

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

Módulo 5: Redes e entrega de conteúdo

Módulo 5: Redes e entrega de conteúdo

Seção 2: Amazon VPC

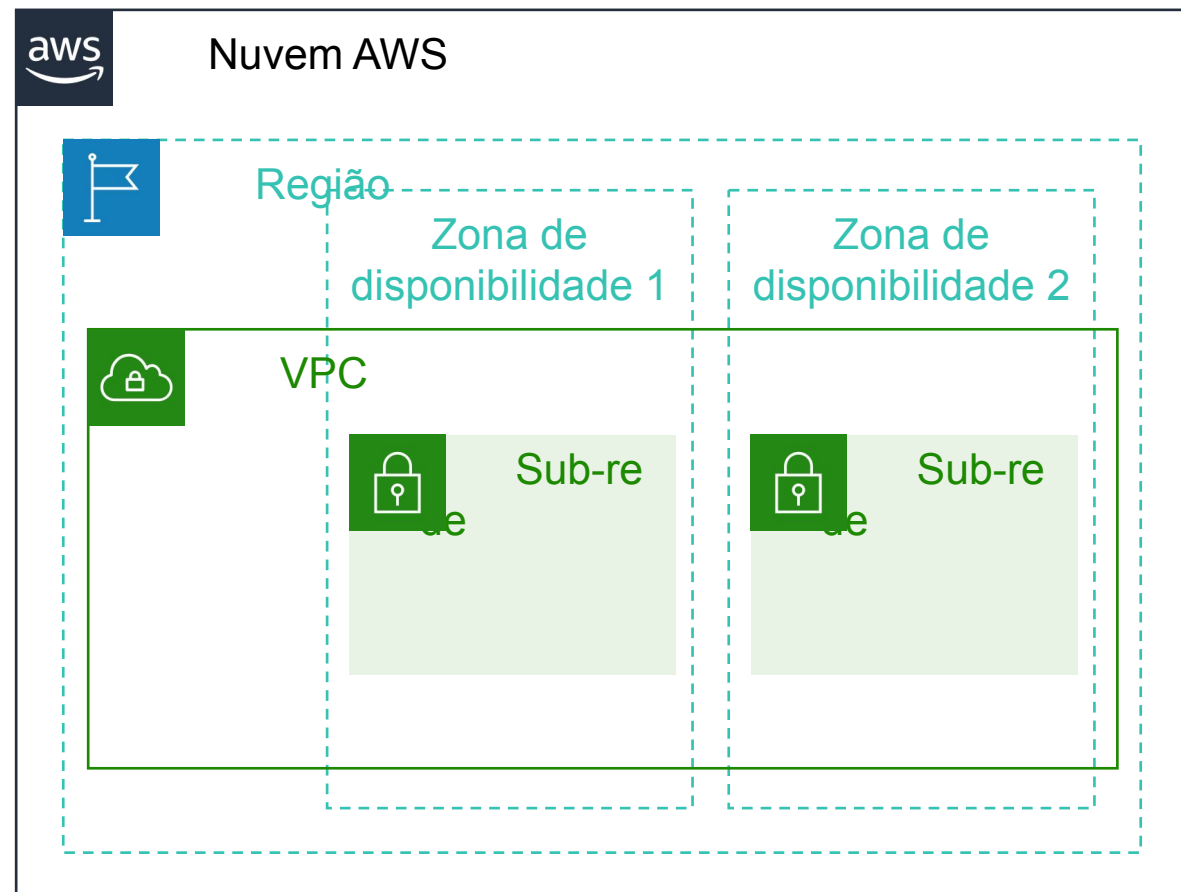


Amazon
VPC


- 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

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

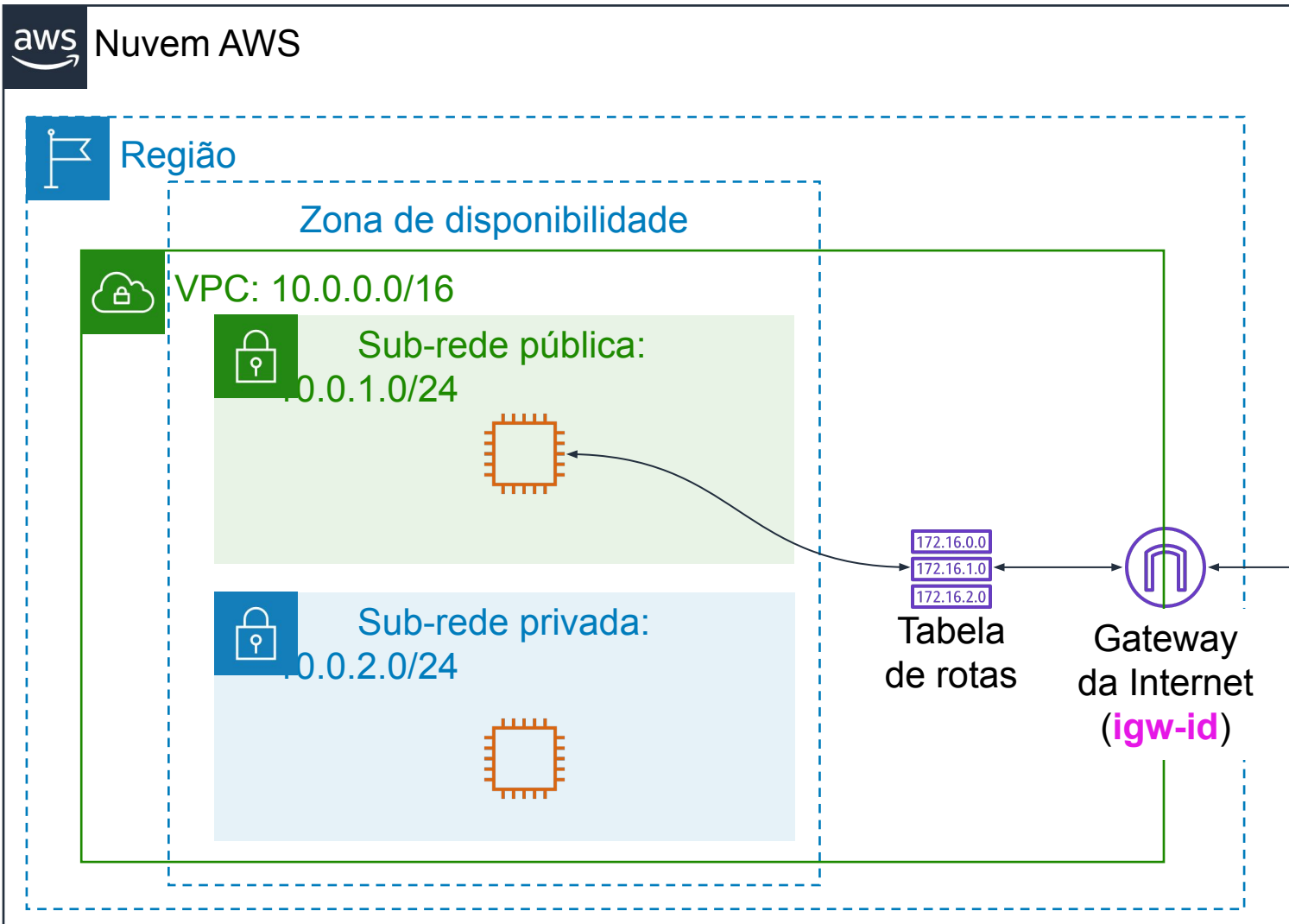
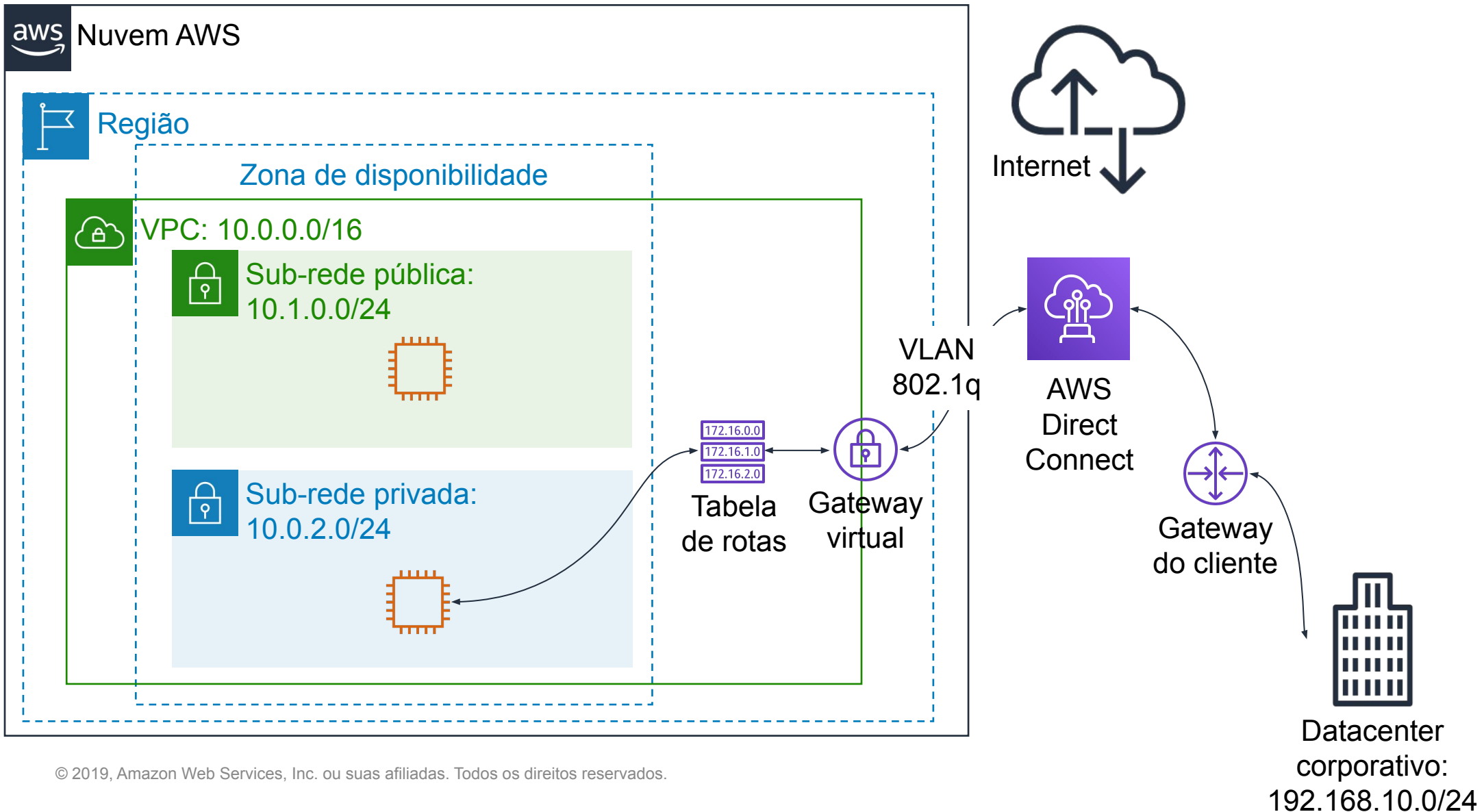


Tabela de rotas da sub-rede pública

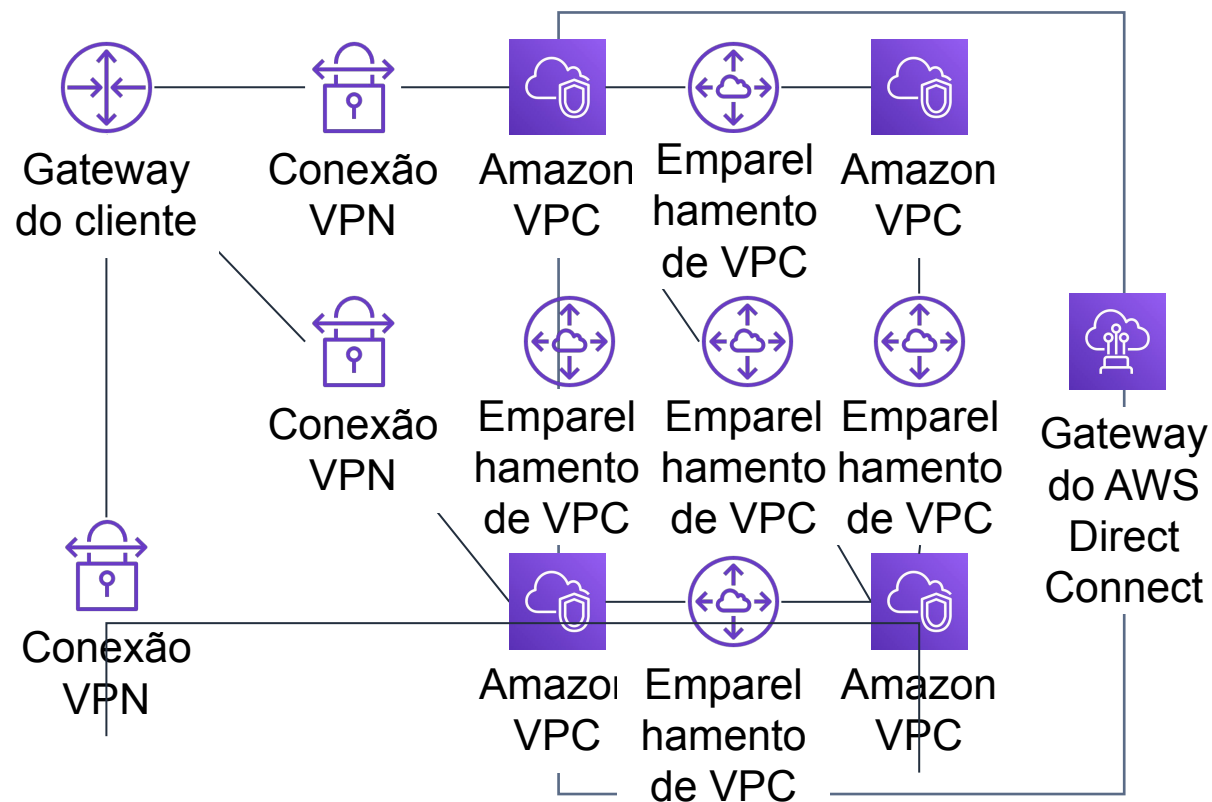
Destino	Destino
10.0.0.0/16	local
0.0.0.0/0	igw-id

AWS Direct Connect

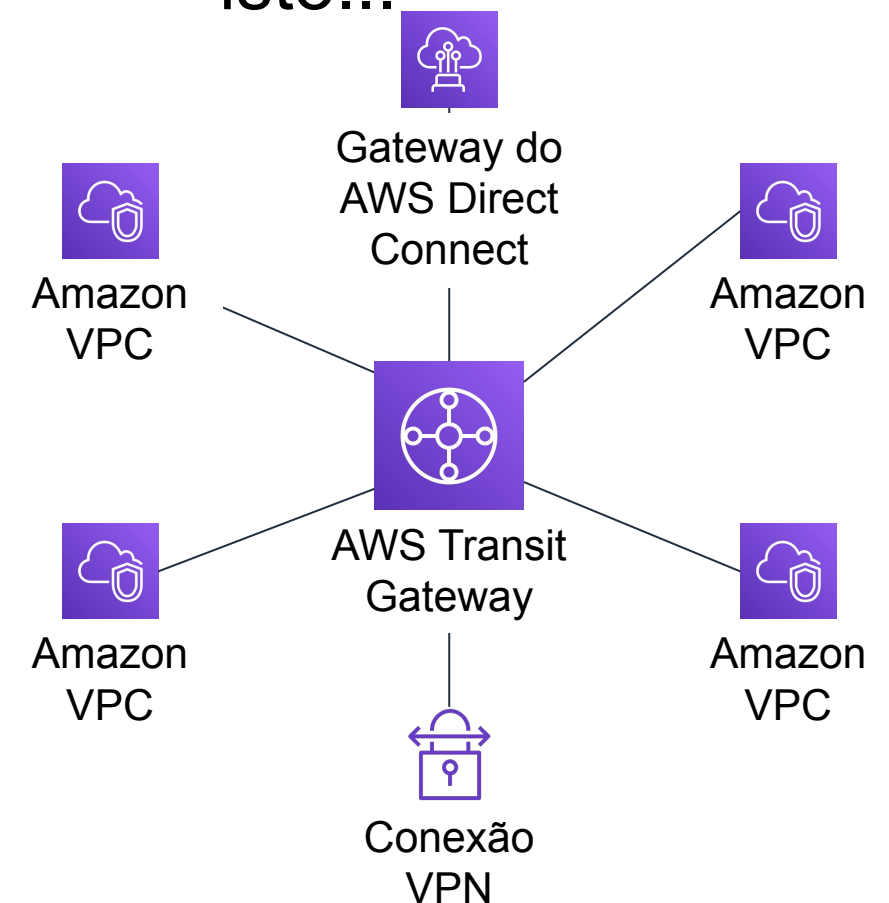


AWS Transit Gateway

Disto...



Para isto...



Principais lições da Seção 3

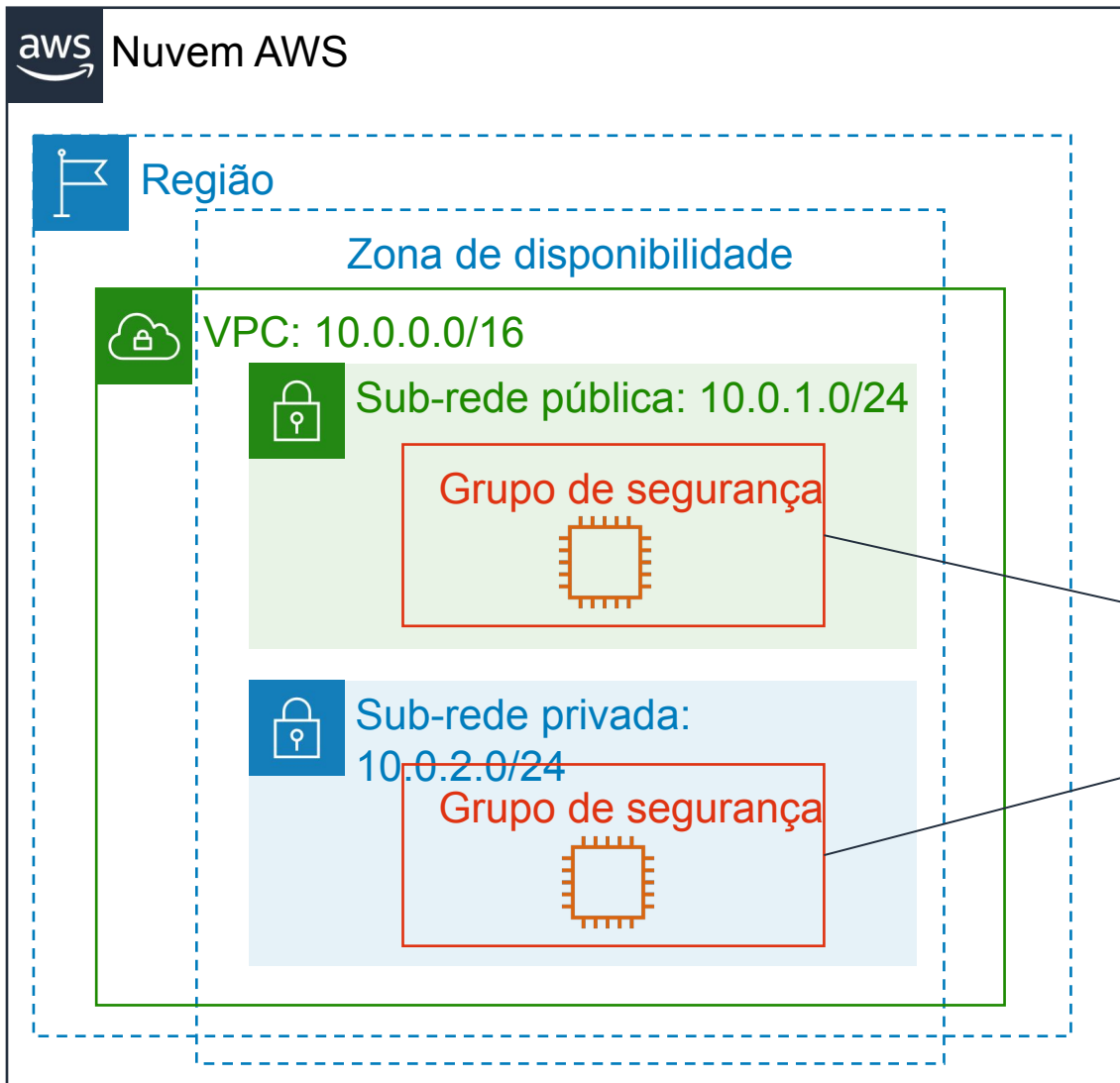


- Existem várias opções de rede da VPC, que incluem:
 - Gateway da Internet
 - AWS Direct Connect
 - AWS Transit Gateway
- Você pode usar o assistente da VPC para implementar seu projeto.

Módulo 5: Redes e entrega de conteúdo

Seção 4: Segurança da VPC

Grupos de segurança



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

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.

Módulo 5: Redes e entrega de conteúdo

Seção 5: 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



Principais lições da seção 5

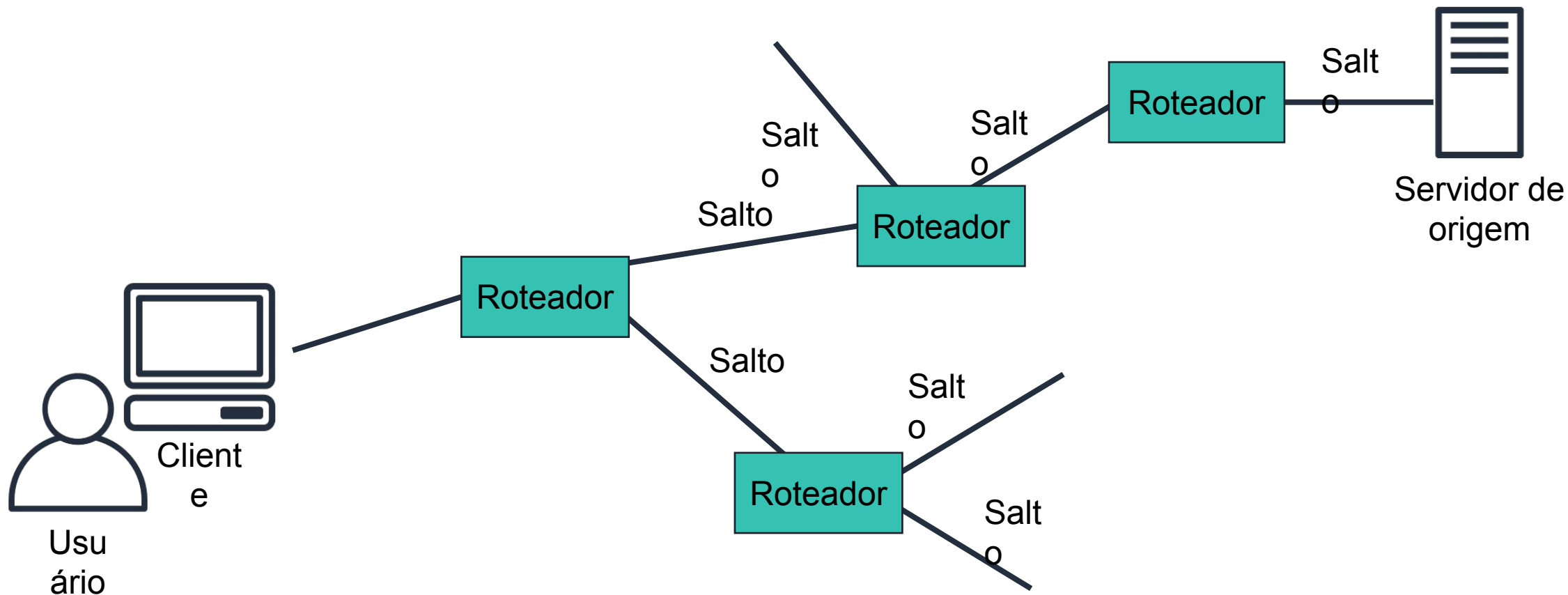


- O Amazon Route 53 é um serviço web de DNS na nuvem altamente disponível e escalável que converte nomes de domínio em endereços IP numéricos.
- O Amazon Route 53 oferece suporte a vários tipos de políticas de roteamento.
- A implantação em várias regiões melhora o desempenho do aplicativo para um público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



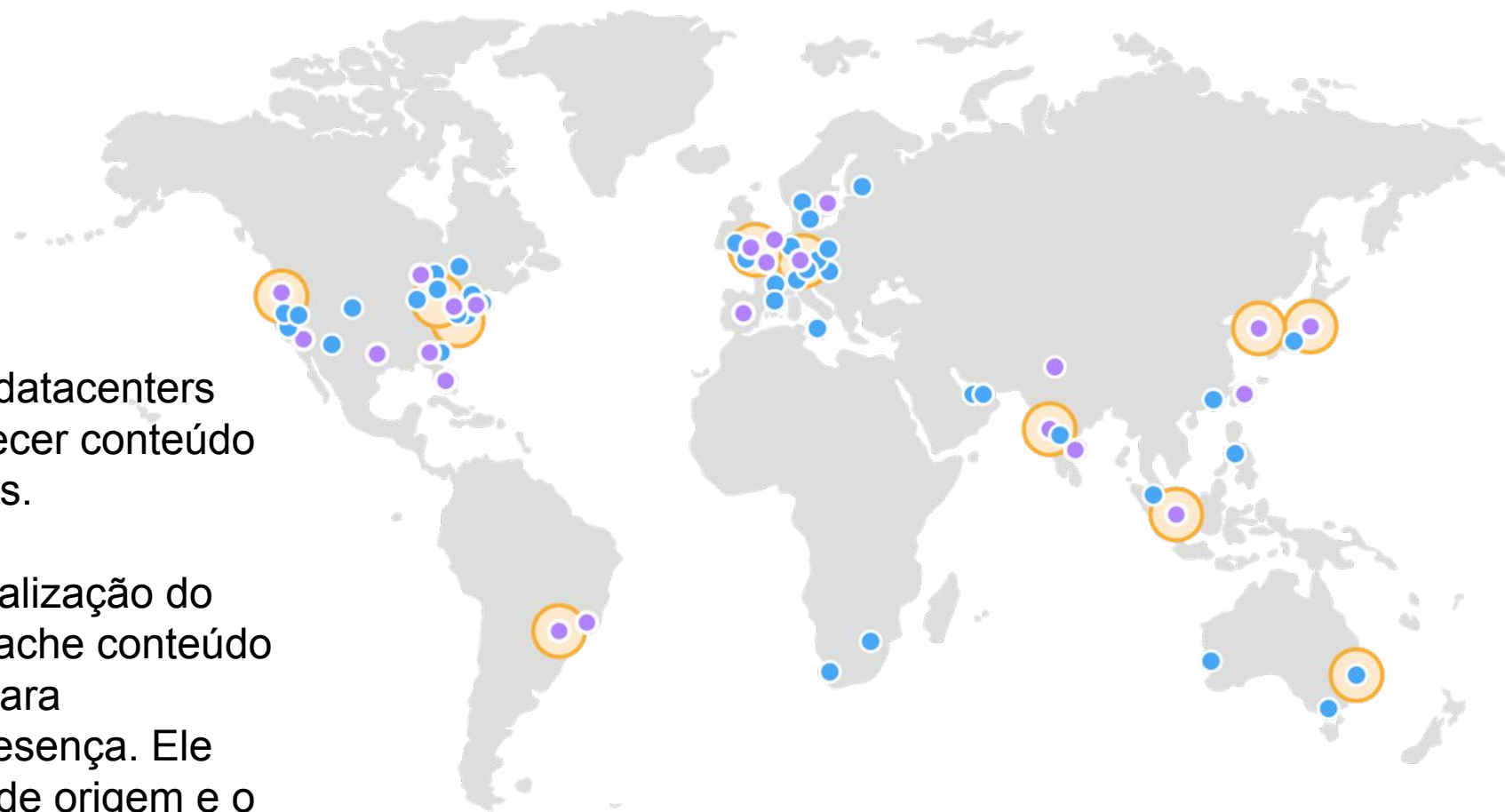
Amazon
CloudFront

- 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.

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