

## Preface:

The screenshot shows the 'Practice Resources' interface for the book 'AWS Certified Advanced Networking - Specialty (ANS-C01) Certification Guide'. At the top, there's a dark header bar with the 'Practice Resources' logo and a 'SHARE FEEDBACK' button. Below the header is a 'DASHBOARD' section featuring the book's cover image and title. Underneath are four expandable sections: 'Mock Exams', 'Chapter Review Questions', 'Flashcards', and 'Exam Tips'. At the bottom left, there's a 'BACK TO THE BOOK' link.

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 McConaughy, Steve McNutt, Christopher Miles

## Chapter 1: Advanced VPC Networking

Practice Resources

DASHBOARD

AWS Certified Advanced Networking – Specialty (ANS-C01) Certification Guide  
A pragmatic guide to acing the AWS ANS-C01 exam

Mock Exams

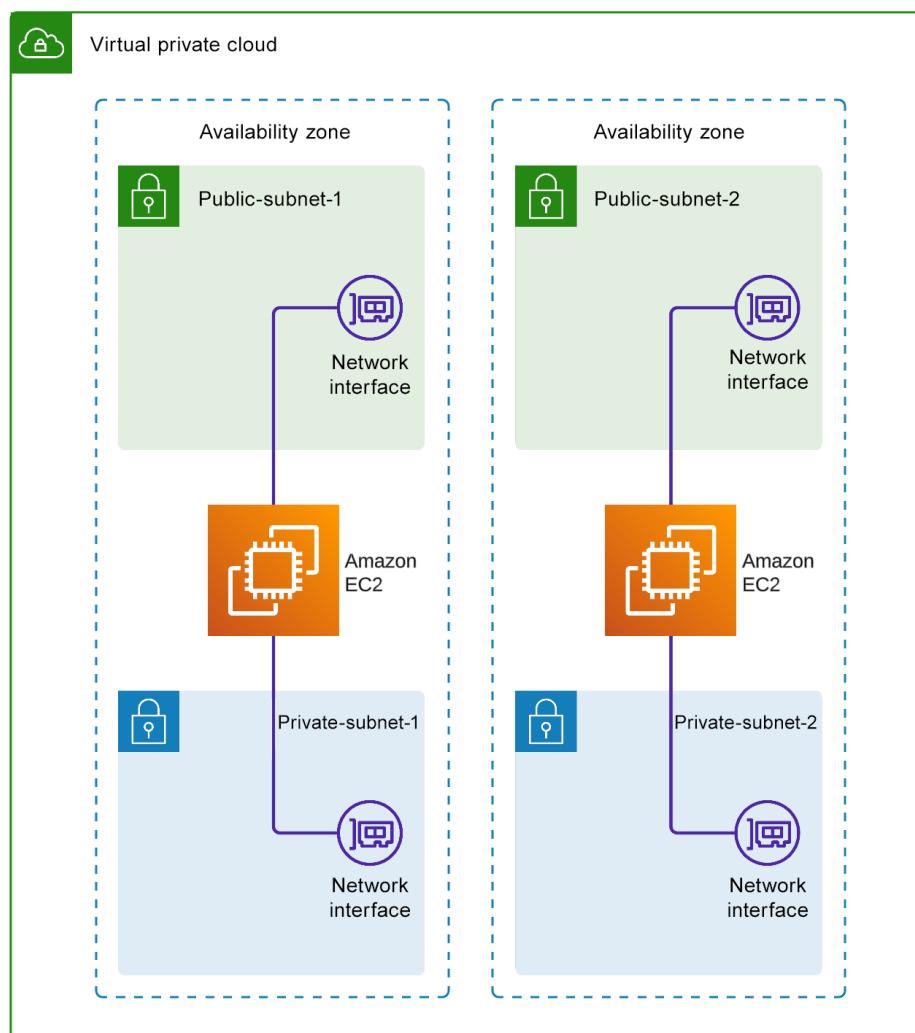
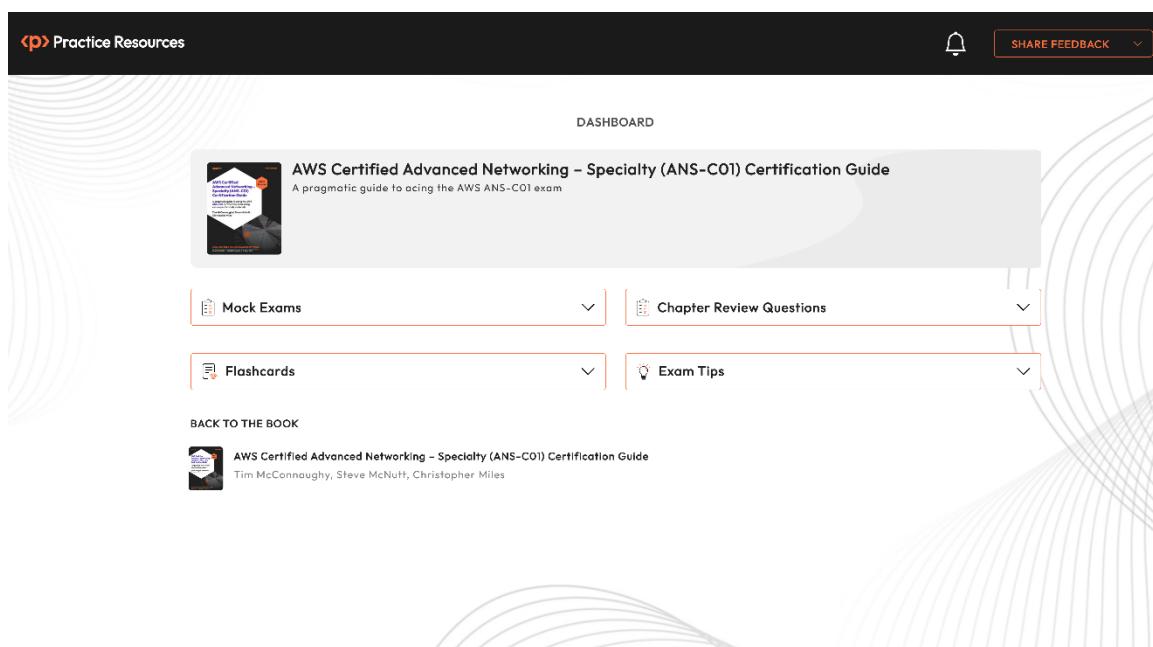
Chapter Review Questions

Flashcards

Exam Tips

BACK TO THE BOOK

AWS Certified Advanced Networking – Specialty (ANS-C01) Certification Guide  
Tim McConaughy, Steve McNutt, Christopher Miles



## 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 X

Network interface  
eni-0507d1d9e8f7288a3

Delete on instance termination

- Enable

[Cancel](#)

[Save](#)

## Change source/destination check X

Network interface  
eni-0507d1d9e8f7288a3

Source/destination check

- Enable

[Cancel](#)

[Save](#)

## 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.

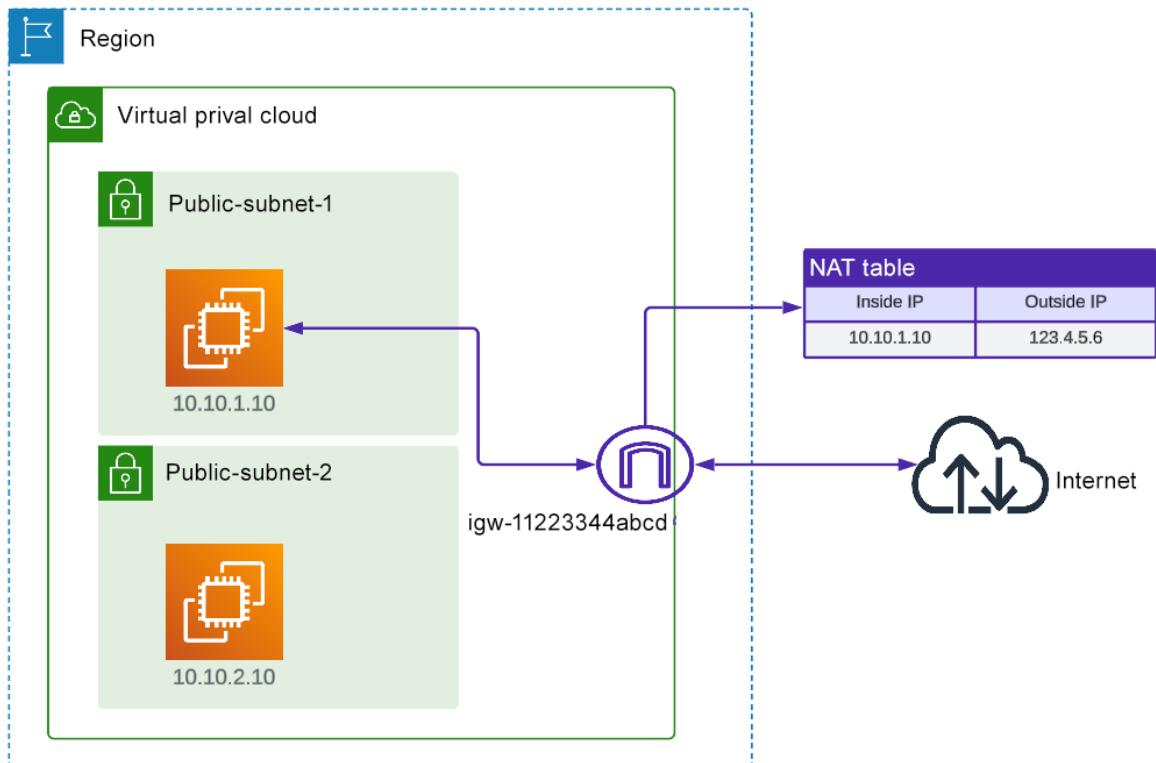
No tags associated with the resource.

[Add new tag](#)

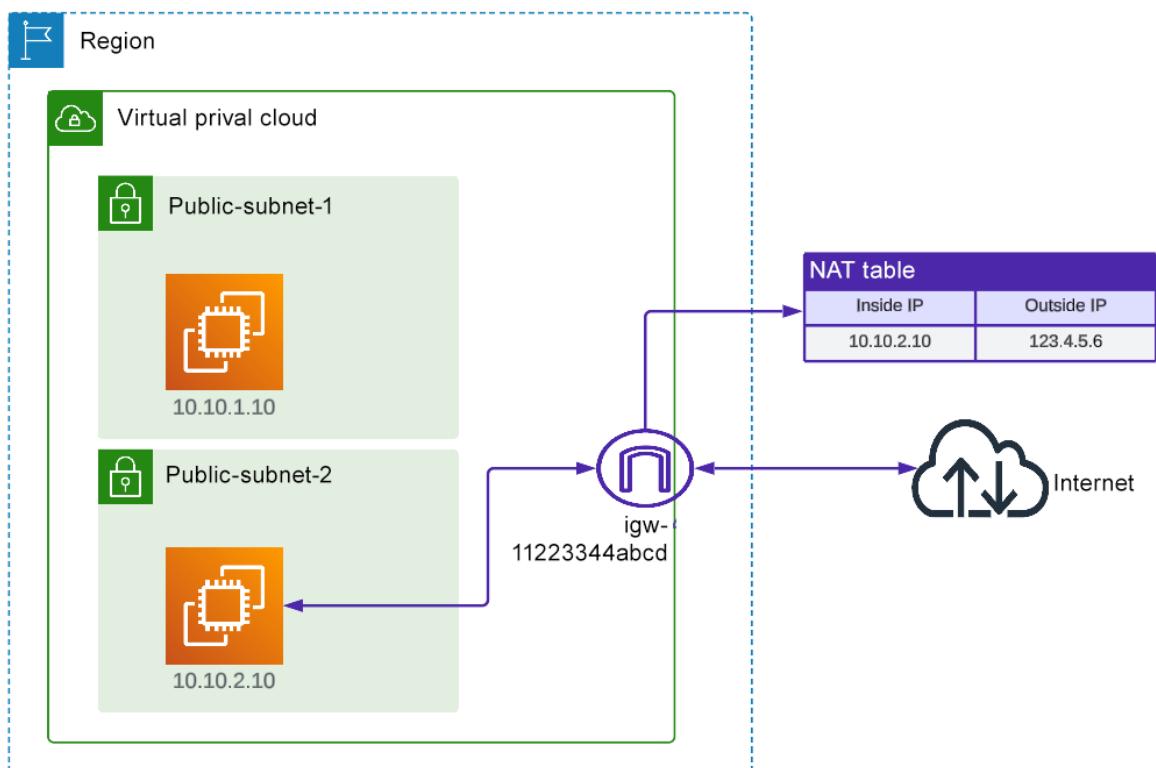
You can add 50 more tags

[Cancel](#)

[Create network interface](#)



Reassociate EIP



## 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



#### 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](#)

### Elastic IP addresses (1/1)


[Actions ▾](#)
[Allocate Elastic IP address](#)
[View details](#)
[Release Elastic IP addresses](#)
1
2


Name



Allocated IPv4 addr...



Type

-

Public IP

[Associate Elastic IP address](#)
[Disassociate Elastic IP address](#)
[Update reverse DNS](#)
[Enable transfers](#)
[Disable transfers](#)
[Accept transfers](#)

**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 Cancel Associate

Private IP address  
The private IP address with which to associate the Elastic IP address.

Choose a private IP address Cancel

Reassociation  
Specify whether the Elastic IP address can be reassigned with a different resource if it already associated with a resource.

Allow this Elastic IP address to be reassigned

**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.

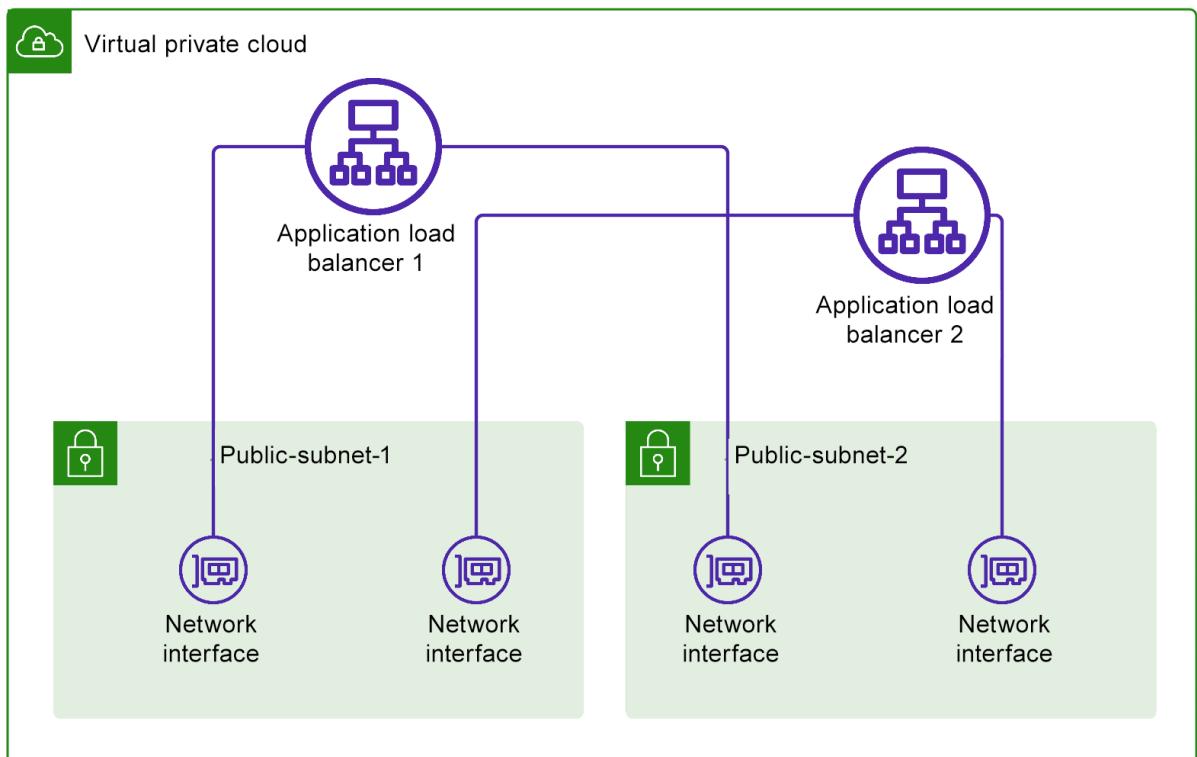
Network interface  Choose a network interface Cancel Associate

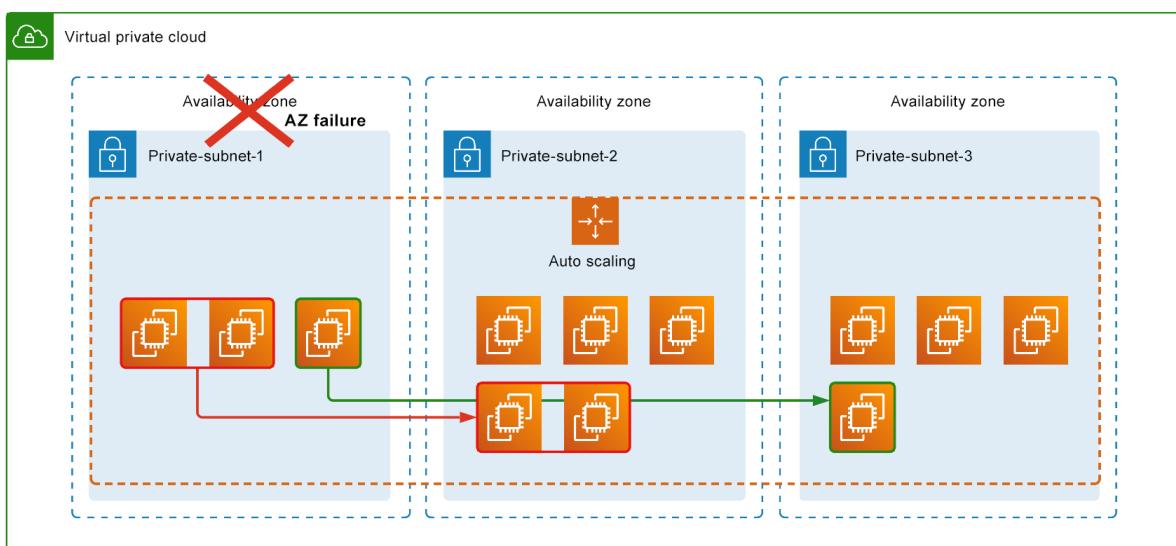
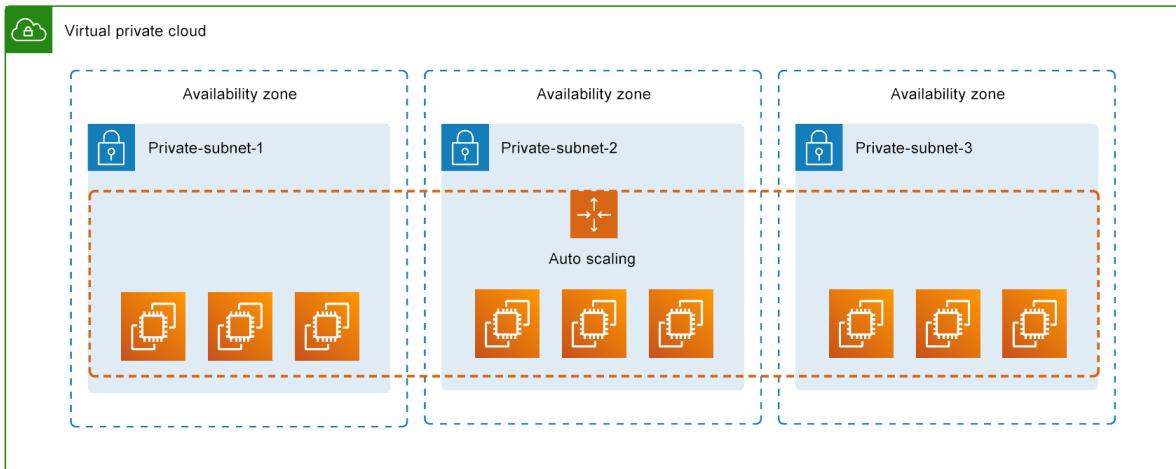
Private IP address  
The private IP address with which to associate the Elastic IP address.

Choose a private IP address Cancel

Reassociation  
Specify whether the Elastic IP address can be reassigned with a different resource if it already associated with a resource.

Allow this Elastic IP address to be reassigned





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

pl-0bc6cf55bd965fb83 - test-pl				
Details	Entries	Associations	Sharing	Tags
<strong>Prefix list entries (3)</strong>				
<input type="text"/> Find entries				
CIDR	Description			
10.0.0.0/24				
10.140.0.0/24				
10.2.0.0/24				

## 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.

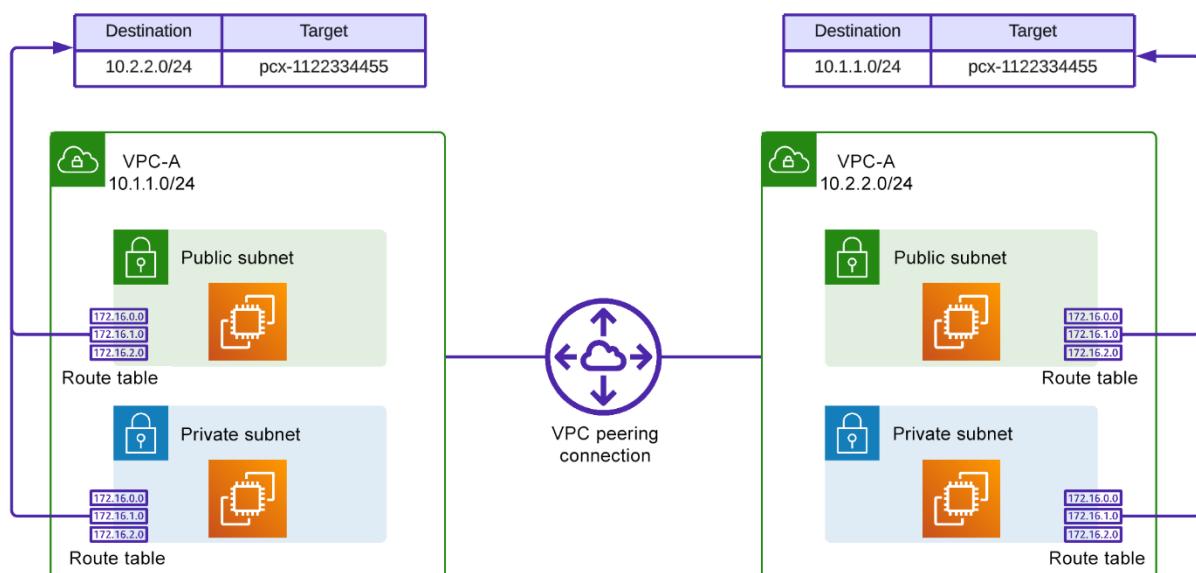
No tags associated with the resource.

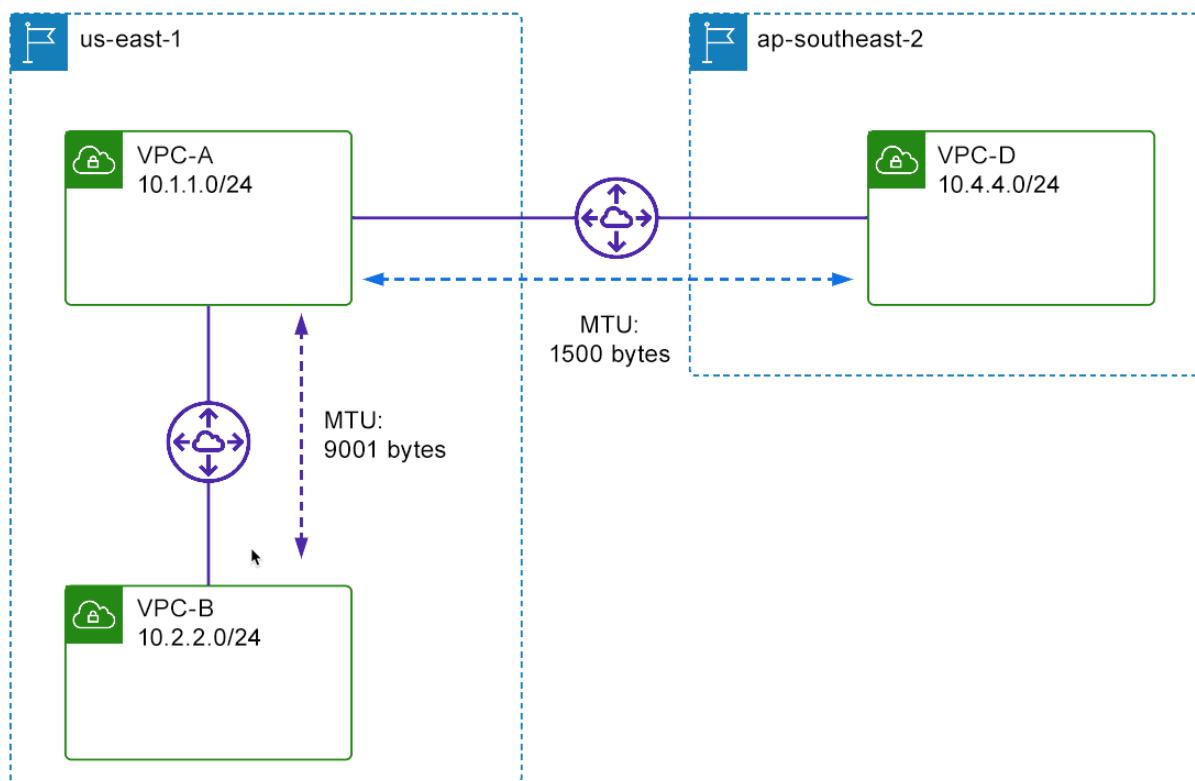
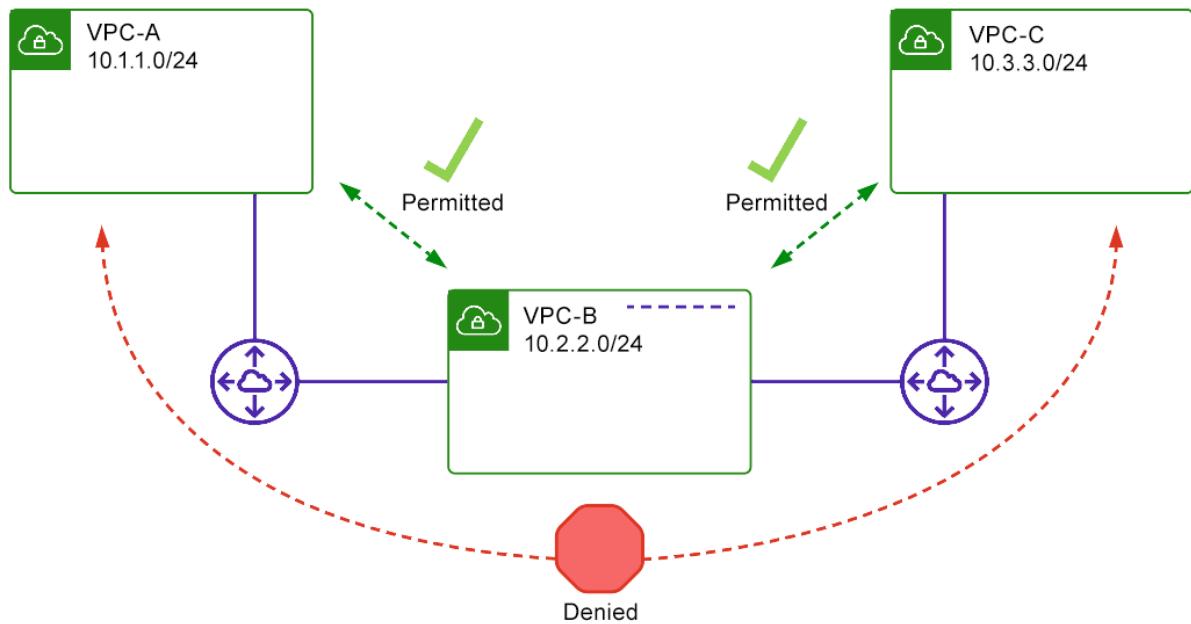
[Add new tag](#)

You can add 50 more tags.

[Cancel](#)

[Create prefix list](#)





## 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 (Acceptor)

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](#)

Find resources by attribute or tag

Peering connection ID : [pcx-0dd6b0c9c972f694d](#) [X](#) [Clear filters](#)

Name	Peering connection ID	Status	Requester VPC	Actions
test-vpc-peering	<a href="#">pcx-0dd6b0c9c972f694d</a>	Pending acceptance	<a href="#">vpc-00e9ff2528611bc47 / vpc-a</a>	<a href="#">View details</a> <a href="#">Accept request</a> <a href="#">Reject request</a> <a href="#">Edit DNS settings</a> <a href="#">Manage tags</a> <a href="#">Delete peering connection</a>

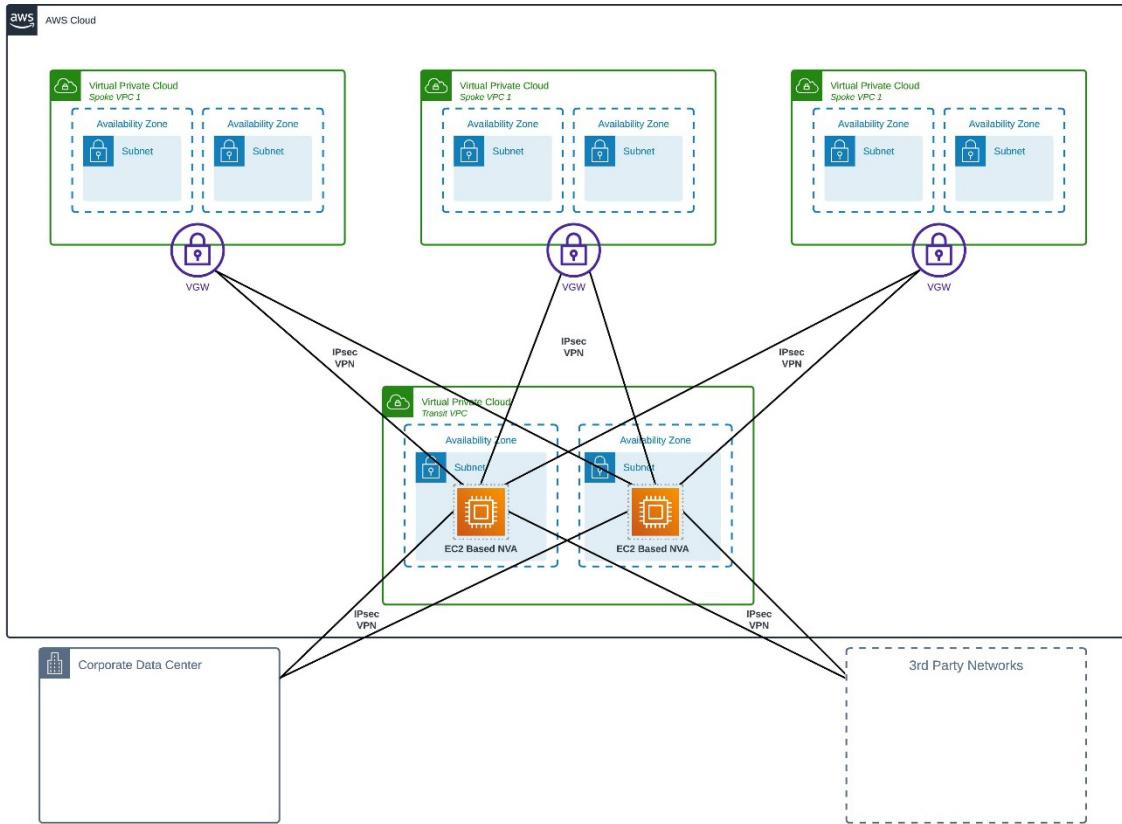
Peering connections (1/1) [Info](#)

Find resources by attribute or tag

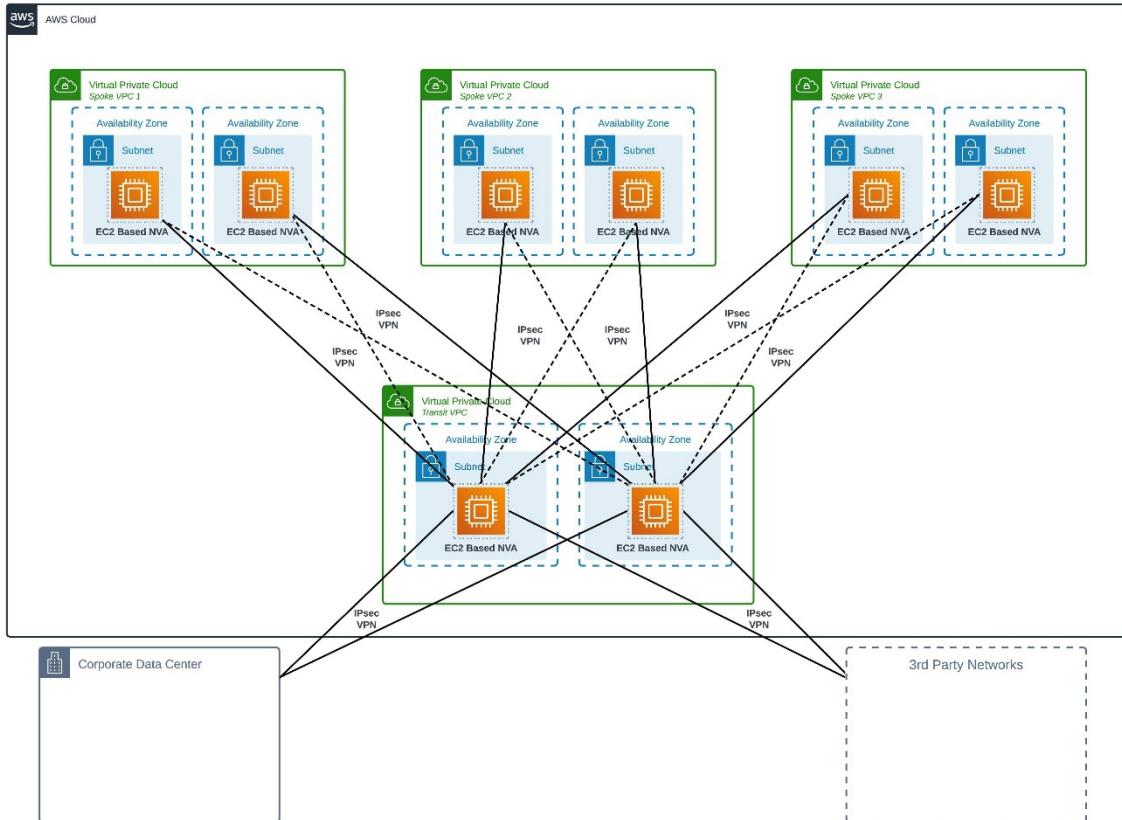
Peering connection ID : [pcx-0dd6b0c9c972f694d](#) [X](#) [Clear filters](#)

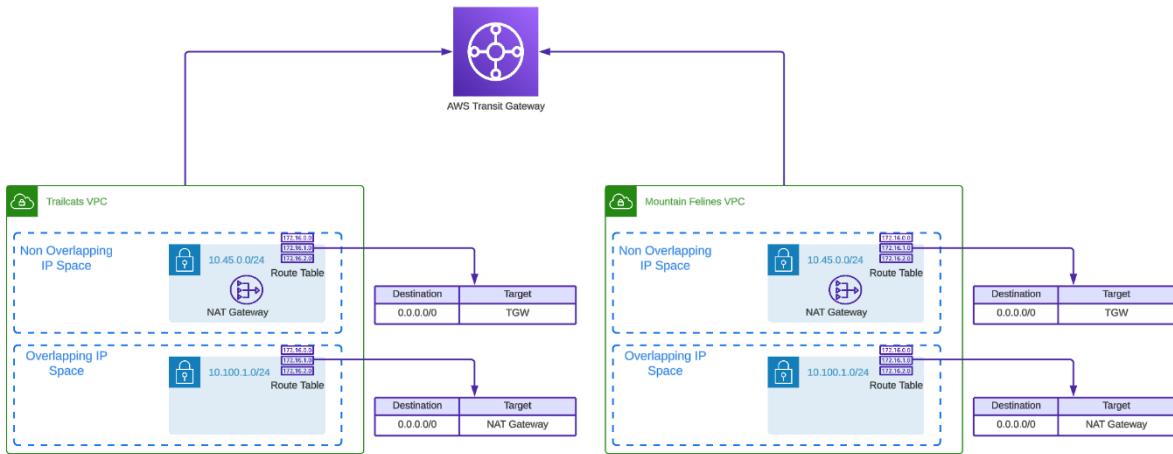
Name	Peering connection ID	Status	Actions
test-vpc-peering	<a href="#">pcx-0dd6b0c9c972f694d</a>	Pending acceptance	<a href="#">View details</a> <a href="#">Accept request</a> <a href="#">Reject request</a> <a href="#">Edit DNS settings</a> <a href="#">Manage tags</a> <a href="#">Delete peering connection</a>

## Option 1:



## Option 2:





## Chapter 2: VPC Traffic and Performance Monitoring

**AWS Network Manager**

**Sites (7)**

ID	Name	Description
site-001a9a1383496a3e5	HQ	New York Headquarters
site-059123f8bb1ab3ef7	APJ Office	Sydney Office
site-0643f6885082c3ea3	China Office	Hong Kong

**AWS Network Manager**

**Dashboard**

**CloudWatch**

**Log group details**

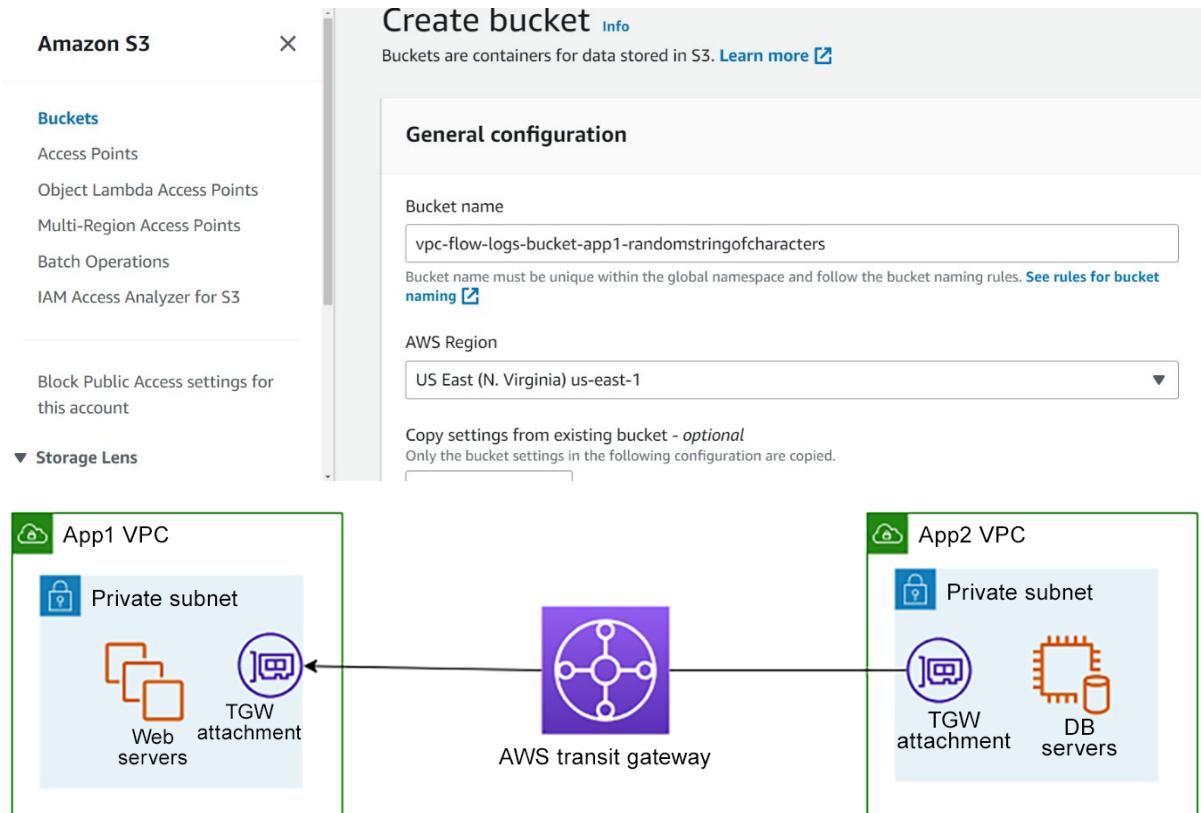
Log group name: vpc-flow-logs

Retention setting: 1 month (30 days)

KMS key ARN - optional:

**Tags**

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



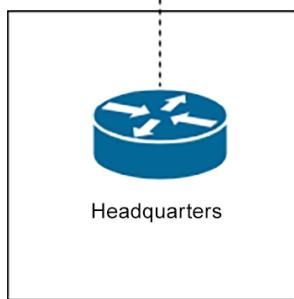
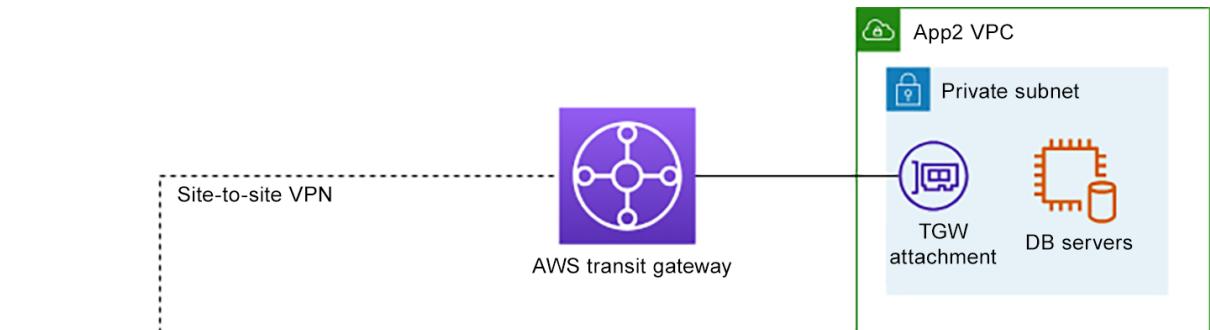
### Log events

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
<input type="text"/> 10.200.2.12 <input type="button" value="X"/>	Clear 1m 30m 1h 12h Custom <input type="button" value=""/>	Display <input type="button" value=""/>

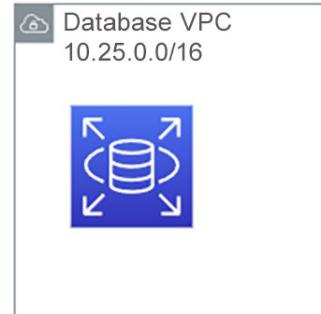
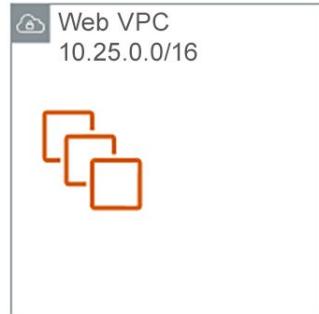
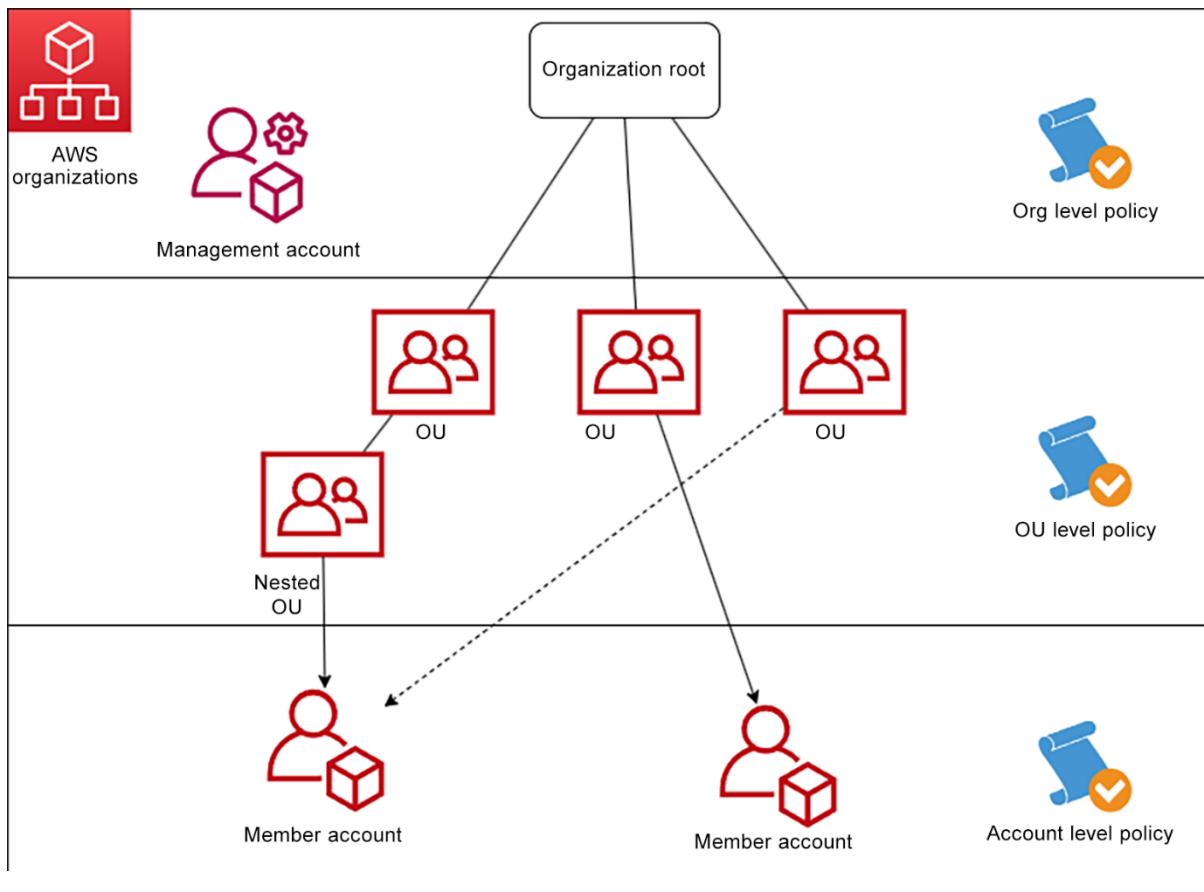
Timestamp	Message
2023-08-05T13:36:29.000-04:00	2 [REDACTED] eni-068b5ed779598f382 10.200.1.36 10.200.2....
2 [REDACTED]	eni-068b5ed779598f382 10.200.1.36 10.200.2.12 0 0 1 55 4620 1691256989 1691257049 REJECT OK
2023-08-05T13:37:30.000-04:00	2 [REDACTED] eni-068b5ed779598f382 10.200.1.36 10.200.2....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

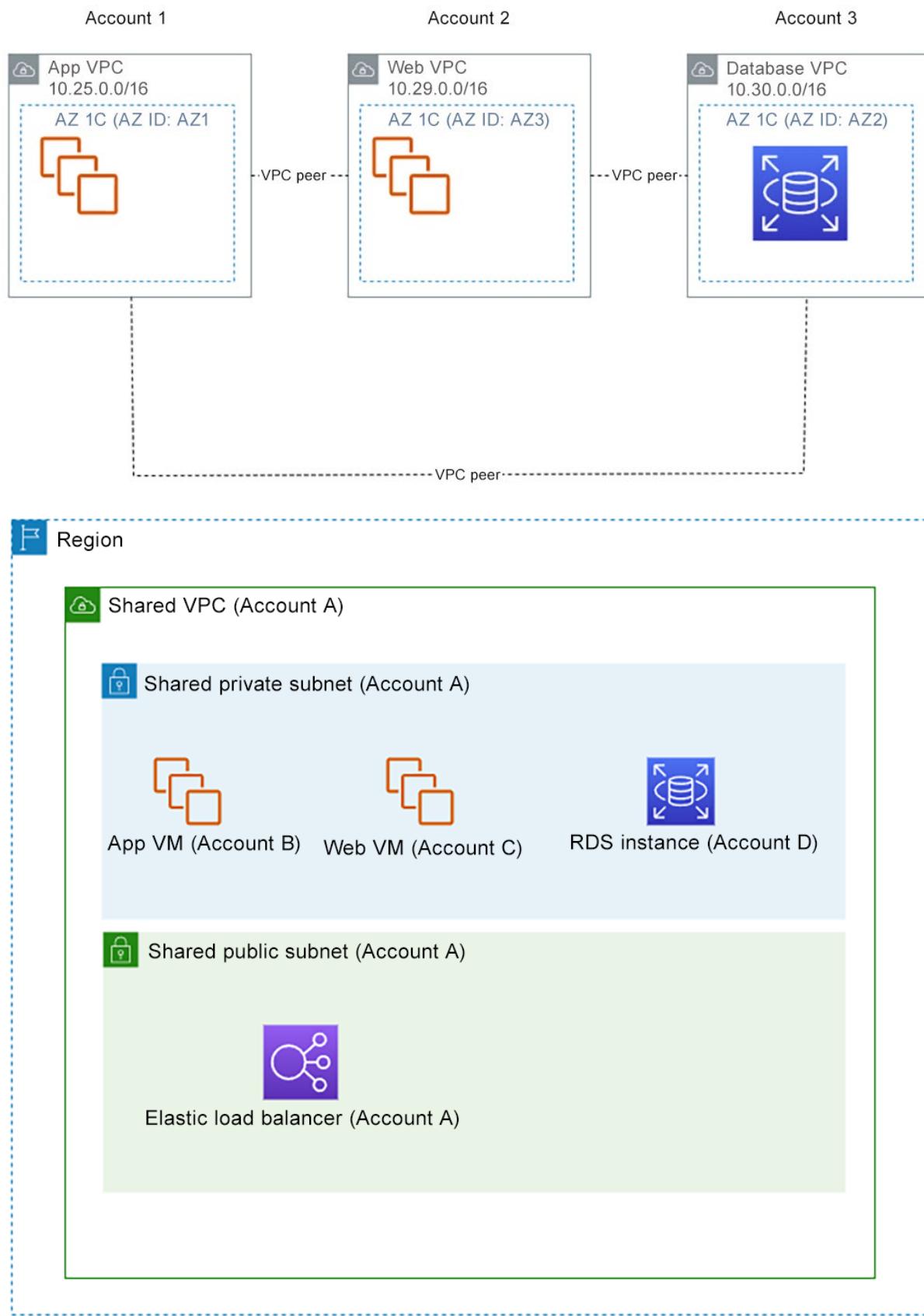
Network ACLs (1/7) <a href="#">Info</a>		
<a href="#">Actions</a>		
<a href="#">Find resources by attribute or tag</a>		
Name	Network ACL ID	Associated with
<b>Outbound rules (3)</b> <a href="#">Edit outbound rules</a>		
<a href="#">Filter outbound rules</a>		
Port range	Destination	Allow/Deny
All	10.200.2.12/32	Deny
All	0.0.0.0/0	Allow
All	0.0.0.0/0	Deny

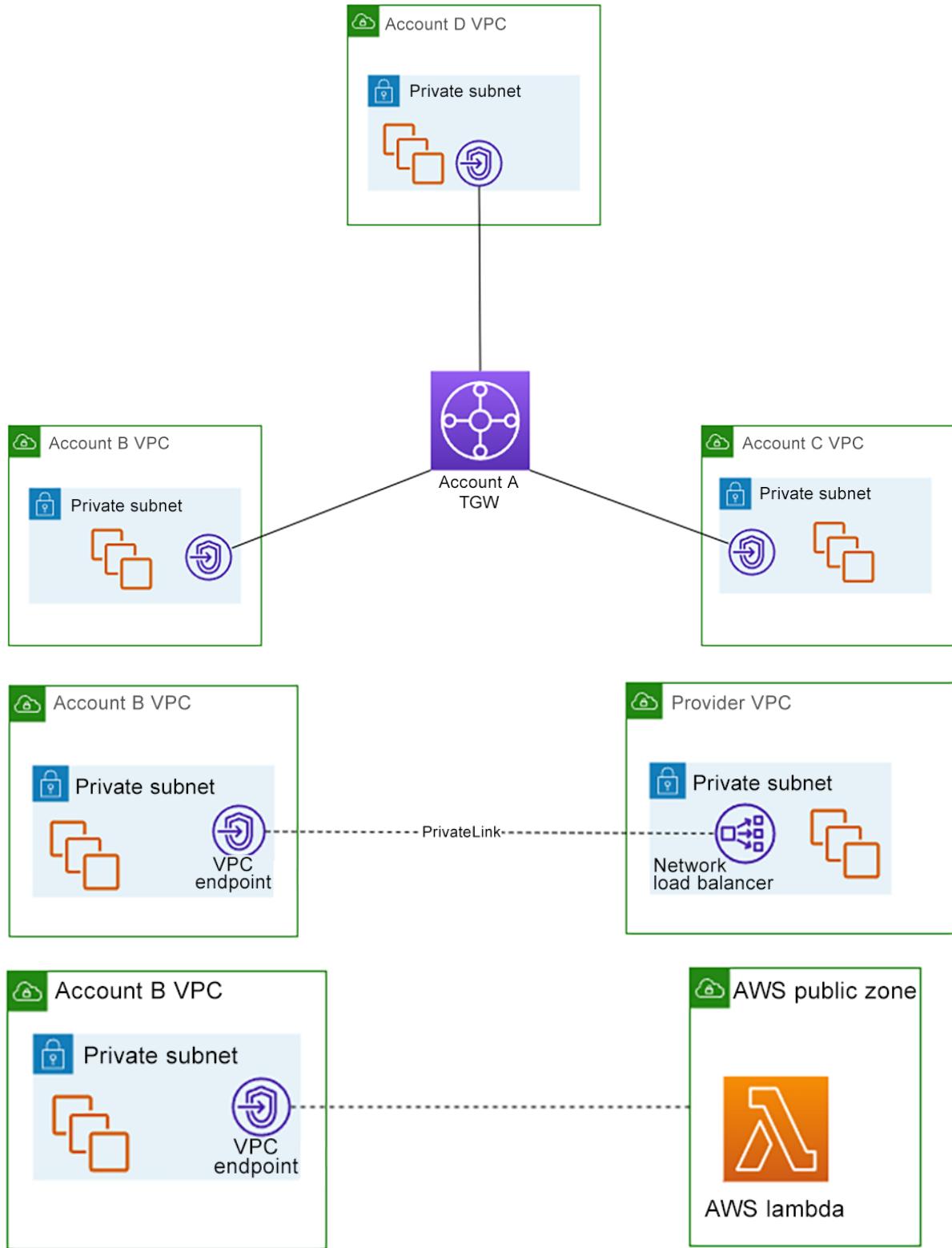


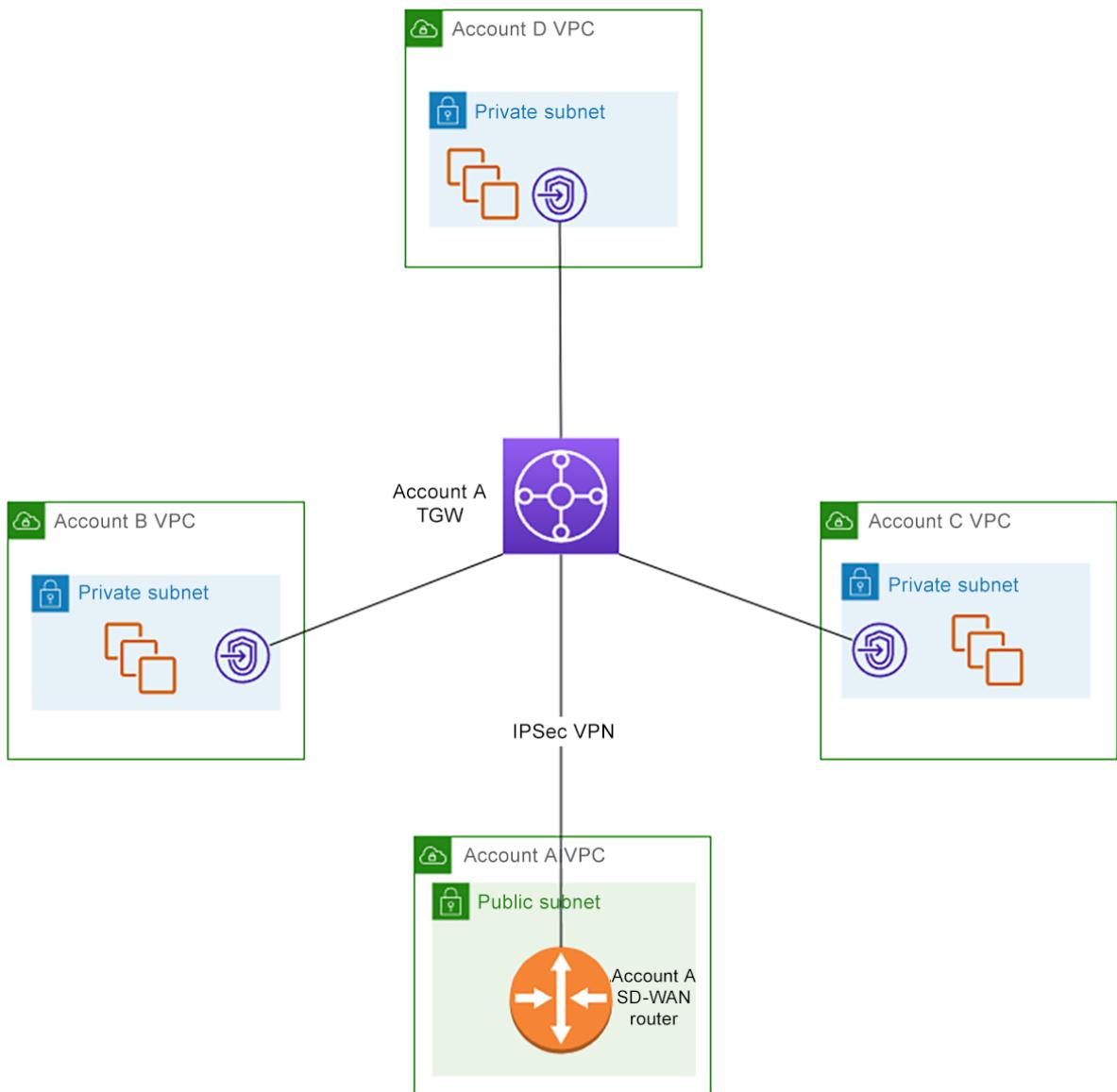
Outside IP Header (Public) 20 bytes	ESP Header 8 bytes	Original IP Header (Private) 20 bytes	Original Payload (variable)	ESP Trailer (variable, usually around 20-22)
---	-----------------------	---	--------------------------------	--

## Chapter 3: Networking Across Multiple AWS Accounts

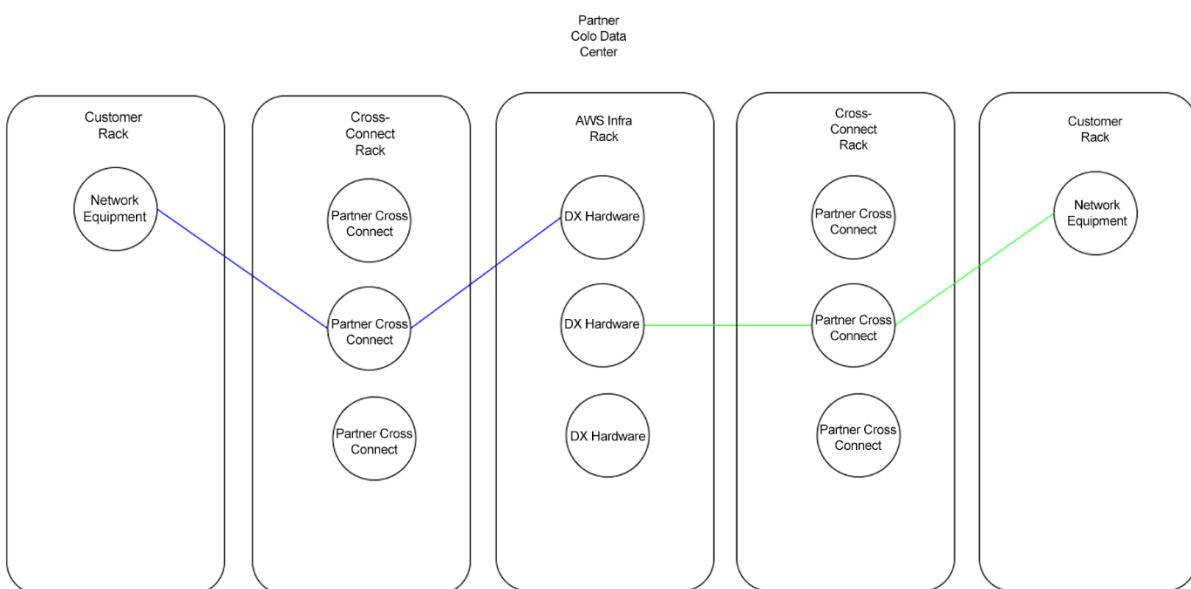
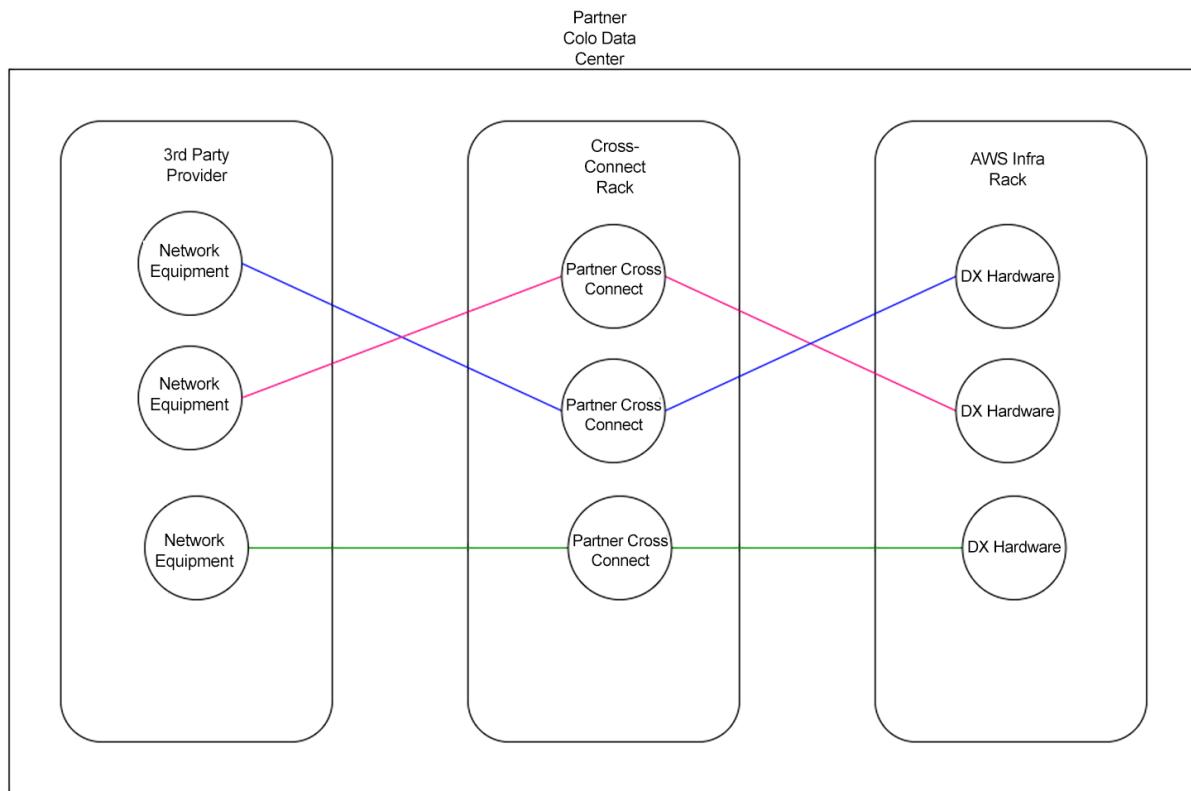


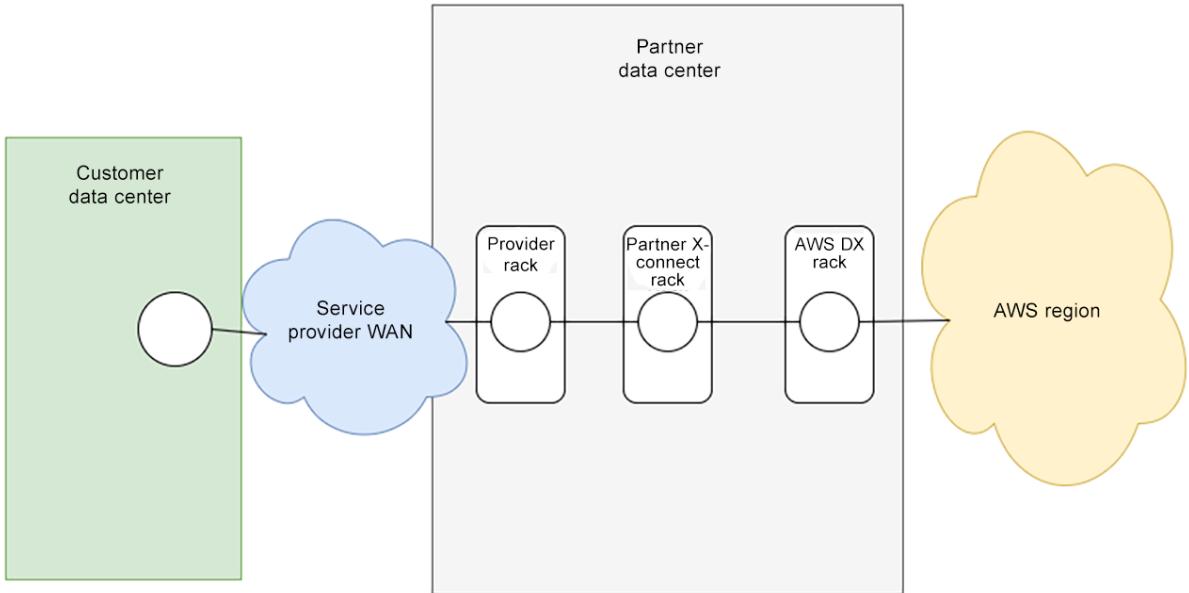




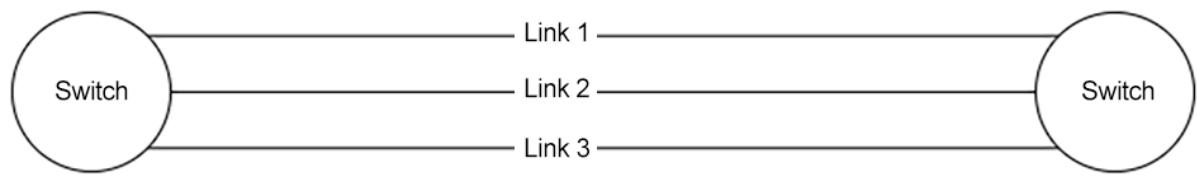


## Chapter 4: AWS Direct Connect





Physical  
Cabling

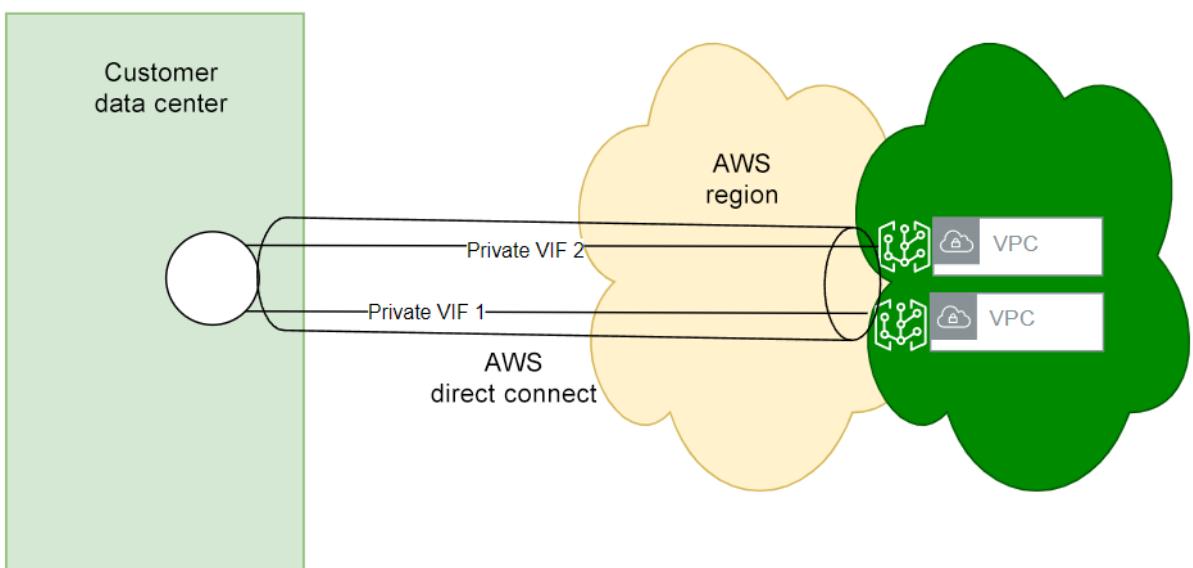
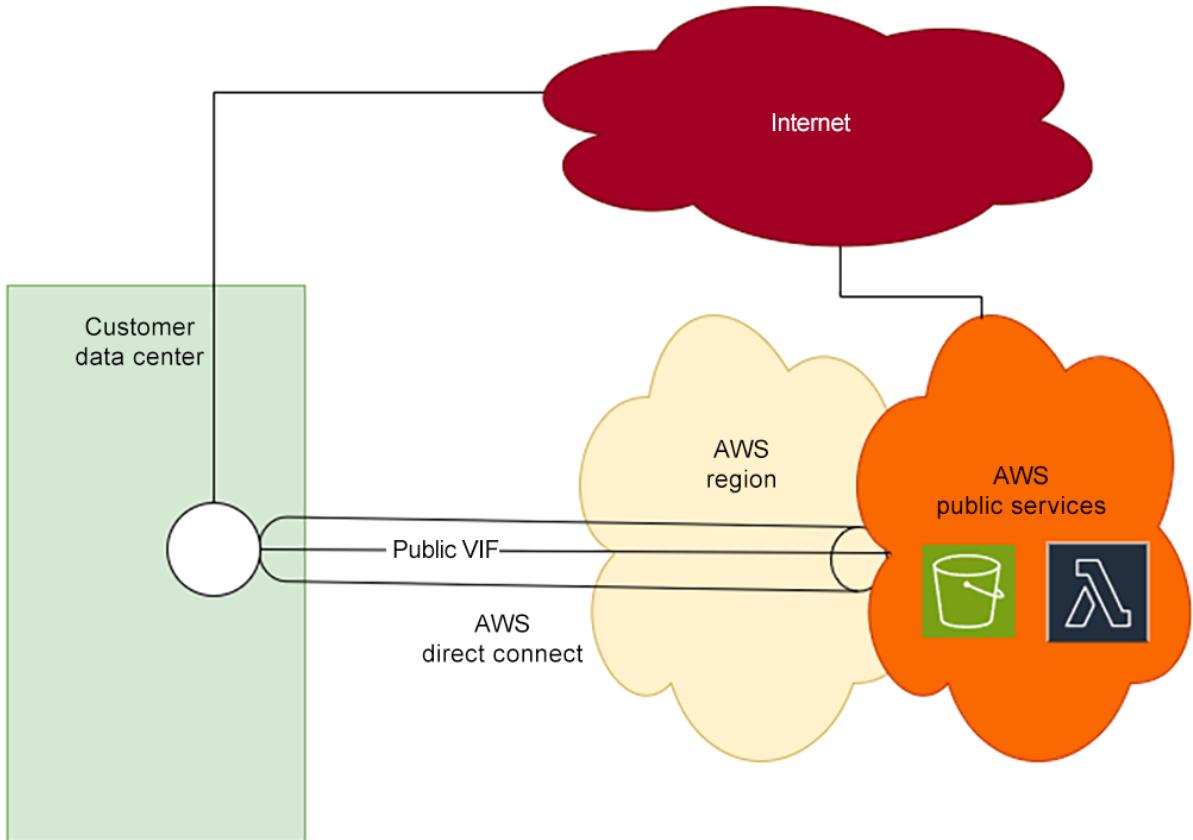


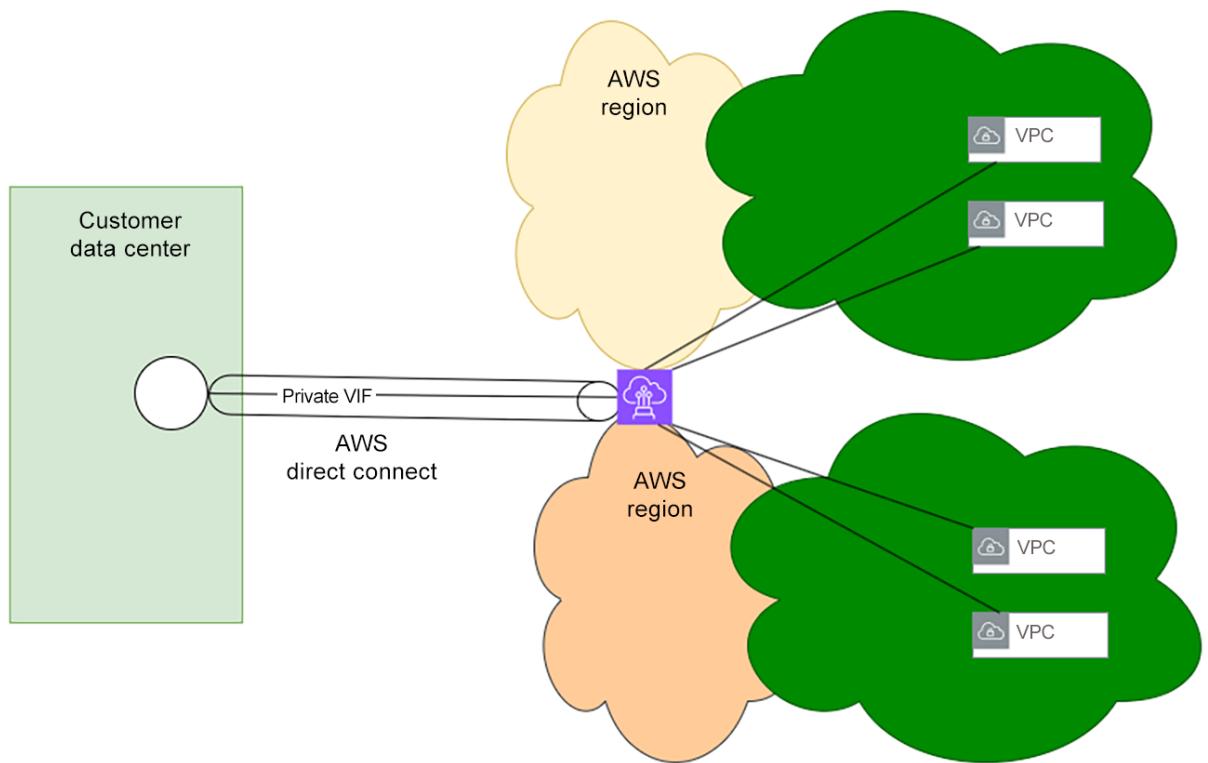
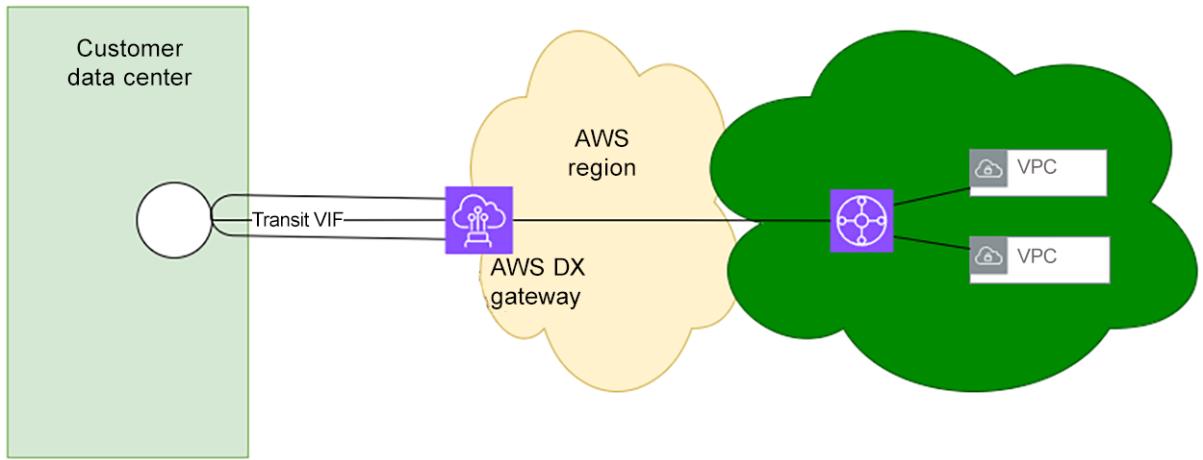
Logical  
Cabling

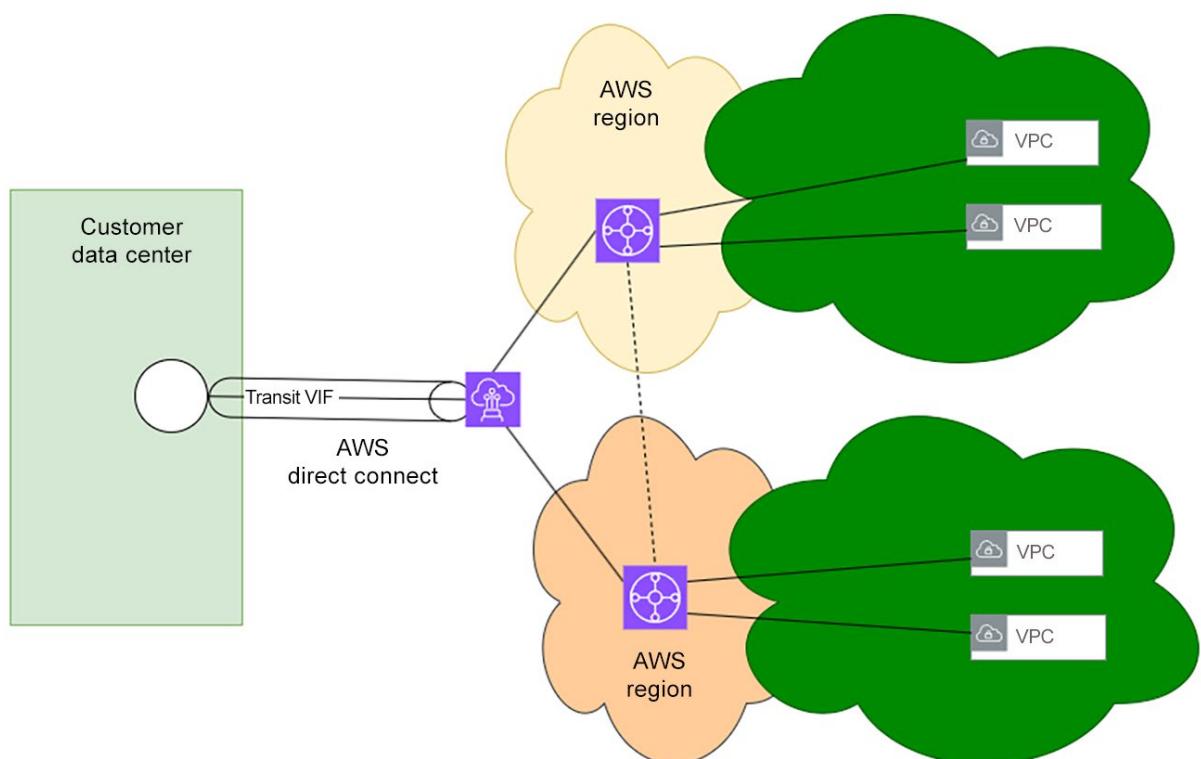
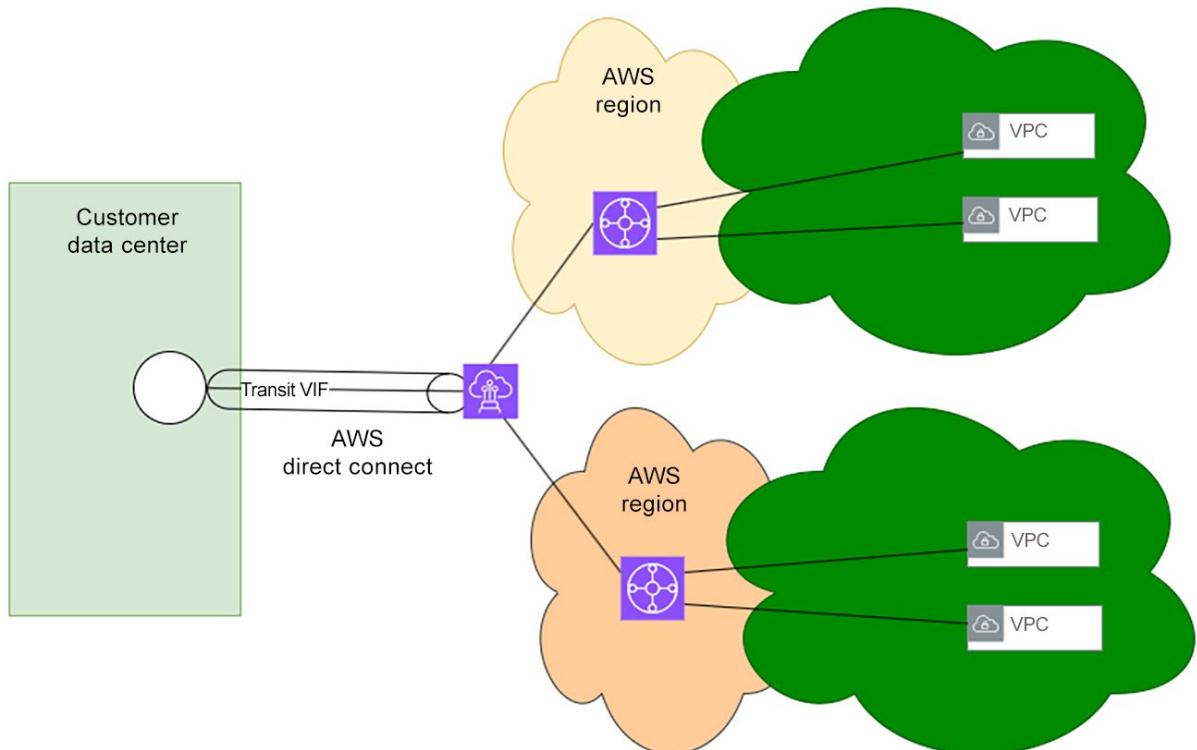


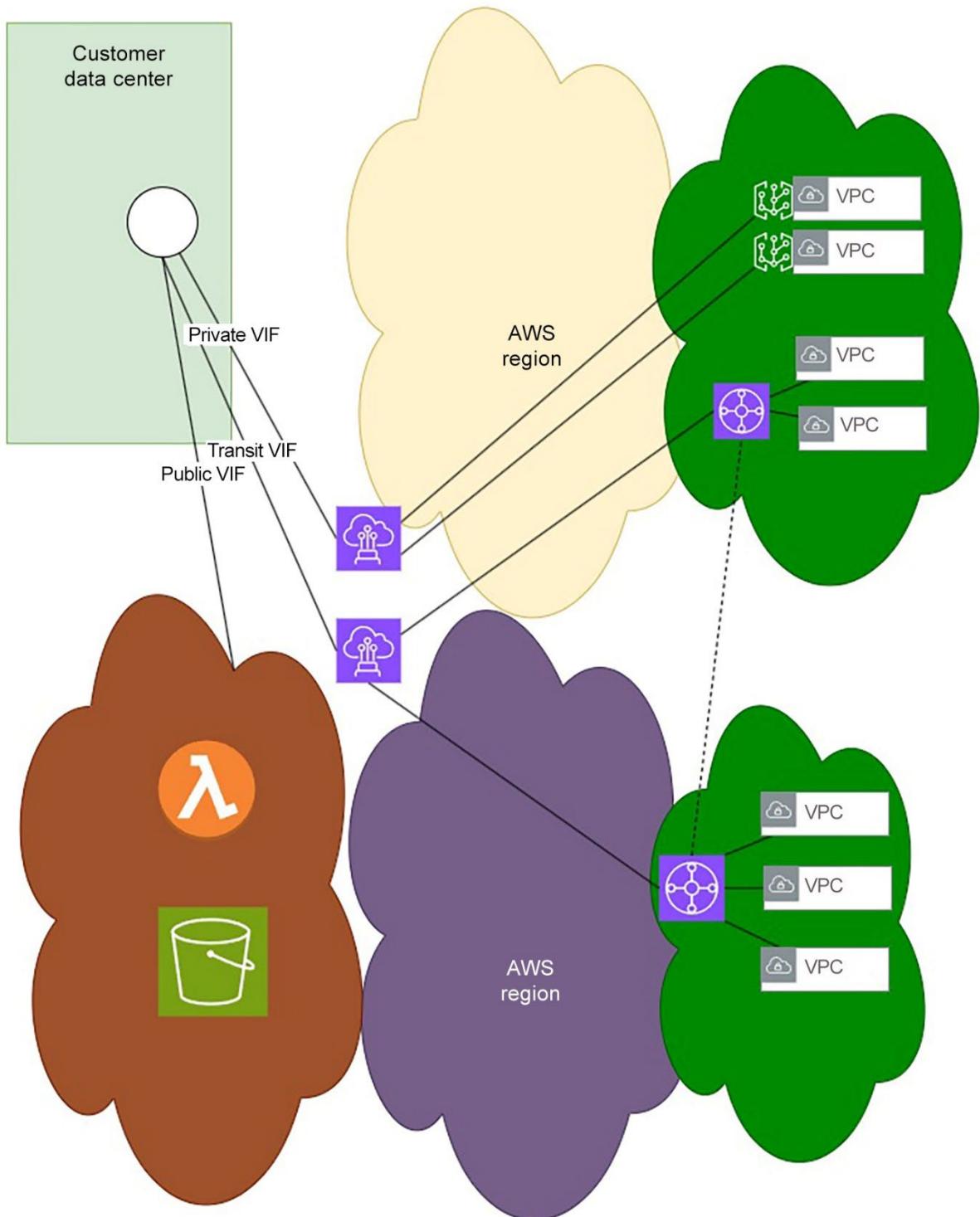
Ethernet frame  
headers

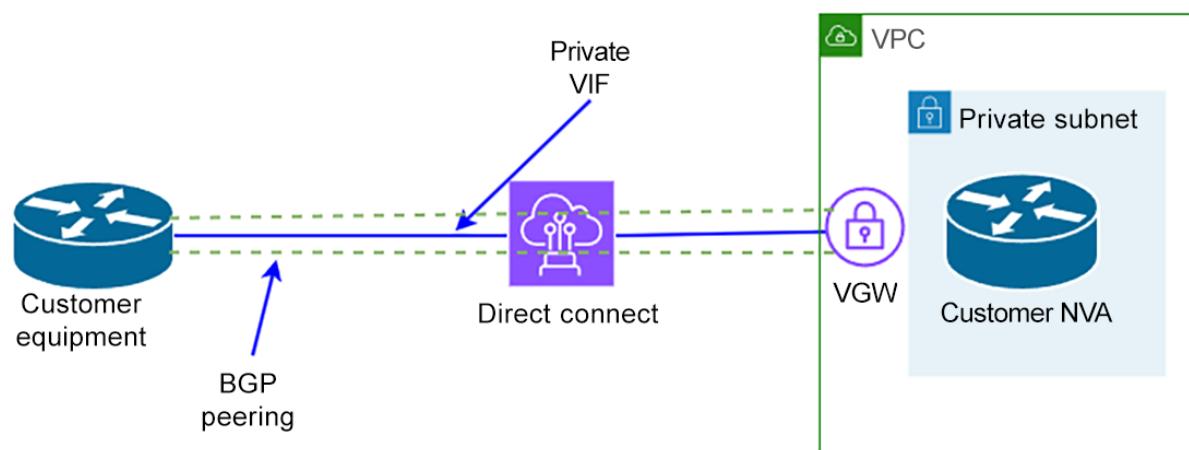
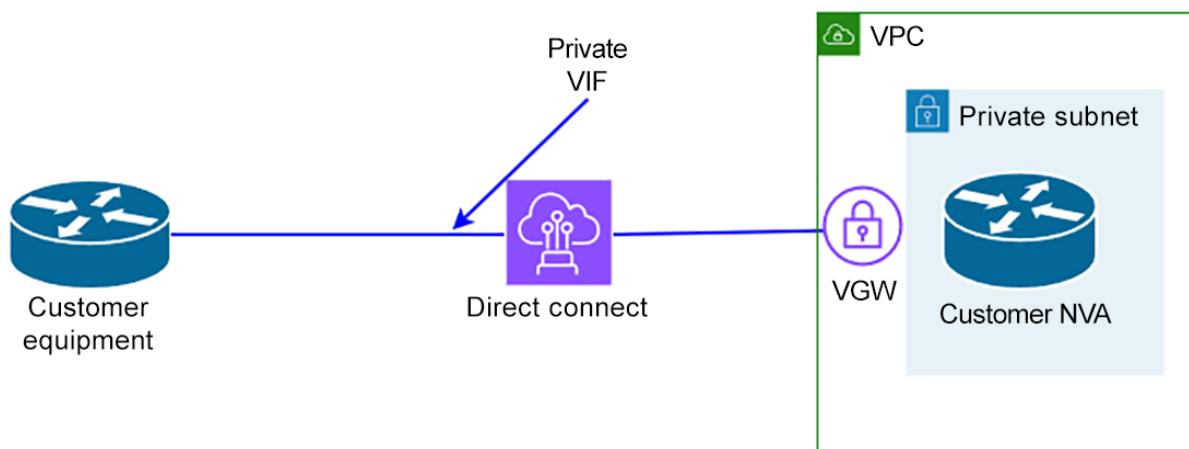
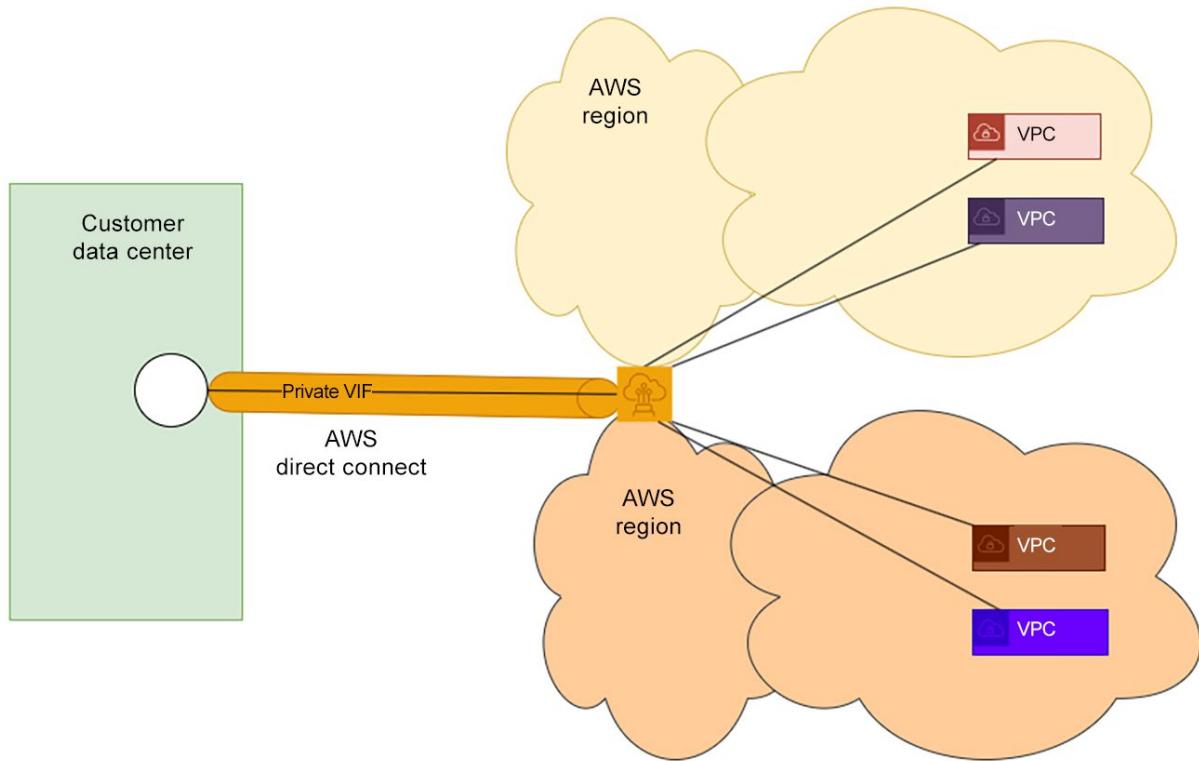


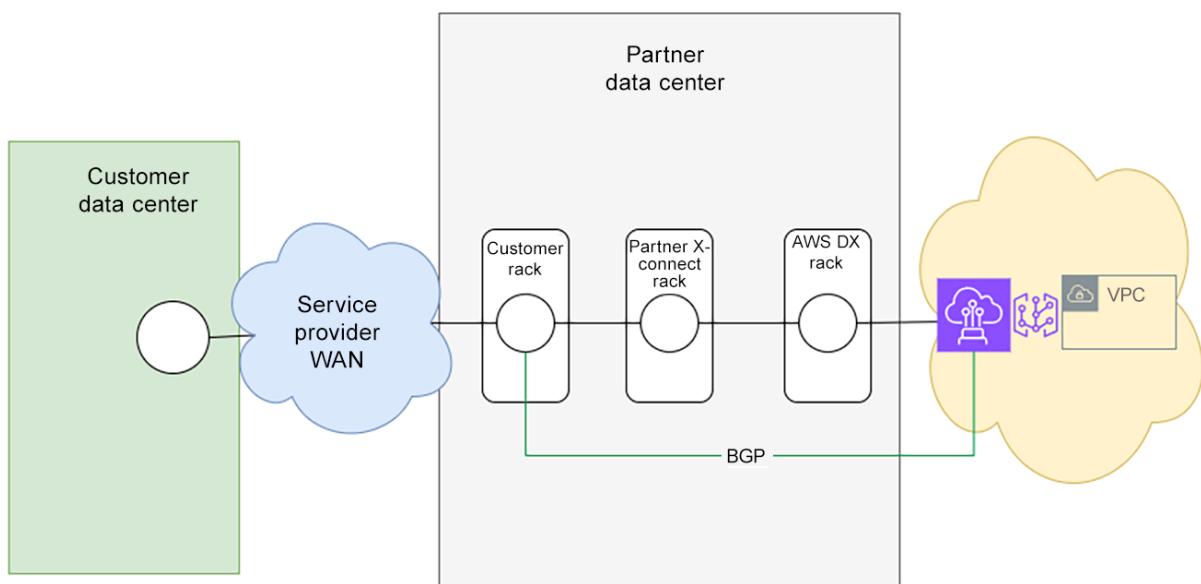
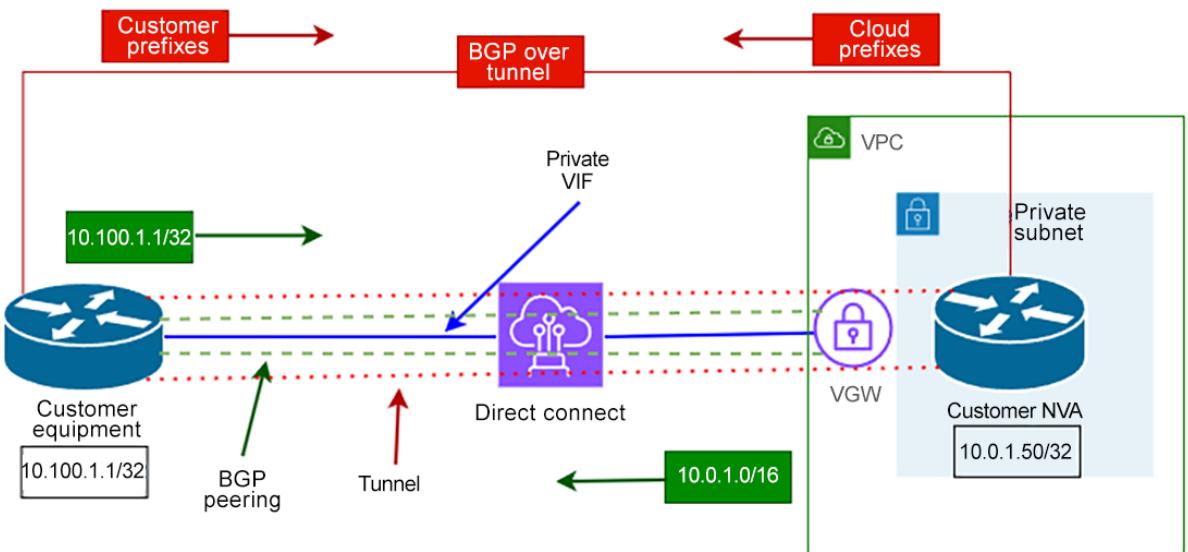
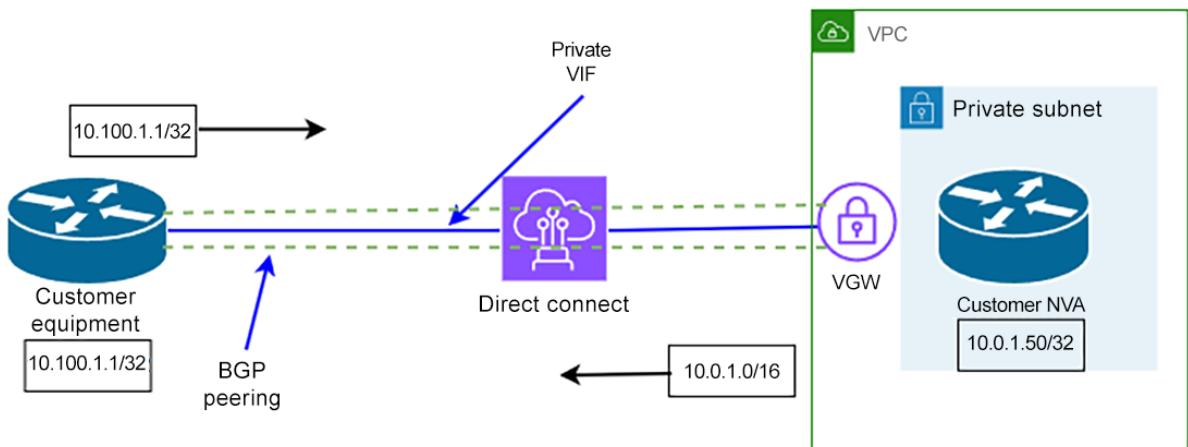


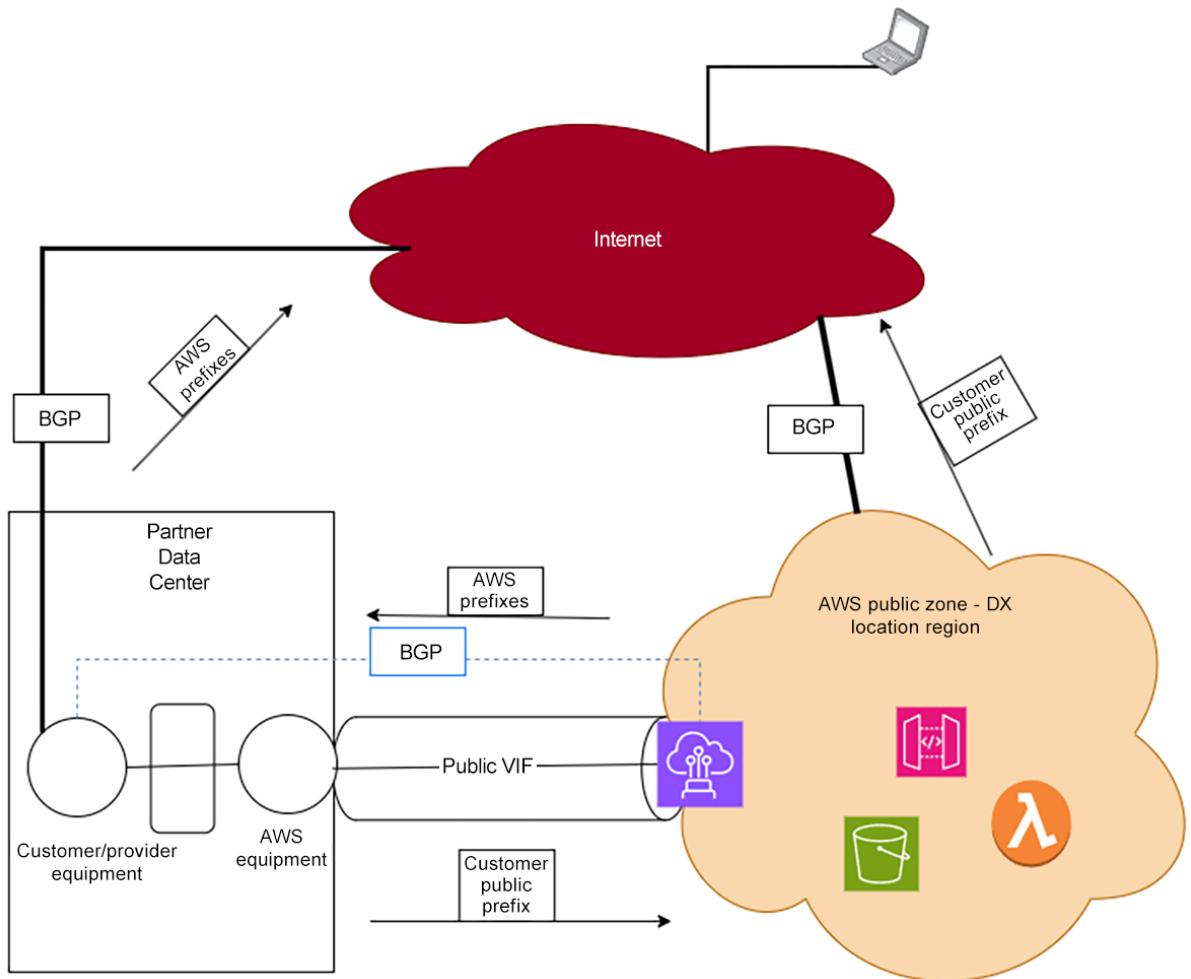


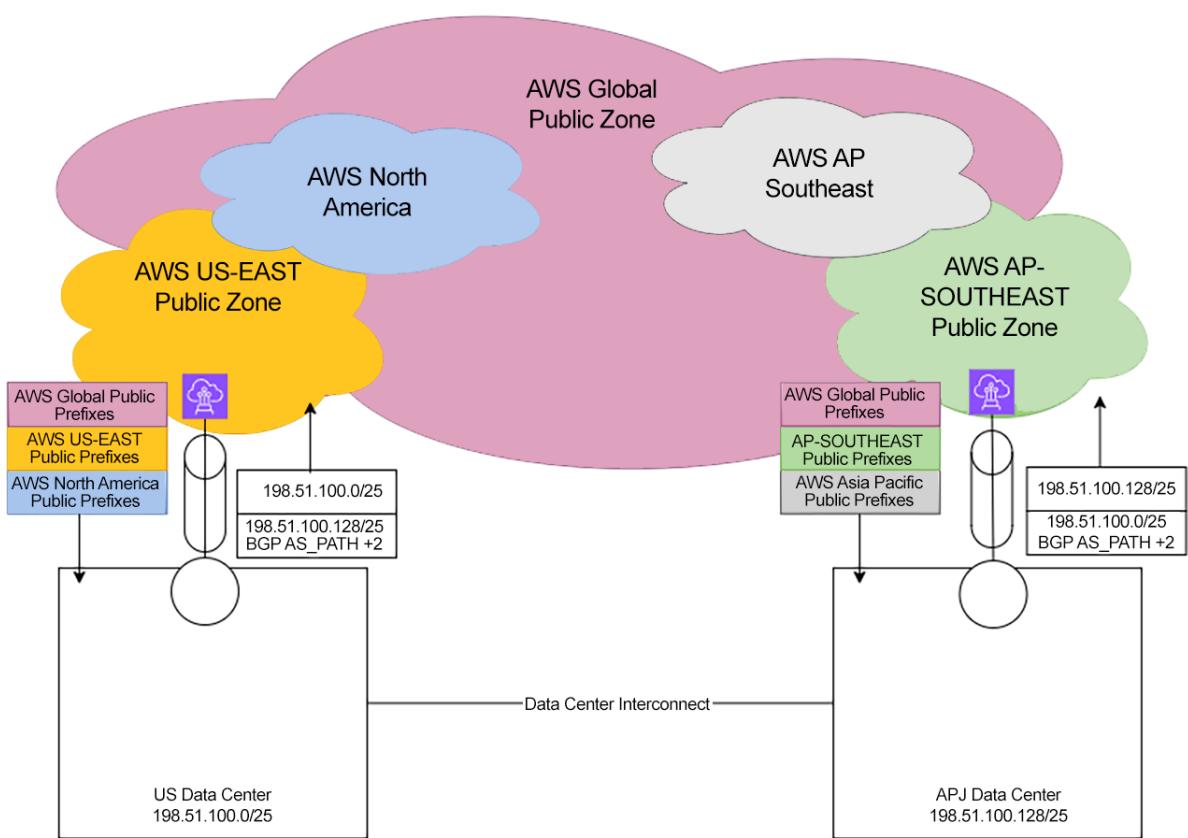
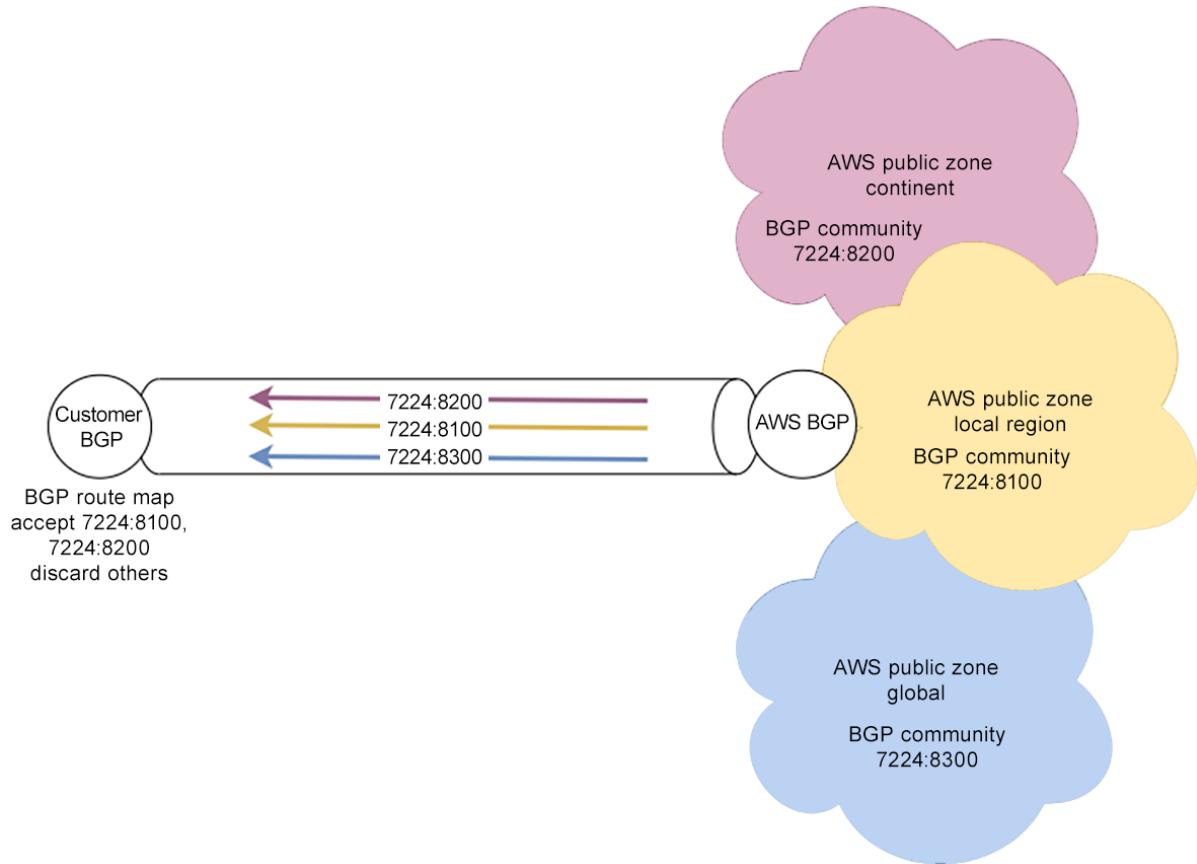


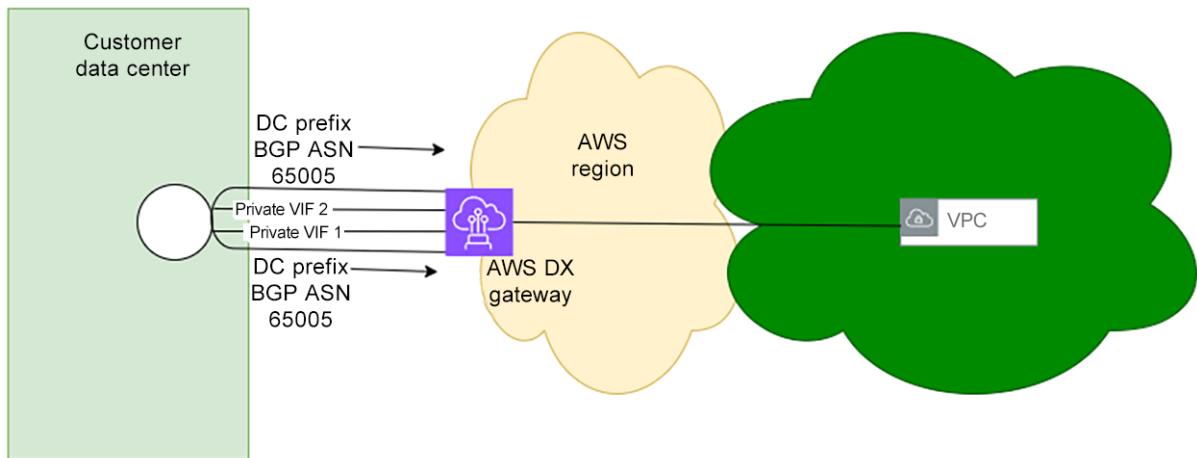




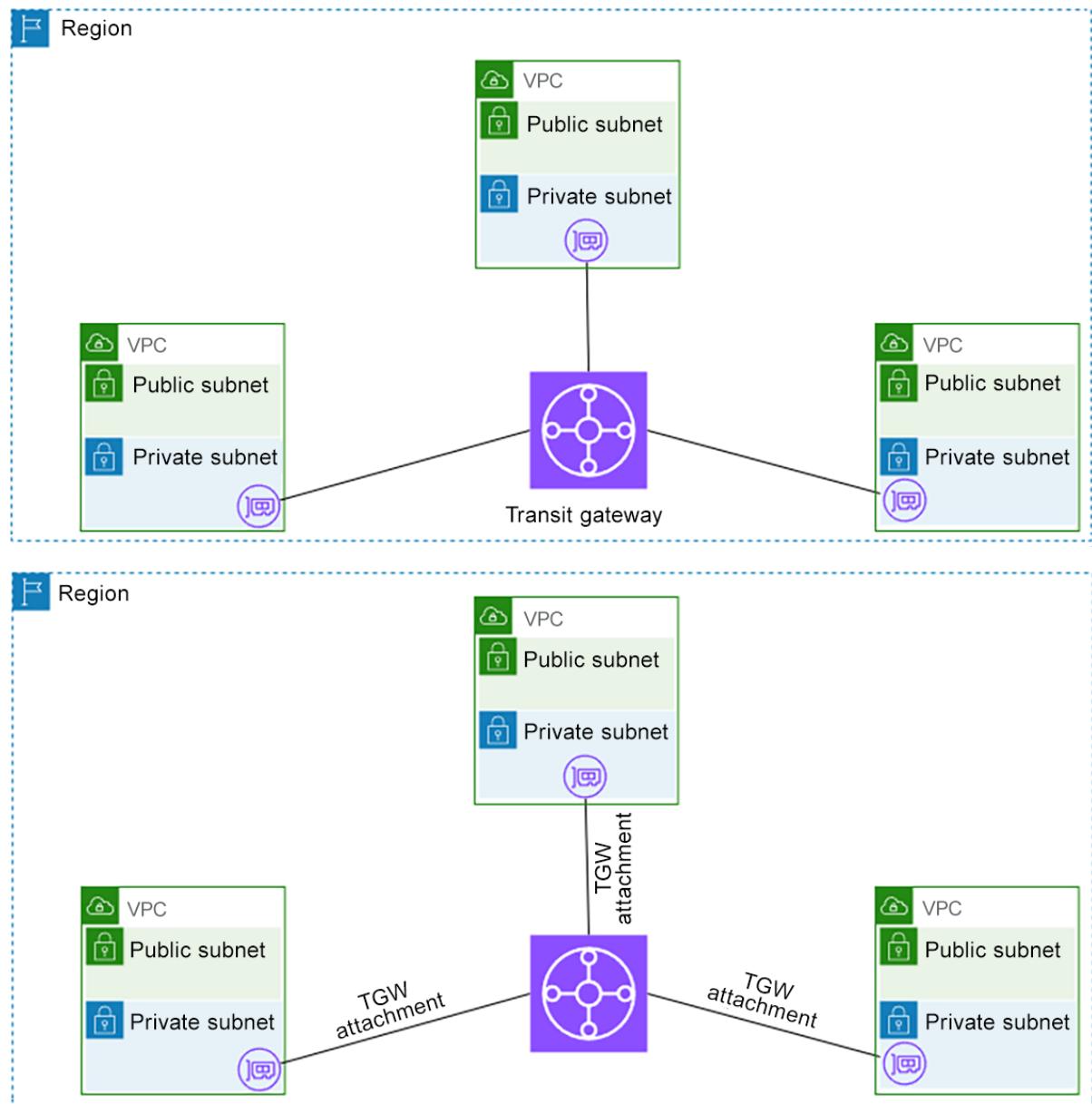


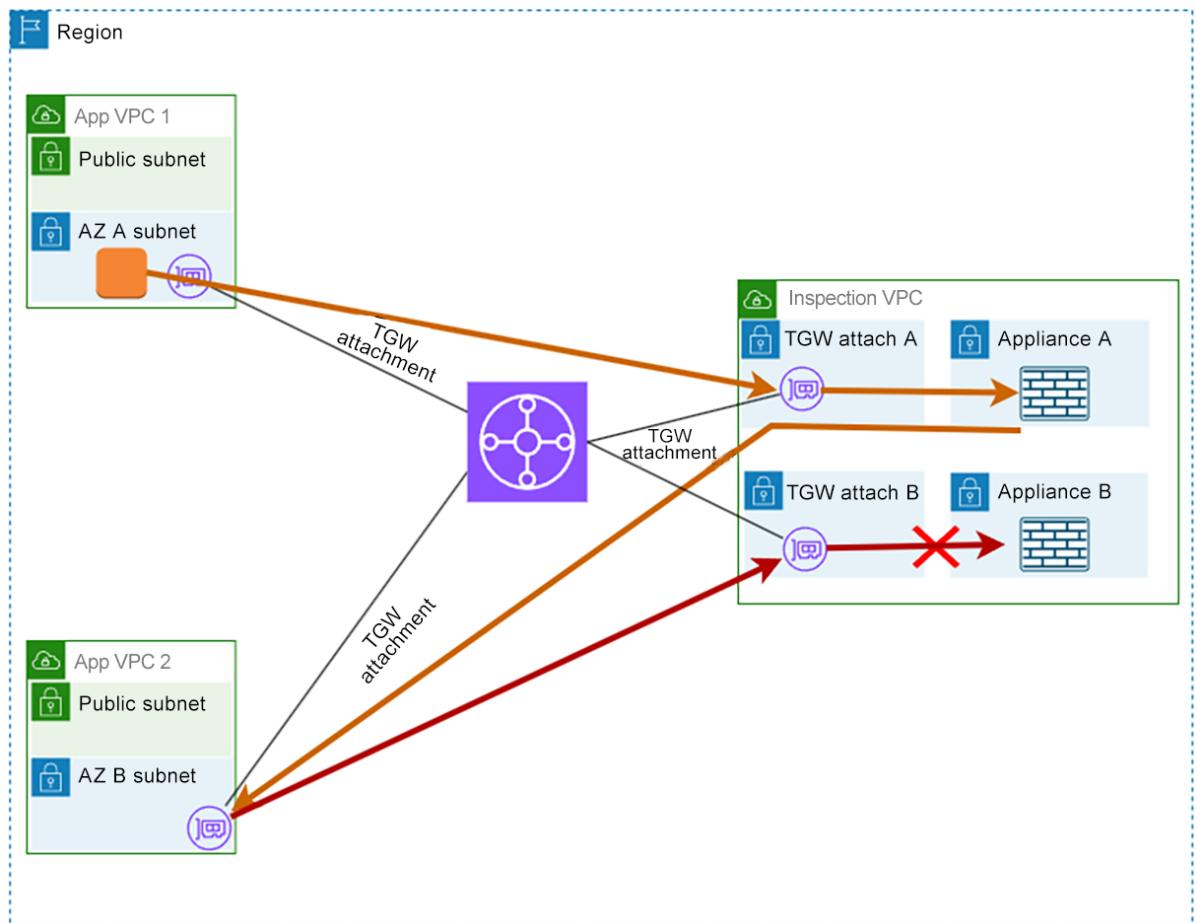
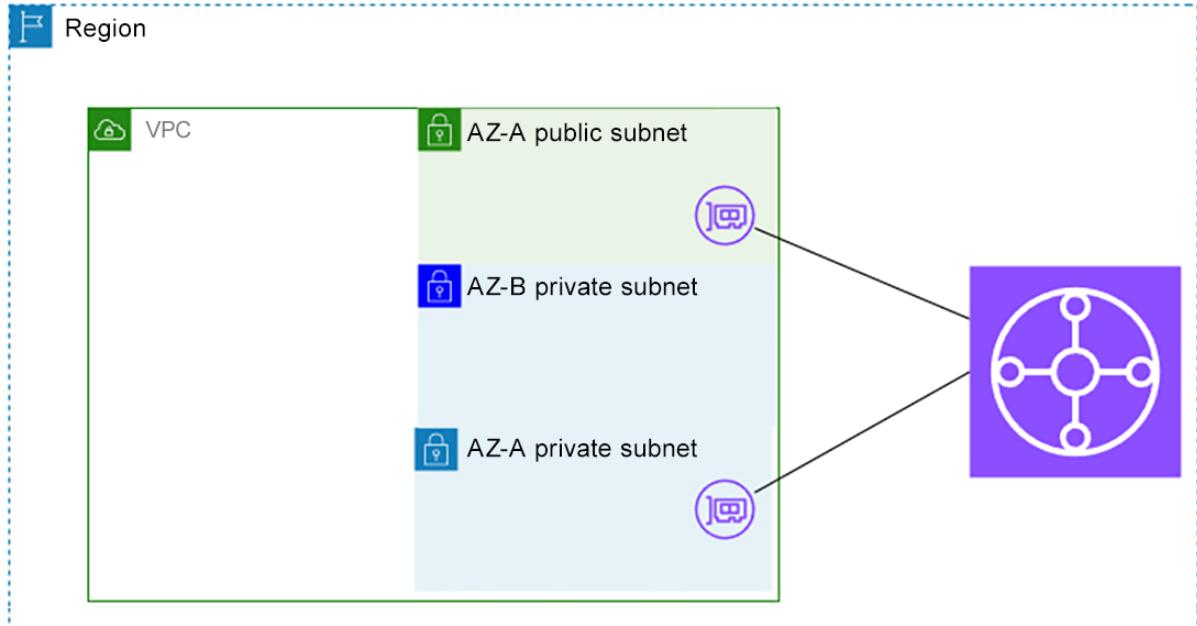


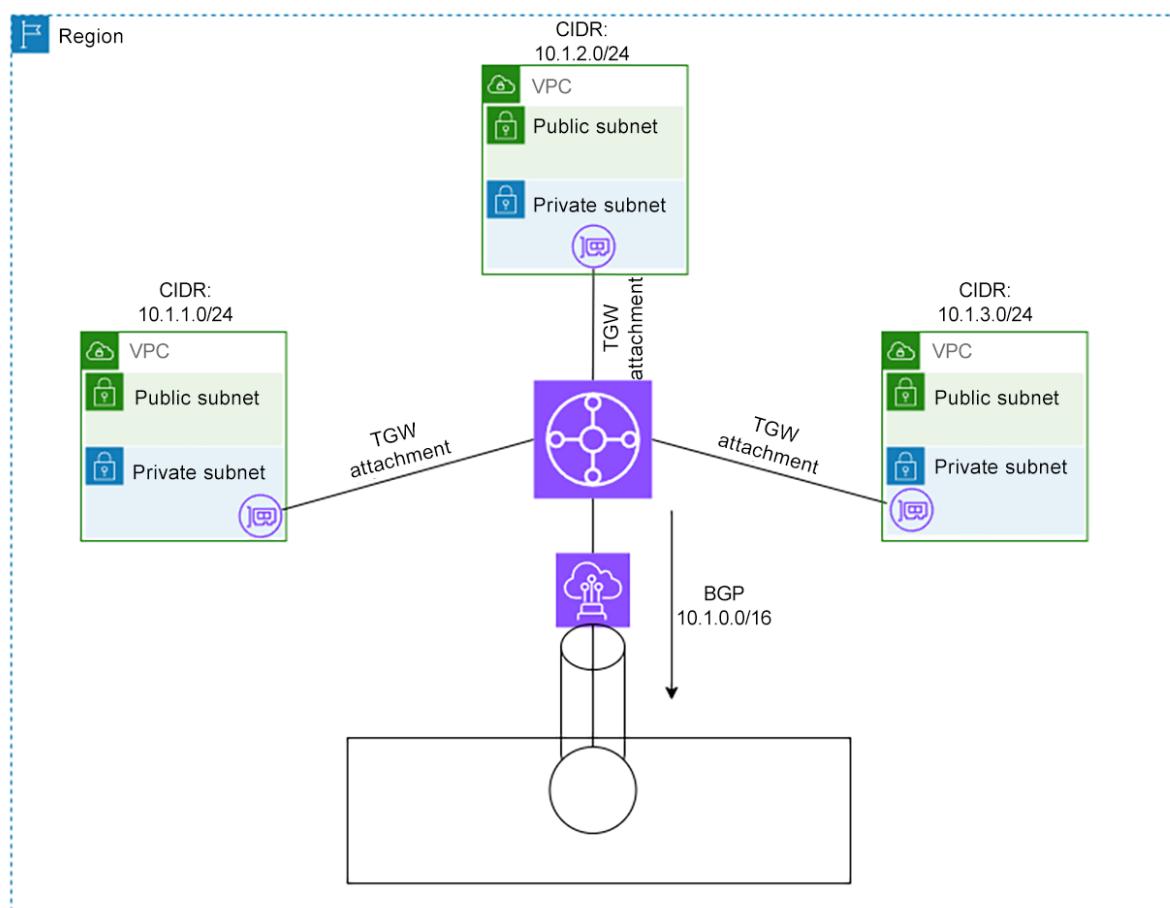
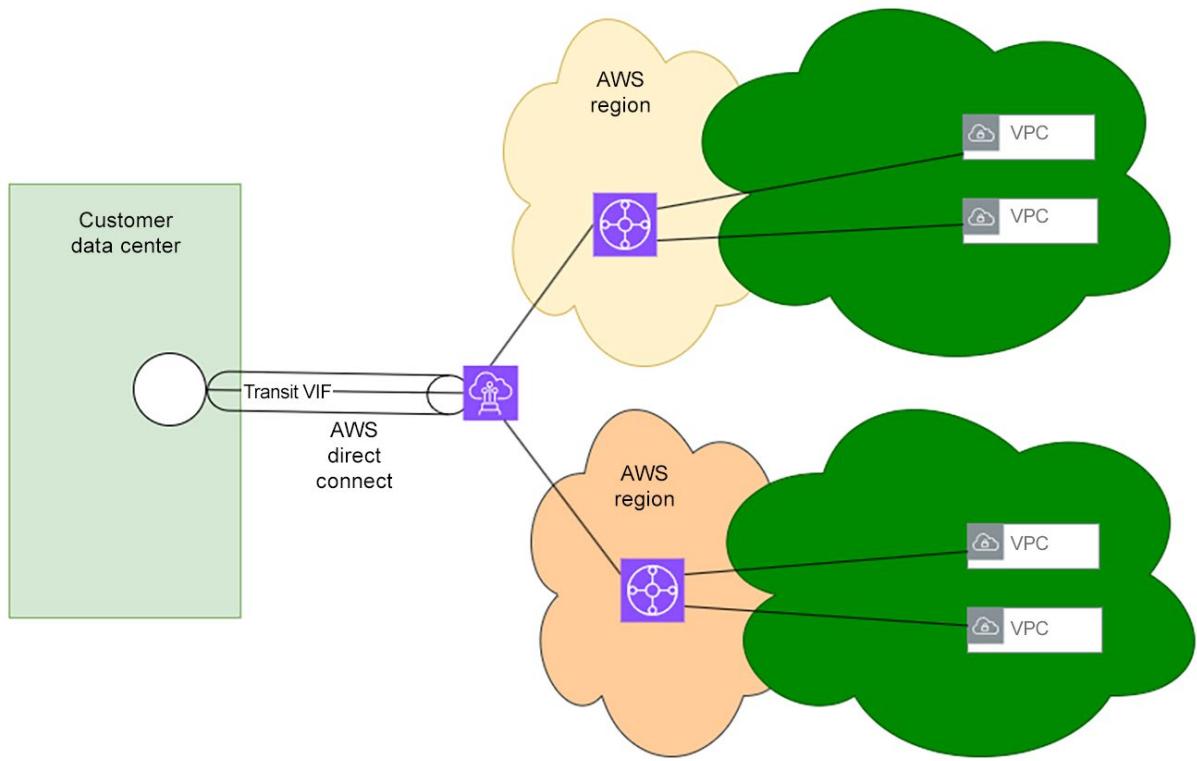


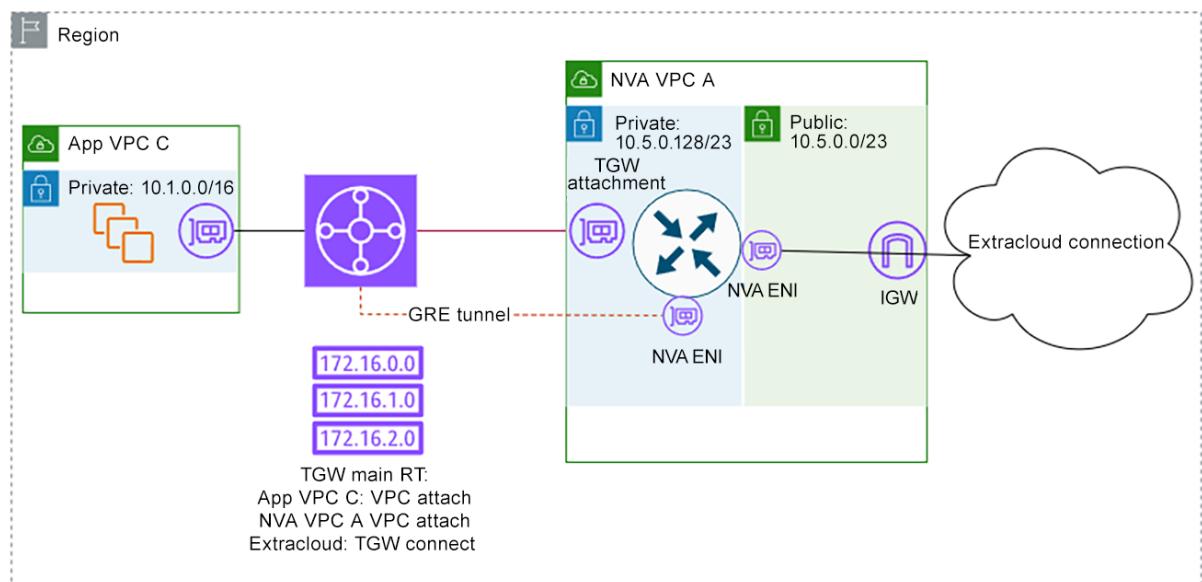
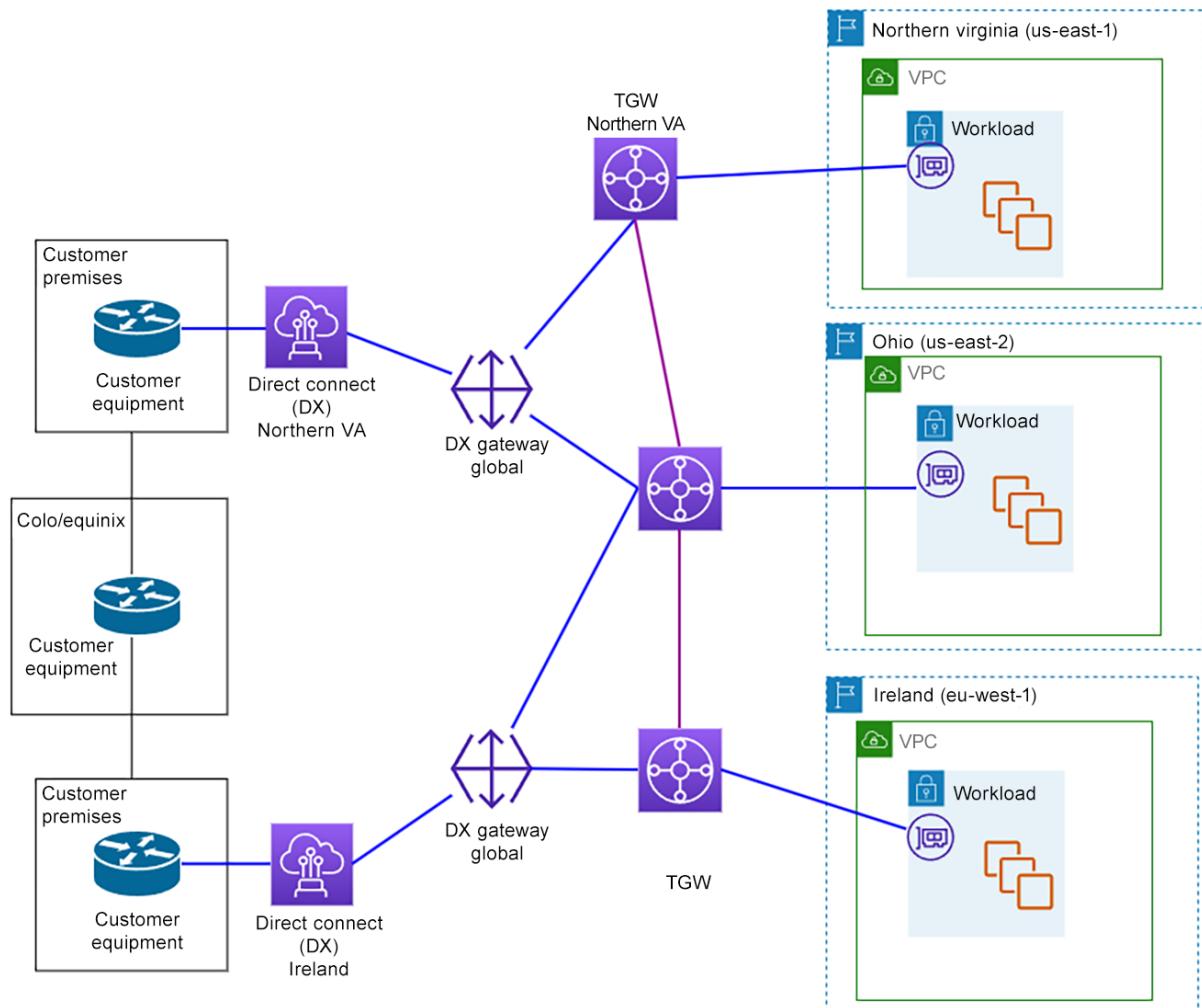


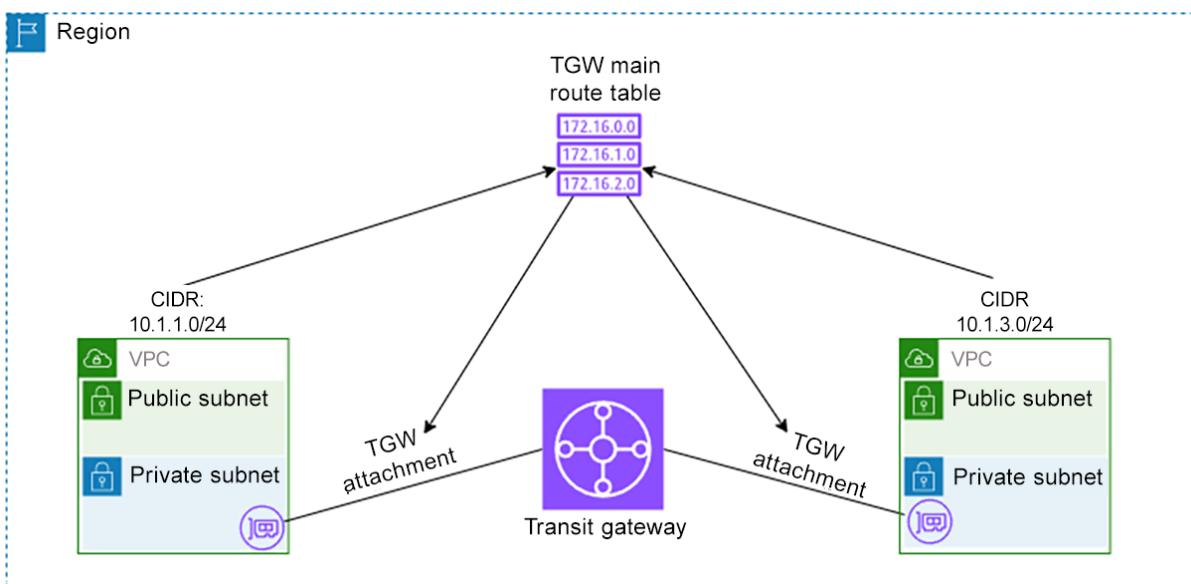
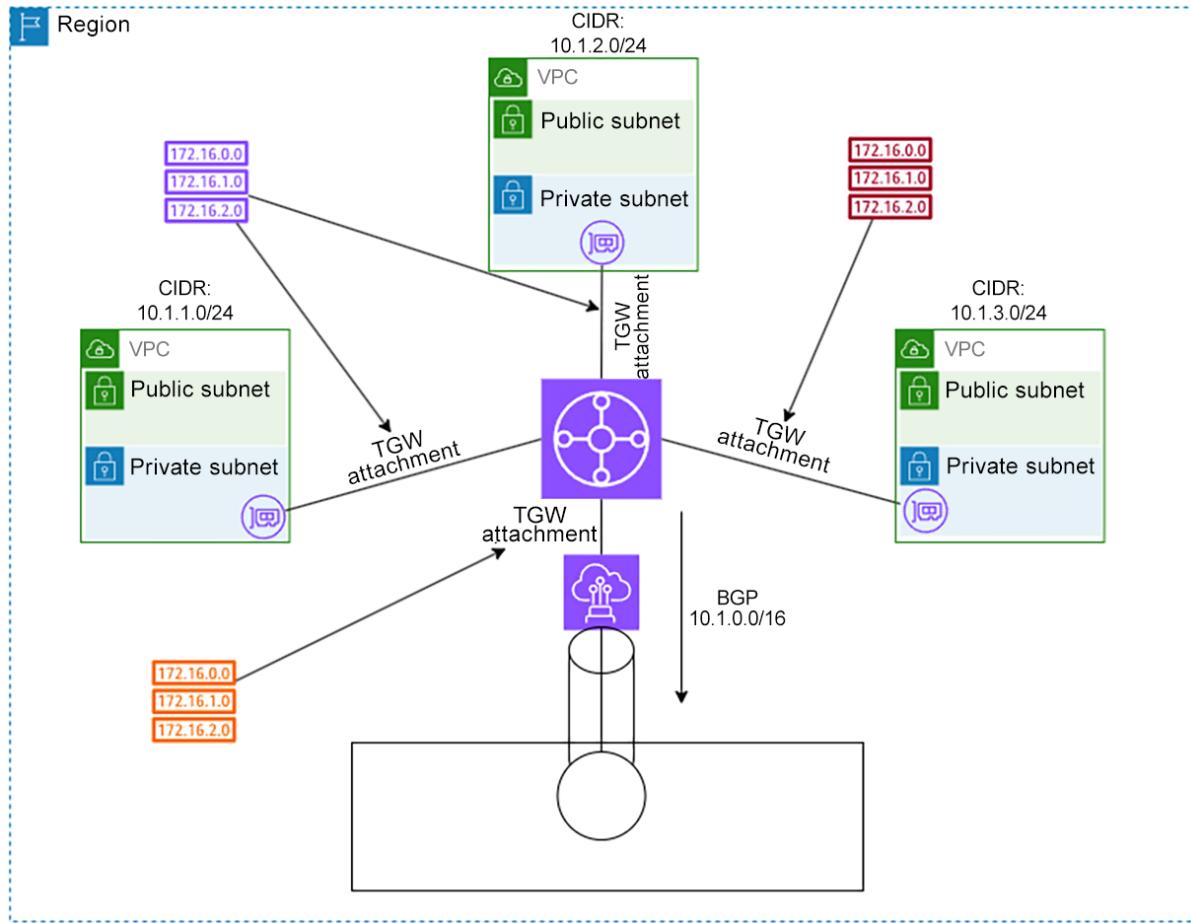
## Chapter 5: Hybrid Networking with AWS Transit Gateway

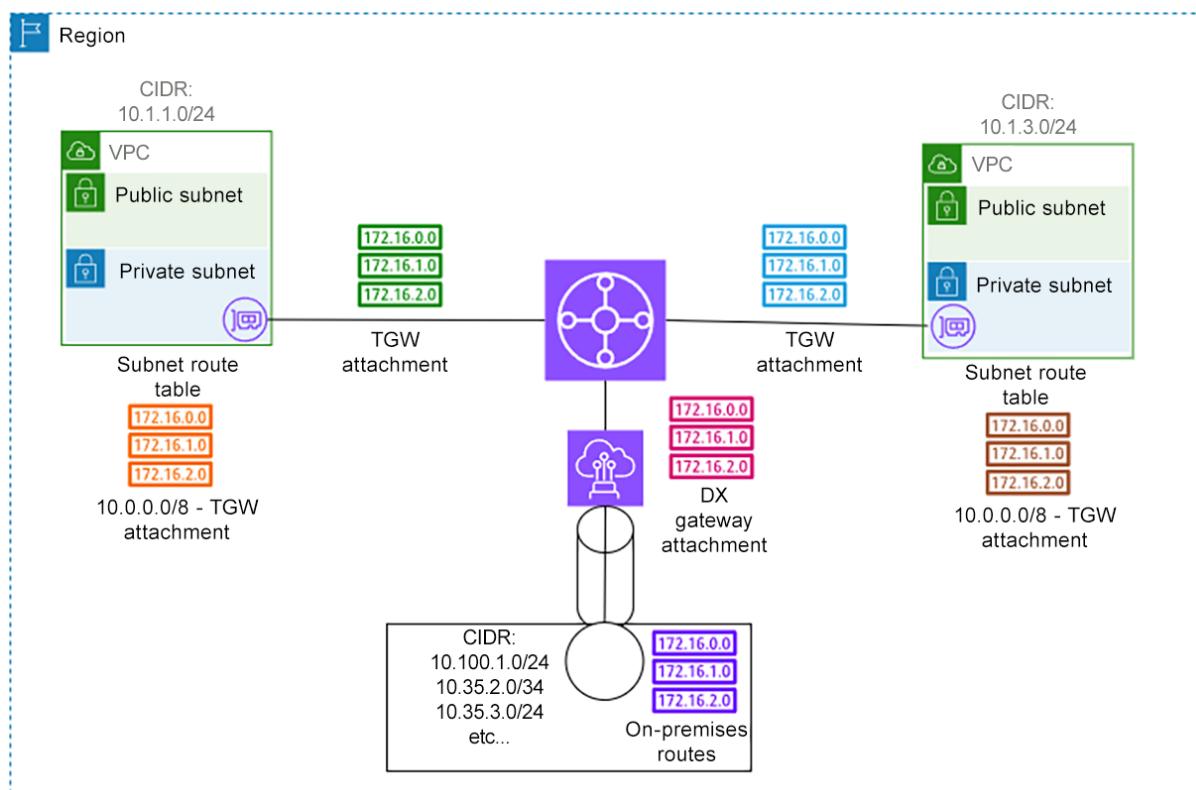
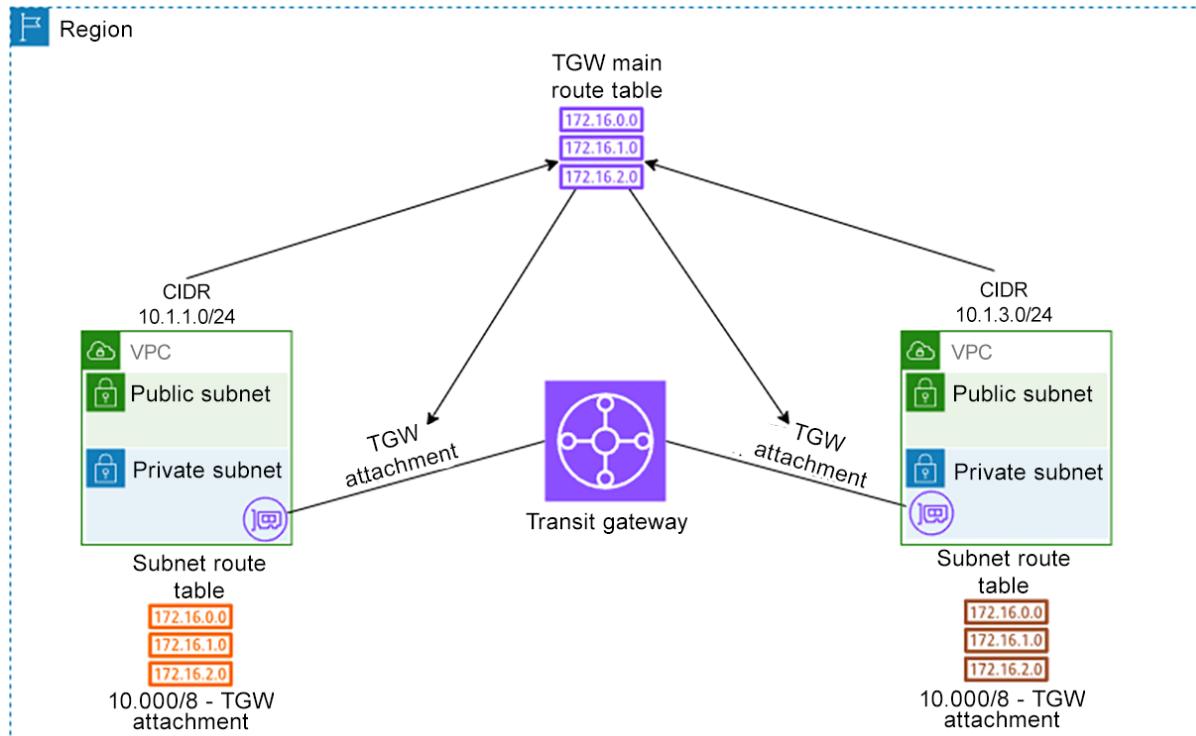


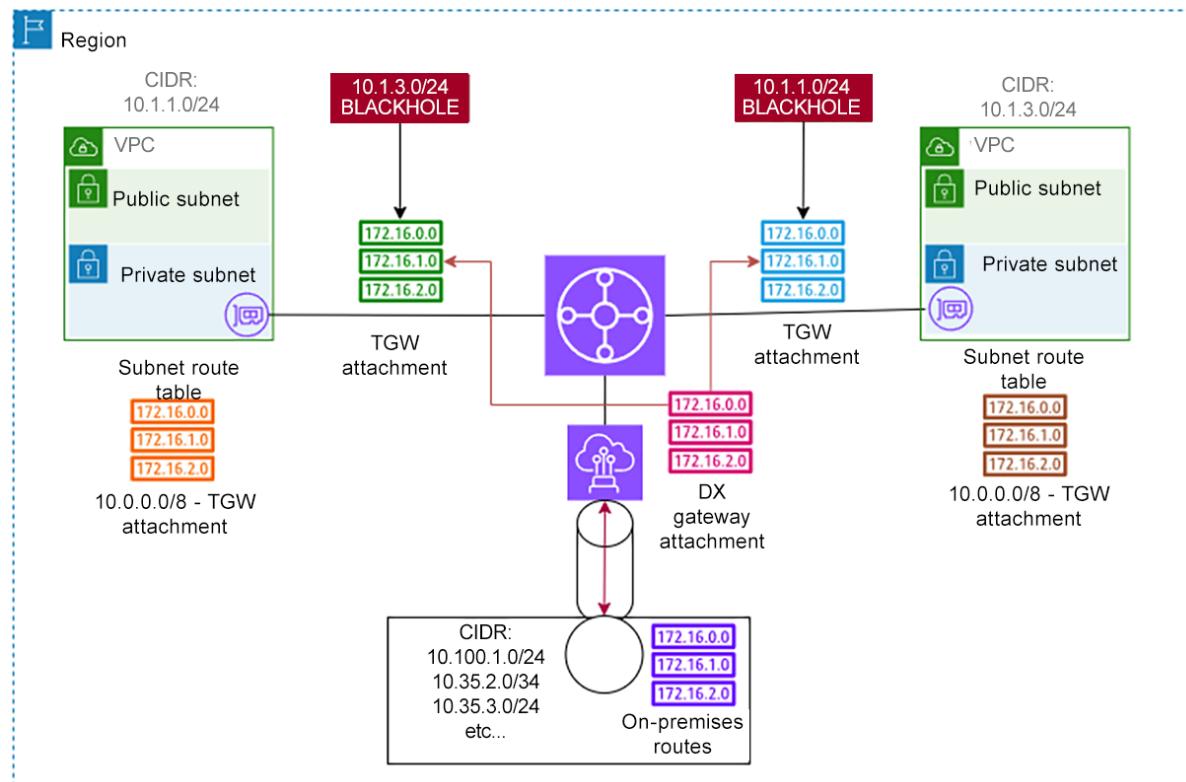
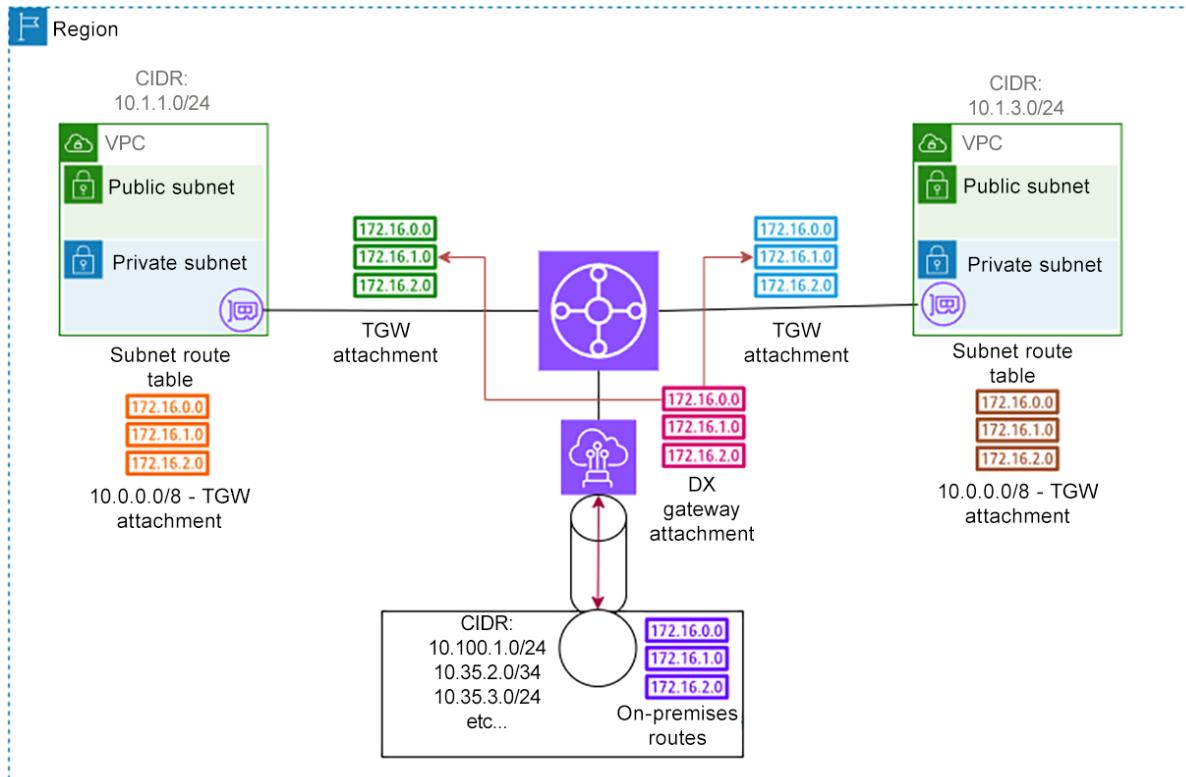


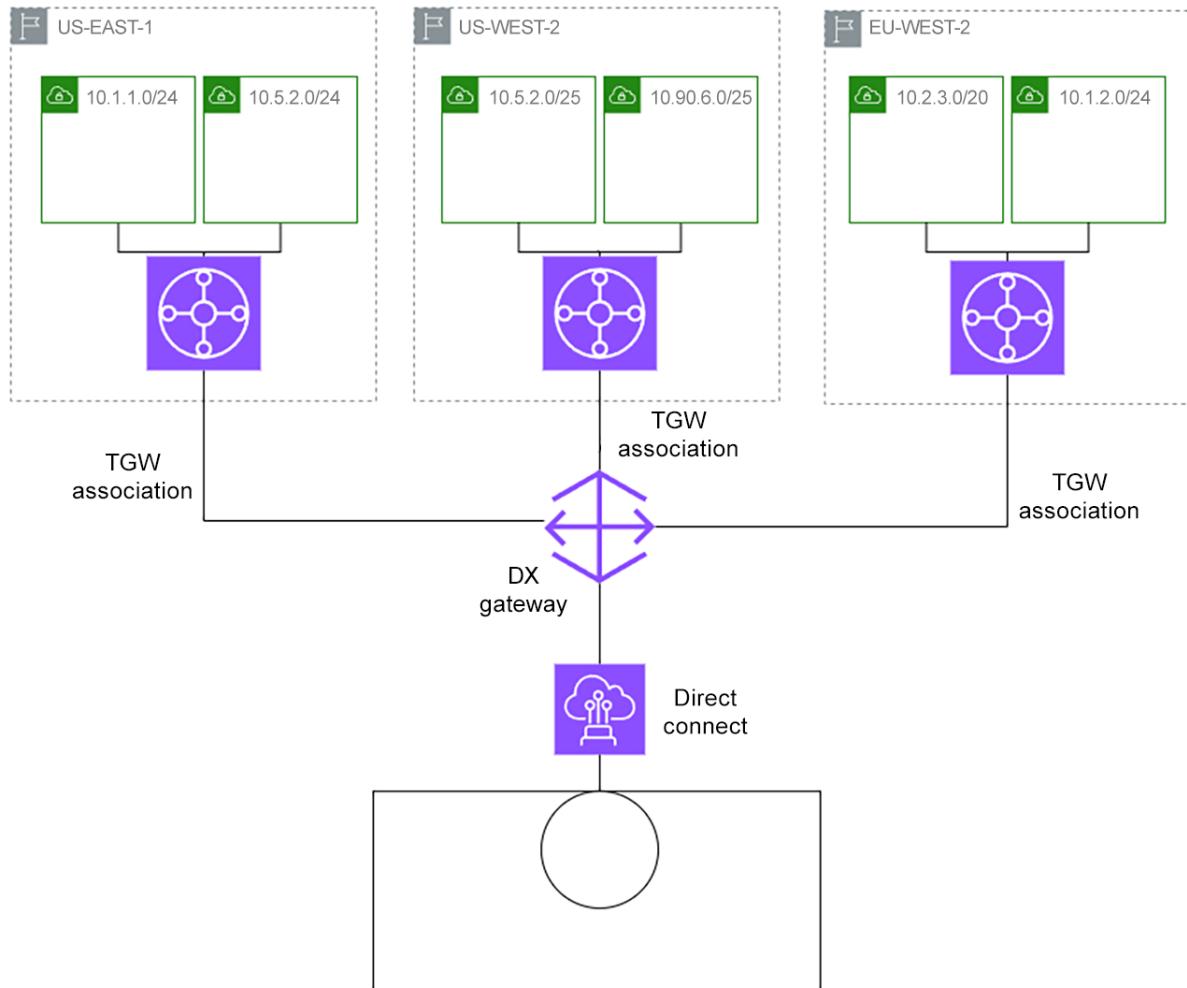


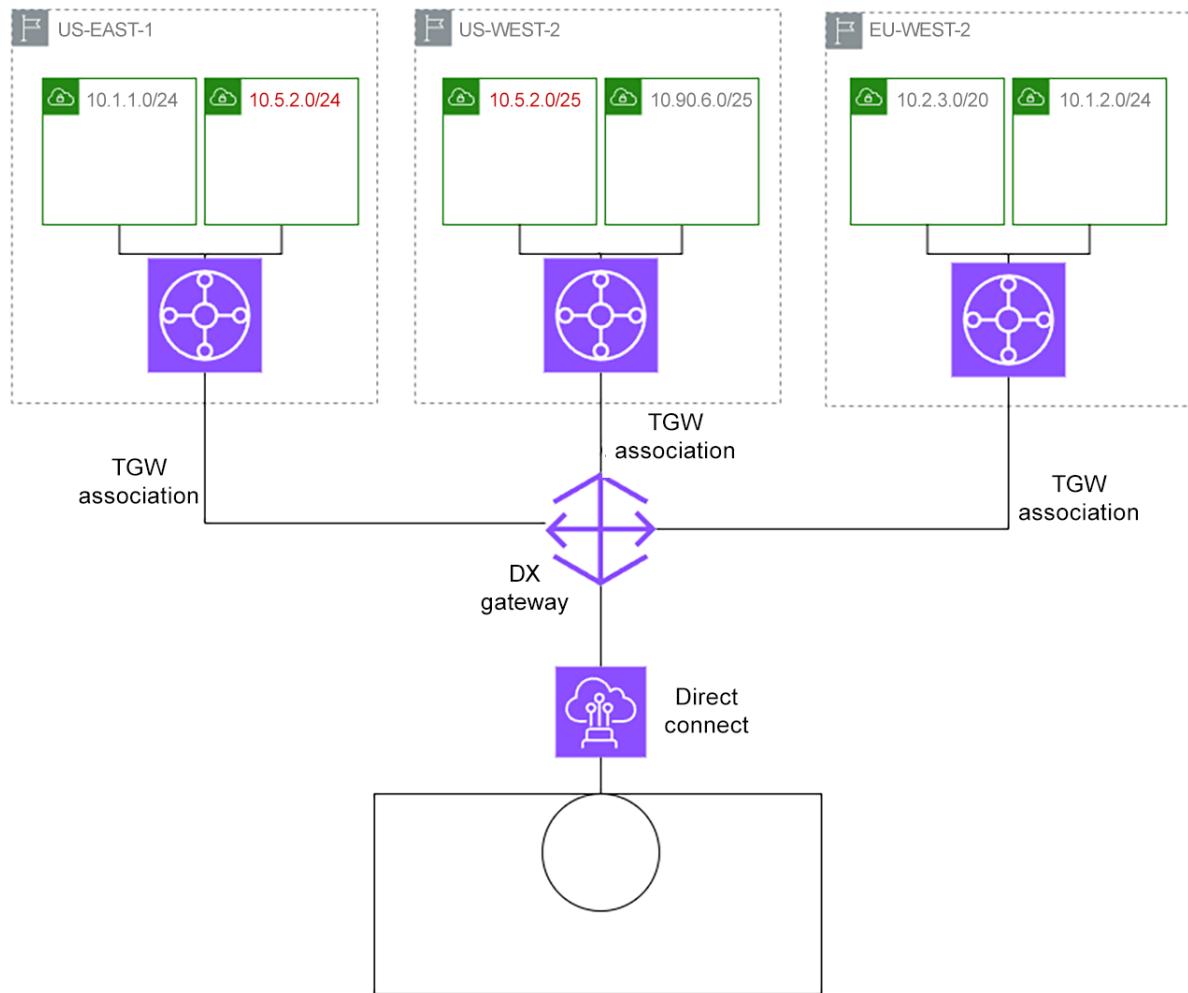


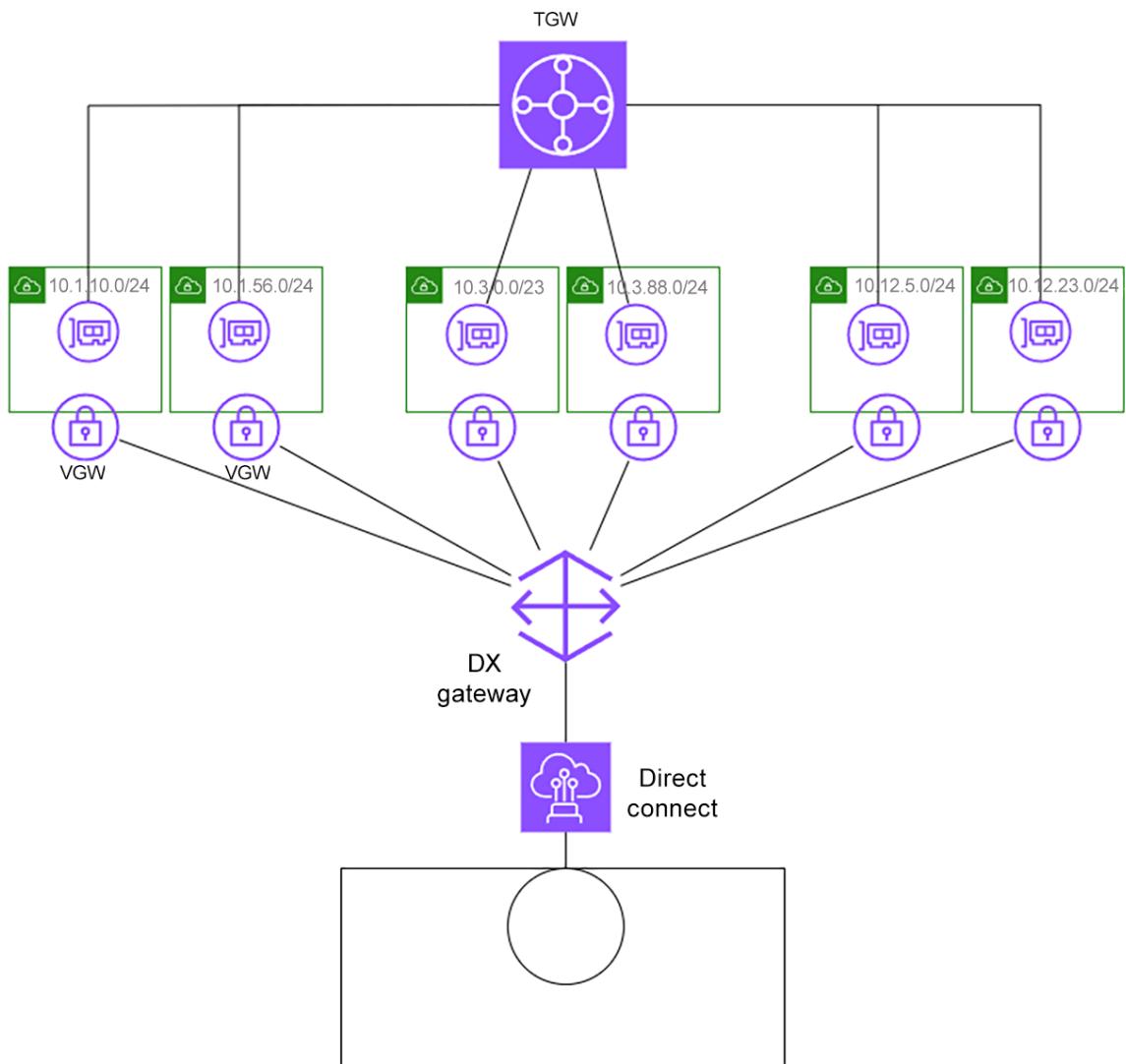


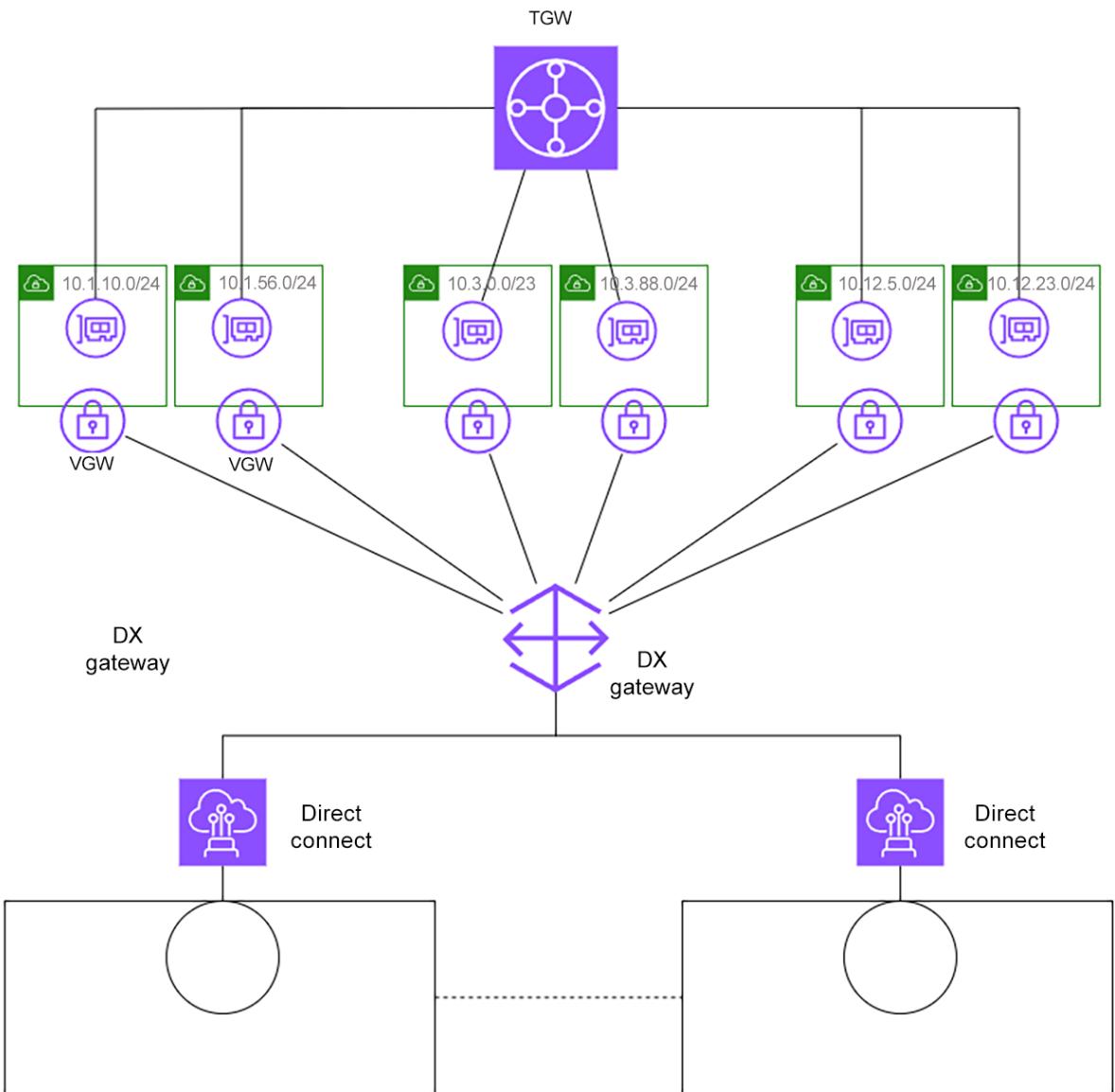


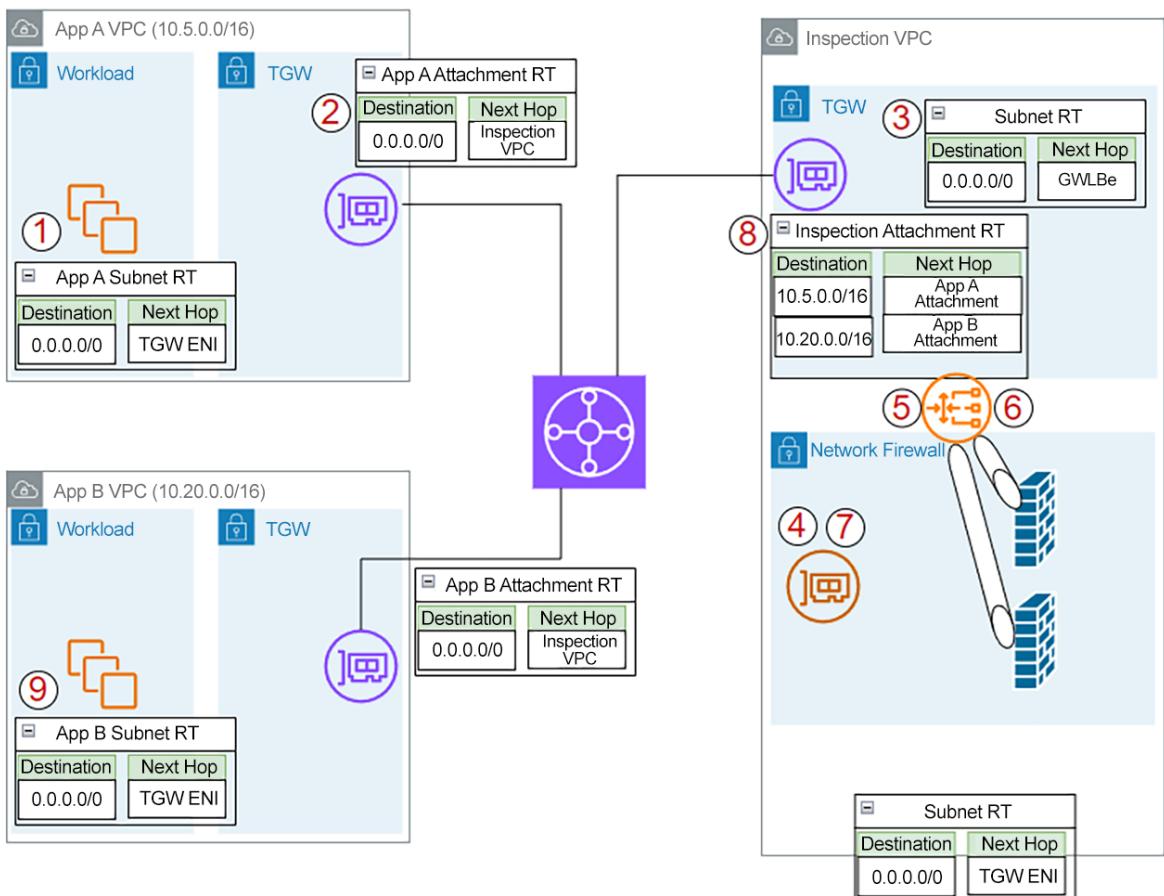
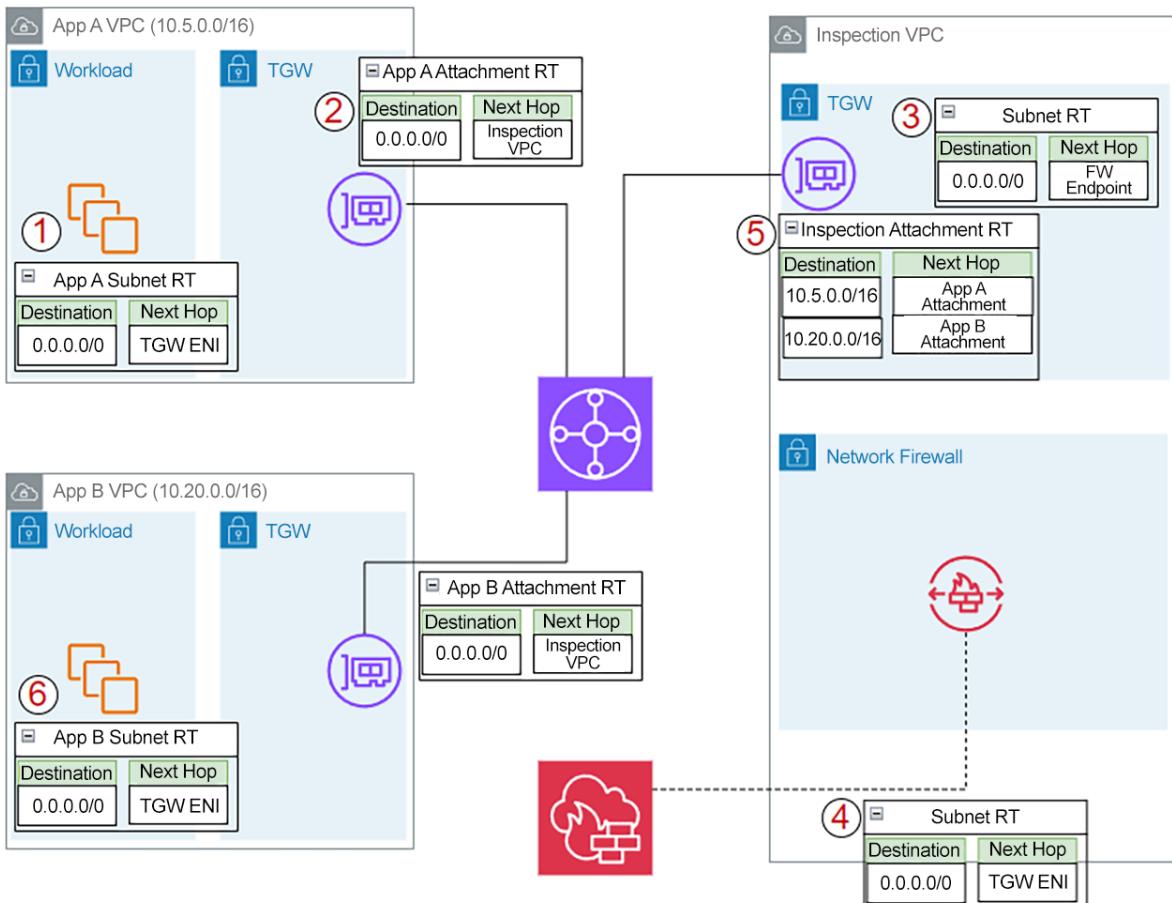




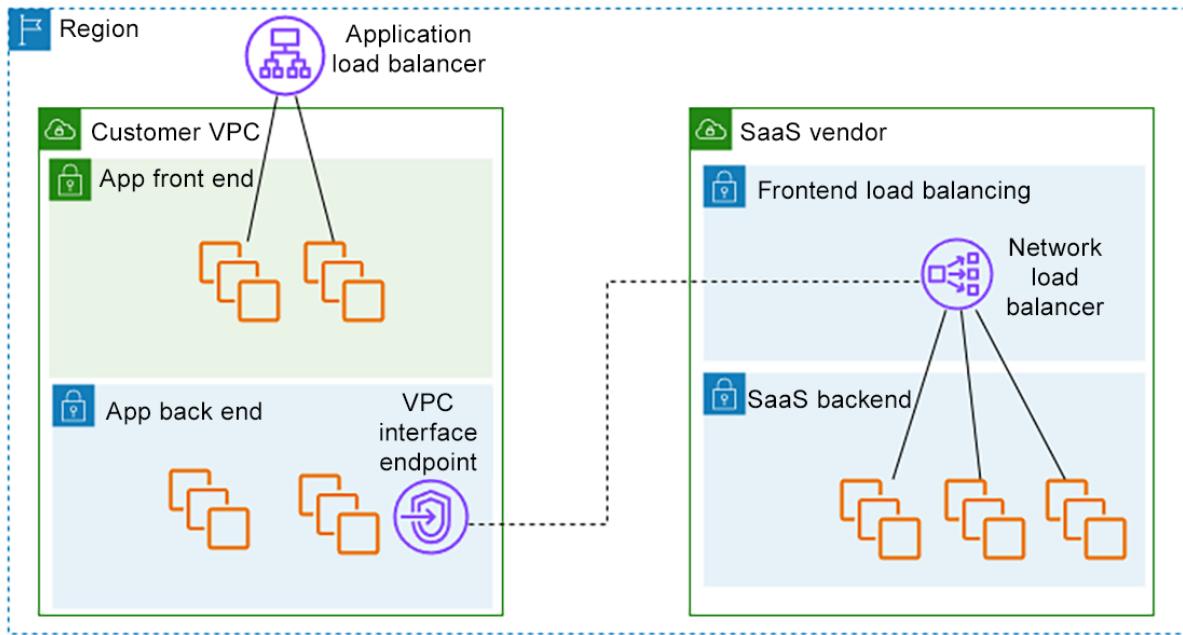








## Chapter 6: Connecting Third-Party Networks to AWS



EC2 > 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  
Allow\_VPN\_IN  
Name cannot be edited after creation.

Description Info  
Allow on-prem resources

VPC info  
vpc-067a04f3bebe45564 (test-vpc)

**Inbound rules Info**

Type <small>Info</small>	Protocol <small>Info</small>	Port range <small>Info</small>	Source <small>Info</small>	Description - optional <small>Info</small>
All TCP	TCP	0 - 65535	Custom	10.100.10.0/24 Allow VPN Resources
10.100.10.0/24 X				

Add rule

## 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.

Value must be 256 characters or less in length.

#### Target gateway type Info

- Virtual private gateway
- Transit gateway
- Not associated

#### Virtual private gateway



#### Customer gateway Info

- Existing
- New

#### Customer gateway ID



#### Routing options Info

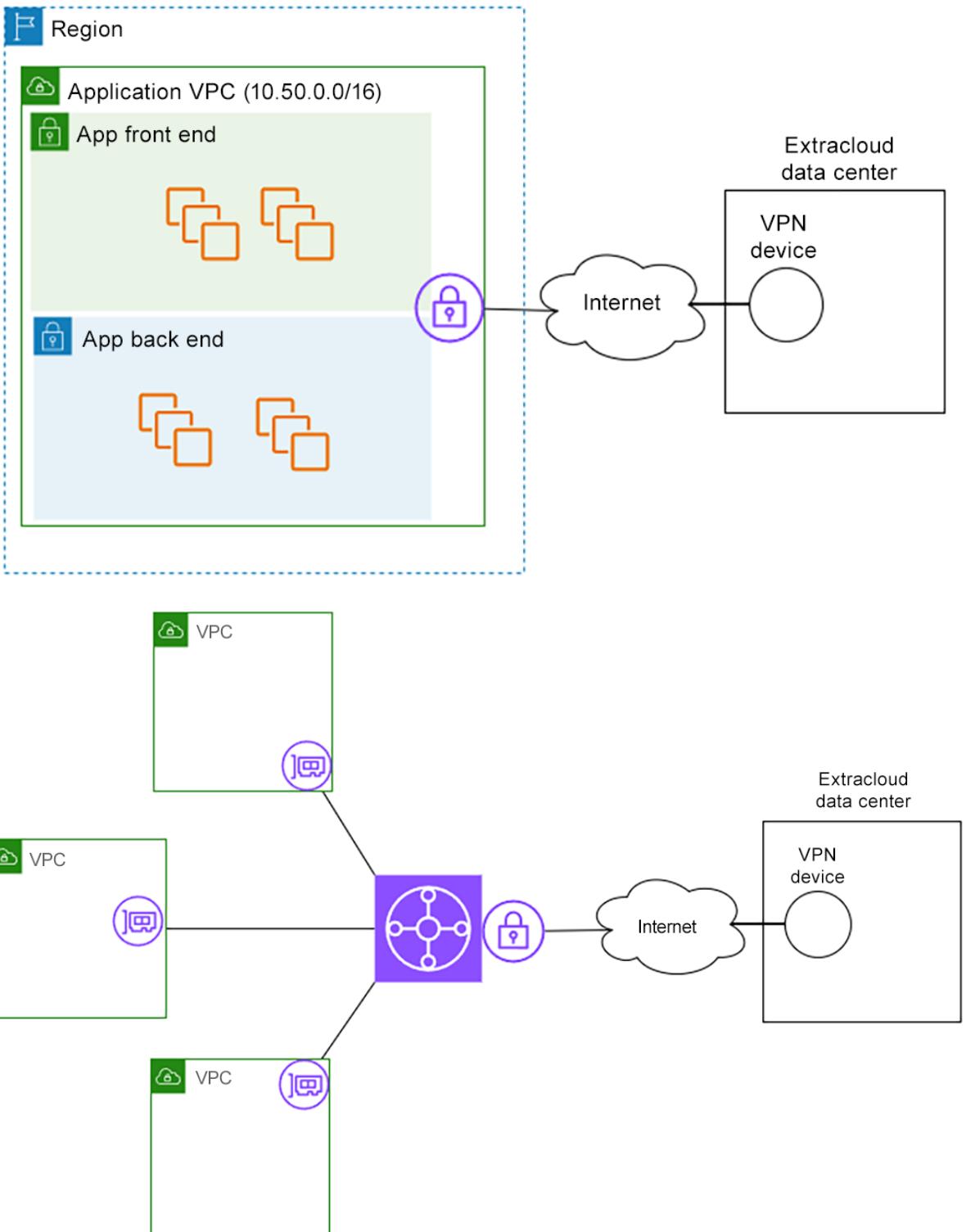
- Dynamic (requires BGP)
- Static

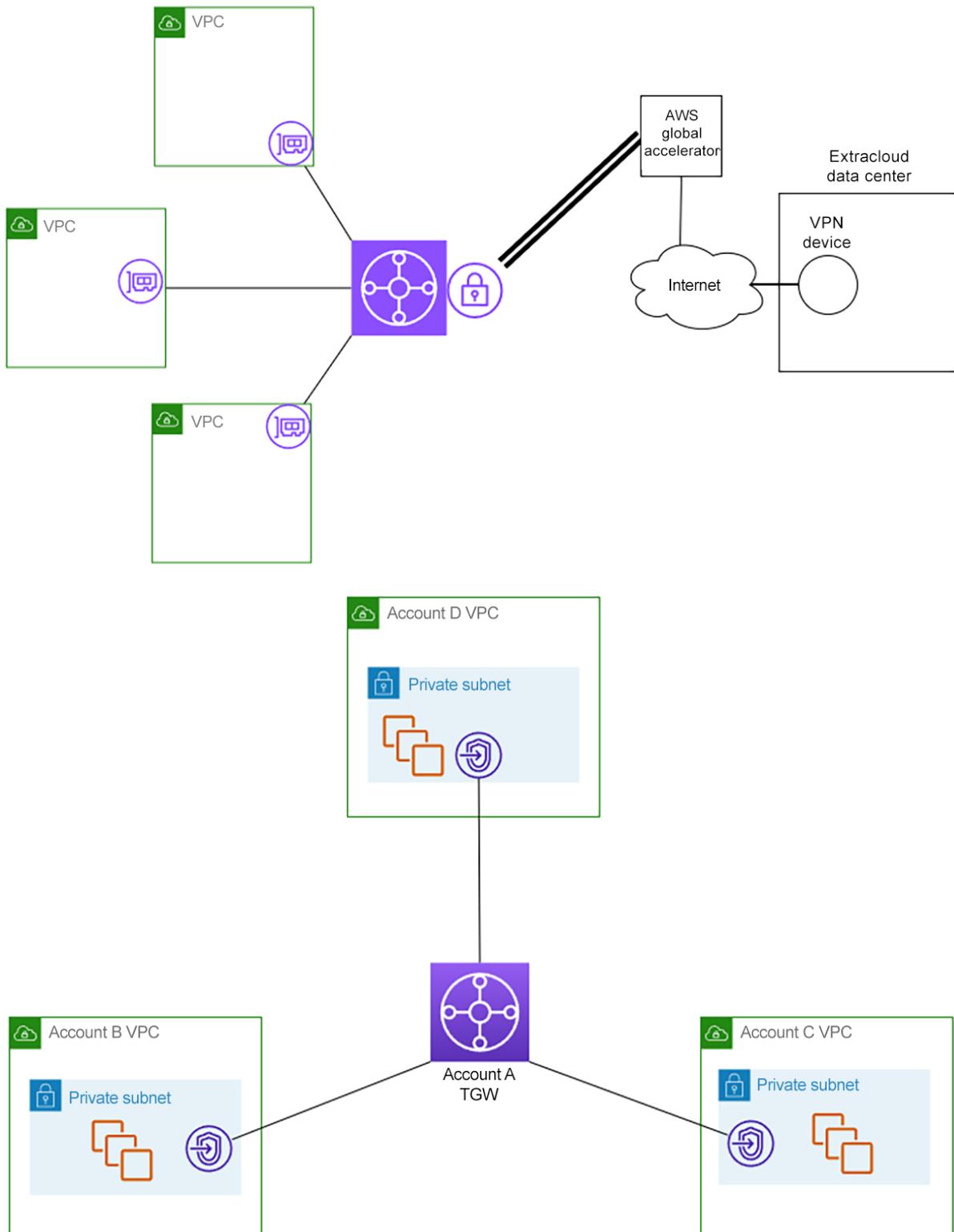
#### Local IPv4 network CIDR - *optional*

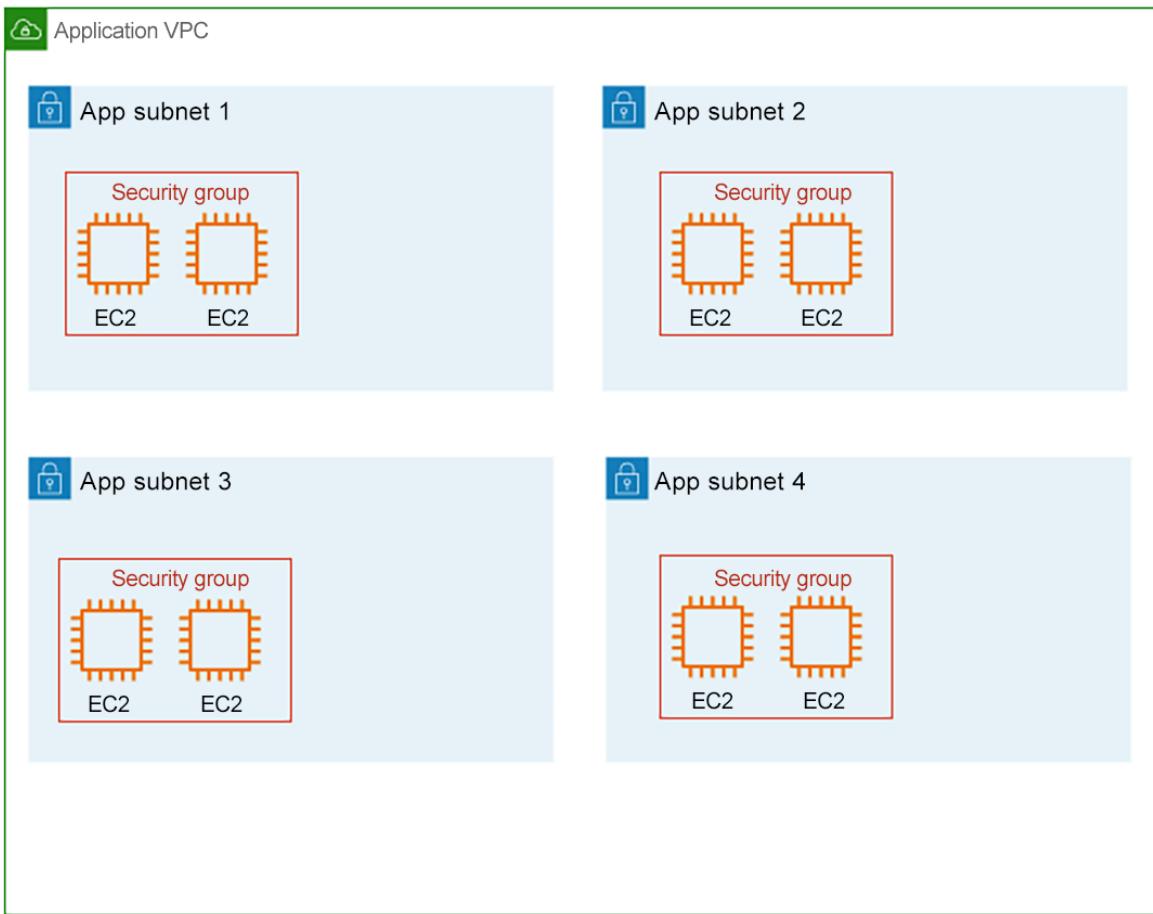
The IPv4 CIDR range on the customer gateway (on-premises) side that is allowed to communicate over the VPN tunnels. The default is 0.0.0.0/0.

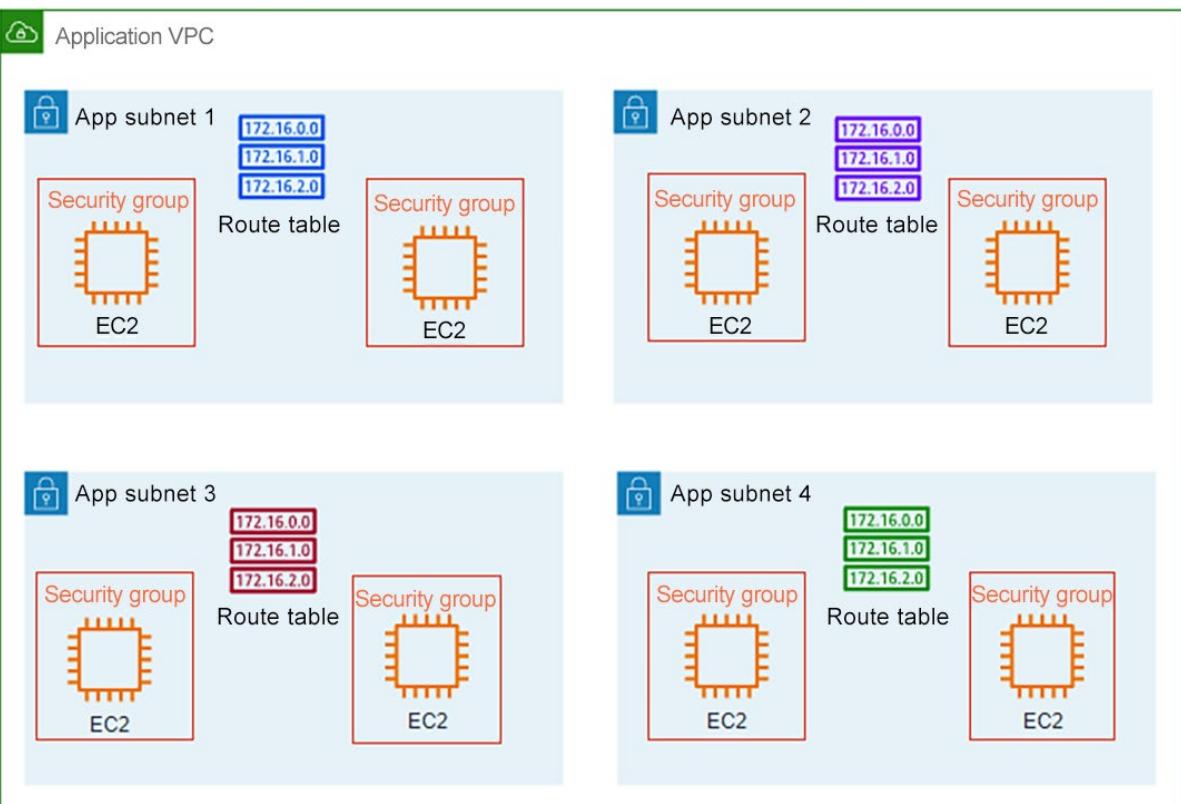
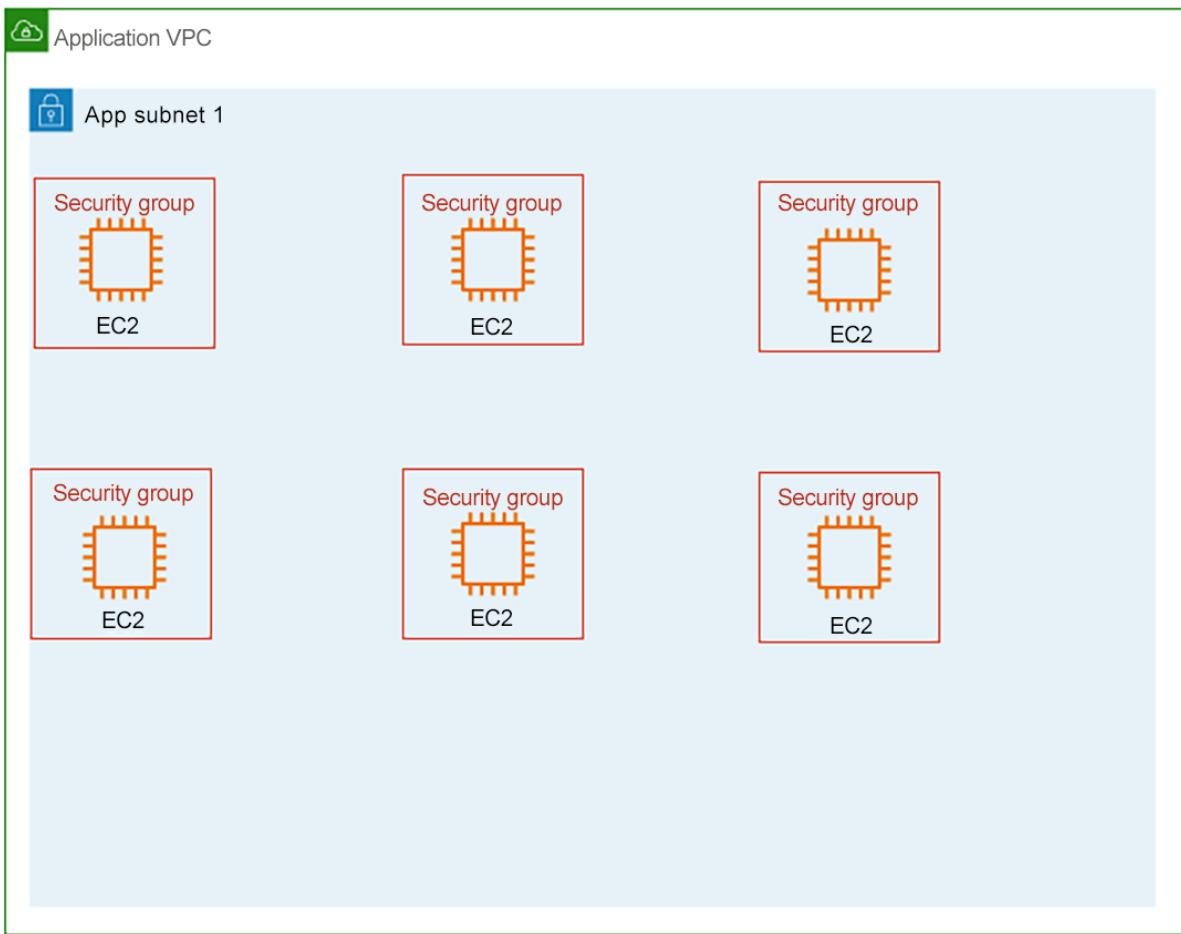
#### Remote IPv4 network CIDR - *optional*

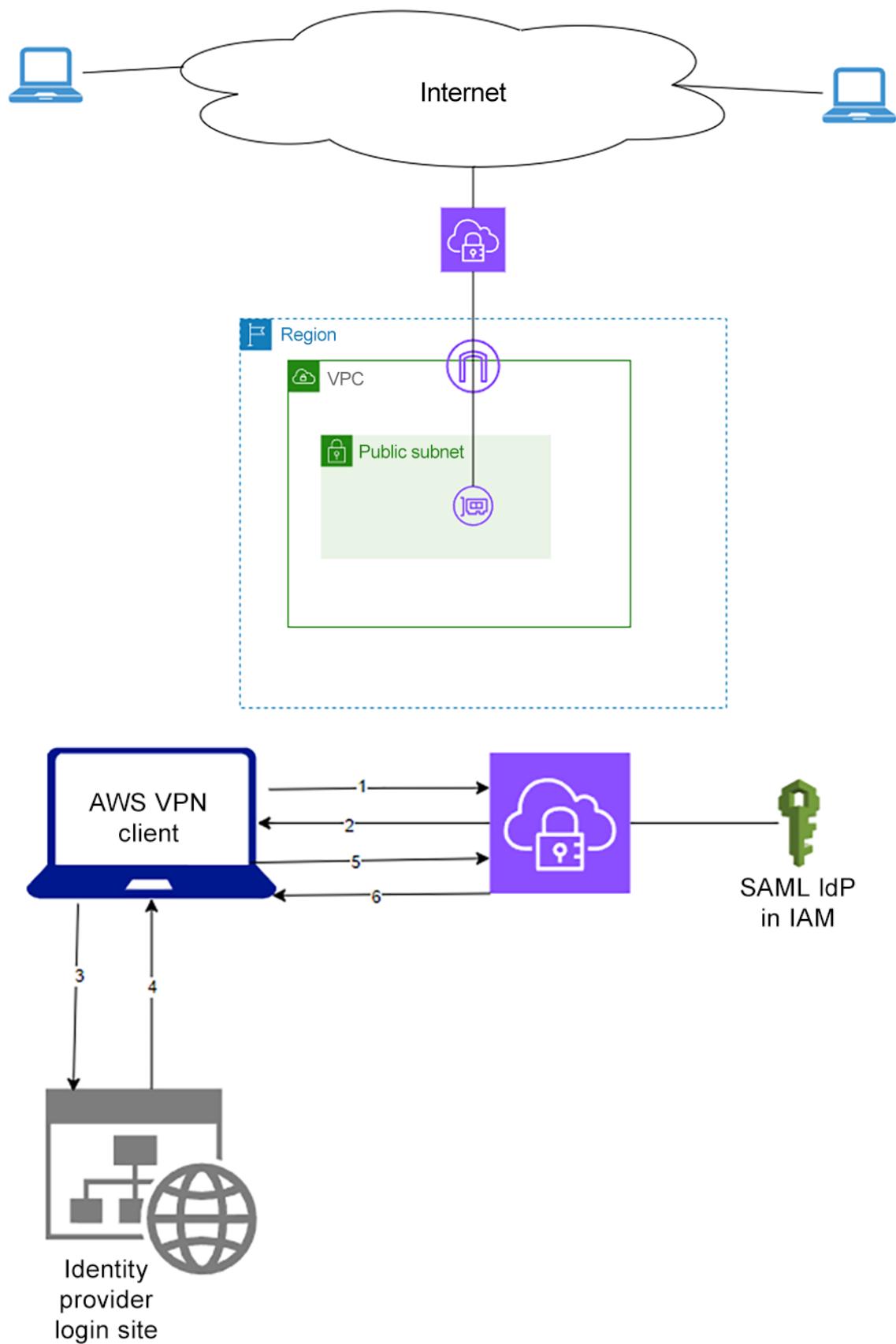
The IPv4 CIDR range on the AWS side that is allowed to communicate over the VPN tunnels. The default is 0.0.0.0/0.

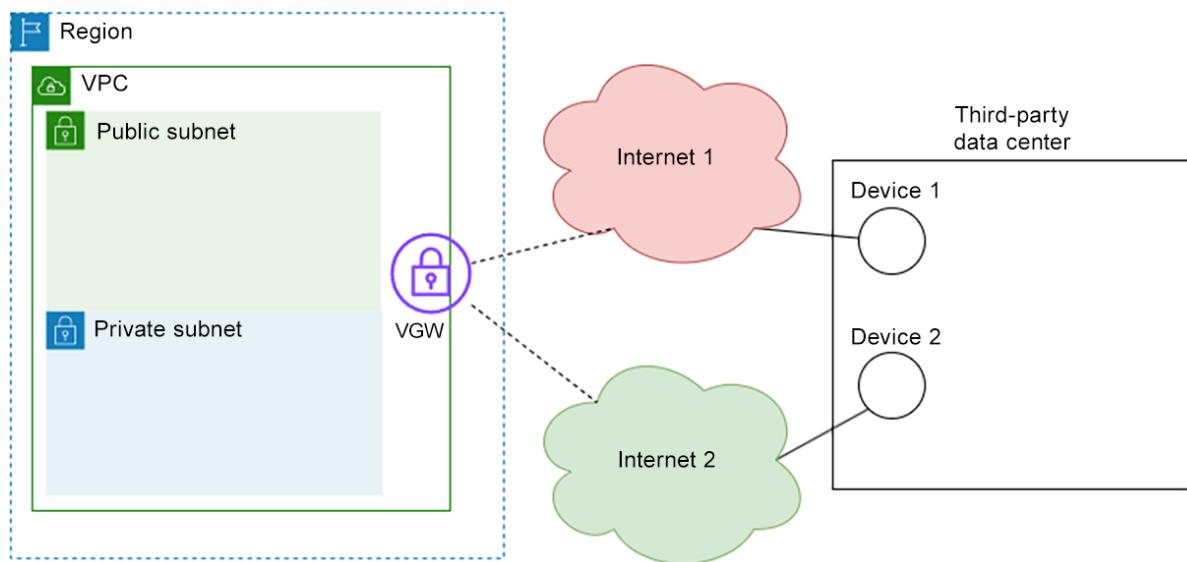
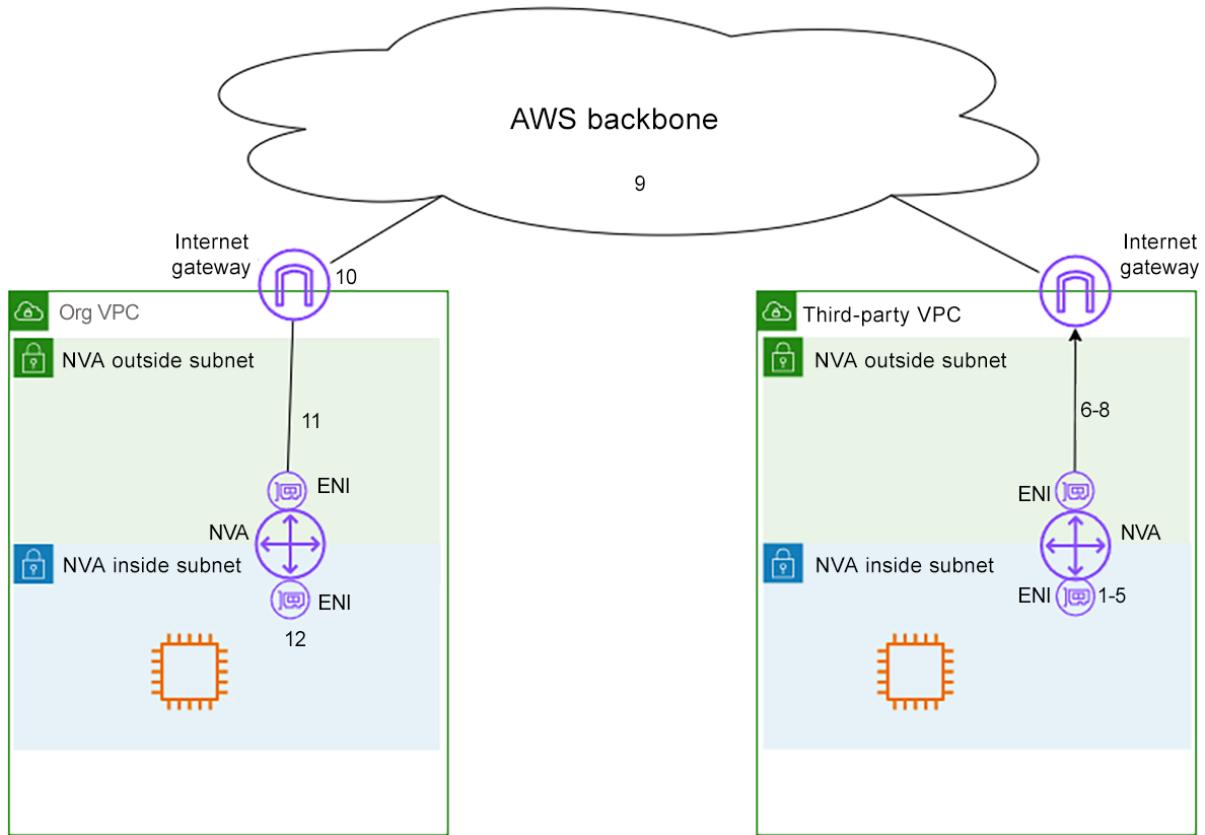


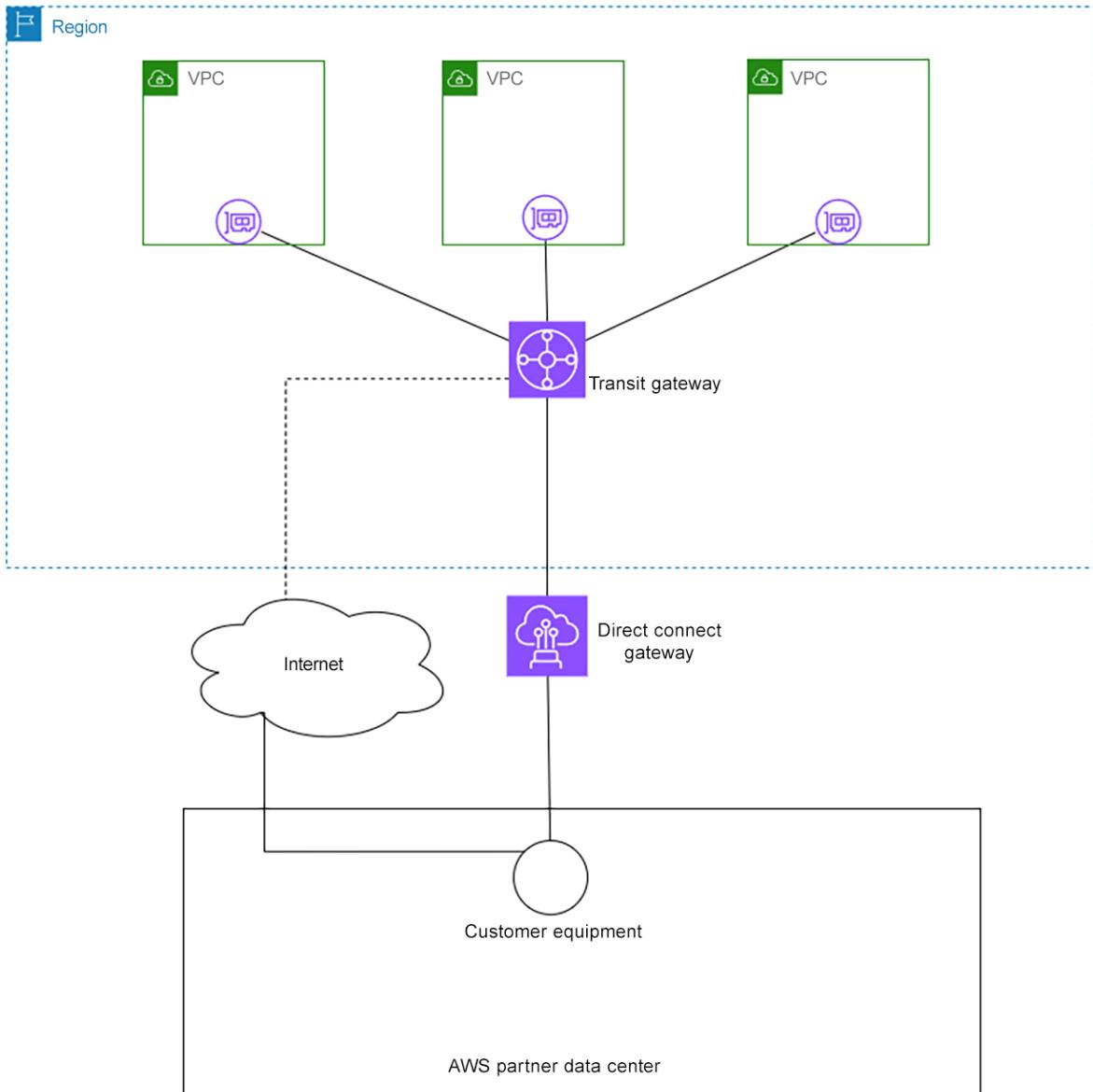


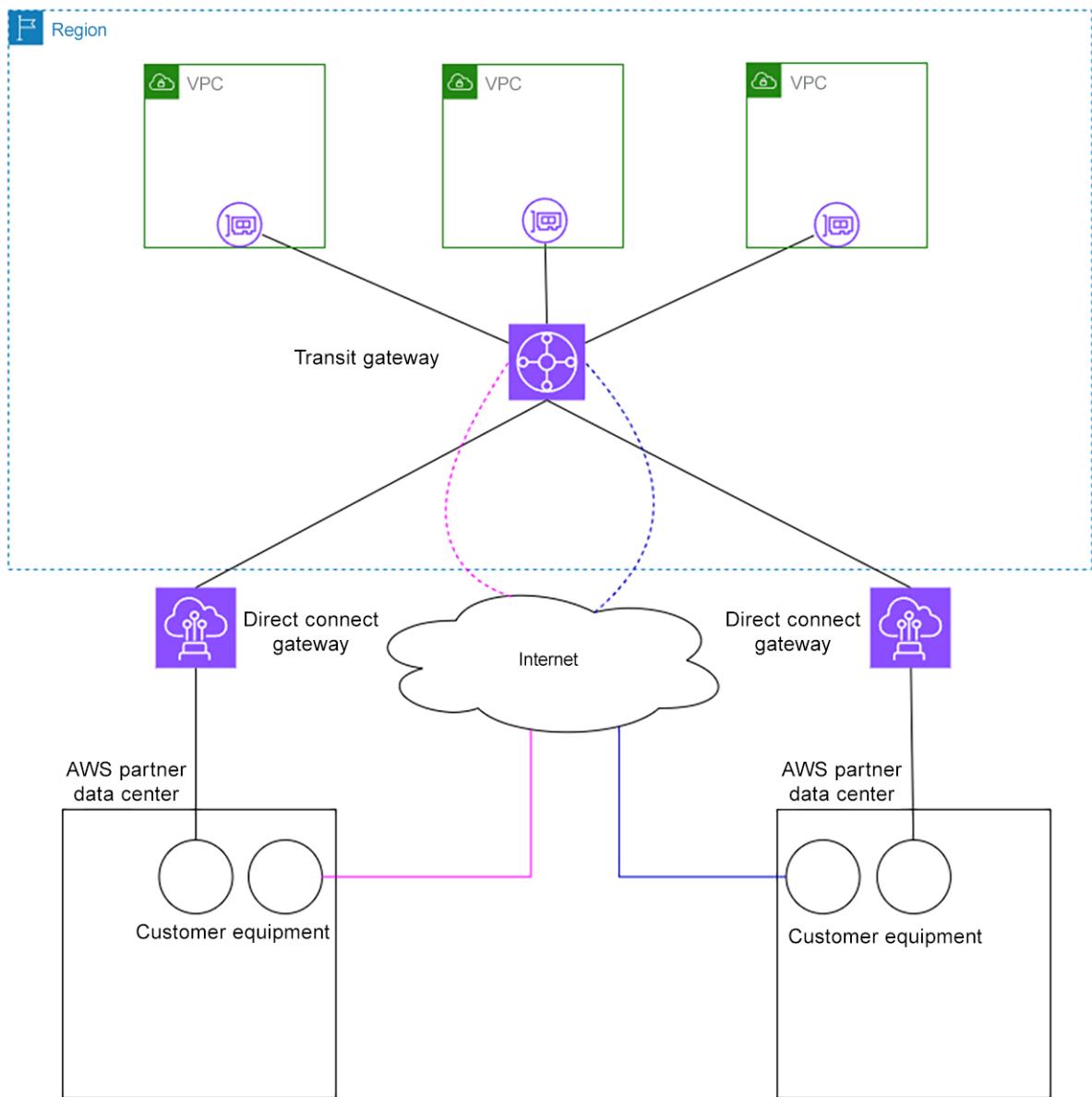


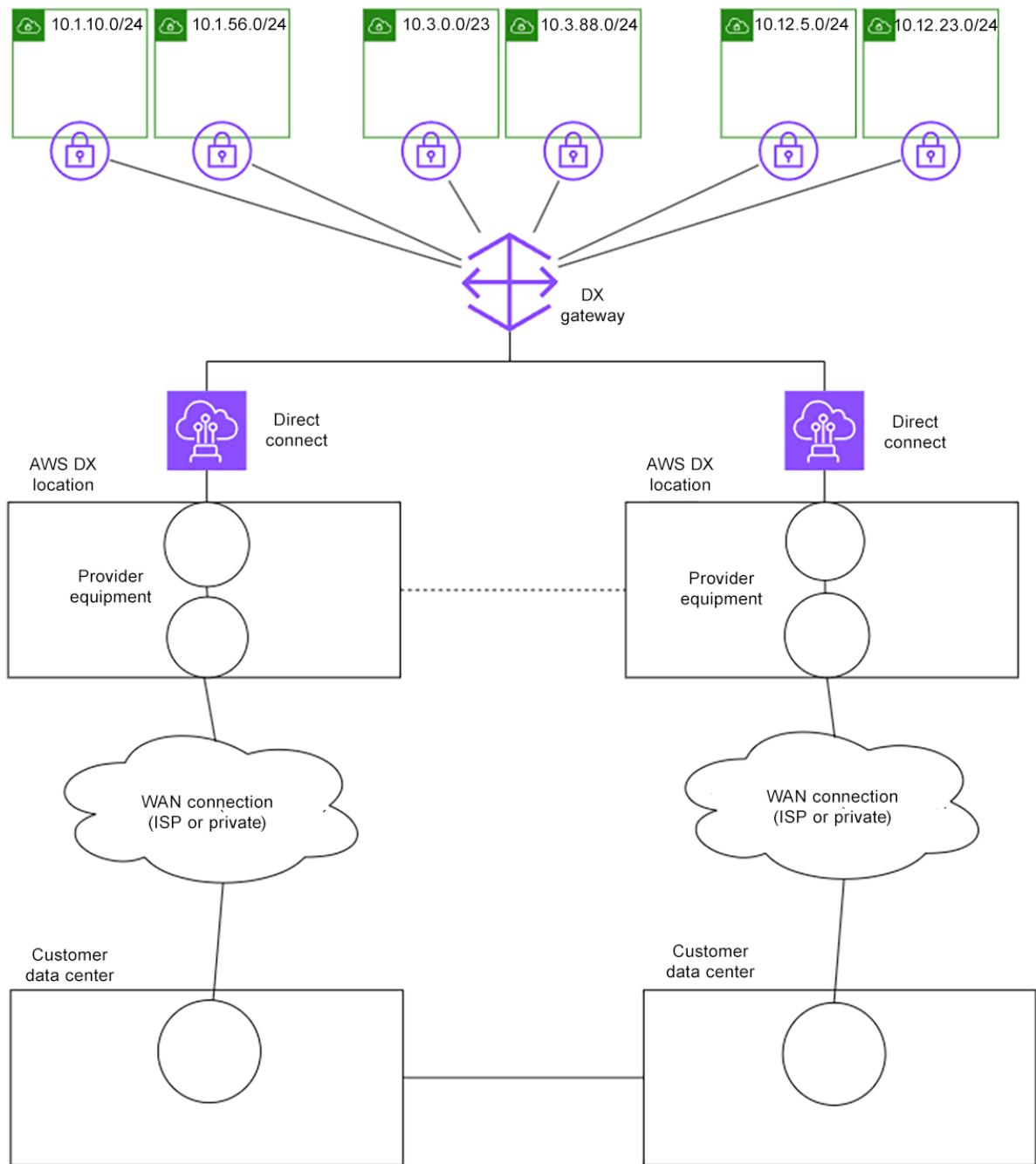


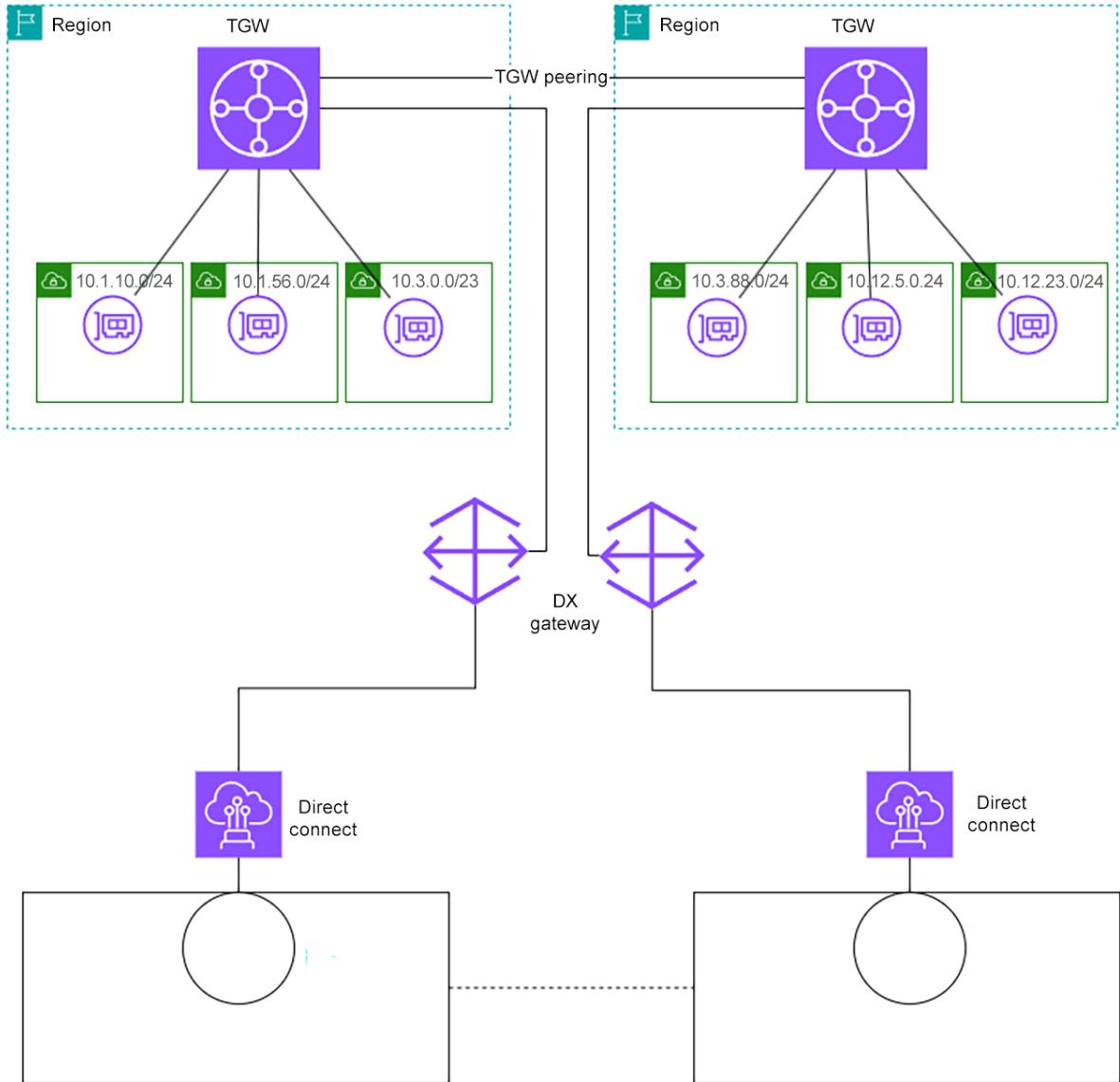


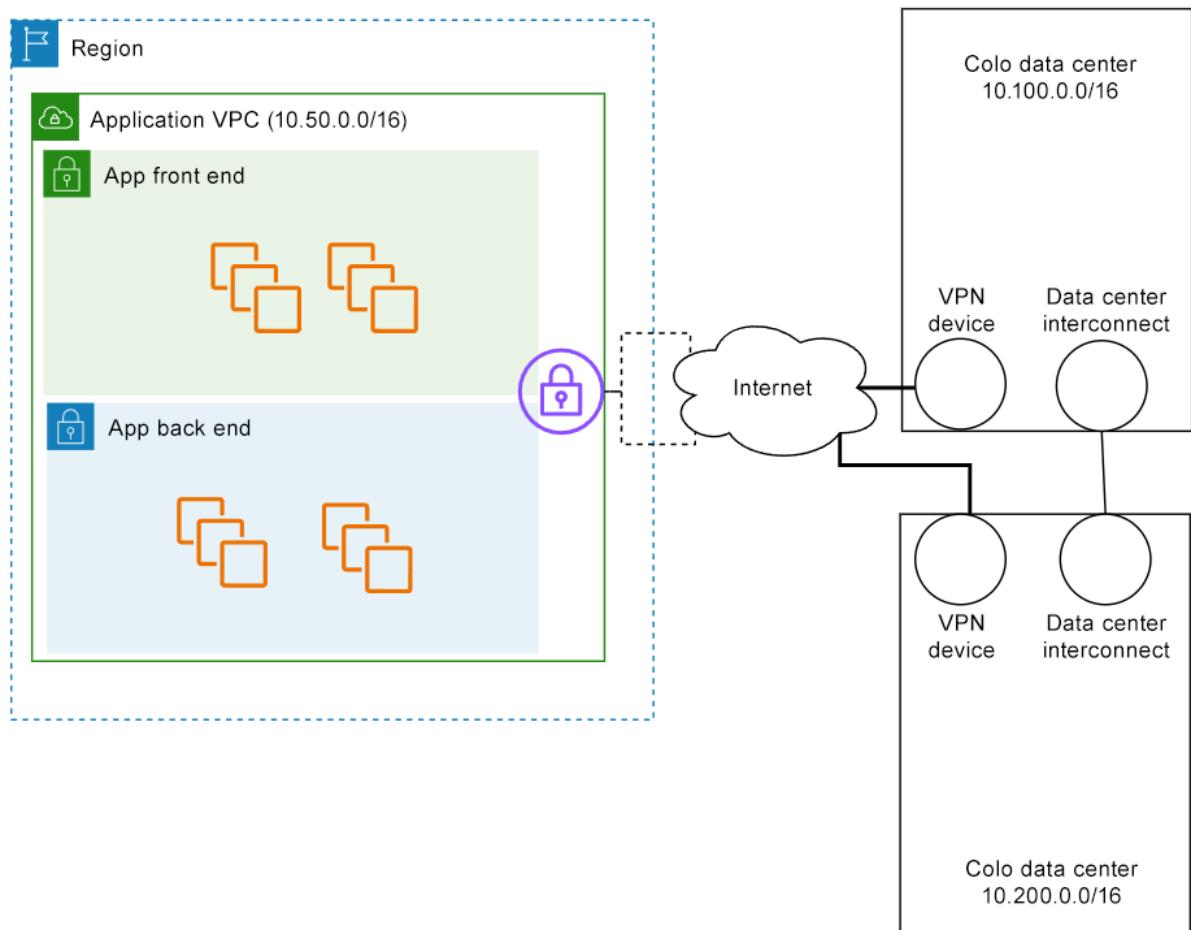
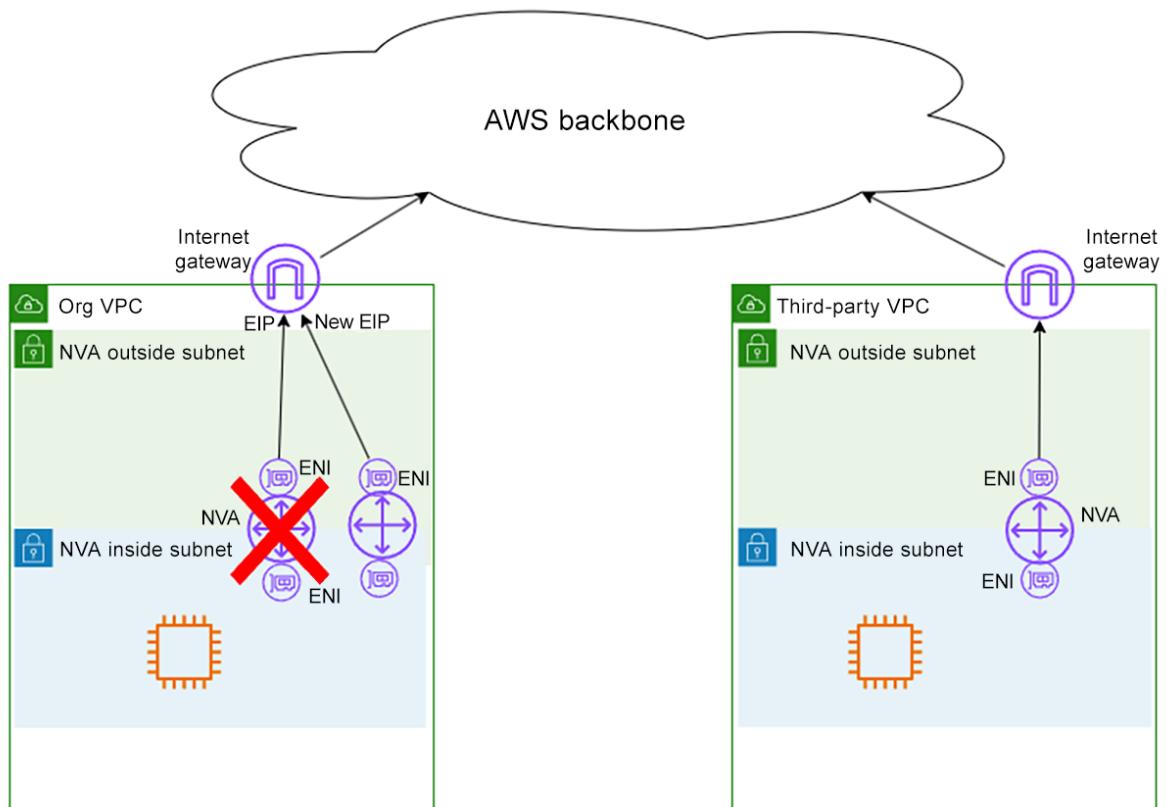


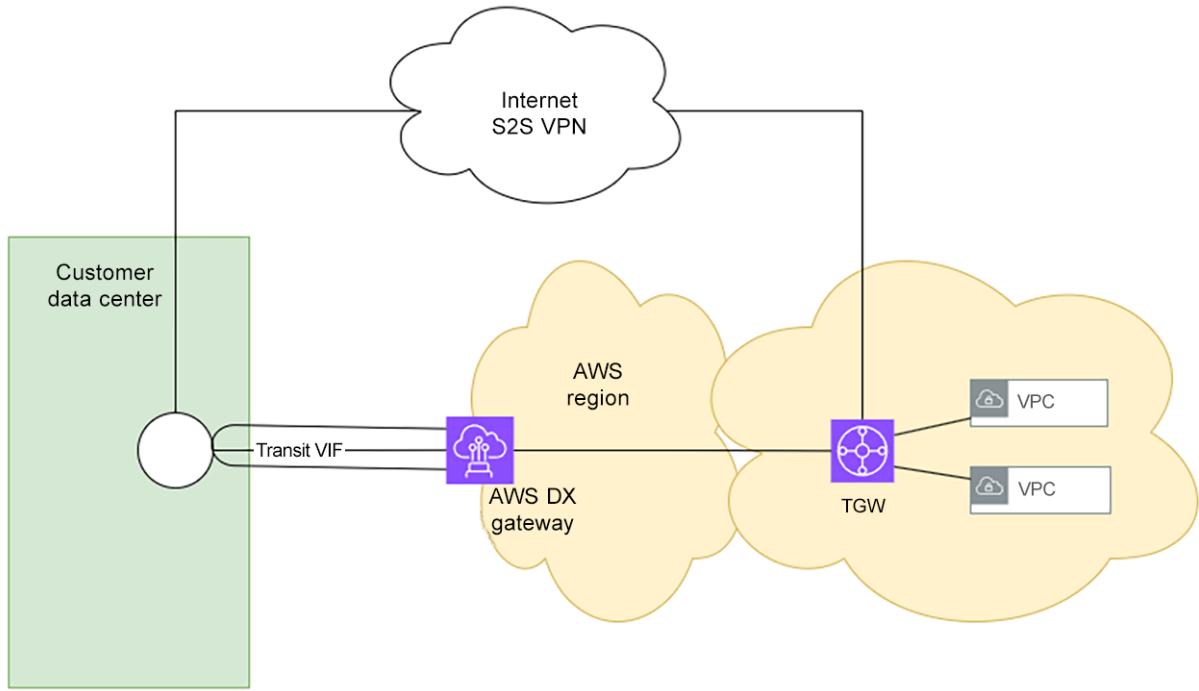


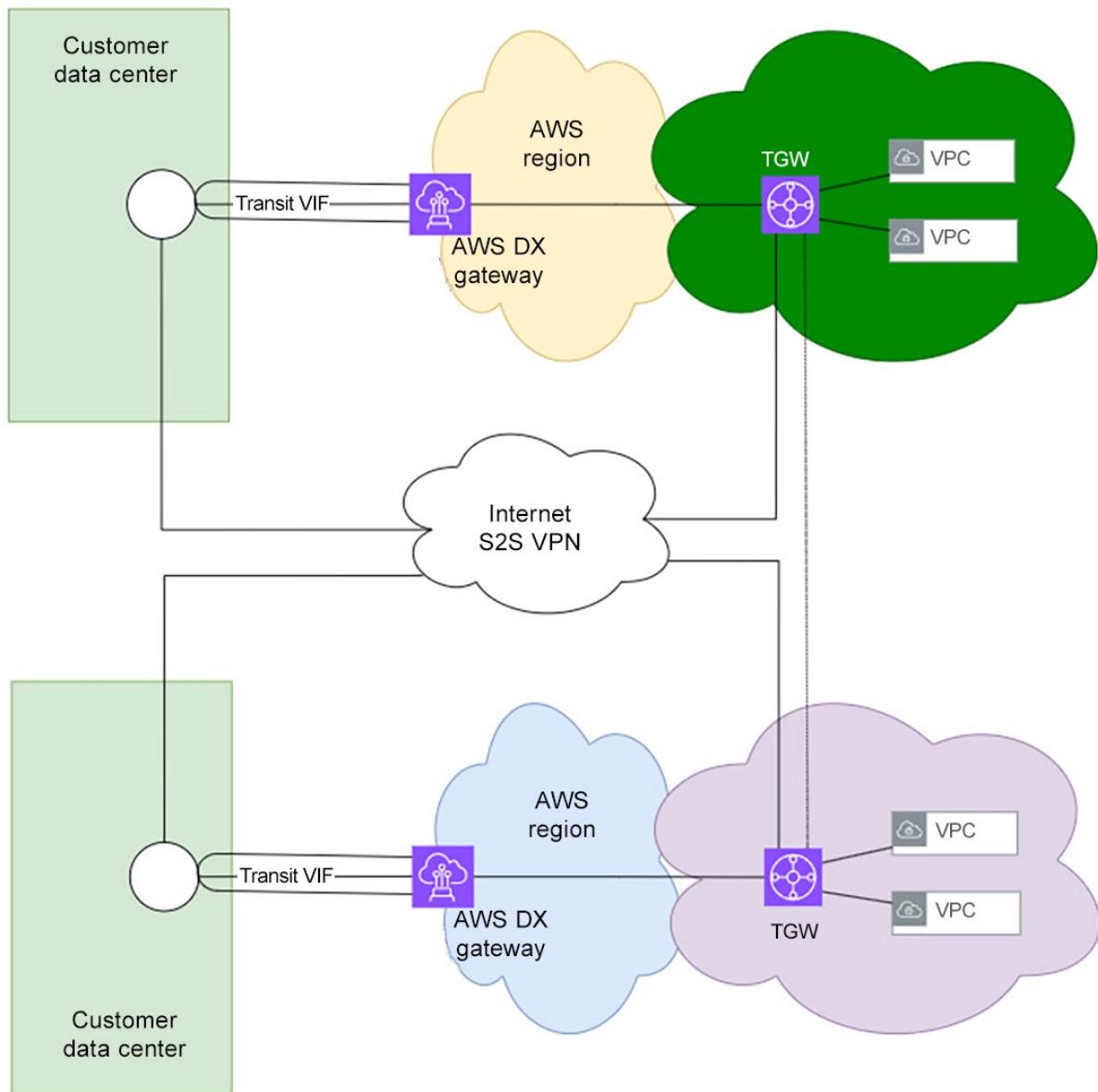




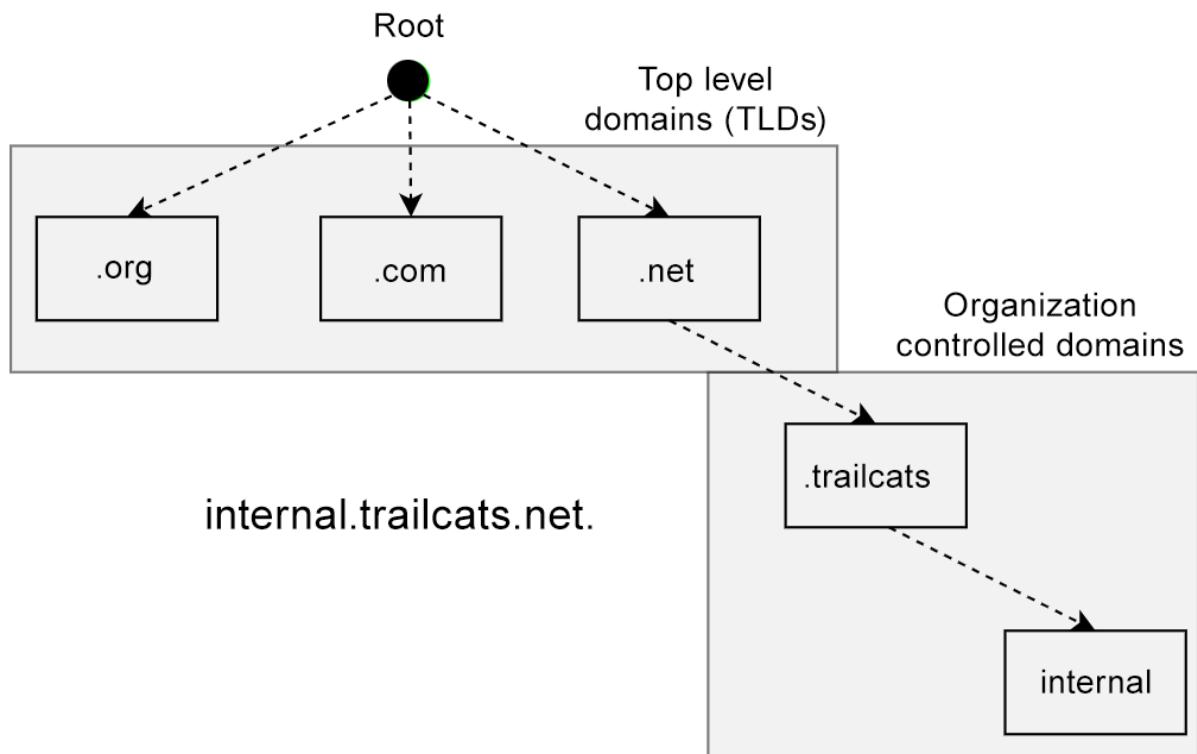








## Chapter 7: AWS Route 53: Basics



```
~ ➔ 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.
```

```

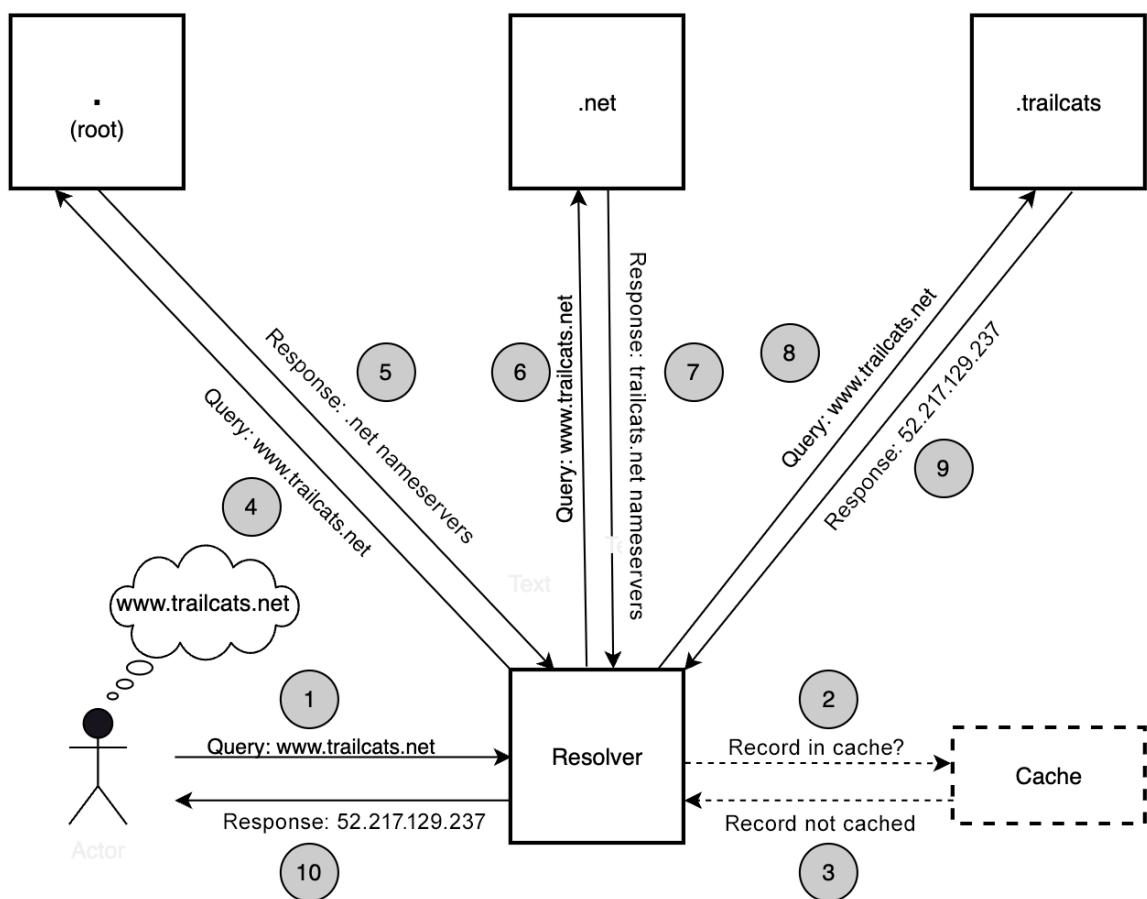
~ dig org. ns

; <>> 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.

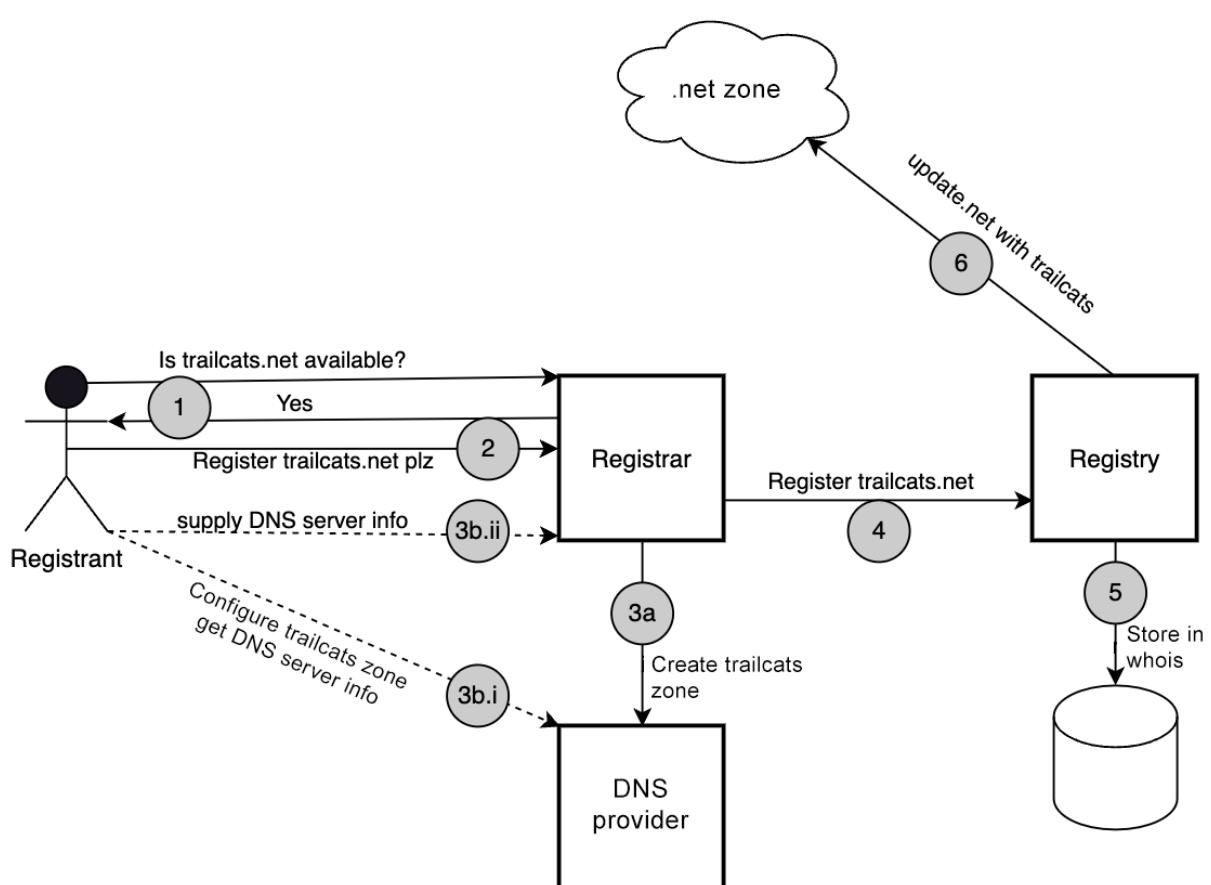
```



```

~/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==
```



Screenshot of the AWS Route 53 console showing the "Register domains" process.

**Left sidebar:**

- Route 53 (highlighted with a red box and circled with a red number 1)
- Dashboard
- Hosted zones
- Health checks
- Profiles New
- IP-based routing
- CIDR collections
- Traffic flow
- Traffic policies
- Policy records
- Domains
- Registered domains (highlighted with a red box and circled with a red number 2)
- Requests
- Resolver
- VPCs
- Inbound endpoints
- Outbound endpoints
- Rules
- Overview (highlighted with a red box and circled with a red number 3)

**Right pane:**

## Register domains Info

Pricing for domain names varies by top-level domain (TLD). For more information, view [price with different TLDs](#).

**Search for domain:** Search for domain (highlighted with a red box and circled with a red number 3) - `packetexample.net` (highlighted with a red box and circled with a red number 4).

**Search result:** Click Select (highlighted with a red box and circled with a red number 5).

Domain	Price/year	Actions
packetexample.net (Exact match)	15.00 USD	Select (highlighted with a red box)

**Suggested available domains (9):**

Domain	Price/year	Actions
packetexample.com	14.00 USD	Select
packetexample.io	71.00 USD	Select

Screenshot of the AWS Route 53 console showing the details of a registered domain.

**Left sidebar:**

- Route 53
- Dashboard
- Hosted zones
- Health checks
- Profiles New
- IP-based routing
- CIDR collections
- Traffic flow
- Traffic policies
- Policy records
- Domains
- Registered domains (highlighted with a red box)

**Right pane:**

## trailcats.net Info

**Details:**

- Registration date: July 28, 2023, 15:21 (UTC-04:00) (highlighted with a red box and circled with a red number 1)
- Expiration date: July 28, 2026 (highlighted with a red box and circled with a red number 2)
- Auto-renew: Off (highlighted with a red box and circled with a red number 3)
- Transfer lock: Off (highlighted with a red box and circled with a red number 4)
- 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

AWS Route 53 dashboard showing the creation of a new hosted zone for `packetexample.net`. The zone is marked as **Public**. A red arrow points from the text "Note that the zone is marked public" to the `packetexample.net` label.

**Hosted zone details:**

- Records (2)**: Contains two records:
  - `packetexample.net` (NS, Simple, TTL 172800)
  - `packetexample.net` (SOA, Simple, TTL 900)
- A new hosted zone has two records:**
  1. Name server
  2. Start of authority

```

~ ➤ 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.

```

The screenshot shows the AWS Route 53 service interface. On the left, a sidebar lists various options: Dashboard, Hosted zones (which is selected and highlighted in blue), Health checks, Profiles, IP-based routing, Traffic flow, Domains, and Resolver. The main content area is titled "Route 53" and shows a "Hosted zones" section. It includes a "Type" dropdown set to "Private hosted zone", a "Description - optional" input field containing "The hosted zone is used for...", and a note stating "This value lets you distinguish hosted zones that have the same name." Below this is a section titled "VPCs to associate with the hosted zone" with a note: "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." A callout box points to the "Add VPC" button with the text "Click here to associate the zone with a VPC".

The screenshot shows the AWS VPC service interface. The navigation path is VPC > Your VPCs > vpc-02139e4fcf609a0dc > Edit VPC settings. The main title is "Edit VPC settings" with an "Info" link. The page is divided into sections: "VPC details", "DHCP settings", and "DNS settings". In the "VPC details" section, the VPC ID is listed as "vpc-02139e4fcf609a0dc" and the Name is "my-vpc-01". In the "DHCP settings" section, the DHCP option set is listed as "dopt-0d605fc1869242513". In the "DNS settings" section, there are two checkboxes: "Enable DNS resolution" (with an "Info" link) and "Enable DNS hostnames" (with an "Info" link). A red arrow points to the "Enable DNS hostnames" checkbox, and a red callout box with the text "Needed for private hosted zones" is positioned above it.

Screenshot of the AWS Route 53 console showing a newly created hosted zone.

The hosted zone is named **packetexample.net** and is designated as **Private**.

**Note that the zone is designated private**

The records table shows two entries:

Record name	Type	Routing policy	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

Screenshot of the AWS Route 53 console showing a newly created record.

The record is named **wwwin** and is of type **A**.

**Newly Created A Record**

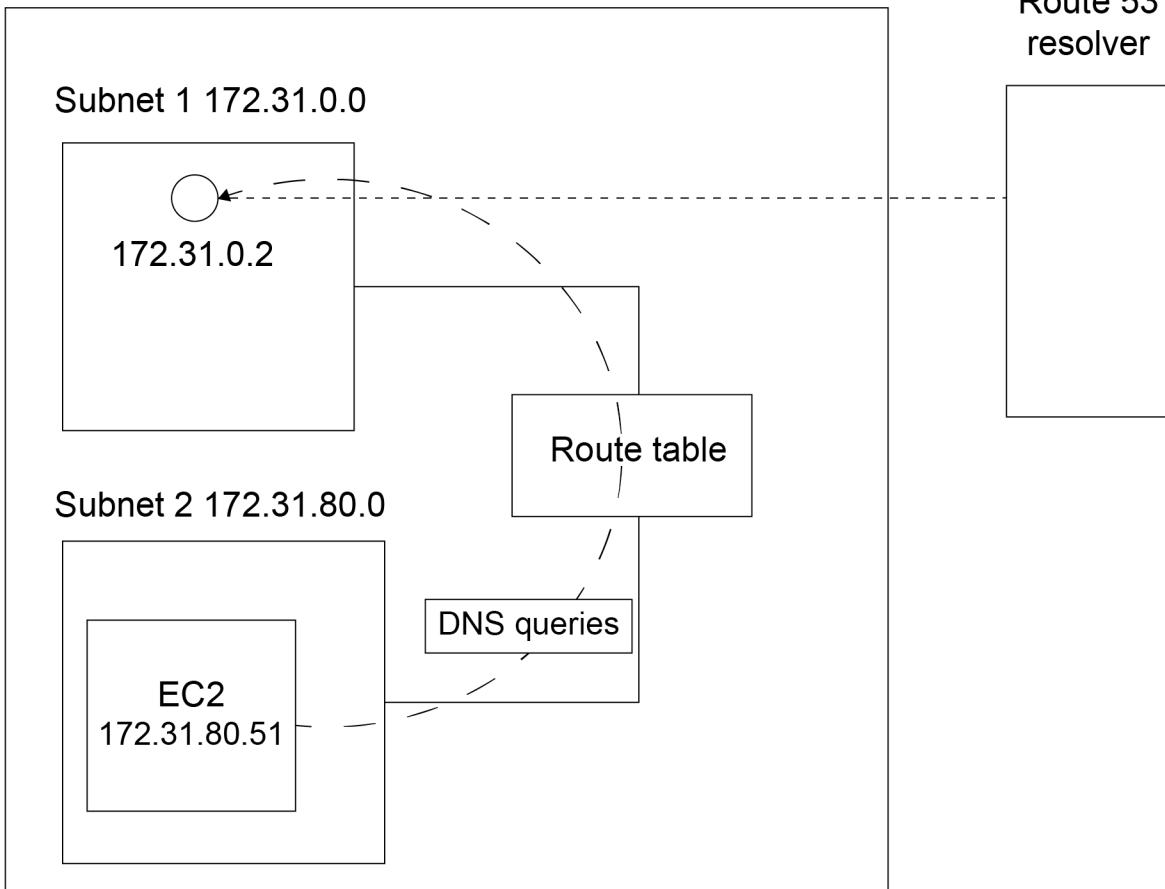
The records table shows one entry:

Record name	Type	Routing policy	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

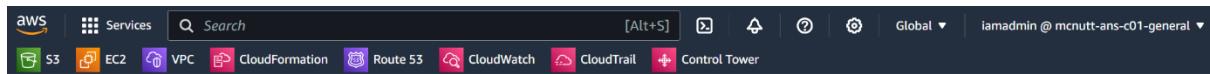
CIDR: 172.31.0/16

Route 53  
resolver



Screenshot of the AWS Route 53 Health checks page:

- Left sidebar:** Shows navigation links for Route 53, Hosted zones, Health checks (selected), Profiles (New), IP-based routing, CIDR collections, Traffic flow, Traffic policies, and Policy records.
- Right panel:** Title: [Route 53](#) > [Health checks](#). Subtitle: **Health checks (0)** [Info](#). Description: "Route 53 health checks monitor the health and performance of your application's servers and endpoints." A red arrow points to the **Create health check** button.
- Table:** Displays a table with columns: ID, Name, Details, Status, Alarm, State, and Actions. The table shows: "No health checks to display."



## 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

- 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

Simple TCP check

Protocol

Domain name \*

Port \*

[Advanced configuration](#)

URL

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

Domain name \*

Port \*

Test to see if resources on server is available

Path

[Advanced configuration](#)

Request interval  Standard (30 seconds)  Fast (10 seconds)

Failure threshold \*

String matching  No  Yes

Latency graphs

10-second checks are an upcharge

Invert health check status

Disable health check  By default, disabled health checks are considered healthy. [Learn more](#)

Health checker regions  Customize  Use recommended

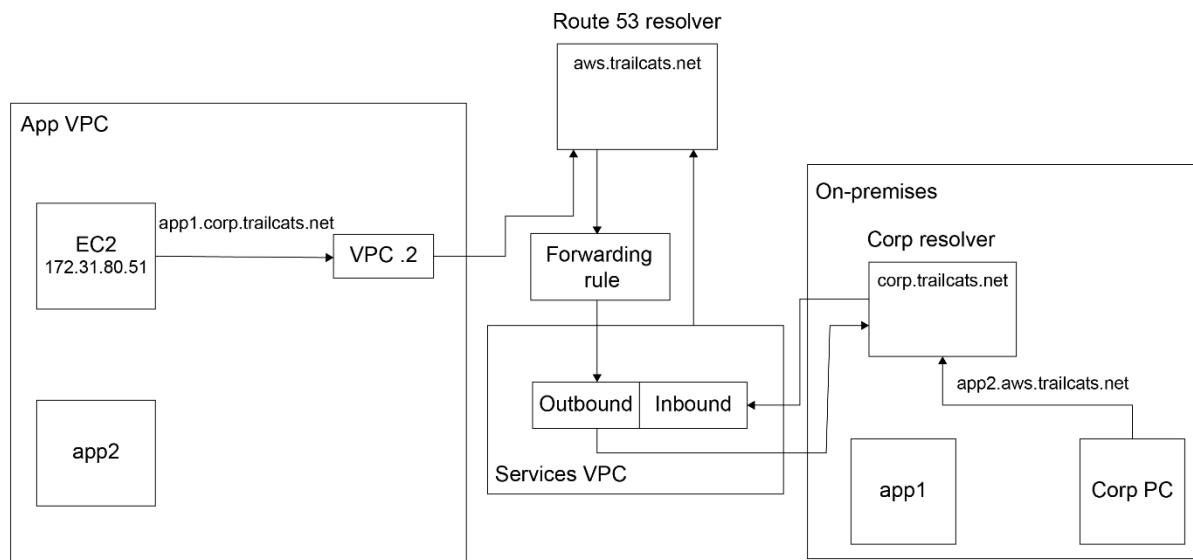
US East (N. Virginia)

US West (N. California)

US West (Oregon)

Select regions

## Chapter 8: AWS Route 53: Advanced



Create traffic policy "booking.trailcats.net" v1    Import traffic policy

**Start point**

DNS type: A: IP address in IPv4 format

**Geoproximity rule**

Region: 1

Endpoint Location: US East (N. Virginia)

Coordinates: Using US East (N. Virginia) Coordinates

**Geoproximity map**

1. North America (blue)

2. Asia (red)

3. Europe (yellow)

4. Australia/Oceania (teal)

5. South America (orange)

**AWS Management Console - Route 53 Requests**

Route 53 > Requests

**Requests**

Operation ID	Domain name	Message	Status	Type	Submitted
d7d0f19d-7aeb-4754-8857-bcc30fa2378a	trailcats.net	-	Successful	Renew domain	July 28, 2024, 13:06 (UTC-04:00)
7e77f247-b443-4766-b903-09c6892b9efc	trailcats.net	-	Successful	Add DNSSEC	August 24, 2023, 07:53 (UTC-04:00)
1452dcff-88e8-41f3-a05d-4f12742eb5b8	trailcats.net	-	Successful	Remove DNSSEC	August 13, 2023, 10:35 (UTC-04:00)
b6550037-a383-					August 05,

1. Requests

2. Domain name

3. Status

4. Type

Screenshot of the AWS Route 53 service dashboard.

The left sidebar shows the following navigation:

- Route 53
- Dashboard
- Hosted zones** (highlighted with a green box)
- Health checks
- Profiles [New](#)
- ▼ IP-based routing
- CIDR collections
- ▼ Traffic flow
- Traffic policies
- Policy records
- ▼ Domains
- Registered domains
- Requests
- ▼ Resolver
- VPCs
- Inbound endpoints

The main content area shows the "Hosted zones" page with the following details:

Route 53 > Hosted zones

**Hosted zones (1/6)**

Hosted zone name	Type	Create...
trailcats.net	Public	Route 53
trailcats.net	Private	Route 53
west.trailcats.net	Private	Route 53

Actions available: [View details](#) (highlighted with a green box), [Edit](#), [Delete](#).

Red annotations:

- Red arrow pointing to the "Hosted zones" link in the sidebar.
- Red arrow pointing to the "Hosted zones" link in the breadcrumb.
- Red arrow pointing to the "View details" button in the top bar.

Screenshot of the AWS Route 53 service dashboard, showing the "Hosted zones" details for "trailcats.net".

The left sidebar shows the following navigation:

- Route 53
- Dashboard
- Hosted zones** (highlighted with a green box)
- Health checks
- Profiles [New](#)
- ▼ IP-based routing

The main content area shows the "trailcats.net" hosted zone details:

Route 53 > Hosted zones > **trailcats.net**

**trailcats.net** [Info](#)

Actions available: [Delete zone](#), [Test record](#), **Configure query logging** (highlighted with a green box).

Red annotations:

- Red arrow pointing to the "Hosted zones" link in the sidebar.
- Red arrow pointing to the "Hosted zones" link in the breadcrumb.
- Red arrow pointing to the "Configure query logging" button.

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** Info

You can choose the name of an existing log group or choose to create a new log group.

**Create log group** C

**New log group name**

**Route53PublicZones**

The log group can have up to 512 characters. Valid characters: a-z, A-Z, 0-9, and . \_ / # - (hyphen)

**Permissions - optional**

**Cancel** **Create**

aws Services Search [Alt+S]

S3 EC2 VPC CloudFormation Route 53 CloudWatch CloudTrail Control Tower

CloudWatch X

Favorites and recents

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)**

By default, we only load up to 10000 log groups.

**Filter log groups or try prefix search**

Log group	Log class	Anomaly d...
<b>Route53PublicZones</b>	Standard	<b>Configure</b>

The screenshot shows the AWS CloudWatch Log Streams interface. At the top, there are tabs for Log streams, Tags, Anomaly detection, Metric filters, Subscription filters, Contributor Insights, and Data processing. The Log streams tab is selected. Below the tabs, there is a search bar with a placeholder 'Filter log streams or try prefix search'. To the right of the search bar are checkboxes for 'Exact match' and 'Show expired'. A red arrow points to the 'route53-test-log-stream' entry in the list, which is highlighted with a green box. The list also includes a 'Log stream' entry with a checkbox.

The screenshot shows the AWS CloudWatch Log Events interface for the 'route53-test-log-stream'. The URL in the browser is 'CloudWatch > Log groups > Route53PublicZones > route53-test-log-stream'. At the top, there are buttons for Actions, Start tailing, and a filter bar with a placeholder 'Filter events - press enter to search'. Below the filter bar are time controls for '1m', '1h', and 'UTC timezone'. The main area shows a table with columns for 'Timestamp' and 'Message'. A message is displayed: 'No older events at this moment. [Retry](#)'. Below this is a log entry: '2024-08-01T01:36:46.050Z Route 53 created a test log event'. A red arrow points to this log entry, which is highlighted with a green box. Below the log entry, a message says 'No newer events at this moment. Auto retry paused. [Resume](#)'.

The screenshot shows the AWS Route 53 Resolver Query logging configuration interface. The URL in the browser is 'Route 53 > Resolver > Query logging'. The top navigation bar includes links for S3, EC2, VPC, CloudFormation, Route 53, CloudWatch, CloudTrail, and Control Tower. The Region selector shows 'N. Virginia'. A red arrow points to the 'Query logging' link in the left sidebar, which is highlighted with a green box and circled with a red number 1. In the main content area, a message says '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.' A red arrow points to the 'Configure query logging' button, which is highlighted with an orange box and circled with a red number 3. Below the message, it says 'Query logging configurations (0)' and 'No configurations'. A red arrow points to the 'Configure query logging' button in the 'Query logging configurations' section, which is highlighted with an orange box and circled with a red number 2.

## 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

C

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.

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-02139e4cf609a0dc

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

2

Close

Add

**VPCs to log queries for - optional (3)** [Info](#)

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.

	VPC ID	VPC name	Status	IPv4 CIDR	IPv6 CIDR	Owner
<input type="checkbox"/>	vpc-02139e4fcf609a0dc	my-vpc-01	<span>Active</span>	10.0.0.0/24	-	36103
<input type="checkbox"/>	vpc-0d5d33e6fb379bf47	-	<span>Active</span>	172.31.0.0/16	-	36103
<input type="checkbox"/>	vpc-0fd250b4d3b990ae4	security-vpc-vpc	<span>Active</span>	10.254.0.0/16	-	36103

**Tags - optional** [Info](#)

No tags associated with the resource.

[Add tag](#)

You can add up to 50 more tags.

[Cancel](#) [Configure query logging](#)

**(1) You successfully created the log group Route53Resolver.**

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 (1)** [Info](#)

Name	ID	Status	Destination type	Destination ARN
<a href="#">ResolverQueryConfiguration</a>	rqlc-1e201b76e5a140c5	<span>Created</span>	CloudWatch Logs	arn:aws:logs:us-east-1:36103702889:log-group:Route53Resolver

S3 EC2 VPC CloudFormation Route 53 CloudWatch CloudTrail Control Tower

### CloudWatch Log groups (2)

Log group Route53PublicZones Route53Resolver

S3 EC2 VPC CloudFormation Route 53 CloudWatch CloudTrail Control Tower

### Route53Resolver Log group details

Log streams (841) log\_stream\_created\_by\_aws\_to\_validate\_log\_delivery\_subscriptions

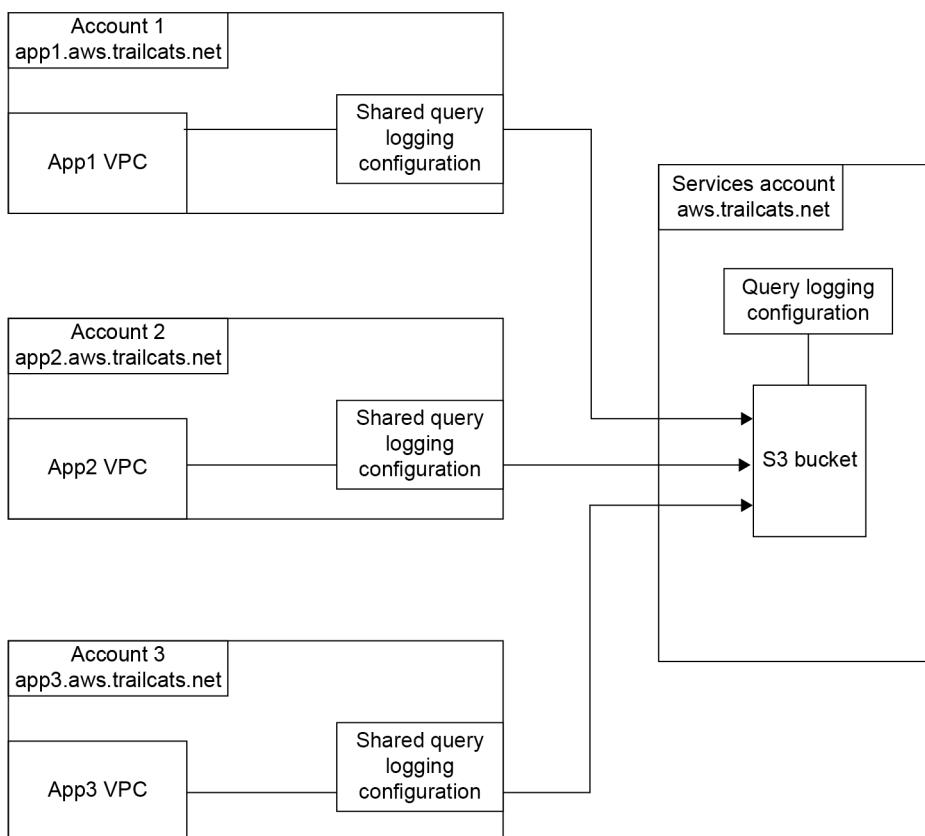
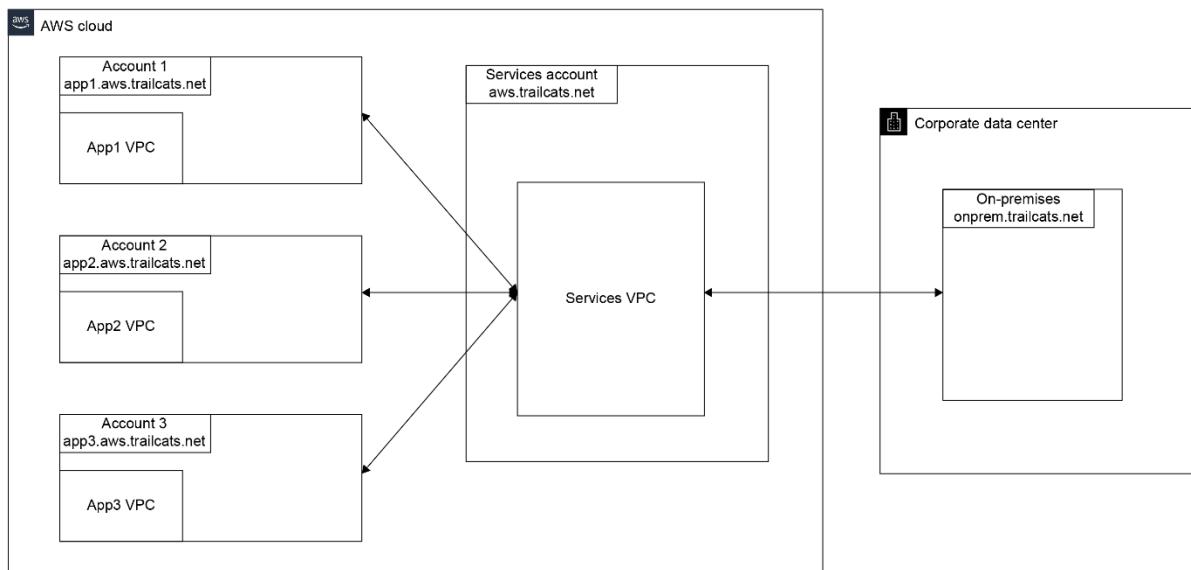
CloudWatch Log groups Route53Resolver log\_stream\_created\_by\_aws\_to\_validate\_log\_delivery\_subscriptions

### Log events

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 ...



S3 EC2 VPC CloudFormation Route 53 CloudWatch CloudTrail Control Tower

Route 53 > Resolver > Query logging > ResolverQueryConfiguration

**ResolverQueryConfiguration configuration**

ID	Status	Sharing status
rqlc-1e201b76e5a140c5	Created	Not shared
Destination type	VPC count	Owner
CloudWatch Logs log group	3	361037072889
Destination ARN	Creation time (UTC)	ARN
arn:aws:logs:us-east-1:361037072889:log-group:Route53Resolver	2024-08-02T03:07:14.69898948Z	arn:aws:route53resolver:us-east-1:361037072889:resolver-query-log-config/rqlc-1e201b76e5a140c5

**VPCs that queries are logged for (3)**

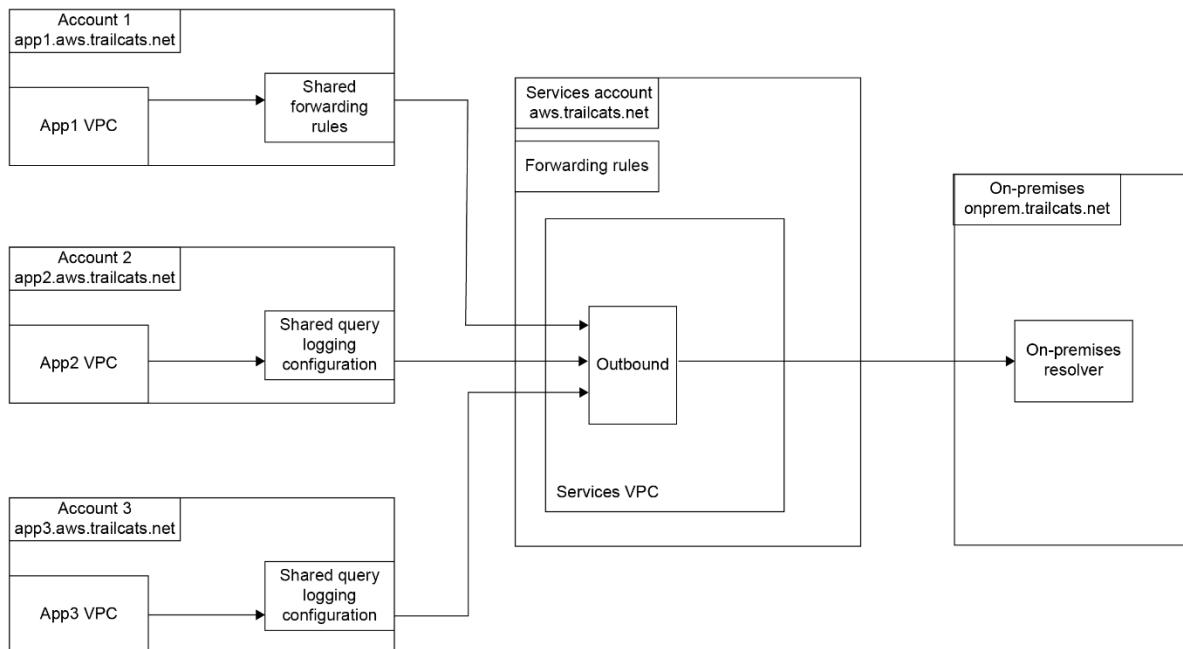
View details Stop logging queries Add VPC

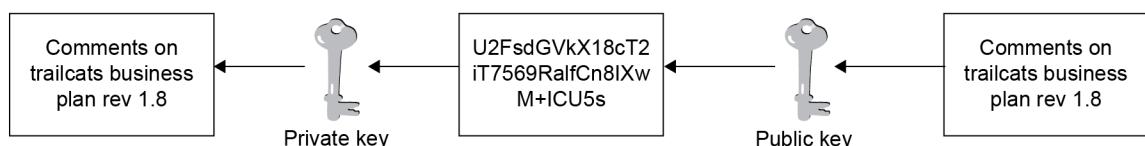
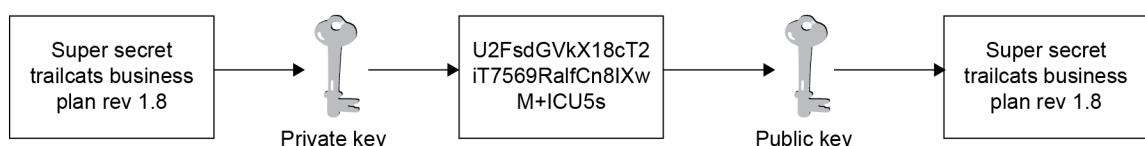
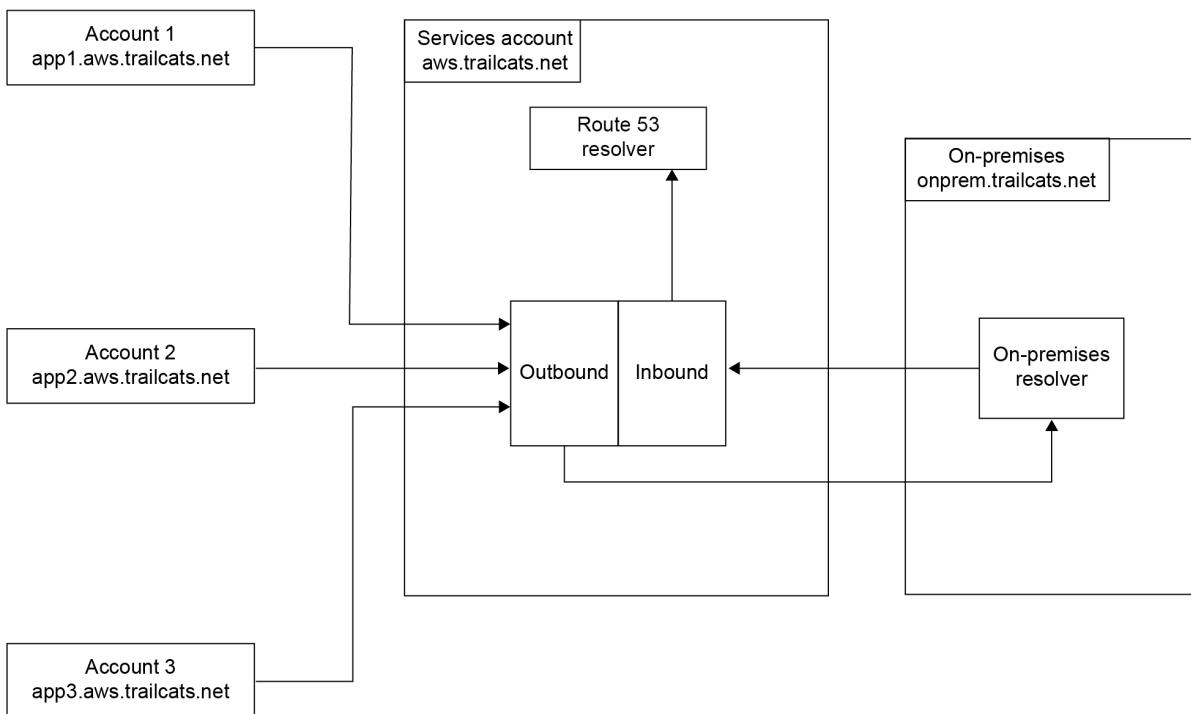
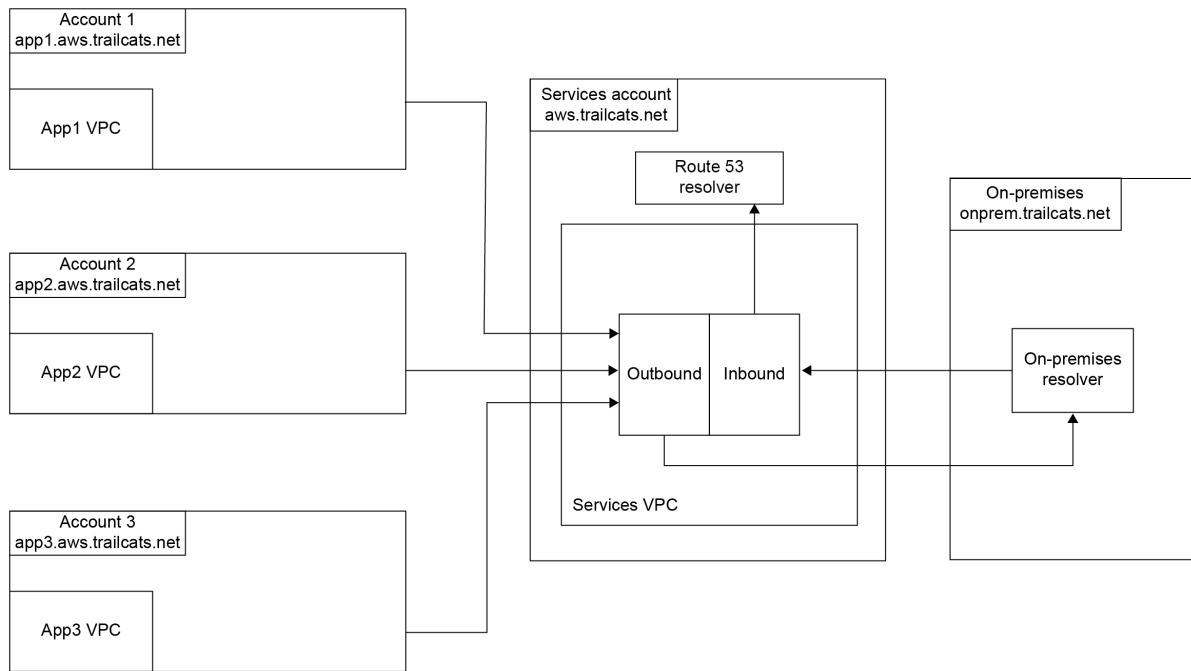
Resolver logs DNS queries that originate in the VPCs that you choose here. If you don't choose any VPCs, Resolver doesn't log any queries.

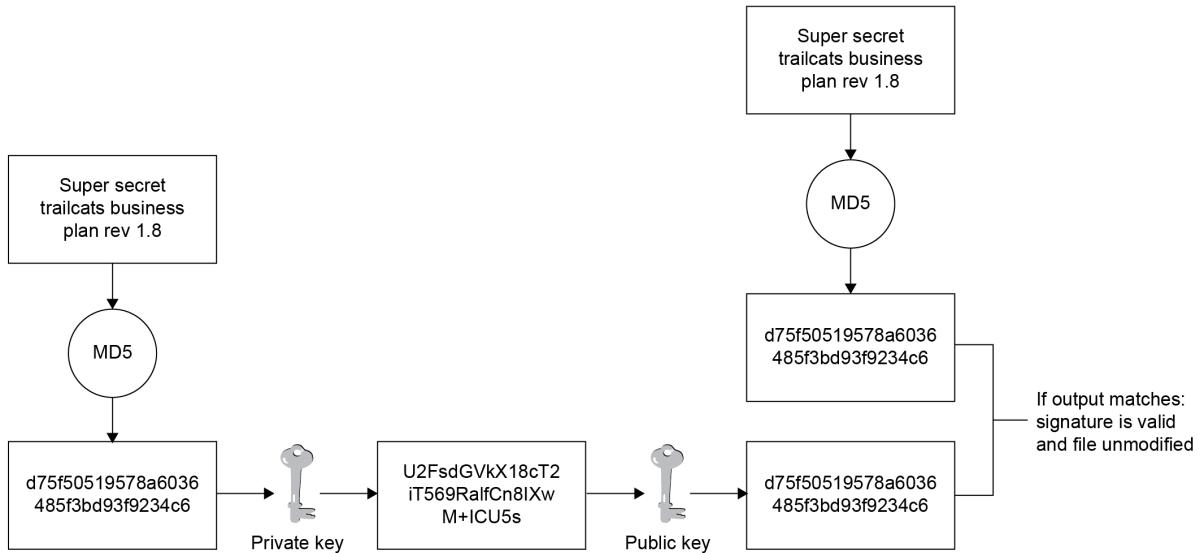
**Query logging**

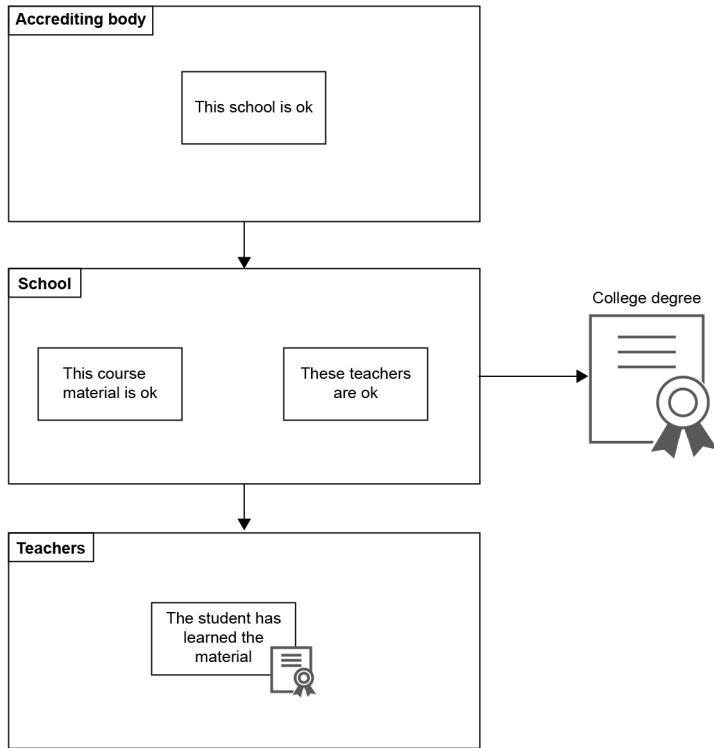
1. **Query logging** button highlighted with a red box and arrow.

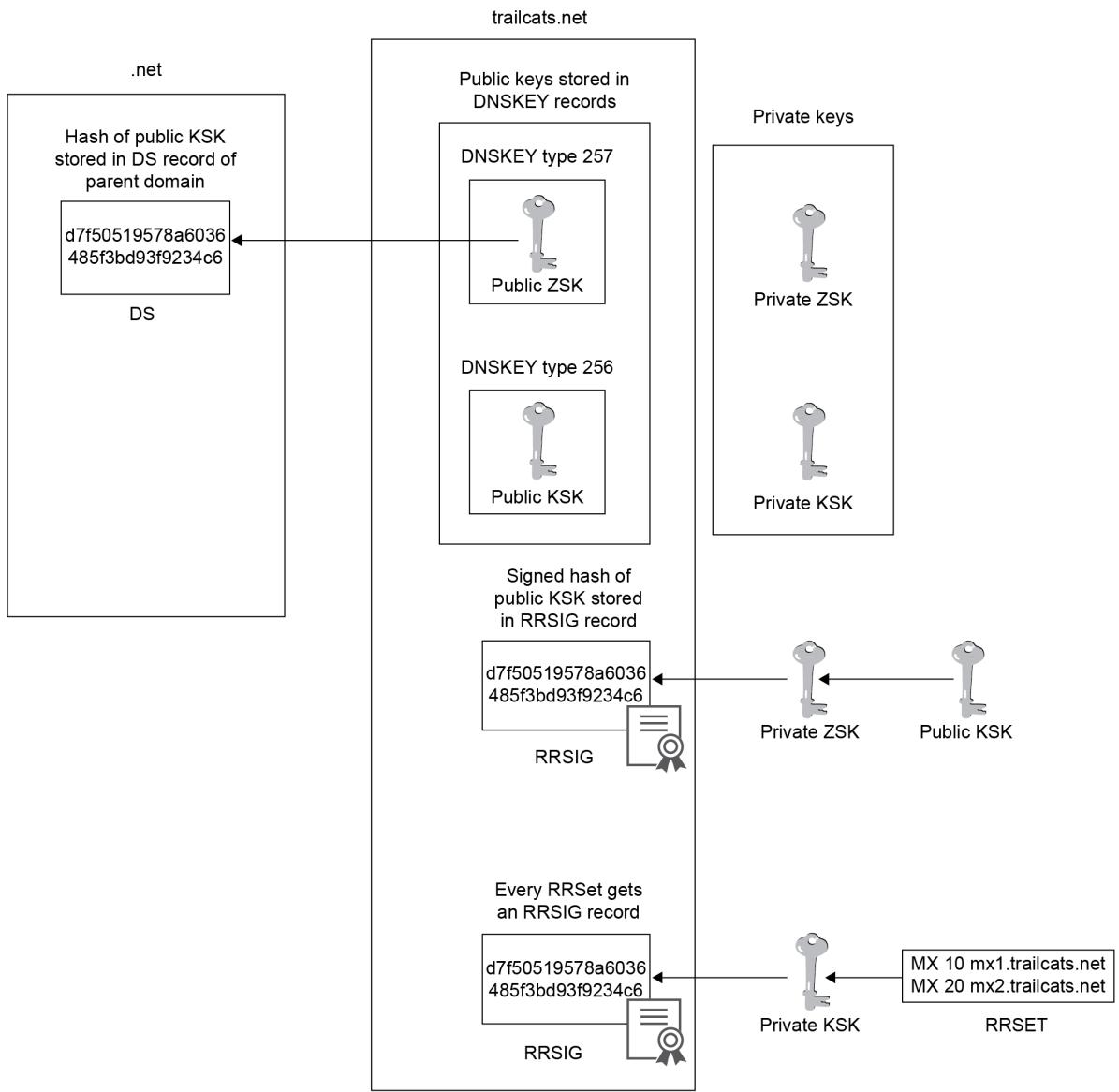
2. **Share configuration** button highlighted with a red box and arrow.











The screenshot shows the AWS Route 53 console interface.

**Left Sidebar (Route 53):**

- Hosted zones (highlighted with a red box and circled 1)
- Health checks
- Profiles New
- IP-based routing
- CIDR collections
- Traffic flow
- Traffic policies
- Policy records
- Domains
- Registered domains
- Requests
- Resolver

**Hosted zones View:**

Hosted zones (1/6)

Hosted zone name	Type	Create...	Record ...	D
trailcats.net	Public	Route 53	8	H
trailcats.net	Private	Route 53	5	-

A red arrow points from the "Hosted zones" link in the sidebar to the "Hosted zones" table in the view. Another red arrow points from the "trailcats.net" row in the table to the "Public" column.

Route 53 > Hosted zones > packetexample.net

## Public packetexample.net Info

[Delete zone](#)

[Test record](#)

[Configure query logging](#)

### Hosted zone details

1

[Edit hosted zone](#)

Records (2)

[DNSSEC signing](#)

Hosted zone tags (0)

#### DNSSEC signing Info

2

[Enable DNSSEC signing](#)

DNSSEC signing status

 Not 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.

##### 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.

##### 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 Service (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

▶ Key properties

Cancel

Create KSK and enable signing

3

4

1

2

## 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](#)

&lt; 1 &gt;

Name

Status

Creation date

 exampleKSK[Active](#)

August 02, 2024, 13:04 (U...)

## 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

Update your parent zone using the following information.

Key type	Signing algorithm
<input checked="" type="checkbox"/> KSK	<input checked="" type="checkbox"/> ECDSAP256SHA256

3

Copied

ba5CgbSdyRVwYdHO44f6/  
2Odfv+DmcNOPr6UxfnVI67Jx  
WFpBLE/0MvxuQ7vdZlgTj0lGY  
m/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 X Registered domains

Registered domains [Info](#)

Download billing report Transfer in Register domains

Search domains by name

Domain name	Expiration date	Auto-renew	Transfer lock
trailcats.net	July 28, 2026	Off	Off

1

2

Registered domains

## trailcats.net Info

Transfer out ▾

Delete domain

### Details Info

Actions ▾

Registration date  
July 28, 2023, 15:21  
(UTC-04:00)

Auto-renew  
Off

Domain status code  
addPeriod  
ok

Name servers  
ns-144.awsdns-  
18.com  
ns-1763.awsdns-  
28.co.uk  
ns-1134.awsdns-  
13.org  
ns-532.awsdns-02.net

Expiration date  
July 28, 2026

Transfer lock  
Off

DNSSEC status  
Configured

Contact information

**DNSSEC keys**

Tags

Add

Delete

### DNSSEC keys (1) Info

DNSSEC keys are used to establish a chain of trust for your domain.

1

2

## Add DNSSEC key

X

**i** After you configure DNSSEC with your DNS service, add the applicable public key to the domain. [Learn more](#) ↗

Key type

257 - KSK

1

Algorithm

13 - ECDSAP256SHA256

▼

Public key

ba5GgbSdyRVwYdHO44f6/2Odfv+DmcN0Pr6UxfnVI67JxWFpBLE/0MvxuQ7vdZlgTj0  
lGYm/brBDzhE1Cr2/EQ==

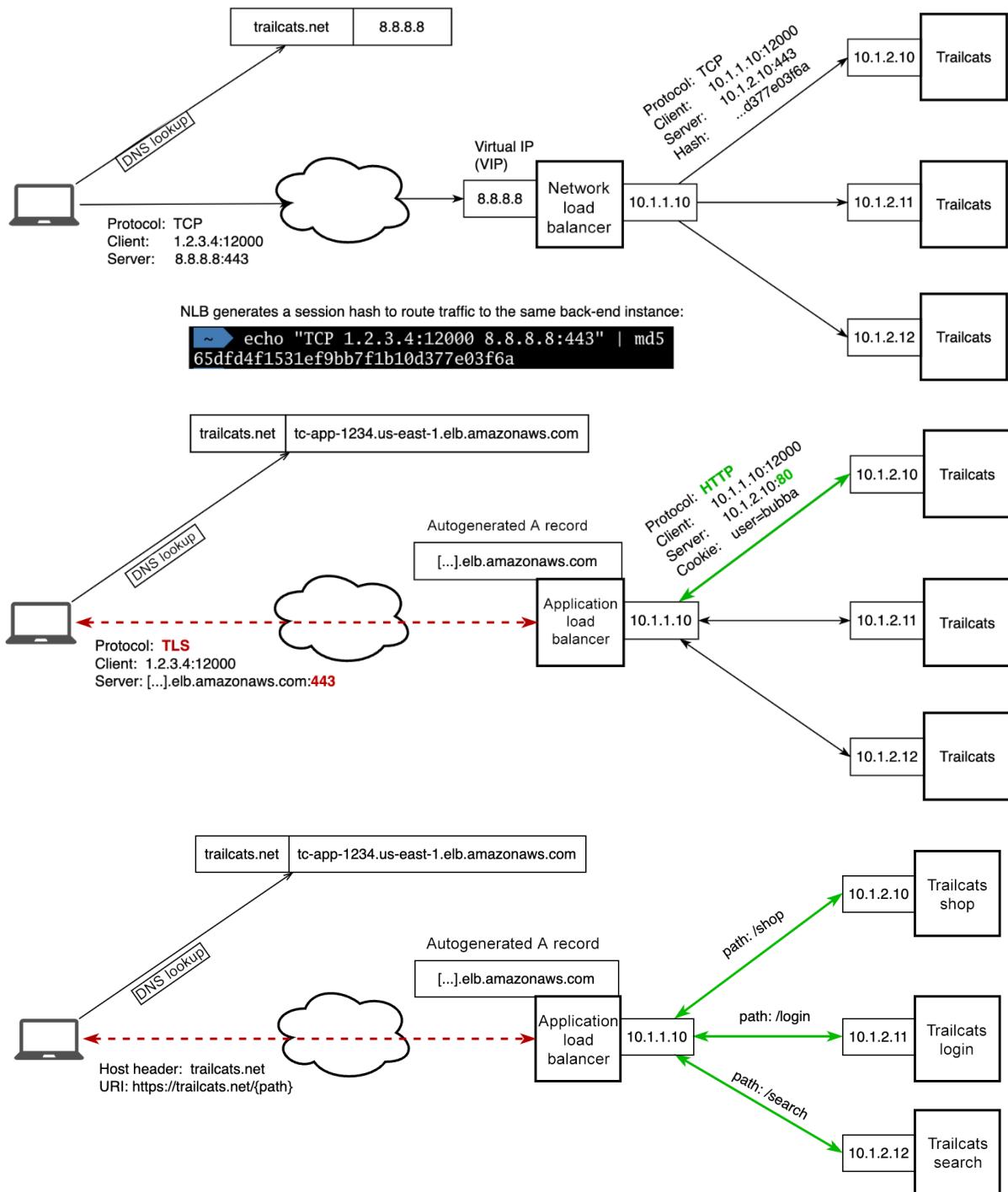
2

3

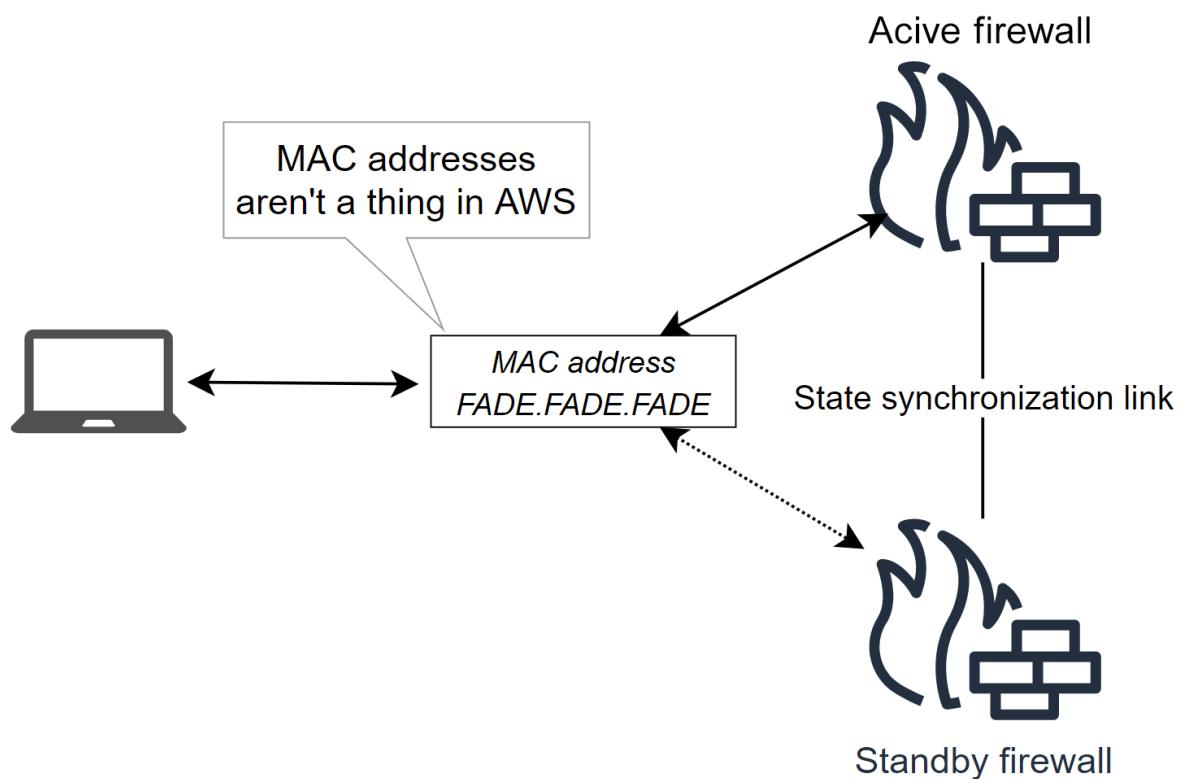
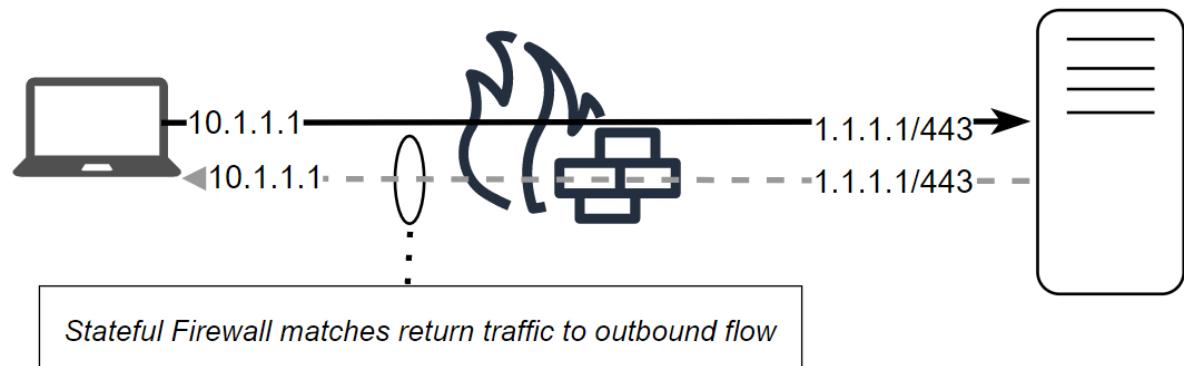
Cancel

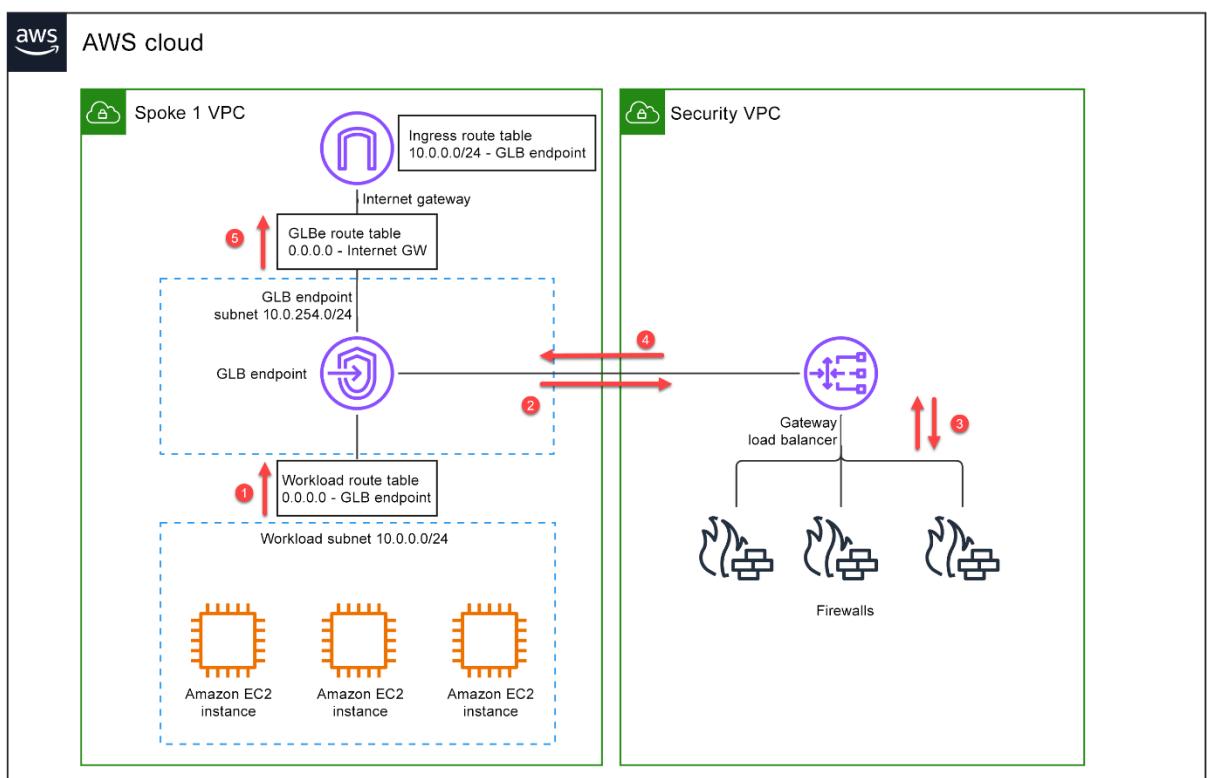
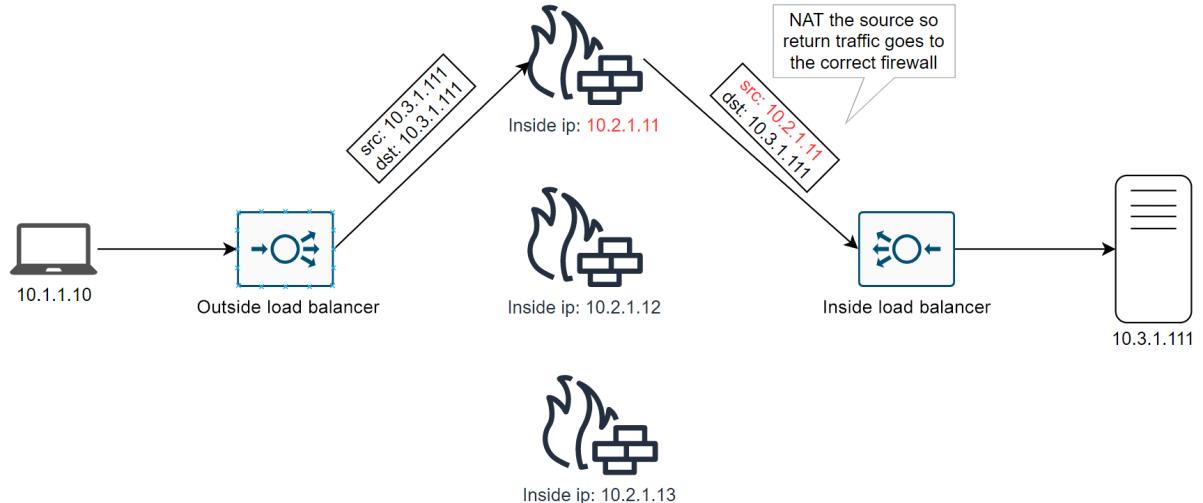
Add

## Chapter 9: AWS Elastic Load Balancing

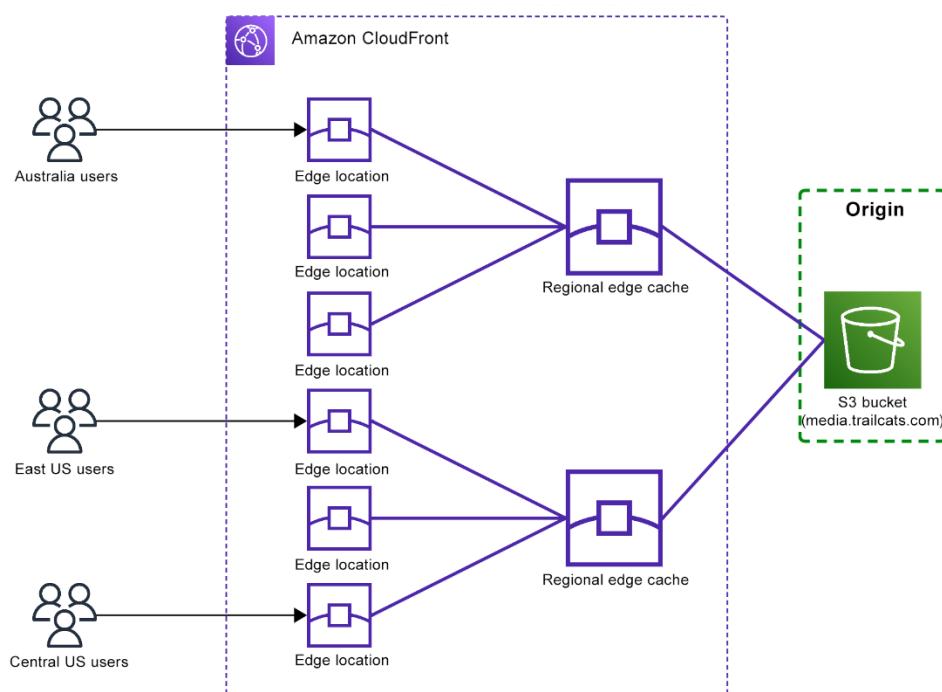
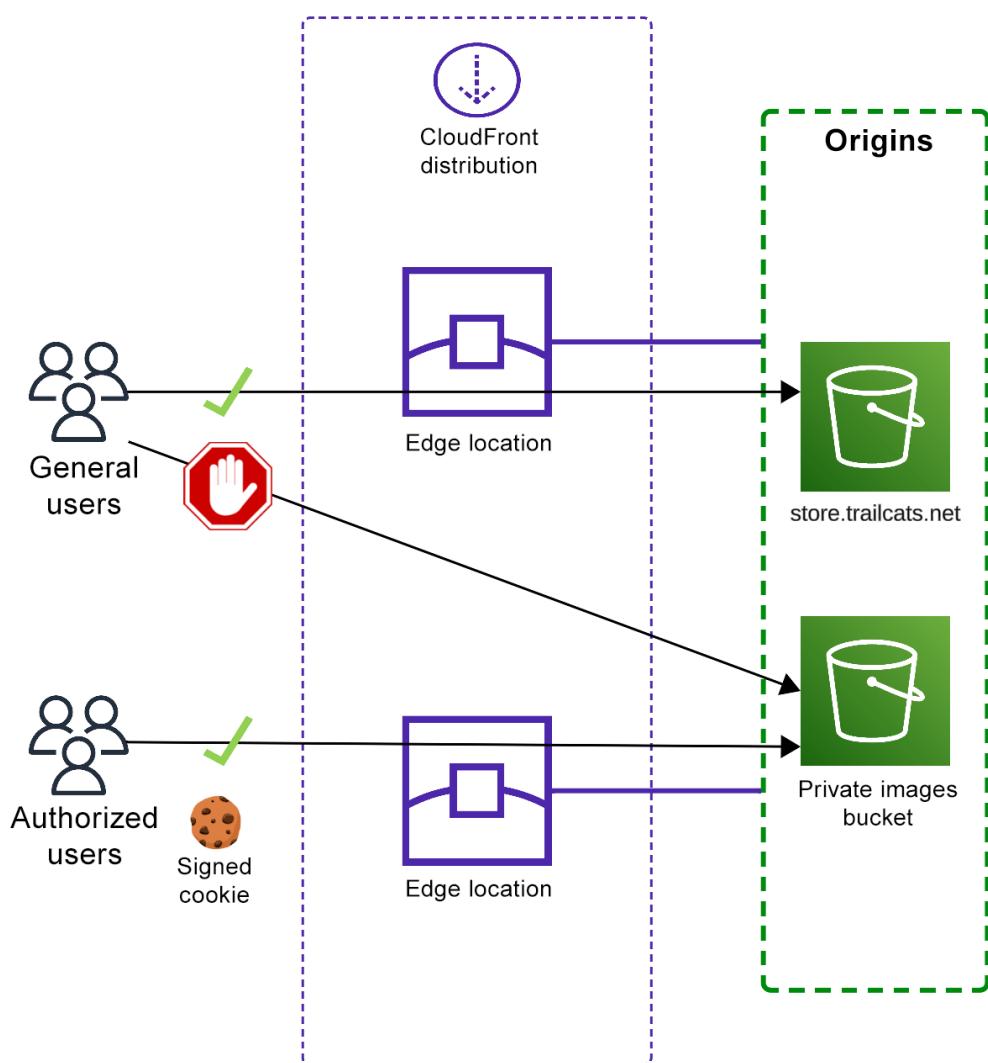


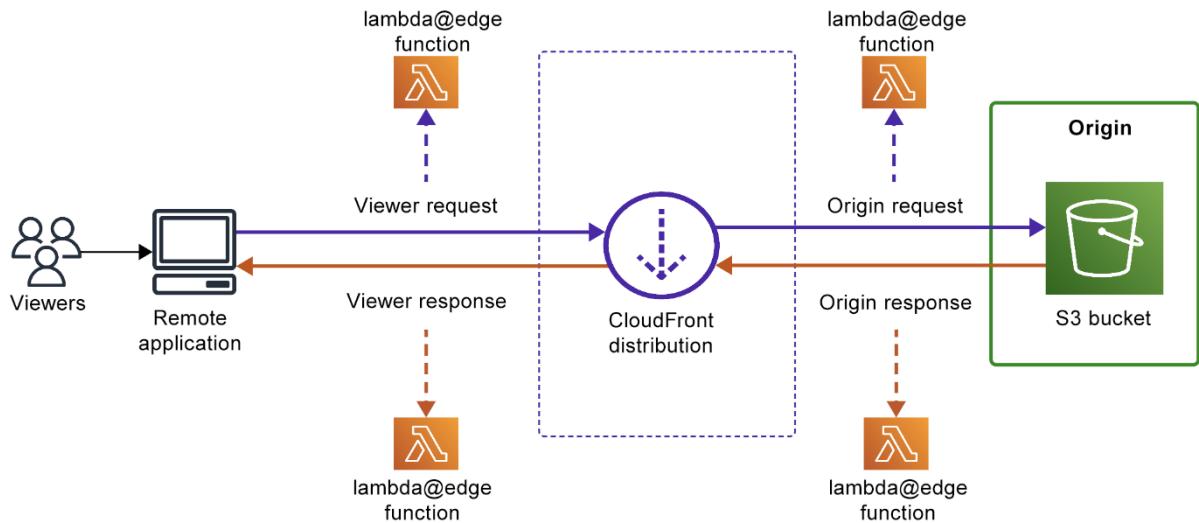
Firewall rule		
Source	Destination	Action
TCP/10.1.1.1/any	TCP/1.1.1.1/443	Allow





## Chapter 10: AWS CDN and Global Traffic Management

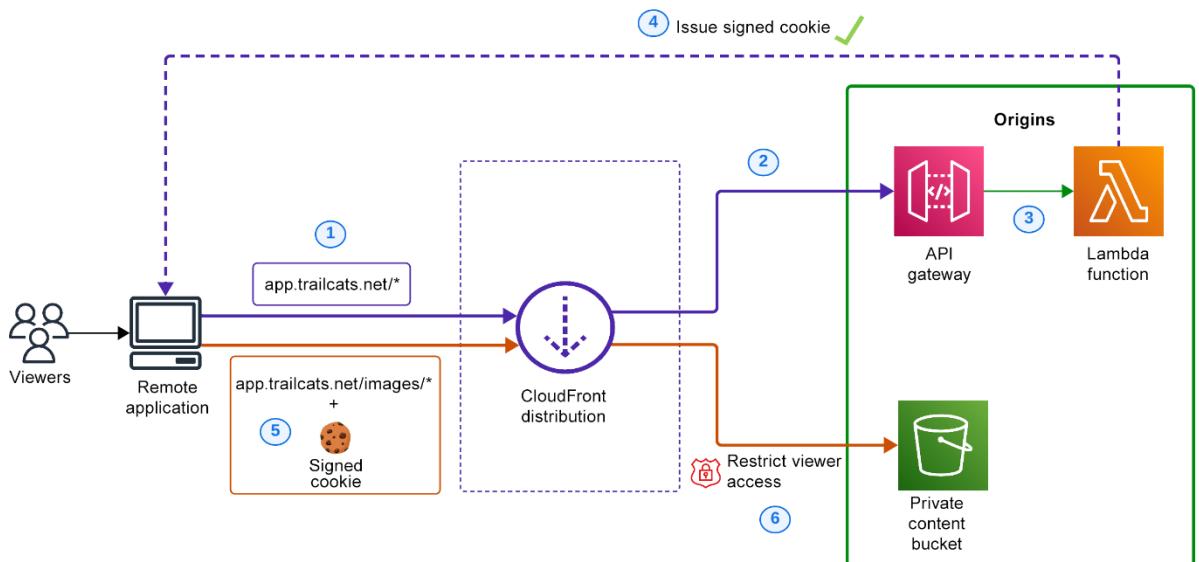


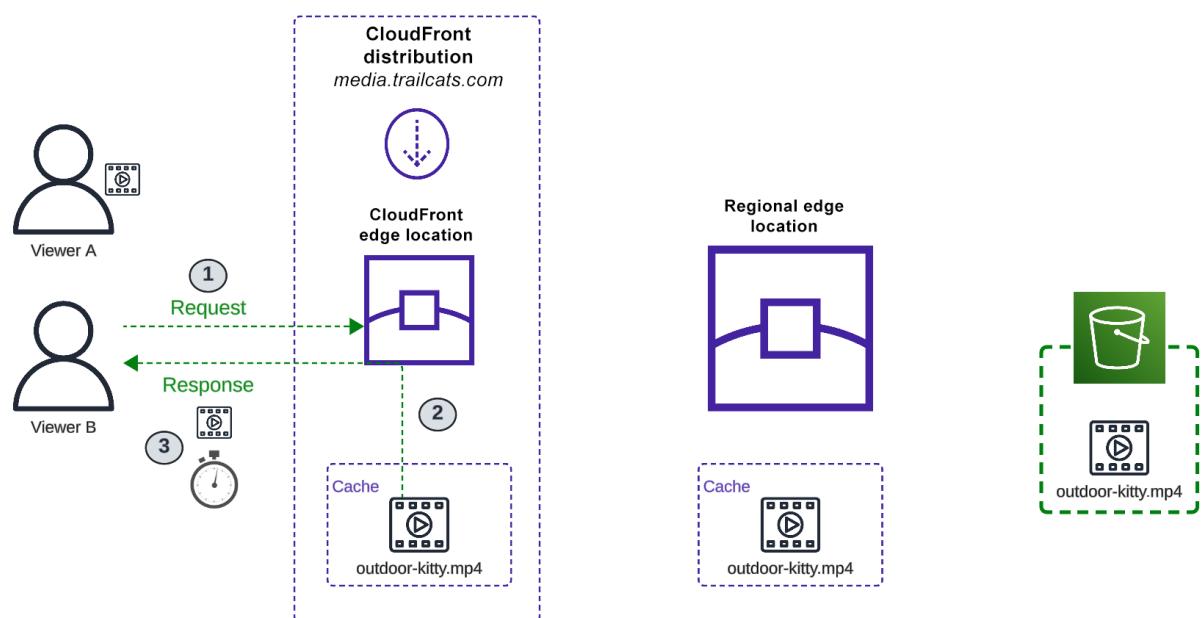
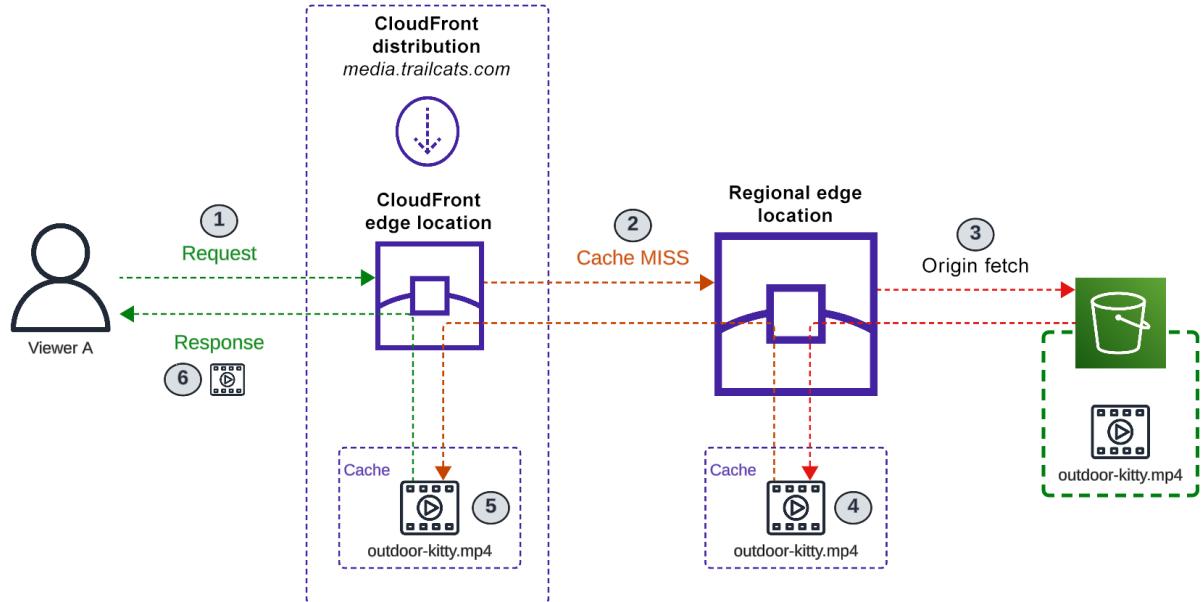


### Function associations - optional Info

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
<b>Viewer request</b> <input checked="" type="checkbox"/>	Lambda@Edge <input type="button" value="▼"/>	<input type="checkbox"/> arn:aws:lambda:us-east-1:1234567
<b>Viewer response</b> <input type="checkbox"/>	No association <input type="button" value="▼"/>	
<b>Origin request</b> <input checked="" type="checkbox"/>	Lambda@Edge <input type="button" value="▼"/>	<input type="checkbox"/> arn:aws:lambda:us-east-1:0987654
<b>Origin response</b> <input type="checkbox"/>	No association <input type="button" value="▼"/>	





## 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

Minimum time to live in seconds.

0

Maximum TTL

Maximum time to live in seconds.

31536000

Default TTL

Default time to live in seconds.

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

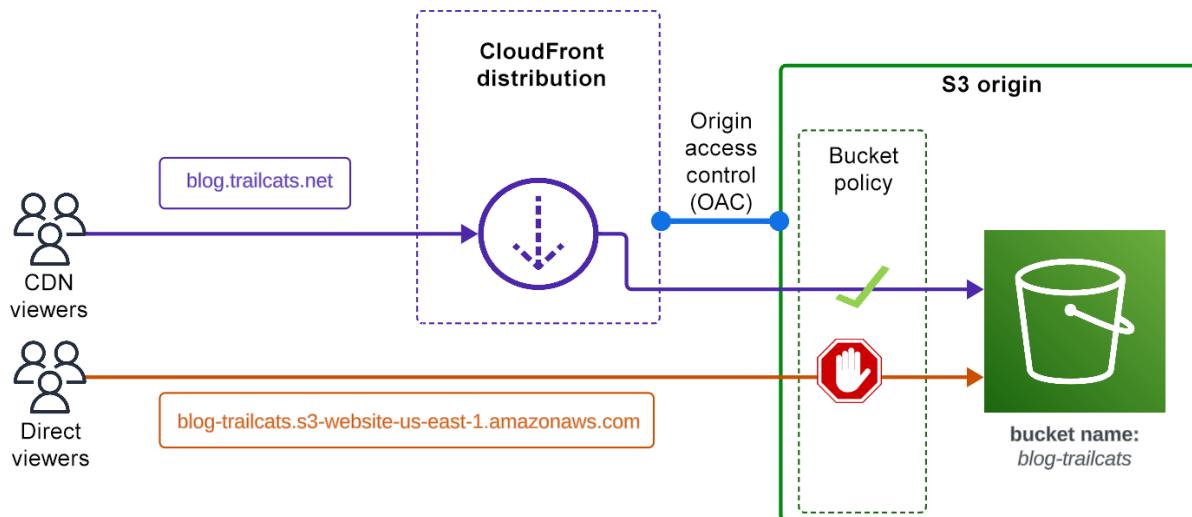
To add object paths individually, use the [standard editor](#).

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

X

### 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

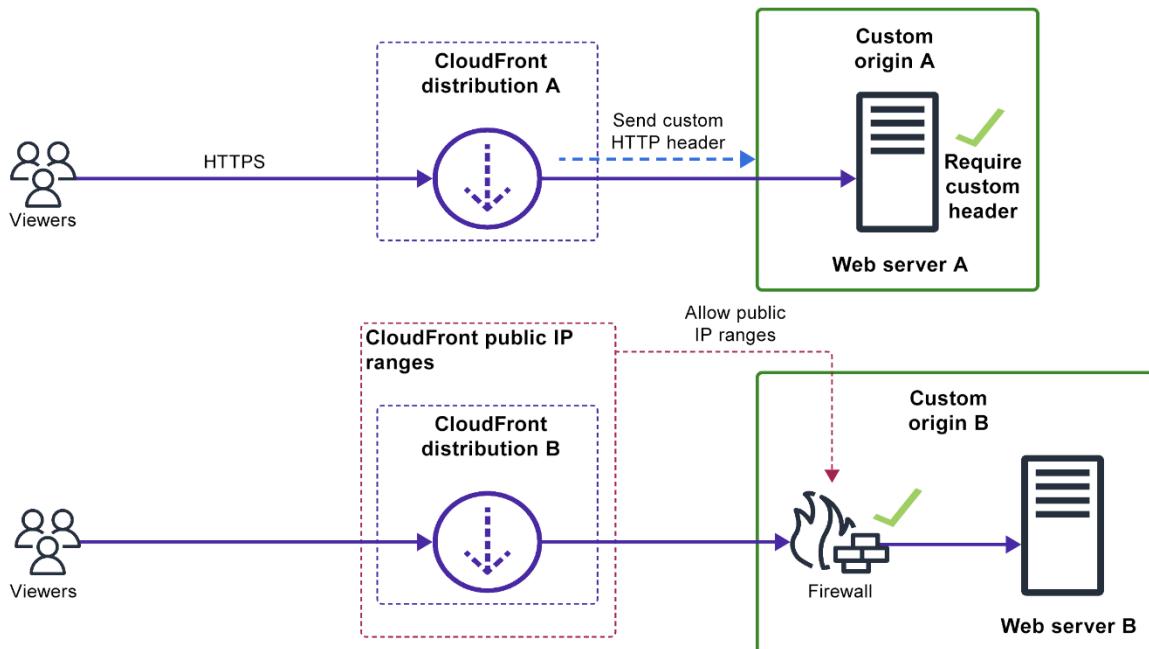
## Bucket policy

[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](#)

```
{  
    "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:::distribution/E3LVSH6OTJ0YDK"  
                }  
            }  
        }  
    ]  
}
```

[Copy](#)

## 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.

RemoveAdd 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 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

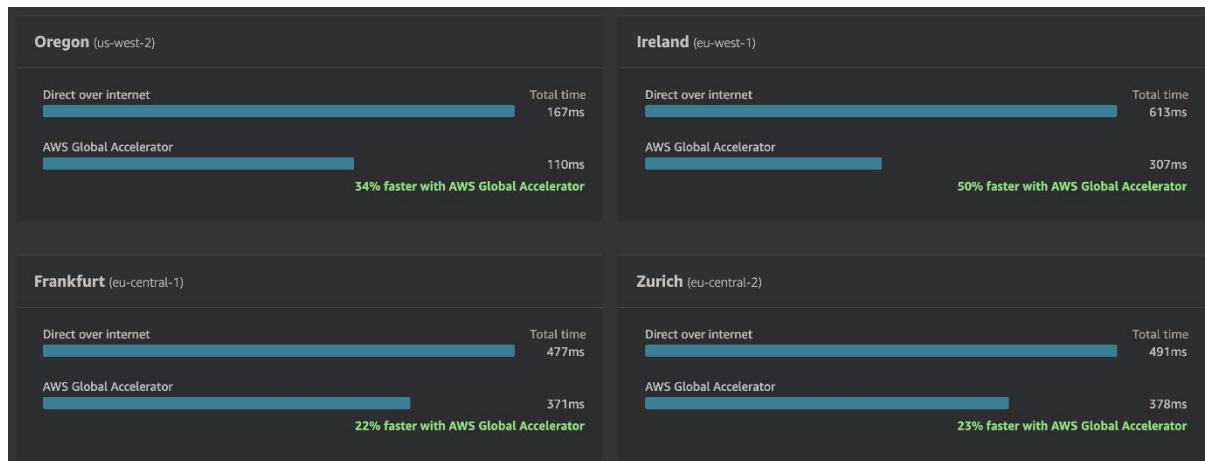
### Countries

Select countries

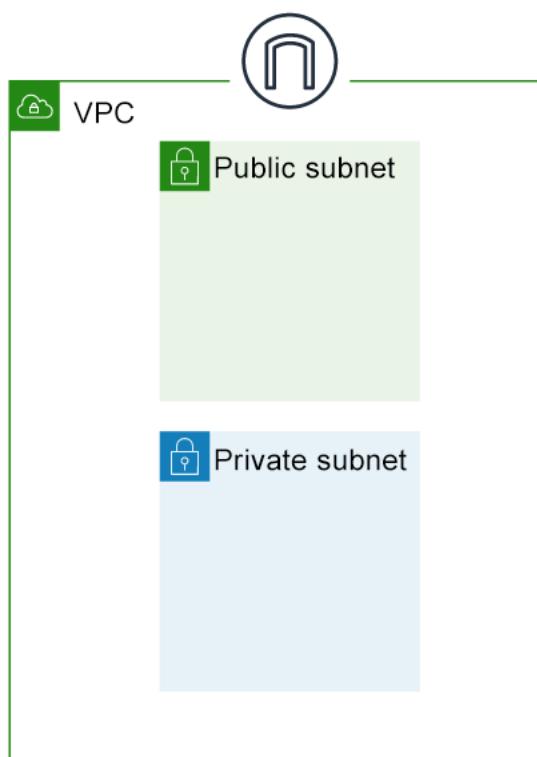
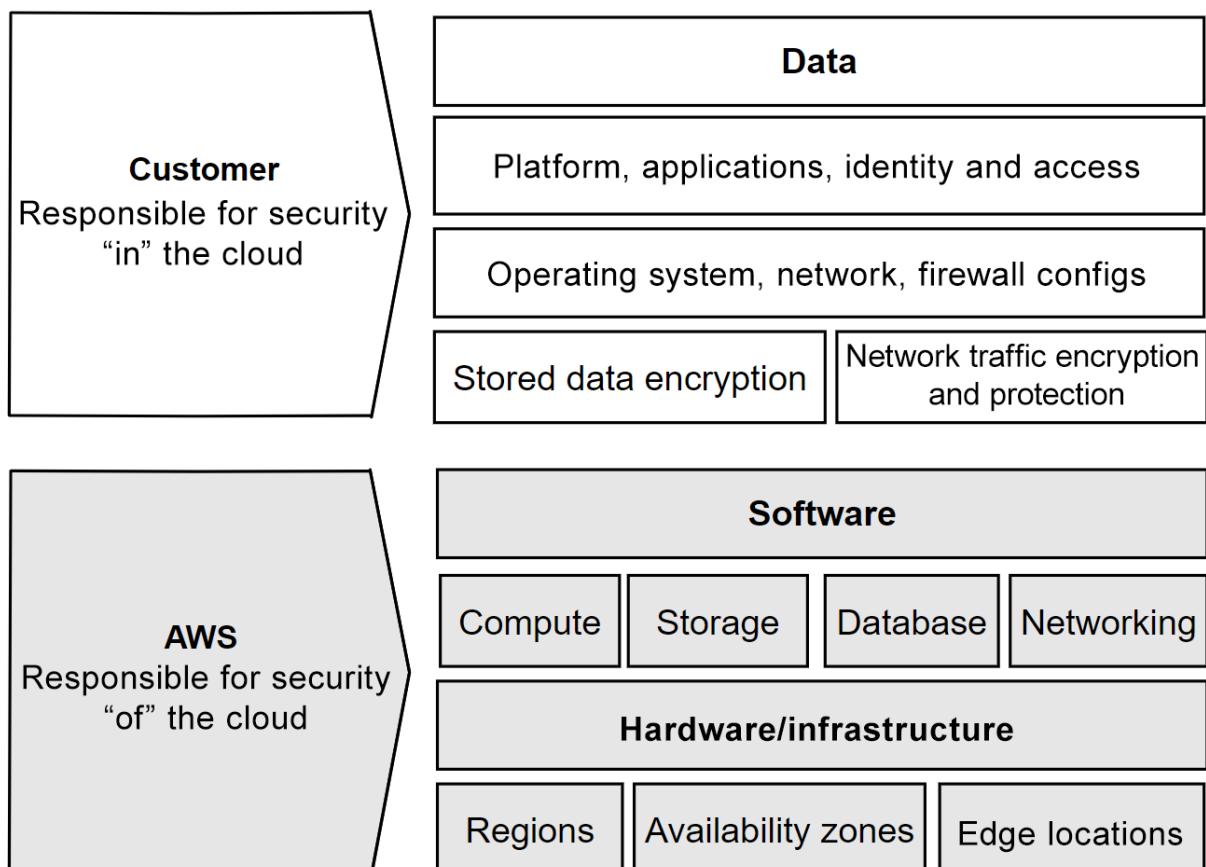
Australia X

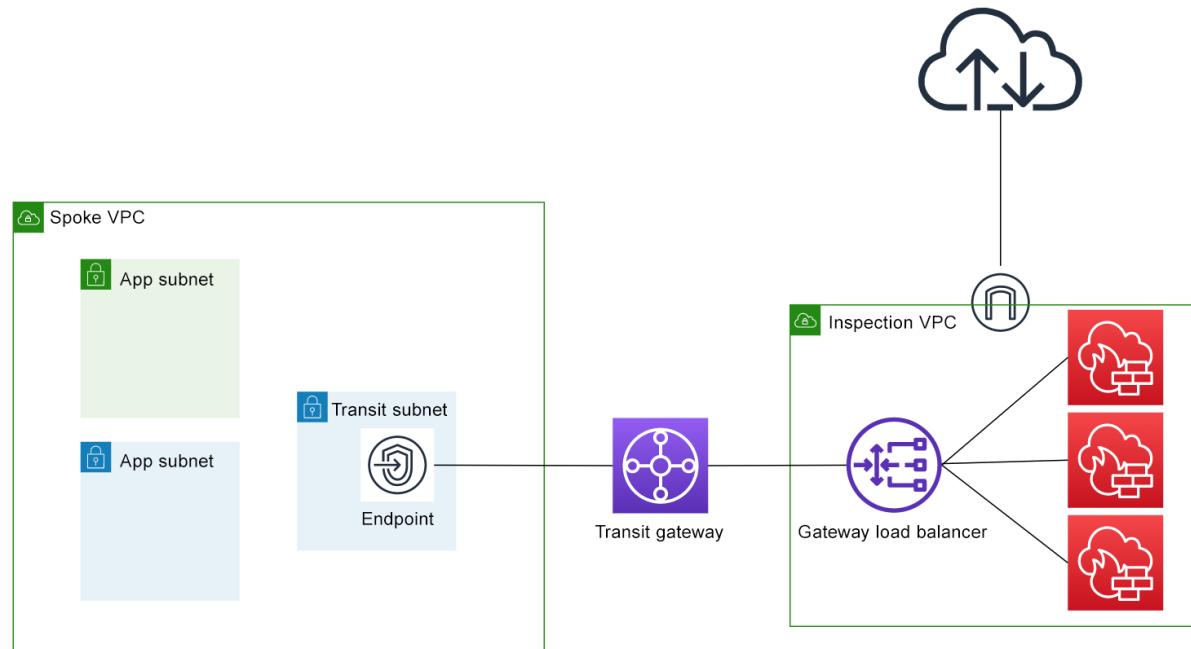
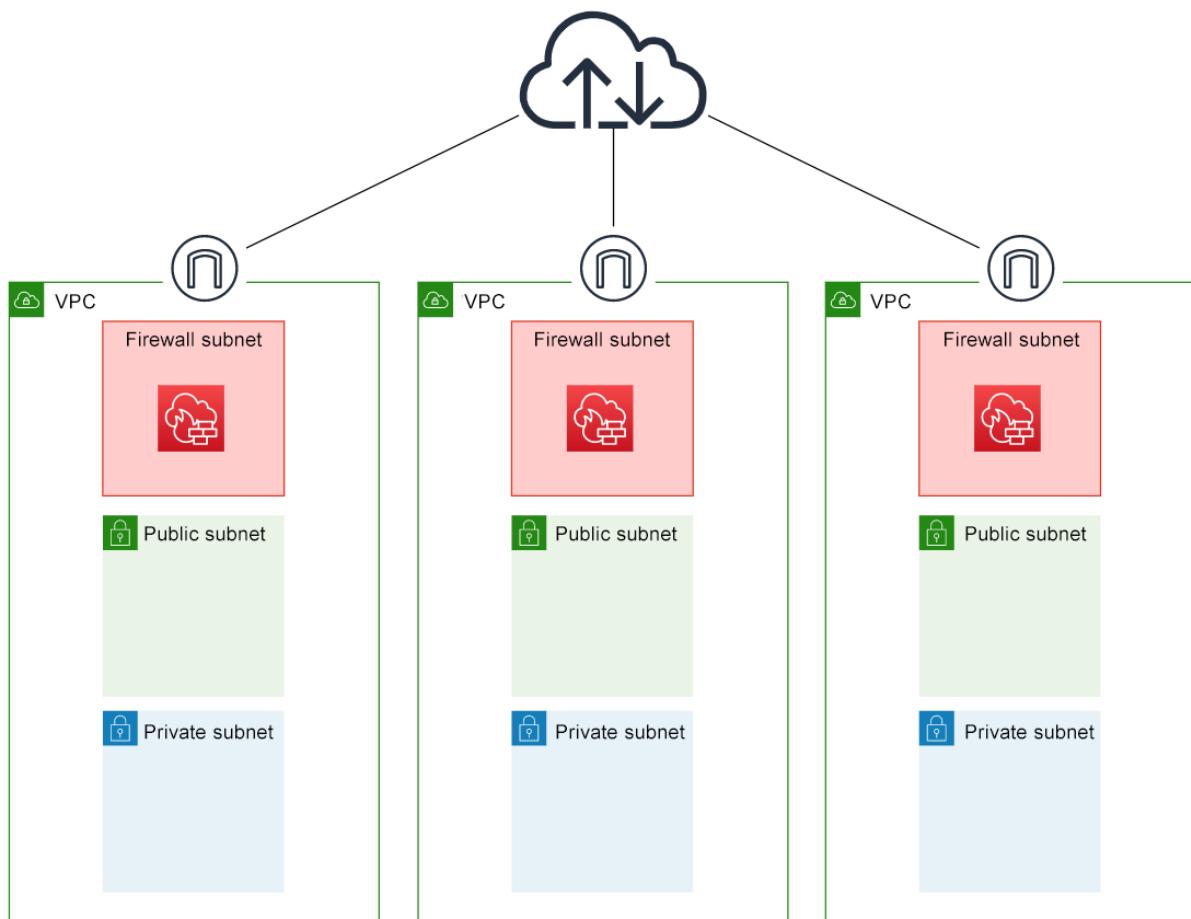
United Kingdom X

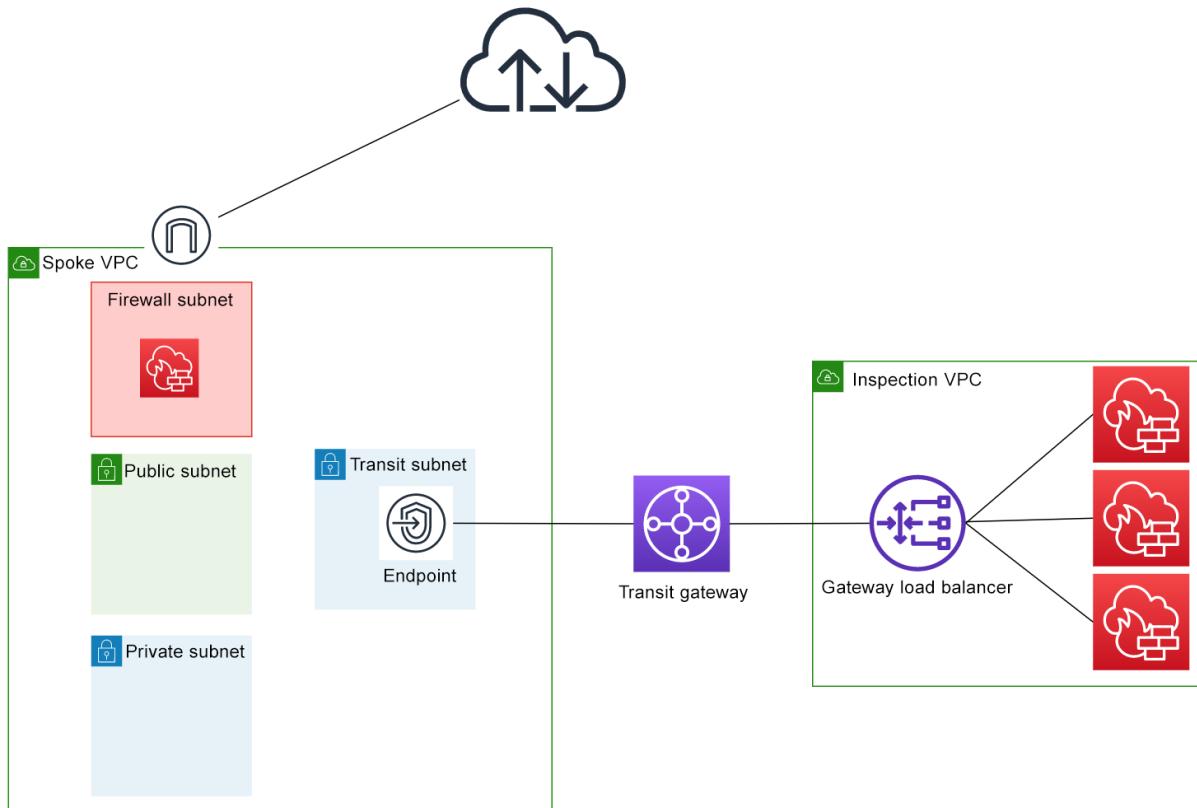
United States X



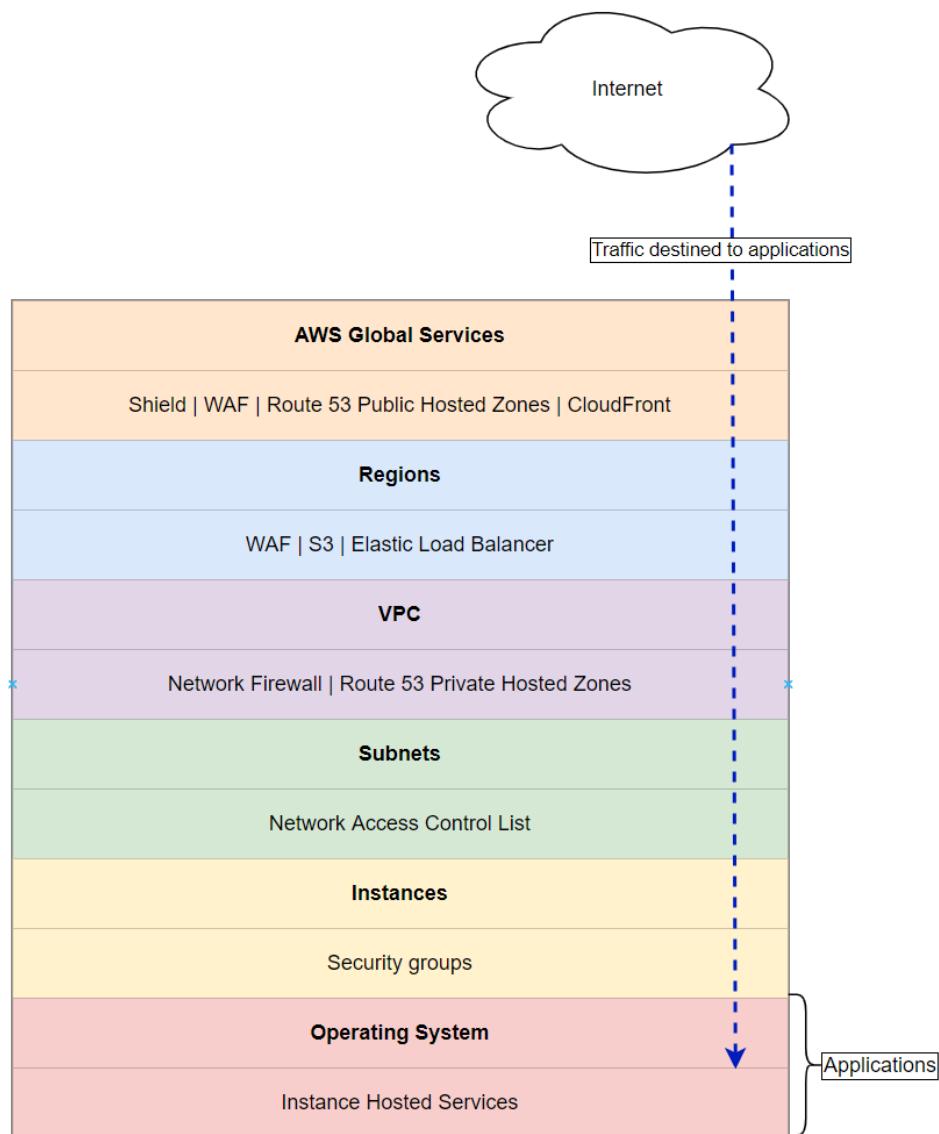
## Chapter 11: Security Framework







## Chapter 12: AWS Security Services



Screenshot of the AWS WAF & Shield console:

- WAF & Shield (highlighted)
- Web ACLs (highlighted)
- Trailcats\_WebACL (highlighted)
- Rules (highlighted)
- Rules (3) table (highlighted)

The screenshot shows the AWS WAF & Shield console with the "Web ACLs" section selected. A new Web ACL named "Trailcats\_WebACL" is being created. The "Rules" tab is selected, showing three rules: Rule1 (Action: Block, Priority: 0, Response: Status 555, 555\_error), Rule2 (Action: Count, Priority: 1, Response: -), and Rule3 (Action: CAPTCHA, Priority: 2, Response: -).

Rule		
Rule name	Type	Region
Rule1	Regular rule	US East (N. Virginia)

If a request matches the statement

**Statement 1**

Request option  
Originates from countries

Country  
Russian Federation - RU

**Country of Origin condition**

## 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.

1 Action Block

2 Custom response code 555

3 Custom response headers Header name x-blocked-reason Header value country of origin not allowed

4 Custom response body 555\_error <div>Error: access denied</div>

## Rules (6)

Edit

Delete

Add rules ▾

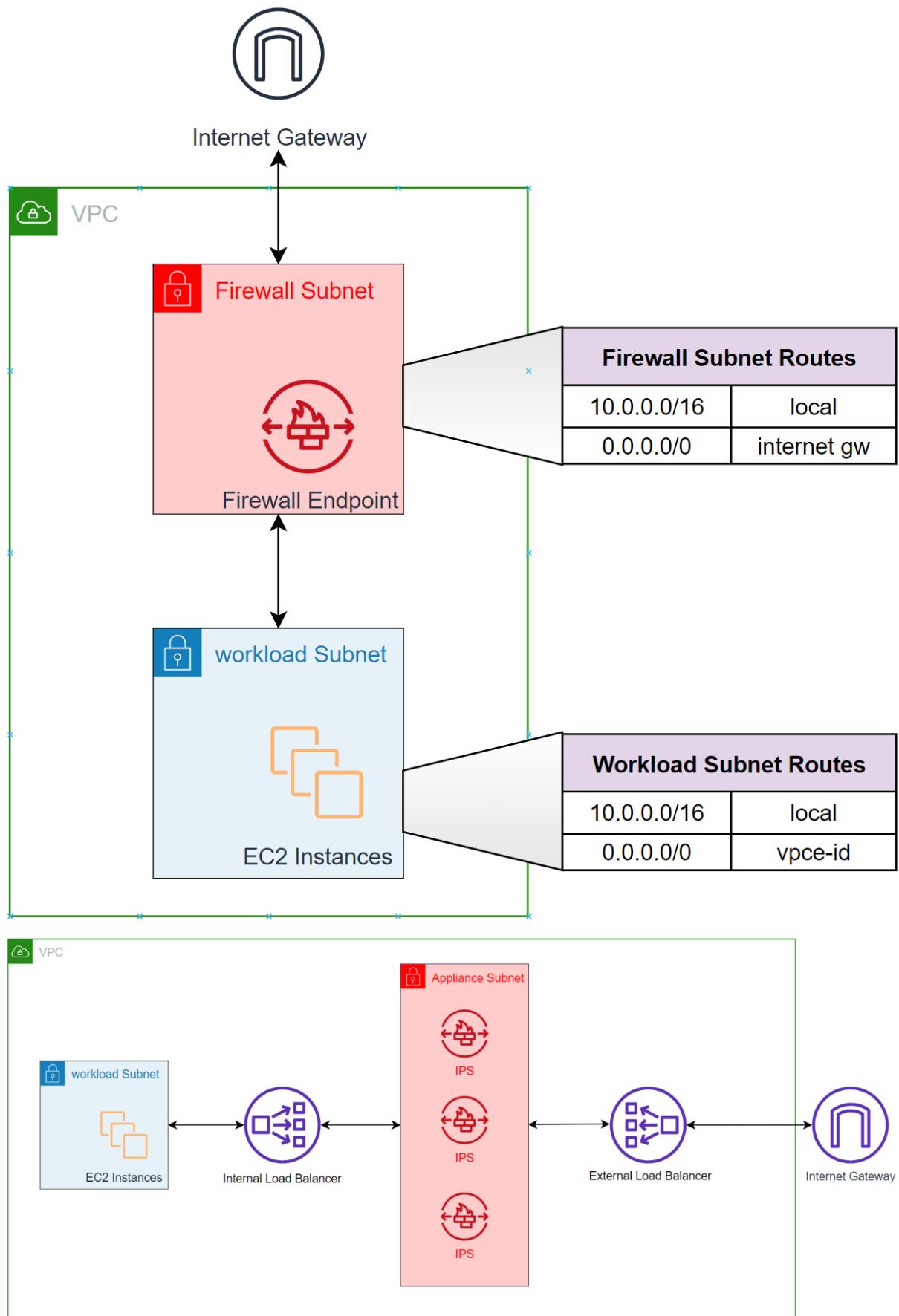
Find rules

### Managed rule groups

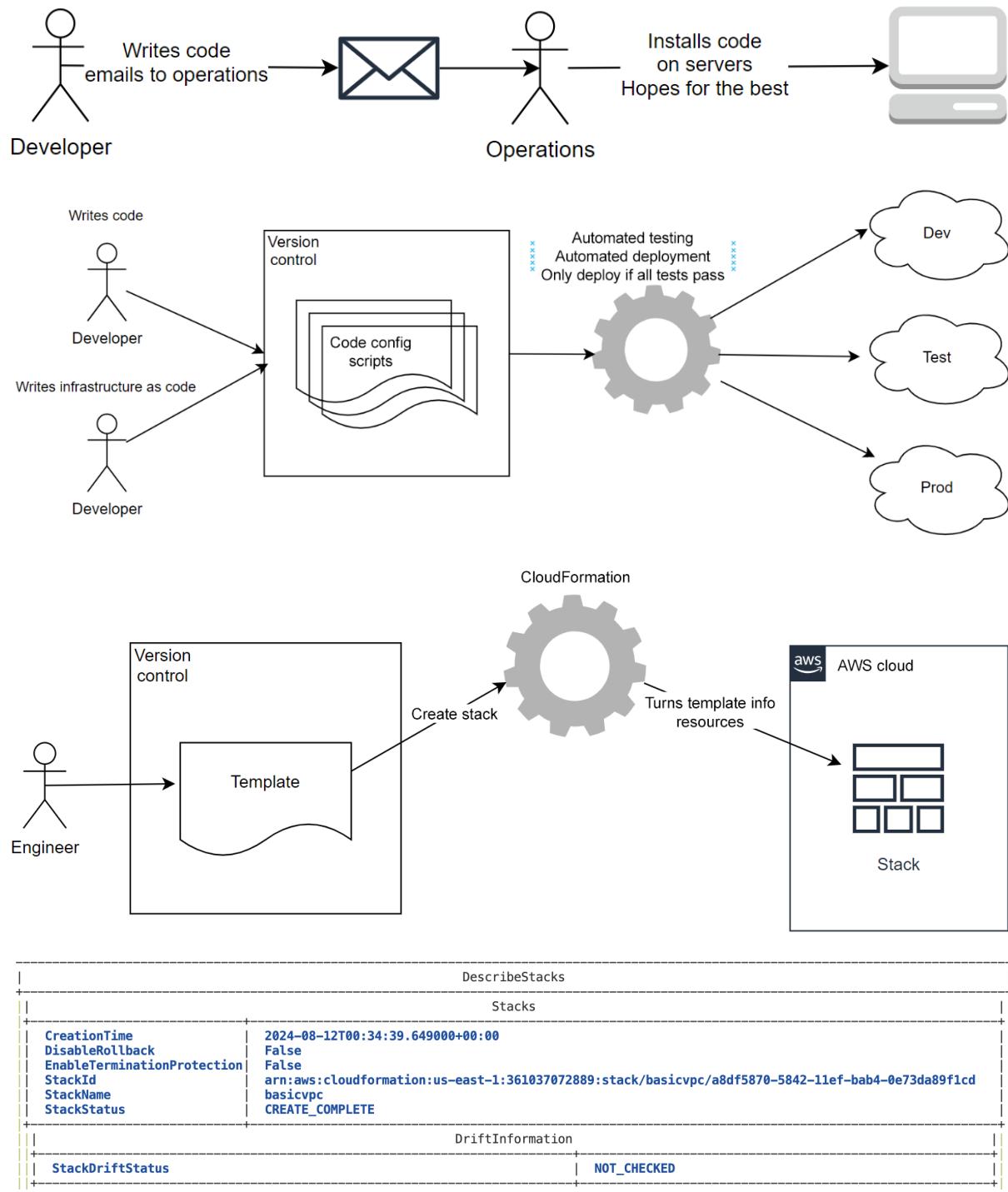
< 1 > ⚙

<input type="checkbox"/>	Name	Action	Priority	Custom response
<input type="checkbox"/>	Rule1	Block	0	Status 555, <a href="#">555_error</a>
<input type="checkbox"/>	<a href="#">AWS-AWSManagedRulesAmazonIpReputationList</a>	Use rule actions	1	-
<input type="checkbox"/>	<a href="#">AWS-AWSManagedRulesAnonymousIpList</a>	Use rule actions	2	-
<input type="checkbox"/>	<a href="#">AWS-AWSManagedRulesCommonRuleSet</a>	Use rule actions	3	-
<input type="checkbox"/>	<a href="#">AWS-AWSManagedRulesKnownBadInputsRuleSet</a>	Use rule actions	4	-
<input type="checkbox"/>	<a href="#">AWS-AWSManagedRulesSQLiRuleSet</a>	Use rule actions	5	-





## Chapter 13: Infrastructure as Code



The screenshot shows the AWS Management Console interface for the VPC service. The top navigation bar includes the AWS logo, a search bar, and a 'Services' dropdown. Below the navigation, the 'Virtual private cloud' section is expanded, showing various options like 'Your VPCs', 'Subnets', 'Route tables', etc. The 'Peering connections' link is highlighted with a red box and the number '1'. The main content area displays a table titled 'Peering connections (1/1)'. The table has columns: Name, Peering connection ID, Status, Requester VPC, and Acceptor VPC. One row is listed, showing a Name of ' - ', Peering connection ID of 'pcx-...', Status of 'Active', Requester VPC of 'vpc-01', and Acceptor VPC of '/security-vpc'. A red box with the number '2' highlights the first column of the table header. At the bottom of the table, there are tabs for 'Details', 'DNS', 'Route tables', and 'Tags'.

Name	Peering connection ID	Status	Requester VPC	Acceptor VPC
-	pcx-...	Active	vpc-01	/security-vpc

Peering connections (1/1) [Info](#)

Find resources by attribute or tag

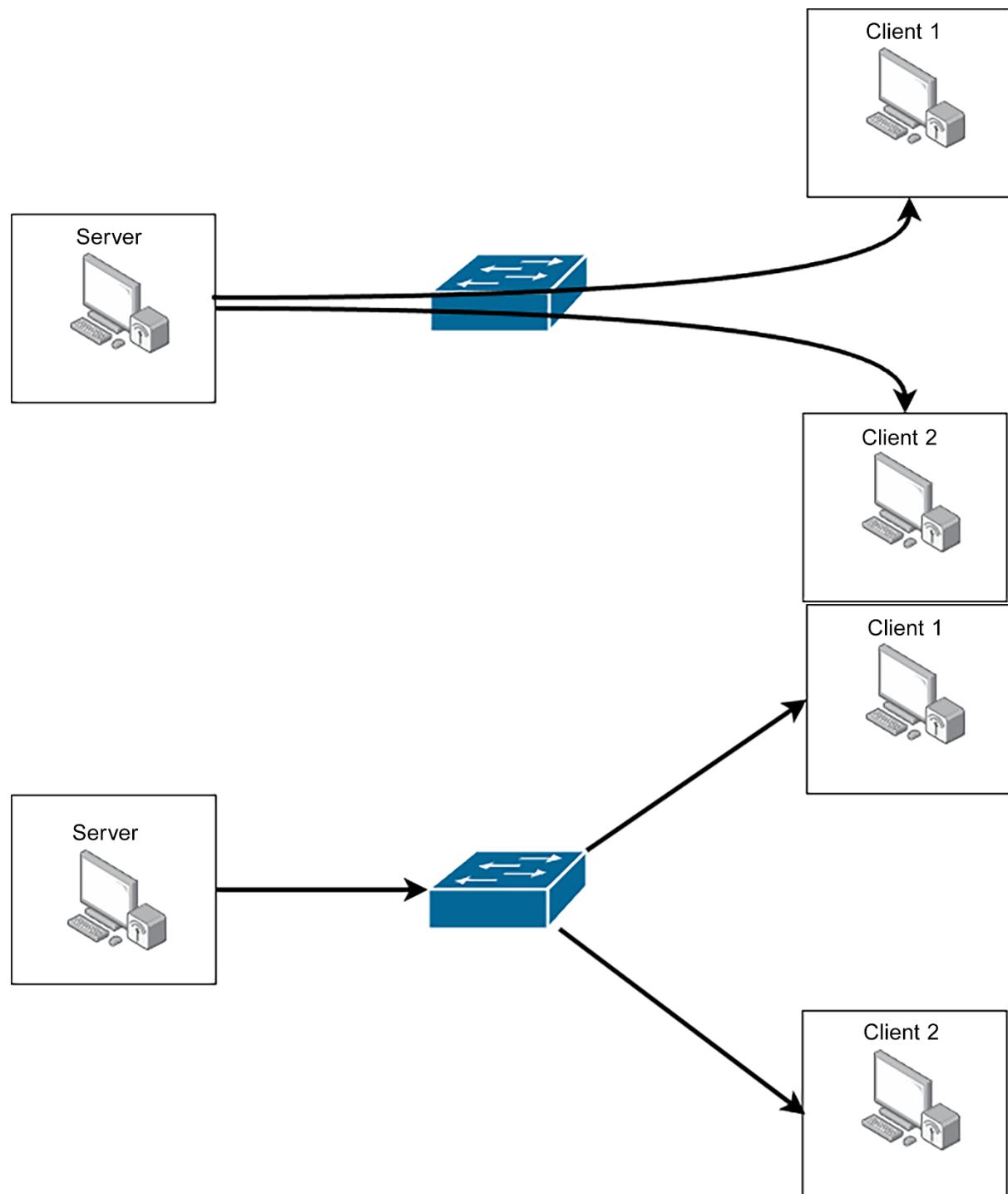
C Actions ▾ Create peering connection

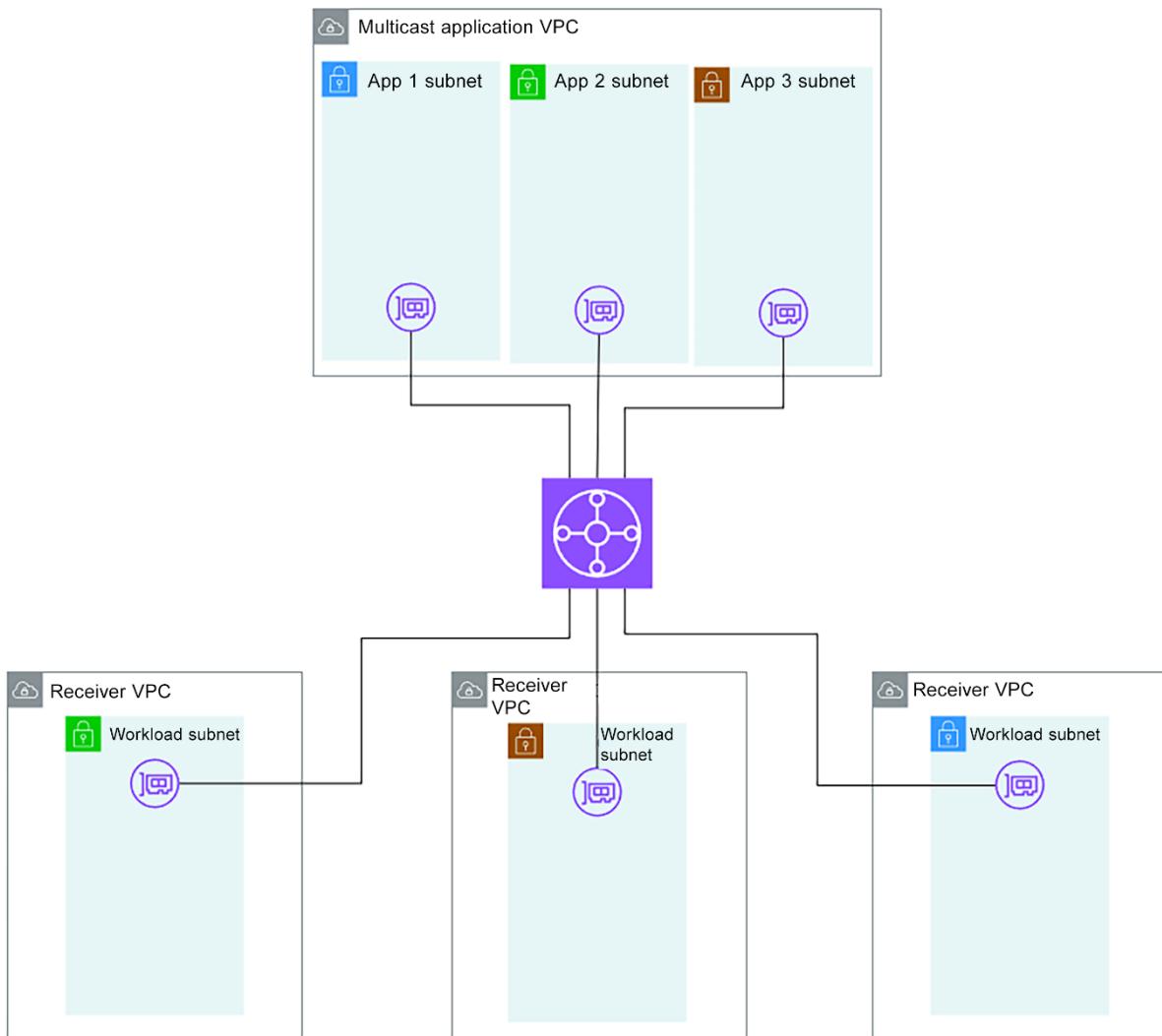
1

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	Description
Trailcats-TGW	-

### 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](#)

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

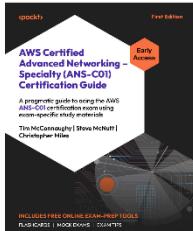
## Chapter 16: Accessing the Online Practice Resources

 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 McConaughy • 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 McConaughy • Steve McNutt • Christopher Miles • Dec 2024 • 515 pages

#### ENTER YOUR PURCHASE DETAILS

Enter Unique Code \*

CPP4153

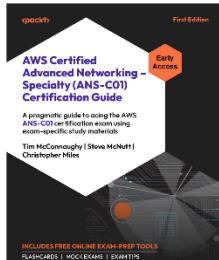
[Where To Find This?](#)

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](#)

## 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 McConaughy • 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](#)

#### 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 McConaughy, Steve McNutt, Christopher Miles



## 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

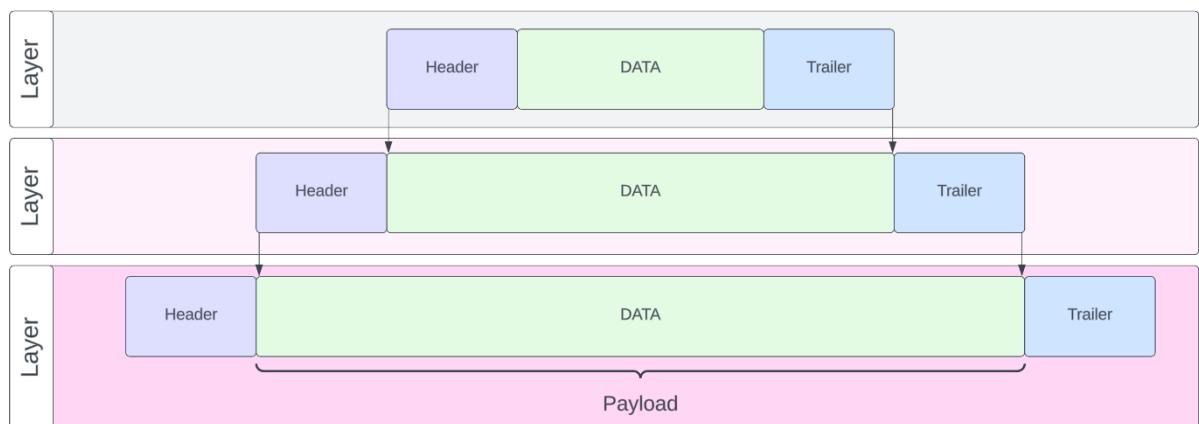
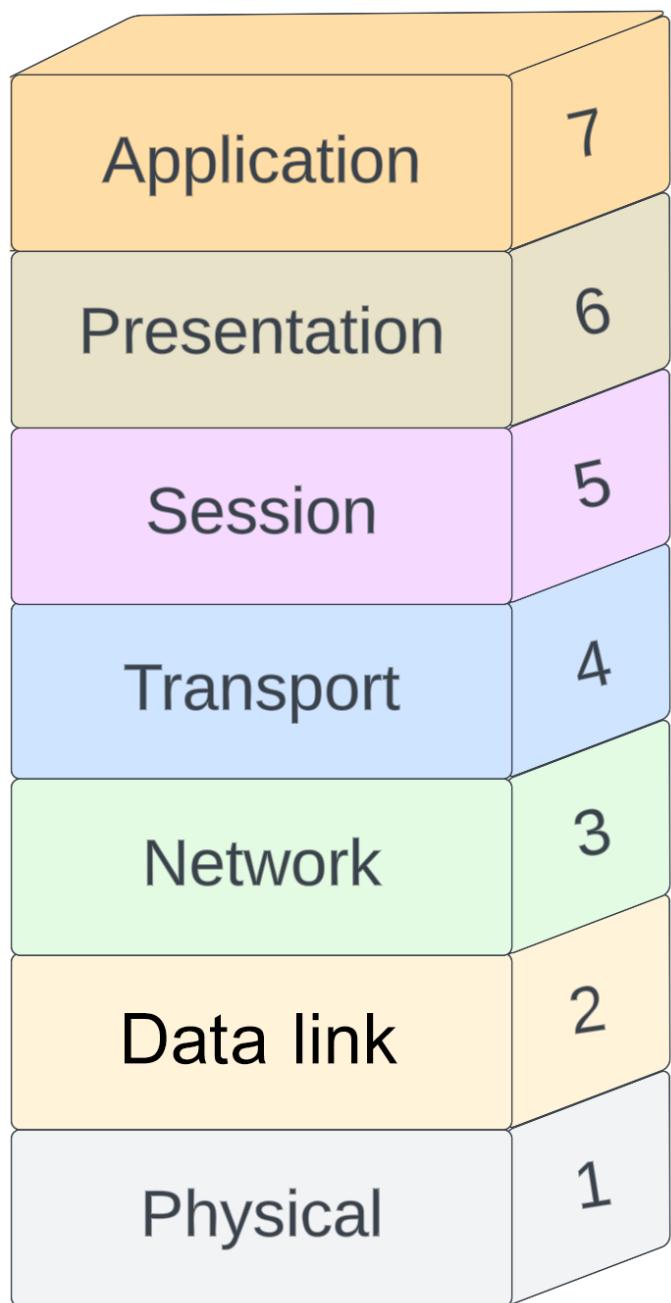
Flashcards

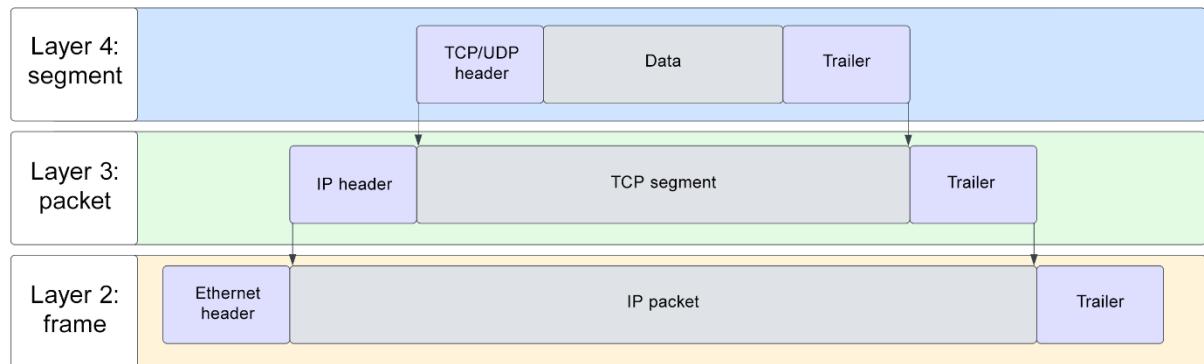
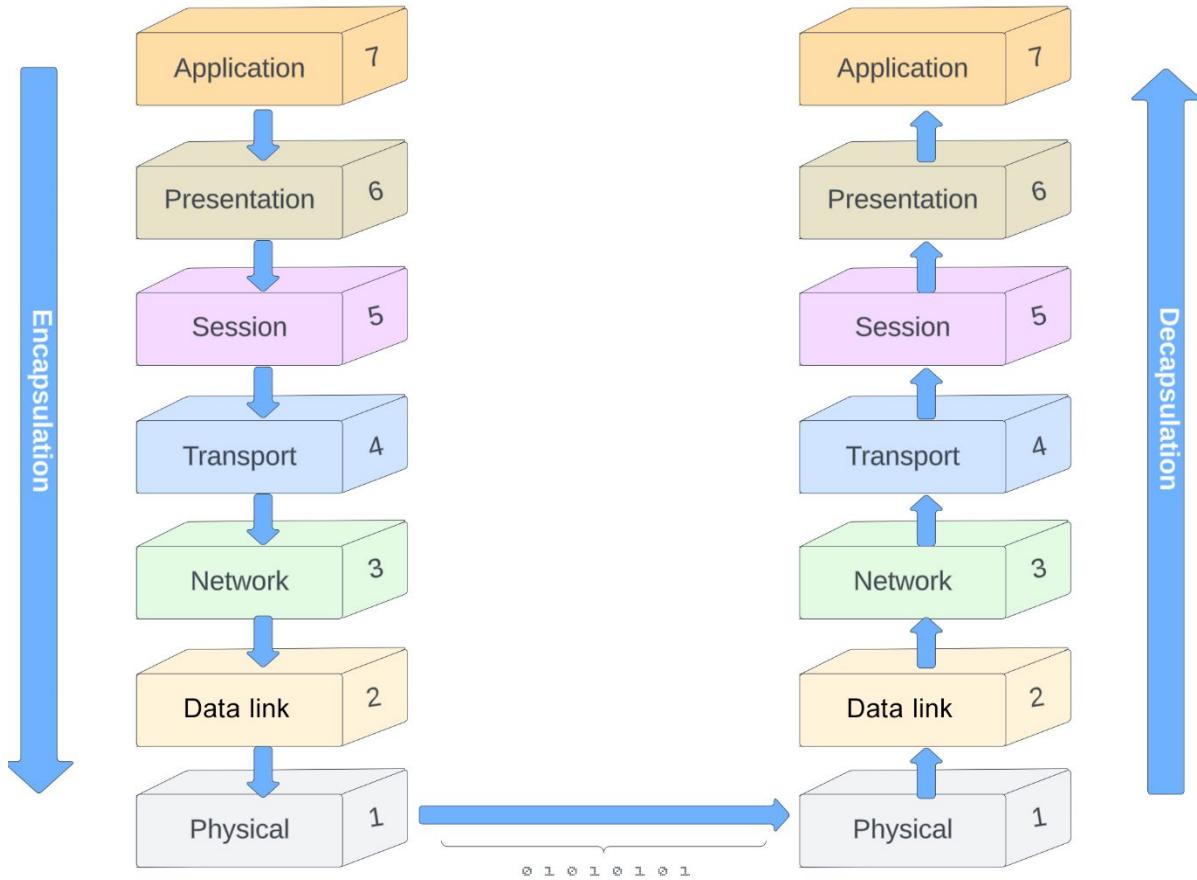
Exam Tips

## BACK TO THE BOOK

**AWS Certified Advanced Networking – Specialty (ANS-C01) Certification Guide**  
Tim McConaughy, Steve McNutt, Christopher Miles

## Appendix 1: Network Fundamentals





# 0.0.0.0

0 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0  
8 Bits            8 Bits            8 Bits            8 Bits

# 255.255.255.255

1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1  
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
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
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
							Add 2 + 1	= 3

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

11111111

Bit position	7	6	5	4	3	2	1	0	
Bit Value	1	1	1	1	1	1	1	1	= 255
Value	128	64	32	16	8	4	2	1	

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

Network		Point of Contact	
Net Range	8.8.8.0 - 8.8.8.255	Name	Google LLC
CIDR	8.8.8.0/24	Handle	ZG39-ARIN
Name	LVLT-GOGL-8-8-8	Company	Google LLC
Handle	NET-8-8-8-0-1	Street	1600 Amphitheatre Parkway
Parent	LVLT-ORG-8-8 (NET-8-0-0-0-1)	City	Mountain View
Net Type	Reallocated	State/Province	CA
Origin AS		Postal Code	94043
Organization	Google LLC (GOGL)	Country	US
Registration Date	2014-03-14	Registration Date	2000-11-30
Last Updated	2014-03-14	Last Updated	2022-11-10
Comments		Comments	
RESTful Link	<a href="https://whois.arin.net/rest/net/NET-8-8-8-0-1">https://whois.arin.net/rest/net/NET-8-8-8-0-1</a>	Phone	+1-650-253-0000 (Office)
See Also	<a href="#">Related organization's POC records</a>	Email	arin-contact@google.com
See Also	<a href="#">Related delegations</a>	RESTful Link	<a href="https://whois.arin.net/rest/poc/ZG39-ARIN">https://whois.arin.net/rest/poc/ZG39-ARIN</a>
Organization		Point of Contact	
Name	Google LLC	Name	Abuse
Handle	GOGL	Handle	ABUSE5250-ARIN
Street	1600 Amphitheatre Parkway	Company	Google Inc.
City	Mountain View	Street	1600 Amphitheatre Parkway
State/Province	CA	City	Mountain View
Postal Code	94043	State/Province	CA
Country	US	Postal Code	94043
Registration Date	2000-03-30	Country	US
Last Updated	2019-10-31	Registration Date	2015-11-06
Comments	Please note that the recommended way to file abuse complaints are located in the following links.  To report abuse and illegal activity: <a href="https://www.google.com/contact/">https://www.google.com/contact/</a>  For legal requests: <a href="http://support.google.com/legal">http://support.google.com/legal</a>  Regards, The Google Team	Last Updated	2022-10-24
RESTful Link	<a href="https://whois.arin.net/rest/org/GOGL">https://whois.arin.net/rest/org/GOGL</a>	Comments	Please note that the recommended way to file abuse complaints are located in the following links.  To report abuse and illegal activity: <a href="https://www.google.com/contact/">https://www.google.com/contact/</a>  For legal requests: <a href="http://support.google.com/legal">http://support.google.com/legal</a>  Regards, The Google Team
Function	Point of Contact	Phone	+1-650-253-0000 (Office)
Admin	ZG39-ARIN (ZG39-ARIN)	Email	network-abuse@google.com
Tech	ZG39-ARIN (ZG39-ARIN)	RESTful Link	<a href="https://whois.arin.net/rest/poc/ABUSE5250-ARIN">https://whois.arin.net/rest/poc/ABUSE5250-ARIN</a>
Abuse	ABUSE5250-ARIN (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

= 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

= 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

1 1 1 1 1 1 1 1 . 1 1 1 1 0 0 0 0 . 0 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0 = /12  
255.240.0.0

1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 . 1 1 1 1 1 1 0 . 0 0 0 0 0 0 0 0 = /23  
255.255.254.0

1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 . 1 1 1 1 1 0 0 0 = /29  
255.255.255.248

IP subnet: <b>192.168.0.0/24</b>	Reserved addresses
<u>1 1 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 . 0 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0</u> Network Host	<b>192.168.0.0</b> (Network address)
<u>1 1 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 . 0 0 0 0 0 0 0 . 1 1 1 1 1 1 1 1</u> Network Host	<b>192.168.0.255</b> (Network address)

IP subnet: <b>10.18.240.64/28</b>	Reserved addresses
<u>0 0 0 0 1 0 1 0 . 0 0 0 1 0 0 1 0 . 1 1 1 1 0 0 0 0 . 0 1 0 0 0 0 0 0</u> Network Host	<b>10.18.240.64</b> (Network address)
<u>0 0 0 0 1 0 1 0 . 0 0 0 1 0 0 1 0 . 1 1 1 1 0 0 0 0 . 0 1 0 0 1 1 1 1</u> Network Host	<b>10.18.240.79</b> (Network address)

Value	128	64	32	16	8	4	2	1

↑                      ↑  
Sufficient            Too small

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)

Value	32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

↑  
Sufficient

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**

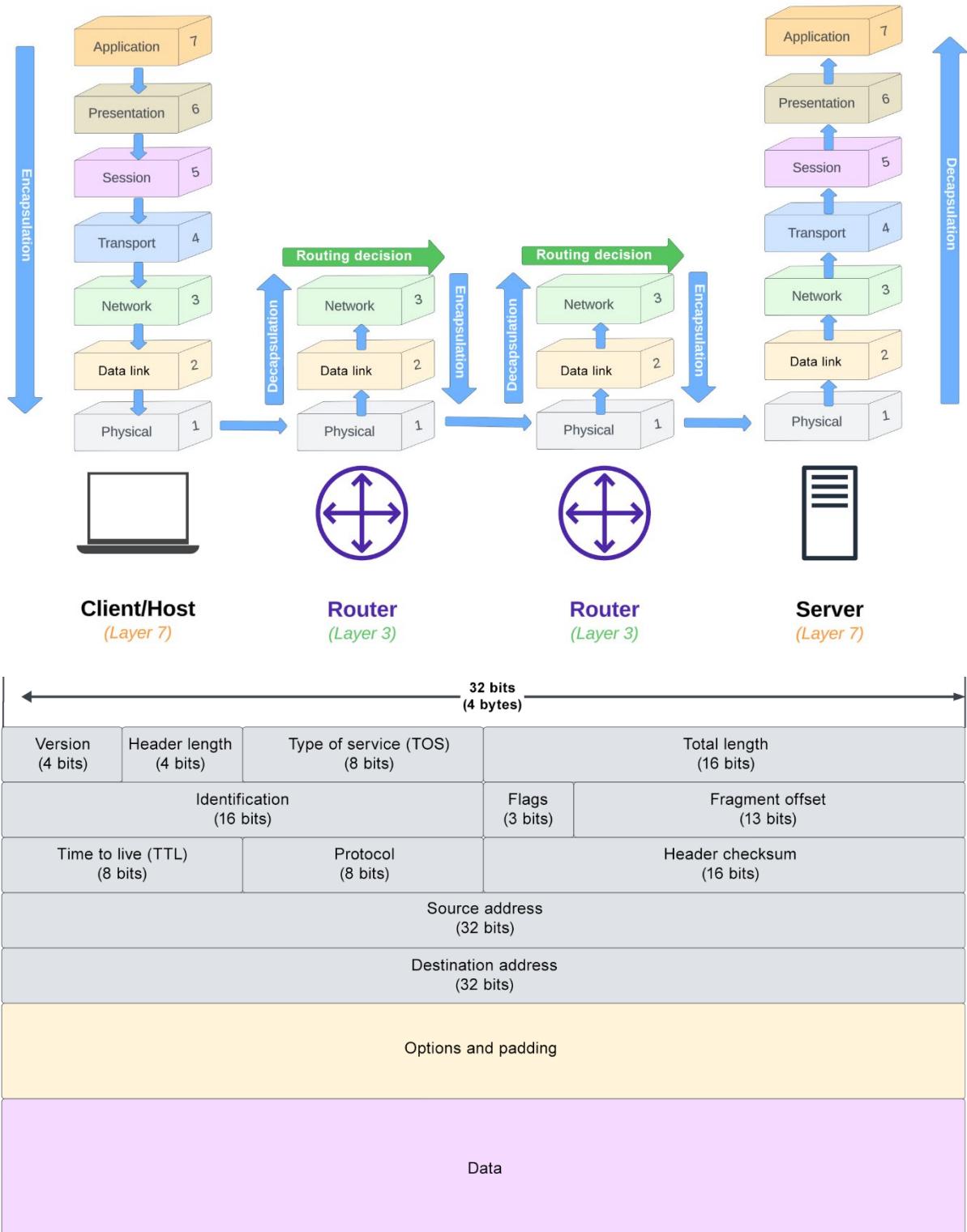
0000000000000000 : 0000000000000000 : 0000000000000000 : 0000000000000000 :  
 ↓                      ↓                      ↓                      ↓  
 16 Bits                16 Bits                16 Bits                16 Bits  
 0000000000000000 : 0000000000000000 : 0000000000000000 : 0000000000000000

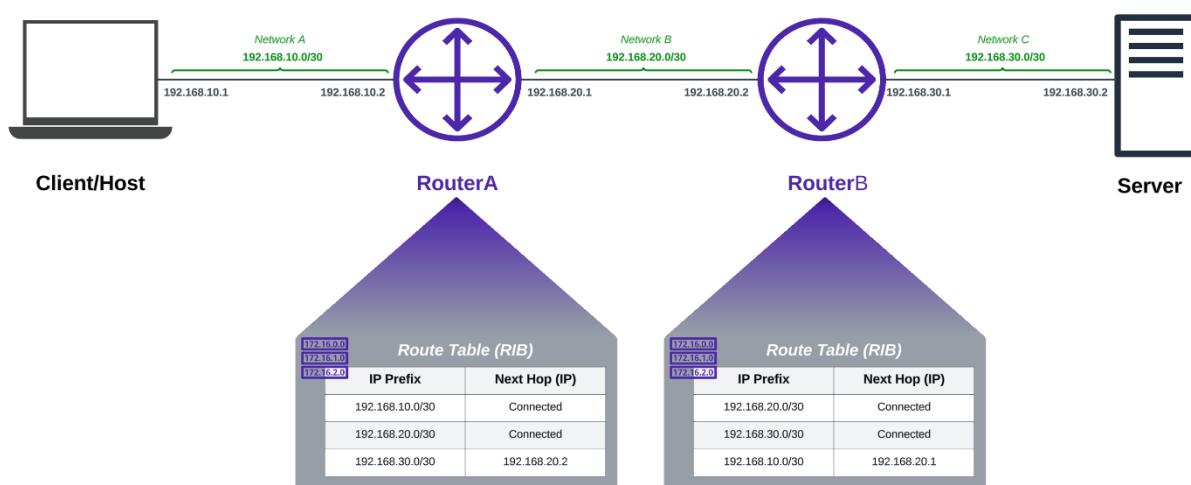
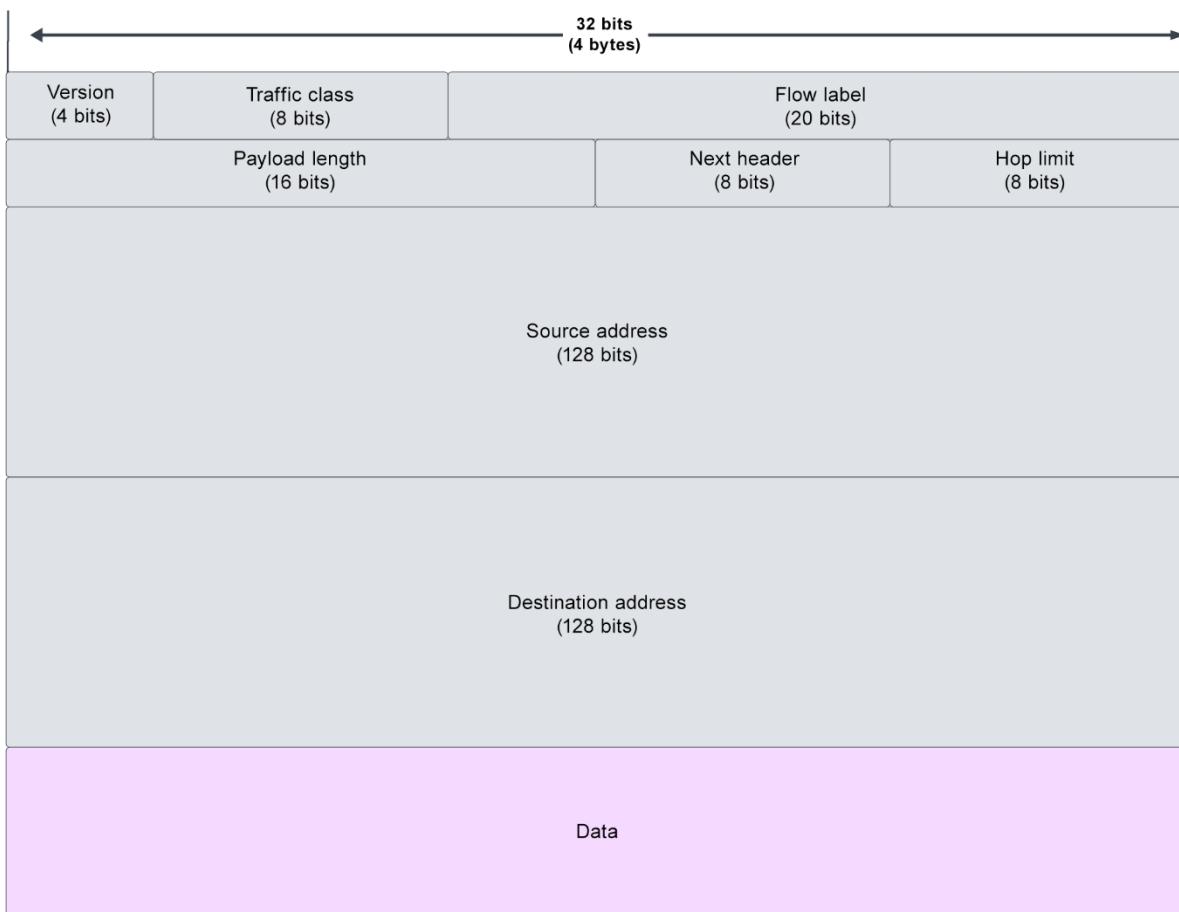
**FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF**

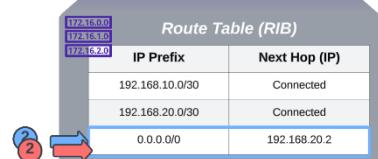
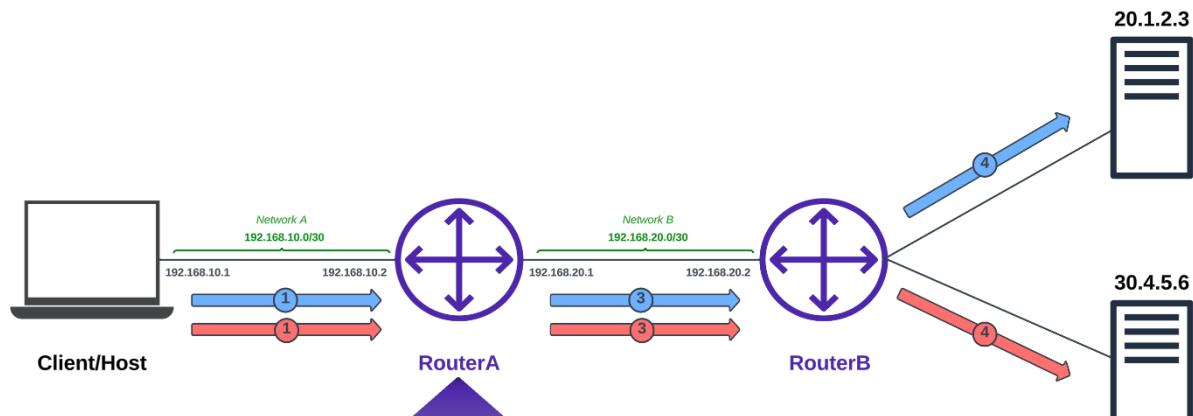
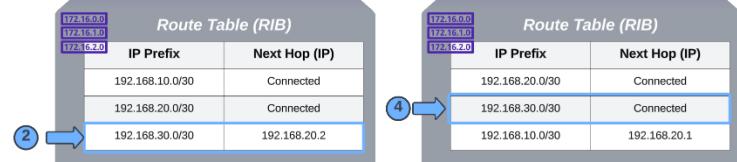
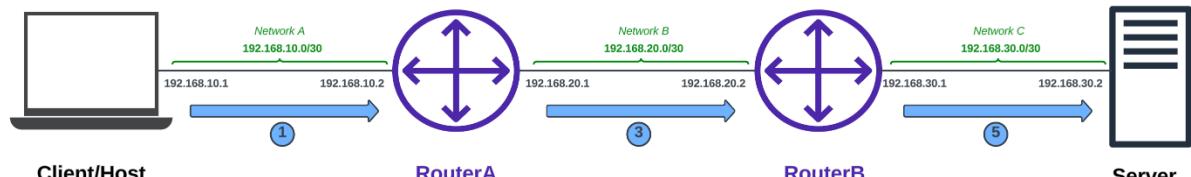
1111111111111111 : 1111111111111111 : 1111111111111111 : 1111111111111111 :  
 ↓                      ↓                      ↓                      ↓  
 16 Bits                16 Bits                16 Bits                16 Bits  
 1111111111111111 : 1111111111111111 : 1111111111111111 : 1111111111111111

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



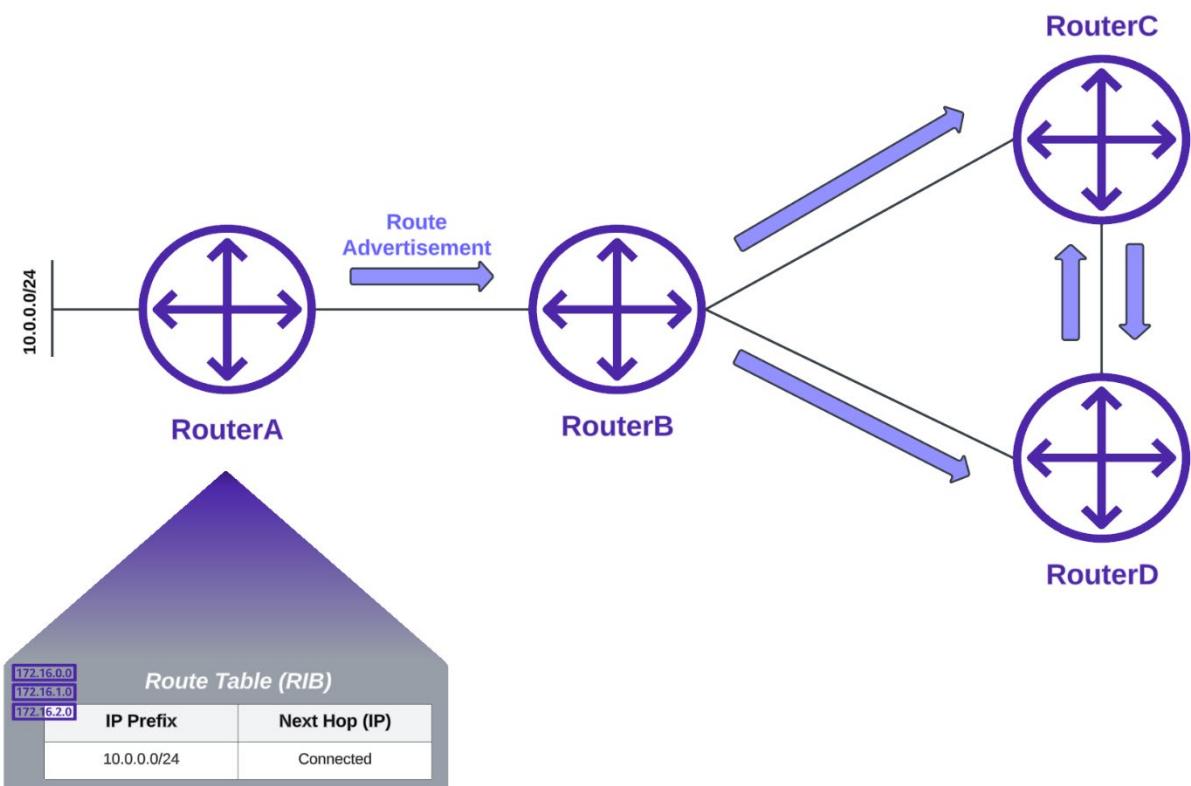




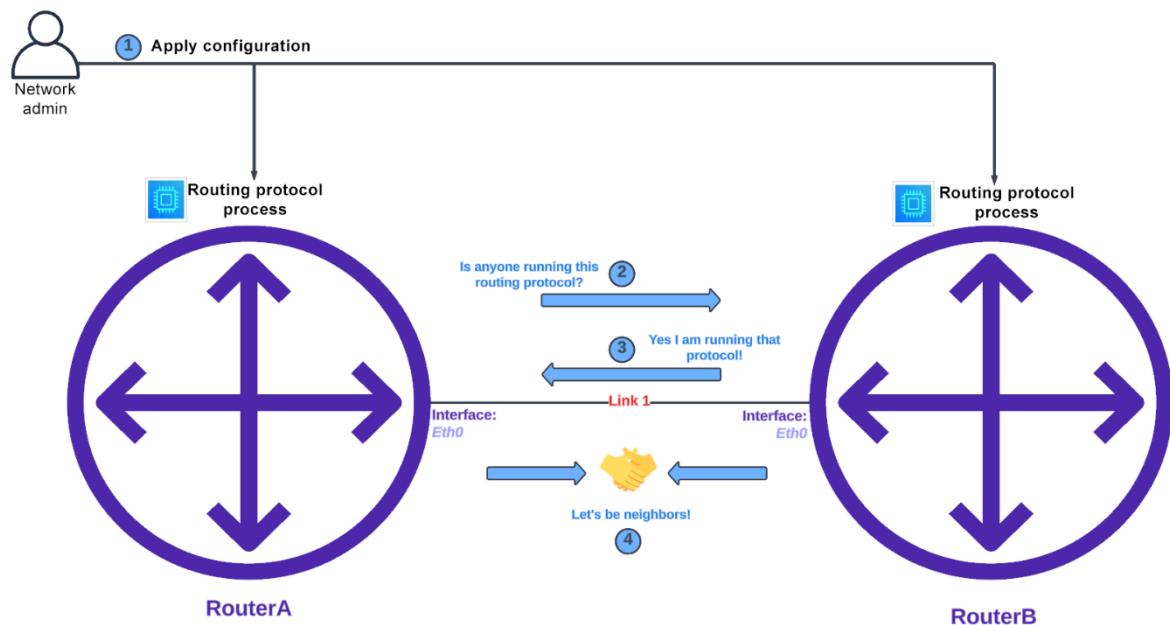
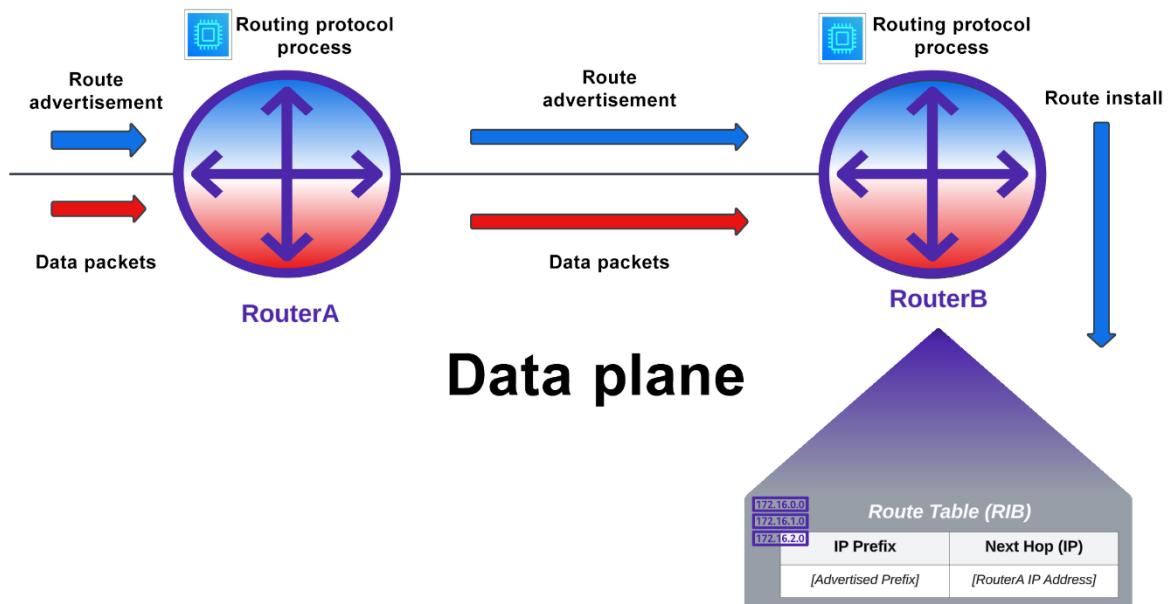
```
C:\Users\█████>route print
=====
Interface List
17...b4 2e 99 39 07 40 ....Intel(R) Ethernet Connection (7) I219-V
7...02 13 ef 1b 01 06 ....Microsoft Wi-Fi Direct Virtual Adapter
11...00 13 ef 1b 01 06 ....Microsoft Wi-Fi Direct Virtual Adapter #2
10...00 50 56 c0 00 01 ....VMware Virtual Ethernet 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
=====

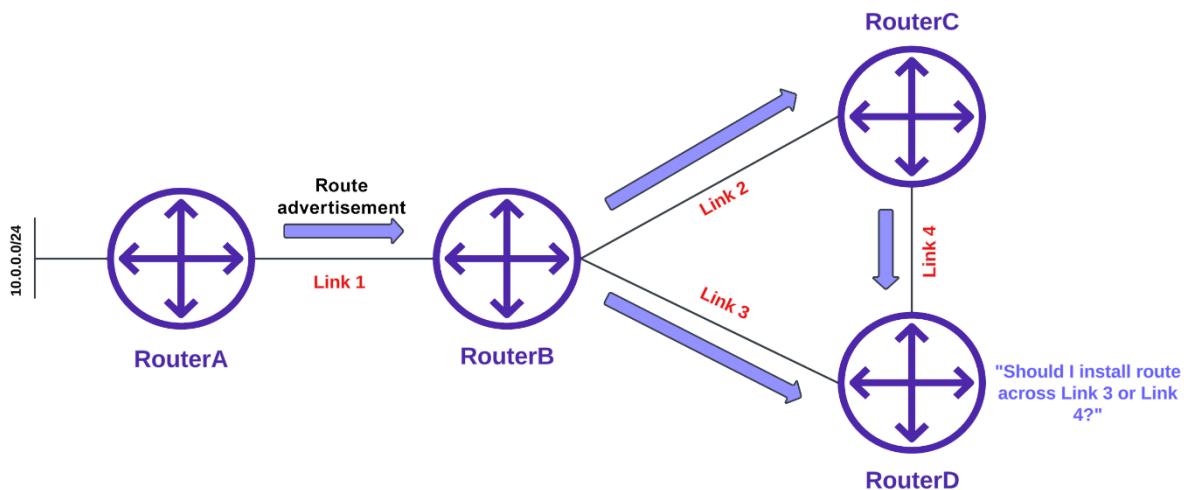
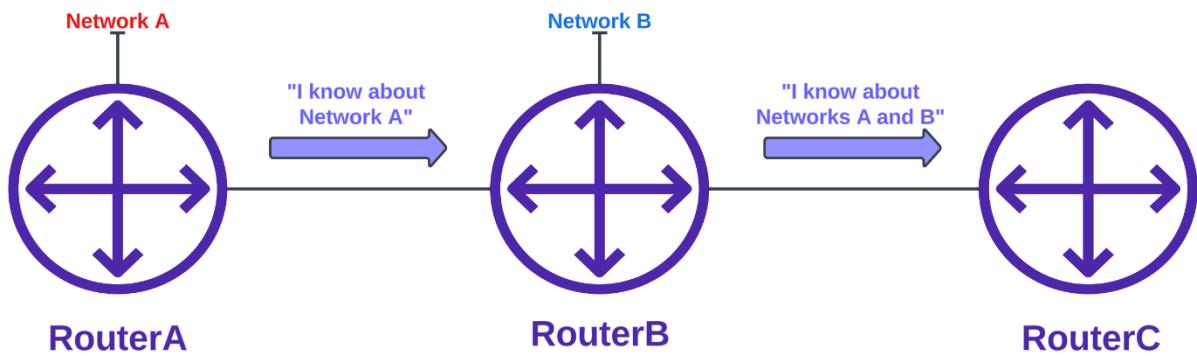
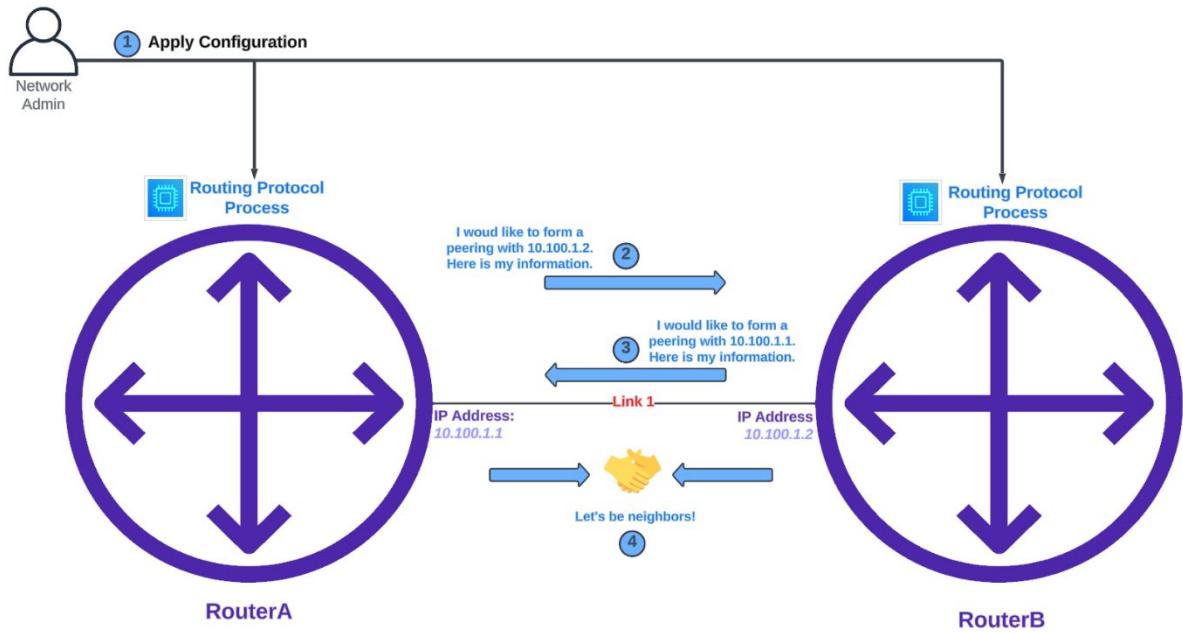
IPv4 Route Table
=====
Active Routes:
Network Destination      Netmask          Gateway        Interface Metric
          0.0.0.0        0.0.0.0    192.168.0.1    192.168.0.37    35
         127.0.0.0      255.0.0.0   On-link        127.0.0.1     331
         127.0.0.1  255.255.255.255   On-link    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

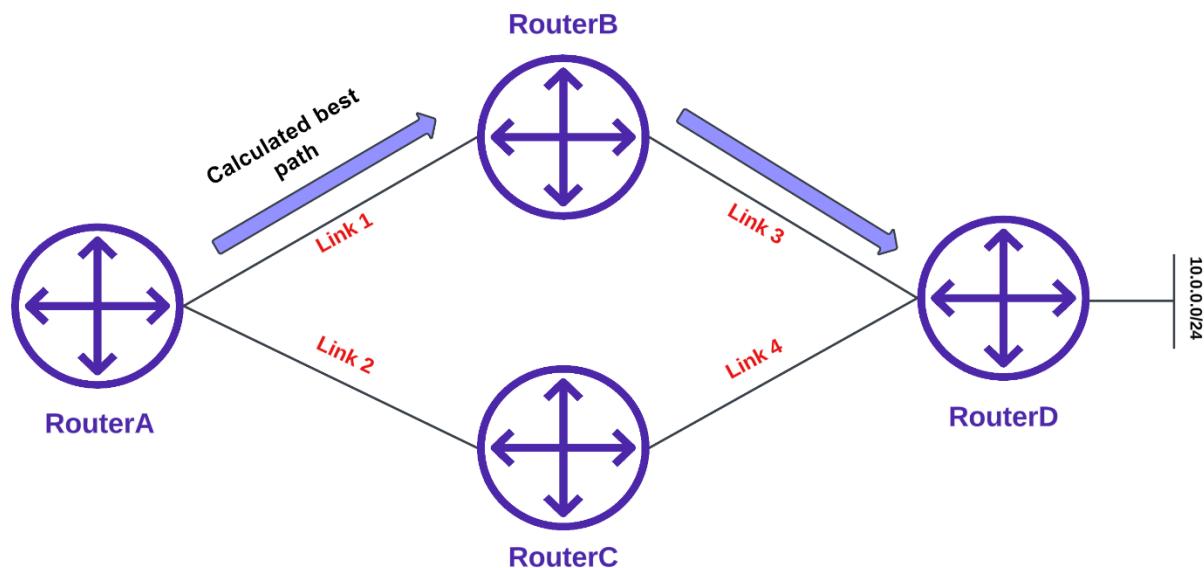
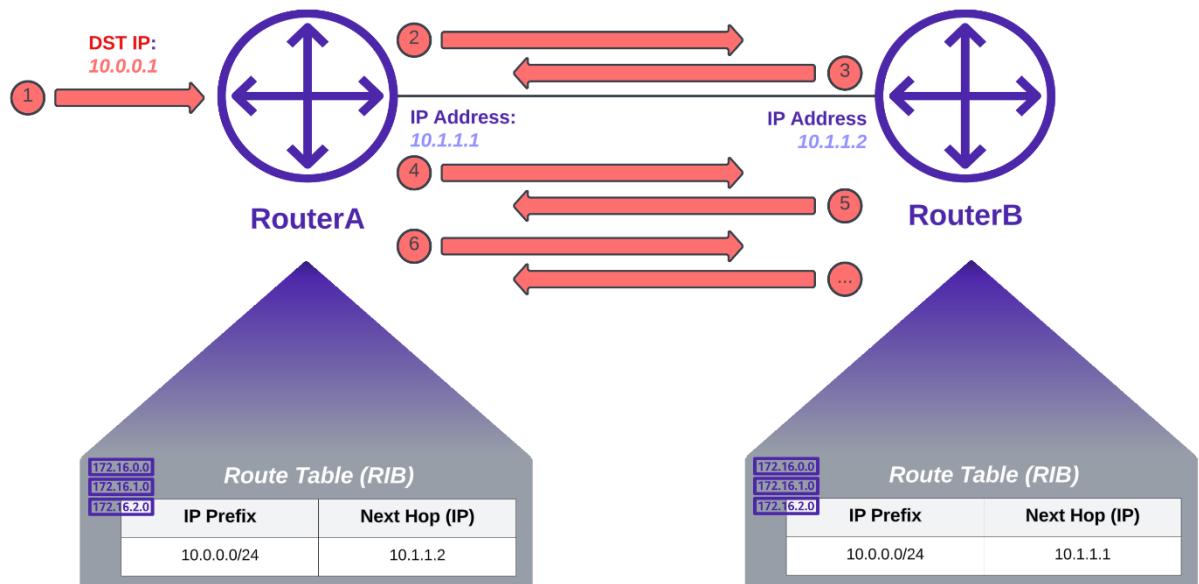
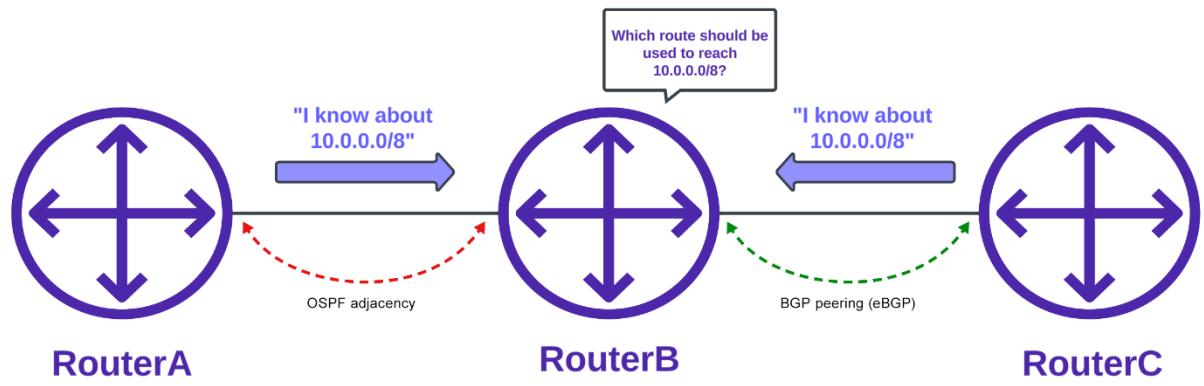
```
█████@ubuntu:~$ netstat -r
Kernel IP routing table
Destination      Gateway          Genmask        Flags  MSS Window irtt Iface
default        _gateway        0.0.0.0        UG        0 0          0 ens33
10.10.0.0      0.0.0.0        255.255.0.0    U        0 0          0 br-1bd7568ce6af
link-local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

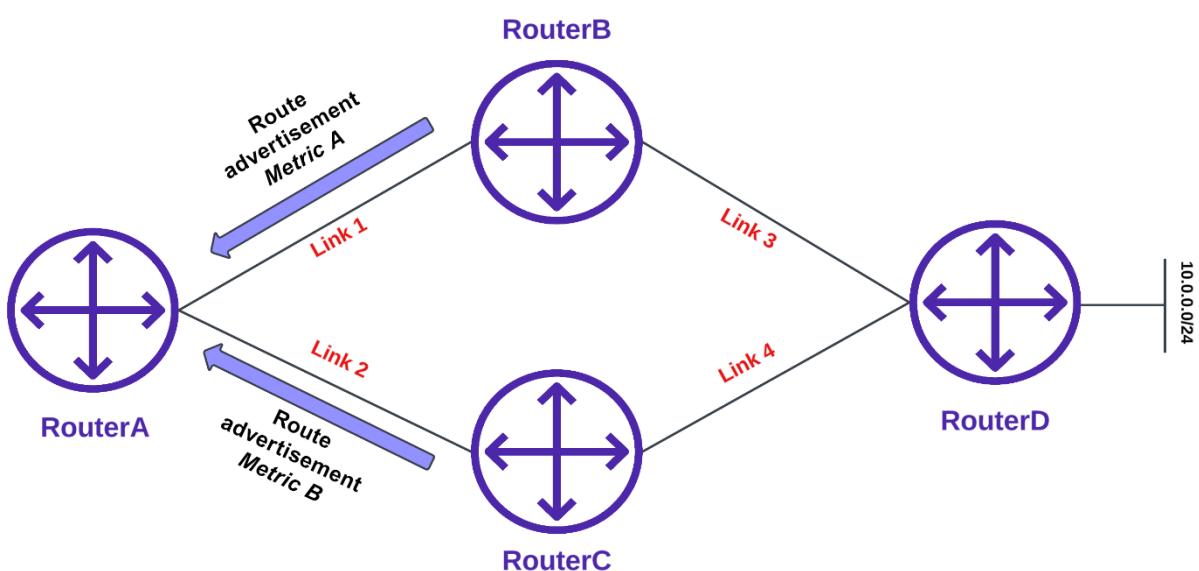
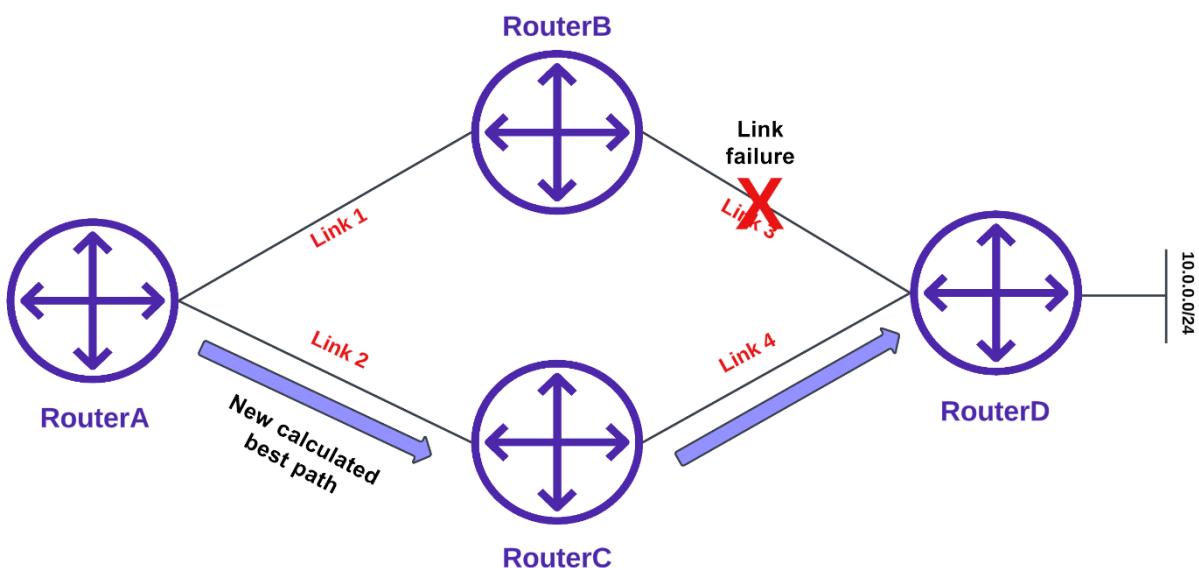
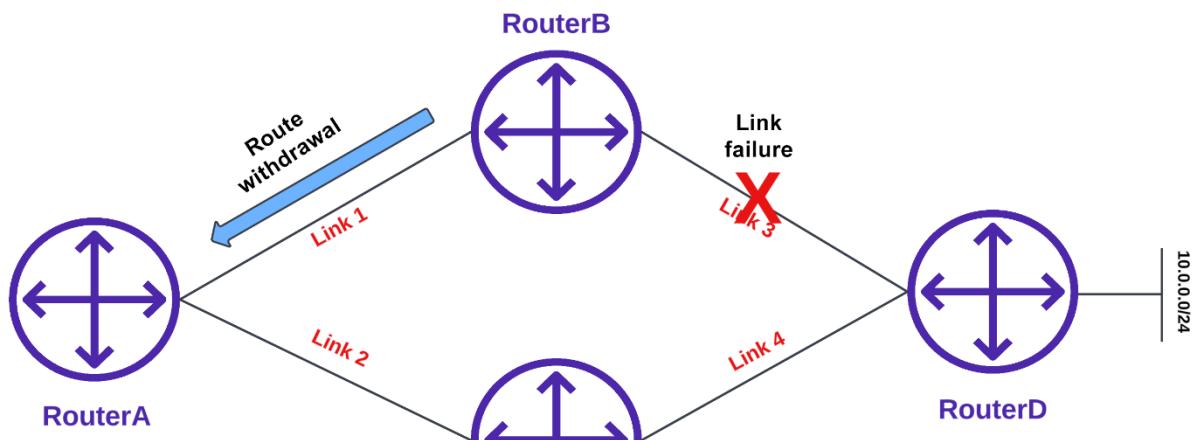


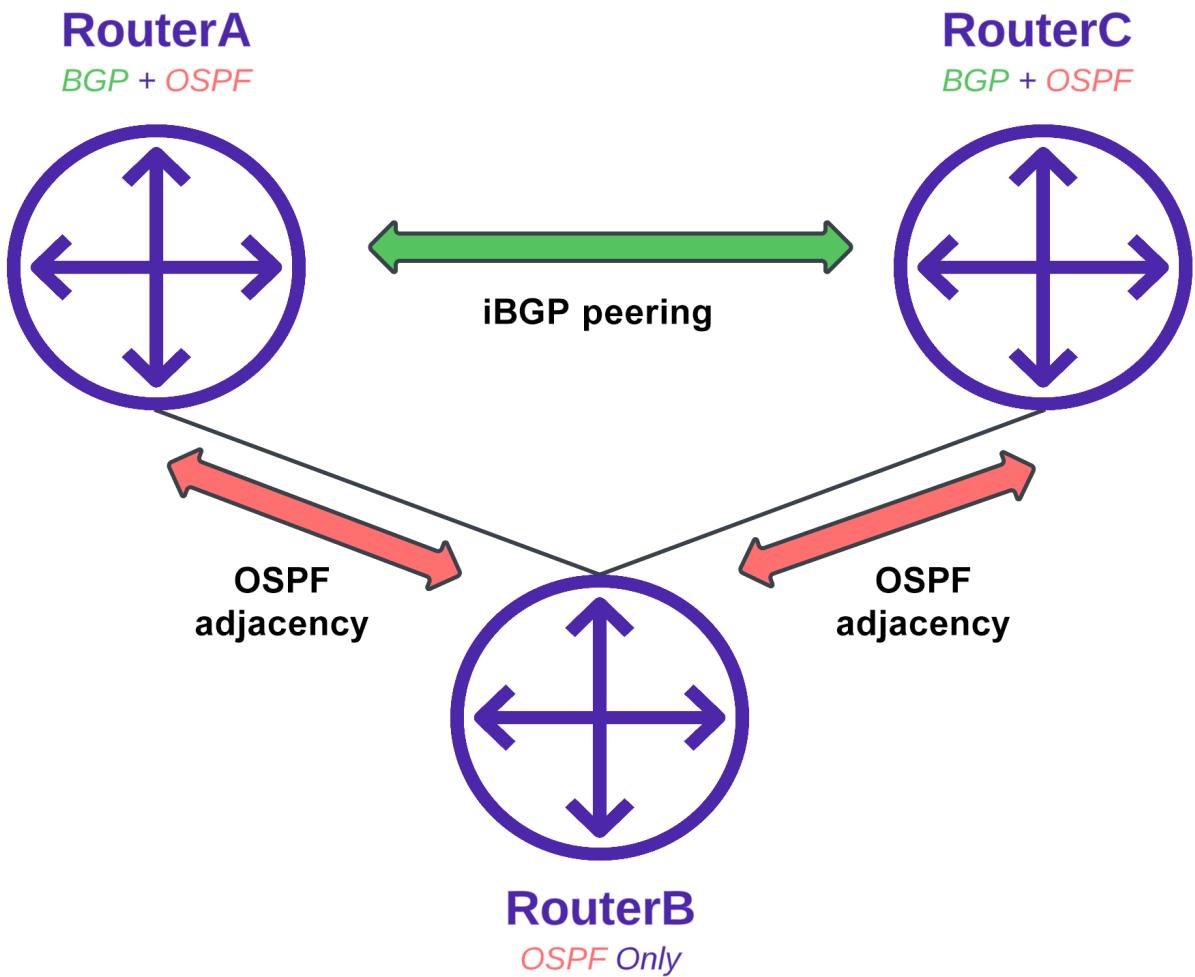
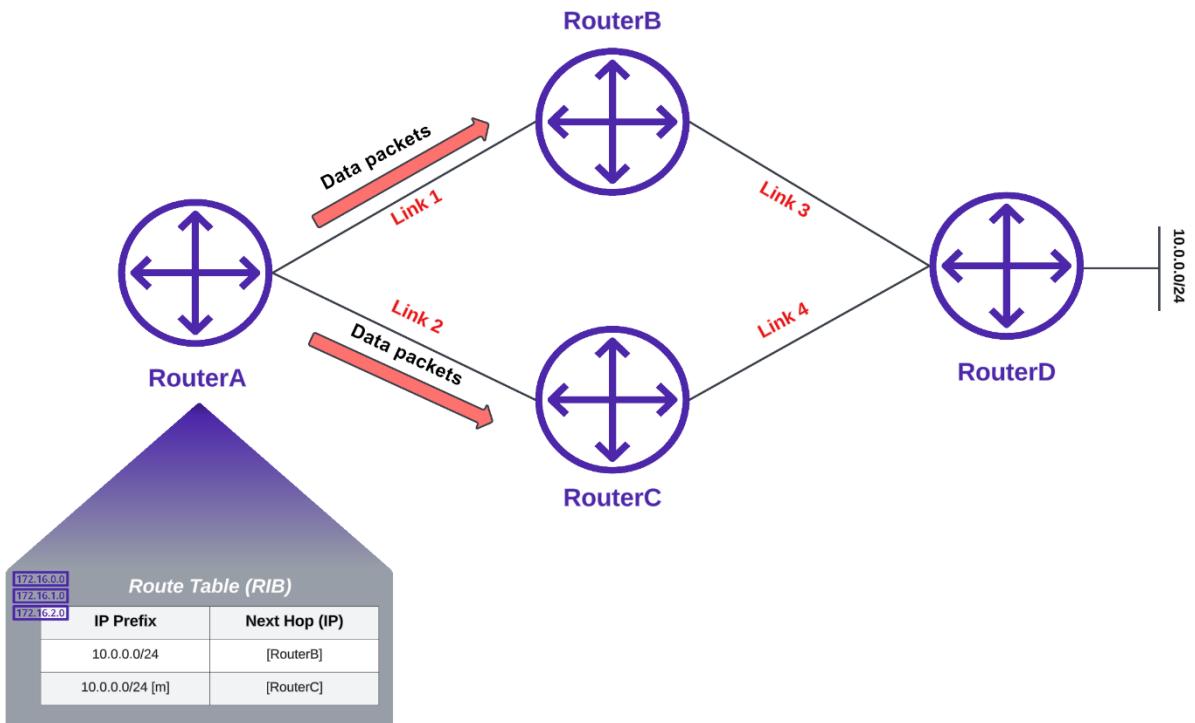
# Control plane

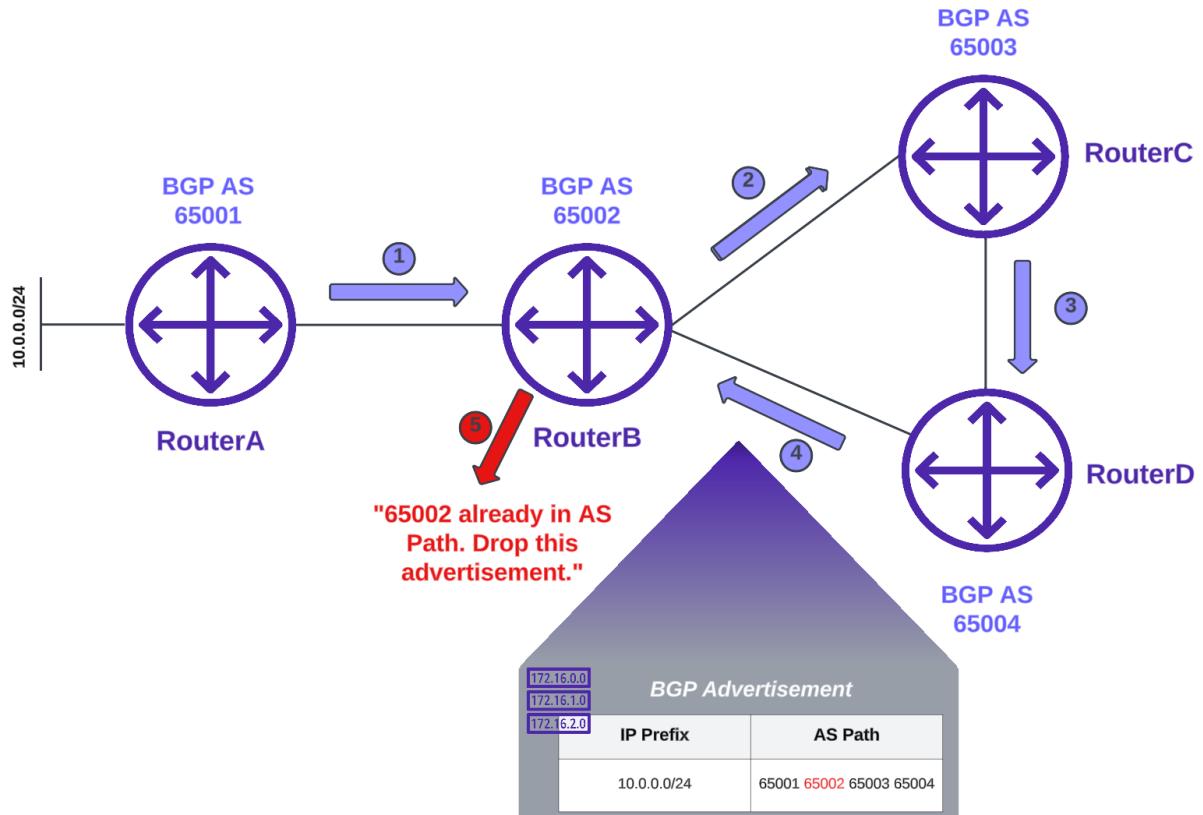




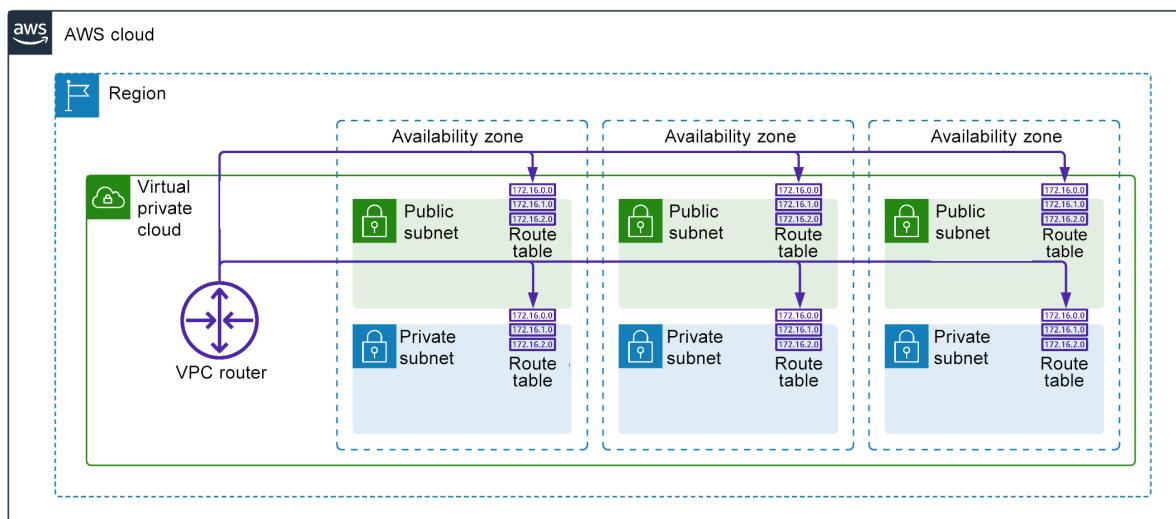
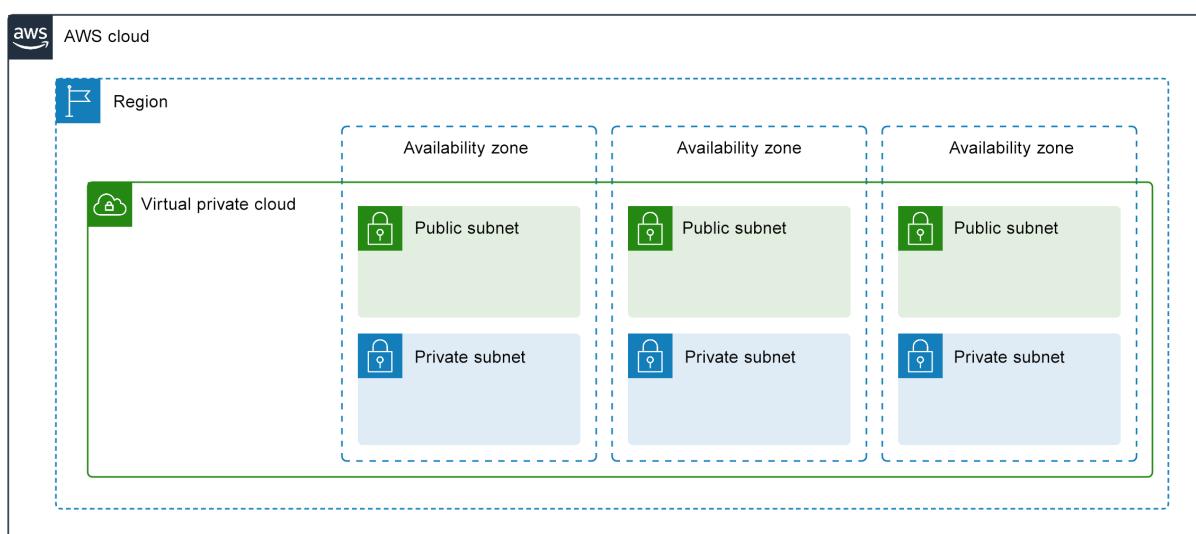
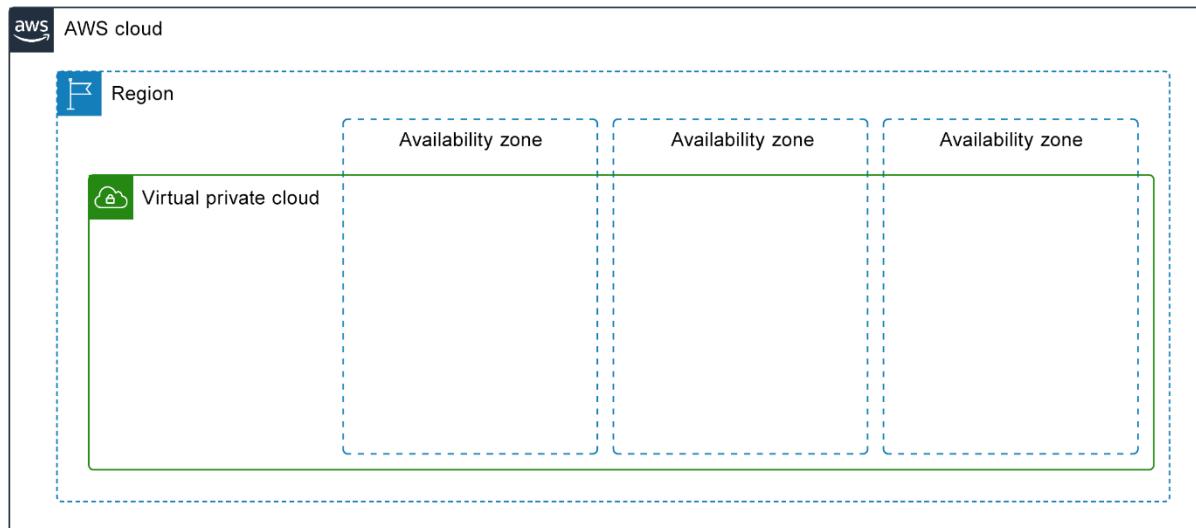


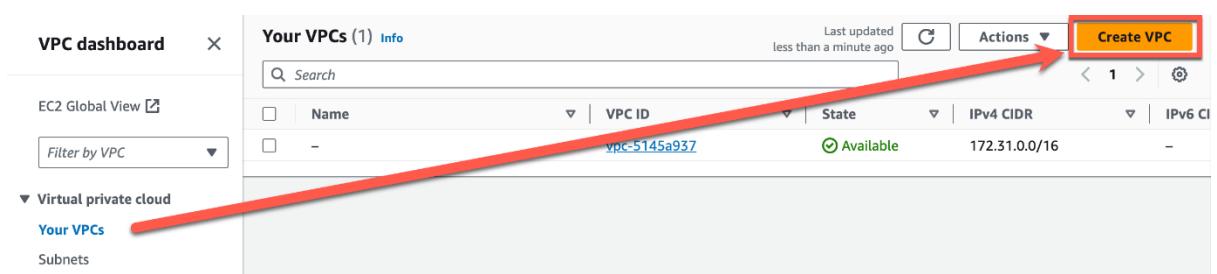
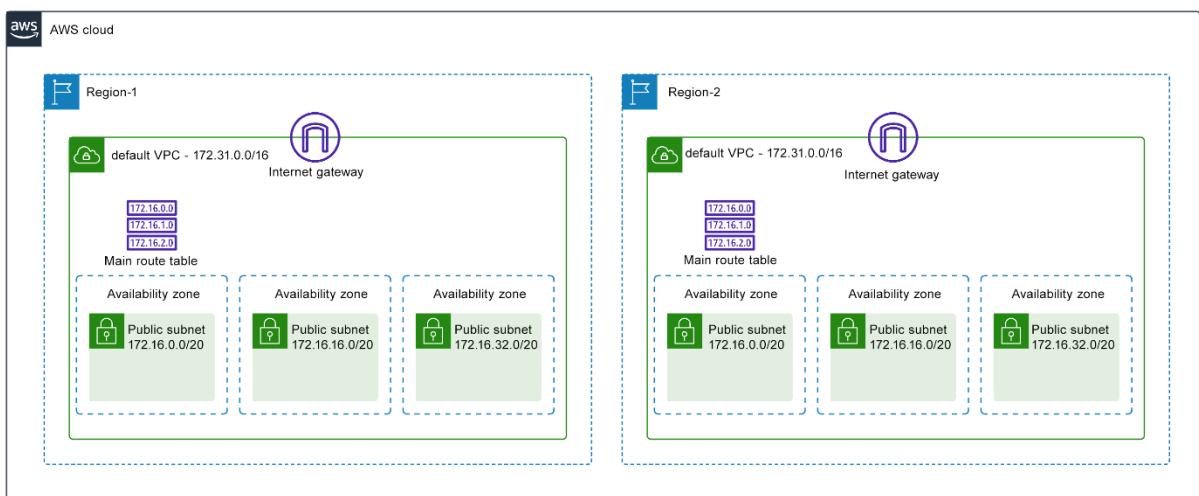
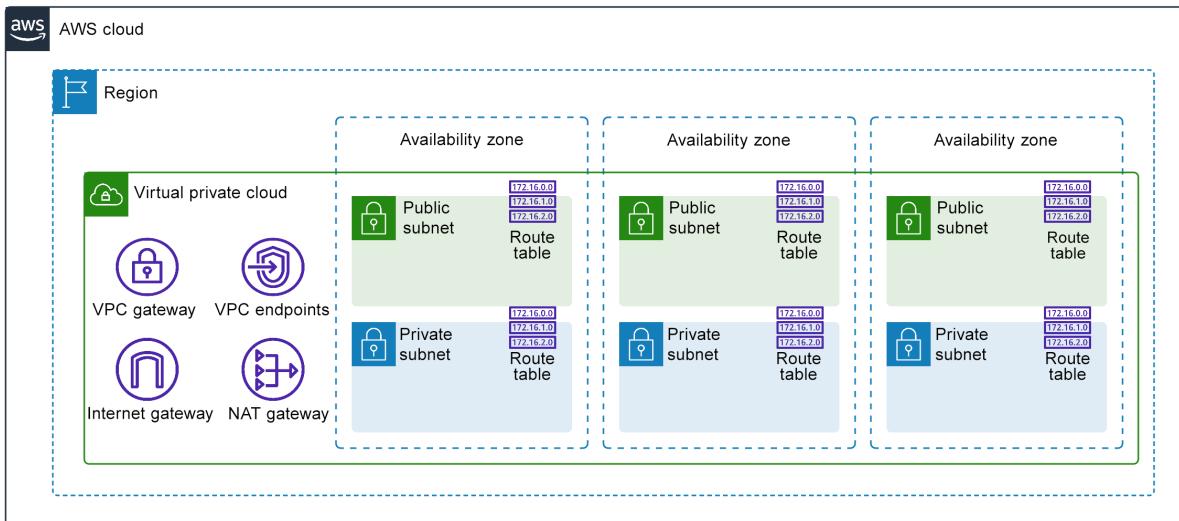






## Appendix 3, VPC Networking Basics





# 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](#)

### 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 auto-generation:** [Info](#)

Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.

Auto-generate

**IPv4 CIDR block:** [Info](#)

Determine the starting IP and the size of your VPC using CIDR notation.

10.0.0.0/16	65,536 IPs
-------------	------------

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

**IPv6 CIDR block:** [Info](#)

No IPv6 CIDR block  Amazon-provided IPv6 CIDR block

**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

### Preview

aws Services Search [Option+S]

EC2 VPC AWS Marketplace S3 CloudFormation Direct Connect Route 53 N. Virginia

**VPC dashboard** ×

Your VPCs (2) [Info](#)

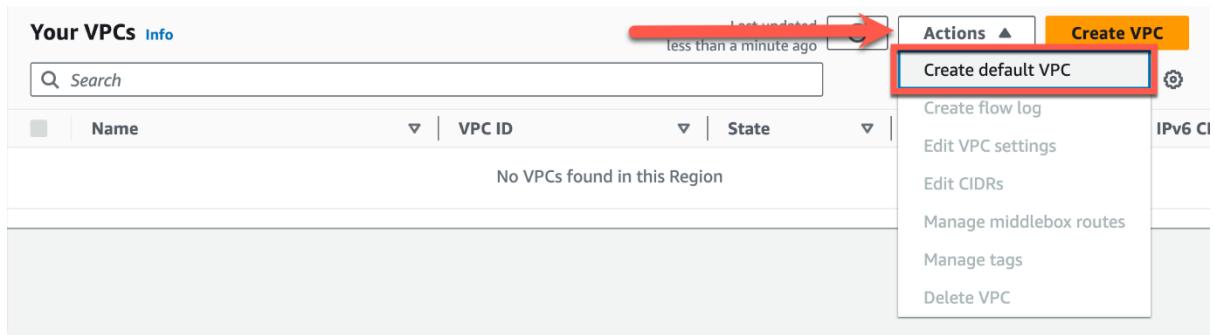
Your VPCs (2) <a href="#">Info</a>						
Last updated less than a minute ago						
<input type="checkbox"/>	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP option set
<input type="checkbox"/>	-	VPC- <span style="background-color: #f0f0f0; border-radius: 5px; padding: 2px 5px;">XXXXXXXXXX</span>	<span style="color: green;">Available</span>	172.31.0.0/16	2600:1f18:326d:3900::/56	<span style="background-color: #f0f0f0; border-radius: 5px; padding: 2px 5px;">XXXXXXXXXX</span>
<input type="checkbox"/>	test-vpc	VPC- <span style="background-color: #f0f0f0; border-radius: 5px; padding: 2px 5px;">XXXXXXXXXX</span>	<span style="color: green;">Available</span>	10.0.0.0/16	-	<span style="background-color: #f0f0f0; border-radius: 5px; padding: 2px 5px;">XXXXXXXXXX</span>

EC2 Global View [Filter by VPC](#)

Virtual private cloud [Your VPCs](#)

Subnets

↗



[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

X

### 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

X

### IPv6 CIDR block

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

### Pool

Choose pool



### Pool CIDRs

-

CancelSelect CIDR

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

Last updated 20 minutes ago [C](#)

<input checked="" type="checkbox"/>	Name	VPC ID	State	
<input checked="" type="checkbox"/>	example-vpc	<a href="#">vpc-061398475af93e0fe</a>	<span>Available</span>	<a href="#">Edit CIDRs</a>

Create default VPC

Create flow log

Edit VPC settings

Edit CIDRsIPv6 C

Manage middlebox routes

Manage tags

Delete VPC

## 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

X

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

X

IPv6 CIDR block

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

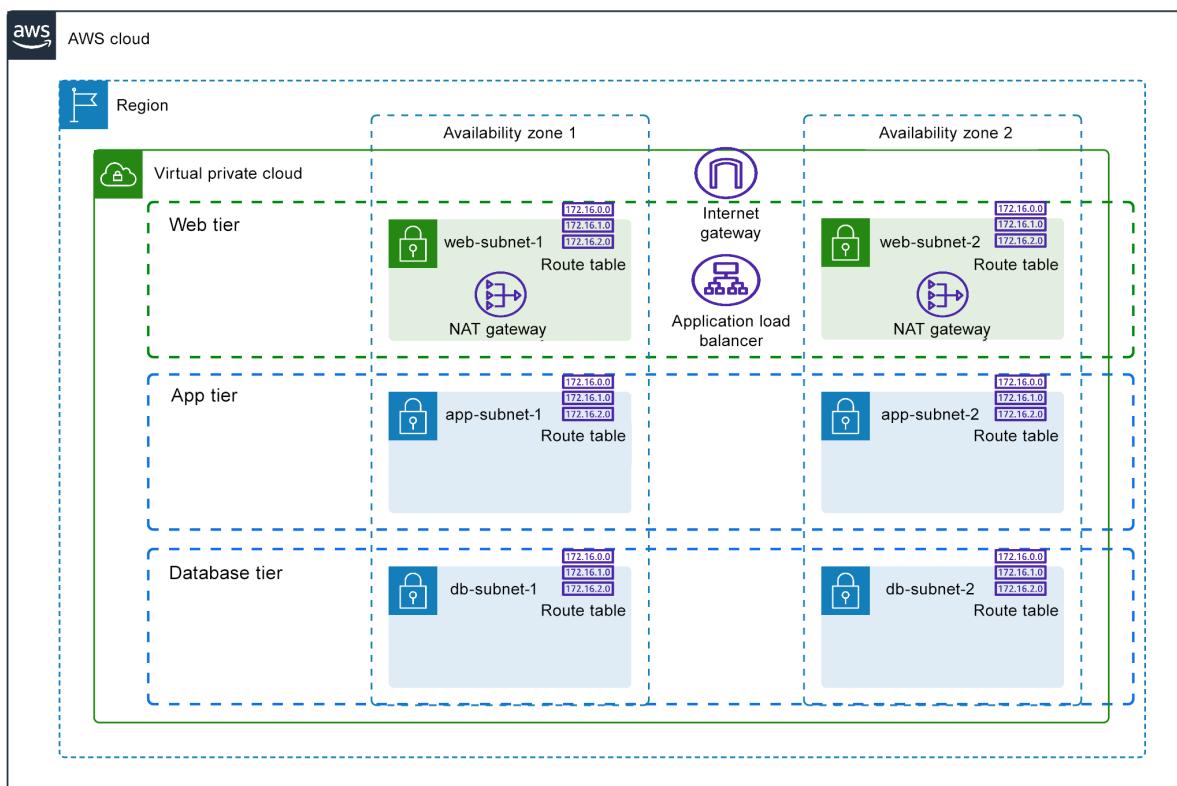
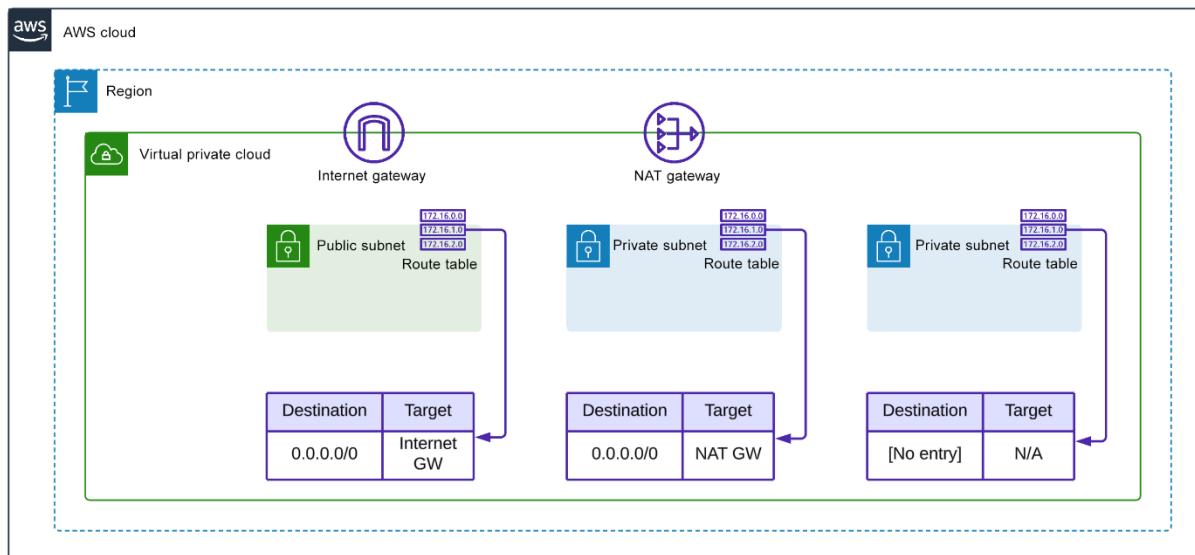
#### Network border group

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



**VPC dashboard**

**Subnets** **Info**

Last updated less than a minute ago

**Create subnet**

**Actions**

**Subnets**

Find resources by attribute or tag

No subnet found

**Select a subnet**

**EC2 Global View**

**Filter by VPC**

**Virtual private cloud**

Your VPCs

**Subnets**

Route tables

Internet gateways

Egress-only Internet gateways

## 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

< > ^ v

##### ▼ Tags - optional

No tags associated with the resource.

Add new tag

You can add 50 more tags.

Remove

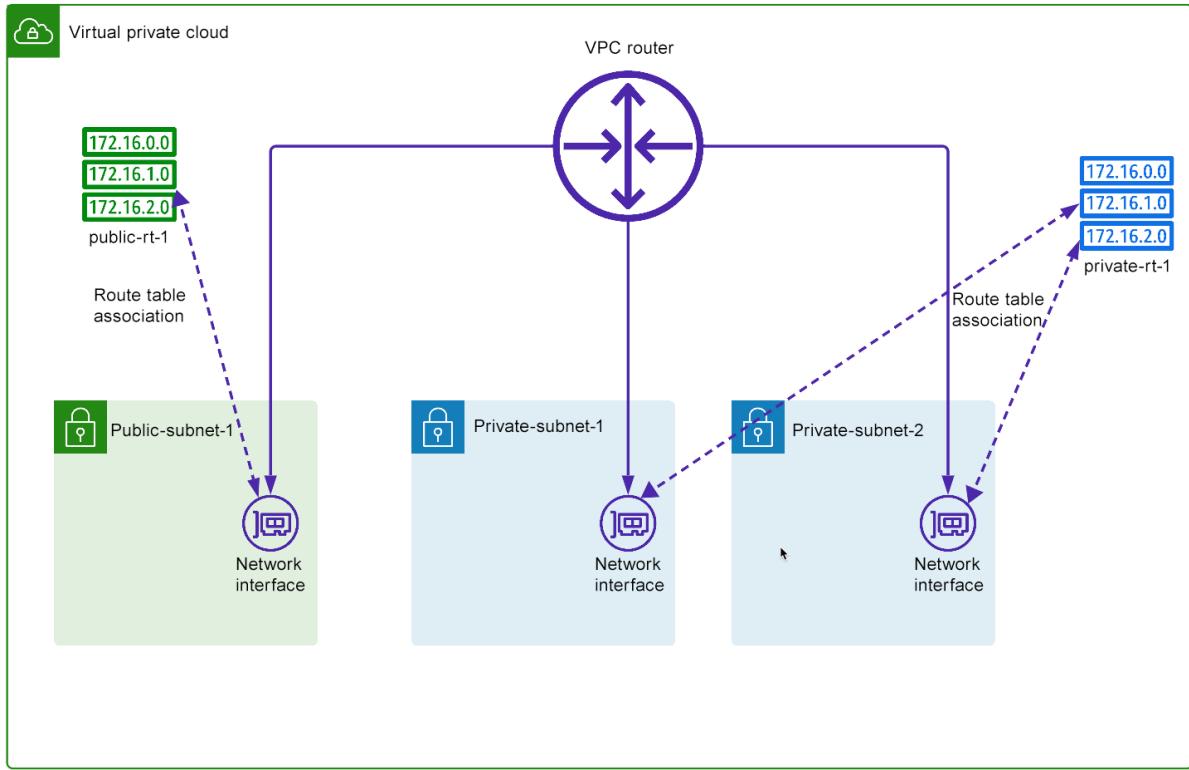
Add new subnet



**Configure additional subnets**

Cancel

Create subnet



[VPC](#) > [Route tables](#) > [rtb-0c6bd67941c2574ef](#)

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

[Actions ▾](#)

Details		Info	
Route table ID	<a href="#">rtb-0c6bd67941c2574ef</a>	Main	<input type="checkbox"/> No
VPC	<a href="#">vpc-021c84d09b2b7a0d0</a>   <a href="#">vpc-use1-test</a>	Owner ID	<input type="checkbox"/>
		Explicit subnet associations	-
		Edge associations	-

[Routes](#) [Subnet associations](#) [Edge associations](#) [Route propagation](#) [Tags](#)

**Routes (3)**

[Filter routes](#) [Both ▾](#) [Edit routes](#)

Destination	Target	Status	Propagated
0.0.0.0/0	<a href="#">igw-0a5bb00ff69314b96</a>	Active	No
10.0.0.0/24	local	Active	No
10.140.0.0/16	<a href="#">pcx-0c0f4d7d60586f64b</a>	Active	No

**Routes (3)**

[Filter routes](#) [Both ▾](#) [Edit routes](#)

Destination	Target	Status	Propagated
0.0.0.0/0	<a href="#">igw-0a5bb00ff69314b96</a>	Active	No
10.0.0.0/24	local	Active	No
10.140.0.0/16	<a href="#">pcx-0c0f4d7d60586f64b</a>	Blackhole	No

Route tables (1/3) [Info](#)

Last updated 12 minutes ago [C](#) Actions [Create route table](#)

<input type="checkbox"/>	Name	Route table ID	Explicit s...	Edge associations	Main
<input checked="" type="checkbox"/>	-	<a href="#">rtb-0088e066078003074</a>	-	-	Yes
<input type="checkbox"/>	route-table-test-01	<a href="#">rtb-0c6bd67941c2574ef</a>	-	-	No

**rtb-0088e066078003074**

[Details](#) | [Routes](#) | [Subnet associations](#) | [Edge associations](#) | [Route propagation](#) | [Tags](#)

**Details**

Route table ID <a href="#">rtb-0088e066078003074</a>	Main <input checked="" type="checkbox"/> Yes	Explicit subnet associations -	Edge associations -
VPC <a href="#">vpc-0c953a08a371039c7</a>	Owner ID <a href="#">[REDACTED]</a>		

Route tables (1/2) [Info](#)

Last updated less than a minute ago [C](#) Actions [Create route table](#)

<input type="checkbox"/>	Name	Route table ID	Explicit subnet associations	Edge associations
<input checked="" type="checkbox"/>	route-table-public-01	<a href="#">rtb-05e23849b86d939a8</a>	<a href="#">subnet-0134258570f74be2f / public-subnet-01</a>	-
<input type="checkbox"/>	route-table-private-01	<a href="#">rtb-0c6bd67941c2574ef</a>	<a href="#">subnet-0ffabbd4cf7346ab6f / private-subnet-01</a>	-

**rtb-05e23849b86d939a8 / route-table-public-01**

[Details](#) | [Routes](#) | [Subnet associations](#) | [Edge associations](#) | [Route propagation](#) | [Tags](#)

**Explicit subnet associations (1)**

[Edit subnet associations](#)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
public-subnet-01	<a href="#">subnet-0134258570f74be2f</a>	10.0.0.16/28	-

**Subnets (1/2) [Info](#)**

Last updated 3 minutes ago [Edit](#) Actions [Create subnet](#)

Find resources by attribute or tag

Name Subnet ID State VPC

<input checked="" type="checkbox"/> public-subnet-01	subnet-0134258570f74be2f	<span>Available</span>	vpc-021c84d09b2b7a0d0   vpc-...
<input type="checkbox"/> private-subnet-01	subnet-0ffabd4cf7346ab6f	<span>Available</span>	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	<a href="#">igw-0a5bb00ff69314b96</a>

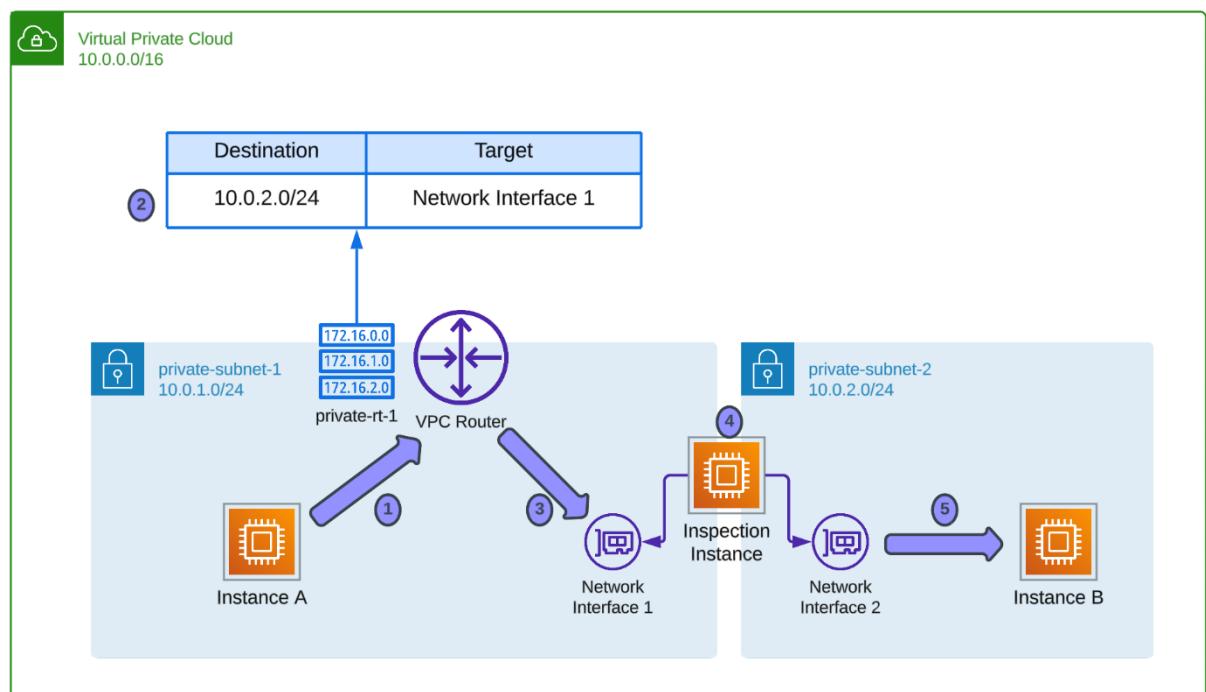
### rtb-05e23849b86d939a8 / route-table-public-01

Details [Routes](#) Subnet associations Edge associations Route propagation Tags

**Routes (2)**

Filter routes

Destination	Target	Status	Propagated
0.0.0.0/0	<a href="#">igw-0a5bb00ff69314b96</a>	<span>Active</span>	No
10.0.0.0/24	local	<span>Active</span>	No



**VPC dashboard**

**Route tables (1) Info**

Last updated 14 minutes ago

**Actions** 

Name	Route table ID	Explicit subnet associations	Edge ass...
-	rtb-009455eca80e7a9c0	-	-

**Virtual private cloud**

- Your VPCs
- Subnets
- Route tables** 
- Internet gateways
- Egress-only Internet

**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.

**VPC**  
The VPC to use for this route table.

### 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**

## rtb-06a2659bc8fc90b7e / example-route-table

[Details](#) [Info](#)

Route table ID  
rtb-06a2659bc8fc90b7e  
VPC  
vpc-061398475af93e0fe |  
example-vpc

Main  
No

Owner ID  
637132168754

Explicit subnet associations

- Actions ▾
- [Set main route table](#)
  - [Edit subnet associations](#)
  - [Edit edge associations](#)
  - [Edit route propagation](#)
  - [Edit routes](#)
  - [Manage tags](#)
  - [Delete](#)

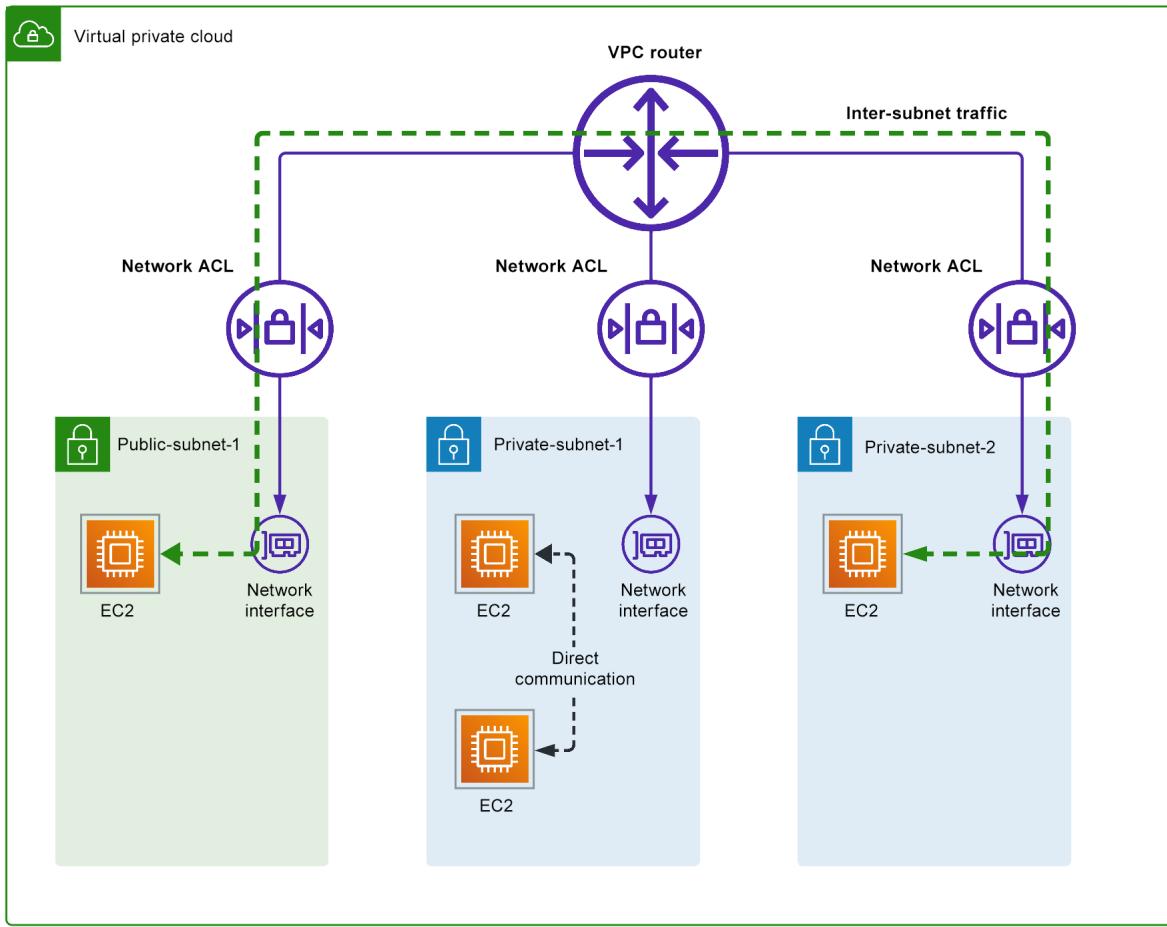
[Routes](#) [Subnet associations](#) [Edge associations](#) [Route propagation](#) [Tags](#)

## Routes (1)

 Filter routes[Both ▾](#) [Edit 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
<b>Inbound rules (5)</b>				
<input type="text"/> Filter inbound rules				
Rule number	Type	Protocol	Port range	Source
100	HTTPS (443)	TCP (6)	443	10.10.0.0/16
150	SSH (22)	TCP (6)	22	10.0.0.0/8
200	All ICMP - IPv4	ICMP (1)	All	0.0.0.0/0
*	All traffic	All	All	0.0.0.0/0
*	All traffic	All	All	::/0

## acl-01e24ab98687a78c8 / test-nacl

Details	Inbound rules	Outbound rules	Subnet associations	Tags
<b>Outbound rules (4)</b>				
<input type="text"/> Filter outbound rules				
Rule number	Type	Protocol	Port range	Destination
100	All traffic	All	All	0.0.0.0/0
200	All traffic	All	All	::/0
*	All traffic	All	All	0.0.0.0/0
*	All traffic	All	All	::/0
<b>Inbound rules (7)</b>				
<input type="text"/> Filter inbound rules				
Rule number	Type	Protocol	Port range	Source
100	HTTPS (443)	TCP (6)	443	10.10.0.0/16
150	SSH (22)	TCP (6)	22	10.0.0.0/8
200	All ICMP - IPv4	ICMP (1)	All	0.0.0.0/0
3000	All traffic	All	All	0.0.0.0/0
3001	All traffic	All	All	::/0
*	All traffic	All	All	0.0.0.0/0
*	All traffic	All	All	::/0

**Network ACLs (1/1) [Info](#)**

[Actions](#) | [Create network ACL](#)

Find resources by attribute or tag

Network ACL ID : [acl-05fedf7c4dd3f36fb](#) [X](#) | [Clear filters](#)

Name	Network ACL ID	Associated with	Default	VPC ID
-	<a href="#">acl-05fedf7c4dd3f36fb</a>	2 Subnets	Yes	<a href="#">vpc-093f39</a>

**acl-05fedf7c4dd3f36fb**

[Details](#) | [Inbound rules](#) | [Outbound rules](#) | [Subnet associations](#) | [Tags](#)

**Inbound rules (4)**

[Edit inbound rules](#)

Filter inbound rules

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	<input checked="" type="checkbox"/> Allow
101	All traffic	All	All	::/0	<input checked="" type="checkbox"/> Allow
*	All traffic	All	All	0.0.0.0/0	<input checked="" type="checkbox"/> Deny
*	All traffic	All	All	::/0	<input checked="" type="checkbox"/> Deny

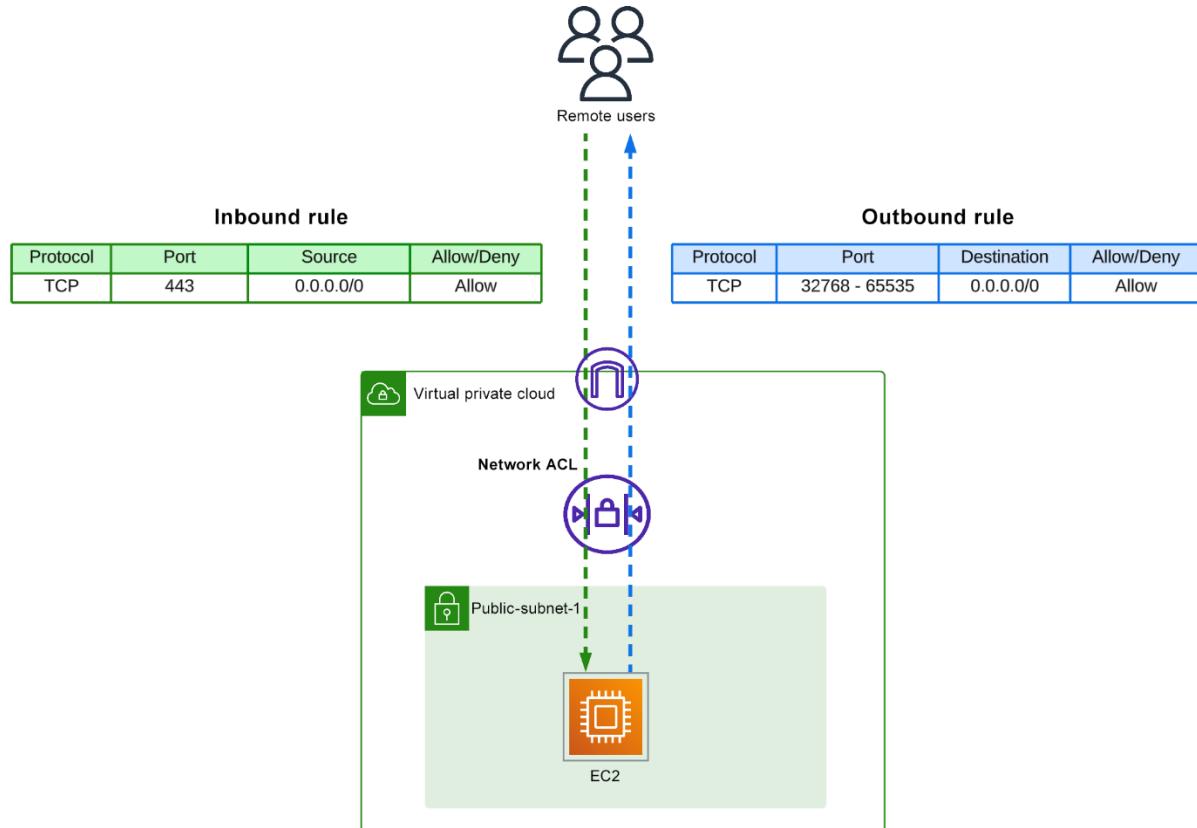
[Details](#) | [Inbound rules](#) | [Outbound rules](#) | [Subnet associations](#) | [Tags](#)

**Outbound rules (4)**

[Edit outbound rules](#)

Filter outbound rules

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	<input checked="" type="checkbox"/> Allow
101	All traffic	All	All	::/0	<input checked="" type="checkbox"/> Allow
*	All traffic	All	All	0.0.0.0/0	<input checked="" type="checkbox"/> Deny
*	All traffic	All	All	::/0	<input checked="" type="checkbox"/> Deny



Inbound rules (7)							Edit inbound rules			
<input type="text"/> Filter inbound rules							<	1	>	⚙️
Rule number	Type	Protocol	Port range	Source	Allow/Deny	⋮				
100	HTTPS (443)	TCP (6)	443	0.0.0.0/0	<input checked="" type="checkbox"/> Allow	⋮				
110	All traffic	All	All	0.0.0.0/0	<input checked="" type="checkbox"/> Allow	⋮				
120	SSH (22)	TCP (6)	22	10.0.0.0/8	<input checked="" type="checkbox"/> Allow	⋮				
130	SSH (22)	TCP (6)	22	0.0.0.0/0	<input checked="" type="checkbox"/> Deny	⋮				
200	All ICMP - IPv4	ICMP (1)	All	0.0.0.0/0	<input checked="" type="checkbox"/> Deny	⋮				
*	All traffic	All	All	0.0.0.0/0	<input checked="" type="checkbox"/> Deny	⋮				

Inbound rules (7)							Edit inbound rules			
<input type="text"/> Filter inbound rules							<	1	>	⚙️
Rule number	Type	Protocol	Port range	Source	Allow/Deny	⋮				
100	HTTPS (443)	TCP (6)	443	0.0.0.0/0	<input checked="" type="checkbox"/> Allow	⋮				
110	SSH (22)	TCP (6)	22	10.0.0.0/8	<input checked="" type="checkbox"/> Allow	⋮				
120	SSH (22)	TCP (6)	22	0.0.0.0/0	<input checked="" type="checkbox"/> Deny	⋮				
130	All ICMP - IPv4	ICMP (1)	All	0.0.0.0/0	<input checked="" type="checkbox"/> Deny	⋮				
200	All traffic	All	All	0.0.0.0/0	<input checked="" type="checkbox"/> Allow	⋮				
*	All traffic	All	All	0.0.0.0/0	<input checked="" type="checkbox"/> Deny	⋮				
*	All traffic	All	All	::/0	<input checked="" type="checkbox"/> Deny	⋮				

Rule number	Type	Protocol	Port range	Source	Allow/Deny
500	Custom ICMP - IPv4	ICMP (1)	Destination Unreachable	0.0.0.0/0	<input checked="" type="checkbox"/> Allow
501	Custom ICMP - IPv6	IPv6-ICMP (58)	Destination Unreachable	::/0	<input checked="" type="checkbox"/> Allow

Rule number	Type	Protocol	Port range	Source	Allow/Deny
600	Custom ICMP - IPv4	ICMP (1)	Time Exceeded	0.0.0.0/0	<input checked="" type="checkbox"/> Allow
601	Custom ICMP - IPv6	IPv6-ICMP (58)	Time Exceeded	::/0	<input checked="" type="checkbox"/> Allow

VPC dashboard X

EC2 Global View [ ]

Filter by VPC ▼

Virtual private cloud

Security ▼

**Network ACLs** [ ] Create network ACL

Security groups

No network ACLs found in this Region

Select a network ACL

[VPC](#) > [Network ACLs](#) > Create network ACL

## Create network ACL Info

A network ACL is an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet.

### Network ACL settings

#### Name - *optional*

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

my-acl-01

#### VPC

VPC to use for this network ACL.

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 tag

You can add 50 more tags

Cancel

**Create network ACL**

**Network ACLs (1/1)** Info

Find resources by attribute or tag

Network ACL ID : acl-0a78bc1f48820cb9 X

Clear filters

Name ▼

Network ACL ID ▼

Associated with ▼

example-nacl

acl-0a78bc1f48820cb9 -

View details

Edit inbound rules

Edit outbound rules

Edit subnet associations

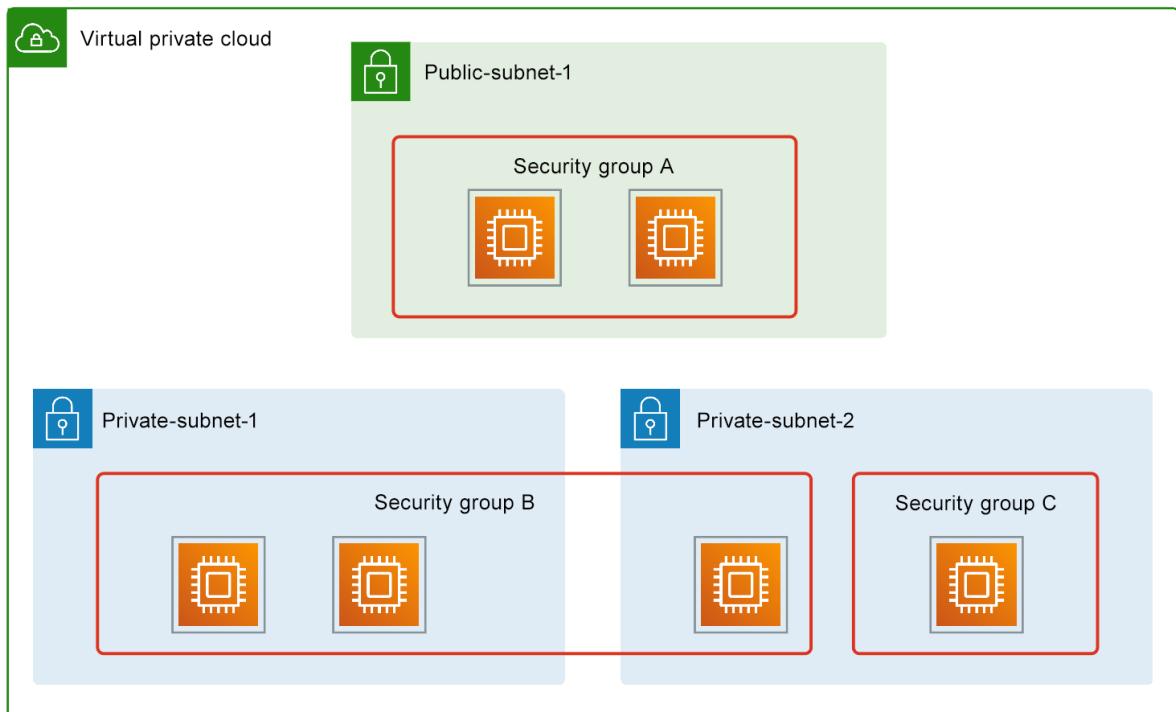
Manage tags

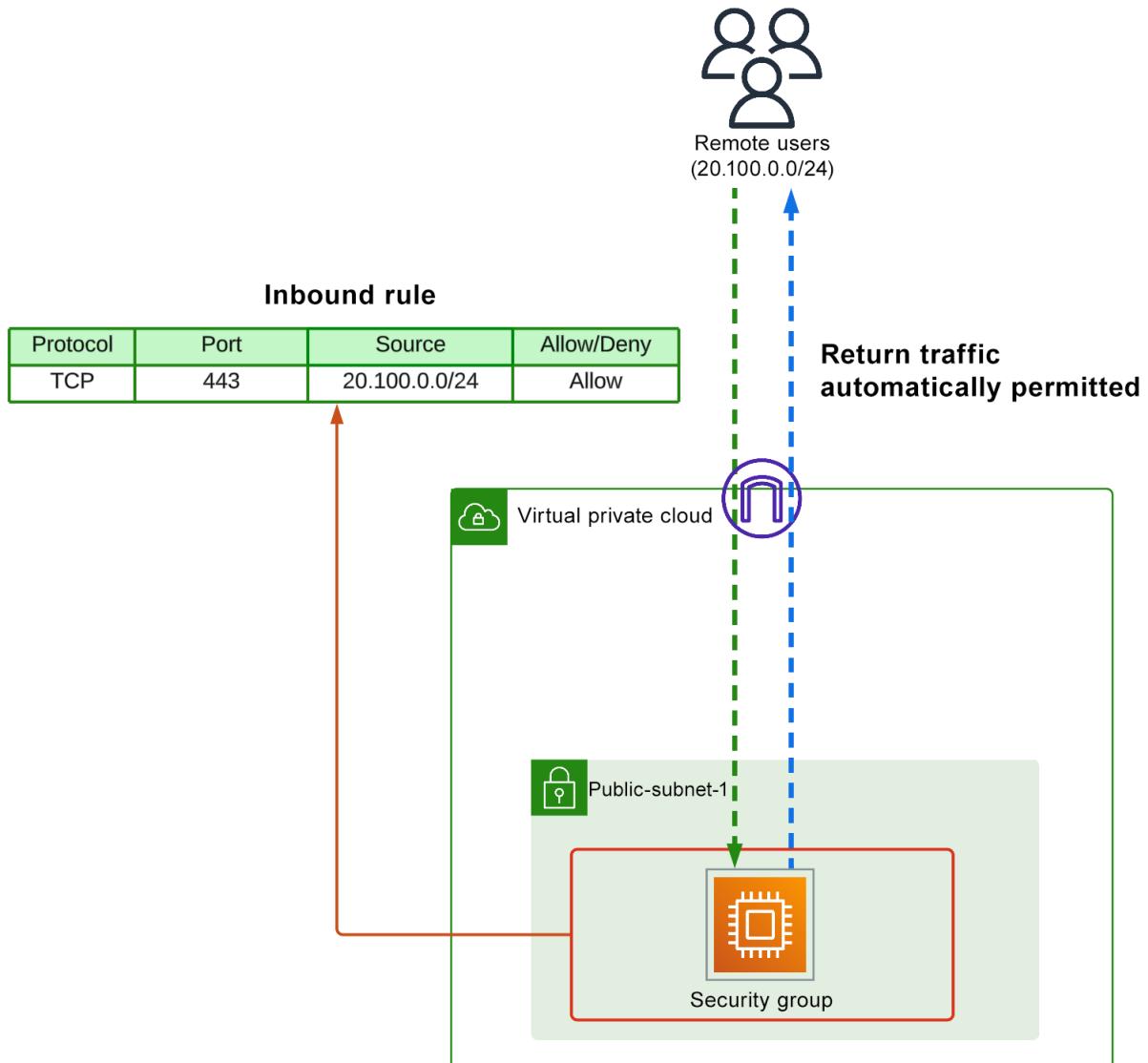
Delete network ACLs

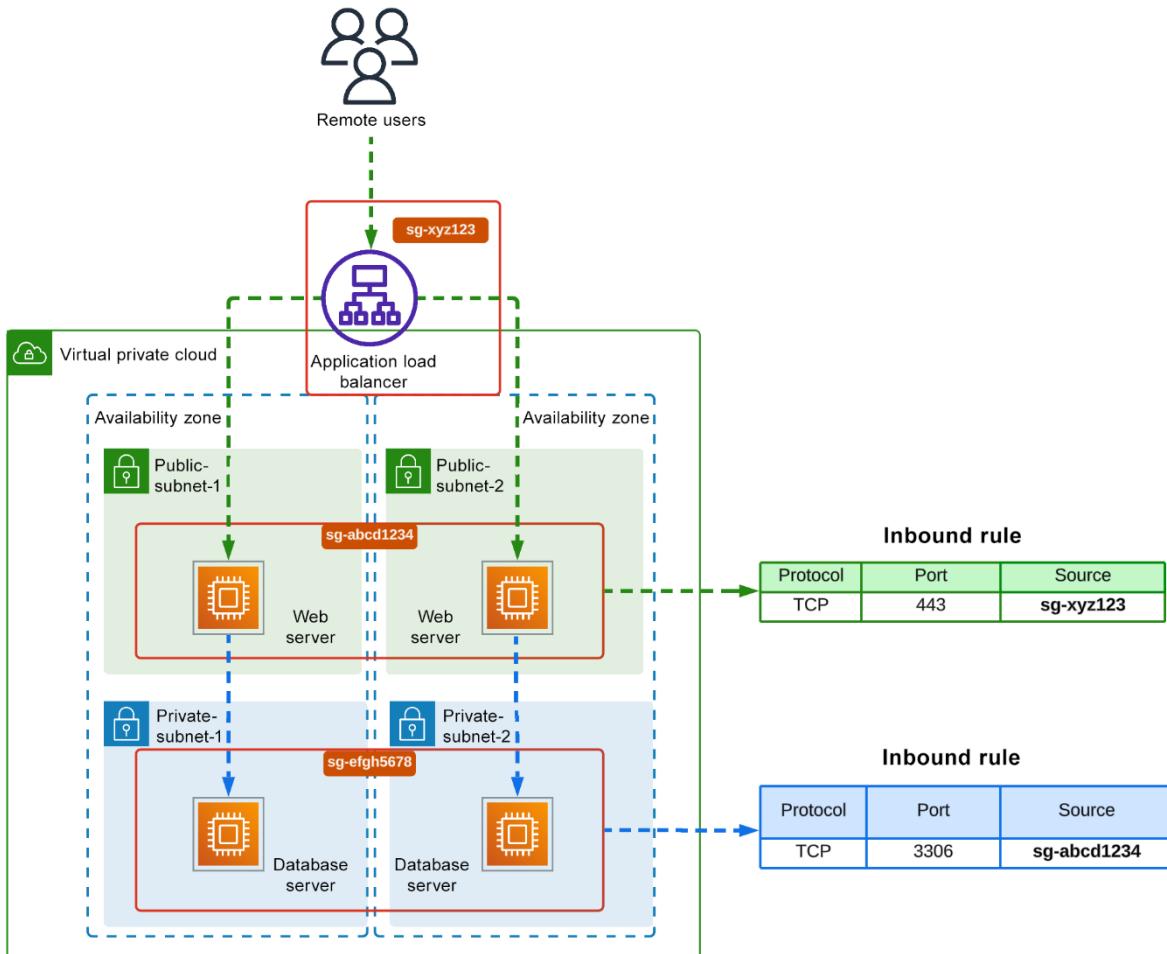
1 > [ ]

VPC ID ▼

vpc-025







The screenshot shows the AWS VPC dashboard with the following interface elements:

- VPC dashboard** sidebar with **EC2 Global View**, **Virtual private cloud**, and **Security groups** (highlighted with a red box).
- Security Groups (1)** table:
 

Name	Security group ID	Security group name	VPC ID
-	sg-	default	vpc-
- Create security group** button highlighted with a red arrow.

## 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

Name cannot be edited after creation.

Description Info

VPC Info

### Inbound rules Info

Type Info

Protocol

Port range Info

Source Info

Description - optional Info

Info

### Outbound rules Info

Type Info

Protocol

Port range Info

Destination Info

Description - optional Info

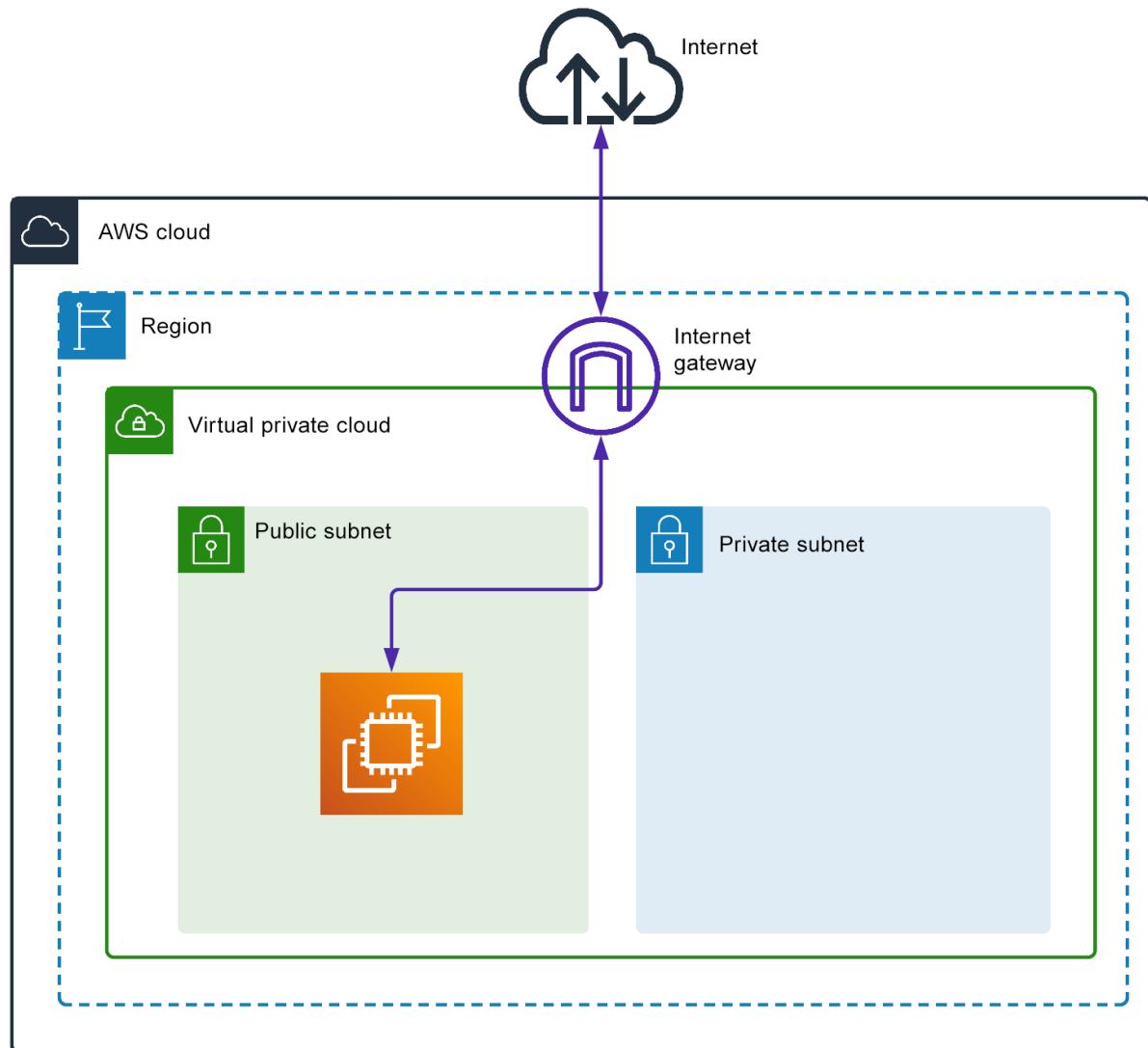
Info

### 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.

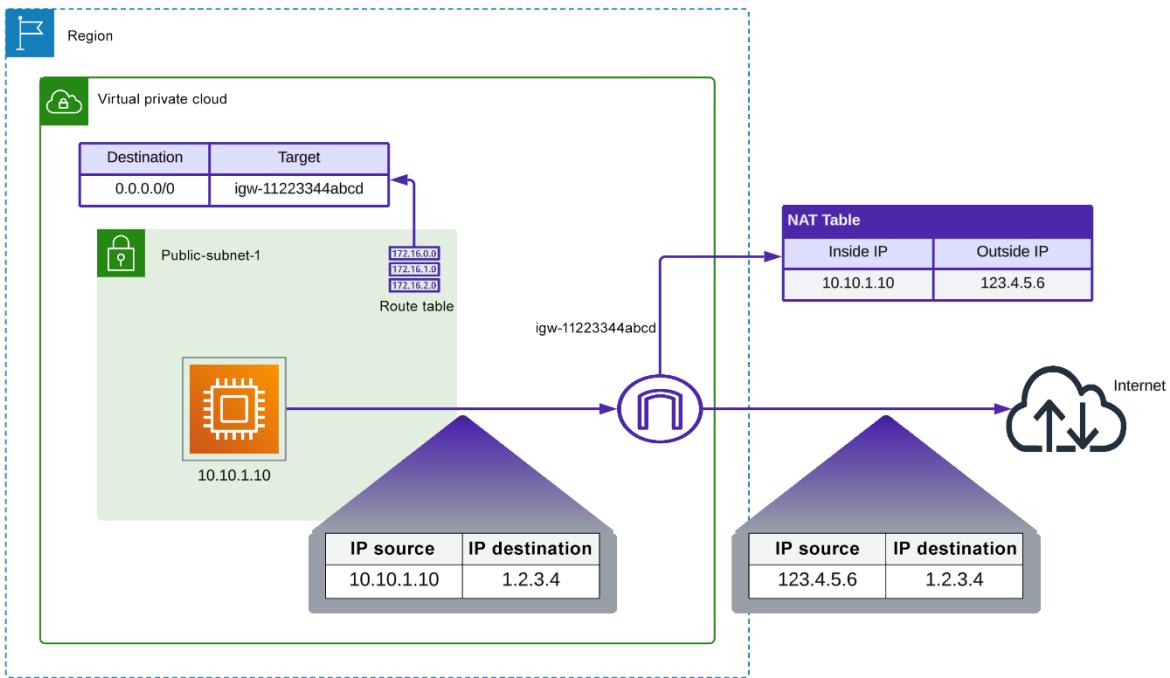
You can add up to 50 more tags



VPC > Subnets > subnet > Edit subnet settings

## Edit subnet settings Info

Subnet	
Subnet ID subnet-	Name public-subnet-01
<b>Auto-assign IP settings <small>Info</small></b> Enable AWS to automatically assign a public IPv4 or IPv6 address to a new primary network interface for an instance in this subnet.	
<input type="checkbox"/> Enable auto-assign public IPv4 address <small>Info</small> ←	
<input checked="" type="checkbox"/> Enable auto-assign customer-owned IPv4 address <small>Info</small> <small>Option disabled because no customer owned pools found.</small>	



**VPC dashboard**

**Internet gateways**

No internet gateways found in this Region

Select an internet gateway above

**igw-05356846932392927 / example-internet-gateway**

**Details**

Internet gateway ID igw-05356846932392927	State Detached	VPC ID -	Owner 63713
--	-------------------	-------------	----------------

**Actions**

- Attach to VPC (highlighted)
- Detach from VPC
- Manage tags
- Delete

**Tags**

Key	Value
Name	example-internet-gateway

**Manage tags**

## 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

Find resources by attribute or tag



Actions ▾

Create egress only internet gateway



Name

Egress only internet gateway ID

Attached VPC ID

No egress only internet gateway found

≡



## 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.

#### VPC

Attach the egress only internet gateway to this 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.

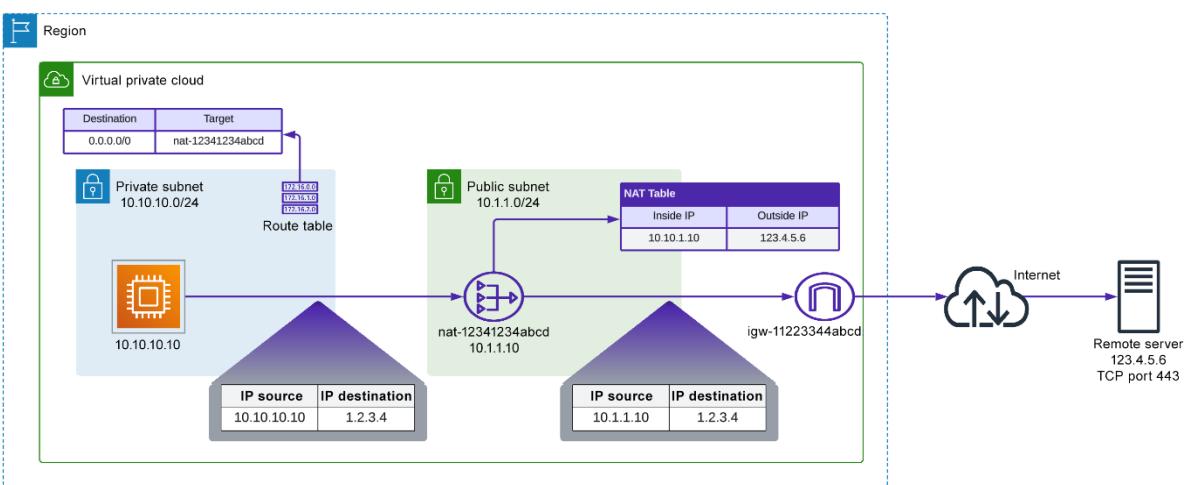
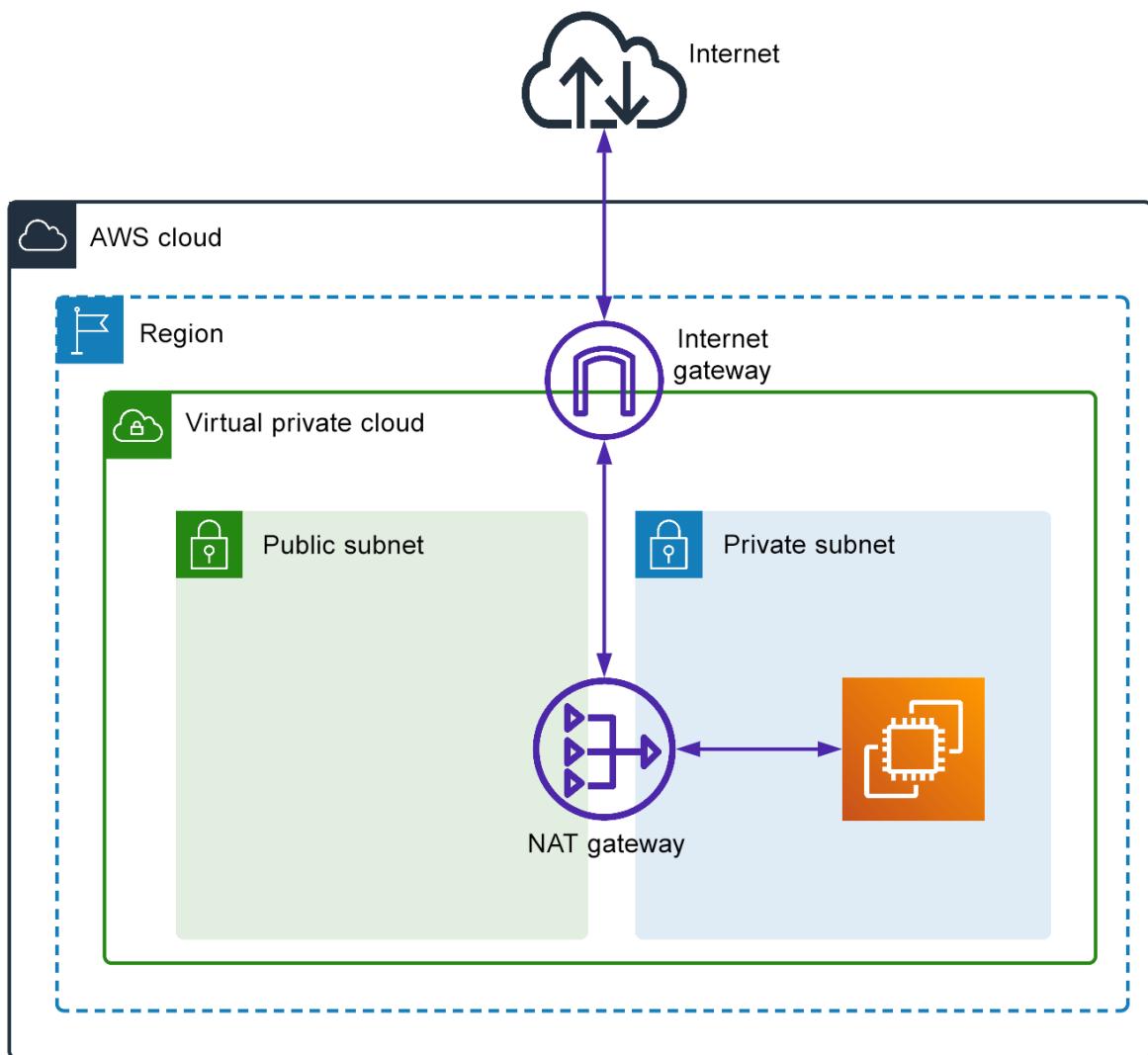
#### Key

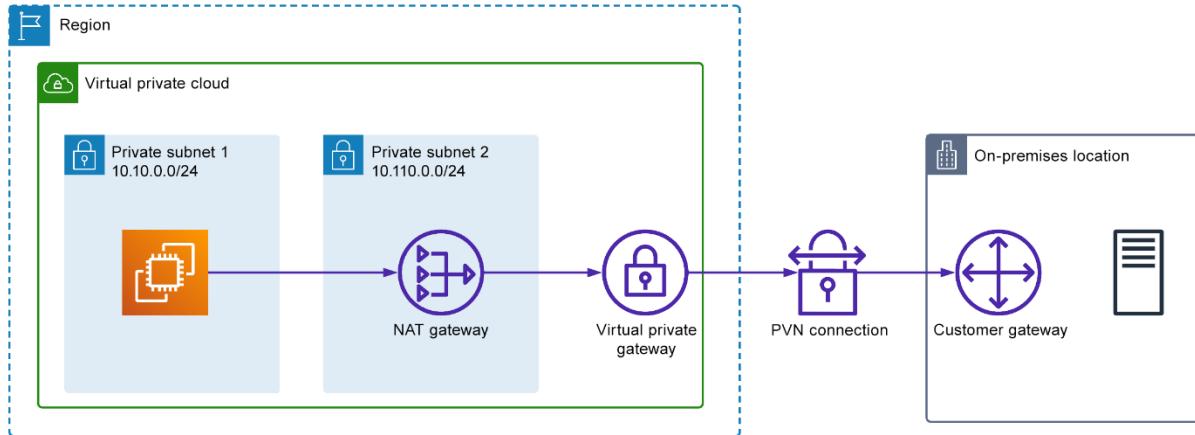
#### Value - *optional*

RemoveAdd new tag

You can add 49 more tags.

CancelCreate egress only internet gateway





**VPC dashboard**

**NAT gateways**

No NAT gateways found

Name	NAT gateway ID	Connectivity...	State	State message	Pr...
------	----------------	-----------------	-------	---------------	-------

**Create NAT gateway**

**NAT gateways**

## 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.

The name can be up to 256 characters long.

#### Subnet

Select a subnet in which to create the NAT gateway.



#### 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 a subnet to display the allocation IDs.

#### ▼ Additional settings Info

#### Primary private IPv4 address - *optional*

### 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.

You can add 50 more tags.