Semana 3

Semana 3

Declaração de tarefa 1.2: Projetar cargas de trabalho e aplicações seguras.

Conhecimento sobre:

- Configuração de aplicações e segurança de credenciais.
- Endpoints de serviço da AWS.
- Controle de portas, protocolos e tráfego de rede na AWS.
- Acesso seguro a aplicações.
- Serviços de segurança com casos de uso apropriados (por exemplo, Amazon Cognito, Amazon GuardDuty, Amazon Macie).
- Vetores de ameaças externos à AWS (por exemplo, DDoS, SQL injection).

Habilidades em:

- Projetar arquiteturas de VPC com componentes de segurança (por exemplo, security groups, tabelas de rotas, ACLs de rede, gateways NAT).
- Determinar estratégias de segmentação de rede (por exemplo, usando sub-redes públicas e privadas).
- Integrar serviços da AWS para proteger aplicações (por exemplo, AWS Shield, AWS WAF, IAM Identity Center, AWS Secrets Manager).
- Proteger conexões de rede externas de e para a nuvem AWS (por exemplo, VPN, AWS Direct Connect).

Do slide anterior, se formos extrair um grupo de palavras muito importantes para estudarmos, quais seriam?

- Endpoints de serviços;
- Amazon Cognito
- Amazon Macie
- Amazon GuardDuty
- Como evitamos DDoS e SQL Injection?
- Security Groups
- Tabela de rotas
- ACLs de rede
- Gateways NAT
- Subredes públicas e privadas
- AWS Shield, AWS WAF e AWS Secrets Manager
- Arquiteturas híbridas (on-prem e nuvem)

VPC

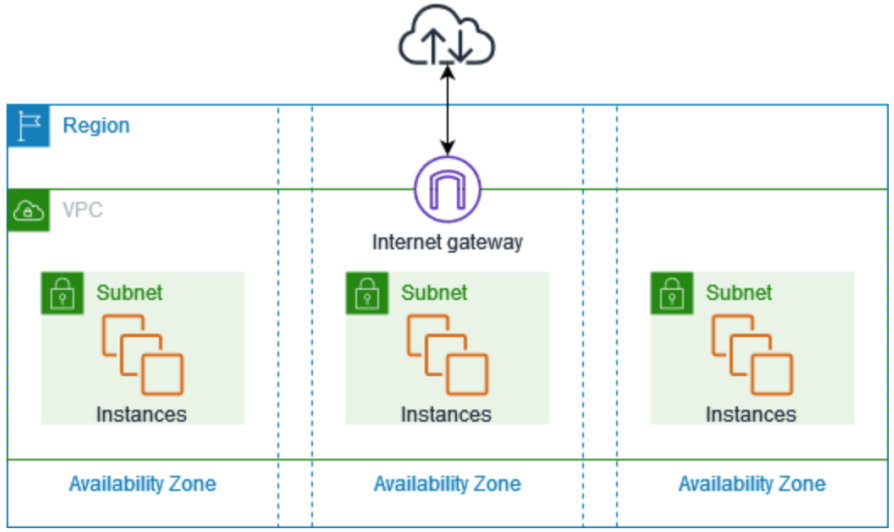
- Importante ressaltar: uma sub-rede por AZ
- A VPC está em várias Azs
- Internet gateway para integrar com a Internet

O que é Amazon VPC?

PDF | RSS

Com a Amazon Virtual Private Cloud (Amazon VPC), é possível iniciar recursos da AWS em uma rede virtual definida por você. Essa rede virtual se assemelha a uma rede tradicional que você operaria no seu data center, com os benefícios de usar a infraestrutura dimensionável da AWS.

O seguinte diagrama mostra uma VPC de exemplo. A VPC tem uma sub-rede em uma das zonas de disponibilidade na região, instâncias do EC2 em cada sub-rede e um gateway da Internet para permitir a comunicação entre os recursos em sua VPC e a Internet.



Virtual Private Cloud

- CIDR: Classless Inter-Domain Routing -> Faixa de endereços de IP disponíveis nessa rede privada.

- Não é possível alterar um bloco CIDR primário após a criação da VPC.

Blocos CIDR IPv4 da VPC

Ao criar uma VPC, você deve especificar um bloco CIDR IPv4 para a VPC. O tamanho permitido para o bloco é entre uma máscara de rede `/16` (65.536 endereços IP) e uma máscara de rede `/28` (16 endereços IP). Depois de criar a VPC, você pode associar blocos CIDR IPv4 adicionais à VPC. Para obter mais informações, consulte Adicionar ou remover um bloco CIDR da sua VPC.

Quando você cria uma VPC, é recomendável especificar um bloco CIDR dos intervalos de endereços IPv4 privados conforme especificado em RFC 1918:

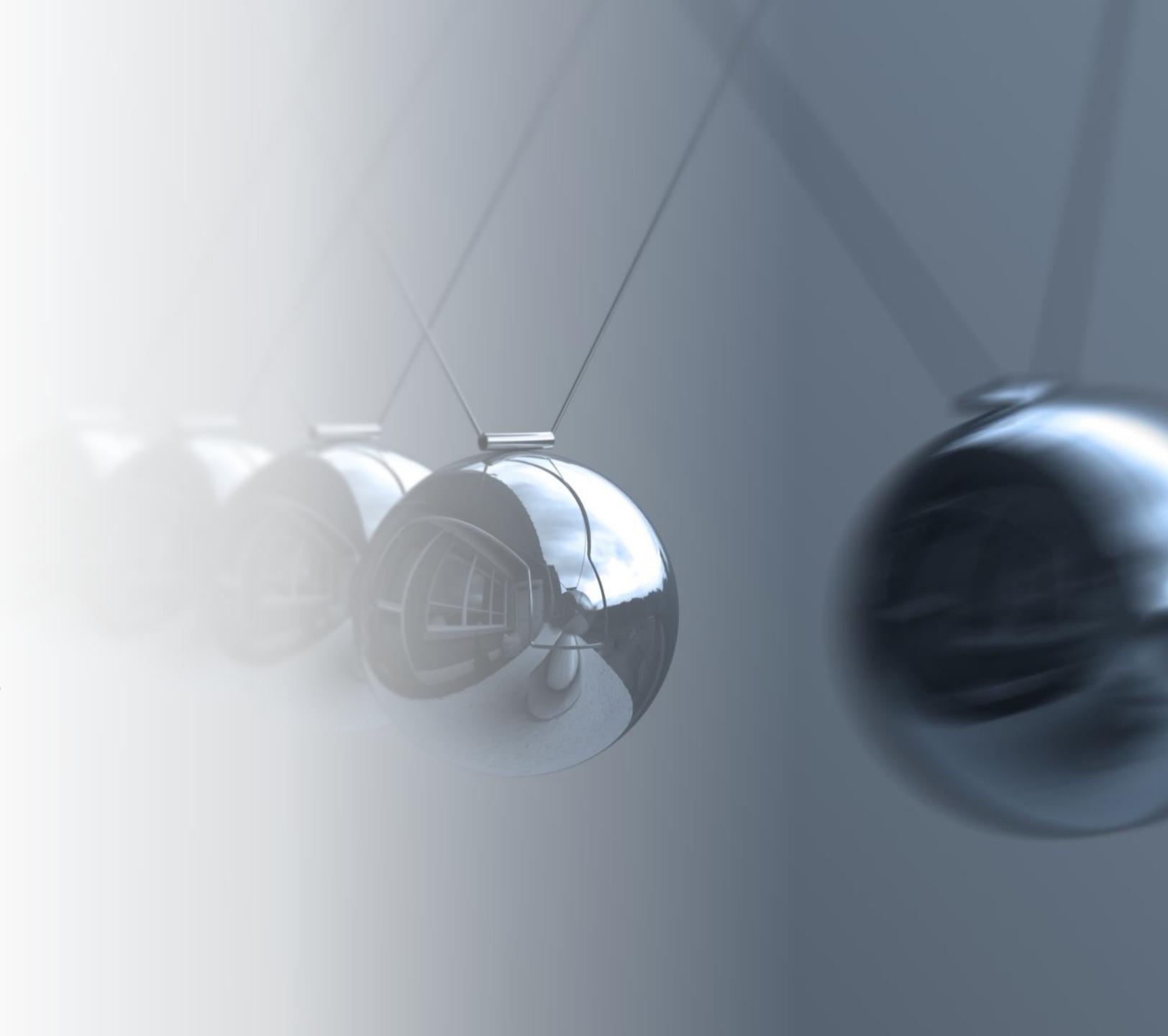
Intervalo do RFC 1918	Bloco CIDR de exemplo
10.0.0.0 - 10.255.255.255 (prefixo 10/8)	10.0.0.0/16
172.16.0.0 - 172.31.255.255 (prefixo 172.16/12)	172.31.0.0/16
192.168.0.0 - 192.168.255.255 (prefixo 192.168/16)	192.168.0.0/20

Quando crio uma VPC, o que vem por padrão?

- VPC vem com NACL (Netowrk Access Control List) padrão -> permite tráfego de entrada e saída
- NACLs customizadas negam todo o tráfego de entrada e saída (até adicionarmos regras)
- Importante reforçar: uma ACL de rede controla o tráfego em nível de sub-rede. Um security group controla o tráfego em nível de um recurso da AWS (EC2, por exemplo).
- Não podemos alterar o bloco CIDR primário após criação da VPC. Mas Podemos criar blocos secundários.

Componentes

(1) Internet gateways (ou virtual private gateways), (2) route tables, (3) network access control lists, (4) subnets e (5) security groups



Sub-rede (subnet)

- Precisa estar associada a uma NACL (access control list – lista de controle de acesso);
- Caso não associemos a uma ACL, será associada automaticamente à default;
- Uma sub-rede tem relação 1 para 1 com uma AZ (Zona de Disponibilidade);
- É um container lógico dentro da nossa rede;

Sub-rede (subnet)

- “Se uma sub-rede estiver associada a uma tabela de rotas que tem uma rota para um gateway da Internet, ela é conhecida como *sub-rede pública*. Se uma sub-rede estiver associada a uma tabela de rotas que não tem uma rota para um gateway da Internet, ela é conhecida como *sub-rede privada*.”

- Interessante aqui observer que o conceito de sub-rede pública ou privada está associada a tabela de rotas e o gateway da Internet.

- **Referência:** https://docs.aws.amazon.com/pt_br/vpc/latest/userguide/vpc-igw-internet-access.html

Internet Gateways

Permite que a VPC tenha um IP público e se conecte à Internet

gateway

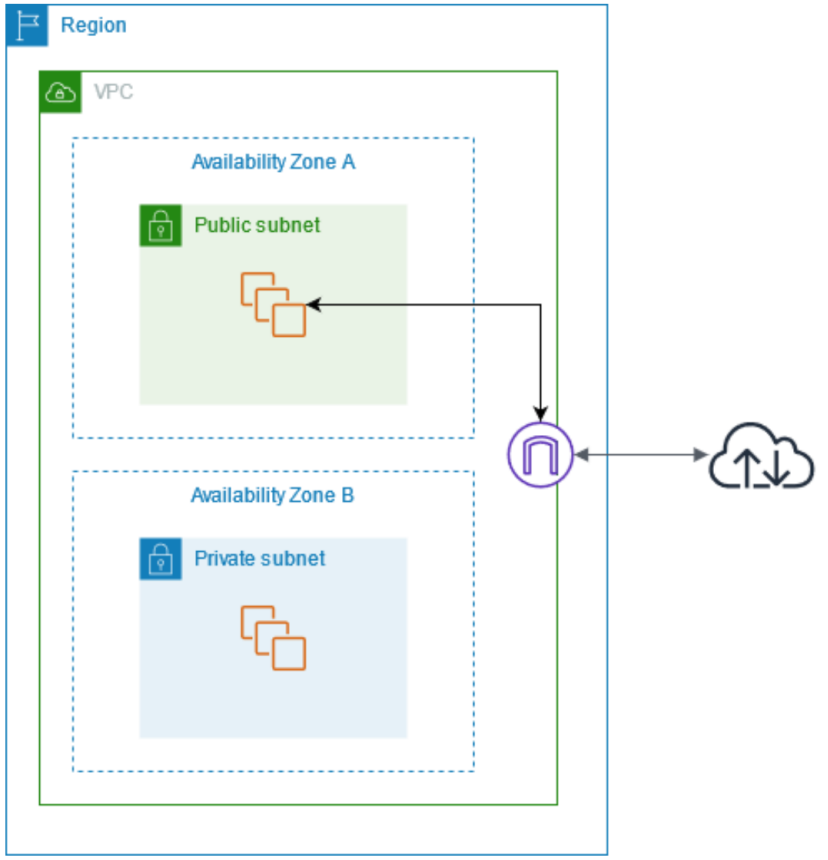
noun [C]

UK /ˈgeɪt.weɪ/ **US** /ˈgeɪt.weɪ/

an entrance through a wall, fence, etc. where there is a gate

portão, portal

*(Tradução de **gateway** do **Cambridge English-Portuguese Dictionary** © Cambridge University Press)*



Route Tables
(Tabela de rotas)

- Mapeia um IP a um serviço
- Está associado a uma ou mais sub-rede(s)
- Quando criamos uma VPC, é criado automaticamente uma “main route table”
- Uma sub-rede não existe sem uma tabela de rotas associada

Configurar tabelas de rotas

PDF | RSS

Uma *tabela de rotas* contém um conjunto de regras, chamado de *rotas*, que determinam para onde o tráfego de rede de sua sub-rede ou gateway é direcionado.

Route Tables (Tabela de rotas)

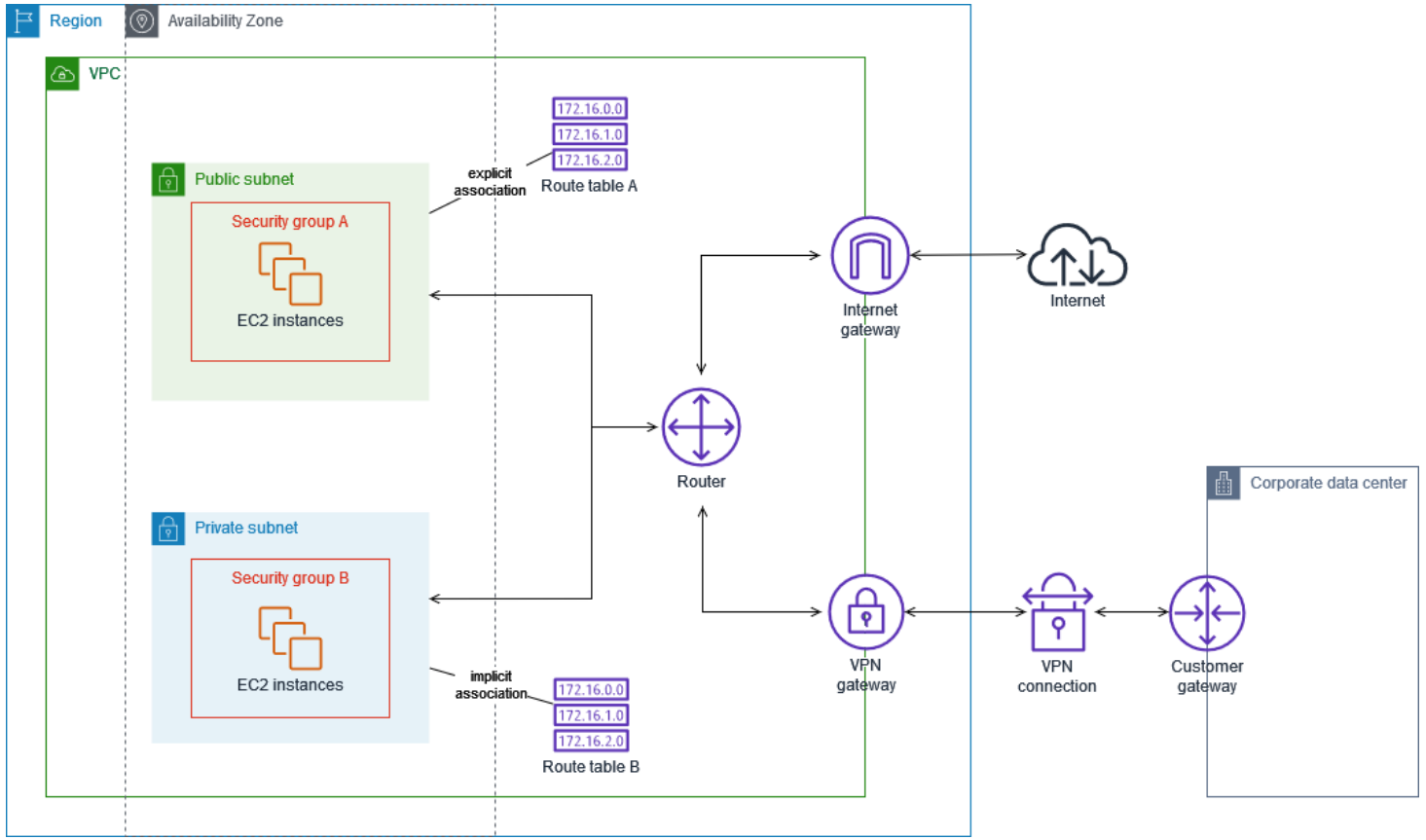
Exemplo

No exemplo a seguir, suponha que uma VPC tem um bloco CIDR IPv4 e um bloco CIDR IPv6. Os tráfegos IPv4 e IPv6 são tratados separadamente, conforme mostrado na tabela de rotas a seguir.

Destination (Destino)	Destino
10.0.0.0/16	Local
2001:db8:1234:1a00::/56	Local
172.31.0.0/16	pcx-11223344556677889
0.0.0.0/0	igw-12345678901234567
::/0	eigw-aabbccddee1122334

- O tráfego IPv4 a ser roteado dentro da VPC (10.0.0.0/16) é abrangido pela rota Local.
- O tráfego IPv6 a ser roteado dentro da VPC (2001:db8:1234:1a00::/56) é abrangido pela rota Local.
- A rota para 172.31.0.0/16 envia o tráfego para uma conexão de emparelhamento.
- A rota para todo o tráfego IPv4 (0.0.0.0/0) envia o tráfego para um gateway da Internet. Portanto, todo o tráfego IPv4, exceto o tráfego dentro da VPC e para a conexão de emparelhamento, é roteado para o gateway da Internet.
- A rota para todo o tráfego IPv6 (::/0) envia o tráfego para um gateway da Internet somente de saída. Portanto, todo o tráfego IPv6, exceto o tráfego dentro da VPC, é roteado para o gateway da Internet somente de saída.

Route Tables (Tabela de rotas)



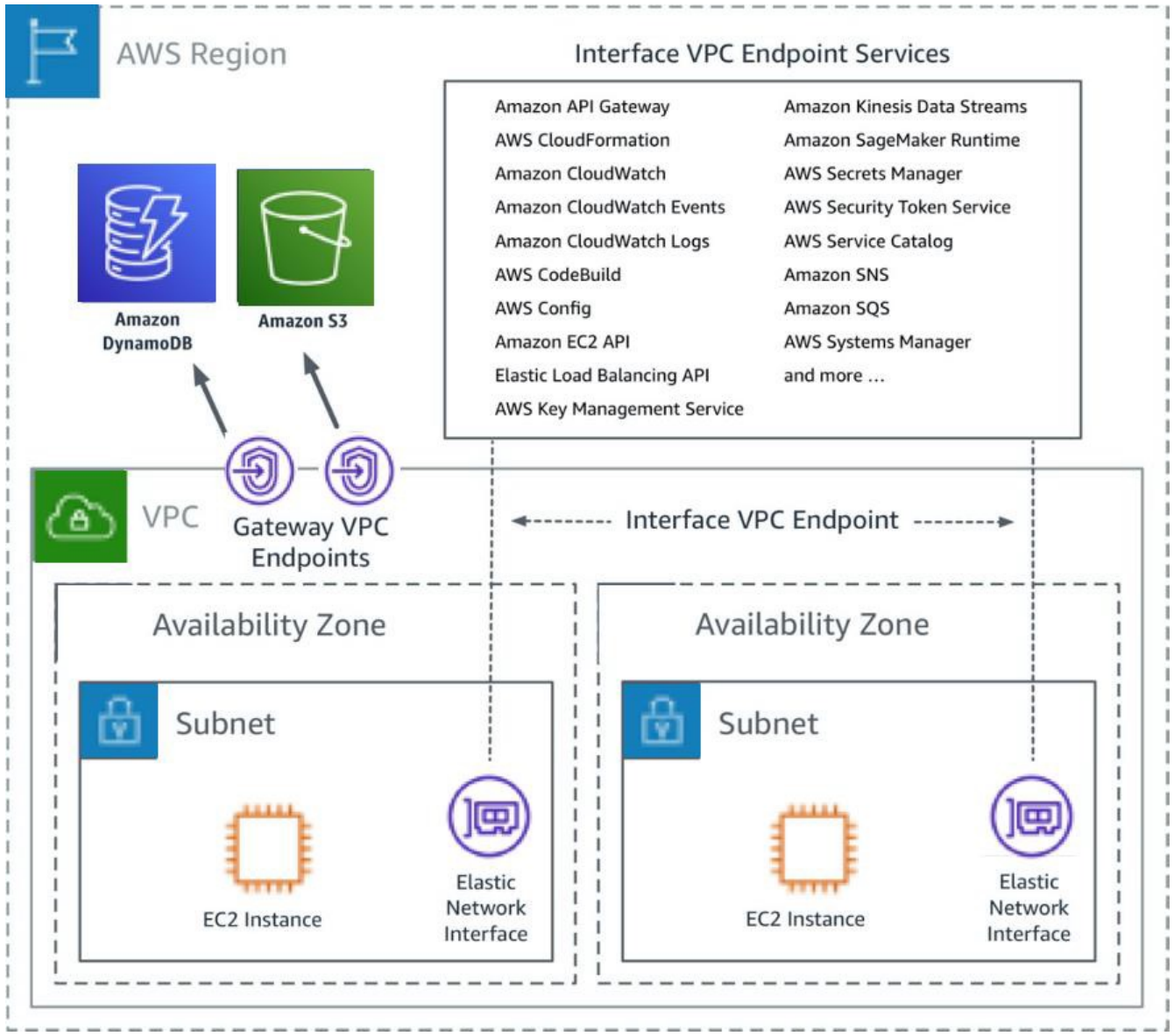
VPC Endpoints

- Conectar serviços sem sair da rede interna da AWS
    - Interface endpoints vs Gateway Endpoints
    - Gateway Endpoints: suporta S3 e DynamoDB
    - Conexões usando IP privado
- Exemplo: tenho uma EC2 numa sub-rede privada e preciso integrar com um bucket no S3 ao final de um processamento de algum fluxo qualquer.

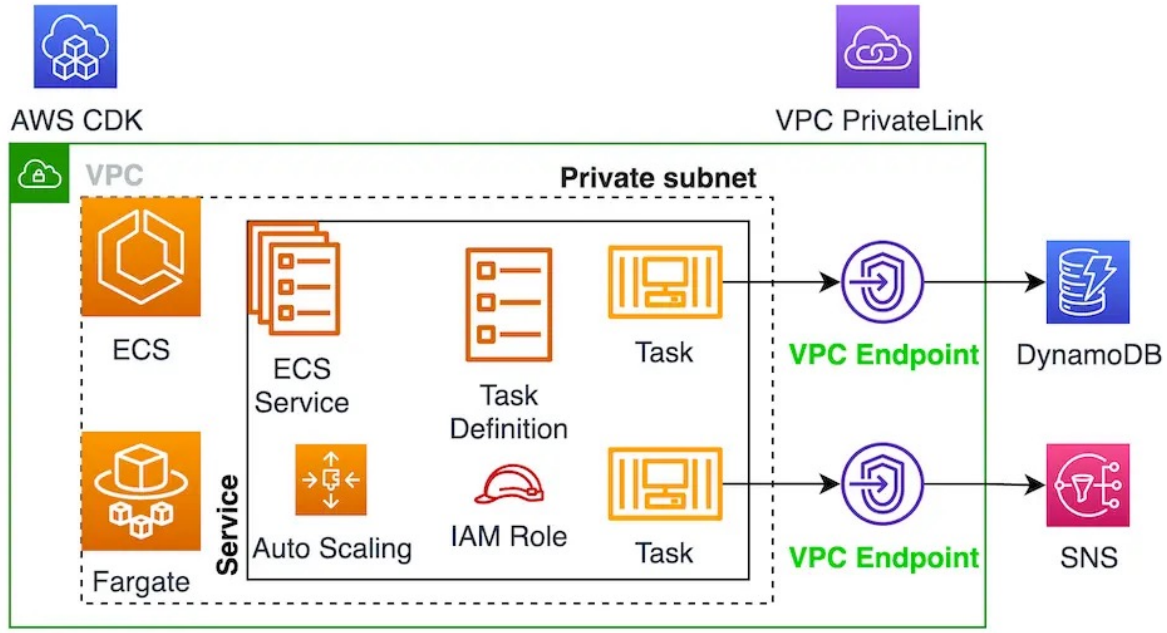
VPC Endpoints

Aspecto	Interface Endpoints	Gateway Endpoints
Serviços Suportados	Vários serviços AWS através do AWS PrivateLink	Amazon S3 e DynamoDB
Implementação	Cria uma ENI em sua sub-rede	Configurado na tabela de rotas da VPC
Segurança	Controle granular de tráfego e políticas	Tráfego privado para S3 e DynamoDB
Custos	Pode incorrer em custos adicionais (ENI)	Normalmente sem custos adicionais
Configuração	Configuração de permissões específicas	Adição de entradas de rotas na tabela de rotas

VPC Endpoints



VPC Endpoints



NAT Gateway

Gateways NAT

PDF | RSS

Um gateway NAT é um serviço de Network Address Translation (NAT – Conversão de endereços de rede). Você pode usar um gateway NAT para que as instâncias em uma sub-rede privada possam se conectar a serviços fora da VPC, mas os serviços externos não podem iniciar uma conexão com essas instâncias.

NAT Gateway

- Não está associado a um grupo de segurança (security group)
- Automaticamente define um endereço de IP público

Característica	NAT Gateway	NAT Instance
Gerenciamento	Totalmente gerenciado pela AWS	Gerenciamento manual
Disponibilidade	Alta disponibilidade por padrão	Deve ser configurada para HA
Escalabilidade	Escala automaticamente	Escalabilidade manual
Desempenho	Alto desempenho	Limitado pela instância EC2
Facilidade de Configuração	Fácil de configurar	Requer configuração manual
Custo	Cobrança por hora e por volume	Potencialmente mais barato, mas complexo
Suporte a IPv6	Apenas IPv4	Apenas IPv4

NAT Gateway

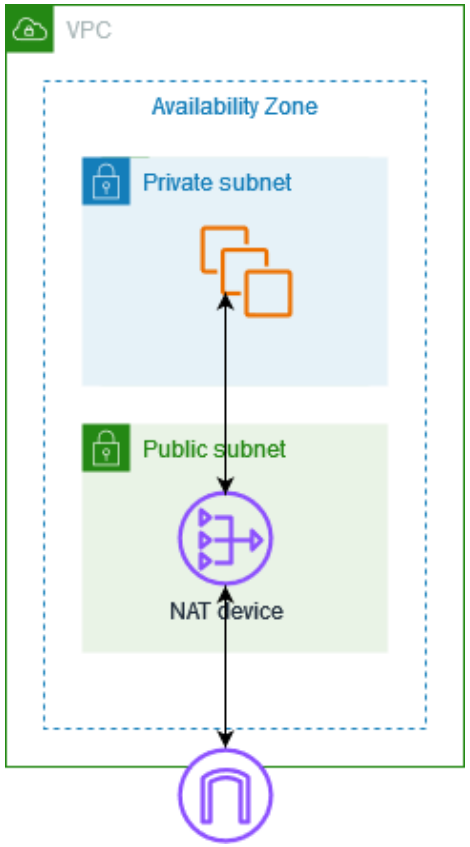
- Casos de uso

Caso de Uso	Descrição	Exemplo
Acesso à Internet para Instâncias Privadas	Permite que instâncias em sub-redes privadas façam solicitações de saída sem expor essas instâncias.	Um servidor de aplicação precisa baixar bibliotecas da internet.
Atualizações de Segurança e Patches	Permite que instâncias obtenham atualizações e patches de software da internet.	Instâncias precisam acessar repositórios de pacotes para atualizar o sistema operacional.
Integração com Serviços AWS	Permite que instâncias em sub-redes privadas acessem endpoints públicos da AWS.	Aplicação em sub-rede privada precisa acessar Amazon S3 ou DynamoDB.
Ambientes de Desenvolvimento e Teste	Fornece acesso controlado à internet para baixar dependências e bibliotecas.	Desenvolvedores baixam ferramentas de desenvolvimento de repositórios de código aberto.
Acesso a Repositórios de Pacotes	Instâncias podem acessar repositórios de pacotes externos durante construção ou execução.	Processo de CI/CD baixando dependências de repositórios de pacotes.
Serviços de Monitoramento e Backup	Ferramentas enviam logs, métricas e backups para serviços externos.	Serviço de monitoramento envia métricas para um sistema externo.
Processamento de Dados e Análise	Workloads acessam fontes de dados externas para ingestão ou exportação de dados.	Pipeline de dados buscando dados de APIs externas para análise.
Segurança Adicional para Ambientes Sensíveis	Mantém instâncias privadas seguras, expondo apenas tráfego de saída necessário.	Aplicação financeira acessando serviços de terceiros sem expor instâncias internas.

NAT Gateway

Contexto arquitetural de exemplo

Por exemplo, o diagrama a seguir mostra um dispositivo NAT em uma sub-rede pública que permite que as instâncias do EC2 em uma sub-rede privada se conectem à Internet por meio de um gateway da Internet. O dispositivo de NAT substitui o endereço IPv4 de origem das instâncias pelo endereço do dispositivo de NAT. Ao enviar tráfego de resposta para as instâncias, o dispositivo de NAT converte os endereços de volta para os endereços IPv4 de origem original.



Security Group

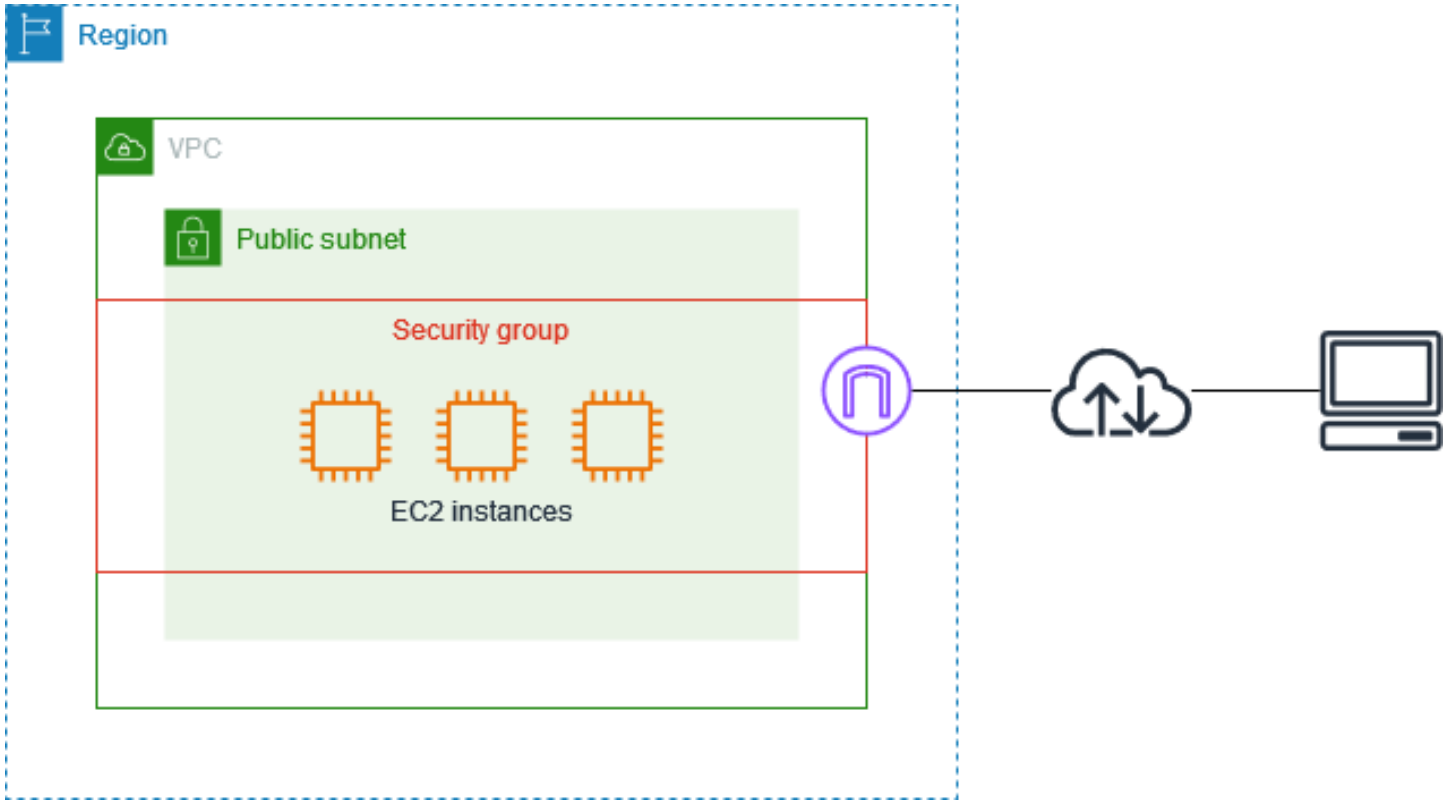
- **Stateful** (guardam o estado da conexão de rede – **com estado**). Isto é, se tenho autorização de inbound, não preciso configurar o outbound

- Se diferenciam das ACLs, as quais não guardam estado da conexão (stateless), já que precisamos configurar as regras de inbound e outbound de forma apartada (são totalmente independentes)

- Comumente vem em cenários associado a uma EC2. Um distrator comum é colocar uma ACL como controle direto para EC2 nas soluções possíveis. Em nível de EC2, vamos trabalhar com security groups.

Security Group

Contexto arquitetural de exemplo



Security Group

- **Análise de caso:** se algum cenário levantar problema de conexão com uma EC2 e disser que as regras de inbound do grupo de segurança estão ok. Neste mesmo cenário é dito que uma alteração nas regras de outbound resolveria o problema. Por que esta afirmação está incorreta?

Security Group

Noções básicas sobre grupos de segurança

- Você pode especificar regras de permissão, mas não regras de negação.

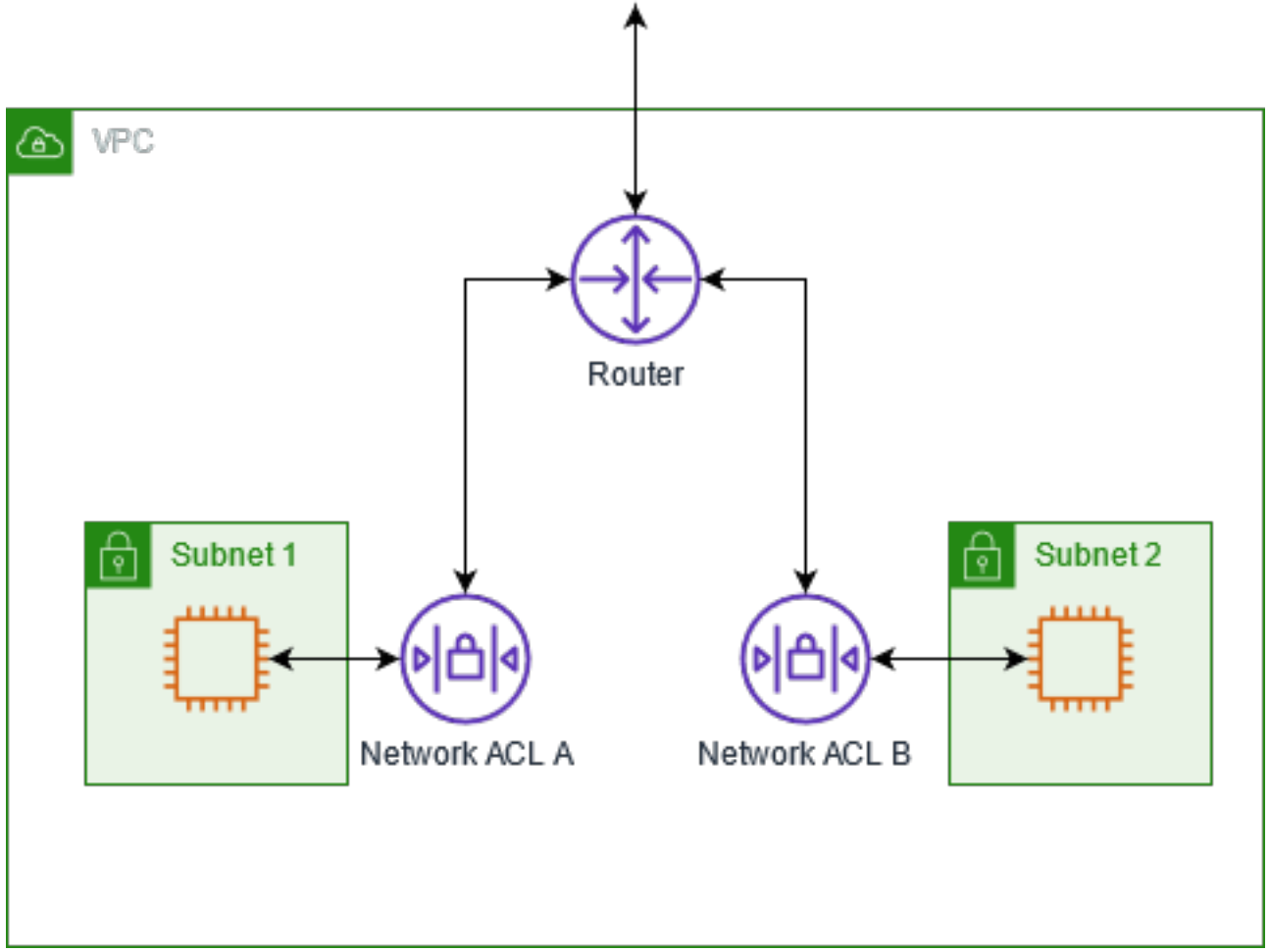
Reforçando novamente: grupos de segurança atuam no nível de instâncias, não de sub-rede

NACL (access control list) – Lista de controle de acesso

- São **stateless (sem estado) – precisamos configurar entrada e saída**
  - Cenários perguntado sobre bloqueio de IP (em caso de ataque)
  - Na prática vai funcionar como um firewall para as sub-redes.

Network ACL (access control list) – Lista de controle de acesso

Contexto arquitetural de exemplo



Network ACL (access control list) – Lista de controle de acesso

- O (*) indica que caso o pacote não se encaixe nas outras regras, usará a regra com a regra do (*);
- **ACL padrão permite todo o tráfego de entrada e saída**
- “As regras são avaliadas a partir da regra de número mais baixo.”

ACL de rede padrão

PDF | RSS

A ACL de rede padrão é configurada para permitir todo o tráfego de entrada e saída das sub-redes com as quais está associada. Além disso, toda ACL de rede contém uma regra cujo número é um asterisco (*). Essa regra garante que, se um pacote não corresponder a nenhuma das outras regras numeradas, o acesso seja negado. Não é possível modificar nem remover essa regra.

Encontra-se a seguir um exemplo de ACL de rede padrão para uma VPC compatível somente com IPv4.

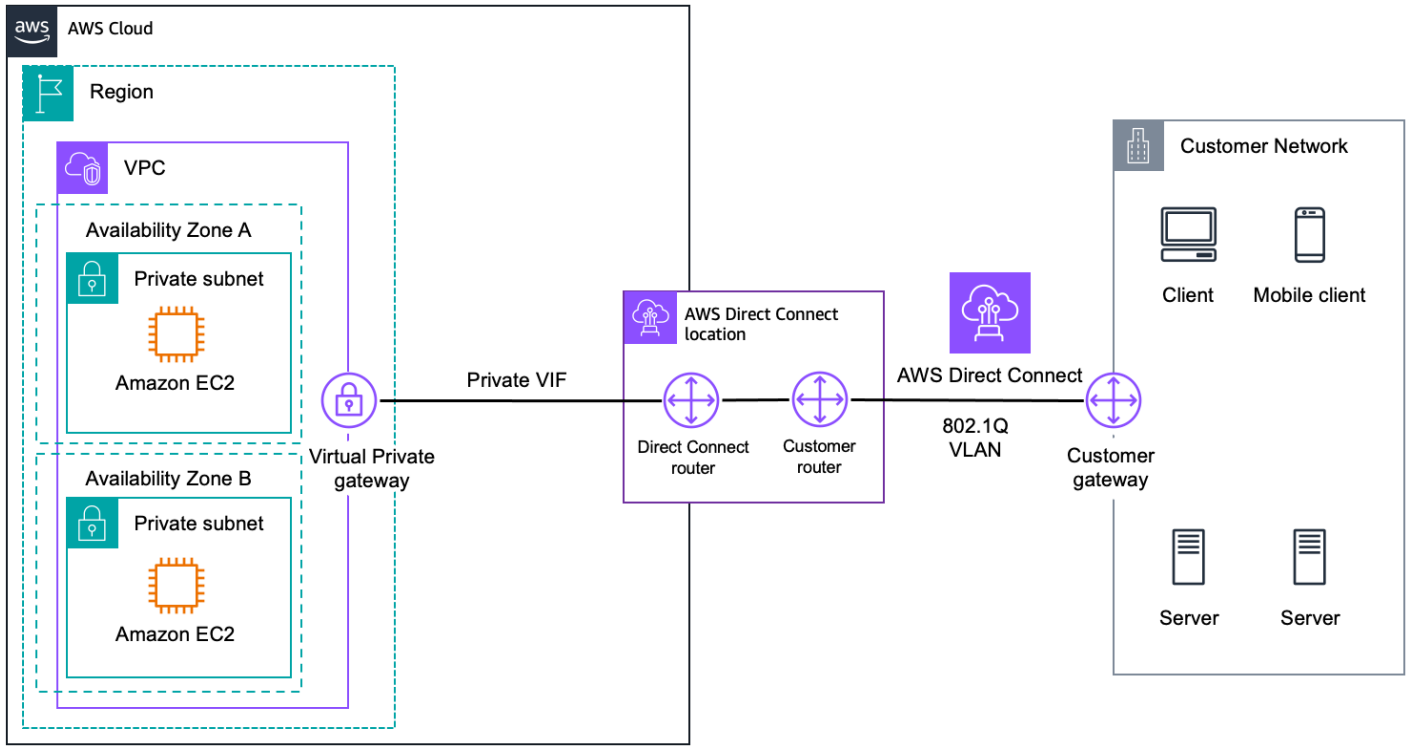
Entrada

Regra nº	Type	Protocolo	Intervalo de portas	Origem	Permissão/Negação
100	Todo tráfego IPv4	Todos	Tudo	0.0.0.0/0	PERMISSÃO
*	Todo tráfego IPv4	Todos	Tudo	0.0.0.0/0	DENY

Contextos Híbridos (on premise + nuvem)

(1) AWS Site-to-Site VPN
(2) AWS Transit Gateway
(3) AWS Direct Connect

Direct Connect

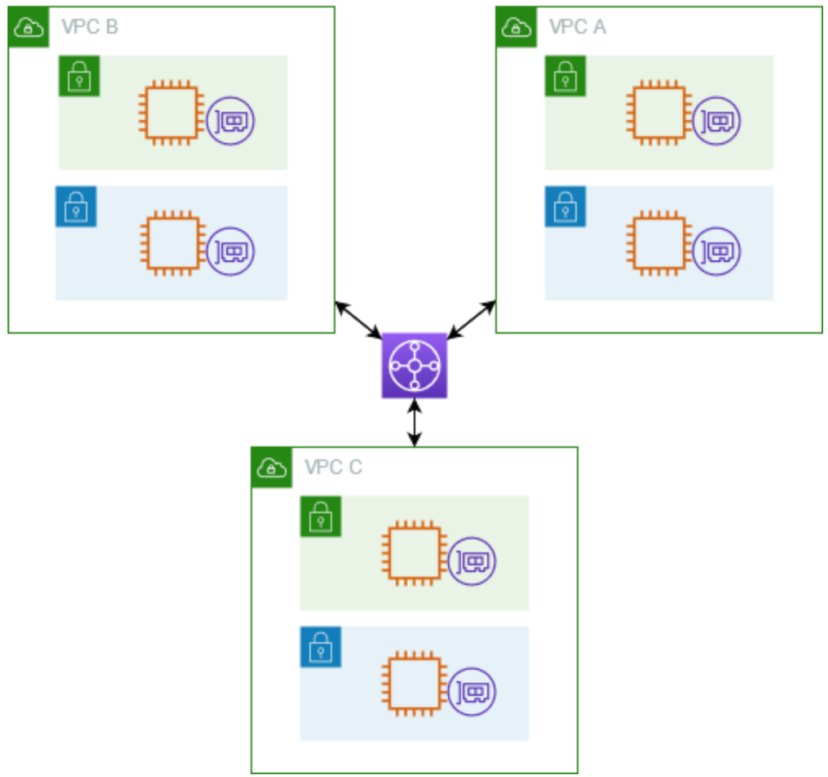


- Comunicação On Premise <–> AWS
- **Quando precisamos aumentar a largura de banda de modo significativo**
- Conexão estável e segura

Transit Gateway

Diagrama de arquitetura

O diagrama a seguir mostra um gateway de trânsito com três anexos de VPC. A tabela de rotas de cada uma dessas VPCs inclui a rota local e rotas que enviam tráfego destinado das outras duas VPCs ao gateway de trânsito.



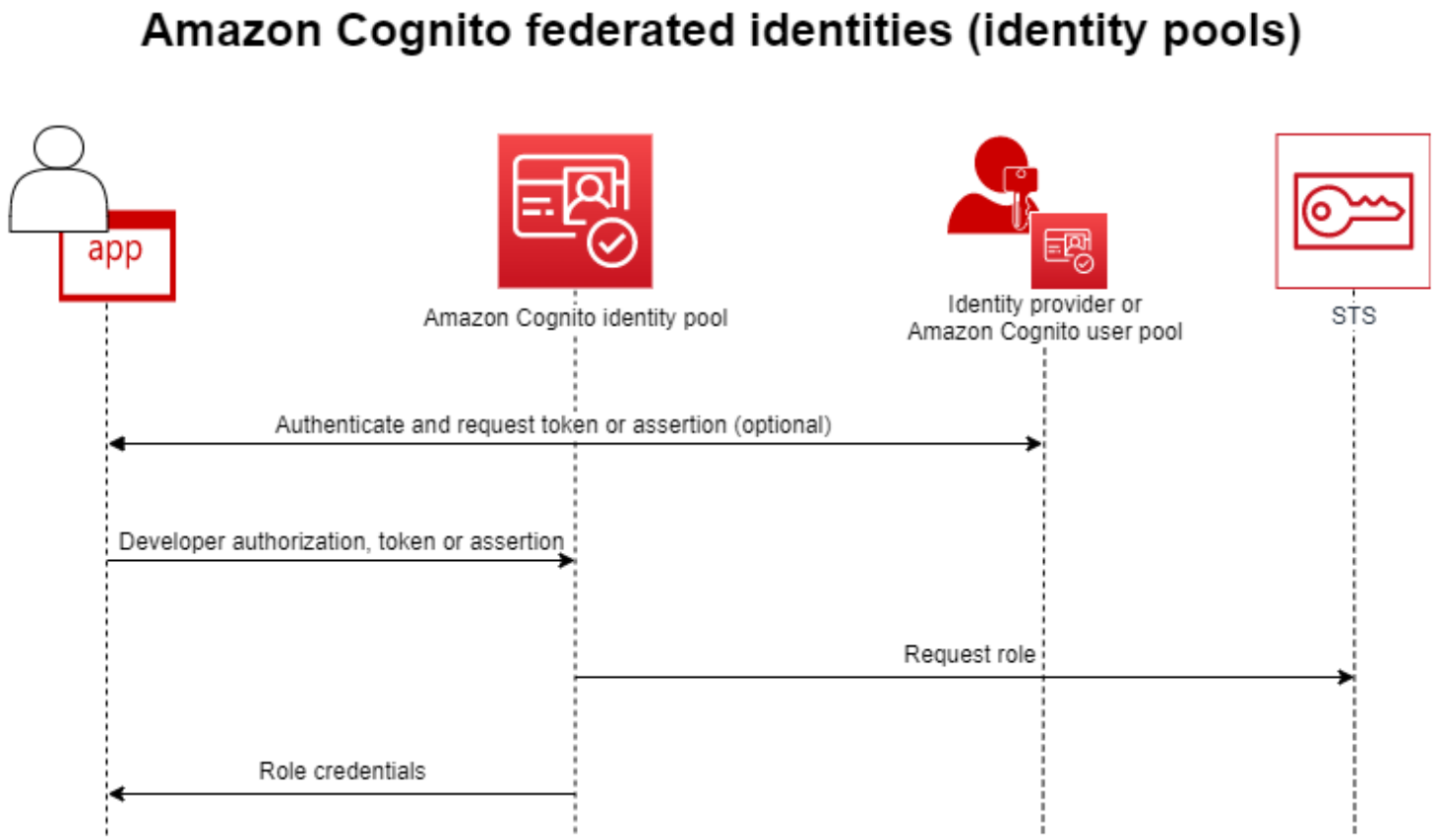
Web Application Firewall

Palavras e contextos chave: (1) Prevenção de SQL injection, (2) monitoramento de requisições HTTP e HTTPS para ELBs e distribuições Cloudfront, (3) Bloqueio de tráfego baseado em padrões de endereços de Ips.

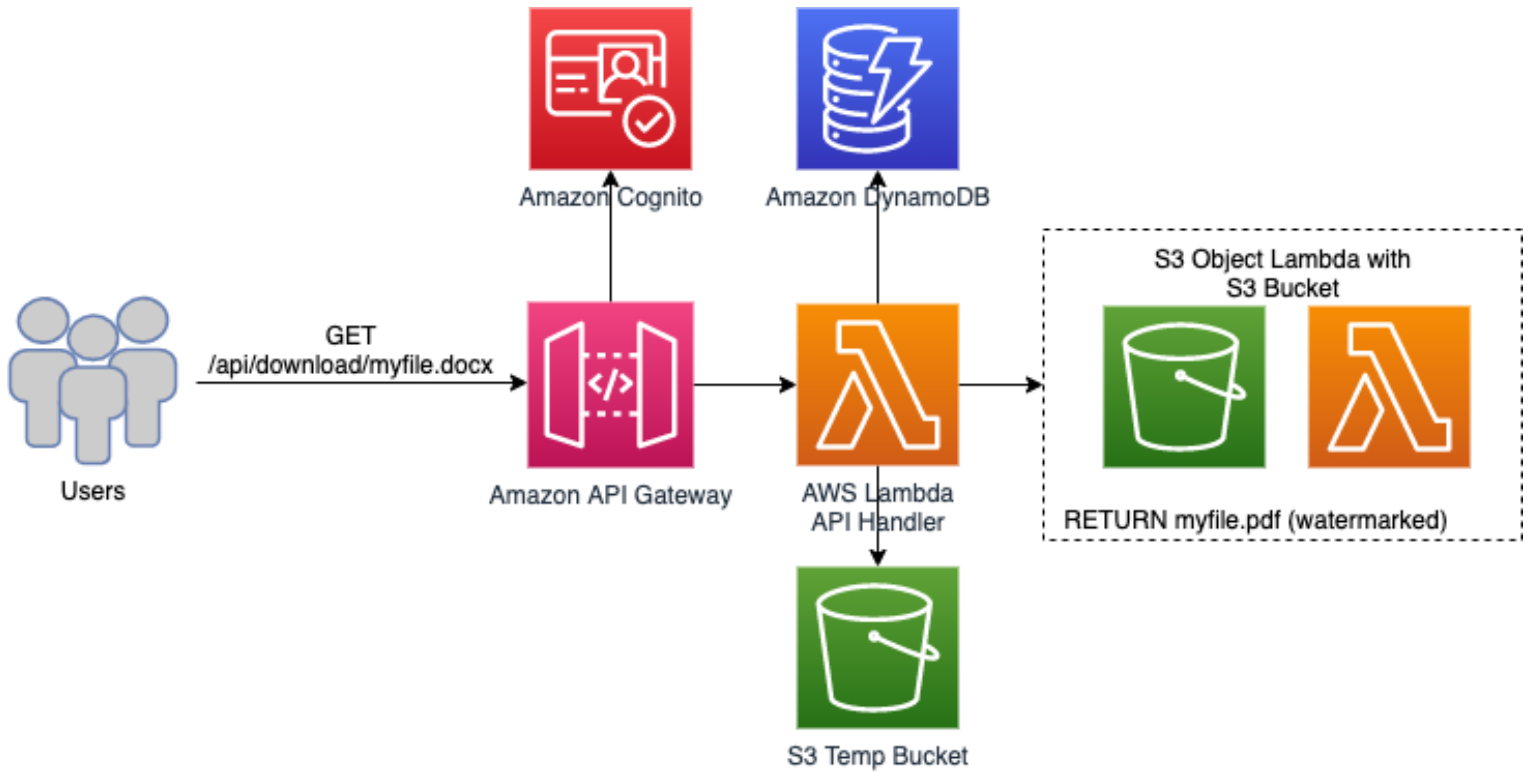
Amazon Macie

Palavras e contextos chave: (1) Vamos associar o Macie ao S3 e proteção de dados sensíveis, (2) proteção de dados sensíveis no contexto do S3.

Amazon Cognito



Amazon Cognito



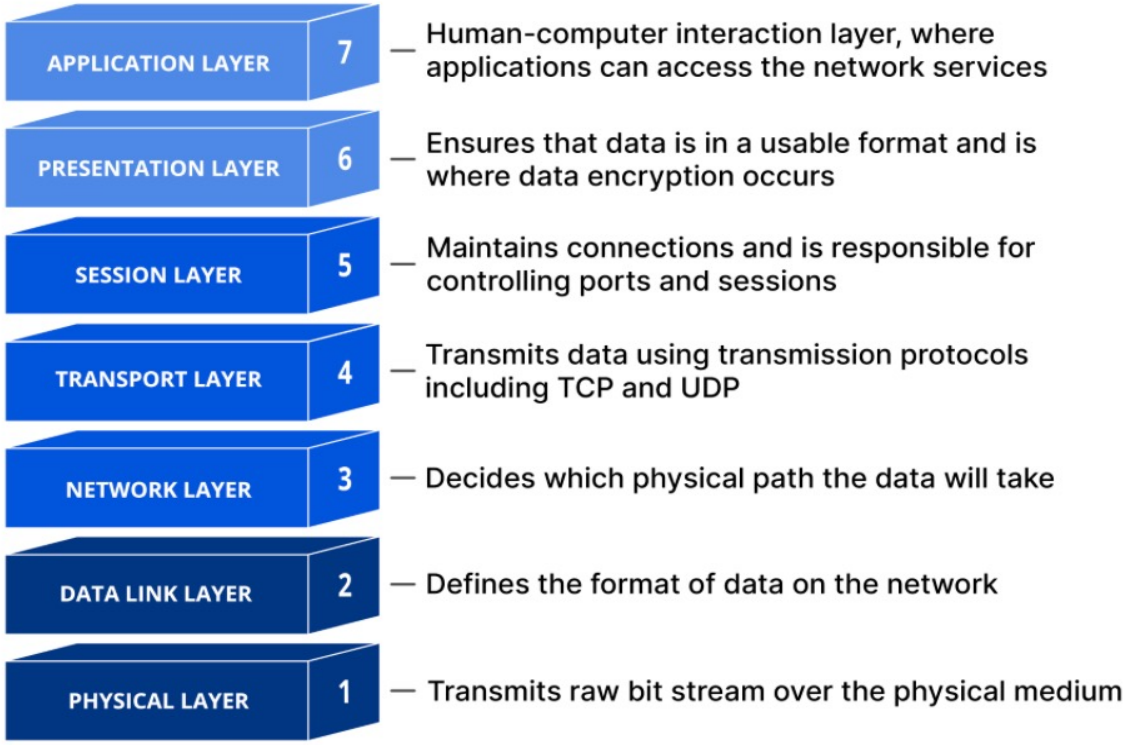
Ref.: https://aws.amazon.com/blogs/architecture/convert-and-watermark-documents-automatically-with-amazon-s3-object-lambda/

AWS Shield

Antes de qualquer coisa, alguns conceitos importantes para esse serviço da AWS

- (1) Modelo OSI
- (2) DDoS

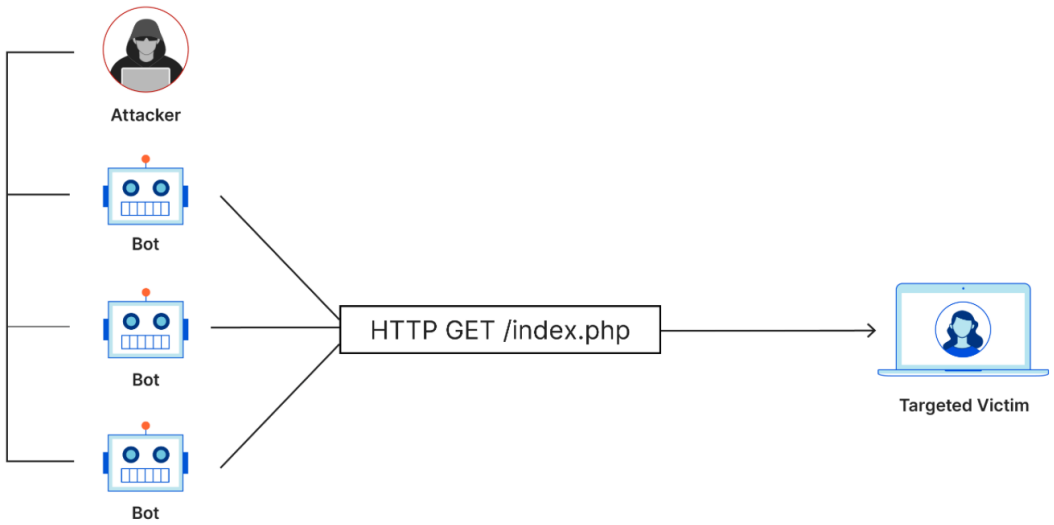
(1) Modelo OSI: O AWS Shield vai atuar nas camadas 3, 4 e 7



Referência: https://www.cloudflare.com/pt-br/learning/ddos/glossary/open-systems-interconnection-model-osi/

(2) DDoS

Exemplo de ataque à Camada de aplicação:

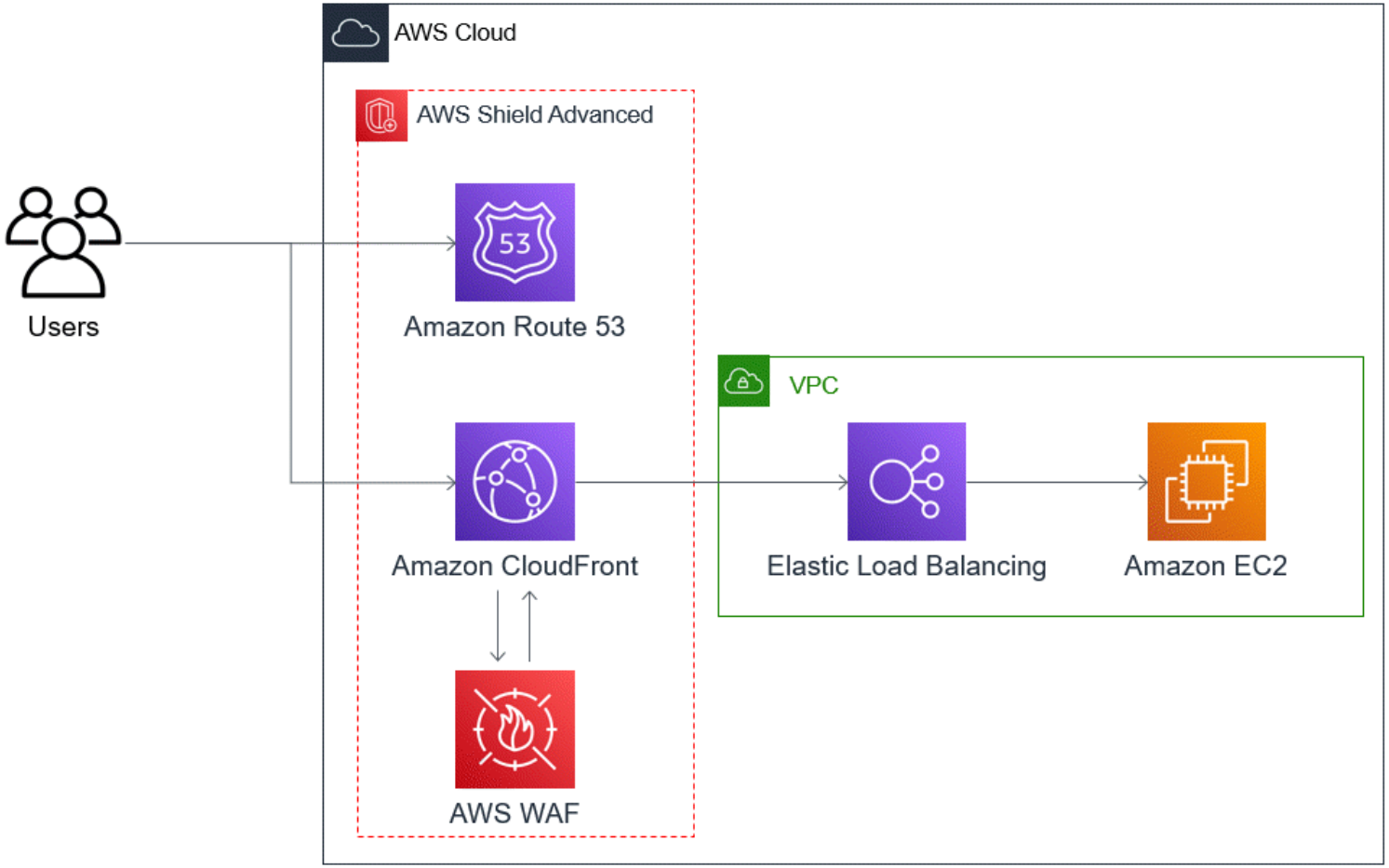


Referência: https://www.cloudflare.com/pt-br/learning/ddos/glossary/open-systems-interconnection-model-osi/

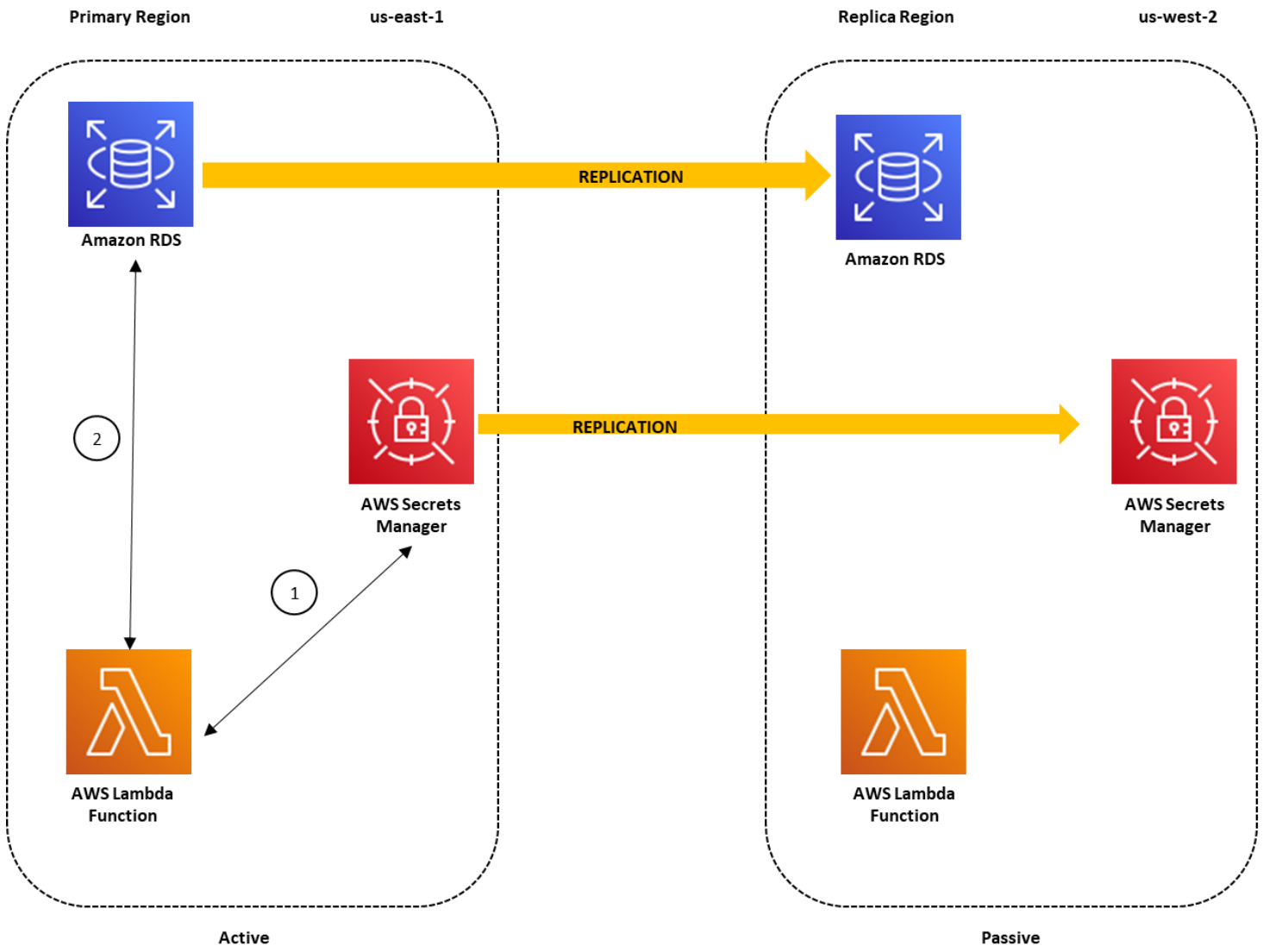
Shield

- Standard: Defesa contra Distributed Denial of Service (DDoS) nas camadas 3 e 4. É automaticamente habilitado para todos os usuários da AWS.

- Advanced: Atua na camada 7. Protege serviços como CloudFront, Route 53 e Elastic Load Balancer



Secrets Manager



Secrets Manager

O que é AWS Secrets Manager?

PDF | RSS

AWS Secrets Manager ajuda você a gerenciar, recuperar e alternar credenciais de banco de dados, credenciais de aplicativos, tokens OAuth, chaves de API e outros segredos em todo o ciclo de vida. Muitos AWS serviços armazenam e usam segredos no Secrets Manager.

O Secrets Manager ajuda você a melhorar seu procedimento de segurança, porque você não precisa mais de credenciais de codificação rígida no código-fonte da aplicação. Armazenar as credenciais no Secrets Manager evita um possível comprometimento por qualquer pessoa que possa inspecionar sua aplicação ou os componentes. Você substitui credenciais de codificação rígida com uma chamada de runtime ao serviço Secrets para recuperar as credenciais dinamicamente quando necessário.

Com o Secrets Manager, você pode configurar uma programação de alternância automática para seus segredos. Isso permite que você substitua os segredos de longo prazo por outros de curto prazo, reduzindo significativamente o risco de comprometimento. Como as credenciais não são mais armazenadas na aplicação, a alternância das credenciais não exige mais a atualização das aplicações e a implantação de alterações nos clientes da aplicação.

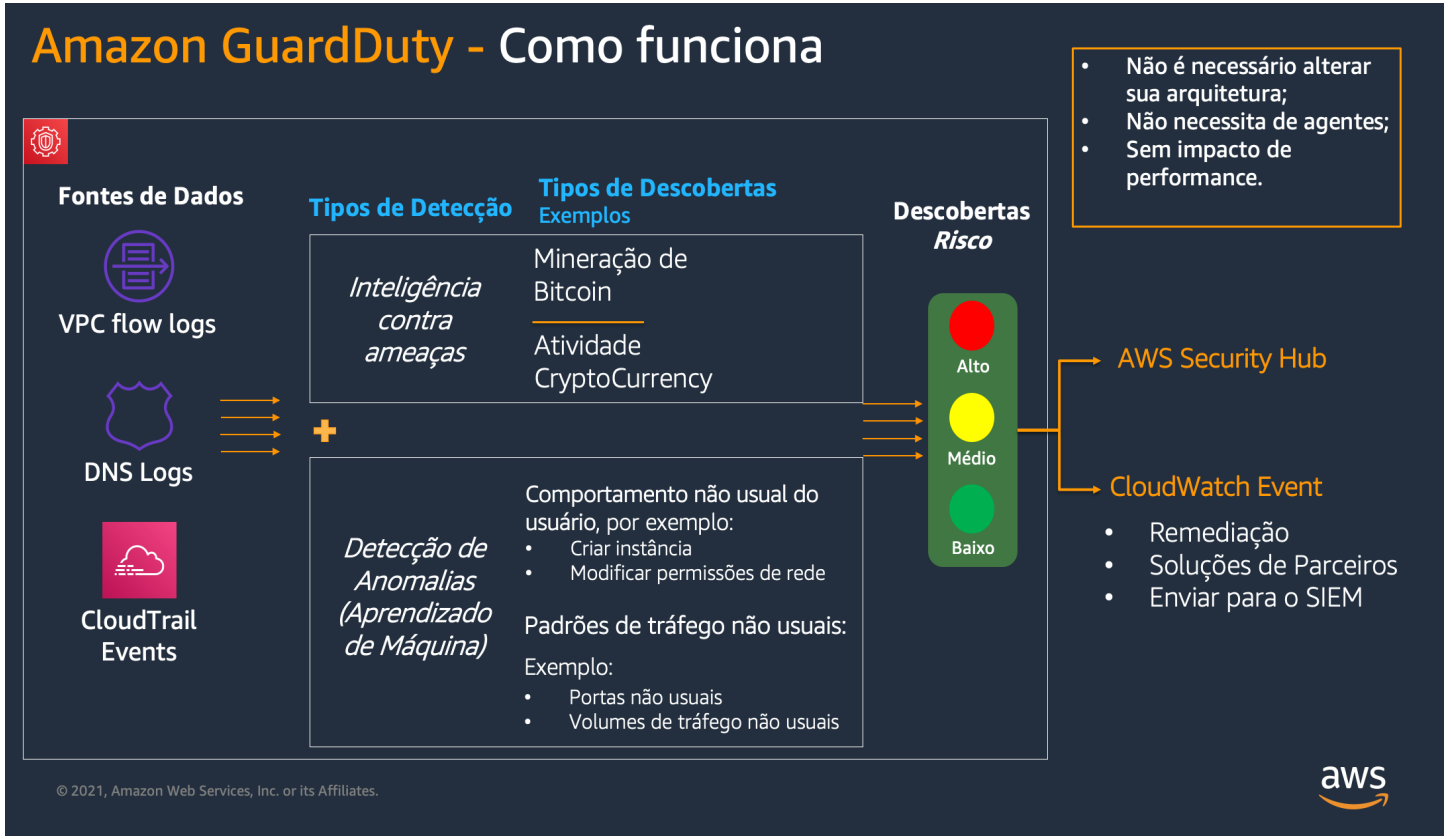
Para outros tipos de segredos que você pode usar em sua organização:

- AWS credenciais — AWS Identity and Access ManagementRecomendamos.
- Chaves de criptografia: recomendamos o AWS Key Management Service.
- Chaves SSH: recomendamos o Amazon EC2 Instance Connect.
- Chaves privadas e certificados: recomendamos o AWS Certificate Manager.

Palavras e contextos chave: (1) rotação periódica de segredos; (2) casos de uso: guardar credenciais de aplicativos, bancos de dados, chaves de API etc. (3) Importante diferenciar o Secrets Manager do KMS e ACM (ver slide anterior).

Secrets Manager

GuardDuty



Referência: https://maturitymodel.security.aws.dev/pt/1.-quickwins/guardduty/

GuardDuty

- AWS SAA-CO3 Study Guide (tradução livre): “Analisa **VPC flow logs**, logs de eventos de gerenciamento do **CloudTrail**, **Route 53 DNS query logs**, buscando endereços de IP maliciosos já conhecidos, nomes de domínios e potencial atividade maliciosa.”

- O GuardDuty atua com foco no tráfego de rede. Não confundir com o Amazon Inspector (comum algum cenário que possa gerar alguma dúvida entre os dois).

Questões

Questão 1

Uma empresa está desenvolvendo uma nova aplicação que requer o armazenamento seguro de segredos, como credenciais de banco de dados, chaves de API e outros dados sensíveis. A solução deve permitir a rotação automática de segredos e a fácil integração com outras ferramentas da AWS.

Qual serviço da AWS você deve utilizar para gerenciar esses segredos de forma segura e eficiente?

A) **AWS Secrets Manager**

B) **AWS Certificate Manager (ACM)**

C) **AWS Key Management Service (KMS)**

D) **AWS Config**

1) Gabarito A

A) **AWS Secrets Manager**
•O AWS Secrets Manager é projetado especificamente para armazenar e gerenciar segredos de forma segura, com suporte para rotação automática e integração com outros serviços AWS.

B) **AWS Certificate Manager (ACM)**
•O AWS Certificate Manager (ACM) é utilizado principalmente para gerenciar certificados SSL/TLS para seus domínios e não é a melhor escolha para o armazenamento de segredos.

C) **AWS Key Management Service (KMS)**
•O AWS Key Management Service (KMS) é utilizado para criar e gerenciar chaves de criptografia, mas não fornece funcionalidades específicas para a rotação automática de segredos ou armazenamento de credenciais de aplicativos.

D) **AWS Config**
•O AWS Config é um serviço que permite avaliar, auditar e avaliar as configurações de recursos da AWS, mas não é adequado para gerenciar segredos.

2) Uma empresa está projetando sua infraestrutura na AWS e precisa garantir a segurança e controle de tráfego tanto em nível de sub-rede quanto em nível de instância EC2. A arquitetura proposta inclui várias sub-redes com diferentes requisitos de segurança e múltiplas instâncias EC2 que necessitam de políticas de acesso específicas. Qual é a diferença principal entre uma ACL de rede e um security group no contexto do controle de tráfego na AWS, e como cada um pode ser utilizado nessa arquitetura?

A) **Uma ACL de rede controla o tráfego em nível de sub-rede, enquanto um security group controla o tráfego em nível de um recurso específico da AWS, como uma instância EC2.**

B) **Uma ACL de rede controla o tráfego em nível de instância EC2, enquanto um security group controla o tráfego em nível de sub-rede.**

C) **Ambos, ACL de rede e security group, controlam o tráfego em nível de instância EC2.**

D) **Uma ACL de rede e um security group são utilizados apenas para controlar o tráfego de entrada, não o de saída.**

2) Gabarito A

A) **Uma ACL de rede controla o tráfego em nível de sub-rede, enquanto um security group controla o tráfego em nível de um recurso específico da AWS, como uma instância EC2.**

Uma **ACL de rede (Network ACL)** é usada para gerenciar o tráfego de entrada e saída em uma sub-rede inteira, permitindo ou negando tráfego com base em regras configuradas. Isso é útil para definir políticas de segurança para todo o tráfego que atravessa a sub-rede. Por outro lado, um **security group** atua como um firewall virtual para instâncias específicas, controlando o tráfego de entrada e saída para esses recursos de forma mais granular, permitindo a definição de regras de acesso específicas para cada instância EC2.

B) **Uma ACL de rede controla o tráfego em nível de instância EC2, enquanto um security group controla o tráfego em nível de sub-rede.**

C) **Ambos, ACL de rede e security group, controlam o tráfego em nível de instância EC2.**

D) **Uma ACL de rede e um security group são utilizados apenas para controlar o tráfego de entrada, não o de saída.**

3) Uma empresa está projetando uma solução na AWS onde os serviços devem se comunicar exclusivamente através da rede interna da AWS, sem expor o tráfego à internet pública. Eles têm uma instância EC2 em uma sub-rede privada e precisam integrar essa instância com um bucket no S3 ao final de um processo de fluxo de trabalho. Qual método de conexão deve ser utilizado para atender a essa necessidade?

A) **Configurar uma Interface Endpoint para o bucket S3, permitindo a comunicação direta usando IP privado.**

B) **Configurar uma Gateway Endpoint para o S3, que suporta a comunicação direta entre a instância EC2 e o bucket S3 usando IP privado.**

C) **Configurar uma VPN para conectar a instância EC2 ao bucket S3.**

D) **Utilizar um Application Load Balancer para roteamento de tráfego entre a instância EC2 e o bucket S3.**

3) **Resposta correta:** B) **Configurar uma Gateway Endpoint para o S3, que suporta a comunicação direta entre a instância EC2 e o bucket S3 usando IP privado.**

A) **Configurar uma Interface Endpoint para o bucket S3, permitindo a comunicação direta usando IP privado.**

B) **Configurar uma Gateway Endpoint para o S3, que suporta a comunicação direta entre a instância EC2 e o bucket S3 usando IP privado.**

C) **Configurar uma VPN para conectar a instância EC2 ao bucket S3.**

D) **Utilizar um Application Load Balancer para roteamento de tráfego entre a instância EC2 e o bucket S3.**

4) Uma empresa está projetando sua arquitetura de rede na AWS e precisa garantir que o controle de tráfego seja configurado de forma eficaz para maximizar a segurança. O arquiteto de soluções da empresa está avaliando o uso de Security Groups e Network ACLs (NACLs) para proteger instâncias EC2 em uma VPC.
Qual das seguintes afirmações descreve corretamente a diferença entre Security Groups e NACLs em relação ao controle de tráfego stateful e stateless?

A) **Security Groups são stateful, o que significa que rastreiam o estado das conexões e permitem automaticamente o tráfego de retorno correspondente. NACLs são stateless, o que significa que cada regra de entrada e saída deve ser explicitamente definida.**

B) **Security Groups são stateless, o que significa que cada regra de entrada e saída deve ser explicitamente definida. NACLs são stateful, o que significa que rastreiam o estado das conexões e permitem automaticamente o tráfego de retorno correspondente.**

C) **Ambos, Security Groups e NACLs, são stateful e rastreiam automaticamente o estado das conexões, permitindo o tráfego de retorno sem regras adicionais.**

D) **Ambos, Security Groups e NACLs, são stateless e requerem regras explícitas para cada conexão de entrada e saída.**

4) **Resposta correta:** A) **Security Groups são stateful, o que significa que rastreiam o estado das conexões e permitem automaticamente o tráfego de retorno correspondente. NACLs são stateless, o que significa que cada regra de entrada e saída deve ser explicitamente definida.**
Justificativa:

•**Security Groups**: São stateful, o que significa que, ao permitir uma conexão de entrada, o tráfego de saída correspondente é automaticamente permitido e vice-versa.

•**NACLs**: São stateless, o que requer que cada regra de entrada e saída seja definida explicitamente, sem rastrear o estado das conexões.

5) **Security Groups vs NACL**
Uma empresa está configurando a segurança de sua VPC na AWS e precisa entender as diferenças entre Security Groups e Network ACLs (NACLs) para aplicar as melhores práticas de segurança em suas instâncias EC2 e sub-redes.

Qual das seguintes afirmações descreve corretamente os níveis de atuação de Security Groups e NACLs?

A) **Security Groups operam no nível da instância (EC2), enquanto Network ACLs operam no nível da sub-rede.**

B) **Security Groups operam no nível da sub-rede, enquanto Network ACLs operam no nível da instância (EC2).**

C) **Ambos, Security Groups e NACLs, operam no nível da instância (EC2).**

D) **Ambos, Security Groups e NACLs, operam no nível da sub-rede.**

Resposta correta: A) **Security Groups operam no nível da instância (EC2), enquanto Network ACLs operam no nível da sub-rede.**
Justificativa: Security Groups são associados a instâncias específicas e controlam o tráfego de entrada e saída para essas instâncias. Network ACLs são aplicados no nível da sub-rede, controlando o tráfego que entra e sai de toda a sub-rede.

5) **Security Groups vs NACL**

Resposta correta: A) **Security Groups operam no nível da instância (EC2), enquanto Network ACLs operam no nível da sub-rede.**

Justificativa: Security Groups são associados a instâncias específicas e controlam o tráfego de entrada e saída para essas instâncias. Network ACLs são aplicados no nível da sub-rede, controlando o tráfego que entra e sai de toda a sub-rede.

6) Uma empresa de comércio eletrônico armazena grandes volumes de dados sensíveis dos clientes, incluindo informações pessoais e financeiras, no Amazon S3. O arquiteto de soluções foi encarregado de implementar uma solução que ajude a identificar e proteger automaticamente esses dados sensíveis.

Qual serviço da AWS deve ser utilizado para atender a essa necessidade?

A) **Amazon Macie**
B) **Amazon Inspector**
C) **AWS Shield**
D) **AWS Config**

6) Gabarito A

A) **Amazon Macie**
•Amazon Macie usa machine learning para descobrir, classificar e proteger dados sensíveis armazenados no Amazon S3.
B) **Amazon GuardDuty**
•GuardDuty é usado para monitoramento contínuo de ameaças e proteção contra atividades maliciosas em sua conta da AWS.
C) **AWS Shield**
•AWS Shield oferece proteção contra ataques DDoS.
D) **AWS Config**
•AWS Config permite avaliar, auditar e avaliar as configurações de recursos da AWS.

Resposta correta: A) **Amazon Macie**
Justificativa: Amazon Macie é a solução ideal para descobrir e proteger automaticamente dados sensíveis em buckets do S3, usando machine learning e técnicas avançadas de análise.

7) Uma empresa está migrando sua aplicação web crítica para a AWS e quer garantir proteção robusta contra ataques de negação de serviço distribuído (DDoS). O arquiteto de soluções precisa escolher um serviço AWS que forneça essa proteção de forma automática e escalável.

Qual serviço da AWS deve ser utilizado para atender a essa necessidade?

A) **Amazon Macie**
B) **Amazon GuardDuty**
C) **AWS Shield**
D) **AWS WAF**

7) Uma empresa está migrando sua aplicação web crítica para a AWS e quer garantir proteção robusta contra ataques de negação de serviço distribuído (DDoS). O arquiteto de soluções precisa escolher um serviço AWS que forneça essa proteção de forma automática e escalável.

Qual serviço da AWS deve ser utilizado para atender a essa necessidade?

A) **Amazon Macie**
•Macie é usado para descoberta e proteção de dados sensíveis.
B) **Amazon GuardDuty**
•GuardDuty é focado na detecção de ameaças e monitoramento contínuo.
C) **AWS Shield**
•AWS Shield oferece proteção contra ataques DDoS, com opções avançadas para proteção mais robusta.
D) **AWS WAF**
•AWS WAF é um firewall de aplicação web que ajuda a proteger suas aplicações web contra explorações na web.

Resposta correta: C) **AWS Shield**

8) Uma startup está desenvolvendo uma aplicação móvel que requer gerenciamento de autenticação e autorização de usuários. A solução precisa suportar login via redes sociais e permitir a integração fácil com a infraestrutura AWS.

Qual serviço da AWS deve ser utilizado para atender a essa necessidade?

A) **Amazon Macie**
B) **Amazon GuardDuty**
C) **AWS Shield**
D) **Amazon Cognito**

8) Uma startup está desenvolvendo uma aplicação móvel que requer gerenciamento de autenticação e autorização de usuários. A solução precisa suportar login via redes sociais e permitir a integração fácil com a infraestrutura AWS.

Qual serviço da AWS deve ser utilizado para atender a essa necessidade?

A) **Amazon Macie**
•Macie é usado para descoberta e proteção de dados sensíveis.
B) **Amazon GuardDuty**
•GuardDuty é focado na detecção de ameaças e monitoramento contínuo.
C) **AWS Shield**
•Shield oferece proteção contra ataques DDoS.
D) **Amazon Cognito**
•Amazon Cognito fornece gerenciamento de autenticação e autorização de usuários, incluindo suporte para login via redes sociais.
Resposta correta: D) **Amazon Cognito**
Justificativa: Amazon Cognito oferece serviços de autenticação e autorização, permitindo a integração de login via redes sociais e gerenciamento de usuários para aplicações móveis e web.

9) Uma empresa está migrando sua aplicação web para a AWS e precisa proteger sua aplicação contra explorações comuns da web, como injeções de SQL e ataques de cross-site scripting (XSS). O arquiteto de soluções deve selecionar um serviço que permita a criação de regras personalizadas para filtrar tráfego HTTP/HTTPS malicioso.

Qual serviço da AWS deve ser utilizado para atender a essa necessidade?

A) **AWS WAF**
B) **AWS Shield**
C) **Amazon Macie**
D) **Amazon GuardDuty**

9) Gabarito A

A) **AWS WAF**
•AWS WAF (Web Application Firewall) permite criar regras personalizadas para proteger aplicações web contra explorações comuns, como injeções de SQL e ataques de cross-site scripting (XSS).

B) **AWS Shield**
•AWS Shield oferece proteção contra ataques DDoS, mas não é específico para filtragem de tráfego HTTP/HTTPS malicioso.

C) **Amazon Macie**
•Amazon Macie é usado para descobrir e proteger dados sensíveis em S3, não para proteger aplicações web contra explorações.

D) **Amazon GuardDuty**
•Amazon GuardDuty fornece monitoramento contínuo e detecção de ameaças, mas não permite criar regras personalizadas para filtrar tráfego HTTP/HTTPS.

Resposta correta: A) **AWS WAF**
Justificativa: AWS WAF permite criar e gerenciar regras personalizadas para filtrar tráfego HTTP/HTTPS malicioso e proteger aplicações web contra explorações comuns da web, como injeções de SQL e ataques de cross-site scripting (XSS). Ele é ideal para empresas que precisam de uma camada adicional de segurança para suas aplicações web na AWS.