AWS Transit Gateway

Amazon VPC

Amazon VPC: AWS Transit Gateway

Table of Contents

O que é AWS Transit Gateway para Amazon VPC?

AWS O Transit Gateway 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, acesse o site do AWS Transit Gateway.

Conceitos de gateway de trânsito

Veja a seguir os principais conceitos de gateways de trânsito:

- Anexos: é possível anexar:
  - Uma ou mais VPCs
  - Um dispositivo de SD-WAN/third-party rede Connect
  - Um AWS Direct Connect gateway
  - Uma conexão de emparelhamento com outro gateway de trânsito
  - Uma conexão VPN a um gateway de trânsito
  - Um concentrador de VPN para um gateway de trânsito
  - Um endpoint Client VPN para um gateway de trânsito
  - Um anexo de função de rede. Para obter mais informações, consulte the section called “Anexos de funções 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, Transit Direct Connect 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.
- Controle de criptografia — Um gateway de trânsito pode ser configurado para suportar o controle de criptografia, que impõe a criptografia em trânsito para todo o tráfego em VPCs conectadas ao gateway de trânsito. Quando o controle de criptografia está ativado, o gateway de trânsito pode ser conectado às VPCs com o controle de criptografia aplicado. Esse recurso garante que todo

o tráfego que flui pelo gateway de trânsito seja criptografado, fornecendo segurança aprimorada para suas comunicações de rede.

- 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:

- Console de gerenciamento da AWS: 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 para cada 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 Referência da API do Amazon EC2.

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. Por padrão, as cobranças de processamento de dados são alocadas à conta proprietária do anexo de origem. Você pode usar a alocação flexível de custos para personalizar a forma como essas cobranças são alocadas com base nas necessidades da sua organização. Para obter mais informações, consulte os preços do AWS Transit Gateway Alocação flexível de custos e.

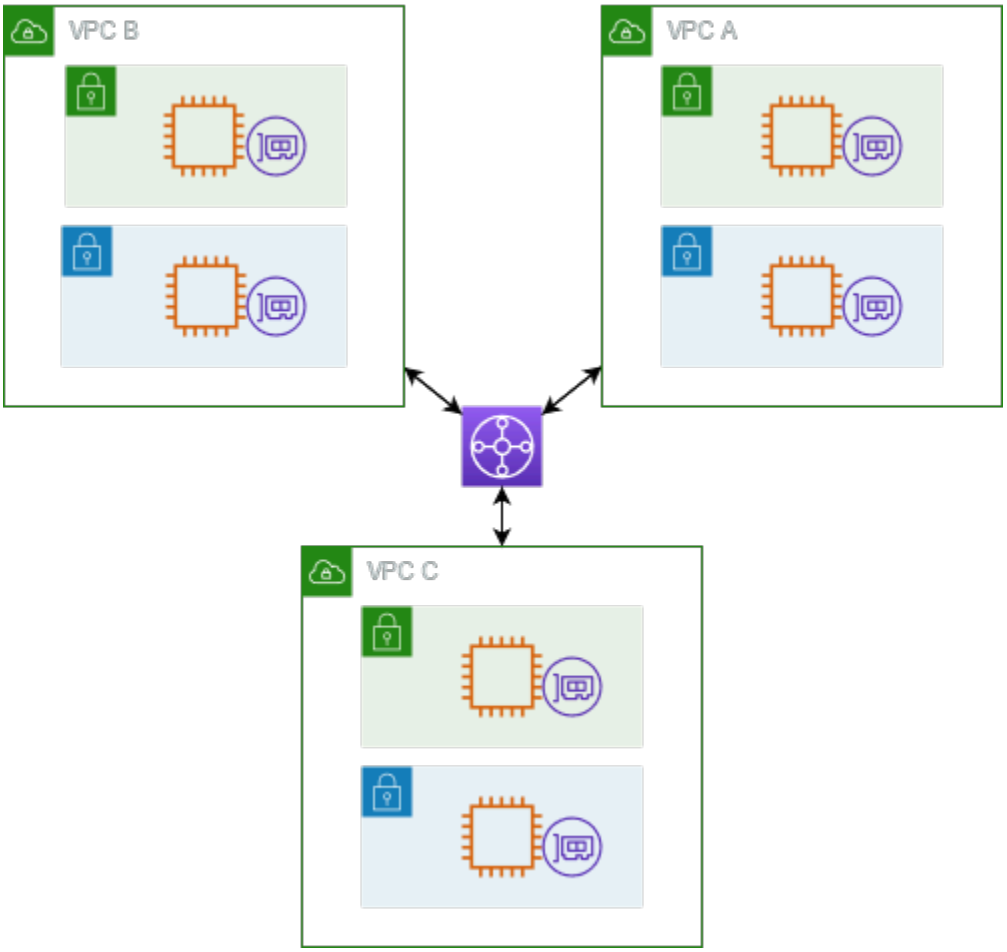
Como funciona o AWS Transit Gateway

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 de cada uma dessas VPCs inclui a rota local e rotas que enviam tráfego destinado das outras duas VPCs ao gateway de trânsito.



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

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:

- Uma ou mais VPCs. AWS O Transit Gateway implanta uma interface de rede elástica nas sub-redes VPC, que é então usada pelo gateway de trânsito para rotear o tráfego de e para as sub-redes escolhidas. Cada zona de disponibilidade precisa ter pelo menos uma sub-rede para que o tráfego chegue aos recursos em cada sub-rede da zona. Durante a criação de anexos, os recursos de uma zona de disponibilidade específica só poderão chegar a um 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 concentradores de 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, você não pode anexar uma VPC com um CIDR 10.1.0. 0/16 com uma segunda VPC usando o mesmo CIDR para um gateway de trânsito e, em seguida, configure 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.
- VPN Concentrator - O VPN Concentrator não suporta ECMP.

> **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 que você habilitar uma zona de disponibilidade ao especificar uma sub-rede, o tráfego poderá ser roteado para todas as sub-redes nessa zona, e não somente para a sub-rede 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

O gateway de trânsito roteia pacotes IPv4 e IPv6 entre anexos usando tabelas de rotas de gateway de trânsito. É possível configurar essas tabelas de rotas para propagar as rotas a partir delas para as VPCs anexadas e conexões VPN anexadas e para os gateways do Direct Connect. 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.

Quando o roteamento dinâmico é usado com um anexo VPN, um anexo VPN Concentrator ou um anexo de gateway Direct Connect, você pode propagar as rotas aprendidas do roteador local por meio do BGP para qualquer tabela de rotas do gateway de trânsito.

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

Para um anexo do Connect, as rotas na tabela de rotas associadas ao anexo do Connect são anunciadas para dispositivos virtuais de terceiros, como SD-WAN dispositivos, executados em uma VPC por meio do 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
  - VPC-propagated rotas
  - Rotas propagadas do gateway do Direct Connect
  - Connect-propagated Rotas do Transit Gateway
  - Site-to-Site VPN em Connect-propagated rotas diretas privadas
  - Site-to-Site VPN-propagated rotas
  - Site-to-Site VPN-Concentrator rotas propagadas
  - Rotas propagadas pelo Client 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

Destino	Destino	Prioridade
192.168.0. 0/16	pcx-12345	2
172.31.0. 0/16	vgw-12345 (estático) ou tgw-12345 (estático)	2
172.31.0. 0/16	vgw-12345 (propagado)	3
0.0.0. 0/0	igw-12345	4

O exemplo a seguir mostra uma tabela de rotas de gateway de trânsito. Caso o anexo do gateway do 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	Prioridade
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 Direct Connect	Com propagação	3
172.31.0. 0/16	tgw-attach-789 | tgw-connect-peer-123	Connect	Com propagação	4
172.31.0. 0/16	tgw-attach-789 | vpn-5678	VPN	Com propagação	5

Anexos de funções 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. Isso elimina a necessidade de criar e gerenciar manualmente VPCs de inspeção.

Com um anexo da 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 sistematicamente 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 diferentes por meio de VPCs diferentes.

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 dispositivo habilitado automaticamente. Isso elimina a necessidade de gerenciar explicitamente VPCs de inspeção.

Com a integração do Network Firewall, você não precisa mais criar e gerenciar VPCs de inspeção para suas implantações do Network Firewall. Em vez de selecionar uma VPC e sub-redes ao criar seu firewall, você seleciona diretamente o Transit Gateway e a AWS provisiona e gerencia 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 RAM-shared 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 é compatível somente com roteamento estático em anexos do Network Firewall.
> - Third-party firewalls não são suportados.

Para obter mais informações sobre firewalls e anexos, consulte Transit gateway network function attachments.

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.

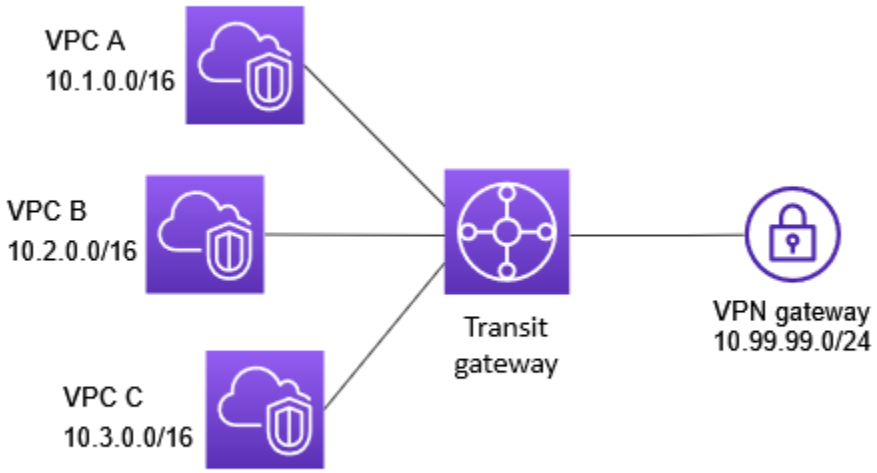
Exemplo: Roteador centralizado

Você pode configurar seu gateway de trânsito como um roteador centralizado que conecta todas as suas VPCs e conexões 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 do

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 os CIDRs da VPC são adicionados 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 padrão para um roteamento IPv4 local na VPC; essa entrada permite que as instâncias na VPC comuniquem-se entre si. A segunda entrada encaminha todos os outros tráfegos da sub-rede IPv4 ao gateway de trânsito. A tabela a seguir mostra as rotas da VPC A.

Destino	Alvo
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 de BGP do gateway do cliente contém os seguintes CIDRs da VPC.

- 10.1.0. 0/16
- 10.2.0. 0/16

- 10.3.0. 0/16

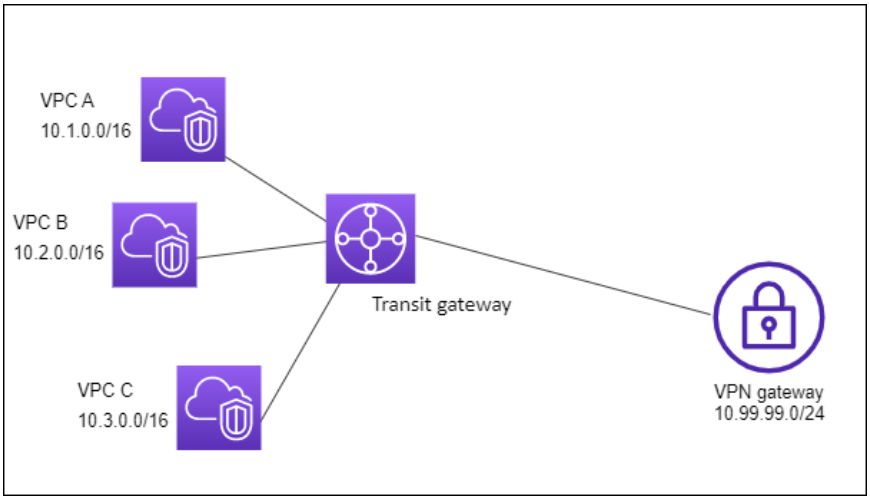
Exemplo: VPCs isoladas

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

Conteúdo

Visão geral do

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 anexos no gateway de trânsito para as 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 estiver ativada, a sessão de BGP será estabelecida, o CIDR da VPN se propagará para a tabela de rotas do gateway de trânsito e os CIDRs da VPC serão adicionados à tabela de BGP do gateway do cliente.

Roteamento

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

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

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

Destino	Alvo
10.1.0. 0/16	local
0.0.0. 0/0	tgw-id

Tabela de rotas do gateway de trânsito

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

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

Destino	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
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 rotas para uma tabela de rotas do Transit Gateway no AWS Transit Gateway.

Tabela do BGP do gateway do cliente

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

- 10.1.0. 0/16
- 10.2.0. 0/16
- 10.3.0. 0/16

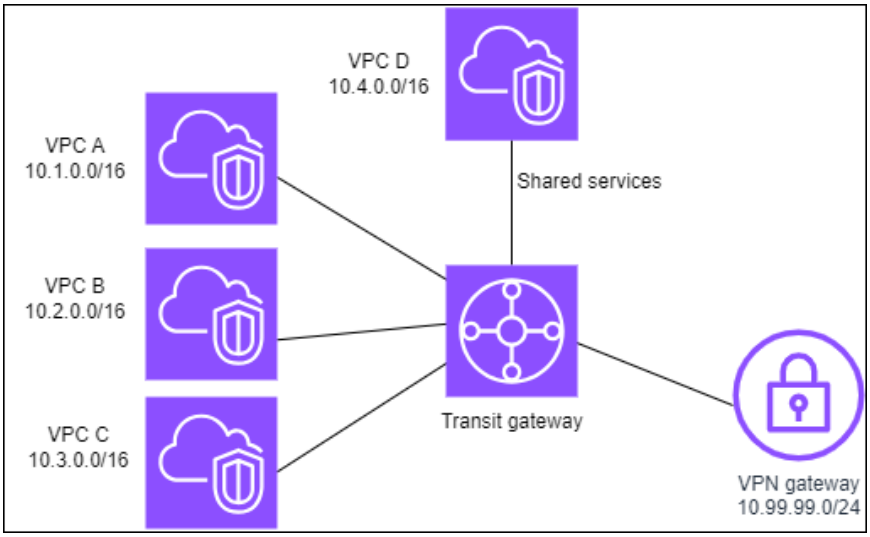
Exemplo: VPCs isoladas com serviços compartilhados

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

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

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

Roteamento

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

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

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

Destino	Alvo
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 as VPCs e uma tabela de rotas para a conexão VPN.

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

Destino	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 uma comunicação com as VPCs da conexão VPN e da VPC de serviços compartilhados.

Destino	Alvo	Tipo de rota
10.1.0. 0/16	*Attachment for VPC A*	com propagação

Destino	Alvo	Tipo de rota
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 rotas para uma tabela de rotas do Transit Gateway no AWS Transit Gateway.

Tabela do BGP do gateway do cliente

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

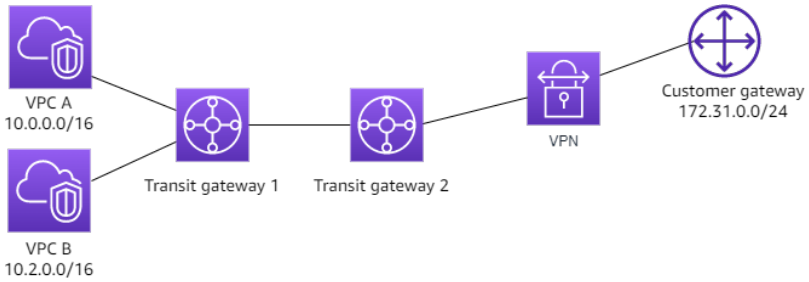
Exemplo: Gateways de trânsito em pares

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

Conteúdo

Visão geral do

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:

- Duas 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 AWS Transit Gateway.

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

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

Roteamento

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

Tabelas de rotas da VPC A e VPC B

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

Destino	Alvo
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*	estático
10.2.0. 0/16	*Attachment ID for peering connection*	estático

Tabela do BGP do gateway do cliente

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

- 10.0.0. 0/16
- 10.2.0. 0/16

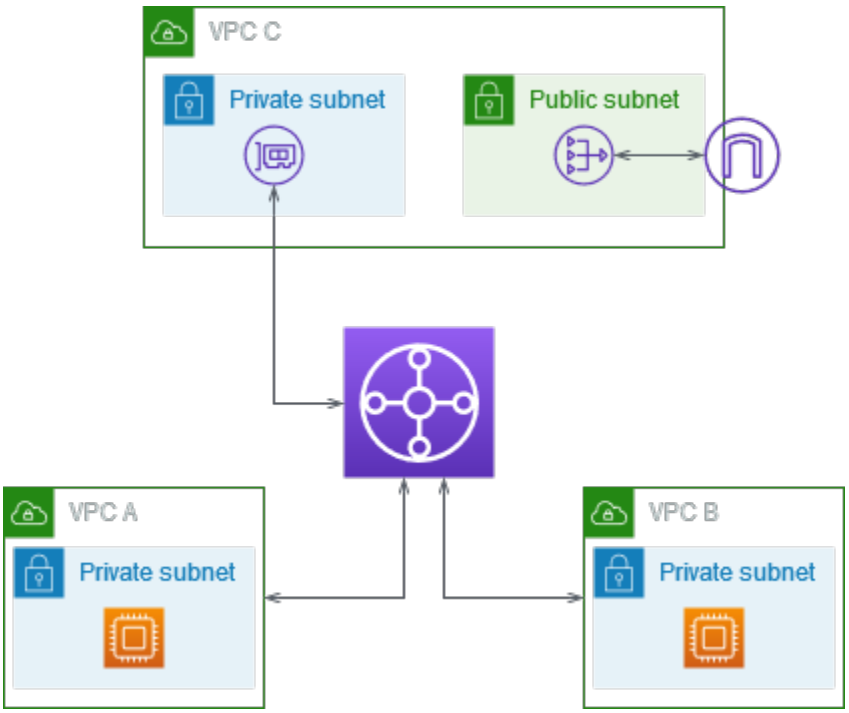
Exemplo: Roteamento de saída centralizado para a Internet

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

Conteúdo

Visão geral do

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 todas as VPCs a um gateway de trânsito. Configure o roteamento para que o tráfego de saída da Internet da VPC A e da VPC B atravesse o gateway de trânsito para a VPC C. O gateway NAT na VPC C 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.
- A VPC A e a VPC B têm sub-redes privadas com instâncias do EC2.
- A VPC C tem o seguinte:
  - Um gateway da Internet anexado à VPC. Para obter mais informações, consulte Criar e anexar um gateway da Internet no Guia do usuário do Amazon VPC.
  - Uma sub-rede pública com um gateway NAT. Para obter mais informações, consulte Criar gateways NAT no Guia do usuário do Amazon VPC.
  - Uma sub-rede privada para o anexo do gateway de trânsito. A sub-rede privada deve estar na mesma zona de disponibilidade da sub-rede pública.
- Um gateway de trânsito. Para obter mais informações, consulte the section called “Criar um gateway de trânsito”.
- Três anexos da VPC no gateway de trânsito. Os blocos CIDR de cada VPC se propagam para a tabela de rotas do gateway de trânsito. Para obter mais informações, consulte the section called “Criar um anexo 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 da sub-rede IPv4 ao 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 da sub-rede IPv4 ao 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. As entradas remanescentes roteiam todos os outros tráfegos IPv4 da 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 roteia todos os outros tráfegos da sub-rede IPv4 ao 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.

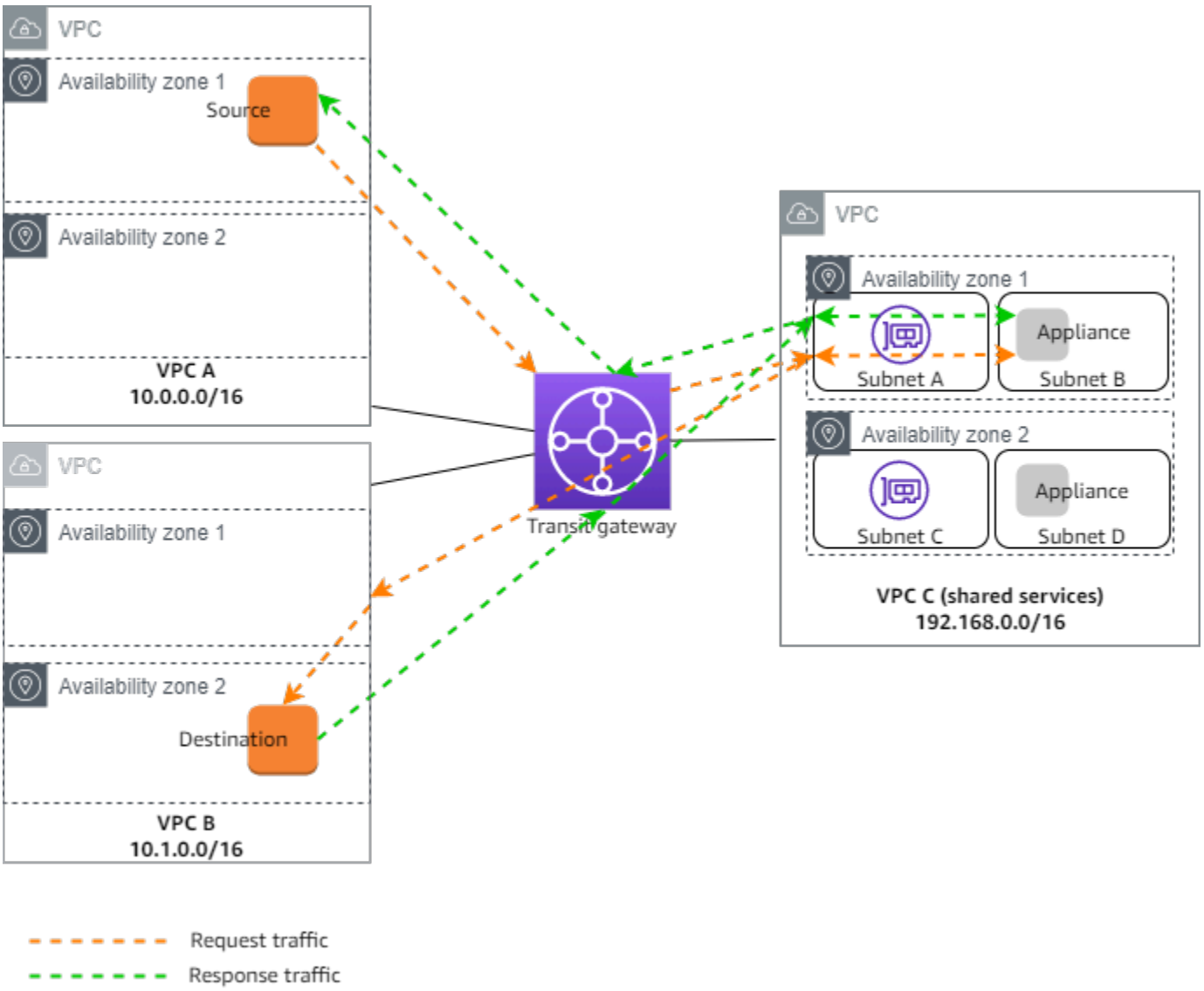
Important

- 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 do

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 anexos de VPC: um para cada VPC. 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. 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

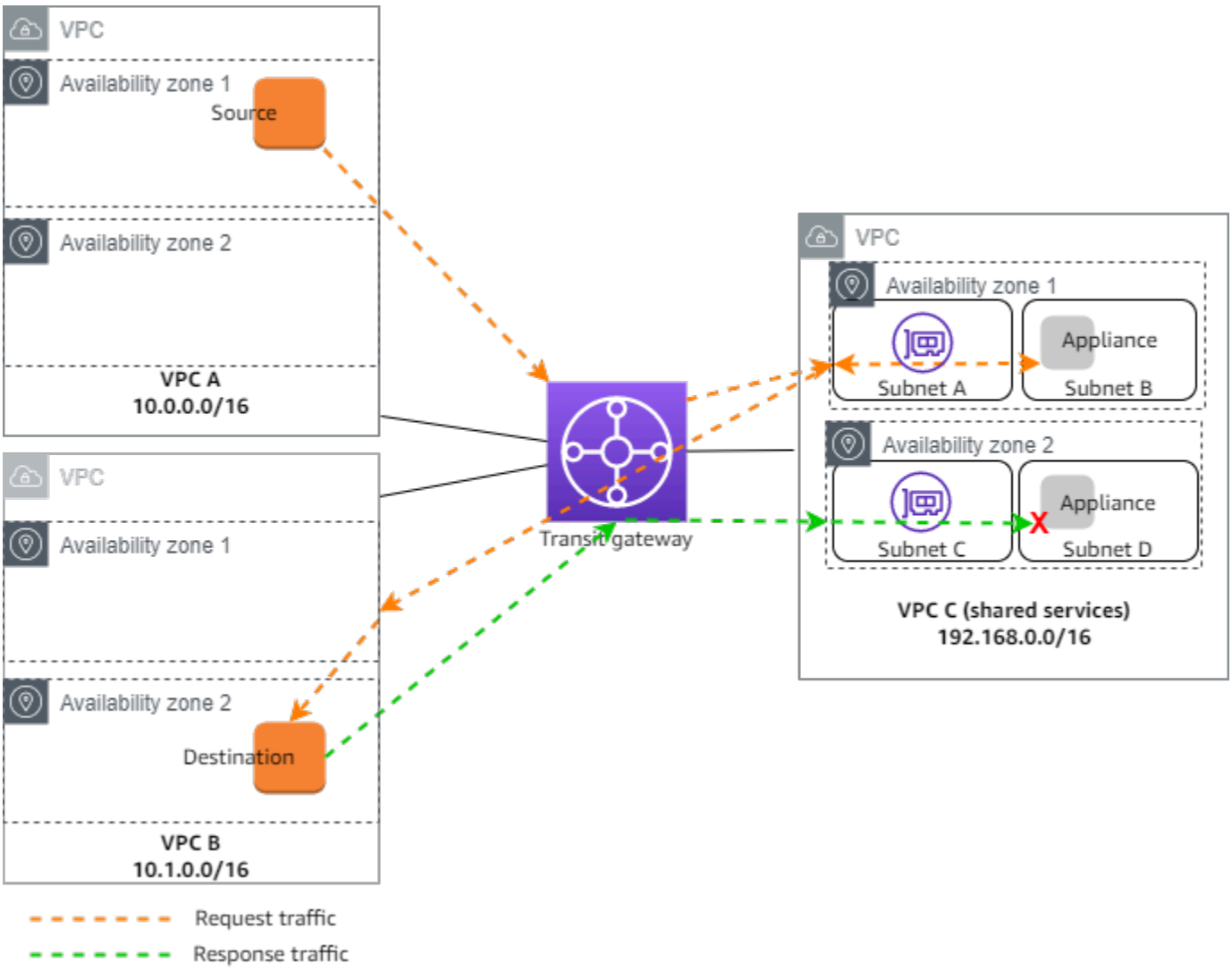
Se os anexos da VPC abrangem várias zonas de disponibilidade e for necessário que o tráfego entre hosts de origem e destino seja roteado pelo mesmo dispositivo para inspeção com estado, habilite o suporte ao modo de dispositivo para o anexo da VPC no qual o dispositivo está localizado.

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

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

Destino	Alvo

Destino	Alvo
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	Alvo
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	Alvo
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: Conceitos básico do AWS Transit Gateway

Os tutoriais a seguir ajudam a obter familiaridade com os gateways de trânsito no AWS Transit Gateway. As tarefas nestes tutoriais orientam você na criação de um gateway de trânsito e na conexão de duas das VPCs usando o gateway de trânsito. Você pode criar um gateway de trânsito usando o console da Amazon VPC ou a AWS CLI.

Tarefas

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

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

Neste tutorial, você aprenderá como usar o consolte da Amazon VPC para criar um gateway de trânsito e conectar duas VPCs a ele. Você criará o gateway de trânsito, conectará as duas VPCs e configurará as rotas necessárias para permitir a comunicação entre o gateway de trânsito e suas VPCs.

Pré-requisitos

- Para um exemplo simples do uso de um gateway de trânsito, crie duas VPCs na mesma região. As VPCs não podem ter CIDRs idênticos nem sobrepostos. Inicie uma instância do Amazon EC2 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 do Amazon EC2.
- Não é possível ter rotas idênticas apontando para duas VPCs diferentes. Um gateway de trânsito não propaga os CIDRs de uma VPC recém-anexada se existir uma rota idêntica nas tabelas de rotas do gateway de trânsito.
- Verifique se há as permissões necessárias para trabalhar com os gateways de trânsito. Para obter mais informações, consulte Gerenciamento de identidade e acesso em AWS Gateway de trânsito.
- 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 grupo de segurança no Guia do usuário do 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 usada quando as VPCs foram criadas.
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. Ele deve ser o ASN para o lado da AWS de uma sessão de Protocolo de Gateway da Borda (BGP).

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

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

        Se 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 conectadas a 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 Configurar opções de compartilhamento entre contas, escolha se deseja Aceitar automaticamente anexos compartilhados. 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 gateway de trânsito, adicione um bloco CIDR de tamanho /24 ou maior para endereços IPv4 ou bloco /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 gateway de trânsito são usados ao configurar anexos Connect (GRE) ou VPNs PrivateIP. O gateway de trânsito atribui IPs para 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: Anexar as VPCs ao gateway de trânsito

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

Confirme que duas VPCs foram criadas e uma instância do EC2 tenha sido executada em cada uma, como descrito em Pré-requisitos.

Criar um anexo do gateway de trânsito para uma VPC

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, 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. Nesse exercício, não ative o Suporte a IPv6.
8. Em ID da VPC, escolha a VPC a ser anexada ao gateway de trânsito.
9. Em IDs de sub-rede, selecione uma sub-rede para cada zona de disponibilidade a ser usada pelo gateway de trânsito para rotear o tráfego. É necessário selecionar pelo menos uma sub-rede. 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: Adicionar rotas entre os gateways de trânsito e as VPCs

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

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

É possível confirmar se o gateway de trânsito foi criado com sucesso conectando uma instância do Amazon EC2 a cada VPC e enviando dados entre elas, como em um comando ping. Para obter mais informações, consulte Conexão com a instância do EC2 no Manual do usuário do Amazon EC2.

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 VPCs e configurará as rotas necessárias para permitir a comunicação entre o gateway de trânsito e o seu VPCs.

Pré-requisitos

Antes de começar, você deve ter o seguinte:

- AWS CLI instalado e configurado com as permissões apropriadas. Se você não tiver a AWS CLI instalada, consulte a Documentação da AWS Command Line Interface.
- 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 instância do EC2 em cada VPC. Para ver as etapas para iniciar uma instância do EC2 em uma VPC, consulte Executar uma instância no Guia do usuário do Amazon EC2.
- Grupos de segurança configurados para permitir tráfego de ICMP entre as instâncias. Para as etapas de controle de tráfego usando grupos de segurança, consulte Controle o tráfego para seus recursos da AWS usando grupos de segurança no Guia do usuário da Amazon VPC.
- Permissões do IAM apropriadas para trabalhar com gateways de trânsito. Para verificar as permissões do IAM do Transit Gateway, consulte Gerenciamento de identidade e acesso em AWS Transit Gateways no AWS Transit Gateway Guia.

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. O exemplo a seguir mostra uma solicitação `create-transit-gateway` na região `us-west-2`. `options` adicionais foram aprovadas 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, as `Options` que são exibidas 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 o ID do gateway de trânsito (`tgw-1234567890abcdef0`), pois ele será necessário nas próximas etapas.

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

Quando você cria um gateway de trânsito, ele é colocado em um estado `pending`. 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 comando `describe-transit-gatweways` usando o ID do gateway de trânsito recém-criado junto com a opção de filtros. A opção `filters` usa pares `Name=state` e `Values=available`. Em seguida, o comando pesquisa para verificar se o estado do seu gateway de trânsito está em um estado disponível. Se estiver, a resposta `"State": "available"` será exibida. Se estiver em qualquer outro estado, ainda não estará 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 o gateway de trânsito estiver disponível, crie um anexo para cada VPC usando `create-transit-gateway-vpc-attachment`. Você precisará incluir `transit-gateway-id`, `vpc-id` e `subnet-ids`.

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 os `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 estado `pending`. Não há necessidade de alterar esse estado, pois ele muda para um estado `available` 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 a `vpc_id` e os `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 estado `pending`.

```
{
    {
    "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 gateway de trânsito estão disponíveis

Os anexos do gateway de trânsito são criados em um estado inicial `pending`. Não será possível usar esses anexos em suas rotas até que o estado mude para `available`. Isso acontece automaticamente. Use o comando `describe-transit-gateways`, junto com o `transit-gateway-id`, para verificar o `State`. 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, os campos opcionais `Name` e de filtros de `Values` são aprovados 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 estado `available`:

```
{
    "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 comando `create-route` junto com a tabela de rotas de `transit-gateway-id` cada VPC. No exemplo a seguir, o comando é executado duas vezes, uma para tabela de rotas. A solicitação inclui o `route-table-id`, o `destination-cidr-block` e o `transit-gateway-id` para cada rota de VPC que você está criando.

Para obter mais informações sobre o comando `create-route`, 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 seguinte comando. Essa rota usa um `route-table-id` e o `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

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

1. Conectar sua instância do EC2 na primeira VPC usando SSH ou EC2 Instance Connect
2. Faça ping do endereço IP privado da instância do EC2 na segunda VPC:

   ```
   ping 10.2.0.50
   ```

> **Note**
>
> Substitua `10.2.0.50` pelo endereço IP privado real de sua instância do EC2 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: exclua os anexos do gateway de trânsito e o gateway de trânsito

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

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 da 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 comando `delete-transit-gateway-vpc-attachment` 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 da 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 estado `deleting` até que sejam excluídos. Depois de excluídos, você pode excluir o gateway de trânsito. Use o comando `delete-transit-gateway` junto com o `transit-gateway-id`. Para obter mais informações sobre `delete-transit-gateway` o comando, consulte delete-transit-gateway.

   O exemplo a seguir exclui o `My Transit Gateway` 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 AWS Transit Gateways. Para cenários mais complexos, como conectar-se a redes on-premises ou implantar configurações de roteamento mais avançadas, consulte o Guia do AWS Transit Gateways.

Melhores práticas de design do AWS Transit Gateway

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 haja mais endereços para recursos do EC2. Ao usar uma sub-rede separada, é possível configurar o seguinte:
  - Mantenha abertas as ACLs de rede de entrada e de saída associadas às sub-redes do gateway de trânsito.
  - Dependendo do fluxo de tráfego, é possível aplicar ACLs de rede às suas sub-redes de workload.
- Crie uma 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 da VPN Site-to-Site do Protocolo de Gateway da Borda (BGP). Se o dispositivo do gateway do cliente ou firewall da conexão for compatível com multipath, ative o recurso.
- Habilite a propagação de rotas para anexos de gateway do Direct Connect e anexos do Site-to-Site VPN do BGP.
- 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 ambas as VPCs ao mesmo tempo para evitar o descarte de pacotes jumbo devido a divergências de tamanho.
- Não é necessário ter gateways de trânsito adicionais para alta disponibilidade, porque os gateways de trânsito estão altamente disponíveis por design.
- Limite o número de tabelas de rotas do gateway de trânsito, a menos que o design exija várias tabelas de rotas do gateway de trânsito.
- Para garantir a redundância, use um único gateway de trânsito em cada região para recuperação de desastres.
- Para implantações em vários 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 Criação de uma rede global usando o emparelhamento entre regiões do AWS Transit Gateway.

Trabalhe com o AWS Transit Gateway

É possível trabalhar com gateways de trânsito usando o console da Amazon VPC ou a AWS CLI. Para obter informações sobre como habilitar e gerenciar o suporte de criptografia para seu gateway de trânsito, consultethe section called “Support à criptografia”.

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.
- Executar todas as APIs de gateway de trânsito, anexos de gateway de trânsito e tabelas de rotas de gateway de trânsito.

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 as APIs que criam e descrevem anexos, como `CreateTransitGatewayVpcAttachment` e `DescribeTransitGatewayVpcAttachments`, nas VPCs.

- Deixar o compartilhamento de um recurso.

Quando um gateway de trânsito é compartilhado, 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 AWS Transit Gateway

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 do VPN Concentrator oferecem suporte somente ao roteamento BGP (dinâmico). 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

- Crie um gateway de trânsito no AWS Transit Gateway
- Visualizar informações do gateway de trânsito no AWS Transit Gateway
- Gerenciar um gateway de trânsito no AWS Transit Gateway
- Modificar um gateway de trânsito no AWS Transit Gateway
- Aceite um compartilhamento de recursos do AWS Transit Gateway usando o AWS Resource Access Manager console
- Aceitar um anexo de emparelhamento no AWS Transit Gateway
- Excluir um gateway de trânsito no AWS Transit Gateway
- Suporte de criptografia para AWS Transit Gateway

Crie um gateway de trânsito no AWS Transit Gateway

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 ???.

> **Note**
>
> Se você quiser habilitar o suporte à criptografia em um gateway de trânsito, não poderá habilitá-lo ao criar o gateway. Depois de criar o gateway de trânsito e ele estar no estado disponível, você poderá modificá-lo para ativar o suporte à criptografia. Para obter mais informações, consulte the section called “Support à criptografia”.

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 ASNs de 16-bit.

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

   Se houver uma implantação em várias regiões, recomenda-se usar um ASN exclusivo para cada um dos gateways de trânsito.
7. Selecione a opção Suporte a DNS, se precisar que a VPC resolva os nomes de host DNS IPv4 públicos para endereços IPv4 privados quando consultado a partir de instâncias em outra VPC anexada ao gateway de trânsito.
8. Ative o atributo Suporte de referência de grupos de segurança, para referenciar um grupo de segurança entre VPCs conectadas 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 os mesmos CIDRs, o tráfego será distribuído igualmente entre eles.

   Quando você seleciona essa opção, o BGP ASN anunciado e, em seguida, os atributos do BGP, como o, devem ser os mesmos. AS-path

   > **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) Em Blocos CIDR do gateway de trânsito, especifique um ou mais blocos CIDR IPv4 ou IPv6 para o gateway de trânsito.

    É possível especificar um bloco CIDR de tamanho /24 ou maior (por exemplo, /23 ou /22) para IPv4, ou um bloco CIDR de tamanho /64 ou maior (por exemplo, /63 ou /62) para IPv6. Você pode associar qualquer intervalo de endereços IP público ou privado, exceto os endereços no 169.254.0. 0/16 intervalo e intervalos que se sobrepõem aos endereços de seus anexos de VPC e redes locais.

    > **Note**
    >
    > Os blocos CIDR do Transit Gateway são usados se você estiver configurando anexos Connect (GRE), VPNs PrivateIP ou anexos Client VPN. O Transit Gateway atribui IPs para os endpoints do túnel (GRE/PrivateIP VPN) e os anexos do Client 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 no AWS Transit Gateway

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 sob a lista de gateways na página.

Como visualizar um gateway de trânsito usando a AWS CLI

Use o comando describe-transit-gateways.

Gerenciar um gateway de trânsito no AWS Transit Gateway

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: Adicionar tags a recursos do Amazon EC2.

Adicionar tags a um gateway de trânsito usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, 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 no AWS Transit Gateway

É possível modificar as opções de configuração de um gateway de trânsito. Ao modificar um gateway de trânsito, nenhum anexo existente do gateway de trânsito sofre nenhuma interrupção do serviço.

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

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

> **Note**
>
> Os gateways de trânsito que têm o Encryption Support ativado podem ser conectados VPCs com controles de criptografia no modo monitor ou no modo Enforce, ou aqueles VPCs que

não tenham os controles de criptografia ativados. VPCs que têm controles de criptografia no modo Enforce SÓ podem ser conectados a gateways de trânsito que tenham o Encryption Support ativado.
Para obter mais informações detalhadas, consulte the section called “Support à criptografia”.

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.

Aceite um compartilhamento de recursos do AWS Transit Gateway usando o AWS Resource Access Manager console

Ao ser adicionado a um compartilhamento de recursos, você receberá um convite para participar desse compartilhamento. É necessário aceitar o compartilhamento de recurso por meio do console do AWS Resource Access Manager (AWS RAM) 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 Shared with me (Compartilhados comigo), Resource shares (Compartilhamento 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 de emparelhamento no AWS Transit Gateway

Se a funcionalidade Aceitar anexos compartilhados automaticamente não foi habilitada ao criar o gateway de trânsito, é necessário aceitar manualmente os anexos entre contas compartilhadas 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).

Como aceitar um anexo compartilhado usando a AWS CLI

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

Excluir um gateway de trânsito no AWS Transit Gateway

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.

Suporte de criptografia para AWS Transit Gateway

Os controles de criptografia permitem que você audite o status de criptografia dos fluxos de tráfego em sua VPC e, em seguida, aplique a criptografia em trânsito para todo o tráfego dentro da VPC. Quando o VPC Encryption Control estiver no modo obrigatório, todas as interfaces de rede elástica (ENI) nessa VPC estarão restritas a serem anexadas somente a instâncias com capacidade de criptografia AWS Nitro; e somente AWS serviços que criptografam dados em trânsito poderão se conectar à VPC aplicada pelo Encryption Controls. Para obter mais informações sobre os controles de criptografia de VPC, consulte esta documentação.

Suporte à criptografia do Transit Gateway e controle de criptografia VPC

O suporte à criptografia no Transit Gateway permite que você aplique a criptografia em trânsito para o tráfego entre VPCs conectadas a um Transit Gateway. Você precisará ativar manualmente o Encryption Support no Transit Gateway usando o comando modify-transit-gateway para criptografar o tráfego entre as VPCs. Depois de ativado, todo o tráfego atravessará links 100% criptografados entre VPCs que estão no modo Enforce (sem exclusões) por meio do Transit Gateway. Você também pode conectar VPCs que não tenham os controles de criptografia ativados ou que estejam no modo Monitor por meio de um Transit Gateway com o Encryption Support ativado. Nesse cenário, é garantido que o Transit Gateway criptografe o tráfego até o anexo do Transit Gateway na VPC, não sendo executado no modo obrigatório. Além disso, depende da instância para a qual o tráfego está sendo enviado na VPC e não está sendo executada no modo obrigatório.

Você só pode adicionar suporte à criptografia a um gateway de trânsito existente e não ao criar um. À medida que o Transit Gateway fizer a transição para o estado Encryption Support Enabled, não haverá tempo de inatividade no Transit Gateway ou nos anexos. A migração é perfeita e transparente, sem perda de tráfego. Para obter as etapas para modificar um gateway de trânsito para adicionar o Encryption Support, consulteModificar um gateway de trânsito.

Requisitos

Antes de ativar o suporte à criptografia em um gateway de trânsito, certifique-se de que:

- O gateway de trânsito não tem anexos Connect
- O gateway de trânsito não tem anexos de emparelhamento
- O gateway de trânsito não tem anexos do Firewall de Rede
- O gateway de trânsito não tem anexos do VPN Concentrator
- O gateway de trânsito não tem anexos do Client VPN

- O gateway de trânsito não tem referências de grupos de segurança habilitadas
- O gateway de trânsito não tem recursos de multicast habilitados

Estados do Encryption Support

Um gateway de trânsito pode ter um dos seguintes estados de criptografia:

- habilitação - O gateway de trânsito está habilitando o suporte à criptografia. Esse processo pode levar até 14 dias para ser concluído.
- ativado - O suporte à criptografia está ativado no gateway de trânsito. Você pode criar anexos de VPC com o Controle de Criptografia aplicado.
- desativando - O gateway de trânsito está desativando o suporte à criptografia.
- desativado - O suporte à criptografia está desativado no gateway de trânsito.

Regras de anexação do Transit Gateway

Quando um gateway de trânsito tem o suporte à criptografia ativado, as seguintes regras de anexo se aplicam:

- Quando o estado de criptografia do Transit Gateway está ativado ou desativado, você pode criar anexos do Direct Connect, anexos VPN e anexos de VPC que não estejam no modo obrigatório ou obrigatório do Controle de Criptografia.
- Quando o estado de criptografia do gateway de trânsito está ativado, você pode criar anexos VPC, Direct Connect, VPN e VPC em qualquer modo de controle de criptografia.
- Quando o estado de criptografia do gateway de trânsito está desativado, você não pode criar novos anexos de VPC com o controle de criptografia aplicado.
- Anexos Connect, anexos de Peering, anexos de Firewall de Rede, anexos de VPN Concentrator, anexos de Client VPN, referências de grupos de segurança e recursos multicast não são compatíveis com o Encryption Support.

A tentativa de criar anexos incompatíveis falhará com um erro de API.

Anexos da Amazon VPC no Transit Gateway AWS

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. As sub-redes especificadas servem como pontos de entrada e saída para o tráfego do gateway de trânsito. O tráfego só pode alcançar recursos em outras sub-redes dentro da mesma zona de disponibilidade se as sub-redes do anexo do gateway de trânsito tiverem rotas apropriadas configuradas em suas tabelas de rotas apontando para as sub-redes de destino.

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.

  > **Note**
  >
  > Nas zonas de disponibilidade que têm anexos do gateway de trânsito, o tráfego só é encaminhado para o gateway de trânsito a partir das sub-redes específicas associadas ao anexo. 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 e o anexo da tabela de rotas da sub-rede contiver rotas apropriadas para o destino pretendido do tráfego dentro da VPC.

- 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 uma VPC for anexada a um gateway de trânsito e seu CIDR for idêntico ao CIDR de outra VPC, ou se sobrepor ao CIDR de outra VPC, que já esteja anexada ao gateway de trânsito, as rotas para a VPC recém-anexada não serão propagadas para a tabela de rotas do gateway de trânsito.
- Não é possível criar um anexo para uma sub-rede da VPC que resida em uma zona local. Porém, 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.

Requisitos de tabela de rotas para anexos de VPC

Os anexos da VPC do Transit Gateway exigem configurações específicas da tabela de rotas para funcionarem adequadamente:

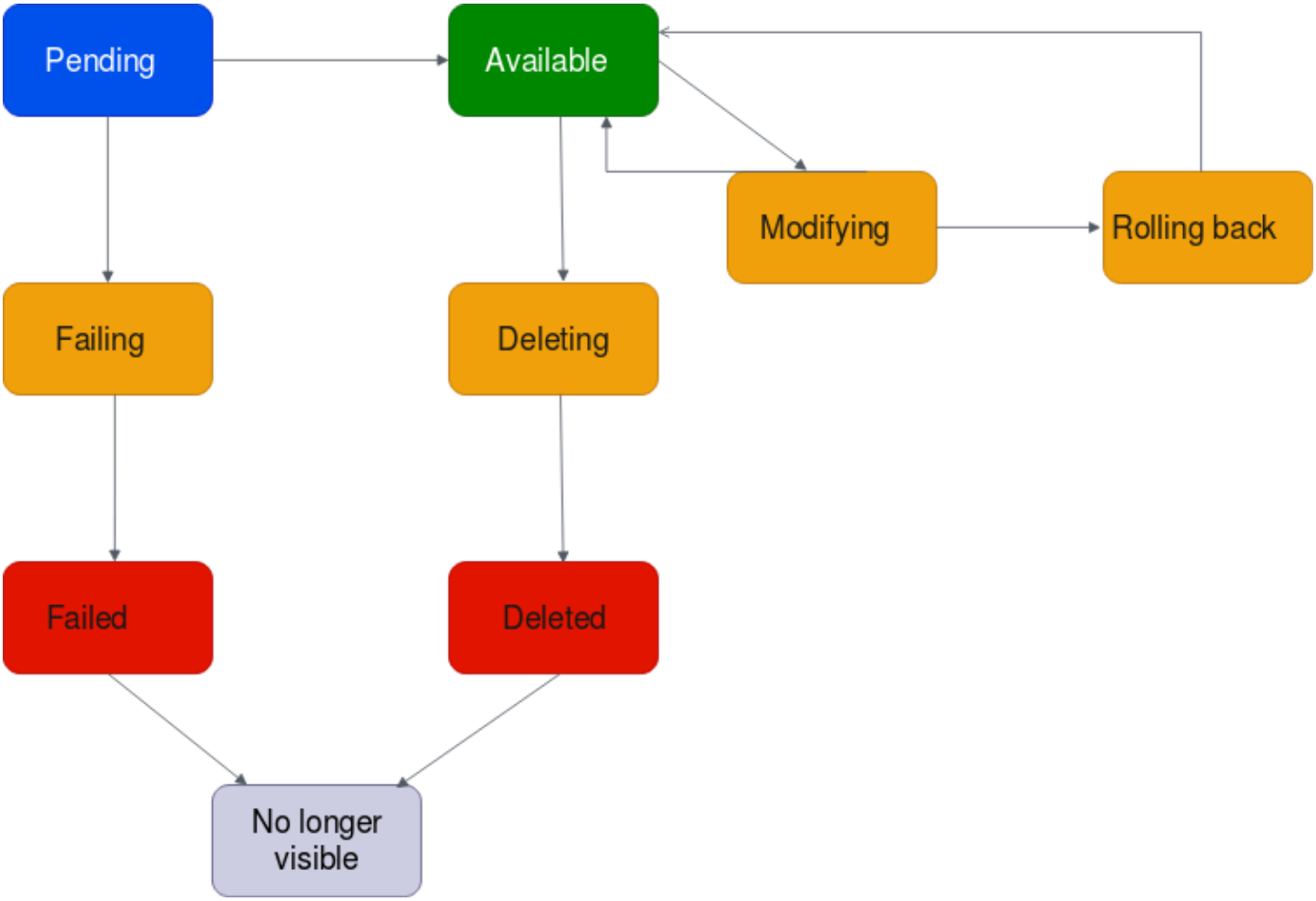
- Tabelas de rotas de sub-redes de anexos: as sub-redes associadas ao anexo do gateway de trânsito devem ter entradas na tabela de rotas para qualquer destino dentro da VPC que precise ser acessado por meio do gateway de trânsito. Isso inclui rotas para outras sub-redes, gateways da Internet, gateways NAT e endpoints da VPC.
- Tabelas de rotas de sub-rede de destino: as sub-redes que contêm recursos que precisam se comunicar por meio do gateway de trânsito devem ter rotas apontando de volta para o gateway de trânsito para retornar o tráfego aos destinos externos.
- Tráfego local da VPC: o anexo do gateway de trânsito não habilita automaticamente a comunicação entre sub-redes dentro da mesma VPC. As regras padrão de roteamento da VPC se aplicam, e a rota local (CIDR da VPC) deve estar presente nas tabelas de rotas para comunicação intra-VPC.

> **Note**
>
> Ter rotas configuradas em sub-redes sem anexos dentro da mesma zona de disponibilidade não permite o fluxo de tráfego. Somente as sub-redes específicas associadas ao anexo do gateway de trânsito podem servir como entry/exit pontos para o tráfego do gateway de trânsito.

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.

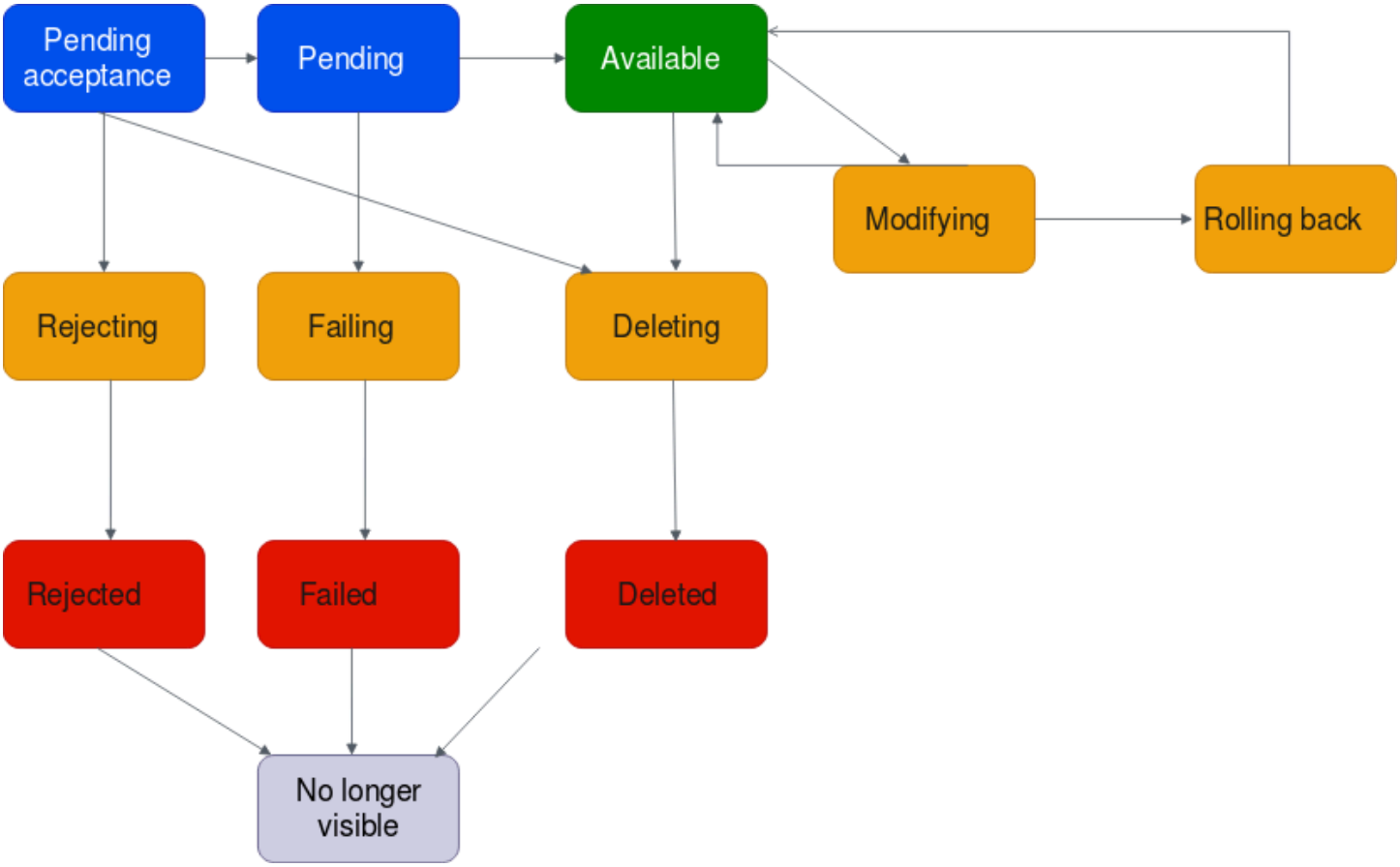
O diagrama a seguir mostra os estados pelos quais um anexo pode passar em uma única configuração de conta ou em uma configuração para várias contas que tenha a opção Aceitar automaticamente os anexos compartilhados ativada.



- 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 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 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 dispositivo seja suportado apenas em anexos VPC, o fluxo de rede pode vir de qualquer outro tipo de anexo do gateway de trânsito, incluindo anexos VPC, VPN e Connect. O modo dispositivo 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 habilitá-lo. Você pode habilitar ou desabilitar o modo de dispositivo 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 dependendo da configuração e dos padrões de tráfego específicos. Estes são cenários de exemplo:

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

Quando o tráfego flui da zona de disponibilidade us-east-1a de destino para a zona de disponibilidade us-east-1a, com anexos da 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 intra-disponibilidade via Appliance VPC

Para o tráfego flui da zona de disponibilidade us-east-1a de destino para a zona de disponibilidade us-east-1b, com anexos da 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 ou us-east-1b dentro da 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 de origem us-east-1a para um destino sem informações de zona de disponibilidade (por exemplo, tráfego com destino à internet), com anexos VPC no modo dispositivo em us-east-1a e us-east-1b, o Gateway de Trânsito 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 no modo dispositivo 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 dispositivo 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 do grupo de segurança pode ser configurado tanto para gateways de trânsito quanto para anexos do VPC do gateway de trânsito e só funcionará se tiver sido habilitado tanto para um gateway de trânsito quanto para seus anexos de VPC.

Limitações

As limitações a seguir se aplicam ao utilizar a referência ao grupo de segurança com um anexo do VPC.

- A referência ao grupo de segurança não oferece suporte para as 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 do grupo 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 no AWS Transit Gateway

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 Attachment type (Tipo de anexo), escolha VPC.
7. Escolha se quer habilitar o Suporte a DNS, o Suporte a IPv6 e o Suporte ao modo de dispositivo.

   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 atributo para referenciar um grupo de segurança entre VPCs conectadas 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 quer habilitar o Suporte a IPv6.
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 IDs de sub-rede, selecione uma sub-rede para cada zona de disponibilidade a ser usada pelo gateway de trânsito para rotear o tráfego. É necessário selecionar pelo menos uma sub-rede. É possível selecionar somente uma sub-rede por zona de disponibilidade.
12. Escolha Create transit gateway attachment (Criar anexo do gateway de trânsito).

Como criar uma VPC usando a AWS CLI

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

Modificar um anexo de VPC no Transit AWS Gateway

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 no AWS Transit Gateway

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 do VPC no AWS Transit Gateway

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.

Como visualizar seus anexos da VPC usando a AWS CLI

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

Excluir um anexo VPC no AWS Transit Gateway

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, escolha Transit Gateway Attachments (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.

Como excluir um anexo de VPC usando a AWS CLI

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

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

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 Security groups (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)

Identificar grupos de segurança AWS Transit Gateway referenciados

Para determinar se o 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 de grupo de segurança do AWS Transit Gateway obsoletas

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 de grupo de segurança obsoletas, é possível excluí-las usando os comandos revoke-security-group-ingress ou revoke-security-group-egress.

Solução de problemas na criação de anexos de VPC do AWS Transit Gateway

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 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 do 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".

Anexos da função de rede do AWS Transit Gateway

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

Com um anexo de firewall, a AWS provisiona e gerencia automaticamente todos os recursos necessários nos bastidores. Você verá um novo anexo do gateway de trânsito em vez de um endpoint de firewall individual. Isso simplifica o processo de implementação da inspeção centralizada do tráfego de rede.

Antes de usar um anexo de firewall, você deve primeiramente criar o anexo no AWS Network Firewall. Para ver as etapas de criação do anexo, consulte Getting Started with AWS Network Firewall Management no Guia do desenvolvedor do AWS Network Firewall. 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
- Exibir anexos da função de rede do AWS Transit Gateway

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

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

Você pode usar o console Amazon VPC ou 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.

Aceitar ou rejeitar 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 gateway de trânsito.

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, selecione Gateways de trânsito.
3. Selecione Anexos do gateway de trânsito
4. Selecione o anexo com um estado de aceitação pendente e um tipo de função de rede.
5. Escolha Ações e, em seguida, 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, por fim, 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.

Visualizar anexo de função de rede usando o console do Gerenciador de Rede

Você pode visualizar anexos de uma função de rede usando o console do Gerenciador de Rede.

Para ver os anexos do firewall no Gerenciador de Rede

1. Abra o console do Network Manager em https://console.aws.amazon.com/networkmanager/casa/.
2. Crie uma rede global no Gerenciador de Rede, se você ainda não tiver uma.
3. Registrar o gateway de trânsito com o Gerenciador de Rede.
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 para o qual deseja visualizar anexos.
7. Escolha a visualização em Árvore de topologia. Os anexos do Network Firewall 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 Gerenciador de Rede fornece informações detalhadas sobre os anexos do firewall, incluindo seu status, gateway de trânsito associado e zonas de disponibilidade.

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

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

Como visualizar tipos de anexo do gateway de trânsito usando o console do 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 a CLI. Para obter as etapas de como atualizar uma associação da tabela de rotas do gateway de trânsito, consulte Associar uma tabela de rotas do gateway de trânsito.

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

Use o console da Amazon VPC 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, selecione Gateways de trânsito.
3. Selecione Tabela de rotas do gateway de trânsito.
4. Selecione a tabela de rotas que você queira modificar.
5. Escolha Ações e 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 permitidas.

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.

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

Use a linha de comando ou a API para rotear um anexo da função de rede do gateway de trânsito.

Para rotear o tráfego por meio de um anexo de função de rede usando a CLI ou uma 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 é:

```
{
  "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 no Transit Gateway AWS

Você pode conectar um anexo Site-to-Site VPN a um gateway de trânsito no AWS Transit Gateway, permitindo que você conecte suas VPCs e redes locais. Há suporte tanto para as rotas dinâmicas quanto para as estáticas, bem como IPv4 e IPv6.

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 VPNs estáticas, primeiro é necessário 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. BGP-based 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

- Crie um anexo de gateway de trânsito a uma VPN no AWS Transit Gateway
- Exibir um anexo de VPN no AWS Transit Gateway
- Excluir um anexo de VPN no AWS Transit Gateway

Crie um anexo de gateway de trânsito a uma VPN no AWS Transit Gateway

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 protegido por um dispositivo de conversão de endereço de rede (NAT) habilitado para NAT traversal (NAT-T), use o endereço IP público do seu dispositivo NAT e ajuste suas 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.

Exibir um anexo de VPN no AWS Transit Gateway

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 no AWS Transit Gateway

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 VPN Concentrator no Transit Gateway AWS

AWS Site-to-Site O VPN Concentrator é um novo recurso que simplifica a conectividade de vários sites para empresas distribuídas. O VPN Concentrator é adequado para clientes que precisam conectar mais de 25 locais remotos AWS, com cada site precisando de baixa largura de banda (menos de 100 Mbps).

Como funciona o VPN Concentrator

Um concentrador de VPN aparece como um único anexo em seu gateway de trânsito, mas pode hospedar várias conexões Site-to-Site VPN.

O tráfego de todas as conexões VPN no Concentrator é roteado pelo mesmo anexo de gateway de trânsito, permitindo que você aplique políticas de roteamento e regras de segurança consistentes em todos os sites conectados. O Concentrator se integra perfeitamente às tabelas de rotas do Transit Gateway, permitindo que você controle o fluxo de tráfego entre seus locais remotos e outros anexos VPCs, como outras conexões VPN e conexões de peering.

Benefícios do VPN Concentrator

- Otimização de custos: reduza os custos consolidando várias conexões VPN de baixa largura de banda em um único anexo de gateway de trânsito, o que é especialmente benéfico quando sites individuais não exigem capacidade total de conexão de VPN.
- Gerenciamento simplificado: gerencie várias conexões de sites remotos por meio de um anexo unificado, mantendo o controle e o monitoramento individuais da conexão VPN.
- Roteamento consistente: aplique políticas de roteamento unificadas em todos os sites conectados por meio de uma única associação de tabela de rotas do gateway de trânsito.
- Arquitetura escalável: conecte até 100 locais remotos usando um único concentrador, com suporte para até 5 concentradores por gateway de trânsito.
- Recursos de VPN padrão: cada conexão VPN oferece suporte aos mesmos recursos de segurança, monitoramento e roteamento das conexões Site-to-Site VPN padrão.

Requisitos e limitações

- Somente roteamento BGP: o VPN Concentrator suporta somente roteamento BGP (dinâmico). O roteamento estático não é suportado no lançamento.

- Requisitos do gateway do cliente: cada local remoto exige um gateway do cliente que ofereça suporte ao roteamento BGP. Antes de criar conexões VPN em um concentrador, revise os requisitos de gateway do cliente em Requisitos para seu dispositivo Site-to-Site VPN de gateway do cliente no Guia do AWS Site-to-Site VPN usuário.
- Considerações de desempenho: Cada conexão VPN em um concentrador foi projetada para uma largura de banda máxima de 100 Mbps. Para maiores requisitos de largura de banda, considere usar anexos VPN padrão do Transit Gateway.

Você pode criar, visualizar ou excluir um anexo do VPN Concentrator usando o console AWS VPC ou a CLI. AWS As conexões VPN individuais no Concentrator são gerenciadas por meio da conexão VPN padrão APIs e das interfaces do console.

Tarefas

- Crie um anexo do VPN Concentrator no AWS Transit Gateway
- Exibir um anexo do VPN Concentrator no AWS Transit Gateway
- Excluir um anexo do VPN Concentrator no AWS Transit Gateway

Crie um anexo do VPN Concentrator no AWS Transit Gateway

Pré-requisitos

- Você deve ter um gateway de trânsito existente em sua conta.

Para criar um anexo do VPN Concentrator usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Site-to-Site VPN Concentrators.
3. Escolha Criar Site-to-Site VPN Concentrator.
4. (Opcional) Em Etiqueta de nome, insira um nome para seu Site-to-Site VPN Concentrator.
5. Para Transit Gateway, selecione um gateway de trânsito existente.
6. (Opcional) Para adicionar outras tags, escolha Adicionar nova tag e especifique a chave e o valor de cada tag.
7. Escolha Criar Site-to-Site VPN Concentrator.

Depois de criar o anexo do VPN Concentrator, ele aparece na lista de anexos com um tipo de recurso de VPN Concentrator e um estado inicial de Pendente. Quando o anexo estiver pronto, o estado mudará para Disponível. Em seguida, você pode criar conexões Site-to-Site VPN neste concentrador.

Para criar um anexo do VPN Concentrator usando o AWS CLI

Use o comando create-vpn-concentrator.

Para criar uma conexão VPN em um VPN Concentrator usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Conexões Site-to-Site VPN.
3. Escolha Create VPN Connection (Criar conexão VPN).
4. Para Target Gateway Type, escolha Site-to-Site VPN Concentrator.
5. Para Site-to-Site VPN Concentrator, escolha o VPN Concentrator onde você deseja criar a conexão 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. Certifique-se de que o gateway do cliente ofereça suporte ao roteamento BGP.
   - Para criar um gateway do cliente, escolha New (Novo). Em Endereço IP, insira o endereço IP público estático do seu dispositivo de gateway do cliente. Para BGP ASN, insira o Número do Sistema Autônomo (ASN) do Border Gateway Protocol (BGP) para o gateway do cliente.

     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.
7. Para opções de roteamento, Dinâmico (requer BGP) é selecionado automaticamente. O VPN Concentrator suporta somente roteamento dinâmico com BGP.
8. Para armazenamento de chaves pré-compartilhadas, selecione Standard ou Secrets Manager.
9. Para largura de banda do túnel, Padrão é selecionado automaticamente. O VPN Concentrator suporta apenas a largura de banda padrão do túnel.
10. Para Túnel dentro da versão IP, selecione IPv4ou IPv6.
11. (Opcional) Selecione Ativar aceleração para melhorar o desempenho dos túneis VPN.
12. (Opcional) Para CIDR IPv4 de rede local, forneça um intervalo de IPv4 CIDR.

13. (Opcional) Para CIDR de IPv4 rede remota, forneça um intervalo de IPv4 CIDR.
14. Para Tipo de endereço IP externo, você pode selecionar Público IPv4 ou IPv6endereço.
15. (Opcional) Para Opções de túnel, você pode definir configurações de túnel, como endereços IP internos do túnel e chaves pré-compartilhadas. Para obter mais informações, consulte Arquiteturas de Site-to-Site VPN no Guia do AWS Site-to-Site VPN usuário.
16. (Opcional) Para adicionar outras tags, escolha Adicionar nova tag e especifique a chave e o valor de cada tag.
17. Escolha Create VPN Connection (Criar conexão VPN).

A conexão VPN aparece na lista de conexões VPN com o VPN Concentrator ID na coluna Transit Gateway ID e um estado inicial de Pendente. Quando a conexão VPN estiver pronta, o estado mudará para Disponível.

Para criar uma conexão VPN em um concentrador de VPN usando o AWS CLI

Use o create-vpn-connectioncomando e especifique o ID do VPN Concentrator usando o `--vpn-concentrator-id` parâmetro.

Exibir um anexo do VPN Concentrator no AWS Transit Gateway

Para visualizar seus anexos do VPN Concentrator 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 VPN Concentrator. Esses são os anexos do VPN Concentrator.
4. Escolha um anexo para visualizar seus detalhes.

Para visualizar conexões VPN em um VPN Concentrator usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Conexões Site-to-Site VPN.
3. Na lista de conexões VPN, identifique as conexões que mostram um VPN Concentrator ID na coluna Transit Gateway ID. Essas são as conexões VPN hospedadas nos VPN Concentrators.
4. Escolha uma conexão VPN para ver seus detalhes.

Para visualizar seus anexos do VPN Concentrator usando o AWS CLI

Use o describe-vpn-concentratorcomando para visualizar os detalhes do VPN Concentrator ou use o describe-transit-gateway-attachmentscomando com um filtro para o tipo de `vpn-concentrator` recurso.

Para visualizar conexões VPN em um concentrador de VPN usando o AWS CLI

Use o describe-vpn-connectionscomando com um filtro `vpn-concentrator-id` para visualizar as conexões VPN associadas a um concentrador específico.

Excluir um anexo do VPN Concentrator no AWS Transit Gateway

Pré-requisitos

- Todas as conexões VPN no VPN Concentrator devem ser excluídas antes que você possa excluir o anexo do Concentrator.
- Certifique-se de ter atualizado suas configurações de roteamento para considerar a remoção do VPN Concentrator e suas conexões VPN associadas.

Para excluir conexões VPN em um VPN Concentrator usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Conexões Site-to-Site VPN.
3. Identifique as conexões VPN associadas ao seu VPN Concentrator procurando o VPN Concentrator ID na coluna Transit Gateway ID.
4. Selecione uma conexão VPN que você deseja excluir.
5. Selecione Ações, Excluir.
6. Quando a confirmação for solicitada, escolha Excluir.
7. Repita as etapas 4 a 6 para cada conexão VPN associada ao VPN Concentrator.

Para excluir um anexo do VPN Concentrator 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 VPN Concentrator que você deseja excluir. Verifique se nenhuma conexão VPN está associada a esse concentrador.

4. Escolha Ações, Excluir anexo.
5. Quando a confirmação for solicitada, escolha Excluir.

O anexo do VPN Concentrator entra no estado de exclusão e será removido da sua conta. Esse processo pode levar alguns minutos para ser concluído.

Para excluir conexões VPN em um concentrador de VPN usando o AWS CLI

Use o delete-vpn-connectioncomando para cada conexão VPN associada ao VPN Concentrator.

Para excluir um anexo do VPN Concentrator usando o AWS CLI

Use o delete-vpn-concentratorcomando depois que todas as conexões VPN tiverem sido excluídas.

Anexos do Client VPN no AWS Transit Gateway

Quando você associa um endpoint do Client VPN a um gateway de trânsito, um anexo do Client VPN é criado automaticamente, permitindo que você roteie o tráfego entre suas VPCs, redes locais e endpoints do Client VPN. AWS O Transit Gateway oferece suporte a anexos de Client VPN entre contas, permitindo que as contas com as quais o gateway de trânsito é compartilhado criem seus próprios anexos Client VPN.

Depois que o endpoint do Client VPN for associado a um gateway de trânsito, você poderá visualizar o anexo no console do Transit Gateway em anexos do Transit Gateway. O anexo será listado com um tipo de Client VPN.

Requisitos e limitações

- Seu gateway de trânsito deve ter um bloco CIDR IPv4 ou IPv6 atribuído antes que você possa criar um anexo de Client VPN.
- A propagação da tabela de rotas deve estar ativada para que os anexos do Client VPN permitam o tráfego entre o endpoint do Client VPN e o gateway de trânsito. Consulte Ativar propagação de rotas.

Tarefas

- Crie um anexo Client VPN no AWS Transit Gateway
- Exibir um anexo do Client VPN no AWS Transit Gateway
- Excluir um anexo do Client VPN no AWS Transit Gateway

- Aceitar ou rejeitar um anexo do Client VPN no AWS Transit Gateway

Crie um anexo Client VPN no AWS Transit Gateway

Pré-requisitos

- Você deve ter um gateway de trânsito existente em sua conta.
- Seu gateway de trânsito deve ter um bloco CIDR IPv4 ou IPv6 atribuído.

Um anexo do Client VPN é criado automaticamente quando você associa um endpoint do Client VPN a um gateway de trânsito.

Para criar um anexo do Client VPN usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Client VPN endpoints.
3. Selecione Create Client VPN endpoint (Criar endpoint da VPN do cliente).
4. Selecione Transit Gateway como o tipo de associação e insira a ID do Transit Gateway a ser usada.
5. Selecione Create Client VPN endpoint (Criar endpoint da VPN do cliente).

Depois de criar o anexo do Client VPN, ele aparece na lista de anexos com um tipo de recurso de Client VPN e um estado inicial de Pendente. Quando o anexo estiver pronto, o estado mudará para Disponível. Se o gateway de trânsito estiver em uma conta diferente, o estado do anexo será Aceitação pendente até que o proprietário do gateway de trânsito o aceite.

Para obter mais informações sobre a criação de endpoints do Client VPN, consulte Getting Started with AWS Client VPN.

Para criar um anexo do Client VPN usando o AWS CLI

Use o comando create-client-vpn-endpoint.

Exibir um anexo do Client VPN no AWS Transit Gateway

Para visualizar seus anexos do Client VPN usando o console

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

2. No painel de navegação, escolha Transit Gateways (Gateways de trânsito).
3. Selecione Anexos do gateway de trânsito
4. Na coluna Tipo de recurso, procure Client VPN.
5. Escolha um anexo para visualizar seus detalhes.

Para visualizar seus anexos do Client VPN usando o AWS CLI

Use o comando describe-transit-gateway-attachments com um filtro para o tipo de recurso. `client-vpn`

Excluir um anexo do Client VPN no AWS Transit Gateway

Para excluir um anexo do Client VPN usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateways (Gateways de trânsito).
3. Selecione Anexos do gateway de trânsito
4. Selecione o anexo do Client VPN que você deseja excluir.
5. SelecioneAções, Excluir anexo do gateway de trânsito.
6. Ao receber a solicitação de confirmação, digite **`delete`** e escolha Excluir.

O anexo do Client VPN entra no estado de exclusão e será removido da sua conta. Esse processo pode levar algum tempo para ser concluído.

Para excluir um anexo do Client VPN usando o AWS CLI

Use o comando delete-transit-gateway-client-vpn-attachment.

Aceitar ou rejeitar um anexo do Client VPN no AWS Transit Gateway

Se um endpoint do Client VPN em outra conta criar um anexo ao seu gateway de trânsito, você deverá aceitar ou rejeitar a solicitação de anexo antes que o tráfego possa fluir.

Para aceitar ou rejeitar um anexo do Client VPN usando o console

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

3. Selecione Anexos do gateway de trânsito
4. Selecione o anexo com um estado de aceitação pendente e um tipo de Client VPN.
5. Escolha Ações e, em seguida, escolha Aceitar anexo ou Rejeitar anexo.
6. Na caixa de diálogo de confirmação, escolha Aceitar ou Rejeitar.

Se você aceitar o anexo, ele se tornará ativo e o AWS Transit Gateway começará a processar o tráfego de e para o endpoint do Client VPN. Se você rejeitar o anexo, ele entrará em um estado rejeitado e, por fim, será excluído.

Para aceitar um anexo do Client VPN usando o AWS CLI

Use o comando accept-transit-gateway-client-vpn-attachment.

Para rejeitar um anexo do Client VPN usando o AWS CLI

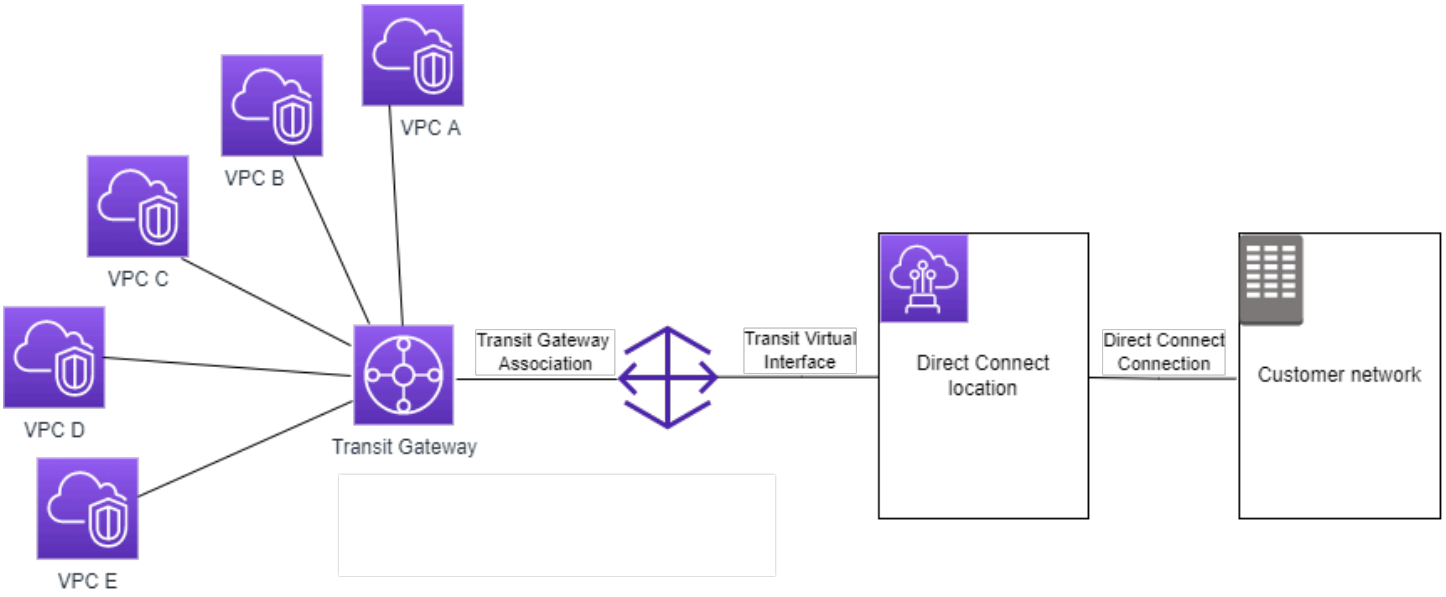
Use o comando reject-transit-gateway-client-vpn-attachment.

Anexos do gateway de trânsito a um gateway do Direct Connect no AWS Transit Gateway

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:

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

O diagrama a seguir ilustra como o gateway do Direct Connect permite criar uma única conexão com a conexão do Direct Connect que pode ser usada por todas as suas VPCs.



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 AWS Transit Gateway

É possível emparelhar gateways de trânsito de dentro e for ada Região e direcionar o tráfego entre eles, incluindo tráfego de IPv4 e IPv6. Para fazer isso, crie um anexo de emparelhamento no seu gateway de trânsito e especifique um gateway de trânsito. O gateway de trânsito de par pode estar em sua conta ou em 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.

Recomenda-se o uso de ASNs exclusivos para cada gateway de trânsito emparelhado, a fim de aproveitar as funcionalidades futuras de propagação de rotas.

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

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

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

Considerações sobre a adesão de regiões da AWS

É possível emparelhar gateways de trânsito através dos limites da região de adesão. Para obter mais informações sobre essas regiões e sobre como aderir, consulte Managing AWS Regions. 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 adesão da região, a AWS compartilha os seguintes dados de conta com a conta que aceita o anexo de emparelhamento:
  - Conta da AWSID do
  - 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 no AWS Transit Gateway
- Aceite ou rejeite uma solicitação de emparelhamento de anexo no AWS Transit Gateway
- Adicionar uma rota a uma tabela de rotas do Transit Gateway usando o AWS Transit Gateway
- Excluir um anexo de emparelhamento no AWS Transit Gateway

Criar um anexo de emparelhamento no AWS Transit Gateway

Antes de começar, confirme o ID do gateway de trânsito a ser anexada. Se o gateway de trânsito estiver em outra Conta da AWS, confirme o ID da Conta da AWS do proprietário do gateway de trânsito. Após a criação do anexo de emparelhamento, o proprietário do gateway de trânsito aceitante deverá aceitar ou rejeitar 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 outra Conta da AWS, selecione 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).

Como criar um anexo de emparelhamento usando a AWS CLI

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

Aceite ou rejeite uma solicitação de emparelhamento de anexo no AWS Transit Gateway

Quando criado, um anexo de emparelhamento de gateway de trânsito é criado automaticamente em um estado `pendingAcceptance` e permanece nesse estado indefinidamente até ser aceito ou rejeitado. Para ativar o anexo de emparelhamento, o proprietário do gateway de trânsito do aceitante deve aceitar a solicitação de anexo de emparelhamento, mesmo que os dois gateways de trânsito estejam na mesma conta. Aceite a solicitação de anexo de emparelhamento da região em que o gateway de trânsito do aceitante está localizado. Como alternativa, se você rejeitar o anexo de emparelhamento, deve rejeitar a solicitação da região em que o gateway de trânsito do aceitante está localizado.

Como aceitar uma solicitação de anexo emparelhamento usando o console

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

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

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

Adicionar uma rota a uma tabela de rotas do Transit Gateway usando o AWS Transit Gateway

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, o anexo de emparelhamento do gateway de trânsito deve ser associado a tabela de rotas 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 no AWS Transit Gateway

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.

Como excluir um anexo de emparelhamento usando a AWS CLI

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

Conecte anexos e conecte pares no Transit Gateway AWS

Você pode criar um anexo do Transit Gateway Connect para estabelecer uma conexão entre um gateway de trânsito e dispositivos virtuais de terceiros (como SD-WAN dispositivos) executados em uma 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 SD-WAN dispositivos com o AWS Transit Gateway Direct Connect e.

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. É necessário especificar um bloco CIDR /29 a partir do intervalo `169.254.0.0/16` para IPv4. Opcionalmente, é possível especificar um bloco CIDR /125 a partir do intervalo `fd00::/8` para IPv6. Os blocos CIDR a seguir 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

É necessário configurar o primeiro endereço do intervalo IPv4 no dispositivo como o endereço IP do BGP. Ao usar o IPv6, se o bloco CIDR interno for fd00::/125, configure o primeiro endereço neste intervalo (fd00::1) na interface de túnel do dispositivo.

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

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 endereço IPv4 ou IPv6, mas deve ser a mesma família de endereços IP que o endereço de 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.

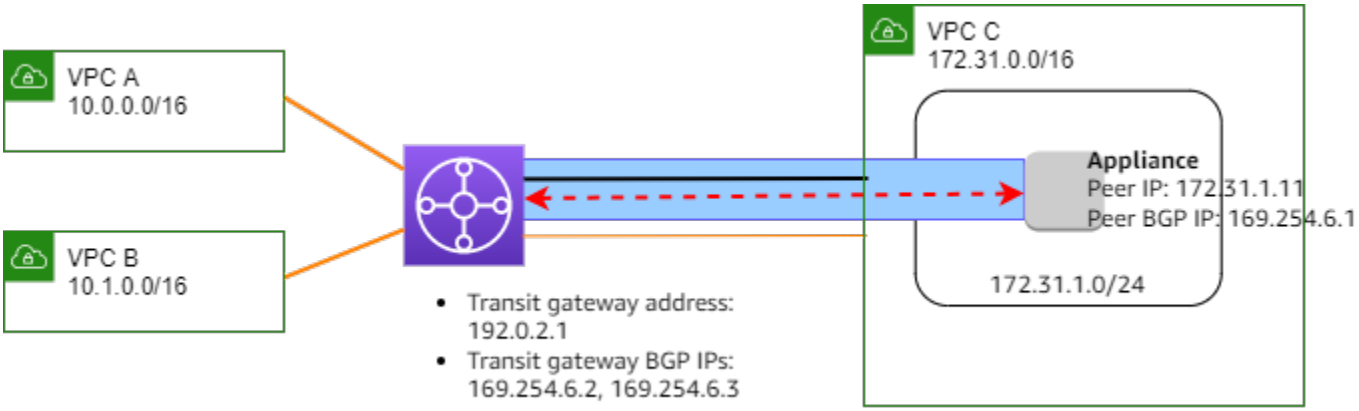
Ao criar ou modificar um gateway de trânsito, é possível adicionar um bloco CIDR de gateway de trânsito.

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

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

O Transit Gateway Connect para o emparelhamento BGP suporta somente o Multiprotocol BGP (MP-BGP), onde o endereçamento IPv4 Unicast é necessário para também estabelecer uma sessão BGP para IPv6 Unicast. É possível usar endereços IPv4 e IPv6 para endereços IP externos do GRE.

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



Componente diagrama	Description
	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	Alvo
172.31.0. 0/16	Local
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 o eBGP for usado, deve-se configurar o ebgp-multihop com um valor de 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 par do iBGP (dispositivo de terceiros), a menos que as rotas tenham origem em um par do eBGP e tenham configuração automática de próximo salto. As rotas anunciadas pelo dispositivo de terceiros sobre o emparelhamento do iBGP devem ter um ASN.
  - MP-BGP (extensões multiprotocolo para BGP): usado para oferecer suporte a vários tipos de protocolo, como famílias de endereços IPv4 e IPv6.
- O tempo limite padrão do keep-alive do BGP é de 10 segundos e o temporizador de espera padrão é de 30 segundos.
- O peering IPv6 BGP não é suportado; somente IPv4-based o peering BGP é suportado. Os prefixos IPv6 são trocados pelo peering IPv4 BGP usando. 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.
- Um Connect peer usando o AS-PATH atributo BGP é a rota preferida quando você tem dois Connect peers.

  Para usar o roteamento de vários caminhos de custo igual (ECMP) entre vários dispositivos, você deve configurar o equipamento 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 número do sistema autônomo (ASN) AS-PATH e o Número do Sistema Autônomo (ASN) devem corresponder. 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 (4 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 1476 bytes (1500 - 4 - 20 = 1476) para evitar a fragmentação do pacote.

Tarefas

- Criar um anexo do Connect no AWS Transit Gateway
- Criar um par do Connect no AWS Transit Gateway
- Visualize anexos do Connect e pares do Connect no Transit Gateway AWS
- Modifique o anexo Connect e as tags Connect peer no AWS Transit Gateway
- Excluir um par do Connect no AWS Transit Gateway
- Excluir um anexo do Connect no AWS Transit Gateway

Criar um anexo do Connect no AWS Transit Gateway

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).

Como criar um anexo do Connect usando a AWS CLI

Use o comando create-transit-gateway-connect.

Criar um par do Connect no AWS Transit Gateway

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. Em BGP em blocos CIDR IPv4, especifique o intervalo de endereços IPv4 internos que são usados para o emparelhamento BGP. Especifique um bloco CIDR /29 no intervalo `169.254.0.0/16`.
8. (Opcional) Em BGP em blocos CIDR IPv6, especifique o intervalo de endereços IPv6 internos que são usados para o emparelhamento BGP. Especifique um bloco CIDR /125 no intervalo `fd00::/8`.
9. (Opcional) 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 o ASN do par for configurado de maneira diferente do ASN de gateway de trânsito (eBGP), configure o ebgp-multihop com um TTL de 2.
10. Selecione Criar par do Connect.

Como criar um par do Connect usando a AWS CLI

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

Visualize anexos do Connect e pares do Connect no Transit Gateway AWS

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.

Modifique o anexo Connect e as tags Connect peer no AWS Transit Gateway

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 de peer do Connect usando o AWS CLI

Use os comandos create-tags e delete-tags.

Excluir um par do Connect no AWS Transit Gateway

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 a AWS CLI

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

Excluir um anexo do Connect no AWS Transit Gateway

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.

Como excluir um anexo do Connect usando a AWS CLI

Use o comando delete-transit-gateway-connect.

Tabelas de rotas do Transit Gateway no AWS Transit Gateway

Use tabelas de rotas de gateway de trânsito para configurar o roteamento para os anexos de gateway de trânsito. Uma tabela de rotas contém regras que direcionam como seu tráfego de rede

é roteado entre as 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, VPN Concentrator, Client VPN, Direct Connect Gateway, Peering e Connect são todos 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 de gateway de trânsito no AWS Transit Gateway
- Exibir tabelas de rotas do Transit Gateway usando o AWS Transit Gateway
- Associar uma tabela de rotas do gateway de trânsito no AWS Transit Gateway
- Excluir uma associação para uma tabela de rotas do Transit Gateway no AWS Transit Gateway
- Habilitar a propagação de rotas para uma tabela de rotas do Transit Gateway no AWS Transit Gateway
- Desabilitar a propagação de rotas no AWS Transit Gateway
- Criar uma rota estática no AWS Transit Gateway
- Excluir uma rota estática no AWS Transit Gateway
- Substituir uma rota estática no AWS Transit Gateway
- Exportar tabelas de rotas para o Amazon S3 no AWS Transit Gateway
- Excluir uma tabela de rotas de gateway de trânsito no AWS Transit Gateway
- Criar uma referência de lista de prefixos de tabela de rotas no AWS Transit Gateway
- Modificar uma referência da lista de prefixos no AWS Transit Gateway
- Excluir uma referência da lista de prefixos no AWS Transit Gateway

Criar uma tabela de rotas de gateway de trânsito no AWS Transit Gateway

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.

Como criar uma tabela de rotas de gateway de trânsito usando a AWS CLI

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

Exibir tabelas de rotas do Transit Gateway usando o AWS Transit Gateway

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 no AWS Transit Gateway

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.

Como associar uma tabela de rotas do gateway de trânsito usando a AWS CLI

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

Excluir uma associação para uma tabela de rotas do Transit Gateway no AWS Transit Gateway

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 rotas para uma tabela de rotas do Transit Gateway no AWS Transit Gateway

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 no AWS Transit Gateway

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 Transit Gateway Route Tables (Tabelas de rotas do gateway de trânsito).
3. Selecione a tabela de rotas da qual você excluirá a propagação.
4. Na parte inferior da página. selecione a guia Propagações.
5. Selecione o anexo, e então, Excluir propagação.
6. Quando a confirmação for solicitada, selecione Excluir propagação.

Como desabilitar a propagação de rotas usando a AWS CLI

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

Criar uma rota estática no AWS Transit Gateway

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

Como criar uma rota estática 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 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, selecione 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 blackhole usando a AWS CLI

Use o comando create-transit-gateway-route.

Excluir uma rota estática no AWS Transit Gateway

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 Transit Gateway Route Tables (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.

Como excluir uma rota estática usando a AWS CLI

Use o comando delete-transit-gateway-route.

Substituir uma rota estática no AWS Transit Gateway

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.

Como substituir uma rota estática usando a AWS CLI

Use o comando replace-transit-gateway-route.

Exportar tabelas de rotas para o Amazon S3 no AWS Transit Gateway

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

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

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Route Tables (Tabelas de rotas do gateway de trânsito).
3. Escolha a tabela e roteamento que inclui as rotas para exportar
4. 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 em https://console.aws.amazon.com/s3/ e navegue até o bucket especificado. O nome do arquivo inclui o ID da Conta da AWS, a região da AWS, 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 de gateway de trânsito no AWS Transit Gateway

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

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateway Route Tables (Tabelas de rotas do gateway de trânsito).
3. Selecione a tabela de rotas a ser excluída.
4. 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 gateway de trânsito usando a AWS CLI

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

Criar uma referência de lista de prefixos de tabela de rotas no AWS Transit Gateway

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, caso os mesmos CIDRs de destino sejam especificados frequentemente em várias tabelas de rotas de gateway de trânsito, é possível gerenciar esses CIDRs em uma única lista de prefixos, em vez de referenciar repetidamente os mesmos 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 da lista de prefixos usando a AWS CLI

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

Modificar uma referência da lista de prefixos no AWS Transit Gateway

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.

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

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

Excluir uma referência da lista de prefixos no AWS Transit Gateway

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.

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

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

Tabelas de política de gateway de trânsito no AWS Transit Gateway

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

- Crie uma tabela de políticas do Transit Gateway no AWS Transit Gateway
- Excluir uma tabela de políticas do Transit Gateway no AWS Transit Gateway

Crie uma tabela de políticas do Transit Gateway no AWS Transit Gateway

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 do Transit Gateway no AWS Transit Gateway

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 no AWS Transit Gateway

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

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 a grupos multicast é definida por interfaces de rede elástica individuais anexadas às instâncias do EC2.

- 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 ingressar, sair e enviar mensagens. A AWS oferece suporte tanto ao protocolo IGMPv2 e a domínios multicast de associação de grupo IGMP como ao estático (baseado em API).

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

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

Considerações

- O multicast do Transit Gateway pode não ser adequado para transações de alta frequência ou aplicativos sensíveis ao desempenho. Recomendamos veementemente que você reveja as cotas de multicast para verificar os limites. Entre em contato com sua equipe de conta ou de Solution Architect para obter uma análise detalhada de seus requisitos de desempenho.
- Para obter informações sobre regiões compatíveis, consulte Perguntas frequentes sobre o AWS Transit Gateway.
- É necessário criar um gateway de trânsito para ser compatível com o multicast.
- A associação ao grupo de multicast é gerenciada usando o Amazon Virtual Private Cloud Console ou a AWS CLI ou 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 desabilitar a caixa de seleção, consulte Alterar a verificação da origem ou do destino no Guia do usuário do Amazon EC2.
- Uma instância que não é do Nitro não pode ser um remetente multicast.

- O roteamento multicast não é compatível com o Direct Connect, a VPN Site-to-Site, os anexos de emparelhamento ou anexos do Connect de gateway de trânsito.
- 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 mensagens JOIN IGMP múltiplas para se juntar a um grupo multicast (tipicamente 2 a 3 novas tentativas). No caso improvável que todas as mensagens JOIN IGMP se percam, o host não será parte do grupo multicast do gateway de trânsito. Em tal cenário, será necessário reacionar a mensagem JOIN IGMP do host usando métodos específicos da aplicação.
- Uma associação ao grupo começa com o recebimento da mensagem JOIN IGMPv2 pelo transit gateway e termina com o recebimento da mensagem LEAVE IGMPv2. O gateway de trânsito mantém o controle dos hosts que se uniram com sucesso ao grupo. Como um roteador multicast em nuvem, o transit gateway emite uma mensagem QUERY IGMPv2 para todos os membros a cada dois minutos. Cada membro envia uma mensagem JOIN IGMPv2 em resposta, que é como os membros renovam sua associação. Se um membro não responder a três consultas consecutivas, o transit gateway removerá essa associação de todos os grupos associados. No entanto, ele continua enviando consultas a esse membro por 12 horas antes de remover permanentemente o membro de sua lista a ser consultada. Uma mensagem LEAVE IGMPv2 explícita remove imediatamente e permanentemente o host de qualquer processamento multicast adicional.
- O gateway de trânsito mantém o controle dos hosts que se uniram com sucesso ao grupo. No caso de uma interrupção do transit gateway, o transit gateway continua enviando dados multicast ao host por sete minutos (420 segundos) após a última mensagem IGMP JOIN bem sucedida. O gateway de trânsito continua a enviar consultas de associação ao host por até 12 horas ou até receber uma mensagem LEAVE IGMP do host.
- O gateway de trânsito envia pacotes de consulta de associação a todos os membros IGMP de modo que possa seguir a associação do grupo multicast. O IP de origem desses pacotes de consulta IGMP é 0.0.0.0/32. O IP de destino é 224.0.0.1/32 e o protocolo é 2. A configuração de grupo de segurança nos hosts IGMP (instâncias) e qualquer configuração de ACLs nas sub-redes de host devem permitir essas mensagens de protocolo IGMP.
- Quando a origem e o destino multicast estão na mesma VPC, não é possível usar a referência do grupo de segurança para definir o grupo de segurança de destino para aceitar o tráfego do grupo de segurança de origem.

- Para grupos e fontes de multicast estáticos, o AWS Transit Gateway remove automaticamente grupos e fontes estáticos de ENIs que não existem mais. Isso é feito assumindo-se periodicamente a função vinculada ao serviço do Transit Gateway para descrever ENIs na conta.
- Somente o multicast estático oferece suporte a 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.

Network ACLs

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

Para tráfego multicast de Internet Group Management Protocol (IGMP), 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 no AWS Transit Gateway

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) Compatibilidade com IGMPv2 (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 é habilitado, é necessário adicionar fontes para um domínio de 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.

Crie um domínio multicast IGMP no AWS Transit Gateway

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 no AWS Transit Gateway

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, escolha 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. Em Compatibilidade com IGMPv2, 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).

Como criar um domínio de multicast estático usando a 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
```

Associando anexos e sub-redes VPC a um domínio multicast no Transit Gateway AWS

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 no Transit Gateway AWS.

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 sub-redes de um domínio de multicast no AWS Transit Gateway

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.

Como desassociar sub-redes usando a AWS CLI

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

Exibir associações de domínio multicast no AWS Transit Gateway

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.

Adicione tags a um domínio de multicast do gateway do AWS Transit Gateway

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 Marcar recursos do Amazon EC2.

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.

Como adicionar tags a um domínio de multicast usando a AWS CLI

Use o comando create-tags.

Excluir um domínio de multicast no AWS Transit Gateway

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, escolha Transit Gateway Multicast (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 de multicast usando a AWS CLI

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

Domínios multicast compartilhados no AWS Transit Gateway

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

- Permissões do domínio de multicast compartilhado
- Faturamento e medição
- Cotas
- Compartilhe recursos entre zonas de disponibilidade no AWS Transit Gateway
- Compartilhe um domínio multicast no AWS Transit Gateway
- Cancelar o compartilhamento de um domínio multicast compartilhado no AWS Transit Gateway
- Identifique um domínio multicast compartilhado no AWS Transit Gateway

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 no AWS Transit Gateway

Para garantir que os recursos sejam distribuídos pelas zonas de disponibilidade de uma região, o AWS Transit Gateway mapeia de forma independente as zonas de disponibilidade s para os nomes de cada conta. Isso pode resultar em diferenças na nomenclatura de zonas de disponibilidade entre contas. Por exemplo, a zona de disponibilidade 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.

Compartilhe um domínio multicast no AWS Transit Gateway

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 multicast compartilhado no AWS Transit Gateway

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.

Identifique um domínio multicast compartilhado no AWS Transit Gateway

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.

Registre fontes com um grupo multicast no AWS Transit Gateway

> **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.

Registre membros com um grupo multicast no AWS Transit Gateway

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 fontes de um grupo de multicast no AWS Transit Gateway

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.

Como remover uma origem usando a AWS CLI

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

Cancele o registro de membros de um grupo multicast no Transit Gateway AWS

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.

Exibir grupos multicast no AWS Transit Gateway

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 AWS Transit Gateway

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

Como configurar o multicast para Windows Server usando o PowerShell

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

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

   > **Note**
   >
   > `New-ItemProperty` é um índice de propriedades que especifica a versão IGMP. Como o IGMP v2 é a versão compatível com multicast, a propriedade `Value` deve ser `3`. Em vez de editar o registro do Windows, 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. Reinicialize a instância do EC2.
5. Teste sua aplicação multicast para garantir que o tráfego esteja fluindo conforme o esperado.

Exemplo: Gerenciar configurações IGMP usando AWS o Transit Gateway

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 obter mais informações, consulte the section called “Associar anexos e sub-redes VPC a um domínio de multicast”.
7. A versão padrão do IGMP para o 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 estática no AWS Transit Gateway

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 estáticas de membros do grupo no AWS Transit Gateway

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”.

Alocação flexível de custos

Por padrão, o Transit Gateway usa um modelo de alocação de custos baseado no remetente, no qual as cobranças de processamento de dados são alocadas à conta proprietária do anexo de origem. Você pode criar políticas de medição personalizadas que definam quais contas devem ser cobradas com base nas propriedades do fluxo de tráfego, como tipos de anexos, IDs de anexos específicos ou endereços de rede.

As políticas de medição consistem em regras ordenadas que são avaliadas do menor para o maior número de regras. Quando o tráfego corresponde a uma regra, a conta especificada é cobrada de acordo com a configuração da regra. Você pode especificar o responsável pela conta para alocar custos a partir das seguintes opções:

- Proprietário do anexo de origem - As cobranças são alocadas à conta proprietária do anexo de origem (comportamento padrão)
- Proprietário do anexo de destino - As cobranças são alocadas à conta proprietária do anexo de destino
- Proprietário do Transit Gateway - As cobranças são alocadas à conta proprietária do Transit Gateway

A alocação flexível de custos permite um melhor gerenciamento de custos para organizações que usam arquiteturas de rede centralizadas, permitindo que os custos sejam alocados às unidades de negócios ou proprietários de aplicativos apropriados, independentemente da topologia da rede.

> **Note**
>
> A alocação flexível de custos permite a alocação flexível do uso da medição e, por sua vez, dos custos para os proprietários de contas de sua escolha. No entanto, as implicações fiscais para as AWS contas podem variar significativamente com base na localização geográfica, nos padrões de uso e em outros fatores. Analise as implicações de cobrança, impostos e gerenciamento de custos para contas em sua AWS organização antes de ativar esse recurso. Referência: O que é AWS Billing and Cost Management?

Políticas de medição

As políticas de medição permitem que você configure regras de alocação de custos para seu gateway de trânsito para controlar quais contas são cobradas pelo processamento de dados e custos de transferência com base nas propriedades do fluxo de tráfego. Esse recurso permite um melhor gerenciamento de custos e recursos de cobrança retroativa para organizações que usam arquiteturas de rede centralizadas.

Uma política de medição é composta pelo seguinte:

- Política de medição - O contêiner de configuração geral que contém as regras da política de medição. Quando criado, ele contém uma única entrada de política de medição padrão que é configurada para cobrar todo o tráfego do proprietário do anexo de origem. Cada gateway de trânsito pode ter somente uma política de medição.
- Entrada da política de medição - regras individuais dentro de uma política de medição que definem critérios de correspondência específicos e a conta para medir o uso. Cada entrada inclui um número de regra para a ordem de avaliação, condições de correspondência de tráfego (como tipos de anexo de origem e destino, IDs de anexo, blocos CIDR, portas e protocolos) e qual proprietário da conta cobrar pelo tráfego correspondente. Uma política pode conter até 50 entradas, avaliadas em ordem do menor para o maior número de regras.

  Você pode alocar o uso da medição para qualquer um dos seguintes:

  - Proprietário do anexo de origem: aloca o uso da medição para a conta proprietária do anexo de origem do tráfego (comportamento padrão)
  - Proprietário do anexo de destino: aloca o uso da medição para a conta proprietária do anexo em que o tráfego termina e
  - proprietário do gateway de trânsito: aloca o uso da medição para a conta proprietária do gateway de trânsito.
- Anexos do Middlebox - (opcional) anexos de gateway de trânsito designados que roteiam o tráfego por meio de dispositivos de rede para inspeção de segurança, balanceamento de carga ou outras funções de rede. O uso de dados para o tráfego que atravessa os anexos do middlebox é medido ao proprietário da conta especificado na política de medição. Você pode especificar no máximo 10 anexos de caixa intermediária. Os tipos de anexo de middlebox compatíveis são anexos de Função de AWS Rede (Firewall de Rede), VPC e VPN.

Como as políticas de medição funcionam

Por padrão, o Transit Gateway usa um modelo de alocação de custos baseado no remetente, no qual as cobranças de processamento de dados são calculadas para a conta proprietária do anexo de origem. Com as políticas de medição, você pode criar regras personalizadas para medir com flexibilidade o uso com base nas seguintes propriedades do fluxo de tráfego:

- Tipos de anexo de origem e destino (VPC, VPN, Client VPN, Direct Connect Gateway, Peering, Network Function e VPN Concentrator)
- IDs de anexo de origem e destino
- Endereços IP de origem e destino, intervalos de portas e protocolos

As políticas de medição consistem em regras ordenadas que são avaliadas do menor para o maior número de regras. Quando o tráfego corresponde a uma regra, a conta especificada é cobrada de acordo com a configuração da conta medida da regra. As políticas de medição abordam vários cenários organizacionais comuns:

- Alocação de custos do ambiente híbrido: aloque os custos AWS da entrada de dados do local por meio do Direct Connect Gateway para o proprietário da conta VPC de destino, em vez do proprietário da conta de administrador de TI central.
- Arquitetura de inspeção centralizada: aloque custos para proprietários individuais de aplicativos ou contas de VPC, em vez da equipe de segurança central, para o tráfego percorrido por meio de VPCs de inspeção.
- Application-based estorno: aloque todos os custos de uso de dados de uma carga de trabalho para o proprietário da VPC, independentemente da direção do tráfego.
- Alocação de custos do cliente: aloque os custos de dados às contas dos clientes quando eles criam anexos ao seu gateway de transporte público.

Anexos Middlebox

As políticas de medição do Transit Gateway oferecem suporte aos anexos do Middlebox, permitindo que você aloque com flexibilidade as taxas de processamento de dados para o tráfego de rede roteado por meio de dispositivos middlebox, como firewalls de rede e balanceadores de carga. Exemplos de anexos de middlebox são anexos de Função de Rede ao AWS Firewall de Rede ou anexos de VPC que roteiam o tráfego para dispositivos de segurança de terceiros em uma VPC. O tráfego entre os anexos do gateway de trânsito de origem e destino passa por esses anexos

de middlebox para casos de uso típicos de inspeção de segurança. Você pode definir políticas de medição para alocar de forma flexível o uso do processamento de dados em anexos do middlebox ao anexo de origem original, ao anexo de destino final ou ao proprietário da conta do gateway de trânsito. Para anexos da Função de Rede, as cobranças de processamento de dados do Firewall de AWS Rede também são alocadas à conta limitada.

Alocação flexível de custos - tipos de uso de medição

A alocação flexível de custos por meio de políticas de medição se aplica aos seguintes tipos de uso de dados:

- Uso do processamento de dados do Transit Gateway em anexos VPC, VPN, Client VPN, VPN Concentrator e Direct Connect
- Uso de transferência e saída de dados do Client VPN em anexos do Client VPN
- Site-to-site Uso de transferência de dados de VPN para fora em anexos de VPN
- Uso da transferência de dados do Direct Connect em anexos do Direct Connect.
- Uso da transferência de dados em anexos de emparelhamento TGW
- Uso do processamento de dados do Transit Gateway em anexos da função de rede
- AWS uso do processamento de dados do firewall de rede (NFW) em anexos da função de rede.

A alocação flexível de custos não se aplica ao uso horário de anexos e ao uso do processamento de dados multicast. Para anexos do Transit Gateway Connect, a política de medição pode ser definida para o anexo VPC de transporte ou Direct Connect subjacente. Para anexos VPN IP privados, a política de medição pode ser definida para o anexo subjacente do Direct Connect de transporte.

Considerações e limitações

Considere o seguinte ao implementar políticas de medição para seu gateway de trânsito.

Permissões

- Somente o proprietário do gateway de trânsito pode criar, modificar ou excluir políticas de medição.
- As configurações de alocação de custos se aplicam no nível do gateway de trânsito.
- Os proprietários do anexo não podem substituir as configurações de alocação de custos definidas pelo proprietário do gateway de trânsito.

Emparelhamento do Transit Gateway

Quando o tráfego atravessa as conexões de emparelhamento do gateway de trânsito:

- Cada gateway de trânsito aplica sua própria política de medição de forma independente.
- As cobranças de dados são alocadas separadamente por cada gateway de trânsito com base em sua política local.
- O tráfego pode ser considerado como dois fluxos separados: conexão de origem ao peering e peering ao anexo de destino.

Integração de WAN em nuvem

Quando um gateway de trânsito é conectado a uma rede principal do Cloud WAN:

- As taxas de transferência de dados do Transit Gateway em conexões de peering são alocadas de acordo com a política de medição do Transit Gateway.
- As políticas de medição não são suportadas nas redes principais do Cloud WAN.

Impacto no desempenho

- As políticas de medição não introduzem nenhuma latência adicional no caminho de dados.
- As políticas de medição não têm impacto na largura de banda máxima por anexo.
- Não há alterações nos recursos de compartilhamento de recursos do gateway de trânsito.

Integração de faturamento

- As etiquetas de alocação de custos continuam funcionando com políticas de medição para organizar os custos por unidade de negócios.
- As políticas de medição definem quais contas incorrem em custos, enquanto as etiquetas de alocação de custos ajudam a categorizar esses custos.
- As alterações nas políticas de medição entrarão em vigor no final da próxima hora de cobrança.

Suporte a IPv6

As políticas de medição são suportadas para tráfego IPv4 e IPv6. A correspondência de blocos CIDR nas entradas de política funciona com ambas as famílias de endereços.

Suporte de anexo Middlebox

- A política de medição da caixa intermediária pressupõe que o tráfego entre o anexo original de origem e o de destino seja fixado por meio do anexo da caixa intermediária especificado (exemplo, inspeção leste-oeste do tráfego). VPC-to-VPC Portanto, a rede de 5 tuplas (source/destination IPs, source/destination portas e protocolo) para fluxos que entram e saem dos anexos intermediários deve corresponder. Fluxos com incompatibilidades de 5 tuplas em anexos de caixa intermediária (por exemplo, transformação NAT na VPC de inspeção) são tratados como fluxos regulares de anexos de origem e destino (em oposição aos fluxos de anexos de caixa intermediária).
- Todos os fluxos somente de saída no anexo da caixa intermediária (por exemplo, tráfego norte-sul para a Internet via IGW em uma VPC de inspeção) são tratados como fluxos regulares de origem e destino (em oposição aos fluxos de conexão da caixa intermediária).
- Para anexos da função de rede, quando o firewall de AWS rede descarta pacotes, todo o uso do processamento de dados é cobrado de volta na conta do remetente, independentemente da configuração da política de medição.

Crie uma política de medição do AWS Transit Gateway

Para habilitar políticas de medição, você deve criar uma política de medição para seu gateway de trânsito e configurar entradas de política que definam como o uso da medição é alocado. A política de medição estabelece a estrutura e as configurações padrão, enquanto as entradas da política contêm as regras específicas que determinam quais contas são monitoradas com base nas características do tráfego.

As entradas da política de medição funcionam como regras ordenadas que são aplicadas sequencialmente do menor para o maior número de regras para o tráfego que flui pelo gateway de trânsito. Cada entrada define critérios de correspondência, como tipos de anexo de origem e destino, blocos CIDR, protocolos e intervalos de portas, junto com a conta que deve ser medida para o tráfego correspondente. Quando um fluxo de tráfego corresponde a várias entradas, a entrada com o menor número de regra tem precedência. Se nenhuma entrada corresponder a um fluxo específico, a conta medida padrão especificada na política será cobrada.

Depois de criar uma política, você precisará adicionar entradas de política para implementar sua lógica de alocação de custos. Para obter as etapas para criar uma entrada de política de medição, consulteCrie uma entrada de política de medição.

Crie uma política de medição usando o console

Crie uma política para definir regras flexíveis de alocação de custos para o uso de dados do gateway de trânsito. Por padrão, todos os fluxos são medidos para o proprietário do anexo de origem. Crie entradas para faturar fluxos de rede específicos para contas diferentes.

Para criar uma política de medição

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Políticas de medição.
3. Escolha Criar política de medição.
4. Para ID do gateway de trânsito, escolha o gateway de trânsito para o qual você gostaria de criar uma política de medição.
5. (Opcional) Para anexo de caixa intermediária IDs, escolha um ou mais anexos de caixa intermediária. Por padrão, o uso de dados é medido para o proprietário do middlebox. O suporte a anexos do Middlebox permite que a política de medição seja aplicada ao tráfego que atravessa os anexos do Middlebox. Anexos adicionais podem ser adicionados posteriormente.
6. (Opcional) Na seção Tags, adicione tags para ajudá-lo a identificar e organizar sua política de medição:
   a. Selecione Adicionar nova tag.
   b. Insira uma chave de tag e, opcionalmente, um valor de tag.
   c. Selecione Adicionar nova tag para adicionar mais tags ou vá para a próxima etapa. É possível adicionar até 50 tags.
7. Escolha Criar política de medição do gateway de trânsito.

> **Note**
>
> A conta monitorada padrão é o proprietário do anexo de origem e, depois de criar uma política de medição, você pode adicionar entradas que definem qual conta será cobrada com base nas propriedades do fluxo de tráfego, observando que a entrada de política padrão (que é a última entrada) não pode ser modificada ou excluída como outras entradas de política.

Crie uma política de medição usando o AWS CLI

Uma política de medição define o comportamento padrão de alocação de custos e as configurações globais para seu gateway de trânsito. Use a create-transit-gateway-meteringpolítica -.

Parâmetros obrigatórios:

- `--transit-gateway-id`- O ID do gateway de trânsito para criar a política para

Parâmetros opcionais:

- `--middle-box-attachment-ids`- IDs de anexo de gateway de trânsito compatíveis para adicionar à política como caixa intermediária
- `--tag-specifications`- etiquetas para política de medição

Para criar uma política de medição usando o AWS CLI

1. Execute o create-transit-gateway-metering-policy comando para criar uma nova política de medição com anexos opcionais do middlebox.

```
aws ec2 create-transit-gateway-metering-policy \
    --transit-gateway-id tgw-07a5946195a67dc47 \
    --middle-box-attachment-ids \
    tgw-attach-0123456789abcdef0 \
    tgw-attach-0abc123def456789a \
    --tag-specifications \
    '[{ "ResourceType": "transit-gateway-metering-policy", \
    "Tags": [ { "Key": "Env", "Value": "Prod" } ] }]'
```

   Esse comando cria uma política de medição para o gateway de trânsito especificado com os anexos e tags de middlebox fornecidos.

2. O comando retorna a seguinte saída quando a política é criada com sucesso:

```
{
    "TransitGatewayMeteringPolicy": {
        "TransitGatewayMeteringPolicyId": "tgw-mp-042d444564d4b2da7",
        "TransitGatewayId": "tgw-07a5946195a67dc47",
        "MiddleboxAttachmentIds":  ["tgw-attach-0123456789abcdef0",
        "tgw-attach-0abc123def456789a"],
```

```
        "State": "pending",
        "UpdateEffectiveAt": "2025-11-05T21:00:00.000Z",
        "Tags": [{"Key": "Env","Value": "Prod"}]
    }
}
```

Observe o ID da política de medição retornado na resposta para uso em comandos subsequentes. describe-transit-gateway-metering-policieso comando pode ser usado para obter a política de medição associada ao gateway de trânsito.

Gerenciar políticas AWS de medição do Transit Gateway

Depois de criar uma política de medição, você pode gerenciá-la visualizando as configurações atuais, modificando as opções de configuração ou excluindo a política quando não for mais necessária. As operações de gerenciamento permitem que você adicione ou remova anexos de middlebox à medida que seus requisitos de rede mudam. Você só pode criar ou excluir uma entrada de política. Se precisar modificar uma regra existente, você pode excluir a entrada e criar uma nova com a configuração modificada. Todas as operações de gerenciamento exigem permissões do proprietário do gateway de trânsito e entram em vigor após duas horas de cobrança.

O gerenciamento eficaz da política de medição é crucial para manter a alocação precisa de custos à medida que sua arquitetura de rede evolui. Muitas vezes, as organizações precisam ajustar suas políticas quando as unidades de negócios mudam, novos aplicativos são implantados ou as topologias de rede são modificadas. Por exemplo, as configurações de suporte à medição do middlebox podem exigir atualizações quando as arquiteturas de segurança do firewall mudam ou quando novos serviços de inspeção são introduzidos no caminho do tráfego.

As modificações de políticas oferecem suporte a vários cenários operacionais, incluindo mudanças sazonais no padrão de tráfego, atividades de fusão e aquisição e atualizações de requisitos de conformidade. Ao gerenciar políticas, considere o impacto nos acordos de cobrança existentes e comunique as mudanças às partes interessadas afetadas antes da implementação.

As revisões regulares das políticas ajudam a garantir que a alocação de custos permaneça alinhada aos objetivos de negócios e às estruturas organizacionais. As melhores práticas incluem documentar mudanças nas políticas, testar modificações em ambientes que não sejam de produção, quando possível, e coordenar com as equipes financeiras para entender as implicações do faturamento. Além disso, considere o momento das mudanças na política para minimizar a interrupção dos ciclos de cobrança mensal e dos processos de relatórios financeiros.

Tópicos

Editar uma política de medição do AWS Transit Gateway

Edite as políticas de medição existentes para modificar as configurações de anexos do middlebox. As modificações da política entrarão em vigor na próxima hora de cobrança e se aplicam a todos os fluxos de tráfego futuros por meio de seu gateway de trânsito.

Editar uma política de medição usando o console

Use o console para modificar as configurações de política de medição existentes para seu gateway de trânsito.

Para editar uma política de medição existente usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Políticas de medição.
3. Selecione a política de medição que você deseja modificar escolhendo sua ID de política
4. Modifique as configurações de política disponíveis em Ações. O console só permite adicionar e remover anexos da caixa central.
    - Anexos do Middlebox - adicione ou remova anexos do Transit Gateway que devem ser tratados como caixas intermediárias para faturamento especializado.

Edite uma política de medição usando o AWS CLI

Use o modify-transit-gateway-metering-policy comando para visualizar e modificar as políticas de medição.

Parâmetros necessários para operações de modificação:

- `--transit-gateway-metering-policy-id`- O ID da política de medição a ser modificada
- `--add-middle-box-attachment-ids`ou `--remove-middle-box-attachment-ids` - IDs de anexo do Transit Gateway compatíveis para adicionar ou remover da política como caixa intermediária

Para visualizar e editar políticas de medição usando a CLI AWS

1. (Opcional) Visualize as políticas de medição existentes usando o describe-transit-gateway-metering-policies comando para ver as configurações atuais:

   ```
   aws ec2 describe-transit-gateway-metering-policies
   ```

   Esse comando retorna todas as políticas de medição em sua conta, mostrando seu estado atual e os anexos habilitados como caixa intermediária para cada política de medição.

2. Modifique uma política de medição usando o modify-transit-gateway-metering-policy comando para atualizar as opções de configuração:

   ```
   aws ec2 modify-transit-gateway-metering-policy \
       --transit-gateway-metering-policy-id tgw-mp-042d444564d4b2da7 \
       --add-middle-box-attachment-ids tgw-attach-0123456789abcdef1  \
       --remove-middle-box-attachment-ids tgw-attach-0abc123def456789a
   ```

   Esse comando modifica uma política de medição adicionando a and/or remoção de anexos da caixa intermediária.

3. O comando retorna a seguinte saída quando a política é modificada com sucesso:

   ```
   {
       "TransitGatewayMeteringPolicy": {
           "TransitGatewayMeteringPolicyId": "tgw-mp-042d444564d4b2da7",
           "TransitGatewayId": "tgw-07a5946195a67dc47",
           "MiddleboxAttachmentIds":  ["tgw-attach-0123456789abcdef0",
           "tgw-attach-0123456789abcdef1"],
           "State": "modifying",
           "UpdateEffectiveAt": "2025-11-05T21:00:00.000Z"
       }
   }
   ```

   As alterações podem levar até duas horas de cobrança para entrarem em vigor.

Excluir uma política de medição do AWS Transit Gateway

Exclua as políticas de medição quando elas não forem mais necessárias para sua estratégia de alocação de custos do gateway de trânsito. A exclusão de uma política reverte a alocação de

custos para o modelo padrão baseado no remetente, em que as cobranças de processamento e transferência de dados são alocadas à conta proprietária do anexo de origem. Todas as entradas de política associadas à política de medição excluída também são removidas.

Excluir uma política de medição usando o console

Use o console para remover políticas de medição que não são mais necessárias.

Para excluir uma política de medição usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Políticas de medição.
3. Selecione a política que você deseja excluir escolhendo sua ID de política.
4. Escolha Actions (Ações) e então Delete (Excluir).
5. Confirme a exclusão digitando **`delete`** na caixa de diálogo de confirmação.
6. Escolha Excluir.

> **Important**
>
> A exclusão de uma política de medição é irreversível. Todas as entradas de política e definições de configuração serão removidas permanentemente, e a alocação de custos será revertida para o modelo padrão baseado no remetente.

Exclua uma política de medição usando o AWS CLI

Use o delete-transit-gateway-metering-policy comando para excluir as políticas de medição programaticamente.

Requisitos:

- Permissões do proprietário do gateway de trânsito

Parâmetros obrigatórios:

- `--transit-gateway-metering-policy-id`- O ID da política de medição a ser excluída

Para visualizar e excluir políticas de medição usando a AWS CLI

1. (Opcional) Visualize as políticas de medição existentes usando o describe-transit-gateway-metering-policies comando para ver as configurações atuais:

```
aws ec2 describe-transit-gateway-metering-policies
```

   Esse comando retorna todas as políticas de medição em sua conta, mostrando o estado e a configuração atuais.

2. Exclua uma política de medição usando o delete-transit-gateway-metering-policy comando para remover permanentemente a política:

```
aws ec2 delete-transit-gateway-metering-policy \
    --transit-gateway-metering-policy-id tgw-mp-042d444564d4b2da7
```

   Esse comando remove permanentemente a política de medição especificada e todas as entradas associadas. A alocação de custos será revertida para o modelo padrão baseado no remetente para todos os fluxos de tráfego futuros. Essa alteração também leva 2 horas de cobrança para entrar em vigor.

3. O comando retorna a seguinte saída quando a política é excluída com sucesso:

```
{
    "TransitGatewayMeteringPolicy": {
        "TransitGatewayMeteringPolicyId": "tgw-mp-042d444564d4b2da7",
        "TransitGatewayId": "tgw-07a5946195a67dc47",
        "MiddleboxAttachmentIds":  ["tgw-attach-0123456789abcdef0",
        "tgw-attach-0123456789abcdef1"],
        "State": "deleting",
        "UpdateEffectiveAt": "2025-11-05T21:00:00.000Z"
    }
}
```

   A resposta confirma que a política está sendo excluída com um `deleting` estado enquanto a remoção é processada na infraestrutura do gateway de trânsito.

Crie um AWS Entrada da política de medição do Transit Gateway

Por padrão, todos os fluxos são medidos para o proprietário do anexo de origem. Para medir fluxos específicos para contas diferentes, crie entradas de política individuais que definam qual conta será cobrada com base nas propriedades do fluxo de tráfego.

As entradas da política de medição funcionam como regras condicionais que são avaliadas em ordem sequencial com base em seus números de regras quando o tráfego flui pelo gateway de trânsito. Cada entrada atua como uma declaração “if-then”: se o tráfego corresponder aos critérios especificados (como tipo de anexo de origem, bloco CIDR de destino ou protocolo), então cobre a conta designada. O sistema avalia as entradas do menor para o maior número de regras, e a primeira entrada correspondente determina a conta de cobrança desse fluxo de tráfego.

As entradas oferecem suporte a uma ampla variedade de critérios de correspondência, incluindo tipos de anexo (VPC, VPN, Client VPN, Direct Connect Gateway, Peering, Network Function e VPN Concentrator), IDs de anexos específicos, blocos CIDR de origem e destino, tipos de protocolo e intervalos de portas. Você pode combinar vários critérios em uma única entrada para criar regras de segmentação precisas. Por exemplo, você pode criar uma entrada que corresponda a todo o tráfego HTTPS (porta 443) dos anexos da VPC a um intervalo CIDR de destino específico e cobrar esses fluxos na conta de uma equipe de segurança. Se nenhuma entrada corresponder a um fluxo de tráfego específico, a conta medida padrão especificada na política de medição principal será cobrada, garantindo que todo o tráfego seja cobrado adequadamente. A criação de uma entrada leva 2 horas de cobrança para entrar em vigor.

> **Important**
>
> - Planeje os números das regras com cuidado — deixe espaços (por exemplo, 10, 20, 30) para permitir futuras inserções
> - Teste as entradas com condições menos específicas antes de adicionar regras mais restritivas
> - Use condições de correspondência específicas para evitar cobranças não intencionais

Crie uma entrada de política de medição usando o console

Uma política de medição define o comportamento padrão de alocação de custos e as configurações globais para seu gateway de trânsito.

Para criar uma entrada de política de medição usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Políticas de medição.
3. Selecione o link do ID da política de medição para ver seus detalhes.
4. Escolha a guia Entradas da política de medição.
5. Escolha Criar entrada de política de medição.
6. Número da regra de política - Esse deve ser um número exclusivo (1 a 32.766) que determina a ordem de avaliação. Números mais baixos têm maior prioridade.
7. Conta medida - Escolha um dos seguintes tipos de conta a serem cobrados pela correspondência dos fluxos de tráfego:

   a. Proprietário do anexo de origem
   b. Proprietário do anexo de destino
   c. Proprietário do anexo do Transit Gateway
8. (Opcional) Escolha condições de regra - Essas condições opcionais definem critérios para corresponder ao tráfego específico:

   - Tipo de anexo de origem ou ID - Filtre por tipo de anexo (VPC, VPN, Client VPN, Direct Connect Gateway, Peering, Network Function e VPN Concentrator) ou ID.
   - Tipo de anexo ou ID de destino - Filtrar por tipo de anexo ou ID de destino
   - Bloco CIDR de origem - Combine o tráfego de intervalos de IP específicos
   - Bloco CIDR de destino - Combine o tráfego com intervalos de IP específicos
   - Intervalo de portas de origem - Combine portas de origem específicas
   - Intervalo de portas de destino - Combine portas de destino específicas
   - Protocolo - Filtre por protocolo para a regra (1, 6, 17, etc.)
9. Escolha Criar entrada de política de medição para salvar a configuração.

Crie uma entrada de política de medição usando o AWS CLI

As entradas de política definem regras específicas para alocação de custos com base nas características do tráfego. As regras são avaliadas na ordem do menor para o maior número de regras.

Parâmetros obrigatórios:

- `--transit-gateway-metering-policy-id`- O ID da política de medição à qual adicionar a entrada
- `--policy-rule-number`- Um número exclusivo (1-32.766) que determina a ordem de avaliação
- `--metered-account`- tipo de pagador (proprietário do anexo de origem/proprietário do anexo de destino/proprietário do gateway de trânsito)

Parâmetros opcionais:

Esses parâmetros opcionais que definem critérios para corresponder ao tráfego específico:

- `--source-transit-gateway-attachment-id`- A ID do anexo do gateway de trânsito de origem.
- `--source-transit-gateway-attachment-type`- O tipo do anexo do gateway de trânsito de origem.
- `--source-cidr-block`- O bloco CIDR de origem da regra.
- `--source-port-range`- O intervalo de portas de origem da regra.
- `--destination-transit-gateway-attachment-id`- A ID do anexo do gateway de trânsito de destino.
- `--destination-transit-gateway-attachment-type`- O tipo do anexo do gateway de trânsito de destino.
- `--destination-cidr-block`- O bloco CIDR de destino da regra.
- `--destination-port-range`- O intervalo de portas de destino da regra.
- `--protocol`- O número do protocolo da regra

Para criar uma entrada de política de medição usando o AWS CLI

1. Use o create-transit-gateway-metering-policy-entry comando para criar uma nova entrada de política que roteie o tráfego da VPC para uma conta limitada específica:

```
aws ec2 create-transit-gateway-metering-policy-entry \
    --transit-gateway-metering-policy-id tgw-mp-042d444564d4b2da7 \
    --policy-rule-number 100 \
    --destination-transit-gateway-attachment-type vpc \
    --metered-account destination-attachment-owner
```

Esse comando cria uma entrada de política com a regra número 100 que corresponde ao tráfego destinado a anexos de VPC e cobra do proprietário do anexo de destino por esses fluxos.

2. O comando retorna a seguinte saída quando a entrada é criada com sucesso:

```
{
    "TransitGatewayMeteringPolicyEntry": {
        "MeteredAccount": "destination-attachment-owner",
        "MeteringPolicyRule": {
            "DestinationTransitGatewayAttachmentType": "vpc"
        },
        "PolicyRuleNumber": 100,
        "State": "available",
        "UpdateEffectiveAt": "2025-11-06T02:00:00.000Z"
    }
}
```

A resposta confirma que a entrada foi criada com um estado “disponível” enquanto está sendo ativada na infraestrutura do gateway de trânsito.

Excluir uma entrada da política de medição do AWS Transit Gateway

Exclua as entradas da política de medição quando as regras específicas de alocação de custos não forem mais necessárias para seus fluxos de tráfego de rede. A exclusão de entradas ajuda a simplificar o gerenciamento de políticas, removendo regras desatualizadas ou desnecessárias, mantendo a estrutura geral da política. Quando você exclui uma entrada, o tráfego que correspondia anteriormente à regra excluída será avaliado em relação às entradas restantes na ordem numérica da regra ou retornará ao comportamento da política padrão se nenhuma outra entrada corresponder.

Antes de excluir as entradas, considere o impacto nos atuais acordos de cobrança e nos fluxos de tráfego. Depois de excluída, a alteração leva até 2 horas de cobrança para entrar em vigor e não pode ser desfeita. Portanto, coordene as alterações com os proprietários da conta e as equipes financeiras afetadas. Analise as entradas restantes para garantir a cobertura adequada do tráfego e a alocação de faturamento após a exclusão. A ordem de avaliação das regras para as entradas restantes permanece inalterada, mantendo um comportamento previsível de alocação de custos para fluxos de tráfego contínuos.

Important

- A exclusão é irreversível
- O tráfego que anteriormente correspondia a essa entrada será reavaliado em relação às entradas restantes
- Revise as entradas restantes para garantir a cobertura adequada do tráfego

Excluir uma entrada de política de medição usando o console

Use o console para remover entradas de política por meio de uma interface intuitiva que fornece caixas de diálogo de confirmação para evitar exclusões acidentais.

Para excluir uma entrada de política usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Políticas de medição.
3. Selecione a política de medição que contém a entrada que você deseja excluir.
4. Selecione a entrada que você deseja remover e escolha Excluir.
5. Na caixa de diálogo de confirmação, revise os detalhes da entrada e digite **`delete`** para confirmar a remoção.
6. Escolha Excluir para remover permanentemente a entrada.

Exclua uma entrada da política de medição usando o AWS CLI

Use o delete-transit-gateway-metering-policy-entry comando para remover entradas de política de forma programática.

Requisitos:

- Permissões do proprietário do gateway de trânsito
- ID da política de medição e número da regra de entrada válidos

Parâmetros obrigatórios:

- `--transit-gateway-metering-policy-id`- O ID da política de medição

- `--policy-rule-number`- O número da regra da entrada a ser excluída

Para visualizar e excluir entradas de política usando a AWS CLI

1. (Opcional) Visualize as entradas de política existentes usando o get-transit-gateway-metering-policy-entries comando para ver as configurações atuais:

```
aws ec2 get-transit-gateway-metering-policy-entries \
    --transit-gateway-metering-policy-id tgw-mp-0123456789abcdefg
```

   Esse comando retorna todas as entradas da política especificada, mostrando seus números de regras, critérios de correspondência e contas monitoradas.

2. Exclua uma entrada de política usando o delete-transit-gateway-metering-policy-entry comando para remover permanentemente a entrada:

```
aws ec2 delete-transit-gateway-metering-policy-entry \
    --transit-gateway-metering-policy-id tgw-mp-0123456789abcdefg \
    --policy-rule-number 100
```

   Esse comando remove permanentemente a entrada especificada da política. O tráfego que correspondia anteriormente a essa entrada será imediatamente reavaliado em relação às entradas restantes ou retornará ao comportamento de política padrão.

3. O comando retorna a seguinte saída quando a entrada é excluída com sucesso:

```
{
    "TransitGatewayMeteringPolicyEntry": [
        {
            "PolicyRuleNumber": 100,
            "MeteredAccount": "destination-attachment-owner",
            "UpdateEffectiveAt": "2024-01-01T01:00:00+00:00",
            "state": "deleted",
            "MeteringPolicyRule": {
                "DestinationTransitGatewayAttachmentType": "vpc"
            }
        }
}
```

A resposta confirma que a entrada está sendo excluída com um estado “excluído” enquanto a remoção é processada na infraestrutura do gateway de trânsito.

Gerenciar anexos da middlebox da política de medição do AWS Transit Gateway

as políticas de medição de gateway de trânsito oferecem suporte a anexos do Middlebox, permitindo que você aloque com flexibilidade as taxas de processamento de dados para o tráfego de rede roteado por meio de dispositivos middlebox, como firewalls de rede e balanceadores de carga. Exemplos de anexos de middlebox são anexos de Função de Rede ao AWS Firewall de Rede ou anexos de VPC que roteiam o tráfego para dispositivos de segurança de terceiros em uma VPC. O tráfego entre os anexos do gateway de trânsito de origem e destino passa por esses anexos de middlebox para casos de uso típicos de inspeção de segurança. Você pode definir políticas de medição para alocar de forma flexível o uso do processamento de dados em anexos do middlebox ao anexo de origem original, ao anexo de destino final ou ao proprietário da conta do gateway de trânsito. Para anexos da Função de Rede, as cobranças de processamento de dados do Firewall de AWS Rede também são alocadas à conta limitada.

Anexos de gateway de trânsito designados que roteiam o tráfego por meio de dispositivos de rede para inspeção de segurança, balanceamento de carga ou outras funções de rede. O uso de dados para o tráfego que atravessa os anexos do middlebox é medido ao proprietário da conta especificado na política de medição. Você pode especificar no máximo 10 anexos de caixa intermediária. Os tipos de anexo de middlebox compatíveis são anexos de Função de AWS Rede (Firewall de Rede), VPC e VPN.

Tópicos

- Adicionar anexos da caixa intermediária da política de medição do AWS Transit Gateway
- Remover os anexos da caixa intermediária da política de medição do AWS Transit Gateway

Adicionar anexos da caixa intermediária da política de medição do AWS Transit Gateway

Você pode adicionar anexos de middlebox para integrar dispositivos de rede à sua política de medição do Transit Gateway. Isso permite rotear tráfego específico por meio de dispositivos de

segurança, balanceadores de carga ou outras funções de rede, mantendo o controle granular da alocação de custos.

> **Important**
>
> - Garanta que os dispositivos middlebox estejam configurados e acessíveis adequadamente
> - Teste o roteamento de tráfego antes de aplicá-lo às cargas de trabalho de produção
> - Monitore o desempenho do middlebox para evitar a introdução de latência
> - Configure o comportamento de failover adequado para alta disponibilidade

Adicione anexos do middlebox usando o console

Para adicionar uma entrada de anexo de caixa intermediária

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Políticas de medição.
3. Selecione o link do ID da política de medição para ver seus detalhes.
4. Escolha a guia Anexos do Middlebox.
5. Escolha Adicionar.
6. Quando solicitado, selecione o anexo da caixa intermediária IDs que deve ser tratado como caixas intermediárias para cobrança especializada. Você pode selecionar até 10 anexos de caixa intermediária.
7. Escolha Adicionar anexos do middlebox para salvar a configuração.

Adicione anexos do middlebox usando o AWS CLI

Use o modify-transit-gateway-metering-policy comando para adicionar anexos.

Antes de começar, verifique se você tem os seguintes parâmetros obrigatórios:

- `--transit-gateway-metering-policy-id`- O ID da política de medição existente
- `--add-middle-box-attachment-ids`- Um ou mais IDs anexos para adicionar à política (para adicionar anexos)

Para adicionar anexos de middlebox a uma política existente usando a CLI AWS

1. No exemplo a seguir, modify-transit-gateway-metering-policy é usado para adicionar quatro anexos de caixa intermediária a uma política de medição existente. O comando adiciona o anexo especificado IDs à lista existente sem remover os anexos atuais:

```
aws ec2 modify-transit-gateway-metering-policy \
    --transit-gateway-metering-policy-id tgw-mp-0123456789abcdefg \
    --add-middle-box-attachment-ids tgw-attach-0bdc681c211bf71f3 tgw-
attach-0987654321fedcba0 tgw-attach-0456789012345abcd tgw-attach-0fedcba0987654321
```

2. No exemplo de resposta a seguir, a saída JSON mostra a configuração de política atualizada com todos os quatro anexos de middlebox agora incluídos:

```
{
    "TransitGatewayMeteringPolicy": {
        "TransitGatewayMeteringPolicyId": "tgw-mp-0123456789abcdefg",
        "TransitGatewayId": "tgw-0ecec6433f4bfe55a",
        "MiddleBoxAttachmentIds": [
            "tgw-attach-0bdc681c211bf71f3",
            "tgw-attach-0987654321fedcba0",
            "tgw-attach-0456789012345abcd",
            "tgw-attach-0fedcba0987654321"
        ],
        "State": "available",
        "UpdateEffectiveAt": "2024-09-05T16:00:00.000Z"
    }
}
```

Remover os anexos da caixa intermediária da política de medição do AWS Transit Gateway

Por padrão, os custos de medição são atribuídos ao proprietário do anexo da caixa intermediária. No entanto, você pode modificar essas atribuições para garantir que os custos sejam alocados adequadamente à origem ou ao destino real do tráfego. Você pode adicionar ou remover até 10 anexos totais de middlebox para uma política de medição.

Remova os anexos do middlebox usando o console

Use o console da Amazon VPC para remover anexos de middlebox da sua configuração de política de medição.

Para remover anexos do middlebox

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Transit Gateways, Metering policies.
3. Selecione a política de medição que você deseja modificar.
4. Escolha a guia Anexos do Middlebox.
5. Selecione até 10 anexos de caixa intermediária para remover da política de medição.
6. Escolha Remover .
7. Quando solicitado, você pode atualizar os anexos do middlebox escolhidos para removê-los. O tráfego por meio de anexos removidos será medido para o proprietário do anexo do middlebox.
8. Escolha Remover anexos do middlebox.

Remova os anexos da caixa intermediária usando o AWS CLI

Use o modify-transit-gateway-metering-policy comando para remover anexos.

Antes de começar, verifique se você tem os seguintes parâmetros obrigatórios:

- `--transit-gateway-metering-policy-id`- O ID da política de medição existente
- `--remove-middle-box-attachment-ids`- Um ou mais IDs anexos a serem removidos da política (para remover anexos)

Para remover anexos do middlebox de uma política existente usando a CLI AWS

1. No exemplo a seguir, modify-transit-gateway-metering-policy é usado para remover dois anexos específicos de middlebox de uma política de medição existente. O comando remove somente o anexo especificado IDs enquanto preserva os anexos restantes:

```
aws ec2 modify-transit-gateway-metering-policy \
    --transit-gateway-metering-policy-id tgw-mp-0123456789abcdefg \
    --remove-middle-box-attachment-ids tgw-attach-0456789012345abcd tgw-
attach-0fedcba0987654321
```

2. No exemplo de resposta a seguir, a saída JSON mostra a configuração de política atualizada com os anexos especificados removidos e os demais anexos ainda ativos:


```
{
    "TransitGatewayMeteringPolicy": {
        "TransitGatewayMeteringPolicyId": "tgw-mp-0123456789abcdefg",
        "TransitGatewayId": "tgw-0ecec6433f4bfe55a",
        "MiddleBoxAttachmentIds": [
            "tgw-attach-0bdc681c211bf71f3",
            "tgw-attach-0987654321fedcba0"
        ],
        "State": "available",
        "UpdateEffectiveAt": "2024-09-05T16:00:00.000Z"
    }
}
```

AWS Registros de fluxo do Transit Gateway

O Transit Gateway Flow Logs é um recurso do AWS Transit Gateway que permite capturar informações sobre o tráfego IP que entra e sai de seus 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”. Para capturar informações sobre o tráfego IP proveniente e direcionado às interfaces de rede em suas VPCs, use os logs de fluxo de VPC. Consulte Como registrar tráfego IP em log com logs de fluxo da VPC no Guia do usuário do Amazon VPC.

> **Note**
>
> Para criar um log de fluxo de gateway de trânsito, 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 AWS Transit Gateway.

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 saber mais, 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.
- O Transit Gateway Flow Logs suporta um máximo de 250 assinaturas por recurso por conta. Para criar mais assinaturas em um recurso que tenha atingido esse limite, você deve primeiro excluir as assinaturas existentes.

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 estiver como texto sem formatação, todos os campos serão do tipo STRING. Se o formato for Parquet, consulte a tabela para os tipos de dados de campo.

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

Campo	Descrição	Versão
version	Indica a versão na qual o campo foi introduzido. O formato padrão inclui todos os campos da versão 2, na mesma ordem em que aparecem na tabela. Tipo de dados em Parquet: INT_32	2
resource-type	O tipo de recurso no qual a assinatura é criada. Para os logs de fluxo do Transit Gateway, 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.	6

Campo	Descrição	Versão
	Tipo de dados em Parquet: STRING	
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 Manual do usuário do Amazon EC2. 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 tempo de vida. 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 estar OR-ed durante o intervalo de agregação. Para conexões curtas, os sinalizadores podem ser definidos na mesma linha no registro do log de fluxo, por exemplo, 19 para SYN-ACK e FIN e 3 para SYN e FIN. Tipo de dados em Parquet: INT_32	3
region	A região que contém o gateway de trânsito no qual o tráfego é registrado. Tipo de dados em Parquet: STRING	4

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

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 os recursos do Amazon EC2 na Referência de API do Amazon EC2.

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

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteFlowLogs",
        "ec2:CreateFlowLogs",
        "ec2:DescribeFlowLogs"
      ],
      "Resource": "*"
    }
  ]
}
```

Algumas configurações adicionais de funções e permissões do IAM são necessárias, dependendo se você está publicando no CloudWatch Logs ou no Amazon S3. Para obter mais informações, consulte AWS Registros de registros de fluxo do Transit Gateway no Amazon CloudWatch Logs e AWS Registros de registros de fluxo do Transit Gateway 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 uma função do IAM para AWS Transit Gateway Flow Logs

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 . Em Caso de uso, selecione 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.

AWS 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.

JSON

```
{
  "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.

JSON

```
{
  "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.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "arn:aws:iam::111122223333:role/flow-log-role-name"
        }
    ]
}
```

Crie um registro de registros de fluxo do AWS Transit Gateway que seja publicado no 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 Console de gerenciamento da AWS 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 AWS 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 AWS 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.

AWS Registros de registros de fluxo do Transit Gateway 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.

JSON

```
{
  "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 Políticas de bucket no Guia do usuário do Amazon Simple Storage Service.

JSON

```
{
    "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:us-east-1:123456789012:*"
                }
            }
        },
        {
            "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:us-east-1:123456789012:*"
                }
            }
        }
    ]
```

```
}
```

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.

Crie a função da conta de origem do AWS 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 Console de gerenciamento da AWS 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. Escolha Criar Perfil.
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.

Crie um registro de registros de fluxo do AWS Transit Gateway que publique 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/'
```

Visualize registros de registros de fluxo do AWS 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 processados AWS de registros de fluxo do Transit Gateway 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.

AWS Transit Gateway, registros de registros de fluxo no Amazon Data Firehose

Tópicos

- Perfis do IAM para entrega entre contas
- Crie a função da conta de origem do AWS Transit Gateway Flow Logs para o Amazon Data Firehose
- Crie a função de conta de destino do AWS Transit Gateway Flow Logs para o Amazon Data Firehose
- Crie um registro de registros de fluxo do AWS Transit Gateway que publique 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.

Preços

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`

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
```

```
            "Resource": "arn:aws:iam::111122223333:role/mySourceRole",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "delivery.logs.amazonaws.com"
                },
                "StringLike": {
                    "iam:AssociatedResourceARN": [
                        "arn:aws:ec2:us-east-1: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::111122223333: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.

JSON

```
{
  "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.

JSON

```
{
  "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.

JSON

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

```
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/mySourceRole"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Crie a função da conta de origem do AWS 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 Console de gerenciamento da AWS 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. Escolha Criar Perfil.
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.

Crie a função de conta de destino do AWS Transit Gateway Flow Logs 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 Console de gerenciamento da AWS 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, escolha Perfis.
6. Escolha Criar Perfil.
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.

Crie um registro de registros de fluxo do AWS Transit Gateway que publique 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 AWS Transit Gateway 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 registros de registros de fluxo do AWS Transit Gateway

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 registros de fluxo do AWS Transit Gateway

É possível adicionar ou remover tags para um log de fluxo nos consoles do Amazon EC2 e da 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 registros de registros de fluxo do AWS Transit Gateway

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 AWS Transit Gateway

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 no AWS Transit Gateway

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 no AWS Transit Gateway.

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 no AWS Transit Gateway

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 de métrica do gateway de trânsito.

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 de AZ são publicadas na conta do proprietário do gateway de trânsito. As métricas de AZ individuais de um anexo também são publicadas na conta do proprietário do anexo. O proprietário do anexo só pode exibir as métricas por AZ de seu próprio anexo.

Todas as métricas são sempre relatadas. Seus valores dependem do tráfego que and/or sai do anexo do gateway de trânsito. Consulte as dimensões suportadas em Dimensões de métrica do gateway de trânsito.

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 de métrica do gateway de trânsito

Filtre os dados da métrica 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 da métrica por gateway de trânsito e por zona de disponibilidade.
`TransitGatewayAttachment`, `AvailabilityZone`	Filtra os dados da métrica por anexo do gateway de trânsito e por zona de disponibilidade.

Registre as chamadas da API AWS Transit Gateway usando AWS CloudTrail

AWS O Transit Gateway; está 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 Console de gerenciamento da AWS 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 contínuos para o bucket do Amazon S3 sem nenhum custo CloudTrail criando uma trilha. No entanto, há cobranças 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.

AWS O Transit Gateway registra todas as operações do plano de controle do Transit Gateway como eventos de gerenciamento. Para obter uma lista das operações do plano de controle do AWS Transit Gateway nas quais o Transit Gateway se conecta CloudTrail, consulte Ações do AWS Transit Gateway na Amazon EC2 API Reference.

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 em AWS Gateway de trânsito

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`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCreateTaggedTGWs",
            "Effect": "Allow",
            "Action": "ec2:CreateTransitGateway",
            "Resource": "arn:aws:ec2:us-east-1:123456789012:transit-gateway/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/stack": "prod"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "stack"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:us-east-1:123456789012: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`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteTransitGatewayRouteTable",
                "ec2:CreateTransitGatewayRouteTable"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1:123456789012: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/*"
```

```
        }
    ]
}
```

Use funções vinculadas a serviços para gateways de trânsito em AWS Gateway de trânsito

A Amazon VPC usa funções vinculadas a serviço para as permissões de que ela precisa para chamar outros serviços da AWS em seu nome. Para obter mais informações, consulte as Service-linkedfunções 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 AWSServiceRoleForVPCTransitGatewaypara 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 AWSServiceRoleForVPCTransitGatewayfunção confia nos seguintes serviços para assumir a função:

- `transitgateway.amazonaws.com`

AWSServiceRoleForVPCTransitGatewayusa a política gerenciadaAWSVPCTransitGatewayServiceRolePolicy.

É necessário configurar as permissões para permitir que uma entidade do IAM (como um usuário, grupo ou perfil) crie, edite ou exclua uma função vinculada ao serviço. Para obter mais informações, consulte as permissões de Service-linked função 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

É possível editar a descrição de 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 AWSServiceRoleForVPCTransitGatewayexclua.

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 perfis vinculados ao serviço. Para obter mais informações, consulte Excluir uma função vinculada ao serviço no Guia do usuário do IAM.

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

AWS políticas gerenciadas para gateways de trânsito em AWS Gateway de trânsito

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) é lançada ou novas operações de API são disponibilizadas para serviços existentes.

Para saber mais, consulte AWS Políticas gerenciadas pela no Guia 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: AWSVPCTransitGatewayServiceRolePolicy

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 AWS políticas 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	1.º de março de 2021

Alteração	Descrição	Data
	suas políticas AWS gerenciadas.	

ACLs de rede para gateways de trânsito em AWS Gateway de trânsito

Uma lista de controle de acesso à rede (NACL) é uma camada opcional de segurança.

As regras de lista de controle de acesso à rede (NACL) são aplicadas de forma diferente, dependendo do cenário:

- the section called “Mesma sub-rede para instâncias do EC2 e a associação do gateway de trânsito”
- the section called “Sub-redes diferentes para instâncias do EC2 e a associação do gateway de trânsito”

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

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

As regras de NACL são aplicadas da seguinte maneira para o tráfego das instâncias para o gateway de trânsito:

- As regras de saída usam o endereço IP de destino para avaliação.
- As regras de entrada usam o endereço IP de origem para avaliação.

As regras de NACL são aplicadas da seguinte maneira para o tráfego do gateway de trânsito para as instâncias:

- As regras de saída não são avaliadas.
- As regras de entrada não são avaliadas.

Sub-redes diferentes para instâncias do EC2 e a associação do gateway de trânsito

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

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

- As regras de saída usam o endereço IP de destino para avaliar o tráfego das instâncias para o gateway de trânsito.
- As regras de entrada usam o endereço IP de origem para avaliar o tráfego do gateway de trânsito para as instâncias.

As regras de NACL são aplicadas da seguinte maneira para a sub-rede do gateway de trânsito:

- As regras de saída usam o endereço IP de destino para avaliar o tráfego do gateway de trânsito para as instâncias.
- As regras de saída não são usadas para avaliar o tráfego das instâncias para o gateway de trânsito.
- As regras de entrada usam o endereço IP de origem para avaliar o tráfego das instâncias para o gateway de trânsito.
- As regras de entrada não são usadas para avaliar o tráfego do gateway de trânsito para as instâncias.

Melhores práticas

Use uma sub-rede separada para cada anexo da VPC do gateway. Para cada sub-rede, use um CIDR pequeno, por exemplo /28, para que você tenha mais endereços para recursos do EC2. Ao usar uma sub-rede separada, é possível configurar o seguinte:

- Mantenha aberta a NACL de entrada e saída associada às sub-redes do gateway de trânsito.
- Dependendo do fluxo de tráfego, é possível aplicar NACLs às sub-redes de workload.

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

AWS Cotas do Transit Gateway

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

Nome	Padrão	Ajustável
Gateways de trânsito por conta	5	Sim
Blocos CIDR por gateway de trânsito	5	Não

Os blocos CIDR são usados no recurso the section called “Anexos do Connect e pares do Connect”.

Roteamento

Nome	Padrão	Ajustável
Tabelas de rotas de gateway de trânsito por gateway de trânsito	20	Sim
Total de rotas combinadas (dinâmicas e estáticas) em todas as tabelas de rotas para um só gateway de trânsito	10.000	Entre em contato com seu arquiteto de soluções (SA) ou gerente técnico de

Nome	Padrão	Ajustável
		contas (TAM) para obter mais assistênc ia.
Rotas dinâmicas anunciadas por um dispositivo do roteador virtual para um par do Connect	1.000	Entre em contato com seu arquiteto de soluções (SA) ou gerente técnico de contas (TAM) para obter mais assistênc ia.
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.

Nome	Padrão	Ajustável
Anexos por gateway de trânsito	5.000	Sim
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

Nome	Padrão	Ajustável
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
Concentradores VPN por gateway de trânsito	5	Não
Conexões VPN por VPN Concentrator	100	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 Direct Connect , ou anexos do gateway de trânsito emparelhados, tentaremos fornecer largura de banda adicional além do valor padrão.

Nome	Padrão	Ajustável
Largura de banda por anexo de VPC por zona de disponibilidade	Até 100 Gbps em cada direção (ou seja, entrada de 100 Gbps e saída de 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

Nome	Padrão	Ajustável
		obter mais assistênc ia.
Largura de banda para conexão de Direct Connect gateway ou gateway de trânsito emparelhado por zona de disponibilidade disponível na região	Até 100 Gbps em cada direção (ou seja, entrada de 100 Gbps e saída de 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 (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 contas (TAM) para obter mais assistênc ia.
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 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.

Para limites de largura de banda e pacotes com túnel VPN, consulte a largura de banda e taxa de transferência da VPN.

Direct Connect gateways

Nome	Padrão	Ajustável
Direct Connect gateways por gateway de trânsito	20	Não
Gateways de trânsito por 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, 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 Path MTU Discovery, consulte Path MTU Discovery no Guia do usuário do Amazon VPC.

Multicast

> **Note**
>
> O multicast do Transit Gateway pode não ser adequado para transações de alta frequência ou aplicativos sensíveis ao desempenho. É muito recomendado analisar os seguintes limites de multicast. Entre em contato com sua equipe de conta ou de Solution Architect para obter uma análise detalhada de seus requisitos de desempenho.

Nome	Padrão	Ajustável
Número de domínios multicast por gateway de trânsito	20	Entre em contato com seu arquiteto de soluções (SA) ou gerente técnico de contas (TAM) para obter mais assistência.
Interfaces de rede multicast por gateway de trânsito	10.000	Entre em contato com seu arquiteto de soluções (SA) ou gerente técnico de contas (TAM) para obter mais assistência.
Associações de domínio de multicast por VPC	20	Entre em contato com seu arquiteto de soluções (SA) ou gerente técnico de contas (TAM) para obter mais assistência.

Nome	Padrão	Ajustável
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 (mais de 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 saber mais, 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 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 do Client VPN	Crie um anexo de Client VPN para conectar um gateway de trânsito a um endpoint de Client VPN.	20 de abril de 2026
Alocação flexível de custos	Configure políticas flexíveis de alocação de custos para controlar como os custos de processamento e transferência de dados são alocados em sua organização.	20 de novembro de 2025
Support de criptografia para gateways de trânsito	Gerenciando o suporte à criptografia em gateways de trânsito para impor a criptografia em trânsito para todo o tráfego.	20 de novembro de 2025
Anexos de funções de rede	Crie um anexo de função de rede para conectar diretamente um gateway de trânsito ao AWS Network Firewall.	16 de junho de 2025
Suporte para referência do grupo de segurança	Agora, é possível referenciar um grupo de segurança entre VPCs conectadas 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 parte do Guia do usuário do AWS Transit Gateway.	2 de dezembro de 2021
Anexos de emparelhamento	É possível criar uma conexão de emparelhamento com um transit gateway na mesma Região.	1º de dezembro de 2021
Transit Gateway Connect	Você pode estabelecer uma conexão entre um gateway de 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 oferece suporte ao roteamento de tráfego multicast entre sub-redes de VPCs anexadas e serve como um roteador multicast para instâncias que enviam tráfego destinado a várias instâncias de recebimento.	3 de dezembro de 2019
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 Direct Connect gateway para conectar sua Direct Connect conexão por meio de uma interface virtual de trânsito às VPCs ou VPNs conectadas ao seu gateway de trânsito.	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.