



Creating a Networking Environment

AWS Academy Cloud
Architecting



Introduction

Creating a Networking Environment

Module objectives

This module prepares you to do the following:

- Explain the role of a virtual private cloud (VPC) in Amazon Web Services (AWS) Cloud networking.
- Identify the components in a VPC that can connect an AWS networking environment to the internet.
- Isolate and secure resources within your AWS networking environment.
- Create and monitor a VPC with subnets, an internet gateway, route tables, and a security group.
- Use the AWS Well-Architected Framework principles when creating and planning a network environment.

Module overview

Presentation sections

- Introducing Amazon VPC
- Securing network resources
- Connecting to managed AWS services
- Monitoring your network
- Applying AWS Well-Architected Framework principles to a network

Demo

- Creating an Amazon VPC in the AWS Management Console

Activity

- Choose the Right Type of Subnet

Knowledge checks

- 10-question knowledge check
- Sample exam question

Hands-on labs in this module

Guided lab

- Creating a Virtual Private Cloud

Challenge (Café) lab



- Creating a VPC Networking Environment for the Café

As a cloud architect designing a network environment:



- I need to design a network that's resilient to failure and can handle the anticipated growth in traffic so that it's available when needed.
- I need to secure my network effectively so that it provides access to users and applications that should have it while preventing unwanted traffic.
- I need to understand how network design decisions impact performance and cost so that I can optimize the value of the network to the business.

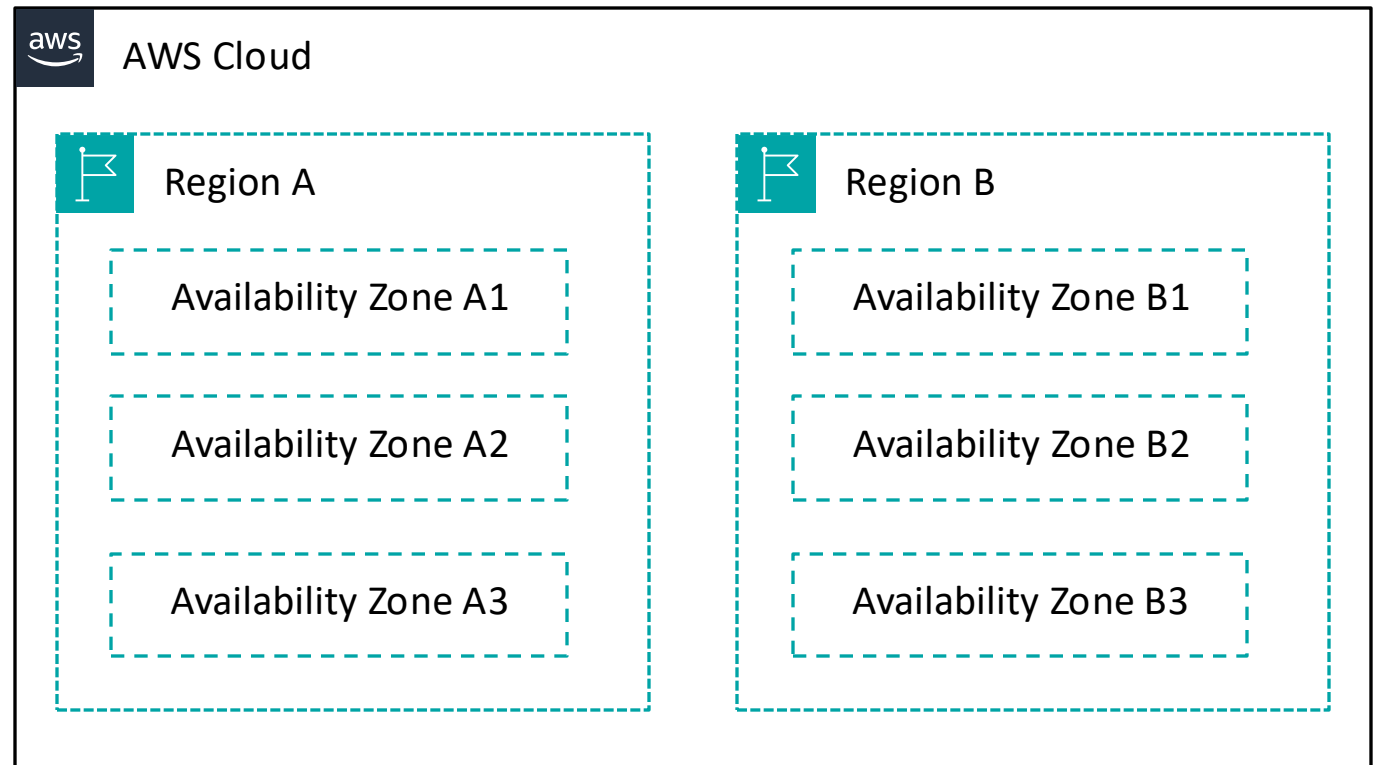


Introducing Amazon VPC

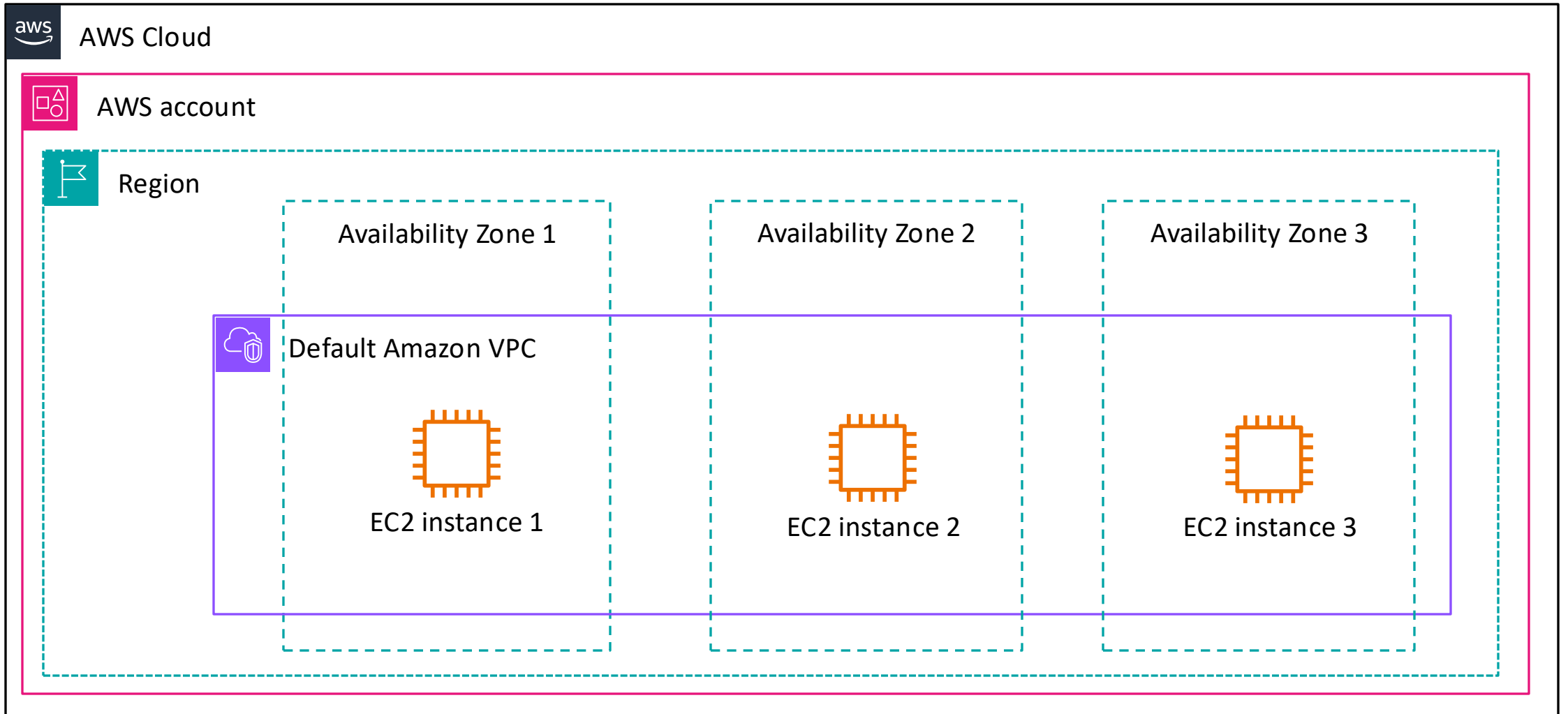
Creating a Networking Environment

AWS physical infrastructure

- AWS Cloud infrastructure resides in data centers which contain thousands of servers built into racks. Every rack has network routers and switches to route traffic.
- Data centers are grouped together in Availability Zones (AZs).
- AZs are connected with single digit millisecond latency network.
- AZs are grouped together in an AWS Region.
- Latency between AWS Regions is 10s of milliseconds.



AWS account resource isolation



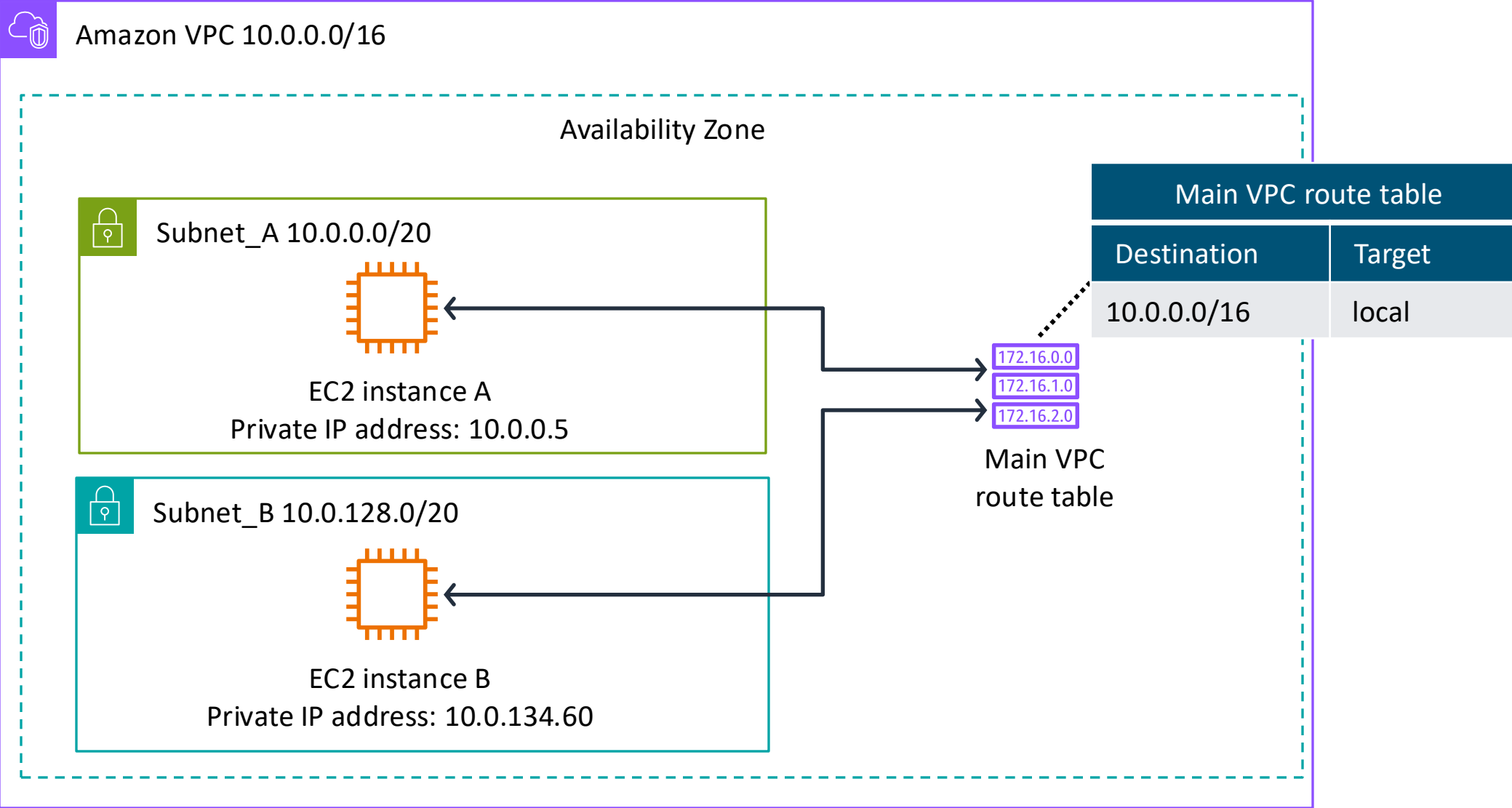
Amazon Virtual Private Cloud



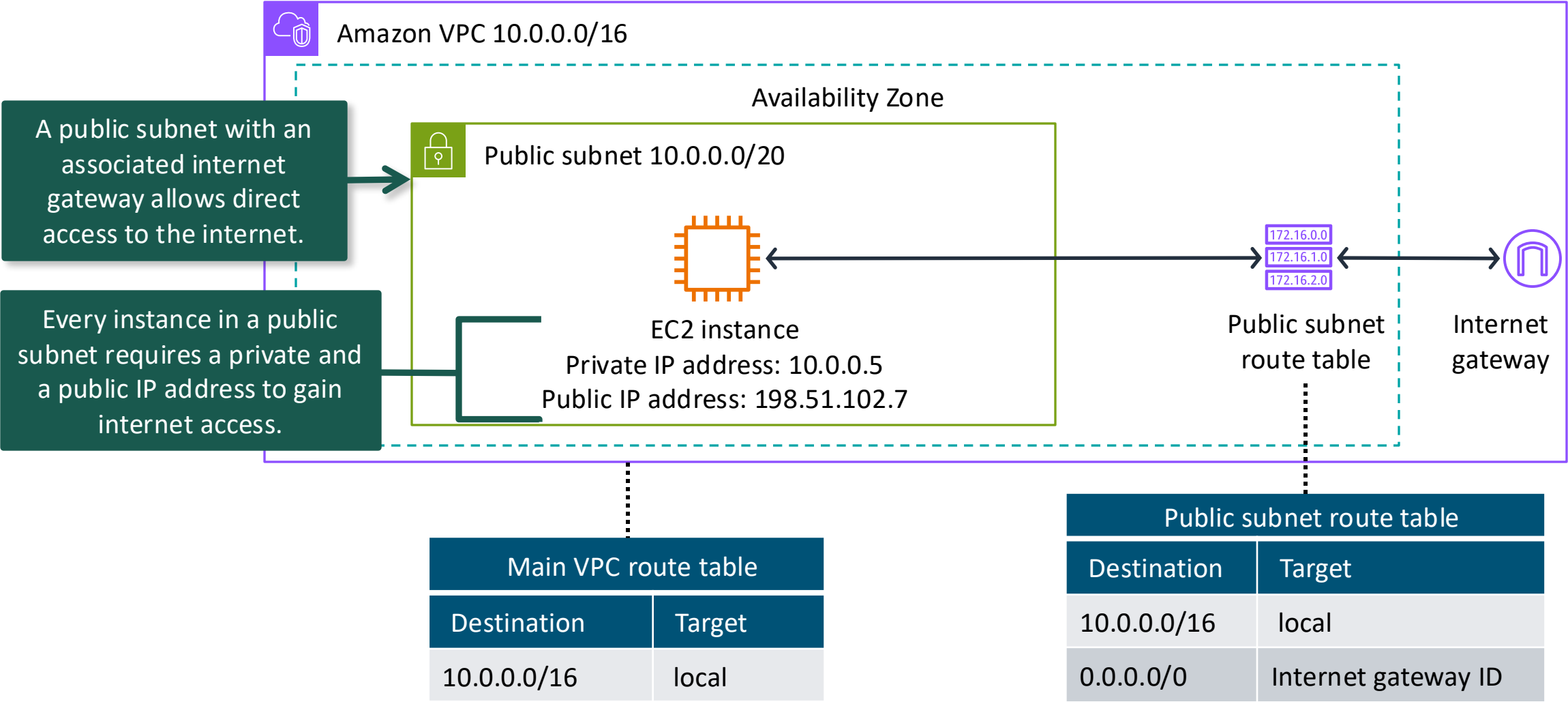
Amazon VPC

- Programmatically defined, logically isolated virtual network similar to a traditional data center network
- Belongs to one Region
- Customizable to control traffic flow to and from the VPC
- Sized by a range of private IP addresses called a CIDR block

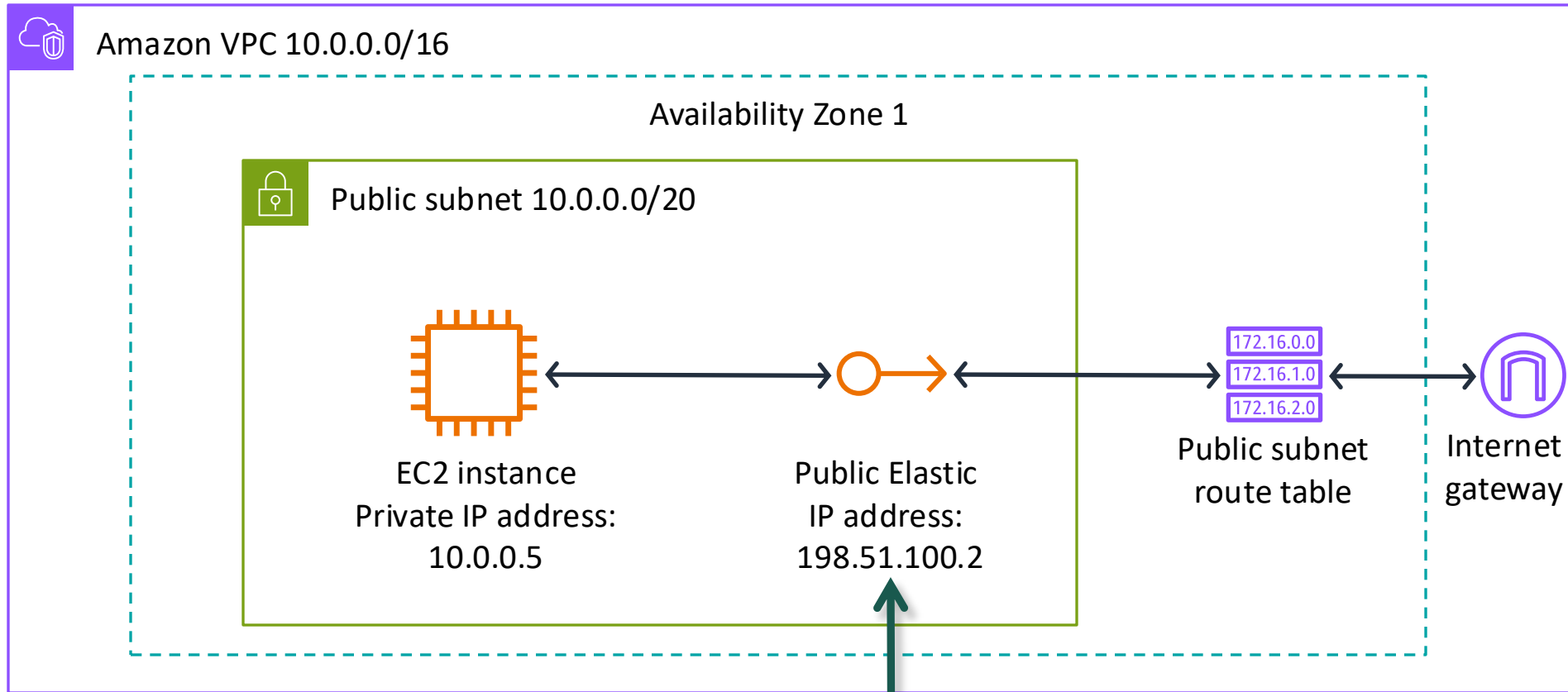
Main route table



Public subnets

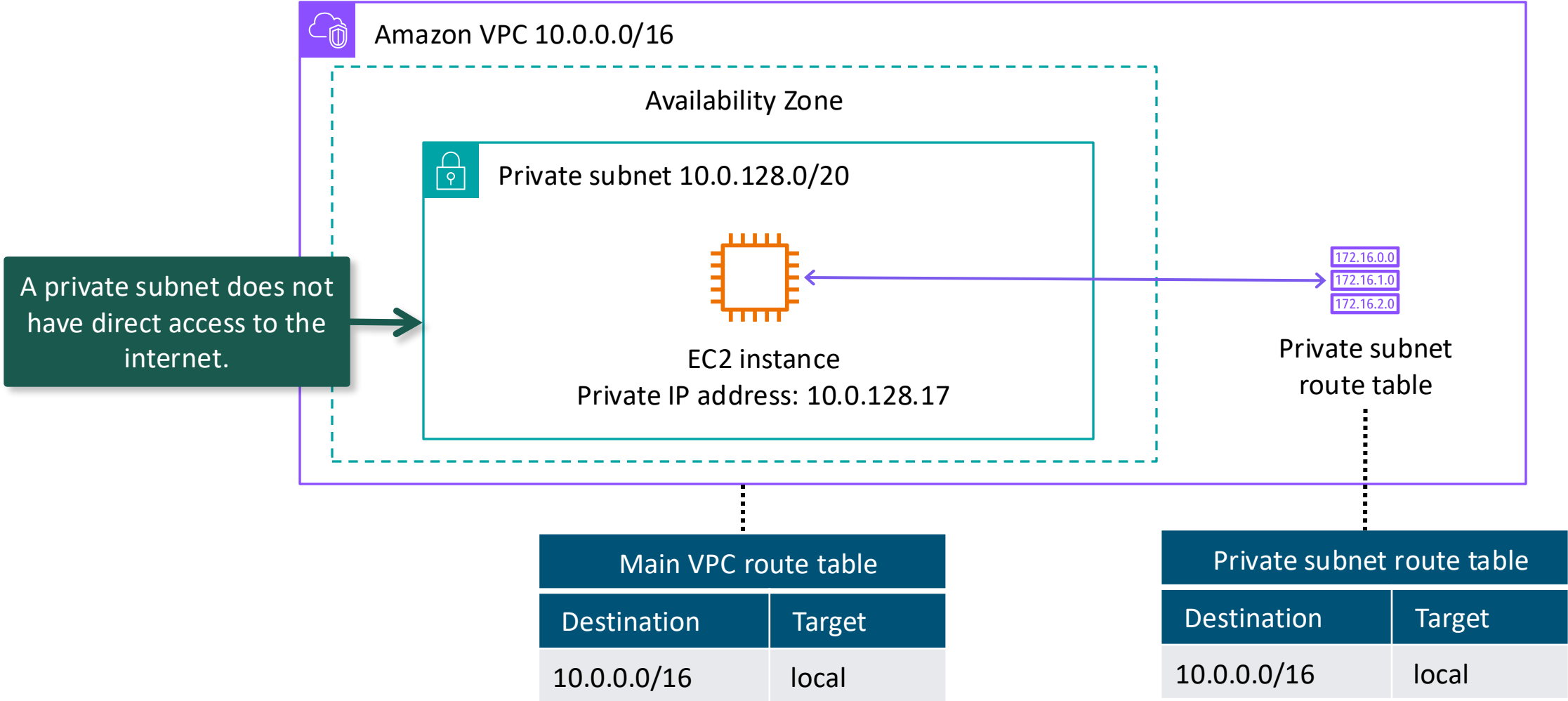


Elastic IP addresses

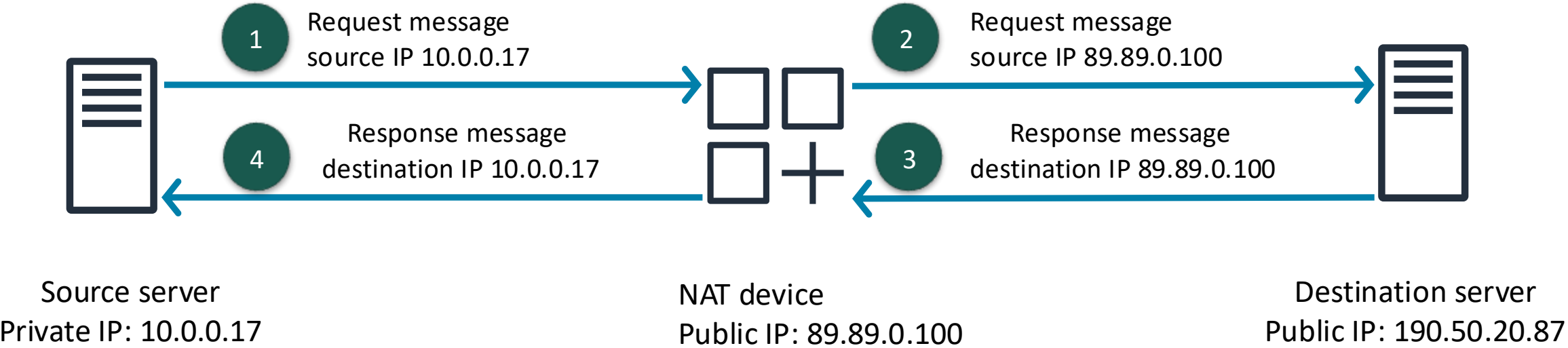


An Elastic IP address is a public, static address associated with an instance. An Elastic IP address can be transferred to a new instance.

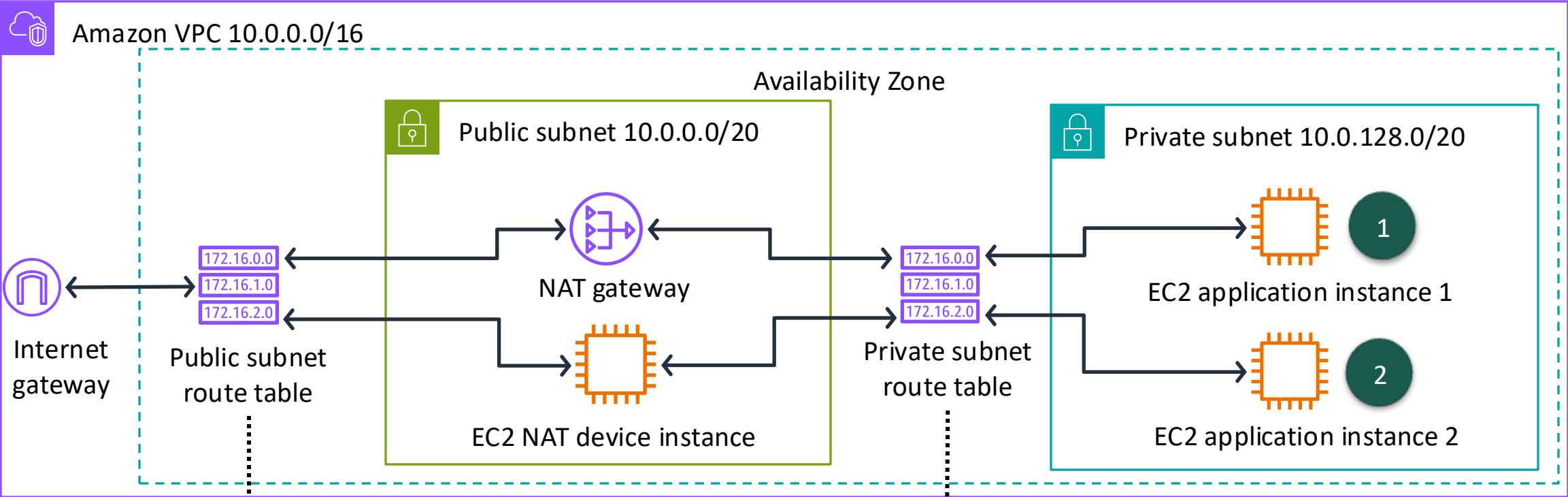
Private subnets



NAT IP mapping



Connecting private subnets to the internet



Public subnet route table	
Destination	Target
10.0.0.0/16	local
0.0.0.0/0	Internet gateway ID

Private subnet route table	
Destination	Target
10.0.0.0/16	local
0.0.0.0/0	NAT gateway ID

Activity: Choose the Right Type of Subnet

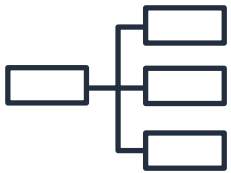


- Decide whether instances should be placed into a public or private subnet.

Choose public or private subnet for each use case



Database instances



Batch-processing instances

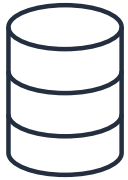


Web application instances



NAT gateway or instance

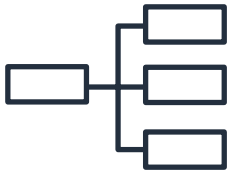
Recommended subnet selections for each use case



Database instances



Private subnet



Batch-processing instances



Private subnet



Web application instances



Public or private subnet



NAT gateway or instance



Public subnet

Key takeaways: Introducing Amazon VPC



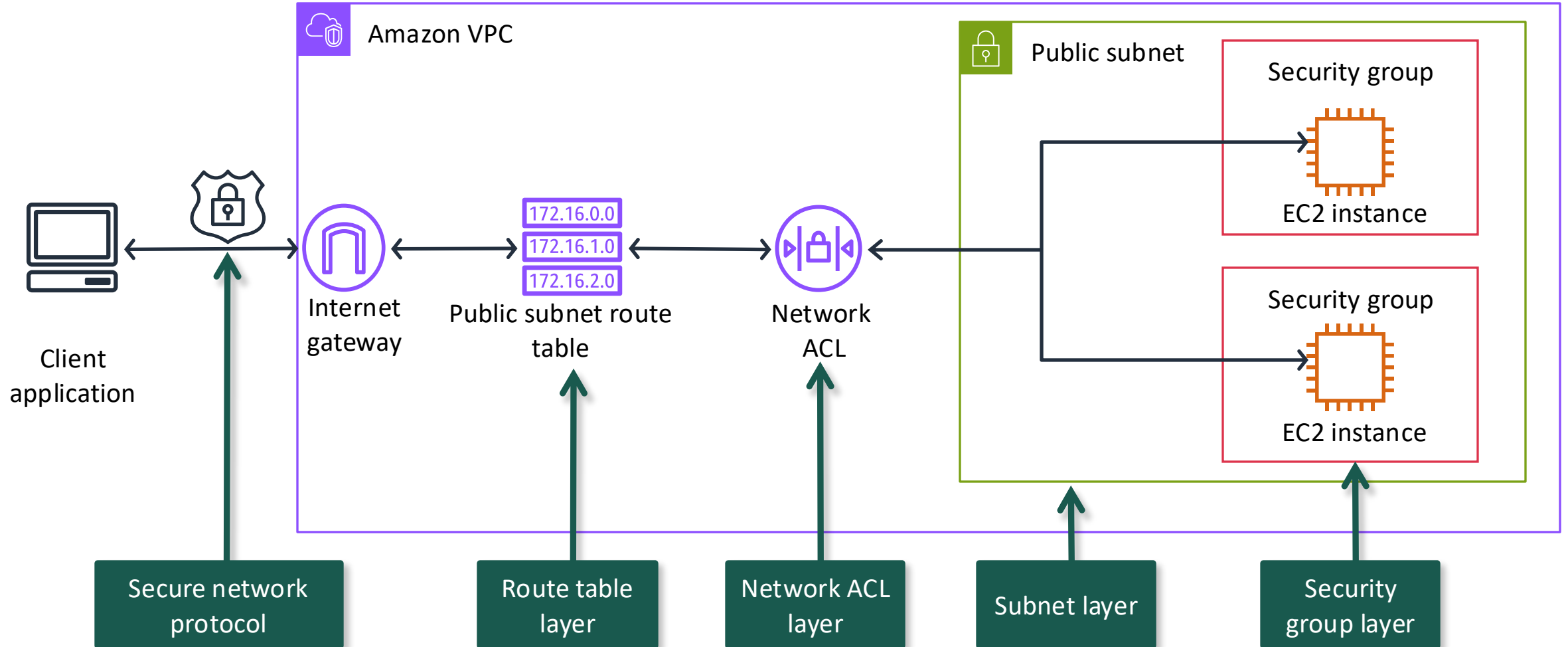
- An Amazon VPC is a programmatically defined, logically isolated virtual network.
- A public subnet with an internet gateway allows direct access to the internet.
- A private subnet does not have direct access to the internet.
- A NAT gateway allows resources in a private subnet to connect to the internet.
- An Elastic IP address can be transferred to a new instance.



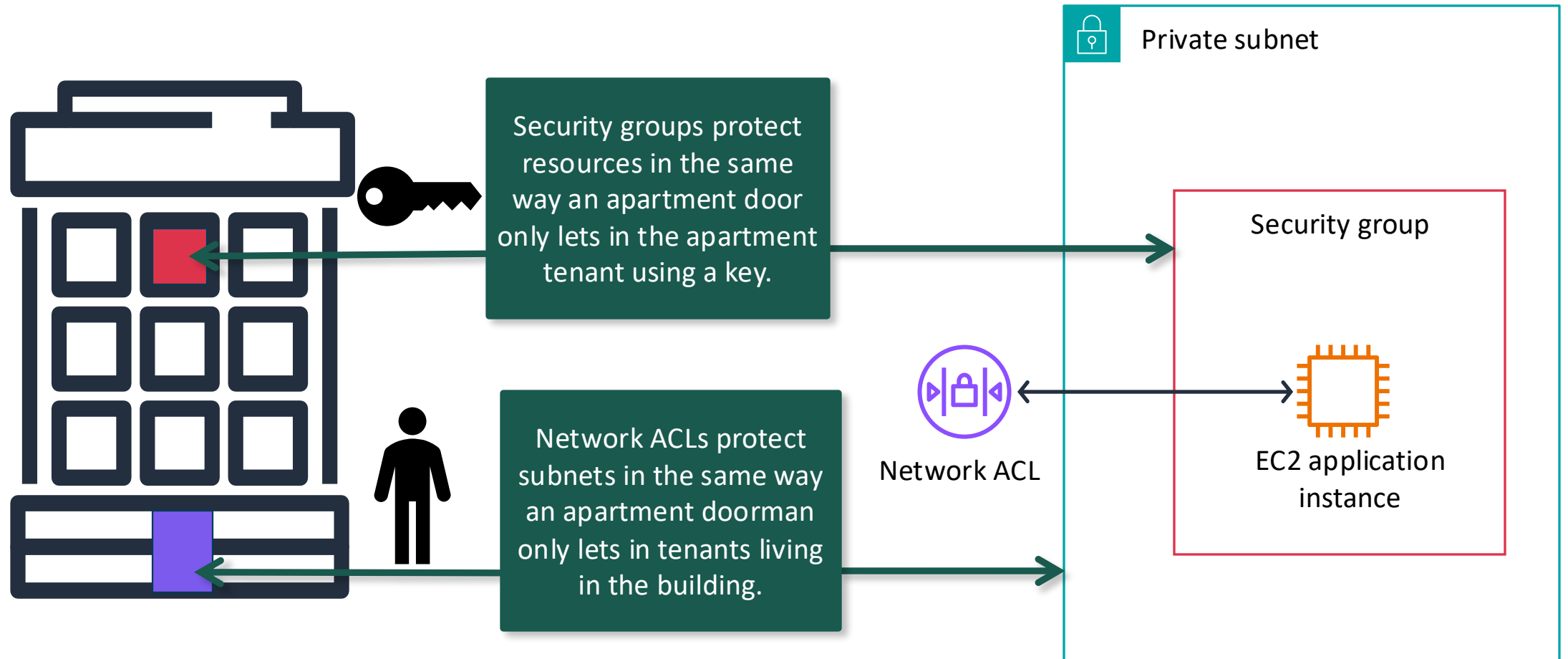
Securing network resources

Creating a Networking Environment

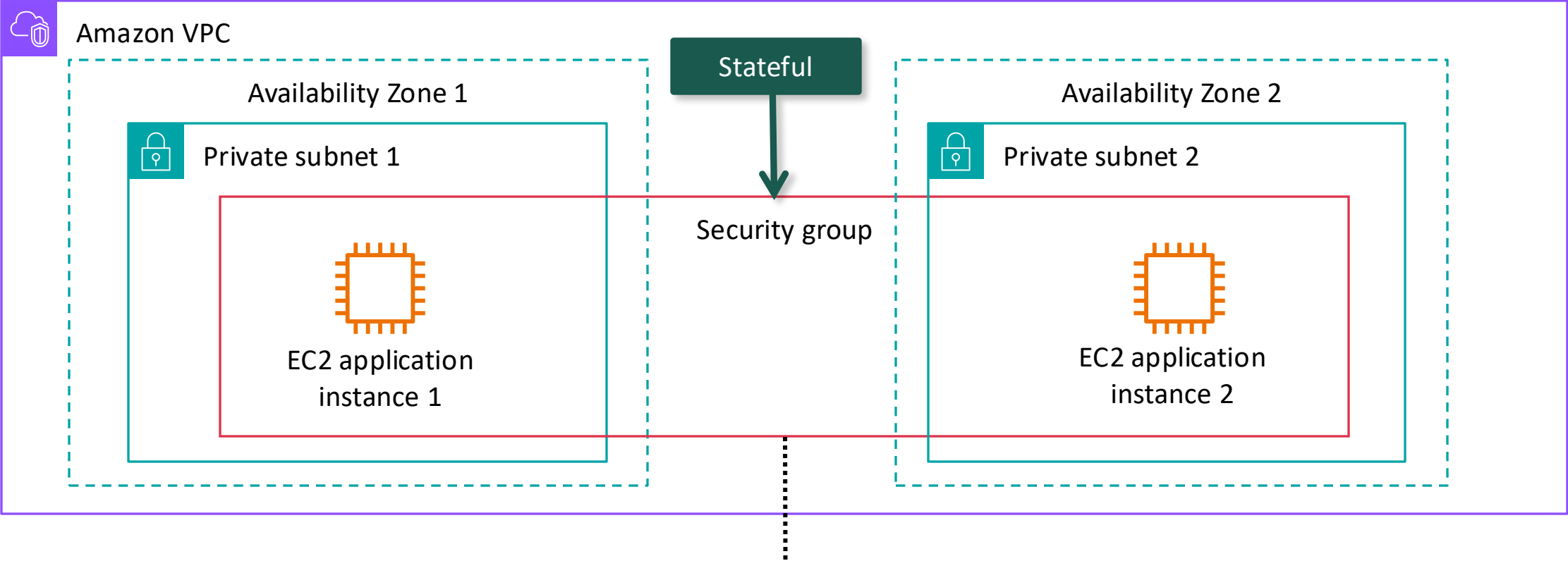
Security layers of defense



Security groups and network ACL scope

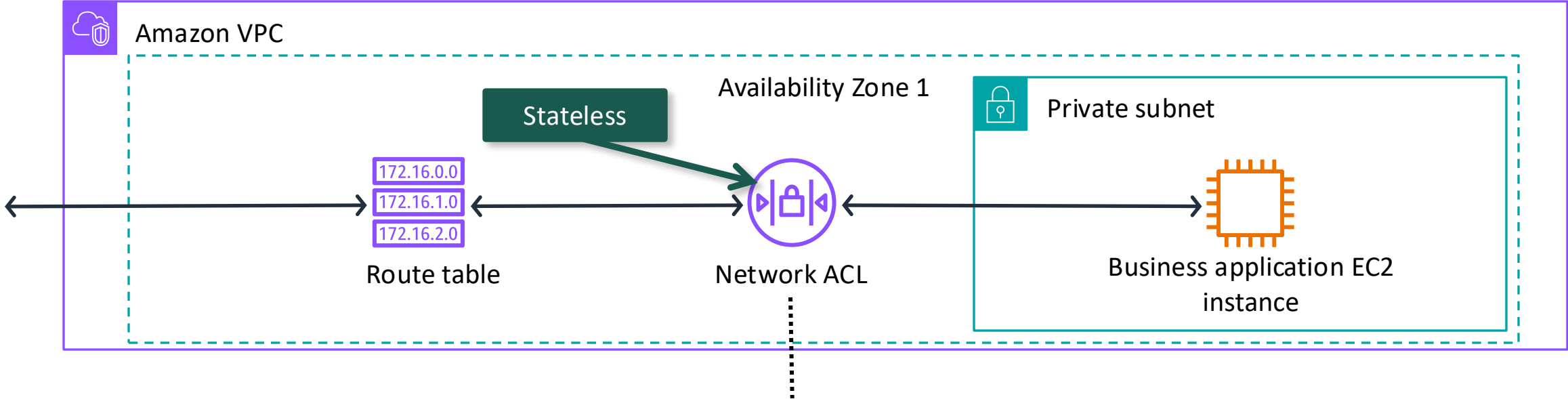


Security groups



Inbound security group rule			
Source	Traffic type	Protocol	Port range
Load balancer security group ID	HTTPS	TCP	443

Network ACL




Rule number	Source	Traffic type	Protocol	Port range	Deny or allow
Inbound ACL rules					
100	188.7.55.9/32	HTTPS	TCP	443	Allow
*	0.0.0.0/0	All traffic	All	All	Deny
Outbound ACL rules					
100	0.0.0.0/0	HTTPS	TCP	443	Allow
*	0.0.0.0/0	All traffic	All	All	Deny


Comparing security groups and network ACLs

Security groups	Network ACLs
Operate at resource level.	Operate at subnet level.
Specify allow traffic rules only.	Specify deny and allow traffic rules.
Rules are stateful.	Rules are stateless.
All rules are evaluated.	Rules are evaluated in number order and evaluation stops if a match is found.
In a new security group, no inbound traffic is allowed by default.	In a new network ACL, all inbound traffic is allowed by default.
In a new security group, all outbound traffic is allowed by default.	In a new network ACL, all outbound traffic is allowed by default.

Response traffic is automatically allowed back through the security group.



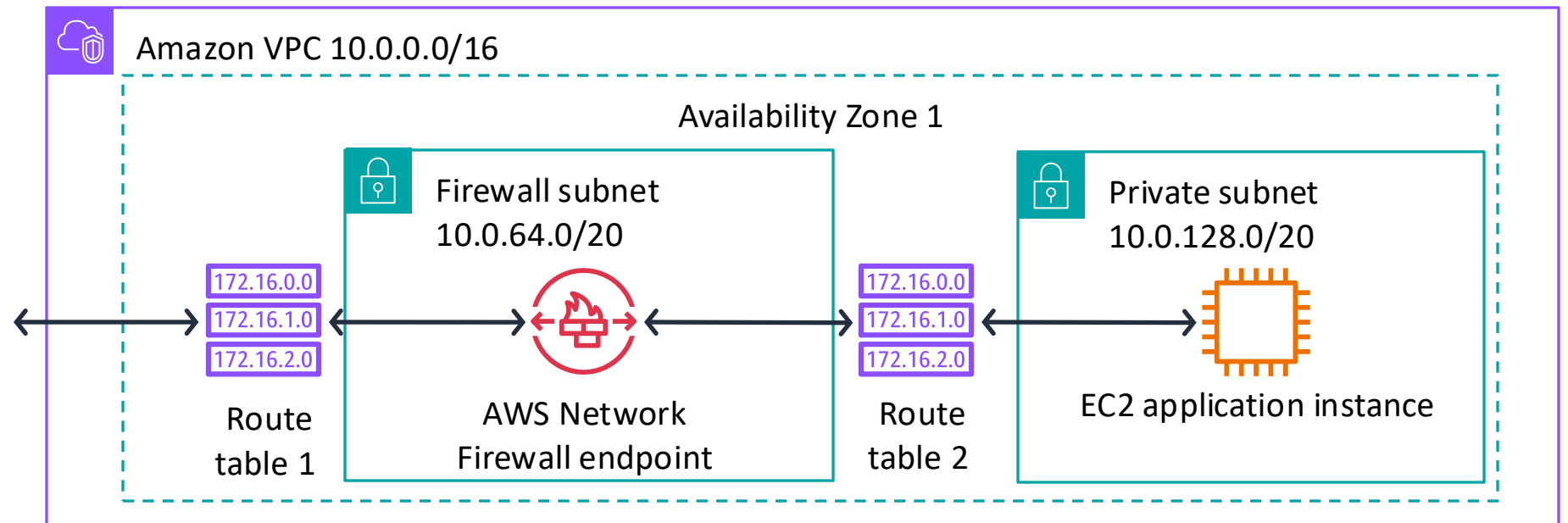
Response traffic is always evaluated against inbound or outbound rule set.



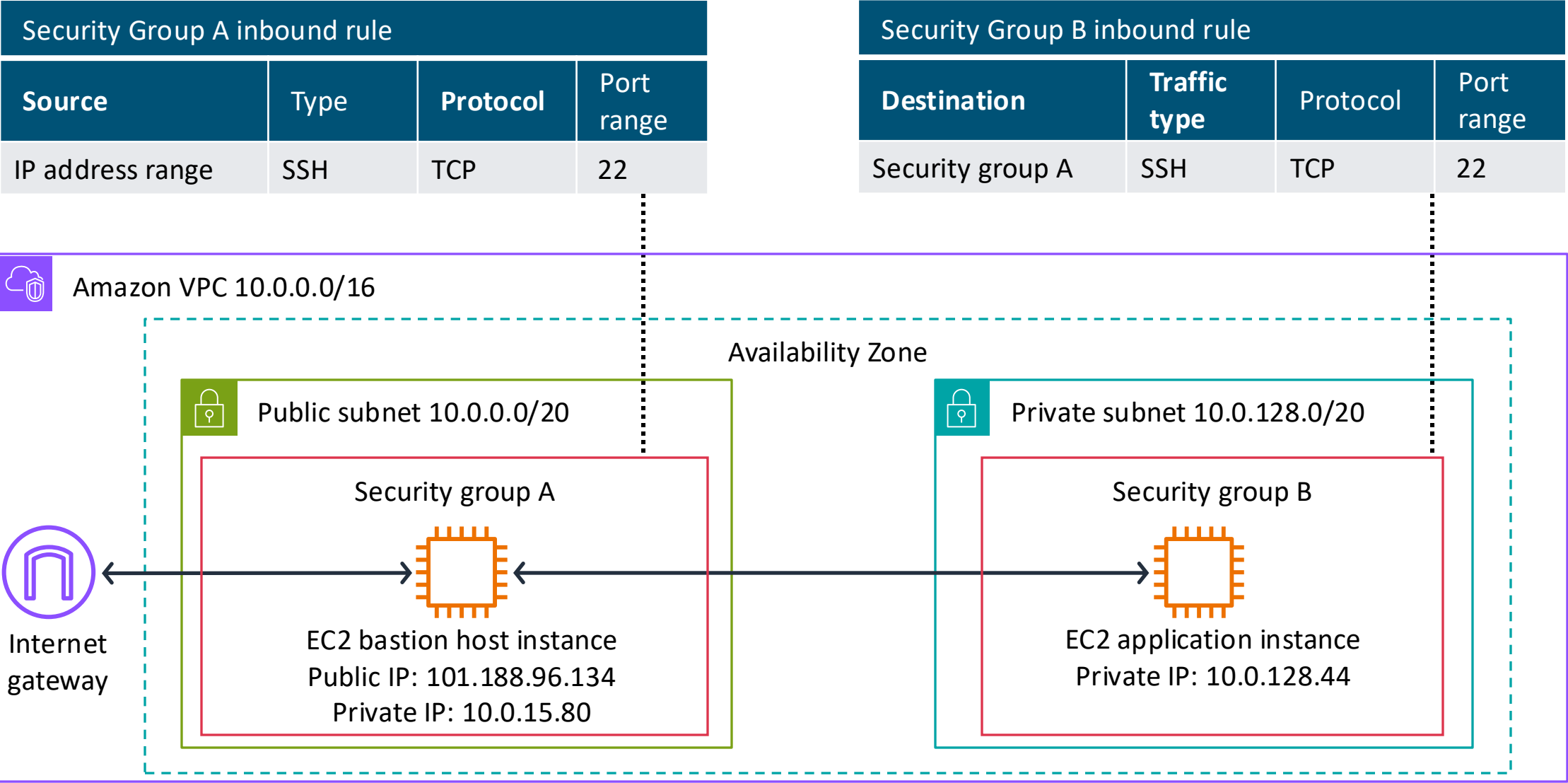
AWS Network Firewall



- Network firewall and intrusion detection and prevention service for an Amazon VPC.
- Adds an additional layer of security.
- Routes external VPC traffic through AWS Network Firewall to protect subnet resources.



Administrrating resources with bastion hosts

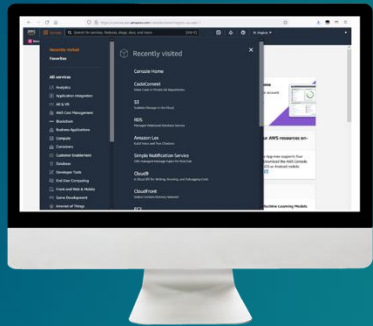


Key takeaways: Securing network resources



- Secure AWS infrastructure with multiple layers of defense.
- A security group in a VPC specifies which traffic is allowed to or from AWS resources. It is stateful.
- A network ACL allows or denies specific inbound or outbound traffic at the subnet level. It is stateless.
- Route external VPC traffic through AWS Network Firewall to add an additional layer of traffic security.
- Use a bastion host to administrate private subnet resources from an on-premises environment.

Demo: Creating an Amazon VPC in the AWS Management Console



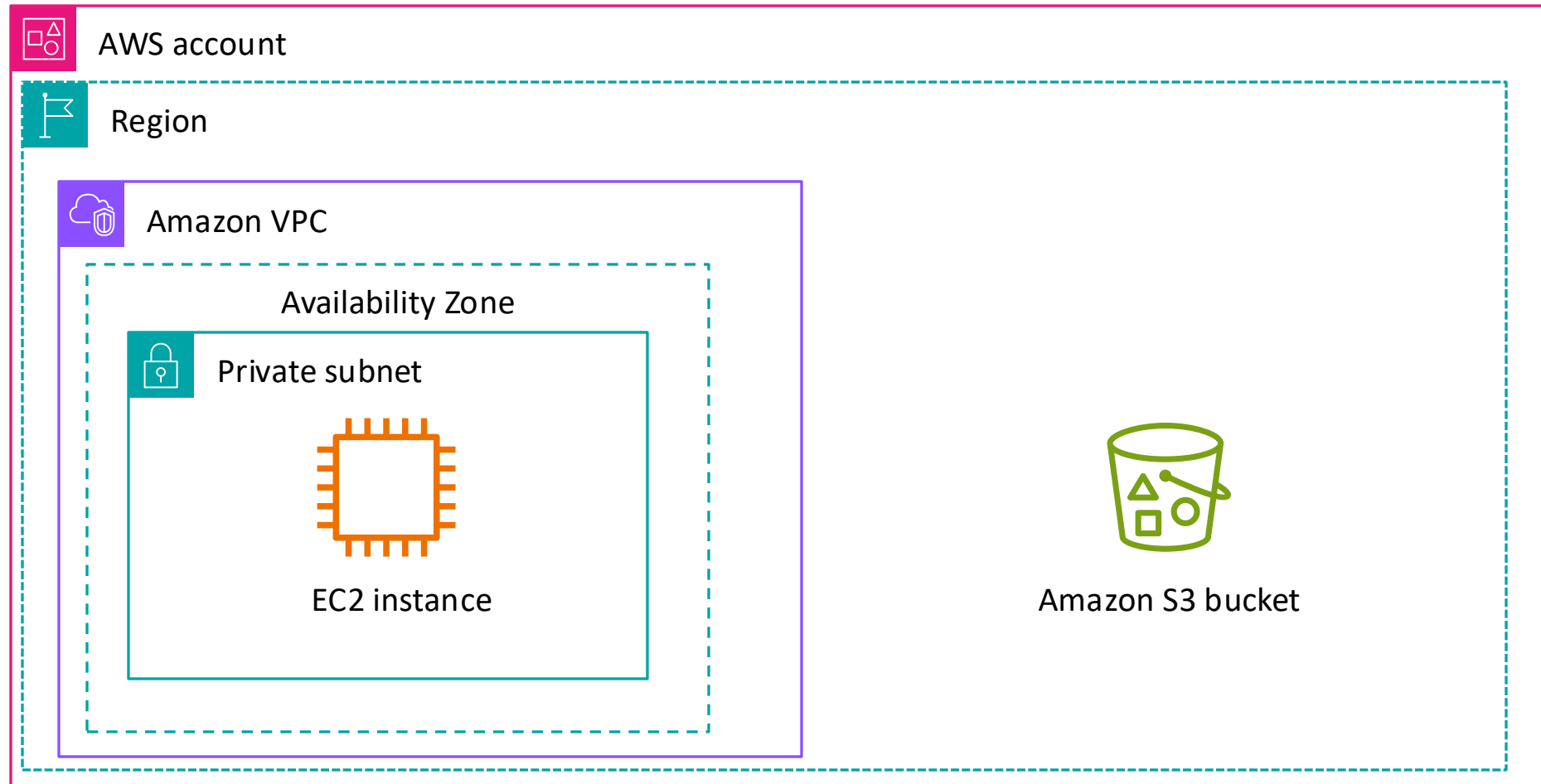
- This demo uses Amazon VPC features, security groups, and an Elastic IP address.
- In this demonstration, you will see how to create a public and private subnet in the VPC each with a subnet route table.
- You will see how to create an internet gateway and attach it to the VPC and configure internet routes.
- Create a NAT gateway and assign an Elastic IP address. Configure NAT gateway routes.
- Create a web server security group.
- Create a database server security group.



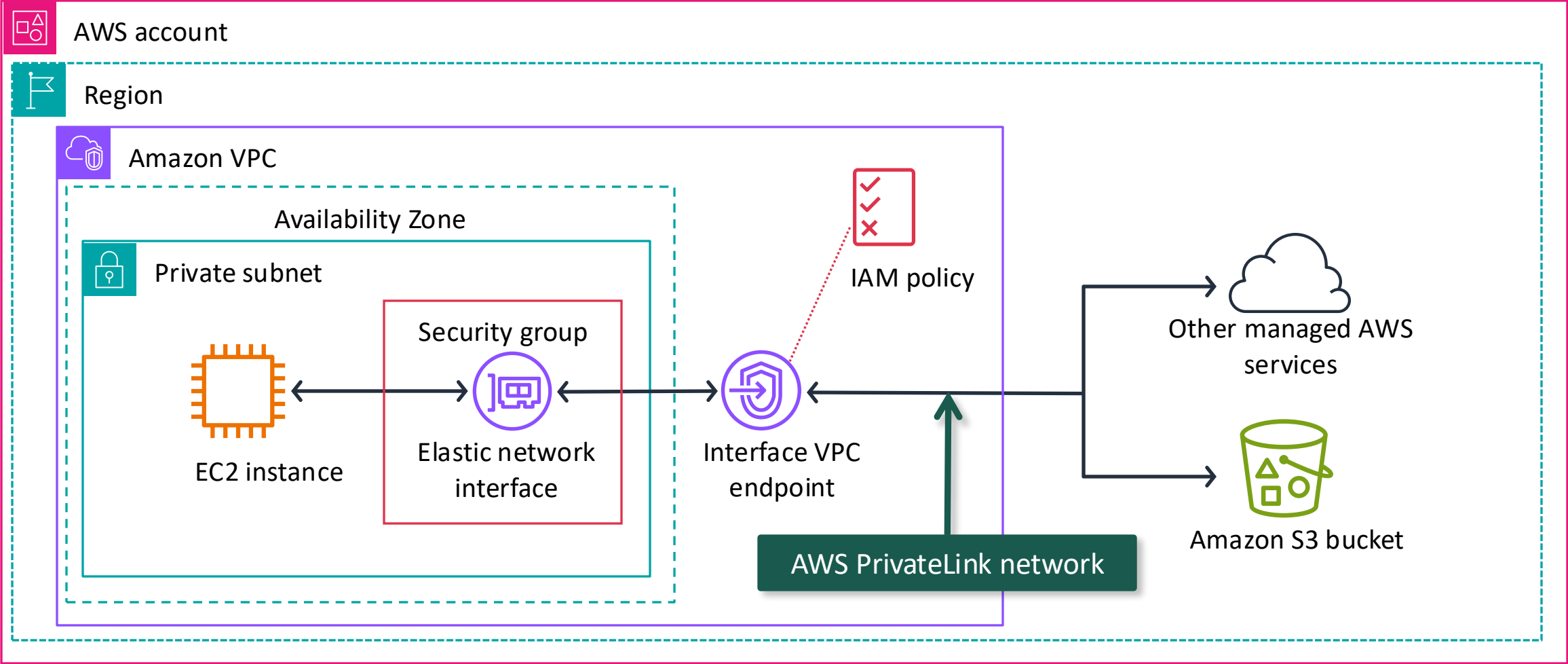
Connecting to managed AWS services

Creating a Networking Environment

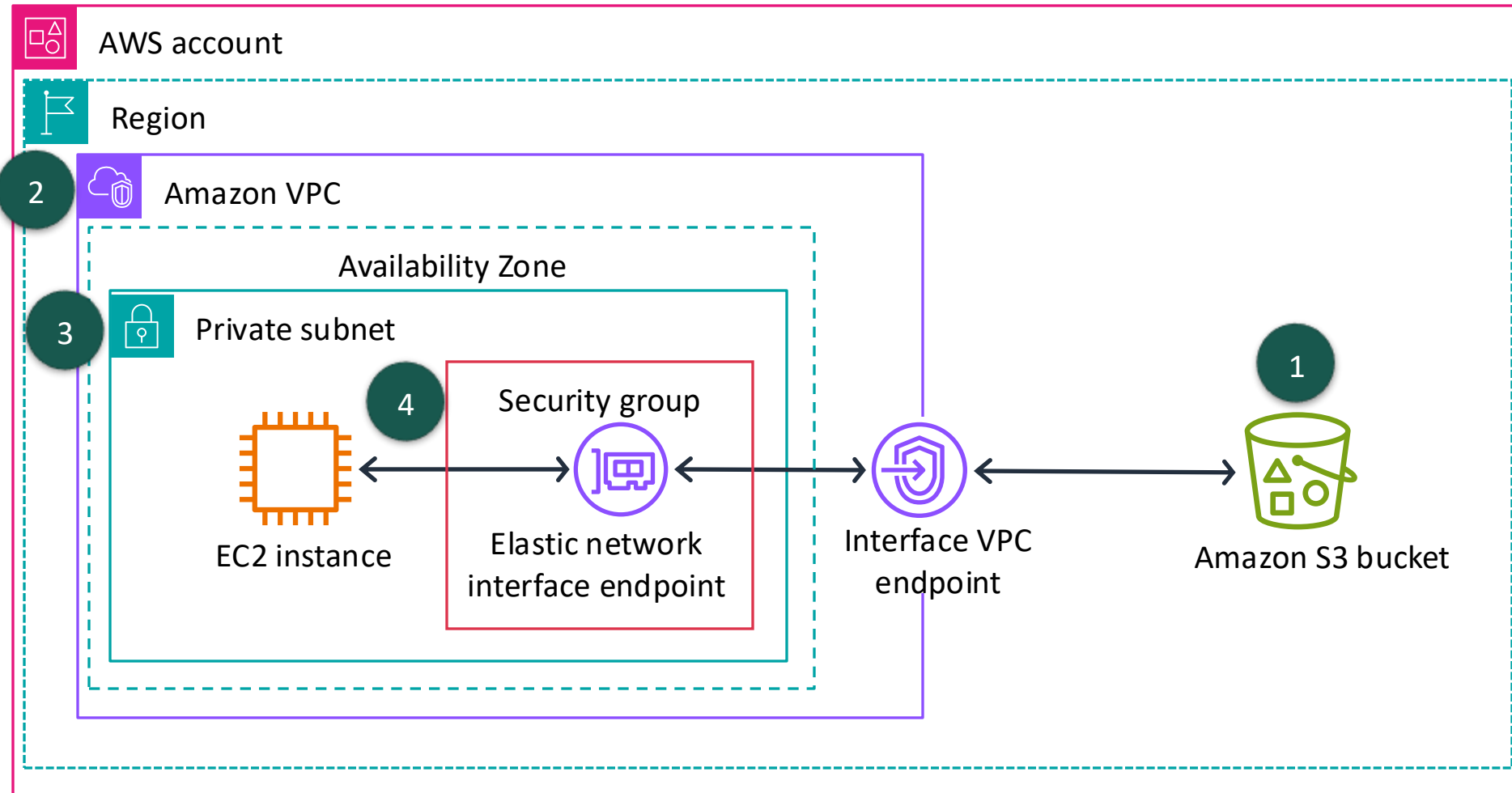
How to connect to managed AWS services



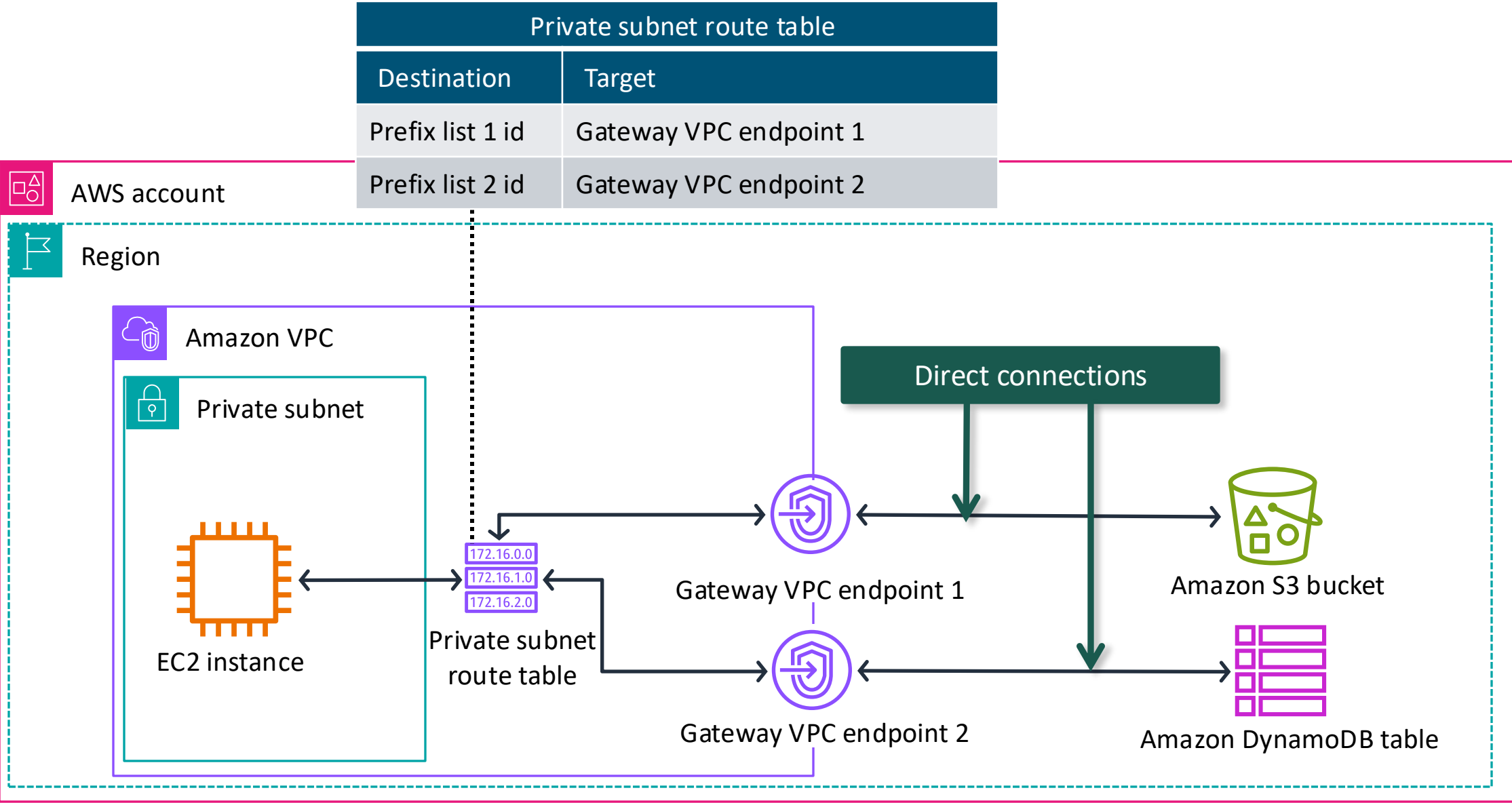
Interface VPC endpoints



How to set up an interface VPC endpoint



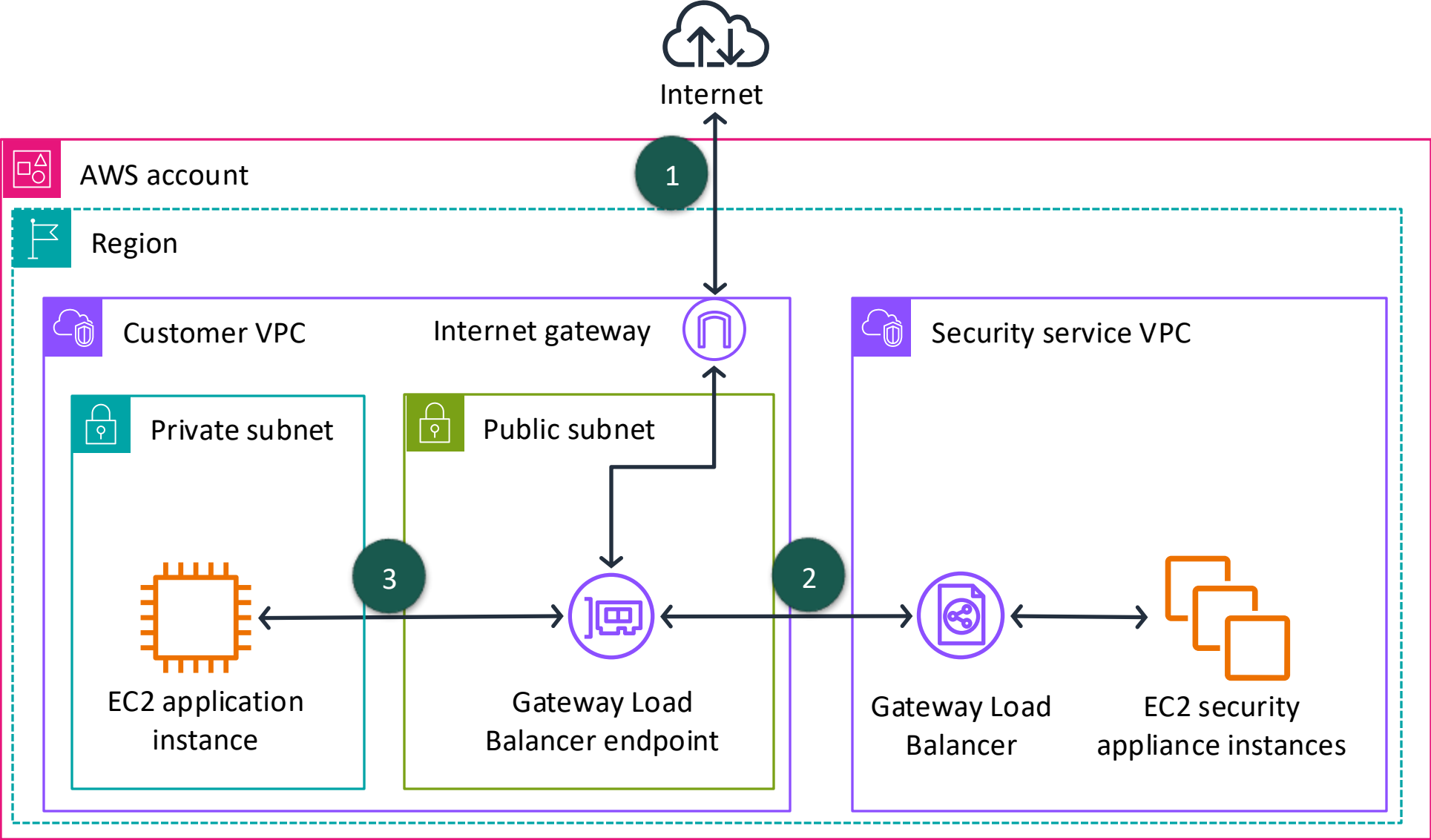
Gateway VPC endpoints



Amazon S3 endpoint considerations

Factor	Interface VPC endpoints	Gateway VPC endpoints
Amazon S3 access point	Private IP addresses from VPC subnet	Amazon S3 public IP addresses
On-premises	Allows access	Does not allow access
Other AWS Region	Allows access	Does not allow access
Cost	Billed	Not billed
Bandwidth	Bandwidth of up to 10 Gbps per AZ, and automatically scales up to 100 Gbps.	No limit
Packet size	Maximum packet size supported is 8500 bytes.	No limit

Gateway Load Balancer endpoint



Key takeaways: Connecting to managed AWS services



- VPC resources can access AWS managed services using VPC endpoints.
- An interface VPC endpoint uses AWS PrivateLink to access AWS managed services. It incurs cost and has throughput limitations.
- A gateway VPC endpoint integrates directly with Amazon S3 and Amazon DynamoDB. It does not incur cost and has no throughput limitations.
- Gateway Load Balancer endpoints are used with Gateway Load Balancers to inspect traffic with security appliances.



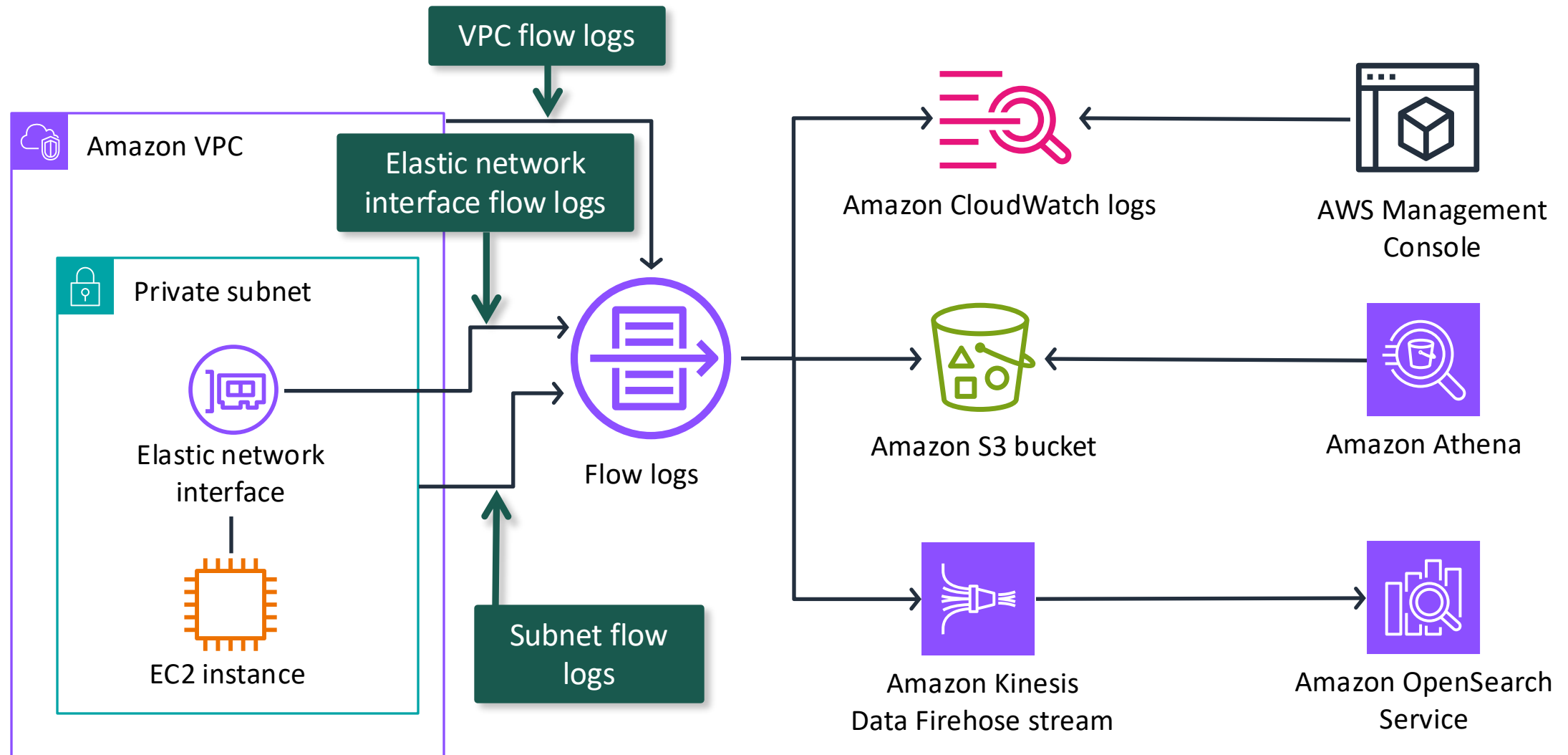
Monitoring your network

Creating a Networking Environment

Network troubleshooting scenarios

- My EC2 instance response times are very slow.
- I can't access my EC2 instance through Secure Shell (SSH).
- My EC2 database instance isn't applying any patches.

Amazon VPC flow logs



Flow log IAM access policy

```
{
  "version": "2012-10-17",
  "statement": [
    {
      "effect": "Allow",
      "action": [
        "ec2:CreateFlowLogs",
        "ec2:DescribeFlowLogs",
        "ec2:DeleteFlowLogs"
      ],
      "resource": "*"
    }
  ]
}
```

IAM policy grants users permissions to create, describe, and delete flow logs.

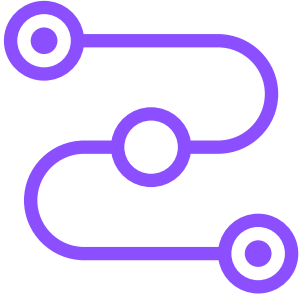
Default flow log record example (1 of 2)

Field name	Field description	Example value
version	VPC Flow Logs version	2
account-id	Network owner AWS account	123456789010
interface-id	Traffic network interface	eni-1235b8ca123456789
srcaddr	Source address for incoming traffic, or the network address interface for outgoing traffic	172.31.16.139
dstaddr	Destination address for outgoing traffic, or the network interface address for incoming traffic	172.31.16.21
srcport	Traffic source port	20641
dstport	Traffic destination port	22
protocol	Traffic IANA protocol number	6 (TCP)

Default flow log record example (2 of 2)

Field name	Field description	Example value
packets	Number of packets transferred	20
bytes	Number of bytes transferred	4249
start	Unix time in seconds of first packet received	1418530010
end	Unix time in seconds of last packet received	1418530070
action	Accept or reject indicator of traffic routing success or failure	ACCEPT
log-status	Flow log status: OK, NODATA, SKIPDATA	OK

More VPC troubleshooting tools



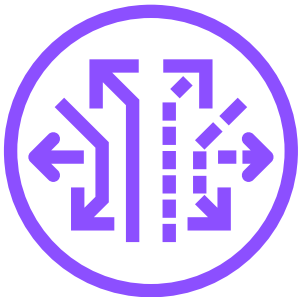
Reachability Analyzer

- Test connectivity between a source and destination resources in a VPC.



Network Access Analyzer

- Identify unintended network access to your resources on AWS.



Traffic Mirroring

- Make a copy of network traffic to send to security and monitoring appliances.

Key takeaways: Monitoring your network



- Use VPC Flow Logs to capture information about the network traffic in your VPC.
- Flow log records consist of all flows within a an aggregation interval.
- Use Reachability Analyzer to test whether two resources in a VPC have connectivity.
- Use Network Access Analyzer to identify unintended network access to resources in your AWS account.
- Use Traffic Mirroring to make a copy of your network traffic to send to security and monitoring appliances.



Applying Well-Architected Framework principles to a network

Creating a Networking Environment

AWS Well-Architected Framework network pillars



Reliability



Security



Performance
Efficiency



Cost
Optimization

Foundations: Plan your network topology



Reliability

Best practice

Ensure IP subnet allocation accounts for expansion and availability.

Infrastructure protection: Protecting networks



Security

Best practices

Create network layers.

Implement inspection and protection.

Control traffic at all layers.

Selection: Network architecture selection



Performance
Efficiency

Best practices

Understand how
networking impacts
performance.

Evaluate available
networking features.

Choose network protocols
to improve performance.

Select the best pricing model



Cost
Optimization

Best practice

Choose Regions based on cost.

Network design issue scenario

Identify the network design mistakes that were made in the following scenario:

- Company A sells fitness shoes and is based in Europe. The company's customer base is in the United States.
- The company deployed their website servers and database servers in the Ireland AWS Region in a single VPC with one public subnet.
- The VPC has a netmask of /27 with 32 IP addresses. The subnet has a netmask of /28 with 16 IP addresses available.
- The security group attached to the website and database servers allows internet traffic to the servers. Company A is projecting rapid growth in the near future.

Common anti-patterns and patterns

Small VPC with
small subnets

Anti-pattern 1

Permissive
security groups

Anti-pattern 2

Direct access to
databases

Anti-pattern 3

AWS Region far
from customers

Anti-pattern 4

Large VPCs with
large public and
private subnets

Pattern 1

Strict security
groups layered
by server usage

Pattern 2

No direct access
to databases

Pattern 3

AWS Region
close to
customers

Pattern 4

Key takeaways: Applying Well- Architected Framework principles to your network



- Ensure IP subnet allocation accounts for expansion and availability.
- Create network layers and control traffic at all layers.
- Understand how networking impacts performance.
- Choose network protocols to improve performance.
- Implement Regions based on cost providing low latency and strong data sovereignty.



Guided lab: Creating a Virtual Private Cloud (VPC lab)

VPC lab tasks



- Create an AWS cloud network environment using the Amazon VPC service.
- Create an Amazon VPC with public subnet and private subnet. Place an application server EC2 instance in the public subnet.
- Configure an internet gateway, route table, and security group to allow internet traffic to the application server.
- Open your lab environment to start the lab and find additional details about the tasks that you will perform.

Debrief: VPC lab

- What layers of isolation did you provide in your VPC?
- What configurations did you apply to the AWS VPC features to define the traffic flow from the internet to the application server?



Café lab: Creating a VPC Networking Environment for the Café (Café VPC lab)

The evolving café architecture (version 4)

Architecture Version	Business reason for update	Description of architecture or updates
V1	Static website for small business	Website hosted on Amazon S3.
V2	Add online ordering	Web application and database deployed on EC2.
V3	Reduce effort to maintain the database and secure its data	Separate web and database layers. Database migrated to Amazon RDS on a private subnet.
V4	Enhance the security of the web application	Use Amazon VPC features to configure and secure public and private subnets.
V5	Create separate access mechanisms based on role	Add IAM groups and attach resource policies to application resources. Add IAM users to groups based on role.
V6	Ensure the website can handle an expected increase in traffic	Add a load balancer, implement auto scaling on the EC2 instances, and distribute compute and database instances across two Availability Zones.



Café VPC lab tasks



In this lab, you will do the following:

- Make the application server more secure.
- Move the application instance to a private subnet. Setup a bastion instance in a public subnet to allow test instance access to the application server. Configure a security group for every instance.
- Allow the application server to download patches from the internet by setting up a NAT gateway in the public subnet.
- Increase security by adding network ACL rules.

Open your lab environment to start the lab and find additional details about the tasks that you will perform.

Debrief: Café VPC lab

- What did you configure for the application instance to be accessed through the bastion instance?
- What configurations did you apply to define the traffic flow from the internet to the application server?

Considerations for the café

- Discuss how the cloud architect's concerns presented in the module introduction are reflected in the VPC that you created in the café lab.





Module wrap-up

Creating a Networking Environment

Module summary

This module prepared you to do the following:

- Explain the role of a virtual private cloud (VPC) in Amazon Web Services (AWS) Cloud networking.
- Identify the components in a VPC that can connect an AWS networking environment to the internet.
- Isolate and secure resources within your AWS networking environment.
- Create and monitor a VPC with subnets, an internet gateway, route tables, and a security group.
- Use the AWS Well-Architected Framework principles when creating and planning a network environment.

Module knowledge check



- The knowledge check is delivered online within your course.
- The knowledge check includes 10 questions based on the material that was presented on the slides and in the slide notes.
- You can retake the knowledge check as many times as you like.

Sample exam question

A company runs a public-facing three-tier web application in a virtual private cloud (VPC) across multiple Availability Zones (AZs). Amazon Elastic Compute Cloud (Amazon EC2) instances for the application tier running in private subnets need to download software patches from the internet. However, the EC2 instances cannot be directly accessible from the internet.

Which actions should be taken to allow the EC2 instances to download the needed patches? (Select TWO.)

Identify the key words and phrases before continuing.

The following are the key words and phrases:

- Public-facing web application
- Needs to download software patches from the internet
- Cannot be directly accessible from the internet

Sample exam question: Response choices

A company runs a **public-facing** three-tier web application in a virtual private cloud (VPC) across multiple Availability Zones (AZs). Amazon Elastic Compute Cloud (Amazon EC2) instances for the application tier running in private **subnets need to download software patches from the internet**. However, the EC2 instances **cannot be directly accessible from the internet**.

Which actions should be taken to allow the EC2 instances to download the needed patches? (Select TWO.)

Choice	Response
A	Configure a NAT gateway in a public subnet.
B	Configure a NAT instance in a private subnet.
C	Define a custom route table with a route to the internet gateway for internet traffic and associate it with the private subnets for the application tier.
D	Define a custom route table with a route to the NAT gateway for internet traffic and associate it with the private subnets for the application tier.
E	Assign Elastic IP addresses to the EC2 instances.

Sample exam question: Answer

The answers are A and D.

Choice	Response
A	Configure a NAT gateway in a public subnet.
D	Define a custom route table with a route to the NAT gateway for internet traffic and associate it with the private subnets for the application tier.



Thank you

Corrections, feedback, or other questions?

Contact us at <https://support.aws.amazon.com/#/contacts/aws-academy>.