

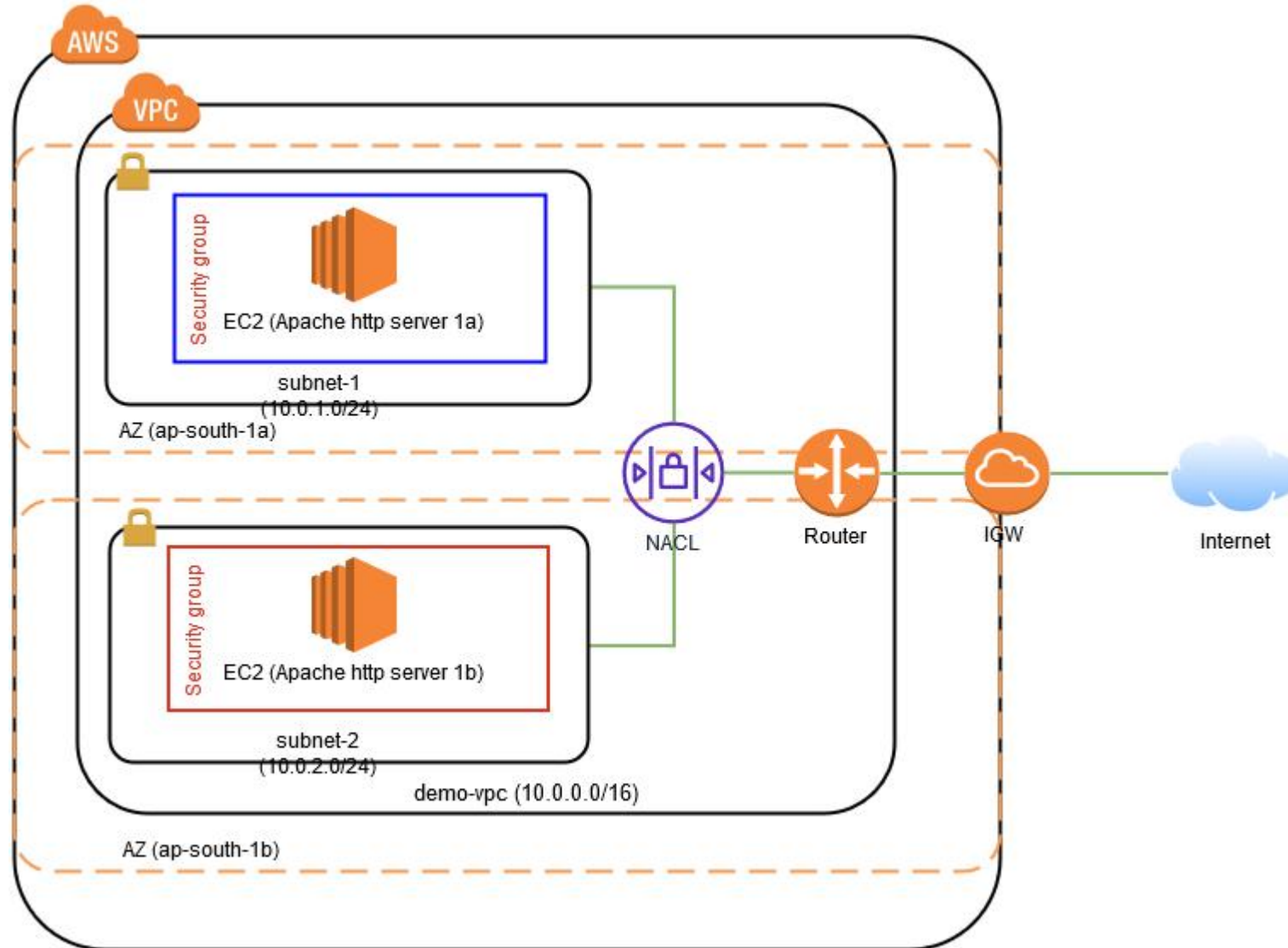


Geek University

Evolua seu lado geek!

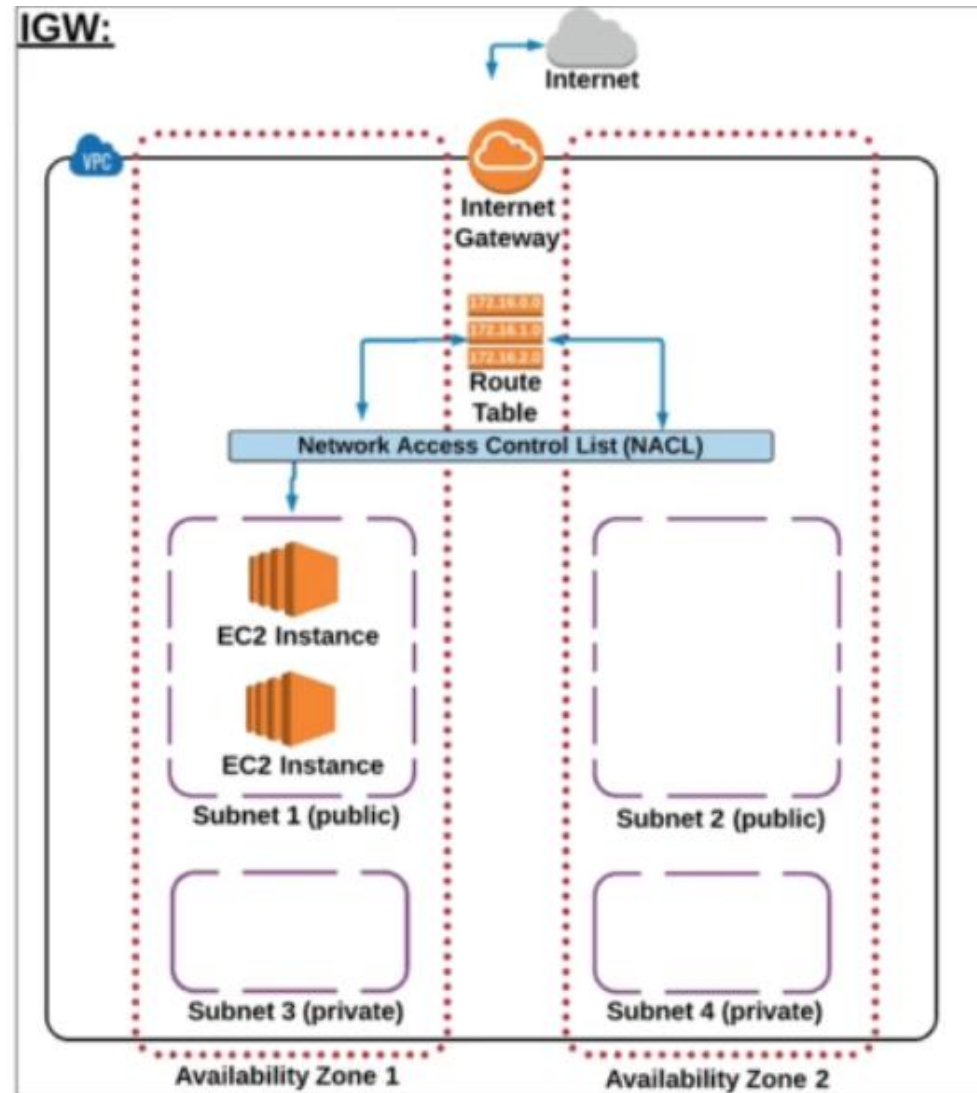
www.geekuniversity.com.br

Entendendo a Lista de Controle de Acesso à Internet



Entendendo a Lista de Controle de Acesso à Internet

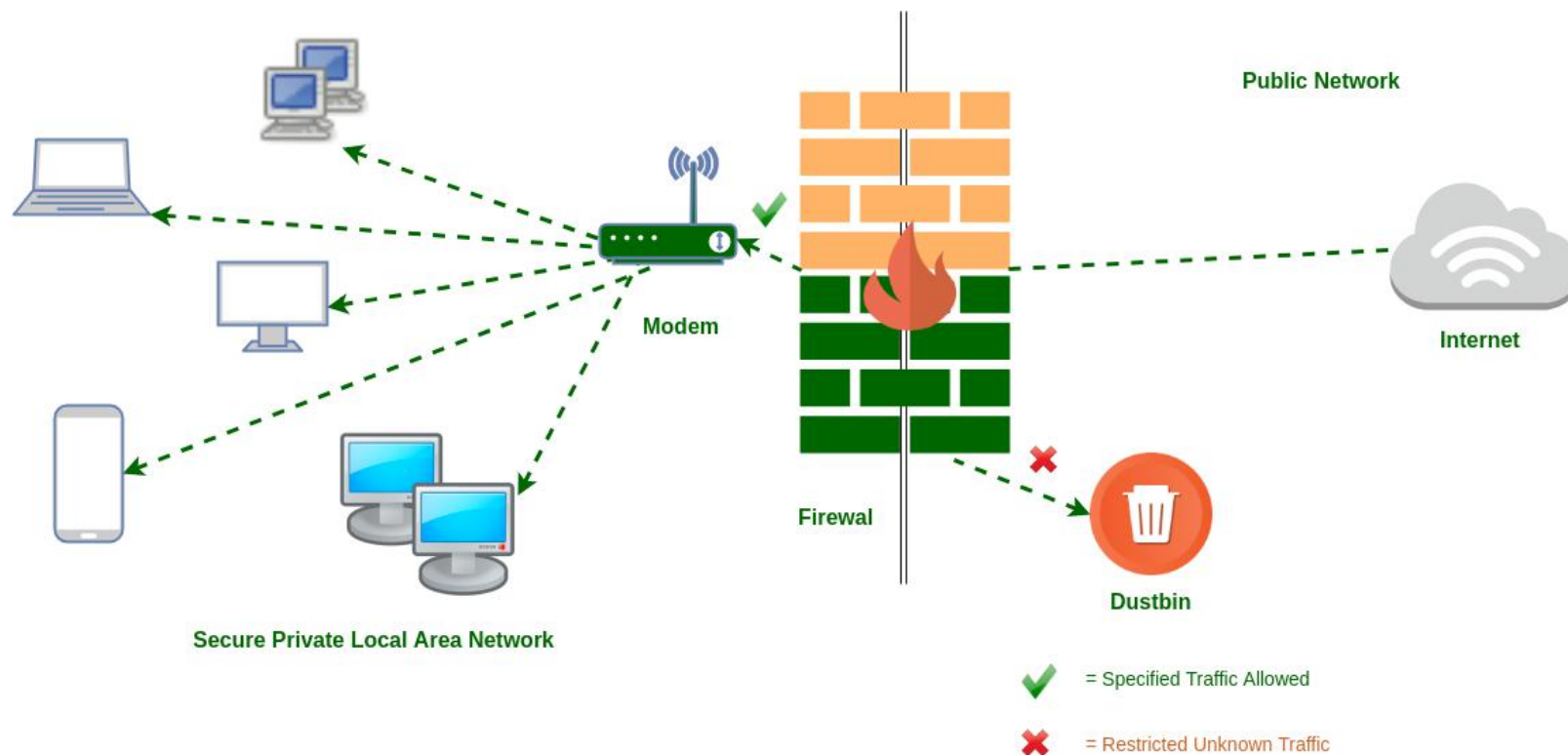
Recapitulando...



Entendendo a Lista de Controle de Acesso à Internet

O que é Network Access Control List (NACL)?

De forma simples, uma NACL é uma camada **opcional** de segurança para nossa VPC que *age como um firewall* controlando o tráfego de entrada e saída de uma ou mais sub-redes.



OBS: Nossa VPC padrão já possui uma NACL ativa e associada às sub-redes presentes.

Entendendo a Lista de Controle de Acesso à Internet

OBS: Nossa VPC padrão já possui uma NACL ativa e associada às sub-redes presentes.

Resources by Region [Refresh Resources](#)

You are using the following Amazon VPC resources

VPCs See all regions ▼	São Paulo 1	NAT Gateways See all regions ▼	São Paulo 0
Subnets See all regions ▼	São Paulo 3	VPC Peering Connections See all regions ▼	São Paulo 0
Route Tables See all regions ▼	São Paulo 1	Network ACLs See all regions ▼	São Paulo 1

Entendendo a Lista de Controle de Acesso à Internet

OBS: Nossa VPC padrão já possui uma NACL ativa e associada às sub-redes presentes.

The screenshot displays the AWS Management Console interface for Network ACLs. The left sidebar contains the navigation menu, with 'Network ACLs' selected under the 'SECURITY' section. The main content area shows a table of Network ACLs. The table has columns for Name, Network ACL ID, Associated with, Default, VPC, and Owner. One entry is visible: 'acl-43e8fa24' associated with '3 Subnets' and 'vpc-c81a03af'. Below the table, the 'Details' tab is active, showing the Network ACL ID and associated VPC.

Name	Network ACL ID	Associated with	Default	VPC	Owner
	acl-43e8fa24	3 Subnets	Yes	vpc-c81a03af	132773150473

Network ACL: acl-43e8fa24

Details | Inbound Rules | Outbound Rules | Subnet associations | Tags

Network ACL ID: acl-43e8fa24

Associated with: 3 Subnets

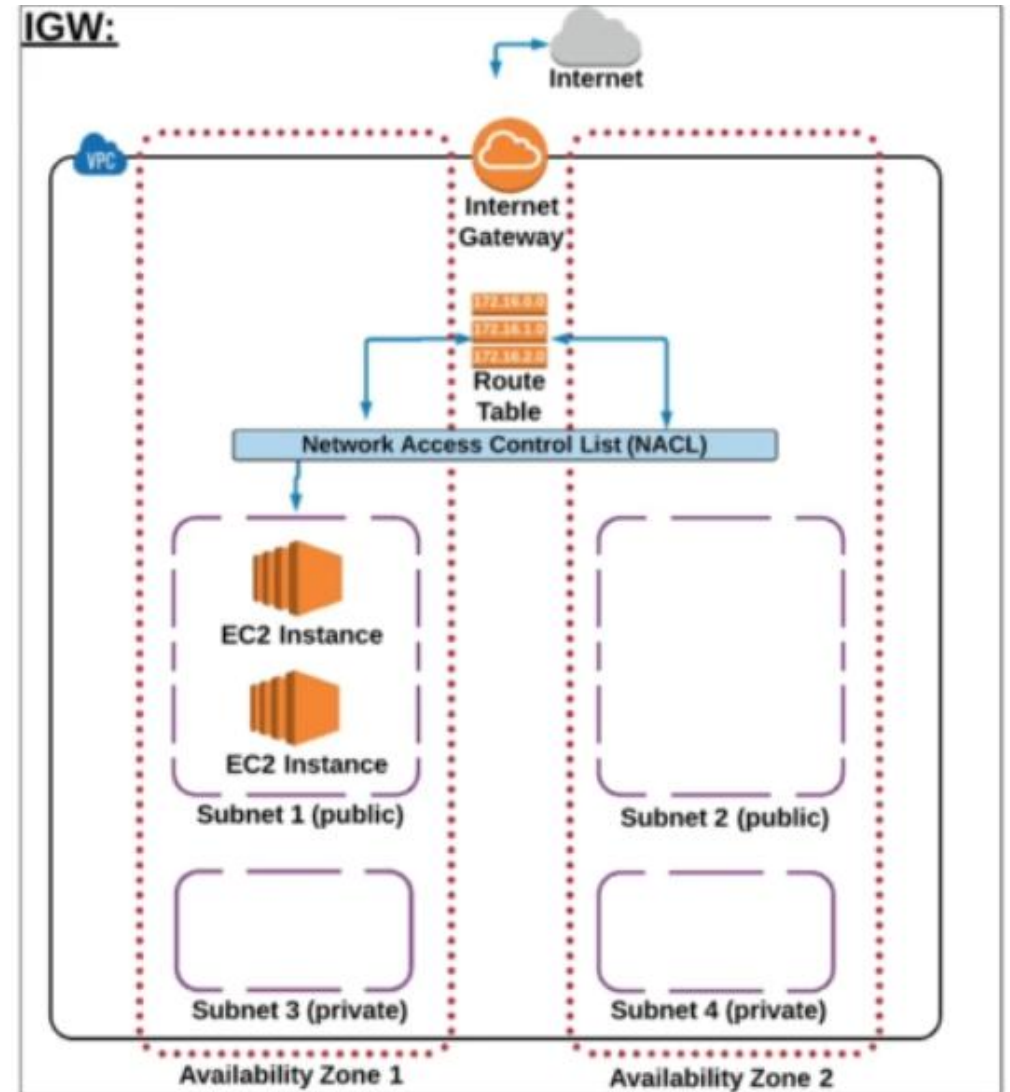
Default: Yes

VPC: vpc-c81a03af

vamos navegar no console da aws...

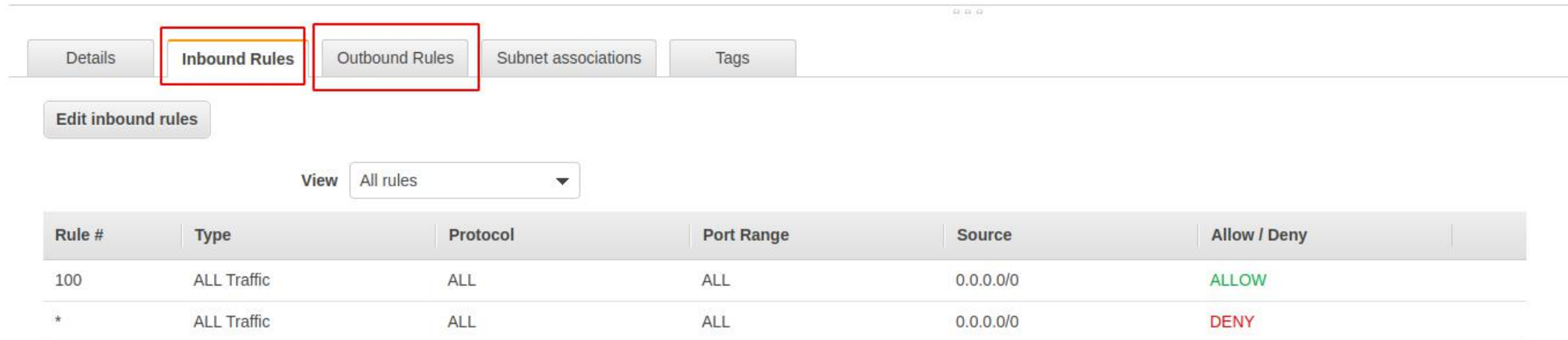
Entendendo a Lista de Controle de Acesso à Internet

Com a NACL definimos as regras para acesso de entrada e saída de dados.



Entendendo a Lista de Controle de Acesso à Internet

Com a NACL definimos as regras para acesso de entrada e saída de dados.



Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

Note que temos 2 regras de entrada definidas, sendo uma com o número 100 e outra com *

O * indica que é a regra 'padrão' e a regra padrão diz que qualquer tráfego de entrada que não esteja definida na regra 100 deverá ser negado.

Entendendo a Lista de Controle de Acesso à Internet

Com a NACL definimos as regras para acesso de entrada e saída de dados.

Details

Inbound Rules

Outbound Rules

Subnet associations

Tags

Edit inbound rules

View

All rules

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

OBS: As regras são executadas de acordo com a numeração, do menor para o maior número. E a primeira regra aplicada não será sobrescrita por outra.

Entendendo a Lista de Controle de Acesso à Internet

Atenção: Ao criar uma nova NACL, por padrão todo o tráfego de entrada e saída é negado por padrão.

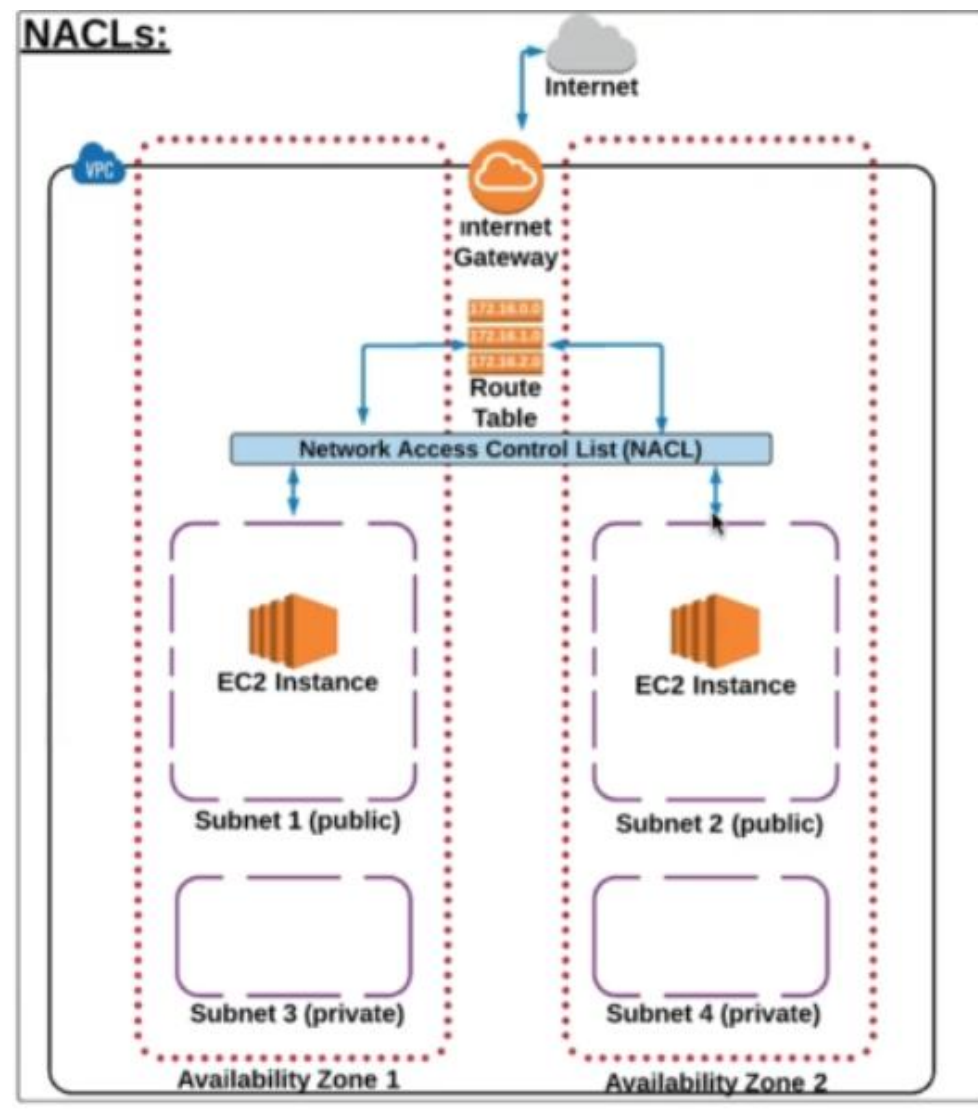
Por outro lado, a NACL criada por padrão durante a criação da conta na AWS é permitido o acesso tanto de entrada quanto de saída para que nossa VPC tenha conectividade total.

Entendendo a Lista de Controle de Acesso à Internet

Agora temos uma NACL atuando em 2 sub-redes da nossa VPC e uma outra NACL atuando na terceira sub-rede.

Veja a importância da definição destas regras de forma que a comunicação seja controlada de forma efetiva nas sub-redes.

Caso a comunicação entre as sub-redes não esteja ocorrendo de forma apropriada, a razão pode ser uma configuração NACL errada.



Entendendo a Lista de Controle de Acesso à Internet

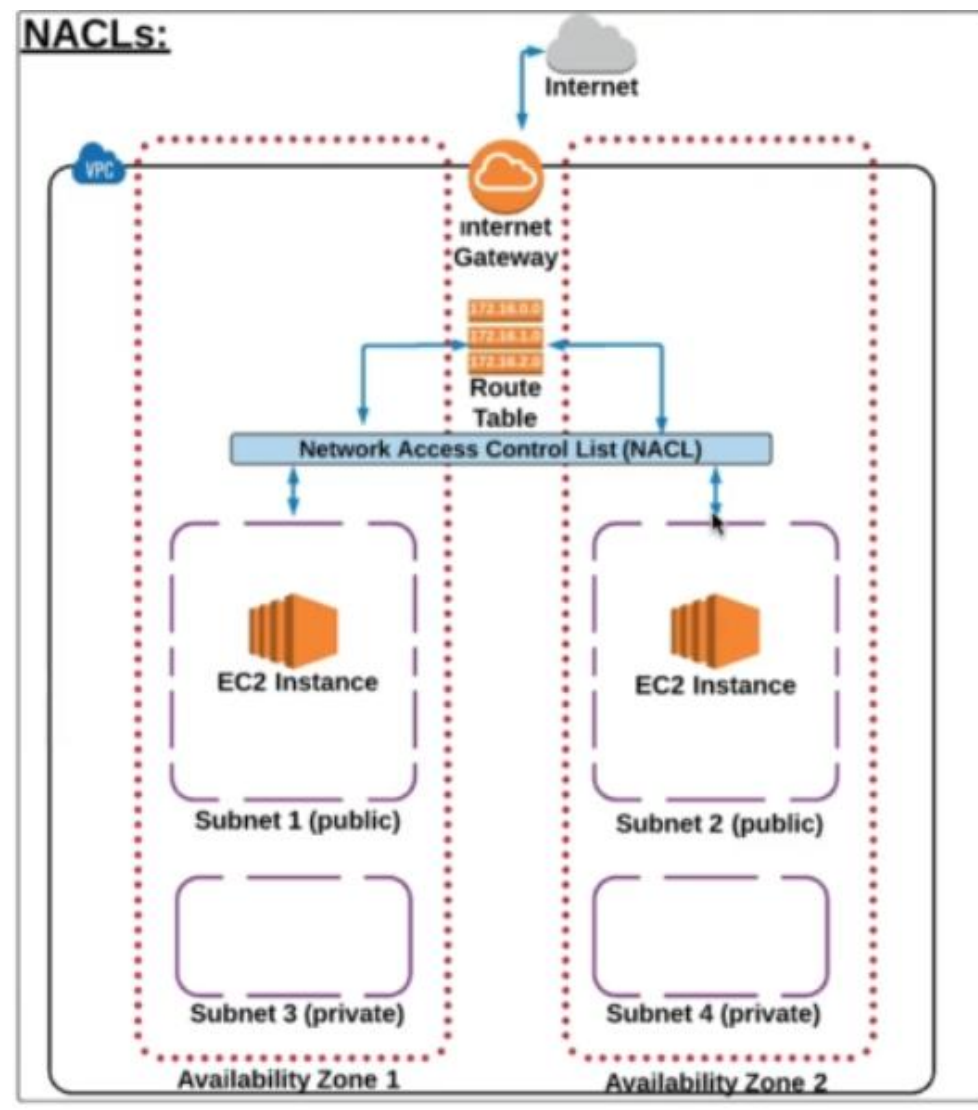
Em resumo, NACL funcionam como um firewall entre as nossas sub-redes e a tabela de rotas.

Uma NACL é criada no momento de criação da nossa conta e esta permite por padrão a comunicação de entrada e saída na nossa rede.

Qualquer outra NACL criada por nós terá entradas e saídas bloqueadas por padrão, sendo necessário que adicionemos regras diferentes desta caso queiramos permitir a comunicação.

Uma sub-rede pode ser associada a apenas uma NACL por vez.

Uma vez o tráfego permitido através de uma NACL, podemos ainda adicionar uma nova barreira, diretamente a um recurso AWS, chamada Security Groups, que iremos estudar ainda neste curso.





Geek University

Evolua seu lado geek!

www.geekuniversity.com.br