analyze logs with Logs Insights and create metrics and alarms.
S3 bucket
An S3 bucket is economical for long-term log archiving. Latency is typically higher.
Kinesis Data Firehose delivery stream
You can stream logs in real time to Elasticsearch, Redshift, or other applications.
CloudWatch Logs log groups
You can either choose a CloudWatch Logs log group that was created by the current account, or choose to create a log group for this query logging configuration.
Create log group
2
New log group name
Route53Resolver
3

CloudWatch Logs log groups

You can either choose a CloudWatch Logs log group that was created by the current account, or choose to create a log group for this query logging configuration.

Create log group

New log group name

Route53Resolver

VPCs to log queries for - *optional* (0) Info

Remove | Add VPC

Resolver logs DNS queries that originate in the VPCs that you choose here. If you don't choose any VPCs, Resolver doesn't log any queries.

Find resource

1

VPC ID	VPC name	Status	IPV4 CIDR	IPV6 CIDR	Owner

No resources

You don't have any resources.

Add VPC

1

Add VPCs

Choose the VPCs that you want to log queries for.

Available VPCs (5/5)

You can only choose VPCs within your current AWS Region: us-east-1.

Find resource

1

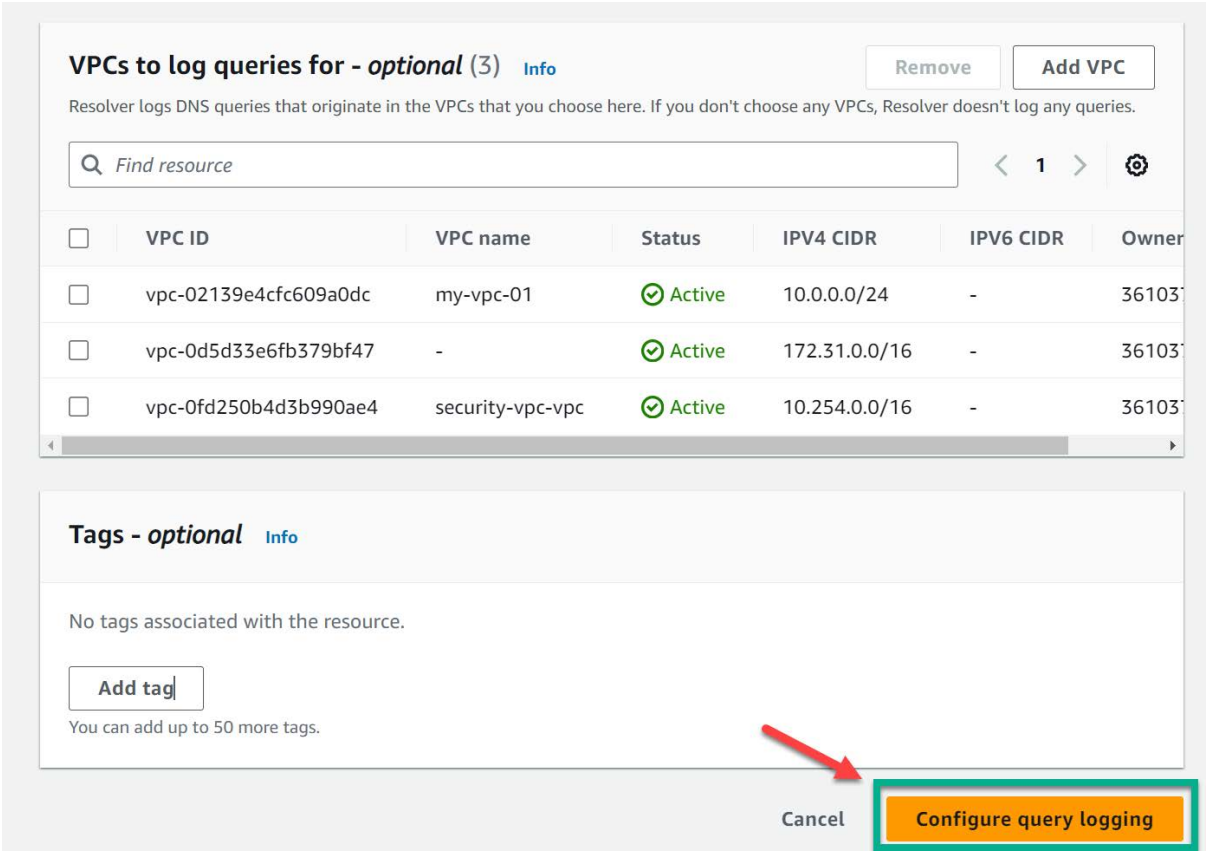
VPC ID	VPC name	Status	IPV4 CIDR	IPV6 CIDR	Owner
vpc-00a9ec30454df66f2	project2-vpc	Active	10.2.0.0/16	-	361037072889
vpc-02139e4cfc609a0dc	my-vpc-01	Active	10.0.0.0/24	-	361037072889
vpc-0bae2adfbe4e8a22c	project-vpc	Active	10.1.0.0/16	-	361037072889
vpc-0d5d33e6fb379bf47	-	Active	172.31.0.0/16	-	361037072889
vpc-0fd250b4d3b990ae4	security-vpc-vpc	Active	10.254.0.0/16	-	361037072889

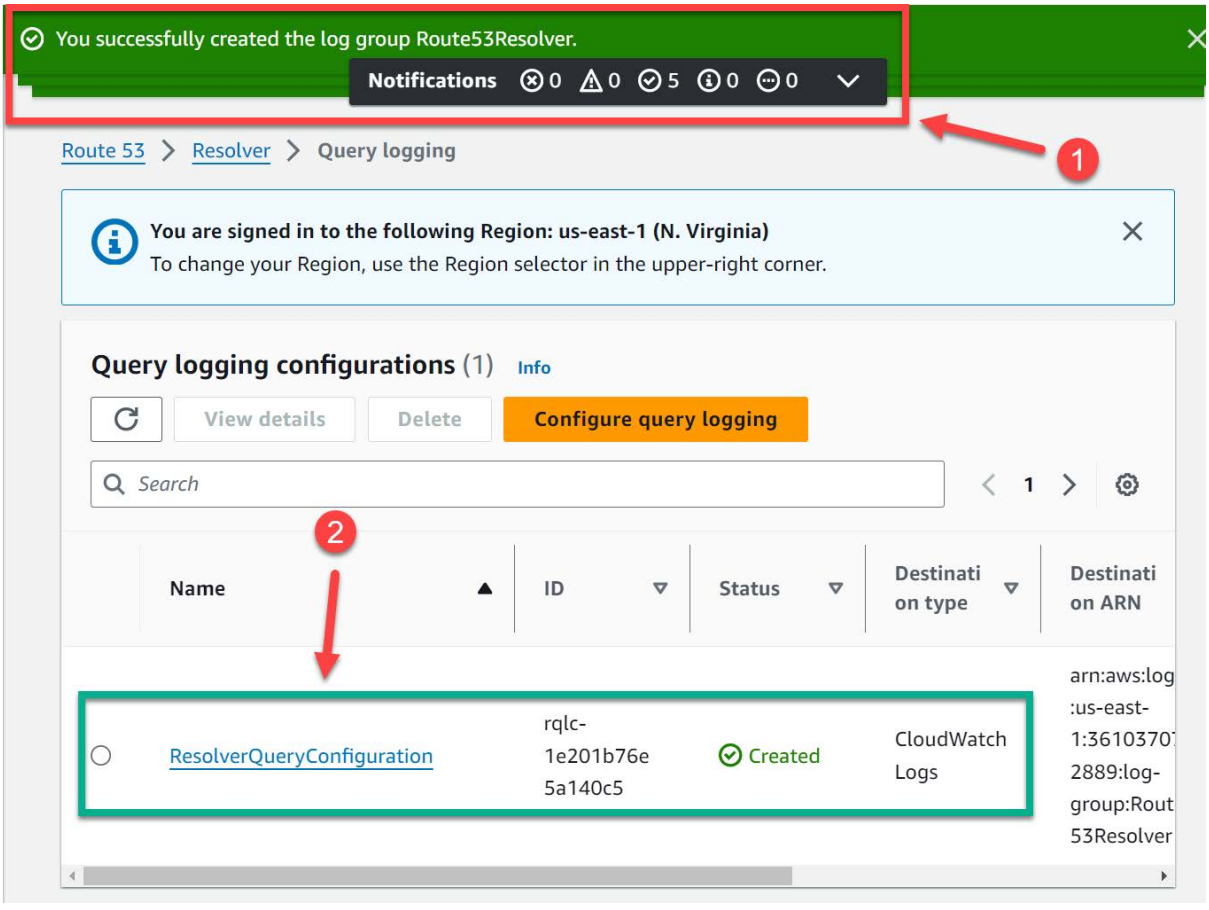
1

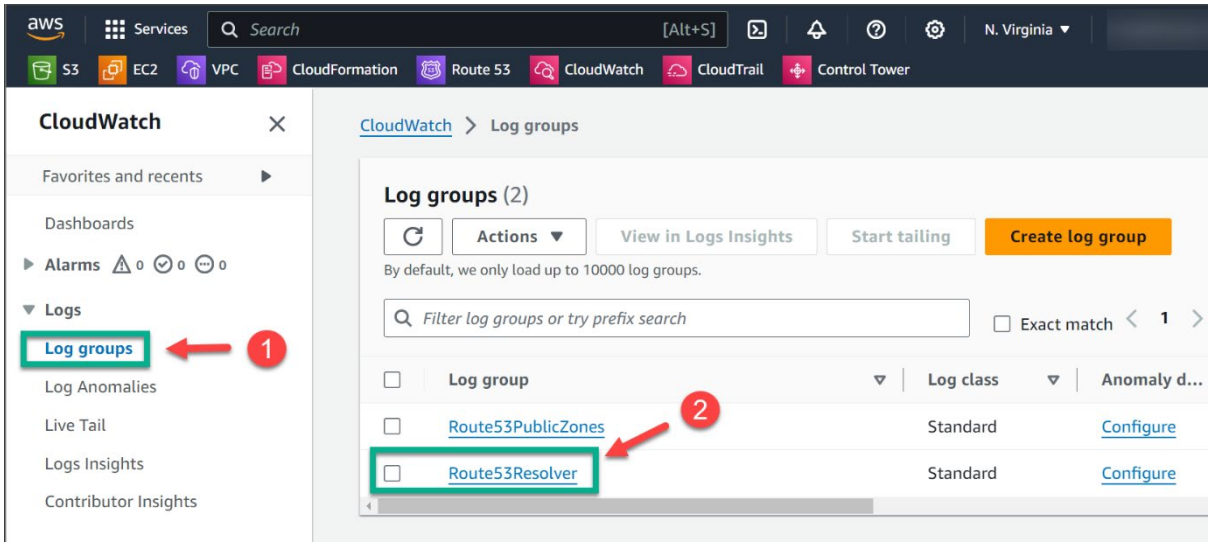
2

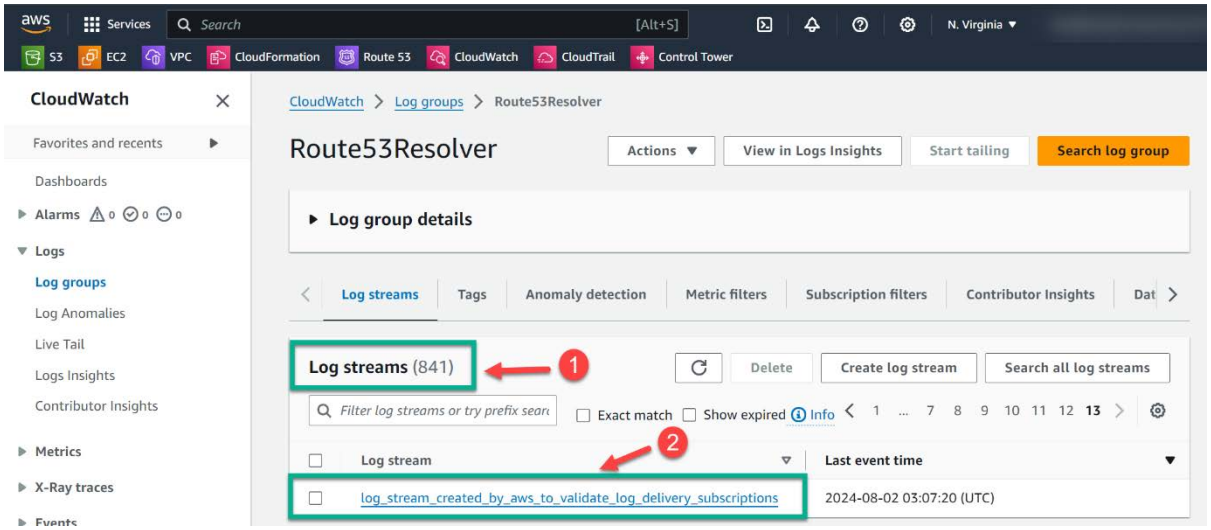
Close

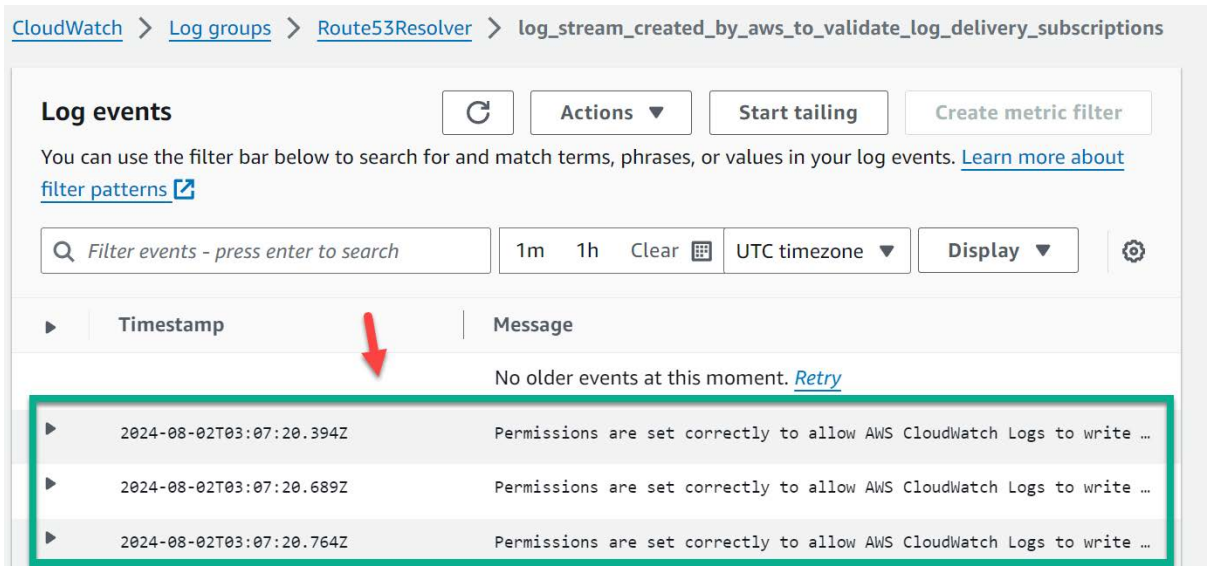
Add

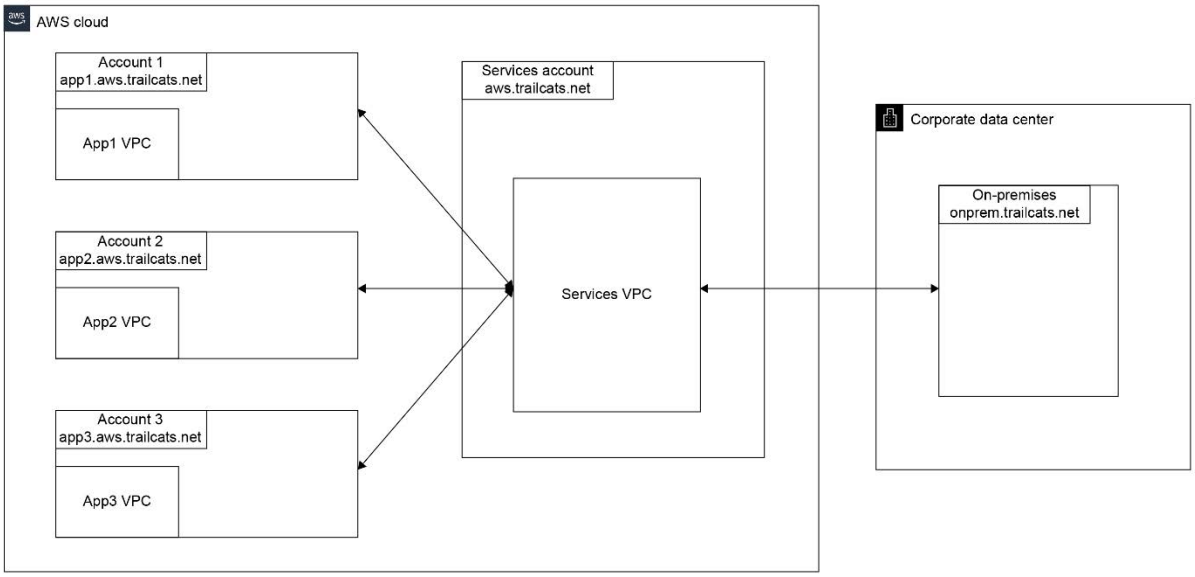

VPCs to log queries for - optional (3) Info
Remove
Add VPC
Resolver logs DNS queries that originate in the VPCs that you choose here. If you don't choose any VPCs, Resolver doesn't log any queries.
Find resource
1
VPC ID
VPC name
Status
IPV4 CIDR
IPV6 CIDR
Owner
vpc-02139e4cfc609a0dc
my-vpc-01
Active
10.0.0.0/24
-
vpc-0d5d33e6fb379bf47
-
Active
172.31.0.0/16
-
vpc-0fd250b4d3b990ae4
security-vpc-vpc
Active
10.254.0.0/16
-
Tags - optional Info
No tags associated with the resource.
Add tag
You can add up to 50 more tags.
Cancel
Configure query logging

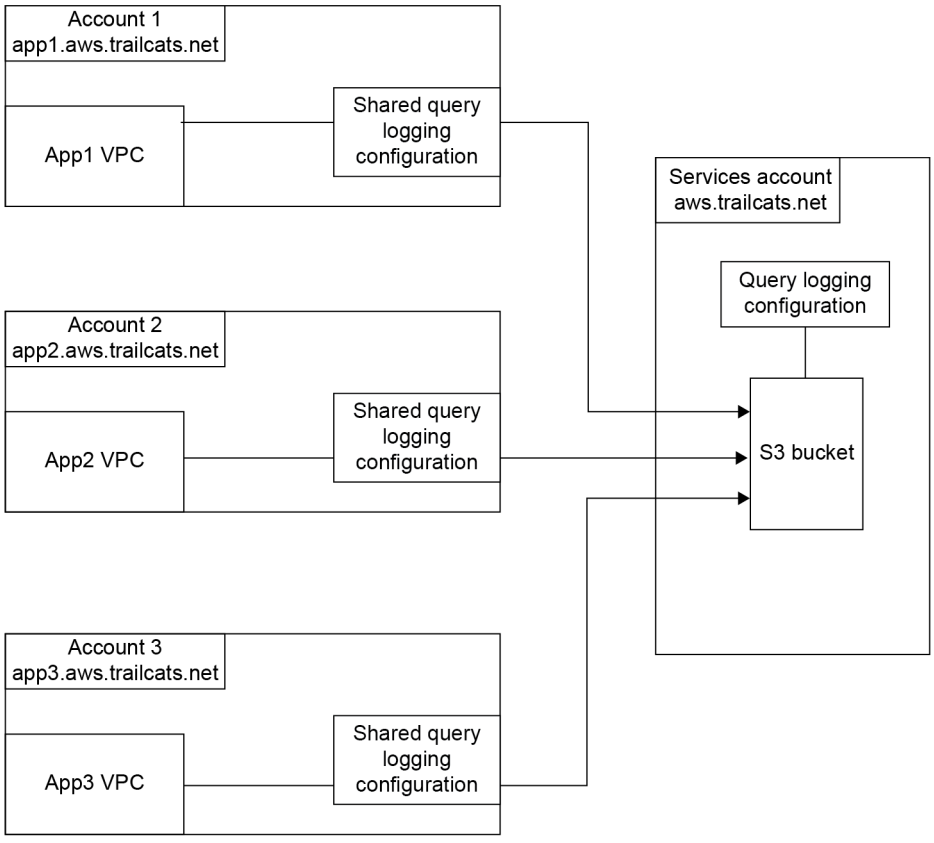

You successfully created the log group Route53Resolver.
Notifications 0 0 5 0 0
Route 53 > Resolver > Query logging
1
You are signed in to the following Region: us-east-1 (N. Virginia)
To change your Region, use the Region selector in the upper-right corner.
Query logging configurations (1) Info
View details
Delete
Configure query logging
Search
1
2
Name
ID
Status
Destination type
Destination ARN
ResolverQueryConfiguration
rqlc-1e201b76e5a140c5
Created
CloudWatch Logs
arn:aws:log:us-east-1:3610370 2889:log-group:Rout 53Resolver

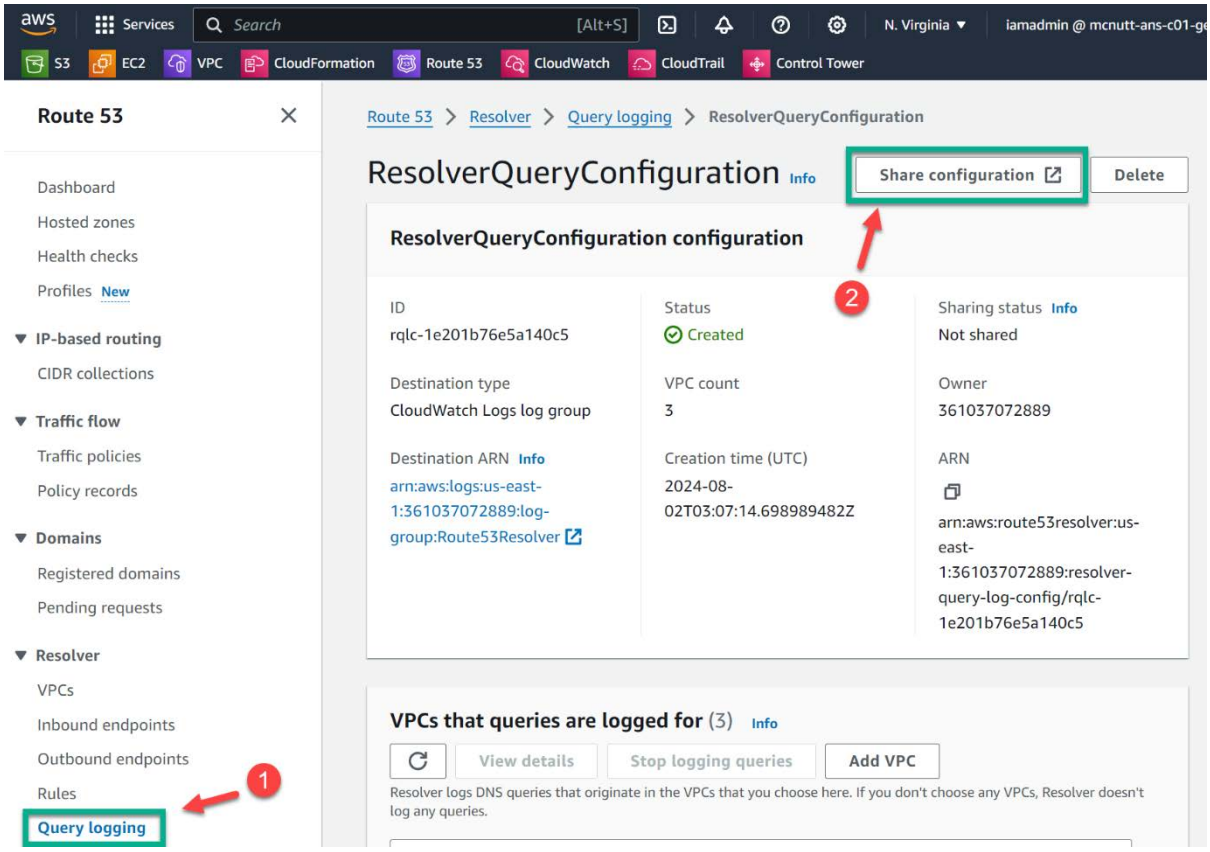

aws
Services
Search
[Alt+S]
N. Virginia
S3
EC2
VPC
CloudFormation
Route 53
CloudWatch
CloudTrail
Control Tower
CloudWatch
Favorites and recents
Dashboards
Alarms
Logs
Log groups
Log Anomalies
Live Tail
Logs Insights
Contributor Insights
1
CloudWatch > Log groups
Log groups (2)
Actions
View in Logs Insights
Start tailing
Create log group
By default, we only load up to 10000 log groups.
Filter log groups or try prefix search
Exact match
Log group
Log class
Anomaly d...
Route53PublicZones
Standard
Configure
2
Route53Resolver
Standard
Configure

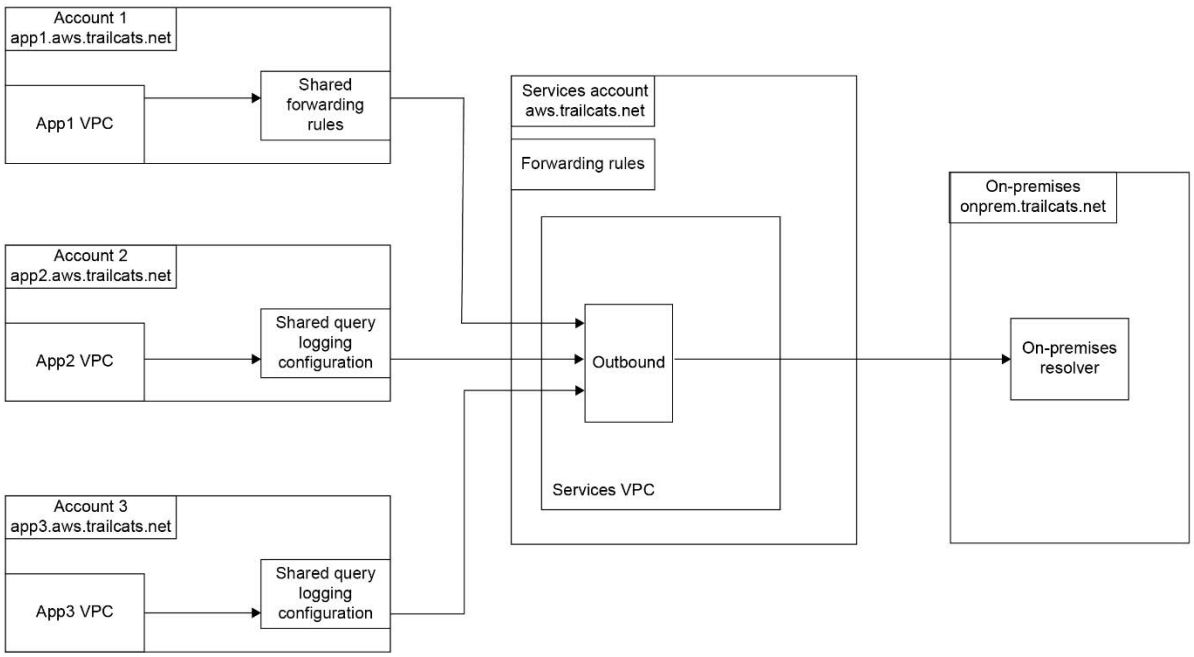

aws
Services
Search
[Alt+S]
N. Virginia
S3
EC2
VPC
CloudFormation
Route 53
CloudWatch
CloudTrail
Control Tower
CloudWatch
Favorites and recents
Dashboards
Alarms
Logs
Log groups
Log Anomalies
Live Tail
Logs Insights
Contributor Insights
Metrics
X-Ray traces
CloudWatch > Log groups > Route53Resolver
Route53Resolver
Actions
View in Logs Insights
Start tailing
Search log group
Log group details
Log streams
Tags
Anomaly detection
Metric filters
Subscription filters
Contributor Insights
Log streams (841)
1
Delete
Create log stream
Search all log streams
Filter log streams or try prefix sear
Exact match
Show expired
Info
2
Log stream
Last event time
log_stream_created_by_aws_to_validate_log_delivery_subscriptions
2024-08-02 03:07:20 (UTC)

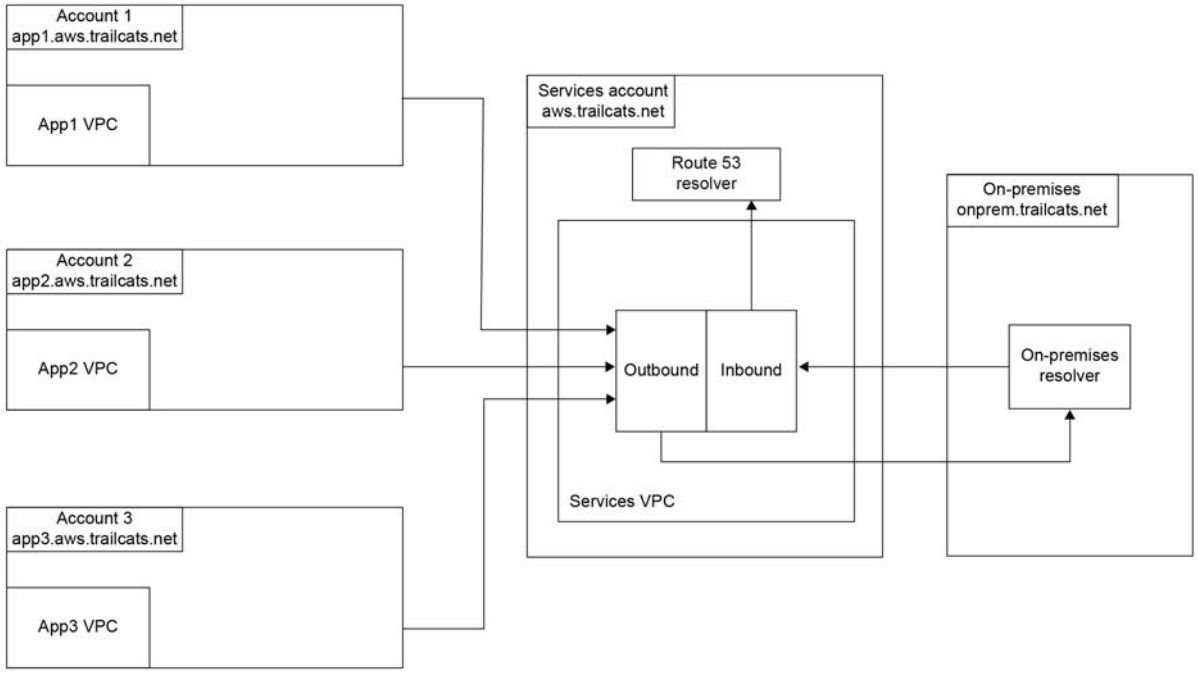

CloudWatch > Log groups > Route53Resolver > log_stream_created_by_aws_to_validate_log_delivery_subscriptions
Log events
Actions
Start tailing
Create metric filter
You can use the filter bar below to search for and match terms, phrases, or values in your log events. Learn more about filter patterns
Filter events - press enter to search
1m
1h
Clear
UTC timezone
Display
Timestamp
Message
No older events at this moment. Retry
2024-08-02T03:07:20.394Z
Permissions are set correctly to allow AWS CloudWatch Logs to write …
2024-08-02T03:07:20.689Z
Permissions are set correctly to allow AWS CloudWatch Logs to write …
2024-08-02T03:07:20.764Z
Permissions are set correctly to allow AWS CloudWatch Logs to write …

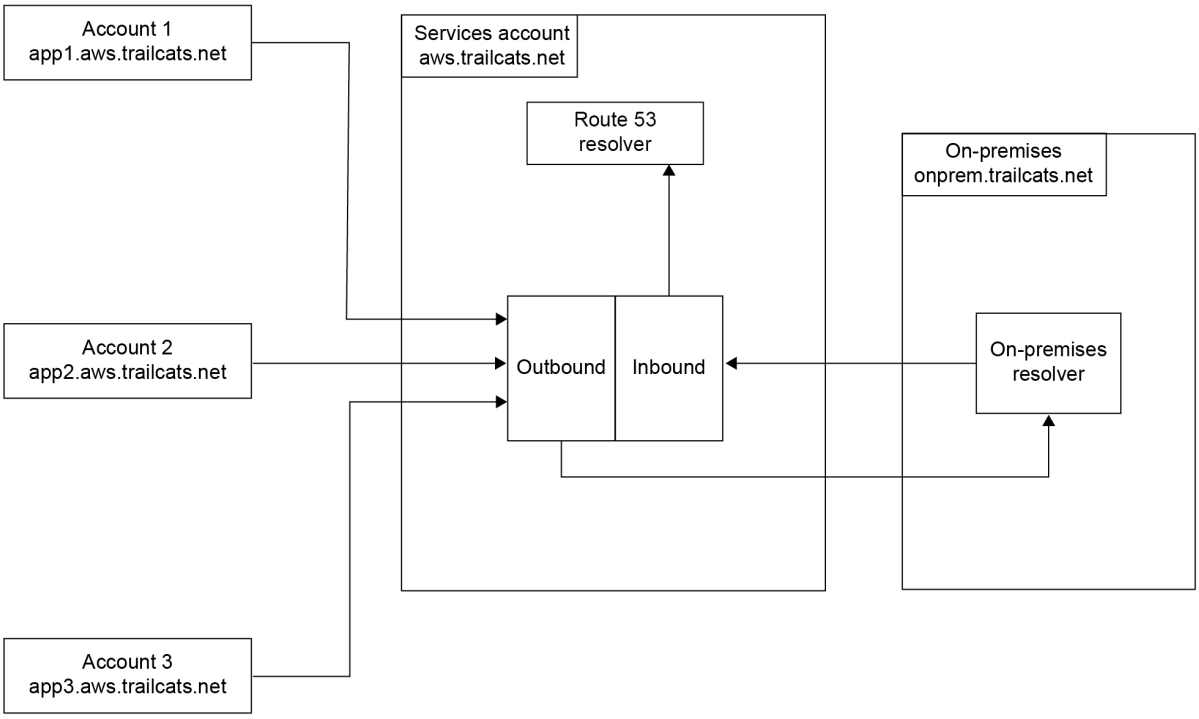

AWS cloud
Account 1
app1.aws.trailcats.net
App1 VPC
Account 2
app2.aws.trailcats.net
App2 VPC
Account 3
app3.aws.trailcats.net
App3 VPC
Services account
aws.trailcats.net
Services VPC
Corporate data center
On-premises
onprem.trailcats.net

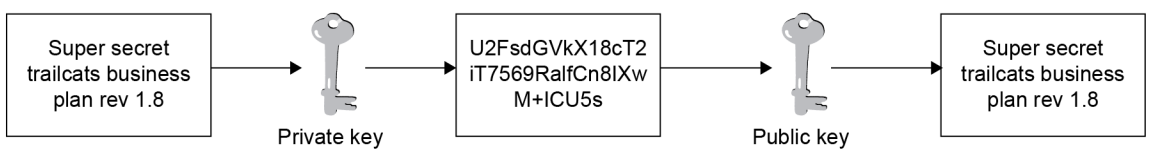

Account 1
app1.aws.trailcats.net
App1 VPC
Shared query logging configuration
Account 2
app2.aws.trailcats.net
App2 VPC
Shared query logging configuration
Account 3
app3.aws.trailcats.net
App3 VPC
Shared query logging configuration
Services account
aws.trailcats.net
Query logging configuration
S3 bucket

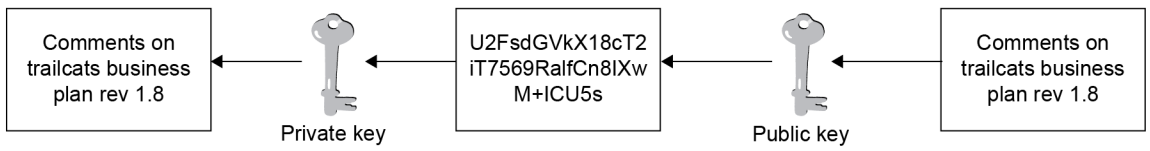

Services
Search
[Alt+S]
N. Virginia
S3
EC2
VPC
CloudFormation
Route 53
CloudWatch
CloudTrail
Control Tower
Route 53
Dashboard
Hosted zones
Health checks
Profiles New
IP-based routing
CIDR collections
Traffic flow
Traffic policies
Policy records
Domains
Registered domains
Pending requests
Resolver
VPCs
Inbound endpoints
Outbound endpoints
Rules
Query logging
1
Route 53 > Resolver > Query logging > ResolverQueryConfiguration
ResolverQueryConfiguration Info
Share configuration
Delete
2
ResolverQueryConfiguration configuration
ID
rqlc-1e201b76e5a140c5
Status
Created
Sharing status Info
Not shared
Destination type
CloudWatch Logs log group
VPC count
3
Owner
361037072889
Destination ARN Info
arn:aws:logs:us-east-1:361037072889:log-group:Route53Resolver
Creation time (UTC)
2024-08-02T03:07:14.698989482Z
ARN
arn:aws:route53resolver:us-east-1:361037072889:resolver-query-log-config/rqlc-1e201b76e5a140c5
VPCs that queries are logged for (3) Info
View details
Stop logging queries
Add VPC
Resolver logs DNS queries that originate in the VPCs that you choose here. If you don't choose any VPCs, Resolver doesn't log any queries.

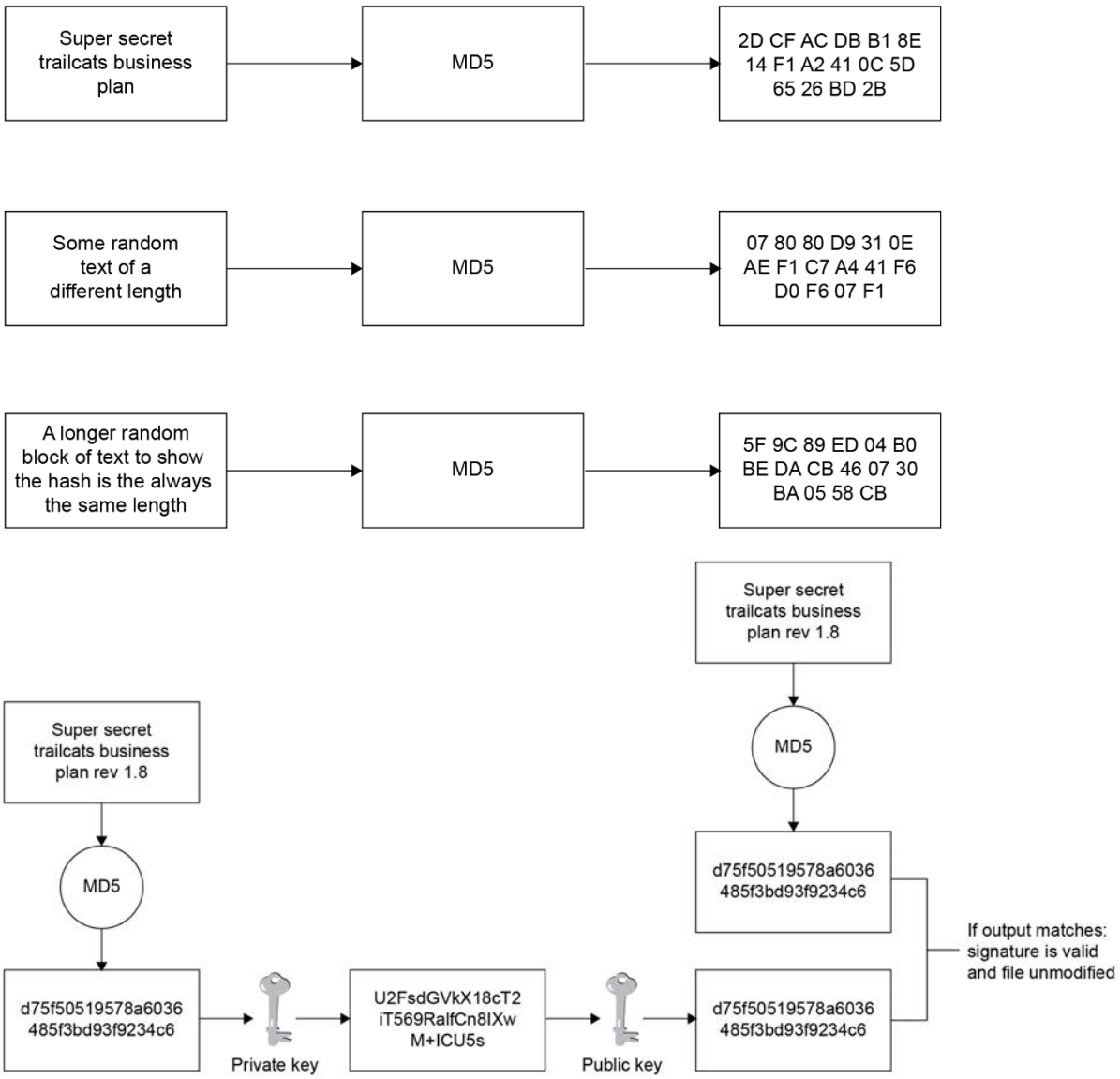

Account 1
app1.aws.trailcats.net
App1 VPC
Shared forwarding rules
Account 2
app2.aws.trailcats.net
App2 VPC
Shared query logging configuration
Account 3
app3.aws.trailcats.net
App3 VPC
Shared query logging configuration
Services account
aws.trailcats.net
Forwarding rules
Outbound
Services VPC
On-premises
onprem.trailcats.net
On-premises resolver

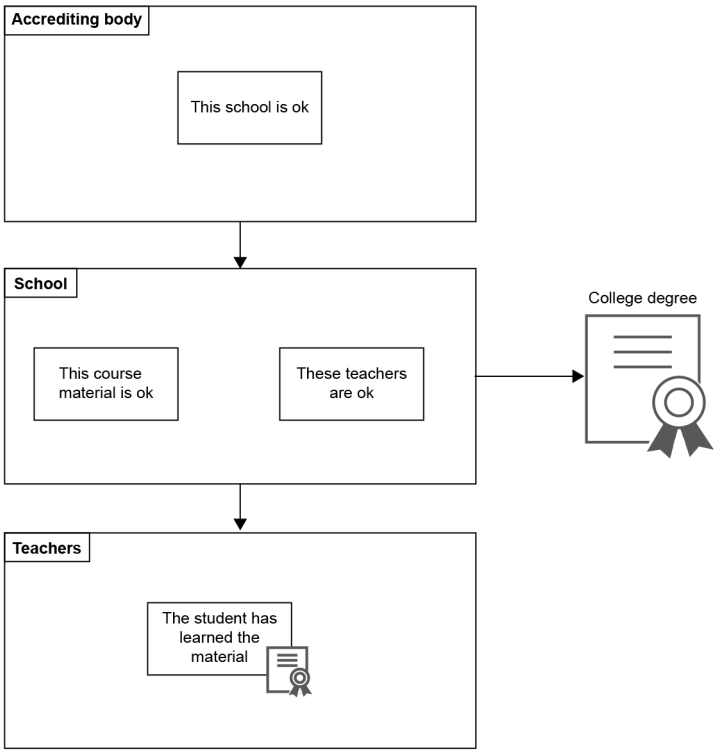

Account 1
app1.aws.trailcats.net
App1 VPC
Account 2
app2.aws.trailcats.net
App2 VPC
Account 3
app3.aws.trailcats.net
App3 VPC
Services account
aws.trailcats.net
Route 53
resolver
Outbound
Inbound
Services VPC
On-premises
onprem.trailcats.net
On-premises
resolver

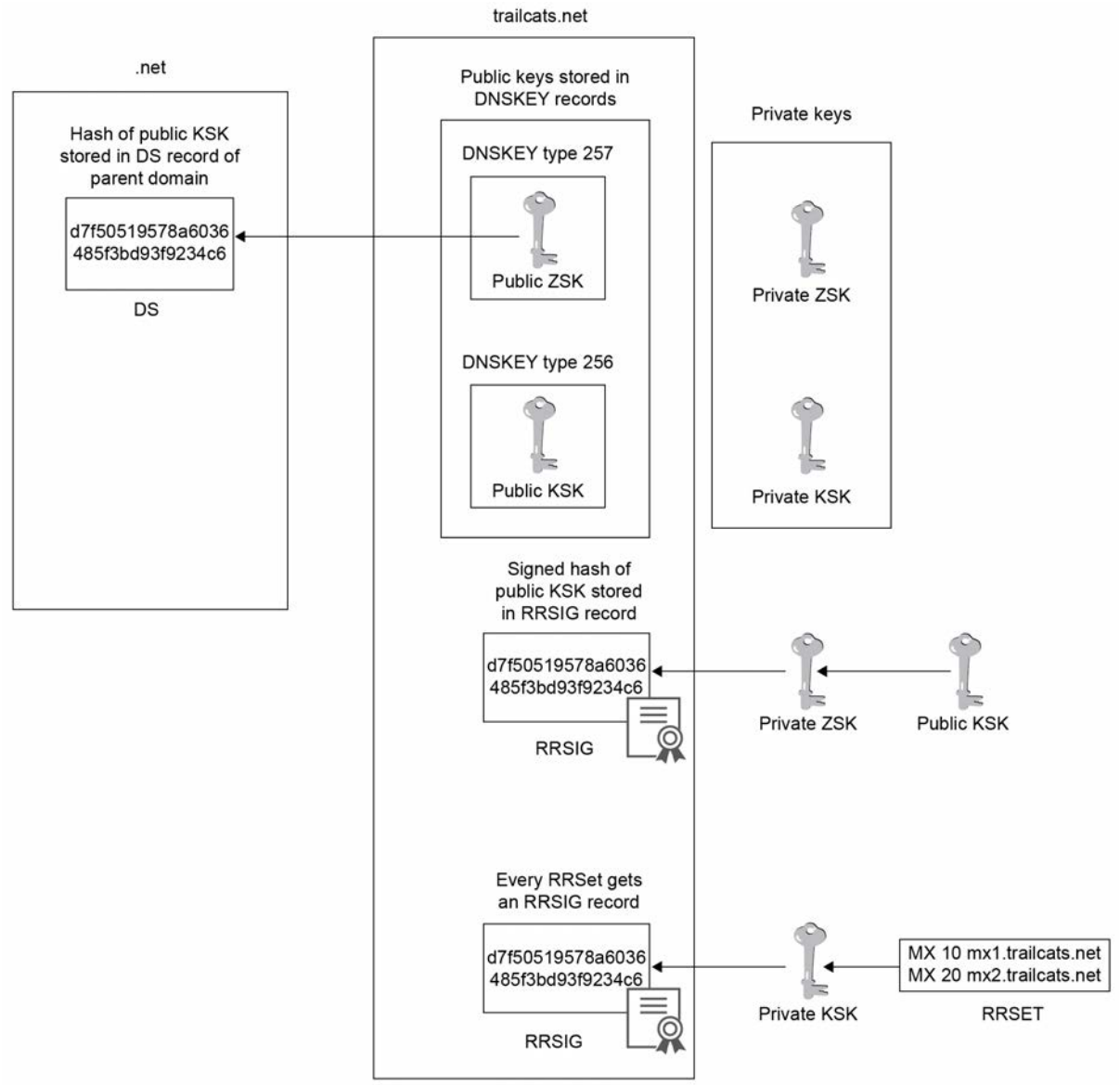

Account 1
app1.aws.trailcats.net
Account 2
app2.aws.trailcats.net
Account 3
app3.aws.trailcats.net
Services account
aws.trailcats.net
Route 53
resolver
Outbound
Inbound
On-premises
onprem.trailcats.net
On-premises
resolver

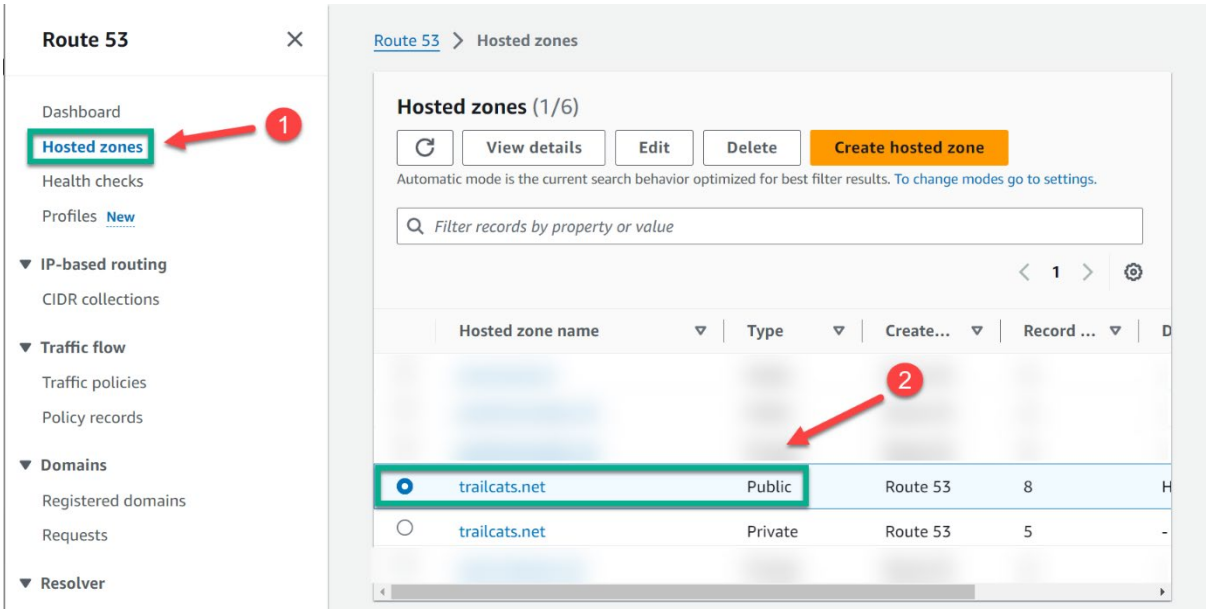

Super secret
trailcats business
plan rev 1.8
Private key
U2FsdGVkX18cT2
iT7569RalfCn8IXw
M+ICU5s
Public key
Super secret
trailcats business
plan rev 1.8

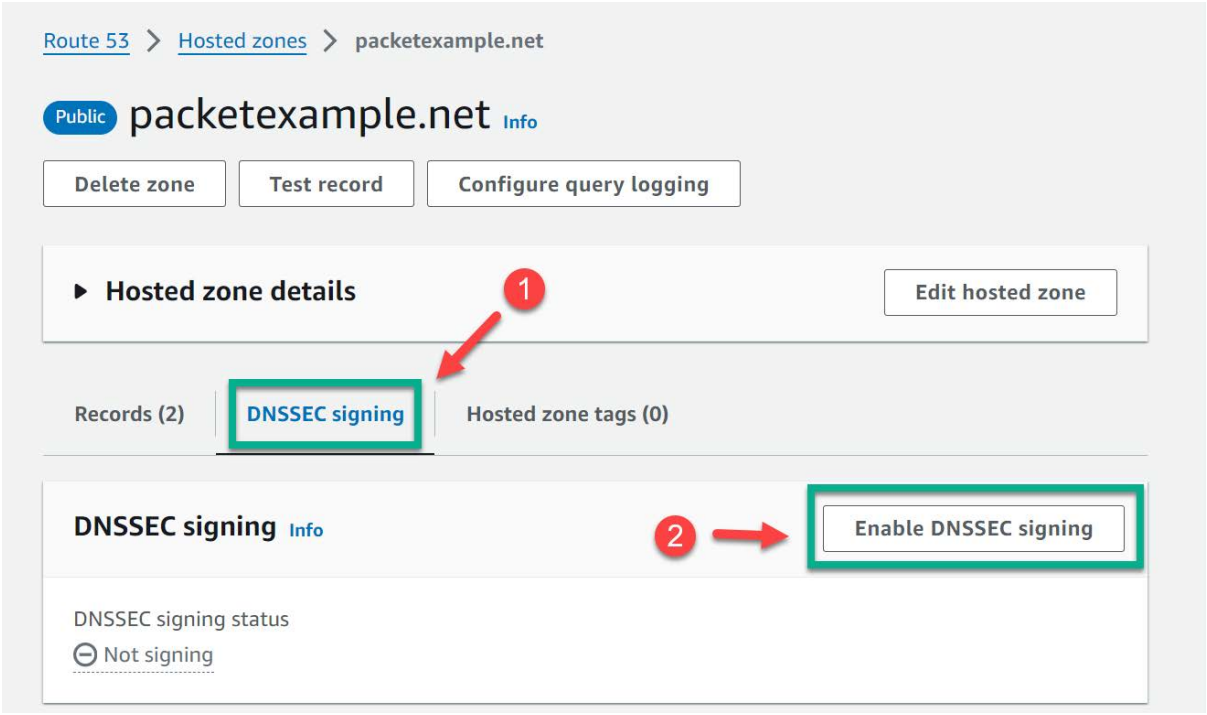

Comments on
trailcats business
plan rev 1.8
Private key
U2FsdGVkX18cT2
iT7569RalfCn8IXw
M+ICU5s
Public key
Comments on
trailcats business
plan rev 1.8

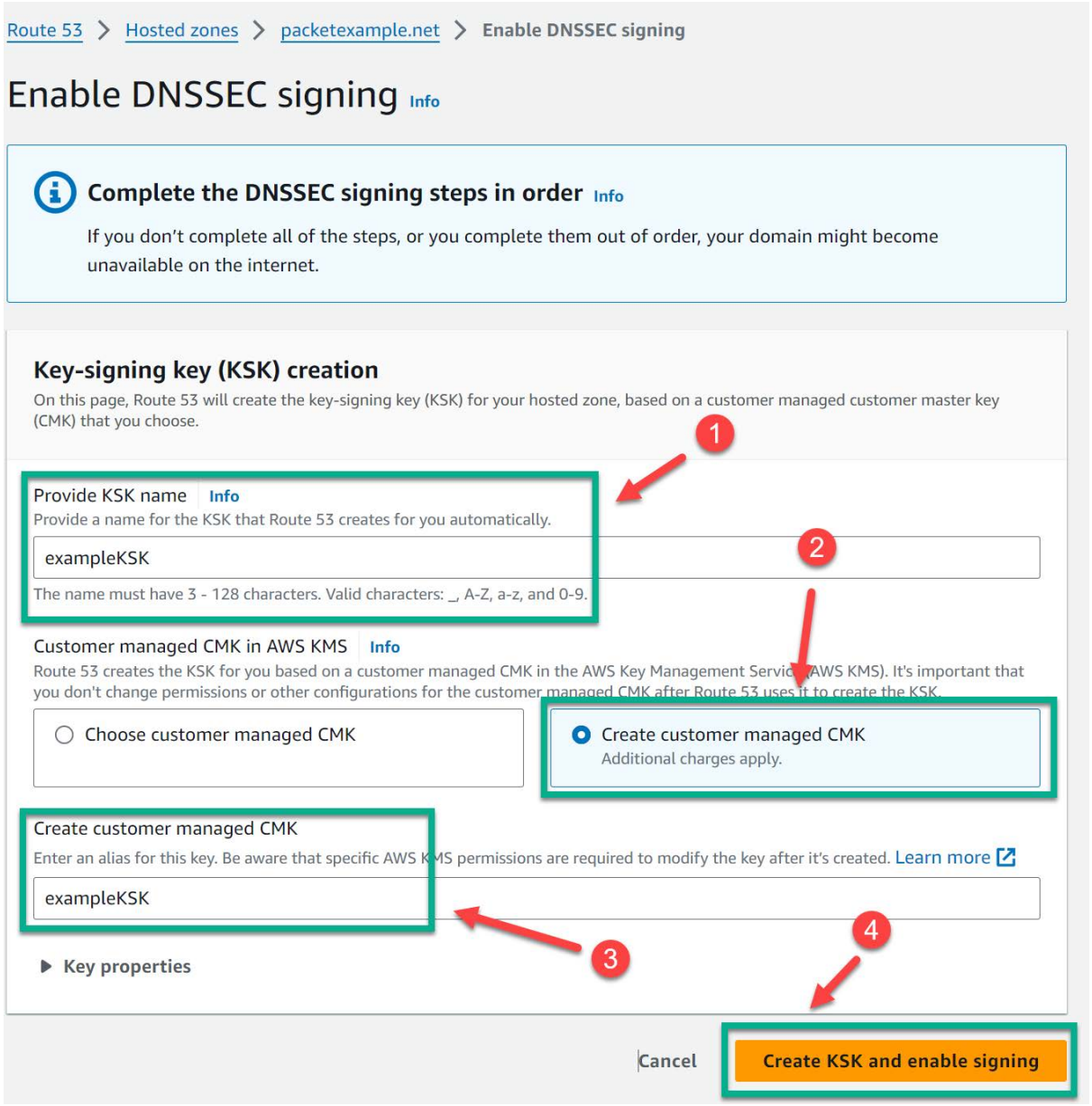

Super secret trailcats business plan
MD5
2D CF AC DB B1 8E 14 F1 A2 41 0C 5D 65 26 BD 2B
Some random text of a different length
MD5
07 80 80 D9 31 0E AE F1 C7 A4 41 F6 D0 F6 07 F1
A longer random block of text to show the hash is the always the same length
MD5
5F 9C 89 ED 04 B0 BE DA CB 46 07 30 BA 05 58 CB
Super secret trailcats business plan rev 1.8
MD5
d75f50519578a6036 485f3bd93f9234c6
Super secret trailcats business plan rev 1.8
MD5
d75f50519578a6036 485f3bd93f9234c6
Private key
U2FsdGVkX18cT2 iT569RalfCn8IXw M+ICU5s
Public key
d75f50519578a6036 485f3bd93f9234c6
If output matches: signature is valid and file unmodified

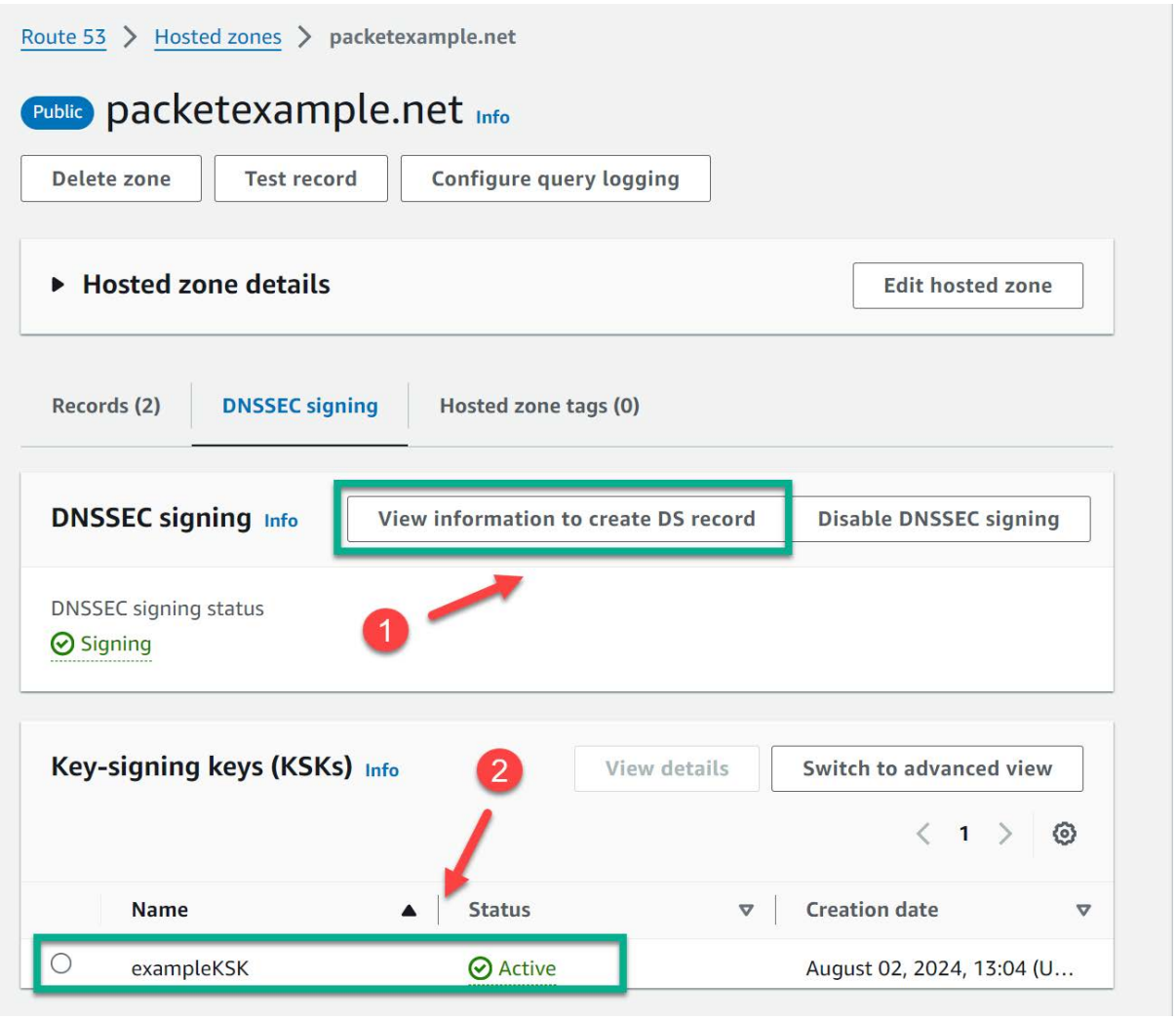

Accrediting body
This school is ok
School
This course material is ok
These teachers are ok
College degree
Teachers
The student has learned the material

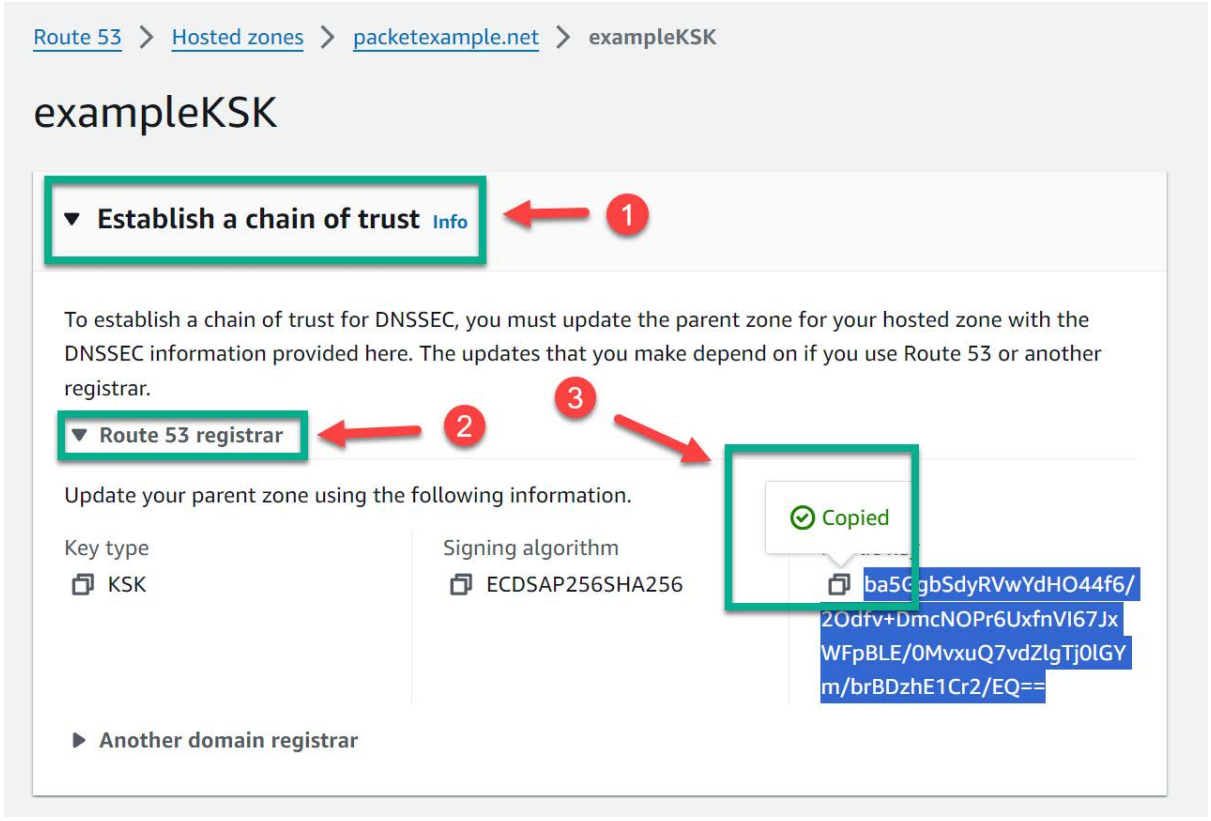

trailcats.net
.net
Hash of public KSK stored in DS record of parent domain
d7f50519578a6036 485f3bd93f9234c6
DS
Public keys stored in DNSKEY records
DNSKEY type 257
Public ZSK
DNSKEY type 256
Public KSK
Private keys
Private ZSK
Private KSK
Signed hash of public KSK stored in RRSIG record
d7f50519578a6036 485f3bd93f9234c6
RRSIG
Private ZSK
Public KSK
Every RRSet gets an RRSIG record
d7f50519578a6036 485f3bd93f9234c6
RRSIG
Private KSK
MX 10 mx1.trailcats.net
MX 20 mx2.trailcats.net
RRSET

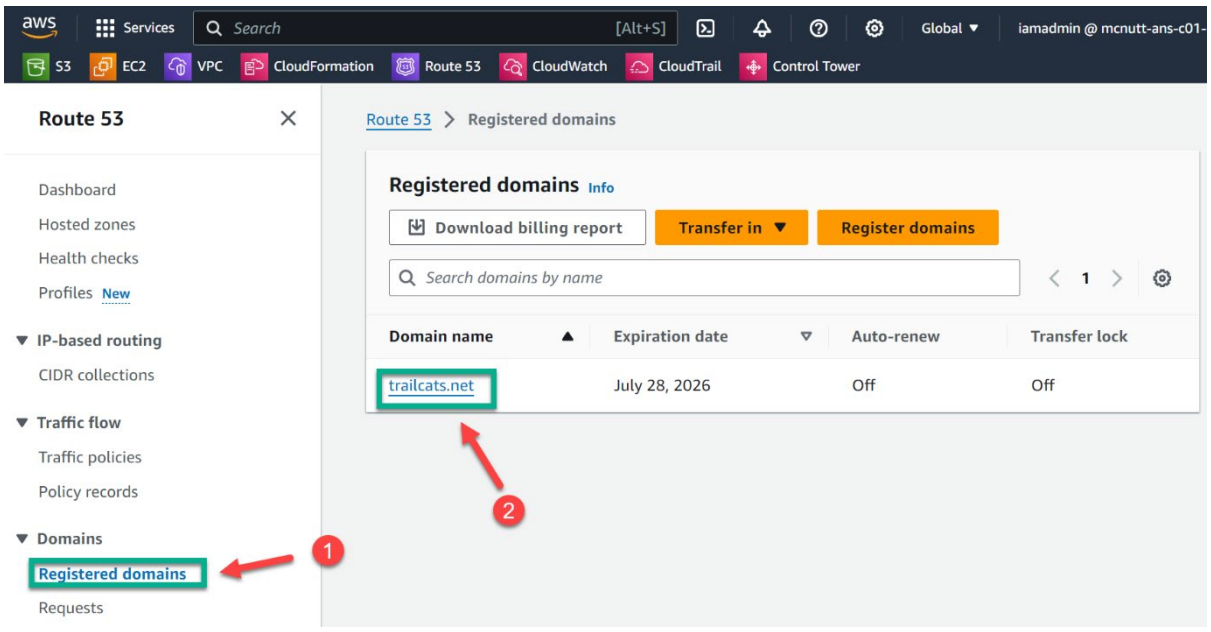

Route 53
Dashboard
Hosted zones
Health checks
Profiles New
IP-based routing
CIDR collections
Traffic flow
Traffic policies
Policy records
Domains
Registered domains
Requests
Resolver
1
Route 53 > Hosted zones
Hosted zones (1/6)
View details
Edit
Delete
Create hosted zone
Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.
Filter records by property or value
Hosted zone name
Type
Create...
Record ...
2
trailcats.net
Public
Route 53
8
trailcats.net
Private
Route 53
5

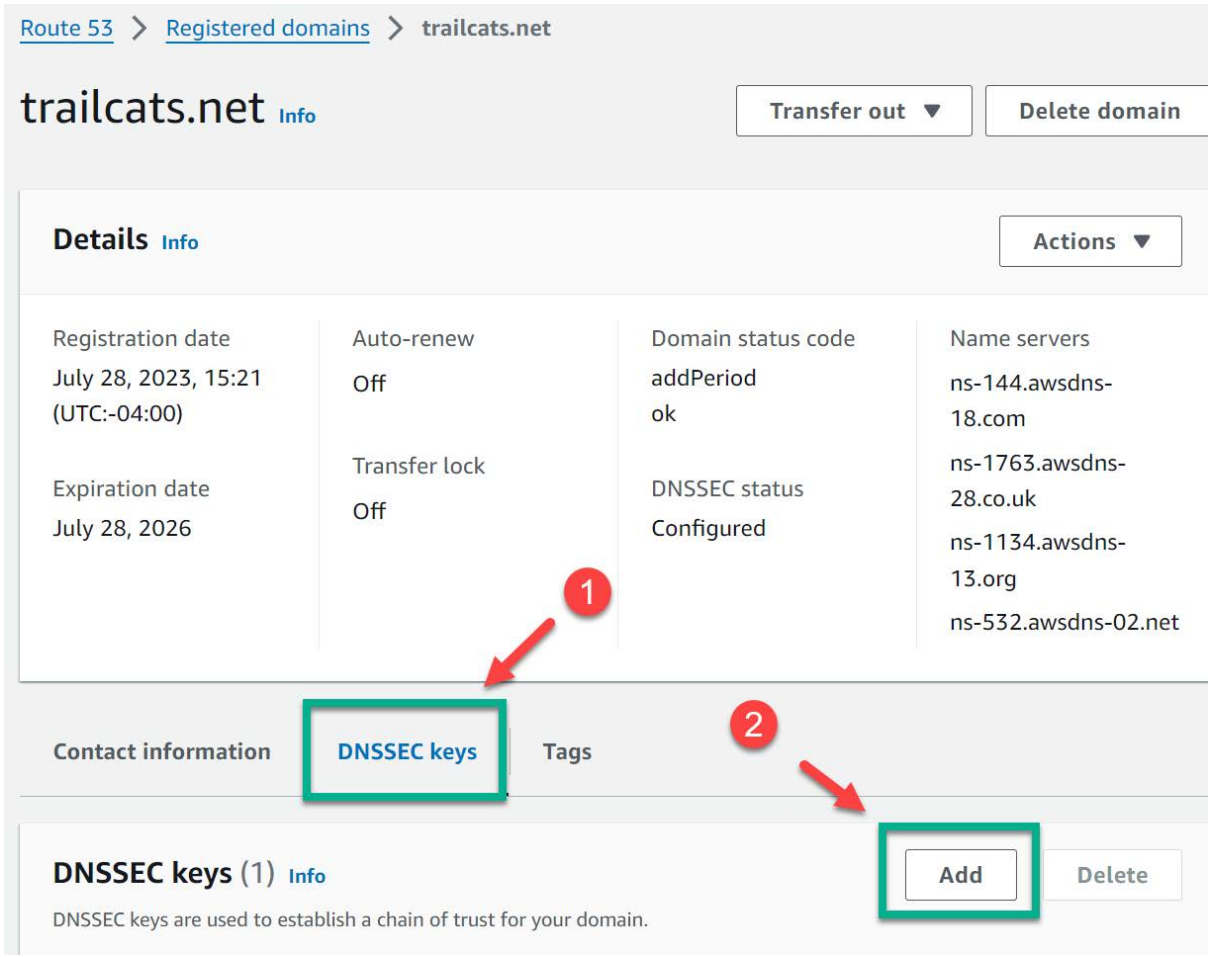

Route 53 > Hosted zones > packetexample.net
Public packetexample.net Info
Delete zone
Test record
Configure query logging
Hosted zone details
Edit hosted zone
1
Records (2)
DNSSEC signing
Hosted zone tags (0)
DNSSEC signing Info
2
Enable DNSSEC signing
DNSSEC signing status
Not signing

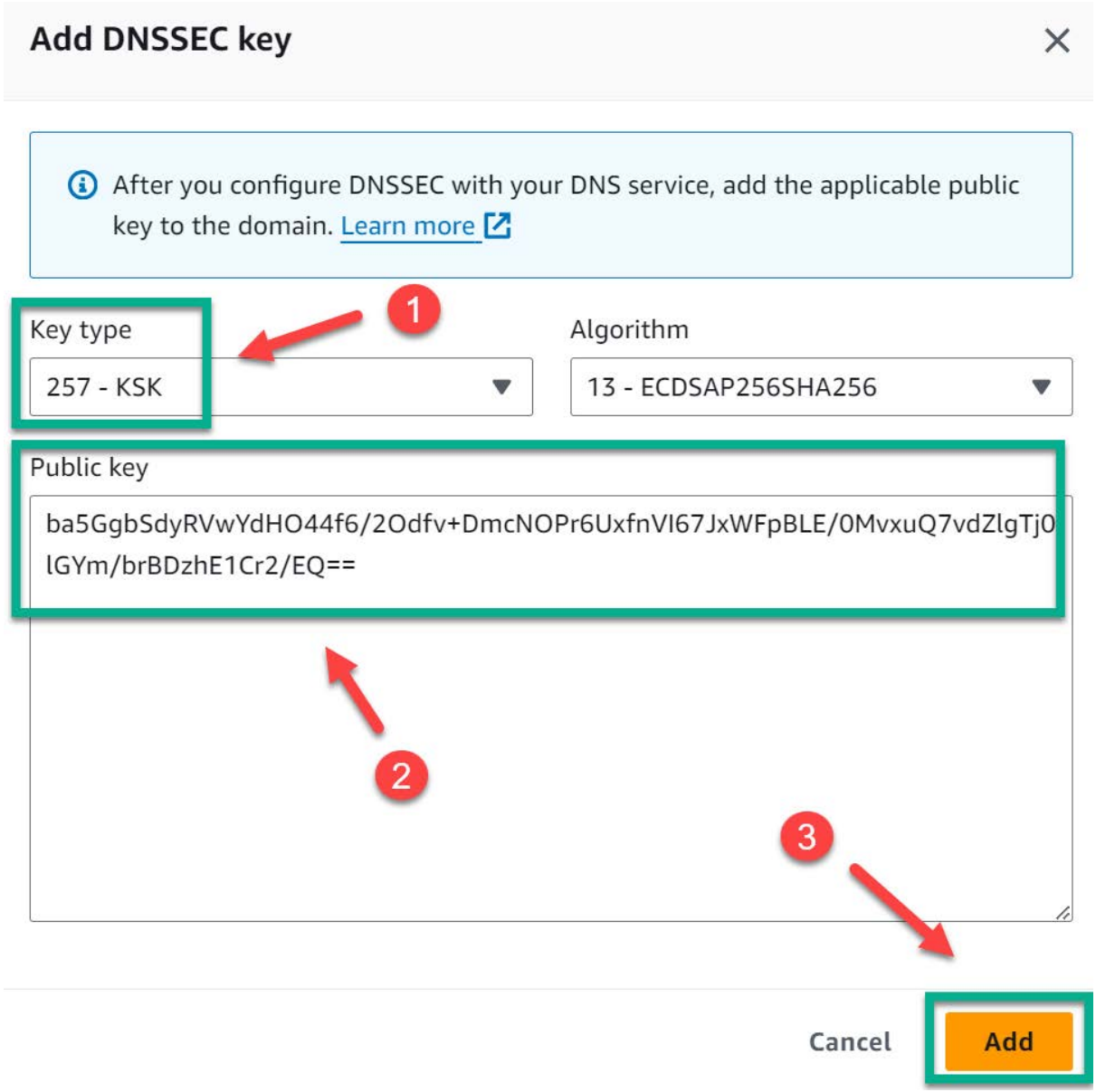

Route 53 > Hosted zones > packetexample.net > Enable DNSSEC signing
Enable DNSSEC signing Info
Complete the DNSSEC signing steps in order Info
If you don't complete all of the steps, or you complete them out of order, your domain might become unavailable on the internet.
Key-signing key (KSK) creation
On this page, Route 53 will create the key-signing key (KSK) for your hosted zone, based on a customer managed customer master key (CMK) that you choose.
1
Provide KSK name Info
Provide a name for the KSK that Route 53 creates for you automatically.
exampleKSK
The name must have 3 - 128 characters. Valid characters: _, A-Z, a-z, and 0-9.
2
Customer managed CMK in AWS KMS Info
Route 53 creates the KSK for you based on a customer managed CMK in the AWS Key Management Servic (AWS KMS). It's important that you don't change permissions or other configurations for the customer managed CMK after Route 53 uses it to create the KSK.
Choose customer managed CMK
Create customer managed CMK
Additional charges apply.
Create customer managed CMK
Enter an alias for this key. Be aware that specific AWS KMS permissions are required to modify the key after it's created. Learn more
exampleKSK
3
Key properties
4
Cancel
Create KSK and enable signing


Route 53 > Hosted zones > packetexample.net
Public packetexample.net Info
Delete zone
Test record
Configure query logging
Hosted zone details
Edit hosted zone
Records (2)
DNSSEC signing
Hosted zone tags (0)
DNSSEC signing Info
View information to create DS record
Disable DNSSEC signing
DNSSEC signing status
Signing
1
Key-signing keys (KSKs) Info
2
View details
Switch to advanced view
1
Name
Status
Creation date
exampleKSK
Active
August 02, 2024, 13:04 (U...

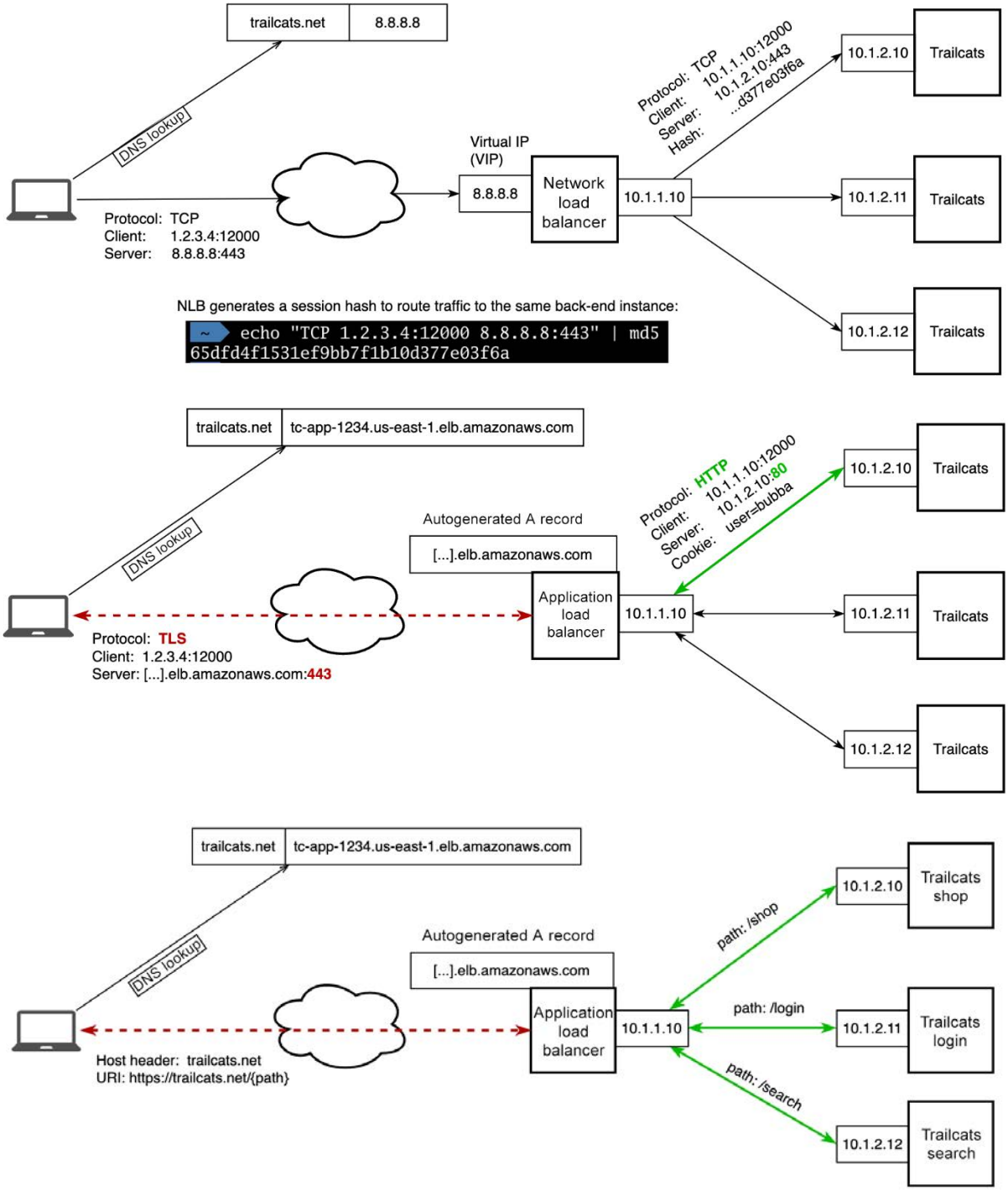

Route 53 > Hosted zones > packetexample.net > exampleKSK
exampleKSK
Establish a chain of trust Info
1
To establish a chain of trust for DNSSEC, you must update the parent zone for your hosted zone with the DNSSEC information provided here. The updates that you make depend on if you use Route 53 or another registrar.
Route 53 registrar
2
3
Update your parent zone using the following information.
Copied
Key type
KSK
Signing algorithm
ECDSAP256SHA256
ba5GgbSdyRVwYdHO44f6/2Odfv+DmcNOPr6UxfnVI67JxWFpBLE/0MvxuQ7vdZlgTj0lGYm/brBDzhE1Cr2/EQ==
Another domain registrar


aws
Services
Search
[Alt+S]
Global
iamadmin @ mcnutt-ans-c01-
S3
EC2
VPC
CloudFormation
Route 53
CloudWatch
CloudTrail
Control Tower
Route 53
Dashboard
Hosted zones
Health checks
Profiles New
IP-based routing
CIDR collections
Traffic flow
Traffic policies
Policy records
Domains
Registered domains
Requests
1
Route 53 > Registered domains
Registered domains Info
Download billing report
Transfer in
Register domains
Search domains by name
1
Domain name
Expiration date
Auto-renew
Transfer lock
trailcats.net
July 28, 2026
Off
Off
2

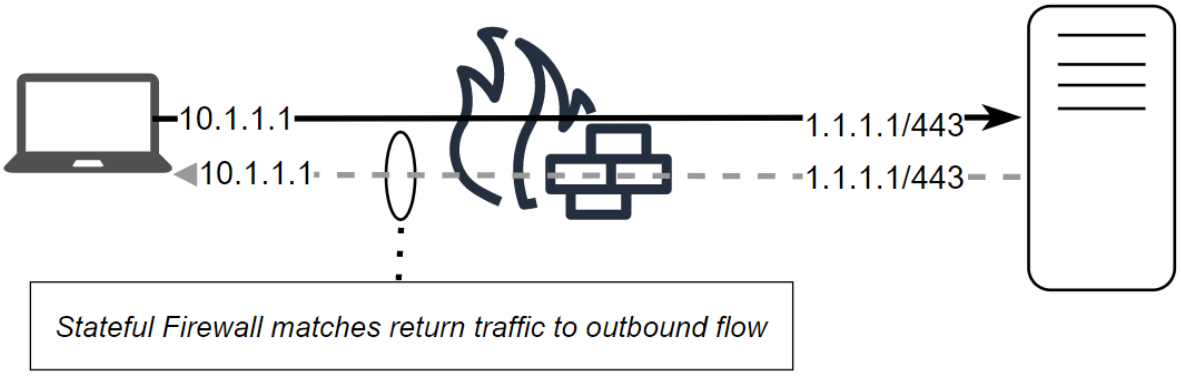

Route 53 > Registered domains > trailcats.net
trailcats.net Info
Transfer out
Delete domain
Details Info
Actions
Registration date
July 28, 2023, 15:21
(UTC:-04:00)
Expiration date
July 28, 2026
Auto-renew
Off
Transfer lock
Off
Domain status code
addPeriod
ok
DNSSEC status
Configured
Name servers
ns-144.awsdns-18.com
ns-1763.awsdns-28.co.uk
ns-1134.awsdns-13.org
ns-532.awsdns-02.net
1
2
Contact information
DNSSEC keys
Tags
DNSSEC keys (1) Info
DNSSEC keys are used to establish a chain of trust for your domain.
Add
Delete

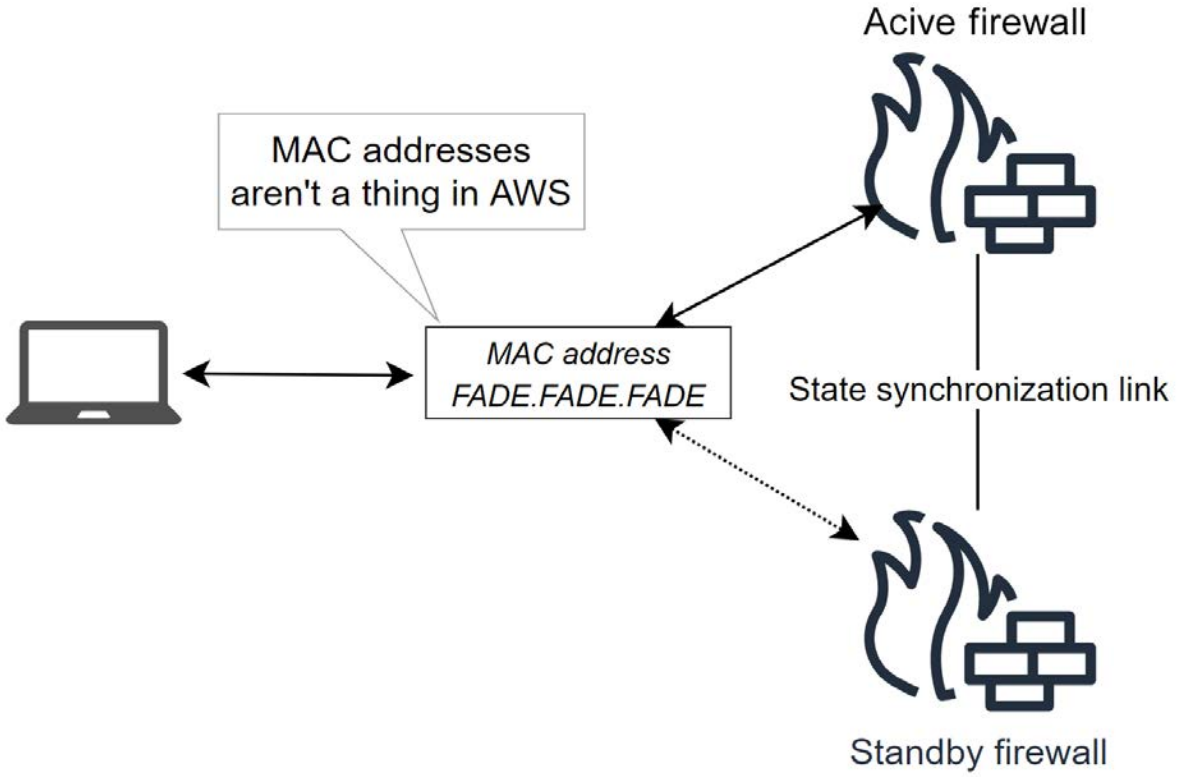

Add DNSSEC key
After you configure DNSSEC with your DNS service, add the applicable public key to the domain. Learn more
Key type
257 - KSK
Algorithm
13 - ECDSAP256SHA256
Public key
ba5GgbSdyRVwYdHO44f6/2Odfv+DmcNOPr6UxfnVI67JxWFpBLE/0MvxuQ7vdZlgTj0
lGYm/brBDzhE1Cr2/EQ==
1
2
3
Cancel
Add

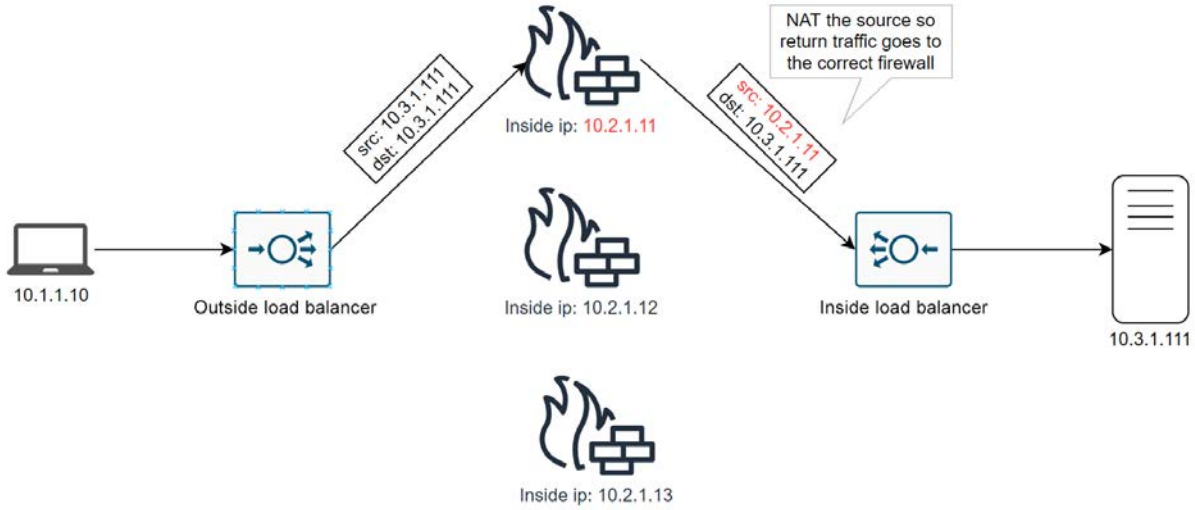
Chapter 9: AWS Elastic Load Balancing

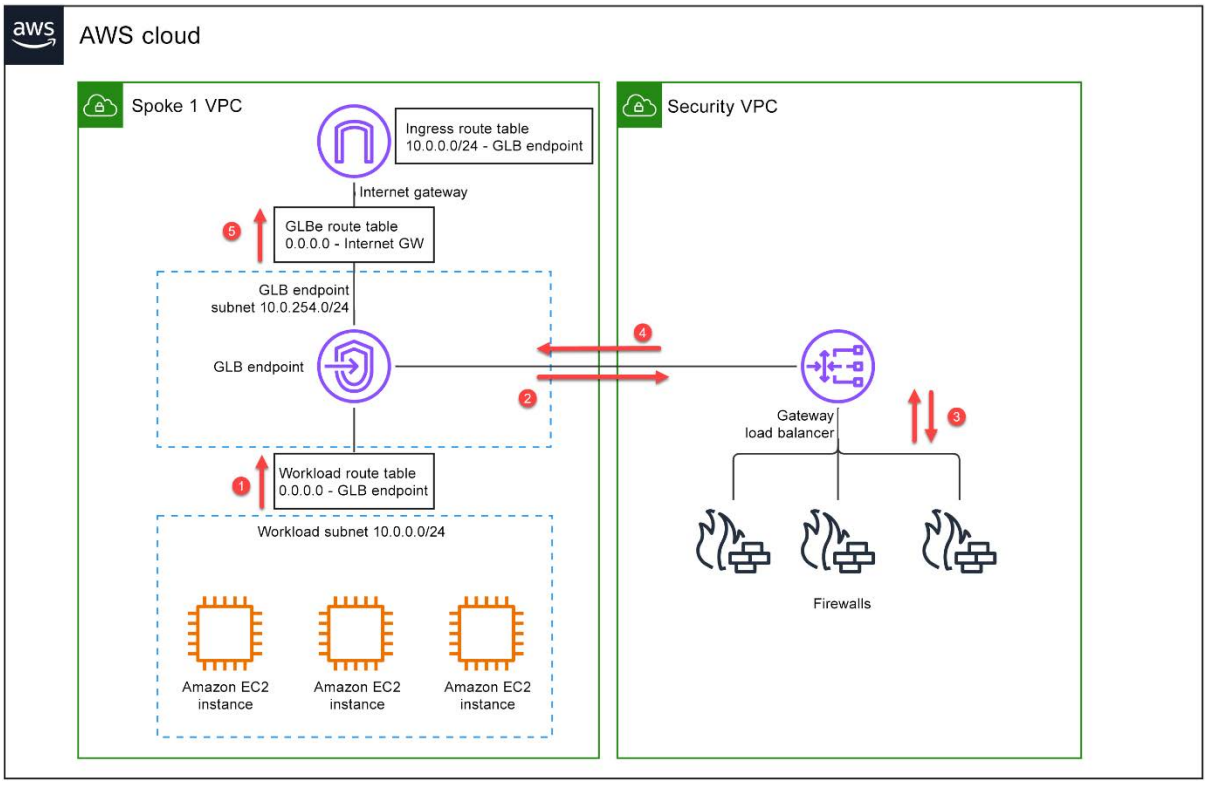


Firewall rule		
Source	Destination	Action
TCP/10.1.1.1/any	TCP/1.1.1.1/443	Allow

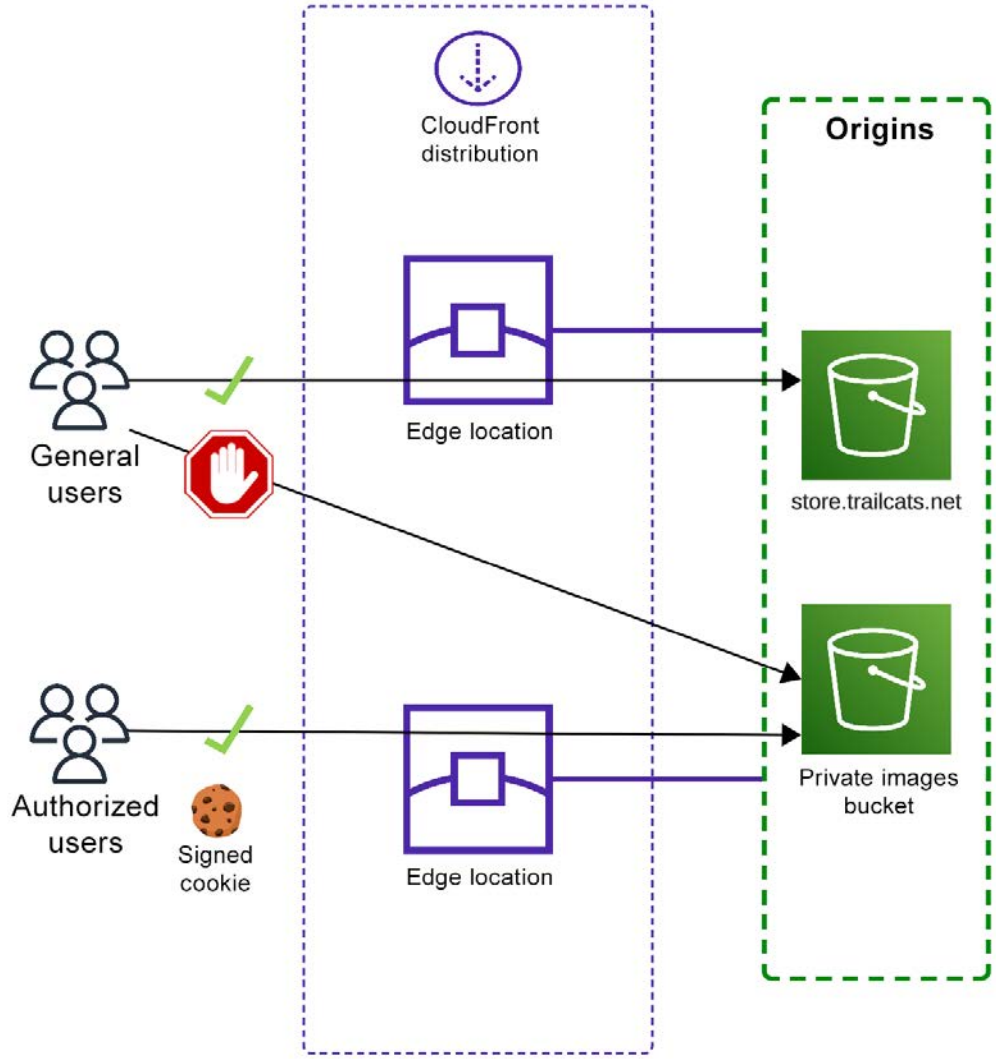


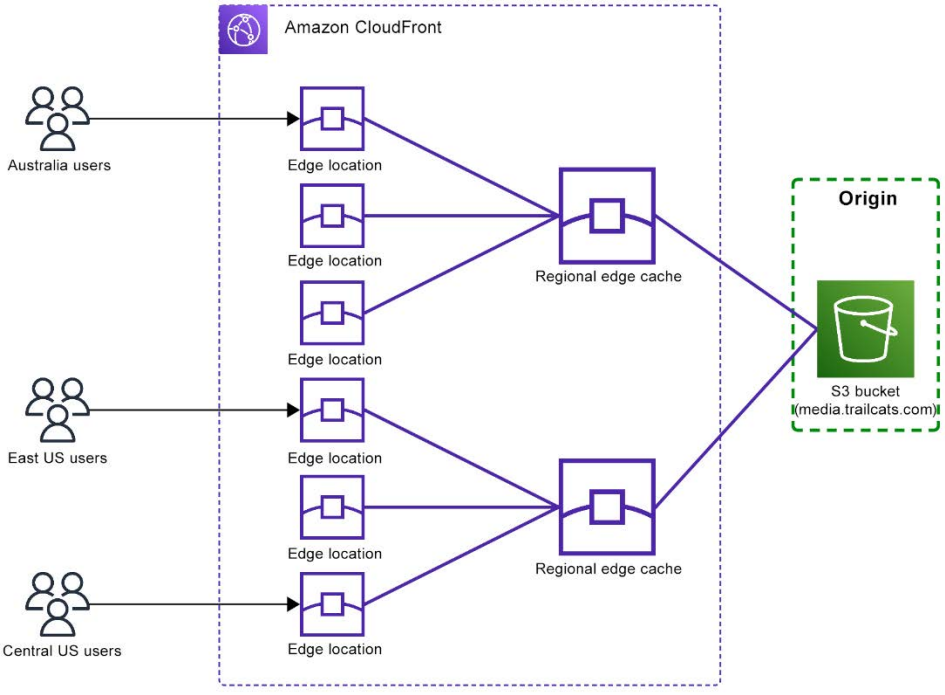


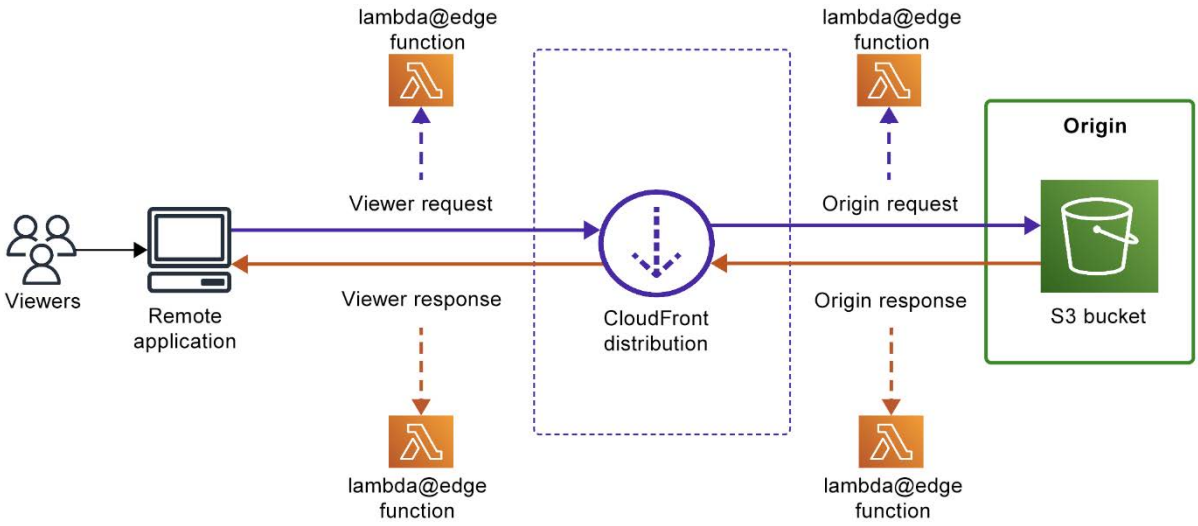

NAT the source so return traffic goes to the correct firewall
src: 10.3.1.111
dst: 10.3.1.111
Inside ip: 10.2.1.11
src: 10.2.1.11
dst: 10.3.1.111
10.1.1.10
Outside load balancer
Inside ip: 10.2.1.12
Inside load balancer
10.3.1.111
Inside ip: 10.2.1.13


AWS cloud
Spoke 1 VPC
Ingress route table
10.0.0.0/24 - GLB endpoint
Internet gateway
GLBe route table
0.0.0.0 - Internet GW
GLB endpoint
subnet 10.0.254.0/24
GLB endpoint
Workload route table
0.0.0.0 - GLB endpoint
Workload subnet 10.0.0.0/24
Amazon EC2 instance
Amazon EC2 instance
Amazon EC2 instance
Security VPC
Gateway load balancer
Firewalls

Chapter 10: AWS CDN and Global Traffic Management



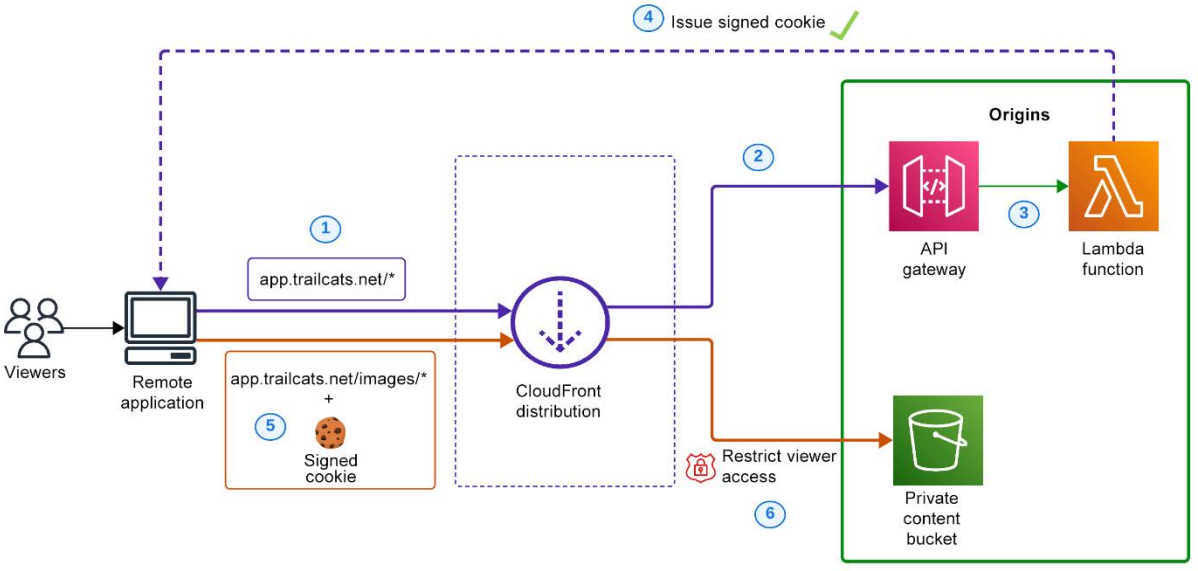


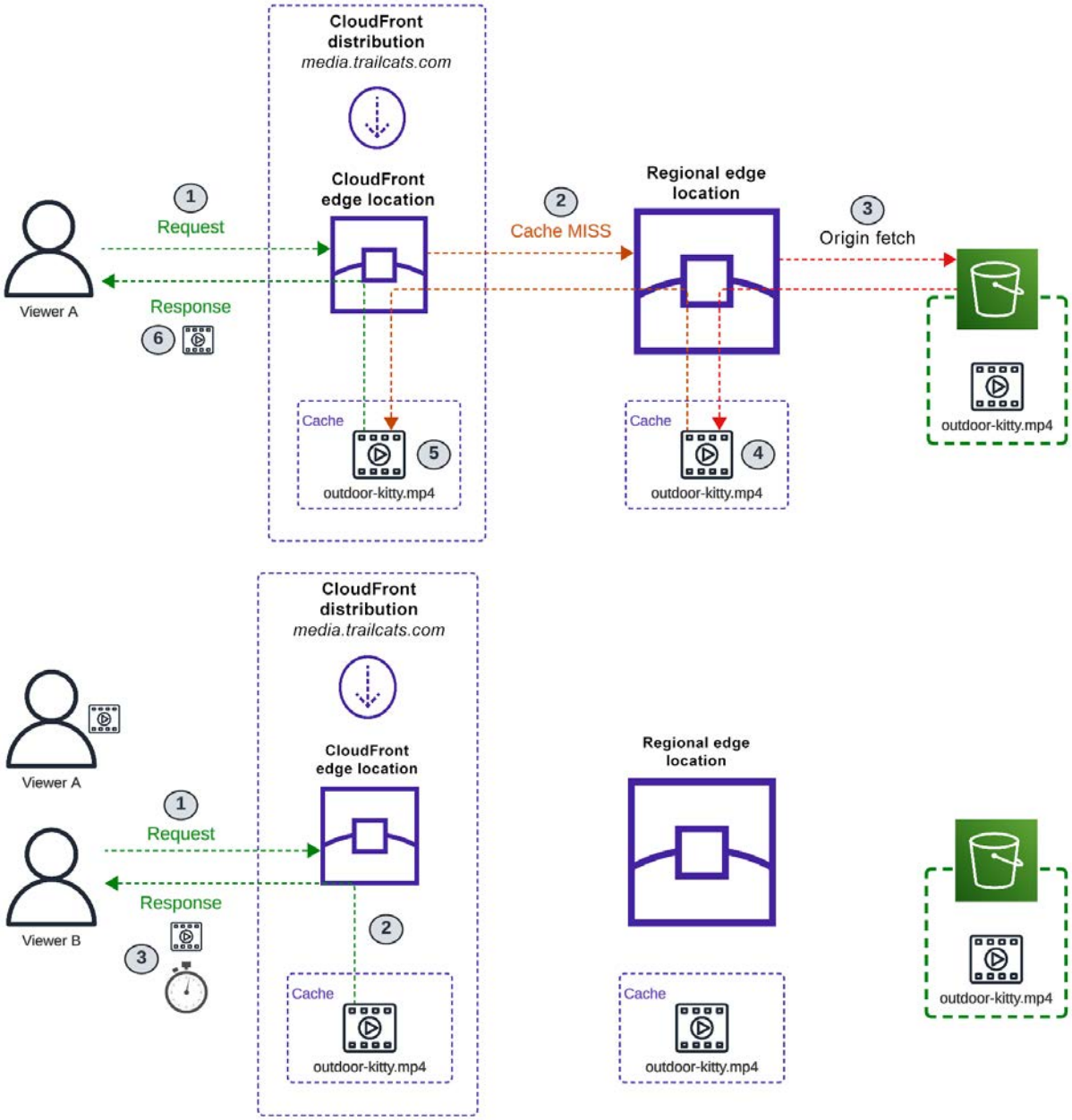


Function associations - *optional* Info

Choose an edge function to associate with this cache behavior, and the CloudFront event that invokes the function.

	Function type	Function ARN / Name	Include body
Viewer request	Lambda@Edge	arn:aws:lambda:us-east-1:1234567	☐
Viewer response	No association		
Origin request	Lambda@Edge	arn:aws:lambda:us-east-1:0987654	☐
Origin response	No association		




CloudFront distribution
media.trailcats.com
CloudFront edge location
Regional edge location
1
Request
2
Cache MISS
3
Origin fetch
Viewer A
Response
6
Cache
5
outdoor-kitty.mp4
Cache
4
outdoor-kitty.mp4
outdoor-kitty.mp4
CloudFront distribution
media.trailcats.com
Viewer A
CloudFront edge location
Regional edge location
1
Request
Viewer B
Response
3
2
Cache
outdoor-kitty.mp4
Cache
outdoor-kitty.mp4
outdoor-kitty.mp4

Cache key and origin requests

We recommend using a cache policy and origin request policy to control the cache key and origin requests.

- ○ Cache policy and origin request policy (recommended)
- ◉ Legacy cache settings

Headers

Choose which headers to include in the cache key.

None

Query strings

Choose which query strings to include in the cache key.

None

Cookies

Choose which cookies to include in the cache key.

None

Object caching

- ○ Use origin cache headers
- ◉ Customize

Minimum TTL	Maximum TTL	Default TTL
Minimum time to live in seconds.	Maximum time to live in seconds.	Default time to live in seconds.
0	31536000	86400

Create invalidation

Object paths Info

Add object paths

Add each object path to remove from the CloudFront cache. To use wildcards (*) in the invalidation, you must put the wildcard at the end of the path.

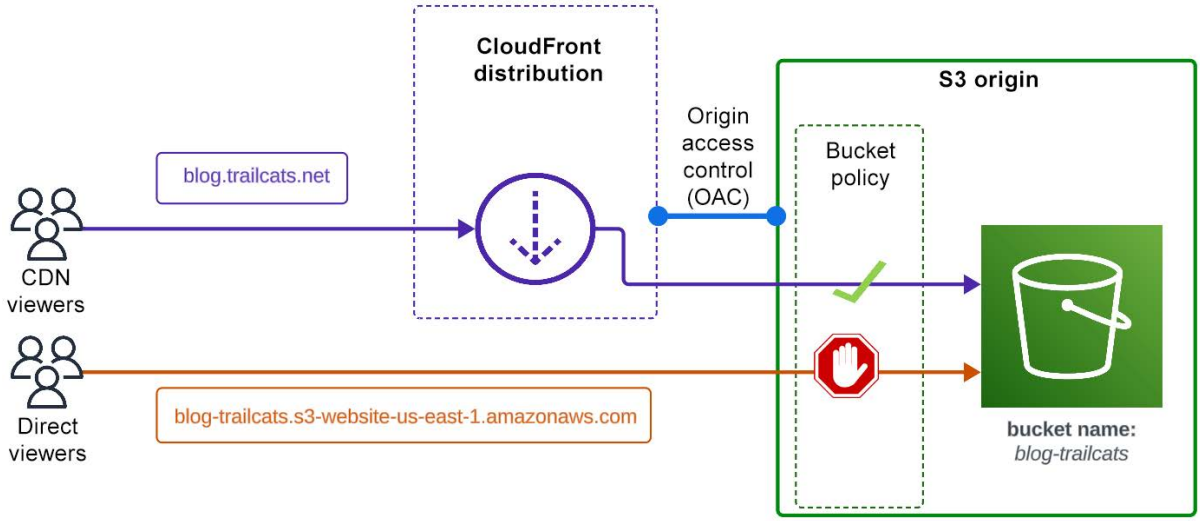
/media/videos/outdoor-kitty.mp4

To add object paths individually, use the standard editor.

Cancel | Create invalidation

Viewer protocol policy

- ◉ HTTP and HTTPS
- ○ Redirect HTTP to HTTPS
- ○ HTTPS only



Origin access Info

- Public
  Bucket must allow public access.
- Origin access control settings (recommended)
  Bucket can restrict access to only CloudFront.
- Legacy access identities
  Use a CloudFront origin access identity (OAI) to access the S3 bucket.

Origin access control

Select an existing origin access control (recommended) or create a new control.

Select an origin access control ▼ | Create new OAC

Add custom header - *optional*

CloudFront includes this header in all requests that it sends to your origin.

Add header

Enable Origin Shield

Origin shield is an additional caching layer that can help reduce the load on your origin and help protect its availability.

- No
- Yes

▼ **Additional settings**

Create new OAC

Name

The name must be unique. Valid characters: letters, numbers and most special characters. Use up to 64 characters.

blog-trailcats.s3.us-east-1.amazonaws.com

Description - *optional*

The description can have up to 256 characters.

Enter description

Signing behavior

- ○ Do not sign requests
- ◉ Sign requests (recommended)
  - ☐ Do not override authorization header
    Do not sign if incoming request has authorization header.

Origin type

S3

The origin type must be the same type as origin domain.

Cancel Create

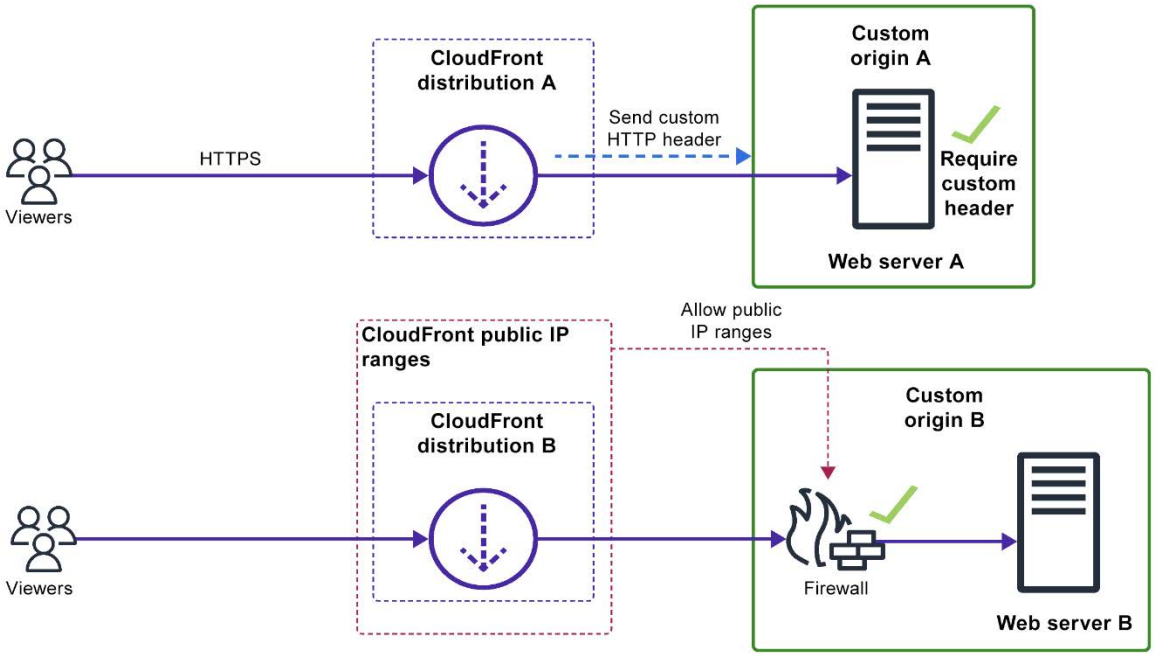
Bucket policy

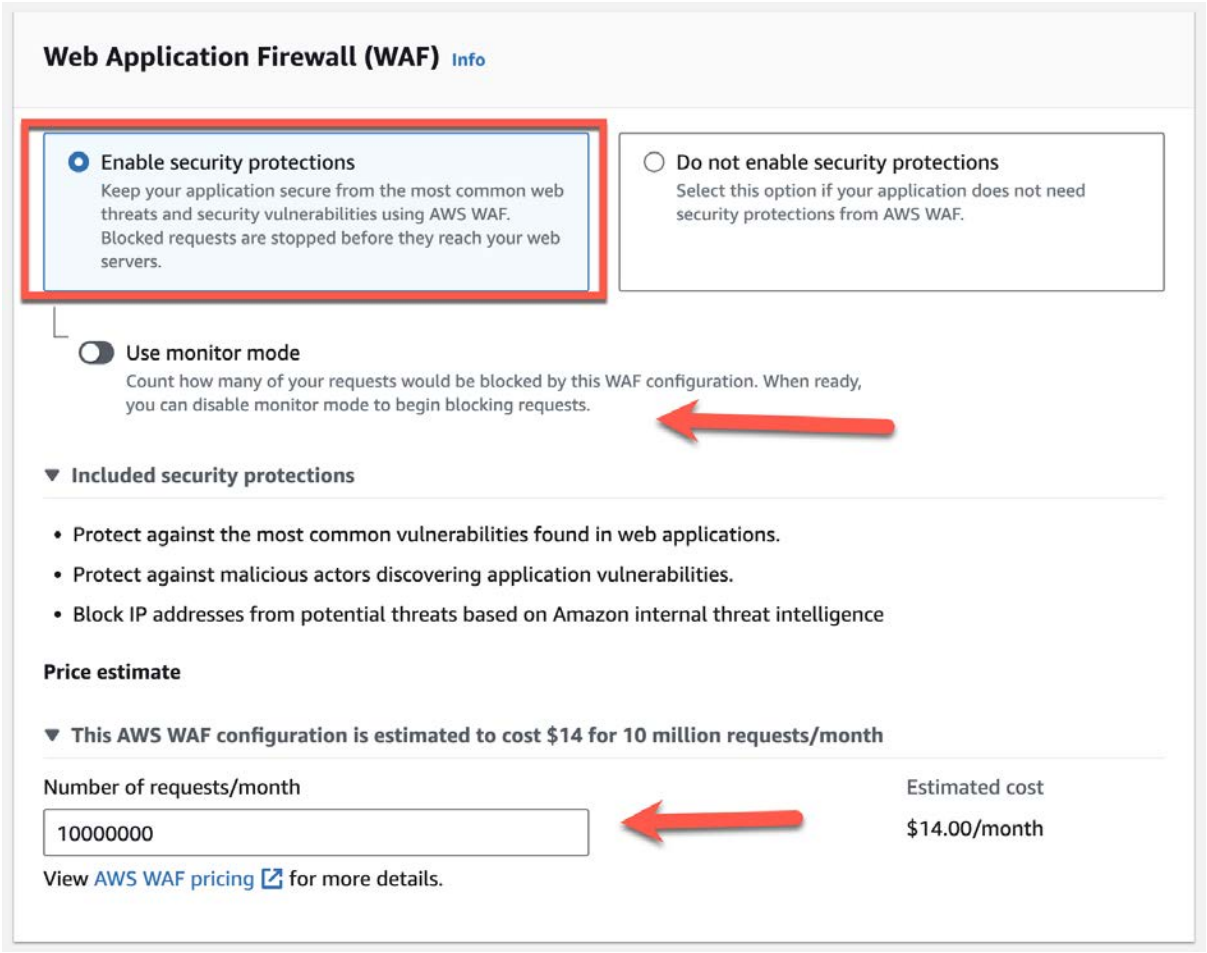
Edit | Delete

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts.
Learn more

Copy

```
{
  "Version": "2008-10-17",
  "Id": "PolicyForCloudFrontPrivateContent",
  "Statement": [
    {
      "Sid": "AllowCloudFrontServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudfront.amazonaws.com"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::blog-trailcats/*",
      "Condition": {
        "StringEquals": {
          "AWS:SourceArn": "arn:aws:cloudfront::[redacted]:distribution/E3LVSH6OTJ0YDK"
        }
      }
    }
  ]
}
```




Web Application Firewall (WAF) Info
Enable security protections
Keep your application secure from the most common web threats and security vulnerabilities using AWS WAF. Blocked requests are stopped before they reach your web servers.
Do not enable security protections
Select this option if your application does not need security protections from AWS WAF.
Use monitor mode
Count how many of your requests would be blocked by this WAF configuration. When ready, you can disable monitor mode to begin blocking requests.
Included security protections
Protect against the most common vulnerabilities found in web applications.
Protect against malicious actors discovering application vulnerabilities.
Block IP addresses from potential threats based on Amazon internal threat intelligence
Price estimate
This AWS WAF configuration is estimated to cost $14 for 10 million requests/month
Number of requests/month
10000000
Estimated cost
$14.00/month
View AWS WAF pricing for more details.

Alternate domain name (CNAME) - *optional*

Add the custom domain names that you use in URLs for the files served by this distribution.

test. .com **Remove**

Add item

Custom domain name

To add a list of alternative domain names, use the bulk editor.

Custom SSL certificate - *optional*

Associate a certificate from AWS Certificate Manager. The certificate must be in the US East (N. Virginia) Region (us-east-1).

test. .com ( )

test. .com Request certificate

SSL Certificate from ACM

Legacy clients support - $600/month prorated charge applies. Most customers do not need this.

CloudFront allocates dedicated IP addresses at each CloudFront edge location to serve your content over HTTPS.

☐ Enabled

For browsers that do not support SNI

Security policy

The security policy determines the SSL or TLS protocol and the specific ciphers that CloudFront uses for HTTPS connections with viewers (clients).

- ◉ TLSv1.2_2021 (recommended)
- ○ TLSv1.2_2019
- ○ TLSv1.2_2018
- ○ TLSv1.1_2016
- ○ TLSv1_2016
- ○ TLSv1

Supported HTTP versions

Add support for additional HTTP versions. HTTP/1.0 and HTTP/1.1 are supported by default.

- ☑ HTTP/2
- ☐ HTTP/3

CloudFront geographic restrictions

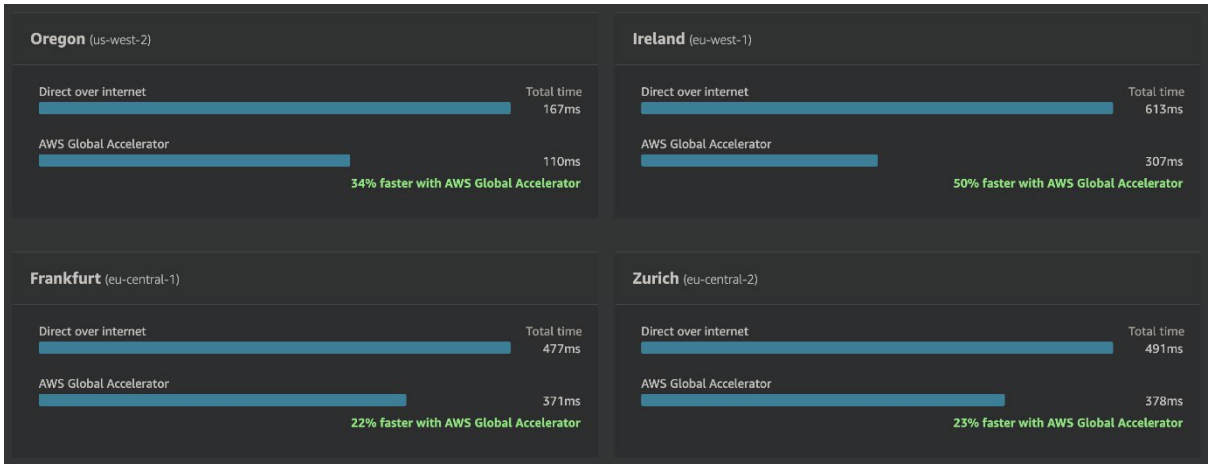
Restriction type

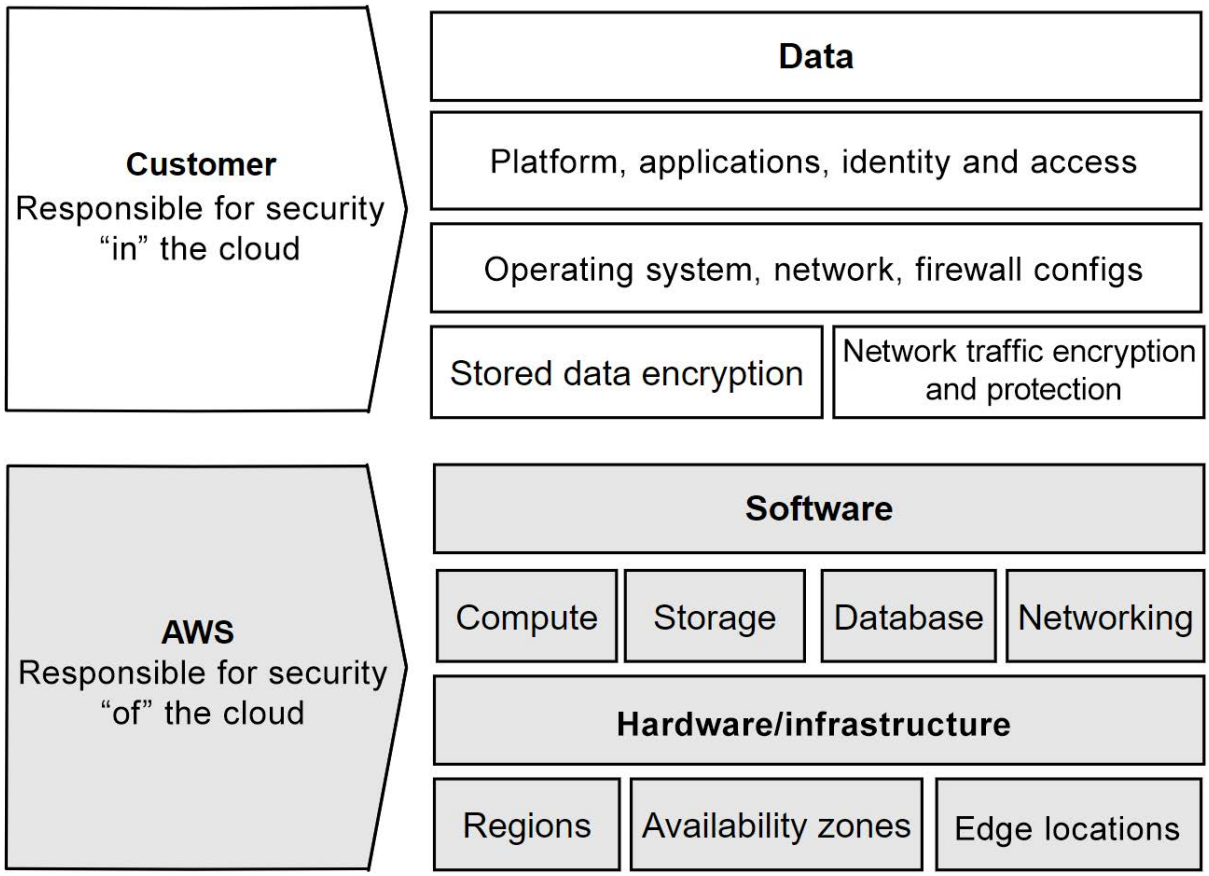
- ○ No restrictions
- ◉ Allow list
- ○ Block list

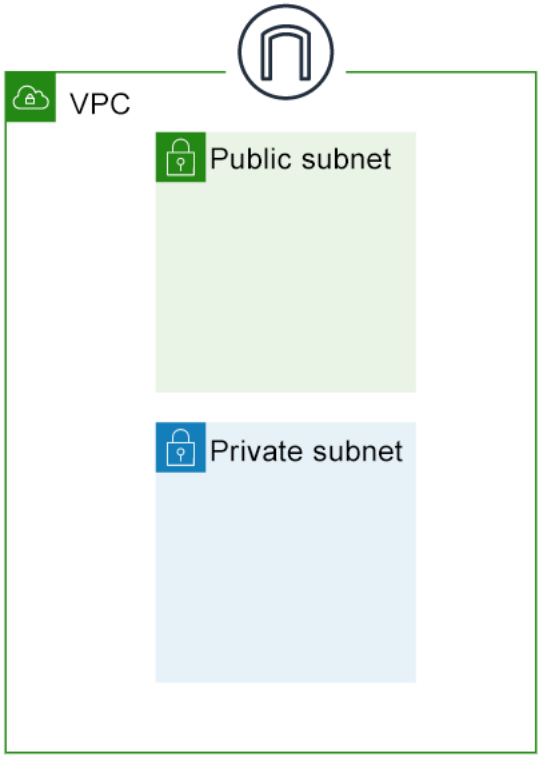
Countries

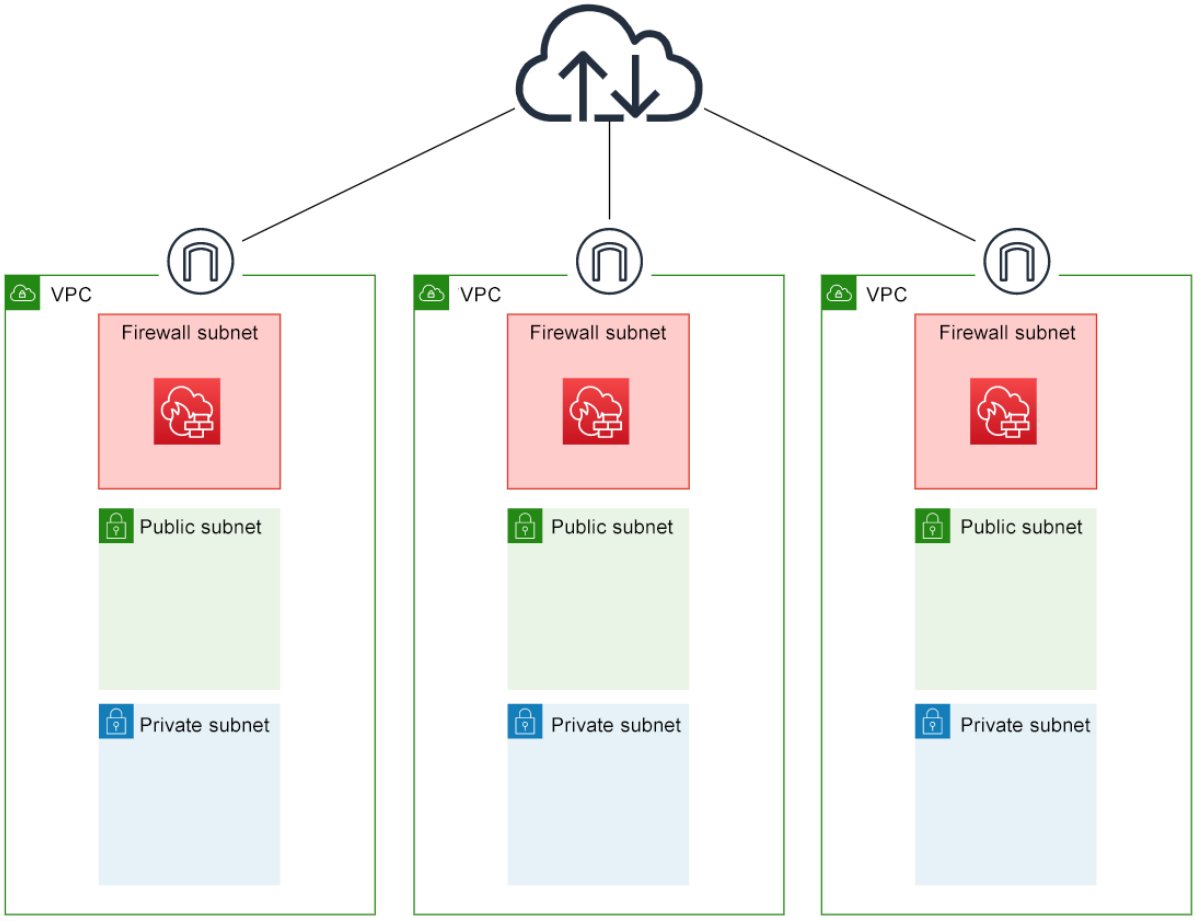
Select countries

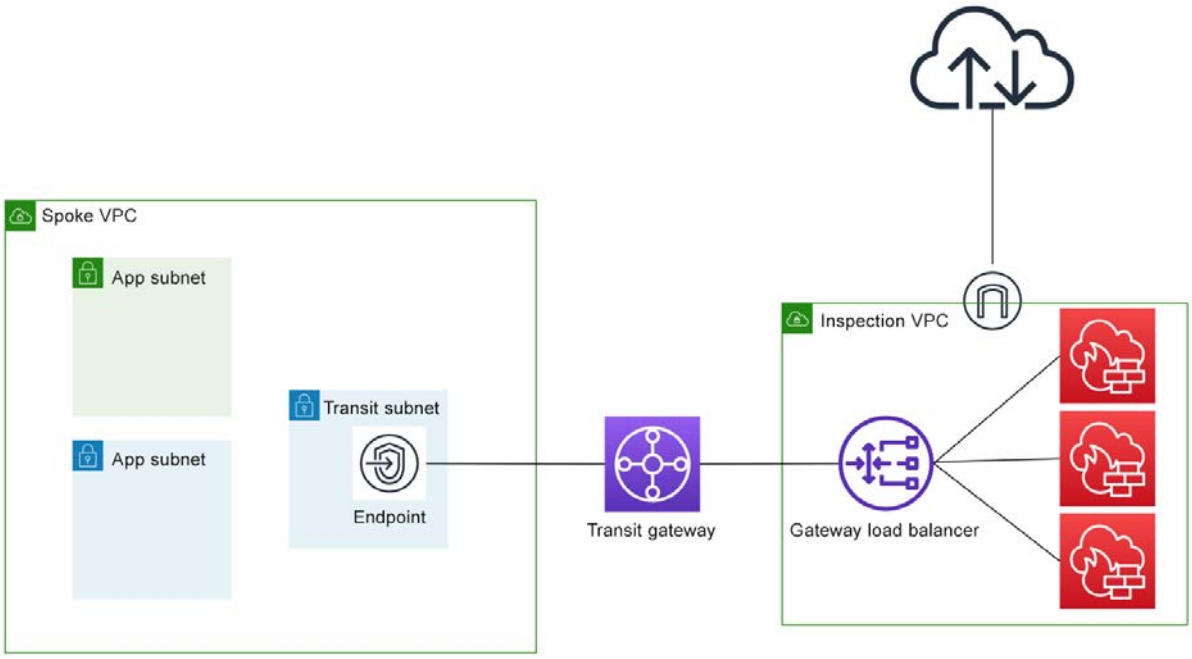
Australia ✕ | United Kingdom ✕ | United States ✕

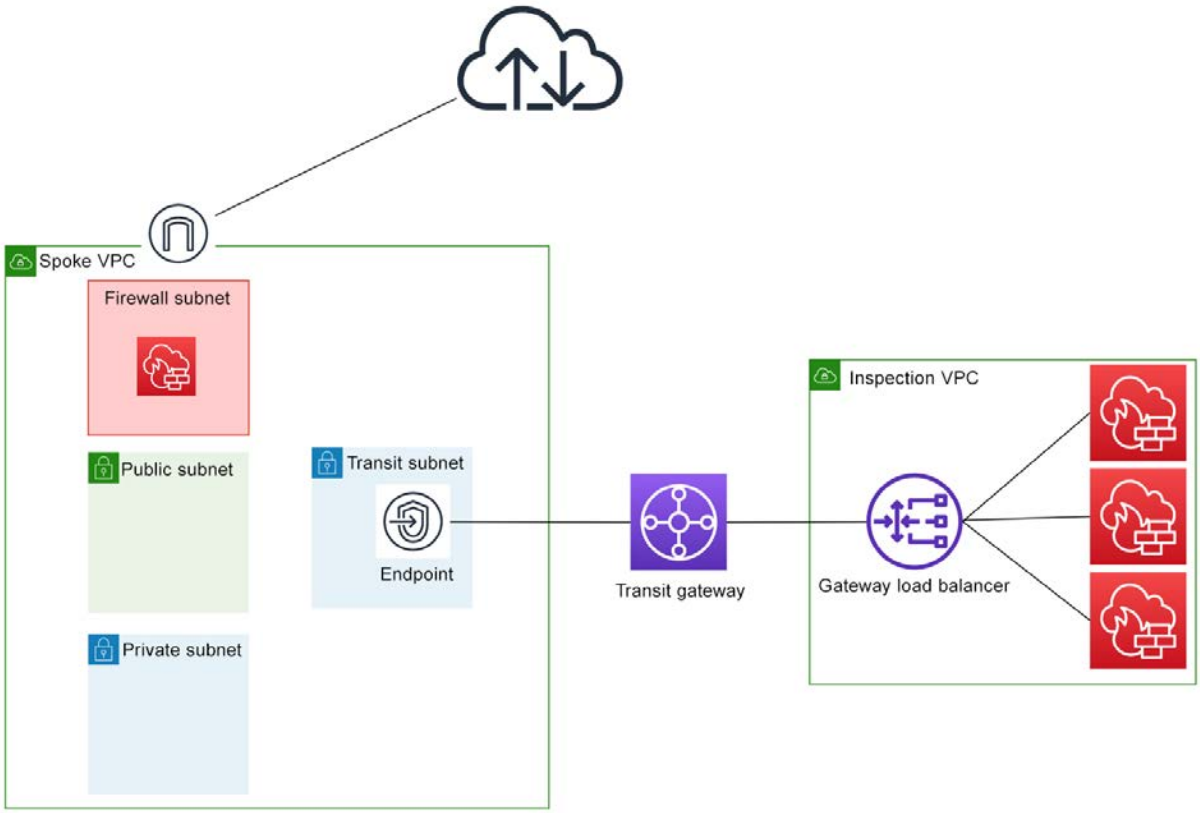



Customer
Responsible for security "in" the cloud
Data
Platform, applications, identity and access
Operating system, network, firewall configs
Stored data encryption
Network traffic encryption and protection
AWS
Responsible for security "of" the cloud
Software
Compute
Storage
Database
Networking
Hardware/infrastructure
Regions
Availability zones
Edge locations

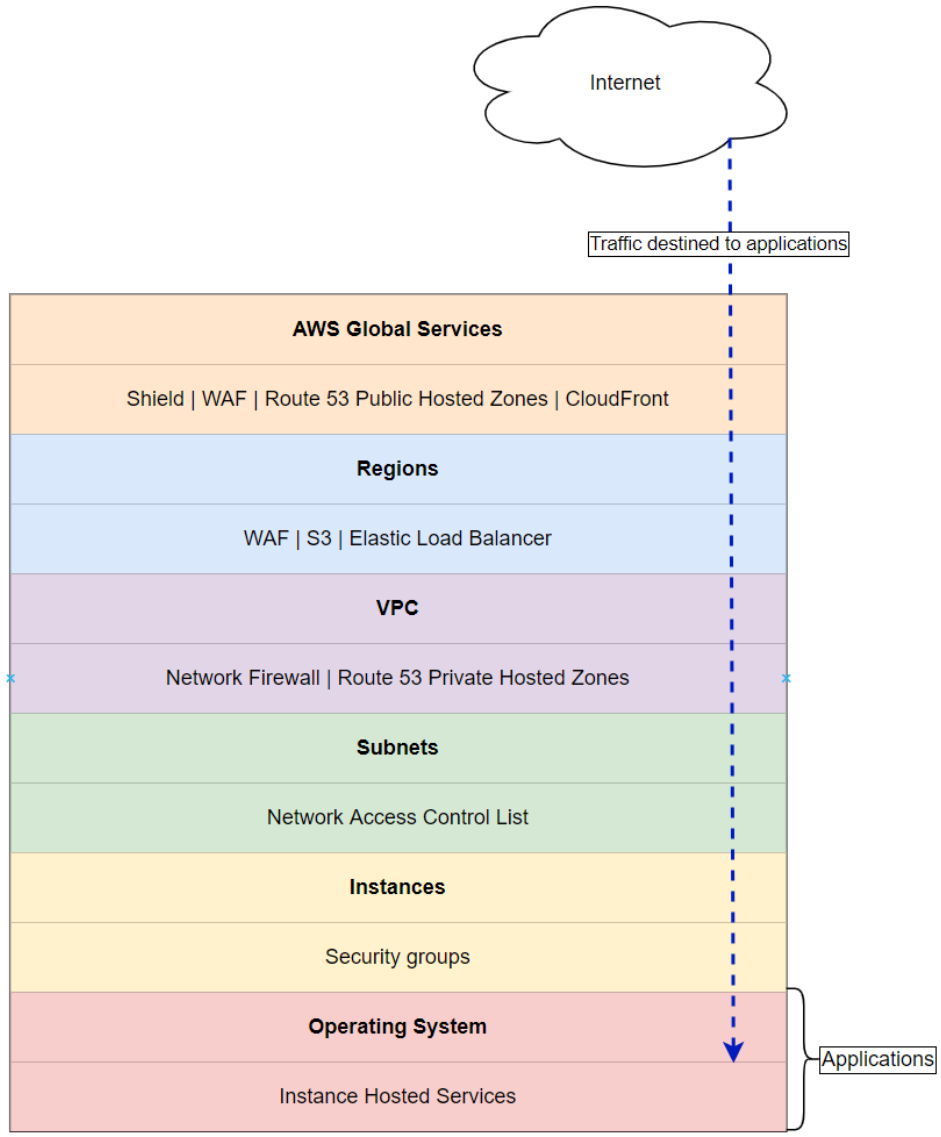

VPC
Public subnet
Private subnet

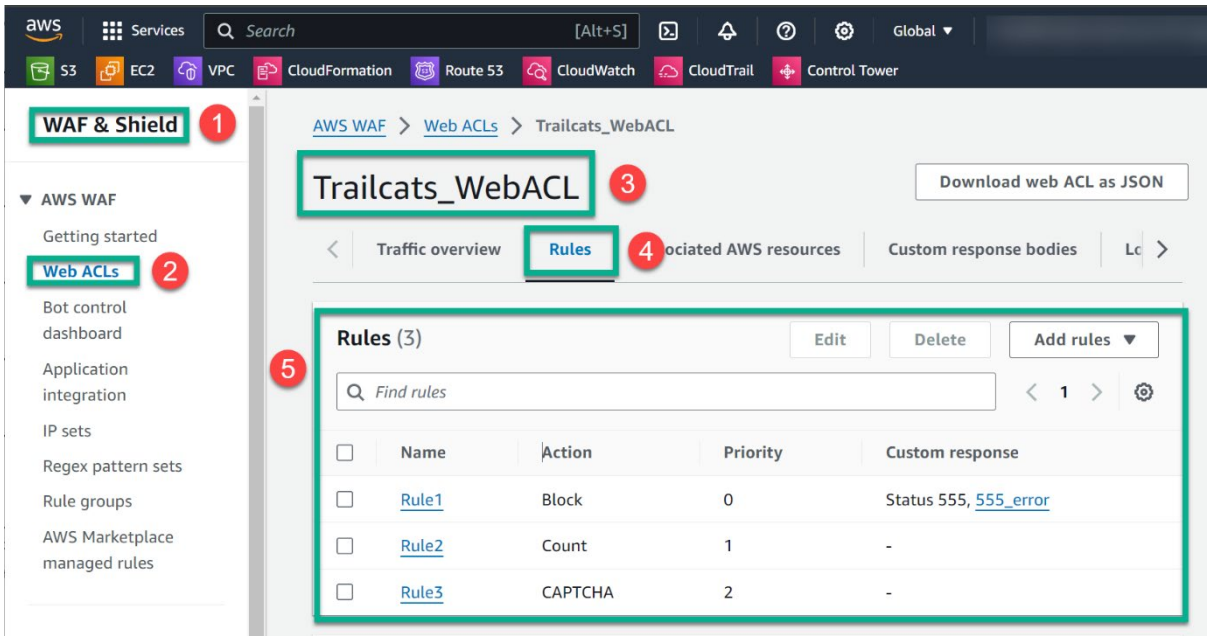

VPC
Firewall subnet
Public subnet
Private subnet
VPC
Firewall subnet
Public subnet
Private subnet
VPC
Firewall subnet
Public subnet
Private subnet

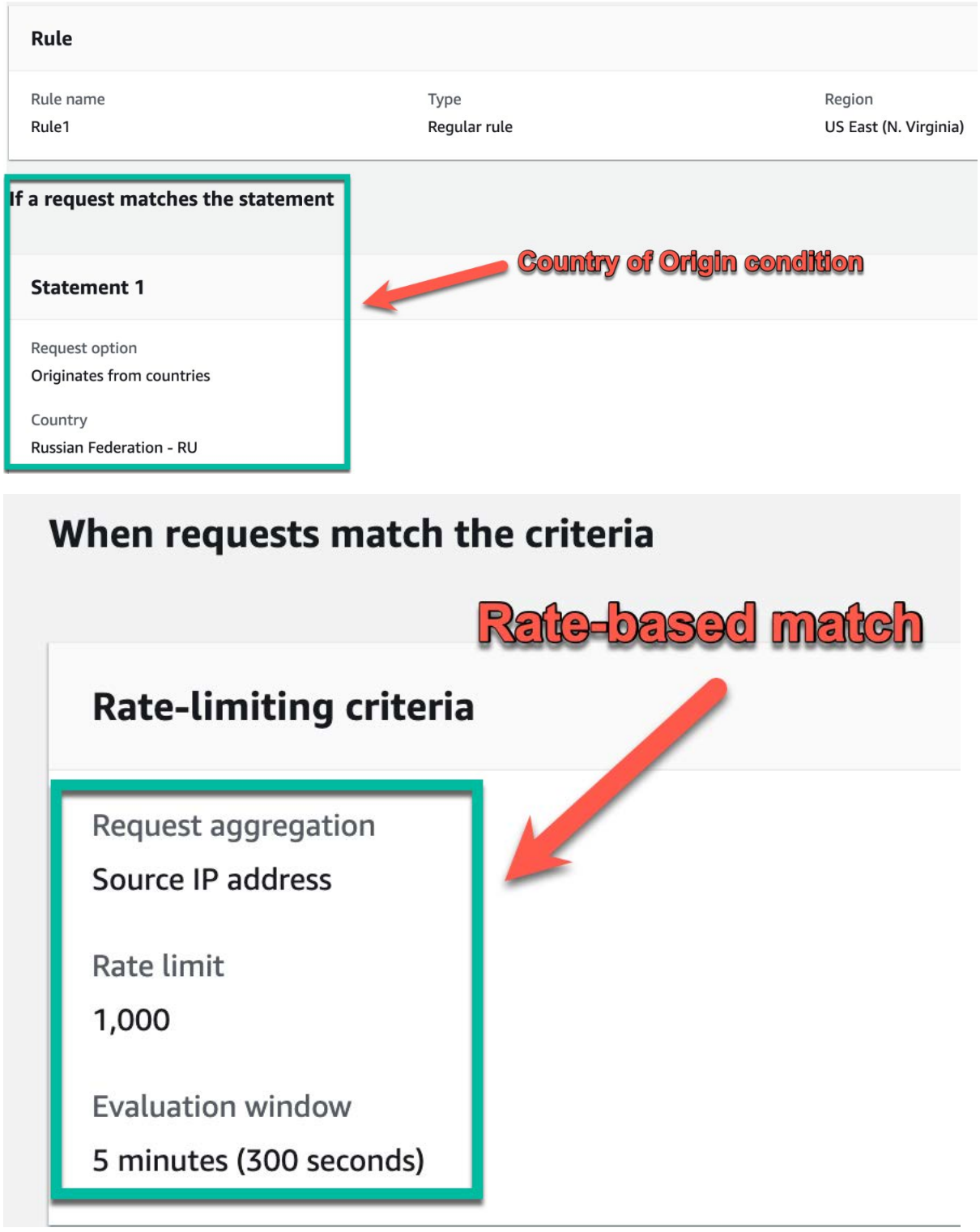

Spoke VPC
App subnet
App subnet
Transit subnet
Endpoint
Transit gateway
Inspection VPC
Gateway load balancer

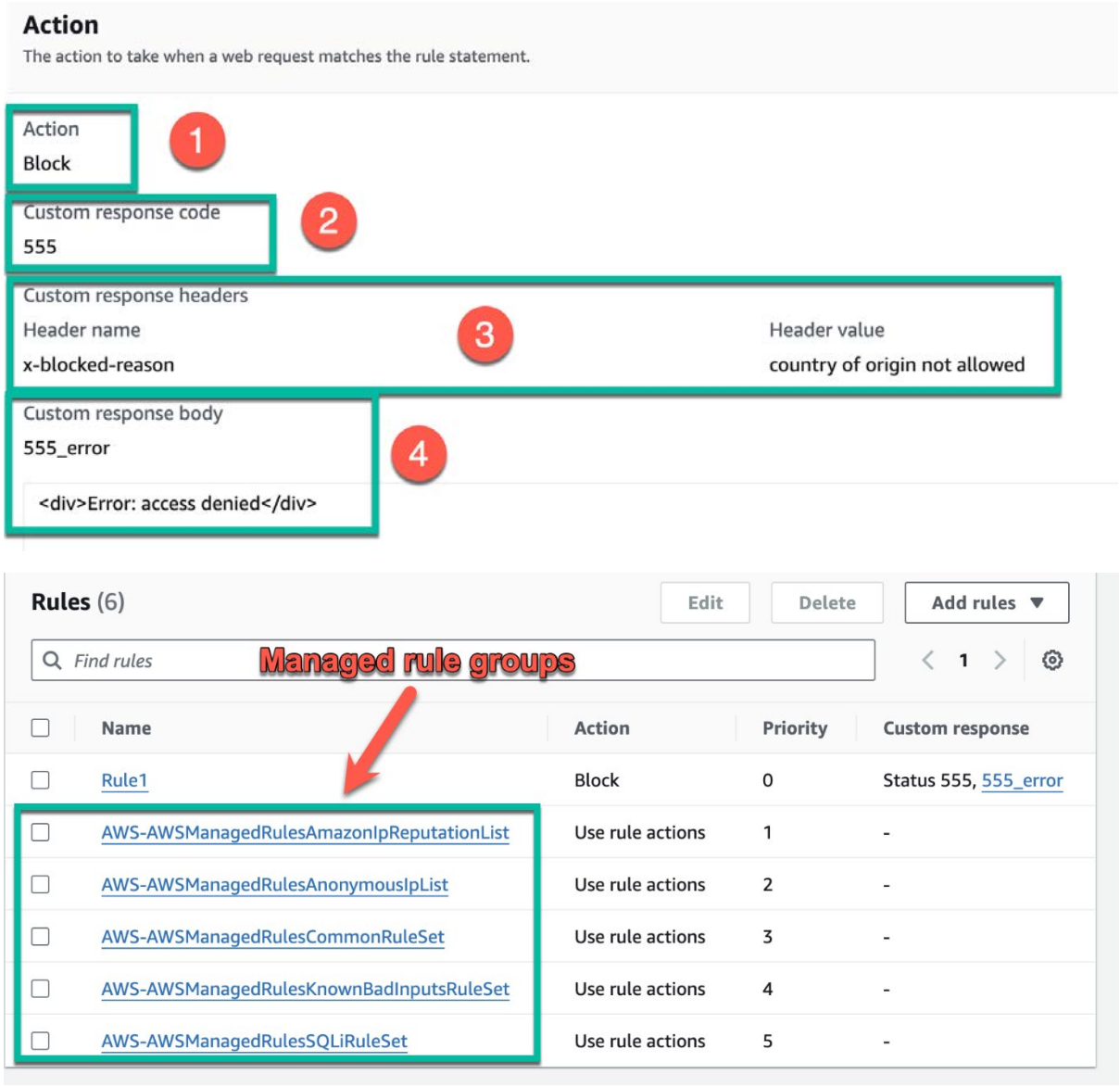

Spoke VPC
Firewall subnet
Public subnet
Transit subnet
Endpoint
Private subnet
Transit gateway
Inspection VPC
Gateway load balancer

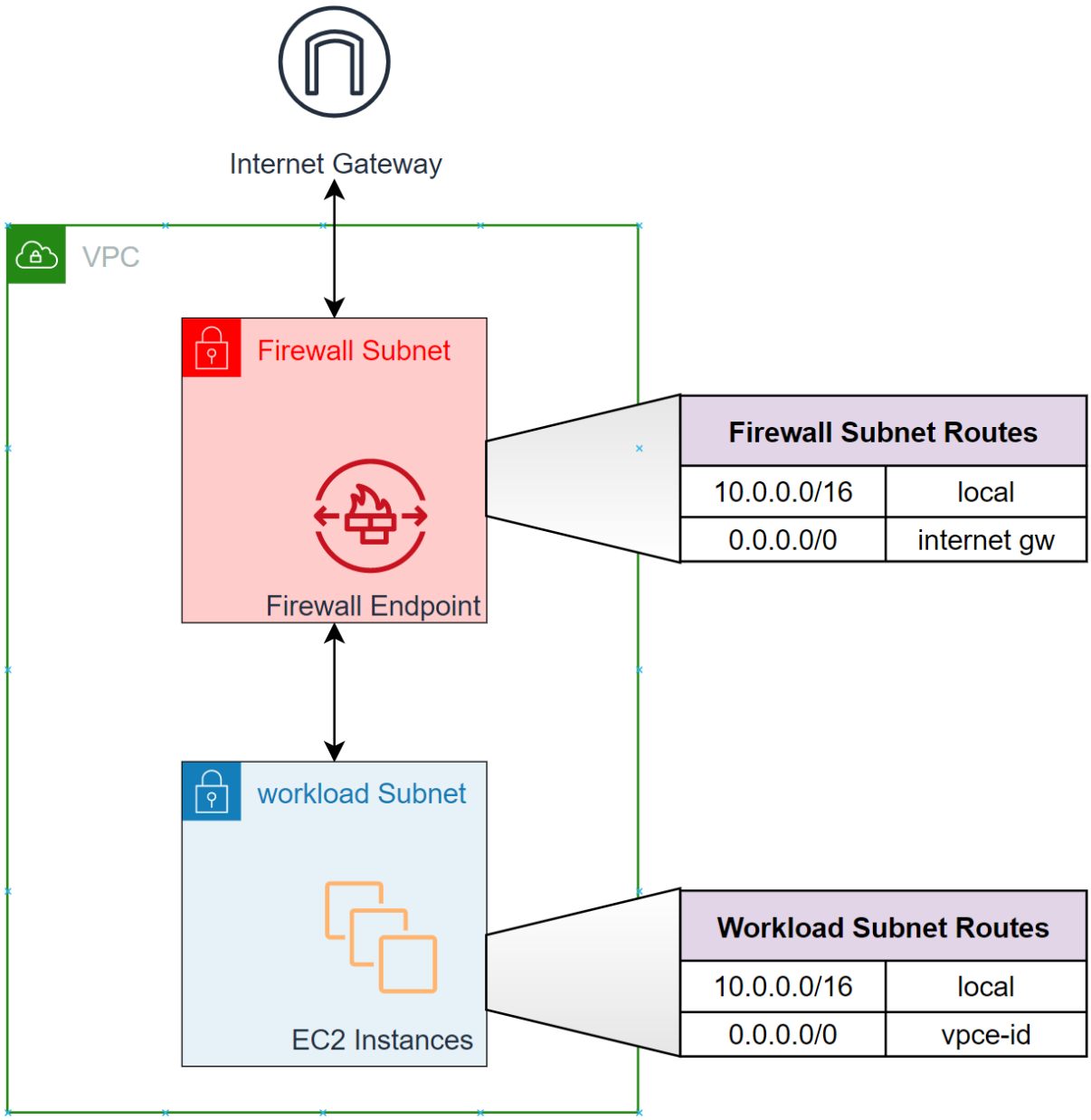
Chapter 12: AWS Security Services

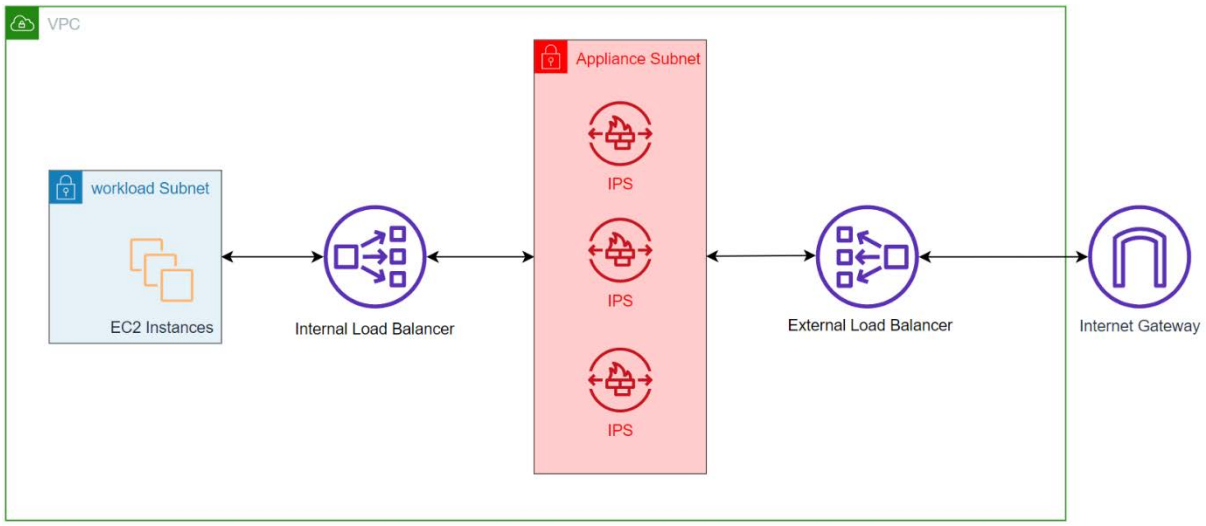




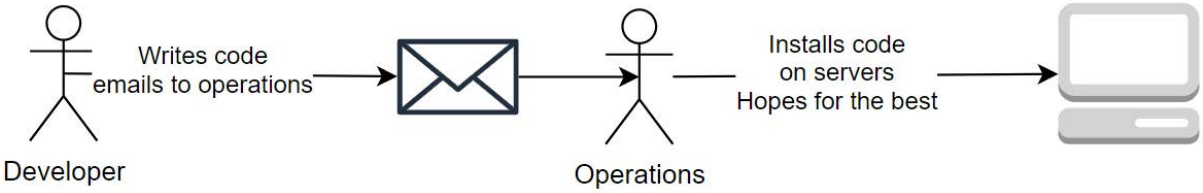

Rule
Rule name
Rule1
Type
Regular rule
Region
US East (N. Virginia)
If a request matches the statement
Statement 1
Country of Origin condition
Request option
Originates from countries
Country
Russian Federation - RU
When requests match the criteria
Rate-based match
Rate-limiting criteria
Request aggregation
Source IP address
Rate limit
1,000
Evaluation window
5 minutes (300 seconds)

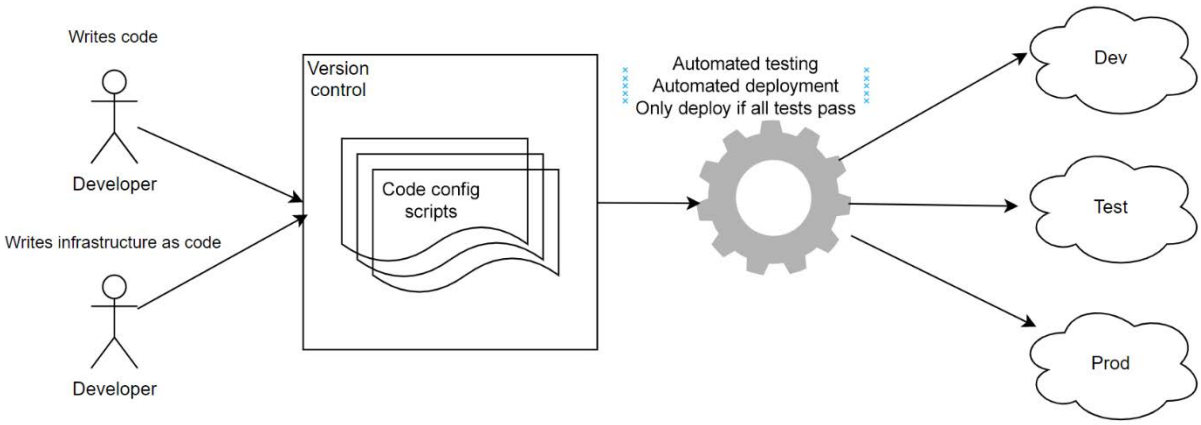

Action
The action to take when a web request matches the rule statement.
Action
Block
1
Custom response code
555
2
Custom response headers
Header name
x-blocked-reason
3
Header value
country of origin not allowed
Custom response body
555_error
4
Error: access denied
Rules (6)
Edit
Delete
Add rules
Find rules
Managed rule groups
1
Name
Action
Priority
Custom response
Rule1
Block
0
Status 555, 555_error
AWS-AWSManagedRulesAmazonIpReputationList
Use rule actions
1
-
AWS-AWSManagedRulesAnonymousIpList
Use rule actions
2
-
AWS-AWSManagedRulesCommonRuleSet
Use rule actions
3
-
AWS-AWSManagedRulesKnownBadInputsRuleSet
Use rule actions
4
-
AWS-AWSManagedRulesSQLiRuleSet
Use rule actions
5
-

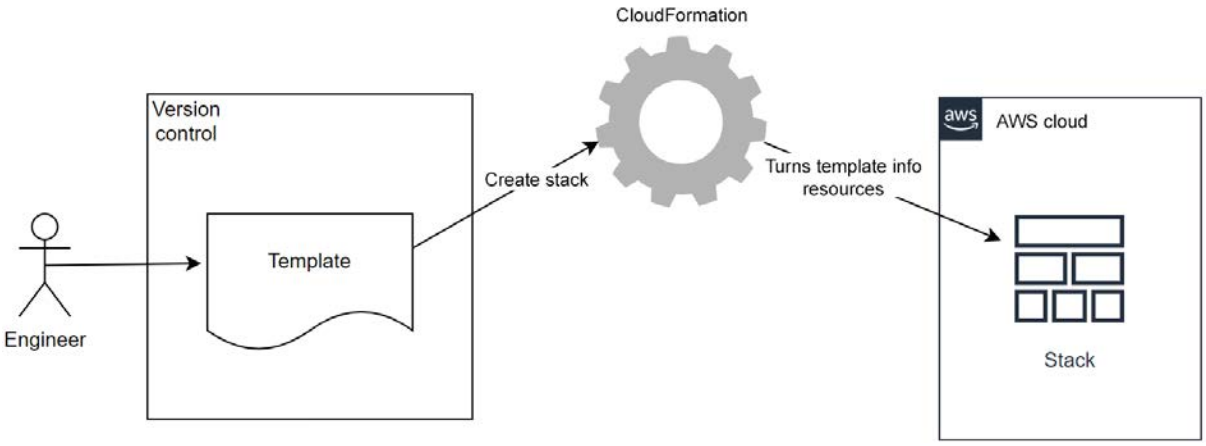

Internet Gateway
VPC
Firewall Subnet
Firewall Endpoint
Firewall Subnet Routes
10.0.0.0/16
local
0.0.0.0/0
internet gw
workload Subnet
EC2 Instances
Workload Subnet Routes
10.0.0.0/16
local
0.0.0.0/0
vpce-id


VPC
Appliance Subnet
IPS
IPS
IPS
workload Subnet
EC2 Instances
Internal Load Balancer
External Load Balancer
Internet Gateway

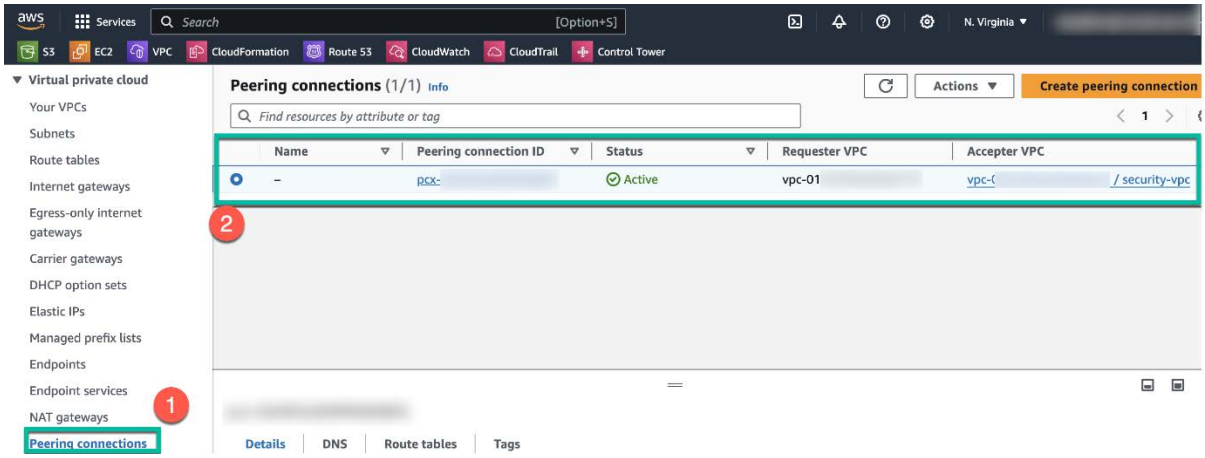
Chapter 13: Infrastructure as Code



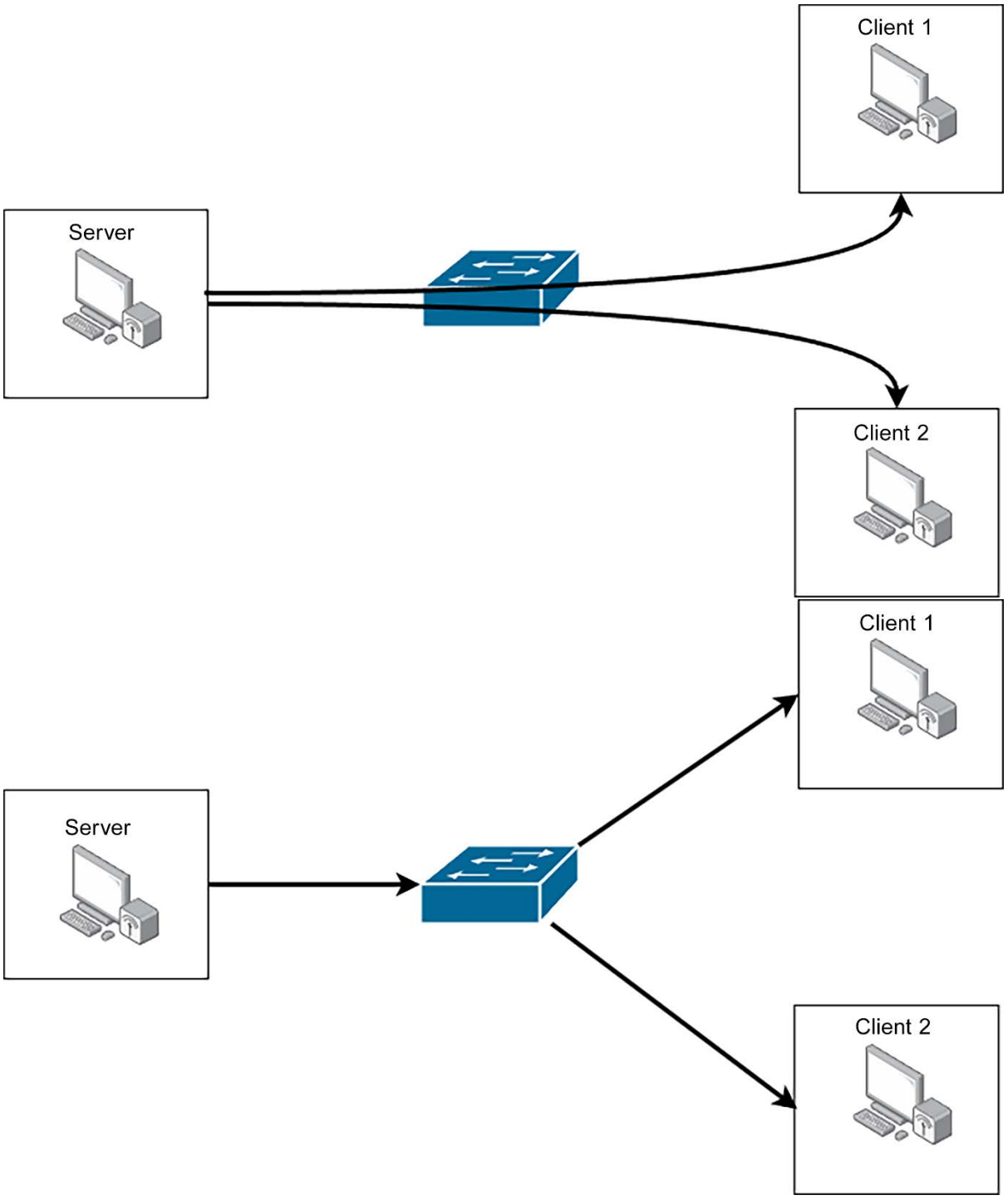


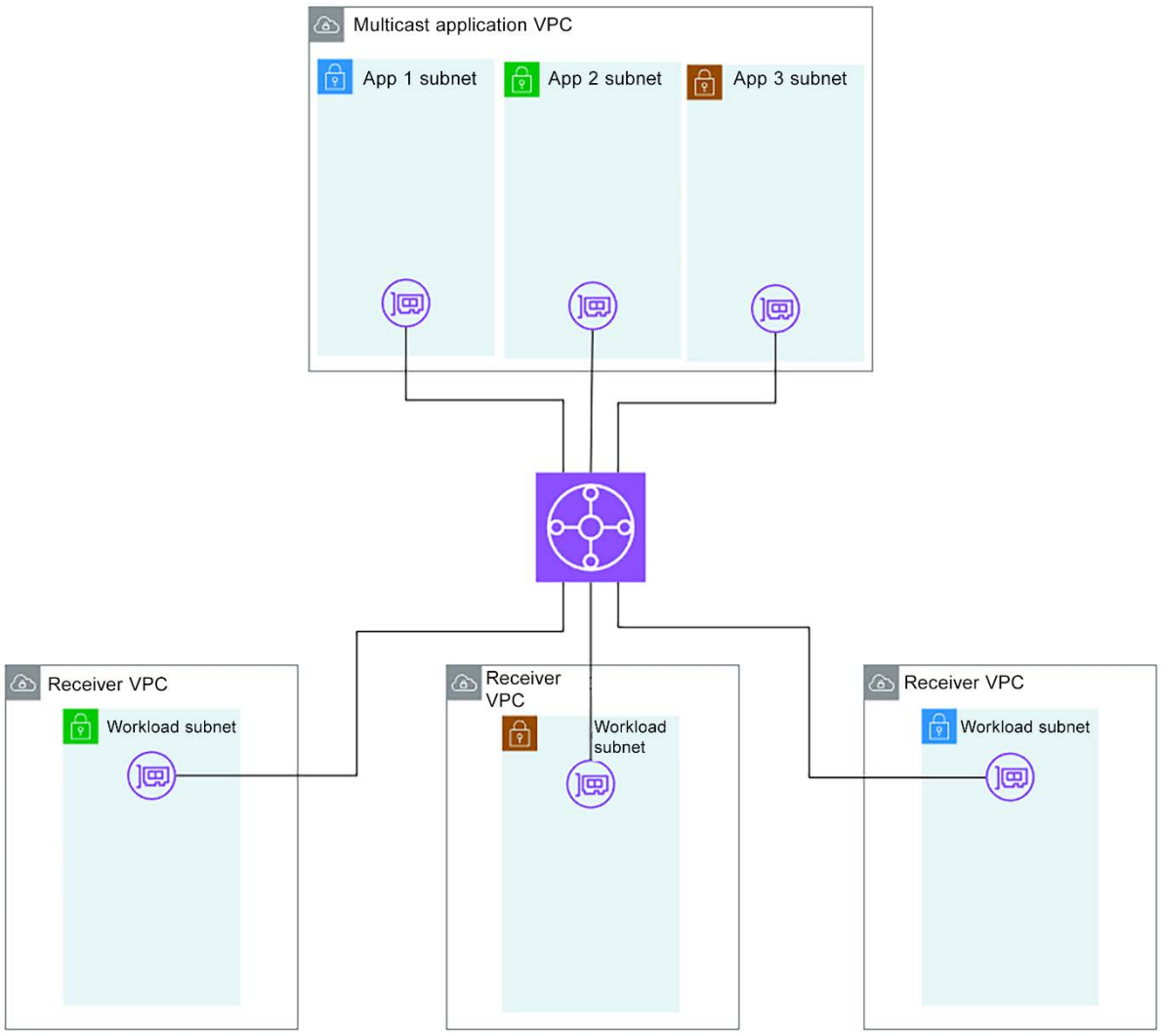



```
DescribeStacks
Stacks
CreationTime                | 2024-08-12T00:34:39.649000+00:00
DisableRollback             | False
EnableTerminationProtection | False
StackId                     | arn:aws:cloudformation:us-east-1:361037072889:stack/basicvpc/a8df5870-5842-11ef-bab4-0e73da89f1cd
StackName                   | basicvpc
StackStatus                 | CREATE_COMPLETE
DriftInformation
StackDriftStatus            | NOT_CHECKED
```


Services
Search
[Option+S]
N. Virginia
S3
EC2
VPC
CloudFormation
Route 53
CloudWatch
CloudTrail
Control Tower
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
1
Peering connections (1/1) Info
Actions
Create peering connection
Find resources by attribute or tag
1
Name
Peering connection ID
Status
Requester VPC
Accepter VPC
–
pcx-
Active
vpc-01
vpc-
/ security-vpc
2
Details
DNS
Route tables
Tags

Chapter 14: Data Analytics and Optimization





Global network settings

Name

A name to help you identify the global network.

My global network

Name must contain no more than 100 characters. Valid characters are a-z, A-Z, 0-9, and - (hyphen).

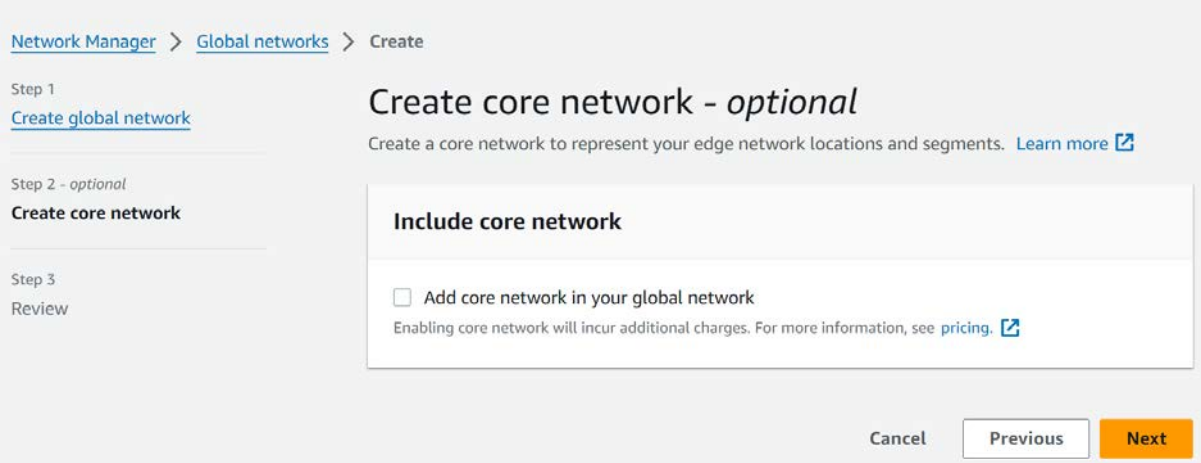
Description - *optional*

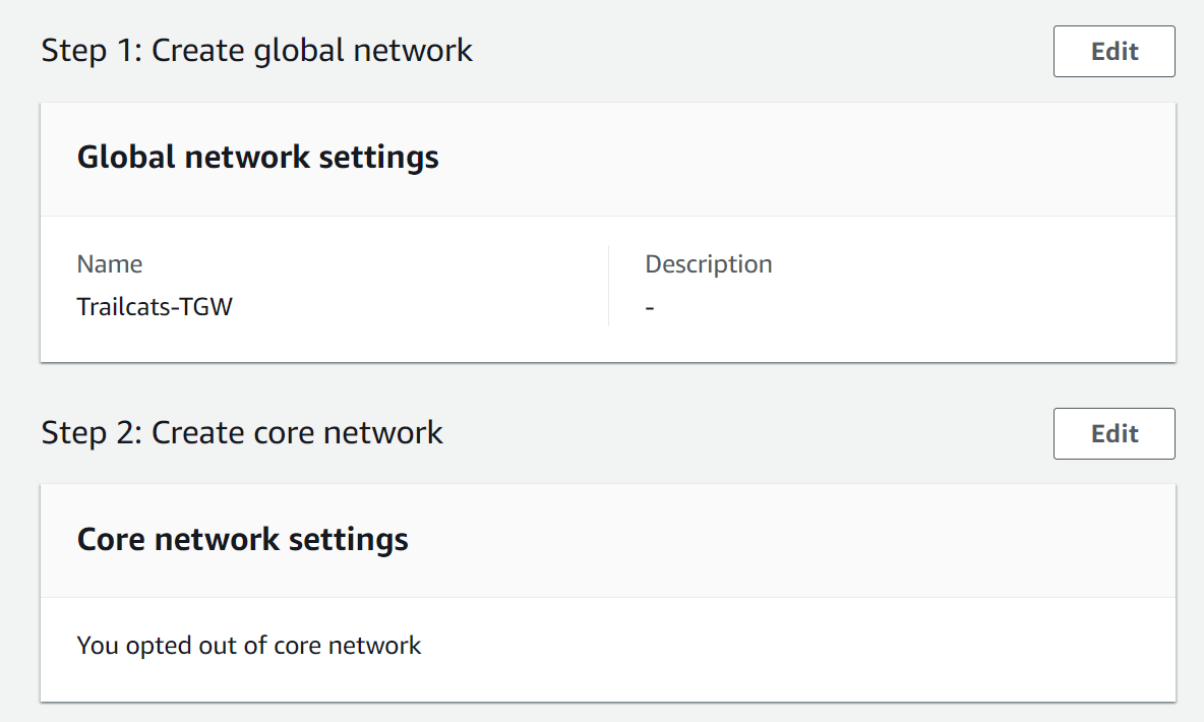
A description to help you identify the global network.

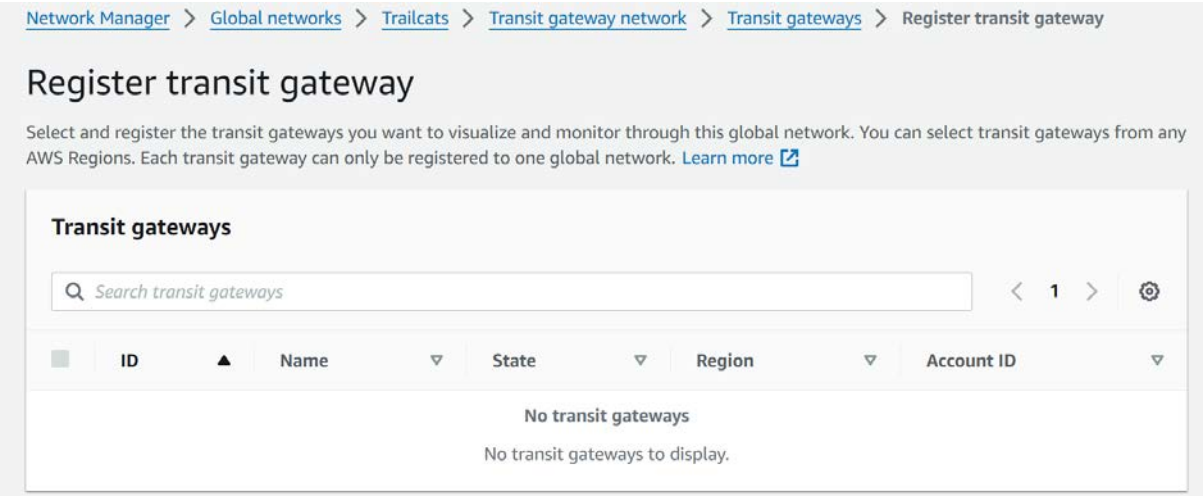
A global network for testing purposes.

Description must contain no more than 100 characters. Valid characters are a-z, A-Z, 0-9, and - (hyphen).

▶ **Additional settings**


Network Manager > Global networks > Create
Step 1
Create global network
Step 2 - optional
Create core network
Step 3
Review
Create core network - optional
Create a core network to represent your edge network locations and segments. Learn more
Include core network
Add core network in your global network
Enabling core network will incur additional charges. For more information, see pricing.
Cancel
Previous
Next


Step 1: Create global network
Edit
Global network settings
Name
Trailcats-TGW
Description
-
Step 2: Create core network
Edit
Core network settings
You opted out of core network


Network Manager > Global networks > Trailcats > Transit gateway network > Transit gateways > Register transit gateway
Register transit gateway
Select and register the transit gateways you want to visualize and monitor through this global network. You can select transit gateways from any AWS Regions. Each transit gateway can only be registered to one global network. Learn more
Transit gateways
Search transit gateways
1
ID
Name
State
Region
Account ID
No transit gateways
No transit gateways to display.

Test pattern

Select log data to test

Custom log data

Log event messages

Type log data to test with your Filter Pattern. Please use line breaks to separate log events.

[83078518-fcc1-4d30-9573-8b9737671438] BENCHMARK : Running Start Crawl for Crawler TestCrawler2
[83078518-fcc1-4d30-9573-8b9737671438] BENCHMARK : Classification complete, writing results to database mygluedatabase
[83078518-fcc1-4d30-9573-8b9737671438] INFO : Crawler configured with SchemaChangePolicy

Test pattern

Log streams | Tags | Anomaly detection | Metric filters

Metric filters (1/1)

Edit

Find metric filters

Ready

Filter pattern

"READY"

Metric

Webserver / Ready

Metric value

1

Conditions

Threshold type

- (●) Static
  Use a value as a threshold
- ( ) Anomaly detection
  Use a band as a threshold

Whenever Ready is...

Define the alarm condition.

- (●) Greater
  > threshold
- ( ) Greater/Equal
  >= threshold
- ( ) Lower/Equal
  <= threshold
- ( ) Lower
  < threshold

Notification

Alarm state trigger

Define the alarm state that will trigger this action.

Remove

- (●) In alarm
  The metric or expression is outside of the defined threshold.
- ( ) OK
  The metric or expression is within the defined threshold.
- ( ) Insufficient data
  The alarm has just started or not enough data is available.

Send a notification to the following SNS topic

Define the SNS (Simple Notification Service) topic that will receive the notification.

- (●) Select an existing SNS topic
- ( ) Create new topic
- ( ) Use topic ARN to notify other accounts

Edit bucket policy Info

Bucket policy

Policy examples | Policy generator

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more

Bucket ARN

arn:aws:s3:::testbucketawsansexamguide2023

Policy

Chapter 16: Accessing the Online Practice Resources

Practice Resources

REPORT ISSUE

UNLOCK YOUR PRACTICE RESOURCES

You're about to unlock the free online content that came with your book. Make sure you have your book with you before you start, so that you can access the resources in minutes.

AWS Certified Advanced Networking – Specialty (ANS-C01) Certification Guide

Book ISBN: 9781835080832

Tim McConnaughy • Steve McNutt • Christopher Miles • Dec 2024 • 515 pages

Do you have a Packt account?

○ Yes, I have an existing Packt account ○ No, I don't have a Packt account

PROCEED

Practice Resources

REPORT ISSUE

UNLOCK YOUR PRACTICE RESOURCES

You're about to unlock the free online content that came with your book. Make sure you have your book with you before you start, so that you can access the resources in minutes.

AWS Certified Advanced Networking – Specialty (ANS-C01) Certification Guide

Book ISBN: 9781835080832

Tim McConnaughy • Steve McNutt • Christopher Miles • Dec 2024 • 515 pages

ENTER YOUR PURCHASE DETAILS

Enter Unique Code *

CPP4153

Where To Find This?

☑ Check this box to receive emails from us about new features and promotions on our other certification books. You can opt out anytime.

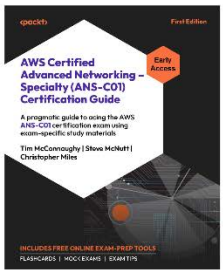
REQUEST ACCESS

Practice Resources

REPORT ISSUE

PACKT PRACTICE RESOURCES

You've just unlocked the free online content that came with your book.



AWS Certified Advanced Networking – Specialty (ANS-C01) Certification Guide

Book ISBN: 9781835080832

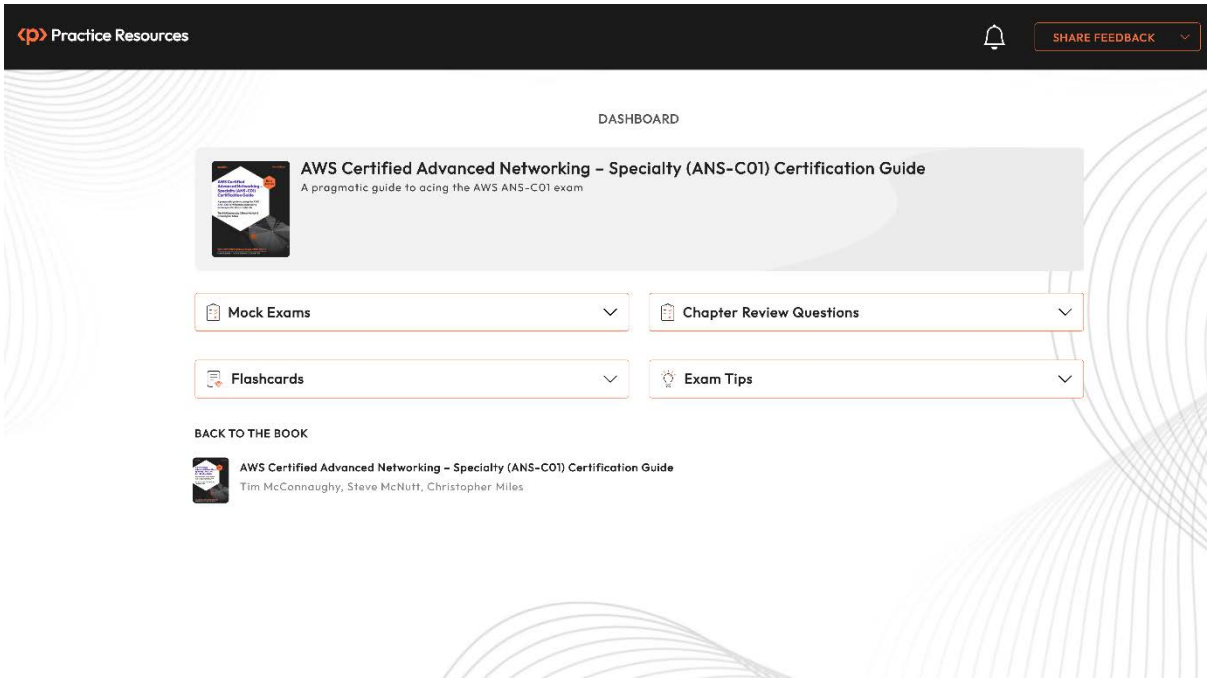
Tim McConnaughy • Steve McNutt • Christopher Miles • Dec 2024 • 515 pages

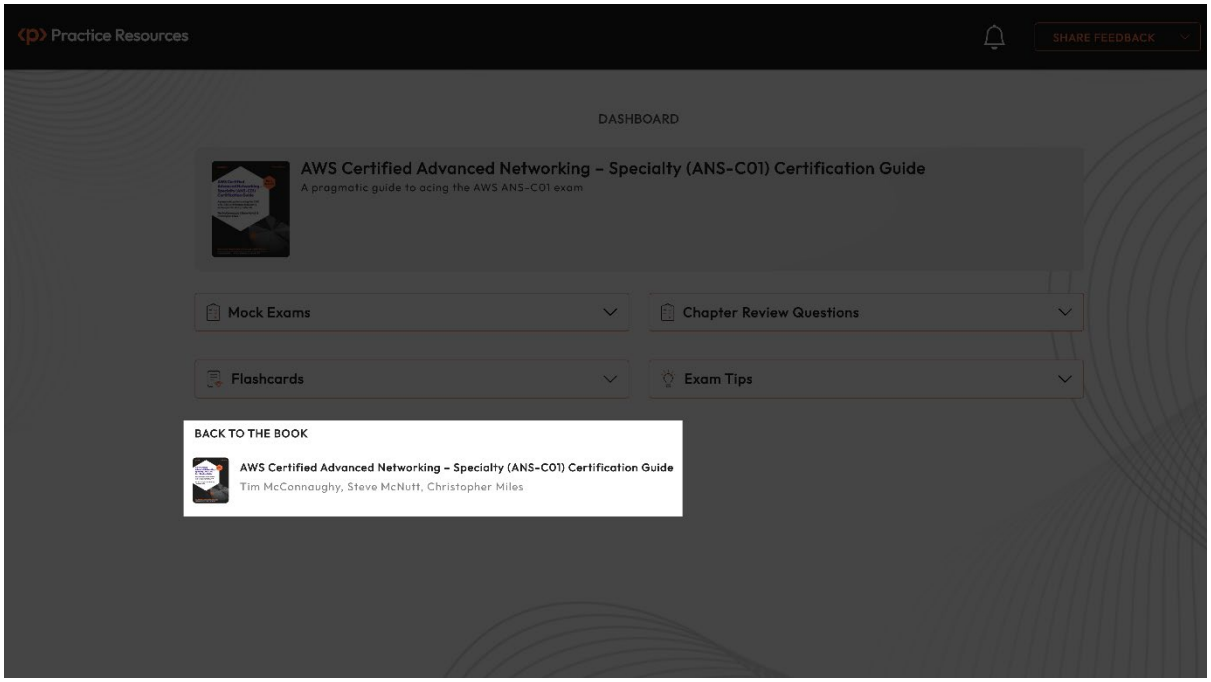
Unlock Successful

Click the following link to access your practice resources at any time.

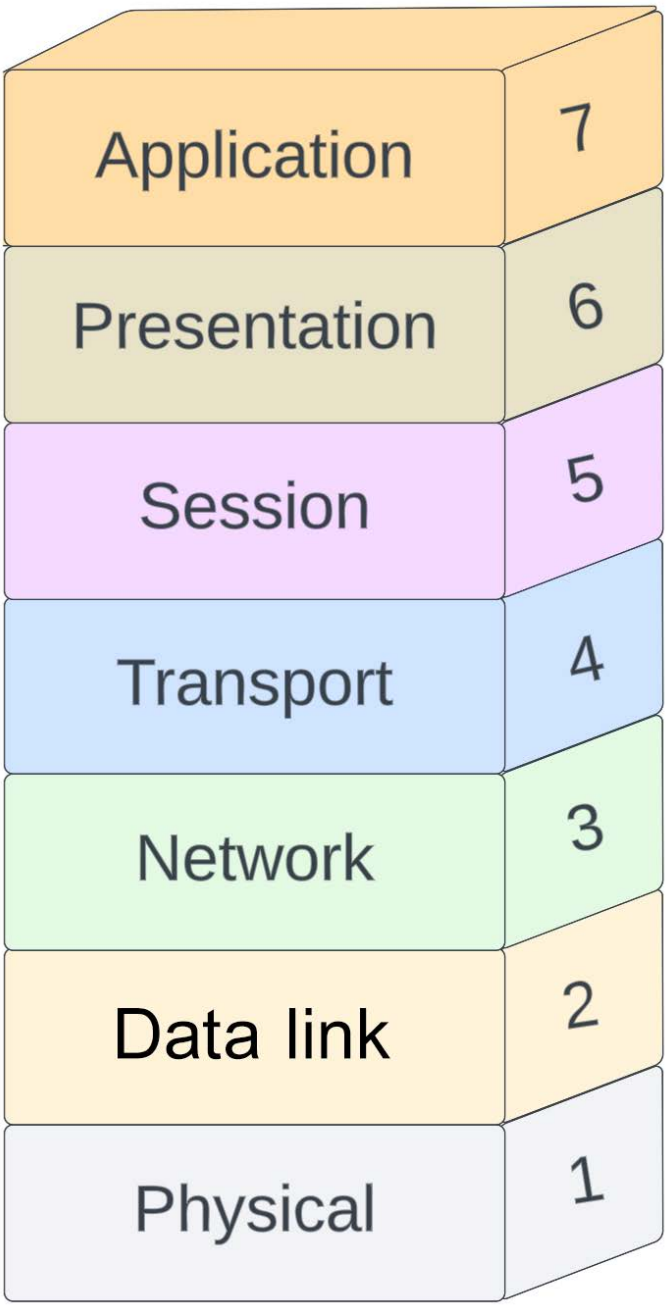
Pro Tip: You can switch seamlessly between the ebook version of the book and the practice resources. You'll find the ebook version of this title in your Owned Content

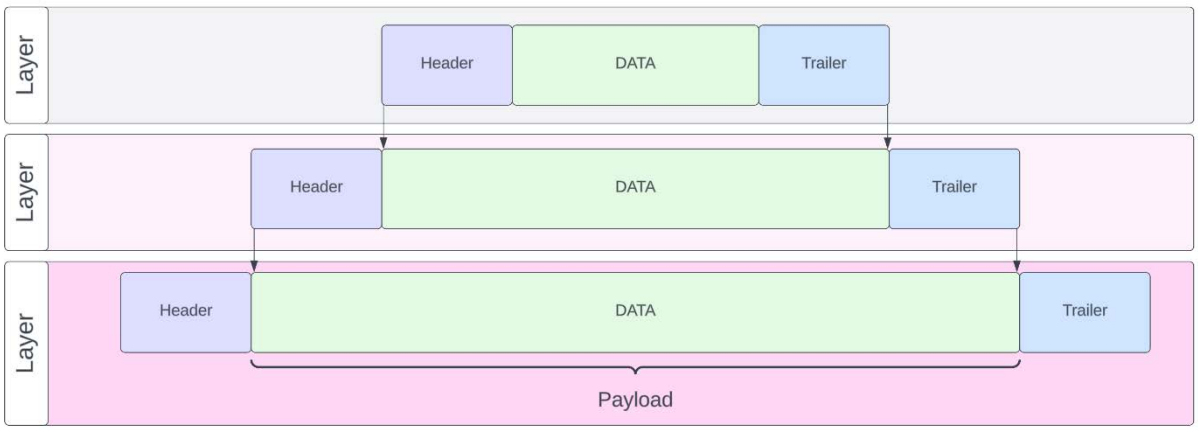
OPEN PRACTICE RESOURCES

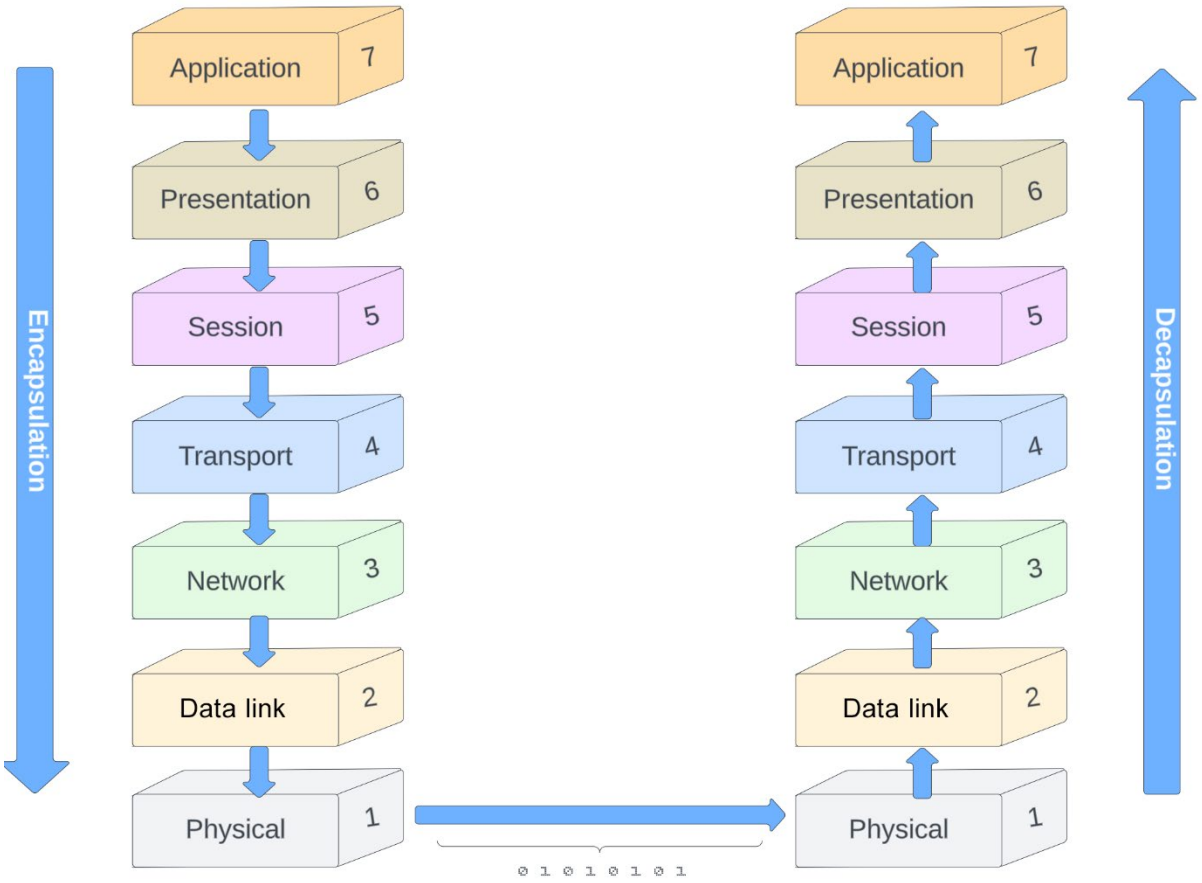


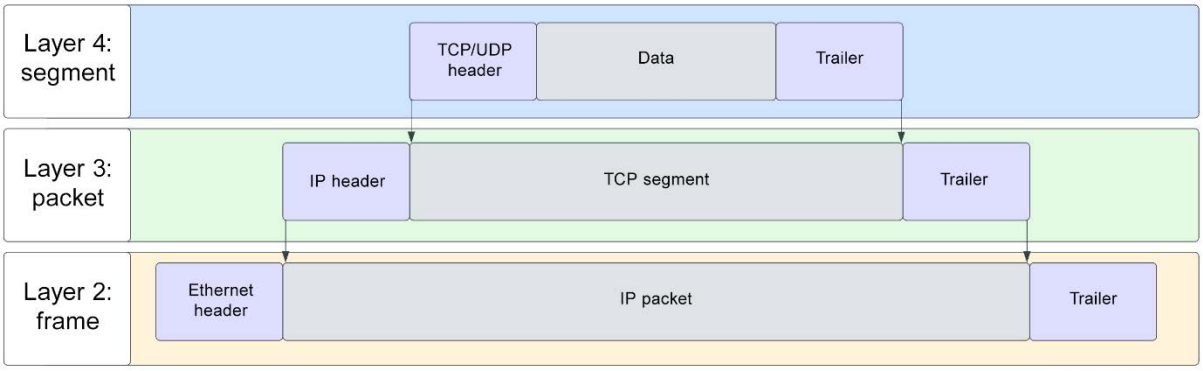

Practice Resources
SHARE FEEDBACK
DASHBOARD
AWS Certified Advanced Networking – Specialty (ANS-C01) Certification Guide
A pragmatic guide to acing the AWS ANS-C01 exam
Mock Exams
Chapter Review Questions
Flashcards
Exam Tips
BACK TO THE BOOK
AWS Certified Advanced Networking – Specialty (ANS-C01) Certification Guide
Tim McConnaughy, Steve McNutt, Christopher Miles

Appendix 1: Network Fundamentals






Encapsulation
Application
7
Presentation
6
Session
5
Transport
4
Network
3
Data link
2
Physical
1
0 1 0 1 0 1 0 1
Application
7
Presentation
6
Session
5
Transport
4
Network
3
Data link
2
Physical
1
Decapsulation


Layer 4: segment
TCP/UDP header
Data
Trailer
Layer 3: packet
IP header
TCP segment
Trailer
Layer 2: frame
Ethernet header
IP packet
Trailer

0.0.0.0

00000000 . 00000000 . 00000000 . 00000000

8 Bits 8 Bits 8 Bits 8 Bits

255.255.255.255

11111111 . 11111111 . 11111111 . 11111111

8 Bits 8 Bits 8 Bits 8 Bits

Bit position	7	6	5	4	3	2	1	0
Value	128	64	32	16	8	4	2	1

00000001

Bit position	7	6	5	4	3	2	1	0	
Bit value	0	0	0	0	0	0	0	1	= 1
Value	128	64	32	16	8	4	2	1	

00000010

Bit position	7	6	5	4	3	2	1	0	
Bit value	0	0	0	0	0	0	1	0	= 2
Value	128	64	32	16	8	4	2	1	

00000011

Bit position	7	6	5	4	3	2	1	0
Bit value	0	0	0	0	0	0	1	1
Value	128	64	32	16	8	4	2	1

= 3

Add
2 + 1

00010011

Bit position	7	6	5	4	3	2	1	0
Bit value	0	0	0	1	0	0	1	1
Value	128	64	32	16	8	4	2	1

= 19

Add
16 +

Add
2 + 1

11111111

Bit position	7	6	5	4	3	2	1	0
Bit Value	1	1	1	1	1	1	1	1
Value	128	64	32	16	8	4	2	1

= 255

Add Add Add Add Add Add Add
128 + 64 + 32 + 16 + 8 + 4 + 2 + 1

Network	
Net Range	8.8.8.0 - 8.8.8.255
CIDR	8.8.8.0/24
Name	LVLT-GOGL-8-8-8
Handle	NET-8-8-8-0-1
Parent	LVLT-ORG-8-8 (NET-8-0-0-0-1)
Net Type	Reallocated
Origin AS	
Organization	Google LLC (GOGL)
Registration Date	2014-03-14
Last Updated	2014-03-14
Comments	
RESTful Link	https://whois.arin.net/rest/net/NET-8-8-8-0-1
See Also	Related organization's POC records.
See Also	Related delegations.

Point of Contact	
Name	Google LLC
Handle	ZG39-ARIN
Company	Google LLC
Street	1600 Amphitheatre Parkway
City	Mountain View
State/Province	CA
Postal Code	94043
Country	US
Registration Date	2000-11-30
Last Updated	2022-11-10
Comments	
Phone	+1-650-253-0000 (Office)
Email	arin-contact@google.com
RESTful Link	https://whois.arin.net/rest/poc/ZG39-ARIN

Organization	
Name	Google LLC
Handle	GOGL
Street	1600 Amphitheatre Parkway
City	Mountain View
State/Province	CA
Postal Code	94043
Country	US
Registration Date	2000-03-30
Last Updated	2019-10-31
Comments	Please note that the recommended way to file abuse complaints are located in the following links. To report abuse and illegal activity: https://www.google.com/contact/ For legal requests: http://support.google.com/legal Regards, The Google Team
RESTful Link	https://whois.arin.net/rest/org/GOGL

Function	Point of Contact
Admin	ZG39-ARIN (ZG39-ARIN)
Tech	ZG39-ARIN (ZG39-ARIN)
Abuse	ABUSE5250-ARIN (ABUSE5250-ARIN)

Point of Contact	
Name	Abuse
Handle	ABUSE5250-ARIN
Company	Google Inc.
Street	1600 Amphitheatre Parkway
City	Mountain View
State/Province	CA
Postal Code	94043
Country	US
Registration Date	2015-11-06
Last Updated	2022-10-24
Comments	Please note that the recommended way to file abuse complaints are located in the following links. To report abuse and illegal activity: https://www.google.com/contact/ For legal requests: http://support.google.com/legal Regards, The Google Team
Phone	+1-650-253-0000 (Office)
Email	network-abuse@google.com
RESTful Link	https://whois.arin.net/rest/poc/ABUSE5250-ARIN

High order bits

Bit position	7	6	5	4	3	2	1	0
Value	128	64	32	16	8	4	2	1

Class A

00000000 . 00000000 . 00000000 . 00000000

Network | Host

Class B

00000000 . 00000000 . 00000000 . 00000000

Network | Host

Class C

00000000 . 00000000 . 00000000 . 00000000

Network | Host

Class A

00000000 . 00000000 . 00000000 . 00000000 =

Network | Host

Subnet masks

11111111 . 00000000 . 00000000 . 00000000

255.0.0.0

Class B

00000000 . 00000000 . 00000000 . 00000000 =

Network | Host

11111111 . 11111111 . 00000000 . 00000000

255.255.0.0

Class C

00000000 . 00000000 . 00000000 . 00000000 =

Network | Host

11111111 . 11111111 . 11111111 . 00000000

255.255.255.0

Subnet masks

11111111 . 00000000 . 00000000 . 00000000 =

255.0.0.0

CIDR notation

11111111 . 00000000 . 00000000 . 00000000

/8

11111111 . 11111111 . 00000000 . 00000000 =

255.255.0.0

11111111 . 11111111 . 00000000 . 00000000

/16

11111111 . 11111111 . 11111111 . 00000000 =

255.255.255.0

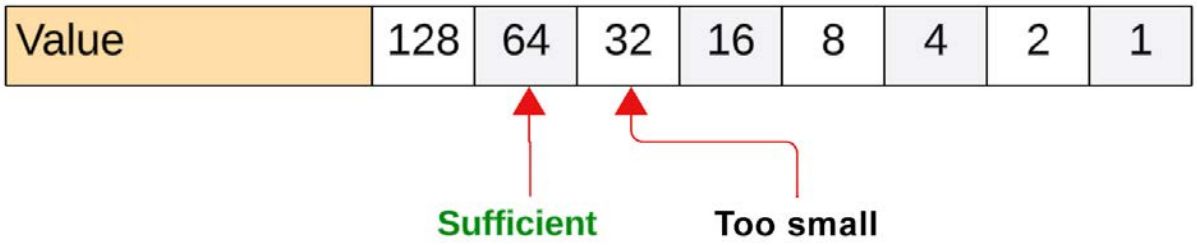
11111111 . 11111111 . 11111111 . 00000000

/24

Subnet masks (VLSM)		Slash notation
11111111 . 11110000 . 00000000 . 00000000 255.240.0.0	=	/12
11111111 . 11111111 . 11111110 . 00000000 255.255.254.0	=	/23
11111111 . 11111111 . 11111111 . 11111000 255.255.255.248	=	/29

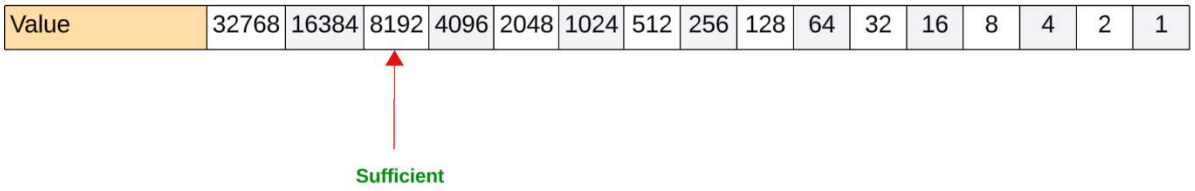
IP subnet: 192.168.0.0/24	Reserved addresses
11000000 . 10101000 . 00000000 . 00000000 Network Host	**192.168.0.0** (Network address)
11000000 . 10101000 . 00000000 . 11111111 Network Host	**192.168.0.255** (Network address)

IP subnet: 10.18.240.64/28	Reserved addresses
00001010 . 00010010 . 11110000 . 01000000 Network Host	**10.18.240.64** (Network address)
00001010 . 00010010 . 11110000 . 01001111 Network Host	**10.18.240.79** (Network address)



Bit position	7	6	5	4	3	2	1	0
Reservation	N	N	H	H	H	H	H	H
Value	128	64	32	16	8	4	2	1

= /26
(32 - 6)



Bit position	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Reservation	N	N	N	H	H	H	H	H	H	H	H	H	H	H	H	H
Value	32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

= /19
(32 - 13)

0000:0000:0000:0000:0000:0000:0000:0000

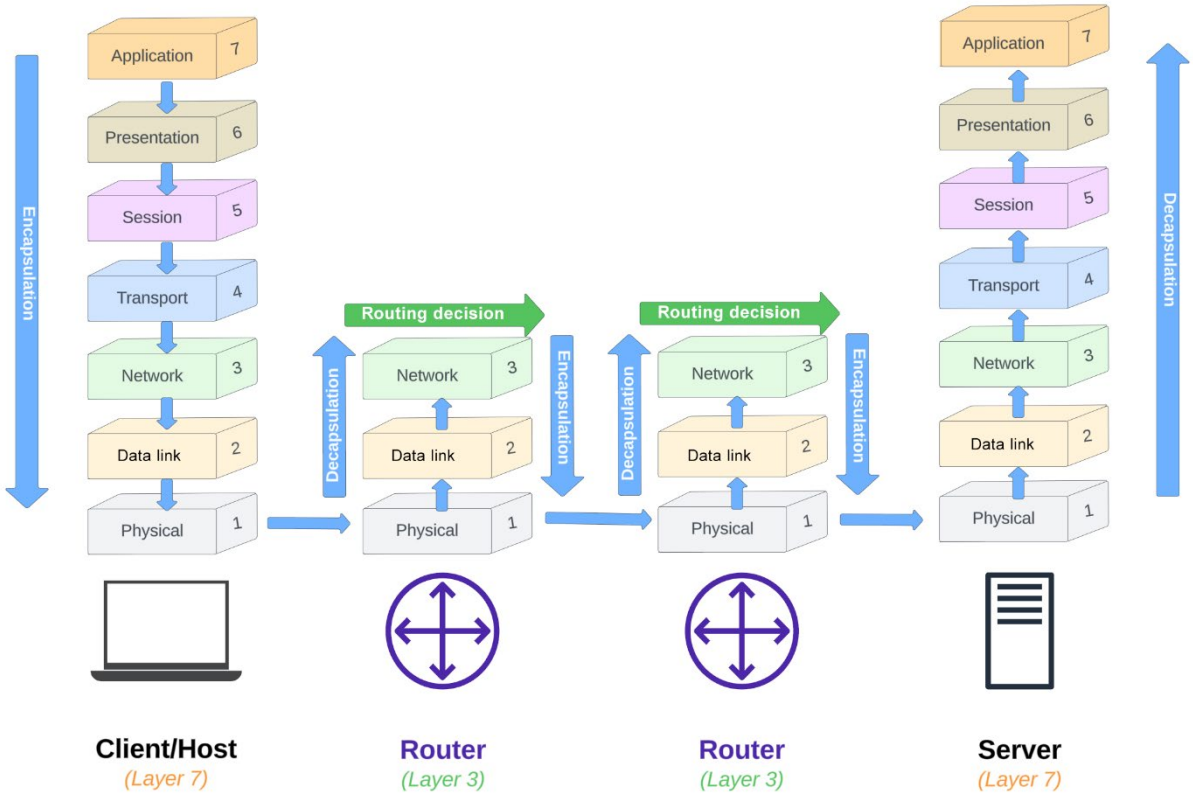
0000000000000000 : 0000000000000000 : 0000000000000000 : 0000000000000000 :
16 Bits 16 Bits 16 Bits 16 Bits
0000000000000000 : 0000000000000000 : 0000000000000000 : 0000000000000000

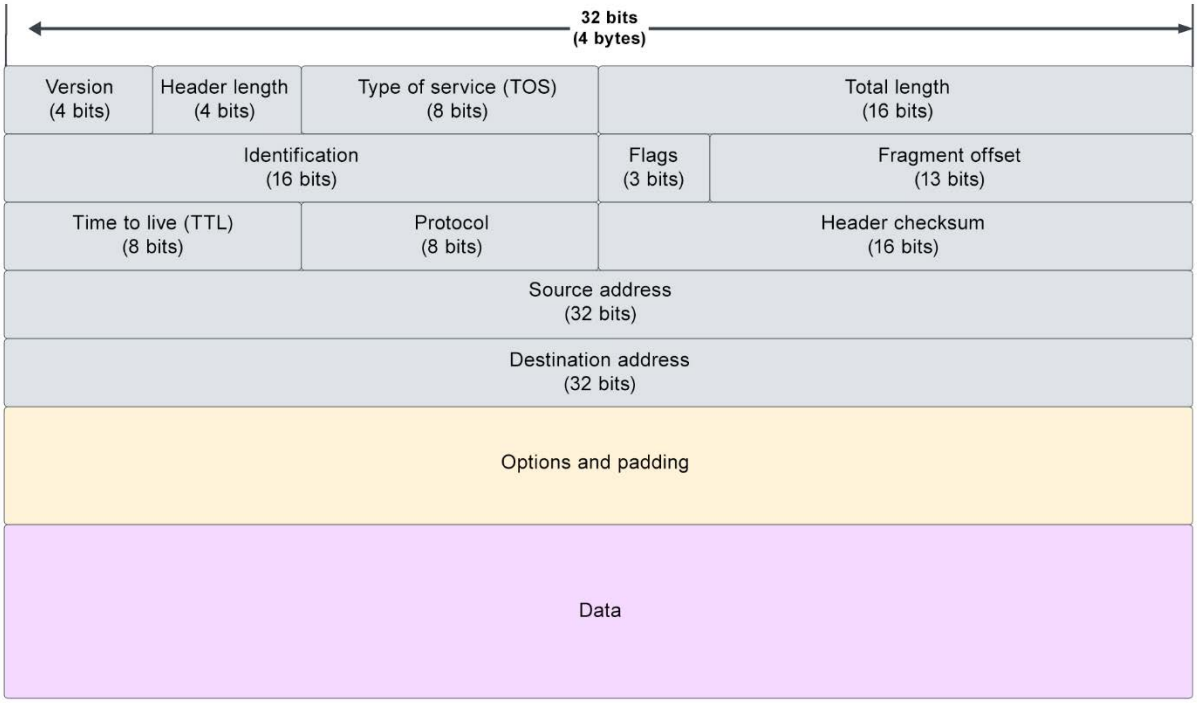
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

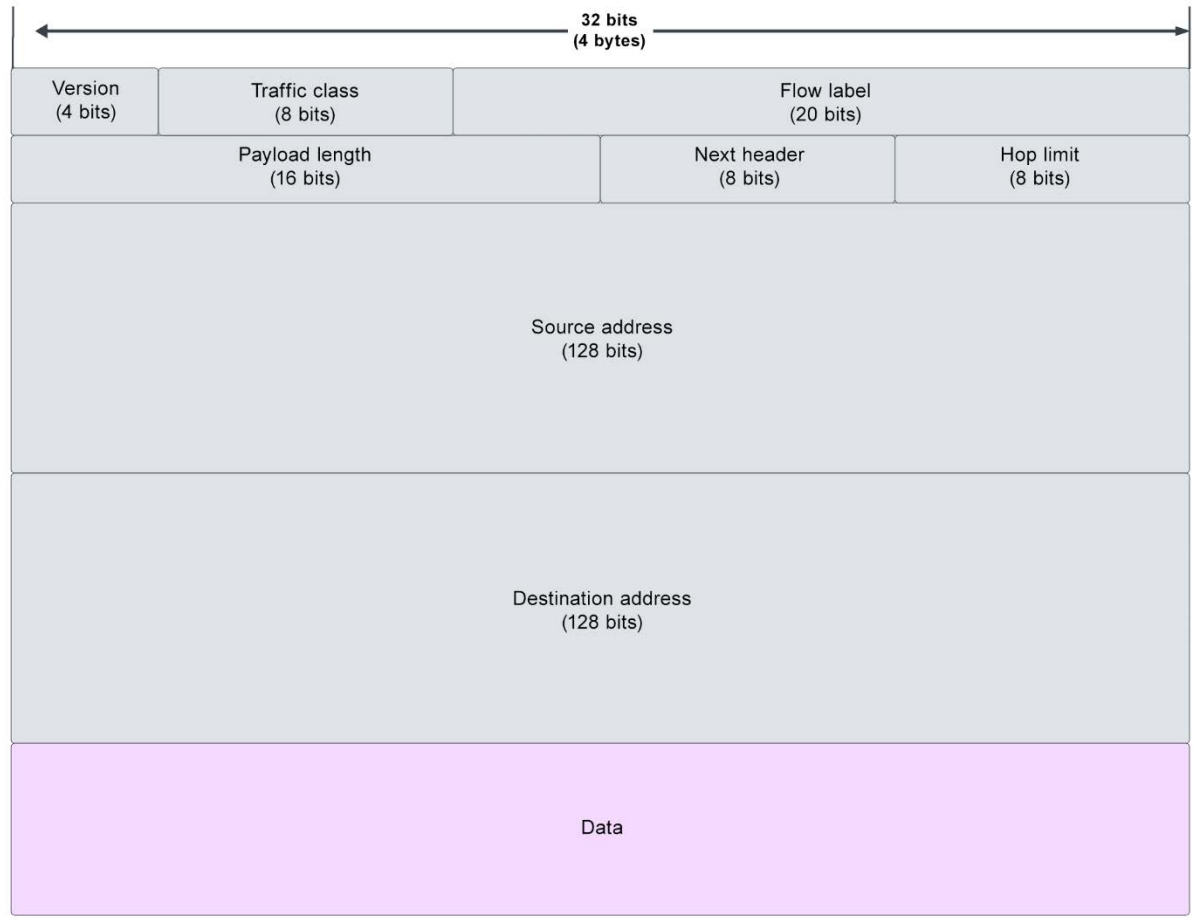
1111111111111111 : 1111111111111111 : 1111111111111111 : 1111111111111111 :
16 Bits 16 Bits 16 Bits 16 Bits
1111111111111111 : 1111111111111111 : 1111111111111111 : 1111111111111111

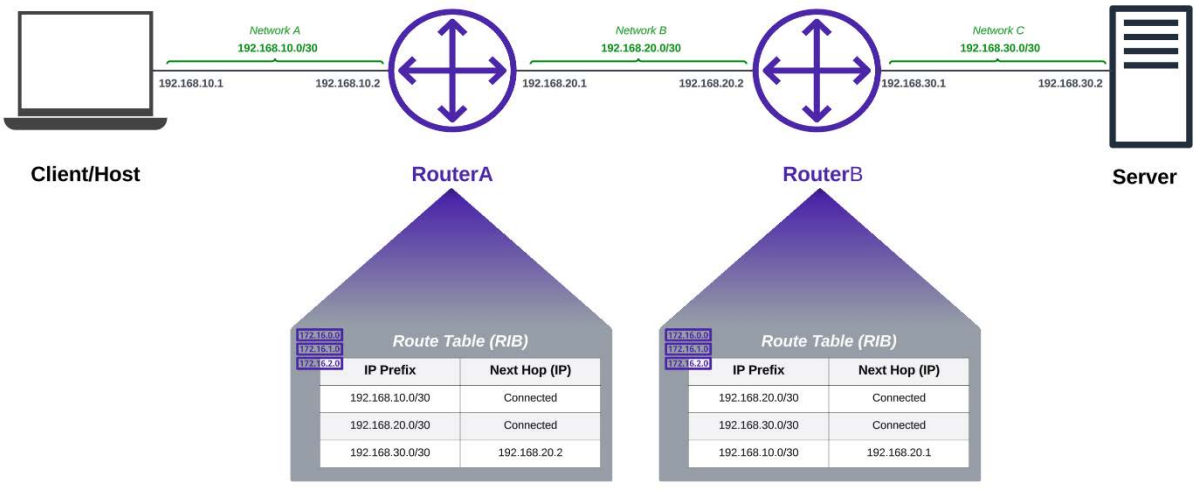
Hexadecimal Digit	Decimal Equivalent	Binary Representation
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
A	10	1010
B	11	1011
C	12	1100
D	13	1101
E	14	1110
F	15	1111

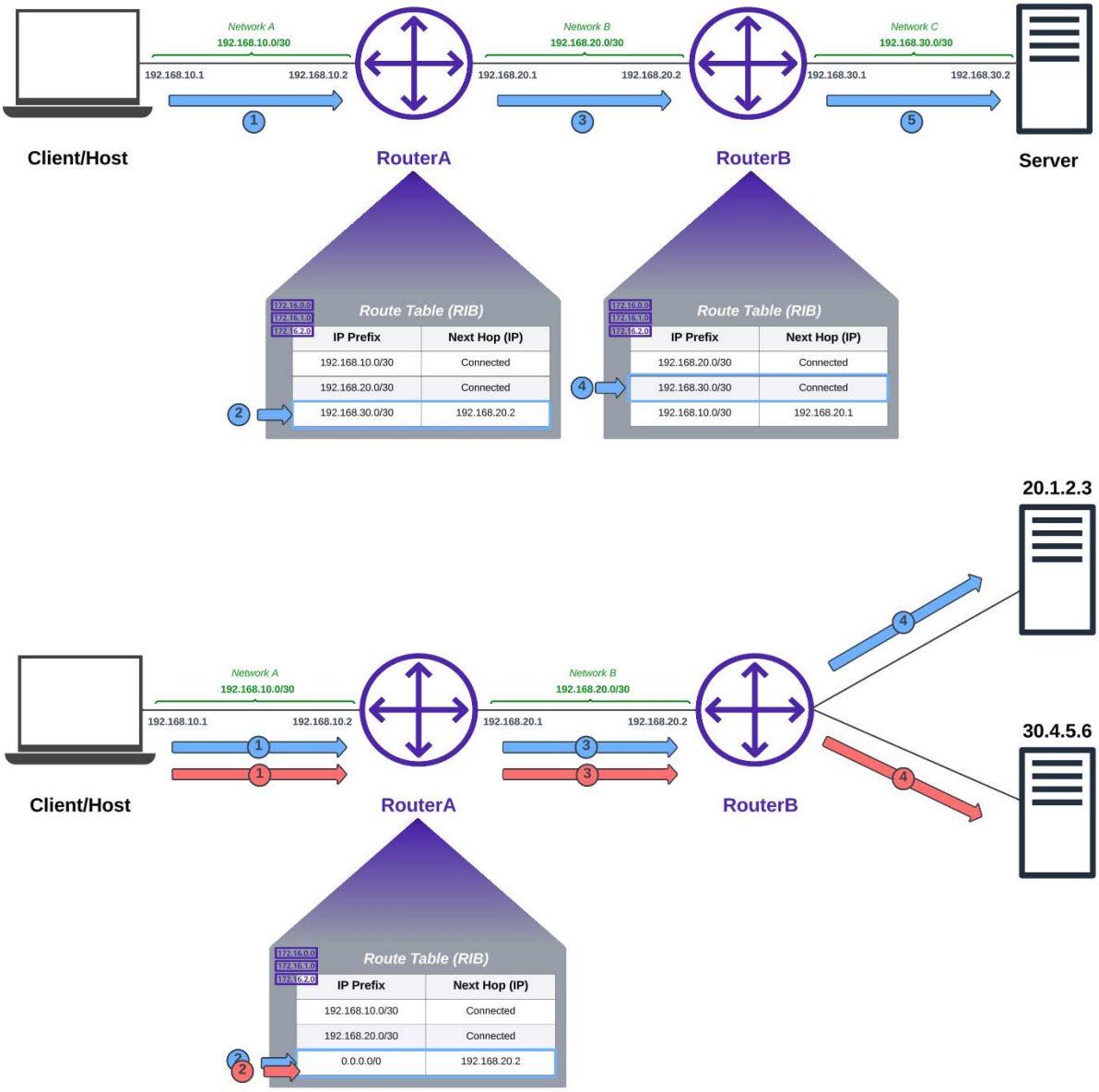
Appendix 2, IP Routing Fundamentals






32 bits
(4 bytes)
Version
(4 bits)
Traffic class
(8 bits)
Flow label
(20 bits)
Payload length
(16 bits)
Next header
(8 bits)
Hop limit
(8 bits)
Source address
(128 bits)
Destination address
(128 bits)
Data

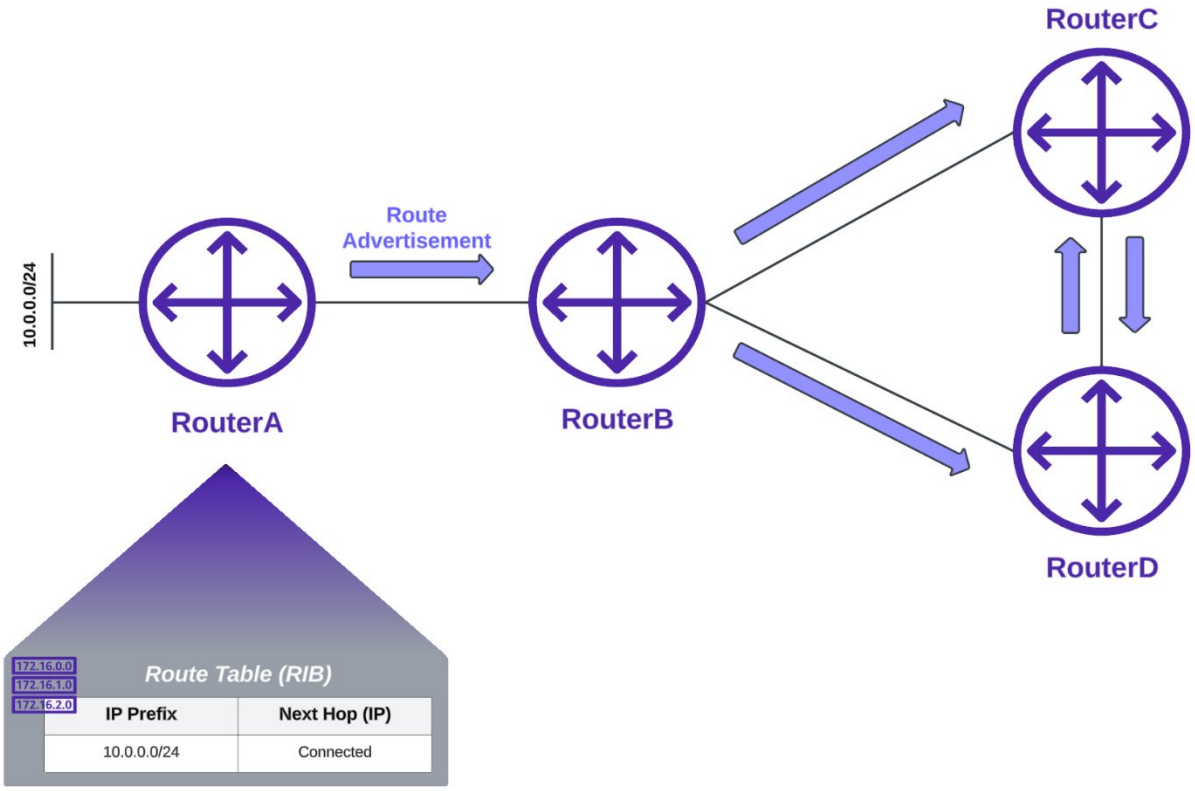

Network A
192.168.10.0/30
192.168.10.1
192.168.10.2
Network B
192.168.20.0/30
192.168.20.1
192.168.20.2
Network C
192.168.30.0/30
192.168.30.1
192.168.30.2
Client/Host
RouterA
RouterB
Server
Route Table (RIB)
IP Prefix
Next Hop (IP)
192.168.10.0/30
Connected
192.168.20.0/30
Connected
192.168.30.0/30
192.168.20.2
Route Table (RIB)
IP Prefix
Next Hop (IP)
192.168.20.0/30
Connected
192.168.30.0/30
Connected
192.168.10.0/30
192.168.20.1


Network A
192.168.10.0/30
192.168.10.1
192.168.10.2
Network B
192.168.20.0/30
192.168.20.1
192.168.20.2
Network C
192.168.30.0/30
192.168.30.1
192.168.30.2
Client/Host
RouterA
RouterB
Server
Route Table (RIB)
172.16.0.0
172.16.1.0
172.16.2.0
IP Prefix
Next Hop (IP)
192.168.10.0/30
Connected
192.168.20.0/30
Connected
192.168.30.0/30
192.168.20.2
Route Table (RIB)
172.16.0.0
172.16.1.0
172.16.2.0
IP Prefix
Next Hop (IP)
192.168.20.0/30
Connected
192.168.30.0/30
Connected
192.168.10.0/30
192.168.20.1

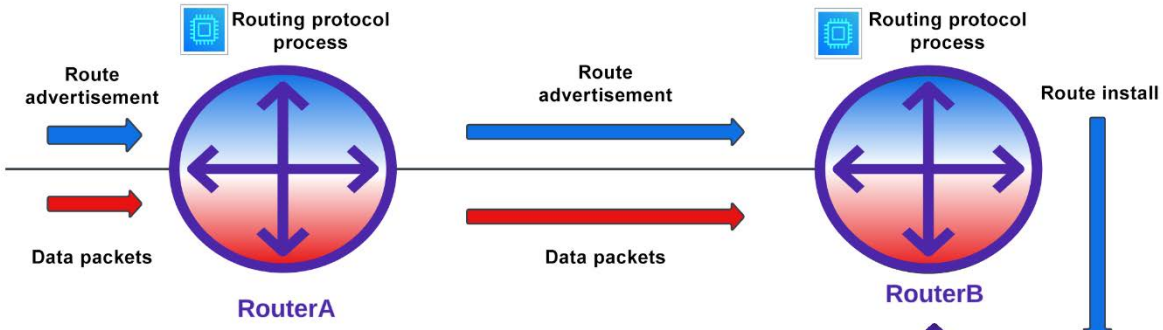
20.1.2.3
30.4.5.6
Network A
192.168.10.0/30
192.168.10.1
192.168.10.2
Network B
192.168.20.0/30
192.168.20.1
192.168.20.2
Client/Host
RouterA
RouterB
Route Table (RIB)
172.16.0.0
172.16.1.0
172.16.2.0
IP Prefix
Next Hop (IP)
192.168.10.0/30
Connected
192.168.20.0/30
Connected
0.0.0.0/0
192.168.20.2

```
C:\Users\[redacted]>route print
===========================================================================
Interface List
 17...b4 2e 99 39 07 40 ......Intel(R) Ethernet Connection (7) I219-V
  7...02 13 ef 1b 01 06 ......Microsoft Wi-Fi Direct Virtual Adapter
 11...00 13 ef 1b 01 06 ......Microsoft Wi-Fi Direct Virtual Adapter #2
 10...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
  6...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
  8...00 13 ef 1b 01 06 ......Realtek 8812BU Wireless LAN 802.11ac USB NIC
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.0.1    192.168.0.37     35
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      192.168.0.0    255.255.255.0         On-link      192.168.0.37    291
    192.168.0.37  255.255.255.255         On-link      192.168.0.37    291
```

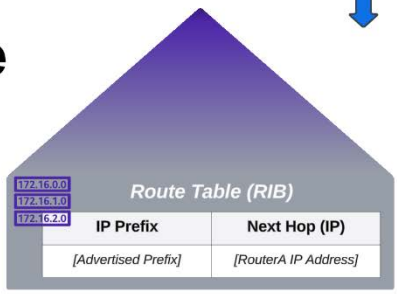
```
[redacted]@ubuntu:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         _gateway        0.0.0.0         UG        0 0          0 ens33
10.10.0.0       0.0.0.0         255.255.0.0     U         0 0          0 br-1bd7568ce6af
link-local      0.0.0.0         255.255.0.0     U         0 0          0 ens33
172.17.0.0      0.0.0.0         255.255.0.0     U         0 0          0 docker0
192.168.18.0    0.0.0.0         255.255.255.0   U         0 0          0 ens33
```

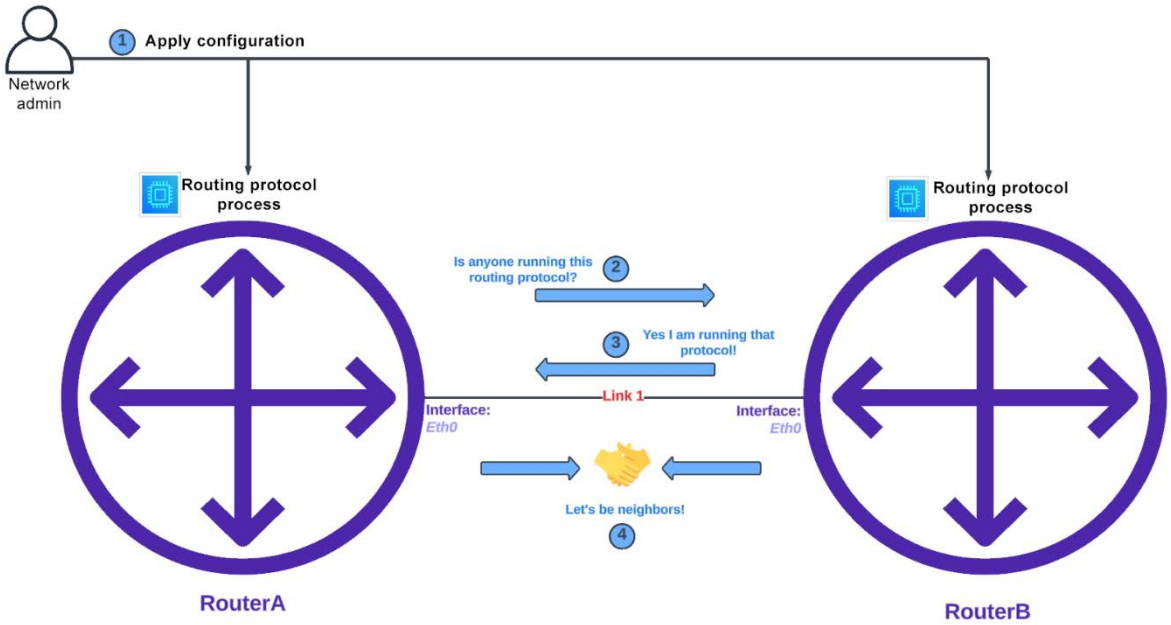


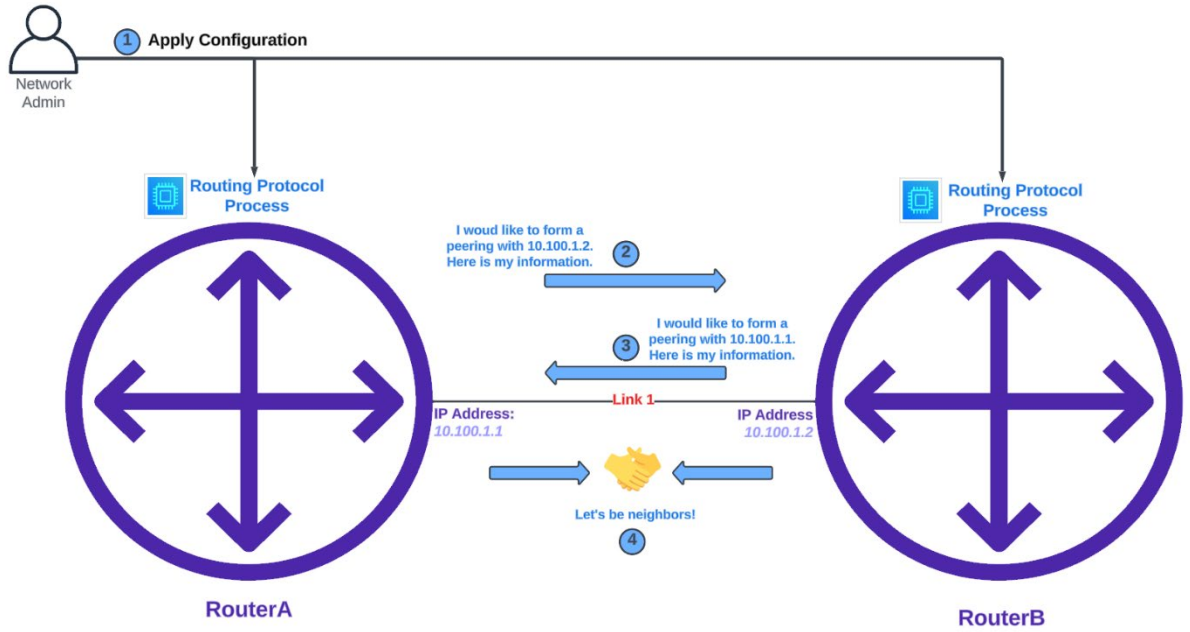
Control plane

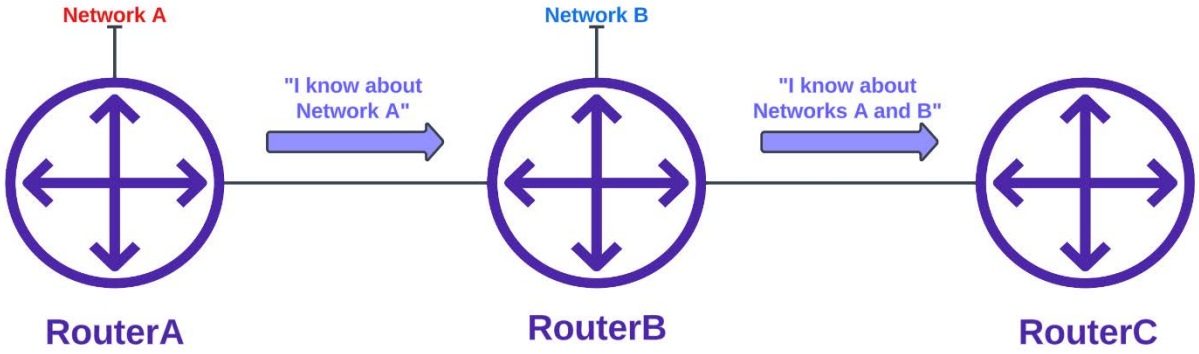


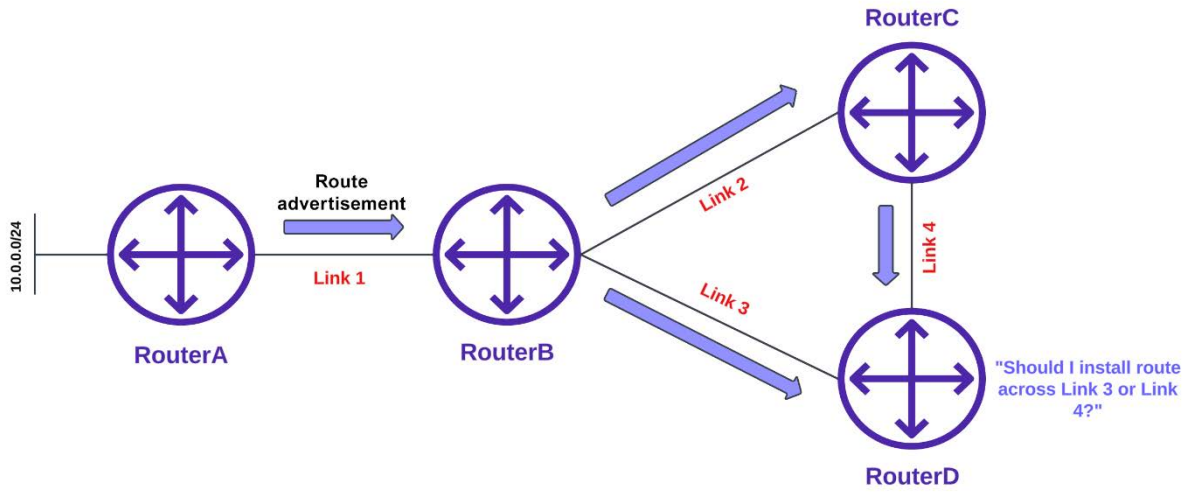
Data plane

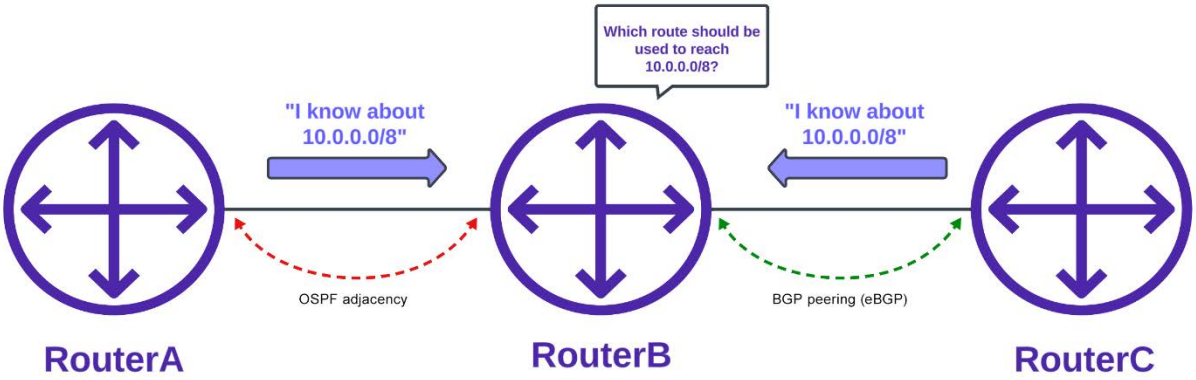


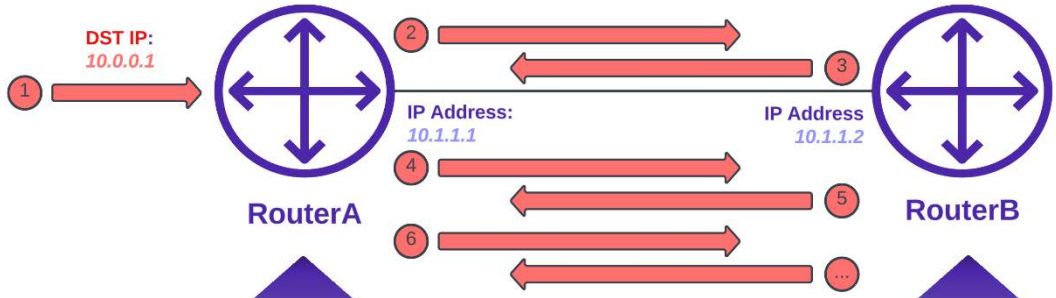


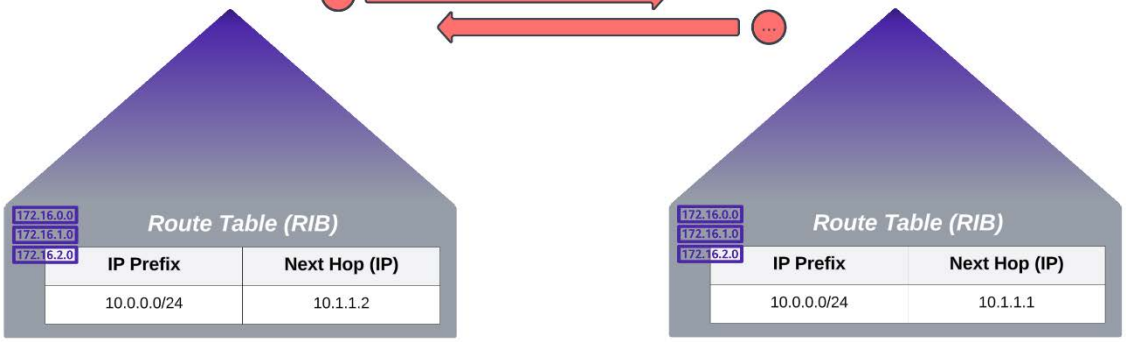

Network Admin
1 Apply Configuration
Routing Protocol Process
Routing Protocol Process
I woud like to form a peering with 10.100.1.2. Here is my information.
2
I would like to form a peering with 10.100.1.1. Here is my information.
3
Link 1
IP Address: 10.100.1.1
IP Address 10.100.1.2
Let's be neighbors!
4
RouterA
RouterB

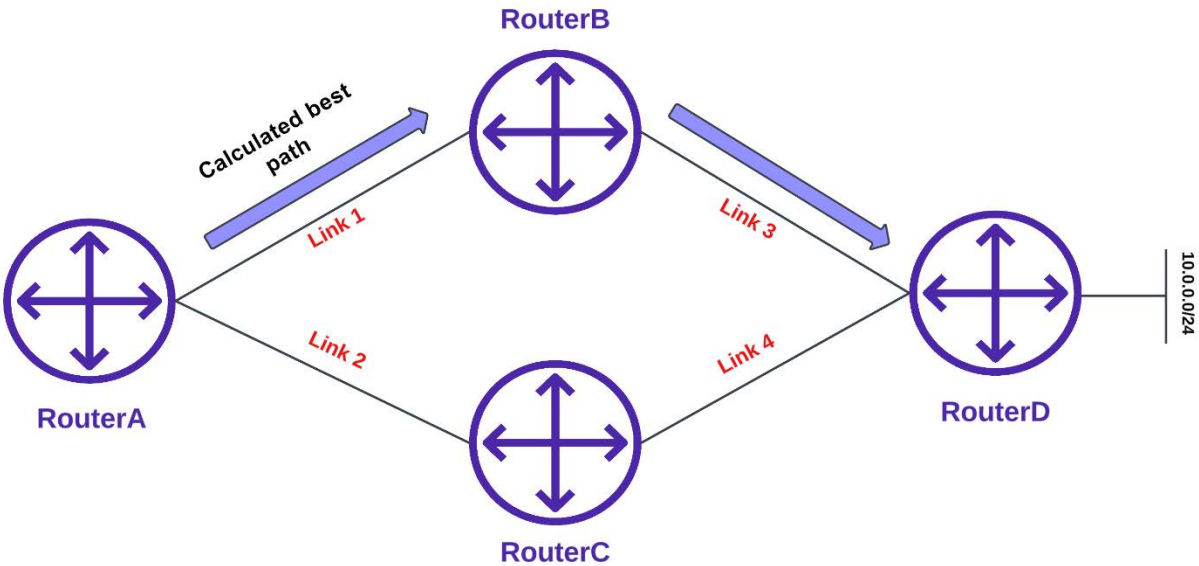

Network A
Network B
"I know about Network A"
"I know about Networks A and B"
RouterA
RouterB
RouterC

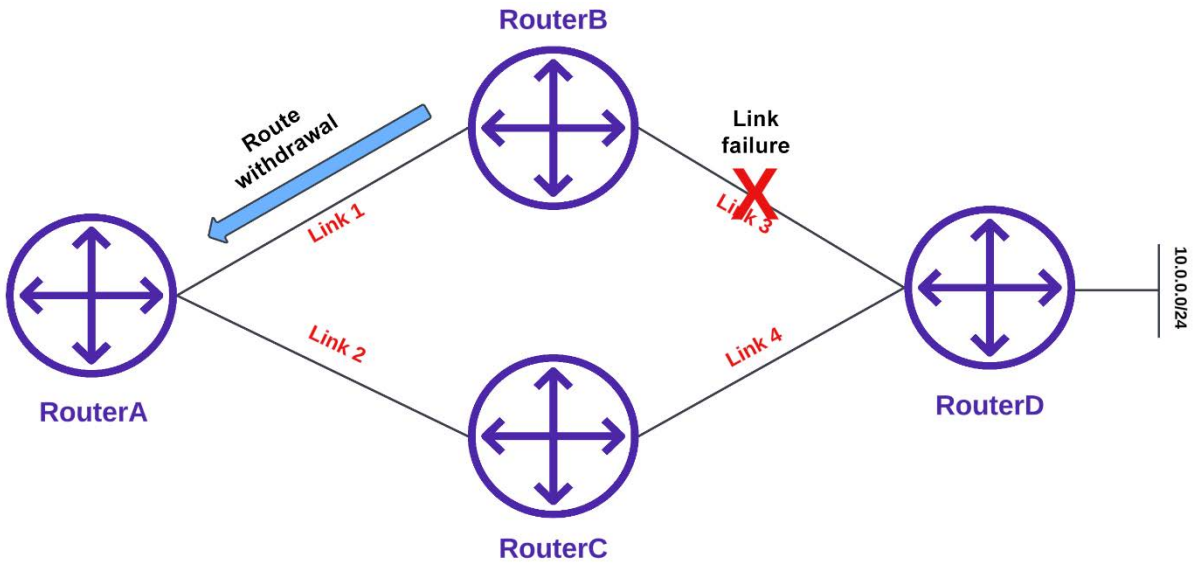

RouterC
Route advertisement
Link 1
Link 2
Link 3
Link 4
10.0.0.0/24
RouterA
RouterB
RouterD
"Should I install route across Link 3 or Link 4?"

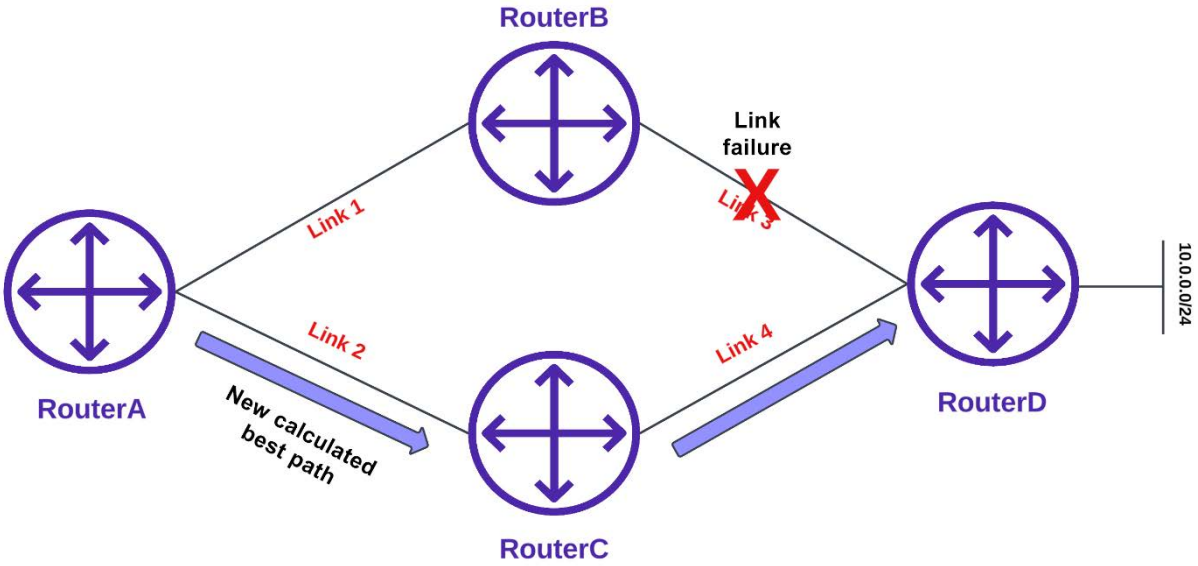

Which route should be used to reach 10.0.0.0/8?
"I know about 10.0.0.0/8"
"I know about 10.0.0.0/8"
OSPF adjacency
BGP peering (eBGP)
RouterA
RouterB
RouterC

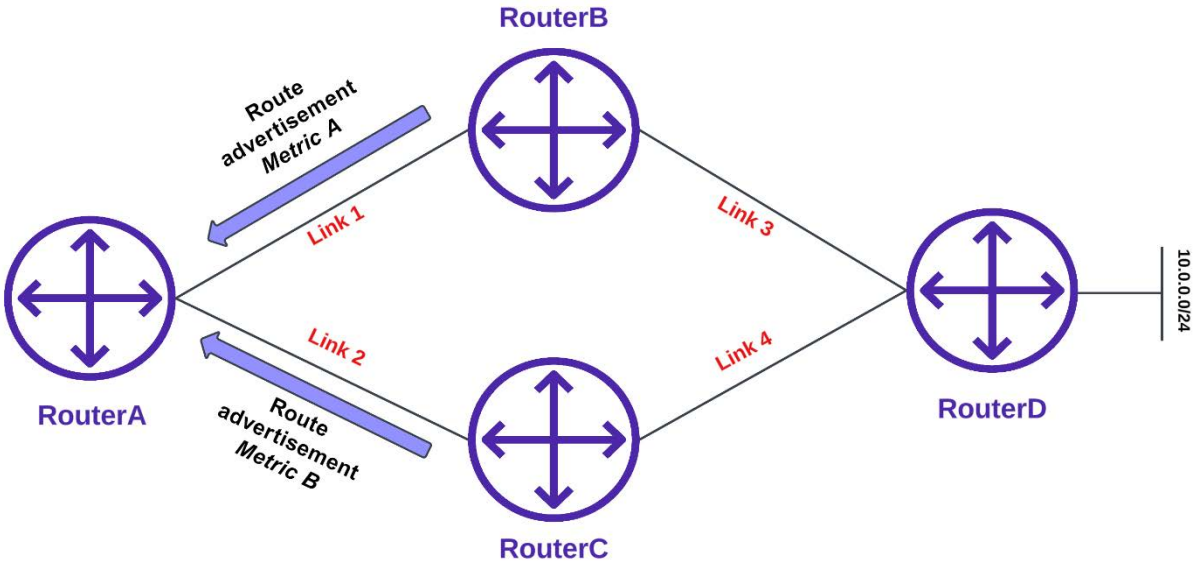

DST IP:
10.0.0.1
1
2
3
IP Address:
10.1.1.1
IP Address
10.1.1.2
4
5
6
...
RouterA
RouterB

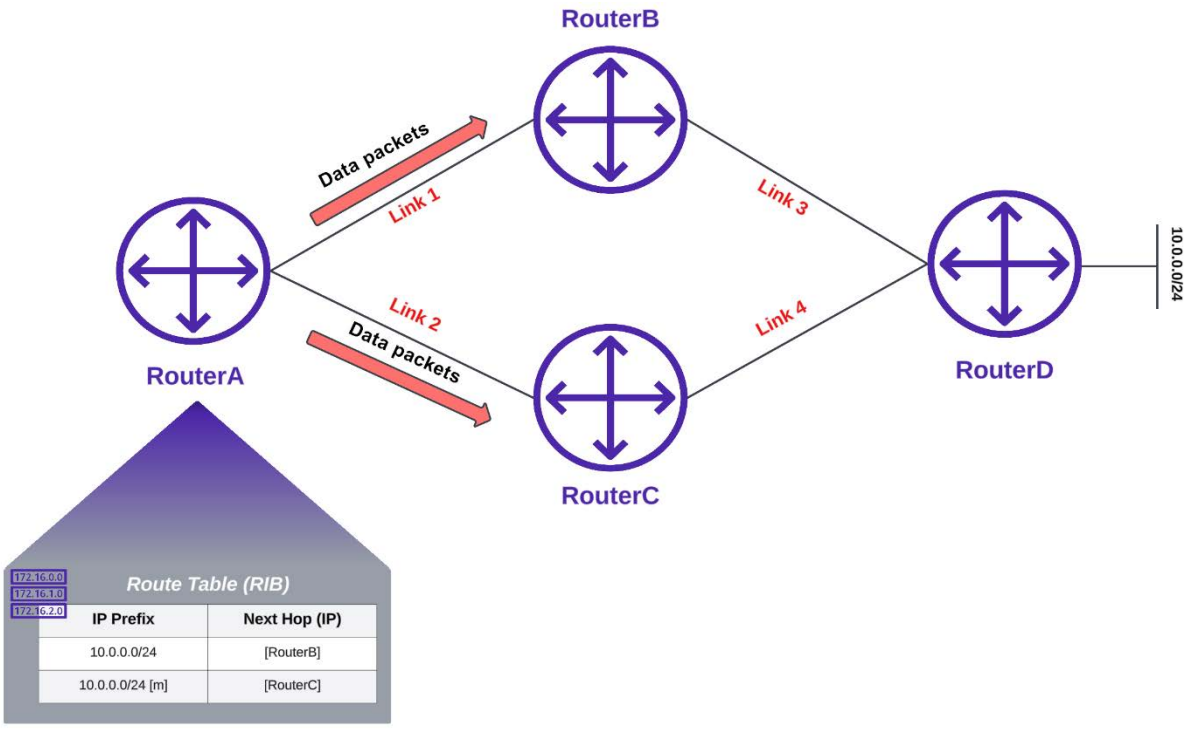

172.16.0.0
172.16.1.0
172.16.2.0
Route Table (RIB)
IP Prefix
Next Hop (IP)
10.0.0.0/24
10.1.1.2
172.16.0.0
172.16.1.0
172.16.2.0
Route Table (RIB)
IP Prefix
Next Hop (IP)
10.0.0.0/24
10.1.1.1

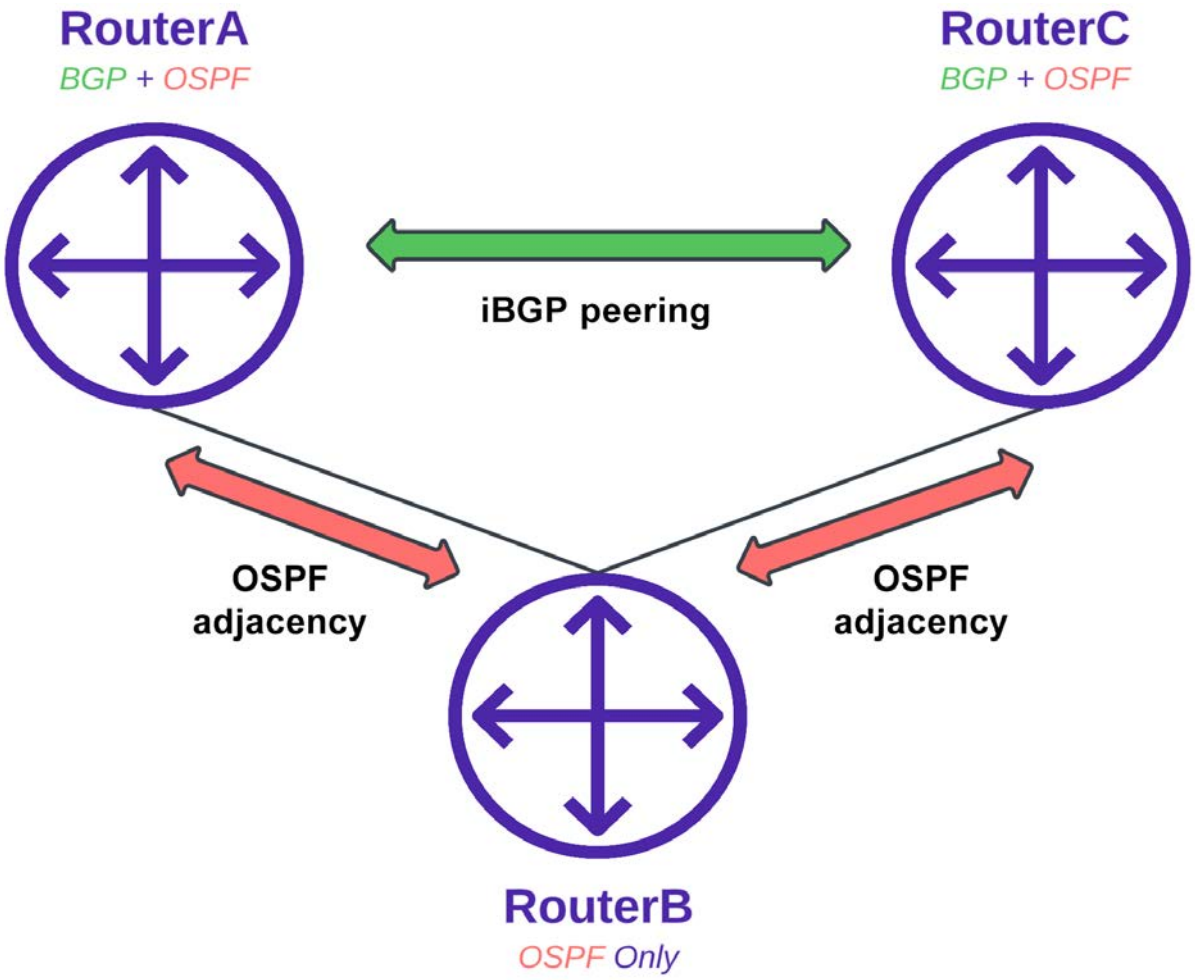

RouterB
Calculated best path
Link 1
Link 2
Link 3
Link 4
RouterA
RouterC
RouterD
10.0.0.0/24

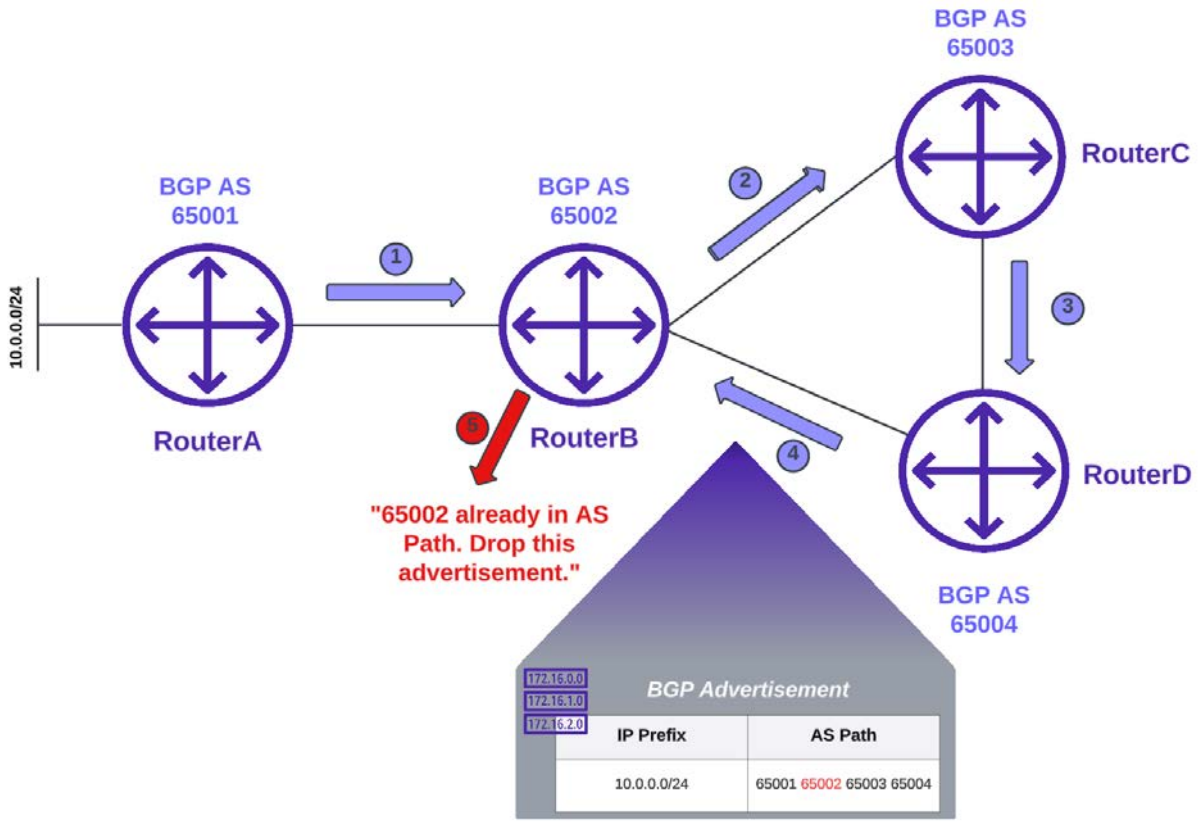

RouterB
Route withdrawal
Link failure
Link 1
Link 3
Link 2
Link 4
RouterA
RouterD
RouterC
10.0.0.0/24


RouterB
Link failure
Link 1
Link 3
Link 2
Link 4
RouterA
New calculated best path
RouterD
RouterC
10.0.0.0/24

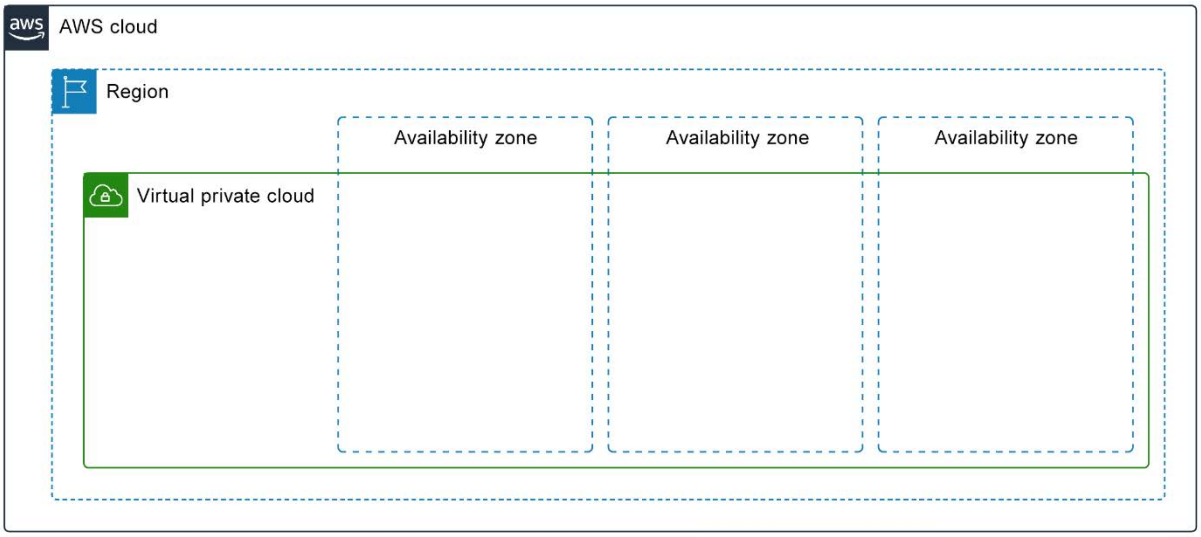

RouterB
Route advertisement Metric A
Link 1
Link 3
Link 2
Link 4
RouterA
Route advertisement Metric B
RouterD
RouterC
10.0.0.0/24

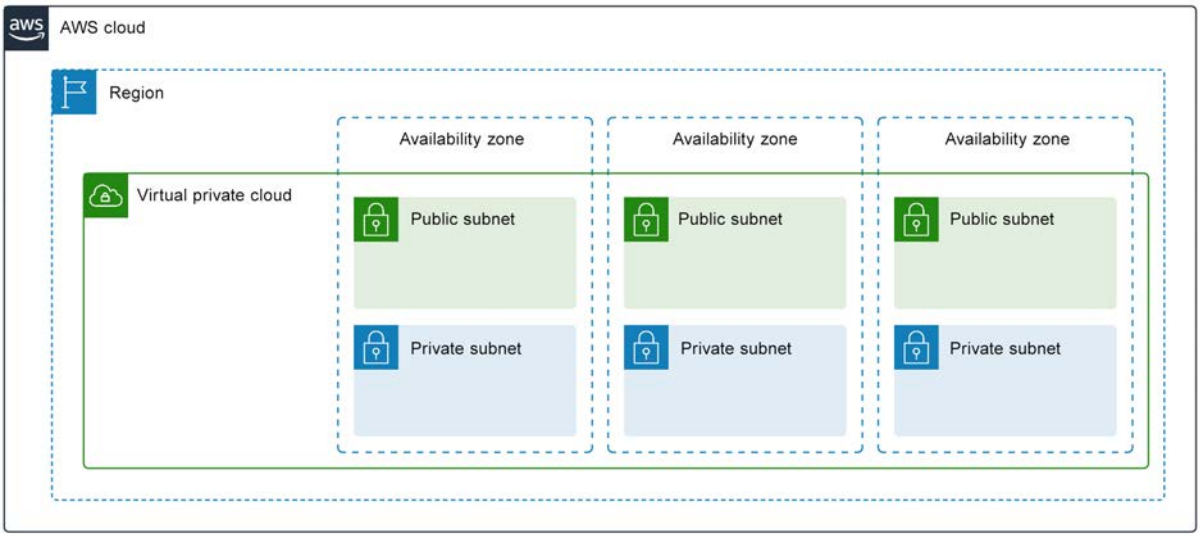

RouterB
Data packets
Link 1
Link 3
10.0.0.0/24
Link 2
Data packets
Link 4
RouterA
RouterD
RouterC
172.16.0.0
172.16.1.0
172.16.2.0
Route Table (RIB)
IP Prefix
Next Hop (IP)
10.0.0.0/24
[RouterB]
10.0.0.0/24 [m]
[RouterC]

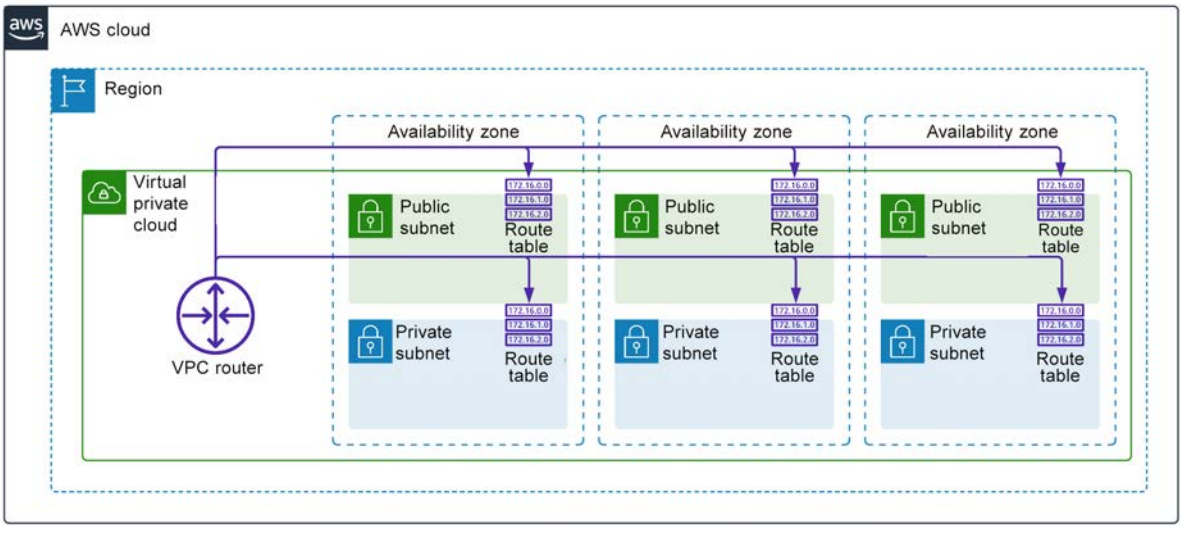

RouterA
BGP + OSPF
RouterC
BGP + OSPF
iBGP peering
OSPF
adjacency
OSPF
adjacency
RouterB
OSPF Only

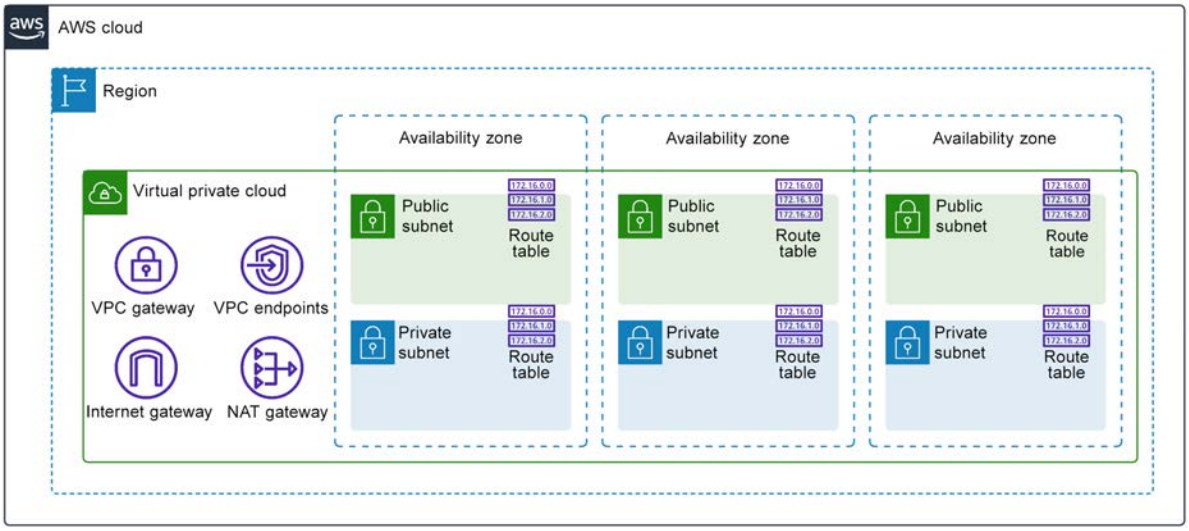

BGP AS
65003
RouterC
BGP AS
65001
BGP AS
65002
2
1
10.0.0.0/24
3
RouterA
5
RouterB
4
RouterD
"65002 already in AS
Path. Drop this
advertisement."
BGP AS
65004
172.16.0.0
172.16.1.0
172.16.2.0
BGP Advertisement
IP Prefix
AS Path
10.0.0.0/24
65001 65002 65003 65004

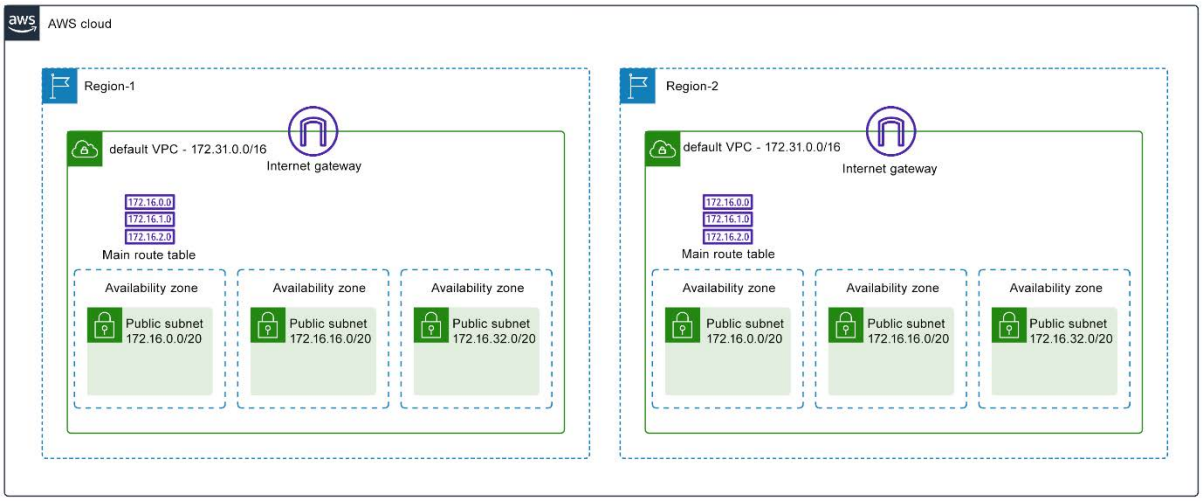
Appendix 3, VPC Networking Basics

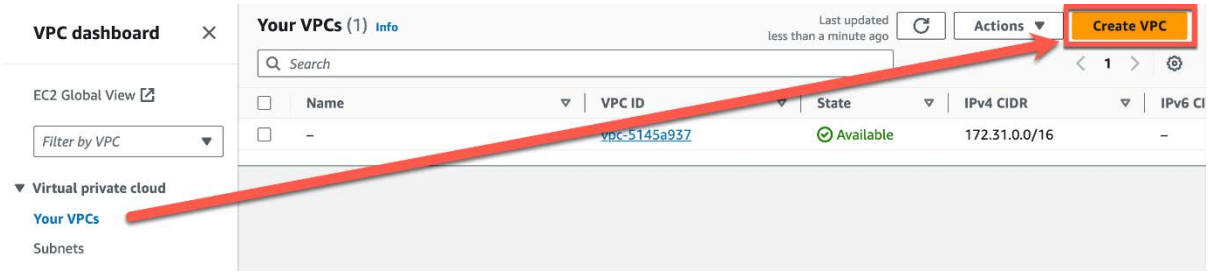







AWS cloud
Region
Availability zone
Availability zone
Availability zone
Virtual private cloud
Public subnet
Route table
Private subnet
VPC gateway
VPC endpoints
Internet gateway
NAT gateway


AWS cloud
Region-1
Region-2
default VPC - 172.31.0.0/16
Internet gateway
Main route table
Availability zone
Public subnet
172.16.0.0/20
172.16.16.0/20
172.16.32.0/20


VPC dashboard
EC2 Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Your VPCs (1) Info
Last updated
less than a minute ago
Actions
Create VPC
Search
Name
VPC ID
State
IPv4 CIDR
vpc-5145a937
Available
172.31.0.0/16

Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create Info

Create only the VPC resource or the VPC and other networking resources.

- (•) VPC only
- ( ) VPC and more

Name tag - *optional*

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

my-vpc-01

IPv4 CIDR block Info

- (•) IPv4 CIDR manual input
- ( ) IPAM-allocated IPv4 CIDR block

IPv4 CIDR

10.0.0.0/24

CIDR block size must be between /16 and /28.

IPv6 CIDR block Info

- (•) No IPv6 CIDR block
- ( ) IPAM-allocated IPv6 CIDR block
- ( ) Amazon-provided IPv6 CIDR block
- ( ) IPv6 CIDR owned by me

Tenancy Info

Default ▼

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.

No tags associated with the resource

Add tag

You can add 50 more tags

Cancel Create VPC

Number of Availability Zones (AZs) Info

Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.

1 | 2 | 3

▶ Customize AZs

Number of public subnets Info

The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.

0 | 2

Number of private subnets Info

The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.

0 | 2 | 4

▶ Customize subnets CIDR blocks

NAT gateways ($) Info

Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway

None | In 1 AZ | 1 per AZ

Egress only internet gateway Info

IPv6 only. Allows outbound communication over IPv6 in your private subnets.

No | Yes

VPC endpoints Info

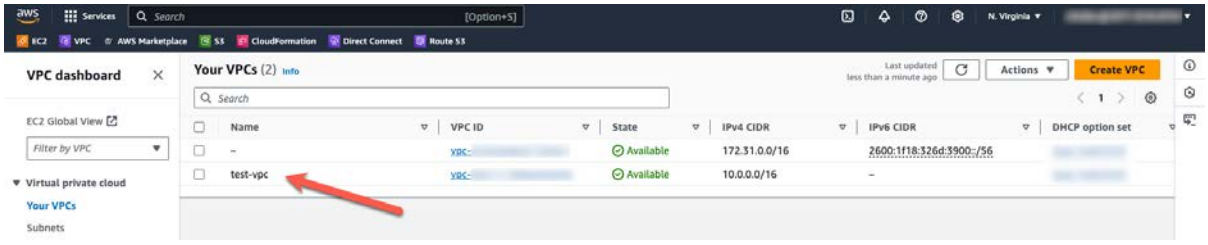
Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.

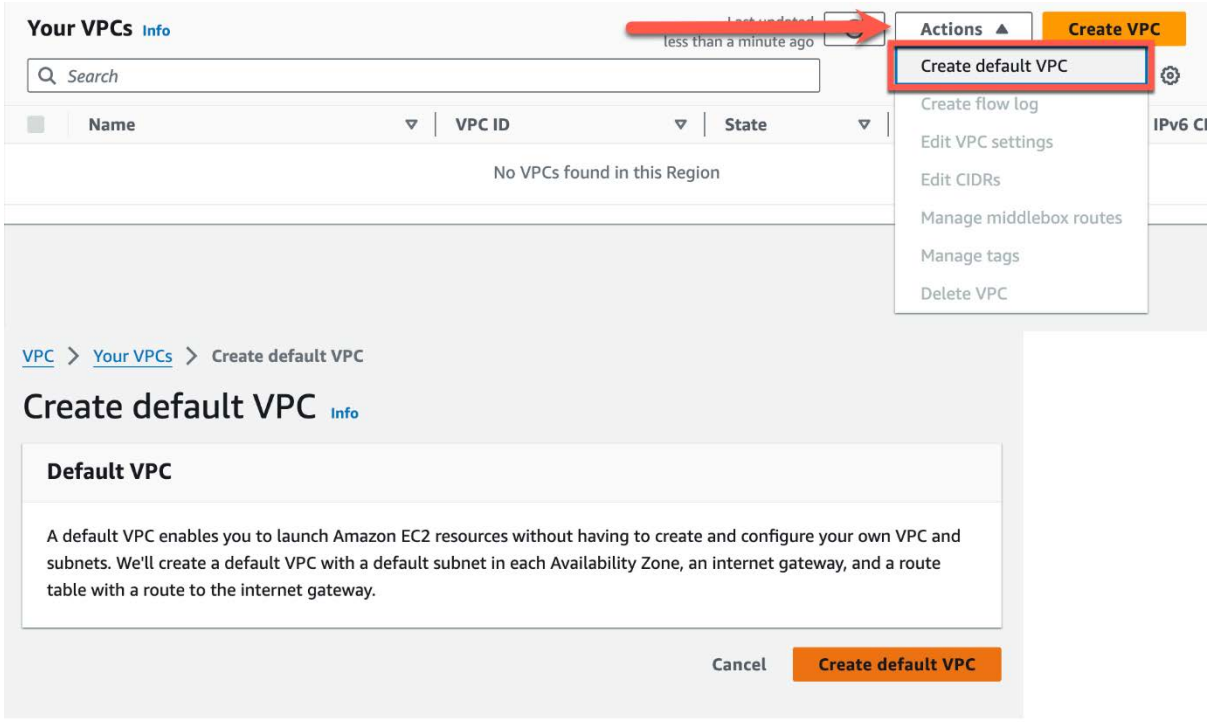
None | S3 Gateway

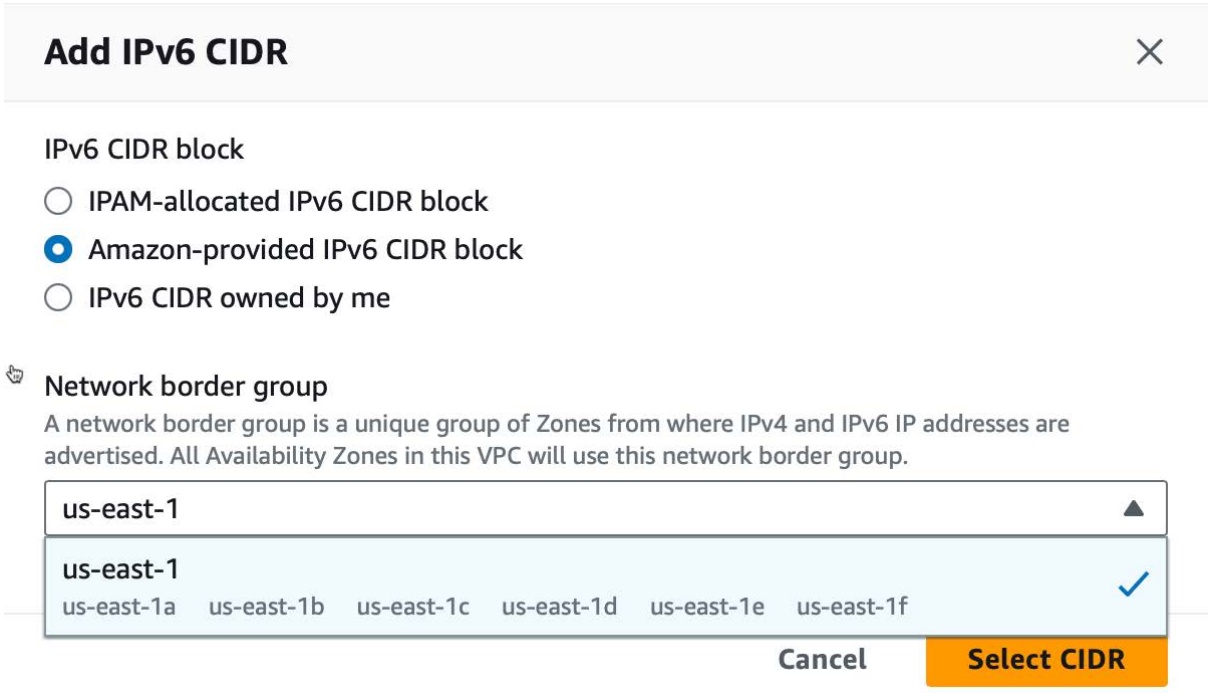
DNS options Info

☑ Enable DNS hostnames

☑ Enable DNS resolution




Your VPCs Info
Last updated
less than a minute ago
Actions
Create VPC
Search
Create default VPC
Create flow log
Edit VPC settings
Edit CIDRs
Manage middlebox routes
Manage tags
Delete VPC
Name
VPC ID
State
IPv6 CI
No VPCs found in this Region
VPC > Your VPCs > Create default VPC
Create default VPC Info
Default VPC
A default VPC enables you to launch Amazon EC2 resources without having to create and configure your own VPC and subnets. We'll create a default VPC with a default subnet in each Availability Zone, an internet gateway, and a route table with a route to the internet gateway.
Cancel
Create default VPC


Add IPv6 CIDR
IPv6 CIDR block
IPAM-allocated IPv6 CIDR block
Amazon-provided IPv6 CIDR block
IPv6 CIDR owned by me
Network border group
A network border group is a unique group of Zones from where IPv4 and IPv6 IP addresses are advertised. All Availability Zones in this VPC will use this network border group.
us-east-1
us-east-1
us-east-1a us-east-1b us-east-1c us-east-1d us-east-1e us-east-1f
Cancel
Select CIDR

Add IPv6 CIDR

IPv6 CIDR block

- ○ IPAM-allocated IPv6 CIDR block
- ○ Amazon-provided IPv6 CIDR block
- ◉ IPv6 CIDR owned by me

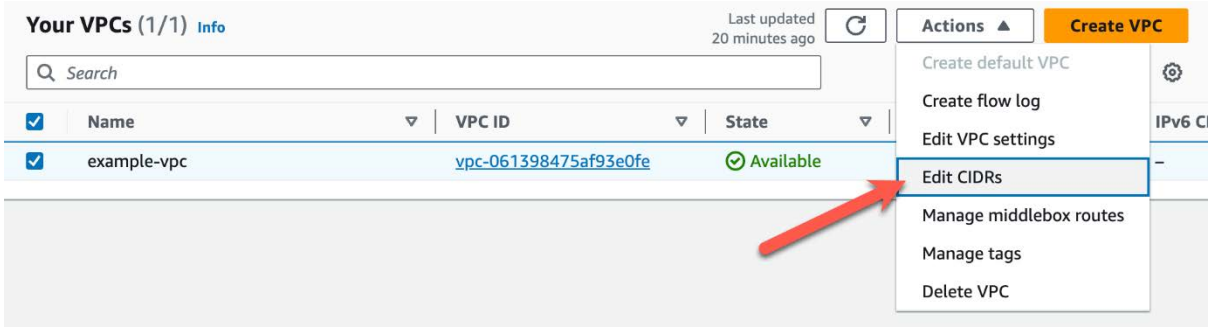
Pool

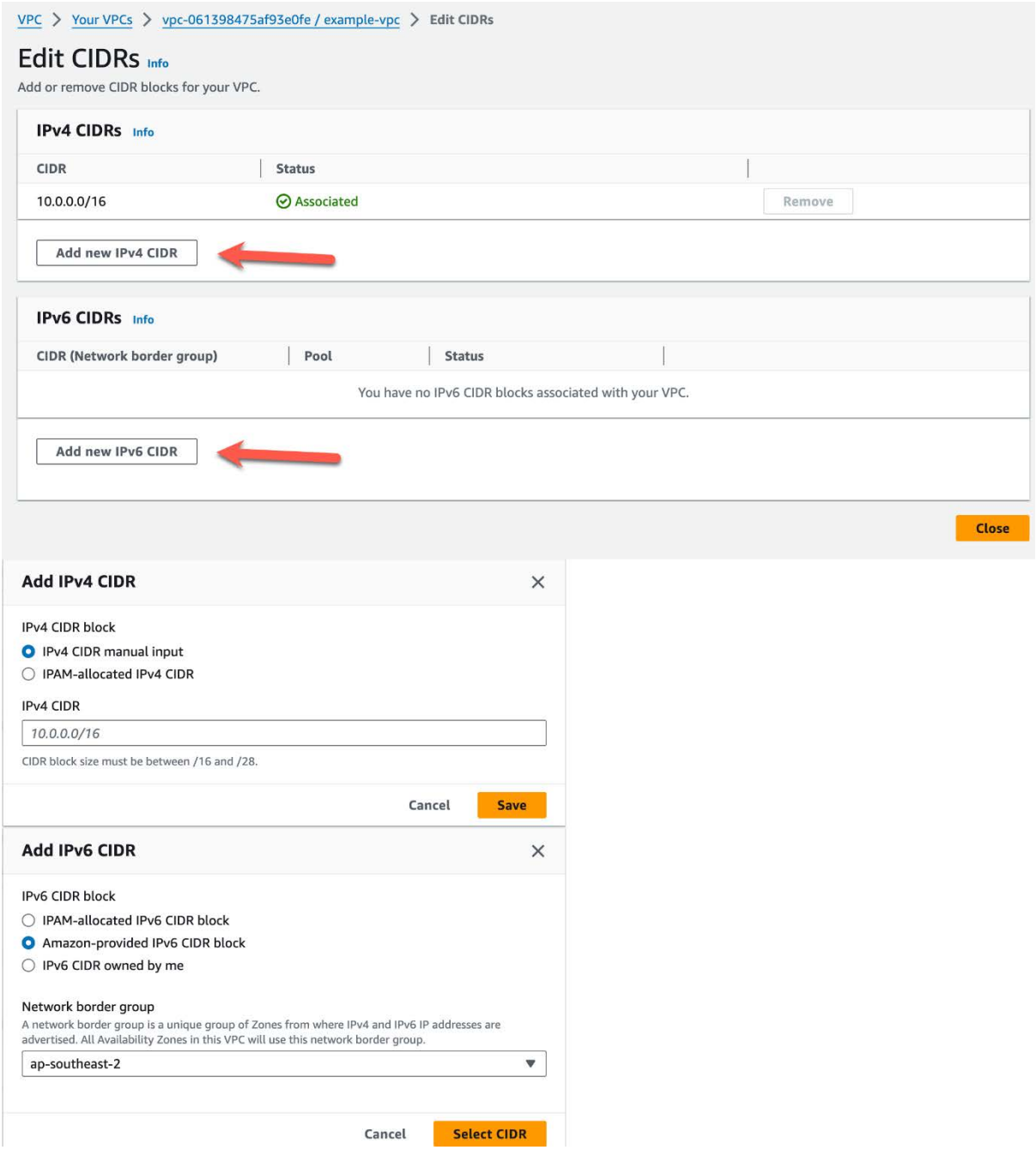
Choose pool

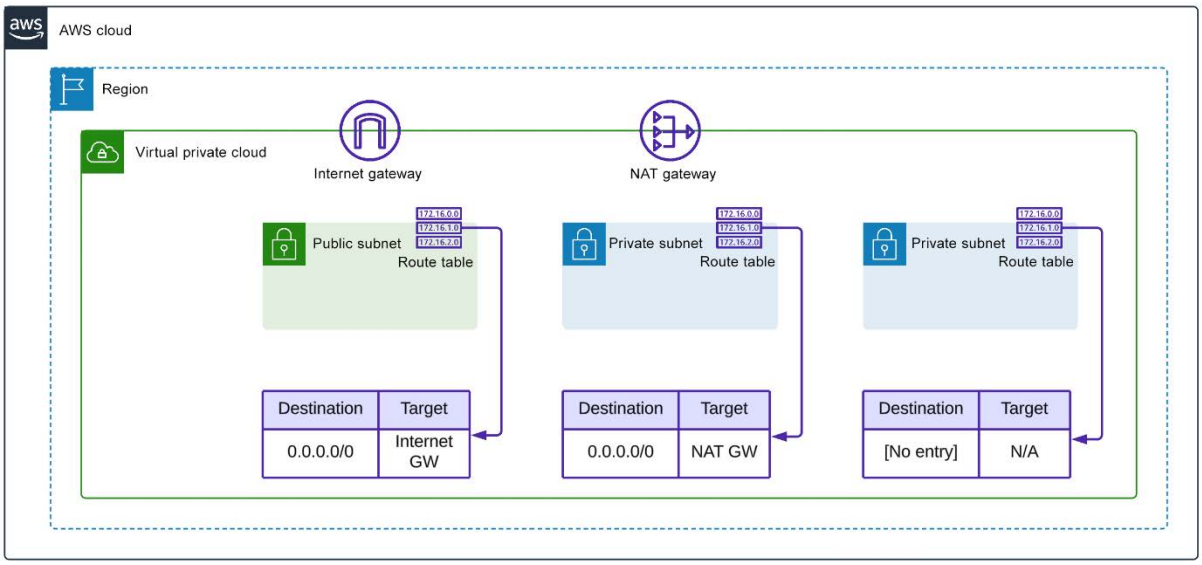
Pool CIDRs

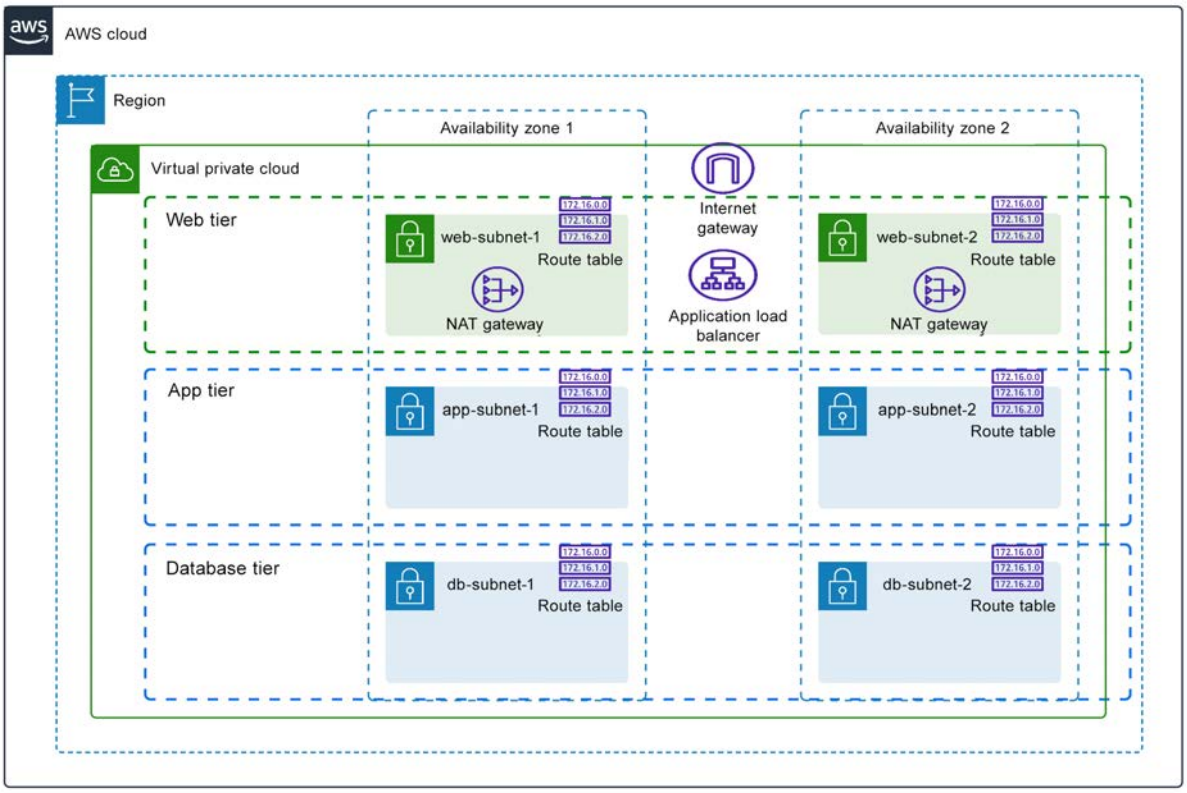
–

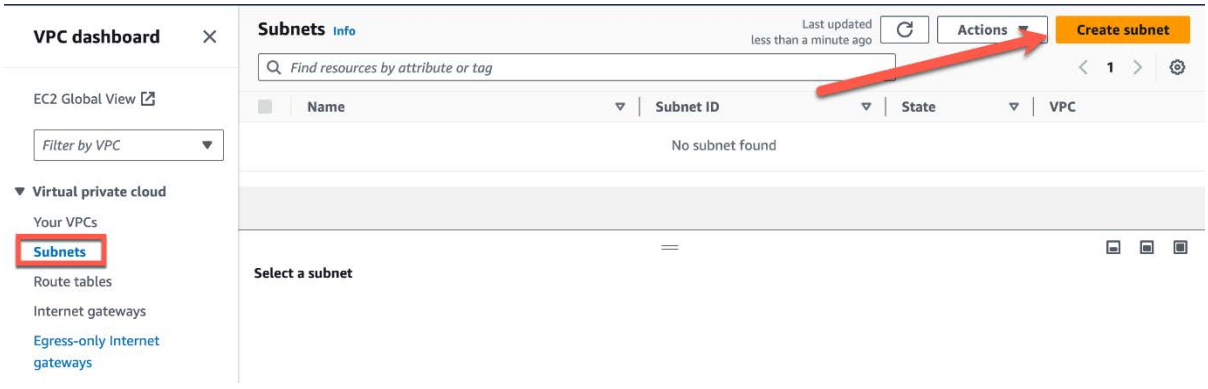
Cancel **Select CIDR**




VPC > Your VPCs > vpc-061398475af93e0fe / example-vpc > Edit CIDRs
Edit CIDRs Info
Add or remove CIDR blocks for your VPC.
IPv4 CIDRs Info
CIDR
Status
10.0.0.0/16
Associated
Remove
Add new IPv4 CIDR
IPv6 CIDRs Info
CIDR (Network border group)
Pool
Status
You have no IPv6 CIDR blocks associated with your VPC.
Add new IPv6 CIDR
Close
Add IPv4 CIDR
IPv4 CIDR block
IPv4 CIDR manual input
IPAM-allocated IPv4 CIDR
IPv4 CIDR
10.0.0.0/16
CIDR block size must be between /16 and /28.
Cancel
Save
Add IPv6 CIDR
IPv6 CIDR block
IPAM-allocated IPv6 CIDR block
Amazon-provided IPv6 CIDR block
IPv6 CIDR owned by me
Network border group
A network border group is a unique group of Zones from where IPv4 and IPv6 IP addresses are advertised. All Availability Zones in this VPC will use this network border group.
ap-southeast-2
Cancel
Select CIDR


AWS cloud
Region
Virtual private cloud
Internet gateway
NAT gateway
Public subnet
Route table
Private subnet
Route table
Private subnet
Route table
Destination
Target
0.0.0.0/0
Internet GW
Destination
Target
0.0.0.0/0
NAT GW
Destination
Target
[No entry]
N/A


AWS cloud
Region
Availability zone 1
Availability zone 2
Virtual private cloud
Internet gateway
Application load balancer
Web tier
web-subnet-1
Route table
NAT gateway
web-subnet-2
Route table
NAT gateway
App tier
app-subnet-1
Route table
app-subnet-2
Route table
Database tier
db-subnet-1
Route table
db-subnet-2
Route table


VPC dashboard
EC2 Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only Internet gateways
Subnets Info
Last updated less than a minute ago
Actions
Create subnet
Find resources by attribute or tag
Name
Subnet ID
State
VPC
No subnet found
Select a subnet

VPC > Subnets > Create subnet

Create subnet Info

VPC

VPC ID
Create subnets in this VPC.
vpc-061398475af93e0fe (example-vpc)

Associated VPC CIDRs

IPv4 CIDRs
10.0.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
my-subnet-01
The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
No preference

IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
10.0.0.0/16

IPv4 subnet CIDR block
10.0.1.0/24 256 IPs

▼ **Tags** - *optional*

No tags associated with the resource.

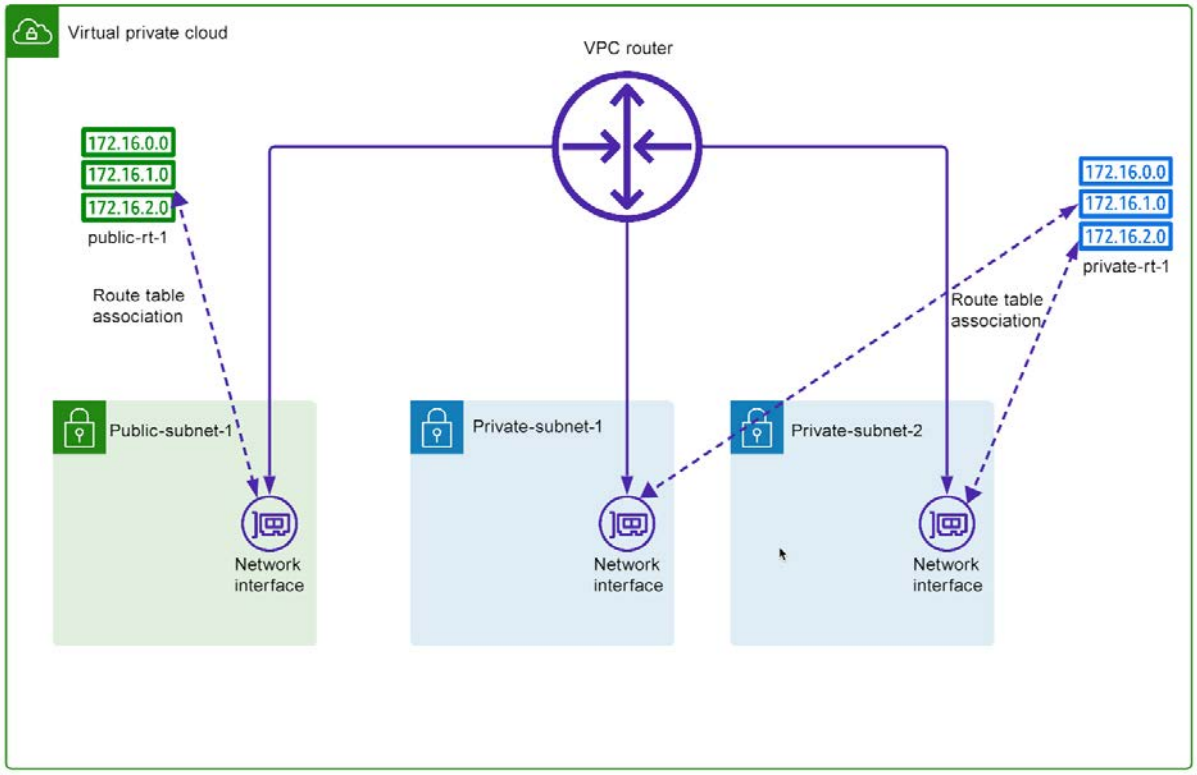
Add new tag
You can add 50 more tags.

Remove

Add new subnet

Configure additional subnets

Cancel Create subnet



VPC > Route tables > rtb-0c6bd67941c2574ef

rtb-0c6bd67941c2574ef / route-table-test-01

Actions

Details Info

Route table ID	Main	Explicit subnet associations	Edge associations
rtb-0c6bd67941c2574ef	No	–	–

VPC: vpc-021c84d09b2b7a0d0 | vpc-use1-test

Owner ID:

Routes | Subnet associations | Edge associations | Route propagation | Tags

Routes (3)

Both | Edit routes

Filter routes

1

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0a5bb00ff69314b96	Active	No
10.0.0.0/24	local	Active	No
10.140.0.0/16	pcx-0c0f4d7d60586f64b	Active	No

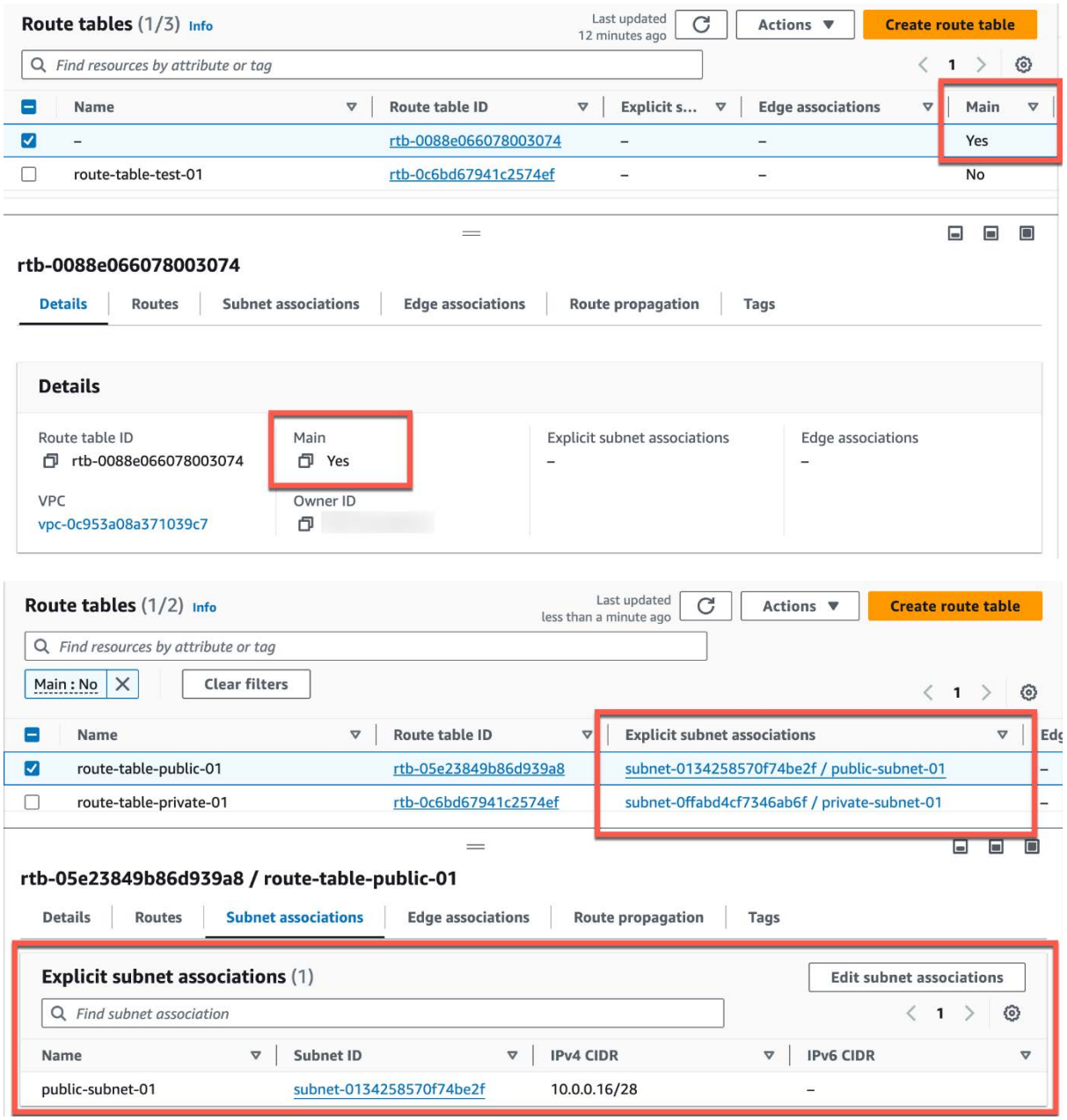
Routes (3)

Both | Edit routes

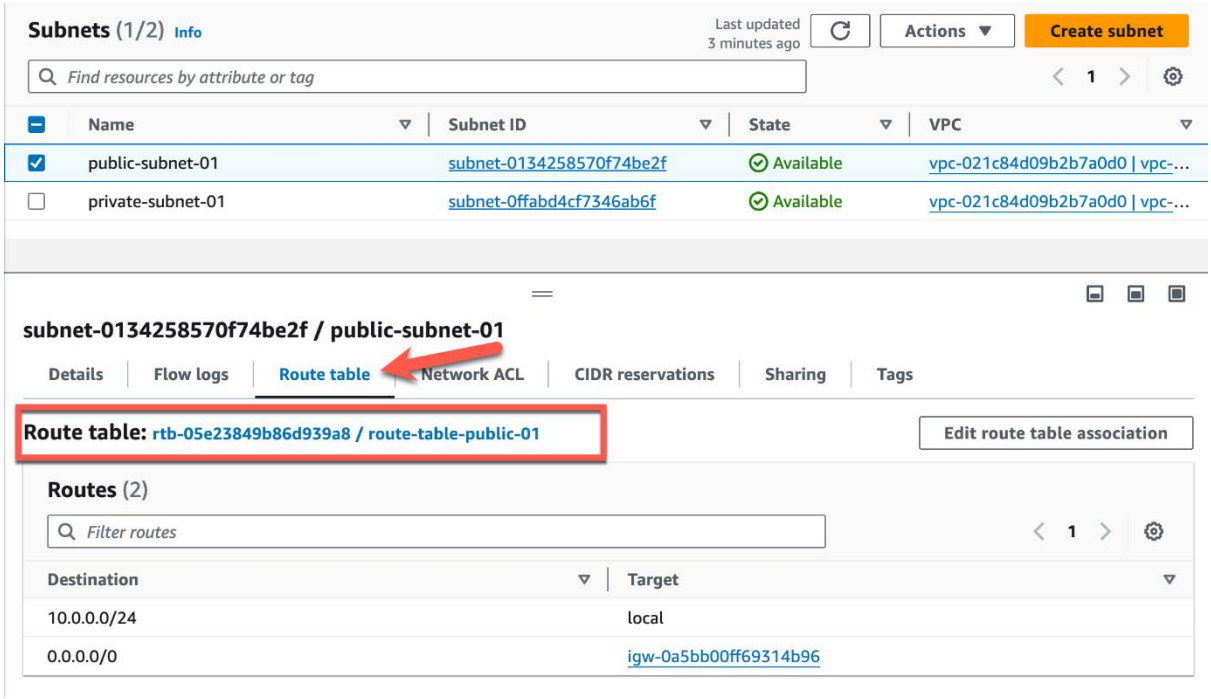
Filter routes

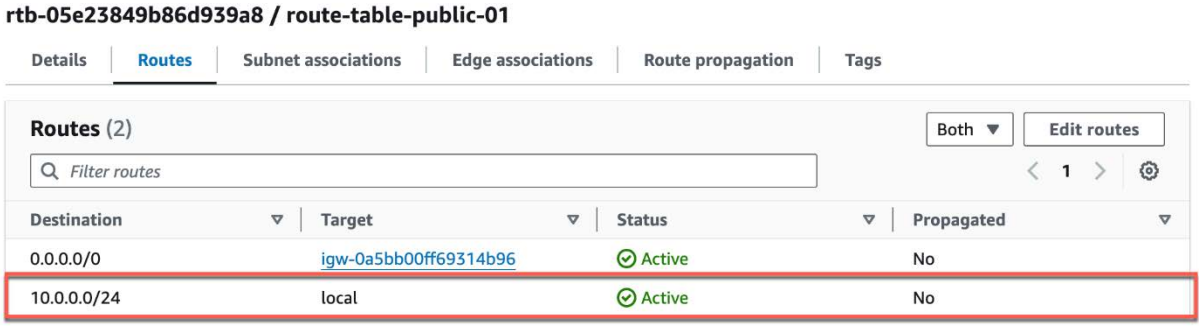
1

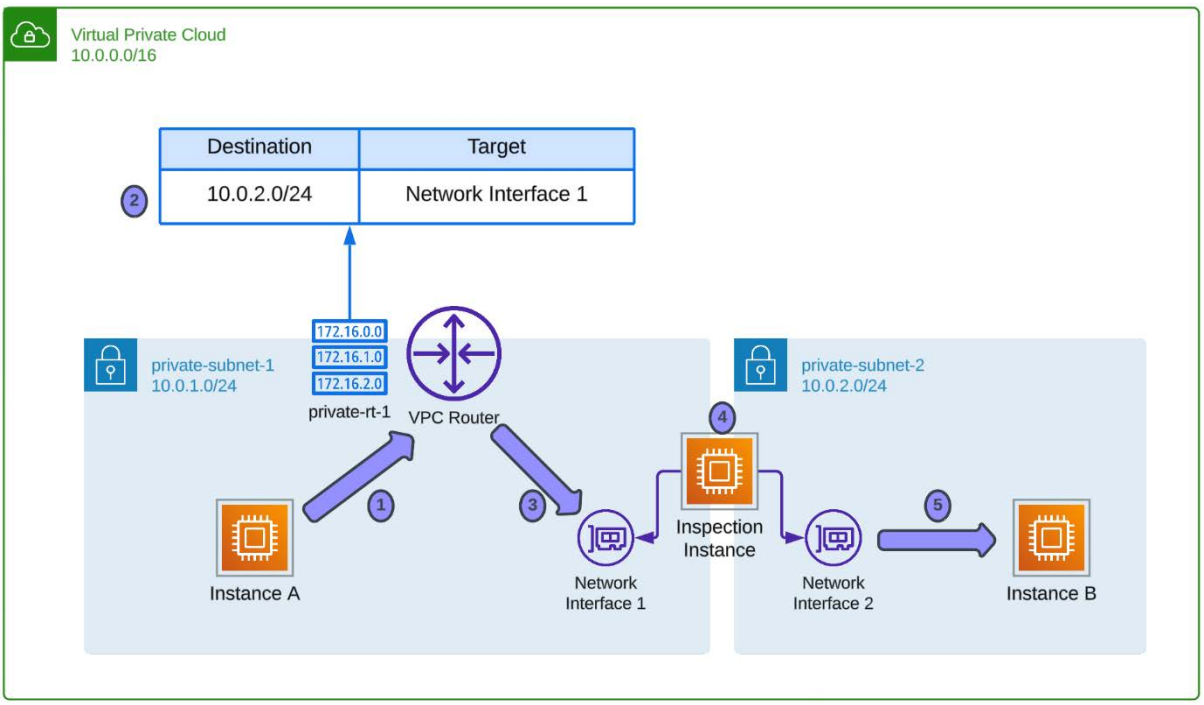
Destination	Target	Status	Propagated
0.0.0.0/0	igw-0a5bb00ff69314b96	Active	No
10.0.0.0/24	local	Active	No
10.140.0.0/16	pcx-0c0f4d7d60586f64b	Blackhole	No

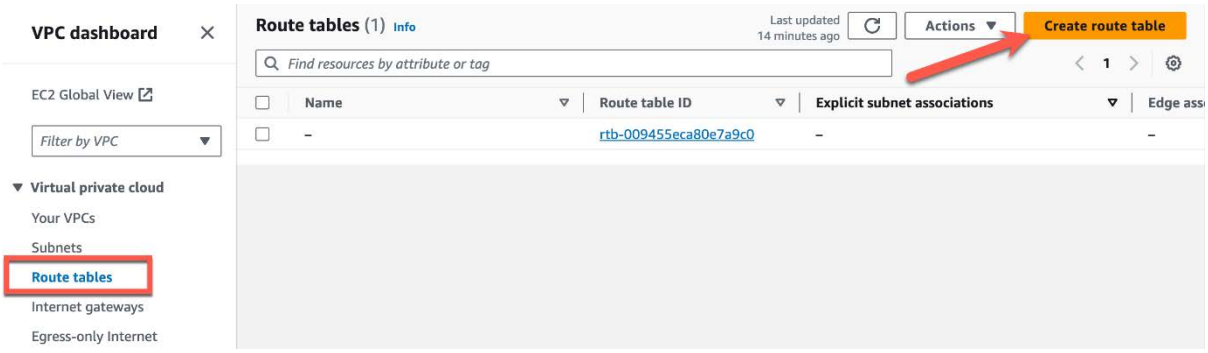

Route tables (1/3) Info
Last updated 12 minutes ago
Actions
Create route table
Find resources by attribute or tag
Name
Route table ID
Explicit s...
Edge associations
Main
– rtb-0088e066078003074 – – Yes
route-table-test-01 rtb-0c6bd67941c2574ef – – No
rtb-0088e066078003074
Details
Routes
Subnet associations
Edge associations
Route propagation
Tags
Details
Route table ID
rtb-0088e066078003074
Main
Yes
Explicit subnet associations
–
Edge associations
–
VPC
vpc-0c953a08a371039c7
Owner ID

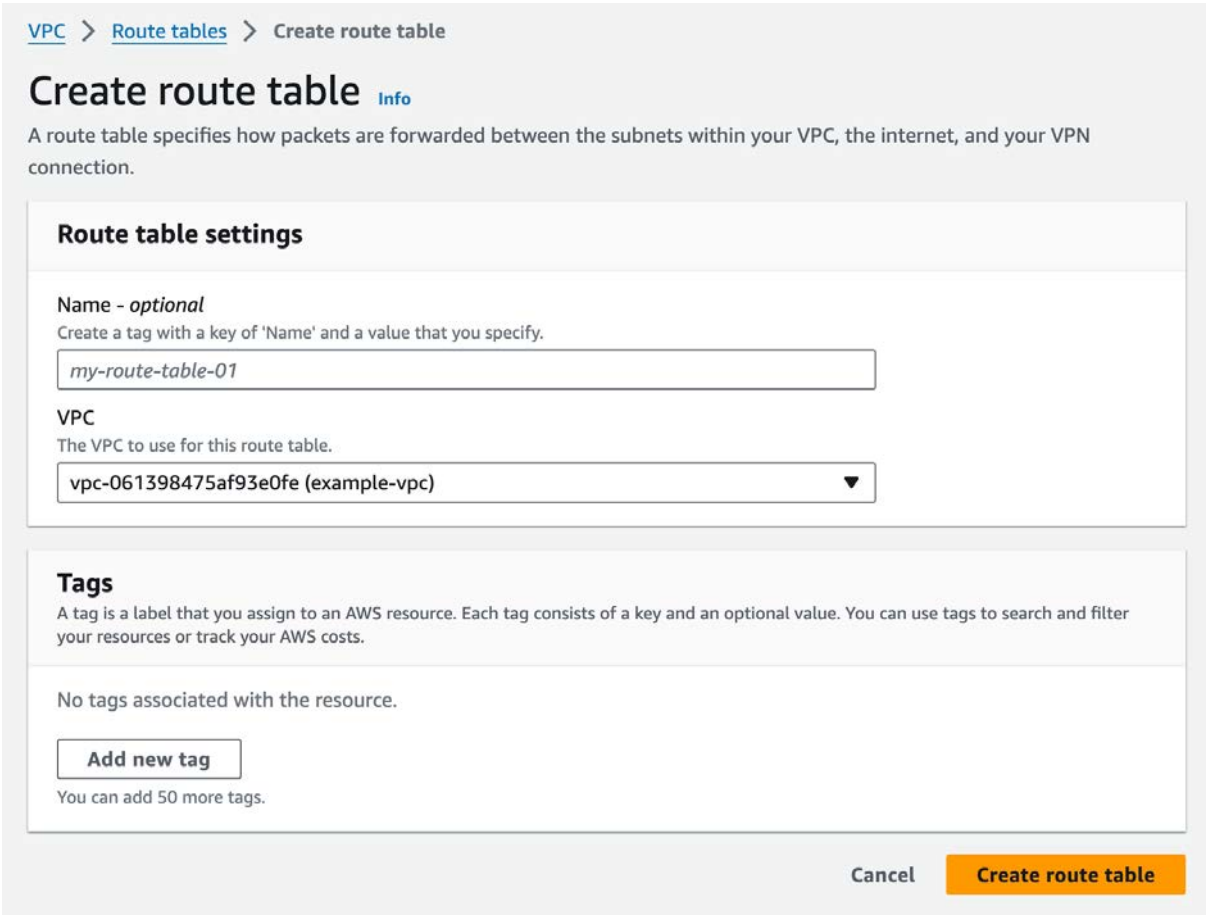
Route tables (1/2) Info
Last updated less than a minute ago
Actions
Create route table
Find resources by attribute or tag
Main : No
Clear filters
Name
Route table ID
Explicit subnet associations
route-table-public-01 rtb-05e23849b86d939a8 subnet-0134258570f74be2f / public-subnet-01
route-table-private-01 rtb-0c6bd67941c2574ef subnet-0ffabd4cf7346ab6f / private-subnet-01
rtb-05e23849b86d939a8 / route-table-public-01
Details
Routes
Subnet associations
Edge associations
Route propagation
Tags
Explicit subnet associations (1)
Edit subnet associations
Find subnet association
Name
Subnet ID
IPv4 CIDR
IPv6 CIDR
public-subnet-01 subnet-0134258570f74be2f 10.0.0.16/28 –

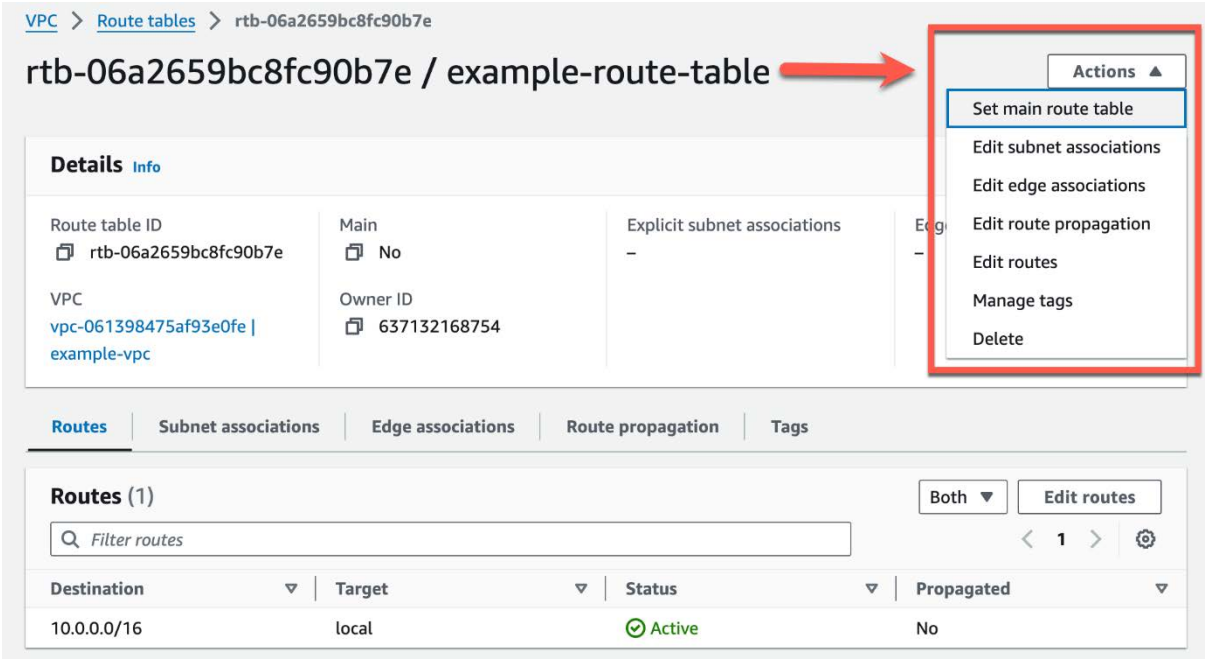

Subnets (1/2) Info
Last updated 3 minutes ago
Actions
Create subnet
Find resources by attribute or tag
Name
Subnet ID
State
VPC
public-subnet-01
subnet-0134258570f74be2f
Available
vpc-021c84d09b2b7a0d0 | vpc-...
private-subnet-01
subnet-0ffabd4cf7346ab6f
Available
vpc-021c84d09b2b7a0d0 | vpc-...
subnet-0134258570f74be2f / public-subnet-01
Details
Flow logs
Route table
Network ACL
CIDR reservations
Sharing
Tags
Route table: rtb-05e23849b86d939a8 / route-table-public-01
Edit route table association
Routes (2)
Filter routes
Destination
Target
10.0.0.0/24
local
0.0.0.0/0
igw-0a5bb00ff69314b96


rtb-05e23849b86d939a8 / route-table-public-01
Details
Routes
Subnet associations
Edge associations
Route propagation
Tags
Routes (2)
Both
Edit routes
Filter routes
Destination
Target
Status
Propagated
0.0.0.0/0
igw-0a5bb00ff69314b96
Active
No
10.0.0.0/24
local
Active
No

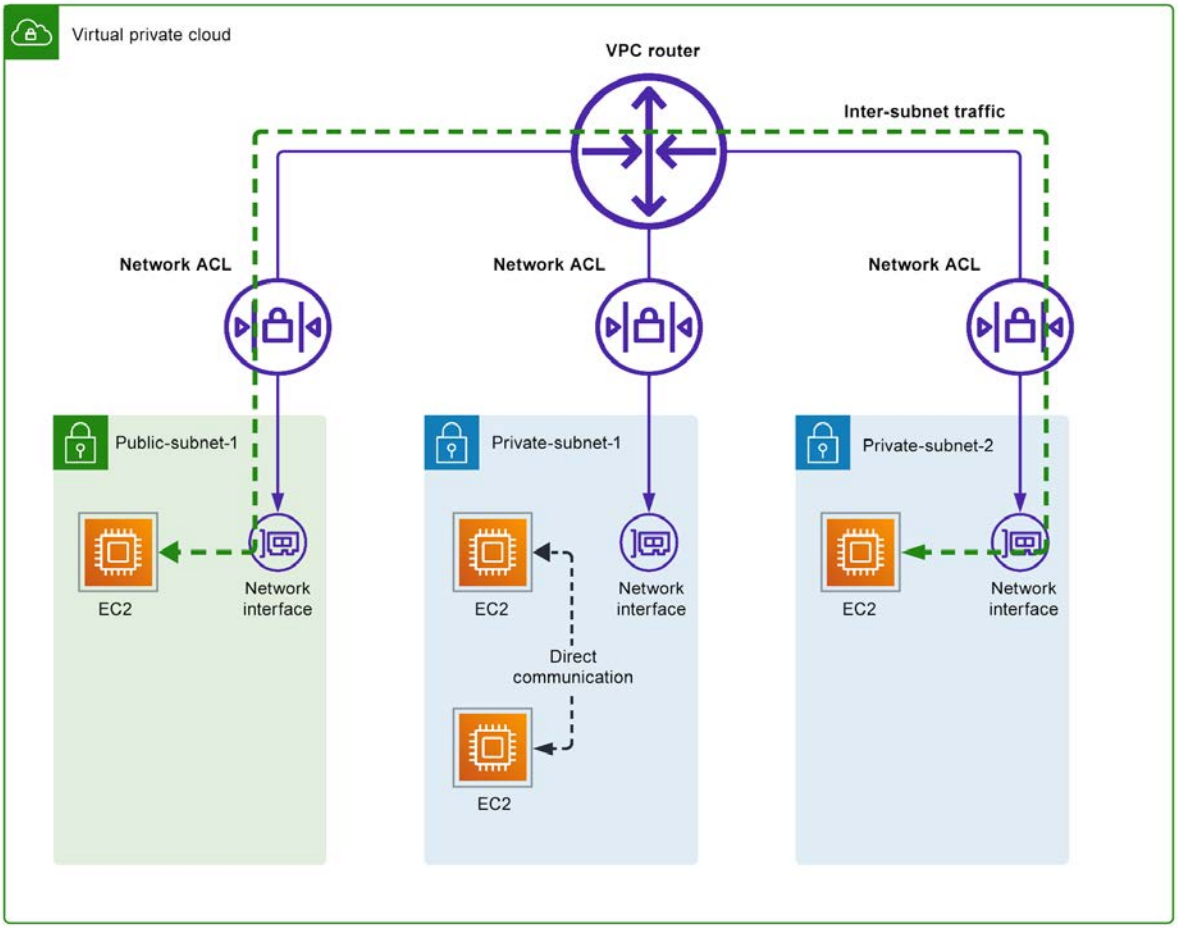

Virtual Private Cloud
10.0.0.0/16
Destination
Target
10.0.2.0/24
Network Interface 1
2
172.16.0.0
172.16.1.0
172.16.2.0
private-rt-1
VPC Router
private-subnet-1
10.0.1.0/24
private-subnet-2
10.0.2.0/24
1
3
4
5
Instance A
Network Interface 1
Inspection Instance
Network Interface 2
Instance B


VPC dashboard
EC2 Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only Internet
Route tables (1) Info
Last updated 14 minutes ago
Actions
Create route table
Find resources by attribute or tag
1
Name
Route table ID
Explicit subnet associations
Edge ass
-
rtb-009455eca80e7a9c0
-
-


VPC > Route tables > Create route table
Create route table Info
A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.
Route table settings
Name - optional
Create a tag with a key of 'Name' and a value that you specify.
my-route-table-01
VPC
The VPC to use for this route table.
vpc-061398475af93e0fe (example-vpc)
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.
No tags associated with the resource.
Add new tag
You can add 50 more tags.
Cancel
Create route table


VPC > Route tables > rtb-06a2659bc8fc90b7e
rtb-06a2659bc8fc90b7e / example-route-table
Actions
Set main route table
Edit subnet associations
Edit edge associations
Edit route propagation
Edit routes
Manage tags
Delete
Details Info
Route table ID
rtb-06a2659bc8fc90b7e
Main
No
Explicit subnet associations
–
VPC
vpc-061398475af93e0fe | example-vpc
Owner ID
637132168754
Routes
Subnet associations
Edge associations
Route propagation
Tags
Routes (1)
Both
Edit routes
Filter routes
1
Destination
Target
Status
Propagated
10.0.0.0/16
local
Active
No

Appendix 4, VPC Security and External Connectivity



acl-01e24ab98687a78c8 / test-nacl

Details | **Inbound rules** | Outbound rules | Subnet associations | Tags

Inbound rules (5)

Edit inbound rules

Filter inbound rules

1

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	HTTPS (443)	TCP (6)	443	10.10.0.0/16	Allow
150	SSH (22)	TCP (6)	22	10.0.0.0/8	Allow
200	All ICMP - IPv4	ICMP (1)	All	0.0.0.0/0	Deny
*	All traffic	All	All	0.0.0.0/0	Deny
*	All traffic	All	All	::/0	Deny

acl-01e24ab98687a78c8 / test-nacl

Details | Inbound rules | Outbound rules | Subnet associations | Tags

Outbound rules (4)

Edit outbound rules

Filter outbound rules

1

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
200	All traffic	All	All	::/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny
*	All traffic	All	All	::/0	Deny

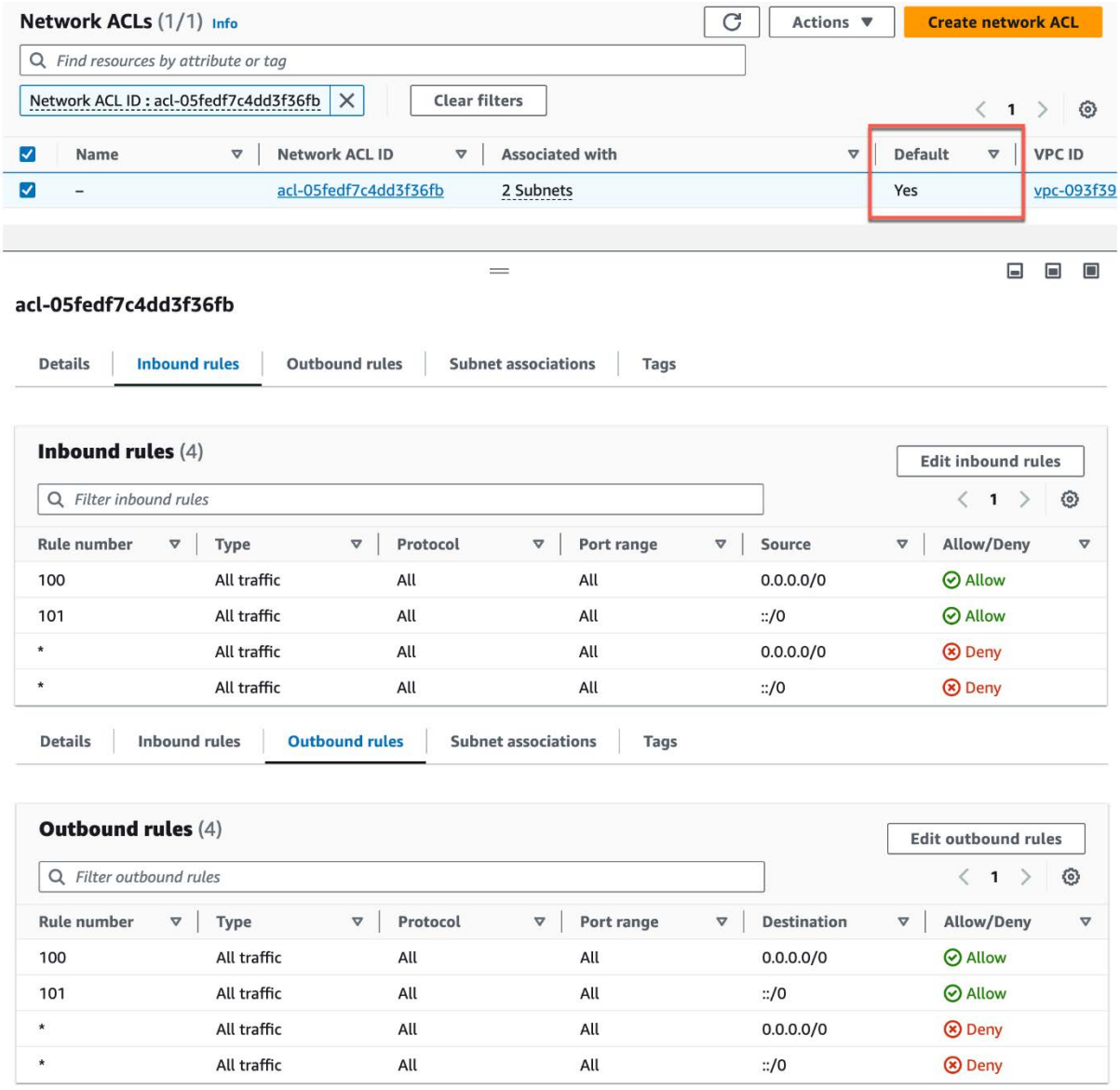
Inbound rules (7)

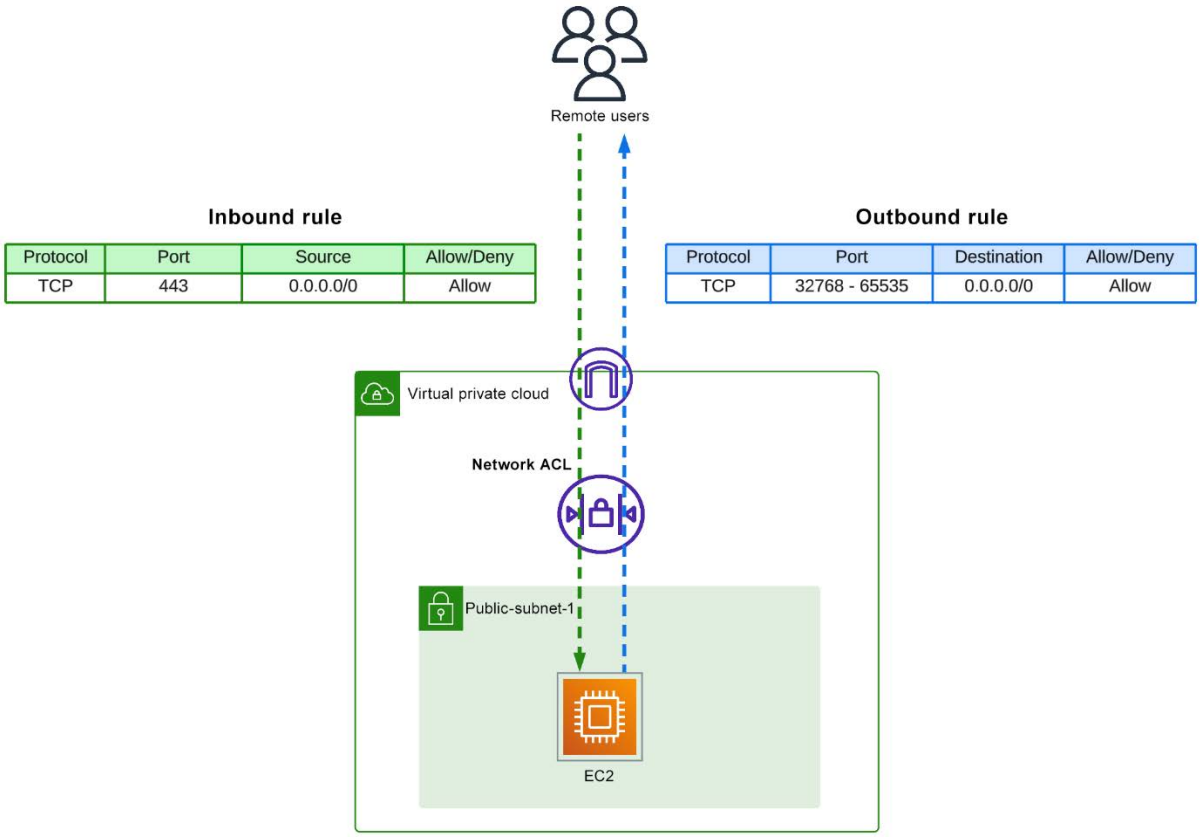
Edit inbound rules

Filter inbound rules

1

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	HTTPS (443)	TCP (6)	443	10.10.0.0/16	Allow
150	SSH (22)	TCP (6)	22	10.0.0.0/8	Allow
200	All ICMP - IPv4	ICMP (1)	All	0.0.0.0/0	Deny
3000	All traffic	All	All	0.0.0.0/0	Allow
3001	All traffic	All	All	::/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny
*	All traffic	All	All	::/0	Deny


Network ACLs (1/1) Info
Actions
Create network ACL
Find resources by attribute or tag
Network ACL ID : acl-05fedf7c4dd3f36fb
Clear filters
1
Name
Network ACL ID
Associated with
Default
VPC ID
–
acl-05fedf7c4dd3f36fb
2 Subnets
Yes
vpc-093f39
acl-05fedf7c4dd3f36fb
Details
Inbound rules
Outbound rules
Subnet associations
Tags
Inbound rules (4)
Edit inbound rules
Filter inbound rules
1
Rule number
Type
Protocol
Port range
Source
Allow/Deny
100 All traffic All All 0.0.0.0/0 Allow
101 All traffic All All ::/0 Allow
* All traffic All All 0.0.0.0/0 Deny
* All traffic All All ::/0 Deny
Details
Inbound rules
Outbound rules
Subnet associations
Tags
Outbound rules (4)
Edit outbound rules
Filter outbound rules
1
Rule number
Type
Protocol
Port range
Destination
Allow/Deny
100 All traffic All All 0.0.0.0/0 Allow
101 All traffic All All ::/0 Allow
* All traffic All All 0.0.0.0/0 Deny
* All traffic All All ::/0 Deny



Inbound rules (7)

Edit inbound rules

Filter inbound rules

1

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	HTTPS (443)	TCP (6)	443	0.0.0.0/0	Allow
110	All traffic	All	All	0.0.0.0/0	Allow
120	SSH (22)	TCP (6)	22	10.0.0.0/8	Allow
130	SSH (22)	TCP (6)	22	0.0.0.0/0	Deny
200	All ICMP - IPv4	ICMP (1)	All	0.0.0.0/0	Deny
*	All traffic	All	All	0.0.0.0/0	Deny

Inbound rules (7)

Edit inbound rules

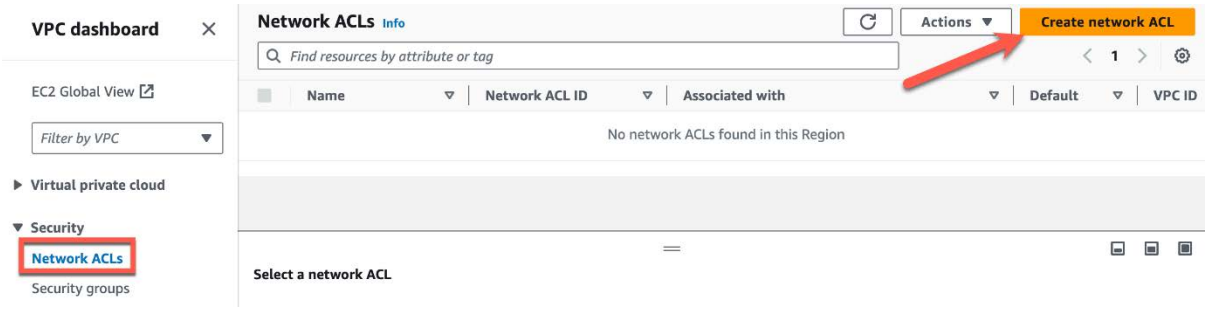
Filter inbound rules

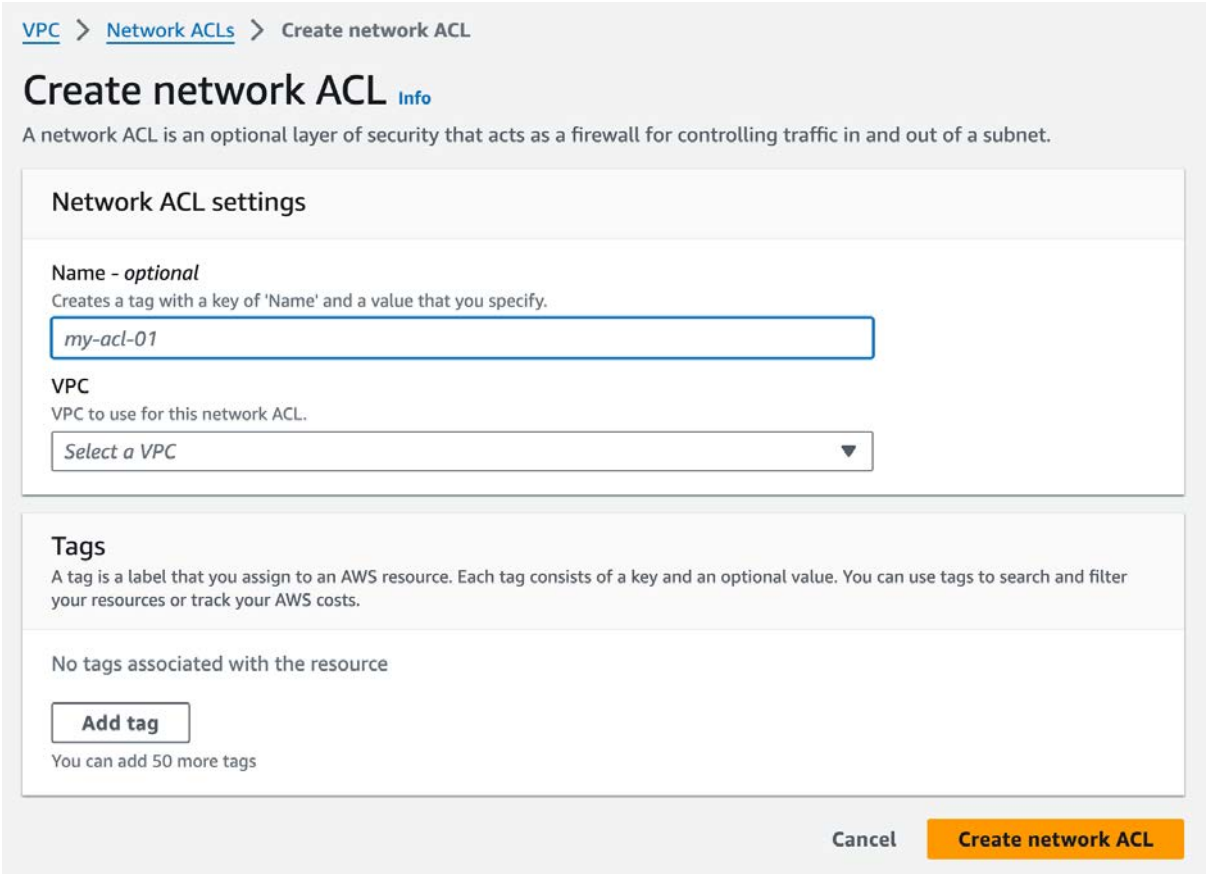
1

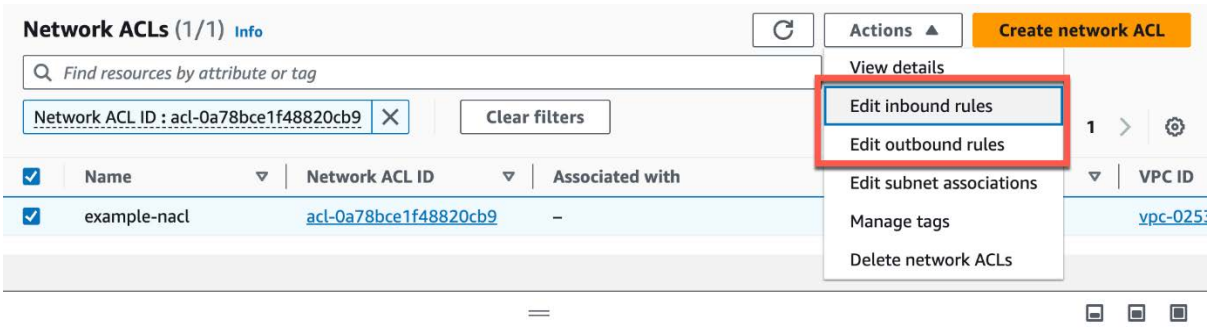
Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	HTTPS (443)	TCP (6)	443	0.0.0.0/0	Allow
110	SSH (22)	TCP (6)	22	10.0.0.0/8	Allow
120	SSH (22)	TCP (6)	22	0.0.0.0/0	Deny
130	All ICMP - IPv4	ICMP (1)	All	0.0.0.0/0	Deny
200	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny
*	All traffic	All	All	::/0	Deny

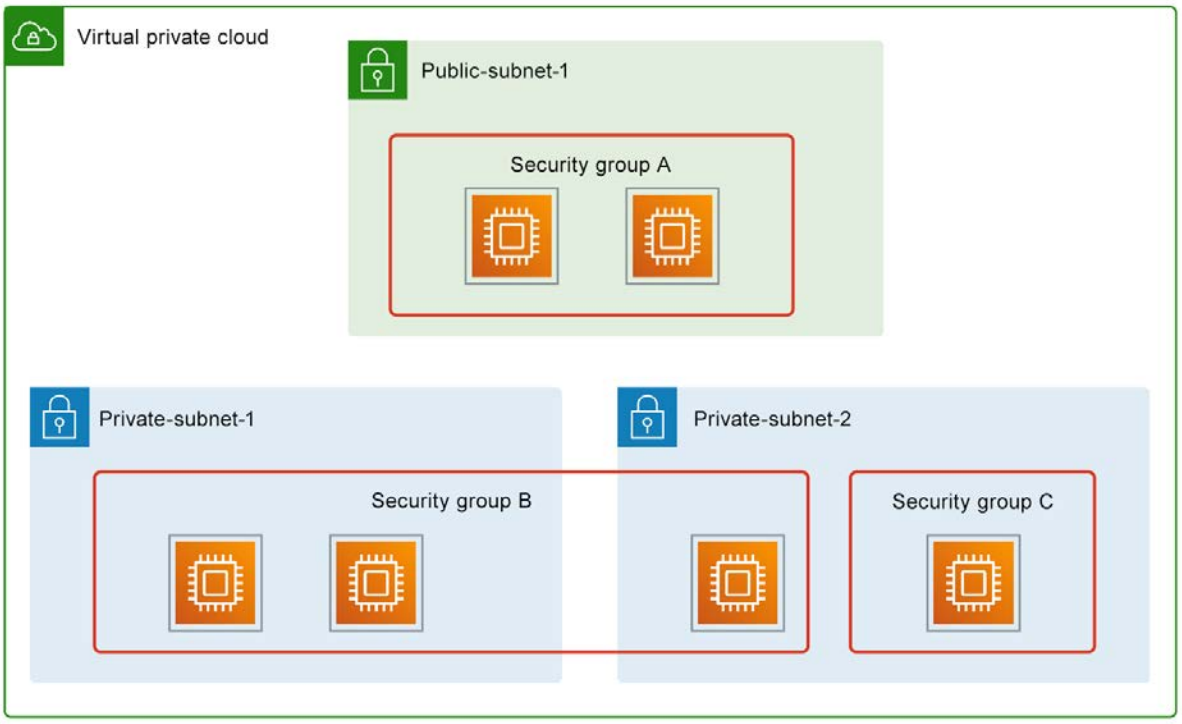
Rule number	Type	Protocol	Port range	Source	Allow/Deny
500	Custom ICMP - IPv4	ICMP (1)	Destination Unreachable	0.0.0.0/0	Allow
501	Custom ICMP - IPv6	IPv6-ICMP (58)	Destination Unreachable	::/0	Allow

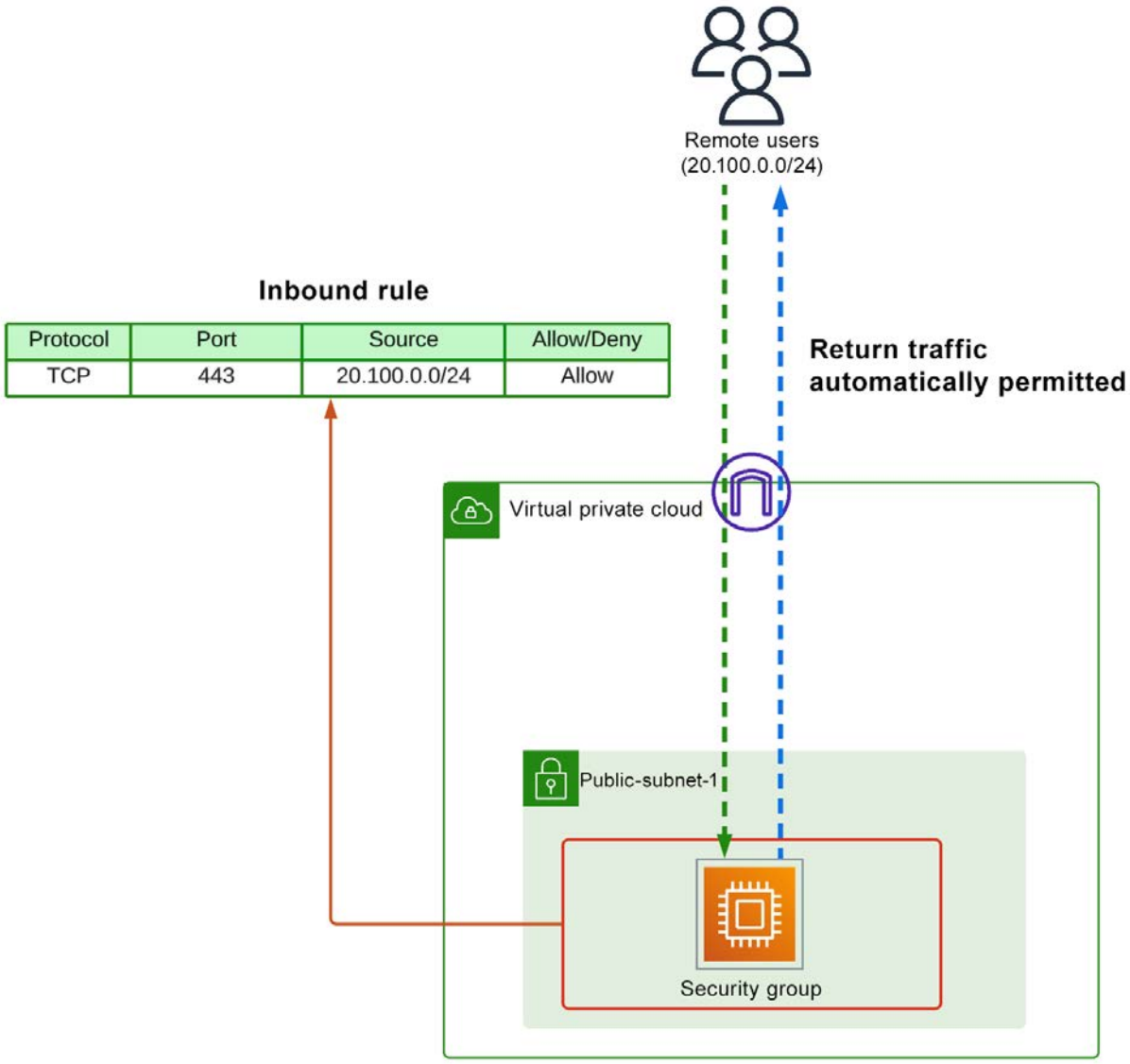
Rule number	Type	Protocol	Port range	Source	Allow/Deny
600	Custom ICMP - IPv4	ICMP (1)	Time Exceeded	0.0.0.0/0	Allow
601	Custom ICMP - IPv6	IPv6-ICMP (58)	Time Exceeded	::/0	Allow

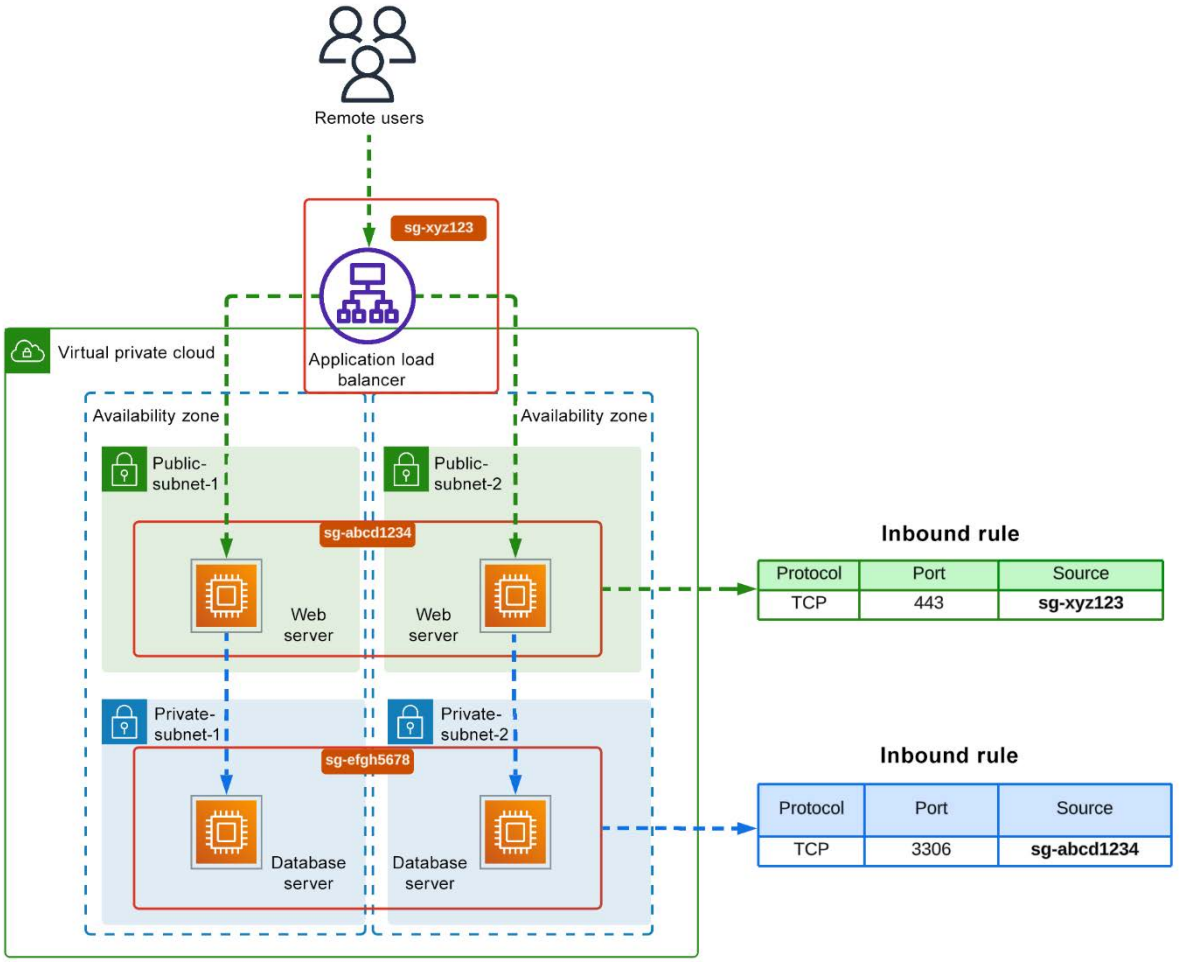


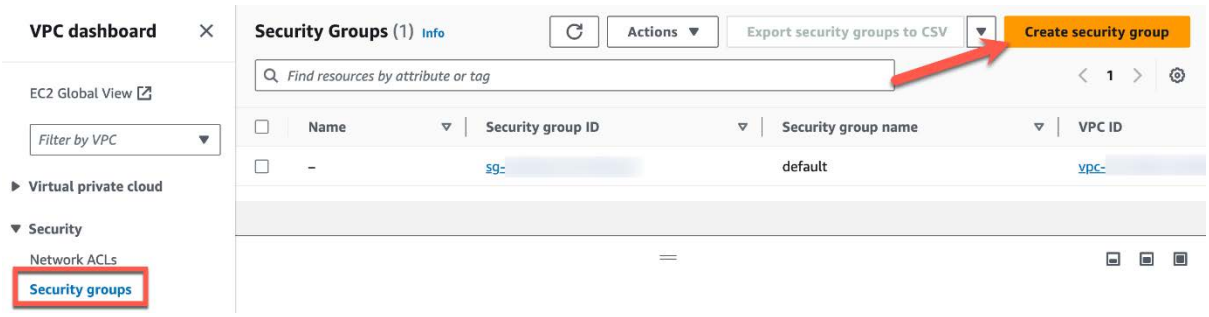





Virtual private cloud
Public-subnet-1
Security group A
Private-subnet-1
Security group B
Private-subnet-2
Security group C


Remote users
(20.100.0.0/24)
Inbound rule
Protocol
Port
Source
Allow/Deny
TCP
443
20.100.0.0/24
Allow
Return traffic
automatically permitted
Virtual private cloud
Public-subnet-1
Security group


Remote users
sg-xyz123
Application load balancer
Virtual private cloud
Availability zone
Availability zone
Public-subnet-1
Public-subnet-2
sg-abcd1234
Web server
Web server
Private-subnet-1
Private-subnet-2
sg-efgh5678
Database server
Database server
Inbound rule
Protocol
Port
Source
TCP
443
sg-xyz123
Inbound rule
Protocol
Port
Source
TCP
3306
sg-abcd1234


VPC dashboard
EC2 Global View
Filter by VPC
Virtual private cloud
Security
Network ACLs
Security groups
Security Groups (1) Info
Actions
Export security groups to CSV
Create security group
Find resources by attribute or tag
Name
Security group ID
Security group name
VPC ID
default

VPC > Security Groups > Create security group

Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name Info

MyWebServerGroup

Name cannot be edited after creation.

Description Info

Allows SSH access to developers

VPC Info

Select a VPC

Inbound rules Info

Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
Custom TCP	TCP	0	Cus...			Delete

Add rule

Outbound rules Info

Type Info	Protocol Info	Port range Info	Destination Info		Description - optional Info	
Custom TCP	TCP	0	Cus...			Delete

Add rule

Tags - *optional*

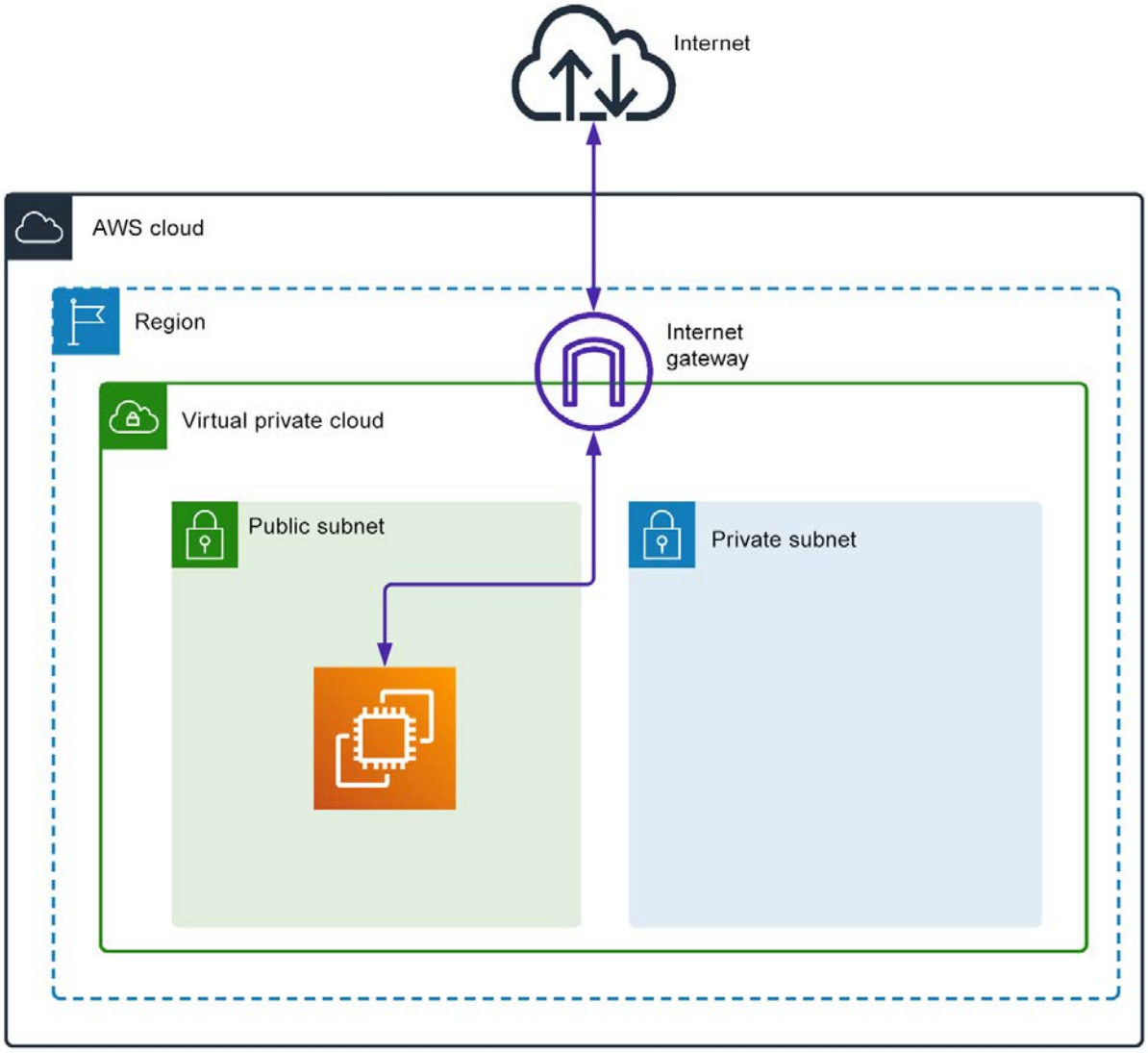
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags

Cancel Create security group



VPC > Subnets > subnet- > Edit subnet settings

Edit subnet settings Info

Subnet

Subnet ID
subnet-

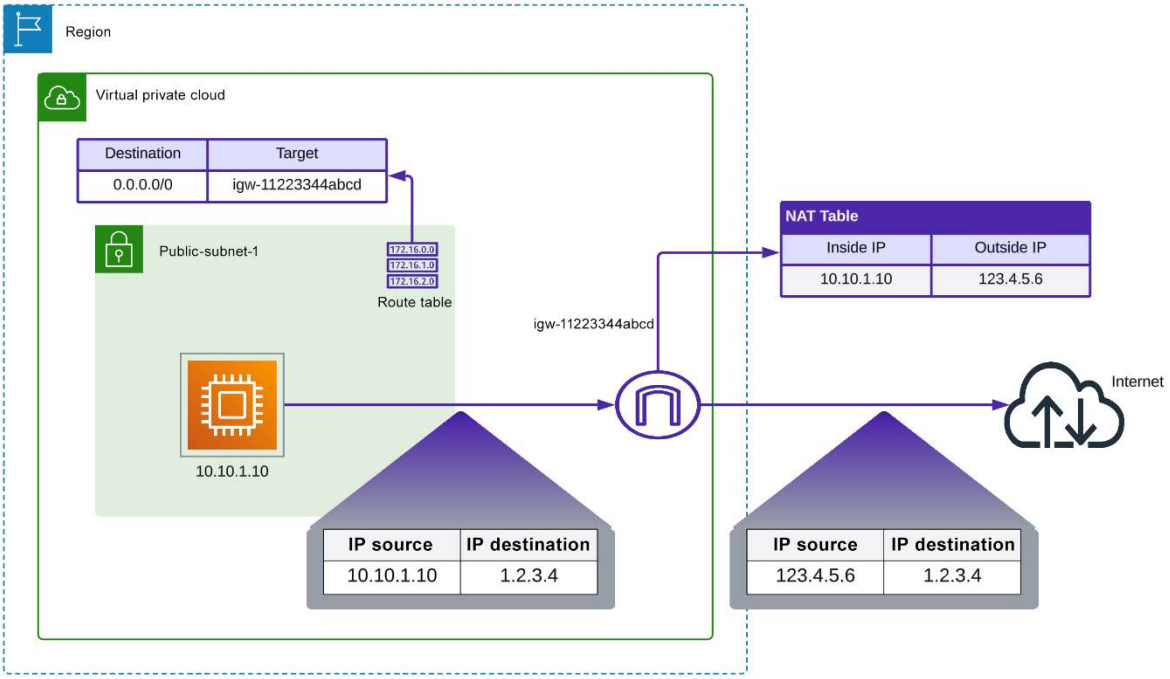
Name
public-subnet-01

Auto-assign IP settings Info

Enable AWS to automatically assign a public IPv4 or IPv6 address to a new primary network interface for an instance in this subnet.

☐ Enable auto-assign public IPv4 address Info

☐ Enable auto-assign customer-owned IPv4 address Info
Option disabled because no customer owned pools found.


Region
Virtual private cloud
Destination
Target
0.0.0.0/0
igw-11223344abcd
Public-subnet-1
172.16.0.0
172.16.1.0
172.16.2.0
Route table
NAT Table
Inside IP
Outside IP
10.10.1.10
123.4.5.6
igw-11223344abcd
Internet
10.10.1.10
IP source
IP destination
10.10.1.10
1.2.3.4
IP source
IP destination
123.4.5.6
1.2.3.4


VPC dashboard
EC2 Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only Internet gateways
DHCP option sets
Internet gateways Info
Actions
Create internet gateway
Search
Name
Internet gateway ID
State
VPC ID
No internet gateways found in this Region
Select an internet gateway above


VPC > Internet gateways > igw-05356846932392927
igw-05356846932392927 / example-internet-gateway
Actions
Attach to VPC
Detach from VPC
Manage tags
Delete
Details Info
Internet gateway ID
igw-05356846932392927
State
Detached
VPC ID
–
Owner
Tags
Manage tags
Search tags
Key
Value
Name
example-internet-gateway


VPC > Internet gateways > Attach to VPC (igw-05356846932392927)
Attach to VPC (igw-05356846932392927) Info
VPC
Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.
Available VPCs
Attach the internet gateway to this VPC.
Select a VPC
AWS Command Line Interface command
Cancel
Attach internet gateway


VPC dashboard
EC2 Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only Internet gateways
DHCP option sets
Egress only internet gateways Info
Actions
Create egress only internet gateway
Find resources by attribute or tag
1
Name
Egress only internet gateway ID
Attached VPC ID
No egress only internet gateway found

VPC > Egress only internet gateways > Create egress only internet gateway

Create egress only internet gateway Info

An Internet Gateway is a virtual router that connects a VPC to the internet.

Egress only internet gateway settings

Name - *optional*

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

example-eigw

VPC

Attach the egress only internet gateway to this VPC.

vpc-061398475af93e0fe (example-vpc)

Tags

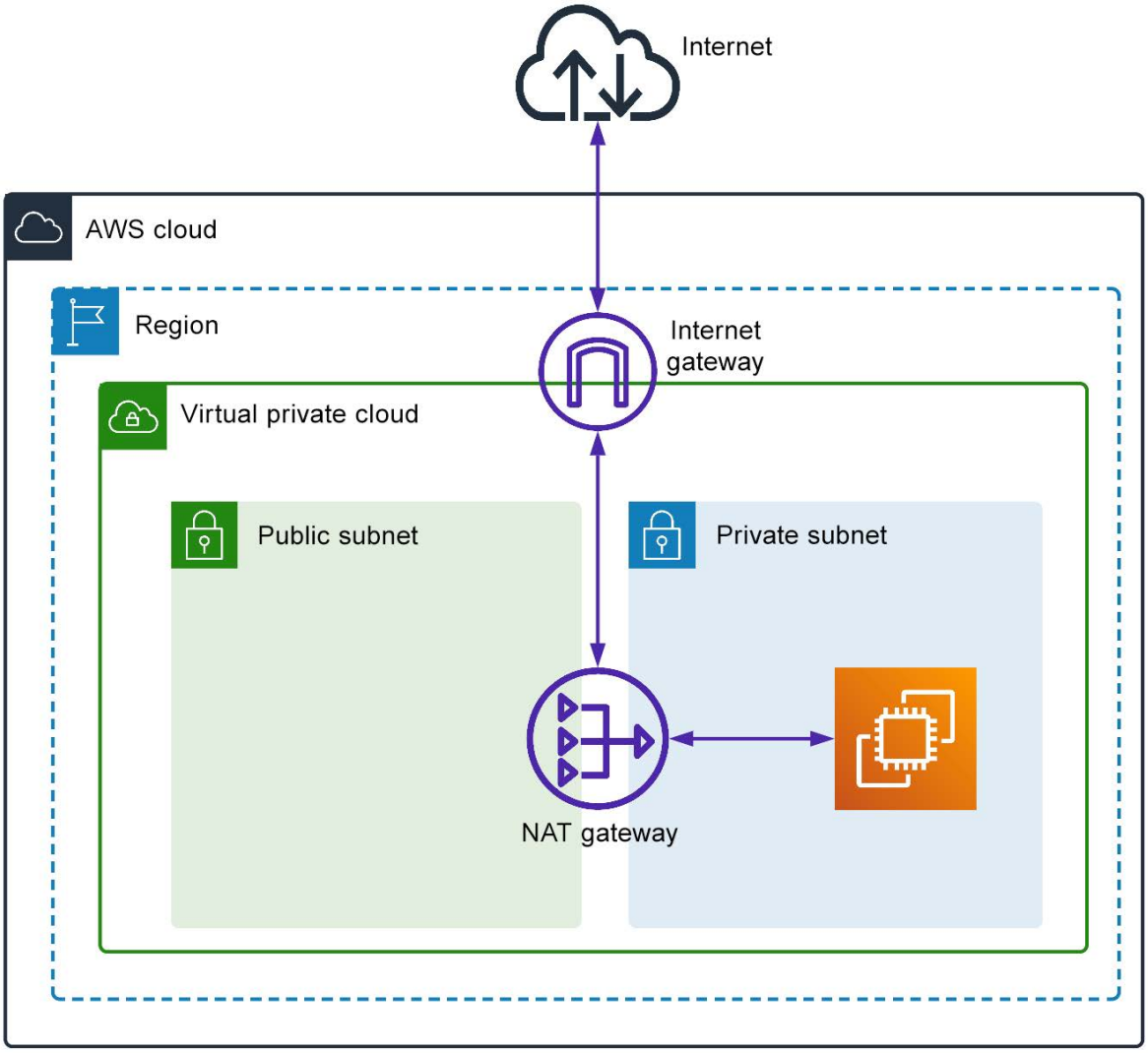
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

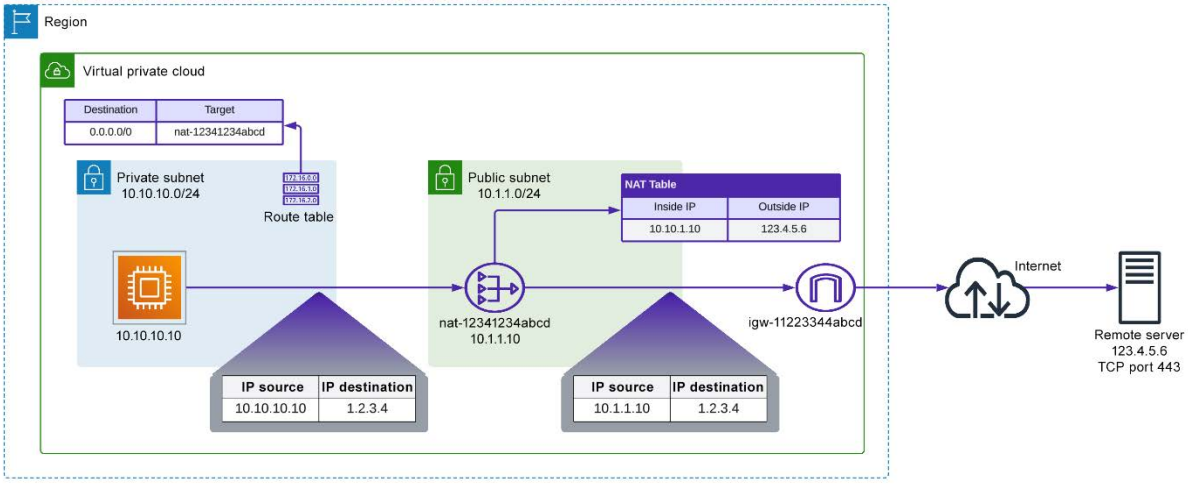
Key	Value - *optional*	
Name	example-eigw	Remove

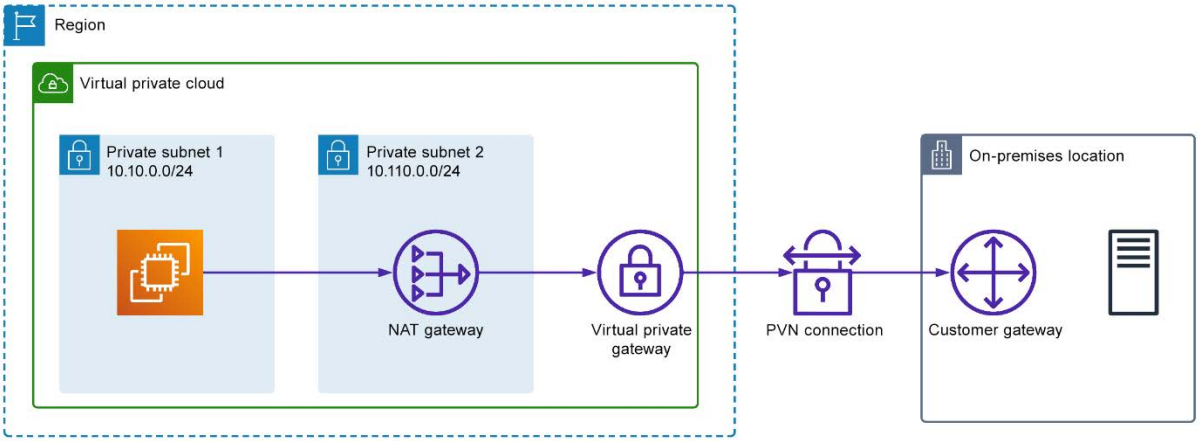
Add new tag

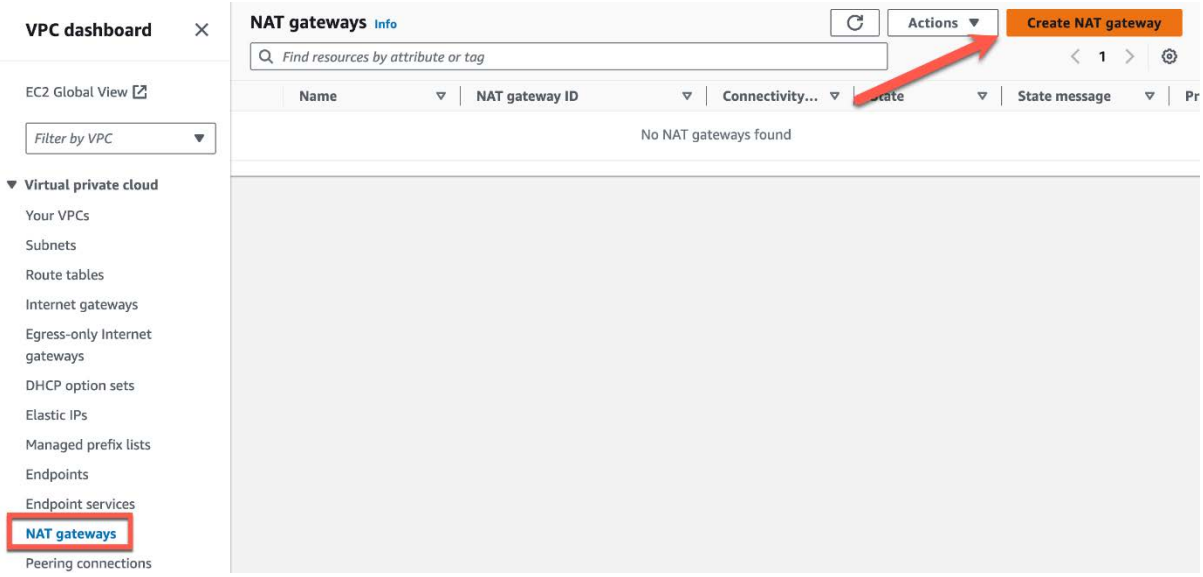
You can add 49 more tags.

Cancel | Create egress only internet gateway


Internet
AWS cloud
Region
Internet gateway
Virtual private cloud
Public subnet
Private subnet
NAT gateway


Region
Virtual private cloud
Destination
Target
0.0.0.0/0
nat-12341234abcd
Private subnet
10.10.10.0/24
Route table
Public subnet
10.1.1.0/24
NAT Table
Inside IP
Outside IP
10.10.1.10
123.4.5.6
10.10.10.10
nat-12341234abcd
10.1.1.10
igw-11223344abcd
Internet
Remote server
123.4.5.6
TCP port 443
IP source
IP destination
10.10.10.10
1.2.3.4
IP source
IP destination
10.1.1.10
1.2.3.4


Region
Virtual private cloud
Private subnet 1
10.10.0.0/24
Private subnet 2
10.110.0.0/24
NAT gateway
Virtual private gateway
PVN connection
On-premises location
Customer gateway


VPC dashboard
EC2 Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only Internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
NAT gateways Info
Actions
Create NAT gateway
Find resources by attribute or tag
Name
NAT gateway ID
Connectivity...
State message
No NAT gateways found

VPC > NAT gateways > Create NAT gateway

Create NAT gateway Info

A highly available, managed Network Address Translation (NAT) service that instances in private subnets can use to connect to services in other VPCs, on-premises networks, or the internet.

NAT gateway settings

Name - *optional*

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

my-nat-gateway-01

The name can be up to 256 characters long.

Subnet

Select a subnet in which to create the NAT gateway.

Select a subnet

Connectivity type

Select a connectivity type for the NAT gateway.

- (•) Public
- ( ) Private

Elastic IP allocation ID Info

Assign an Elastic IP address to the NAT gateway.

Select an Elastic IP | Allocate Elastic IP

Select a subnet to display the allocation IDs.

▼ Additional settings Info

Primary private IPv4 address - *optional*

10.0.0.10

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.

No tags associated with the resource.

Add new tag

You can add 50 more tags.

Cancel | Create NAT gateway