AWS Transit Gateway

Amazon VPC

Amazon VPC: AWS Transit Gateway

Table of Contents

Was ist AWS Transit Gateway für Amazon VPC?

AWS Transit Gateway ist ein Netzwerk-Transit-Hub, der zur Verbindung von virtuellen privaten Clouds (VPCs) und lokalen Netzwerken verwendet wird. Da Ihre Cloud-Infrastruktur weltweit expandiert, verbindet regionsübergreifendes Peering Transit-Gateways mithilfe der globalen Infrastruktur miteinander. AWS Der gesamte Netzwerkverkehr zwischen AWS -Rechenzentren wird automatisch auf der physischen Ebene verschlüsselt.

Weitere Informationen finden Sie auf der AWS Transit Gateway-Website.

Transit-Gateway-Konzepte

Die wichtigsten Konzepte für Transit Gateways sind folgende:

- Anhänge – Sie können Folgendes anhängen:
  - Eine oder mehrere VPCs
  - Eine SD-WAN/third-party Connect-Netzwerk-Appliance
  - Ein AWS Direct Connect Gateway
  - Eine Peering-Verbindung zu einem anderen Transit Gateway
  - Eine VPN-Verbindung zu einem Transit Gateway
  - Ein VPN-Konzentrator zu einem Transit-Gateway
  - Ein Client-VPN-Endpunkt zu einem Transit-Gateway
  - Ein Anhang mit einer Netzwerkfunktion. Weitere Informationen finden Sie unter the section called “Anlagen für Netzwerkfunktionen”.
- Maximale Transit-Gateway-Übertragungseinheit (MTU) – Die maximale Übertragungseinheit (MTU) einer Netzwerkverbindung ist die Größe (in Byte) des größten zulässigen Datenpakets, das über die Verbindung übermittelt werden kann. Je größer die MTU einer Verbindung, desto mehr Daten können in einem einzelnen Paket übergeben werden. Ein Transit-Gateway unterstützt eine MTU von 8500 Byte für den Verkehr zwischen VPCs Direct Connect, Transit Gateway Connect und Peering-Anhängen (regionsinterne, regionsübergreifende und Cloud-WAN-Peering-Anhänge). Datenverkehr über VPN-Verbindungen kann eine MTU von 1 500 Byte haben.
- Verschlüsselungssteuerung — Ein Transit-Gateway kann so konfiguriert werden, dass es die Verschlüsselungssteuerung unterstützt, die Verschlüsselung während der Übertragung für den gesamten Datenverkehr auf VPCs erzwingt, die an das Transit-Gateway angeschlossen

sind. Wenn die Verschlüsselungssteuerung aktiviert ist, kann das Transit-Gateway an VPCs angeschlossen werden, wobei die Verschlüsselungskontrolle erzwungen wird. Diese Funktion stellt sicher, dass der gesamte Datenverkehr, der über das Transit-Gateway fließt, verschlüsselt wird, wodurch die Sicherheit Ihrer Netzwerkkommunikation erhöht wird.

- Transit-Gateway-Routing-Tabelle – Ein Transit Gateway verfügt über eine Standard-Routing-Tabelle und optional über zusätzliche Routing-Tabellen. Eine Routing-Tabelle umfasst dynamische und statische Routen, die den nächsten Hop basierend auf der Ziel-IP-Adresse des Pakets bestimmen. Das Ziel dieser Routen kann ein beliebiger Transit-Gateway-Anhang sein. Standardmäßig sind Transit-Gateway-Anhänge mit der standardmäßigen Transit-Gateway-Routing-Tabelle verknüpft.
- Zuordnungen: Jeder Anhang ist immer genau einer Routing-Tabelle zugeordnet. Routing-Tabellen können keiner, aber auch mehreren Anhängen zugeordnet sein.
- Routing-Verteilung – Eine VPC oder VPN-Verbindung oder ein Direct-Connect-Gateway kann Routen dynamisch auf eine Transit-Gateway-Routing-Tabelle übertragen. Bei einem Connect-Anhang werden die Routen standardmäßig an eine Transit-Gateway-Routing-Tabelle weitergegeben. Im Falle einer VPC müssen Sie statische Routen erstellen, um Datenverkehr an das Transit-Gateway zu senden. Im Falle einer VPN-Verbindung werden Routen unter Verwendung des Border Gateway Protocol (BGP) vom Transit-Gateway auf Ihren On-Premises-Router übertragen. Bei einem Direct-Connect-Gateway werden die zulässigen Präfixe mithilfe von BGP auf Ihren On-Premises-Router übertragen. Bei einem Peering-Anhang müssen Sie in der Routing-Tabelle des Transit Gateways eine statische Route erstellen, um auf den Peering-Anhang zu verweisen.

Erste Schritte mit Transit Gateways

Verwenden Sie die folgenden Ressourcen, um ein Transit Gateway zu erstellen und zu verwenden.

- Funktionsweise von Transit Gateways
- Beginnen Sie mit Transit Gateways
- Bewährte Methoden für das Design

Arbeiten mit Transit Gateways

Sie können Ihre Transit-Gateway-Ressourcen über die folgenden Schnittstellen erstellen und verwalten:

- AWS-Managementkonsole – Bietet eine Webschnittstelle für den Zugriff auf Ihre Transit Gateways.
- AWS Befehlszeilenschnittstelle (AWS CLI) — Stellt Befehle für eine Vielzahl von AWS Diensten bereit, einschließlich Amazon VPC, und wird unter Windows, macOS und Linux unterstützt. Weitere Informationen finden Sie unter AWS Command Line Interface.
- AWS SDKs — Stellt sprachspezifische API-Operationen bereit und kümmert sich um viele Verbindungsdetails, wie z. B. die Berechnung von Signaturen, die Bearbeitung von Wiederholungsversuchen von Anfragen und die Behandlung von Fehlern. Weitere Informationen finden Sie unter AWS -SDKs.
- Abfrage-API – Bietet API-Aktionen auf niedriger Ebene, die Sie mithilfe von HTTPS-Anforderungen aufrufen. Die Verwendung der Abfrage-API ist die direkteste Möglichkeit für den Zugriff auf die Amazon VPC. Allerdings müssen dann viele technische Abläufe, wie beispielsweise das Erzeugen des Hashwerts zum Signieren der Anforderung und die Fehlerbehandlung in der Anwendung durchgeführt werden. Weitere Informationen finden Sie in der Amazon-EC2-API-Referenz.

Preisgestaltung

Jeder Anhang an ein Transit Gateway wird Ihnen stündlich berechnet, und Ihnen wird der auf dem Transit Gateway verarbeitete Datenverkehr in Rechnung gestellt. Standardmäßig werden die Datenverarbeitungsgebühren dem Konto zugewiesen, dem der Quellanhang gehört. Mithilfe der flexiblen Kostenzuweisung können Sie die Zuweisung dieser Gebühren an Ihre Unternehmensanforderungen anpassen. Weitere Informationen finden Sie unter Preise für AWS Transit Gateway undFlexible Kostenverteilung.

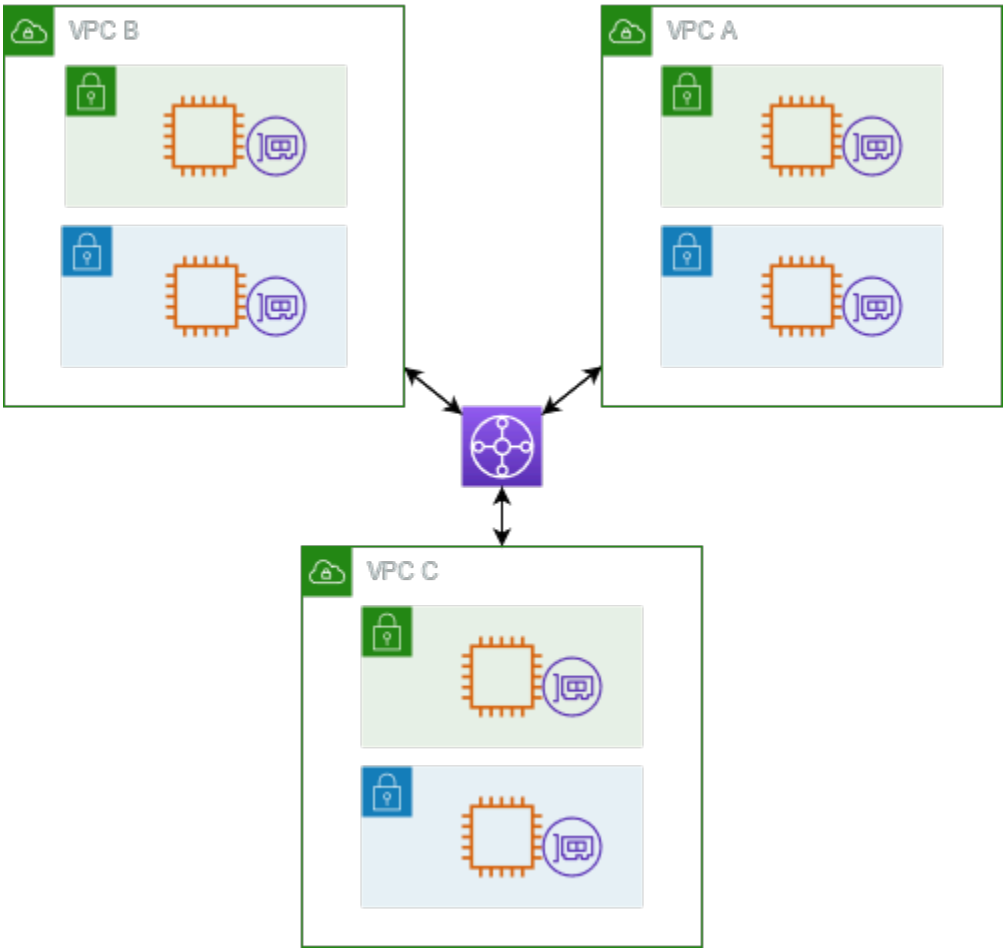
So funktioniert AWS Transit Gateway

In AWS Transit Gateway fungiert ein Transit-Gateway als regionaler virtueller Router für den Datenverkehr zwischen Ihren Virtual Private Clouds (VPCs) und lokalen Netzwerken. Ein Transit Gateway wird basierend auf dem Volumen an Netzwerkdatenverkehr elastisch skaliert. Das Routing über ein Transit-Gateway erfolgt auf Ebene 3, wo die Pakete auf der Grundlage der Ziel-IP-Adressen an einen bestimmten Next-Hop-Anhang gesendet werden.

Topics

Beispiel für ein Architekturdiagramm

Im folgenden Diagramm ist ein Transit Gateway mit drei VPC-Anhängen abgebildet. Die Routentabelle für jede dieser VPCs enthält die lokale Route und Routen, die den für die anderen beiden VPCs bestimmten Datenverkehr an das Transit-Gateway senden.



Im Folgenden finden Sie ein Beispiel für eine Standard-Transit-Gateway-Routing-Tabelle für die im vorherigen Diagramm gezeigten Anhänge. Die CIDR-Blöcke für jede VPC werden an die Routing-Tabelle übertragen. Daher kann jeder Anhang Pakete an die beiden anderen Anhänge weiterleiten.

Bestimmungsort	Ziel	Routing-Typ
VPC A CIDR	*Attachment for VPC A*	verbreitet
VPC B CIDR	*Attachment for VPC B*	verbreitet
VPC C CIDR	*Attachment for VPC C*	verbreitet

Ressourcen-Anhänge

Ein Transit-Gateway-Anhang ist sowohl eine Quelle als auch ein Ziel für Pakete. Sie können die folgenden Ressourcen an Ihr Transit-Gateway anhängen:

- Eine oder mehrere VPCs. AWS Transit Gateway stellt eine elastic network interface innerhalb von VPC-Subnetzen bereit, die dann vom Transit-Gateway verwendet wird, um den Verkehr zu und von den ausgewählten Subnetzen weiterzuleiten. Sie müssen mindestens ein Subnetz für jede Availability Zone haben, das es dann ermöglicht, Datenverkehr an Ressourcen in jedem Subnetz dieser Zone weiterzuleiten. Während der Anhangserstellung können Ressourcen innerhalb einer bestimmten Availability Zone nur dann ein Transit Gateway erreichen, wenn ein Subnetz innerhalb derselben Zone aktiviert ist. Wenn eine Subnetz-Routing-Tabelle eine Route zum Transit Gateway enthält, wird der Datenverkehr nur dann an das Transit Gateway weitergeleitet, wenn das Transit Gateway einen Anhang im Subnetz derselben Availability Zone hat.
- Eine oder mehrere VPN-Verbindungen
- Ein oder mehrere VPN-Konzentratoren
- Ein oder mehrere Gateways AWS Direct Connect
- Eine oder mehrere Transit-Gateway-Connect-Anhänge
- Eine oder mehrere Transit-Gateway-Peering-Verbindungen

Mehrpfad-Routing zu gleichen Kosten

AWS Transit Gateway unterstützt Equal Cost Multipath (ECMP) -Routing für die meisten Anlagen. Für einen VPN-Anhang können Sie die ECMP-Unterstützung mithilfe der Konsole aktivieren oder deaktivieren, wenn Sie ein Transit Gateway erstellen oder ändern. Für alle anderen Anhangstypen gelten die folgenden ECMP-Einschränkungen:

- VPC – VPC unterstützt ECMP nicht, da sich CIDR-Blöcke nicht überschneiden können. Sie können beispielsweise keine VPC mit einem CIDR 10.1.0 anhängen. 0/16 mit einer zweiten VPC, die dasselbe CIDR für ein Transit-Gateway verwendet, und richten Sie dann das Routing ein, um den Datenverkehr zwischen ihnen auszurichten.
- VPN – Wenn die Option VPN-ECMP-Unterstützung deaktiviert ist, verwendet ein Transit Gateway interne Metriken, um den bevorzugten Pfad zu ermitteln, falls gleiche Präfixe über mehrere Pfade verteilt sind. Weitere Informationen zum Aktivieren oder Deaktivieren von ECMP für einen VPN-Anhang finden Sie unter the section called “Transit Gateways”.
- AWS Transit Gateway AWS Transit Gateway Connect — Connect-Anlagen unterstützen automatisch ECMP.
- AWS Direct Connect AWS Direct Connect Gateway — Gateway-Anhänge unterstützen ECMP automatisch für mehrere Direct Connect Gateway-Anhänge, wenn Netzwerkpräfix, Präfixlänge und AS_PATH exakt identisch sind.

- Transit-Gateway-Peering – Transit-Gateway-Peering unterstützt ECMP nicht, da es weder dynamisches Routing unterstützt noch Sie dieselbe statische Route für zwei verschiedene Ziele konfigurieren können.
- VPN Concentrator — VPN Concentrator unterstützt ECMP nicht.

> **Note**
>
> - BGP Multipath AS-Path Relax wird nicht unterstützt, sodass Sie ECMP nicht über verschiedene autonome Systemnummern (ASNs) verwenden können.
> - ECMP wird zwischen verschiedenen Anhangstypen nicht unterstützt. Beispielsweise können Sie ECMP nicht zwischen einer VPN und einem VPC-Anhang aktivieren. Stattdessen werden Transit-Gateway-Routen ausgewertet und der Datenverkehr entsprechend der ausgewerteten Route weitergeleitet. Weitere Informationen finden Sie unter the section called “Reihenfolge der Routenauswertung”.
> - Ein einziges Direct Connect-Gateway unterstützt ECMP über mehrere virtuelle Transitschnittstellen. Daher empfehlen wir, nur ein einziges Direct Connect-Gateway einzurichten und zu verwenden und nicht mehrere Gateways einzurichten und zu verwenden, um ECMP nutzen zu können. Weitere Informationen zu Direct Connect-Gateways und öffentlichen virtuellen Schnittstellen finden Sie unter Wie richte ich eine Active/Active oder Active/Passive Direct Connect-Verbindung AWS von einer öffentlichen virtuellen Schnittstelle aus ein? .

Verfügbarkeitszonen

Wenn Sie einem Transit Gateway eine VPC anhängen, müssen Sie eine oder mehrere Availability Zones aktivieren, die das Transit Gateway für die Weiterleitung des Datenverkehrs zu Ressourcen in den VPC-Subnetzen verwenden wird. Zur Aktivierung der einzelnen Availability Zones geben Sie genau ein Subnetz an. Das Transit Gateway platziert unter Verwendung einer IP-Adresse aus dem Subnetz eine Netzwerkschnittstelle in diesem Subnetz. Nachdem Sie eine Availability Zone durch Angabe eines Subnetzes aktiviert haben, kann der Datenverkehr an alle Subnetze in dieser Availability Zone weitergeleitet werden, nicht nur an das von Ihnen angegebene. Allerdings können nur Ressourcen in Availability Zones mit Transit-Gateway-Anhang das Transit Gateway erreichen.

Wenn der Verkehr aus einer Availability Zone stammt, in der sich der Zielanhang nicht befindet, leitet AWS Transit Gateway diesen Datenverkehr intern an eine zufällige Availability Zone weiter, in der

der Anhang vorhanden ist. Für diese Art von Verkehr in der gesamten Availability Zone fallen keine zusätzlichen Transit-Gateway-Gebühren an.

Zur Sicherstellung der Verfügbarkeit sollten Sie mehrere Availability Zones aktivieren.

Verwenden des Applicance-Modus-Supports

Wenn Sie eine zustandsbehaftete Netzwerk-Appliance in Ihrer VPC konfigurieren möchten, können Sie die Unterstützung des Appliance-Modus für diese VPC-Anhänge, in welcher sich die Appliance befindet, aktivieren. Dadurch wird sichergestellt, dass das Transit Gateway während der gesamten Lebensdauer eines Verkehrsflusses zwischen Quelle und Ziel dieselbe Availability Zone für diese VPC-Anhänge verwendet. Dies ermöglicht dem Transit Gateway auch, Datenverkehr an jede Availability Zone in der VPC zu senden, solange in dieser Availability Zone eine Subnetz-Zuordnung vorhanden ist. Weitere Informationen finden Sie unter Beispiel: Appliance in einer VPC mit freigegeben Services.

Routing

Ihr Transit Gateway leitet IPv4- und IPv6-Pakete mithilfe von Transit-Gateway-Routing-Tabellen zwischen Anhängen weiter. Sie können diese Routing-Tabellen konfigurieren, damit Routen aus den Routing-Tabellen für die angehängten VPCs, VPN-Verbindungen und Direct Connect-Gateways propagiert werden. Sie können den Transit-Gateway-Routing-Tabellen auch statische Routen hinzufügen. Wenn ein Paket von einem Anhang ankommt, wird es anhand der Route, die seiner Ziel-IP-Adresse entspricht, an einen anderen Anhang weitergeleitet.

Für Transit-Gateway-Peering-Anhänge werden nur statische Routen unterstützt.

Themen zur Weiterleitung

- Routing-Tabellen
- Routing-Tabellenzuordnung
- Routing-Propagierung
- Routen für Peering-Anhänge
- Reihenfolge der Routenauswertung

Routing-Tabellen

Ihr Transit Gateway verfügt automatisch über eine Standard-Routing-Tabelle. Diese Routing-Tabelle wird standardmäßig als Standard-Zuordnungs-Routing-Tabelle und standardmäßige

Route-Propagierung-Tabelle verwendet. Wenn Sie sowohl die Route-Propagierung als auch die Zuordnung von Routing-Tabellen deaktivieren, AWS wird keine Standard-Routing-Tabelle für das Transit-Gateway erstellt. Wenn jedoch entweder die Route-Propagierung oder die Route-Tabellenverknüpfung aktiviert ist, AWS wird eine Standard-Routing-Tabelle erstellt.

Sie können zusätzliche Routing-Tabellen für Ihr Transit Gateway erstellen. Auf diese Weise können Sie Teilmengen von Anhängen isolieren. Jeder Anhang kann einer Routing-Tabelle zugeordnet sein. Ein Anhang kann ihre Routen an eine oder mehrere Routing-Tabelle propagieren.

Sie können eine Blackhole-Route in Ihrer Transit-Gateway-Routing-Tabelle erstellen, die den Datenverkehr unterbricht, der der Route entspricht.

Wenn Sie einem Transit Gateway eine VPC anhängen, müssen Sie der Subnetz-Routing-Tabelle eine Route hinzufügen, damit der Datenverkehr über das Transit Gateway weitergeleitet wird. Weitere Informationen finden Sie unter Routing für ein Transit Gateway im Amazon-VPC-Benutzerhandbuch.

Routing-Tabellenzuordnung

Ein Transit-Gateway-Anhang kann einer einzigen Routing-Tabelle zugeordnet werden. Jede Routing-Tabelle kann keiner, aber auch mehreren Anhängen zugeordnet werden und Pakete an Anhänge oder andere Routing-Tabellen weiterleiten.

Routing-Propagierung

Jeder Anhang bietet Routen, die in einer oder mehreren Transit-Gateway-Routing-Tabellen installiert werden können. Wenn ein Anhang auf eine Transit-Gateway-Routing-Tabelle übertragen wird, werden diese Routen in der Routing-Tabelle installiert. Sie können nicht nach angekündigten Routen filtern.

Bei einem VPC-Anhang werden die CIDR-Blöcke der VPC an die Routing-Tabelle des Transit Gateways weitergegeben.

Wenn dynamisches Routing mit einem VPN-Anhang, einem VPN Concentrator-Anhang oder einem Direct Connect-Gateway-Anhang verwendet wird, können Sie die vom lokalen Router gelernten Routen über BGP an jede der Transit-Gateway-Routentabellen weitergeben.

Wenn dynamisches Routing mit einem VPN-Anhang oder einem VPN Concentrator-Anhang verwendet wird, werden die Routen in der Routentabelle, die dem VPN-Anhang oder dem VPN Concentrator-Anhang zugeordnet sind, dem Kunden-Gateway über BGP angekündigt.

Bei einem Connect-Anhang werden Routen in der Routentabelle, die dem Connect-Anhang zugeordnet ist, den virtuellen Appliances von Drittanbietern, z. B. SD-WAN Appliances, die in einer VPC über BGP ausgeführt werden, angekündigt.

Bei einem Direct Connect-Gateway-Anhang steuern zulässige Präfixe, von welchen Routen aus das Kundennetzwerk angekündigt wird. AWS

Wenn eine statische Route und eine propagierte Route das gleiche Ziel haben, hat die statische Route die höhere Priorität, sodass die propagierte Route nicht in der Routing-Tabelle enthalten ist. Wenn Sie die statische Route entfernen, wird die überlappende propagierte Route in die Routing-Tabelle aufgenommen.

Routen für Peering-Anhänge

Sie können für zwei Transit Gateways Peering durchführen und den Verkehr zwischen ihnen weiterleiten. Dazu erstellen Sie einen Peering-Anhang auf Ihrem Transit Gateway und geben das Peer-Transit-Gateway an, mit dem die Peering-Verbindung erstellt werden soll. Anschließend erstellen Sie eine statische Route in der Transit-Gateway-Routing-Tabelle, um Datenverkehr an den Transit-Gateway-Peering-Anhang weiterzuleiten. Datenverkehr, der an das Peer-Transit-Gateway weitergeleitet wird, kann dann an die VPC- und VPN-Anhänge für das Peer-Transit-Gateway weitergeleitet werden.

Weitere Informationen finden Sie unter Beispiel: Per Peering verbundene Transit Gateways.

Reihenfolge der Routenauswertung

Transit-Gateway-Routen werden in der folgenden Reihenfolge ausgewertet:

- die spezifischste Route für die Zieladresse.
- Für Routen mit demselben CIDR, aber von unterschiedlichen Anhangstypen, lautet die Routenpriorität wie folgt:
  - Statische Routen (z. B. statische Site-to-Site VPN-Routen)
  - Präfixlisten referenzierter Routen
  - VPC-propagated Routen
  - Vom Direct Connect-Gateway weitergeleitete Routen
  - Transit Gateway Connect-propagated Gateway-Strecken
  - Site-to-Site VPN über private direkte Connect-propagated Routen

- Site-to-Site VPN-propagated Routen
- Site-to-Site VPN-Concentrator propagierte Routen
- Client VPN weitergeleitete Routen
- Per Peering-Übertragung übertragene Transit Gateway Gateway-Routen (Cloud WAN)

Einige Anlagen unterstützen Routenwerbung über BGP. Bei Routen mit demselben CIDR und demselben Anhangstyp wird die Routenpriorität durch BGP-Attribute gesteuert:

- Kürzere AS-Pfadlänge
- Niedrigerer MED-Wert
- eBGP- statt iBGP-Routen werden bevorzugt, wenn der Anhang dies unterstützt

> **Important**
>
> - AWS kann keine konsistente Reihenfolge der Routenpriorisierung für BGP-Routen mit demselben CIDR, demselben Anhangstyp und denselben BGP-Attributen wie oben aufgeführt garantieren.
> - Für Routen, die einem Transit-Gateway ohne MED angekündigt werden, weist AWS Transit Gateway die folgenden Standardwerte zu:
>   - 0 für eingehende Routen, die in Direct Connect-Anhängen angekündigt werden.
>   - 100 für eingehende Routen, die in VPN- und Connect-Anhängen beworben werden.

AWS Transit Gateway zeigt nur eine bevorzugte Route an. Eine Backup-Route wird nur dann in der Routentabelle des Transit-Gateways angezeigt, wenn die zuvor aktive Route nicht mehr angekündigt wird — zum Beispiel, wenn Sie dieselben Routen über das Direct Connect-Gateway und über Site-to-Site VPN ankündigen. AWS Transit Gateway zeigt nur die Routen an, die von der Direct Connect-Gateway-Route empfangen wurden, was die bevorzugte Route ist. Das Site-to-Site VPN, die Backup-Route, wird nur angezeigt, wenn das Direct Connect-Gateway nicht mehr beworben wird.

Unterschiede in der Routentabelle von VPC und Transit Gateway

Die Auswertung von Routentabellen unterscheidet sich je nachdem, ob Sie eine VPC-Routentabelle oder eine Transit-Gateway-Routentabelle verwenden.

Das folgende Beispiel zeigt eine VPC-Routentabelle. Die lokale VPC-Route hat höchste Priorität, gefolgt von den Routen, die am spezifischsten sind. Wenn eine statische und eine propagierte Route dasselbe Ziel haben, hat die statische Route eine höhere Priorität.

Zielbereich	Ziel	Priorität
10.0.0. 0/16	local	1
192,168,0. 0/16	pcx-12345	2
172,31,0. 0/16	vgw-12345 (statisch) oder tgw-12345 (statisch)	2
172,31,0. 0/16	vgw-12345 (propagiert)	3
0,0.0. 0/0	igw-12345	4

Das folgende Beispiel zeigt eine Transit-Gateway-Routentabelle. Wenn Sie den Direct Connect -Gateway-Anhang vor dem VPN-Anhang verwenden möchten, verwenden Sie eine BGP-VPN-Verbindung und propagieren Sie die Routen in der Transit-Gateway-Routing-Tabelle.

Zielbereich	Anhang (Ziel)	Ressourcentyp	Routing-Typ	Priorität
10.0.0. 0/16	tgw-attach-123 | vpc-1234	VPC	Statisch oder propagiert	1
192,168,0. 0/16	tgw-attach-789 | vpn-5678	VPN	Statisch	2
172,31,0. 0/16	tgw-attach-456 | dxgw_id	Direct Connect Gateway	Propagiert	3
172,31,0. 0/16	tgw-attach-789 | tgw-connect-peer-123	Verbinden	Propagiert	4
172,31,0. 0/16	tgw-attach-789 | vpn-5678	VPN	Propagiert	5

Anlagen für Netzwerkfunktionen

Ein Netzwerkfunktionsanhang ist eine Ressource, die eine Netzwerksicherheitsfunktion — z. B. eine AWS Network Firewall Anlage — direkt mit Ihrem Transit-Gateway verbindet. Dadurch entfällt die Notwendigkeit, Inspektions-VPCs manuell zu erstellen und zu verwalten.

Mit einem Anschluss an eine Netzwerkfunktion:

- AWS erstellt und verwaltet automatisch die zugrundeliegende Infrastruktur
- Der Verkehr kann überprüft werden, während er durch Ihr Transit-Gateway fließt
- Sicherheitsrichtlinien werden in Ihrem gesamten Netzwerk einheitlich angewendet

- Sie können den Datenverkehr mithilfe einfacher Routing-Regeln durch die Firewall leiten
- Der Anhang funktioniert in mehreren Availability Zones und sorgt so für hohe Verfügbarkeit

Diese Integration vereinfacht die Netzwerksicherheit, da Sie Firewalls direkt an Ihr Transit-Gateway anschließen können, anstatt komplexe Routing-Konfigurationen zu erstellen und separate Endpunkte über separate VPCs zu verwalten.

AWS Network Firewall Integration

AWS Network Firewall Die Integration ermöglicht es Ihnen, eine Firewall in Form einer Gruppe von Gateway Load Balancer-Endpunkten, einen pro Availability Zone, in einer vom Service verwalteten Puffer-VPC zu verbinden. Ein Netzwerk-Firewall-Anhang wird erstellt, wobei der Appliance-Modus automatisch aktiviert ist. Dadurch entfällt die Notwendigkeit, Inspektions-VPCs explizit zu verwalten.

Dank der Netzwerk-Firewall-Integration müssen Sie keine Inspektions-VPCs mehr für Ihre Netzwerk-Firewall-Bereitstellungen erstellen und verwalten. Anstatt bei der Erstellung Ihrer Firewall eine VPC und Subnetze auszuwählen, wählen Sie direkt das Transit Gateway aus, das AWS automatisch alle erforderlichen Ressourcen im Hintergrund bereitstellt und verwaltet. Sie werden einen neuen Transit-Gateway-Netzwerkfunktionsanhang anstelle eines einzelnen Firewall-Endpunkts sehen.

In kontenübergreifenden Szenarien kann das Transit Gateway RAM-shared vom Transit Gateway-Besitzer zum Netzwerk-Firewall-Besitzerkonto übertragen werden, sodass jedes Konto den Firewall-Anhang verwalten kann. Sobald Ihre Firewall und Ihr Anhang bereit sind, können Sie einfach Ihre Transit Gateway Gateway-Routentabellen ändern, um den Verkehr zur Überprüfung an den Anhang zu senden.

> **Note**
>
> - Transit Gateway unterstützt nur statisches Routing für Netzwerkfirewall-Anlagen.
> - Third-party Firewalls werden nicht unterstützt.

Weitere Informationen zu Firewalls und Anhängen finden Sie in den Anhängen zu den Netzwerkfunktionen des Transit-Gateways.

Beispiele für Transit-Gateway-Szenarien

Die folgenden Szenarien sind gängige Anwendungsfälle für Transit-Gateways. Ihre Transit Gateways sind nicht auf diese Anwendungsfälle beschränkt.

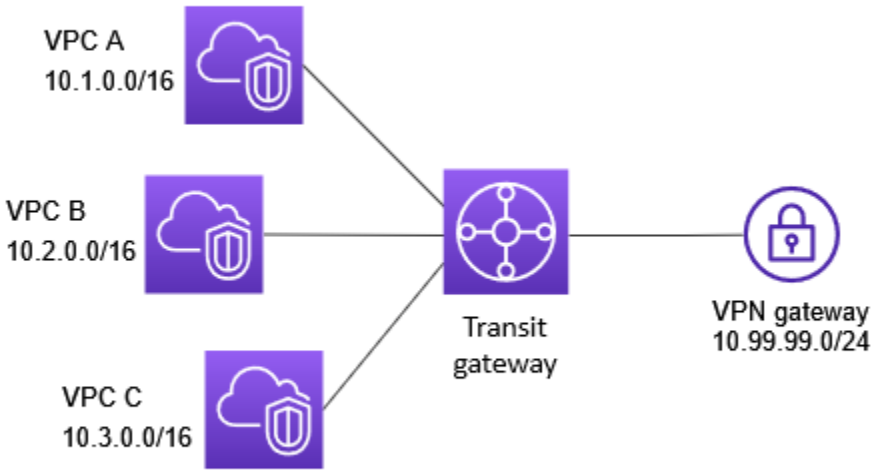
Beispiel: Zentralisierter Router

Sie können Ihr Transit-Gateway als zentralen Router konfigurieren, der alle Ihre VPCs und Site-to-Site VPN-Verbindungen verbindet. AWS Direct Connect In diesem Szenario sind alle Anhänge der standardmäßigen Transit-Gateway-Routing-Tabelle zugeordnet und propagieren an die standardmäßige Transit-Gateway-Routing-Tabelle. Daher können alle Anhänge Pakete untereinander weiterleiten, wobei das Transit Gateway dient als einfacher Layer-3-IP-Router dient.

Inhalt

-Übersicht

Die folgende Abbildung zeigt die Hauptkomponenten der Konfiguration für dieses Szenario. In diesem Szenario gibt es drei VPC-Anhänge und einen Site-to-Site VPN-Anhang zum Transit-Gateway. Pakete aus den Subnetzen in VPC A, VPC B und VPC C, die für ein Subnetz in einer anderen VPC oder für die VPN-Verbindung bestimmt sind, werden zuerst an das Transit Gateway gesendet.



Ressourcen

Erstellen Sie die folgenden Ressourcen für dieses Szenario:

- Drei VPCs. Weitere Informationen finden Sie unter VPC erstellen im Amazon-VPC-Benutzerhandbuch.
- Ein Transit Gateway. Weitere Informationen finden Sie unter the section called “Erstellen eines Transit-Gateways”.
- Drei VPC-Anhänge im Transit Gateway. Weitere Informationen finden Sie unter the section called “Erstellen Sie einen VPC-Anhang”.
- Ein Site-to-Site VPN-Anhang am Transit-Gateway. Die CIDR-Blöcke für jede VPC werden an die Transit-Gateway-Routing-Tabelle übertragen. Wenn die VPN-Verbindung hergestellt ist, wird die BGP-Sitzung eingerichtet und das Site-to-Site VPN-CIDR wird an die Transit-Gateway-Routentabelle weitergegeben, und die VPC-CIDRs werden der BGP-Tabelle des Kunden-Gateways hinzugefügt. Weitere Informationen finden Sie unter the section called “Erstellen eines Transit-Gateway-Anhangs an ein VPN”.

  Überprüfen Sie die Anforderungen für Ihr Kunden-Gateway-Gerät im AWS Site-to-Site VPN - Benutzerhandbuch.

Routing

Jede VPC hat eine Routing-Tabelle und es ist eine Routing-Tabelle für das Transit Gateway vorhanden.

VPC-Routing-Tabellen

Jede VPC hat eine Routing-Tabelle mit 2 Einträgen. Der erste Eintrag ist der Standardeintrag für lokales IPv4-Routing in der VPC; dieser Eintrag befähigt die Instances in dieser VPC miteinander zu kommunizieren. Der zweite Eintrag leitet den gesamten anderen IPv4-Subnetz-Datenverkehr an das Transit Gateway weiter. Die folgende Tabelle zeigt die VPC-A-Routen.

Zielbereich	Target
10.1.0. 0/16	local
0,0.0. 0/0	tgw-id

Routing-Tabelle für Transit Gateway

Folgendes ist ein Beispiel für eine Standard-Routing-Tabelle für die Anhänge aus der vorherigen Grafik. Die Routing-Verbreitung ist aktiviert.

Zielbereich	Ziel	Routing-Typ
10.1.0. 0/16	*Attachment for VPC A*	verbreitet
10.2.0. 0/16	*Attachment for VPC B*	verbreitet
10.3.0. 0/16	*Attachment for VPC C*	verbreitet
10,99,99. 0/24	*Attachment for VPN connection*	verbreitet

Kunden-Gateway-BGP-Tabelle

Die Kunden-Gateway-BGP-Tabelle enthält die folgenden VPC-CIDRs.

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

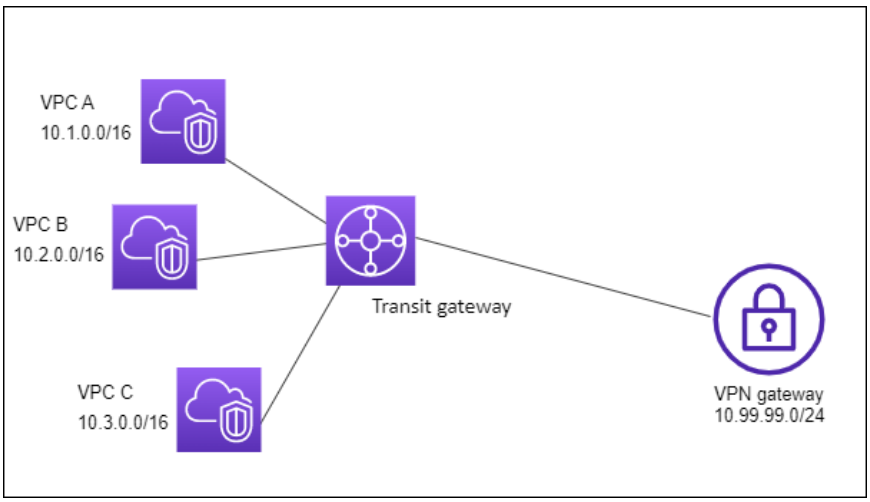
Beispiel: Isolierte VPCs

Sie können Ihr Transit-Gateway als mehrere isolierte Router konfigurieren. Dies gleicht der Verwendung mehrerer Transit-Gateways, bietet aber mehr Flexibilität, falls sich die Routen und Anfügungen ändern. In diesem Szenario verfügt jeder isolierte Router über eine einzige Routing-Tabelle. Alle Anfügungen, die diesem isolierten Router zugeordnet sind, verbreiten mit seiner Routing-Tabelle und werden ihr zugeordnet. Die Anfügungen, die einem isolierten Router zugeordnet sind, können Pakete untereinander weiterleiten. Sie können aber keine Pakete an Anfügungen eines anderen isolierten Routers leiten oder Pakete von ihnen empfangen.

Inhalt

-Übersicht

Die folgende Abbildung zeigt die Hauptkomponenten der Konfiguration für dieses Szenario. Pakete von VPC A, VPC B und VPC C werden an das Transit-Gateway weitergeleitet. Pakete aus den Subnetzen in VPC A, VPC B und VPC C, die das Internet als Ziel haben, werden zuerst durch das Transit-Gateway und dann zur Site-to-Site VPN-Verbindung weitergeleitet (wenn sich das Ziel innerhalb dieses Netzwerks befindet). Pakete von einer VPC, die als Ziel ein Subnetz in einer anderen VPC haben, z. B. von 10.1.0.0 nach 10.2.0.0, werden über das Transit-Gateway weitergeleitet, wo sie blockiert werden, da für sie keine Route in der Transit-Gateway-Routing-Tabelle vorhanden ist.



Ressourcen

Erstellen Sie die folgenden Ressourcen für dieses Szenario:

- Drei VPCs. Weitere Informationen finden Sie unter VPC erstellen im Amazon-VPC-Benutzerhandbuch.
- Ein Transit Gateway. Weitere Informationen finden Sie unter the section called “Erstellen eines Transit-Gateways”.
- Drei Anfügungen im Transit-Gateway für die drei VPCs. Weitere Informationen finden Sie unter the section called “Erstellen Sie einen VPC-Anhang”.
- Ein Site-to-Site VPN-Anhang auf dem Transit-Gateway. Weitere Informationen finden Sie unter the section called “Erstellen eines Transit-Gateway-Anhangs an ein VPN”. Überprüfen Sie die Anforderungen für Ihr Kunden-Gateway-Gerät im AWS Site-to-Site VPN -Benutzerhandbuch.

Wenn die VPN-Verbindung besteht, wird die BGP-Sitzung hergestellt und das VPN-CIDR wird auf die Transit-Gateway-Routing-Tabelle übertragen. Die VPC-CIDRs werden dann der BGP-Kunden-Gateway-Tabelle hinzugefügt.

Routing

Jede VPC verfügt über eine Routing-Tabelle, und das Transit-Gateway über zwei Routing.Tabellen – eine für die VPCs und eine für die VPN-Verbindung.

Routing-Tabellen VPC A, VPC B und VPC C

Jede VPC hat eine Routing-Tabelle mit 2 Einträgen. Der erste Eintrag ist der Standardeintrag für das lokale IPv4-Routing innerhalb der VPC. Dieser Eintrag ermöglicht es den Instances in dieser

VPC, miteinander zu kommunizieren. Der zweite Eintrag leitet den gesamten anderen IPv4-Subnetz-Datenverkehr an das Transit Gateway weiter. Die folgende Tabelle zeigt die VPC-A-Routen.

Zielbereich	Target
10.1.0. 0/16	local
0,0.0. 0/0	tgw-id

Transit-Gateway-Routing-Tabellen

In diesem Szenario werden eine Routing-Tabelle für die VPCs und eine Routing-Tabelle für die VPN-Verbindung verwendet.

Die VPC-Anhänge sind der folgenden Routing-Tabelle zugeordnet, die eine weitergegebene Route für den VPN-Anhang enthält.R

Zielbereich	Ziel	Routing-Typ
10,99,99. 0/24	*Attachment for VPN connection*	verbreitet

Der VPN-Anhang ist der folgenden Routing-Tabelle zugeordnet, in der die Routen für die einzelnen VPC-Anhänge verteilt wurden.

Zielbereich	Ziel	Routing-Typ
10.1.0. 0/16	*Attachment for VPC A*	verbreitet
10.2.0. 0/16	*Attachment for VPC B*	verbreitet
10.3.0. 0/16	*Attachment for VPC C*	verbreitet

Weitere Informationen zum Übertragen von Routen in einer Transit-Gateway-Routing-Tabelle finden Sie unter Route-Propagierung zu einer Transit-Gateway-Routentabelle in AWS Transit Gateway aktivieren.

Kunden-Gateway-BGP-Tabelle

Die Kunden-Gateway-BGP-Tabelle enthält die folgenden VPC-CIDRs.

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

Beispiel: Isolierte VPCs mit freigegeben Services

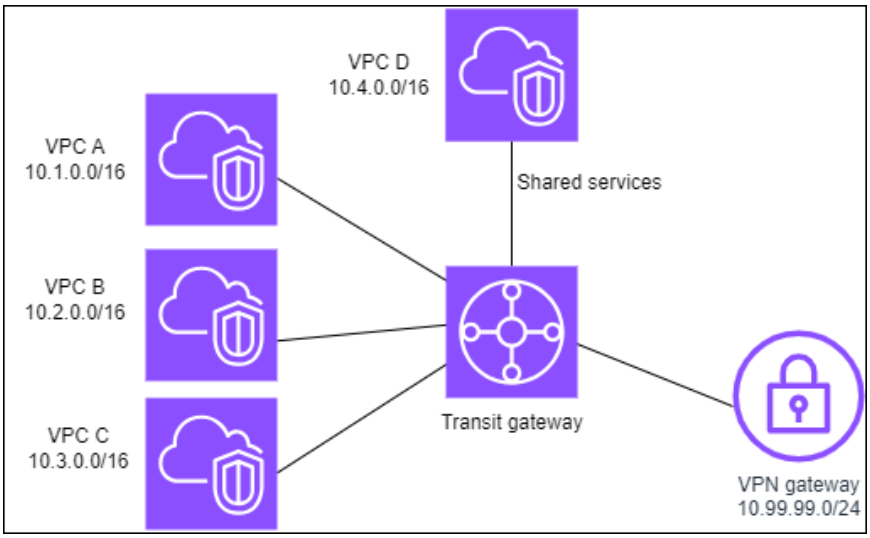
Sie können Ihr Transit-Gateway als mehrere isolierte Router konfigurieren, die einen freigegebenen Service verwenden. Dies gleicht der Verwendung mehrerer Transit-Gateways, bietet aber mehr Flexibilität, falls sich die Routen und Anfügungen ändern. In diesem Szenario verfügt jeder isolierte Router über eine einzige Routing-Tabelle. Alle Anfügungen, die diesem isolierten Router zugeordnet sind, verbreiten mit seiner Routing-Tabelle und werden ihr zugeordnet. Die Anfügungen, die einem isolierten Router zugeordnet sind, können Pakete untereinander weiterleiten. Sie können aber keine Pakete an Anfügungen eines anderen isolierten Routers leiten oder Pakete von ihnen empfangen. Anfügungen können Pakete an freigegebene Services weiterleiten oder sie davon empfangen. Sie können dieses Szenario verwenden, wenn Sie Gruppen haben, die isoliert sein müssen, aber einen freigegebenen Service verwenden, z. B. ein Produktionssystem.

Inhalt

-Übersicht

Die folgende Abbildung zeigt die Hauptkomponenten der Konfiguration für dieses Szenario. Pakete aus den Subnetzen in VPC A, VPC B und VPC C, die das Internet als Ziel haben, werden zuerst über das Transit-Gateway und dann zum Kunden-Gateway für VPN weitergeleitet. Site-to-Site Pakete aus Subnetzen in VPC A, VPC B oder VPC C, die als Ziel ein Subnetz in VPC A, VPC B oder VPC C haben, werden über das Transit-Gateway weitergeleitet, in dem sie blockiert werden, da für sie in der

Transit-Gateway-Routing-Tabelle keine Route vorhanden ist. Pakete aus VPC A, VPC B und VPC C, die VPC D als Zielroute haben, werden über das Transit-Gateway und dann an VPC D weitergeleitet.



Ressourcen

Erstellen Sie die folgenden Ressourcen für dieses Szenario:

- Vier VPCs. Weitere Informationen finden Sie unter VPC erstellen im Amazon-VPC-Benutzerhandbuch.
- Ein Transit-Gateway. Weitere Informationen finden Sie unter Erstellen eines Transit-Gateways.
- Vier Anhänge im Transit Gateway, eine pro VPC. Weitere Informationen finden Sie unter the section called “Erstellen Sie einen VPC-Anhang”.
- Ein Site-to-Site VPN-Anhang auf dem Transit-Gateway. Weitere Informationen finden Sie unter the section called “Erstellen eines Transit-Gateway-Anhangs an ein VPN”.

  Überprüfen Sie die Anforderungen für Ihr Kunden-Gateway-Gerät im AWS Site-to-Site VPN - Benutzerhandbuch.

Wenn die VPN-Verbindung besteht, wird die BGP-Sitzung hergestellt und das VPN-CIDR wird auf die Transit-Gateway-Routing-Tabelle übertragen. Die VPC-CIDRs werden dann der BGP-Kunden-Gateway-Tabelle hinzugefügt.

- Jede isolierte VPC wird der isolierten Routing-Tabelle zugeordnet und an die freigegebene Routing-Tabelle weitergegeben.
- Jede freigegebene Services-VPC wird der freigegebenen Routing-Tabelle zugeordnet und an beide Routing-Tabellen weitergegeben.

Routing

Jede VPC besitzt eine Routing-Tabelle, und das Transit-Gateway verfügt über zwei Routing-Tabellen – eine für die VPCs und eine für die VPN-Verbindung und VPC freigegebener Services.

VPC A-, VPC B-, VPC C- und VPC-D-Routing-Tabellen

Jede VPC hat eine Routing-Tabelle mit zwei Einträgen. Der erste Eintrag ist der Standardeintrag für lokales Routing in der VPC; dieser Eintrag befähigt die Instances in der VPC miteinander zu kommunizieren. Der zweite Eintrag leitet den gesamten anderen IPv4-Subnetz-Datenverkehr an das Transit Gateway weiter.

Zielbereich	Target
10.1.0. 0/16	local
0,0.0. 0/0	*transit gateway ID*

Transit-Gateway-Routing-Tabellen

In diesem Szenario werden eine Routing-Tabelle für die VPCs und eine Routing-Tabelle für die VPN-Verbindung verwendet.

Die VPC A-, B- und C-Anhänge sind der folgenden Routing-Tabelle zugeordnet, die eine propagierte Route für den VPN-Anhang und eine propagierte Route für den Anhang für VPC D enthält.

Zielbereich	Ziel	Routing-Typ
10,99,99. 0/24	*Attachment for VPN connection*	verbreitet
10,4,0. 0/16	*Attachment for VPC D*	verbreitet

Der VPN-Anhang und Anhänge der VPC mit freigegebenen Services (VPC D) sind der folgenden Routing-Tabelle zugeordnet, die Einträge enthält, die auf die einzelnen VPC-Anhänge verweisen. Dies ermöglicht die Kommunikation mit den VPCs von der VPN-Verbindung und der VPC mit freigegebenen Services.

Zielbereich	Ziel	Routing-Typ
10.1.0. 0/16	*Attachment for VPC A*	verbreitet
10.2.0. 0/16	*Attachment for VPC B*	verbreitet
10.3.0. 0/16	*Attachment for VPC C*	verbreitet

Weitere Informationen finden Sie unter Route-Propagierung zu einer Transit-Gateway-Routentabelle in AWS Transit Gateway aktivieren.

Kunden-Gateway-BGP-Tabelle

Die Kunden-Gateway-BGP-Tabelle enthält CIDRs für alle vier VPCs.

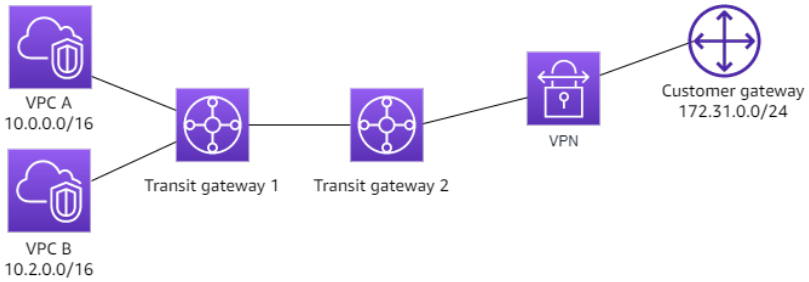
Beispiel: Per Peering verbundene Transit Gateways

Sie können eine Transit Gateway-Peering-Verbindung zwischen Transit Gateways erstellen. Anschließend können Sie den Datenverkehr zwischen den Anlagen für jedes Transit Gateway weiterleiten. In diesem Szenario sind alle VPC- und VPN-Anhänge den standardmäßigen Transit-Gateway-Routing-Tabellen zugeordnet und an die standardmäßige Transit-Gateway-Routing-Tabelle geleitet. Jede Transit-Gateway-Routing-Tabelle verfügt über eine statische Route, die auf den Peering-Anhang des Transit Gateways verweist.

Inhalt

-Übersicht

Die folgende Abbildung zeigt die Hauptkomponenten der Konfiguration für dieses Szenario. Transit-Gateway 1 hat zwei VPC-Anhänge und Transit-Gateway 2 hat einen Site-to-Site VPN-Anhang. Pakete aus den Subnetzen in VPC A und VPC B, die das Internet als Ziel haben, werden zuerst durch das Transit Gateway 1, dann durch das Transit Gateway 2 und schließlich an die VPN-Verbindung weitergeleitet.



Ressourcen

Erstellen Sie die folgenden Ressourcen für dieses Szenario:

- Zwei VPCs. Weitere Informationen finden Sie unter VPC erstellen im Amazon-VPC-Benutzerhandbuch.
- Zwei Transit Gateways. Sie können sich in derselben Region oder in verschiedenen Regionen befinden. Weitere Informationen finden Sie unter the section called “Erstellen eines Transit-Gateways”.
- Zwei VPC-Anhänge auf dem ersten Transit Gateway. Weitere Informationen finden Sie unter the section called “Erstellen Sie einen VPC-Anhang”.
- Ein Site-to-Site VPN-Anhang am zweiten Transit-Gateway. Weitere Informationen finden Sie unter the section called “Erstellen eines Transit-Gateway-Anhangs an ein VPN”. Überprüfen Sie die Anforderungen für Ihr Kunden-Gateway-Gerät im AWS Site-to-Site VPN -Benutzerhandbuch.
- Ein Transit-Gateway-Peering-Anhang zwischen den beiden Transit Gateways. Weitere Informationen finden Sie unter Transit-Gateway-Peering-Anlagen in AWS Transit Gateway.

Wenn Sie den VPC-Anhang erstellen, werden die CIDRs für jede VPC auf die Routing-Tabelle für Transit Gateway 1 übertragen. Wenn die VPN-Verbindung besteht, werden die folgenden Aktionen ausgeführt:

- Die BGP-Sitzung wird eingerichtet
- Das Site-to-Site VPN-CIDR wird an die Routing-Tabelle für Transit-Gateway 2 weitergegeben
- Die VPC-CIDRs werden der Kunden-Gateway-BGP-Tabelle hinzugefügt.

Routing

Jede VPC verfügt über eine Routing-Tabelle und jedes Transit Gateway hat ebenfalls eine Routing-Tabelle.

VPC-A- und VPC-B-Routing-Tabellen

Jede VPC hat eine Routing-Tabelle mit 2 Einträgen. Der erste Eintrag ist der Standardeintrag für das lokale IPv4-Routing innerhalb der VPC. Mit diesem Standardeintrag können die Ressourcen in dieser VPC miteinander kommunizieren. Der zweite Eintrag leitet den gesamten anderen IPv4-Subnetz-Datenverkehr an das Transit Gateway weiter. Die folgende Tabelle zeigt die VPC-A-Routen.

Zielbereich	Target
10.0.0. 0/16	local
0,0.0. 0/0	tgw-1-id

Transit-Gateway-Routing-Tabellen

Im Folgenden finden Sie ein Beispiel für die Standard-Routing-Tabelle für Transit Gateway 1 mit aktivierter Routen-Propagierung.

Zielbereich	Ziel	Routing-Typ
10.0.0. 0/16	*Attachment ID for VPC A*	verbreitet
10.2.0. 0/16	*Attachment ID for VPC B*	verbreitet
0,0.0. 0/0	*Attachment ID for peering connection*	statisch

Im Folgenden finden Sie ein Beispiel für die Standard-Routing-Tabelle für Transit Gateway 2 mit aktivierter Routen-Propagierung.

Zielbereich	Ziel	Routing-Typ
172,31,0. 0/24	*Attachment ID for VPN connection*	verbreitet
10.0.0. 0/16	*Attachment ID for peering connection*	statisch
10.2.0. 0/16	*Attachment ID for peering connection*	statisch

Kunden-Gateway-BGP-Tabelle

Die Kunden-Gateway-BGP-Tabelle enthält die folgenden VPC-CIDRs.

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

Beispiel: Zentralisiertes Outbound-Routing ins Internet

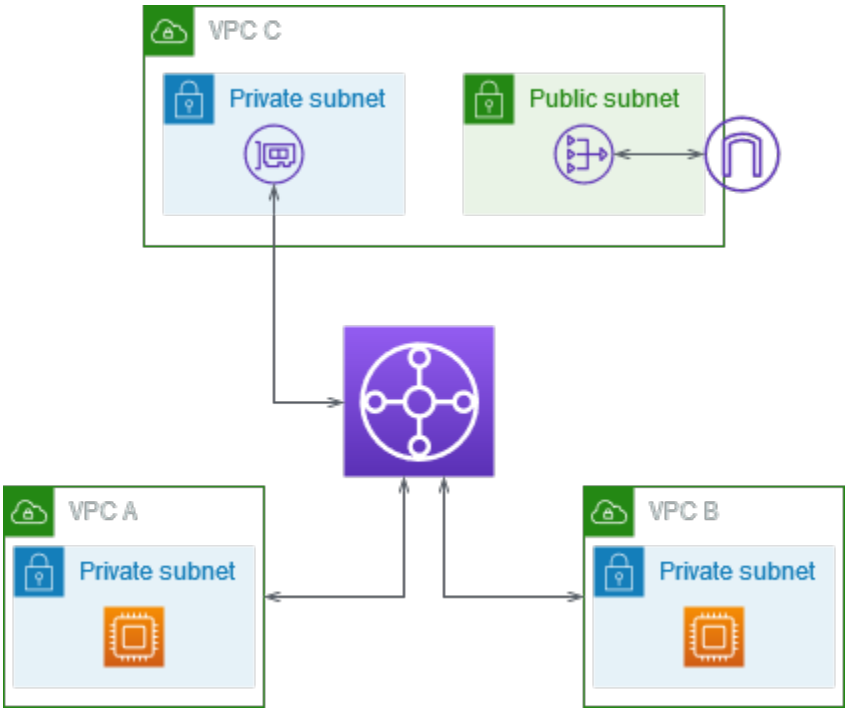
Sie können ein Transit-Gateway konfigurieren, um den ausgehenden Internetverkehr von einer VPC ohne Internet-Gateway an eine VPC zu leiten, die ein NAT-Gateway und ein Internet-Gateway enthält.

Inhalt

-Übersicht

Die folgende Abbildung zeigt die Hauptkomponenten der Konfiguration für dieses Szenario. Sie haben Anwendungen in VPC A und VPC B, die nur ausgehenden Internetzugang benötigen. Sie konfigurieren VPC C mit einem öffentlichen NAT-Gateway und einem Internet-Gateway sowie einem privaten Subnetz für den VPC-Anhang. Verbinden Sie alle VPCs mit einem Transit-Gateway. Konfigurieren Sie das Routing so, dass ausgehender Internetdatenverkehr von VPC A und VPC B

das Transit Gateway zu VPC C durchquert. Das NAT-Gateway in VPC C leitet den Datenverkehr an das Internet-Gateway weiter.



Ressourcen

Erstellen Sie die folgenden Ressourcen für dieses Szenario:

- Drei VPCs mit IP-Adressbereichen, die weder identisch sind noch sich überschneiden. Weitere Informationen finden Sie unter VPC erstellen im Amazon-VPC-Benutzerhandbuch.
- VPC A und VPC B verfügen jeweils über private Subnetze mit EC2-Instances.
- VPC C verfügt über Folgendes:
  - Ein Internet-Gateway, das an die VPC angefügt ist. Weitere Informationen finden Sie unter Erstellen und Anfügen eines Internet-Gateways im Amazon-VPC-Benutzerhandbuch.
  - Ein öffentliches Subnetz mit einem NAT-Gateway. Weitere Informationen finden Sie unter Erstellen und Anfügen eines NAT-Gateways im Amazon-VPC-Benutzerhandbuch.
  - Ein privates Subnetz für den Transit-Gateway-Anhang. Das private Subnetz sollte sich in derselben Availability Zone wie das öffentliche Subnetz befinden.
- Ein Transit-Gateway Weitere Informationen finden Sie unter the section called “Erstellen eines Transit-Gateways”.
- Drei VPC-Anhänge im Transit Gateway. Die CIDR-Blöcke für jede VPC werden an die Transit-Gateway-Routing-Tabelle übertragen. Weitere Informationen finden Sie unter the section called

"Erstellen Sie einen VPC-Anhang". Für VPC C müssen Sie den Anhang mithilfe des privaten Subnetzes erstellen. Wenn Sie den Anhang mithilfe des öffentlichen Subnetzes erstellen, wird der Instance-Datenverkehr an das Internet-Gateway weitergeleitet, aber das Internet-Gateway lehnt den Datenverkehr ab, da die Instances keine öffentlichen IP-Adressen haben. Durch das Platzieren des Anhangs im privaten Subnetz wird der Datenverkehr an das NAT-Gateway weitergeleitet, und das NAT-Gateway sendet über die Elastic IP-Adresse als Quell-IP-Adresse den Datenverkehr an das öffentliche Internet-Gateway.

Routing

Es gibt Routing-Tabellen für jede VPC und eine Routing-Tabelle für das Transit Gateway.

Routing-Tabellen

- Routing-Tabelle für VPC A
- Routing-Tabelle für VPC B
- Routing-Tabellen für VPC C
- Routing-Tabelle für Transit Gateway

Routing-Tabelle für VPC A

Es folgt ein Beispiel für eine Routing-Tabelle. Dieser erste Eintrag ermöglicht es den Instances in dieser VPC, miteinander zu kommunizieren. Der zweite Eintrag leitet den gesamten anderen IPv4-Subnetz-Datenverkehr an das Transit Gateway weiter.

Zielbereich	Ziel
VPC A CIDR	Local
0.0.0. 0/0	*transit-gateway-id*

Routing-Tabelle für VPC B

Es folgt ein Beispiel für eine Routing-Tabelle. Dieser erste Eintrag ermöglicht es den Instances in dieser VPC, miteinander zu kommunizieren. Der zweite Eintrag leitet den gesamten anderen IPv4-Subnetz-Datenverkehr an das Transit Gateway weiter.

Zielbereich	Ziel
VPC B CIDR	Local
0,0.0. 0/0	*transit-gateway-id*

Routing-Tabellen für VPC C

Konfigurieren Sie das Subnetz mit dem NAT-Gateway als öffentliches Subnetz, indem Sie dem Internet-Gateway eine Route hinzufügen. Das andere Subnetz bleibt ein privates Subnetz.

Im Folgenden finden Sie ein Beispiel einer Routing-Tabelle für das öffentliche Subnetz. Dieser erste Eintrag ermöglicht es den Instances in dieser VPC, miteinander zu kommunizieren. Die zweiten und dritten Einträge leiten Datenverkehr für VPC A und VPC B zum Transit Gateway. Der verbleibende Eintrag leitet den übrigen IPv4-Datenverkehr des Subnetzes an das Internet-Gateway.

Zielbereich	Ziel
VPC C CIDR	Local
VPC A CIDR	*transit-gateway-id*
VPC B CIDR	*transit-gateway-id*
0,0.0. 0/0	*internet-gateway-id*

Das Folgende ist ein Beispiel einer Routing-Tabelle für das private Subnetz. Dieser erste Eintrag ermöglicht es den Instances in dieser VPC, miteinander zu kommunizieren. Der zweite Eintrag leitet den gesamten anderen IPv4-Subnetz-Datenverkehr an das NAT-Gateway weiter.

Zielbereich	Ziel
VPC C CIDR	Local
0,0.0. 0/0	*nat-gateway-id*

Routing-Tabelle für Transit Gateway

Es folgt ein Beispiel für die Routing-Tabelle des Transit-Gateways. Die CIDR-Blöcke für jede VPC werden an die Transit-Gateway-Routing-Tabelle übertragen. Sie können die Kommunikation zwischen VPC C optional verhindern, indem Sie ein Blackhole-Routing für jede VPC CIDR hinzufügen.

CIDR	Attachment	Routing-Typ
VPC A CIDR	*Attachment for VPC A*	verbreitet
VPC B CIDR	*Attachment for VPC B*	verbreitet
VPC C CIDR	*Attachment for VPC C*	verbreitet
0,0.0. 0/0	*Attachment for VPC C*	statisch

Beispiel: Appliance in einer VPC mit freigegeben Services

Sie können in einer VPC freigegebener Services eine Appliance (z. B. eine Sicherheits-Appliance) konfigurieren. Der gesamte Datenverkehr, der zwischen Transit-Gateway-Anhängen weitergeleitet wird, wird zuerst von der Appliance in der VPC freigegebener Services überprüft. Wenn der Appliance-Modus aktiviert ist, wählt ein Transit Gateway eine einzelne Netzwerkschnittstelle in der Appliance-VPC unter Verwendung eines Flow-Hash-Algorithmus aus, an die er während der gesamten Lebensdauer des Datenflusses Datenverkehr sendet. Das Transit Gateway verwendet dieselbe Netzwerkschnittstelle für den Rückverkehr. Dadurch wird sichergestellt, dass der bidirektionale Datenverkehr symmetrisch weitergeleitet wird – er wird während der gesamten Lebensdauer des Datenflusses durch dieselbe Availability Zone in den VPC-Anhang weitergeleitet. Wenn Sie mehrere Transit Gateways in Ihrer Architektur haben, behält jedes Transit Gateway seine eigene Sitzungsaffinität bei und jedes Transit Gateway kann eine andere Netzwerkschnittstelle auswählen.

Sie müssen genau ein Transit Gateway mit der Appliance-VPC verbinden, um die Flow-Stickiness zu gewährleisten. Durch das Verbinden mehrerer Transit Gateways mit einer einzelnen Appliance-VPC

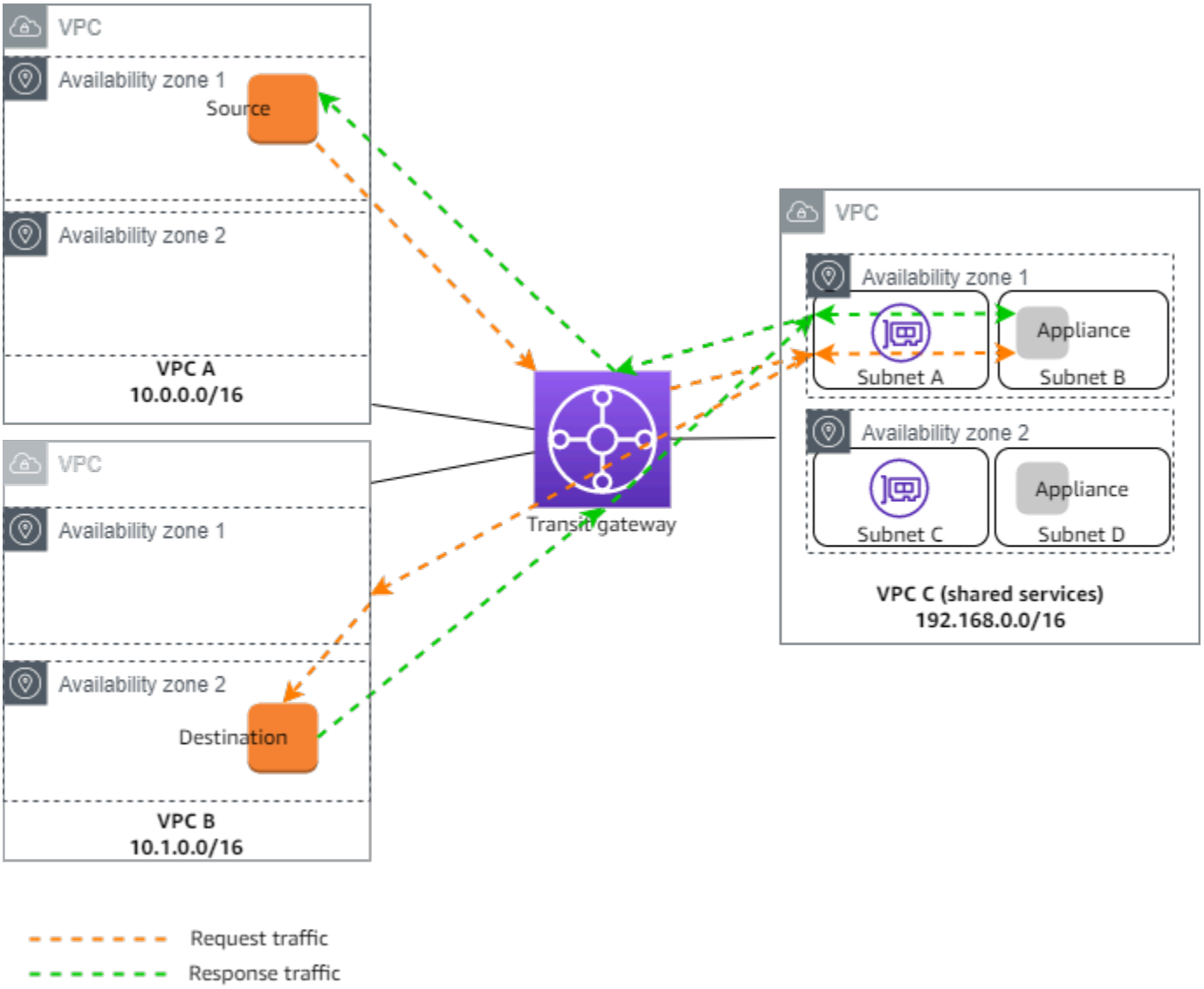
wird die Flow-Stickiness nicht gewährleistet, da die Transit Gateways keine Flussstatusinformationen miteinander teilen.

> **Important**
>
> - Der Datenverkehr im Appliance-Modus wird korrekt weitergeleitet, solange der Quell- und Zieldatenverkehr von demselben Transit-Gateway-Anhang auf eine zentrale VPC (Inspection VPC) gelangt. Der Verkehr kann sinken, wenn sich Quelle und Ziel auf zwei verschiedenen Transit-Gateway-Anhängen befinden. Der Verkehr kann sinken, wenn die zentralisierte VPC den Verkehr von einem anderen Gateway empfängt — z. B. einem Internet-Gateway — und diesen Datenverkehr dann nach der Inspektion an den Transit-Gateway-Anhang sendet.
> - Die Aktivierung des Appliance-Modus für einen vorhandenen Anhang kann sich auf die aktuelle Route dieses Anhangs auswirken, da der Anhang jede Availability Zone passieren kann. Wenn der Appliance-Modus nicht aktiviert ist, wird der Datenverkehr in der ursprünglichen Availability Zone belassen.

Inhalt

-Übersicht

Die folgende Abbildung zeigt die Hauptkomponenten der Konfiguration für dieses Szenario. Das Transit Gateway hat drei VPC-Anhänge. VPC C ist eine freigegebene Services-VPC. Der Datenverkehr zwischen VPC A und VPC B wird an das Transit Gateway und dann zur Überprüfung an eine Sicherheits-Appliance in VPC C weitergeleitet, bevor er zum endgültigen Ziel weitergeleitet wird. Da die Appliance ist eine zustandsbehaftete Appliance ist, wird sowohl der Anforderungs- als auch der Antwortdatenverkehr überprüft. Für hohe Verfügbarkeit gibt es in jeder Availability Zone in VPC C eine Appliance.



Sie erstellen die folgenden Ressourcen für dieses Szenario:

- Drei VPCs. Weitere Informationen finden Sie unter VPC erstellen im Amazon-VPC-Benutzerhandbuch.
- Ein Transit Gateway. Weitere Informationen finden Sie unter the section called “Erstellen eines Transit-Gateways”.
- Drei VPC-Anhänge – einer für jede der VPCs. Weitere Informationen finden Sie unter the section called “Erstellen Sie einen VPC-Anhang”.

  Geben Sie für jeden VPC-Anhang ein Subnetz in jeder Availability Zone an. Für die VPC freigegebener Services sind dies die Subnetze, in denen der Datenverkehr vom Transit Gateway an die VPC geleitet wird. Im vorangehenden Beispiel sind dies Subnetze A und C.

Aktivieren Sie für den VPC-Anhang für VPC C die Unterstützung des Appliance-Modus, damit der Antwortdatenverkehr an dieselbe Availability Zone in VPC C wie der Quelldatenverkehr weitergeleitet wird.

Die Amazon-VPC-Konsole unterstützt den Appliance-Modus. Sie können auch die Amazon VPC-API, ein AWS SDK, verwenden, AWS CLI um den Appliance-Modus zu aktivieren, oder CloudFormation. Fügen Sie `--options ApplianceModeSupport=enable` zum Beispiel den Befehl create-transit-gateway-vpc-attachment oder modify-transit-gateway-vpc-attachment hinzu.

> **Note**
>
> Flow-Stickiness im Appliance-Modus ist nur für Quell- und Zieldatenverkehr gewährleistet, der von der Inspection-VPC ausgeht.

Statusbehaftete Appliances und Appliance-Modus

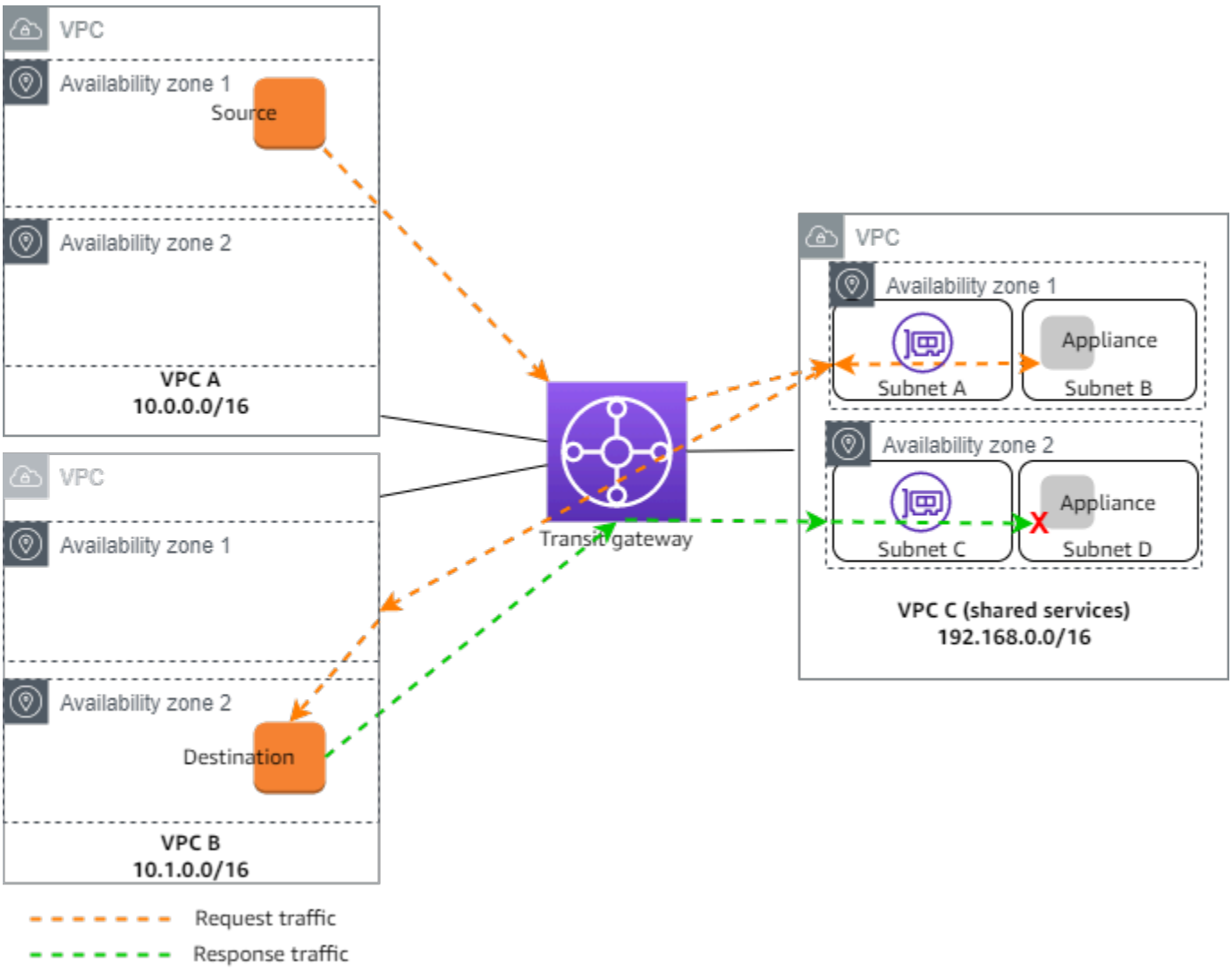
Wenn sich Ihre VPC-Anhänge über mehrere Availability Zones erstrecken und Sie verlangen, dass der Datenverkehr zwischen Quell- und Zielhosts zur zustandsbehafteten Prüfung über dieselbe Appliance geleitet wird, aktivieren Sie die Unterstützung des Appliance-Modus für den VPC-Anhang, in der sich die Appliance befindet.

Weitere Informationen finden Sie im AWS Blog unter Zentralisierte Inspektionsarchitektur.

Verhalten bei nicht aktiviertem Appliance-Modus

Wenn der Appliance-Modus nicht aktiviert ist, versucht ein Transit Gateway, den Datenverkehr zwischen VPC-Anhängen in der ursprünglichen Availability Zone weitergeleitet zu halten, bis er sein Ziel erreicht. Der Datenverkehr durchquert Availability Zones zwischen Anhängen nur dann, wenn ein Availability Zone-Ausfall vorliegt oder wenn keine Subnetze mit einem VPC-Anhang in dieser Availability Zone verknüpft sind.

Das folgende Diagramm zeigt einen Datenverkehrsfluss, wenn die Unterstützung des Appliance-Modus nicht aktiviert ist. Der Antwortdatenverkehr, der von Availability Zone 2 in VPC B stammt, wird vom Transit Gateway zur gleichen Availability Zone in VPC C weitergeleitet. Der Datenverkehr wird daher unterbrochen, da der Appliance in Availability Zone 2 die ursprüngliche Anforderung von der Quelle in VPC A nicht bekannt ist.



Routing

Jede VPC verfügt über eine oder mehrere Routing-Tabellen und das Transit Gateway verfügt über zwei Routing-Tabellen.

VPC-Routing-Tabellen

VPC A und VPC B

VPCs A und B haben Routing-Tabellen mit 2 Einträgen. Der erste Eintrag ist der Standardeintrag für das lokale IPv4-Routing innerhalb der VPC. Mit diesem Standardeintrag können die Ressourcen in dieser VPC miteinander kommunizieren. Der zweite Eintrag leitet den gesamten anderen IPv4-Subnetz-Datenverkehr an das Transit Gateway weiter. Das Folgende ist die Routing-Tabelle für VPC A.

Zielbereich	Target
10.0.0. 0/16	local
0,0.0. 0/0	tgw-id

VPC C

Die VPC freigegebener Services (VPC C) verfügt für jedes Subnetz über unterschiedliche Routing-Tabellen. Subnetz A wird vom Transit Gateway verwendet (Sie geben dieses Subnetz an, wenn Sie den VPC-Anhang erstellen). Die Routing-Tabelle für Subnetz A leitet den gesamten Datenverkehr an die Appliance im Subnetz B.

Zielbereich	Target
192,168,0. 0/16	local
0,0.0. 0/0	appliance-eni-id

Die Routing-Tabelle für Subnetz B (die die Appliance enthält) leitet den Datenverkehr zurück zum Transit Gateway.

Zielbereich	Target
192,168,0. 0/16	local
0,0.0. 0/0	tgw-id

Transit-Gateway-Routing-Tabellen

Dieses Transit Gateway verwendet eine Routing-Tabelle für VPC A und VPC B und eine Routing-Tabelle für die VPC freigegebener Services (VPC C).

Die VPC A- und VPC B-Anhänge sind der folgenden Routing-Tabelle zugeordnet. Die Routing-Tabelle leitet den gesamten Datenverkehr zu VPC C.

Zielbereich	Ziel	Routing-Typ
0,0.0. 0/0	*Attachment ID for VPC C*	statisch

Der VPC C-Anhang ist mit der folgenden Routing-Tabelle verknüpft. Sie leitet den Datenverkehr zu VPC A und VPC B.

Zielbereich	Ziel	Routing-Typ
10.0.0. 0/16	*Attachment ID for VPC A*	verbreitet
10.1.0. 0/16	*Attachment ID for VPC B*	verbreitet

Tutorials: Erste Schritte mit AWS Transit Gateway

Die folgenden Tutorials helfen Ihnen, sich mit Transit-Gateways in AWS Transit Gateway vertraut zu machen. Die Aufgaben in den folgenden Tutorials führen Sie durch die Erstellung eines Transit-Gateways und die anschließende Verbindung zweier Geräte, die dieses Transit-Gateway VPCs verwenden. Sie können ein Transit-Gateway entweder mit der Amazon VPC-Konsole oder mit dem AWS CLI erstellen.

Aufgaben

- Tutorial: Erstellen Sie ein AWS Transit Gateway mit der Amazon VPC-Konsole
- Tutorial: Erstellen Sie ein AWS Transit Gateway über die AWS Befehlszeile

Tutorial: Erstellen Sie ein AWS Transit Gateway mit der Amazon VPC-Konsole

In diesem Tutorial erfahren Sie, wie Sie die Amazon VPC-Konsole verwenden, um ein Transit-Gateway zu erstellen und zwei damit VPCs zu verbinden. Sie erstellen das Transit-Gateway, fügen beide hinzu und konfigurieren dann die erforderlichen Routen VPCs, um die Kommunikation zwischen dem Transit-Gateway und Ihrem VPCs zu ermöglichen.

Voraussetzungen

- Um ein einfaches Beispiel für die Verwendung eines Transit-Gateways zu demonstrieren, erstellen Sie zwei VPCs in derselben Region. VPCs Sie können weder identisch noch überlappend CIDRs sein. Starten Sie eine EC2 Amazon-Instance in jeder VPC. Weitere Informationen finden Sie unter Erstellen einer VPC im Amazon VPC-Benutzerhandbuch und Starten einer Instance im EC2 Amazon-Benutzerhandbuch.
- Es können keine identischen Routen auf zwei verschiedene Routen verweisen. VPCs Ein Transit-Gateway verbreitet die Daten einer neu angeschlossenen VPC nicht, wenn in den Routentabellen CIDRs des Transit-Gateways eine identische Route vorhanden ist.
- Vergewissern Sie sich, dass Sie über die erforderlichen Berechtigungen zum Arbeiten mit Transit Gateways verfügen. Weitere Informationen finden Sie unter Identitäts- und Zugriffsmanagement in AWS Transit Gateway.

- Sie können nicht zwischen Hosts pingen, wenn Sie keiner der Host-Sicherheitsgruppen eine ICMP-Regel hinzugefügt haben. Weitere Informationen finden Sie unter Sicherheitsgruppenregeln konfigurieren im Amazon VPC-Benutzerhandbuch.

Schritte

Schritt 1: Erstellen des Transit Gateway

Wenn Sie ein Transit Gateway erstellen, erstellen wir eine Standard-Transit-Gateway-Routing-Tabelle und verwenden sie als Standard-Zuordnungs-Routing-Tabelle und als standardmäßige Route-Propagierung-Tabelle.

So erstellen Sie ein Transit Gateway

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie in der Regionsauswahl die Region aus, die Sie bei der Erstellung von verwendet haben. VPCs
3. Klicken Sie im Navigationsbereich auf Transit Gateways.
4. Wählen Sie Create Transit Gateway (Transit Gateway erstellen) aus.
5. (Optional) Geben Sie für Name tag (Namens-Tag) einen Namen für das Transit Gateway ein. Dadurch wird ein Tag mit "Name" als Schlüssel und dem Namen, den Sie angegeben haben, als Wert erstellt.
6. (Optional) Geben Sie im Feld Description (Beschreibung) eine Beschreibung für das Transit Gateway ein.
7. Gehen Sie im Abschnitt Transit-Gateway konfigurieren wie folgt vor:

    1. Geben Sie bei Amazon side Autonomous System Number (ASN) (Amazon-seitige ASN) die private autonome Systemnummer (ASN) für Ihr Transit Gateway ein. Dies sollte die ASN für die AWS Seite einer Border Gateway Protocol (BGP) -Sitzung sein.

Der Bereich reicht von 64512 bis 65534 für 16-Bit. ASNs

Der Bereich reicht von 4200000000 bis 4294967294 für 32-Bit. ASNs

Für eine Multiregion-Bereitstellung empfehlen wir die Verwendung einer eindeutigen ASN für jedes Ihrer Transit Gateways.

2. (Optional) Wählen Sie aus, ob eine der folgenden Optionen aktiviert werden soll:
   - DNS-Unterstützung für Verbindungen VPCs zu diesem Transit-Gateway.
   - VPN ECMP-Unterstützung für VPN-Verbindungen, die an das Transit-Gateway angeschlossen sind.
   - Standardroutentabellenzuweisung, die Transit-Gateway-Anlagen automatisch der Standard-Routing-Tabelle dieses Transit-Gateways zuordnet.
   - Standardweiterleitung von Routentabellen, bei der Routentabellenanhänge automatisch an die Standardroutentabelle dieses Transit-Gateways weitergegeben werden.
   - Multicast-Unterstützung, mit der Sie Multicast-Domänen in diesem Transit-Gateway erstellen können.

8. (Optional) Wählen Sie im Bereich „Configure-cross-account Freigabeoptionen“ aus, ob gemeinsam genutzte Anlagen automatisch akzeptiert werden sollen. Wenn diese Option aktiviert ist, werden Anlagen automatisch akzeptiert. Andernfalls müssen Sie Anhangsanforderungen annehmen oder ablehnen.
9. (Optional) Fügen Sie im Abschnitt CIDR-Blöcke des Transit-Gateways einen CIDR-Block der Größe /24 oder größer für IPv4 Adressen oder einen CIDR-Block oder größer für Adressen hinzu. IPv6 Sie können jeden öffentlichen oder privaten IP-Adressbereich zuordnen, mit Ausnahme von Adressen im Bereich von 169.254.0.0/16 und Bereichen, die sich mit den Adressen für Ihre VPC-Anhänge und On-Premises-Netzwerke überschneiden.

   > **Note**
   >
   > CIDR-Blöcke des Transit-Gateways werden verwendet, wenn Sie Connect (GRE) - Anhänge oder VPNs PrivateIP konfigurieren. Transit Gateway weist IPs den Tunnel-Endpunkten (GRE/PrivateIP VPN) aus diesem Bereich zu.

10. (Optional) Fügen Sie diesem Transit-Gateway Key-Value-Tags hinzu, um es besser identifizieren zu können.

    1. Wählen Sie Neues Tag hinzufügen aus.

2. Geben Sie einen Schlüsselnamen und den zugehörigen Wert ein.
3. Wählen Sie Neues Tag hinzufügen, um weitere Tags hinzuzufügen, oder fahren Sie mit dem nächsten Schritt fort.

11. Wählen Sie Create Transit Gateway (Transit Gateway erstellen) aus. Wenn das Gateway erstellt wird, ist der Ausgangszustand des Transit-Gateways `pending`.

Schritt 2: Verbinden Sie Ihre VPCs mit Ihrem Transit-Gateway

Warten Sie, bis das im vorherigen Abschnitt erstellte Transit Gateway als verfügbar angezeigt wird, bevor Sie mit dem Erstellen eines Anhangs beginnen. Erstellen Sie einen Anhang für jede VPC.

Vergewissern Sie sich, dass Sie zwei erstellt VPCs und in jeder EC2 Instanz eine Instanz gestartet haben, wie unter beschriebenVoraussetzungen.

Erstellen eines Transit-Gateway-Anhangs an eine VPC

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit Gateway-Anhänge).
3. Wählen Sie Create Transit Gateway Attachment (Transit-Gateway-Anhang erstellen) aus.
4. (Optional) Geben Sie unter Name tag (Namens-Tag) einen Namen für den Anhang ein.
5. Wählen Sie für Transit Gateway-ID das Transit Gateway aus, das für den Anhang verwendet werden soll.
6. Wählen Sie bei Attachment type (Anhangstyp) die Option VPC aus.
7. Wählen Sie aus, ob Sie DNS support (DNS-Unterstützung) aktivieren möchten. Aktivieren Sie für diese Übung keinen IPv6 Support.
8. Wählen Sie für VPC ID die VPC aus, die dem Transit-Gateway angefügt werden soll.
9. Wählen Sie unter Subnetz für jede Availability Zone ein Subnetz aus IDs, das vom Transit-Gateway zur Weiterleitung des Datenverkehrs verwendet werden soll. Sie müssen mindestens ein Subnetz auswählen. Sie können nur ein Subnetz pro Availability Zone auswählen.
10. Wählen Sie Create Transit Gateway Attachment (Transit-Gateway-Anhang erstellen) aus.

Jeder Anhang ist immer genau einer Routing-Tabelle zugeordnet. Routing-Tabellen können keinem, aber auch mehreren Anhängen zugeordnet sein. Um die zu konfigurierenden Routen zu bestimmen, entscheiden Sie sich für den Anwendungsfall Ihres Transit Gateways und konfigurieren Sie dann die

Routen. Weitere Informationen finden Sie unter the section called “Beispiele für Transit-Gateway-Szenarien”.

Schritt 3: Fügen Sie Routen zwischen dem Transit-Gateway und Ihrem hinzu VPCs

Eine Routentabelle enthält dynamische und statische Routen, die anhand der Ziel-IP-Adresse des Pakets bestimmen, welcher Hop als Nächstes zugeordnet VPCs wird. Konfigurieren Sie eine Route, die ein Ziel für nicht-lokale Routen und das Ziel der Transit-Gateway-Anhangs-ID hat. Weitere Informationen finden Sie unter Routing für ein Transit Gateway im Amazon-VPC-Benutzerhandbuch.

Hinzufügen einer Route zu einer VPC-Routing-Tabelle

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Route Tables (Routing-Tabellen) aus.
3. Wählen Sie die Routing-Tabelle aus, die Ihrer VPC zugeordnet ist.
4. Klicken Sie auf der Registerkarte Routes (Routen) auf Edit routes (Routen bearbeiten).
5. Wählen Sie Add Route (Route hinzufügen) aus.
6. Geben Sie in der Spalte Destination (Ziel) den Ziel-IP-Adressbereich ein. Als Target (Ziel) wählen Sie Transit Gateway dann die ID des Transit-Gateways aus.
7. Wählen Sie Änderungen speichern aus.

Schritt 4: Testen des Transit Gateways

Sie können überprüfen, ob das Transit-Gateway erfolgreich erstellt wurde, indem Sie in jeder VPC eine Verbindung zu einer EC2 Amazon-Instance herstellen und dann Daten zwischen ihnen senden, z. B. einen Ping-Befehl. Weitere Informationen finden Sie unter Connect zu Ihrer EC2 Instance herstellen im EC2 Amazon-Benutzerhandbuch.

Schritt 5: Löschen des Transit Gateway

Wenn Sie ein Transit Gateway nicht mehr benötigen, können Sie es löschen.

Transit Gateways mit angefügten Ressourcen können nicht gelöscht werden. Wenn Sie versuchen, ein Transit-Gateway mit Anhängen zu löschen, werden Sie aufgefordert, zuerst diese Anhänge zu löschen, bevor Sie das Transit-Gateway löschen können. Sobald das Transit Gateway gelöscht wurde, fallen keine Gebühren dafür mehr an.

So löschen Sie Ihr Transit Gateway

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateways.
3. Wählen Sie das Transit-Gateway und dann Actions (Aktionen), Delete transit gateway (Transit-Gateway löschen) aus.
4. Geben Sie **`delete`** ein und wählen Sie Delete (Löschen).

   Der State (Status) des Transit-Gateway auf der Seite Transit gateways (Transit-Gateways) lautet Deleting (Wird gelöscht). Nach dem Löschen wird das Transit-Gateway von der Seite entfernt.

Tutorial: Erstellen Sie ein AWS Transit Gateway über die AWS Befehlszeile

In diesem Tutorial erfahren Sie, wie Sie mit AWS CLI dem ein Transit-Gateway erstellen und zwei VPCs damit verbinden. Sie erstellen das Transit-Gateway, fügen beide hinzu und konfigurieren dann die erforderlichen Routen VPCs, um die Kommunikation zwischen dem Transit-Gateway und Ihrem zu ermöglichen VPCs.

Voraussetzungen

Bevor Sie beginnen, stellen Sie sicher, dass Sie über Folgendes verfügen:

- AWS CLI mit den entsprechenden Berechtigungen installiert und konfiguriert. Wenn Sie das nicht AWS CLI installiert haben, lesen Sie in der Dokumentation zur AWS Befehlszeilenschnittstelle nach.
- VPCs Sie können weder identisch noch überlappend CIDRs sein. Weitere Informationen finden Sie unter VPC erstellen im Amazon-VPC-Benutzerhandbuch.
- Eine EC2-Instance in jeder VPC. Die Schritte zum Starten einer EC2-Instance in einer VPC finden Sie unter Launch an Instance im Amazon EC2 EC2-Benutzerhandbuch.
- Sicherheitsgruppen, die so konfiguriert sind, dass sie ICMP-Verkehr zwischen den Instances zulassen. Die Schritte zur Steuerung des Datenverkehrs mithilfe von Sicherheitsgruppen finden Sie unter Steuern des Datenverkehrs zu Ihren AWS Ressourcen mithilfe von Sicherheitsgruppen im Amazon VPC-Benutzerhandbuch.

- Entsprechende IAM-Berechtigungen für die Arbeit mit Transit-Gateways. Informationen zur Überprüfung der IAM-Berechtigungen für Transit-Gateways finden Sie im Handbuch unter Identitäts- und Zugriffsverwaltung in AWS Transit Gateways.AWS Transit Gateway

Schritte

Schritt 1: Erstellen des Transit-Gateway

Wenn Sie ein Transit-Gateway erstellen, AWS erstellt es eine Standard-Transit-Gateway-Routentabelle und verwendet sie als Standard-Zuordnungs-Routentabelle und Standard-Propagierungsroutentabelle. Im Folgenden wird ein Beispiel für eine `create-transit-gateway` Anfrage in der `us-west-2` Region gezeigt. Weitere `options` wurden in der Anfrage übergeben. Weitere Informationen zu dem `create-transit-gateway` Befehl, einschließlich einer Liste der Optionen, die Sie in der Anforderung übergeben können, finden Sie unter create-transit-gateway.

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

Die Antwort zeigt dann, dass das Transit-Gateway erstellt wurde. In der Antwort `Options` werden alle Standardwerte zurückgegeben.

```
{
    "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**
>
> Dieser Befehl gibt Informationen über Ihr neues Transit-Gateway zurück, einschließlich seiner ID. Notieren Sie sich die Transit-Gateway-ID (`tgw-1234567890abcdef0`), da Sie sie in den nachfolgenden Schritten benötigen.

Schritt 2: Überprüfen Sie den Verfügbarkeitsstatus des Transit-Gateways

Wenn Sie ein Transit-Gateway erstellen, wird es in einen `pending` Status versetzt. Der Status wird automatisch von „Ausstehend“ zu „Verfügbar“ geändert. Solange dies nicht der Fall ist, können Sie keinen Status hinzufügen, VPCs bis sich der Status ändert. Um den Status zu überprüfen, führen Sie den `describe-transit-gatweways` Befehl mit der neu erstellten Transit-Gateway-ID zusammen mit der Filteroption aus. Die `filters` Option verwendet `Name=state` und `Values=available` paart. Der Befehl überprüft dann, ob der Status Ihres Transit-Gateways verfügbar ist. Ist dies der Fall, wird die Antwort angezeigt`"State": "available"`. Wenn es sich in einem anderen Bundesstaat befindet, kann es noch nicht verwendet werden. Warten Sie einige Minuten, bevor Sie den Befehl ausführen.

Weitere Informationen zum Befehl `describe-transit-gateways` finden Sie unter describe-transit-gateways.

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

Warten Sie, bis sich der Status des Transit-Gateways von `pending` zu ändert, `available` bevor Sie fortfahren. In der folgenden Antwort `State` hat sich der zu geändert`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"
                }
            ]
        }
    ]
}
```

Schritt 3: Schließen Sie Ihre VPCs an Ihr Transit-Gateway an

Sobald Ihr Transit-Gateway verfügbar ist, erstellen Sie mit dem einen Anhang für jede VPC. `create-transit-gateway-vpc-attachment` Sie müssen die`transit-gateway-id`, die und `vpc-id` die `subnet-ids` angeben.

Weitere Informationen zu dem `create-transit-vpc attachment` Befehl finden Sie unter create-transit-gateway-vpc-attachment.

Im folgenden Beispiel wird der Befehl zweimal ausgeführt, einmal für jede VPC.

Führen Sie für die erste VPC Folgendes mit dem ersten `vpc_id` und `subnet-ids` aus:

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

Die Antwort zeigt den erfolgreichen Anhang. Der Anhang wurde in einem `pending` Zustand erstellt. Dieser Status muss nicht geändert werden, da er automatisch in einen `available` Status wechselt. Dies kann einige Minuten dauern.

```
{
    "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"
        }
    }
```

```
}
```

Führen Sie für die zweite VPC denselben Befehl wie oben mit der zweiten aus `vpc_id` und`subnet-ids`:

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

Die Antwort auf diesen Befehl zeigt auch, dass das Anhängen erfolgreich war und sich der Anhang derzeit in einem `pending` Status befindet.

```
{
    {
    "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"
        }
    }
}
```

Schritt 4: Stellen Sie sicher, dass die Transit-Gateway-Anlagen verfügbar sind

Transit Gateway-Anhänge werden in einem `pending` Anfangszustand erstellt. Sie können diese Anlagen erst dann in Ihren Routen verwenden, wenn sich der Status auf ändert`available`. Das passiert automatisch. Verwenden Sie den `describe-transit-gateways` Befehl zusammen

mit demtransit-gateway-id, um das zu überprüfenState. Weitere Informationen zum Befehl describe-transit-gateways finden Sie unter describe-transit-gateways.

Führen Sie den folgenden Befehl aus, um den Status zu überprüfen. In diesem Beispiel werden optionale Felder Name und Values Filterfelder in der Anfrage übergeben:

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

Die folgende Antwort zeigt, dass sich beide Anlagen in einem available Zustand befinden:

```
{
    "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": []
        }
    ]
}
```

Schritt 5: Fügen Sie Routen zwischen Ihrem Transit-Gateway hinzu und VPCs

Konfigurieren Sie Routen in der Routentabelle jeder VPC, um den Verkehr über das Transit-Gateway an die andere VPC weiterzuleiten, indem Sie den `create-route` Befehl zusammen mit der Routentabelle `transit-gateway-id` für jede VPC verwenden. Im folgenden Beispiel wird der Befehl zweimal ausgeführt, einmal für jede Routentabelle. Die Anfrage umfasst die `route-table-iddestination-cidr-block`, und `transit-gateway-id` für jede VPC-Route, die Sie erstellen.

Weitere Informationen zum `create-route` Befehl finden Sie unter create-route.

Führen Sie für die Routing-Tabelle der ersten VPC den folgenden Befehl aus:

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

Führen Sie für die Routentabelle der zweiten VPC den folgenden Befehl aus. Diese Route verwendet eine `route-table-id` und, die `destination-cidr-block` sich von der ersten VPC unterscheidet. Da Sie jedoch nur ein einziges Transit-Gateway verwenden, `transit-gateway-id` wird dasselbe verwendet.

```
aws ec2 create-route \
  --route-table-id rtb-abcdef1234567890 \
  --destination-cidr-block 10.1.0.0/16 \
  --transit-gateway-id tgw-1234567890abcdef0
```

Die Antwort wird `true` für jede Route zurückgegeben und gibt an, dass die Routen erstellt wurden.

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

> **Note**
>
> Ersetzen Sie die Ziel-CIDR-Blöcke durch die tatsächlichen CIDR-Blöcke Ihrer. VPCs

Schritt 6: Testen Sie das Transit-Gateway

Sie können überprüfen, ob das Transit-Gateway erfolgreich erstellt wurde, indem Sie eine Verbindung zu einer EC2-Instance in einer VPC herstellen und eine Instance in der anderen VPC pingen und dann den Befehl ausführen. `ping`

1. Stellen Sie mithilfe von SSH oder EC2 Instance Connect eine Connect zu Ihrer EC2-Instance in der ersten VPC her
2. Pingen Sie die private IP-Adresse der EC2-Instance in der zweiten VPC:

   ```
   ping 10.2.0.50
   ```

   > **Note**
   >
   > `10.2.0.50`Ersetzen Sie durch die tatsächliche private IP-Adresse Ihrer EC2-Instance in der zweiten VPC.

Wenn der Ping erfolgreich ist, ist Ihr Transit-Gateway korrekt konfiguriert und leitet den Verkehr zwischen Ihren. VPCs

Schritt 7: Löschen Sie die Transit-Gateway-Anhänge und das Transit-Gateway

Wenn Sie das Transit-Gateway nicht mehr benötigen, können Sie es löschen. Zunächst müssen Sie alle Anlagen löschen. Führen Sie den `delete-transit-gateway-vpc-attachment` Befehl aus und verwenden Sie `transit-gateway-attachment-id` für jeden Anhang den. Verwenden Sie nach der Ausführung des Befehls, `delete-transit-gateway` um das Transit-Gateway zu

löschen. Löschen Sie im Folgenden die beiden VPC-Anlagen und das einzelne Transit-Gateway, die in den vorherigen Schritten erstellt wurden.

> **Important**
>
> Sobald Sie alle Transit-Gateway-Anlagen gelöscht haben, fallen keine Gebühren mehr an.

1. Löschen Sie die VPC-Anlagen mit dem `delete-transit-gateway-vpc-attachment` Befehl. Weitere Informationen zum `delete-transit-gateway-vpc-attachment` Befehl finden Sie unter delete-transit-gateway-vpc-attachment.

   Führen Sie für den ersten Anhang den folgenden Befehl aus:

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

   Die Löschantwort für den ersten VPC-Anhang gibt Folgendes zurück:

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

   Führen Sie den `delete-transit-gateway-vpc-attachment` Befehl für den zweiten Anhang aus:

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

   Die Löschantwort für den zweiten VPC-Anhang gibt Folgendes zurück:

   ```
   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. Anlagen befinden sich in einem `deleting` Zustand, bis sie gelöscht werden. Nach dem Löschen können Sie das Transit-Gateway löschen. Verwenden Sie den `delete-transit-gateway` Befehl zusammen mit dem`transit-gateway-id`. Weitere Hinweise zum `delete-transit-gateway` Befehl finden Sie unter delete-transit-gateway.

   Im folgenden Beispiel wird `My Transit Gateway` die Datei gelöscht, die Sie im ersten Schritt oben erstellt haben:

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

   Im Folgenden wird die Antwort auf die Anfrage gezeigt, die die gelöschte Transit-Gateway-ID und den gelöschten Namen sowie die ursprünglichen Optionen enthält, die für das Transit-Gateway bei der Erstellung festgelegt wurden.

   ```
   {
       "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"
            }
        ]
    }
}
```

Schlussfolgerung

Sie haben erfolgreich ein Transit-Gateway erstellt, zwei VPCs daran angehängt, das Routing zwischen ihnen konfiguriert und die Konnektivität überprüft. Dieses einfache Beispiel demonstriert die grundlegende Funktionalität von AWS Transit Gateways. Komplexere Szenarien, wie z. B. die Verbindung zu lokalen Netzwerken oder die Implementierung erweiterter Routing-Konfigurationen, finden Sie im AWS Transit Gateways Guide.

AWS Bewährte Methoden für das Design von Transit Gateway

Im Folgenden finden Sie die bewährten Methoden für Ihr Transit-Gateway-Design:

- Verwenden Sie für jeden Transit-Gateway-VPC-Anhang ein separates Subnetz. Verwenden Sie für jedes Subnetz beispielsweise ein kleines CIDR/28, damit Sie mehr Adressen für EC2 Ressourcen haben. Wenn Sie ein separates Subnetz verwenden, können Sie Folgendes konfigurieren:
  - Halten Sie das eingehende und ausgehende Netzwerk, das den ACLs Transit-Gateway-Subnetzen zugeordnet ist, offen.
  - Abhängig von Ihrem Datenverkehrsfluss können Sie das Netzwerk auf Ihre ACLs Workload-Subnetze anwenden.
- Erstellen Sie eine Netzwerk-ACL und weisen Sie diese allen Subnetzen zu, die mit dem Transit Gateway verbunden sind. Halten Sie die Netzwerk-ACL sowohl in der Richtung für eingehenden als auch in der Richtung für ausgehender Datenverkehr geöffnet.
- Ordnen Sie dieselbe VPC-Routentabelle allen Subnetzen zu, die dem Transit Gateway zugeordnet sind, es sei denn, Ihr Netzwerkdesign erfordert mehrere VPC-Routing-Tabellen (z. B. eine Middlebox-VPC, die den Verkehr über mehrere NAT-Gateways weiterleitet).
- Verwenden Sie Border Gateway Protocol (BGP) Site-to-Site VPN-Verbindungen. Wenn Ihr Kunden-Gateway-Gerät oder Ihre Firewall Mehrwegverbindungen für die Verbindung unterstützt, aktivieren Sie das Feature.
- Aktivieren Sie die Route-Propagierung für Direct Connect Gateway-Anhänge und Site-to-Site BGP-VPN-Anhänge.
- Bei der Migration von VPC-Peering zur Verwendung eines Transit-Gateways. Eine Nichtübereinstimmung der MTU-Größe zwischen VPC-Peering und dem Transit Gateway kann dazu führen, dass einige Pakete für asymmetrischen Datenverkehr gelöscht werden. Aktualisieren Sie beide VPCs Pakete gleichzeitig, um zu verhindern, dass Jumbo-Pakete aufgrund von Größenabweichungen verloren gehen.
- Für die Hochverfügbarkeit benötigen Sie keine zusätzlichen Transit Gateways, da Transit Gateways speziell auf Hochverfügbarkeit ausgelegt sind.
- Begrenzen Sie die Anzahl der Transit-Gateway-Routing-Tabellen, es sei denn, Ihr Design erfordert mehrere Transit-Gateway-Routing-Tabellen.

- Verwenden Sie für die Redundanz ein einziges Transit Gateway in jeder Region für die Notfallwiederherstellung.
- Bei Bereitstellungen mit mehreren Transit Gateways empfehlen wir, dass Sie für jedes Ihrer Transit Gateways eine eindeutige autonome Systemnummer (ASN) verwenden. Sie können auch interregionales Peering verwenden. Weitere Informationen finden Sie unter Aufbau eines globalen Netzwerks mithilfe von AWS Transit Gateway regionsübergreifendem Peering.

Arbeiten Sie mit AWS Transit Gateway

Sie können Transit Gateways über die Amazon-VPC-Konsole oder die AWS CLI verwenden. Informationen zur Aktivierung und Verwaltung der Verschlüsselungsunterstützung für Ihr Transit Gateway finden Sie unterthe section called “Support für Verschlüsselung”.

Themen

Gemeinsam genutzte Transit-Gateways

Sie können AWS Resource Access Manager (RAM) verwenden, um ein Transit-Gateway für VPC-Anlagen kontenübergreifend oder unternehmensweit gemeinsam zu nutzen. AWS Organizations RAM muss aktiviert sein und Ressourcen müssen mit einer Organisation gemeinsam genutzt werden. Weitere Informationen finden Sie unter Ressourcenfreigabe für AWS Organizations aktivieren im AWS RAM -Benutzerhandbuch.

Überlegungen

Berücksichtigen Sie Folgendes, wenn Sie ein Transit Gateway freigeben möchten.

- Ein AWS Site-to-Site VPN Anhang muss in demselben AWS Konto erstellt werden, dem das Transit-Gateway gehört.
- Ein Anhang zu einem Direct Connect-Gateway verwendet eine Transit-Gateway-Zuordnung und kann sich in demselben AWS Konto wie das Direct Connect-Gateway oder in einem anderen Konto als das Direct Connect-Gateway befinden.

Standardmäßig sind Benutzer nicht berechtigt, AWS RAM Ressourcen zu erstellen oder zu ändern. Um Benutzern zu erlauben, Ressourcen zu erstellen oder zu ändern und Aufgaben durchzuführen, müssen Sie IAM-Richtlinien erstellen, die Berechtigungen gewähren, bestimmte Ressourcen und API-Aktionen zu nutzen. Ordnen Sie dann diese Richtlinien den IAM-Benutzern oder -Gruppen zu, die diese Berechtigungen benötigen.

Nur der Ressourcen-Besitzer kann die folgenden Vorgänge ausführen:

- Erstellen einer Ressourcen-Freigabe
- Aktualisieren einer Ressourcen-Freigabe
- Anzeigen einer Ressourcen-Freigabe
- Anzeigen der von Ihrem Konto freigegebenen Ressourcen innerhalb aller Ressourcen-Freigaben
- Anzeigen der Pinzipale, für die Sie Ihre Ressourcen freigeben, innerhalb aller Ressourcen-Freigaben. Durch Anzeigen der Prinzipale, für die Sie Ressourcen freigeben, können Sie bestimmen, wer Zugriff auf Ihre freigegebenen Ressourcen hat.
- Löschen einer Ressourcen-Freigabe
- Führen Sie alle APIs für Transit Gateways, Transit-Gateway-Anhänge und Transit-Gateway-Routing-Tabellen aus.

Sie können die folgenden Operationen für Ressourcen ausführen, die für Sie freigegeben sind:

- Annehmen oder Ablehnen einer Einladung zur Ressourcen-Freigabe
- Anzeigen einer Ressourcen-Freigabe
- Anzeigen der freigegebenen Ressourcen, auf die Sie Zugriff haben
- Anzeigen einer Liste aller der Prinzipale, die Ressourcen für Sie freigeben. Sie können sehen, welche Ressourcen und Ressourcen-Freigaben sie für Sie freigegeben haben.
- Ausführen der `DescribeTransitGateways`-API
- Ausführen der APIs, die in ihren VPCs Anhänge erstellen und beschreiben, beispielsweise `CreateTransitGatewayVpcAttachment` und `DescribeTransitGatewayVpcAttachments`.

- Verlassen einer Ressourcen-Freigabe

Wenn ein Transit Gateway für Sie freigegeben wurde, können Sie seine Transit-Gateway-Routing-Tabellen oder dessen Transit-Gateway-Routing-Tabellenpropagationen und -zuordnungen erstellen, ändern oder löschen.

Wenn Sie ein Transit Gateway erstellen, wird das Transit Gateway in der Availability Zone erstellt, die Ihrem Konto zugeordnet und unabhängig von anderen Konten ist. Wenn sich das Transit Gateway und die Anhangs-Entitäten in verschiedenen Konten befinden, können Sie die Availability Zone mithilfe der Availability Zone-ID eindeutig und konsistent identifizieren. Beispielsweise ist use1-az1 eine AZ-ID für die Region us-east-1 und wird in jedem Konto demselben Standort zugeordnet. AWS

Aufheben der Freigabe eines Transit Gateways

Wenn der Besitzer der Freigabe die Freigabe des Transit Gateways aufhebt, gelten die folgenden Regeln:

- Der Transit-Gateway-Anhang funktioniert weiterhin.
- Das freigegebene Konto kann das Transit Gateway nicht beschreiben.
- Der Besitzer des Transit Gateways und der Freigabe-Besitzer sind zum Löschen des Transit-Gateway-Anhangs berechtigt.

Wenn die gemeinsame Nutzung eines Transit-Gateways mit einem anderen AWS Konto aufgehoben wird oder wenn das AWS Konto, mit dem das Transit-Gateway gemeinsam genutzt wird, aus der Organisation entfernt wird, hat dies keine Auswirkungen auf das Transit-Gateway selbst.

Gemeinsam genutzte Subnetze

Ein VPC-Besitzer kann ein Transit-Gateway an das gemeinsam genutzte VPC-Subnetz anfügen. Die Teilnehmer können es nicht. Der Datenverkehr von den Ressourcen des Teilnehmers kann die Anhänge verwenden, abhängig von den Routen, die der VPC-Besitzer im gemeinsam genutzten VPC-Subnetz eingerichtet hat.

Weitere Informationen finden Sie unter Freigeben Ihrer VPC für andere Konten im Amazon-VPC-Benutzerhandbuch.

Transit-Gateways im AWS Transit Gateway

Ein Transit-Gateway ermöglicht es Ihnen, VPCs VPN-Verbindungen herzustellen und den Verkehr zwischen ihnen weiterzuleiten. Ein Transit-Gateway funktioniert überall AWS-Konten, und Sie können es verwenden, AWS RAM um Ihr Transit-Gateway mit anderen Konten zu teilen. Nachdem Sie ein Transit-Gateway mit einem anderen geteilt haben AWS-Konto VPCs , kann der Kontoinhaber es mit Ihrem Transit-Gateway verknüpfen. Benutzer in einem der Konten können die Anhang jederzeit löschen.

Sie können Multicast auf einem Transit Gateway aktivieren und dann eine Transit Gateway-Multicast-Domain erstellen, mit der Multicast-Datenverkehr von der Multicast-Quelle über VPC-Anhängen, die Sie der Domain zuordnen, an Multicast-Gruppenmitglieder gesendet werden kann.

Jede VPC- oder VPN-Anhang ist einer einzigen Routing-Tabelle zugeordnet. Diese Routing-Tabelle bestimmt den nächsten Hop für Datenverkehr, der von diesem Ressourcen-Anhang kommt. Eine Routentabelle innerhalb des Transit-Gateways ermöglicht sowohl als auch IPv4 Ziele. IPv6 CIDRs Die Ziele sind VPCs und VPN-Verbindungen. Wenn Sie eine VPC anhängen oder eine VPN-Verbindung auf einem Transit Gateway erstellen, wird der Anhang der Standard-Routing-Tabelle des Transit-Gateways zugeordnet.

Sie können zusätzliche Routing-Tabellen innerhalb des Transit Gateways erstellen und die VPC- oder VPN-Zuordnung auf diese Routing-Tabellen umstellen. Das ermöglicht Ihnen die Segmentierung Ihres Netzwerks. Sie können beispielsweise die Entwicklung VPCs einer Routentabelle und die Produktion VPCs einer anderen Routentabelle zuordnen. Auf diese Weise können Sie isolierte Netzwerke innerhalb eines Transit-Gateways erstellen, die dem virtuellen Routing und der Weiterleitung (VRFs) in herkömmlichen Netzwerken ähneln.

Transit-Gateways unterstützen dynamisches und statisches Routing zwischen verbundenen Verbindungen VPCs und VPN-Verbindungen. Sie können die Route-Propagierung für jeden Anhang aktivieren oder deaktivieren. VPN Concentrator-Anhänge unterstützen nur BGP-Routing (dynamisches). Transit-Gateway-Peering-Anhänge unterstützen nur statisches Routing. Sie können Routen in den Routentabellen des Transit-Gateways auf den Peering-Anhang verweisen, um den Verkehr zwischen den Peering-Gateways weiterzuleiten.

Sie können Ihrem Transit-Gateway optional einen oder mehrere IPv4 oder IPv6 CIDR-Blöcke zuordnen. Sie geben eine IP-Adresse aus dem CIDR-Block an, wenn Sie einen Transit-Gateway-Connect-Peer für einen Transit-Gateway-Connect-Anhang einrichten. Sie können jeden öffentlichen oder privaten IP-Adressbereich zuordnen, mit Ausnahme von Adressen im `169.254.0.0/16`

Bereich und Bereichen, die sich mit den Adressen für Ihre VPC-Anhänge und On-Premises-Netzwerke überschneiden. Weitere Informationen zu IPv4 und IPv6 CIDR-Blöcken finden Sie unter IP-Adressierung im Amazon VPC-Benutzerhandbuch.

Aufgaben

- Erstellen Sie ein Transit-Gateway in AWS Transit Gateway
- Transit-Gateway-Informationen in AWS Transit Gateway anzeigen
- Transit-Gateway-Tags in AWS Transit Gateway verwalten
- Ändern Sie ein Transit-Gateway in AWS Transit Gateway
- Akzeptieren Sie eine AWS Transit Gateway Gateway-Ressourcenfreigabe mithilfe der AWS Resource Access Manager Konsole
- Akzeptieren Sie einen geteilten Anhang in AWS Transit Gateway
- Löschen Sie ein Transit-Gateway in AWS Transit Gateway
- Verschlüsselungsunterstützung für AWS Transit Gateway

Erstellen Sie ein Transit-Gateway in AWS Transit Gateway

Wenn Sie ein Transit-Gateway erstellen, erstellen wir eine Standard-Transit-Gateway-Routing-Tabelle und verwenden sie als Standard-Zuordnungs-Routing-Tabelle und als standardmäßige Route-Propagierung-Tabelle. Wenn Sie die Standard-Transit-Gateway-Routing-Tabelle nicht erstellen möchten, können Sie später eine erstellen. Weitere Informationen über Routen und Routing-Tabellen finden Sie unter ???.

> **Note**
>
> Wenn Sie die Verschlüsselungsunterstützung auf einem Transit-Gateway aktivieren möchten, können Sie sie bei der Erstellung des Gateways nicht aktivieren. Nachdem Sie das Transit-Gateway erstellt haben und es sich im Status „Verfügbar“ befindet, können Sie es ändern, um die Verschlüsselungsunterstützung zu aktivieren. Weitere Informationen finden Sie unter the section called “Support für Verschlüsselung”.

So erstellen Sie ein Transit Gateway mit der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.

2. Klicken Sie im Navigationsbereich auf Transit Gateways.
3. Wählen Sie Create Transit Gateway (Transit Gateway erstellen) aus.
4. Geben Sie für Name tag (Namens-Tag) optional einen Namen für das Transit Gateway ein. Ein Namens-Tag kann die Identifizierung eines bestimmten Gateways in der Liste von Gateways erleichtern. Wenn Sie ein Name tag (Namens-Tag) hinzufügen, wird ein Tag mit dem Schlüssel Name und einem Wert erstellt, der dem von Ihnen eingegebenen Wert entspricht.
5. Geben Sie im Feld Description (Beschreibung) optional eine Beschreibung für das Transit Gateway ein.
6. Belassen Sie für Amazon side Autonomous System Number (ASN) (Amazon-seitige ASN) entweder den Standardwert, um die standardmäßige ASN zu verwenden, oder geben Sie die private ASN für Ihr Transit Gateway ein. Dies sollte die ASN für die AWS Seite einer Border Gateway Protocol (BGP) -Sitzung sein.

   Für 16-Bit-ASNs liegt der Bereich zwischen 64 512 und 65 534.

   Für 32-Bit-ASNs liegt der Bereich zwischen 4 200 000 000 und 4 294 967 294.

   Für eine Multiregion-Bereitstellung empfehlen wir die Verwendung einer eindeutigen ASN für jedes Ihrer Transit Gateways.
7. Bei DNS support (DNS-Unterstützung) wählen Sie diese Option aus, wenn die VPC bei Abfragen von Instances in einer anderen VPC, die dem Transit Gateway angefügt ist, öffentliche IPv4-DNS-Hostnamen in private IPv4-Adressen auflösen soll.
8. Um die Referenzierung von Sicherheitsgruppen zu unterstützen, aktivieren Sie diese Funktion, um auf eine Sicherheitsgruppe für alle VPCs zu verweisen, die an ein Transit-Gateway angeschlossen sind. Weitere Informationen zur Referenzierung von Sicherheitsgruppen finden Sie unter. the section called “Referenzierung von Sicherheitsgruppen”
9. Wählen Sie diese Option bei VPN ECMP support (VPN-ECMP-Unterstützung), wenn ECMP-Routing (Equal Cost Multipath-Routing) zwischen VPN-Tunnel unterstützt werden soll. Wenn Verbindungen die gleichen CIDRs angeben, wird der Datenverkehr gleichmäßig zwischen ihnen aufgeteilt.

   Wenn Sie diese Option auswählen, müssen die angekündigte BGP ASN und dann die BGP-Attribute wie die identisch AS-path sein.

> **Note**
>
> Zur Verwendung von ECMP müssen Sie eine VPN-Verbindung herstellen, die dynamisches Routing nutzt. VPN-Verbindungen, die statisches Routing nutzen, unterstützen ECMP nicht.

10. Wählen Sie diese Option für Default route table association (Standard-Routing-Tabellenzuordnung), damit Transit-Gateway-Anhänge automatisch der Standard-Routing-Tabelle für das Transit Gateway zugeordnet werden.
11. Wählen Sie diese Option für Default route table propagation (standardmäßige Route-Propagierung-Tabellenverbreitung), damit Transit-Gateway-Anhänge automatisch auf die Standard-Routing-Tabelle für das Transit Gateway übertragen werden.
12. (Optional) Um das Transit Gateway als Router für Multicast-Datenverkehr zu verwenden, wählen Sie Multicast support (Multicast-Unterstützung) aus.
13. (Optional) Wählen Sie im Bereich „Configure-cross-account Freigabeoptionen“ aus, ob gemeinsam genutzte Anlagen automatisch akzeptiert werden sollen. Wenn diese Option aktiviert ist, werden Anlagen automatisch akzeptiert. Andernfalls müssen Sie Anhangsanforderungen annehmen oder ablehnen.

    Wählen Sie diese Option für Auto accept shared attachments (Gemeinsame Anhänge automatisch akzeptieren), um kontoübergreifende Anhänge automatisch zu akzeptieren.
14. (Optional) Geben Sie für CIDR-Blöcke mit Transit Gateway einen oder mehrere IPv4- oder IPv6-CIDR-Blöcke für Ihr Transit Gateway an.

    Sie können einen CIDR-Block der Größe /24 oder größer (z. B. /23 oder /22) für IPv4 oder einen CIDR-Block der Größe /64 oder größer (z. B. /63 oder /62) für IPv6 angeben. Sie können jeden öffentlichen oder privaten IP-Adressbereich zuordnen, mit Ausnahme von Adressen in der 169.254.0. 0/16 Bereich und Bereiche, die sich mit den Adressen für Ihre VPC-Anlagen und lokalen Netzwerke überschneiden.

    > **Note**
    >
    > CIDR-Blöcke des Transit-Gateways werden verwendet, wenn Sie Connect (GRE) - Anhänge, PrivateIP-VPNs oder Client-VPN-Anhänge konfigurieren. Transit Gateway

weist IPs für die Tunnelendpunkte (GRE/PrivateIP VPN) und Client-VPN-Anhänge aus diesem Bereich zu.

15. Wählen Sie Create Transit Gateway (Transit Gateway erstellen) aus.

Um ein Transit-Gateway mit dem zu erstellen AWS CLI

Verwenden Sie den Befehl create-transit-gateway.

Transit-Gateway-Informationen in AWS Transit Gateway anzeigen

Sehen Sie sich eines Ihrer Transit-Gateways an.

So zeigen Sie ein Transit-Gateway mithilfe der Konsole an

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateways. Details für das Transit-Gateway werden unter der Liste der Gateways auf der Seite angezeigt.

Um ein Transit-Gateway mit dem anzuzeigen AWS CLI

Verwenden Sie den describe-transit-gateways-Befehl.

Transit-Gateway-Tags in AWS Transit Gateway verwalten

Fügen Sie Ihren Ressourcen-Tags hinzu, um sie einfacher ordnen und identifizieren zu können, beispielsweise nach Zweck, Besitzer oder Umgebung. Sie können jedem Transit Gateway mehrere Tags hinzufügen. Tag-Schlüssel müssen für jedes Transit Gateway eindeutig sein. Wenn Sie ein Tag mit einem Schlüssel hinzufügen, der dem Transit Gateway bereits zugeordnet ist, ändert sich der Wert dieses Tags. Weitere Informationen finden Sie unter Taggen Ihrer EC2 Amazon-Ressourcen.

Hinzufügen von Tags zu einem Transit Gateway mit der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateways.
3. Wählen Sie das Transit-Gateway aus, für das Sie Tags hinzufügen oder bearbeiten möchten.
4. Wählen Sie die Registerkarte Tags im unteren Bereich der Seite aus.
5. Wählen Sie Tags verwalten aus.

6. Wählen Sie Neues Tag hinzufügen aus.
7. Geben Sie einen Key (Schlüssel) und einen Value (Wert) für das Tag ein.
8. Wählen Sie Speichern.

Ändern Sie ein Transit-Gateway in AWS Transit Gateway

Sie können die Konfigurationsoptionen für ein Transit-Gateway ändern. Wenn Sie ein Transit-Gateway ändern, kommt es bei allen vorhandenen Transit-Gateway-Anhängen nicht zu Betriebsunterbrechungen.

Sie können kein Transit Gateway ändern, der für Sie freigegeben wurde.

Sie können einen CIDR-Block für das Transit-Gateway nicht entfernen, wenn eine der IP-Adressen derzeit für einen Connect-Peerverwendet wird.

> **Note**
>
> Transit-Gateways, für die die Verschlüsselungsunterstützung aktiviert ist, können VPCs mit Encryption Controls im Überwachungs- oder Erzwingungsmodus oder an Gateways, für VPCs die Encryption Controls nicht aktiviert ist, angeschlossen werden. VPCs für die Encryption Controls im Erzwingungsmodus aktiviert ist, können NUR Transit-Gateways hinzugefügt werden, für die die Verschlüsselungsunterstützung aktiviert ist. Detailliertere Informationen erhalten Sie unter the section called “Support für Verschlüsselung”.

So ändern Sie ein Transit-Gateway

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateways.
3. Wählen Sie das zu ändernde Transit Gateway aus.
4. Wählen Sie Aktionen, Ändern des Transit Gateways aus.
5. Ändern Sie die Optionen wie benötigt. Wählen Sie anschließend Modify transit gateway (Transit Gateway ändern) aus.

Um Ihr Transit-Gateway mit dem zu ändern AWS CLI

Verwenden Sie den Befehl modify-transit-gateway.

Akzeptieren Sie eine AWS Transit Gateway Gateway-Ressourcenfreigabe mithilfe der AWS Resource Access Manager Konsole

Wenn Sie zu einer Ressourcenfreigabe hinzugefügt wurden, erhalten Sie eine Einladung, um der Ressourcenfreigabe beizutreten. Sie müssen die gemeinsame Nutzung der Ressource über die Konsole AWS Resource Access Manager (AWS RAM) akzeptieren, bevor Sie auf die gemeinsam genutzten Ressourcen zugreifen können.

Akzeptieren einer Ressourcenfreigabe

1. Öffnen Sie die AWS RAM Konsole unter https://console.aws.amazon.com/ram/.
2. Wählen Sie im Navigationsbereich Shared with me (Für mich freigegeben) und Resources shares (Ressourcenfreigaben).
3. Wählen Sie die Ressourcenfreigabe aus.
4. Wählen Sie Accept resource share (Ressourcenfreigabe akzeptieren) aus.
5. Öffnen Sie die Seite Transit Gateways in der Amazon-VPC-Konsole, um das freigegebene Transit Gateway anzuzeigen.

Akzeptieren Sie einen geteilten Anhang in AWS Transit Gateway

Wenn Sie bei der Erstellung Ihres Transit-Gateways die Funktion „Geteilte Anlagen automatisch akzeptieren“ nicht aktiviert haben, müssen Sie kontoübergreifende (gemeinsam genutzte) Dateianhänge entweder über die Amazon VPC-Konsole oder die AWS CLI manuell akzeptieren.

So akzeptieren Sie einen freigegebene Anhang manuell:

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit-Gateway-Anhänge).
3. Wählen Sie den Transit-Gateway-Anhang aus, für den die Annahme aussteht.
4. Wählen Sie Aktionen, Akzeptieren des Transit-Gateway-Anhangs aus.

Um einen gemeinsam genutzten Anhang zu akzeptieren, verwenden Sie AWS CLI

Verwenden Sie den Befehl accept-transit-gateway-vpc-attachment.

Löschen Sie ein Transit-Gateway in AWS Transit Gateway

Ein Transit Gateway mit vorhandenen Anhängen kann nicht gelöscht werden. Um ein Transit Gateway löschen zu können, müssen Sie zunächst alle Anhänge löschen.

So löschen Sie ein Transit Gateway mit der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie das zu löschende Transit Gateway aus.
3. Wählen Sie Aktionen, Löschen des Transit Gateways aus. Geben Sie **`delete`** ein und wählen Sie dann Löschen, um das Löschen zu bestätigen.

Um ein Transit-Gateway mit dem zu löschen AWS CLI

Verwenden Sie den Befehl delete-transit-gateway.

Verschlüsselungsunterstützung für AWS Transit Gateway

Mit Encryption Controls können Sie den Verschlüsselungsstatus der Verkehrsflüsse in Ihrer VPC überprüfen und anschließend die Verschlüsselung während der Übertragung für den gesamten Datenverkehr innerhalb der VPC erzwingen. Wenn sich VPC Encryption Control im Erzwingungsmodus befindet, sind alle Elastic Network Interfaces (ENI) in dieser VPC darauf beschränkt, nur Instances anzuhängen, die AWS Nitro-Verschlüsselung unterstützen. Und nur AWS Dienste, die Daten während der Übertragung verschlüsseln, dürfen sich an Encryption Controls Enforced VPC anhängen. Weitere Informationen zu VPC Encryption Controls finden Sie in dieser Dokumentation.

Transit Gateway Gateway-Verschlüsselungsunterstützung und VPC-Verschlüsselungssteuerung

Mit der Verschlüsselungsunterstützung auf dem Transit Gateway können Sie die Verschlüsselung während der Übertragung für den Datenverkehr zwischen VPCs erzwingen, die an ein Transit Gateway angeschlossen sind. Sie müssen die Verschlüsselungsunterstützung auf dem Transit Gateway manuell aktivieren, indem Sie den Befehl modify-transit-gateway verwenden, um den Verkehr zwischen den VPCs zu verschlüsseln. Nach der Aktivierung durchläuft der gesamte Datenverkehr zu 100% verschlüsselte Verbindungen zwischen VPCs, die sich im Erzwingungsmodus (ohne Ausschlüsse) befinden, über das Transit Gateway. Sie können VPCs, für die Encryption Controls nicht aktiviert ist oder die sich im Überwachungsmodus befinden, auch über ein Transit

Gateway verbinden, für das die Verschlüsselungsunterstützung aktiviert ist. In diesem Szenario verschlüsselt Transit Gateway garantiert den Verkehr bis zum Transit Gateway Gateway-Anhang in der VPC, die nicht im Erzwingungsmodus läuft. Darüber hinaus hängt es von der Instanz ab, an die der Datenverkehr in der VPC gesendet wird, die nicht im Erzwingungsmodus läuft.

Sie können Verschlüsselungsunterstützung nur zu einem vorhandenen Transit-Gateway hinzufügen und nicht, während Sie eines erstellen. Wenn das Transit Gateway in den Status Encryption Support Enabled übergeht, wird es keine Ausfallzeiten auf dem Transit Gateway oder den Anhängen geben. Die Migration ist nahtlos und transparent, ohne dass der Datenverkehr unterbrochen wird. Die Schritte zum Ändern eines Transit-Gateways, um Verschlüsselungsunterstützung hinzuzufügen, finden Sie unterÄndern eines Transit Gateways.

Voraussetzungen

Bevor Sie die Verschlüsselungsunterstützung auf einem Transit-Gateway aktivieren, stellen Sie sicher, dass:

- Das Transit-Gateway hat keine Connect-Anlagen
- Das Transit-Gateway hat keine Peering-Anhänge
- Das Transit-Gateway hat keine Netzwerkfirewall-Anhänge
- Das Transit-Gateway hat keine VPN Concentrator-Anhänge
- Das Transit-Gateway hat keine Client-VPN-Anhänge
- Für das Transit-Gateway sind keine Sicherheitsgruppenreferenzen aktiviert
- Für das Transit-Gateway sind keine Multicast-Funktionen aktiviert

Status der Verschlüsselungsunterstützung

Ein Transit-Gateway kann einen der folgenden Verschlüsselungsstatus haben:

- aktivieren — Das Transit-Gateway aktiviert gerade die Verschlüsselungsunterstützung. Dieser Vorgang kann bis zu 14 Tage dauern.
- aktiviert — Die Verschlüsselungsunterstützung ist auf dem Transit-Gateway aktiviert. Sie können VPC-Anlagen mit erzwungener Encryption Control erstellen.
- Deaktivierung — Das Transit-Gateway ist dabei, die Verschlüsselungsunterstützung zu deaktivieren.
- deaktiviert — Die Verschlüsselungsunterstützung ist auf dem Transit-Gateway deaktiviert.

Regeln für Dateianhänge in Transit Gateway

Wenn für ein Transit-Gateway die Verschlüsselungsunterstützung aktiviert ist, gelten die folgenden Verbindungsregeln:

- Wenn der Verschlüsselungsstatus des Transit-Gateways aktiviert oder deaktiviert ist, können Sie Direct Connect-Anlagen, VPN-Anlagen und VPC-Anlagen erstellen, die sich nicht im Modus Encryption Control Enforced oder Enforced befinden.
- Wenn der Verschlüsselungsstatus des Transit-Gateways aktiviert ist, können Sie VPC-, Direct Connect-Anlagen, VPN-Anlagen und VPC-Anlagen in jedem Encryption Control-Modus erstellen.
- Wenn der Verschlüsselungsstatus des Transit-Gateways deaktiviert ist, können Sie keine neuen VPC-Anlagen mit erzwungener Verschlüsselungskontrolle erstellen.
- Connect-Anlagen, Peering-Anlagen, Network Firewall Firewall-Anlagen, VPN Concentrator-Anlagen, Client-VPN-Anhänge, Sicherheitsgruppenreferenzen und Multicast-Funktionen werden mit Encryption Support nicht unterstützt.

Der Versuch, inkompatible Anhänge zu erstellen, schlägt mit einem API-Fehler fehl.

Amazon VPC-Anlagen in AWS Transit Gateway

Eine Amazon Virtual Private Cloud (VPC-) Verbindung zu einem Transit-Gateway ermöglicht es Ihnen, den Verkehr zu und von einem oder mehreren VPC-Subnetzen weiterzuleiten. Wenn Sie einem Transit Gateway eine VPC anhängen, müssen Sie ein Subnetz aus jeder Availability Zone angeben, die das Transit Gateway für die Weiterleitung des Datenverkehrs verwenden soll. Die angegebenen Subnetze dienen als Eingangs- und Ausgangspunkte für den Transit-Gateway-Verkehr. Der Verkehr kann Ressourcen in anderen Subnetzen innerhalb derselben Availability Zone nur erreichen, wenn für die Transit-Gateway-Anhangssubnetze in ihren Routentabellen, die auf die Zielsubnetze verweisen, entsprechende Routen konfiguriert sind.

Einschränkungen

- Wenn Sie eine VPC an ein Transit Gateway anhängen, können keine Ressourcen in Availability Zones ohne Transit-Gateway-Anhang das Transit Gateway nicht erreichen.

> **Note**
>
> Innerhalb von Availability Zones, die Transit-Gateway-Anlagen haben, wird der Verkehr nur von den spezifischen Subnetzen, die dem Anhang zugeordnet sind, an das Transit-

Gateway weitergeleitet. Wenn es in einer Subnetz-Routentabelle eine Route zum Transit-Gateway gibt, wird der Verkehr nur dann an das Transit-Gateway weitergeleitet, wenn das Transit-Gateway eine Verbindung in einem Subnetz in derselben Availability Zone hat und die Routentabelle des Anhangssubnetzes entsprechende Routen zum beabsichtigten Ziel des Datenverkehrs innerhalb der VPC enthält.

- Ein Transit-Gateway unterstützt keine DNS-Auflösung für benutzerdefinierte DNS-Namen von angehängten VPCs Einrichtungen, die private gehostete Zonen in Amazon Route 53 verwenden. Informationen zur Konfiguration der Namensauflösung für privat gehostete Zonen für alle, die an ein Transit-Gateway VPCs angeschlossen sind, finden Sie unter Zentralisierte DNS-Verwaltung der Hybrid Cloud mit Amazon Route 53 und AWS Transit Gateway.
- Ein Transit-Gateway unterstützt kein Routing zwischen identischen Verbindungen CIDRs oder wenn sich ein CIDR in einem Bereich VPCs mit einem CIDR in einer angeschlossenen VPC überschneidet. Wenn Sie eine VPC an ein Transit-Gateway anhängen und ihr CIDR mit dem CIDR einer anderen VPC, die bereits an das Transit-Gateway angeschlossen ist, identisch ist oder sich mit diesem überschneidet, werden die Routen für die neu hinzugefügte VPC nicht an die Transit-Gateway-Routentabelle weitergegeben.
- Sie können keinen Anhang für ein VPC-Subnetz erstellen, das sich in einer Local Zone befindet. Jedoch können Sie Ihr Netzwerk so konfigurieren, dass Subnetze in der Local Zone eine Verbindung mit einem Transit-Gateway über die übergeordnete Availability Zone herstellen. Weitere Informationen finden Sie unter Verbinden von Subnetzen der Local Zone mit einem Transit Gateway.
- Sie können keinen Transit-Gateway-Anhang erstellen, der nur Subnetze verwendet. IPv6 Subnetze für Transit-Gateway-Anhänge müssen auch Adressen unterstützen. IPv4
- Ein Transit-Gateway muss mindestens einen VPC-Anhang haben, bevor dieses Transit-Gateway zu einer Routing-Tabelle hinzugefügt werden kann.

Anforderungen an die Routentabelle für VPC-Anlagen

Für die korrekte Funktion von Transit-Gateway-VPC-Anhängen sind spezielle Routing-Tabellenkonfigurationen erforderlich:

- Routing-Tabellen für Anhang-Subnetze: Die Subnetze, die dem Transit-Gateway-Anhang zugeordnet sind, müssen Routentabelleneinträge für alle Ziele innerhalb der VPC enthalten, die über das Transit-Gateway erreichbar sein müssen. Dazu gehören Routen zu anderen Subnetzen, Internet-Gateways, NAT-Gateways und VPC-Endpunkten.

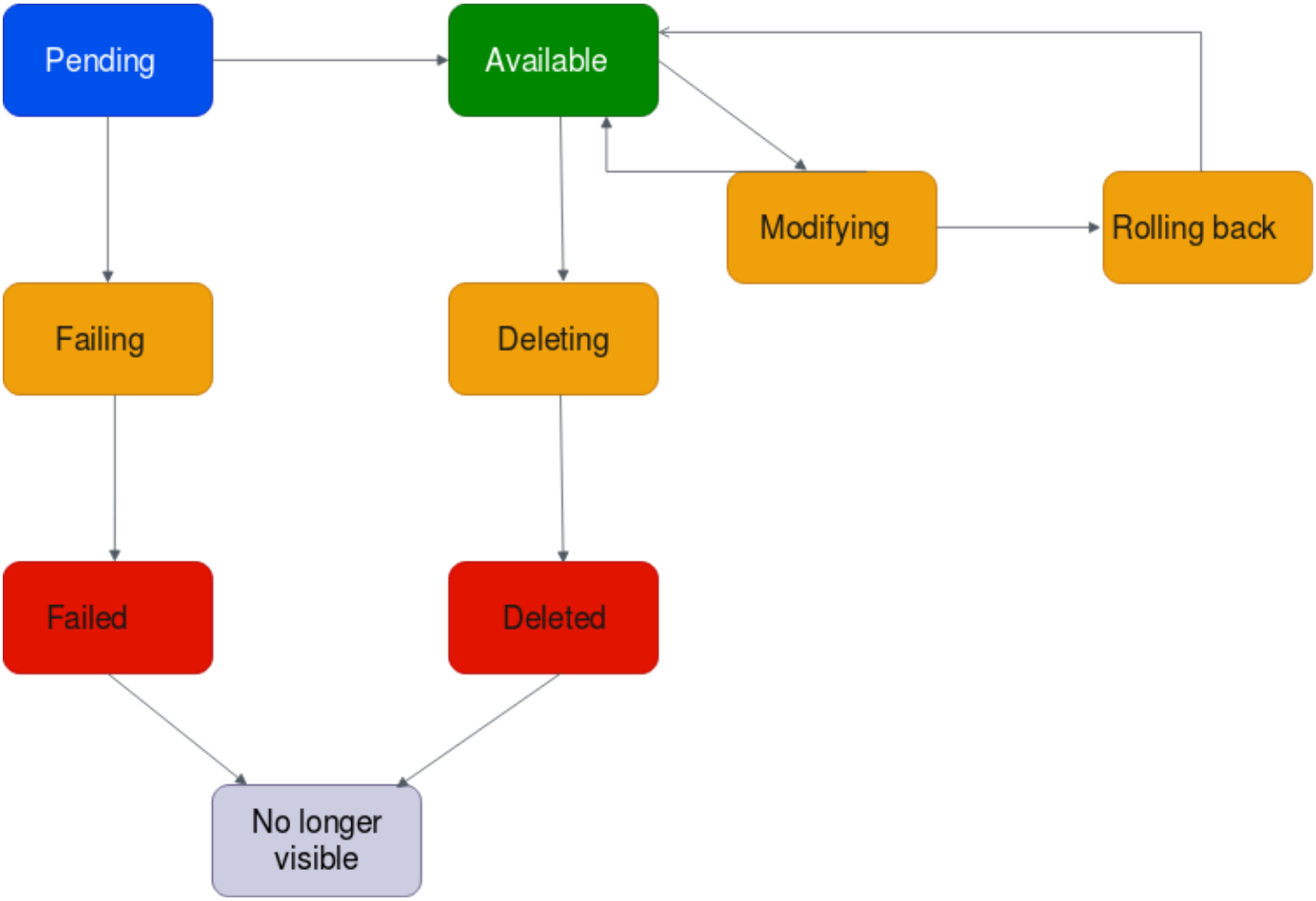
- Routing-Tabellen für Zielsubnetze: Subnetze, die Ressourcen enthalten, die über das Transit-Gateway kommunizieren müssen, müssen über Routen verfügen, die auf das Transit-Gateway verweisen, damit der Verkehr zu externen Zielen zurückgesendet wird.
- Lokaler VPC-Verkehr: Die Transit-Gateway-Verbindung ermöglicht nicht automatisch die Kommunikation zwischen Subnetzen innerhalb derselben VPC. Es gelten die Standard-VPC-Routingregeln, und die lokale Route (VPC CIDR) muss in Routentabellen für die VPC-interne Kommunikation vorhanden sein.

> **Note**
>
> Wenn Routen in Subnetzen ohne Verbindung innerhalb derselben Availability Zone konfiguriert sind, wird der Verkehrsfluss nicht aktiviert. Nur die spezifischen Subnetze, die dem Transit-Gateway-Anhang zugeordnet sind, können als entry/exit Punkte für den Transit-Gateway-Verkehr dienen.

Lebenszyklus von VPC-Anhängen

Eine VPC-Anhang durchläuft verschiedene Phasen, die mit der Einleitung der Anforderung beginnen. In jeder Phase kann es Aktionen geben, die Sie einleiten können. Am Ende Ihres Lebenszyklus bleibt der VPC-Anhang in der Amazon Virtual Private Cloud Console und in der API- oder Befehlszeilenausgabe eine Zeit lang sichtbar.

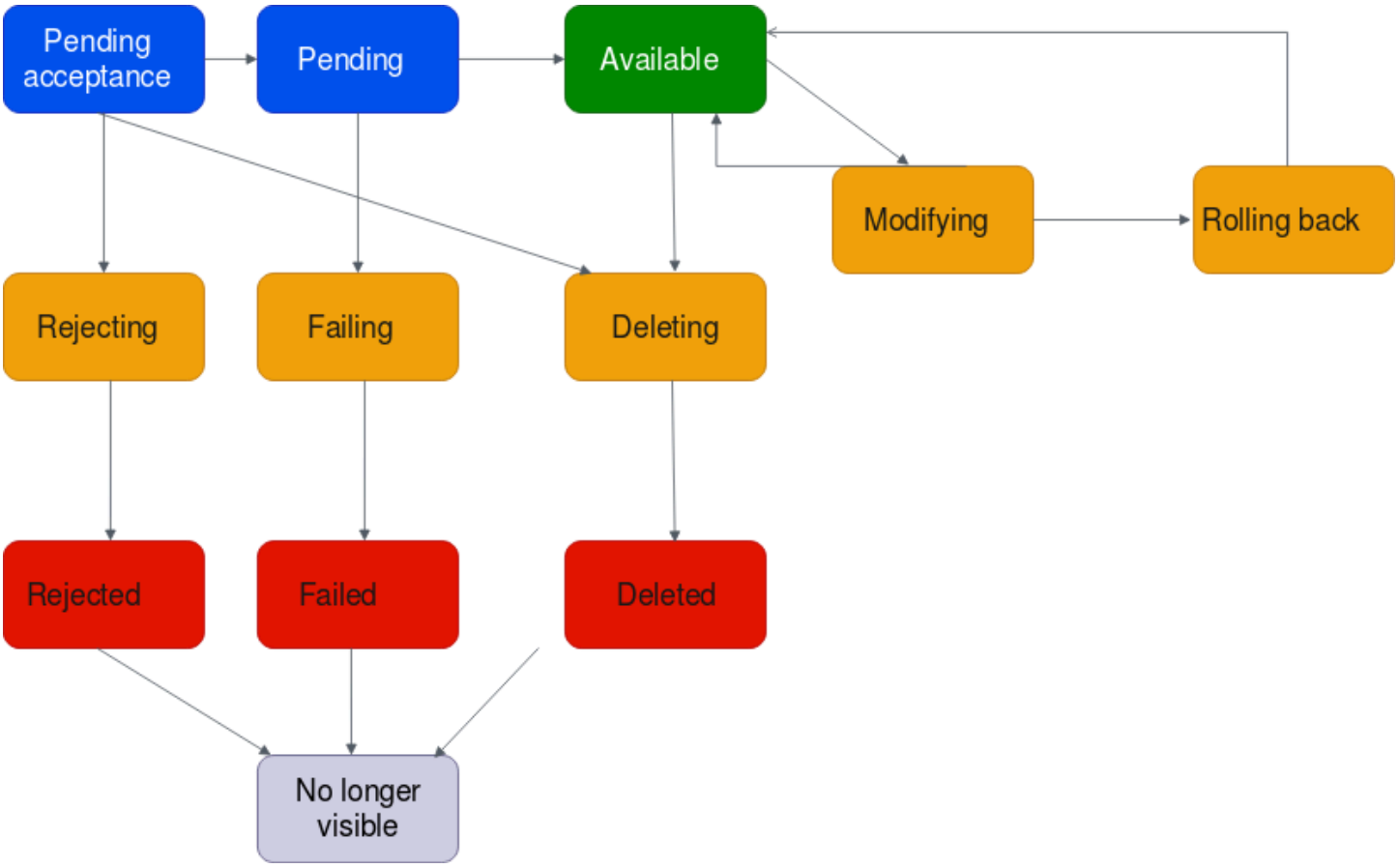
Das folgende Diagramm zeigt die Phasen, die eine Anhang in einer einzelnen Kontokonfiguration oder eine kontoübergreifende Konfiguration durchlaufen kann, bei der Auto accept shared attachments (Gemeinsame Anhänge automatisch akzeptieren) werden aktiviert ist.



- Ausstehend: Eine Anfrage für einen VPC-Anfügung wurde initiiert und befindet sich im Bereitstellungsprozess. In dieser Phase kann eine Anfügung fehlschlagen oder nach `available` verschoben werden.
- Fehlgeschlagen: Eine Anfrage für einen VPC-Anfügung schlägt fehl. In dieser Phase kann die VPC-Anfügung nach `failed` verschoben werden.
- Fehlgeschlagen: Die Anforderung für die VPC-Anfügungen ist fehlgeschlagen. In dieser Phase kann er nicht gelöscht werden. Der fehlgeschlagene VPC-Anhang bleibt 2 Stunden lang sichtbar und ist dann nicht mehr sichtbar.
- Verfügbar: Die VPC-Anfügung ist verfügbar und der Datenverkehr kann zwischen der VPC und dem Transit-Gateway fließen. In dieser Phase kann eine Anfügung fehlschlagen oder nach `modifying` bzw. `deleting` verschoben werden.
- Löschen: Eine VPC-Anfügung , die gerade gelöscht wird. In dieser Phase kann eine Anfügung fehlschlagen oder nach `deleted` verschoben werden.

- Gelöscht: Eine `available`-VPC-Anfügung wurde gelöscht. In dieser Phase kann der VPC-Anhang nicht geändert werden. Der VPC-Anhang bleibt 2 Stunden lang sichtbar und ist dann nicht mehr sichtbar.
- Ändern: Es wurde eine Anfrage zum Ändern der Eigenschaften der VPC-Anfügung gestellt. In dieser Phase kann eine Anfügung fehlschlagen oder nach `available` bzw. `rolling back` verschoben werden.
- Wiederherstellen: Die VPC-Anfügungsanforderung kann nicht abgeschlossen werden, und das System macht alle vorgenommenen Änderungen rückgängig. In dieser Phase kann eine Anfügung fehlschlagen oder nach `available` verschoben werden.

Das folgende Diagramm zeigt die Phasen, die eine Anfügung in einer kontoübergreifenden Konfiguration durchlaufen kann, bei der Auto accept shared attachments (Gemeinsame Anfügungen automatisch akzeptieren) deaktiviert ist.



- Ausstehende Annahme: Die VPC-Anfügungsanfrage wartet auf Annahme. In dieser Phase kann die Anfügung nach `pending`, `rejecting` oder `deleting` verschoben werden.

- Ablehnen: Eine VPC-Anfügung, die gerade abgelehnt wird. In dieser Phase kann eine Anfügung fehlschlagen oder nach `rejected` verschoben werden.
- Abgelehnt: Eine `pending acceptance`-VPC-Anfügung wurde abgelehnt. In dieser Phase kann der VPC-Anhang nicht geändert werden. Der VPC-Anhang bleibt 2 Stunden lang sichtbar und ist dann nicht mehr sichtbar.
- Ausstehend: Die VPC-Anfügung wurde angenommen und befindet sich im Bereitstellungsprozess. In dieser Phase kann eine Anfügung fehlschlagen oder nach `available` verschoben werden.
- Fehlgeschlagen: Eine Anfrage für einen VPC-Anfügung schlägt fehl. In dieser Phase kann die VPC-Anfügung nach `failed` verschoben werden.
- Fehlgeschlagen: Die Anforderung für die VPC-Anfügungen ist fehlgeschlagen. In dieser Phase kann er nicht gelöscht werden. Der fehlgeschlagene VPC-Anhang bleibt 2 Stunden lang sichtbar und ist dann nicht mehr sichtbar.
- Verfügbar: Die VPC-Anfügung ist verfügbar und der Datenverkehr kann zwischen der VPC und dem Transit-Gateway fließen. In dieser Phase kann eine Anfügung fehlschlagen oder nach `modifying` bzw. `deleting` verschoben werden.
- Löschen: Eine VPC-Anfügung , die gerade gelöscht wird. In dieser Phase kann eine Anfügung fehlschlagen oder nach `deleted` verschoben werden.
- Gelöscht: Ein `available`- oder `pending acceptance`-VPC-Anhang wurde gelöscht. In dieser Phase kann der VPC-Anhang nicht geändert werden. Der VPC-Anhang bleibt 2 Stunden sichtbar und ist dann nicht mehr sichtbar.
- Ändern: Es wurde eine Anfrage zum Ändern der Eigenschaften der VPC-Anfügung gestellt. In dieser Phase kann eine Anfügung fehlschlagen oder nach `available` bzw. `rolling back` verschoben werden.
- Wiederherstellen: Die VPC-Anfügungsanforderung kann nicht abgeschlossen werden, und das System macht alle vorgenommenen Änderungen rückgängig. In dieser Phase kann eine Anfügung fehlschlagen oder nach `available` verschoben werden.

Appliance-Modus

Wenn Sie planen, eine statusbehaftete Netzwerk-Appliance in Ihrer VPC zu konfigurieren, können Sie die Appliance-Modus-Unterstützung für den VPC-Anhang aktivieren, in dem sich die Appliance befindet, wenn Sie einen Anhang erstellen. Dadurch wird sichergestellt, dass AWS Transit Gateway während der gesamten Lebensdauer des Datenverkehrs zwischen einer Quelle und einem Ziel dieselbe Availability Zone für diesen VPC-Anhang verwendet. Es ermöglicht einem Transit-Gateway

auch, Datenverkehr an eine beliebige Availability Zone in der VPC zu senden, sofern in dieser Zone eine Subnetzverbindung besteht. Der Appliance-Modus wird zwar nur für VPC-Anlagen unterstützt, der Netzwerkfluss kann jedoch von jedem anderen Transit-Gateway-Anhangstyp stammen, einschließlich VPC-, VPN- und Connect-Anhängen. Der Appliance-Modus funktioniert auch für Netzwerkflüsse mit unterschiedlichen Quellen und Zielen. AWS-Regionen Netzwerkflüsse können möglicherweise zwischen verschiedenen Availability Zones neu verteilt werden, wenn Sie den Appliance-Modus zunächst nicht aktivieren, aber später die Anhangskonfiguration bearbeiten, um ihn zu aktivieren. Sie können den Appliance-Modus entweder über die Konsole, die Befehlszeile oder die API aktivieren oder deaktivieren.

Der Appliance-Modus in AWS Transit Gateway optimiert das Traffic-Routing, indem er bei der Bestimmung des Pfads durch eine VPC im Appliance-Modus die Quell- und Ziel-Availability Zones berücksichtigt. Dieser Ansatz verbessert die Effizienz und reduziert die Latenz. Das Verhalten hängt von der spezifischen Konfiguration und den Datenverkehrsmustern ab. Im Folgenden finden Sie Beispielszenarien.

Szenario 1: Datenverkehrs-Routing innerhalb der Availability Zone über Appliance-VPC

Wenn der Verkehr von der Quell-Availability Zone us-east-1a zur zielseitigen Availability Zone us-east-1a fließt, mit VPC-Anhängen im Appliance-Modus sowohl in us-east-1a als auch us-east-1b, wählt Transit Gateway innerhalb der Appliance-VPC eine Netzwerkschnittstelle von us-east-1a aus. Diese Availability Zone wird für die gesamte Dauer des Datenverkehrs zwischen Quelle und Ziel beibehalten.

Szenario 2: Datenverkehrs-Routing zwischen Availability Zones über Appliance-VPC

Für den Verkehr, der von der Quell-Availability Zone us-east-1a zur Ziel-Availability Zone us-east-1b fließt, mit VPC-Anhängen im Appliance-Modus sowohl in us-east-1a als auch us-east-1b, verwendet Transit Gateway einen Flow-Hash-Algorithmus, um entweder us-east-1a oder us-east-1b in der Appliance-VPC auszuwählen. Die gewählte Availability Zone wird während der gesamten Lebensdauer des Datenflusses konsistent verwendet.

Szenario 3: Weiterleitung des Datenverkehrs über eine Appliance-VPC ohne Availability Zone-Daten

Wenn der Verkehr von der Quell-Availability Zone us-east-1a zu einem Ziel ohne Availability Zone-Informationen (z. B. internetgebundener Verkehr) mit VPC-Anhängen im Appliance-Modus sowohl

in us-east-1a als auch us-east-1b stammt, wählt Transit Gateway innerhalb der Appliance-VPC eine Netzwerkschnittstelle von us-east-1a aus.

Szenario 4: Weiterleitung des Datenverkehrs durch eine Appliance-VPC in einer Availability Zone, die sich entweder von der Quelle oder dem Ziel unterscheidet

Wenn der Verkehr von der Quell-Availability Zone us-east-1a zur Ziel-Availability Zone us-east-1b fließt und VPC-Anhänge im Appliance-Modus in verschiedenen Availability Zones liegen, z. B. us-east-1c und us-east-1d, verwendet Transit Gateway einen Flow-Hash-Algorithmus, um entweder us-east-1c oder us-east-1d in der Appliance-VPC auszuwählen. Die gewählte Availability Zone wird während der gesamten Lebensdauer des Datenflusses konsistent verwendet.

> **Note**
>
> Der Appliance-Modus wird nur für VPC-Anhänge unterstützt. Stellen Sie sicher, dass die Routenverbreitung für eine Routentabelle aktiviert ist, die einem VPC-Anhang der Appliance zugeordnet ist.

Referenzierung von Sicherheitsgruppen

Sie können diese Funktion verwenden, um die Verwaltung von Sicherheitsgruppen und die Kontrolle des instance-to-instance Datenverkehrs zu vereinfachen VPCs , der an dasselbe Transit-Gateway angeschlossen ist. Sie können nur in Regeln für eingehenden Datenverkehr Querverweise auf Sicherheitsgruppen erstellen. Sicherheitsregeln für ausgehende Nachrichten unterstützen keine Verweise auf Sicherheitsgruppen. Mit der Aktivierung oder Verwendung der Sicherheitsgruppenreferenzierung sind keine zusätzlichen Kosten verbunden.

Die Unterstützung von Verweisen auf Sicherheitsgruppen kann sowohl für Transit-Gateways als auch für Transit-Gateway-VPC-Anlagen konfiguriert werden und funktioniert nur, wenn sie sowohl für ein Transit-Gateway als auch für dessen VPC-Anlagen aktiviert wurde.

Einschränkungen

Die folgenden Einschränkungen gelten, wenn Sie die Sicherheitsgruppenreferenzierung mit einem VPC-Anhang verwenden.

- Die Referenzierung von Sicherheitsgruppen wird für Transit-Gateway-Peering-Verbindungen nicht unterstützt. Beide VPCs müssen an dasselbe Transit-Gateway angeschlossen sein.

- Die Referenzierung von Sicherheitsgruppen wird für VPC-Anlagen in der Availability Zone use1-az3 nicht unterstützt.
- Die Referenzierung von Sicherheitsgruppen wird für Endpoints nicht unterstützt. PrivateLink Wir empfehlen die Verwendung von IP-CIDR-basierten Sicherheitsregeln als Alternative.
- Die Referenzierung von Sicherheitsgruppen funktioniert für Elastic File System (EFS), solange für die EFS-Schnittstellen in der VPC eine Sicherheitsgruppenregel „Allow All Egress“ konfiguriert ist.
- Für Local Zone-Konnektivität über ein Transit-Gateway werden nur die folgenden Local Zones unterstützt: 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 und us-west-2-phx-2a.
- Wir empfehlen, diese Funktion auf VPC-Anhangsebene für VPCs Subnetze in nicht unterstützten Local Zones, AWS Outposts und AWS Wavelength Zones zu deaktivieren, da dies zu Dienstunterbrechungen führen kann.
- Wenn Sie über eine Inspektions-VPC verfügen, funktioniert die Referenzierung von Sicherheitsgruppen über das Transit-Gateway nicht über den AWS Gateway Load Balancer oder eine AWS Network Firewall hinweg.

Aufgaben

- Erstellen Sie einen VPC-Anhang in AWS Transit Gateway
- Ändern Sie einen VPC-Anhang in AWS Transit Gateway
- Ändern Sie VPC-Anhangs-Tags in AWS Transit Gateway
- Einen VPC-Anhang in AWS Transit Gateway anzeigen
- Löschen Sie einen VPC-Anhang in AWS Transit Gateway
- AWS Transit Gateway Sicherheitsgruppenregeln für eingehende Nachrichten aktualisieren
- Identifizieren Sie AWS Transit Gateway referenzierte Sicherheitsgruppen
- Entfernen Sie veraltete AWS Transit Gateway Sicherheitsgruppenregeln
- Problembehandlung bei der AWS Erstellung von VPC-Anhängen für Transit Gateway

Erstellen Sie einen VPC-Anhang in AWS Transit Gateway

Erstellen eines VPC-Anhangs mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.

2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit Gateway-Anhänge).
3. Wählen Sie Create Transit Gateway Attachment (Transit-Gateway-Anhang erstellen) aus.
4. Geben Sie für Name tag (Namens-Tag) optional einen Namen für den Transit-Gateway-Anhang ein.
5. Wählen Sie für Transit-Gateway-ID das Transit Gateway für den Anhang aus. Sie können ein Transit Gateway auswählen, das Sie besitzen, oder ein Transit Gateway, das für Sie freigegeben wurde.
6. Wählen Sie bei Attachment type (Anhangstyp) die Option VPC aus.
7. Wählen Sie aus, ob DNS-Support, IPv6Support und Appliance-Modus-Support aktiviert werden sollen.

   Wenn der Appliance-Modus ausgewählt ist, verwendet der Verkehrsfluss zwischen einer Quelle und einem Ziel für die gesamte Lebensdauer dieses Flusses dieselbe Availability Zone für den VPC-Anhang.
8. Wählen Sie aus, ob die Unterstützung für die Referenzierung von Sicherheitsgruppen aktiviert werden soll. Aktivieren Sie diese Funktion, um auf eine Sicherheitsgruppe zu verweisen, die mit einem Transit-Gateway VPCs verbunden ist. Weitere Informationen zur Referenzierung von Sicherheitsgruppen finden Sie unterthe section called “Referenzierung von Sicherheitsgruppen”.
9. Wählen Sie aus, ob IPv6Support aktiviert werden soll.
10. Wählen Sie für VPC ID die VPC aus, die dem Transit-Gateway angefügt werden soll.

    Dieser VPC muss mindestens ein Subnetz zugeordnet sein.
11. Wählen Sie unter Subnetz ein Subnetz für jede Availability Zone aus IDs, das vom Transit-Gateway zur Weiterleitung des Datenverkehrs verwendet werden soll. Sie müssen mindestens ein Subnetz auswählen. Sie können nur ein Subnetz pro Availability Zone auswählen.
12. Wählen Sie Create Transit Gateway Attachment (Transit-Gateway-Anhang erstellen) aus.

So erstellen Sie einen VPC-Anhang mit dem AWS CLI

Verwenden Sie den Befehl create-transit-gateway-vpc-attachment.

Ändern Sie einen VPC-Anhang in AWS Transit Gateway

So zeigen Sie VPC-Anhänge mit der Konsole an

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.

2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit-Gateway-Anhang).
3. Wählen Sie den VPC-Anhang und dann Aktionen, Ändern des Transit-Gateway-Anhangs aus.
4. Aktivieren oder deaktivieren Sie eine der folgenden Optionen:
   - DNS-Unterstützung
   - IPv6 Unterstützung
   - Unterstützung für den Appliance-Modus
5. Um dem Anhang ein Subnetz hinzuzufügen oder daraus zu entfernen, aktivieren oder deaktivieren Sie das Kontrollkästchen neben der Subnetz-ID, die Sie hinzufügen oder entfernen möchten.

   > **Note**
   >
   > Das Hinzufügen oder Ändern eines VPC-Anhangs-Subnetzes kann sich auf den Datenverkehr auswirken, während sich der Anhang in einem Änderungszustand befindet.

6. Um auf eine Sicherheitsgruppe verweisen zu können, die mit einem Transit-Gateway VPCs verbunden ist, wählen Sie Unterstützung für die Referenzierung von Sicherheitsgruppen aus. Weitere Informationen zur Referenzierung von Sicherheitsgruppen finden Sie unter. the section called “Referenzierung von Sicherheitsgruppen”

   > **Note**
   >
   > Wenn Sie die Sicherheitsgruppenreferenzierung für ein vorhandenes Transit-Gateway deaktivieren, wird sie für alle VPC-Anlagen deaktiviert.

7. Wählen Sie Ändern des Transit-Gateway-Anhangs aus.

So ändern Sie Ihre VPC-Anlagen mit dem AWS CLI

Verwenden Sie den Befehl modify-transit-gateway-vpc-attachment.

Ändern Sie VPC-Anhangs-Tags in AWS Transit Gateway

So zeigen Sie VPC-Anhang-Tags mit der Konsole an

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.

2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit-Gateway-Anhang).
3. Wählen Sie den VPC-Anhang und dann Actions (Aktionen), Manage tags (Tags verwalten) aus.
4. [Tag (Markierung) hinzufügen] Wählen Sie Add new tag (Neuen Tag (Markierung) hinzufügen), und führen Sie die folgenden Schritte aus:
   - Geben Sie bei Key (Schlüssel) den Schlüsselnamen ein.
   - Geben Sie bei Value (Wert) den Wert des Schlüssels ein.
5. [Tag entfernen] Wählen Sie neben dem Tag die Option Remove (Entfernen) aus.
6. Wählen Sie Speichern.

VPC-Anhangs-Tags können nur mit der Konsole geändert werden.

Einen VPC-Anhang in AWS Transit Gateway anzeigen

Anzeigen Ihrer VPC-Anhänge mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit-Gateway-Anhang).
3. Suchen Sie in der Spalte Resource type (Ressourcentyp) nach VPC. Dies sind die VPC-Anhänge.
4. Wählen Sie einen Anhang aus, um dessen Details anzuzeigen.

So zeigen Sie Ihre VPC-Anlagen mit dem AWS CLI

Verwenden Sie den Befehl describe-transit-gateway-vpc-attachments.

Löschen Sie einen VPC-Anhang in AWS Transit Gateway

Löschen eines VPC-Anhangs mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit-Gateway-Anhang).
3. Wählen Sie den VPC-Anhang aus.
4. Wählen Sie Aktionen, Löschen des Transit-Gateway-Anhangs aus.
5. Geben Sie bei der Aufforderung **`delete`** ein und wählen Sie Delete (Löschen) aus.

Um einen VPC-Anhang mit dem AWS CLI

Verwenden Sie den Befehl delete-transit-gateway-vpc-attachment.

AWS Transit Gateway Sicherheitsgruppenregeln für eingehende Nachrichten aktualisieren

Sie können alle Sicherheitsgruppenregeln für eingehenden Datenverkehr aktualisieren, die einem Transit-Gateway zugeordnet sind. Sie können Sicherheitsgruppenregeln entweder über die Amazon VPC-Konsolenkonsole oder über die Befehlszeile oder API aktualisieren. Weitere Informationen zur Referenzierung von Sicherheitsgruppen finden Sie unter. the section called “Referenzierung von Sicherheitsgruppen”

So aktualisieren Sie Ihre Sicherheitsgruppenregeln mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Sicherheitsgruppen aus.
3. Wählen Sie die Sicherheitsgruppe aus und klicken Sie auf Aktionen, Regeln für eingehenden Datenverkehr bearbeiten, um die Regeln für eingehenden Datenverkehr zu ändern.
4. Um eine Regel hinzuzufügen, wählen Sie Regel hinzufügen und geben Sie bei Bedarf den Typ, das Protokoll und den Portbereich an. Geben Sie für Quelle (eingehende Regel) die ID der Sicherheitsgruppe in der VPC ein, die mit dem Transit-Gateway verbunden ist.

   > **Note**
   >
   > Sicherheitsgruppen in einer VPC, die mit dem Transit Gateway verbunden ist, werden nicht automatisch angezeigt.

5. Um eine bestehende Regel zu bearbeiten, ändern Sie ihre Werte (z. B. die Quelle oder die Beschreibung).
6. Um eine Regel zu löschen, wählen Sie die Schaltfläche Löschen neben der Regel.
7. Wählen Sie Save rules (Regeln speichern) aus.

So aktualisieren Sie Regeln für eingehenden Datenverkehr über die Befehlszeile

- 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)

Identifizieren Sie AWS Transit Gateway referenzierte Sicherheitsgruppen

Verwenden Sie einen der folgenden Befehle, um festzustellen, ob in den Regeln einer Sicherheitsgruppe in einer VPC, die an dasselbe Transit-Gateway angeschlossen ist, auf Ihre Sicherheitsgruppe verwiesen wird.

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

Entfernen Sie veraltete AWS Transit Gateway Sicherheitsgruppenregeln

Eine veraltete Sicherheitsgruppenregel ist eine Regel, die auf eine gelöschte Sicherheitsgruppe in derselben VPC oder in einer VPC verweist, die mit demselben Transit-Gateway verbunden ist. Wenn eine Sicherheitsgruppenregel veraltet ist, wird sie nicht automatisch aus der Sicherheitsgruppe entfernt – Sie müssen Sie manuell entfernen.

Sie können die veralteten Sicherheitsgruppenregeln einer VPC mit der Amazon VPC-Konsole anzeigen und löschen.

So zeigen Sie veraltete Sicherheitsgruppenregeln an und löschen sie

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Sicherheitsgruppen aus.
3. Klicken Sie auf Actions (Aktionen), Manage stale rules (Verwalten veraltter Regeln).
4. Wählen Sie unter VPC die VPC mit den veraltbaren Regeln aus.
5. Wählen Sie Bearbeiten aus.
6. Wählen Sie die Schaltfläche Löschen neben der Regel, die Sie löschen möchten. Wählen Sie Preview changes (Änderungen überprüfen), Save rules (Regeln speichern).

Um Ihre veralteten Sicherheitsgruppenregeln mithilfe der Befehlszeile zu beschreiben

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

Nachdem Sie die veralteten Sicherheitsgruppenregeln identifiziert haben, können Sie sie mit den Befehlen revoke-security-group-ingressoder revoke-security-group-egresslöschen.

Problembehandlung bei der AWS Erstellung von VPC-Anhängen für Transit Gateway

Das folgende Thema kann Ihnen bei der Behebung von Problemen helfen, die beim Erstellen eines VPC-Anhangs auftreten könnten.

Problem

Der VPC-Anhang ist fehlgeschlagen.

Ursache

Dies kann folgende Ursachen haben:

1. Der Benutzer, der den VPC-Anhang erstellt, hat keine korrekten Berechtigungen zum Erstellen einer serviceverknüpften Rolle.
2. Es gibt ein Problem mit der Drosselung aufgrund zu vieler IAM-Anforderungen. Sie verwenden zum Beispiel CloudFormation , um Berechtigungen und Rollen zu erstellen.
3. Das Konto hat die serviceverknüpfte Rolle, und die serviceverknüpfte Rolle wurde geändert.
4. Das Transit-Gateway befindet sich nicht in der Phase `available`.

Lösung

Versuchen Sie je nach Ursache Folgendes:

1. Stellen Sie sicher, dass der Benutzer über die richtigen Berechtigungen zum Erstellen von serviceverknüpften Rollen verfügt. Weitere Informationen finden Sie unter serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch. Nachdem der Benutzer die Berechtigungen hat, erstellen Sie den VPC-Anhang.
2. Erstellen Sie den VPC-Anhang manuell. Weitere Informationen finden Sie unter the section called “Erstellen Sie einen VPC-Anhang”.
3. Stellen Sie sicher, dass die serviceverknüpfte Rolle die richtigen Berechtigungen hat. Weitere Informationen finden Sie unter the section called “Transit Gateway”.
4. Prüfen Sie, ob das Transit-Gateway sich in der Phase `available` befindet. Weitere Informationen finden Sie unter the section called “Ein Transit-Gateway anzeigen”.

AWS Transit Gateway Gateway-Netzwerkfunktionsanhänge

Sie können einen Netzwerkfunktionsanhang erstellen, mit dem Sie Ihr Transit-Gateway direkt verbinden können AWS Network Firewall. Dadurch entfällt die Notwendigkeit, Inspektionen zu erstellen und zu verwalten VPCs.

Mit einem Firewall-Anhang werden im Hintergrund AWS automatisch alle erforderlichen Ressourcen bereitgestellt und verwaltet. Sie sehen einen neuen Transit-Gateway-Anhang und nicht einzelne Firewall-Endpunkte. Dies vereinfacht den Prozess der Implementierung einer zentralen Inspektion des Netzwerkverkehrs.

Bevor Sie einen Firewall-Anhang verwenden können, müssen Sie den Anhang zunächst in erstellen AWS Network Firewall. Die Schritte zum Erstellen des Anhangs finden Sie unter Erste Schritte mit der AWS Network Firewall Verwaltung im AWS Network Firewall Entwicklerhandbuch. Nachdem die Firewall erstellt wurde, können Sie den Anhang in der Transit Gateway Gateway-Konsole im Abschnitt Anlagen anzeigen. Der Anhang wird mit einer Art von Netzwerkfunktion aufgeführt.

Themen

- Einen AWS Transit Gateway Gateway-Netzwerkfunktionsanhang annehmen oder ablehnen
- AWS Transit Gateway Gateway-Netzwerkfunktionsanhänge anzeigen
- Leiten Sie den Verkehr über einen AWS Transit Gateway Gateway-Netzwerkfunktionsanhang weiter

Einen AWS Transit Gateway Gateway-Netzwerkfunktionsanhang annehmen oder ablehnen

Sie können entweder die Amazon VPC-Konsole oder die AWS Network Firewall CLI oder API verwenden, um einen Transit-Gateway-Netzwerkfunktionsanhang, einschließlich Netzwerk-Firewall-Anhängen, anzunehmen oder abzulehnen. Wenn Sie der Eigentümer eines Transit-Gateways sind und jemand von einem anderen Konto aus einen Firewall-Anhang zu Ihrem Transit-Gateway erstellt hat, müssen Sie die Anhangsanforderung akzeptieren oder ablehnen.

Informationen zum Annehmen oder Ablehnen eines Anhangs mit einer Netzwerkfunktion mithilfe der Netzwerk-Firewall-CLI finden Sie unter `AcceptNetworkFirewallTransitGatewayAttachment` oder `RejectNetworkFirewallTransitGatewayAttachment` APIs in der AWS Network Firewall API-Referenz.

Akzeptieren oder lehnen Sie einen Netzwerkfunktionsanhang über die Konsole ab

Verwenden Sie die Amazon VPC-Konsole, um den Anhang einer Transit-Gateway-Netzwerkfunktion anzunehmen oder abzulehnen.

So akzeptieren oder lehnen Sie einen Netzwerkfunktionsanhang über die Konsole ab

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Transit Gateways aus.
3. Wählen Sie Transit Gateway-Anlagen aus.
4. Wählen Sie den Anhang mit dem Status Ausstehende Annahme und dem Typ Netzwerkfunktion aus.
5. Wählen Sie „Aktionen“ und anschließend entweder „Anlage annehmen“ oder „Anlage ablehnen“.
6. Wählen Sie im Bestätigungsdialogfeld „Annehmen“ oder „Ablehnen“.

Wenn Sie den Anhang akzeptieren, wird er aktiv und die Firewall kann den Datenverkehr überprüfen. Wenn Sie den Anhang ablehnen, wechselt er in den Status Abgelehnt und wird schließlich gelöscht.

AWS Transit Gateway Gateway-Netzwerkfunktionsanhänge anzeigen

Sie können Ihre Netzwerkfunktionsanhänge, einschließlich Ihrer AWS Network Firewall Anlagen, entweder mit der Amazon VPC-Konsole oder der Network Manager-Konsole anzeigen, um eine visuelle Darstellung Ihrer Netzwerktopologie zu erhalten.

Sehen Sie sich mit der Network Manager-Konsole einen Anhang zu Netzwerkfunktionen an

Mit der Network Manager-Konsole können Sie Anlagen zu Netzwerkfunktionen anzeigen.

So zeigen Sie Firewall-Anhänge im Network Manager an

1. Öffnen Sie die Network Manager-Konsole zu https://console.aws.amazon.com/networkmanager/Hause/.
2. Erstellen Sie in Network Manager ein globales Netzwerk, falls Sie noch keines haben.
3. Registrieren Sie Ihr Transit-Gateway bei Network Manager.
4. Wählen Sie unter Globale Netzwerke das globale Netzwerk aus, in dem sich der Anhang befindet.

5. Klicken Sie im Navigationsbereich auf Transit Gateways.
6. Wählen Sie das Transit-Gateway aus, für das Sie Anlagen anzeigen möchten.
7. Wählen Sie Topologie-Baumansicht. Netzwerk-Firewall-Anhänge werden mit einem Netzwerkfunktionssymbol angezeigt.
8. Um Details zu einem bestimmten Firewall-Anhang anzuzeigen, wählen Sie das Transit-Gateway in der Topologieansicht und dann die Registerkarte Netzwerkfunktion aus.

Die Network Manager-Konsole bietet detaillierte Informationen zu Ihren Firewall-Anhängen, einschließlich ihres Status, des zugehörigen Transit-Gateways und der Availability Zones.

Einen Netzwerkfunktionsanhang mit der Amazon VPC-Konsolenkonsole anzeigen

Verwenden Sie die VPC-Konsole, um eine Liste Ihrer Transit-Gateway-Anhangstypen anzuzeigen.

So zeigen Sie Transit-Gateway-Anhangstypen mit der VPC-Konsole an

- Siehe VPC-Anhang anzeigen.

Leiten Sie den Verkehr über einen AWS Transit Gateway Gateway-Netzwerkfunktionsanhang weiter

Nachdem Sie einen Netzwerkfunktionsanhang erstellt haben, müssen Sie Ihre Transit-Gateway-Routentabellen aktualisieren, um den Verkehr entweder mit der Amazon VPC-Konsole oder mithilfe der CLI zur Überprüfung durch die Firewall zu senden. Die Schritte zum Aktualisieren der Zuordnung einer Transit-Gateway-Routentabelle finden Sie unterZuordnen einer Transit-Gateway-Routing-Tabelle.

Leiten Sie den Verkehr mithilfe der Konsole durch einen Firewall-Anhang

Verwenden Sie die Amazon VPC-Konsolenkonsole, um den Datenverkehr über einen Transit-Gateway-Netzwerkfunktionsanhang weiterzuleiten.

Um den Verkehr mithilfe der Konsole über einen Netzwerkfunktionsanhang weiterzuleiten

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Transit Gateways aus.
3. Wählen Sie Transit Gateway-Routentabellen aus.

4. Wählen Sie die Routentabelle aus, die Sie ändern möchten.
5. Wählen Sie Aktionen und dann Statische Route erstellen aus.
6. Geben Sie für CIDR den CIDR-Zielblock für die Route ein.
7. Wählen Sie für Attachment die Netzwerkfunktion Attachment aus. Dies kann beispielsweise ein AWS Network Firewall Anhang sein.
8. Wählen Sie Create static route (Statische Route erstellen) aus.

> **Note**
>
> Es werden nur statische Routen unterstützt.

Datenverkehr, der dem CIDR-Block in Ihrer Routing-Tabelle entspricht, wird nun zur Überprüfung an den Firewall-Anhang gesendet, bevor er an sein endgültiges Ziel weitergeleitet wird.

Leiten Sie den Datenverkehr mithilfe der CLI oder API über einen Netzwerkfunktionsanhang weiter

Verwenden Sie die Befehlszeile oder API, um einen Transit-Gateway-Netzwerkfunktionsanhang weiterzuleiten.

Um den Datenverkehr mithilfe der Befehlszeile oder API durch einen Netzwerkfunktionsanhang weiterzuleiten

- Verwenden Sie `create-transit-gateway-route`.

  Die Anfrage könnte beispielsweise darin bestehen, einen Netzwerk-Firewall-Anhang weiterzuleiten:

```
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
```

  Die Ausgabe gibt dann zurück:

```
{
  "Route": {
    "DestinationCidrBlock": "0.0.0.0/0",
    "TransitGatewayAttachments": [
```

```
      {
        "ResourceId": "network-firewall",
        "TransitGatewayAttachmentId": "tgw-attach-0123456789abcdef0",
        "ResourceType": "network-function"
      }
    ],
    "Type": "static",
    "State": "active"
  }
}
```

Der Datenverkehr, der dem CIDR-Block in Ihrer Routing-Tabelle entspricht, wird nun zur Überprüfung an den Firewall-Anhang gesendet, bevor er an sein endgültiges Ziel weitergeleitet wird.

AWS Site-to-Site VPN Anlagen in AWS Transit Gateway

Sie können einen Site-to-Site VPN-Anhang mit einem Transit-Gateway in AWS Transit Gateway verbinden, sodass Sie Ihre VPCs und lokalen Netzwerke verbinden können. Sowohl dynamische als auch statische Routen werden unterstützt, ebenso IPv4 und IPv6.

Voraussetzungen

- Um eine VPN-Verbindung mit Ihrem Transit-Gateway verbinden zu können, müssen Sie das VPN-Kunden-Gateway angeben, für das spezifische Geräteanforderungen gelten. Bevor Sie einen Site-to-Site VPN-Anhang erstellen, überprüfen Sie die Kunden-Gateway-Anforderungen, um sicherzustellen, dass Ihr Gateway korrekt eingerichtet ist. Weitere Informationen zu diesen Anforderungen, einschließlich Beispieldateien für die Gateway-Konfiguration, finden Sie im AWS Site-to-Site VPN Benutzerhandbuch unter Anforderungen für Ihr Site-to-Site VPN-Kunden-Gateway-Gerät.
- Bei statischen VPNs müssen Sie außerdem zuerst die statischen Routen zur Routentabelle des Transit-Gateways hinzufügen. Statische Routen in einer Transit-Gateway-Routentabelle, die auf eine VPN-Verbindung abzielen, werden vom Site-to-Site VPN nicht gefiltert, da dies einen unbeabsichtigten ausgehenden Datenfluss bei der Verwendung eines VPN ermöglichen könnte. BGP-based Die Schritte zum Hinzufügen einer statischen Route zu einer Routentabelle für Transit-Gateways finden Sie unter. Erstellen einer statischen Route

Sie können einen Site-to-Site Transit-Gateway-VPN-Anhang entweder mit der Amazon VPC-Konsole oder mit der AWS CLI erstellen, anzeigen oder löschen.

Aufgaben

- Erstellen Sie einen Transit-Gateway-Anhang zu einem VPN in AWS Transit Gateway
- Einen VPN-Anhang in AWS Transit Gateway anzeigen
- Löschen Sie einen VPN-Anhang in AWS Transit Gateway

Erstellen Sie einen Transit-Gateway-Anhang zu einem VPN in AWS Transit Gateway

Erstellen eines VPN-Anhangs mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit Gateway-Anhänge).
3. Wählen Sie Create Transit Gateway Attachment (Transit-Gateway-Anhang erstellen) aus.
4. Wählen Sie für Transit-Gateway-ID das Transit Gateway für den Anhang aus. Sie können ein Transit Gateway auswählen, das Ihnen gehört.
5. Wählen Sie bei Attachment type (Anfügungstyp) die Option VPN aus.
6. Wählen Sie bei Customer Gateway (Kunden-Gateway) eine der folgenden Vorgehensweise:
   - Zum Verwenden eines vorhandenen Kunden-Gateways wählen Sie Existing (Vorhanden) und dann das zu verwendende Gateway aus.

     Wenn sich Ihr Kunden-Gateway hinter einem NAT-Gerät (Network Address Translation) befindet, das für NAT-Traversal (NAT-T) aktiviert ist, verwenden Sie die öffentliche IP-Adresse Ihres NAT-Geräts und passen Sie Ihre Firewallregeln an, um den UDP-Port 4500 zu entsperren.
   - Zum Erstellen eines Kunden-Gateways wählen Sie New (Neu) aus. Bei IP Address (IP-Adresse) geben Sie dann eine statische öffentliche IP-Adresse und eine BGP ASN (BGP-ASN) ein.

     Bei Routing options (Routing-Optionen) wählen Sie aus, ob Dynamic (Dynamisch) oder Static (Statisch) verwendet werden soll. Weitere Informationen finden Sie unter Site-to-Site VPN-Routing-Optionen im AWS Site-to-Site VPN Benutzerhandbuch.
7. Geben Sie für Tunnel Options (Tunneloptionen) die CIDR-Bereiche und Pre-Shared-Schlüssel für Ihren Tunnel ein. Weitere Informationen finden Sie unter Site-to-Site VPN-Architekturen.
8. Wählen Sie Create Transit Gateway Attachment (Transit-Gateway-Anhang erstellen) aus.

Um einen VPN-Anhang mit dem zu erstellen AWS CLI

Verwenden Sie den Befehl create-vpn-connection.

Einen VPN-Anhang in AWS Transit Gateway anzeigen

Anzeigen Ihrer VPN-Anhänge mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit-Gateway-Anhang).
3. Suchen Sie in der Spalte Resource type (Ressourcentyp) nach VPN. Dies sind die VPN-Anhänge.
4. Wählen Sie einen Anhang aus, um dessen Details anzuzeigen oder ihm Tags hinzuzufügen.

Um Ihre VPN-Anhänge mit dem anzusehen AWS CLI

Verwenden Sie den Befehl describe-transit-gateway-attachments.

Löschen Sie einen VPN-Anhang in AWS Transit Gateway

Löschen eines VPN-Anhangs mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit-Gateway-Anhang).
3. Wählen Sie den VPN-Anhang aus.
4. Wählen Sie die Ressourcen-ID der VPN-Verbindung aus, um zur Seite VPN Connections (VPN-Verbindungen) zu gelangen.
5. Wählen Sie Actions, Delete.
6. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Delete (Löschen) aus.

Um einen VPN-Anhang mit dem zu löschen AWS CLI

Verwenden Sie den Befehl delete-vpn-connection.

VPN Concentrator-Anhänge im AWS Transit Gateway

AWS Site-to-Site VPN Concentrator ist eine neue Funktion, die die Konnektivität mehrerer Standorte für verteilte Unternehmen vereinfacht. VPN Concentrator eignet sich für Kunden, die mehr als 25 Remote-Standorte verbinden müssen AWS, wobei jeder Standort eine geringe Bandbreite (unter 100 Mbit/s) benötigt.

Wie funktioniert VPN Concentrator

Ein VPN Concentrator erscheint als einzelner Anhang auf Ihrem Transit-Gateway, kann aber mehrere Site-to-Site VPN-Verbindungen hosten.

Der Datenverkehr von allen VPN-Verbindungen auf dem Concentrator wird über denselben Transit-Gateway-Anhang geleitet, sodass Sie konsistente Routing-Richtlinien und Sicherheitsregeln für alle verbundenen Standorte anwenden können. Der Concentrator lässt sich nahtlos in die Routentabellen des Transit-Gateways integrieren, sodass Sie den Verkehrsfluss zwischen Ihren Remote-Standorten und anderen Anhängen VPCs, z. B. anderen VPN-Verbindungen und Peering-Verbindungen, steuern können.

Vorteile von VPN Concentrator

- Kostenoptimierung: Senken Sie die Kosten, indem Sie mehrere VPN-Verbindungen mit niedriger Bandbreite auf einem einzigen Transit-Gateway-Anschluss konsolidieren. Dies ist besonders vorteilhaft, wenn einzelne Standorte nicht die volle VPN-Verbindungskapazität benötigen.
- Vereinfachtes Management: Verwalten Sie mehrere Verbindungen an entfernten Standorten über einen einheitlichen Anhang und behalten Sie gleichzeitig die individuelle Steuerung und Überwachung der VPN-Verbindungen bei.
- Konsistentes Routing: Wenden Sie einheitliche Routing-Richtlinien für alle verbundenen Standorte über eine einzige Transit-Gateway-Routentabellenzuordnung an.
- Skalierbare Architektur: Connect bis zu 100 Remote-Standorte mit einem einzigen Concentrator, der bis zu 5 Concentrators pro Transit-Gateway unterstützt.
- Standard-VPN-Funktionen: Jede VPN-Verbindung unterstützt dieselben Sicherheits-, Überwachungs- und Routing-Funktionen wie Site-to-Site Standard-VPN-Verbindungen.

Anforderungen und Einschränkungen

- Nur BGP-Routing: VPN Concentrator unterstützt nur BGP-Routing (dynamisches). Statisches Routing wird beim Start nicht unterstützt.
- Kunden-Gateway-Anforderungen: Jeder Remote-Standort benötigt ein Kunden-Gateway, das BGP-Routing unterstützt. Bevor Sie VPN-Verbindungen auf einem Concentrator einrichten, überprüfen Sie die Kunden-Gateway-Anforderungen im Abschnitt Anforderungen an Ihr Site-to-Site VPN-Kunden-Gateway-Gerät im AWS Site-to-Site VPN Benutzerhandbuch.
- Überlegungen zur Leistung: Jede VPN-Verbindung auf einem Concentrator ist für eine maximale Bandbreite von 100 Mbit/s ausgelegt. Bei höheren Bandbreitenanforderungen sollten Sie die Verwendung von standardmäßigen Transit-Gateway-VPN-Anhängen in Betracht ziehen.

Sie können einen VPN Concentrator-Anhang entweder mit der AWS VPC-Konsole oder der CLI erstellen, anzeigen oder löschen. AWS Einzelne VPN-Verbindungen auf dem Concentrator werden über die Standard-VPN-Verbindung APIs und die Konsolenschnittstellen verwaltet.

Aufgaben

- Erstellen Sie einen VPN Concentrator-Anhang in AWS Transit Gateway
- Einen VPN Concentrator-Anhang in AWS Transit Gateway anzeigen
- Löschen Sie einen VPN Concentrator-Anhang in AWS Transit Gateway

Erstellen Sie einen VPN Concentrator-Anhang in AWS Transit Gateway

Voraussetzungen

- In Ihrem Konto muss ein vorhandenes Transit-Gateway vorhanden sein.

Um einen VPN Concentrator-Anhang mit der Konsole zu erstellen

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Site-to-Site VPN Concentrators aus.
3. Wählen Sie Create Site-to-Site VPN Concentrator aus.
4. (Optional) Geben Sie als Namenstag einen Namen für Ihren Site-to-Site VPN Concentrator ein.
5. Wählen Sie für Transit-Gateway ein vorhandenes Transit-Gateway aus.
6. (Optional) Um weitere Tags hinzuzufügen, wählen Sie Neues Tag hinzufügen und geben Sie den Schlüssel und den Wert für jedes Tag an.

7. Wählen Sie Create Site-to-Site VPN Concentrator aus.

Nachdem Sie den VPN Concentrator-Anhang erstellt haben, wird er in der Liste der Anlagen mit dem Ressourcentyp VPN Concentrator und dem Anfangsstatus Ausstehend angezeigt. Wenn der Anhang bereit ist, ändert sich der Status in Verfügbar. Sie können dann Site-to-Site VPN-Verbindungen auf diesem Concentrator erstellen.

Um einen VPN Concentrator-Anhang mit dem zu erstellen AWS CLI

Verwenden Sie den Befehl create-vpn-concentrator.

So erstellen Sie mithilfe der Konsole eine VPN-Verbindung auf einem VPN Concentrator

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Site-to-Site VPN-Verbindungen aus.
3. Wählen Sie Create VPN connection (VPN-Verbindung erstellen) aus.
4. Wählen Sie als Target Gateway Type die Option Site-to-Site VPN Concentrator aus.
5. Wählen Sie für Site-to-Site VPN Concentrator den VPN Concentrator aus, für den Sie die VPN-Verbindung herstellen möchten.
6. Wählen Sie bei Customer Gateway (Kunden-Gateway) eine der folgenden Vorgehensweise:
   - Zum Verwenden eines vorhandenen Kunden-Gateways wählen Sie Existing (Vorhanden) und dann das zu verwendende Gateway aus. Stellen Sie sicher, dass das Kunden-Gateway BGP-Routing unterstützt.
   - Um ein Kunden-Gateway zu erstellen, wählen Sie New (Neu) aus. Geben Sie unter IP-Adresse die statische öffentliche IP-Adresse für Ihr Kunden-Gateway-Gerät ein. Geben Sie für BGP ASN die Border Gateway Protocol (BGP) Autonomous System Number (ASN) für Ihr Kunden-Gateway ein.

     Wenn sich Ihr Kunden-Gateway hinter einem NAT-Gerät (Network Address Translation) befindet, das für die NAT-Übersetzung (NAT-T) aktiviert ist, verwenden Sie die öffentliche IP-Adresse Ihres NAT-Geräts und ändern Sie Ihre Firewall-Regeln derart, das die Blockierung des UDP-Ports 4500 aufgehoben wird.
7. Für die Routing-Optionen wird automatisch Dynamisch (erfordert BGP) ausgewählt. VPN Concentrator unterstützt nur dynamisches Routing mit BGP.
8. Wählen Sie für Pre-Shared Key Storage entweder Standard oder Secrets Manager aus.

9. Für die Tunnelbandbreite wird automatisch Standard ausgewählt. VPN Concentrator unterstützt nur Standard-Tunnelbandbreite.
10. Wählen Sie für die IP-Version „Tunnel innerhalb von IP“ entweder IPv4oder IPv6aus.
11. (Optional) Wählen Sie Beschleunigung aktivieren aus, um die Leistung von VPN-Tunneln zu verbessern.
12. (Optional) Geben Sie für CIDR im lokalen IPv4 Netzwerk einen IPv4 CIDR-Bereich an.
13. (Optional) Geben Sie für CIDR im IPv4 Remote-Netzwerk einen CIDR-Bereich an IPv4 .
14. Für den Typ der externen IP-Adresse können Sie entweder Öffentlich IPv4 oder IPv6Adresse auswählen.
15. (Optional) Für Tunneloptionen können Sie Tunneleinstellungen wie interne Tunnel-IP-Adressen und Pre-Shared-Keys konfigurieren. Weitere Informationen finden Sie im AWS Site-to-Site VPN Benutzerhandbuch unter Site-to-Site VPN-Architekturen.
16. (Optional) Um weitere Tags hinzuzufügen, wählen Sie Neues Tag hinzufügen und geben Sie den Schlüssel und den Wert für jedes Tag an.
17. Wählen Sie Create VPN connection (VPN-Verbindung erstellen) aus.

Die VPN-Verbindung wird in der Liste der VPN-Verbindungen mit der VPN Concentrator-ID in der Spalte Transit Gateway Gateway-ID und dem Anfangsstatus Ausstehend angezeigt. Wenn die VPN-Verbindung bereit ist, ändert sich der Status in Verfügbar.

Um eine VPN-Verbindung auf einem VPN Concentrator herzustellen, verwenden Sie AWS CLI

Verwenden Sie den create-vpn-connectionBefehl und geben Sie die VPN Concentrator-ID mithilfe des `--vpn-concentrator-id` Parameters an.

Einen VPN Concentrator-Anhang in AWS Transit Gateway anzeigen

Um Ihre VPN Concentrator-Anhänge über die Konsole anzuzeigen

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit-Gateway-Anhang).
3. Suchen Sie in der Spalte Ressourcentyp nach VPN Concentrator. Dies sind die VPN Concentrator-Anhänge.
4. Wählen Sie einen Anhang aus, um dessen Details anzuzeigen.

Um VPN-Verbindungen auf einem VPN Concentrator mithilfe der Konsole anzuzeigen

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Site-to-Site VPN-Verbindungen aus.
3. Identifizieren Sie in der Liste der VPN-Verbindungen Verbindungen, für die in der Spalte Transit Gateway Gateway-ID eine VPN Concentrator-ID angezeigt wird. Dies sind die VPN-Verbindungen, die auf VPN Concentrators gehostet werden.
4. Wählen Sie eine VPN-Verbindung aus, um deren Details anzuzeigen.

Um Ihre VPN Concentrator-Anhänge anzuzeigen, verwenden Sie den AWS CLI

Verwenden Sie den describe-vpn-concentratorBefehl, um die Details des VPN Concentrators anzuzeigen, oder verwenden Sie den describe-transit-gateway-attachmentsBefehl mit einem Filter für den Ressourcentyp. `vpn-concentrator`

Um VPN-Verbindungen auf einem VPN Concentrator anzuzeigen, verwenden Sie den AWS CLI

Verwenden Sie den describe-vpn-connectionsBefehl mit einem Filter für`vpn-concentrator-id`, um VPN-Verbindungen anzuzeigen, die einem bestimmten Concentrator zugeordnet sind.

Löschen Sie einen VPN Concentrator-Anhang in AWS Transit Gateway

Voraussetzungen

- Alle VPN-Verbindungen auf dem VPN Concentrator müssen gelöscht werden, bevor Sie den Concentrator-Anhang löschen können.
- Stellen Sie sicher, dass Sie Ihre Routing-Konfigurationen aktualisiert haben, um der Entfernung des VPN Concentrators und der zugehörigen VPN-Verbindungen Rechnung zu tragen.

So löschen Sie VPN-Verbindungen auf einem VPN Concentrator mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Site-to-Site VPN-Verbindungen aus.
3. Identifizieren Sie die mit Ihrem VPN Concentrator verknüpften VPN-Verbindungen, indem Sie in der Spalte Transit Gateway ID nach der VPN Concentrator-ID suchen.
4. Wählen Sie eine VPN-Verbindung aus, die Sie löschen möchten.
5. Wählen Sie Actions, Delete.

6. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Delete (Löschen) aus.
7. Wiederholen Sie die Schritte 4-6 für jede VPN-Verbindung, die dem VPN Concentrator zugeordnet ist.

Um einen VPN Concentrator-Anhang mithilfe der Konsole zu löschen

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit-Gateway-Anhang).
3. Wählen Sie den VPN Concentrator-Anhang aus, den Sie löschen möchten. Stellen Sie sicher, dass diesem Concentrator keine VPN-Verbindungen zugeordnet sind.
4. Wählen Sie „Aktionen“, „Anhang löschen“.
5. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Delete (Löschen).

Der VPN Concentrator-Anhang wechselt in den Status Löschen und wird aus Ihrem Konto entfernt. Es kann einige Minuten dauern, bis dieser Vorgang abgeschlossen ist.

Um VPN-Verbindungen auf einem VPN Concentrator zu löschen, verwenden Sie den AWS CLI

Verwenden Sie den delete-vpn-connectionBefehl für jede VPN-Verbindung, die dem VPN Concentrator zugeordnet ist.

Um einen VPN Concentrator-Anhang mit dem zu löschen AWS CLI

Verwenden Sie den delete-vpn-concentratorBefehl, nachdem alle VPN-Verbindungen gelöscht wurden.

Client-VPN-Anhänge im AWS Transit Gateway

Wenn Sie einen Client-VPN-Endpunkt mit einem Transit-Gateway verknüpfen, wird automatisch ein Client-VPN-Anhang erstellt, mit dem Sie den Datenverkehr zwischen Ihren VPCs, lokalen Netzwerken und Client-VPN-Endpunkten weiterleiten können. AWS Transit Gateway unterstützt kontoübergreifende Client-VPN-Anlagen, sodass Konten, mit denen das Transit-Gateway geteilt wird, ihre eigenen Client-VPN-Anlagen erstellen können.

Nachdem der Client-VPN-Endpunkt einem Transit Gateway zugeordnet wurde, können Sie den Anhang in der Transit Gateway-Konsole unter Transit Gateway-Anlagen anzeigen. Der Anhang wird mit einem Client-VPN-Typ aufgeführt.

Anforderungen und Einschränkungen

- Ihrem Transit-Gateway muss ein IPv4- oder IPv6-CIDR-Block zugewiesen sein, bevor Sie einen Client-VPN-Anhang erstellen können.
- Die Weitergabe von Routing-Tabellen muss für Client-VPN-Anlagen aktiviert sein, um Datenverkehr zwischen Ihrem Client-VPN-Endpunkt und dem Transit-Gateway zuzulassen. Siehe Route-Propagierung aktivieren.

Aufgaben

- Erstellen Sie einen Client-VPN-Anhang in AWS Transit Gateway
- Einen Client-VPN-Anhang in AWS Transit Gateway anzeigen
- Löschen Sie einen Client-VPN-Anhang in AWS Transit Gateway
- Einen Client-VPN-Anhang in AWS Transit Gateway akzeptieren oder ablehnen

Erstellen Sie einen Client-VPN-Anhang in AWS Transit Gateway

Voraussetzungen

- In Ihrem Konto muss ein vorhandenes Transit-Gateway vorhanden sein.
- Ihrem Transit-Gateway muss ein IPv4- oder IPv6-CIDR-Block zugewiesen sein.

Ein Client-VPN-Anhang wird automatisch erstellt, wenn Sie einen Client-VPN-Endpunkt mit einem Transit-Gateway verknüpfen.

So erstellen Sie mit der Konsole einen Client-VPN-Anhang

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Client VPN Endpoints aus.
3. Wählen Sie Create Client VPN endpoint (Client-VPN-Endpunkt erstellen) aus.
4. Wählen Sie Transit Gateway als Zuordnungstyp und geben Sie die zu verwendende Transit Gateway Gateway-ID ein.
5. Wählen Sie Create Client VPN endpoint (Client-VPN-Endpunkt erstellen) aus.

Nachdem Sie den Client-VPN-Anhang erstellt haben, wird er in der Liste der Anlagen mit dem Ressourcentyp Client VPN und dem Anfangsstatus Ausstehend angezeigt. Wenn der Anhang

fertig ist, ändert sich der Status in Verfügbar. Wenn sich das Transit-Gateway in einem anderen Konto befindet, lautet der Status des Anhangs solange, bis der Besitzer des Transit-Gateways ihn akzeptiert.

Weitere Informationen zum Erstellen von Client-VPN-Endpunkten finden Sie unter Erste Schritte mit AWS Client VPN.

Um einen Client-VPN-Anhang mit dem zu erstellen AWS CLI

Verwenden Sie den Befehl create-client-vpn-endpoint.

Einen Client-VPN-Anhang in AWS Transit Gateway anzeigen

So zeigen Sie Ihre Client-VPN-Anhänge mit der Konsole an

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Transit Gateways aus.
3. Wählen Sie Transit-Gateway-Anlagen aus.
4. Suchen Sie in der Spalte Ressourcentyp nach Client VPN.
5. Wählen Sie einen Anhang aus, um dessen Details anzuzeigen.

Um Ihre Client-VPN-Anhänge mit dem AWS CLI

Verwenden Sie den Befehl describe-transit-gateway-attachments mit einem Filter für den Ressourcentyp. `client-vpn`

Löschen Sie einen Client-VPN-Anhang in AWS Transit Gateway

So löschen Sie einen Client-VPN-Anhang mit der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Transit Gateways aus.
3. Wählen Sie Transit-Gateway-Anlagen aus.
4. Wählen Sie den Client-VPN-Anhang aus, den Sie löschen möchten.
5. Wählen Sie Aktionen, Löschen des Transit-Gateway-Anhangs aus.
6. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`delete`** ein und wählen Sie Löschen aus.

Der Client-VPN-Anhang wechselt in den Status Löschen und wird aus Ihrem Konto entfernt. Es kann einige Zeit dauern, bis dieser Vorgang abgeschlossen ist.

Um einen Client-VPN-Anhang mit dem AWS CLI

Verwenden Sie den Befehl delete-transit-gateway-client-vpn-attachment.

Einen Client-VPN-Anhang in AWS Transit Gateway akzeptieren oder ablehnen

Wenn ein Client-VPN-Endpunkt in einem anderen Konto einen Anhang zu Ihrem Transit-Gateway erstellt, müssen Sie die Anhangsanforderung akzeptieren oder ablehnen, bevor der Verkehr fließen kann.

So akzeptieren oder lehnen Sie einen Client-VPN-Anhang über die Konsole ab

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Transit Gateways aus.
3. Wählen Sie Transit-Gateway-Anlagen aus.
4. Wählen Sie den Anhang mit dem Status Ausstehende Annahme und dem Typ Client VPN aus.
5. Wählen Sie Aktionen und dann entweder Anhang akzeptieren oder Anhang ablehnen.
6. Wählen Sie im Bestätigungsdialogfeld „Annehmen“ oder „Ablehnen“.

Wenn Sie den Anhang akzeptieren, wird er aktiv und AWS Transit Gateway beginnt mit der Verarbeitung des Datenverkehrs zum und vom Client-VPN-Endpunkt. Wenn Sie den Anhang ablehnen, wechselt er in den Status Abgelehnt und wird schließlich gelöscht.

Um einen Client-VPN-Anhang zu akzeptieren, verwenden Sie den AWS CLI

Verwenden Sie den Befehl accept-transit-gateway-client-vpn-attachment.

Um einen Client-VPN-Anhang abzulehnen, verwenden Sie den AWS CLI

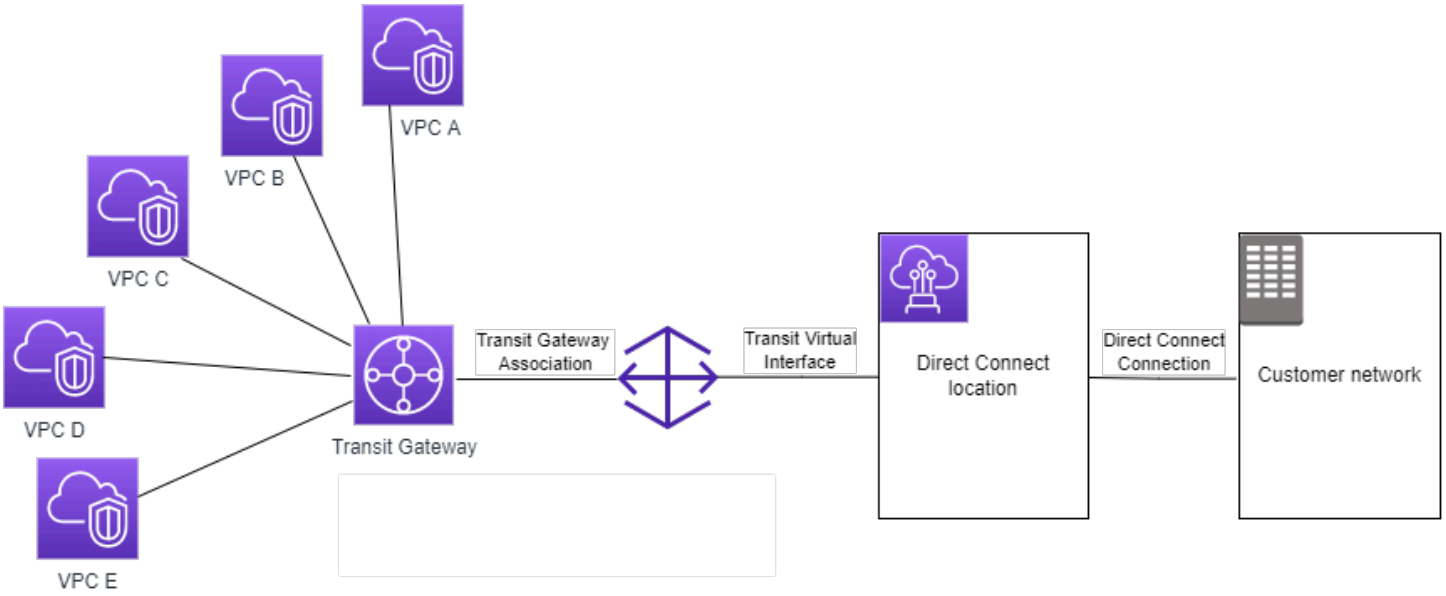
Verwenden Sie den Befehl reject-transit-gateway-client-vpn-attachment.

Transit-Gateway-Anlagen an ein Direct Connect-Gateway in AWS Transit Gateway

Sie können einem Direct-Connect-Gateway mithilfe einer virtuellen Transit-Schnittstelle ein Transit-Gateway anhängen. Diese Konfiguration bietet die folgenden Vorteile. Sie haben folgende Möglichkeiten:

- Verwaltet eine einzelne Verbindung für mehrere Verbindungen VPCs oder Verbindungen VPNs , die sich in derselben Region befinden.
- Kündigen Sie Präfixe von lokal zu AWS und von zu lokal AWS an.

Das folgende Diagramm zeigt, wie Sie mit dem Direct Connect-Gateway eine einzige Verbindung zu Ihrer Direct Connect-Verbindung herstellen können, die alle verwenden VPCs können.



Die Lösung umfasst die folgenden Komponenten:

- Ein Transit Gateway.
- Ein Direct-Connect-Gateway
- Eine Zuordnung zwischen dem Direct-Connect-Gateway und dem Transit Gateway.
- Eine dem Direct-Connect-Gateway angefügte virtuelle Transit-Schnittstelle

Informationen zur Konfiguration von Direct-Connect-Gateways mit Transit Gateways finden Sie unter Transit-Gateway-Zuordnungen im AWS Direct Connect -Direct-Connect-Benutzerhandbuch.

Transit-Gateway-Peering-Anlagen in AWS Transit Gateway

Sie können sowohl regionsinterne als auch regionsübergreifende Transit-Gateways miteinander verbinden und den Verkehr zwischen ihnen weiterleiten, was auch den Datenverkehr einschließt. IPv4 IPv6 Erstellen Sie dazu einen Peering-Anhang auf Ihrem Transit Gateway und geben Sie einen Transit Gateway an. Das Peer-Transit-Gateway kann sich entweder in Ihrem Konto befinden oder von einem anderen Konto stammen. Sie können auch einen Peering-Anhang von Ihrem eigenen Konto an ein Transit-Gateway in einem anderen Konto anfordern.

Nachdem Sie eine Peering-Anhangs-Anforderung erstellt haben, muss der Besitzer des Peer-Transit-Gateways (auch als Accepter Transit Gatewaybezeichnet) die Anforderung akzeptieren. Um Datenverkehr zwischen durch Peering verbundenen Transit Gateways weiterzuleiten, müssen Sie der Transit-Gateway-Routing-Tabelle eine statische Route hinzufügen, die auf den Peering-Anhang des Transit Gateways verweist.

Wir empfehlen, ASNs für jedes Peering-Transit-Gateway ein eigenes zu verwenden, um die Vorteile der future Route-Propagierung zu nutzen.

Das Transit-Gateway-Peering unterstützt nicht die Auflösung von öffentlichen oder privaten IPv4 DNS-Hostnamen in private IPv4 Adressen VPCs auf beiden Seiten der Transit-Gateway-Peering-Verbindung unter Verwendung von in einer anderen Region. Amazon Route 53 Resolver Weitere Informationen zum Route 53 Resolver finden Sie unter Was ist Route 53 Resolver? im Entwicklerhandbuch zu Amazon Route 53.

Interregionales Gateway-Peering verwendet dieselbe Netzwerkinfrastruktur wie VPC-Peering. Daher wird der Datenverkehr mit AES-256-Verschlüsselung auf der virtuellen Netzwerkschicht verschlüsselt, während er zwischen Regionen verläuft. Der Datenverkehr wird auch mit AES-256-Verschlüsselung auf der physischen Ebene verschlüsselt, wenn er Netzwerkverbindungen durchquert, die außerhalb der physischen Kontrolle von AWS liegen. Aus diesem Grund wird der Datenverkehr auf Netzwerkverbindungen, die sich der physischen Kontrolle von entziehen, doppelt verschlüsselt. AWS Innerhalb derselben Region wird der Datenverkehr nur dann auf der physischen Ebene verschlüsselt, wenn er Netzwerkverbindungen durchquert, die außerhalb der physischen Kontrolle von AWS liegen.

Informationen darüber, welche Regionen Transit-Gateway-Peering-Anlagen unterstützen, finden Sie unter AWS Transit Gateways FAQs.

Überlegungen zur Region, für die Sie sich anmelden AWS

Sie können Peering-Verbindungen zwischen Transit Gateways über Opt-In-Regionengrenzen hinweg herstellen. Informationen zu diesen Regionen und dazu, wie Sie sich anmelden können, finden Sie unter AWS Regionen verwalten. Berücksichtigen Sie Folgendes, wenn Sie Transit-Gateway-Peering in diesen Regionen verwenden:

- Sie können ein Peering in einer Opt-in-Region durchführen, solange sich das Konto, das der Peering-Anhang akzeptiert, für diese Region angemeldet ist.
- Teilt unabhängig vom Opt-In-Status der Region AWS die folgenden Kontodaten mit dem Konto, das den Peering-Anhang akzeptiert:
  - AWS-Konto ID
  - Transit-Gateway-ID
  - Regionscode
- Wenn Sie den Transit-Gateway-Anhang löschen, werden die oben genannten Kontodaten gelöscht.
- Wir empfehlen, dass Sie den Peering-Anhang des Transit Gateways löschen, bevor Sie sich von der Region abmelden. Wenn Sie den Peering-Anhang nicht löschen, wird der Datenverkehr möglicherweise weiterhin über den Anhang geleitet und es entstehen weiterhin Gebühren. Wenn Sie den Anhang nicht löschen, können Sie sich wieder anmelden und den Anhang dann löschen.
- Im Allgemeinen verfügt das Transit Gateway über ein Modell, in dem der Sender zahlt. Durch die Verwendung eines Transit-Gateway-Peering-Anhangs über eine Opt-in-Grenze hinweg können Gebühren in einer Region anfallen, die den Anhang akzeptiert, einschließlich der Regionen, für die Sie sich nicht angemeldet haben. Weitere Informationen finden Sie unter AWS -Transit-Gateway-Preise.

Aufgaben

- Erstellen Sie einen Peering-Anhang in AWS Transit Gateway
- Eine Peering-Anhangsanforderung in AWS Transit Gateway annehmen oder ablehnen
- Hinzufügen einer Route zu einer Transit-Gateway-Routentabelle mithilfe von AWS Transit Gateway
- Löschen Sie einen Peering-Anhang in AWS Transit Gateway

Erstellen Sie einen Peering-Anhang in AWS Transit Gateway

Bevor Sie beginnen, stellen Sie sicher, dass Sie über die ID des Transit Gateways verfügen, das Sie anhängen möchten. Wenn sich das Transit-Gateway in einem anderen befindet AWS-Konto, stellen Sie sicher, dass Sie die AWS-Konto ID des Besitzers des Transit-Gateways haben. Nachdem Sie den Peering-Anhang erstellt haben, muss der Besitzer des Transit-Gateways, der die Anlage akzeptiert hat, die Anhangsanforderung annehmen oder ablehnen.

So erstellen Sie einen Peering-Anhang mit der Konsole:

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit Gateway-Anhänge).
3. Wählen Sie Create Transit Gateway Attachment (Transit-Gateway-Anhang erstellen) aus.
4. Wählen Sie für Transit-Gateway-ID das Transit Gateway für den Anhang aus. Sie können ein Transit Gateway auswählen, das Ihnen gehört. Transit-Gateways, die mit Ihnen gemeinsam genutzt werden, sind nicht für Peering verfügbar.
5. Wählen Sie für Attachment type (Anhangstyp) die Option Peering Connection (Peering-Verbindung).
6. Geben Sie optional ein Namen-Tag für den Anhang ein.
7. Führen Sie unter Account (Konto) eine der folgenden Aktionen aus:
   - Wenn sich das Transit Gateway in Ihrem Konto befindet, wählen Sie My account (Mein Konto) aus.
   - Wenn sich das Transit-Gateway in einem anderen befindet AWS-Konto, wählen Sie Anderes Konto. Geben Sie für Konto-ID die AWS-Konto -ID ein.
8. Wählen Sie unter Region die Region aus, in der sich das Transit Gateway befindet.
9. Geben Sie für Transit Gateway (Accepter) die ID des Transit Gateways ein, das Sie anhängen möchten.
10. Wählen Sie Create Transit Gateway Attachment (Transit-Gateway-Anhang erstellen) aus.

Um einen Peering-Anhang mit dem zu erstellen AWS CLI

Verwenden Sie den Befehl create-transit-gateway-peering-attachment.

Eine Peering-Anhangsanforderung in AWS Transit Gateway annehmen oder ablehnen

Bei der Erstellung wird ein Transit-Gateway-Peering-Anhang automatisch in einem bestimmten `pendingAcceptance` Zustand erstellt und verbleibt auf unbestimmte Zeit in diesem Zustand, bis er entweder akzeptiert oder abgelehnt wird. Um den Peering-Anhang zu aktivieren, muss der Besitzer des akzeptierenden Transit-Gateways die Anfrage für den Peering-Anhang akzeptieren, auch wenn beide Transit-Gateways demselben Konto angehören. Akzeptieren Sie die Peering-Anhangs-Anforderung aus der Region, in der sich das Transit Gateway des Empfängers befindet. Wenn Sie den Peering-Anhang ablehnen, müssen Sie alternativ die Anfrage aus der Region ablehnen, in der sich das akzeptierende Transit-Gateway befindet.

So akzeptieren Sie eine Peering-Anhangs-Anforderung über die Konsole:

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit-Gateway-Anhang).
3. Wählen Sie den Peering-Anhang des Transit Gateways aus, für den die Annahme aussteht.
4. Wählen Sie Aktionen, Akzeptieren des Transit-Gateway-Anhangs aus.
5. Fügen Sie die statische Route zur Transit-Gateway-Routing-Tabelle hinzu. Weitere Informationen finden Sie unter the section called “Erstellen einer statischen Route”.

So lehnen Sie eine Peering-Anhangs-Anforderung über die Konsole ab:

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit-Gateway-Anhang).
3. Wählen Sie den Peering-Anhang des Transit Gateways aus, für den die Annahme aussteht.
4. Wählen Sie Aktionen, Ablehnen des Transit-Gateway-Anhangs aus.

Um einen Peering-Anhang anzunehmen oder abzulehnen, verwenden Sie AWS CLI

Verwenden Sie die Befehle accept-transit-gateway-peering-attachment und reject-transit-gateway-peering-attachment.

Hinzufügen einer Route zu einer Transit-Gateway-Routentabelle mithilfe von AWS Transit Gateway

Um Datenverkehr zwischen durch Peering verbundenen Transit Gateways weiterzuleiten, müssen Sie der Routing-Tabelle des Transit Gateways eine statische Route hinzufügen, die auf die Peering-Anlage des Transit Gateways verweist. Der Besitzer des annehmenden Transit Gateways muss auch eine statische Route zur Routing-Tabelle ihres Transit Gateways hinzufügen.

So erstellen Sie eine Route mit der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Route Tables (Transit Gateway-Routing-Tabellen).
3. Wählen Sie die Routing-Tabelle aus, für die eine Route erstellt werden soll.
4. Wählen Sie Actions (Aktionen), Create static route (Statische Route erstellen) aus.
5. Geben Sie auf der Seite Create static route (Statische Route erstellen) den CIDR-Block an, für den die Route erstellt werden soll. Geben Sie beispielsweise den CIDR-Block einer VPC an, die mit dem Peer-Transport-Gateway verbunden ist.
6. Wählen Sie den Peering-Anhang für die Route aus.
7. Wählen Sie Create static route (Statische Route erstellen) aus.

Um eine statische Route mit dem zu erstellen AWS CLI

Verwenden Sie den Befehl create-transit-gateway-route.

> **Important**
>
> Nachdem Sie die Route erstellt haben, muss der Transit-Gateway-Peering-Anhang bereits mit der Transit-Gateway-Routentabelle verknüpft sein. Weitere Informationen finden Sie unter the section called “Zuordnen einer Transit-Gateway-Routing-Tabelle”.

Löschen Sie einen Peering-Anhang in AWS Transit Gateway

Sie können einen Transit-Gateway-Peering-Anhang löschen. Der Besitzer eines der Transit-Gateways kann den Anhang löschen.

So löschen Sie einen Peering-Anhang über die Konsole:

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit-Gateway-Anhänge).
3. Wählen Sie den Peering-Anhang des Transit Gateways aus.
4. Wählen Sie Aktionen, Löschen des Transit-Gateway-Anhangs aus.
5. Geben Sie **`delete`** ein und wählen Sie Delete (Löschen).

Um einen Peering-Anhang mit dem zu löschen AWS CLI

Verwenden Sie den Befehl delete-transit-gateway-peering-attachment.

Connect Anlagen und Connect Peers in AWS Transit Gateway

Sie können einen Transit Gateway Connect-Anhang erstellen, um eine Verbindung zwischen einem Transit-Gateway und virtuellen Appliances von Drittanbietern (z. B. SD-WAN Appliances) herzustellen, die in einer VPC ausgeführt werden. Ein Connect-Anhang unterstützt das Generic Routing Encapsulation (GRE) Tunnelprotokoll für hohe Leistung und das Border Gateway Protocol (BGP) für dynamisches Routing. Nachdem Sie einen Connect-Anhang erstellt haben, können Sie einen oder mehrere GRE-Tunnel (auch Transit-Gateway-Connect-Peersgenannt) in dem Connect-Anhang erstellen, um das Transit Gateway und die Drittanbieter-Appliance zu verbinden. Sie bauen zwei BGP-Sitzungen über den GRE-Tunnel auf, um Routing-Informationen auszutauschen.

> **Important**
>
> Ein Transit Gateway Connect-Peer besteht aus zwei BGP-Peering-Sitzungen, die auf AWS einer verwalteten Infrastruktur enden. Die beiden BGP-Peering-Sitzungen bieten Redundanz der Routingebene und stellen sicher, dass der Verlust einer BGP-Peering-Sitzung Ihren Routing-Vorgang nicht beeinträchtigt. Die von beiden BGP-Sitzungen empfangenen Routing-Informationen werden für den angegebenen Connect-Peer gesammelt. Die beiden BGP-Peering-Sitzungen schützen auch vor AWS -Infrastrukturvorgängen wie routinemäßige Wartung, Patches, Hardware-Upgrades und Austausch. Wenn Ihr Connect-Peer ohne die empfohlene duale BGP-Peering-Sitzung arbeitet, die für Redundanz konfiguriert ist, kann es während des Infrastrukturbetriebs zu einem vorübergehenden Verbindungsverlust kommen. AWS Wir empfehlen dringend, dass Sie beide BGP-Peering-Sitzungen auf Ihrem Connect-Peer konfigurieren. Wenn Sie mehrere Connect-Peers konfiguriert haben, um

Hochverfügbarkeit auf Geräteseite zu unterstützen, empfehlen wir Ihnen, beide BGP-Peering-Sitzungen auf jedem Ihrer Connect-Peers zu konfigurieren.

Ein Connect-Anhang verwendet eine vorhandene VPC- oder einen -Direct-Connect-Anhang als zugrundeliegenden Transportmechanismus. Dies wird als Transport-Anhang bezeichnet. Das Transit Gateway identifiziert übereinstimmende GRE-Pakete der Drittanbieter-Appliance als Datenverkehr aus dem Connect-Anhang. Es behandelt alle anderen Pakete, einschließlich GRE-Pakete mit falschen Quell- oder Zielinformationen, als Datenverkehr aus dem Transport-Anhang.

Note

Um einen Direct Connect-Anhang als Transportmechanismus zu verwenden, müssen Sie Direct Connect zunächst in AWS Transit Gateway integrieren. Die Schritte zum Erstellen dieser Integration finden Sie unter SD-WAN Geräte in AWS Transit Gateway integrieren und Direct Connect.

Connect-Peers

Ein Connect-Peer (GRE-Tunnel) besteht aus folgenden Komponenten.

Innere CIDR-Blöcke (BGP-Adressen)

Die inneren IP-Adressen, die für BGP-Peering verwendet werden. Sie müssen einen /29 CIDR-Block aus dem `169.254.0.0/16` Bereich für IPv4 angeben. Sie können optional einen /125 CIDR-Block aus dem `fd00::/8` Bereich für IPv6 angeben. Die folgenden CIDR-Blöcke sind reserviert und können nicht verwendet werden:

- 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

Sie müssen die erste Adresse aus dem IPv4-Bereich der Appliance als BGP-IP-Adresse konfigurieren. Wenn Sie IPv6 verwenden und Ihr innerer CIDR-Block fd00:: /125 ist, müssen Sie die erste Adresse in diesem Bereich (fd00:: 1) auf der Tunnel-Schnittstelle der Appliance konfigurieren.

Die BGP-Adressen müssen in allen Tunneln eines Transit Gateways eindeutig sein.

Peer-IP-Adressen

Die Peer-IP-Adresse (äußere GRE-IP-Adresse) auf der Appliance-Seite des Connect-Peers. Dies kann eine beliebige IP-Adresse sein. Die IP-Adresse kann eine IPv4- oder IPv6-Adresse sein, muss jedoch von derselben IP-Adressfamilie wie die Transit-Gateway-Adresse sein.

Transit-Gateway-Adresse

Die Peer-IP-Adresse (äußere GRE-IP-Adresse) auf der Transit-Gateway-Seite des Connect-Peers. Die IP-Adresse muss aus dem CIDR-Block des Transit Gateways angegeben werden und für Connect-Anhänge auf dem Transit Gateway eindeutig sein. Wenn Sie keine IP-Adresse angeben, wird die erste verfügbare Adresse aus dem CIDR-Block des Transit Gateways verwendet.

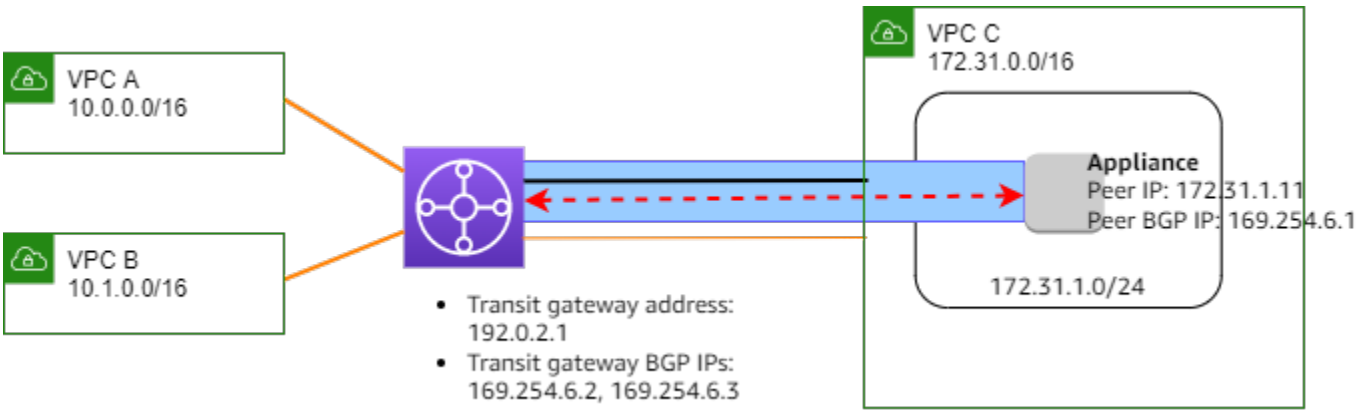
Sie können einen CIDR-Block für das Transit Gateway hinzufügen, wenn Sie ein Transit Gateway erstellen oder ändern .

Die IP-Adresse kann eine IPv4- oder IPv6-Adresse sein, muss jedoch von derselben IP-Adressfamilie sein wie die Peer-IP-Adresse.

Die Peer-IP-Adresse und die Transit-Gateway-Adresse werden verwendet, um den GRE-Tunnel eindeutig zu identifizieren. Sie können beide Adressen für mehrere Tunnel wiederverwenden, aber nicht beide im selben Tunnel.

Transit Gateway Connect für das BGP-Peering unterstützt nur Multiprotocol BGP (MP-BGP), wobei IPv4-Unicast-Adressierung erforderlich ist, um auch eine BGP-Sitzung für IPv6-Unicast einzurichten. Sie können IPv4- und IPv6-Adressen für die äußeren IP-Adressen der GRE verwenden.

Das folgende Beispiel zeigt einen Connect-Anhang zwischen einem Transit Gateway und einer Appliance in einer VPC.



Diagrammkomponente	Description
	VPC-Anhang
	Connect-Anhang
	GRE-Tunnel (Connect-Peer)
	BGP-Peering-Sitzung

Im vorherigen Beispiel wird ein Transit-Gateway-Connect-Anhang auf einem vorhandenen VPC-Anhang (dem Transport-Anhang) erstellt. In der Connect-Anfügung wird ein Connect-Peer erstellt, um eine Verbindung zu einer Appliance in der VPC herzustellen. Die Adresse des Transit Gateways ist `192.0.2.1`, und der Bereich der BGP-Adressen ist `169.254.6.0/29`. Die erste IP-Adresse in dem Bereich (`169.254.6.1`) wird auf der Appliance als Peer-BGP-IP-Adresse konfiguriert.

Die Subnetz-Routing-Tabelle für VPC C umfasst eine Route, die den für den CIDR-Block des Transit Gateways bestimmten Datenverkehr zum Transit Gateway anzeigt.

Zielbereich	Target
172.31.0. 0/16	Local
192,0,2. 0/24	tgw-id

Anforderungen und Überlegungen

Nachfolgend werden Anforderungen und Überlegungen für einen Connect-Anhang aufgeführt:

- Informationen dazu, welche Regionen Connect-Anhänge unterstützen, finden Sie unter AWS – Häufig gestellte Fragen.
- Die Drittanbieter-Appliance muss so konfiguriert sein, dass sie mit dem Connect-Anhang Datenverkehr über einen GRE-Tunnel zum und vom Transit Gateway sendet und empfängt.
- Die Drittanbieter-Appliance muss so konfiguriert sein, dass sie BGP für dynamische Routen-Aktualisierungen und Zustandsprüfungen verwendet.
- Folgende Arten von BGP werden unterstützt:
  - Exterior BGP (eBGP): Wird für die Verbindung mit Routern verwendet, die sich in einem anderen autonomen System befinden als das Transit Gateway. Wenn Sie eBGP verwenden, müssen Sie ebgp-multihop mit einem Time-to-Live-Wert (TTL) von 2 konfigurieren.
  - Interior BGP (iBGP): Wird für die Verbindung mit Routern verwendet, die sich im selben autonomen System wie das Transit Gateway befinden. Das Transit-Gateway installiert keine Routen von einem iBGP-Peer (Drittanbieter-Appliance), es sei denn, die Routen stammen von einem eBGP-Peer und sollten mit next-hop-self konfiguriert sein. Die Routen, die von einer Drittanbieter-Appliance über das iBGP-Peering angekündigt werden, müssen über eine ASN verfügen.
  - MP-BGP (Multiprotokollerweiterungen für BGP): Wird für die Unterstützung mehrerer Protokolltypen wie IPv4- und IPv6-Adressfamilien verwendet.
- Das standardmäßige BGP-Keep-Alive-Timeout beträgt 10 Sekunden und der standardmäßige Hold-Timer beträgt 30 Sekunden.
- IPv6-BGP-Peering wird nicht unterstützt; nur BGP-Peering wird unterstützt. IPv4-based IPv6-Präfixe werden über IPv4-BGP-Peering ausgetauscht. MP-BGP
- Bidirectional Forwarding Detection (BFD) wird nicht unterstützt.
- Der kontrollierte Neustart von BGP wird nicht unterstützt.
- Wenn Sie einen Transit-Gateway-Peer erstellen und keine Peer-ASN-Nummer angeben, wählen wir die ASN-Nummer des Transit Gateways aus. Das bedeutet, dass sich Ihre Appliance und Ihr Transit Gateway im selben autonomen System wie IBGP befinden.
- Ein Connect-Peer, der das AS-PATH BGP-Attribut verwendet, ist die bevorzugte Route, wenn Sie zwei Connect-Peers haben.

Um das ECMP-Routing (Equal-Cost Multi-Path) zwischen mehreren Appliances zu verwenden, müssen Sie die Appliance so konfigurieren, dass sie dem Transit-Gateway dieselben Präfixe mit demselben BGP-Attribut ankündigt. AS-PATH Damit das Transit-Gateway alle verfügbaren ECMP-Pfade auswählen kann, müssen die Nummer AS-PATH und die Autonome Systemnummer (ASN) übereinstimmen. Das Transit-Gateway kann ECMP zwischen Connect-Peers für dieselbe Connect-Anfügung oder zwischen Connect-Anfügungen auf demselben Transit-Gateway verwenden. Für das Transit Gateway ist kein ECMP zwischen den beiden redundanten BGP-Peerings möglich.

- Bei einem Connect-Anhang werden die Routen standardmäßig an eine Transit-Gateway-Routing-Tabelle weitergegeben.
- Statische Routen werden nicht unterstützt.
- Konfigurieren Sie die GRE-Tunnel-MTU so, dass sie kleiner als die MTU der externen Schnittstelle ist, indem Sie den Overhead des GRE-Headers (4 Byte) und des äußeren IP-Headers (20 Byte) subtrahieren. Wenn die MTU Ihrer externen Schnittstelle beispielsweise 1500 Byte beträgt, legen Sie die GRE-Tunnel-MTU auf 1476 Byte (1500 — 4 — 20 = 1476) fest, um eine Paketfragmentierung zu verhindern.

Aufgaben

- Erstellen Sie einen Connect-Anhang in AWS Transit Gateway
- Erstellen Sie einen Connect-Peer in AWS Transit Gateway
- Connect-Anhänge und Connect-Peers in AWS Transit Gateway anzeigen
- Ändern Sie den Connect-Anhang und die Connect-Peer-Tags in AWS Transit Gateway
- Löschen Sie einen Connect-Peer in AWS Transit Gateway
- Löschen Sie einen Connect-Anhang in AWS Transit Gateway

Erstellen Sie einen Connect-Anhang in AWS Transit Gateway

Um einen Connect-Anhang zu erstellen, müssen Sie einen vorhandenen Anhang als Transport-Anhang angeben. Sie können eine VPC-Anfügung oder eine Direct Connect-Anfügung als Transportanfügung angeben.

So erstellen Sie einen Peering-Anhang über die Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit-Gateway-Anhänge).

3. Wählen Sie Create Transit Gateway Attachment (Transit-Gateway-Anhang erstellen) aus.
4. (Optional) Geben Sie unter Name tag (Namens-Tag) einen Namens-Tag für den Anhang an.
5. Wählen Sie für Transit-Gateway-ID das Transit Gateway für den Anhang aus.
6. Wählen Sie bei Attachment type (Anhangstyp) die Option Connect aus.
7. Wählen Sie für die Transport Attachment ID (ID des Transport-Anhangs) die ID eines vorhandenen Anhangs (der Transport-Anhang).
8. Wählen Sie Create Transit Gateway Attachment (Transit-Gateway-Anhang erstellen) aus.

So erstellen Sie einen Connect-Anhang mit dem AWS CLI

Verwenden Sie den create-transit-gateway-connect-Befehl.

Erstellen Sie einen Connect-Peer in AWS Transit Gateway

Sie können einen Connect-Peer (GRE-Tunnel) für eine bestehende Connect-Anfügung erstellen. Stellen Sie zuvor sicher, dass Sie einen CIDR-Block für das Transit Gateway konfiguriert haben. Sie können einen CIDR-Block für Transit Gateways konfigurieren, wenn Sie ein Transit Gateway erstellen oder ändern .

Wenn Sie den Connect-Peer erstellen, müssen Sie die äußere GRE-IP-Adresse auf der Appliance-Seite des Connect-Peers angeben.

So erstellen Sie einen Connect-Peer über die Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit-Gateway-Anhänge).
3. Wählen Sie den Connect-Anhang aus und wählen Sie Actions (Aktionen), Create Connect Peer (Connect-Peer erstellen).
4. (Optional) Geben Sie für Name tag (Namens-Tag) einen Namenstag für den Connect-Peer an.
5. (Optional) Geben Sie für Transit Gateway GRE Address (Transit-Gateway-GRE-Adresse) die äußere GRE-IP-Adresse für das Transit Gateway an. Standardmäßig wird die erste verfügbare Adresse aus dem CIDR-Block des Transit Gateways verwendet.
6. Geben Sie für Peer GRE Address (Peer-GRE-Adresse)die äußere GRE-IP-Adresse für die Appliance-Seite des Connect-Peers an.

7. Geben Sie für BGP Inside CIDR-Blöcke den Bereich der internen IPv4 Adressen an IPv4, die für BGP-Peering verwendet werden. Ein CIDR-Block der Größe /29 aus dem Bereich `169.254.0.0/16`.
8. (Optional) Geben Sie für BGP Inside CIDR-Blöcke den Bereich der internen IPv6 Adressen an IPv6, die für BGP-Peering verwendet werden. Ein CIDR-Block der Größe /125 aus dem Bereich `fd00::/8`.
9. (Optional) Geben Sie für Peer-ASNdie Border Gateway Protocol (BGP) Autonomous System Number (ASN) für die Appliance an. Sie können eine bereits zu Ihrem Netzwerk zugewiesene ASN verwenden. Wenn Sie über keine ASN verfügen, können Sie eine private ASN im Bereich zwischen 64512 und 65534 (16-Bit-ASN) oder 4200000000 und 4294967294 (32-Bit-ASN) verwenden.

   Der Standardwert ist die gleiche ASN wie das Transit Gateway. Wenn Sie die Peer-ASN so konfigurieren, dass sie sich von der Transit-Gateway-ASN (eBGP) unterscheidet, müssen Sie ebgp-multihop mit einem (TTL) -Wert von 2 konfigurieren. time-to-live
10. Wählen Sie Connect Peer erstellen aus.

Um einen Connect-Peer mit dem zu erstellen AWS CLI

Verwenden Sie den Befehl create-transit-gateway-connect-peer.

Connect-Anhänge und Connect-Peers in AWS Transit Gateway anzeigen

Sehen Sie sich Ihre Connect-Anhänge und Connect-Peers an.

So können Sie sich Ihre Connect-Anfügungen und Connect-Peers über die Konsole anzeigen lassen

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit-Gateway-Anhänge).
3. Wählen Sie den Connect-Anhang aus.
4. Um die Connect-Peers für die Anfügung einzusehen, wählen Sie die Registerkarte Connect-Peers.

Um Ihre Connect-Anlagen und Connect-Peers anzuzeigen, verwenden Sie den AWS CLI

Verwenden Sie die Befehle describe-transit-gateway-connectsund describe-transit-gateway-connect-peers.

Ändern Sie den Connect-Anhang und die Connect-Peer-Tags in AWS Transit Gateway

Sie können die Tags für Ihren Connect-Anhang ändern.

So können Sie sich Connect-Anhangs-Tags über die Konsole anzeigen lassen

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit-Gateway-Anhänge).
3. Wählen Sie den Connect-Anhang und dann Actions (Aktionen), Manage tags (Tags verwalten) aus.
4. Um einen Tag hinzuzufügen, wählen Sie Neues Tag hinzufügen und geben Sie den Schlüsselnamen und den Schlüsselwert an.
5. Klicken Sie zum Entfernen eines Tags auf Remove (Entfernen).
6. Wählen Sie Speichern.

Sie können die Tags für Ihren Connect-Peer ändern.

So ändern Sie Ihre Connect Peer-Tags über die Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit-Gateway-Anhänge).
3. Wählen Sie den Connect-Anhang und dann Connect peers (Connect-Peers) aus.
4. Wählen Sie den Connect-Peer aus und wählen Sie dann Actions (Aktionen), Manage tags (Tags verwalten).
5. Um einen Tag hinzuzufügen, wählen Sie Neues Tag hinzufügen und geben Sie den Schlüsselnamen und den Schlüsselwert an.
6. Klicken Sie zum Entfernen eines Tags auf Remove (Entfernen).
7. Wählen Sie Speichern.

Um Ihren Connect-Anhang und Ihre Connect-Peer-Tags mit dem zu ändern AWS CLI

Verwenden Sie die Befehle create-tags und delete-tags.

Löschen Sie einen Connect-Peer in AWS Transit Gateway

Wenn Sie einen Connect-Peer nicht mehr benötigen, können Sie diesen löschen.

So löschen Sie einen Connect-Peer über die Konsole:

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit-Gateway-Anhänge).
3. Wählen Sie den Connect-Anhang aus.
4. Wählen Sie auf der Registerkarte Connect Peers den Connect-Peer aus und wählen Sie Actions (Aktionen), Delete Connect Peer (Connect-Peer löschen).

Um einen Connect-Peer mit dem zu löschen AWS CLI

Verwenden Sie den Befehl delete-transit-gateway-connect-peer.

Löschen Sie einen Connect-Anhang in AWS Transit Gateway

Wenn Sie einen Connect-Anhang nicht mehr benötigen, können Sie ihn löschen. Sie müssen zunächst alle Connect-Peers für die Anfügung löschen.

So löschen Sie einen Peering-Anhang über die Konsole:

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Attachments (Transit-Gateway-Anhänge).
3. Wählen Sie den Connect-Anhang aus und wählen Sie Aktionen, Löschen von Transit-Gateway-Anhang.
4. Geben Sie **`delete`** ein und wählen Sie Delete (Löschen).

Um einen Connect-Anhang mit dem zu löschen AWS CLI

Verwenden Sie den delete-transit-gateway-connect-Befehl.

Transit-Gateway-Routentabellen in AWS Transit Gateway

Verwenden Sie Transit-Gateway-Routing-Tabellen, um die Weiterleitung für Ihre Transit-Gateway-Anhänge zu konfigurieren. Eine Routing-Tabelle ist eine Tabelle, die Regeln enthält, die bestimmen,

wie Ihr Netzwerkverkehr zwischen Ihren VPCs und VPNs weitergeleitet wird. Jede Route in der Tabelle enthält den Bereich der IP-Adressen für die Ziele, an die Sie Datenverkehr senden möchten.

Mithilfe von Transit-Gateway-Routentabellen können Sie eine Tabelle einem Transit-Gateway-Anhang zuordnen. VPC, VPN, VPN Concentrator, Client VPN, Direct Connect Gateway, Peering und Connect-Anhänge werden alle unterstützt. Wenn sie verknüpft sind, werden die Routen für diese Anlagen von der Anlage an die Routentabelle des Ziel-Transit-Gateways weitergegeben. Ein Anhang kann an mehrere Routentabellen weitergegeben werden.

Zusätzlich können Sie statische Routen mit einer Routentabelle erstellen und verwalten. Beispielsweise können Sie über eine statische Route verfügen, die als Backup-Route für den Fall einer Netzwerkunterbrechung verwendet wird, die sich auf dynamische Routen auswirkt.

Aufgaben

- Erstellen Sie eine Transit-Gateway-Routentabelle in AWS Transit Gateway
- Transit-Gateway-Routentabellen mit AWS Transit Gateway anzeigen
- Ordnen Sie eine Transit-Gateway-Routentabelle in AWS Transit Gateway zu
- Löschen Sie eine Zuordnung für eine Transit-Gateway-Routentabelle in AWS Transit Gateway
- Route-Propagierung zu einer Transit-Gateway-Routentabelle in AWS Transit Gateway aktivieren
- Deaktivieren Sie die Routenverbreitung in AWS Transit Gateway
- Erstellen Sie eine statische Route in AWS Transit Gateway
- Löschen Sie eine statische Route in AWS Transit Gateway
- Ersetzen Sie eine statische Route in AWS Transit Gateway
- Exportieren Sie Routentabellen in AWS Transit Gateway nach Amazon S3
- Löschen Sie eine Transit-Gateway-Routentabelle in AWS Transit Gateway
- Erstellen Sie eine Referenz zur Präfixliste einer Routentabelle in AWS Transit Gateway
- Ändern Sie eine Präfixlistenreferenz in AWS Transit Gateway
- Löschen Sie eine Präfixlistenreferenz in AWS Transit Gateway

Erstellen Sie eine Transit-Gateway-Routentabelle in AWS Transit Gateway

So erstellen Sie eine Transit-Gateway-Routing-Tabelle mit der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.

2. Klicken Sie im Navigationsbereich auf Transit Gateway Route Tables (Transit Gateway-Routing-Tabellen).
3. Wählen Sie Create Transit Gateway Route Table (Transit-Gateway-Routing-Tabelle erstellen) aus.
4. (Optional) Geben Sie für Name tag (Namens-Tag) einen Namen für die Routing-Tabelle des Transit-Gateways ein. Dadurch wird ein Tag erstellt, das "Name" als Tag-Schlüssel und den von Ihnen angegebenen Namen als Tag-Wert hat.
5. Wählen Sie für Transit-Gateway-ID das Transit Gateway für die Routing-Tabelle aus.
6. Wählen Sie Create Transit Gateway Route Table (Transit-Gateway-Routing-Tabelle erstellen) aus.

Um eine Transit-Gateway-Routentabelle mit dem zu erstellen AWS CLI

Verwenden Sie den Befehl create-transit-gateway-route-table.

Transit-Gateway-Routentabellen mit AWS Transit Gateway anzeigen

So zeigen Sie Ihre Transit-Gateway-Routing-Tabellen mit der Konsole an

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Route Tables (Transit Gateway-Routing-Tabellen).
3. (Optional) Zum Finden einer bestimmte Routing-Tabelle oder einer Reihe von Tabellen geben Sie den Namen, das Schlüsselwort oder das Attribut ganz oder teilweise in das Filterfeld ein.
4. Aktivieren Sie das Kontrollkästchen für eine Routentabelle oder wählen Sie ihre ID aus, um Informationen über ihre Zuordnungen, Propagationen, Routen und Tags anzuzeigen.

Um Ihre Transit-Gateway-Routentabellen mit dem AWS CLI

Verwenden Sie den Befehl describe-transit-gateway-route-tables.

Um die Routen für eine Transit-Gateway-Routentabelle mit dem AWS CLI

Verwenden Sie den Befehl search-transit-gateway-routes.

Um die Route-Propagationen für eine Transit-Gateway-Routentabelle anzuzeigen, verwenden Sie AWS CLI

Verwenden Sie den Befehl get-transit-gateway-route-table-propagations.

Um die Verknüpfungen für eine Transit-Gateway-Routentabelle mit dem AWS CLI

Verwenden Sie den Befehl get-transit-gateway-route-table-associations.

Ordnen Sie eine Transit-Gateway-Routentabelle in AWS Transit Gateway zu

Sie können eine Transit-Gateway-Routing-Tabelle einem Transit-Gateway-Anhang zuordnen.

So ordnen Sie eine Transit-Gateway-Routing-Tabelle mit der Konsole zu

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Route Tables (Transit Gateway-Routing-Tabellen).
3. Wählen Sie die Routing-Tabelle aus.
4. Wählen Sie unten auf der Seite die Registerkarte Associations (Zuordnungen) aus.
5. Wählen Sie Create association (Zuordnung erstellen) aus.
6. Wählen Sie die für die Zuordnung zu verwendende Anfügung und dann Create association (Zuordnung erstellen) aus.

Um eine Transit-Gateway-Routentabelle zuzuordnen, verwenden Sie den AWS CLI

Verwenden Sie den Befehl associate-transit-gateway-route-table.

Löschen Sie eine Zuordnung für eine Transit-Gateway-Routentabelle in AWS Transit Gateway

Sie können die Zuordnung einer Transit-Gateway-Routing-Tabelle zu einem Transit-Gateway-Anhang aufheben.

So heben Sie die Zuordnung einer Transit-Gateway-Routing-Tabelle mit der Konsole auf

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Route Tables (Transit Gateway-Routing-Tabellen).
3. Wählen Sie die Routing-Tabelle aus.

4. Wählen Sie unten auf der Seite die Registerkarte Associations (Zuordnungen) aus.
5. Wählen Sie die für das Aufheben der Zuordnung zu verwendende Anfügung und dann Delete association (Zuordnung löschen) aus.
6. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Delete association (Zuordnung löschen) aus.

Um die Zuordnung einer Transit-Gateway-Routentabelle aufzuheben, verwenden Sie den AWS CLI

Verwenden Sie den Befehl disassociate-transit-gateway-route-table.

Route-Propagierung zu einer Transit-Gateway-Routentabelle in AWS Transit Gateway aktivieren

Verwenden Sie die Route-Propagierung, um eine Route aus einer Anhang zu einer Routing-Tabelle hinzuzufügen.

So verbreiten Sie eine Route an eine Routing-Tabelle für Transit-Gateway-Anhänge

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Route Tables (Transit Gateway-Routing-Tabellen).
3. Wählen Sie die Routing-Tabelle aus, für die eine Propagierung erstellt werden soll.
4. Wählen Sie Actions (Aktionen) und Create propagation (Verbreitung erstellen) aus.
5. Wählen Sie auf der Seite Create propagation (Verbreitung erstellen) die Anfügung aus.
6. Wählen Sie Create propagation (Verbreitung erstellen) aus.

Um die Route-Propagierung mit dem zu aktivieren AWS CLI

Verwenden Sie den Befehl enable-transit-gateway-route-table-propagation.

Deaktivieren Sie die Routenverbreitung in AWS Transit Gateway

Sie können eine verbreitete Route aus einer Routing-Tabellen-Anhang entfernen.

Deaktivieren der Route-Propagierung mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.

2. Klicken Sie im Navigationsbereich auf Transit Gateway Route Tables (Transit Gateway-Routing-Tabellen).
3. Wählen Sie die Routing-Tabelle aus, aus der die Propagierung gelöscht werden soll.
4. Wählen Sie unten auf der Seite die Registerkarte Propagations (Verbreitungen) aus.
5. Wählen Sie die Anfügung und dann Delete propagation (Verbreitung erstellen) aus.
6. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Delete propagation (Verbreitung löschen) aus.

Um die Routenverbreitung mit dem zu deaktivieren AWS CLI

Verwenden Sie den Befehl disable-transit-gateway-route-table-propagation.

Erstellen Sie eine statische Route in AWS Transit Gateway

Erstellen Sie eine statische Route für einen VPC-, VPN- oder Transit-Gateway-Peering-Anhang, oder Sie können eine Blackhole-Route erstellen, die den Datenverkehr ableitet, der der Route entspricht.

Statische Routen in einer Transit-Gateway-Routentabelle, die auf einen VPN-Anhang abzielen, werden vom VPN nicht gefiltert. Site-to-Site Dies kann einen unbeabsichtigten ausgehenden Datenverkehr erlauben, wenn ein BGP-basiertes VPN verwendet wird.

So erstellen Sie eine Route mit der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Route Tables (Transit Gateway-Routing-Tabellen).
3. Wählen Sie die Routing-Tabelle aus, für die eine Route erstellt werden soll.
4. Wählen Sie Actions (Aktionen), Create static route (Statische Route erstellen) aus.
5. Geben Sie auf der Seite Create route (Route erstellen) den CIDR-Block an, für den die Route erstellt werden soll. Wählen Sie dann Active aus.
6. Wählen Sie die Anhang für die Route aus.
7. Wählen Sie Create static route (Statische Route erstellen) aus.

So erstellen Sie eine Blackhole-Route mit der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.

2. Klicken Sie im Navigationsbereich auf Transit Gateway Route Tables (Transit Gateway-Routing-Tabellen).
3. Wählen Sie die Routing-Tabelle aus, für die eine Route erstellt werden soll.
4. Wählen Sie Actions (Aktionen), Create static route (Statische Route erstellen) aus.
5. Geben Sie auf der Seite Create static route (Statische Route erstellen) den CIDR-Block an, für den die Route erstellt werden soll. Wählen Sie dann Blackhole aus.
6. Wählen Sie Create static route (Statische Route erstellen) aus.

Um eine statische Route oder Blackhole-Route mit dem zu erstellen AWS CLI

Verwenden Sie den create-transit-gateway-route-Befehl.

Löschen Sie eine statische Route in AWS Transit Gateway

Löschen Sie statische Routen aus einer Transit-Gateway-Routentabelle.

So löschen Sie eine statische Route mit der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Route Tables (Transit Gateway-Routing-Tabellen).
3. Wählen Sie die Routing-Tabelle, aus der eine Route gelöscht werden soll, und dann Routes (Routen) aus.
4. Wählen Sie die zu löschende Route aus.
5. Wählen Sie Statischen Route löschen aus.
6. Wählen Sie im Bestätigungsfeld Delete static route (Statische Route löschen) aus.

Um eine statische Route mit dem zu löschen AWS CLI

Verwenden Sie den delete-transit-gateway-route-Befehl.

Ersetzen Sie eine statische Route in AWS Transit Gateway

Ersetzen Sie eine statische Route in einer Transit-Gateway-Routentabelle durch eine andere statische Route.

So ersetzen Sie eine statische Route mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Route Tables (Transit Gateway-Routing-Tabellen).
3. Wählen Sie in der Routing-Tabelle die Route aus, die Sie ersetzen möchten.
4. Wählen Sie im Abschnitt Details die Registerkarte Routen aus.
5. Wählen Sie Aktionen, Statische Route ersetzen aus.
6. Wählen Sie als Typ entweder Aktiv oder Blackhole aus.
7. Wählen Sie in der Dropdown-Liste Anhang auswählen das Transit-Gateway aus, das das aktuelle Gateway in der Routing-Tabelle ersetzen soll.
8. Wählen Sie Statische Route ersetzen aus.

Um eine statische Route mit dem zu ersetzen AWS CLI

Verwenden Sie den replace-transit-gateway-route-Befehl.

Exportieren Sie Routentabellen in AWS Transit Gateway nach Amazon S3

Sie können die Routen in den Transit-Gateway-Routing-Tabellen in einen Amazon-S3-Bucket exportieren. Die Routen werden im angegebenen Amazon-S3-Bucket in einer JSON-Datei gespeichert.

So exportieren Sie Transit-Gateway-Routing-Tabellen mit der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Route Tables (Transit Gateway-Routing-Tabellen).
3. Wählen Sie die Routing-Tabelle aus, die die zu exportierenden Routen enthält.
4. Wählen Sie Actions (Aktionen) und Export routes (Routen exportieren) aus.
5. Geben Sie auf der Seite Export routes (Routen exportieren) bei S3 bucket name (S3-Bucket-Name) den Namen des S3-Buckets ein.
6. Zum Filtern der Routen, die exportiert werden, geben Sie Filterparameter im Abschnitt Filters (Filter) der Seite ein.
7. Wählen Sie Export routes (Routen exportieren) aus.

Um auf die exportierten Routen zuzugreifen, öffnen Sie die Amazon S3 S3-Konsole unter https://console.aws.amazon.com/s3/und navigieren Sie zu dem Bucket, den Sie angegeben haben. Der Dateiname umfasst die AWS-Konto ID, die AWS Region, die Routentabellen-ID und einen Zeitstempel. Wählen Sie die Datei aus und klicken Sie auf Download (Herunterladen). Im Folgenden finden Sie ein Beispiel für eine JSON-Datei, die Informationen zu zwei verbreiteten Routen für VPC-Anhänge enthält.

```
{
  "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"
    }
  ]
```

```
}
```

Löschen Sie eine Transit-Gateway-Routentabelle in AWS Transit Gateway

So löschen Sie eine Transit-Gateway-Routing-Tabelle mit der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Route Tables (Transit Gateway-Routing-Tabellen).
3. Wählen Sie die Routing-Tabelle aus, die gelöscht werden soll.
4. Wählen Sie Aktionen, Löschen der Transit-Gateway-Routing-Tabelle aus.
5. Geben Sie **`delete`** ein und wählen Sie dann Löschen, um das Löschen zu bestätigen.

Um eine Transit-Gateway-Routentabelle mit dem zu löschen AWS CLI

Verwenden Sie den Befehl delete-transit-gateway-route-table.

Erstellen Sie eine Referenz zur Präfixliste einer Routentabelle in AWS Transit Gateway

Sie können in der Transit-Gateway-Routing-Tabelle auf eine Präfixliste verweisen. Eine Präfixliste ist ein Satz von einem oder mehreren CIDR-Blockeinträgen, die Sie definieren und verwalten. Zur Vereinfachung der Verwaltung der IP-Adressen, auf die Sie in Ihren Ressourcen zur Weiterleitung von Netzwerkdatenverkehr verweisen, können Sie eine Präfixliste verwenden. Wenn Sie beispielsweise häufig dasselbe Ziel in CIDRs mehreren Transit-Gateway-Routentabellen angeben, können Sie diese CIDRs in einer einzigen Präfixliste verwalten, anstatt CIDRs in jeder Routentabelle wiederholt auf dasselbe zu verweisen. Wenn Sie einen CIDR-Zielblock entfernen müssen, können Sie seinen Eintrag aus der Präfixliste entfernen, anstatt die Route aus jeder betroffenen Routingtabelle zu entfernen.

Wenn Sie in Ihrer Transit-Gateway-Routing-Tabelle einen Präfixlisten-Verweis erstellen, wird jeder Präfixlisten-Eintrag in der Transit-Gateway-Routing-Tabelle als Route dargestellt.

Weitere Informationen zu Präfixlisten finden Sie unter Präfixlisten im Amazon VPC-Benutzerhandbuch.

So erstellen Sie einen Präfixlisten-Verweis über die Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Route Tables (Transit-Gateway-Routing-Tabellen).
3. Wählen Sie die Routing-Tabelle des Transit Gateways aus.
4. Wählen Sie Actions (Aktionen), Create prefix list reference (Präfixlistenreferenz erstellen) aus.
5. Wählen Sie in Prefix list ID (Präfixlisten-ID) die ID der Präfixliste aus.
6. Wählen Sie für Typ aus, ob Datenverkehr zu dieser Präfixliste zulässig sein soll (Aktiv) oder aufgegeben (Blackhole).
7. Wählen Sie in Transit gateway attachment ID (Transit-Gateway-Anhangs-ID) die ID des Anhangs aus, an den der Datenverkehr weitergeleitet werden soll.
8. Wählen Sie Create prefix list reference (Präfixlistenreferenz erstellen).

Um eine Präfixlistenreferenz zu erstellen, verwenden Sie AWS CLI

Verwenden Sie den Befehl create-transit-gateway-prefix-list-reference.

Ändern Sie eine Präfixlistenreferenz in AWS Transit Gateway

Sie können einen Präfixlisten-Verweis ändern, indem Sie den Anhang ändern, an den der Datenverkehr weitergeleitet wird. Sie können auch angeben, ob der Datenverkehr gelöscht werden soll, der mit der Route übereinstimmt.

Sie können auf der Registerkarte Routes (Routen) die einzelnen Routen für eine Präfixliste nicht ändern. Um die Einträge in der Präfixliste zu ändern, müssen Sie das Fenster Managed Prefix Lists (Verwaltete Präfixlisten) verwenden. Weitere Informationen finden Sie unter Ändern einer Präfixliste im Amazon VPC-Benutzerhandbuch.

So ändern Sie einen Präfixlisten-Verweis über die Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Route Tables (Transit-Gateway-Routing-Tabellen).
3. Wählen Sie die Routing-Tabelle des Transit-Gateways aus.
4. Wählen Sie im unteren Bereich Prefix list references (Präfixlistenreferenzen)aus.

5. Wählen Sie die Präfixlistenreferenz und anschließend Modify references (Referenzen ändern) aus.
6. Wählen Sie für Typ aus, ob Datenverkehr zu dieser Präfixliste zulässig sein soll (Aktiv) oder aufgegeben (Blackhole).
7. Wählen Sie in Transit gateway attachment ID (Transit-Gateway-Anhangs-ID) die ID des Anhangs aus, an den der Datenverkehr weitergeleitet werden soll.
8. Wählen Sie Modify prefix list reference (Präfixlistenreferenz ändern) aus.

Um eine Referenz auf eine Präfixliste mit dem zu ändern AWS CLI

Verwenden Sie den Befehl modify-transit-gateway-prefix-list-reference.

Löschen Sie eine Präfixlistenreferenz in AWS Transit Gateway

Wenn Sie einen Präfixlisten-Verweis nicht mehr benötigen, können Sie diese aus der Transit-Gateway-Routing-Tabelle löschen. Durch das Löschen des Verweises wird die Präfixliste nicht gelöscht.

So löschen Sie einen Präfixlisten-Verweis über die Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Route Tables (Transit-Gateway-Routing-Tabellen).
3. Wählen Sie die Routing-Tabelle des Transit Gateways aus.
4. Wählen Sie die Präfixlistenreferenz und anschließend Delete references (Referenzen löschen) aus.
5. Wählen Sie Delete references (Referenzen löschen) aus.

Um eine Referenz auf eine Präfixliste mit dem zu ändern AWS CLI

Verwenden Sie den Befehl delete-transit-gateway-prefix-list-reference.

Richtlinientabellen für Transit Gateway in AWS Transit Gateway

Dynamisches Transit-Gateway-Routing verwendet Richtlinientabellen, um den Netzwerkverkehr für AWS -Cloud-WAN zu leiten. Die Tabelle enthält Richtlinienregeln für den Abgleich des

Netzwerkverkehrs nach Richtlinienattributen und ordnet dann den Datenverkehr, der mit der Regel übereinstimmt, einer Ziel-Routing-Tabelle zu.

Sie können dynamisches Routing für Transit-Gateways verwenden, um Routing- und Erreichbarkeitsinformationen automatisch mit Peered-Transit-Gateway-Typen auszutauschen. Im Gegensatz zu einer statischen Route kann der Datenverkehr basierend auf Netzwerkbedingungen wie Pfadausfällen oder Überlastung auf einem anderen Pfad weitergeleitet werden. Dynamisches Routing bietet außerdem eine zusätzliche Sicherheitsebene, da es einfacher ist, den Datenverkehr im Falle einer Netzwerkverletzung oder eines Netzwerkeinbruchs umzuleiten.

> **Note**
>
> Transit-Gateway-Richtlinientabellen werden derzeit nur in Cloud WAN unterstützt, wenn eine Transit-Gateway-Peering-Verbindung erstellt wird. Beim Erstellen einer Peering-Verbindung können Sie diese Tabelle der Verbindung zuordnen. Die Zuordnung füllt die Tabelle dann automatisch mit den Richtlinienregeln.
> Weitere Informationen zu Peering-Verbindungen in Cloud WAN finden Sie unter Peerings im Benutzerhandbuch von AWS Cloud WAN.

Aufgaben

- Erstellen Sie eine Transit-Gateway-Richtlinientabelle in AWS Transit Gateway
- Löschen Sie eine Transit-Gateway-Richtlinientabelle in AWS Transit Gateway

Erstellen Sie eine Transit-Gateway-Richtlinientabelle in AWS Transit Gateway

So erstellen Sie eine Transit-Gateway-Richtlinientabelle mit der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Policy Table (Transit-Gateway-Richtlinientabelle).
3. Wählen Sie Create Transit Gateway Policy Table (Transit-Gateway-Richtlinientabelle erstellen) aus.

4. (Optional) Geben Sie für Name tag (Namens-Tag) einen Namen für die Transit-Gateway-Richtlinientabelle ein. Dadurch wird ein Tag erstellt und der Wert ist der von Ihnen angegebene Name.
5. Wählen Sie für Transit-Gateway-ID das Transit Gateway für die Richtlinientabelle aus.
6. Wählen Sie Create Transit Gateway Policy Table (Transit-Gateway-Richtlinientabelle erstellen) aus.

Um eine Richtlinientabelle für das Transit Gateway zu erstellen, verwenden Sie AWS CLI

Verwenden Sie den Befehl create-transit-gateway-policy-table.

Löschen Sie eine Transit-Gateway-Richtlinientabelle in AWS Transit Gateway

Löschen Sie eine Transit-Gateway-Richtlinientabelle. Wenn eine Tabelle gelöscht wird, werden alle Richtlinienregeln in dieser Tabelle gelöscht.

So löschen Sie eine Transit-Gateway-Richtlinientabelle mit der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Policy Tables (Transit-Gateway-Richtlinientabellen).
3. Wählen Sie die zu löschende Transit-Gateway-Richtlinientabelle aus.
4. Wählen Sie Actions (Aktionen) und anschließend Delete policy table (Richtlinientabelle löschen) aus.
5. Bestätigen Sie, dass Sie die Tabelle löschen möchten.

Um eine Richtlinientabelle für das Transit Gateway mit dem zu löschen AWS CLI

Verwenden Sie den Befehl delete-transit-gateway-policy-table.

Multicast im AWS Transit Gateway

Multicast ist ein Kommunikationsprotokoll, das für die gleichzeitige Bereitstellung eines einzelnen Datenstroms an mehrere empfangende Computer verwendet wird. Transit Gateway unterstützt

das Routing von Multicast-Verkehr zwischen Subnetzen verbundener Verbindungen und dient als Multicast-Router für Instanzen VPCs, die Datenverkehr senden, der für mehrere empfangende Instances bestimmt ist.

Themen

Multicast-Konzepte

Die wichtigsten Konzepte für Multicast sind folgende:

- Multicast-Domain – Ermöglicht die Segmentierung eines Multicast-Netzwerks in verschiedene Domains und sorgt dafür, dass das Transit Gateway als mehrere Multicast-Router fungiert. Sie definieren die Mitgliedschaft von Multicast-Domains auf Subnetzebene.
- Multicast-Gruppe – Identifiziert eine Gruppe von Hosts, die denselben Multicast-Verkehr senden und empfangen. Eine Multicast-Gruppe wird durch eine Gruppen-IP-Adresse identifiziert. Die Multicast-Gruppenmitgliedschaft wird durch einzelne elastische Netzwerkschnittstellen definiert, die den Instances zugeordnet sind. EC2
- Internet Group Management Protocol (IGMP) – Internetprotokoll, das es Hosts und Routern ermöglicht, die Multicast-Gruppenmitgliedschaft dynamisch zu verwalten. Eine IGMP-Multicast-

Domain enthält Hosts, die das IGMP-Protokoll verwenden, um Nachrichten beizutreten, zu verlassen und Nachrichten zu senden. AWS unterstützt das IGMPv2 Protokoll und sowohl IGMP- als auch Multicast-Domänen mit statischer (API-basierter) Gruppenmitgliedschaft.

- Multicast-Quelle — Eine elastic network interface, die einer unterstützten EC2 Instance zugeordnet ist und statisch für das Senden von Multicast-Verkehr konfiguriert ist. Eine Multicast-Quelle gilt nur für statische Quellenkonfigurationen.

  Eine Multicast-Domain mit statischer Quelle enthält Hosts, die das IGMP-Protokoll nicht zum Beitreten, Verlassen und Senden von Nachrichten verwenden. Sie verwenden die AWS CLI , um eine Quelle und Gruppenmitglieder hinzuzufügen. Die statisch hinzugefügte Quelle sendet Multicast-Datenverkehr und die Mitglieder erhalten Multicast-Datenverkehr.
- Multicast-Gruppenmitglied — Eine elastic network interface, die einer unterstützten EC2 Instance zugeordnet ist, die Multicast-Verkehr empfängt. Eine Multicast-Gruppe hat mehrere Gruppenmitglieder. In einer Gruppenmitgliedschaft mit statischer Quelle können Multicast-Gruppenmitglieder nur Datenverkehr empfangen. In einer IGMP-Gruppenkonfiguration können Mitglieder sowohl Datenverkehr senden als auch empfangen.

Überlegungen

- Transit-Gateway-Multicast ist möglicherweise nicht für Hochfrequenzhandel oder leistungssensitive Anwendungen geeignet. Es wird dringend empfohlen, die Multicast-Kontingente auf die Limits zu überprüfen. Wenden Sie sich an Ihr Konto- oder Solution Architect-Team, um eine detaillierte Überprüfung Ihrer Leistungsanforderungen zu erhalten.
- Informationen zu unterstützten Regionen finden Sie unter AWS Transit Gateway FAQs.
- Sie müssen ein neues Transit Gateway erstellen, damit Multicast unterstützt wird.
- Die Mitgliedschaft in Multicast-Gruppen wird mithilfe von Amazon Virtual Private Cloud Console oder AWS CLI, oder IGMP verwaltet.
- Ein Subnetz kann sich nur in einer Multicast-Domain befinden.
- Wenn Sie eine Nicht-Nitro-Instanz verwenden, müssen Sie das Kontrollkästchen Source/Dest deaktivieren. Informationen zur Deaktivierung der Prüfung finden Sie unter Ändern der Quell- oder Zielüberprüfung im EC2 Amazon-Benutzerhandbuch.
- Eine Nicht-Nitro-Instance kann kein Multicast-Sender sein.
- Multicast-Routing wird nicht über Site-to-Site VPN Direct Connect, Peering-Anlagen oder Transit-Gateway-Connect-Anlagen unterstützt.

- Ein Transit Gateway unterstützt keine Fragmentierung von Multicast-Paketen. Fragmentierte Multicast-Pakete werden verworfen. Weitere Informationen finden Sie unter Maximum Transmission Unit (MTU).
- Beim Startup sendet ein IGMP-Host mehrere JOIN-IGMP-Nachrichten, um einer Multicast-Gruppe beizutreten (normalerweise 2 bis 3 Wiederholungsversuche). In dem unwahrscheinlichen Fall, dass alle JOIN IGMP-Nachrichten verloren gehen, wird der Host nicht Teil der Transit-Gateway-Multicast-Gruppe. In einem solchen Szenario müssen Sie die JOIN IGMP-Nachricht vom Host mit anwendungsspezifischen Methoden erneut auslösen.
- Eine Gruppenmitgliedschaft beginnt mit dem Empfang der IGMPv2 JOIN Nachricht durch das Transit-Gateway und endet mit dem Empfang der IGMPv2 LEAVE Nachricht. Das Transit Gateway verfolgt Hosts, die der Gruppe erfolgreich beigetreten sind. Als Cloud-Multicast-Router sendet das Transit Gateway alle zwei Minuten eine IGMPv2 QUERY Nachricht an alle Mitglieder. Jedes Mitglied sendet daraufhin eine IGMPv2 JOIN Nachricht, mit der die Mitglieder ihre Mitgliedschaft verlängern. Wenn ein Mitglied nicht auf drei aufeinanderfolgende Anfragen antwortet, entfernt das Transit Gateway diese Mitgliedschaft aus allen verbundenen Gruppen. Es sendet jedoch weiterhin 12 Stunden lang Anfragen an dieses Mitglied, bevor es dauerhaft aus seiner to-be-queried Liste entfernt wird. Eine explizite IGMPv2 LEAVE Nachricht entfernt den Host sofort und dauerhaft von jeder weiteren Multicast-Verarbeitung.
- Das Transit Gateway verfolgt Hosts, die der Gruppe erfolgreich beigetreten sind. Im Falle eines Ausfalls des Transit Gateways sendet das Transit Gateway nach der letzten erfolgreichen IGMP JOIN-Nachricht weiterhin Multicastdaten für 7 Minuten (420 Sekunden) an den Host. Das Transit-Gateway sendet weiterhin Mitgliedschaftsabfragen für bis zu 12 Stunden an den Host oder bis er eine LEAVE IGMP-Nachricht vom Host erhält.
- Das Transit Gateway sendet Mitgliedschaftsabfrage-Pakete an alle IGMP-Mitglieder, um die Multicast-Gruppenmitgliedschaft zu verfolgen. Die Quell-IP dieser IGMP-Abfragepakete ist 0.0.0.0/32, die Ziel-IP ist 224.0.0.1/32 und das Protokoll ist 2. Ihre Sicherheitsgruppenkonfiguration auf den IGMP-Hosts (Instances) und jede ACLs Konfiguration in den Host-Subnetzen müssen diese IGMP-Protokollnachrichten zulassen.
- Wenn sich die Multicast-Quelle und das Ziel in derselben VPC befinden, können Sie keine Sicherheitsgruppen-Referenzierung verwenden, um die Zielsicherheitsgruppe so festzulegen, dass sie Datenverkehr von der Sicherheitsgruppe der Quelle akzeptiert.
- Für statische Multicast-Gruppen und -Quellen entfernt AWS Transit Gateway automatisch statische Gruppen und Quellen ENIs , für die es nicht mehr gibt. Dies erfolgt, indem in regelmäßigen Abständen die dienstbezogene Rolle des Transit Gateway übernommen wird, die ENIs im Konto beschrieben wird.

- Nur statisches Multicast wird unterstützt. IPv6 Dynamisches Multicast tut dies nicht.

Multicast-Routing

Wenn Sie Multicast auf einem Transit Gateway aktivieren, fungiert es als Multicast-Router. Der gesamte Multicast-Datenverkehr wird an den der betreffenden Multicast-Domain zugeordneten Transit Gateway gesendet, wenn Sie dieser Multicast-Domain ein Subnetz hinzufügen.

Netzwerk ACLs

Die Regeln für Netzwerk-ACL arbeiten auf Subnetz-Ebene. Sie gelten für Multicast-Datenverkehr, da sich Transit Gateways außerhalb des Subnetzes befinden. Weitere Informationen finden Sie unter Netzwerk ACLs im Amazon VPC-Benutzerhandbuch.

Für den Multicast-Datenverkehr des Internet Group Management Protocol (IGMP) gelten die folgenden Mindestregeln für eingehenden Verkehr. Der Remote-Host ist der Host, der den Multicast-Datenverkehr sendet.

Typ	Protokoll	Quelle	Beschreibung
Benutzerdefiniertes Protokoll	IGMP(2)	0.0.0.0/32	IGMP-Abfrage
Benutzerdefiniertes UDP-Protokoll	UDP	IP-Adresse des Remote-Hosts	Eingehender Multicast-Datenverkehr

Im Folgenden sind die Mindestregeln für ausgehenden Datenverkehr für IGMP aufgeführt.

Typ	Protokoll	Zielbereich	Beschreibung
Benutzerdefiniertes Protokoll	IGMP(2)	224.0.0.2/32	IGMP verlassen
Benutzerdefiniertes Protokoll	IGMP(2)	IP-Adresse der Multicast-Gruppe	IGMP beitreten
Benutzerdefiniertes UDP-Protokoll	UDP	IP-Adresse der Multicast-Gruppe	Ausgehenden Multicast-Datenverkehr

Sicherheitsgruppen

Sicherheitsgruppenregeln werden auf Instance-Ebene ausgeführt. Sie können sowohl auf eingehenden als auch auf ausgehenden Multicast-Datenverkehr angewendet werden. Das Verhalten ist dasselbe wie beim Unicast-Datenverkehr. Sie müssen für alle Gruppenmitglied-Instances von der Gruppenquelle eingehenden Datenverkehr zulassen. Weitere Informationen finden Sie unter Sicherheitsgruppen im Amazon-VPC-Benutzerhandbuch.

Sie müssen mindestens die folgenden eingehenden Regeln für IGMP-Multicast-Datenverkehr haben. Der Remote-Host ist der Host, der den Multicast-Datenverkehr sendet. Sie können keine Sicherheitsgruppe als Quelle der UDP-Eingangsregel angeben.

Typ	Protokoll	Quelle	Beschreibung
Benutzerdefiniertes Protokoll	2	0.0.0.0/32	IGMP-Abfrage
Benutzerdefiniertes UDP-Protokoll	UDP	IP-Adresse des Remote-Hosts	Eingehender Multicast-Datenverkehr

Sie müssen mindestens die folgenden Regeln für ausgehenden IGMP-Multicast-Datenverkehr haben.

Typ	Protokoll	Zielbereich	Beschreibung
Benutzerdefiniertes Protokoll	2	224.0.0.2/32	IGMP verlassen
Benutzerdefiniertes Protokoll	2	IP-Adresse der Multicast-Gruppe	IGMP beitreten
Benutzerdefiniertes UDP-Protokoll	UDP	IP-Adresse der Multicast-Gruppe	Ausgehenden Multicast-Datenverkehr

Multicast-Domänen im AWS Transit Gateway

Eine Multicast-Domäne ermöglicht die Segmentierung eines Multicast-Netzwerks in verschiedene Domänen. Um Multicast mit einem Transit Gateway zu verwenden, erstellen Sie eine Multicast-Domäne und ordnen Sie dann Subnetze der Domäne zu.

Multicast-Domänenattribute

Die folgende Tabelle enthält Details zu den Multicast-Domänenattributen. Sie können nicht beide Attribute gleichzeitig aktivieren.

Attribut	Beschreibung
`Igmpv2Support` (AWS CLI) IGMPv2 Unterstützung (Konsole)	Dieses Attribut legt fest, wie Gruppenmitglieder einer Multicast-Gruppe beitreten oder diese verlassen. Wenn dieses Attribut deaktiviert ist, müssen Sie die Gruppenmitglieder manuell zur Domäne hinzufügen. Aktivieren Sie dieses Attribut, wenn mindestens ein Mitglied das IGMP-Protokoll verwendet. Mitglieder treten der Multicast-Gruppe auf eine der folgenden Arten bei: • Mitglieder, die IGMP unterstützen, verwenden die `JOIN` und `LEAVE` Nachrichten. • Mitglieder, die IGMP nicht unterstützen, müssen mithilfe der Amazon-VPC-Konsole oder der AWS CLI zur Gruppe hinzugefügt oder daraus entfernt werden. Wenn Sie Mitglieder von Multicast-Gruppen registrieren, müssen Sie sie auch abmelden. Das Transit Gateway ignoriert `LEAVE`-IGMP-Nachrichten, die von einem manuell hinzugefügten Gruppenmitglied gesendet werden.
`StaticSourcesSupport` (AWS CLI)	Dieses Attribut legt fest, ob es statische Multicast-Quellen für die Gruppe gibt. Wenn dieses Attribut aktiviert ist, müssen Sie mithilfe von register-transit-gateway-multicast-group-sources Quellen für

Attribut	Beschreibung
Unterstützung für statische Quellen (Konsole)	eine Multicast-Domain hinzufügen. Nur Multicast-Quellen können Multicast-Datenverkehr senden. Wenn dieses Attribut auf Disable (Deaktivieren) gesetzt ist, gibt es keine designierten Multicast-Quellen. Alle Instances, die sich in Subnetzen befinden, die mit der Multicast-Domäne verknüpft sind, können Multicast-Datenverkehr senden, und die Gruppenmitglieder erhalten den Multicast-Datenverkehr.

Erstellen Sie eine IGMP-Multicast-Domäne in Transit Gateway AWS

Wenn Sie dies noch nicht getan haben, überprüfen Sie die verfügbaren Multicast-Domänen-Attribute. Weitere Informationen finden Sie unter the section called “Multicast-Domänen”.

So erstellen Sie eine Multicast-Domäne mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Multicast.
3. Wählen Sie Create Transit Gateway Multicast Domain (Transit-Gateway-Multicast-Domäne erstellen) aus.
4. Geben Sie unter Name tag (Namens-Tag) einen Namen für die Domäne ein.
5. Wählen Sie für Transit Gateway ID (Transit-Gateway-ID) das Transit Gateway aus, das den Multicast-Datenverkehr verarbeitet.
6. Wenn Sie IGMPv2 Unterstützung benötigen, aktivieren Sie das Kontrollkästchen.
7. Wenn Sie Unterstützung für statische Quellen benötigen, deaktivieren Sie das Kontrollkästchen.
8. Um automatisch kontoübergreifende Subnetzzuordnungen für diese Multicast-Domäne zu akzeptieren, wählen Sie Auto accept shared associations (Freigegebene Zuordnungen automatisch akzeptieren).
9. Wählen Sie Create Transit Gateway Multicast Domain (Transit-Gateway-Multicast-Domäne erstellen) aus.

Um eine IGMP-Multicast-Domäne mit dem zu erstellen AWS CLI

Verwenden Sie den Befehl create-transit-gateway-multicast-domain.

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

Erstellen Sie eine statische Quell-Multicast-Domain in AWS Transit Gateway

Wenn Sie dies noch nicht getan haben, überprüfen Sie die verfügbaren Multicast-Domänen-Attribute. Weitere Informationen finden Sie unter the section called “Multicast-Domänen”.

So erstellen Sie eine statische Multicast-Domäne mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Multicast.
3. Wählen Sie Create Transit Gateway Multicast Domain (Transit-Gateway-Multicast-Domäne erstellen) aus.
4. Geben Sie für Name Tag (Namens-Tag) einen Namen ein, um die Domäne zu identifizieren.
5. Wählen Sie für Transit Gateway ID (Transit-Gateway-ID) das Transit Gateway aus, das den Multicast-Datenverkehr verarbeitet.
6. Wenn Sie IGMPv2 Unterstützung benötigen, deaktivieren Sie das Kontrollkästchen.
7. Wenn Sie Unterstützung für statische Quellen benötigen, aktivieren Sie das Kontrollkästchen.
8. Um automatisch kontoübergreifende Subnetzzuordnungen für diese Multicast-Domäne zu akzeptieren, wählen Sie Auto accept shared associations (Freigegebene Zuordnungen automatisch akzeptieren).
9. Wählen Sie Create Transit Gateway Multicast Domain (Transit-Gateway-Multicast-Domäne erstellen) aus.

Um eine statische Multicast-Domain zu erstellen, verwenden Sie AWS CLI

Verwenden Sie den Befehl create-transit-gateway-multicast-domain.

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

Zuordnen von VPC-Anhängen und Subnetzen zu einer Multicast-Domäne in Transit Gateway AWS

Gehen Sie wie folgt vor, um einen VPC-Anhang einer Multicast-Domäne zuzuordnen. Wenn Sie eine Zuordnung erstellen, können Sie dann die Subnetze auswählen, die in die Multicast-Domäne aufgenommen werden sollen.

Bevor Sie beginnen, müssen Sie auf Ihrem Transit-Gateway einen VPC-Anhang erstellen. Weitere Informationen finden Sie unter Amazon VPC-Anlagen in AWS Transit Gateway.

So verknüpfen Sie VPC-Anhänge mit einer Multicast-Domäne über die Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Multicast.
3. Wählen Sie die Multicast-Domäne aus und anschließend Actions (Aktionen), Create association (Zuordnung erstellen).
4. Wählen Sie für Anhang zum Zuordnen wählen den Transit-Gateway-Anhang aus.
5. Wählen Sie unter Choose subnets to associate (Subnetze für Zuordnung auswählen) die Subnetze aus, die in die Multicast-Domäne aufgenommen werden sollen.
6. Wählen Sie Create association (Zuordnung erstellen) aus.

Um VPC-Anlagen mit einer Multicast-Domäne zu verknüpfen, verwenden Sie AWS CLI

Verwenden Sie den Befehl associate-transit-gateway-multicast-domain.

Trennen Sie die Zuordnung eines Subnetzes zu einer Multicast-Domäne in Transit Gateway AWS

Gehen Sie wie folgt vor, um Subnetze von einer Multicast-Domäne zu trennen.

So trennen Sie die Zuordnung von Subnetzen über die Konsole:

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Multicast.
3. Wählen Sie die Multicast-Domäne aus.
4. Wählen Sie die Registerkarte Associations (Zuordnungen).
5. Wählen Sie das Subnetz aus und dann Aktionen, Verknüpfung löschen.

Um Subnetze zu trennen, verwenden Sie AWS CLI

Verwenden Sie den Befehl disassociate-transit-gateway-multicast-domain.

Multicast-Domänenzuordnungen in AWS Transit Gateway anzeigen

Sehen Sie sich Ihre Multicast-Domänen an, um sicherzustellen, dass sie verfügbar sind und ob sie die entsprechenden Subnetze und Anlagen enthalten.

So lassen Sie sich eine Multicast-Domäne mithilfe der Konsole anzeigen

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Multicast.
3. Wählen Sie die Multicast-Domäne aus.
4. Wählen Sie die Registerkarte Associations (Zuordnungen).

Um eine Multicast-Domain anzuzeigen, verwenden Sie AWS CLI

Verwenden Sie den Befehl describe-transit-gateway-multicast-domains.

Hinzufügen von Tags zu einer Multicast-Domain in AWS Transit Gateway

Fügen Sie Ihren Ressourcen Tags hinzu, um sie einfacher ordnen und identifizieren zu können, beispielsweise nach Zweck, Besitzer oder Umgebung. Sie können jeder Multicast-Domäne mehrere Tags hinzufügen. Tag-Schlüssel müssen für jede Multicast-Domäne eindeutig sein. Wenn Sie ein Tag mit einem Schlüssel hinzufügen, der der Multicast-Domäne bereits zugeordnet ist, ändert sich der Wert dieses Tags. Weitere Informationen finden Sie unter Taggen Ihrer EC2 Amazon-Ressourcen.

So können Sie Tags zu einer Multicast-Domäne mithilfe der Konsole anfügen

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Multicast.
3. Wählen Sie die Multicast-Domäne aus.
4. Klicken Sie auf Actions (Aktionen), Manage tags (Markierungen verwalten).
5. Wählen Sie für jede Markierung Neue Markierung hinzufügen und geben Sie den Schlüssel und Wert der Markierung ein.
6. Wählen Sie Speichern.

Um einer Multicast-Domain Tags hinzuzufügen, verwenden Sie den AWS CLI

Verwenden Sie den Befehl create-tags.

Löschen Sie eine Multicast-Domäne in AWS Transit Gateway

Gehen Sie folgendermaßen vor, um eine Multicast-Domäne zu löschen.

So löschen Sie eine Multicast-Domäne mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Multicast.
3. Wählen Sie die Multicast-Domäne aus und anschließend Actions (Aktionen), Delete multicast domain (Multicast-Domäne löschen).
4. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`delete`** ein und wählen Sie dann Löschen aus.

Um eine Multicast-Domäne mit dem zu löschen AWS CLI

Verwenden Sie den Befehl delete-transit-gateway-multicast-domain.

Gemeinsam genutzte Multicast-Domänen in AWS Transit Gateway

Mit der gemeinsamen Nutzung von Multicast-Domänen können Besitzer von Multicast-Domänen die Domäne mit anderen AWS -Konten innerhalb ihrer Organisation oder über Organisationen hinweg in AWS Organizations teilen. Als Besitzer der Multicast-Domäne können Sie die Multicast-Domäne zentral erstellen und verwalten. Nach der Freigabe können diese Benutzer die folgenden Vorgänge in einer gemeinsam genutzten Multicast-Domäne ausführen:

- Registrieren und Abmelden von Gruppenmitgliedern oder Gruppenquellen in der Multicast-Domäne
- Verknüpfen eines Subnetzes mit der Multicast-Domäne und Trennen von Subnetzen von der Multicast-Domäne

Ein Multicast-Domäneninhaber kann eine Multicast-Domäne teilen mit:

- AWS Konten innerhalb ihrer Organisation oder organisationsübergreifend in AWS Organizations
- Eine Organisationseinheit innerhalb ihrer Organisation in AWS Organizations

- Ihre gesamte Organisation ist in AWS Organizations
- AWS Konten außerhalb von AWS Organizations.

  Um eine Multicast-Domain mit einem AWS Konto außerhalb Ihrer Organisation gemeinsam zu nutzen, müssen Sie eine Ressourcenfreigabe mit erstellen und dann bei der Auswahl der Principals AWS Resource Access Manager, mit denen Sie die Multicast-Domain teilen möchten, die Option Freigabe für alle zulassen auswählen. Informationen zum Erstellen einer Ressourcenfreigabe finden Sie unter Erstellen einer Ressourcenfreigabe in AWS RAM im AWS RAM -Benutzerhandbuch.

Inhalt

Voraussetzungen für die gemeinsame Nutzung einer Multicast-Domäne

- Um eine Multicast-Domain gemeinsam zu nutzen, müssen Sie sie in Ihrem Konto besitzen. AWS Sie können keine Multicast-Domäne freigeben, die mit Ihnen geteilt wurde.
- Um eine Multicast-Domain mit Ihrer Organisation oder einer Organisationseinheit gemeinsam zu nutzen AWS Organizations, müssen Sie das Teilen mit aktivieren. AWS Organizations Weitere Informationen finden Sie unter Freigabe für AWS Organizations aktivieren im AWS RAM - Benutzerhandbuch.

Zugehörige Services

Die gemeinsame Nutzung von Multicast-Domänen ist in AWS Resource Access Manager ()AWS RAM integriert. AWS RAM ist ein Dienst, mit dem Sie Ihre AWS Ressourcen mit einem

beliebigen AWS Konto oder über AWS Organizations dieses teilen können. Mit AWS RAM geben Sie Ressourcen in Ihrem Besitz frei, indem Sie eine Ressourcenfreigabe erstellen. Eine Ressourcenfreigabe gibt die Ressourcen an, die gemeinsam genutzt werden sollen, und die Benutzer, mit denen sie geteilt werden sollen. Bei Verbrauchern kann es sich um einzelne AWS Konten, Organisationseinheiten oder eine gesamte Organisation handeln AWS Organizations.

Weitere Informationen zu AWS RAM finden Sie im AWS RAM Benutzerhandbuch.

Berechtigungen für freigegebene Multicast-Domänen

Berechtigungen für Besitzer

Die Besitzer sind für die Verwaltung der Multicast-Domain und der Mitglieder und Anhänge verantwortlich, die sie registrieren oder mit der Domain verknüpfen. Besitzer können die Freigabe jederzeit ändern oder widerrufen. Sie können AWS Organizations verwenden, um Ressourcen anzuzeigen, zu ändern und zu löschen, die Verbraucher in gemeinsam genutzten Multicast-Domänen erstellen.

Berechtigungen für Konsumenten

Benutzer der gemeinsam genutzten Multicast-Domäne können die folgenden Vorgänge in gemeinsam genutzten Multicast-Domänen genauso ausführen wie in von ihnen erstellten Multicast-Domänen:

- Registrieren und Abmelden von Gruppenmitgliedern oder Gruppenquellen in der Multicast-Domäne
- Verknüpfen eines Subnetzes mit der Multicast-Domäne und Trennen von Subnetzen von der Multicast-Domäne

Konsumenten sind verantwortlich für die Verwaltung der Ressourcen, die sie auf der gemeinsam genutzten Multicast-Domäne erstellen.

Kunden können keine Ressourcen anzeigen lassen oder ändern, die anderen Konsumenten oder dem Besitzer der Multicast-Domäne gehören, und sie können keine Multicast-Domänen ändern, die mit ihnen geteilt werden.

Fakturierung und Messung

Weder für den Besitzer noch für den Konsumenten fallen keine zusätzlichen Gebühren für die gemeinsame Nutzung von Multicast-Domänen an.

Kontingente

Eine gemeinsam genutzte Multicast-Domain wird auf die Multicast-Domänenkontingente des Besitzers und des gemeinsam genutzten Benutzers angerechnet.

Teilen Sie Ressourcen in allen Availability Zones in AWS Transit Gateway

Um sicherzustellen, dass die Ressourcen auf die Availability Zones einer Region verteilt sind, ordnet AWS Transit Gateway die Availability Zones unabhängig voneinander den Namen für jedes Konto zu. Dies könnte zu in mehreren Konten unterschiedlich benannten Availability Zones führen. Beispielsweise hat die Availability Zone `us-east-1a` für Ihr AWS Konto möglicherweise nicht denselben Standort wie `us-east-1a` für ein anderes AWS Konto.

Um den Ort Ihrer Multicast-Domäne relativ zu Ihren Konten zu bestimmen, verwenden Sie die Availability Zone-ID (AZ-ID). Die AZ-ID ist eine eindeutige und konsistente Kennung für eine Availability Zone für alle AWS Konten. Dies `use1-az1` ist beispielsweise eine AZ-ID für die `us-east-1` Region und es handelt sich in jedem AWS Konto um denselben Standort.

Um die AZ IDs für die Availability Zones in Ihrem Konto anzuzeigen

1. Öffnen Sie die AWS RAM Konsole zu https://console.aws.amazon.com/ram/Hause.
2. Die AZ IDs für die aktuelle Region werden im Bereich „Ihre AZ-ID“ auf der rechten Seite des Bildschirms angezeigt.

Teilen Sie eine Multicast-Domain in AWS Transit Gateway

Wenn ein Eigentümer eine Multicast-Domain mit Ihnen teilt, können Sie Folgendes tun:

- Registrieren und Abmelden von Gruppenmitgliedern oder Gruppenquellen
- Verknüpfen und Trennen von Subnetzen

> **Note**
>
> Um eine Multicast-Domäne zu teilen, müssen Sie sie zu einer Ressourcenfreigabe hinzufügen. Eine Ressourcenfreigabe ist eine AWS RAM Ressource, mit der Sie Ihre Ressourcen für mehrere AWS Konten gemeinsam nutzen können. Eine Ressourcenfreigabe gibt die freizugebenden Ressourcen und die Konsumenten an, für die sie freigegeben werden. Wenn Sie eine Multicast-Domain mithilfe von gemeinsam nutzen Amazon Virtual

Private Cloud Console, fügen Sie sie einer vorhandenen Ressourcenfreigabe hinzu. Um die Multicast-Domäne zu einer neuen Ressourcenfreigabe hinzuzufügen, müssen Sie zunächst die Ressourcenfreigabe mithilfe der AWS RAM -Konsoleerstellen.
Wenn Sie Teil einer Organisation sind AWS Organizations und die gemeinsame Nutzung innerhalb Ihrer Organisation aktiviert ist, erhalten Verbraucher in Ihrer Organisation automatisch Zugriff auf die gemeinsam genutzte Multicast-Domain. Andernfalls erhalten Verbraucher eine Einladung zur Teilnahme an der Ressourcenfreigabe, und nach Annahme der Einladung wird ihnen Zugriff auf die freigegebene Multicast-Domäne gewährt.

Sie können eine Multicast-Domain, die Sie besitzen, mithilfe der Amazon Virtual Private Cloud Konsole, AWS RAM der Konsole oder der gemeinsam nutzen. AWS CLI

So teilen Sie eine Multicast-Domäne, die Sie besitzen, mit der *Amazon Virtual Private Cloud Console

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Multicast-Domänenaus.
3. Wählen Sie Ihre Multicast-Domäne aus und anschließend Actions (Aktionen), Share multicast domain (Multicast-Domäne freigeben).
4. Wählen Sie Ihre Ressourcenfreigabe und anschließend Share multicast domain (Multicast-Domäne freigeben) aus.

Um eine Multicast-Domain, die Ihnen gehört, mithilfe der Konsole gemeinsam zu nutzen AWS RAM

Siehe Erstellen einer Ressourcenfreigabe im AWS RAM -Benutzerhandbuch.

Um eine Multicast-Domain, die Sie besitzen, mit dem AWS CLI

Verwenden Sie den Befehl create-resource-share.

Teilen Sie eine gemeinsam genutzte Multicast-Domain in AWS Transit Gateway auf

Wenn die Freigabe einer gemeinsam genutzten Multicast-Domäne aufgehoben wird, passiert Folgendes mit den Ressourcen der Verbraucher-Multicast-Domäne:

- Verbraucher-Subnetze werden von der Multicast-Domäne getrennt. Die Subnetze verbleiben im Verbraucherkonto.
- Quellen der Verbrauchergruppe und Gruppenmitglieder werden von der Multicast-Domäne getrennt und dann vom Verbraucherkonto gelöscht.

Um die Freigabe einer Multicast-Domäne aufzuheben, müssen Sie sie aus der Ressourcenfreigabe entfernen. Sie können dies von der AWS RAM Konsole oder dem aus tun AWS CLI.

Um die Freigabe einer freigegebenen Multicast-Domäne, deren Eigentümer Sie sind, aufzuheben, müssen Sie sie aus der Ressourcenfreigabe entfernen. Sie können dies mit der Amazon Virtual Private Cloud, AWS RAM console oder der tun AWS CLI.

So heben Sie die Freigabe einer gemeinsam genutzten Multicast-Domäne, deren Besitzer Sie sind, mit der au *Amazon Virtual Private Cloud Console

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Multicast-Domänenaus.
3. Wählen Sie Ihre Multicast-Domäne und dann Actions (Aktionen), Stop sharing (Freigabe aufheben) aus.

Um die gemeinsame Nutzung einer gemeinsam genutzten Multicast-Domain, die Ihnen gehört, mithilfe der Konsole aufzuheben AWS RAM

Siehe Aktualisieren einer Ressourcenfreigabe im AWS RAM -Benutzerhandbuch.

Um die gemeinsame Nutzung einer gemeinsam genutzten Multicast-Domain aufzuheben, die Sie besitzen, verwenden Sie die AWS CLI

Verwenden Sie den Befehl disassociate-resource-share.

Identifizieren Sie eine gemeinsam genutzte Multicast-Domain in AWS Transit Gateway

Eigentümer und Verbraucher können gemeinsam genutzte Multicast-Domänen mithilfe von und identifizieren Amazon Virtual Private Cloud AWS CLI

So identifizieren Sie eine gemeinsam genutzte Multicast-Domäne mit der *Amazon Virtual Private Cloud Console

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Multicast-Domänenaus.
3. Wählen Sie Ihre Multicast-Domäne aus.
4. Sehen Sie sich auf der Seite mit den Transit-Multicast-Domänendetails die Besitzer-ID an, um die AWS Konto-ID der Multicast-Domain zu identifizieren.

Um eine gemeinsam genutzte Multicast-Domain zu identifizieren, verwenden Sie den AWS CLI

Verwenden Sie den Befehl describe-transit-gateway-multicast-domains. Der Befehl gibt die Multicast-Domänen zurück, die Sie besitzen, und die Multicast-Domänen, die mit Ihnen gemeinsam genutzt werden. `OwnerId`zeigt die AWS Konto-ID des Multicast-Domänenbesitzers an.

Registrieren Sie Quellen mit einer Multicast-Gruppe in AWS Transit Gateway

> **Note**
>
> Dieses Verfahren ist nur erforderlich, wenn Sie das AttributUnterstützung statischer Quellen auf Enable (Aktivieren)gesetzt haben.

Gehen Sie wie folgt vor, um Quellen bei einer Multicast-Gruppe zu registrieren. Die Quelle ist die Netzwerkschnittstelle, die Multicast-Datenverkehr sendet.

Sie benötigen die folgenden Informationen, bevor Sie eine Quelle hinzufügen:

- Die ID der Multicast-Domäne
- Die IDs Netzwerkschnittstellen der Quellen
- Die IP-Adresse der Multicast-Gruppe

So registrieren Sie Quellen über die Konsole:

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Multicast.
3. Wählen Sie die Multicast-Domäne aus und anschließend Actions (Aktionen), Add group sources (Gruppenquellen hinzufügen).
4. Geben Sie als Gruppen-IP-Adresse entweder den IPv4 CIDR-Block oder den CIDR-Block ein, der der IPv6 Multicast-Domäne zugewiesen werden soll.
5. Wählen Sie unter Choose network interfaces (Netzwerkschnittstellen auswählen) die Netzwerkschnittstellen der Multicast-Sender aus.
6. Wählen Sie Add sources (Quellen hinzufügen).

Um Quellen mit dem zu registrieren AWS CLI

Verwenden Sie den Befehl register-transit-gateway-multicast-group-sources.

Mitglieder in einer Multicast-Gruppe in AWS Transit Gateway registrieren

Gehen Sie wie folgt vor, um Gruppenmitglieder bei einer Multicast-Gruppe zu registrieren.

Sie benötigen die folgenden Informationen, bevor Sie Mitglieder hinzufügen:

- Die ID der Multicast-Domäne
- Die IDs Netzwerkschnittstellen der Gruppenmitglieder
- Die IP-Adresse der Multicast-Gruppe

So registrieren Sie Mitglieder über die Konsole:

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Multicast.
3. Wählen Sie die Multicast-Domäne und anschließend Actions (Aktionen), Add group members (Gruppenmitglieder hinzufügen).
4. Geben Sie als Gruppen-IP-Adresse entweder den IPv4 CIDR-Block oder den CIDR-Block ein, der der IPv6 Multicast-Domäne zugewiesen werden soll.
5. Wählen Sie unter Choose network interfaces (Netzwerkschnittstellen auswählen) die Netzwerkschnittstellen der Multicast-Empfänger aus.
6. Wählen Sie Add members (Mitglieder hinzufügen).

Um Mitglieder mit dem zu registrieren AWS CLI

Verwenden Sie den Befehl register-transit-gateway-multicast-group-members.

Quellen aus einer Multicast-Gruppe in Transit Gateway abmelden AWS

Sie müssen diesen Vorgang nur ausführen, wenn Sie der Multicast-Gruppe manuell eine Quelle hinzugefügt haben.

So entfernen Sie eine Quelle über die Konsole:

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.

2. Klicken Sie im Navigationsbereich auf Transit Gateway Multicast.
3. Wählen Sie die Multicast-Domäne aus.
4. Wählen Sie die Registerkarte Groups (Gruppen).
5. Wählen Sie die Quellen aus und anschließend Remove source (Quelle entfernen).

Um eine Quelle mit dem zu entfernen AWS CLI

Verwenden Sie den Befehl deregister-transit-gateway-multicast-group-sources.

Mitglieder aus einer Multicast-Gruppe in Transit Gateway abmelden AWS

Sie müssen diesen Vorgang nur ausführen, wenn Sie der Multicast-Gruppe manuell ein Mitglied hinzugefügt haben.

So entfernen Sie die Registrierung von Mitgliedern über die Konsole:

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Multicast.
3. Wählen Sie die Multicast-Domäne aus.
4. Wählen Sie die Registerkarte Groups (Gruppen).
5. Wählen Sie die Mitglieder aus und klicken Sie dann auf Remove member (Mitglied entfernen).

Um Mitglieder mit dem abzumelden AWS CLI

Verwenden Sie den Befehl deregister-transit-gateway-multicast-group-members.

Multicast-Gruppen in AWS Transit Gateway anzeigen

Sie können Informationen zu Ihren Multicast-Gruppen einsehen, um zu überprüfen, ob Mitglieder mithilfe des IGMPv2 Protokolls erkannt wurden. Der Mitgliedstyp (in der Konsole) oder `MemberType` (im AWS CLI) zeigt IGMP an, wenn Mitglieder mit dem AWS Protokoll erkannt wurden.

So zeigen Sie Multicast-Gruppen mithilfe der Konsole an:

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateway Multicast.
3. Wählen Sie die Multicast-Domäne aus.

4. Wählen Sie die Registerkarte Groups (Gruppen).

Um Multicast-Gruppen anzuzeigen, verwenden Sie AWS CLI

Verwenden Sie den Befehl search-transit-gateway-multicast-groups.

Das folgende Beispiel zeigt, dass das IGMP-Protokoll Multicast-Gruppenmitglieder entdeckt hat.

```
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"
        }
    ]
}
```

Multicast für Windows Server in AWS Transit Gateway einrichten

Sie müssen zusätzliche Schritte ausführen, wenn Sie Multicast für die Verwendung mit Transit-Gateways unter Windows Server 2019 oder 2022 einrichten. Um dies einzurichten PowerShell, müssen Sie die folgenden Befehle verwenden und ausführen:

Um Multicast für Windows Server einzurichten, verwenden Sie PowerShell

1. Ändern Sie Windows Server so, dass es IGMPv2 statt IGMPv3 für den TCP/IP Stack verwendet wird:

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

> **Note**
>
> `New-ItemProperty`ist ein Eigenschaftsindex, der die IGMP-Version angibt. Da IGMP v2 die unterstützte Version für Multicast ist, muss die Eigenschaft `Value` lauten. `3` Anstatt die Windows-Registrierung zu bearbeiten, können Sie den folgenden Befehl ausführen, um die IGMP-Version auf 2 festzulegen. : `Set-NetIPv4Protocol -IGMPVersion Version2`

2. Die Windows-Firewall verwirft standardmäßig den größten Teil des UDP-Datenverkehrs. Sie müssen zunächst überprüfen, welches Verbindungsprofil für Multicast verwendet wird:

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

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

3. Aktualisieren Sie das Verbindungsprofil aus dem vorherigen Schritt, um den Zugriff auf die erforderlichen UDP-Ports zu ermöglichen:

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

4. Starten Sie die EC2 Instanz neu.
5. Testen Sie Ihre Multicast-Anwendung, um sicherzustellen, dass der Datenverkehr wie erwartet fließt.

Beispiel: Verwaltung von IGMP-Konfigurationen mit AWS Transit Gateway

Dieses Beispiel zeigt mindestens einen Host, der das IGMP-Protokoll für Multicast-Verkehr verwendet. AWS erstellt die Multicast-Gruppe automatisch, wenn sie eine `JOIN` IGMP-Nachricht von einer Instanz empfängt, und fügt die Instanz dann als Mitglied zu dieser Gruppe hinzu. Mithilfe von können Sie einer Gruppe auch statisch Nicht-IGMP-Hosts als Mitglieder hinzufügen. AWS CLI Alle Instances, die sich in Subnetzen befinden, die mit der Multicast-Domäne verknüpft sind, können Datenverkehr senden, und die Gruppenmitglieder erhalten den Multicast-Datenverkehr.

Führen Sie für diese Konfiguration die folgenden Schritte aus:

1. Erstellen Sie eine VPC. Weitere Informationen finden Sie unter VPC erstellen im Amazon-VPC-Benutzerhandbuch.

2. Erstellen Sie als Nächstes ein Subnetz in der VPC. Weitere Informationen finden Sie unter Erstellen eines Subnetzes im Amazon VPC-Benutzerhandbuch.
3. Erstellen Sie ein Transit Gateway, das für Multicast-Datenverkehr konfiguriert ist. Weitere Informationen finden Sie unter the section called “Erstellen eines Transit-Gateways”.
4. Erstellen eines VPC-Anhangs Weitere Informationen finden Sie unter the section called “Erstellen Sie einen VPC-Anhang”.
5. Erstellen Sie eine Multicast-Domäne, die für IGMP-Unterstützung konfiguriert ist. Weitere Informationen finden Sie unter the section called “Erstellen Sie eine IGMP-Multicast-Domäne”.

   Verwenden Sie die folgenden Einstellungen:

   - Aktivieren Sie IGMPv2 die Unterstützung.
   - Deaktivieren von Unterstützung für statische Quellen.
6. Erstellen Sie eine Verknüpfung zwischen Subnetzen in dem VPC-Anhang des Transit Gateways und der Multicast-Domäne. Weitere Informationen finden Sie unter the section called “Verknüpfen von VPC-Anhängen und Subnetzen mit einer Multicast-Domäne”.
7. Die Standard-IGMP-Version für EC2 ist. IGMPv3 Sie müssen die Version für alle Mitglieder der IGMP-Gruppe ändern. Sie können folgenden Befehl ausführen:

   ```
   sudo sysctl net.ipv4.conf.eth0.force_igmp_version=2
   ```
8. Fügen Sie die Mitglieder, die das IGMP-Protokoll nicht verwenden, der Multicast-Gruppe hinzu. Weitere Informationen finden Sie unter the section called “Registrieren von Mitgliedern bei einer Multicast-Gruppe”.

Beispiel: Verwaltung statischer Quellkonfigurationen in AWS Transit Gateway

In diesem Beispiel werden einer Gruppe statisch Multicast-Quellen hinzugefügt. Hosts verwenden das IGMP-Protokoll nicht, um Multicast-Gruppen beizutreten oder diese zu verlassen. Sie müssen die Gruppenmitglieder, die den Multicast-Datenverkehr erhalten, statisch hinzufügen.

Führen Sie für diese Konfiguration die folgenden Schritte aus:

1. Erstellen Sie eine VPC. Weitere Informationen finden Sie unter VPC erstellen im Amazon-VPC-Benutzerhandbuch.

2. Erstellen Sie als Nächstes ein Subnetz in der VPC. Weitere Informationen finden Sie unter Erstellen eines Subnetzes im Amazon VPC-Benutzerhandbuch.
3. Erstellen Sie ein Transit Gateway, das für Multicast-Datenverkehr konfiguriert ist. Weitere Informationen finden Sie unter the section called “Erstellen eines Transit-Gateways”.
4. Erstellen eines VPC-Anhangs Weitere Informationen finden Sie unter the section called “Erstellen Sie einen VPC-Anhang”.
5. Erstellen Sie eine Multicast-Domäne, die so konfiguriert ist, dass sie keine IGMP-Unterstützung oder Unterstützung für das statische Hinzufügen von Quellen bietet. Weitere Informationen finden Sie unter the section called “Erstellen Sie eine statische Quell-Multicast-Domäne”.

   Verwenden Sie die folgenden Einstellungen:

   - Deaktivieren Sie die UnterstützungIGMPv2 .
   - Um Quellen manuell hinzuzufügen, setzen Sie Static sources support (Unterstützung statischer Quellen) auf Enable (Aktivieren).

     Quellen sind die einzigen Ressourcen, die Multicast-Datenverkehr senden können, wenn das Attribut aktiviert ist. Andernfalls können alle Instances, die sich in Subnetzen befinden, die mit der Multicast-Domäne verknüpft sind, Multicast-Datenverkehr senden, und die Gruppenmitglieder erhalten den Multicast-Datenverkehr.
6. Erstellen Sie eine Verknüpfung zwischen Subnetzen in dem VPC-Anhang des Transit Gateways und der Multicast-Domäne. Weitere Informationen finden Sie unter the section called “Verknüpfen von VPC-Anhängen und Subnetzen mit einer Multicast-Domäne”.
7. Wenn Sie Static sources support (Unterstützung statischer Quellen) auf Enable (Aktivieren)festlegen, fügen Sie die Quelle der Multicast-Gruppe hinzu. Weitere Informationen finden Sie unter the section called “Registrieren von Quellen bei einer Multicast-Gruppe”.
8. Fügen Sie die Mitglieder der Multicast-Gruppe hinzu. Weitere Informationen finden Sie unter the section called “Registrieren von Mitgliedern bei einer Multicast-Gruppe”.

Beispiel: Konfiguration statischer Gruppenmitglieder in AWS Transit Gateway verwalten

Dieses Beispiel zeigt das statische Hinzufügen von Multicast-Mitgliedern zu einer Gruppe. Hosts können das IGMP-Protokoll nicht verwenden, um Multicast-Gruppen beizutreten oder diese zu verlassen. Alle Instances, die sich in Subnetzen befinden, die mit der Multicast-Domäne verknüpft

sind, können Multicast-Datenverkehr senden, und die Gruppenmitglieder erhalten den Multicast-Datenverkehr.

Führen Sie für diese Konfiguration die folgenden Schritte aus:

1. Erstellen Sie eine VPC. Weitere Informationen finden Sie unter VPC erstellen im Amazon-VPC-Benutzerhandbuch.
2. Erstellen Sie als Nächstes ein Subnetz in der VPC. Weitere Informationen finden Sie unter Erstellen eines Subnetzes im Amazon VPC-Benutzerhandbuch.
3. Erstellen Sie ein Transit Gateway, das für Multicast-Datenverkehr konfiguriert ist. Weitere Informationen finden Sie unter the section called “Erstellen eines Transit-Gateways”.
4. Erstellen eines VPC-Anhangs Weitere Informationen finden Sie unter the section called “Erstellen Sie einen VPC-Anhang”.
5. Erstellen Sie eine Multicast-Domäne, die so konfiguriert ist, dass sie keine IGMP-Unterstützung oder Unterstützung für das statische Hinzufügen von Quellen bietet. Weitere Informationen finden Sie unter the section called “Erstellen Sie eine statische Quell-Multicast-Domäne”.

   Verwenden Sie die folgenden Einstellungen:

   - Deaktivieren Sie die UnterstützungIGMPv2 .
   - Deaktivieren von Unterstützung für statische Quellen.
6. Erstellen Sie eine Verknüpfung zwischen Subnetzen in dem VPC-Anhang des Transit Gateways und der Multicast-Domäne. Weitere Informationen finden Sie unter the section called “Verknüpfen von VPC-Anhängen und Subnetzen mit einer Multicast-Domäne”.
7. Fügen Sie die Mitglieder der Multicast-Gruppe hinzu. Weitere Informationen finden Sie unter the section called “Registrieren von Mitgliedern bei einer Multicast-Gruppe”.

Flexible Kostenverteilung

Standardmäßig verwendet Transit Gateway ein senderbasiertes Kostenzuweisungsmodell, bei dem die Datenverarbeitungsgebühren dem Konto zugewiesen werden, dem der Quellanhang gehört. Sie können benutzerdefinierte Messrichtlinien erstellen, die definieren, welche Konten auf der Grundlage von Verkehrsflusseigenschaften wie Anhangstypen, bestimmten Anhängen oder Netzwerkadressen IDs belastet werden sollen.

Messrichtlinien bestehen aus geordneten Regeln, die von der niedrigsten zur höchsten Regelnummer bewertet werden. Wenn der Datenverkehr einer Regel entspricht, wird das angegebene Konto

entsprechend der Konfiguration der Regel belastet. Sie können den Kontoinhaber für die Kostenzuweisung aus den folgenden Optionen angeben:

- Eigentümer des Quellanhangs — Die Gebühren werden dem Konto zugewiesen, dem der Quellanhang gehört (Standardverhalten)
- Besitzer des Zielanhangs — Die Gebühren werden dem Konto zugewiesen, dem der Zielanhang gehört
- Inhaber des Transit-Gateways — Gebühren werden dem Konto zugewiesen, dem das Transit Gateway gehört

Die flexible Kostenzuweisung ermöglicht Unternehmen, die zentralisierte Netzwerkarchitekturen verwenden, ein besseres Kostenmanagement, sodass die Kosten unabhängig von der Netzwerktopologie den entsprechenden Geschäftsbereichen oder Anwendungsbesitzern zugewiesen werden können.

> **Note**
>
> Die flexible Kostenzuweisung ermöglicht eine flexible Zuordnung der Nutzung der Messgeräte und damit der Kosten zu den Kontoinhabern Ihrer Wahl. Die steuerlichen Auswirkungen auf AWS Konten können jedoch je nach geografischem Standort, Nutzungsmustern und anderen Faktoren erheblich variieren. Bitte überprüfen Sie die Auswirkungen auf Abrechnung, Steuern und Kostenmanagement für Konten in Ihrer AWS Organisation, bevor Sie diese Funktion aktivieren. Referenz: Was ist AWS Billing and Cost Management?

Richtlinien für die Erfassung

Mit Messrichtlinien können Sie Regeln zur Kostenzuweisung für Ihr Transit-Gateway konfigurieren, um anhand der Eigenschaften des Verkehrsflusses zu steuern, welchen Konten die Datenverarbeitungs- und Übertragungskosten in Rechnung gestellt werden. Diese Funktion ermöglicht Unternehmen, die zentralisierte Netzwerkarchitekturen verwenden, ein besseres Kostenmanagement und bessere Chargeback-Funktionen.

Eine Messrichtlinie besteht aus folgenden Komponenten:

- Messrichtlinie — Der allgemeine Konfigurationscontainer, der die Regeln für die Messrichtlinie enthält. Nach der Erstellung enthält er einen einzigen Standardeintrag für die Messrichtlinie, der so

konfiguriert ist, dass der gesamte Datenverkehr dem Eigentümer des Quellanhangs in Rechnung gestellt wird. Jedes Transit-Gateway kann nur über eine Messrichtlinie verfügen.

- Eingabe von Messrichtlinien — Einzelne Regeln innerhalb einer Messrichtlinie, die spezifische Abgleichskriterien und die Nutzung zwischen den einzelnen Messgeräten definieren. Jeder Eintrag enthält eine Regelnummer für die Bewertungsreihenfolge, die Bedingungen für die Zuordnung des Datenverkehrs (wie Quell- und Zielanhangstypen, Verbindungen IDs, CIDR-Blöcke, Ports und Protokolle) und den Kontoinhaber, der für den Abgleich des Datenverkehrs Gebühren erheben soll. Eine Richtlinie kann bis zu 50 Einträge enthalten, die in der Reihenfolge von der niedrigsten zur höchsten Regelnummer ausgewertet werden.

  Sie können die Nutzungsmessung einer der folgenden Optionen zuordnen:

  - Besitzer des Quellanhangs: Weist dem Konto zu, das Eigentümer des Anhangs ist, aus dem der Datenverkehr stammt (Standardverhalten)
  - Besitzer des Zielanhangs: Weist dem Konto zu, das Eigentümer des Anhangs ist, wo der Verkehr endet, und
  - Besitzer des Transit-Gateways: Weist die Messungsnutzung dem Konto zu, dem das Transit-Gateway gehört.
- Middlebox-Anlagen — (optional) Spezialisierte Transit-Gateway-Anlagen, die den Datenverkehr zur Sicherheitsinspektion, zum Lastenausgleich oder für andere Netzwerkfunktionen über Netzwerkgeräte weiterleiten. Die Datennutzung für den Datenverkehr, der Middlebox-Anhänge passiert, wird dem Kontoinhaber zugerechnet, der in der Messrichtlinie angegeben ist. Sie können maximal 10 Middlebox-Anhänge angeben. Unterstützte Middlebox-Anhangstypen sind Netzwerkfunktion (AWS Network Firewall), VPC- und VPN-Anhänge.

So funktionieren Messrichtlinien

Standardmäßig verwendet Transit Gateway ein absenderbasiertes Kostenzuweisungsmodell, bei dem die Datenverarbeitungsgebühren auf das Konto abgerechnet werden, dem der Quellanhang gehört. Mit Messrichtlinien können Sie benutzerdefinierte Regeln erstellen, um die Nutzung auf der Grundlage der folgenden Verkehrsflusseigenschaften flexibel zu messen:

- Quell- und Zielanhangstypen (VPC, VPN, Direct Connect Gateway, Peering, Netzwerkfunktion und VPN-Konzentrator)
- Quell- und Zielanhang IDs
- Quell- und Ziel-IP-Adressen, Portbereiche und Protokolle

Messrichtlinien bestehen aus geordneten Regeln, die von der niedrigsten zur höchsten Regelnummer bewertet werden. Wenn der Traffic einer Regel entspricht, wird das angegebene Konto entsprechend den in der Regel festgelegten Kontoeinstellungen belastet. Die Messrichtlinien beziehen sich auf mehrere gängige Unternehmensszenarien:

- Kostenzuweisung für Hybridumgebungen: Weisen Sie die Kosten für die AWS Dateneingabe vor Ort über Direct Connect Gateway dem Besitzer des Ziel-VPC-Kontos zu und nicht dem Besitzer des zentralen IT-Administratorkontos.
- Zentralisierte Inspektionsarchitektur: Weisen Sie die Kosten einzelnen Anwendungs- oder VPC-Kontoinhabern zu und nicht dem zentralen Sicherheitsteam für den Datenverkehr, der über die Inspektion fließt. VPCs
- Anwendungsbasierte Rückbuchung: Ordnen Sie alle Datennutzungskosten für einen Workload dem VPC-Besitzer zu, unabhängig von der Verkehrsrichtung.
- Kundenkostenzuweisung: Ordnen Sie die Datenkosten den Kundenkonten zu, wenn diese Anlagen zu Ihrem Transit-Gateway erstellen.

Middlebox-Anhänge

Die Metering-Richtlinien für Transit-Gateways unterstützen Middlebox-Anhänge, sodass Sie Datenverarbeitungsgebühren für den Netzwerkverkehr, der über Middlebox-Appliances wie Netzwerkfirewalls und Load Balancer geleitet wird, flexibel zuweisen können. Beispiele für Middlebox-Anhänge sind Netzwerkfunktionsanhänge an die AWS Network Firewall oder VPC-Anhänge, die den Datenverkehr an Sicherheits-Appliances von Drittanbietern in einer VPC weiterleiten. Der Datenverkehr zwischen Anhängen des Quell- und Ziel-Transit-Gateways wird bei typischen Sicherheitsüberprüfungen über diese Middlebox-Anhänge abgewickelt. Sie können Messrichtlinien definieren, um die Datenverarbeitungsnutzung für Middlebox-Anlagen flexibel dem ursprünglichen Quellanhang, dem endgültigen Zielanhang oder dem Inhaber des Transit-Gateway-Kontos zuzuweisen. Bei Anhängen von Netzwerkfunktionen werden die Datenverarbeitungsgebühren der AWS Network Firewall ebenfalls dem gebührenpflichtigen Konto zugewiesen.

Flexible Kostenzuweisung — Nutzungsarten erfassen

Die flexible Kostenzuweisung über Messrichtlinien gilt für die folgenden Datennutzungsarten:

- Nutzung der Transit-Gateway-Datenverarbeitung auf VPC-, VPN-, VPN Concentrator- und Direct Connect-Anhängen
- Site-to-site Nutzung der ausgehenden VPN-Datenübertragung bei VPN-Anhängen

- Verwendung von Direct Connect Data Transfer Out für Direct Connect-Anlagen.
- Nutzung der Datenübertragung bei TGW-Peering-Anhängen
- Transit-Gateway Nutzung der Datenverarbeitung bei Anhängen von Network Function
- AWS Nutzung der Netzwerk-Firewall (NFW) -Datenverarbeitung bei Anhängen von Network Function.

Die flexible Kostenzuweisung gilt nicht für die stündliche Nutzung von Anhängen und die Nutzung der Multicast-Datenverarbeitung. Für Transit Gateway Connect-Anlagen kann eine Messrichtlinie für den zugrunde liegenden Transport-VPC- oder Direct Connect-Anhang definiert werden. Für private IP-VPN-Anlagen kann eine Messrichtlinie für den zugrunde liegenden Direct Connect-Transportanhang definiert werden.

Überlegungen und Einschränkungen

Beachten Sie bei der Implementierung von Messrichtlinien für Ihr Transit-Gateway Folgendes.

Berechtigungen

- Nur der Besitzer des Transit-Gateways kann Messrichtlinien erstellen, ändern oder löschen.
- Die Einstellungen für die Kostenzuweisung gelten auf der Ebene des Transit-Gateways.
- Besitzer von Anhängen können die vom Eigentümer des Transit-Gateways konfigurierten Einstellungen für die Kostenzuweisung nicht überschreiben.

Transit-Gateway-Peering

Wenn der Verkehr die Transit-Gateway-Peering-Verbindungen durchquert:

- Jedes Transit-Gateway wendet unabhängig seine eigenen Messrichtlinien an.
- Datengebühren werden von jedem Transit-Gateway auf der Grundlage seiner lokalen Richtlinien separat zugewiesen.
- Man kann sich den Datenverkehr als zwei separate Datenflüsse vorstellen: Verbindung zwischen Quelle und Peering und Verbindung mit Zielverbindung.

Cloud-WAN-Integration

Wenn ein Transit-Gateway an ein Cloud-WAN-Kernnetzwerk angeschlossen ist:

- Die Gebühren für die Datenübertragung am Transit-Gateway für Peering-Verbindungen werden gemäß der Metering-Richtlinie für Transit-Gateways zugewiesen.
- Messrichtlinien werden in Cloud-WAN-Kernnetzwerken nicht unterstützt.

Auswirkung auf die Leistung

- Messrichtlinien führen zu keiner zusätzlichen Latenz bei Datenpfaden.
- Messrichtlinien haben keinen Einfluss auf die maximale Bandbreite pro Anhang.
- Es wurden keine Änderungen an den Funktionen zur gemeinsamen Nutzung von Ressourcen am Transit-Gateway vorgenommen.

Integration der Abrechnung

- Tags für die Kostenzuweisung funktionieren weiterhin mit Richtlinien zur Erfassung der Kosten nach Geschäftsbereichen.
- Richtlinien zur Erfassung definieren, für welche Konten Kosten anfallen, und anhand von Kostenzuordnungskennzeichnungen lassen sich diese Kosten kategorisieren.
- Änderungen der Messrichtlinien werden am Ende der nächsten Abrechnungsstunde wirksam.

IPv6 Unterstützung

Messrichtlinien werden sowohl für den Verkehr als auch für IPv4 den IPv6 Datenverkehr unterstützt. Der CIDR-Blockabgleich in Richtlinieneinträgen funktioniert mit beiden Adressfamilien.

Unterstützung für Middlebox-Anhänge

- Bei der Middlebox-Messing-Richtlinie wird davon ausgegangen, dass der Verkehr zwischen dem ursprünglichen Quell- und dem Zielanhang über den angegebenen Middle-Box-Anhang verbunden wird (Beispiel: Ost-West-Inspektion des Datenverkehrs). VPC-to-VPC Daher muss das Netzwerk-5-Tupel (source/destination IPs, source/destinationPorts und Protokoll) für eingehende und ausgehende Datenflüsse aus Middle-Box-Anhängen übereinstimmen. Datenflüsse mit 5-Tupel-Nichtübereinstimmungen bei Middle-Box-Anhängen (z. B. NAT-Transformation in Inspection-VPC) werden als reguläre Quell-Ziel-Anhangsflüsse behandelt (im Gegensatz zu Middle-Box-Anhang-Flows).

- Alle reinen Ausgangsflüsse auf dem Middlebox-Anhang (z. B. Nord-Süd-Verkehr zum Internet über IGW in einer Inspektions-VPC) werden als reguläre Quell- und Zielflüsse behandelt (im Gegensatz zu Middle-Box-Attachment-Flows).
- Bei Anhängen mit Netzwerkfunktionen, wenn die AWS Netzwerk-Firewall Pakete verwirft, wird der gesamte Datenverarbeitungsaufwand unabhängig von der Konfiguration der Messrichtlinie dem Absenderkonto in Rechnung gestellt.

Erstellen Sie eine AWS Transit Gateway Gateway-Messrichtlinie

Um Messrichtlinien zu aktivieren, müssen Sie eine Messrichtlinie für Ihr Transit-Gateway erstellen und Richtlinieneinträge konfigurieren, die definieren, wie die Messnutzung zugewiesen wird. Die Messrichtlinie legt den Rahmen und die Standardeinstellungen fest, während die Richtlinieneinträge die spezifischen Regeln enthalten, mit denen festgelegt wird, welche Konten auf der Grundlage von Verkehrsmerkmalen erfasst werden.

Die Richtlinieneinträge zur Erfassung funktionieren als geordnete Regeln, die sequentiell von der niedrigsten zur höchsten Regelnummer für den über Ihr Transit-Gateway fließenden Verkehr angewendet werden. Jeder Eintrag definiert übereinstimmende Kriterien wie Quell- und Zielanhangstypen, CIDR-Blöcke, Protokolle und Portbereiche sowie das Konto, für das der entsprechende Datenverkehr gemessen werden soll. Wenn ein Datenverkehrsfluss mehreren Einträgen entspricht, hat der Eintrag mit der niedrigsten Regelnummer Vorrang. Wenn keine Einträge einem bestimmten Datenfluss entsprechen, wird das in der Richtlinie angegebene Standardkonto mit Zählerkonto belastet.

Nachdem Sie eine Richtlinie erstellt haben, müssen Sie Richtlinieneinträge hinzufügen, um Ihre Kostenzuweisungslogik zu implementieren. Die Schritte zum Erstellen eines Eintrags für eine Messrichtlinie finden Sie unterErstellen Sie einen Eintrag für eine Messrichtlinie.

Erstellen Sie mithilfe der Konsole eine Messrichtlinie

Erstellen Sie eine Richtlinie zur Definition flexibler Kostenzuweisungsregeln für die Datennutzung am Transit-Gateway. Standardmäßig wird für alle Datenflüsse der Besitzer des Quellanhangs berechnet. Erstellen Sie Einträge, um bestimmte Netzwerkflüsse verschiedenen Konten in Rechnung zu stellen.

Um eine Messrichtlinie zu erstellen

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich die Option Messrichtlinien aus.

3. Wählen Sie Messrichtlinie erstellen aus.
4. Wählen Sie unter Transit-Gateway-ID das Transit-Gateway aus, für das Sie eine Messrichtlinie erstellen möchten.
5. (Optional) Wählen Sie für einen Middlebox-Anhang IDs einen oder mehrere Middlebox-Anhänge aus. Standardmäßig wird die Datennutzung dem Middlebox-Besitzer zugerechnet. Durch die Unterstützung von Middlebox-Anhängen können Messrichtlinien für den Datenverkehr angewendet werden, der Middlebox-Anhänge durchquert. Zusätzliche Anlagen können später hinzugefügt werden.
6. (Optional) Fügen Sie im Abschnitt „Tags“ Tags hinzu, die Ihnen helfen, Ihre Messrichtlinie zu identifizieren und zu organisieren:
   a. Wählen Sie Neues Tag hinzufügen aus.
   b. Geben Sie einen Tag-Schlüssel und optional einen Tag-Wert ein.
   c. Wählen Sie Neues Tag hinzufügen, um weitere Tags hinzuzufügen, oder fahren Sie mit dem nächsten Schritt fort. Sie können bis zu 50 Tags hinzufügen.
7. Wählen Sie Messrichtlinie für Transit-Gateways erstellen aus.

> **Note**
>
> Das Standardkonto ist der Eigentümer des Quellanhangs. Nachdem Sie eine Messrichtlinie erstellt haben, können Sie Einträge hinzufügen, die anhand der Eigenschaften des Datenverkehrs definieren, welches Konto belastet wird. Beachten Sie dabei, dass der Standardrichtlinieneintrag (der letzte Eintrag) nicht wie andere Richtlinieneinträge geändert oder gelöscht werden kann.

Erstellen Sie eine Messrichtlinie mit dem AWS CLI

Eine Messrichtlinie definiert das Standardverhalten bei der Kostenzuweisung und die globalen Einstellungen für Ihr Transit-Gateway. Verwenden Sie die create-transit-gateway-metering-Policy.

Erforderliche Parameter

- `--transit-gateway-id`- Die ID des Transit-Gateways, für das die Richtlinie erstellt werden soll

Optionale Parameter

- `--middle-box-attachment-ids`- Unterstützte Transit-Gateway-Anhangs-IDs, die der Richtlinie als Middlebox hinzugefügt werden sollen
- `--tag-specifications`- Tags für die Messrichtlinie

Um eine Messrichtlinie mit dem zu erstellen AWS CLI

1. Führen Sie den create-transit-gateway-metering-policy Befehl aus, um eine neue Messrichtlinie mit optionalen Middlebox-Anhängen zu erstellen.

```
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" } ] }]'
```

   Dieser Befehl erstellt eine Messrichtlinie für das angegebene Transit-Gateway mit den bereitgestellten Middlebox-Anhängen und -Tags.

2. Der Befehl gibt die folgende Ausgabe zurück, wenn die Richtlinie erfolgreich erstellt wurde:

```
{
    "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"}]
    }
}
```

   Notieren Sie sich die in der Antwort zurückgegebene Messrichtlinien-ID zur Verwendung in nachfolgenden Befehlen. describe-transit-gateway-metering-policiesDer Befehl kann verwendet werden, um die dem Transit-Gateway zugeordnete Messrichtlinie abzurufen.

Messrichtlinien für AWS Transit Gateway verwalten

Nachdem Sie eine Messrichtlinie erstellt haben, können Sie sie verwalten, indem Sie die aktuellen Einstellungen anzeigen, die Konfigurationsoptionen ändern oder die Richtlinie löschen, wenn sie nicht mehr benötigt wird. Mithilfe von Verwaltungsvorgängen können Sie Middlebox-Anlagen hinzufügen oder entfernen, wenn sich Ihre Netzwerkanforderungen ändern. Sie können nur einen Richtlinieneintrag erstellen oder löschen. Wenn Sie eine bestehende Regel ändern müssen, können Sie den Eintrag löschen und eine neue Regel mit der geänderten Konfiguration erstellen. Alle Verwaltungsvorgänge erfordern die Rechte des Besitzers des Transit-Gateways und werden nach zwei Abrechnungsstunden wirksam.

Ein effektives Management der Messrichtlinien ist entscheidend für die Aufrechterhaltung einer genauen Kostenverteilung bei der Weiterentwicklung Ihrer Netzwerkarchitektur. Organizations müssen ihre Richtlinien häufig anpassen, wenn sich Geschäftsbereiche ändern, neue Anwendungen bereitgestellt oder Netzwerktopologien geändert werden. Beispielsweise können die Einstellungen zur Unterstützung von Middlebox Metering Aktualisierungen erfordern, wenn sich die Firewall-Sicherheitsarchitekturen ändern oder wenn neue Inspektionsdienste für den Datenverkehrspfad eingeführt werden.

Richtlinienänderungen unterstützen verschiedene Betriebsszenarien, darunter saisonale Änderungen der Verkehrsmuster, Fusions- und Übernahmeaktivitäten sowie Aktualisierungen der Compliance-Anforderungen. Berücksichtigen Sie bei der Verwaltung der Richtlinien die Auswirkungen auf die bestehenden Abrechnungsregelungen und teilen Sie den betroffenen Akteuren die Änderungen vor der Umsetzung mit.

Regelmäßige Überprüfungen der Richtlinien tragen dazu bei, dass die Kostenverteilung weiterhin den Geschäftszielen und Organisationsstrukturen entspricht. Zu den bewährten Methoden gehören die Dokumentation von Richtlinienänderungen, das Testen von Änderungen in Produktionsumgebungen, wenn möglich, und die Abstimmung mit den Finanzteams, um die Auswirkungen auf die Abrechnung zu verstehen. Berücksichtigen Sie außerdem den Zeitpunkt der Richtlinienänderungen, um Unterbrechungen der monatlichen Abrechnungszyklen und der Finanzberichterstattung zu minimieren.

Themen

Eine AWS Transit Gateway Gateway-Messrichtlinie bearbeiten

Bearbeiten Sie bestehende Messrichtlinien, um die Konfigurationen von Middlebox-Anhängen zu ändern. Änderungen der Richtlinien werden zur nächsten Abrechnungsstunde wirksam und gelten für alle future Verkehrsflüsse über Ihr Transit-Gateway.

Bearbeiten Sie eine Messrichtlinie mithilfe der Konsole

Verwenden Sie die Konsole, um die vorhandenen Einstellungen der Messrichtlinie für Ihr Transit-Gateway zu ändern.

Um eine bestehende Messrichtlinie mit der Konsole zu bearbeiten

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich die Option Messrichtlinien aus.
3. Wählen Sie die Messrichtlinie aus, die Sie ändern möchten, indem Sie deren Richtlinien-ID auswählen
4. Ändern Sie die verfügbaren Richtlinieneinstellungen unter Aktionen. Die Konsole erlaubt nur das Hinzufügen und Entfernen von Middle-Box-Anhängen.
    - Middlebox-Anlagen — Fügen Sie Transit-Gateway-Anlagen hinzu oder entfernen Sie sie, die für spezielle Abrechnungen als Middleboxen behandelt werden sollten.

Bearbeiten Sie eine Messrichtlinie mit dem AWS CLI

Verwenden Sie den modify-transit-gateway-metering-policy Befehl, um Messrichtlinien anzuzeigen und zu ändern.

Erforderliche Parameter für Änderungsvorgänge:

- `--transit-gateway-metering-policy-id`- Die ID der Messrichtlinie, die geändert werden soll
- `--add-middle-box-attachment-ids`oder `--remove-middle-box-attachment-ids` — Unterstützte Transit-Gateway-Anhangs-IDs, die als Middlebox zur Richtlinie hinzugefügt oder daraus entfernt werden sollen

So zeigen Sie Messrichtlinien mit der AWS CLI an und bearbeiten sie

1. (Optional) Zeigen Sie vorhandene Messrichtlinien an, indem Sie den describe-transit-gateway-metering-policies Befehl verwenden, um die aktuellen Konfigurationseinstellungen zu sehen:

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

   Mit diesem Befehl werden alle Messrichtlinien in Ihrem Konto zurückgegeben, wobei ihr aktueller Status und die als Middlebox aktivierten Anlagen für jede Messrichtlinie angezeigt werden.

2. Ändern Sie eine Messrichtlinie mithilfe des modify-transit-gateway-metering-policy Befehls zum Aktualisieren der Konfigurationsoptionen:

   ```
   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
   ```

   Mit diesem Befehl wird eine Messrichtlinie geändert, indem Middlebox-Anlagen hinzugefügt und and/or entfernt werden.

3. Der Befehl gibt die folgende Ausgabe zurück, wenn die Richtlinie erfolgreich geändert wurde:

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

   Es kann bis zu zwei Abrechnungsstunden dauern, bis die Änderungen wirksam werden.

Löschen Sie eine AWS Transit Gateway Gateway-Messrichtlinie

Löschen Sie Messrichtlinien, wenn sie für Ihre Strategie zur Kostenzuweisung für Transit-Gateways nicht mehr erforderlich sind. Durch das Löschen einer Richtlinie wird die Kostenzuweisung auf

das absenderbasierte Standardmodell zurückgesetzt, bei dem die Datenverarbeitungs- und Datenübertragungsgebühren dem Konto zugewiesen werden, dem der Quellanhang gehört. Alle Richtlinieneinträge, die mit der gelöschten Messrichtlinie verknüpft sind, werden ebenfalls entfernt.

Löschen Sie eine Messrichtlinie mithilfe der Konsole

Verwenden Sie die Konsole, um Messrichtlinien zu entfernen, die nicht mehr benötigt werden.

Um eine Messrichtlinie mit der Konsole zu löschen

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich die Option Messrichtlinien aus.
3. Wählen Sie die Richtlinie aus, die Sie löschen möchten, indem Sie deren Richtlinien-ID auswählen.
4. Wählen Sie Actions (Aktionen) und anschließend Delete (Löschen) aus.
5. Bestätigen Sie den Löschvorgang, indem Sie **`delete`** etwas in das Bestätigungsdialogfeld eingeben.
6. Wählen Sie Löschen aus.

> **Important**
>
> Das Löschen einer Messrichtlinie kann nicht rückgängig gemacht werden. Alle Richtlinieneinträge und Konfigurationseinstellungen werden dauerhaft entfernt, und die Kostenzuweisung wird auf das absenderbasierte Standardmodell zurückgesetzt.

Löschen Sie eine Messrichtlinie mit dem AWS CLI

Verwenden Sie den delete-transit-gateway-metering-policy Befehl, um Messrichtlinien programmgesteuert zu löschen.

Voraussetzungen:

- Rechte des Besitzers des Transit Gateways

Erforderliche Parameter

- `--transit-gateway-metering-policy-id`- Die ID der Messrichtlinie, die gelöscht werden soll

So zeigen Sie Messrichtlinien mit der AWS CLI an und löschen sie

1. (Optional) Zeigen Sie vorhandene Messrichtlinien mit dem describe-transit-gateway-metering-policies Befehl an, um die aktuellen Konfigurationseinstellungen zu sehen:

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

   Dieser Befehl gibt alle Messrichtlinien in Ihrem Konto zurück und zeigt deren aktuellen Status und Konfiguration an.

2. Löschen Sie eine Messrichtlinie mit dem delete-transit-gateway-metering-policy folgenden Befehl, um die Richtlinie dauerhaft zu entfernen:

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

   Mit diesem Befehl werden die angegebene Messrichtlinie und alle zugehörigen Einträge dauerhaft entfernt. Die Kostenzuweisung wird für alle future Verkehrsflüsse auf das absenderbasierte Standardmodell zurückgesetzt. Es dauert außerdem zwei Abrechnungsstunden, bis diese Änderung wirksam wird.

3. Der Befehl gibt die folgende Ausgabe zurück, wenn die Richtlinie erfolgreich gelöscht wurde:

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

   In der Antwort wird bestätigt, dass die Richtlinie gelöscht wird, wobei ein `deleting` Status angegeben wird, während die Entfernung in der Transit-Gateway-Infrastruktur verarbeitet wird.

Einen Eintrag für eine AWS Transit Gateway Gateway-Messrichtlinie erstellen

Standardmäßig wird für alle Datenflüsse der Eigentümer des Quellanhangs berechnet. Um bestimmte Datenflüsse an verschiedene Konten zu erfassen, erstellen Sie individuelle Richtlinieneinträge, in denen anhand der Eigenschaften des Datenverkehrs definiert wird, für welches Konto Gebühren anfallen.

Die Richtlinieneinträge für die Erfassung dienen als bedingte Regeln, die in sequentieller Reihenfolge anhand ihrer Regelnummern ausgewertet werden, wenn der Verkehr über Ihr Transit-Gateway fließt. Jeder Eintrag dient als Wenn-Dann-Aussage: Wenn der Datenverkehr den angegebenen Kriterien entspricht (z. B. Art des Quellanhangs, CIDR-Zielblock oder Protokoll), wird das angegebene Konto belastet. Das System bewertet die Einträge von der niedrigsten zur höchsten Regelnummer, und der erste übereinstimmende Eintrag bestimmt das Rechnungskonto für diesen Verkehrsfluss.

Die Einträge unterstützen eine Vielzahl von Übereinstimmungskriterien, darunter Anhangstypen (VPC, VPN, Direct Connect Gateway), spezifische Anhänge IDs, Quell- und Ziel-CIDR-Blöcke, Protokolltypen und Portbereiche. Sie können mehrere Kriterien in einem einzigen Eintrag kombinieren, um präzise Targeting-Regeln zu erstellen. Sie könnten beispielsweise einen Eintrag erstellen, der den gesamten HTTPS-Verkehr (Port 443) von VPC-Anhängen zu einem bestimmten CIDR-Zielbereich abgleicht und diese Ströme dem Konto eines Sicherheitsteams belastet. Wenn keine Einträge einem bestimmten Verkehrsfluss entsprechen, wird das in der übergeordneten Messrichtlinie angegebene Standardkonto mit Zählerfassung belastet, sodass sichergestellt wird, dass der gesamte Datenverkehr ordnungsgemäß abgerechnet wird. Es dauert 2 Abrechnungsstunden, bis die Erstellung eines Eintrags wirksam wird.

Important

- Planen Sie die Regelnummern sorgfältig — lassen Sie Lücken (z. B. 10, 20, 30), um future Einfügungen zu ermöglichen
- Testen Sie zuerst Einträge mit weniger spezifischen Bedingungen, bevor Sie restriktivere Regeln hinzufügen
- Verwenden Sie spezifische Abgleichsbedingungen, um eine unbeabsichtigte Abrechnung zu vermeiden

Erstellen Sie mithilfe der Konsole einen Eintrag für die Messrichtlinie

Eine Messrichtlinie definiert das Standardverhalten bei der Kostenzuweisung und die globalen Einstellungen für Ihr Transit-Gateway.

So erstellen Sie mit der Konsole einen Eintrag für eine Messrichtlinie

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich die Option Messrichtlinien aus.
3. Wählen Sie den Link zur Messrichtlinien-ID aus, um die zugehörigen Details anzuzeigen.
4. Wählen Sie die Registerkarte Messrichtlinien-Einträge.
5. Wählen Sie Eintrag für Messrichtlinien erstellen aus.
6. Nummer der Richtlinienregel — Dabei sollte es sich um eine eindeutige Zahl (1 — 32.766) handeln, die die Reihenfolge der Auswertung bestimmt. Niedrigere Zahlen haben eine höhere Priorität.
7. Gebührenpflichtiges Konto — Wählen Sie einen der folgenden Kontotypen aus, für den Gebühren für den entsprechenden Datenverkehr berechnet werden sollen:
   a. Eigentümer des Quellanhangs
   b. Besitzer des Zielanhangs
   c. Besitzer Transit Gateway Gateway-Anhangs
8. (Optional) Wählen Sie „Regelbedingungen“ — Diese optionalen Bedingungen definieren Kriterien, die einem bestimmten Datenverkehr entsprechen:
   - Art oder ID des Quellanhangs — Filtern Sie nach Anhangstyp (VPC, VPN, Direct Connect Gateway, Peering) oder ID.
   - Typ oder ID des Zielanhangs — Filtern Sie nach Art oder ID des Zielanhangs
   - Quell-CIDR-Block — Ordnet Datenverkehr aus bestimmten IP-Bereichen zu
   - Ziel-CIDR-Block — Ordnet den Verkehr bestimmten IP-Bereichen zu
   - Quellportbereich — Entspricht bestimmten Quellports
   - Zielportbereich — Entspricht bestimmten Zielports
   - Protokoll — Filtern Sie nach Protokoll für die Regel (1, 6, 17 usw.)
9. Wählen Sie Eintrag für Messrichtlinien erstellen, um die Konfiguration zu speichern.

Erstellen Sie einen Eintrag für die Messrichtlinie mit dem AWS CLI

Richtlinieneinträge definieren spezifische Regeln für die Kostenzuweisung auf der Grundlage von Verkehrsmerkmalen. Regeln werden in der Reihenfolge von der niedrigsten zur höchsten Regelnummer bewertet.

Erforderliche Parameter

- `--transit-gateway-metering-policy-id`- Die ID der Messrichtlinie, zu der der Eintrag hinzugefügt werden soll
- `--policy-rule-number`- Eine eindeutige Zahl (1—32.766), die die Reihenfolge der Auswertung bestimmt
- `--metered-account`- Art des Zahlers (//) source-attachment-owner destination-attachment-owner transit-gateway-owner

Optionale Parameter

Diese optionalen Parameter, die Kriterien definieren, die einem bestimmten Datenverkehr entsprechen:

- `--source-transit-gateway-attachment-id`- Die ID des Quell-Transit-Gateway-Anhangs.
- `--source-transit-gateway-attachment-type`- Der Typ des Quell-Transit-Gateway-Anhangs.
- `--source-cidr-block`- Der Quell-CIDR-Block für die Regel.
- `--source-port-range`- Der Quellportbereich für die Regel.
- `--destination-transit-gateway-attachment-id`— Die ID des Ziel-Transit-Gateway-Anhangs.
- `--destination-transit-gateway-attachment-type`- Der Typ des Ziel-Transit-Gateway-Anhangs.
- `--destination-cidr-block`- Der Ziel-CIDR-Block für die Regel.
- `--destination-port-range`- Der Zielportbereich für die Regel.
- `--protocol`- Die Protokollnummer für die Regel

Um einen Eintrag für eine Messrichtlinie mit dem zu erstellen AWS CLI

1. Verwenden Sie den create-transit-gateway-metering-policy-entry Befehl, um einen neuen Richtlinieneintrag zu erstellen, der VPC-Verkehr an ein bestimmtes gemessenes Konto weiterleitet:

```
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
```

   Dieser Befehl erstellt einen Richtlinieneintrag mit der Regelnummer 100, der dem für VPC-Anlagen bestimmten Datenverkehr entspricht, und dem Besitzer der Zielanhänge eine Gebühr für diese Datenflüsse berechnet.

2. Der Befehl gibt die folgende Ausgabe zurück, wenn der Eintrag erfolgreich erstellt wurde:

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

   Die Antwort bestätigt, dass der Eintrag während der Aktivierung in der gesamten Transit-Gateway-Infrastruktur mit dem Status „verfügbar“ erstellt wurde.

Löschen Sie einen Eintrag für eine AWS Transit Gateway Gateway-Messrichtlinie

Löschen Sie die Einträge in den Messrichtlinien, wenn bestimmte Regeln zur Kostenzuweisung für Ihren Netzwerkdatenverkehr nicht mehr erforderlich sind. Durch das Löschen von Einträgen wird die Richtlinienverwaltung vereinfacht, da veraltete oder unnötige Regeln entfernt und gleichzeitig

die allgemeine Richtlinienstruktur beibehalten wird. Wenn Sie einen Eintrag löschen, wird der Datenverkehr, der zuvor der gelöschten Regel entsprach, anhand der verbleibenden Einträge in der Reihenfolge der Regelnummern bewertet, oder es wird auf das standardmäßige Richtlinienverhalten zurückgegriffen, wenn keine anderen Einträge übereinstimmen.

Bevor Sie Einträge löschen, sollten Sie die Auswirkungen auf die aktuellen Abrechnungsmodalitäten und den Verkehrsfluss berücksichtigen. Nach dem Löschen dauert es bis zu 2 Abrechnungsstunden, bis die Änderung wirksam wird. Sie kann nicht rückgängig gemacht werden. Stimmen Sie die Änderungen daher mit den betroffenen Kontoinhabern und Finanzteams ab. Überprüfe die verbleibenden Einträge, um sicherzustellen, dass der Datenverkehr und die Abrechnung nach dem Löschen korrekt sind. Die Reihenfolge der Regelauswertung für die verbleibenden Einträge bleibt unverändert, sodass ein vorhersehbares Verhalten bei der Kostenzuweisung bei fortgesetzten Datenströmen gewährleistet wird.

⚠ Important

- Das Löschen ist irreversibel
- Datenverkehr, der zuvor mit diesem Eintrag übereinstimmt, wird anhand der verbleibenden Einträge erneut bewertet
- Überprüfen Sie die verbleibenden Einträge, um sicherzustellen, dass der Verkehr ordnungsgemäß abgedeckt ist

Löschen Sie einen Eintrag für eine Messrichtlinie mithilfe der Konsole

Verwenden Sie die Konsole, um Richtlinieneinträge über eine intuitive Benutzeroberfläche zu entfernen, die Bestätigungsdialogfelder enthält, um versehentliche Löschungen zu verhindern.

Um einen Richtlinieneintrag mit der Konsole zu löschen

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich die Option Messrichtlinien aus.
3. Wählen Sie die Messrichtlinie aus, die den Eintrag enthält, den Sie löschen möchten.
4. Wählen Sie den Eintrag aus, den Sie entfernen möchten, und klicken Sie auf Löschen.
5. Überprüfen Sie im Bestätigungsdialogfeld die Eintragsdetails und geben Sie den Text ein**`delete`**, um das Entfernen zu bestätigen.

6. Wählen Sie Löschen, um den Eintrag dauerhaft zu entfernen.

Löschen Sie einen Eintrag für eine Messrichtlinie mithilfe der AWS CLI

Verwenden Sie den delete-transit-gateway-metering-policy-entry Befehl, um Richtlinieneinträge programmgesteuert zu entfernen.

Voraussetzungen:

- Rechte des Besitzers des Transit Gateways
- Gültige Messrichtlinien-ID und Eintragsregelnummer

Erforderliche Parameter

- `--transit-gateway-metering-policy-id`- Die ID der Messrichtlinie
- `--policy-rule-number`- Die Regelnummer des zu löschenden Eintrags

So zeigen Sie Richtlinieneinträge mit der AWS CLI an und löschen sie

1. (Optional) Zeigen Sie vorhandene Richtlinieneinträge mit dem get-transit-gateway-metering-policy-entries Befehl an, um die aktuellen Konfigurationseinstellungen zu sehen:

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

   Dieser Befehl gibt alle Einträge für die angegebene Richtlinie zurück und zeigt deren Regelnummern, Übereinstimmungskriterien und Zählerkonten an.
2. Löschen Sie einen Richtlinieneintrag mit dem delete-transit-gateway-metering-policy-entry folgenden Befehl, um den Eintrag dauerhaft zu entfernen:

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

   Mit diesem Befehl wird der angegebene Eintrag dauerhaft aus der Richtlinie entfernt. Datenverkehr, der zuvor mit diesem Eintrag übereinstimmt, wird sofort mit den verbleibenden Einträgen verglichen oder es wird auf das standardmäßige Richtlinienverhalten zurückgegriffen.

3. Der Befehl gibt die folgende Ausgabe zurück, wenn der Eintrag erfolgreich gelöscht wurde:

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

Die Antwort bestätigt, dass der Eintrag gelöscht wird und den Status „Gelöscht“ hat, während der Löschvorgang in der gesamten Transit-Gateway-Infrastruktur verarbeitet wird.

Middlebox-Anhänge für die AWS Transit Gateway Gateway-Messrichtlinie verwalten

Die Metering-Richtlinien für Transit-Gateways unterstützen Middlebox-Anhänge, sodass Sie Datenverarbeitungsgebühren für den Netzwerkverkehr, der über Middlebox-Appliances wie Netzwerk-Firewalls und Load Balancer geleitet wird, flexibel zuweisen können. Beispiele für Middlebox-Anhänge sind Netzwerkfunktionsanhänge an die AWS Network Firewall oder VPC-Anhänge, die den Datenverkehr an Sicherheits-Appliances von Drittanbietern in einer VPC weiterleiten. Der Datenverkehr zwischen Anhängen des Quell- und Ziel-Transit-Gateways wird bei typischen Sicherheitsüberprüfungen über diese Middlebox-Anhänge abgewickelt. Sie können Messrichtlinien definieren, um die Datenverarbeitungsnutzung für Middlebox-Anlagen flexibel dem ursprünglichen Quellanhang, dem endgültigen Zielanhang oder dem Inhaber des Transit-Gateway-Kontos zuzuweisen. Bei Anhängen von Netzwerkfunktionen werden die Datenverarbeitungsgebühren der AWS Network Firewall ebenfalls dem gebührenpflichtigen Konto zugewiesen.

Spezifizierte Transit-Gateway-Anlagen, die den Datenverkehr zur Sicherheitsinspektion, zum Lastenausgleich oder für andere Netzwerkfunktionen über Netzwerkgeräte weiterleiten. Die Datennutzung für den Datenverkehr, der Middlebox-Anhänge passiert, wird an den Kontoinhaber abgerechnet, der in der Messrichtlinie angegeben ist. Sie können maximal 10 Middlebox-Anhänge

angeben. Unterstützte Middlebox-Anhangstypen sind Netzwerkfunktion (AWS Network Firewall), VPC- und VPN-Anhänge.

Themen

Middlebox-Anlagen für die AWS Transit Gateway Gateway-Messrichtlinie hinzufügen

Sie können Middlebox-Anhänge hinzufügen, um Netzwerkgeräte in Ihre Transit Gateway Gateway-Messrichtlinie zu integrieren. Auf diese Weise können Sie bestimmten Datenverkehr über Sicherheitsgeräte, Load Balancer oder andere Netzwerkfunktionen weiterleiten und gleichzeitig die detaillierte Kontrolle über die Kostenzuweisung beibehalten.

⚠ Important

- Stellen Sie sicher, dass die Middlebox-Appliances ordnungsgemäß konfiguriert und zugänglich sind
- Testen Sie das Traffic-Routing, bevor Sie es auf Produktionsworkloads anwenden
- Überwachen Sie die Middlebox-Leistung, um Latenz zu vermeiden
- Konfigurieren Sie ein geeignetes Failover-Verhalten für hohe Verfügbarkeit

Fügen Sie Middlebox-Anhänge mithilfe der Konsole hinzu

Um einen Middlebox-Anhangseintrag hinzuzufügen

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich die Option Messrichtlinien aus.
3. Wählen Sie den Link zur Messrichtlinien-ID aus, um die zugehörigen Details anzuzeigen.
4. Wählen Sie die Registerkarte Middlebox-Anhänge.
5. Wählen Sie Hinzufügen aus.
6. Wenn Sie dazu aufgefordert werden, wählen Sie den Middlebox-Anhang aus IDs , der für spezielle Abrechnungen als Middleboxen behandelt werden soll. Sie können bis zu 10 Middlebox-Anlagen auswählen.

7. Wählen Sie Middlebox-Anhänge hinzufügen, um die Konfiguration zu speichern.

Fügen Sie Middlebox-Anhänge hinzu, indem Sie AWS CLI

Verwenden Sie den modify-transit-gateway-metering-policy Befehl, um Anlagen hinzuzufügen.

Bevor Sie beginnen, stellen Sie sicher, dass Sie über die folgenden erforderlichen Parameter verfügen:

- `--transit-gateway-metering-policy-id`- Die ID der vorhandenen Messrichtlinie
- `--add-middle-box-attachment-ids`- Ein oder mehrere Anlagen IDs , die der Richtlinie hinzugefügt werden sollen (zum Hinzufügen von Anhängen)

So fügen Sie Middlebox-Anhänge mit der CLI zu einer vorhandenen Richtlinie hinzu AWS

1. Im folgenden Beispiel modify-transit-gateway-metering-policy wird verwendet, um einer vorhandenen Messrichtlinie vier Middlebox-Anhänge hinzuzufügen. Der Befehl fügt den angegebenen Anhang IDs zur vorhandenen Liste hinzu, ohne die aktuellen Anlagen zu entfernen:

```
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. In der folgenden Beispielantwort zeigt die JSON-Ausgabe die aktualisierte Richtlinienkonfiguration mit allen vier Middlebox-Anhängen, die jetzt enthalten sind:

```
{
    "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"
```

```
    }
}
```

Middlebox-Anhänge für die AWS Transit Gateway Gateway-Messrichtlinie entfernen

Standardmäßig werden die Messkosten dem Eigentümer des Middlebox-Anhangs zugerechnet. Sie können diese Zuweisungen jedoch ändern, um sicherzustellen, dass die Kosten ordnungsgemäß der tatsächlichen Quelle oder dem Ziel des Datenverkehrs zugewiesen werden. Sie können insgesamt bis zu 10 Middlebox-Anhänge für eine Messrichtlinie hinzufügen oder entfernen.

Entfernen Sie Middlebox-Anhänge mithilfe der Konsole

Verwenden Sie die Amazon VPC-Konsole, um Middlebox-Anhänge aus Ihrer Messrichtlinien-Konfiguration zu entfernen.

Um Middlebox-Anhänge zu entfernen

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Transit Gateways, Metering Policies aus.
3. Wählen Sie die Messrichtlinie aus, die Sie ändern möchten.
4. Wählen Sie die Registerkarte Middlebox-Anhänge.
5. Wählen Sie bis zu 10 Middlebox-Anhänge aus, die aus der Messrichtlinie entfernt werden sollen.
6. Wählen Sie Remove (Entfernen) aus.
7. Wenn Sie dazu aufgefordert werden, können Sie die ausgewählten Middlebox-Anhänge aktualisieren, um sie zu entfernen. Der Datenverkehr durch entfernte Anhänge wird dem Eigentümer des Middlebox-Anhangs zugerechnet.
8. Wählen Sie Middlebox-Anhänge entfernen aus.

Entfernen Sie Middlebox-Anhänge mit dem AWS CLI

Verwenden Sie den modify-transit-gateway-metering-policy Befehl, um Anhänge zu entfernen.

Bevor Sie beginnen, stellen Sie sicher, dass Sie über die folgenden erforderlichen Parameter verfügen:

- `--transit-gateway-metering-policy-id`- Die ID der vorhandenen Messrichtlinie

- `--remove-middle-box-attachment-ids`- Ein oder mehrere Anlagen IDs , die aus der Richtlinie entfernt werden sollen (zum Entfernen von Anhängen)

So entfernen Sie Middlebox-Anhänge mithilfe der CLI aus einer vorhandenen Richtlinie AWS

1. Im folgenden Beispiel modify-transit-gateway-metering-policy wird verwendet, um zwei spezifische Middlebox-Anhänge aus einer vorhandenen Messrichtlinie zu entfernen. Der Befehl entfernt nur den angegebenen Anhang, IDs wobei die verbleibenden Anlagen erhalten bleiben:

```
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. In der folgenden Beispielantwort zeigt die JSON-Ausgabe die aktualisierte Richtlinienkonfiguration, bei der die angegebenen Anlagen entfernt wurden und die verbleibenden Anlagen weiterhin aktiv sind:

```
{
    "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 Transit Gateway Gateway-Flow-Protokolle

Transit Gateway Flow Logs ist eine Funktion von AWS Transit Gateway, mit der Sie Informationen über den IP-Verkehr zu und von Ihren Transit-Gateways erfassen können. Flow-Protokolldaten können in Amazon CloudWatch Logs, Amazon S3 oder Firehose veröffentlicht werden. Nachdem Sie ein Flow-Protokoll erstellt haben, können Sie die darin enthaltenen Daten abrufen und an dem gewählten Ziel anzeigen. Flow-Potokolldaten werden außerhalb des Pfades des Netzwerkdatenverkehrs erfasst und wirken sich daher nicht auf den Netzwerkdurchsatz oder die Latenz aus. Sie können Flow-Protokolle erstellen oder löschen, ohne dass die Netzwerkleistung beeinträchtigt wird. Flow-Protokolle für Transit-Gateway erfassen Informationen, die sich ausschließlich auf Transit-Gateways beziehen, die in the section called “Flow-Protokolldatensätze für Transit-Gateway” beschrieben sind. Wenn Sie Informationen zum ein- und ausgehenden IP-Datenverkehr über Netzwerkschnittstellen in Ihren VPCs erfassen möchten, nutzen Sie VPC-Flow-Protokolle. Weitere Informationen finden Sie unter Protokollieren von IP-Datenverkehr mit VPC-Flow-Protokollen im Amazon-VPC-Benutzerhandbuch.

> **Note**
>
> Um ein Transit-Gateway-Flow-Protokoll zu erstellen, müssen Sie der Eigentümer des Transit-Gateways sein. Wenn Sie nicht der Besitzer sind, muss Ihnen der Eigentümer des Transit-Gateways die Erlaubnis geben.

Flow-Protokolldaten für ein überwachtes Transit-Gateway werden als Flow-Protokolldatensätze aufgezeichnet. Hierbei handelt es sich um Protokollereignisse bestehend aus Feldern, die den Datenverkehrfluss beschreiben. Weitere Informationen finden Sie unter Flow-Protokolldatensätze für Transit-Gateway.

Für die Erstellung eines Flow-Protokolls geben Sie Folgendes an:

- Die Ressource, für die das Flow-Protokoll erstellt werden soll
- Die Ziele, an die die Flow-Protokolldaten veröffentlicht werden sollen.

Nach dem Erstellen eines Flow-Protokolls kann es einige Minuten dauern, bis Daten erfasst und an den gewünschten Zielen veröffentlicht werden. Flow-Protokolle erfassen keine Echtzeitprotokollstreams für Ihre Transit-Gateways.

Sie können auf Ihre Flow-Protokolle Tags anwenden. Jeder Tag besteht aus einem Schlüssel und einem optionalen Wert, beides können Sie bestimmen. Tags können Ihnen dabei helfen, Ihre Flow-Protokolle zu organisieren, z. B. nach Zweck oder Besitzer.

Wenn Sie ein Flow-Protokoll nicht mehr benötigen, können Sie es löschen. Durch das Löschen eines Flow-Protokolls wird der Flow-Log-Service für die Ressource deaktiviert, und es werden keine neuen Flow-Protokolldatensätze erstellt oder in CloudWatch Logs oder Amazon S3 veröffentlicht. Durch das Löschen des Flow-Protokolls werden keine vorhandenen Flow-Protokolldatensätze oder Protokollstreams (für CloudWatch Logs) oder Protokolldateiobjekte (für Amazon S3) für ein Transit-Gateway gelöscht. Um einen vorhandenen Protokollstream zu löschen, verwenden Sie die CloudWatch Logs-Konsole. Vorhandene Protokolldateiobjekte können auf der Amazon S3-Konsole gelöscht werden. Nach dem Löschen eines Flow-Protokolls kann es einige Minuten dauern, bis keine Daten mehr erfasst werden. Weitere Informationen finden Sie unter Löschen Sie einen AWS Transit Gateway Flow Logs-Datensatz.

Sie können Flow-Protokolle für Ihre Transit-Gateways erstellen, die Daten in CloudWatch Logs, Amazon S3 oder Amazon Data Firehose veröffentlichen können. Weitere Informationen finden Sie hier:

- Erstellen Sie ein Flow-Protokoll, das in CloudWatch Logs veröffentlicht wird
- Erstellen Sie ein Flow-Protokoll, das auf Amazon S3 veröffentlicht wird
- Erstellen Sie ein Flow-Protokoll, das in Firehose veröffentlicht wird

Einschränkungen

Die folgenden Einschränkungen gelten für Transit Gateway Flow Logs:

- Multicast-Verkehr wird nicht unterstützt.
- Connect-Anlagen werden nicht unterstützt. Alle Connect-Flow-Protokolle werden unter dem Transportanhang angezeigt und müssen daher auf dem Transit-Gateway oder dem Connect-Transportanhang aktiviert sein.
- Transit Gateway Flow Logs unterstützt maximal 250 Abonnements pro Ressource und Konto. Um zusätzliche Abonnements für eine Ressource zu erstellen, die dieses Limit erreicht hat, müssen Sie zuerst bestehende Abonnements löschen.

Flow-Protokolldatensätze für Transit-Gateway

Ein Flow-Protokolldatensatz repräsentiert einen Netzwerk-Flow in Ihrem Transit-Gateway. Jeder Datensatz ist ein String mit durch Leerzeichen getrennten Feldern. Der Datensatz enthält Werte für die verschiedenen Komponenten des Datenverkehrsflusses, zum Beispiel Quelle, Ziel und Protokoll.

Wenn Sie ein Flow-Protokoll erstellen, können Sie das Standardformat für den Flow-Protokolldatensatz verwenden oder ein benutzerdefiniertes Format angeben.

Inhalt

Standardformat

Mit dem Standardformat enthalten die Flow-Protokolldatensätze alle Felder der Versionen 2 bis 6 in der Reihenfolge, die in der Tabelle Verfügbare Felder angezeigt wird. Das Standardformat kann nicht angepasst oder geändert werden. Um zusätzliche Felder oder eine unterschiedliche Teilmenge an Feldern zu erfassen, müssen Sie stattdessen ein benutzerdefiniertes Format angeben.

Benutzerdefiniertes Format

Mit einem benutzerdefinierten Format geben Sie an, welche Felder in den Flow-Protokolldatensätzen in welcher Reihenfolge enthalten sind. Auf diese Weise können Sie spezifische Flow-Protokolle für Ihre Anforderungen erstellen und Felder auslassen, die nicht relevant sind. Ein benutzerdefiniertes Format kann dazu beitragen, dass weniger separate Prozesse erforderlich sind, um spezifische Informationen aus veröffentlichten Flow-Protokollen zu extrahieren. Sie können eine beliebige Anzahl an verfügbaren Flow-Protokollfeldern angeben, Sie müssen jedoch mindestens eins angeben.

Verfügbare Felder

Die folgende Tabelle beschreibt alle verfügbaren Felder für einen Flow-Protokolldatensatz für Transit-Gateway. In der Spalte Version wird die Version angegeben, in der das Feld eingeführt wurde.

Beim Veröffentlichen von Flow-Protokoll-Daten in Amazon S3 hängt der Datentyp für die Felder vom Flow-Protokoll-Format ab. Wenn das Format reiner Text ist, sind alle Felder vom Typ STRING. Wenn das Format Parquet ist, lesen Sie die Tabelle für die Felddatentypen.

Wenn ein Feld für einen bestimmten Datensatz nicht anwendbar ist oder nicht verarbeitet werden konnte, wird für diesen Eintrag „-“ angezeigt. Metadatenfelder, die nicht direkt aus dem Paket-Header stammen, sind Best-Effort-Annäherungen, und ihre Werte können fehlen oder ungenau sein.

Feld	Beschreibung	Version
version	Gibt die Version an, in der das Feld eingeführt wurde. Das Standardformat enthält alle Felder der Version 2 in der Reihenfolge, in der sie in der Tabelle angezeigt werden. Parquet-Datentyp: INT_32	2
resource-type	Der Ressourcentyp, für den das Abonnement erstellt wird. Für Transit Gateway Flow Logs wird dies der Fall seinTransitGateway. Parquet-Datentyp: STRING	6
account-id	Die AWS-Konto ID des Besitzers des Quell-Transit-Gateways. Parquet-Datentyp: STRING	2
tgw-id	ID des Transit-Gateways, für das der Datenverkehr aufgezeichnet wird. Parquet-Datentyp: STRING	6
tgw-attachment-id	ID des Transit-Gateway-Anhangs, für den der Datenverkehr aufgezeichnet wird. Parquet-Datentyp: STRING	6
tgw-src-vpc-account-id	Die AWS-Konto ID für den Quell-VPC-Verkehr. Parquet-Datentyp: STRING	6
tgw-dst-vpc-account-id	Die AWS-Konto ID für den Ziel-VPC-Verkehr. Parquet-Datentyp: STRING	6
tgw-src-vpc-id	Die ID der Quell-VPC für das Transit-Gateway Parquet-Datentyp: STRING	6

Feld	Beschreibung	Version
tgw-dst-vpc-id	Die ID der Ziel-VPC für das Transit-Gateway. Parquet-Datentyp: STRING	6
tgw-src-subnet-id	Die ID des Subnetzes für den Transit-Gateway-Quelldatenverkehr. Parquet-Datentyp: STRING	6
tgw-dst-subnet-id	Die ID des Subnetzes für den Transit-Gateway-Zieldatenverkehr. Parquet-Datentyp: STRING	6
tgw-src-eni	Die ID der Anhang-ENI des Quell-Transit-Gateways für den Flow. Parquet-Datentyp: STRING	6
tgw-dst-eni	Die ID der Anhang-ENI des Ziel-Transit-Gateways für den Flow. Parquet-Datentyp: STRING	6
tgw-src-az-id	Die ID der Availability Zone, die den Quell-Transit-Gateway enthält, für die der Datenverkehr aufgezeichnet wird. Wenn der Datenverkehr von einem untergeordneten Standort stammt, zeigt der Datensatz das Symbol „-“ für dieses Feld an. Parquet-Datentyp: STRING	6
tgw-dst-az-id	Die ID der Availability Zone, die das Ziel-Transit-Gateway enthält, für das der Datenverkehr aufgezeichnet wird. Parquet-Datentyp: STRING	6
tgw-pair-attachment-id	Abhängig von der Flow-Richtung ist dies entweder die Egress- oder die Ingress-Anhangs-ID des Flows. Parquet-Datentyp: STRING	6
srcaddr	Die Quelladresse für eingehenden Datenverkehr. Parquet-Datentyp: STRING	2

Feld	Beschreibung	Version
dstaddr	Die Zieladresse für ausgehenden Datenverkehr. Parquet-Datentyp: STRING	2
srcport	Der Quellport des Datenverkehrs Parquet-Datentyp: INT_32	2
dstport	Der Zielport des Datenverkehrs Parquet-Datentyp: INT_32	2
protocol	Die IANA-Protokollnummer des Datenverkehrs. Weitere Informationen finden Sie unter Zugewiesene IP-Nummern. Parquet-Datentyp: INT_32	2
packets	Die Anzahl der Pakete, die während des Flows übertragen wurden Parquet-Datentyp: INT_64	2
bytes	Die Anzahl der Bytes, die während des Flows übertragen wurden Parquet-Datentyp: INT_64	2
start	Die Zeit, in Unix-Sekunden, in der das erste Paket des Flows innerhalb des Aggregationsintervalls empfangen wurde. Dies kann bis zu 60 Sekunden dauern, nachdem das Paket auf dem Transit-Gateway übertragen oder empfangen wurde. Parquet-Datentyp: INT_64	2
end	Die Zeit, in Unix-Sekunden, in der das letzte Paket des Flows innerhalb des Aggregationsintervalls empfangen wurde. Dies kann bis zu 60 Sekunden dauern, nachdem das Paket auf dem Transit-Gateway übertragen oder empfangen wurde. Parquet-Datentyp: INT_64	2

Feld	Beschreibung	Version
log-status	Der Status des Flow-Protokolls: • OK – Daten werden normal auf den ausgewählten Zielen protokolliert. • NODATA – Während des Aggregationsintervalls gab es keinen Netzwerkverkehr zu oder von der Netzwerkschnittstelle. • SKIPDATA – Einige Flow-Protokolldatensätze wurden während des Aggregationsintervalls übersprungen. Dies kann an internen Kapazitätsbeschränkungen oder einem internen Fehler liegen. Parquet-Datentyp: STRING	2
type	Der Typ des Datenverkehrs. Mögliche Werte sind IPv4 | IPv6 | EFA. Weitere Informationen finden Sie unter Elastic Fabric Adapter im Amazon EC2 EC2-Benutzerhandbuch. Parquet-Datentyp: STRING	3
packets-lost-no-route	Die Pakete gingen verloren, weil keine Route angegeben wurde. Parquet-Datentyp: INT_64	6
packets-lost-blackhole	Die Pakete gingen aufgrund eines schwarzen Lochs verloren. Parquet-Datentyp: INT_64	6
packets-lost-mtu-exceeded	Die Pakete gingen aufgrund der Größe verloren, welche die MTU überschreitet. Parquet-Datentyp: INT_64	6
packets-lost-ttl-expired	Die Pakete gingen aufgrund des Ablaufs der Time-to-Live verloren. Parquet-Datentyp: INT_64	6

Feld	Beschreibung	Version
tcp-flags	Der Bitmasken-Wert für die folgenden TCP-Flags: • FIN — 1 • SYN — 2 • RST — 4 • PSH – 8 • ACK – 16 • SYN-ACK — 18 • URG – 32 **Important** Wenn ein Flow-Protokolleintrag nur aus ACK-Paketen besteht, ist der Flag-Wert 0, nicht 16. Allgemeine Informationen zu TCP-Flags (z. B. die Bedeutung von Flags wie FIN, SYN und ACK) finden Sie unter TCP-Segmentstruktur auf Wikipedia. TCP-Flags können OR-ed während des Aggregationsintervalls verwendet werden. Bei kurzen Verbindungen können die Flags in derselben Zeile im Flow-Log-Datensatz gesetzt werden, z. B. 19 für SYN-ACK und FIN und 3 für SYN und FIN. Parquet-Datentyp: INT_32	3
region	Die Region, die das Transit-Gateway enthält, in der der Datenverkehr aufgezeichnet wird. Parquet-Datentyp: SCHNUR	4

Feld	Beschreibung	Version
flow-direction	Die Flussrichtung in Bezug auf das Transit-Gateway. Die möglichen Werte sind: ingress | egress. Parquet-Datentyp: SCHNUR	5
pkt-src-aws-service	Der Name der Teilmenge von IP-Adressbereichen für den Fall, srcaddr ob die Quell-IP-Adresse für einen AWS Dienst bestimmt ist. Die möglichen Werte sind: AMAZON | AMAZON_APPFLOW | AMAZON_CONNECT | API_GATEWAY | CHIME_MEETINGS | CHIME_VOICECONNECTOR | CLOUD9 | CLOUDFRON T | CODEBUILD | DYNAMODB | EBS | EC2 | EC2_INSTA NCE_CONNECT | GLOBALACCELERATOR | KINESIS_V IDEO_STREAMS | ROUTE53 | ROUTE53_HEALTHCHECKS | ROUTE53_HEALTHCHECKS_PUBLISHING | ROUTE53_R ESOLVER | S3 | WORKSPACES_GATEWAYS. Parquet-Datentyp: SCHNUR	5
pkt-dst-aws-service	Der Name der Teilmenge der IP-Adressbereiche für das dstaddr Feld, wenn die Ziel-IP-Adresse für einen AWS Dienst bestimmt ist. Eine Liste möglicher Werte finden Sie im Feld pkt-src-aws-service. Parquet-Datentyp: SCHNUR	5

Kontrollieren der Nutzung von Flow-Protokollen

Standardmäßig haben -Benutzer keine Berechtigungen zum Arbeiten mit Flow-Protokollen. Sie können eine Benutzerrichtlinie erstellen, über die Benutzer die Berechtigungen zum Erstellen, Ändern, Beschreiben und Löschen von Flow-Protokollen erhalten. Weitere Informationen finden Sie unter IAM-Benutzern die für Amazon EC2-Ressourcen benötigten Berechtigungen erteilen in der Amazon EC2-API-Referenz.

Nachfolgend finden Sie eine Beispielrichtlinie, die Benutzern uneingeschränkte Berechtigungen erteilt, um Flow-Protokolle zu erstellen, zu beschreiben und zu löschen.

JSON

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

Je nachdem, ob Sie in CloudWatch Logs oder Amazon S3 veröffentlichen, sind zusätzliche IAM-Rollen- und Berechtigungskonfigurationen erforderlich. Weitere Informationen erhalten Sie unter AWS Transit Gateway Flow Logs-Aufzeichnungen in Amazon CloudWatch Logs und AWS Transit Gateway Flow Logs-Datensätze in Amazon S3.

Flow-Protokolle für Transit-Gateway – Preise

Es fallen Datenerfassungs- und Speichergebühren für Verkaufsprotokolle an, wenn Sie Transit-Gateway-Flow-Protokolle veröffentlichen. Weitere Informationen zu den Preisen bei der Veröffentlichung von Verkaufslogs erhalten Sie, indem Sie Amazon CloudWatch Pricing öffnen und dann unter Tarif „Bezahlt“ die Option Logs auswählen und nach Verkaufte Logs suchen.

Eine IAM-Rolle für AWS Transit Gateway Flow Logs erstellen oder aktualisieren

Sie können eine vorhandene Rolle aktualisieren oder das folgende Verfahren verwenden, um mithilfe der AWS Identity and Access Management Konsole eine neue Rolle für die Verwendung mit Flow-Protokollen zu erstellen.

So erstellen Sie eine IAM-Rolle für Flow-Protokolle

1. Öffnen Sie unter https://console.aws.amazon.com/iam/ die IAM-Konsole.
2. Wählen Sie im Navigationsbereich Roles (Rollen) und Create Role (Rolle erstellen) aus.
3. Wählen Sie unter Select type of trusted entity (Typ der vertrauenswürdigen Entität wählen) die Option AWS Service aus. Wählen Sie für Use case (Anwendungsfall) die Option EC2 aus. Wählen Sie Weiter aus.
4. Wählen Sie auf der Seite Add permissions (Berechtigungen hinzufügen) die Option Next: Tags (Weiter: Tags) sowie zusätzliche Tags aus. Wählen Sie Weiter aus.
5. Geben Sie auf der Seite Name, Prüfung und Erstellung einen Namen für Ihre Rolle ein und geben Sie optional eine Beschreibung ein. Wählen Sie Rolle erstellen aus.
6. Wählen Sie den Namen der Rolle aus. Wählen Sie auf der Registerkarte Add permissions (Berechtigungen hinzufügen) die Option Create Inline Policy (Inline-Richtlinie erstellen) und anschließend die Registerkarte JSON aus.
7. Kopieren Sie die erste Richtlinie aus IAM-Rollen für die Veröffentlichung von Flow-Logs in CloudWatch Logs, und fügen Sie sie in das Fenster ein. Wählen Sie Richtlinie prüfen.
8. Geben Sie einen Namen für Ihre Richtlinie ein und wählen Sie Create policy (Richtlinie erstellen).
9. Wählen Sie den Namen der Rolle aus. Wählen Sie auf der Registerkarte Trust Relationships (Vertrauensstellungen) Edit Trust Relationship (Vertrauensstellungen bearbeiten) aus. Ändern Sie im vorhandenen Richtliniendokument den Service von `ec2.amazonaws.com` zu `vpc-flow-logs.amazonaws.com`. Wählen Sie Update Trust Policy.
10. Notieren Sie sich auf der Seite Summary (Zusammenfassung) den ARN der Rolle. Sie benötigen diesen ARN beim Erstellen des Flow-Protokolls.

AWS Transit Gateway Flow Logs-Aufzeichnungen in Amazon CloudWatch Logs

Flow Logs können Flow-Protokolldaten direkt auf Amazon veröffentlichen CloudWatch.

Bei der Veröffentlichung in CloudWatch Logs werden die Flow-Protokolldaten in einer Protokollgruppe veröffentlicht, und jedes Transit-Gateway hat einen eigenen Protokollstream in der Protokollgruppe. Protokollstreams enthalten Flow-Protokolldatensätze. Sie können mehrere Flow-Protokolle erstellen, die Daten in derselben Protokollgruppe veröffentlichen. Wenn dasselbe Transit-Gateway in einem oder mehreren Flow-Protokollen innerhalb derselben Protokollgruppe besteht, hat es einen kombinierten Protokollstream. Wenn Sie ein Flow-Protokoll zum Erfassen von abgelehntem

Datenverkehr und ein weiteres Flow-Protokoll zum Erfassen von zulässigem Datenverkehr erstellt haben, erfasst der kombinierte Protokollstream sämtlichen Datenverkehr.

Wenn Sie Flow-Protokolle in Logs veröffentlichen, fallen Gebühren für Datenaufnahme und Archivierung für verkaufte Protokolle an. CloudWatch Weitere Informationen finden Sie unter CloudWatch Amazon-Preise.

In CloudWatch Logs entspricht das Zeitstempelfeld der Startzeit, die im Flow-Log-Datensatz erfasst wurde. Das Feld ingestionTime gibt das Datum und die Uhrzeit an, an dem der Flow-Protokolldatensatz von Logs empfangen wurde. CloudWatch Der Zeitstempel ist später als die Endzeit, die im Flow-Protokolldatensatz erfasst wird.

Weitere Informationen zu CloudWatch Logs finden Sie unter Logs sent to CloudWatch Logs im Amazon CloudWatch Logs-Benutzerhandbuch.

Inhalt

IAM-Rollen für die Veröffentlichung von Flow-Logs in CloudWatch Logs

Die IAM-Rolle, die Ihrem Flow-Protokoll zugeordnet ist, muss über ausreichende Berechtigungen verfügen, um Flow-Logs in der angegebenen Protokollgruppe in CloudWatch Logs zu veröffentlichen. Die IAM-Rolle muss Ihrer gehören. AWS-Konto

Die IAM-Richtlinie, die mit Ihrer IAM-Rolle verknüpft ist, muss mindestens folgende Berechtigungen enthalten:

JSON

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

```
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource": "*"
    }
  ]
}
```

Stellen Sie auch sicher, dass Ihre Rolle über eine Vertrauensstellung verfügt, die es dem Flow-Protokoll-Service ermöglicht, die Rolle anzunehmen:

JSON

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

Wir empfehlen Ihnen, die `aws:SourceAccount`- und `aws:SourceArn`-Bedingungsschlüssel zu verwenden, um sich vor dem Problem des verwirrten Stellvertreters zu schützen. Beispielsweise können Sie der vorherigen Vertrauensrichtlinie den folgenden Bedingungsblock hinzufügen. Das Quellkonto ist der Eigentümer des Flow-Protokolls und der Quell-ARN ist der Flow Protokoll-ARN. Wenn Sie die Flow-Protokoll-ID nicht kennen, können Sie diesen Teil des ARN durch einen Platzhalter (*) ersetzen und dann die Richtlinie aktualisieren, nachdem Sie das Flow-Protokoll erstellt haben.

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

Berechtigungen für IAM-Benutzer zum Übergeben einer Rolle

Benutzer müssen auch über die Berechtigungen verfügen, die Aktion `iam:PassRole` für die IAM-Rolle zu verwenden, die dem Flow-Protokoll zugeordnet ist.

JSON

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

Erstellen Sie einen AWS Transit Gateway Flow Logs-Datensatz, der veröffentlicht wird in Amazon CloudWatch Logs

Sie können Flow-Protokolle für Transit-Gateways erstellen. Wenn Sie diese Schritte als IAM-Benutzer ausführen, stellen Sie sicher, dass Sie über Berechtigungen zum Verwenden der `iam:PassRole`-Aktion verfügen. Weitere Informationen finden Sie unter Berechtigungen für IAM-Benutzer zum Übergeben einer Rolle.

Sie können ein Amazon CloudWatch Flow-Protokoll entweder mit der Amazon VPC-Konsole oder der AWS CLI erstellen.

So erstellen Sie ein Flow-Protokoll für Transit-Gateway mit der Konsole

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateways.
3. Aktivieren Sie die Kontrollkästchen für ein oder mehrere Transit-Gateways und wählen Sie Aktionen, Flow-Protokoll erstellen aus.
4. Wählen Sie als Ziel die Option An Protokolle senden aus. CloudWatch
5. Für Ziel-Protokollgruppe, wählen Sie den Namen einer aktuellen Ziel-Protokollgruppe aus.

   > **Note**
   >
   > Wenn die Ziel-Protokollgruppe noch nicht existiert, wird durch Eingabe eines neuen Namens in dieses Feld eine neue Ziel-Protokollgruppe erstellt.

6. Geben Sie für die IAM-Rolle den Namen der Rolle an, die berechtigt ist, Logs in Logs zu CloudWatch veröffentlichen.
7. Für Log record format (Datensatzformat protokollieren) wählen Sie das Format für den Flow-Protokolldatensatz aus.
   - Wenn Sie das Standardformat verwenden möchten, wählen Sie AWS default format (-Standardformat) aus.
   - Um ein benutzerdefiniertes Format zu verwenden, wählen Sie Custom format (Benutzerdefiniertes Format) und dann Felder aus Log format (Format protokollieren) aus.
8. (Optional) Wählen Sie Add new tag (Neuen Tag hinzufügen) aus, um Tags auf das Flow-Protokoll anzuwenden.
9. Wählen Sie Create flow log (Flussprotokoll erstellen) aus.

So erstellen Sie ein Flow-Protokoll mit der Befehlszeile

Verwenden Sie einen der folgenden Befehle.

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

Im folgenden AWS CLI Beispiel wird ein Flow-Protokoll erstellt, das Transit-Gateway-Informationen erfasst. Die Flow-Protokolle werden mithilfe der IAM-Rolle an eine Protokollgruppe in CloudWatch Logs mit dem Namen `my-flow-logs` 123456789101 übermittelt. `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
```

AWS Transit Gateway Flow Logs-Datensätze in Amazon anzeigen CloudWatch

Sie können Ihre Flow-Protokolldatensätze je nach ausgewähltem Zieltyp mit der CloudWatch Logs-Konsole oder der Amazon S3 S3-Konsole anzeigen. Es kann nach dem Erstellen eines Flow-Protokolls einige Minuten dauern, bis das Protokoll in der Konsole angezeigt wird.

Um die in Logs veröffentlichten Flow-Log-Datensätze einzusehen CloudWatch

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Logs (Protokolle) und danach die Protokollgruppe mit Ihrem Flow-Protokoll. Es wird eine Liste der Protokollstreams für die einzelnen Transit-Gateways angezeigt.
3. Wählen Sie den Protokollstream aus, der die ID des Transit-Gateways enthält, für das Sie die Flow-Protokolldatensätze anzeigen möchten. Weitere Informationen finden Sie unter Flow-Protokolldatensätze für Transit-Gateway.

AWS Transit Gateway Flow Logs-Datensätze in Amazon CloudWatch Logs verarbeiten

Sie können mit Flow-Protokolldatensätzen genauso arbeiten wie mit allen anderen Protokollereignissen, die von CloudWatch Logs erfasst werden. Weitere Informationen zur Überwachung von Protokolldaten und Metrikfiltern finden Sie unter Metriken aus Protokollereignissen mithilfe von Filtern erstellen im CloudWatch Amazon-Benutzerhandbuch.

Beispiel: Erstellen Sie einen CloudWatch metrischen Filter und einen Alarm für ein Flow-Protokoll

In diesem Beispiel haben Sie ein Flow-Protokoll für `tgw-123abc456bca`. Sie möchten einen Alarm erstellen, um benachrichtigt zu werden, wenn ein Verbindungsversuch zu Ihrer Instance über den TCP-Port 22 (SSH) innerhalb einer Stunde mindestens 10 Mal fehlschlägt. Zuerst müssen Sie einen Metrikfilter erstellen, der mit dem Datenverkehrsmuster übereinstimmt, für das Sie den Alarm erstellen möchten. Danach können Sie einen Alarm für den Metrikfilter erstellen.

So erstellen Sie einen Metrikfilter für abgelehnten SSH-Datenverkehr und einen Alarm für den Filter

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Logs (Protokolle), Log groups (Protokollgruppen) aus.
3. Aktivieren Sie das Kontrollkästchen für die Protokollgruppe und wählen Sie dann Aktionen, Metrikfilter erstellen aus.
4. Geben Sie für Filter Pattern (Filtermuster) folgende Informationen ein.

```
[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. Wählen Sie für Select Log Data to Test (Die zu testenden Protokolldaten auswählen) den Protokollstream Ihres Transit-Gateways aus. (Optional) Um die Zeilen der Protokolldaten anzuzeigen, die mit dem Filtermuster übereinstimmen, wählen Sie Test Pattern (Testmuster). Wählen Sie danach Next (Weiter) aus.
6. Geben Sie einen Filternamen, einen Metrik-Namespace und einen Metriknamen ein. Legen Sie den Metrikwert auf **1** fest. Wenn Sie fertig sind, wählen Sie Next (Weiter) und dann Create metric filter (Metrikfilter erstellen) aus.
7. Wählen Sie im Navigationsbereich Alarms (Alarme) und All alarms (Alle Alarme) aus.
8. Wählen Sie Create alarm (Alarm erstellen) aus.
9. Wählen Sie den Namespace für den Metrikfilter aus, den Sie erstellt haben.

   Es kann einige Minuten dauern, bis neu erstellte Metriken in der Konsole angezeigt werden.

10. Wählen Sie den Metriknamen aus, den Sie erstellt haben, und klicken Sie dann auf Select metric (Metrik auswählen).
11. Konfigurieren Sie den Alarm wie folgt, und wählen Sie dann Weiter:
    - Wählen Sie für Statistic (Statistik) Sum (Summe) aus. Dadurch wird sichergestellt, dass Sie die Gesamtzahl der Datenpunkte für den angegebenen Zeitraum erfassen.
    - Wählen Sie als Period (Zeitraum) 1 Hour (1 Stunde) aus.
    - Wählen Sie für Whenever (Jederzeit) Greater/Equal (Größer/Gleich) aus und geben Sie **10** für den Schwellenwert ein.
    - Belassen Sie für Additional configuration (Zusätzliche Konfiguration), Datapoints to alarm (Zu alarmierende Datenpunkte) den Standardwert **1**.
12. Wählen Sie für Notification (Benachrichtigung) ein vorhandenes SNS-Thema aus oder wählen Sie Create new topic (Neues Thema erstellen), um ein neues zu erstellen. Wählen Sie Weiter aus.
13. Geben Sie einen Namen und eine Beschreibung für den Alarm ein und wählen Sie Next (Weiter).
14. Wenn Sie mit der Konfiguration des Alarms fertig sind, wählen Sie Create alarm (Alarm erstellen).

AWS Transit Gateway Flow Logs-Datensätze in Amazon S3

Flow-Protokolle können Flow-Protokolldaten direkt in Amazon S3 veröffentlichen.

Beim Veröffentlichen in Amazon S3 werden Flow-Protokolldaten in einem vorhandenen Amazon S3-Bucket veröffentlicht, den Sie zuvor angegeben haben. Flow-Protokolldatensätze für alle überwachten Transit-Gateways werden in eine Reihe von Protokolldateiobjekten veröffentlicht, die im Bucket abgelegt sind.

Gebühren für Datenaufnahme und Archivierung werden von Amazon CloudWatch for vended logs erhoben, wenn Sie Flow-Logs auf Amazon S3 veröffentlichen. Weitere Informationen zu den CloudWatch Preisen für verkaufte Logs erhalten Sie, wenn Sie Amazon CloudWatch Pricing öffnen, Logs auswählen und dann nach Vended Logs suchen.

Informationen zum Erstellen eines Amazon-S3-Buckets für die Verwendung mit Flow-Protokollen finden Sie unter Erstellen eines Buckets im Benutzerhandbuch zu Amazon S3.

Weitere Informationen zur Protokollierung mehrerer Konten finden Sie unter Zentrale Protokollierung in der AWS Solutions Library.

Weitere Informationen zu CloudWatch Logs finden Sie unter An Amazon S3 gesendete Logs im Amazon CloudWatch Logs-Benutzerhandbuch.

Inhalt

Flow-Protokolldateien

VPC-Flow-Protokolle sind eine Funktion, die Flow-Protokoll-Datensätze sammelt, sie in Protokolldateien konsolidiert und die Protokolldateien dann in 5-Minuten-Intervallen im Amazon-S3-Bucket veröffentlicht. Jede Protokolldatei enthält Flow-Protokolldatensätze für den in den letzten fünf Minuten aufgezeichneten IP-Verkehr.

Die maximale Dateigröße für eine Protokolldatei beträgt 75 MB. Wenn die Protokolldatei die Dateigrößenbeschränkung innerhalb des 5-Minuten-Zeitraums erreicht, fügt das Flow-Protokoll keine weiteren Flow-Protokolldatensätze hinzu. Anschließend wird das Flow-Protokoll im Amazon S3-Bucket veröffentlicht und eine neue Protokolldatei erstellt.

In Amazon S3 gibt das Feld Last modified (Zuletzt geändert) für die Flow-Protokolldatei Datum und Uhrzeit an, zu dem/der die Datei in den Amazon S3-Bucket hochgeladen wurde. Dieser Zeitpunkt ist später als der Zeitstempel im Dateinamen und die Differenz ist die Zeitspanne, die zum Upload der Datei in den Amazon S3-Bucket benötigt wird.

Protokolldateiformat

Sie können eines der folgenden Formate für die Protokolldateien festlegen. Jede Datei wird in eine einzelne Gzip-Datei komprimiert.

- Text – Klartext. Dies ist das Standardformat.
- Parquet – Apache Parquet ist ein spaltenförmiges Datenformat. Abfragen zu Daten im Parquet-Format sind 10 bis 100 Mal schneller im Vergleich zu Abfragen zu Daten im Klartext. Daten im Parquet-Format mit Gzip-Komprimierung benötigen 20 Prozent weniger Speicherplatz als Nur-Text bei Gzip-Komprimierung.

Protokolldateioptionen

Optional können Sie folgende Optionen angeben.

- HIVE-kompatible S3-Präfixe – Aktivieren Sie HIVE-kompatible Präfixe, anstatt Partitionen in Ihre HIVE-kompatiblen Tools zu importieren. Bevor Sie Abfragen ausführen, verwenden Sie den MSCK REPAIR TABLE-Befehl.
- Stündliche Partitionen – Wenn Sie über eine große Anzahl von Protokollen verfügen und Abfragen normalerweise auf eine bestimmte Stunde richten, können Sie schnellere Ergebnisse erzielen und Abfragekosten sparen, indem Sie Protokolle stündlich partitionieren.

S3-Bucket-Struktur der Protokolldatei

Protokolldateien werden im angegebenen Amazon-S3-Bucket mit einer Ordnerstruktur gespeichert, die auf der ID, der Region, dem Erstellungsdatum und den Zieloptionen des Flow-Protokolls basiert.

Standardmäßig werden die Dateien an den folgenden Speicherort geliefert.

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

Wenn Sie HIVE-kompatible S3-Präfixe aktivieren, werden die Dateien an den folgenden Speicherort geliefert.

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

Wenn Sie stündliche Partitionen aktivieren, werden die Dateien an den folgenden Speicherort geliefert.

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

Wenn Sie HIVE-kompatible Partitionen aktivieren und das Flow-Protokoll pro Stunde partitionieren, werden die Dateien an den folgenden Speicherort geliefert.

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

Protokolldateinamen

Der Dateiname einer Protokolldatei basiert auf der Flow-Protokoll-ID, der Region sowie dem Erstellungsdatum und der Uhrzeit. Dateinamen verwenden das folgende Format:

```
aws_account_id_vpcflowlogs_region_flow_log_id_YYYYMMDDTHHmmZ_hash.log.gz
```

Im Folgenden sehen Sie ein Beispiel für eine Protokolldatei für ein Flow-Protokoll, das von AWS-Konto 123456789012 für eine Ressource in der us-east-1-Region am June 20, 2018 um 16:20 UTC erstellt wurde. Die Datei enthält die Flow-Protokolldatensätze mit einer Endzeit zwischen 16:20:00 und 16:24:59.

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

IAM-Richtlinie für IAM-Prinzipale, die Flow-Protokolle in Amazon S3 veröffentlichen

Der IAM-Prinzipal, der das Flow-Protokoll erstellt, muss über die folgenden Berechtigungen verfügen, die für die Veröffentlichung von Flow-Protokollen im Amazon-S3-Ziel-Bucket erforderlich sind.

JSON

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

```
  ]
}
```

Amazon S3-Bucket-Berechtigungen für Flow-Protokolle

Standardmäßig sind Amazon S3-Buckets und die darin enthaltenen Objekte privat. Nur der Bucket-Besitzer kann auf den Bucket und die darin gespeicherten Objekte zugreifen. Der Bucket-Besitzer kann jedoch anderen Ressourcen und Benutzern Zugriffsberechtigungen erteilen, indem er eine Zugriffsrichtlinie schreibt.

Wenn der Benutzer, der das Flow-Protokoll erstellt, Eigentümer des Buckets ist und `PutBucketPolicy`- und `GetBucketPolicy`-Berechtigungen für den Bucket besitzt, fügen wir automatisch die folgende Richtlinie an den Bucket an. Diese neue automatisch generierte Richtlinie wird an die ursprüngliche Richtlinie angehängt.

Ansonsten muss der Bucket-Eigentümer diese Richtlinie zum Bucket hinzufügen und dabei die AWS-Konto -ID des Flow-Protokoll-Erstellers oder die Erstellung des Flow-Logs schlägt fehl. Weitere Informationen finden Sie unter Bucket-Richtlinien im Amazon Simple Storage Service-Benutzerhandbuch.

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:*"
                }
            }
        }
    ]
}
```

Der ARN, für den Sie angeben, *my-s3-arn* hängt davon ab, ob Sie HIVE-kompatible S3-Präfixe verwenden.

- Standardpräfixe

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

- HIVE-kompatible S3-Präfixe

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

Als bewährte Methode empfehlen wir, dass Sie diese Berechtigungen dem Prinzipal des Protokollzustellungsdienstes und nicht der Einzelperson gewähren. AWS-Konto ARNs Es ist auch eine bewährte Methode, die `aws:SourceAccount`- und `aws:SourceArn`-Bedingungsschlüssel zum Schutz vor dem Problem des verwirrten Stellvertreters zu verwenden. Das Quellkonto

ist der Eigentümer des Flow-Protokolls und der Quell-ARN ist der Platzhalter-AARN (*) des Protokolldienstes.

Erforderliche Schlüsselrichtlinie zur Verwendung mit SSE-KMS

Sie können die Daten in Ihrem Amazon-S3-Bucket schützen, indem Sie entweder Serverseitige Verschlüsselung mit von Amazon S3 verwalteten Schlüsseln (SSE-S3) oder Serverseitige Verschlüsselung mit KMS-Schlüsseln (SSE-KMS) aktivieren. Weitere Informationen finden Sie unter Schützen von Daten mithilfe serverseitiger Verschlüsselung im Amazon S3-Entwicklerhandbuch.

Mit SSE-KMS können Sie entweder einen AWS verwalteten Schlüssel oder einen vom Kunden verwalteten Schlüssel verwenden. Mit einem AWS verwalteten Schlüssel können Sie die kontoübergreifende Zustellung nicht verwenden. Flow-Protokolle werden vom Protokollbereitstellungskonto bereitgestellt, daher müssen Sie Zugriff für die kontoübergreifende Bereitstellung gewähren. Um kontoübergreifenden Zugriff auf Ihren S3 Bucket zu gewähren, verwenden Sie einen kundenverwalteten Schlüssel und geben den Amazon-Ressourcennamen (ARN) des vom Kunden verwalteten Schlüssel an, wenn Sie die Bucket-Verschlüsselung aktivieren. Weitere Informationen finden Sie unter Festlegen einer serverseitigen Verschlüsselung mit AWS KMS im Amazon S3-Benutzerhandbuch.

Wenn Sie SSE-KMS mit einem von Kunden verwalteten Schlüssel verwenden, müssen Sie der Schlüsselrichtlinie für Ihren Schlüssel (nicht der Bucket-Richtlinie für Ihren S3 Bucket) Folgendes hinzufügen, damit VPC-Flow-Protokolle in Ihren S3 Bucket schreiben können.

> **Note**
>
> Durch die Verwendung von S3 Bucket Keys können Sie bei AWS Key Management Service (AWS KMS) -Anforderungskosten sparen, GenerateDataKey indem Sie Ihre Anfragen auf AWS KMS Verschlüsselungs- und Entschlüsselungsvorgänge mithilfe eines Schlüssels auf Bucket-Ebene reduzieren. Standardmäßig führen nachfolgende Anfragen, die diesen Schlüssel auf Bucket-Ebene nutzen, nicht zu AWS KMS API-Anfragen und validieren den Zugriff nicht anhand der Schlüsselrichtlinie. AWS KMS

```
{
    "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": "*"
}
```

Amazon S3-Protokolldateiberechtigungen

Zusätzlich zu den erforderlichen Bucket-Richtlinien verwendet Amazon S3 Zugriffskontrolllisten (ACLs), um den Zugriff auf die von einem Flow-Protokoll erstellten Protokolldateien zu verwalten. Standardmäßig hat der Bucket-Eigentümer `FULL_CONTROL`-Berechtigungen für jede Protokolldatei. Der Protokollbereitstellungseigentümer hat keine Berechtigungen, wenn er nicht gleichzeitig der Bucket-Eigentümer ist. Das Konto für die Protokollbereitstellung hat `READ`- und `WRITE`-Berechtigungen. Weitere Informationen finden Sie unter Übersicht über die Zugriffskontrollliste (ACL) im Amazon Simple Storage Service-Benutzerhandbuch.

Erstellen Sie die AWS Transit Gateway Flow Logs-Quellkontorolle für Amazon S3

Erstellen Sie vom Quellkonto aus die Quellrolle in der AWS Identity and Access Management Konsole.

So erstellen Sie die Rolle des Quellkontos

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Richtlinien.
3. Wählen Sie Richtlinie erstellen aus.
4. Führen Sie auf der Seite Create policy (Richtlinie erstellen) die folgenden Schritte aus:

    1. Wählen Sie JSON.

2. Ersetzen Sie den Inhalt dieses Fensters durch die Berechtigungsrichtlinie am Anfang dieses Abschnitts.
3. Wählen Sie Next: Tags (Weiter: Tags) und Next: Review (Weiter: Prüfen) aus.
4. Geben Sie einen Namen und eine optionale Beschreibung für Ihre Richtlinie ein und wählen Sie dann Create Policy (Richtlinie erstellen) aus.

5. Wählen Sie im Navigationsbereich Rollen aus.
6. Wählen Sie Create role (Rolle erstellen) aus.
7. Für Trusted entity type (Vertrauenstyp der Entität) wählen Sie Custom trust policy (Benutzerdefinierte Vertrauensrichtlinie). Für Custom trust policy (Benutzerdefinierte Vertrauensrichtlinie), ersetzen Sie `"Principal": {},` mit dem Folgenden, was den Protokollbereitstellungsdienst spezifiziert. Wählen Sie Weiter aus.

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

8. Wählen Sie auf der Seite Add permissions (Berechtigungen hinzufügen) die zuvor in diesem Verfahren erstellte Richtlinie und anschließend Next (Weiter).
9. Geben Sie einen Namen für die Rolle sowie optional eine Beschreibung ein.
10. Wählen Sie Rolle erstellen aus.

Erstellen Sie einen AWS Transit Gateway Flow Logs-Datensatz, der auf Amazon S3 veröffentlicht wird

Nachdem Sie Ihren Amazon S3-Bucket erstellt und konfiguriert haben, können Sie Flow-Protokolle für Transit-Gateways erstellen. Sie können ein Amazon S3 S3-Flow-Protokoll entweder mit der Amazon VPC-Konsole oder der AWS CLI erstellen.

So erstellen Sie ein Flow-Protokoll für Transit-Gateway, das mithilfe der Konsole in Amazon S3 veröffentlicht

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Transit Gateways oder Transit Gateway Attachments (Transit-Gateway-Anhänge) aus.

3. Aktivieren Sie die Kontrollkästchen für ein oder mehrere Transit-Gateways oder Transit-Gateway-Anhänge.
4. Klicken Sie auf Actions (Aktionen), Create flow log (Flow-Protokoll erstellen).
5. Konfigurieren Sie die Flow-Protokoll-Einstellungen. Weitere Informationen finden Sie unter So konfigurieren Sie Flow-Protokoll-Einstellungen.

So konfigurieren Sie Flow-Protokolleinstellungen mithilfe der Konsole

1. Wählen Sie für Destination (Ziel) die Option Send to an Amazon S3 bucket (An einen S3 Bucket senden).
2. Geben Sie für S3 bucket ARN (S3-Bucket-ARN) den Amazon-Ressourcennamen (ARN) eines vorhandenen Amazon S3-Buckets an. Sie können optional einen Unterordner einfügen. Um beispielsweise den Unterordner `my-logs` im Bucket `my-bucket` anzugeben, verwenden Sie den folgenden ARN:

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

   Der Bucket kann als Unterordnername nicht `AWSLogs` verwenden, da dieser Begriff reserviert ist.

   Wenn Sie der Eigentümer des Buckets sind, erstellen wir automatisch eine Ressourcenrichtlinie und fügen sie dem Bucket hinzu. Weitere Informationen finden Sie unter Amazon S3-Bucket-Berechtigungen für Flow-Protokolle.
3. Für Log record format (Datensatzformat protokollieren) geben Sie das Format für den Flow-Protokolldatensatz an.

   - Wenn Sie das Standardformat für Flow-Protokolldatensätze verwenden möchten, wählen Sie AWS default format (-Standardformat).
   - Wenn Sie ein benutzerdefiniertes Format erstellen möchten, wählen Sie Custom format (Benutzerdefiniertes Format). Wählen Sie für Protokollformat die Felder, die im Flow-Protokolldatensatz berücksichtigt werden sollen.
4. Geben Sie für Log file format (Protokolldateiformat) das Format für die Protokolldatei an.

   - Text – Klartext. Dies ist das Standardformat.
   - Parquet – Apache Parquet ist ein spaltenförmiges Datenformat. Abfragen zu Daten im Parquet-Format sind 10 bis 100 Mal schneller im Vergleich zu Abfragen zu Daten im

Klartext. Daten im Parquet-Format mit Gzip-Komprimierung benötigen 20 Prozent weniger Speicherplatz als Nur-Text bei Gzip-Komprimierung.

5. (Optional) Um Hive-kompatible S3-Präfixe zu verwenden, wählen Sie Hive-compatible S3 prefix (Hive-kompatibles S3-Präfix), Enable (Aktivieren).
6. (Optional) Um Ihre Flow-Protokolle pro Stunde zu partitionieren, wählen Sie Every 1 hour (60 mins) (Jede 1 Stunde (60 Minuten)).
7. (Optional) Um dem Flow-Protokoll ein Tag hinzuzufügen, wählen Sie Add new tag (Neues Tag hinzufügen) und geben Sie den Tag-Schlüssel und -Wert an.
8. Wählen Sie Create flow log (Flussprotokoll erstellen) aus.

So erstellen Sie ein Flow-Protokoll, das mithilfe eines Befehlszeilen-Tools in Amazon S3 veröffentlicht

Verwenden Sie einen der folgenden Befehle.

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

Das folgende AWS CLI Beispiel erstellt ein Flow-Protokoll, das den gesamten Transit-Gateway-Verkehr für VPC erfasst `tgw-00112233344556677` und die Flow-Logs an einen Amazon S3 S3-Bucket namens `flow-log-bucket` übermittelt. Der Parameter `--log-format` legt ein benutzerdefiniertes Format für die Flow-Protokolldatensätze fest.

```
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/'
```

AWS Transit Gateway Flow Logs-Datensätze in Amazon S3 anzeigen

So zeigen Sie in Amazon S3 veröffentlichte Flow-Protokolldatensätze an

1. Öffnen Sie die Amazon S3 S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Wählen Sie für Bucket name (Bucket-Name) den Bucket aus, in den die Flow-Protokolle veröffentlicht werden.
3. Wählen Sie für Name das Kontrollkästchen neben der Protokolldatei aus. Wählen Sie im Objektübersichtsfeld Download.

Verarbeitete AWS Transit Gateway Flow Logs-Datensätze in Amazon S3

Die Protokolldateien werden komprimiert. Wenn Sie die Protokolldateien unter Verwendung der Amazon S3-Konsole öffnen, werden sie dekomprimiert und die Flow-Protokolldatensätze werden angezeigt. Wenn Sie die Dateien herunterladen, müssen Sie sie dekomprimieren, um die Flow-Protokolldatensätze anzuzeigen.

AWS Transit Gateway, Flow Logs-Datensätze in Amazon Data Firehose

Themen

Flow-Logs können Flow-Log-Daten direkt in Firehose veröffentlichen. Sie können wählen, ob Sie Flow-Protokolle für dasselbe Konto wie den Ressourcenmonitor oder für ein anderes Konto veröffentlichen möchten.

Voraussetzungen

Bei der Veröffentlichung in Firehose werden die Flow-Protokolldaten in einem Firehose-Lieferstream im Klartextformat veröffentlicht. Sie müssen zuerst einen Firehose-Lieferstream erstellt haben. Die Schritte zum Erstellen eines Delivery Streams finden Sie unter Creating an Amazon Data Firehose Delivery Stream im Amazon Data Firehose Developer Guide.

Preise

Es fallen die üblichen Kosten für Einnahme und Lieferung an. Weitere Informationen finden Sie unter Amazon CloudWatch Pricing, wählen Sie Logs aus und suchen Sie nach Vending Logs.

IAM-Rollen für die kontoübergreifende Bereitstellung

Wenn Sie in Kinesis Data Firehose veröffentlichen, können Sie einen Bereitstellungsstream auswählen, der sich in demselben Konto wie die zu überwachende Ressource (das Quellkonto) oder

in einem anderen Konto (dem Zielkonto) befindet. Um die kontoübergreifende Übermittlung von Flow-Protokollen an Firehose zu ermöglichen, müssen Sie eine IAM-Rolle im Quellkonto und eine IAM-Rolle im Zielkonto erstellen.

Rollen

- Rolle des Quellkontos
- Rolle des Zielkontos

Rolle des Quellkontos

Erstellen Sie im Quellkonto eine Rolle, die die folgenden Berechtigungen gewährt. In diesem Beispiel lautet der Name der Rolle `mySourceRole`, allerdings können Sie einen anderen Namen für diese Rolle wählen. Die letzte Anweisung ermöglicht es der Rolle im Zielkonto, diese Rolle zu übernehmen. Die Bedingungsanweisungen stellen sicher, dass diese Rolle nur an den Protokollbereitstellungsservice und nur beim Überwachen der angegebenen Ressource übergeben wird. Wenn Sie Ihre Richtlinie erstellen, geben Sie die VPCs Netzwerkschnittstellen oder Subnetze, die Sie überwachen, mit dem Bedingungsschlüssel `iam:AssociatedResourceARN` an.

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"
        }
    ]
}
```

Stellen Sie sicher, dass Ihre Rolle die folgende Vertrauensrichtlinie hat, die es dem Protokollservice erlaubt, die Rolle zu übernehmen.

JSON

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

Rolle des Zielkontos

Erstellen Sie im Zielkonto eine Rolle mit einem Namen, der mit beginnt AWSLogDeliveryFirehoseCrossAccountRole. Die Rolle muss die folgenden Berechtigungen enthalten.

JSON

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

Stellen Sie sicher, dass diese Rolle über die folgende Vertrauensrichtlinie verfügt, mit der die Rolle, die Sie im Quellkonto erstellt haben, diese Rolle übernehmen kann.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/mySourceRole"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Erstellen Sie die AWS Transit Gateway Flow Logs-Quellkontorolle für Amazon Data Firehose

Erstellen Sie vom Quellkonto aus die Quellrolle in der AWS Identity and Access Management Konsole.

So erstellen Sie die Rolle des Quellkontos

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Richtlinien.
3. Wählen Sie Richtlinie erstellen aus.
4. Führen Sie auf der Seite Create policy (Richtlinie erstellen) die folgenden Schritte aus:
    1. Wählen Sie JSON.
    2. Ersetzen Sie den Inhalt dieses Fensters durch die Berechtigungsrichtlinie am Anfang dieses Abschnitts.
    3. Wählen Sie Next: Tags (Weiter: Tags) und Next: Review (Weiter: Prüfen) aus.
    4. Geben Sie einen Namen und eine optionale Beschreibung für Ihre Richtlinie ein und wählen Sie dann Create Policy (Richtlinie erstellen) aus.
5. Wählen Sie im Navigationsbereich Rollen aus.
6. Wählen Sie Create role (Rolle erstellen) aus.
7. Für Trusted entity type (Vertrauenstyp der Entität) wählen Sie Custom trust policy (Benutzerdefinierte Vertrauensrichtlinie). Für Custom trust policy (Benutzerdefinierte Vertrauensrichtlinie), ersetzen Sie `"Principal": {},` mit dem Folgenden, was den Protokollbereitstellungsdienst spezifiziert. Wählen Sie Weiter aus.

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

8. Wählen Sie auf der Seite Add permissions (Berechtigungen hinzufügen) die zuvor in diesem Verfahren erstellte Richtlinie und anschließend Next (Weiter).
9. Geben Sie einen Namen für die Rolle sowie optional eine Beschreibung ein.
10. Wählen Sie Rolle erstellen aus.

Erstellen Sie die AWS Transit Gateway Flow Logs-Zielkontorolle für Amazon Data Firehose

Erstellen Sie vom Zielkonto aus die Zielrolle in der AWS Identity and Access Management Konsole.

So erstellen Sie die Rolle des Zielkontos

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Richtlinien.
3. Wählen Sie Richtlinie erstellen aus.
4. Führen Sie auf der Seite Create policy (Richtlinie erstellen) die folgenden Schritte aus:
    1. Wählen Sie JSON.
    2. Ersetzen Sie den Inhalt dieses Fensters durch die Berechtigungsrichtlinie am Anfang dieses Abschnitts.
    3. Wählen Sie Next: Tags (Weiter: Tags) und Next: Review (Weiter: Prüfen) aus.
    4. Geben Sie einen Namen für Ihre Richtlinie ein, der mit beginnt AWSLogDeliveryFirehoseCrossAccountRole, und wählen Sie dann Richtlinie erstellen aus.
5. Wählen Sie im Navigationsbereich Rollen aus.
6. Wählen Sie Create role (Rolle erstellen) aus.
7. Für Trusted entity type (Vertrauenstyp der Entität) wählen Sie Custom trust policy (Benutzerdefinierte Vertrauensrichtlinie). Für Custom trust policy (Benutzerdefinierte Vertrauensrichtlinie), ersetzen Sie `"Principal": {},` mit dem Folgenden, was den Protokollbereitstellungsdienst spezifiziert. Wählen Sie Weiter aus.

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

8. Wählen Sie auf der Seite Add permissions (Berechtigungen hinzufügen) die zuvor in diesem Verfahren erstellte Richtlinie und anschließend Next (Weiter).
9. Geben Sie einen Namen für die Rolle sowie optional eine Beschreibung ein.
10. Wählen Sie Rolle erstellen aus.

Erstellen Sie einen AWS Transit Gateway Flow Logs-Datensatz, der in Amazon Data Firehose veröffentlicht wird

Erstellen Sie ein Transit Gateway Flow Log, das in Amazon Data Firehose veröffentlicht wird. Bevor Sie das Flow-Protokoll erstellen können, stellen Sie sicher, dass Sie die Quell- und Ziel-IAM-Kontorollen für die kontoübergreifende Zustellung eingerichtet haben und dass Sie den Firehose-Lieferstream erstellt haben. Weitere Informationen finden Sie unter Datenflussprotokolle von Amazon Data Firehose. Sie können ein Firehose-Flow-Protokoll entweder mit der Amazon VPC-Konsole oder der AWS CLI erstellen.

So erstellen Sie ein Transit-Gateway-Flow-Protokoll, das mithilfe der Konsole in Firehose veröffentlicht wird

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Transit Gateways oder Transit Gateway Attachments (Transit-Gateway-Anhänge) aus.
3. Aktivieren Sie die Kontrollkästchen für ein oder mehrere Transit-Gateways oder Transit-Gateway-Anhänge.
4. Klicken Sie auf Actions (Aktionen), Create flow log (Flow-Protokoll erstellen).
5. Wählen Sie als Destination (Ziel) die Option Send to a Firehose Delivery System (An ein Firehose Delivery System senden) aus.
6. Wählen Sie für den Firehose Delivery Stream ARN (Firehose-Bereitstellungs-Stream-ARN den ARN eines von Ihnen erstellten Bereitstellungs-Streams aus, in dem das Flow-Protokoll veröffentlicht werden soll.
7. Für Log record format (Datensatzformat protokollieren) geben Sie das Format für den Flow-Protokolldatensatz an.
   - Wenn Sie das Standardformat für Flow-Protokolldatensätze verwenden möchten, wählen Sie AWS default format (-Standardformat).
   - Wenn Sie ein benutzerdefiniertes Format erstellen möchten, wählen Sie Custom format (Benutzerdefiniertes Format). Wählen Sie für Protokollformat die Felder, die im Flow-Protokolldatensatz berücksichtigt werden sollen.
8. (Optional) Um dem Flow-Protokoll ein Tag hinzuzufügen, wählen Sie Add new tag (Neues Tag hinzufügen) und geben Sie den Tag-Schlüssel und -Wert an.
9. Wählen Sie Create flow log (Flussprotokoll erstellen) aus.

Um ein Flow-Protokoll zu erstellen, das mit dem Befehlszeilentool in Firehose veröffentlicht wird

Verwenden Sie einen der folgenden Befehle:

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

Das folgende AWS CLI-Beispiel erstellt ein Flow-Protokoll, das Transit-Gateway-Informationen erfasst und das Flow-Protokoll an den angegebenen Firehose-Lieferstream übermittelt.

```
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
```

Das folgende AWS CLI-Beispiel erstellt ein Flow-Protokoll, das Transit-Gateway-Informationen erfasst und das Flow-Protokoll an einen anderen Firehose-Lieferstream als das Quellkonto übermittelt.

```
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
```

AWS Transit Gateway Flow Logs mit APIs oder der CLI erstellen und verwalten

Sie können die auf dieser Seite beschriebenen Aufgaben über die Befehlszeile ausführen.

Bei der Verwendung des create-flow-logsBefehls gelten die folgenden Einschränkungen:

- `--resource-ids` hat eine maximale Beschränkung von 25 `TransitGateway` oder `TransitGatewayAttachment` Ressourcentypen.
- `--traffic-type` ist standardmäßig kein erforderliches Feld. Ein Fehler wird zurückgegeben, wenn Sie dies für Transit-Gateway-Ressourcentypen angeben. Dieses Limit gilt nur für Transit-Gateway-Ressourcentypen.
- `--max-aggregation-interval` besitzt den `60`-Standardwert und ist der einzige akzeptierte Wert für Transit-Gateway-Ressourcentypen. Wenn Sie versuchen, einen anderen Wert zu übergeben, wird ein Fehler zurückgegeben. Dieses Limit gilt nur für Transit-Gateway-Ressourcentypen.
- `--resource-type` unterstützt zwei neue Ressourcentypen: `TransitGateway` und `TransitGatewayAttachment`.
- `--log-format` schließt alle Protokollfelder für Transit-Gateway-Ressourcentypen ein, wenn Sie nicht festlegen, welche Felder Sie einbeziehen möchten. Dies gilt nur für Transit-Gateway-Ressourcentypen.

Erstellen eines Flow-Protokolls

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

Beschreibung Ihrer Flow-Protokolle

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

Anzeigen Ihrer Flow-Protokolldatensätze (Protokollereignisse)

- get-log-events (AWS CLI)
- CWLLogGet-Event (AWS Tools for Windows PowerShell)

Löschen eines Flow-Protokolls

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

AWS Transit Gateway Flow Logs-Datensätze anzeigen

Zeigen Sie Informationen zu Ihren Transit-Gateway-Flow-Logs über die Amazon VPC an. Wenn Sie eine Ressource auswählen, werden alle Flow-Logs für diese Ressource aufgelistet. Es werden folgende Informationen angezeigt: die ID des Flow-Protokolls, die Flow-Protokollkonfiguration sowie Informationen zum Status des Flow-Protokolls.

So zeigen Sie Informationen zu Flow-Protokollen für Transit-Gateways an

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Transit Gateways oder Transit Gateway Attachments (Transit-Gateway-Anhänge) aus.
3. Wählen Sie ein Transit-Gateway oder Transit-Gateway-Anhang aus und wählen Sie Flow Logs (Flow-Protokolle) aus. Die Informationen zu den Flow-Protokollen werden auf der Registerkarte angezeigt. Die Spalte Destination type (Zieltyp) zeigt das Ziel an, in dem die Flow-Protokolle veröffentlicht werden.

AWS Transit Gateway Flow Logs-Tags verwalten

Sie können Tags für ein Flow-Protokoll in den Konsolen von Amazon EC2 und Amazon VPC hinzufügen oder entfernen.

So fügen Sie Tags für ein Flow-Protokoll für Transit-Gateway hinzu oder entfernen sie

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Transit Gateways oder Transit Gateway Attachments (Transit-Gateway-Anhänge) aus.
3. Wählen Sie ein Transit-Gateway oder einen Transit-Gateway-Anhang
4. Wählen Sie Manage tags (Tags verwalten) für das jeweilige Flow-Protokoll.
5. Um ein neues Tag hinzuzufügen, wählen Sie Create Tag. Zum Entfernen eines Tags wählen Sie die „Löschen“-Schaltfläche (x) aus.
6. Wählen Sie Speichern.

AWS Transit Gateway Flow Logs-Datensätze durchsuchen

Sie können Ihre Flow-Protokolleinträge, die in Logs veröffentlicht wurden, mithilfe der CloudWatch CloudWatch Logs-Konsole durchsuchen. Sie können Metrikfilter verwenden, um Flow-Protokolldatensätze zu filtern. Flow-Protokolldatensätze sind durch Leerzeichen getrennt.

So suchen Sie mit der CloudWatch Logs-Konsole nach Flow-Log-Datensätzen

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Logs (Protokolle) und dann Log groups (Protokollgruppen) aus.
3. Wählen Sie die Protokollgruppe mit Ihrem Flow-Protokoll. Es wird eine Liste der Protokollstreams für die einzelnen Transit-Gateways angezeigt.
4. Wählen Sie den einzelnen Protokollstream aus, wenn Sie den Transit-Gateway kennen, nach dem Sie suchen. Alternativ können Sie Search Log Group (Log-Gruppe durchsuchen) wählen, um die gesamte Protokollgruppe zu durchsuchen. Dies kann einige Zeit in Anspruch nehmen, wenn sich viele Transit-Gateways in Ihrer Protokollgruppe befinden oder je nach ausgewähltem Zeitbereich.
5. Geben Sie für Filter events (Filterereignisse) die folgende Zeichenfolge ein. Hierbei wird davon ausgegangen, dass der Flow-Protokolldatensatz das Standardformat verwendet.

```
[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. Ändern Sie den Filter nach Bedarf, indem Sie Werte für die Felder angeben. In den folgenden Beispielen wird nach bestimmten Quell-IP-Adressen gefiltert.

```
[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]
```

Das folgende Beispiel filtert nach Transit-Gateway-ID tgw-123abc456bca, Zielport und Anzahl der 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]
```

Löschen Sie einen AWS Transit Gateway Flow Logs-Datensatz

Sie können ein Flow-Protokoll für Transit-Gateway über die Amazon VPC-Konsole löschen.

Mithilfe dieser Verfahren wird der Flow-Protokoll-Service für eine Ressource deaktiviert. Durch das Löschen eines Flow-Protokolls werden die vorhandenen Protokollstreams aus CloudWatch Protokollen oder Protokolldateien aus Amazon S3 nicht gelöscht. Vorhandene Flow-Protokolldaten müssen über die Konsole des jeweiligen Service gelöscht werden. Darüber hinaus werden beim Löschen eines Flow-Protokolls, das in Amazon S3 veröffentlicht wird, die Bucket-Richtlinien und die Zugriffskontrolllisten für Protokolldateien (ACLs) nicht entfernt.

So löschen Sie ein Flow-Protokoll für Transit-Gateway

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Transit Gateways.
3. Wählen Sie eine Transit-Gateway-ID aus.

4. Wählen Sie im Abschnitt „Flow-Protokolle“ die Flow-Protokolle aus, die Sie löschen möchten.
5. Wählen Sie Actions (Aktionen) und dann Delete flow logs group (Flow-Protokolle löschen) aus.
6. Bestätigen Sie, dass Sie den Flow löschen möchten, indem Sie Delete (Löschen) auswählen.

Metriken und Ereignisse in AWS Transit Gateway

Sie können die folgenden Features verwenden, um Ihre Transit Gateways zu überwachen, Datenverkehrsmuster zu analysieren und Probleme mit Ihren Transit Gateways beheben.

CloudWatch Metriken

Sie können Amazon verwenden CloudWatch , um Statistiken über Datenpunkte für Ihre Transit-Gateways als geordneten Satz von Zeitreihendaten, sogenannten Metriken, abzurufen. Mit diesen Metriken können Sie überprüfen, ob Ihr System die erwartete Leistung zeigt. Weitere Informationen finden Sie unter CloudWatch Metriken in AWS Transit Gateway.

Flow-Protokolle für Transit-Gateway

Sie können mit Flow-Protokollen für Transit-Gateway detaillierte Informationen über den Netzwerkverkehr auf Ihren Transit-Gateways erfassen. Weitere Informationen finden Sie unter Flow-Protokolle für Transit-Gateway.

VPC-Flow-Protokolle

Sie können VPC Flow Logs verwenden, um detaillierte Informationen über den Verkehr zu und von den, VPCs die an Ihre Transit-Gateways angeschlossen sind, zu erfassen. Weitere Informationen finden Sie unter VPC-Flow-Protokolle im Benutzerhandbuch für Amazon VPC.

CloudTrail Logs

Sie können AWS CloudTrail damit detaillierte Informationen über die Aufrufe der Transit-Gateway-API erfassen und sie als Protokolldateien in Amazon S3 speichern. Sie können diese CloudTrail Protokolle verwenden, um festzustellen, welche Anrufe getätigt wurden, von welcher Quell-IP-Adresse der Anruf kam, wer den Anruf getätigt hat, wann der Anruf getätigt wurde usw. Weitere Informationen finden Sie unter CloudTrail protokolliert.

CloudWatch Ereignisse mit Network Manager

Sie können Ereignisse AWS Network Manager an CloudWatch Zielfunktionen oder Streams weiterleiten und diese Ereignisse dann an diese weiterleiten. Network Manager generiert Events für Topologieänderungen, Routing-Updates und Statusaktualisierungen, die alle verwendet werden können, um Sie auf Änderungen an Ihren Transit-Gateways aufmerksam zu machen. Weitere Informationen finden Sie unter Überwachen Ihres globalen Netzwerks mithilfe von CloudWatch Ereignissen im Benutzerhandbuch für AWS globale Netzwerke für Transit Gateways.

CloudWatch Metriken in AWS Transit Gateway

Amazon VPC veröffentlicht Datenpunkte CloudWatch für Ihre Transit-Gateways und Transit-Gateway-Anhänge an Amazon. CloudWatchermöglicht es Ihnen, Statistiken über diese Datenpunkte in Form eines geordneten Satzes von Zeitreihendaten, sogenannten Metriken, abzurufen. Sie können sich eine Metrik als eine zu überwachende Variable und die Datenpunkte als die Werte dieser Variable im Laufe der Zeit vorstellen. Jeder Datenpunkt verfügt über einen zugewiesenen Zeitstempel und eine optionale Maßeinheit.

Mit den Metriken können Sie überprüfen, ob Ihr System die erwartete Leistung zeigt. Sie können beispielsweise einen CloudWatch Alarm erstellen, um eine bestimmte Metrik zu überwachen und eine Aktion einzuleiten (z. B. das Senden einer Benachrichtigung an eine E-Mail-Adresse), wenn die Metrik außerhalb des für Sie akzeptablen Bereichs liegt.

Amazon VPC misst und sendet seine Metriken CloudWatch in 60-Sekunden-Intervallen.

Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.

Inhalt

Transit-Gateway-Metriken

Der `AWS/TransitGateway`-Namespace enthält die folgenden Metriken.

Alle Metriken werden immer gemeldet. Ihre Werte hängen vom Verkehr ab, der über das Transit-Gateway fließt. Die Metrische Abmessungen des Transit-Gateways unterstützten Abmessungen finden Sie unter.

Metrik	Beschreibung
`BytesDropCountBlackhole`	Die Anzahl der verworfenen Bytes, weil sie einer `blackhole` -Route entsprachen Statistiken: Die einzige aussagekräftige Statistik ist `Sum`.

Metrik	Beschreibung
BytesDropCountNoRoute	Die Anzahl der verworfenen Bytes, weil sie keiner Route entsprachen. Statistiken: Die einzige aussagekräftige Statistik ist Sum.
BytesIn	Die Anzahl der vom Transit Gateway empfangenen Bytes. Statistiken: Die einzige aussagekräftige Statistik ist Sum.
BytesOut	Die Anzahl der vom Transit Gateway gesendeten Bytes. Statistiken: Die einzige aussagekräftige Statistik ist Sum.
PacketsIn	Die Anzahl der vom Transit Gateway empfangenen Pakete. Statistiken: Die einzige aussagekräftige Statistik ist Sum.
PacketsOut	Die Anzahl der vom Transit Gateway gesendeten Pakete. Statistiken: Die einzige aussagekräftige Statistik ist Sum.
PacketDropCountBlackhole	Die Anzahl der verworfenen Pakete, weil sie einer blackhole -Route entsprachen Statistiken: Die einzige aussagekräftige Statistik ist Sum.
PacketDropCountNoRoute	Die Anzahl der verworfenen Pakete, weil sie keiner Route entsprachen Statistiken: Die einzige aussagekräftige Statistik ist Sum.
PacketDropCountTTLExpired	Die Anzahl der Pakete, die verworfen wurden, weil die TTL abgelaufen ist. Statistiken: Die einzige aussagekräftige Statistik ist Sum.

Metriken auf Anhangsebene und Availability Zone

Die folgenden Metriken sind für Transit-Gateway-Anhänge verfügbar. Alle Anhangs-Metriken werden im Konto des Transit-Gateway-Besitzers veröffentlicht. Alle Anhangs-Metriken werden im Konto des Anhang-Besitzers veröffentlicht. Der Anhang-Besitzer kann nur die Metriken für seinen eigenen Anhang anzeigen. Weitere Informationen zu den unterstützten Anlagentypen finden Sie unter the section called “Ressourcen-Anhänge”.

Messwerte für Verfügbarkeitszonen sind für aktivierte Availability Zones (AZs) auf Transit-Gateway-Anhängen verfügbar. Nur VPC-Anhänge unterstützen Pro-AZ-Metriken. Alle Metriken auf AZ-Ebene werden auf dem Konto des Transit-Gateway-Besitzers veröffentlicht. Einzelne AZ-Metriken für einen Anhang werden auch auf dem Konto des Besitzers des Anhangs veröffentlicht. Der Eigentümer des Anhangs kann nur die Kennzahlen pro AZ für seinen eigenen Anhang einsehen.

Es werden immer alle Messwerte gemeldet. Ihre Werte hängen vom Datenverkehr ab, der and/or aus dem Transit-Gateway-Anhang eingeht. Die Metrische Abmessungen des Transit-Gateways unterstützten Abmessungen finden Sie unter.

Metrik	Beschreibung
`BytesDropCountBlackhole`	Die Anzahl der Bytes, die gelöscht wurden, weil sie einer `blackhole` -Route auf dem Transit-Gateway-Anhang entsprachen. Statistiken: Die einzige aussagekräftige Statistik ist `Sum`.
`BytesDropCountNoRoute`	Die Anzahl der Bytes, die gelöscht wurden, weil sie nicht mit einer Route auf dem Transit-Gateway-Anhang übereinstimmten. Statistiken: Die einzige aussagekräftige Statistik ist `Sum`.
`BytesIn`	Die Anzahl der von dem Transit-Gateway-Anhang empfangenen Bytes. Statistiken: Die einzige aussagekräftige Statistik ist `Sum`.
`BytesOut`	Die Anzahl der vom Transit Gateway an den Anhang gesendeten Bytes. Statistiken: Die einzige aussagekräftige Statistik ist `Sum`.

Metrik	Beschreibung
PacketsIn	Die Anzahl der Pakete, die das Transit Gateway von dem Anhang empfangen hat. Statistiken: Die einzige aussagekräftige Statistik ist Sum.
PacketsOut	Die Anzahl der vom Transit Gateway an den Anhang gesendeten Pakete. Statistiken: Die einzige aussagekräftige Statistik ist Sum.
PacketDropCountBlackhole	Die Anzahl der Pakete, die gelöscht wurden, weil sie einer blackhole -Route auf dem Transit-Gateway-Anhang entsprachen. Statistiken: Die einzige aussagekräftige Statistik ist Sum.
PacketDropCountNoRoute	Die Anzahl der verworfenen Pakete, weil sie keiner Route entsprachen Statistiken: Die einzige aussagekräftige Statistik ist Sum.
PacketDropCountTTLExpired	Die Anzahl der Pakete, die verworfen wurden, weil die TTL abgelaufen ist. Statistiken: Die einzige aussagekräftige Statistik ist Sum.

Metrische Abmessungen des Transit-Gateways

Filtern Sie Metrikdaten des Transit-Gateways anhand der folgenden Dimensionen:

Dimension	Beschreibung
TransitGateway	Filtert die Metrikdaten nach Transit Gateway.
TransitGatewayAttachment	Filtert die Metrikdaten nach Transit-Gateway-Anhang.

Dimension	Beschreibung
`TransitGateway` , `AvailabilityZone`	Filtert die Metrikdaten sowohl nach Transit-Gateway als auch nach Verfügbarkeitszone.
`TransitGatewayAttachment` , `AvailabilityZone`	Filtert die Metrikdaten sowohl nach der Transit-Gateway-Verbindung als auch nach der Verfügbarkeitszone.

AWS Transit Gateway Gateway-API-Aufrufe protokollieren mit AWS CloudTrail

AWS Transit Gateway; ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem ausgeführten Aktionen bereitstellt AWS-Service. CloudTrail erfasst alle API-Aufrufe für Transit Gateway als Ereignisse. Zu den erfassten Anrufen gehören Anrufe von der Transit Gateway Gateway-Konsole und Code-Aufrufe an die Transit Gateway Gateway-API-Operationen. Anhand der von gesammelten Informationen können Sie die Anfrage CloudTrail, die an Transit Gateway gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wann sie gestellt wurde, und weitere Details ermitteln.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anforderung mit Anmeldeinformationen des Root-Benutzers oder des Benutzers gestellt wurde.
- Die Anforderung wurde im Namen eines IAM-Identity-Center-Benutzers erstellt.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anforderung aus einem anderen AWS-Service gesendet wurde.

CloudTrail ist in Ihrem aktiv AWS-Konto , wenn Sie das Konto erstellen, und Sie haben automatisch Zugriff auf den CloudTrail Eventverlauf. Der CloudTrail Ereignisverlauf bietet eine einsehbare,

durchsuchbare, herunterladbare und unveränderliche Aufzeichnung der aufgezeichneten Verwaltungsereignisse der letzten 90 Tage in einem. AWS-Region Weitere Informationen finden Sie im AWS CloudTrail Benutzerhandbuch unter Arbeiten mit dem CloudTrail Ereignisverlauf. Für die Anzeige des Eventverlaufs CloudTrail fallen keine Gebühren an.

Für eine fortlaufende Aufzeichnung der Ereignisse in AWS-Konto den letzten 90 Tagen erstellen Sie einen Trail- oder CloudTrailLake-Event-Datenspeicher.

CloudTrail Pfade

Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Alle mit dem erstellten Pfade AWS-Managementkonsole sind regionsübergreifend. Sie können mithilfe von AWS CLI einen Einzel-Region- oder einen Multi-Region-Trail erstellen. Es wird empfohlen, einen Trail mit mehreren Regionen zu erstellen, da Sie alle Aktivitäten AWS-Regionen in Ihrem Konto erfassen. Wenn Sie einen Einzel-Region-Trail erstellen, können Sie nur die Ereignisse anzeigen, die im AWS-Region des Trails protokolliert wurden. Weitere Informationen zu Trails finden Sie unter Erstellen eines Trails für Ihr AWS-Konto und Erstellen eines Trails für eine Organisation im AWS CloudTrail -Benutzerhandbuch.

Sie können eine Kopie Ihrer laufenden Verwaltungsereignisse kostenlos an Ihren Amazon S3 S3-Bucket senden, CloudTrail indem Sie einen Trail erstellen. Es fallen jedoch Amazon S3 S3-Speichergebühren an. Weitere Informationen zur CloudTrail Preisgestaltung finden Sie unter AWS CloudTrail Preise. Informationen zu Amazon-S3-Preisen finden Sie unter Amazon S3 – Preise.

CloudTrail Datenspeicher für Ereignisse in Lake

CloudTrail Mit Lake können Sie SQL-basierte Abfragen für Ihre Ereignisse ausführen. CloudTrail Lake konvertiert bestehende Ereignisse im zeilenbasierten JSON-Format in das Apache ORC-Format. ORC ist ein spaltenförmiges Speicherformat, das für den schnellen Abruf von Daten optimiert ist. Die Ereignisse werden in Ereignisdatenspeichern zusammengefasst, bei denen es sich um unveränderliche Sammlungen von Ereignissen handelt, die auf Kriterien basieren, die Sie mit Hilfe von erweiterten Ereignisselektoren auswählen. Die Selektoren, die Sie auf einen Ereignisdatenspeicher anwenden, steuern, welche Ereignisse bestehen bleiben und für Sie zur Abfrage verfügbar sind. Weitere Informationen zu CloudTrail Lake finden Sie unter Arbeiten mit AWS CloudTrail Lake im AWS CloudTrail Benutzerhandbuch.

CloudTrail Für das Speichern und Abfragen von Ereignisdaten in Lake fallen Kosten an. Beim Erstellen eines Ereignisdatenspeichers wählen Sie die Preisoption aus, die für den Ereignisdatenspeicher genutzt werden soll. Die Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauer

für den Ereignisdatenspeicher. Weitere Informationen zur CloudTrail Preisgestaltung finden Sie unter AWS CloudTrail Preise.

Verwaltungsereignisse für Transit Gateway

Verwaltungsereignisse enthalten Informationen über Verwaltungsvorgänge, die an Ressourcen in Ihrem ausgeführt werden AWS-Konto. Sie werden auch als Vorgänge auf Steuerebene bezeichnet. CloudTrail Protokolliert standardmäßig Verwaltungsereignisse.

AWS Transit Gateway protokolliert alle Operationen der Transit Gateway Gateway-Steuerebene als Verwaltungsereignisse. Eine Liste der Operationen der AWS Transit Gateway-Steuerebene, bei denen sich Transit Gateway anmeldet CloudTrail, finden Sie unter AWS Transit Gateway Gateway-Aktionen in der Amazon EC2 EC2-API-Referenz.

Beispiele für Transit Gateway Gateway-Ereignisse

Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält Informationen über den angeforderten API-Vorgang, Datum und Uhrzeit des Vorgangs, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass Ereignisse nicht in einer bestimmten Reihenfolge angezeigt werden.

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Die Protokolldateien enthalten Ereignisse für alle API-Aufrufe für Ihr AWS Konto, nicht nur für Transit-Gateway-API-Aufrufe. Sie können Aufrufe der Transit-Gateway-API finden, indem Sie nach `eventSource`-Elementen mit dem Wert `ec2.amazonaws.com` suchen. Um einen Datensatz für eine bestimmte Aktion anzuzeigen, z. B. `CreateTransitGateway`, suchen Sie nach `eventName`-Elementen mit dem Aktionsnamen.

Im Folgenden finden Sie ein Beispiel für einen CloudTrail Protokolldatensatz für die Transit-Gateway-API für einen Benutzer, der mithilfe der Konsole ein Transit-Gateway erstellt hat. Sie können die Konsole mithilfe des `userAgent`-Elements identifizieren. Sie können den angeforderten API-Aufruf mithilfe der `eventName`-Elemente identifizieren. Informationen zum Benutzer (`Alice`) finden Sie im `userIdentity`-Element.

Example Beispiel: 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"
}
```

Identitäts- und Zugriffsmanagement in AWS Transit Gateway

AWS verwendet Sicherheitsanmeldedaten, um Sie zu identifizieren und Ihnen Zugriff auf Ihre AWS Ressourcen zu gewähren. Sie können Funktionen von AWS Identity and Access Management (IAM) verwenden, um anderen Benutzern, Diensten und Anwendungen die vollständige oder eingeschränkte Nutzung Ihrer AWS Ressourcen zu ermöglichen, ohne Ihre Sicherheitsanmeldeinformationen weiterzugeben.

Standardmäßig sind IAM-Benutzer nicht berechtigt, Ressourcen zu erstellen, anzuzeigen oder zu ändern AWS . Um einem Benutzer zu erlauben, auf Ressourcen wie ein Transit Gateway zuzugreifen und Aufgaben auszuführen, müssen Sie eine IAM-Richtlinie erstellen, die dem Benutzer die Berechtigung zum Verwenden der spezifischen benötigten Ressourcen und API-Funktionen gewährt. Fügen Sie dann die Richtlinie an die Gruppe an, welcher der Benutzer angehört. Wenn Sie einem Benutzer oder einer Benutzergruppe eine Richtlinie zuordnen, wird den Benutzern die Ausführung der angegebenen Aufgaben für die angegebenen Ressourcen gestattet oder verweigert.

Um mit einem Transit-Gateway zu arbeiten, könnte eine der folgenden AWS verwalteten Richtlinien Ihren Anforderungen entsprechen:

- AmazonEC2FullAccess
- AmazonEC2ReadOnlyAccess
- PowerUserAccess
- ReadOnlyAccess

Beispielrichtlinien für die Verwaltung von Transit Gateways

Im Folgenden finden Sie IAM-Beispielrichtlinien für das Arbeiten mit Transit Gateways.

Erstellen eines Transit Gateways mit den erforderlichen Tags

Im folgenden Beispiel können Benutzer Transit Gateways erstellen. Der `aws:RequestTag`-Bedingungsschlüssel erfordert, dass Benutzer das Transit Gateway mit dem `stack=prod`-Tag kennzeichnen. Der `aws:TagKeys`-Bedingungsschlüssel verwendet den Modifikator `ForAllValues`, um anzuzeigen, dass nur der Schlüssel `stack` in der Anforderung zulässig ist (es können keine anderen Tags angegeben werden). Wenn Benutzer dieses spezifische Tag beim Erstellen des Transit Gateways nicht übergeben, oder wenn sie überhaupt keine Tags angeben, schlägt die Anforderung fehl.

Die zweite Anweisung enthält den `ec2:CreateAction`-Bedingungsschlüssel, sodass die Benutzer Tags nur im Kontext von `CreateTransitGateway` erstellen können.

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"
                }
            }
        }
    ]
}
```

Arbeiten mit Transit-Gateway-Routing-Tabellen

Im folgenden Beispiel können Benutzer nur für ein bestimmtes Transit Gateway Routing-Tabellen erstellen und löschen (`tgw-11223344556677889`). Benutzer können Routen auch in einer beliebigen Routing-Tabelle des Transit Gateways erstellen und ersetzen, jedoch nur für Anhänge mit dem 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/*"
```

```
        }
    ]
}
```

Verwenden Sie serviceverknüpfte Rollen für Transit-Gateways in AWS Transit Gateway

Amazon VPC nutzt serviceverknüpfte Rollen für die Berechtigungen, die für den Aufruf anderer AWS -Services in Ihrem Namen benötigt werden. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Service-linkedRollen.

Serviceverknüpfte Rolle für Transit Gateways

Amazon VPC verwendet serviceverknüpfte Rollen für die Berechtigungen, die für den Aufruf anderer AWS -Services in Ihrem Namen benötigt werden, wenn Sie mit einem Transit Gateway arbeiten.

Von der serviceverknüpften Rolle erteilte Berechtigungen

Amazon VPC verwendet die benannte serviceverknüpfte Rolle AWSServiceRoleForVPCTransitGateway, um die folgenden Aktionen in Ihrem Namen aufzurufen, wenn Sie mit einem Transit-Gateway arbeiten:

- `ec2:CreateNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2:ModifyNetworkInterfaceAttribute`
- `ec2:DeleteNetworkInterface`
- `ec2:CreateNetworkInterfacePermission`
- `ec2:AssignIpv6Addresses`
- `ec2:UnAssignIpv6Addresses`

Die AWSServiceRoleForVPCTransitGatewayRolle vertraut darauf, dass die folgenden Dienste die Rolle übernehmen:

- `transitgateway.amazonaws.com`

AWSServiceRoleForVPCTransitGatewayverwendet die verwaltete RichtlinieAWSVPCTransitGatewayServiceRolePolicy.

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter Service-linked Rollenberechtigungen im IAM-Benutzerhandbuch.

Erstellen der serviceverknüpften Rolle

Sie müssen die Rolle AWSServiceRoleForVPCTransitGateway nicht manuell erstellen. Amazon VPC erstellt diese Rolle für Sie, wenn Sie eine VPC in Ihrem Konto an ein Transit Gateway anhängen.

Bearbeiten der serviceverknüpften Rolle

Sie können die Beschreibung der AWSServiceRoleForVPCTransitGatewayVerwendung von IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rollenbeschreibung im IAM-Benutzerhandbuch.

Löschen der serviceverknüpften Rolle

Wenn Sie Transit-Gateways nicht mehr verwenden müssen, empfehlen wir Ihnen, diese zu löschen. AWSServiceRoleForVPCTransitGateway

Sie können diese serviceverknüpfte Rolle erst löschen, nachdem Sie alle Transit-Gateway-VPC-Anlagen in Ihrem AWS Konto gelöscht haben. Auf diese Weise wird sichergestellt, dass Sie nicht versehentlich die Berechtigung für den Zugriff auf Ihre VPC-Anhänge entfernen.

Sie können die IAM-Konsole, die IAM-CLI oder die IAM-API verwenden, um serviceverknüpfte Rollen zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Nach dem Löschen erstellt Amazon VPC die Rolle erneut AWSServiceRoleForVPCTransitGateway, wenn Sie eine VPC in Ihrem Konto an ein Transit-Gateway anhängen.

AWS verwaltete Richtlinien für Transit-Gateways in AWS Transit Gateway

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet AWS wird. AWS Verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele gängige

Anwendungsfälle bereitstellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie allen AWS Kunden zur Verfügung stehen. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

Um mit einem Transit-Gateway zu arbeiten, könnte eine der folgenden AWS verwalteten Richtlinien Ihren Anforderungen entsprechen:

- AmazonEC2FullAccess
- AmazonEC2ReadOnlyAccess
- PowerUserAccess
- ReadOnlyAccess

AWS verwaltete Richtlinie: AWSVPCTransitGatewayServiceRolePolicy

Diese Richtlinie ist der Rolle beigefügt AWSServiceRoleForVPCTransitGateway. Auf diese Weise kann Amazon VPC Ressourcen für Ihre Transit-Gateway-Anhänge erstellen und verwalten.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter AWSVPCTransitGatewayServiceRolePolicy in der Referenz zu von AWS verwalteten Richtlinien.

Transit Gateway-Aktualisierungen AWS verwalteter Richtlinien

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für Transit-Gateways an, seit Amazon VPC im März 2021 damit begonnen hat, diese Änderungen zu verfolgen.

Änderungen	Beschreibung	Date
Amazon VPC hat mit der Verfolgung von Änderungen begonnen	Amazon VPC hat damit begonnen, Änderungen an seinen AWS verwalteten Richtlinien nachzuverfolgen.	1. März 2021

Netzwerk-ACLs für Transit-Gateways in AWS Transit Gateway

Eine Netzwerk-ACL (Network Access Control List; NACL) ist eine optionale Sicherheitsebene.

NACL-Regeln werden je nach Szenario unterschiedlich angewendet:

- the section called “Gleiches Subnetz für EC2-Instances und Transit-Gateway-Zuordnung”
- the section called “Verschiedene Subnetze für EC2-Instances und Transit-Gateway-Zuordnung”

Gleiches Subnetz für EC2-Instances und Transit-Gateway-Zuordnung

Betrachten Sie eine Konfiguration, bei der Sie über EC2-Instances und eine Transit-Gateway-Zuordnung im selben Subnetz verfügen. Die gleiche Netzwerk-ACL wird sowohl für den Datenverkehr von den EC2-Instances zum Transit-Gateway als auch für den Datenverkehr vom Transit-Gateway zu den Instances verwendet.

NACL-Regeln werden auf folgende Weise für den Datenverkehr von Instances zum Transit Gateway angewendet:

- Ausgehende Regeln verwenden die Ziel-IP-Adresse für die Auswertung.
- Eingehende Regeln verwenden die Quell-IP-Adresse für die Auswertung.

NACL-Regeln werden auf folgende Weise für den Datenverkehr vom Transit Gateway zu den Instances angewendet:

- Ausgehende Regeln werden nicht ausgewertet.
- Eingehende Regeln werden nicht ausgewertet.

Verschiedene Subnetze für EC2-Instances und Transit-Gateway-Zuordnung

Betrachten Sie eine Konfiguration, bei der Sie EC2-Instances in einem Subnetz und eine Transit-Gateway-Zuordnung in einem anderen Subnetz haben und jedes Subnetz einer anderen Netzwerk-ACL zugeordnet ist.

Netzwerk-ACL-Regeln werden für das EC2-Instance-Subnetz wie folgt angewendet:

- Ausgehende Regeln verwenden die Ziel-IP-Adresse, um den Datenverkehr von den Instances auf das Transit-Gateway auszuwerten.
- Eingehende Regeln verwenden die Quell-IP-Adresse, um den Datenverkehr vom Transit-Gateway zu den Instances auszuwerten.

NACL-Regeln werden für das Transit-Gateway-Subnetz wie folgt angewendet:

- Ausgehende Regeln verwenden die Ziel-IP-Adresse, um den Datenverkehr vom Transit-Gateway zu den Instances auszuwerten.
- Ausgehende Regeln werden nicht verwendet, um den Datenverkehr von den Instances zum Transit-Gateway auszuwerten.
- Eingehende Regeln verwenden die Quell-IP-Adresse, um den Datenverkehr von den Instances auf das Transit-Gateway auszuwerten.
- Eingehende Regeln werden nicht verwendet, um den Datenverkehr vom Transit-Gateway zu den Instances auszuwerten.

Bewährte Methoden

Verwenden Sie für jeden Transit-Gateway-VPC-Anhang ein separates Subnetz. Verwenden Sie für jedes Subnetz einen kleinen CIDR, z. B. /28, damit Sie mehr Adressen für EC2-Ressourcen haben. Wenn Sie ein separates Subnetz verwenden, können Sie Folgendes konfigurieren:

- Halten Sie die eingehende und ausgehende NACL offen, die den Transit-Gateway-Subnetzen zugeordnet ist.
- Abhängig von Ihrem Datenverkehrsfluss können Sie NACLs auf Ihre Workload-Subnetze anwenden.

Weitere Informationen zu der Funktionsweise von VPC-Anhängen finden Sie unter the section called “Ressourcen-Anhänge”.

AWS Kontingente für Transit Gateway

Ihr AWS-Konto hat die folgenden Kontingente (früher als Limits bezeichnet) in Bezug auf Transit-Gateways. Sofern nicht anders angegeben, gilt jedes Kontingent spezifisch für eine Region.

Die Service-Quotas-Konsole enthält Informationen zu Kontingenten für Ihr Konto. Sie können die Service Quotas-Konsole verwenden, um Standard-Kontingente anzuzeigen und Kontingent-Erhöhungen für einstellbare Kontingente anzufordern. Weitere Informationen finden Sie unter Beantragen einer Kontingenterhöhung im Service Quotas-Benutzerhandbuch.

Wenn in Service Quotas noch kein anpassbares Kontingent verfügbar ist, können Sie einen Supportfall öffnen.

General

Name	Standard	Anpassbar
Transit Gateways pro Konto	5	Ja
CIDR-Blöcke pro Transit Gateway	5	Nein

Die CIDR-Blöcke werden im the section called “Connect-Anfügungen und Connect-Peers”-Feature verwendet.

Routing

Name	Standard	Anpassbar
Transit-Gateway-Routing-Tabellen pro Transit Gateway	20	Ja
Gesamtzahl kombinierter Routen (dynamisch und statisch) über alle Routentabellen für ein einzelnes Transit-Gateway	10.000	Wenden Sie sich für weitere Unterstützung an Ihren Solutions Architect (SA) oder

Name	Standard	Anpassbar
		Technical Account Manager (TAM).
Von einer virtuellen Router-Appliance an einen Connect-Peer angekündigte dynamische Routen	1.000	Wenden Sie sich für weitere Unterstützung an Ihren Solutions Architect (SA) oder Technical Account Manager (TAM).
Von einem Connect-Peer auf einem Transit Gateway an eine virtuelle Router-Appliance angekündigte Routen	5,000	Nein
Statische Routen für ein Präfix eines einzelnen Anhangs	1	Nein

Die angekündigten Routen stammen aus der Routing-Tabelle für den Connect-Anhang.

Transit-Gateway-Anhänge

Ein Transit Gateway darf nicht mehr als einen VPC-Anhang zur selben VPC haben.

Name	Standard	Anpassbar
Anhänge pro Transit Gateway	5,000	Ja
Transit Gateways pro VPC	5	Nein
Peering-Anhänge pro Transit Gateway	50	Ja
Ausstehende Peering-Anhänge pro Transit Gateway	10	Ja
Peering-Verbindungen zwischen zwei Transit-Gateways oder zwischen einem Transit-Gateway	1	Nein

Name	Standard	Anpassbar
und einem Cloud WAN-Core-Netzwerk-Edge (CNE)		
Connect-Peers (GRE-Tunnel) pro Connect-Anfügung	4	Nein
VPN-Konzentratoren pro Transit-Gateway	5	Nein
VPN-Verbindungen pro VPN-Konzentrator	100	Nein

Bandbreite

Es gibt viele Faktoren, die die durch eine Site-to-Site VPN-Verbindung realisierte Bandbreite beeinflussen können. Dazu gehören unter anderem: Paketgröße, Verkehrsmix (TCP/UDP), Shaping- oder Drosselungsrichtlinien in Zwischennetzwerken, Internetwetter und spezifische Anwendungsanforderungen. Für VPC-Anhänge, Direct Connect Gateways oder Peering-Transit-Gateway-Anhänge werden wir versuchen, zusätzliche Bandbreite bereitzustellen, die über den Standardwert hinausgeht.

Name	Standard	Anpassbar
Bandbreite pro VPC-Anhang pro Availability Zone	Bis zu 100 Gbit/s pro Richtung (d. h. 100 Gbit/s Eingang und 100 Gbit/s Ausgang)	Wenden Sie sich für weitere Unterstützung an Ihren Solutions Architect (SA) oder Technical Account Manager (TAM).
Pakete pro Sekunde pro Transit-Gateway-VPC-Anhang pro Availability Zone	Bis zu 7 500 000	Wenden Sie sich für weitere Unterstützung an Ihren Solutions Architect (SA) oder Technical Account Manager (TAM).

Name	Standard	Anpassbar
Bandbreite für Direct Connect Gateway- oder Peer-Transit-Gateway-Verbindungen pro verfügbarer Availability Zone in der Region	Bis zu 100 Gbit/s pro Richtung (d. h. 100 Gbit/s Eingang und 100 Gbit/s Ausgang)	Wenden Sie sich für weitere Unterstützung an Ihren Solutions Architect (SA) oder Technical Account Manager (TAM).
Pakete pro Sekunde pro Transit-Gateway-Anlage (Direct Connect und Peering-Anlagen) pro verfügbarer Availability Zone in der Region	Bis zu 7 500 000	Wenden Sie sich für weitere Unterstützung an Ihren Solutions Architect (SA) oder Technical Account Manager (TAM).
Maximale Bandbreite pro Transit-Gateway-Connect-Peer (GRE-Tunnel) pro Connect-Anhang	Bis zu 5 GBit	Nein
Maximale Anzahl der Pakete pro Sekunde pro Connect-Peer	Bis zu 300.000	Nein

Sie können Equal-Cost Multipath Routing (ECMP) verwenden, um eine höhere VPN-Bandbreite zu erzielen, indem Sie mehrere VPN-Tunnel aggregieren. Zur Verwendung von ECMP muss die VPN-Verbindung für dynamisches Routing konfiguriert sein. ECMP wird nicht für VPN-Verbindungen unterstützt, die statisches Routing nutzen.

Sie können bis zu 4 Connect-Peers pro Connect-Anhang erstellen (bis zu 20 Gbit/s Gesamtbandbreite pro Connect-Anhang), sofern der zugrunde liegende Transportanhang (VPC oder Direct Connect) die erforderliche Bandbreite unterstützt. Sie können Equal-Cost-Multi-Path-Routing (ECMP) verwenden, um eine höhere Bandbreite zu erhalten, indem Sie die horizontale Skalierung über mehrere Connect-Peers derselben Connect-Verbindung oder über mehrere Connect-Verbindungen am selben Transit Gateway nutzen. Für den Transit-Gateway ist kein ECMP zwischen den BGP-Peerings desselben Connect-Peers möglich.

Informationen zu Bandbreiten- und Paketbeschränkungen mit VPN-Tunnel finden Sie unter VPN-Bandbreite und -durchsatz.

Direct Connect Gateways

Name	Standard	Anpassbar
Direct Connect Gateways pro Transit-Gateway	20	Nein
Transit-Gateways pro Gateway Direct Connect	6	Nein

Maximum Transmission Unit (MTU)

- Die MTU einer Netzwerkverbindung ist die Größe (in Byte) des größten zulässigen Datenpakets, das über die Verbindung übergeben werden kann. Je größer die MTU einer Verbindung, desto mehr Daten können in einem einzelnen Paket übergeben werden. Ein Transit-Gateway unterstützt eine MTU von 8500 Byte für den Verkehr zwischen VPCs, Direct Connect, Transit Gateway Connect und Peering-Anhängen (regionsinterne, regionsübergreifende und Cloud WAN-Peering-Anlagen). Datenverkehr über VPN-Verbindungen kann eine MTU von 1 500 Byte haben.
- Eine Nichtübereinstimmung der MTU-Größe zwischen VPC-Peering und dem Transit Gateway kann dazu führen, dass einige Pakete für asymmetrischen Datenverkehr gelöscht werden. Aktualisieren Sie beide Pakete VPCs gleichzeitig, um zu verhindern, dass Jumbo-Pakete aufgrund einer Größenabweichung verloren gehen.
- Das Transit Gateway erzwingt das Klemmen der maximalen Segmentgröße (MSS) für alle Pakete. Weitere Informationen finden Sie unter RFC879.
- Einzelheiten zu Site-to-Site VPN-Kontingenten für MTU finden Sie unter Maximum Transmission Unit (MTU) im Benutzerhandbuch.AWS Site-to-Site VPN
- Transit-Gateways unterstützen Path MTU Discovery (PMTUD) für eingehenden Datenverkehr auf VPC- und Connect-Anhängen. Das Transit-Gateway generiert die `FRAG_NEEDED` Pakete für und für Pakete. ICMPv4 `Packet Too Big (PTB)` ICMPv6 Transit Gateways unterstützt PMTUD für Site-to-site VPN-, Direct Connect- und Peering-Anhänge nicht. Weitere Informationen zu Path MTU Discovery finden Sie unter Path MTU Discovery im Amazon VPC-Benutzerhandbuch

Multicast

> **Note**
>
> Transit-Gateway-Multicast ist möglicherweise nicht für Hochfrequenzhandel oder leistungssensitive Anwendungen geeignet. Wir empfehlen Ihnen dringend, die folgenden Multicast-Limits zu überprüfen. Wenden Sie sich an Ihren Account oder Ihr Solution Architect-Team, um eine detaillierte Überprüfung Ihrer Leistungsanforderungen zu erhalten.

Name	Standard	Anpassbar
Multicast-Domains pro Transit Gateway	20	Wenden Sie sich für weitere Unterstützung an Ihren Solutions Architect (SA) oder Technical Account Manager (TAM).
Multicast-Netzwerkschnittstellen pro Transit Gateway	10.000	Wenden Sie sich für weitere Unterstützung an Ihren Solutions Architect (SA) oder Technical Account Manager (TAM).
Multicast-Domainzuordnungen pro VPC	20	Wenden Sie sich für weitere Unterstützung an Ihren Solutions Architect (SA) oder Technical Account Manager (TAM).
Mitglieder und Quellen statischer und IGMPv2 Multicast-Gruppen pro Transit-Gateway	10.000	Nein

Name	Standard	Anpassbar
Mitglieder von statischen und IGMPv2 Multicast -Gruppen pro Transit-Gateway-Multicast-G ruppe	100	Nein
Maximaler Multicast-Durchsatz pro Flow	1 Gbit/s	Nein
Maximaler aggregierter Multicast-Durchsatz pro Availability Zone	20 Gbit/s	Nein
Maximale Anzahl an Paketen pro Sekunde pro Datenfluss (weniger als 10 Empfänger)	75 000	Nein
Maximale Anzahl an Paketen pro Sekunde pro Datenfluss (mehr als 10 Empfänger)	15 000	Nein
Maximale Gesamtanzahl von Paketen pro Sekunde (weniger als 10 Empfänger)	2.500.000	Nein
Maximale Gesamtanzahl von Paketen pro Sekunde (mehr als 10 Empfänger)	500 000	Nein

AWS Netzwerk-Manager

Name	Standard	Anpassbar
Globale Netzwerke pro AWS-Konto	5	Ja
Geräte pro globales Netzwerk	200	Ja
Links pro globales Netzwerk	200	Ja
Standorte pro globales Netzwerk	200	Ja
Verbindungen pro globales Netzwerk	500	Nein

Zusätzliche Kontingentressourcen

Weitere Informationen finden Sie hier:

- Site-to-Site VPN-Kontingente im AWS Site-to-Site VPN Benutzerhandbuch
- Amazon-VPC-Kontingente im Amazon-VPC-Benutzerhandbuch
- Direct Connect -KontingenteimAWS Direct Connect Benutzerhandbuch

Dokumentverlauf für Transit Gateways

In der folgenden Tabelle werden die Veröffentlichungen für Transit Gateways beschrieben.

Änderung	Beschreibung	Datum
Client-VPN-Anhänge	Erstellen Sie einen Client-VPN-Anhang, um ein Transit-Gateway mit einem Client-VPN-Endpunkt zu verbinden.	20. April 2026
Flexible Kostenverteilung	Konfigurieren Sie flexible Kostenzuweisungsrichtlinien, um zu kontrollieren, wie die Datenverarbeitungs- und Übertragungskosten in Ihrem Unternehmen verteilt werden.	20. November 2025
Verschlüsselungsunterstützung für Transit-Gateways	Verwaltung der Verschlüsselungsunterstützung auf Transit-Gateways, um die Verschlüsselung während der Übertragung für den gesamten Datenverkehr durchzusetzen.	20. November 2025
Anhänge für Netzwerkfunktionen	Erstellen Sie einen Netzwerkfunktionsanhang, mit dem Sie ein Transit-Gateway direkt verbinden können AWS Network Firewall.	16. Juni 2025
Unterstützung für Referenzierung von Sicherheitsgruppen	Sie können jetzt für alle VPCs, die an ein Transit-Gateway angeschlossen sind, auf eine Sicherheitsgruppe verweisen.	25. September 2024

AWS Kontingente für Transit Gateway	Bandbreitenbeschränkungen wurden hinzugefügt.	14. August 2023
AWS Transit Gateway Gateway-Flow-Protokolle	Transit Gateways unterstützen jetzt Flow-Protokolle für Transit-Gateway, wodurch Sie den Netzwerkverkehr zwischen Transit-Gateways überwachen und protokollieren können.	14. Juli 2022
Transit-Gateway-Richtlinientabellen	Verwenden Sie Richtlinientabellen, um für ein automatisches Austauschen von Routing- und Erreichbarkeitsinformationen mit Peered-Transit-Gateway-Typen ein dynamisches Routing für Transit-Gateways einzurichten.	13. Juli 2022
Benutzerhandbuch zu Network Manager	Network Manager wurde als eigenständiger Leitfaden erstellt und ist nicht mehr Teil des Benutzerhandbuchs zu AWS Transit Gateway.	2. Dezember 2021
Peering-Anlagen	Sie können eine Peering-Verbindung mit einem Transit Gateway in der gleichen Region erstellen.	1. Dezember 2021

Transit Gateway Connect	Sie können eine Verbindung zwischen einem Transit Gateway und virtuellen Appliances von Drittanbietern herstellen, die in einer VPC ausgeführt werden.	10. Dezember 2020
Appliance-Modus	Sie können den Appliance-Modus für einen VPC-Anhang aktivieren, um sicherzustellen, dass der bidirektionale Datenverkehr durch dieselbe Availability Zone für den Anhang fließt.	29. Oktober 2020
Präfixlistenreferenzen	Sie können in der Transit-Gateway-Routing-Tabelle auf eine Präfixliste verweisen.	24. August 2020
Ändern des Transit-Gateways	Sie können die Konfigurations-Optionen für den Transit Gateway ändern.	24. August 2020
CloudWatch Metriken für Transit-Gateway-Anhänge	Sie können CloudWatch Messwerte für einzelne Transit-Gateway-Anhänge anzeigen.	6. Juli 2020
Network Manager Route Analyzer	Sie können die Routen in den Transit-Gateway-Routing-Tabellen in Ihrem globalen Netzwerk analysieren.	4. Mai 2020
Peering-Anlagen	Sie können eine Peering-Verbindung mit einem Transit Gateway in einer anderen Region erstellen.	3. Dezember 2019

Multicast-Unterstützung	Transit Gateway unterstützt das Routing von Multicast-Datenverkehr zwischen Subnetzen angefügter VPCs und dient als Multicast-Router für Instances, die Datenverkehr an mehrere empfangende Instances senden.	3. Dezember 2019
AWS Network Manager	Sie können globale Netzwerke visualisieren und überwachen, die auf Transit Gateways basieren.	3. Dezember 2019
AWS Direct Connect Unterstützung	Sie können ein Direct Connect Gateway verwenden, um Ihre Direct Connect Verbindung über eine virtuelle Transitschnittstelle mit den VPCs oder VPNs zu verbinden, die an Ihr Transit-Gateway angeschlossen sind.	27. März 2019
Erstversion	In dieser Version werden Transit Gateways eingeführt.	26. November 2018

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.