AWS Transit Gateway

Amazon VPC

Amazon VPC: AWS Transit Gateway

Table of Contents

O que são Gateways de trânsito da Amazon VPC?

O Amazon VPC Transit Gateways é um hub de trânsito de rede usado para interconectar nuvens privadas virtuais (VPCs) e redes locais. À medida que sua infraestrutura de nuvem se expande globalmente, o peering entre regiões conecta os gateways de trânsito usando a infraestrutura global. 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: é possível anexar:
  - Um ou mais VPCs
  - Um dispositivo de rede Connect SD-WAN/de terceiros
  - Uma AWS Direct Connect porta de entrada
  - Uma conexão de emparelhamento com outro gateway de trânsito
  - Uma conexão VPN a um gateway de trânsito
  - Um anexo de função de rede. Para obter mais informações, consulte the section called “Anexos de função de rede”.
- Unidade de transmissão máxima (MTU) 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 suporta uma MTU de 8500 bytes para tráfego entre VPCs, AWS Direct Connect, Transit Gateway Connect e anexos de emparelhamento (anexos de emparelhamento intra-região, inter-região e Cloud WAN). 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, é necessário 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
- Começando a usar os gateways de trânsito
- 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.
- AWS Interface de linha de comando (AWS CLI) — Fornece comandos para um amplo conjunto de AWS serviços, incluindo Amazon VPC, e é compatível com Windows, macOS e Linux. Para obter mais informações, consulte AWS Command Line Interface.
- AWS SDKs— fornece operações de API específicas do idioma e cuida de muitos detalhes da conexão, como calcular assinaturas, lidar com novas tentativas de solicitação e lidar com 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 Amazon EC2 API Reference.

Preços

A cobrança por cada anexo em um gateway de trânsito e pela quantidade de tráfego processada no gateway de trânsito é feita por hora. Para obter mais informações, consulte Preços do AWS Transit Gateway.

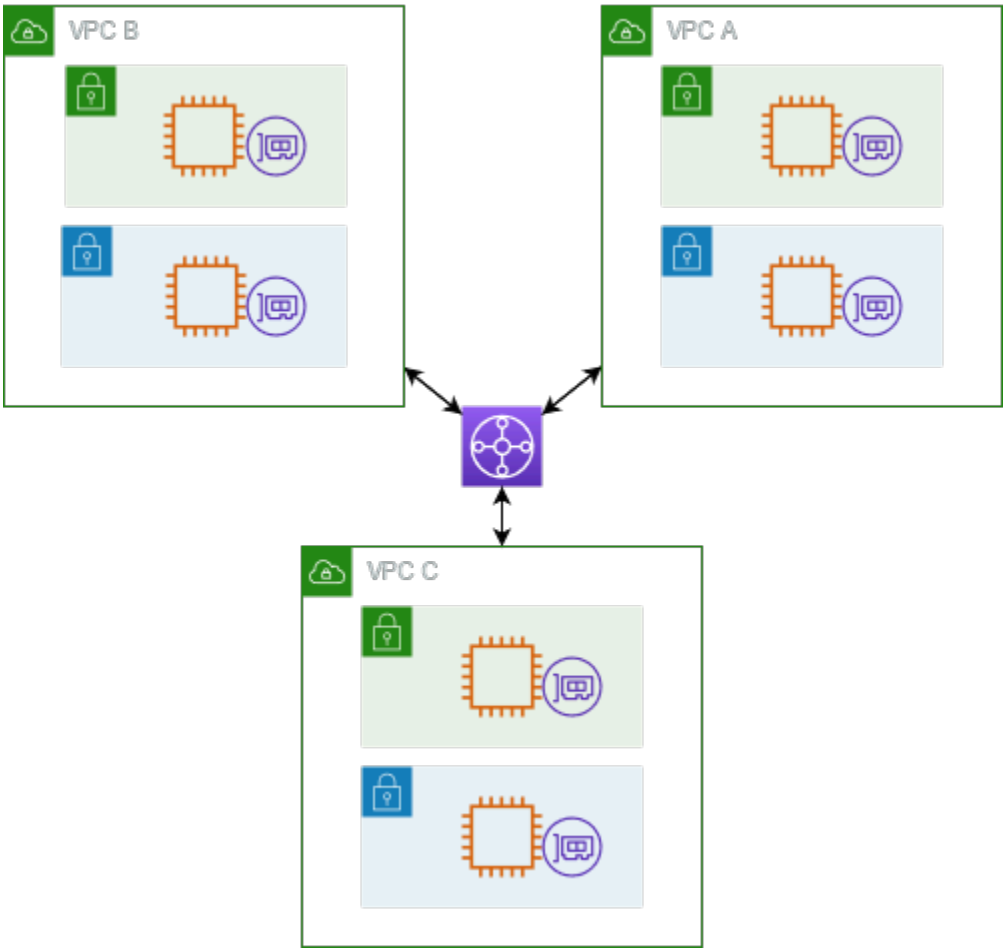
Como o Amazon VPC Transit Gateways funciona

No AWS Transit Gateway, um gateway de trânsito atua como um roteador virtual regional para o tráfego que flui entre suas nuvens privadas virtuais (VPCs) e redes locais. 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.

Tópicos

Exemplo de diagrama de arquitetura

O diagrama a seguir mostra um gateway de trânsito com três anexos de VPC. A tabela de rotas para cada uma delas VPCs inclui a rota local e as rotas que enviam o tráfego destinado às outras duas VPCs para o 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.

Destino	Alvo	Tipo de rota
VPC A CIDR	*Attachment for VPC A*	com propagação
VPC B CIDR	*Attachment for VPC B*	com propagação
VPC C CIDR	*Attachment for VPC C*	com propagação

Anexos de recursos

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

- Um 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 gateway de trânsito se uma sub-rede estiver ativada na mesma zona. Se a tabela de rotas de uma sub-rede incluir uma rota para o gateway de trânsito, o tráfego só será enviado ao gateway se este 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

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, é possível 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: a VPC não oferece suporte a ECMP, pois não pode haver sobreposição entre os blocos CIDR. Por exemplo, não é possível 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 Compatibilidade com ECMP para 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. Também não é possível configurar a mesma rota estática em dois destinos diferentes.

> **Note**
>
> - O BGP Multipath AS-Path Relax não é suportado, então você não pode usar o ECMP em diferentes Números de Sistema Autônomo (). ASNs
> - Não há compatibilidade com ECMP entre diferentes tipos de anexos. Por exemplo, não é possível 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 obter 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, recomenda-se que somente um gateway do Direct Connect seja configurado e usado, em vez de configurar e usar vários gateways, aproveitando, assim, o recurso ECMP. Para obter mais informações sobre gateways Direct Connect e interfaces virtuais públicas, consulte Como faço para configurar uma conexão Active/Active ou Active/Passive Direct Connect a AWS partir de uma interface virtual pública? .

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 de 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.

Recomenda-se que várias zonas de disponibilidade sejam habilitadas, para garantir a disponibilidade.

Usar o suporte ao modo de dispositivo

Se há planos para configurar um dispositivo de rede com estado na VPC, é possível 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 obter mais informações, consulte Exemplo: dispositivo em uma VPC de serviços compartilhados.

Roteamento

Seu gateway de trânsito encaminha IPv4 e IPv6 empacota entre anexos usando tabelas de rotas de gateway de trânsito. Você pode configurar essas tabelas de rotas para propagar rotas das tabelas de rotas para as conexões VPN conectadas VPCs e os gateways Direct Connect. Também é possível 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.

Tópicos de roteamento

- Tabelas de rotas
- Associação da tabela de rotas
- Propagação de rotas
- Rotas para anexos de emparelhamento
- Ordem de avaliação de rotas

Tabelas de rotas

O 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. Se você desabilitar a propagação de rotas e a associação da tabela de rotas, AWS não cria uma tabela de rotas padrão para o gateway de trânsito. No entanto, se a propagação

de rotas ou a associação de tabelas de rotas estiverem ativadas, AWS criará uma tabela de rotas padrão.

É possível criar tabelas de rotas adicionais para o gateway de trânsito. Assim, pode-se 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, é necessário adicionar uma rota à 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. Ao 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 no 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 na 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 CIDR, mas de tipos de anexos diferentes, a prioridade da rota será a seguinte:
  - Rotas estáticas (por exemplo, rotas estáticas de 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
  - Site-to-Site VPN em rotas privadas propagadas pelo Direct Connect
  - Site-to-Site Rotas propagadas por VPN
  - Rotas propagadas pelo emparelhamento do Transit Gateway (Cloud WAN)

Alguns anexos oferecem suporte à publicidade de rotas pelo BGP. Para as rotas com o mesmo CIDR e do mesmo tipo de anexo, a prioridade da rota será controlada pelos atributos do BGP:

- Tamanho do caminho AS mais curto
- Menor valor de MED

- As rotas eBGP sobre iBGP são preferidas, se forem compatíveis com o anexo

> **Important**
>
> - AWS não é possível garantir uma ordem consistente de priorização de rotas para rotas BGP com o mesmo CIDR, tipo de anexo e atributos de BGP listados acima.
> - Para rotas anunciadas em um gateway de trânsito sem MED, o AWS Transit Gateway atribuirá os seguintes valores padrão:
>   - 0 para rotas de entrada anunciadas nos anexos do Direct Connect.
>   - 100 para rotas de entrada anunciadas em anexos VPN e Connect.

AWS O Transit Gateway mostra apenas uma rota preferencial. Uma rota de backup só aparecerá na tabela de rotas do Transit Gateway se a rota anteriormente ativa não for mais anunciada — por exemplo, se você estiver anunciando as mesmas rotas pelo gateway Direct Connect e pela Site-to-Site VPN. AWS O Transit Gateway mostrará somente as rotas recebidas da rota do gateway Direct Connect, que é a rota preferencial. A Site-to-Site VPN, que é a rota de backup, só será exibida quando o gateway Direct Connect não for mais anunciado.

Diferenças da tabela de rotas do gateway de trânsito e VPC

A avaliação da tabela de rotas difere caso uma tabela de rotas VPC ou uma tabela de rotas de gateway de trânsito sejam usadas.

O exemplo a seguir mostra uma tabela de rotas 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	Prioridade
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

Destino	Destino	Prioridade
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 de gateway de trânsito. Caso o anexo do gateway do AWS Direct Connect seja preferido ao anexo de VPN, use uma conexão VPN do BGP e propague as rotas na tabela de rotas do gateway de trânsito.

Destino	Anexo (Alvo)	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
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	Connect	Com propagação	4
172.31.0.0/16	tgw-attach-789 | vpn-5678	VPN	Com propagação	5

Anexos de função de rede

Um anexo de função de rede é um recurso que conecta uma função de segurança de rede — por exemplo, um AWS Network Firewall anexo — diretamente ao seu gateway de trânsito. Ele elimina a necessidade de criar e gerenciar manualmente a inspeção VPCs.

Com um anexo de função de rede:

- AWS cria e gerencia automaticamente a infraestrutura subjacente

- O tráfego pode ser inspecionado à medida que flui pelo seu gateway de trânsito
- As políticas de segurança são aplicadas de forma consistente em toda a sua rede

- Você pode direcionar o tráfego pelo firewall usando regras de roteamento simples
- O anexo funciona em várias zonas de disponibilidade para alta disponibilidade

Essa integração simplifica a segurança da rede, permitindo que você conecte firewalls diretamente ao seu gateway de trânsito, em vez de criar configurações de roteamento complexas e gerenciar endpoints separados por meio de configurações separadas. VPCs

AWS Network Firewall integração

AWS Network Firewall a integração permite que você conecte um firewall na forma de um grupo de endpoints do Gateway Load Balancer, um por zona de disponibilidade, em uma VPC de buffer gerenciada por serviços. Um anexo do Network Firewall é criado com o modo appliance ativado automaticamente. Isso elimina a necessidade de gerenciar explicitamente a inspeção VPCs.

Com a integração do Firewall de Rede, você não precisa mais criar e gerenciar a inspeção VPCs para suas implantações do Firewall de Rede. Em vez de selecionar uma VPC e sub-redes ao criar seu firewall, você seleciona diretamente o Transit Gateway e provisiona e gerencia AWS automaticamente todos os recursos necessários nos bastidores. Você verá um novo anexo de função de rede do Transit Gateway em vez de um endpoint de firewall individual.

Para cenários de várias contas, o Transit Gateway pode ser compartilhado pela RAM do proprietário do Transit Gateway para a conta do proprietário do Network Firewall, permitindo que qualquer uma das contas gerencie o anexo do firewall. Quando o firewall e o anexo estiverem prontos, você pode simplesmente modificar as tabelas de rotas do Transit Gateway para enviar tráfego ao anexo para inspeção.

> **Note**
>
> - O Transit Gateway suporta somente roteamento estático em anexos do Firewall de Rede.
> - Não há suporte para firewalls de terceiros.

Para obter mais informações sobre firewalls e anexos, consulte Anexos da função de rede do Transit Gateway.

Exemplos de cenários de gateway de trânsito

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

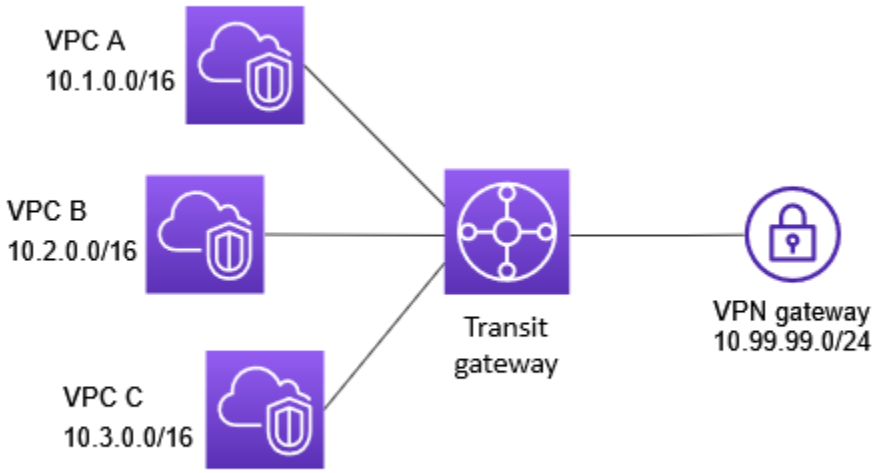
Exemplo: Roteador centralizado

Você pode configurar seu gateway de trânsito como um roteador centralizado que conecta todas as suas VPCs conexões e Site-to-Site VPN. AWS Direct Connect 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.

Sumário

Visão geral

O diagrama a seguir mostra os principais componentes da configuração deste cenário. Nesse cenário, há três anexos de VPC e um anexo de Site-to-Site VPN no 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, consulte Criar uma VPC no Guia do usuário da 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 de VPC”.
- Um anexo de 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 está ativa, a sessão BGP é estabelecida e o Site-to-Site VPN CIDR se propaga para a tabela de rotas do gateway de trânsito e a VPC CIDRs é adicionada à tabela BGP do gateway do cliente. Para obter mais informações, consulte the section called “Criar um anexo do gateway de trânsito para 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 entrada padrão para IPv4 roteamento local na VPC; essa entrada permite que as instâncias dessa VPC se comuniquem entre si. A segunda entrada encaminha todos os outros tráfegos de IPv4 sub-rede para o 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

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

Destino	Alvo	Tipo de rota
10.1.0.0/16	*Attachment for VPC A*	com propagação
10.2.0.0/16	*Attachment for VPC B*	com propagação
10.3.0.0/16	*Attachment for VPC C*	com propagação
10.99.99.0/24	*Attachment for VPN connection*	com propagação

Tabela do BGP do gateway do cliente

A tabela BGP do gateway do cliente contém a seguinte VPC. CIDRs

- 10.1.0.0/16

- 10.2.0.0/16
- 10.3.0.0/16

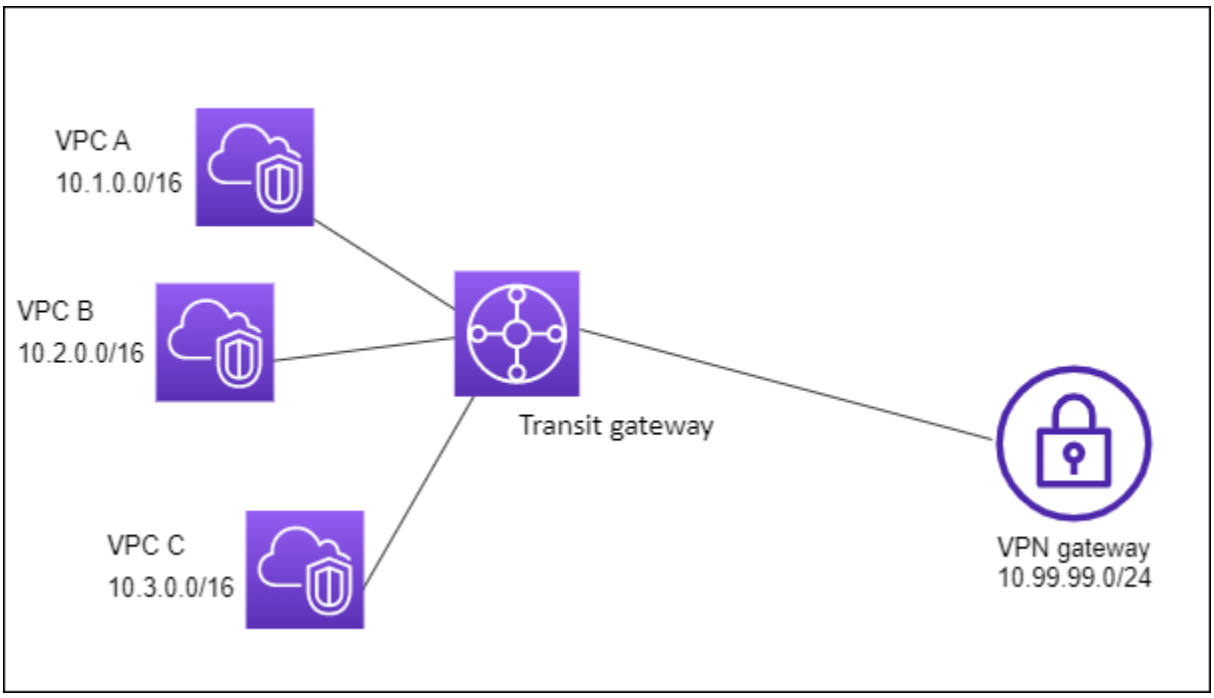
Exemplo: Isolado VPCs

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.

Conteúdo

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. Pacotes das sub-redes na VPC A, na VPC B e na VPC C que têm a Internet como destino primeiro passam pelo gateway de trânsito e depois são roteados para a conexão VPN (se Site-to-Site o destino estiver dentro dessa 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, consulte Criar uma VPC no Guia do usuário da Amazon VPC.
- Um gateway de trânsito Para obter mais informações, consulte the section called “Criar um gateway de trânsito”.
- Três acessórios no gateway de trânsito para os três. VPCs Para obter mais informações, consulte the section called “Criar um anexo de VPC”.
- Um anexo de Site-to-Site VPN no gateway de trânsito. Para obter mais informações, consulte the section called “Criar um anexo do gateway de trânsito para 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 está ativa, a sessão BGP é estabelecida e o VPN CIDR se propaga para a tabela de rotas do gateway de trânsito e a VPC CIDRs é adicionada à tabela 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 a VPCs e outra 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 entrada padrão para IPv4 roteamento local na VPC. Essa entrada permite que as instâncias nesta VPC se comuniquem entre si. A segunda entrada encaminha todos os outros tráfegos de IPv4 sub-rede para o 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 a 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	Alvo	Tipo de rota
10.99.99.0/24	*Attachment for VPN connection*	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	Alvo	Tipo de rota
10.1.0.0/16	*Attachment for VPC A*	com propagação
10.2.0.0/16	*Attachment for VPC B*	com propagação

Destino	Alvo	Tipo de rota
10.3.0.0/16	*Attachment for VPC C*	com propagação

Para obter mais informações sobre como propagar rotas em uma tabela de rotas do gateway de trânsito, consulte Habilitar a propagação de rota para uma tabela de rotas do gateway de trânsito usando Amazon VPC Transit Gateways.

Tabela do BGP do gateway do cliente

A tabela BGP do gateway do cliente contém a seguinte VPC. CIDRs

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

Exemplo: isolado VPCs com serviços compartilhados

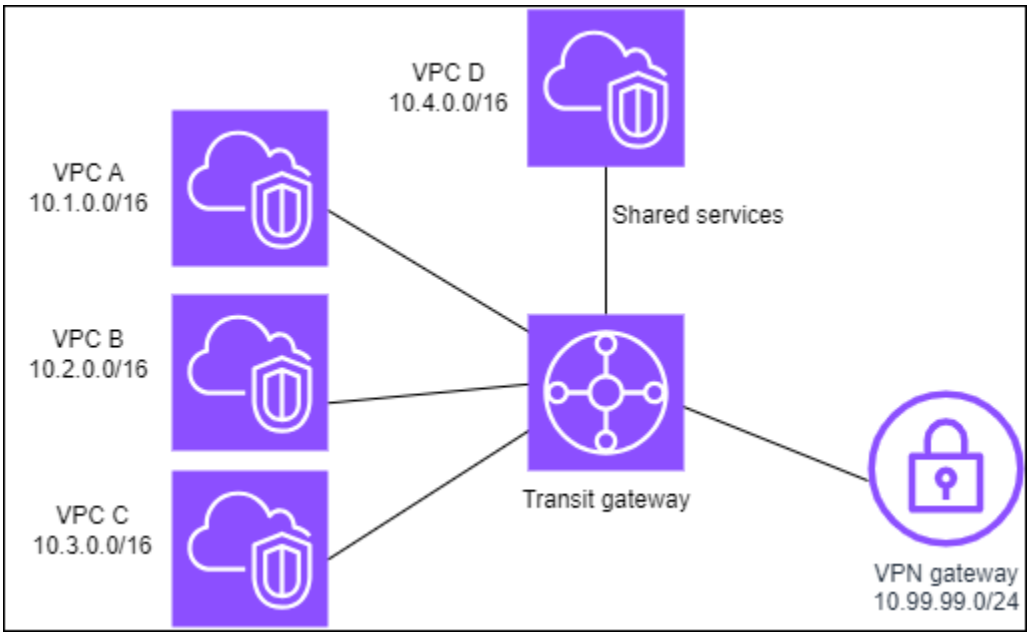
É possível configurar seu gateway de trânsito como vários roteadores isolados que usam um serviço compartilhado. É semelhante ao uso de vários gateways de trânsito, mas permite mais flexibilidade nos casos em que as rotas e os anexos puderem mudar. Nesse cenário, cada roteador isolado tem uma única tabela 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. É possível usar este cenário quando tiver grupos que precisam ser isolados, mas que usam um serviço compartilhado, como um sistema de produção.

Conteúdo

Visão geral

O diagrama a seguir mostra os principais componentes da configuração deste cenário. Os pacotes das sub-redes na VPC A, na VPC B e na VPC C que têm a Internet como destino são roteados

primeiro pelo gateway de trânsito e depois pelo gateway do cliente para VPN. Site-to-Site 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, consulte Criar uma VPC no Guia do usuário da 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 de VPC”.
- Um anexo de Site-to-Site VPN no gateway de trânsito. Para obter mais informações, consulte the section called “Criar um anexo do gateway de trânsito para 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 está ativa, a sessão BGP é estabelecida e o VPN CIDR se propaga para a tabela de rotas do gateway de trânsito e a VPC CIDRs é adicionada à tabela 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 a e outra para a conexão VPN VPCs 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 de IPv4 sub-rede para o gateway de trânsito.

Destino	Destino
10.1.0.0/16	local
0.0.0.0/0	*transit gateway ID*

Tabela de rotas do gateway de trânsito

Esse cenário usa uma tabela de rotas para a 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	Alvo	Tipo de rota
10.99.99.0/24	*Attachment for VPN connection*	com propagação
10.4.0.0/16	*Attachment for 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 a comunicação VPCs entre a conexão VPN e a VPC de serviços compartilhados.

Destino	Alvo	Tipo de rota
10.1.0.0/16	*Attachment for VPC A*	com propagação
10.2.0.0/16	*Attachment for VPC B*	com propagação
10.3.0.0/16	*Attachment for VPC C*	com propagação

Para obter mais informações, consulte Habilitar a propagação de rota para uma tabela de rotas do gateway de trânsito usando Amazon VPC Transit Gateways.

Tabela do BGP do gateway do cliente

A tabela BGP do gateway do cliente contém o CIDRs para todos os quatro. VPCs

Exemplo: Gateways de trânsito em pares

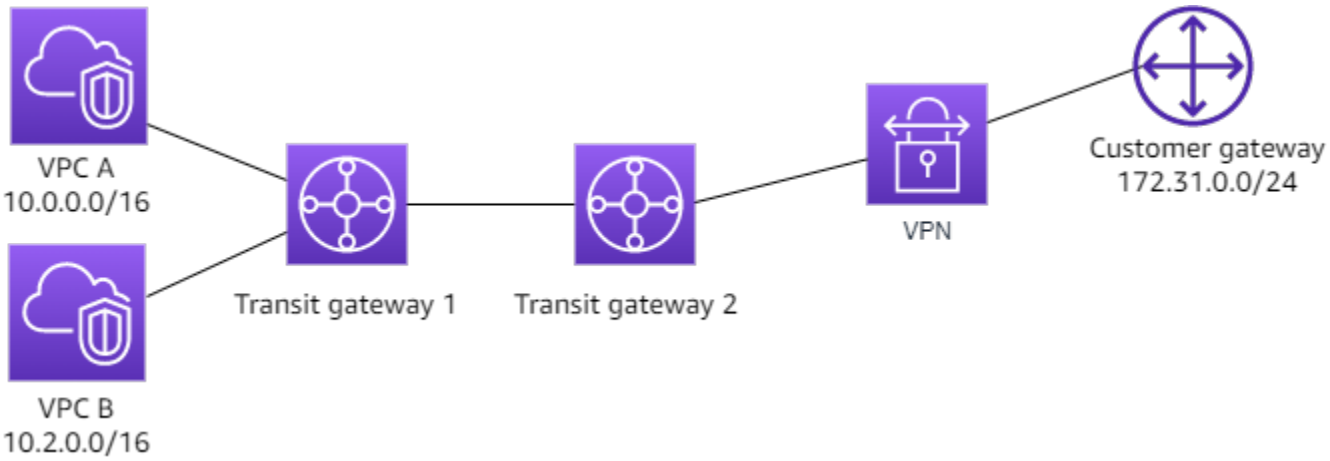
É possível criar uma conexão de emparelhamento de transit gateway entre transit gateways. Depois, é possível rotear o tráfego entre os anexos para cada um dos gateways de trânsito. Nesse cenário, todos os anexos da VPC e da VPN estão associados à tabela de rotas padrão do gateway de trânsito e são propagados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

Conteúdo

Visão geral

O diagrama a seguir mostra os principais componentes da configuração deste cenário. O Transit Gateway 1 tem dois anexos de VPC e o Transit Gateway 2 tem um anexo de VPN. Site-to-Site 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:

- Dois VPCs. Para obter mais informações, consulte Criar uma VPC no Guia do usuário da Amazon VPC.
- Dois gateways de trânsito. 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 de VPC”.
- Um anexo de Site-to-Site VPN no segundo gateway de trânsito. Para obter mais informações, consulte the section called “Criar um anexo do gateway de trânsito para 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 de gateway de trânsito no Amazon VPC Transit Gateways.

Quando você cria os anexos da VPC, os de CIDRs 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 Site-to-Site VPN CIDR se propaga para a tabela de rotas do gateway de trânsito 2
- As VPC CIDRs são adicionadas à tabela 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 entrada padrão para IPv4 roteamento local na VPC. Essa entrada padrão permite que os recursos nessa VPC se comuniquem entre si. A segunda entrada encaminha todos os outros tráfegos de IPv4 sub-rede para o 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	Alvo	Tipo de rota
10.0.0.0/16	*Attachment ID for VPC A*	com propagação
10.2.0.0/16	*Attachment ID for VPC B*	com propagação
0.0.0.0/0	*Attachment ID for peering connection*	estático

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

Destino	Alvo	Tipo de rota
172.31.0.0/24	*Attachment ID for VPN connection*	com propagação
10.0.0.0/16	*Attachment ID for peering connection*	estática
10.2.0.0/16	*Attachment ID for peering connection*	estático

Tabela do BGP do gateway do cliente

A tabela BGP do gateway do cliente contém a seguinte VPC. CIDRs

- 10.0.0.0/16
- 10.2.0.0/16

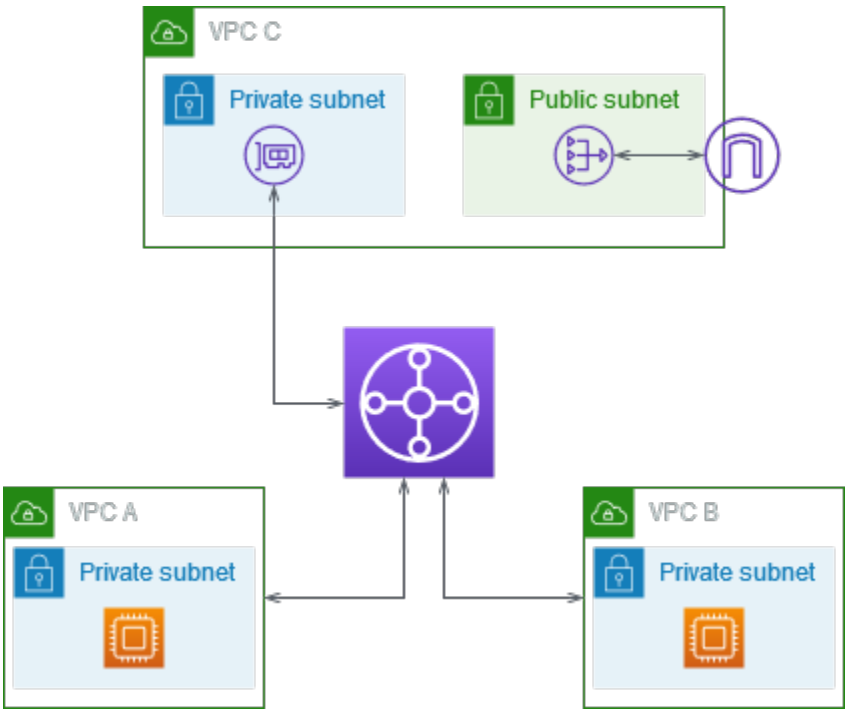
Exemplo: Roteamento de saída centralizado para a Internet

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.

Conteúdo

Visão geral

O diagrama a seguir mostra os principais componentes da configuração deste cenário. Há aplicativos na VPC A e na VPC B que precisam de acesso à Internet apenas de saída. Configure 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 tudo 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 roteie o tráfego para o gateway da Internet.



Recursos

Crie os seguintes recursos para este cenário:

- Três VPCs com intervalos de endereços IP que não são idênticos nem se sobrepõem. Para obter mais informações, consulte Criar uma VPC no Guia do usuário da Amazon VPC.
- Cada VPC A e VPC B têm sub-redes privadas com instâncias. 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 de VPC”. Para a VPC C, é necessário criar o anexo usando a sub-rede privada. Se o anexo for cirado 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 gateway de trânsito

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 de IPv4 sub-rede para o gateway de trânsito.

Destino	Destino
VPC A CIDR	local
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 de IPv4 sub-rede para o gateway de trânsito.

Destino	Destino

Destino	Destino
VPC B CIDR	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. A entrada restante encaminha todos os outros tráfegos de IPv4 sub-rede para o gateway da Internet.

Destino	Destino
VPC C CIDR	local
VPC A CIDR	*transit-gateway-id*
VPC B CIDR	*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 encaminha todos os outros tráfegos de IPv4 sub-rede para o gateway NAT.

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

Tabela de rotas do gateway de trânsito

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. Opcionalmente, também é possível impedir a comunicação entre as VPCs adicionando uma rota blackhole para cada CIDR de VPC.

CIDR	Attachment	Tipo de rota
VPC A CIDR	*Attachment for VPC A*	com propagação
VPC B CIDR	*Attachment for VPC B*	com propagação
VPC C CIDR	*Attachment for VPC C*	com propagação
0.0.0.0/0	*Attachment for VPC C*	estático

Exemplo: dispositivo em uma VPC de serviços compartilhados

É possível 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 houver vários gateways de trânsito na arquitetura, cada um deles mantém a própria afinidade de sessão e pode selecionar uma interface de rede diferente.

É necessário 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.

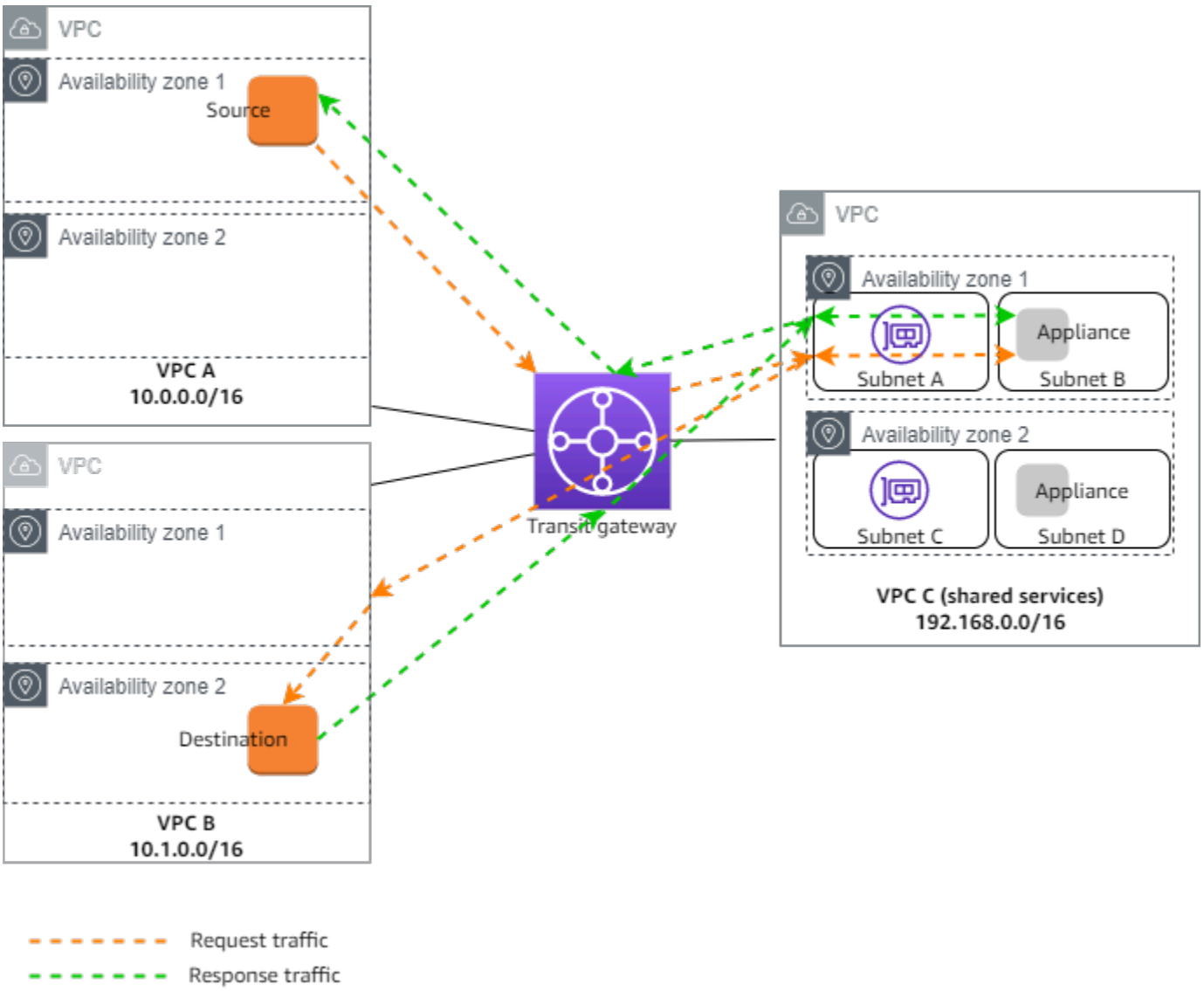
Important

- 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 estiverem em dois anexos do gateway de trânsito diferentes. O tráfego pode diminuir se a VPC centralizada receber o tráfego de um gateway diferente — por exemplo, um gateway da Internet — e depois enviar esse tráfego para o anexo do gateway de trânsito após a inspeção.
- Ativar o modo de aparelho 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 mais informações, consulte Criar uma VPC no Guia do usuário da Amazon VPC.
- Um gateway de trânsito Para obter mais informações, consulte the section called “Criar um gateway de trânsito”.
- Três acessórios de VPC - um para cada um dos. VPCs Para obter mais informações, consulte the section called “Criar um anexo de 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. Você também pode usar a API Amazon VPC, um AWS SDK, o AWS CLI para ativar o modo de dispositivo ou. 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

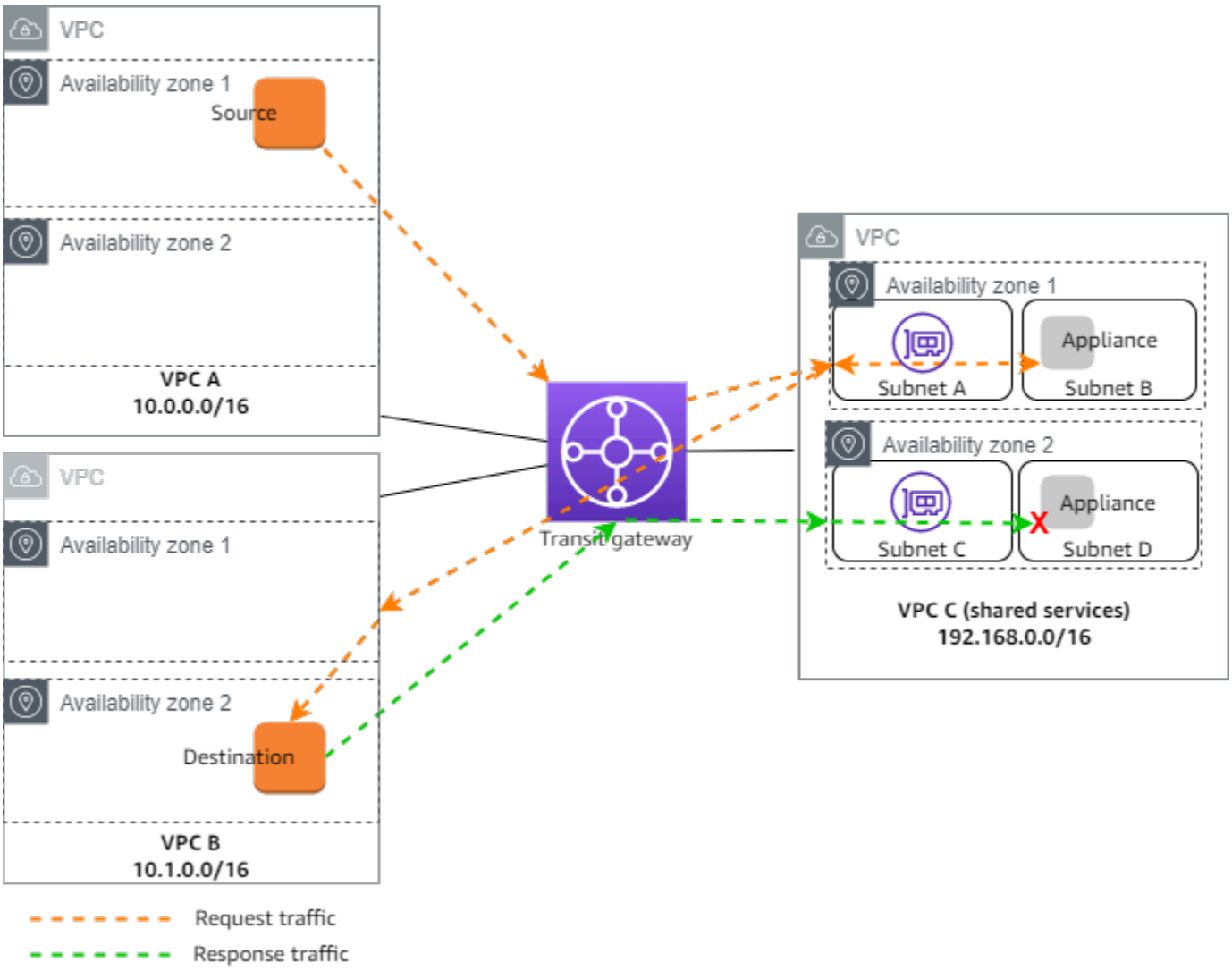
Se os anexos da VPC abrangem várias zonas de disponibilidade e for necessário que o tráfego entre hosts de origem e destino seja roteado pelo mesmo dispositivo para inspeção com estado, habilite o suporte ao modo de dispositivo para o anexo da VPC no qual o dispositivo está localizado.

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

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

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

Destino	Destino

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	Alvo	Tipo de rota
0.0.0.0/0	*Attachment ID for 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	Alvo	Tipo de rota
10.0.0.0/16	*Attachment ID for VPC A*	com propagação
10.1.0.0/16	*Attachment ID for VPC B*	com propagação

Tutoriais: Comece a usar os Amazon VPC Transit Gateways

Os tutoriais a seguir ajudam você a se familiarizar com os gateways de trânsito no Amazon VPC Transit Gateways. As tarefas nos tutoriais a seguir orientam você na criação de um gateway de trânsito e, em seguida, na conexão de dois de seus VPCs usando esse gateway de trânsito. Você pode criar um gateway de trânsito usando o console Amazon VPC ou usando o. AWS CLI

Tarefas

- Tutorial: Crie um AWS Transit Gateway usando o console da Amazon VPC
- Tutorial: Crie um AWS Transit Gateway usando a linha de AWS comando

Tutorial: Crie um AWS Transit Gateway usando o console da Amazon VPC

Neste tutorial, você aprenderá a usar o console da Amazon VPC para criar um gateway de trânsito e conectar dois VPCs a ele. Você criará o gateway de trânsito, conectará os dois e VPCs, em seguida, configurará as rotas necessárias para permitir a comunicação entre o gateway de trânsito e o seu VPCs.

Pré-requisitos

- Para demonstrar um exemplo simples do uso de um gateway de trânsito, crie dois VPCs na mesma região. Eles não VPCs podem ser idênticos nem sobrepostos CIDRs. Execute uma EC2 instância da Amazon em cada VPC. Para obter mais informações, consulte Criar uma VPC no Guia do usuário da Amazon VPC e Iniciar uma instância no Guia do usuário da Amazon. EC2
- Você não pode ter rotas idênticas apontando para duas diferentes VPCs. Um gateway de trânsito não propagará a CIDRs de uma VPC recém-conectada se existir uma rota idêntica nas tabelas de rotas do gateway de trânsito.
- Verifique se há as permissões necessárias para trabalhar com os gateways de trânsito. Para obter mais informações, consulte Gerenciamento de identidade e acesso no Amazon VPC Transit Gateways .
- Não é possível fazer ping entre hosts se uma regra ICMP não for adicionada a cada um dos grupos de segurança do host. Para obter mais informações, consulte Configurar regras de grupos de segurança no Guia do usuário da Amazon VPC.

Etapas

Etapa 1: Criar o gateway de trânsito

Ao criar um gateway de trânsito, uma tabela de rotas padrão é criada para ele. Ela é usada 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 ao criar o. VPCs
3. No painel de navegação, selecione Gateways de trânsito.
4. Selecione Criar gateway de trânsito.
5. (Opcional) Em 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 Descrição, digite uma descrição para o gateway de trânsito.
7. Na seção Configurar o gateway de trânsito, faça o seguinte:

    1. Em Número de sistema autônomo (ASN) do lado da Amazon, 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 16 bits. ASNs

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

        Se houver uma implantação em várias regiões, recomenda-se usar um ASN exclusivo para cada um dos gateways de trânsito.
    2. (Opcional) Selecione se deseja ativar um dos seguintes itens:
        - Suporte de DNS para VPCs conexão com esse gateway de trânsito.

- Suporte VPN ECMP para conexões VPN conectadas ao gateway de trânsito.
- Associação de tabela de rotas padrão, que associa automaticamente os anexos do gateway de trânsito à tabela de rotas padrão para o gateway de trânsito.
- Propagação da tabela de rotas padrão, que propaga automaticamente os anexos da tabela de rotas à tabela de rotas padrão desse gateway de trânsito.
- Suporte multicast, que permite criar domínios multicast nesse gateway de trânsito.

8. (Opcional) Na seção de opções de Configure-cross-account compartilhamento, escolha se deseja aceitar anexos compartilhados automaticamente. Se habilitado, os anexos serão aceitos automaticamente. Se não, será necessário aceitar ou rejeitar as solicitações de anexos.
9. (Opcional) Na seção Blocos CIDR do Transit Gateway, adicione um bloco CIDR de tamanho /24 ou maior para IPv4 endereços ou um bloco CIDR /64 ou maior para endereços. IPv6 É possível 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.

   > **Note**
   >
   > Os blocos CIDR do Transit Gateway são usados se você estiver configurando anexos Connect (GRE) ou PrivateIP. VPNs O Transit Gateway atribui IPs os endpoints do túnel (GRE/PrivateIP VPN) desse intervalo.

10. (Opcional) Adicione tags de valor-chave a esse gateway de trânsito para ajudar ainda mais a identificá-lo.

    1. Selecione Adicionar nova tag.
    2. Insira um nome de Chave e o Valor associado.
    3. Selecione Adicionar nova tag para adicionar mais tags ou vá para a próxima etapa.

11. Escolha Create transit gateway (Criar gateway de trânsito). Após a criação do gateway, o estado inicial do gateway de trânsito é `pending`.

Etapa 2: conecte seu VPCs ao seu 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 se você criou duas VPCs e executou uma EC2 instância em cada uma, conforme descrito emPré-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, selecione Anexos do gateway de trânsito.
3. Escolha Create Transit Gateway Attachment (Criar anexo do Transit Gateway).
4. (Opcional) Em Tag de nome, insira um nome para o anexo.
5. Em ID do gateway de trânsito, escolha o gateway de trânsito que será usado no anexo.
6. Em Tipo de anexo, escolha VPC.
7. Escolha se quer habilitar o Suporte a DNS. Para este exercício, não ative o IPv6 suporte.
8. Em ID da VPC, escolha a VPC a ser anexada ao gateway de trânsito.
9. Em Sub-rede IDs, 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. É possível 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 the section called “Exemplos de cenários de gateway de trânsito”.

Etapa 3: adicione rotas entre o gateway de trânsito e seu VPCs

Uma tabela de rotas inclui rotas dinâmicas e estáticas que determinam o próximo salto associado VPCs 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.

Como 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, selecione Tabelas de rotas.
3. Escolha uma tabela de roteamento associada à sua VPC.
4. Selecione a guia Rotas e Editar rotas.

5. Selecione Adicionar rota.
6. Na coluna Destino, informe o intervalo de endereços IP de destino. Para Alvo, selecione Gateway de trânsito e, em seguida, escolha o ID do gateway de trânsito.
7. Selecione Salvar alterações.

Etapa 4: Testar o gateway de trânsito

Você pode confirmar que o gateway de trânsito foi criado com sucesso conectando-se a uma EC2 instância da Amazon em cada VPC e enviando dados entre eles, como um comando ping. Para obter mais informações, consulte Connect to your EC2 instance no Amazon EC2 User Guide.

Etapa 5: Excluir o gateway de trânsito

Quando não precisar mais de um gateway de trânsito, é possível excluí-lo.

Não é possível excluir um gateway de trânsito que tenha anexos de recursos. Ao 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, selecione Gateways de trânsito.
3. Selecione o gateway de trânsito e escolha Ações e Excluir gateway de trânsito.
4. Insira **`delete`** e selecione Excluir.

   O Estado do gateway de trânsito na página Gateways de trânsito é Excluindo. Depois de excluído, o gateway de trânsito é removido da página.

Tutorial: Crie um AWS Transit Gateway usando a linha de AWS comando

Neste tutorial, você aprenderá a usar o AWS CLI para criar um gateway de trânsito e conectar dois VPCs a ele. Você criará o gateway de trânsito, conectará os dois e VPCs, em seguida, configurará as rotas necessárias para permitir a comunicação entre o gateway de trânsito e o seu VPCs.

Pré-requisitos

Antes de começar, verifique se você tem:

- AWS CLI instalado e configurado com as permissões apropriadas. Se você não tiver o AWS CLI instalado, consulte a documentação da interface de linha de AWS comando.
- Eles não VPCs podem ser idênticos nem sobrepostos CIDRs. Para obter mais informações, consulte Criar uma VPC no Guia do usuário da Amazon VPC.
- Uma EC2 instância em cada VPC. Para ver as etapas para iniciar uma EC2 instância em uma VPC, consulte Iniciar uma instância no Guia EC2 do usuário da Amazon.
- Grupos de segurança configurados para permitir tráfego ICMP entre as instâncias. Para ver as etapas para controlar o tráfego usando grupos de segurança, consulte Controle o tráfego para seus AWS recursos usando grupos de segurança no Guia do usuário da Amazon VPC.
- Permissões apropriadas do IAM para trabalhar com gateways de trânsito. Para verificar as permissões do IAM do gateway de trânsito, consulte Gerenciamento de identidade e acesso nos gateways de trânsito da Amazon VPC no Guia.AWS Transit Gateway

Etapas

Etapa 1: Criar o gateway de trânsito

Quando você cria um gateway de trânsito,AWS cria uma tabela de rotas padrão do gateway de trânsito e a usa como tabela de rotas de associação padrão e tabela de rotas de propagação padrão. Veja a seguir um exemplo de `create-transit-gateway` solicitação na `us-west-2` Região. Outros `options` foram aprovados na solicitação. Para obter mais informações sobre o `create-`

`transit-gateway` comando, incluindo uma lista das opções que você pode passar na solicitação, consulte create-transit-gateway.

```
aws ec2 create-transit-gateway \
  --description "My Transit Gateway" \
  --region us-west-2
```

A resposta então mostra que o gateway de trânsito foi criado. Na resposta, os `Options` que são retornados são todos valores padrão.

```
{
    "TransitGateway": {
        "TransitGatewayId": "tgw-1234567890abcdef0",
        "TransitGatewayArn": "arn:aws:ec2:us-west-2:123456789012:transit-gateway/
tgw-1234567890abcdef0",
        "State": "pending",
        "OwnerId": "123456789012",
        "Description": "My Transit Gateway",
        "CreationTime": "2025-06-23T17:39:33+00:00",
        "Options": {
            "AmazonSideAsn": 64512,
            "AutoAcceptSharedAttachments": "disable",
            "DefaultRouteTableAssociation": "enable",
            "AssociationDefaultRouteTableId": "tgw-rtb-abcdef1234567890a",
            "DefaultRouteTablePropagation": "enable",
            "PropagationDefaultRouteTableId": "tgw-rtb-abcdef1234567890a",
            "VpnEcmpSupport": "enable",
            "DnsSupport": "enable",
            "SecurityGroupReferencingSupport": "disable",
            "MulticastSupport": "disable"
        }
    }
}
```

> **Note**
>
> Esse comando retorna informações sobre seu novo gateway de trânsito, incluindo seu ID. Anote a ID do gateway de trânsito (`tgw-1234567890abcdef0`), pois você precisará dela nas etapas subsequentes.

Etapa 2: Verificar o estado de disponibilidade do gateway de trânsito

Quando você cria um gateway de trânsito, ele é colocado em um `pending` estado. O estado mudará de pendente para disponível automaticamente, mas até que isso aconteça, você não poderá anexar nenhum VPCs até que o estado mude. Para verificar o estado, execute o `describe-transit-gatweways` comando usando o ID do gateway de trânsito recém-criado junto com a opção de filtros. A `filters` opção usa `Name=state` e `Values=available` emparelha. Em seguida, o comando pesquisa para verificar se o estado do seu gateway de trânsito está em um estado disponível. Se for, a resposta será exibida`"State": "available"`. Se estiver em qualquer outro estado, ainda não está disponível para uso. Aguarde alguns minutos antes de executar o comando.

Para obter mais informações sobre o comando `describe-transit-gateways`, consulte describe-transit-gateways.

```
aws ec2 describe-transit-gateways \
  --transit-gateway-ids tgw-1234567890abcdef0 \
  --filters Name=state,Values=available
```

Espere até que o estado do gateway de trânsito mude de `pending` para `available` antes de continuar. Na resposta a seguir, o `State` mudou para`available`.

```
{
    "TransitGateways": [
        {
            "TransitGatewayId": "tgw-1234567890abcdef0",
            "TransitGatewayArn": "arn:aws:ec2:us-west-2:123456789012:transit-gateway/
tgw-1234567890abcdef0",
            "State": "available",
            "OwnerId": "123456789012",
            "Description": "My Transit Gateway",
            "CreationTime": "2022-04-20T19:58:25+00:00",
            "Options": {
                "AmazonSideAsn": 64512,
                "AutoAcceptSharedAttachments": "disable",
                "DefaultRouteTableAssociation": "enable",
                "AssociationDefaultRouteTableId": "tgw-rtb-abcdef1234567890a",
                "DefaultRouteTablePropagation": "enable",
                "PropagationDefaultRouteTableId": "tgw-rtb-abcdef1234567890a",
                "VpnEcmpSupport": "enable",
                "DnsSupport": "enable",
                "SecurityGroupReferencingSupport": "disable",
```

```
                "MulticastSupport": "disable"
            },
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "example-transit-gateway"
                }
            ]
        }
    ]
}
```

Etapa 3: conecte seu VPCs ao seu gateway de trânsito

Quando seu gateway de trânsito estiver disponível, crie um anexo para cada VPC usando o. `create-transit-gateway-vpc-attachment` Você precisará incluir o `transit-gateway-idvpc-id`, o e `subnet-ids` o.

Para obter mais informações sobre o `create-transit-vpc attachment` comando, consulte create-transit-gateway-vpc-attachment.

No exemplo a seguir, o comando é executado duas vezes, uma para cada VPC.

Para a primeira VPC, execute o seguinte usando a primeira `vpc_id` e: `subnet-ids`

```
aws ec2 create-transit-gateway-vpc-attachment \
  --transit-gateway-id tgw-1234567890abcdef0 \
  --vpc-id vpc-1234567890abcdef0 \
  --subnet-ids subnet-1234567890abcdef0
```

A resposta mostra o anexo bem-sucedido. O anexo é criado em um `pending` estado. Não há necessidade de alterar esse estado, pois ele muda para um `available` estado automaticamente. Isso pode demorar vários minutos.

```
{
    "TransitGatewayVpcAttachment": {
        "TransitGatewayAttachmentId": "tgw-attach-1234567890abcdef0",
        "TransitGatewayId": "tgw-1234567890abcdef0",
        "VpcId": "vpc-1234567890abcdef0",
        "VpcOwnerId": "123456789012",
        "State": "pending",
        "SubnetIds": [
```

```
            "subnet-1234567890abcdef0",
            "subnet-abcdef1234567890"
        ],
        "CreationTime": "2025-06-23T18:35:11+00:00",
        "Options": {
            "DnsSupport": "enable",
            "SecurityGroupReferencingSupport": "enable",
            "Ipv6Support": "disable",
            "ApplianceModeSupport": "disable"
        }
    }
}
```

Para a segunda VPC, execute o mesmo comando acima usando a segunda `vpc_id` e: `subnet-ids`

```
aws ec2 create-transit-gateway-vpc-attachment \
  --transit-gateway-id tgw-1234567890abcdef0 \
  --vpc-id vpc-abcdef1234567890 \
  --subnet-ids subnet-abcdef01234567890
```

A resposta para esse comando também mostra um anexo bem-sucedido, com o anexo atualmente em um `pending` estado.

```
{
    {
    "TransitGatewayVpcAttachment": {
        "TransitGatewayAttachmentId": "tgw-attach-abcdef1234567890",
        "TransitGatewayId": "tgw-1234567890abcdef0",
        "VpcId": "vpc-abcdef1234567890",
        "VpcOwnerId": "123456789012",
        "State": "pending",
        "SubnetIds": [
            "subnet-fedcba0987654321",
            "subnet-0987654321fedcba"
        ],
        "CreationTime": "2025-06-23T18:42:56+00:00",
        "Options": {
            "DnsSupport": "enable",
            "SecurityGroupReferencingSupport": "enable",
            "Ipv6Support": "disable",
            "ApplianceModeSupport": "disable"
        }
    }
```

```
}
```

Etapa 4: Verificar se os anexos do Transit Gateway estão disponíveis

Os anexos do Transit Gateway são criados em um estado inicial`pending`. Você não poderá usar esses anexos em suas rotas até que o estado mude para. `available` Isso acontece automaticamente. Use o `describe-transit-gateways` comando, junto com o`transit-gateway-id`, para verificar `State` o. Para obter mais informações sobre o comando `describe-transit-gateways`, consulte describe-transit-gateways.

Execute o comando a seguir para verificar o status. Neste exemplo, `Values` os campos opcionais `Name` e de filtros são passados na solicitação:

```
aws ec2 describe-transit-gateway-vpc-attachments \
  --filters Name=transit-gateway-id,Values=tgw-1234567890abcdef0
```

A resposta a seguir mostra que os dois anexos estão em um `available` estado:

```
{
    "TransitGatewayVpcAttachments": [
        {
            "TransitGatewayAttachmentId": "tgw-attach-1234567890abcdef0",
            "TransitGatewayId": "tgw-1234567890abcdef0",
            "VpcId": "vpc-1234567890abcdef0",
            "VpcOwnerId": "123456789012",
            "State": "available",
            "SubnetIds": [
                "subnet-1234567890abcdef0",
                "subnet-abcdef1234567890"
            ],
            "CreationTime": "2025-06-23T18:35:11+00:00",
            "Options": {
                "DnsSupport": "enable",
                "SecurityGroupReferencingSupport": "enable",
                "Ipv6Support": "disable",
                "ApplianceModeSupport": "disable"
            },
            "Tags": []
        },
        {
            "TransitGatewayAttachmentId": "tgw-attach-abcdef1234567890",
            "TransitGatewayId": "tgw-1234567890abcdef0",
```

```
            "VpcId": "vpc-abcdef1234567890",
            "VpcOwnerId": "123456789012",
            "State": "available",
            "SubnetIds": [
                "subnet-fedcba0987654321",
                "subnet-0987654321fedcba"
            ],
            "CreationTime": "2025-06-23T18:42:56+00:00",
            "Options": {
                "DnsSupport": "enable",
                "SecurityGroupReferencingSupport": "enable",
                "Ipv6Support": "disable",
                "ApplianceModeSupport": "disable"
            },
            "Tags": []
        }
    ]
}
```

Etapa 5: Adicione rotas entre seu gateway de trânsito e VPCs

Configure rotas em cada tabela de rotas da VPC para direcionar o tráfego para a outra VPC por meio do gateway de trânsito usando o `create-route` comando junto com a tabela de rotas de `transit-gateway-id` cada VPC. No exemplo a seguir, o comando é executado duas vezes, uma para cada tabela de rotas. A solicitação inclui o `route-table-iddestination-cidr-block`, o e `transit-gateway-id` para cada rota de VPC que você está criando.

Para obter mais informações sobre o `create-route` comando, consulte create-route.

Para a primeira tabela de rotas da VPC, execute o seguinte comando:

```
aws ec2 create-route \
  --route-table-id rtb-1234567890abcdef0 \
  --destination-cidr-block 10.2.0.0/16 \
  --transit-gateway-id tgw-1234567890abcdef0
```

Para a segunda tabela de rotas da VPC, execute o comando a seguir. Essa rota usa um `route-table-id` e é `destination-cidr-block` diferente da primeira VPC. No entanto, como você está usando apenas um único gateway de trânsito, o mesmo `transit-gateway-id` é usado.

```
aws ec2 create-route \
```

```
  --route-table-id rtb-abcdef1234567890 \
  --destination-cidr-block 10.1.0.0/16 \
  --transit-gateway-id tgw-1234567890abcdef0
```

A resposta retorna `true` para cada rota, indicando que as rotas foram criadas.

```
{
    "Return": true
}
```

> **Note**
>
> Substitua os blocos CIDR de destino pelos blocos CIDR reais do seu. VPCs

Etapa 6: testar o gateway de trânsito

Você pode confirmar se o gateway de trânsito foi criado com sucesso conectando-se a uma EC2 instância em uma VPC, fazendo ping em uma instância na outra VPC e, em seguida, executando o comando. `ping`

1. Conecte-se à sua EC2 instância na primeira VPC usando SSH ou Instance Connect EC2
2. Faça o ping do endereço IP privado da EC2 instância na segunda VPC:

   ```
   ping 10.2.0.50
   ```

   > **Note**
   >
   > `10.2.0.50`Substitua pelo endereço IP privado real da sua EC2 instância na segunda VPC.

Se o ping for bem-sucedido, seu gateway de trânsito está configurado corretamente e roteará o tráfego entre seus VPCs.

Etapa 7: Excluir os anexos do gateway de trânsito e o gateway de trânsito

Quando você não precisar mais do gateway de trânsito, poderá excluí-lo. Primeiro, você deve excluir todos os anexos. Execute o `delete-transit-gateway-vpc-attachment` comando usando

o `transit-gateway-attachment-id` para cada anexo. Depois de executar o comando, use `delete-transit-gateway` para excluir o gateway de trânsito. Para o seguinte, exclua os dois anexos de VPC e o gateway de trânsito único que foram criados nas etapas anteriores.

> **Important**
>
> Você deixará de incorrer em cobranças depois de excluir todos os anexos do Transit Gateway.

1. Exclua os anexos da VPC usando o comando. `delete-transit-gateway-vpc-attachment` Para obter mais informações sobre o `delete-transit-gateway-vpc-attachment` comando, consulte delete-transit-gateway-vpc-attachment.

   Para o primeiro anexo, execute o seguinte comando:

   ```
   aws ec2 delete-transit-gateway-vpc-attachment \
     --transit-gateway-attachment-id tgw-attach-1234567890abcdef0
   ```

   A resposta de exclusão para o primeiro anexo de VPC retorna o seguinte:

   ```
   {
       "TransitGatewayVpcAttachment": {
           "TransitGatewayAttachmentId": "tgw-attach-1234567890abcdef0",
           "TransitGatewayId": "tgw-1234567890abcdef0",
           "VpcId": "vpc-abcdef1234567890",
           "VpcOwnerId": "123456789012",
           "State": "deleting",
           "CreationTime": "2025-06-23T18:42:56+00:00"
       }
   }
   ```

   Execute o `delete-transit-gateway-vpc-attachment` comando para o segundo anexo:

   ```
   aws ec2 delete-transit-gateway-vpc-attachment \
     --transit-gateway-attachment-id tgw-attach-abcdef1234567890
   ```

   A resposta de exclusão para o segundo anexo de VPC retorna o seguinte:

```
The response returns:
{
    "TransitGatewayVpcAttachment": {
        "TransitGatewayAttachmentId": "tgw-attach-abcdef1234567890",
        "TransitGatewayId": "tgw-1234567890abcdef0",
        "VpcId": "vpc-abcdef1234567890",
        "VpcOwnerId": "123456789012",
        "State": "deleting",
        "CreationTime": "2025-06-23T18:42:56+00:00"
    }
}
```

2. Os anexos ficam em um `deleting` estado até serem excluídos. Depois de excluído, você pode excluir o gateway de trânsito. Use o `delete-transit-gateway` comando junto com `transit-gateway-id` o. Para obter mais informações sobre `delete-transit-gateway` o comando, consulte delete-transit-gateway.

   O exemplo a seguir exclui `My Transit Gateway` o que você criou na primeira etapa acima:

   ```
   aws ec2 delete-transit-gateway \
     --transit-gateway-id tgw-1234567890abcdef0
   ```

   Veja a seguir a resposta à solicitação, que inclui o ID e o nome do gateway de trânsito excluídos, junto com as opções originais definidas para o gateway de trânsito quando ele foi criado.

   ```
   {
       "TransitGateway": {
           "TransitGatewayId": "tgw-1234567890abcdef0",
           "TransitGatewayArn": "arn:aws:ec2:us-west-2:123456789012:transit-gateway/
   tgw-1234567890abcdef0",
           "State": "deleting",
           "OwnerId": "123456789012",
           "Description": "My Transit Gateway",
           "CreationTime": "2025-06-23T17:39:33+00:00",
           "Options": {
               "AmazonSideAsn": 64512,
               "AutoAcceptSharedAttachments": "disable",
               "DefaultRouteTableAssociation": "enable",
               "AssociationDefaultRouteTableId": "tgw-rtb-abcdef1234567890a",
               "DefaultRouteTablePropagation": "enable",
               "PropagationDefaultRouteTableId": "tgw-rtb-abcdef1234567890a",
   ```

```
            "VpnEcmpSupport": "enable",
            "DnsSupport": "enable",
            "SecurityGroupReferencingSupport": "disable",
            "MulticastSupport": "disable"
        },
        "Tags": [
            {
                "Key": "Name",
                "Value": "example-transit-gateway"
            }
        ]
    }
}
```

Conclusão

Você criou com sucesso um gateway de trânsito, anexou dois VPCs a ele, configurou o roteamento entre eles e verificou a conectividade. Este exemplo simples demonstra a funcionalidade básica dos Amazon VPC Transit Gateways. Para cenários mais complexos, como conectar-se a redes locais ou implementar configurações de roteamento mais avançadas, consulte o Guia do usuário do Amazon VPC Transit Gateways.

Melhores práticas de design do Amazon VPC Transit Gateways

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 EC2 recursos. Ao usar uma sub-rede separada, é possível configurar o seguinte:
  - Mantenha aberta a rede de entrada e saída ACLs associada às sub-redes do Transit Gateway.
  - Dependendo do seu fluxo de tráfego, você pode aplicar ACLs a rede às suas sub-redes de carga de trabalho.
- Crie uma ACL de rede e associe-a a todas as sub-redes que estão associadas ao gateway de trânsito. Mantenha a ACL de rede 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 desenho 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 Site-to-Site VPN do Border Gateway Protocol (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 Site-to-Site BGP VPN.
- Ao migrar do emparelhamento 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 os dois VPCs ao mesmo tempo para evitar a queda de pacotes enormes devido a incompatibilidades 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 gateways de trânsito, recomenda-se 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.

Trabalhe com gateways de trânsito usando Amazon VPC Transit Gateways

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

Tópicos

Gateways de trânsito compartilhados

Você pode usar o AWS Resource Access Manager (RAM) para compartilhar um gateway de trânsito para anexos de VPC entre contas ou em toda a sua organização em. 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 .

Considerações

Considere o seguinte quando quiser compartilhar um gateway de trânsito.

- Um AWS Site-to-Site VPN anexo deve ser criado na mesma AWS conta proprietária do gateway de trânsito.

- Um anexo a um gateway Direct Connect usa uma associação de gateway de trânsito e pode estar na mesma AWS conta do gateway Direct Connect ou em uma conta diferente do gateway Direct Connect.

Por padrão, os usuários não têm permissão para criar ou modificar AWS RAM recursos. Para permitir que os usuários criem ou alterem recursos e realizem tarefas, é necessário 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.

Apenas 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 as entidades principais com as quais os recursos estão sendo compartilhados, em todos os compartilhamentos de recursos. Visualizar as entidades principais com as quais os recursos estão sendo compartilhados permite determinar quem tem acesso aos recursos compartilhados.
- Excluir o compartilhamento de um recurso.
- Execute todas as tabelas do gateway de trânsito, anexo do gateway de trânsito e rotas do gateway de trânsito APIs.

É possível executar as operações a seguir nos recursos compartilhados:

- Aceitar ou rejeitar o convite de um compartilhamento de recursos.
- Exibir o compartilhamento de um recurso.
- Visualizar os recursos compartilhados que podem ser acessados.
- Visualizar uma lista de todas as entidades principais que estão compartilhando recursos. É possível ver quais recursos e compartilhamentos de recursos foram compartilhados.
- É possível executar a API do `DescribeTransitGateways`.
- Execute os APIs que criam e descrevem anexos, por exemplo `CreateTransitGatewayVpcAttachment` e`DescribeTransitGatewayVpcAttachments`, em seus. VPCs
- Deixar o compartilhamento de um recurso.

Quando um gateway de trânsito é compartilhado, 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.

Ao criar um gateway de trânsito, ele é criado na zona de disponibilidade que é mapeada para sua conta, sendo 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 uma ID AZ para a região us-east-1 e mapeia para o mesmo local em todas as contas. AWS

Cancelar o compartilhamento de um gateway de trânsito

Quando o proprietário cancelar o compartilhamento 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.
- Tanto proprietário do gateway de trânsito como o proprietário do compartilhamento podem excluir o anexo do gateway de trânsito.

Quando um gateway de trânsito não é compartilhado com outra AWS conta, ou se a AWS conta com a qual o gateway de trânsito é compartilhado for removida da organização, o gateway de trânsito em si não será afetado.

Sub-redes compartilhadas

O proprietário da VPC pode anexar um gateway de trânsito a uma sub-rede de VPC compartilhada. Os participantes não podem fazer isso. 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.

Gateways de trânsito no Amazon VPC Transit Gateways

Um gateway de trânsito permite que você conecte conexões VPN VPCs e roteie o 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 anexá-lo 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 rotas. 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 os alvos IPv4 ou IPv6 CIDRs e. Os alvos são VPCs conexões VPN. Quando uma VPC é anexada ou uma conexão VPN é criada 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, é possível segmentar a rede. Por exemplo, você pode associar o desenvolvimento VPCs a uma tabela de rotas e a produção VPCs a uma tabela de rotas diferente. Isso permite criar redes isoladas dentro de um gateway de trânsito semelhante ao roteamento e encaminhamento virtuais (VRFs) nas redes tradicionais.

Os gateways de trânsito oferecem suporte ao roteamento dinâmico e estático entre conexões conectadas VPCs e VPN. 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. Também é possível apontar rotas nas tabelas de rotas do gateway de trânsito para o anexo de emparelhamento para rotear o tráfego entre os gateways de trânsito emparelhados.

Opcionalmente, você pode associar um IPv4 ou mais blocos IPv6 CIDR ao seu 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. É possível associar qualquer intervalo de endereços IP públicos ou privados, 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 blocos IPv6 CIDR IPv4 e blocos, consulte Endereçamento IP no Guia do usuário da Amazon VPC.

Tarefas

- Criar um gateway de trânsito usando Amazon VPC Transit Gateways
- Visualizar informações do gateway de trânsito usando os Amazon VPC Transit Gateways
- Adicionar ou editar tags a um gateway de trânsito usando Amazon VPC Transit Gateways
- Modificar um gateway de trânsito usando os Amazon VPC Transit Gateways

- Aceitar um compartilhamento de recursos usando Amazon VPC Transit Gateways
- Aceitar um anexo compartilhado usando o Amazon VPC Transit Gateways
- Excluir um gateway de trânsito usando Amazon VPC Transit Gateways

Criar um gateway de trânsito usando Amazon VPC Transit Gateways

Ao criar um um gateway de trânsito, uma tabela de rotas padrão é criada para ele, sendo usada como tabela padrão de associação e propagação. Se não desejar criar a tabela de rotas padrão do gateway de trânsito, 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, selecione Gateways de trânsito.
3. Escolha Create transit gateway (Criar gateway de trânsito).
4. Opcionalmente, insira um nome para o gateway de trânsito em Tag de nome. Uma tag de nome pode facilitar a identificação de um gateway de trânsito a partir de uma lista de gateways. Ao adicionar uma Tag de nome, uma tag é criada com uma chave de Nome e um valor igual ao valor que você inserir.
5. Como opção, em Descrição, insira uma descrição para o gateway de trânsito.
6. Em Número de sistema autônomo (ASN) 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 16 bits. ASNs

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

   Se houver uma implantação em várias regiões, recomenda-se usar um ASN exclusivo para cada um dos gateways de trânsito.
7. Para suporte a DNS, selecione essa opção se precisar que a VPC resolva nomes de host DNS IPv4 públicos em endereços IPv4 privados quando consultados de instâncias em outra VPC conectada ao gateway de trânsito.
8. Para suporte de referência de grupos de segurança, ative esse recurso para referenciar um grupo de segurança VPCs conectado a um gateway de trânsito. Para obter mais informações

sobre referência de grupo de segurança, consulte the section called “Referenciamento de grupo de segurança”.

9. Em 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 o mesmo CIDRs, o tráfego será distribuído igualmente entre elas.

   Ao selecionar essa opção, o BGP ASN anunciado, os atributos do BGP, como AS-path, 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.

10. Selecione Associação de tabela de rotas padrão, para associar automaticamente os anexos de gateway de trânsito à tabela de rotas padrão para o gateway de trânsito.
11. Selecione Propagação de tabela de rotas padrão, para propagar automaticamente os anexos de gateway de trânsito à tabela de rotas padrão para o gateway de trânsito.
12. (Opcional) Para usar o gateway de trânsito como roteador para tráfego de multicast, selecione Suporte a multicast.
13. (Opcional) Na seção de opções de Configure-cross-account compartilhamento, escolha se deseja aceitar anexos compartilhados automaticamente. Se habilitado, os anexos serão aceitos automaticamente. Se não, será necessário aceitar ou rejeitar as solicitações de anexos.

    Em Aceitar automaticamente anexos compartilhados, selecione essa opção para aceitar automaticamente anexos entre contas.
14. (Opcional) Para blocos CIDR do Transit Gateway, especifique um IPv4 ou mais blocos IPv6 CIDR para o Transit Gateway.

    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 É possível 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.

> **Note**
>
> Os blocos CIDR do Transit Gateway são usados se você estiver configurando anexos Connect (GRE) ou PrivateIP. VPNs O Transit Gateway atribui IPs os endpoints do túnel (GRE/PrivateIP VPN) desse intervalo.

15. Selecione Criar gateway de trânsito.

Para criar um gateway de trânsito usando o AWS CLI

Use o comando create-transit-gateway.

Visualizar informações do gateway de trânsito usando os Amazon VPC Transit Gateways

Visualize qualquer gateway de trânsito.

Como visualizar 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, selecione Gateways de trânsito. Os detalhes do gateway de trânsito são exibidos abaixo da lista de gateways na página.

Para visualizar um gateway de trânsito usando o AWS CLI

Use o comando describe-transit-gateways.

Adicionar ou editar tags a um gateway de trânsito usando Amazon VPC Transit Gateways

Adicione tags aos recursos para ajudar a organizá-los e identificá-los, por exemplo, por finalidade, 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 uma tag for adicionada com uma chave que já esteja associada ao gateway de trânsito, o valor dessa tag será atualizado. Para obter mais informações, consulte Como marcar seus EC2 recursos da Amazon.

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, selecione Gateways de trânsito.
3. Escolha o gateway de trânsito para o qual deseja adicionar ou editar tags.
4. Selecione a guia Tags na parte inferior da página.
5. Selecione Gerenciar tags.
6. Selecione Adicionar nova tag.
7. Insira uma Chave e um Valor para a tag.
8. Escolha Salvar.

Modificar um gateway de trânsito usando os Amazon VPC Transit Gateways

Você pode modificar as opções de configuração de um gateway de trânsito. Quando você modifica um gateway de trânsito, nenhum anexo existente do gateway de trânsito sofre nenhuma interrupção no 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 par Connect.

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 que será modificado.
4. Selecione Ações, Modificar gateway de trânsito.
5. Modifique as opções conforme necessário e selecione Modificar gateway de trânsito.

Para modificar seu gateway de trânsito usando o AWS CLI

Use o comando modify-transit-gateway.

Aceitar um compartilhamento de recursos usando Amazon VPC Transit Gateways

Ao ser adicionado a um compartilhamento de recursos, você 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, selecione Compartilhados comigo, Compartilhamentos de recursos.
3. Selecione o compartilhamento de recursos.
4. Selecione Aceitar compartilhamento de recursos.
5. Para visualizar o gateway de trânsito compartilhado, abra a página Gateways de trânsito no console da Amazon VPC.

Aceitar um anexo compartilhado usando o Amazon VPC Transit Gateways

Se você não ativou a funcionalidade de aceitação automática de anexos compartilhados ao criar seu gateway de trânsito, deverá aceitar manualmente anexos entre contas (compartilhados) usando o console Amazon VPC ou a CLI. AWS

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 usando Amazon VPC Transit Gateways

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 a ser excluído.
3. Selecione Ações, Excluir gateway de trânsito. Para confirmar a exclusão, digite **`delete`** e selecione Excluir.

Para excluir um gateway de trânsito usando o AWS CLI

Use o comando delete-transit-gateway.

Anexos da Amazon VPC nos Amazon VPC Transit Gateways

Um anexo Amazon Virtual Private Cloud (VPC) a um gateway de trânsito permite rotear o tráfego de e para uma ou mais sub-redes 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 do gateway de trânsito alcançará este 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.
- Um gateway de trânsito não oferece suporte à resolução de DNS para nomes DNS personalizados da VPCs configuração anexada usando zonas hospedadas privadas no Amazon Route 53. Para configurar a resolução de nomes para zonas hospedadas privadas para todas VPCs conectadas a um gateway de trânsito, consulte Gerenciamento centralizado de DNS da nuvem híbrida com o Amazon Route 53 e o AWS Transit Gateway.
- Um gateway de trânsito não oferece suporte ao roteamento entre VPCs idênticos CIDRs, ou se um CIDR em um intervalo se sobrepõe a um CIDR em uma VPC conectada. Se você conectar

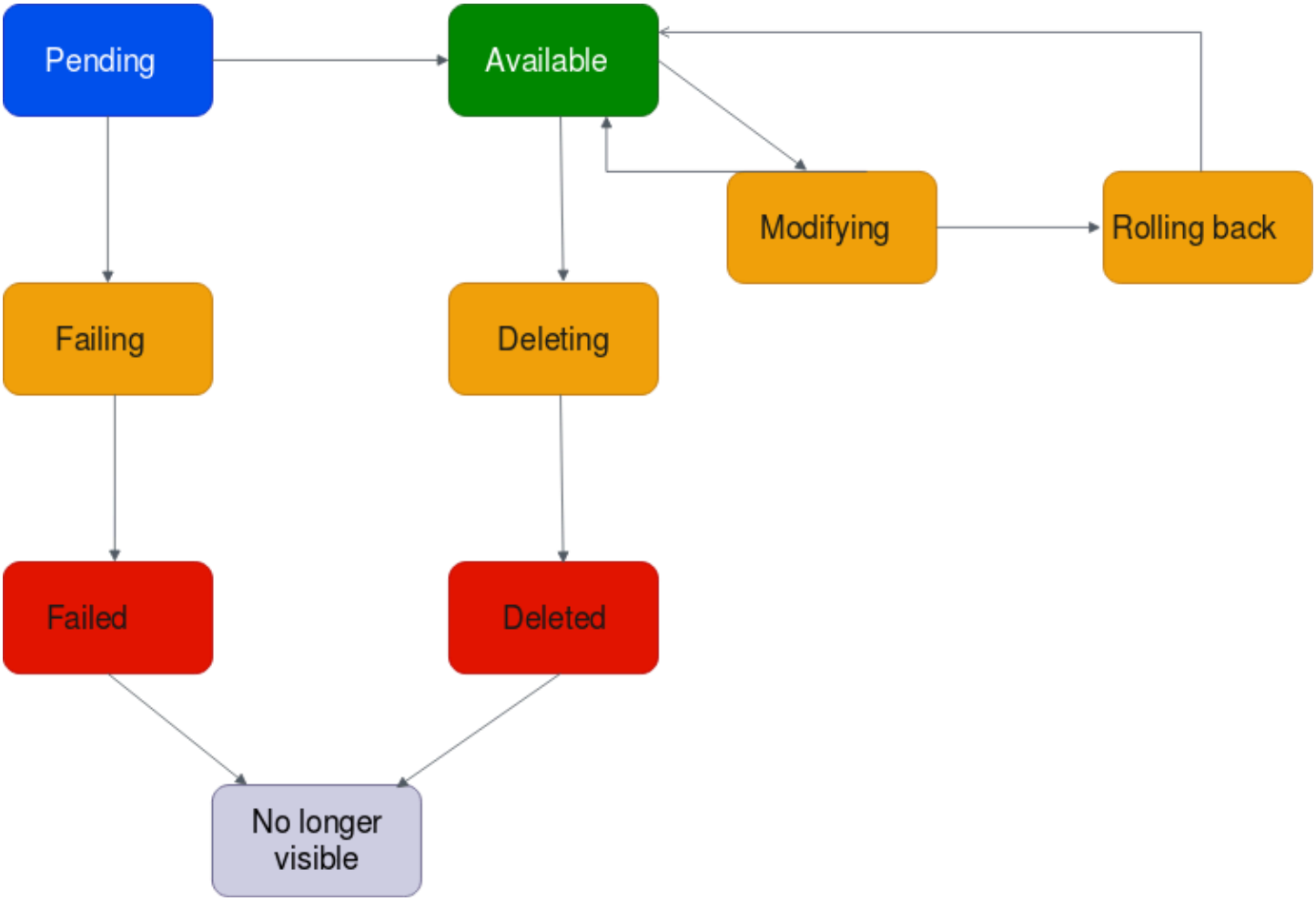
uma VPC a um gateway de trânsito e seu CIDR for idêntico ou se sobrepor ao CIDR de outra VPC que já esteja conectada ao gateway de trânsito, as rotas da VPC recém-conectada não serão propagadas para a tabela de rotas do gateway de trânsito.

- Não é possível criar um anexo para uma sub-rede da VPC que resida em uma zona local. Porém, é possível configurar a rede para que as sub-redes na Zona Local se conectem a um gateway de trânsito por meio da Zona de Disponibilidade principal. Para obter mais informações, consulte Conectar sub-redes da Zona Local a um gateway de trânsito.
- Você não pode criar um anexo de gateway de trânsito usando IPv6 sub-redes somente. As sub-redes de anexos do Transit Gateway também devem oferecer suporte IPv4 a endereços.
- 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.

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 possíveis, e, ao 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.

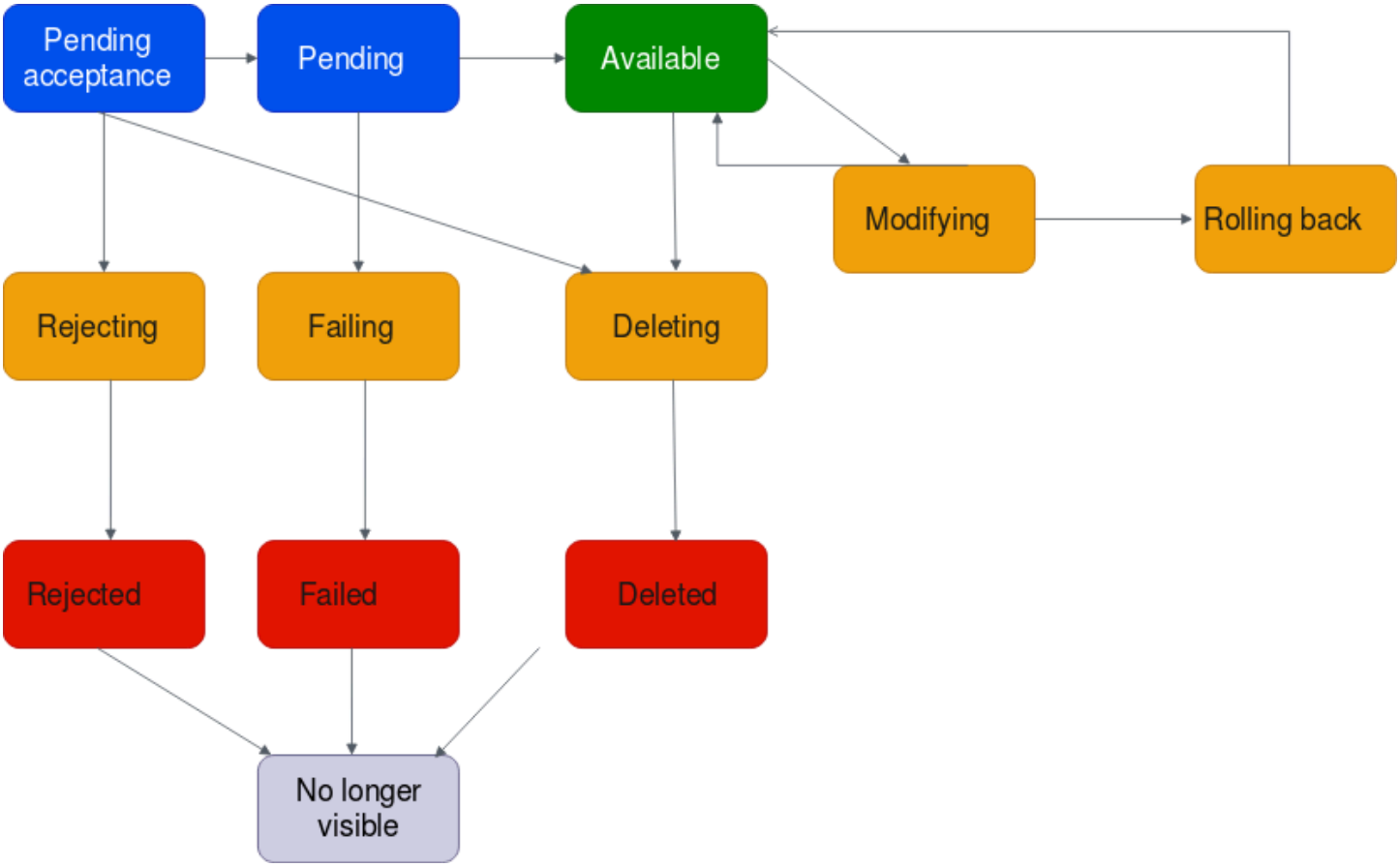
O diagrama a seguir mostra os estados pelos quais um anexo pode passar em uma única configuração de conta ou em uma configuração para várias contas que tenha a opção Aceitar automaticamente os anexos compartilhados ativada.



- 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 VPC `available` 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 Aceitar automaticamente os anexos 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`.
- Rejeitando: um anexo da VPC que está em processo de ser rejeitado. Nesta fase, o anexo pode ir para `rejected`.
- Rejeitado: um anexo da VPC `pending acceptance` 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 da VPC `available` ou `pending acceptance` 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`.

Modo do dispositivo

Se você planeja configurar um dispositivo de rede com estado em sua VPC, você pode habilitar o suporte ao modo de dispositivo para o anexo de VPC no qual o dispositivo está localizado ao criar um anexo. Isso garante que o AWS Transit Gateway use a mesma zona de disponibilidade para esse anexo de VPC durante toda a vida útil do fluxo de tráfego entre a origem e o destino. Também permite que um gateway de trânsito envie tráfego para qualquer zona de disponibilidade na VPC, desde que haja uma associação de sub-rede nessa zona. Embora o modo appliance seja suportado apenas em anexos VPC, o fluxo de rede pode vir de qualquer outro tipo de anexo de gateway de trânsito, incluindo anexos VPC, VPN e Connect. O modo appliance também funciona para fluxos de rede que têm origens e destinos diferentes Regiões da AWS. Os fluxos de rede podem ser potencialmente rebalanceados em diferentes zonas de disponibilidade se você não ativar inicialmente o modo de dispositivo, mas depois editar a configuração do anexo para ativá-lo. Você pode ativar ou desativar o modo de equipamento usando o console, a linha de comando ou a API.

O modo de dispositivo no AWS Transit Gateway otimiza o roteamento de tráfego considerando as zonas de disponibilidade de origem e destino ao determinar o caminho por meio de uma VPC no modo de dispositivo. Essa abordagem aumenta a eficiência e reduz a latência. O comportamento

varia de acordo com a configuração específica e os padrões de tráfego. Veja a seguir exemplos de cenários.

Cenário 1: roteamento de tráfego de zona intra-disponibilidade via Appliance VPC

Quando o tráfego flui da zona de disponibilidade de origem us-east-1a para a zona de disponibilidade de destino us-east-1a, com anexos VPC do modo de dispositivo em us-east-1a e us-east-1b, o Transit Gateway seleciona uma interface de rede de us-east-1a dentro da VPC do dispositivo. Essa zona de disponibilidade é mantida por toda a duração do fluxo de tráfego entre a origem e o destino.

Cenário 2: roteamento de tráfego de zona de interdisponibilidade via appliance VPC

Para o tráfego que flui da zona de disponibilidade de origem us-east-1a para a zona de disponibilidade de destino us-east-1b, com anexos VPC do modo de dispositivo em us-east-1a e us-east-1b, o Transit Gateway usa um algoritmo de hash de fluxo para selecionar us-east-1a ou us-east-1b na VPC do dispositivo. A zona de disponibilidade escolhida é usada de forma consistente durante a vida útil do fluxo.

Cenário 3: roteamento de tráfego por meio de uma VPC de dispositivo sem dados da zona de disponibilidade

Quando o tráfego se origina da Zona de Disponibilidade us-east-1a de origem para um destino sem informações da Zona de Disponibilidade (por exemplo, tráfego vinculado à Internet), com anexos VPC do Modo de Dispositivo em us-east-1a e us-east-1b, o Transit Gateway seleciona uma interface de rede de us-east-1a dentro da VPC do dispositivo.

Cenário 4: roteamento de tráfego por meio de uma VPC de dispositivo em uma zona de disponibilidade distinta da origem ou do destino

Quando o tráfego flui da zona de disponibilidade de origem us-east-1a para a zona de disponibilidade de destino us-east-1b, com anexos VPC do modo appliance em diferentes zonas de disponibilidade, por exemplo us-east-1c e us-east-1d, o Transit Gateway usa um algoritmo de hash de fluxo para selecionar us-east-1c ou us-east-1d na VPC do dispositivo. A zona de disponibilidade escolhida é usada de forma consistente durante a vida útil do fluxo.

> **Note**
>
> O modo appliance só é compatível com anexos de VPC. Certifique-se de que a propagação de rotas esteja habilitada para uma tabela de rotas associada a um anexo VPC do appliance.

Referenciamento de grupo de segurança

Você pode usar esse recurso para simplificar o gerenciamento de grupos de segurança e o controle do instance-to-instance tráfego entre VPCs aqueles conectados ao mesmo gateway de trânsito. Só é possível fazer referência cruzada a grupos de segurança em regras de entrada. As regras de segurança de saída não são compatíveis com o referenciamento de grupos de segurança. Não há custos adicionais associados à ativação ou ao uso da referenciamento de grupos de segurança.

O suporte de referência de grupos de segurança pode ser configurado tanto para gateways de trânsito quanto para anexos VPC do gateway de trânsito e só funcionará se tiver sido habilitado para um gateway de trânsito e seus anexos de VPC.

Limitações

As limitações a seguir se aplicam ao usar a referência de grupos de segurança com um anexo de VPC.

- A referência a grupos de segurança não é suportada nas conexões de emparelhamento do Transit Gateway. Ambos VPCs devem estar conectados ao mesmo gateway de trânsito.
- Não há suporte para a referência de grupos de segurança para anexos da VPC na zona de disponibilidade use1-az3.
- A referência a grupos de segurança não é suportada para PrivateLink endpoints. Recomendamos o uso de regras de segurança baseadas em IP CIDR como alternativa.
- A referência de grupos de segurança funciona para o Elastic File System (EFS), desde que uma regra de grupo de segurança de permissão para todas as saídas esteja configurada para as interfaces EFS na VPC.
- Para conectividade de Zona Local por meio de um gateway de trânsito, há suporte apenas para as seguintes Zonas Locais: us-east-1-atl-2a, us-east-1-dfw-2a, us-east-1-iah-2a, us-west-2-lax-1a, us-west-2-lax-1b, us-east-1-mia-2a, us-east-1-chi-2a e us-west-2-phx-2a.

- Recomendamos desativar esse recurso no nível de anexo da VPC VPCs para sub-redes em Zonas Locais, AWS Outposts e Zonas de AWS Wavelength sem suporte, pois isso pode causar interrupção do serviço.
- Se você tiver uma VPC de inspeção, a referência ao grupo de segurança por meio do gateway de trânsito não funcionará no Gateway Load AWS Balancer ou no Network Firewall. AWS

Tarefas

- Criar um anexo de VPC usando Amazon VPC Transit Gateways
- Modificar um anexo de VPC usando Amazon VPC Transit Gateways
- Modificar as tags de anexo da VPC usando os gateways de trânsito da Amazon VPC
- Visualizar um anexo de VPC usando Amazon VPC Transit Gateways
- Excluir um anexo de VPC usando Amazon VPC Transit Gateways
- Atualizar as regras de entrada do grupo de AWS Transit Gateway segurança
- Identifique AWS Transit Gateway grupos de segurança referenciados
- Remover regras obsoletas do grupo AWS Transit Gateway de segurança
- Solucionar problemas de criação de anexos VPC da Amazon VPC Transit Gateways

Criar um anexo de VPC usando Amazon VPC Transit Gateways

Como criar um anexo de VPC usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Anexos do gateway de trânsito.
3. Escolha Create transit gateway attachment (Criar anexo do gateway de trânsito).
4. Em Tag 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 suporte ao modo DNS Support, IPv6Support e Appliance.

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

8. Escolha se deseja ativar o suporte de referência de grupos de segurança. Ative esse recurso para referenciar um grupo de segurança VPCs conectado a um gateway de trânsito. Para obter mais informações sobre referência ao grupo de segurança, consulte: the section called “Referenciamento de grupo de segurança”.
9. Escolha se deseja ativar o IPv6Support.
10. Em ID da VPC, escolha a VPC a ser anexada ao gateway de trânsito.

    Essa VPC precisa estar associada a pelo menos uma sub-rede.
11. Em Sub-rede IDs, 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. É possível selecionar somente uma sub-rede por zona de disponibilidade.
12. 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 um anexo de VPC usando Amazon VPC Transit Gateways

Como modificar seus anexos de VPC usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Anexos do gateway de trânsito.
3. Escolha o anexo da VPC e selecione Ações, Modificar anexo do gateway de trânsito.
4. Ative ou desative qualquer uma das seguintes opções:

   - Suporte a DNS
   - IPv6 apoio
   - Suporte ao modo de dispositivo
5. Para adicionar ou remover uma sub-rede do anexo, selecione ou desmarque a caixa de seleção ao lado da ID da sub-rede que você deseja adicionar ou remover.

> **Note**
>
> Adicionar ou modificar uma sub-rede de anexos de VPC pode afetar o tráfego de dados enquanto o anexo estiver sendo modificado.

6. Para poder referenciar um grupo de segurança VPCs conectado a um gateway de trânsito, selecione Suporte de referência de grupos de segurança. Para obter mais informações sobre referência ao grupo de segurança, consulte: the section called “Referenciamento de grupo de segurança”.

   > **Note**
   >
   > Se você desativar a referência de grupos de segurança para um gateway de trânsito existente, ela será desativada em todos os anexos da VPC.

7. Selecione 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 anexo da VPC usando os gateways de trânsito da Amazon VPC

Como modificar as tags de 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, selecione Anexos do gateway de trânsito.
3. Selecione o anexo da VPC e então, Ações, Gerenciar tags.
4. [Adicionar uma tag] Selecione Adicionar nova tag e faça o seguinte:
   - Em Chave, insira o nome da chave.
   - Em Valor insira o valor da chave.
5. [Remover uma tag] Ao lado da tag, selecione Remover.
6. Selecione Salvar.

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

Visualizar um anexo de VPC usando Amazon VPC Transit Gateways

Como 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, selecione Anexos do gateway de trânsito.
3. Na coluna Tipo de recurso, procure por VPC. Os anexos da VPC serão exibidos.
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 de VPC usando Amazon VPC Transit Gateways

Como excluir um anexo de VPC usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Anexos do gateway de trânsito.
3. Escolha o anexo de VPC.
4. Selecione Ações, Excluir anexo do gateway de trânsito.
5. Quando solicitado, digite **`delete`** e escolha Excluir.

Para excluir um anexo de VPC usando o AWS CLI

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

Atualizar as regras de entrada do grupo de AWS Transit Gateway segurança

É possível atualizar qualquer uma das regras de entrada do grupo de segurança associadas a um gateway de trânsito. É possível atualizar regras do grupo de segurança usando o console do Amazon VPC, a linha de comando ou a API. Para obter mais informações sobre referência ao grupo de segurança, consulte: the section called “Referenciamento de grupo de segurança”.

Atualizar as regras do grupo de segurança usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Grupos de segurança.
3. Escolha o grupo de segurança e selecione Ações, Editar regras de entrada para modificar as regras de entrada.
4. Para adicionar uma regra, selecione Adicionar regra e especifique o tipo, protocolo e intervalo de porta. Em Origem (regra de entrada), insira o ID do grupo de segurança na VPC conectada ao gateway de trânsito.

   > **Note**
   >
   > Os grupos de segurança em uma VPC conectada ao gateway de trânsito não são exibidos automaticamente.

5. Para editar uma regra existente, altere seus valores (por exemplo, a origem ou a descrição).
6. Para excluir uma regra, selecione Excluir, próximo à regra.
7. Selecione Salvar rules.

Como atualizar regras de entrada usando a linha de comando

- authorize-security-group-ingress (AWS CLI)
- Grant-EC2SecurityGroupIngress (AWS Tools for Windows PowerShell)
- Revoke-EC2SecurityGroupIngress (AWS Tools for Windows PowerShell)
- revoke-security-group-ingress (AWS CLI)

Identifique AWS Transit Gateway grupos de segurança referenciados

Para determinar se seu grupo de segurança está sendo referenciado nas regras de um grupo de segurança em uma VPC conectada ao mesmo gateway de trânsito, use um dos comandos a seguir.

- describe-security-group-references (AWS CLI)
- Get-EC2SecurityGroupReference (AWS Tools for Windows PowerShell)

Remover regras obsoletas do grupo AWS Transit Gateway de segurança

Uma regra de grupo de segurança obsoleta é uma regra que referencia um grupo de segurança excluído na mesma VPC ou na VPC anexada ao mesmo gateway de trânsito. Quando uma regra de grupo de segurança se torna obsoleta, ela não é automaticamente removida do grupo de segurança, portanto, é preciso removê-la manualmente.

É possível visualizar e excluir as regras de grupo de segurança obsoletas para uma VPC usando o console da Amazon VPC.

Como visualizar e excluir regras do grupo de segurança obsoletas

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Security groups (Grupos de segurança).
3. Selecione Ações, Gerenciar regras obsoletas.
4. Em VPC, escolha a VPC com as regras obsoletas.
5. Selecione Editar.
6. Selecione o botão Excluir ao lado da regra que deseja excluir. Selecione Visualizar alterações, Salvar regras.

Como descrever as regras desatualizadas do seu grupo de segurança usando a linha de comando

- describe-stale-security-groups (AWS CLI)
- Get-EC2StaleSecurityGroup (AWS Tools for Windows PowerShell)

Depois de identificar as regras obsoletas do grupo de segurança, você pode excluí-las usando os revoke-security-group-egresscomandos revoke-security-group-ingressou.

Solucionar problemas de criação de anexos VPC da Amazon VPC Transit Gateways

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

Problema

Falha no anexo da VPC.

Causa

A causa pode ser uma das seguintes:

1. O usuário que estiver criando o anexo da VPC não tem as permissões corretas para criar o perfil vinculada ao serviço.
2. Há um problema de controle de utilização devido a muitas solicitações do IAM. Por exemplo, o AWS CloudFormation está sendo usado para criar permissões e perfis.
3. A conta tem o perfil vinculado a serviços e esse perfil foi modificado.
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 perfis vinculados a serviços. Para obter mais informações, consulte Permissões de perfis vinculados a serviços no Guia do usuário do IAM. Uma vez que o usuário tenha as permissões, crie o anexo da VPC.
2. Crie o anexo VPC manualmente. Para obter mais informações, consulte the section called “Criar um anexo de VPC”.
3. Verifique se a função vinculada a serviços tem as permissões corretas. Para obter mais informações, consulte the section called “Transit gateway”.
4. Verifique se o gateway de trânsito está no estado `available`. Para obter mais informações, consulte the section called “Visualizar um gateway de trânsito”.

AWS Anexos da função de rede Transit Gateway

Você pode criar um anexo de função de rede para conectar seu gateway de trânsito diretamente ao AWS Network Firewall. Isso elimina a necessidade de criar e gerenciar a inspeção VPCs.

Com um anexo de firewall, provisiona e gerencia AWS automaticamente todos os recursos necessários nos bastidores. Você verá um novo anexo do Transit Gateway em vez de terminais de firewall individuais. Isso simplifica o processo de implementação da inspeção centralizada do tráfego de rede.

Antes de usar um anexo de firewall, você deve primeiro criar o anexo em AWS Network Firewall. Para ver as etapas de criação do anexo, consulte Introdução ao AWS Network Firewall

gerenciamento no Guia do AWS Network Firewall desenvolvedor Depois que o firewall for criado, você poderá visualizar o anexo no console do Transit Gateway na seção Anexos. O anexo será listado com um tipo de função de rede.

Tópicos

Aceitar ou rejeitar um anexo de função de rede do AWS Transit Gateway

Você pode usar o console Amazon VPC, a AWS Network Firewall CLI ou a API para aceitar ou rejeitar um anexo de função de rede do Transit Gateway, incluindo anexos do Firewall de Rede. Se você for proprietário de um gateway de trânsito e alguém tiver criado um anexo de firewall para seu gateway de trânsito a partir de outra conta, você precisará aceitar ou rejeitar a solicitação de anexo.

Para aceitar ou rejeitar um anexo de função de rede usando a CLI do Firewall de Rede, consulte `AcceptNetworkFirewallTransitGatewayAttachment` ou `RejectNetworkFirewallTransitGatewayAttachment` APIs na Referência da AWS Network Firewall API.

Aceite ou rejeite um anexo de função de rede usando o console

Use o console da Amazon VPC para aceitar ou rejeitar um anexo de função de rede do Transit Gateway.

Para aceitar ou rejeitar um anexo de função de rede 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.
3. Escolha os anexos do Transit Gateway.
4. Selecione o anexo com um estado de aceitação pendente e um tipo de função de rede.
5. Escolha Ações e escolha Aceitar anexo ou Rejeitar anexo.
6. Na caixa de diálogo de confirmação, escolha Aceitar ou Rejeitar.

Se você aceitar o anexo, ele ficará ativo e o firewall poderá inspecionar o tráfego. Se você rejeitar o anexo, ele entrará em um estado rejeitado e, eventualmente, será excluído.

Exibir anexos da função de rede do AWS Transit Gateway

Você pode visualizar seus anexos de funções de rede, incluindo seus AWS Network Firewall anexos, usando o console da Amazon VPC ou o console do Network Manager para obter uma representação visual da sua topologia de rede.

Exibir um anexo de função de rede usando o console do Network Manager

Você pode visualizar os anexos de uma função de rede usando o console do Network Manager.

Para ver os anexos do firewall no Network Manager

1. Abra o console do Network Manager em https://console.aws.amazon.com/networkmanager/casa/.
2. Crie uma rede global no Network Manager, se você ainda não tiver uma.
3. Registre seu gateway de trânsito com o Network Manager.
4. Em Redes globais, escolha a rede global em que o anexo está localizado.
5. No painel de navegação, selecione Gateways de trânsito.
6. Escolha o gateway de trânsito do qual você deseja visualizar os anexos.
7. Escolha Visualização em árvore de topologia. Os anexos do Firewall de Rede aparecem com um ícone de função de rede.
8. Para ver detalhes sobre um anexo de firewall específico, selecione o gateway de trânsito na visualização de topologia e, em seguida, selecione a guia Função de rede.

O console do Network Manager fornece informações detalhadas sobre os anexos do firewall, incluindo seu status, gateway de trânsito associado e zonas de disponibilidade.

Visualize um anexo de função de rede usando o console do Amazon VPC Console

Use o console da VPC para ver uma lista dos tipos de anexos do gateway de trânsito.

Para visualizar os tipos de anexo do Transit Gateway usando o console VPC

- Consulte Visualizar um anexo da VPC.

Roteie o tráfego por meio de um anexo de função de rede do AWS Transit Gateway

Depois de criar um anexo de função de rede, você precisa atualizar as tabelas de rotas do gateway de trânsito para enviar tráfego pelo firewall para inspeção usando o console da Amazon VPC ou usando a CLI. Para obter as etapas para atualizar uma associação de tabela de rotas do Transit Gateway, consulteAssociar uma tabela de rotas do gateway de trânsito.

Roteie o tráfego por meio de um anexo de firewall usando o console

Use o console do Amazon VPC Console para rotear o tráfego por meio de um anexo de função de rede de gateway de trânsito.

Para rotear o tráfego por meio de um anexo de função de rede 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.
3. Escolha as tabelas de rotas do Transit Gateway.
4. Selecione a tabela de rotas que você deseja modificar.
5. Escolha Ações e, em seguida, escolha Criar rota estática.
6. Para CIDR, insira o bloco CIDR de destino para a rota.
7. Em Anexo, selecione o anexo da função de rede. Por exemplo, isso pode ser um AWS Network Firewall anexo.
8. Selecione Criar rota estática.

> **Note**
>
> Somente rotas estáticas são suportadas.

O tráfego correspondente ao bloco CIDR em sua tabela de rotas agora será enviado ao anexo do firewall para inspeção antes de ser encaminhado ao seu destino final.

Roteie o tráfego por meio de um anexo de função de rede usando a CLI ou a API

Use a linha de comando ou a API para rotear um anexo de função de rede do Transit Gateway.

Para rotear o tráfego por meio de um anexo de função de rede usando a linha de comando ou a API

- Use `create-transit-gateway-route`.

  Por exemplo, a solicitação pode ser rotear um anexo de firewall de rede:

```
aws ec2 create-transit-gateway-route \
  --transit-gateway-route-table-id tgw-rtb-0123456789abcdef0 \
  --destination-cidr-block 0.0.0.0/0 \
  --transit-gateway-attachment-id tgw-attach-0123456789abcdef0
```

  A saída então retorna:

```
{
  "Route": {
    "DestinationCidrBlock": "0.0.0.0/0",
    "TransitGatewayAttachments": [
      {
        "ResourceId": "network-firewall",
        "TransitGatewayAttachmentId": "tgw-attach-0123456789abcdef0",
        "ResourceType": "network-function"
      }
    ],
    "Type": "static",
    "State": "active"
  }
}
```

O tráfego correspondente ao bloco CIDR em sua tabela de rotas agora será enviado ao anexo do firewall para inspeção antes de ser encaminhado ao seu destino final.

AWS Site-to-Site VPN anexos nos Amazon VPC Transit Gateways

Você pode conectar um anexo de Site-to-Site VPN a um gateway de trânsito nos Amazon VPC Transit Gateways, permitindo que você conecte sua VPCs rede à rede local. Tanto as rotas dinâmicas quanto as estáticas são suportadas, assim como IPv4 IPv6 e.

Requisitos

- Anexar uma conexão VPN ao gateway de trânsito requer a especificação do gateway do cliente da VPN, que tem requisitos específicos do dispositivo. Antes de criar um anexo de Site-to-Site VPN, revise os requisitos do gateway do cliente para garantir que seu gateway esteja configurado corretamente. Para obter mais informações sobre esses requisitos, incluindo exemplos de arquivos de configuração de gateway, consulte Requisitos para seu dispositivo de gateway de cliente Site-to-Site VPN no Guia AWS Site-to-Site VPN do usuário.
- Para estática VPNs, você também precisará primeiro adicionar as rotas estáticas à tabela de rotas do gateway de trânsito. As rotas estáticas em uma tabela de rotas de gateway de trânsito que têm como alvo um anexo de VPN não são filtradas pela Site-to-Site VPN, pois isso pode permitir um fluxo de tráfego de saída não intencional ao usar uma VPN baseada em BGP. Para ver as etapas necessárias para adicionar uma rota estática à tabela de rotas de gateway de trânsito, consulte Criar uma rota estática.

Você pode criar, visualizar ou excluir um anexo Site-to-Site VPN do Transit Gateway usando o console Amazon VPC ou usando a CLI AWS .

Tarefas

- Criar um anexo do gateway de trânsito para uma VPN usando Amazon VPC Transit Gateways
- Visualizar um anexo de VPN usando Amazon VPC Transit Gateways
- Excluir um anexo de VPN usando Amazon VPC Transit Gateways

Criar um anexo do gateway de trânsito para uma VPN usando Amazon VPC Transit Gateways

Como 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, selecione Anexos do gateway de trânsito.
3. Selecione Criar anexo do gateway de trânsito.
4. Em 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 Tipo de anexo, escolha VPN.
6. Em Gateway do cliente, siga uma destas opções:

- Para usar um gateway do cliente existente, selecione Existente e escolha o gateway que deseja usar.

  Se o gateway do cliente estiver atrás de um dispositivo de conversão de endereços 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, selecione Novo, em Endereço IP, insira um endereço IP público estático e BGP ASN.

  Em Opções de roteamento, escolha entre Dinâmico ou Estático. Para obter mais informações, consulte Opções de roteamento de Site-to-Site VPN no Guia do AWS Site-to-Site VPN usuário.

7. Em Opções de túnel, insira os intervalos CIDR e as chaves pré-compartilhadas para o túnel. Para obter mais informações, consulte Arquiteturas de Site-to-Site VPN.
8. Selecione Criar anexo do gateway de trânsito.

Para criar um anexo VPN usando o AWS CLI

Use o comando create-vpn-connection.

Visualizar um anexo de VPN usando Amazon VPC Transit Gateways

Como 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, selecione Anexos do gateway de trânsito.
3. Na coluna Tipo de recurso, procure por VPN. Os anexos da VPN serão exibidos.
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.

Excluir um anexo de VPN usando Amazon VPC Transit Gateways

Como excluir 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, selecione Anexos do gateway de trânsito.
3. Selecione o anexo da VPN.
4. Escolha o ID do recurso da conexão VPN para acessar a página Conexões VPN.
5. Selecione Ações, Excluir.
6. Quando a confirmação for solicitada, escolha Excluir.

Para excluir um anexo de VPN usando o AWS CLI

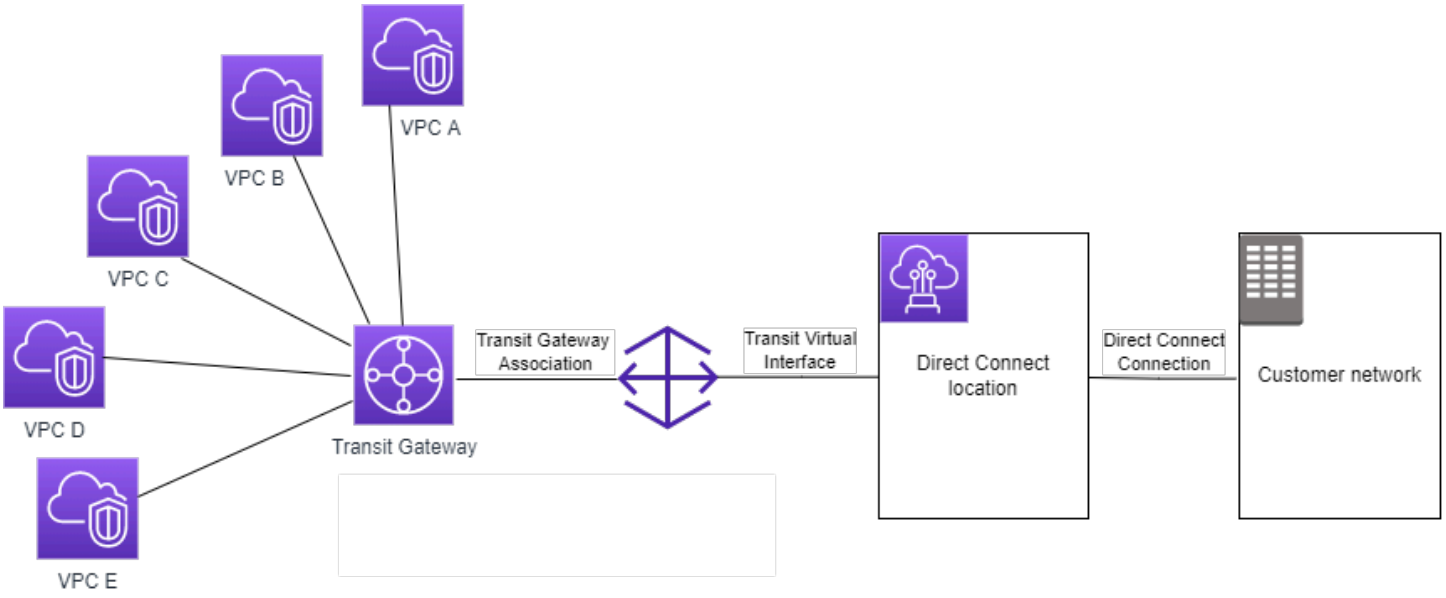
Use o comando delete-vpn-connection.

Anexos do gateway de trânsito a um gateway do Direct Connect no Amazon VPC Transit Gateways

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

- Gerencie uma única conexão para várias VPCs ou VPNs que estejam na mesma região.
- Anuncie prefixos do local para AWS e do AWS local para o local.

O diagrama a seguir ilustra como o gateway Direct Connect permite que você crie uma única conexão com sua conexão Direct Connect que todos VPCs possam usar.



A solução envolve os componentes abaixo:

- Um gateway de trânsito
- Gateway do Direct Connect
- Uma associação entre o gateway do Direct Connect e o gateway de trânsito.
- Uma interface virtual de trânsito que é anexada ao gateway do 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 de gateway de trânsito no Amazon VPC Transit Gateways

Você pode emparelhar gateways de trânsito entre regiões e entre regiões e rotear o tráfego entre eles, o que inclui tráfego e. IPv4 IPv6 Para fazer isso, crie um anexo de emparelhamento no seu gateway de trânsito e especifique um gateway de trânsito. O gateway de trânsito entre pares pode estar na sua conta ou ser de outra conta. Você também pode solicitar um anexo de emparelhamento de sua própria conta a um gateway de trânsito em outra conta.

Depois de criar 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 exclusivo ASNs para cada gateway de trânsito emparelhado para aproveitar os recursos futuros de propagação de rotas.

O emparelhamento do gateway de trânsito não suporta a resolução de nomes de host IPv4 DNS públicos ou privados em IPv4 endereços privados em nenhum dos VPCs lados do anexo de emparelhamento do gateway de trânsito 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 gateways de trânsito, consulte AWS Transit Gateways. FAQs

Considerações sobre a AWS região de aceitação

É possível emparelhar gateways de trânsito através dos limites da região de adesão. Para obter informações sobre essas regiões e como se inscrever, consulte Gerenciando AWS regiões. Leve o seguinte em consideração ao usar o emparelhamento de gateway de trânsito nestas regiões:

- É possível 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 aceitação da região, AWS compartilha os seguintes dados da conta com a conta que aceita o anexo de emparelhamento:
  - Conta da AWS ID
  - ID de gateway de trânsito
  - Código da região
- Quando o anexo do gateway de trânsito é excluído, os dados da conta acima também são excluídos.
- Recomenda-se excluir o anexo de emparelhamento do gateway de trânsito antes de cancelar a adesão à região. Caso o anexo de emparelhamento não seja excluído, o tráfego poderá continuar a passar pelo anexo e as cobranças continuarão sendo recebidas. Se o anexo não for excluído, é possível 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, pode-se incorrer em cobranças em uma Região que aceita o anexo, incluindo as Regiões não aderidas. Para obter mais informações, consulte Preços do AWS Transit Gateway.

Tarefas

- Criar um anexo de emparelhamento usando Amazon VPC Transit Gateways
- Aceitar ou rejeitar uma solicitação de anexo emparelhamento usando o Amazon VPC Transit Gateways

- Adicionar uma rota à tabela de rotas do gateway de trânsito usando Amazon VPC Transit Gateways
- Excluir um anexo de emparelhamento usando o Amazon VPC Transit Gateways

Criar um anexo de emparelhamento usando Amazon VPC Transit Gateways

Antes de começar, confirme o ID do gateway de trânsito a ser anexada. Se o gateway de trânsito estiver em outro Conta da AWS, verifique se você tem a Conta da AWS ID do proprietário do gateway de trânsito.

Após a criação do anexo de emparelhamento, o proprietário do gateway de trânsito aceitante 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, selecione Anexos do gateway de trânsito.
3. Selecione Criar anexo do gateway de trânsito.
4. Em ID do gateway de trânsito, escolha o gateway de trânsito para o anexo. É possível escolher um gateway de trânsito que se possua. Os gateways de trânsito compartilhados não estão disponíveis para emparelhamento.
5. Em Tipo de anexo, selecione Conexão de emparelhamento.
6. Se desejar, insira uma tag de nome para o anexo.
7. Em Conta, siga um destes procedimentos:
   - Se o gateway de trânsito estiver em sua conta, selecione Minha conta.
   - Se o gateway de trânsito estiver em um local diferente Conta da AWS, escolha Outra conta. Em ID da conta, insira o ID da Conta da AWS .
8. Em Região, selecione a região na qual o gateway de trânsito está localizado.
9. Em 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).

Para criar um anexo de emparelhamento usando o AWS CLI

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

Aceitar ou rejeitar uma solicitação de anexo emparelhamento usando o Amazon VPC Transit Gateways

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, é possível rejeitar qualquer solicitação de conexão de emparelhamento recebida que esteja no estado `pendingAcceptance`. É necessário 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. SelecioneAções, 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. SelecioneAções, Rejeitar anexo do gateway de trânsito.

Para aceitar ou rejeitar um anexo de emparelhamento usando o 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 usando Amazon VPC Transit Gateways

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 aceitante também deve adicionar uma rota estática à tabela de rotas do gateway de trânsito.

Como criar 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 tabela de rotas para a qual a rota será criada.
4. Selecione Ações, Criar rota estática.
5. Na página 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. Selecione Criar rota estática.

Para criar uma rota estática usando o 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”.

Excluir um anexo de emparelhamento usando o Amazon VPC Transit Gateways

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. SelecioneAções, Excluir anexo do gateway de trânsito.
5. Insira **`delete`** e selecione Excluir.

Para excluir um anexo de emparelhamento usando o AWS CLI

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

Conecte anexos e Connect peers nos Amazon VPC Transit Gateways

É possível 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 é compatível com 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, é possível 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 peer do Transit Gateway Connect consiste em duas sessões de emparelhamento do BGP que terminam na infraestrutura gerenciada. 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 seu peer Connect estiver operando sem a sessão de peering BGP dupla recomendada configurada para redundância, ele poderá sofrer uma perda momentânea de conectividade durante as operações de infraestrutura. AWS É altamente recomendável configurar ambas as sessões de emparelhamento BGP no par de Connect. Ao configurar 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 já existente como mecanismo de transporte subjacente. Isto é chamado 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 mecanismo de transporte, primeiro você precisará integrar o Direct Connect ao AWS Transit Gateway. Para ver as etapas para criar essa integração, consulte Integrar dispositivos SD-WAN com o AWS Transit Gateway e. AWS Direct Connect

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 do `169.254.0.0/16` intervalo para. IPv4 Opcionalmente, você pode especificar um bloco CIDR /125 do `fd00::/8` intervalo 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 IPv4 intervalo no equipamento como o endereço IP do BGP. Ao usar IPv6, se o bloco CIDR interno for fd00: :/125, você deverá configurar o primeiro endereço nesse intervalo (fd00: :1) na interface de túnel do equipamento.

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

Endereço IP do par

O endereço IP de par (endereço IP externo GRE) no lado do dispositivo do par do Connect. Pode ser qualquer endereço IP. O endereço IP pode ser um IPv6 endereço IPv4 or, mas deve ser da mesma família de endereços IP do endereço do gateway de trânsito.

Endereço do 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 um endereço IP não for especificado, o primeiro endereço disponível do bloco CIDR do gateway de trânsito será utilizado.

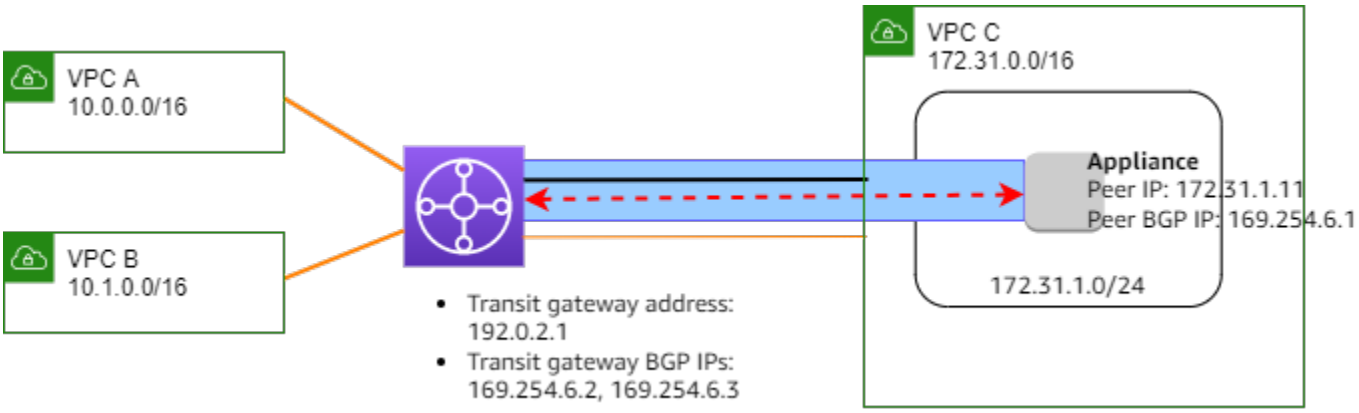
Ao criar ou modificar um gateway de trânsito, é possível adicionar um bloco CIDR de gateway de trânsito.

O endereço IP pode ser um IPv6 endereço IPv4 or, mas deve ser da mesma família de endereços IP que o endereço IP do mesmo nível.

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

O Transit Gateway Connect para emparelhamento BGP suporta somente BGP multiprotocolo (MP-BGP), em que o endereçamento Unicast é necessário para estabelecer também uma sessão BGP para IPv4 Unicast. IPv6 Você pode usar os dois IPv6 endereços IPv4 e para os 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 usar o eBGP, deverá configurar o ebgp-multihop com um valor time-to-live (TTL) de 2.
  - BGP interno (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 peer iBGP (dispositivo de terceiros), a menos que as rotas sejam originadas de um peer eBGP e devam ter sido configuradas. next-hop-self As rotas anunciadas pelo dispositivo de terceiros sobre o emparelhamento do iBGP devem ter um ASN.
  - MP-BGP (extensões multiprotocolo para BGP): usado para oferecer suporte a vários tipos de protocolos, como famílias de endereços. IPv4 IPv6
- O tempo limite padrão do keep-alive do BGP é de 10 segundos e o temporizador de espera padrão é de 30 segundos.
- IPv6 O emparelhamento BGP não é suportado; somente o emparelhamento BGP IPv4 baseado é suportado. IPv6 prefixos são trocados pelo peering BGP usando IPv4 MP-BGP.
- Não há suporte para Detecção de encaminhamento bidirecional (BFD).
- Não há suporte para reinício normal do BGP.
- Ao criar um par de gateway de trânsito, se um número ASN de par não for especificado, será atribuído um número ASN do gateway de trânsito. Isso significa que o dispositivo e o gateway de trânsito estarão no mesmo sistema autônomo executando 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 vários caminhos de mesmo custo (ECMP) entre dispositivos múltiplos, é necessário 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 deve corresponder ao Número de sistema autônomo (ASN). 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.
- Não há compatibilidade com rotas estáticas.
- Configure a MTU do túnel GRE para ser menor que a MTU da interface externa subtraindo a sobrecarga do cabeçalho GRE (8 bytes) e do cabeçalho IP externo (20 bytes). Por exemplo, se a MTU da interface externa for de 1500 bytes, defina a MTU do túnel GRE para 1472 bytes (1500 - 8 - 20 = 1472) para evitar a fragmentação do pacote.

Tarefas

- Criar um anexo Connect usando Amazon VPC Transit Gateways
- Criar um par do Connect usando gateways de trânsito da Amazon VPC
- Visualizar anexos e pares do Connect usando Amazon VPC Transit Gateways
- Modificar anexos do Connect e as tags de pares do Connect usando Amazon VPC Transit Gateways
- Excluir um par do Connect usando Amazon VPC Transit Gateways
- Excluir um anexo Connect usando gateways de trânsito da Amazon VPC

Criar um anexo Connect usando Amazon VPC Transit Gateways

Para criar um anexo do Connect, é necessário especificar um anexo já existente como anexo de transporte. É possível especificar um anexo da VPC ou um anexo do Direct Connect como o anexo de transporte.

Como 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, selecione Anexos do gateway de trânsito.
3. Escolha Create transit gateway attachment (Criar anexo do gateway de trânsito).
4. (Opcional) Em Tag de nome, especifique uma tag de nome para o anexo.
5. Em ID do gateway de trânsito, escolha o gateway de trânsito para o anexo.
6. Em Tipo do anexo, selecione Connect.
7. Em ID do anexo de transporte, 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 o AWS CLI

Use o comando create-transit-gateway-connect.

Criar um par do Connect usando gateways de trânsito da Amazon VPC

É possível 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. Pode-se configurar um bloco CIDR de gateway de trânsito ao criar ou modificar um gateway de trânsito.

Ao criar o par do Connect, é necessário especificar o endereço IP externo GRE no lado do dispositivo do par do Connect.

Como 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, selecione Anexos do gateway de trânsito.
3. Escolha o anexo do Connect, e selecione Ações, Criar um par do Connect.
4. (Opcional) Em Tag de nome, especifique uma tag de nome para o par do Connect.
5. (Opcional) Em 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. Em Endereço de GRE do par, especifique o endereço IP externo GRE para o lado do dispositivo do par do Connect.

7. Para blocos BGP Inside CIDR IPv4, especifique o intervalo de IPv4 endereços internos que são usados para emparelhamento de BGP. Especifique um bloco CIDR /29 no intervalo `169.254.0.0/16`.
8. (Opcional) Para blocos BGP Inside CIDR IPv6, especifique o intervalo de IPv6 endereços internos que são usados para emparelhamento de BGP. Especifique um bloco CIDR /125 no intervalo `fd00::/8`.
9. (Opcional) Em ASN do 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, é possível 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 configurar o Peer ASN para ser diferente do Transit Gateway ASN (eBGP), deverá configurar o ebgp-multihop com um valor (TTL) de 2. time-to-live
10. Selecione Criar par do Connect.

Para criar um Connect peer usando o AWS CLI

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

Visualizar anexos e pares do Connect usando Amazon VPC Transit Gateways

Visualize os anexos e os pares do Connect.

Como visualizar anexos e 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, selecione Anexos do gateway de trânsito.
3. Selecione o anexo do Connect.
4. Para visualizar os pares do Connect para o anexo, selecione a guia Pares do Connect.

Para visualizar seus anexos do Connect e seus pares do Connect usando o AWS CLI

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

Modificar anexos do Connect e as tags de pares do Connect usando Amazon VPC Transit Gateways

É possível modificar as tags do anexo do Connect.

Como 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, selecione Anexos do gateway de trânsito.
3. Escolha o anexo do Connect e selecione Ações, Gerenciar tags.
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 Salvar.

É possível 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. Escolha o anexo do Connect e, em seguida, selecione Pares do Connect.
4. Escolha o par do Connect e selecione 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 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 usando Amazon VPC Transit Gateways

É possível excluir um par do Connect, caso ele não seja mais necessário.

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, selecione 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 o AWS CLI

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

Excluir um anexo Connect usando gateways de trânsito da Amazon VPC

É possível excluir um anexo do Connect, caso ele não seja mais necessário. Primeiro, você deve excluir todos os pares do Connect para o anexo.

Como 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 então, Ações, Excluir anexo do gateway de trânsito.
4. Insira **`delete`** e selecione Excluir.

Para excluir um anexo do Connect usando o AWS CLI

Use o comando delete-transit-gateway-connect.

Tabelas de rotas de gateway de trânsito no Amazon VPC Transit Gateways

Use tabelas de rotas de gateway de trânsito para configurar o roteamento para os anexos de gateway de trânsito. Uma tabela de rotas é uma tabela que contém regras que direcionam como seu tráfego de rede é roteado entre você VPCs e. VPNs Cada rota na tabela contém o intervalo de endereços IP para os destinos para os quais deseja-se enviar tráfego.

As tabelas de rotas do gateway de trânsito permitem a associação de uma tabela a um anexo do gateway de trânsito. Todos os anexos VPC, VPN, gateway do Direct Connect, Peering e Connect são compatíveis. Quando associadas, as rotas desses anexos são propagadas do anexo para a tabela de rotas do gateway de trânsito de destino. Um anexo pode ser propagado para várias tabelas de rotas.

Além disso, é possível criar e gerenciar rotas estáticas com uma tabela de rotas. Por exemplo, pode-se usar uma rota estática como rota de backup no caso de uma interrupção na rede que afete qualquer rota dinâmica.

Tarefas

- Criar uma tabela de rotas do gateway de trânsito usando gateways de trânsito da Amazon VPC
- Visualizar tabelas de rotas do gateway de trânsito usando Amazon VPC Transit Gateways
- Associar uma tabela de rotas do gateway de trânsito usando Amazon VPC Transit Gateways
- Excluir uma associação da tabela de rotas de um gateway de trânsito usando Amazon VPC Transit Gateways
- Habilitar a propagação de rota para uma tabela de rotas do gateway de trânsito usando Amazon VPC Transit Gateways
- Desabilitar a propagação de rotas usando Amazon VPC Transit Gateways
- Crie uma rota estática usando Amazon VPC Transit Gateways
- Excluir uma rota estática usando Amazon VPC Transit Gateways
- Substituir uma rota estática usando Amazon VPC Transit Gateways
- Exportar tabelas de rotas para o Amazon S3 usando Amazon VPC Transit Gateways
- Excluir uma tabela de rotas do gateway de trânsito usando Amazon VPC Transit Gateways
- Criar uma referência de lista de prefixos de tabela de rotas usando o Amazon VPC Transit Gateways
- Modificar uma referência da lista de prefixos usando Amazon VPC Transit Gateways
- Excluir uma referência da lista de prefixos usando Amazon VPC Transit Gateways

Criar uma tabela de rotas do gateway de trânsito usando gateways de trânsito da Amazon VPC

Como criar 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 Tabelas de rotas do gateway de trânsito.
3. Escolha Create transit gateway route table (Criar tabela de roteamento do gateway de trânsito).
4. (Opcional) Em 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 ID do gateway de trânsito, selecione o gateway de trânsito para a tabela de rotas.
6. Selecione Criar tabela de rotas do gateway de trânsito.

Para criar uma tabela de rotas do gateway de trânsito usando o AWS CLI

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

Visualizar tabelas de rotas do gateway de trânsito usando Amazon VPC Transit Gateways

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 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 de uma tabela de rotas ou escolha sua ID para exibir informações sobre suas 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 usando Amazon VPC Transit Gateways

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, selecione Tabelas de rotas do gateway de trânsito.
3. Selecione a tabela de rotas.
4. Na parte inferior da página, selecione a guia Associações.
5. Selecione Criar associação.
6. Escolha o anexo para associar e selecione Criar associação.

Para associar uma tabela de rotas do gateway de trânsito usando o AWS CLI

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

Excluir uma associação da tabela de rotas de um gateway de trânsito usando Amazon VPC Transit Gateways

É possível desassociar uma tabela de rotas do gateway de trânsito de um anexo do 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, selecione Tabelas de rotas do gateway de trânsito.
3. Selecione a tabela de rotas.

4. Na parte inferior da página, selecione a guia Associações.
5. Escolha o anexo para desassociar e selecione Excluir associação.
6. Quando a confirmação for solicitada, selecione Excluir associação.

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

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

Habilitar a propagação de rota para uma tabela de rotas do gateway de trânsito usando Amazon VPC Transit Gateways

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 Tabelas de rotas do gateway de trânsito.
3. Escolha a tabela de rotas para a qual você criará a propagação.
4. Selecione Ações, Criar propagação.
5. Na página Criar propagação, escolha o anexo.
6. Selecione 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 usando Amazon VPC Transit Gateways

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

Como 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 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. selecione a guia Propagações.
5. Selecione o anexo, e então, Excluir propagação.

6. Quando a confirmação for solicitada, selecione Excluir propagação.

Para desativar a propagação de rotas usando o AWS CLI

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

Crie uma rota estática usando Amazon VPC Transit Gateways

É possível criar uma rota estática para uma VPC, para uma VPN 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 Transit Gateway que têm como alvo um anexo de VPN não são filtradas pela Site-to-Site VPN. Isso pode permitir que o tráfego de saída flua de maneira não intencional ao usar uma VPN baseada em BGP.

Como criar 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 tabela de rotas para a qual a rota será criada.
4. Selecione Ações, Criar rota estática.
5. Na página Criar rota estática, insira o bloco CIDR para o qual deseja criar a rota e escolha Ativa.
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 a rota será criada.
4. Escolha Actions (Ações), Create static route (Criar rota estática).
5. Na página Criar rota estática, insira o bloco CIDR para o qual deseja criar a rota e escolha Blackhole.

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 usando Amazon VPC Transit Gateways

Exclua 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 Tabelas de rotas do gateway de trânsito.
3. Escolha a tabela de rotas da qual excluirá a rota e selecione Rotas.
4. Escolha a rota e ser excluída.
5. Selecione Excluir rota estática.
6. Na caixa de diálogo de confirmação, selecione Excluir rota estática.

Para excluir uma rota estática usando o AWS CLI

Use o comando delete-transit-gateway-route.

Substituir uma rota estática usando Amazon VPC Transit Gateways

Substitua uma rota estática em uma tabela de rotas do gateway de trânsito por outra rota estática.

Como 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 Tabelas de rotas do gateway de trânsito.
3. Escolha a rota que você deseja substituir na tabela de rotas.
4. Na seção de detalhes, selecione a guia Rotas.
5. Selecione Ações, Substituir rota estática.
6. Em Tipo, escolha Ativo ou Blackhole.
7. No menu suspenso Selecionar anexo, escolha o gateway de trânsito que substituirá o atual na tabela de rotas.

8. Selecione 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 usando Amazon VPC Transit Gateways

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 Tabelas de rotas do gateway de trânsito.
3. Escolha a tabela e roteamento que inclui as rotas para exportar
4. Selecione Ações, Exportar rotas.
5. Na página Exportar rotas, em nome do bucket do S3, digite o nome do bucket S3.
6. Para filtrar as rotas exportadas, especifique os parâmetros de filtro na seção Filtros da página.
7. Selecione Exportar rotas.

Para acessar as rotas exportadas, abra o console do Amazon S3 https://console.aws.amazon.com/s3/em e navegue até o bucket que você especificou. 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. Escolha o arquivo e selecione 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 usando Amazon VPC Transit Gateways

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 Tabelas de rotas do gateway de trânsito.
3. Selecione a tabela de rotas a ser excluída.
4. Selecione Ações, 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.

Criar uma referência de lista de prefixos de tabela de rotas usando o Amazon VPC Transit Gateways

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 pode ser definida e gerenciada. É possível usar uma lista de prefixos para simplificar o gerenciamento dos endereços IP referenciados nos recursos para rotear o tráfego de rede. Por exemplo, se você freqüentemente especifica o mesmo destino CIDRs em várias tabelas de rotas do Transit Gateway, você pode gerenciá-las CIDRs em uma única lista de prefixos, em vez de referenciar repetidamente o mesmo CIDRs em cada tabela de rotas. Caso seja necessário remover um bloco CIDR de destino, pode-se 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.

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 Tabelas de rotas do gateway de trânsito.
3. Escolha a tabela de rotas do gateway de trânsito.
4. Selecione Ações, Criar referência da lista de prefixos.
5. Em ID da lista de prefixos, selecione o ID da lista de prefixos.
6. Em Tipo, escolha se o tráfego para essa lista de prefixos deve ser permitido (Ativo) ou desconectado (Blackhole).
7. Em ID do anexo do gateway de trânsito, selecione o ID do anexo para o qual deseja rotear o tráfego.
8. Selecione Criar referência da lista de prefixos.

Para criar uma referência de lista de prefixos usando o AWS CLI

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

Modificar uma referência da lista de prefixos usando Amazon VPC Transit Gateways

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 Rotas. Para modificar as entradas na lista de prefixos, use a tela Listas de prefixos gerenciadas. 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 Tabelas de rotas do gateway de trânsito.
3. Selecione a tabela de rotas do gateway de trânsito.
4. No painel inferior, selecione Referências de lista de prefixos.
5. Escolha a referência da lista de prefixos e selecione Modificar referências.
6. Em Tipo, escolha se o tráfego para essa lista de prefixos deve ser permitido (Activo) ou desconectado (Blackhole).
7. Em ID do anexo do gateway de trânsito, selecione o ID do anexo para o qual deseja rotear o tráfego.
8. Selecione Modificar referência da lista de prefixos.

Para modificar uma referência de lista de prefixos usando o AWS CLI

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

Excluir uma referência da lista de prefixos usando Amazon VPC Transit Gateways

Caso uma referência da lista de prefixos não seja mais necessária, é possível 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 Tabelas de rotas do gateway de trânsito.
3. Escolha a tabela de rotas do gateway de trânsito.
4. Escolha a referência da lista de prefixos e selecione Excluir referências.
5. Selecione Excluir referências.

Para modificar uma referência de lista de prefixos usando o AWS CLI

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

Tabelas de política de gateway de trânsito no Amazon VPC Transit Gateways

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.

É possível 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, pode-se 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.

Tarefas

- Criar uma tabela de políticas de gateway de trânsito usando gateway de trânsito da Amazon VPC

- Excluir uma tabela de políticas de gateway de trânsito usando o Amazon VPC Transit Gateways

Criar uma tabela de políticas de gateway de trânsito usando gateway de trânsito da Amazon VPC

Como criar uma tabela de políticas 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, selecione Tabela de políticas de gateway de trânsito.
3. Selecione Criar tabela de políticas de gateway de trânsito.
4. (Opcional) Em Tag de nome, insira um nome para a política de gateway de trânsito. Isso cria uma tag cujo valor é o nome especificado.
5. Em 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 usando o Amazon VPC Transit Gateways

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

Como excluir uma tabela de políticas 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, selecione Tabelas de políticas de gateway de trânsito.
3. Escolha a tabela de políticas de gateway de trânsito a ser excluída.
4. Selecione Ações e, em seguida, Excluir tabela de políticas.
5. Confirme a exclusão da tabela.

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

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

Multicast nos gateways de trânsito da Amazon VPC

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

Tópicos

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. A associação do domínio multicast é definida 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 ao grupo multicast é definida por interfaces de rede elástica individuais conectadas às EC2 instâncias.

- Protocolo de gerenciamento de grupo da internet (IGMP): 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 IGMPv2 protocolo e os domínios multicast de associação a grupos IGMP e estáticos (baseados em API).

- Fonte multicast — uma interface de rede elástica associada a uma EC2 instância compatível que é 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 multicast — Uma interface de rede elástica associada a uma EC2 instância compatível que recebe tráfego 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

- O multicast do Transit Gateway pode não ser adequado para negociação de alta frequência ou aplicativos sensíveis ao desempenho. É altamente recomendável que você revise os limites das cotas de multicast. Entre em contato com sua conta ou com a equipe do Solution Architect para obter uma análise detalhada de seus requisitos de desempenho.
- Para obter informações sobre as regiões suportadas, consulte AWS Transit Gateway FAQs.
- 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 uma instância que não é do Nitro for usada, será necessário desativar a caixa de seleção Origem/Destino. Para obter informações sobre como desativar a verificação, consulte Alterar a verificação de origem ou destino no Guia do EC2 usuário da Amazon.
- Uma instância que não é do Nitro não pode ser um remetente multicast.

- O roteamento multicast não é suportado por meio de Site-to-Site VPN 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 obter mais informações, consulte Unidade de transmissão máxima (MTU).
- Na inicialização, um host IGMP envia vários IGMP JOIN mensagens para ingressar em um grupo multicast (normalmente de 2 a 3 tentativas). No caso improvável de que todo o IGMP JOIN se as mensagens forem perdidas, o host não se tornará parte do grupo multicast do Transit Gateway. Nesse cenário, você precisará reativar o IGMP JOIN mensagem do host usando métodos específicos do aplicativo.
- A associação ao grupo começa com o recebimento de IGMPv2 JOIN mensagem pelo gateway de trânsito e termina com o recebimento do IGMPv2 LEAVE mensagem. O gateway de trânsito mantém o controle dos hosts que se uniram com sucesso ao grupo. Como um roteador multicast em nuvem, o gateway de trânsito emite um IGMPv2 QUERY mensagem para todos os membros a cada dois minutos. Cada membro envia um IGMPv2 JOIN mensagem 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 de sua to-be-queried lista. Um explícito IGMPv2 LEAVE a mensagem remove imediata 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 gateway de trânsito, o gateway de trânsito continua enviando dados multicast ao host por sete minutos (420 segundos) após o último IGMP bem-sucedido JOIN mensagem. O gateway de trânsito continua enviando consultas de associação ao host por até 12 horas ou até receber um IGMP LEAVE mensagem do anfitrião.
- 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. A configuração do grupo de segurança nos hosts IGMP (instâncias) e qualquer ACLs configuração nas sub-redes do host deve permitir essas mensagens do 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 multicast estáticos, os Amazon VPC Transit Gateways removem automaticamente grupos e fontes estáticos, ENIs pois eles não existem mais. Isso é realizado

assumindo periodicamente a função vinculada ao serviço Transit Gateway a ser descrita ENIs na conta.

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

Roteamento multicast

Ao permitir o multicast em um gateway de trânsito, este atua como um roteador de multicast. Ao adicionar uma sub-rede a um domínio multicast, todo o tráfego multicast é enviado para o gateway de trânsito que está associado a esse domínio multicast.

Rede 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 Rede ACLs no Guia do usuário da Amazon VPC.

Para tráfego multicast de Internet Group Management Protocol (IGMP), é necessário 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, é necessário permitir o tráfego de entrada da origem do grupo. Para obter mais informações, consulte Grupos de segurança no Manual do usuário da Amazon VPC.

É necessário 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.

Tipo	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

É necessário estabelecer ao menos as regras de saída 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

Domínios de multicast nos Amazon VPC Transit Gateways

Um domínio de multicast permite a segmentação de uma rede multicast em diferentes domínios. Para começar a usar a multicast com um gateway de trânsito, crie um domínio de multicast e associe sub-redes ao domínio.

Atributos do domínio de multicast

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

Atributo	Descrição
`Igmpv2Support` (AWS CLI) IGMPv2 suporte (console)	Esse atributo determina como os membros do grupo se unem ou saem de um grupo de 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 e 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. Ao registrar membros do grupo multicast, também é necessári o cancelar o registro deles. O gateway de trânsito ignora uma mensagem IGMP `LEAVE` enviada por um membro do grupo adicionado manualmente.
`StaticSourcesSupport` (AWS CLI) Compatibilidade com fontes estáticas (console)	Esse atributo determina se há origens multicast estáticas para o grupo. 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

Atributo	Descrição
	associadas ao domínio de multicast podem enviar tráfego multicast, e os membros do grupo recebem esse tráfego.

Criar um domínio de multicast do IGMP usando os Amazon VPC Transit Gateways

Revise os atributos de domínio de multicast disponíveis, caso isso ainda não tenha sido feito. Para obter mais informações, consulte the section called “Domínios de multicast”.

Como criar um domínio de 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, selecione Multicast do gateway de trânsito.
3. Escolha Create transit gateway multicast domain (Criar domínio de multicast do gateway de trânsito).
4. Em Tag 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 obter IGMPv2 suporte, marque a caixa de seleção.
7. Em Compatibilidade com fontes 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).

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 de multicast de origem estática usando Amazon VPC Transit Gateways

Revise os atributos de domínio de multicast disponíveis, caso isso ainda não tenha sido feito. Para obter mais informações, consulte the section called “Domínios de multicast”.

Como criar um domínio de multicast estático usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Multicast do gateway de trânsito.
3. Escolha Create transit gateway multicast domain (Criar domínio de multicast do gateway de trânsito).
4. Em Tag de nome, 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 obter IGMPv2 suporte, desmarque a caixa de seleção.
7. Em 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).

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 de multicast usando Amazon VPC Transit Gateways

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 obter mais informações, consulte Anexos da Amazon VPC nos Amazon VPC Transit Gateways.

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

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Multicast do gateway de trânsito.
3. Selecione o domínio de multicast e depois Ações, Criar associação.
4. Em Selecione o anexo para associar, escolha o anexo do gateway de trânsito.
5. Em Selecione sub-redes para associar, escolha as sub-redes nas quais deseja incluir o domínio de multicast.
6. Selecione Criar associação.

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

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

Desassociar uma sub-rede de um domínio de multicast usando Amazon VPC Transit Gateways

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

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, selecione Multicast do gateway de trânsito.
3. Selecione o domínio multicast.
4. Selecione a guia Associações.
5. Escolha a sub-rede e selecione Ações, Excluir associação.

Para desassociar sub-redes usando o AWS CLI

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

Visualizar as associações de domínio de multicast usando Amazon VPC Transit Gateways

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

Como visualizar um domínio de multicast usando o console

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

Para visualizar um domínio multicast usando o AWS CLI

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

Adicionar tags a um domínio de multicast usando Amazon VPC Transit Gateways

Adicione tags aos recursos para ajudar a organizá-los e identificá-los, por exemplo, por finalidade, proprietário ou ambiente. É possível adicionar várias tags a cada domínio de multicast. As chaves de tag devem ser exclusivas para cada domínio de multicast. Uma tag com uma chave que já está associada ao domínio de multicast for adicionada, o valor dessa tag será atualizado. Para obter mais informações, consulte Como marcar seus EC2 recursos da Amazon.

Como adicionar tags a um domínio de multicast usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Multicast do gateway de trânsito.
3. Selecione o domínio multicast.
4. Selecione Ações, Gerenciar tags.
5. Para cada tag, selecione Adicionar nova tag e insira uma Chave e um Valor para a tag.
6. Escolha Salvar.

Para adicionar tags a um domínio multicast usando o AWS CLI

Use o comando create-tags.

Excluir um domínio de multicast usando Amazon VPC Transit Gateways

Use o procedimento a seguir para excluir um domínio de multicast.

Para excluir um domínio de multicast usando o console

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

Para excluir um domínio multicast usando o AWS CLI

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

Domínios de multicast compartilhados nos Amazon VPC Transit Gateways

Com o compartilhamento de domínio de multicast, os proprietários de domínio de multicast podem compartilhar o domínio com outras contas da AWS dentro da organização ou entre organizações no AWS Organizations. O proprietário do domínio de multicast, pode criar e gerenciar esse domínio de forma centralizada. Uma vez compartilhado, esses usuários podem executar as seguintes operações sobre um domínio de 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 de multicast pode compartilhar um domínio de multicast com:

- AWS contas dentro de sua organização ou entre organizações em AWS Organizations
- Uma unidade organizacional dentro de sua organização em AWS Organizations
- Toda a sua organização em AWS Organizations
- AWS contas externas de AWS Organizations.

  Para compartilhar um domínio multicast com uma AWS conta fora da sua organização, você deve criar um compartilhamento de recursos usando e AWS Resource Access Manager, em seguida, escolher Permitir compartilhamento com qualquer pessoa ao selecionar os principais com os quais compartilhar o domínio multicast. 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 .

Conteúdo

Pré-requisitos para compartilhar um domínio de multicast

- Para compartilhar um domínio multicast, você deve possuí-lo em sua AWS conta. Não é possível compartilhar um domínio de multicast que tenha sido compartilhado com você.
- Para compartilhar um domínio multicast com sua organização ou uma unidade organizacional em AWS Organizations, você deve habilitar o compartilhamento com 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 se integra com AWS Resource Access Manager ()AWS RAM. AWS RAM é um serviço que permite que você compartilhe seus AWS recursos com qualquer AWS conta ou por meio de AWS Organizations. Com o AWS RAM, pode-se compartilhar recursos possuídos criando um compartilhamento de recursos. Um compartilhamento de recursos especifica os recursos a serem compartilhados, e os usuários com os quais compartilhá-los. Os consumidores podem ser AWS contas individuais, unidades organizacionais ou uma organização inteira em AWS Organizations.

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

Permissões do domínio de multicast compartilhado

Permissões para proprietários

Os proprietários são responsáveis por gerenciar o domínio de 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 AWS Organizations para visualizar, modificar e excluir recursos que os consumidores criam em domínios multicast compartilhados.

Permissões para clientes

Os clientes podem executar as seguintes operações em domínios de multicast compartilhados da mesma maneira que fariam em domínios de multicast criados por eles:

- 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 clientes são responsáveis por gerenciar os recursos que criados por eles no domínio de multicast compartilhado.

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

Faturamento e medição

Proprietários e clientes não recebem cobranças adicionais para compartilhar domínios de multicast.

Cotas

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

Compartilhe recursos entre zonas de disponibilidade nos Amazon VPC Transit Gateways

Para garantir a distribuição de recursos entre as zonas de disponibilidade de uma região, os Amazon VPC Transit Gateways mapeiam as zonas de disponibilidade de forma independente aos nomes de cada conta. Isso pode resultar em diferenças na nomenclatura de zonas de disponibilidade entre contas. Por exemplo, a zona de disponibilidade da `us-east-1a` sua AWS conta pode não ter a mesma localização `us-east-1a` de outra AWS conta.

Para identificar o local dos domínios de multicast relativos às suas contas, use o ID da Zona de Disponibilidade (AZ ID). O ID AZ é um identificador exclusivo e consistente para uma zona de disponibilidade em todas as AWS contas. Por exemplo, `use1-az1` é uma ID AZ para a `us-east-1` região e está no mesmo local em todas as AWS contas.

Para visualizar o AZ IDs das zonas de disponibilidade em sua conta

1. Abra o AWS RAM console em https://console.aws.amazon.com/ram/casa.
2. As AZ IDs da região atual são exibidas no painel Sua ID de AZ no lado direito da tela.

Compartilhar um domínio de multicast usando Amazon VPC Transit Gateways

Quando um proprietário compartilha um domínio de multicast com você, as seguintes ações são possíveis:

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

> **Note**
>
> Para compartilhar um domínio de multicast, você deve adicioná-lo a um compartilhamento de recursos. Um compartilhamento de recursos é um AWS RAM recurso que permite que você compartilhe seus recursos entre AWS contas. Um compartilhamento de recursos especifica os recursos a serem compartilhados, e os clientes com os quais compartilhá-los. Ao compartilhar um domínio multicast usando o Amazon Virtual Private Cloud Console, você o adiciona a um compartilhamento de recursos existente. Para adicionar o domínio de multicast a um novo compartilhamento de recursos, primeiro crie o compartilhamento de recursos usando o console do AWS RAM.
>
> Se você faz parte de uma organização AWS Organizations e o compartilhamento dentro de sua organização está habilitado, os consumidores em sua organização recebem automaticamente acesso ao domínio multicast compartilhado. Caso contrário, os clientes receberão um convite para integrar o compartilhamento de recursos e recebem acesso ao domínio de multicast depois de aceitar o convite.

Você pode compartilhar um domínio multicast de sua propriedade usando o Amazon Virtual Private Cloud console, o AWS RAM console ou o. AWS CLI

Como compartilhar um domínio de multicast que você possui 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, selecione Domínios de multicast.
3. Escolha o domínio de multicast e, em seguida, Ações, Excluir domínio de multicast.
4. Selecione seu compartilhamento de recurso e escolha Compartilhar domínio de multicast.

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

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

Para compartilhar um domínio multicast que você possui usando o AWS CLI

Use o comando create-resource-share.

Cancelar o compartilhamento de um domínio de multicast compartilhado usando Amazon VPC Transit Gateways

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

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

Para cancelar o compartilhamento de um domínio de multicast, você deve removê-lo do compartilhamento de recursos. Você pode fazer isso no AWS RAM console ou no AWS CLI.

Para cancelar o compartilhamento de um domínio de multicast que você possui, é preciso removê-lo do compartilhamento de recursos. Você pode fazer isso usando o Amazon Virtual Private Cloud, AWS RAM console ou AWS CLI o.

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

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

2. No painel de navegação, selecione Domínios de multicast.
3. Escolha seu domínio de multicast e, em seguida, Ações, Encerrar compartilhamento.

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

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

Para cancelar o compartilhamento de um domínio multicast compartilhado que você possui usando o AWS CLI

Use o comando disassociate-resource-share.

Identificar um domínio de multicast compartilhado usando Amazon VPC Transit Gateways

Proprietários e consumidores podem identificar domínios multicast compartilhados usando o e Amazon Virtual Private Cloud AWS CLI

Como identificar um domínio de multicast compartilhado usando o *Amazon Virtual Private Cloud Console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Domínios de multicast.
3. Selecione seu domínio de multicast.
4. Na página Detalhes do Domínio Multicast de Trânsito, visualize a ID do Proprietário para identificar a ID da AWS conta do domínio multicast.

Para identificar um domínio multicast compartilhado usando o AWS CLI

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

Registrar fontes com um grupo de multicast usando Amazon VPC Transit Gateways

> **Note**
>
> Esse procedimento só é necessário quando o atributo suporte para origens estáticas for definido como 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 de multicast
- As IDs interfaces de rede das fontes
- Endereço IP do grupo de multicast

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, selecione Multicast do gateway de trânsito.
3. Selecione o domínio de multicast e, em seguida, Ações, Adicionar fontes do grupo.
4. Em Endereço IP do grupo, insira o bloco IPv4 CIDR ou o bloco IPv6 CIDR a ser atribuído ao domínio multicast.
5. Em Selecionar interfaces de rede, selecione as interfaces da rede dos remetentes multicast.
6. Selecione Adicionar origens.

Para registrar fontes usando o AWS CLI

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

Registrar membros com um grupo multicast usando gateways de trânsito Amazon VPC

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
- As IDs interfaces de rede dos membros do grupo
- Endereço IP do grupo de multicast

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 Multicast do gateway de trânsito.
3. Selecione o domínio multicast e, em seguida, Ações, Adicionar membros do grupo.
4. Em Endereço IP do grupo, insira o bloco IPv4 CIDR ou o bloco IPv6 CIDR a ser atribuído ao domínio multicast.
5. Em Selecionar interfaces de rede, selecione as interfaces de rede dos receptores de multicast.
6. Selecione Adicionar membros.

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 usando Amazon VPC Transit Gateways

Não é necessário seguir este procedimento a menos que seja adicionada uma origem ao grupo multicast manualmente.

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, selecione Multicast do gateway de trânsito.
3. Selecione o domínio multicast.
4. Selecione a guia Grupos.
5. Escolha as origens e escolha Remover origem.

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 de multicast usando Amazon VPC Transit Gateways

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

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, selecione Multicast do gateway de trânsito.
3. Selecione o domínio multicast.
4. Escolha a guia Grupos.
5. Selecione os membros e escolha Remover membro.

Para cancelar o registro de membros usando o AWS CLI

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

Visualizar grupos multicast usando Amazon VPC Transit Gateways

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

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, selecione Multicast do gateway de trânsito.
3. Selecione o domínio multicast.
4. Selecione a guia Grupos.

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"
        }
    ]
}
```

Configurar multicast para Windows Server no Amazon VPC Transit Gateways

São necessárias etapas adicionais ao configurar o multicast para funcionar com gateways de trânsito no Windows Server 2019 ou 2022. Para configurar isso PowerShell, você precisará usar e executar os seguintes comandos:

Para configurar o multicast para o Windows Server usando PowerShell

1. Altere o Windows Server para usar IGMPv2 em vez da IGMPv3 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, o comando a seguir pode ser executado para definir a versão IGMP para 2.:
   > `Set-NetIPv4Protocol -IGMPVersion Version2`

2. O Firewall do Windows elimina a maior parte do tráfego UDP por padrão. Primeiro, é necessário 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. Reinicie a EC2 instância.
5. Teste sua aplicação multicast para garantir que o tráfego esteja fluindo conforme o esperado.

Exemplo: Gerenciar configurações IGMP usando Amazon VPC Transit Gateways

Quando há pelo menos um host que usa o protocolo IGMP para tráfego multicast, a AWS cria automaticamente o grupo multicast quando recebe uma mensagem IGMP `JOIN` 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 de 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, consulte Criar uma VPC no Guia do usuário da Amazon VPC.
2. Crie uma sub-rede na VPC. Para obter mais informações, consulte Criar uma sub-rede no Guia do usuário da Amazon VPC.
3. Crie um gateway de trânsito configurado para o tráfego multicast. Para obter mais informações, consulte the section called “Criar um gateway de trânsito”.
4. Crie um anexo da VPC Para obter mais informações, consulte the section called “Criar um anexo de VPC”.
5. Crie um domínio de multicast configurado para ser compatível com IGMP. Para obter mais informações, consulte the section called “Criar um domínio de multicast do IGMP”.

   Use as seguintes configurações:

- Ative o IGMPv2 suporte.
- Desabilite Compatibilidade com fontes estáticas.

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

Exemplo: Gerenciar configurações de origem estáticas usando Amazon VPC Transit Gateways

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

   Use as seguintes configurações:

- Desative IGMPv2 o suporte.
- Para adicionar fontes manualmente, habilite a 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 de 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 de multicast”.
7. Se habilitar Compatibilidade com fontes estáticas, adicione a fonte ao grupo multicast. Para obter mais informações, consulte the section called “Registrar origens com um grupo de multicast”.
8. Adicione os membros ao grupo multicast. Para obter mais informações, consulte the section called “Registrar membros com um grupo de multicast”.

Exemplo: Gerenciar configurações de membros de grupo estático no Amazon VPC Transit Gateways

Este exemplo mostra 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, consulte Criar uma VPC no Guia do usuário da Amazon VPC.
2. Crie uma sub-rede na VPC. Para obter mais informações, consulte Criar uma sub-rede no Guia do usuário da Amazon VPC.
3. Crie um gateway de trânsito configurado para o tráfego multicast. Para obter mais informações, consulte the section called “Criar um gateway de trânsito”.
4. Crie um anexo da VPC Para obter mais informações, consulte the section called “Criar um anexo de VPC”.

5. Crie um domínio de multicast configurado para não ser compatível com IGMP e para ser compatível com a adição de origens estaticamente. Para obter mais informações, consulte the section called “Criar um domínio de multicast de origem estática”.

   Use as seguintes configurações:

   - Desative IGMPv2 o suporte.
   - Desabilite 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 de multicast”.
7. Adicione os membros ao grupo multicast. Para obter mais informações, consulte the section called “Registrar membros com um grupo de multicast”.

Logs de fluxo de Gateways de trânsito da Amazon VPC

Os logs de fluxo de gateway de trânsito são um atributo do Amazon VPC Transit Gateways 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 o throughput nem a latência da rede. É possível criar ou excluir logs de fluxo sem qualquer risco de impacto na performance 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 de e para as interfaces de rede em sua VPCs, use os registros 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, é necessário ser o proprietário do gateway de trânsito. O proprietário do gateway de trânsito deve conceder permissão ao 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 obter 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 deseja publicar os dados de log de fluxo

Depois de 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.

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

Caso não precise mais de um log de fluxo, é possível 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. Após excluir um log de fluxo, pode levar vários minutos para a coleta de dados se encerrar. Para obter mais informações, consulte Excluir um registro de registros de fluxo do Amazon VPC Transit Gateways.

Você pode criar registros de fluxo para seus gateways de trânsito que podem publicar dados no CloudWatch Logs, no Amazon S3 ou no Amazon Data Firehose. Para obter mais informações, consulte:

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

Limitações

As limitações a seguir se aplicam aos logs de fluxo de gateway de trânsito:

- Não há compatibilidade com o tráfego multicast.
- Não há compatibilidade com os anexos do Connect. Todos os registros de fluxo do Connect aparecem sob o anexo de transporte e, portanto, devem ser habilitados no gateway de trânsito ou no anexo de transporte do Connect.

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, é possível especificar quais campos estão incluídos nos registros de log de fluxo e em qual ordem. Isso permite a criação de logs de fluxo específicos para as necessidades específicas, omitindo 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 deve-se 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 for texto sem formatação, todos os campos são do tipo STRING. Se o formato for Parquet, consulte a tabela para ver os tipos de dados do 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	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.	2

Campo	Descrição	Versão
	Tipo de dados em Parquet: INT_32	
resource-type	O tipo de recurso no qual a assinatura é criada. Para registros de fluxo do Transit Gateway, isso será TransitGateway. Tipo de dados em Parquet: STRING	6
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

Campo	Descrição	Versão
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
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

Campo	Descrição	Versão
srcaddr	O endereço de origem do tráfego de entrada. Tipo de dados em Parquet: STRING	2
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 informaçõ es, consulte Números de Protocolo da Internet Designados. Tipo de dados em Parquet: INT_32	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. Este valor 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	Versão
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
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 provenien te 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 Guia EC2 do usuário da Amazon. 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

Campo	Descrição	Versão
packets-lost-ttl-expired	Os pacotes foram perdidos devido à expiração do time-to-live. Tipo de dados em Parquet: INT_64	6
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 0, e 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

Campo	Descrição	Versão
region	A região que contém o gateway de trânsito no qual o tráfego é registrado. Tipo de dados em Parquet: STRING	4
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 de 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 de um AWS serviço. Para obter uma lista de valores possíveis, consulte o pkt-src-aws-service campo. Tipo de dados em Parquet: STRING	5

Controlar o uso de logs de fluxo

Por padrão, os usuários do não têm permissão para trabalhar com logs de fluxo. É possível 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 EC2 recursos da Amazon na Amazon EC2 API Reference.

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 ter mais informações, consulte Registros de registros de fluxo do Transit Gateway no Amazon CloudWatch Logs e Registros de fluxo de log dos Transit Gateways no Amazon S3 .

Preços dos logs de fluxo do Transit Gateway

As cobranças por ingestão de dados e armazenamento de dados para logs fornecidos são aplicáveis ao publicar 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.

Criar ou atualizar um perfil do IAM para logs de fluxo dos Amazon VPC Transit Gateways

Você pode atualizar uma função existente ou usar o procedimento a seguir para criar uma nova função para uso com registros de fluxo usando o AWS Identity and Access Management console.

Como criar um perfil do IAM para logs de fluxos

1. Abra o console do IAM em https://console.aws.amazon.com/iam/.

2. No painel de navegação, selecione Perfil e então, Criar perfil.
3. Em Selecionar tipo de entidade confiável, selecione serviço da AWS . Para Caso de uso, escolha EC2. Escolha Próximo.
4. Na página Adicionar permissões, selecione Avançar: Tags e, se desejar, adicione tags. Escolha Próximo.
5. Na página Nomear, revisar e criar, insira um nome para o perfil e, opcionalmente, forneça uma descrição. Selecione Criar perfil.
6. Escolha o nome do seu perfil. Em Adicionar permissões, selecione Criar política em linha e, em seguida, selecione 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. Selecione Revisar política.
8. Insira um nome para a política e selecione Criar política.
9. Selecione o nome do perfil. Em Relacionamentos de confiança, selecione Editar relacionamento de confiança. No documento da política existente, altere o serviço de `ec2.amazonaws.com` para `vpc-flow-logs.amazonaws.com`. Selecione Atualizar política de confiança.
10. Na página Resumo, anote o ARN do perfil. Esse ARN é necessário para criar o log de fluxo.

Registros de registros de fluxo do Transit Gateway no Amazon CloudWatch Logs

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 logs contêm registros do log de fluxos. Você pode criar vários logs de fluxos 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 for especificado que um log de fluxos deve capturar o tráfego rejeitado e outro log de fluxos deve capturar o tráfego aceito, o fluxo de logs combinado capturará todo o tráfego.

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 A data/hora é posterior à hora de término capturada no registro de log do 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 ao seu perfil 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 o seu perfil tem um relacionamento de confiança que permite que o serviço de logs de fluxo assuma o perfil.

```
{
  "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 fluxos, poderá substituir essa parte do ARN por um caractere curinga (*) e, em seguida, atualizar a política depois de criar o log de fluxos.

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

Permissões para que os usuários do IAM passem um perfil

Os usuários também devem ter permissões para usar a ação `iam:PassRole` para o perfil do IAM associado ao log de fluxos.

```
{
```

```
  "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 registros de fluxo do Transit Gateways que seja publicado em Amazon CloudWatch Logs

É possível criar logs de fluxos 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 obter mais informações, consulte Permissões para que os usuários do IAM passem um perfil.

Você pode criar um registro de CloudWatch fluxo da Amazon usando o console Amazon VPC ou a CLI AWS .

Como criar um log de fluxos do gateway de trânsito usando o console

1. Faça login no AWS Management Console e abra o console da Amazon VPC em. https://console.aws.amazon.com/vpc/
2. No painel de navegação, selecione Gateways de trânsito.
3. Marque as caixas de seleção de um ou mais gateways de trânsito e selecione Ações, Criar log de fluxos.
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. Em Formato de registro do log , selecione o formato para o registro de log de fluxo.

- Para usar o formato padrão, escolha AWS Formato padrão.
- Para usar um formato personalizado, escolha Formato personalizado e, em seguida, selecione os campos de Formato de log.

8. (Opcional) Selecione Adicionar nova tag para aplicar tags ao log de fluxo.
9. Selecione Criar log de fluxo.

Como criar um log de fluxo usando a linha de comando

Use um dos seguintes comandos.

- create-flow-logs (AWS CLI)
- New-EC2FlowLog (AWS Tools for Windows PowerShell)

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
```

Veja os registros de registros de fluxo do Transit Gateway na Amazon CloudWatch

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 log 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 fluxos. 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 obter mais informações, consulte Registros de log de fluxo de gateway de trânsito.

Processar registros de registros de fluxo do Transit Gateway no Amazon 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 Criação de métricas a partir de eventos de log usando filtros no Guia CloudWatch do usuário da Amazon.

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

Neste exemplo, há um log de fluxo para `tgw-123abc456bca`. 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.

Como 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, selecione Logs, Grupos de log.
3. Marque a caixa de seleção do grupo de logs e, em seguida, selecione Ações, Criar filtro de métrica.
4. Em Padrão do 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 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, selecione Testar padrão. Quando estiver pronto, selecione Avançar.
6. Insira um nome de filtro, um namespace para a métrica e o nome da métrica. Defina o valor da métrica como **1**. Quando terminar, selecione Avançar e, em seguida, selecione Criar filtro de métrica.

7. No painel de navegação, selecione Alarmes, 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 Selecionar métrica.
11. Configure o alarme como indicado a seguir e, em seguida, selecione Avançar:

    - Em Estatística, selecione Soma. Isso garante que o número total de pontos de dados do período especificado seja capturado.
    - Em Período, selecione 1 hora.
    - Em Sempre que, selecione Maior que/igual a e insira **10** como limite.
    - Em Configurações adicionais, Pontos de dados para alarme, deixe o padrão de **1**.
12. Em Notificação, selecione um tópico do SNS existente ou Criar novo tópico, para criar um novo. Escolha Próximo.
13. Insira um nome e uma descrição para o alarme e selecione Avançar.
14. Quando terminar de configurar o alarme, selecione Criar alarme.

Registros de fluxo de log dos Transit Gateways 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 usar com logs de fluxo, consulte Criação de um bucket no Guia do usuário do Amazon S3.

Para obter mais informações sobre o registro em log de várias contas, consulte Logs centralizados na Biblioteca de soluções AWS .

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

Conteúdo

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 Última modificação do arquivo de log de fluxo indica a data e hora em que o arquivo foi carregado no bucket do Amazon S3. Esta indicação 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

É possível 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, é possível especificar as seguintes opções.

- 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 houver um grande volume de logs e tipicamente direcionar consultas para uma hora específica, pode-se 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/
```

Ao 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/
```

Ao 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/
```

Ao 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 este bucket, as políticas a seguir serão automaticamente anexadas. Essa nova política gerada automaticamente é anexada à política original.

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 as 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": "arn:aws:s3:::bucket_name/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceAccount": "123456789012"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:region:123456789012:*"
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryCheck",
            "Effect": "Allow",
            "Principal": {"Service": "delivery.logs.amazonaws.com"},
            "Action": ["s3:GetBucketAcl"],
            "Resource": "arn:aws:s3:::bucket_name",
            "Condition": {
                "StringEquals": {
```

```
                    "aws:SourceAccount": "123456789012"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:region:123456789012:*"
                }
            }
        }
    ]
}
```

O ARN que você especifica *my-s3-arn* depende do uso de prefixos S3 compatíveis com o 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 individualmente Conta da AWS ARNs. 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, é necessário 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.

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

> **Note**
>
> O uso do S3 Bucket Keys permite que você economize nos custos de solicitação AWS Key Management Service (AWS KMS) diminuindo suas solicitações AWS KMS para as operações Encrypt, GenerateDataKey, e Decrypt por meio do uso de uma chave em nível de bucket. Por definição, as solicitações subsequentes que aproveitam essa chave em nível de bucket não resultam em solicitações de AWS KMS API nem validam o acesso em relação à AWS KMS política de chaves.

```
{
    "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 a função da conta de origem do Transit Gateway Flow Logs para o Amazon S3

Na conta de origem, crie a função de origem no AWS Identity and Access Management console.

Como criar a função da conta de origem

1. Faça login no AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, selecione Políticas.
3. Selecione Criar política.
4. Na página Criar política siga estes passos:
    1. Escolha JSON.
    2. Substitua o conteúdo dessa janela pela política de permissões no início desta seção.
    3. Selecione Avançar: tags e Avançar: revisar.
    4. Insira um nome e uma descrição opcional para a política e selecione Criar política.
5. No painel de navegação, selecione Perfis.
6. Selecione Create role.
7. Na opção Tipo de entidade confiável, escolha Política de confiança personalizada. Em Política de confiança personalizada, substitua `"Principal": {},` pelo seguinte, que especifica o serviço de entrega de logs. Selecione Avançar.

```
"Principal": {
   "Service": "delivery.logs.amazonaws.com"
},
```

8. Na página Adicionar permissões, marque a caixa de seleção correspondente à política criada anteriormente neste procedimento e, em seguida, escolha Avançar.
9. Insira um nome para a função e, opcionalmente, uma descrição.
10. Selecione Criar perfil.

Criar um registro de logs de fluxos do gateway de trânsito que seja publicado no Amazon S3

Depois de criar e configurar o bucket do Amazon S3, pode-se criar logs de fluxo para gateways de trânsito. É possível criar um log de fluxos do Amazon S3 usando o console do Amazon VPC ou a AWS CLI.

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

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Gateways de trânsito ou 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. Selecione Ações, 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.

Como definir as configurações do log de fluxo usando o console

1. Em Destino, selecione Enviar para um bucket do S3.
2. Em 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, uma política de recurso será automaticamernte criada e anexada ao bucket. Para obter mais informações, consulte Permissões do bucket do Amazon S3 para logs de fluxo.
3. Em 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 Formato padrão.

- Para criar um formato personalizado, escolha Formato personalizado. Em Formato de log, selecione os campos a serem incluídos no registro de log de fluxo.

4. Em 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 Prefixo do S3 compatível com Hive, Habilitar.
6. (Opcional) Para particionar seus logs de fluxo por hora, selecione A cada 1 hora (60 minutos).
7. (Opcional) Para adicionar uma etiqueta ao log de fluxo, escolha Adicionar nova tag e especifique a chave e o valor da tag.
8. Selecione 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-EC2FlowLog (AWS Tools for Windows PowerShell)

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/'
```

Visualizar registros de logs de fluxo do Transit Gateway no Amazon S3

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 Nome do bucket, selecione o bucket no qual os logs de fluxo são publicados.
3. Em Nome, marque a caixa de seleção ao lado do arquivo de log. No painel de visão geral do objeto, selecione Baixar.

Registros de log de fluxo processados no Amazon S3

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

Registros de fluxo de log dos Transit Gateways no Amazon Data Firehose

Tópicos

- Perfis do IAM para entrega entre contas
- Criar a função da conta de origem do Transit Gateway Flow Logs para o Amazon Data Firehose
- Criar a função de conta de destino dos logs de fluxo do Transit Gateway para o Amazon Data Firehose
- Criar um registro de logs de fluxos do gateway de trânsito que seja publicado no Amazon Data Firehose

Os logs de fluxo podem publicar dados de log de fluxo diretamente no Firehose. É possível 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 de logs de fluxo são publicados em um fluxo de entrega do Firehose, em formato de texto sem formatação. É necessário primeiro ter criado um fluxo de entrega do Firehose. Para saber as etapas de criação de fluxos de entrega, consulte Como criar um fluxo 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, é possível 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 de logs de fluxo entre contas para o Firehose, é necessário criar um perfil do IAM na conta de origem e um perfil do IAM na conta de destino.

Perfis

- Perfil da conta de origem
- Perfil da conta de destino

Perfil da conta de origem

Na conta de origem, crie um perfil que conceda as seguintes permissões. Neste exemplo, o nome do perfil é `mySourceRole`, mas é possível escolher um nome diferente para este perfil. A última instrução permite que o perfil na conta de destino assuma este perfil. As instruções de condição garantem que esse perfil seja passado somente para o serviço de entrega de logs e somente ao monitorar o recurso especificado. Ao criar sua política, especifique as VPCs interfaces de rede ou 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 esse perfil tem a política de confiança a seguir, que permite que o serviço de entrega de logs assuma o perfil.

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

Perfil da conta de destino

Na conta de destino, crie uma função com um nome que comece com AWSLogDeliveryFirehoseCrossAccountRole. Esse perfil deve conceder as seguintes permissões.

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

Certifique-se de que esse perfil tenha a seguinte política de confiança, que permite que este perfil seja assumido pelo perfil criado na conta de origem.

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

Criar a função da conta de origem do Transit Gateway Flow Logs para o Amazon Data Firehose

Na conta de origem, crie a função de origem no AWS Identity and Access Management console.

Como criar a função da conta de origem

1. Faça login no AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, selecione Políticas.

3. Selecione Criar política.
4. Na página Criar política siga estes passos:

    1. Escolha JSON.
    2. Substitua o conteúdo dessa janela pela política de permissões no início desta seção.
    3. Selecione Avançar: tags e Avançar: revisar.
    4. Insira um nome e uma descrição opcional para a política e selecione Criar política.
5. No painel de navegação, selecione Perfis.
6. Selecione Create role.
7. Na opção Tipo de entidade confiável, escolha Política de confiança personalizada. Em Política de confiança personalizada, substitua `"Principal": {},` pelo seguinte, que especifica o serviço de entrega de logs. Selecione Avançar.

    ```
    "Principal": {
       "Service": "delivery.logs.amazonaws.com"
    },
    ```
8. Na página Adicionar permissões, marque a caixa de seleção correspondente à política criada anteriormente neste procedimento e, em seguida, escolha Avançar.
9. Insira um nome para a função e, opcionalmente, uma descrição.
10. Selecione Criar perfil.

Criar a função de conta de destino dos logs de fluxo do Transit Gateway para o Amazon Data Firehose

Na conta de destino, crie a função de destino no AWS Identity and Access Management console.

Para criar a função da conta de destino

1. Faça login no AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, selecione Políticas.
3. Selecione Criar política.
4. Na página Criar política siga estes passos:

    1. Escolha JSON.

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

5. No painel de navegação, selecione Perfis.
6. Selecione Create role.
7. Na opção Tipo de entidade confiável, escolha Política de confiança personalizada. Em Política de confiança personalizada, substitua `"Principal": {},` pelo seguinte, que especifica o serviço de entrega de logs. Selecione Avançar.

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

8. Na página Adicionar permissões, marque a caixa de seleção correspondente à política criada anteriormente neste procedimento e, em seguida, escolha Avançar.
9. Insira um nome para a função e, opcionalmente, uma descrição.
10. Selecione Criar perfil.

Criar um registro de logs de fluxos do gateway de trânsito que seja publicado no Amazon Data Firehose

Crie um log de fluxos do gateway de trânsito que seja publicado no Amazon Data Firehose. Antes de criar o log de fluxo, certifique-se de ter configurado as funções da conta IAM de origem e destino para entrega entre contas e de ter criado o stream de entrega do Firehose. Consulte Logs de fluxo no Amazon Data Firehose para obter mais informações. Você pode criar um registro de fluxo do Firehose usando o console Amazon VPC ou a CLI. AWS

Como criar um log de fluxo de gateway de trânsito que publique no Firehose usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Gateways de trânsito ou 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. Selecione Ações, Criar log de fluxo.

5. Em Destino, escolha Enviar para um Sistema de entrega Firehose.
6. Em ARN do fluxo de entrega do Firehose, escolha o ARN de um fluxo de entrega criado e no qual o log de fluxo deverá ser publicado.
7. Em 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 Formato padrão.
   - Para criar um formato personalizado, escolha Formato personalizado. Em Formato de log, selecione os campos a serem incluídos no registro de log de fluxo.
8. (Opcional) Para adicionar uma etiqueta ao log de fluxo, escolha Adicionar nova tag e especifique a chave e o valor da tag.
9. Selecione Criar log de fluxo.

Como criar um log de fluxo publicado no Firehose usando a ferramenta de linha de comando

Use um dos seguintes comandos:

- create-flow-logs (CLI)AWS
- New-EC2FlowLog (AWS Tools for Windows PowerShell)

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
```

Crie e gerencie registros de fluxo do Amazon VPC Transit Gateways usando APIs ou a CLI

É possível executar as tarefas descritas nesta página por meio da linha de comando.

As seguintes limitações se aplicam ao usar o create-flow-logscomando:

- `--resource-ids` tem uma restrição máxima de 25 tipos de recurso `TransitGateway` ou `TransitGatewayAttachment`.
- `--traffic-type` não é um campo obrigatório por padrão. Uma mensagem de erro será exibida se esse valor for fornecido 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. Uma mensagem de erro será exibida se qualquer outro valor for fornecido. 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 os campos a serem incluidos não forem definidos. Esse limite se aplica apenas a recursos do tipo gateway de trânsito.

Criar um log de fluxos

- create-flow-logs (AWS CLI)
- New-EC2FlowLog (AWS Tools for Windows PowerShell)

Descrever logs de fluxo

- describe-flow-logs (AWS CLI)
- Get-EC2FlowLog (AWS Tools for Windows PowerShell)

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

- get-log-events (AWS CLI)
- Obter- CWLLog Evento (AWS Tools for Windows PowerShell)

Excluir um log de fluxo

- delete-flow-logs (AWS CLI)
- Remove-EC2FlowLog (AWS Tools for Windows PowerShell)

Exibir os registros de log de fluxo do Amazon VPC Transit Gateways

Exiba informações sobre os registros de logs fluxo do seu gateway de trânsito por meio do Amazon VPC. Ao escolher um 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.

Como visualizar informações sobre logs de fluxo para gateways 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) ou Transit gateway attachments (Anexos do gateway de trânsito).
3. Escolha um gateway de trânsito ou um anexo do gateway de trânsito e selecione Logs de fluxo. As informações sobre os logs de fluxo são exibidas nessa guia. A coluna Tipo de destino indica o destino no qual os logs de fluxo são publicados.

Gerenciar tags de logs de fluxo do Amazon VPC Transit Gateways

Você pode adicionar ou remover tags para um log de fluxo nos consoles Amazon EC2 e Amazon VPC.

Como adicionar ou remover tags de um log de fluxo do 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) ou Transit gateway attachments (Anexos do gateway de trânsito).

3. Selecione um gateway de trânsito ou um anexo do gateway de trânsito
4. Escolha Gerenciar tags para o log de fluxo necessário.
5. Para adicionar uma nova tag, escolha Criar tag. Para remover uma tag, seelcione o botão de exclusão (x).
6. Selecione Salvar.

Pesquisar os registros de logs de fluxo da Amazon VPC Transit Gateways

Você pode pesquisar seus registros de registro de fluxo que são publicados no CloudWatch Logs usando o console do CloudWatch Logs. Os filtros de métrica podem ser usados 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 logs.
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 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 registro de registros de fluxo do Amazon VPC Transit Gateways

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 é publicado no Amazon S3 não remove as políticas do bucket e as listas de controle de acesso ao arquivo de log (). ACLs

Como excluir um log de fluxo de gateway de trânsito

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Gateways de trânsito.
3. Escolha um ID de gateway de trânsito.
4. Na seção Logs de fluxos, escolha os logs de fluxos que deseja excluir.
5. Escolha Ações e depois Excluir grupo de logs.
6. Confirme a exclusão do fluxo selecionando Excluir.

Métricas e eventos nos Amazon VPC Transit Gateways

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.

CloudWatch métricas

Você pode usar CloudWatch a Amazon para recuperar estatísticas sobre pontos de dados para seus gateways de trânsito como um conjunto ordenado de dados de séries temporais, conhecido como métricas. Essas métricas podem ser usadas para verificar se o sistema está executando conforme o esperado. Para obter mais informações, consulte CloudWatch métricas nos Amazon VPC Transit Gateways.

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.

Logs de fluxo da VPC

Você pode usar os registros de fluxo da VPC para capturar informações detalhadas sobre o tráfego de e para o VPCs que está conectado aos seus gateways de trânsito. Para obter mais informações, consulte Logs de fluxo da VPC no Guia do usuário do Amazon Virtual Private Cloud.

CloudTrail troncos

Você pode usar AWS CloudTrail para capturar informações detalhadas sobre as chamadas feitas para a API do Transit Gateway e armazená-las como arquivos de log no Amazon S3. Você pode usar esses CloudTrail registros para determinar quais chamadas foram feitas, o endereço IP de origem da chamada, quem fez a chamada, quando a chamada foi feita e assim por diante. Para obter mais informações, consulte CloudTrail troncos.

CloudWatch Eventos usando o Network Manager

Você pode usar AWS Network Manager para encaminhar eventos para e CloudWatch, em seguida, rotear 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 Monitorando sua rede global com CloudWatch eventos no Guia do usuário de redes AWS globais para gateways de trânsito.

CloudWatch métricas nos Amazon VPC Transit Gateways

A Amazon VPC publica pontos de dados na Amazon CloudWatch para seus gateways de trânsito e anexos de gateway de trânsito. CloudWatchpermite que você recupere estatísticas sobre esses pontos de dados como um conjunto ordenado de dados de séries temporais, conhecido 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.

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

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

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

Conteúdo

Métricas do gateway de trânsito

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

Todas as métricas são sempre relatadas. Seus valores dependem do tráfego através do gateway de trânsito. Consulte as dimensões suportadas em Dimensões métricas do Transit Gateway .

Métrica	Descrição
`BytesDropCountBlackhole`	O número de bytes removidos porque corresponderam a uma rota `blackhole` . Estatísticas: a única estatística significativa é `Sum`.
`BytesDropCountNoRoute`	Número de bytes removidos porque não corresponderam a uma rota.

Métrica	Descrição
	Estatísticas: a única estatística significativa é `Sum`.
`BytesIn`	O número de bytes recebidos pelo gateway de trânsito. Estatísticas: a única estatística significativa é `Sum`.
`BytesOut`	O número de bytes enviados do gateway de trânsito. Estatísticas: a única estatística significativa é `Sum`.
`PacketsIn`	O número de pacotes recebidos pelo gateway de trânsito. Estatísticas: a única estatística significativa é `Sum`.
`PacketsOut`	O número de pacotes enviados pelo gateway de trânsito. Estatísticas: a única estatística significativa é `Sum`.
`PacketDropCountBlackhole`	O número de pacotes removidos porque corresponderam a uma rota `blackhole` . Estatísticas: a única estatística significativa é `Sum`.
`PacketDropCountNoRoute`	Número de pacotes removidos porque não corresponderam a uma rota. Estatísticas: a única estatística significativa é `Sum`.
`PacketDropCountTTLExpired`	O número de pacotes descartados porque o TTL expirou. Estatísticas: a única estatística significativa é `Sum`.

Métricas de nível de anexo e zona de disponibilidade

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 suportados, consulte the section called “Anexos de recursos”.

As métricas da zona de disponibilidade estão disponíveis para zonas de disponibilidade ativadas (AZs) em anexos do gateway de trânsito. Somente anexos de VPC oferecem suporte a métricas por AZ. Todas as métricas de nível AZ são publicadas na conta do proprietário do gateway de trânsito. As métricas AZ individuais de um anexo também são publicadas na conta do proprietário do anexo. O proprietário do anexo pode visualizar somente as métricas por AZ de seu próprio anexo.

Todas as métricas são sempre relatadas. Seus valores dependem do tráfego de entrada e/ou saída do anexo do gateway de trânsito. Consulte as dimensões suportadas em Dimensões métricas do Transit Gateway .

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

Métrica	Descrição
	Estatísticas: a única estatística significativa é `Sum`.
`PacketDropCountNoRoute`	Número de pacotes removidos porque não corresponderam a uma rota. Estatísticas: a única estatística significativa é `Sum`.
`PacketDropCountTTLExpired`	O número de pacotes descartados porque o TTL expirou. Estatísticas: a única estatística significativa é `Sum`.

Dimensões métricas do Transit Gateway

Filtre os dados métricos do gateway de trânsito usando as seguintes dimensões:

Dimensão	Descrição
`TransitGateway`	Filtra os dados da métrica pelo gateway de trânsito.
`TransitGatewayAttachment`	Filtra os dados da métrica por anexo do gateway de trânsito.
`TransitGateway`, `AvailabilityZone`	Filtra os dados métricos por gateway de trânsito e zona de disponibilidade.
`TransitGatewayAttachment`, `AvailabilityZone`	Filtra os dados métricos por anexo do gateway de trânsito e zona de disponibilidade.

Registre chamadas de API dos Amazon VPC Transit Gateways usando AWS CloudTrail

O Amazon VPC Transit Gateways é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou um. AWS service (Serviço da AWS) CloudTrail captura todas as chamadas de API para o Transit Gateway como eventos. As chamadas capturadas incluem chamadas do console do gateway de trânsito e chamadas de código para as operações de API do gateway de trânsito. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita ao Transit Gateway, o endereço IP do qual a solicitação foi feita, quando foi feita e detalhes adicionais.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar o seguinte:

- Se a solicitação foi feita com credenciais de usuário raiz ou credenciais de usuário.
- Se a solicitação foi feita em nome de um usuário do Centro de Identidade do IAM.
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro AWS service (Serviço da AWS).

CloudTrail está ativo Conta da AWS quando você cria a conta e você tem acesso automático ao histórico de CloudTrail eventos. O histórico de CloudTrail eventos fornece um registro visível, pesquisável, baixável e imutável dos últimos 90 dias de eventos de gerenciamento registrados em um. Região da AWS Para obter mais informações, consulte Trabalhando com o histórico de CloudTrail eventos no Guia AWS CloudTrail do usuário. Não há CloudTrail cobrança pela visualização do histórico de eventos.

Para um registro contínuo dos eventos dos Conta da AWS últimos 90 dias, crie uma trilha ou um armazenamento de dados de eventos do CloudTrailLake.

CloudTrail trilhas

Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Todas as trilhas criadas usando o AWS Management Console são multirregionais. Só é possível criar uma trilha de região única ou de várias regiões usando a AWS CLI. É recomendável criar uma trilha multirregional porque você captura todas as atividades Regiões da AWS em sua conta. Ao criar uma trilha de região única, é possível visualizar somente os eventos registrados na Região da

AWS da trilha. Para obter mais informações sobre trilhas, consulte Criar uma trilha para a Conta da AWS e Criar uma trilha para uma organização no Guia do usuário do AWS CloudTrail .

Você pode entregar uma cópia dos seus eventos de gerenciamento em andamento para o bucket do Amazon S3 sem nenhum custo CloudTrail criando uma trilha. No entanto, existem taxas de armazenamento do Amazon S3. Para obter mais informações sobre CloudTrail preços, consulte AWS CloudTrail Preços. Para receber informações sobre a definição de preços do Amazon S3, consulte Definição de preços do Amazon S3.

CloudTrail Armazenamentos de dados de eventos em Lake

CloudTrail O Lake permite que você execute consultas baseadas em SQL em seus eventos. CloudTrail O Lake converte eventos existentes no formato JSON baseado em linhas para o formato Apache ORC. O ORC é um formato colunar de armazenamento otimizado para recuperação rápida de dados. Os eventos são agregados em armazenamentos de dados de eventos, que são coleções imutáveis de eventos baseados nos critérios selecionados com a aplicação de seletores de eventos avançados. Os seletores que aplicados a um armazenamento de dados de eventos controlam quais eventos persistem e estão disponíveis para consulta. Para obter mais informações sobre o CloudTrail Lake, consulte Trabalhando com o AWS CloudTrail Lake no Guia AWS CloudTrail do Usuário.

CloudTrail Os armazenamentos e consultas de dados de eventos em Lake incorrem em custos. Ao criar um armazenamento de dados de eventos, você escolhe a opção de preço que deseja usar para ele. A opção de preço determina o custo para a ingestão e para o armazenamento de eventos, e o período de retenção padrão e máximo para o armazenamento de dados de eventos. Para obter mais informações sobre CloudTrail preços, consulte AWS CloudTrail Preços.

Eventos de gerenciamento do Transit Gateway

Os eventos de gerenciamento fornecem informações sobre as operações de gerenciamento que são realizadas nos recursos do seu Conta da AWS. Também são conhecidas como operações de ambiente de gerenciamento. Por padrão, CloudTrail registra eventos de gerenciamento.

Amazon VPC Transit Gateways geram logs de todas as operações do ambiente de gerenciamento como eventos de gerenciamento. Para obter uma lista das operações do plano de controle do Amazon VPC Transit Gateways nas quais o Transit Gateway se conecta CloudTrail, consulte a Referência da API do Amazon VPC Transit Gateways.

Exemplos de eventos do gateway de trânsito

Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a operação de API solicitada, a data e a hora da operação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, os eventos não aparecem em nenhuma ordem específica.

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log 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 da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

Os arquivos de log incluem eventos para todas as chamadas de API para sua AWS conta, 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 um exemplo de registro de CloudTrail log da API do Transit Gateway para um usuário que criou um Transit Gateway usando o console. O console pode ser identificado usando o elemento `userAgent`. As chamadas de APIs solicitadas podem ser identificadas 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"
}
```

Gerenciamento de identidade e acesso no Amazon VPC Transit Gateways

AWS usa credenciais de segurança para identificá-lo e conceder acesso aos seus AWS recursos. Você pode usar os recursos do AWS Identity and Access Management (IAM) para permitir que outros usuários, serviços e aplicativos usem seus AWS recursos de forma total ou limitada, sem compartilhar suas credenciais de segurança.

Por padrão, os usuários do IAM não têm permissão para criar, visualizar ou modificar AWS recursos. 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. Ao anexar uma política a um usuário ou grupo de usuários, isso concede ou nega aos usuários permissão para realizar as tarefas especificadas nos atributos especificados.

Para trabalhar com um gateway de trânsito, uma das seguintes políticas AWS gerenciadas 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/*"
        }
    ]
}
```

Usar funções vinculadas a serviço para gateways de trânsito no Amazon VPC Transit Gateways

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 Perfis vinculados 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`

AWSServiceRoleForVPCTransitO Gateway usa a política gerenciadaAWSVPCTransitGatewayServiceRolePolicy.

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua um perfil vinculado a serviço. Para obter mais informações, consulte Permissões de perfil vinculado ao serviço no Guia do usuário do IAM.

Criar a função vinculada ao serviço

Você não precisa criar manualmente a função AWSServiceRoleForVPCTransitGateway. A Amazon VPC cria essa função quando você anexa uma VPC a um gateway de trânsito na sua conta.

Editar a função vinculada ao serviço

Você pode editar a descrição do AWSServiceRoleForVPCTransitGateway usando o IAM. Para obter mais informações, consulte Editar uma descrição de perfil vinculado ao serviço no Guia do usuário do IAM.

Excluir a função vinculada ao serviço

Se você não precisar mais usar gateways de trânsito, recomendamos que você exclua o AWSServiceRoleForVPCTransitGateway.

Você pode excluir essa função vinculada ao serviço somente depois de excluir todos os anexos VPC do Transit Gateway em sua conta. AWS Isso garante que a permissão para acessar os anexos da VPC não seja removida por engano.

É possível 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.

Depois de excluir o AWSServiceRoleForVPCTransitGateway, a Amazon VPC cria a função novamente se você anexar uma VPC em sua conta a um gateway de trânsito.

AWS políticas gerenciadas para gateways de trânsito no Amazon VPC Transit Gateways

Uma política AWS gerenciada é uma política autônoma criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns, para que você possa começar a atribuir permissões a usuários, grupos e funções.

Lembre-se de que as políticas AWS gerenciadas podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque elas estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo as políticas gerenciadas pelo cliente que são específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) for lançada ou novas operações de API forem disponibilizadas para serviços existentes.

Para mais informações, consulte Políticas gerenciadas pela AWS no Manual do usuário do IAM.

Para trabalhar com um gateway de trânsito, uma das seguintes políticas AWS gerenciadas pode atender às suas necessidades:

- AmazonEC2FullAccess
- AmazonEC2ReadOnlyAccess
- PowerUserAccess
- ReadOnlyAccess

AWS política gerenciada: AWSVPCTransit GatewayServiceRolePolicy

Essa política está anexada à função AWSServiceRoleForVPCTransitGateway. Isso permite que o Amazon VPC crie e gerencie recursos para os anexos de gateway de trânsito.

Para visualizar as permissões para esta política, consulte AWSVPCTransitGatewayServiceRolePolicy na Referência de políticas gerenciadas pela AWS .

Atualizações do Transit Gateway para políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas para gateways de trânsito desde que a Amazon VPC começou a monitorar essas mudanças em março de 2021.

Alteração	Descrição	Data
A Amazon VPC passou a monitorar alterações	A Amazon VPC começou a monitorar as alterações em suas políticas AWS gerenciadas.	1.º de março de 2021

Rede ACLs para gateways de trânsito no Amazon VPC Transit Gateways

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 EC2 instâncias e associação de gateway de trânsito”
- the section called “Sub-redes diferentes para EC2 instâncias e associação de gateway de trânsito”

Mesma sub-rede para EC2 instâncias e associação de gateway de trânsito

Considere uma configuração em que você tenha EC2 instâncias e uma associação de gateway de trânsito na mesma sub-rede. A mesma ACL de rede é usada tanto para o tráfego das EC2 instâncias para o gateway de trânsito quanto para 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 EC2 instâncias e associação de gateway de trânsito

Considere uma configuração em que você tenha EC2 instâncias em uma sub-rede e uma associação de gateway de trânsito em uma sub-rede diferente, e cada sub-rede esteja associada a uma ACL de rede diferente.

As regras de ACL de rede são aplicadas da seguinte forma para a sub-rede da EC2 instância:

- 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. 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 seu fluxo de tráfego, você pode se inscrever em suas NACLs sub-redes de carga de trabalho.

Para obter mais informações sobre como os anexos da VPC funcionam, consulte the section called “Anexos de recursos”.

Cotas de gateways de trânsito da Amazon VPC

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 para a 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

Name	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

Name	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

Name	Padrão	Ajustável
Rotas dinâmicas anunciadas por um dispositivo do roteador virtual para um par do Connect	1.000	Sim
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 gateway de trânsito não pode ter mais de um anexo à mesma VPC.

Name	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
Anexos de emparelhamento 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 obtida por meio de uma conexão Site-to-Site VPN, incluindo, mas não se limitando a: tamanho do pacote, combinação de tráfego (TCP/UDP), definição ou limitação de políticas em redes intermediárias, clima da Internet e requisitos específicos de aplicativos. Para anexos de VPC, os gateways da AWS Direct Connect , ou anexos do gateway de trânsito emparelhados, tentaremos fornecer largura de banda adicional além do valor padrão.

Name	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

Name	Padrão	Ajustável
		contas (TAM) para obter mais assistênc ia.
Largura de banda máxima por túnel da 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. Pode-se 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

Name	Padrão	Ajustável
AWS Direct Connect gateways por gateway de trânsito	20	Não
Gateways de trânsito por AWS Direct Connect gateway	6	Não

Unidade de transmissão máxima (MTU)

- A MTU de uma conexão de rede é o tamanho, em bytes, do maior pacote permissível 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, AWS Direct Connect, Transit Gateway Connect e anexos de emparelhamento (anexos de emparelhamento intra-região, inter-região e Cloud WAN). 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 os dois ao VPCs mesmo tempo para evitar a queda de pacotes enormes devido a uma incompatibilidade de tamanho.
- 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 cotas de Site-to-Site VPN para MTU, consulte Unidade máxima de transmissão (MTU) no Guia do AWS Site-to-Site VPN usuário.
- Os gateways de trânsito oferecem suporte ao Path MTU Discovery (PMTUD) para entrada de tráfego em anexos VPC e Connect. O Transit Gateway gera o `FRAG_NEEDED` para ICMPv4 pacotes e `Packet Too Big (PTB)` para ICMPv6 pacotes. Os gateways de trânsito não oferecem suporte a PMTUD em anexos VPN Site-to-site, Direct Connect e Peering. Para obter mais informações sobre o Path MTU Discovery, consulte Path MTU Discovery no Guia do usuário da Amazon VPC

Multicast

> **Note**
>
> O multicast do Transit Gateway pode não ser adequado para negociação de alta frequência ou aplicativos sensíveis ao desempenho. É altamente recomendável que você analise os seguintes limites de multicast. Entre em contato com sua conta ou com a equipe do Solution Architect para obter uma análise detalhada de seus requisitos de desempenho.

Name	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
Membros e fontes de grupos estáticos e IGMPv2 multicast por gateway de trânsito	10.000	Não
Membros do grupo estático e IGMPv2 multicast por grupo multicast do 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
Máximo de pacotes por segundo por fluxo (menos de 10 receptores)	75,000	Não
Máximo de pacotes por segundo por fluxo (maior que 10 receptores)	15.000	Não
Máximo de pacotes agregados por segundo (menos de 10 receptores)	2.500.000	Não
Máximo de pacotes agregados por segundo (mais de 10 receptores)	500.000	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
Sites por rede global	200	Sim
Conexões por rede global	500	Não

Recursos de cota adicionais

Para obter mais informações, consulte:

- Site-to-Site Cotas de VPN no Guia do AWS Site-to-Site VPN Usuário
- 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
Anexos de função de rede	Crie um anexo de função de rede para conectar diretamente um gateway de trânsito AWS Network Firewall.	16 de junho de 2025
Suporte para referência do grupo de segurança	Agora você pode referenciar um grupo de segurança VPCs conectado a um gateway de trânsito.	25 de setembro de 2024
AWS Cotas do Transit Gateway	Limites de largura de banda foram adicionados.	14 de agosto de 2023
AWS Registros de fluxo do 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 Network Manager	O Network Manager foi criado como um guia autônomo e não está mais incluído como	2 de dezembro de 2021

	parte do Guia do usuário do AWS Transit Gateway.	
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 trânsito e dispositivos virtuais de terceiros em execução na VPC.	10 de dezembro de 2020
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
CloudWatch métricas para anexos do Transit Gateway	Você pode visualizar CloudWatch métricas para anexos individuais do Transit Gateway.	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 suporta o roteamento de tráfego multicast entre sub-redes conectadas VPCs e serve como um roteador multicast para instâncias que enviam tráfego destinado a várias instâncias receptoras.	3 de dezembro de 2019
AWS Gerenciador de rede	É possível visualizar e monitorar as redes globais criadas em torno de gateways de trânsito.	3 de dezembro de 2019
AWS Direct Connect apoio	Você pode usar um AWS Direct Connect gateway para conectar sua AWS Direct Connect conexão por meio de uma interface virtual de trânsito ao gateway de trânsito VPCs ou VPNs conectada a ele.	27 de março de 2019
Lançamento 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.