AWS Transit Gateway

Amazon VPC

Amazon VPC: AWS Transit Gateway

Table of Contents

Cos'è AWS Transit Gateway per Amazon VPC?

AWS Transit Gateway è un hub di transito di rete utilizzato per interconnettere cloud privati virtuali (VPCs) e reti locali. Man mano che l'infrastruttura cloud si espande a livello globale, il peering interregionale collega i gateway di transito utilizzando l'infrastruttura globale. AWS Tutto il traffico di rete tra AWS i data center viene automaticamente crittografato a livello fisico.

Per ulteriori informazioni, consulta il sito Web AWS Transit Gateway.

Concetti dei gateway di transito

Di seguito sono riportati i concetti chiave per i gateway di transito:

- Collegamenti: puoi decidere di collegare quanto segue:
  - Uno o più VPCs
  - Un'appliance di rete Connect SD-WAN/di terze parti
  - Un AWS Direct Connect gateway
  - Una connessione peering con un altro gateway di transito
  - Una connessione VPN a un gateway di transito
  - Un concentratore VPN verso un gateway di transito
  - Un collegamento a una funzione di rete. Per ulteriori informazioni, consulta the section called “Allegati alle funzioni di rete”.
- Unità massima di trasmissione (MTU) del gateway di transito: l'unità massima di trasmissione (MTU) di una connessione di rete è la dimensione, in byte, del pacchetto più grande che può essere trasmesso con la connessione. Maggiore è la MTU di una connessione, maggiore è la quantità di dati trasferibili in un unico pacchetto. Un gateway di transito supporta un MTU di 8500 byte per il traffico tra VPCs, Transit Direct Connect Gateway Connect e gli allegati di peering (allegati peering intra-regionali, interregionali e Cloud WAN). Il traffico su connessioni VPN può avere una MTU di 1500 byte.
- Controllo della crittografia: un gateway di transito può essere configurato per supportare il controllo della crittografia, che si applica a tutto il traffico collegato al gateway di transito. encryption-in-transit VPCs Quando il controllo della crittografia è abilitato, è possibile collegare il gateway di transito VPCs con Encryption Control applicato. Questa funzionalità garantisce che tutto il traffico che fluisce attraverso il gateway di transito sia crittografato, garantendo una maggiore sicurezza per le comunicazioni di rete.

- Tabella di routing del gateway di transito: un gateway di transito ha una tabella di routing predefinita e facoltativamente può avere tabelle di routing aggiuntive. Una tabella di routing include route dinamiche e statiche che determinano il segmento di rete successivo in base all'indirizzo IP di destinazione del pacchetto. L'obiettivo di queste route potrebbe essere qualsiasi collegamento di un gateway di transito. Per impostazione predefinita, gli allegati del gateway di transito sono associati alla tabella di route del gateway di transito predefinita.
- Associazioni: ogni collegamento è associato a una sola tabella di routing. Le tabelle di routing possono essere associate a nessuno o a molti collegamenti.
- Propagazione delle route: un VPC, una connessione VPN o un gateway Direct Connect possono propagare le route in modo dinamico verso una tabella di instradamento di un gateway di transito. Per impostazione predefinita, con un allegato Connect le route vengono propagate a una tabella di routing del gateway di transito. Con un VPC, per inviare traffico verso il gateway di transito è necessario creare route statici. Con una connessione VPN, i route sono propagati dal gateway di transito verso il router locale tramite il Border Gateway Protocol (BGP). Con un gateway Direct Connect, i prefissi consentiti sono generati verso il router on-premise tramite il protocollo BGP. Con un allegato di peering, è necessario creare un route statico nella tabella di routing del gateway di transito per puntare all'allegato di peering.

Come iniziare a usare i gateway di transito

Utilizza le risorse seguenti per creare e utilizzare un gateway di transito.

- Come funzionano i gateway di transito
- Inizia a usare i gateway di transito
- Best Practice di progettazione

Utilizzo dei gateway di transito

Puoi creare, accedere e gestire i gateway di transito utilizzando una qualsiasi delle seguenti interfacce:

- Console di gestione AWS — Fornisce un'interfaccia web da utilizzare per l'accesso ai gateway di transito.

- AWS Command Line Interface (AWS CLI): fornisce comandi per un'ampia gamma di AWS servizi, tra cui Amazon VPC, ed è supportato su Windows, macOS e Linux. Per ulteriori informazioni, consulta AWS Command Line Interface.
- AWS SDKs— Fornisce operazioni API specifiche per la lingua e si occupa di molti dettagli di connessione, come il calcolo delle firme, la gestione dei tentativi di richiesta e la gestione degli errori. Per ulteriori informazioni, consulta AWS SDKs.
- API di query: forniscono operazioni API di basso livello accessibili tramite richieste HTTPS. L'API di interrogazione è il modo più diretto per accedere ad Amazon VPC, ma richiede che la propria applicazione gestisca dettagli di basso livello, come la generazione di un hash per la firma della richiesta e la gestione degli errori. Per ulteriori informazioni, consulta Amazon EC2 API Reference.

Prezzi

Ti verrà addebitata ogni ora per ogni allegato in un gateway di transito e ti verrà addebitata la quantità di traffico elaborata sul gateway di transito. Per impostazione predefinita, i costi di elaborazione dei dati vengono assegnati all'account proprietario dell'allegato di origine. È possibile utilizzare l'allocazione flessibile dei costi per personalizzare il modo in cui questi addebiti vengono allocati in base alle esigenze organizzative. Per ulteriori informazioni, consulta i prezzi di AWS Transit Gateway eAllocazione flessibile dei costi.

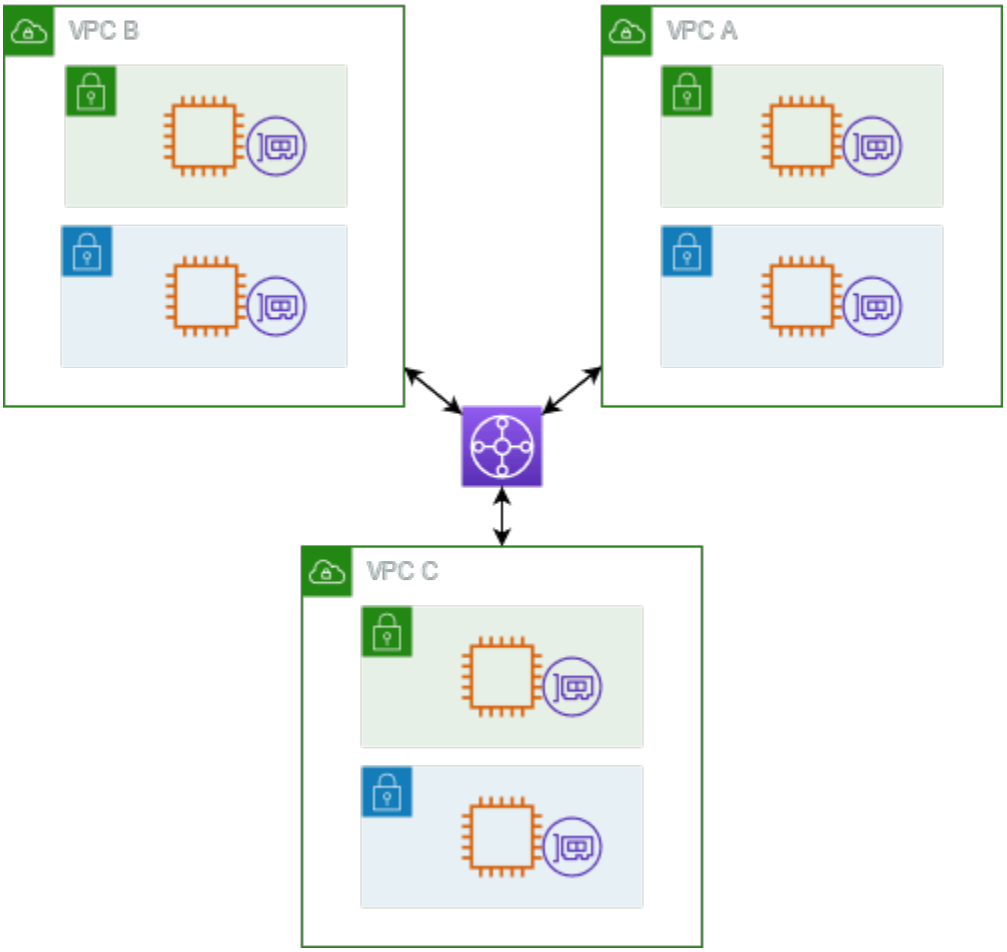
Come funziona AWS Transit Gateway

In AWS Transit Gateway, un gateway di transito funge da router virtuale regionale per il traffico che scorre tra i cloud privati virtuali (VPCs) e le reti locali. Un gateway di transito si ridimensiona in modo elastico sulla base del volume di traffico di rete. Il routing attraverso un gateway di transito opera al livello 3, dove i pacchetti vengono inviati a uno specifico allegato next-hop, in base agli indirizzi IP di destinazione.

Argomenti

Esempio di diagramma di architettura

Il seguente diagramma mostra un gateway di transito con tre collegamenti VPC. La tabella delle rotte per ognuna di queste VPCs include la rotta locale e le rotte che inviano il traffico destinato agli altri due VPCs al gateway di transito.



Di seguito è riportato un esempio di una tabella di instradamento del gateway di transito di default per i collegamenti mostrati nel diagramma precedente. I blocchi CIDR per ogni VPC si propagano alla tabella di instradamento. Pertanto, ogni collegamento può instradare i pacchetti agli altri due collegamenti.

Destinazione	Target	Tipo di route
VPC A CIDR	*Attachment for VPC A*	propagata
VPC B CIDR	*Attachment for VPC B*	propagata
VPC C CIDR	*Attachment for VPC C*	propagata

Collegamenti alle risorse

Un collegamento a un gateway di transito costituisce sia una sorgente che una destinazione di pacchetti. È possibile allegare le seguenti risorse al gateway di transito:

- Uno o più VPCs. AWS Transit Gateway implementa un'interfaccia di rete elastica all'interno delle sottoreti VPC, che viene quindi utilizzata dal gateway di transito per instradare il traffico da e verso le sottoreti scelte. È necessario disporre di almeno una sottorete per ciascuna zona di disponibilità, che consente al traffico di raggiungere le risorse in tutte le sottorete di tale zona. Durante la creazione di allegati, le risorse all'interno di una particolare zona di disponibilità possono raggiungere un gateway di transito solo se una sottorete è abilitata all'interno della stessa zona. Se una tabella di routing di sottorete include un routing al gateway di transito, il traffico viene inoltrato al gateway di transito solo quando il gateway di transito dispone di un allegato in una sottorete nella stessa zona di disponibilità.
- Una o più connessioni VPN
- Uno o più concentratori VPN
- Uno o più gateway AWS Direct Connect
- Uno o più allegati Transit Gateway Connect
- Una o più connessioni di peering del gateway di transito

Instradamento Equal Cost Multipath

AWS Transit Gateway supporta il routing Equal Cost Multipath (ECMP) per la maggior parte degli allegati. Per un collegamento VPN, è possibile abilitare o disabilitare il supporto ECMP utilizzando la console durante la creazione o la modifica di un gateway di transito. Per tutti gli altri tipi di collegamenti, si applicano le seguenti restrizioni ECMP:

- VPC: VPC non supporta ECMP poiché i blocchi CIDR non possono sovrapporsi. Ad esempio, non è possibile collegare un VPC con un CIDR 10.1.0.0/16 con un secondo VPC che utilizza lo stesso CIDR a un gateway di transito e quindi configurare l'instradamento per bilanciare il carico del traffico tra di essi.
- VPN: quando l'opzione di supporto VPN ECMP è disabilitata, un gateway di transito utilizza parametri interni per determinare il percorso preferito in caso di prefissi uguali su più percorsi. Per ulteriori informazioni sull'attivazione o la disattivazione di ECMP per un collegamento VPN, consulta the section called “Gateway di transito”.

- AWS Transit Gateway Connect: gli allegati AWS Transit Gateway Connect supportano automaticamente ECMP.
- AWS Direct Connect Gateway: gli allegati del AWS Direct Connect gateway supportano automaticamente l'ECMP su più allegati Direct Connect Gateway quando il prefisso di rete, la lunghezza del prefisso e AS_PATH sono esattamente gli stessi.
- Peering del gateway di transito: il peering del gateway di transito non supporta ECMP poiché non supporta l'instradamento dinamico né è possibile configurare lo stesso percorso statico su due destinazioni diverse.
- VPN Concentrator - VPN Concentrator non supporta ECMP.

> **Note**
>
> - BGP Multipath AS-Path Relax non è supportato, quindi non è possibile utilizzare ECMP su diversi Autonomous System Numbers (). ASNs
> - ECMP non è supportato tra diversi tipi di collegamenti. Ad esempio, non è possibile abilitare ECMP tra una VPN e un collegamento VPC. Invece, vengono valutate le route del gateway di transito e il traffico viene indirizzato in base alla route valutata. Per ulteriori informazioni, consulta the section called “Ordine di valutazione route”.
> - Un singolo gateway Direct Connect supporta ECMP su più interfacce virtuali di transito. Pertanto, si consiglia di configurare e utilizzare un solo gateway Direct Connect e di non configurare e utilizzare più gateway per sfruttare ECMP. Per ulteriori informazioni sui gateway Direct Connect e sulle interfacce virtuali pubbliche, vedi Come si configura una connessione Active/Active o Active/Passive Direct Connect AWS da un'interfaccia virtuale pubblica? .

Zone di disponibilità

Quando si collega un VPC a un gateway di transito, è necessario abilitare una o più zone di disponibilità che il gateway di transito utilizza per indirizzare il traffico verso le risorse nelle sottoreti del VPC. Per abilitare ogni zona di disponibilità, è necessario specificare una sola sottorete. Il gateway di transito crea un'interfaccia di rete in tale sottorete usando un indirizzo IP della sottorete stessa. Dopo aver abilitato una zona di disponibilità specificando una sottorete, il traffico può essere indirizzato a tutte le sottoreti di quella zona di disponibilità, non solo a quella specificata. Tuttavia,

solo le risorse che risiedono nelle zone di disponibilità in cui è presente un collegamento del gateway di transito alla VPN possono raggiungere il gateway di transito.

Se il traffico proviene da una zona di disponibilità in cui l'allegato di destinazione non è presente, AWS Transit Gateway indirizzerà internamente tale traffico verso una zona di disponibilità casuale in cui è presente l'allegato. Non è previsto alcun costo aggiuntivo per il gateway di transito per questo tipo di traffico tra Zone di disponibilità.

Per assicurare la disponibilità, raccomandiamo di abilitare molteplici zone di disponibilità.

Utilizzo del supporto della modalità accessorio

Se si prevede di configurare un'appliance di rete con stato nel VPC, è possibile abilitare il supporto della modalità appliance per l'allegato VPC in cui si trova l'appliance. Ciò garantisce che il gateway di transito utilizzi la stessa zona di disponibilità per l'allegato VPC per tutta la durata di un flusso di traffico tra origine e destinazione. Consente inoltre al gateway di transito di inviare traffico a qualsiasi zona di disponibilità nel VPC, a condizione che vi sia un'associazione di subnet in tale zona. Per ulteriori informazioni, consulta Esempio: appliance in un VPC di servizi condivisi.

Routing

Il gateway di transito indirizza IPv4 e invia IPv6 pacchetti tra gli allegati utilizzando le tabelle di routing del gateway di transito. È possibile configurare queste tabelle di routing per propagare le route dalle tabelle di routing per le connessioni VPN collegate VPCs e i gateway Direct Connect. È inoltre possibile aggiungere route statiche alle tabelle di route del gateway di transito. Quando un pacchetto proviene da un collegamento, viene indirizzato a un altro collegamento utilizzando la route che contiene una regola per l'indirizzo IP di destinazione.

Per gli allegati di peering del gateway di transito, sono supportati solo route statici.

Argomenti di routing

- Tabelle di instradamento
- Associazione di tabelle di routing
- Propagazione delle tabelle di routing
- Route per gli allegati peering
- Ordine di valutazione route

Tabelle di instradamento

Il gateway di transito viene fornito automaticamente con una tabella dei percorsi predefinita. Per impostazione predefinita, questa tabella di routing è la tabella di routing predefinita per i collegamenti nonché la tabella di routing predefinita per la propagazione. Se si disabilita sia la propagazione delle rotte che l'associazione delle tabelle di rotte, AWS non crea una tabella di routing predefinita per il gateway di transito. Tuttavia, se è abilitata la propagazione delle rotte o l'associazione delle tabelle di rotte AWS , crea una tabella di routing predefinita.

È possibile creare tabelle di route aggiuntive per il gateway di transito. Ciò permette di isolare gruppi di collegamenti. Ogni allegato può essere associato a una tabella di instradamento. Un allegato può propagare i propri instradamenti a una o più tabelle di routing

È possibile creare una route blackhole nella tabella di routing del gateway di transito che intercetti il traffico corrispondente alla route.

Quando colleghi un VPC a un gateway di transito, devi aggiungere un instradamento alla tabella di routing della sottorete affinché il traffico sia instradato attraverso il gateway di transito. Per maggiori informazioni, consulta Routing per un gateway di transito nella Guida per l'utente di Amazon VPC.

Associazione di tabelle di routing

È possibile associare un allegato del gateway di transito a una singola tabella di route. Ogni tabella di routing può essere associata da zero a molti collegamenti e può inoltrare i pacchetti agli altri allegati.

Propagazione delle tabelle di routing

Ogni collegamento dispone di route che possono essere installate in una o più tabelle di routing del gateway di transito. Quando un collegamento è propagato a una tabella di routing del gateway di transito, tali route sono aggiunte alla tabella di routing. Non è possibile filtrare i percorsi pubblicizzati.

Per un allegato VPC, i blocchi CIDR del VPC vengono propagati alla tabella di instradamento del gateway di transito.

Quando il routing dinamico viene utilizzato con un allegato VPN, un allegato VPN Concentrator o un allegato gateway Direct Connect, è possibile propagare i percorsi appresi dal router locale tramite BGP a qualsiasi tabella di routing del gateway di transito.

Quando il routing dinamico viene utilizzato con un allegato VPN o un allegato VPN Concentrator, i percorsi nella tabella di routing associata all'allegato VPN o all'allegato VPN Concentrator vengono pubblicizzati al gateway del cliente tramite BGP.

Per un allegato Connect, i routing nella tabella di instradamento associati all'allegato Connect vengono pubblicizzati alle appliance virtuali di terze parti, come le appliance SD-WAN, in esecuzione in un VPC tramite BGP.

Per un collegamento al gateway Direct Connect, le interazioni con prefissi consentiti controllano da quali percorsi vengono pubblicizzati alla rete del cliente. AWS

Quando una route statica e una route propagata hanno la stessa destinazione, la route statica ha la priorità più alta e la route propagata non viene quindi inclusa nella tabella di instradamento. Se si rimuove la route statica, la route propagata sovrapposta viene inclusa nella tabella di instradamento.

Route per gli allegati peering

È possibile eseguire il peering di due gateway di transito e instradare il traffico tra di loro. A tale scopo, creare un allegato di peering nel gateway di transito e specificare il gateway di transito peer con cui creare la connessione di peering. È quindi necessario creare una route statica nella tabella di route del gateway di transito per instradare il traffico all'allegato peering del gateway di transito. Il traffico instradato al gateway di transito peer può quindi essere instradato agli allegati VPC e VPN per il gateway di transito peer.

Per ulteriori informazioni, consulta Esempio: gateway di transito in peering.

Ordine di valutazione route

I route dei gateway di transito sono valutati nell'ordine seguente:

- Il percorso più specifico per l'indirizzo di destinazione.
- Per i percorsi con lo stesso CIDR, ma con tipi di allegati diversi, la priorità del percorso è la seguente:
  - Percorsi statici (ad esempio, percorsi statici Site-to-Site VPN)
  - Route referenziate dell'elenco di prefissi
  - Percorsi propagati tramite VPC
  - Percorsi propagati dal gateway Direct Connect
  - Percorsi propagati da Transit Gateway Connect
  - Site-to-Site VPN su percorsi privati propagati da Direct Connect
  - Site-to-Site Percorsi propagati tramite VPN
  - Site-to-Site Percorsi propagati da VPN Concentrator

- Percorsi propagati tramite peering Transit Gateway (Cloud WAN)

Alcuni allegati supportano la pubblicità dei percorsi tramite BGP. Per i percorsi con lo stesso CIDR e lo stesso tipo di allegato, la priorità del percorso è controllata dagli attributi BGP:

- Lunghezza del percorso AS più breve
- Valore MED inferiore
- I percorsi eBGP rispetto a iBGP sono preferiti, se l'allegato lo supporta

> **Important**
>
> - AWS non può garantire un ordine di prioritizzazione delle rotte coerente per le rotte BGP con gli stessi CIDR, tipo di allegato e attributi BGP elencati sopra.
> - Per le rotte pubblicizzate verso un gateway di transito senza MED, AWS Transit Gateway assegnerà i seguenti valori predefiniti:
>   - 0 per le rotte in entrata pubblicizzate sugli allegati Direct Connect.
>   - 100 per le rotte in entrata pubblicizzate sugli allegati VPN e Connect.

AWS Transit Gateway mostra solo una rotta preferita. Un percorso di backup verrà visualizzato nella tabella delle rotte del gateway di transito solo se il percorso precedentemente attivo non è più pubblicizzato, ad esempio se pubblicizzi gli stessi percorsi sul gateway Direct Connect e tramite Site-to-Site VPN. AWS Transit Gateway mostrerà solo le rotte ricevute dalla rotta gateway Direct Connect, che è la rotta preferita. La Site-to-Site VPN, che è il percorso di backup, verrà visualizzata solo quando il gateway Direct Connect non viene più pubblicizzato.

Differenze nelle tabelle di routing tra VPC e gateway di transito

La valutazione della tabella delle rotte varia a seconda che si utilizzi una tabella di routing VPC o una tabella di routing del gateway di transito.

L'esempio seguente mostra una tabella di routing VPC. Il route VPC locale ha la priorità più alta, seguito dai route più specifici. Quando un route statico e propagato hanno la stessa destinazione, la route statica ha la priorità più alta.

Destinazione	Target	Priorità
10.0.0.0/16	locale	1
192.168.0.0/16	pcx-12345	2
172.31.0.0/16	vgw-12345 (statico) o tgw-12345 (statico)	2
172.31.0.0/16	vgw-12345 (propagato)	3
0.0.0.0/0	igw-12345	4

L'esempio seguente mostra una tabella delle rotte del gateway di transito. Se si preferisce l'allegato gateway Direct Connect all'allegato VPN, utilizzare una connessione VPN BGP e propagare le route nella tabella di instradamento del gateway di transito.

Destinazione	Allegato (target)	Tipo di risorsa	Tipo di route	Priorità
10.0.0.0/16	tgw-attach-123 | vpc-1234	VPC	Statico o propagato	1
192.168.0.0/16	tgw-attach-789 | vpn-5678	VPN	Statico	2
172.31.0.0/16	tgw-attach-456 | dxgw_id	Direct Connect gateway	Propagato	3
172.31.0.0/16	tgw-attach-789 | -123 tgw-connect-peer	Connect (Connetti)	Propagato	4
172.31.0.0/16	tgw-attach-789 | vpn-5678	VPN	Propagato	5

Allegati alle funzioni di rete

Un collegamento a una funzione di rete è una risorsa che collega una funzione di sicurezza della rete, ad esempio un AWS Network Firewall allegato, direttamente al gateway di transito. Elimina la necessità di creare e gestire manualmente le ispezioni VPCs.

Con un collegamento alla funzione di rete:

- AWS crea e gestisce automaticamente l'infrastruttura sottostante
- Il traffico può essere ispezionato mentre attraversa il gateway di transito
- Le politiche di sicurezza vengono applicate in modo coerente in tutta la rete

- È possibile indirizzare il traffico attraverso il firewall utilizzando semplici regole di routing
- L'allegato funziona su più zone di disponibilità per un'elevata disponibilità

Questa integrazione semplifica la sicurezza della rete consentendo di collegare i firewall direttamente al gateway di transito anziché creare configurazioni di routing complesse e gestire endpoint separati tramite sistemi separati. VPCs

AWS Network Firewall integrazione

AWS Network Firewall l'integrazione consente di connettere un firewall sotto forma di un gruppo di Gateway Load Balancer Endpoint, uno per zona di disponibilità, in un VPC buffer gestito dal servizio. Viene creato un allegato Network Firewall con la modalità appliance abilitata automaticamente. Ciò elimina la necessità di gestire in modo esplicito l'ispezione. VPCs

Con l'integrazione del Network Firewall, non è più necessario creare e gestire l'ispezione VPCs per le implementazioni del Network Firewall. Invece di selezionare un VPC e delle sottoreti durante la creazione del firewall, si seleziona direttamente il Transit Gateway e si occupa AWS automaticamente del provisioning e della gestione di tutte le risorse necessarie dietro le quinte. Vedrai un nuovo allegato alla funzione di rete Transit Gateway anziché un singolo endpoint firewall.

Per gli scenari con più account, il Transit Gateway può essere condiviso dalla RAM del proprietario del Transit Gateway all'account proprietario del Network Firewall, permettendo a entrambi gli account di gestire l'allegato del firewall. Una volta che il firewall e l'allegato sono pronti, è sufficiente modificare le tabelle di routing del Transit Gateway per inviare il traffico all'allegato per l'ispezione.

> **Note**
>
> - Transit Gateway supporta solo il routing statico sugli allegati Network Firewall.
> - I firewall di terze parti non sono supportati.

Per ulteriori informazioni su firewall e allegati, consulta gli allegati delle funzioni di rete del gateway Transit.

Esempi di scenari di gateway di transito

Di seguito sono riportati casi di utilizzo comuni per i gateway di transito. I gateway di transito non sono limitati a questi casi di utilizzo.

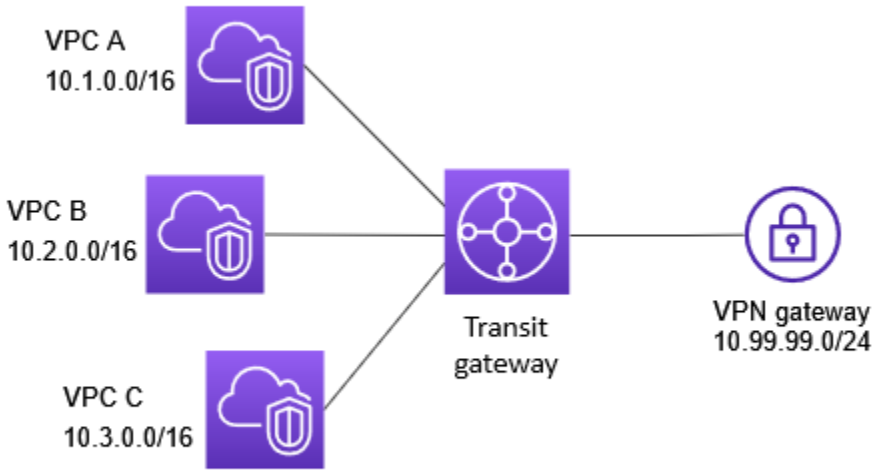
Esempio: router centralizzato

Puoi configurare il tuo gateway di transito come un router centralizzato che collega tutte le tue VPCs connessioni e Site-to-Site VPN. AWS Direct Connect In questo scenario, tutti i allegati sono associati alla tabella di routing predefinita del gateway di transito e si propagano alla tabella di routing del gateway di transito. Pertanto, tutti i collegamenti possono instradare i pacchetti tra di essi, con il gateway di transito che assume il ruolo di un semplice router IP di livello 3.

Indice

Panoramica

Il seguente diagramma illustra i componenti principali della configurazione di questo scenario. In questo scenario, ci sono tre allegati VPC e un allegato Site-to-Site VPN al gateway di transito. I pacchetti delle sottoreti in VPC A, VPC B e VPC C destinati a una sottorete in un altro VPC o per la connessione VPN vengono instradati per la prima volta attraverso il gateway di transito.



Resources

Crea le seguenti risorse per questo scenario:

- Tre. VPCs Per ulteriori informazioni, consulta Crea un VPC nella Guida per l'utente di Amazon VPC.
- Un gateway di transito. Per ulteriori informazioni, consulta the section called “Creazione di un gateway di transito”.
- Tre allegati VPC sul gateway di transito. Per ulteriori informazioni, consulta the section called “Creare un allegato VPC”.
- Un allegato Site-to-Site VPN sul gateway di transito. I blocchi CIDR per ogni VPC si propagano alla tabella di instradamento del gateway di transito. Quando la connessione VPN è attiva, viene stabilita la sessione BGP e il CIDR Site-to-Site VPN si propaga alla tabella di routing del gateway di transito e il VPC CIDRs viene aggiunto alla tabella BGP del gateway del cliente. Per ulteriori informazioni, consulta the section called “Creare un collegamento del gateway di transito a una VPN”.

  Rivedi i requisiti per il dispositivo gateway cliente nel Manuale dell'utente AWS Site-to-Site VPN .

Routing

Ogni VPC ha una tabella di routing ed esiste una tabella di routing per gateway di transito.

Tabelle di routing VPC

Ogni VPC ha una tabella di instradamento con 2 voci. La prima voce è la voce predefinita per il IPv4 routing locale nel VPC; questa voce consente alle istanze di questo VPC di comunicare tra loro. La seconda voce indirizza tutto il resto del traffico di IPv4 sottorete verso il gateway di transito. La tabella seguente mostra i route VPC A.

Destinazione	Target
10.1.0.0/16	locale
0.0.0.0/0	tgw-id

Tabella di routing del gateway di transito

Di seguito è riportato un esempio di una tabella di instradamento predefinita per i collegamenti mostrati nel diagramma precedente, con la propagazione delle route abilitate.

Destinazione	Target	Tipo di route
10.1.0.0/16	*Attachment for VPC A*	propagata
10.2.0.0/16	*Attachment for VPC B*	propagata
10.3.0.0/16	*Attachment for VPC C*	propagata
10.99.99.0/24	*Attachment for VPN connection*	propagata

Tabella BGP gateway del cliente

La tabella BGP del gateway del cliente contiene il seguente VPC. CIDRs

- 10.1.0.0/16

- 10.2.0.0/16
- 10.3.0.0/16

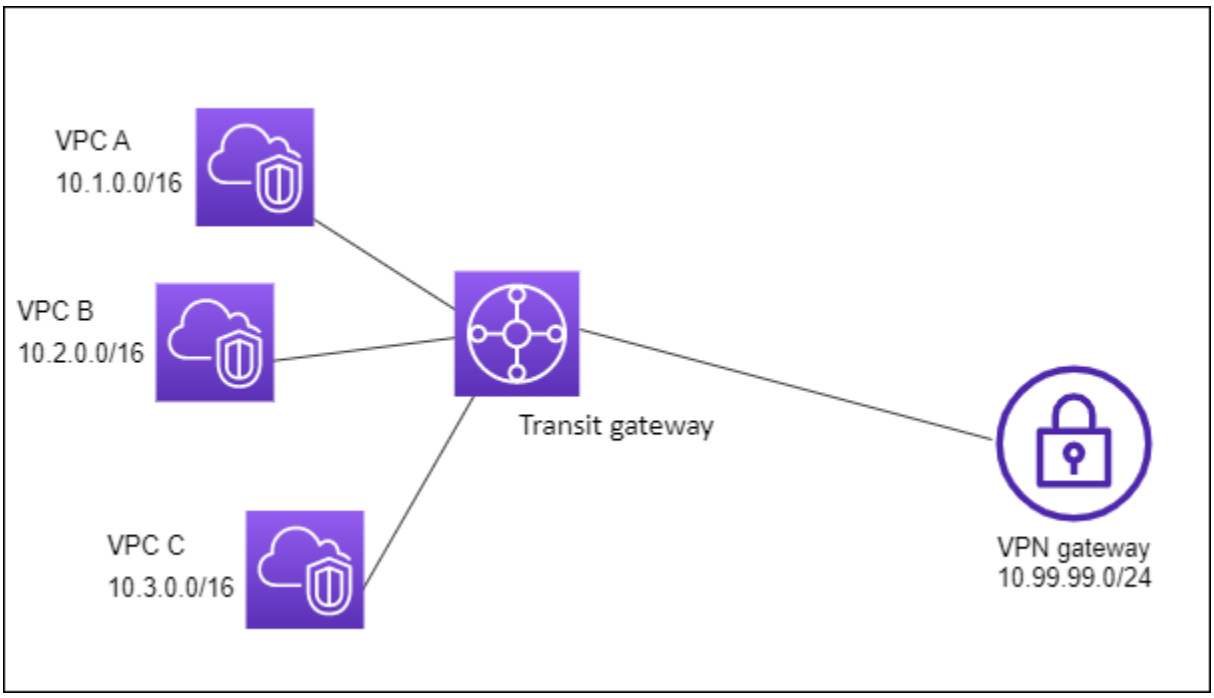
Esempio: isolato VPCs

È possibile configurare il gateway di transito come più router isolati. Il caso d'uso è simile a quello dell'utilizzo di gateway di transito multipli, ma offre maggiore flessibilità nei casi in cui gli instradamenti e gli allegati siano soggetti a modifica. In questo scenario, ogni router isolato dispone di una singola tabella di routing. Tutti i collegamenti associati a un router isolato propagano e associano la sua tabella di instradamento. I collegamenti associati a un router isolato possono instradare i pacchetti tra loro, ma non possono instradare o ricevere pacchetti dai collegamenti di un altro router isolato.

Indice

Panoramica

Il seguente diagramma illustra i componenti principali della configurazione di questo scenario. I pacchetti da VPC A, VPC B e VPC C instradano al gateway di transito. I pacchetti provenienti dalle sottoreti in VPC A, VPC B e VPC C che hanno Internet come destinazione vengono prima instradati attraverso il gateway di transito e poi vengono indirizzati verso la connessione VPN (se la destinazione si trova Site-to-Site all'interno di quella rete). I pacchetti da un VPC che hanno una destinazione di una sottorete in un altro VPC, ad esempio da 10.1.0.0 a 10.2.0.0, vengono instradati tramite il gateway di transito, dove vengono bloccati perché per questi non è specificato un route nella tabella di routing nel gateway di transito.



Resources

Crea le seguenti risorse per questo scenario:

- Tre VPCs. Per ulteriori informazioni, consulta Crea un VPC nella Guida per l'utente di Amazon VPC.
- Un gateway di transito. Per ulteriori informazioni, consulta the section called “Creazione di un gateway di transito”.
- Tre allegati sul gateway di transito per tre VPCs. Per ulteriori informazioni, consulta the section called “Creare un allegato VPC”.
- Un allegato Site-to-Site VPN sul gateway di transito. Per ulteriori informazioni, consulta the section called “Creare un collegamento del gateway di transito a una VPN”. Rivedi i requisiti per il dispositivo gateway cliente nel Manuale dell'utente AWS Site-to-Site VPN .

Quando la connessione VPN è attiva, viene stabilita la sessione BGP e il CIDR VPN si propaga alla tabella di routing del gateway di transito e il VPC CIDRs viene aggiunto alla tabella BGP del gateway del cliente.

Routing

Ogni VPC ha una tabella di routing e il gateway di transito ha due tabelle di routing, una per la connessione VPN VPCs e una per la connessione VPN.

Tabelle di routing VPC A, VPC B e VPC C

Ogni VPC ha una tabella di instradamento con 2 voci. La prima voce è la voce predefinita per il IPv4 routing locale nel VPC. Questa voce consente alle istanze di questo VPC di comunicare tra loro. La seconda voce indirizza tutto il resto del traffico di IPv4 sottorete verso il gateway di transito. La tabella seguente mostra i route VPC A.

Destinazione	Target
10.1.0.0/16	locale
0.0.0.0/0	tgw-id

Tabelle di routing del gateway di transito

Questo scenario utilizza una tabella di routing per la VPCs e una tabella di route per la connessione VPN.

Gli allegati VPC sono associati alla seguente tabella di instradamento, che ha una route propagata per l'allegato VPN.

Destinazione	Target	Tipo di route
10.99.99.0/24	*Attachment for VPN connection*	propagata

L'allegato VPN è associato alla seguente tabella di instradamento, con route propagate per ciascuno degli allegati VPC.

Destinazione	Target	Tipo di route
10.1.0.0/16	*Attachment for VPC A*	propagata
10.2.0.0/16	*Attachment for VPC B*	propagata

Destinazione	Target	Tipo di route
10.3.0.0/16	*Attachment for VPC C*	propagata

Per ulteriori informazioni sulla propagazione delle route in una tabella di routing del gateway di transito, consulta Abilita la propagazione del percorso su una tabella di routing del gateway di transito in AWS Transit Gateway.

Tabella BGP gateway del cliente

La tabella BGP del gateway del cliente contiene il seguente VPC. CIDRs

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

Esempio: isolato VPCs con servizi condivisi

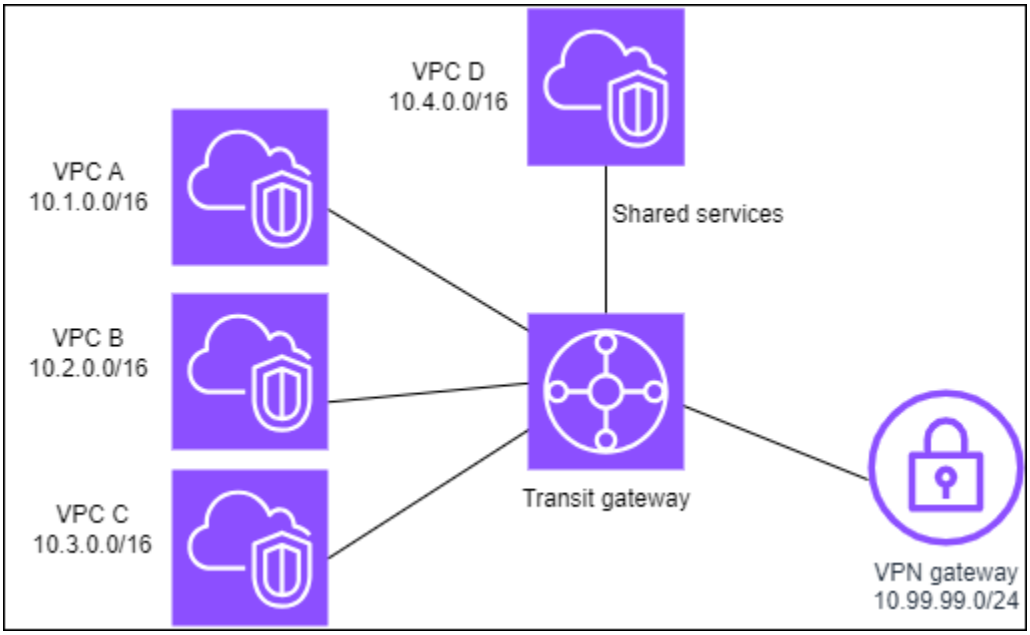
È possibile configurare il gateway di transito come molteplici router isolati che utilizzano un servizio condiviso. Il caso d'uso è simile a quello dell'utilizzo di gateway di transito multipli, ma offre maggiore flessibilità nei casi in cui gli instradamenti e gli allegati siano soggetti a modifica. In questo scenario, ogni router isolato dispone di una singola tabella di routing. Tutti i collegamenti associati a un router isolato propagano e associano la sua tabella di instradamento. I collegamenti associati a un router isolato possono instradare i pacchetti tra loro, ma non possono instradare o ricevere pacchetti dai collegamenti di un altro router isolato. Gli allegati possono instradare pacchetti oppure per ricevere i pacchetti dai servizi condivisi. È possibile utilizzare questo scenario in presenza di gruppi che devono essere isolati, ma che utilizzano un servizio condiviso, ad esempio un sistema di produzione.

Indice

Panoramica

Il seguente diagramma illustra i componenti principali della configurazione di questo scenario. I pacchetti provenienti dalle sottoreti in VPC A, VPC B e VPC C che hanno Internet come destinazione,

vengono prima instradati attraverso il gateway di transito e poi verso il gateway del cliente per la VPN. Site-to-Site I pacchetti provenienti da sottoreti nel VPC A, VPC B o VPC C che hanno una destinazione di una sottorete in VPC A, VPC B o VPC C si instradano attraverso il gateway di transito, dove sono bloccati perché non vi è alcuna route per loro nella tabella di instradamento del gateway di transito. I pacchetti da VPC A, VPC B e VPC C che hanno VPC D come destinazione vengono instradati tramite il gateway di transito al VPC D.



Resources

Crea le seguenti risorse per questo scenario:

- Quattro. VPCs Per ulteriori informazioni, consulta Crea un VPC nella Guida per l'utente di Amazon VPC.
- Un gateway di transito. Per ulteriori informazioni, consulta Gateway di transito.
- Quattro allegati sul gateway di transito, uno per VPC. Per ulteriori informazioni, consulta the section called “Creare un allegato VPC”.
- Un allegato Site-to-Site VPN sul gateway di transito. Per ulteriori informazioni, consulta the section called “Creare un collegamento del gateway di transito a una VPN”.

  Rivedi i requisiti per il dispositivo gateway cliente nel Manuale dell'utente AWS Site-to-Site VPN .

Quando la connessione VPN è attiva, viene stabilita la sessione BGP e il CIDR VPN si propaga alla tabella di routing del gateway di transito e il VPC CIDRs viene aggiunto alla tabella BGP del gateway del cliente.

- Ogni VPC isolato è associato alla tabella di instradamento isolata ed è propagato alla tabella di instradamento condivisa.
- Ogni VPC dei servizi condivisi è associato alla tabella di instradamento isolata ed è propagato a entrambe le tabelle di instradamento.

Routing

Ogni VPC ha una tabella di routing e il gateway di transito ha due tabelle di routing, una per la connessione VPN e l'altra per la connessione VPN VPCs e i servizi condivisi VPC.

Tabelle di routing VPC A, VPC B, VPC C e VPC D

Ogni VPC ha una tabella di instradamento con due voci. La prima voce è quella predefinita per il routing locale nel VPC; questa voce abilita la comunicazione tra le istanze in questo VPC. La seconda voce indirizza tutto il resto del traffico di IPv4 sottorete verso il gateway di transito.

Destinazione	Target
10.1.0.0/16	locale
0.0.0.0/0	*transit gateway ID*

Tabelle di routing del gateway di transito

Questo scenario utilizza una tabella di routing per la VPCs e una tabella di route per la connessione VPN.

I collegamenti VPC A, B e C sono associati alla seguente tabella di instradamento, che ha una route propagata per il collegamento VPN e una route propagata per il collegamento VPC D.

Destinazione	Target	Tipo di route
10.99.99.0/24	*Attachment for VPN connection*	propagata
10.4.0.0/16	*Attachment for VPC D*	propagata

Il collegamento VPN e i collegamenti VPC dei servizi condivisi (VPC D) sono associati alla seguente tabella di instradamento, che contiene voci che puntano a ciascuno dei collegamenti VPC. Ciò consente la comunicazione VPCs tra la connessione VPN e il VPC dei servizi condivisi.

Destinazione	Target	Tipo di route
10.1.0.0/16	*Attachment for VPC A*	propagata
10.2.0.0/16	*Attachment for VPC B*	propagata
10.3.0.0/16	*Attachment for VPC C*	propagata

Per ulteriori informazioni, consulta Abilita la propagazione del percorso su una tabella di routing del gateway di transito in AWS Transit Gateway.

Tabella BGP gateway del cliente

La tabella Customer Gateway BGP contiene i dati CIDRs per tutti e quattro. VPCs

Esempio: gateway di transito in peering

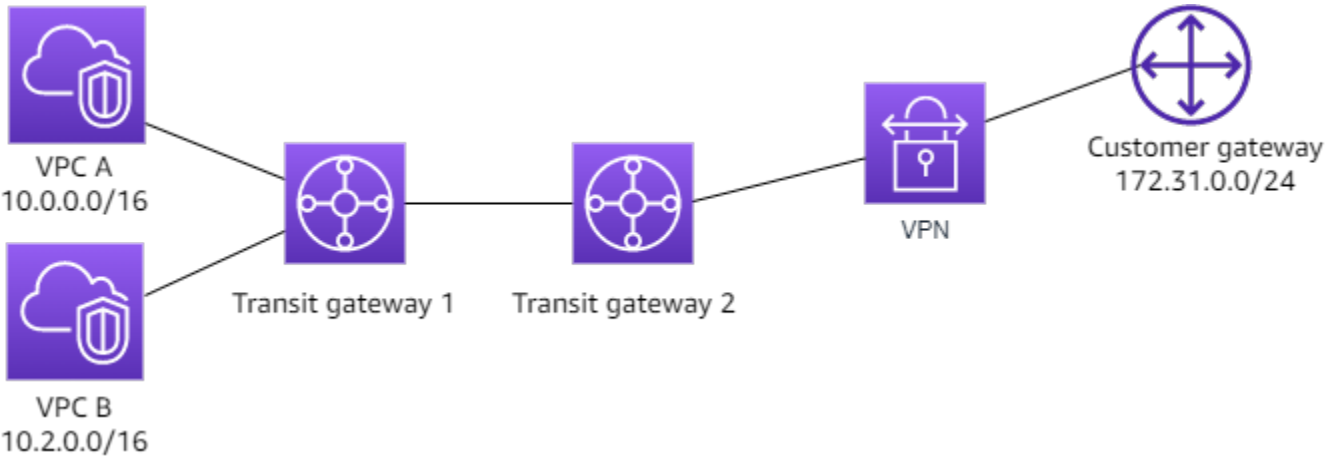
È possibile creare una connessione di peering del gateway di transito tra gateway di transito. È quindi possibile instradare il traffico tra gli allegati per ciascuno dei gateway di transito. In questo scenario, tutti gli allegati VPC e VPN sono associati alla tabella di instradamento predefinita del gateway di transito e si propagano alla tabella di instradamento del gateway di transito. Ogni tabella di instradamento del gateway di transito ha un route statico che punta all'allegato peering del gateway di transito.

Indice

Panoramica

Il seguente diagramma illustra i componenti principali della configurazione di questo scenario. Il gateway di transito 1 ha due allegati VPC e il gateway di transito 2 ha un Site-to-Site allegato VPN.

Pacchetti dalle sottoreti in VPC A e VPC B che hanno Internet come primo route di destinazione attraverso il gateway di transito 1, poi il gateway di transito 2 e quindi instradano alla connessione VPN.



Resources

Crea le seguenti risorse per questo scenario:

- Due. VPCs Per ulteriori informazioni, consulta Crea un VPC nella Guida per l'utente di Amazon VPC.
- Due gateway di transito. Possono trovarsi nella stessa regione o in diverse regioni. Per ulteriori informazioni, consulta the section called “Creazione di un gateway di transito”.
- Due allegati VPC sul primo gateway di transito. Per ulteriori informazioni, consulta the section called “Creare un allegato VPC”.
- Un allegato Site-to-Site VPN sul secondo gateway di transito. Per ulteriori informazioni, consulta the section called “Creare un collegamento del gateway di transito a una VPN”. Rivedi i requisiti per il dispositivo gateway cliente nel Manuale dell'utente AWS Site-to-Site VPN .
- Un allegato peering del gateway di transito tra i due gateway di transito. Per ulteriori informazioni, consulta Allegati di peering del gateway di transito in AWS Transit Gateway.

Quando crei gli allegati VPC, per CIDRs ogni VPC si propagano alla tabella di routing per il gateway di transito 1. Quando la connessione VPN è attiva, si verificano le seguenti operazioni:

- Viene stabilita la sessione BGP
- Il CIDR Site-to-Site VPN si propaga alla tabella di routing per il gateway di transito 2
- I VPC CIDRs vengono aggiunti alla tabella BGP del gateway del cliente

Routing

Ogni VPC ha una tabella di route e ogni gateway di transito ha una tabella di route.

Tabelle di routing VPC A e VPC B

Ogni VPC ha una tabella di instradamento con 2 voci. La prima voce è la voce predefinita per il IPv4 routing locale nel VPC. Questa voce predefinita consente alle risorse di questo VPC di comunicare tra loro. La seconda voce indirizza tutto il resto del traffico di IPv4 sottorete verso il gateway di transito. La tabella seguente mostra i route VPC A.

Destinazione	Target
10.0.0.0/16	locale
0.0.0.0/0	tgw-1-id

Tabelle di routing del gateway di transito

Di seguito è riportato un esempio della tabella di instradamento predefinita per il gateway di transito 1, con la propagazione del percorso abilitata.

Destinazione	Target	Tipo di route
10.0.0.0/16	*Attachment ID for VPC A*	propagata
10.2.0.0/16	*Attachment ID for VPC B*	propagata
0.0.0.0/0	*Attachment ID for peering connection*	static

Di seguito è riportato un esempio di tabella di instradamento predefinita per il gateway di transito 2, con la propagazione del routing attivata.

Destinazione	Target	Tipo di route
172.31.0.0/24	*Attachment ID for VPN connection*	propagata
10.0.0.0/16	*Attachment ID for peering connection*	static
10.2.0.0/16	*Attachment ID for peering connection*	static

Tabella BGP gateway del cliente

La tabella BGP del gateway del cliente contiene il seguente VPC. CIDRs

- 10.0.0.0/16
- 10.2.0.0/16

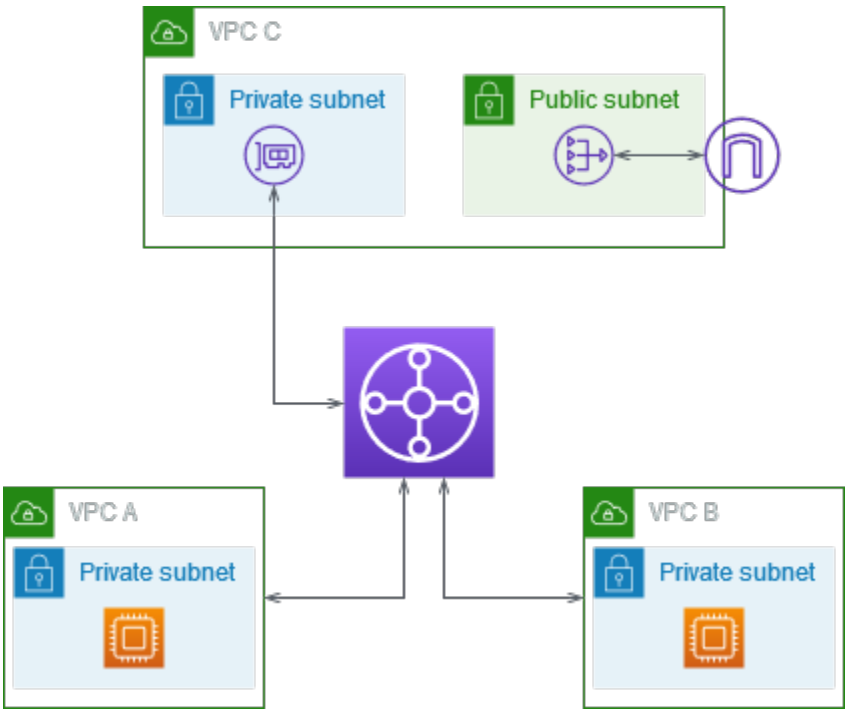
Esempio: Routing in uscita centralizzato verso Internet

È possibile configurare un gateway di transito per instradare il traffico Internet in uscita da un VPC senza gateway Internet a un VPC che contiene un gateway NAT e un gateway Internet.

Indice

Panoramica

Il seguente diagramma illustra i componenti principali della configurazione di questo scenario. Sono presenti applicazioni in VPC A e VPC B che richiedono l'accesso a Internet solo in uscita. Puoi configurare il VPC C con un gateway NAT pubblico e un gateway Internet e una sottorete privata per il collegamento VPC. Connect tutto VPCs a un gateway di transito. Configura il routing in modo che il traffico Internet in uscita da VPC A e VPC B attraversi il gateway di transito e arrivi a VPC C. Il gateway NAT in VPC C instrada il traffico al gateway Internet.



Resources

Crea le seguenti risorse per questo scenario:

- Tre VPCs con intervalli di indirizzi IP che non sono né identici né sovrapposti. Per ulteriori informazioni, consulta Crea un VPC nella Guida per l'utente di Amazon VPC.
- VPC A e VPC B dispongono ciascuno di sottoreti private con istanze. EC2
- VPC C ha le seguenti caratteristiche:
  - Un gateway Internet collegato al VPC. Per ulteriori informazioni, consulta Creazione e collegamento di un gateway Internet nella Guida per l'utente di Amazon VPC.
  - Una sottorete pubblica con un gateway NAT. Per ulteriori informazioni, consulta Creazione di gateway NAT nella Guida per l'utente di Amazon VPC.
  - Una sottorete privata per il collegamento del gateway di transito alla VPN. La sottorete privata deve trovarsi nella stessa zona di disponibilità della sottorete pubblica.
- Un gateway di transito Per ulteriori informazioni, consulta the section called “Creazione di un gateway di transito”.
- Tre allegati VPC sul gateway di transito. I blocchi CIDR per ogni VPC si propagano alla tabella di routing del gateway di transito. Per ulteriori informazioni, consulta the section called “Creare un allegato VPC”. Per il VPC C, è necessario creare il collegamento utilizzando la sottorete privata. Se crei l'allegato utilizzando la sottorete pubblica, il traffico dell'istanza viene indirizzato al gateway

Internet, ma il gateway Internet interrompe il traffico perché le istanze non dispongono di indirizzi IP pubblici. Inserendo il collegamento nella sottorete privata, il traffico viene indirizzato al gateway NAT e il gateway NAT invia il traffico al gateway Internet usando l'indirizzo IP elastico (EIP) come indirizzo IP di origine.

Routing

Sono presenti tabelle di routing per ogni VPC e una tabella di routing per il gateway di transito.

Tabelle di routing

- Tabella di routing per VPC A
- Tabella di routing per VPC B
- Tabelle di instradamento per VPC C
- Tabella di routing del gateway di transito

Tabella di routing per VPC A

Di seguito è riportato un esempio di tabella di instradamento. La prima voce consente alle istanze del VPC di comunicare tra loro. La seconda entrata indirizza tutto il resto del traffico di IPv4 sottorete verso il gateway di transito.

Destinazione	Target
VPC A CIDR	locale
0.0.0.0/0	*transit-gateway-id*

Tabella di routing per VPC B

Di seguito è riportato un esempio di tabella di instradamento. La prima voce consente alle istanze del VPC di comunicare tra loro. La seconda entrata indirizza tutto il resto del traffico di IPv4 sottorete verso il gateway di transito.

Destinazione	Target

Destinazione	Target
VPC B CIDR	locale
0.0.0.0/0	*transit-gateway-id*

Tabelle di instradamento per VPC C

Configura la sottorete pubblica con il gateway NAT aggiungendo una route al gateway Internet. Lascia l'altra sottorete come sottorete privata.

Di seguito è riportata una tabella di instradamento di esempio per la sottorete pubblica. La prima voce consente alle istanze del VPC di comunicare tra loro. La seconda e la terza voce instradano il traffico per VPC A e VPC B al gateway di transito. La voce di ingresso rimanente indirizza tutto il resto del traffico di IPv4 sottorete verso il gateway Internet.

Destinazione	Target
VPC C CIDR	locale
VPC A CIDR	*transit-gateway-id*
VPC B CIDR	*transit-gateway-id*
0.0.0.0/0	*internet-gateway-id*

Di seguito è riportata una tabella di instradamento di esempio per la sottorete privata. La prima voce consente alle istanze del VPC di comunicare tra loro. La seconda entrata indirizza tutto il resto del traffico di IPv4 sottorete verso il gateway NAT.

Destinazione	Target
VPC C CIDR	locale
0.0.0.0/0	*nat-gateway-id*

Tabella di routing del gateway di transito

Di seguito è riportato un esempio della tabella di instradamento del gateway di transito. I blocchi CIDR per ogni VPC si propagano alla tabella di instradamento del gateway di transito. La route statica invia il traffico Internet in uscita a VPC C. Puoi opzionalmente impedire la comunicazione tra VPC aggiungendo una route blackhole per ogni CIDR VPC.

CIDR	Collegamento	Tipo di routing
VPC A CIDR	*Attachment for VPC A*	propagata
VPC B CIDR	*Attachment for VPC B*	propagata
VPC C CIDR	*Attachment for VPC C*	propagata
0.0.0.0/0	*Attachment for VPC C*	static

Esempio: appliance in un VPC di servizi condivisi

È possibile configurare un accessorio (ad esempio un'appliance di sicurezza) in un VPC di servizi condivisi. Tutto il traffico instradato tra gli allegati del gateway di transito viene prima ispezionato dall'appliance nel VPC di servizi condivisi. Quando la modalità accessorio è abilitata, un gateway di transito seleziona un'unica interfaccia di rete nel VPC dell'appliance, utilizzando un algoritmo hash di flusso, a cui inviare il traffico per tutta la durata del flusso. Il gateway di transito utilizza la stessa interfaccia di rete per il traffico di ritorno. In questo modo, il traffico bidirezionale viene instradato simmetricamente: viene instradato attraverso la stessa zona di disponibilità nell'allegato VPC per tutta la durata del flusso. Se nell'architettura sono presenti più gateway di transito, ogni gateway di transito mantiene la propria affinità di sessione e può selezionare un'interfaccia di rete diversa.

È necessario collegare esattamente un gateway di transito al VPC dell'appliance per garantire l'aderenza del flusso. Il collegamento di più gateway di transito a un singolo VPC dell'appliance non garantisce l'aderenza del flusso in quanto i gateway di transito non condividono le informazioni sullo stato del flusso tra loro.

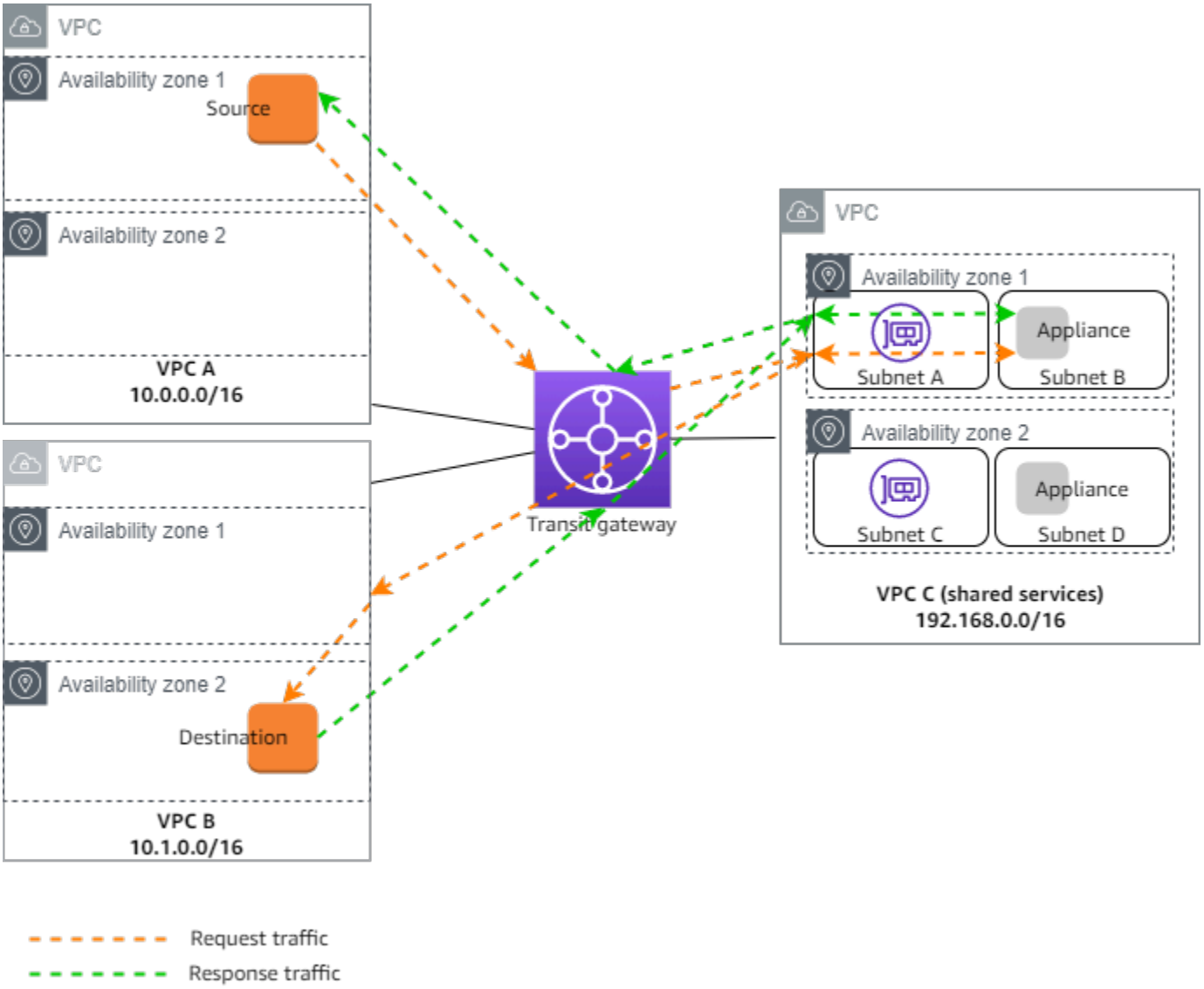
Important

- Il traffico in modalità appliance viene instradato correttamente a condizione che il traffico di fonte e di destinazione arrivi a un VPC centralizzato (VPC di ispezione) dallo stesso allegato del gateway di transito. Il traffico può diminuire se l'origine e la destinazione si trovano su due diversi allegati del gateway di transito. Il traffico può diminuire se il VPC centralizzato riceve il traffico da un gateway diverso, ad esempio un gateway Internet, e quindi lo invia all'allegato del gateway di transito dopo l'ispezione.
- L'attivazione della modalità appliance su un allegato esistente potrebbe influire sul percorso corrente dell'allegato, in quanto l'allegato può attraversare qualsiasi zona di disponibilità. Quando la modalità appliance non è abilitata, il traffico viene mantenuto verso la zona di disponibilità di origine.

Indice

Panoramica

Il seguente diagramma illustra i componenti principali della configurazione di questo scenario. Il gateway di transito dispone di tre allegati VPC. VPC C è un VPC di servizi condivisi. Il traffico tra VPC A e VPC B viene instradato al gateway di transito, quindi instradato a un'appliance di sicurezza in VPC C per l'ispezione prima di essere instradato alla destinazione finale. L'appliance è un'appliance stateful, pertanto viene ispezionato sia il traffico di richiesta che di risposta. Per l'elevata disponibilità, è presente un accessorio in ogni zona di disponibilità in VPC C.



In questo scenario, si creano le seguenti risorse:

- Tre. VPCs Per ulteriori informazioni, consulta Crea un VPC nella Guida per l'utente di Amazon VPC.
- Un gateway di transito. Per ulteriori informazioni, consulta the section called “Creazione di un gateway di transito”.
- Tre allegati VPC, uno per ciascuno. VPCs Per ulteriori informazioni, consulta the section called “Creare un allegato VPC”.

  Per ogni allegato VPC, specificare una sottorete in ogni zona di disponibilità. Per i servizi condivisi VPC, queste sono le sottoreti in cui il traffico viene instradato al VPC dal gateway di transito. Nell'esempio precedente, si tratta di sottoreti A e C.

Per l'allegato VPC per VPC C, attivare il supporto della modalità accessorio in modo che il traffico di risposta venga instradato alla stessa zona di disponibilità in VPC C del traffico di origine.

La console Amazon VPC non supporta la modalità accessorio. Puoi anche utilizzare l'API Amazon VPC, un AWS SDK, AWS CLI abilitare la modalità appliance oppure. CloudFormationAd esempio, aggiungi `--options ApplianceModeSupport=enable` al comando -attachment o create-transit-gateway-vpc-attachment. modify-transit-gateway-vpc

> **Note**
>
> La costanza del flusso in modalità appliance è garantita solo per il traffico di origine e di destinazione proveniente dal VPC di ispezione.

Appliance con stato e modalità appliance

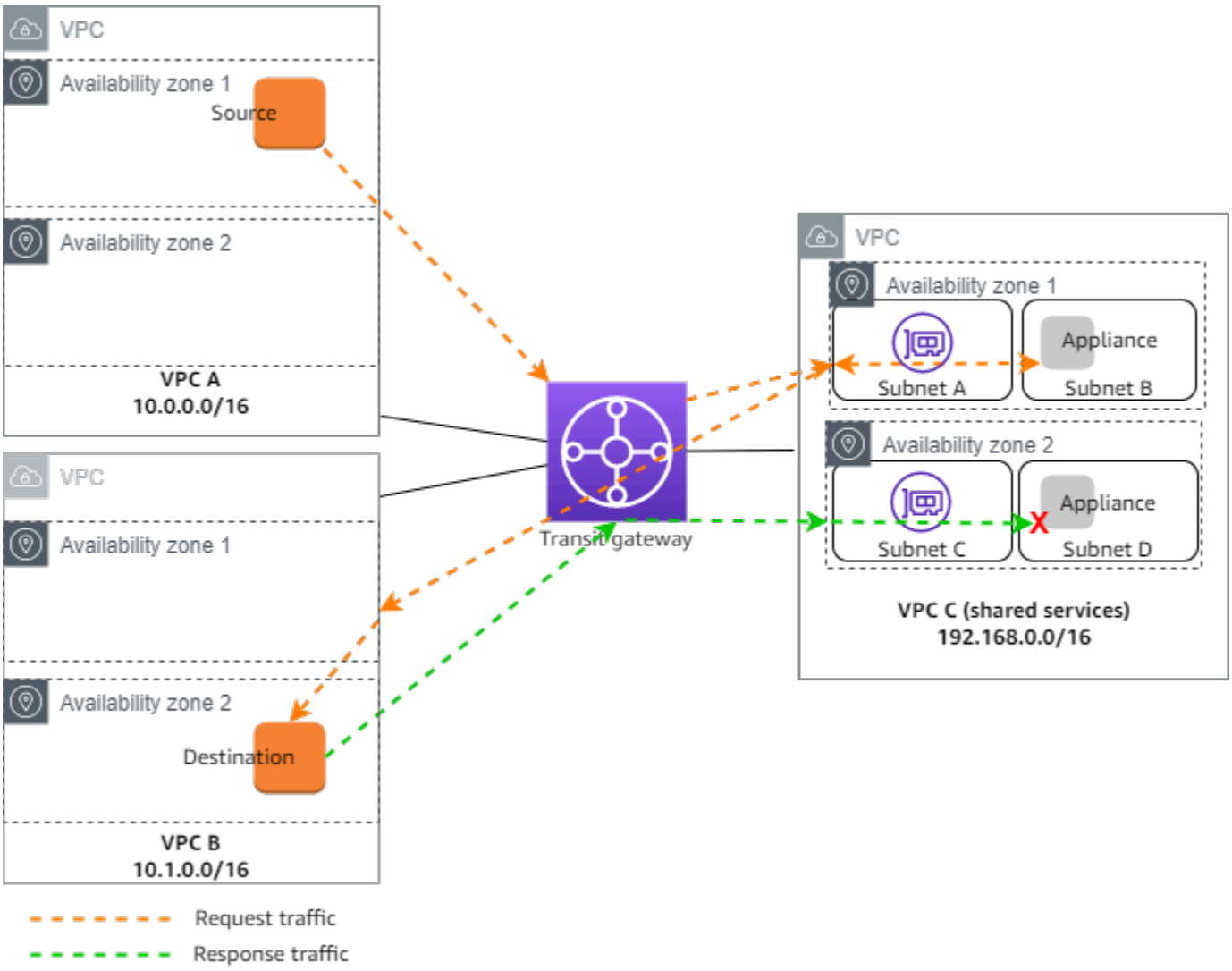
Se gli allegati VPC si estendono su più zone di disponibilità e si richiede che il traffico tra host di origine e di destinazione venga instradato attraverso lo stesso accessorio per l'ispezione con stato, abilitare il supporto in modalità accessorio per l'allegato VPC in cui si trova l'appliance

Per ulteriori informazioni, consulta Architettura di ispezione centralizzata nel blog. AWS

Comportamento quando la modalità appliance non è abilitata

Quando la modalità appliance non è abilitata, un gateway di transito tenta di mantenere il traffico instradato tra gli allegati VPC nella zona di disponibilità di origine fino a quando non raggiunge la destinazione. Il traffico attraversa le zone di disponibilità tra gli allegati solo se si verifica un errore nella zona di disponibilità o se non vi sono subnet associate a un allegato VPC in tale zona di disponibilità.

Il diagramma seguente mostra un flusso di traffico quando il supporto della modalità appliance non è abilitato. Il traffico di risposta che proviene dalla zona di disponibilità 2 in VPC B viene instradato dal gateway di transito alla stessa zona di disponibilità in VPC C. Il traffico viene pertanto interrotto, poiché l'appliance nella zona di disponibilità 2 non è a conoscenza della richiesta originale proveniente dall'origine in VPC A.



Routing

Ogni VPC dispone di una o più tabelle di route e il gateway di transito dispone di due tabelle di route.

Tabelle di routing VPC

VPC A e VPC B

VPCs A e B dispongono di tabelle di percorso con 2 voci. La prima voce è la voce predefinita per il IPv4 routing locale nel VPC. Questa voce predefinita consente alle risorse di questo VPC di comunicare tra loro. La seconda voce indirizza tutto il resto del traffico di IPv4 sottorete verso il gateway di transito. Di seguito è riportata la tabella dei percorsi per VPC A.

Destinazione	Target

Destinazione	Target
10.0.0.0/16	locale
0.0.0.0/0	tgw-id

VPC C

Il VPC (VPC C) di servizi condivisi dispone di tabelle di route diverse per ogni sottorete. La sottorete A viene utilizzata dal gateway di transito (è possibile specificare questa sottorete quando si crea l'allegato VPC). La tabella di route per la sottorete A indirizza tutto il traffico all'accessorio nella sottorete B.

Destinazione	Target
192.168.0.0/16	locale
0.0.0.0/0	appliance-eni-id

La tabella dei percorsi per la sottorete B (che contiene l'accessorio) indirizza il traffico al gateway di transito.

Destinazione	Target
192.168.0.0/16	locale
0.0.0.0/0	tgw-id

Tabelle di routing del gateway di transito

Questo gateway di transito utilizza una tabella di route per VPC A e VPC B e una tabella di route per i servizi condivisi VPC (VPC C).

Gli allegati VPC A e VPC B sono associati alla seguente tabella di route. La tabella dei percorsi indirizza tutto il traffico verso VPC C.

Destinazione	Target	Tipo di route
0.0.0.0/0	*Attachment ID for VPC C*	static

L'allegato VPC C è associato alla seguente tabella di route. Instrada il traffico verso VPC A e VPC B.

Destinazione	Target	Tipo di route
10.0.0.0/16	*Attachment ID for VPC A*	propagata
10.1.0.0/16	*Attachment ID for VPC B*	propagata

Tutorial: Inizia a usare Transit Gateway AWS

I seguenti tutorial ti aiutano a familiarizzare con i gateway di transito in Transit Gateway AWS . Le attività illustrate nei seguenti tutorial ti guidano nella creazione di un gateway di transito e nella successiva connessione di due dei tuoi VPCs gateway di transito utilizzando quel gateway di transito. Puoi creare un gateway di transito utilizzando la console Amazon VPC o utilizzando il. AWS CLI

Attività

- Tutorial: creare un AWS Transit Gateway utilizzando la console Amazon VPC
- Tutorial: creare un AWS Transit Gateway utilizzando la AWS riga di comando

Tutorial: creare un AWS Transit Gateway utilizzando la console Amazon VPC

In questo tutorial, imparerai come utilizzare la console Amazon VPC per creare un gateway di transito e VPCs collegarne due. Dovrai creare il gateway di transito, collegarli entrambi VPCs e quindi configurare i percorsi necessari per abilitare la comunicazione tra il gateway di transito e il tuo VPCs.

Prerequisiti

- Per dimostrare un semplice esempio di utilizzo di un gateway di transito, VPCs creane due nella stessa regione. Non VPCs possono essere né identici né sovrapposti CIDRs. Avvia un' EC2 istanza Amazon in ogni VPC. Per ulteriori informazioni, consulta Create a VPC nella Amazon VPC User Guide e Launch an instance nella Amazon User Guide. EC2
- Non puoi avere percorsi identici che puntano a due percorsi diversi. VPCs Un gateway CIDRs di transito non propaga il VPC appena collegato se esiste una route identica nelle tabelle di routing del gateway di transito.
- Verificare di disporre delle autorizzazioni necessarie per l'utilizzo di gateway di transito. Per ulteriori informazioni, consulta Gestione delle identità e degli accessi in AWS Transit Gateway .
- Non è possibile eseguire il ping tra gli host se non hai aggiunto una regola ICMP a ciascuno dei gruppi di sicurezza dell'host. Per ulteriori informazioni, consulta Configura le regole dei gruppi di sicurezza nella Amazon VPC User Guide.

Fasi

Fase 1: creazione del gateway di transito

Quando crei un gateway di transito, viene creata una tabella di routing predefinita per il gateway di transito e questa viene utilizzata come tabella di routing predefinita per le associazioni nonché come tabella di routing predefinita per la propagazione.

Creazione di un gateway di transito

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel selettore Regione, scegli la regione che hai usato quando hai creato il. VPCs
3. Nel riquadro di navigazione, selezionare Transit Gateways (Gateway di transito).
4. Selezionare Create Transit Gateway (Crea gateway di transito).
5. (Facoltativo) Per Name tag (Tag nome), immettere un nome per il gateway di transito. Tale azione crea un tag con chiave "Name" e il nome specificato come valore.
6. (Facoltativo) In Description (Descrizione) inserire una descrizione per il gateway di transito.
7. Nella sezione Configura il gateway di transito, procedi come segue:

    1. In Amazon side Autonomous System Number (ASN lato Amazon), inserire ASN privato per il gateway di transito. Dovrebbe essere l'ASN per il AWS lato di una sessione BGP (Border Gateway Protocol).

        L'intervallo è compreso tra 64512 e 65534 per 16 bit. ASNs

        L'intervallo va da 4200000000 a 4294967294 per 32 bit. ASNs

        Se si dispone di una distribuzione tra regioni, si consiglia di utilizzare un ASN univoco per ognuno dei propri gateway di transito.
    2. (Facoltativo) Scegliete se abilitare una delle seguenti opzioni:
        - Supporto DNS per il collegamento VPCs a questo gateway di transito.

- Supporto VPN ECMP per connessioni VPN collegate al gateway di transito.
- Associazione alla tabella di routing predefinita, che associa automaticamente gli allegati del gateway di transito alla tabella di routing predefinita di questo gateway di transito.
- Propagazione della tabella di routing predefinita, che propaga automaticamente gli allegati della tabella di routing alla tabella di routing predefinita di questo gateway di transito.
- Supporto multicast, che consente di creare domini multicast in questo gateway di transito.

8. (Facoltativo) Nella sezione delle opzioni di Configure-cross-account condivisione, scegli se accettare automaticamente gli allegati condivisi. Se abilitato, gli allegati vengono accettati automaticamente. Altrimenti, è necessario accettare o rifiutare le richieste di allegati.
9. (Facoltativo) Nella sezione Blocchi CIDR del gateway di transito, aggiungi un blocco CIDR di dimensione /24 o superiore per IPv4 gli indirizzi o un blocco CIDR /64 o più grande per gli indirizzi. IPv6 Puoi quindi associare qualsiasi intervallo di indirizzi IP pubblici o privati, ad eccezione degli indirizzi nell'intervallo 169.254.0.0/16, e gli intervalli che si sovrappongono agli indirizzi degli allegati VPC e delle reti locali.

   > **Note**
   >
   > I blocchi CIDR del gateway di transito vengono utilizzati se si configurano gli allegati Connect (GRE) o PrivateIP. VPNs Transit Gateway assegna IPs gli endpoint Tunnel (GRE/PrivateIP VPN) da questo intervallo.

10. (Facoltativo) Aggiungi tag chiave-valore a questo gateway di transito per facilitarne ulteriormente l'identificazione.

    1. Scegli Aggiungi nuovo tag.
    2. Inserisci il nome della chiave e il valore associato.
    3. Scegli Aggiungi nuovo tag per aggiungere altri tag o vai al passaggio successivo.

11. Selezionare Create Transit Gateway (Crea gateway di transito). Quando il gateway viene creato, lo stato iniziale del gateway di transito è `pending`.

Passaggio 2: collega il tuo VPCs al tuo gateway di transito

Prima di procedere con la creazione di un collegamento, attendere fino a quando il gateway di transito creato nella sezione precedente è indicato come disponibile. Creare un collegamento per ogni VPC.

Conferma di averne creati due VPCs e avviato un' EC2 istanza in ciascuna, come descritto inPrerequisiti.

Creare un collegamento del gateway di transito a un VPC

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Collegamenti del gateway di transito).
3. Selezionare Create transit gateway attachments (Crea collegamenti del gateway di transito).
4. (Facoltativo) In Name tag (Tag nome), inserire il nome del collegamento.
5. In Transit gateway ID (ID gateway di transito), selezionare il gateway di transito da usare per il collegamento.
6. In Attachment type (Tipo collegamento), selezionare VPC.
7. Selezionare se abilitare il DNS support (Supporto DNS). Per questo esercizio, non attivate IPv6 il supporto.
8. Per VPC ID (ISD VPC), scegliere il VPC da collegare al gateway di transito.
9. Per Subnet IDs, selezionare una sottorete per ogni zona di disponibilità da utilizzare dal gateway di transito per instradare il traffico. È necessario selezionare almeno una sottorete. È possibile selezionare solo una sottorete per ogni zona di disponibilità.
10. Selezionare Create transit gateway attachments (Crea collegamenti del gateway di transito).

Ogni collegamento è sempre associato a una sola tabella di instradamento. Le tabelle di routing possono essere associate a nessuno o a molti collegamenti. Per determinare le route da configurare, decidere il caso d'uso per il gateway di transito, quindi configurare le route. Per ulteriori informazioni, consulta the section called “Esempi di scenari di gateway di transito”.

Fase 3: Aggiungi percorsi tra il gateway di transito e il VPCs

Una tabella di routing include route dinamiche e statiche che determinano l'hop successivo da associare in VPCs base all'indirizzo IP di destinazione del pacchetto. Configura un instradamento con una destinazione per gli instradamenti non locali e la destinazione dell'ID allegato del gateway di transito. Per maggiori informazioni, consulta Routing per un gateway di transito nella Guida per l'utente di Amazon VPC.

Per aggiungere una nuova route a una tabella di instradamento di un VPC

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Route Tables (Tabelle di routing).
3. Selezionare la tabella di instradamento personalizzata associata al VPC.
4. selezionare la scheda Routes (Route), selezionare Edit routes (Modifica route).
5. Selezionare Add route (Aggiungi route).
6. Nella colonna Destination (Destinazione), immettere l'intervallo di indirizzi IP di destinazione. Per Target, scegliere Gateway di transito e quindi scegliere l'ID del gateway di transito.
7. Scegli Save changes (Salva modifiche).

Fase 4: testa il gateway di transito

Puoi confermare che il gateway di transito è stato creato correttamente connettendoti a un' EC2 istanza Amazon in ogni VPC e quindi inviando dati tra di loro, ad esempio un comando ping. Per ulteriori informazioni, consulta Connect to your EC2 istance nella Amazon EC2 User Guide.

Fase 5: eliminare il gateway di transito

Quando non è più necessario un gateway di transito, è possibile eliminarlo.

Non è possibile eliminare un gateway di transito con allegati di risorse. Se provi a eliminare un gateway di transito che ha degli allegati, ti verrà richiesto di eliminare prima gli allegati. Non appena il gateway di transito viene eliminato, smetti di incorrere in addebiti per esso.

Per eliminare il gateway di transito

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateways (Gateway di transito).
3. Seleziona il gateway di transito, quindi scegli Actions (Operazioni), Delete transit gateway (Elimina gateway di transito).
4. Immettere **`delete`** e scegliere Delete (Elimina).

   Lo stato del gateway di transito sulla pagina Transit gateways (Gateway di transito) è Deleting (Eliminazione in corso). Una volta eliminato, il gateway di transito viene rimosso dalla pagina.

Tutorial: creare un AWS Transit Gateway utilizzando la AWS riga di comando

In questo tutorial, imparerai come utilizzare il per AWS CLI creare un gateway di transito e VPCs collegarne due. Creerai il gateway di transito, collegherai entrambi VPCs e quindi configurerai i percorsi necessari per abilitare la comunicazione tra il gateway di transito e il tuo VPCs.

Prerequisiti

Prima di iniziare, assicurati di avere:

- AWS CLI installato e configurato con le autorizzazioni appropriate. Se non lo hai AWS CLI installato, consulta la documentazione dell'interfaccia a riga di AWS comando.
- Non VPCs possono essere né identici né sovrapposti CIDRs. Per ulteriori informazioni, consulta Crea un VPC nella Guida per l'utente di Amazon VPC.
- Un' EC2 istanza in ogni VPC. Per i passaggi per avviare un' EC2 istanza in un VPC, consulta Launch an instance nella Amazon EC2 User Guide.
- Gruppi di sicurezza configurati per consentire il traffico ICMP tra le istanze. Per i passaggi per controllare il traffico utilizzando i gruppi di sicurezza, consulta Controlla il traffico verso AWS le tue risorse utilizzando i gruppi di sicurezza nella Amazon VPC User Guide.
- Autorizzazioni IAM appropriate per lavorare con i gateway di transito. Per verificare le autorizzazioni IAM del gateway di transito, consulta la sezione Gestione delle identità e degli accessi nei gateway di AWS transito nella Guida.AWS Transit Gateway

Fasi

Fase 1: creazione del gateway di transito

Quando crei un gateway di transito, AWS crea una tabella di routing del gateway di transito predefinita e la utilizza come tabella di routing di associazione predefinita e tabella di routing di propagazione predefinita. Di seguito viene illustrato un esempio di `create-transit-gateway` richiesta nella `us-west-2` regione. Nella richiesta `options` sono state inserite altre informazioni. Per ulteriori informazioni sul `create-transit-gateway` comando, incluso un elenco delle opzioni che è possibile inserire nella richiesta, vedere create-transit-gateway.

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

La risposta mostra quindi che il gateway di transito è stato creato. Nella risposta, `0ptions` i valori restituiti sono tutti valori predefiniti.

```
{
    "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**
>
> Questo comando restituisce informazioni sul nuovo gateway di transito, incluso il relativo ID. Prendi nota dell'ID del gateway di transito (`tgw-1234567890abcdef0`) poiché ti servirà nei passaggi successivi.

Fase 2: Verifica lo stato di disponibilità del gateway di transito

Quando crei un gateway di transito, questo viene inserito in uno `pending` stato. Lo stato passerà automaticamente da pendente a disponibile, ma finché non lo farà non potrai allegarne nessuno VPCs finché non cambierà lo stato. Per verificare lo stato, esegui il `describe-transit-gatweways` comando utilizzando l'ID del gateway di transito appena creato insieme all'opzione filters. L'`filters`opzione utilizza `Name=state` e `Values=available` accoppia. Il comando esegue quindi una ricerca per verificare se lo stato del gateway di transito è disponibile. In caso affermativo, viene visualizzata `"State": "available"` la risposta. Se si trova in qualsiasi altro stato, non è ancora disponibile per l'uso. Attendi alcuni minuti prima di eseguire il comando.

Per ulteriori informazioni sul comando `describe-transit-gateways`, consulta describe-transit-gateways.

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

Attendi che lo stato del gateway di transito cambi da `pending` a `available` prima di procedere. Nella risposta seguente, `State` è cambiato in`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"
                }
            ]
        }
    ]
}
```

Fase 3: Collega il tuo VPCs al tuo gateway di transito

Una volta che il gateway di transito è disponibile, crea un allegato per ogni VPC utilizzando il. `create-transit-gateway-vpc-attachment` Dovrai includere il `transit-gateway-id`vpc-id, il e il`subnet-ids`.

Per ulteriori informazioni sul `create-transit-vpc attachment` comando, vedere create-transit-gateway-vpc-attachment.

Nell'esempio seguente, il comando viene eseguito due volte, una volta per ogni VPC.

Per il primo VPC esegui quanto segue utilizzando il primo `vpc_id` e: `subnet-ids`

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

La risposta mostra l'allegato riuscito. L'allegato viene creato in uno `pending` stato. Non è necessario modificare questo stato poiché passa automaticamente a uno `available` stato. Questo processo potrebbe richiedere diversi minuti.

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

Per il secondo VPC, esegui lo stesso comando di cui sopra usando il secondo `vpc_id` e: `subnet-ids`

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

La risposta a questo comando mostra anche un allegato riuscito, con l'allegato attualmente in uno `pending` stato.

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

Fase 4: Verificare che gli allegati del gateway di transito siano disponibili

Gli allegati del gateway di transito vengono creati in uno stato inizialepending. Non potrai utilizzare questi allegati nei tuoi percorsi finché lo stato non cambierà a. available Ciò avviene automaticamente. Usa il describe-transit-gateways comando, insieme atransit-gateway-id, per controllare ilState. Per ulteriori informazioni sul comando describe-transit-gateways, consulta describe-transit-gateways.

Esegui il comando seguente per controllare lo stato. In questo esempio, i campi opzionali Name e i Values filtri vengono passati nella richiesta:

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

La risposta seguente mostra che entrambi gli allegati sono in uno available stato:

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

Passaggio 5: aggiungi percorsi tra il tuo gateway di transito e VPCs

Configura i percorsi nella tabella di routing di ogni VPC per indirizzare il traffico verso l'altro VPC attraverso il gateway di transito utilizzando il `create-route` comando insieme alla tabella di routing for `transit-gateway-id` each VPC. Nell'esempio seguente, il comando viene eseguito due volte, una volta per ogni tabella di routing. La richiesta include il `route-table-iddestination-cidr-block`, e `transit-gateway-id` per ogni route VPC che stai creando.

Per ulteriori informazioni sul `create-route` comando, consulta create-route.

Per la prima tabella di routing del VPC esegui il seguente comando:

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

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

Per la tabella di routing del secondo VPC esegui il seguente comando. Questo percorso utilizza un `route-table-id` VPC `destination-cidr-block` diverso dal primo. Tuttavia, poiché si utilizza un solo gateway di transito, `transit-gateway-id` viene utilizzato lo stesso.

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

La risposta viene restituita `true` per ogni percorso, indicando che i percorsi sono stati creati.

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

> **Note**
>
> Sostituisci i blocchi CIDR di destinazione con i blocchi CIDR effettivi del tuo. VPCs

Passaggio 6: testare il gateway di transito

Puoi confermare che il gateway di transito è stato creato correttamente connettendoti a un' EC2 istanza in un VPC e eseguendo il ping di un'istanza nell'altro VPC, quindi eseguendo il comando. `ping`

1. Connettiti alla tua EC2 istanza nel primo VPC tramite SSH o Instance Connect EC2
2. Esegui il ping dell'indirizzo IP privato dell' EC2 istanza nel secondo VPC:

   ```
   ping 10.2.0.50
   ```

> **Note**
>
> Sostituiscilo `10.2.0.50` con l'indirizzo IP privato effettivo dell' EC2 istanza nel secondo VPC.

Se il ping ha esito positivo, il gateway di transito è configurato correttamente e il traffico viene instradato tra di voi. VPCs

Passo 7: Eliminare gli allegati del gateway di transito e il gateway di transito

Quando non è più necessario il gateway di transito, è possibile eliminarlo. Innanzitutto, è necessario eliminare tutti gli allegati. Esegui il `delete-transit-gateway-vpc-attachment` comando utilizzando il comando `transit-gateway-attachment-id` per ogni allegato. Dopo aver eseguito il comando, utilizzare `delete-transit-gateway` per eliminare il gateway di transito. Per quanto segue, elimina i due allegati VPC e il gateway di transito singolo creati nei passaggi precedenti.

> **Important**
>
> Smetterai di incorrere in addebiti una volta eliminati tutti gli allegati del gateway di transito.

1. Eliminare gli allegati VPC utilizzando il comando. `delete-transit-gateway-vpc-attachment` Per ulteriori informazioni sul `delete-transit-gateway-vpc-attachment` comando, vedere delete-transit-gateway-vpc -attachment.

   Per il primo allegato, esegui il comando seguente:

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

   La risposta di eliminazione per il primo allegato VPC restituisce quanto segue:

   ```
   {
       "TransitGatewayVpcAttachment": {
           "TransitGatewayAttachmentId": "tgw-attach-1234567890abcdef0",
           "TransitGatewayId": "tgw-1234567890abcdef0",
           "VpcId": "vpc-abcdef1234567890",
   ```

```
        "VpcOwnerId": "123456789012",
        "State": "deleting",
        "CreationTime": "2025-06-23T18:42:56+00:00"
    }
}
```

Esegui il `delete-transit-gateway-vpc-attachment` comando per il secondo allegato:

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

La risposta di eliminazione per il secondo allegato VPC restituisce quanto segue:

```
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. Gli allegati rimangono in uno `deleting` stato finché non vengono eliminati. Una volta eliminato, puoi eliminare il gateway di transito. Usa il `delete-transit-gateway` comando insieme `atransit-gateway-id`. Per ulteriori informazioni sul `delete-transit-gateway` comando, vedere delete-transit-gateway.

   L'esempio seguente elimina ciò `My Transit Gateway` che è stato creato nel primo passaggio precedente:

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

   Di seguito viene mostrata la risposta alla richiesta, che include l'ID e il nome del gateway di transito eliminati, insieme alle opzioni originali impostate per il gateway di transito al momento della creazione.

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


Conclusioni

Hai creato con successo un gateway di transito, ne hai collegati due VPCs , configurato il routing tra di essi e hai verificato la connettività. Questo semplice esempio dimostra le funzionalità di base dei AWS Transit Gateways. Per scenari più complessi, come la connessione a reti locali o l'implementazione di configurazioni di routing più avanzate, consulta la Transit Gateways Guide.AWS

AWS Best practice per la progettazione di Transit Gateway

Di seguito sono riportate le best practice per la progettazione del gateway di transito:

- Utilizza una sottorete separata per ogni allegato VPC del gateway di transito. Per ogni sottorete, ad esempio, utilizzate un piccolo CIDR/28, in modo da avere più indirizzi per le EC2 risorse. Quando usi una sottorete separata, puoi configurare quanto segue:
  - Mantieni aperta la rete in entrata e in uscita ACLs associata alle sottoreti del gateway di transito.
  - A seconda del flusso di traffico, puoi applicare la rete alle sottoreti del carico ACLs di lavoro.
- Crea una lista di controllo degli accessi di rete e associala a tutte le sottoreti associate al gateway di transito. Mantieni aperta la lista di controllo degli accessi di rete in entrata e in uscita.
- Associa la stessa tabella di routing VPC a tutte le sottoreti associate al gateway di transito, a meno che la progettazione di rete non richieda più tabelle di routing VPC (ad esempio, un VPC middle-box che instrada il traffico attraverso più gateway NAT).
- Utilizza le connessioni VPN Border Gateway Protocol (BGP). Site-to-Site Se il dispositivo gateway del cliente o il firewall per la connessione supporta la funzione percorso multiplo, abilita la caratteristica.
- Abilita la propagazione delle rotte per gli allegati Direct Connect gateway e gli allegati VPN BGP. Site-to-Site
- Durante la migrazione dal peering VPC all'utilizzo di un gateway di transito. Una mancata corrispondenza delle dimensioni MTU tra il peering VPC e il gateway di transito potrebbe causare il calo di alcuni pacchetti per il traffico asimmetrico. Aggiorna entrambi VPCs contemporaneamente per evitare che i pacchetti jumbo cadano a causa di disallineamenti tra le dimensioni.
- Non sono necessari gateway di transito aggiuntivi per un'elevata disponibilità, perché i gateway di transito sono altamente disponibili in base alla progettazione.
- Limitare il numero di tabelle di route gateway di transito a meno che la progettazione non richieda più tabelle di route gateway di transito.
- Per la ridondanza, utilizza un unico gateway di transito in ogni regione per il ripristino di emergenza.
- Per distribuzioni con più gateway di transito, ti consigliamo di utilizzare un Autonomous System Number univoco (ASN) per ciascuno dei gateway di transito. È anche possibile usare il peering tra regioni. Per ulteriori informazioni, consulta Creazione di una rete globale utilizzando il peering interregionale. AWS Transit Gateway

Lavora con AWS Transit Gateway

È possibile utilizzare i gateway di transito con la console Amazon VPC o la AWS CLI. Per informazioni sull'attivazione e la gestione del supporto di crittografia per il gateway di transito, consultathe section called “Supporto per la crittografia”.

Argomenti

Gateway di transito condivisi

Puoi utilizzare AWS Resource Access Manager (RAM) per condividere un gateway di transito per gli allegati VPC tra account o in tutta l'organizzazione in. AWS Organizations La RAM deve essere abilitata e le risorse devono essere condivise con un'organizzazione. Per ulteriori informazioni, consulta Abilitare la condivisione delle risorse con AWS Organizations nella Guida per l'utente di AWS RAM .

Considerazioni

Se desideri condividere un gateway di transito, tieni presente quanto segue.

- È necessario creare un AWS Site-to-Site VPN allegato nello stesso AWS account proprietario del gateway di transito.
- Un collegamento a un gateway Direct Connect utilizza un'associazione di gateway di transito e può trovarsi nello stesso AWS account del gateway Direct Connect o in uno diverso dal gateway Direct Connect.

Per impostazione predefinita, gli utenti non dispongono dell'autorizzazione per creare o modificare AWS RAM risorse. Per consentire agli utenti di creare o modificare risorse ed eseguire attività, devi creare delle policy IAM che forniscano l'autorizzazione per l'uso di risorse e operazioni API specifiche. Quindi, collega queste policy agli utenti o ai gruppi IAM che hanno bisogno delle autorizzazioni.

Solo il proprietario della risorsa è in grado di eseguire le operazioni descritte di seguito:

- Creare una condivisione di risorse.
- Aggiornare una condivisione di risorse.
- Visualizzare una condivisione di risorse.
- Visualizzare le risorse condivise dall'account in tutte le condivisioni di risorse.
- Visualizzare i principali con cui condividi le risorse in tutte le condivisioni di risorse. Visualizzare i principali con si effettua la condivisione consente di determinare gli utenti che hanno accesso alle risorse condivise.
- Eliminare una condivisione di risorse.
- Esegui tutte le tabelle di routing dei gateway di transito, degli allegati dei gateway di transito e dei gateway di transito APIs.

Puoi eseguire le operazioni illustrate di seguito sulle risorse condivise con te:

- Accettare o respingere un invito alla condivisione di risorse.
- Visualizzare una condivisione di risorse.
- Visualizzare le risorse condivise a cui accedere.
- Visualizzare un elenco di tutti i principali che condividono risorse con l'utente. Puoi vedere le risorse e le condivisioni di risorse con te condivise.
- Puoi eseguire l'API `DescribeTransitGateways`.
- Esegui quelli APIs che creano e descrivono gli allegati, ad esempio `CreateTransitGatewayVpcAttachment` e`DescribeTransitGatewayVpcAttachments`, nella loro VPCs.

- Lasciare una condivisione di risorse.

Quando un gateway di transito viene condiviso con te, non potrai creare, modificare o eliminare le tabelle di instradamento del gateway di transito o le propagazioni e le associazioni di queste tabelle.

Quando si crea un gateway di transito, il gateway di transito viene creato nella zona di disponibilità mappata all'account ed è indipendente da altri account. Quando il gateway di transito e le entità dell'allegato si trovano in account diversi, utilizzare gli ID della zona di disponibilità per identificare in modo univoco e coerente la zona di disponibilità. Ad esempio, use1-az1 è un ID AZ per la regione us-east-1 ed è mappato alla stessa posizione in ogni account. AWS

Eliminare la condivisione di un gateway di transito

Quando il proprietario della condivisione annula la condivisione del gateway di transito, si applicano le seguenti regole:

- L'allegato del gateway di transito rimane funzionante.
- L'account condiviso non può descrivere il gateway di transito.
- Il proprietario del gateway di transito e il proprietario della condivisione possono eliminare l'allegato del gateway di transito.

Quando un gateway di transito non viene condiviso con un altro AWS account o se l' AWS account con cui è condiviso il gateway di transito viene rimosso dall'organizzazione, il gateway di transito stesso non ne risentirà.

Sottoreti condivise

Il proprietario del VPC può collegare un gateway di transito a una sottorete condivisa del VPC. I partecipanti non possono. Il traffico proveniente dalle risorse dei partecipanti può utilizzare gli allegati a seconda dei percorsi impostati sulla sottorete condivisa del VPC dal proprietario del VPC.

Per ulteriori informazioni, consulta Condivisione del VPC con altri account nella Guida per l'utente di Amazon VPC.

Gateway di transito in AWS Transit Gateway

Un gateway di transito consente di collegare connessioni VPN VPCs e di instradare il traffico tra di esse. Un gateway di transito funziona trasversalmente Account AWS e puoi AWS RAM utilizzarlo per

condividere il gateway di transito con altri account. Dopo aver condiviso un gateway di transito con un altro Account AWS, il proprietario dell'account può collegarlo VPCs al gateway di transito. Un utente di uno qualsiasi degli account può eliminare il collegamento in qualsiasi momento.

È possibile abilitare il multicast in un gateway di transito, quindi creare un dominio del gateway di transito multicast che consenta l'invio del traffico multicast dall'fonte multicast ai membri del gruppo multicast tramite allegati VPC associati al dominio.

Ogni collegamento di VPC o VPN è associato a una singola tabella di instradamento. La tabella di instradamento definisce il successivo segmento di rete su cui inoltrare il traffico proveniente dallo specifico collegamento della risorsa. Una tabella delle rotte all'interno del gateway di transito consente IPv4 sia l'operatore che IPv6 CIDRs gli obiettivi. Gli obiettivi sono VPCs le connessioni VPN. Quando colleghi un VPC o crei una connessione VPN verso un gateway di transito, il collegamento viene associato alla tabella di routing predefinita del gateway di transito.

Puoi creare tabelle di routing aggiuntive all'interno del gateway di transito e modificare l'associazione di VPC o VPN in queste tabelle di routing. Tale azione consente la segmentazione della rete. Ad esempio, è possibile VPCs associare lo sviluppo a una tabella di routing e la produzione VPCs a una tabella di routing diversa. Ciò consente di creare reti isolate all'interno di un gateway di transito in modo simile al routing e all'inoltro virtuali (VRFs) nelle reti tradizionali.

I gateway di transito supportano il routing dinamico e statico tra connessioni collegate e VPN. VPCs Per ogni collegamento puoi abilitare o disabilitare la propagazione delle route. Gli allegati VPN Concentrator supportano solo il routing BGP (dinamico). Gli allegati di peering del gateway di transito supportano solo il routing statico. È possibile indirizzare i percorsi nelle tabelle di routing dei gateway di transito all'allegato di peering per instradare il traffico tra i gateway di transito peer.

Facoltativamente, puoi associare uno IPv4 o più blocchi IPv6 CIDR al tuo gateway di transito. Specifica un indirizzo IP dal blocco CIDR quando stabilisci un peer di Transit Gateway Connect per un collegamento Connect del gateway di transito. Puoi associare qualsiasi intervallo di indirizzi IP pubblici o privati, ad eccezione degli indirizzi nell'intervallo `169.254.0.0/16` e gli intervalli che si sovrappongono agli indirizzi per gli allegati VPC e le reti locali. Per ulteriori informazioni sui IPv4 blocchi IPv6 CIDR, consulta l'indirizzo IP nella Amazon VPC User Guide.

Processi

- Crea un gateway di transito in AWS Transit Gateway
- Visualizza le informazioni sul gateway di transito in AWS Transit Gateway
- Gestisci i tag del gateway di AWS transito in Transit Gateway

- Modifica un gateway di transito in AWS Transit Gateway
- Accetta una condivisione di risorse AWS Transit Gateway utilizzando la AWS Resource Access Manager console
- Accetta un allegato condiviso in AWS Transit Gateway
- Eliminare un gateway di transito in AWS Transit Gateway
- Supporto alla crittografia per AWS Transit Gateway

Crea un gateway di transito in AWS Transit Gateway

Quando crei un gateway di transito, viene creata una tabella di routing predefinita per il gateway di transito e questa viene utilizzata come tabella di routing predefinita per le associazioni nonché come tabella di routing predefinita per la propagazione. Se scegli di non creare la tabella di routing del gateway di transito predefinita, è possibile crearne una in un secondo momento. Per ulteriori informazioni sui routing e sulle tabelle di routing, consulta ???.

> **Note**
>
> Se desideri abilitare il supporto per la crittografia su un gateway di transito, non puoi abilitarlo durante la creazione del gateway. Dopo aver creato il gateway di transito ed averlo raggiunto nello stato disponibile, puoi modificarlo per abilitare il supporto per la crittografia. Per ulteriori informazioni, consulta the section called “Supporto per la crittografia”.

Per creare un gateway di transito utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateways (Gateway di transito).
3. Selezionare Create Transit Gateway (Crea gateway di transito).
4. Per Tag nome, è possibile inserire un nome per il gateway di transito. Un tag nome può semplificare l'identificazione di uno specifico gateway nell'elenco dei gateway. Quando aggiungi un Name tag (Tag nome), viene creato un tag con chiave Name e il valore corrispondente a quello inserito.
5. In Description (Descrizione), immettere una descrizione facoltativa per il gateway di transito.
6. In Amazon side Autonomous System Numbr (ASN lato Amazon), non modificare il valore predefinito per utilizzare l'Autonomous System Number (ASN) predefinito, oppure inserire l'ASN

privato del gateway di transito. Dovrebbe essere l'ASN per il AWS lato di una sessione BGP (Border Gateway Protocol).

L'intervallo è compreso tra 64512 e 65534 per 16 bit. ASNs

L'intervallo è compreso tra 4200000000 e 4294967294 per 32 bit. ASNs

Se si dispone di una distribuzione tra regioni, si consiglia di utilizzare un ASN univoco per ognuno dei propri gateway di transito.

7. Per il supporto DNS, seleziona questa opzione se hai bisogno che il VPC risolva i nomi host DNS IPv4 pubblici in indirizzi IPv4 privati quando vengono richiesti da istanze in un altro VPC collegato al gateway di transito.
8. Per il supporto Security Group Referencing, abilita questa funzionalità per fare riferimento a un gruppo di sicurezza collegato a un gateway di transito. VPCs Per ulteriori informazioni sui riferimenti ai gruppi di sicurezza, vedere. the section called “Riferimenti dei gruppi di sicurezza”
9. In supporto VPN ECMP, selezionare abilita se è necessario disporre del supporto per l'instradamento Equal Cost Multipath (ECMP) tra i tunnel VPN. Se le connessioni pubblicizzano lo stesso messaggio CIDRs, il traffico viene distribuito equamente tra di loro.

   Quando si seleziona questa opzione, l'ASN BGP pubblicizzato e gli attributi BGP come AS-Path devono essere gli stessi.

   > **Note**
   >
   > Per utilizzare ECMP, è necessario creare una connessione VPN che utilizzi il routing dinamico. Le connessioni VPN che utilizzano il routing statico non supportano ECMP.

10. In Default route table association (Associazione tabella di routing predefinita), selezionare abilita per associare automaticamente gli allegati del gateway di transito alla tabella di routing predefinita per il gateway di transito.
11. In Default route table propagation (Propagazione tabella di routing predefinita), selezionare abilita per propagare automaticamente gli allegati del gateway di transito alla tabella di routing predefinita per il gateway di transito.
12. (Facoltativo) Per utilizzare il gateway di transito come router per il traffico multicast, selezionare Multicast support (Supporto multicast).

13. (Facoltativo) Nella sezione delle opzioni di Configure-cross-account condivisione, scegli se accettare automaticamente gli allegati condivisi. Se abilitato, gli allegati vengono accettati automaticamente. Altrimenti, è necessario accettare o rifiutare le richieste di allegati.

    In Auto accept shared attachments (Accetta automaticamente i collegamenti condivisi), selezionare abilita per accettare automaticamente i collegamenti multi-account.

14. (Facoltativo) Per i blocchi CIDR del gateway di transito, specifica uno IPv4 o più blocchi IPv6 CIDR per il gateway di transito.

    È possibile specificare un blocco CIDR di dimensione /24 o superiore (ad esempio, /23 o /22) per IPv4, oppure un blocco CIDR di dimensione /64 o superiore (ad esempio, /63 o /62) per. IPv6 Puoi quindi associare qualsiasi intervallo di indirizzi IP pubblici o privati, ad eccezione degli indirizzi nell'intervallo 169.254.0.0/16, e gli intervalli che si sovrappongono agli indirizzi degli allegati VPC e delle reti locali.

    > **Note**
    >
    > I blocchi CIDR del gateway di transito vengono utilizzati se si configurano gli allegati Connect (GRE) o PrivateIP. VPNs Transit Gateway assegna IPs gli endpoint Tunnel (GRE/PrivateIP VPN) da questo intervallo.

15. Selezionare Create Transit Gateway (Crea gateway di transito).

Per creare un gateway di transito utilizzando il AWS CLI

Utilizza il comando create-transit-gateway.

Visualizza le informazioni sul gateway di transito in AWS Transit Gateway

Visualizza tutti i tuoi gateway di transito.

Per visualizzare un gateway di transito utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateways (Gateway di transito). I dettagli del gateway di transito vengono visualizzati sotto l'elenco dei gateway della pagina.

Per visualizzare un gateway di transito utilizzando il AWS CLI

Utilizza il comando describe-transit-gateways.

Gestisci i tag del gateway di AWS transito in Transit Gateway

Aggiungi tag alle risorse per aiutarti a organizzarle e identificarle, differenziandole ad esempio per scopo, proprietario o ambiente. È possibile aggiungere più tag a ogni gateway di transito. Le chiavi di tag devono essere univoche per ogni gateway di transito. Se aggiungi un tag con una chiave già associata al gateway di transito, il valore del tag viene aggiornato. Per ulteriori informazioni, consulta Tagging your Amazon EC2 Resources.

Aggiungere tag a un gateway di transito utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateways (Gateway di transito).
3. Scegli il gateway di transito per il quale desideri aggiungere o modificare i tag.
4. Selezionare la scheda Tags (Tag) nella parte inferiore della pagina.
5. Scegliere Gestisci tag.
6. Scegliere Aggiungi nuovo tag.
7. Digitare una Key (Chiave) e un Value (Valore) per il tag.
8. Scegli Save (Salva).

Modifica un gateway di transito in AWS Transit Gateway

È possibile modificare le opzioni di configurazione per un gateway di transito. Quando si modifica un gateway di transito, gli eventuali allegati del gateway di transito esistenti non subiscono interruzioni del servizio.

Non è possibile modificare un gateway di transito condiviso con l'utente.

Non puoi rimuovere un blocco CIDR per il gateway di transito se uno qualsiasi degli indirizzi IP è correntemente utilizzato per un peer Connect.

> **Note**
>
> È necessario abilitare l'Encryption Support su un Transit Gateway in modo esplicito per crittografare il traffico tra utenti VPCs che hanno i controlli di crittografia attivati.

Il traffico tra due persone VPCs in modalità enforce (senza esclusioni) viene end-to-end crittografato tramite il TGW. Encryption on Transit Gateway consente inoltre di connetterne due VPCs che si trovano in diverse modalità di Encryption Controls. È garantito che il traffico tra VPCs (uno in modalità enforce e l'altro in modalità Monitor o OFF) venga crittografato solo tra il VPC in esecuzione in modalità enforce, fino al Transit Gateway. Inoltre, dipende dalla risorsa in esecuzione nel VPC non applicato e non è garantito che venga crittografata tra il Transit Gateway e il VPC non applicato.
Per informazioni più dettagliate, consulta the section called “Supporto per la crittografia”.

Come modificare un gateway di transito

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateways (Gateway di transito).
3. Scegliere il gateway di transito da modificare.
4. Scegliere Azioni, Modifica gateway di transito.
5. Modificare le opzioni in base alle esigenze e scegliere Modifica gateway di transito.

Per modificare il gateway di transito utilizzando il AWS CLI

Utilizza il comando modify-transit-gateway.

Accetta una condivisione di risorse AWS Transit Gateway utilizzando la AWS Resource Access Manager console

Se sei stato aggiunto a una condivisione di risorse, riceverai un invito a partecipare alla condivisione stessa. È necessario accettare la condivisione delle risorse tramite la console AWS Resource Access Manager (AWS RAM) prima di poter accedere alle risorse condivise.

Per accettare una condivisione di risorse

1. Apri la AWS RAM console all'indirizzo https://console.aws.amazon.com/ram/.
2. Nel riquadro di navigazione, scegliere Shared with me (Condivise con me), Resource shares (Condivisioni di risorse).
3. Selezionare la condivisione di risorse.
4. Selezionare Accept resource share (Accetta condivisione di risorse).

5. Per visualizzare il gateway di transito condiviso, apri la pagina Gateway di transito nella console Amazon VPC.

Accetta un allegato condiviso in AWS Transit Gateway

Se non hai abilitato la funzionalità di accettazione automatica degli allegati condivisi quando hai creato il gateway di transito, devi accettare manualmente gli allegati tra account (condivisi) utilizzando la console Amazon VPC o la CLI. AWS

Per accettare manualmente un allegato condiviso

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Collegamenti del gateway di transito).
3. Selezionare l'allegato del gateway di transito in attesa di accettazione.
4. Scegli Actions (Operazioni), Accept transit gateway attachment (Accetta il collegamento del gateway di transito alla VPN).

Per accettare un allegato condiviso utilizzando AWS CLI

Utilizzare il comando accept-transit-gateway-vpc-attachment.

Eliminare un gateway di transito in AWS Transit Gateway

Non è possibile eliminare un gateway di transito con allegati esistenti. Prima di poter eliminare un gateway di transito è necessario eliminare tutti i collegamenti.

Per eliminare un gateway di transito utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Scegliere il gateway di transito da eliminare.
3. Scegliere Azioni, Eliminare il gateway di transito. Immettere **`delete`** e quindi scegliere Delete (Elimina) per confermare l'eliminazione.

Per eliminare un gateway di transito utilizzando il AWS CLI

Utilizza il comando delete-transit-gateway.

Supporto alla crittografia per AWS Transit Gateway

L'Encryption Support on Transit Gateway consente encryption-in-transit di applicare tutto il traffico VPCs collegato al Transit Gateway. Quando il supporto per la crittografia è abilitato sul TGW, il traffico del gateway di transito verrà crittografato tra coloro VPCs che sono in modalità Enforce. Traffico verso il quale non sono attivati i controlli di crittografia o VPCs che è in modalità Monitor, TGW ha la garanzia di crittografare il traffico fino all'allegato TGW nel VPC. Inoltre, dipende dall'istanza a cui viene inviato il traffico nel VPC.

Supporto per la crittografia Transit Gateway e controllo della crittografia VPC

Encryption Controls consente di verificare lo stato di crittografia dei flussi di traffico nel VPC e quindi applicarlo encryption-in-transit per tutto il traffico sul VPC. Quando verrà applicato VPC EC, tutte le Elastic Network Interface (ENI) in quel VPC potranno collegarsi solo alle istanze con funzionalità di crittografia AWS Nitro; e solo i AWS servizi che crittografano i dati in transito potranno collegarsi al VPC applicato dalla CE.

Per supportare la crittografia end-to-end dei dati VPCs tramite il TGW, anche il gateway di transito collegato al VPC deve avere abilitato l'Encryption Support. Transit gateway offre la possibilità di abilitare le encryption-in-transit funzionalità utilizzando istanze con funzionalità di crittografia AWS Nitro.

Puoi aggiungere il supporto per la crittografia solo a un gateway di transito esistente e non durante la creazione di uno. Man mano che il TGW passerà a Encryption Support Enabled, non ci saranno tempi di inattività sul TGW o sugli allegati. La migrazione è semplice e trasparente senza interruzioni di traffico. Per i passaggi per modificare un gateway di transito per aggiungere Encryption Support, vedereModificare un gateway di transito.

Requisiti

Prima di abilitare il supporto per la crittografia su un gateway di transito, assicuratevi che:

- Tutti i VPCs dispositivi collegati al gateway di transito devono essere in modalità di monitoraggio
- Il gateway di transito non dispone di allegati Connect
- Il gateway di transito non dispone di allegati Peering
- Il gateway di transito non dispone di allegati Network Firewall
- Il gateway di transito non dispone di allegati VPN Concentrator
- Il gateway di transito non ha i riferimenti ai gruppi di sicurezza abilitati

- Il gateway di transito non ha le funzionalità Multicast abilitate

> **Note**
>
> È possibile abilitare Encryption Support su un Transit Gateway per crittografare il traffico tra utenti VPCs che hanno i controlli di crittografia attivati (in modalità Monitor o Enforce). Per abilitare la crittografia sugli elementi esistenti TGWs VPCs collegati, è necessario abilitare i controlli di crittografia VPC in modalità Monitor in tutti gli ambienti associati VPCs prima di abilitare Encryption Support sul TGW. Una volta abilitato TGW Encryption Support, è possibile modificare la conformità VPCs in modalità Enforce. I dispositivi non connessi VPCs che sono in modalità Enforce possono essere collegati tramite un nuovo TGW con supporto di crittografia abilitato.

Stati di Encryption Support

Un gateway di transito può avere uno dei seguenti stati di crittografia:

- attivazione: il gateway di transito sta abilitando il supporto per la crittografia. Il completamento di questo processo può richiedere fino a 14 giorni.
- abilitato: il supporto per la crittografia è abilitato sul gateway di transito. È possibile creare allegati VPC con Encryption Control Enforced.
- disabilitazione: il gateway di transito sta disabilitando il supporto per la crittografia.
- disabilitato: il supporto per la crittografia è disabilitato sul gateway di transito.

Regole di collegamento del Transit Gateway

Quando un gateway di transito ha il supporto per la crittografia abilitato, si applicano le seguenti regole per gli allegati:

- Quando lo stato di crittografia del gateway di transito è abilitato o disabilitato, è possibile creare allegati Direct Connect, allegati VPN e allegati VPC non in modalità Encryption Control applicata o applicata.
- Quando lo stato di crittografia del gateway di transito è abilitato, è possibile creare VPC, allegati Direct Connect, allegati VPN e allegati VPC in qualsiasi modalità di Encryption Control.
- Quando lo stato di crittografia del gateway di transito è disabilitato, non è possibile creare nuovi allegati VPC con il controllo di crittografia applicato.

- Gli allegati Connect, gli allegati di peering, i riferimenti ai gruppi di sicurezza e le funzionalità multicast non sono supportati con Encryption Support.

Il tentativo di creare allegati incompatibili fallirà e verrà generato un errore API.

Allegati Amazon VPC in Transit Gateway AWS

Un allegato Amazon Virtual Private Cloud (VPC) a un gateway di transito consente di indirizzare il traffico da e verso una o più sottoreti VPC. Quando si collega un VPC a un gateway di transito, è necessario specificare una sottorete di ciascuna zona di disponibilità che deve essere utilizzata dal gateway di transito per instradare il traffico. Le sottoreti specificate fungono da punti di ingresso e uscita per il traffico del gateway di transito. Il traffico può raggiungere le risorse in altre sottoreti all'interno della stessa zona di disponibilità solo se le sottoreti allegate al gateway di transito dispongono di percorsi appropriati configurati nelle tabelle di routing che puntano alle sottoreti di destinazione.

Limits

- Quando si associa un VPC a un gateway di transito, le eventuali risorse nelle zone di disponibilità in cui non vi sia un collegamento con il gateway di transito non possono raggiungere il gateway di transito.

  > **Note**
  >
  > Nelle zone di disponibilità che dispongono di allegati al gateway di transito, il traffico viene inoltrato al gateway di transito solo dalle sottoreti specifiche associate all'allegato. Se è presente un percorso verso il gateway di transito in una tabella di routing di sottorete, il traffico viene inoltrato al gateway di transito solo quando il gateway di transito ha un allegato in una sottorete nella stessa zona di disponibilità e la tabella di routing della subnet allegata contiene percorsi appropriati verso la destinazione prevista del traffico all'interno del VPC.

- Un gateway di transito non supporta la risoluzione DNS per i nomi DNS personalizzati della VPCs configurazione collegata utilizzando zone ospitate private in Amazon Route 53. Per configurare la risoluzione dei nomi per le zone ospitate private per tutte le aree VPCs collegate a un gateway di transito, consulta Gestione DNS centralizzata del cloud ibrido con Amazon Route 53 e AWS Transit Gateway.

- Un gateway di transito non supporta il routing tra file VPCs identici CIDRs o se un CIDR in un intervallo si sovrappone a un CIDR in un VPC collegato. Se colleghi un VPC a un gateway di transito e il relativo CIDR è identico o si sovrappone al CIDR di un altro VPC già collegato al gateway di transito, le route per il VPC appena collegato non vengono propagate nella tabella delle rotte del gateway di transito.
- Non è possibile creare un allegato per una sottorete VPC che risiede in una zona locale. Tuttavia, puoi configurare la rete in modo che le sottoreti nella zona locale possano connettersi a un gateway di transito attraverso la zona di disponibilità padre. Per ulteriori informazioni, vedi Connessione delle sottoreti delle zone locali a un gateway di transito.
- Non è possibile creare un allegato al gateway di transito utilizzando le sottoreti -only. IPv6 Le sottoreti allegate del gateway Transit devono supportare anche gli indirizzi. IPv4
- Un gateway di transito deve avere almeno un allegato VPC prima di poter essere aggiunto a una tabella di routing.

Requisiti della tabella di routing per gli allegati VPC

Gli allegati VPC Transit Gateway richiedono configurazioni specifiche della tabella di percorso per funzionare correttamente:

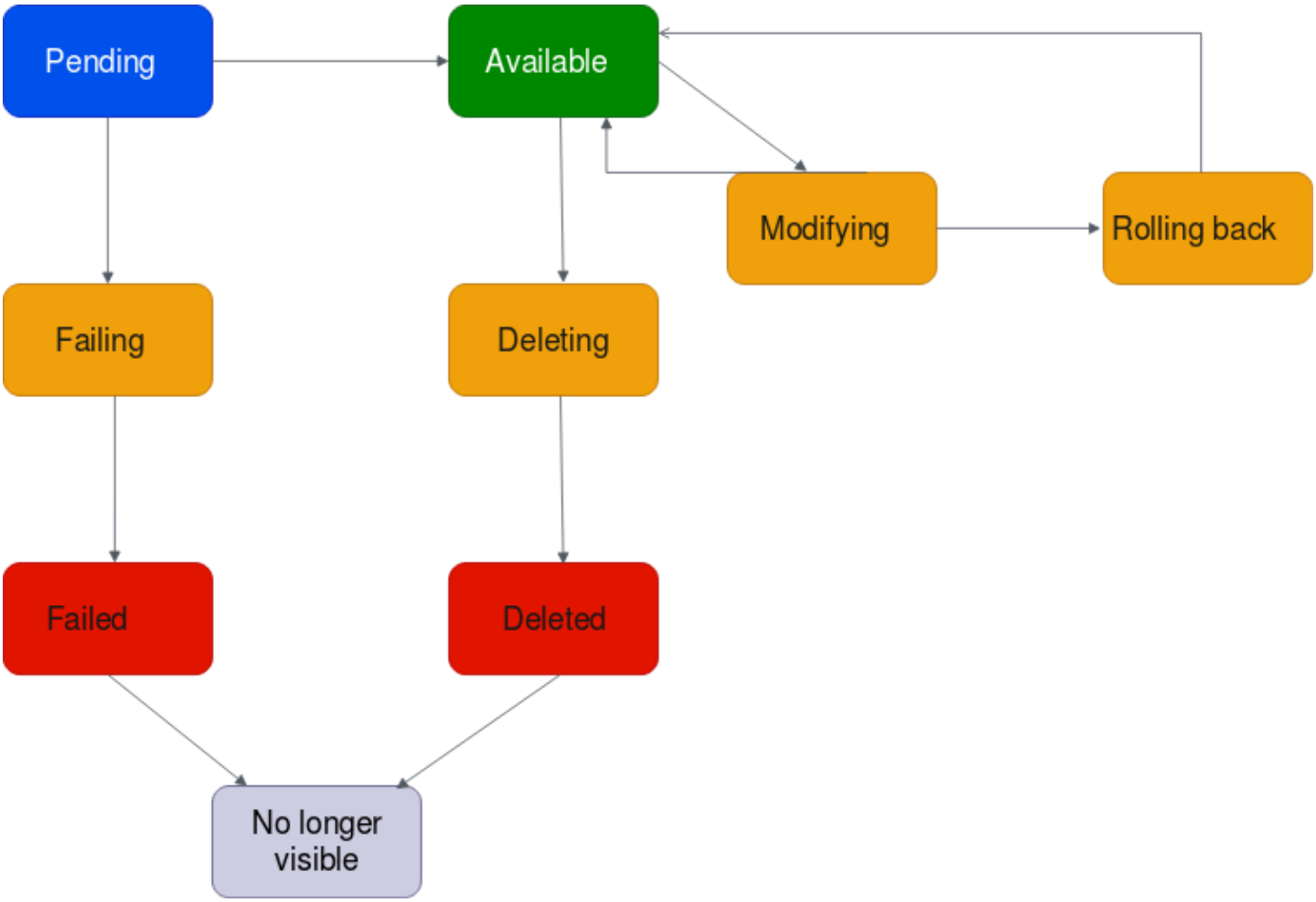
- Tabelle di routing della sottorete degli allegati: le sottoreti associate all'allegato del gateway di transito devono avere voci nella tabella di routing per tutte le destinazioni all'interno del VPC che devono essere raggiungibili tramite il gateway di transito. Ciò include i percorsi verso altre sottoreti, gateway Internet, gateway NAT ed endpoint VPC.
- Tabelle di routing delle sottoreti di destinazione: le sottoreti contenenti risorse che devono comunicare attraverso il gateway di transito devono avere percorsi che rimandano al gateway di transito per il traffico di ritorno verso destinazioni esterne.
- Traffico VPC locale: l'attacco del gateway di transito non abilita automaticamente la comunicazione tra sottoreti all'interno dello stesso VPC. Si applicano le regole di routing VPC standard e la route locale (VPC CIDR) deve essere presente nelle tabelle di routing per la comunicazione intra-VPC.

> **Note**
>
> La configurazione delle rotte in sottoreti non collegate all'interno della stessa zona di disponibilità non abilita il flusso di traffico. Solo le sottoreti specifiche associate all'allegato del gateway di transito possono fungere da entry/exit punti per il traffico del gateway di transito.

Ciclo di vita del collegamento VPC

Un collegamento VPC passa attraverso varie fasi, a partire dal momento in cui viene avviata la richiesta. È possibile che in ogni fase sia necessario eseguire alcune operazioni e che, alla fine del relativo ciclo di vita, il collegamento VPC rimanga visibile nella Amazon Virtual Private Cloud Console e nell'API o nell'output della riga di comando per un determinato periodo di tempo.

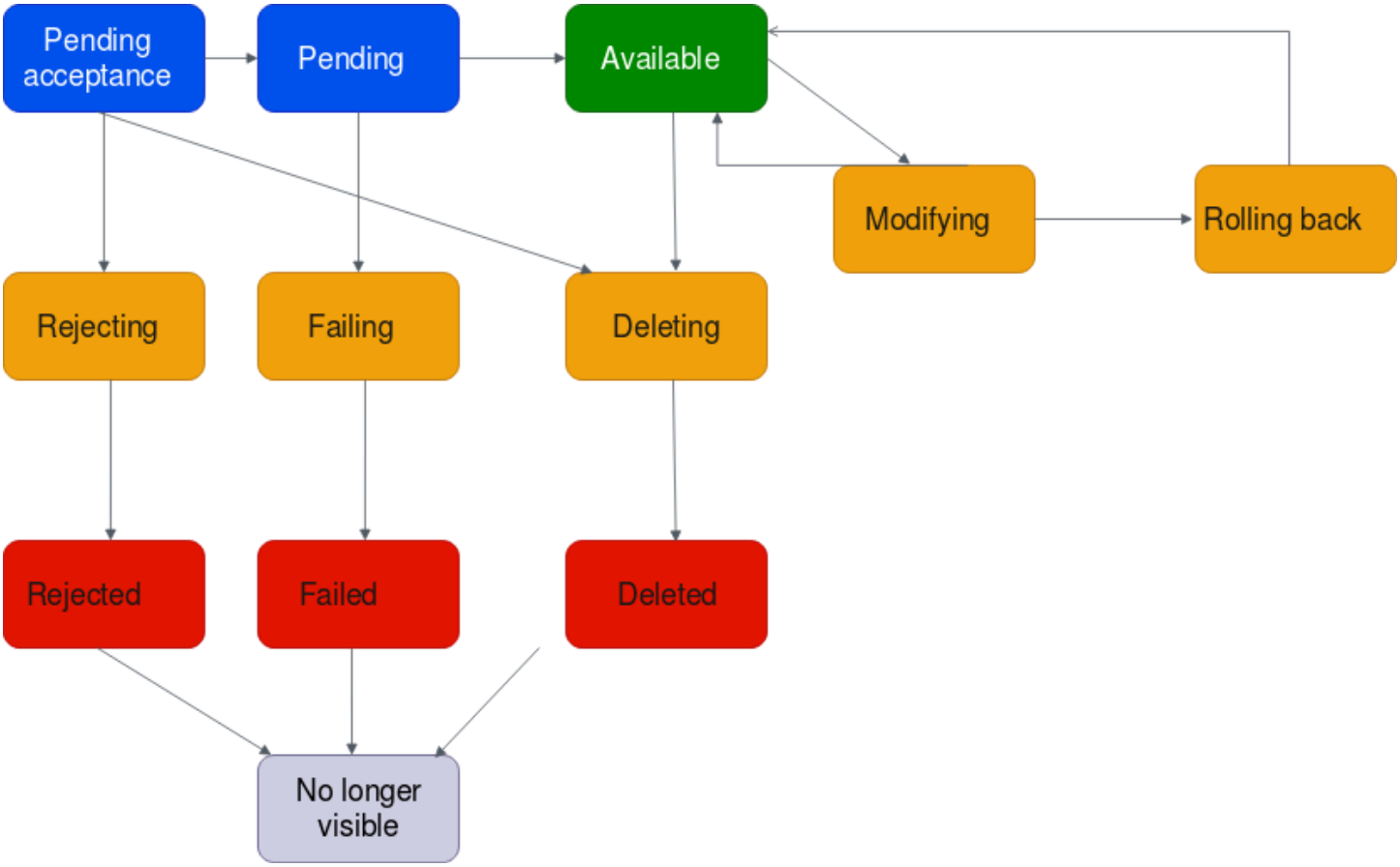
Il diagramma seguente mostra gli stati che un collegamento può avere nella configurazione di un unico account o nella configurazione di più account per cui è attivata l'opzione Accetta automaticamente collegamenti condivisi.



- In sospeso: una richiesta per un collegamento VPC è stata avviata e si trova nel processo di provisioning. In questa fase, il collegamento può non riuscire o passare allo stato `available`.
- Errore: una richiesta per un collegamento VPC ha avuto esito negativo. In questa fase, il collegamento VPC passa allo stato `failed`.

- Non riuscita: la richiesta di collegamento VPC non è riuscita. Mentre si trova in questo stato, non può essere eliminata. Il collegamento VPC non riuscito rimane visibile per 2 ore, dopo di che non è più visibile.
- Disponibile: il collegamento VPC è disponibile e il traffico può fluire tra il VPC e il gateway di transito. In questa fase, il collegamento può passare allo stato `modifying` o allo stato `deleting`.
- Eliminazione: un collegamento VPC che è in fase di eliminazione. In questa fase, il collegamento può passare allo stato `deleted`.
- Eliminato: un collegamento VPC `available` è stato eliminato. In questo stato, il collegamento VPC non può essere modificato. Il collegamento VPC rimane visibile per 2 ore, dopo di che non è più visibile.
- Modifica: è stata effettuata una richiesta di modifica delle proprietà del collegamento VPC. In questa fase, il collegamento può passare allo stato `available` o allo stato `rolling back`.
- Rollback: la richiesta di modifica del collegamento VPC non può essere completata e il sistema sta annullando le modifiche apportate. In questa fase, il collegamento può passare allo stato `available`.

Il diagramma seguente mostra gli stati che un collegamento può avere nella configurazione di più account per cui è attivata l'opzione Accetta automaticamente collegamenti condivisi.



- Pending-acceptance: la richiesta di collegamento VPC è in attesa di essere accettata. In questa fase, il collegamento può passare allo stato `pending`, allo stato `rejecting` o allo stato `deleting`.
- Rifiuto: un collegamento VPC che sta per essere rifiutato. In questa fase, il collegamento può passare allo stato `rejected`.
- Rifiutato: un collegamento VPC `pending acceptance` è stato rifiutato. In questo stato, il collegamento VPC non può essere modificato. Il collegamento VPC rimane visibile per 2 ore, dopo di che non è più visibile.
- In sospeso: un collegamento VPC è stato accettato e si trova nel processo di provisioning. In questa fase, il collegamento può non riuscire o passare allo stato `available`.
- Errore: una richiesta per un collegamento VPC ha avuto esito negativo. In questa fase, il collegamento VPC passa allo stato `failed`.
- Non riuscita: la richiesta di collegamento VPC non è riuscita. Mentre si trova in questo stato, non può essere eliminata. Il collegamento VPC non riuscito rimane visibile per 2 ore, dopo di che non è più visibile.

- Disponibile: il collegamento VPC è disponibile e il traffico può fluire tra il VPC e il gateway di transito. In questa fase, il collegamento può passare allo stato `modifying` o allo stato `deleting`.
- Eliminazione: un collegamento VPC che è in fase di eliminazione. In questa fase, il collegamento può passare allo stato `deleted`.
- Eliminato: un collegamento VPC `available` o `pending acceptance` è stato eliminato. In questo stato, il collegamento VPC non può essere modificato. Il collegamento VPC rimane visibile per 2 ore, dopo di che non è più visibile.
- Modifica: è stata effettuata una richiesta di modifica delle proprietà del collegamento VPC. In questa fase, il collegamento può passare allo stato `available` o allo stato `rolling back`.
- Rollback: la richiesta di modifica del collegamento VPC non può essere completata e il sistema sta annullando le modifiche apportate. In questa fase, il collegamento può passare allo stato `available`.

Modalità Appliance

Se prevedi di configurare un'appliance di rete con stato nel tuo VPC, puoi abilitare il supporto in modalità appliance per l'attacco VPC in cui si trova l'appliance quando crei un allegato. Ciò garantisce che AWS Transit Gateway utilizzi la stessa zona di disponibilità per quell'allegato VPC per tutta la durata del flusso di traffico tra un'origine e una destinazione. Consente inoltre a un gateway di transito di inviare traffico a qualsiasi zona di disponibilità nel VPC purché esista un'associazione di sottoreti in quella zona. Sebbene la modalità appliance sia supportata solo sugli allegati VPC, il flusso di rete può provenire da qualsiasi altro tipo di allegato del gateway di transito, inclusi gli allegati VPC, VPN e Connect. La modalità Appliance funziona anche per i flussi di rete che hanno origini e destinazioni diverse. Regioni AWS I flussi di rete possono potenzialmente essere ribilanciati tra diverse zone di disponibilità se inizialmente non si abilita la modalità appliance ma successivamente si modifica la configurazione degli allegati per abilitarla. È possibile abilitare o disabilitare la modalità appliance utilizzando la console, la riga di comando o l'API.

La modalità Appliance in AWS Transit Gateway ottimizza il routing del traffico considerando le zone di disponibilità di origine e di destinazione quando si determina il percorso attraverso un VPC in modalità appliance. Questo approccio migliora l'efficienza e riduce la latenza. Il comportamento varia in base alla configurazione specifica e ai modelli di traffico. Di seguito sono riportati alcuni scenari di esempio.

Scenario 1: routing del traffico all'interno delle zone di disponibilità tramite VPC dell'appliance

Quando il traffico scorre dalla zona di disponibilità di origine us-east-1a alla zona di disponibilità di destinazione us-east-1a, con allegati VPC in modalità appliance sia in us-east-1a che in us-east-1b, Transit Gateway seleziona un'interfaccia di rete da us-east-1a all'interno del VPC dell'appliance. Questa zona di disponibilità viene mantenuta per l'intera durata del flusso di traffico tra origine e destinazione.

Scenario 2: routing del traffico tra zone di disponibilità tramite VPC dell'appliance

Per il traffico che scorre dalla zona di disponibilità di origine us-east-1a alla zona di disponibilità di destinazione us-east-1b, con allegati VPC in modalità appliance sia in us-east-1a che in us-east-1b, Transit Gateway utilizza un algoritmo di hash di flusso per selezionare us-east-1a o us-east-1b nel VPC dell'appliance. La zona di disponibilità scelta viene utilizzata in modo coerente per tutta la durata del flusso.

Scenario 3: instradamento del traffico attraverso un VPC dell'appliance senza dati sulla zona di disponibilità

Quando il traffico proviene dalla zona di disponibilità di origine us-east-1a verso una destinazione senza informazioni sulla zona di disponibilità (ad esempio, traffico legato a Internet), con allegati VPC in modalità appliance sia in us-east-1a che in us-east-1b, Transit Gateway seleziona un'interfaccia di rete da us-east-1a all'interno del VPC dell'appliance.

Scenario 4: instradamento del traffico attraverso un VPC dell'appliance in una zona di disponibilità distinta dall'origine o dalla destinazione

Quando il traffico scorre dalla zona di disponibilità di origine us-east-1a alla zona di disponibilità di destinazione us-east-1b, con allegati VPC in modalità appliance in diverse zone di disponibilità, ad esempio us-east-1c e us-east-1d, Transit Gateway utilizza un algoritmo di hash di flusso per selezionare us-east-1c o us-east-1d nel VPC dell'appliance. La zona di disponibilità scelta viene utilizzata in modo coerente per tutta la durata del flusso.

> **Note**
>
> La modalità Appliance è supportata solo per gli allegati VPC. Assicurati che la propagazione delle rotte sia abilitata per una tabella di routing associata a un allegato VPC dell'appliance.

Riferimenti dei gruppi di sicurezza

È possibile utilizzare questa funzionalità per semplificare la gestione dei gruppi di sicurezza e il controllo del instance-to-instance traffico tra VPCs quelli collegati allo stesso gateway di transito. È possibile fare riferimenti incrociati ai gruppi di sicurezza solo nelle regole in entrata. Le regole di sicurezza in uscita non supportano i riferimenti ai gruppi di sicurezza. Non sono previsti costi aggiuntivi associati all'attivazione o all'utilizzo dei riferimenti ai gruppi di sicurezza.

Il supporto per i riferimenti ai gruppi di sicurezza può essere configurato sia per i gateway di transito che per gli allegati VPC del gateway di transito e funzionerà solo se è stato abilitato sia per un gateway di transito che per i relativi allegati VPC.

Limitazioni

Le seguenti limitazioni si applicano quando si utilizza il riferimento a gruppi di sicurezza con un allegato VPC.

- Il riferimento ai gruppi di sicurezza non è supportato nelle connessioni peering del gateway di transito. Entrambi VPCs devono essere collegati allo stesso gateway di transito.
- Il riferimento ai gruppi di sicurezza non è supportato per gli allegati VPC nella zona di disponibilità use1-az3.
- Il riferimento ai gruppi di sicurezza non è supportato per gli endpoint. PrivateLink Si consiglia di utilizzare regole di sicurezza basate su IP CIDR come alternativa.
- Il riferimento ai gruppi di sicurezza funziona per Elastic File System (EFS) purché sia configurata una regola del gruppo di sicurezza Allow Output per le interfacce EFS nel VPC.
- Per la connettività alla zona locale tramite un gateway di transito, sono supportate solo le seguenti Local Zone: us-east-1-atl-2a, us-east-1-dfw-2a, us-east-1-iah-2a, us-west-2-lax-1a, us-west-2-lax-1b, us-east-1-mia-2a, us-east-1-chi-2a e us-west-2-phx-2a.
- Ti consigliamo di disabilitare questa funzionalità a livello di collegamento VPC VPCs per le sottoreti in Local Zones, AWS Outposts e AWS Wavelength Zones non supportate, poiché potrebbe causare interruzioni del servizio.
- Se disponi di un VPC di ispezione, il riferimento al gruppo di sicurezza tramite il gateway di transito non funziona tramite Gateway Load AWS Balancer o un Network Firewall. AWS

Processi

- Crea un allegato VPC in AWS Transit Gateway

- Modifica un allegato VPC in AWS Transit Gateway
- Modifica i tag degli allegati VPC in AWS Transit Gateway
- Visualizza un allegato VPC in AWS Transit Gateway
- Eliminare un allegato VPC in AWS Transit Gateway
- Aggiornare le AWS Transit Gateway regole in entrata dei gruppi di sicurezza
- Identifica i AWS Transit Gateway gruppi di sicurezza referenziati
- Rimuovi le regole obsolete AWS Transit Gateway dei gruppi di sicurezza
- Risoluzione dei problemi relativi alla creazione di allegati VPC AWS Transit Gateway

Crea un allegato VPC in AWS Transit Gateway

Per creare un collegamento a un VPC utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Collegamenti del gateway di transito).
3. Selezionare Create transit gateway attachments (Crea collegamenti del gateway di transito).
4. Per Name tag (Tag nome), è possibile inserire un nome per il gateway di transito.
5. Per Transit gateway ID (ID gateway di transito), scegliere il gateway di transito per l'allegato. È possibile scegliere un gateway di transito di cui si è proprietari o un gateway di transito condiviso con l'utente.
6. In Attachment type (Tipo collegamento), selezionare VPC.
7. Scegli se abilitare il supporto DNS Support, IPv6Support e Appliance.

   Se viene scelta la modalità appliance, il flusso di traffico tra un'origine e una destinazione utilizza la stessa zona di disponibilità per l'allegato VPC per tutta la durata di quel flusso.
8. Scegli se abilitare il supporto Security Group Referencing. Abilita questa funzionalità per fare riferimento a un gruppo di sicurezza VPCs collegato a un gateway di transito. Per ulteriori informazioni sui riferimenti ai gruppi di sicurezza, vederethe section called “Riferimenti dei gruppi di sicurezza”.
9. Scegli se abilitare IPv6Support.
10. Per VPC ID (ISD VPC), scegliere il VPC da collegare al gateway di transito.

Questo VPC deve possedere almeno una sottorete associata ad esso.

11. Per Subnet IDs, seleziona una sottorete per ogni zona di disponibilità da utilizzare dal gateway di transito per instradare il traffico. È necessario selezionare almeno una sottorete. È possibile selezionare solo una sottorete per ogni zona di disponibilità.
12. Selezionare Create transit gateway attachments (Crea collegamenti del gateway di transito).

Per creare un allegato VPC utilizzando AWS CLI

Utilizzate il comando create-transit-gateway-vpc-attachment.

Modifica un allegato VPC in AWS Transit Gateway

Per modificare i collegamenti al VPC utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Collegamenti del gateway di transito).
3. Selezionare l'allarme, quindi scegliere Actions (Azioni), Modifica collegamento del gateway di transito.
4. Abilita o disabilita una delle seguenti opzioni:

   - Supporto DNS
   - IPv6 supporto
   - Supporto in modalità appliance
5. Per aggiungere o rimuovere una sottorete dall'allegato, selezionate o deselezionate la casella di controllo accanto all'ID di sottorete che desiderate aggiungere o rimuovere.

   > **Note**
   >
   > L'aggiunta o la modifica di una sottorete di allegati VPC potrebbe influire sul traffico dei dati mentre l'allegato è in uno stato di modifica.
6. Per poter fare riferimento a un gruppo di sicurezza tramite collegamento a un gateway VPCs di transito, seleziona Security Group Referencing support. Per ulteriori informazioni sulla referenziazione dei gruppi di sicurezza, vedere. the section called “Riferimenti dei gruppi di sicurezza”

> **Note**
>
> Se disabiliti il riferimento ai gruppi di sicurezza per un gateway di transito esistente, verrà disabilitato su tutti gli allegati VPC.

7. Scegliere Modifica collegamento del gateway di transito.

Per modificare gli allegati VPC utilizzando il AWS CLI

Usa il comando modify-transit-gateway-vpc-attachment.

Modifica i tag degli allegati VPC in AWS Transit Gateway

Per modificare i tag dei collegamenti al VPC utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Collegamenti del gateway di transito).
3. Selezionare il collegamento VPC, quindi scegliere Actions (Azioni), Manage tags (Gestisci tag).
4. [Aggiunta di un tag] Scegli Aggiungi nuovo tag e procedi come segue:
   - In Chiave, immetti il nome della chiave.
   - In Valore, immetti il valore della chiave.
5. [Rimuovere un tag] Accanto al tag, scegliere Rimuovi.
6. Scegli Save (Salva).

I tag degli allegati VPC possono essere modificati solo utilizzando la console.

Visualizza un allegato VPC in AWS Transit Gateway

Per visualizzare i collegamenti al VPC utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Collegamenti del gateway di transito).
3. Nella colonna Tipo di risorsa, cercaVPC. Questi sono gli allegati del VPC.

4. Selezionare un collegamento per visualizzarne i dettagli.

Per visualizzare gli allegati del VPC utilizzando AWS CLI

Usa il comando describe-transit-gateway-vpc-attachments.

Eliminare un allegato VPC in AWS Transit Gateway

Per eliminare un collegamento a un VPC utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Collegamenti del gateway di transito).
3. Selezionare un collegamento a un VPC.
4. Scegliere Operazioni,Eliminare l'allegato del gateway.
5. Quando richiesto, digitare **`delete`** e scegliere Delete (Elimina).

Per eliminare un allegato VPC utilizzando il AWS CLI

Utilizzare il comando delete-transit-gateway-vpc-attachment.

Aggiornare le AWS Transit Gateway regole in entrata dei gruppi di sicurezza

È possibile aggiornare qualsiasi regola del gruppo di sicurezza in entrata associata a un gateway di transito. Puoi aggiornare le regole dei gruppi di sicurezza utilizzando la console Amazon VPC o utilizzando la riga di comando o l'API. Per ulteriori informazioni sulla referenziazione dei gruppi di sicurezza, consulta. the section called “Riferimenti dei gruppi di sicurezza”

Per aggiornare le regole di gruppo di sicurezza tramite la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Gruppi di sicurezza.
3. Seleziona il gruppo di sicurezza e scegli Azioni, Modifica regole in entrata per modificare le regole in entrata.

4. Per aggiungere una regola, scegli Aggiungi regola e specifica il tipo, il protocollo e l'intervallo di porte. Per Source (regola in entrata), inserisci l'ID del gruppo di sicurezza nel VPC collegato al gateway di transito.

   > **Note**
   >
   > I gruppi di sicurezza in un VPC collegato al gateway di transito non vengono visualizzati automaticamente.

5. Per modificare una regola esistente, cambia i relativi valori (ad esempio, l'origine o la descrizione).
6. Per eliminare una regola, seleziona il pulsante Elimina accanto alla regola corrispondente.
7. Scegliere Salva regole.

Per aggiornare le regole in entrata tramite la riga di comando

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

Identifica i AWS Transit Gateway gruppi di sicurezza referenziati

Per determinare se il tuo gruppo di sicurezza è referenziato nelle regole di un gruppo di sicurezza in un VPC collegato allo stesso gateway di transito, usa uno dei seguenti comandi.

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

Rimuovi le regole obsolete AWS Transit Gateway dei gruppi di sicurezza

Una regola del gruppo di sicurezza obsoleta è una regola che fa riferimento a un gruppo di sicurezza eliminato nello stesso VPC o in VPC collegato allo stesso gateway di transito. Quando una regola di gruppo di sicurezza diventa obsoleta, non viene automaticamente rimossa dal gruppo di sicurezza, ma deve essere eliminata manualmente.

Puoi visualizzare ed eliminare le regole di gruppo di sicurezza obsolete per un VPC tramite la console Amazon VPC.

Per visualizzare Ed eliminare regole di gruppo di sicurezza obsolete

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Fare clic su Security Groups (Gruppi di sicurezza) nel riquadro di navigazione.
3. Seleziona Actions (Operazioni), Manage stale rules (Gestisci regole obsolete).
4. Per VPC, seleziona il VPC con le regole obsolete.
5. Seleziona Edit (Modifica).
6. Scegliere il pulsante Delete (Elimina) a destra della regola da eliminare. Scegliere Preview changes (Anteprima modifiche), Save rules (Salva regole).

Per descrivere le regole obsolete del gruppo di sicurezza utilizzando la riga di comando

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

Dopo aver identificato le regole obsolete del gruppo di sicurezza, potete eliminarle utilizzando i comandi revoke-security-group-ingresso revoke-security-group-egress.

Risoluzione dei problemi relativi alla creazione di allegati VPC AWS Transit Gateway

Nel seguente argomento viene descritto come risolvere i problemi che si possono verificare quando si crea un collegamento VPC.

Problema

Il collegamento VPC non è riuscito.

Causa

Di seguito è riportata la possibile causa:

1. L'utente che sta creando il collegamento VPC non dispone delle autorizzazioni corrette per creare un ruolo collegato al servizio.

2. C'è un problema di limitazione a causa delle troppe richieste IAM, ad esempio si utilizza CloudFormation per creare autorizzazioni e ruoli.
3. L'account è dotato del ruolo collegato al servizio e il ruolo collegato al servizio è stato modificato.
4. Il gateway di transito non è nello stato `available`.

Soluzione

A seconda della causa, provare quanto segue:

1. Verificare che l'utente disponga delle autorizzazioni corrette per creare ruoli collegati ai servizi. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM. Dopo che l'utente riceve le autorizzazioni, creare il collegamento VPC.
2. Crea l'allegato VPC manualmente. Per ulteriori informazioni, consulta the section called “Creare un allegato VPC”.
3. Verificare che il ruolo collegato al servizio disponga delle autorizzazioni corrette. Per ulteriori informazioni, consulta the section called “Gateway di transito”.
4. Verificare che il gateway di transito sia nello stato `available`. Per ulteriori informazioni, consulta the section called “Visualizza un gateway di transito”.

AWS Allegati alle funzioni di rete Transit Gateway

È possibile creare un collegamento a una funzione di rete a cui connettere direttamente il gateway di transito AWS Network Firewall. In questo modo si elimina la necessità di creare e gestire le ispezioni VPCs.

Con un attacco firewall, AWS fornisce e gestisce automaticamente tutte le risorse necessarie dietro le quinte. Vedrai un nuovo allegato del gateway di transito anziché singoli endpoint del firewall. Ciò semplifica il processo di implementazione dell'ispezione centralizzata del traffico di rete.

Prima di poter utilizzare un allegato del firewall, è necessario crearlo in. AWS Network Firewall Per la procedura di creazione dell'allegato, consulta Guida introduttiva alla AWS Network Firewall gestione nella Guida per gli AWS Network Firewall sviluppatori Dopo la creazione del firewall, è possibile visualizzare l'allegato nella console Transit Gateway nella sezione Allegati. L'allegato verrà elencato con un tipo di funzione di rete.

Argomenti

- Accettare o rifiutare un collegamento alla funzione di rete AWS Transit Gateway
- Visualizza gli allegati delle funzioni di rete AWS Transit Gateway
- Indirizza il traffico attraverso un collegamento alla funzione di rete AWS Transit Gateway

Accettare o rifiutare un collegamento alla funzione di rete AWS Transit Gateway

Puoi utilizzare la console Amazon VPC o la AWS Network Firewall CLI o l'API per accettare o rifiutare un allegato alla funzione di rete del gateway di transito, inclusi gli allegati Network Firewall. Se sei il proprietario di un gateway di transito e qualcuno ha creato un allegato firewall al tuo gateway di transito da un altro account, devi accettare o rifiutare la richiesta di allegato.

Per accettare o rifiutare un collegamento a una funzione di rete utilizzando la CLI Network Firewall, consulta `RejectNetworkFirewallTransitGatewayAttachment` APIs o `AcceptNetworkFirewallTransitGatewayAttachment` AWS Network Firewall nel riferimento API.

Accetta o rifiuta un allegato a una funzione di rete utilizzando la console

Utilizza la console Amazon VPC per accettare o rifiutare un collegamento alla funzione di rete Transit Gateway.

Per accettare o rifiutare un collegamento a una funzione di rete utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli Transit Gateways.
3. Scegli gli allegati del gateway Transit.
4. Seleziona l'allegato con lo stato In attesa di accettazione e un tipo di funzione di rete.
5. Scegliete Azioni, quindi scegliete Accetta allegato o Rifiuta allegato.
6. Nella finestra di dialogo di conferma, scegliete Accetta o Rifiuta.

Se accettate l'allegato, questo diventa attivo e il firewall può ispezionare il traffico. Se si rifiuta l'allegato, questo passa allo stato di rifiuto e alla fine verrà eliminato.

Visualizza gli allegati delle funzioni di rete AWS Transit Gateway

Puoi visualizzare gli allegati delle funzioni di rete, inclusi AWS Network Firewall gli allegati, utilizzando la console Amazon VPC o la console Network Manager per ottenere una rappresentazione visiva della topologia di rete.

Visualizza un allegato a una funzione di rete utilizzando la console Network Manager

È possibile visualizzare gli allegati di una funzione di rete utilizzando la console Network Manager.

Per visualizzare gli allegati del firewall in Network Manager

1. Apri la console di Network Manager a https://console.aws.amazon.com/networkmanager/casa/.
2. Crea una rete globale in Network Manager se non ne hai già una.
3. Registra il tuo gateway di transito con Network Manager.
4. In Global Networks, scegli la rete globale in cui si trova l'allegato.
5. Nel riquadro di navigazione selezionare Transit gateways (Gateway di transito).
6. Scegliete il gateway di transito per il quale desiderate visualizzare gli allegati.
7. Scegliete la visualizzazione ad albero della topologia. Gli allegati del Network Firewall vengono visualizzati con l'icona di una funzione di rete.
8. Per visualizzare i dettagli su uno specifico allegato del firewall, seleziona il gateway di transito nella visualizzazione topologica, quindi seleziona la scheda Funzione di rete.

La console Network Manager fornisce informazioni dettagliate sugli allegati del firewall, tra cui lo stato, il gateway di transito associato e le zone di disponibilità.

Visualizza un collegamento a una funzione di rete utilizzando la console Amazon VPC Console

Utilizza la console VPC per visualizzare un elenco dei tipi di allegati del gateway di transito.

Per visualizzare i tipi di allegati del gateway di transito utilizzando la console VPC

- Consultare Visualizza un allegato VPC.

Indirizza il traffico attraverso un collegamento alla funzione di rete AWS Transit Gateway

Dopo aver creato un allegato alla funzione di rete, devi aggiornare le tabelle di routing del gateway di transito per inviare il traffico attraverso il firewall per l'ispezione utilizzando la console Amazon VPC o utilizzando la CLI. Per i passaggi per aggiornare un'associazione di tabelle di routing del gateway di transito, consulta. Associare una tabella di instradamento di un gateway di transito.

Indirizza il traffico attraverso un allegato del firewall utilizzando la console

Usa la console Amazon VPC per instradare il traffico attraverso un collegamento alla funzione di rete Transit Gateway.

Per indirizzare il traffico attraverso un collegamento alla funzione di rete utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli Transit Gateways.
3. Scegli le tabelle degli itinerari del gateway Transit.
4. Seleziona la tabella delle rotte che desideri modificare.
5. Scegli Azioni, quindi scegli Crea percorso statico.
6. Per CIDR, inserisci il blocco CIDR di destinazione per il percorso.
7. Per Allegato, selezionare l'allegato alla funzione di rete. Ad esempio, potrebbe trattarsi di un AWS Network Firewall allegato.
8. Scegliere Create static route (Crea route statico).

> **Note**
>
> Sono supportate solo le route statiche.

Il traffico corrispondente al blocco CIDR nella tabella delle rotte verrà ora inviato all'allegato del firewall per l'ispezione prima di essere inoltrato alla destinazione finale.

Indirizza il traffico attraverso un allegato di funzione di rete utilizzando la CLI o l'API

Utilizza la riga di comando o l'API per indirizzare un allegato alla funzione di rete Transit Gateway.

Per indirizzare il traffico attraverso un allegato di funzione di rete utilizzando la riga di comando o l'API

- Utilizza `create-transit-gateway-route`.

  Ad esempio, la richiesta potrebbe riguardare il routing di un allegato del firewall di rete:

```
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
```

  L'output restituisce quindi:

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

Il traffico corrispondente al blocco CIDR nella tabella delle rotte verrà ora inviato all'allegato del firewall per l'ispezione prima di essere inoltrato alla destinazione finale.

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

Puoi connettere un allegato Site-to-Site VPN a un gateway di transito in AWS Transit Gateway, consentendoti di connettere le tue reti VPCs e quelle locali. Sono supportate sia le route dinamiche che quelle statiche, così come IPv4 e IPv6.

Requisiti

- Per collegare una connessione VPN al gateway di transito è necessario specificare il gateway VPN per il cliente, che ha requisiti specifici per i dispositivi. Prima di creare un allegato Site-to-Site VPN, esamina i requisiti del gateway del cliente per assicurarti che il gateway sia configurato correttamente. Per ulteriori informazioni su questi requisiti, inclusi esempi di file di configurazione del gateway, consulta Requisiti per il dispositivo gateway Site-to-Site VPN per il cliente nella Guida per l'AWS Site-to-Site VPN utente.
- Per quanto riguarda le rotte statiche VPNs, è inoltre necessario aggiungere prima le rotte statiche alla tabella delle rotte del gateway di transito. Le rotte statiche in una tabella di routing del gateway di transito che hanno come destinazione un allegato VPN non vengono filtrate dalla Site-to-Site VPN in quanto ciò potrebbe consentire un flusso di traffico in uscita involontario quando si utilizza una VPN basata su BGP. Per i passaggi per aggiungere una route statica a una tabella di routing del gateway di transito, consulta. Creare una route statica

Puoi creare, visualizzare o eliminare un allegato Site-to-Site VPN del gateway di transito utilizzando la console Amazon VPC o l'interfaccia a riga di comando AWS .

Attività

- Crea un collegamento gateway di transito a una VPN in AWS Transit Gateway
- Visualizza un allegato VPN in AWS Transit Gateway
- Eliminare un allegato VPN in AWS Transit Gateway

Crea un collegamento gateway di transito a una VPN in AWS Transit Gateway

Per creare un collegamento a una VPN utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Collegamenti del gateway di transito).
3. Selezionare Create Transit Gateway Attachments (Crea collegamenti del gateway di transito).
4. Per Transit gateway ID (ID gateway di transito), scegliere il gateway di transito per l'allegato. È possibile scegliere un gateway di transito che possiedi.
5. In Attachment type (Tipo collegamento), selezionare VPN.
6. In Customer Gateway (Gateway del cliente), eseguire una delle seguenti operazioni:

- Per utilizzare un gateway del cliente esistente selezionare Existing (Esistente) e quindi selezionare il gateway da utilizzare.

  Se il gateway del cliente si trova dietro un dispositivo NAT abilitato per NAT Traversal (NAT-T), utilizzare l'indirizzo IP pubblico del dispositivo NAT e modificare le regole del firewall per sbloccare la porta UDP 4500.
- Per creare un gateway del cliente, selezionare New (Nuovo), quindi in IP Address (Indirizzo IP), inserire un indirizzo IP pubblico statico e il BGP ASN (ASN BGP).

  In Routing options (Opzioni di routing), selezionare se utilizzare la modalità Dynamic (Dinamica) o Static (Statica). Per ulteriori informazioni, consulta Opzioni di routing Site-to-Site VPN nella Guida per l'AWS Site-to-Site VPN utente.

7. In Tunnel Options (Opzioni tunnel), specifica gli intervalli CIDR e le chiavi pre-condivise per il tuo tunnel. Per ulteriori informazioni, consulta Architetture Site-to-Site VPN.
8. Selezionare Create Transit Gateway Attachments (Crea collegamenti del gateway di transito).

Per creare un allegato VPN utilizzando il AWS CLI

Utilizza il comando create-vpn-connection.

Visualizza un allegato VPN in AWS Transit Gateway

Per visualizzare i collegamenti alla VPN utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Collegamenti del gateway di transito).
3. Nella colonna Tipo di risorsa, cercaVPN. Questi sono gli allegati VPN.
4. Selezionare un collegamento per visualizzarne i dettagli o aggiungere tag.

Per visualizzare gli allegati VPN utilizzando il AWS CLI

Utilizza il comando describe-transit-gateway-attachments.

Eliminare un allegato VPN in AWS Transit Gateway

Per eliminare un collegamento a una VPN utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Collegamenti del gateway di transito).
3. Selezionare un collegamento a una VPN.
4. Selezionare la risorsa ID della connessione VPN per raggiungere la pagina VPN Connections (Connessioni VPN).
5. Selezionare Actions (Operazioni), Delete (Elimina).
6. Quando viene richiesta la conferma, selezionare Delete (Elimina).

Per eliminare un allegato VPN utilizzando il AWS CLI

Utilizza il comando delete-vpn-connection.

Allegati VPN Concentrator in AWS Transit Gateway

AWS Site-to-Site VPN Concentrator è una nuova funzionalità che semplifica la connettività multisito per le imprese distribuite. VPN Concentrator è adatto ai clienti che devono connettere più di 25 siti remoti AWS, ognuno dei quali necessita di una larghezza di banda ridotta (meno di 100 Mbps).

Come funziona VPN Concentrator

Un VPN Concentrator appare come un singolo allegato sul gateway di transito, ma può ospitare più Site-to-Site connessioni VPN.

Il traffico proveniente da tutte le connessioni VPN sul Concentrator viene instradato attraverso lo stesso allegato del gateway di transito, consentendoti di applicare politiche di routing e regole di sicurezza coerenti su tutti i siti connessi. Il Concentrator si integra perfettamente con le tabelle di routing dei gateway di transito, consentendoti di controllare il flusso di traffico tra i siti remoti e altri allegati VPCs, come altre connessioni VPN e connessioni peering.

Vantaggi di VPN Concentrator

- Ottimizzazione dei costi: riduci i costi consolidando più connessioni VPN a bassa larghezza di banda su un unico collegamento gateway di transito, particolarmente utile quando i singoli siti non richiedono una capacità completa di allegati VPN.
- Gestione semplificata: gestisci più connessioni a siti remoti tramite un allegato unificato mantenendo il controllo e il monitoraggio delle singole connessioni VPN.
- Routing coerente: applica politiche di routing unificate su tutti i siti connessi tramite un'unica associazione di tabelle di routing del gateway di transito.
- Architettura scalabile: Connect fino a 100 siti remoti utilizzando un unico concentratore, con supporto per un massimo di 5 concentratori per gateway di transito.
- Funzionalità VPN standard: ogni connessione VPN supporta le stesse funzionalità di sicurezza, monitoraggio e routing delle connessioni VPN standard. Site-to-Site

Requisiti e limitazioni

- Solo routing BGP: VPN Concentrator supporta solo il routing BGP (dinamico). Il routing statico non è supportato al momento del lancio.
- Requisiti del gateway del cliente: ogni sito remoto richiede un gateway cliente che supporti il routing BGP. Prima di creare connessioni VPN su un Concentrator, consulta i requisiti del gateway del cliente nella sezione Requisiti per il tuo dispositivo gateway clienti Site-to-Site VPN nella Guida per l'utente.AWS Site-to-Site VPN
- Considerazioni sulle prestazioni: ogni connessione VPN su un Concentrator è progettata per una larghezza di banda massima di 100 Mbps. Per requisiti di larghezza di banda più elevati, prendi in considerazione l'utilizzo di allegati VPN per gateway di transito standard.

Puoi creare, visualizzare o eliminare un allegato VPN Concentrator utilizzando la console AWS VPC o la CLI AWS . Le singole connessioni VPN sul Concentrator sono gestite tramite la connessione APIs VPN standard e le interfacce della console.

Processi

- Crea un allegato VPN Concentrator in AWS Transit Gateway
- Visualizza un allegato VPN Concentrator in AWS Transit Gateway
- Eliminare un allegato VPN Concentrator in AWS Transit Gateway

Crea un allegato VPN Concentrator in AWS Transit Gateway

Prerequisiti

- È necessario disporre di un gateway di transito esistente nel proprio account.

Per creare un allegato VPN Concentrator utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli Site-to-Site VPN Concentrators.
3. Scegli Create Site-to-Site VPN Concentrator.
4. (Facoltativo) Nel campo Nome, inserisci un nome per il tuo Site-to-Site VPN Concentrator.
5. Per Transit gateway, seleziona un gateway di transito esistente.
6. (Facoltativo) Per aggiungere altri tag, scegliete Aggiungi nuovo tag e specificate la chiave e il valore per ogni tag.
7. Scegli Create Site-to-Site VPN Concentrator.

Dopo aver creato l'allegato VPN Concentrator, questo appare nell'elenco degli allegati con un tipo di risorsa VPN Concentrator e lo stato iniziale di In sospeso. Quando l'allegato è pronto, lo stato diventa Disponibile. È quindi possibile creare connessioni Site-to-Site VPN su questo Concentrator.

Per creare un allegato VPN Concentrator utilizzando il AWS CLI

Utilizza il comando create-vpn-concentrator.

Per creare una connessione VPN su un VPN Concentrator utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli Connessioni Site-to-Site VPN.
3. Scegliere Create VPN Connection (Crea connessione VPN).
4. Per Target Gateway Type, scegli Site-to-Site VPN Concentrator.
5. Per Site-to-Site VPN Concentrator, scegli il VPN Concentrator su cui desideri creare la connessione VPN.
6. In Customer Gateway (Gateway del cliente), eseguire una delle seguenti operazioni:

- Per utilizzare un gateway del cliente esistente selezionare Existing (Esistente) e quindi selezionare il gateway da utilizzare. Assicurati che il gateway del cliente supporti il routing BGP.
- Per creare un gateway del cliente, scegliere New (Nuovo). Per Indirizzo IP, inserisci l'indirizzo IP pubblico statico per il dispositivo gateway del cliente. Per BGP ASN, inserisci il Border Gateway Protocol (BGP) Autonomous System Number (ASN) per il gateway clienti.

  Se il gateway del cliente si trova dietro un dispositivo NAT abilitato per NAT Traversal (NAT-T), utilizzare l'indirizzo IP pubblico del dispositivo NAT e modificare le regole del firewall per sbloccare la porta UDP 4500.

7. Per le opzioni di routing, viene selezionato automaticamente Dynamic (richiede BGP). VPN Concentrator supporta solo il routing dinamico con BGP.
8. Per l'archiviazione delle chiavi già condivise, selezionare Standard o Secrets Manager.
9. Per la larghezza di banda del tunnel, viene selezionato automaticamente Standard. VPN Concentrator supporta solo la larghezza di banda del tunnel standard.
10. Per la versione Tunnel inside IP, seleziona o IPv4. IPv6
11. (Facoltativo) Seleziona Abilita l'accelerazione per migliorare le prestazioni dei tunnel VPN.
12. (Facoltativo) Per il CIDR IPv4 della rete locale, fornisci un IPv4 intervallo CIDR.
13. (Facoltativo) Per il CIDR IPv4 della rete remota, fornisci un IPv4 intervallo CIDR.
14. Per Tipo di indirizzo IP esterno, puoi selezionare Pubblico IPv4 o IPv6Indirizzo.
15. (Facoltativo) Per Tunnel Options, è possibile configurare le impostazioni del tunnel, ad esempio gli indirizzi IP interni del tunnel e le chiavi già condivise. Per ulteriori informazioni, consulta Architetture Site-to-Site VPN nella Guida per l'AWS Site-to-Site VPN utente.
16. (Facoltativo) Per aggiungere altri tag, scegli Aggiungi nuovo tag e specifica la chiave e il valore per ogni tag.
17. Scegliere Create VPN Connection (Crea connessione VPN).

La connessione VPN viene visualizzata nell'elenco delle connessioni VPN con l'ID VPN Concentrator nella colonna Transit Gateway ID e lo stato iniziale di Pending. Quando la connessione VPN è pronta, lo stato diventa Disponibile.

Per creare una connessione VPN su un VPN Concentrator utilizzando il AWS CLI

Usa il create-vpn-connectioncomando e specifica l'ID VPN Concentrator utilizzando il `--vpn-concentrator-id` parametro.

Visualizza un allegato VPN Concentrator in AWS Transit Gateway

Per visualizzare gli allegati di VPN Concentrator utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Collegamenti del gateway di transito).
3. Nella colonna Tipo di risorsa, cerca VPN Concentrator. Questi sono gli allegati di VPN Concentrator.
4. Selezionare un collegamento per visualizzarne i dettagli.

Per visualizzare le connessioni VPN su un VPN Concentrator utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli Connessioni Site-to-Site VPN.
3. Nell'elenco delle connessioni VPN, identifica le connessioni che mostrano un VPN Concentrator ID nella colonna Transit Gateway ID. Queste sono le connessioni VPN ospitate su VPN Concentrators.
4. Scegli una connessione VPN per visualizzarne i dettagli.

Per visualizzare gli allegati di VPN Concentrator, utilizza il AWS CLI

Usa il describe-vpn-concentratorcomando per visualizzare i dettagli di VPN Concentrator o usa il describe-transit-gateway-attachmentscomando con un filtro per il tipo di risorsa. `vpn-concentrator`

Per visualizzare le connessioni VPN su un VPN Concentrator utilizzando il AWS CLI

Utilizza il describe-vpn-connectionscomando con un filtro `vpn-concentrator-id` per visualizzare le connessioni VPN associate a un concentratore specifico.

Eliminare un allegato VPN Concentrator in AWS Transit Gateway

Prerequisiti

- Tutte le connessioni VPN su VPN Concentrator devono essere eliminate prima di poter eliminare l'allegato Concentrator.

- Assicurati di aver aggiornato le configurazioni di routing per tenere conto della rimozione di VPN Concentrator e delle connessioni VPN associate.

Per eliminare le connessioni VPN su un VPN Concentrator utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli Connessioni Site-to-Site VPN.
3. Identifica le connessioni VPN associate al tuo VPN Concentrator cercando l'ID VPN Concentrator nella colonna Transit Gateway ID.
4. Seleziona una connessione VPN che desideri eliminare.
5. Selezionare Actions (Operazioni), Delete (Elimina).
6. Quando viene richiesta la conferma, selezionare Delete (Elimina).
7. Ripeti i passaggi 4-6 per ogni connessione VPN associata a VPN Concentrator.

Per eliminare un allegato VPN Concentrator utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Collegamenti del gateway di transito).
3. Seleziona l'allegato VPN Concentrator che desideri eliminare. Verifica che nessuna connessione VPN sia associata a questo Concentrator.
4. Scegli Azioni, Elimina allegato.
5. Quando viene richiesta la conferma, seleziona Delete (Elimina).

L'allegato VPN Concentrator entra nello stato di Eliminazione e verrà rimosso dal tuo account. Il completamento di questo processo potrebbe richiedere alcuni minuti.

Per eliminare le connessioni VPN su un VPN Concentrator, utilizza il AWS CLI

Utilizza il delete-vpn-connectioncomando per ogni connessione VPN associata a VPN Concentrator.

Per eliminare un allegato VPN Concentrator utilizzando il AWS CLI

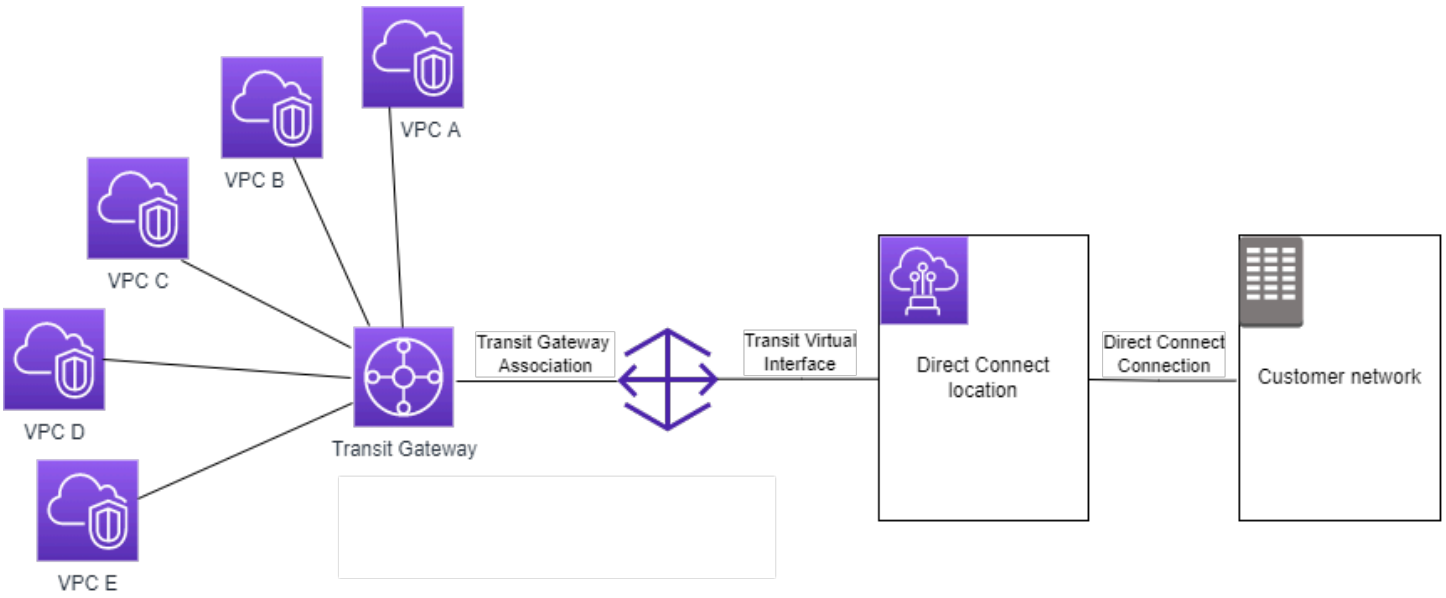
Utilizza il delete-vpn-concentratorcomando dopo che tutte le connessioni VPN sono state eliminate.

Collegamenti del gateway di transito a un gateway Direct Connect in AWS Transit Gateway

Collegare un gateway di transito a un gateway Direct Connect usando un'interfaccia virtuale di transito. Questa configurazione offre i seguenti vantaggi. È possibile:

- Gestisci una singola connessione per più VPCs o VPNs che si trovano nella stessa regione.
- Pubblicizza prefissi da locale a locale AWS e da locale a locale. AWS

Il diagramma seguente illustra come il gateway Direct Connect consente di creare una singola connessione alla connessione Direct Connect VPCs utilizzabile da tutti.



La soluzione prevede i seguenti componenti:

- Un gateway di transito.
- Un gateway Direct Connect.
- Un'associazione tra il gateway Direct Connect e il gateway di transito.
- Un'interfaccia virtuale di transito collegata al gateway Direct Connect.

Per informazioni sulla configurazione dei gateway Direct Connect con gateway di transito, vedere Associazioni gateway di transito nel Manuale per l'utente di AWS Direct Connect .

Allegati di peering del gateway di transito in AWS Transit Gateway

È possibile effettuare il peering dei gateway di transito interregionali e interregionali e instradare il traffico tra di essi, incluso il traffico e il traffico. IPv4 IPv6 A tale scopo, creare un allegato di peering sul gateway di transito e specificare un gateway di transito. Il gateway di transito peer può trovarsi nel tuo account o provenire da un altro account. Puoi anche richiedere un allegato di peering dal tuo account a un gateway di transito di un altro account.

Dopo aver creato una richiesta di allegato di peering, il proprietario del gateway di transito peer (denominato anche gateway di transito accettatore) deve accettare la richiesta. Per instradare il traffico tra i gateway di transito, è necessario aggiungere un route statico alla tabella di routing del gateway di transito che punti all'allegato di peering del gateway di transito.

Ti consigliamo di utilizzare unique ASNs per ogni gateway di transito peer-to-peer per sfruttare le future funzionalità di propagazione delle rotte.

Il peering del gateway di transito non supporta la risoluzione di nomi host IPv4 DNS pubblici o privati in IPv4 indirizzi privati VPCs su entrambi i lati dell'allegato di peering del gateway di transito utilizzando l'allegato di peering del gateway di transito utilizzando l'allegato in un'altra regione. Amazon Route 53 Resolver Per maggiori informazioni sul resolver Route 53, consulta Cos'è un resolver Route 53? nella Guida per gli sviluppatori di Amazon Route 53.

Il peering del gateway tra le regioni utilizza la stessa infrastruttura di rete del peering VPC. Pertanto il traffico viene crittografato utilizzando la crittografia AES-256 a livello di rete virtuale mentre si sposta tra le regioni. Il traffico viene crittografato anche utilizzando la crittografia AES-256 a livello fisico quando attraversa collegamenti di rete che sono al di fuori del controllo fisico di AWS. Di conseguenza, il traffico viene crittografato due volte su collegamenti di rete al di fuori del controllo fisico di. AWS Nella stessa regione, il traffico viene crittografato a livello fisico solo quando attraversa collegamenti di rete che sono al di fuori del controllo fisico di AWS.

Per informazioni sulle regioni che supportano gli allegati di peering del gateway di transito, consulta AWS Transit Gateways. FAQs

Considerazioni relative alla regione di opt-in AWS

Puoi eseguire il peering dei gateway di transito attraverso i confini della regione di attivazione. Per informazioni su queste regioni e su come aderire, consulta Gestione delle AWS regioni. Se utilizzi il peering del gateway di transito in queste regioni, tieni in considerazione quanto segue:

- Puoi eseguire il peering in una regione di attivazione a condizione che l'account che accetta il collegamento peering abbia optato per tale regione.
- Indipendentemente dallo stato di attivazione della regione, AWS condivide i seguenti dati dell'account con l'account che accetta l'allegato di peering:
  - Account AWS ID
  - ID gateway di transito
  - Codice regione
- Quando elimini il collegamento del gateway di transito, i dati dell'account sopra riportati vengono eliminati.
- Si consiglia di eliminare il collegamento del peering del gateway di transito prima di disattivare la regione. Se non elimini il collegamento del peering, il traffico potrebbe continuare ad essere instradato sul collegamento e potresti continuare a sostenerne i costi. Se non elimini il collegamento, puoi riattivare e quindi eliminarlo.
- In generale, il gateway di transito ha un modello di pagamento a carico del richiedente. Utilizzando un collegamento peering del gateway di transito attraverso un limite di attivazione, potresti sostenere addebiti in una regione che accetta il collegamento, incluse le regioni che non hai scelto. Per ulteriori informazioni, consulta Prezzi di AWS Transit Gateway.

Attività

- Creare un allegato di peering in AWS Transit Gateway
- Accetta o rifiuta una richiesta di peering di allegati in AWS Transit Gateway
- Aggiungi un percorso a una tabella di routing del gateway di transito utilizzando AWS Transit Gateway
- Eliminare un allegato di peering in AWS Transit Gateway

Creare un allegato di peering in AWS Transit Gateway

Prima di iniziare, assicurarsi di disporre dell'ID del gateway di transito che si desidera allegare. Se il gateway di transito si trova in un altro Account AWS, assicurati di avere l' Account AWS ID del proprietario del gateway di transito. Dopo aver creato l'allegato di peering, il proprietario del gateway di transito accettante deve accettare o rifiutare la richiesta di allegato.

Per creare un allegato di peering utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Collegamenti del gateway di transito).
3. Selezionare Create Transit Gateway Attachments (Crea collegamenti del gateway di transito).
4. Per Transit gateway ID (ID gateway di transito), scegliere il gateway di transito per l'allegato. È possibile scegliere un gateway di transito che possiedi. I gateway di transito condivisi con te non sono disponibili per il peering.
5. Per Attachment type (Tipo di allegato), scegliere Peering Connection (Connessione peering).
6. Facoltativamente immettere un tag nome per l'allegato.
7. In Add account (Aggiungi account), eseguire una delle seguenti operazioni:
   - Se il gateway di transito è nel tuo account, scegliere Il mio account.
   - Se il gateway di transito è diverso Account AWS, scegli Altro account. In Account ID (ID account) immettere l'ID dell'account Account AWS .
8. Per Regione, scegliere la regione in cui si trova il gateway di transito.
9. Per Transit gateway (accettatore), immettere l'ID del gateway di transito che si desidera allegare.
10. Selezionare Create transit gateway attachment (Crea collegamento del gateway di transito).

Per creare un allegato di peering utilizzando il AWS CLI

Utilizzate il comando create-transit-gateway-peering-attachment.

Accetta o rifiuta una richiesta di peering di allegati in AWS Transit Gateway

Una volta creato, un allegato di peering del gateway di transito viene creato automaticamente in uno `pendingAcceptance` stato e rimane in questo stato a tempo indeterminato finché non viene accettato o rifiutato. Per attivare l'allegato di peering, il proprietario dell'Accepter Transit Gateway deve accettare la richiesta di peering attachment, anche se entrambi i gateway di transito si trovano nello stesso account. Accettare la richiesta di allegato peering dall'area geografica in cui si trova il gateway di transito accettatore. In alternativa, se si rifiuta l'allegato di peering, è necessario rifiutare la richiesta proveniente dalla regione in cui si trova il gateway di transito accettante.

Per accettare una richiesta di allegato peering utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.

2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Collegamenti del gateway di transito).
3. Selezionare l'allegato peering del gateway di transito in attesa di accettazione.
4. Scegli Actions (Operazioni), Accept transit gateway attachment (Accetta il collegamento del gateway di transito alla VPN).
5. Aggiungere il route statico alla tabella di route del gateway di transito. Per ulteriori informazioni, consulta the section called “Creare una route statica”.

Per rifiutare una richiesta di allegato peering utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Collegamenti del gateway di transito).
3. Selezionare l'allegato peering del gateway di transito in attesa di accettazione.
4. Scegli Actions (Operazioni), Reject transit gateway attachment (Rifiuta il collegamento del gateway di transito alla VPN).

Per accettare o rifiutare un allegato di peering utilizzando il AWS CLI

Utilizzate i comandi accept-transit-gateway-peering-attachment e reject-transit-gateway-peering-attachment.

Aggiungi un percorso a una tabella di routing del gateway di transito utilizzando AWS Transit Gateway

Per instradare il traffico tra i gateway di transito con peering, è necessario aggiungere una route statica alla tabella di routing del gateway di transito che punti all'allegato di peering del gateway di transito. Il proprietario del gateway di transito dell'accettante deve inoltre aggiungere un route statico alla tabella dei percorsi del gateway di transito.

Per creare una route statica mediante la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Route Tables (Tabelle di routing del gateway di transito).

3. Selezionare la tabella di instradamento per la quale creare il routing.
4. Scegliere Actions (Operazioni), Create static route (Crea routing statico).
5. Nella pagina Create static route (Crea route statico), immettere il blocco CIDR per cui creare una route. Ad esempio, specificare il blocco CIDR di un VPC collegato al gateway di transito peer.
6. Scegliere l'allegato di peering per il percorso.
7. Scegliere Create static route (Crea route statico).

Per creare una rotta statica utilizzando il AWS CLI

Utilizza il comando create-transit-gateway-route.

> **Important**
>
> Dopo aver creato la route, l'allegato di peering del gateway di transito deve essere già associato alla tabella delle rotte del gateway di transito. Per ulteriori informazioni, consulta the section called “Associare una tabella di instradamento di un gateway di transito.”.

Eliminare un allegato di peering in AWS Transit Gateway

È possibile eliminare un allegato peering del gateway di transito. Il proprietario di uno dei gateway di transito può eliminare l'allegato.

Per eliminare un allegato di peering utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Collegamenti del gateway di transito).
3. Selezionare l'allegato peering del gateway di transito.
4. Scegliere Operazioni, Eliminare collegamento del gateway di transito.
5. Immettere **`delete`** e scegliere Delete (Elimina).

Per eliminare un allegato di peering utilizzando il AWS CLI

Utilizzate il comando delete-transit-gateway-peering-attachment.

Connetti gli allegati e collega i peer in AWS Transit Gateway

Puoi creare un collegamento Connect del gateway di transito per stabilire una connessione tra un gateway di transito e appliance virtuali di terze parti (ad esempio le appliance SD-WAN) in esecuzione in un VPC. Un collegamento Connect supporta il protocollo del tunnel GRE (Generic Routing Encapsulation) per prestazioni elevate e Border Gateway Protocol (BGP) per il routing dinamico. Dopo aver creato un collegamento Connect, puoi creare uno o più tunnel GRE (detti anche peer di Transit Gateway Connect) sul collegamento Connect in modo da connettere il gateway di transito e l'appliance di terze parti. In questo modo vengono stabilite due sessioni BGP attraverso il tunnel GRE per scambiare informazioni di routing.

Important

Un peer Transit Gateway Connect è costituito da due sessioni di peering BGP che terminano su un'infrastruttura gestita. AWS Le due sessioni di peering BGP forniscono la ridondanza del piano di routing, assicurando che la perdita di una sessione di peering BGP non influisca sulle operazioni di routing. Le informazioni di routing ricevute da entrambe le sessioni BGP vengono accumulate per il peer di Connect specificato. Le due sessioni di peering BGP proteggono anche da qualsiasi operazione sull'infrastruttura AWS come manutenzione ordinaria, applicazione di patch, aggiornamenti hardware e sostituzioni. Se il peer Connect funziona senza la doppia sessione di peering BGP consigliata configurata per la ridondanza, potrebbe verificarsi una perdita momentanea di connettività durante le operazioni dell'infrastruttura. AWS Consigliamo vivamente di configurare entrambe le sessioni di peering BGP sul peer di Connect. Se più peer di Connect sono stati configurati per supportare l'elevata disponibilità lato appliance, si consiglia di configurare entrambe le sessioni di peering BGP su ciascuno dei peer di Connect.

Un collegamento Connect utilizza un collegamento VPC o Direct Connect esistente come meccanismo di trasporto sottostante. Questo è detto collegamento di trasporto. Il gateway di transito identifica i pacchetti GRE corrispondenti dell'appliance di terze parti come traffico proveniente dal collegamento Connect. Tutti gli altri pacchetti, inclusi i pacchetti GRE con informazioni di origine o di destinazione errate, verranno trattati come traffico proveniente dal collegamento di trasporto.

Note

Per utilizzare un collegamento Direct Connect come meccanismo di trasporto, devi prima integrare Direct Connect con AWS Transit Gateway. Per i passaggi per creare questa

integrazione, consulta Integrazione dei dispositivi SD-WAN con AWS Transit Gateway e. Direct Connect

Peer Connect

Un peer Connect (tunnel GRE) è costituito dai componenti riportati di seguito.

Blocchi CIDR interni (indirizzi BGP)

Gli indirizzi IP interni utilizzati per il peering BGP. È necessario specificare un blocco CIDR /29 dall'intervallo per. `169.254.0.0/16` IPv4 Facoltativamente, è possibile specificare un blocco CIDR /125 dall'intervallo per. `fd00::/8` IPv6 I seguenti blocchi CIDR sono riservati e non possono essere utilizzati:

- 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

È necessario configurare il primo indirizzo dell' IPv4 intervallo sull'appliance come indirizzo IP BGP. Quando si utilizza IPv6, se il blocco CIDR interno è fd00: :/125, è necessario configurare il primo indirizzo in questo intervallo (fd00: :1) sull'interfaccia tunnel dell'appliance.

Gli indirizzi BGP devono essere univoci in tutti i tunnel di un gateway di transito.

Indirizzo IP peer

L'indirizzo IP peer (indirizzo IP esterno GRE) sul lato appliance del peer Connect. Questo può essere un qualsiasi indirizzo IP. L'indirizzo IP può essere un IPv6 indirizzo IPv4 o, ma deve appartenere alla stessa famiglia di indirizzi IP dell'indirizzo del gateway di transito.

Indirizzo gateway di transito

L'indirizzo IP peer (indirizzo IP esterno GRE) sul lato gateway di transito del peer Connect. L'indirizzo IP deve essere specificato dal blocco CIDR del gateway di transito e deve essere

univoco tra i collegamenti Connect nel gateway di transito. Se non specifichi un indirizzo IP, verrà utilizzato il primo indirizzo disponibile dal blocco CIDR del gateway di transito.

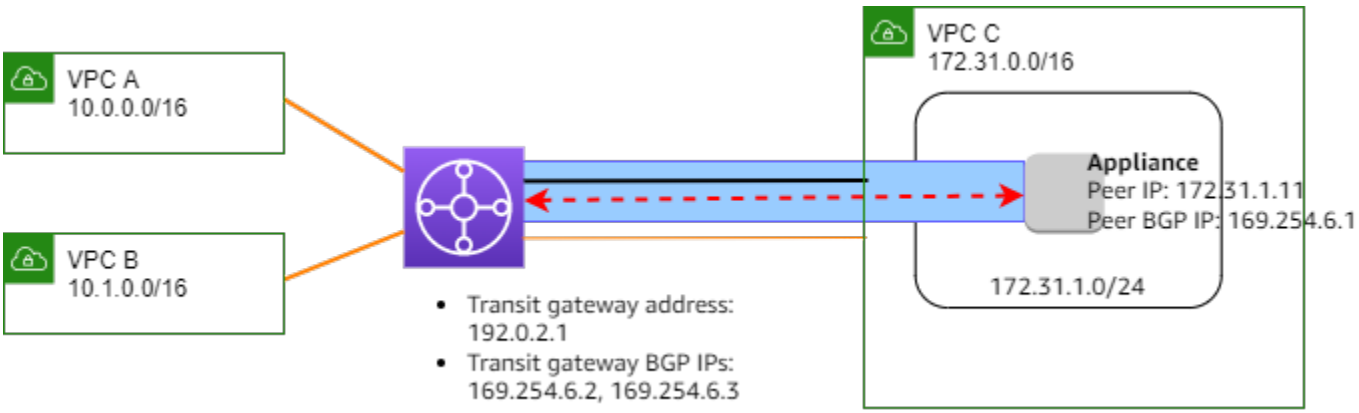
Puoi aggiungere un blocco CIDR del gateway di transito quando crei o modifichi un gateway di transito.

L'indirizzo IP può essere un IPv6 indirizzo IPv4 or, ma deve appartenere alla stessa famiglia di indirizzi IP dell'indirizzo IP peer.

L'indirizzo IP peer e l'indirizzo del gateway di transito vengono utilizzati per identificare in modo univoco il tunnel GRE. Puoi riutilizzare entrambi gli indirizzi in più tunnel, ma non entrambi nello stesso tunnel.

Transit Gateway Connect per il peering BGP supporta solo BGP multiprotocollo (MP-BGP), in cui l'indirizzamento Unicast è necessario per stabilire anche una sessione BGP per IPv4 Unicast. IPv6 È possibile utilizzare entrambi gli indirizzi e per gli indirizzi IP esterni GRE. IPv4 IPv6

Nell'esempio seguente viene riportato un collegamento Connect tra un gateway di transito e un'appliance in un VPC.



Componente diagramma	Descrizione
	Collegamento VPC
	Collegamento Connect
	Tunnel GRE (peer Connect)

Componente diagramma	Descrizione
	Sessione di peering BGP

Nell'esempio precedente viene creato un collegamento Connect su un collegamento VPC esistente (il collegamento di trasporto). Viene quindi creato un peer Connect sul collegamento Connect per stabilire una connessione a un'appliance nel VPC. L'indirizzo del gateway di transito è `192.0.2.1`, e l'intervallo di indirizzi BGP è `169.254.6.0/29`. Il primo indirizzo IP dell'intervallo (`169.254.6.1`) viene configurato sull'appliance come indirizzo IP BGP peer.

La tabella di routing della rottorete per il VPC C dispone di una route che instrada il traffico destinato al blocco CIDR del gateway di transito al gateway di transito.

Destinazione	Target
172.31.0.0/16	Locale
192.0.2.0/24	tgw-id

Requisiti e considerazioni

Di seguito sono riportati i requisiti e le considerazioni per un collegamento Connect.

- Per informazioni sulle regioni che supportano i collegamenti Connect, consulta le Domande frequenti su Transit Gateway di AWS.
- L'appliance di terze parti deve essere configurata per inviare e ricevere traffico attraverso un tunnel GRE da e verso il gateway di transito tramite il collegamento Connect.
- L'appliance di terze parti deve essere configurata per utilizzare BGP per gli aggiornamenti delle route dinamiche e i controlli di integrità.
- Sono supportati i seguenti tipi di BGP:
  - BGP esterno (eBGP): utilizzato per la connessione a router che si trovano in un sistema autonomo diverso da quello del gateway di transito. Se usi eBGP, devi configurare ebgp-multihop con un valore (TTL) pari a time-to-live 2.
  - BGP interno (iBGP): utilizzato per la connessione a router che si trovano nello stesso sistema autonomo del gateway di transito. Il gateway di transito non installerà percorsi da un peer iBGP

(dispositivo di terze parti), a meno che i percorsi non provengano da un peer eBGP e non abbiano dovuto essere configurati. next-hop-self Le route pubblicizzate dall'appliance di terze parti tramite il peering iBGP devono avere un ASN.

  - MP-BGP (estensioni multiprotocollo per BGP): utilizzate per supportare più tipi di protocolli, ad esempio famiglie di indirizzi. IPv4 IPv6
- Il timeout di keep-alive BGP predefinito è di 10 secondi e il timer di attesa predefinito è di 30 secondi.
- IPv6 Il peering BGP non è supportato; è supportato solo il peering BGP basato. IPv4 IPv6 i prefissi vengono scambiati tramite peering BGP utilizzando MP-BGP. IPv4
- Il rilevamento bidirezionale di inoltro (BFD) non è supportato.
- Non è supportato il riavvio gestito automaticamente di BGP.
- Se crei un peer del gateway di transito, se non specifichi un numero ASN peer, verrà selezionato il numero ASN del gateway di transito. Ciò significa che l'appliance e il gateway di transito saranno nello stesso sistema autonomo che esegue iBGP.
- Un peer di Connect che utilizza l'attributo BGP AS-PATH è il percorso preferito quando disponi di due peer Connect.

  Per utilizzare il routing ECMP (Equal-Cost Multi-Path) tra più appliance, dovrai configurare l'appliance in modo che pubblicizzi gli stessi prefissi al gateway di transito con lo stesso attributo BGP AS-PATH. Affinché il gateway di transito scelga tutti i percorsi ECMP disponibili, l'AS-PATH e il numero di sistema autonomo (ASN) devono corrispondere. Il gateway di transito può utilizzare ECMP tra peer Connect per lo stesso collegamento Connect o tra collegamenti Connect sullo stesso gateway di transito. Il gateway di transito non può utilizzare ECMP tra entrambi i peering BGP ridondanti che un singolo peer stabilisce.
- Per impostazione predefinita, con un allegato Connect le route vengono propagate a una tabella di routing del gateway di transito.
- Le route statiche non sono supportate.
- Configura l'MTU del tunnel GRE in modo che sia più piccolo dell'MTU dell'interfaccia esterna sottraendo l'overhead dell'intestazione GRE (24 byte) e dell'intestazione IP esterna (20 byte). Ad esempio, se l'MTU dell'interfaccia esterna è di 1500 byte, imposta l'MTU del tunnel GRE su 1456 byte (1500 - 24 - 20 = 1456) per evitare la frammentazione dei pacchetti.

Attività

- Creare un allegato Connect in AWS Transit Gateway

- Crea un peer Connect in AWS Transit Gateway
- Visualizza gli allegati Connect e i peer Connect in AWS Transit Gateway
- Modifica l'allegato Connect e i tag peer Connect in AWS Transit Gateway
- Eliminare un peer Connect in AWS Transit Gateway
- Eliminare un allegato Connect in AWS Transit Gateway

Creare un allegato Connect in AWS Transit Gateway

Per creare un collegamento Connect, devi specificare un collegamento esistente come collegamento di trasporto. Puoi specificare un collegamento VPC o un collegamento Direct Connect come collegamento di trasporto.

Per creare un collegamento Connect utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, seleziona Collegamenti del gateway di transito alla VPN.
3. Selezionare Create transit gateway attachments (crea collegamenti del gateway di transito).
4. (Facoltativo) In Tag nome, specifica un nome di tag per il collegamento.
5. Per ID gateway di transito, scegliere il gateway di transito per il collegamento.
6. In Tipo collegamento, seleziona Connect.
7. Per ID collegamento di trasporto, seleziona l'ID di un collegamento esistente (collegamento di trasporto).
8. Selezionare Create transit gateway attachments (Crea collegamenti del gateway di transito).

Per creare un allegato Connect utilizzando AWS CLI

Utilizza il comando create-transit-gateway-connect.

Crea un peer Connect in AWS Transit Gateway

Puoi creare un peer Connect (tunnel GRE) per un collegamento Connect esistente. Prima di iniziare, assicurarsi di aver configurato un blocco CIDR del gateway di transito. Puoi configurare un blocco CIDR del gateway di transito quando crei o modifichi un gateway di transito.

Quando crei il peer Connect, devi specificare l'indirizzo IP esterno GRE sul lato appliance del peer Connect.

Per creare un peer Connect utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, seleziona Collegamenti del gateway di transito alla VPN.
3. Seleziona il collegamento Connect e scegli Azioni, Crea peer connect.
4. (Facoltativo) In Tag nome, specifica un tag di nome per il peer di Connect.
5. (Facoltativo) In indirizzo GRE del gateway di transito, specifica l'indirizzo IP esterno GRE per il gateway di transito. Per impostazione predefinita, viene utilizzato il primo indirizzo disponibile dal blocco CIDR del gateway di transito.
6. Per Indirizzo GRE peer, specifica l'indirizzo IP esterno GRE per il lato appliance del peer Connect.
7. Per i blocchi CIDR BGP Inside IPv4, specifica l'intervallo di IPv4 indirizzi interni utilizzati per il peering BGP. Specifica un blocco CIDR /29 dall'intervallo `169.254.0.0/16`.
8. (Facoltativo) Per i blocchi CIDR BGP Inside IPv6, specifica l'intervallo di indirizzi interni utilizzati per il peering BGP. IPv6 Specifica un blocco CIDR /125 dall'intervallo `fd00::/8`.
9. (Facoltativo) In ASN peer, specifica il Border Gateway Protocol (BGP) Autonomous System Number (ASN) per l'appliance. Puoi utilizzare un ASN esistente assegnato alla tua rete. Se non ne hai uno, puoi utilizzare un ASN privato compreso nell'intervallo 64512–65534 (ASN a 16 bit) o 4200000000–4294967294 (ASN a 32 bit).

   Il valore predefinito è lo stesso ASN del gateway di transito. Se configuri l'ASN peer in modo che sia diverso dall'ASN del gateway di transito (eBGP), devi configurare ebgp-multihop con un valore (TTL) pari a 2. time-to-live
10. Scegliere Crea peer connect.

Per creare un peer Connect utilizzando AWS CLI

Usate il comando create-transit-gateway-connect-peer.

Visualizza gli allegati Connect e i peer Connect in AWS Transit Gateway

Visualizza gli allegati Connect e i colleghi Connect.

Per visualizzare i collegamenti Connect e i peer Connect utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, seleziona Collegamenti del gateway di transito alla VPN.

3. Seleziona il collegamento Connect.
4. Per visualizzare i peer Connect per il collegamento, seleziona la scheda Peer Connect .

Per visualizzare gli allegati Connect e i colleghi Connect utilizzando il AWS CLI

Usa i comandi describe-transit-gateway-connectse describe-transit-gateway-connect-peers.

Modifica l'allegato Connect e i tag peer Connect in AWS Transit Gateway

Puoi modificare i tag per il collegamento Connect.

Per modificare i tag del collegamento Connect utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, seleziona Collegamenti del gateway di transito.
3. Seleziona il collegamento Connect, quindi seleziona Operazioni, Gestisci tag.
4. Per aggiungere un tag, seleziona Aggiungi un nuovo tag e specifica il nome e il valore della chiave.
5. Per rimuovere un tag, scegli Remove (Rimuovi).
6. Scegli Save (Salva).

Puoi modificare i tag per il peer Connect.

Per modificare i tag del peer Connect utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, seleziona Collegamenti del gateway di transito.
3. Seleziona il collegamento Connect, quindi seleziona Peer Connect.
4. Seleziona il peer di Connect, quindi scegli Operazioni, Gestisci tag.
5. Per aggiungere un tag, seleziona Aggiungi un nuovo tag e specifica il nome e il valore della chiave.
6. Per rimuovere un tag, scegli Remove (Rimuovi).
7. Scegli Save (Salva).

Per modificare l'allegato Connect e i tag del peer Connect utilizzando la AWS CLI

Utilizza i comandi create-tags e delete-tags.

Eliminare un peer Connect in AWS Transit Gateway

Se non hai più bisogno di un peer Connect, puoi eliminarlo.

Per eliminare un peer Connect utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, seleziona Collegamenti del gateway di transito alla VPN.
3. Seleziona il collegamento Connect.
4. Nella scheda Peer di Connect, seleziona il peer Connect e scegli Azioni, Elimina peer Connect.

Per eliminare un peer Connect utilizzando il AWS CLI

Usa il comando delete-transit-gateway-connect-peer.

Eliminare un allegato Connect in AWS Transit Gateway

Se non hai più bisogno di un collegamento Connect, puoi eliminarlo. Per prima cosa, devi eliminare tutti i peer Connect per il collegamento.

Per eliminare un collegamento Connect utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, seleziona Collegamenti del gateway di transito alla VPN.
3. Seleziona il collegamento Connect e scegli Operazioni, Eliminare il collegamento del gateway.
4. Inserire **`delete`**, quindi scegliere Delete (Elimina).

Per eliminare un allegato Connect utilizzando il AWS CLI

Utilizza il comando delete-transit-gateway-connect.

Tabelle dei percorsi del gateway di AWS transito in Transit Gateway

Utilizzare le tabelle di route del gateway di transito per configurare il routing per gli allegati del gateway di transito. Una tabella di routing è una tabella che contiene regole che stabiliscono il modo

in cui il traffico di rete viene instradato tra il tuo VPCs e. VPNs Ogni route della tabella contiene l'intervallo di indirizzi IP per le destinazioni a cui si desidera inviare il traffico.

Le tabelle di routing del gateway di transito consentono di associare una tabella a un allegato del gateway di transito. Gli allegati VPC, VPN, VPN Concentrator, Direct Connect gateway, Peering e Connect sono tutti supportati. Se associati, i percorsi per questi allegati vengono propagati dall'allegato alla tabella di routing del gateway di transito di destinazione. Un allegato può essere propagato a più tabelle di routing.

Inoltre è possibile creare e gestire percorsi statici con una tabella di routing. Ad esempio, potresti avere una route statica che viene utilizzata come route di backup in caso di interruzione della rete che influisca su qualsiasi route dinamica.

Processi

- Crea una tabella di routing del gateway di AWS transito in Transit Gateway
- Visualizza le tabelle dei percorsi dei gateway di AWS transito utilizzando Transit Gateway
- Associa una tabella di routing del gateway di AWS transito in Transit Gateway
- Eliminare un'associazione per una tabella di routing del gateway di AWS transito in Transit Gateway
- Abilita la propagazione del percorso su una tabella di routing del gateway di transito in AWS Transit Gateway
- Disabilita la propagazione delle rotte in AWS Transit Gateway
- Crea un percorso statico in AWS Transit Gateway
- Eliminare una route statica in AWS Transit Gateway
- Sostituisci una route statica in AWS Transit Gateway
- Esporta le tabelle di routing su Amazon S3 in AWS Transit Gateway
- Eliminare una tabella di routing del gateway di AWS transito in Transit Gateway
- Crea un riferimento all'elenco dei prefissi della tabella di percorso in AWS Transit Gateway
- Modificare un riferimento all'elenco di prefissi in AWS Transit Gateway
- Eliminare un riferimento all'elenco di prefissi in AWS Transit Gateway

Crea una tabella di routing del gateway di AWS transito in Transit Gateway

Per creare una tabella di route del gateway di transito utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Route Tables (Tabelle di routing del gateway di transito).
3. Selezionare Create Transit Gateway Route Table (Crea una tabella di routing del gateway di transito).
4. (Facoltativo) Per Tag nome, digitare un nome per la tabella di route del gateway di transito. Questa operazione crea un tag con la chiave impostata a "Name" e il valore corrispondente al nome indicato.
5. Per ID gateway di transito, selezionare il gateway di transito per la tabella di routing.
6. Selezionare Create transit gateway route table (Crea una tabella di routing del gateway di transito).

Per creare una tabella di routing del gateway di transito utilizzando il AWS CLI

Utilizzate il comando create-transit-gateway-route-table.

Visualizza le tabelle dei percorsi dei gateway di AWS transito utilizzando Transit Gateway

Visualizzazione delle tabelle di instradamento del gateway di transito tramite la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Route Tables (Tabelle di routing del gateway di transito).
3. (Facoltativo) Per trovare una tabella di instradamento specifica o un insieme di tabelle, inserisci tutto il nome o una sua parte, una parola chiave o un attributo nel campo di filtro.
4. Seleziona la casella di controllo per una tabella di instradamento o scegli il suo ID per visualizzare informazioni sulle relative associazioni, propagazioni, route e tag.

Per visualizzare le tabelle delle rotte del gateway di transito, utilizza il AWS CLI

Utilizzate il comando describe-transit-gateway-route-tables.

Per visualizzare le rotte per una tabella delle rotte di un gateway di transito utilizzando il AWS CLI

Utilizza il comando search-transit-gateway-routes.

Per visualizzare le propagazioni delle rotte per una tabella delle rotte di un gateway di transito utilizzando il AWS CLI

Utilizzate il comando get-transit-gateway-route-table-propagations.

Per visualizzare le associazioni per una tabella di routing del gateway di transito utilizzando il AWS CLI

Utilizzate il comando get-transit-gateway-route-table-associations.

Associa una tabella di routing del gateway di AWS transito in Transit Gateway

È possibile associare una tabella di route del gateway di transito a un allegato del gateway di transito.

Per associare una tabella di route del gateway di transito tramite la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Route Tables (Tabelle di routing del gateway di transito).
3. Selezionare la tabella di instradamento.
4. Nella parte inferiore della pagina, selezionare la scheda Associations (Associazioni).
5. Selezionare Create association (Crea associazione).
6. Selezionare il collegamento da associare e quindi selezionare Create association (Crea associazione).

Per associare una tabella di routing del gateway di transito utilizzando AWS CLI

Utilizzate il comando associate-transit-gateway-route-table.

Eliminare un'associazione per una tabella di routing del gateway di AWS transito in Transit Gateway

È possibile disassociare una tabella di route del gateway di transito da un allegato del gateway di transito.

Per disassociare una tabella di route del gateway di transito utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Route Tables (Tabelle di routing del gateway di transito).
3. Selezionare la tabella di instradamento.
4. Nella parte inferiore della pagina, selezionare la scheda Associations (Associazioni).
5. Selezionare il collegamento per il quale eliminare l'associazione e quindi selezionare Delete association (Elimina associazione).
6. Quando viene richiesta la conferma, selezionare Delete association (Elimina associazione).

Per dissociare una tabella di routing del gateway di transito utilizzando la AWS CLI

Utilizzate il comando disassociate-transit-gateway-route-table.

Abilita la propagazione del percorso su una tabella di routing del gateway di transito in AWS Transit Gateway

Utilizza la propagazione delle route per aggiungere una route da un collegamento a una tabella di routing.

Per propagare un route a una tabella di route degli allegati del gateway di transito

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Route Tables (Tabelle di routing del gateway di transito).
3. Selezionare la tabella di instradamento per la quale creare la propagazione.
4. Selezionare Actions (Operazioni), Create propagation (Crea propagazione).
5. Selezionare il collegamento nella pagina Create propagation (Crea propagazione).
6. Selezionare Create propagation (Crea propagazione).

Per abilitare la propagazione delle rotte utilizzando AWS CLI

Utilizzate il comando enable-transit-gateway-route-table-propagation.

Disabilita la propagazione delle rotte in AWS Transit Gateway

Rimuovere una route propagata dalla tabella di instradamento di un collegamento.

Per disabilitare la propagazione delle route utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Route Tables (Tabelle di routing del gateway di transito).
3. Selezionare la tabella di instradamento dalla quale eliminare la propagazione.
4. Nella parte inferiore della pagina, selezionare la scheda Propagations (Propagazioni).
5. Selezionare il collegamento e quindi selezionare Delete propagation (Elimina propagazione).
6. Quando viene richiesta la conferma, selezionare Delete propagation (Elimina propagazione).

Per disabilitare la propagazione delle rotte utilizzando AWS CLI

Utilizzate il comando disable-transit-gateway-route-table-propagation.

Crea un percorso statico in AWS Transit Gateway

Crea un percorso statico per un allegato di peering VPC, VPN o gateway di transito oppure puoi creare un percorso a buco nero che riduca il traffico corrispondente al percorso.

Le route statiche in una tabella di routing del gateway di transito destinate a un allegato VPN non vengono filtrate dalla VPN. Site-to-Site Ciò potrebbe consentire un flusso di traffico in uscita non intenzionale quando si utilizza una VPN basata su BGP.

Per creare una route statica mediante la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Route Tables (Tabelle di routing del gateway di transito).
3. Selezionare la tabella di instradamento per la quale creare il routing.
4. Scegliere Actions (Operazioni), Create static route (Crea routing statico).
5. Nella pagina Create route (Crea routing), immettere il blocco CIDR per cui creare il routing, quindi selezionare Active (Attiva).

6. Selezionare il collegamento per la route.
7. Scegliere Create static route (Crea routing statico).

Per creare una route blackhole mediante la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Route Tables (Tabelle di routing del gateway di transito).
3. Selezionare la tabella di instradamento per la quale creare il routing.
4. Scegliere Actions (Operazioni), Create static route (Crea routing statico).
5. Nella pagina Create route (Crea route), immettere il blocco CIDR per cui creare il routing, quindi selezionare Blackhole.
6. Scegliere Create static route (Crea routing statico).

Per creare una route statica o una route blackhole utilizzando il AWS CLI

Utilizza il comando create-transit-gateway-route.

Eliminare una route statica in AWS Transit Gateway

Elimina percorsi statici da una tabella di routing del gateway di transito.

Per eliminare una route statica mediante la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Route Tables (Tabelle di routing del gateway di transito).
3. Selezionare la tabella di instradamento da cui eliminare la route e scegliere Routes (Route).
4. Selezionare la route da eliminare.
5. Scegliere Eliminare routing statico.
6. Nella finestra del box di conferma, selezionare Delete static route (Elimina routing statico).

Per eliminare una route statica utilizzando il AWS CLI

Utilizza il comando delete-transit-gateway-route.

Sostituisci una route statica in AWS Transit Gateway

Sostituisci una route statica in una tabella di routing del gateway di transito con una route statica diversa.

Sostituire una route statica mediante la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Route Tables (Tabelle di routing del gateway di transito).
3. Scegli il percorso che desideri sostituire nella tabella di routing.
4. Nella sezione dei dettagli, scegli la scheda Route.
5. Scegli Azioni, Sostituisci route statica.
6. Per il Tipo, scegli Attivo o Blackhole.
7. Dal menu a discesa Scegli allegato, scegli il gateway di transito che sostituirà quello corrente nella tabella di routing.
8. Scegl Sostituisci route statica.

Per sostituire una route statica utilizzando il AWS CLI

Utilizza il comando replace-transit-gateway-route.

Esporta le tabelle di routing su Amazon S3 in AWS Transit Gateway

È possibile esportare le route nelle tabelle di routing del gateway di transito in un bucket Amazon S3. Le route vengono salvate nel bucket Amazon S3 specificato in un file JSON.

Per esportare le tabelle di route del gateway di transito utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Route Tables (Tabelle di routing del gateway di transito).
3. Selezionare la tabella di instradamento che include le route da esportare.
4. Selezionare Actions (Operazioni), Export routes (Esporta route).
5. Nella pagina Export routes (Esporta routes), in S3 bucket name (Nome bucket S3), indicare il nome del bucket S3.

6. Per filtrare le route esportate, specificare i parametri di filtro nella sezione Filters (Filtri) della pagina.
7. Selezionare Export routes (Esporta route).

Per accedere ai percorsi esportati, apri la console Amazon S3 https://console.aws.amazon.com/s3/all'indirizzo e accedi al bucket specificato. Il nome del file include l' Account AWS ID, la AWS regione, l'ID della tabella di percorso e un timestamp. Selezionare il file e scegliere Download (Scarica). Di seguito è riportato un esempio di un file JSON contenente informazioni su due route propagate per gli allegati VPC.


```
{
  "filter": [
    {
      "name": "route-search.subnet-of-match",
      "values": [
        "0.0.0.0/0",
        "::/0"
      ]
    }
  ],
  "routes": [
    {
      "destinationCidrBlock": "10.0.0.0/16",
      "transitGatewayAttachments": [
        {
          "resourceId": "vpc-0123456abcd123456",
          "transitGatewayAttachmentId": "tgw-attach-1122334455aabbcc1",
          "resourceType": "vpc"
        }
      ],
      "type": "propagated",
      "state": "active"
    },
    {
      "destinationCidrBlock": "10.2.0.0/16",
      "transitGatewayAttachments": [
        {
          "resourceId": "vpc-abcabc123123abca",
          "transitGatewayAttachmentId": "tgw-attach-6677889900aabbcc7",
          "resourceType": "vpc"
        }
```

```
      ],
      "type": "propagated",
      "state": "active"
    }
  ]
}
```

Eliminare una tabella di routing del gateway di AWS transito in Transit Gateway

Per eliminare una tabella di route del gateway di transito utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Route Tables (Tabelle di routing del gateway di transito).
3. Selezionare la tabella di instradamento da eliminare.
4. Scegliere Operazioni,Eliminare la tabella di instradamento del gateway di transito.
5. Immettere **`delete`**, quindi scegliere Delete (Elimina) per confermare l'eliminazione

Per eliminare una tabella di routing del gateway di transito utilizzando il AWS CLI

Utilizzate il comando delete-transit-gateway-route-table.

Crea un riferimento all'elenco dei prefissi della tabella di percorso in AWS Transit Gateway

È possibile fare riferimento a un elenco di prefissi nella tabella di instradamento del gateway di transito. Un elenco di prefissi è un insieme di una o più voci di blocco CIDR definite e gestite dall'utente. È possibile utilizzare un elenco di prefissi per semplificare la gestione degli indirizzi IP a cui si fa riferimento nelle risorse per instradare il traffico di rete. Ad esempio, se specificate spesso la stessa destinazione CIDRs in più tabelle di routing dei gateway di transito, potete gestirle CIDRs in un unico elenco di prefissi, invece di fare ripetutamente riferimento allo stesso CIDRs in ogni tabella di routing. Se hai la necessità di rimuovere un blocco CIDR di destinazione, puoi rimuovere la voce dall'elenco dei prefissi anziché rimuovere l'instradamento da ogni tabella di instradamento interessata.

Quando si crea un riferimento all'elenco di prefissi nella tabella di instradamento del gateway di transito, ogni voce dell'elenco dei prefissi viene rappresentata come route nella tabella route del gateway di transito.

Per maggiori informazioni sugli elenchi di prefissi, consulta Elenchi di prefissi nella Guida dell'utente di Amazon VPC.

Per creare un riferimento all'elenco di prefissi utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Tabelle di routing del gateway di transito.
3. Seleziona la tabella di instradamento del gateway di transito.
4. Scegliere Operazioni, Crea riferimento all'elenco dei prefissi.
5. Per ID elenco prefissi, scegliere l'ID dell'elenco dei prefissi.
6. PerType (Tipo), scegliere se è consentito il traffico verso questo elenco di prefissi (Active (Attivo)) o abbandonato (Blackhole).
7. Per Transit gateway attachment ID (ID allegato gateway di transito), scegliere l'ID dell'allegato a cui indirizzare il traffico routing.
8. Scegliere Crea riferimento elenco di prefissi.

Per creare un riferimento all'elenco di prefissi utilizzando il AWS CLI

Utilizzate il comando create-transit-gateway-prefix-list-reference.

Modificare un riferimento all'elenco di prefissi in AWS Transit Gateway

È possibile modificare un riferimento a un elenco di prefissi modificando l'allegato a cui viene instradato il traffico o indicando se eliminare il traffico corrispondente al percorso.

Non è possibile modificare le singole route per un elenco di prefissi nella scheda Route. Per modificare le voci nell'elenco dei prefissi, utilizzare la schermata Elenchi prefissi gestiti. Per maggiori informazioni, consulta Modifica di un elenco di prefissi nella Guida dell'utente di Amazon VPC.

Per modificare un riferimento a un elenco di prefissi utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Tabelle di routing del gateway di transito.

3. Seleziona la tabella di instradamento del gateway di transito.
4. Nel riquadro inferiore, scegliere Riferimenti elenco prefissi.
5. Scegliete il riferimento all'elenco dei prefissi e scegliete Modifica riferimenti.
6. PerType (Tipo), scegliere se è consentito il traffico verso questo elenco di prefissi (Active (Attivo)) o abbandonato (Blackhole).
7. Per Transit gateway attachment ID (ID allegato gateway di transito), scegliere l'ID dell'allegato a cui indirizzare il traffico routing.
8. Scegliere Modifica riferimento elenco prefissi.

Per modificare un riferimento a un elenco di prefissi utilizzando il AWS CLI

Utilizzate il comando modify-transit-gateway-prefix-list-reference.

Eliminare un riferimento all'elenco di prefissi in AWS Transit Gateway

Se non è più necessario un riferimento all'elenco di prefissi, è possibile eliminarlo dalla tabella di instradamento del gateway di transito. L'eliminazione del riferimento non comporta l'eliminazione dell'elenco dei prefissi.

Per eliminare un riferimento a un elenco di prefissi utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Tabelle di routing del gateway di transito.
3. Seleziona la tabella di instradamento del gateway di transito.
4. Scegliere la referenza all'elenco dei prefissi, quindi selezionare Elimina riferimenti.
5. Scegliere Elimina riferimenti.

Per modificare un riferimento a un elenco di prefissi utilizzando AWS CLI

Utilizzate il comando delete-transit-gateway-prefix-list-reference.

Tabelle delle politiche del gateway di AWS transito in Transit Gateway

Il routing dinamico del gateway di transito utilizza tabelle di policy per instradare il traffico di rete per AWS Cloud WAN. La tabella contiene le regole di policy per la corrispondenza del traffico di rete in

base agli attributi delle policy, quindi mappa il traffico che corrisponde alla regola in una tabella di instradamento di destinazione.

È possibile utilizzare il routing dinamico per i gateway di transito per lo scambio automatico di informazioni di instradamento e raggiungibilità con tipi di gateway di transito in peering. A differenza di un instradamento statico, il traffico può essere instradato lungo un percorso diverso in base alle condizioni della rete, come guasti del percorso o congestione. Il routing dinamico aggiunge anche un ulteriore livello di sicurezza in quanto è più facile reinstradare il traffico in caso di violazione o incursione nella rete.

> **Note**
>
> Le tabelle di policy del gateway di transito al momento sono supportate in Cloud WAN solo quando si crea una connessione di peering del gateway di transito. Quando crei una connessione peering, puoi associare quella tabella alla connessione. L'associazione quindi compila automaticamente la tabella con le regole delle policy.
> Per ulteriori informazioni sulle connessioni peering in Cloud WAN, consulta Peerings (Peering) nella Guida per l'utente di AWS Cloud WAN.

Attività

- Crea una tabella delle politiche del gateway di AWS transito in Transit Gateway
- Eliminare una tabella di policy del gateway di AWS transito in Transit Gateway

Crea una tabella delle politiche del gateway di AWS transito in Transit Gateway

Per creare una tabella di policy del gateway di transito utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit gateway policy table (Tabella di policy del gateway di transito).
3. Selezionare Create transit gateway policy table (Crea tabella di policy del gateway di transito).
4. (Facoltativo) Per Name tag (Tag nome), immettere un nome per la policy del gateway di transito. In questo modo viene creato un tag con valore corrispondente al nome specificato.

5. Per Transit gateway ID (ID gateway di transito), selezionare il gateway di transito per la tabella di policy.
6. Selezionare Create transit gateway policy table (Crea tabella di policy del gateway di transito).

Per creare una tabella delle politiche del gateway di transito utilizzando il AWS CLI

Utilizzate il comando create-transit-gateway-policy-table.

Eliminare una tabella di policy del gateway di AWS transito in Transit Gateway

Eliminazione di una tabella di policy di un gateway di transito. Quando una tabella viene eliminata, tutte le regole di policy all'interno di tale tabella vengono eliminate.

Per eliminare una tabella di policy del gateway di transito utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit gateway policy tables (Tabelle di policy del gateway di transito).
3. Selezionare la tabella di policy del gateway di transito da eliminare.
4. Seleziona Actions (Operazioni), quindi Delete policy table (Elimina tabella della policy).
5. Confermare l'eliminazione della tabella.

Per eliminare una tabella delle politiche del gateway di transito utilizzando il AWS CLI

Utilizzate il comando delete-transit-gateway-policy-table.

Multicast in AWS Transit Gateway

Multicast è un protocollo di comunicazione utilizzato per fornire un singolo flusso di dati a più computer riceventi contemporaneamente. Transit Gateway supporta il routing del traffico multicast tra sottoreti collegate VPCs e funge da router multicast per le istanze che inviano traffico destinato a più istanze di ricezione.

Argomenti

- Concetti multicast

Concetti multicast

Di seguito sono elencati i concetti fondamentali relativi al multicast:

- Dominio multicast: consente la segmentazione di una rete multicast in domini diversi e fa sì che il gateway di transito agisca come router multicast multipli. È possibile definire l'appartenenza al dominio multicast a livello di sottorete.
- Gruppo multicast: identifica un insieme di host che invieranno e riceveranno lo stesso traffico multicast. Un gruppo multicast è identificato da un indirizzo IP del gruppo. L'appartenenza ai gruppi multicast è definita da singole interfacce di rete elastiche collegate alle istanze. EC2
- IGMP (Internet Group Management Protocol): un protocollo Internet che consente agli host e ai router di gestire dinamicamente l'appartenenza ai gruppi multicast. Un dominio multicast IGMP contiene host che utilizzano il protocollo IGMP per partecipare, lasciare e inviare messaggi. AWS supporta il IGMPv2 protocollo e i domini multicast di appartenenza ai gruppi sia IGMP che statici (basati su API).

- Sorgente multicast: interfaccia di rete elastica associata a un' EC2 istanza supportata configurata staticamente per inviare traffico multicast. Un'origine multicast si applica solo alle configurazioni di origine statica.

Un dominio multicast di origine statica contiene host che non utilizzano il protocollo IGMP per unire, abbandonare e inviare messaggi. Si utilizza AWS CLI per aggiungere una fonte e i membri del gruppo. L'origine aggiunta staticamente invia traffico multicast e i membri ricevono traffico multicast.

- Membro del gruppo multicast: un'interfaccia di rete elastica associata a un' EC2 istanza supportata che riceve traffico multicast. Un gruppo multicast dispone di più membri del gruppo. In una configurazione di appartenenza a un gruppo di origine statica, i membri del gruppo multicast possono ricevere solo traffico. In una configurazione di gruppo IGMP, i membri possono sia inviare che ricevere traffico.

Considerazioni

- Transit Gateway Multicast potrebbe non essere adatto per il trading ad alta frequenza o per applicazioni sensibili alle prestazioni. Ti consigliamo vivamente di consultare le quote Multicast per conoscere i limiti. Contatta il tuo account o il team di Solution Architect per una revisione dettagliata dei tuoi requisiti prestazionali.
- Per informazioni sulle regioni supportate, consulta AWS Transit Gateway FAQs.
- Per supportare il multicast è necessario creare un nuovo gateway di transito.
- L'appartenenza a gruppi multicast viene gestita utilizzando Amazon Virtual Private Cloud Console o the AWS CLI o IGMP.
- Una sottorete può trovarsi in un solo dominio multicast.
- Se utilizzi un'istanza non Nitro, devi disabilitare la casella di controllo Source/Dest. Per informazioni sulla disabilitazione del controllo, consulta Changing the source or destination checking nella Amazon EC2 User Guide.
- Un'istanza non Nitro non può essere un mittente multicast.
- Il routing multicast non è supportato sugli allegati Site-to-Site VPN Direct Connect, peering o Transit Gateway Connect.
- Un gateway di transito non supporta la frammentazione dei pacchetti multicast. I pacchetti multicast frammentati vengono eliminati. Per ulteriori informazioni, consulta Unità di trasmissione massima (MTU).
- All'avvio, un host IGMP invia più messaggi JOIN IGMP per unirsi a un gruppo multicast (in genere, 2-3 tentativi). Nel caso improbabile che tutti i messaggi JOIN IGMP vengano persi, l'host non

entrerà a far parte del gruppo multicast del gateway di transito. In tale scenario dovrai riattivare il messaggio JOIN IGMP dall'host utilizzando metodi specifici dell'applicazione.

- L'appartenenza a un gruppo inizia con la ricezione del IGMPv2 JOIN messaggio da parte del gateway di transito e termina con la ricezione del messaggio. IGMPv2 LEAVE Il gateway di transito tiene traccia degli host che sono entrati a far parte correttamente del gruppo. Essendo un router multicast cloud, Transit Gateway invia un IGMPv2 QUERY messaggio a tutti i membri ogni due minuti. Ogni membro invia un IGMPv2 JOIN messaggio in risposta, che è il modo in cui i membri rinnovano la propria iscrizione. Se un membro non risponde a tre query consecutive, il gateway di transito rimuove questa appartenenza da tutti i gruppi di cui si è entrati fa parte. Tuttavia, continua a inviare domande a questo membro per 12 ore prima di rimuoverlo definitivamente dalla sua to-be-queried lista. Un IGMPv2 LEAVE messaggio esplicito rimuove immediatamente e permanentemente l'host da qualsiasi ulteriore elaborazione multicast.
- Il gateway di transito tiene traccia degli host che sono entrati a far parte correttamente del gruppo. In caso di interruzione del gateway di transito, questo continuerà a inviare dati multicast all'host per sette minuti (420 secondi) dopo l'ultimo messaggio JOIN IGMP inviato correttamente. Il gateway di transito continua a inviare query di appartenenza all'host per un massimo di 12 ore o fino a quando non riceve un messaggio LEAVE IGMP dall'host.
- Il gateway di transito invia pacchetti di query di appartenenza a tutti i membri IGMP in modo che possa tenere traccia dell'appartenenza al gruppo multicast. L'IP di origine di questi pacchetti di query IGMP è 0.0.0.0/32, l'IP di destinazione è 224.0.0.1/32 e il protocollo è 2. La configurazione del gruppo di sicurezza sugli host IGMP (istanze) e qualsiasi ACLs configurazione sulle sottoreti host devono consentire questi messaggi del protocollo IGMP.
- Quando l'origine e la destinazione multicast si trovano nello stesso VPC, non è possibile utilizzare i riferimenti ai gruppi di sicurezza per impostare il gruppo di sicurezza di destinazione affinché accetti il traffico dal gruppo di sicurezza di origine.
- Per i gruppi e le sorgenti multicast statici, AWS Transit Gateway rimuove automaticamente i gruppi statici e le fonti ENIs che non esistono più. Questa operazione viene eseguita assumendo periodicamente il ruolo collegato al servizio Transit Gateway da descrivere ENIs nell'account.
- Supporta solo il multicast statico. IPv6 Il multicast dinamico non lo fa.

Routing multicast

Quando si abilita il multicast in un gateway di transito, esso funge da router multicast. Quando a un dominio multicast viene aggiunta una sottorete, tutto il traffico multicast viene inviato al gateway di transito che è associato a quel dominio multicast.

Rete ACLs

Le regole ACL di rete funzionano a livello di sottorete. Si applicano al traffico multicast, poiché i gateway di transito risiedono all'esterno della sottorete. Per ulteriori informazioni, consulta Network ACLs in the Amazon VPC User Guide.

Per il traffico multicast IGMP, le regole minime in entrata sono le seguenti. L'host remoto è l'host che invia il traffico multicast.

Tipo	Protocollo	Crea	Descrizione
Protocollo personalizzato	IGMP(2)	0.0.0.0/32	Query IGMP
Protocollo UDP personalizzato	UDP	Indirizzo IP dell'host remoto	Traffico multicast in entrata

Di seguito sono riportate le regole minime in uscita per IGMP.

Tipo	Protocollo	Destinazione	Descrizione
Protocollo personalizzato	IGMP(2)	224.0.0.2/32	Uscita IGMP
Protocollo personalizzato	IGMP(2)	Indirizzo IP del gruppo multicast	Join IGMP
Protocollo UDP personalizzato	UDP	Indirizzo IP del gruppo multicast	Traffico multicast in uscita

Gruppi di sicurezza

Le regole dei gruppi di sicurezza operano a livello di istanza. Possono essere applicati sia al traffico multicast in entrata che in uscita. Il comportamento è lo stesso del traffico unicast. Per tutte le istanze dei membri del gruppo, è necessario consentire il traffico in ingresso dall'origine del gruppo. Per ulteriori informazioni, consulta Gruppi di sicurezza nella Guida per l'utente di Amazon VPC.

Per il traffico multicast IGMP, è necessario disporre almeno delle seguenti regole in entrata. L'host remoto è l'host che invia il traffico multicast. Non è possibile specificare un gruppo di sicurezza come origine della regola UDP in entrata.

Tipo	Protocollo	Crea	Descrizione
Protocollo personalizzato	2	0.0.0.0/32	Query IGMP
Protocollo UDP personalizzato	UDP	Indirizzo IP dell'host remoto	Traffico multicast in entrata

Per il traffico multicast IGMP, è necessario disporre almeno delle seguenti regole in uscita.

Tipo	Protocollo	Destinazione	Descrizione
Protocollo personalizzato	2	224.0.0.2/32	Uscita IGMP
Protocollo personalizzato	2	Indirizzo IP del gruppo multicast	Join IGMP
Protocollo UDP personalizzato	UDP	Indirizzo IP del gruppo multicast	Traffico multicast in uscita

Domini multicast in AWS Transit Gateway

Un dominio multicast consente la segmentazione di una rete multicast in diversi domini. Per iniziare a utilizzare il multicast con un gateway di transito, crea un dominio multicast e associa quindi le sottoreti al dominio.

Attributi di dominio multicast

Nella tabella seguente vengono descritti in dettaglio gli attributi del dominio multicast. Non è possibile abilitare entrambi gli attributi contemporaneamente.

Attributo	Descrizione
`Igmpv2Support` (AWS CLI) IGMPv2 supporto (console)	Questo attributo determina il modo in cui i membri del gruppo si uniscono o abbandonano un gruppo multicast. Quando questo attributo è disattivato, è necessario aggiungere manualmente i membri del gruppo al dominio. Abilita questo attributo se almeno un membro utilizza il protocollo IGMP. I membri si uniscono al gruppo multicast in uno dei seguenti modi: • I membri che supportano IGMP utilizzano i messaggi `JOIN` e `LEAVE`. • I membri che non supportano IGMP devono essere aggiunti o rimossi dal gruppo utilizzando la console Amazon VPC o la AWS CLI. Se registri membri del gruppo multicast, è necessario anche annullarne la registrazione. Il gateway di transito ignora un messaggio `LEAVE` IGMP inviato da un membro del gruppo aggiunto manualmente.
`StaticSourcesSupport` (AWS CLI) Supporto per origini statiche (console)	Questo attributo determina se esistono origini multicast statiche per il gruppo. Quando questo attributo è abilitato, è necessario aggiungere sorgenti per un dominio multicast utilizzando register-transit-gateway-multicast-group-sources. Solo le origini multicast possono inviare traffico multicast. Quando questo attributo è impostato su disabilitato, non esistono origini multicast designate. Tutte le istanze presenti nelle sottoreti associate al dominio multicast possono inviare traffico multicast e i membri del gruppo ricevono traffico multicast.

Creare un dominio multicast IGMP in AWS Transit Gateway

Se non lo hai già fatto, esamina gli attributi del dominio multicast disponibili. Per ulteriori informazioni, consulta the section called “Domini multicast”.

Per creare un dominio multicast IGMP utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Allegati del gateway di transito).
3. Scegliere Crea dominio multicast gateway di transito.
4. Per Name tag (Tag nome) immettere un nome per il dominio.
5. Per ID gateway di transito, seleziona il gateway di transito che elabora il traffico multicast.
6. Per IGMPv2 assistenza, seleziona la casella di controllo.
7. Per il supporto delle fonti statiche, deseleziona la casella di controllo.
8. Per accettare automaticamente le associazioni di sottoreti tra account per questo dominio multicast, seleziona Accetta automaticamente associazioni condivise.
9. Scegliere Crea dominio multicast gateway di transito.

Per creare un dominio multicast IGMP utilizzando AWS CLI

Utilizzate il comando create-transit-gateway-multicast-domain.

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

Crea un dominio multicast di origine statica in AWS Transit Gateway

Se non lo hai già fatto, esamina gli attributi del dominio multicast disponibili. Per ulteriori informazioni, consulta the section called “Domini multicast”.

Per creare un dominio multicast statico utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Allegati del gateway di transito).

3. Scegliere Crea dominio multicast gateway di transito.
4. (Facoltativo) Per Tag nome, specifica un nome per identificare il dominio.
5. Per ID gateway di transito, seleziona il gateway di transito che elabora il traffico multicast.
6. Per IGMPv2 assistenza, deseleziona la casella di controllo.
7. Per il supporto delle fonti statiche, seleziona la casella di controllo.
8. Per accettare automaticamente le associazioni di sottoreti tra account per questo dominio multicast, seleziona Accetta automaticamente associazioni condivise.
9. Scegliere Crea dominio multicast gateway di transito.

Per creare un dominio multicast statico utilizzando AWS CLI

Utilizzate il comando create-transit-gateway-multicast-domain.

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

Associazione di allegati e sottoreti VPC a un dominio multicast in Transit Gateway AWS

Utilizzare la procedura seguente per associare un allegato VPC a un dominio multicast. Quando si crea un'associazione, è possibile selezionare le sottoreti da includere nel dominio multicast.

Prima di iniziare, è necessario creare un allegato VPC sul gateway di transito. Per ulteriori informazioni, consulta Allegati Amazon VPC in Transit Gateway AWS.

Per associare allegati VPC a un dominio multicast utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Allegati del gateway di transito).
3. Seleziona il dominio multicast, quindi scegli Operazioni, Crea associazione.
4. Per Scegli l'allegato da associare, selezionare l'allegato del gateway di transito.
5. In Scegli sottoreti da associare, seleziona le sottoreti da includere nel dominio.
6. Selezionare Create association (Crea associazione).

Per associare gli allegati VPC a un dominio multicast utilizzando il AWS CLI

Utilizzare il comando -domainassociate-transit-gateway-multicast.

Dissociare una sottorete da un dominio multicast in Transit Gateway AWS

Utilizza la procedura riportata di seguito per dissociare le sottoreti da un dominio multicast.

Per disassociare le sottoreti utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Allegati del gateway di transito).
3. Seleziona il dominio multicast.
4. Scegliere la scheda Associations (Associazioni).
5. Selezionare la sottorete, quindi scegli Operazioni,Elimina associazione.

Per dissociare le sottoreti utilizzando il AWS CLI

Utilizzate il comando -domaindisassociate-transit-gateway-multicast.

Visualizza le associazioni di domini multicast in AWS Transit Gateway

Visualizza i tuoi domini multicast per verificare che siano disponibili e che contengano le sottoreti e gli allegati appropriati.

Per visualizzare un dominio multicast utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Allegati del gateway di transito).
3. Seleziona il dominio multicast.
4. Scegliere la scheda Associations (Associazioni).

Per visualizzare un dominio multicast utilizzando AWS CLI

Utilizzate il comando describe-transit-gateway-multicast-domains.

Aggiungere tag a un dominio multicast in AWS Transit Gateway

Aggiungi tag alle risorse per aiutarti a organizzarle e identificarle, differenziandole ad esempio per scopo, proprietario o ambiente. Puoi aggiungere più tag a ciascun dominio multicast. Le chiavi di tag devono essere univoche per ogni dominio multicast. Se aggiungi un tag con una chiave già associata al dominio multicast, il valore del tag viene aggiornato. Per ulteriori informazioni, consulta Tagging your Amazon EC2 Resources.

Per aggiungere tag a un dominio multicast utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Allegati del gateway di transito).
3. Seleziona il dominio multicast.
4. Scegliere Actions (Operazioni), Manage tags (Gestisci tag).
5. (Facoltativo) Per ogni tag, seleziona Aggiungi nuovo tag e immetti una chiave e un valore per il tag.
6. Scegli Save (Salva).

Per aggiungere tag a un dominio multicast utilizzando il AWS CLI

Utilizzare il comando crea tag.

Eliminare un dominio multicast in AWS Transit Gateway

Utilizza la procedura riportata di seguito per eliminare un dominio multicast.

Per eliminare un dominio multicast utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Allegati del gateway di transito).
3. Seleziona il dominio multicast, quindi scegli Operazioni, Elimina dominio multicast.
4. Quando viene richiesta la conferma, immettere **`delete`** e quindi scegliere Elimina.

Per eliminare un dominio multicast utilizzando AWS CLI

Utilizzate il comando delete-transit-gateway-multicast-domain.

Domini multicast condivisi in AWS Transit Gateway

Con la condivisione di domini multicast, i proprietari di domini multicast possono condividere il dominio con altri account AWS all'interno della propria organizzazione in AWS Organizations. In qualità di proprietario del dominio multicast, puoi creare e gestire il dominio multicast a livello centrale. Una volta condivise, tali utenti possono eseguire le seguenti operazioni su un dominio multicast condiviso:

- Registrare e annullare la registrazione dei membri del gruppo o delle origini del gruppo nel dominio multicast
- Associare una sottorete al dominio multicast e dissociare le sottoreti dal dominio multicast

Un proprietario di dominio multicast può condividere un dominio multicast con:

- AWS account all'interno della propria organizzazione o tra organizzazioni in AWS Organizations
- Un'unità organizzativa all'interno della propria organizzazione in AWS Organizations
- La sua intera organizzazione in AWS Organizations
- AWS conti esterni a AWS Organizations.

  Per condividere un dominio multicast con un AWS account esterno all'organizzazione, è necessario creare una condivisione di risorse utilizzando AWS Resource Access Manager e quindi scegliere Consenti la condivisione con chiunque quando selezioni i Principali con cui condividere il dominio multicast. Per ulteriori informazioni sulla creazione di una condivisione di risorse, consulta Creazione di una condivisione di risorse AWS RAM nella Guida per l'utente di AWS RAM .

Indice

- Annulla la condivisione di un dominio multicast condiviso in AWS Transit Gateway
- Identifica un dominio multicast condiviso in AWS Transit Gateway

Prerequisiti per la condivisione di un dominio multicast

- Per condividere un dominio multicast, devi possederlo nel tuo account. AWS Non puoi condividere un dominio multicast che è stato condiviso.
- Per condividere un dominio multicast con la tua organizzazione o un'unità organizzativa in AWS Organizations, devi abilitare la condivisione con. AWS Organizations Per ulteriori informazioni, consulta Abilita la condivisione con AWS Organizations nella Guida per l'utente AWS RAM .

Servizi correlati

La condivisione di domini multicast si integra con AWS Resource Access Manager ().AWS RAM AWS RAM è un servizio che ti consente di condividere AWS le tue risorse con qualsiasi AWS account o tramite. AWS Organizations Con AWS RAM, condividi le risorse di cui sei proprietario creando una condivisione delle risorse. Una condivisione di risorse specifica le risorse da condividere e gli utenti con cui condividerle. I consumatori possono essere singoli AWS account, unità organizzative o un'intera organizzazione. AWS Organizations

Per ulteriori informazioni in merito AWS RAM, consulta la Guida AWS RAM per l'utente.

Autorizzazioni del dominio multicast condiviso

Autorizzazioni per i proprietari

I proprietari sono responsabili della gestione del dominio multicast e dei membri e degli allegati che registrano o associano al dominio. I proprietari possono modificare o revocare l'accesso condiviso in qualsiasi momento. Possono utilizzare AWS Organizations per visualizzare, modificare ed eliminare le risorse create dai consumatori su domini multicast condivisi.

Autorizzazioni per gli utenti

Gli utenti del dominio multicast condiviso possono eseguire le seguenti operazioni sui domini multicast condivisi nello stesso modo in cui lo farebbero sui domini multicast da loro creati:

- Registrare e annullare la registrazione dei membri del gruppo o delle origini del gruppo nel dominio multicast
- Associare una sottorete al dominio multicast e dissociare le sottoreti dal dominio multicast

I consumer sono responsabili della gestione delle risorse create nel dominio multicast condiviso.

I clienti non possono visualizzare o modificare le risorse di proprietà di altri consumer o del proprietario del dominio multicast e non possono modificare i domini multicast con loro condivisi.

Fatturazione e misurazione

Non sono previsti costi aggiuntivi per la condivisione di domini multicast per il proprietario o per i consumer.

Quote

Un dominio multicast condiviso viene conteggiato ai fini delle quote di dominio multicast del proprietario e dell'utente condiviso.

Condividi le risorse tra le zone di disponibilità in AWS Transit Gateway

Per garantire che le risorse siano distribuite tra le zone di disponibilità di una regione, AWS Transit Gateway mappa in modo indipendente le zone di disponibilità ai nomi di ciascun account. Questo potrebbe comportare una diversa denominazione delle zone di disponibilità tra i diversi account. Ad esempio, la zona `us-east-1a` di disponibilità del tuo AWS account potrebbe non avere la stessa posizione `us-east-1a` di un altro AWS account.

Per individuare la posizione del dominio multicast relativamente ai tuoi account, devi utilizzare l'ID della zona di disponibilità (ID AZ). L'ID AZ è un identificatore univoco e coerente per una zona di disponibilità per tutti gli AWS account. Ad esempio, `use1-az1` è un ID AZ per la `us-east-1` regione ed è la stessa posizione in ogni AWS account.

Per visualizzare la AZ IDs per le zone di disponibilità nel tuo account

1. Apri la AWS RAM console a https://console.aws.amazon.com/ram/casa.
2. Le AZ IDs per la regione corrente vengono visualizzate nel pannello Your AZ ID sul lato destro dello schermo.

Condividi un dominio multicast in AWS Transit Gateway

Quando un proprietario condivide un dominio multicast con te, puoi fare quanto segue:

- Registrare e annullare la registrazione dei membri del gruppo o delle origini del gruppo
- Associare e dissociare sottoreti

> **Note**
>
> Per condividere un dominio multicast, dovrai aggiungerlo a una condivisione di risorse. Una condivisione di risorse è una AWS RAM risorsa che consente di condividere le risorse tra AWS account. Una condivisione di risorse specifica le risorse da condividere e i consumatori con cui sono condivise. Quando condividi un dominio multicast utilizzando il Amazon Virtual Private Cloud Console, lo aggiungi a una condivisione di risorse esistente. Per aggiungere il dominio multicast a una nuova condivisione di risorse, dovrai innanzitutto creare la condivisione di risorse tramite la console AWS RAM.
> Se fai parte di un'organizzazione AWS Organizations e la condivisione all'interno dell'organizzazione è abilitata, ai consumatori dell'organizzazione viene automaticamente concesso l'accesso al dominio multicast condiviso. In caso contrario, i consumer ricevono l'invito a partecipare alla condivisione di risorse e, dopo averlo accettato, ottengono l'accesso al dominio multicast condiviso.

Puoi condividere un dominio multicast di tua proprietà utilizzando la Amazon Virtual Private Cloud console, la AWS RAM console o il. AWS CLI

Per condividere un dominio multicast di tua proprietà utilizzando la *Amazon Virtual Private Cloud Console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, seleziona Domini multicast.
3. Seleziona il dominio multicast, quindi scegli Operazioni, Condividi dominio multicast.
4. Seleziona la condivisione di risorse e scegli Condividi dominio multicast.

Per condividere un dominio multicast di tua proprietà utilizzando la console AWS RAM

Consulta Creazione di una condivisione di risorse in Guida per l'utente di AWS RAM .

Per condividere un dominio multicast di tua proprietà utilizzando il AWS CLI

Utilizza il comando create-resource-share.

Annulla la condivisione di un dominio multicast condiviso in AWS Transit Gateway

Quando un dominio multicast condiviso non viene più condiviso, per le risorse del dominio multicast del consumer si verifica quanto segue:

- Le sottoreti del consumer vengono dissociate dal dominio multicast. Le sottoreti rimangono nell'account del consumer.
- Le origini dei gruppi di consumer e i membri del gruppo vengono dissociati dal dominio multicast e quindi eliminati dall'account del consumer.

Per annullare la condivisione di un dominio multicast, devi rimuoverlo dalla condivisione di risorse. Puoi farlo dalla AWS RAM console o dal AWS CLI.

Per annullare la condivisione di un dominio multicast condiviso di tua proprietà, devi rimuoverlo dalla condivisione di risorse. È possibile eseguire questa operazione utilizzando Amazon Virtual Private Cloud, AWS RAM console o AWS CLI.

Per annullare la condivisione di un dominio multicast condiviso di proprietà utilizzando la *Amazon Virtual Private Cloud Console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, seleziona Domini multicast.
3. Seleziona il dominio multicast, quindi scegli Operazioni, Interrompi condivisione.

Per annullare la condivisione di un dominio multicast condiviso di tua proprietà utilizzando la console AWS RAM

Consulta Aggiornamento di una condivisione di risorse in Guida per l'utente di AWS RAM .

Per annullare la condivisione di un dominio multicast condiviso di tua proprietà utilizzando il AWS CLI

Utilizza il comando disassociate-resource-share.

Identifica un dominio multicast condiviso in AWS Transit Gateway

I proprietari e i consumatori possono identificare i domini multicast condivisi utilizzando e Amazon Virtual Private Cloud AWS CLI

Per identificare un dominio multicast condiviso utilizzando la *Amazon Virtual Private Cloud Console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, seleziona Domini multicast.
3. Seleziona il dominio multicast.

4. Nella pagina Dettagli del dominio multicast di transito, visualizza l'ID proprietario per identificare l'ID AWS account del dominio multicast.

Per identificare un dominio multicast condiviso utilizzando il AWS CLI

Utilizzate il comando describe-transit-gateway-multicast-domains. Il comando restituisce i domini multicast di tua proprietà e i domini multicast condivisi con te. `OwnerId`mostra l'ID dell' AWS account del proprietario del dominio multicast.

Registra le fonti con un gruppo multicast in AWS Transit Gateway

> **Note**
>
> Questa procedura è necessaria solo se l'attributo Supporto origini statiche è stato impostato su enable.

Utilizzare la procedura seguente per registrare le origini con un gruppo multicast. L'origine è l'interfaccia di rete che invia il traffico multicast.

Prima di aggiungere un'origine, sono necessarie le seguenti informazioni:

- L'ID del dominio multicast
- Le IDs interfacce di rete dei sorgenti
- L'indirizzo IP del gruppo multicast

Per registrare le origini utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Allegati del gateway di transito).
3. Seleziona il dominio multicast, quindi scegli Operazioni, Aggiungi origini gruppo.
4. Per l'indirizzo IP di gruppo, inserisci il blocco IPv4 CIDR o IPv6 il blocco CIDR da assegnare al dominio multicast.
5. In Choose network interfaces (Scegli interfacce di rete), selezionare le interfacce di rete dei mittenti multicast.

6. Scegliere Add sources (Aggiungi origini).

Per registrare le fonti utilizzando il AWS CLI

Utilizzate il comando register-transit-gateway-multicast-group-sources.

Registrare i membri con un gruppo multicast in AWS Transit Gateway

Utilizzare la procedura seguente per registrare i membri del gruppo con un gruppo multicast.

Prima di aggiungere membri, sono necessarie le seguenti informazioni:

- L'ID del dominio multicast
- Le IDs interfacce di rete dei membri del gruppo
- L'indirizzo IP del gruppo multicast

Per registrare i membri utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Allegati del gateway di transito).
3. Seleziona il dominio multicast, quindi scegli Operazioni, Aggiungi membri del gruppo.
4. Per l'indirizzo IP del gruppo, inserisci il blocco IPv4 CIDR o il blocco IPv6 CIDR da assegnare al dominio multicast.
5. In Choose network interfaces (Scegli interfacce di rete), selezionare le interfacce di rete dei ricevitori multicast.
6. Scegliere Add members (Aggiungi membri).

Per registrare i membri utilizzando il AWS CLI

Utilizzare il comando register-transit-gateway-multicast-group-members.

Annulla la registrazione delle fonti da un gruppo multicast in Transit Gateway AWS

Non è necessario seguire questa procedura a meno che non sia stata aggiunta manualmente un'origine al gruppo multicast.

Per rimuovere un'origine utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Allegati del gateway di transito).
3. Seleziona il dominio multicast.
4. Scegliere la scheda Groups (Gruppi).
5. Selezionare le origini, quindi scegliere Remove source (Rimuovi origine).

Per rimuovere una fonte usando il AWS CLI

Utilizzate il comando deregister-transit-gateway-multicast-group-sources.

Annullare la registrazione dei membri di un gruppo multicast in Transit Gateway AWS

Non è necessario seguire questa procedura a meno che non sia stato aggiunto manualmente un membro al gruppo multicast.

Per annullare la registrazione dei membri utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Allegati del gateway di transito).
3. Seleziona il dominio multicast.
4. Scegliere la scheda Groups (Gruppi).
5. Selezionare i membri, quindi scegliere Remove member (Rimuovi membro).

Per annullare la registrazione dei membri utilizzando il AWS CLI

Utilizzare il comando deregister-transit-gateway-multicast-group-members.

Visualizza i gruppi multicast in AWS Transit Gateway

È possibile visualizzare le informazioni sui gruppi multicast per verificare che i membri siano stati scoperti utilizzando il IGMPv2 protocollo. Il tipo di membro (nella console) o `MemberType` (nella AWS CLI) visualizza IGMP quando vengono AWS rilevati membri con il protocollo.

Per visualizzare gruppi multicast utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, selezionare Transit Gateway Attachments (Allegati del gateway di transito).
3. Seleziona il dominio multicast.
4. Scegliere la scheda Groups (Gruppi).

Per visualizzare i gruppi multicast utilizzando il AWS CLI

Utilizzate il comando search-transit-gateway-multicast-groups.

Nell'esempio seguente viene riportato che il protocollo IGMP ha rilevato membri del gruppo multicast.

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

Configurare il multicast per Windows Server in AWS Transit Gateway

Sarà necessario eseguire passaggi aggiuntivi per configurare il multicast (trasmissione uno a molti) per funzionare con i gateway di transito su Windows Server 2019 o 2022. Per configurarlo dovrai usare PowerShell ed eseguire i seguenti comandi:

Per configurare il multicast per Windows Server utilizzando PowerShell

1. Modificare Windows Server per utilizzarlo IGMPv2 anziché IGMPv3 per lo TCP/IP stack:

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

> **Note**
>
> `New-ItemProperty`è un indice di proprietà che specifica la versione IGMP. Poiché IGMP v2 è la versione supportata per il multicast, la proprietà deve essere. `Value 3` Invece di modificare il registro di Windows, è possibile eseguire il comando seguente per impostare la versione IGMP su 2. :
> `Set-NetIPv4Protocol -IGMPVersion Version2`

2. Per impostazione predefinita, Windows Firewall elimina la maggior parte del traffico UDP. Per prima cosa devi verificare quale profilo di connessione viene utilizzato per il multicast (trasmissione uno a molti):

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

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

3. Aggiorna il profilo di connessione dal passaggio precedente per consentire l'accesso alle porte UDP richieste:

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

4. Riavviare l' EC2 istanza.
5. Esegui il test della tua applicazione multicast (trasmissione uno a molti) per assicurarti che il traffico scorra come previsto.

Esempio: gestione delle configurazioni IGMP utilizzando AWS Transit Gateway

Questo esempio mostra almeno un host che utilizza il protocollo IGMP per il traffico multicast. AWS crea automaticamente il gruppo multicast quando riceve un `JOIN` messaggio IGMP da un'istanza, quindi aggiunge l'istanza come membro di questo gruppo. È inoltre possibile aggiungere staticamente host non IGMP come membri a un gruppo utilizzando. AWS CLI Tutte le istanze presenti nelle

sottoreti associate al dominio multicast possono inviare traffico e i membri del gruppo ricevono il traffico multicast.

Completa la procedura riportata di seguito per questa configurazione.

1. Creare un VPC. Per ulteriori informazioni, consulta Crea un VPC nella Guida per l'utente di Amazon VPC.
2. Crea una sottorete nel VPC. Per ulteriori informazioni, consulta Creare una sottorete nella Amazon VPC User Guide.
3. Crea un gateway di transito configurato per il traffico multicast. Per ulteriori informazioni, consulta the section called “Creazione di un gateway di transito”.
4. Elimina un collegamento a un VPC. Per ulteriori informazioni, consulta the section called “Creare un allegato VPC”.
5. Crea un dominio multicast configurato per il supporto IGMP. Per ulteriori informazioni, consulta the section called “Creare un dominio multicast IGMP”.

   Utilizzare le seguenti impostazioni:

   - Abilita IGMPv2 il supporto.
   - Disabilita Supporto per origini statiche.
6. Crear un'associazione tra sottoreti nell'allegato VPC del gateway di transito e nel dominio multicast. Per ulteriori informazioni, consultare the section called “Associazione di allegati VPC e sottoreti a un dominio multicast”.
7. La versione IGMP predefinita per EC2 è IGMPv3. È necessario modificare la versione per tutti i membri del gruppo IGMP. È anche possibile emettere il seguente comando:

   ```
   sudo sysctl net.ipv4.conf.eth0.force_igmp_version=2
   ```
8. Aggiungi i membri che non utilizzano il protocollo IGMP al gruppo multicast. Per ulteriori informazioni, consulta the section called “Registrare membri con un gruppo multicast”.

Esempio: gestione delle configurazioni di origine statica in AWS Transit Gateway

Questo esempio aggiunge staticamente sorgenti multicast a un gruppo. Gli host non utilizzano il protocollo IGMP per unire o abbandonare gruppi multicast. Dovrai aggiungere staticamente i membri del gruppo che ricevono il traffico multicast.

Completa la procedura riportata di seguito per questa configurazione.

1. Creare un VPC. Per ulteriori informazioni, consulta Crea un VPC nella Guida per l'utente di Amazon VPC.
2. Crea una sottorete nel VPC. Per ulteriori informazioni, consulta Creare una sottorete nella Amazon VPC User Guide.
3. Crea un gateway di transito configurato per il traffico multicast. Per ulteriori informazioni, consulta the section called “Creazione di un gateway di transito”.
4. Elimina un collegamento a un VPC. Per ulteriori informazioni, consulta the section called “Creare un allegato VPC”.
5. Crea un dominio multicast configurato senza supporto IGMP e supporto per l'aggiunta statica di origini. Per ulteriori informazioni, consulta the section called “Crea un dominio multicast di origine statica”.

   Utilizzare le seguenti impostazioni:

   - Disattiva IGMPv2 il supporto.
   - Per aggiungere manualmente le origini, imposta Supporto origini statiche.

     Le origini sono le uniche risorse che possono inviare traffico multicast quando l'attributo è impostato su abilitato. In caso contrario, tutte le istanze presenti nelle sottoreti associate al dominio multicast possono inviare traffico multicast e i membri del gruppo ricevono il traffico multicast.
6. Crear un'associazione tra sottoreti nell'allegato VPC del gateway di transito e nel dominio multicast. Per ulteriori informazioni, consultare the section called “Associazione di allegati VPC e sottoreti a un dominio multicast”.
7. Se imposti l'attributo Supporto origini statiche, aggiungi l'origine al gruppo multicast. Per ulteriori informazioni, consultare the section called “Registrare le origini con un gruppo multicast”.

8. Aggiungere i membri al gruppo multicast. Per ulteriori informazioni, consulta the section called “Registrare membri con un gruppo multicast”.

Esempio: gestione delle configurazioni statiche dei membri del gruppo in AWS Transit Gateway

Questo esempio mostra l'aggiunta statica di membri multicast a un gruppo. Gli host non possono utilizzare il protocollo IGMP per unire o abbandonare gruppi multicast. Tutte le istanze presenti nelle sottoreti associate al dominio multicast possono inviare traffico multicast e i membri del gruppo ricevono traffico multicast.

Completa la procedura riportata di seguito per questa configurazione.

1. Creare un VPC. Per ulteriori informazioni, consulta Crea un VPC nella Guida per l'utente di Amazon VPC.
2. Crea una sottorete nel VPC. Per ulteriori informazioni, consulta Creare una sottorete nella Amazon VPC User Guide.
3. Crea un gateway di transito configurato per il traffico multicast. Per ulteriori informazioni, consulta the section called “Creazione di un gateway di transito”.
4. Elimina un collegamento a un VPC. Per ulteriori informazioni, consulta the section called “Creare un allegato VPC”.
5. Crea un dominio multicast configurato senza supporto IGMP e supporto per l'aggiunta statica di origini. Per ulteriori informazioni, consulta the section called “Crea un dominio multicast di origine statica”.

   Utilizzare le seguenti impostazioni:

   - Disattiva IGMPv2 il supporto.
   - Disabilita Supporto per origini statiche.
6. Crear un'associazione tra sottoreti nell'allegato VPC del gateway di transito e nel dominio multicast. Per ulteriori informazioni, consultare the section called “Associazione di allegati VPC e sottoreti a un dominio multicast”.
7. Aggiungere i membri al gruppo multicast. Per ulteriori informazioni, consulta the section called “Registrare membri con un gruppo multicast”.

Allocazione flessibile dei costi

Per impostazione predefinita, transit gateway utilizza un modello di allocazione dei costi basato sul mittente in cui i costi di elaborazione dei dati vengono assegnati all'account proprietario dell'allegato di origine. È possibile creare politiche di misurazione personalizzate che definiscono quali account devono essere addebitati in base alle proprietà del flusso di traffico, come tipi di allegati, allegati specifici o indirizzi di rete. IDs

Le politiche di misurazione sono costituite da regole ordinate che vengono valutate dal numero di regole più basso a quello più alto. Quando il traffico corrisponde a una regola, all'account specificato viene addebitato l'importo in base alla configurazione della regola. È possibile specificare il proprietario dell'account per l'allocazione dei costi tra le seguenti opzioni:

- Proprietario dell'allegato di origine: gli addebiti vengono assegnati all'account proprietario dell'allegato di origine (comportamento predefinito)
- Proprietario dell'allegato di destinazione: gli addebiti vengono assegnati all'account proprietario dell'allegato di destinazione
- Proprietario del Transit Gateway: gli addebiti vengono assegnati all'account proprietario del gateway di transito

L'allocazione flessibile dei costi consente una migliore gestione dei costi per le organizzazioni che utilizzano architetture di rete centralizzate, consentendo di allocare i costi alle unità aziendali o ai proprietari delle applicazioni appropriate indipendentemente dalla topologia di rete.

> **Note**
>
> L'allocazione flessibile dei costi consente un'allocazione flessibile dell'utilizzo della misurazione e, a sua volta, dei costi ai titolari degli account di vostra scelta. Tuttavia, le implicazioni fiscali per AWS gli account possono variare in modo significativo in base alla posizione geografica, ai modelli di utilizzo e ad altri fattori. Prima di attivare questa funzionalità, consulta le implicazioni relative alla fatturazione, alle tasse e alla gestione dei costi per gli account della tua AWS organizzazione. Riferimento: Che cos'è AWS Billing and Cost Management?

Politiche di misurazione

Le politiche di misurazione consentono di configurare le regole di allocazione dei costi per il gateway di transito per controllare a quali account vengono addebitati i costi di elaborazione e trasferimento dei dati in base alle proprietà del flusso di traffico. Questa funzionalità consente una migliore gestione dei costi e funzionalità di chargeback per le organizzazioni che utilizzano architetture di rete centralizzate.

Una politica di misurazione è composta dai seguenti elementi:

- Politica di misurazione: il contenitore di configurazione generale che contiene le regole della politica di misurazione. Una volta creato, contiene un'unica voce predefinita della politica di misurazione configurata per addebitare tutto il traffico al proprietario dell'allegato di origine. Ogni gateway di transito può avere una sola politica di misurazione.
- Inserimento della politica di misurazione: regole individuali all'interno di una politica di misurazione che definiscono criteri di corrispondenza specifici e l'utilizzo dell'account da misurare. Ogni voce include un numero di regola per l'ordine di valutazione, le condizioni di corrispondenza del traffico (ad esempio tipi di allegati di origine e destinazione IDs, allegati, blocchi CIDR, porte e protocolli) e il proprietario dell'account addebitare per il traffico corrispondente. Una policy può contenere fino a 50 voci, valutate in base al numero di regole più basso a quello più alto.

  È possibile assegnare l'utilizzo della misurazione a uno dei seguenti elementi:

  - Proprietario dell'allegato di origine: alloca l'utilizzo della misurazione all'account proprietario dell'allegato da cui proviene il traffico (comportamento predefinito)
  - Proprietario dell'allegato di destinazione: alloca l'utilizzo della misurazione all'account proprietario dell'allegato da cui termina il traffico e
  - proprietario del gateway di transito: alloca l'utilizzo della misurazione all'account proprietario del gateway di transito.
- Allegati Middlebox: (Facoltativi) Allegati del gateway di transito designati che instradano il traffico attraverso le apparecchiature di rete per l'ispezione di sicurezza, il bilanciamento del carico o altre funzioni di rete. L'utilizzo dei dati per il traffico che attraversa gli allegati middlebox viene misurato in base al proprietario dell'account specificato nella politica di misurazione. Puoi specificare un massimo di 10 allegati middlebox. I tipi di allegati middlebox supportati sono gli allegati Network Function (AWS Network Firewall), VPC e VPN.

Come funzionano le politiche di misurazione

Per impostazione predefinita, transit gateway utilizza un modello di allocazione dei costi basato sul mittente in cui i costi di elaborazione dei dati vengono contabilizzati sull'account proprietario dell'allegato di origine. Con le politiche di misurazione, puoi creare regole personalizzate per misurare in modo flessibile l'utilizzo in base alle seguenti proprietà del flusso di traffico:

- Tipi di allegati di origine e destinazione (VPC, VPN, Direct Connect Gateway, Peering, Network Function e VPN Concentrator)
- Allegato di origine e destinazione IDs
- Indirizzi IP di origine e destinazione, intervalli di porte e protocolli

Le politiche di misurazione sono costituite da regole ordinate che vengono valutate dal numero di regole più basso a quello più alto. Quando il traffico corrisponde a una regola, all'account specificato viene addebitato l'importo in base all'impostazione dell'account misurato della regola. Le politiche di misurazione riguardano diversi scenari organizzativi comuni:

- Allocazione dei costi dell'ambiente ibrido: alloca i costi per l'immissione dei dati AWS da locale tramite Direct Connect Gateway al proprietario dell'account VPC di destinazione anziché al proprietario dell'account amministratore IT centrale.
- Architettura di ispezione centralizzata: alloca i costi ai proprietari delle singole applicazioni o degli account VPC anziché al team di sicurezza centrale per l'attraversamento del traffico tramite ispezione. VPCs
- Chargeback basato sulle applicazioni: alloca tutti i costi di utilizzo dei dati per un carico di lavoro al proprietario del VPC indipendentemente dalla direzione del traffico.
- Allocazione dei costi dei clienti: alloca i costi dei dati agli account dei clienti quando creano allegati al gateway di transito.

Allegati Middlebox

Le policy di misurazione del gateway di transito supportano gli allegati Middlebox, che consentono di allocare in modo flessibile i costi di elaborazione dei dati per il traffico di rete instradato tramite dispositivi middlebox come firewall di rete e sistemi di bilanciamento del carico. Esempi di allegati middlebox sono l'allegato Network Function al AWS Network Firewall o gli allegati VPC che indirizzano il traffico verso dispositivi di sicurezza di terze parti in un VPC. Il traffico tra gli allegati del gateway di transito di origine e di destinazione attraversa questi allegati middlebox per i tipici casi

d'uso delle ispezioni di sicurezza. È possibile definire politiche di misurazione per allocare in modo flessibile l'utilizzo dell'elaborazione dei dati sugli allegati middlebox all'allegato di origine, all'allegato di destinazione finale o al proprietario dell'account Transit Gateway. Per gli allegati Network Function, i costi di elaborazione dei dati del AWS Network Firewall vengono assegnati anche all'account misurato.

Allocazione flessibile dei costi: misurazione dei tipi di utilizzo

L'allocazione flessibile dei costi tramite politiche di misurazione si applica ai seguenti tipi di utilizzo dei dati:

- Utilizzo dell'elaborazione dati del gateway di transito su allegati VPC, VPN, VPN Concentrator e Direct Connect
- Site-to-site Utilizzo del VPN Data Transfer Out sugli allegati VPN
- Utilizzo di Direct Connect Data Transfer Out sugli allegati Direct Connect.
- Utilizzo del trasferimento dati sugli allegati di peering TGW
- Transit Gateway Utilizzo dell'elaborazione dei dati sugli allegati Network Function
- AWS Utilizzo dell'elaborazione dei dati del firewall di rete (NFW) sugli allegati Network Function.

L'allocazione flessibile dei costi non si applica all'utilizzo orario degli allegati e all'utilizzo dell'elaborazione dati multicast. Per gli allegati Transit Gateway Connect, è possibile definire una politica di misurazione per il VPC di trasporto sottostante o l'allegato Direct Connect. Per gli allegati VPN con IP privato, è possibile definire una politica di misurazione per l'allegato Direct Connect di trasporto sottostante.

Considerazioni e limitazioni

Quando implementate le politiche di misurazione per il vostro gateway di transito, tenete presente quanto segue.

Permissions

- Solo il proprietario del gateway di transito può creare, modificare o eliminare le politiche di misurazione.
- Le impostazioni di allocazione dei costi si applicano a livello di gateway di transito.
- I proprietari degli allegati non possono sostituire le impostazioni di allocazione dei costi configurate dal proprietario del gateway di transito.

Peering Transit Gateway

Quando il traffico attraversa le connessioni peering del gateway di transito:

- Ogni gateway di transito applica la propria politica di misurazione in modo indipendente.
- I costi per i dati vengono assegnati separatamente da ciascun gateway di transito in base alla politica locale.
- Il traffico può essere considerato come due flussi distinti: il collegamento della sorgente al peering e il peering all'allegato di destinazione.

Integrazione cloud WAN

Quando un gateway di transito è collegato a una rete centrale Cloud WAN:

- I costi di trasferimento dati del gateway di transito sulle connessioni peering vengono assegnati in base alla politica di misurazione del gateway di transito.
- Le politiche di misurazione non sono supportate sulle reti principali di Cloud WAN.

Impatto sulle prestazioni

- Le politiche di misurazione non introducono alcuna latenza aggiuntiva del percorso dati.
- Le politiche di misurazione non hanno alcun impatto sulla larghezza di banda massima per allegato.
- Non sono state apportate modifiche alle funzionalità di condivisione delle risorse del gateway di transito.

Integrazione della fatturazione

- I tag di allocazione dei costi continuano a funzionare con le politiche di misurazione per l'organizzazione dei costi per unità aziendale.
- Le politiche di misurazione definiscono quali account comportano costi, mentre i tag di allocazione dei costi aiutano a classificare tali costi.
- Le modifiche alle politiche di misurazione entrano in vigore alla fine dell'ora di fatturazione successiva.

IPv6 supporto

Le politiche di misurazione sono supportate sia per il traffico che per IPv4 il IPv6 traffico. La corrispondenza dei blocchi CIDR nelle voci delle policy funziona con entrambe le famiglie di indirizzi.

Supporto per gli allegati Middlebox

- La politica di misurazione di Middlebox presuppone che il traffico tra l'allegato di origine e quello di destinazione venga concentrato tramite l'allegato middlebox specificato (ad esempio, ispezione est-ovest del traffico). VPC-to-VPC Pertanto, le 5 tuple di rete (source/destination IPs, source/destinationporte e protocollo) per i flussi in ingresso e in uscita dagli allegati della casella centrale devono corrispondere. I flussi con mancata corrispondenza di 5 tuple sugli allegati del riquadro centrale (ad esempio la trasformazione NAT in VPC di ispezione) vengono trattati come normali flussi di allegati origine-destinazione (al contrario dei flussi di allegati del riquadro centrale).
- Tutti i flussi di sola uscita sull'allegato middlebox (ad esempio il traffico nord-sud verso Internet tramite IGW in un VPC di ispezione) vengono trattati come normali flussi origine-destinazione (al contrario dei flussi di allegati middlebox).
- Per gli allegati Network Function, quando AWS Network Firewall rilascia i pacchetti, tutto l'utilizzo dell'elaborazione dei dati viene riaddebitato all'account del mittente indipendentemente dalla configurazione della politica di misurazione.

Creare una politica di misurazione del AWS Transit Gateway

Per abilitare le politiche di misurazione, è necessario creare una politica di misurazione per il gateway di transito e configurare voci di policy che definiscano la modalità di allocazione dell'utilizzo dei contatori. La politica di misurazione stabilisce il quadro e le impostazioni predefinite, mentre le voci di policy contengono le regole specifiche che determinano quali account vengono misurati in base alle caratteristiche del traffico.

Le voci relative alle policy di misurazione funzionano come regole ordinate che vengono applicate in sequenza dal numero di regola più basso a quello più alto per il traffico che attraversa il gateway di transito. Ogni voce definisce criteri di corrispondenza come i tipi di allegati di origine e destinazione, i blocchi CIDR, i protocolli e gli intervalli di porte, oltre all'account da misurare per il traffico corrispondente. Quando un flusso di traffico corrisponde a più voci, la voce con il numero di regola più basso ha la precedenza. Se nessuna voce corrisponde a un determinato flusso, viene addebitato l'account di misurazione predefinito specificato nella politica.

Dopo aver creato una politica, dovrai aggiungere voci di policy per implementare la logica di allocazione dei costi. Per i passaggi per creare una voce relativa alla politica di misurazione, consulta. Creare una voce relativa alla politica di misurazione

Crea una politica di misurazione utilizzando la console

Crea una politica per definire regole flessibili di allocazione dei costi per l'utilizzo dei dati del gateway di transito. Per impostazione predefinita, tutti i flussi vengono contabilizzati in base al proprietario dell'allegato di origine. Crea voci per fatturare flussi di rete specifici a diversi account.

Per creare una politica di misurazione

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Politiche di misurazione.
3. Scegli Crea politica di misurazione.
4. Per Transit gateway ID scegli il gateway di transito per il quale desideri creare una politica di misurazione.
5. (Facoltativo) Per l'allegato Middlebox IDs, scegli uno o più allegati middlebox. Per impostazione predefinita, l'utilizzo dei dati viene calcolato in base al proprietario del middlebox. Il supporto degli allegati Middlebox consente di applicare la politica di misurazione per il traffico che attraversa gli allegati middlebox. Gli allegati aggiuntivi possono essere aggiunti in un secondo momento.
6. (Facoltativo) Nella sezione Tag, aggiungi tag per aiutarti a identificare e organizzare la tua politica di misurazione:
   a. Scegli Aggiungi nuovo tag.
   b. Inserisci un tag Key e, facoltativamente, un tag Value.
   c. Scegli Aggiungi nuovo tag per aggiungere altri tag o vai al passaggio successivo. Puoi aggiungere fino a 50 tag.
7. Scegli Crea una politica di misurazione del gateway di transito.

> **Note**
>
> L'account di misurazione predefinito è il proprietario dell'allegato di origine e, dopo aver creato una politica di misurazione, è possibile aggiungere voci che definiscono a quale account viene addebitato l'importo in base alle proprietà del flusso di traffico, tenendo

presente che la voce di policy predefinita (che è l'ultima voce) non può essere modificata o eliminata come le altre voci della politica.

Crea una politica di misurazione utilizzando il AWS CLI

Una politica di misurazione definisce il comportamento predefinito di allocazione dei costi e le impostazioni globali per il gateway di transito. Usa la -policycreate-transit-gateway-metering.

Parametri obbligatori:

- `--transit-gateway-id`- L'ID del gateway di transito per cui creare la politica per

Parametri facoltativi:

- `--middle-box-attachment-ids`- ID degli allegati del gateway di transito supportati da aggiungere alla policy come middlebox
- `--tag-specifications`- tag per la politica di misurazione

Per creare una politica di misurazione utilizzando il AWS CLI

1. Esegui il create-transit-gateway-metering-policy comando per creare una nuova politica di misurazione con allegati middlebox opzionali.

```
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" } ] }]'
```

   Questo comando crea una politica di misurazione per il gateway di transito specificato con gli allegati e i tag middlebox forniti.
2. Il comando restituisce il seguente risultato quando la policy viene creata correttamente:

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

Nota l'ID della politica di misurazione restituito nella risposta per l'utilizzo nei comandi successivi. describe-transit-gateway-metering-policiesil comando può essere utilizzato per ottenere la politica di misurazione associata al gateway di transito.

Gestione delle politiche AWS di misurazione Transit Gateway

Dopo aver creato una politica di misurazione, è possibile gestirla visualizzando le impostazioni correnti, modificando le opzioni di configurazione o eliminando la politica quando non è più necessaria. Le operazioni di gestione consentono di aggiungere o rimuovere gli allegati middlebox man mano che i requisiti di rete cambiano. È possibile creare o eliminare solo una voce di policy. Se è necessario modificare una regola esistente, è possibile eliminare la voce e crearne una nuova con la configurazione modificata. Tutte le operazioni di gestione richiedono le autorizzazioni del proprietario del gateway di transito e hanno effetto dopo due ore di fatturazione.

Una gestione efficace delle politiche di misurazione è fondamentale per mantenere un'accurata allocazione dei costi man mano che l'architettura di rete si evolve. Le organizzazioni spesso devono modificare le proprie politiche quando le unità aziendali cambiano, vengono implementate nuove applicazioni o vengono modificate le topologie di rete. Ad esempio, le impostazioni di supporto del middlebox metering possono richiedere aggiornamenti quando le architetture di sicurezza del firewall cambiano o quando vengono introdotti nuovi servizi di ispezione nel percorso di traffico.

Le modifiche alle policy supportano vari scenari operativi, tra cui cambiamenti stagionali del modello di traffico, attività di fusione e acquisizione e aggiornamenti dei requisiti di conformità. Nella gestione delle politiche, considera l'impatto sugli accordi di fatturazione esistenti e comunica le modifiche alle parti interessate prima dell'implementazione.

Le revisioni periodiche delle politiche aiutano a garantire che l'allocazione dei costi rimanga in linea con gli obiettivi aziendali e le strutture organizzative. Le migliori pratiche includono la documentazione delle modifiche alle politiche, la verifica delle modifiche in ambienti non di produzione, ove possibile,

e il coordinamento con i team finanziari per comprendere le implicazioni di fatturazione. Inoltre, considera la tempistica delle modifiche alle politiche per ridurre al minimo le interruzioni dei cicli di fatturazione mensili e dei processi di rendicontazione finanziaria.

Argomenti

Modificare una AWS politica di misurazione Transit Gateway

Modifica le politiche di misurazione esistenti per modificare le configurazioni degli allegati middlebox. Le modifiche alle politiche entrano in vigore all'ora di fatturazione successiva e si applicano a tutti i flussi di traffico futuri attraverso il gateway di transito.

Modifica una politica di misurazione utilizzando la console

Usa la console per modificare le impostazioni delle politiche di misurazione esistenti per il tuo gateway di transito.

Per modificare una politica di misurazione esistente utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Politiche di misurazione.
3. Seleziona la politica di misurazione che desideri modificare selezionando l'ID della politica
4. Modifica le impostazioni delle politiche disponibili in Azioni. La console consente solo l'aggiunta e la rimozione degli allegati della casella centrale.
    - Allegati Middlebox: aggiungi o rimuovi gli allegati del gateway di transito che devono essere considerati come middlebox per la fatturazione specializzata.

Modifica una politica di misurazione utilizzando il AWS CLI

Utilizzare il modify-transit-gateway-metering-policy comando per visualizzare e modificare le politiche di misurazione.

Parametri richiesti per le operazioni di modifica:

- `--transit-gateway-metering-policy-id`- L'ID della politica di misurazione da modificare

- `--add-middle-box-attachment-ids`oppure `--remove-middle-box-attachment-ids` - ID degli allegati del gateway di transito supportati da aggiungere o rimuovere dalla policy come middlebox

Per visualizzare e modificare le politiche di misurazione utilizzando la CLI AWS

1. (Facoltativo) Visualizza le politiche di misurazione esistenti utilizzando il describe-transit-gateway-metering-policies comando per visualizzare le impostazioni di configurazione correnti:

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

   Questo comando restituisce tutte le politiche di misurazione del tuo account, mostrandone lo stato attuale, e gli allegati abilitati come riquadro intermedio per ciascuna politica di misurazione.

2. Modifica una politica di misurazione utilizzando il comando per aggiornare le opzioni di configurazionemodify-transit-gateway-metering-policy:

   ```
   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
   ```

   Questo comando modifica una politica di misurazione aggiungendo la and/or rimozione degli allegati middlebox.

3. Il comando restituisce il seguente risultato quando la politica viene modificata correttamente:

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

   Le modifiche possono richiedere fino a due ore di fatturazione per avere effetto.

Eliminare una politica di misurazione AWS Transit Gateway

Eliminate le politiche di misurazione quando non sono più necessarie per la strategia di allocazione dei costi del gateway di transito. L'eliminazione di una policy riporta l'allocazione dei costi al modello predefinito basato sul mittente, in cui i costi di elaborazione e trasferimento dei dati vengono allocati all'account proprietario dell'allegato di origine. Vengono inoltre rimosse tutte le voci di policy associate alla politica di misurazione eliminata.

Eliminare una politica di misurazione utilizzando la console

Utilizza la console per rimuovere le politiche di misurazione che non sono più necessarie.

Per eliminare una politica di misurazione utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Politiche di misurazione.
3. Seleziona la politica che desideri eliminare scegliendo l'ID della politica.
4. Scegliere Actions (Operazioni), quindi Delete (Elimina).
5. Conferma l'eliminazione digitando **`delete`** nella finestra di dialogo di conferma.
6. Scegli Elimina.

> **Important**
>
> L'eliminazione di una politica di misurazione è irreversibile. Tutte le voci di policy e le impostazioni di configurazione verranno rimosse definitivamente e l'allocazione dei costi tornerà al modello predefinito basato sul mittente.

Eliminare una politica di misurazione utilizzando il AWS CLI

Utilizzare il delete-transit-gateway-metering-policy comando per eliminare le politiche di misurazione a livello di codice.

Requisiti:

- Autorizzazioni del proprietario del gateway di transito

Parametri obbligatori:

- `--transit-gateway-metering-policy-id`- L'ID della politica di misurazione da eliminare

Per visualizzare ed eliminare le politiche di misurazione utilizzando la CLI AWS

1. (Facoltativo) Visualizza le politiche di misurazione esistenti utilizzando il describe-transit-gateway-metering-policies comando per visualizzare le impostazioni di configurazione correnti:

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

   Questo comando restituisce tutte le politiche di misurazione del tuo account, mostrandone lo stato e la configurazione correnti.

2. Elimina una politica di misurazione utilizzando il delete-transit-gateway-metering-policy comando per rimuovere definitivamente la politica:

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

   Questo comando rimuove definitivamente la politica di misurazione specificata e tutte le voci associate. L'allocazione dei costi tornerà al modello predefinito basato sul mittente per tutti i flussi di traffico futuri. Questa modifica richiede inoltre 2 ore di fatturazione per avere effetto.

3. Il comando restituisce il seguente output quando la policy viene eliminata con successo:

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

   La risposta conferma che la policy viene eliminata con uno `deleting` stato mentre la rimozione viene elaborata attraverso l'infrastruttura del gateway di transito.

Creare una voce relativa alla politica di misurazione del AWS Transit Gateway

Per impostazione predefinita, tutti i flussi vengono contabilizzati in base al proprietario dell'allegato di origine. Per contabilizzare flussi specifici su account diversi, crea voci di policy individuali che definiscono a quale account verrà addebitato l'importo in base alle proprietà del flusso di traffico.

Le voci relative alle politiche di misurazione funzionano come regole condizionali che vengono valutate in ordine sequenziale in base ai numeri delle regole quando il traffico attraversa il gateway di transito. Ogni voce funziona come un'istruzione «if-then»: se il traffico corrisponde ai criteri specificati (come il tipo di allegato di origine, il blocco CIDR di destinazione o il protocollo), addebita l'importo all'account designato. Il sistema valuta le voci dal numero di regola più basso a quello più alto e la prima voce corrispondente determina l'account di fatturazione per quel flusso di traffico.

Le voci supportano un'ampia gamma di criteri di corrispondenza, tra cui tipi di allegati (VPC, VPN, Direct Connect Gateway), allegati specifici IDs, blocchi CIDR di origine e destinazione, tipi di protocollo e intervalli di porte. È possibile combinare più criteri all'interno di una singola voce per creare regole di targeting precise. Ad esempio, potresti creare una voce che corrisponda a tutto il traffico HTTPS (porta 443) dagli allegati VPC a un intervallo CIDR di destinazione specifico e addebiti tali flussi all'account di un team di sicurezza. Se nessuna voce corrisponde a un determinato flusso di traffico, viene addebitato l'account con misurazione predefinito specificato nella politica di misurazione principale, garantendo che tutto il traffico venga fatturato correttamente. La creazione di una voce richiede 2 ore di fatturazione per avere effetto.

> **Important**
>
> - Pianifica attentamente i numeri delle regole: lascia degli spazi vuoti (ad esempio, 10, 20, 30) per consentire inserimenti futuri
> - Verifica le iscrizioni con condizioni meno specifiche prima di aggiungere regole più restrittive
> - Utilizza condizioni di abbinamento specifiche per evitare fatturazioni involontarie

Crea una voce relativa alla politica di misurazione utilizzando la console

Una politica di misurazione definisce il comportamento predefinito di allocazione dei costi e le impostazioni globali per il gateway di transito.

Per creare una voce relativa alla politica di misurazione utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Politiche di misurazione.
3. Seleziona il link ID della politica di misurazione per visualizzarne i dettagli.
4. Scegli la scheda Voci della politica di misurazione.
5. Scegli Crea voce della politica di misurazione.
6. Numero della regola politica: deve essere un numero univoco (1- 32.766) che determina l'ordine di valutazione. I numeri più bassi hanno una priorità più alta.
7. Account misurato: scegli uno dei seguenti tipi di account a cui addebitare i costi per i flussi di traffico corrispondenti:
   a. Proprietario dell'allegato di origine
   b. Proprietario dell'allegato di destinazione
   c. Proprietario dell'allegato Transit Gateway
8. (Facoltativo) Scegli le condizioni della regola: queste condizioni opzionali definiscono i criteri per soddisfare il traffico specifico:
   - Tipo o ID di allegato di origine: filtra per tipo di allegato (VPC, VPN, Direct Connect Gateway, Peering) o ID.
   - Tipo o ID di allegato di destinazione: filtra per tipo o ID di allegato di destinazione
   - Blocco CIDR di origine: abbina il traffico proveniente da intervalli IP specifici
   - Blocco CIDR di destinazione: abbina il traffico a intervalli IP specifici
   - Intervallo di porte di origine: corrisponde a porte di origine specifiche
   - Intervallo di porte di destinazione: corrisponde a porte di destinazione specifiche
   - Protocollo: filtra per protocollo per la regola (1, 6, 17, ecc.)
9. Scegli la voce Crea politica di misurazione per salvare la configurazione.

Crea una voce relativa alla politica di misurazione utilizzando il AWS CLI

Le voci di policy definiscono regole specifiche per l'allocazione dei costi in base alle caratteristiche del traffico. Le regole vengono valutate in base al numero di regole più basso a quello più alto.

Parametri obbligatori:

- `--transit-gateway-metering-policy-id`- L'ID della politica di misurazione a cui aggiungere la voce
- `--policy-rule-number`- Un numero univoco (1-32.766) che determina l'ordine di valutazione
- `--metered-account`- tipo di pagatore (//) source-attachment-owner destination-attachment-owner transit-gateway-owner

Parametri facoltativi:

Questi parametri opzionali che definiscono i criteri per corrispondere al traffico specifico:

- `--source-transit-gateway-attachment-id`- L'ID dell'allegato del gateway di transito di origine.
- `--source-transit-gateway-attachment-type`- Il tipo di allegato del gateway di transito di origine.
- `--source-cidr-block`- Il blocco CIDR di origine della regola.
- `--source-port-range`- L'intervallo di porte di origine per la regola.
- `--destination-transit-gateway-attachment-id`- L'ID dell'allegato del gateway di transito di destinazione.
- `--destination-transit-gateway-attachment-type`- Il tipo di allegato del gateway di transito di destinazione.
- `--destination-cidr-block`- Il blocco CIDR di destinazione per la regola.
- `--destination-port-range`- L'intervallo di porte di destinazione per la regola.
- `--protocol`- Il numero di protocollo per la regola

Per creare una voce relativa alla politica di misurazione utilizzando il AWS CLI

1. Usa il create-transit-gateway-metering-policy-entry comando per creare una nuova voce di policy che indirizza il traffico VPC a un account misurato specifico:

```
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
```

Questo comando crea una voce di policy con la regola numero 100 che corrisponde al traffico destinato agli allegati VPC e addebita al proprietario degli allegati di destinazione tali flussi.

2. Il comando restituisce il seguente output quando la voce viene creata correttamente:

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

La risposta conferma che la voce è stata creata con uno stato «disponibile» mentre veniva attivata attraverso l'infrastruttura del gateway di transito.

Eliminare una voce della politica di misurazione AWS Transit Gateway

Elimina le voci relative alla politica di misurazione quando non sono più necessarie regole specifiche di allocazione dei costi per i flussi di traffico di rete. L'eliminazione delle voci aiuta a semplificare la gestione delle policy rimuovendo le regole obsolete o non necessarie e mantenendo al contempo la struttura generale delle politiche. Quando si elimina una voce, il traffico che in precedenza corrispondeva alla regola eliminata verrà valutato rispetto alle voci rimanenti in ordine numerico di regola, oppure tornerà al comportamento predefinito delle policy se non vi sono altre voci corrispondenti.

Prima di eliminare le voci, considera l'impatto sulle disposizioni di fatturazione e sui flussi di traffico correnti. Una volta eliminata, la modifica richiede fino a 2 ore di fatturazione per diventare effettiva e non può essere annullata, quindi coordina le modifiche con i proprietari degli account e i team finanziari interessati. Controlla le voci rimanenti per garantire la corretta copertura del traffico e l'allocazione della fatturazione dopo l'eliminazione. L'ordine di valutazione delle regole per le voci rimanenti rimane invariato, mantenendo un comportamento prevedibile di allocazione dei costi per flussi di traffico continui.

Important

- L'eliminazione è irreversibile
- Il traffico che in precedenza corrispondeva a questa voce verrà rivalutato rispetto alle entrate rimanenti
- Controlla le voci rimanenti per garantire una copertura del traffico adeguata

Elimina una voce relativa alla politica di misurazione utilizzando la console

Utilizza la console per rimuovere le voci di policy tramite un'interfaccia intuitiva che fornisce finestre di dialogo di conferma per evitare eliminazioni accidentali.

Per eliminare una voce di policy utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Metering policies.
3. Seleziona la politica di misurazione contenente la voce che desideri eliminare.
4. Seleziona la voce che desideri rimuovere e scegli Elimina.
5. Nella finestra di dialogo di conferma, rivedi i dettagli della voce e digita **`delete`** per confermare la rimozione.
6. Scegliete Elimina per rimuovere definitivamente la voce.

Eliminare una voce della politica di misurazione utilizzando il AWS CLI

Utilizzate il delete-transit-gateway-metering-policy-entry comando per rimuovere le voci di policy a livello di codice.

Requisiti:

- Autorizzazioni del proprietario del Transit Gateway
- ID della politica di misurazione e numero della regola di ingresso validi

Parametri obbligatori:

- `--transit-gateway-metering-policy-id`- L'ID della politica di misurazione

- `--policy-rule-number`- Il numero della regola della voce da eliminare

Per visualizzare ed eliminare le voci di policy utilizzando la AWS CLI

1. (Facoltativo) Visualizzate le voci di policy esistenti utilizzando il get-transit-gateway-metering-policy-entries comando per visualizzare le impostazioni di configurazione correnti:

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

   Questo comando restituisce tutte le voci relative alla politica specificata, mostrandone i numeri delle regole, i criteri di corrispondenza e gli account misurati.

2. Eliminare una voce di policy utilizzando il delete-transit-gateway-metering-policy-entry comando per rimuovere definitivamente la voce:

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

   Questo comando rimuove definitivamente la voce specificata dalla politica. Il traffico che in precedenza corrispondeva a questa voce verrà immediatamente rivalutato rispetto alle voci rimanenti o tornerà al comportamento predefinito della policy.

3. Il comando restituisce il seguente output quando la voce viene eliminata con successo:

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

La risposta conferma che la voce viene eliminata con lo stato «eliminato» mentre la rimozione viene elaborata attraverso l'infrastruttura del gateway di transito.

Gestione degli allegati middlebox della politica di misurazione AWS Transit Gateway

Le policy di misurazione del gateway di transito supportano gli allegati Middlebox, che consentono di allocare in modo flessibile i costi di elaborazione dei dati per il traffico di rete instradato tramite dispositivi middlebox come firewall di rete e sistemi di bilanciamento del carico. Esempi di allegati middlebox sono l'allegato Network Function al AWS Network Firewall o gli allegati VPC che indirizzano il traffico verso dispositivi di sicurezza di terze parti in un VPC. Il traffico tra gli allegati del gateway di transito di origine e di destinazione attraversa questi allegati middlebox per i tipici casi d'uso delle ispezioni di sicurezza. È possibile definire politiche di misurazione per allocare in modo flessibile l'utilizzo dell'elaborazione dei dati sugli allegati middlebox all'allegato di origine, all'allegato di destinazione finale o al proprietario dell'account Transit Gateway. Per gli allegati Network Function, i costi di elaborazione dei dati del AWS Network Firewall vengono assegnati anche all'account misurato.

Allegati del gateway di transito designati che instradano il traffico attraverso le apparecchiature di rete per l'ispezione di sicurezza, il bilanciamento del carico o altre funzioni di rete. L'utilizzo dei dati per gli allegati middlebox che attraversano il traffico viene misurato in base al proprietario dell'account specificato nella politica di misurazione. È possibile specificare un massimo di 10 allegati middlebox. I tipi di allegati middlebox supportati sono gli allegati Network Function (AWS Network Firewall), VPC e VPN.

Argomenti

Aggiungi gli allegati middlebox della politica di misurazione AWS Transit Gateway

Puoi aggiungere allegati middlebox per integrare le appliance di rete nella tua politica di misurazione Transit Gateway. Ciò consente di indirizzare il traffico specifico attraverso dispositivi di sicurezza, sistemi di bilanciamento del carico o altre funzioni di rete, mantenendo al contempo un controllo granulare dell'allocazione dei costi.

Important

- Assicurati che i dispositivi middlebox siano configurati e accessibili correttamente
- Testa il routing del traffico prima di applicarlo ai carichi di lavoro di produzione
- Monitora le prestazioni del middlebox per evitare l'introduzione di latenza
- Configura il comportamento di failover appropriato per un'elevata disponibilità

Aggiungi gli allegati middlebox utilizzando la console

Per aggiungere una voce di allegato nella casella centrale

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Metering policies.
3. Seleziona il link ID della politica di misurazione per visualizzarne i dettagli.
4. Scegli la scheda degli allegati di Middlebox.
5. Scegliere Aggiungi.
6. Quando richiesto, seleziona l'allegato middlebox IDs che deve essere considerato come middlebox per la fatturazione specializzata. Puoi selezionare fino a 10 allegati middlebox.
7. Scegli Aggiungi allegati middlebox per salvare la configurazione.

Aggiungi gli allegati middlebox utilizzando il AWS CLI

Usa il modify-transit-gateway-metering-policy comando per aggiungere allegati.

Prima di iniziare, assicuratevi di avere i seguenti parametri obbligatori:

- `--transit-gateway-metering-policy-id`- L'ID della politica di misurazione esistente
- `--add-middle-box-attachment-ids`- Uno o più allegati IDs da aggiungere alla politica (per aggiungere allegati)

Per aggiungere allegati middlebox a una policy esistente utilizzando la CLI AWS

1. Nell'esempio seguente, modify-transit-gateway-metering-policy viene utilizzato per aggiungere quattro allegati middlebox a una politica di misurazione esistente. Il comando aggiunge l'allegato specificato all'elenco esistente senza IDs rimuovere gli allegati correnti:

```
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. Nel seguente esempio di risposta, l'output JSON mostra la configurazione aggiornata delle policy con tutti e quattro gli allegati middlebox ora inclusi:

```
{
    "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"
    }
}
```

Rimuovi gli allegati middlebox della policy di misurazione AWS Transit Gateway

Per impostazione predefinita, i costi di misurazione vengono attribuiti al proprietario dell'allegato middlebox. Tuttavia, è possibile modificare queste assegnazioni per garantire che i costi vengano allocati correttamente all'origine o alla destinazione effettiva del traffico. È possibile aggiungere o rimuovere fino a 10 allegati middlebox in totale per una politica di misurazione.

Rimuovi gli allegati middlebox utilizzando la console

Usa la console Amazon VPC per rimuovere gli allegati middlebox dalla configurazione della tua politica di misurazione.

Per rimuovere gli allegati middlebox

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli Transit Gateway, Metering policies.

3. Seleziona la politica di misurazione che desideri modificare.
4. Scegli la scheda degli allegati di Middlebox.
5. Seleziona fino a 10 allegati middlebox da rimuovere dalla politica di misurazione.
6. Scegli Rimuovi.
7. Quando richiesto, puoi aggiornare gli allegati middlebox scelti per rimuoverli. Il traffico proveniente dagli allegati rimossi verrà indirizzato al proprietario dell'allegato middlebox.
8. Scegli Rimuovi gli allegati middlebox.

Rimuovi gli allegati middlebox utilizzando il AWS CLI

Usa il modify-transit-gateway-metering-policy comando per rimuovere gli allegati.

Prima di iniziare, assicuratevi di avere i seguenti parametri obbligatori:

- `--transit-gateway-metering-policy-id`- L'ID della politica di misurazione esistente
- `--remove-middle-box-attachment-ids`- Uno o più allegati da IDs rimuovere dalla politica (per rimuovere gli allegati)

Per rimuovere gli allegati middlebox da una policy esistente utilizzando la CLI AWS

1. Nell'esempio seguente, modify-transit-gateway-metering-policy viene utilizzato per rimuovere due allegati middlebox specifici da una politica di misurazione esistente. Il comando rimuove solo l'allegato specificato IDs preservando gli allegati rimanenti:

```
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. Nel seguente esempio di risposta, l'output JSON mostra la configurazione aggiornata delle policy con gli allegati specificati rimossi e gli allegati rimanenti ancora attivi:

```
{
    "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 Registri di flusso Transit Gateway

Transit Gateway Flow Logs è una funzionalità di AWS Transit Gateway che consente di acquisire informazioni sul traffico IP in entrata e in uscita dai gateway di transito. I dati dei log di flusso possono essere pubblicati su Amazon CloudWatch Logs, Amazon S3 o Firehose. Dopo aver creato un log di flusso, puoi recuperare e visualizzarne i dati nella destinazione scelta. I dati di log del flusso vengono raccolti al di fuori del percorso del traffico di rete e pertanto non influiscono sulla velocità effettiva o sulla latenza della rete. È possibile creare o eliminare i log di flusso senza alcun rischio di impatto sulle prestazioni della rete. I registri di flusso del gateway di transito acquisiscono informazioni relative solo ai gateway di transito, descritti in the section called “Log di flusso del gateway di transito”. Se desideri acquisire informazioni sul traffico IP in entrata e in uscita dalle interfacce di rete del tuo computer VPCs, utilizza VPC Flow Logs. Per ulteriori informazioni consulta Logging IP traffic using VPC Flow Logs (Registrazione del traffico IP utilizzando i registri di flusso VPC) nella Guida per l'utente di Amazon VPC.

> **Note**
>
> Per creare un log di flusso del gateway di transito, devi essere il proprietario del gateway di transito. Se non sei il proprietario, il proprietario del gateway di transito deve darti l'autorizzazione.

I dati del log di flusso per un gateway di transito monitorato vengono registrati come record del log di flusso, ossia eventi di log costituiti da campi che descrivono il flusso di traffico. Per ulteriori informazioni, consulta Log di flusso del gateway di transito.

Per creare un log di flusso, occorre specificare:

- La risorsa per cui creare il log di flusso
- Le destinazioni in cui pubblicare i dati del log di flusso

Dopo aver creato un flusso di log, potrebbero essere necessari diversi minuti prima di iniziare a raccogliere dati e pubblicarli nelle destinazioni scelte. I registri di flusso non acquisiscono flussi di log in tempo reale per i gateway di transito.

È possibile applicare tag ai log di flusso. Ogni tag è composto da una chiave e da un valore opzionale, entrambi personalizzabili. I tag consentono di organizzare i log di flusso, ad esempio per scopo o proprietario.

Se un log di flusso non è più necessario, puoi eliminarlo. L'eliminazione di un log di flusso disattiva il servizio di log di flusso per la risorsa e nessun nuovo record del log di flusso viene creato o pubblicato su CloudWatch Logs o Amazon S3. L'eliminazione del log di flusso non elimina alcun record o flusso di log di flusso esistente (per CloudWatch Logs) o oggetti di file di log (per Amazon S3) per un gateway di transito. Per eliminare un flusso di log esistente, usa la console Logs. CloudWatch Per eliminare oggetti file di log esistenti, utilizza la console Amazon S3. Dopo aver eliminato un log di flusso, potrebbero essere necessari diversi minuti per interrompere la raccolta dati. Per ulteriori informazioni, consulta Eliminare un record AWS Transit Gateway Flow Logs.

Puoi creare log di flusso per i tuoi gateway di transito in grado di pubblicare dati su CloudWatch Logs, Amazon S3 o Amazon Data Firehose. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Crea un Flow Log da pubblicare su Logs CloudWatch
- Crea un log di flusso da pubblicare su Amazon S3
- Creare un log di flusso da pubblicare su Firehose

Limitazioni

Le seguenti limitazioni si applicano ai Transit Gateway Flow Logs:

- Il traffico multicast non è supportato.
- Gli allegati Connect non sono supportati. Tutti i log di flusso di Connect vengono visualizzati sotto l'allegato di trasporto e devono quindi essere abilitati sul gateway di transito o sull'allegato di trasporto Connect.

Log di flusso del gateway di transito

Un record del log di flusso rappresenta un flusso di rete nel gateway di transito. Ogni record è una stringa con campi separati da spazi. Un record include valori per i vari componenti del flusso di traffico tra cui, ad esempio, origine, destinazione e protocollo.

Quando crei un log di flusso, puoi utilizzare il formato predefinito oppure specificare un formato personalizzato.

Indice

Formato predefinito

Con il formato predefinito, i record del log di flusso includono tutti i campi dalla versione 2 alla versione 6, nell'ordine mostrato nella tabella dei campi disponibili. Non è possibile personalizzare o modificare il formato predefinito. Per acquisire i campi aggiuntivi o un diverso sottoinsieme di campi, specifica un formato personalizzato.

Formato personalizzato

Con un formato personalizzato, è possibile specificare quali campi sono inclusi nei record del log di flusso e il relativo ordine. Ciò permette di creare registri di flusso specifici per le proprie esigenze e omettere i campi non pertinenti. L'uso di un formato personalizzato può anche ridurre la necessità di processi separati per estrarre informazioni specifiche dai log di flusso pubblicati. Puoi specificare un numero qualsiasi di campi del log di flusso disponibili, ma devi specificarne almeno uno.

Campi disponibili

Nella tabella seguente sono descritti tutti i campi disponibili per un record del log di flusso di un gateway di transito. La colonna Version (Versione) indica la versione in cui è stato introdotto il campo.

Quando si pubblicano i dati del flusso di log su Amazon S3, il tipo di dati per i campi dipende dal formato del flusso di log. Se il formato è di testo normale, tutti i campi sono di tipo STRING. Se il formato è Parquet, vedere la tabella per i tipi di dati di campo.

Se un campo non è applicabile o non può essere calcolato per un record specifico, il record visualizza un simbolo "-" per tale voce. I campi dei metadati che non provengono direttamente dall'intestazione del pacchetto sono approssimazioni ottimali e i loro valori potrebbero essere mancanti o imprecisi.

Campo	Descrizione	Versione
version	Indica la versione in cui è stato introdotto il campo. Il formato predefinito include tutti i campi della versione 2 nello stesso ordine in cui sono riportati nella tabella. Tipo di dati Parquet: INT_32	2
resource-type	Il tipo di risorsa su cui viene creata la sottoscrizione. Per i Transit Gateway Flow Logs, questo saràTransitGateway. Tipo di dati Parquet: STRING	6
account-id	L' Account AWS ID del proprietario del gateway di transito di origine. Tipo di dati Parquet: STRING	2
tgw-id	L'ID del gateway di transito per il quale viene registrato il traffico. Tipo di dati Parquet: STRING	6
tgw-attachment-id	L'ID del collegamento del gateway di transito alla VPN per il quale viene registrato il traffico. Tipo di dati Parquet: STRING	6
tgw-src-vpc-account-id	L' Account AWS ID per il traffico VPC di origine. Tipo di dati Parquet: STRING	6
tgw-dst-vpc-account-id	L' Account AWS ID per il traffico VPC di destinazione. Tipo di dati Parquet: STRING	6
tgw-src-vpc-id	L'ID del VPC di origine per il gateway di transito Tipo di dati Parquet: STRING	6
tgw-dst-vpc-id	L'ID del VPC di destinazione per il gateway di transito. Tipo di dati Parquet: STRING	6

Campo	Descrizione	Versione
tgw-src-subnet-id	L'ID della sottorete per il traffico di origine del gateway di transito. Tipo di dati Parquet: STRING	6
tgw-dst-subnet-id	L'ID della sottorete per il traffico di destinazione del gateway di transito. Tipo di dati Parquet: STRING	6
tgw-src-eni	L'ID dell'ENI del collegamento del gateway di transito alla VPN di origine per il flusso. Tipo di dati Parquet: STRING	6
tgw-dst-eni	L'ID dell'ENI del collegamento del gateway di transito alla VPN di destinazione per il flusso. Tipo di dati Parquet: STRING	6
tgw-src-az-id	L'ID della zona di disponibilità che contiene il gateway di transito di origine per cui viene registrato il traffico. Se il traffico proviene da una posizione secondaria, il record visualizza un simbolo ’-’ per questo campo. Tipo di dati Parquet: STRING	6
tgw-dst-az-id	L'ID della zona di disponibilità che contiene il gateway di transito di destinazione per cui viene registrato il traffico. Tipo di dati Parquet: STRING	6
tgw-pair-attachment-id	A seconda della direzione del flusso, questo è l'ID allegato in uscita o in ingresso del flusso. Tipo di dati Parquet: STRING	6
srcaddr	L'indirizzo di origine per traffico in entrata. Tipo di dati Parquet: STRING	2

Campo	Descrizione	Versione
dstaddr	L'indirizzo di destinazione per il traffico in uscita. Tipo di dati Parquet: STRING	2
srcport	La porta di origine del traffico. Tipo di dati parquet: INT_32	2
dstport	La porta di destinazione del traffico. Tipo di dati Parquet: INT_32	2
protocol	Il numero di protocollo IANA del traffico. Per ulteriori informazioni, consulta la sezione relativa ai numeri di protocollo Internet assegnati. Tipo di dati Parquet: INT_32	2
packets	Il numero di pacchetti trasferiti durante il flusso. Tipo di dati parquet: INT_64	2
bytes	Il numero di byte trasferiti durante il flusso. Tipo di dati Parquet: INT_64	2
start	L'ora, in secondi Unix, di ricezione del primo pacchetto del flusso all'interno dell'intervallo di aggregazione. Potrebbe durare fino a 60 secondi oltre l'avvenuta trasmissione o ricezione del pacchetto da parte del gateway di transito. Tipo di dati Parquet: INT_64	2
end	L'ora, in secondi Unix, in cui l'ultimo pacchetto del flusso è stato ricevuto entro l'intervallo di aggregazione. Potrebbe durare fino a 60 secondi oltre l'avvenuta trasmissione o ricezione del pacchetto da parte del gateway di transito. Tipo di dati Parquet: INT_64	2

Campo	Descrizione	Versione
log-status	Lo stato del log di flusso: • OK: i dati vengono registrati normalmente nelle destinazioni scelte. • NODATA: non vi è alcun traffico di rete da o per l'interfaccia di rete durante l'intervallo di aggregazione. • SKIPDATA: alcuni record del log di flusso sono stati ignorati durante l'intervallo di aggregazione. Ciò può essere causato da un vincolo di capacità interna o da un errore interno. Tipo di dati Parquet: STRING	2
type	Il tipo di traffico. I valori possibili sono IPv4 | IPv6 | EFA. Per ulteriori informazioni, consulta Elastic Fabric Adapter nella Amazon EC2 User Guide. Tipo di dati parquet: STRING	3
packets-lost-no-route	I pacchetti sono andati persi perché non è stata specificata alcuna route. Tipo di dati Parquet: INT_64	6
packets-lost-blackhole	I pacchetti sono andati persi a causa di un buco nero. Tipo di dati Parquet: INT_64	6
packets-lost-mtu-exceeded	I pacchetti sono andati persi a causa delle dimensioni che superano la MTU. Tipo di dati Parquet: INT_64	6
packets-lost-ttl-expired	I pacchetti persi a causa della scadenza di time-to-live. Tipo di dati Parquet: INT_64	6

Campo	Descrizione	Versione
tcp-flags	Il valore bitmask per i seguenti flag TCP: • FIN - 1 • SYN - 2 • RST - 4 • PSH - 8 • ACK - 16 • SYN-ACK - 18 • URG - 32 **Important** Quando una voce del log di flusso è composta solo da pacchetti ACK, il valore del flag è 0, non 16. Per informazioni generali sui flag TCP (come il significato di flag come FIN, SYN e ACK), consulta Struttura del segmento TCP su Wikipedia. I flag TCP sono introdotti da un operatore OR durante l'intervallo di aggregazione. Per le connessioni brevi, i flag possono essere impostati sulla stessa riga nel record del log di flusso, ad esempio 19 per SYN-ACK e FIN e 3 per SYN e FIN. Tipo di dati parquet: INT_32	3
region	La Regione che contiene il gateway di transito in cui viene registrato il traffico. Tipo di dati parquet: STRING	4

Campo	Descrizione	Versione
flow-direction	La direzione del flusso rispetto all'interfaccia in cui viene catturato il traffico. I valori possibili sono: ingress | egress. Tipo di dati parquet: STRING	5
pkt-src-aws-service	Il nome del sottoinsieme di indirizzi IP indica srcaddr se l'indirizzo IP di origine è per un AWS servizio. I valori possibili sono: AMAZON | AMAZON_APPFLOW | AMAZON_CONNECT | API_GATEWAY | CHIME_MEETINGS | CHIME_VOICECONNECTOR | CLOUD9 | CLOUDFRONT | CODEBUILD | DYNAMODB | EBS | EC2 | EC2_INSTANCE_CONNECT | GLOBALACCELERATOR | KINESIS_VIDEO_STREAMS | ROUTE53 | ROUTE53_HEALTHCHECKS | ROUTE53_HEALTHCHECKS_PUBLISHING | ROUTE53_RESOLVER | S3 | WORKSPACES_GATEWAYS. Tipo di dati parquet: STRING	5
pkt-dst-aws-service	Il nome del sottoinsieme di intervalli di indirizzi IP per il dstaddr campo, se l'indirizzo IP di destinazione è per un AWS servizio. Per un elenco di possibili valori, consulta il campo pkt-src-aws-service. Tipo di dati parquet: STRING	5

Controllo dell'utilizzo dei log di flusso

Per impostazione predefinita, gli utenti non dispongono dell'autorizzazione per utilizzare log di flusso. Puoi creare una policy dell'utente che concede agli utenti le autorizzazioni per creare, descrivere ed eliminare log di flusso. Per ulteriori informazioni, consulta Concessione delle autorizzazioni richieste agli utenti IAM per le EC2 risorse Amazon nell'Amazon EC2 API Reference.

Di seguito è riportata una policy di esempio che concede agli utenti autorizzazioni complete per creare, descrivere ed eliminare log di flusso.

JSON

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

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

È necessaria una configurazione aggiuntiva dei ruoli e delle autorizzazioni IAM, a seconda che tu stia pubblicando su CloudWatch Logs o Amazon S3. Per ulteriori informazioni, consultare AWS Transit Gateway Flow registra i record in Amazon CloudWatch Logs e AWS Transit Gateway Flow registra i record in Amazon S3 .

Prezzi dei log di flusso di Transit Gateway

Gli addebiti per l'importazione dei dati e l'archiviazione per i log distribuiti vengono applicati quando si pubblicano i log di flusso del gateway di transito. Per ulteriori informazioni sui prezzi per la pubblicazione dei log venduti, apri Amazon CloudWatch Pricing, quindi, in Livello a pagamento, seleziona Log e trova Vended Logs.

Creare o aggiornare un ruolo IAM per AWS Transit Gateway Flow Logs

È possibile aggiornare un ruolo esistente o utilizzare la procedura seguente per creare un nuovo ruolo da utilizzare con i log di flusso utilizzando la AWS Identity and Access Management console.

Per creare un ruolo IAM per i log di flusso

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione seleziona Ruoli, quindi Crea ruolo.
3. In Seleziona tipo di entità attendibile, scegli Servizio AWS . Per Use case, scegli EC2. Scegli Next (Successivo).

4. Nella pagina Add permissions (Aggiungi autorizzazioni), scegli Next: Tags (Successivo: Tag) e aggiungi facoltativamente i tag. Scegli Next (Successivo).
5. Nella pagina Nome, rivedi e crea, inserisci un nome per il tuo ruolo e, facoltativamente, fornisci una descrizione. Scegli Crea ruolo.
6. Scegli il nome del ruolo. In Add permissions (Aggiungi autorizzazioni), scegli Create inline policy (Crea policy in linea), quindi seleziona la scheda JSON.
7. Copiare la prima policy da Ruoli IAM per la pubblicazione dei log di flusso in Logs CloudWatch e incollarla nella finestra. Scegliere Review policy (Esamina policy).
8. Immettere un nome per la policy e scegliere Create policy (Crea policy).
9. Selezionare il nome del ruolo. In Trust Relationships (Relazioni di trust), scegliere Edit Trust Relationship (Modifica relazione di trust). Nel documento di policy esistente, cambiare il servizio da `ec2.amazonaws.com` a `vpc-flow-logs.amazonaws.com`. Selezionare Update Trust Policy (Aggiorna policy di trust).
10. Nella pagina Summary (Riepilogo), prendere nota dell'ARN per il ruolo. Questo ARN sarà necessario al momento della creazione del log di flusso.

AWS Transit Gateway Flow registra i record in Amazon CloudWatch Logs

I log di flusso possono pubblicare i dati dei log di flusso direttamente su Amazon CloudWatch.

Quando vengono pubblicati su CloudWatch Logs, i dati del log di flusso vengono pubblicati in un gruppo di log e ogni gateway di transito ha un flusso di log unico nel gruppo di log. I flussi di log contengono record del log di flusso. Puoi creare più log di flusso che pubblicano dati nello stesso gruppo di log. Se lo stesso gateway di transito è presente in uno o più registri di flusso nello stesso gruppo di flussi di log, esso dispone di un flusso di log combinato. Se è stato specificato che un log di flusso deve acquisire traffico rifiutato e l'altro log di flusso deve acquisire traffico accettato, il flusso di log combinato acquisisce tutto il traffico.

I costi di inserimento e archiviazione dei dati per i log venduti si applicano quando si pubblicano i log di flusso su Logs. CloudWatch Per ulteriori informazioni, consulta la pagina CloudWatch dei prezzi di Amazon.

In CloudWatch Logs, il campo timestamp corrisponde all'ora di inizio registrata nel record del log di flusso. Il campo IngestionTime fornisce la data e l'ora in cui il record del log di flusso è stato ricevuto

da Logs. CloudWatch Questo timestamp è successivo all'ora di fine acquisita nel record del log di flusso.

Per ulteriori informazioni sui CloudWatch log, consulta Logs sent to Logs nella Amazon CloudWatch CloudWatch Logs User Guide.

Indice

Ruoli IAM per la pubblicazione dei log di flusso in Logs CloudWatch

Il ruolo IAM associato al log di flusso deve disporre di autorizzazioni sufficienti per pubblicare i log di flusso nel gruppo di log specificato in Logs. CloudWatch Il ruolo IAM deve appartenere al tuo. Account AWS

La policy IAM collegata al ruolo IAM deve includere almeno le autorizzazioni seguenti:

JSON

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

Accertarti inoltre che il ruolo disponga di una relazione di trust che consenta al servizio log di flusso di assumere il ruolo.

JSON

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

Si consiglia di utilizzare il le chiavi di condizione `aws:SourceAccount` e `aws:SourceArn` per proteggersi dal problema del "confused deputy". Ad esempio, è possibile aggiungere il seguente blocco di condizione alla policy di attendibilità precedente. L'account di origine è il proprietario del flusso di log e l'ARN di origine è l'ARN del flusso di log. Se non si conosce l'ID del flusso di log, è possibile sostituire quella parte dell'ARN con un carattere jolly (*) e quindi aggiornare la policy dopo aver creato il flusso di log.

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

Autorizzazioni per gli utenti IAM per passare un ruolo

Gli utenti devono anche disporre delle autorizzazioni per utilizzare l'operazione `iam:PassRole` per il ruolo IAM associato al log di flusso.

JSON

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

Crea un record AWS Transit Gateway Flow Logs da pubblicare su Amazon CloudWatch Logs

È possibile creare registri di flusso per i gateway di transito. Se si esegue questa procedura come utente IAM, assicurarsi di disporre delle autorizzazioni per utilizzare l'operazione `iam:PassRole`. Per ulteriori informazioni, consulta Autorizzazioni per gli utenti IAM per passare un ruolo.

Puoi creare un log di CloudWatch flusso Amazon utilizzando la console Amazon VPC o la CLI AWS .

Per creare un log di flusso del gateway di transito utilizzando la console

1. Accedi Console di gestione AWS e apri la console Amazon VPC all'indirizzo. https://console.aws.amazon.com/vpc/
2. Nel riquadro di navigazione selezionare Transit gateways (Gateway di transito).
3. Scegli le caselle di controllo per uno o più gateway di transito e scegli Azioni, Crea log di flusso.
4. Per Destinazione, scegli Invia ai registri. CloudWatch
5. Per Gruppo di log di destinazione, scegli il nome di un gruppo di log di destinazione corrente.

> **Note**
>
> Se il gruppo di log di destinazione non esiste ancora, l'inserimento di un nuovo nome in questo campo creerà un nuovo gruppo di log di destinazione.

6. Per il ruolo IAM, specifica il nome del ruolo che dispone delle autorizzazioni per pubblicare i log in Logs. CloudWatch
7. Per Formato record di log, seleziona il formato per il record del log di flusso.
   - Per utilizzare il formato del record di log di flusso predefinito, seleziona Formato predefinito AWS .
   - Per utilizzare un formato personalizzato, scegli Formato personalizzato, quindi seleziona i campi da Formato di log .
8. (Facoltativo) Seleziona Aggiungi tag per applicare i tag al log di flusso.
9. Selezionare Create flow log (Crea log di flusso).

Per creare un log di flusso utilizzando la riga di comando

Utilizzare uno dei seguenti comandi.

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

L' AWS CLI esempio seguente crea un log di flusso che acquisisce le informazioni sul gateway di transito. I log di flusso vengono consegnati a un gruppo di log in CloudWatch Logs chiamato`my-flow-logs`, nell'account 123456789101, utilizzando il ruolo IAM. `publishFlowLogs`

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

Visualizza i record dei log di AWS Transit Gateway Flow in Amazon CloudWatch

Puoi visualizzare i record dei log di flusso utilizzando la console CloudWatch Logs o la console Amazon S3, a seconda del tipo di destinazione scelto. Dopo che il flusso di log è stato creato, potrebbero essere necessari alcuni minuti prima che sia visibile nella console.

Per visualizzare i record dei log di flusso pubblicati su Logs CloudWatch

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.

2. Nel riquadro di navigazione, scegliere Logs (Log) e selezionare il gruppo di log contenente il log di flusso. Viene mostrato un elenco di flussi di log per ogni gateway di transito.
3. Selezionare il flusso di log contenente l'ID del gateway di transito per il quale si desidera visualizzare i record del registro di flusso. Per ulteriori informazioni, consulta Log di flusso del gateway di transito.

Elaborazione dei record di AWS Transit Gateway Flow Logs in Amazon CloudWatch Logs

È possibile utilizzare i record del log di flusso come con qualsiasi altro evento di registro raccolto da CloudWatch Logs. Per ulteriori informazioni sul monitoraggio dei dati di log e sui filtri delle metriche, consulta Creazione di metriche dagli eventi di registro utilizzando i filtri nella Amazon CloudWatch User Guide.

Esempio: crea un filtro CloudWatch metrico e un allarme per un log di flusso

In questo esempio, si dispone di un log di flusso per `tgw-123abc456bca`. Si desidera creare un allarme che avvisa se si sono verificati almeno 10 tentativi di connessione all'istanza sulla porta TCP 22 (SSH) entro un periodo di tempo di 1 ora. Innanzitutto, crea un filtro parametri che corrisponde al modello di traffico per il quale creare l'allarme. Quindi, puoi creare un allarme per il filtro parametri.

Per creare il filtro parametri per traffico SSH rifiutato e creare un allarme per il filtro

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel pannello di navigazione a sinistra, scegli Log, Gruppi di log.
3. Seleziona la casella di controllo per il gruppo di log, quindi scegli Azioni, Crea filtro metrico.
4. Per Filter Pattern (Modello di filtro), immettere quanto segue.

```
[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. Per Select Log Data to Test (Seleziona i dati di registro per il test), seleziona il flusso di log per il gateway di transito. (Facoltativo) Per visualizzare le righe di dati di log che corrispondono al modello di filtro, scegli Test Pattern (Modello di test). Al termine, scegli Next (Successivo).
6. Inserisci un nome per il filtro, uno spazio dei nomi dei parametri e il nome del parametro. Imposta il valore del parametro su **1**. Al termine, scegli Next (Successivo) e in seguito Create metric filter (Crea filtri parametri).
7. Nel pannello di navigazione, seleziona Alarms (Allarmi), All alarms (Tutti gli allarmi).
8. Scegli Crea allarme.
9. Scegli lo spazio dei nomi per il filtro parametri che hai creato.

   Per visualizzare il nuovo parametro nella console potrebbero essere necessari alcuni minuti.
10. Seleziona il nome del parametro creato e scegli Next (Successivo).
11. Configura l'allarme come segue, quindi scegli Next (Successivo):

    - Per Statistic (Statistica), scegliere Sum (Somma). Ciò ti garantisce di acquisire il numero totale di punti di dati per il periodo di tempo specificato.
    - Per Period (Periodo), scegli 1 Hour (1 ora).
    - Per Whenever (Ogni volta che) , scegli Greater/Equal (Maggiore di/Uguale a) e inserisci **10** come soglia.
    - In Additional configuration (Configurazione aggiuntiva), per Datapoints to alarm (Punti dati per allarme) lascia il valore predefinito **1**.
12. Per Notification (Notifica), scegli un argomento SNS esistente oppure scegli Create new topic (Crea nuovo argomento) per crearne uno nuovo. Scegli Next (Successivo).
13. Inserisci un nome e una descrizione per l'allarme, quindi scegli Next (Successivo).
14. Al termine della configurazione dell'allarme, scegli Create alarm (Crea allarme).

AWS Transit Gateway Flow registra i record in Amazon S3

I log di flusso possono pubblicare dati di log di flusso in Amazon S3.

Durante la pubblicazione in Amazon S3, i dati del log di flusso vengono pubblicati in un bucket Amazon S3 esistente specificato. I record del log di flusso per tutti i gateway di transito monitorati vengono pubblicati in una serie di oggetti file di log che sono archiviati nel bucket.

I costi di inserimento e archiviazione dei dati vengono applicati ai log venduti quando si pubblicano Amazon CloudWatch i log di flusso su Amazon S3. Per ulteriori informazioni sui CloudWatch prezzi dei log venduti, apri Amazon CloudWatch Pricing, scegli Logs, quindi trova Vending Logs.

Per creare un bucket Amazon S3 da utilizzare con i flussi di log, consulta Creazione di un bucket nella Guida per l'utente di Amazon S3.

Per ulteriori informazioni sulla registrazione di più account, consulta Registrazione centrale nella libreria di soluzioni di AWS .

Per ulteriori informazioni sui CloudWatch log, consulta Logs sent to Amazon S3 nella Amazon Logs User Guide CloudWatch .

Indice

File di log di flusso

Log di flusso VPC è una caratteristica che raccoglie record di log di flusso, li consolida in file di log e pubblica questi ultimi nel bucket Amazon S3 a intervalli di cinque minuti. Ogni file di log contiene record di log di flusso per il traffico IP registrato nei cinque minuti precedenti.

Le dimensioni file massime per un file di log sono di 75 MB. Se il file di log raggiunge le dimensioni massime previste entro il periodo di 5 minuti, il log di flusso smette di aggiungervi record. Pubblica il file di log nel bucket Amazon S3 e crea un nuovo file di log.

In Amazon S3, il campo Last modified (Ultima modifica) per il file di log di flusso indica la data e l'ora in cui il file è stato caricato nel bucket Amazon S3. Questa è successiva al timestamp nel nome del file e differisce per il tempo impiegato per caricare il file nel bucket Amazon S3.

Formato dei file di log

Per i file di log, puoi specificare uno dei seguenti formati. Ciascun file viene compresso in un singolo file Gzip.

- Text: Testo normale. Questo è il formato predefinito.
- Parquet: Apache Parquet è un formato dati colonnare. Le query sui dati in formato Parquet sono da 10 a 100 volte più veloci, rispetto alle query sui dati in testo normale. I dati in formato Parquet con compressione Gzip occupano il 20% di spazio di archiviazione in meno, rispetto al testo normale con compressione Gzip.

Opzioni di file di log

È inoltre possibile specificare le seguenti opzioni.

- Hive-compatible S3 prefixes (Prefissi S3 compatibili con Hive): Abilita i prefissi compatibili con Hive invece di importare partizioni negli strumenti compatibili. Prima di eseguire query, utilizza il comando MSCK REPAIR TABLE.
- Hourly partitions (Partizioni orarie): se disponi di un grande volume di registri e di solito indirizzi le query a un'ora specifica, partizionando i log su base oraria puoi ottenere risultati più rapidi e risparmiare sui costi delle query.

Struttura del bucket S3 dei file di log

I file di log vengono salvati nel bucket Amazon S3; utilizzando una struttura di cartelle determinata dall'ID del flusso di log, dalla Regione e dalla loro data di creazione.

Per impostazione predefinita, i file vengono recapitati alla seguente posizione.

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

Se abiliti i prefissi S3 compatibili con Hive, i file vengono recapitati nella seguente posizione.

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

Se abiliti le partizioni orarie, i file vengono recapitati nella seguente posizione.

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

Se abiliti le partizioni compatibili con Hive e partizioni il flusso di log per ora, i file vengono recapitati nella posizione seguente.

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

Nome del file di log

Il nome di un file di log si basa sull'ID del flusso di log, sulla Regione e sulla data e ora di creazione. I nomi file utilizzano il formato seguente.

```
aws_account_id_vpcflowlogs_region_flow_log_id_YYYYMMDDTHHmmZ_hash.log.gz
```

Ad esempio, di seguito viene mostrata la struttura di cartelle e il nome di un file di log per un flusso di log creato dall' Account AWS 123456789012, per una risorsa nella Regione us-east-1 su June 20, 2018 in 16:20 UTC. Il file contiene i registri dei flussi di log con un'ora di fine tra 16:20:00 e 16:24:59.

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

Policy IAM per le entità IAM che pubblicano i log di flusso in Amazon S3

Il principale IAM che crea il log di flusso deve disporre delle autorizzazioni seguenti, necessarie per pubblicare log di flusso nel bucket Amazon S3 di destinazione.

JSON

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

```
    }
  ]
}
```

Autorizzazioni dei bucket Amazon S3 per log di flusso

Per impostazione predefinita, i bucket Amazon S3 e gli oggetti che contengono sono privati. Solo il proprietario del bucket può accedere al bucket e agli oggetti in esso archiviati. Il proprietario del bucket, tuttavia, può concedere l'accesso ad altre risorse e ad altri utenti scrivendo una policy di accesso.

Se l'utente che crea il flusso di log è il proprietario del bucket e ha le autorizzazioni `PutBucketPolicy` e `GetBucketPolicy` per il bucket, verrà automaticamente allegata la seguente policy al bucket. Questa nuova policy generata automaticamente viene aggiunta alla policy originale.

In caso contrario, il proprietario del bucket deve aggiungere tale policy al bucket, specificando l'ID dell' Account AWS del creatore del flusso di log o la creazione del flusso di log fallirà. Per ulteriori informazioni, consulta le politiche di Bucket nella Guida per l'utente di Amazon Simple Storage Service.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::bucket_name/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceAccount": "123456789012"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:us-east-1:123456789012:*"
```

```
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryCheck",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": [
                "s3:GetBucketAcl"
            ],
            "Resource": "arn:aws:s3:::bucket_name",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:us-east-1:123456789012:*"
                }
            }
        }
    ]
}
```

L'ARN specificato *my-s3-arn* dipende dall'utilizzo o meno di prefissi S3 compatibili con Hive.

- Prefissi di default

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

- Prefissi S3 compatibili con Hive

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

Come procedura ottimale, si consiglia di concedere queste autorizzazioni al responsabile del servizio di consegna dei log anziché al singolo individuo. Account AWS ARNs Una best practice è anche usare le chiavi di condizione `aws:SourceAccount` e `aws:SourceArn` per proteggersi dal problema del "confused deputy". L'account di origine è il proprietario del flusso di log e l'ARN di origine è l'ARN jolly (*) del servizio log.

Policy di chiave richiesta per l'uso con SSE-KMS

Puoi proteggere i dati nel tuo bucket Amazon S3 abilitando la crittografia lato server con Amazon S3 Managed Keys (SSE-S3) o la crittografia lato server con chiavi archiviate in KMS (SSE-KMS). Per ulteriori informazioni, consulta Protezione dei dati con la crittografia lato server nella Guida per l'utente di Amazon S3.

Con SSE-KMS, puoi utilizzare una chiave gestita o una chiave AWS gestita dal cliente. Con una chiave AWS gestita, non è possibile utilizzare la consegna tra account. I log di flusso vengono recapitati dall'account di recapito del log, pertanto è necessario concedere l'accesso per la consegna tra account. Per concedere l'accesso tra account al tuo bucket S3, usa una chiave gestita dal cliente e specifica l'Amazon Resource Name (ARN) della chiave gestita dal cliente quando abiliti la crittografia del bucket. Per ulteriori informazioni, consulta Specifica della crittografia lato server con AWS KMS nella Guida per l'utente di Amazon S3.

Quando utilizzi SSE-KMS con una chiave gestita dal cliente, dovrai aggiungere quanto segue alla policy di chiavi per la tua chiave (non la policy di bucket per il bucket S3), in modo che i flussi di log del VPC possano scrivere nel bucket S3.

> **Note**
>
> L'utilizzo di S3 Bucket Keys ti consente di risparmiare sui AWS Key Management Service (AWS KMS) costi delle richieste diminuendo le richieste alle AWS KMS operazioni di crittografia e decrittografia tramite l'uso di una chiave a livello di bucket. GenerateDataKey In base alla progettazione, le richieste successive che sfruttano questa chiave a livello di bucket non generano richieste API né convalidano l'accesso in AWS KMS base alla policy della chiave. 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": "*"
}
```

Autorizzazioni del file di log Amazon S3

Oltre alle policy dei bucket richieste, Amazon S3 utilizza le liste di controllo degli accessi ACLs () per gestire l'accesso ai file di registro creati da un log di flusso. Per impostazione predefinita, il proprietario del bucket dispone di autorizzazioni `FULL_CONTROL` su ogni file di log. Il proprietario della distribuzione dei log, se diverso dal proprietario del bucket, non dispone di autorizzazioni. L'account di distribuzione dei log dispone delle autorizzazioni `READ` e `WRITE`. Per ulteriori informazioni, consulta la panoramica dell'elenco di controllo degli accessi (ACL) nella Guida per l'utente di Amazon Simple Storage Service.

Creare il ruolo dell'account di origine AWS Transit Gateway Flow Logs per Amazon S3

Dall'account di origine, crea il ruolo di origine nella AWS Identity and Access Management console.

Creazione del ruolo dell'account di origine

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione, scegli Policy.
3. Scegli Create Policy (Crea policy).
4. Nella pagina Create policy (Crea policy), eseguire le operazioni seguenti:
    1. Scegli JSON.
    2. Sostituisci il contenuto di questa finestra con la policy delle autorizzazioni all'inizio di questa sezione.
    3. Scegli Next: Tags (Successivo: Tag) e Next: Review (Successivo: Rivedi).
    4. Immetti un nome per la policy e una descrizione facoltativa, quindi scegli Create policy (Crea policy).

5. Nel pannello di navigazione, seleziona Roles (Ruoli).
6. Selezionare Create role (Crea ruolo).
7. Per Trusted entity type (Tipo di entità attendibile), scegli Custom trust policy (Policy di attendibilità personalizzata). Per Custom trust policy (Policy di attendibilità personalizzata), sostituisci `"Principal": {},` con quanto segue, che specifica il servizio di consegna dei log. Scegli Next (Successivo).

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

8. Sulla pagina Add permissions (Aggiungi autorizzazioni), seleziona la casella di controllo relativa alla policy creata in precedenza in questa procedura, quindi scegli Next (Successivo).
9. Immetti un nome per il ruolo e fornisci una descrizione facoltativa.
10. Seleziona Create role (Crea ruolo).

Crea un record AWS Transit Gateway Flow Logs da pubblicare su Amazon S3

Dopo aver creato e configurato il bucket Amazon S3, è possibile creare registri di flusso per i gateway di transito. Puoi creare un log di flusso Amazon S3 utilizzando la console Amazon VPC o l'interfaccia a riga di comando. AWS

Creare un log di flusso del gateway di transito che pubblichi in Amazon S3 utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegliere Transit Gateway (Gateway di transito) o Transit Gateway Attachments (Collegamenti del gateway di transito alla VPN).
3. Selezionare le caselle di controllo per uno o più gateway di transito o collegamenti del gateway di transito alla VPN.
4. Scegli Actions (Operazioni), Create flow log (Crea flusso di log).
5. Configura le impostazioni del flusso di log. Per ulteriori informazioni, consulta Come configurare le impostazioni del flusso di log.

Configurazione delle impostazioni del flusso di log utilizzando la console

1. Per Destination (Destinazione), scegli Send to an S3 bucket (Invia a un bucket S3).
2. Per S3 bucket ARN (ARN bucket S3), specificare il nome della risorsa Amazon (ARN) di un bucket Amazon S3 esistente. Puoi anche includere una sottocartella. Ad esempio, per specificare una sottocartella denominata `my-logs` in un bucket denominato `my-bucket`, utilizzare il seguente ARN:

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

   Il bucket non può utilizzare `AWSLogs` come nome di sottocartella, in quanto si tratta di un termine riservato.

   Se si è il proprietario del bucket, noi creiamo automaticamente una policy delle risorse e la colleghiamo al bucket. Per ulteriori informazioni, consulta Autorizzazioni dei bucket Amazon S3 per log di flusso.
3. Per Log record format (Formato registro di log), seleziona il formato per il registro del flusso di log.

   - Per utilizzare il formato di record di log di flusso predefinito, seleziona Formato predefinito AWS .
   - Per creare un formato personalizzato, scegliere Custom format (Formato personalizzato). Per Log format (Formato log), scegliere i campi da includere nel record di log di flusso.
4. Per Log file format (Formato dei file di log), specifica il formato per il file di log.

   - Text: Testo normale. Questo è il formato predefinito.
   - Parquet: Apache Parquet è un formato dati colonnare. Le query sui dati in formato Parquet sono da 10 a 100 volte più veloci, rispetto alle query sui dati in testo normale. I dati in formato Parquet con compressione Gzip occupano il 20% di spazio di archiviazione in meno, rispetto al testo normale con compressione Gzip.
5. (Facoltativo) Per utilizzare prefissi S3 compatibili con Hive, scegli Hive-compatible S3 prefix (Prefisso S3 compatibile con Hive),Enable (Abilita).
6. (Facoltativo) Per partizionare i flussi di log per ora, scegli Every 1 hour (60 mins) Ogni ora (60 minuti).
7. (Facoltativo) Per aggiungere un tag al flusso di log, scegli Add new tag (Aggiungi nuovo tag) e specifica la chiave e il valore del tag.
8. Selezionare Create flow log (Crea log di flusso).

Per creare un log di flusso che pubblica in Amazon S3 utilizzando uno strumento a riga di comando

Utilizzare uno dei seguenti comandi.

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

L' AWS CLI esempio seguente crea un log di flusso che acquisisce tutto il traffico del gateway di transito per `tgw-00112233344556677` VPC e consegna i log di flusso a un bucket Amazon S3 chiamato. `flow-log-bucket` Il parametro `--log-format` specifica un formato personalizzato per i record di log di flusso.

```
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/'
```

Visualizza i record dei log di flusso del AWS Transit Gateway in Amazon S3

Per visualizzare i record del log di flusso pubblicati in Amazon S3

1. Apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/
2. Per Bucket name (Nome bucket), selezionare il bucket in cui vengono pubblicati i log di flusso.
3. Per Nome, seleziona la casella di controllo accanto al file di registro. Nel pannello di panoramica dell'oggetto, scegliere Download (Scarica).

Record di AWS Transit Gateway Flow Logs elaborati in Amazon S3

I file di log sono compressi. Se si aprono i file di log utilizzando la console Amazon S3, vengono decompressi e i record del log di flusso visualizzati. Se i file vengono scaricati, devono essere decompressi per visualizzare i record del log di flusso.

AWS Transit Gateway, record di Flow Logs in Amazon Data Firehose

Argomenti

- Ruoli IAM per la consegna tra account

- Creare il ruolo dell'account di origine AWS Transit Gateway Flow Logs per Amazon Data Firehose
- Creare il ruolo dell'account di destinazione AWS Transit Gateway Flow Logs per Amazon Data Firehose
- Crea un record AWS Transit Gateway Flow Logs da pubblicare su Amazon Data Firehose

I log di flusso possono pubblicare i dati dei log di flusso direttamente su Firehose. Puoi scegliere di pubblicare i log di flusso sullo stesso account del monitor delle risorse o su un altro account.

Prerequisiti

Durante la pubblicazione su Firehose, i dati del log di flusso vengono pubblicati in un flusso di distribuzione Firehose, in formato testo semplice. È innanzitutto necessario aver creato un flusso di distribuzione Firehose. Per i passaggi per creare un flusso di distribuzione, consulta Creating an Amazon Data Firehose Delivery Stream nella Amazon Data Firehose Developer Guide.

Prezzi

Si applicano le spese standard di acquisizione e consegna. Per ulteriori informazioni, apri Amazon CloudWatch Pricing, seleziona Logs e trova Vending Logs.

Ruoli IAM per la consegna tra account

Quando si pubblica su Kinesis Data Firehose, è possibile scegliere un flusso di consegna che si trova nello stesso account della risorsa da monitorare (l'account di origine) o in un altro account (l'account di destinazione). Per consentire la consegna dei log di flusso su più account a Firehose, è necessario creare un ruolo IAM nell'account di origine e un ruolo IAM nell'account di destinazione.

Roles

- Ruolo dell’account di origine
- Ruolo dell’account di destinazione

Ruolo dell’account di origine

Nell’account di origine, crea un ruolo che conceda le seguenti autorizzazioni. In questo esempio, il nome del ruolo è `mySourceRole` ma è possibile scegliere un nome diverso. L’ultima istruzione consente al ruolo nell’account di destinazione di assumere questo ruolo. Le istruzioni sulle condizioni assicurano che questo ruolo venga passato solo al servizio di consegna dei log e solo durante il

monitoraggio della risorsa specificata. Quando crei la tua policy, specifica le VPCs interfacce di rete o le sottoreti che stai monitorando con la chiave di condizione. `iam:AssociatedResourceARN`

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::111122223333:role/mySourceRole",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "delivery.logs.amazonaws.com"
                },
                "StringLike": {
                    "iam:AssociatedResourceARN": [
                        "arn:aws:ec2:region:source-account:transit-gateway/
tgw-0fb8421e2da853bf"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogDelivery",
                "logs:DeleteLogDelivery",
                "logs:ListLogDeliveries",
                "logs:GetLogDelivery"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::111122223333:role/
AWSLogDeliveryFirehoseCrossAccountRole"
        }
    ]
}
```

Verifica che questo ruolo abbia la seguente policy di attendibilità che consente al servizio di consegna dei log di assumere il ruolo.

JSON

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

Ruolo dell’account di destinazione

Nell'account di destinazione, crea un ruolo con un nome che inizia con AWSLogDeliveryFirehoseCrossAccountRole. Questo ruolo deve concedere le autorizzazioni riportate di seguito.

JSON

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

Assicurarsi che questo ruolo abbia la seguente policy di attendibilità, che consenta al ruolo creato nell'account di origine di assumere questo ruolo.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/mySourceRole"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Creare il ruolo dell'account di origine AWS Transit Gateway Flow Logs per Amazon Data Firehose

Dall'account di origine, crea il ruolo di origine nella AWS Identity and Access Management console.

Creazione del ruolo dell'account di origine

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione, scegli Policy.
3. Scegli Create Policy (Crea policy).
4. Nella pagina Create policy (Crea policy), eseguire le operazioni seguenti:
    1. Scegli JSON.
    2. Sostituisci il contenuto di questa finestra con la policy delle autorizzazioni all'inizio di questa sezione.
    3. Scegli Next: Tags (Successivo: Tag) e Next: Review (Successivo: Rivedi).
    4. Immetti un nome per la policy e una descrizione facoltativa, quindi scegli Create policy (Crea policy).

5. Nel pannello di navigazione, seleziona Roles (Ruoli).
6. Selezionare Create role (Crea ruolo).
7. Per Trusted entity type (Tipo di entità attendibile), scegli Custom trust policy (Policy di attendibilità personalizzata). Per Custom trust policy (Policy di attendibilità personalizzata), sostituisci `"Principal": {},` con quanto segue, che specifica il servizio di consegna dei log. Scegli Next (Successivo).

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

8. Sulla pagina Add permissions (Aggiungi autorizzazioni), seleziona la casella di controllo relativa alla policy creata in precedenza in questa procedura, quindi scegli Next (Successivo).
9. Immetti un nome per il ruolo e fornisci una descrizione facoltativa.
10. Seleziona Create role (Crea ruolo).

Creare il ruolo dell'account di destinazione AWS Transit Gateway Flow Logs per Amazon Data Firehose

Dall'account di destinazione, crea il ruolo di destinazione nella AWS Identity and Access Management console.

Creazione del ruolo dell’account di destinazione

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione, scegli Policy.
3. Scegli Create Policy (Crea policy).
4. Nella pagina Create policy (Crea policy), eseguire le operazioni seguenti:
    1. Scegli JSON.
    2. Sostituisci il contenuto di questa finestra con la policy delle autorizzazioni all'inizio di questa sezione.
    3. Scegli Next: Tags (Successivo: Tag) e Next: Review (Successivo: Rivedi).
    4. Inserisci un nome per la tua policy che inizia con AWSLogDeliveryFirehoseCrossAccountRole, quindi scegli Crea policy.

5. Nel pannello di navigazione, seleziona Roles (Ruoli).
6. Selezionare Create role (Crea ruolo).
7. Per Trusted entity type (Tipo di entità attendibile), scegli Custom trust policy (Policy di attendibilità personalizzata). Per Custom trust policy (Policy di attendibilità personalizzata), sostituisci `"Principal": {},` con quanto segue, che specifica il servizio di consegna dei log. Scegli Next (Successivo).

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

8. Sulla pagina Add permissions (Aggiungi autorizzazioni), seleziona la casella di controllo relativa alla policy creata in precedenza in questa procedura, quindi scegli Next (Successivo).
9. Immetti un nome per il ruolo e fornisci una descrizione facoltativa.
10. Seleziona Create role (Crea ruolo).

Crea un record AWS Transit Gateway Flow Logs da pubblicare su Amazon Data Firehose

Crea un Transit Gateway Flow Log da pubblicare su Amazon Data Firehose. Prima di creare il log di flusso, assicurati di aver impostato i ruoli dell'account IAM di origine e di destinazione per la distribuzione tra account e di aver creato il flusso di distribuzione Firehose. Per ulteriori informazioni, consulta Registri di flusso di Amazon Data Firehose. Puoi creare un log di flusso Firehose utilizzando la console Amazon VPC o la CLI. AWS

Per creare un log di flusso del gateway di transito da pubblicare su Firehose utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegliere Transit Gateway (Gateway di transito) o Transit Gateway Attachments (Collegamenti del gateway di transito alla VPN).
3. Selezionare le caselle di controllo per uno o più gateway di transito o collegamenti del gateway di transito alla VPN.
4. Scegli Actions (Operazioni), Create flow log (Crea flusso di log).
5. Per Destination (Destinazione), scegli Send to a Firehose Delivery System (Invia a un sistema di consegna Firehose).

6. Per Firehose Delivery Stream ARN (ARN flusso di consegna Firehose), scegli l'ARN di un flusso di consegna che hai creato dove deve essere pubblicato il log di flusso.
7. Per Log record format (Formato registro di log), seleziona il formato per il registro del flusso di log.
   - Per utilizzare il formato di record di log di flusso predefinito, seleziona Formato predefinito AWS .
   - Per creare un formato personalizzato, scegliere Custom format (Formato personalizzato). Per Log format (Formato log), scegliere i campi da includere nel record di log di flusso.
8. (Facoltativo) Per aggiungere un tag al flusso di log, scegli Add new tag (Aggiungi nuovo tag) e specifica la chiave e il valore del tag.
9. Selezionare Create flow log (Crea log di flusso).

Per creare un log di flusso da pubblicare su Firehose utilizzando lo strumento da riga di comando

Utilizzare uno dei seguenti comandi:

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

Il seguente esempio AWS CLI crea un log di flusso che acquisisce le informazioni sul gateway di transito e invia il log di flusso al flusso di distribuzione Firehose specificato.

```
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
```

Il seguente esempio AWS CLI crea un log di flusso che acquisisce le informazioni sul gateway di transito e invia il log di flusso a un flusso di consegna Firehose diverso dall'account di origine.

```
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
```

Crea e gestisci i log di flusso del AWS Transit Gateway utilizzando APIs o la CLI

Puoi eseguire le attività descritte in questa pagina tramite la riga di comando.

Le seguenti limitazioni si applicano all'utilizzo del comando: create-flow-logs

- `--resource-ids` ha un vincolo massimo di 25 tipi di risorse `TransitGateway` o `TransitGatewayAttachment`.
- `--traffic-type` non è un campo obbligatorio per impostazione predefinita. Se lo si fornisce per i tipi di risorse del gateway di transito, viene restituito un errore. Questo limite si applica solo ai tipi di risorsa del gateway di transito.
- `--max-aggregation-interval` ha un valore predefinito di `60`, ed è l'unico valore accettato per i tipi di risorse del gateway di transito. Se si tenta di passare qualsiasi altro valore, viene restituito un errore. Questo limite si applica solo ai tipi di risorsa del gateway di transito.
- `--resource-type` supporta due nuovi tipi di risorsa, il `TransitGateway` e il `TransitGatewayAttachment`.
- Se non si impostano i campi che si desiderano includere, `--log-format` include tutti i campi di log per i tipi di risorsa del gateway di transito. Questo vale solo per i tipi di risorse del gateway di transito.

Creazione di un log di flusso

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

Descrizione dei log di flusso

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

Visualizzazione dei record del log di flusso (eventi di log)

- get-log-events (AWS CLI)
- Get- CWLLog Event (AWS Tools for Windows PowerShell)

Eliminazione di un log di flusso

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

Visualizza i record dei log del AWS Transit Gateway Flow

Visualizza le informazioni sui log di flusso del tuo gateway di transito tramite Amazon VPC. Quando scegli una risorsa, vengono elencati tutti i log di flusso relativi a quella risorsa. Le informazioni visualizzate includono l'ID del log di flusso, la configurazione del log di flusso e le informazioni relative allo stato del log di flusso.

Per visualizzare informazioni sui registri di flusso per i gateway di transito

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegliere Transit Gateway (Gateway di transito) o Transit Gateway Attachments (Collegamenti del gateway di transito alla VPN).
3. Selezionare un gateway di transito o un collegamento del gateway di transito alla VPN e scegliere Flow Logs (Registri di flusso). Le informazioni relative ai log di flusso vengono visualizzate nella scheda. La colonna Destination type (Tipo di destinazione) indica la destinazione in cui i log di flusso vengono pubblicati.

Gestione dei AWS tag Transit Gateway Flow Logs

Puoi aggiungere o rimuovere tag per un log di flusso nelle console Amazon EC2 e Amazon VPC.

Per aggiungere o rimuovere tag per un log di flusso del gateway di transito

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegliere Transit Gateway (Gateway di transito) o Transit Gateway Attachments (Collegamenti del gateway di transito alla VPN).

3. Selezionare un gateway di transito o un collegamento del gateway di transito alla VPN
4. Scegliere Manage tags (Gestisci tag) per il log di flusso richiesto.
5. Per aggiungere un nuovo tag, scegliere Create Tag (Crea tag). Per rimuovere un tag, scegliere il pulsante Elimina (x).
6. Scegli Save (Salva).

Cerca nei record di AWS Transit Gateway Flow Logs

Puoi cercare i record dei log di flusso pubblicati su CloudWatch Logs utilizzando la CloudWatch console Logs. È possibile utilizzare filtri metrici per filtrare i record del log di flusso. I record del log di flusso sono delimitati da spazio.

Per cercare i record del log di flusso utilizzando la CloudWatch console Logs

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel pannello di navigazione scegli Log, quindi Gruppi di log.
3. Selezionare il gruppo di flussi di log contenente il registro di flusso. Viene mostrato un elenco di flussi di log per ogni gateway di transito.
4. Selezionare il singolo flusso di log se si conosce il gateway di transito che si sta cercando. In alternativa, scegliere Cerca gruppo di log per cercare l'intero gruppo di log. Ciò potrebbe richiedere del tempo se nel gruppo di flussi di log sono presenti molti gateway di transito, o in base all'intervallo di tempo selezionato.
5. Per gli Eventi Filtro, immettere la stringa seguente. Ciò presuppone che il record del log di flusso utilizzi il formato predefinito.

```
[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. Modificare il filtro in base alle esigenze specificando i valori per i campi. Negli esempi seguenti il filtro viene applicato in base a specifici indirizzi IP di origine.

```
[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]
```

L'esempio seguente filtra in base all'ID del gateway di transito tgw-123abc456bca, alla porta di destinazione e al numero di byte.

```
[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]
```

Eliminare un record AWS Transit Gateway Flow Logs

È possibile eliminare un log di flusso del gateway di transito usando la console Amazon VPC.

Queste procedure disabilitano il servizio del log di flusso per una risorsa. L'eliminazione di un log di flusso non elimina i flussi di log esistenti da CloudWatch Logs o i file di log da Amazon S3. I dati del log di flusso esistenti devono essere eliminati utilizzando la rispettiva console del servizio. Inoltre, l'eliminazione di un log di flusso pubblicato su Amazon S3 non rimuove le policy dei bucket e gli elenchi di controllo degli accessi ai file di registro (). ACLs

Per eliminare un log di flusso del gateway di transito

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione selezionare Transit gateways (Gateway di transito).
3. Scegliere un Transit gateway ID (ID gateway di transito).
4. Nella sezione Flow logs (Registri di flusso), scegliere i registri di flusso che si desiderano eliminare.
5. Scegliere Actions (Operazioni), quindi scegliere Delete flow logs (Elimina registri di flusso).
6. Confermare che si desidera eliminare il flusso scegliendo Delete (Elimina).

Metriche ed eventi in AWS Transit Gateway

È possibile utilizzare le seguenti funzionalità per monitorare i gateway di transito, analizzare i modelli di traffico e risolvere i problemi relativi ai gateway di transito.

CloudWatch metriche

Puoi utilizzare Amazon CloudWatch per recuperare le statistiche sui punti dati per i tuoi gateway di transito sotto forma di set ordinato di dati di serie temporali, noti come metriche. È possibile utilizzare questi parametri per verificare che le prestazioni del sistema siano quelle previste. Per ulteriori informazioni, consulta CloudWatch metriche in AWS Transit Gateway.

Registri di flusso di Transit Gateway

È possibile utilizzare i registri di flusso di Transit Gateway per acquisire informazioni dettagliate sul traffico di rete sui gateway di transito. Per ulteriori informazioni, consulta Registri di flusso di Transit Gateway.

Log di flusso VPC

Puoi utilizzare i log di flusso VPC per acquisire informazioni dettagliate sul traffico in entrata e in uscita dai gateway di transito collegati ai tuoi gateway di transito. VPCs Per ulteriori informazioni, consulta Log di flusso VPC nella Guida per l'utente di Amazon VPC.

CloudTrail registri

Puoi utilizzarle AWS CloudTrail per acquisire informazioni dettagliate sulle chiamate effettuate all'API del gateway di transito e archiviarle come file di registro in Amazon S3. È possibile utilizzare questi CloudTrail registri per determinare quali chiamate sono state effettuate, l'indirizzo IP di origine da cui proviene la chiamata, chi ha effettuato la chiamata, quando è stata effettuata la chiamata e così via. Per ulteriori informazioni, consulta CloudTrail registri.

CloudWatch Eventi che utilizzano Network Manager

È possibile utilizzarli AWS Network Manager per inoltrare CloudWatch gli eventi e quindi indirizzarli a funzioni o flussi di destinazione. Network Manager genera eventi per le modifiche alla topologia, gli aggiornamenti del routing e gli aggiornamenti di stato, che possono essere utilizzati per avvisare l'utente dei cambiamenti nei gateway di transito. Per ulteriori informazioni, consulta Monitoraggio della rete globale con CloudWatch eventi nella Guida per l'utente di AWS Global Networks for Transit Gateways.

CloudWatch metriche in AWS Transit Gateway

Amazon VPC pubblica punti dati su Amazon CloudWatch per i tuoi gateway di transito e gli allegati dei gateway di transito. CloudWatchconsente di recuperare le statistiche su tali punti dati sotto forma di un insieme ordinato di dati di serie temporali, noti come metriche. Pensa a una metrica come a una variabile da monitorare e ai dati di utilizzo come ai valori di questa variabile nel tempo. A ogni dato sono associati una marcatura temporale e un'unità di misura facoltativa.

Puoi utilizzare le metriche per verificare che le prestazioni del sistema siano quelle previste. Ad esempio, puoi creare un CloudWatch allarme per monitorare una metrica specifica e avviare un'azione (come l'invio di una notifica a un indirizzo e-mail) se la metrica non rientra nell'intervallo che consideri accettabile.

Amazon VPC misura e invia i propri parametri a CloudWatch intervalli di 60 secondi.

Per ulteriori informazioni, consulta la Amazon CloudWatch User Guide.

Indice

Metriche dei gateway di transito

Il namespace `AWS/TransitGateway` include le metriche descritte di seguito.

Tutte le metriche vengono sempre riportate. I loro valori dipendono dal traffico attraverso il gateway di transito. Vedi Dimensioni metriche del gateway di transito per le dimensioni supportate.

Parametro	Descrizione
`BytesDropCountBlackhole`	Il numero di byte persi perché intercettati da una route `blackhole` . Statistiche: l'unica statistica significativa è `Sum`.
`BytesDropCountNoRoute`	Il numero di byte persi perché non corrispondenti a una route esistente.

Parametro	Descrizione
	Statistiche: l'unica statistica significativa è `Sum`.
`BytesIn`	Numero di byte ricevuti dal gateway di transito. Statistiche: l'unica statistica significativa è `Sum`.
`BytesOut`	Numero di byte inviati dal gateway di transito. Statistiche: l'unica statistica significativa è `Sum`.
`PacketsIn`	Il numero di pacchetti ricevuti dal gateway di transito. Statistiche: l'unica statistica significativa è `Sum`.
`PacketsOut`	Il numero di pacchetti inviati dal gateway di transito. Statistiche: l'unica statistica significativa è `Sum`.
`PacketDropCountBlackhole`	Il numero di pacchetti persi perché intercettati da una route `blackhole` . Statistiche: l'unica statistica significativa è `Sum`.
`PacketDropCountNoRoute`	Il numero di pacchetti persi perché non presente una route corrispondente. Statistiche: l'unica statistica significativa è `Sum`.
`PacketDropCountTTLExpired`	Il numero di pacchetti persi a causa della scadenza del TTL. Statistiche: l'unica statistica significativa è `Sum`.

Metriche a livello di allegato e zona di disponibilità

Le metriche seguenti sono disponibili per gli allegati del gateway di transito. Tutti i parametri degli allegati vengono pubblicati nell'account del proprietario del gateway di transito. Anche i singoli parametri degli allegati vengono pubblicati nell'account del proprietario dell'allegato. Il proprietario dell'allegato può visualizzare solo i parametri del proprio allegato. Per ulteriori informazioni sui tipi di allegati supportati, vedi the section called “Collegamenti alle risorse”.

Le metriche delle zone di disponibilità sono disponibili per aver abilitato le zone di disponibilità () sugli allegati del gateway di transito. AZs Solo gli allegati VPC supportano le metriche Per-AZ. Tutte le metriche di livello AZ vengono pubblicate sull'account del proprietario del gateway di transito. Le metriche AZ individuali per un allegato vengono pubblicate anche nell'account del proprietario dell'allegato. Il proprietario dell'allegato può visualizzare solo le metriche per-AZ per il proprio allegato.

Tutte le metriche vengono sempre riportate. I loro valori dipendono dal traffico in and/or uscita dall'allegato del gateway di transito. Vedi Dimensioni metriche del gateway di transito per le dimensioni supportate.

Parametro	Descrizione
`BytesDropCountBlackhole`	Numero di byte eliminati perché corrispondono a una route `blackhole` nell'allegato del gateway di transito. Statistiche: l'unica statistica significativa è `Sum`.
`BytesDropCountNoRoute`	Numero di byte eliminati perché non corrispondono a una route nell'allegato del gateway di transito. Statistiche: l'unica statistica significativa è `Sum`.
`BytesIn`	Numero di byte ricevuti dal gateway di transito dall'allegato. Statistiche: l'unica statistica significativa è `Sum`.
`BytesOut`	Numero di byte inviati dal gateway di transito all'allegato. Statistiche: l'unica statistica significativa è `Sum`.
`PacketsIn`	Numero di pacchetti ricevuti dal gateway di transito dall'allegato. Statistiche: l'unica statistica significativa è `Sum`.
`PacketsOut`	Numero di pacchetti inviati dal gateway di transito all'allegato. Statistiche: l'unica statistica significativa è `Sum`.
`PacketDropCountBlackhole`	Numero di pacchetti eliminati perché corrispondono a una route `blackhole` nell'allegato del gateway di transito.

Parametro	Descrizione
	Statistiche: l'unica statistica significativa è `Sum`.
`PacketDropCountNoRoute`	Il numero di pacchetti persi perché non presente una route corrispondente. Statistiche: l'unica statistica significativa è `Sum`.
`PacketDropCountTTLExpired`	Il numero di pacchetti persi a causa della scadenza del TTL. Statistiche: l'unica statistica significativa è `Sum`.

Dimensioni metriche del gateway di transito

Filtra i dati metrici del gateway di transito utilizzando le seguenti dimensioni:

Dimensione	Descrizione
`TransitGateway`	Filtra i dati delle metriche in base al gateway di transito.
`TransitGatewayAttachment`	Filtra i dati delle metriche in base all'allegato del gateway di transito.
`TransitGateway` , `AvailabilityZone`	Filtra i dati metrici sia per gateway di transito che per zona di disponibilità.
`TransitGatewayAttachment` , `AvailabilityZone`	Filtra i dati metrici sia in base all'allegato del gateway di transito che alla zona di disponibilità.

Registra le chiamate API AWS Transit Gateway utilizzando AWS CloudTrail

AWS Transit Gateway; è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, ruolo o un Servizio AWS. CloudTrail acquisisce tutte le chiamate API per Transit Gateway come eventi. Le chiamate acquisite includono chiamate dalla console Transit Gateway e chiamate in codice alle operazioni dell'API Transit Gateway. Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare la richiesta effettuata a Transit Gateway, l'indirizzo IP da cui è stata effettuata la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con le credenziali utente root o utente.
- Se la richiesta è stata effettuata per conto di un utente del Centro identità IAM.
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro Servizio AWS.

CloudTrail è attivo nel tuo account Account AWS quando crei l'account e hai automaticamente accesso alla cronologia degli CloudTrail eventi. La cronologia CloudTrail degli eventi fornisce un record visualizzabile, ricercabile, scaricabile e immutabile degli ultimi 90 giorni di eventi di gestione registrati in un. Regione AWSPer ulteriori informazioni, consulta Lavorare con la cronologia degli CloudTrail eventi nella Guida per l'utente.AWS CloudTrail Non sono CloudTrail previsti costi per la visualizzazione della cronologia degli eventi.

Per una registrazione continua degli eventi degli Account AWS ultimi 90 giorni, crea un trail o un data store di eventi CloudTrailLake.

CloudTrail sentieri

Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Tutti i percorsi creati utilizzando il Console di gestione AWS sono multiregionali. È possibile creare un trail per una singola Regione o per più Regioni tramite AWS CLI. La creazione di un percorso multiregionale è consigliata in quanto consente di registrare l'intera attività del proprio Regioni AWS account. Se si crea un trail per una singola Regione, è possibile visualizzare solo gli eventi registrati nella

Regione AWS del trail. Per ulteriori informazioni sui trail, consulta Creating a trail for your Account AWS e Creating a trail for an organization nella Guida per l'utente di AWS CloudTrail .

Puoi inviare gratuitamente una copia dei tuoi eventi di gestione in corso al tuo bucket Amazon S3 CloudTrail creando un percorso, tuttavia ci sono costi di storage di Amazon S3. Per ulteriori informazioni sui CloudTrail prezzi, consulta la pagina Prezzi.AWS CloudTrail Per informazioni sui prezzi di Amazon S3, consulta Prezzi di Amazon S3.

CloudTrail Archivi di dati sugli eventi di Lake

CloudTrail Lake ti consente di eseguire query basate su SQL sui tuoi eventi. CloudTrail Lake converte gli eventi esistenti in formato JSON basato su righe in formato Apache ORC. ORC è un formato di archiviazione a colonne ottimizzato per il recupero rapido dei dati. Gli eventi vengono aggregati in archivi di dati degli eventi, che sono raccolte di eventi immutabili basate sui criteri selezionati applicando i selettori di eventi avanzati. I selettori applicati a un archivio di dati degli eventi controllano quali eventi persistono e sono disponibili per l'esecuzione della query. Per ulteriori informazioni su CloudTrail Lake, consulta Working with AWS CloudTrail Lake nella Guida per l'utente.AWS CloudTrail

CloudTrail Gli archivi e le richieste di dati sugli eventi di Lake comportano dei costi. Quando crei un datastore di eventi, scegli l'opzione di prezzo da utilizzare per tale datastore. L'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi, nonché il periodo di conservazione predefinito e quello massimo per il datastore di eventi. Per ulteriori informazioni sui CloudTrail prezzi, consulta Prezzi.AWS CloudTrail

Eventi di gestione Transit Gateway

Gli eventi di gestione forniscono informazioni sulle operazioni di gestione eseguite sulle risorse del sistema Account AWS. Queste operazioni sono definite anche operazioni del piano di controllo (control-plane). Per impostazione predefinita, CloudTrail registra gli eventi di gestione.

AWS Transit Gateway registra tutte le operazioni del piano di controllo Transit Gateway come eventi di gestione. Per un elenco delle operazioni del piano di controllo AWS Transit Gateway a cui Transit Gateway accede CloudTrail, consulta le azioni AWS Transit Gateway nell'Amazon EC2 API Reference.

Esempi di eventi Transit Gateway

Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'operazione API richiesta, la data e l'ora dell'operazione, i parametri della richiesta e così via.

CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi gli eventi non vengono visualizzati in un ordine specifico.

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

I file di registro includono eventi per tutte le chiamate API per il tuo AWS account, non solo per le chiamate API Transit Gateway. Puoi individuare le chiamate all'API del gateway di transito controllando gli elementi `eventSource` con il valore `ec2.amazonaws.com`. Per visualizzare il record di un'operazione specifica, ad esempio `CreateTransitGateway`, verifica la presenza di elementi `eventName` con il nome dell'operazione.

Di seguito è riportato un esempio di record di CloudTrail registro per l'API Transit Gateway per un utente che ha creato un gateway di transito utilizzando la console. Puoi identificare l'interfaccia a riga di comando utilizzando l'elemento `userAgent`. Puoi identificare le chiamate API invocate utilizzando l'elemento `eventName`. Le informazioni relative all'utente (`Alice`) sono disponibili nell'elemento `userIdentity`.

Example Esempio: 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"
}
```

Gestione delle identità e degli accessi in AWS Transit Gateway

AWS utilizza credenziali di sicurezza per identificarti e concederti l'accesso alle tue AWS risorse. Puoi utilizzare le funzionalità di AWS Identity and Access Management (IAM) per consentire ad altri utenti, servizi e applicazioni di utilizzare le tue AWS risorse completamente o in modo limitato, senza condividere le tue credenziali di sicurezza.

Per impostazione predefinita, gli utenti IAM non sono autorizzati a creare, visualizzare o modificare AWS le risorse. Per consentire a un utente di accedere a risorse come un gateway di transito e di eseguire attività, è necessario creare una policy IAM che conceda all'utente l'autorizzazione per utilizzare le risorse specifiche e le operazioni API di cui ha bisogno, quindi collegare la policy al gruppo a cui appartiene tale utente. Quando si collega una policy a un utente o a un gruppo di utenti, viene concessa o rifiutata agli utenti l'autorizzazione per l'esecuzione delle attività specificate sulle risorse specificate.

Per lavorare con un gateway di transito, una delle seguenti politiche AWS gestite potrebbe soddisfare le tue esigenze:

- AmazonEC2FullAccess
- AmazonEC2ReadOnlyAccess
- PowerUserAccess
- ReadOnlyAccess

Policy di esempio per la gestione dei gateway di transito

Di seguito sono riportate le policy IAM di esempio per l'utilizzo dei gateway di transito.

Creazione di un gateway di transito con i tag necessari

L'esempio seguente consente agli utenti di creare gateway di transito. La chiave di condizione `aws:RequestTag` richiede agli utenti di contrassegnare il gateway di transito con il tag `stack=prod`. La chiave di condizione `aws:TagKeys` utilizza il modificatore `ForAllValues` per indicare che soltanto la chiave `stack` è consentita nella richiesta (non è possibile specificare altri tag). Se gli utenti non passano questo tag specifico quando creano il gateway di transito o se non specificano affatto i tag, la richiesta non riesce.

La seconda istruzione utilizza la chiave di condizione `ec2:CreateAction` per consentire agli utenti di creare i tag soltanto nel contesto di `CreateTransitGateway`.

JSON

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

Utilizzo delle tabelle di routing del gateway di transito

L'esempio seguente consente agli utenti di creare ed eliminare tabelle di routing del gateway di transito solo per un gateway di transito specifico (`tgw-11223344556677889`). Gli utenti possono inoltre creare e sostituire route in qualsiasi tabella di routing del gateway di transito, ma solo per gli allegati con il 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/*"
```

```
        }
    ]
}
```

Usa ruoli collegati ai servizi per i gateway di transito in Transit Gateway AWS

Amazon VPC utilizza ruoli collegati ai servizi per le autorizzazioni di cui ha bisogno per eseguire chiamate ad altri servizi AWS per tuo conto. Per ulteriori informazioni, consulta Ruoli collegati ai servizi nella Guida per l'utente di IAM.

Ruolo collegato ai servizi per il gateway di transito

Amazon VPC utilizza ruoli collegati ai servizi per le autorizzazioni di cui ha bisogno per eseguire chiamate ad altri servizi AWS per tuo conto quando lavori con un gateway di transito.

Autorizzazioni concesse dal ruolo collegato ai servizi

Amazon VPC utilizza il ruolo collegato al servizio denominato AWSServiceRoleForVPCTransitGateway per eseguire le seguenti azioni per tuo conto quando lavori con un gateway di transito:

- `ec2:CreateNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2:ModifyNetworkInterfaceAttribute`
- `ec2:DeleteNetworkInterface`
- `ec2:CreateNetworkInterfacePermission`
- `ec2:AssignIpv6Addresses`
- `ec2:UnAssignIpv6Addresses`

Il ruolo AWSServiceRoleForVPCTransitGateway prevede che i seguenti servizi assumano il ruolo:

- `transitgateway.amazonaws.com`

AWSServiceRoleForVPCTransitGateway utilizza la policy AWSVPCTransitGatewayServiceRolePolicy gestita.

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato al servizio è necessario configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente IAM.

Creazione del ruolo collegato ai servizi

Non è necessario creare manualmente il ruolo AWSServiceRoleForVPCTransitGateway. Amazon VPC crea questo ruolo quando colleghi un VPC nel tuo account a un gateway di transito.

Modifica del ruolo collegato ai servizi

Puoi modificare la descrizione di AWSServiceRoleForVPCTransitGateway utilizzando IAM. Per ulteriori informazioni, consulta Edit a service-linked role description nella Guida per l'utente IAM.

Eliminazione del ruolo collegato ai servizi

Se non hai più bisogno di utilizzare i gateway di transito, ti consigliamo di eliminare AWSServiceRoleForVPCTransitGateway.

Puoi eliminare questo ruolo collegato al servizio solo dopo aver eliminato tutti gli allegati VPC del gateway di transito nel tuo account. AWS Questa procedura impedisce di rimuovere involontariamente l'autorizzazione ad accedere ai collegamenti al VPC.

Per eliminare i ruoli collegati ai servizi, puoi utilizzare la console IAM, l'interfaccia a riga di comando IAM CLI o l'API IAM. Per ulteriori dettagli, consulta Delete a service-linked role nella Guida per l'utente IAM.

Dopo aver eliminato AWSServiceRoleForVPCTransitGateway, Amazon VPC crea nuovamente il ruolo se colleghi un VPC nel tuo account a un gateway di transito.

AWS politiche gestite per i gateway di transito in AWS Transit Gateway

Una politica AWS gestita è una politica autonoma creata e amministrata da AWS. AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Si consiglia

pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i propri casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare Policy gestite da AWS nella Guida per l'utente di IAM.

Per lavorare con un gateway di transito, una delle seguenti politiche AWS gestite potrebbe soddisfare le tue esigenze:

- AmazonEC2FullAccess
- AmazonEC2ReadOnlyAccess
- PowerUserAccess
- ReadOnlyAccess

AWS politica gestita: AWSVPCTransit GatewayServiceRolePolicy

Questa politica è allegata al ruolo AWSServiceRoleForVPCTransitGateway. Ciò consente ad Amazon VPC di creare e gestire risorse per collegamento del gateway di transito alla VPN.

Per vedere le autorizzazioni per questa policy, consulta AWSVPCTransitGatewayServiceRolePolicy nella Guida di riferimento sulle policy gestite da AWS .

Transit Gateway si aggiorna alle politiche AWS gestite

Visualizza i dettagli sugli aggiornamenti alle politiche AWS gestite per i gateway di transito da quando Amazon VPC ha iniziato a tracciare queste modifiche nel marzo 2021.

Modifica	Descrizione	Data
Amazon VPC ha iniziato a monitorare le modifiche	Amazon VPC ha iniziato a tracciare le modifiche alle sue politiche AWS gestite.	1° marzo 2021

Rete ACLs per gateway di transito in AWS Transit Gateway

Una lista di controllo accessi di rete (NACL) è un livello facoltativo di protezione.

Le regole delle liste di controllo accessi di rete (NACL) vengono applicate in modo diverso, a seconda dello scenario:

- the section called “Stessa sottorete per le EC2 istanze e l'associazione dei gateway di transito”
- the section called “Sottoreti diverse per EC2 le istanze e l'associazione dei gateway di transito”

Stessa sottorete per le EC2 istanze e l'associazione dei gateway di transito

Prendi in considerazione una configurazione in cui siano presenti EC2 istanze e un'associazione di gateway di transito nella stessa sottorete. Lo stesso ACL di rete viene utilizzato sia per il traffico dalle EC2 istanze al gateway di transito sia per il traffico dal gateway di transito alle istanze.

Le regole delle liste di controllo accessi di rete (NACL) per il traffico dalle istanze al gateway di transito vengono applicate nel modo seguente:

- Le regole in uscita utilizzano l'indirizzo IP di destinazione per la valutazione.
- Le regole in ingresso utilizzano l'indirizzo IP di origine per la valutazione.

Le regole delle liste di controllo accessi di rete (NACL) per il traffico dal gateway di transito alle istanze vengono applicate nel modo seguente:

- Le regole in uscita non vengono valutate.
- Le regole in entrata non vengono valutate.

Sottoreti diverse per EC2 le istanze e l'associazione dei gateway di transito

Prendi in considerazione una configurazione in cui sono presenti EC2 istanze in una sottorete e un'associazione di gateway di transito in una sottorete diversa e ogni sottorete è associata a un ACL di rete diverso.

Le regole ACL di rete vengono applicate come segue per la sottorete dell'istanza: EC2

- Le regole in uscita utilizzano l'indirizzo IP di destinazione per valutare il traffico dalle istanze al gateway di transito.

- Le regole in entrata utilizzano l'indirizzo IP di origine per valutare il traffico dal gateway di transito alle istanze.

Le regole dell'NACL per la sottorete del gateway di transito vengono applicate come segue:

- Le regole in uscita utilizzano l'indirizzo IP di destinazione per valutare il traffico dal gateway di transito alle istanze.
- Le regole in uscita non vengono utilizzate per valutare il traffico dalle istanze al gateway di transito.
- Le regole in entrata utilizzano l'indirizzo IP di origine per valutare il traffico dalle istanze al gateway di transito.
- Le regole in entrata non vengono utilizzate per valutare il traffico dal gateway di transito alle istanze.

Best practice

Utilizza una sottorete separata per ogni allegato VPC del gateway di transito. Per ogni sottorete, utilizzate un piccolo CIDR, ad esempio /28, in modo da avere più indirizzi per le risorse. EC2 Quando usi una sottorete separata, puoi configurare quanto segue:

- Tieni aperta la lista di controllo accessi di rete in ingresso e in uscita associata alla sottorete del gateway di transito.
- A seconda del flusso di traffico, puoi applicarlo NACLs alle sottoreti del carico di lavoro.

Per ulteriori informazioni sul funzionamento degli allegati VPC, consulta the section called “Collegamenti alle risorse”.

AWS Quote Transit Gateway

Hai Account AWS le seguenti quote (precedentemente denominate limiti) relative ai gateway di transito. Salvo diversa indicazione, ogni quota si applica a una Regione specifica.

La console Service Quotas fornisce informazioni sulle quote per il tuo account. È possibile utilizzare la console Service Quotas per visualizzare le quote di default e richiedere aumenti delle quote per le quote regolabili. Per ulteriori informazioni, consulta Richiesta di un aumento di quota nella Guida per l'utente delle Service Quotas.

Se una quota regolabile non è ancora disponibile nelle Service Quotas, è possibile aprire un ticket di supporto.

Ambito generale

Name	Predefinita	Adattabile
Gateway di transito per account	5	Sì
Blocchi CIDR per gateway di transito	5	No

I blocchi CIDR sono utilizzati nella funzione the section called “Collegamenti Connect e peer Connect”.

Routing

Name	Predefinita	Adattabile
Tabelle di routing del gateway di transito per gateway di transito	20	Sì
Percorsi combinati totali (dinamici e statici) su tutte le tabelle delle rotte per un singolo gateway di transito	10.000	Contatta il tuo Solutions Architect (SA) o il Technical Account Manager

Name	Predefinita	Adattabile
		(TAM) per ulteriore assistenza.
Instradamenti dinamici annunciati da un'appliance router virtuale a un peer Connect	1.000	Contatta il tuo Solutions Architect (SA) o il Technical Account Manager (TAM) per ulteriore assistenza.
Instradamenti annunciati da un peer Connect su un gateway di transito a un'appliance router virtuale	5.000	No
Route statiche per un prefisso di un singolo allegato	1	No

Gli instradamenti annunciati provengono dalla tabella di instradamento associata al collegamento Connect.

Collegamenti del gateway di transito

Un gateway di transito non può avere più di un allegato VPC allo stesso VPC.

Name	Predefinita	Adattabile
Collegamenti per gateway di transito	5.000	Sì
Gateway di transito per VPC	5	No
Collegamenti peering per gateway di transito	50	Sì
Collegamenti peering in sospeso per gateway di transito	10	Sì

Name	Predefinita	Adattabile
Allegati di peering tra due gateway di transito o tra un gateway di transito e un core network edge (CNE) di Cloud WAN	1	No
Peer di Connect (tunnel GRE) per collegamento Connect	4	No
Concentratori VPN per gateway di transito	5	No
Connessioni VPN per VPN Concentrator	100	No

Larghezza di banda

Esistono molti fattori che possono influire sulla larghezza di banda ottenuta tramite una connessione Site-to-Site VPN, tra cui, a titolo esemplificativo ma non esaustivo: dimensione dei pacchetti, mix di traffico (TCP/UDP), definizione o limitazione delle politiche sulle reti intermedie, condizioni meteorologiche relative a Internet e requisiti applicativi specifici. Per i collegamenti VPC, gateway Direct Connect , o collegamenti del gateway di transito alla VPN peer-to-peer, cercheremo di fornire una larghezza di banda aggiuntiva oltre al valore predefinito.

Name	Predefinita	Adattabile
Larghezza di banda per collegamento VPC per zona di disponibilità	Fino a 100 Gb/s	Contatta il tuo Solutions Architect (SA) o il Technical Account Manager (TAM) per ulteriore assistenza.
Pacchetti al secondo per gateway di transito, collegamento VPC per zona di disponibilità	Fino a 7.500.000	Contatta il tuo Solutions Architect (SA) o il Technical Account Manager (TAM) per ulteriore assistenza.

Name	Predefinita	Adattabile
Larghezza di banda per la connessione Direct Connect gateway o gateway di transito peer-to-peer per zona di disponibilità disponibile nella regione	Fino a 100 Gb/s	Contatta il tuo Solutions Architect (SA) o il Technical Account Manager (TAM) per ulteriore assistenza.
Pacchetti al secondo per allegato del gateway di transito (Direct Connect e allegati peering) per zona di disponibilità disponibile nella regione	Fino a 7.500.000	Contatta il tuo Solutions Architect (SA) o il Technical Account Manager (TAM) per ulteriore assistenza.
Larghezza di banda massima per peer Connect (tunnel GRE) per collegamento Connect	Fino a 5 Gb/s	No
Numero massimo di pacchetti al secondo per peer Connect	Fino a 300.000	No

È possibile utilizzare routing a percorsi multipli a costo uguale ECMP per ottenere una larghezza di banda VPN maggiore tramite l'aggregazione di molteplici tunnel VPN. Per utilizzare ECMP, la connessione VPN deve essere configurata per il routing dinamico. ECMP non è supportato nelle connessioni VPN che utilizzano routing statico.

È possibile creare fino a 4 peer Connect per allegato Connect (fino a 20 Gbps di larghezza di banda totale per allegato Connect), purché l'allegato di trasporto sottostante (VPC o Direct Connect) supporti la larghezza di banda richiesta. Puoi utilizzare l'instradamento ECMP per ottenere una lunghezza di banda maggiore con il dimensionamento orizzontale tra più peer di Connect dello stesso collegamento Connect o tra più collegamenti Connect sullo stesso gateway di transito. Il gateway di transito non può utilizzare ECMP tra peering BGP dello stesso peer Connect.

Per i limiti di larghezza di banda e pacchetti con il tunnel VPN, fai riferimento alla larghezza di banda e al throughput della VPN.

Direct Connect gateway

Name	Predefinita	Adattabile
Direct Connect gateway per gateway di transito	20	No
Gateway di transito per gateway Direct Connect	6	No

Unità di trasmissione massima (MTU)

- L'unità massima di trasmissione (MTU) di una connessione di rete è la dimensione, in byte, del pacchetto più grande consentito trasferibile attraverso la connessione. Maggiore è la MTU di una connessione, maggiore è la quantità di dati trasferibili in un unico pacchetto. Un gateway di transito supporta un MTU di 8500 byte per il traffico tra VPCs, Transit Direct Connect Gateway Connect e gli allegati di peering (allegati peering intra-regionali, interregionali e Cloud WAN). Il traffico su connessioni VPN può avere una MTU di 1500 byte.
- Quando si esegue la migrazione dal peering VPC per utilizzare un gateway di transito, una mancata corrispondenza di dimensioni MTU tra il peering VPC e il gateway di transito potrebbe causare il calo di alcuni pacchetti di traffico asimmetrico. Aggiorna entrambi contemporaneamente per evitare che i pacchetti VPCs jumbo cadano a causa di una mancata corrispondenza delle dimensioni.
- Il gateway di transito applica il clamping MSS (Maximum Segment Size) a tutti i pacchetti. Per ulteriori informazioni, consulta RFC879.
- Per informazioni dettagliate sulle quote Site-to-Site VPN per MTU, consulta Maximum Transmission Unit (MTU) nella Guida per l'utente.AWS Site-to-Site VPN
- I gateway di transito supportano Path MTU Discovery (PMTUD) per l'ingresso del traffico sugli allegati VPC e Connect. Il gateway di transito genera i pacchetti for e for packets. `FRAG_NEEDED` ICMPv4 `Packet Too Big (PTB)` ICMPv6 I gateway di transito non supportano PMTUD sugli allegati VPN Site-to-site, Direct Connect e Peering. Per ulteriori informazioni su Path MTU Discovery, consulta Path MTU Discovery nella Amazon VPC User Guide

Multicast

> **Note**
>
> Transit gateway multicast potrebbe non essere adatto per il trading ad alta frequenza o per applicazioni sensibili alle prestazioni. Ti consigliamo vivamente di rivedere i seguenti limiti per il multicast. Contatta il tuo account o il team di Solution Architect per una revisione dettagliata dei tuoi requisiti prestazionali.

Name	Predefinita	Adattabile
Domini multicast per gateway di transito	20	Contatta il tuo Solutions Architect (SA) o il Technical Account Manager (TAM) per ulteriore assistenza.
Interfacce di rete multicast per gateway di transito	10.000	Contatta il tuo Solutions Architect (SA) o il Technical Account Manager (TAM) per ulteriore assistenza.
Associazioni di dominio multicast per VPC	20	Contatta il tuo Solutions Architect (SA) o il Technical Account Manager (TAM) per ulteriore assistenza.
Membri e sorgenti di gruppi statici e IGMPv2 multicast per gateway di transito	10.000	No

Name	Predefinita	Adattabile
Membri del gruppo statico e IGMPv2 multicast per gruppo multicast del gateway di transito	100	No
Throughput multicast massimo per flusso	1 Gb/s	No
Throughput multicast aggregato massimo per zona di disponibilità	20 Gb/s	No
Numero massimo di pacchetti al secondo per flusso (meno di 10 ricevitori)	75.000	No
Numero massimo di pacchetti al secondo per flusso (superiore a 10 ricevitori)	15.000	No
Numero massimo di pacchetti aggregati al secondo (meno di 10 ricevitori)	2.500.000	No
Numero massimo di pacchetti aggregati al secondo (più di 10 ricevitori)	500.000	No

AWS Gestore di rete

Nome	Predefinita	Adattabile
Reti globali per Account AWS	5	Sì
Dispositivi per rete globale	200	Sì
Collegamenti per rete globale	200	Sì
Siti per rete globale	200	Sì
Connessioni per rete globale	500	No

Risorse aggiuntive delle quote

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Site-to-Site Quote VPN nella Guida per l'AWS Site-to-Site VPN utente
- Quote Amazon VPC nella Guida per l'utente di Amazon VPC
- Quote di Direct Connect nella Guida per l'utente AWS Direct Connect

Cronologia dei documenti per i gateway di transito

Nella tabella seguente vengono descritte le release per i gateway di transito.

Modifica	Descrizione	Data
Allocazione flessibile dei costi	Configura politiche flessibili di allocazione dei costi per controllare la modalità di allocazione dei costi di elaborazione e trasferimento dei dati all'interno dell'organizzazione.	20 novembre 2025
Supporto di crittografia per gateway di transito	Gestione dell'Encryption Support sui gateway di transito encryption-in-transit per applicarlo a tutto il traffico.	20 novembre 2025
Allegati alle funzioni di rete	Crea un collegamento a una funzione di rete a cui connettere direttamente un gateway di transito. AWS Network Firewall	16 giugno 2025
Supporto per il riferimento ai gruppi di sicurezza	Ora puoi fare riferimento a un gruppo di sicurezza tramite collegamento VPCs a un gateway di transito.	25 settembre 2024
AWS Quote Transit Gateway	Sono stati aggiunti limiti di larghezza di banda.	14 agosto 2023
AWS Registri di flusso Transit Gateway	I gateway di transito ora supportano i registri di flusso di Transit Gateway, consentendo di monitorare e registrare il	14 luglio 2022

	traffico di rete tra i gateway di transito.	
Tabelle di policy del gateway di transito	Utilizzare le tabelle di policy per impostare il routing dinamico per i gateway di transito per lo scambio automatico di informazioni di instradamento e raggiungibilità con tipi di gateway di transito in peering.	13 luglio 2022
Guida per l'utente di Network Manager	Network Manager è stato creato come guida autonoma e non è più incluso come parte della Guida per l'utente di AWS Transit Gateway.	2 dicembre 2021
Peering di allegati	È possibile creare una connessione di peering con un gateway di transito nella stessa regione.	1 dicembre 2021
Transit Gateway Connect	Puoi stabilire una connessio ne tra un gateway di transito e appliance virtuali di terzi in esecuzione in un VPC.	10 dicembre 2020
Modalità Appliance	È possibile attivare la modalità appliance su un allegato VPC per garantire che il traffico bidirezionale scorra attraverso la stessa zona di disponibilità per l'allegato.	29 ottobre 2020

Riferimenti elenco dei prefissi	È possibile fare riferimento a un elenco di prefissi nella tabella di instradamento del gateway di transito.	24 agosto 2020
Modifica gateway di transito	È possibile modificare le opzioni di configurazione per il gateway di transito.	24 agosto 2020
CloudWatch metriche per gli allegati del gateway di transito	È possibile visualizzare le CloudWatch metriche per i singoli allegati del gateway di transito.	6 luglio 2020
Network Manager Route Analyzer	È possibile analizzare le route nelle tabelle di routing del gateway di transito nella rete globale.	4 maggio 2020
Peering di allegati	È possibile creare una connessione di peering con un gateway di transito in un'altra regione.	3 dicembre 2019
Supporto multicast	Transit Gateway supporta il routing del traffico multicast tra le sottoreti di dispositivi collegati VPCs e funge da router multicast per le istanze che inviano traffico destinato a più istanze di ricezione.	3 dicembre 2019
AWS Network Manager	È possibile visualizzare e monitorare le reti globali costruite attorno ai gateway di transito.	3 dicembre 2019

AWS Direct Connect supporto	È possibile utilizzare un Direct Connect gateway per connettere la Direct Connect connessione tramite un'interfaccia virtuale di transito al gateway di transito VPCs o VPNs collegata allo stesso.	27 marzo 2019
Versione iniziale	Questa versione introduce i gateway di transito.	26 novembre 2018

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.