



Entendendo a Criação de uma VPC na AWS

Como funciona a rede virtual que isola sua infraestrutura na nuvem

Tópicos

01

VPC

O que é e como funciona a rede virtual

02

Subnets

Pública vs Privada — segmentando a rede

03

Route Tables

Como o tráfego é direcionado

04

Internet Gateway

Conectando a VPC à internet

05

CIDR & IPs

Calculando endereços disponíveis

O que é uma VPC?

Virtual Private Cloud

Uma VPC é uma rede virtual isolada dentro da AWS onde você provisiona todos os seus recursos.

Pense nela como o "terreno" da sua infraestrutura na nuvem. Você define o espaço de endereçamento IP (bloco CIDR) e tudo que você cria — EC2, RDS, ECS — vive dentro dessa rede.

Cada VPC é completamente isolada das outras. Isso permite separar ambientes como DEV, HML e PRD sem interferência entre eles.

AWS Cloud

VPC — DEV

11.0.0.0/24

VPC — HML

12.0.0.0/24

VPC — PRD

13.0.0.0/24

Subnets

Dividindo a VPC em segmentos menores

Subnets são subdivisões da VPC que permitem segmentar a rede em blocos menores. Cada subnet é associada a uma Availability Zone (AZ) específica, trazendo resiliência e organização à arquitetura.

Subnet Pública

- Possui rota para o Internet Gateway
- Recursos podem receber tráfego direto da internet
- Uso típico: ALB (Load Balancer), NAT Gateway, Bastion Host
- Recursos precisam de IP público ou Elastic IP

Subnet Privada

- Sem rota direta para o Internet Gateway
- Recursos protegidos e inacessíveis pela internet
- Uso típico: ECS Tasks, RDS, Lambda, instâncias internas
- Acessa internet via NAT Gateway (só saída)

Route Tables

O GPS da sua rede na AWS

Route Tables são tabelas de roteamento que definem para onde o tráfego de rede deve ser direcionado. Cada subnet precisa estar associada a uma Route Table.

Toda Route Table possui uma rota "local" automática, permitindo comunicação entre todos os recursos da mesma VPC. As rotas adicionais determinam se a subnet é pública ou privada.

Route Table – Subnet Pública

Destino	Target
11.0.0.0/24	local
0.0.0.0/0	Internet Gateway

Route Table – Subnet Privada

Destino	Target
11.0.0.0/24	local
0.0.0.0/0	NAT Gateway

A rota 0.0.0.0/0 é o que diferencia uma subnet pública de uma privada: Internet Gateway = pública, NAT Gateway = privada.

Internet Gateway

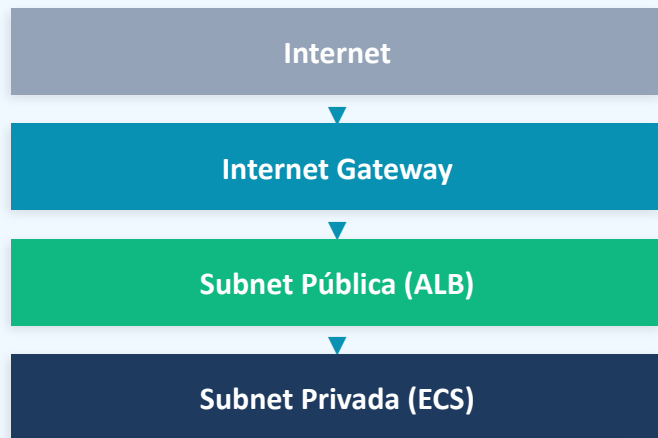
A porta de entrada e saída da VPC

O Internet Gateway (IGW) é o componente que conecta a VPC à internet pública.

Sem um IGW, a VPC fica completamente isolada do mundo externo. Ele é altamente disponível e escalável por padrão — a AWS gerencia isso automaticamente.

Cada VPC pode ter apenas um IGW associado.

Fluxo de Comunicação



E o NAT Gateway? Ele fica na subnet pública e permite que recursos em subnets privadas acessem a internet (para baixar pacotes, atualizações, etc.), sem ficarem expostos a tráfego de entrada. O tráfego é só de saída.

Calculando IPs no CIDR

Quantos endereços cabem na sua rede?

Fórmula

$$\text{Total de IPs} = 2 ^ { (32 - \text{prefixo}) }$$

IPs Utilizáveis = Total - 5 (AWS reserva 5 IPs por subnet)

Exemplo: VPC DEV — 11.0.0.0/24

- 1 Prefixo /24 → bits livres para hosts = $32 - 24 = 8$ bits
- 2 Total de IPs = $2^8 = 256$ endereços
- 3 Range: 11.0.0.0 até 11.0.0.255
- 4 IPs utilizáveis na AWS = $256 - 5 = 251$ endereços por subnet

IPs Reservados pela AWS

Por que perdemos 5 IPs por subnet?

Endereço	Exemplo (/24)	Uso
Primeiro IP	11.0.0.0	Endereço de rede
Segundo IP	11.0.0.1	Roteador da VPC (AWS)
Terceiro IP	11.0.0.2	Servidor DNS da AWS
Quarto IP	11.0.0.3	Reservado para uso futuro
Último IP	11.0.0.255	Broadcast (não suportado na VPC)

Referência Rápida – CIDRs Comuns

/16

65.536 IPs (65.531 úteis)

/20

4.096 IPs (4.091 úteis)

/24

256 IPs (251 úteis)

/27

32 IPs (27 úteis)

Subnets Públicas e Privadas (Aplicação)

Nome	CIDR	AZ	Finalidade
futura-pvt-subnet-app-1-dev	11.0.0.0/27	us-east-2a	EC2 / ECS Aplicação
futura-pvt-subnet-app-2-dev	11.0.0.32/27	us-east-2b	EC2 / ECS Aplicação
futura-pub-subnet-app-1-dev	11.0.0.64/27	us-east-2a	ALB / Recursos públicos
futura-pub-subnet-app-2-dev	11.0.0.96/27	us-east-2b	ALB / Recursos públicos

Subnets Públicas e Privadas (Jenkins)

Nome	CIDR	AZ	Finalidade
futura-jenkins-pvt-subnet-cicd-1-dev	11.1.0.0/27	us-east-2a	Jenkins Agents (privado)
futura-jenkins-pvt-subnet-cicd-2-dev	11.1.0.32/27	us-east-2b	Jenkins Agents (privado)
futura-jenkins-pub-subnet-cicd-1-dev	11.1.0.64/27	us-east-2a	Jenkins CI/CD (público)
futura-jenkins-pub-subnet-cicd-2-dev	11.1.0.96/27	us-east-2b	Jenkins CI/CD (público)

VPC futura-vpc-app-dev

Subnets (4)

Subnets within this VPC

us-east-2a

A futura-pub-subnet-app-1-dev

11.0.0.64/27

No IPv6

A futura-pvt-subnet-app-1-dev

11.0.0.0/27

No IPv6

us-east-2b

B futura-pub-subnet-app-2-dev

11.0.0.96/27

No IPv6

B futura-pvt-subnet-app-2-dev

11.0.0.32/27

No IPv6

Route tables (3)

Route network traffic to resources

futura-rt-app-pub-dev

2 subnet associations

2 routes including local

futura-rt-app-pvt-dev

2 subnet associations

3 routes including local

rtb-028230a7c174d28b0

No subnet associations

1 route including local

Network Connections (2)

Connections to other networks

futura-igw-app-dev

Internet routes to 2 public subnets

2 private subnets route to the Internet

futura-nat-app-dev

Public NAT gateway

1 ENI with 1 EIP

VPC futura-vpc-app-dev

Subnets (4)

Subnets within this VPC

us-east-2a

A futura-pub-subnet-app-1-dev

11.0.0.64/27
No IPv6

A futura-pvt-subnet-app-1-dev

11.0.0.0/27
No IPv6

us-east-2b

B futura-pub-subnet-app-2-dev

11.0.0.96/27
No IPv6

B futura-pvt-subnet-app-2-dev

11.0.0.32/27
No IPv6

Route tables (3)

Route network traffic to resources

futura-rt-app-pub-dev

2 subnet associations
2 routes including local

futura-rt-app-pvt-dev

2 subnet associations
3 routes including local

rtb-028230a7c174d28b0

No subnet associations
1 route including local

Network Connections (2)

Connections to other networks

futura-igw-app-dev

Internet routes to 2 public subnets
2 private subnets route to the Internet

futura-nat-app-dev

Public NAT gateway
1 ENI with 1 EIP

VPC futura-vpc-app-dev

Subnets (4)

Subnets within this VPC

us-east-2a

A futura-pub-subnet-app-1-dev

11.0.0.64/27

No IPv6

A futura-pvt-subnet-app-1-dev

11.0.0.0/27

No IPv6

us-east-2b

B futura-pub-subnet-app-2-dev

11.0.0.96/27

No IPv6

B futura-pvt-subnet-app-2-dev

11.0.0.32/27

No IPv6

Route tables (3)

Route network traffic to resources

futura-rt-app-pub-dev

2 subnet associations

2 routes including local

futura-rt-app-pvt-dev

2 subnet associations

3 routes including local

rtb-028230a7c174d28b0

No subnet associations

1 route including local

Network Connections (2)

Connections to other networks

futura-igw-app-dev

Internet routes to 2 public subnets

2 private subnets route to the Internet

futura-nat-app-dev

Public NAT gateway

1 ENI with 1 EIP

VPC futura-vpc-app-dev

Subnets (4)

Subnets within this VPC

us-east-2a

A futura-pub-subnet-app-1-dev

11.0.0.64/27

No IPv6

A futura-pvt-subnet-app-1-dev

11.0.0.0/27

No IPv6

us-east-2b

B futura-pub-subnet-app-2-dev

11.0.0.96/27

No IPv6

B futura-pvt-subnet-app-2-dev

11.0.0.32/27

No IPv6

Route tables (3)

Route network traffic to resources

futura-rt-app-pub-dev

2 subnet associations

2 routes including local

futura-rt-app-pvt-dev

2 subnet associations

3 routes including local

rtb-028230a7c174d28b0

No subnet associations

1 route including local

Network Connections (2)

Connections to other networks

futura-igw-app-dev

Internet routes to 2 public subnets

2 private subnets route to the Internet

futura-nat-app-dev

Public NAT gateway

1 ENI with 1 EIP



VPC futura-jenkins-vpc-cicd-dev

Subnets (4)

Subnets within this VPC

us-east-2a

A futura-jenkins-pub-subnet-cicd-1-dev

11.1.0.64/27
No IPv6

A futura-jenkins-pvt-subnet-cicd-1-dev

11.1.0.0/27
No IPv6

us-east-2b

B futura-jenkins-pub-subnet-cicd-2-dev

11.1.0.96/27
No IPv6

B futura-jenkins-pvt-subnet-cicd-2-dev

11.1.0.32/27
No IPv6

Route tables (3)

Route network traffic to resources

futura-jenkins-rt-cicd-pvt-dev

2 subnet associations
1 route including local

rtb-039bf559edb0c55c8

No subnet associations
1 route including local

futura-jenkins-rt-cicd-pub-dev

2 subnet associations
2 routes including local

Network Connections (1)

Connections to other networks

futura-jenkins-igw-cicd-dev

Internet routes to 2 public subnets
0 private subnets route to the Internet

VPC futura-jenkins-vpc-cicd-dev

Subnets (4)

Subnets within this VPC

us-east-2a

A futura-jenkins-pub-subnet-cicd-1-dev

11.1.0.64/27

No IPv6

A futura-jenkins-pvt-subnet-cicd-1-dev

11.1.0.0/27

No IPv6

us-east-2b

B futura-jenkins-pub-subnet-cicd-2-dev 

11.1.0.96/27

No IPv6

B futura-jenkins-pvt-subnet-cicd-2-dev

11.1.0.32/27

No IPv6

Route tables (3)

Route network traffic to resources

futura-jenkins-rt-cicd-pvt-dev

2 subnet associations

1 route including local

rtb-039bf559edb0c55c8

No subnet associations

1 route including local

futura-jenkins-rt-cicd-pub-dev

2 subnet associations

2 routes including local

Network Connections (1)

Connections to other networks

futura-jenkins-igw-cicd-dev

Internet routes to 2 public subnets

0 private subnets route to the Internet

VPC futura-jenkins-vpc-cicd-dev

Subnets (4)

Subnets within this VPC

us-east-2a

A futura-jenkins-pub-subnet-cicd-1-dev

11.1.0.64/27
No IPv6

A futura-jenkins-pvt-subnet-cicd-1-dev

11.1.0.0/27
No IPv6

us-east-2b

B futura-jenkins-pub-subnet-cicd-2-dev

11.1.0.96/27
No IPv6

B futura-jenkins-pvt-subnet-cicd-2-dev

11.1.0.32/27
No IPv6

Route tables (3)

Route network traffic to resources

futura-jenkins-rt-cicd-pvt-dev

2 subnet associations
1 route including local

rtb-039bf559edb0c55c8

No subnet associations
1 route including local

futura-jenkins-rt-cicd-pub-dev

2 subnet associations
2 routes including local

Network Connections (1)

Connections to other networks

futura-jenkins-igw-cicd-dev

Internet routes to 2 public subnets
0 private subnets route to the Internet

VPC futura-jenkins-vpc-cicd-dev

Subnets (4)

Subnets within this VPC

us-east-2a

A futura-jenkins-pub-subnet-cicd-1-dev

11.1.0.64/27

No IPv6

A futura-jenkins-pvt-subnet-cicd-1-dev

11.1.0.0/27

No IPv6

us-east-2b

B futura-jenkins-pub-subnet-cicd-2-dev

11.1.0.96/27

No IPv6

B futura-jenkins-pvt-subnet-cicd-2-dev 

11.1.0.32/27

No IPv6

Route tables (3)

Route network traffic to resources

futura-jenkins-rt-cicd-pvt-dev

2 subnet associations

1 route including local

rtb-039bf559edb0c55c8

No subnet associations

1 route including local

futura-jenkins-rt-cicd-pub-dev

2 subnet associations

2 routes including local

Network Connections (1)

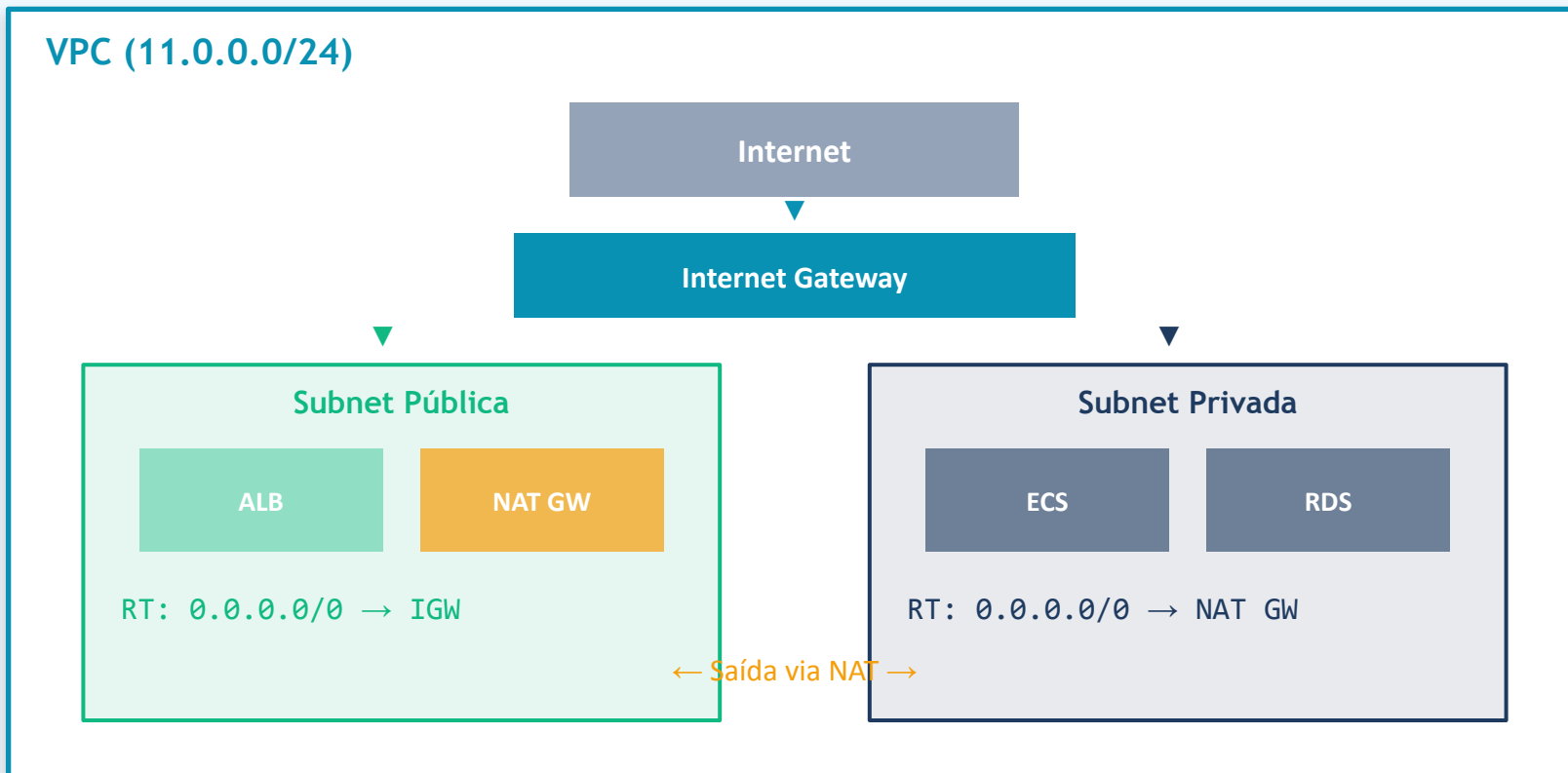
Connections to other networks

futura-jenkins-igw-cicd-dev

Internet routes to 2 public subnets

0 private subnets route to the Internet

Resumo – Como Tudo se Conecta





A VPC é a fundação de toda infraestrutura na AWS.

Entender como ela funciona é essencial para construir
ambientes seguros, organizados e escaláveis.

Obrigado!