# Leitura 2.7: Amazon VPC Routing and Security

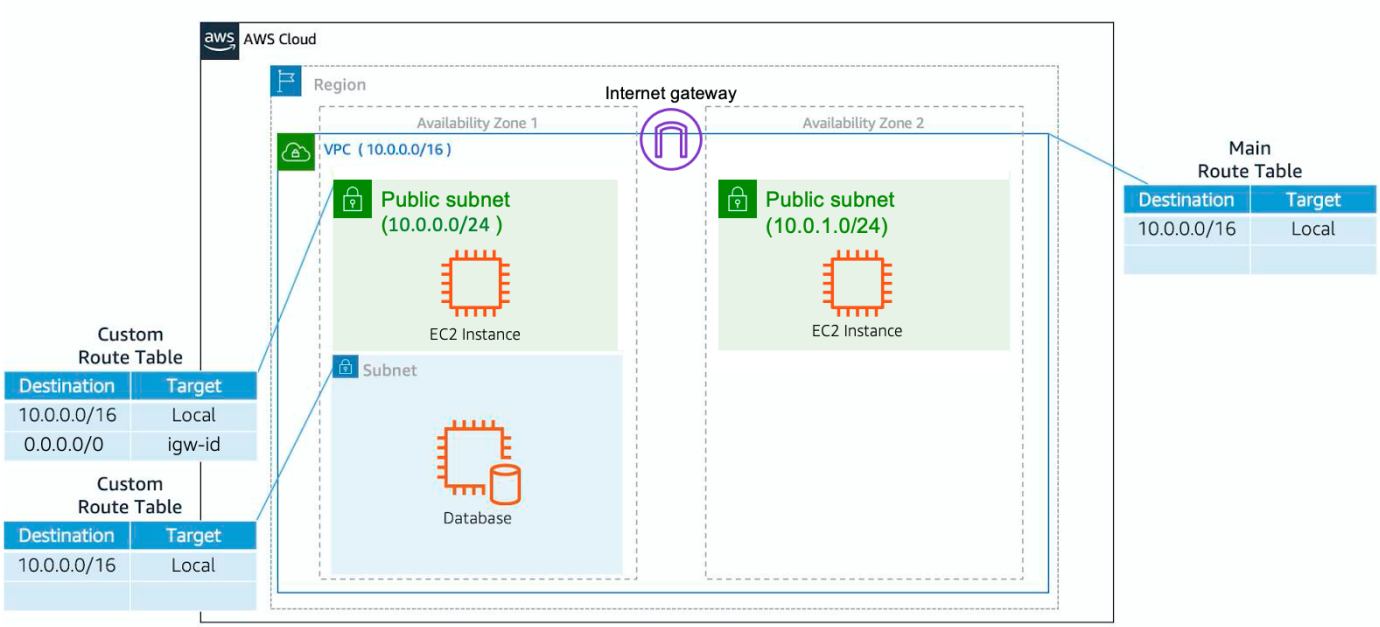
## A Tabela de Rota Principal

Quando você cria um VPC, o AWS cria uma tabela de rota chamada tabela de rota principal. Uma tabela de rotas contém um conjunto de regras, chamadas rotas, que são usadas para determinar para onde o tráfego da rede é direcionado. A AWS pressupõe que, ao criar um novo VPC com sub-redes, você deseja que o tráfego flua entre eles. Portanto, a configuração padrão da tabela de rota principal é permitir o tráfego entre todas as sub-redes na rede local. Abaixo está um exemplo de uma tabela de rota principal: Existem duas partes principais para esta tabela de rota.

- O destino, que é um intervalo de endereços IP para onde você deseja que o tráfego vá. No exemplo do envio de uma carta, você precisa de um destino para encaminhar a carta ao local apropriado. O mesmo é verdadeiro para o tráfego de roteamento. Nesse caso, o destino é o intervalo de IP de nossa rede VPC.
- O destino, que é a conexão por meio da qual enviar o tráfego. Nesse caso, o tráfego é roteado pela rede VPC local.

## Tabelas de rotas personalizadas

Embora a tabela de rota principal controle o roteamento de seu VPC, você pode querer ser mais granular sobre como rotear seu tráfego para sub-redes específicas. Por exemplo, seu aplicativo pode consistir em um front-end e um banco de dados. Você pode criar sub-redes separadas para esses recursos e fornecer rotas diferentes para cada um deles. Se você associar uma tabela de rota personalizada a uma sub-rede, a sub-rede a usará em vez da tabela de rota principal. Por padrão, cada tabela de rota personalizada que você criar já terá a rota local dentro dela, permitindo que a comunicação flua entre todos os recursos e sub-redes dentro do VPC.




## Proteja suas sub-redes com ACLs de rede

Pense em uma ACL de rede como um firewall no nível de sub-rede. Uma ACL de rede permite que você controle que tipo de tráfego pode entrar ou sair da sua sub-rede. Você pode configurar isso configurando regras que definem o que você deseja filtrar. Aqui está um exemplo.

**De entrada**

| Regra # | Modelo | Protocolo | Faixa Portuária | Fonte | Permitem negar |
|---|---|---|---|---|---|
| 100 | Todo o tráfego IPv4 | Tudo | Tudo | 0.0.0.0/0 | PERMITIR |
| * | Todo o tráfego IPv4 | Tudo | Tudo | 0.0.0.0/0 | NEGAR |

**Saída**

| Regra # | Modelo | Protocolo | Faixa Portuária | Fonte | Permitem negar |
|---|---|---|---|---|---|
| 100 | Todo o tráfego IPv4 | Tudo | Tudo | 0.0.0.0/0 | PERMITIR |
| * | Todo o tráfego IPv4 | Tudo | Tudo | 0.0.0.0/0 | NEGAR |

A ACL de rede padrão, mostrada na tabela acima, permite todo o tráfego de entrada e saída de sua sub-rede. Para permitir que os dados fluam livremente para sua sub-rede, este é um bom ponto de partida. No entanto, você pode querer restringir os dados no nível da sub-rede. Por exemplo, se você tiver um aplicativo da web, poderá restringir sua rede para permitir o tráfego HTTPS e protocolo de área de trabalho remota (RDP) para seus servidores da web.

**De entrada**

| Regra # | IP fonte | Protocolo | Porta | Permitem negar | Comentários |
|---|---|---|---|---|---|
| 100 | Todo o tráfego IPv4 | TCP | 443 | PERMITIR | Permite tráfego HTTPS de entrada de qualquer lugar |

| Regra # | IP fonte | Protocolo | Porta | Permitem negar | Comentários |
|---|---|---|---|---|---|
| 130 | 192.0.2.0/24 | TCP | 3389 | PERMITIR | Permite o tráfego RDP de entrada para os servidores da web a partir do intervalo de endereços IP públicos da sua rede doméstica (através do gateway de internet) |
| * | Todo o tráfego IPv4 | Tudo | Tudo | NEGAR | Nega todo o tráfego de entrada ainda não tratado por uma regra anterior (não modificável) |

**Saída**

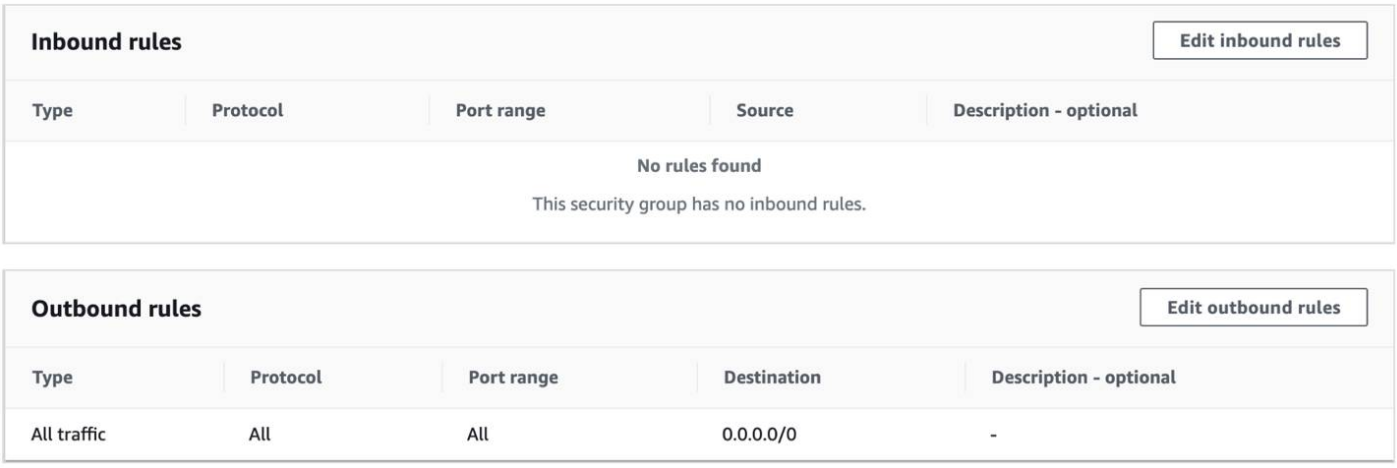
| Regra # | IP de destino | Protocolo | Porta | Permitem negar | Comentários |
|---|---|---|---|---|---|
| 120 | 0.0.0.0/0 | TCP | 1025-65535 | PERMITIR | Permite respostas de saída para clientes na internet (atendendo pessoas que visitam os servidores da web na sub-rede) |
| * | 0.0.0.0/0 | Tudo | Tudo | NEGAR | Nega todo o tráfego de saída ainda não tratado por uma regra anterior (não modificável) |

Observe que no exemplo de ACL de rede acima, você permite 443 de entrada e intervalo de saída 1025-65535. Isso ocorre porque o HTTP usa a porta 443 para iniciar uma conexão e responderá a uma porta efêmera. As ACLs de rede são consideradas sem estado, portanto, você precisa incluir as portas de entrada e saída usadas

para o protocolo. Se você não incluir o intervalo de saída, seu servidor responderá, mas o tráfego nunca sairá da sub-rede. Como as ACLs de rede são configuradas por padrão para permitir o tráfego de entrada e saída, você não precisa alterar suas configurações iniciais, a menos que precise de camadas de segurança adicionais.

### Proteja suas instâncias EC2 com grupos de segurança

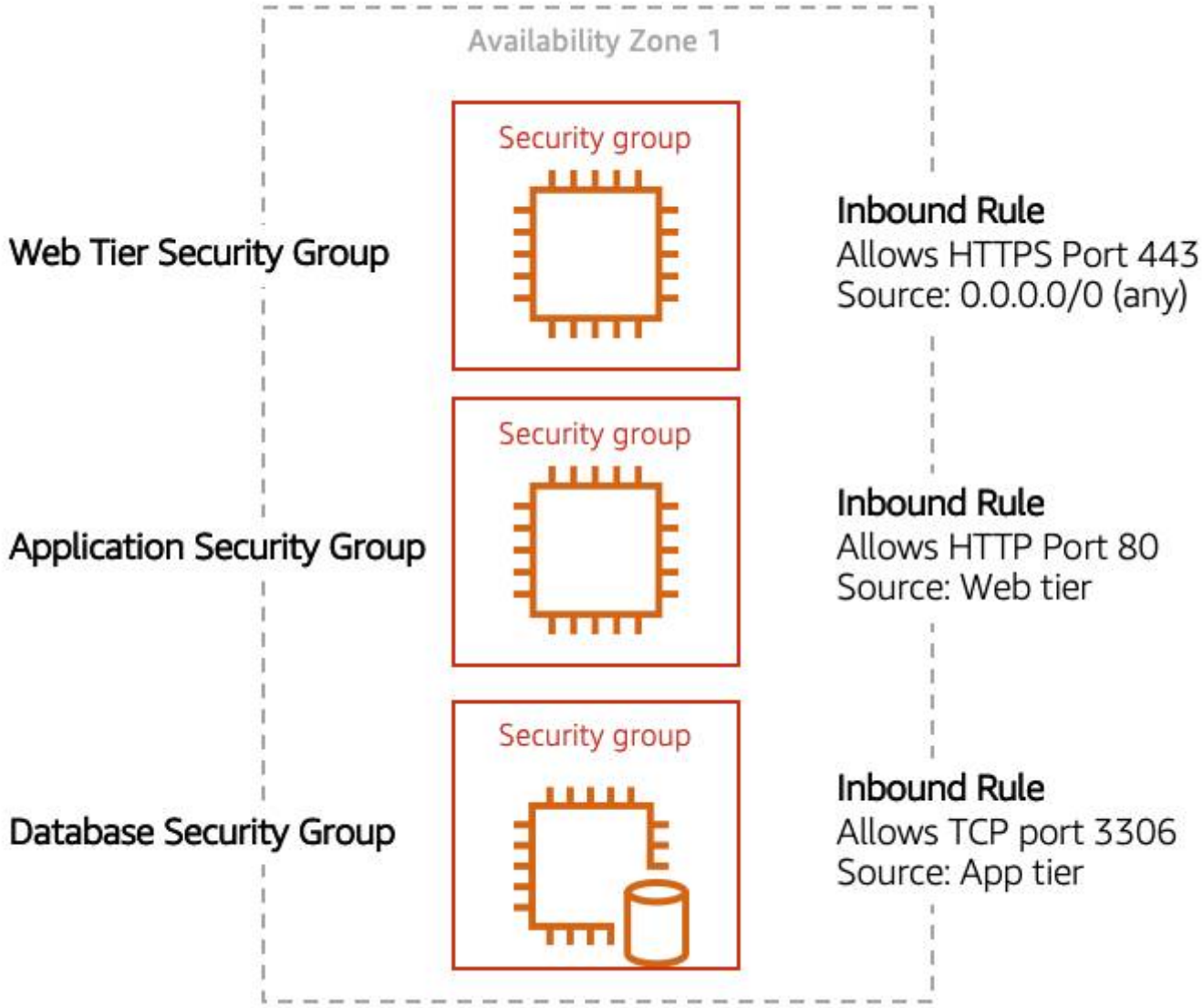
A próxima camada de segurança é para suas instâncias EC2. Aqui, você pode criar um firewall chamado grupo de segurança. A configuração padrão de um grupo de segurança bloqueia todo o tráfego de entrada e permite todo o tráfego de saída.




Você deve estar se perguntando: “Isso não impediria que todas as instâncias do EC2 recebessem a resposta de qualquer solicitação do cliente?” Bem, os grupos de segurança têm estado, o que significa que eles se lembrarão se uma conexão foi originalmente iniciada pela instância EC2 ou de fora e permitirão temporariamente que o tráfego responda sem ter que modificar as regras de entrada. Se você deseja que sua instância EC2 aceite tráfego da Internet, será necessário abrir portas de entrada. Se você tiver um servidor da web, talvez precise aceitar solicitações HTTP e HTTPS para permitir esse tipo de tráfego por meio de seu grupo de segurança. Você pode criar uma regra de entrada que permitirá a porta 80 (HTTP) e a porta 443 (HTTPS) conforme mostrado abaixo.

| Modelo | Protocolo | Faixa Portuária | Fonte |
|---|---|---|---|
| HTTP (80) | TCP (6) | 80 | 0.0.0.0/0 |
| HTTP (80) | TCP (6) | 80 | ::/0 |
| HTTPS (443) | TCP (6) | 443 | 0.0.0.0/0 |
| HTTPS (443) | TCP (6) | 443 | ::/0 |

Você aprendeu em uma unidade anterior que as sub-redes podem ser usadas para separar o tráfego entre os computadores em sua rede. Os grupos de segurança podem ser usados para fazer a mesma coisa. Um padrão de design comum é organizar seus recursos em grupos diferentes e criar grupos de segurança para cada um para controlar a comunicação de rede entre eles.




Este exemplo permite definir três camadas e isolar cada camada com as regras do grupo de segurança que você definir. Nesse caso, você só permite o tráfego da Internet para a camada da web por HTTPS, camada da Web para camada de aplicativo sobre HTTP e camada de aplicativo para camada de banco de dados sobre MySQL. Isso é diferente dos ambientes locais tradicionais, nos quais você isola grupos de recursos por meio da configuração de VLAN. Na AWS, os grupos de segurança permitem que você obtenha o mesmo isolamento sem vinculá-lo à sua rede.