Contents

[**AWS NETWORKING** 1](#_Toc148431384)

[**Amazon Virtual Private Cloud (Amazon VPC)** 1](#_Toc148431385)

[**Grupo de segurança** 12](#_Toc148431386)

[**AWS DirectX Connect** 12](#_Toc148431387)

[**Domain Name System (DNS)** 14](#_Toc148431388)

[**Amazon Route 53** 15](#_Toc148431389)

[**Amazon CloudFront** 15](#_Toc148431390)

[**Entregue conteúdo com segurança com baixa latência e altas velocidades de transferência** 15](#_Toc148431391)

[**LightSail** 15](#_Toc148431392)

# **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.

Uma VPC tem escopo **regional** e ela é responsável por manter segura e isolada (de outras infra-estruturas) todos os serviços e recursos de uma infra-estrutura.

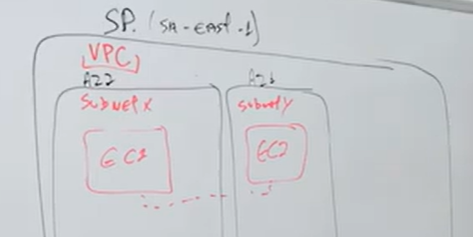
Uma VPC é composta pode sub redes (subnets), umas para cada zona de disponilidade. Lembre-se que uma zona de disponibilidade é uma datacenter, é uma estrutura física e independente e são conecatadas com as subnets.

VPC (Virginia EUA) Ipv4 10.0.0.0/16

VPC (São Paulo) Ipv4 11.0.0.0/16

subnet us-east-1b Ipv4 10.0.1.0/16

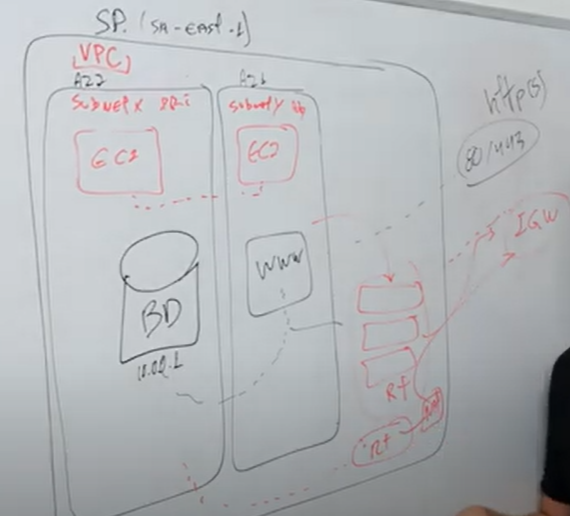
subnet us-east-1b Ipv4 10.0.1.0/16



A AWS tem uma VPC padrão, mas não é recomendado usar ela (ela foi criada para fazer o mapeamento dos recursos fundamentais da sua conta e não para o seus projetos). Você ainda pode usar faixas de ip´s para recursos especificos, uma faixa para API, outra para workers e assim por diante.



O RT (route table) define como as subnet estarão organizadas e o IGW (internet gate way) faz o tráfico com a internert



<https://www.youtube.com/watch?v=3UCwOfHKZ38>

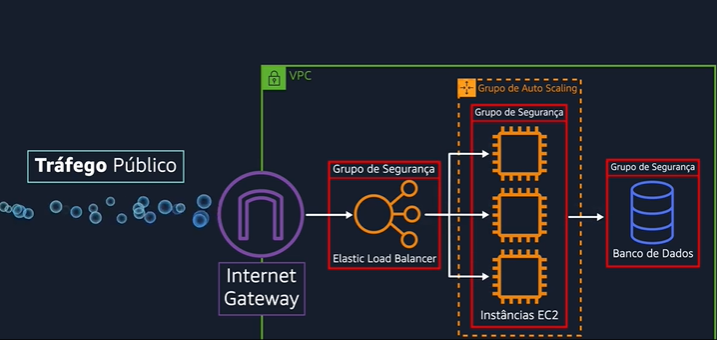
A VPC permite que você defina o seu intervalo de preços privados para fazer a alocação de recursos, como instâncias EC2 e Load Balancing dentro da sua rede.

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

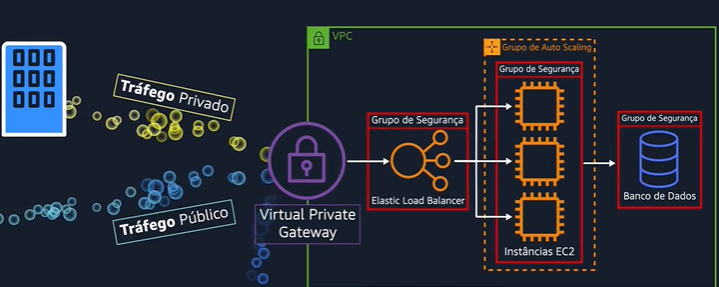
Existem cenários onde você pode ter recursos que deseja que sejam acessíveis apenas se alguém estiver conectado à sua rede privada. Por exemplo, aplicações internas como uma aplicação de RH ou um banco de dados.

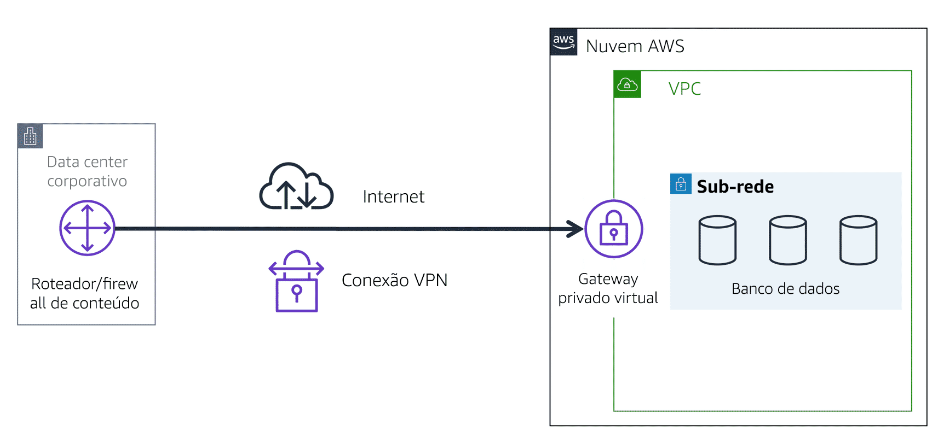
**Publico**: Para permitir a comunicação de tráfego que vem da internet para sua VPC, você deve associar um recurso que chamamos de internet Gateway, ou GW, a sua VPC

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.



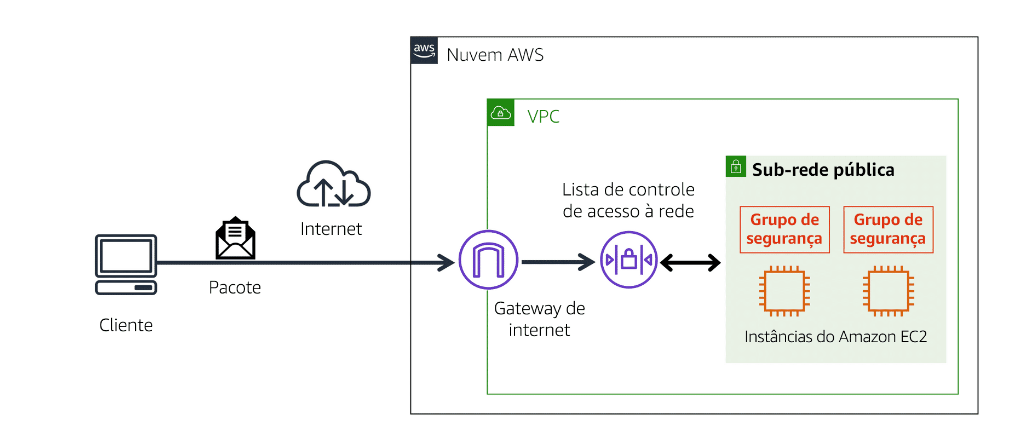


O AWS Direct Connect fornece uma linha física que conecta sua rede do datacenter à sua VPC. Isso pode ajudar você a atender às necessidades regulamentares e de conformidade bem como contornar potenciais problemas de largura de banda.

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.**



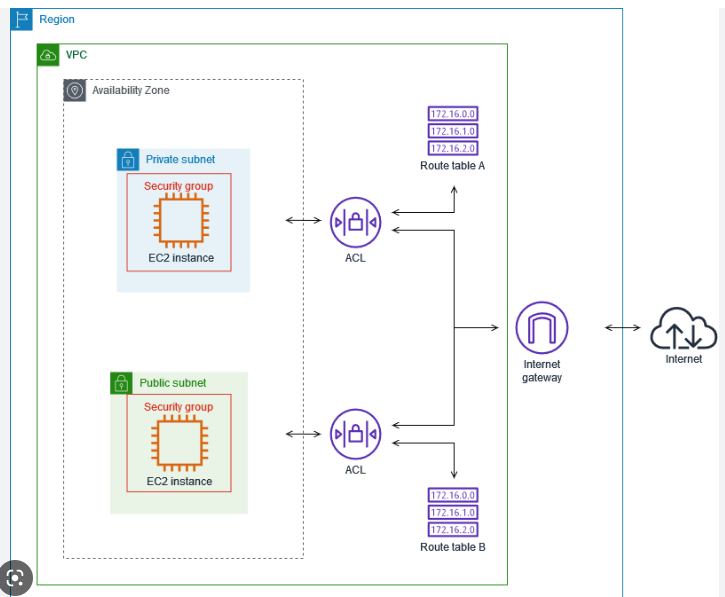
 E essa verificação é necessária para validar se o pacote tem permissões para sair ou entrar na subnet com base em quem enviou e como ele está tentando se comunicar. As network ACLs verificam o fluxo de dados que entram e saem de uma subnet. Da mesma forma que o controle de passaportes. O fluxo de dados 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.



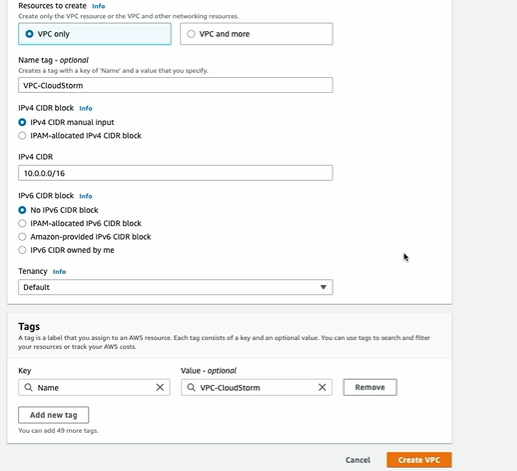
As ACLs de rede (listas de controle de acesso de rede) fazem a filtragem de pacotes stateless . Elas não se lembram de nada e verificam os pacotes que atravessam a fronteira da sub-rede em todos os sentidos: entrada e saída.

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.

**VPC – na pratica**

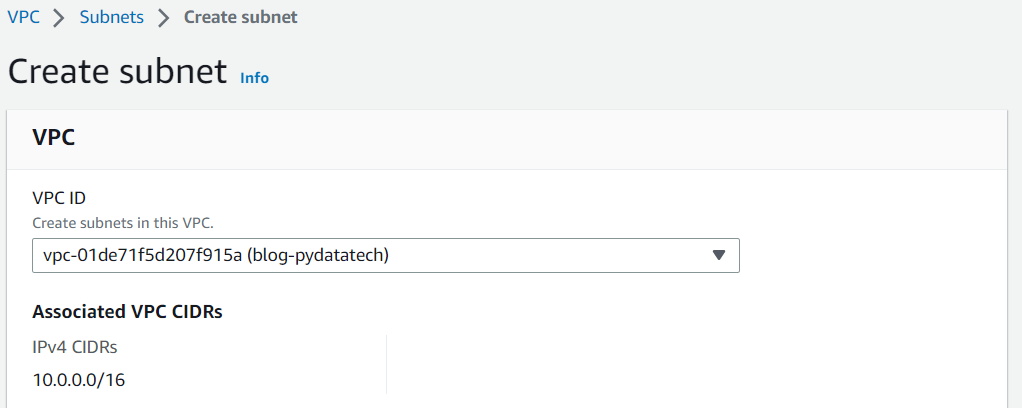
1 ) Criamos uma VPC com o IPV4 – CIDR igual a 10.0.0.0/16. Na região da Viginia.



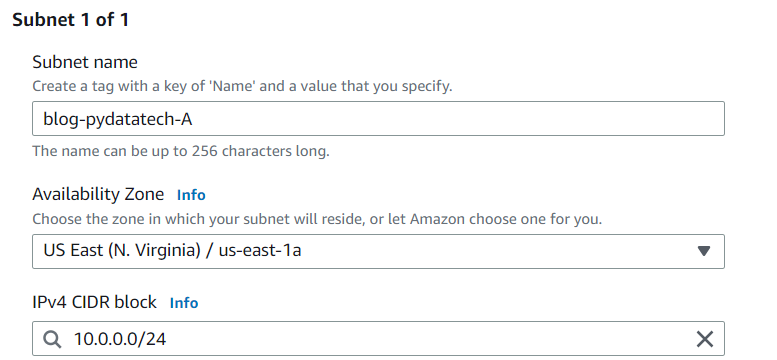
2) Criar subnet

Como as VPC foi criada no nivel 16, as subnets precisam ser criadas no nivel 24 porque estão 1 nivel abaixo da topologia dessa rede.

Ao clicar em criar subnet é precis conectar com a VPC que foi criada



As subnet serão criadas para cada zona de disponibilidade seguindo um padrão.



**Subnet 1**:

Name: blog-pydatatech-**A**  
Zona: US East (N.Virginia) / us-east-1**a**   
Ipv4: 10.0.**0**.0/24

**Subnet 2**:

Name: blog-pydatatech-**B**  
Zona: US East (N.Virginia) / us-east-1**b**  
Ipv4: 10.0.**1**.0/24

**Subnet 3**:

Name: blog-pydatatech-**C**  
Zona: US East (N.Virginia) / us-east-1c  
Ipv4: 10.0.**2**.0/24

**Subnet 4**:

Name: blog-pydatatech-**D**  
Zona: US East (N.Virginia) / us-east-1d  
Ipv4: 10.0.**3**.0/24

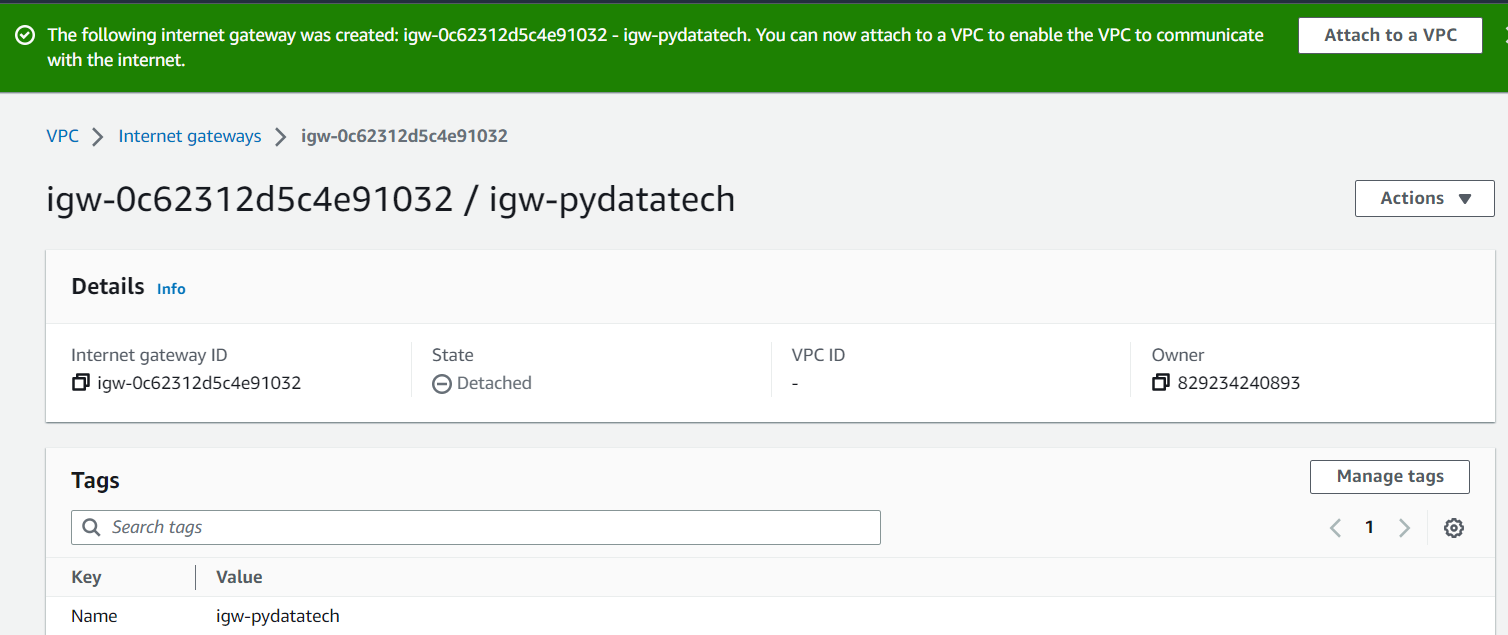
**Subnet 5**:

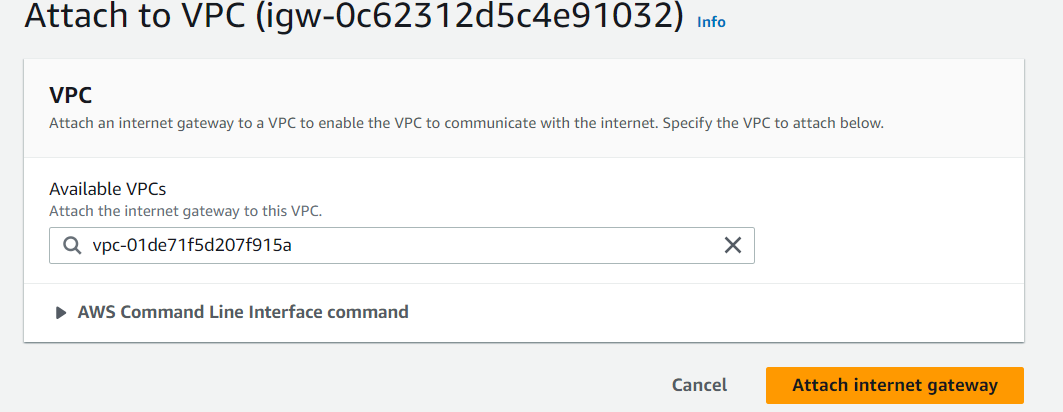
Name: blog-pydatatech-**E**  
Zona: US East (N.Virginia) / us-east-1**e**  
Ipv4: 10.0.**4**.0/24

**Subnet 6**:

Name: blog-pydatatech-F  
Zona: US East (N.Virginia) / us-east-1f  
Ipv4: 10.0.**5**.0/24

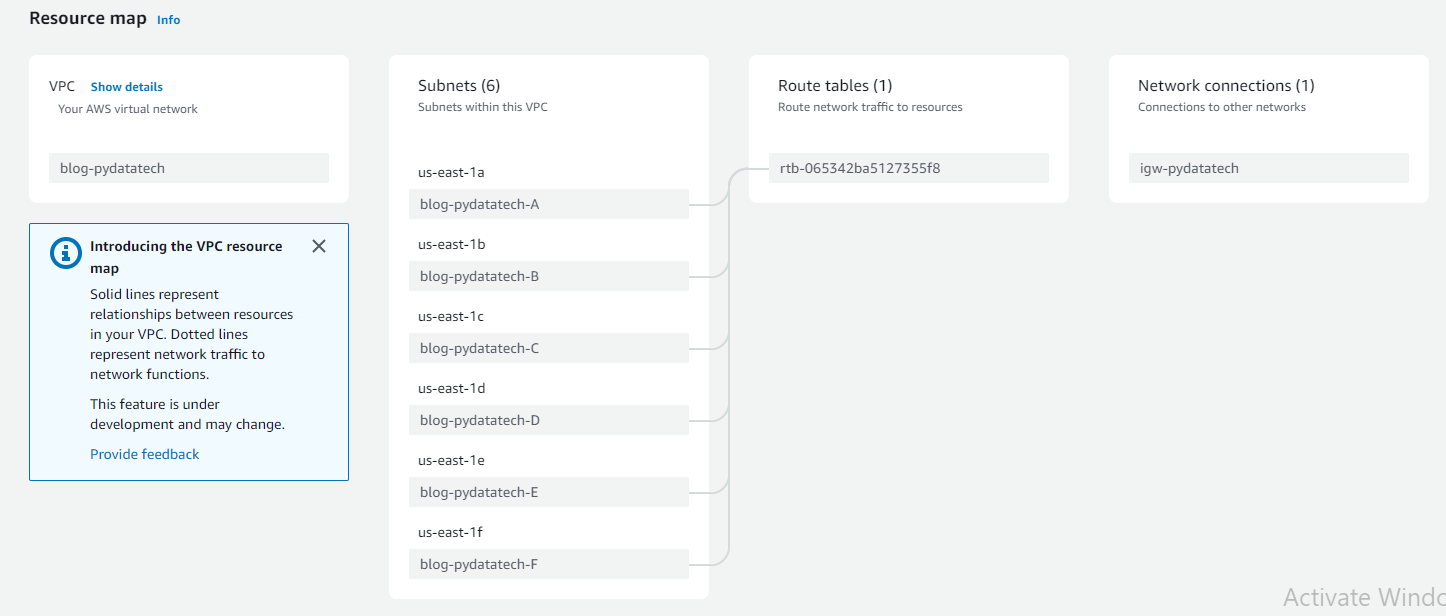
**3)** Criar o internet gate way e associar com a VPC (attach to a VPC)

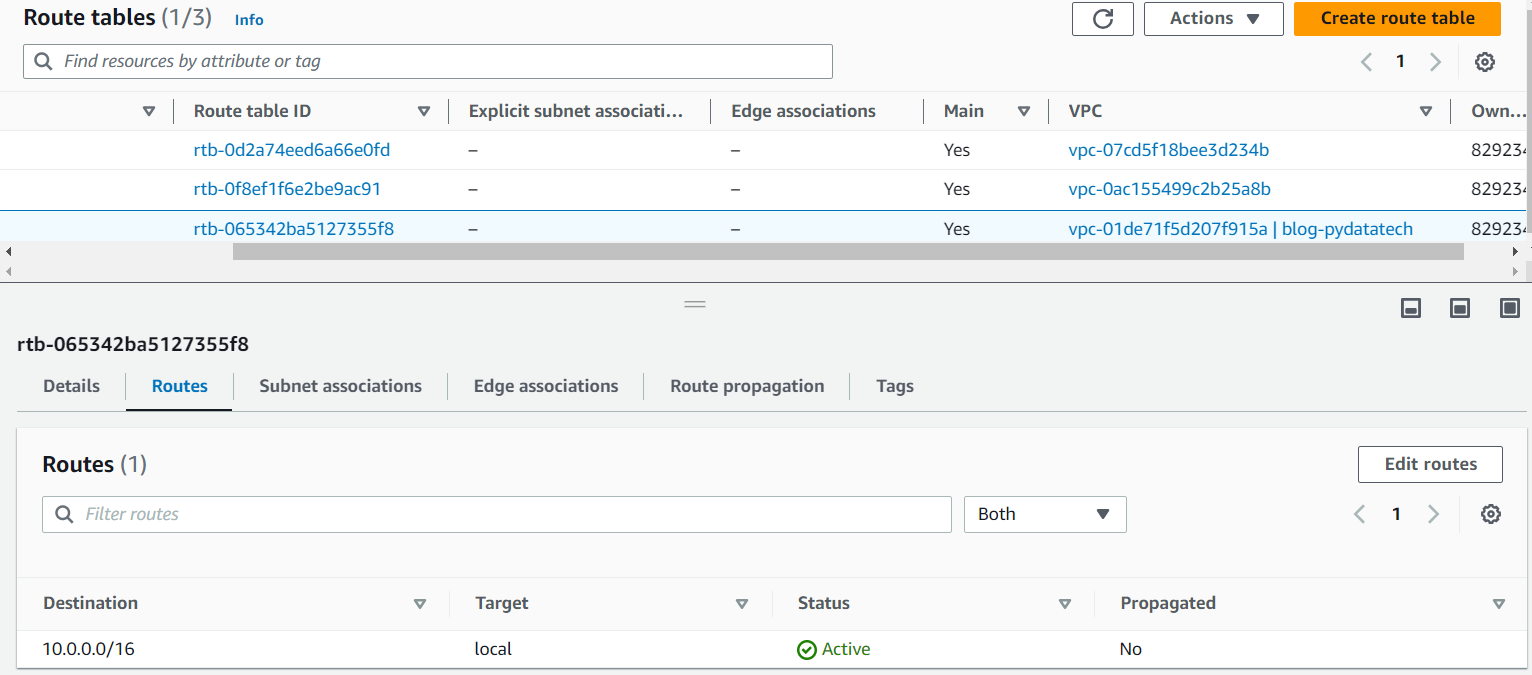
[](https://aws.amazon.com/directconnect/)

[](https://aws.amazon.com/directconnect/)

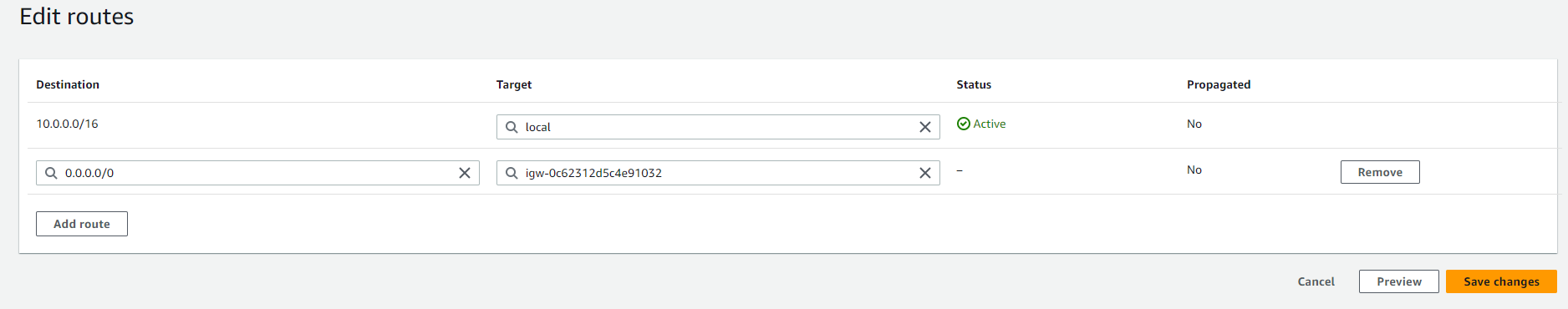
Aos criar uma VPC, foi criar automaticamente uma tabelas de roteamento, mas ela não está conectada com o gateway, é preciso entrar nas tabelas de roteamento e criar a conexão.

Antes

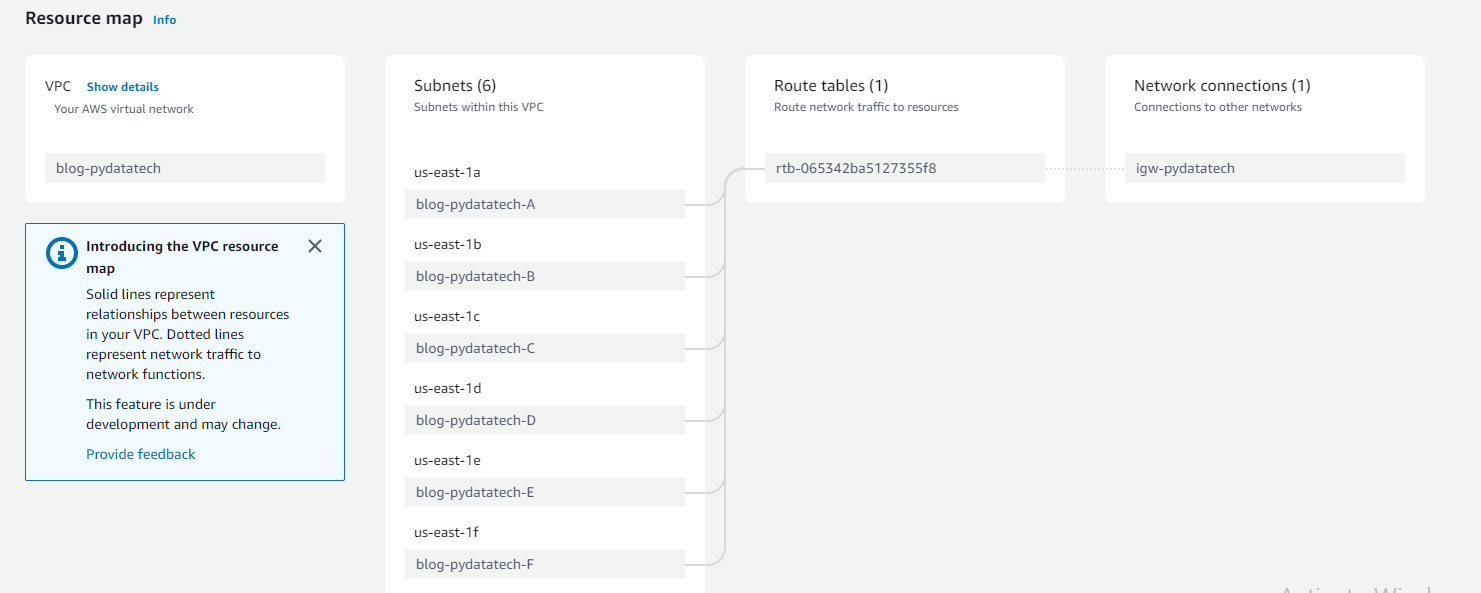




Clique em Edit routes depois clique em add routes e adicionar o 0.0.0.0/0 e procure por internet gateway e adcionte o gateway que criamos

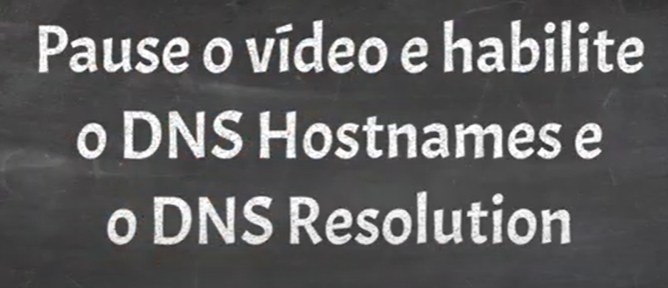


Depois de conectar



Topicos para verificar na VPC:  
enable DNS resolution: habilite para criar DNS.

enadisable auto assign public ip aws



## [**Grupo de segurança**](https://aws.amazon.com/directconnect/)

É o quem dá permissão a um recurso acessar outro recurso ou serviços através da rede (não é a mesma coisa que o grupo do IAM).

Quando uma VPC é criada, o grupo de segurança também é criado, mas é recomendado criar seus próprios grupos.

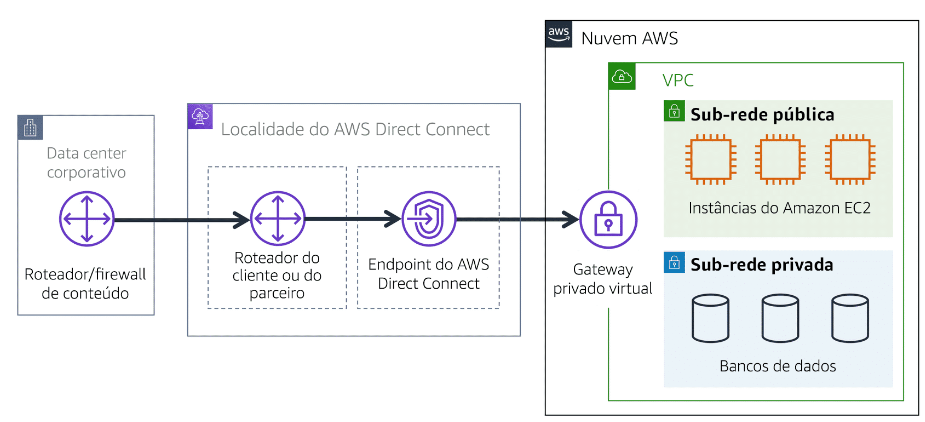
## [**AWS DirectX Connect**](https://aws.amazon.com/directconnect/)

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.

## **Edge Locations :**

Edge Location ou Pontos de Presença são pequenos data centers utilizados para distribuir serviços com a menor latência possível, como Route 53, CloudFront , WAF/Shield.

Tipos:

-

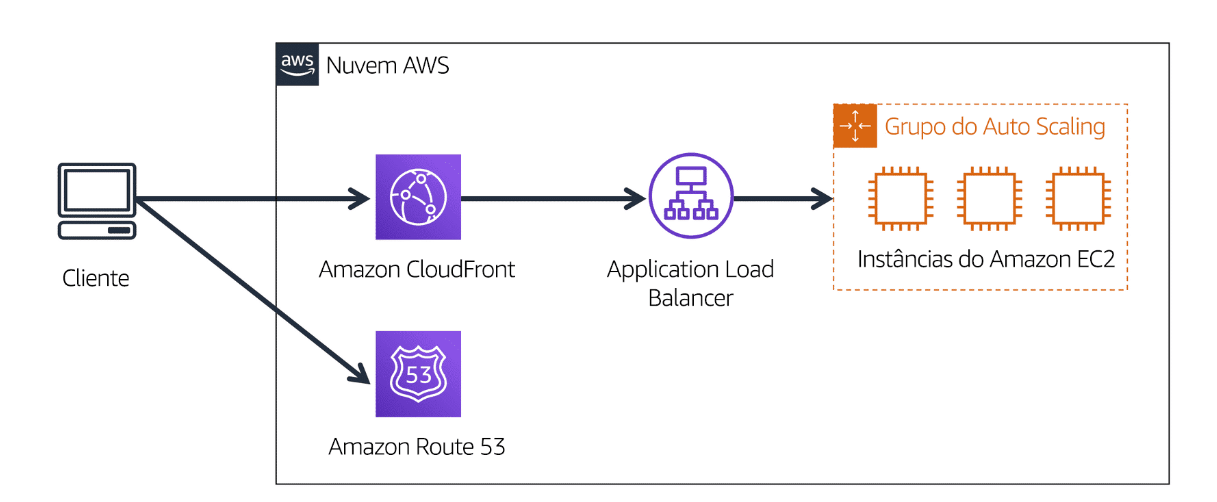
<https://aws.amazon.com/pt/cloudfront/features/?whats-new-cloudfront.sort-by=item.additionalFields.postDateTime&whats-new-cloudfront.sort-order=desc#Global_Edge_Network>

## **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)

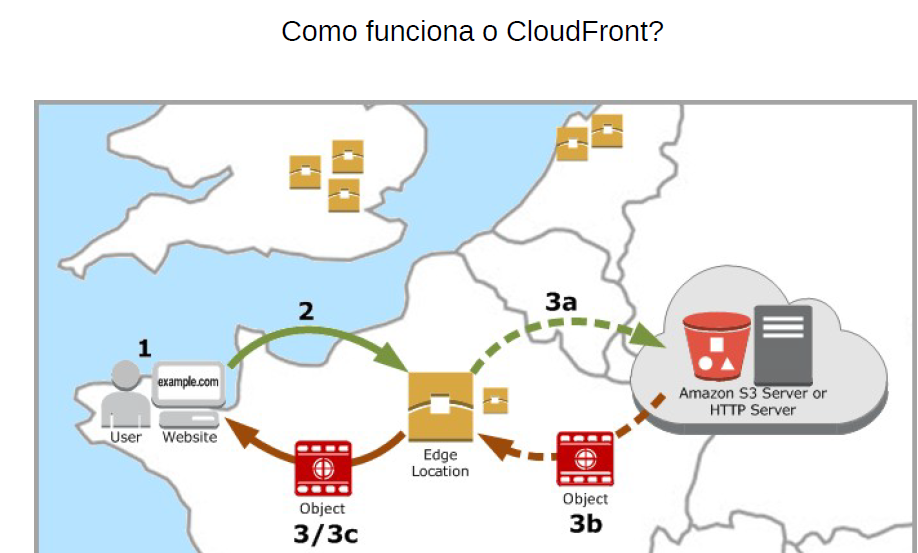
é um serviço web de DNS. Oferece aos desenvolvedores e empresas uma maneira confiável de rotear os usuários finais para aplicativos da internet hospedados na AWS



## **Amazon CloudFront**

O Amazon CloudFront é um serviço que **acelera a distribuição do** conteúdo estático e dinâmico da web (CDN), como arquivos .html, .css, .js e arquivos de imagem, para os usuários. Quando um usuário solicita um conteúdo que você está disponibilizando com o CloudFront, a solicitação é roteada para o ponto de presença que fornece a menor latência (atraso), assim o conteúdo é entregue com a melhor performance possível

É um Serviço de CDN Content Delivery Network que atua na camada de distribuição de conteúdo estático nas bordas (Edge location) ou pontos de presença da AWS para agilizar a entrega de conteúdo ao usuário de acordo com sua localização para ter a menor latência na entrega e performance de sua aplicação.



**1) O usuário acessa o site/aplicativo solicitando um ou mais arquivos**

**2) O DNS roteia a solicitação**

**3) O CloudFront procura os arquivos solicitados no Cache e aplica as tratativas. para o Ponto de Presença (Edge Location).**

**3a) O CloudFront compara a solicitação e encaminha ao servidor de origem**

**3b) Os servidores de origem enviam os arquivos aos Pontos de Presença**

**3c) O CloudFront armazena em cache os arquivos e os envia para o usuário**

**Vantagens e Casos de uso**

* Acelerar a entrega de conteúdo estático
* Fornecer vídeos de streaming ao vivo ou sobre demanda
* Criptografar campos específicos durante todo o processamento do sistema
* Personalizar na borde
* Fornecer conteúdo privado usando as personalizações do Lambda@Edge

Por meio de uma policy é possível configurar para que somente o cloud front acesse o S3, mesmo se a pessoa tiver o endereço do S3

**Entregue conteúdo com segurança com baixa latência e altas velocidades de transferência**

Atua integrado com diversos serviços gerenciados da aws como por exemplo S3,

* EC2, ELB entre outros.

Possui uma camada de segurança integrado ao serviço AWS Sheild Stardard e WAF por default para atuar na defesa de ataques DDOS.

https://aws.amazon.com/pt/cloudformation/features/

## **LightSail**

O Amazon Lightsail oferece instâncias de servidor privado virtual (VPS) fáceis de usar, contêineres, armazenamento, bancos de dados e muito mais a um preço mensal econômico.

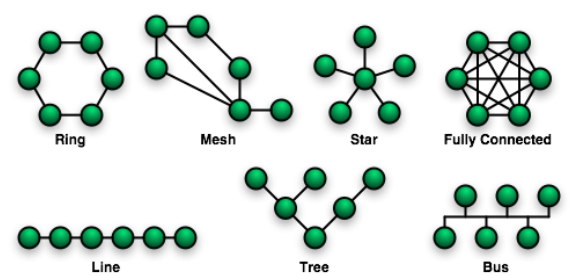
**Topologia**

Topologia de rede é a forma como os dispositivos estão conectados, como as maquinas os hubs (é o processo pelo qual se transmite ou difunde determinada informação )

1º Topologia física: se refere a como os cabos e dispositivos estão conectados:

2ª topologia logica. Fluxo de dados e sinais através da rede.

Diversos tipos de topologia: <https://pt.wikipedia.org/wiki/Topologia_de_rede>



**classes IP**

ou também nível de IP, grupo de IP (varia de autor para autor)

<https://www.meridianoutpost.com/resources/articles/IP-classes.php>

<https://pplware.sapo.pt/tutoriais/networking/classes-de-endereos-ip-sabe-quais-so/>

[https://pt.wikipedia.org/wiki/Endere%C3%A7o\_IP](https://pt.wikipedia.org/wiki/Endereço_IP)

<https://www.youtube.com/@StartiOficial/featured>