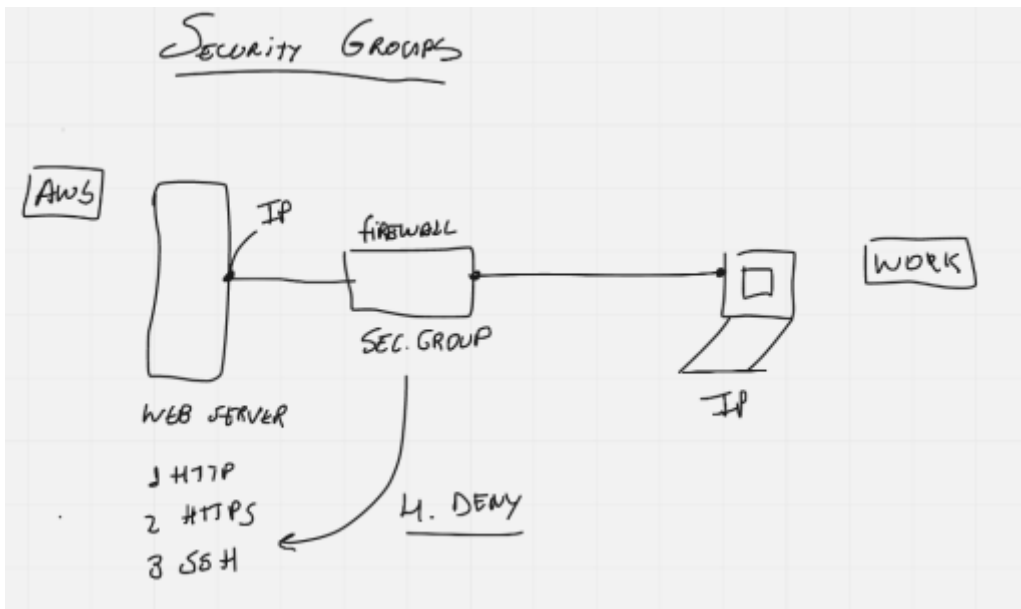


8 - ENTENDENDO E APLICANDO OS SECURITYS GROUPS

- Na aula anterior montamos um web service usando APACHE hospedando nossa pagina, e depois que terminamos de rodar o web service, o serviço não foi ativado porque não tínhamos permitido HTTP e HTTPS.
- Imagine que voce esta no seu trabalho com seu PC com endereçamento IP;
- Temos a estrutura da AWS na AZ que escolhemos.
- A conexão da sua maquina e o servidor AWS passa por o que o professor chama de FIREWALL (AWS _ Security Group), que conecta com o endereço IP do servidor.
- Dentro do Security Group permitimos (HTTP, HTTPS, SSH)
- Todos os outros serviços dentro desse FIREWALL estão com a negação (DENY - ALL).
 - Regra basica de firewall, se adicionamos uma regra a ultima linha sempre será um deny all.



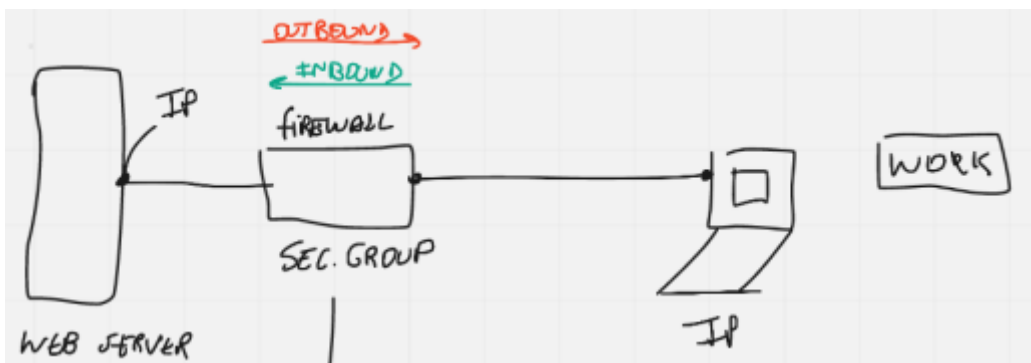
- Lembre-se que os Securitys Groups são por regioao, logo é como se tivesse um firewll para cada regioao(flexibilidade).
- Toda regioao possui uma security group default

| Name | Security group ID | Security group name | VPC ID | Description | Inbound rules count | Outbound rules count |
|-----------|----------------------|---------------------|--------------|----------------------------|----------------------|----------------------|
| WebServer | sg-08589e215917dbaf1 | linuxweb | vpc-301bb849 | launch-wizard-1 create... | 5 Permission entries | 1 Permission entry |
| - | sg-b34fe4e2 | default | vpc-301bb849 | default VPC security gr... | 1 Permission entry | 1 Permission entry |

| | | | |
|---------------------------------|---|--|------------------------|
| sg-08589e215917dbaf1 - linuxweb | | | |
| Details | | | |
| Security group name linuxweb | Security group ID sg-08589e215917dbaf1 | Description launch-wizard-1 created 2021-05-17T18:17:04.920-08:00 | VPC ID vpc-301bb849 |
| Owner 000436465845 | Inbound rules count 5 Permission entries | Outbound rules count 1 Permission entry | |

INBOUND RULES

- São as regras de entrada.



- Que tipo de trafego pode vir do mundo para dentro do servidor

| Inbound rules (5) | | | | |
|-------------------|----------|------------|-----------|------------------------|
| Type | Protocol | Port range | Source | Description - optional |
| HTTP | TCP | 80 | 0.0.0.0/0 | - |
| HTTP | TCP | 80 | ::/0 | - |
| SSH | TCP | 22 | 0.0.0.0/0 | - |
| HTTPS | TCP | 443 | 0.0.0.0/0 | - |
| HTTPS | TCP | 443 | ::/0 | - |

OUTBOUNDS RULES

- O que pode sair do servidor

sg-08589e215017ebaf1 - linuxweb

Details | Inbound rules | **Outbound rules** | Tags

Outbound rules (1)

| Type | Protocol | Port range |
|-------------|----------|------------|
| All traffic | All | All |

- Todo trafego pode sair do servidor, mas o que acontece se mudarmos, deixarmos o outbound bloqueado? O servidor web vai parar de funcionar?

- O que acontece se pegarmos nossa security group e alterarmos nossa outbound rule?

- A pergunta eh a pagina irá continuar a funcionar?

- A pagina continua sendo mostrada.

- Esse tipo de FIREWALL é o que chamamos de STATEFULL, significa que se temos uma regra de entrar ele irá criar uma regra de saida para dar fluxo no trafego.

- Se quisermos bloquear o trafego é outra coisa... vamos verificar.

- Vamos agora na parte de inbound remover o HTTP

- Entenda que a partir do momento que clicamos em save, imediatamente essa regra será aplicada, não da tempo nem de trocar de abas.

- Podemos tbm criar um security groupu diferente.

- windows RDP

- descrição > acesso RDP maquinas windows

- regras: acesso rdp, oracle-RDS

| Name | Security group ID | Security group name | VPC ID | Description | Inbound rules count | Outbound rules count |
|--------------|----------------------|---------------------|--------------|----------------------------|----------------------|----------------------|
| AngularPleio | sg-05582b7f9a48955a | WindowsRDP | vpc-3019b649 | RDP Access Windows ... | 2 Permission entries | 1 Permission entry |
| WebServer | sg-08589e215017ebaf1 | linuxweb | vpc-3019b649 | launch-wizard-1 create... | 3 Permission entries | 1 Permission entry |
| - | sg-b34f4e2 | default | vpc-3019b649 | default VPC security gr... | 1 Permission entry | 1 Permission entry |

- Voltando na instancia do servidor que esta rodando, como vemos qual regra esta associada a ele?

SECURITY >

Instance: i-0e728dd9941f5d2f2

Details | **Security** | Networking | Storage | Status checks | Monitoring | Tags

▼ Security details

IAM Role: --

Owner ID: 060436486945

Launch time: Mon May 17 2021 10:18:00 GMT-0300 (Horário Padrão de Brasília)

Security groups: sg-08589e215017ebaf1 (linuxweb)

▼ Inbound rules

Filter rules

| Port range | Protocol | Source | Security groups |
|------------|----------|-----------|-----------------|
| 80 | TCP | 0.0.0.0/0 | linuxweb |
| 22 | TCP | 0.0.0.0/0 | linuxweb |
| 443 | TCP | 0.0.0.0/0 | linuxweb |

- Se quisermos apontar dois securitys groups para o mesmo servidor, conseguimos tbm.

security>change_security_groups

Change security groups Info

Amazon EC2 evaluates all the rules of the selected security groups to control inbound and outbound traffic to and from your instance. You can use this window to add and remove security groups.

Instance details

Instance ID: i-0e728dd9941f5d2f2

Network interface ID: eni-04ce14ab6dcf6cfab

Associated security groups

Add one or more security groups to the network interface. You can also remove security groups.

Select security groups Add security group

Security groups associated with the network interface (eni-04ce14ab6dcf6cfab)

| Security group name | Security group ID | |
|---------------------|----------------------|--------|
| linuxweb | sg-08589e215017ebaf1 | Remove |

Cancel Save

Change security groups [Info](#)

Amazon EC2 evaluates all the rules of the selected security groups to control inbound and outbound traffic to and from your instance. You can use this window to add and remove security groups.

Instance details

| | |
|------------------------------------|---|
| Instance ID i-0e728dd9941f5d2f2 | Network interface ID eni-04ce14ab6dcf6cfab |
|------------------------------------|---|

Associated security groups
Add one or more security groups to the network interface. You can also remove security groups.

Security groups associated with the network interface (eni-04ce14ab6dcf6cfab)

| Security group name | Security group ID | |
|---------------------|----------------------|---------------------------------------|
| linuxweb | sg-08589e215017ebaf1 | <input type="button" value="Remove"/> |
| WindowsRDP | sg-05582b7f08a88655a | <input type="button" value="Remove"/> |

- Lembre-se que tudo que voce faz nos securitys gropus voce esta mexendo no firewall da regioao.
CUIDADOOOOOOOOOOOOOOOOOO