Contents

[**AWS NETWORKING** 1](#_Toc135123755)

[**Amazon Virtual Private Cloud (Amazon VPC)** 1](#_Toc135123756)

[**AWS Direct Connect** 5](#_Toc135123757)

[**Domain Name System (DNS)** 7](#_Toc135123758)

[**Amazon Route 53** 7](#_Toc135123759)

[**SECURITY** 8](#_Toc135123760)

[**Modelo de responsabilidade compartilhada** 8](#_Toc135123761)

[**AWS Organizations** 8](#_Toc135123762)

[**AWS Artifact** é um serviço que fornece acesso sob demanda a relatórios de segurança e conformidade da AWS e a contratos on-line selecionados. O AWS Artifact tem duas seções principais: AWS Artifact Agreements e o AWS Artifact Reports. 9](#_Toc135123763)

[**DDoS ou DDoS. Negação de serviço distribuída.** 10](#_Toc135123764)

[**AWS Key Management Service (AWS KMS)** 10](#_Toc135123765)

[**AWS WAF** 11](#_Toc135123766)

# **AWS NETWORKING**

## **Amazon Virtual Private Cloud (Amazon VPC)**

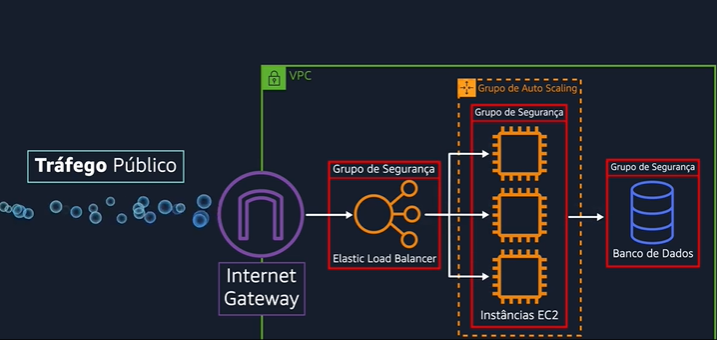
 VPC, Virtual Private Cloud, é o serviço que você utiliza para criar a sua própria rede privada na AWS. A VPC permite que você defina o seu intervalo de preços privados para fazer a alocação de recursos, como instâncias EC2 e Load Balancing dentro da sua rede.

Mas você não pode simplesmente jogar os seus recursos em uma VPC e seguir em frente. Você precisa colocá los em sub-redes. Cada sub-rede possui uma porção dos endereços de IP da sua VPC e permite que você faça o deploy de diversos recursos. Sub-redes, juntamente com as regras de redes, que abordaremos mais tarde, controlam se os recursos estarão disponíveis de forma pública ou privada

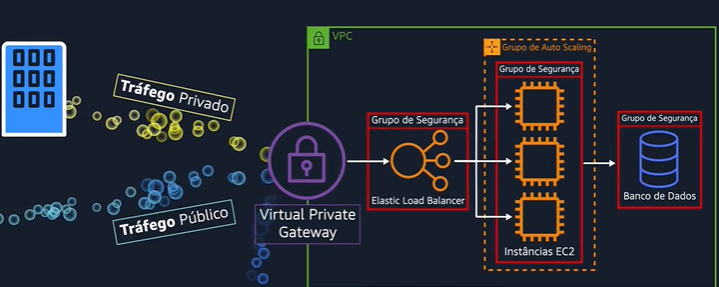
Existem cenários onde você pode ter recursos que deseja que sejam acessíveis apenas se alguém estiver conectado à sua rede privada. Por exemplo, aplicações internas como uma aplicação de RH ou um banco de dados.

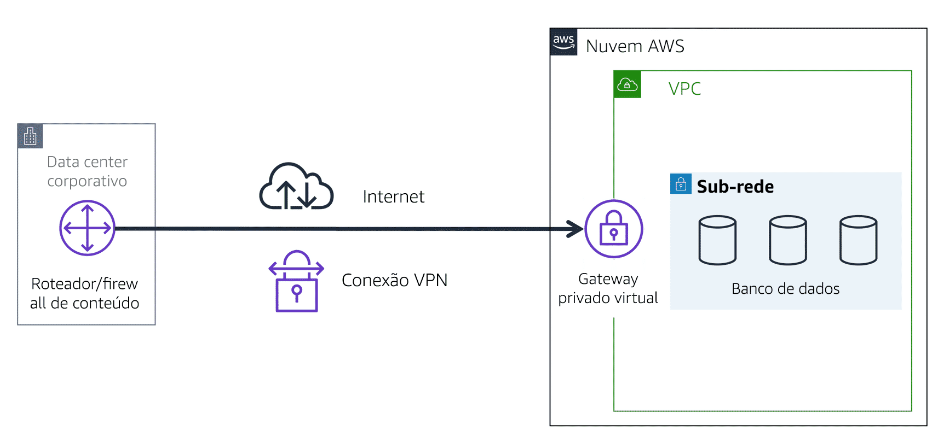
**Publico**: Para permitir a comunicação de tráfego que vem da internet para sua VPC, você deve associar um recurso que chamamos de internet Gateway, ou GW, a sua VPC

Um internet gateway é como se fosse uma porta aberta para o público.



**privados internos:** Não queremos que qualquer um, de qualquer lugar, seja capaz de alcançar esses recursos. Então, nós não queremos o Internet Gateway conectado à nossa VPC. Em vez disso, queremos um gateway privado, que vai permitir somente a entrada de pessoas que estiverem vindo de uma rede privada, não da Internet pública. Esse Gateway privado é chamado de Virtual Private Gateway, que é um recurso que permite que você crie uma conexão VPN entre uma rede privada que pode ser, por exemplo, seu data center ou uma rede corporativa interna com sua VPC.



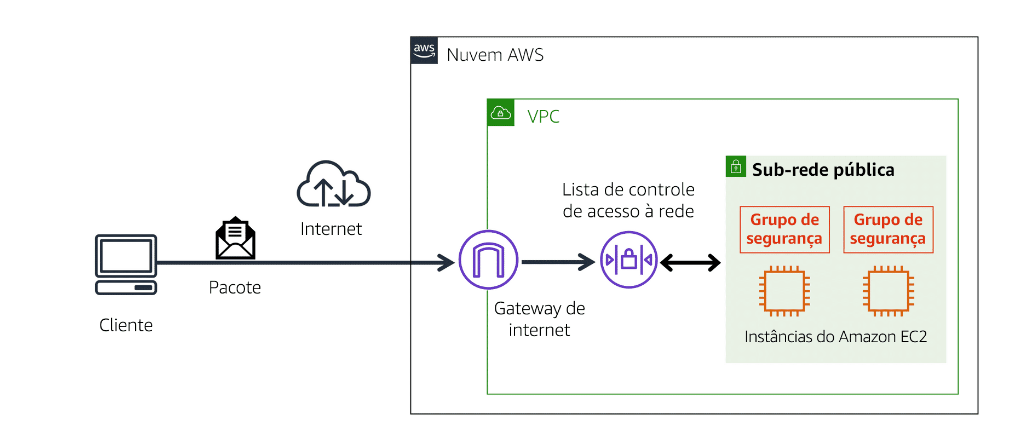


O AWS Direct Connect fornece uma linha física que conecta sua rede do datacenter à sua VPC. Isso pode ajudar você a atender às necessidades regulamentares e de conformidade bem como contornar potenciais problemas de largura de banda.

A AWS tem uma ampla variedade de serviços que cobre cada uma das camadas de segurança. Proteção de rede, segurança de aplicações identidades de usuário, autorização, autenticação, proteção contra ataques de negação de serviço distribuído, ou DDoS, integridade dos dados criptografia e muito mais.

**O principal motivo para usar subnets em uma VPC é controlar o acesso aos gateways**

**Pacotes** são mensagens na internet e cada pacote que cruza os limites de uma subnet é verificado por um recurso chamado de **Lista de controle de acesso à rede**, ou **network ACL.**



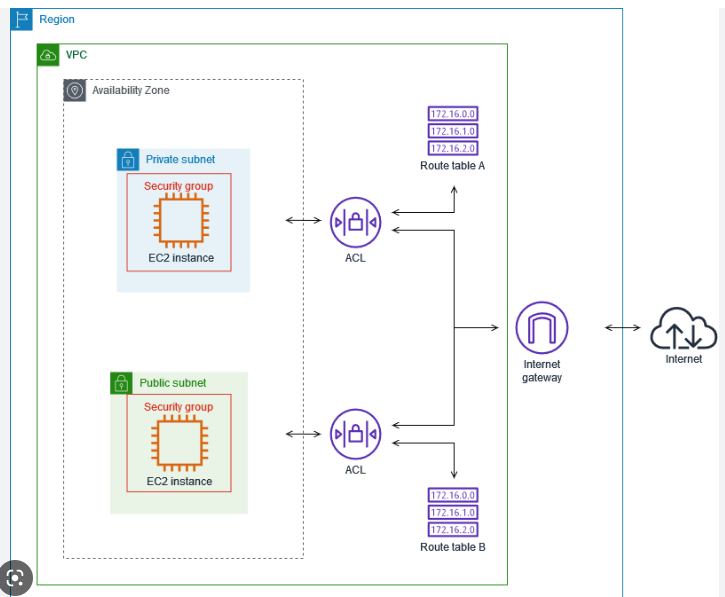
 E essa verificação é necessária para validar se o pacote tem permissões para sair ou entrar na subnet com base em quem enviou e como ele está tentando se comunicar. As network ACLs verificam o fluxo de dados que entram e saem de uma subnet. Da mesma forma que o controle de passaportes. O fluxo de dados que foi aprovado pode passar até o seu destino e o fluxo de dados potencialmente prejudicial, como tentativas de obter o controle de um sistema através das requisições na central de administração, são bloqueados antes de chegarem no alvo. Você não pode hackear o que não pode alcançar.

A network ACL somente pode controlar se um pacote cruza o limite de uma subnet tentando entrar ou sair. Ela não avalia se o pacote pode ir até uma instância EC2 específica ou não. Às vezes, você vai ter várias instâncias EC2 na mesma subnet mas pode precisar de regras diferentes relacionadas a quem pode enviar os pacotes para qual porta esses pacotes podem ser enviados. Então, você precisa de uma segurança de rede no nível da instância também.

Para resolver questões de acesso no nível da instância, podemos adicionar aqui os grupos de segurança.

**o grupo de segurança é Stateful**, o que quer dizer que ele tem uma espécie de memória quando se trata de permitir a entrada ou saída. Se um pacote for verificado uma vez, na próxima vez não será verificado

**o network ACL é Stateless,** ou seja, ele não se lembra de nada e verifica cada pacote que cruza sua fronteira, independentemente da situação.



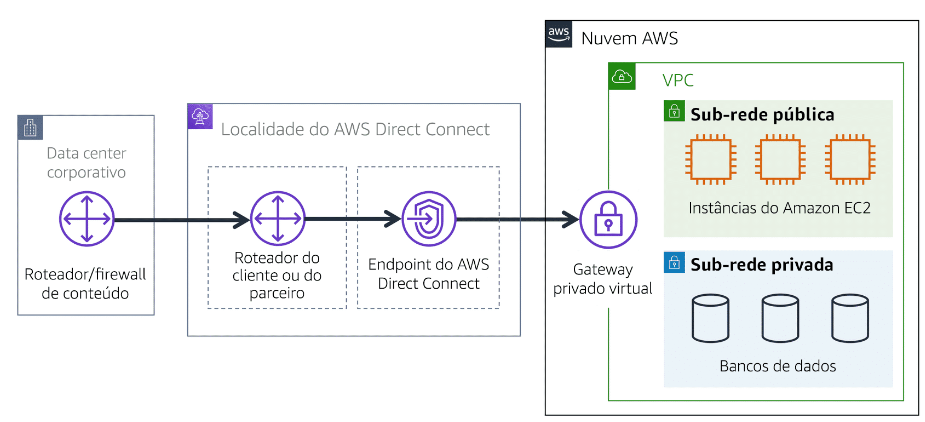
As ACLs de rede (listas de controle de acesso de rede) fazem a filtragem de pacotes stateless . Elas não se lembram de nada e verificam os pacotes que atravessam a fronteira da sub-rede em todos os sentidos: entrada e saída.  
  
Cada conta AWS tem uma ACL de rede comum. Ao configurar a VPC, você pode usar a ACL de rede comum da conta ou criar ACLs de rede personalizadas.  
  
Por padrão, a ACL de rede comum da conta permite todo o tráfego de entrada e saída, mas você pode modificá-la adicionando suas próprias regras. Para ACLs de rede personalizadas, todo o tráfego de entrada e saída é negado até que você adicione regras para especificar qual tráfego deve ser permitido. Além disso, todas as ACLs de rede têm uma regra de negação explícita. Essa regra garante que, se um pacote não corresponder a nenhuma das outras regras na lista, ele será negado.

## [**AWS Direct Connect**](https://aws.amazon.com/directconnect/)

é um serviço que permite estabelecer uma conexão privada dedicada entre seu data center e uma VPC.

Suponha que haja um prédio com um corredor que liga o prédio diretamente à cafeteria. Somente os moradores do prédio podem passar por esse corredor.  
Esse corredor privado fornece o mesmo tipo de conexão dedicada que o AWS Direct Connect. Os moradores conseguem entrar na cafeteria sem precisarem usar a estrada pública compartilhada com outros clientes.

A conexão privada que o AWS Direct Connect fornece ajuda você a reduzir os custos de rede e a aumentar a quantidade de largura de banda que pode trafegar pela sua rede.



Sub-rede privada : Isola bancos de dados contendo informações pessoais dos clientes.

Sub-rede pública : É compatível com o site voltado para o cliente.

Gateway privado virtual: Cria uma conexão VPN entre a VPC e a rede corporativa interna.

AWS Direct Connect: Estabelece uma conexão dedicada entre o data center local e a VPC.

1 - Exercicio  
Sua empresa tem um aplicativo que usa instâncias do Amazon EC2 para executar o site voltado para o cliente e instâncias de banco de dados do Amazon RDS para armazenar informações pessoais dos clientes. Como o desenvolvedor deve configurar a VPC de acordo com as práticas recomendadas?

Resposta:   
Colocar as instâncias do Amazon EC2 em uma sub-rede pública e as instâncias de bancos de dados do Amazon RDS em uma sub-rede privada.

Uma **sub-rede** é uma seção de uma VPC na qual você pode agrupar recursos com base em necessidades operacionais ou de segurança. As sub-redes podem ser públicas ou privadas.  
  
As sub-redes públicas têm recursos que precisam ser acessíveis pelo público, como o site de uma loja on-line.  
  
As sub-redes privadas têm recursos que devem ser acessíveis apenas pela sua rede privada, como um banco de dados contendo informações pessoais dos clientes e históricos de pedidos.

2-

Qual declaração descreve melhor a lista de controle de **acesso de rede comum de uma conta AWS**?

a) Ela é stateless e nega todo o tráfego de entrada e saída.

b) Ela é stateful e permite todo o tráfego de entrada e saída.

c) Ela é stateless e permite todo o tráfego de entrada e saída.

d) Ela é stateful e nega todo o tráfego de entrada e saída.

As ACLs de rede (listas de controle de acesso de rede) fazem a filtragem de pacotes **stateless**. Elas não se lembram de nada e verificam os pacotes que atravessam a fronteira da sub-rede em todos os sentidos: entrada e saída.  
  
Cada conta AWS tem uma ACL de rede comum. Ao configurar a VPC, você pode usar a ACL de rede comum da conta ou criar ACLs de rede personalizadas.  
  
Por padrão, a ACL de rede comum da conta permite todo o tráfego de entrada e saída, mas você pode modificá-la adicionando suas próprias regras. Para ACLs de rede personalizadas, todo o tráfego de entrada e saída é negado até que você adicione regras para especificar qual tráfego deve ser permitido. Além disso, todas as ACLs de rede têm uma regra de negação explícita. Essa regra garante que, se um pacote não corresponder a nenhuma das outras regras na lista, ele será negado.

Qual declaração descreve melhor os grupos de segurança?

1. Eles são stateful e negam todo o tráfego de entrada por padrão.
2. Eles são stateful e permitem todo o tráfego de entrada por padrão.
3. Eles são stateless e negam todo o tráfego de entrada por padrão.
4. Eles são stateless e permitem todo o tráfego de entrada por padrão.

Grupos de segurança são stateful. Isso significa que eles usam padrões e fluxos de tráfego anteriores ao avaliar novas solicitações para uma instância.  
  
Por padrão, os grupos de segurança negam todo o tráfego de entrada, mas você pode adicionar regras personalizadas para atender às suas necessidades operacionais e de segurança.

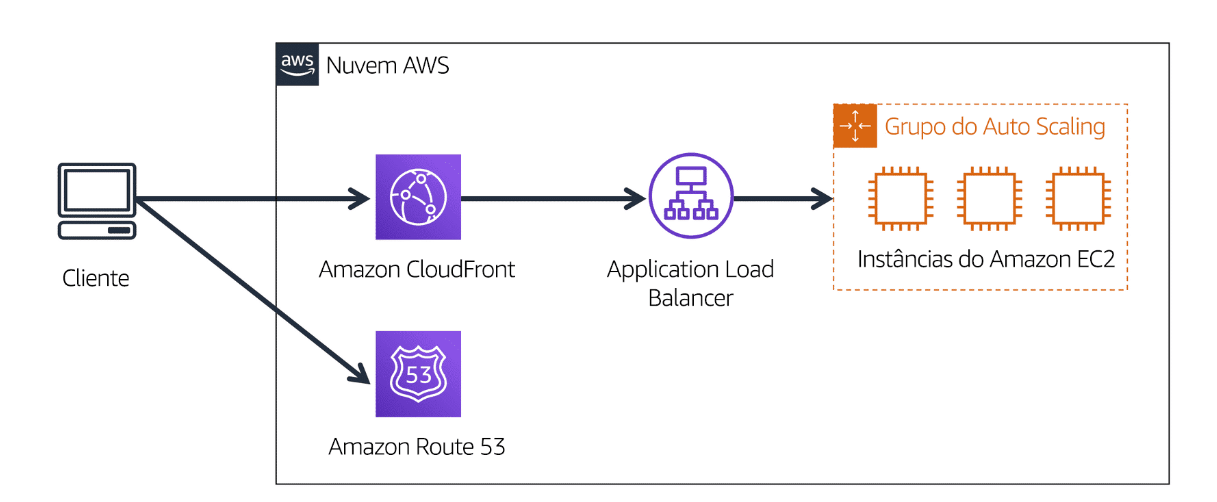
* O Amazon Virtual Private Cloud (Amazon VPC) é um serviço que permite provisionar uma seção isolada da nuvem AWS. Nesta seção isolada, é possível iniciar recursos em uma rede virtual definida por você.
* O AWS Direct Connect é um serviço que permite estabelecer uma conexão privada dedicada entre o seu data center e a VPC.
* O Amazon CloudFront é um serviço de entrega de conteúdo. Ele usa uma rede de locais de borda para armazenar conteúdo em cache e entregar conteúdo para clientes em todo o mundo.

## **Domain Name System (DNS)**

traduz nomes de sites para endereços IP (Internet Protocol). Os servidores DNS (Domain Name System, ou Sistema de Nomes de Domínios) são os responsáveis por localizar e traduzir para números [IP (Internet Protocol)](https://canaltech.com.br/software/o-que-e-ip/) os endereços dos sites que digitamos nos navegadores

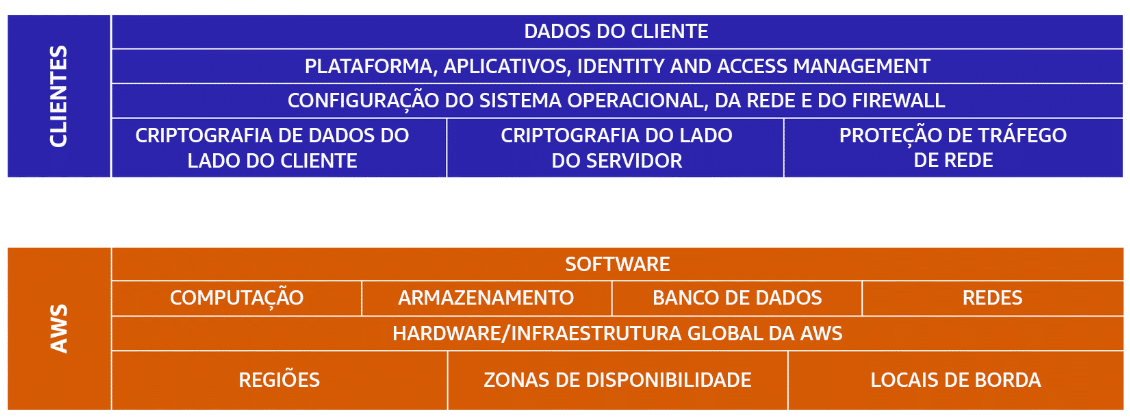
## [**Amazon Route 53**](https://aws.amazon.com/route53)

é um serviço web de DNS. Oferece aos desenvolvedores e empresas uma maneira confiável de rotear os usuários finais para aplicativos da internet hospedados na AWS



# **SECURITY**

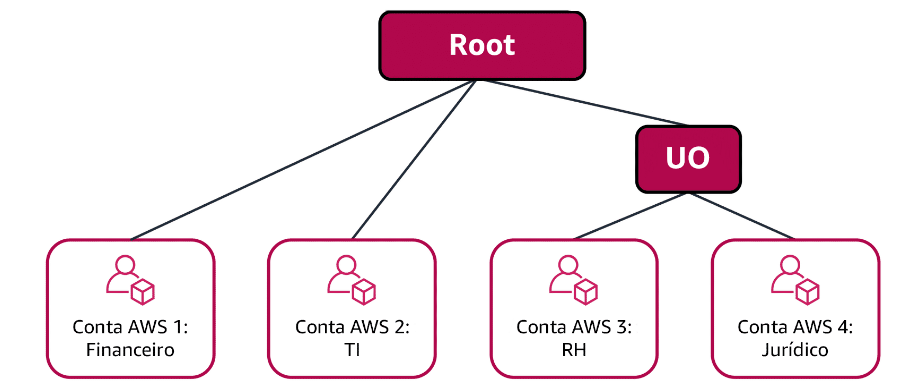
## **Modelo de responsabilidade compartilhada**



## **AWS Organizations**

A maneira mais fácil de pensar no Organizations é como um local central para gerenciar várias contas da AWS.

principais recursos:

* gerenciamento centralizado de todas as suas contas na AWS. Outra vantagem do faturamento consolidado é o desconto em massa.
* agrupamento hierárquico de suas contas para atender a requisitos de segurança, conformidade ou necessidades orçamentais, Isso significa que você pode agrupar contas em unidades organizacionais, ou OUs, tipos de negócios ou business units. 
* faturamento consolidado de todas as contas de membros.  você pode usar a conta principal da sua organização para consolidar e pagar todas as contas de outros membros.
* controle sobre serviços da WS e as ações de API. Cada conta pode acessar como administrador da conta principal de uma organização.

cobrança consolidada é outro recurso do AWS Organizations

## [**AWS Artifact**](https://aws.amazon.com/artifact) é um serviço que fornece acesso sob demanda a relatórios de segurança e conformidade da AWS e a contratos on-line selecionados. O AWS Artifact tem duas seções principais: AWS Artifact Agreements e o AWS Artifact Reports.

Vc pode **Acessar relatórios de conformidade da AWS sob demanda. Analisar, aceitar e gerenciar seus contratos com a AWS.**

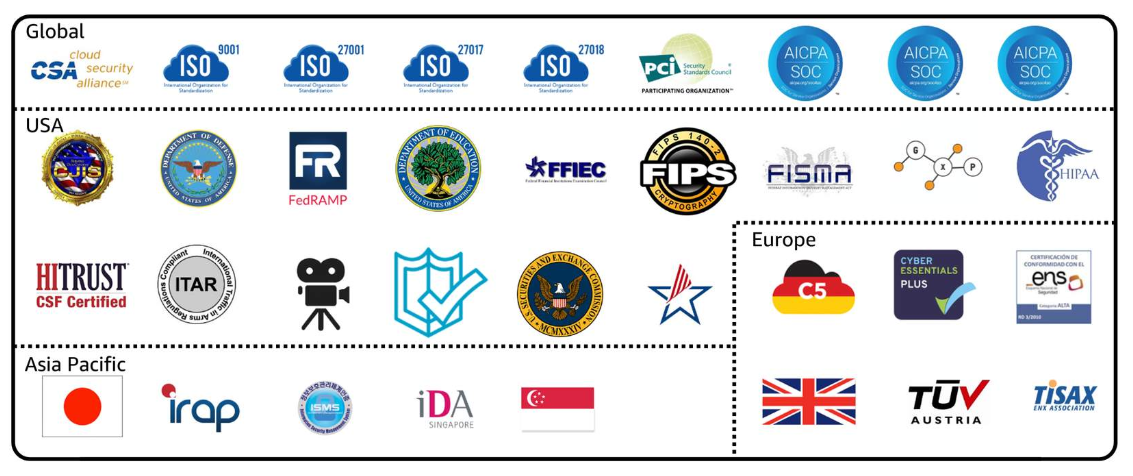
* **AWS Artifact Agreements**

Suponha que sua empresa precise assinar um contrato com a AWS em relação ao uso de determinados tipos de informações em todos os serviços AWS. Você pode fazer isso pelo **AWS Artifact Agreements**.  
No AWS Artifact Agreements, você pode revisar, aceitar e gerenciar contratos para uma conta individual e para todas as suas contas no AWS Organizations. Diferentes tipos de acordos são oferecidos para atender às necessidades dos clientes sujeitos a regulamentações específicas, como a Lei de Portabilidade e Responsabilidade dos Provedores de Saúde dos EUA (HIPAA).

* **AWS Artifact Reports**

Suponha que um membro da equipe de desenvolvimento da sua empresa esteja criando um aplicativo e precise de mais informações sobre a responsabilidade em cumprir determinados padrões regulatórios. Você pode recomendar o acesso a essas informações em **AWS Artifact Reports**.  
O AWS Artifact Reports fornece relatórios de conformidade por auditores terceirizados. Esses auditores testaram e verificaram se a AWS está em conformidade com diversas normas e regulamentações de segurança globais, regionais e específicas do setor. O AWS Artifact Reports se mantém atualizado com os relatórios publicados mais recentes. Você pode fornecer os artefatos de auditoria da AWS aos auditores ou reguladores como evidência dos controles de segurança da AWS.

O [**Centro de conformidade para o cliente**](https://aws.amazon.com/compliance/customer-center/) contém recursos que ajudam você a saber mais sobre a conformidade da AWS.



## **DDoS ou DDoS. Negação de serviço distribuída.**

Em um ataque DDoS, o agente mal-intencionado tenta sobrecarregar a capacidade da sua aplicação para que qualquer outra requisição que ocorra nos seus serviços seja negada.

**AWS Shield Standard** protege automaticamente todos os clientes AWS sem nenhum custo. Ele protege seus recursos AWS contra os tipos de ataques DDoS mais comuns e frequentes.  
À medida que o tráfego de rede ingressa em seus aplicativos, o AWS Shield Standard usa diversas técnicas de análise para detectar tráfego mal-intencionado em tempo real e mitigá-lo automaticamente.

O **AWS Shield Advanced** é um serviço pago que fornece diagnósticos detalhados de ataques e a capacidade de detectar e mitigar ataques elaborados de DDoS.  
Ele também se integra a outros serviços, como o Amazon CloudFront, o Amazon Route 53 e o Elastic Load Balancing. Além disso, você pode integrar o AWS Shield ao AWS WAF escrevendo regras personalizadas para mitigar ataques complexos de DDoS.

## [**AWS Key Management Service (AWS KMS)**](https://aws.amazon.com/kms)

permite que você execute operações de criptografia pelo uso de **chaves de criptografia**. Uma chave de criptografia é uma cadeia aleatória de dígitos usada para bloquear (criptografar) e desbloquear (descriptografar) dados. Você pode usar o AWS KMS para criar, gerenciar e usar chaves de criptografia. Você também pode controlar o uso de chaves em uma ampla gama de serviços e em seus aplicativos.

você deve garantir que os dados de seus aplicativos estejam protegidos durante o armazenamento **(criptografia em repouso)** e sendo transmitidos **(criptografia em trânsito)**.

## [**AWS WAF**](https://aws.amazon.com/waf)

é um firewall de aplicativo web que permite monitorar solicitações de rede que entram em seus aplicativos web.

O AWS WAF trabalha em conjunto com o Amazon CloudFront e um balanceador de carga de aplicativo. Lembre-se das listas de controle de acesso de rede que você aprendeu em um módulo anterior. O AWS WAF funciona de forma semelhante para bloquear ou permitir o tráfego. No entanto, ele faz isso usando uma [**lista de controle de acesso (ACL) da web**](https://docs.aws.amazon.com/waf/latest/developerguide/web-acl.html) para proteger seus recursos AWS.

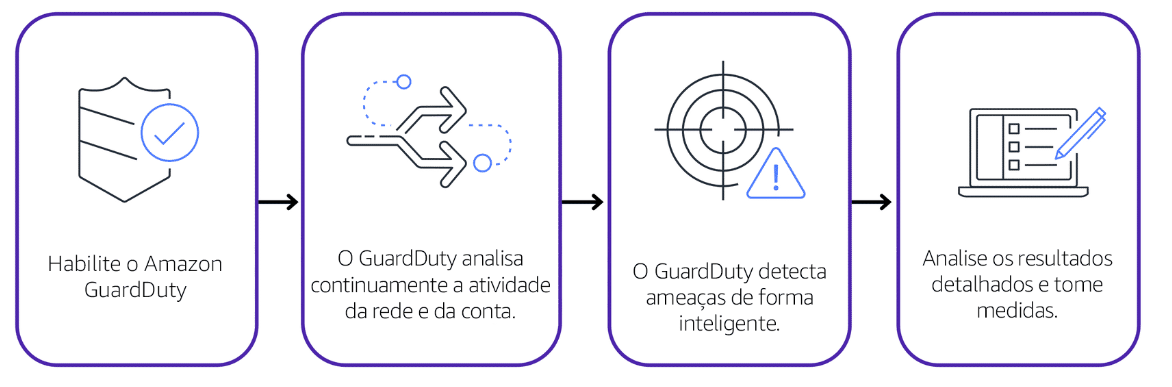
Veja um exemplo de como você pode usar o AWS WAF para permitir e bloquear solicitações específicas.

Suponha que o aplicativo tenha recebido solicitações de rede mal-intencionadas de vários endereços IP. Você quer impedir que essas solicitações continuem a acessar seu aplicativo, mas também deseja garantir que usuários legítimos ainda possam acessá-lo. Você configura a ACL da web para permitir todas as solicitações, exceto aquelas dos endereços IP que você especificou.

Quando uma solicitação entra no AWS WAF, ele confere a lista de regras configurada na ACL da web. Se uma solicitação não for proveniente de um dos endereços IP bloqueados, o AWS WAF permite o acesso ao aplicativo.

[**Amazon GuardDuty**](https://aws.amazon.com/guardduty)

é um serviço que fornece detecção inteligente de ameaças para sua infraestrutura e seus recursos AWS. Ele identifica ameaças monitorando continuamente a atividade da rede e o comportamento da conta no seu ambiente AWS.



Depois de habilitar o GuardDuty para sua conta AWS, ele começa a monitorar sua atividade de rede e conta. Você não precisa implantar ou gerenciar nenhum outro software de segurança. O GuardDuty analisa continuamente dados de várias fontes da AWS, incluindo logs de fluxo de VPC e logs de DNS.

Se ele detectar ameaças, você poderá revisar as descobertas detalhadas no AWS Management Console. As descobertas incluem etapas recomendadas para a correção. Você também pode configurar as funções do AWS Lambda para executar as etapas de correção automaticamente em resposta às descobertas de segurança do GuardDuty.

Sempre gratuito

[https://aws.amazon.com/pt/free/?all-free-tier.sort-by=item.additionalFields.SortRank&all-free-tier.sort-order=asc&awsf.Free%20Tier%20Types=\*all&awsf.Free%20Tier%20Categories=\*all](https://aws.amazon.com/pt/free/?all-free-tier.sort-by=item.additionalFields.SortRank&all-free-tier.sort-order=asc&awsf.Free%20Tier%20Types=*all&awsf.Free%20Tier%20Categories=*all)

<https://aws.amazon.com/pt/premiumsupport/plans/>