AWS Transit Gateway

Amazon VPC

Amazon VPC: AWS Transit Gateway

Table of Contents

O que é um gateway de trânsito?

O gateway de trânsito é uma central de trânsito de rede que pode ser usada para interconectar as Virtual Private Clouds (VPCs) e as redes on-premises. À medida que sua infraestrutura de nuvem se expande globalmente, o emparelhamento entre regiões conecta gateways de trânsito juntos usando a infraestrutura global da AWS. Todo o tráfego de rede entre os datacenters da AWS é criptografado automaticamente na camada física.

Para obter mais informações, consulte AWS Transit Gateway.

Conceitos de gateway de trânsito

Veja a seguir os principais conceitos de gateways de trânsito:

- Anexos: você pode anexar o seguinte:
  - Uma ou mais VPCs
  - Um dispositivo de rede Connect SD-WAN/de terceiros
  - Um gateway do AWS Direct Connect
  - Uma conexão de emparelhamento com outro gateway de trânsito
  - Uma conexão VPN a um gateway de trânsito
- Maximum Transmission Unit (MTU – Unidade de transmissão máxima) do gateway de trânsito: a unidade de transmissão máxima (MTU) de uma conexão de rede é o tamanho, em bytes, do maior pacote permissível que pode ser transmitido pela conexão. Quanto maior a MTU de uma conexão, mais dados podem ser passados em um único pacote. Um gateway de trânsito oferece suporte a uma MTU de 8500 bytes para tráfego entre VPCs, ao AWS Direct Connect, ao Transit Gateway Connect e aos anexos de emparelhamento. O tráfego que passa pelas conexões VPN pode ter uma MTU de 1.500 bytes.
- Tabela de rotas do gateway de trânsito: um gateway de trânsito tem uma tabela de rotas padrão e pode ter tabelas de rotas adicionais opcionalmente. Uma tabela de roteamento inclui rotas dinâmicas e estáticas que determinam o próximo salto com base no endereço IP de destino do pacote. O destino dessas rotas pode ser qualquer anexo de gateway de trânsito. Por padrão, os anexos do gateway de trânsito são associados à tabela de rotas do gateway de trânsito padrão.
- Associações: cada anexo é associado a exatamente uma tabela de rotas. Cada tabela de roteamento pode ser associada a nenhum ou a vários anexos.

- Propagação de rotas: uma VPC, conexão VPN ou o gateway do Direct Connect pode propagar rotas de forma dinâmica a uma tabela de rotas do gateway de trânsito. Com um anexo do Connect, as rotas são propagadas para uma tabela de rotas de gateway de trânsito por padrão. Com uma VPC, é necessário criar rotas estáticas para enviar o tráfego ao gateway de trânsito. Com uma conexão VPN, as rotas são propagadas do gateway de trânsito para os roteadores on-premise usando o Border Gateway Protocol (BGP). Com um gateway do Direct Connect, os prefixos permitidos são originados para seus roteadores on-premises usando o BGP. Com um anexo de emparelhamento, você deve criar uma rota estática na tabela de rotas do gateway de trânsito para apontar para o anexo de emparelhamento.

Conceitos básicos dos gateways de trânsito

Use os seguintes recursos para ajudar a criar e usar um gateway de trânsito.

- Como funcionam os gateways de trânsito
- Conceitos básicos
- Melhores práticas de design

Trabalhar com gateways de trânsito

É possível criar, acessar e gerenciar os gateways de trânsito usando qualquer uma das seguintes interfaces:

- AWS Management Console — fornece uma interface da Web que pode ser usada para acessar os gateways de trânsito.
- Interface da linha de comando da AWS (AWS CLI): fornece comandos para um amplo conjunto de serviços da AWS, inclusive a Amazon VPC, e é compatível com Windows, macOS e Linux. Para obter mais informações, consulte AWS Command Line Interface.
- AWS SDKs: fornecem operações de API específicas da linguagem e cuidam de muitos dos detalhes da conexão, como cálculo de assinaturas, tratamento de novas tentativas de solicitação e tratamento de erros. Para obter mais informações, consulte AWS SDKs.
- API de consulta: fornece ações de API de baixo nível que são chamadas usando solicitações HTTPS. Usar a API de consulta é a maneira mais direta para acessar a Amazon VPC, mas exige que a aplicação lide com detalhes de baixo nível, como geração de hash para assinar a solicitação

e tratamento de erros. Para obter mais informações, consulte a Referência de API do Amazon EC2.

Preços

Você será cobrado por hora por cada anexo em um gateway de trânsito e pela quantidade de tráfego processada no gateway de trânsito. Para obter mais informações, consulte Preços do AWS Transit Gateway.

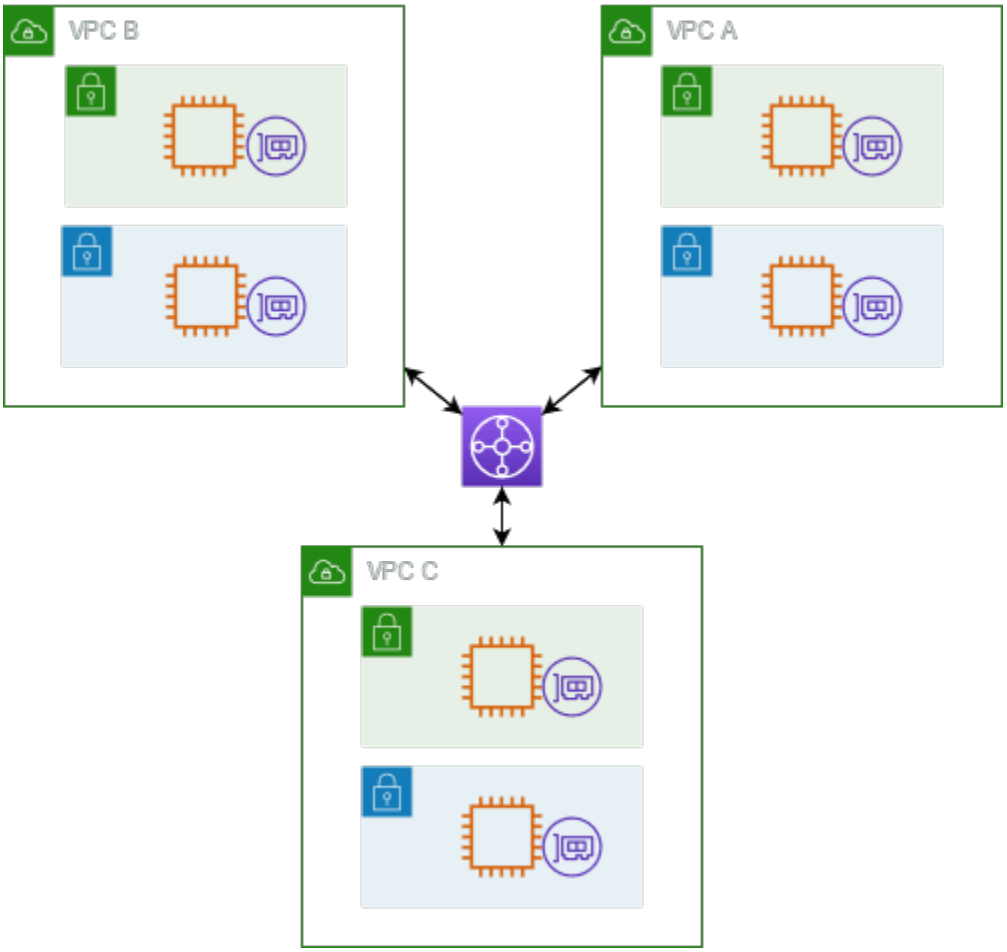
Como funcionam os gateways de trânsito

Um gateway de trânsito age como um roteador virtual regional para o tráfego entre virtual private clouds (VPC – nuvens privadas virtuais) e redes on-premises. Um gateway de trânsito é dimensionado de maneira elástica com base no volume do tráfego de rede. O roteamento por um gateway de trânsito opera na camada 3, onde os pacotes são enviados para um anexo de próximo salto específico, com base nos endereços IP de destino.

Conteúdo

Diagrama de arquitetura

O diagrama a seguir mostra um gateway de trânsito com três anexos de VPC. A tabela de rotas de cada uma dessas VPCs inclui a rota local e rotas que enviam tráfego destinado das outras duas VPCs ao gateway de trânsito.



Veja a seguir um exemplo de tabela de rotas do gateway de trânsito padrão para os anexos exibidos no diagrama anterior. Os blocos CIDR de cada VPC se propagam para a tabela de rotas. Portanto, cada anexo é capaz de rotear pacotes aos outros dois anexos.

Destination (Destino)	Destino	Tipo de rota
CIDR da VPC A	*Anexo para a VPC A*	com propagação
CIDR da VPC B	*Anexo para a VPC B*	com propagação
CIDR da VPC C	*Anexo para a VPC C*	com propagação

Anexos de recursos

O anexo de gateway de trânsito é origem e destino dos pacotes. É possível anexar os recursos a seguir ao gateway de trânsito:

- Uma ou mais VPCs. AWS O Transit Gateway implanta uma interface de rede elástica nas sub-redes VPC, que é então usada pelo gateway de trânsito para rotear o tráfego de e para as sub-redes escolhidas. Cada zona de disponibilidade precisa ter pelo menos uma sub-rede para que o tráfego chegue aos recursos em cada sub-rede da zona. Durante a criação de anexos, os recursos de uma zona de disponibilidade específica só poderão chegar a um transit gateway se uma sub-rede estiver ativada na mesma zona. Se a tabela de rotas de uma sub-rede incluir uma rota para o transit gateway, o tráfego só será enviado ao transit gateway se esse gateway tiver um anexo na sub-rede da mesma zona de disponibilidade.
- Uma ou mais conexões VPN
- Um ou mais AWS Direct Connect gateways
- Um ou mais anexos do Transit Gateway Connect
- Uma ou mais conexões de emparelhamento de gateway de trânsito
- Um anexo do gateway de trânsito pode ser uma origem e um destino dos pacotes.

Roteamento de múltiplos caminhos de mesmo custo

AWS O Transit Gateway oferece suporte ao roteamento Equal Cost Multipath (ECMP) para a maioria dos anexos. Para um anexo de VPN, você pode habilitar ou desabilitar o suporte a ECMP usando o console ao criar ou modificar um gateway de trânsito. Para todos os outros tipos de anexos, as seguintes restrições de ECMP são aplicáveis:

- VPC: o VPC não oferece suporte a ECMP, pois não pode haver sobreposição entre os blocos CIDR. Por exemplo, você não pode anexar uma VPC com um CIDR 10.1.0.0/16 com uma segunda VPC usando o mesmo CIDR a um gateway de trânsito e então configurar o roteamento para balancear a carga do tráfego entre elas.
- VPN: quando a opção VPN ECMP support (Suporte a ECMP de VPN) estiver desabilitada, o gateway de trânsito usará métricas internas para determinar o caminho preferencial no caso de prefixos iguais em vários caminhos. Para obter mais informações sobre como habilitar ou desabilitar o ECMP para um anexo da VPN, consulte the section called “Gateways de trânsito”.
- AWS Transit Gateway Connect - Os anexos AWS Transit Gateway Connect suportam automaticamente o ECMP.
- AWS Direct Connect Gateway - Os anexos do AWS Direct Connect gateway oferecem suporte automático ao ECMP em vários anexos do Direct Connect Gateway quando o prefixo da rede, o comprimento do prefixo e o AS_PATH são exatamente os mesmos.

- Emparelhamento de gateway de trânsito: O emparelhamento de gateway de trânsito não é compatível com ECMP, pois não oferece suporte ao roteamento dinâmico nem você pode configurar a mesma rota estática em dois destinos diferentes.

> **Note**
>
> - Não há compatibilidade com BGP Multipath AS-Path Relax, então você não pode usar ECMP em diferentes números de sistema autônomo (ASN).
> - Não há compatibilidade com ECMP entre diferentes tipos de anexos. Por exemplo, você não pode habilitar o ECMP entre uma VPN e um anexo da VPC. Em vez disso, as rotas do gateway de trânsito são avaliadas, e o tráfego é roteado de acordo com a rota avaliada. Para ter mais informações, consulte the section called “Ordem de avaliação de rotas”.
> - Um só gateway do Direct Connect oferece suporte a ECMP em várias interfaces virtuais de trânsito. Portanto, recomendamos que você configure e use somente um gateway do Direct Connect e que não configure e use vários gateways para aproveitar o recurso ECMP. Para obter mais informações sobre gateways Direct Connect e interfaces virtuais públicas, consulte Como faço para configurar uma conexão de conexão direta ativa/ativa ou ativa/passiva a partir de uma interface virtual pública? AWS .

Zonas de disponibilidade

Ao anexar uma VPC a um gateway de trânsito, é preciso habilitar uma ou mais zonas de disponibilidade para serem usadas pelo gateway de trânsito para rotear o tráfego a recursos nas sub-redes da VPC. Para habilitar cada zona de disponibilidade, especifique exatamente uma sub-rede. O gateway de trânsito coloca uma interface de rede na sub-rede usando um endereço IP da sub-rede. Depois que você habilitar uma zona de disponibilidade, o tráfego poderá ser roteado para todas as sub-redes na VPC, e não somente para a sub-rede ou a zona de disponibilidade especificada. Contudo, os recursos que residem nas zonas de disponibilidade em que não há nenhum anexo do gateway de trânsito não podem alcançar o gateway de trânsito.

Se o tráfego for originado de uma zona de disponibilidade na qual o anexo de destino não está presente, o AWS Transit Gateway roteará internamente esse tráfego para uma zona de disponibilidade aleatória onde o anexo está presente. Não há cobrança adicional de gateway de trânsito para esse tipo de tráfego entre zonas de disponibilidade.

Recomendamos que você habilite várias zonas de disponibilidade para garantir a disponibilidade.

Usar o suporte ao modo de dispositivo

Se você planeja configurar um dispositivo de rede com estado em sua VPC, poderá habilitar o suporte ao modo de dispositivo para o anexo da VPC em que o dispositivo está localizado. Isso garante que o gateway de trânsito use a mesma zona de disponibilidade para esse anexo de VPC durante o tempo de vida de um fluxo de tráfego entre a origem e o destino. Também permite que o gateway de trânsito envie tráfego para qualquer zona de disponibilidade na VPC, desde que haja uma associação de sub-rede nessa zona. Para ter mais informações, consulte Exemplo: dispositivo em uma VPC de serviços compartilhados.

Roteamento

Seu gateway de trânsito roteia pacotes IPv4 e IPv6 entre anexos usando tabelas de rotas de gateway de trânsito. É possível configurar essas tabelas de rotas para propagar as rotas a partir delas para as VPCs anexadas e conexões VPN anexadas e para os gateways do Direct Connect. Você também pode adicionar rotas estáticas às tabelas de rotas de gateway de trânsito. Quando um pacote surge de um anexo, ele é roteado para outro anexo usando a rota que corresponde ao endereço IP de destino.

Para anexos de emparelhamento de gateway de trânsito, somente rotas estáticas são compatíveis.

Conteúdo

Tabelas de rotas

Seu gateway de trânsito vem automaticamente com uma tabela de rotas padrão. Por padrão, essa tabela de roteamento é a tabela de roteamento de associação padrão e a tabela de roteamento de propagação padrão. Como alternativa, se você desabilitar a propagação de rotas e a associação da tabela de rotas, a AWS não criará uma tabela de rotas padrão para o gateway de trânsito.

É possível criar tabelas de rotas adicionais para o gateway de trânsito. Assim você pode isolar os subconjuntos dos anexos. Cada anexo pode ser associado a uma tabela de rotas. Um anexo pode propagar as rotas para uma ou mais tabelas de rotas.

É possível criar uma rota blackhole na tabela de rotas do gateway de trânsito que solta o tráfego correspondente à rota.

Ao anexar uma VPC a um gateway de trânsito, você deverá adicionar uma rota à sua tabela de rotas de sub-rede para que o tráfego seja roteado pelo gateway de trânsito. Para obter mais informações, consulte Roteamento para um gateway de trânsito no Guia do usuário da Amazon VPC.

Associação da tabela de rotas

É possível associar um anexo de gateway de trânsito a uma única tabela de rotas. Cada tabela de rotas pode ser associada a vários anexos (ou nenhum) e pode encaminhar pacotes a outros anexos.

Propagação de rotas

Cada anexo vem com rotas que podem ser instaladas em uma ou mais tabelas de rotas do gateway de trânsito. Quando um anexo é propagado com uma tabela de rotas do gateway de trânsito, essas rotas são instaladas na tabela. Não é possível filtrar as rotas anunciadas.

Para um anexo da VPC, os blocos CIDR da VPC são propagados para a tabela de rotas do gateway de trânsito.

Ao usar o roteamento dinâmico com um anexo da VPN ou um anexo de gateway do Direct Connect, é possível propagar as rotas aprendidas do roteador on-premises por meio do BGP a qualquer uma das tabelas de rotas do gateway de trânsito.

Quando o roteamento dinâmico é usado com um anexo da VPN, as rotas na tabela de rotas associadas ao anexo da VPN são anunciadas ao gateway do cliente por meio do BGP.

Para um anexo do Connect, as rotas da tabela de rotas associada ao anexo do Connect são informadas aos dispositivos virtuais de terceiros, como dispositivos SD-WAN, em execução em uma VPC pelo BGP.

Para um anexo ao gateway Direct Connect, as interações de prefixos permitidos controlam de quais rotas são anunciadas para a rede do cliente. AWS

Quando uma rota estática e uma propagada têm o mesmo destino, a estática tem maior prioridade. Portanto, a rota propagada não é incluída na tabela de rotas. Se você remover a rota estática, a rota propagada sobreposta será incluída na tabela de rotas.

Rotas para anexos de emparelhamento

É possível emparelhar dois gateways de trânsito e rotear o tráfego entre eles. Para fazer isso, crie um anexo de emparelhamento em seu gateway de trânsito e especifique o gateway de trânsito de mesmo nível com o qual criar a conexão de emparelhamento. Depois, crie uma rota estática em sua tabela de rotas de gateway de trânsito para rotear o tráfego para o anexo de emparelhamento do gateway de trânsito. O tráfego que é roteado para o gateway de trânsito de mesmo nível pode então ser roteado para os anexos de VPC e VPN para o gateway de trânsito do mesmo nível.

Para obter mais informações, consulte Exemplo: Gateways de trânsito em pares.

Ordem de avaliação de rotas

As rotas do gateway de trânsito são avaliadas na seguinte ordem:

- A rota mais específica para o endereço de destino.
- Para as rotas com o mesmo endereço IP de destino, mas alvos diferentes, a prioridade da rota será a seguinte:
  - Rotas estáticas (por exemplo, rotas estáticas do Site-to-Site VPN)
  - Rotas referenciadas da lista de prefixos
  - Rotas propagadas da VPC
  - Rotas propagadas do gateway do Direct Connect
  - Rotas propagadas do Transit Gateway Connect
  - Rotas propagadas privadas de VPN site-to-site
  - Rotas propagadas por VPN pública site a site
  - Rotas propagadas pelo emparelhamento do Transit Gateway (Cloud WAN)

O Transit Gateway mostra apenas uma rota preferida. Uma rota de backup só aparecerá na tabela de rotas do Transit Gateway se essa rota não for mais anunciada. Por exemplo, se você estiver anunciando as mesmas rotas pelo gateway Direct Connect e pela VPN Site-to-Site. AWS O Transit Gateway mostrará somente as rotas recebidas da rota do gateway Direct Connect, que é a rota

preferencial. A VPN de local a local, que é a rota de backup, só é exibida quando o gateway do Direct Connect não é mais informado.

Diferenças na tabela de rotas do VPC e do Transit Gateway

A avaliação da tabela de rotas difere se você está usando uma tabela de rotas VPC ou uma tabela de rotas de gateway de trânsito.

O exemplo a seguir mostra uma tabela de rotas de VPC. A rota local da VPC tem a maior prioridade, seguida pelas rotas mais específicas. Quando uma rota estática e uma rota propagada têm o mesmo destino, a rota estática tem maior prioridade.

Destino	Destino	Priority
10.0.0.0/16	local	1
192.168.0.0/16	pcx-12345	2
172.31.0.0/16	vgw-12345 (estático) ou tgw-12345 (estático)	2
172.31.0.0/16	vgw-12345 (propagado)	3
0.0.0.0/0	igw-12345	4

O exemplo a seguir mostra uma tabela de rotas do gateway de trânsito. Se você preferir o anexo do gateway do AWS Direct Connect ao anexo de VPN, use uma conexão da VPN do BGP e propague as rotas na tabela de rotas do gateway de trânsito.

Destino	Anexo (Destino)	Tipo de recurso	Tipo de rota	Priority
10.0.0.0/16	tgw-attach-123 | vpc-1234	VPC	Estático ou propagado	1
192.168.0.0/16	tgw-attach-789 | vpn-5678	VPN	Estático	2

Destino	Anexo (Destino)	Tipo de recurso	Tipo de rota	Priority
172.31.0.0/16	tgw-attach-456 | dxgw_id	Gateway AWS Direct Connect	Com propagação	3
172.31.0.0/16	tgw-attach-789 | -123 tgw-connect-peer	Conectar	Com propagação	4
172.31.0.0/16	tgw-attach-789 | vpn-5678	VPN	Com propagação	5

Conceitos básicos dos gateways de trânsito

As tarefas a seguir ajudam você a se familiarizar com os gateways de trânsito. Você criará um gateway de trânsito e conectará duas das VPCs usando o gateway de trânsito.

Tarefas

- Pré-requisitos
- Etapa 1: Criar o gateway de trânsito
- Etapa 2: Anexar as VPCs ao gateway de trânsito
- Etapa 3: Adicionar rotas entre os gateways de trânsito e as VPCs
- Etapa 4: Testar o gateway de trânsito
- Etapa 5: Excluir o gateway de trânsito

Pré-requisitos

- Para um exemplo simples do uso de um gateway de trânsito, crie duas VPCs na mesma região. As VPC não podem sobrepor os CIDRs Inicie uma instância do Amazon EC2 em cada VPC. Para obter mais informações, consulte Conceitos básicos da Amazon VPC no Manual do usuário da Amazon VPC.
- Não é possível ter rotas idênticas apontando para duas VPCs diferentes. Um gateway de trânsito não propaga os CIDRs de uma VPC recém-anexada se existir uma rota idêntica nas tabelas de rotas do gateway de trânsito.
- Verifique se você tem as permissões necessárias para trabalhar com os gateways de trânsito. Para obter mais informações, consulte Identity and Access Management para gateways de trânsito.
- Não é possível fazer ping entre hosts se você não tiver adicionado uma regra ICMP a cada um dos grupos de segurança do host. Para obter mais informações, consulte Trabalhar com grupos de segurança no Guia do usuário da Amazon VPC.

Etapa 1: Criar o gateway de trânsito

Quando você cria um gateway de trânsito, nós criamos uma tabela de rotas padrão para ele e a usamos como tabela padrão de associação e propagação.

Como criar um gateway de trânsito

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No seletor de região, escolha a região que você usou quando criou as VPCs.
3. No painel de navegação, escolha Transit Gateways (Gateways de trânsito).
4. Escolha Create transit gateway (Criar gateway de trânsito).
5. (Opcional) Em Name tag (Tag de nome), digite um nome para o gateway de trânsito. Essa ação cria uma tag com "Nome" sendo a chave e nome que você especificou como o valor.
6. (Opcional) Em Description (Descrição), digite uma descrição para o gateway de trânsito.
7. Em Amazon side Autonomous System Number (ASN) (Número de sistema autônomo no lado da Amazon), insira o ASN privado para o gateway de trânsito. Ele deve ser o ASN para o lado da AWS de uma sessão de Border Gateway Protocol (BGP).

   O intervalo é de 64512 a 65534 para ASNs de 16 bits.

   O intervalo é de 4200000000 to 4294967294 para ASNs de 32 bits.

   Se você tiver uma implantação em várias regiões, recomendamos usar um ASN exclusivo para cada um dos gateways de trânsito.
8. (Opcional) É possível modificar as configurações padrão se você precisar desabilitar o suporte do DNS, ou se não quiser a tabela de roteamento padrão para associação ou propagação.
9. Escolha Create transit gateway (Criar gateway de trânsito). Após a criação do gateway, o estado inicial do gateway de trânsito é `pending`.

Etapa 2: Anexar as VPCs ao gateway de trânsito

Espere até que o gateway de trânsito criado na seção anterior esteja disponível antes de prosseguir com a criação do anexo. Crie um anexo para cada VPC.

Confirme que você criou duas VPCs e executou uma instância do EC2 em cada uma, como descrito em Pré-requisitos.

Criar um anexo do gateway de trânsito para uma VPC

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Attachments (Anexos do gateway de trânsito).

3. Escolha Create Transit Gateway Attachment (Criar anexo do Transit Gateway).
4. (Opcional) Em Name tag (Etiqueta de nome), insira um nome para o anexo.
5. Em Transit Gateway ID (ID do gateway de trânsito), escolha o gateway de trânsito que será usado no anexo.
6. Em Attachment type (Tipo de anexo), escolha VPC.
7. Escolha se quer habilitar o DNS support (Suporte do DNS). Nesse exercício, não ative IPv6 support (Suporte de IPv6).
8. Em VPC ID (ID da VPC), escolha a VPC a ser anexada ao gateway de trânsito.
9. Em Subnet IDs (IDs de sub-rede), selecione uma sub-rede para cada zona de disponibilidade a ser usada pelo gateway de trânsito para rotear o tráfego. É necessário selecionar pelo menos uma sub-rede. Você pode selecionar somente uma sub-rede por zona de disponibilidade.
10. Escolha Create Transit Gateway Attachment (Criar anexo do Transit Gateway).

Cada anexo é sempre associado a exatamente uma tabela de roteamento. As tabelas de rotas podem ser associadas a nenhum ou a quantos anexos for preciso. Para determinar as rotas a serem configuradas, decida sobre o caso de uso do gateway de trânsito e configure as rotas. Para obter mais informações, consulte Exemplo de casos de uso do.

Etapa 3: Adicionar rotas entre os gateways de trânsito e as VPCs

Uma tabela de roteamento inclui rotas dinâmicas e estáticas que determinam o próximo salto das VPCs associadas com base no endereço IP de destino do pacote. Configure uma rota que tenha um destino para rotas não locais e com o destino do ID do anexo do gateway de trânsito. Para obter mais informações, consulte Roteamento para um gateway de trânsito no Guia do usuário da Amazon VPC.

Para adicionar uma rota a uma tabela de roteamento da VPC

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Route Tables (Tabelas de rotas).
3. Escolha uma tabela de roteamento associada à sua VPC.
4. Escolha a guia Routes (Rotas) e Edit routes (Editar rotas).
5. Escolha Add route (Adicionar rota).

6. Na coluna Destination (Destino), informe o intervalo de endereços IP de destino. Para Target (Destino), escolha Transit Gateway (Gateway de trânsito) e, em seguida, escolha o ID do gateway de trânsito.
7. Escolha Save changes (Salvar alterações).

Etapa 4: Testar o gateway de trânsito

É possível confirmar se o gateway de trânsito foi criado com sucesso conectando uma instância do Amazon EC2 a cada VPC e enviando dados entre elas, como em um comando ping. Para obter mais informações, consulte Conectar-se à instância do Linux ou Conectar-se à instância do Windows.

Etapa 5: Excluir o gateway de trânsito

Quando não precisar mais de um gateway de trânsito, você pode excluí-lo.

Não é possível excluir um gateway de trânsito que tenha anexos de recursos. Se você tentar excluir um gateway de trânsito com anexos, primeiro será solicitado a excluir esses anexos antes de poder excluir o gateway de trânsito. Assim que o gateway de trânsito for excluído, a cobrança será interrompida.

Como excluir o gateway de trânsito

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateways (Gateways de trânsito).
3. Selecione o gateway de trânsito e escolha Actions (Ações) e Delete transit gateway (Excluir gateway de trânsito).
4. Insira **`delete`** e escolha Delete (Excluir).

   O State (Estado) do gateway de trânsito na página Transit gateways (Gateways de trânsito) é Deleting (Excluindo). Depois de excluído, o gateway de trânsito é removido da página.

Melhores práticas de design do gateway de trânsito

Veja a seguir as melhores práticas para o design do gateway de trânsito:

- Use uma sub-rede separada para cada anexo da VPC do gateway. Para cada sub-rede, use um CIDR pequeno, por exemplo `/28`, para que você tenha mais endereços para recursos do EC2. Ao usar uma sub-rede separada, é possível configurar o seguinte:
  - Mantenha abertas as ACLs de rede de entrada e de saída associadas às sub-redes do gateway de trânsito.
  - Dependendo do fluxo de tráfego, é possível aplicar ACLs de rede às suas sub-redes de workload.
- Crie uma network ACL e associe-a a todas as sub-redes que estão associadas ao gateway de trânsito. Mantenha a network ACL aberta nas direções de entrada e saída.
- Associe a mesma tabela de rotas da VPC a todas as sub-redes associadas ao gateway de trânsito, a menos que o design da rede exija várias tabelas de rotas da VPC (por exemplo, uma VPC de caixa intermediária que roteia o tráfego por meio de vários gateways NAT).
- Use conexões do Site-to-Site VPN do Protocolo de Gateway da Borda (BGP). Se o dispositivo do gateway do cliente ou firewall da conexão for compatível com multipath, ative o recurso.
- Ative a propagação de rotas para anexos de AWS Direct Connect gateway e anexos VPN BGP Site-to-Site.
- Ao migrar do emparelhamento de VPC para usar um gateway de trânsito. A incompatibilidade de tamanho da MTU entre o emparelhamento da VPC e o transit gateway pode fazer com que alguns pacotes do tráfego assimétrico sejam descartados. Atualize ambas as VPCs ao mesmo tempo para evitar o descarte de pacotes jumbo devido a divergências de tamanho.
- Não é necessário ter gateways de trânsito adicionais para alta disponibilidade, porque os gateways de trânsito estão altamente disponíveis por design.
- Limite o número de tabelas de rotas do gateway de trânsito, a menos que o design exija várias tabelas de rotas do gateway de trânsito.
- Para garantir a redundância, use um único gateway de trânsito em cada região para recuperação de desastres.
- Para implantações em vários transit gateways, recomendamos usar um Número de Sistema Autônomo (ASN) único para cada um dos seus transit gateways. Também é possível usar emparelhamento entre regiões. Para obter mais informações, consulte Construindo uma rede global usando o AWS Transit Gateway peering entre regiões.

Exemplos de casos de uso para gateways de trânsito

Veja a seguir os casos de uso comuns para gateways de trânsito. Seus gateways de trânsito não são limitados a esses casos de uso.

Exemplos

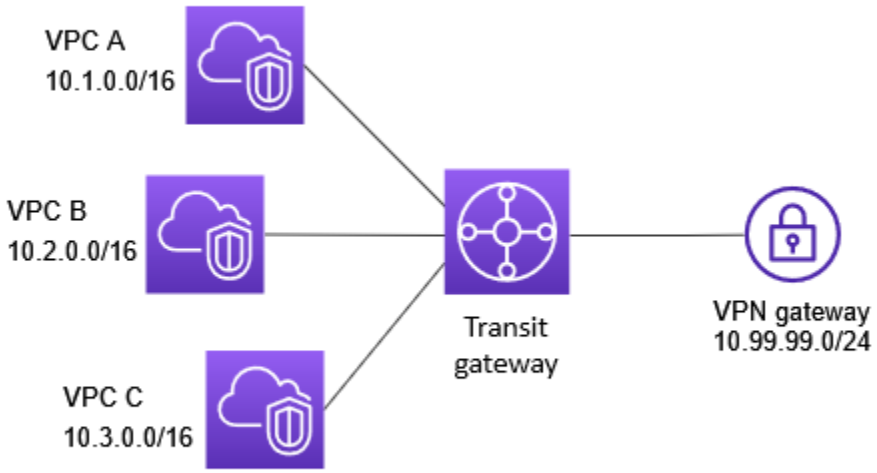
Exemplo: Roteador centralizado

É possível configurar o gateway de trânsito como um roteador centralizado que conecta todas as conexões de VPCs, do AWS Direct Connect e do Site-to-Site VPN. Nesse caso, todos os anexos estão associados à tabela de rotas padrão do gateway de trânsito e a propagam. Sendo assim, todos os anexos podem rotear pacotes uns para os outros, e o gateway de trânsito funciona como um simples roteador com IPs da camada 3.

Conteúdos

Visão geral

O diagrama a seguir mostra os principais componentes da configuração deste cenário. Neste cenário, há três anexos da VPC e um anexo do Site-to-Site VPN para o gateway de trânsito. Os pacotes das sub-redes na VPC A, VPC B e VPC C que têm como destino uma sub-rede em outra VPC ou a conexão VPN são roteados primeiro por meio do gateway de trânsito.



Recursos

Crie os seguintes recursos para este cenário:

- Três VPCs. Para obter mais informações sobre como criar uma VPC, consulte Criar uma VPC no Guia do usuário do Amazon VPC.
- Um gateway de trânsito Para obter mais informações, consulte the section called “Criar um gateway de trânsito”.
- Três anexos da VPC no gateway de trânsito. Para obter mais informações, consulte the section called “Criar um anexo do gateway de trânsito para uma VPC”.
- Um anexo do Site-to-Site VPN no gateway de trânsito. Os blocos CIDR de cada VPC se propagam para a tabela de rotas do gateway de trânsito. Quando a conexão VPN estiver ativada, a sessão de BGP será estabelecida, o CIDR do Site-to-Site VPN se propagará para a tabela de rotas do gateway de trânsito e os CIDRs da VPC serão adicionados à tabela de BGP do gateway do cliente. Para obter mais informações, consulte the section called “Criar um anexo de gateway de trânsito a uma VPN”.

  Revise os requisitos para o dispositivo de gateway do cliente no Guia do usuário do AWS Site-to-Site VPN.

Roteamento

Cada VPC tem uma tabela de rotas e há uma tabela de rotas para o gateway de trânsito.

Tabelas de rotas da VPC

Cada VPC tem uma tabela de rotas com 2 entradas. A primeira entrada é a padrão para um roteamento IPv4 local na VPC; essa entrada permite que as instâncias na VPC comuniquem-se entre si. A segunda entrada encaminha todos os outros tráfegos da sub-rede IPv4 ao gateway de trânsito. A tabela a seguir mostra as rotas da VPC A.

Destino	Destino
10.1.0.0/16	local
0.0.0.0/0	tgw-id

Tabela de rotas do Transit Gateway

A seguir, um exemplo de tabela de roteamento padrão para os anexos exibidos no diagrama anterior, com a propagação de rotas ativada.

Destino	Destino	Tipo de rota
10.1.0.0/16	*Anexo para a VPC A*	com propagação
10.2.0.0/16	*Anexo para a VPC B*	com propagação
10.3.0.0/16	*Anexo para a VPC C*	com propagação
10.99.99.0/24	*Anexo para a conexão VPN*	com propagação

Tabela do BGP do gateway do cliente

A tabela de BGP do gateway do cliente contém os seguintes CIDRs da VPC.

- 10.1.0.0/16
- 10.2.0.0/16
- 10.3.0.0/16

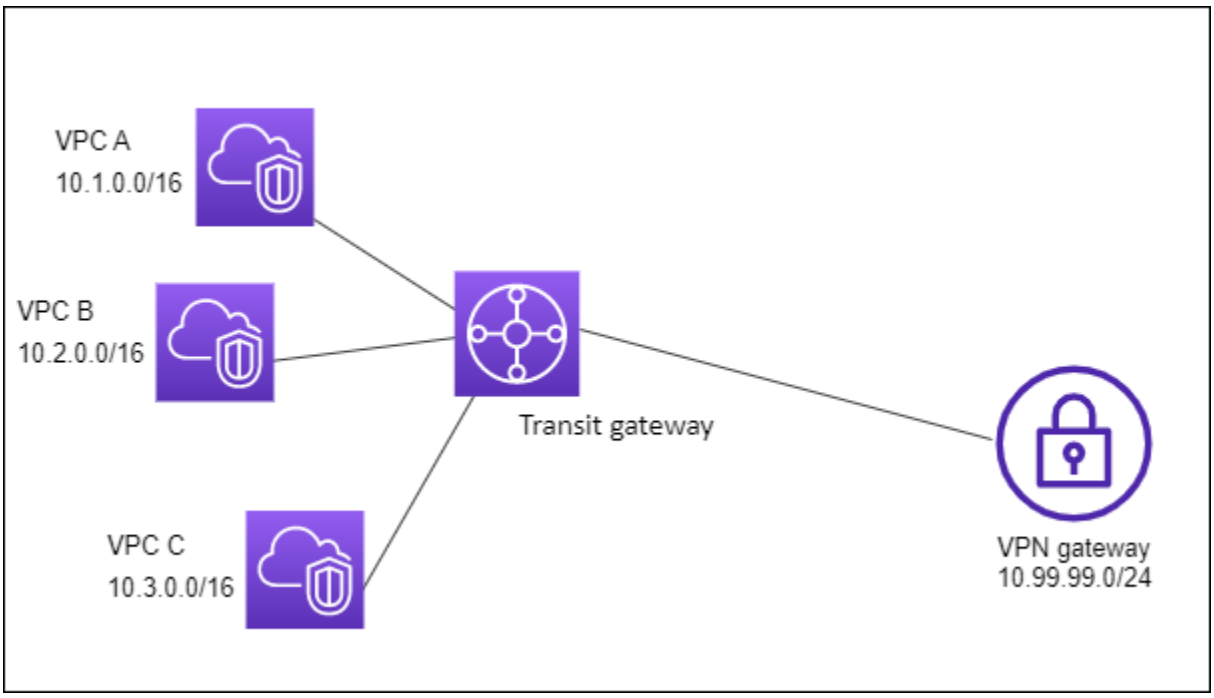
Exemplo: VPCs isoladas

É possível configurar o gateway de trânsito como vários roteadores isolados. É semelhante ao uso de vários gateways de trânsito, mas permite mais flexibilidade nos casos em que as rotas e os anexos puderem mudar. Nesse cenário, cada roteador isolado tem uma única tabela de roteamento. Todos os anexos associados a uma rota isolada propagam e associam com a tabela de roteamento. Os anexos associados a um roteador isolado podem rotear pacotes entre eles, mas não podem rotear ou receber pacotes dos anexos de outro roteador isolado.

Conteúdos

Visão geral

O diagrama a seguir mostra os principais componentes da configuração deste cenário. Pacotes da VPC A, VPC B e VPC C são roteados para o gateway de trânsito. Os pacotes das sub-redes na VPC A, na VPC B e na VPC C que têm a Internet como primeiro destino são roteados pelo gateway de trânsito e, em seguida, para a conexão do Site-to-Site VPN (se o destino estiver nessa rede). Pacotes de uma VPC que tenham como destino uma sub-rede de outra VPC, como de 10.1.0.0 para 10.2.0.0, são roteados pelo gateway de trânsito, onde são bloqueados porque não há uma rota para eles na tabela de rotas do gateway de trânsito.



Recursos

Crie os seguintes recursos para este cenário:

- Três VPCs. Para obter mais informações sobre como criar uma VPC, consulte Criar uma VPC no Guia do usuário do Amazon VPC.
- Um gateway de trânsito Para obter mais informações, consulte the section called “Criar um gateway de trânsito”.
- Três anexos no gateway de trânsito para as três VPCs. Para obter mais informações, consulte the section called “Criar um anexo do gateway de trânsito para uma VPC”.
- Um anexo do Site-to-Site VPN no gateway de trânsito. Para obter mais informações, consulte the section called “Criar um anexo de gateway de trânsito a uma VPN”. Revise os requisitos para o dispositivo de gateway do cliente no Guia do usuário do AWS Site-to-Site VPN.

Quando a conexão VPN estiver ativada, a sessão de BGP será estabelecida, o CIDR da VPN se propagará para a tabela de rotas do gateway de trânsito e os CIDRs da VPC serão adicionados à tabela de BGP do gateway do cliente.

Roteamento

Cada VPC tem uma tabela de rotas, e o gateway de trânsito tem duas tabelas de rotas: uma para as VPCs e uma para a conexão VPN.

Tabelas de rotas da VPC A, VPC B e VPC C

Cada VPC tem uma tabela de rotas com 2 entradas. A primeira entrada é a padrão do roteamento IPv4 local na VPC. Essa entrada permite que as instâncias nesta VPC se comuniquem entre si. A segunda entrada encaminha todos os outros tráfegos da sub-rede IPv4 ao gateway de trânsito. A tabela a seguir mostra as rotas da VPC A.

Destino	Destino
10.1.0.0/16	local
0.0.0.0/0	tgw-id

Tabela de rotas do gateway de trânsito

Esse cenário usa uma tabela de rotas para as VPCs e uma tabela de rotas para a conexão VPN.

Os anexos da VPC são associados à tabela de rotas a seguir, que tem uma rota propagada para o anexo da VPN.

Destino	Destino	Tipo de rota
10.99.99.0/24	*Anexo para a conexão VPN*	com propagação

O anexo da VPN é associado à tabela de rotas a seguir, que propagou rotas para cada um dos anexos da VPC.

Destino	Destino	Tipo de rota

Destino	Destino	Tipo de rota
10.1.0.0/16	*Anexo para a VPC A*	com propagação
10.2.0.0/16	*Anexo para a VPC B*	com propagação
10.3.0.0/16	*Anexo para a VPC C*	com propagação

Para obter mais informações sobre como propagar rotas em uma tabela de rotas do gateway de trânsito, consulte Propagar uma rota para uma tabela de rotas do gateway de trânsito.

Tabela do BGP do gateway do cliente

A tabela de BGP do gateway do cliente contém os seguintes CIDRs da VPC.

- 10.1.0.0/16
- 10.2.0.0/16
- 10.3.0.0/16

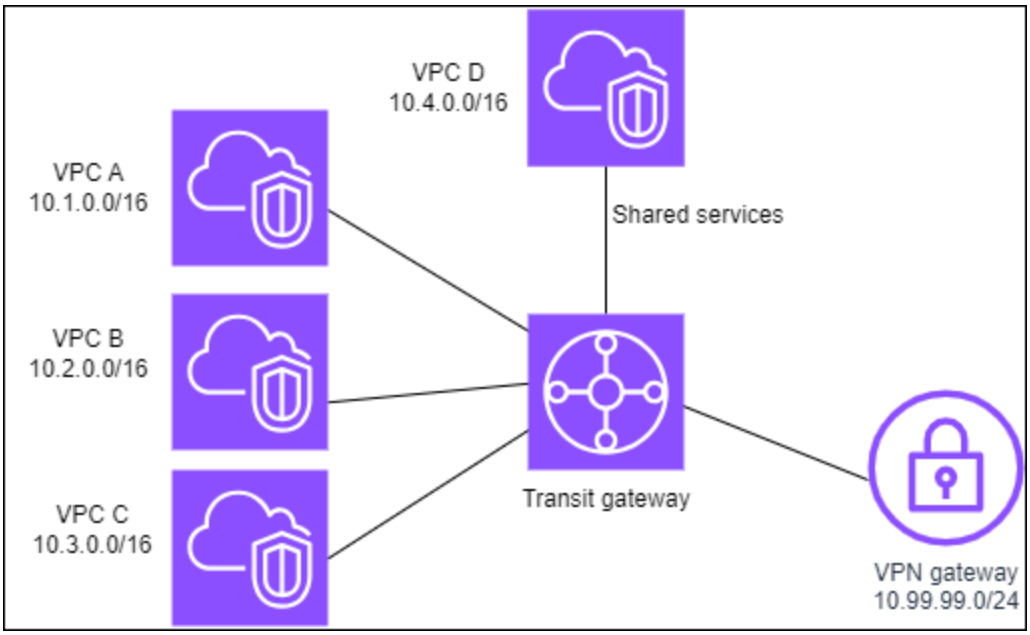
Exemplo: VPCs isoladas com serviços compartilhados

É possível configurar seu gateway de trânsito como vários roteadores isolados que usam um serviço compartilhado. É semelhante ao uso de vários gateways de trânsito, mas permite mais flexibilidade nos casos em que as rotas e os anexos puderem mudar. Nesse cenário, cada roteador isolado tem uma única tabela de roteamento. Todos os anexos associados a uma rota isolada propagam e associam com a tabela de roteamento. Os anexos associados a um roteador isolado podem rotear pacotes entre eles, mas não podem rotear ou receber pacotes dos anexos de outro roteador isolado. Anexos podem fazer o roteamento de pacotes ou receber pacotes dos serviços compartilhados. Você pode usar este cenário quando tiver grupos que precisam ser isolados, mas que usam um serviço compartilhado, como um sistema de produção.

Conteúdos

Visão geral

O diagrama a seguir mostra os principais componentes da configuração deste cenário. Os pacotes das sub-redes na VPC A, VPC B e VPC C que têm a Internet como destino são roteados primeiro por meio do gateway de trânsito e, depois, para o gateway do cliente para a Site-to-Site VPN. Os pacotes de sub-redes na VPC A, VPC B ou VPC C que têm como destino uma sub-rede na VPC A, VPC B ou VPC C são roteados por meio do gateway de trânsito, onde são bloqueados porque não há uma rota para eles na tabela de rotas do gateway de trânsito. Os pacotes da VPC A, VPC B e VPC C que têm a VPC D como destino são roteados por meio do gateway de trânsito e, depois, para a VPC D.



Recursos

Crie os seguintes recursos para este cenário:

- Quatro VPCs. Para obter mais informações sobre como criar uma VPC, consulte Criar uma VPC no Guia do usuário do Amazon VPC.
- Um gateway de trânsito Para obter mais informações, consulte Criar um gateway de trânsito.
- Quatro anexos no gateway de trânsito, um por VPC. Para obter mais informações, consulte the section called “Criar um anexo do gateway de trânsito para uma VPC”.
- Um anexo do Site-to-Site VPN no gateway de trânsito. Para obter mais informações, consulte the section called “Criar um anexo de gateway de trânsito a uma VPN”.

Revise os requisitos para o dispositivo de gateway do cliente no Guia do usuário do AWS Site-to-Site VPN.

Quando a conexão VPN estiver ativada, a sessão de BGP será estabelecida, o CIDR da VPN se propagará para a tabela de rotas do gateway de trânsito e os CIDRs da VPC serão adicionados à tabela de BGP do gateway do cliente.

- Cada VPC isolada é associada à tabela de rotas isolada e propagada para a tabela de rotas compartilhada.
- Cada VPC de serviços compartilhado é associada à tabela de rotas compartilhada e propagada em ambas as tabela de rotas.

Roteamento

Cada VPC tem uma tabela de rotas, e o gateway de trânsito tem duas tabelas de rotas: uma para as VPCs e uma para a conexão VPN e a VPC de serviços compartilhados.

Tabelas de rotas das VPCs A, B, C e D

Cada VPC tem uma tabela de rotas com duas entradas. A primeira entrada é a padrão para um roteamento local na VPC; essa entrada permite que as instâncias na VPC comuniquem-se entre si. A segunda entrada encaminha todos os outros tráfegos da sub-rede IPv4 ao gateway de trânsito.

Destino	Destino
10.1.0.0/16	local
0.0.0.0/0	*ID de gateway de trânsito*

Tabela de rotas do gateway de trânsito

Esse cenário usa uma tabela de rotas para as VPCs e uma tabela de rotas para a conexão VPN.

Os anexos da VPC A, B e C são associados à tabela de rotas a seguir, que tem uma rota propagada para o anexo da VPN e uma rota propagada para o anexo da VPC D.

Destino	Destino	Tipo de rota
10.99.99.0/24	*Anexo para a conexão VPN*	com propagação
10.4.0.0/16	*Anexo para a VPC D*	com propagação

O anexo da VPN e os anexos da VPC de serviços compartilhados (VPC D) são associados à tabela de rotas a seguir, que tem entradas que apontam para cada um dos anexos da VPC. Isso permite uma comunicação com as VPCs da conexão VPN e da VPC de serviços compartilhados.

Destino	Destino	Tipo de rota
10.1.0.0/16	*Anexo para a VPC A*	com propagação
10.2.0.0/16	*Anexo para a VPC B*	com propagação
10.3.0.0/16	*Anexo para a VPC C*	com propagação

Para obter mais informações, consulte Propagar uma rota para uma tabela de rotas do gateway de trânsito.

Tabela do BGP do gateway do cliente

A tabela de BGP do gateway do cliente contém os CIDRs das quatro VPCs.

Exemplo: Gateways de trânsito em pares

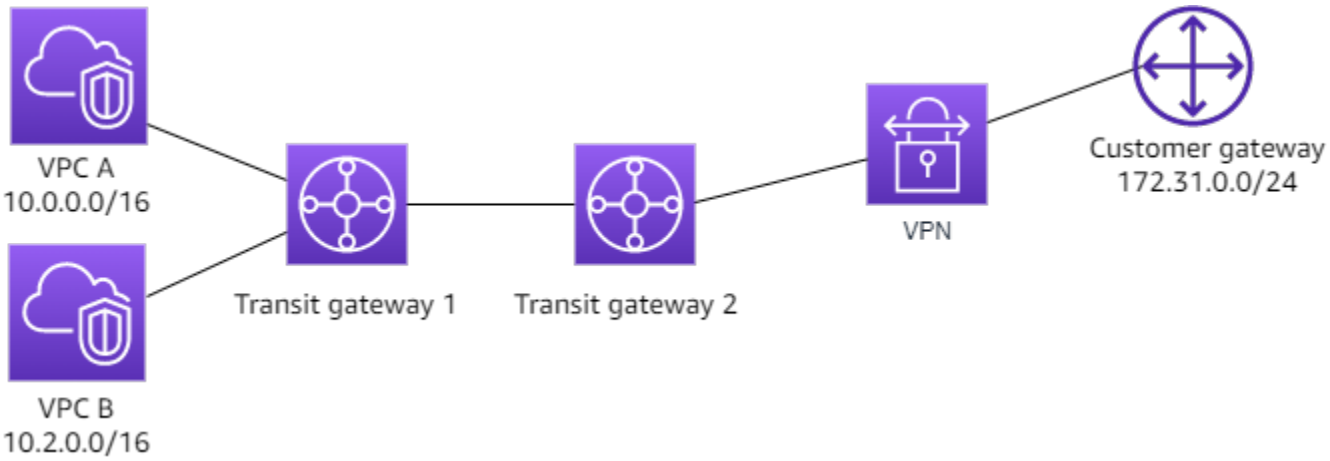
É possível criar uma conexão de emparelhamento de transit gateway entre transit gateways. Depois, é possível rotear o tráfego entre os anexos para cada um dos gateways de trânsito. Nesse cenário, todos os anexos da VPC e da VPN estão associados à tabela de rotas padrão do gateway de trânsito e são propagados para as tabelas de rotas padrão do gateway de trânsito. Cada tabela de rotas do gateway de trânsito tem uma rota estática que aponta para o anexo de emparelhamento do gateway de trânsito.

Conteúdos

- Recursos
- Roteamento

Visão geral

O diagrama a seguir mostra os principais componentes da configuração deste cenário. O gateway de trânsito 1 tem dois anexos da VPC e o gateway de trânsito 2 tem um anexo do Site-to-Site VPN. Os pacotes das sub-redes na VPC A e VPC B que têm a Internet como destino são roteados primeiro por meio do gateway de trânsito 1, depois por meio do gateway de trânsito 2 e, logo depois, são roteados para a conexão VPN.



Recursos

Crie os seguintes recursos para este cenário:

- Duas VPCs. Para obter mais informações sobre como criar uma VPC, consulte Criar uma VPC no Guia do usuário do Amazon VPC.
- Dois transit gateways. Eles podem estar na mesma Região ou em diferentes Regiões. Para obter mais informações, consulte the section called “Criar um gateway de trânsito”.
- Dois anexos de VPC no primeiro gateway de trânsito. Para obter mais informações, consulte the section called “Criar um anexo do gateway de trânsito para uma VPC”.
- Um anexo do Site-to-Site VPN no segundo gateway de trânsito. Para obter mais informações, consulte the section called “Criar um anexo de gateway de trânsito a uma VPN”. Revise os requisitos para o dispositivo de gateway do cliente no Guia do usuário do AWS Site-to-Site VPN.
- Um anexo de emparelhamento do gateway de trânsito entre os dois gateways de trânsito. Para obter mais informações, consulte Anexos de emparelhamento do gateway de trânsito.

Ao criar os anexos da VPC, os CIDRs de cada VPC se propagam para a tabela de rotas do gateway de trânsito 1. Quando a conexão VPN estiver ativada, ocorrerão as seguintes ações:

- A sessão BGP é estabelecida
- O CIDR do Site-to-Site VPN se propaga para a tabela de rotas do gateway de trânsito 2
- Os CIDRs da VPC são adicionados à tabela de BGP do gateway do cliente

Roteamento

Cada VPC tem uma tabela de rotas e cada gateway de trânsito tem uma tabela de rotas.

Tabelas de rotas da VPC A e VPC B

Cada VPC tem uma tabela de rotas com 2 entradas. A primeira entrada é a padrão do roteamento IPv4 local na VPC. Essa entrada padrão permite que os recursos nessa VPC se comuniquem entre si. A segunda entrada encaminha todos os outros tráfegos da sub-rede IPv4 ao gateway de trânsito. A tabela a seguir mostra as rotas da VPC A.

Destino	Destino
10.0.0.0/16	local
0.0.0.0/0	tgw-1-id

Tabela de rotas do gateway de trânsito

Veja a seguir um exemplo da tabela de rotas padrão para o gateway de trânsito 1, com a propagação de rotas ativada.

Destino	Destino	Tipo de rota
10.0.0.0/16	*ID do anexo da VPC A*	com propagação
10.2.0.0/16		com propagação

Destino	Destino	Tipo de rota
	ID do anexo da VPC B	
0.0.0.0/0	*ID do anexo da conexão emparelhada*	estático

Veja a seguir um exemplo da tabela de rotas padrão do gateway de trânsito 2, com a propagação de rotas ativada.

Destino	Destino	Tipo de rota
172.31.0.0/24	*ID do anexo da conexão VPN*	com propagação
10.0.0.0/16	*ID do anexo da conexão emparelhada*	static
10.2.0.0/16	*ID do anexo da conexão emparelhada*	static

Tabela do BGP do gateway do cliente

A tabela de BGP do gateway do cliente contém os seguintes CIDRs da VPC.

- 10.0.0.0/16
- 10.2.0.0/16

Exemplo: Roteamento de saída centralizado para a Internet

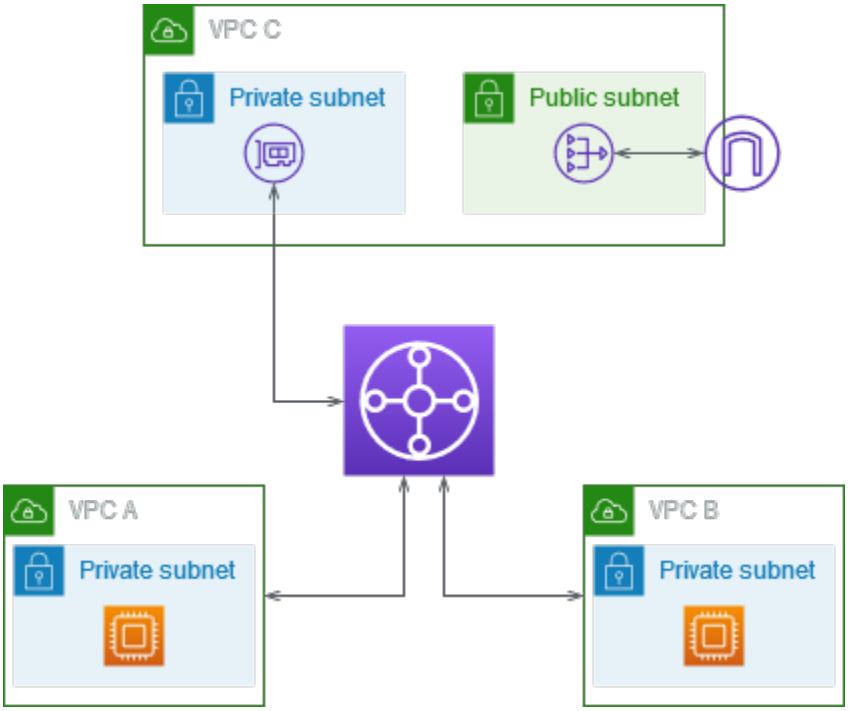
É possível configurar um gateway de trânsito para rotear o tráfego de saída da Internet de uma VPC sem um gateway da Internet para uma VPC que contém um gateway NAT e um gateway da Internet.

Conteúdos

- Roteamento

Visão geral

O diagrama a seguir mostra os principais componentes da configuração deste cenário. Você tem aplicativos na VPC A e na VPC B que precisam de acesso à Internet apenas de saída. Você configura a VPC C com um gateway NAT público e um gateway da Internet, além de uma sub-rede privada para o anexo da VPC. Conecte todas as VPCs a um gateway de trânsito. Configure o roteamento para que o tráfego de saída da Internet da VPC A e da VPC B atravesse o gateway de trânsito para a VPC C. O gateway NAT na VPC C roteia o tráfego para o gateway da Internet.



Recursos

Crie os seguintes recursos para este cenário:

- Três VPCs com intervalos de endereços IP que não se sobrepõem. Para obter mais informações, consulte Criar uma VPC no Guia do usuário da Amazon VPC.
- A VPC A e a VPC B têm sub-redes privadas com instâncias do EC2.
- A VPC C tem o seguinte:
  - Um gateway da Internet anexado à VPC. Para obter mais informações, consulte Criar e anexar um gateway da Internet no Guia do usuário do Amazon VPC.

  - Uma sub-rede pública com um gateway NAT. Para obter mais informações, consulte Criar gateways NAT no Guia do usuário do Amazon VPC.
  - Uma sub-rede privada para o anexo do gateway de trânsito. A sub-rede privada deve estar na mesma zona de disponibilidade da sub-rede pública.
- Um gateway de trânsito. Para obter mais informações, consulte the section called “Criar um gateway de trânsito”.
- Três anexos da VPC no gateway de trânsito. Os blocos CIDR de cada VPC se propagam para a tabela de rotas do gateway de trânsito. Para obter mais informações, consulte the section called “Criar um anexo do gateway de trânsito para uma VPC”. Para a VPC C, você precisa criar o anexo usando a sub-rede privada. Se você criar o anexo usando a sub-rede pública, o tráfego da instância será roteado para o gateway da Internet, mas o gateway da Internet descartará o tráfego porque as instâncias não têm endereços IP públicos. Ao colocar o anexo na sub-rede privada, o tráfego será roteado para o gateway NAT e o gateway NAT enviará o tráfego para o gateway da Internet usando o endereço IP elástico como endereço IP de origem.

Roteamento

Existem tabelas de rotas para cada VPC e uma tabela de rotas para o gateway de trânsito.

Tabelas de rotas

- Tabela de rotas para a VPC A
- Tabela de rotas para a VPC B
- Tabelas de rotas para VPC C
- Tabela de rotas do Transit Gateway

Tabela de rotas para a VPC A

Veja a seguir um exemplo de tabela de rotas. A primeira entrada permite que as instâncias na VPC se comuniquem entre si. A segunda entrada encaminha todos os outros tráfegos da sub-rede IPv4 ao gateway de trânsito.

Destino	Destino
CIDR da VPC A	local

Destino	Destino
0.0.0.0/0	*transit-gateway-id*

Tabela de rotas para a VPC B

Veja a seguir um exemplo de tabela de rotas. A primeira entrada permite que as instâncias na VPC se comuniquem entre si. A segunda entrada encaminha todos os outros tráfegos da sub-rede IPv4 ao gateway de trânsito.

Destino	Destino
CIDR da VPC B	local
0.0.0.0/0	*transit-gateway-id*

Tabelas de rotas para VPC C

Configure a sub-rede com o gateway NAT como uma sub-rede pública adicionando uma rota para o gateway da Internet. Deixe a outra sub-rede como uma sub-rede privada.

Veja a seguir um exemplo de tabela de rotas para a sub-rede pública. A primeira entrada permite que as instâncias na VPC se comuniquem entre si. A segunda e terceira entradas roteiam o tráfego da VPC A e da VPC B para o gateway de trânsito. As entradas remanescentes roteiam todos os outros tráfegos IPv4 da sub-rede para o gateway da Internet.

Destino	Destino
CIDR da VPC C	local
CIDR da VPC A	*transit-gateway-id*
CIDR da VPC B	*transit-gateway-id*
0.0.0.0/0	*internet-gateway-id*

Veja a seguir um exemplo de tabela de rotas da sub-rede privada. A primeira entrada permite que as instâncias na VPC se comuniquem entre si. A segunda entrada roteia todos os outros tráfegos da sub-rede IPv4 ao gateway NAT.

Destino	Destino
CIDR da VPC C	local
0.0.0.0/0	*nat-gateway-id*

Tabela de rotas do Transit Gateway

Veja a seguir um exemplo da tabela de rotas de gateway de trânsito. Os blocos CIDR de cada VPC se propagam para a tabela de rotas do gateway de trânsito. A rota estática envia o tráfego de saída da Internet para a VPC C. Você pode, opcionalmente, impedir a comunicação entre as VPCs adicionando uma rota blackhole para cada CIDR de VPC.

CIDR	Attachment	Tipo de rota
CIDR da VPC A	*Anexo para a VPC A*	com propagação
CIDR da VPC B	*Anexo para a VPC B*	com propagação
CIDR da VPC C	*Anexo para a VPC C*	com propagação
0.0.0.0/0	*Anexo para a VPC C*	estático

Exemplo: dispositivo em uma VPC de serviços compartilhados

Você pode configurar um dispositivo (como um dispositivo de segurança) em uma VPC de serviços compartilhados. Todo o tráfego que é roteado entre anexos de gateway de trânsito é inspecionado primeiro pelo dispositivo na VPC de serviços compartilhados. Quando o modo de dispositivo está habilitado, um gateway de trânsito seleciona uma única interface de rede no dispositivo da VPC, usando um algoritmo de hash de fluxo, para enviar tráfego durante a vida útil do fluxo. O gateway

de trânsito usa a mesma interface de rede para o tráfego de retorno. Isso garante que o tráfego bidirecional seja roteado simetricamente. Ele é roteado pela mesma zona de disponibilidade no anexo da VPC durante a vida útil do fluxo. Se você tiver vários gateways de trânsito na arquitetura, cada um deles mantém a própria afinidade de sessão e pode selecionar uma interface de rede diferente.

Você deve conectar exatamente um gateway de trânsito à VPC do dispositivo para garantir a aderência do fluxo. Conectar vários gateways de trânsito a uma única VPC de dispositivo não garante a aderência do fluxo porque os gateways de trânsito não compartilham informações de estado de fluxo entre si.

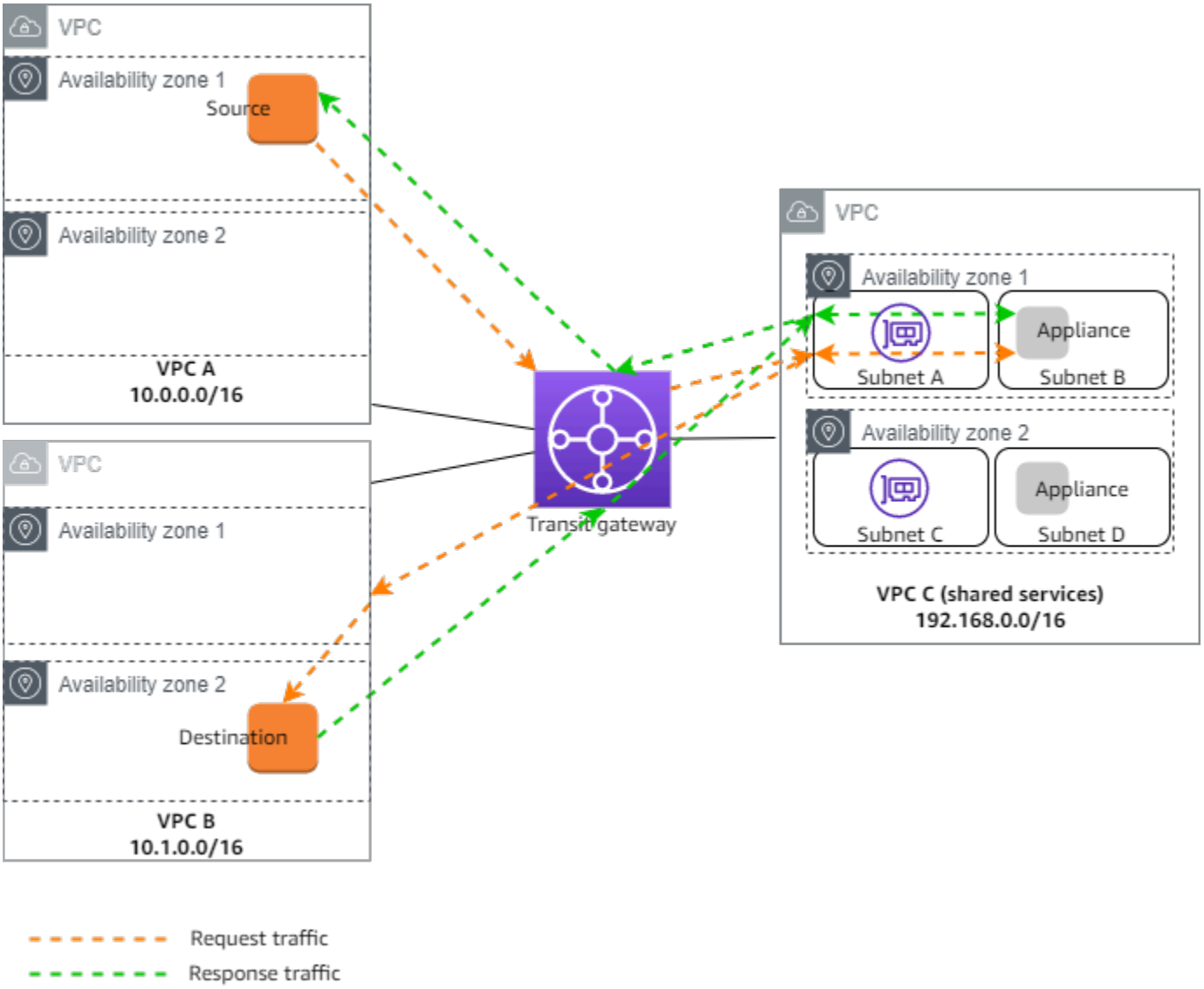
Important

- O tráfego no modo de dispositivo é roteado corretamente, desde que o tráfego de origem e de destino chegue a uma VPC centralizada (VPC de inspeção) do mesmo anexo do Transit Gateway. O tráfego pode ser descartado se a origem e o destino vierem de dois anexos do Transit Gateway diferentes. O modo do dispositivo não se aplica ao tráfego que entra na rede por meio de uma VPN.
- Ativar o modo de equipamento em um anexo existente pode afetar a rota atual desse anexo, pois o anexo pode fluir por qualquer zona de disponibilidade. Quando o modo de dispositivo não está ativado, o tráfego é mantido na zona de disponibilidade de origem.

Conteúdo

Visão geral

O diagrama a seguir mostra os principais componentes da configuração deste cenário. O gateway de trânsito tem três anexos de VPC. A VPC C é uma VPC de serviços compartilhados. O tráfego entre a VPC A e a VPC B é roteado para o gateway de trânsito e, depois, roteado para um dispositivo de segurança na VPC C para inspeção antes de ser encaminhado para o destino final. O dispositivo é com estado, consequentemente o tráfego do solicitação e resposta é inspecionado. Para alta disponibilidade, há um dispositivo em cada zona de disponibilidade na VPC C.



Crie os seguintes recursos para esse cenário:

- Três VPCs. Para obter informações sobre como criar uma VPC, consulte Criar uma VPC no Guia do usuário da Amazon Virtual Private Cloud.
- Um gateway de trânsito Para obter mais informações, consulte the section called “Criar um gateway de trânsito”.
- Três anexos de VPC: um para cada VPC. Para obter mais informações, consulte the section called “Criar um anexo do gateway de trânsito para uma VPC”.

  Para cada anexo de VPC, especifique uma sub-rede em cada zona de disponibilidade. Para a VPC de serviços compartilhados, essas são as sub-redes onde o tráfego é roteado para a VPC a partir do gateway de trânsito. No exemplo anterior, estas são as sub-redes A e C.

Para o anexo da VPC C, habilite o suporte ao modo de dispositivo para que o tráfego de resposta seja encaminhado para a mesma zona de disponibilidade na VPC C que o tráfego de origem.

O console da Amazon VPC oferece suporte ao modo de dispositivo. Também é possível usar a API da Amazon VPC, um SDK da AWS ou a AWS CLI para habilitar o modo de dispositivo ou o AWS CloudFormation. Por exemplo, adicione `--options ApplianceModeSupport=enable` ao comando create-transit-gateway-vpc-attachment ou modify-transit-gateway-vpc-attachment.

> **Note**
>
> A aderência ao fluxo no modo de dispositivo só é garantida para o tráfego de origem e destino com origem em direção à VPC de inspeção.

Dispositivos com estado e modo de dispositivo

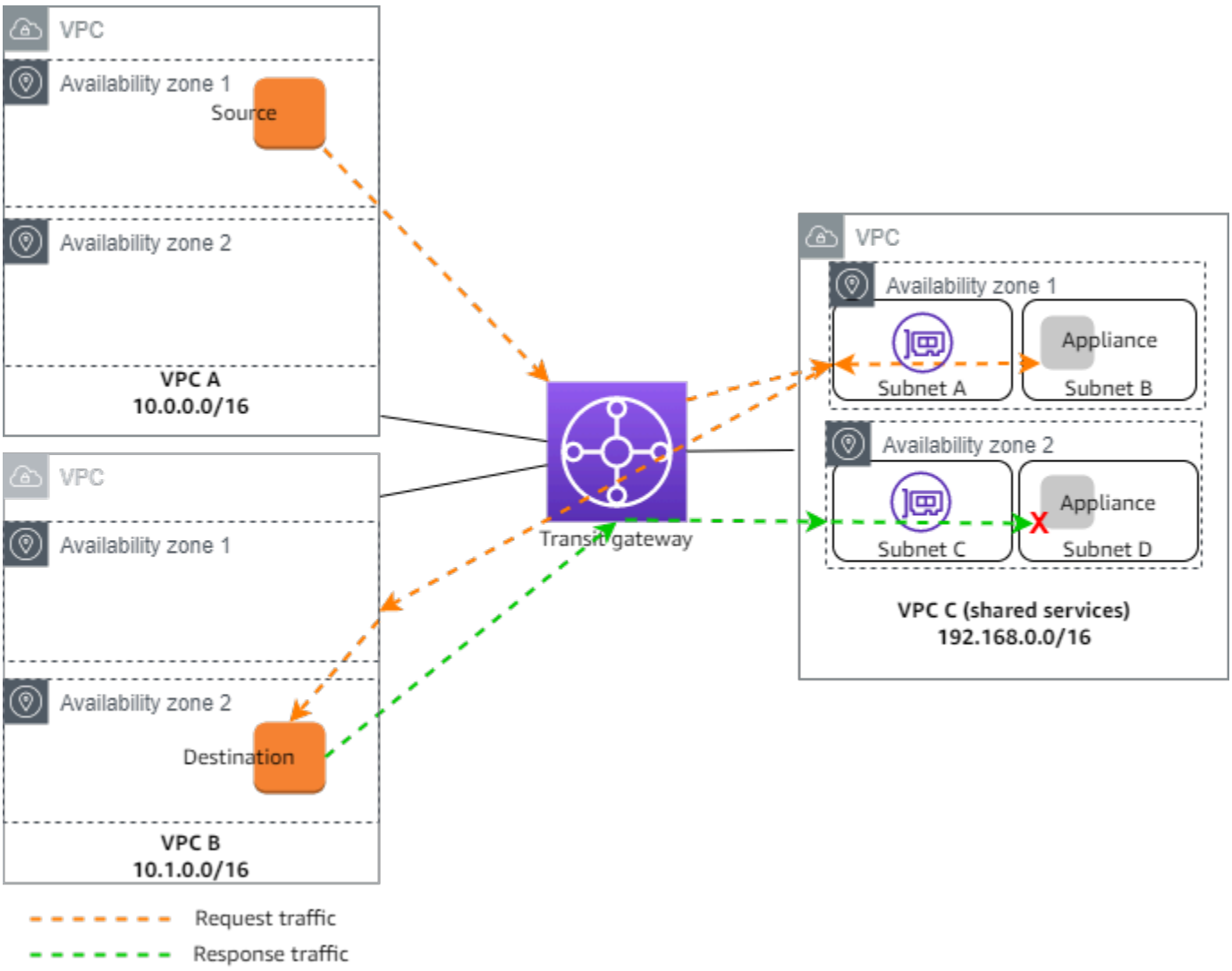
Se seus anexos da VPC abrangem várias zonas de disponibilidade e você precisar que o tráfego entre hosts de origem e destino seja roteado pelo mesmo dispositivo para inspeção com estado, habilite o suporte ao modo de dispositivo para o anexo da VPC no qual o dispositivo está localizado.

Para obter mais informações, consulte Arquitetura de inspeção centralizada no blog da AWS.

Comportamento quando o modo de dispositivo não está habilitado

Quando o modo de dispositivo não está habilitado, um gateway de trânsito tenta manter o tráfego roteado entre anexos da VPC na zona de disponibilidade de origem até atingir o destino. O tráfego cruzará as zonas de disponibilidade entre anexos somente se houver uma falha na zona de disponibilidade ou se não houver sub-redes associadas a um anexo da VPC nessa zona de disponibilidade.

O diagrama a seguir mostra um fluxo de tráfego quando o suporte ao modo de dispositivo não está habilitado. O tráfego de resposta que se origina da zona de disponibilidade 2 na VPC B é roteado pelo gateway de trânsito para a mesma zona de disponibilidade na VPC C. Consequentemente, o tráfego é descartado porque o dispositivo na zona de disponibilidade 2 não está ciente da solicitação original da origem na VPC A.



Roteamento

Cada VPC tem uma ou mais tabelas de rotas e o gateway de trânsito tem duas tabelas de rotas.

Tabelas de rotas da VPC

VPC A e VPC B

As VPCs A e B têm tabelas de rotas com 2 entradas. A primeira entrada é a padrão do roteamento IPv4 local na VPC. Essa entrada padrão permite que os recursos nessa VPC se comuniquem entre si. A segunda entrada encaminha todos os outros tráfegos da sub-rede IPv4 ao gateway de trânsito. Veja a seguir a tabela de rotas para a VPC A.

Destino	Destino
10.0.0.0/16	local
0.0.0.0/0	tgw-id

VPC C

A VPC de serviços compartilhados (VPC C) tem tabelas de rotas diferentes para cada sub-rede. A sub-rede A é usada pelo gateway de trânsito (essa sub-rede é especificada na criação do anexo da VPC). A tabela de rotas para a sub-rede A roteia todo o tráfego ao dispositivo na sub-rede B.

Destino	Destino
192.168.0.0/16	local
0.0.0.0/0	appliance-eni-id

A tabela de rotas para a sub-rede B (que contém o dispositivo) roteia o tráfego de volta ao gateway de trânsito.

Destino	Destino
192.168.0.0/16	local
0.0.0.0/0	tgw-id

Tabela de rotas do gateway de trânsito

Esse gateway de trânsito usa uma tabela de rotas para a VPC A e a VPC B e uma tabela de rotas para a VPC de serviços compartilhados (VPC C).

Os anexos da VPC A e da VPC B estão associados à tabela de rotas a seguir. A tabela de rotas roteia todo o tráfego para a VPC C.

Destino	Destino	Tipo de rota
0.0.0.0/0	*ID do anexo da VPC C*	estático

O anexo da VPC C está associado à tabela de rotas a seguir. Ele encaminha o tráfego para a VPC A e a VPC B.

Destino	Destino	Tipo de rota
10.0.0.0/16	*ID do anexo da VPC A*	com propagação
10.1.0.0/16	*ID do anexo da VPC B*	com propagação

Trabalhar com gateways de trânsito

É possível trabalhar com gateways de trânsito usando o console da Amazon VPC ou a AWS CLI.

Conteúdo

Gateways de trânsito

Um gateway de trânsito permite anexar VPCs e conexões VPN e rotear tráfego entre elas. Um gateway de trânsito funciona Contas da AWS transversalmente e você pode usá-lo AWS RAM para compartilhar seu gateway de trânsito com outras contas. Depois de compartilhar um gateway de trânsito com outro Conta da AWS, o proprietário da conta pode conectar suas VPCs ao seu gateway de trânsito. Um usuário de qualquer uma das contas pode excluir o anexo a qualquer momento.

É possível ativar o multicast em um gateway de trânsito e, depois, criar um domínio de multicast do gateway de trânsito que permita ao tráfego de multicast ser enviado da origem de multicast para membros do grupo de multicast em anexos da VPC associados ao domínio.

Cada anexo da VPC ou VPN está associado a uma única tabela de roteamento. Essa tabela decide o próximo salto para o tráfego que vem do anexo do recurso. Uma tabela de rotas dentro do gateway de trânsito permite alvos e CIDRs IPv4 e IPv6. Os alvos são conexões VPN e VPCs. Quando você anexa uma VPC ou cria uma conexão VPN em um gateway de trânsito, o anexo é associado à tabela de rotas padrão do gateway de trânsito.

É possível criar tabelas de rotas adicionais dentro do gateway de trânsito e alterar as associações de VPN e VPC em cada uma das tabelas. Assim, você pode segmentar sua rede. Por exemplo, você

pode associar VPCs de desenvolvimento a uma tabela de roteamento, e VPCs de produção a uma tabela diferente. Isso permitirá a criação de redes isoladas dentro do gateway de trânsito, de forma semelhante ao Virtual Routing and Forwarding (VRFs) em redes tradicionais.

Os gateways de trânsito oferecem suporte a roteamento dinâmico e estático entre conexões VPN e VPCs anexadas. É possível habilitar ou desabilitar a propagação de rotas em cada anexo. Os anexos de emparelhamento do gateway de trânsito são compatíveis somente com roteamento estático. No entanto, você não pode adicionar uma rota estática que aponte para um emparelhamento entre dois gateways de trânsito na mesma região.

Opcionalmente, você pode associar um ou mais blocos CIDR IPv4 ou IPv6 ao gateway de trânsito. Especifique um endereço IP do bloco CIDR ao estabelecer um par do Transit Gateway Connect para um anexo do Transit Gateway Connect. Você pode associar qualquer intervalo de endereços IP público ou privado, exceto endereços no intervalo `169.254.0.0/16` e intervalos que se sobrepõem a endereços para os anexos VPC e redes on-premises. Para obter mais informações sobre os blocos CIDR de IPv4 e IPv6, consulte VPCs e sub-redes no Guia do usuário do Amazon VPC.

Tarefas

- Criar um gateway de trânsito
- Visualizar os gateways de trânsito
- Adicionar ou editar tags para um gateway de trânsito
- Modificar um gateway de trânsito
- Compartilhar um gateway de trânsito
- Aceitar um compartilhamento de recursos
- Aceitar um anexo compartilhado
- Excluir um gateway de trânsito

Criar um gateway de trânsito

Quando você cria um gateway de trânsito, nós criamos uma tabela de rotas padrão para ele e a usamos como tabela padrão de associação e propagação. Se você não quiser criar a tabela de rotas padrão do transit gateway, poderá criar uma posteriormente. Para obter mais informações sobre rotas e tabelas de rotas, consulte ???.

Como criar um gateway de trânsito usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.

2. No painel de navegação, escolha Transit Gateways (Gateways de trânsito).
3. Escolha Create transit gateway (Criar gateway de trânsito).
4. Para Name tag (Tag de nome), opcionalmente, insira um nome para o gateway de trânsito. Uma tag de nome pode facilitar a identificação de um gateway de trânsito a partir de uma lista de gateways. Quando você adiciona uma Name tag (Tag de nome), uma tag é criada com uma chave de Name (Nome) e um valor igual ao valor que você inserir.
5. Como opção, em Description (Descrição), insira uma descrição para o gateway de trânsito.
6. Em Amazon side Autonomous System Number (ASN) (Número de sistema autônomo no lado da Amazon), deixe o valor padrão para usar o ASN padrão ou insira o ASN privado para o gateway de trânsito. Esse deve ser o ASN do AWS lado de uma sessão do Border Gateway Protocol (BGP).

   O intervalo é de 64512 a 65534 para ASNs de 16-bit.

   O intervalo e de 4200000000 a 4294967294 para ASNs de 32 bits.

   Se você tiver uma implantação em várias regiões, recomendamos usar um ASN exclusivo para cada um dos gateways de trânsito.
7. Em DNS support (Compatibilidade com DNS), selecione essa opção se precisar que a VPC resolva os nomes de host DNS IPv4 públicos para endereços IPv4 privados quando consultado de instâncias em outra VPC anexada ao gateway de trânsito.
8. Em VPN ECMP support (Compatibilidade com ECMP da VPN), selecione essa opção se precisar de suporte ao roteamento de Equal Cost Multipath (ECMP – Múltiplos caminhos de mesmo custo) entre os túneis da VPN. Se as conexões anunciarem os mesmos CIDRs, o tráfego será distribuído igualmente entre eles.

   Ao selecionar essa opção, o BGP ASN anunciado, os atributos do BGP, como AS-path, e as comunidades de preferência devem ser iguais.

   > **Note**
   >
   > Para usar o ECMP, é necessário criar uma conexão VPN que use roteamento dinâmico. Conexões VPN que usam roteamento estático não oferecem suporte a ECMP.
9. Em Default route table association (Associação de tabela de rotas padrão), selecione essa opção para associar automaticamente os anexos de gateway de trânsito à tabela de rotas padrão para o gateway de trânsito.

10. Em Default route table propagation (Propagação de tabela de rotas padrão), selecione essa opção para propagar automaticamente os anexos de gateway de trânsito à tabela de rotas padrão para o gateway de trânsito.
11. (Opcional) Para usar o gateway de trânsito como roteador para tráfego de multicast, selecione Multicast support (Suporte a multicast).
12. Em Auto accept shared attachments (Aceitar automaticamente anexos compartilhados), selecione essa opção para aceitar automaticamente anexos entre contas.
13. (Opcional) Em Transit gateway CIDR blocks (Blocos CIDR do gateway de trânsito), especifique um ou mais blocos CIDR IPv4 ou IPv6 para o gateway de trânsito.

    Você pode especificar um bloco CIDR de tamanho /24 ou maior (por exemplo, /23 ou /22) para IPv4, ou um bloco CIDR de tamanho /64 ou maior (por exemplo, /63 ou /62) para IPv6. Você pode associar qualquer intervalo de endereços IP público ou privado, exceto os endereços no intervalo 169.254.0.0/16 e intervalos que se sobrepõem aos endereços dos anexos da VPC e das redes on-premises.
14. Escolha Create transit gateway (Criar gateway de trânsito).

Para criar um gateway de trânsito usando o AWS CLI

Use o comando create-transit-gateway.

Visualizar os gateways de trânsito

Como visualizar os gateways de trânsito usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateways (Gateways de trânsito). Os detalhes do gateway de trânsito são exibidos sob a lista de gateways na página.

Para visualizar seus portais de transporte público usando o AWS CLI

Use o comando describe-transit-gateways.

Adicionar ou editar tags para um gateway de trânsito

Adicione tags aos seus recursos para ajudar a organizá-los e identificá-los, por exemplo, por propósito, proprietário ou ambiente. É possível adicionar várias tags a cada gateway de trânsito. As

chaves de tag devem ser exclusivas para cada gateway de trânsito. Se você adicionar uma tag com uma chave que já esteja associada ao gateway de trânsito, o valor dessa tag será atualizado. Para obter mais informações, consulte Marcar recursos do Amazon EC2.

Adicionar tags a um gateway de trânsito usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateways (Gateways de trânsito).
3. Escolha o gateway de trânsito para o qual adicionar ou editar tags.
4. Entre na guia Tags na parte inferior da página.
5. Selecione Gerenciar tags.
6. Selecione Add new tag (Adicionar nova etiqueta).
7. Insira uma Key (Chave) e um Value (Valor) para a tag.
8. Escolha Salvar.

Modificar um gateway de trânsito

É possível modificar as opções de configuração do gateway de trânsito. Ao modificar um gateway de trânsito, as opções modificadas são aplicadas somente a novos anexos do gateway de trânsito. Os anexos do gateway de trânsito existentes não são modificados e não detectam nenhuma interrupção do serviço.

Não é possível modificar um gateway de trânsito que tenha sido compartilhado com você.

Não é possível remover um bloco CIDR para o gateway de trânsito se algum dos endereços IP estiver sendo usado para um Connect peer.

Como modificar um gateway de trânsito

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateways (Gateways de trânsito).
3. Escolha o gateway de trânsito para modificar.
4. SelecioneActions (Ações), Modify transit gateway (Modificar gateway de trânsito).
5. Modifique as opções conforme necessário e selecione Modify transit gateway (Modificar gateway de trânsito).

Para modificar seu gateway de trânsito usando o AWS CLI

Use o comando modify-transit-gateway.

Compartilhar um gateway de trânsito

Você pode usar AWS RAM para compartilhar um gateway de trânsito entre contas ou em toda a sua organização em AWS Organizations. Use o procedimento a seguir para compartilhar um gateway de trânsito que você possua.

É necessário habilitar o compartilhamento de recursos a partir da conta mestra da sua organização. Para obter informações sobre como habilitar o compartilhamento de recursos, consulte Enable Sharing with AWS Organizations no Guia AWS RAM do Usuário.

Como compartilhar um gateway de trânsito

1. Abra o AWS RAM console em https://console.aws.amazon.com/ram/.
2. Escolha Create a resource share (Criar um compartilhamento de recursos).
3. Em Name (Nome), insira um nome descritivo para o compartilhamento de recursos.
4. Em Select resource type (Selecionar tipo de recurso), escolha Transit Gateways (Gateways de trânsito). Selecione o gateway de trânsito.
5. (Opcional) em Principals (Principais), adicione os principais ao compartilhamento de recursos. Para cada uma Conta da AWS, OU ou organização, especifique sua ID e escolha Adicionar.

   Em Permitir contas externas, escolha se deseja permitir o compartilhamento desse recurso com Contas da AWS pessoas externas à sua organização.
6. (Opcional) Em Tags, insira uma chave de tag e um par de valores de tag para cada tag. Essas tags são aplicadas ao compartilhamento de recursos, mas não ao gateway de trânsito.
7. Escolha Create resource share (Criar compartilhamento de recursos).

Aceitar um compartilhamento de recursos

Se você foi adicionado a um compartilhamento de recursos, receberá um convite para participar desse compartilhamento. É necessário aceitar o compartilhamento de recurso antes de acessar os recursos compartilhados.

Aceitar um compartilhamento de recursos

1. Abra o AWS RAM console em https://console.aws.amazon.com/ram/.
2. No painel de navegação, escolha Shared with me (Compartilhados comigo), Resource shares (Compartilhamentos de recursos).
3. Selecione o compartilhamento de recursos.
4. Escolha Accept resource share (Aceitar compartilhamento de recurso).
5. Para visualizar o gateway de trânsito compartilhado, abra a página Transit Gateways (Gateways de trânsito) no console da Amazon VPC.

Aceitar um anexo compartilhado

Se você não habilitou a funcionalidade Auto accept shared attachments (Aceitar anexos compartilhados automaticamente) ao criar o gateway de trânsito, é necessário aceitar manualmente os anexos entre contas (compartilhados).

Como aceitar manualmente um anexo compartilhado

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Attachments (Anexos do gateway de trânsito).
3. Selecione o anexo do gateway de trânsito que está pendente de aceitação.
4. SelecioneActions (Ações), Accept transit gateway attachment (Aceitar anexo do gateway de trânsito).

Para aceitar um anexo compartilhado usando o AWS CLI

Use o comando accept-transit-gateway-vpc-attachment.

Excluir um gateway de trânsito

Não é possível excluir um gateway de trânsito com anexos existentes. É preciso excluir todos os anexos para conseguir excluir um gateway de trânsito.

Como excluir um gateway de trânsito usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.

2. Escolha o gateway de trânsito para excluir.
3. Escolha Actions (Ações), Delete transit gateway (Excluir gateway de trânsito). Para confirmar a exclusão, digite **`delete`** e escolha Delete (Excluir).

Para excluir um gateway de trânsito usando o AWS CLI

Use o comando delete-transit-gateway.

Anexos de gateway de trânsito a uma VPC

Quando uma VPC é anexada a um gateway de trânsito, é necessário especificar uma sub-rede de cada zona de disponibilidade a ser usada pelo gateway de trânsito para rotear o tráfego. Especificar uma sub-rede de uma zona de disponibilidade permite que o tráfego chegue até os recursos em cada sub-rede nessa zona de disponibilidade.

Limites

- Quando uma VPC é anexada a um gateway de trânsito, nenhum recurso nas zonas de disponibilidade em que não houver um anexo de gateway de trânsito alcançará o gateway de trânsito. Se houver uma rota para o gateway de trânsito em uma tabela de rotas de sub-rede, o tráfego será enviado ao gateway de trânsito somente quando este tiver um anexo em uma sub-rede na mesma zona de disponibilidade.
- Os recursos em uma VPC anexada a um gateway de trânsito não podem acessar os grupos de segurança de uma VPC diferente que também esteja anexada ao mesmo gateway de trânsito.
- Um gateway de trânsito não é compatível com a resolução de DNS para nomes de DNS personalizados de VPCs anexadas configuradas usando zonas hospedadas privadas no Amazon Route 53. Para configurar a resolução de nomes para zonas hospedadas privadas para todas as VPCs conectadas a um gateway de trânsito, consulte Gerenciamento centralizado de DNS da nuvem híbrida com o Amazon Route 53 e o Transit Gateway AWS.
- Um gateway de trânsito não é compatível com o roteamento entre VPCs com CIDRs idênticos. Se você anexar uma VPC a um gateway de trânsito e seu CIDR for idêntico ao CIDR de outra VPC que já esteja anexada ao gateway de trânsito, as rotas para a VPC recém-anexada não serão propagadas para a tabela de rotas do gateway de trânsito.
- Não é possível criar um anexo para uma sub-rede da VPC que resida em uma zona local. Porém, você pode configurar a rede para que as sub-redes na Zona Local se conectem a um transit gateway por meio da Zona de Disponibilidade principal. Para obter mais informações, consulte

Connect Local Zone subnets to a transit gateway (Conectar sub-redes da Zona Local a um transit gateway).

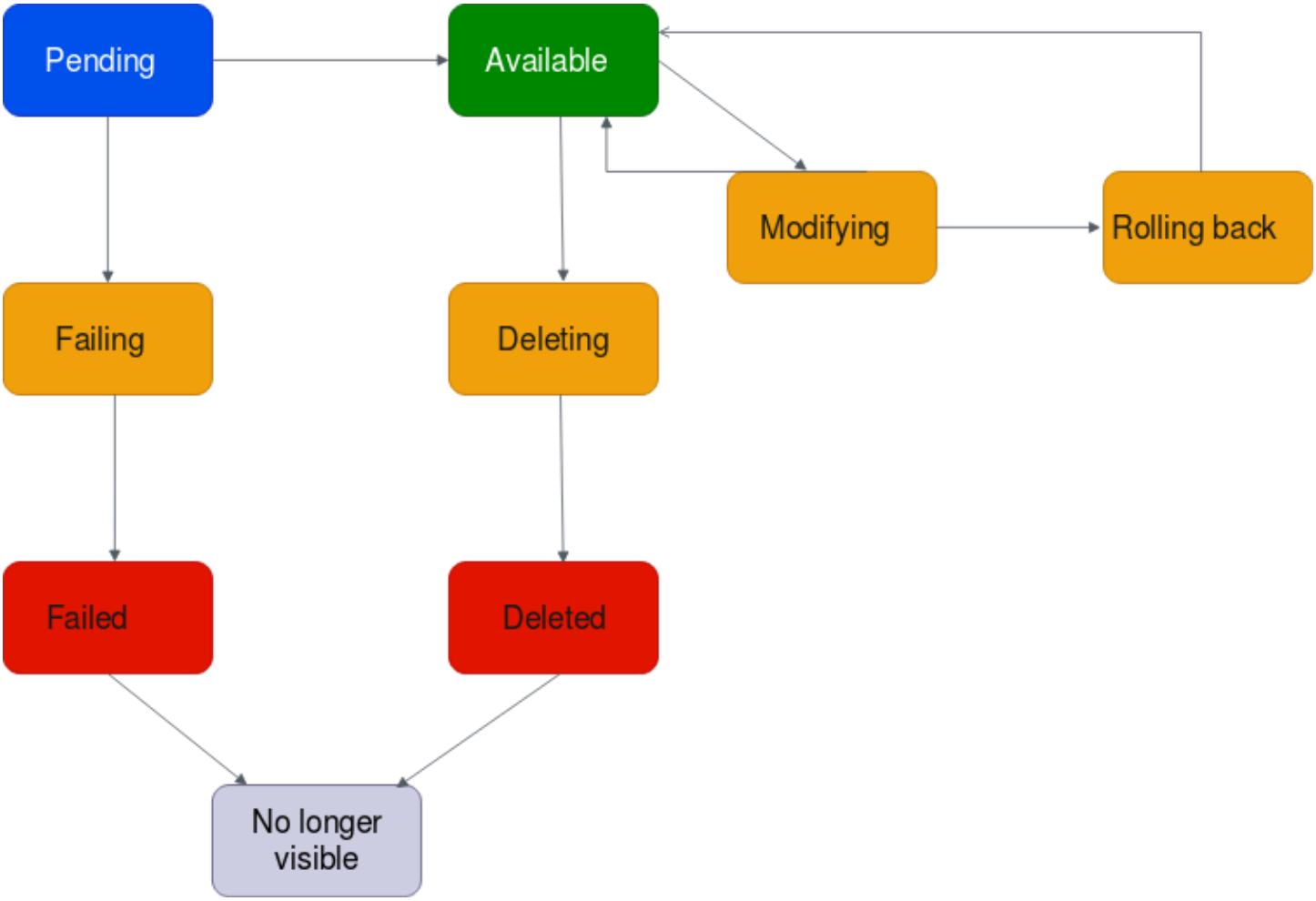
- Não é possível criar um anexo do gateway de trânsito usando sub-redes exclusivamente IPv6. As sub-redes do anexo do gateway de trânsito também devem ser compatíveis com endereços IPv4.
- Um gateway de trânsito deve ter pelo menos um anexo de VPC antes que esse gateway de trânsito possa ser adicionado a uma tabela de rotas.

Conteúdo

Ciclo de vida do anexo da VPC

Um anexo da VPC passa por vários estágios, começando quando a solicitação é iniciada. Em cada etapa, pode haver ações que você pode realizar e, no final do ciclo de vida, o anexo da VPC permanece visível no Amazon Virtual Private Cloud Console e na API ou na saída de linha de comando por um período.

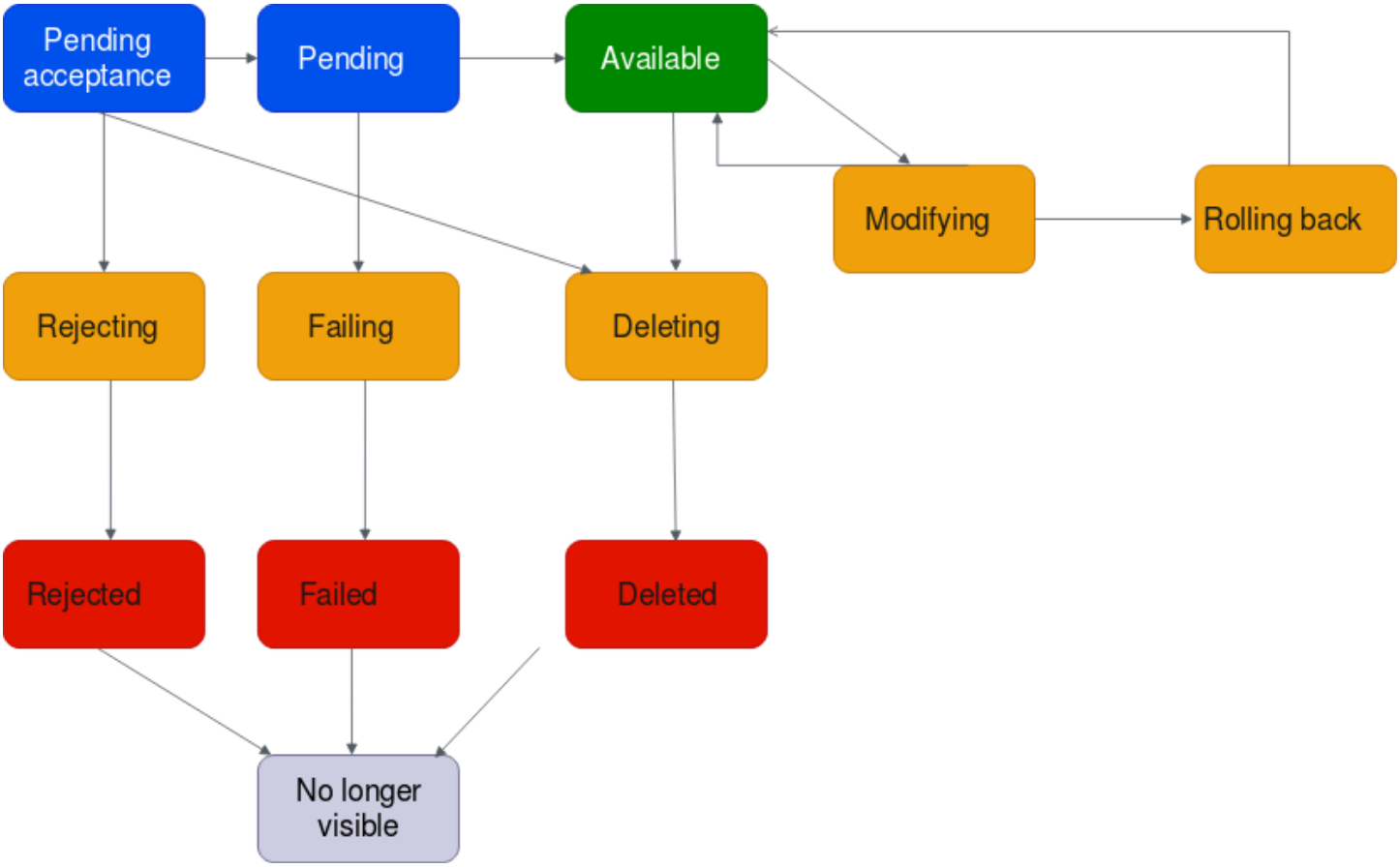
O diagrama a seguir mostra os estados pelos quais um anexo pode passar em uma única configuração de conta ou em uma configuração para várias contas que tenha a opção Auto accept shared attachments (Aceitar automaticamente os anexos compartilhados) ativada.



- Pendente: uma solicitação de anexo da VPC foi iniciada e está no processo de provisionamento. Nesta fase, o anexo pode falhar, ou pode ir para `available`.
- Falhando: uma solicitação de anexo da VPC está mostrando falhas. Nesta fase, o anexo da VPC vai para `failed`.
- Falha: a solicitação de anexo da VPC falhou. Enquanto estiver neste estado, ela não pode ser excluída. O anexo da VPC com falha permanece visível por 2 horas e, em seguida, não será mais visível.
- Disponível: o anexo da VPC está disponível e o tráfego pode fluir entre a VPC e o gateway de trânsito. Nesta fase, o anexo pode ir para `modifying`, ou para `deleting`.
- Excluindo: um anexo da VPC que está em processo de ser excluído. Nesta fase, o anexo pode ir para `deleted`.
- Excluído: um anexo da `available` VPC foi excluído. Enquanto estiver nesse estado, o anexo da VPC não pode ser modificado. O anexo da VPC permanece visível por 2 horas e, em seguida, não será mais visível.

- Modificando: foi feita uma solicitação para modificar as propriedades do anexo da VPC. Nesta fase, o anexo pode ir para `available`, ou para `rolling back`.
- Revertendo: a solicitação de modificação do anexo da VPC não pode ser concluída e o sistema está desfazendo todas as alterações feitas. Nesta fase, o anexo pode ir para `available`.

O diagrama a seguir mostra os estados pelos quais um anexo pode passar em uma configuração de várias contas que tenha a opção Auto accept shared attachments (Aceitar automaticamente os anexo compartilhados) desativada.



- Aceitação pendente: a solicitação de anexo da VPC está aguardando aceitação. Nesta fase, o anexo pode ir para `pending`, para `rejecting` ou para `deleting`.
- Rejeitado: um anexo da VPC que está em processo de ser rejeitado. Nesta fase, o anexo pode ir para `rejected`.
- Rejeitado: um anexo `pending acceptance` da VPC foi rejeitado. Enquanto estiver nesse estado, o anexo da VPC não pode ser modificado. O anexo da VPC permanece visível por 2 horas e, em seguida, não será mais visível.

- Pendente: um anexo da VPC foi aceito e está no processo de provisionamento. Nesta fase, o anexo pode falhar, ou pode ir para `available`.
- Falhando: uma solicitação de anexo da VPC está mostrando falhas. Nesta fase, o anexo da VPC vai para `failed`.
- Falha: a solicitação de anexo da VPC falhou. Enquanto estiver neste estado, ela não pode ser excluída. O anexo da VPC com falha permanece visível por 2 horas e, em seguida, não será mais visível.
- Disponível: o anexo da VPC está disponível e o tráfego pode fluir entre a VPC e o gateway de trânsito. Nesta fase, o anexo pode ir para `modifying`, ou para `deleting`.
- Excluindo: um anexo da VPC que está em processo de ser excluído. Nesta fase, o anexo pode ir para `deleted`.
- Excluída: um anexo `available` ou `pending acceptance` VPC foi excluído. Enquanto estiver nesse estado, o anexo da VPC não pode ser modificado. O anexo da VPC permanece visível por 2 horas e, em seguida, não será mais visível.
- Modificando: foi feita uma solicitação para modificar as propriedades do anexo da VPC. Nesta fase, o anexo pode ir para `available`, ou para `rolling back`.
- Revertendo: a solicitação de modificação do anexo da VPC não pode ser concluída e o sistema está desfazendo todas as alterações feitas. Nesta fase, o anexo pode ir para `available`.

Criar um anexo do gateway de trânsito para uma VPC

Para criar um anexo da VPC usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Attachments (Anexos do gateway de trânsito).
3. Escolha Create transit gateway attachment (Criar anexo do gateway de trânsito).
4. Em Name tag (Etiqueta de nome), como opção, insira um nome para o anexo do gateway de trânsito.
5. Em Transit Gateway ID (ID do gateway de trânsito), escolha o gateway de trânsito para o anexo. Você pode escolher um gateway de trânsito de sua propriedade ou um que tenha sido compartilhado com você.
6. Em Tipo de anexo, escolha VPC.
7. Escolha se deseja ativar o DNS Support, o IPv6 Support e o suporte ao modo Appliance.

Se o modo de dispositivo for escolhido, o fluxo de tráfego entre a origem e o destino usará a mesma zona de disponibilidade para o anexo VPC durante a vida útil desse fluxo.

8. Em VPC ID (ID da VPC), escolha a VPC a ser anexada ao gateway de trânsito.

   Essa VPC precisa estar associada a pelo menos uma sub-rede.

9. Em Subnet IDs (IDs de sub-rede), selecione uma sub-rede para cada zona de disponibilidade a ser usada pelo gateway de trânsito para rotear o tráfego. É necessário selecionar pelo menos uma sub-rede. Você pode selecionar somente uma sub-rede por zona de disponibilidade.
10. Escolha Create transit gateway attachment (Criar anexo do gateway de trânsito).

Para criar um anexo de VPC usando o AWS CLI

Use o comando create-transit-gateway-vpc-attachment.

Modificar seu anexo da VPC

Como modificar seus anexos da VPC usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Attachments (Anexos do gateway de trânsito).
3. Selecione o anexo da VPC e escolha Actions (Ações), Modify transit gateway attachment (Modificar anexo do gateway de trânsito).
4. Para habilitar o suporte do DNS, selecione DNS support (Suporte do DNS).
5. Para adicionar uma sub-rede ao anexo, marque a caixa ao lado da sub-rede.

   Adicionar ou modificar uma sub-rede de anexos de VPC pode afetar o tráfego de dados enquanto o anexo estiver em um estado de modificação.

6. Escolha Modify transit gateway attachment (Modificar anexo do gateway de trânsito).

Para modificar seus anexos de VPC usando o AWS CLI

Use o comando modify-transit-gateway-vpc-attachment.

Modificar as tags de seu anexo da VPC

Como modificar as tags de seu anexo da VPC usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Attachments (Anexos do gateway de trânsito).
3. Selecione o anexo da VPC e escolha Actions (Ações), Manage tags (Gerenciar etiquetas).
4. [Adicionar uma tag] Escolha Adicionar nova tag e faça o seguinte:
   - Em Key (Chave), insira o nome da chave.
   - Em Valor, insira o valor da chave.
5. [Remover uma tag] Ao lado da tag, escolha Remove (Remover).
6. Escolha Salvar.

As tags de anexo da VPC só podem ser modificadas usando o console.

Visualizar os anexos da VPC

Para visualizar seus anexos da VPC usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Attachments (Anexos do gateway de trânsito).
3. Na coluna Resource type (Tipo de recurso), procure por VPC. Ela exibe os anexos da VPC.
4. Escolha um anexo para visualizar seus detalhes.

Para visualizar seus anexos de VPC usando o AWS CLI

Use o comando describe-transit-gateway-vpc-attachments.

Excluir um anexo da VPC

Para excluir um anexo da VPC usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.

2. No painel de navegação, escolha Transit Gateway Attachments (Anexos do gateway de trânsito).
3. Selecione o anexo da VPC.
4. Escolha Actions (Ações), Delete transit gateway attachment (Excluir anexo do gateway de trânsito).
5. Quando solicitado, digite **`delete`** e escolha Delete (Excluir).

Para excluir um anexo de VPC usando o AWS CLI

Use o comando delete-transit-gateway-vpc-attachment.

Solucionar problemas de criação de anexos da VPC

O tópico a seguir pode ajudar a solucionar problemas que possam surgir quando você cria um anexo da VPC.

Problema

Selecione o anexo da VPC com falha.

Causa

A causa pode ser uma das seguintes:

1. O usuário que estiver criando o anexo da VPC não tem permissões corretas para criar a função vinculada a serviços.
2. Há um problema de controle de utilização devido a muitas solicitações do IAM. Por exemplo, você está usando o AWS CloudFormation para criar permissões e funções.
3. A conta tem a função vinculada a serviços e essa função foi modificada.
4. O gateway de trânsito não está no estado `available`.

Solução

Dependendo da causa, tente o seguinte:

1. Verifique se o usuário tem as permissões corretas para criar funções vinculadas a serviços. Para obter mais informações, consulte Permissões de perfil vinculado a serviços no Guia do usuário do IAM. Depois que o usuário tiver as permissões, crie o anexo da VPC.

2. Crie o anexo da VPC manualmente por meio do console ou da API. Para ter mais informações, consulte the section called “Criar um anexo do gateway de trânsito para uma VPC”.
3. Verifique se a função vinculada a serviços tem as permissões corretas. Para ter mais informações, consulte the section called “Transit gateway”.
4. Verifique se o gateway de trânsito está no estado `available`. Para ter mais informações, consulte the section called “Visualizar os gateways de trânsito”.

Anexos da VPN de gateway de trânsito

Para anexar uma conexão VPN ao seu gateway de trânsito, é necessário especificar o gateway do cliente. Para obter mais informações sobre os requisitos para um gateway do cliente, consulte Requisitos para seu gateway do cliente no Guia do usuário do AWS Site-to-Site VPN .

Para VPNs estáticas, adicione as rotas estáticas à tabela de rotas de gateway de trânsito.

Criar um anexo de gateway de trânsito a uma VPN

Para criar um anexo da VPN usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Attachments (Anexos do gateway de trânsito).
3. Escolha Create transit gateway attachment (Criar anexo do gateway de trânsito).
4. Em Transit Gateway ID (ID do gateway de trânsito), escolha o gateway de trânsito para o anexo. É possível escolher um gateway de trânsito que você possua.
5. Em Attachment type (Tipo de anexo), escolha VPN.
6. Em Customer Gateway (Gateway do cliente, siga uma das opções a seguir:
   - Para usar um gateway do cliente existente, escolha Existing (Existente) e selecione o gateway que você quer usar.

     Se o gateway do cliente estiver atrás de um dispositivo de tradução de endereço de rede (NAT), que esteja habilitado para NAT traversal (NAT-T), use o endereço IP público do dispositivo NAT e ajuste as regras de firewall para desbloquear a porta UDP 4500.
   - Para criar um gateway do cliente, escolha New (Novo), em IP Address (Endereço IP), insira um endereço IP público estático e BGP ASN.

Em Routing options (Opções de roteamento), escolha entre Dynamic (Dinâmico) ou Static (Estático). Para obter mais informações, consulte Opções de roteamento de VPN lugar a lugar no Guia do usuário do AWS Site-to-Site VPN .

7. Em Tunnel Options (Opções de túnel), insira os intervalos CIDR e as chaves pré-compartilhadas para o túnel. Para obter mais informações, consulte Site-to-Site VPN architectures (Arquiteturas da VPN Site-to-Site).
8. Escolha Create transit gateway attachment (Criar anexo do gateway de trânsito).

Para criar um anexo VPN usando o AWS CLI

Use o comando create-vpn-connection.

Visualizar os anexos da VPN

Para visualizar seus anexos da VPN usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Attachments (Anexos do gateway de trânsito).
3. Na coluna Resource type (Tipo de recurso), procure por VPN. Ela exibe os anexos da VPN.
4. Escolha um anexo para visualizar os detalhes ou adicionar tags.

Para visualizar seus anexos de VPN usando o AWS CLI

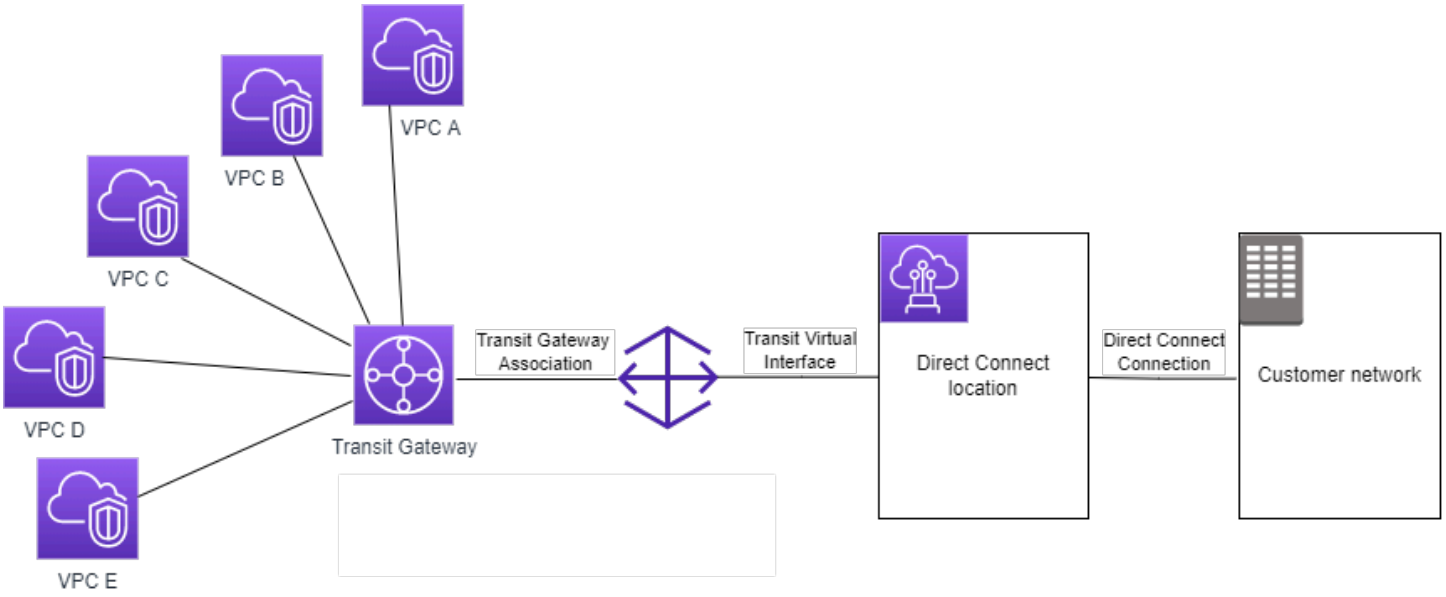
Use o comando describe-transit-gateway-attachments.

Anexos do gateway de trânsito a um gateway Direct Connect

Anexe um gateway de trânsito a um gateway Direct Connect usando uma interface virtual de trânsito. Essa configuração oferece os benefícios abaixo. É possível:

- Gerenciar uma única conexão para várias VPCs ou VPNs que estão na mesma região.
- Anunciar prefixos de on-premises para a AWS e da AWS para on-premises.

O diagrama a seguir ilustra como o gateway Direct Connect permite que você crie uma única conexão com a conexão do Direct Connect que todas as suas VPCs podem usar.



A solução envolve os componentes abaixo:

- Um gateway de trânsito
- Gateway Direct Connect
- Uma associação entre o gateway Direct Connect e o gateway de trânsito.
- Uma interface virtual de trânsito que é anexada ao gateway Direct Connect.

Para obter informações sobre como configurar gateways do Direct Connect com gateways de trânsito, consulte Associações de gateway de trânsito no Manual do usuário do AWS Direct Connect.

Anexos de emparelhamento do gateway de trânsito

É possível emparelhar tanto gateways de trânsito intrarregional e inter-regional e direcionar o tráfego entre eles, o que inclui tráfego de IPv4 e IPv6. Para fazer isso, crie um anexo de emparelhamento no seu transit gateway e especifique um transit gateway. O gateway de trânsito de mesmo nível pode estar em sua conta ou em outra Conta da AWS.

Depois que você cria uma solicitação de anexo de emparelhamento, o proprietário do gateway de trânsito de mesmo nível (também chamado de gateway de trânsito do aceitante) deve aceitar a solicitação. Para rotear o tráfego entre os gateways de trânsito, adicione uma rota estática à tabela de rotas do gateway de trânsito que aponte para o anexo de emparelhamento do gateway de trânsito.

Recomendamos o uso de ASNs exclusivos para cada gateway de trânsito emparelhado a fim de aproveitar as funcionalidades futuras de propagação de rotas.

O emparelhamento do gateway de trânsito não oferece suporte à resolução de nomes de host de DNS IPv4 públicos ou privados em endereços IPv4 privados em VPCs em ambos os lados do anexo de emparelhamento do transit gateway usando o Amazon Route 53 Resolver em outra região. Para obter mais informações sobre o Route 53 Resolver, consulte O que é Route 53 Resolver? no Guia do desenvolvedor do Amazon Route 53.

O emparelhamento de gateway entre regiões usa a mesma infraestrutura de rede que o emparelhamento da VPC. Portanto, o tráfego é criptografado usando criptografia AES-256 na camada de rede virtual à medida que viaja entre regiões. O tráfego também é criptografado usando criptografia AES-256 na camada física quando atravessa os links de rede que estão fora do controle físico da AWS. Como resultado, o tráfego é criptografado duas vezes em links de rede fora do controle físico da AWS. Dentro da mesma região, o tráfego é criptografado na camada física somente quando atravessa links de rede que estão fora do controle físico da AWS.

Para obter informações sobre quais regiões oferecem suporte a anexos de emparelhamento de gateway de trânsito, consulte Perguntas frequentes sobre o AWS Transit Gateway.

Criar um anexo de emparelhamento

Antes de começar, verifique se você tem o ID do gateway de trânsito que deseja anexar. Se o gateway de trânsito estiver em outra Conta da AWS, verifique se você tem o ID da Conta da AWS do proprietário do gateway de trânsito.

Depois que você criar o anexo de emparelhamento, o proprietário do gateway de trânsito receptor deverá aceitar a solicitação de anexo.

Como criar um anexo de emparelhamento usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Attachments (Anexos do gateway de trânsito).
3. Escolha Create transit gateway attachment (Criar anexo do gateway de trânsito).
4. Em Transit gateway ID (ID do gateway de trânsito), escolha o gateway de trânsito para o anexo. Você pode escolher um gateway de trânsito de sua propriedade ou um que tenha sido compartilhado com você.

5. Em Attachment type (Tipo de anexo), selecione Peering Connection (Conexão de emparelhamento).
6. Se desejar, insira uma tag de nome para o anexo.
7. Em Account (Conta), siga um destes procedimentos:
   - Se o gateway de trânsito estiver na sua conta, escolha My account (Minha conta).
   - Se o gateway de trânsito estiver em outra Conta da AWS, escolha Outra conta. Em Account ID (ID da conta), insira o ID da Conta da AWS.
8. Em Region (Região), selecione a região na qual o gateway de trânsito está localizado.
9. Em Transit gateway (accepter) (Gateway de trânsito [aceitante]), insira o ID do gateway de trânsito que deseja anexar.
10. Escolha Create transit gateway attachment (Criar anexo do gateway de trânsito).

Como criar um anexo de emparelhamento usando a AWS CLI

Use o comando create-transit-gateway-peering-attachment.

Aceitar ou rejeitar uma solicitação de anexo de emparelhamento

Para ativar o anexo de emparelhamento, o proprietário do gateway de trânsito do aceitante deve aceitar a solicitação de anexo de emparelhamento. Isso é necessário mesmo se ambos os gateways de trânsito estiverem na mesma conta. O anexo de emparelhamento deve estar no estado `pendingAcceptance`. Aceite a solicitação de anexo de emparelhamento da região em que o gateway de trânsito do aceitante está localizado.

Se preferir, você poderá rejeitar qualquer solicitação de conexão de emparelhamento recebida que esteja no estado `pendingAcceptance`. Você deve rejeitar a solicitação da região em que o gateway de trânsito do aceitante está localizado.

Como aceitar uma solicitação de anexo emparelhamento usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Attachments (Anexos do gateway de trânsito).
3. Selecione o anexo de emparelhamento do gateway de trânsito que está com a aceitação pendente.

4. SelecioneActions (Ações), Accept transit gateway attachment (Aceitar anexo do gateway de trânsito).
5. Adicione a rota estática à tabela de rotas do gateway de trânsito. Para obter mais informações, consulte the section called “Criar uma rota estática”.

Como rejeitar uma solicitação de anexo emparelhamento usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Attachments (Anexos do gateway de trânsito).
3. Selecione o anexo de emparelhamento do gateway de trânsito que está com a aceitação pendente.
4. SelecioneActions (Ações), Reject transit gateway attachment (Rejeitar anexo do gateway de trânsito).

Como aceitar ou rejeitar um anexo de emparelhamento usando a AWS CLI

Use os comandos accept-transit-gateway-peering-attachment e reject-transit-gateway-peering-attachment.

Adicionar uma rota à tabela de rotas do gateway de trânsito

Para rotear o tráfego entre os gateways de trânsito emparelhados, é necessário adicionar uma rota estática à tabela de rotas do gateway de trânsito que aponte para o anexo de emparelhamento do gateway de trânsito. O proprietário do gateway de trânsito receptor também deve adicionar uma rota estática à tabela de rotas do gateway de trânsito.

Como criar uma rota usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Route Tables (Tabelas de rotas do gateway de trânsito).
3. Selecione a tabela de rotas para a qual criar a rota.
4. Escolha Actions (Ações), Create static route (Criar rota estática).

5. Na página Create static route (Criar rota estática), insira o bloco CIDR para o qual deseja criar a rota. Por exemplo, especifique o bloco CIDR de uma VPC anexada ao gateway de trânsito de mesmo nível.
6. Escolha o anexo de emparelhamento para a rota.
7. Escolha Create static route (Criar rota estática).

Como criar uma rota estática usando a AWS CLI

Use o comando create-transit-gateway-route.

> **Important**
>
> Depois de criar a rota, associe a tabela de rotas do gateway de trânsito ao anexo de emparelhamento do gateway de trânsito. Para obter mais informações, consulte the section called “Associar uma tabela de rotas do gateway de trânsito”.

Visualizar os anexos da conexão de emparelhamento do gateway de trânsito

É possível visualizar os anexos de emparelhamento do gateway de trânsito e as informações sobre eles.

Como visualizar seus anexos de emparelhamento usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Attachments (Anexos do gateway de trânsito).
3. Na coluna Resource type (Tipo de recurso), procure por Peering (Emparelhamento). Nela, você verá os anexos de emparelhamento.
4. Escolha um anexo para visualizar seus detalhes.

Como visualizar os anexos de emparelhamento do gateway de trânsito usando a AWS CLI

Use o comando describe-transit-gateway-peering-attachments.

Excluir um anexo de emparelhamento

É possível excluir um anexo de emparelhamento do gateway de trânsito. O proprietário de qualquer um dos gateways de trânsito pode excluir o anexo.

Como excluir um anexo de emparelhamento usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Attachments (Anexos do gateway de trânsito).
3. Selecione o anexo de emparelhamento do gateway de trânsito.
4. SelecioneActions (Ações), Delete transit gateway attachment (Excluir anexo do gateway de trânsito).
5. Insira **`delete`** e escolha Delete (Excluir).

Como excluir um anexo de emparelhamento usando a AWS CLI

Use o comando delete-transit-gateway-peering-attachment.

Considerações sobre a região da AWS de adesão

Você pode emparelhar gateways de trânsito através dos limites da região de adesão. Para obter mais informações sobre essas regiões e sobre como aderir, consulte Gerenciar regiões da AWS na Referência geral da Amazon Web Services. Leve o seguinte em consideração ao usar o emparelhamento de gateway de trânsito nestas regiões:

- Você pode emparelhar em uma região de adesão, desde que a conta que aceita o anexo de emparelhamento tenha aderido à essa região.
- Independentemente do status de adesão da região, a AWS compartilha os seguintes dados de conta com a conta que aceita o anexo de emparelhamento:
  - ID da Conta da AWS
  - ID de gateway de trânsito
  - Código da região
- Quando você exclui o anexo do gateway de trânsito, os dados da conta acima são excluídos.
- Recomendamos que você exclua o anexo de emparelhamento do gateway de trânsito antes de cancelar a adesão à região. Se você não excluir o anexo de peering, o tráfego poderá continuar a

passar pelo anexo e você continuará a receber cobranças. Se você não excluir o anexo, poderá aderir novamente e, em seguida, excluir o anexo.

- Em geral, o gateway de trânsito tem um modelo de pagamento de remetente. Ao usar um anexo de emparelhamento de gateway de trânsito em um limite de opção, você pode incorrer em cobranças em uma Região que aceita o anexo, incluindo as Regiões em que você não aderiu. Para obter mais informações, consulte Preços do AWS Transit Gateway.

Anexos do Transit Gateway Connect e pares do Transit Gateway Connect

Você pode criar um anexo do Transit Gateway Connect para estabelecer uma conexão entre um gateway de trânsito e dispositivos virtuais de terceiros (como dispositivos SD-WAN) em execução na VPC. Um anexo do Connect apoia o protocolo de túnel do Generic Routing Encapsulation (GRE) para alta performance, e o Border Gateway Protocol (BGP) para o roteamento dinâmico. Depois de criar um anexo do Connect, você pode criar um ou mais túneis GRE (também conhecidos como pares do Transit Gateway Connect) nesse anexo para conectar o gateway de trânsito e o dispositivo de terceiros. Estabeleça duas sessões BGP sobre o túnel GRE para trocar informações de roteamento.

> **Important**
>
> Um par do Transit Gateway Connect consiste em duas sessões de emparelhamento BGP que terminam na infraestrutura gerenciada pela AWS. As duas sessões de emparelhamento BGP fornecem redundância do ambiente de roteamento, garantindo que a perda de uma sessão de emparelhamento BGP não afete a operação de roteamento. As informações de roteamento recebidas de ambas as sessões de emparelhamento BGP são acumuladas para o par de Connect em questão. As duas sessões de emparelhamento BGP também protegem contra qualquer operação na infraestrutura da AWS, como manutenção de rotina, aplicação de patches, atualizações e substituições de hardware. Se o par de Connect estiver operando sem a recomendada sessão dupla de emparelhamento BGP configurada para redundância, poderá ocorrer uma perda momentânea de conectividade durante as operações na infraestrutura da AWS. É altamente recomendável configurar ambas as sessões de emparelhamento BGP no par de Connect. Se você configurou vários pares de Connect para garantir alta disponibilidade no lado do equipamento, é recomendável configurar ambas as sessões de emparelhamento BGP em cada um dos pares de Connect.

Um anexo do Connect usa um anexo da VPC ou do Direct Connect existente como mecanismo de transporte subjacente. Isto é referido como o anexo de transporte. O gateway de trânsito identifica pacotes GRE combinados do dispositivo de terceiros como tráfego do anexo do Connect. Ele trata todos os outros pacotes, incluindo pacotes GRE com informação incorreta da origem ou do destino, como o tráfego do anexo do transporte.

> **Note**
>
> Para usar um anexo do Direct Connect como um mecanismo de transporte, primeiro é necessário integrar o Direct Connect ao AWS Transit Gateway. Para obter as etapas para a criação dessa integração, consulte Integrar dispositivos SD-WAN com o AWS Transit Gateway e AWS Direct Connect.

Conteúdos

Pares do Connect

Um par do Connect (túnel GRE) consiste nos seguintes componentes.

Blocos CIDR internos (endereços BGP)

Os endereços IP internos que são usados para o peering BGP. Você deve especificar um bloco CIDR /29 a partir do intervalo `169.254.0.0/16` para IPv4. Opcionalmente, você pode especificar um bloco CIDR /125 a partir do intervalo `fd00::/8` para IPv6. Os seguintes blocos CIDR são reservados e não podem ser usados:

- 169.254.0.0/29

- 169.254.1.0/29
- 169.254.2.0/29
- 169.254.3.0/29
- 169.254.4.0/29
- 169.254.5.0/29
- 169.254.169.248/29

Você deve configurar o primeiro endereço do intervalo IPv4 no dispositivo como o endereço IP do BGP. Quando você usa o IPv6, se o seu bloco CIDR interno for fd00::/125, configure o primeiro endereço neste intervalo (fd00::1) na interface de túnel do dispositivo.

Os endereços BGP devem ser exclusivos em todos os túneis em um gateway de trânsito.

Endereços IP de par

O endereço IP de par (endereço IP externo GRE) no lado do dispositivo do par do Connect. Isso pode ser qualquer endereço IP. O endereço IP pode ser um endereço IPv4 ou IPv6, mas deve ser a mesma família de endereços IP que o endereço de gateway de trânsito.

Endereço de gateway de trânsito

O endereço IP do par (endereço IP externo GRE) no lado do gateway de trânsito do par do Connect. O endereço IP deve ser especificado no bloco CIDR do gateway de trânsito e deve ser exclusivo nos anexos do Connect no gateway de trânsito. Se você não especificar um endereço IP, usaremos o primeiro endereço disponível do bloco CIDR do gateway de trânsito.

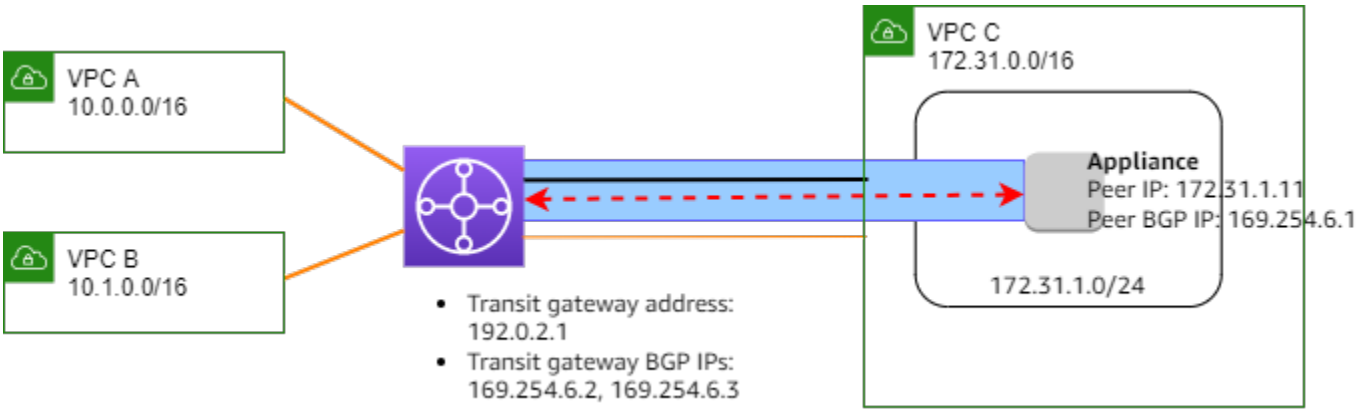
Você pode adicionar um bloco CIDR de gateway de trânsito ao criar ou modificar um gateway de trânsito.

O endereço IP pode ser um endereço IPv4 ou IPv6, mas deve ser a mesma família de endereços IP que o endereço IP do par.

O endereço IP do par e o endereço do gateway de trânsito são usados para identificar exclusivamente o túnel GRE. Você pode reutilizar um ou outro endereço através de vários túneis, mas não ambos no mesmo túnel.

O Transit Gateway Connect para o emparelhamento BGP é compatível apenas com BGP multiprotocolo (MP-BGP), em que o endereçamento IPv4 Unicast também é necessário para estabelecer uma sessão BGP para IPv6 Unicast. Você pode usar endereços IPv4 e IPv6 para endereços IP externos do GRE.

O exemplo a seguir mostra um anexo do Connect entre um gateway de trânsito e um dispositivo em uma VPC.



Componente diagrama	Descrição
	Anexo da VPC
	Anexo do Connect
	Túnel GRE (par do Connect)
	Sessão de emparelhamento BGP

No exemplo anterior, um anexo do Connect é criado em um anexo da VPC existente (o anexo de transporte). Um par do Connect é criado no anexo do Connect para estabelecer uma conexão com um dispositivo na VPC. O endereço de gateway de trânsito é `192.0.2.1`, e o intervalo de endereços BGP é `169.254.6.0/29`. O primeiro endereço IP no intervalo (`169.254.6.1`) é configurado no dispositivo como o endereço IP do par BGP.

A tabela de rotas de sub-rede para a VPC C tem uma rota que aponta o tráfego destinado ao bloco CIDR do gateway de trânsito para o gateway de trânsito.

Destino	Destino
172.31.0.0/16	Local

Destino	Destino
192.0.2.0/24	tgw-id

Requisitos e considerações

Veja a seguir requisitos e considerações para o anexo do Connect.

- Para obter informações sobre quais regiões oferecem suporte a anexos do Connect, consulte Perguntas frequentes sobre os AWS Transit Gateways.
- O dispositivo de terceiros deve ser configurado para enviar e receber tráfego através de um túnel GRE de e para o gateway de trânsito usando o anexo do Connect.
- O dispositivo de terceiros deve ser configurado para usar o BGP para atualizações de rotas dinâmicas e verificações de integridade.
- Os seguintes tipos de BGP são compatíveis:
  - O BGP exterior (eBGP): usado para conexão com os roteadores que estão em um sistema autônomo diferente do gateway de trânsito. Se você usa o eBGP, configure o ebgp-multihop com um valor de time-to-live (TTL – vida útil) de 2.
  - BGP interior (iBGP): usado para conexão com os roteadores que estão no mesmo sistema autônomo que o gateway de trânsito. O gateway de trânsito não instalará rotas de um par do iBGP (dispositivo de terceiros), a menos que as rotas tenham origem em um par do eBGP e tenham configuração automática de próximo salto. As rotas anunciadas pelo dispositivo de terceiros sobre o emparelhamento do iBGP devem ter um ASN.
  - Multiprotocol extensions for BGP (MP-BGP –extensões multiprotocolo para BGP): usadas para serem compatíveis com vários tipos de protocolo, como famílias de endereços IPv4 e IPv6.
- O tempo limite padrão do keep-alive do BGP é de 10 segundos e o temporizador de espera padrão é de 30 segundos.
- Não há suporte para o emparelhamento do BGP baseado em IPv6. Somente o emparelhamento do BGP baseado em IPv4 tem suporte. Os prefixos IPv6 são trocados pelo emparelhamento do BGP baseado em IPv4 usando o MP-BGP.
- Não há suporte para Bidirectional Forwarding Detection (BFD – Detecção de encaminhamento bidirecional).
- Não há suporte para reinício normal do BGP.

- Quando você cria um par de gateway de trânsito, se você não especifica um número ASN de par, nós escolhemos o número ASN do gateway de trânsito. Isso significa que seu dispositivo e gateway de trânsito estarão no mesmo sistema autônomo fazendo iBGP.
- Quando houver dois pares do Connect, a rota preferencial será um par do Connect usando o atributo BGP AS-PATH.

  Para usar o roteamento equal-cost multi-path (ECMP – vários caminhos de mesmo custo) entre dispositivos múltiplos, você deve configurar o dispositivo para anunciar os mesmos prefixos ao gateway de trânsito com o mesmo atributo BGP AS-PATH. Para que o gateway de trânsito escolha todos os caminhos ECMP disponíveis, o AS-PATH e o Autonomous System Number (ASN – Número de sistema autônomo) devem combinar. O gateway de trânsito pode usar o ECMP entre pares do Connect para o mesmo anexo do Connect ou entre anexos dele no mesmo gateway de trânsito. O transit gateway não pode usar o ECMP entre os dois pares redundantes do BGP que um único par estabelece a ele.
- Com um anexo do Connect, as rotas são propagadas para uma tabela de rotas de gateway de trânsito por padrão.
- Rotas estáticas não são compatíveis.
- A Unidade Máxima de Transmissão (MTU) da interface externa do dispositivo de terceiros (fonte do túnel) deverá
  - corresponder ao MTU da interface do túnel GRE ou
  - deverá ser maior do que a interface do túnel GRE.

Criar um anexo do Connect

Para criar um anexo do Connect, você deve especificar um já existente como anexo de transporte. Você pode especificar um anexo da VPC ou um anexo do Direct Connect como o anexo de transporte.

Para criar um anexo do Connect usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Anexos do gateway de trânsito.
3. Escolha Create transit gateway attachment (Criar anexo do gateway de trânsito).
4. (Opcional) Em Name tag (Etiqueta de nome), especifique uma etiqueta de nome para o anexo.
5. Em Transit Gateway ID (ID do gateway de trânsito), escolha o gateway de trânsito para o anexo.

6. Em Attachment type, escolha Connect.
7. Em Transport attachment ID, escolha o ID de um anexo existente (o anexo de transporte).
8. Escolha Create transit gateway attachment (Criar anexo do gateway de trânsito).

Para criar um anexo do Connect usando a AWS CLI

Use o comando create-transit-gateway-connect.

Criar um par do Connect (túnel GRE)

Você pode criar um par do Connect (túnel GRE) para um anexo do Connect existente. Antes de começar, certifique-se de ter configurado um bloco CIDR de gateway de trânsito. Você pode configurar um bloco CIDR de gateway de trânsito ao criar ou modificar um gateway de trânsito.

Quando você cria o par do Connect, você deve especificar o endereço IP externo GRE no lado do dispositivo do par do Connect.

Para criar um par do Connect usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Anexos do gateway de trânsito.
3. Selecione o anexo do Connect, e escolha Actions (Ações), Create Connect peer (Criar par de conexão).
4. (Opcional) Para Tag de nome, especifique uma etiqueta de nome para o par do Connect.
5. (Opcional) Para o Transit gateway GRE Address (Endereço GRE do gateway de trânsito), especifique o endereço IP externo de GRE para o gateway de trânsito. Por padrão, o primeiro endereço disponível do bloco CIDR do gateway de trânsito é usado.
6. Para o Endereço de GRE de par, especifique o endereço IP externo GRE para o lado do dispositivo do par do Connect.
7. Para BGP Inside CIDR blocks IPv4, especifique o intervalo de endereços IPv4 internos que são usados para o emparelhamento BGP. Especifique um bloco CIDR /29 no intervalo `169.254.0.0/16`.
8. (Opcional) Para BGP Inside CIDR blocks IPv6, especifique o intervalo de endereços IPv6 internos que são usados para o emparelhamento BGP. Especifique um bloco CIDR /125 no intervalo `fd00::/8`.

9. (Opcional) Para o ASN de par, especifique o número de sistema autônomo (ASN) do Protocolo de Gateway da Borda (BGP) para o dispositivo. É possível usar um ASN já existente e atribuído para a rede. Se não possuir um, você poderá usar um ASN privado no intervalo de 64512–65534 (ASN de 16 bits) ou 4200000000–4294967294 (ASN de 32 bits).

   O padrão é o mesmo ASN que o gateway de trânsito. Se você configura o Peer ASN de maneira diferente do ASN de gateway de trânsito (eBGP), configure o ebgp-multihop com um TTL de 2.
10. Escolha Create connect peer (Criar par do Connect).

Para criar um par do Connect usando a AWS CLI

Use o comando create-transit-gateway-connect-peer.

Ver os anexos do Connect e os pares do Connect

Você pode ver os anexos do Connect e os pares do Connect.

Para ver os anexos e os pares do Connect usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Anexos do gateway de trânsito.
3. Selecione o anexo do Connect.
4. Para ver os pares do Connect para o anexo, escolha a guia Connect Peers.

Para ver os anexos e os pares do Connect usando a AWS CLI

Use os comandos describe-transit-gateway-connect e describe-transit-gateway-connect-peers .

Modificar as tags de pares e anexo do Connect

Você pode modificar as tags do anexo do Connect.

Para modificar as tags do anexo do Connect usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Attachments.
3. Selecione o anexo do Connect e escolha Actions (Ações), Manage tags (Gerenciar etiquetas).

4. Para adicionar uma etiqueta, selecione Add new tag (Adicionar nova etiqueta) e especifique o nome e o valor da chave.
5. Para remover uma tag, selecione Remover.
6. Escolha Save (Salvar).

Você pode modificar as tags do par do Connect.

Para modificar as tags do par do Connect usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Attachments.
3. Selecione o anexo do Connect e, em seguida, selecione Connect peers.
4. Selecione o par do Connect e escolha Ações, Gerenciar tags.
5. Para adicionar uma etiqueta, selecione Add new tag (Adicionar nova etiqueta) e especifique o nome e o valor da chave.
6. Para remover uma tag, selecione Remover.
7. Escolha Save (Salvar).

Para modificar o anexo do Connect e as tags do par do Connect usando a AWS CLI

Use os comandos create-tags e delete-tags.

Excluir um par do Connect

Você pode excluir um par do Connect, caso não precise mais dele.

Para excluir um par do Connect usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Anexos do gateway de trânsito.
3. Selecione o anexo do Connect.
4. Na aba Pares do Connect , selecione o par do Connect e, em seguida, Ações, Excluir par do Connect.

Para excluir um par do Connect usando a AWS CLI

Use o comando delete-transit-gateway-connect-peer.

Excluir um par do Connect

Você pode excluir um par do anexo do Connect, caso não precise mais dele. Primeiro, você deve excluir todos os pares do Connect para o anexo.

Para excluir um anexo do Connect usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Anexos do gateway de trânsito.
3. Selecione o anexo do Connect e escolha Actions (Ações), Delete transit gateway attachment (Excluir anexo do gateway de trânsito).
4. Insira **`delete`** e escolha Delete (Excluir).

Para excluir um anexo do Connect usando a AWS CLI

Use o comando delete-transit-gateway-connect.

Tabela de rotas do gateway de trânsito

Use tabelas de rotas de gateway de trânsito para configurar o roteamento para seus anexos de gateway de trânsito.

Criar uma tabela de rotas do gateway de trânsito

Como criar uma tabela de rotas de gateway de trânsito usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Route Tables (Tabelas de rotas do gateway de trânsito).
3. Escolha Create transit gateway route table (Criar tabela de roteamento do gateway de trânsito).
4. (Opcional) Para Name tag (Tag de nome), digite um nome para a tabela de rotas do gateway de trânsito. Essa ação cria uma tag com a chave "Nome", e o valor da tag é o nome que você especificou.
5. Em Transit Gateway ID (ID do gateway de trânsito), selecione o gateway de trânsito para a tabela de rotas.

6. Escolha Create transit gateway route table (Criar tabela de roteamento do gateway de trânsito).

Para criar uma tabela de rotas do Transit Gateway usando o AWS CLI

Use o comando create-transit-gateway-route-table.

Visualizar tabelas de rotas do gateway de trânsito

Como visualizar as tabelas de rotas do gateway de trânsito usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Route Tables (Tabelas de rotas do gateway de trânsito).
3. (Opcional) Para encontrar uma tabela ou um conjunto de tabelas de rotas específico, digite o nome completo ou parte dele, palavra-chave ou atributo no campo do filtro.
4. Marque a caixa de seleção ou escolha o ID de uma tabela de rotas para exibir informações sobre as associações, propagações, rotas e tags.

Para visualizar as tabelas de rotas do gateway de trânsito usando o AWS CLI

Use o comando describe-transit-gateway-route-tables.

Para visualizar as rotas de uma tabela de rotas do Transit Gateway usando o AWS CLI

Use o comando search-transit-gateway-routes.

Para visualizar as propagações de rotas para uma tabela de rotas do Transit Gateway usando o AWS CLI

Use o comando get-transit-gateway-route-table-propagations.

Para visualizar as associações de uma tabela de rotas de gateway de trânsito usando o AWS CLI

Use o comando get-transit-gateway-route-table-association.

Associar uma tabela de rotas do gateway de trânsito

É possível associar uma tabela de rotas do gateway de trânsito a um anexo de gateway de trânsito.

Como associar uma tabela de rotas do gateway de trânsito usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Route Tables (Tabelas de rotas do gateway de trânsito).
3. Selecione a tabela de rotas.
4. Na parte inferior da página. escolha a guia Associations (Associações).
5. Escolha Create association (Criar associação).
6. Escolha o anexo para associar e escolha Create association (Criar associação).

Para associar uma tabela de rotas do Transit Gateway usando o AWS CLI

Use o comando associate-transit-gateway-route-table.

Excluir uma associação da tabela de rotas de um gateway de trânsito

É possível desassociar uma tabela de rotas do gateway de trânsito de um anexo de gateway de trânsito.

Como desassociar uma tabela de rotas do gateway de trânsito usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Route Tables (Tabelas de rotas do gateway de trânsito).
3. Selecione a tabela de rotas.
4. Na parte inferior da página. escolha a guia Associations (Associações).
5. Escolha o anexo para desassociar e escolha Delete association (Excluir associação).
6. Quando a confirmação for solicitada, escolha Delete association (Excluir associação).

Para desassociar uma tabela de rotas do Transit Gateway usando o AWS CLI

Use o comando disassociate-transit-gateway-route-table.

Propagar uma rota para uma tabela de rotas do gateway de trânsito

Use a propagação de rotas para adicionar uma rota de um anexo a uma tabela de rotas.

Como propagar uma rota para uma tabela de rotas de anexo de gateway de trânsito

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Route Tables (Tabelas de rotas do gateway de trânsito).
3. Selecione a tabela de rotas para a qual você criará a propagação.
4. Escolha Actions (Ações), Create propagation (Criar propagação).
5. Na página Create propagation (Criar propagação), escolha o anexo.
6. Escolha Create propagation (Criar propagação).

Para habilitar a propagação de rotas usando o AWS CLI

Use o comando enable-transit-gateway-route-table-propagation.

Desabilitar a propagação de rotas

Remova uma rota propagada de um anexo da tabela de roteamento.

Para desativar a propagação de rotas usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Route Tables (Tabelas de rotas do gateway de trânsito).
3. Selecione a tabela de rotas da qual você excluirá a propagação.
4. Na parte inferior da página. escolha a guia Propagations (Propagações).
5. Selecione o anexo e Delete propagation (Excluir propagação).
6. Quando a confirmação for solicitada, escolha Delete propagation (Excluir propagação).

Para desativar a propagação de rotas usando o AWS CLI

Use o comando disable-transit-gateway-route-table-propagation.

Criar uma rota estática

É possível criar uma rota estática para uma VPC, para uma VPC ou para um anexo de emparelhamento de gateway de trânsito ou criar uma rota blackhole que descarta o tráfego correspondente à rota.

As rotas estáticas em uma tabela de rotas do gateway de trânsito para um anexo da VPN não são filtradas pela VPN de local a local. Isso pode permitir que o tráfego de saída flua de maneira não intencional ao usar uma VPN baseada em BGP.

Como criar uma rota usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Route Tables (Tabelas de rotas do gateway de trânsito).
3. Selecione a tabela de rotas para a qual criar a rota.
4. Escolha Actions (Ações), Create static route (Criar rota estática).
5. Na página Create static route (Criar rota estática), insira o bloco CIDR para o qual deseja criar a rota e escolha Active (Ativo).
6. Escolha o anexo para a rota.
7. Escolha Create static route (Criar rota estática).

Como criar uma rota blackhole usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Route Tables (Tabelas de rotas do gateway de trânsito).
3. Selecione a tabela de rotas para a qual criar a rota.
4. Escolha Actions (Ações), Create static route (Criar rota estática).
5. Na página Create static route (Criar rota estática), insira o bloco CIDR para o qual deseja criar a rota e escolha Blackhole (Buraco negro).
6. Escolha Create static route (Criar rota estática).

Para criar uma rota estática ou rota de buraco negro usando o AWS CLI

Use o comando create-transit-gateway-route.

Excluir uma rota estática

Você pode excluir rotas estáticas de uma tabela de rotas do gateway de trânsito.

Como excluir uma rota estática usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Route Tables (Tabelas de rotas do gateway de trânsito).
3. Selecione a tabelas de rotas da qual excluir a rota e escolha Routes (Rotas).
4. Escolha a rota e ser excluída.
5. Escolha Delete static route (Excluir rota estática).
6. Na caixa de diálogo de confirmação, escolha Delete static route (Excluir rota estática).

Para excluir uma rota estática usando o AWS CLI

Use o comando delete-transit-gateway-route.

Substituir uma rota estática

Você pode substituir uma rota estática em uma tabela de rotas do gateway de trânsito por outra rota estática.

Para substituir uma rota estática usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Route Tables (Tabelas de rotas do gateway de trânsito).
3. Escolha a rota que você deseja substituir na tabela de rotas.
4. Na seção de detalhes, escolha a guia Rotas.
5. Escolha Ações, Substituir rota estática.
6. Em Tipo, escolha Ativo ou Buraco negro.
7. No menu suspenso Escolher anexo, escolha o gateway de trânsito que substituirá o atual na tabela de rotas.
8. Escolha Substituir rota estática.

Para substituir uma rota estática usando o AWS CLI

Use o comando replace-transit-gateway-route.

Exportar tabelas de rotas para o Amazon S3

É possível exportar as rotas nas tabelas de rotas do gateway de trânsito para um bucket do Amazon S3. As rotas são salvas no bucket do Amazon S3 especificado em um arquivo JSON.

Como exportar tabelas de rotas do gateway de trânsito usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Route Tables (Tabelas de rotas do gateway de trânsito).
3. Escolha a tabela e roteamento que inclui as rotas para exportar
4. Escolha Actions (Ações), Export routes (Exportar rotas).
5. Na página Export routes (Exportar rotas), em S3 bucket name (nome do bucket do S3), digite o nome do bucket S3.
6. Para filtrar as rotas exportadas, especifique os parâmetros de filtro na seção Filters (Filtros) da página.
7. Escolha Export routes (Exportar rotas).

Para acessar as rotas exportadas, abra o console do Amazon S3 em https://console.aws.amazon.com/s3/ e navegue até o bucket especificado. O nome do arquivo inclui o Conta da AWS ID, a AWS região, o ID da tabela de rotas e um carimbo de data/hora. Selecione o arquivo e escolha Download. Veja a seguir um exemplo de um arquivo JSON que contém informações sobre duas rotas propagadas para anexos da VPC.

```
{
  "filter": [
    {
      "name": "route-search.subnet-of-match",
      "values": [
        "0.0.0.0/0",
        "::/0"
      ]
    }
  ],
  "routes": [
    {
      "destinationCidrBlock": "10.0.0.0/16",
      "transitGatewayAttachments": [
```

```
        {
          "resourceId": "vpc-0123456abcd123456",
          "transitGatewayAttachmentId": "tgw-attach-1122334455aabbcc1",
          "resourceType": "vpc"
        }
      ],
      "type": "propagated",
      "state": "active"
    },
    {
      "destinationCidrBlock": "10.2.0.0/16",
      "transitGatewayAttachments": [
        {
          "resourceId": "vpc-abcabc123123abca",
          "transitGatewayAttachmentId": "tgw-attach-6677889900aabbcc7",
          "resourceType": "vpc"
        }
      ],
      "type": "propagated",
      "state": "active"
    }
  ]
}
```

Excluir uma tabela de rotas do gateway de trânsito

Como excluir uma tabela de rotas do gateway de trânsito usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Route Tables (Tabelas de rotas do gateway de trânsito).
3. Selecione a tabela de rotas a ser excluída.
4. Escolha Actions (Ações), Delete transit gateway route table (Excluir tabela de rotas do gateway de trânsito).
5. Para confirmar a exclusão, digite **`delete`** e escolha Delete (Excluir).

Para excluir uma tabela de rotas do Transit Gateway usando o AWS CLI

Use o comando delete-transit-gateway-route-table.

Referências da lista de prefixos

É possível fazer referência a uma lista de prefixos na tabela de rotas do gateway de trânsito. Uma lista de prefixos é um conjunto de uma ou mais entradas de bloco CIDR que você define e gerencia. É possível usar uma lista de prefixos para simplificar o gerenciamento dos endereços IP aos quais você faz referência nos recursos para rotear o tráfego de rede. Por exemplo, se você especificar frequentemente os mesmos CIDRs de destino em várias tabelas de rotas de gateway de trânsito, poderá gerenciar esses CIDRs em uma única lista de prefixos, em vez de referenciar repetidamente os mesmos CIDRs em cada tabela de rotas. Se você precisar remover um bloco CIDR de destino, poderá remover a entrada da lista de prefixos em vez de remover a rota de cada tabela de rotas afetada.

Ao criar uma referência de lista de prefixos na tabela de rotas do gateway de trânsito, cada entrada na lista de prefixos é representada como uma rota na tabela de rotas do gateway de trânsito.

Para obter mais informações sobre listas de prefixos, consulte Listas de prefixos no Guia do usuário da Amazon VPC.

Criar uma referência de lista de prefixos

É possível criar uma referência a uma lista de prefixos na tabela de rotas do gateway de trânsito.

Como criar uma referência de lista de prefixos usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Transit Gateway Route Tables (Tabelas de rotas do Transit Gateway).
3. Selecione a tabela de rotas do gateway de trânsito.
4. Selecione Actions (Ações), Create prefix list reference (Criar referência da lista de prefixos).
5. Em Prefix list ID (ID da lista de prefixos), selecione o ID da lista de prefixos.
6. Em Type (Tipo), escolha se o tráfego para essa lista de prefixos deve ser permitido (Active [Ativo]) ou desconectado (Blackhole [Buraco negro]).
7. Em Transit gateway attachment ID (ID do anexo do gateway de trânsito), selecione o ID do anexo para o qual deseja rotear o tráfego.
8. Selecione Create prefix list reference (Criar referência da lista de prefixos).

Para criar uma referência da lista de prefixos usando a AWS CLI

Use o comando create-transit-gateway-prefix-list-reference.

Visualizar referências da lista de prefixos

É possível visualizar as referências da lista de prefixos na tabela de rotas do gateway de trânsito. Também é possível visualizar cada entrada na lista de prefixos como uma rota individual na tabela de rotas do gateway de trânsito. O tipo de rota de uma rota de lista de prefixos é `propagated`.

Como visualizar uma referência de lista de prefixos usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Transit Gateway Route Tables (Tabelas de rotas do Transit Gateway).
3. Selecione a tabela de rotas do gateway de trânsito.
4. No painel inferior, selecione Prefix list references (Referências de lista de prefixos). As referências da lista de prefixos são listadas.
5. Selecione Routes (Rotas). Cada entrada de lista de prefixos é listada como uma rota na tabela de rotas.

Para visualizar uma referência da lista de prefixos usando a AWS CLI

Use o comando get-transit-gateway-prefix-list-references.

Modificar uma referência da lista de prefixos

É possível modificar uma referência da lista de prefixos alterando o anexo para o qual o tráfego é roteado ou indicando se o tráfego correspondente à rota deve ser descartado.

Não é possível modificar as rotas individuais de uma lista de prefixos na guia Routes (Rotas). Para modificar as entradas na lista de prefixos, use a tela Managed Prefix Lists (Listas de prefixos gerenciados). Para obter mais informações, consulte Modificar uma lista de prefixos no Guia do usuário da Amazon VPC.

Como modificar uma referência da lista de prefixos usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Transit Gateway Route Tables (Tabelas de rotas do Transit Gateway).

3. Selecione a tabela de rotas do gateway de trânsito.
4. No painel inferior, selecione Prefix list references (Referências de lista de prefixos).
5. Escolha a referência da lista de prefixos e selecione Modify references (Modificar referências).
6. Em Type (Tipo), escolha se o tráfego para essa lista de prefixos deve ser permitido (Active [Ativo]) ou desconectado (Blackhole [Buraco negro]).
7. Em Transit gateway attachment ID (ID do anexo do gateway de trânsito), selecione o ID do anexo para o qual deseja rotear o tráfego.
8. Selecione Modify prefix list reference (Modificar referência da lista de prefixos).

Para modificar uma referência da lista de prefixos usando a AWS CLI

Use o comando modify-transit-gateway-prefix-list-reference.

Excluir uma referência da lista de prefixos

Se não precisar mais de uma referência da lista de prefixos, você poderá excluí-la da tabela de rotas do gateway de trânsito. Excluir a referência não exclui a lista de prefixos.

Como excluir uma referência da lista de prefixos usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Transit Gateway Route Tables (Tabelas de rotas do Transit Gateway).
3. Selecione a tabela de rotas do gateway de trânsito.
4. Escolha a referência da lista de prefixos e selecione Delete references (Excluir referências).
5. Selecione Delete references (Excluir referências).

Para excluir uma referência da lista de prefixos usando a AWS CLI

Use o comando delete-transit-gateway-prefix-list-reference.

Tabelas de políticas de gateway de trânsito

O roteamento dinâmico de gateways de trânsito usa tabelas de políticas para rotear o tráfego de rede para o AWS Cloud WAN. A tabela contém regras de política para comparar o tráfego de rede com os

atributos da política e, em seguida, mapear o tráfego que corresponde à regra para uma tabela de rotas de destino.

Você pode usar o roteamento dinâmico em gateways de trânsito para a troca automática informações de roteamento e acessibilidade com tipos de gateway de trânsito emparelhados. Ao contrário do que acontece com uma rota estática, o tráfego pode ser roteado por um caminho diferente com base nas condições da rede, como falhas de caminho ou congestionamento. O roteamento dinâmico também adiciona mais uma camada de segurança, pois é mais fácil redirecionar o tráfego no caso de uma violação ou invasão de rede.

> **Note**
>
> No momento, as tabelas de políticas de gateway de trânsito só são compatíveis com o Cloud WAN ao criar uma conexão de emparelhamento de gateway de trânsito. Ao criar uma conexão de emparelhamento, você pode associar essa tabela à conexão. Em seguida, a associação preenche a tabela automaticamente com as regras de política.
> Para obter mais informações sobre emparelhamento de conexões no Cloud WAN, consulte Emparelhamentos no Guia do usuário do AWS Cloud WAN.

Criar uma tabela de políticas de gateway de trânsito

Para criar uma tabela de políticas de gateway de trânsito usando o console

1. Abra o console do Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit gateway policy table (Tabela de políticas de gateway de trânsito).
3. Escolha Create transit gateway route table (Criar tabela de políticas de gateway de trânsito).
4. (Opcional) Em Name tag (Tag de nome), insira um nome para a política de gateway de trânsito. Isso cria uma tag cujo valor é o nome que você especifica.
5. Em Transit Gateway ID (ID do gateway de trânsito), selecione o gateway de trânsito para a tabela de políticas.
6. Escolha Create transit gateway route table (Criar tabela de políticas de gateway de trânsito).

Para criar uma tabela de políticas de gateway de trânsito usando o AWS CLI

Use o comando create-transit-gateway-policy-table.

Excluir uma tabela de políticas de gateway de trânsito

Exclua uma tabela de políticas de gateway de trânsito. Quando uma tabela é excluída, todas as regras de políticas incluídas nessa tabela são excluídas.

Para excluir uma tabela de políticas de gateway de trânsito usando o console

1. Abra o console do Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit gateway policy tables (Tabelas de políticas de gateway de trânsito).
3. Escolha a tabela de políticas de gateway de trânsito a ser excluída.
4. Escolha Actions (Ações) e, em seguida, escolha Delete policy table (Excluir tabela de políticas).
5. Confirme que você deseja excluir a tabela.

Para excluir uma tabela de políticas de gateway de trânsito usando o AWS CLI

Use o comando delete-transit-gateway-policy-table.

Multicast em gateways de trânsito

Multicast é um protocolo de comunicação usado para fornecer um único streaming de dados para vários computadores de recebimento simultaneamente. O Transit Gateway é compatível com o roteamento de tráfego multicast entre sub-redes de VPCs anexadas e serve como um roteador multicast para instâncias que enviam tráfego destinado a várias instâncias de recebimento.

Conceitos de multicast

Veja a seguir os principais conceitos de multicast:

- Domínio multicast: permite a segmentação de uma rede multicast em diferentes domínios e faz com que o gateway de trânsito atue como vários roteadores multicast. Você define a associação do domínio multicast no nível da sub-rede.
- Grupo multicast: identifica um grupo de anfitriões que enviarão e receberão o mesmo tráfego multicast. Um grupo de multicast é identificado por um endereço IP do grupo. A associação a grupos multicast é definida por interfaces de rede elástica individuais anexadas às instâncias do EC2.

- Internet Group Management Protocol (IGMP – Protocolo de gerenciamento de grupo da Internet): um protocolo de Internet que permite que anfitriões e roteadores gerenciem dinamicamente a associação de grupo multicast. Um domínio multicast IGMP contém hosts que usam o protocolo IGMP para entrar, sair e enviar mensagens. AWS suporta o protocolo IGMPv2 e os domínios multicast de associação a grupos IGMP e estáticos (baseados em API).

- Origem multicast: uma interface de rede elástica associada a uma instância do EC2 compatível que está configurada estaticamente para enviar tráfego multicast. Uma origem multicast aplica-se somente às configurações de origem estática.

  Um domínio multicast de origem estática contém hosts que não usam o protocolo IGMP para unir, sair e enviar mensagens. Você usa o AWS CLI para adicionar uma fonte e membros do grupo. A origem estaticamente adicionada envia o tráfego multicast e os membros recebem esse tráfego.
- Membro do grupo de multicast: uma interface de rede elástica associada a uma instância do EC2 compatível que recebe tráfego de multicast. Um grupo de multicast tem vários membros. Em uma configuração de associação de grupo de origem estática, os membros do grupo multicast podem somente receber o tráfego. Em uma configuração de grupo IGMP, os membros podem enviar e receber tráfego.

Considerações

- Para obter informações sobre regiões compatíveis, consulte Perguntas frequentes sobre o AWS Transit Gateway.
- É necessário criar um gateway de trânsito para ser compatível com o multicast.
- A associação ao grupo multicast é gerenciada usando o Amazon Virtual Private Cloud Console ou o AWS CLI, ou o IGMP.
- Uma sub-rede só pode estar em um domínio multicast.
- Se usar uma instância que não é do Nitro, você deverá desativar a verificação de Source/Dest (Origem/Destino). Para obter informações sobre como desabilitar a verificação, consulte Alterar a verificação da origem ou do destino no Guia do usuário do Amazon EC2 para instâncias do Linux.
- Uma instância que não é do Nitro não pode ser um remetente multicast.
- O roteamento multicast não é suportado por meio de VPN Site-to-Site AWS Direct Connect, anexos de emparelhamento ou anexos do Transit Gateway Connect.

- Um gateway de trânsito não é compatível com a fragmentação de pacotes de multicast. Pacotes multicast fragmentados são descartados. Para ter mais informações, consulte A unidade de transmissão máxima (MTU)..
- Na inicialização, um host IGMP envia mensagens JOIN IGMP múltiplas para se juntar a um grupo multicast (tipicamente 2 a 3 novas tentativas). No caso improvável que todas as mensagens JOIN IGMP se percam, o host não será parte do grupo multicast do gateway de trânsito. Em tal cenário, você precisará reacionar a mensagem JOIN IGMP do host usando métodos específicos da aplicação.
- Uma associação ao grupo começa com o recebimento da mensagem JOIN IGMPv2 pelo transit gateway e termina com o recebimento da mensagem LEAVE IGMPv2. O gateway de trânsito mantém o controle dos hosts que se uniram com sucesso ao grupo. Como um roteador multicast em nuvem, o transit gateway emite uma mensagem QUERY IGMPv2 para todos os membros a cada dois minutos. Cada membro envia uma mensagem JOIN IGMPv2 em resposta, que é como os membros renovam sua associação. Se um membro não responder a três consultas consecutivas, o transit gateway removerá essa associação de todos os grupos associados. No entanto, ele continua enviando consultas a esse membro por 12 horas antes de remover permanentemente o membro da to-be-queried lista. Uma mensagem LEAVE IGMPv2 explícita remove imediatamente e permanentemente o host de qualquer processamento multicast adicional.
- O gateway de trânsito mantém o controle dos hosts que se uniram com sucesso ao grupo. No caso de uma interrupção do transit gateway, o transit gateway continua enviando dados multicast ao host por sete minutos (420 segundos) após a última mensagem IGMP JOIN bem sucedida. O gateway de trânsito continua a enviar consultas de associação ao host por até 12 horas ou até receber uma mensagem LEAVE IGMP do host.
- O gateway de trânsito envia pacotes de consulta de associação a todos os membros IGMP de modo que possa seguir a associação do grupo multicast. O IP de origem desses pacotes de consulta IGMP é 0.0.0.0/32. O IP de destino é 224.0.0.1/32 e o protocolo é 2. Sua configuração de grupo de segurança nos hosts IGMP (instâncias) e qualquer configuração de ACLs nas sub-redes de host devem permitir essas mensagens de protocolo IGMP.
- Quando a origem e o destino multicast estão na mesma VPC, não é possível usar a referência do grupo de segurança para definir o grupo de segurança de destino para aceitar o tráfego do grupo de segurança de origem.
- Para grupos e fontes de multicast estáticos, os Amazon VPC Transit Gateways removem automaticamente grupos e fontes estáticos de ENIs que não existem mais. Isso é feito assumindo-se periodicamente a função vinculada ao serviço do Transit Gateway para descrever ENIs na conta.

- Somente o multicast estático suporta IPv6. O multicast dinâmico não.

Multicast com Windows Server

Você precisará executar etapas adicionais ao configurar o multicast para funcionar com gateways de trânsito no Windows Server 2019 ou 2022. Usando PowerShell, execute os seguintes comandos:

1. Altere o Windows Server para usar IGMPv2 em vez de IGMPv3 para a pilha TCP/IP:

   ```
   PS C:\> New-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Services
   \Tcpip\Parameters -Name IGMPVersion -PropertyType DWord -Value 3
   ```

   > **Note**
   >
   > `New-ItemProperty`é um índice de propriedades que especifica a versão IGMP. Como o IGMP v2 é a versão compatível com multicast, a propriedade `Value` deve ser. 3 Em vez de editar o registro do Windows, você pode executar o seguinte comando para definir a versão IGMP como 2. :
   > `Set-NetIPv4Protocol -IGMPVersion Version2`

2. O Firewall do Windows elimina a maior parte do tráfego UDP por padrão. Primeiro, você precisará verificar qual perfil de conexão está sendo usado para o multicast:

   ```
   PS C:\> Get-NetConnectionProfile | Select-Object NetworkCategory

   NetworkCategory
   ---------------
            Public
   ```

3. Atualize o perfil de conexão da etapa anterior para permitir o acesso às portas UDP necessárias:

   ```
   PS C:\> Set-NetFirewallProfile -Profile Public -Enabled False
   ```

4. Reinicialize a instância do EC2.
5. Teste sua aplicação multicast para garantir que o tráfego esteja fluindo conforme o esperado.

Roteamento multicast

Quando você permite o multicast em um gateway de trânsito, atua como um roteador de multicast. Quando você adiciona uma sub-rede a um domínio multicast, enviamos todo o tráfego multicast para o gateway de trânsito que está associado a esse domínio multicast.

Network ACLs

As regras de ACL da rede operam no nível da sub-rede. Elas se aplicam ao tráfego multicast, porque os gateways de trânsito residem fora da sub-rede. Para obter mais informações, consulte ACLs da rede no Guia do usuário da Amazon VPC

Para tráfego multicast de Internet Group Management Protocol (IGMP), você deve ter no mínimo as regras de entrada a seguir. O host remoto é aquele que envia o tráfego multicast.

Type	Protocolo	Origem	Descrição
Protocolo personalizado	IGMP (2)	0.0.0.0/32	Consulta IGMP
Protocolo UDP personalizado	UDP	Endereço IP do host remoto	Tráfego multicast de entrada

A seguir estão as regras mínimas de saída para IGMP.

Tipo	Protocolo	Destino	Descrição
Protocolo personalizado	IGMP (2)	224.0.0.2/32	IGMP sai
Protocolo personalizado	IGMP (2)	Endereço IP do grupo de multicast	IGMP entra
Protocolo UDP personalizado	UDP	Endereço IP do grupo de multicast	Tráfego multicast de saída

Grupos de segurança

As regras do grupo de segurança operam no nível da instância. Elas podem ser aplicadas ao tráfego multicast de entrada e de saída. O comportamento é o mesmo do tráfego de unicast. Para todas as

instâncias membro do grupo, você deve permitir o tráfego de entrada da origem do grupo. Para obter mais informações, consulte Grupos de segurança no Manual do usuário da Amazon VPC.

Você deve ter no mínimo as regras de entrada a seguir para o tráfego multicast do IGMP. O host remoto é aquele que envia o tráfego multicast. Não é possível especificar um grupo de segurança como a origem da regra de entrada UDP.

Type	Protocolo	Origem	Descrição
Protocolo personalizado	2	0.0.0.0/32	Consulta IGMP
Protocolo UDP personalizado	UDP	Endereço IP do host remoto	Tráfego multicast de entrada

Você deve ter no mínimo as regras de saída a seguir para o tráfego multicast do IGMP.

Type	Protocolo	Destino	Descrição
Protocolo personalizado	2	224.0.0.2/32	IGMP sai
Protocolo personalizado	2	Endereço IP do grupo de multicast	IGMP entra
Protocolo UDP personalizado	UDP	Endereço IP do grupo de multicast	Tráfego multicast de saída

Trabalhar com multicast

É possível configurar o multicast em gateways de trânsito usando o console ou a AWS CLI da Amazon VPC.

Antes de criar um domínio multicast, você precisa saber se seus hosts usam o protocolo IGMP para o tráfego multicast.

Conteúdo

- Gerenciar configurações de origem estáticas
- Gerenciar configurações de membros de grupo estático
- Gerenciar domínios multicast
- Gerenciar grupos multicast
- Trabalhar com domínios multicast compartilhados

Atributos de domínio multicast

A tabela a seguir detalha os atributos de domínio multicast. Você não pode habilitar ambos os atributos ao mesmo tempo.

Atributo	Descrição
`Igmpv2Support` (AWS CLI) Compatibilidade com IGMPv2 (console)	Este atributo determina como os membros do grupo se unem ou saem de um grupo multicast. Quando esse atributo estiver desabilitado, é necessário adicionar manualmente os membros do grupo ao domínio. Habilite esse atributo quando pelo menos um membro usar o protocolo IGMP. Os membros se juntam ao grupo multicast de uma das seguintes maneiras: • Os membros compatíveis com IGMP usam as mensagens `JOIN` e `LEAVE`. • Os membros que não são compatíveis com IGMP devem ser adicionados ou removidos do grupo usando o console ou a AWS CLI da Amazon VPC. Se registrar membros do grupo multicast, também é necessári o cancelar o registro deles. O gateway de trânsito ignora uma mensagem `LEAVE` IGMP enviada por um membro do grupo adicionado manualmente.
`StaticSourcesSupport` (AWS CLI)	Este atributo determina se há origens multicast estáticas para o grupo.

Atributo	Descrição
Compatibilidade com fontes estáticas (console)	Quando esse atributo está habilitado, você deve adicionar fontes para um domínio multicast usando register-transit-gateway-multicast-group-sources. Somente origens multicast podem enviar tráfego multicast. Quando esse atributo é desabilitado, não há fontes multicast designadas. Todas as instâncias que estão nas sub-redes associadas ao domínio multicast podem enviar tráfego multicast, e os membros do grupo recebem esse tráfego.

Gerenciar configurações IGMP

Quando você tem pelo menos um host que usa o protocolo IGMP para tráfego multicast, a AWS cria automaticamente o grupo multicast quando recebe uma mensagem `JOIN` IGMP de uma instância e, em seguida, adiciona a instância como membro nesse grupo. Você também pode adicionar estaticamente hosts não IGMP como membros de um grupo usando o. AWS CLI Todas as instâncias que estão nas sub-redes associadas ao domínio multicast podem enviar tráfego, e os membros do grupo recebem o tráfego multicast.

Siga as etapas a seguir para concluir essa configuração:

1. Crie uma VPC. Para obter mais informações sobre como criar VPCs, consulte Criação de uma VPC no Guia do usuário da Amazon VPC.
2. Crie uma sub-rede na VPC. Para obter mais informações sobre como criar sub-redes, consulte Criação de uma sub-rede na VPC no Guia do usuário da Amazon VPC.
3. Crie um gateway de trânsito configurado para o tráfego multicast. Para ter mais informações, consulte the section called “Criar um gateway de trânsito”.
4. Crie um anexo da VPC Para ter mais informações, consulte the section called “Criar um anexo do gateway de trânsito para uma VPC”.
5. Crie um domínio multicast configurado para ser compatível com IGMP. Para ter mais informações, consulte the section called “Criar um domínio multicast IGMP”.

   Use as seguintes configurações:

   - Habilite IGMPv2 support (Compatibilidade com IGMPv2).

- Desabilite Static sources support (Compatibilidade com fontes estáticas).

6. Crie uma associação entre sub-redes no anexo VPC do gateway de trânsito e no domínio multicast. Para obter mais informações, consulte the section called “Associar anexos e sub-redes VPC a um domínio multicast”.
7. A versão padrão do IGMP para EC2 é IGMPv3. Você precisa mudar a versão para todos os membros do grupo IGMP. Você pode executar o seguinte comando:

   ```
   sudo sysctl net.ipv4.conf.eth0.force_igmp_version=2
   ```

8. Adicione os membros que não usam o protocolo IGMP ao grupo multicast. Para ter mais informações, consulte the section called “Registrar membros com um grupo multicast”.

Gerenciar configurações de origem estáticas

Nesta configuração, você precisa adicionar estaticamente origens multicast em um grupo. Os hosts não usam o protocolo IGMP para se juntar ou sair de grupos multicast. Você precisa adicionar estaticamente os membros do grupo que recebem o tráfego multicast.

Siga as etapas a seguir para concluir essa configuração:

1. Crie uma VPC. Para obter mais informações sobre como criar VPCs, consulte Criação de uma VPC no Guia do usuário da Amazon VPC.
2. Crie uma sub-rede na VPC. Para obter mais informações sobre como criar sub-redes, consulte Criação de uma sub-rede na VPC no Guia do usuário da Amazon VPC.
3. Crie um gateway de trânsito configurado para o tráfego multicast. Para ter mais informações, consulte the section called “Criar um gateway de trânsito”.
4. Crie um anexo da VPC Para ter mais informações, consulte the section called “Criar um anexo do gateway de trânsito para uma VPC”.
5. Crie um domínio multicast configurado para não ser compatível com IGMP e para ser compatível com a adição de origens estaticamente. Para ter mais informações, consulte the section called “Criar um domínio multicast de origem estática”.

   Use as seguintes configurações:

   - Desabilite IGMPv2 support (Compatibilidade com IGMPv2).
   - Para adicionar fontes manualmente, habilite Static sources support (Compatibilidade com fontes estáticas).

As fontes são os únicos recursos que podem enviar o tráfego multicast quando o atributo está habilitado. Caso contrário, todas as instâncias que estão nas sub-redes associadas ao domínio multicast podem enviar tráfego multicast, e os membros do grupo recebem esse tráfego.

6. Crie uma associação entre sub-redes no anexo VPC do gateway de trânsito e no domínio multicast. Para mais informações, consulte the section called “Associar anexos e sub-redes VPC a um domínio multicast”.
7. Se habilitar Static sources support (Compatibilidade com fontes estáticas), adicione a fonte ao grupo multicast. Para ter mais informações, consulte the section called “Registrar origens com um grupo multicast”.
8. Adicione os membros ao grupo multicast. Para ter mais informações, consulte the section called “Registrar membros com um grupo multicast”.

Gerenciar configurações de membros de grupo estático

Nesta configuração, você precisa adicionar estaticamente membros multicast a um grupo. Os hosts não podem usar o protocolo IGMP para se unir ou deixar grupos multicast. Todas as instâncias que estão nas sub-redes associadas ao domínio multicast podem enviar tráfego multicast, e os membros do grupo recebem esse tráfego.

Siga as etapas a seguir para concluir essa configuração:

1. Crie uma VPC. Para obter mais informações sobre como criar VPCs, consulte Criação de uma VPC no Guia do usuário da Amazon VPC.
2. Crie uma sub-rede na VPC. Para obter mais informações sobre como criar sub-redes, consulte Criação de uma sub-rede na VPC no Guia do usuário da Amazon VPC.
3. Crie um gateway de trânsito configurado para o tráfego multicast. Para ter mais informações, consulte the section called “Criar um gateway de trânsito”.
4. Crie um anexo da VPC Para ter mais informações, consulte the section called “Criar um anexo do gateway de trânsito para uma VPC”.
5. Crie um domínio multicast configurado para não ser compatível com IGMP e para ser compatível com a adição de origens estaticamente. Para ter mais informações, consulte the section called “Criar um domínio multicast de origem estática”.

   Use as seguintes configurações:

- Desabilite IGMPv2 support (Compatibilidade com IGMPv2).
- Desabilite Static sources support (Compatibilidade com fontes estáticas).

6. Crie uma associação entre sub-redes no anexo VPC do gateway de trânsito e no domínio multicast. Para obter mais informações, consulte the section called “Associar anexos e sub-redes VPC a um domínio multicast”.
7. Adicione os membros ao grupo multicast. Para ter mais informações, consulte the section called “Registrar membros com um grupo multicast”.

Gerenciar domínios multicast

Para começar a usar a multicast com um gateway de trânsito, crie um domínio multicast e associe sub-redes ao domínio.

Tópicos

- Criar um domínio multicast IGMP
- Criar um domínio multicast de origem estática
- Associar anexos e sub-redes VPC a um domínio multicast
- Visualizar suas associações de domínio multicast
- Desassociar sub-redes de um domínio multicast
- Adicionar tags a um domínio multicast
- Excluir um domínio multicast

Criar um domínio multicast IGMP

Se você ainda não fez isso, revise os atributos de domínio multicast disponíveis. Para ter mais informações, consulte the section called “Trabalhar com multicast”.

Console

Para criar um domínio multicast do IGMP usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Multicast (Multicast do gateway de trânsito).

3. Escolha Create transit gateway multicast domain (Criar domínio de multicast do gateway de trânsito).
4. Em Name tag (Etiqueta de nome), insira um nome para o domínio.
5. Em Transit gateway ID (ID do gateway de trânsito), selecione o gateway de trânsito que processa o tráfego multicast.
6. Para compatibilidade com IGMPv2, marque a caixa de seleção.
7. Para compatibilidade com origens estáticas, desmarque a caixa de seleção.
8. Para aceitar automaticamente associações de sub-rede entre contas para este domínio multicast, selecione Aceitar automaticamente associações compartilhadas.
9. Escolha Create transit gateway multicast domain (Criar domínio de multicast do gateway de trânsito).

Command line

Para criar um domínio multicast IGMP usando o AWS CLI

Use o comando create-transit-gateway-multicast-domain.

```
aws ec2 create-transit-gateway-multicast-domain --transit-gateway-
id tgw-0xexampleid12345 --options StaticSourcesSupport=disable,Igmpv2Support=enable
```

Criar um domínio multicast de origem estática

Se você ainda não fez isso, revise os atributos de domínio multicast disponíveis. Para ter mais informações, consulte the section called “Trabalhar com multicast”.

Console

Como criar um domínio multicast estático usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Multicast (Multicast do gateway de trânsito).
3. Escolha Create transit gateway multicast domain (Criar domínio de multicast do gateway de trânsito).
4. Em Name tag, insira um nome para identificar o domínio.

5. Em Transit gateway ID (ID do gateway de trânsito), selecione o gateway de trânsito que processa o tráfego multicast.
6. Para Compatibilidade com IGMPv2, desmarque a caixa de seleção.
7. Em Static sources support (Compatibilidade com fontes estáticas), marque a caixa de seleção.
8. Para aceitar automaticamente associações de sub-rede entre contas para este domínio multicast, selecione Aceitar automaticamente associações compartilhadas.
9. Escolha Create transit gateway multicast domain (Criar domínio de multicast do gateway de trânsito).

Command line

Para criar um domínio multicast estático usando o AWS CLI

Use o comando create-transit-gateway-multicast-domain.

```
aws ec2 create-transit-gateway-multicast-domain --transit-gateway-
id tgw-0xexampleid12345 --options StaticSourcesSupport=enable,Igmpv2Support=disable
```

Associar anexos e sub-redes VPC a um domínio multicast

Use o procedimento a seguir para associar um anexo da VPC a um domínio de multicast. Ao criar uma associação, você pode selecionar as sub-redes para incluir o domínio de multicast.

Antes de começar, é necessário criar um anexo da VPC no gateway de trânsito. Para ter mais informações, consulte Anexos de gateway de trânsito a uma VPC.

Console

Como associar anexos da VPC a um domínio multicast usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Multicast (Multicast do gateway de trânsito).
3. Selecione o domínio multicast e depois Actions, Create association.
4. Em Choose attachment to associate (Escolha o anexo para associar), selecione o anexo do gateway de trânsito.

5. Em Choose subnets to associate, selecione as sub-redes nas quais você quer incluir o domínio multicast.
6. Escolha Create association (Criar associação).

Command line

Para associar anexos de VPC a um domínio multicast usando o AWS CLI

Use o comando associate-transit-gateway-multicast-domain.

Visualizar suas associações de domínio multicast

É possível visualizar seus domínios multicast para verificar se eles estão disponíveis e se eles contêm as sub-redes e anexos apropriados.

Console

Para visualizar um domínio multicast usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Multicast (Multicast do gateway de trânsito).
3. Selecione o domínio multicast.
4. Escolha a guia Associations (Associações).

Command line

Para visualizar um domínio multicast usando o AWS CLI

Use o comando describe-transit-gateway-multicast-domains.

Desassociar sub-redes de um domínio multicast

Use o procedimento a seguir para desassociar sub-redes de um domínio multicast.

Console

Como desassociar sub-redes usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Multicast (Multicast do gateway de trânsito).
3. Selecione o domínio multicast.
4. Escolha a guia Associations (Associações).
5. Selecione a sub-rede e escolha Actions (Ações), Delete association (Excluir associação).

Command line

Para desassociar sub-redes usando o AWS CLI

Use o comando disassociate-transit-gateway-multicast-domain.

Adicionar tags a um domínio multicast

Adicione tags aos seus recursos para ajudar a organizá-los e identificá-los, por exemplo, por propósito, proprietário ou ambiente. É possível adicionar várias tags a cada domínio multicast. As chaves de tag devem ser exclusivas para cada domínio multicast. Se você adicionar uma tag com uma chave que já está associada ao domínio multicast, isso atualizará o valor dessa tag. Para obter mais informações, consulte Marcar recursos do Amazon EC2.

Console

Para adicionar etiquetas a um domínio multicast usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Multicast (Multicast do gateway de trânsito).
3. Selecione o domínio multicast.
4. Escolha Actions (Ações), Manage tags (Gerenciar tags).
5. Para cada etiqueta, escolha Add new tag (Adicionar nova etiqueta) e insira uma Key (Chave) e Value (Valor) para a etiqueta.

6. Escolha Salvar.

Command line

Para adicionar tags a um domínio multicast usando o AWS CLI

Use o comando create-tags.

Excluir um domínio multicast

Use o procedimento a seguir para excluir um domínio multicast.

Console

Para excluir um domínio multicast usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Multicast (Multicast do gateway de trânsito).
3. Selecione o domínio multicast e, em seguida, Actions, Delete multicast domain.
4. Quando a confirmação for solicitada, insira **`delete`** e escolha Excluir.

Command line

Para excluir um domínio multicast usando o AWS CLI

Use o comando delete-transit-gateway-multicast-domain.

Gerenciar grupos multicast

Tópicos

- Registrar origens com um grupo multicast
- Registrar membros com um grupo multicast
- Cancelar o registro de origens de um grupo multicast
- Cancelar o registro de membros de um grupo multicast
- Visualizar os grupos multicast

Registrar origens com um grupo multicast

> **Note**
>
> Este procedimento só é necessário quando você tiver definido o atributo compatibilidade com origens estáticas para habilitar.

Use o procedimento a seguir para registrar fontes com um grupo de multicast. A origem é a interface de rede que envia um tráfego de multicast.

Antes de adicionar uma fonte, são necessárias as informações a seguir:

- ID do domínio multicast
- Os IDs das interfaces de rede das origens
- Endereço IP do grupo de multicast

Console

Como registrar as fontes usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Multicast (Multicast do gateway de trânsito).
3. Selecione o domínio multicast e, em seguida, Actions, Add group sources.
4. Em Group IP address (Endereço IP do grupo), insira o bloco CIDR IPv4 ou o bloco CIDR IPv6 para atribuir ao domínio de multicast.
5. Em Choose network interfaces (Selecionar interfaces de rede), selecione as interfaces da rede dos remetentes multicast.
6. Escolha Adicionar origens.

Command line

Para registrar fontes usando o AWS CLI

Use o comando register-transit-gateway-multicast-group-sources.

Registrar membros com um grupo multicast

Use o procedimento a seguir para registrar membros do grupo com um grupo de multicast.

Antes de adicionar membros, são necessárias as informações a seguir:

- ID do domínio multicast
- IDs das interfaces de rede dos membros do grupo
- Endereço IP do grupo de multicast

Console

Como registrar membros usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Multicast (Multicast do gateway de trânsito).
3. Selecione o domínio multicast e, em seguida, Actions, Add group members.
4. Em Group IP address (Endereço IP do grupo), insira o bloco CIDR IPv4 ou o bloco CIDR IPv6 para atribuir ao domínio de multicast.
5. Em Choose network interfaces (Selecionar interfaces de rede), selecione as interfaces de rede dos receptores de multicast.
6. Escolha Add members (Adicionar membros).

Command line

Para registrar membros usando o AWS CLI

Use o comando register-transit-gateway-multicast-group-members.

Cancelar o registro de origens de um grupo multicast

Você não precisa seguir este procedimento a menos que você adicionou manualmente uma origem ao grupo multicast.

Console

Como remover uma origem usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Multicast (Multicast do gateway de trânsito).
3. Selecione o domínio multicast.
4. Escolha a guia Groups.
5. Selecione as origens e escolha Remove source (Remover origem).

Command line

Para remover uma fonte usando o AWS CLI

Use o comando deregister-transit-gateway-multicast-group-sources.

Cancelar o registro de membros de um grupo multicast

Não é necessário seguir este procedimento, a menos que tenha adicionado manualmente um membro ao grupo multicast.

Console

Como cancelar o registro de membros usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Multicast (Multicast do gateway de trânsito).
3. Selecione o domínio multicast.
4. Escolha a guia Groups.
5. Selecione os membros e escolha Remove member (Remover membro).

Command line

Para cancelar o registro de membros usando o AWS CLI

Use o comando deregister-transit-gateway-multicast-group-members.

Visualizar os grupos multicast

Você pode ver informações sobre seus grupos multicast para verificar se os membros foram descobertos usando o protocolo IGMPv2. O tipo de membro (no console) ou `MemberType` (no AWS CLI) exibe IGMP quando são AWS descobertos membros com o protocolo.

Console

Como visualizar grupos de multicast usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Multicast (Multicast do gateway de trânsito).
3. Selecione o domínio multicast.
4. Escolha a guia Groups.

Command line

Para visualizar grupos multicast usando o AWS CLI

Use o comando search-transit-gateway-multicast-groups.

O exemplo a seguir mostra que o protocolo IGMP descobriu membros do grupo multicast.

```
aws ec2 search-transit-gateway-multicast-groups --transit-gateway-multicast-
domain tgw-mcast-domain-000fb24d04EXAMPLE
{
    "MulticastGroups": [
        {
            "GroupIpAddress": "224.0.1.0",
            "TransitGatewayAttachmentId": "tgw-attach-0372e72386EXAMPLE",
            "SubnetId": "subnet-0187aff814EXAMPLE",
            "ResourceId": "vpc-0065acced4EXAMPLE",
            "ResourceType": "vpc",
            "NetworkInterfaceId": "eni-03847706f6EXAMPLE",
            "MemberType": "igmp"
        }
    ]
```

```
}
```

Trabalhar com domínios multicast compartilhados

Com o compartilhamento de domínio multicast, os proprietários de domínio multicast podem compartilhar o domínio com outras contas da AWS dentro da organização ou entre organizações no AWS Organizations. Como proprietário do domínio multicast, você pode criar e gerenciar esse domínio centralmente. Os consumidores podem executar as seguintes operações em um domínio multicast compartilhado:

- Registrar e cancelar o registro de membros do grupo ou origens de grupo no domínio multicast
- Associar uma sub-rede ao domínio multicast e desassociar sub-redes desse domínio

Um proprietário de domínio multicast pode compartilhar um domínio multicast com:

- Contas da AWS dentro da organização ou entre organizações no AWS Organizations
- Uma unidade organizacional dentro da organização no AWS Organizations
- Toda a organização no AWS Organizations
- Contas da AWS externas ao AWS Organizations.

  Para compartilhar um domínio multicast com uma conta da AWS externa ao Organization, você deve criar um compartilhamento de recursos usando o AWS Resource Access Manager e, em seguida, escolher Permitir compartilhamento com qualquer pessoa ao selecionar as entidades principais com as quais o domínio multicast será compartilhado. Para obter mais informações sobre como criar um compartilhamento de recursos, consulte Como criar um compartilhamento de recursos no AWS RAM no Guia do usuário do AWS RAM.

Índice

- Permissões do domínio multicast compartilhado
- Faturamento e medição
- Cotas

Pré-requisitos para compartilhar um domínio multicast

- Para compartilhar um domínio multicast, você deve tê-lo na conta da AWS. Não é possível compartilhar um domínio multicast que tenha sido compartilhado com você.
- Para compartilhar um domínio multicast com a sua organização ou com uma unidade organizacional no AWS Organizations, é necessário habilitar o compartilhamento com o AWS Organizations. Para obter mais informações, consulte Habilitar o compartilhamento com o AWS Organizations no Guia do usuário do AWS RAM.

Serviços relacionados

O compartilhamento de domínio multicast integra-se ao AWS Resource Access Manager (AWS RAM). O AWS RAM é um serviço que permite compartilhar seus recursos da AWS com qualquer conta da AWS ou por meio do AWS Organizations. Com o AWS RAM, você compartilha recursos que possui criando um compartilhamento de recursos. Um compartilhamento de recursos especifica os recursos a serem compartilhados, e os consumidores com os quais compartilhá-los. Os consumidores podem ser contas individuais da AWS, unidades organizacionais ou toda uma organização do AWS Organizations.

Para obter mais informações sobre o AWS RAM, consulte o Guia do usuário do AWS RAM.

Compartilhamento entre zonas de disponibilidade

Para garantir a distribuição de recursos entre as zonas de disponibilidade de uma região, mapeamos as zonas de disponibilidade de forma independente para os nomes de cada conta. Isso pode resultar em diferenças na nomenclatura de zonas de disponibilidade entre contas. Por exemplo, a zona de disponibilidade `us-east-1a` de sua conta da AWS pode não ter o mesmo local que a `us-east-1a` de outra conta da AWS.

Para identificar o local dos domínios multicast relativos às contas, use o Availability Zone ID (AZ ID – ID da zona de disponibilidade). O AZ ID é um identificador exclusivo e consistente de uma zona de disponibilidade em todas as contas da AWS. Por exemplo, `use1-az1` é um ID de AZ da região `us-east-1` e é o mesmo local em cada conta da AWS.

Para visualizar os IDs de AZs das zonas de disponibilidade em sua conta

1. Abra o console do AWS RAM em https://console.aws.amazon.com/ram.
2. Os IDs de AZs da região atual são exibidos no painel Your AZ ID (Seu ID de AZ) no lado direito da tela.

Compartilhar um domínio multicast

Quando um proprietário compartilha um domínio multicast com um consumidor, o consumidor pode fazer o seguinte:

- Registrar e cancelar o registro de membros do grupo ou origens do grupo
- Associar e desassociar sub-redes

Para compartilhar um domínio multicast, você deve adicioná-lo a um compartilhamento de recursos. Um compartilhamento de recursos é um recurso do AWS RAM que permite que você compartilhe seus recursos entre contas da AWS. Um compartilhamento de recursos especifica os recursos a serem compartilhados, e os consumidores com os quais compartilhá-los. Quando você compartilha um domínio multicast usando o Amazon Virtual Private Cloud Console, você o adiciona a um compartilhamento de recursos existente. Para adicionar o domínio multicast a um novo compartilhamento de recursos, primeiro crie o compartilhamento de recursos usando o console do AWS RAM.

Se você fizer parte de uma organização no AWS Organizations e o compartilhamento estiver habilitado na organização, os consumidores da organização receberão acesso automaticamente ao domínio multicast compartilhado. Caso contrário, os consumidores receberão um convite para integrar o compartilhamento de recursos e recebem acesso ao domínio multicast depois de aceitar o convite.

Você pode compartilhar um domínio multicast seu usando o console da *Amazon Virtual Private Cloud Console, o console do AWS RAM ou a AWS CLI.

Para compartilhar um domínio multicast que você tem usando a *Amazon Virtual Private Cloud Console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Multicast Domains.
3. Selecione o domínio multicast e, em seguida, Actions, Delete multicast domain.

4. Selecione seu compartilhamento de recurso e escolha Share multicast domain.

Para compartilhar um domínio multicast que você tem usando o console do AWS RAM

Consulte Criar um compartilhamento de recursos no Manual do usuário do AWS RAM.

Para compartilhar um domínio multicast de sua propriedade usando a AWS CLI

Use o comando create-resource-share.

Cancelar o compartilhamento de um domínio multicast compartilhado

Quando o compartilhamento de um domínio multicast compartilhado é cancelado, o seguinte acontece com os recursos de domínio multicast do consumidor:

- As sub-redes de consumo são desassociadas do domínio multicast. As sub-redes permanecem na conta do consumidor.
- Os membros do grupo e os origens do grupo de consumidores são desassociados do domínio multicast e, em seguida, excluídos da conta de consumidor.

Para cancelar o compartilhamento de um domínio multicast, você deve removê-lo do compartilhamento de recursos. Isso pode ser feito no console do AWS RAM ou na AWS CLI.

Para cancelar o compartilhamento de um domínio multicast de sua propriedade, é necessário removê-lo do compartilhamento de recursos. É possível fazer isso usando o *Amazon Virtual Private Cloud Console, o console da AWS RAM ou a AWS CLI.

Para cancelar o compartilhamento de um domínio multicast compartilhado que você tem usando a *Amazon Virtual Private Cloud Console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Multicast Domains.
3. Selecione seu domínio multicast e, em seguida, Actions, Stop sharing.

Para cancelar o compartilhamento de um domínio multicast compartilhado que você tem usando o console do AWS RAM

Consulte Atualização de um compartilhamento de recursos no Guia do usuário do AWS RAM.

Para cancelar o compartilhamento de um domínio multicast compartilhado de sua propriedade usando a AWS CLI

Use o comando disassociate-resource-share.

Identificar um domínio multicast compartilhado

Os proprietários e os consumidores podem identificar domínios multicast compartilhados usando o *Amazon Virtual Private Cloud Console e a AWS CLI

Para identificar um domínio multicast compartilhado usando a *Amazon Virtual Private Cloud Console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Multicast Domains.
3. Selecione seu domínio multicast.
4. Na página Detalhes do domínio multicast do trânsito, veja o ID do proprietário para identificar o ID da conta da AWS do domínio multicast.

Para identificar um domínio multicast compartilhado usando a AWS CLI

Use o comando describe-transit-gateway-multicast-domains. O comando retorna os domínios multicast que você tem e domínios multicast que são compartilhados com você. `OwnerId` mostra o ID da conta da AWS do proprietário do domínio multicast.

Permissões do domínio multicast compartilhado

Permissões para proprietários

Os proprietários são responsáveis por gerenciar o domínio multicast, assim como os membros e anexos que eles registram ou associam ao domínio. Os proprietários podem alterar ou revogar o acesso compartilhado a qualquer momento. Eles podem usar o AWS Organizations para visualizar, modificar e excluir recursos criados pelos consumidores em domínios multicast compartilhados.

Permissões para consumidores

Os consumidores podem executar as seguintes operações em domínios multicast compartilhados da mesma maneira que eles fariam em domínios multicast que eles criaram:

- Registrar e cancelar o registro de membros do grupo ou origens de grupo no domínio multicast
- Associar uma sub-rede ao domínio multicast e desassociar sub-redes desse domínio

Os consumidores são responsáveis por gerenciar os recursos que eles criam no domínio multicast compartilhado.

Os clientes não podem visualizar ou modificar recursos pertencentes a outros consumidores ou a outro proprietário do domínio multicast e não podem modificar domínios multicast compartilhados com eles.

Faturamento e medição

Proprietários e consumidores não recebem cobranças adicionais para compartilhar domínios multicast.

Cotas

Um domínio multicast compartilhado conta para as cotas de domínio multicast do proprietário e do consumidor.

Considerações sobre compartilhamento do gateway de trânsito

É possível usar o AWS Resource Access Manager (RAM) para compartilhar um gateway de trânsito para anexos da VPC em contas ou em toda a organização no AWS Organizations. A RAM deve estar habilitada e os recursos compartilhados com uma organização. Para obter mais informações, consulte Habilitar o compartilhamento de recursos com o AWS Organizations no Manual do usuário do AWS RAM.

Considere o seguinte quando quiser compartilhar um gateway de trânsito.

- Um anexo do AWS Site-to-Site VPN deve ser criado na mesma conta da AWS que possui o gateway de trânsito.
- O anexo a um gateway do Direct Connect usa uma associação do gateway de trânsito e pode estar na mesma conta da AWS que o gateway do Direct Connect, ou em uma conta diferente.

Por padrão, os usuários não têm permissão para criar ou modificar recursos do AWS RAM. Para permitir que os usuários criem ou alterem recursos e realizem tarefas, você deve criar políticas do IAM que concedam permissão para usar os recursos e as ações de API específicos necessários. Em seguida, anexe essas políticas aos usuários ou grupos do IAM que exigem essas permissões.

O proprietário do recurso pode realizar as seguintes operações:

- Criar o compartilhamento de um recurso.
- Atualizar o compartilhamento de um recurso.
- Exibir o compartilhamento de um recurso.
- Visualizar os recursos compartilhados por sua conta em todos os compartilhamentos de recursos.
- Visualizar os principais com os quais você está compartilhando seus recursos em todos os compartilhamentos de recursos. Visualizar os principais com os quais você está compartilhando permite determinar quem tem acesso aos seus recursos compartilhados.
- Excluir o compartilhamento de um recurso.
- Execute todas as APIs de gateway de trânsito, anexos de gateway de trânsito e tabelas de rotas de gateway de trânsito.

Você pode executar as operações a seguir nos recursos compartilhados contigo:

- Aceitar ou rejeitar o convite de um compartilhamento de recursos.
- Exibir o compartilhamento de um recurso.
- Visualizar os recursos compartilhados que você pode acessar.
- Visualizar uma lista de todos os principais que estão compartilhando recursos com você. É possível ver quais recursos e compartilhamentos de recursos foram compartilhados com você.
- Pode executar a API do `DescribeTransitGateways`.
- Execute as APIs que criam e descrevem anexos, como `CreateTransitGatewayVpcAttachment` e `DescribeTransitGatewayVpcAttachments`, nas VPCs.
- Deixar o compartilhamento de um recurso.

Quando um gateway de trânsito é compartilhado com você, não é possível criar, modificar nem excluir as tabelas de rotas do gateway de trânsito ou as propagações e associações da tabela de rotas do gateway de trânsito.

Quando você cria um gateway de trânsito, ele é criado na zona de disponibilidade que é mapeada para sua conta e é independente de outras contas. Quando o gateway de trânsito e as entidades de anexo estiverem em contas diferentes, use o ID da zona de disponibilidade para identificar a zona de disponibilidade de maneira exclusiva e consistente. Por exemplo, use1-az1 é um ID de zona de disponibilidade para a região us-east-1 e mapeia para o mesmo local em todas as contas da AWS.

Cancelar o compartilhamento de um gateway de trânsito

Quando o proprietário descompartilhar o gateway de trânsito, serão aplicadas as seguintes regras:

- O anexo do gateway de trânsito permanece funcional.
- A conta compartilhada não pode descrever o gateway de trânsito.
- O proprietário do gateway de trânsito e o proprietário do compartilhamento podem excluir o anexo do gateway de trânsito.

Quando um gateway de trânsito não é compartilhado com outro conta da AWS, ou se a conta da AWS com a qual o gateway de trânsito é compartilhado é removido da organização, o próprio gateway de trânsito não será afetado.

Sub-redes compartilhadas

O proprietário de VPC pode anexar um gateway de trânsito a uma sub-rede de VPC compartilhada. Os participantes não podem. O tráfego dos recursos do participante pode usar os anexos dependendo das rotas configuradas na sub-rede da VPC compartilhada pelo proprietário da VPC.

Para obter informações, consulte Compartilhar sua VPC com outras contas no Guia do usuário da Amazon VPC.

Registrar tráfego de rede usando logs de fluxo do Transit Gateway

Os logs de fluxo de gateway de trânsito são um recurso que permite capturar informações sobre o tráfego IP de entrada e saída nos gateways de trânsito. Os dados do log de fluxo podem ser publicados no Amazon CloudWatch Logs, no Amazon S3 ou no Firehose. Após criar um log de fluxo, será possível recuperar e visualizar seus dados no destino selecionado. Os dados do log de fluxo são coletados fora do caminho do tráfego de rede e, portanto, não afetam a throughput nem a latência da rede. É possível criar ou excluir logs de fluxo sem qualquer risco de impacto na pérformance da rede. Os logs de fluxo de gateway de trânsito capturam informações relacionadas exclusivamente aos gateways de trânsito, descritas em the section called “Registros de log de fluxo de gateway de trânsito”. Se você quiser capturar informações sobre o tráfego IP proveniente e direcionado às interfaces de rede em suas VPCs, use os logs de fluxo de VPC. Consulte Como registrar tráfego IP em log com logs de fluxo da VPC no Guia do usuário do Amazon VPC.

> **Note**
>
> Para criar um log de fluxo de gateway de trânsito, você deve ser o proprietário do gateway de trânsito ou, se você não for o proprietário do gateway de trânsito, o proprietário do gateway de trânsito deve conceder permissão ao seu usuário.

Os dados de log de fluxo para um gateway de trânsito monitorado são registrados como registros de log de fluxo, que são eventos de logs que consistem em campos que descrevem o fluxo de tráfego. Para ter mais informações, consulte Registros de log de fluxo de gateway de trânsito.

Para criar um log de fluxo, especifique:

- O recurso para o qual criar o log de fluxo
- Os destinos em que você quer publicar os dados de log de fluxo

Depois que você criar um log de fluxo, pode demorar alguns minutos para começar a coletar e publicar dados nos destinos selecionados. Os logs de fluxo não capturam fluxos de logs em tempo real para as interfaces de rede. Para ter mais informações, consulte Criar um log de fluxo.

É possível aplicar tags aos logs de fluxo. Cada tag consiste de uma chave e um valor opcional, ambos definidos por você. As tags podem ajudar você a organizar seus logs de fluxo. Por exemplo, por finalidade ou proprietário.

Caso não precise mais de um log de fluxo, você pode excluí-lo. A exclusão de um log de fluxo desativa o serviço de log de fluxo para o recurso, e nenhum novo registro de log de fluxo é criado ou publicado no CloudWatch Logs ou no Amazon S3. A exclusão do registro de fluxo não exclui nenhum registro ou fluxo de log existente (para CloudWatch Logs) ou objetos de arquivo de log (para Amazon S3) para um gateway de trânsito. Para excluir um stream de registros existente, use o console de CloudWatch registros. Para excluir objetos de arquivo de log existentes, use o console do Amazon S3. Depois que você exclui um log de fluxo, pode levar vários minutos para a coleta de dados se encerrar. Para ter mais informações, consulte Excluir um log de fluxo.

Conteúdo

Registros de log de fluxo de gateway de trânsito

Um registro de log de fluxo representa um fluxo de rede no gateway de trânsito. Cada registro é uma string com campos separados por espaços. Um registro inclui valores para os diferentes componentes do fluxo de tráfego como, por exemplo, a origem, o destino e o protocolo.

Ao criar um log de fluxo, é possível usar o formato padrão do registro de log de fluxo ou especificar um formato personalizado.

Conteúdo

Formato padrão

Com o formato padrão, os registros de log de fluxo incluem todos os campos da versão 2 à versão 6, na ordem mostrada na tabela de campos disponíveis. Não é possível personalizar ou alterar o formato padrão. Para capturar campos adicionais disponíveis ou um subconjunto de campos diferente, especifique um formato personalizado em vez disso.

Formato personalizado

Com um formato personalizado, você especifica quais campos estão incluídos nos registros de log de fluxo e em qual ordem. Isso permite que você crie logs de fluxo específicos para as suas necessidades e omita os campos que não forem relevantes. Usar um formato personalizado pode diminuir a necessidade de processos separados para extrair informações específicas dos logs de fluxo publicados. É possível especificar qualquer quantidade de campos disponíveis do log de fluxo, mas você deve especificar pelo menos um.

Campos disponíveis

A tabela a seguir descreve todos os campos disponíveis para um registro de log de fluxo de gateway de trânsito. A coluna Versão indica em qual versão o campo foi introduzido.

Ao publicar dados de log de fluxo no Amazon S3, o tipo de dados para os campos dependerá do formato do log de fluxo. Se o formato estiver como texto sem formatação, todos os campos serão do tipo STRING. Se o formato for Parquet, consulte a tabela para os tipos de dados de campo.

Se um campo não for aplicável ou não puder ser computado para um registro específico, o registro exibirá o símbolo '-' para essa entrada. Os campos de metadados que não vêm diretamente do cabeçalho do pacote são aproximações e seus valores podem estar ausentes ou imprecisos.

Campo	Descrição	Version (Versão)
version	Indica a versão na qual o campo foi introduzido. O formato padrão inclui todos os campos da versão 2, na mesma ordem em que aparecem na tabela. Tipo de dados em Parquet: INT_32	2
resource-type	O tipo de recurso no qual a assinatura é criada. Pode ser TransitGateway ou TransitGatewayAttachment.	6

Campo	Descrição	Version (Versão)
	Tipo de dados em Parquet: STRING	
account-id	O Conta da AWS ID do proprietário do gateway de trânsito de origem. Tipo de dados em Parquet: STRING	2
tgw-id	O ID do gateway de trânsito para o qual o tráfego está sendo registrado. Tipo de dados em Parquet: STRING	6
tgw-attachment-id	O ID do anexo do gateway de trânsito para o qual o tráfego está sendo registrado. Tipo de dados em Parquet: STRING	6
tgw-src-vpc-account-id	O Conta da AWS ID do tráfego VPC de origem. Tipo de dados em Parquet: STRING	6
tgw-dst-vpc-account-id	O Conta da AWS ID do tráfego VPC de destino. Tipo de dados em Parquet: STRING	6
tgw-src-vpc-id	O ID da VPC de origem para o gateway de trânsito Tipo de dados em Parquet: STRING	6
tgw-dst-vpc-id	O ID da VPC de destino para o gateway de trânsito. Tipo de dados em Parquet: STRING	6
tgw-src-subnet-id	O ID da VPC da sub-rede para o tráfego de origem do gateway de trânsito. Tipo de dados em Parquet: STRING	6

Campo	Descrição	Version (Versão)
tgw-dst-subnet-id	O ID da VPC da sub-rede para o tráfego de destino do gateway de trânsito. Tipo de dados em Parquet: STRING	6
tgw-src-eni	O ID da ENI do anexo do gateway de trânsito de origem para o fluxo. Tipo de dados em Parquet: STRING	6
tgw-dst-eni	O ID da ENI do anexo do gateway de trânsito de destino para o fluxo. Tipo de dados em Parquet: STRING	6
tgw-src-az-id	O ID da zona de disponibilidade que contém o gateway de trânsito de origem para o qual o tráfego é registrado. Se o tráfego for de uma sublocalização, o registro exibirá um símbolo '-' para este campo. Tipo de dados em Parquet: STRING	6
tgw-dst-az-id	O ID da zona de disponibilidade que contém o gateway de trânsito de destino para o qual o tráfego é registrado. Tipo de dados em Parquet: STRING	6
tgw-pair-attachment-id	Dependendo da direção do fluxo, esse é o ID do anexo de saída ou entrada do fluxo. Tipo de dados em Parquet: STRING	6
srcaddr	O endereço de origem do tráfego de entrada. Tipo de dados em Parquet: STRING	2

Campo	Descrição	Version (Versão)
dstaddr	O endereço de destino do tráfego de saída. Tipo de dados em Parquet: STRING	2
srcport	A porta de origem do tráfego. Tipo de dados em Parquet: INT_32	2
dstport	A porta de destino do tráfego. Tipo de dados em Parquet: INT_32	2
protocol	O número do protocolo IANA do tráfego. Para obter mais informações, consulte Assigned Internet Protocol Numbers. Tipo de dados em Parquet: INT_64	2
packets	O número de pacotes transferidos durante o fluxo. Tipo de dados em Parquet: INT_64	2
bytes	O número de bytes transferidos durante o fluxo. Tipo de dados em Parquet: INT_64	2
start	O tempo, em segundos Unix, quando o primeiro pacote de fluxo foi recebido no intervalo de agregação. Isso pode ser até 60 segundos após o pacote ter sido transmitido ou recebido no gateway de trânsito. Tipo de dados em Parquet: INT_64	2
end	O tempo, em segundos Unix, quando o último pacote de fluxo foi recebido dentro do intervalo de agregação. Isso pode ser até 60 segundos após o pacote ter sido transmitido ou recebido no gateway de trânsito. Tipo de dados em Parquet: INT_64	2

Campo	Descrição	Version (Versão)
log-status	O status do log de fluxo: • OK — Os dados são registrados em log normalmente nos destinos selecionados. • NODATA — Não havia nenhum tráfego de rede para ou proveniente da interface de rede durante o intervalo de agregação. • SKIPDATA — Alguns registros de log de fluxo foram ignorados durante o intervalo de agregação. Isso pode ocorrer em virtude de uma restrição de capacidade interna ou de um erro interno. Tipo de dados em Parquet: STRING	2
type	O tipo de tráfego. Os valores possíveis são IPv4 | IPv6 | EFA. Para obter mais informações, consulte Elastic Fabric Adapter no Manual do usuário do Amazon EC2 para instâncias do Linux. Tipo de dados em Parquet: STRING	3
packets-lost-no-route	Os pacotes foram perdidos devido a nenhuma rota ter sido especificada. Tipo de dados em Parquet: INT_64	6
packets-lost-blackhole	Os pacotes foram perdidos devido a um buraco negro. Tipo de dados em Parquet: INT_64	6
packets-lost-mtu-exceeded	Os pacotes foram perdidos devido ao tamanho exceder a MTU. Tipo de dados em Parquet: INT_64	6
packets-lost-ttl-expired	Os pacotes foram perdidos devido à expiração do time-to-live. Tipo de dados em Parquet: INT_64	6

Campo	Descrição	Version (Versão)
tcp-flags	O valor da máscara de bits para os seguintes sinalizadores TCP: • FIN: 1 • SYN: 2 • RST: 4 • PSH: 8 • ACK: 16 • SYN-ACK: 18 • URG: 32 **Important** Quando uma entrada de log de fluxo é formada somente por pacotes ACK, o valor do sinalizador é 0e , não 16. Para obter informações gerais sobre sinalizadores TCP (por exemplo, o significado de sinalizadores FIN, SYN e ACK), consulte Estrutura de segmentos TCP, na Wikipédia. Os sinalizadores TCP podem ser processados com o operador OR durante o intervalo de agregação. Para conexões curtas, os sinalizadores podem ser definidos na mesma linha no registro de log de fluxo, por exemplo, 19 para SYN-ACK e FIN, e 3 para SYN e FIN. Tipo de dados em Parquet: INT_32	3
region	A região que contém o gateway de trânsito no qual o tráfego é registrado. Tipo de dados em Parquet: STRING	4

Campo	Descrição	Version (Versão)
flow-direction	O sentido do fluxo em relação à interface onde o tráfego é capturado. Os valores possíveis são: ingress | egress. Tipo de dados em Parquet: STRING	5
pkt-src-aws-service	O nome do subconjunto de intervalos de endereços IP para o srcaddr se o endereço IP de origem for para um AWS serviço. Os valores possíveis são: AMAZON | AMAZON_APPFLOW | AMAZON_CONNECT | API_GATEWAY | CHIME_MEETINGS | CHIME_VOICECONNECTOR | CLOUD9 | CLOUDFRONT | CODEBUILD | DYNAMODB | EBS | EC2 | EC2_INSTANCE_CONNECT | GLOBALACCELERATOR | KINESIS_VIDEO_STREAMS | ROUTE53 | ROUTE53_HEALTHCHECKS | ROUTE53_HEALTHCHECKS_PUBLISHING | ROUTE53_RESOLVER | S3 | WORKSPACES_GATEWAYS. Tipo de dados em Parquet: STRING	5
pkt-dst-aws-service	O nome do subconjunto de intervalos de endereços IP para o dstaddr campo, se o endereço IP de destino for para um AWS serviço. Para uma lista de valores possíveis, consulte o campo pkt-src-aws-service. Tipo de dados em Parquet: STRING	5

Preços dos logs de fluxo do Transit Gateway

As cobranças por ingestão e armazenamento de dados para logs fornecidos são aplicáveis quando você publica logs de fluxo do gateway de trânsito. Para obter mais informações sobre preços ao publicar registros vendidos, abra Amazon CloudWatch Pricing e, em Nível pago, selecione Logs e encontre Vended Logs.

Crie um registro de fluxo que publique no Logs CloudWatch

Os registros de fluxo podem publicar dados de registros de fluxo diretamente na Amazon CloudWatch.

Quando publicados no CloudWatch Logs, os dados do log de fluxo são publicados em um grupo de registros, e cada gateway de trânsito tem um fluxo de log exclusivo no grupo de registros. Os fluxos de log contêm registros de log de fluxo. Você pode criar vários logs de fluxo que publicam dados no mesmo grupo de logs. Se um mesmo gateway de trânsito estiver presente em um ou mais logs de fluxo no mesmo grupo de logs, ele terá um único fluxo de logs combinado. Se tiver especificado que um log de fluxo deve capturar tráfego rejeitado e outro log de fluxo deve capturar o tráfego aceito, o stream misto de logs capturará todos os tráfegos.

As cobranças de ingestão e arquivamento de dados para registros vendidos se aplicam quando você publica registros de fluxo no Logs. CloudWatch Para obter mais informações, consulte Amazon CloudWatch Pricing.

Em CloudWatch Registros, o campo de carimbo de data/hora corresponde à hora de início capturada no registro do log de fluxo. O campo IngestionTime fornece a data e a hora em que o registro do log de fluxo foi recebido pelo Logs. CloudWatch O campo timestamp é posterior à hora final capturada no registro de log de fluxo.

Para obter mais informações sobre CloudWatch registros, consulte Registros enviados para CloudWatch registros no Guia do usuário do Amazon CloudWatch Logs.

Conteúdo

Funções do IAM para publicar registros de fluxo em CloudWatch registros

A função do IAM associada ao seu registro de fluxo deve ter permissões suficientes para publicar registros de fluxo no grupo de registros especificado em CloudWatch Registros. A função do IAM deve pertencer à sua Conta da AWS.

A política do IAM anexada à sua função do IAM deve incluir pelo menos as permissões a seguir.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource": "*"
    }
  ]
}
```

Além disso, verifique se a sua função tem um relacionamento de confiança que permite que o serviço de logs de fluxo assuma a função.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpc-flow-logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Recomendamos o uso das chaves de condição `aws:SourceAccount` e `aws:SourceArn` para se proteger contra O problema do agente confuso. Por exemplo, você poderia adicionar o bloco de condições a seguir na política de confiança anterior. A conta de origem é o proprietário do log de fluxo e o ARN de origem é o ARN do log de fluxo. Se você não souber o ID do log de fluxo, poderá substituir essa parte do ARN por um curinga (*) e, em seguida, atualizar a política depois de criar o log de fluxo.

```
"Condition": {
```

```
    "StringEquals": {
        "aws:SourceAccount": "account_id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:ec2:region:account_id:vpc-flow-log/flow-log-id"
    }
}
```

Crie ou atualize uma função do IAM para logs de fluxo

Você pode atualizar uma função existente ou usar o seguinte procedimento para criar uma nova para os logs de fluxo.

Como criar uma função do IAM para logs de fluxo

1. Abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Roles e depois Create Role.
3. Em Selecionar tipo de entidade confiável, selecione serviço AWS . Em Use case (Caso de uso), selecione EC2. Escolha Próximo.
4. Na página Add permissions (Adicionar permissões), selecione Next: Tags (Próximo: etiquetas) e, se desejar, adicione etiquetas. Escolha Próximo.
5. Na página Name, review, and create (Nomear, analisar e criar), insira um nome para a função e, opcionalmente, forneça uma Description (Descrição). Selecione Criar função.
6. Escolha o nome da sua função. Em Add permissions (Adicionar permissões), escolha Create inline policy (Criar política em linha) e, em seguida, escolha a guia JSON.
7. Copie a primeira política de Funções do IAM para publicar registros de fluxo em CloudWatch registros e cole-a na janela. Escolha Revisar política.
8. Insira um nome para a política e selecione Create policy (Criar política).
9. Selecione o nome de sua função. Em Trust relationships (Relacionamentos de confiança), selecione Edit trust relationship (Editar relacionamento de confiança). No documento da política existente, altere o serviço de `ec2.amazonaws.com` para `vpc-flow-logs.amazonaws.com`. Escolha Update Trust Policy.
10. Na página Summary (Resumo), anote o ARN da sua função. Você precisa desse ARN para criar o log de fluxo.

Permissões para que os usuários do IAM passem uma função

Os usuários também devem ter permissões para usar a ação `iam:PassRole` para a função do IAM associada ao log de fluxo.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["iam:PassRole"],
      "Resource": "arn:aws:iam::account-id:role/flow-log-role-name"
    }
  ]
}
```

Crie um registro de fluxo que publique no Logs CloudWatch

Você pode criar logs de fluxo para gateways de trânsito. Se executar essas etapas como um usuário do IAM, verifique se você tem permissões para usar a ação `iam:PassRole`. Para ter mais informações, consulte Permissões para que os usuários do IAM passem uma função.

Para criar um log de fluxo de gateway de trânsito usando o console

1. Faça login AWS Management Console e abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateways (Gateways de trânsito).
3. Marque as caixas de seleção de um ou mais gateways de trânsito e escolha Actions (Ações), Create flow log (Criar log de fluxo).
4. Em Destino, escolha Enviar para CloudWatch registros.
5. Para Grupo de log de destino, escolha o nome do grupo de log de destino que você criou.

   > **Note**
   >
   > Se o grupo de logs de destino ainda não existir, inserir um novo nome nesse campo criará um novo grupo de logs de destino.

6. Para a função do IAM, especifique o nome da função que tem permissões para publicar registros no CloudWatch Logs.

7. Para Log record format (Formato de registro de log) , selecione o formato para o registro de log de fluxo.
   - Para usar o formato padrão, escolha AWS default format (Formato padrão da).
   - Para usar um formato personalizado, escolha Custom format (Formato personalizado) e, em seguida, selecione os campos de Log format (Formato de log) .
8. (Opcional) Escolha Add new tag (Adicionar nova tag) para aplicar tags ao log de fluxo.
9. Selecione Create flow log (Criar log de fluxo).

Para criar um log de fluxo usando a linha de comando

Use um dos seguintes comandos.

- create-flow-logs (AWS CLI)
- New-EC2FlowLogs (AWS Tools for Windows PowerShell)
- CreateFlowLogs(API de consulta do Amazon EC2)

O AWS CLI exemplo a seguir cria um registro de fluxo que captura as informações do gateway de trânsito. Os registros de fluxo são entregues a um grupo de CloudWatch registros em Logs chamado`my-flow-logs`, na conta 123456789101, usando a função do IAM. `publishFlowLogs`

```
aws ec2 create-flow-logs --resource-type TransitGateway --resource-ids
 tgw-1a2b3c4d --log-group-name my-flow-logs --deliver-logs-permission-arn
 arn:aws:iam::123456789101:role/publishFlowLogs
```

Registros de log de fluxo de processo em CloudWatch Logs

Você pode trabalhar com registros de log de fluxo da mesma forma que faria com qualquer outro evento de log coletado pelo CloudWatch Logs. Para obter mais informações sobre o monitoramento de dados de log e filtros métricos, consulte Pesquisando e filtrando dados de log no Guia do CloudWatch usuário da Amazon.

Exemplo: criar um filtro CloudWatch métrico e um alarme para um registro de fluxo

Neste exemplo, você tem um log de fluxo para `eni-1a2b3c4d`. Pode ser útil criar um alarme que o alerte se houver 10 ou mais tentativas rejeitadas de conexão à sua instância pela porta TCP 22 (SSH) no período de 1 hora. Primeiro, você deve criar um filtro de métrica que corresponda ao

padrão do tráfego para o qual o alarme será criado. Depois, você pode criar um alarme para o filtro de métricas.

Para criar um filtro de métricas para tráfego SSH rejeitado e um alarme para o filtro

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, escolha Logs, Log groups (Grupos de log).
3. Marque a caixa de seleção do grupo de log e, em seguida, escolha Actions (Ações), Create metric filter (Criar filtro de métrica).
4. Em Filter Pattern (Padrão de filtro), insira o seguinte.

```
[version, resource_type, account_id,tgw_id="tgw-123abc456bca”, tgw_attachment_id,
 tgw_src_vpc_account_id, tgw_dst_vpc_account_id, tgw_src_vpc_id, tgw_dst_vpc_id,
 tgw_src_subnet_id, tgw_dst_subnet_id, tgw_src_eni, tgw_dst_eni, tgw_src_az_id,
 tgw_dst_az_id, tgw_pair_attachment_id, srcaddr= "10.0.0.1", dstaddr,
 srcport=“80”, dstport, protocol=“6”, packets, bytes,start,end, log_status,
 type,packets_lost_no_route, packets_lost_blackhole, packets_lost_mtu_exceeded,
 packets_lost_ttl_expired, tcp_flags,region, flow_direction, pkt_src_aws_service,
 pkt_dst_aws_service]
```

5. Em Select log data to test (Selecionar dados de log para teste), selecione o fluxo de logs do gateway de trânsito. (Opcional) Para visualizar as linhas de dados de log que correspondem ao padrão do filtro, escolha Test Pattern (Padrão de teste). Quando estiver pronto, escolha Next (Avançar).
6. Insira um nome de filtro, um namespace de métrica e o nome da métrica. Defina o valor da métrica como **1**. Quando terminar, escolha Next (Avançar) e, em seguida, escolha Create metric filter (Criar filtro de métrica).
7. No painel de navegação, escolha Alarms (Alarmes), All alarms (Todos os alarmes).
8. Selecione Criar alarme.
9. Escolha o namespace do filtro de métrica que você criou.

   Pode levar alguns minutos para uma nova métrica ser exibida no console.
10. Selecione o nome da métrica que você criou e, em seguida. escolha Select metric (Selecionar métrica).
11. Siga as instruções a seguir para configurar o alarme e, em seguida, escolha Next (Avançar):

    - Em Estatística, selecione Soma. Isso garante que você esteja capturando o número total de pontos de dados do período especificado.

- Em Period (Período), selecione 1 hour (1 hora).
- Em Whenever (Sempre que), escolha Greater/Equal (Maior que/igual a) e insira **10** como limite.
- Em Additional configuration (Configuração adicional), Datapoints to alarm (Pontos de dados para alarme), deixe o padrão de **1**.

12. Em Notification (Notificação), selecione um tópico do SNS existente ou Create new topic (Criar novo tópico) para criar um novo. Escolha Próximo.
13. Insira um nome e uma descrição para o alarme e selecione Next (Avançar).
14. Quando terminar de configurar o alarme, escolha Create alarm (Criar alarme).

Criar um log de fluxo para publicação no Amazon S3

Os logs de fluxo podem publicar dados de log de fluxo no Amazon S3.

Quando é feita uma publicação no Amazon S3, os dados de log de fluxo são publicados no bucket existente do Amazon S3 especificado. Os registros de log de fluxo para todos os gateways de trânsito monitorados são publicados em uma série de objetos de arquivos de log armazenados no bucket.

As taxas de ingestão e arquivamento de dados são aplicadas Amazon CloudWatch pelos registros vendidos quando você publica registros de fluxo no Amazon S3. Para obter mais informações sobre CloudWatch preços de registros vendidos, abra Amazon CloudWatch Pricing, escolha Logs e, em seguida, encontre Vended Logs.

Para criar um bucket do Amazon S3 para uso com logs de fluxo, consulte Criar um bucket no Guia do usuário do Amazon Simple Storage Service.

Para obter mais informações sobre o registro em log de várias contas, consulte Registro central na Biblioteca de soluções da AWS .

Para obter mais informações sobre CloudWatch registros, consulte Registros enviados para o Amazon S3 no Guia do usuário do Amazon CloudWatch Logs.

Conteúdo

- Permissões do bucket do Amazon S3 para logs de fluxo
- Política de chaves obrigatórias para uso com SSE-KMS
- Permissões de arquivo de log do Amazon S3
- Criar um log de fluxo para publicação no Amazon S3
- Processar registros de log de fluxo no Amazon S3

Arquivos de log de fluxo

Os logs de fluxo da VPC são um recurso que coleta registros de log de fluxo, consolida-os em arquivos de log e publica os arquivos de log no bucket do Amazon S3 a intervalos de cinco minutos. Cada arquivo de log contém os registros de log de fluxo para o tráfego de IP registrado nos últimos cinco minutos.

O tamanho máximo de um arquivo de log é de 75 MB. Se o arquivo de log atingir o limite de tamanho no período de 5 minutos, o log de fluxo deixará de adicionar registros de log de fluxo. Depois, ele publicará o log de fluxo no bucket do Amazon S3 e criará um novo arquivo de log.

No Amazon S3, o campo Last modified (Última modificação) do arquivo de log de fluxo indica a data e hora em que o arquivo foi carregado no bucket do Amazon S3. Isso é posterior à data/hora no nome do arquivo e difere pela quantidade de tempo necessária para carregar o arquivo para o bucket do Amazon S3.

Formato do arquivo de log

Você pode especificar um dos formatos a seguir para os arquivos de log. Cada arquivo é compactado em um único arquivo Gzip.

- Texto: texto sem formatação. Esse é o formato padrão.
- Parquet: Apache Parquet é um formato colunar de dados. Consultas sobre dados no formato Parquet são 10 a 100 vezes mais rápidas em comparação com consultas em dados em texto simples. Dados em formato Parquet com compressão Gzip ocupam 20% menos espaço de armazenamento do que o texto simples com compactação Gzip.

Opções do arquivo de log

Opcionalmente, você pode especificar as opções a seguir.

- Prefixos S3 compatíveis com Hive: habilite prefixos compatíveis com o Hive em vez de importar partições para as ferramentas compatíveis com o Hive. Antes de executar consultas, use o comando MSCK REPAIR TABLE.
- Partições por hora: se você tiver um grande volume de logs e tipicamente direcionar consultas para uma hora específica, poderá obter resultados mais rápidos e economizar em custos de consulta ao particionar os logs a cada hora.

Estrutura do arquivo de log do bucket do S3

Os arquivos de log são salvos no bucket do Amazon S3 especificado por meio de uma estrutura de pastas determinada pelo ID do log de fluxo, pela região, pela data de criação e pelas opções de destino.

Por padrão, os arquivos são entregues no local a seguir.

```
bucket-and-optional-prefix/AWSLogs/account_id/vpcflowlogs/region/year/month/day/
```

Se você habilitar prefixos S3 compatíveis com HIVE, os arquivos serão entregues no local a seguir.

```
bucket-and-optional-prefix/AWSLogs/aws-account-id=account_id/service=vpcflowlogs/aws-
region=region/year=year/month=month/day=day/
```

Se você habilitar partições por hora, os arquivos serão entregues no local a seguir.

```
bucket-and-optional-prefix/AWSLogs/account_id/vpcflowlogs/region/year/month/day/hour/
```

Se você habilitar partições compatíveis com o Hive e particionar o log de fluxo por hora, os arquivos serão entregues no local a seguir.

```
bucket-and-optional-prefix/AWSLogs/aws-account-id=account_id/service=vpcflowlogs/aws-
region=region/year=year/month=month/day=day/hour=hour/
```

Nomes do arquivo de log

O nome de um arquivo de log é baseado na ID do log de fluxo, na região e na data e na hora de criação. Os nomes de arquivo usam o seguinte formato.

```
aws_account_id_vpcflowlogs_region_flow_log_id_YYYYMMDDTHHmmZ_hash.log.gz
```

Veja a seguir um exemplo de arquivo de log para um log de fluxo criado pela 123456789012 da Conta da AWS para um recurso na região us-east-1 em June 20, 2018 às 16:20 UTC. O arquivo contém os registros de log de fluxo com um horário de término entre 16:20:00 e 16:24:59.

```
123456789012_vpcflowlogs_us-east-1_fl-1234abcd_20180620T1620Z_fe123456.log.gz
```

Política do IAM para entidades principais do IAM que publicam logs de fluxo no Amazon S3

A entidade principal do IAM que cria o log de fluxo deve ter as permissões a seguir, necessárias para publicar logs de fluxo no bucket de destino do Amazon S3.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
        ],
      "Resource": "*"
    }
  ]
}
```

Permissões do bucket do Amazon S3 para logs de fluxo

Por padrão, os buckets do Amazon S3 e os objetos que eles contêm são privados. Somente o proprietário do bucket pode acessá-los. No entanto, o proprietário do bucket pode conceder acesso a outros recursos e usuários por meio da criação de uma política de acesso.

Se o usuário que cria um log de fluxo for proprietário do bucket e tiver as permissões `PutBucketPolicy` e `GetBucketPolicy` para o mesmo, anexamos automaticamente as políticas a seguir para o bucket. Esta política substitui qualquer política existente anexada ao bucket.

Caso contrário, o proprietário do bucket deve adicionar essa política ao bucket, especificando o ID da Conta da AWS do criador de log de fluxo ou falha na criação do log de fluxo. Para obter mais informações, consulte Uso de políticas de bucket no Guia do usuário do Amazon Simple Storage Service.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
            "Action": "s3:PutObject",
            "Resource": "my-s3-arn",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceAccount": account_id
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:region:account_id:*"
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryCheck",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
            "Action": ["s3:GetBucketAcl", "s3:ListBucket"],
            "Resource": "arn:aws:s3:::bucket_name",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": account_id
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:region:account_id:*"
                }
            }
        }
    ]
}
```

O ARN que você especificar para *my-s3-arn* depende do uso ou não de prefixos S3 compatíveis com Hive.

- Prefixos padrão

```
arn:aws:s3:::bucket_name/optional_folder/AWSLogs/account_id/*
```

- Prefixos S3 compatíveis com Hive

```
arn:aws:s3:::bucket_name/optional_folder/AWSLogs/aws-account-id=account_id/*
```

Como prática recomendada, recomendamos que você conceda essas permissões ao responsável pelo serviço de entrega de registros em vez de Conta da AWS ARNs individuais. Outra prática recomendada é o uso das chaves de condição `aws:SourceAccount` e `aws:SourceArn` para se proteger contra O problema do agente confuso. A conta de origem é o proprietário do log de fluxo e o ARN de origem é o ARN curinga (*) do serviço de logs.

Política de chaves obrigatórias para uso com SSE-KMS

É possível proteger os dados no bucket do Amazon S3 habilitando a criptografia no lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3) ou a criptografia no lado do servidor com chaves do KMS (SSE-KMS). Para obter mais informações, consulte Proteger dados usando criptografia do lado do servidor no Manual do usuário do Amazon S3.

Com o SSE-KMS, você pode usar uma chave gerenciada ou uma chave AWS gerenciada pelo cliente. Com uma chave AWS gerenciada, você não pode usar a entrega entre contas. Os logs de fluxo são entregues a partir da conta de entrega de log, portanto, você deve conceder acesso para entrega entre contas. Para conceder acesso entre contas ao bucket do S3, use uma chave gerenciada pelo cliente e especifique o nome do recurso da Amazon (ARN) da chave gerenciada pelo cliente quando habilitar a criptografia de bucket. Para obter mais informações, consulte Especificação de criptografia no lado do servidor com o AWS KMS no Manual do usuário do Amazon S3.

Quando você usa o SSE-KMS com uma chave gerenciada pelo cliente, deve adicionar o seguinte à política de chave da sua chave (não à política de bucket do bucket do S3) para que o VPC Flow Logs possa gravar no bucket do S3.

```
{
    "Sid": "Allow Transit Gateway Flow Logs to use the key",
    "Effect": "Allow",
    "Principal": {
        "Service": [
```

```
            "delivery.logs.amazonaws.com"
        ]
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": "*"
}
```

Permissões de arquivo de log do Amazon S3

Além das políticas de bucket necessárias, o Amazon S3 usa listas de controle de acesso (ACLs) para gerenciar o acesso aos arquivos de log criados por um log de fluxo. Por padrão, o proprietário do bucket tem permissões `FULL_CONTROL` em cada arquivo de log. O proprietário da entrega de logs, se é diferente do proprietário do bucket, não tem nenhuma permissão. A conta de entrega de logs tem permissões `READ` e `WRITE`. Para obter mais informações, consulte Visão geral da lista de controle de acesso (ACL) no Guia do usuário do Amazon Simple Storage Service.

Criar um log de fluxo para publicação no Amazon S3

Depois de criar e configurar o bucket do Amazon S3, você poderá criar logs de fluxo para gateways de trânsito.

Para criar um log de fluxo de gateway de trânsito que publique no Amazon S3 usando o console

1. Abra o console do Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit gateways (Gateways de trânsito) ou Transit gateway attachments (Anexos do gateway de trânsito).
3. Marque a caixa de seleção de um ou mais gateways de trânsito ou anexos do gateway de trânsito.
4. Escolha Actions (Ações), Create flow log (Criar log de fluxo).
5. Defina as configurações do log de fluxo. Para obter mais informações, consulte Para definir as configurações do log de fluxo.

Para definir as configurações do log de fluxo usando o console

1. Em Destination (Destino), escolha Send to an S3 bucket (Enviar para um bucket do S3).
2. Para S3 bucket ARN (ARN do bucket do S3), especifique o nome de recurso da Amazon (ARN) de um bucket existente do Amazon S3. Opcionalmente, é possível incluir uma subpasta. Por exemplo, para especificar uma subpasta chamada `my-logs` em um bucket chamado `my-bucket`, use o seguinte ARN:

   ```
   arn:aws::s3:::my-bucket/my-logs/
   ```

   O bucket não pode usar `AWSLogs` como um nome de subpasta, pois se trata de um termo reservado.

   Se você for o proprietário do bucket, criamos automaticamente uma política de recurso e a anexamos ao bucket. Para ter mais informações, consulte Permissões do bucket do Amazon S3 para logs de fluxo.
3. Em Log record format (Formato de registro de log), selecione o formato para o registro de log de fluxo.

   - Para usar o formato de registro de log de fluxo padrão, escolha AWS default format (Formato padrão da).
   - Para criar um formato personalizado, escolha Custom format (Formato personalizado). Em Log format (Formato de log), escolha os campos a serem incluídos no registro de log de fluxo.
4. Em Log file format (Formato de registro de log), especifique o formato do arquivo de log.

   - Texto: texto sem formatação. Esse é o formato padrão.
   - Parquet: Apache Parquet é um formato colunar de dados. Consultas sobre dados no formato Parquet são 10 a 100 vezes mais rápidas em comparação com consultas em dados em texto simples. Dados em formato Parquet com compressão Gzip ocupam 20% menos espaço de armazenamento do que o texto simples com compactação Gzip.
5. (Opcional) Para usar prefixos S3 compatíveis com o Hive, escolha Hive-compatible S3 prefix (Prefixo do S3 compatível com Hive), Enable (Habilitar).
6. (Opcional) Para particionar seus logs de fluxo por hora, escolha Every 1 hour (60 mins) (A cada 1 hora [60 minutos]).
7. (Opcional) Para adicionar uma etiqueta ao log de fluxo, escolha Add new tag (Adicionar nova etiqueta) e especifique a chave e o valor da etiqueta.
8. Selecione Create flow log (Criar log de fluxo).

Como criar um log de fluxo publicado no Amazon S3 usando uma ferramenta de linha de comando

Use um dos seguintes comandos.

- create-flow-logs (AWS CLI)
- New-EC2FlowLogs (AWS Tools for Windows PowerShell)
- CreateFlowLogs(API de consulta do Amazon EC2)

O AWS CLI exemplo a seguir cria um log de fluxo que captura todo o tráfego do gateway de trânsito para a `tgw-00112233344556677` VPC e entrega os registros de fluxo para um bucket do Amazon S3 chamado. `flow-log-bucket` O parâmetro `--log-format` especifica um formato personalizado para os registros de log de fluxo.

```
aws ec2 create-flow-logs --resource-type TransitGateway --resource-ids
 tgw-00112233344556677 --log-destination-type s3 --log-destination arn:aws:s3:::flow-
log-bucket/my-custom-flow-logs/'
```

Processar registros de log de fluxo no Amazon S3

Os arquivos de log são compactados. Se você abrir os arquivos de log usando o console do Amazon S3, eles serão descompactados, e os registros de log de fluxo serão exibidos. Se você baixar os arquivos, será necessário descompactá-los para visualizar os registros de log de fluxo.

Publique registros de fluxo no Firehose

Tópicos

- Perfis do IAM para entrega entre contas
- Crie um registro de fluxo que publique no Firehose

Os registros de fluxo podem publicar dados de registro de fluxo diretamente no Firehose. Você pode optar por publicar logs de fluxo na mesma conta do monitor de recursos ou em uma conta diferente.

Pré-requisitos

Ao publicar no Firehose, os dados do log de fluxo são publicados em um stream de distribuição do Firehose, em formato de texto simples. Primeiro, você deve ter criado um stream de entrega do

Firehose. Para ver as etapas para criar um stream de entrega, consulte Criação de um stream de entrega do Amazon Data Firehose no Guia do desenvolvedor do Amazon Data Firehose.

Definição de preço

São aplicadas as taxas padrão de ingestão e entrega. Para obter mais informações, abra o Amazon CloudWatch Pricing, selecione Logs e encontre Vended Logs.

Perfis do IAM para entrega entre contas

Ao publicar no Kinesis Data Firehose, você pode escolher um fluxo de entrega que esteja na mesma conta que o recurso a ser monitorado (a conta de origem) ou em uma conta diferente (a conta de destino). Para permitir a entrega entre contas de registros de fluxo para o Firehose, você deve criar uma função do IAM na conta de origem e uma função do IAM na conta de destino.

Funções

- Função da conta de origem
- Função da conta de destino

Função da conta de origem

Na conta de origem, crie uma função que conceda as seguintes permissões. Neste exemplo, o nome da função é `mySourceRole`, mas você pode escolher um nome diferente para esta função. A última instrução permite que a função na conta de destino assuma esta função. As instruções de condição garantem que essa função seja passada somente para o serviço de entrega de logs e somente ao ser monitorado o recurso especificado. Ao criar sua política, especifique as VPCs, as interfaces de rede ou as sub-redes que você está monitorando com a chave de condição `iam:AssociatedResourceARN`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::source-account:role/mySourceRole",
      "Condition": {
          "StringEquals": {
              "iam:PassedToService": "delivery.logs.amazonaws.com"
```

```
          },
          "StringLike": {
              "iam:AssociatedResourceARN": [
                  "arn:aws:ec2:region:source-account:transit-gateway/
tgw-0fb8421e2da853bf"
              ]
          }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
          "logs:CreateLogDelivery",
          "logs:DeleteLogDelivery",
          "logs:ListLogDeliveries",
          "logs:GetLogDelivery"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::destination-account:role/
AWSLogDeliveryFirehoseCrossAccountRole"
    }
  ]
}
```

Verifique se a essa função tem a política de confiança a seguir, que permite que o serviço de entrega de logs assuma a função.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Na conta de origem, use o procedimento a seguir para criar a função.

Para criar a função da conta de origem

1. Faça login AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Policies.
3. Escolha Create policy.
4. Na página Create policy (Criar política) faça o seguinte:
    1. Selecione JSON.
    2. Substitua o conteúdo dessa janela pela política de permissões no início desta seção.
    3. Selecione Next: Tags (Próximo: tags) e Next: Review (Próximo: revisar).
    4. Insira um nome e uma descrição opcional para a política e escolha Create policy (Criar política).
5. No painel de navegação, escolha Roles.
6. Escolha Criar Perfil.
7. Na opção Trusted entity type (Tipo de entidade confiável), escolha Custom trust policy (Política de confiança personalizada). Em Custom trust policy (Política de confiança personalizada), substitua `"Principal": {},` pelo seguinte, que especifica o serviço de entrega de logs. Escolha Próximo.

    ```
    "Principal": {
       "Service": "delivery.logs.amazonaws.com"
    },
    ```
8. Na página Add permissions (Adicionar permissões), marque a caixa de seleção correspondente à política que você criou anteriormente neste procedimento e, em seguida, escolha Next (Próximo).
9. Insira um nome para a função e, opcionalmente, uma descrição.
10. Selecione Criar função.

Função da conta de destino

Na conta de destino, crie uma função com um nome que comece com AWSLogsDeliveryFirehoseCrossAccountRole. Essa função deve conceder as seguintes permissões.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
          "iam:CreateServiceLinkedRole",
          "firehose:TagDeliveryStream"
      ],
      "Resource": "*"
    }
  ]
}
```

Certifique-se de que essa função tenha a seguinte política de confiança, que permite que a função que você criou na conta de origem assuma esta função.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
          "AWS": "arn:aws:iam::source-account:role/mySourceRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Na conta de destino, use o procedimento a seguir para criar a função.

Para criar a função da conta de destino

1. Faça login AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Policies.
3. Escolha Create policy.
4. Na página Create policy (Criar política) faça o seguinte:

    1. Selecione JSON.

2. Substitua o conteúdo dessa janela pela política de permissões no início desta seção.
3. Selecione Next: Tags (Próximo: tags) e Next: Review (Próximo: revisar).
4. Insira um nome para sua política que comece com e AWSLogDeliveryFirehoseCrossAccountRole, em seguida, escolha Criar política.

5. No painel de navegação, escolha Roles.
6. Escolha Criar Perfil.
7. Na opção Trusted entity type (Tipo de entidade confiável), escolha Custom trust policy (Política de confiança personalizada). Em Custom trust policy (Política de confiança personalizada), substitua `"Principal": {},` pelo seguinte, que especifica o serviço de entrega de logs. Escolha Próximo.

```
"Principal": {
   "AWS": "arn:aws:iam::source-account:role/mySourceRole"
},
```

8. Na página Add permissions (Adicionar permissões), marque a caixa de seleção correspondente à política que você criou anteriormente neste procedimento e, em seguida, escolha Next (Próximo).
9. Insira um nome para a função e, opcionalmente, uma descrição.
10. Selecione Criar função.

Crie um registro de fluxo que publique no Firehose

Para criar um registro de fluxo do gateway de trânsito que é publicado no Firehose usando o console

1. Abra o console do Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit gateways (Gateways de trânsito) ou Transit gateway attachments (Anexos do gateway de trânsito).
3. Marque a caixa de seleção de um ou mais gateways de trânsito ou anexos do gateway de trânsito.
4. Escolha Actions (Ações), Create flow log (Criar log de fluxo).
5. Em Destination (Destino), escolha Enviar para um Firehose Delivery System (Sistema de entrega Firehose).
6. Para o Firehose Delivery Stream ARN (ARN do fluxo de entrega do Firehose), escolha o ARN de um fluxo de entrega que você criou e no qual o log de fluxo deverá ser publicado.

7. Em Log record format (Formato de registro de log), selecione o formato para o registro de log de fluxo.
   - Para usar o formato de registro de log de fluxo padrão, escolha AWS default format (Formato padrão da).
   - Para criar um formato personalizado, escolha Custom format (Formato personalizado). Em Log format (Formato de log), escolha os campos a serem incluídos no registro de log de fluxo.
8. (Opcional) Para adicionar uma etiqueta ao log de fluxo, escolha Add new tag (Adicionar nova etiqueta) e especifique a chave e o valor da etiqueta.
9. Selecione Create flow log (Criar log de fluxo).

Para criar um registro de fluxo que seja publicado no Firehose usando a ferramenta de linha de comando

Use um dos seguintes comandos:

- create-flow-logs (CLI)AWS
- New-EC2FlowLogs (AWS Tools for Windows PowerShell)
- CreateFlowLogs(API de consulta do Amazon EC2)

O exemplo de AWS CLI a seguir cria um log de fluxo que captura informações do gateway de trânsito e entrega o log de fluxo ao stream de entrega especificado do Firehose.

```
aws ec2 create-flow-logs \
                --resource-type TransitGateway \
                --resource-ids tgw-1a2b3c4d \
                --log-destination-type kinesis-data-firehose \
                --log-destination arn:aws:firehose:us-
east-1:123456789012:deliverystream:flowlogs_stream
```

O exemplo de AWS CLI a seguir cria um log de fluxo que captura as informações do gateway de trânsito e entrega o log de fluxo para um stream de entrega do Firehose diferente da conta de origem.

```
aws ec2 create-flow-logs  \
  --resource-type TransitGateway \
  --resource-ids gw-1a2b3c4d \
```

```
  --log-destination-type kinesis-data-firehose \
  --log-destination arn:aws:firehose:us-
east-1:123456789012:deliverystream:flowlogs_stream \
  --deliver-logs-permission-arn arn:aws:iam::source-account:role/mySourceRole \
  --deliver-cross-account-role arn:aws:iam::destination-account:role/
AWSLogDeliveryFirehoseCrossAccountRole
```

Trabalhar com os logs de fluxo do Transit Gateway

Você pode trabalhar com os logs de fluxo do Transit Gateway usando os consoles Amazon EC2, Amazon VPC e CloudWatch Amazon S3.

Tarefas

- Controlar o uso de logs de fluxo
- Criar um log de fluxo
- Exibir logs de fluxo
- Adicionar ou remover tags para logs de fluxo
- Exibir registros de log de fluxo
- Procurar registros de log de fluxo
- Excluir um log de fluxo
- Visão geral e limitações da API e da CLI

Controlar o uso de logs de fluxo

Por padrão, os usuários do não têm permissão para trabalhar com logs de fluxo. Você pode criar uma política de usuário que conceda permissões aos usuários para criar, descrever e excluir logs de fluxo. Para obter mais informações, consulte Conceder aos usuários do IAM as permissões necessárias para os recursos do Amazon EC2 na Referência de API do Amazon EC2.

Veja a seguir uma política de exemplo que concede aos usuários as permissões totais para criar, descrever e excluir logs de fluxo.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteFlowLogs",
        "ec2:CreateFlowLogs",
        "ec2:DescribeFlowLogs"
      ],
      "Resource": "*"
    }
  ]
}
```

Algumas configurações adicionais de funções e permissões do IAM são necessárias, dependendo se você está publicando no CloudWatch Logs ou no Amazon S3. Para obter mais informações, consulte Crie um registro de fluxo que publique no Logs CloudWatch e Criar um log de fluxo para publicação no Amazon S3.

Criar um log de fluxo

Você pode criar registros de fluxo para seus gateways de trânsito que podem publicar dados no CloudWatch Logs, no Amazon S3 ou no Firehose.

Para mais informações, consulte:

- Crie um registro de fluxo que publique no Logs CloudWatch
- Criar um log de fluxo para publicação no Amazon S3
- Crie um registro de fluxo que publique no Firehose

Exibir logs de fluxo

Você pode visualizar informações sobre os logs de fluxo no console da Amazon VPC visualizando a guia Flow Logs (Logs de fluxo) de um recurso específico. Quando você seleciona o recurso, todos os logs de fluxo desse recurso são listados. As informações exibidas incluem o ID do log de fluxo, a configuração do log de fluxo e o status do log de fluxo.

Para visualizar informações sobre logs de fluxo para gateways de trânsito

1. Abra o console do Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit gateways (Gateways de trânsito) ou Transit gateway attachments (Anexos do gateway de trânsito).

3. Selecione um gateway de trânsito ou um anexo do gateway de trânsito e escolha Flow Logs (Logs de fluxo). As informações sobre os logs de fluxo são exibidas nessa guia. A coluna Destination type (Tipo de destino) indica o destino no qual os logs de fluxo são publicados.

Adicionar ou remover tags para logs de fluxo

É possível adicionar ou remover tags para um log de fluxo nos consoles do Amazon EC2 e da Amazon VPC.

Para adicionar ou remover tags de um log de fluxo do gateway de trânsito

1. Abra o console do Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit gateways (Gateways de trânsito) ou Transit gateway attachments (Anexos do gateway de trânsito).
3. Selecione um gateway de trânsito ou um anexo do gateway de trânsito
4. Escolha Manage tags (Gerenciar tags) para o log de fluxo necessário.
5. Para adicionar uma nova tag, escolha Criar tag. Para remover uma tag, escolha o botão Excluir (x).
6. Escolha Salvar.

Exibir registros de log de fluxo

Você pode visualizar seus registros de log de fluxo usando o console CloudWatch Logs ou o console Amazon S3, dependendo do tipo de destino escolhido. Depois que o log de fluxo é criado, pode levar alguns minutos para ele ficar visível no console.

Para ver os registros do registro de fluxo publicados no CloudWatch Logs

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, selecione Logs e o grupo de logs que contém o seu log de fluxo. É exibida uma lista de fluxos de logs para cada gateway de trânsito.
3. Selecione o fluxo de logs que contém o ID do gateway de trânsito para o qual você deseja visualizar os registros de log de fluxo. Para ter mais informações, consulte Registros de log de fluxo de gateway de trânsito.

Como visualizar os registros de log de fluxo publicados no Amazon S3

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Em Bucket name (Nome do bucket), selecione o bucket no qual os logs de fluxo são publicados.
3. Em Name (Nome), marque a caixa de seleção ao lado do arquivo de log. No painel de visão geral do objeto, selecione Download (Baixar).

Procurar registros de log de fluxo

Você pode pesquisar seus registros de registro de fluxo que são publicados no CloudWatch Logs usando o console do CloudWatch Logs. Você pode usar filtros de métrica para filtrar registros de log de fluxo. Os registros de log de fluxo são delimitados por espaço.

Para pesquisar registros de registros de fluxo usando o console CloudWatch de registros

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, escolha Logs e, em seguida, escolha Grupos de log.
3. Selecione o grupo de logs que contém o log de fluxo desejado. É exibida uma lista de fluxos de logs para cada gateway de trânsito.
4. Selecione o fluxo de logs individual se souber qual é o gateway de trânsito que está procurando. Como alternativa, escolha Pesquisar grupo de logs para pesquisar todo o grupo de logs. Isso pode levar algum tempo se houver muitos gateways de trânsito no grupo de logs ou dependendo do intervalo de tempo selecionado.
5. Em Filter events (Filtrar eventos), insira a string a seguir. Isso pressupõe que o registro de log de fluxo usa o formato padrão.

```
[version, resource_type, account_id,tgw_id, tgw_attachment_id,
 tgw_src_vpc_account_id, tgw_dst_vpc_account_id, tgw_src_vpc_id, tgw_dst_vpc_id,
 tgw_src_subnet_id, tgw_dst_subnet_id, tgw_src_eni, tgw_dst_eni, tgw_src_az_id,
 tgw_dst_az_id, tgw_pair_attachment_id, srcaddr, dstaddr, srcport, dstport,
 protocol, packets, bytes,start,end, log_status, type,packets_lost_no_route,
 packets_lost_blackhole, packets_lost_mtu_exceeded, packets_lost_ttl_expired,
 tcp_flags,region, flow_direction, pkt_src_aws_service, pkt_dst_aws_service]
```

6. Modifique o filtro conforme necessário especificando valores para os campos. Os exemplos a seguir filtram por endereços IP de origem específicos.

```
[version, resource_type, account_id,tgw_id, tgw_attachment_id,
 tgw_src_vpc_account_id, tgw_dst_vpc_account_id, tgw_src_vpc_id, tgw_dst_vpc_id,
 tgw_src_subnet_id, tgw_dst_subnet_id, tgw_src_eni, tgw_dst_eni, tgw_src_az_id,
 tgw_dst_az_id, tgw_pair_attachment_id, srcaddr= 10.0.0.1, dstaddr,
 srcport, dstport, protocol, packets, bytes,start,end, log_status,
 type,packets_lost_no_route, packets_lost_blackhole, packets_lost_mtu_exceeded,
 packets_lost_ttl_expired, tcp_flags,region, flow_direction, pkt_src_aws_service,
 pkt_dst_aws_service]
[version, resource_type, account_id,tgw_id, tgw_attachment_id,
 tgw_src_vpc_account_id, tgw_dst_vpc_account_id, tgw_src_vpc_id, tgw_dst_vpc_id,
 tgw_src_subnet_id, tgw_dst_subnet_id, tgw_src_eni, tgw_dst_eni, tgw_src_az_id,
 tgw_dst_az_id, tgw_pair_attachment_id, srcaddr= 10.0.2.*, dstaddr,
 srcport, dstport, protocol, packets, bytes,start,end, log_status,
 type,packets_lost_no_route, packets_lost_blackhole, packets_lost_mtu_exceeded,
 packets_lost_ttl_expired, tcp_flags,region, flow_direction, pkt_src_aws_service,
 pkt_dst_aws_service]
```

O exemplo a seguir filtra por ID de gateway de trânsito tgw-123abc456bca, porta de destino e número de bytes.

```
[version, resource_type, account_id,tgw_id=tgw-123abc456bca, tgw_attachment_id,
 tgw_src_vpc_account_id, tgw_dst_vpc_account_id, tgw_src_vpc_id, tgw_dst_vpc_id,
 tgw_src_subnet_id, tgw_dst_subnet_id, tgw_src_eni, tgw_dst_eni, tgw_src_az_id,
 tgw_dst_az_id, tgw_pair_attachment_id, srcaddr, dstaddr, srcport, dstport =
 80 || dstport = 8080, protocol, packets, bytes >= 500,start,end, log_status,
 type,packets_lost_no_route, packets_lost_blackhole, packets_lost_mtu_exceeded,
 packets_lost_ttl_expired, tcp_flags,region, flow_direction, pkt_src_aws_service,
 pkt_dst_aws_service]
```

Excluir um log de fluxo

É possível excluir um log de fluxo de gateway de trânsito usando o console da Amazon VPC.

Esses procedimentos desabilitam o serviço de log de fluxo para um recurso. A exclusão de um log de fluxo não exclui os fluxos de log existentes dos CloudWatch Logs ou dos arquivos de log do Amazon S3. Os dados de log de fluxo existentes devem ser excluídos por meio do respectivo console de serviço. Além disso, a exclusão de um log de fluxo que publica no Amazon S3 não remove as políticas de bucket e as listas de controle de acesso (ACLs).

Para excluir um log de fluxo de gateway de trânsito

1. Abra o console do Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateways (Gateways de trânsito).
3. Escolha um Transit gateway ID (ID de gateway de trânsito).
4. Na seção Flow logs (Logs de fluxos), escolha os logs de fluxos que você deseja excluir.
5. Escolha Actions (Ações) e depois Delete log group (Excluir grupo de logs).
6. Confirme que você deseja excluir o fluxo escolhendo Delete (Excluir).

Visão geral e limitações da API e da CLI

Você pode executar as tarefas descritas nesta página usando a linha de comando ou uma API.

As seguintes limitações se aplicam ao usar a API `CreateFlowLogs` ou a CLI `create-flow-logs`:

- `--resource-ids` tem uma restrição máxima de 25 tipos de recurso `TransitGateway` ou `TransitGatewayAttachment`.
- `--traffic-type` não é um campo obrigatório por padrão. Um erro será retornado se você fornecer esse valor para recursos do tipo gateway de trânsito. Esse limite se aplica apenas a recursos do tipo gateway de trânsito.
- `--max-aggregation-interval` tem um valor padrão de `60` e é o único valor aceito para recursos do tipo gateway de trânsito. Um erro será retornado se você tentar passar qualquer outro valor. Esse limite se aplica apenas a recursos do tipo gateway de trânsito.
- `--resource-type` é compatível com dois tipos de recursos novos, `TransitGateway` e `TransitGatewayAttachment`.
- `--log-format` inclui todos os campos de log para os recursos do tipo gateway de trânsito se você não definir quais campos deseja incluir. Esse limite se aplica apenas a recursos do tipo gateway de trânsito.

Criar um log de fluxo

- create-flow-logs (AWS CLI)
- New-EC2FlowLog (AWS Tools for Windows PowerShell)
- CreateFlowLogs(API de consulta do Amazon EC2)

Descrever seus logs de fluxo

- describe-flow-logs (AWS CLI)
- Get-EC2FlowLog (AWS Tools for Windows PowerShell)
- DescribeFlowLogs(API de consulta do Amazon EC2)

Visualizar seus registros de log de fluxo (eventos de log)

- get-log-events (AWS CLI)
- Obter CWL () LogEventAWS Tools for Windows PowerShell
- GetLogEvents(CloudWatchAPI)

Excluir um log de fluxo

- delete-flow-logs (AWS CLI)
- Remove-EC2FlowLog (AWS Tools for Windows PowerShell)
- DeleteFlowLogs(API de consulta do Amazon EC2)

Monitorar gateways de trânsito

É possível usar os recursos a seguir para monitorar seus gateways de trânsito, analisar padrões de tráfego e solucionar problemas com seus gateways de trânsito.

Métricas do CloudWatch

É possível usar o Amazon CloudWatch para recuperar estatísticas sobre pontos de dados para seus gateways de trânsito como um conjunto ordenado de dados de séries temporais, conhecido como métricas. Você pode usar essas métricas para verificar se o sistema está executando conforme o esperado. Para obter mais informações, consulte Métricas do CloudWatch para os gateways de trânsito.

Logs de fluxo do Transit Gateway

É possível usar os logs de fluxo do Transit Gateway para capturar informações detalhadas sobre o tráfego da rede nos gateways de trânsito. Para obter mais informações, consulte Logs de fluxo do Transit Gateway.

VPC Flow Logs

É possível usar os logs de fluxo da VPC para capturar informações detalhadas sobre o tráfego de entrada e saída das VPCs anexadas aos gateways de trânsito. Para obter mais informações, consulte Logs de fluxo da VPC no Manual do usuário da Amazon VPC.

Logs do CloudTrail

É possível usar o AWS CloudTrail para capturar informações detalhadas sobre as chamadas feitas para a API de gateway de trânsito e armazená-las como arquivos de log no Amazon S3. Você pode usar esses logs do CloudTrail para determinar quais chamadas foram feitas, o endereço IP de origem da chamada, quem fez a chamada, quando ela foi feita, etc. Para obter mais informações, consulte Registrar em log as chamadas de API para o gateway de trânsito usando o AWS CloudTrail.

CloudWatch Events usando o Network Manager

Você pode usar o AWS Network Manager para encaminhar eventos para o CloudWatch e, em seguida, direcionar esses eventos para funções ou fluxos de destino. O Network Manager gera eventos para alterações de topologia, atualizações de roteamento e atualizações de status. Tudo isso pode ser usado para alertar você sobre alterações em seus gateways de trânsito. Para obter

mais informações, consulte Monitoramento da sua rede global com o CloudWatch Events no Guia do usuário das Redes Globais para Gateways de Trânsito da AWS.

Métricas do CloudWatch para os gateways de trânsito

A Amazon VPC publica pontos de dados no Amazon CloudWatch para seus gateways de trânsito e anexos de gateway de trânsito. O CloudWatch permite recuperar estatísticas sobre esses pontos de dados como um conjunto ordenado de dados de séries temporais, conhecidos como métricas. Considere uma métrica como uma variável a ser monitorada, e os pontos de dados como os valores dessa variável ao longo do tempo. Cada ponto de dados tem um time stamp associado e uma unidade de medida opcional.

Você pode usar métricas para verificar se o sistema está executando conforme o esperado. Por exemplo, você pode criar um alarme do CloudWatch para monitorar uma métrica específica e iniciar uma ação (como enviar uma notificação para um endereço de e-mail) se a métrica sair do que você considera um intervalo aceitável.

A Amazon VPC mede e envia suas métricas para o CloudWatch em intervalos de 60 segundos.

Para obter mais informações, consulte o Guia do usuário do Amazon CloudWatch.

Tópicos

Métricas do gateway de trânsito

O namespace `AWS/TransitGateway` inclui as métricas a seguir.

Métrica	Descrição
`BytesDropCountBlackhole`	O número de bytes removidos porque corresponderam a uma rota `blackhole` .
`BytesDropCountNoRoute`	Número de bytes removidos porque não corresponderam a uma rota.
`BytesIn`	O número de bytes recebidos pelo gateway de trânsito.

Métrica	Descrição
`BytesOut`	O número de bytes enviados do gateway de trânsito.
`PacketsIn`	O número de pacotes recebidos pelo gateway de trânsito.
`PacketsOut`	O número de pacotes enviados pelo gateway de trânsito.
`PacketDropCountBlackhole`	O número de pacotes removidos porque corresponderam a uma rota `blackhole` .
`PacketDropCountNoRoute`	Número de pacotes que caíram porque não corresponderam a uma rota.

Métricas no nível de anexo

As métricas a seguir estão disponíveis para anexos de gateway de trânsito. Todas as métricas de anexo são publicadas na conta do proprietário do gateway de trânsito. As métricas de anexo individuais também são publicadas na conta do proprietário do anexo. O proprietário do anexo só pode exibir as métricas de seu próprio anexo. Para obter mais informações sobre os tipos de anexo compatíveis, consulte the section called “Anexos de recursos”.

Métrica	Descrição
`BytesDropCountBlackhole`	O número de bytes removidos porque corresponderam a uma rota `blackhole` no anexo do gateway de trânsito.
`BytesDropCountNoRoute`	O número de bytes removidos porque não corresponderam a uma rota no anexo do gateway de trânsito.
`BytesIn`	O número de bytes recebidos pelo gateway de trânsito do anexo.
`BytesOut`	O número de bytes enviados do gateway de trânsito para o anexo.
`PacketsIn`	O número de pacotes recebidos pelo gateway de trânsito do anexo.
`PacketsOut`	O número de pacotes enviados pelo gateway de trânsito para o anexo.

Métrica	Descrição
`PacketDropCountBlackhole`	O número de pacotes removidos porque corresponderam a uma rota `blackhole` no anexo do gateway de trânsito.
`PacketDropCountNoRoute`	O número de pacotes removidos porque não corresponderam a uma rota no anexo do gateway de trânsito.

Dimensões de métricas para gateways de trânsito

Para filtrar as métricas dos gateways de trânsito, use as dimensões a seguir.

Dimensão	Descrição
`TransitGateway`	Filtra os dados da métrica pelo gateway de trânsito.
`TransitGatewayAttachment`	Filtra os dados da métrica por anexo de gateway de trânsito.

Registrar em log as chamadas de API para o gateway de trânsito usando o AWS CloudTrail

O AWS CloudTrail é um serviço que fornece um registro das ações realizadas por um usuário, função ou serviço da AWS. O CloudTrail captura todas as chamadas de API de gateway de trânsito como eventos. As chamadas capturadas incluem chamadas do AWS Management Console e chamadas de código para as operações de API de gateway de trânsito. Se você criar uma trilha, poderá habilitar a entrega contínua de eventos do CloudTrail para um bucket do Amazon S3, incluindo eventos para gateways de trânsito. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Event history (Histórico de eventos). Usando as informações coletadas pelo CloudTrail, é possível determinar a solicitação feita para a API do gateway de trânsito, o endereço IP pelo qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita, além de detalhes adicionais.

Para obter mais informações sobre as APIs de gateway de trânsito, consulte Ações do AWS Transit Gateway na Referência de API do Amazon EC2.

Para obter mais informações sobre o CloudTrail, consulte o Manual do usuário do AWS CloudTrail.

Informações de gateway de trânsito no CloudTrail

O CloudTrail é habilitado em sua conta da AWS quando ela é criada. Quando ocorre atividade por meio da API do gateway de trânsito, essa atividade é registrada em um evento do CloudTrail junto com outros eventos de serviços da AWS em Event history (Histórico de eventos). Você pode visualizar, pesquisar e fazer download de eventos recentes em sua conta da AWS. Para obter mais informações, consulte Como visualizar eventos com o histórico de eventos do CloudTrail.

Para ter um registro contínuo de eventos na sua conta da AWS, incluindo os eventos da API do gateway de trânsito, crie uma trilha. Uma trilha permite que o CloudTrail entregue arquivos de log a um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as regiões da . A trilha registra em log eventos de todas as regiões na partição da AWS e entrega os arquivos de log para o bucket do Amazon S3 especificado por você. Além disso, é possível configurar outros serviços da AWS para analisar mais ainda mais e agir com base nos dados de eventos coletados nos logs do CloudTrail. Para obter mais informações, consulte:

- Visão geral da criação de uma trilha
- Serviços e integrações compatíveis com o CloudTrail
- Configurar notificações do Amazon SNS para o CloudTrail
- Receber arquivos de log do CloudTrail de várias regiões e receber arquivos de log do CloudTrail de várias contas

Todas as chamadas para ações de gateway de trânsito são registradas pelo CloudTrail. Por exemplo, chamadas da ação `CreateTransitGateway` geram entradas nos arquivos de log do CloudTrail.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário da raiz ou do AWS Identity and Access Management.
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado.
- Se a solicitação foi feita por outro serviço da AWS.

Para obter mais informações, consulte o Elemento userIdentity do CloudTrail.

Noções básicas das entradas dos arquivos de log do gateway de trânsito

Uma trilha é uma configuração que permite a entrega de eventos como registros de log a um bucket do Amazon S3 especificado. Os arquivos de log do CloudTrail contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros de solicitação e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública. Dessa forma, eles não são exibidos em uma ordem específica.

Os arquivos de log incluem eventos para todas as chamadas de API para sua conta da AWS, não apenas chamadas de API do gateway de trânsito. É possível localizar chamadas para a API do gateway de trânsito verificando os elementos `eventSource` com o valor `ec2.amazonaws.com`. Para visualizar um registro para uma ação específica, como `CreateTransitGateway`, verifique os elementos `eventName` com o nome da ação.

Veja a seguir registros de log demonstrativos do CloudTrail para a API de gateway de trânsito para um usuário que criou um gateway de trânsito usando o console. Você pode identificar o console usando o elemento `userAgent`. Você pode identificar as chamadas de APIs solicitadas usando os elementos `eventName`. Informações sobre o usuário (`Alice`) podem ser encontradas no elemento `userIdentity`.

Example Exemplo: CreateTransitGateway

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
    },
    "eventTime": "2018-11-15T05:25:50Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "CreateTransitGateway",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "console.ec2.amazonaws.com",
```

```
    "requestParameters": {
        "CreateTransitGatewayRequest": {
            "Options": {
                "DefaultRouteTablePropagation": "enable",
                "AutoAcceptSharedAttachments": "disable",
                "DefaultRouteTableAssociation": "enable",
                "VpnEcmpSupport": "enable",
                "DnsSupport": "enable"
            },
            "TagSpecification": {
                "ResourceType": "transit-gateway",
                "tag": 1,
                "Tag": {
                    "Value": "my-tgw",
                    "tag": 1,
                    "Key": "Name"
                }
            }
        }
    },
    "responseElements": {
        "CreateTransitGatewayResponse": {
            "xmlns": "http://ec2.amazonaws.com/doc/2016-11-15/",
            "requestId": "a07c1edf-c201-4e44-bffb-3ce90EXAMPLE",
            "transitGateway": {
                "tagSet": {
                    "item": {
                        "value": "my-tgw",
                        "key": "Name"
                    }
                },
                "creationTime": "2018-11-15T05:25:50.000Z",
                "transitGatewayId": "tgw-0a13743bd6c1f5fcb",
                "options": {
                    "propagationDefaultRouteTableId": "tgw-rtb-0123cd602be10b00a",
                    "amazonSideAsn": 64512,
                    "defaultRouteTablePropagation": "enable",
                    "vpnEcmpSupport": "enable",
                    "autoAcceptSharedAttachments": "disable",
                    "defaultRouteTableAssociation": "enable",
                    "dnsSupport": "enable",
                    "associationDefaultRouteTableId": "tgw-rtb-0123cd602be10b00a"
                },
                "state": "pending",
```

```
                "ownerId": 123456789012
            }
        }
    },
    "requestID": "a07c1edf-c201-4e44-bffb-3ce90EXAMPLE",
    "eventID": "e8fa575f-4964-4ab9-8ca4-6b5b4EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
```

Identity and Access Management para gateways de trânsito

A AWS usa credenciais de segurança para identificar você e conceder acesso aos seus recursos da AWS. Você pode usar recursos do AWS Identity and Access Management (IAM) para permitir que outros usuários, serviços e aplicações usem seus recursos da AWS, totalmente ou de maneira limitada, sem compartilhar suas credenciais de segurança.

Por padrão, os usuários do IAM não têm permissão para criar, visualizar ou modificar os recursos da AWS. Para permitir que um usuário acesse recursos (como um gateway de trânsito) para executar tarefas, é necessário criar uma política do IAM que conceda permissão ao usuário para usar os recursos e as ações de API específicos de que precisa e, sem seguida, anexar a política ao grupo ao qual esse usuário pertence. Quando você anexa uma política a um usuário ou grupo de usuários, isso concede ou nega aos usuários permissão para realizar as tarefas especificadas nos recursos especificados.

Para trabalhar com um gateway de trânsito, uma das seguintes políticas gerenciadas da AWS pode atender às suas necessidades:

- AmazonEC2FullAccess
- AmazonEC2ReadOnlyAccess
- PowerUserAccess
- ReadOnlyAccess

Exemplos de políticas para gerenciar gateways de trânsito

Veja a seguir exemplos de políticas do IAM para trabalhar com gateways de trânsito.

Criar um gateway de trânsito com tags obrigatórias

O exemplo a seguir permite que os usuários criem gateways de trânsito. A chave de condição `aws:RequestTag` exige que os usuários marquem o gateway de trânsito com a tag `stack=prod`. A chave de condição `aws:TagKeys` usa o modificador `ForAllValues` para indicar que somente a chave `stack` é permitida na solicitação (nenhuma outra tag pode ser especificada). Se os usuários não passarem essa tag específica quando criarem o gateway de trânsito, ou se não especificarem tags, a solicitação falhará.

A segunda declaração usa a chave de condição `ec2:CreateAction` para permitir que os usuários criem tags somente no contexto de `CreateTransitGateway`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCreateTaggedTGWs",
            "Effect": "Allow",
            "Action": "ec2:CreateTransitGateway",
            "Resource": "arn:aws:ec2:region:account-id:transit-gateway/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/stack": "prod"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "stack"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:region:account-id:transit-gateway/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateTransitGateway"
                }
            }
        }
    ]
}
```

Trabalhar com tabelas de rotas do gateway de trânsito

O exemplo a seguir permite que os usuários criem e excluam tabelas de rotas do gateway de trânsito somente para um gateway de trânsito específico (`tgw-11223344556677889`). Os usuários também podem criar e substituir rotas em qualquer tabela de rotas do gateway de trânsito, mas somente para anexos que tenham a tag `network=new-york-office`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteTransitGatewayRouteTable",
                "ec2:CreateTransitGatewayRouteTable"
            ],
            "Resource": [
                "arn:aws:ec2:region:account-id:transit-gateway/tgw-11223344556677889",
                "arn:aws:ec2:*:*:transit-gateway-route-table/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTransitGatewayRoute",
                "ec2:ReplaceTransitGatewayRoute"
            ],
            "Resource": "arn:aws:ec2:*:*:transit-gateway-attachment/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/network": "new-york-office"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTransitGatewayRoute",
                "ec2:ReplaceTransitGatewayRoute"
            ],
            "Resource": "arn:aws:ec2:*:*:transit-gateway-route-table/*"
        }
    ]
}
```

Exemplos de políticas para gerenciar o Gerenciador de rede AWS

Para ver exemplos de políticas, consulte Exemplos de políticas para gerenciar o Network Manager no Guia do usuário do AWS Global Networks for Transit Gateways.

Use funções vinculadas ao serviço para gateways de trânsito

A Amazon VPC usa funções vinculadas a serviço para as permissões de que ela precisa para chamar outros serviços da AWS em seu nome. Para obter mais informações, consulte Usar funções vinculadas ao serviço no Guia do usuário do IAM.

Função vinculada ao serviço do gateway de trânsito

A Amazon VPC usa funções vinculadas a serviços para as permissões necessárias para chamar os outros serviços da AWS em seu nome ao trabalhar com um gateway de trânsito.

Permissões concedidas pela função vinculada ao serviço

A Amazon VPC usa a função vinculada ao serviço chamada AWSServiceRoleForVPCTransitGateway para chamar as seguintes ações em seu nome quando você trabalha com um gateway de trânsito:

- `ec2:CreateNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2:ModifyNetworkInterfaceAttribute`
- `ec2:DeleteNetworkInterface`
- `ec2:CreateNetworkInterfacePermission`
- `ec2:AssignIpv6Addresses`
- `ec2:UnAssignIpv6Addresses`

A função AWSServiceRoleForVPCTransitGateway confia nos seguintes serviços para assumir a função:

- `transitgateway.amazonaws.com`

AWSServiceRoleForVPCTransitGateway usa a política gerenciada AWSVPCTransitGatewayServiceRolePolicy.

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua uma função vinculada ao serviço. Para obter mais informações, consulte Service-linked role permissions (Permissões de função vinculada a serviços) no Guia do usuário do IAM.

Criar a função vinculada ao serviço

Não é necessário criar manualmente a função AWSServiceRoleForVPCTransitGateway. A Amazon VPC cria essa função quando você anexa uma VPC a um gateway de trânsito na sua conta.

Para que a Amazon VPC crie uma função vinculada ao serviço em seu nome, é necessário ter as permissões obrigatórias. Para obter mais informações, consulte Service-linked role permissions (Permissões de função vinculada a serviços) no Guia do usuário do IAM.

Editar a função vinculada ao serviço

É possível editar a descrição da função AWSServiceRoleForVPCTransitGateway usando o IAM. Para obter mais informações, consulte Editar uma função vinculada a serviço no Guia do usuário do IAM.

Excluir a função vinculada ao serviço

Se você não precisa mais usar o gateway de trânsito, recomendamos excluir AWSServiceRoleForVPCTransitGateway.

É possível excluir essa função vinculada ao serviço somente depois de excluir todos os anexos de VPC do gateway de trânsito da sua conta da AWS. Isso garante que você não remova por engano a permissão para acessar os anexos de VPC.

Você pode usar o console, a CLI ou a API do IAM para excluir funções vinculadas ao serviço. Para obter mais informações, consulte Excluir uma função vinculada ao serviço no Guia do usuário do IAM.

Após excluir a AWSServiceRoleForVPCTransitGateway, a Amazon VPC cria a função novamente se você anexar uma VPC a um gateway de trânsito na sua conta.

Políticas gerenciadas da AWS para transit gateways

Uma política gerenciada pela AWS é uma política independente criada e administrada pela AWS. As políticas gerenciadas pela AWS são criadas para fornecer permissões a vários casos de uso comuns a fim de que você possa começar a atribuir permissões a usuários, grupos e perfis.

Lembre-se de que as políticas gerenciadas pela AWS podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque estão disponíveis para todos os clientes da AWS usarem. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente específicas para seus casos de uso.

Você não pode alterar as permissões definidas em políticas gerenciadas pela AWS. Se a AWS atualiza as permissões definidas em um política gerenciada pela AWS, a atualização afeta todas as identidades de entidades principais (usuários, grupos e perfis) às quais a política está vinculada. É mais provável que a AWS atualize uma política gerenciada pela AWS quando um novo AWS service (Serviço da AWS) é lançado ou novas operações de API são disponibilizadas para os serviços existentes.

Para obter mais informações, consulte Políticas gerenciadas pela AWS no Manual do usuário do IAM.

Para trabalhar com um gateway de trânsito, uma das seguintes políticas gerenciadas da AWS pode atender às suas necessidades:

- AmazonEC2FullAccess
- AmazonEC2ReadOnlyAccess
- PowerUserAccess
- ReadOnlyAccess

Política gerenciada da AWS: AWSVPCTransitGatewayServiceRolePolicy

Esta política está anexada à função AWSServiceRoleForVPCTransitGateway. Isso permite que o Amazon VPC crie e gerencie recursos para seus anexos de gateway de trânsito.

Para visualizar as permissões para esta política, consulte AWSVPCTransitGatewayServiceRolePolicy na Referência de Política Gerenciada da AWS.

Atualizações do gateway de trânsito para políticas gerenciadas da AWS

Veja detalhes sobre atualizações em políticas gerenciadas pela AWS para gateways de trânsito desde que o Amazon VPC começou a rastrear essas alterações em março de 2021.

Alteração	Descrição	Data
O Amazon VPC passou a monitorar alterações	O Amazon VPC passou a controlar as alterações nas políticas gerenciadas da AWS.	1º de março de 2021

Como as network ACLs funcionam com gateways de trânsito

Uma lista de controle de acesso à rede (NACL) é uma camada opcional de segurança.

As regras de lista de controle de acesso à rede (NACL) são aplicadas de forma diferente, dependendo do cenário:

- the section called “Mesma sub-rede para instâncias do EC2 e a associação do gateway de trânsito”
- the section called “Sub-redes diferentes para instâncias do EC2 e a associação do gateway de trânsito”

Mesma sub-rede para instâncias do EC2 e a associação do gateway de trânsito

Considere uma configuração em que você tenha uma instâncias do EC2 e uma associação do gateway de trânsito que tenha a mesma sub-rede. A mesma ACL de rede é usada para o tráfego das instâncias do EC2 para o gateway de trânsito e o tráfego do gateway de trânsito para as instâncias.

As regras de NACL são aplicadas da seguinte maneira para o tráfego das instâncias para o gateway de trânsito:

- As regras de saída usam o endereço IP de destino para avaliação.
- As regras de entrada usam o endereço IP de origem para avaliação.

As regras de NACL são aplicadas da seguinte maneira para o tráfego do gateway de trânsito para as instâncias:

- As regras de saída não são avaliadas.
- As regras de entrada não são avaliadas.

Sub-redes diferentes para instâncias do EC2 e a associação do gateway de trânsito

Considere uma configuração em que você tem instâncias do EC2 em uma sub-rede e uma associação de gateway de trânsito em uma sub-rede diferente, e cada sub-rede está associada a uma ACL de rede diferente.

As regras de ACL de rede são aplicadas da seguinte forma para a sub-rede da instância do EC2:

- As regras de saída usam o endereço IP de destino para avaliar o tráfego das instâncias para o gateway de trânsito.
- As regras de entrada usam o endereço IP de origem para avaliar o tráfego do gateway de trânsito para as instâncias.

As regras de NACL são aplicadas da seguinte maneira para a sub-rede do gateway de trânsito:

- As regras de saída usam o endereço IP de destino para avaliar o tráfego do gateway de trânsito para as instâncias.
- As regras de saída não são usadas para avaliar o tráfego das instâncias para o gateway de trânsito.
- As regras de entrada usam o endereço IP de origem para avaliar o tráfego das instâncias para o gateway de trânsito.
- As regras de entrada não são usadas para avaliar o tráfego do gateway de trânsito para as instâncias.

Melhores práticas

Use uma sub-rede separada para cada anexo da VPC do gateway. Para cada sub-rede, use um CIDR pequeno, por exemplo /28, para que você tenha mais endereços para recursos do EC2. Ao usar uma sub-rede separada, é possível configurar o seguinte:

- Mantenha aberta a NACL de entrada e saída associada às sub-redes do gateway de trânsito.
- Dependendo do fluxo de tráfego, é possível aplicar NACLs às sub-redes de workload.

Para obter mais informações sobre como os anexos da VPC funcionam, consulte the section called “Anexos de recursos”.

Cotas para os gateways de trânsito

Você Conta da AWS tem as seguintes cotas (anteriormente chamadas de limites) relacionadas aos gateways de trânsito. A menos que especificado de outra forma, cada cota é específica da região .

O console do Service Quotas fornece informações sobre as cotas para sua conta. É possível usar o console do Service Quotas para visualizar cotas padrão e solicitar aumentos de cota para cotas ajustáveis. Para obter mais informações, consulte Solicitar um aumento da cota no Guia do usuário do Service Quotas.

Se uma cota ajustável ainda não estiver disponível em Service Quotas, você poderá abrir um caso de suporte.

Geral

Nome	Padrão	Ajustável
Gateways de trânsito por conta	5	Sim
Blocos CIDR por gateway de trânsito	5	Não

Os blocos CIDR são usados no recurso the section called “Anexos do Connect e pares do Connect”.

Roteamento

Nome	Padrão	Ajustável
Tabelas de rotas de gateway de trânsito por gateway de trânsito	20	Sim
Total de rotas combinadas (dinâmicas e estáticas) em todas as tabelas de rotas para um só gateway de trânsito	10.000	Sim
Rotas dinâmicas anunciadas por um dispositivo do roteador virtual para um par do Connect	1.000	Sim

Nome	Padrão	Ajustável
Rotas anunciadas por um par Connect em um gateway de trânsito para um dispositivo do roteador virtual	5.000	Não
Rotas estáticas de um prefixo para um único anexo	1	Não

As rotas publicadas vêm da tabela de rotas associada ao anexo do Connect.

Anexos do gateway de trânsito

Um transit gateway não pode ter mais de um anexo à mesma VPC.

Nome	Padrão	Ajustável
Anexos por gateway de trânsito	5.000	Não
Gateways de trânsito por VPC	5	Não
Anexos de emparelhamento por gateway de trânsito	50	Sim
Anexos de emparelhamento pendentes por gateway de trânsito	10	Sim
Emparelhamento de anexos entre dois gateways de trânsito ou entre um gateway de trânsito e uma borda de rede central (CNE) do Cloud WAN	1	Não
Pares do Connect (túneis GRE) por anexo do Connect	4	Não

Largura de banda

Há muitos fatores que podem afetar a largura de banda realizada por meio de uma conexão Site-to-Site VPN, incluindo, mas não limitado a: tamanho do pacote, combinação de tráfego (TCP/UDP), políticas de controle de utilização em redes intermediárias, clima da Internet e requisitos específicos de aplicações. Para anexos de VPC, os gateways da AWS Direct Connect , ou anexos do gateway de trânsito emparelhado, tentaremos fornecer largura de banda adicional além do valor padrão.

Nome	Padrão	Ajustável
Largura de banda por anexo de VPC por zona de disponibilidade	Até 100 Gbps	Entre em contato com seu arquiteto de soluções (SA) ou gerente técnico de contas (TAM) para obter mais assistênc ia.
Pacotes por segundo por anexo de VPC do gateway de trânsito, por zona de disponibi lidade	Até 7.500.000	Entre em contato com seu arquiteto de soluções (SA) ou gerente técnico de contas (TAM) para obter mais assistênc ia.
Largura de banda para conexão de AWS Direct Connect gateway ou gateway de trânsito emparelhado por zona de disponibilidade disponível na região	Até 100 Gbps	Entre em contato com seu arquiteto de soluções (SA) ou gerente técnico de contas (TAM) para obter mais assistênc ia.
Pacotes por segundo por anexo de gateway de trânsito (AWS Direct Connect e anexos de emparelhamento) por zona de disponibilidade disponível na região	Até 7.500.000	Entre em contato com seu arquiteto de soluções (SA) ou gerente técnico de

Nome	Padrão	Ajustável
		contas (TAM) para obter mais assistênc ia.
Largura de banda máxima por túnel de VPN	Até 1,25 Gbps	Não
Máximo de pacotes por segundo por túnel da VPN	Até 140.000	Não
Largura de banda máxima por par do Connect (túnel GRE) por anexo do Connect	Até 5 Gbps	Não
Máximo de pacotes por segundo por par do Connect	Até 300.000	Não

É possível usar o roteamento multipath de custo igual (ECMP) para obter uma largura de banda maior de VPN ao agregar vários túneis de VPN. Para usar o ECMP, a conexão VPN deve ser configurada para roteamento dinâmico. O ECMP não é compatível com conexões VPN que usam roteamento estático.

Você pode criar até 4 Connect peers por anexo Connect (até 20 Gbps na largura de banda total por anexo Connect), desde que o anexo de transporte subjacente (VPC ou AWS Direct Connect) suporte a largura de banda necessária. Você pode usar o ECMP para obter uma largura de banda maior com o dimensionamento horizontal em vários pares do Connect no mesmo anexo do Connect ou em vários anexos do Connect no mesmo gateway de trânsito. O gateway de trânsito não pode usar o ECMP entre os emparelhamentos BGP do mesmo par do Connect.

AWS Direct Connect gateways

Nome	Padrão	Ajustável
AWS Direct Connect gateways por gateway de trânsito	20	Não
Gateways de trânsito por AWS Direct Connect gateway	6	Não

A unidade de transmissão máxima (MTU).

- A MTU de uma conexão de rede é o tamanho, em bytes, do maior pacote permitido que pode ser passado pela conexão. Quanto maior a MTU de uma conexão, mais dados podem ser passados em um único pacote. Um gateway de trânsito suporta uma MTU de 8500 bytes para tráfego entre VPCs, Transit AWS Direct Connect Gateway Connect e anexos de emparelhamento. O tráfego que passa pelas conexões VPN pode ter uma MTU de 1.500 bytes.
- Na migração do emparelhamento da VPC para o uso de um transit gateway, a incompatibilidade de tamanho da MTU entre o emparelhamento e o transit gateway pode fazer com que alguns pacotes do tráfego assimétrico sejam descartados. Atualize ambas as VPCs ao mesmo tempo para evitar o descarte de pacotes jumbo devido à incompatibilidade de tamanho.
- Pacotes com um tamanho maior que 8500 bytes que chegam ao gateway de trânsito são descartados.
- O gateway de trânsito não gera o FRAG_NEEDED para o pacote ICMPv4, ou o Packet Too Big (PTB) para o pacote ICMPv6. Consequentemente, o Path MTU Discovery (PMTUD) não é compatível.
- O gateway de trânsito aplica o ajuste do tamanho máximo de segmento (MSS) a todos os pacotes. Para obter mais informações, consulte RFC879.
- Para obter detalhes sobre as cotas de Site-to-Site VPN para MTU, consulte Unidade máxima de transmissão (MTU) no Guia do usuário do AWS Site-to-Site VPN .

Multicast

Nome	Padrão	Ajustável
Número de domínios multicast por gateway de trânsito	20	Sim
Interfaces de rede multicast por gateway de trânsito	10.000	Sim
Associações de domínio de multicast por VPC	20	Sim
Fontes por grupo multicast do gateway de trânsito	1	Sim

Nome	Padrão	Ajustável
Membros e origens do grupo multicast estático e do grupo multicast IGMPv2 por gateway de trânsito	10.000	Não
Membros do grupo multicast estático e do grupo multicast IGMPv2 por grupo multicast de gateway de trânsito	100	Não
Throughput de multicast máxima por fluxo	1 Gbps	Não
Throughput de multicast máxima agregada por zona de disponibilidade	20 Gbps	Não

AWS Gerente de rede

Nome	Padrão	Ajustável
Redes globais por Conta da AWS	5	Sim
Dispositivos por rede global	200	Sim
Links por rede global	200	Sim
Lugares por rede global	200	Sim
Conexões por rede global	500	Não

Recursos de cota adicionais

Para obter mais informações, consulte:

- Cotas do Site-to-Site VPN no Manual do usuário do AWS Site-to-Site VPN
- Cotas da Amazon VPC no Manual do usuário da Amazon VPC
- Cotas do AWS Direct Connect no Manual do usuário do AWS Direct Connect

Histórico do documento dos gateways de trânsito

A tabela a seguir descreve as versões dos gateways de trânsito.

Alteração	Descrição	Data
Cotas de gateways de trânsito da AWS	Limites de largura de banda foram adicionados.	14 de agosto de 2023
Logs de fluxo do AWS Transit Gateway	Os gateways de trânsito agora são compatíveis com os logs de fluxo do Transit Gateway, permitindo monitorar e registrar tráfego de rede entre gateways de trânsito.	14 de julho de 2022
Tabelas de políticas de gateway de trânsito	Use tabelas de políticas para configurar roteamento dinâmico para gateways de trânsito para troca automática informações de roteamento e acessibilidade com os tipos de gateway de trânsito emparelhados.	13 de julho de 2022
Guia do usuário do Gerenciador de rede	O Network Manager foi criado como um guia autônomo e não está mais incluído como parte do Guia do usuário do AWS Transit Gateway.	2 de dezembro de 2021
Anexos de emparelhamento	É possível criar uma conexão de emparelhamento com um transit gateway na mesma Região.	1º de dezembro de 2021
Transit Gateway Connect	Você pode estabelecer uma conexão entre um gateway de	10 de dezembro de 2020

	trânsito e dispositivos virtuais de terceiros em execução na VPC.	
Modo do dispositivo	É possível habilitar o modo do dispositivo em um anexo da VPC para garantir que o tráfego bidirecional flua pela mesma zona de disponibi lidade para o anexo.	29 de outubro de 2020
Referências da lista de prefixos	É possível fazer referência a uma lista de prefixos na tabela de rotas do gateway de trânsito.	24 de agosto de 2020
Modificar gateway de trânsito	É possível modificar as opções de configuração do gateway de trânsito.	24 de agosto de 2020
Métricas do CloudWatch para anexos do gateway de trânsito	É possível visualizar as métricas do CloudWatch para anexos de gateway de trânsito individuais.	6 de julho de 2020
Route Analyzer do Network Manager	É possível analisar as rotas nas tabelas de rotas do gateway de trânsito na rede global.	4 de maio de 2020
Anexos de emparelhamento	É possível criar uma conexão de emparelhamento com um gateway de trânsito em outra região.	3 de dezembro de 2019

Suporte a multicast	O Transit Gateway oferece suporte ao roteamento de tráfego multicast entre sub-redes de VPCs anexadas e serve como um roteador multicast para instâncias que enviam tráfego destinado a várias instâncias de recebimento.	3 de dezembro de 2019
Gerenciador de rede AWS	É possível visualizar e monitorar as redes globais criadas em torno de gateways de trânsito.	3 de dezembro de 2019
Suporte do AWS Direct Connect	É possível usar um gateway do AWS Direct Connect para criar uma conexão do AWS Direct Connect por meio de uma interface virtual de trânsito às VPCs ou VPNs anexadas ao seu gateway de trânsito.	27 de março de 2019
Versão inicial	Esta versão apresenta gateways de trânsito.	26 de novembro de 2018

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.