Amazon Virtual Private Cloud (VPC): Subnets, Routing, NACLs, and Security Groups

Andru Estes
Principal Author
andru-estes

VPC Internet Gateways

Internet Gateway

...a horizontally scaled, redundant, and highly available VPC component that allows communication between your VPC and the internet

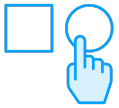
Citation: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html

Internet Gateways Concepts

Supports both IPv4 and IPv6 traffic

Automatically scales for traffic and offers high-availability

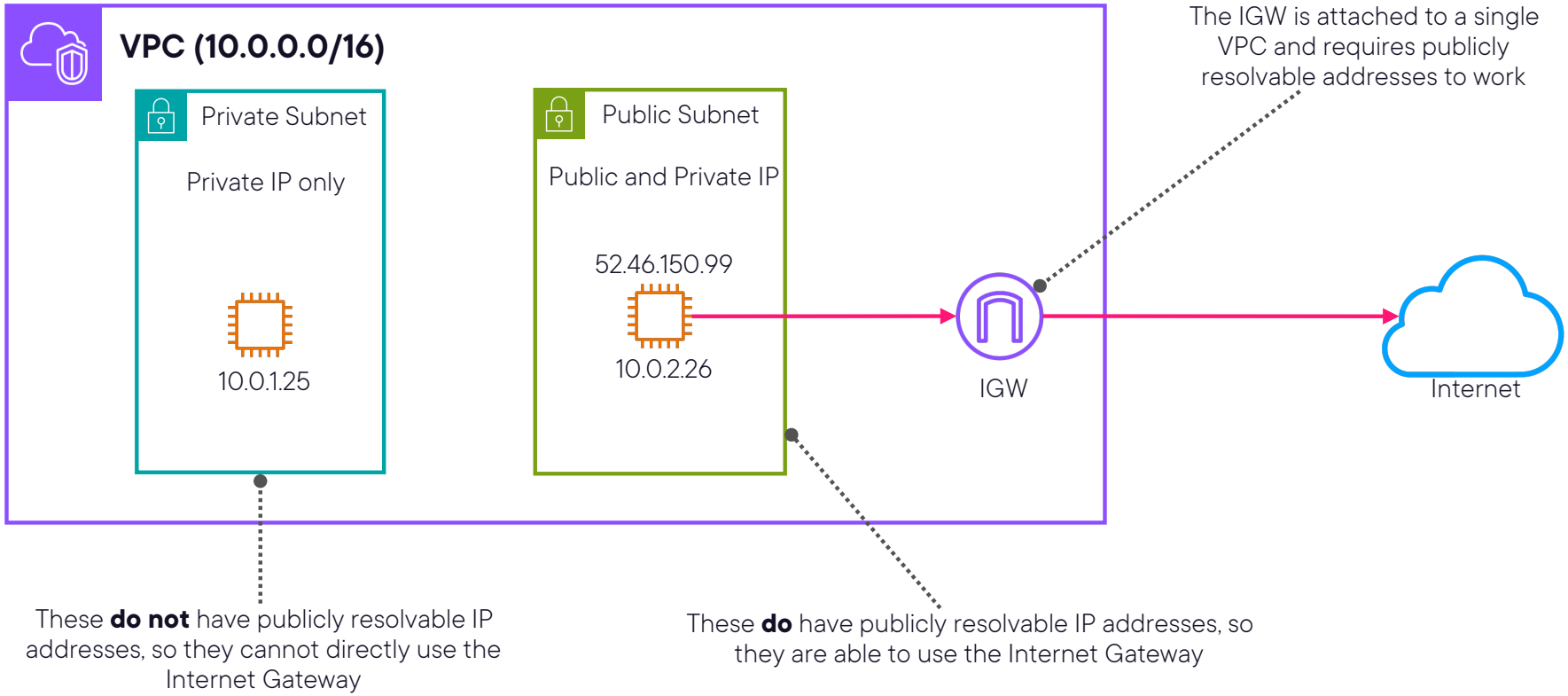
Enables public subnet resources to connect to the internet



Give you a target in your VPC for internet-routable traffic to flow through

Created separately from the VPC, and only attachable to a single VPC

Internet Gateway Architecture - High-level



VPC Subnets

VPC Subnets

Range of IP addresses within your VPC for hosting resources

Subnets are bound to a single Availability Zone (AZ)

Subnets support IPv4 only, Dual stack, and IPv6 only

Four Types: public, private, VPN-only, and isolated

AWS reserves 5 IP addresses per subnet.

This means plan your subnet spaces accordingly.

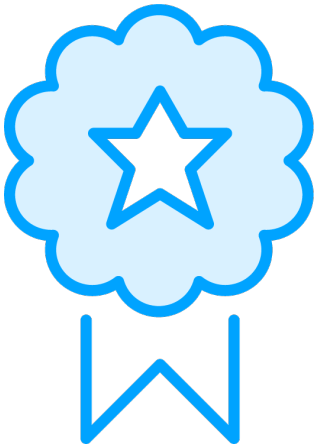
Assuming we have a /28 subnet CIDR, that means you really only have 11 *(16 - 5)* useable IP addresses.

Reserved Subnet IPs

VPC CIDR: 10.0.0.0/16
Subnet CIDR: 10.0.0.0/24

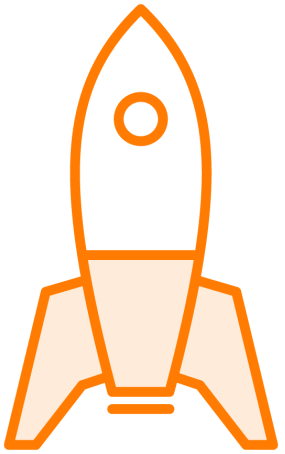
10.0.0.0 Network address	10.0.0.1 VPC Router	10.0.0.2 VPC DNS Server
10.0.0.3 Future Use	10.0.0.255 Broadcast Address	

Public and Private Subnets



Public Subnets

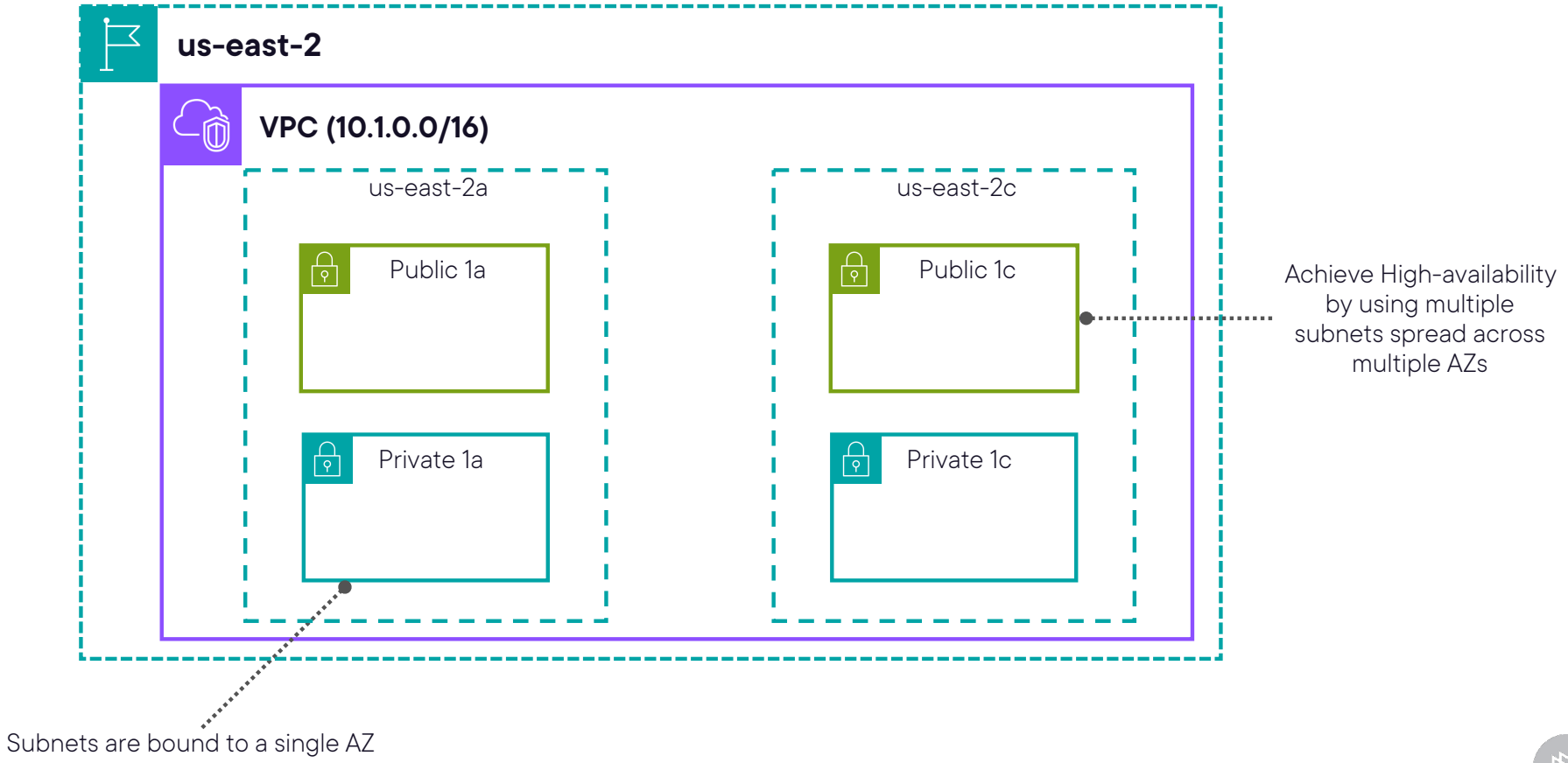
Have a direct route to the Internet via an Internet Gateway. Requires publicly resolvable IP addresses.



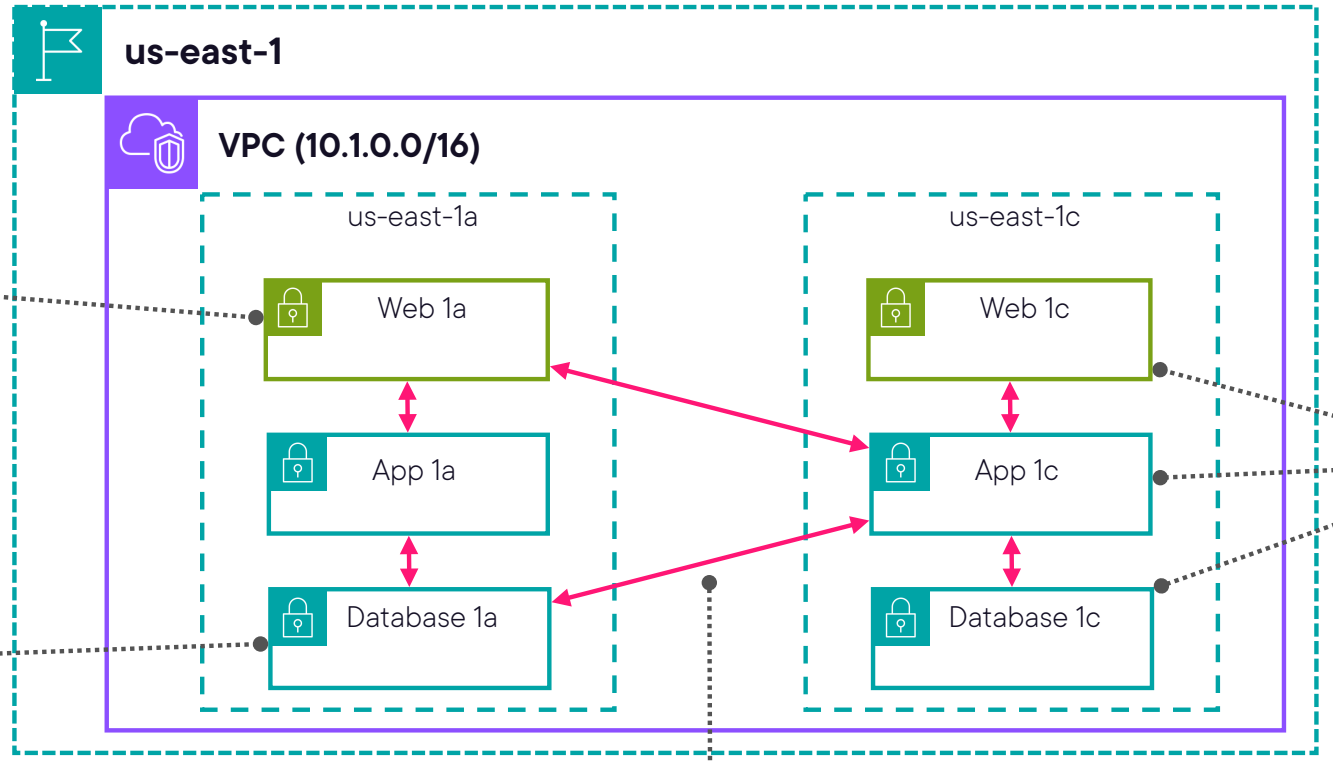
Private Subnets

Do NOT have a direct route to the internet. Require a NAT device to access the Internet. Private IP addresses.

VPC Subnets Architecture Diagram



VPC Subnets Architecture Multi-tier Diagram



A "**tier**" in a VPC represents a logically isolated section of your network

Having multiple tiers allows you to design a more secure network by using a "**security in layers**" approach

You can restrict the layers that are able to communicate with each other

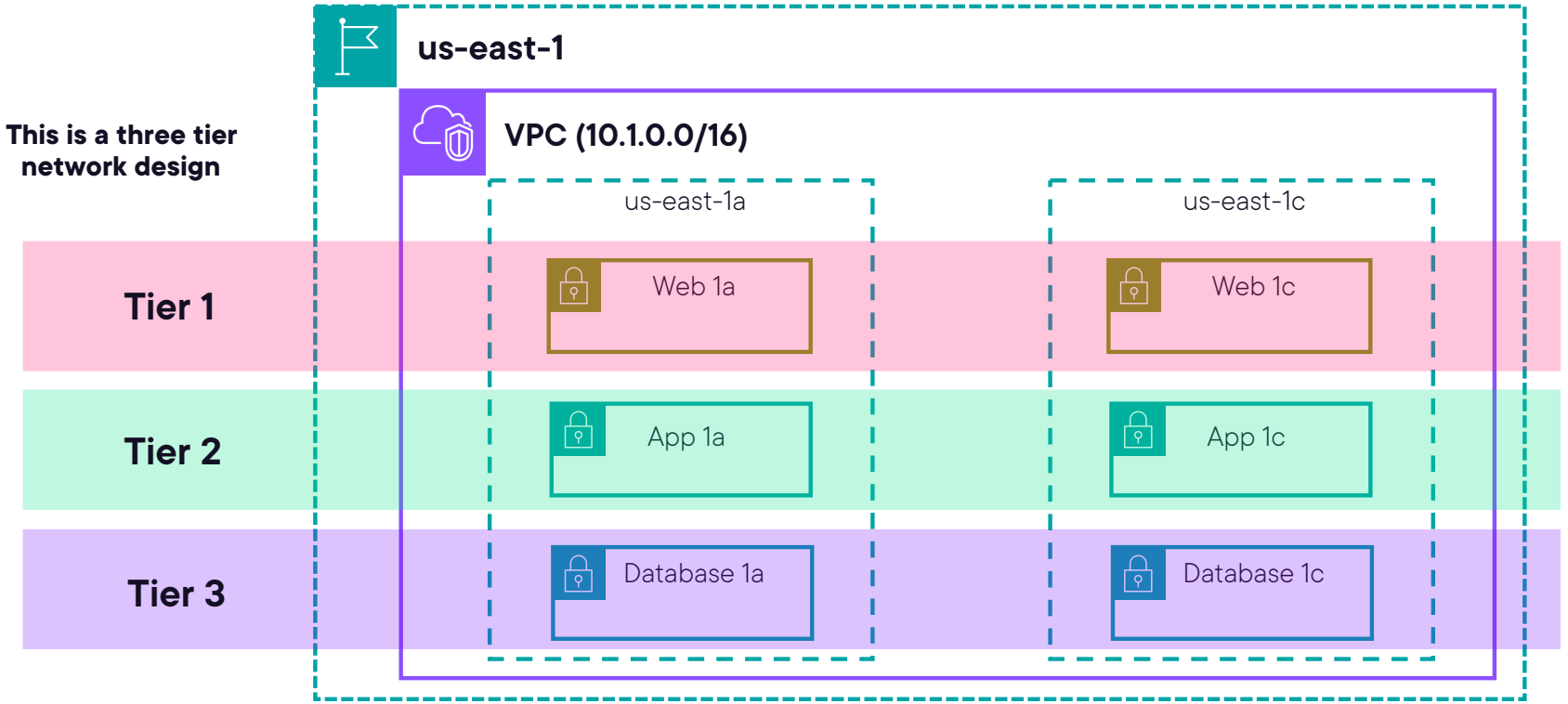
Multi-tiered VPC designs are a best practice that you should follow

Multi-tiered means 2 or more layers of subnets

The most common design is to have Web, App, and Database tiers

Subnets can communicate across AZs automatically, but beware, there is a **cost** associated with cross-AZ traffic

VPC Subnets Architecture Multi-tier Diagram



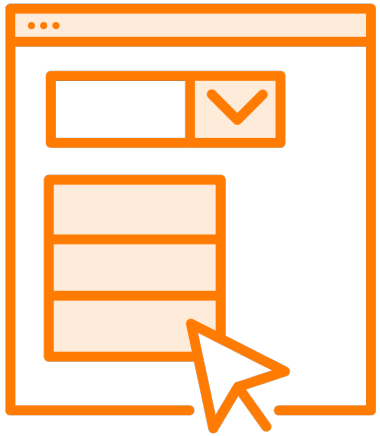
VPC Route Tables

Route Tables contains rules, aka routes, that tell your network traffic where to go

Route Table Types

Main Route Table

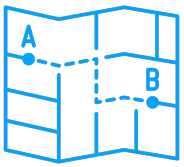
Automatically comes with your VPC and acts as the default table for any leftover, unassociated subnets



Custom Route Table

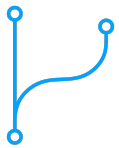
Route table that you fully define and associate with subnets

Custom Route Tables Concepts and Terms



Destination: Range of IP Address (CIDR) where you want to direct your traffic towards (*192.168.0.0/24*)

Target: The different gateway, network interfaces, or other connections where the destination traffic should go (*Internet Gateway*)

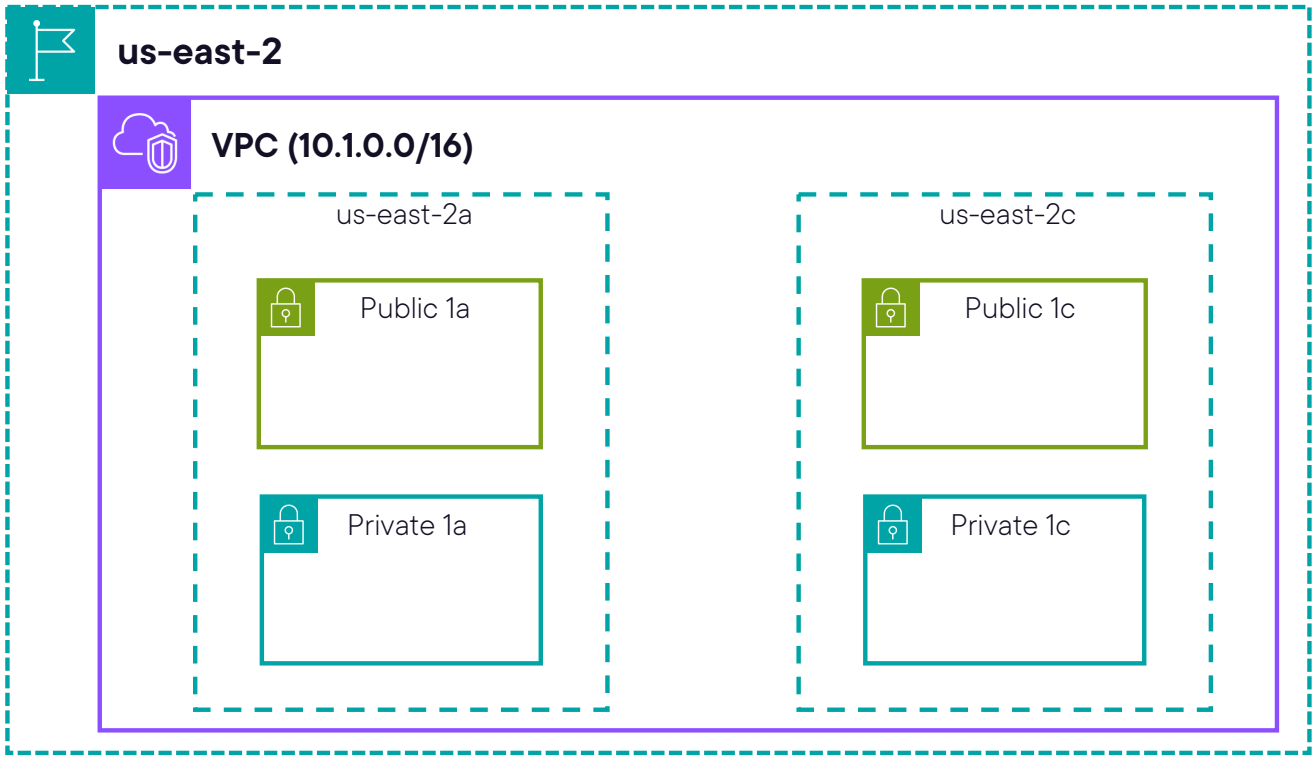


Local Route: Every route table has a local route applied for any VPC-bound traffic

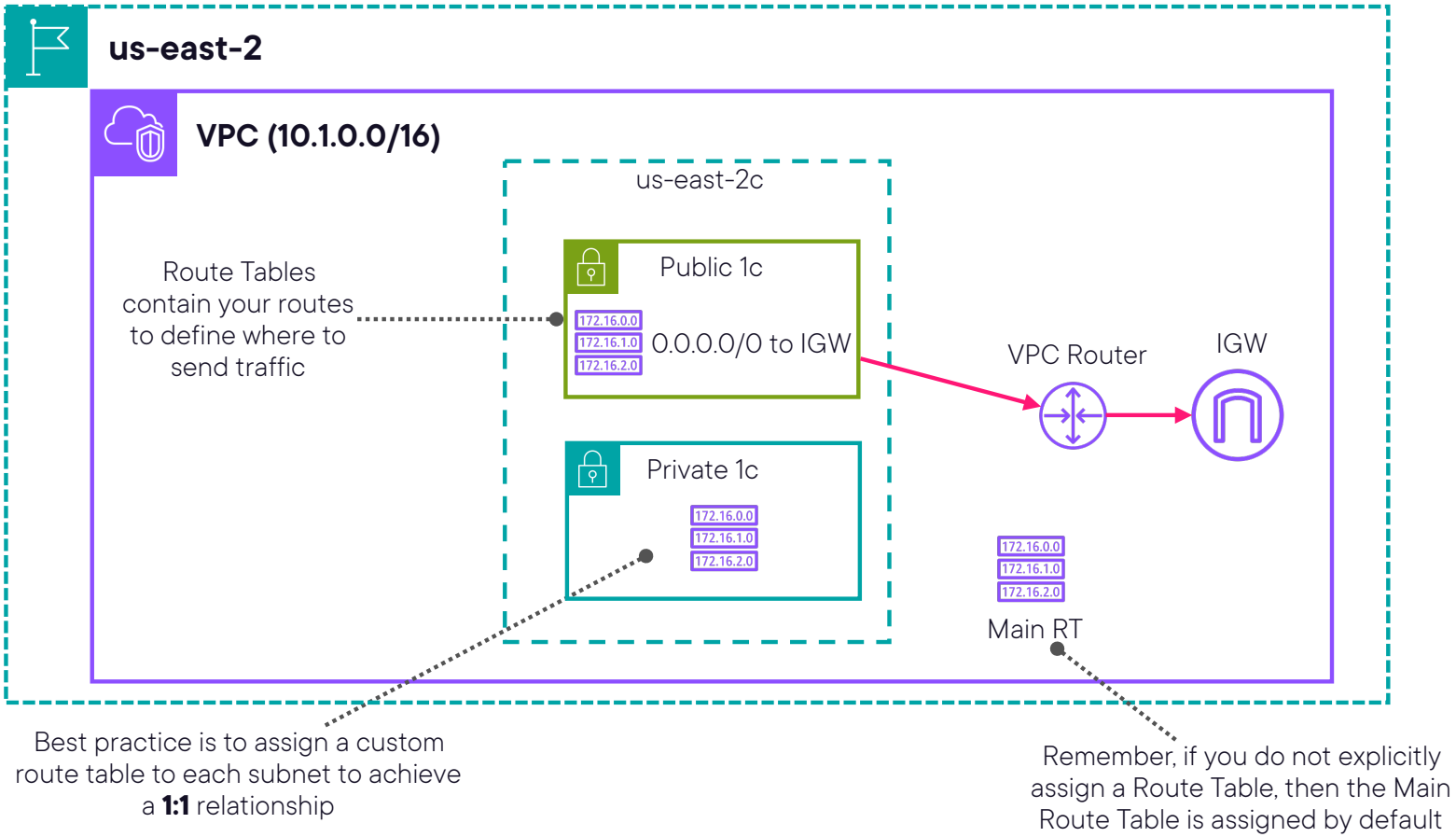
Association: You associate subnets with a route table to apply the chosen rules for any network traffic in the subnet

Generally, it is best practice to have a 1:1 relationship for subnets and route tables

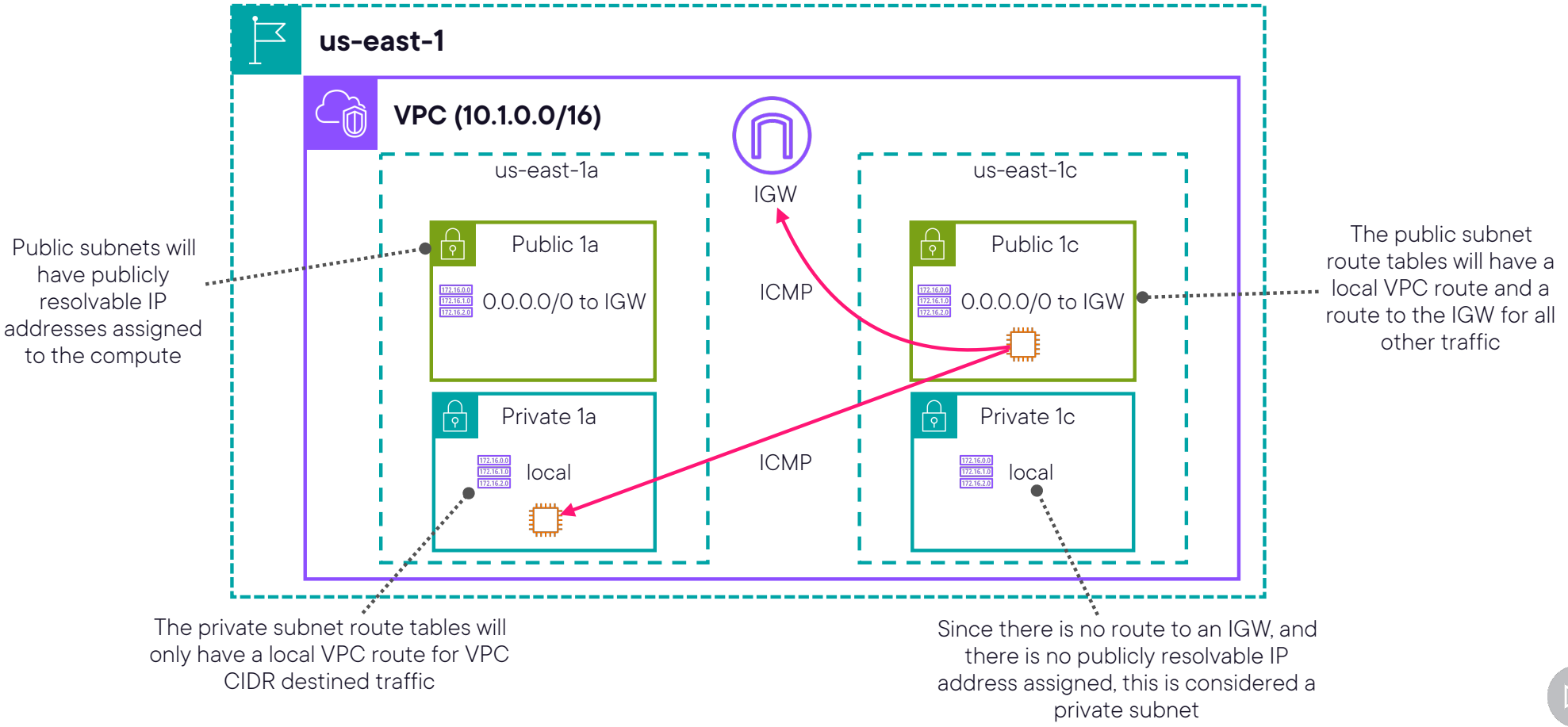
VPC Route Tables Architecture Diagram



VPC Route Tables Architecture Diagram



Demo: VPC Route Tables and Subnets



Network Access Control Lists (NACLs)

Network ACL

...allows or denies specific inbound or outbound traffic at the subnet level

Citation: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html

Network ACLs

Essentially a stateless firewall to control traffic at the subnet level

Stateless: Must explicitly define both inbound and outbound traffic rules

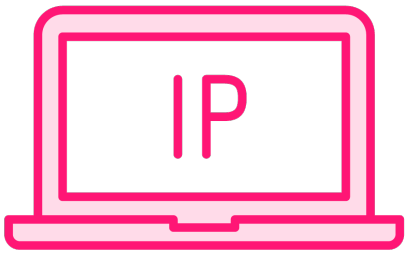
Assign one NACL per subnet, with a Default NACL in place if needed

Newly created NACLs will deny all traffic by default

List of ascending numbered, prioritized rules where the first match wins

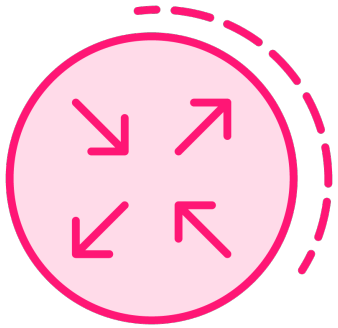
Traffic NACLs Don't Work With

Amazon Domain Name Services (DNS)



Amazon Dynamic Host Configuration Protocol (DHCP)

Amazon EC2 instance metadata

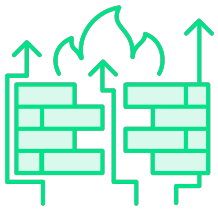


Reserved IP addresses used by the default VPC router

Information to Know: Ephemeral Ports

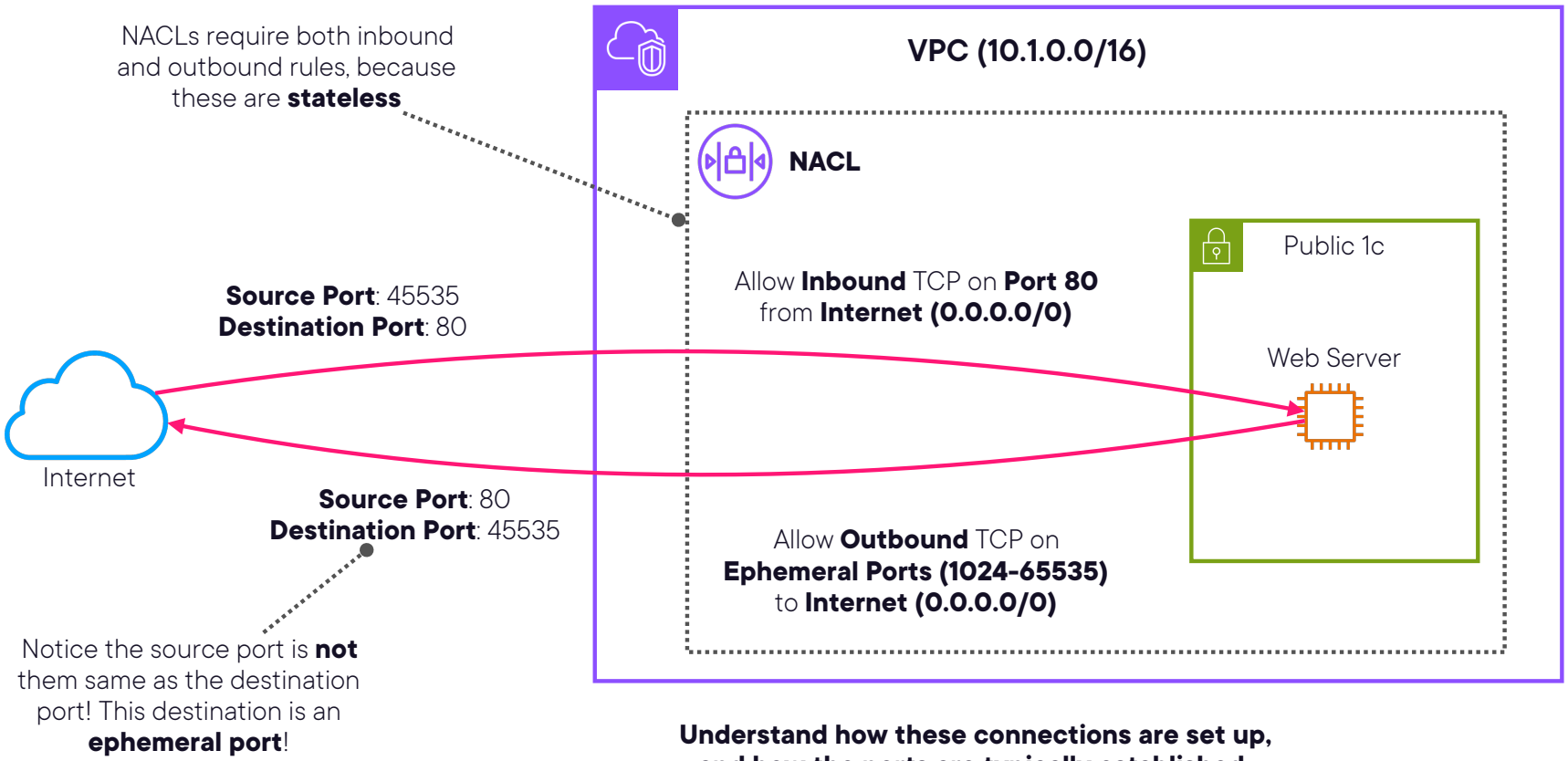
Short-lived transport protocol ports that operating systems allocate for client-side transmissions when they connect to a server

Ephemeral port ranges vary by operating system



Example: Inbound HTTP connections use port 80, but the outbound connection will be on a port between 1024-65535

NACLs and Ephemeral Ports Architecture Diagram



Understand how these connections are set up, and how the ports are typically established.

This is a popular exam scenario!

Also, please remember NACLs are stateless and applied at the subnet level!

Security Groups

Security Group

...controls the traffic that is allowed to reach and leave the resources that it is associated with

Citation: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-security-groups.html

Security Groups

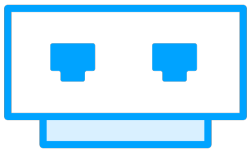
Stateful virtual firewalls attached at the EC2 and network Interface level

Only define allowed traffic, no deny rules are ever created!

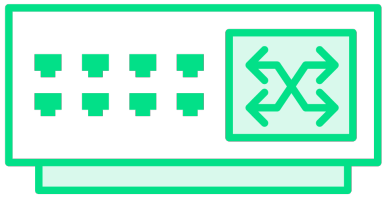
All rules get evaluated before logic is applied. Most restrictive match wins.

Implicit deny is in place for anything not explicitly allowed.

Security Group Components



Protocol
Which protocol are you allowing? TCP, UDP, ICMP?

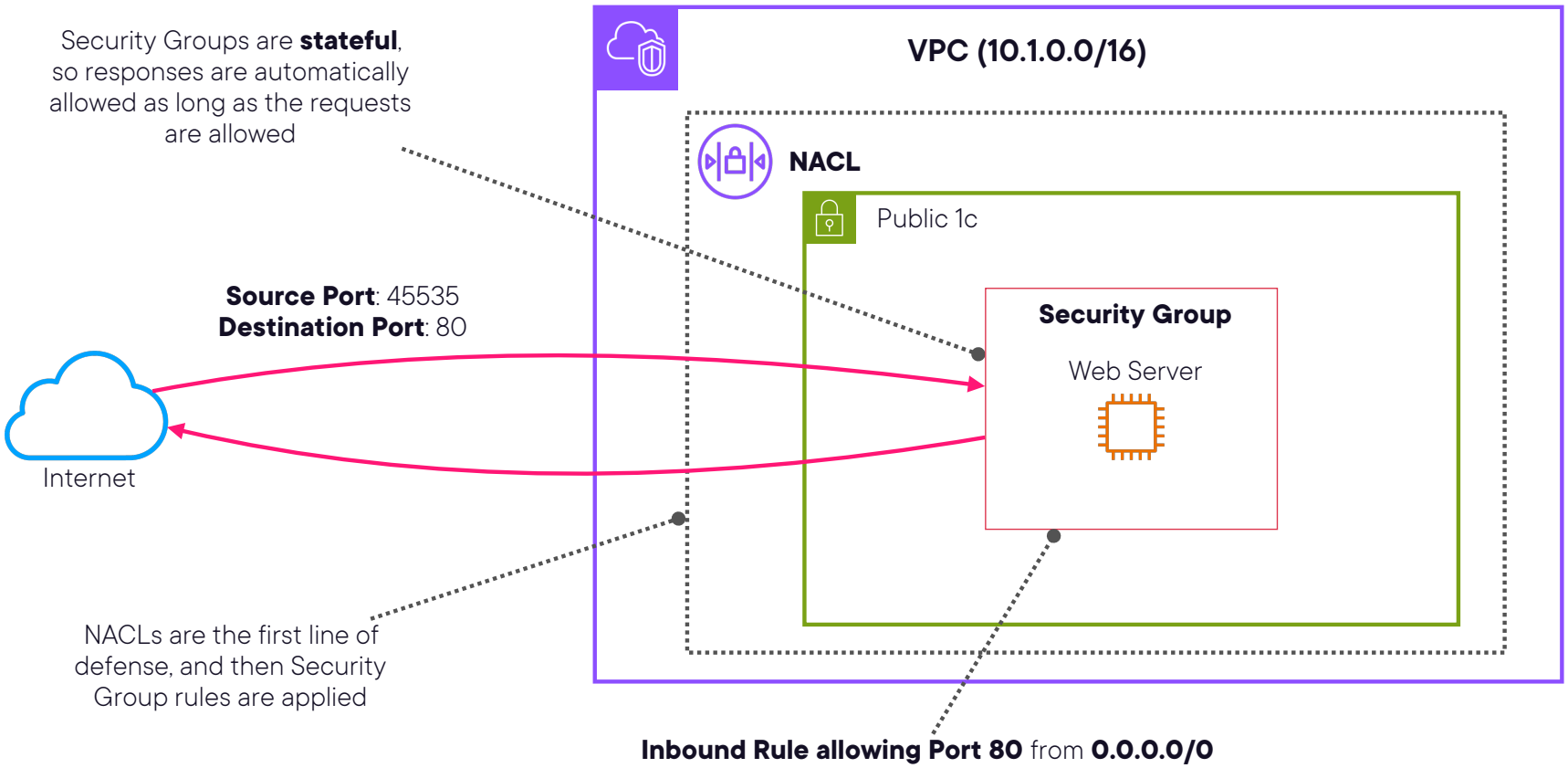


Port Range
What port or ports are you allowing? 22, 443, 1024-6535?

Source or Destination
Which source or destination IP ranges are you allowing in or out?

Pro Exam Tip: You can reference other Security Groups IDs within your Security Group rules

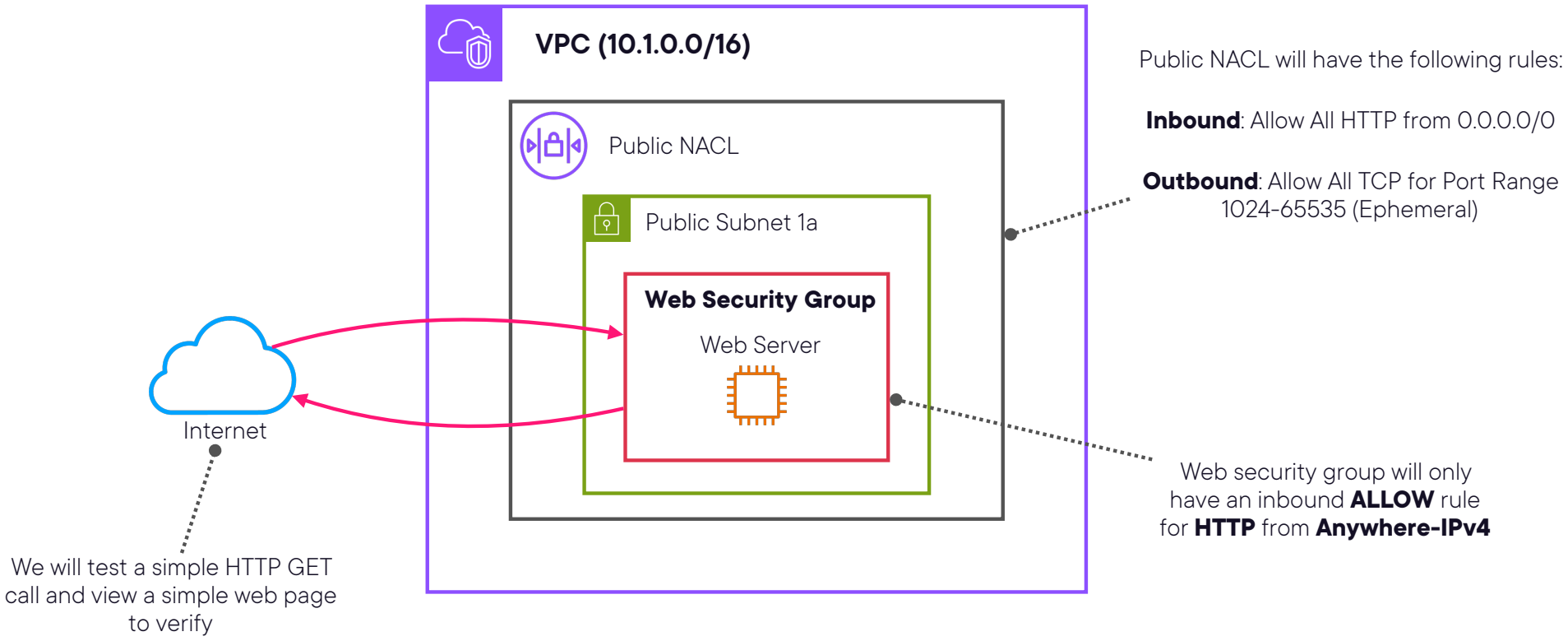
Security Groups Architecture Diagram



If an incoming request is allowed, then the outgoing response is automatically allowed.

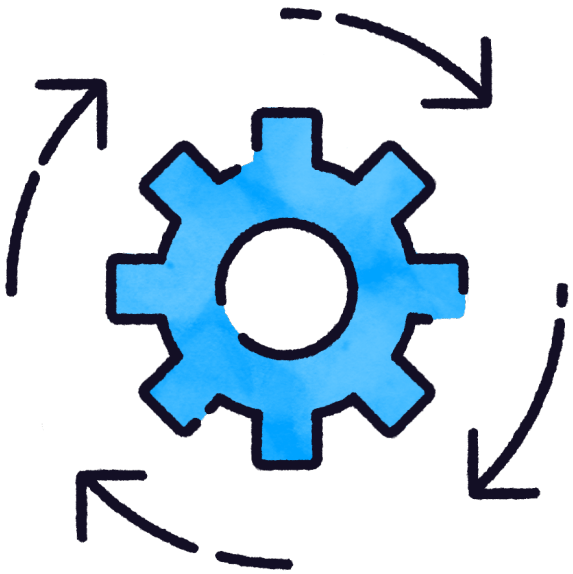
If an outgoing request is allowed, then the incoming response is automatically allowed.

Demo: Creating NACLs and Security Groups



DHCP Option Sets

What Are DHCP Option Sets?



A DHCP option set is a group of network settings used by resources in your VPC

These allow you to control the following aspects of the network configuration in your VPC:

- DNS servers
- Domain names
- NTP servers
- Whether you want DNS resolution turned on or off in the VPC

You can associate a DHCP option set with multiple VPCs!

However, each VPC can have only one associated DHCP option set!

DHCP Option Set Concepts

Each AWS Region has a default DHCP option set

Each VPC uses the default DHCP option set for its Region unless you specify otherwise

You can create and associate a custom DHCP option set with the VPC, or use no DHCP option set

You cannot modify a DHCP option set once it is created!

Exam scenario: If you need to modify DHCP option set configurations, you have to create a new one with the updated settings and associate it with the VPC!

Module Summary and Exam Tips

Subnets and Route Tables

Subnets	VS.	Route Tables
Range of reserved IP space in a VPC		Set of rules on how to route traffic
Deployed within one Availability Zone		Longest prefix match wins
Support IPv4, IPv6, and Dual stack		Each VPC has a Main Route Table
Remember Public v. Private		Primarily set Destination and Target
Have exactly one route table assigned		Can associate with many subnets

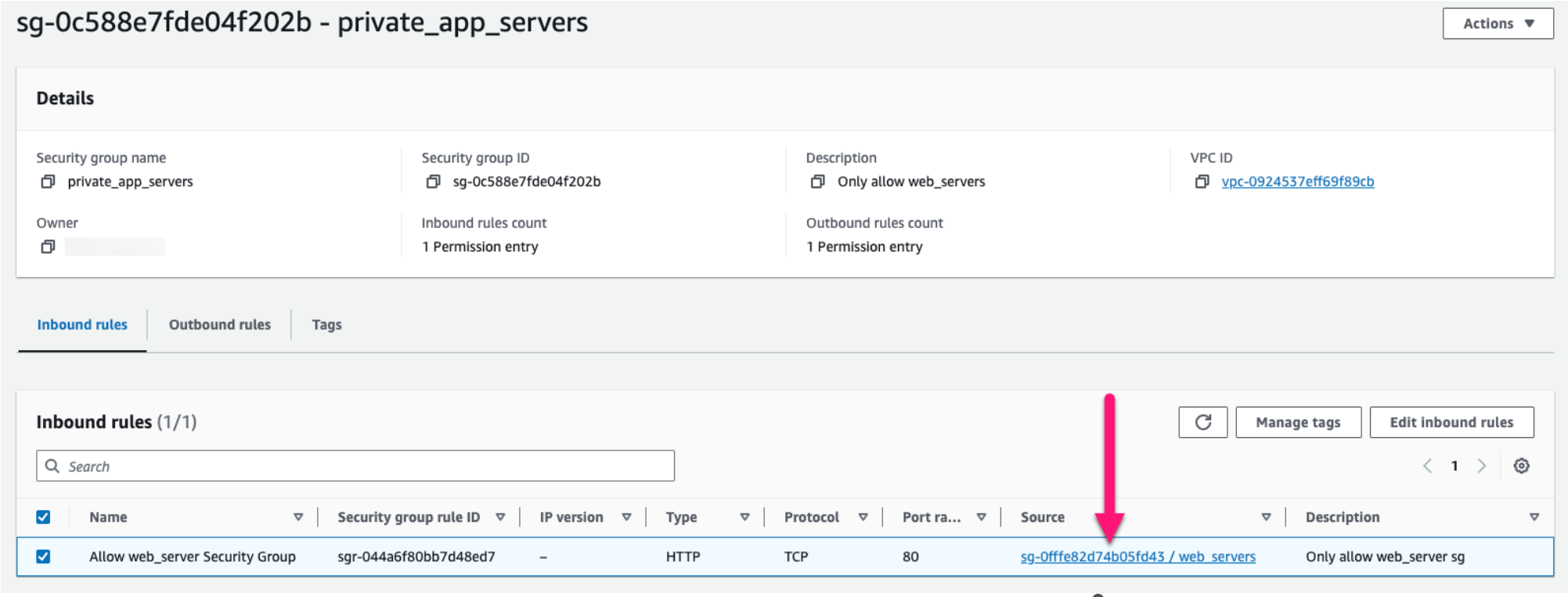
Remember that AWS reserves 5 IP addresses per subnet CIDR block!

Security Groups and Network ACLs

Security Groups	VS.	Network ACLs
Stateful firewall		Stateless firewall
Assigned at the ENI/EC2 level		Assigned at the subnet level
Only create allow rules, no deny		Specify both inbound and outbound rules, separately
Specify source, port range, and protocol for each rule		First match in the rule list wins
Capable of aggregating rules from multiple security groups at once		Can only assign one to a single subnet at a time

You can reference Security Groups IDs within your Security Group rules in place of IP ranges.

Security Group References



Referencing an existing security group

You cannot modify a DHCP Option Set once it is created!