aws academy

CSCI 5902 Adv. Cloud Architecting
Fall 2023
Instructor: Lu Yang

Module 6 Creating a Networking Environment
(Sections 1 - 4)
Oct 20, 2023

© 2020 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Housekeeping items and feedback

1. Start recording
2. Midterm in class Friday, Oct 27 — cheatsheet letter size double sides
3. Lab assignment 3 due today
4. Architecture design assignment 2 due today

Question:

A3

When a failover happens, does the new RDS primary instance wait for the secondary instance to finish synchronization?

AWS Academy Cloud Architecting

Module 6: Creating a Networking Environment

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Module overview

Sections

1. Architectural need
2. Creating an AWS networking environment
3. Connecting your AWS networking environment to the internet
4. Securing your AWS networking environment

Labs

- Guided Lab: Creating a Virtual Private Cloud
- Challenge Lab: Creating a VPC Networking Environment for the Café

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Module objectives

At the end of this module, you should be able to:

- Explain the foundational role of a virtual private cloud (VPC) in Amazon Web Services (AWS) Cloud networking
- Identify how to connect your AWS networking environment to the internet
- Describe how to isolate resources within your AWS networking environment
- Create a VPC with subnets, an internet gateway, route tables, and a security group

NACL

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

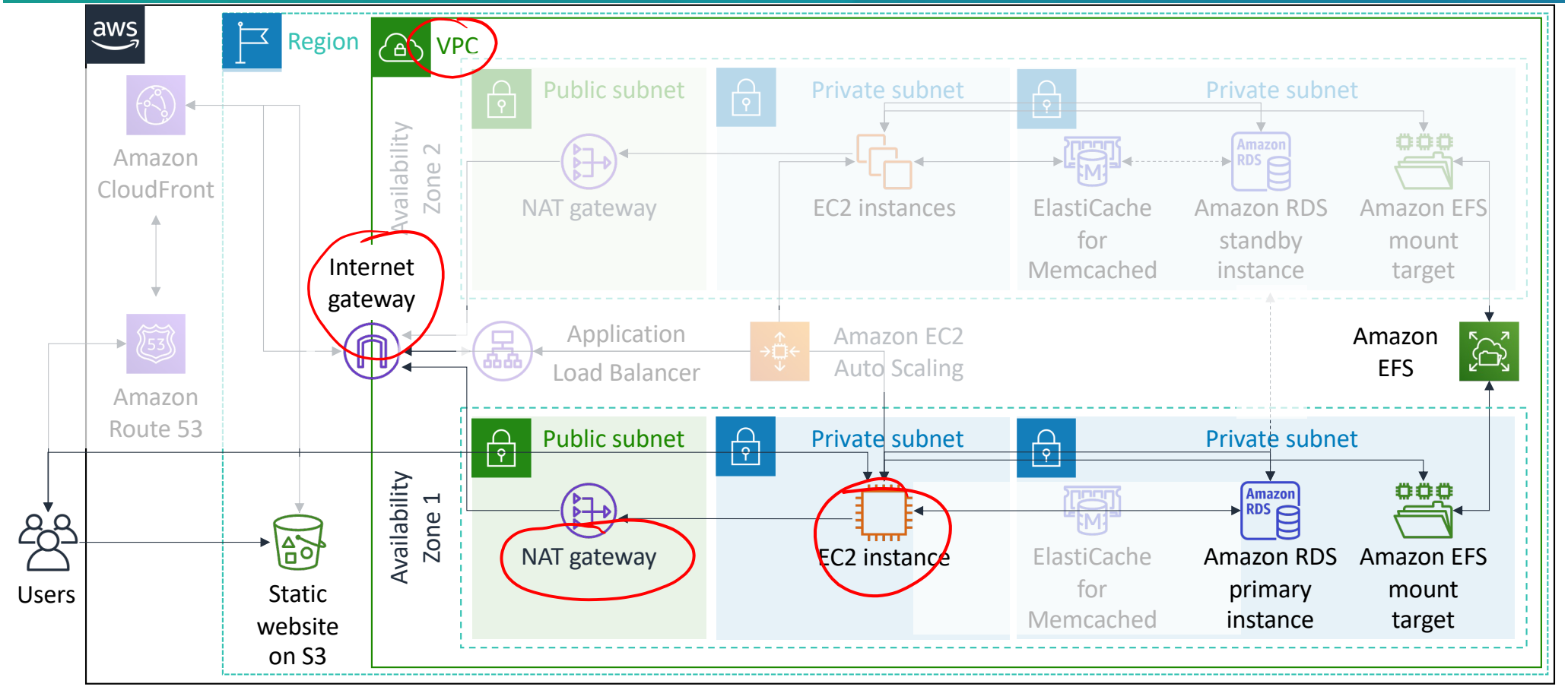
Module 6: Creating a Networking Environment

Section 1: Architectural need

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws academy

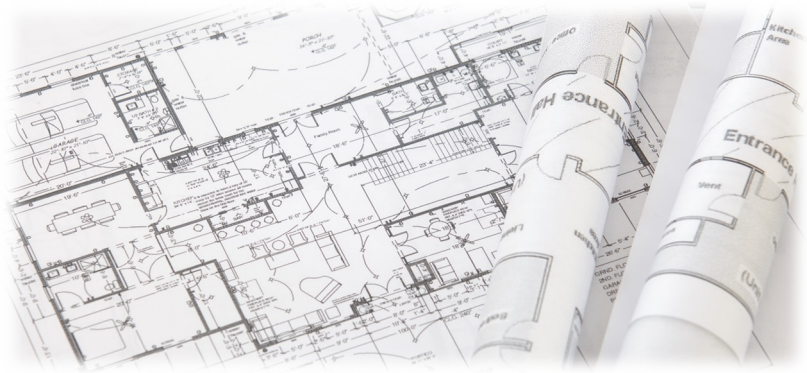
Networking as part of a larger architecture



© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Café business requirement

The café must deploy and manage AWS resources in a secure, isolated network environment.



© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Module 6: Creating a Networking Environment

Section 2: Creating an AWS networking environment

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws academy

Amazon VPC

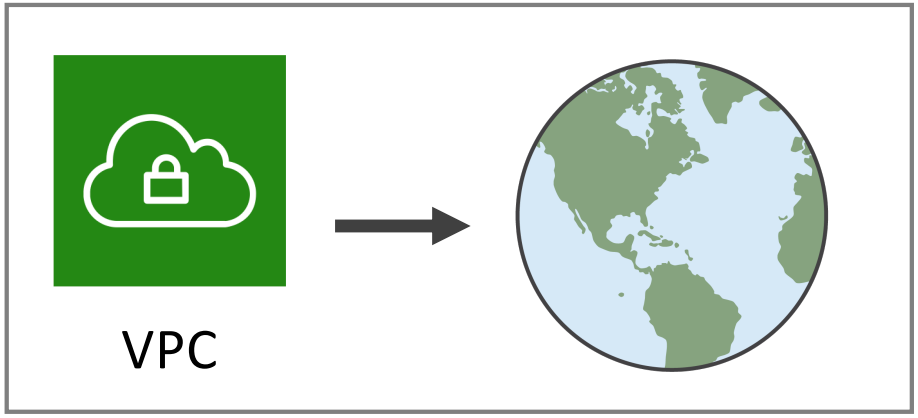
Provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define.

Bring your own network

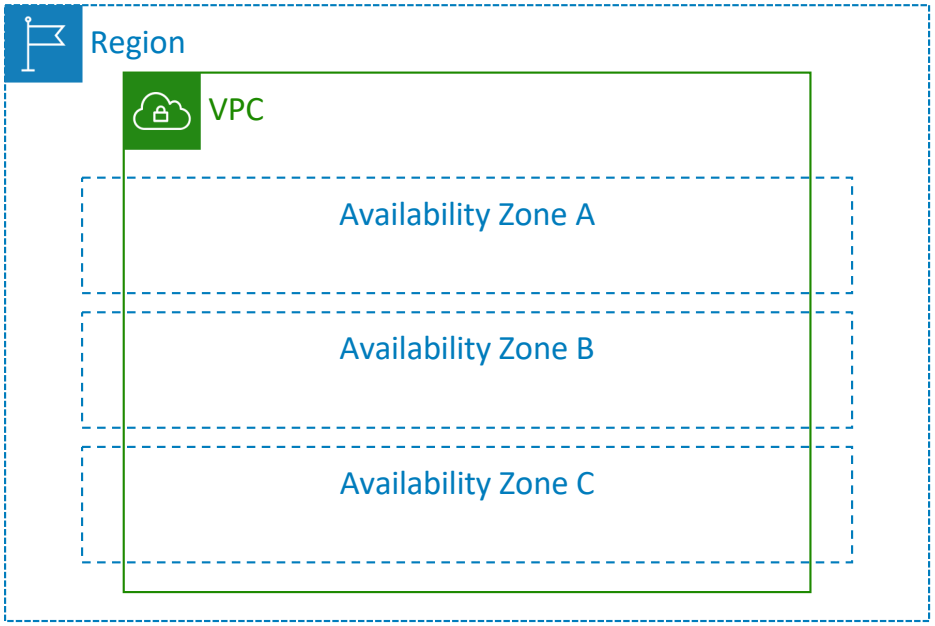
IP Addresses | Subnets | Routing rules | Network configuration | Security rules

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

VPC deployment



You can deploy a VPC in any AWS Region.



A VPC can host supported resources from any Availability Zone within its Region.

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Classless Inter-Domain Routing (CIDR)

0.0.0.0/0	= All IP addresses
10.22.33.44/32	= 10.22.33.44
10.22.33.0/24	= 10.22.33.*
10.22.0.0/16	= 10.22.*.*

CIDR	Total IP addresses
/28	16
…	…
/20	4,096
/19	8,192
/18	16,384
/17	32,768
/16	65,536

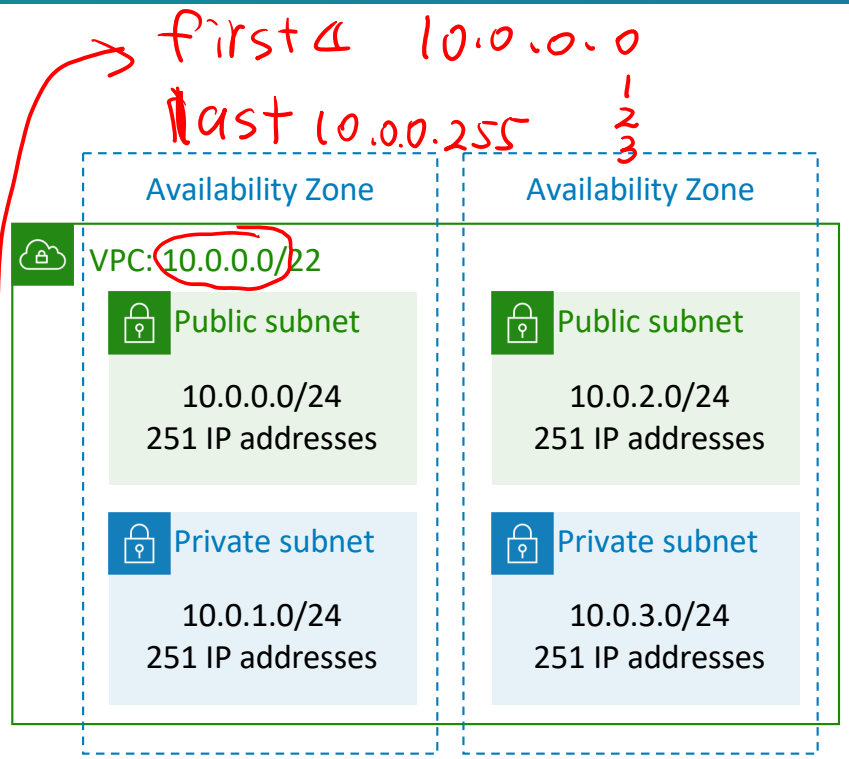
Private IP

- 10.0.0.0 – 10.255.255.255 (10.0.0.0/8) for big networks
- 172.16.0.0 – 172.31.255.255 (172.31.0.0/12)
- 192.168.0.0 – 192.168.255.255 (192.168.0.0/16) for home networks

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Subnets: Dividing your VPC

- A subnet is a segment or partition of a VPC's IP address range where you can allocate a group of resources
- Subnets are not isolation boundaries
- Subnets are a subset of the VPC CIDR block
- Subnet CIDR blocks cannot overlap
- Each subnet resides entirely within one Availability Zone
- You can add one or more subnets in each Availability Zone or in a Local Zone
- AWS reserves five IP addresses in each subnet



Example: A VPC with CIDR /22 includes 1,024 total IP addresses.

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

VPC design best practices

- Create one subnet per available Availability Zone for each group of hosts that have unique routing requirements.
- Divide your VPC network range evenly across all available Availability Zones in a Region.
- Do not allocate all network addresses at once. Instead, ensure that you reserve some address space for future use.
- Size your VPC CIDR and subnets to support significant growth for the expected workloads.
- Ensure that your VPC network range (CIDR block) does not overlap with your organization's other private network ranges.

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Single VPC deployment

There are limited use cases where deploying one VPC might be appropriate:

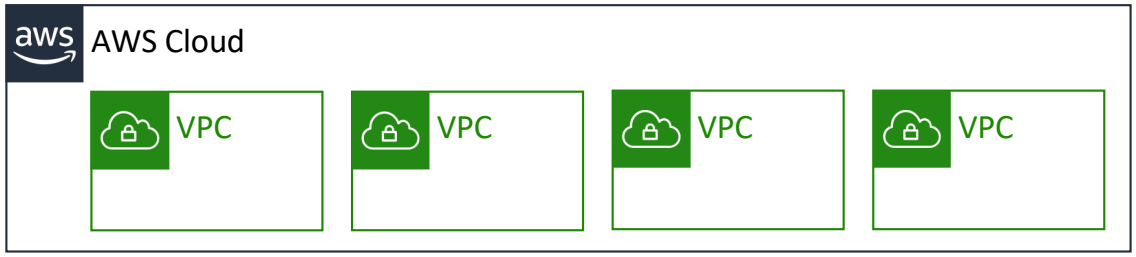
- Small, single applications managed by a small team
- High performance computing (HPC)
- Identity management

For most use cases, there are two primary patterns for organizing your infrastructure: multi-VPC and multi-account.

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Multiple VPCs

- Best suited for –
  - Single team or single organizations, such as managed service providers
  - Limited teams, which makes it easier to maintain standards and manage access
- Exception –
  - Governance and compliance standards might require greater workload isolation regardless of organizational complexity



© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

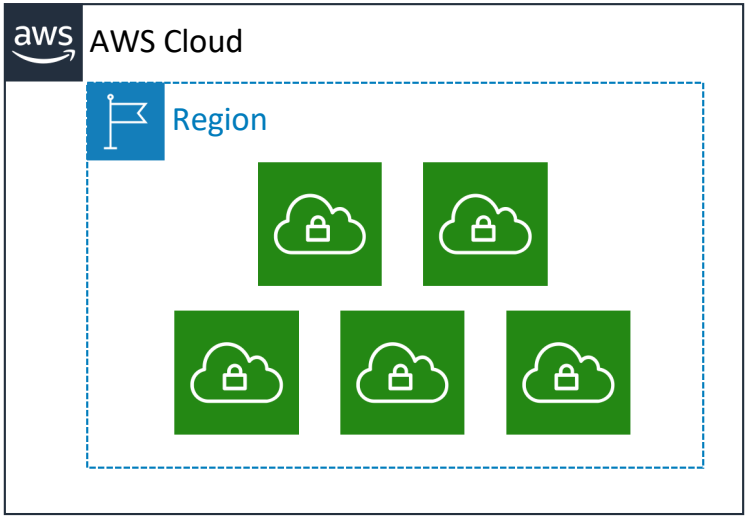
Multiple accounts

- Best suited for –
  - Large organizations and organizations with multiple IT teams
  - Medium-sized organizations that anticipate rapid growth
- Why?
  - It can be more challenging to manage access and standards in more complex organizations

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Amazon VPC quotas

Default quota: 5 VPCs per Region per account *



* The default quota is 5 VPCs per Region, but you can request a quota increase.

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Section 2 key takeaways

- Amazon VPC enables you to provision VPCs, which are logically isolated sections of the AWS Cloud where you can launch your AWS resources.
- A VPC belongs to only one Region and is divided into subnets.
- A subnet belongs to one Availability Zone or Local Zone. It is a subset of the VPC CIDR block.
- You can create multiple VPCs in the same Region or in different Regions, and in the same account or different accounts.
- Follow best practices when you design your VPC.

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Module 6: Creating a Networking Environment

Section 3: Connecting your AWS networking environment to the internet

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws academy

Default VPC

- A default VPC is configured and ready for you to use. For example, it has
  - a *default subnet* in each Availability Zone in the Region,
  - an attached internet gateway,
  - a route in the main route table that sends all traffic to the internet gateway,
  - and DNS settings that automatically assign public DNS hostnames to instances with public IP addresses and enable DNS resolution through the Amazon-provided DNS server. Therefore, an EC2 instance that is launched in a default subnet automatically has access to the internet.
  - If you have a default VPC in a Region and you don't specify a subnet when you launch an EC2 instance into that Region, AWS chooses one of the default subnets and launch the instance into that subnet.
- You can also create your own VPC, and configure it as you need. This is known as a *nondefault VPC*. Subnets that you create in your nondefault VPC and additional subnets that you create in your default VPC are called *nondefault subnets*.

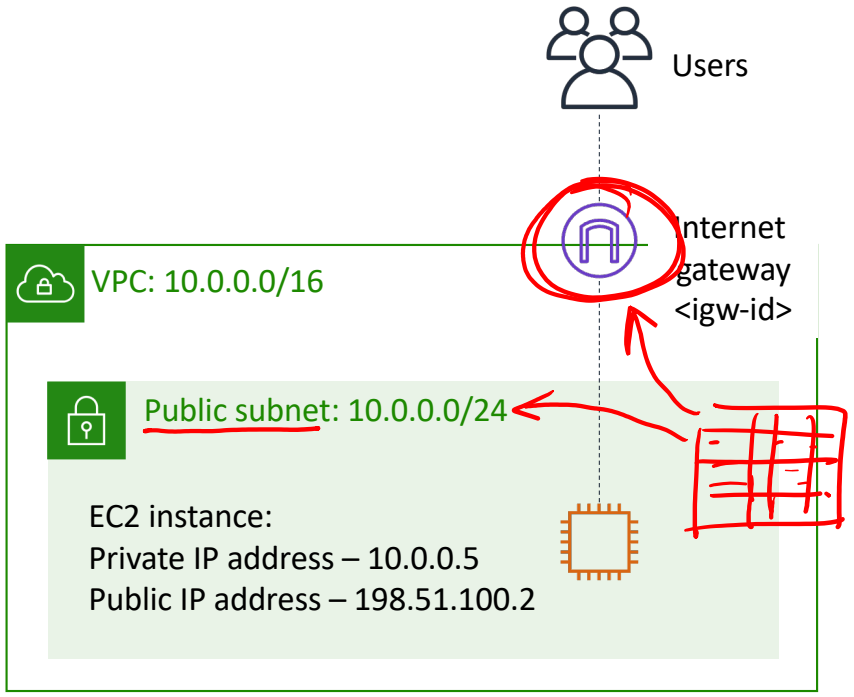
© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

https://docs.aws.amazon.com/vpc/latest/userguide/how-it-works.html

Creating a public subnet

Internet gateways

- Allow communication between resources in your VPC and the internet
- Are horizontally scaled, redundant, and highly available by default
- Provide a target in your subnet route tables for internet-routable traffic
- IGW performs Network Address Translation (NAT) for instances

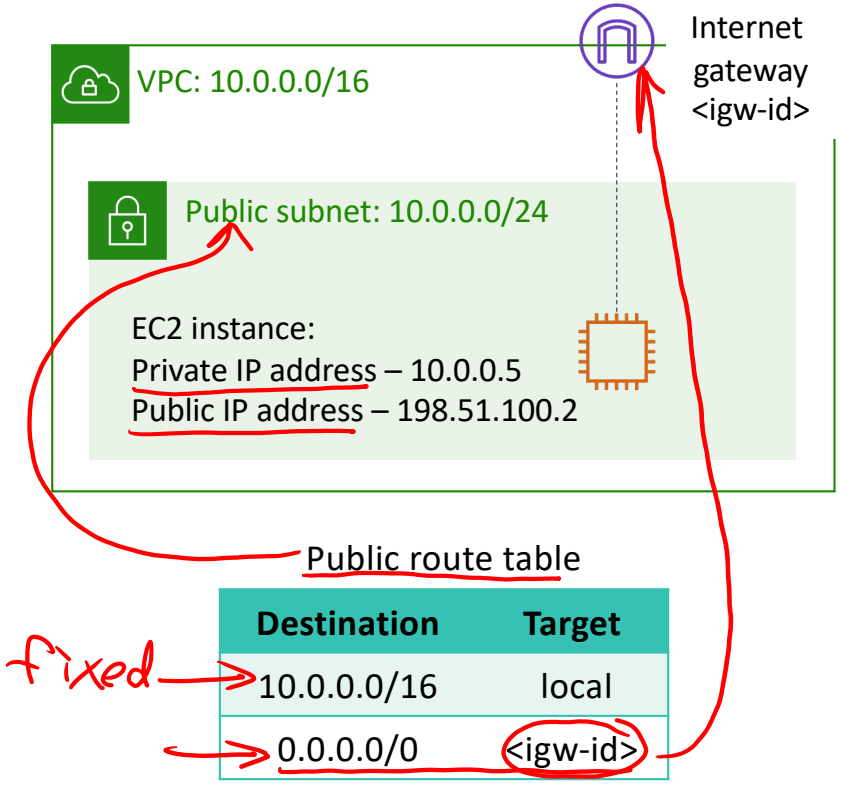


© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Directing traffic between VPC resources

- Route tables are required to direct traffic between VPC resources
- Each VPC has a main (default) route table
- Each subnet must be associated with a route table
- You can create custom route tables

Best practice: Use custom route tables for each subnet.



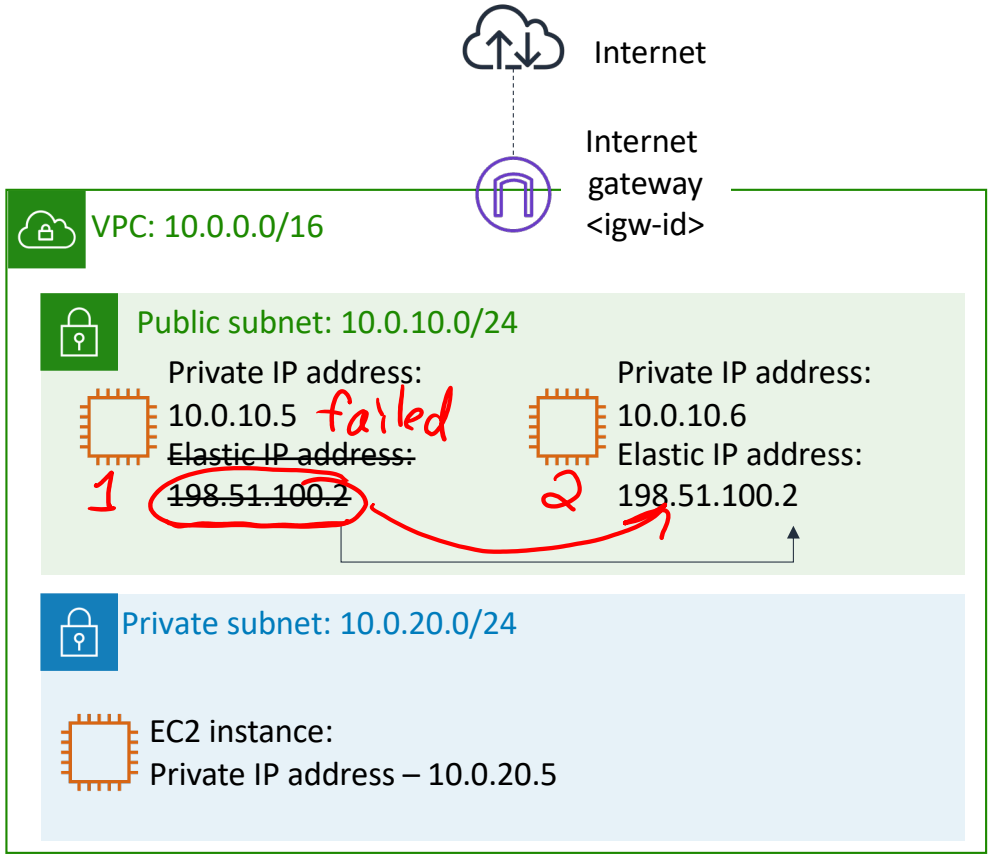
© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Remapping an IP address from one instance to another

aws academy

Elastic IP addresses

- Are static, public IPv4 addresses associated with your AWS account
- Can be associated with an instance or elastic network interface
- Can be remapped to another instance in your account
- Are useful for redundancy when load balancers are not an option



© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Connecting private subnets to the internet

NAT gateways

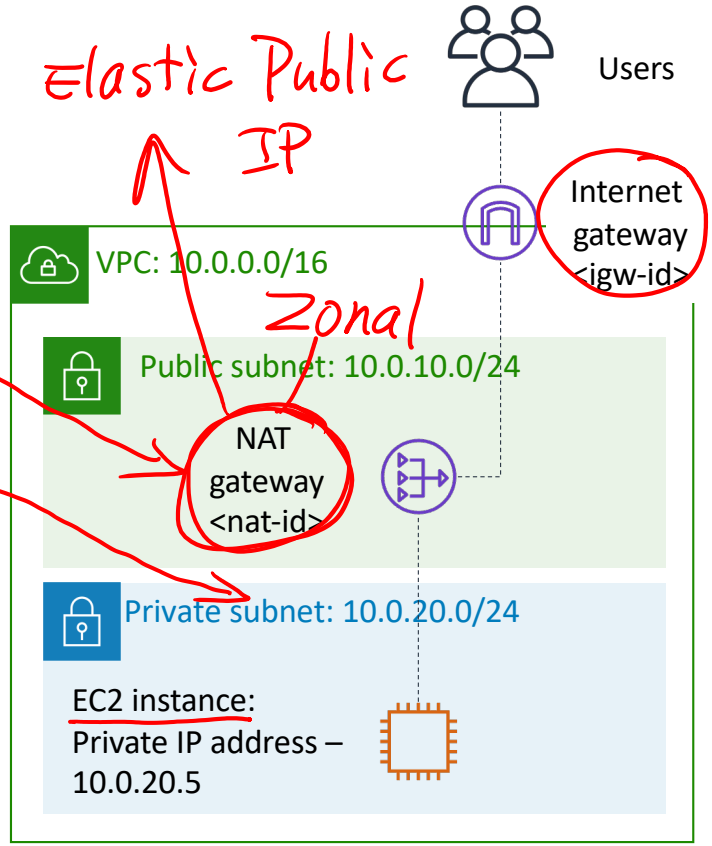
- Enable instances in a private subnet to initiate outbound traffic to the internet or other AWS services
- Prevent private instances from receiving inbound connection requests from the internet

Public route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	<igw-id>

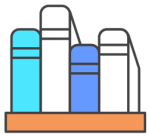
Private route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	<nat-id>



© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Subnet use case examples (1 of 2)



Data store instances

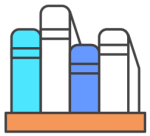
Batch-processing instances

Backend instances

Web application instances

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Subnet use case examples (2 of 2)



Data store instances → Private subnet

Batch-processing instances → Private subnet

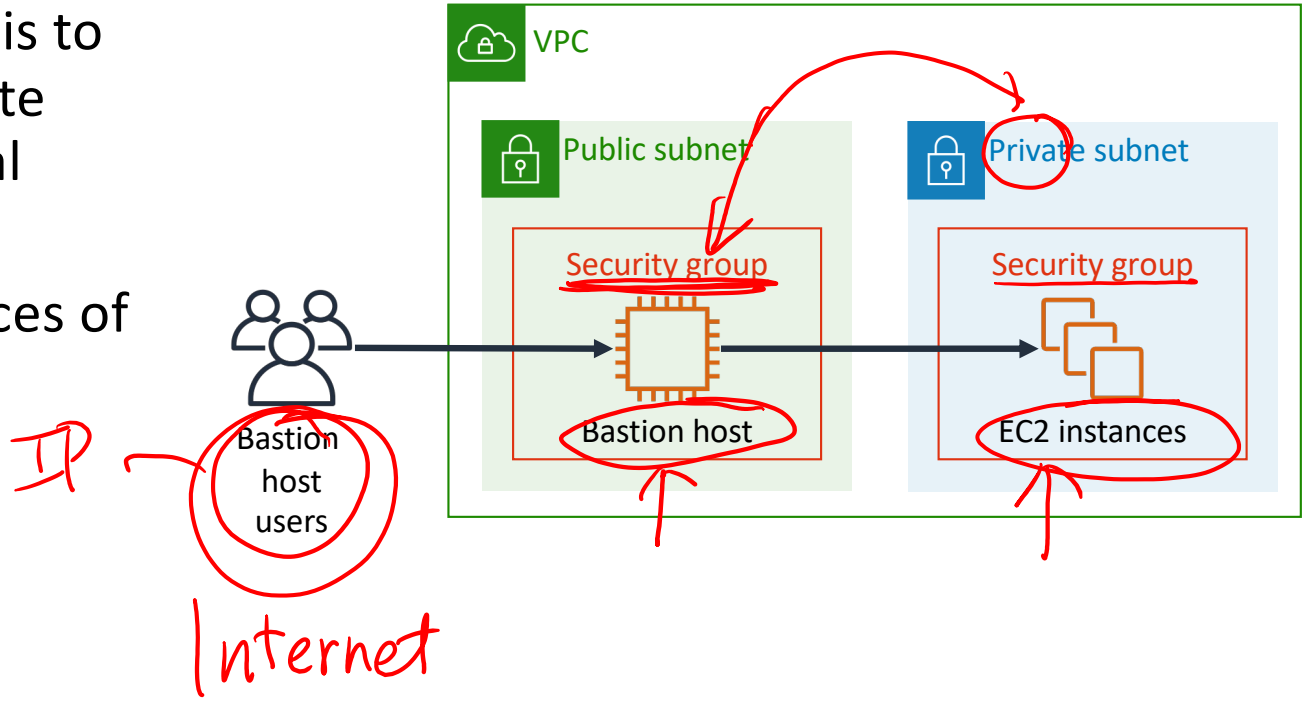
Backend instances → Private subnet

Web application instances → Public or private subnet

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Bastion hosts

- A server whose purpose is to provide access to a private network from an external network
- Must minimize the chances of penetration



© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Demonstration: Creating a Virtual Private Cloud

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Section 3 key takeaways

- An internet gateway allows communication between instances in your VPC and the internet.
- Route tables control traffic from your subnet or gateway.
- Elastic IP addresses are static, public IPv4 addresses that can be associated with an instance or elastic network interface. They can be remapped to another instance in your account.
- NAT gateways enable instances in the private subnet to initiate outbound traffic to the internet or other AWS services.
- A bastion host is a server whose purpose is to provide access to a private network from an external network, such as the internet.

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Module 6: Creating a Networking Environment

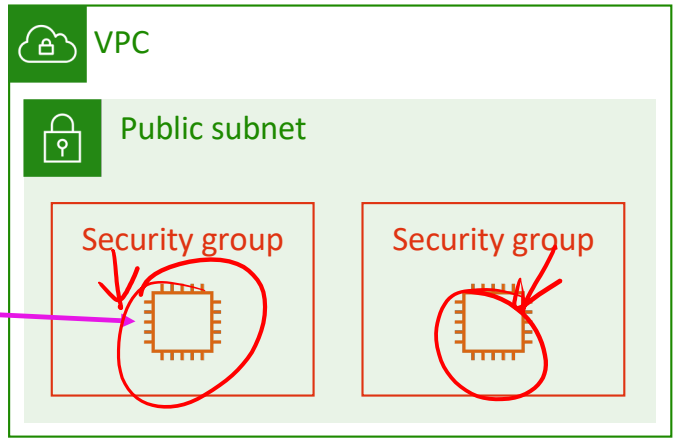
Section 4: Securing your AWS networking environment

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws academy

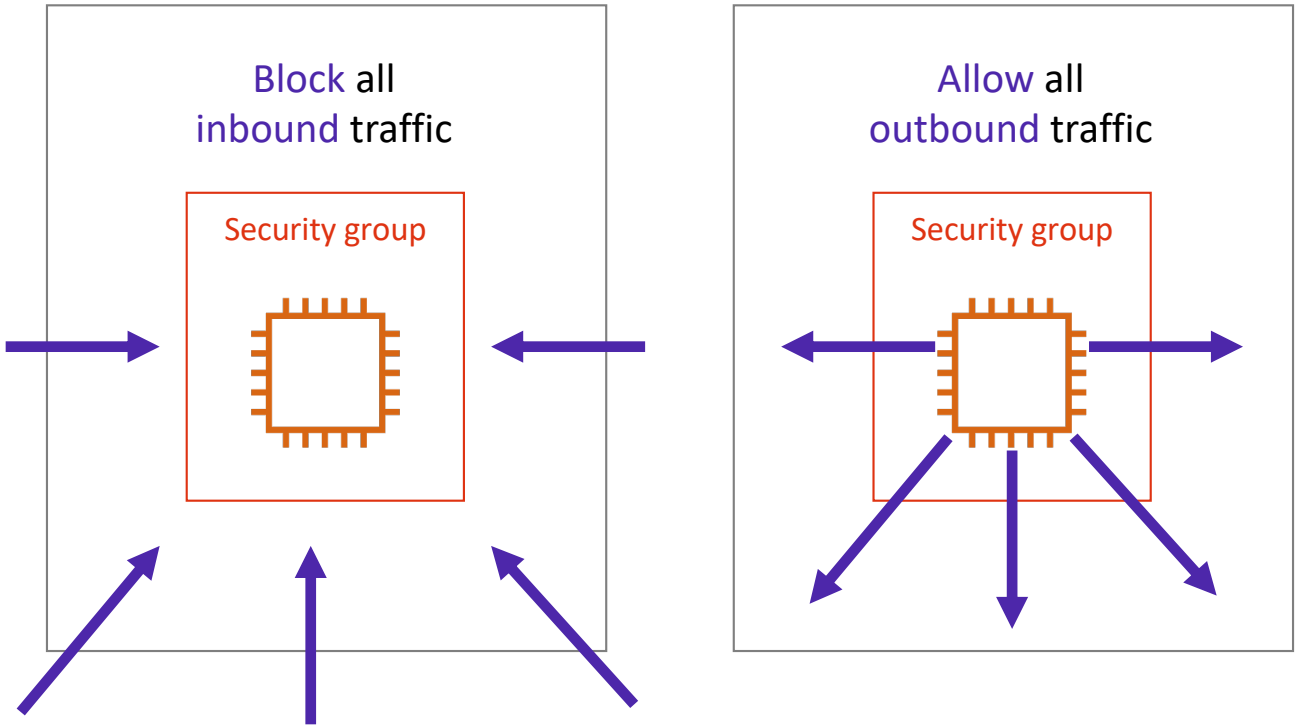
Security groups

- Are stateful firewalls that control inbound and outbound traffic to AWS resources
- Act at the level of the instance or network interface



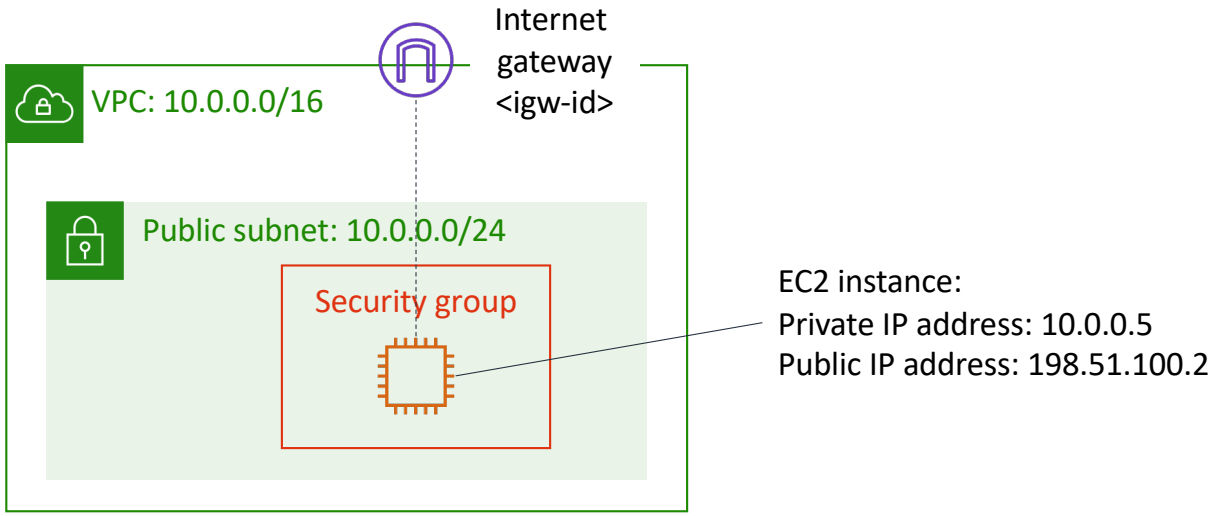
© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Default security groups



© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

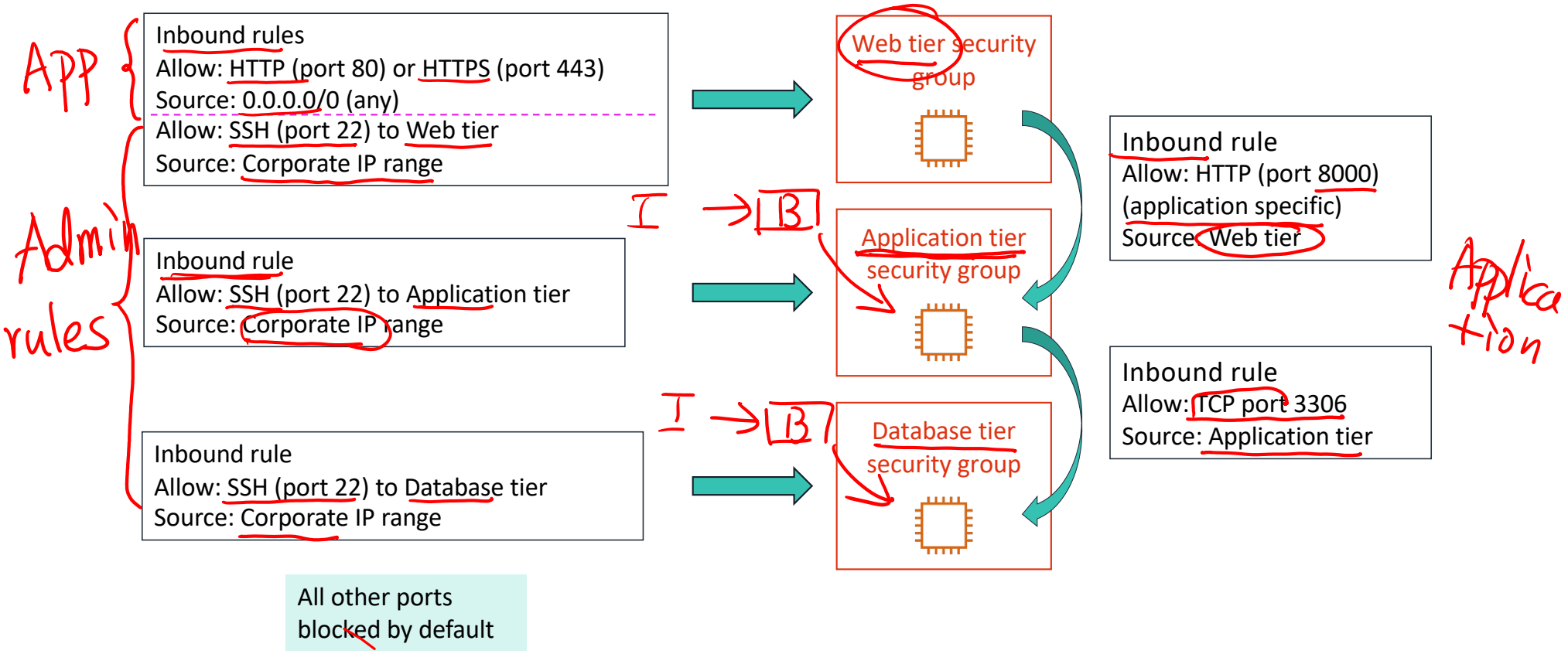
Custom security groups



Inbound				
Type	Protocol	Port Range	Source	Destination
HTTP	TCP	80	Anywhere	Allow web access

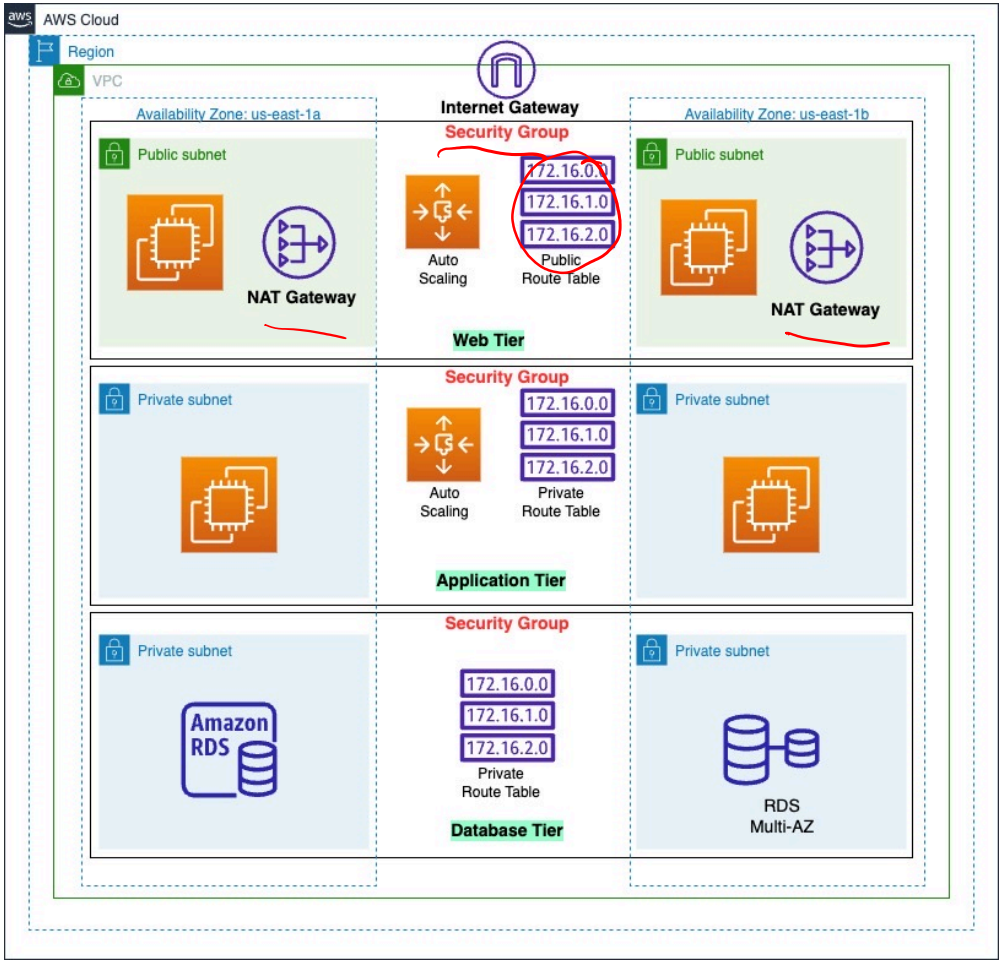
© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Chaining security groups



© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Use Case Study Revisit - Creating a three-tier architecture



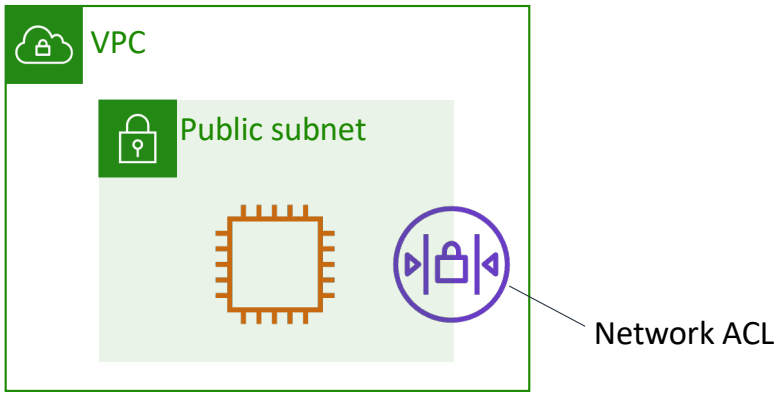
Web tier is a top-level tier and its main purpose is to display and collect information from the user and send its contents to the browser in the form of HTML/JS/CSS. Its main purpose is to display information to and collect information from the user.

Application tier is the brains of the application. This tier houses the business logic used to process user inputs. The application tier can also add, delete or modify data in the database tier.

Database tier is the data or backend tier of a web application. It is where the information processed by the application is stored and managed.

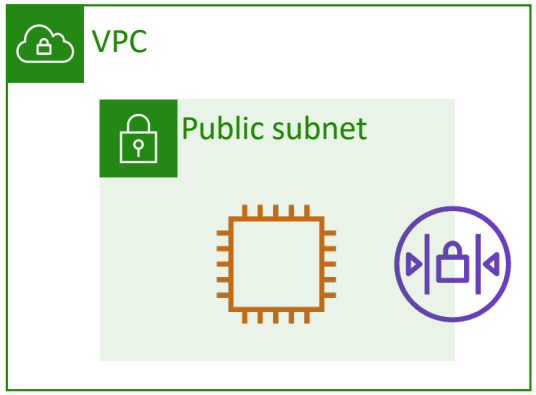
Network access control lists (network ACLs)

- Act at the subnet level
- Allow all inbound and outbound traffic by default
- Are stateless firewalls that require explicit rules for both inbound and outbound traffic



© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Custom network ACLs



Nacl-11223344

Inbound:
Rules # 100: SSH 172.31.1.2/32 ALLOW
Rules # *: ALL traffic 0.0.0.0/0 DENY

Outbound:
Rules # 100: Custom TCP 172.31.1.2/31 ALLOW
Rules # *: All traffic 0.0.0.0/0 DENY

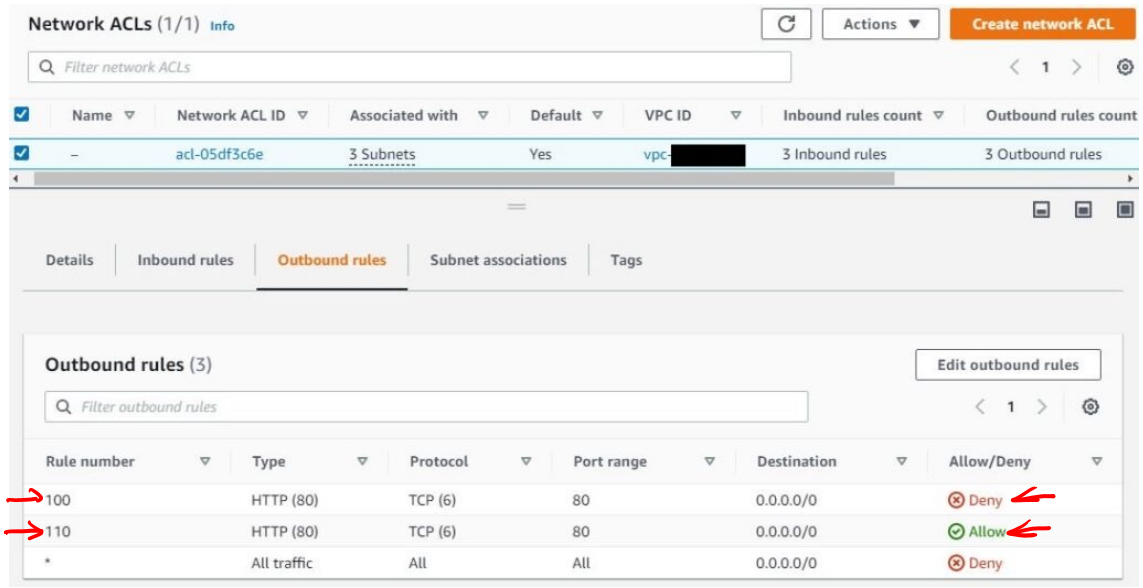
© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Regarding NACL rule numbers:

- Rule Number Range: NACL rule numbers must be between 1 and 32766 (inclusive). Rule numbers cannot be negative or zero.
- Rule Evaluation Order: NACL rules are processed in ascending order based on their rule numbers. Lower rule numbers have higher priority and are evaluated first.
- Rule Overriding: If multiple rules match a specific traffic flow, the rule with the lowest number takes precedence. Once a matching rule is found, the evaluation process stops, and the corresponding action defined in that rule is applied.
- Rule Modification: You can add, remove, or modify rules in an NACL without changing the rule numbers of existing rules. If a new rule is added, it will be assigned the next available rule number.
- Implicit Deny: By default, NACLs have an implicit "deny all" rule at the end, with the rule number 32767. This means that if no explicit rule matches a traffic flow, it will be denied.
- Rule Priority: Rule numbers do not necessarily reflect the priority of rules based on their position in the NACL. Each rule is evaluated independently based on its rule number, regardless of its order in the list.

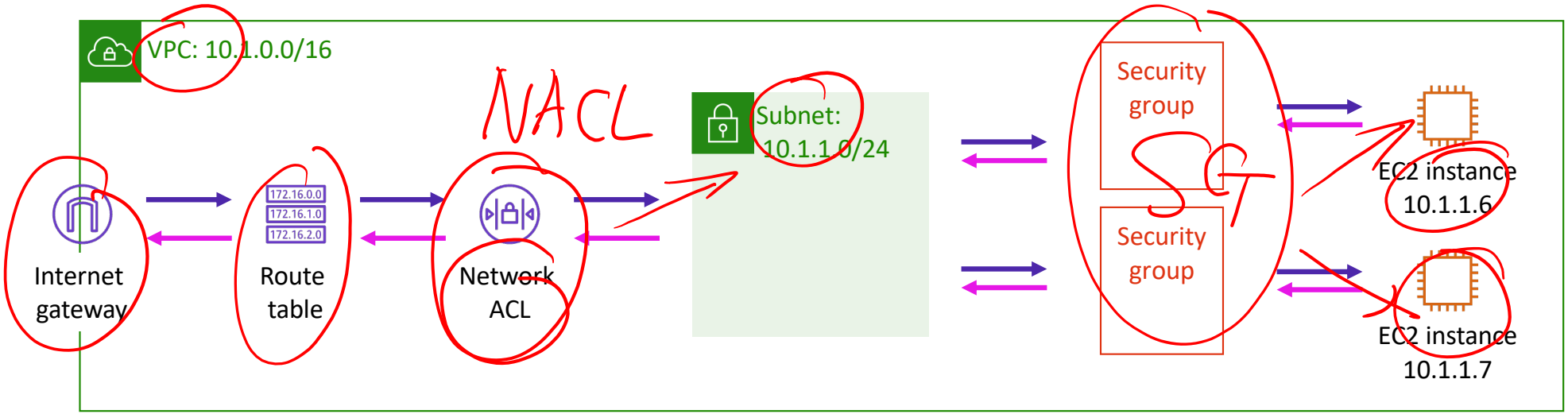
Custom network ACLs

Example:



- In this example:
  - There are two rules.
  - Rule number 100 is denying the HTTP(80) traffic from all IPs.
  - Rule number 110 is allowing the HTTP(80) traffic from all IPs.
  - As stated above, when there is matching rule found no further evaluation happens.
  - For this scenario, rule 100 is matched. If we modify the rule number 110 to less than 100. Let's say 90 then "all the HTTP(80) traffic from all IPs will be allowed". The deny rule number 100 won't be considered.

Structure your infrastructure with multiple layers of defense

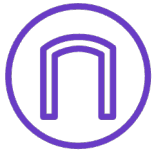


© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Review: How to create a public subnet

To create a public subnet to allow communication between instances in your VPC and the internet, you must:

1



Attach an internet gateway to your VPC.

2

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	<igw-id>

Point your instance subnet's route table to the internet gateway.

3

Make sure that your instances have public IP or Elastic IP addresses.

4

Security group

Make sure that your security groups and network ACLs allow relevant traffic to flow.

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Section 4 key takeaways

- Security groups are stateful firewalls that act at the instance level
- Network ACLs are stateless firewalls that act at the subnet level
- When you set inbound and outbound rules to allow traffic to flow from the top tier to the bottom tier of your architecture, you can chain security groups together to isolate a security breach
- You should structure your infrastructure with multiple layers of defense

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Module 6: Creating a Networking Environment

Module wrap-up

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws academy

Module summary

In summary, in this module, you learned how to:

- Explain the foundational role of VPC in AWS Cloud networking
- Identify how to connect your AWS networking environment to the internet
- Describe how to isolate resources within your AWS networking environment
- Create a VPC with subnets, an internet gateway, route tables, and a security group

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Thank you, and Kahoot!

© 2020 Amazon Web Services, Inc. or its affiliates. All rights reserved. This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited. Corrections or feedback on the course, please email us at: aws-course-feedback@amazon.com. For all other questions, contact us at: https://aws.amazon.com/contact-us/aws-training/. All trademarks are the property of their owners.

aws academy