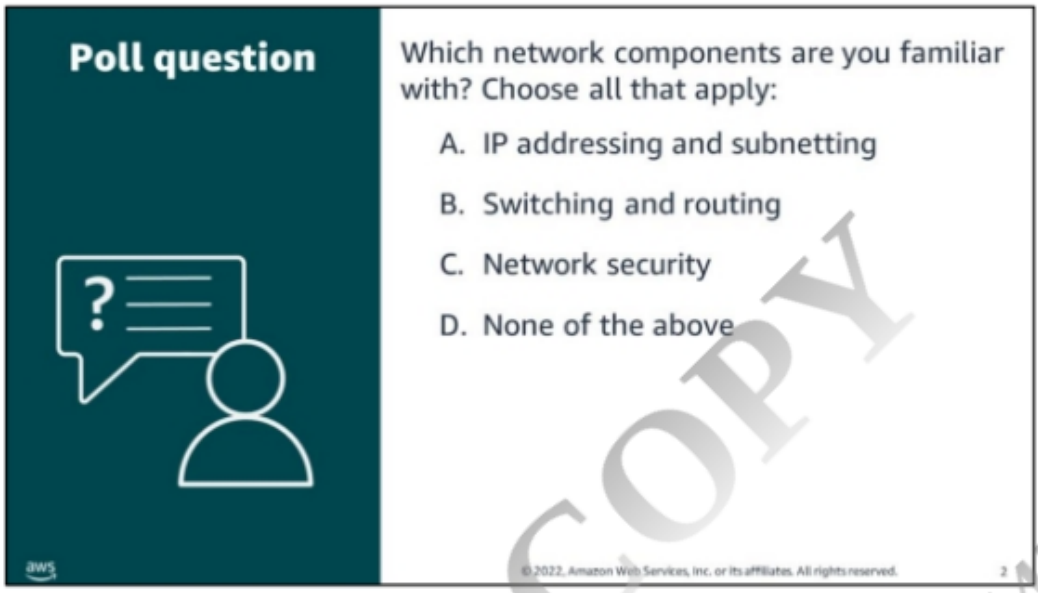
Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

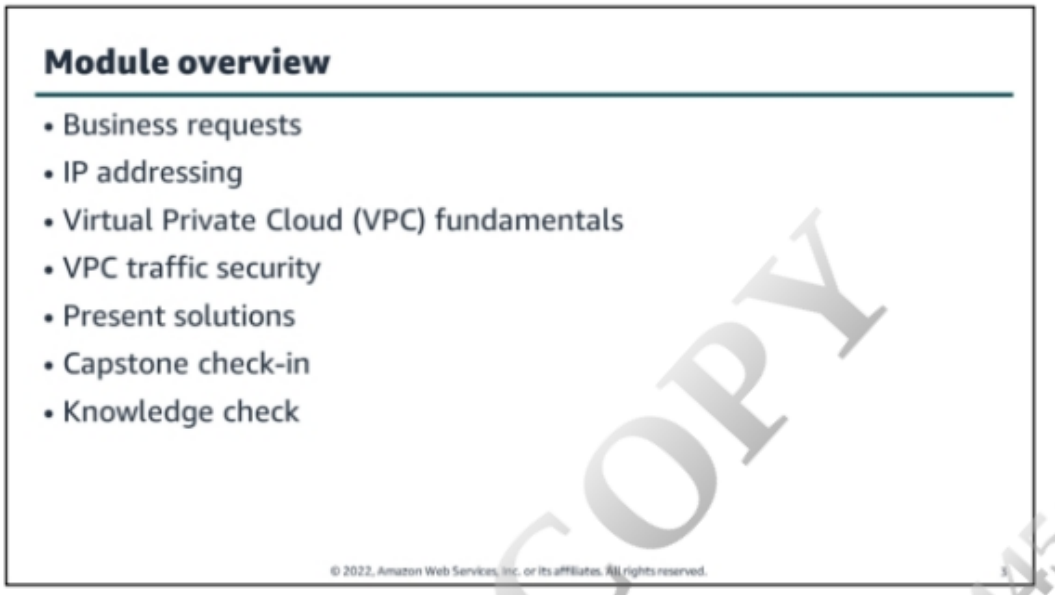
Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

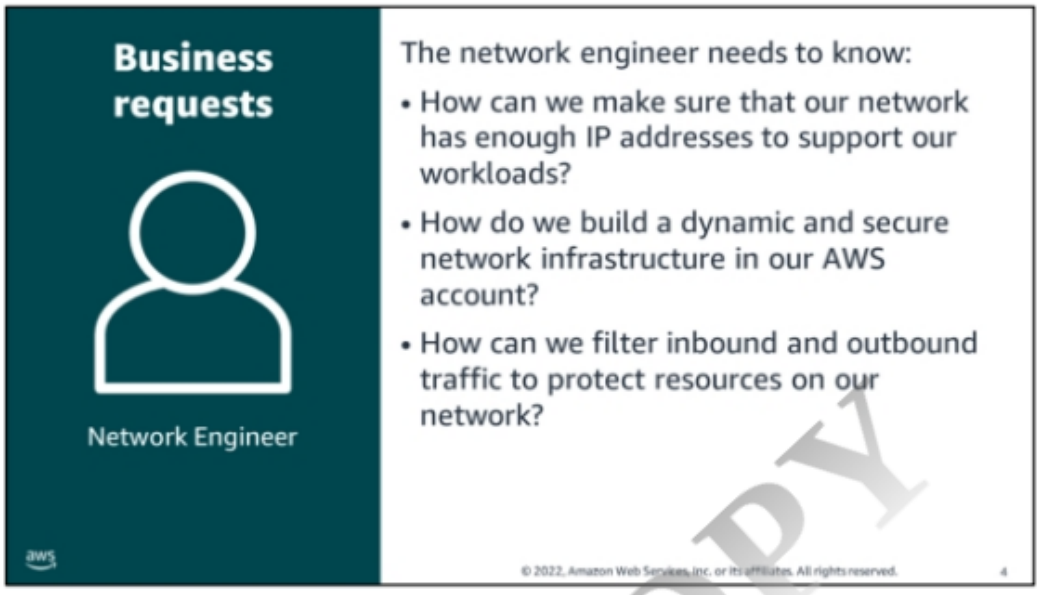
Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



Imagine your network engineer meets with you to discuss how to build networking infrastructure in the cloud. Here are some questions they are asking.

At the end of this module, you meet with the network engineer and present some solutions.

DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

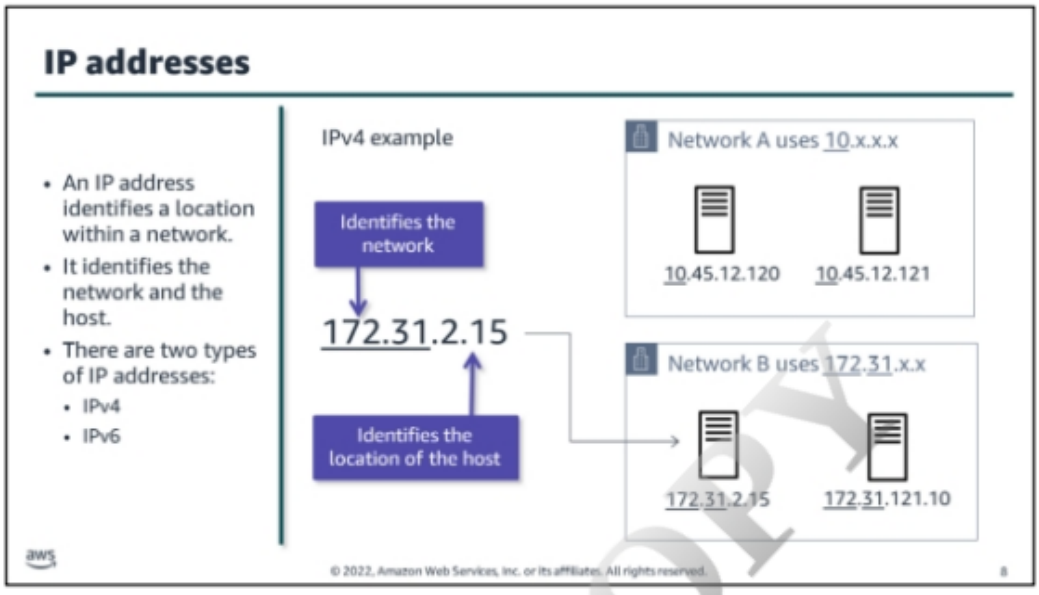
The network engineer asks, "How can we make sure that our network has enough IP addresses to support our workloads?"

The engineer and their team need to start planning to build a network. They would like you to explain how to define IP addresses ranges on AWS.

DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



An IP address includes information about the location of a resource within a network. One part of the address identifies the network, and another part identifies the host.

This example shows a sample IPv4 address of 172.31.2.15. Each of the four numbers separated by dots is called an octet. The destination network, network B, uses the first two octets to identify the network and the last two to identify the host. Network A, however, only uses the first octet to identify the network and the other three to identify the host.

There are two IP address types:

IPv4 addresses
IPv4 was developed in the early 1980s and uses 32-bit addresses. The bits are grouped into four sets of 8 bits called octets. Addresses in IPv4 are written using numeric dot-decimal notation. IPv4 addresses can create **4.3 billion addresses.**

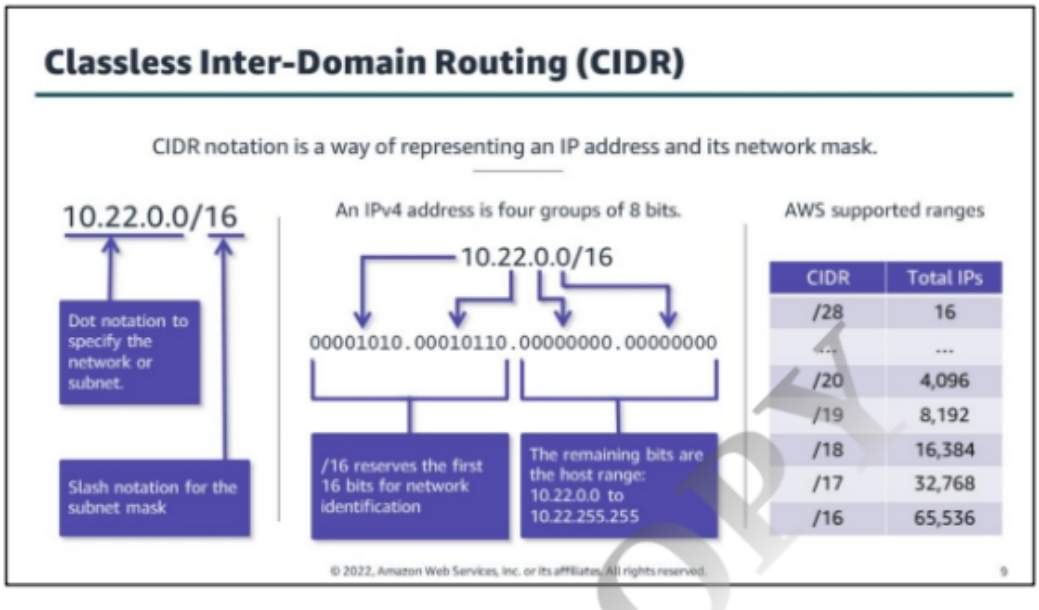
IPv6 addresses
IPv6 was developed in 1998 to replace IPv4. IPv6 uses 128-bit addresses. IPv6 addresses are eight groups of four hexadecimal digits for a total of 16 octets. The groups are written with a colon as a separator. A full IPv6 address is often expressed in a shortened form; for example, 50b2:6400:0000:0000:0000:6c3a:b17d:0:10a9 can be written as 50b2:6400::6c3a:b17d:0:10a9. The addresses allow for **340 trillion trillion trillion addresses**. IPv6 supports automatic configuration. Global unicast address (GUA) is a unique IPv6 address assigned to a host interface.

Note: You cannot remove IPv4 support from your VPC.

DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



CIDR notation defines an IP address range for a network or a subnet. This range is referred to as a CIDR block. When building your network in AWS using VPC components, you specify CIDR blocks for your VPC and subnets. You must allocate enough IP addresses to support the resources on your network. Your VPC can have up to five CIDR blocks, and their address ranges cannot overlap.

A CIDR block identifies the network using dot notation. It specifies the subnet mask using slash notation. The subnet mask defines which portion of the IP address is dedicated to network identification and which can be used for host IP addresses. For example, an IPv4 address has 32 bits divided into four octets. A subnet mask of /16 reserves the first 16 bits, or two octets, for network identification. The remaining 16 bits are used for host identification.

Each octet can have a number between 0 and 255, which creates a range of 65,536 addresses. Some of the addresses are reserved by the network and are not usable, one address for the network and four addresses for other reasons discussed later.

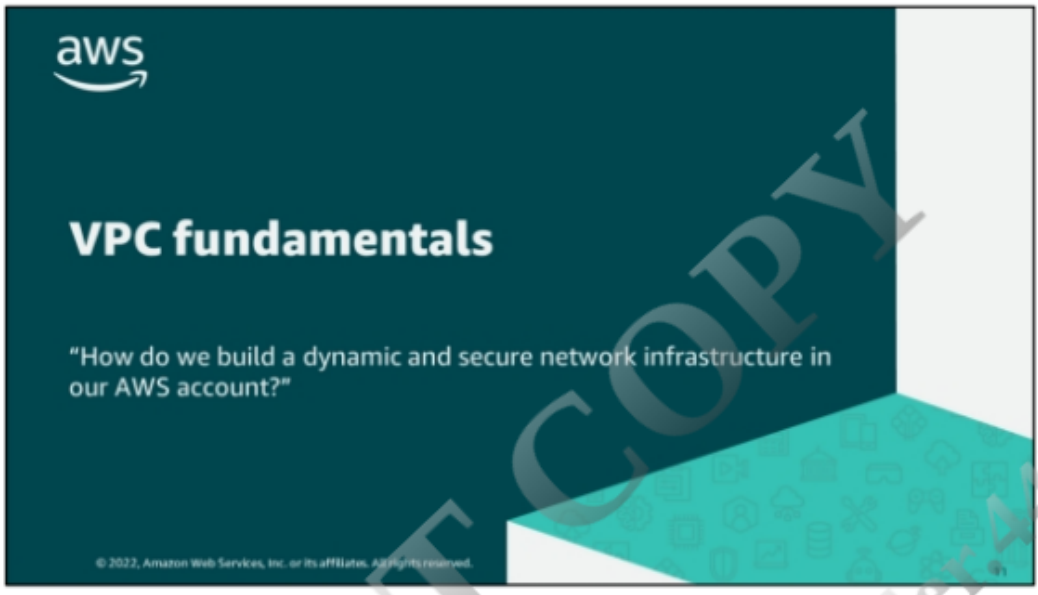
You can assign block sizes between /28 (16 IP addresses) and /16 (65,536 IP addresses) for IPv4 subnets. The size of the IPv6 CIDR block for IPv6-only subnets has a fixed prefix length of /64.

Amazon VPC supports IPv4 and IPv6 addressing and it has different CIDR block size limits for each. By default, all VPCs must have IPv4 CIDR blocks—you can't change this behavior. You can optionally associate an IPv6 CIDR block with a dual-stack VPC.

DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



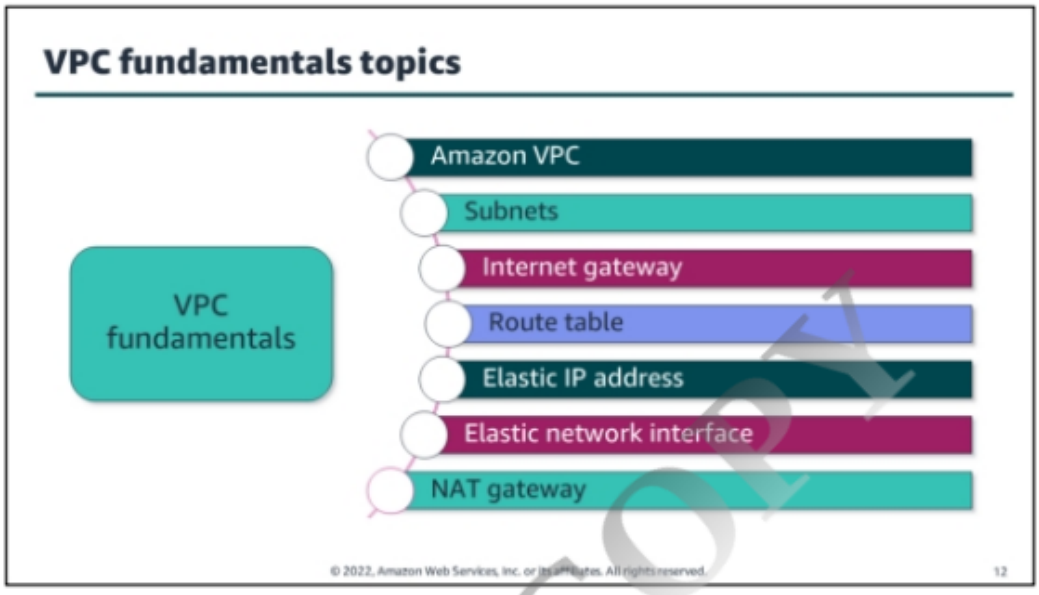
The network engineer asks, "How do we build a dynamic and secure network infrastructure in our AWS account?"

The network engineer needs to identify the elements that build an elastic, secure virtual network that includes private, public, and protected subnets. They would like you to explain the common networking components on AWS and how they work together.

DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

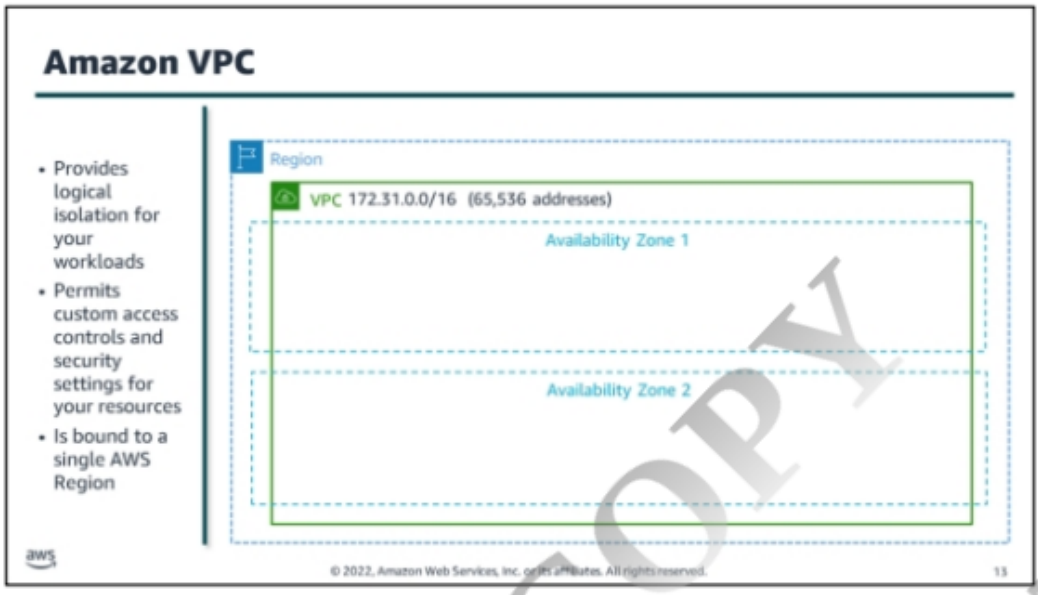
Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



Amazon Virtual Private Cloud (Amazon VPC) is your network environment in the cloud. With Amazon VPC, you can launch AWS resources into a virtual network that you have defined. VPCs deploy into one of the AWS Regions and can host resources from any Availability Zone within its Region.

Amazon VPC is designed to provide greater control over the isolation of your environments and their resources. With Amazon VPC, you can:

- Select your own IP address range
- Create subnets
- Configure route tables and network gateways

This VPC uses a CIDR block of 172.31.0.0/16, which provides a range of 65,536 addresses.

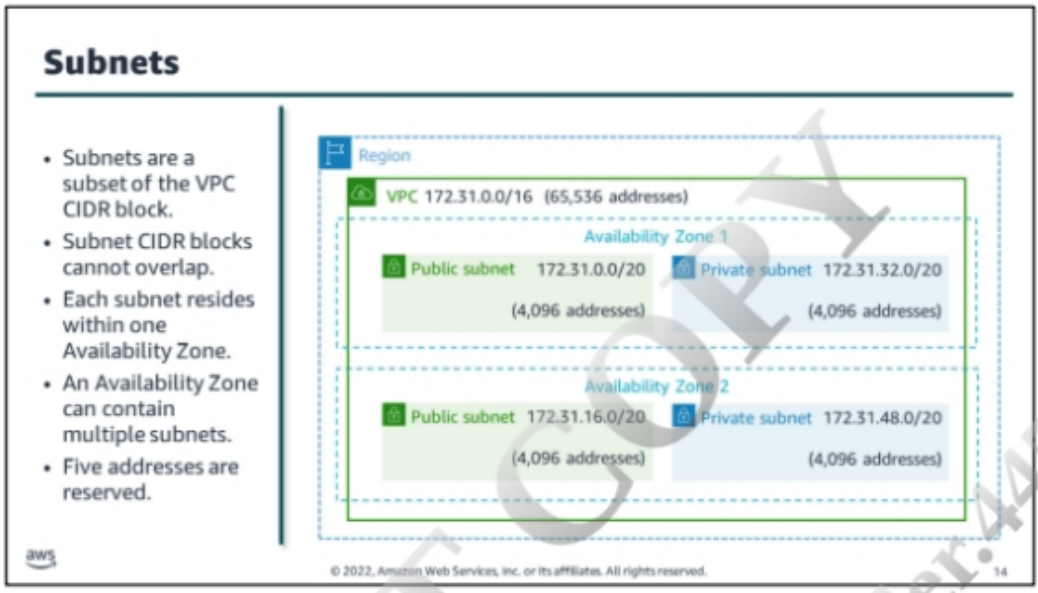
You can use both IPv4 and IPv6 in your VPC for secure and easy access to resources and applications. A VPC is a virtual network dedicated to your AWS account.

For more information about Amazon VPC, see "What is Amazon VPC?" in the *Amazon Virtual Private Cloud User Guide* (https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html).

DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



A subnet is a range of IP addresses in your VPC. You can launch AWS resources into a specified subnet. Use a public subnet for resources that must be connected to the internet and a private subnet for resources that won't be connected to the internet. A subnet resides within one Availability Zone.

In this example, the VPC CIDR block 172.31.0.0/16 allows a total of 65,536 IP addresses. These are divided between its four subnets as follows:

- Public subnet 1: 172.31.0.0/20 allows 4,096 addresses between 172.31.0.1 – 172.31.15.254
- Public subnet 2: 172.31.16.0/20 allows 4,096 addresses between 172.31.16.1 – 172.31.31.254
- Private subnet 1: 172.31.0.0/20 allows 4,096 addresses between 172.31.32.1 – 172.31.47.254
- Private subnet 2: 172.31.0.0/20 allows 4,096 addresses between 172.31.48.1 – 172.31.63.254

These subnets do not use all of the available addresses in the VPC. You can use these extra addresses to support future growth.

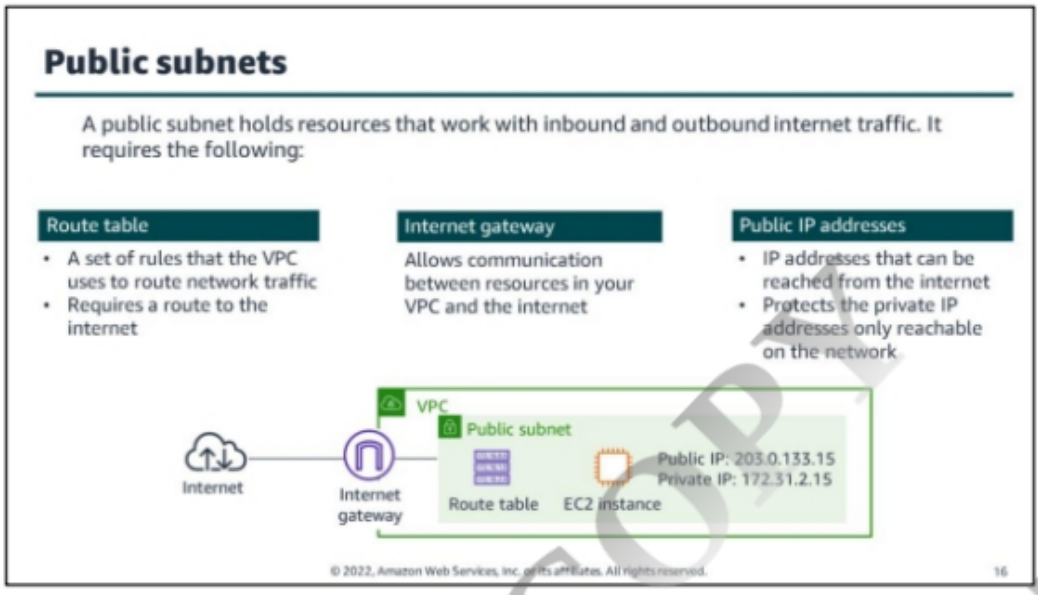
The first four IP addresses and the last IP address in each subnet CIDR block are not available and cannot be assigned to an instance. For example, in a subnet with CIDR block 10.0.0.0/24, the following five IP addresses are reserved:

- **10.0.0.0:** Network address.
- **10.0.0.1:** Reserved by AWS for the VPC router.
- **10.0.0.2:** Reserved by AWS. The IP address of the DNS server is always the base of the VPC network range plus 2.
- **10.0.0.3:** Reserved by AWS for future use.
- **10.0.0.255:** Network broadcast address. We do not support broadcast in a VPC; therefore, we reserve this address.

Consider larger subnets over smaller ones (/24 and larger). You are less likely to waste or run out of IPs if you distribute your workload into larger subnets.

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



Your public subnet configuration acts as a two-way door—allowing traffic to flow in either direction, invited or not invited. Since there is no automatic outbound routing, you must configure a subnet to be public.

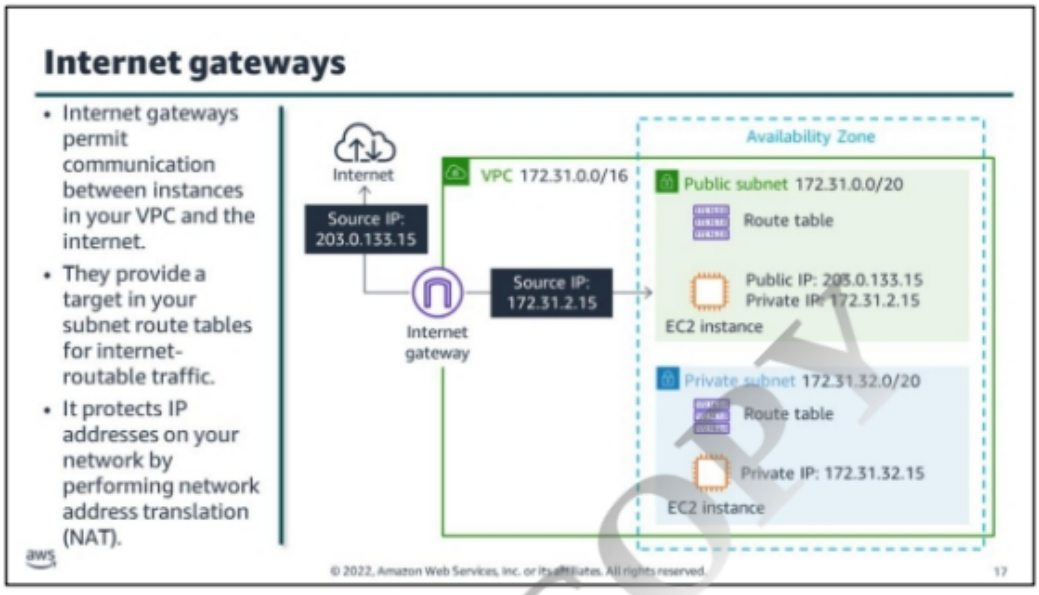
A public subnet requires the following:

- Internet gateway: The internet gateway allows communication between resources in your VPC and the internet.
- Route table: A route table contains a set of rules (routes) that are used to determine where network traffic is directed. It can direct traffic to the internet gateway.
- Public IP addresses: These are addresses that are accessible from the internet. Public IP addresses obscure the private IP addresses, which are only reachable within the network.

DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



An internet gateway is a horizontally scaled, redundant, and highly available VPC component that permits communication between instances in your VPC and the internet. It imposes no availability risks or bandwidth constraints on your network traffic.

An internet gateway serves two purposes:

1. **It provides a target in your route table for internet-routable traffic.**
2. **It protects IP addresses on your network by performing network address translation (NAT).**

Provides a target in your route table for internet-routable traffic

A subnet does not allow outbound traffic by default. Your VPC uses route tables to determine where to route traffic. To allow your VPC to route internet traffic, you create an outbound route in your route table with an internet gateway as a target, or destination.

Protects IP addresses on your network by performing network address translation (NAT)

Resources on your network that connect to the internet should use two kinds of IP addresses:

- **Private IP**: Use private IPs for communication within your private network. These addresses are not reachable over the internet.
- **Public IP**: Use public IP addresses for communication between resources in your VPC and the internet. A public IP address is reachable over the internet.

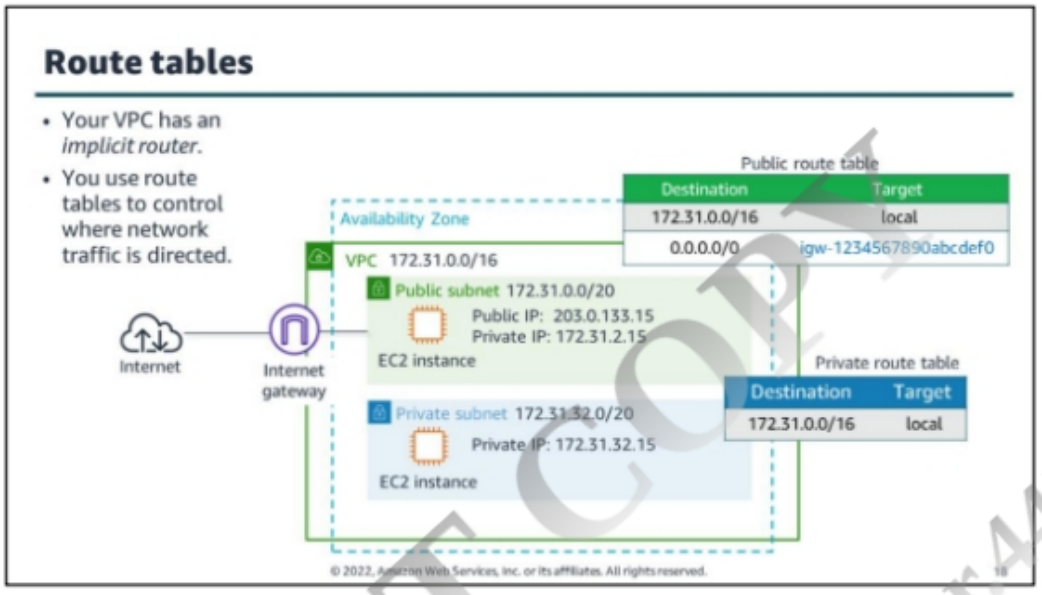
An internet gateway performs NAT by mapping a public and private IP address. In this example, the internet gateway translates the source IP of a request from the private IP used on the network (172.31.2.15) to the public IP address (203.0.133.15). The recipient directs its response to the public IP address. The internet gateway receives the response and translates the public IP to the matching private IP address. The VPC routes the response to the requester.

An internet gateway supports IPv4 and IPv6 traffic.

For more information, see "Connect to the internet using an internet gateway" in the *Amazon Virtual Private Cloud User Guide* (https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html).

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



A route table contains a set of rules (routes) that the VPC uses to determine where to direct network traffic. When you create a VPC, it automatically has a main route table. Initially, the main route table (and every route table in a VPC) contains only a single route. This is a local route that permits communication for all the resources within the VPC. You can't modify the local route in a route table. Whenever you launch an instance in the VPC, the local route automatically covers that instance. You can create additional custom route tables for your VPC.

Each subnet in your VPC must be associated with a route table. If you don't explicitly associate a subnet with a particular route table, the subnet is implicitly associated with and uses the main route table. A subnet can be associated with only one route table at a time, but you can associate multiple subnets with the same route table. Use custom route tables for each subnet to permit granular routing for destinations.

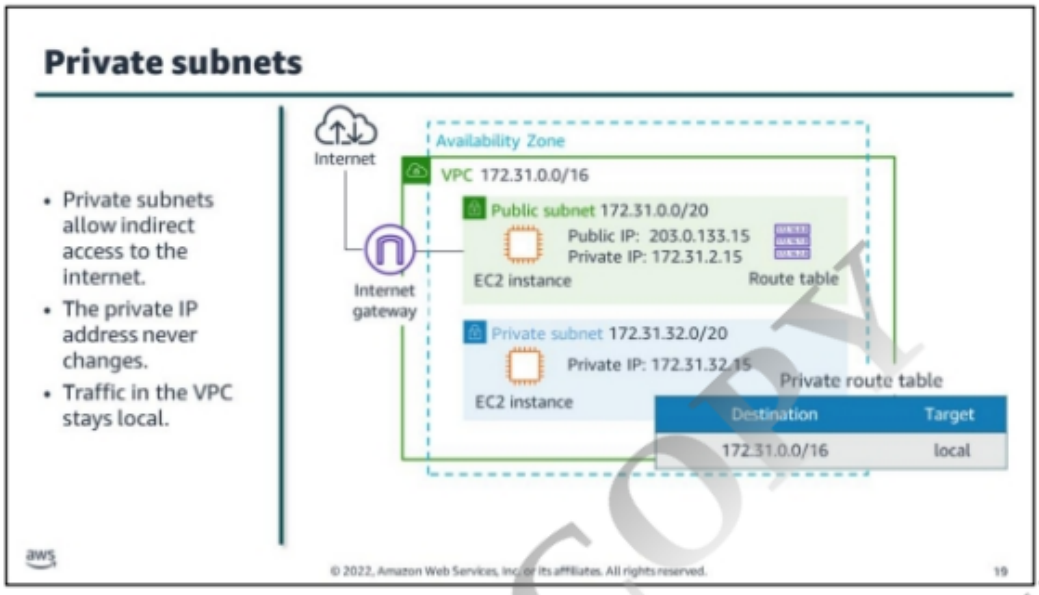
In this example, both route tables direct network traffic locally, but the public route table includes routes to the internet gateway.

For more information, see "Configure route tables" in the *Amazon Virtual Private Cloud User Guide* (https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html).

DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



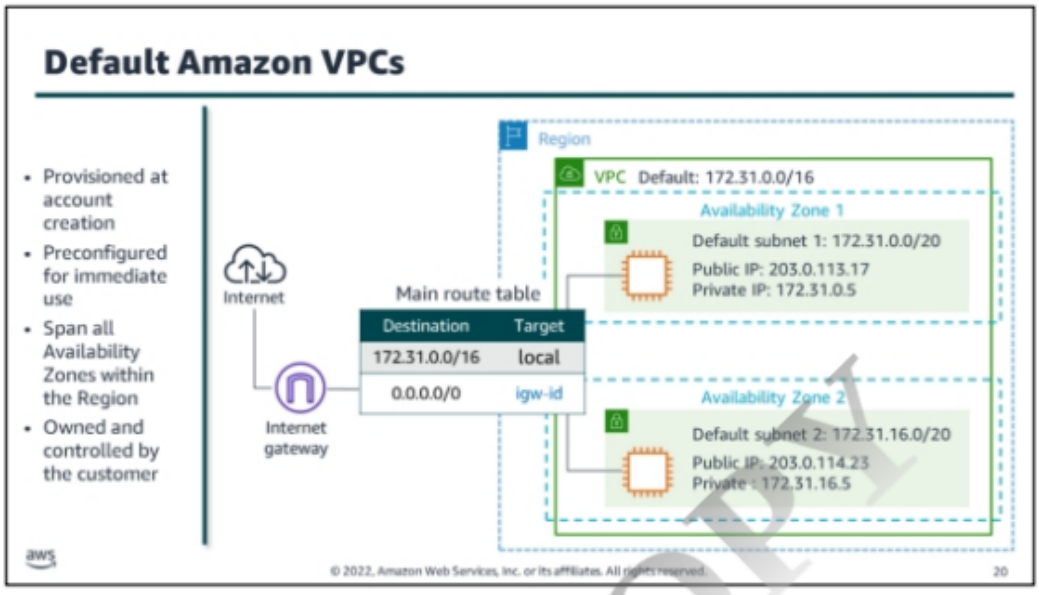
Private subnets allow indirect access to the internet. Traffic stays within your private network. A private IP address assigned to an EC2 instance will never change unless you manually assign a new IP address on the network interface of the EC2 instance.

While you can put web-tier instances into a public subnet, we recommend that you put web-tier instances inside private subnets behind a load balancer placed in a public subnet. Elastic Load Balancing is discussed later in this course.

DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



Each AWS account comes with a default Amazon VPC that is preconfigured for you to use immediately. The default Amazon VPC is suitable for getting started quickly and for launching public instances, such as a blog or simple website.

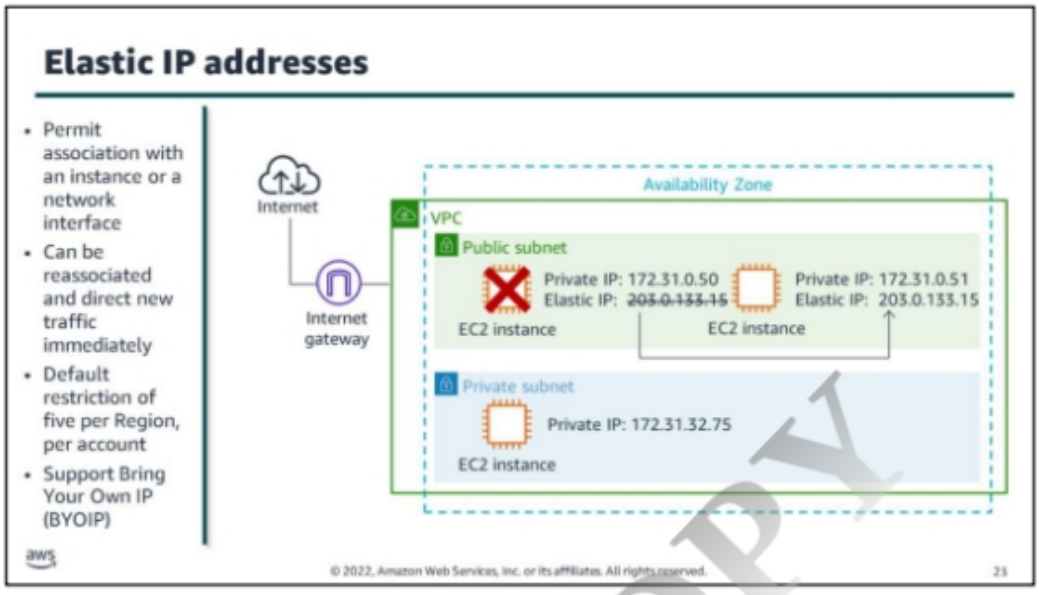
This diagram is a default Amazon VPC. The CIDR block for the default VPC is always a /16 subnet mask. In this example, the CIDR block of 172.31.0.0/16 means that this VPC can provide up to 65,536 IP addresses. It includes one public subnet in each Availability Zone in the Region. These subnets use a /20 subnet mask, providing 4,096 addresses per subnet. It also includes an internet gateway. The VPC uses a main route table to connect the subnets to the internet gateway.

For more information about how to modify the IPv4 address range, see "How do I modify the IPv4 address range of my Amazon VPC?" (https://aws.amazon.com/premiumsupport/knowledge-center/vpc-ip-address-range/).

DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



An Elastic IP address is a static, public IPv4 address designed for dynamic cloud computing. You can associate an Elastic IP address with any instance or network interface for any VPC in your account. With an Elastic IP address, you can mask the failure of an instance by rapidly remapping the address to another instance in your VPC.

In this example, an EC2 instance using an Elastic IP address of 203.0.133.15 fails. This Elastic IP address is assigned to a new EC2 instance.

You can move an Elastic IP address from one instance to another. The instance can be in the same VPC or another VPC. An Elastic IP address is accessed through the internet gateway of a VPC. If you have set up a VPN connection between your VPC and your network, the VPN traffic traverses a virtual private gateway, not an internet gateway, and therefore cannot access the Elastic IP address.

You are limited to five Elastic IP addresses. To help conserve them, you can use a NAT device. We strongly encourage you to use an Elastic IP address primarily for the ability to remap the address to another instance in the case of instance failure, and to use DNS hostnames for all other inter-node communication.

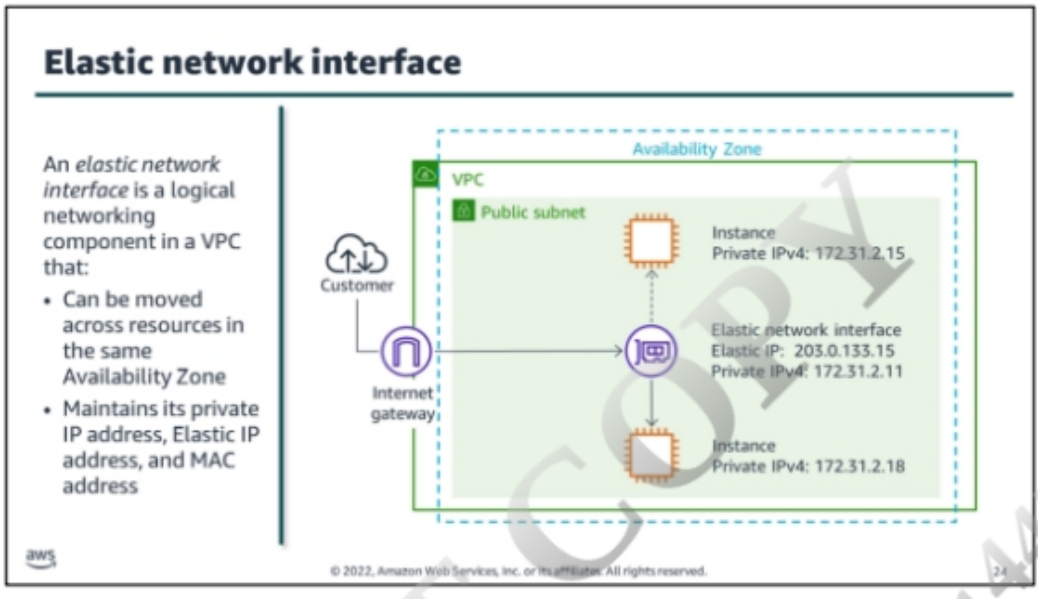
You can create Bring Your Own IP (BYOIP) addresses, but it requires significant additional configuration.

**For Accessibility: VPC in a single AZ with a public and private subnet. Customers connect to the VPC through an internet gateway. The private subnet has one EC2 instance with a private IP of 172.31.128.75. The public subnet has two EC2 instances. The one with a private IP of 172.31.0.50 fails. The second, with a private IP of 172.31.32.51, is still running. The Elastic IP address is reassigned from the failed instance to the running instance. End Description

DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



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

For Amazon Elastic Compute Cloud (Amazon EC2), you can create a network interface, attach it to an instance, detach it from an instance, and attach it to another instance. When moved to a new instance, the network interface maintains its public and Elastic IP address, private IP and Elastic IP address, and MAC address. The attributes of a network interface follow it.

When you move a network interface from one instance to another, network traffic is redirected to the new instance. Each instance in a VPC has a default network interface (the primary network interface).

Each instance is assigned a private IP address from the IP address range of your VPC. You cannot detach a primary network interface from an instance. You can create and attach additional network interfaces. Attaching multiple network interfaces to an instance is useful when you want to do the following:

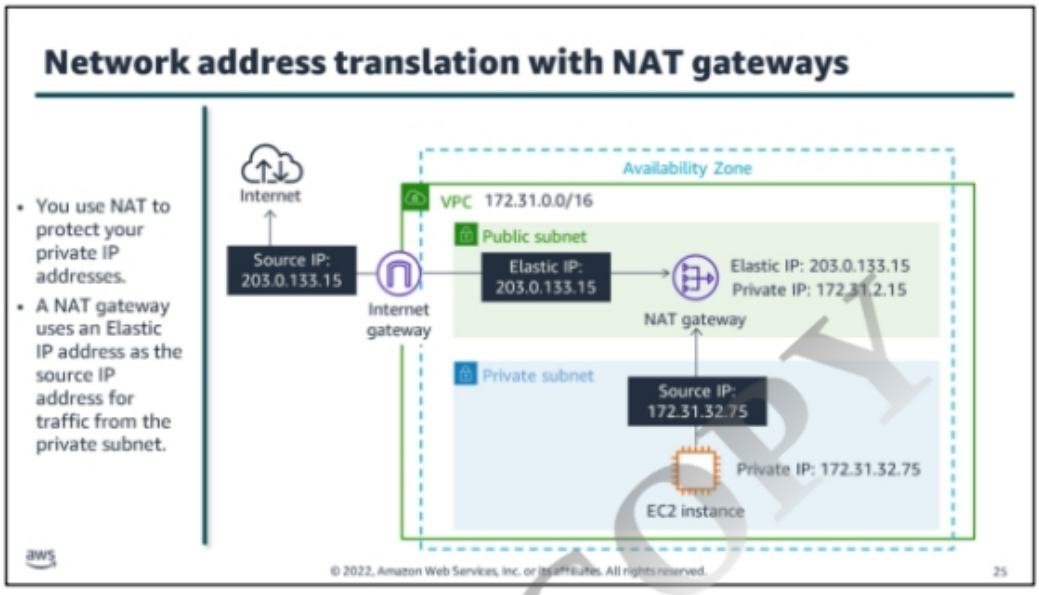
- Create a management network.
- Use network and security appliances in your VPC.
- Create dual-homed instances with workloads or roles on distinct subnets.
- Create a low-budget, high-availability solution.

You can attach a network interface in one subnet to an instance in another subnet in the same VPC. However, both the network interface and the instance must reside in the same Availability Zone. This limits its use for disaster recovery (DR) scenarios, where you would want to redirect traffic to another Availability Zone.

**For Accessibility: A VPC in one Availability Zone with a public subnet containing two EC2 instances and an elastic network interface. Customers connect to the VPC through an internet gateway. Traffic routes to an elastic network interface with a private IP address of 172.31.2.11 and an Elastic IP address of 203.0.133.15 . You attach the elastic network interface to an EC2 instance with a private IP address of 172.31.2.15. The interface can be reassigned to a second EC2 instance with a private IP address of 172.31.2.18. End Description.

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



NAT maps one IP address to another in a message. You use NAT for IP address conservation. Because NAT maps private IP addresses to a public IP address, you can use it to allow private IP networks to connect to the internet. A single device, such as a router, can act as an agent between the internet (public network) and a local network (private network).

NAT gateways communicate between instances in your VPC and the internet. They are horizontally scaled, redundant, and highly available by default. NAT gateways provide a target in your subnet route tables for internet-routable traffic.

- Instances in the private subnet can initiate outbound traffic to the internet or other AWS services.
- NAT gateways managed by AWS prevent private instances from receiving inbound traffic from the internet.

You can put NAT gateways in both public and private subnets. If you need more control over your NAT gateway, you can install one on an EC2 instance to create a NAT instance.

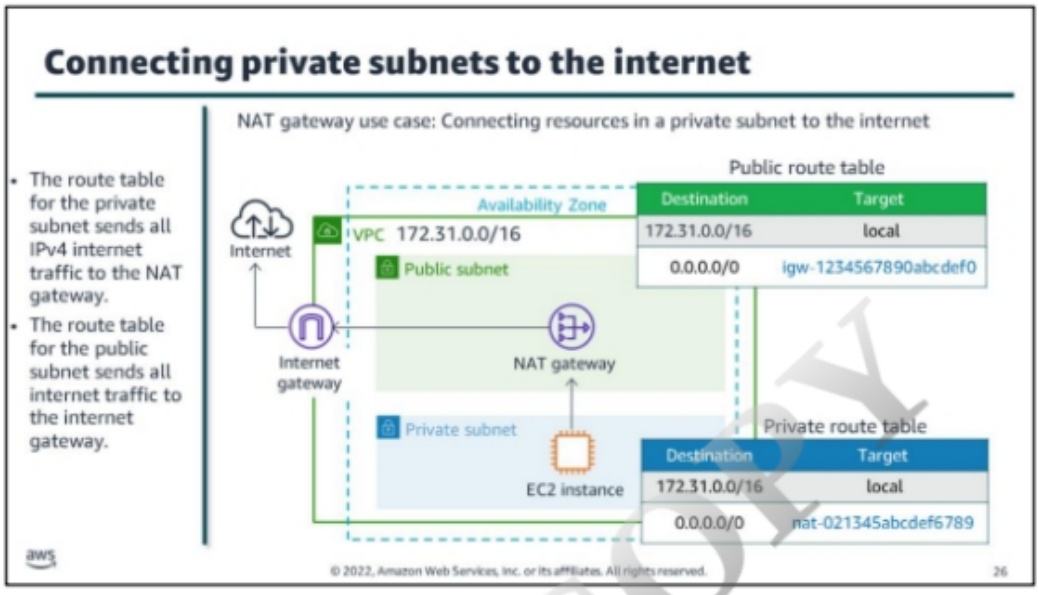
You can also use a private NAT gateway to enable communication between networks even if they have overlapping CIDR ranges.

**For Accessibility: A VPC in a single Availability Zone with an internet gateway, a public subnet, and a private subnet. The VPC uses a CIDR of 172.31.0.0/16. The public subnet contains a NAT gateway with an Elastic IP address of 203.0.133.15. The private subnet contains an EC2 instance with a private IP address of 172.31.128.75. Outbound traffic to the internet from the private subnet flows to the NAT gateway. The NAT gateway translates the source address to 203.0.133.15 to obscure the private instance's private IP address and then sends the traffic to the internet gateway. End Description

DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



You can use a NAT gateway for a one-way connection between private subnet instances and the internet or other AWS services. This type of connection prevents external traffic from connecting with your private instances.

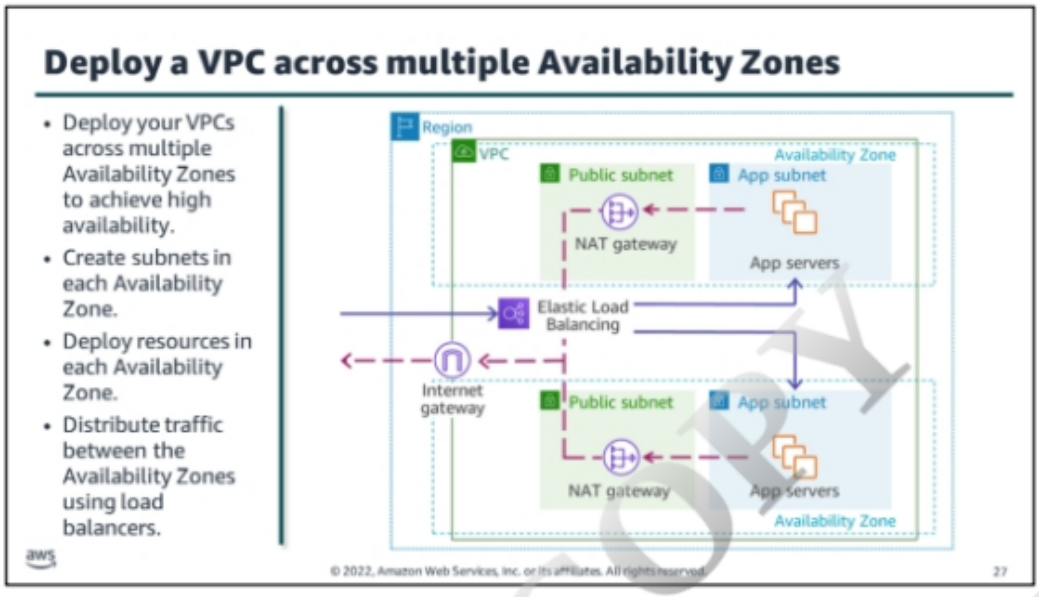
- The route table for the private subnet sends all IPv4 internet traffic to the NAT gateway.
- The NAT gateway uses its Elastic IP address as the source IP address for traffic from the private subnet.
- The route table for the public subnet sends all internet traffic to the internet gateway. This is not supported for IPv6.

**For Accessibility: A VPC in a single Availability Zone with an internet gateway, a public subnet, and a private subnet. The VPC uses a CIDR of 172.31.0.0/16. The public subnet contains a NAT gateway. The private subnet contains an EC2 instance. A private route table sets the target for internet traffic in the private subnet to the NAT gateway in the public subnet. The public route table in the public subnet sets the target for internet traffic to the internet gateway. End Description

DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



Deploying a VPC across multiple Availability Zones creates an architecture that achieves high availability by distributing traffic while provide data security. If you have an outage in one Availability Zone, you can fail over to the other.

In this diagram of a VPC spanning two Availability Zones, the backend servers are in two private subnets in the two separate Availability Zones. They send outbound traffic to NAT gateways in public subnets located in their Availability Zone. Backend traffic from both NAT gateways route to an internet gateway.

Elastic Load Balancing receives inbound traffic and routes it to the application servers in the private subnets of both Availability Zones.

DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

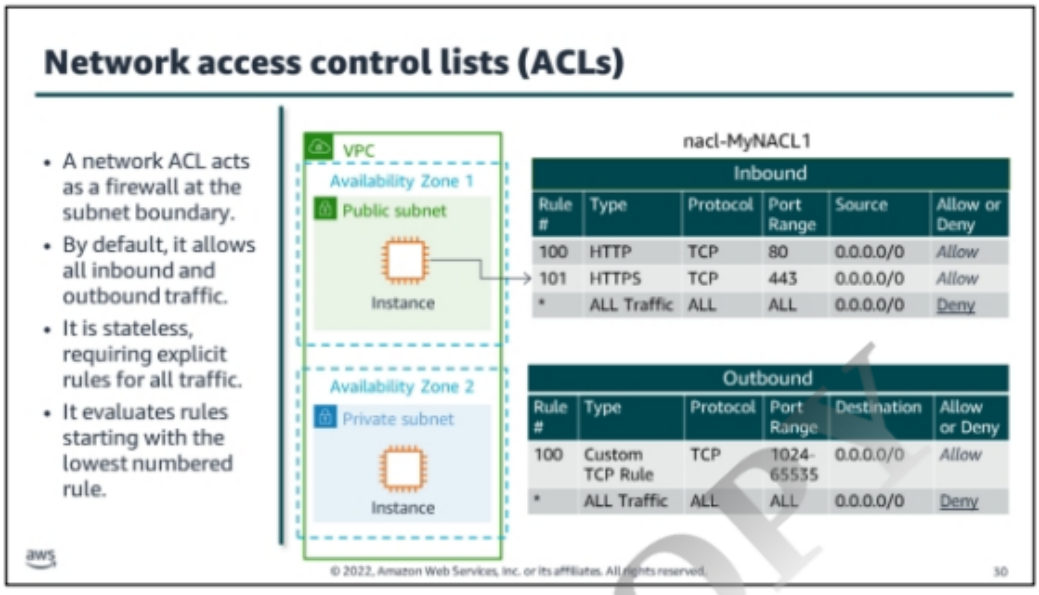
The network engineer asks, "How can we filter inbound and outbound traffic to protect resources on our network?"

The team needs information to determine strategies for a layered security approach to VPC subnets. They want your advice for how to best control traffic in and out of your network.

DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



A network ACL is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. Every VPC automatically comes with a default network ACL. It allows all inbound and outbound IPv4 traffic. You can create a custom network ACL and associate it with a subnet. By default, *custom network ACLs* deny all inbound and outbound traffic until you add rules.

A network ACL contains a numbered list of rules, which are evaluated in order, starting with the lowest numbered rule. If a rule matches traffic, the rule is applied even if any higher-numbered rule contradicts it. Each network ACL has a rule whose number is an asterisk. This rule denies a packet doesn't match any of the numbered rules.

Components of a network ACL rule include the following:

- **Rule number** – Rules are evaluated starting with the lowest numbered rule.
- **Type** – The type of traffic, for example, Secure Shell (SSH). You can also specify all traffic or a custom range.
- **Protocol** – You can specify any protocol that has a standard protocol number.
- **Port range** – The listening port or port range for the traffic, for example, 80 for HTTP traffic.
- **Source** – For inbound rules only, the source of the traffic (CIDR range).
- **Destination** – For outbound rules only, the destination for the traffic (CIDR range).
- **Allow or Deny** – Whether to allow or deny the specified traffic.

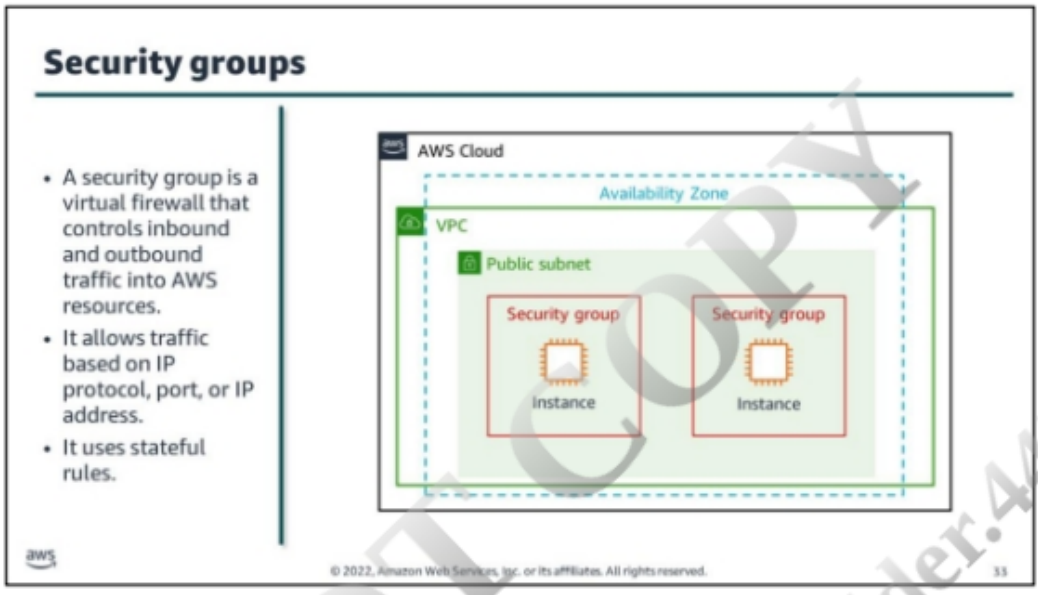
Network ACLs are stateless, which means that responses to allowed inbound traffic are subject to the rules for outbound traffic (and the other way around).

For more information about network ACLs, see "Control traffic to subnets using Network ACLs" in the *Amazon Virtual Private Cloud User Guide* (https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html).

DO NOT COPY 2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



A **security group** acts as a virtual firewall for your instance to control inbound and outbound traffic. Security groups act at the network interface level, not the subnet level, and they support Allow rules only. The default group allows inbound communication from other members of the same group and outbound communication to any destination. Traffic can be restricted by any IP protocol, by service port, and by source or destination IP address (individual IP address or CIDR block).

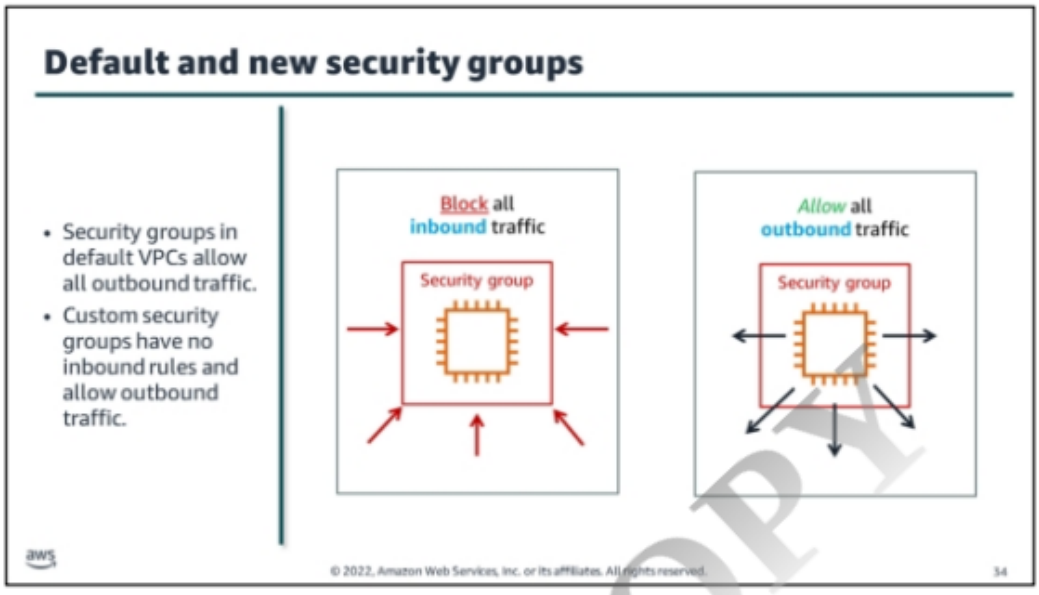
As an example regarding stateful rules, if you initiate an Internet Control Message Protocol (ICMP) ping command to your instance from your home computer and your inbound security group rules allow ICMP traffic, information about the connection (including the port information) is tracked. Response traffic from the instance for the ping command is not tracked as a new request, but as an established connection, and is allowed to flow out of the instance, even if your outbound security group rules restrict outbound ICMP traffic.

Not all flows of traffic are tracked. If a security group rule permits TCP or User Datagram Protocol (UDP) flows for all traffic (0.0.0.0/0) and there is a corresponding rule in the other direction that permits the response traffic, that flow of traffic is not tracked. The response traffic is therefore allowed to flow based on the inbound or outbound rule that permits the response traffic, and not on tracking information.

DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



A security group created with a default VPC includes an outbound rule that allows all outbound traffic. You can remove the rule and add outbound rules that allow specific outbound traffic only. If your security group has no outbound rules, no outbound traffic originating from your instance is allowed. Traffic can be restricted by protocol, by service port, and by source IP address (individual IP address or CIDR block) or security group.

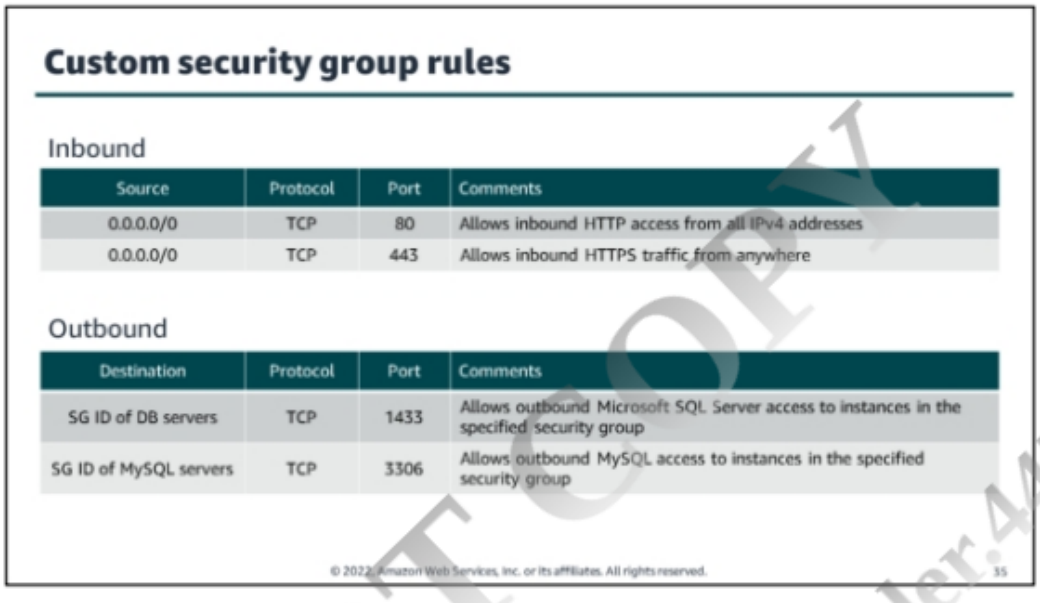
Security groups can be configured to set different rules for different classes of instances. Consider the case of a traditional three-tiered web application. The group for the web servers would have port 80 (HTTP) or port 443 (HTTPS) open to the internet. The group for the application servers would have port 8000 (application specific) accessible only to the web server group. The group for the database servers would have port 3306 (MySQL) open only to the application server group. All three groups would permit administrative access on port 22 (SSH), but only from the customer's corporate network. With this mechanism, you can deploy highly secure applications.

For more information about security groups for your VPC, see "Control traffic to resources using security groups" in the *Amazon Virtual Private Cloud User Guide* (https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html).

DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



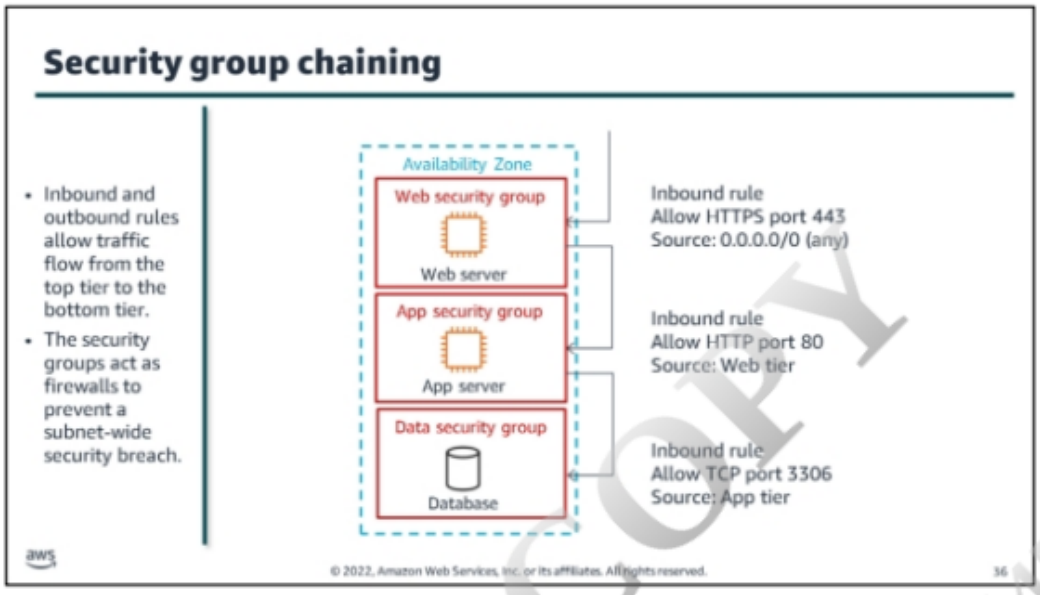
With security group rules, you can filter traffic based on protocols and port numbers. Security groups are stateful—if you send a request from your instance, the response traffic for that request is allowed to flow in regardless of inbound security group rules.

This table displays both inbound and outbound security group rules for a web server. The inbound rules allow for traffic on port 80 and port 443. Any user requesting the web server would be allowed in and the web server would return the response back to their request. From the outbound perspective, if trying to send traffic, not in response to something that was requested on 480 or 443, you are limited to the port 1433 and 3306.

DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

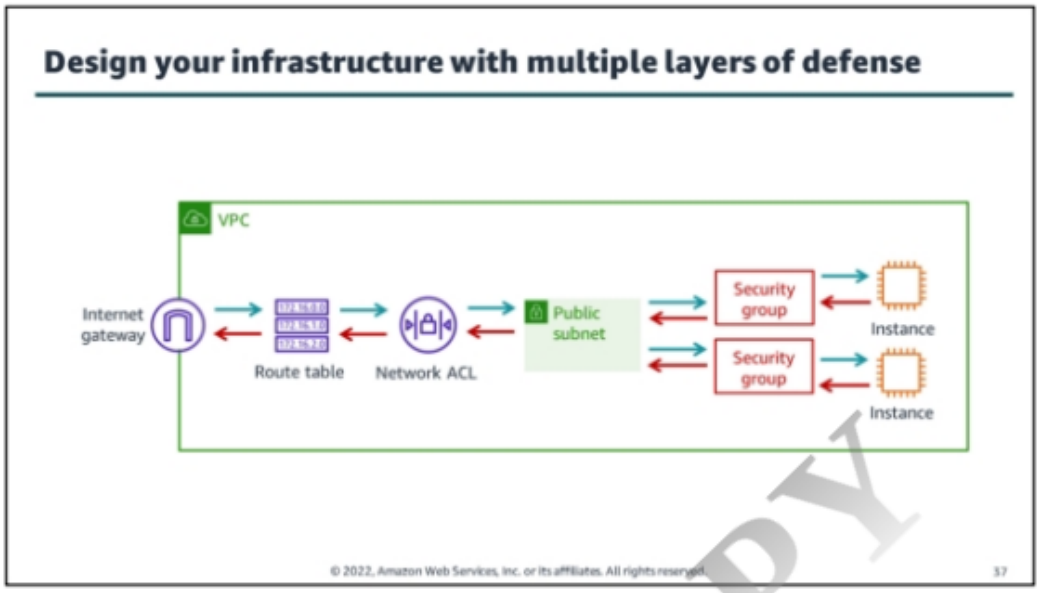


Here's an example of a chain of security groups. The inbound and outbound rules are set up in a way that traffic can only flow from the top tier to the bottom tier and back up again. The security groups act as firewalls to prevent a security breach in one tier to automatically provide subnet-wide access of all resources to the compromised client.

DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



As a best practice, you should secure your infrastructure with multiple layers of defense. You can control which instances are exposed to the internet by running your infrastructure in a VPC with a properly configured internet gateway and route tables. You can also define security groups and network ACLs to further protect your infrastructure at the interface and subnet levels. Additionally, you should secure your instances with a firewall at the operating system level and follow other security best practices.

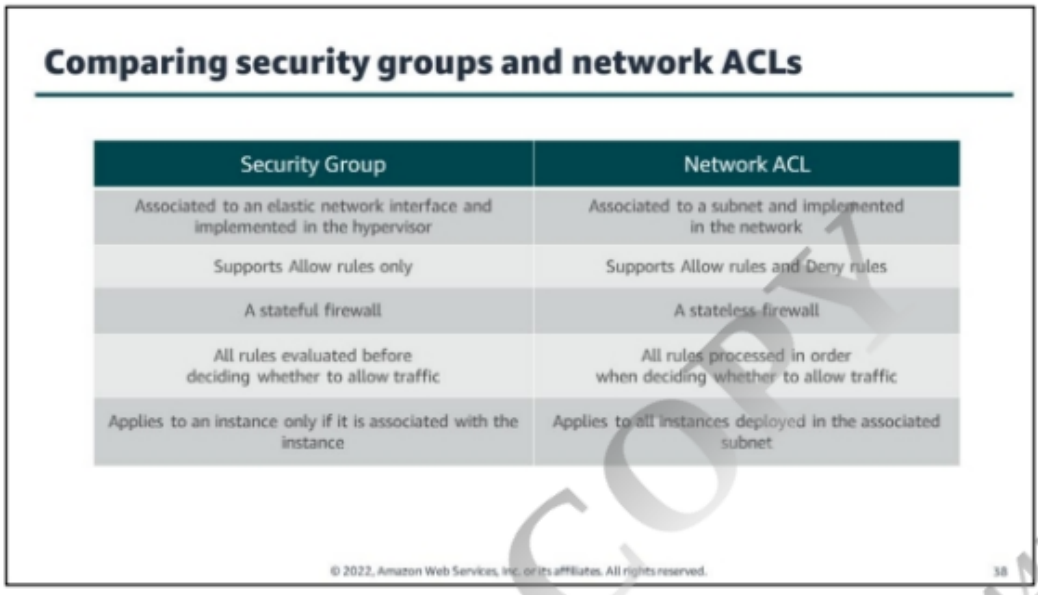
AWS customers typically use security groups as their primary method of network packet filtering. They are more versatile than network ACLs because of their ability to perform stateful packet filtering and to use rules that reference other security groups. However, network ACLs can be effective as a secondary control for denying a specific subset of traffic or providing high-level guard rails for a subnet.

By implementing both network ACLs and security groups as a defense-in-depth means of controlling traffic, a mistake in the configuration of one of these controls will not expose the host to unwanted traffic.

DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



A security group acts as a firewall for associated EC2 instances, controlling both inbound and outbound traffic at the instance level. Network ACLs act as a firewall for associated subnets, controlling both inbound and outbound traffic at the subnet level.

Both can have different default configurations depending on how they are created.

Security groups
- Security groups in default VPCs allow all traffic.
- New security groups have no inbound rules and allow outbound traffic.

Network ACLs
- Network ACLs in default VPCs allow all inbound and outbound IPv4 traffic.
- Custom network ACLs deny all inbound and outbound traffic, until you add rules.

DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

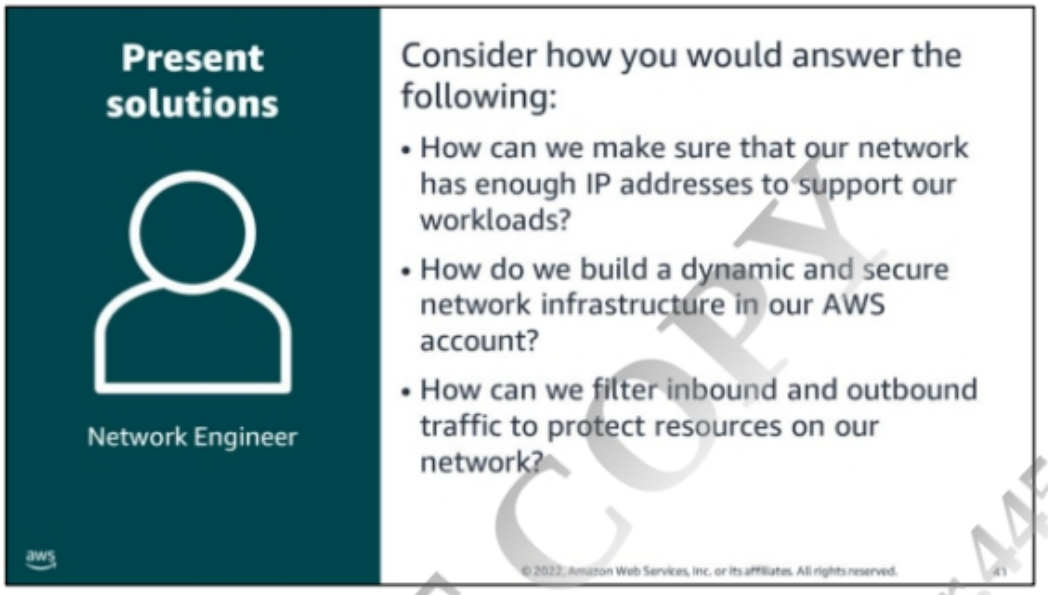
© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



Imagine you are now ready to talk to the network engineer and present solutions that meet their architectural needs.

Think about how you would answer the questions from the beginning of the lesson.

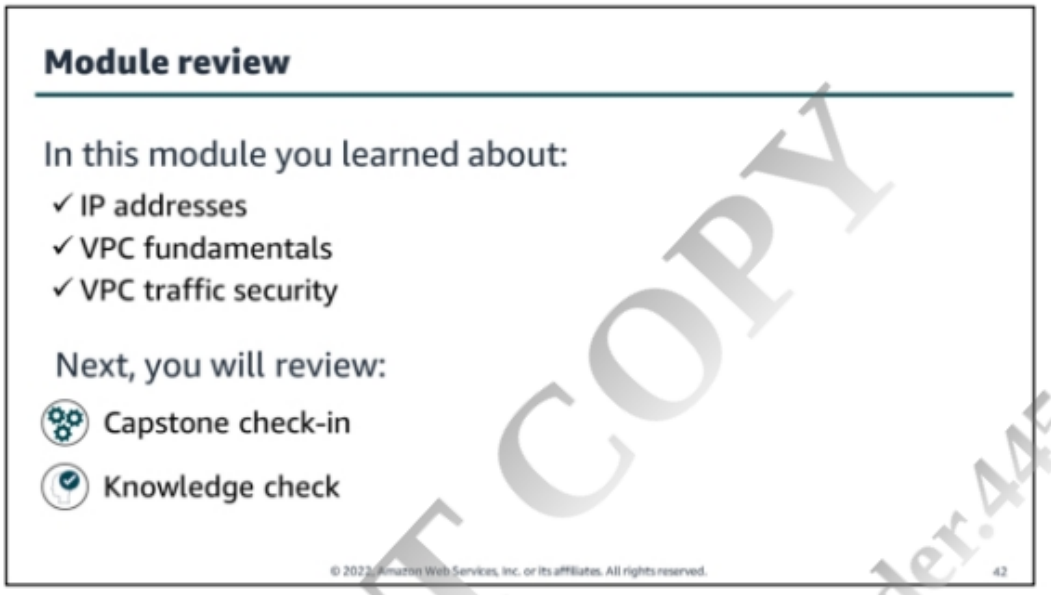
Your answers should include the following solutions:

- With AWS, you define IP address ranges using CIDR blocks. You can assign block sizes between /28 (16 IP addresses) and /16 (65,536 IP addresses) for IPv4 subnets.
- Build a dynamic and secure network infrastructure using VPC components.
- Protect the network by filtering inbound and outbound traffic with network access control lists and security groups.

DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

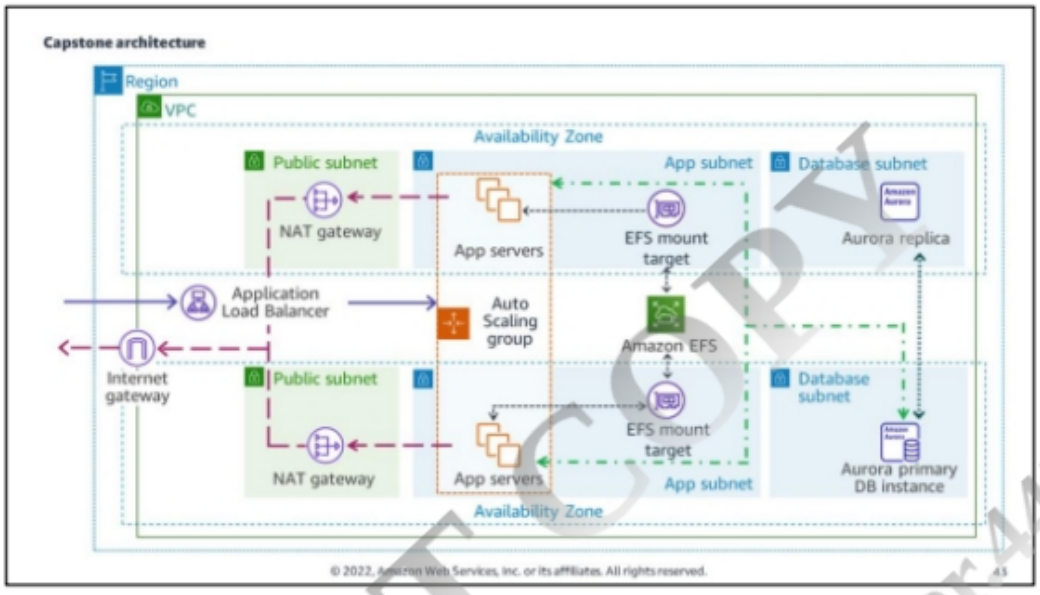
© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

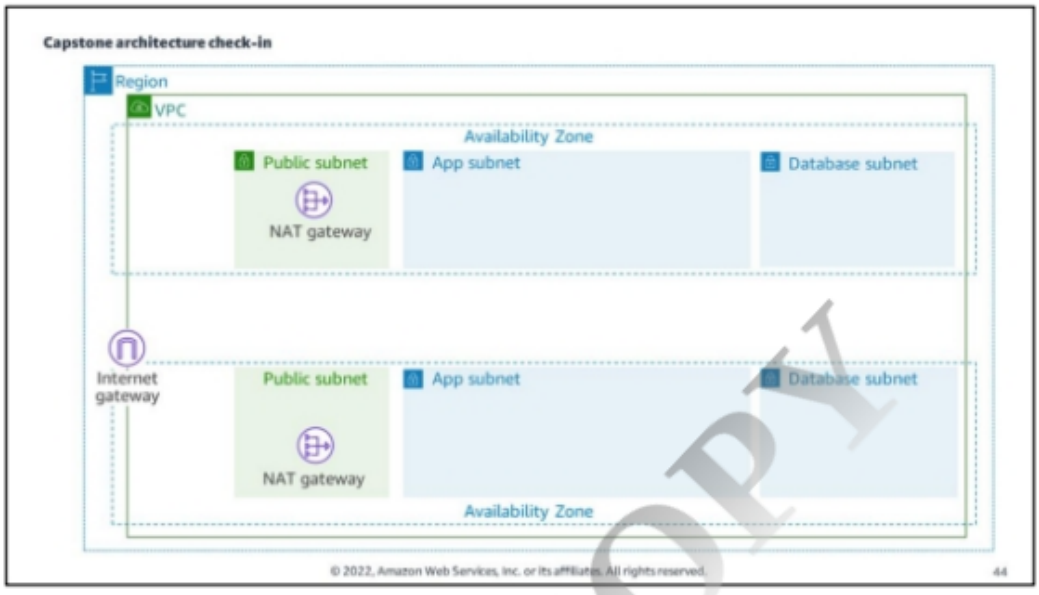


At the end of this course is a Capstone Lab project. You will be provided a scenario and asked to build an architecture based on project data, best practices, and the Well-Architected Framework.

DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



In this module, you explored AWS networking services and resources.

Review the capstone architecture to explore some of the design decisions. This architecture helps you provide the following benefits:

- You achieve high availability by setting up an Amazon VPC across two Availability Zones. If one Availability Zone stops working, you can direct traffic to the remaining Availability Zone.
- You protect resources by dividing them into separate subnets: public, application, and data. You can control the traffic that reaches each group of resources. You can also better isolate errors and vulnerabilities that occur in a subnet.
- You create one of each of these subnets in both Availability Zones.
- To allow internet access on your network, you set up an internet gateway. The internet gateway also protects private IP addresses of resources on your network. The internet gateway performs network address translation between public and private IP addresses.
- You set up NAT gateways in the public subnets to handle outbound traffic to the internet from private subnets. This provides internet connectivity while preventing external traffic from connecting with your private instances.

DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

The correct answer is B, false.

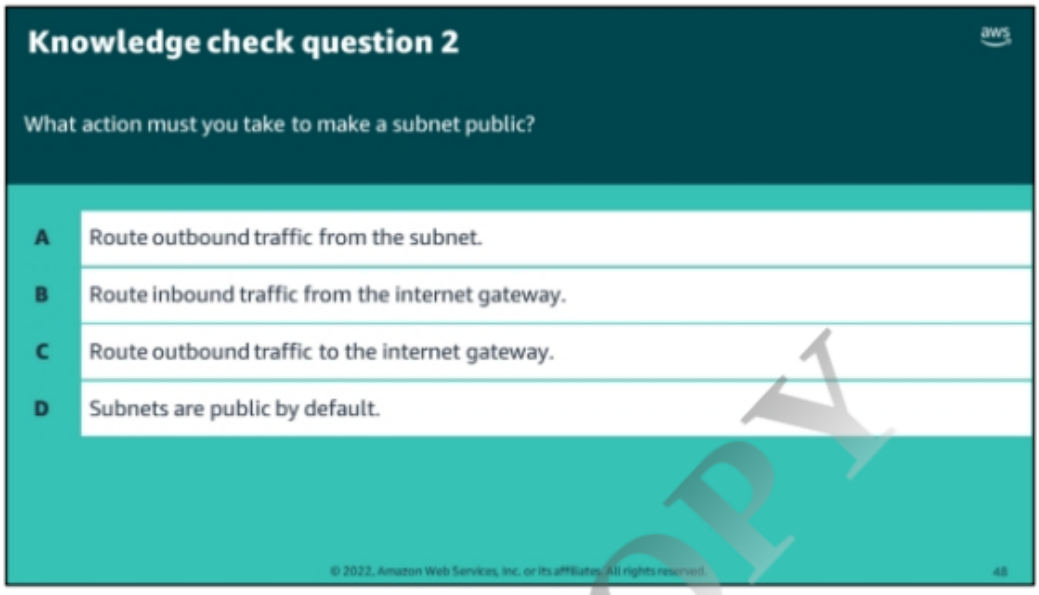
A VPC spans all of the Availability Zones in one Region.

For more information, see "Virtual private clouds (VPC)" in the *Amazon Virtual Cloud User Guide* (https://docs.aws.amazon.com/vpc/latest/userguide/configure-your-vpc.html).

DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

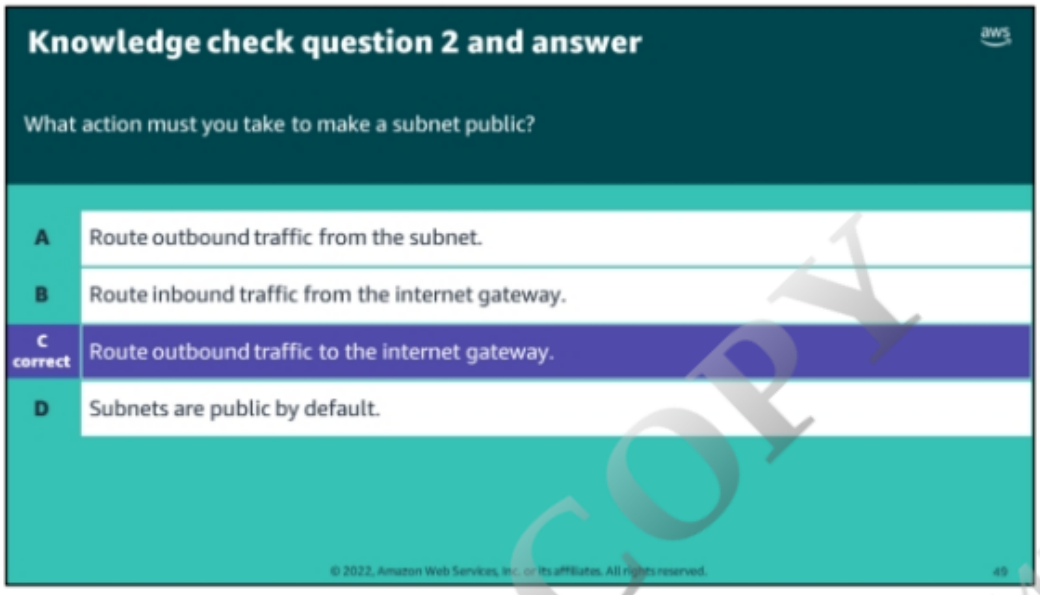
Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



The correct answer is C, route outbound traffic to the internet gateway.

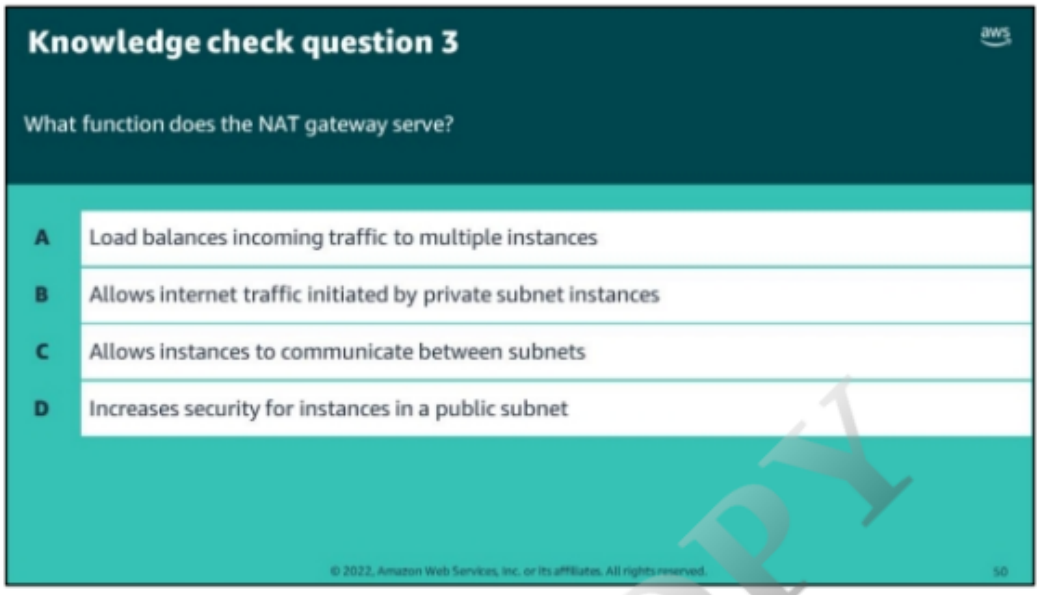
In your public subnet's route table, you can specify a route for the internet gateway to all destinations not explicitly known to the route table (0.0.0.0/0 for IPv4 or ::/0 for IPv6). Alternatively, you can scope the route to a narrower range of IP addresses, for example, the public IPv4 addresses of your company's public endpoints outside of AWS, or the Elastic IP addresses of other Amazon EC2 instances outside of your VPC.

For more information, see "Connect to the internet using an internet gateway" in the *Amazon VPC User Guide* (https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html).

DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

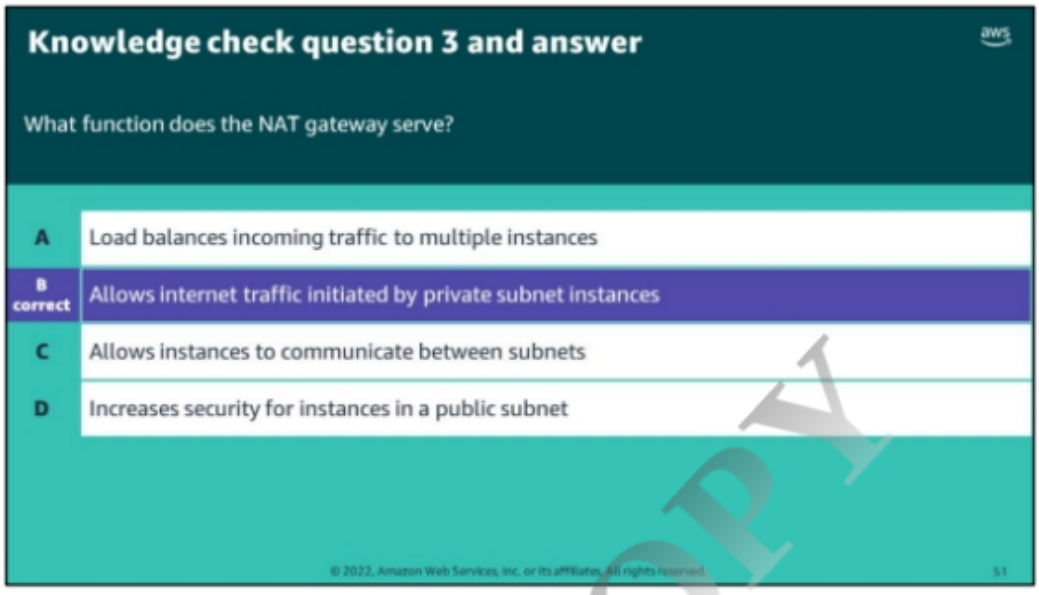
Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



The correct answer is B, allows internet traffic initiated by private subnet instances.

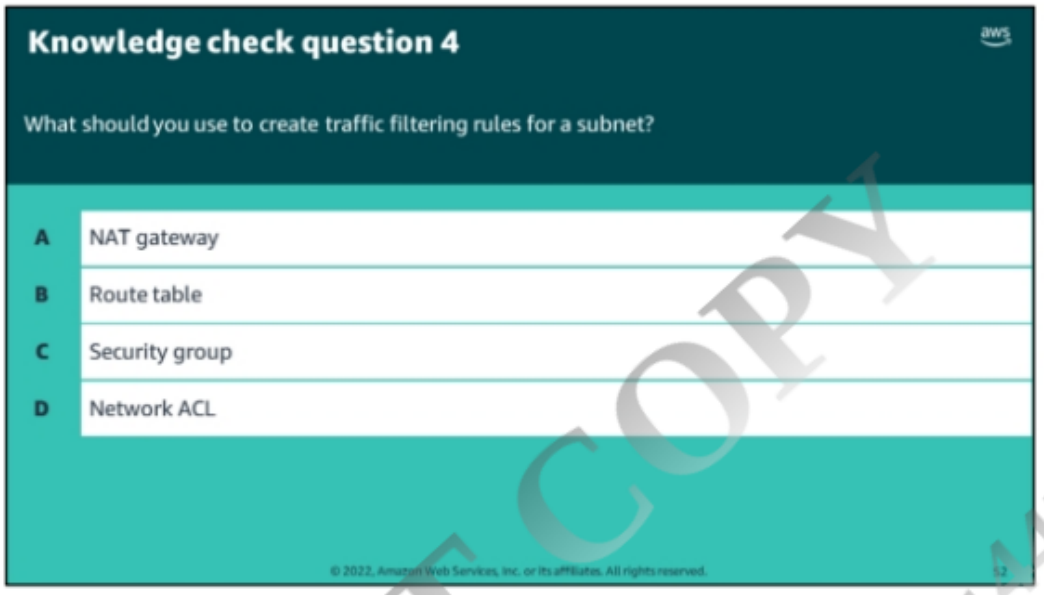
You can use a NAT device to allow instances in private subnets to connect to the internet, other VPCs, or on-premises networks. These instances can communicate with services outside of the VPC, but they cannot receive unsolicited connection requests.

For more information about NAT gateways, see "Connect to the internet or other networks using NAT devices" in the *Amazon VPC User Guide* (https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat.html).

DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

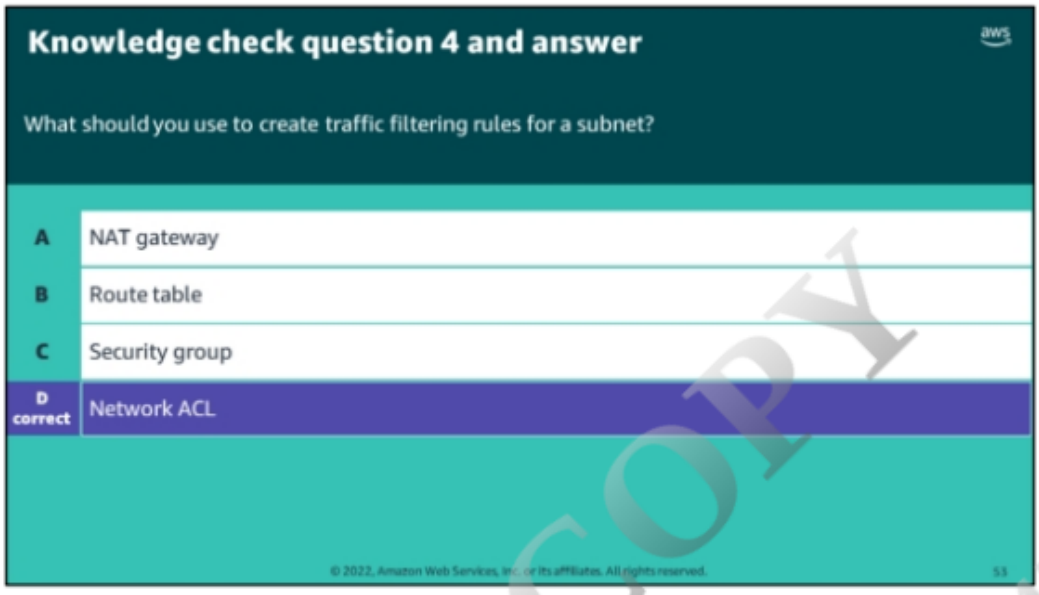
Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



The correct answer is D, network ACL.

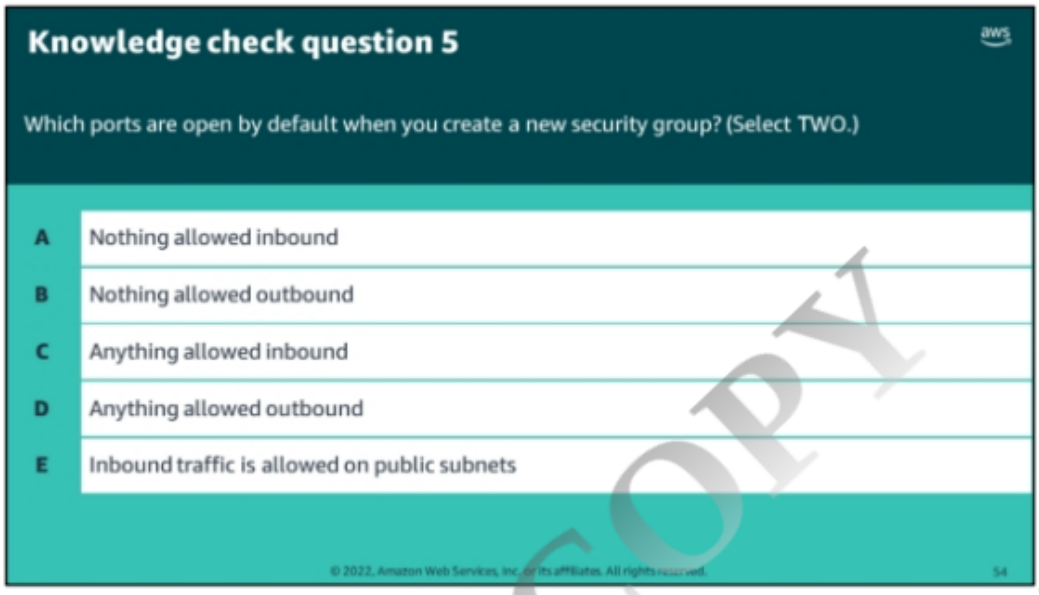
A network ACL contains a numbered list of rules. You evaluate the rules in order, starting with the lowest numbered rule, to determine whether traffic is allowed in or out of any subnet associated with the network ACL.

To learn more about Network ACLs, see "Control traffic to subnets using Network ACLs" in the *Amazon VPC User Guide* (https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html).

DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

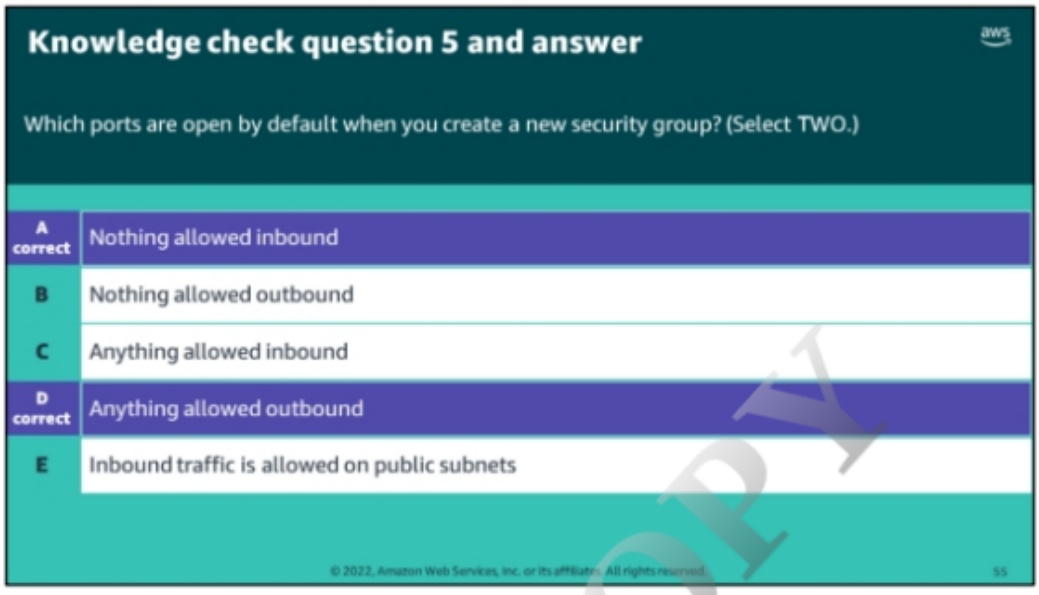
Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



The correct answers are A, nothing allowed inbound, and D, anything allowed outbound.

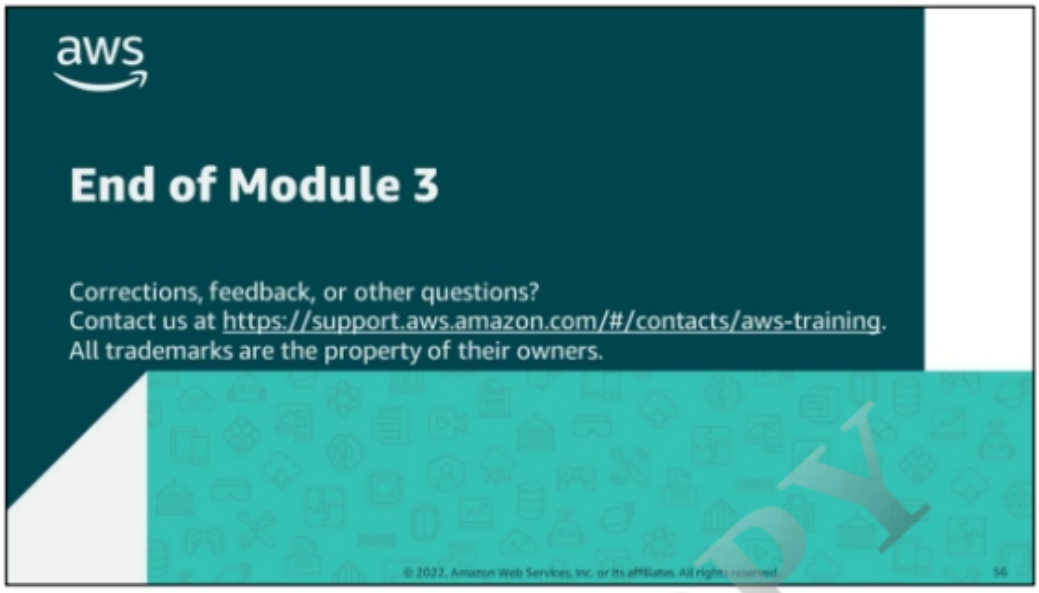
Nothing is allowed inbound and anything is allowed outbound. New security groups have no inbound rules and allow outbound traffic.

For more information about security groups, see "Control traffic to resources using security groups" in the *Amazon VPC User Guide* (https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html).

DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Printed by: 2d35e8483186bd2@placeholder.44518.edu. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



DO NOT COPY
2d35e8483186bd2@placeholder.44518.edu

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.