

AWS Academy Cloud Foundations (Fundamentos de nuvem da AWS Academy)

Módulo 5: Redes e entrega de conteúdo



Tópicos

- Noções básicas de redes
- Amazon VPC
- Redes da VPC
- Segurança da VPC
- Amazon Route 53
- Amazon CloudFront

Atividades

- Rotular um diagrama de rede
- Projetar uma arquitetura básica de VPC

Demonstração

- Demonstração da VPC

Laboratório

- Crie uma VPC e inicie um servidor Web



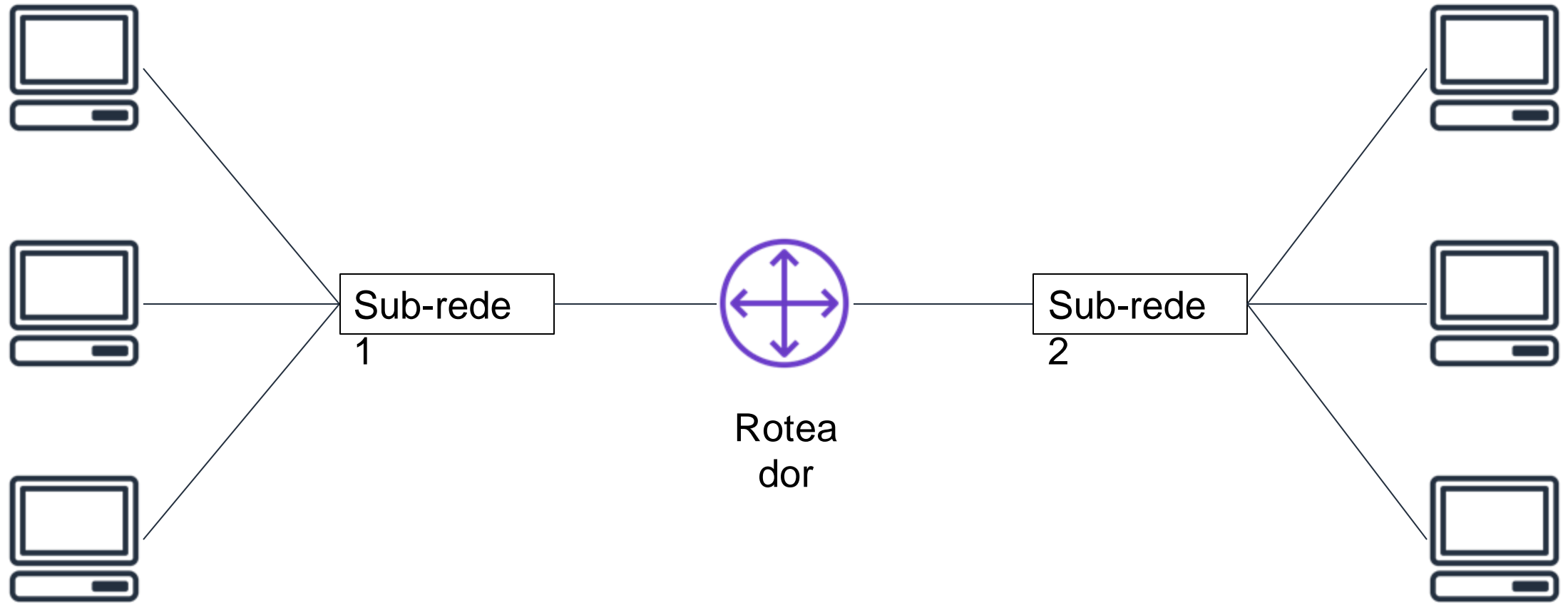
**Teste de
conhecimento**

Depois de concluir este módulo, você deverá ser capaz de:

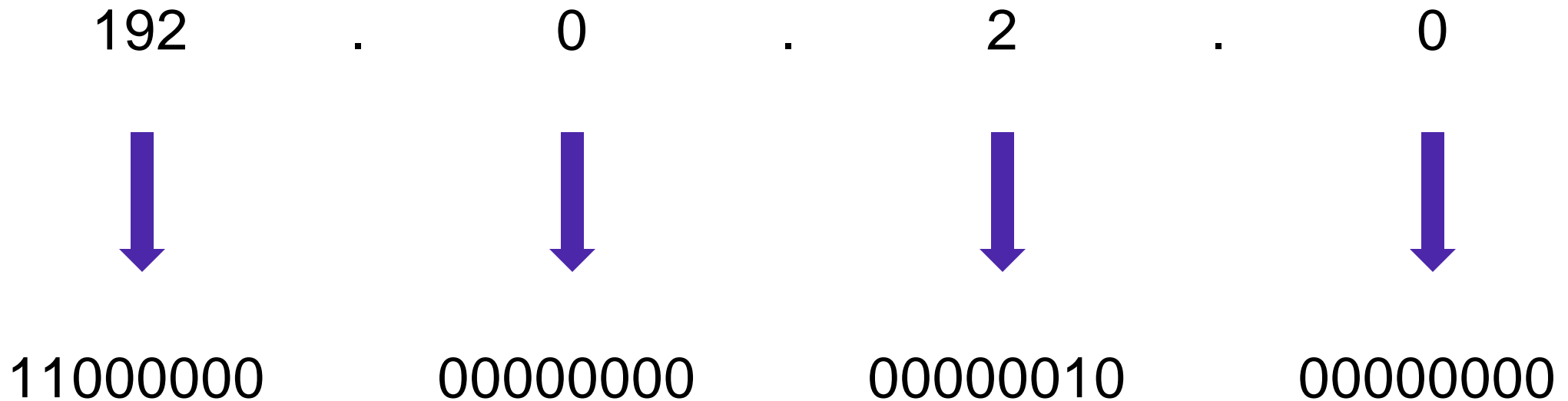
- Reconhecer os conceitos básicos de redes
- Descrever as redes virtuais na nuvem com a Amazon VPC
- Rotular um diagrama de rede
- Projetar uma arquitetura básica de VPC
- Indicar as etapas para criar uma VPC
- Identificar grupos de segurança
- Criar sua própria VPC e incluir outros componentes nela para produzir uma rede personalizada
- Identificar os fundamentos do Amazon Route 53
- Reconhecer os benefícios do Amazon CloudFront

Módulo 5: Redes e entrega de conteúdo

Seção 1: Noções básicas de redes



Endereços IP



Endereços IPv4 e IPv6

Endereço IPv4 (32 bits):

192.0.2.0

Endereço IPv6 (128 bits): 2600:1f18:22ba:8c00:ba86:a05e:a5ba:00FF

Roteamento sem classe entre domínios (CIDR)

Identificador de rede (prefixo de roteamento)

192 . 0 . 2



11000000

Fixo



00000000

Fixo



00000010

Fixo

Identificador do host

. 0 /



00000000
para 11111111

Flexível

|

24

Informa
quantos bits
estão fixos

Modelo Open Systems Interconnection (OSI - Interconexão de sistemas abertos)

Camada	Número	Função	Protocolo/endereço
Aplicativo	7	Meios para um aplicativo acessar uma rede de computadores	HTTP(S), FTP, DHCP, LDAP
Apresentação	6	<ul style="list-style-type: none">• Garante que a camada do aplicativo possa ler os dados• Criptografia	ASCII, ICA
Sessão	5	Permite a troca ordenada de dados	NetBIOS, RPC
rede/	4	Fornecer protocolos para oferecer suporte à comunicação host a host	TCP, UDP
Rede	3	Roteamento e encaminhamento de pacotes (roteadores)	IP
Link de dados	2	Transferir dados na mesma rede LAN (hubs e switches)	MAC
Físico	1	Transmissão e recepção de fluxo de bits brutos em um meio físico	Sinais (1s e 0s)

Módulo 5: Redes e entrega de conteúdo

Seção 2: Amazon VPC

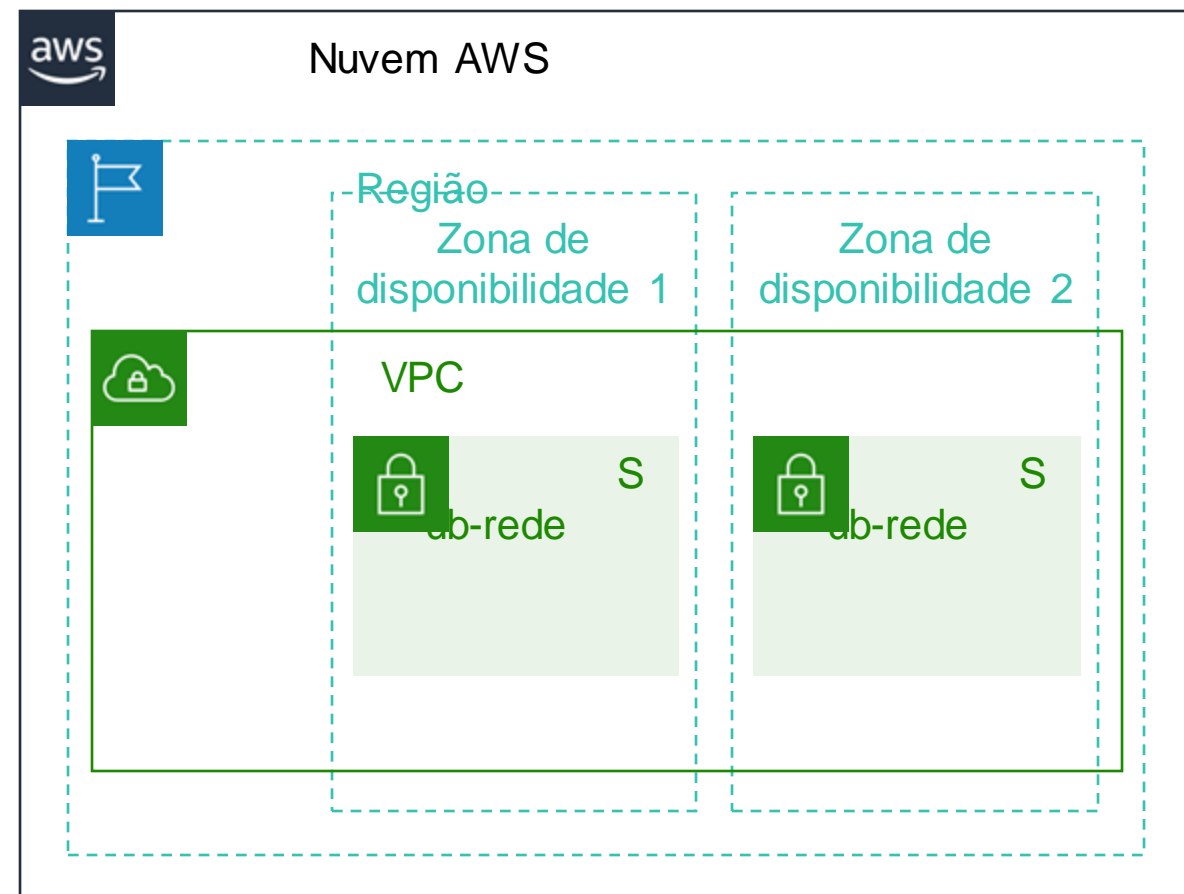


Amazon
VPC


- Permite provisionar uma seção **isolada logicamente** da Nuvem AWS onde você pode executar recursos da AWS em uma rede virtual que você mesmo define
- Fornece **controle sobre seus recursos de rede virtual**, incluindo:
 - Seleção do intervalo de endereços IP
 - Criação de sub-redes
 - Configuração de tabelas de rotas e gateways de rede
- Permite **personalizar a configuração de rede** para sua VPC
- Permite usar **várias camadas de segurança**

VPCs e sub-redes

- VPCs:
 - **Logicamente isoladas** de outras VPCs
 - **Dedicadas** à sua conta da AWS
 - Pertencem a uma única **região da AWS** e podem abranger várias zonas de disponibilidade
- Sub-redes:
 - **Intervalo de endereços IP** que dividem uma VPC
 - Pertencem a uma única **zona de disponibilidade**
 - Classificadas como **públicas** ou **privadas**



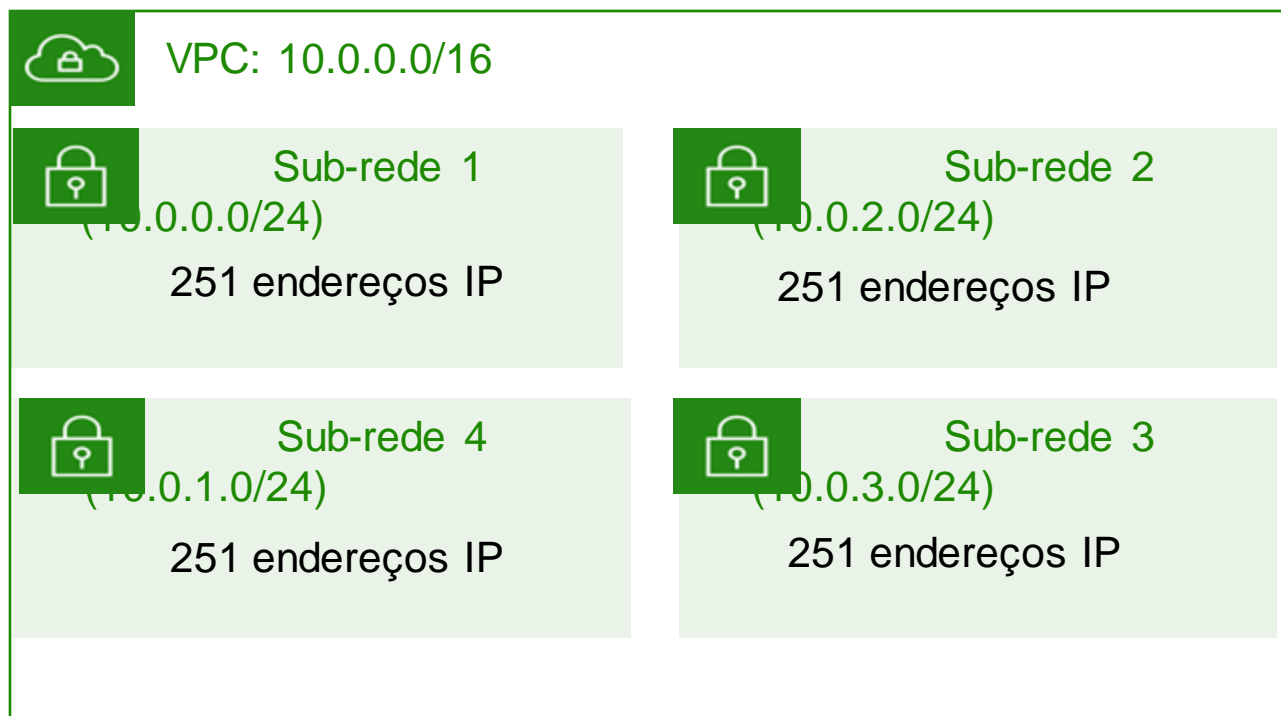
- Ao criar uma VPC, você a atribui a um **bloco CIDR IPv4** (intervalo de endereços IPv4 **privados**).
- Você **não pode alterar o intervalo de endereços** depois de criar a VPC.
- O **maior** tamanho de bloco CIDR IPv4 é **/16**.
- O **menor** tamanho do bloco CIDR IPv4 é **/28**.
- O IPv6 também é compatível (com um limite de tamanho de bloco diferente).
- Os blocos CIDR de sub-redes **não podem se sobrepor**.

 VPC

x.x.x.x/16 ou 65.536 endereços
(máximo)
to
x.x.x.x/28 ou 16 endereços (mínimo)

Endereços IP reservados

Exemplo: uma VPC com um bloco CIDR IPv4 de 10.0.0.0/16 tem 65.536 endereços IP no total. A VPC tem quatro sub-redes de tamanho igual. Somente 251 endereços IP estão disponíveis para uso por cada sub-rede.



Endereços IP para o bloco CIDR 10.0.0.0/24	Reservado para
10.0.0.0	Endereço de rede
10.0.0.1	Comunicação interna
10.0.0.2	Resolução do Domain Name System (DNS)
10.0.0.3	Uso futuro
10.0.0.255	Endereço de transmissão de rede

Endereço IPv4 público

- Atribuído manualmente por meio de um endereço IP elástico
- Atribuído automaticamente por meio das configurações de endereço IP público de atribuição automática no nível da sub-rede

Endereço IP elástico

- Associado a uma conta da AWS
- Pode ser alocado e remapeado a qualquer momento
- Custos adicionais podem ser aplicados

Interface de rede elástica

- Uma interface de rede elástica é uma **interface de rede virtual** que você pode:
 - Anexar a uma instância.
 - Separar da instância e anexar a outra instância para redirecionar o tráfego de rede.
- Seus **atributos a seguem** quando são reanexadas a uma nova instância.
- Cada instância em sua VPC tem uma **interface de rede padrão** que recebe um endereço IPv4 privado do intervalo de endereços IPv4 de sua VPC.



Tabelas de rotas e rotas

- Uma **tabela de rotas** contém um conjunto de regras (ou rotas) que **você pode configurar** para direcionar o tráfego de rede da sub-rede.
- Cada **rota** especifica um destino e um destino.
- Por padrão, toda tabela de rotas contém uma **rota local** para comunicação dentro da VPC.
- Cada **sub-rede deve estar associada a uma tabela de rotas** (no máximo uma).

Tabela de rotas principal (padrão)

Destino	Destino
10.0.0.0/16	local

Bloco CIDR da VPC



Principais lições da Seção 2

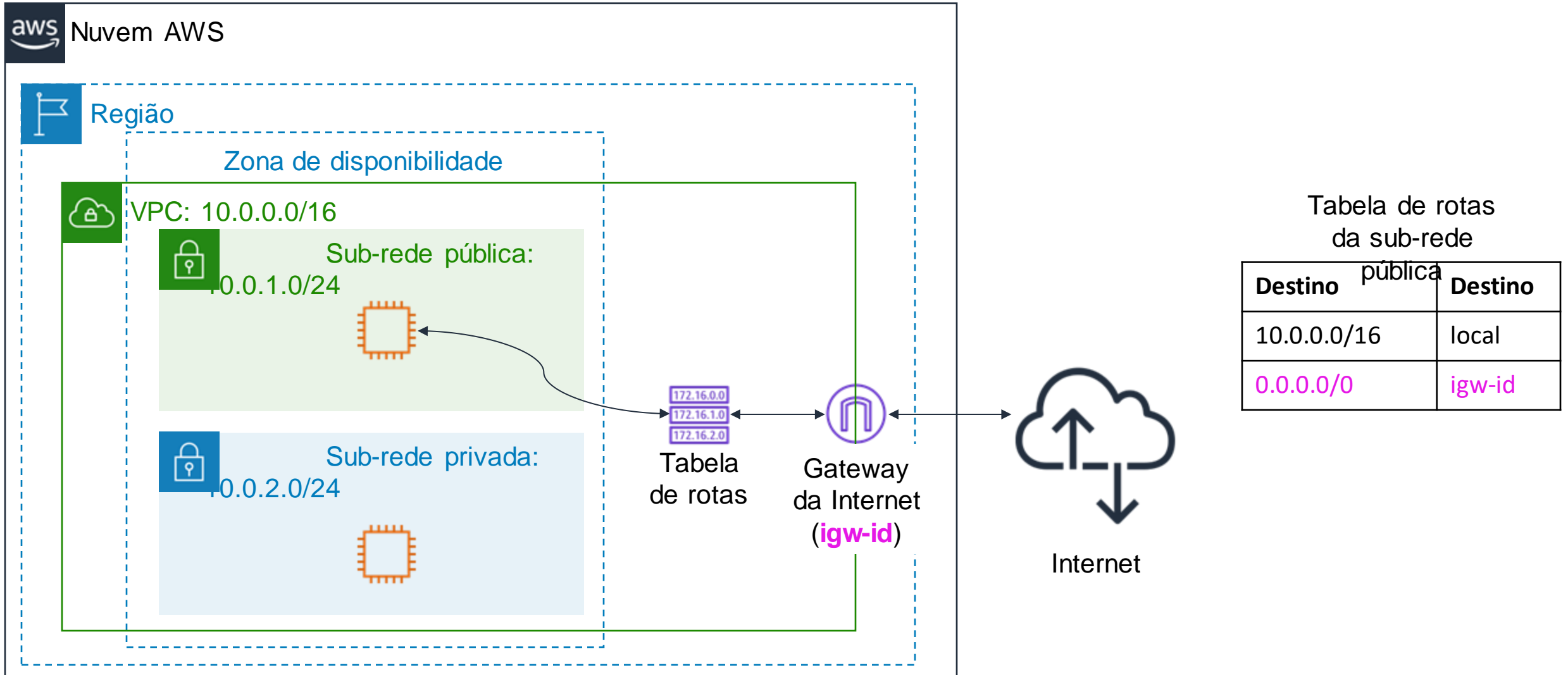


- Uma VPC é uma seção isolada logicamente da Nuvem AWS.
- Uma VPC pertence a uma região e requer um bloco CIDR.
- Uma VPC é subdividida em sub-redes.
- Uma sub-rede pertence a uma zona de disponibilidade e requer um bloco CIDR.
- As tabelas de rotas controlam o tráfego de uma sub-rede.
- As tabelas de rotas têm uma rota local integrada.
- Você adiciona outras rotas à tabela.
- Não é possível excluir a rota local.

Módulo 5: Redes e entrega de conteúdo

Seção 3: Redes VPC

Gateway da Internet



Gateway de tradução de endereços de rede (NAT)

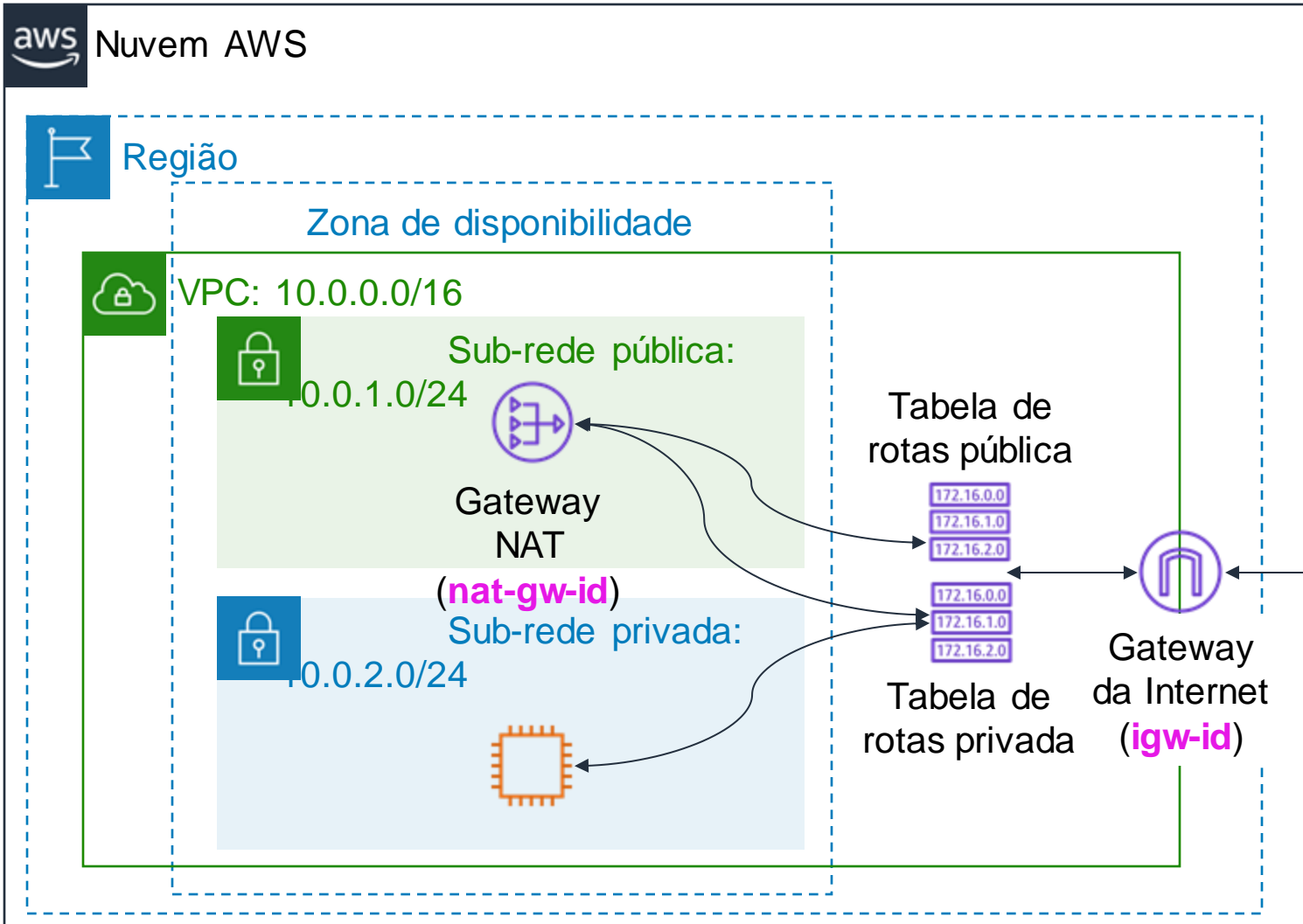


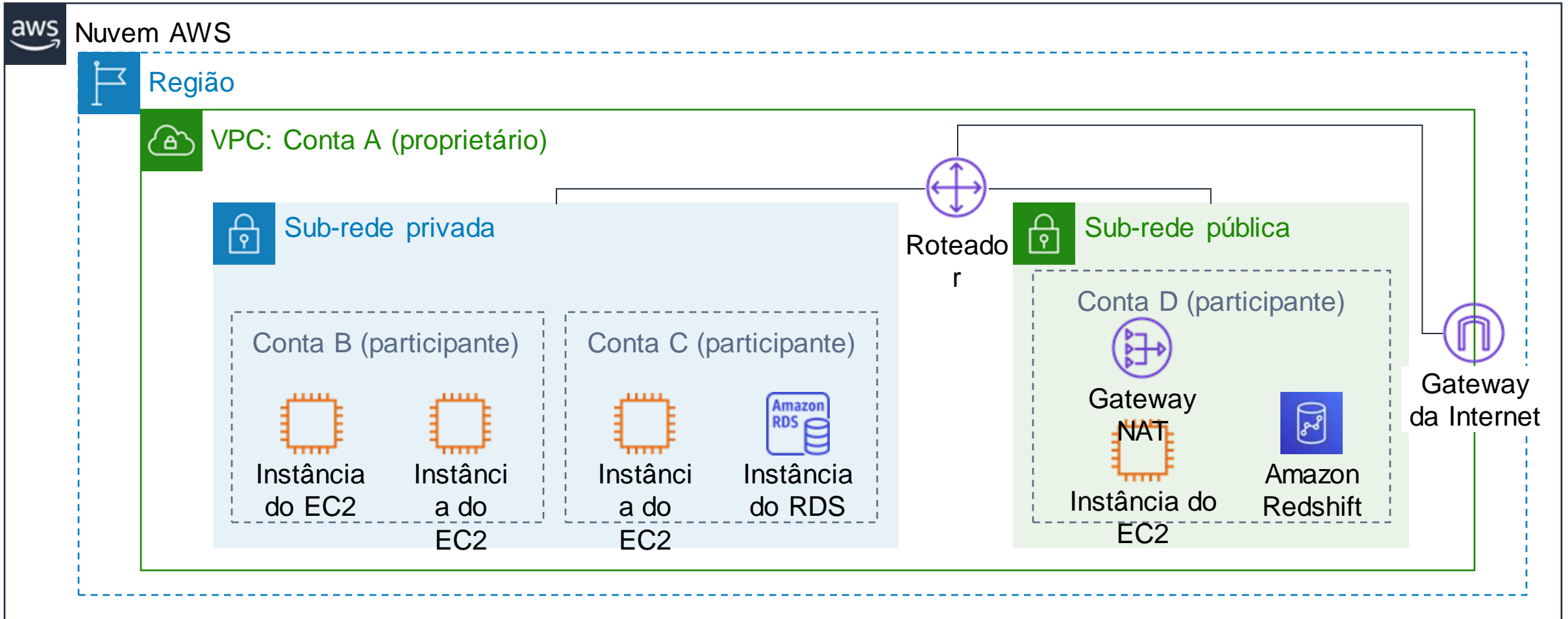
Tabela de rotas da sub-rede pública

Destino pública	Destino
10.0.0.0/16	local
0.0.0.0/0	igw-id

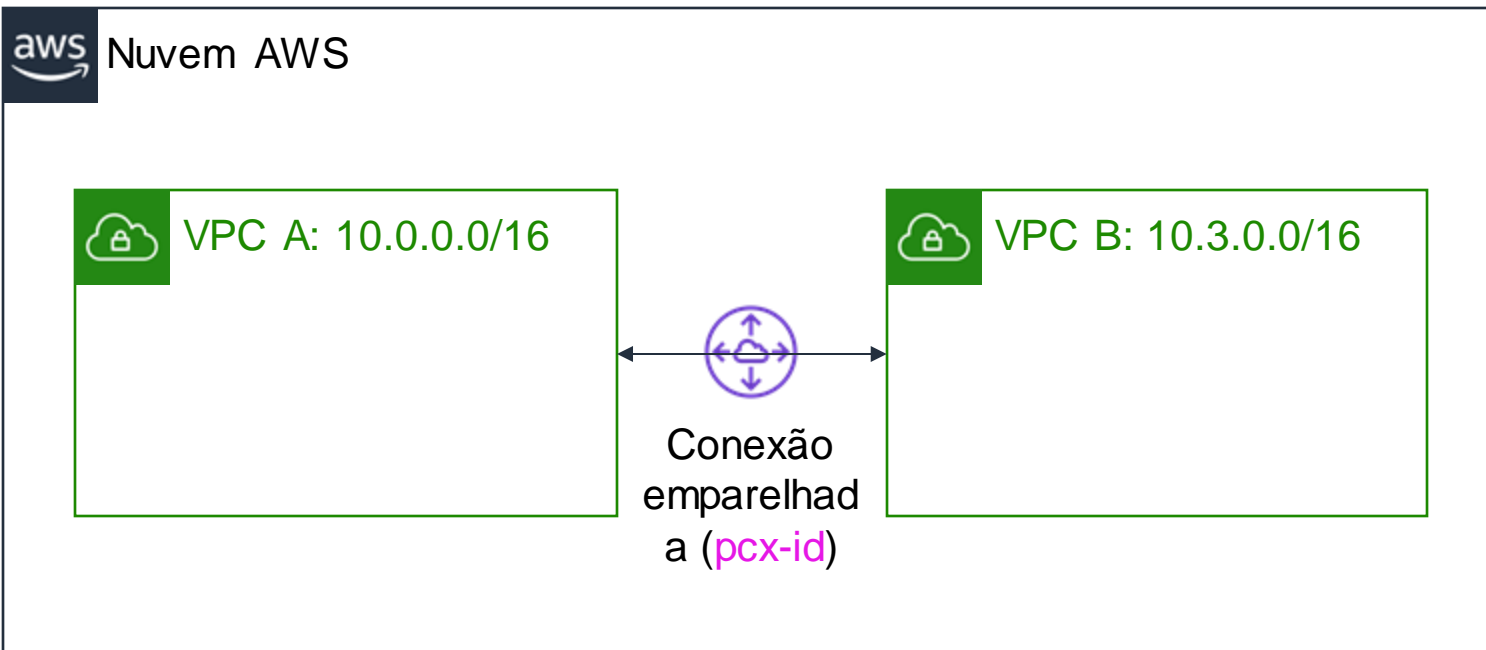
Tabela de rotas da sub-rede privada

Destino privada	Destino
10.0.0.0/16	local
0.0.0.0/0	nat-gw-id

Compartilhamento da VPC



Emparelhamento de VPC



Você pode conectar VPCs em sua própria conta da AWS, entre contas da AWS ou entre regiões da AWS.

Restrições:

- Espaços IP não podem se sobrepor.
- O emparelhamento transitivo não é compatível.
- Você pode ter apenas um recurso de emparelhamento entre as mesmas duas VPCs.

Tabela de rotas para VPC A

Destino	Destino
10.0.0.0/16	local
10.3.0.0/16	pcx-id

Tabela de rotas para VPC B

Destino	Destino
10.3.0.0/16	local
10.0.0.0/16	pcx-id

AWS Site-to-Site VPN

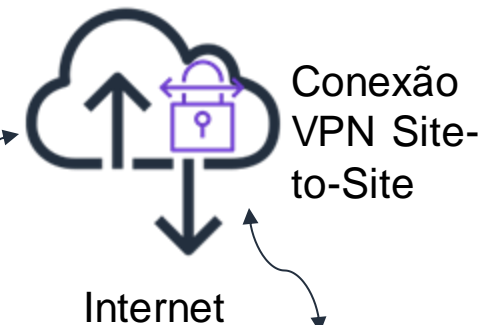
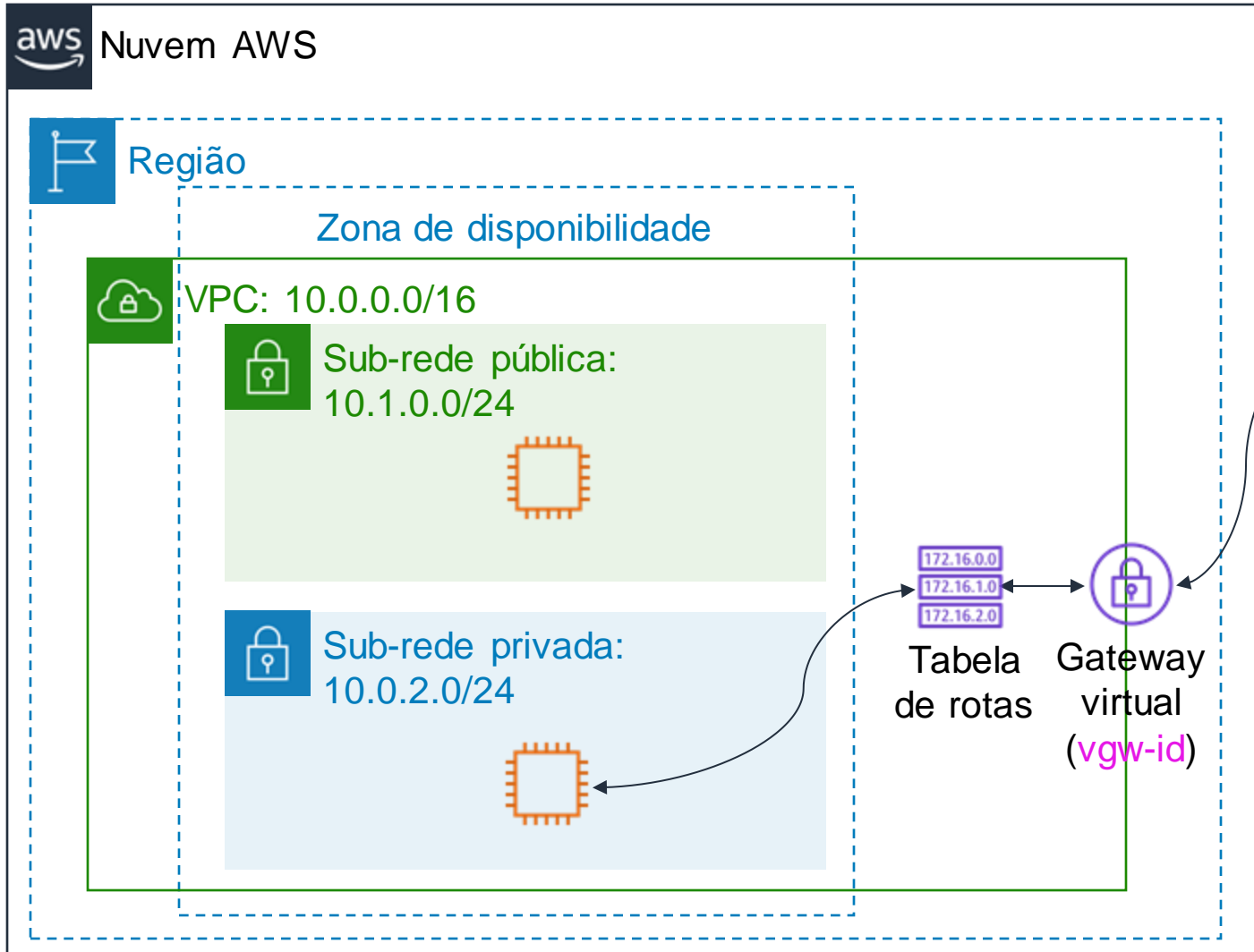


Tabela de rotas da sub-rede pública

Destino	Destino
10.0.0.0/16	local
0.0.0.0/0	igw-id

Tabela de rotas da sub-rede privada

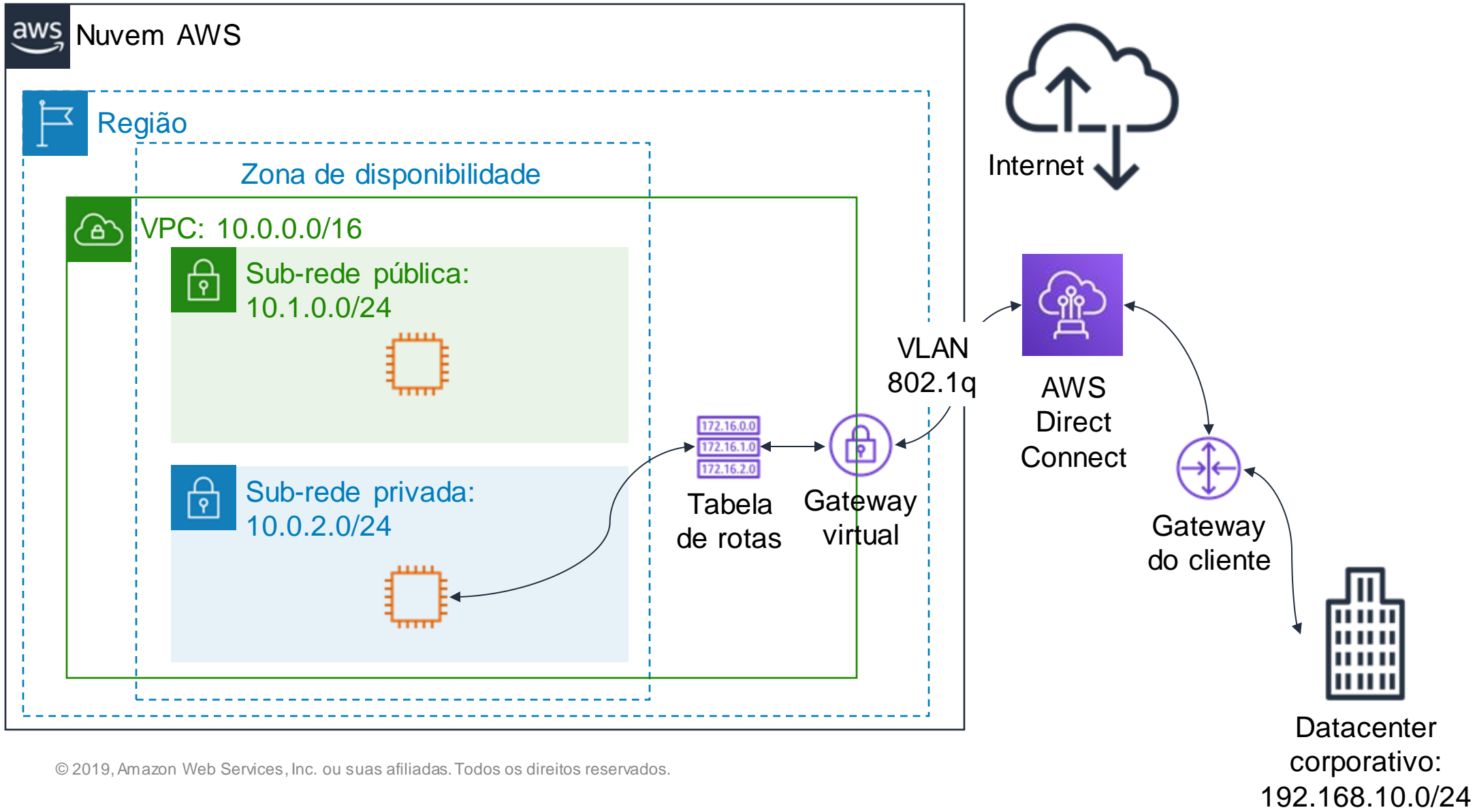
Destino	Destino
10.0.0.0/16	local
192.168.10.0/24	vgw-id



Datacenter corporativo:

192.168.10.0/24

AWS Direct Connect



VPC Endpoints

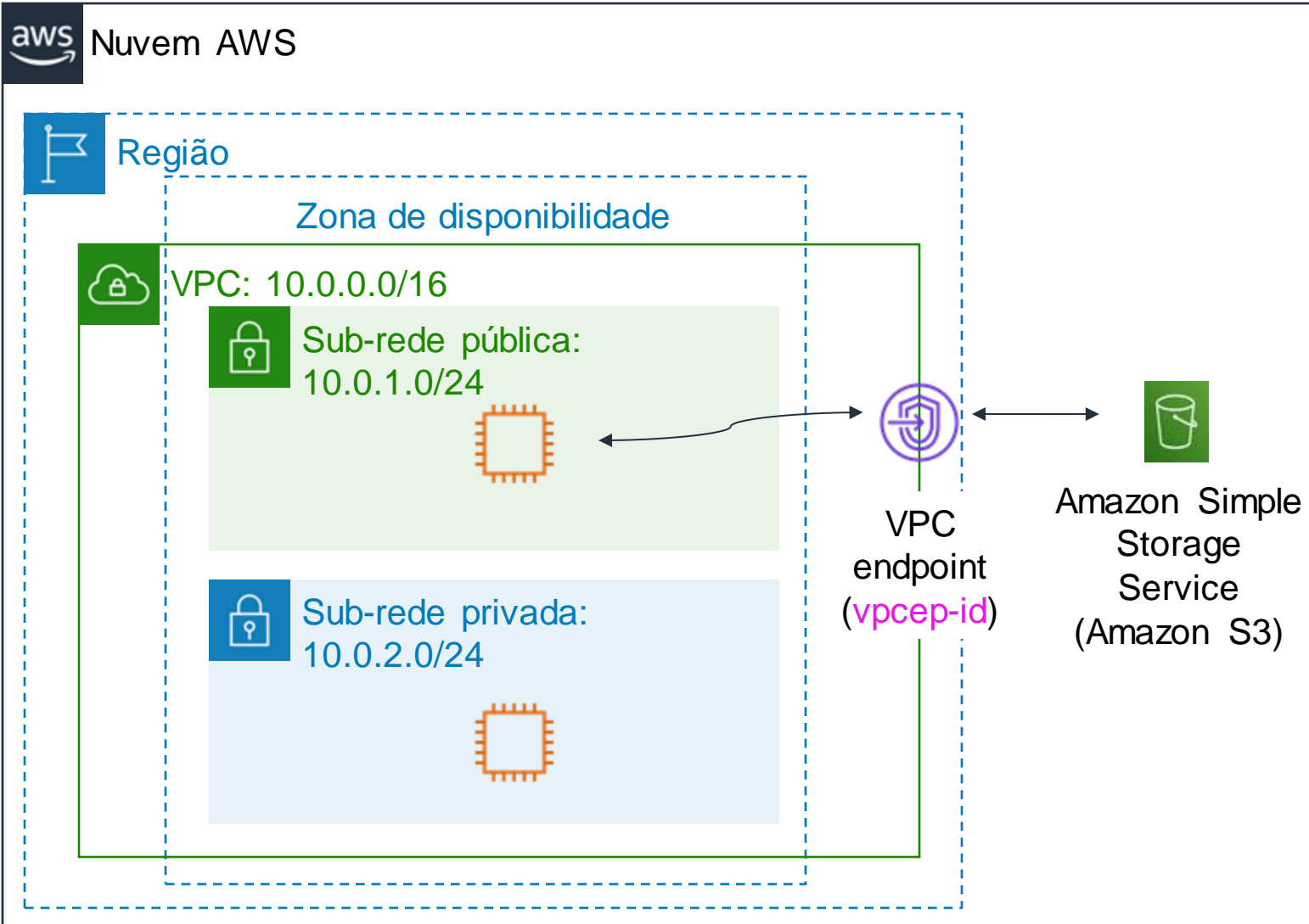


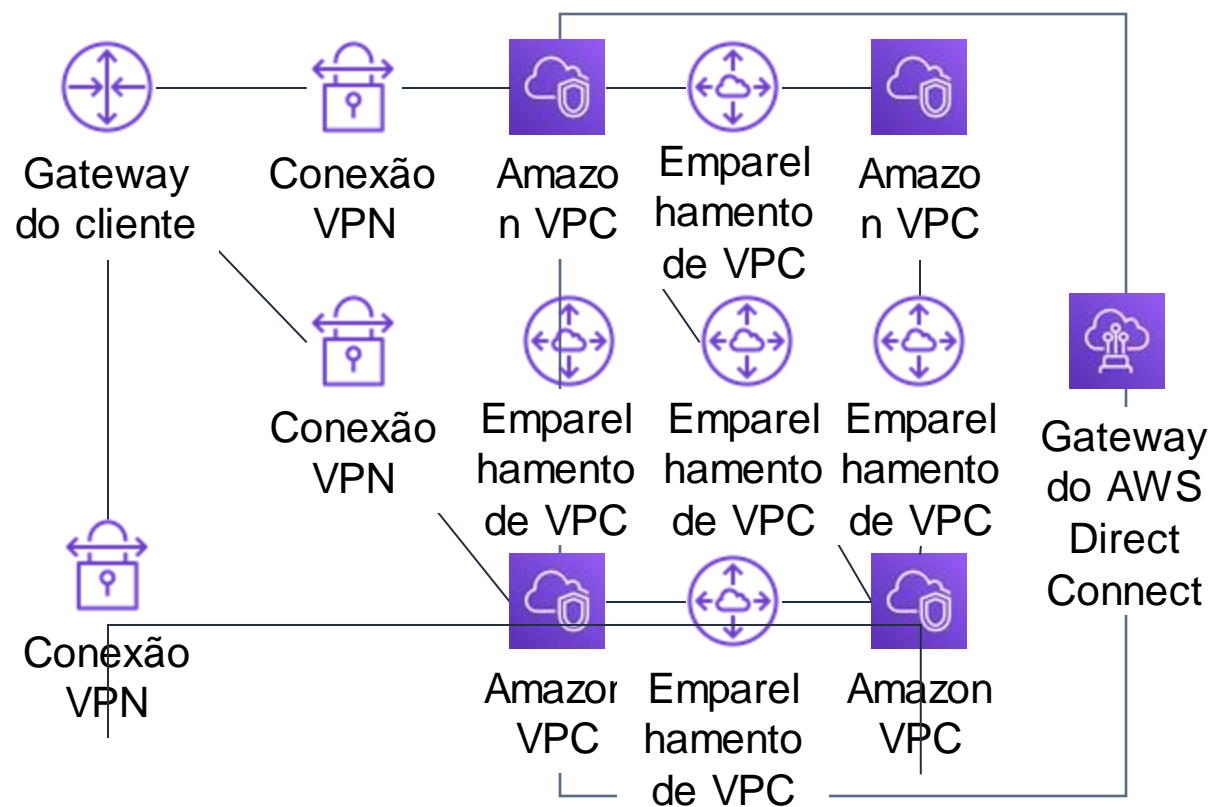
Tabela de rotas da sub-rede

Destino pública	Destino
10.0.0.0/16	local
ID do Amazon S3	vpcep-id

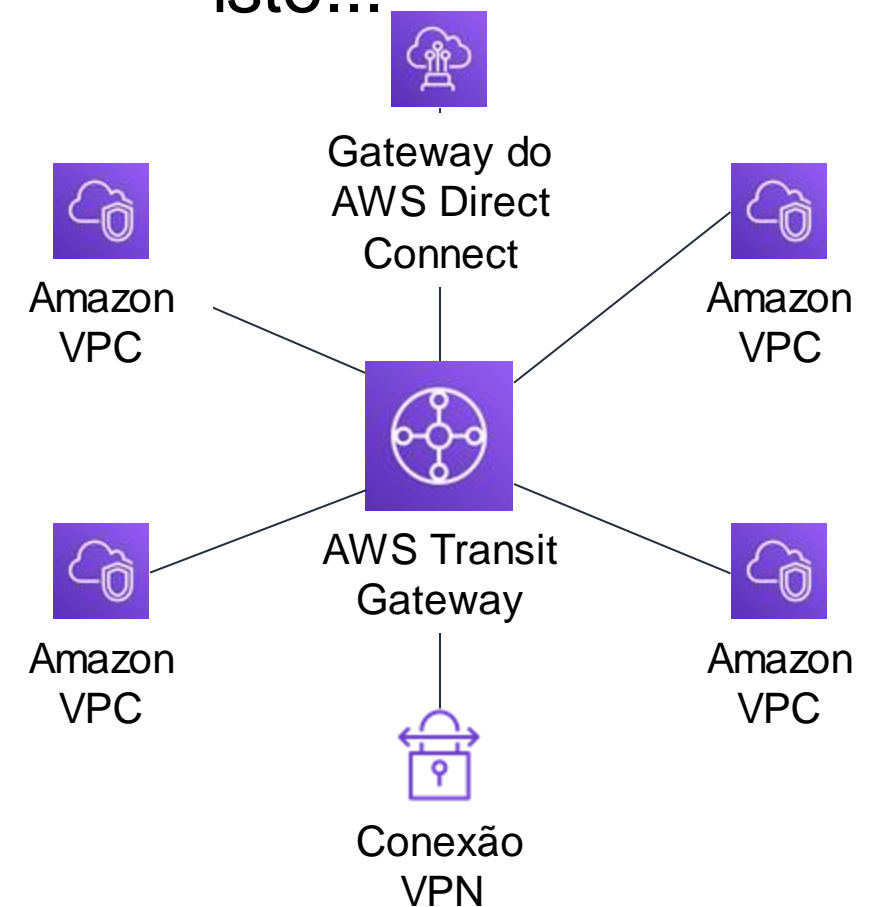
- Dois tipos de endpoints:
- Endpoints da **interface** (desenvolvidos pelo AWS PrivateLink)
 - Endpoints do **gateway** (Amazon S3 e Amazon DynamoDB)

AWS Transit Gateway

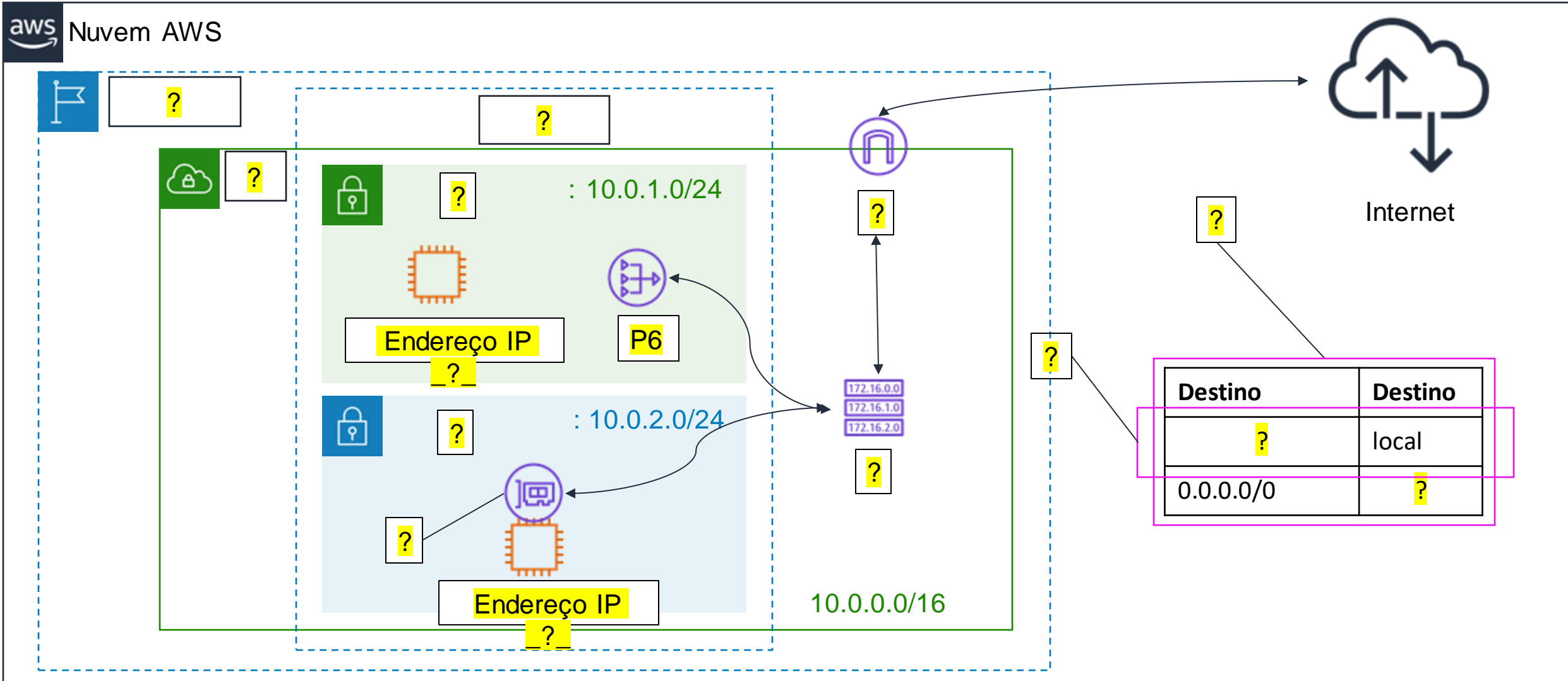
Disto...



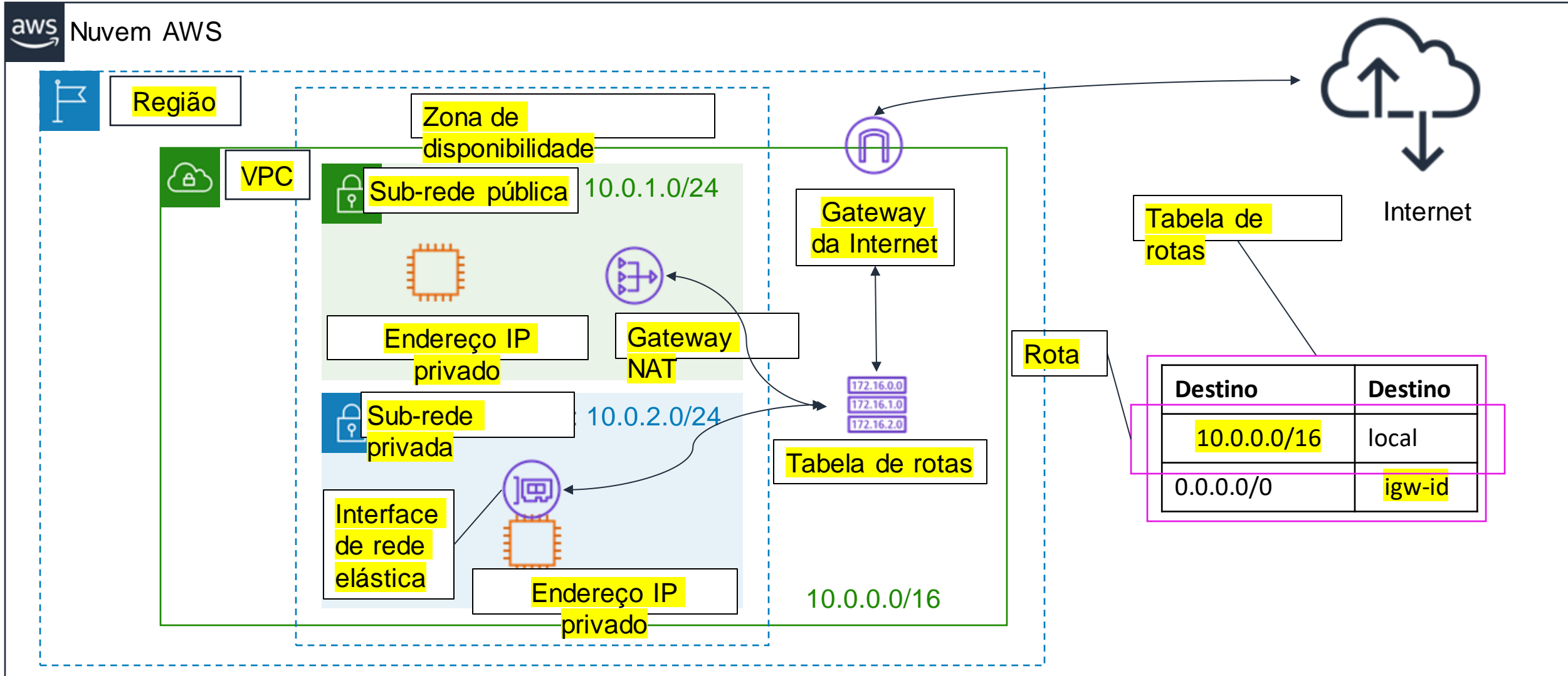
Para isto...



Atividade: rotular este diagrama de rede



Atividade: Solução



Demonstração gravada da Amazon VPC



Configurar demonstração

Amazon Virtual Private Cloud (VPC)

Principais lições da Seção 3

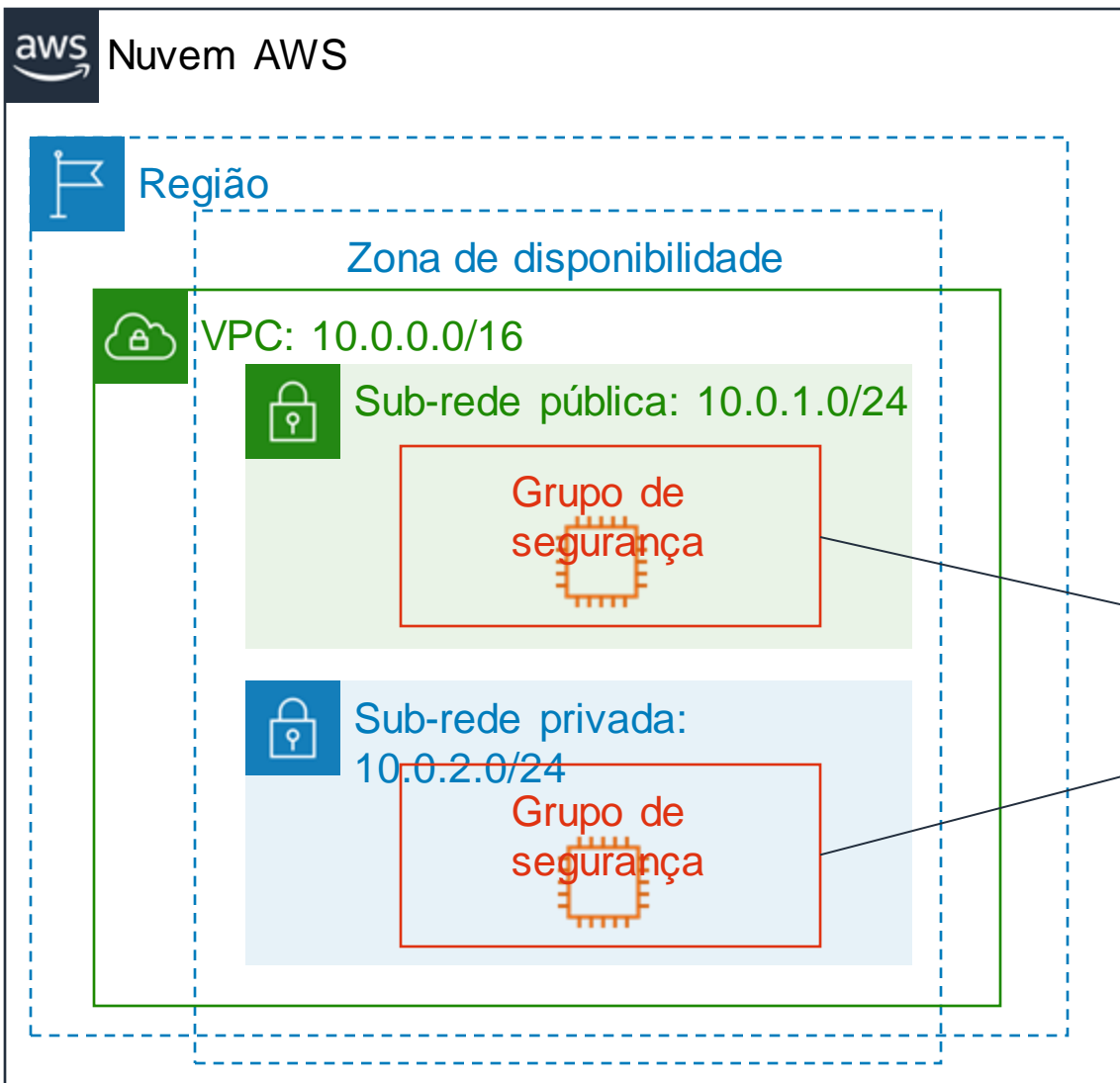


- Existem várias opções de rede da VPC, que incluem:
 - Gateway da Internet
 - Gateway NAT
 - VPC endpoint
 - Emparelhamento de VPC
 - Compartilhamento da VPC
 - AWS Site-to-Site VPN
 - AWS Direct Connect
 - AWS Transit Gateway
- Você pode usar o assistente da VPC para implementar seu projeto.

Módulo 5: Redes e entrega de conteúdo

Seção 4: Segurança da VPC

Grupos de segurança



Os grupos de segurança atuam no **nível da instância**.

Entrada				
Tipo	Protocolo	Intervalo de portas	Origem	Descrição
Todo tráfego	Todos	Todos	sg-xxxxxxxx	
Saída				
Tipo	Protocolo	Intervalo de portas	Origem	Descrição
Todo tráfego	Todos	Todos	sg-xxxxxxxx	

- Os grupos de segurança têm **regras** que controlam o tráfego de instâncias de entrada e saída.
- Os grupos de segurança padrão **negam todo o tráfego de entrada** e **permitem todo o tráfego de saída**.

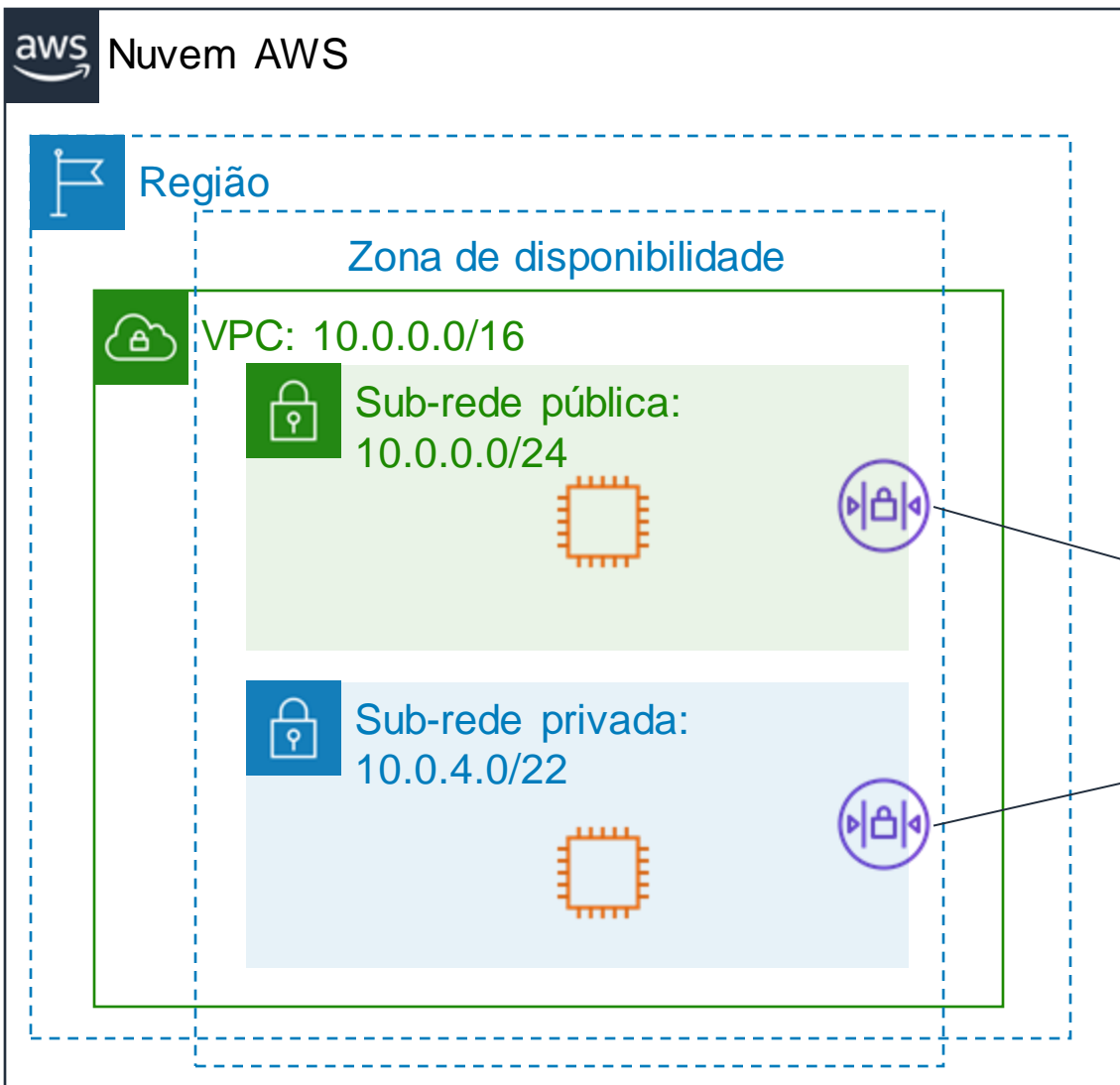
- Os grupos de segurança são **stateful**

Grupos de segurança personalizados

Entrada				
Tipo	Protocolo	Intervalo de portas	Origem	Descrição
HTTP	TCP	80	0.0.0.0/0	Todo o tráfego da web
HTTPS	TCP	443	0.0.0.0/0	Todo o tráfego da web
SSH	TCP	22	54.24.12.19/32	Endereço comercial
Saída				
Tipo	Protocolo	Intervalo de portas	Origem	Descrição
Todo tráfego	Todos	Todos	0.0.0.0/0	
Todo tráfego	Todos	Todos	::/0	

- Você pode **especificar regras de permissão**, mas não de negação.
- **Todas as regras são avaliadas** antes da decisão de permitir o tráfego.

Listas de controle de acesso à rede (ACLs de rede)



As ACLs de rede atuam
no **nível da sub-rede**.

Entrada					
Nº da regra	Tipo	Protocolo	Intervalo de portas	Origem	Permitir/Negar
100	Todo tráfego IPv4	Todos	Todos	0.0.0.0/0	PERMITIR
*	Todo tráfego IPv4	Todos	Todos	0.0.0.0/0	NEGAR
Saída					
Nº da regra	Tipo	Protocolo	Intervalo de portas	Origem	Permitir/Negar
100	Todo tráfego IPv4	Todos	Todos	0.0.0.0/0	PERMITIR
*	Todo tráfego IPv4	Todos	Todos	0.0.0.0/0	NEGAR

- Uma ACL de rede tem **regras de entrada e saída separadas**, e cada regra pode **permitir ou rejeitar tráfego**.
- As ACLs de rede **padrão permitem** todo o tráfego IPv4 de entrada e saída.
- As ACLs de rede são **stateless**.

ACLs de rede personalizadas

Entrada					
Nº da regra	Tipo	Protocolo	Intervalo de portas	Origem	Permitir/Negar
103	SSH	TCP	22	0.0.0.0/0	PERMITIR
100	HTTPS	TCP	443	0.0.0.0/0	PERMITIR
*	Todo tráfego IPv4	Todos	Todos	0.0.0.0/0	NEGAR
Saída					
Nº da regra	Tipo	Protocolo	Intervalo de portas	Origem	Permitir/Negar
103	SSH	TCP	22	0.0.0.0/0	PERMITIR
100	HTTPS	TCP	443	0.0.0.0/0	PERMITIR
*	Todo tráfego IPv4	Todos	Todos	0.0.0.0/0	NEGAR

- As ACLs de rede **personalizadas negam** todo o tráfego de entrada e saída até que você adicione regras.
- Você pode especificar regras **de permissão e negação**.
- As regras são avaliadas em ordem numérica, começando com o **menor número**.

Comparação entre grupos de segurança e ACLs de rede

Atributo	Grupos de segurança	ACLs de rede
Escopo	Nível da instância	Nível de sub-rede
Regras compatíveis	Permitir somente regras	Regras de permissão e negação
Estado	Stateful (o tráfego de retorno é permitido automaticamente, independentemente das regras)	Stateless (o tráfego de retorno deve ser explicitamente permitido pelas regras)
Ordem das regras	Todas as regras são avaliadas antes da decisão de permitir o tráfego	As regras são avaliadas em ordem numérica antes da decisão de permitir tráfego

Atividade: projetar uma VPC

Cenário: você tem uma pequena empresa com um site hospedado em uma instância do Amazon Elastic Compute Cloud (Amazon EC2). Você tem dados do cliente armazenados em um banco de dados de back-end que deseja manter privados. Você deseja usar a Amazon VPC para configurar uma VPC que atenda aos seguintes requisitos:

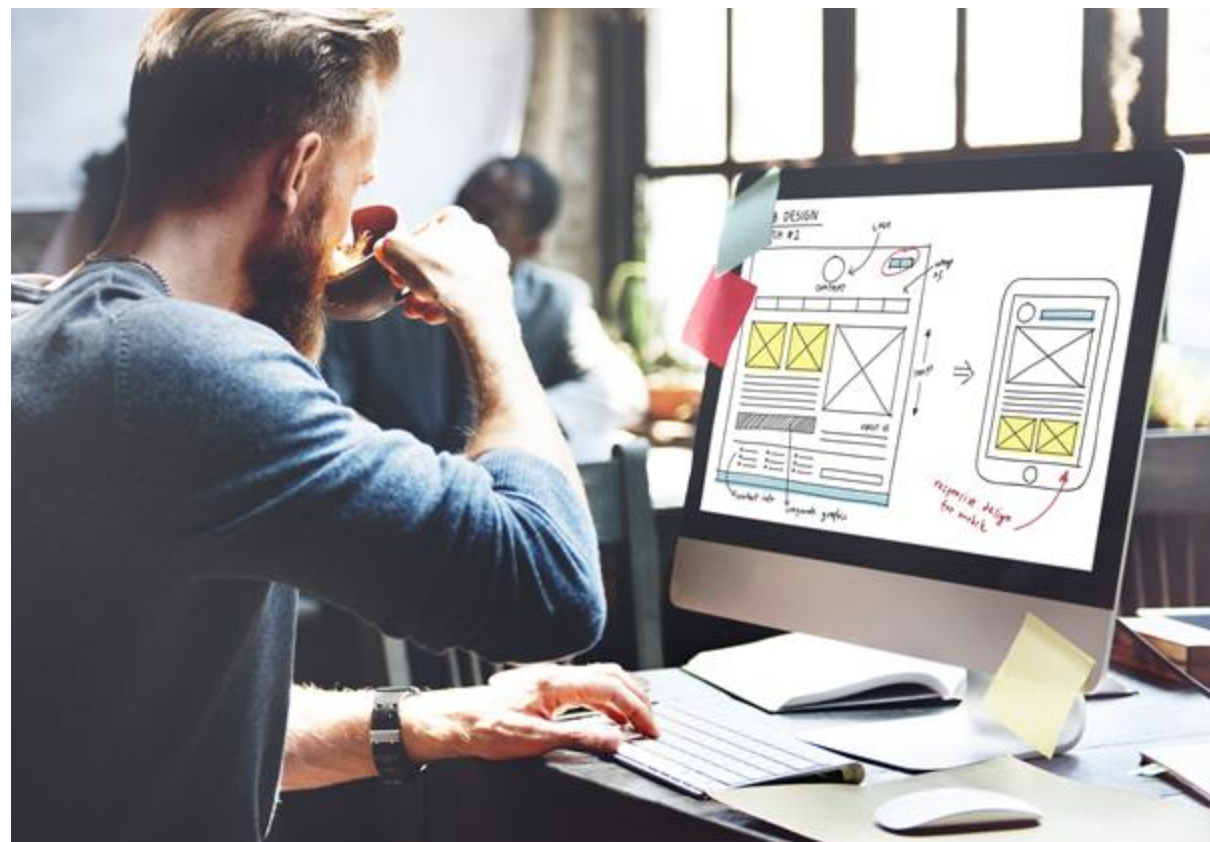
- O servidor web e o servidor de banco de dados devem estar em sub-redes separadas.
- O primeiro endereço da rede deve ser 10.0.0.0. Cada sub-rede deve ter um total de 256 endereços IPv4.
- Seus clientes devem sempre ser capazes de acessar seu servidor Web.
- Seu servidor de banco de dados deve ser capaz de acessar a Internet para fazer atualizações de patches.
- Sua arquitetura deve ser altamente disponível e usar pelo menos uma camada de firewall personalizada.

Principais lições da Seção 4



- Criar segurança em sua arquitetura de VPC:
 - Isolar sub-redes, se possível.
 - Escolher o dispositivo de gateway ou conexão VPN apropriado para suas necessidades.
 - Usar firewalls.
- Grupos de segurança e ACLs de rede são opções de firewall que você pode usar para proteger sua VPC.

Laboratório 2: Crie uma VPC e inicie um servidor Web



Laboratório 2: Cenário

Neste laboratório, você usa a Amazon VPC para **criar sua própria VPC** e adicionar alguns componentes para produzir uma rede personalizada. Você **cria um grupo de segurança** para sua VPC. Você também **cria uma instância do EC2** e a **configura** para executar um servidor web e usar o grupo de segurança. Em seguida, execute a instância do EC2 na VPC.



Amazon
VPC



Amazon
EC2

Laboratório 2: Tarefas



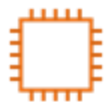
- Criar uma VPC



- Criar sub-redes adicionais.

Grupo de
segurança

- Criar um grupo de segurança da VPC.



- Iniciar uma instância de servidor Web.

Laboratório 2: Produto final

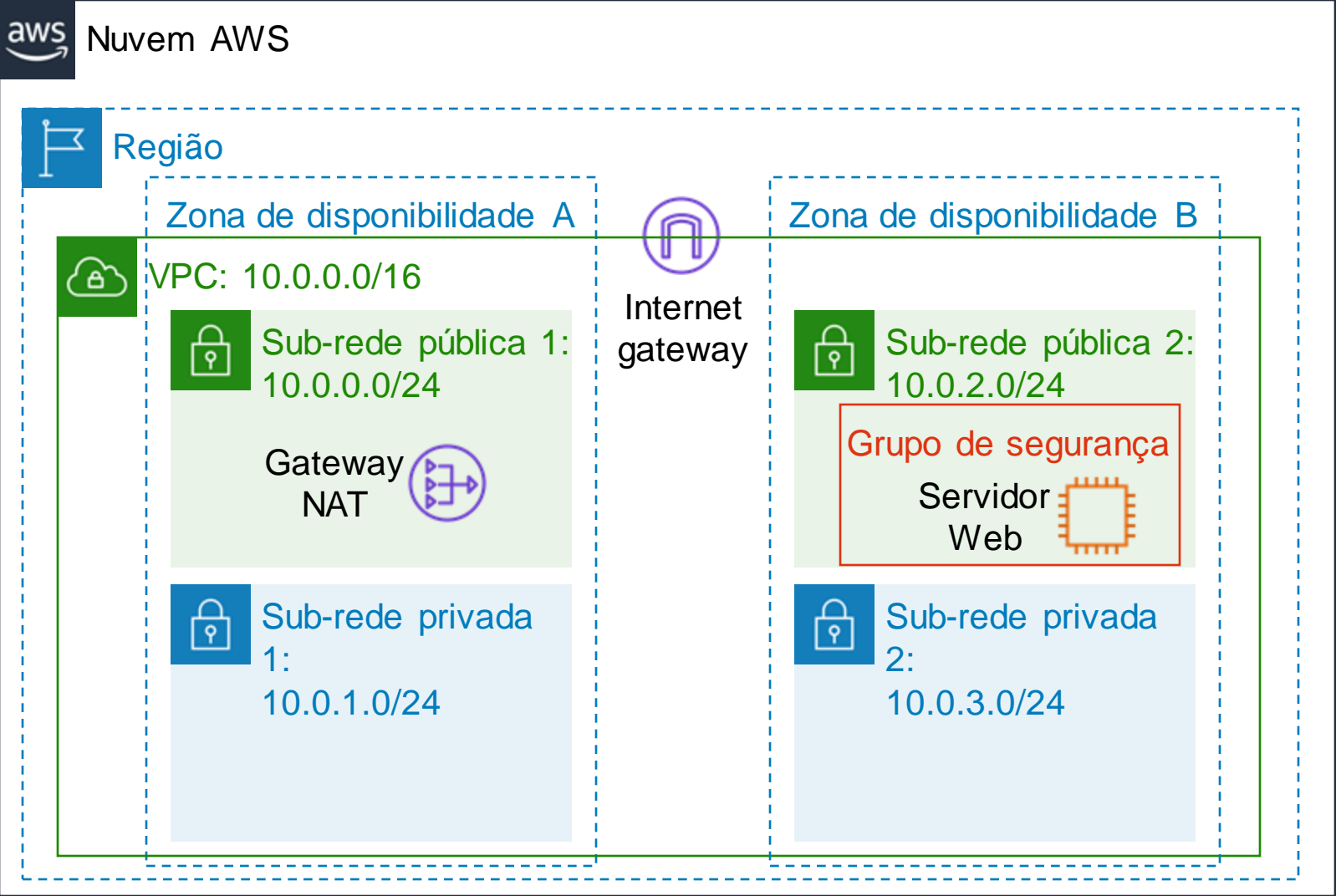


Tabela de rotas


Destino	Destino
10.0.0.0/16	Local
0.0.0.0/0	Gateway da Internet

Tabela de rotas

Destino	Destino
10.0.0.0/16	Local
0.0.0.0/0	Gateway NAT



Aproximadamente 30 minutos

A top-down photograph of a teal ceramic coffee cup filled with dark coffee, topped with a layer of white foam. The cup sits on a matching teal saucer. To the left of the cup is a wooden scoop filled with dark brown coffee beans, with several beans scattered on the dark, textured surface next to it. A light-colored cloth is partially visible on the left side.

Inicie o Laboratório 2: crie sua VPC e execute um servidor web

Resumo do laboratório: principais lições



Módulo 5: Redes e entrega de conteúdo

Seção 5: Amazon Route 53

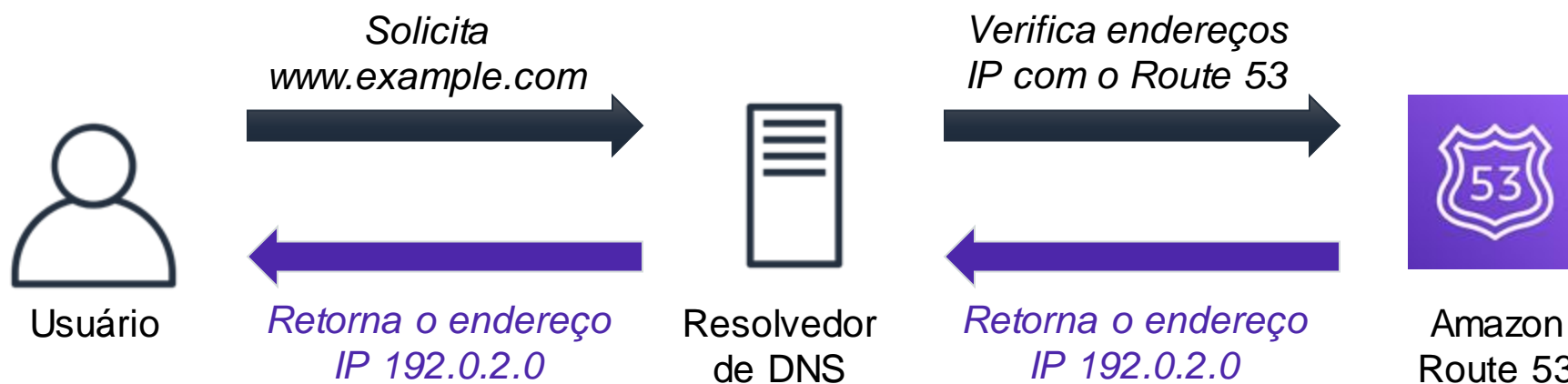
Amazon Route 53



Amazon
Route 53

- É um servidor Web do Domain Name System (DNS) altamente disponível e escalável
- É usado para rotear usuários finais para aplicativos da Internet ao traduzir nomes (como www.exemplo.com) em endereços IP numéricos (como `192.0.2.1`) que os computadores usam para se conectarem uns aos outros
- É totalmente compatível com IPv4 e IPv6
- Conecta solicitações de usuários à infraestrutura executada na AWS e também fora da AWS
- É usado para verificar a integridade de seus recursos
- Recursos de fluxo de tráfego
- Permite registrar nomes de domínio

Resolução de DNS do Amazon Route 53



Roteamento compatível com o Amazon Route 53



- **Roteamento simples** - use em ambientes de servidor único
- **Roteamento ponderado Round Robin** - atribua pesos a conjuntos de registros de recursos para especificar a frequência
- **Roteamento de latência** - ajude a melhorar seus aplicativos globais
- **Roteamento de localização geográfica** - roteie o tráfego com base na localização de seus usuários
- **Roteamento de geoproximidade** - roteie o tráfego com base na localização de seus recursos
- **Roteamento de failover** - faça failover para um site de backup se o site principal se tornar inacessível
- **Roteamento de resposta com valores múltiplos** - responda a consultas DNS com até oito registros íntegros selecionados aleatoriamente

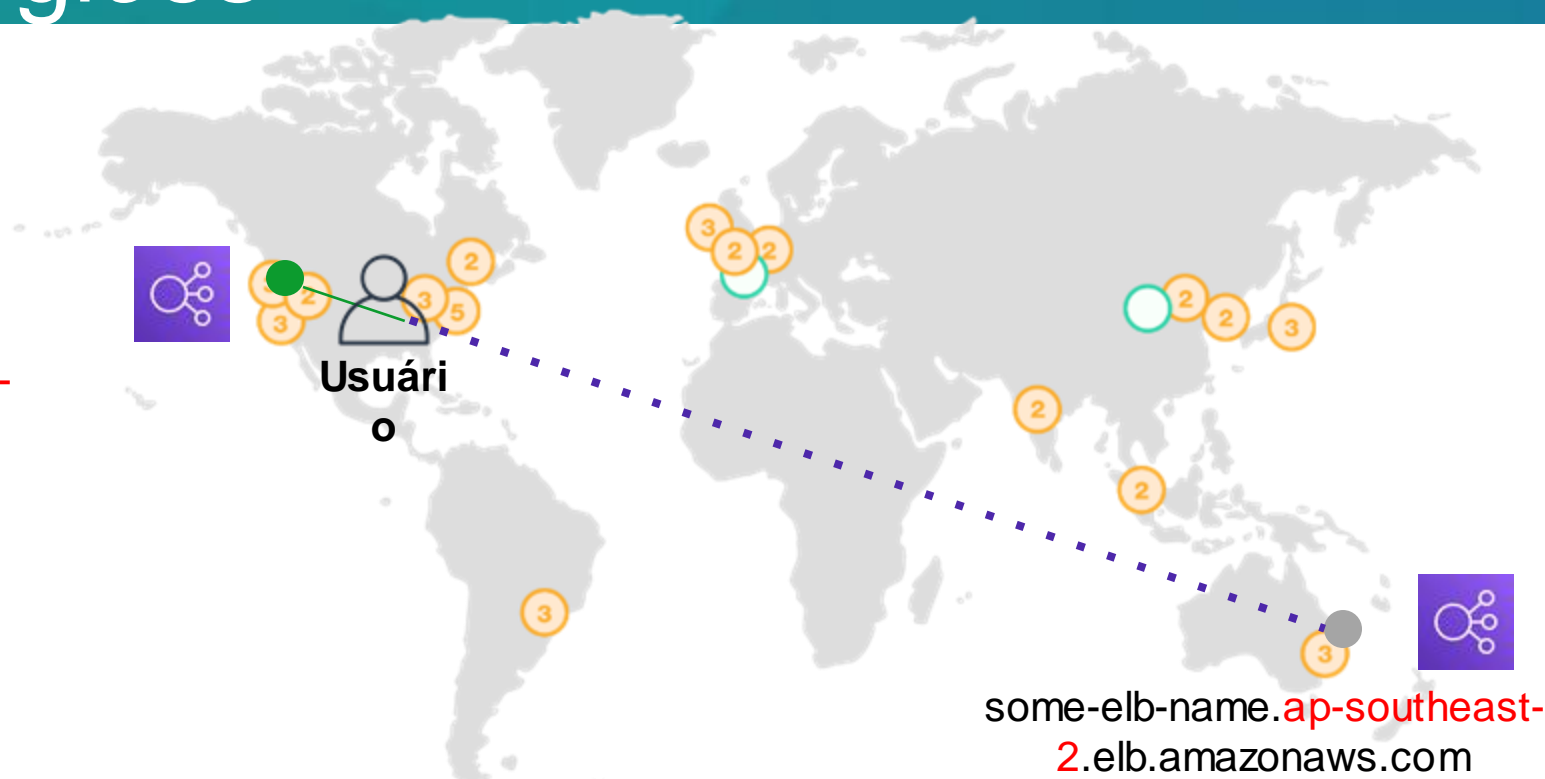
Caso de uso: implantação em várias regiões



Amazon Route

53

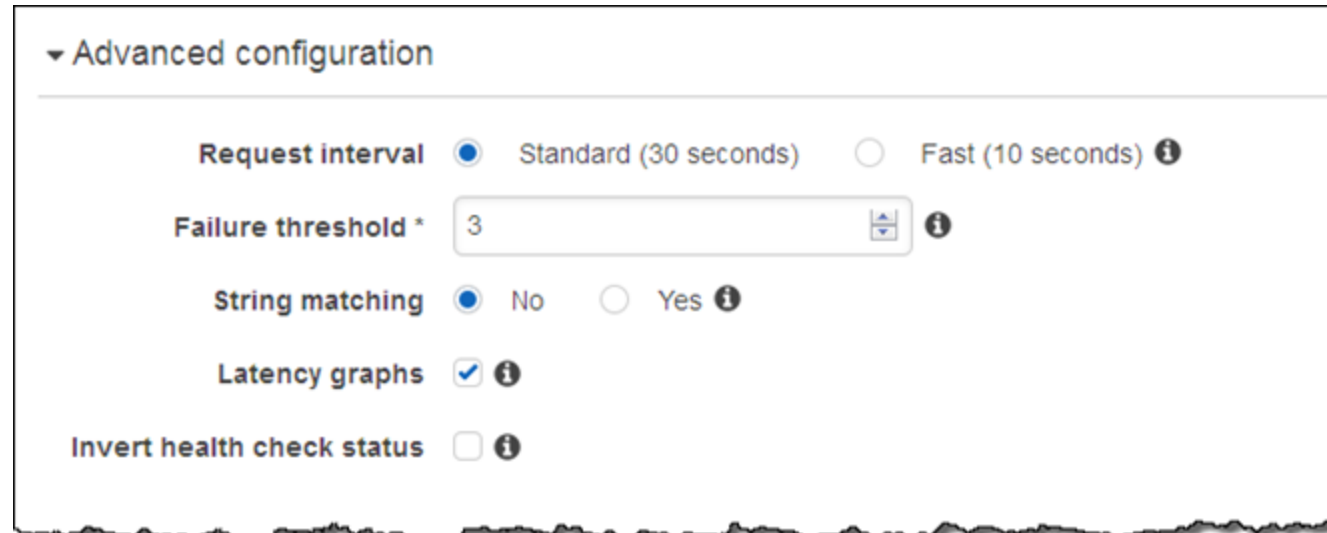
some-elb-name.us-west-
2.elb.amazonaws.com



Nome	Tipo	Valor
example.com	ALIAS	some-elb-name.us-west-2.elb.amazonaws.com
example.com	ALIAS	some-elb-name.ap-southeast-2.elb.amazonaws.com

Melhore a disponibilidade dos aplicativos executados na AWS:

- Configurando cenários de backup e failover para seus próprios aplicativos
- Habilitando arquiteturas multirregião altamente disponíveis na AWS
- Criação de verificações de integridade



▼ Advanced configuration

Request interval ☒ Standard (30 seconds) ☐ Fast (10 seconds) ⓘ

Failure threshold * ⓘ

String matching ☒ No ☐ Yes ⓘ

Latency graphs ☒ ⓘ

Invert health check status ☐ ⓘ

Failover de DNS para um aplicativo web multicamadas

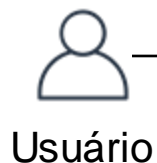
Conjuntos de registros

CNAME www

elastic_load_balancer
Política de roteamento =
Failover
Tipo de registro = Principal

Site do Amazon S3
Política de roteamento =
Failover

Tipo de registro = Secundário



Usuário



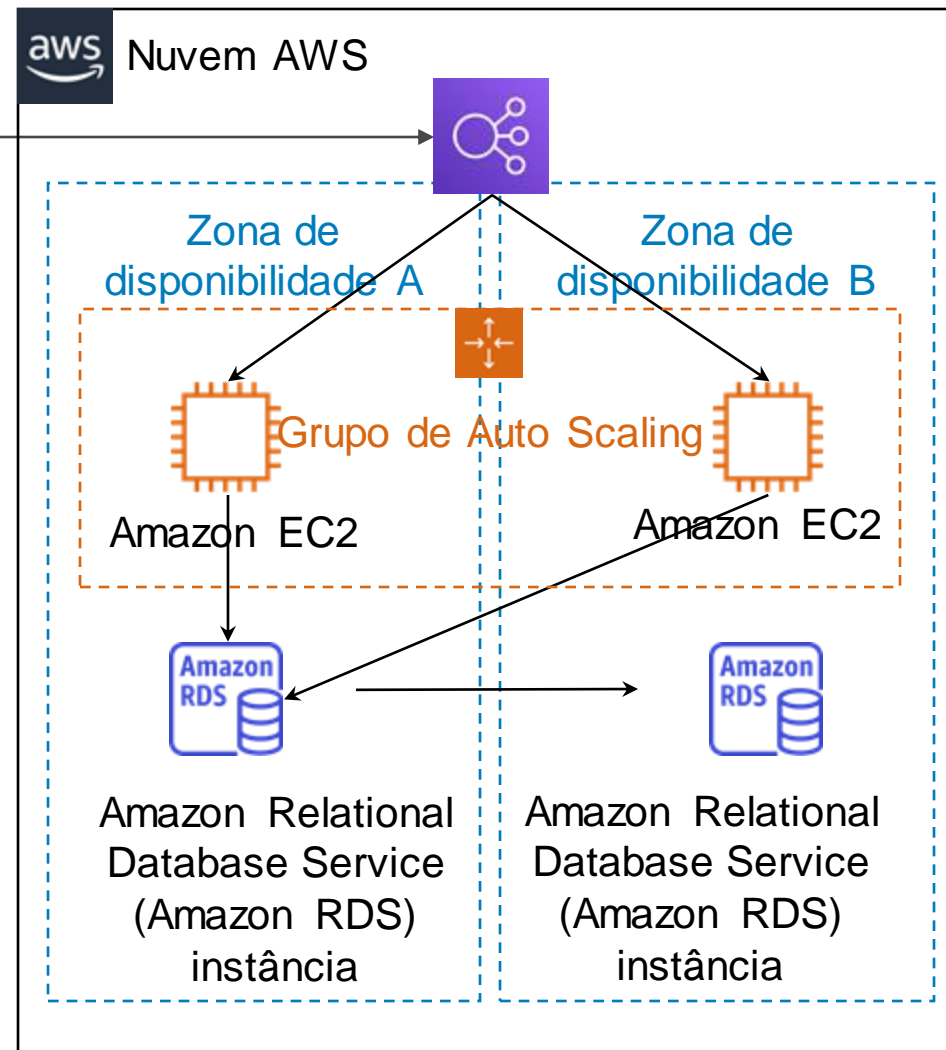
Amazon
Route 53

Primário

Secundário



Site estático
do Amazon S3



Principais lições da seção 5

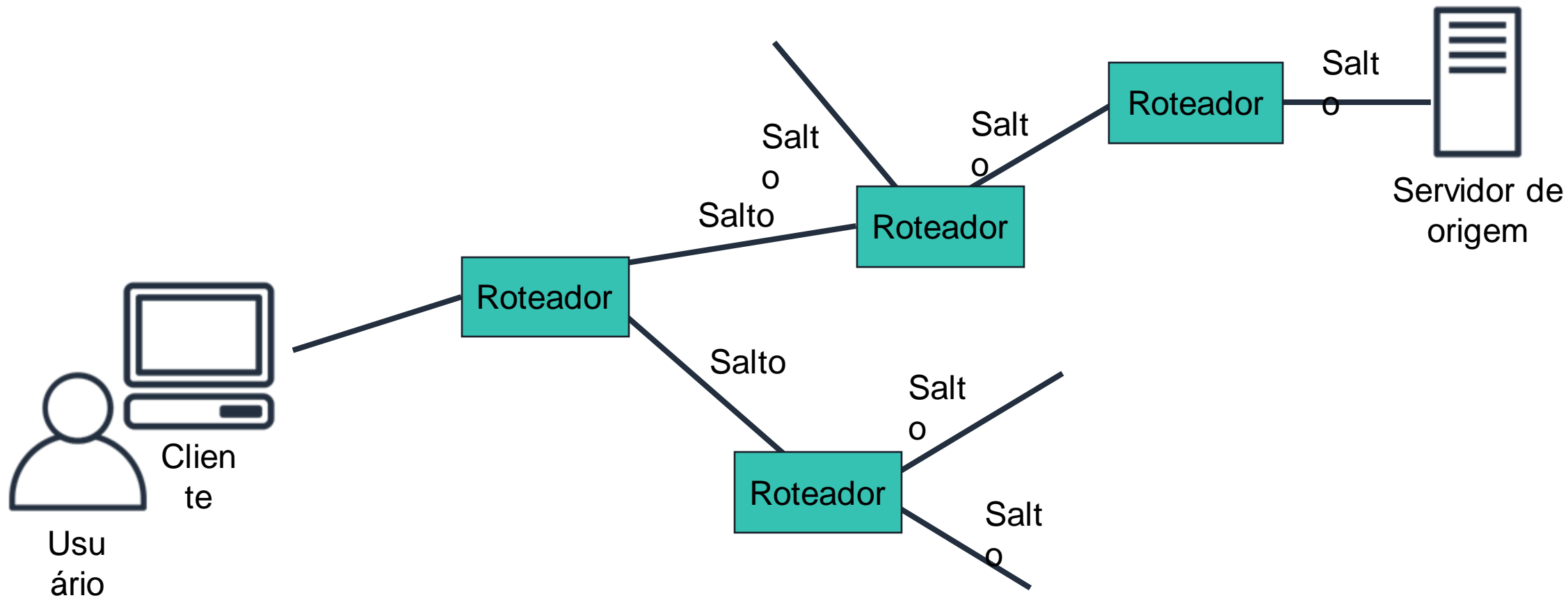


- O Amazon Route 53 é um serviço web de DNS na nuvem altamente disponível e escalável que converte nomes de domínio em endereços IP numéricos.
- O Amazon Route 53 oferece suporte a vários tipos de políticas de roteamento.
- A implantação em várias regiões melhora o desempenho do aplicativo para um público global.
- Você pode usar o failover do Amazon Route 53 para melhorar a disponibilidade dos seus aplicativos.

Módulo 5: Redes e entrega de conteúdo

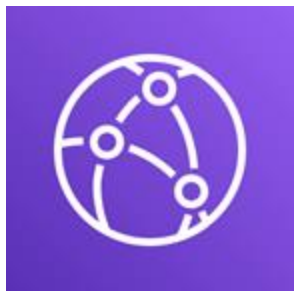
Seção 6: Amazon CloudFront

Entrega de conteúdo e latência de rede



Rede de entrega de conteúdo (CDN)

- É um sistema distribuído globalmente de servidores de armazenamento em cache
- Armazena cópias de arquivos comumente solicitados (conteúdo estático) em cache
- Fornece uma cópia local do conteúdo solicitado de um ponto de presença ou ponto de presença de cache próximo
- Acelera a entrega de conteúdo dinâmico
- Melhora o desempenho e a escalabilidade do aplicativo



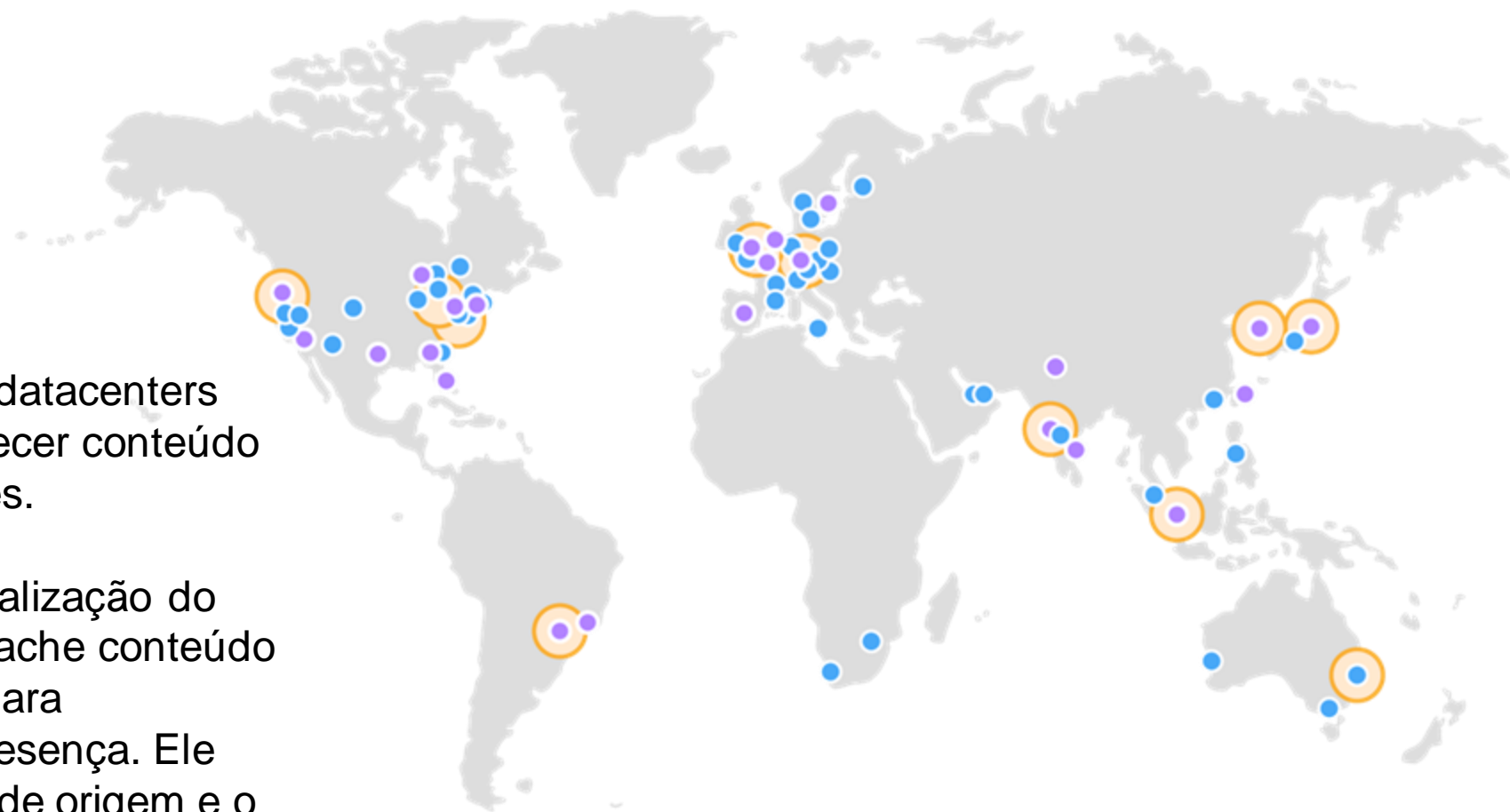
Amazon
CloudFront

- Serviço de CDN rápido, global e seguro
- Rede global de pontos de presença e pontos de presença de caches regionais
- Modelo de autoatendimento
- Definição de preço com pagamento conforme o uso

Infraestrutura Amazon CloudFront

- Pontos de presença
- Vários pontos de presença
- Caches de borda regionais

- **Pontos de presença** - rede de datacenters que o CloudFront usa para fornecer conteúdo popular rapidamente aos clientes.
- **Cache de ponto regional** - Localização do CloudFront que armazena em cache conteúdo que não é popular o suficiente para permanecer em um ponto de presença. Ele está localizado entre o servidor de origem e o ponto de presença global.



Benefícios do Amazon CloudFront



- Rápido e global
- Segurança na borda
- Altamente programável
- Profundamente integrado à AWS
- Econômico

"Definição de preços do Amazon CloudFront"

Transferência de dados para fora

- Cobrado pelo volume de dados transferidos do ponto de presença do Amazon CloudFront para a Internet ou para sua origem.

Solicitações HTTP (S)

- Cobrado pelo número de solicitações HTTP (S).

Solicitações de invalidação

- Não há cobrança adicional para os primeiros 1.000 caminhos solicitados para invalidação a cada mês. Depois disso, 0,005 USD por caminho solicitado para invalidação.

IP dedicado SSL personalizado

- 600 USD por mês para cada certificado SSL personalizado associado com uma ou mais distribuições do CloudFront usando a versão com IP dedicado do suporte de certificado SSL personalizado.

Principais lições da Seção 6



- Uma CDN é um sistema distribuído globalmente de servidores de armazenamento em cache que acelera a entrega de conteúdo.
- O Amazon CloudFront é um serviço de CDN rápido que entrega dados, vídeos, aplicativos e APIs com segurança em uma infraestrutura global com baixa latência e altas velocidades de transferência.
- O Amazon CloudFront oferece muitos benefícios.

Módulo 5: Redes e entrega de conteúdo

Conclusão do módulo

Resumindo, neste módulo você aprendeu a:

- Reconhecer os conceitos básicos de redes
- Descrever as redes virtuais na nuvem com a Amazon VPC
- Rotular um diagrama de rede
- Projetar uma arquitetura básica de VPC
- Indicar as etapas para criar uma VPC
- Identificar grupos de segurança
- Crie sua própria VPC e adicione componentes adicionais a ela para produzir uma rede personalizada
- Identificar os fundamentos do Amazon Route 53
- Reconhecer os benefícios do Amazon CloudFront

Conclua o teste de conhecimento



Exemplo de pergunta do exame

Qual serviço de rede da AWS permite que uma empresa crie uma rede virtual dentro da AWS?

- A. AWS Config
- B. Amazon Route 53
- C. AWS Direct Connect
- D. Amazon VPC

- [Página de visão geral da Amazon VPC](#)
- Artigo técnico [Amazon Virtual Private Cloud Connectivity Options](#)
- Publicação no blog de arquitetura da AWS [One to Many: Evolving VPC Design](#)
- [Guia do usuário da Amazon VPC](#)
- [Página de visão geral do Amazon CloudFront](#)

Obrigado

© 2019 Amazon Web Services, Inc. ou suas afiliadas. Todos os direitos reservados. Este trabalho não pode ser reproduzido ou redistribuído, no todo ou em parte, sem a permissão prévia por escrito da Amazon Web Services, Inc. É proibido copiar, emprestar ou vender para fins comerciais. Para correções ou comentários sobre o curso, envie um e-mail para: aws-course-feedback@amazon.com. Para todas as outras perguntas, entre em contato conosco em: <https://aws.amazon.com/contact-us/aws-training/>. Todas as marcas comerciais pertencem a seus proprietários.

