



AWS 트랜짓 게이트웨이

Amazon VPC



Amazon VPC: AWS 트랜짓 게이트웨이

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon의 상표 및 브랜드 디자인은 Amazon 외 제품 또는 서비스와 함께, Amazon 브랜드 이미지를 떨어뜨리거나 고객에게 혼동을 일으킬 수 있는 방식으로 사용할 수 없습니다. Amazon이 소유하지 않은 기타 모든 상표는 Amazon 계열사, 관련 업체 또는 Amazon의 지원 업체 여부에 상관없이 해당 소유자의 자산입니다.

Table of Contents

Transit Gateway란 무엇입니까?	1
Transit Gateway 개념	1
Transit Gateway를 시작하는 방법	2
Transit Gateway로 작업	2
요금	2
Transit Gateway 작동 원리	3
아키텍처 다이어그램	3
리소스 연결	4
Equal Cost Multipath 라우팅	5
가용 영역	6
라우팅	7
라우팅 테이블	7
라우팅 테이블 연결	7
경로 전파	8
피어링 연결에 대한 라우팅	8
경로 평가 순서	8
시작하기	11
사전 조건	11
1단계: Transit Gateway 생성	11
2단계: VPC를 Transit Gateway에 연결	12
3단계: Transit Gateway와 VPC 사이에 경로 추가	13
4단계: Transit Gateway 테스트	13
5단계: Transit Gateway 삭제	14
설계 모범 사례	15
사용 사례 예시	16
중앙 집중식 라우터	16
개요	16
리소스	17
라우팅	17
격리된 VPC	19
개요	19
리소스	20
라우팅	20
공유 서비스를 사용하는 격리된 VPC	22

개요	22
리소스	23
라우팅	24
피어링	25
개요	25
리소스	26
라우팅	27
중앙 집중식 아웃바운드 라우팅	28
개요	28
리소스	29
라우팅	30
어플라이언스 VPC	32
개요	33
상태 저장 어플라이언스 및 어플라이언스 모드	35
라우팅	36
Transit Gateway로 작업	39
Transit Gateway	39
Transit Gateway 생성	40
Transit Gateway 보기	42
Transit Gateway에 대한 태그 추가 또는 편집	42
Transit Gateway 수정	43
Transit Gateway 공유	43
리소스 공유 수락	44
공유 연결 수락	44
Transit Gateway 삭제	45
VPC 연결	45
VPC 연결 수명 주기	47
VPC에 대한 Transit Gateway Attachment 생성	49
VPC 연결 수정	50
VPC 연결 태그 수정	51
VPC 연결 보기	51
VPC 연결 삭제	51
VPC 연결 문제 해결	52
VPN 연결	53
VPN에 대한 Transit Gateway Attachment 생성	53
VPN 연결 보기	54

Direct Connect 게이트웨이에 연결	54
피어링 연결	55
피어링 연결 생성	56
피어링 연결 요청 수락 또는 거부	57
Transit Gateway 라우팅 테이블에 경로 추가	58
Transit Gateway 피어링 연결 보기	58
피어링 연결 삭제	59
옵트인 AWS 리전 고려 사항	59
Connect 연결 및 Connect 피어	60
Connect 피어	61
요구 사항 및 고려 사항	64
Connect 연결을 생성합니다	65
Connect 피어(GRE 터널) 생성	65
Connect 연결 및 Connect 피어 보기	66
Connect 연결 및 Connect 피어 태그 수정	67
Connect 피어 삭제	68
Connect 연결을 삭제합니다	68
Transit Gateway 라우팅 테이블	68
Transit Gateway 라우팅 테이블 생성	69
Transit Gateway 라우팅 테이블 보기	69
Transit Gateway 라우팅 테이블 연결	70
Transit Gateway 라우팅 테이블에 대한 연결 삭제	70
Transit Gateway 라우팅 테이블에 라우팅 전파	71
경로 전파 비활성화	71
정적 경로 생성	72
정적 경로 삭제	73
정적 경로 바꾸기	73
Amazon S3에 라우팅 테이블 내보내기	74
Transit Gateway 라우팅 테이블 삭제	75
접두사 목록 참조	75
Transit Gateway 정책 테이블	78
Transit Gateway 정책 테이블 생성	79
전송 게이트웨이 정책 테이블 삭제	79
Transit Gateway의 멀티캐스트	80
멀티캐스트 개념	1
고려 사항	80

Windows Server의 멀티캐스트	82
멀티캐스트 라우팅	83
멀티캐스트 작업	84
Transit Gateway 공유	103
Transit Gateway 공유 해제	104
공유 서브넷	104
전송 게이트웨이 흐름 로그	105
제한 사항	106
전송 게이트웨이 흐름 로그 레코드	106
기본 형식	106
사용자 지정 형식	106
사용 가능한 필드	107
Transit Gateway 흐름 로그 요금	112
로그에 CloudWatch 게시	112
플로우 로그를 로그에 게시하기 CloudWatch 위한 IAM 역할	113
IAM 사용자가 역할을 전달할 수 있는 권한	115
Logs에 게시하는 흐름 로그를 생성하십시오. CloudWatch	115
로그에서 흐름 로그 기록을 처리합니다. CloudWatch	117
Amazon S3에 게시	118
흐름 로그 파일	119
Amazon S3에 플로우 로그를 게시하는 IAM 보안 주체에 대한 IAM 정책	121
Amazon S3 버킷의 흐름 로그에 대한 권한	121
SSE-KMS를 사용할 경우 필요한 키 정책	123
Amazon S3 로그 파일 권한	124
Amazon S3에 게시하는 흐름 로그 생성	124
Amazon S3에서 흐름 로그 레코드 처리	125
Kinesis Data Firehose에 게시	126
교차 계정 전송에 대한 IAM 역할	126
Firehose에 게시하는 흐름 로그 만들기	130
흐름 로그 작업	132
흐름 로그 사용 제어	132
흐름 로그 생성	133
흐름 로그 보기	133
흐름 로그에 대한 태그 추가 또는 제거	133
흐름 로그 레코드 보기	134
흐름 로그 레코드 검색	135

흐름 로그 삭제	136
API 및 CLI 개요 및 제한	137
전송 게이트웨이 모니터링	139
CloudWatch 지표	140
Transit Gateway 지표	140
전송 게이트웨이의 지표 차원	142
CloudTrail 로그	142
CloudTrail의 전송 게이트웨이 정보	142
Transit Gateway 로그 파일 항목 이해	143
ID 및 액세스 관리	146
Transit Gateway를 관리하는 정책의 예	146
AWS Network Manager를 관리하는 정책 예	148
서비스 연결 역할	148
Transit Gateway	149
AWS 관리형 정책	150
AWSVPCTransitGatewayServiceRolePolicy	151
정책 업데이트	151
네트워크 ACL	151
EC2 인스턴스 및 Transit Gateway 연결에 동일한 서브넷 사용	151
EC2 인스턴스 및 Transit Gateway 연결에 다른 서브넷 사용	152
모범 사례	152
할당량	154
일반	154
라우팅	154
Transit Gateway Attachment	155
대역폭	155
AWS Direct Connect 게이트웨이	157
최대 전송 단위(MTU)	157
멀티캐스트	158
Network Manager	158
추가 할당량 리소스	159
문서 기록	160
.....	clxiii

Transit Gateway란 무엇입니까?

Transit Gateway는 가상 사설 클라우드(VPC)와 온프레미스 네트워크를 상호 연결하는 데 사용할 수 있는 네트워크 전송 허브입니다. 클라우드 인프라가 전 세계적으로 확장됨에 따라 리전 간 피어링은 AWS 글로벌 인프라를 사용하여 Transit Gateway를 함께 연결합니다. AWS 데이터 센터 간의 모든 네트워크 트래픽은 물리 계층에서 자동으로 암호화됩니다.

자세한 내용은 [AWS Transit Gateway](#) 섹션을 참조하세요.

Transit Gateway 개념

다음은 Transit Gateway의 핵심 개념입니다.

- 연결 — 다음을 연결할 수 있습니다.
 - 하나 이상의 VPC
 - Connect SD-WAN/서드 파티 네트워크 어플라이언스
 - AWS Direct Connect 게이트웨이
 - 다른 Transit Gateway와의 피어링 연결
 - Transit Gateway에 대한 VPN 연결
- Transit Gateway MTU(최대 전송 단위) — 네트워크 연결의 MTU(최대 전송 단위)는 연결을 통해 전달할 수 있는 허용되는 최대 크기의 패킷 크기(바이트)입니다. 연결의 MTU가 클수록 하나의 패킷으로 전달할 수 있는 데이터의 양이 늘어납니다. Transit Gateway는 VPC, AWS Direct Connect, Transit Gateway Connect 및 피어링 연결 간의 트래픽에 대해 8,500바이트의 MTU를 지원합니다. VPN 연결을 통한 트래픽은 1,500바이트의 MTU를 가질 수 있습니다.
- Transit Gateway 라우팅 테이블 — Transit Gateway는 기본 라우팅 테이블을 가지며 선택적으로 추가 라우팅 테이블을 가질 수 있습니다. 라우팅 테이블에는 패킷의 대상 IP 주소를 기반으로 다음 홉을 결정하는 동적 및 정적 라우팅이 포함됩니다. 이러한 경로의 대상은 모든 Transit Gateway Attachment일 수 있습니다. 기본적으로 Transit Gateway 연결은 기본 Transit Gateway 라우팅 테이블과 연결됩니다.
- 연결 — 각 연결은 항상 정확히 하나의 라우팅 테이블과 연결됩니다. 라우팅 테이블은 0개 이상의 연결과 연관될 수 있습니다.
- 라우팅 전파 — VPC, VPN 연결 또는 Direct Connect 게이트웨이는 Transit Gateway 라우팅 테이블에 라우팅을 동적으로 전파할 수 있습니다. Connect 연결을 사용하면 라우팅이 기본적으로 Transit Gateway 라우팅 테이블에 전파됩니다. VPC를 사용하는 경우 트래픽을 전송 게이트웨이로 보내려면 정적 라우팅을 생성해야 합니다. VPN 연결을 사용하면 BGP(Border Gateway Protocol)를 사용하

여 전송 게이트웨이에서 온프레미스 라우터로 라우팅이 전파됩니다. Direct Connect 게이트웨이를 사용하면 허용된 접두사는 BGP를 사용하여 온프레미스 라우터로 생성됩니다. 피어링 연결을 사용하는 경우 피어링 연결을 가리키도록 Transit Gateway 라우팅 테이블에서 정적 라우팅을 만들어야 합니다.

Transit Gateway를 시작하는 방법

다음 리소스를 사용하여 Transit Gateway를 생성하고 사용할 수 있습니다.

- [Transit Gateway 작동 원리](#)
- [시작하기](#)
- [설계 모범 사례](#)

Transit Gateway로 작업

다음 인터페이스 중 하나를 사용하여 Transit Gateway를 생성하고, 액세스하고, 관리할 수 있습니다.

- AWS Management Console — Transit Gateway에 액세스할 때 사용할 수 있는 웹 인터페이스를 제공합니다.
- AWS 명령줄 인터페이스(AWS CLI) — Amazon VPC를 비롯한 다양한 AWS 서비스에 명령을 제공하며 Windows, macOS 및 Linux에서 지원됩니다. 자세한 내용은 [AWS Command Line Interface](#) 섹션을 참조하세요.
- AWS SDK — 언어별 API 작업을 제공하고, 서명 계산, 요청 재시도 처리 및 오류 처리와 같은 많은 연결 세부 정보를 관리합니다. 자세한 정보는 [AWS SDK](#)를 참조하세요.
- 쿼리 API — HTTPS 요청을 사용하여 호출하는 하위 수준의 API 작업을 제공합니다. 쿼리 API 사용이 Amazon VPC에 액세스하는 가장 직접적인 방법이지만, 애플리케이션에서 요청에 서명할 해시 생성 및 오류 처리와 같은 하위 수준의 세부 정보를 처리해야 합니다. 자세한 내용은 [Amazon EC2 API 참조](#)를 확인하세요.

요금

Transit Gateway의 각 연결에 대해 시간당 요금이 청구되며, Transit Gateway에서 처리된 트래픽 양에 대한 요금이 청구됩니다. 자세한 내용은 [AWS Transit Gateway 요금](#)을 참조하세요.

Transit Gateway 작동 원리

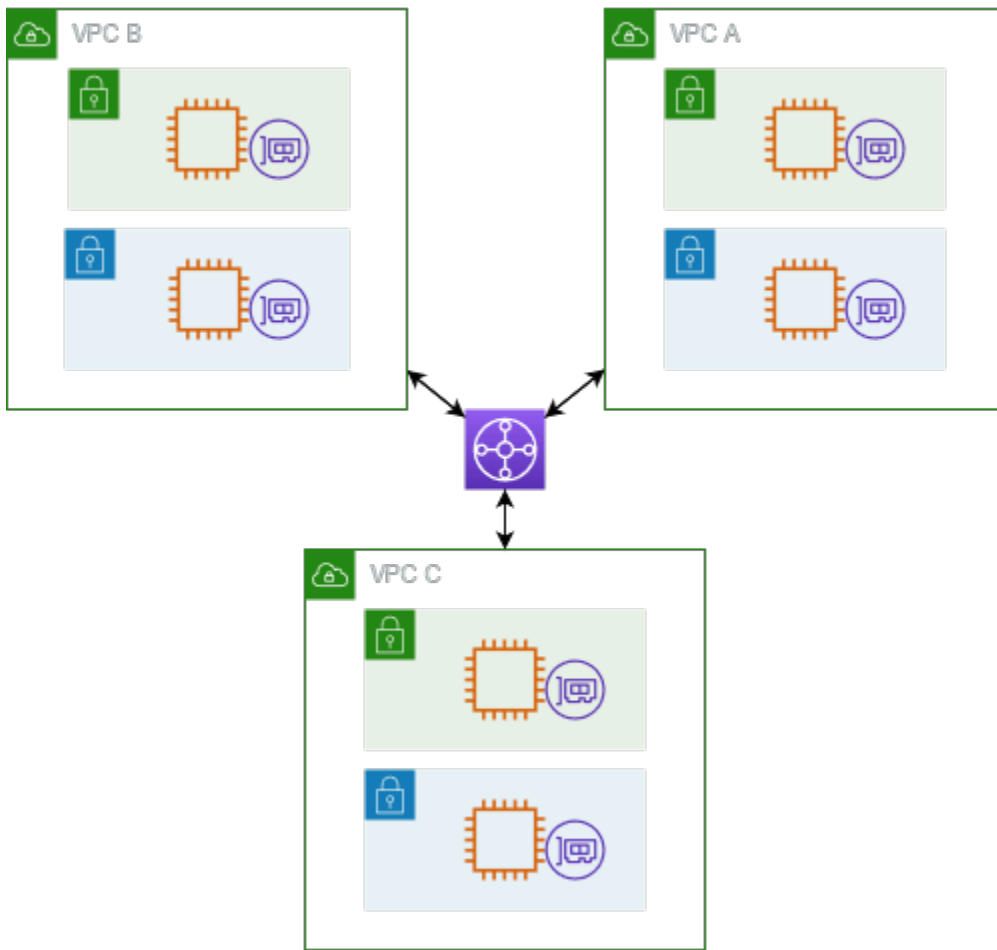
Transit Gateway는 Virtual Private Cloud(VPC)와 온프레미스 네트워크 간의 트래픽에 대한 리전별 가상 라우터 역할을 합니다. Transit Gateway는 네트워크 트래픽의 볼륨에 따라 탄력적으로 조정됩니다. Transit Gateway를 통한 라우팅은 패킷이 대상 IP 주소를 기반으로 특정 다음 홉 연결로 전송되는 계층 3에서 작동합니다.

내용

- [아키텍처 다이어그램](#)
- [리소스 연결](#)
- [Equal Cost Multipath 라우팅](#)
- [가용 영역](#)
- [라우팅](#)

아키텍처 다이어그램

다음 다이어그램에서는 3개의 VPC 연결이 있는 Transit Gateway를 보여 줍니다. 이러한 각 VPC의 라우팅 테이블에는 다른 두 VPC를 대상으로 하는 트래픽을 Transit Gateway로 보내는 로컬 경로가 포함됩니다.



다음은 이전 다이어그램에 표시된 연결에 대한 기본 Transit Gateway 라우팅 테이블의 예입니다. 각 VPC의 CIDR 블록이 라우팅 테이블에 전파됩니다. 따라서 각 연결은 패킷을 다른 두 가지 연결로 경로 지정할 수 있습니다.

대상 주소	대상	경로 유형
VPC A CIDR	VPC A ##	전파
VPC B CIDR	VPC B ##	전파
VPC C CIDR	VPC C ##	전파

리소스 연결

Transit Gateway Attachment는 패킷의 소스이자 대상입니다. 다음 리소스를 Transit Gateway에 연결할 수 있습니다.

- 하나 이상의 VPC AWS Transit Gateway는 VPC 서브넷 내에 Elastic Network 인터페이스를 배포합니다. 그러면 Transit Gateway는 이 인터페이스를 사용하여 선택한 서브넷을 오가는 트래픽을 라우팅합니다. 각 가용 영역에 하나 이상의 서브넷이 있어야 합니다. 그러면 트래픽이 해당 영역의 모든 서브넷에 있는 리소스에 도달할 수 있습니다. 연결을 생성하는 동안 특정 가용 영역 내의 리소스는 동일한 영역 내에 서브넷이 활성화된 경우에만 Transit Gateway에 도달할 수 있습니다. 서브넷 라우팅 테이블은 Transit Gateway에 대한 경로를 포함합니다. 트래픽은 동일한 가용 영역의 서브넷에 연결이 있는 경우에만 Transit Gateway에 전달됩니다.
- 하나 이상의 VPN 연결
- 하나 이상의 게이트웨이 AWS Direct Connect
- 하나 이상의 Transit Gateway Connect 연결
- 하나 이상의 Transit Gateway 피어링 연결
- Transit Gateway Attachment 하나가 패킷의 소스이자 대상일 수 있습니다

Equal Cost Multipath 라우팅

AWS Transit Gateway는 대부분의 첨부 파일에 대해 균등 비용 멀티패스 (ECMP) 라우팅을 지원합니다. VPN 연결의 경우, Transit Gateway를 생성하거나 수정할 때 콘솔을 사용해 ECMP 지원을 활성화하거나 비활성화할 수 있습니다. 다른 모든 연결 유형의 경우, 다음과 같은 ECMP 제한 사항이 적용됩니다.

- VPC - VPC는 CIDR 블록이 중첩될 수 없기 때문에 ECMP를 지원하지 않습니다. 예를 들어, CIDR 10.1.0.0/16을 포함한 VPC를 Transit Gateway에 대하여 같은 CIDR을 사용하는 두 번째 VPC와 연결하여 둘 사이의 트래픽을 로드 밸런싱할 라우팅을 설정할 수는 없습니다.
- VPN - VPN ECMP support(VPN ECMP 지원) 옵션이 비활성화된 경우, Transit Gateway는 여러 경로에 걸쳐 같은 접두사가 발생하는 경우 내부 지표를 사용해 기본 설정 경로를 판단합니다. VPN 연결에 대한 ECMP 활성화 또는 비활성화에 대한 자세한 내용은 [the section called “Transit Gateway”](#)를 참조하세요.
- AWS Transit Gateway 연결 - AWS Transit Gateway 연결 첨부 파일은 자동으로 ECMP를 지원합니다.
- AWS Direct Connect 게이트웨이 - AWS Direct Connect 게이트웨이 첨부 파일은 네트워크 접두사, 접두사 길이 및 AS_PATH가 정확히 동일한 경우 여러 Direct Connect Gateway 연결에서 ECMP를 자동으로 지원합니다.
- Transit Gateway 피어링 - Transit Gateway 피어링은 동적 라우팅을 지원하지도 않고, 서로 다른 두 대상에 대하여 같은 정적 경로를 구성할 수도 없기 때문에 ECMP를 지원하지 않습니다.

Note

- BGP Multipath AS-Path Relax가 지원되지 않으므로 Autonomous System Number(ASN)가 서로 다른 경우 ECMP를 사용할 수 없습니다.
- 서로 다른 연결 유형 간에는 ECMP가 지원되지 않습니다. 예를 들어 VPN과 VPC 연결 사이에서 ECMP를 활성화할 수는 없습니다. 대신, Transit Gateway 경로가 평가되며 트래픽은 그에 따라 평가된 경로로 라우팅됩니다. 자세한 정보는 [the section called “경로 평가 순서”](#)을 참조하세요.
- 단일 Direct Connect 게이트웨이는 여러 전송 가상 인터페이스에서 ECMP를 지원합니다. 따라서 Direct Connect 게이트웨이는 하나만 설정하여 사용하는 것이 좋습니다. ECMP를 유리하게 활용하기 위해 게이트웨이를 여러 개 설정하여 사용하지 마세요. Direct Connect 게이트웨이 및 퍼블릭 가상 인터페이스에 대한 자세한 내용은 퍼블릭 가상 인터페이스에서 [액티브/액티브 또는 액티브/패시브 Direct Connect 연결을 설정하려면 어떻게 해야 합니까?](#) 를 참조하십시오. AWS .

가용 영역

Transit Gateway에 VPC를 연결할 때는 Transit Gateway에서 하나 이상의 가용 영역을 사용하여 트래픽을 VPC 서브넷의 리소스로 라우팅해야 합니다. 각 가용 영역을 활성화하려면 정확히 하나의 서브넷을 지정해야 합니다. Transit Gateway는 서브넷의 IP 주소 하나를 사용하여 해당 서브넷에 네트워크 인터페이스를 배치합니다. 가용 영역을 활성화하면 지정된 서브넷이나 가용 영역이 아닌 VPC의 모든 서브넷으로 트래픽을 라우팅할 수 있습니다. 그러나 Transit Gateway Attachment가 있는 가용 영역에 상주하는 리소스만 Transit Gateway에 도달할 수 있습니다.

대상 첨부 파일이 없는 가용 영역에서 트래픽이 유입되는 경우 AWS Transit Gateway는 해당 트래픽을 연결 파일이 있는 임의의 가용 영역으로 내부적으로 라우팅합니다. 이러한 유형의 가용 영역 간 트래픽에는 추가 전송 게이트웨이 요금이 부과되지 않습니다.

가용성을 위해 여러 개의 가용 영역을 활성화하는 것이 좋습니다.

어플라이언스 모드 지원 사용

VPC에서 상태 저장 네트워크 어플라이언스를 구성하려는 경우 어플라이언스가 위치한 해당 VPC 연결에 대해 어플라이언스 모드 지원을 활성화할 수 있습니다. 이렇게 하면 Transit Gateway가 소스와 대상 간의 트래픽 흐름이 끝날 때까지 해당 VPC 연결에 동일한 가용 영역을 사용할 수 있습니다. 또한 해당 영역에 서브넷 연결이 있는 경우 Transit Gateway는 VPC의 모든 가용 영역으로 트래픽을 전송할 수 있습니다. 자세한 정보는 [예: 공유 서비스 VPC의 어플라이언스](#)을 참조하세요.

라우팅

Transit Gateway는 Transit Gateway 라우팅 테이블을 사용하여 연결 간에 IPv4 및 IPv6 패킷을 라우팅합니다. 연결된 VPC, VPN 연결 및 Direct Connect 게이트웨이에 대한 라우팅 테이블의 경로를 전파하도록 이러한 라우팅 테이블을 구성할 수 있습니다. Transit Gateway 라우팅 테이블에 정적 경로를 추가할 수도 있습니다. 패킷이 한 연결에서 오는 경우 이 패킷은 대상 IP 주소와 일치하는 경로를 사용하여 다른 연결로 라우팅됩니다.

Transit Gateway 피어링 연결의 경우 정적 경로만 지원됩니다.

내용

- [라우팅 테이블](#)
- [라우팅 테이블 연결](#)
- [경로 전파](#)
- [피어링 연결에 대한 라우팅](#)
- [경로 평가 순서](#)

라우팅 테이블

Transit Gateway는 자동으로 기본 라우팅 테이블과 함께 제공됩니다. 기본적으로 이 라우팅 테이블은 기본 연결 라우팅 테이블과 기본 전파 라우팅 테이블입니다. 경로 전파 및 라우팅 테이블 연결을 비활성화한 경우 AWS는 Transit Gateway에 대한 기본 라우팅 테이블을 생성하지 않습니다.

Transit Gateway에 사용할 추가 라우팅 테이블을 만들 수 있습니다. 이렇게 하면 연결의 서브넷을 격리할 수 있습니다. 각 연결은 라우팅 테이블 하나와 연결할 수 있습니다. 한 연결은 하나 이상의 라우팅 테이블에 해당 경로를 전파할 수 있습니다.

Transit Gateway 라우팅 테이블에 경로와 일치하는 트래픽을 삭제하는 블랙홀 경로를 만들 수 있습니다.

Transit Gateway에 VPC를 연결할 때 트래픽이 Transit Gateway를 통해 라우팅되도록 경로를 서브넷 라우팅 테이블에 추가해야 합니다. 자세한 내용은 Amazon VPC 사용 설명서의 [Transit Gateway에 대한 라우팅](#)을 참조하세요.

라우팅 테이블 연결

Transit Gateway Attachment를 단일 라우팅 테이블과 연결할 수 있습니다. 각 라우팅 테이블은 0개 이상의 연결과 연결할 수 있으며 패킷을 다른 연결에 전달할 수 있습니다.

경로 전파

각 연결에는 하나 이상의 Transit Gateway 라우팅 테이블에 설치할 수 있는 경로가 있습니다. 연결이 Transit Gateway 라우팅 테이블에 전파되면 이러한 경로가 라우팅 테이블에 설치됩니다. 알려진 경로는 필터링할 수 없습니다.

VPC 연결의 경우 VPC의 CIDR 블록이 Transit Gateway 라우팅 테이블로 전파됩니다.

VPN 연결이나 Direct Connect 게이트웨이 연결과 함께 동적 라우팅이 사용되는 경우 BGP를 통해 온 프레미스 라우터에서 학습한 경로를 Transit Gateway 라우팅 테이블로 전파할 수 있습니다.

VPN 연결과 함께 동적 라우팅을 사용하는 경우 VPN 연결과 연결된 라우팅 테이블의 경로가 BGP를 통해 고객 게이트웨이에 전달됩니다.

Connect 연결 파일의 경우 Connect 연결 파일과 연결된 라우팅 테이블의 경로가 BGP를 통해 VPC에서 실행되는 SD-WAN 어플라이언스와 같은 서드 파티 가상 어플라이언스에 전달됩니다.

Direct Connect 게이트웨이 연결의 경우 [허용된 접두사 상호 작용에](#) 따라 고객 네트워크에 알려지는 경로가 결정됩니다. AWS

정적 경로와 전파 경로의 대상이 동일한 경우 정적 경로의 우선순위가 높으므로 전파 경로는 라우팅 테이블에 포함되지 않습니다. 정적 경로를 제거하면 중복 전파 경로가 라우팅 테이블에 포함됩니다.

피어링 연결에 대한 라우팅

두 개의 Transit Gateway를 피어링하고 두 게이트웨이 간에 트래픽을 라우팅할 수 있습니다. 이렇게 하려면 Transit Gateway에서 피어링 연결을 생성하고 함께 피어링 연결을 생성할 피어 Transit Gateway를 지정해야 합니다. 그런 다음 Transit Gateway 라우팅 테이블에서 정적 경로를 생성하여 트래픽을 Transit Gateway 피어링 연결로 라우팅합니다. 피어 Transit Gateway로 라우팅된 트래픽은 피어 Transit Gateway에 대한 VPC 및 VPN 연결로 라우팅될 수 있습니다.

자세한 내용은 [예: 피어링된 Transit Gateway](#) 단원을 참조하세요.

경로 평가 순서

Transit Gateway 경로는 다음과 같은 순서로 평가됩니다.

- 대상 주소의 가장 구체적인 경로입니다.
- CIDR은 같지만 연결 유형이 다른 경로의 경우 경로 우선 순위는 다음과 같습니다.

- 정적 경로(예: Site-to-Site VPN 정적 경로)
- 참조된 경로 접두사 목록
- VPC 전파 경로
- Direct Connect 게이트웨이 전파 경로
- Transit Gateway Connect 전파 경로
- Site-to-Site VPN 전파 경로
- Transit Gateway 피어링 전파 경로(클라우드 WAN)

일부 첨부 파일은 BGP를 통한 경로 광고를 지원합니다. CIDR이 동일하고 첨부 파일 유형이 동일한 경로의 경우 경로 우선 순위는 BGP 속성에 의해 제어됩니다.

- 더 짧은 AS 경로 길이
- 낮은 MED 값
- 첨부 파일이 지원하는 경우 iBGP 경로보다 eBGP 경로가 선호됩니다.

Important

AWS 위에 나열된 것과 동일한 CIDR, 첨부 파일 유형 및 BGP 속성을 가진 BGP 경로에 대해 일관된 경로 우선 순위 지정 순서를 보장할 수 없습니다.

AWS Transit Gateway에는 선호 경로만 표시됩니다. 백업 경로는 해당 경로가 더 이상 광고되지 않는 경우 (예: Direct Connect 게이트웨이와 Site-to-Site VPN을 통해 동일한 경로를 광고하는 경우)에만 Transit Gateway 라우팅 테이블에 표시됩니다. AWS Transit Gateway에는 기본 경로인 Direct Connect 게이트웨이 경로에서 수신한 경로만 표시됩니다. 백업 경로인 Site-to-Site VPN은 Direct Connect 게이트웨이가 더 이상 광고되지 않는 경우에만 표시됩니다.

VPC 및 트랜짓 게이트웨이 라우팅 테이블 차이

라우팅 테이블 평가는 VPC 라우팅 테이블을 사용하는지 아니면 트랜짓 게이트웨이 라우팅 테이블을 사용하는지에 따라 다릅니다.

다음 예제는 VPC 라우팅 테이블을 보여줍니다. VPC 로컬 경로는 우선순위가 가장 높으며, 그 다음은 가장 구체적인 경로입니다. 정적 경로와 전파 경로의 대상이 같은 경우, 정적 경로 우선순위가 더 높습니다.

대상 주소	대상	우선순위
10.0.0.0/16	로컬	1
192.168.0.0/16	pcx-12345	2
172.31.0.0/16	vgw-12345(정적) 또는 tgw-12345(정적)	2
172.31.0.0/16	vgw-12345(전파)	3
0.0.0.0/0	igw-12345	4

다음 예는 트랜짓 게이트웨이 라우팅 테이블을 보여줍니다. VPN 연결보다 AWS Direct Connect 게이트웨이 연결을 사용하고 싶은 경우, BGP VPN 연결을 사용하고 Transit Gateway 라우팅 테이블의 경로를 전파합니다.

대상 주소	연결(대상)	리소스 유형	경로 유형	우선순위
10.0.0.0/16	tgw-attach-123 vpc-1234	VPC	정적 또는 전파	1
192.168.0.0/16	tgw-attach-789 vpn-5678	VPN	정적	2
172.31.0.0/16	tgw-attach-456 dxgw_id	AWS Direct Connect 게이트 웨이	전파 완료	3
172.31.0.0/16	tgw-attach-789 -123 tgw-conne ct-peer	연결	전파	4
172.31.0.0/16	tgw-attach-789 vpn-5678	VPN	전파 완료	5

Transit Gateway 시작하기

다음 작업은 Transit Gateway에 익숙해지는 데 도움이 됩니다. Transit Gateway를 생성한 다음 Transit Gateway를 사용하여 VPC 두 개를 연결합니다.

작업

- [사전 조건](#)
- [1단계: Transit Gateway 생성](#)
- [2단계: VPC를 Transit Gateway에 연결](#)
- [3단계: Transit Gateway와 VPC 사이에 경로 추가](#)
- [4단계: Transit Gateway 테스트](#)
- [5단계: Transit Gateway 삭제](#)

사전 조건

- Transit Gateway를 사용하는 간단한 예를 보여주기 위해 동일한 리전에 두 개의 VPC를 만듭니다. VPC는 중복 CIDR을 가질 수 없습니다. 각 VPC에서 하나의 Amazon EC2 인스턴스를 시작합니다. 자세한 내용은 Amazon VPC 사용 설명서의 [Amazon VPC 시작하기](#)를 참조하세요.
- 동일한 라우팅에서 두 개의 서로 다른 VPC를 가리킬 수 없습니다. Transit Gateway 라우팅 테이블에 동일한 라우팅이 있는 경우 Transit Gateway는 새로 연결된 VPC의 CIDR을 전파하지 않습니다.
- Transit Gateway로 작업하는 데 필요한 권한이 있는지 확인합니다. 자세한 내용은 [전송 게이트웨이의 Identity and Access Management](#) 섹션을 참조하세요.
- 각 호스트 보안 그룹에 ICMP 규칙을 추가하지 않은 경우에는 호스트 간에 ping을 수행할 수 없습니다. 자세한 내용은 Amazon VPC 사용 설명서의 [보안 그룹 작업](#)을 참조하세요.

1단계: Transit Gateway 생성

Transit Gateway를 생성할 때 기본 Transit Gateway 라우팅 테이블을 만들어 기본 연결 라우팅 테이블과 기본 전파 라우팅 테이블로 사용합니다.

Transit Gateway를 생성하려면

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 리전 선택기에서 VPC를 만들 때 사용한 리전을 선택합니다.

3. 탐색 창에서 Transit Gateway를 선택합니다.
4. Transit Gateway 생성(Create Transit Gateway)을 선택합니다.
5. (선택 사항) 이름 태그에 Transit Gateway의 이름을 입력합니다. 그러면 '이름'이 키로 지정되고 이름이 값으로 지정된 태그가 생성됩니다.
6. (선택 사항) 설명에 Transit Gateway에 대한 설명을 입력합니다.
7. Amazon 측 자율 시스템 번호(ASN)(Amazon side Autonomous System Number (ASN))에 Transit Gateway의 프라이빗 ASN를 입력합니다. 이 번호는 경계 게이트웨이 프로토콜(BGP) 세션의 AWS 측에 대한 ASN이어야 합니다.

16비트 ASN의 경우 범위는 64512~65534입니다.

32비트 ASN의 경우 범위는 4200000000~4294967294입니다.

다중 리전 배포가 있는 경우 각 Transit Gateway에 고유한 ASN을 사용하는 것이 좋습니다.

8. (선택 사항) DNS 지원을 비활성화해야 하거나 기본 연결 라우팅 테이블이나 기본 전파 라우팅 테이블을 원하지 않는 경우 기본 설정을 수정할 수 있습니다.
9. Transit Gateway 생성(Create Transit Gateway)을 선택합니다. 게이트웨이가 생성되면 Transit Gateway의 초기 상태는 pending입니다.

2단계: VPC를 Transit Gateway에 연결

연결을 생성하기 전에 이전 섹션에서 생성한 Transit Gateway가 사용 가능하다고 표시될 때까지 기다립니다. 각 VPC에 대한 연결을 생성합니다.

에서 설명하는 것처럼 VPC 두 개를 만들고 각 VPC에서 EC2 인스턴스를 시작했는지 확인합니다 [사전 조건](#)

VPC에 대한 Transit Gateway Attachment 생성

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway Attachments를 선택합니다.
3. Transit Gateway Attachment 생성(Create Transit Gateway attachment)을 선택합니다.
4. (선택 사항) 이름 태그(Name tag)에 연결 이름을 입력합니다.
5. Transit Gateway ID에서 연결에 사용할 Transit Gateway를 선택합니다.
6. 연결 유형(Attachment type)에서 VPC를 선택합니다.

7. DNS 지원을 활성화할지 선택합니다. 이 연습에서는 IPv6 지원을 활성화하지 마세요.
8. VPC ID에서 Transit Gateway에 연결할 VPC를 선택합니다.
9. 서브넷 ID에서 트래픽을 라우팅하기 위해 Transit Gateway에서 사용할 각 가용 영역에 대해 하나의 서브넷을 선택합니다. 하나 이상의 서브넷을 선택해야 합니다. 가용 영역당 서브넷 한 개만 선택할 수 있습니다.
10. Transit Gateway Attachment 생성(Create Transit Gateway attachment)을 선택합니다.

각 연결은 항상 정확히 하나의 라우팅 테이블과 연결됩니다. 라우팅 테이블은 0개 이상의 연결과 연관될 수 있습니다. 구성할 라우팅을 결정하려면 Transit Gateway의 사용 사례를 결정한 다음 라우팅을 구성합니다. 자세한 내용은 [사용 사례 예시](#) 단원을 참조하세요.

3단계: Transit Gateway와 VPC 사이에 경로 추가

라우팅 테이블에는 패킷의 대상 IP 주소를 기반으로 연결된 VPC의 다음 홉을 결정하는 동적 및 정적 경로가 포함되어 있습니다. 로컬이 아닌 경로에 대한 대상과 Transit Gateway Attachment ID의 대상이 있는 경로를 구성합니다. 자세한 내용은 Amazon VPC 사용 설명서의 [Transit Gateway에 대한 라우팅](#)을 참조하세요.

VPC 라우팅 테이블에 경로 추가

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 라우팅 테이블을 선택합니다.
3. VPC와 연결된 라우팅 테이블을 선택합니다.
4. 경로(Routes) 탭에서 경로 편집(Edit routes)을 선택합니다.
5. 경로 추가(Add route)를 선택합니다.
6. 대상(Destination) 열에 대상 IP 주소 범위를 입력합니다. 대상(Target)의 경우, 전송 게이트웨이(Transit Gateway)를 선택한 다음 전송 게이트웨이 ID를 선택합니다.
7. Save changes(변경 사항 저장)를 선택합니다.

4단계: Transit Gateway 테스트

각 VPC의 Amazon EC2 인스턴스에 연결한 다음 ping 명령 등을 통해 데이터를 전송하면 Transit Gateway가 성공적으로 생성되었는지 확인할 수 있습니다. 자세한 내용은 [Linux 인스턴스에 연결](#) 또는 [Windows 인스턴스 연결](#)을 참조하세요.

5단계: Transit Gateway 삭제

Transit Gateway가 필요하지 않다면 삭제해도 됩니다.

리소스 첨부 파일이 있는 Transit Gateway는 삭제할 수 없습니다. 연결이 있는 전송 게이트웨이를 삭제하려고 시도할 경우 먼저 연결을 삭제한 다음 전송 게이트웨이를 삭제하라는 메시지가 나옵니다. Transit Gateway가 삭제되면 그 즉시 요금 청구가 중지됩니다.

Transit Gateway를 삭제하려면

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway를 선택합니다.
3. 전송 게이트웨이를 선택한 다음, 작업(Actions), 전송 게이트웨이 삭제>Delete transit gateway)를 선택합니다.
4. **delete**를 입력한 다음 삭제>Delete)를 선택합니다.

Transit gateways 페이지에 있는 전송 게이트웨이의 상태(State)는 Deleting입니다. 전송 게이트웨이가 삭제되면 페이지에서 제거됩니다.

Transit Gateway 설계 모범 사례

다음은 Transit Gateway 설계에 대한 모범 사례입니다.

- 각 Transit Gateway VPC 첨부 파일에 대해 별도의 서브넷을 사용합니다. 서브넷별로 작은 CIDR(예: /28)을 사용하여 EC2 리소스를 위한 주소를 더 많이 확보하세요. 별도의 서브넷을 사용하는 경우 다음을 구성할 수 있습니다.
 - Transit Gateway 서브넷과 연결된 인바운드 및 아웃바운드 네트워크 ACL을 계속 열어 둡니다.
 - 트래픽 흐름에 따라 네트워크 ACL을 워크로드 서브넷에 적용할 수 있습니다.
- 네트워크 ACL 하나를 만들어 Transit Gateway에 연결된 모든 서브넷과 연결합니다. 인바운드 및 아웃바운드 방향 모두에서 네트워크 ACL을 열어 둡니다.
- 네트워크 설계에 여러 VPC 라우팅 테이블(예: 여러 NAT 게이트웨이를 통해 트래픽을 라우팅하는 중간 상자 VPC)이 필요한 경우를 제외하고 동일한 VPC 라우팅 테이블을 Transit Gateway에 연결된 모든 서브넷과 연결합니다.
- BGP(Border Gateway Protocol) Site-to-Site VPN 연결을 사용합니다. 연결을 위한 고객 게이트웨이 디바이스 또는 방화벽이 다중 경로를 지원하는 경우 이 기능을 활성화합니다.
- AWS Direct Connect 게이트웨이 연결 및 BGP Site-to-Site VPN 연결에 대한 경로 전파를 활성화합니다.
- VPC 피어링에서 마이그레이션하여 트랜짓 게이트웨이를 사용하는 경우 VPC 피어링과 Transit Gateway 간에 MTU 크기가 일치하지 않으면 비대칭 트래픽에 대해 일부 패킷이 삭제될 수 있습니다. 크기 불일치로 인해 점보 패킷이 삭제되지 않도록 두 VPC를 동시에 업데이트합니다.
- Transit Gateway는 기본적으로고가용성이므로고가용성을 위해 추가 Transit Gateway가 필요하지는 않습니다.
- 설계상 여러 Transit Gateway 라우팅 테이블이 필요할 때를 제외하면 Transit Gateway 라우팅 테이블 수를 제한해야 합니다.
- 중복성을 위해 재해 복구를 위한 각 리전에 단일 전송 게이트웨이를 사용합니다.
- Transit Gateway 여러 개가 있는 배포의 경우 각 Transit Gateway에 대해 고유한 자율 시스템 번호(ASN)를 사용하는 것이 좋습니다. 리전 내 피어링도 사용할 수 있습니다. 자세한 내용은 지역 간 피어링을 [사용한 AWS Transit Gateway 글로벌 네트워크 구축을](#) 참조하십시오.

다음은 전송 게이트웨이의 일반적인 사용 사례입니다

다음은 전송 게이트웨이의 일반적인 사용 사례입니다. 전송 게이트웨이는 이러한 사용 사례에만 국한되지 않습니다.

예시

- [예: 중앙 집중식 라우터](#)
- [예: 격리된 VPC](#)
- [예: 공유 서비스를 사용하는 격리된 VPC](#)
- [예: 피어링된 Transit Gateway](#)
- [예: 인터넷으로의 중앙 집중식 아웃바운드 라우팅](#)
- [예: 공유 서비스 VPC의 어플라이언스](#)

예: 중앙 집중식 라우터

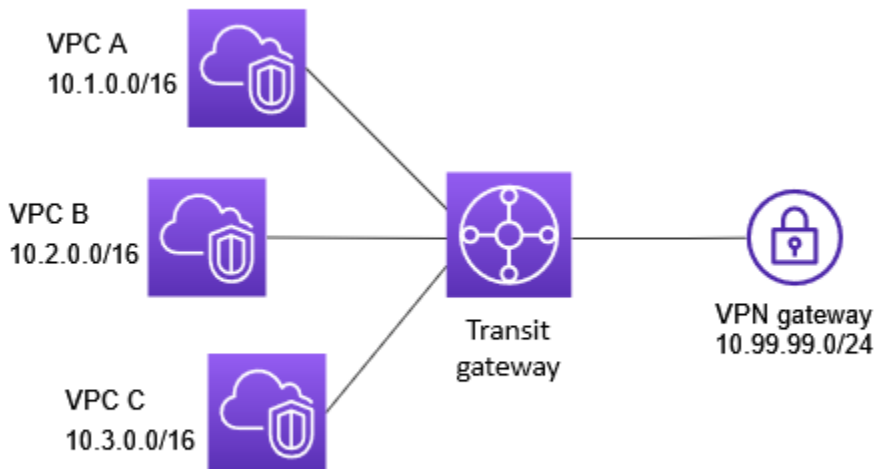
Transit Gateway를 모든 VPC, AWS Direct Connect 및 Site-to-Site VPN 연결을 연결하는 중앙 집중식 라우터로 구성할 수 있습니다. 이 시나리오에서는 모든 연결이 Transit Gateway 기본 라우팅 테이블과 연결되어 Transit Gateway 기본 라우팅 테이블에 전파됩니다. 따라서 모든 연결은 패킷을 서로 라우팅할 수 있으며 Transit Gateway는 단순한 계층 3 IP 라우터 역할을 합니다.

내용

- [개요](#)
- [리소스](#)
- [라우팅](#)

개요

다음 다이어그램은 이 시나리오를 위한 구성의 주요 구성 요소를 보여줍니다. 이 시나리오에서는 Transit Gateway에 대한 VPC 연결 3개와 Site-to-Site VPN 연결 1개가 있습니다. 다른 VPC의 서브넷 또는 VPN 연결로 향하는 VPC A, VPC B 및 VPC C에 있는 서브넷의 패킷은 먼저 Transit Gateway를 통해 라우팅됩니다.



리소스

이 시나리오에서는 다음 리소스를 생성합니다.

- VPC 3개. VPC 만들기에 대한 자세한 내용은 Amazon VPC 사용 설명서의 [VPC 만들기](#)를 참조하세요.
- 전송 게이트웨이. 자세한 내용은 [the section called “Transit Gateway 생성”](#) 섹션을 참조하세요.
- Transit Gateway의 VPC 연결 3개. 자세한 내용은 [the section called “VPC에 대한 Transit Gateway Attachment 생성”](#) 섹션을 참조하세요.
- Transit Gateway의 Site-to-Site VPN 연결. 각 VPC의 CIDR 블록이 전송 게이트웨이 라우팅 테이블에 전파됩니다. VPN 연결이 가동되면 BGP 세션이 설정되고 Site-to-Site VPN CIDR이 Transit Gateway 라우팅 테이블로 전파되며 VPC CIDR이 고객 게이트웨이 BGP 테이블에 추가됩니다. 자세한 내용은 [the section called “VPN에 대한 Transit Gateway Attachment 생성”](#) 섹션을 참조하세요.

AWS Site-to-Site VPN 사용 설명서의 [고객 게이트웨이 디바이스 요구 사항](#)을 검토해야 합니다.

라우팅

각 VPC에는 라우팅 테이블이 있고 Transit Gateway용 라우팅 테이블도 있습니다.

VPC 라우팅 테이블

각 VPC에는 항목 2개가 포함된 라우팅 테이블이 있습니다. 첫 번째 항목은 VPC의 로컬 IPv4 라우팅에 대한 기본 항목으로서, 이 VPC의 인스턴스가 서로 통신할 수 있게 해줍니다. 두 번째 항목은 기타 IPv4 서브넷 트래픽을 모두 Transit Gateway로 라우팅합니다. 다음 표에 VPC A 경로가 나와 있습니다.

대상 주소	대상
10.1.0.0/16	로컬
0.0.0.0/0	tgw-id

Transit Gateway 라우팅 테이블

다음은 라우팅 전파가 활성화된 이전 다이어그램의 연결에 대한 기본 라우팅 테이블의 예입니다.

대상 주소	대상	경로 유형
10.1.0.0/16	VPC A ##	전파
10.2.0.0/16	VPC B ##	전파
10.3.0.0/16	VPC C ##	전파
10.99.99.0/24	VPN ### ## ##	전파

고객 게이트웨이 BGP 테이블

고객 게이트웨이 BGP 테이블에는 다음과 같은 VPC CIDR이 포함되어 있습니다.

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

예: 격리된 VPC

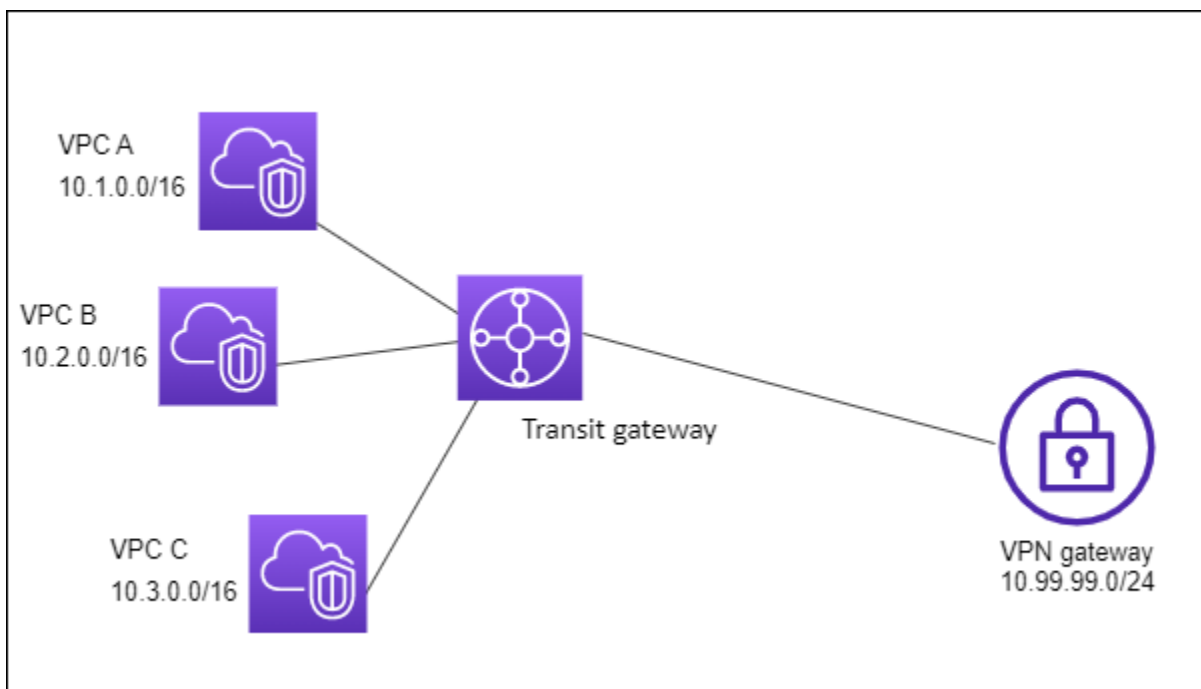
Transit Gateway를 여러 격리된 라우터로 구성할 수 있습니다. 이는 여러 개의 Transit Gateway를 사용하는 것과 유사하지만 라우팅 및 연결이 변경될 수 있는 경우 더 많은 유연성을 제공합니다. 이 시나리오에서는 격리된 각 라우터에 단일 라우팅 테이블이 있습니다. 격리된 라우터와 연결된 모든 연결이 전파되어 해당 라우팅 테이블과 연결됩니다. 하나의 격리된 라우터와 연결된 경우 패킷을 서로 라우팅할 수 있지만, 격리된 다른 라우터에 연결된 경우 패킷을 라우팅하거나 수신할 수 없습니다.

내용

- [개요](#)
- [리소스](#)
- [라우팅](#)

개요

다음 다이어그램은 이 시나리오를 위한 구성의 주요 구성 요소를 보여줍니다. VPC A, VPC B, VPC C의 패킷은 Transit Gateway로 라우팅됩니다. 인터넷이 대상인 VPC A, VPC B, VPC C에 있는 서브넷의 패킷은 먼저 Transit Gateway를 통해 라우팅된 후 Site-to-Site VPN 연결로 라우팅됩니다(대상이 해당 네트워크 내에 있는 경우). 대상이 다른 VPC의 서브넷인 한 VPC의 패킷(예: 10.1.0.0~10.2.0.0)은 Transit Gateway를 통해 라우팅되고, Transit Gateway 라우팅 테이블에 해당 경로가 없으므로 차단됩니다.



리소스

이 시나리오에서는 다음 리소스를 생성합니다.

- VPC 3개. VPC 만들기에 대한 자세한 내용은 Amazon VPC 사용 설명서의 [VPC 만들기](#)를 참조하세요.
- 전송 게이트웨이. 자세한 내용은 [the section called “Transit Gateway 생성”](#) 섹션을 참조하세요.
- VPC 3개에 대한 Transit Gateway의 연결 3개. 자세한 내용은 [the section called “VPC에 대한 Transit Gateway Attachment 생성”](#) 섹션을 참조하세요.
- Transit Gateway의 Site-to-Site VPN 연결. 자세한 내용은 [the section called “VPN에 대한 Transit Gateway Attachment 생성”](#) 섹션을 참조하세요. AWS Site-to-Site VPN 사용 설명서의 [고객 게이트웨이 디바이스 요구 사항](#)을 검토해야 합니다.

VPN 연결이 가동되면 BGP 세션이 설정되고 VPN CIDR이 Transit Gateway 라우팅 테이블로 전파되며 VPC CIDR이 고객 게이트웨이 BGP 테이블에 추가됩니다.

라우팅

각 VPC에는 라우팅 테이블 하나가 있으며 Transit Gateway에는 라우팅 테이블 두 개가 있습니다. 하나는 VPC용이며 다른 하나는 VPN 연결용입니다.

VPC A, VPC B 및 VPC C 라우팅 테이블

각 VPC에는 항목 2개가 포함된 라우팅 테이블이 있습니다. 첫 번째 항목은 VPC의 로컬 IPv4 라우팅에 대한 기본 항목입니다. 이 항목을 사용하면 이 VPC의 인스턴스가 서로 통신할 수 있습니다. 두 번째 항목은 기타 IPv4 서브넷 트래픽을 모두 Transit Gateway로 라우팅합니다. 다음 표에 VPC A 경로가 나와 있습니다.

대상 주소	대상
10.1.0.0/16	로컬
0.0.0.0/0	tgw-id

Transit Gateway 라우팅 테이블

이 시나리오에서는 VPC에 대한 라우팅 테이블 하나와 VPN 연결에 대한 라우팅 테이블 하나를 사용합니다.

VPC 연결은 다음 라우팅 테이블과 연결되며, 해당 테이블에는 VPN 연결에 대한 전파된 라우팅이 있습니다.

대상 주소	대상	경로 유형
10.99.99.0/24	<i>VPN ### ## ##</i>	전파

VPC 연결은 다음 라우팅 테이블과 연결되며, 해당 테이블에는 각 VPN 연결에 대한 전파된 라우팅이 있습니다.

대상 주소	대상	경로 유형
10.1.0.0/16	<i>VPC A ##</i>	전파
10.2.0.0/16	<i>VPC B ##</i>	전파
10.3.0.0/16	<i>VPC C ##</i>	전파

전송 게이트웨이 라우팅 테이블에서 라우팅을 전파하는 방법에 대한 자세한 내용은 [Transit Gateway 라우팅 테이블에 라우팅 전파](#)를 참조하십시오.

고객 게이트웨이 BGP 테이블

고객 게이트웨이 BGP 테이블에는 다음과 같은 VPC CIDR이 포함되어 있습니다.

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

예: 공유 서비스를 사용하는 격리된 VPC

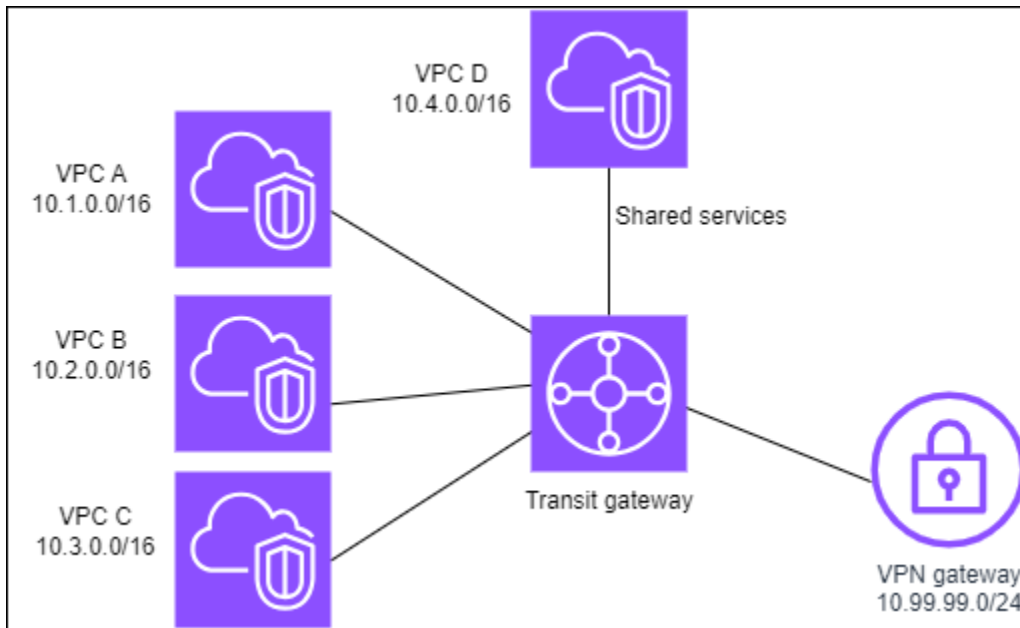
Transit Gateway를 공유 서비스를 사용하는 여러 격리된 라우터로 구성할 수 있습니다. 이는 여러 개의 Transit Gateway를 사용하는 것과 유사하지만 라우팅 및 연결이 변경될 수 있는 경우 더 많은 유연성을 제공합니다. 이 시나리오에서는 격리된 각 라우터에 단일 라우팅 테이블이 있습니다. 격리된 라우터와 연결된 모든 연결이 전파되어 해당 라우팅 테이블과 연결됩니다. 하나의 격리된 라우터와 연결된 경우 패킷을 서로 라우팅할 수 있지만, 격리된 다른 라우터에 연결된 경우 패킷을 라우팅하거나 수신할 수 없습니다. 연결은 공유 서비스로 패킷을 라우팅하거나 공유 서비스에서 패킷을 수신할 수 있습니다. 격리해야 하는 그룹이 있지만 공유 서비스(예: 프로덕션 시스템)를 사용하는 경우 이 시나리오를 사용할 수 있습니다.

내용

- [개요](#)
- [리소스](#)
- [라우팅](#)

개요

다음 다이어그램은 이 시나리오를 위한 구성의 주요 구성 요소를 보여줍니다. 인터넷이 대상인 VPC A, VPC B 및 VPC C에 있는 서브넷의 패킷은 먼저 Transit Gateway를 통해 라우팅된 후 Site-to-Site VPN을 위한 고객 게이트웨이로 라우팅됩니다. 대상이 VPC A, VPC B 또는 VPC C의 서브넷인 VPC A, VPC B 또는 VPC C에 있는 서브넷의 패킷은 Transit Gateway를 통해 라우팅되지만, Transit Gateway 라우팅 테이블에 경로가 없어 차단됩니다. 대상이 VPC D인 VPC A, VPC B, VPC C의 패킷은 Transit Gateway를 통해 라우팅된 후 VPC D로 라우팅됩니다.



리소스

이 시나리오에서는 다음 리소스를 생성합니다.

- VPC 4개. VPC 만들기에 대한 자세한 내용은 Amazon VPC 사용 설명서의 [VPC 만들기](#)를 참조하세요.
- 전송 게이트웨이. 자세한 내용은 [Transit Gateway 생성](#)을 참조하십시오.
- Transit Gateway의 VPC 연결 3개(VPC당 1개). 자세한 내용은 [the section called “VPC에 대한 Transit Gateway Attachment 생성”](#) 섹션을 참조하세요.
- Transit Gateway의 Site-to-Site VPN 연결. 자세한 내용은 [the section called “VPN에 대한 Transit Gateway Attachment 생성”](#) 섹션을 참조하세요.

AWS Site-to-Site VPN 사용 설명서의 [고객 게이트웨이 디바이스 요구 사항](#)을 검토해야 합니다.

VPN 연결이 가동되면 BGP 세션이 설정되고 VPN CIDR이 Transit Gateway 라우팅 테이블로 전파되며 VPC CIDR이 고객 게이트웨이 BGP 테이블에 추가됩니다.

- 각 격리된 VPC는 격리된 라우팅 테이블과 연결되고 공유된 라우팅 테이블로 전파됩니다.
- 각 공유된 서비스 VPC는 공유된 라우팅 테이블과 연결되고 두 라우팅 테이블로 전파됩니다.

라우팅

각 VPC에는 라우팅 테이블 하나가 있으며 Transit Gateway에는 라우팅 테이블 두 개가 있습니다. 하나는 VPC용이며 다른 하나는 VPN 연결 및 공유 서비스 VPC용입니다.

VPC A, VPC B, VPC C, VPC D 라우팅 테이블

각 VPC에는 항목 2개가 포함된 라우팅 테이블이 있습니다. 첫 번째 항목은 VPC의 로컬 라우팅에 대한 기본 항목으로서, 이 VPC의 인스턴스가 서로 통신할 수 있게 해줍니다. 두 번째 항목은 기타 IPv4 서브넷 트래픽을 모두 Transit Gateway로 라우팅합니다.

대상 주소	대상
10.1.0.0/16	로컬
0.0.0.0/0	<i>Transit Gateway ID</i>

Transit Gateway 라우팅 테이블

이 시나리오에서는 VPC에 대한 라우팅 테이블 하나와 VPN 연결에 대한 라우팅 테이블 하나를 사용합니다.

VPC A, B 및 C 연결은 다음 라우팅 테이블과 연결되며, 해당 테이블에는 VPN 연결에 대한 전파된 라우팅과 VPC D의 연결에 대한 전파된 라우팅이 있습니다.

대상 주소	대상	경로 유형
10.99.99.0/24	<i>VPN ### ## ##</i>	전파
10.4.0.0/16	<i>VPC D ##</i>	전파

VPN 연결 및 공유 서비스 VPC(VPC D) 연결은 각 VPC 연결을 가리키는 항목이 있는 다음 라우팅 테이블과 연결됩니다. 이렇게 하면 VPN 연결 및 공유 서비스 VPC에서 VPC와 통신할 수 있습니다.

대상 주소	대상	경로 유형
10.1.0.0/16	<i>VPC A ##</i>	전파

대상 주소	대상	경로 유형
10.2.0.0/16	VPC B ##	전파
10.3.0.0/16	VPC C ##	전파

자세한 내용은 [Transit Gateway 라우팅 테이블에 라우팅 전파](#) 섹션을 참조하세요.

고객 게이트웨이 BGP 테이블

고객 게이트웨이 BGP 테이블에는 4개의 VPC 모두에 대한 CIDR이 포함되어 있습니다.

예: 피어링된 Transit Gateway

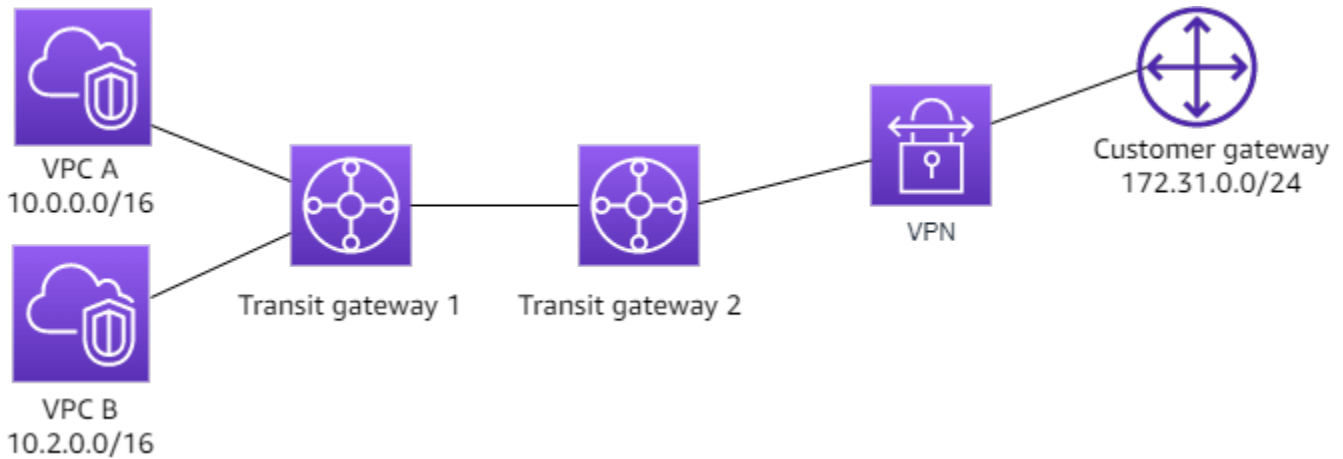
Transit Gateway 간에 Transit Gateway 피어링 연결을 생성할 수 있습니다. 그런 다음 각 Transit Gateway 연결 간에 트래픽을 라우팅할 수 있습니다. 이 시나리오에서는 VPC 및 VPN 연결이 Transit Gateway 기본 라우팅 테이블과 연결되어 Transit Gateway 기본 라우팅 테이블에 전파됩니다. 각 Transit Gateway 라우팅 테이블에는 Transit Gateway 피어링 연결을 가리키는 정적 라우팅이 있습니다.

내용

- [개요](#)
- [리소스](#)
- [라우팅](#)

개요

다음 다이어그램은 이 시나리오를 위한 구성의 주요 구성 요소를 보여줍니다. Transit Gateway 1에는 두 개의 VPC 연결이 있고, Transit Gateway 2에는 하나의 Site-to-Site VPN 연결이 있습니다. 인터넷이 대상인 VPC A 및 VPC B에 있는 서버의 패킷은 Transit Gateway 1, Transit Gateway 2, VPN 연결 순으로 라우팅됩니다.



리소스

이 시나리오에서는 다음 리소스를 생성합니다.

- VPC 2개. VPC 만들기에 대한 자세한 내용은 Amazon VPC 사용 설명서의 [VPC 만들기](#)를 참조하세요.
- 두 개의 전송 게이트웨이. 이들은 동일한 리전에 있거나 서로 다른 리전에 있을 수 있습니다. 자세한 내용은 [the section called “Transit Gateway 생성”](#) 섹션을 참조하세요.
- 첫 번째 Transit Gateway에 두 개의 VPC 연결. 자세한 내용은 [the section called “VPC에 대한 Transit Gateway Attachment 생성”](#) 섹션을 참조하세요.
- 두 번째 Transit Gateway의 Site-to-Site VPN 연결. 자세한 내용은 [the section called “VPN에 대한 Transit Gateway Attachment 생성”](#) 섹션을 참조하세요. AWS Site-to-Site VPN 사용 설명서의 [고객 게이트웨이 디바이스 요구 사항](#)을 검토해야 합니다.
- 두 Transit Gateway 간의 Transit Gateway 피어링 연결. 자세한 내용은 [Transit Gateway 피어링 연결](#) 섹션을 참조하세요.

VPC 연결을 생성할 때 각 VPC의 CIDR이 Transit Gateway 1의 라우팅 테이블에 전파됩니다. VPN 연결이 작동 중이면 다음 작업이 수행됩니다.

- BGP 세션이 설정됩니다.
- Site-to-Site VPN CIDR이 Transit Gateway 2의 라우팅 테이블로 전파됩니다.
- VPC CIDR이 고객 게이트웨이 BGP 테이블에 추가됩니다.

라우팅

각 VPC에는 라우팅 테이블이 있고 각 Transit Gateway에는 라우팅 테이블이 있습니다.

VPC A 및 VPC B 라우팅 테이블

각 VPC에는 항목 2개가 포함된 라우팅 테이블이 있습니다. 첫 번째 항목은 VPC의 로컬 IPv4 라우팅에 대한 기본 항목입니다. 이 기본 항목을 사용하면 이 VPC의 리소스가 서로 통신할 수 있습니다. 두 번째 항목은 기타 IPv4 서브넷 트래픽을 모두 Transit Gateway로 라우팅합니다. 다음 표에 VPC A 경로가 나와 있습니다.

대상 주소	대상
10.0.0.0/16	로컬
0.0.0.0/0	tgw-1-id

Transit Gateway 라우팅 테이블

다음은 라우팅 전파가 활성화된 Transit Gateway 1의 기본 라우팅 테이블의 예입니다.

대상 주소	대상	경로 유형
10.0.0.0/16	<i>VPC A# ## ID</i>	전파
10.2.0.0/16	<i>VPC B# ## ID</i>	전파
0.0.0.0/0	<i>### ### ## ID</i>	정적

다음은 라우팅 전파가 활성화된 Transit Gateway 2의 기본 라우팅 테이블의 예입니다.

대상 주소	대상	경로 유형
172.31.0.0/24	<i>VPN ### ## ## ID</i>	전파

대상 주소	대상	경로 유형
10.0.0.0/16	### ### ## ID	고정
10.2.0.0/16	### ### ## ID	정적

고객 게이트웨이 BGP 테이블

고객 게이트웨이 BGP 테이블에는 다음과 같은 VPC CIDR이 포함되어 있습니다.

- 10.0.0.0/16
- 10.2.0.0/16

예: 인터넷으로의 중앙 집중식 아웃바운드 라우팅

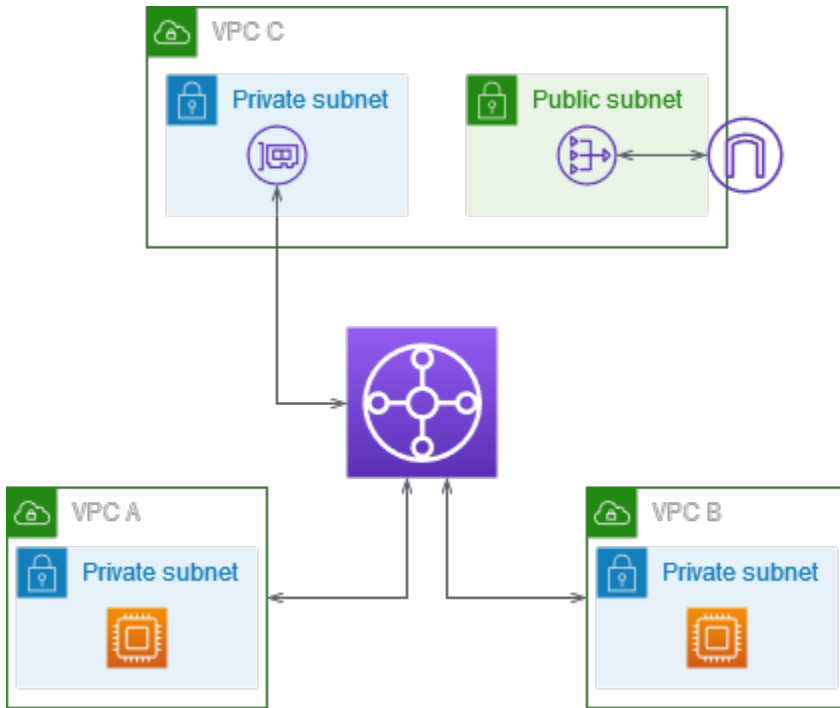
인터넷 게이트웨이 없이 VPC에서 NAT 게이트웨이와 인터넷 게이트웨이가 포함된 VPC로 아웃바운드 인터넷 트래픽을 라우팅하도록 전송 게이트웨이를 구성할 수 있습니다.

내용

- [개요](#)
- [리소스](#)
- [라우팅](#)

개요

다음 다이어그램은 이 시나리오를 위한 구성의 주요 구성 요소를 보여줍니다. 아웃바운드 전용 인터넷 액세스가 필요한 여러 VPC A 및 VPC B에 애플리케이션이 있습니다. VPC C는 퍼블릭 NAT 게이트웨이와 인터넷 게이트웨이 및 VPC 연결에 대한 프라이빗 서브넷으로 구성합니다. 전송 게이트웨이에 모든 VPC를 연결합니다. VPC A 및 VPC B에서 아웃바운드 인터넷 트래픽이 전송 게이트웨이를 VPC C로 통과하도록 라우팅을 구성합니다. VPC C의 NAT 게이트웨이는 트래픽을 인터넷 게이트웨이로 라우팅합니다.



리소스

이 시나리오에서는 다음 리소스를 생성합니다.

- IP 주소 범위가 겹치지 않는 VPC 3개입니다. 자세한 내용은 Amazon VPC 사용 설명서의 [VPC 생성](#)을 참조하세요.
- VPC A와 VPC B에는 각각 EC2 인스턴스가 있는 프라이빗 서브넷이 있습니다.
- VPC C에는 다음과 같은 기능이 있습니다.
 - VPC에 인터넷 게이트웨이 연결 자세한 내용은 Amazon VPC 사용 설명서의 [인터넷 게이트웨이 생성 및 연결](#)을 참조하세요.
 - NAT 게이트웨이를 포함한 퍼블릭 서브넷. 자세한 내용은 Amazon VPC 사용 설명서의 [NAT 게이트웨이 생성](#)을 참조하세요.
 - Transit Gateway Attachment를 위한 프라이빗 서브넷. 프라이빗 서브넷은 퍼블릭 서브넷과 같은 가용 영역에 있어야 합니다.
- 하나의 전송 게이트웨이입니다. 자세한 내용은 [the section called “Transit Gateway 생성”](#) 섹션을 참조하세요.
- Transit Gateway의 VPC 연결 3개. 각 VPC의 CIDR 블록이 전송 게이트웨이 라우팅 테이블에 전파됩니다. 자세한 내용은 [the section called “VPC에 대한 Transit Gateway Attachment 생성”](#) 섹션을 참조하세요. VPC C의 경우, 프라이빗 서브넷을 사용해 연결을 생성해야 합니다. 퍼블릭 서브넷을 사용해 연결을 생성하면 인스턴스 트래픽이 인터넷 게이트웨이로 라우팅되지만, 인스턴스에 퍼블릭 IP 주소

가 없기 때문에 인터넷 게이트웨이가 트래픽을 삭제합니다. 연결을 프라이빗 서브넷에 배치해야 트래픽이 NAT 게이트웨이로 라우팅되고, NAT 게이트웨이가 자체 탄력적 IP 주소를 소스 IP 주소로 사용하여 해당 트래픽을 인터넷 게이트웨이로 보냅니다.

라우팅

각 VPC에는 라우팅 테이블이 있고 전송 게이트웨이용 라우팅 테이블도 있습니다.

라우팅 테이블

- [VPC A의 라우팅 테이블](#)
- [VPC B의 라우팅 테이블](#)
- [VPC C의 라우팅 테이블](#)
- [Transit Gateway 라우팅 테이블](#)

VPC A의 라우팅 테이블

다음은 라우팅 테이블의 예입니다. 첫 번째 항목을 사용하면 VPC의 인스턴스가 서로 통신할 수 있습니다. 두 번째 항목은 기타 IPv4 서브넷 트래픽을 모두 Transit Gateway로 라우팅합니다.

대상 주소	대상
<i>VPC A CIDR</i>	로컬
0.0.0.0/0	<i>transit-gateway-id</i>

VPC B의 라우팅 테이블

다음은 라우팅 테이블의 예입니다. 첫 번째 항목을 사용하면 VPC의 인스턴스가 서로 통신할 수 있습니다. 두 번째 항목은 기타 IPv4 서브넷 트래픽을 모두 Transit Gateway로 라우팅합니다.

대상 주소	대상
	로컬

대상 주소	대상
<i>VPC B CIDR</i>	
0.0.0.0/0	<i>transit-gateway-id</i>

VPC C의 라우팅 테이블

인터넷 게이트웨이에 경로를 추가하여 NAT 게이트웨이를 퍼블릭 서브넷으로 서브넷을 구성합니다. 다른 서브넷은 프라이빗 서브넷으로 둡니다.

다음은 퍼블릭 서브넷의 라우팅 테이블 예입니다. 첫 번째 항목을 사용하면 VPC의 인스턴스가 서로 통신할 수 있습니다. 두 번째 및 세 번째 항목은 VPC A 및 VPC B에 대한 트래픽을 전송 게이트웨이로 라우팅합니다. 남은 항목에서는 기타 IPv4 서브넷 트래픽을 모두 인터넷 게이트웨이로 라우팅합니다.

대상 주소	대상
<i>VPC C CIDR</i>	로컬
<i>VPC A CIDR</i>	<i>transit-gateway-id</i>
<i>VPC B CIDR</i>	<i>transit-gateway-id</i>
0.0.0.0/0	<i>internet-gateway-id</i>

다음은 프라이빗 서브넷의 라우팅 테이블 예입니다. 첫 번째 항목을 사용하면 VPC의 인스턴스가 서로 통신할 수 있습니다. 두 번째 항목은 기타 IPv4 서브넷 트래픽을 모두 NAT 게이트웨이로 라우팅합니다.

대상 주소	대상
<i>VPC C CIDR</i>	로컬
0.0.0.0/0	<i>nat-gateway-id</i>

Transit Gateway 라우팅 테이블

다음은 Transit Gateway 라우팅 테이블의 예입니다. 각 VPC의 CIDR 블록이 Transit Gateway 라우팅 테이블에 전파됩니다. 정적 라우팅은 아웃바운드 인터넷 트래픽을 VPC C로 보냅니다. 필요에 따라 각 VPC CIDR에 블랙홀 경로를 추가하여 VPC 간 통신을 방지할 수 있습니다.

CIDR	연결	경로 유형
<i>VPC A CIDR</i>	<i>VPC A ##</i>	전파
<i>VPC B CIDR</i>	<i>VPC B ##</i>	전파
<i>VPC C CIDR</i>	<i>VPC C ##</i>	전파
0.0.0.0/0	<i>VPC C ##</i>	고정

예: 공유 서비스 VPC의 어플라이언스

공유 서비스 VPC에 있는 어플라이언스(예: 보안 어플라이언스)를 구성할 수 있습니다. Transit Gateway Attachment 간에 라우팅되는 모든 트래픽은 먼저 공유 서비스 VPC의 어플라이언스에서 검사합니다. 어플라이언스 모드가 활성화되면 Transit Gateway는 흐름 해시 알고리즘을 사용하여 어플라이언스 VPC에서 단일 네트워크 인터페이스를 선택하여 흐름 수명 동안 트래픽을 전송합니다. Transit Gateway는 반환 트래픽에 대해 동일한 네트워크 인터페이스를 사용합니다. 이렇게 하면 양방향 트래픽이 대칭적으로 라우팅됩니다. 즉, 트래픽 흐름은 수명이 다할 때까지 VPC 연결의 동일한 가용 영역을 통해 라우팅됩니다. 아키텍처에 여러 Transit Gateway가 있는 경우 각 Transit Gateway는 자체 세션 선호도를 유지하며 각 Transit Gateway는 다른 네트워크 인터페이스를 선택할 수 있습니다.

흐름 안정성을 보장하려면 정확히 하나의 전송 게이트웨이를 어플라이언스 VPC에 연결해야 합니다. 여러 전송 게이트웨이를 단일 어플라이언스 VPC에 연결해도 전송 게이트웨이가 흐름 상태 정보를 서로 공유하지 않기 때문에 흐름 안정성이 보장되지 않습니다.

Important

- 소스 및 대상 트래픽이 동일한 Transit Gateway Attachment에서 중앙 VPC(검사 VPC)로 들어오는 한 어플라이언스 모드의 트래픽은 올바르게 라우팅됩니다. 두 개의 서로 다른 Transit

Gateway Attachment에서 소스와 대상이 들어오는 경우 트래픽이 삭제될 수 있습니다. 어플라이언스 모드는 VPN을 통해 네트워크에 들어가는 트래픽에는 적용되지 않습니다.

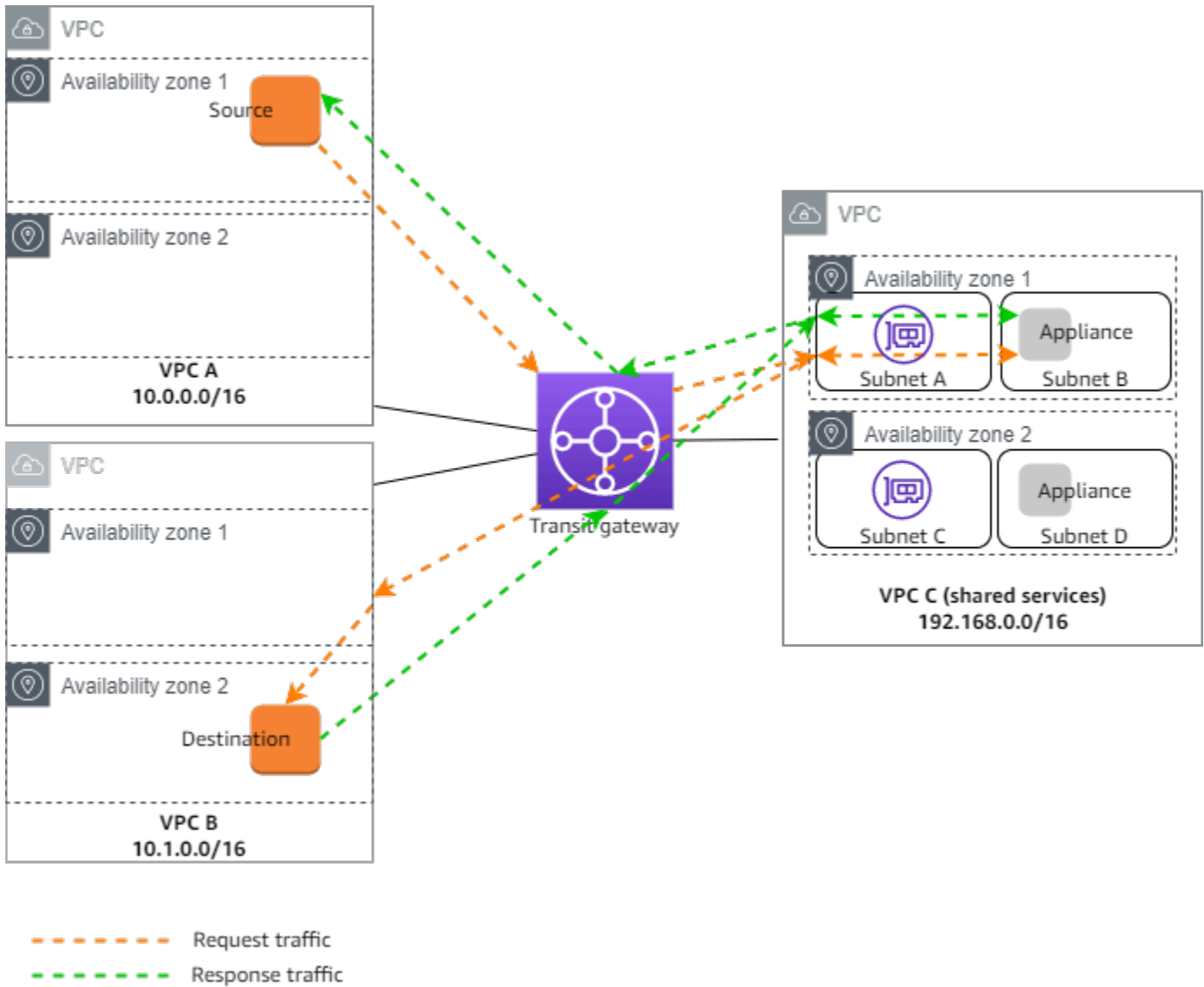
- 기존 첨부 파일에서 어플라이언스 모드를 활성화하면 첨부 파일이 모든 가용 영역을 통과할 수 있으므로 해당 첨부 파일의 현재 경로에 영향을 미칠 수 있습니다. 어플라이언스 모드가 활성화되지 않은 경우 트래픽은 원래 가용 영역으로 유지됩니다.

내용

- [개요](#)
- [상태 저장 어플라이언스 및 어플라이언스 모드](#)
- [라우팅](#)

개요

다음 다이어그램은 이 시나리오를 위한 구성의 주요 구성 요소를 보여줍니다. Transit Gateway에는 VPC 연결 3개가 있습니다. VPC C는 공유 서비스 VPC입니다. VPC A와 VPC B 간의 트래픽은 Transit Gateway로 라우팅되며, 검사를 위해 VPC C의 보안 어플라이언스로 라우팅된 다음 최종 대상으로 라우팅됩니다. 어플라이언스는 상태 저장 장치이므로 요청 트래픽과 응답 트래픽을 모두 검사합니다. 고가용성을 위해 VPC C의 각 가용 영역에 어플라이언스가 있습니다.



이 시나리오에서는 다음 리소스를 생성합니다.

- VPC 3개. VPC 생성에 대한 자세한 내용은 Amazon Virtual Private Cloud 사용 설명서의 [VPC 생성](#)을 참조하세요.
- Transit Gateway. 자세한 내용은 [the section called “Transit Gateway 생성”](#) 단원을 참조하세요.
- VPC 연결 3개 - 각 VPC에 하나씩 존재합니다. 자세한 내용은 [the section called “VPC에 대한 Transit Gateway Attachment 생성”](#) 단원을 참조하세요.

각 VPC 연결의 각 가용 영역에 서브넷을 지정합니다. 공유 서비스 VPC의 경우에는 트래픽이 Transit Gateway에서 VPC로 라우팅되는 서브넷을 지정해야 합니다. 앞의 예에서는 서브넷 A와 C가 여기에 해당합니다.

VPC C에 대한 VPC 연결의 경우에는 어플라이언스 모드 지원을 활성화하여 응답 트래픽이 소스 트래픽과 같은 VPC C의 가용 영역으로 라우팅되게 해야 합니다.

Amazon VPC 콘솔은 어플라이언스 모드를 지원합니다. 또한 Amazon VPC API, AWS SDK, AWS CLI을(를) 사용하여 어플라이언스 모드 또는 AWS CloudFormation을(를) 활성화할 수 있습니다. 예를 들어 `-attachment` 또는 [create-transit-gateway-vpcmodify-transit-gateway-vpc-attachment 명령어](#)에 추가하십시오 `--options ApplianceModeSupport=enable`.

Note

어플라이언스 모드의 흐름 안정성은 검사 VPC를 향해 발생하는 소스 및 대상 트래픽에 대해서만 보장됩니다.

상태 저장 어플라이언스 및 어플라이언스 모드

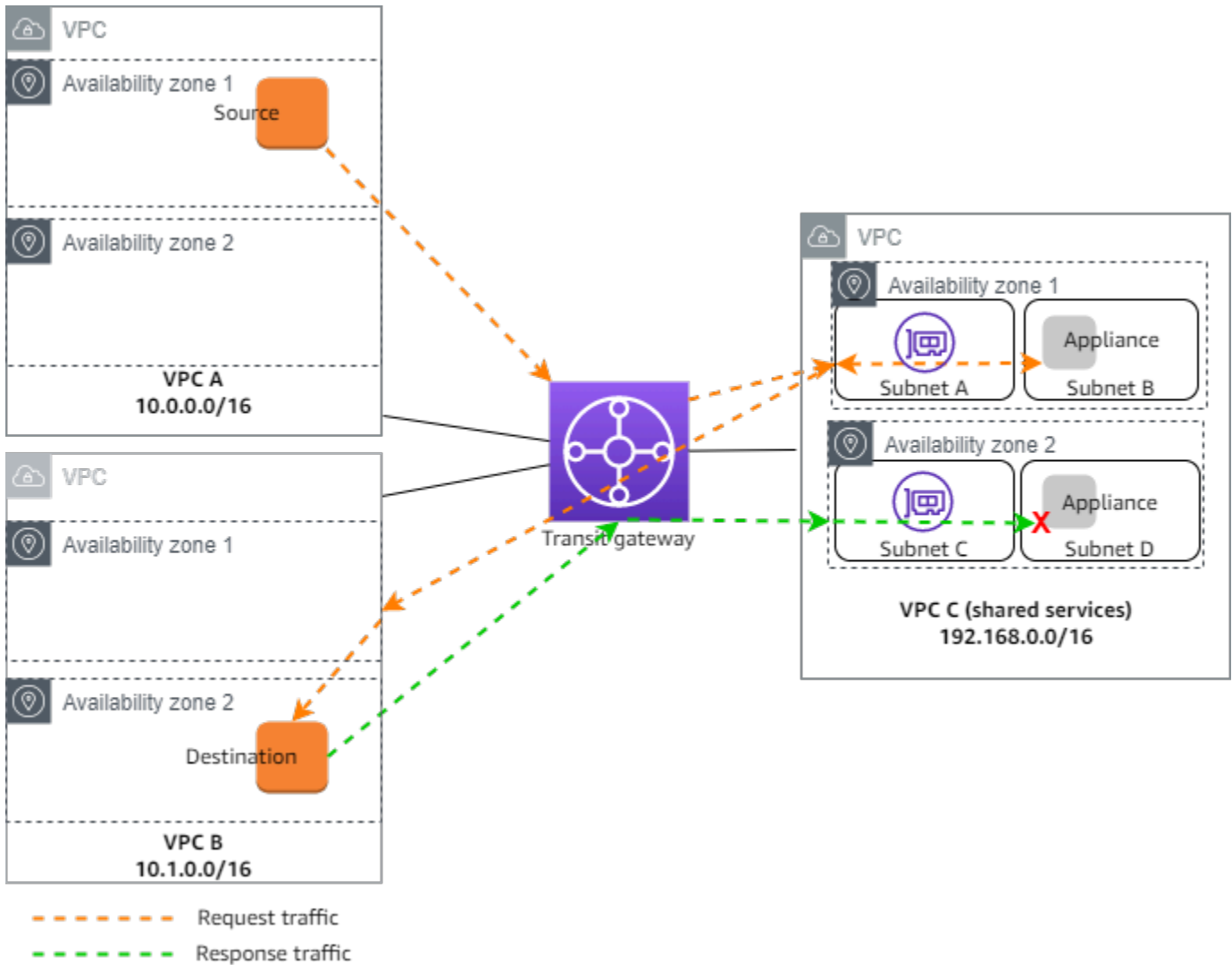
VPC 연결이 여러 가용 영역에 걸쳐 있고 상태 저장 검사를 위해 소스 및 대상 호스트 간의 트래픽을 동일한 어플라이언스를 통해 라우팅해야 하는 경우, 어플라이언스가 있는 VPC 연결에 대한 어플라이언스 모드 지원을 활성화합니다.

자세한 내용은 AWS 블로그의 [중앙 집중식 검사 아키텍처](#)를 참조하세요.

어플라이언스 모드가 활성화되지 않은 경우의 동작

어플라이언스 모드가 활성화되지 않은 경우, Transit Gateway는 대상에 도달할 때까지 트래픽이 원래 가용 영역의 VPC 연결 간에 라우팅을 유지하려고 합니다. 트래픽은 가용 영역 장애가 있거나 가용 영역에 VPC 연결과 연결된 서브넷이 없는 경우에만 연결 사이의 가용 영역을 지납니다.

다음 다이어그램은 어플라이언스 모드 지원이 활성화되지 않은 경우의 트래픽 흐름을 보여 줍니다. VPC B의 가용 영역 2에서 시작된 응답 트래픽은 Transit Gateway에 의해 VPC C의 동일한 가용 영역으로 라우팅됩니다. 따라서 가용 영역 2의 어플라이언스가 VPC A에 있는 소스의 원래 요청을 인식하지 못하기 때문에 트래픽이 삭제됩니다.



라우팅

각 VPC에는 하나 이상의 라우팅 테이블이 있고 Transit Gateway에는 라우팅 테이블 두 개가 있습니다.

VPC 라우팅 테이블

VPC A 및 VPC B

VPC A와 B에는 항목 두 개가 있는 라우팅 테이블이 있습니다. 첫 번째 항목은 VPC의 로컬 IPv4 라우팅에 대한 기본 항목입니다. 이 기본 항목을 사용하면 이 VPC의 리소스가 서로 통신할 수 있습니다. 두 번째 항목은 기타 IPv4 서브넷 트래픽을 모두 Transit Gateway로 라우팅합니다. 다음은 VPC A의 라우팅 테이블입니다.

대상 주소	대상
10.0.0.0/16	로컬
0.0.0.0/0	tgw-id

VPC C

공유 서비스 VPC(VPC C)에는 서브넷마다 다른 라우팅 테이블이 있습니다. 서브넷 A는 Transit Gateway서 사용합니다(VPC 연결을 만들 때 이 서브넷을 지정합니다). 서브넷 A의 라우팅 테이블은 모든 트래픽을 서브넷 B의 어플라이언스로 라우팅합니다.

대상 주소	대상
192.168.0.0/16	로컬
0.0.0.0/0	appliance-eni-id

(어플라이언스가 있는) 서브넷 B에 대한 라우팅 테이블은 트래픽을 Transit Gateway로 돌려보냅니다.

대상 주소	대상
192.168.0.0/16	로컬
0.0.0.0/0	tgw-id

Transit Gateway 라우팅 테이블

이 Transit Gateway는 VPC A 및 VPC B에 하나의 라우팅 테이블을, 공유 서비스 VPC(VPC C)에 하나의 라우팅 테이블을 사용합니다.

VPC A 및 VPC B 연결은 다음 라우팅 테이블과 연결됩니다. 라우팅 테이블은 모든 트래픽을 VPC C로 라우팅합니다.

대상 주소	대상	경로 유형
0.0.0.0/0	<i>VPC C# ## ID</i>	고정

VPC C 연결은 다음 라우팅 테이블과 연결됩니다. 이 연결은 트래픽을 VPC A와 VPC B로 라우팅합니다.

대상 주소	대상	경로 유형
10.0.0.0/16	<i>VPC A# ## ID</i>	전파
10.1.0.0/16	<i>VPC B# ## ID</i>	전파

Transit Gateway로 작업

Amazon VPC 콘솔 또는 AWS CLI를 사용하여 Transit Gateway로 작업할 수 있습니다.

내용

- [Transit Gateway](#)
- [VPC에 대한 Transit Gateway Attachment](#)
- [Transit Gateway VPN 연결](#)
- [Direct Connect 게이트웨이에 Transit Gateway 연결](#)
- [Transit Gateway 피어링 연결](#)
- [Transit Gateway Connect 연결 및 Transit Gateway Connect 피어](#)
- [Transit Gateway 라우팅 테이블](#)
- [Transit Gateway 정책 테이블](#)
- [Transit Gateway의 멀티캐스트](#)

Transit Gateway

Transit Gateway를 사용하면 VPC와 VPN 연결을 연결하고 두 리전 간의 트래픽을 라우팅할 수 있습니다. 트랜짓 게이트웨이는 여러 곳에서 작동하며 AWS 계정, 트랜짓 게이트웨이를 다른 계정과 공유하는 AWS RAM 데 사용할 수 있습니다. 다른 AWS 계정사람과 트랜짓 게이트웨이를 공유한 후 계정 소유자가 자신의 VPC를 트랜짓 게이트웨이에 연결할 수 있습니다. 두 계정의 사용자는 언제든지 연결을 삭제할 수 있습니다.

Transit Gateway에서 멀티캐스트를 활성화한 다음 도메인과 연결된 VPC 연결을 통해 멀티캐스트 소스에서 멀티캐스트 그룹 멤버로 멀티캐스트 트래픽을 보낼 수 있는 Transit Gateway 멀티캐스트 도메인을 생성할 수 있습니다.

각 VPC 또는 VPN 연결은 단일 라우팅 테이블과 연결됩니다. 해당 라우팅 테이블은 해당 리소스 연결에서 들어오는 트래픽에 대한 다음 홉을 결정합니다. Transit Gateway 내부의 라우팅 테이블은 IPv4 또는 IPv6 CIDR 및 대상에 대해 모두 허용됩니다. 대상은 VPC 및 VPN 연결입니다. Transit Gateway에서 VPC를 연결하거나 VPN 연결을 생성하면 Transit Gateway의 기본 라우팅 테이블과 연결됩니다.

Transit Gateway 내부에 추가 라우팅 테이블을 생성하고 VPC 또는 VPN 연결을 이 라우팅 테이블로 변경할 수 있습니다. 이를 통해 네트워크를 세분화할 수 있습니다. 예를 들어, 개발 VPC를 라우팅 테이블

하나와 연결하고 프로덕션 VPC를 다른 라우팅 테이블과 연결할 수 있습니다. 이를 통해 기존 네트워크에서 가상 라우팅 및 전달(VRF)과 유사한 Transit Gateway 내부의 격리된 네트워크를 생성할 수 있습니다.

Transit Gateway는 연결된 VPC와 VPN 연결 간의 동적 및 정적 라우팅을 지원합니다. 각 연결에 대해 라우팅 전파를 활성화하거나 비활성화할 수 있습니다. Transit Gateway 피어링 연결은 정적 라우팅만 지원합니다. 하지만 같은 지역에 있는 두 트랜짓 게이트웨이 간의 피어링을 가리키는 고정 경로를 추가할 수 없습니다.

선택적으로 하나 이상의 IPv4 또는 IPv6 CIDR 블록을 Transit Gateway와 연결할 수 있습니다. [Transit Gateway Connect 연결](#)에 대한 Transit Gateway Connect 피어를 설정할 때 CIDR 블록에서 IP 주소를 지정합니다. 169.254.0.0/16 범위 내의 주소와 VPC 연결 및 온프레미스 네트워크의 주소와 겹치는 범위를 제외한 모든 퍼블릭 또는 프라이빗 IP 주소 범위를 연결할 수 있습니다. IPv4 및 IPv6 CIDR 블록에 대한 자세한 내용은 Amazon VPC 사용 설명서에서 [VPC 및 서브넷](#)을 참조하세요.

Tasks

- [Transit Gateway 생성](#)
- [Transit Gateway 보기](#)
- [Transit Gateway에 대한 태그 추가 또는 편집](#)
- [Transit Gateway 수정](#)
- [Transit Gateway 공유](#)
- [리소스 공유 수락](#)
- [공유 연결 수락](#)
- [Transit Gateway 삭제](#)

Transit Gateway 생성

Transit Gateway를 생성할 때 기본 Transit Gateway 라우팅 테이블을 만들어 기본 연결 라우팅 테이블과 기본 전파 라우팅 테이블로 사용합니다. 기본 Transit Gateway 라우팅 테이블을 생성하지 않도록 선택한 경우 나중에 생성할 수 있습니다. 경로 및 라우팅 테이블에 대한 자세한 내용은 [??? 단원](#)을 참조하세요.

콘솔을 사용하여 Transit Gateway 생성

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway를 선택합니다.

3. Transit Gateway 생성(Create Transit Gateway)을 선택합니다.
4. (선택 사항) 이름 태그에 Transit Gateway의 이름을 입력합니다. 이름 태그를 사용하면 게이트웨이 목록에서 특정 게이트웨이를 쉽게 식별할 수 있습니다. 이름 태그(Name tag)를 추가하면 키가 이름이고 입력한 값과 동일한 값을 가진 태그가 생성됩니다.
5. (선택 사항) 설명에 Transit Gateway에 대한 설명을 입력합니다.
6. Amazon 측 자율 시스템 번호(ASN)(Amazon side Autonomous System Number(ASN))의 경우 기본 ASN을 사용하도록 기본값을 그대로 두거나 Transit Gateway용 프라이빗 ASN을 입력합니다. 이는 BGP (보더 게이트웨이 프로토콜) 세션 AWS 측의 ASN이어야 합니다.

16비트 ASN의 경우 범위는 64512~65534입니다.

32비트 ASN의 경우 범위는 4200000000~4294967294입니다.

다중 리전 배포가 있는 경우 각 Transit Gateway에 고유한 ASN을 사용하는 것이 좋습니다.

7. Transit Gateway에 연결된 다른 VPC의 인스턴스에서 쿼리할 때 퍼블릭 IPv4 DNS 호스트 이름을 프라이빗 IPv4 주소로 확인하기 위해 VPC가 필요한 경우 DNS 지원(DNS support)에서 이 옵션을 선택합니다.
8. VPN 터널 간에 ECMP(Equal Cost Multipath) 라우팅 지원이 필요한 경우 VPN ECMP 지원(VPN ECMP support)에서 이 옵션을 선택합니다. 연결에서 동일한 CIDR을 광고하는 경우 해당 트래픽은 이러한 CIDR 간에 균등하게 분산됩니다.

이 옵션을 선택하는 경우 알려진 BGP ASN, AS-path와 같은 BGP 속성 및 기본 설정의 커뮤니티가 동일해야 합니다.

Note

ECMP를 사용하려면 동적 라우팅을 사용하는 VPN 연결을 생성해야 합니다. 정적 라우팅을 사용하는 VPN 연결은 ECMP를 지원하지 않습니다.

9. 전송 게이트웨이의 기본 라우팅 테이블이 있는 Transit Gateway Attachment에 자동으로 연결하려면 기본 라우팅 테이블 연결(Default route table association)에서 이 옵션을 선택합니다.
10. Transit Gateway Attachment를 전송 게이트웨이의 기본 라우팅 테이블로 자동으로 전파하려면 기본 라우팅 테이블 전파(Default route table propagation)에서 이 옵션을 선택합니다.
11. (선택 사항) Transit Gateway를 멀티캐스트 트래픽의 라우터로 사용하려면 멀티캐스트 지원(Multicast support)을 선택합니다.
12. 교차 계정 연결을 자동으로 수락하려면 공유 연결 자동 수락(Auto accept shared attachments)에서 이 옵션을 선택합니다.

13. (선택 사항) Transit Gateway CIDR 블록(Transit gateway CIDR blocks)에서 Transit Gateway에 대해 하나 이상의 IPv4 또는 IPv6 CIDR 블록을 지정합니다.

IPv4의 경우 크기 /24 이상의 CIDR 블록(예: /23 또는 /22) 또는 IPv6의 경우 크기 /64 이상의 CIDR 블록(예: /63 또는 /62)을 지정할 수 있습니다. 169.254.0.0/16 범위 내의 주소와 VPC 연결 및 온프레미스 네트워크의 주소와 겹치는 범위를 제외한 모든 퍼블릭 또는 프라이빗 IP 주소 범위를 연결할 수 있습니다.

14. Transit Gateway 생성(Create Transit Gateway)을 선택합니다.

를 사용하여 트랜짓 게이트웨이를 만들려면 AWS CLI

[create-transit-gateway](#) 명령을 사용합니다.

Transit Gateway 보기

콘솔을 사용하여 Transit Gateway 보기

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway를 선택합니다. Transit Gateway 세부 정보는 페이지의 게이트웨이 목록 아래에 표시됩니다.

를 사용하여 트랜짓 게이트웨이를 보려면 AWS CLI

[describe-transit-gateways](#) 명령을 사용합니다.

Transit Gateway에 대한 태그 추가 또는 편집

리소스에 태그를 추가하면 용도, 소유자 또는 환경과 같은 기준으로 태그를 구성하고 식별할 수 있습니다. 각 Transit Gateway에 여러 태그를 추가할 수 있습니다. 태그 키는 Transit Gateway별로 고유해야 합니다. Transit Gateway에 이미 연결된 키를 통해 태그를 추가하면 태그의 값이 업데이트됩니다. 자세한 내용은 [Amazon EC2 리소스에 태깅](#)을 참조하세요.

콘솔을 사용하여 Transit Gateway에 태그 추가

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway를 선택합니다.
3. 태그를 추가하거나 편집할 Transit Gateway를 선택합니다.

4. 페이지 아래쪽에서 태그(Tags) 탭을 선택합니다.
5. 태그 관리를 선택합니다.
6. 새 태그 추가를 선택합니다.
7. 해당 태그의 키와 값을 입력합니다.
8. 저장(Save)을 선택합니다.

Transit Gateway 수정

Transit Gateway에 대한 구성 옵션을 수정할 수 있습니다. Transit Gateway를 수정하는 경우 수정된 옵션은 새 Transit Gateway Attachment에만 적용됩니다. 기존 Transit Gateway Attachment는 수정되지 않으며 서비스 중단이 발생하지 않습니다.

공유된 Transit Gateway는 수정할 수 없습니다.

IP 주소 중 하나라도 현재 [Connect 피어](#)에 사용되는 경우 전송 게이트웨이의 CIDR 블록을 제거할 수 없습니다.

Transit Gateway 수정

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateways를 선택합니다.
3. 수정할 Transit Gateway를 선택합니다.
4. 작업(Actions), Transit Gateway 수정(Modify Transit Gateway)을 선택합니다.
5. 필요에 따라 옵션을 수정하고 Transit Gateway 수정(Modify transit gateway)을 선택합니다.

를 사용하여 트랜짓 게이트웨이를 수정하려면 AWS CLI

[modify-transit-gateway](#) 명령을 사용합니다.

Transit Gateway 공유

를 AWS RAM 사용하여 계정 간 또는 조직 전체에서 [트랜짓 게이트웨이를 공유할 수](#) AWS Organizations 있습니다. 소유하고 있는 Transit Gateway를 공유하려면 다음 절차를 따릅니다.

조직의 관리 계정에서 리소스 공유를 활성화해야 합니다. 리소스 공유를 활성화하는 방법에 대한 자세한 내용은 [사용 AWS RAM 설명서의 AWS Organizations와 공유 활성화](#)를 참조하십시오.

Transit Gateway 공유

1. <https://console.aws.amazon.com/ram/> 에서 AWS RAM 콘솔을 엽니다.
2. 리소스 공유 생성(Create a resource share)을 선택합니다.
3. 이름(Name)에 리소스 공유에 대한 서술형 이름을 입력합니다.
4. 리소스 유형 선택(Select resource type)에서 Transit Gateway를 선택합니다. Transit Gateway를 선택합니다.
5. (선택 사항) 보안 주체(Principals)에서 리소스 공유에 보안 주체를 추가합니다. 각 AWS 계정, OU 또는 조직에 대해 해당 ID를 지정하고 추가를 선택합니다.

외부 계정 허용의 경우 조직 외부 사용자와 AWS 계정 이 리소스를 공유할 수 있도록 허용할지 여부를 선택합니다.

6. (선택 사항) 태그(Tags) 아래에 각 태그에 대한 태그 키와 태그 값 페어를 입력합니다. 이러한 태그는 리소스 공유에는 적용되지만 Transit Gateway에는 적용되지 않습니다.
7. 리소스 공유 생성(Create resource share)을 선택합니다.

리소스 공유 수락

리소스 공유에 추가되면 해당 리소스 공유에 가입하라는 초대기가 발송됩니다. 공유 리소스에 액세스하려면 먼저 리소스 공유를 수락해야 합니다.

리소스 공유 수락

1. <https://console.aws.amazon.com/ram/> 에서 AWS RAM 콘솔을 엽니다.
2. 탐색 창에서 나와 공유됨(Shared with me), 리소스 공유(Resource shares)를 선택합니다.
3. 리소스 공유를 선택합니다.
4. 리소스 공유 수락(Accept resource share)을 선택합니다.
5. 공유 Transit Gateway를 보려면 Amazon VPC 콘솔에서 Transit Gateways 페이지를 엽니다.

공유 연결 수락

Transit Gateway를 생성할 때 공유 연결 자동 수락(Auto accept shared attachments) 기능을 활성화하지 않은 경우 교차 계정(공유) 연결을 수동으로 수락해야 합니다.

공유 연결 수동 수락

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway Attachments를 선택합니다.
3. 수락이 보류 중인 Transit Gateway Attachment를 선택합니다.
4. 작업(Actions), Transit Gateway Attachment 수락(Accept transit gateway attachment)을 선택합니다.

를 사용하여 공유 첨부 파일을 수락하려면 AWS CLI

[accept-transit-gateway-vpc-attach](#) 명령을 사용합니다.

Transit Gateway 삭제

기존 연결이 있는 Transit Gateway는 삭제할 수 없습니다. Transit Gateway를 삭제하려면 먼저 모든 연결을 삭제해야 합니다.

콘솔을 사용하여 Transit Gateway 삭제

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 삭제할 Transit Gateway를 선택합니다.
3. 작업(Actions), Transit Gateway 삭제>Delete Transit Gateway)를 선택합니다. **delete**를 입력하고 삭제>Delete)를 선택하여 삭제를 확인합니다.

를 사용하여 트랜짓 게이트웨이를 삭제하려면 AWS CLI

[delete-transit-gateway](#) 명령을 사용합니다.

VPC에 대한 Transit Gateway Attachment

VPC를 Transit Gateway에 연결하는 경우 트래픽을 라우팅하기 위해 Transit Gateway에서 사용할 각 가용 영역의 서브넷을 하나 지정해야 합니다. 가용 영역에서 하나의 서브넷을 지정하면 해당 가용 영역의 모든 서브넷에 있는 리소스에 트래픽이 도달할 수 있습니다.

Limits

- VPC를 전송 게이트웨이에 연결하면 Transit Gateway Attachment가 없는 가용 영역의 모든 리소스는 전송 게이트웨이에 도달할 수 없습니다. 서브넷 라우팅 테이블에 Transit Gateway에 대한 경로가 있는 경우 동일한 가용 영역의 서브넷에 연결이 있을 때만 트래픽이 Transit Gateway에 전달됩니다.
- Transit Gateway에 연결된 VPC의 리소스는 동일한 Transit Gateway에도 연결된 다른 VPC의 보안 그룹에 액세스할 수 없습니다.
- Transit Gateway는 Amazon Route 53에서 프라이빗 호스팅 영역을 사용하여 설정된 연결된 VPC의 사용자 지정 DNS 이름에 대한 DNS 확인은 지원하지 않습니다. 전송 게이트웨이에 연결된 모든 VPC의 프라이빗 호스팅 영역에 대한 이름 확인을 구성하려면 [Amazon Route 53 및 AWS Transit Gateway를 사용한 하이브리드 클라우드의 중앙 집중식 DNS 관리를 참조하십시오](#).
- Transit Gateway는 동일한 CIDR을 가진 VPC 간의 라우팅을 지원하지 않습니다. VPC를 Transit Gateway에 연결하고 해당 CIDR이 이미 Transit Gateway에 연결된 다른 VPC의 CIDR과 동일한 경우 새로 연결된 VPC의 경로가 Transit Gateway 라우팅 테이블로 전파되지 않습니다.
- 로컬 영역에 상주하는 VPC 서브넷에 대해서는 연결을 생성할 수 없습니다. 대신 로컬 영역의 서브넷이 상위 가용 영역을 통해 Transit Gateway에 연결할 수 있도록 네트워크를 구성할 수 있습니다. 자세한 내용은 [Transit Gateway에 로컬 영역 서브넷 연결](#)을 참조하세요.
- IPv6 전용 서브넷을 사용하여 Transit Gateway Attachment를 생성할 수 없습니다. Transit Gateway Attachment 서브넷은 IPv4 주소도 지원해야 합니다.
- 전송 게이트웨이에 하나 이상의 VPC 연결 파일이 있어야 해당 전송 게이트웨이를 라우팅 테이블에 추가할 수 있습니다.

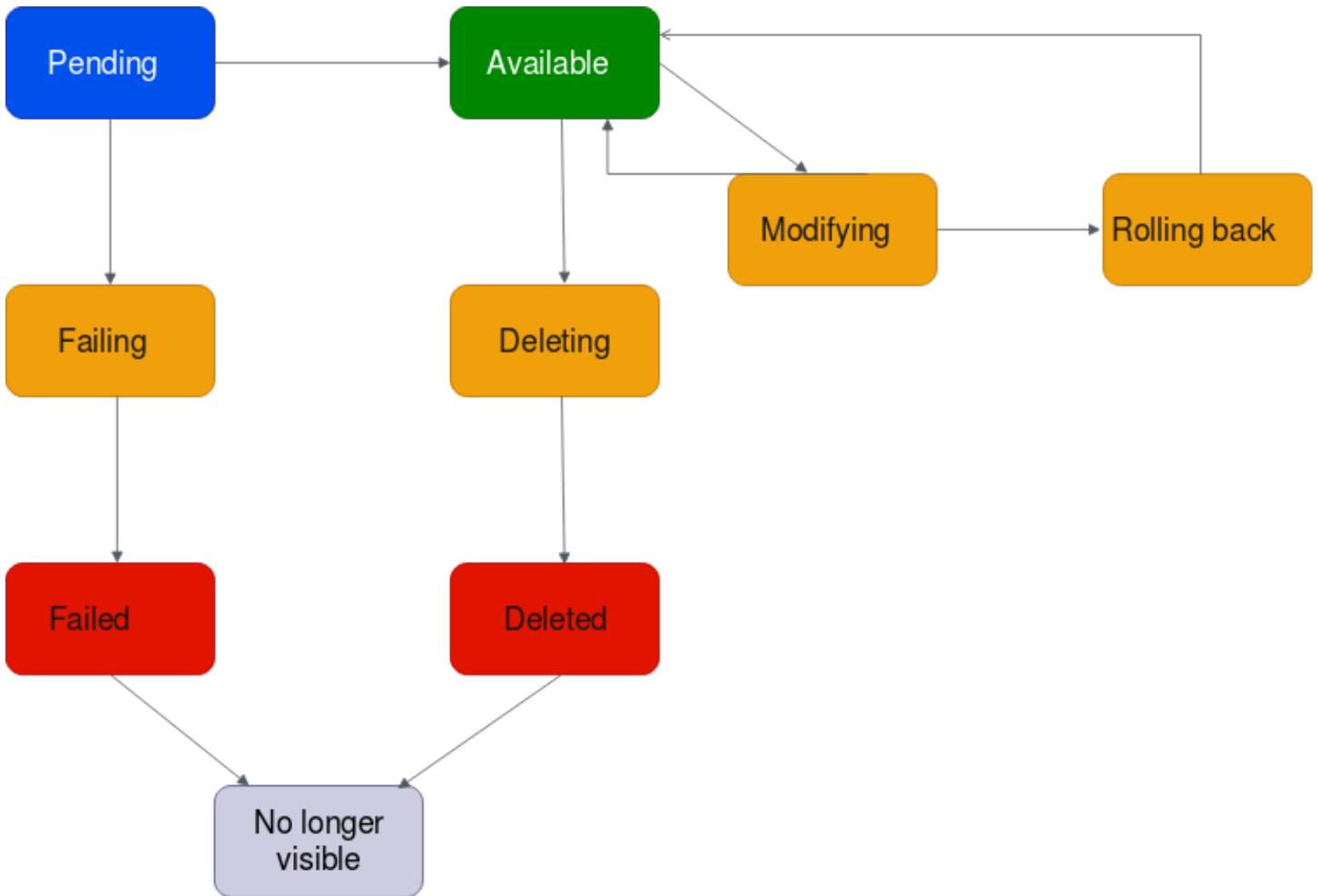
내용

- [VPC 연결 수명 주기](#)
- [VPC에 대한 Transit Gateway Attachment 생성](#)
- [VPC 연결 수정](#)
- [VPC 연결 태그 수정](#)
- [VPC 연결 보기](#)
- [VPC 연결 삭제](#)
- [VPC 연결 생성 문제 해결](#)

VPC 연결 수명 주기

VPC 연결은 요청이 시작될 때부터 다양한 단계를 거칩니다. 각 단계에는 취할 수 있는 몇 가지 조치가 있으며, 수명 주기가 끝날 때 VPC 연결은 Amazon Virtual Private Cloud Console 과 API 또는 명령줄 출력에 일정 시간 동안 표시됩니다.

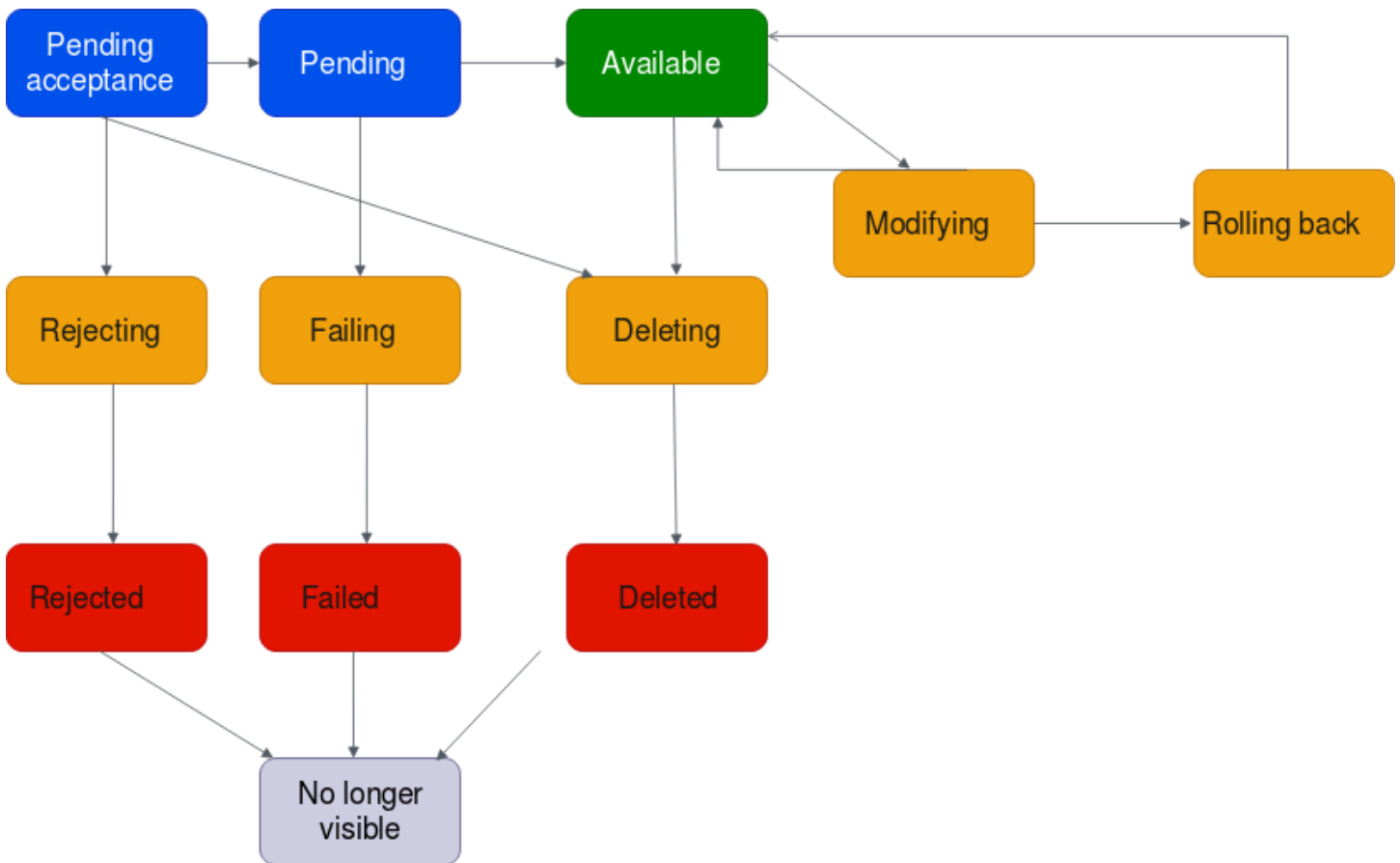
다음 다이어그램에서는 단일 계정 구성이나 공유 연결 자동 수락을 설정한 교차 계정 구성에서 연결이 진행될 수 있는 상태를 보여줍니다.



- 대기 중: VPC 연결에 대한 요청이 시작되어 프로비저닝 프로세스 중입니다. 이 단계에서 연결은 실패하거나 available로 이동할 수 있습니다.
- 실패 중: VPC 연결에 대한 요청의 실패가 처리 중입니다. 이 단계에서 VPC 연결은 failed로 이동합니다.
- 실패: VPC 연결에 대한 요청이 실패했습니다. 이 상태에서는 삭제할 수 없습니다. 실패한 VPC 연결은 2시간 동안 표시된 후에 사라집니다.

- 사용 가능: VPC 연결이 사용 가능하며, 트래픽이 VPC와 전송 게이트웨이 간에 전송될 수 있습니다. 이 단계에서 연결은 `modifying` 또는 `deleting`으로 이동할 수 있습니다.
- 삭제: VPC 연결이 삭제되고 있습니다. 이 단계에서 연결은 `deleted`로 이동할 수 있습니다.
- 삭제: `available` VPC 연결이 삭제되었습니다. 이 상태에서는 VPC 연결을 수정할 수 없습니다. VPC 연결은 2시간 동안 표시된 후에 사라집니다.
- 수정 중: VPC 연결의 속성을 수정하라는 요청을 제출했습니다. 이 단계에서 연결은 `available` 또는 `rolling back`으로 이동할 수 있습니다.
- 롤백 중: VPC 연결 요청을 완료할 수 없으며, 시스템에서 변경된 내용을 실행 취소합니다. 이 단계에서 연결은 `available`로 이동할 수 있습니다.

다음 다이어그램에서는 공유 연결 자동 수락이 해제되어 있는 교차 계정 구성에서 연결이 진행될 수 있는 상태를 보여줍니다.



- 수락 대기 중: VPC 연결 요청이 수락을 기다리고 있습니다. 이 단계에서 연결은 `pending`, `rejecting` 또는 `deleting`으로 이동할 수 있습니다.

- 거부 중: VPC 연결의 거부가 처리되고 있습니다. 이 단계에서 연결은 `rejected`로 이동할 수 있습니다.
- 거부: `pending acceptance` VPC 연결이 거부되었습니다. 이 상태에서는 VPC 연결을 수정할 수 없습니다. VPC 연결은 2시간 동안 표시된 후에 사라집니다.
- 대기 중: VPC 연결이 수락되었으며 프로비저닝 프로세스 중입니다. 이 단계에서 연결은 실패하거나 `available`로 이동할 수 있습니다.
- 실패 중: VPC 연결에 대한 요청의 실패가 처리 중입니다. 이 단계에서 VPC 연결은 `failed`로 이동합니다.
- 실패: VPC 연결에 대한 요청이 실패했습니다. 이 상태에서는 삭제할 수 없습니다. 실패한 VPC 연결은 2시간 동안 표시된 후에 사라집니다.
- 사용 가능: VPC 연결이 사용 가능하며, 트래픽이 VPC와 전송 게이트웨이 간에 전송될 수 있습니다. 이 단계에서 연결은 `modifying` 또는 `deleting`으로 이동할 수 있습니다.
- 삭제: VPC 연결이 삭제되고 있습니다. 이 단계에서 연결은 `deleted`로 이동할 수 있습니다.
- 삭제: `available` 또는 `pending acceptance` VPC 연결이 삭제되었습니다. 이 상태에서는 VPC 연결을 수정할 수 없습니다. VPC 연결은 2시간 동안 표시된 후에 사라집니다.
- 수정 중: VPC 연결의 속성을 수정하라는 요청을 제출했습니다. 이 단계에서 연결은 `available` 또는 `rolling back`으로 이동할 수 있습니다.
- 롤백 중: VPC 연결 요청을 완료할 수 없으며, 시스템에서 변경된 내용을 실행 취소합니다. 이 단계에서 연결은 `available`로 이동할 수 있습니다.

VPC에 대한 Transit Gateway Attachment 생성

콘솔을 사용하여 VPC 연결을 생성하려면

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway Attachments를 선택합니다.
3. Transit Gateway Attachment 생성(Create transit gateway attachment)을 선택합니다.
4. (선택 사항) 이름 태그(Name tag)에 Transit Gateway Attachment의 이름을 입력합니다.
5. Transit gateway ID에서 연결에 사용할 Transit Gateway를 선택합니다. 소유한 Transit Gateway나 공유하는 Transit Gateway를 선택하면 됩니다.
6. 연결 유형(Attachment type)에서 VPC를 선택합니다.
7. DNS 지원, IPv6 지원 및 어플라이언스 모드 지원을 활성화할지 여부를 선택합니다.

어플라이언스 모드를 선택한 경우 소스와 대상 간의 트래픽 흐름은 해당 흐름의 수명 기간 동안 VPC 연결에 대해 동일한 가용 영역을 사용합니다.

8. VPC ID에서 Transit Gateway에 연결할 VPC를 선택합니다.

이 VPC에는 적어도 하나의 서브넷이 연결되어 있어야 합니다.

9. 서브넷 ID에서 트래픽을 라우팅하기 위해 Transit Gateway에서 사용할 각 가용 영역에 대해 하나의 서브넷을 선택합니다. 하나 이상의 서브넷을 선택해야 합니다. 가용 영역당 서브넷 한 개만 선택할 수 있습니다.
10. Transit Gateway Attachment 생성(Create Transit Gateway attachment)을 선택합니다.

를 사용하여 VPC 첨부 파일을 만들려면 AWS CLI

[create-transit-gateway-vpc-attach](#) 명령을 사용합니다.

VPC 연결 수정

콘솔을 사용하여 VPC 연결 수정

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway Attachments를 선택합니다.
3. VPC 연결을 선택한 다음 작업(Actions), Transit Gateway Attachment 수정(Modify transit gateway attachment)을 선택합니다.
4. DNS 지원을 활성화하려면 DNS support(DNS 지원)를 선택합니다.
5. 서브넷을 연결에 추가하려면 서브넷 옆에 있는 확인란을 선택합니다.

VPC 연결 서브넷을 추가하거나 수정하면 연결이 수정 상태에 있는 동안 데이터 트래픽에 영향을 줄 수 있습니다.

6. Transit Gateway Attachment 수정(Modify transit gateway attachment)을 선택합니다.

를 사용하여 VPC 첨부 파일을 수정하려면 AWS CLI

[modify-transit-gateway-vpc-attach](#) 명령을 사용합니다.

VPC 연결 태그 수정

콘솔을 사용하여 VPC 연결 태그 수정

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway Attachments를 선택합니다.
3. VPC 연결을 선택한 다음 작업(Actions), 태그 관리(Manage tags)를 선택합니다.
4. [태그 추가] 새 태그 추가를 선택하고 다음을 수행합니다.
 - 키에서 키 이름을 입력합니다.
 - 값에 키 값을 입력합니다.
5. [태그 제거] 태그 옆에 있는 제거를 선택합니다.
6. Save를 선택합니다.

VPC 연결 태그는 콘솔로만 수정할 수 있습니다.

VPC 연결 보기

콘솔을 사용하여 VPC 연결 보기

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway Attachments를 선택합니다.
3. 리소스 유형(Resource type) 열에서 VPC를 찾습니다. 이것이 VPC 연결입니다.
4. 세부 정보를 볼 연결을 선택합니다.

를 사용하여 VPC 첨부 파일을 보려면 AWS CLI

[describe-transit-gateway-vpc-attach](#) 명령을 사용합니다.

VPC 연결 삭제

콘솔을 사용하여 VPC 연결 삭제

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway Attachments를 선택합니다.
3. VPC 연결을 선택합니다.

4. 작업(Actions), Transit Gateway Attachment 삭제>Delete transit gateway attachment)를 선택합니다.
5. 메시지가 표시되면 **delete**를 입력한 후 삭제>Delete)를 선택합니다.

를 사용하여 VPC 첨부 파일을 삭제하려면 AWS CLI

[delete-transit-gateway-vpc-attach 명령을 사용합니다.](#)

VPC 연결 생성 문제 해결

다음 주제는 VPC 연결을 생성할 때 발생할 수 있는 문제를 해결하는 데 도움이 될 수 있습니다.

문제

VPC 연결에 실패했습니다.

원인

원인은 다음 중 하나일 수 있습니다.

1. VPC 연결을 생성하는 사용자에게 서비스 연결 역할을 생성할 수 있는 올바른 권한이 없습니다.
2. IAM 요청이 너무 많아 조절 문제가 발생했습니다. 예를 들어, AWS CloudFormation 을 사용하여 권한 및 역할을 생성하는 경우입니다.
3. 계정에 서비스 연결 역할이 있고 서비스 연결 역할이 수정되었습니다.
4. 전송 게이트웨이가 available 상태가 아닙니다.

Solution

원인에 해당하는 다음 작업을 수행하세요.

1. 사용자에게 서비스 연결 역할을 생성할 수 있는 올바른 권한이 있는지 확인합니다. 자세한 내용은 IAM 사용 설명서의 [서비스 연결 역할 권한](#)을 참조하세요. 사용자에게 권한이 부여되면 VPC 연결을 생성합니다.
2. 콘솔 또는 API를 통해 수동으로 VPC 연결을 생성합니다. 자세한 정보는 [the section called “VPC에 대한 Transit Gateway Attachment 생성”](#)을 참조하세요.
3. 서비스 연결 역할의 사용 권한이 올바른지 확인합니다. 자세한 정보는 [the section called “Transit Gateway”](#)을 참조하세요.

4. 전송 게이트웨이가 available 상태인지 확인합니다. 자세한 정보는 [the section called “Transit Gateway 보기”](#)을 참조하세요.

Transit Gateway VPN 연결

Transit Gateway에 VPN 연결을 연결하려면 고객 게이트웨이를 지정해야 합니다. 고객 게이트웨이 디바이스 요구 사항에 대한 자세한 정보는 AWS Site-to-Site VPN 사용 설명서의 [고객 게이트웨이 디바이스 요구 사항](#)을 참조하세요.

정적 VPN의 경우 Transit Gateway 라우팅 테이블에 정적 경로를 추가합니다.

VPN에 대한 Transit Gateway Attachment 생성

콘솔을 사용하여 VPN 연결 생성

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway Attachments를 선택합니다.
3. Transit Gateway Attachment 생성(Create transit gateway attachment)을 선택합니다.
4. Transit gateway ID에서 연결에 사용할 Transit Gateway를 선택합니다. 소유한 Transit Gateway를 선택할 수 있습니다.
5. Attachment type(연결 유형)에서 VPN을 선택합니다.
6. 고객 게이트웨이에서 다음 중 하나를 수행합니다.

- 기존 고객 게이트웨이를 사용하려면 기존을 선택한 다음 사용할 게이트웨이를 선택합니다.

고객 게이트웨이가 NAT-T(NAT traversal)를 지원하는 NAT(Network Address Translation) 디바이스 뒤에 상주하는 경우 NAT 디바이스의 퍼블릭 IP 주소를 사용하고 UDP 포트 4500 차단을 해제하도록 방화벽 규칙을 수정합니다.

- 고객 게이트웨이를 생성하려면 새로 만들기를 선택한 다음 IP Address(IP 주소)에 대해 정적 퍼블릭 IP 주소 및 BGP ASN을 입력합니다.

라우팅 옵션에서 동적 또는 정적을 선택합니다. 자세한 내용은 AWS Site-to-Site VPN 사용 설명서의 [Site-to-Site VPN 라우팅 옵션](#)을 참조하세요.

7. 터널 옵션(Tunnel Options)에 터널에 사용할 CIDR 범위와 사전 공유 키를 입력합니다. 자세한 내용은 [Site-to-Site VPN 아키텍처](#)를 참조하세요.
8. Transit Gateway Attachment 생성(Create transit gateway attachment)을 선택합니다.

를 사용하여 VPN 첨부 파일을 만들려면 AWS CLI

[create-vpn-connection](#) 명령을 사용합니다.

VPN 연결 보기

콘솔을 사용하여 VPN 연결을 보려면

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway Attachments를 선택합니다.
3. 리소스 유형(Resource type) 열에서 VPN을 찾습니다. 이것이 VPN 연결입니다.
4. 세부 정보를 보거나 태그를 추가할 연결을 선택합니다.

를 사용하여 VPN 첨부 파일을 보려면 AWS CLI

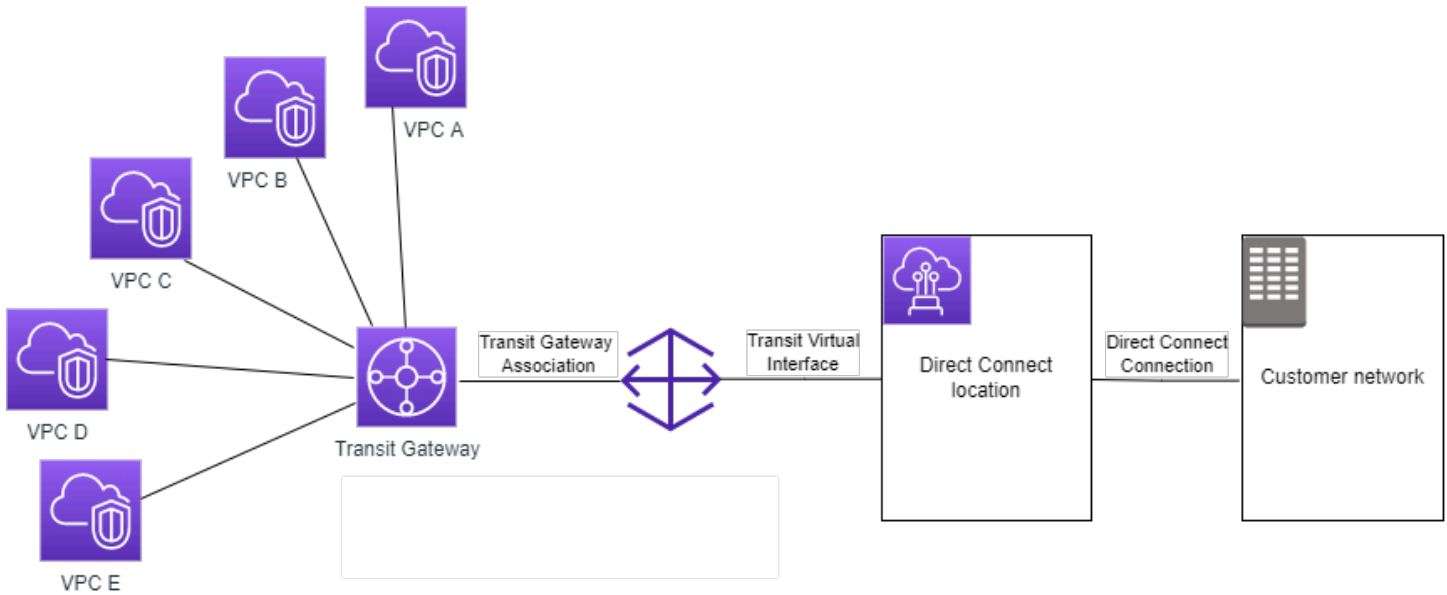
[describe-transit-gateway-attachments](#) 명령을 사용합니다.

Direct Connect 게이트웨이에 Transit Gateway 연결

전송 가상 인터페이스를 사용하여 Transit Gateway를 Direct Connect 게이트웨이에 연결합니다. 이 구성을 사용하면 다음과 같은 이점이 있습니다. 다음을 할 수 있습니다.

- 동일한 리전에 있는 여러 VPC 또는 VPN에 대한 단일 연결을 관리합니다.
- 온프레미스에서 AWS로, AWS에서 온프레미스로 접두사를 공급합니다.

다음 다이어그램에서는 Direct Connect 게이트웨이를 사용하여 모든 VPC에서 사용할 수 있는 Direct Connect 연결에 대한 단일 연결을 만드는 방법을 보여줍니다.



이 솔루션에는 다음 구성 요소가 포함됩니다.

- Transit Gateway.
- Direct Connect 게이트웨이
- Direct Connect 게이트웨이와 Transit Gateway의 연결
- Direct Connect 게이트웨이에 연결되는 전송 가상 인터페이스

Transit Gateway를 이용한 Direct Connect 게이트웨이 구성에 관한 자세한 내용은 AWS Direct Connect 사용 설명서의 [Transit Gateway 연결](#)을 참조하세요.

Transit Gateway 피어링 연결

리전 내 및 리전 간 전송 게이트웨이를 모두 피어링하고 둘 사이에서 IPv4 및 IPv6 트래픽을 포함한 트래픽을 라우팅할 수 있습니다. 이렇게 하려면 Transit Gateway에서 피어링 연결을 생성하고 Transit Gateway를 지정해야 합니다. 피어 Transit Gateway는 사용자 계정 또는 다른 AWS 계정에 있을 수 있습니다.

피어링 연결 요청을 생성한 후에는 피어 Transit Gateway의 소유자(수락자 Transit Gateway라고도 함)가 요청을 수락해야 합니다. Transit Gateway 간에 트래픽을 라우팅하려면 Transit Gateway 피어링 연결을 가리키는 Transit Gateway 라우팅 테이블에 정적 경로를 추가합니다.

향후 경로 전파 기능을 활용하려면 각각의 피어링된 Transit Gateway에 고유한 ASN을 사용하는 것이 좋습니다.

Transit Gateway 피어링은 다른 리전의 Amazon Route 53 Resolver를 사용하여 Transit Gateway 피어링 연결의 양쪽에 있는 VPC에서 퍼블릭 또는 프라이빗 IPv4 DNS 호스트 이름을 프라이빗 IPv4 주소로 확인하는 것을 지원하지 않습니다. Route 53 Resolver에 대한 자세한 내용은 Amazon Route 53 개발자 안내서의 [Route 53 Resolver란 무엇인가요?](#) 단원을 참조하세요.

리전 간 게이트웨이 피어링은 VPC 피어링과 동일한 네트워크 인프라를 사용합니다. 따라서 트래픽은 리전 간에 이동할 때 가상 네트워크 계층에서 AES-256 암호화를 사용하여 암호화됩니다. 트래픽은 AWS의 물리적 제어 범위를 벗어나는 네트워크 링크를 통과할 때에도 물리적 계층에서 AES-256 암호화를 사용하여 암호화됩니다. 결과적으로 트래픽은 AWS의 물리적 제어 범위를 벗어나는 네트워크 링크에서 이중 암호화됩니다. 동일한 리전 내에서 트래픽은 AWS의 물리적 제어 범위를 벗어나는 네트워크 링크를 통과할 때에만 물리적 계층에서 암호화됩니다.

Transit Gateway 피어링 연결을 지원하는 리전에 대한 자세한 내용은 [AWS Transit Gateways FAQ](#)를 참조하세요.

피어링 연결 생성

시작하기 전에 연결할 Transit Gateway의 ID가 있는지 확인합니다. Transit Gateway가 다른 AWS 계정에 있는 경우 Transit Gateway 소유자의 AWS 계정 ID가 있어야 합니다.

피어링 연결을 생성한 후 수락자 Transit Gateway의 소유자가 연결 요청을 수락해야 합니다.

콘솔을 사용하여 피어링 연결 생성

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway Attachments를 선택합니다.
3. Transit Gateway Attachment 생성(Create transit gateway attachment)을 선택합니다.
4. Transit gateway ID에서 연결에 사용할 Transit Gateway를 선택합니다. 소유한 Transit Gateway나 공유하는 Transit Gateway를 선택하면 됩니다.
5. 연결 유형(Attachment type)에서 피어링 연결(Peering Connection)을 선택합니다.
6. 선택적으로 연결에 대한 이름 태그를 입력합니다.
7. 계정(Account)에서 다음 중 하나를 수행합니다.
 - Transit Gateway가 계정에 있는 경우 내 계정(My account)을 선택합니다.
 - Transit Gateway가 다른 AWS 계정에 있는 경우 기타 계정(Other account)을 선택합니다. [계정 ID(Account ID)]에 AWS 계정 ID를 입력합니다.
8. 리전(Region)에서 Transit Gateway가 위치한 리전을 선택합니다.

9. Transit Gateway(수락자)(Transit gateway (accepter))에 연결할 Transit Gateway의 ID를 입력합니다.
10. Transit Gateway Attachment 생성(Create Transit Gateway attachment)을 선택합니다.

AWS CLI를 사용하여 피어링 연결 생성

[create-transit-gateway-peering-attachment](#) 명령을 사용합니다.

피어링 연결 요청 수락 또는 거부

피어링 연결을 활성화하려면 수락자 Transit Gateway의 소유자가 피어링 연결 요청을 수락해야 합니다. 두 Transit Gateway가 동일한 계정에 있는 경우에도 이 작업이 필요합니다. 피어링 연결은 pendingAcceptance 상태에 있어야 합니다. 수락자 Transit Gateway가 있는 리전의 피어링 연결 요청을 수락합니다.

또는 pendingAcceptance 상태로 받은 피어링 연결 요청을 거부할 수 있습니다. 수락자 Transit Gateway가 있는 리전에서 요청을 거부해야 합니다.

콘솔을 사용하여 피어링 연결 요청 수락

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway Attachments를 선택합니다.
3. 수락 보류 중인 Transit Gateway 피어링 연결을 선택합니다.
4. 작업(Actions), Transit Gateway Attachment 수락(Accept Transit Gateway attachment)을 선택합니다.
5. Transit Gateway 라우팅 테이블에 정적 경로를 추가합니다. 자세한 내용은 [the section called “정적 경로 생성”](#) 단원을 참조하세요.

콘솔을 사용하여 피어링 연결 요청 거부

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway Attachments를 선택합니다.
3. 수락 보류 중인 Transit Gateway 피어링 연결을 선택합니다.
4. 작업(Actions), Transit Gateway Attachment 거부(Reject Transit Gateway attachment)를 선택합니다.

AWS CLI를 사용하여 피어링 연결을 수락 또는 거부

[accept-transit-gateway-peering-attachment](#) 및 [reject-transit-gateway-peering-attachment](#) 명령을 사용합니다.

Transit Gateway 라우팅 테이블에 경로 추가

피어링된 Transit Gateway 간에 트래픽을 라우팅하려면 Transit Gateway 피어링 연결을 가리키는 Transit Gateway 라우팅 테이블에 정적 경로를 추가해야 합니다. 수락자 Transit Gateway의 소유자는 Transit Gateway의 라우팅 테이블에 정적 경로도 추가해야 합니다.

콘솔을 사용하여 정적 경로 생성

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway Route Tables(전송 게이트웨이 라우팅 테이블)를 선택합니다.
3. 경로를 생성할 라우팅 테이블을 선택합니다.
4. Actions(작업), 정적 경로 생성(Create static route)을 선택합니다.
5. 정적 경로 생성(Create static route) 페이지에 경로를 생성할 CIDR 블록을 입력합니다. 예를 들어 피어 Transit Gateway에 연결된 VPC의 CIDR 블록을 지정합니다.
6. 해당 경로에 대한 피어링 연결을 선택합니다.
7. 정적 경로 생성(Create static route)을 선택합니다.

AWS CLI을 사용하여 정적 경로 생성

[create-transit-gateway-route](#) 명령을 사용합니다.

Important

라우팅을 생성한 후 Transit Gateway 라우팅 테이블을 Transit Gateway 피어링 연결과 연결합니다. 자세한 내용은 [the section called “Transit Gateway 라우팅 테이블 연결”](#) 단원을 참조하세요.

Transit Gateway 피어링 연결 보기

Transit Gateway 피어링 연결 및 해당 연결에 대한 정보를 볼 수 있습니다.

콘솔을 사용하여 피어링 연결 보기

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway Attachments를 선택합니다.
3. 리소스 유형(Resource type) 열에서 피어링(Peering)을 찾습니다. 이것이 피어링 연결입니다.
4. 세부 정보를 볼 연결을 선택합니다.

AWS CLI를 사용하여 Transit Gateway 피어링 연결 보기

[describe-transit-gateway-peering-attachments](#) 명령을 사용합니다.

피어링 연결 삭제

Transit Gateway 피어링 연결을 삭제할 수 있습니다. Transit Gateway의 소유자가 연결을 삭제할 수 있습니다.

콘솔을 사용하여 피어링 연결 삭제

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway Attachments를 선택합니다.
3. Transit Gateway 피어링 연결을 선택합니다.
4. 작업(Actions), Transit Gateway Attachment 삭제>Delete transit gateway attachment)를 선택합니다.
5. **delete**를 입력한 다음 삭제>Delete)를 선택합니다.

AWS CLI를 사용하여 피어링 연결 삭제

[delete-transit-gateway-peering-attachment](#) 명령을 사용합니다.

옵트인 AWS 리전 고려 사항

옵트인 리전 경계를 넘어 Transit Gateway를 피어링할 수 있습니다. 이러한 리전 관련 정보와 옵트인 방법에 대한 자세한 내용은 Amazon Web Services 일반 참조의 [AWS 리전 관리](#)를 참조하세요. 이러한 리전에서 Transit Gateway 피어링을 사용할 때 다음 사항을 고려합니다.

- 피어링 연결을 수락한 계정이 해당 리전으로 옵트인한다면 옵트인 리전으로 피어링할 수 있습니다.
- 리전 옵트인 상태와 관계없이 AWS는 피어링 연결을 수락한 계정과 다음 계정 데이터를 공유합니다.

- AWS 계정 ID
- Transit Gateway ID
- 리전 코드
- Transit Gateway Attachment를 삭제하면 위의 계정 데이터가 삭제됩니다.
- 따라서 리전을 옵트아웃하기 전에 Transit Gateway 피어링 연결을 삭제하는 것이 좋습니다. 피어링 연결을 삭제하지 않으면 트래픽이 해당 연결을 통해 계속 전달되어 요금이 계속 발생할 수 있습니다. 연결을 삭제하지 않은 경우 다시 옵트인하고 연결을 삭제할 수 있습니다.
- 일반적으로 Transit Gateway에는 발신자 지불 모델이 있습니다. 옵트인 경계를 지나는 Transit Gateway 피어링 연결을 사용하면 옵트인하지 않은 리전을 포함하여 연결을 수락하는 리전에서 요금이 발생할 수 있습니다. 자세한 내용은 [AWS Transit Gateway 요금](#)을 참조하세요.

Transit Gateway Connect 연결 및 Transit Gateway Connect 피어

Transit Gateway Connect 연결을 생성하여 VPC에서 실행 중인 전송 게이트웨이와 서드 파티 가상 어플라이언스(예: SD-WAN 어플라이언스) 간에 연결을 설정할 수 있습니다. Connect 연결은 고성능을 위한 일반 라우팅 캡슐화(GRE) 터널 프로토콜과 동적 경로를 위한 경계 게이트웨이 프로토콜(BGP)을 지원합니다. Connect 연결을 생성한 후 Connect 연결에 하나 이상의 GRE 터널(Transit Gateway Connect 피어라고도 함)을 생성하여 Transit Gateway 및 서드 파티 어플라이언스를 연결할 수 있습니다. GRE 터널을 통해 두 BGP 세션을 설정하여 라우팅 정보를 교환합니다.

Important

Transit Gateway Connect 피어는 AWS-관리형 인프라에서 종료되는 두 개의 BGP 피어링 세션으로 구성됩니다. 두 개의 BGP 피어링 세션은 라우팅 플레인 중복성을 제공하여 하나의 BGP 피어링 세션이 손실되어도 라우팅 작업에 영향을 미치지 않도록 합니다. 두 BGP 세션에서 수신된 라우팅 정보는 지정된 Connect 피어에 대해 누적됩니다. 2개의 BGP 피어링 세션은 또한 일상적인 유지 관리, 패치 적용, 하드웨어 업그레이드 및 교체와 같은 모든 AWS 인프라 작업으로부터 보호합니다. Connect 피어가 이중화에 대해 구성된 권장 이중 BGP 피어링 세션 없이 작동하는 경우 AWS 인프라 작업 중에 연결이 일시적으로 끊길 수 있습니다. Connect 피어에서 두 BGP 피어링 세션을 모두 구성하는 것이 좋습니다. 어플라이언스 측에서고가용성을 지원하도록 여러 Connect 피어를 구성한 경우 각 Connect 피어에서 두 BGP 피어링 세션을 모두 구성하는 것이 좋습니다.

Connect 연결에서는 기존 VPC 또는 Direct Connect 연결을 기본 전송 메커니즘으로 사용합니다. 이를 전송 연결이라고 합니다. Transit Gateway는 서드 파티 어플라이언스에서 일치하는 GRE 패킷을

Connect 연결의 트래픽으로 식별합니다. 또한 소스 또는 대상 정보가 잘못된 GRE 패킷을 포함하여 다른 모든 패킷을 전송 연결의 트래픽으로 처리합니다.

Note

Attachment를 전송 메커니즘으로 사용하려면 우선 Direct Connect를 AWS Transit Gateway와 통합해야 합니다. 이 통합을 만드는 단계는 [SD-WAN 디바이스를 AWS Transit Gateway 및 AWS Direct Connect와\(과\) 통합](#)을 참조하세요.

내용

- [Connect 피어](#)
- [요구 사항 및 고려 사항](#)
- [Connect 연결을 생성합니다](#)
- [Connect 피어\(GRE 터널\) 생성](#)
- [Connect 연결 및 Connect 피어 보기](#)
- [Connect 연결 및 Connect 피어 태그 수정](#)
- [Connect 피어 삭제](#)
- [Connect 연결을 삭제합니다](#)

Connect 피어

Connect 피어(GRE 터널)는 다음과 같은 구성 요소로 이루어집니다.

내부 CIDR 블록(BGP 주소)

BGP 피어링에 사용되는 내부 IP 주소입니다. IPv4의 169.254.0.0/16 범위에서 /29 CIDR 블록을 지정해야 합니다. 선택적으로 IPv6의 fd00::/8 범위에서 /125 CIDR 블록을 지정할 수 있습니다. 다음 CIDR 블록은 예약되어 사용할 수 없습니다.

- 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

어플라이언스에서 IPv4 범위의 첫 번째 주소를 BGP IP 주소로 구성해야 합니다. IPv6을 사용할 때 내부 CIDR 블록이 fd00::/125인 경우 어플라이언스의 터널 인터페이스에서 이 범위(fd00::1)의 첫 번째 주소를 구성해야 합니다.

BGP 주소는 Transit Gateway의 모든 터널에서 고유해야 합니다.

피어 IP 주소

Connect 피어의 어플라이언스 측에 있는 피어 IP 주소(GRE 외부 IP 주소)입니다. 모든 IP 주소가 될 수 있습니다. IP 주소는 IPv4 또는 IPv6 주소일 수 있지만 Transit Gateway 주소와 동일한 IP 주소 패밀리여야 합니다.

Transit Gateway 주소

Connect 피어의 전송 게이트웨이 측에 있는 피어 IP 주소(GRE 외부 IP 주소)입니다. IP 주소는 Transit Gateway CIDR 블록에서 지정되어야 하며 Transit Gateway의 Connect 연결 간에서 고유해야 합니다. IP 주소를 지정하지 않으면 Transit Gateway CIDR 블록에서 사용 가능한 첫 번째 주소를 사용합니다.

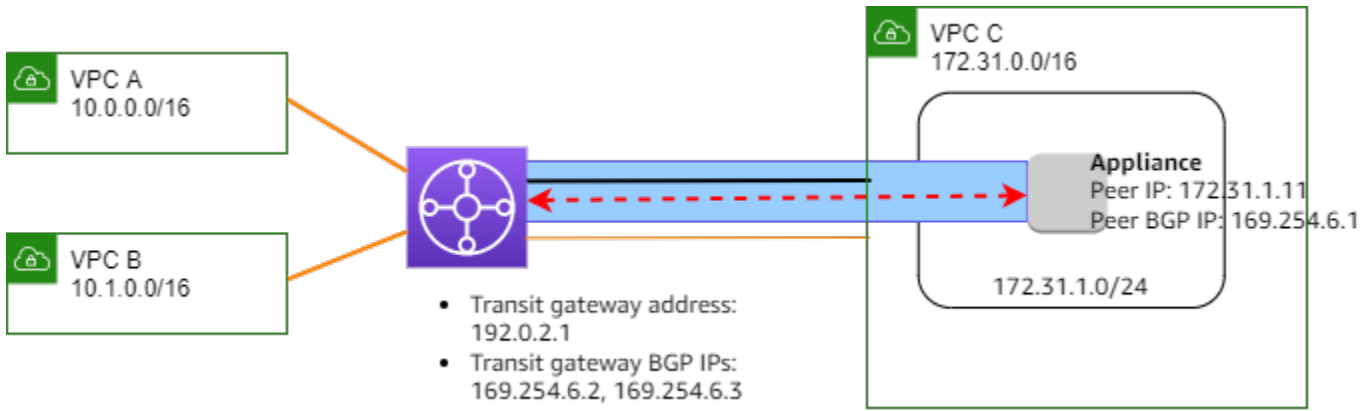
Transit Gateway를 [생성](#)하거나 [수정](#)할 때 Transit Gateway CIDR 블록을 추가할 수 있습니다.



IP 주소는 IPv4 또는 IPv6 주소일 수 있지만 피어 IP 주소와 동일한 IP 주소 패밀리여야 합니다.

피어 IP 주소와 Transit Gateway 주소는 GRE 터널을 고유하게 식별하는 데 사용됩니다. 두 주소 중 하나를 여러 터널에서 다시 사용할 수 있지만 동일한 터널에서 둘 다 사용할 수는 없습니다.

BGP 피어링용 Transit Gateway Connect는 IPv6 유니캐스트용 BGP 세션을 설정하려면 IPv4 유니캐스트 주소 지정이 필요한 Multiprotocol BGP(MP-BGP)만 지원합니다. GRE 외부 IP 주소에는 IPv4 및 IPv6 주소를 모두 사용할 수 있습니다.

다음 예에서는 VPC의 Transit Gateway 및 어플라이언스 간의 Connect 연결을 보여 줍니다.



다이어그램 구성 요소	Description
	VPC 연결
	Connect 연결
	GRE 터널(Connect 피어)
	BGP 피어링 세션

이전 예에서는 기존 VPC 연결(전송 연결)에 Connect 연결이 생성됩니다. Connect 연결에 Connect 피어가 생성되어 VPC의 어플라이언스에 대한 연결을 설정합니다. Transit Gateway 주소는 192.0.2.1이고 BGP 주소의 범위는 169.254.6.0/29입니다. 범위(169.254.6.1)의 첫 번째 IP 주소는 어플라이언스에서 피어 BGP IP 주소로 구성됩니다.

VPC C의 서브넷 라우팅 테이블에는 Transit Gateway CIDR 블록으로 향하는 트래픽을 Transit Gateway로 전달되게 하는 경로가 있습니다.

대상 주소	대상
172.31.0.0/16	로컬
192.0.2.0/24	tgw-id

요구 사항 및 고려 사항

다음은 Connect 연결에 대한 요구 사항 및 고려 사항입니다.

- Connect 연결을 지원하는 리전에 대한 자세한 내용은 [AWS Transit Gateway FAQ](#)를 참조하세요.
- 서드 파티 어플라이언스는 Connect 연결을 사용하여 Transit Gateway와 주고 받는 트래픽을 GRE 터널을 통해 보내고 받도록 구성해야 합니다.
- 서드 파티 어플라이언스는 동적 경로 업데이트 및 상태 확인에 BGP를 사용하도록 구성해야 합니다.
- 다음과 같은 유형의 BGP가 지원됩니다.
 - 외부 BGP(eBGP): Transit Gateway와 다른 자율 시스템에 있는 라우터에 연결하는 데 사용됩니다. eBGP를 사용하는 경우 TTL(Time-to-Live) 값이 2인 ebgp-multihop을 구성해야 합니다.
 - 내부 BGP(iBGP): Transit Gateway와 동일한 자율 시스템에 있는 라우터에 연결하는 데 사용됩니다. 경로가 eBGP 피어에서 시작되어 next-hop-self를 구성해야 하는 경우가 아니면 Transit Gateway는 iBGP 피어(서드 파티 어플라이언스)에서 경로를 설치하지 않습니다. 서드 파티 어플라이언스가 iBGP 피어링을 통해 제공하는 경로에는 ASN이 있어야 합니다.
 - MP-BGP(BGP용 다중 프로토콜 익스텐션): IPv4 및 IPv6 주소 패밀리와 같은 여러 프로토콜 유형을 지원하는 데 사용됩니다.
- 기본 BGP 연결 유지 시간제한은 10초이고 기본 대기 타이머는 30초입니다.
- IPv6 BGP 피어링은 지원되지 않으며 IPv4 기반 BGP 피어링만 지원됩니다. IPv6 접두사는 MP-BGP를 사용하여 IPv4 BGP 피어링을 통해 교환됩니다.
- BFD(Bidirectional Detection)는 지원되지 않습니다.
- BGP의 정상적인 재시작이 지원되지 않습니다.
- Transit Gateway 피어를 생성할 때 피어 ASN 번호를 지정하지 않으면 자동으로 Transit Gateway ASN 번호가 선택됩니다. 즉, 어플라이언스와 Transit Gateway가 iBGP를 수행하는 동일한 자율 시스템 안에 있어야 합니다.
- 두 개의 Connect 피어가 있는 경우 BGP AS-PATH 특성을 사용하는 Connect 피어가 기본 경로가 됩니다.

여러 어플라이언스 간에서 등가 다중 경로(ECMP) 라우팅을 사용하려면 BGP AS-PATH 속성이 같은 Transit Gateway에 동일한 접두사를 알리도록 어플라이언스를 구성해야 합니다. Transit Gateway가 사용 가능한 모든 ECMP 경로를 선택하려면 AS-PATH 및 자율 시스템 번호(ASN)가 일치해야 합니다. 전송 게이트웨이는 동일한 Connect 연결의 Connect 피어 사이 또는 동일한 전송 게이트웨이의 Connect 연결 사이에서 ECMP를 사용할 수 있습니다. Transit Gateway는 단일 피어가 설정하는 중복 BGP 피어링 사이에 ECMP를 사용할 수 없습니다.

- Connect 연결을 사용하면 라우팅이 기본적으로 Transit Gateway 라우팅 테이블에 전파됩니다.
- 정적 경로는 지원되지 않습니다.
- 타사 어플라이언스 외부 인터페이스(터널 소스) MTU(최대 전송 단위)가 다음 중 하나인지 확인하세요.
 - GRE 터널 인터페이스의 MTU와 일치하거나
 - GRE 터널 인터페이스보다 커야 합니다.

Connect 연결을 생성합니다

Connect 연결을 생성하려면 기존 연결을 전송 연결로 지정해야 합니다. VPC 연결 또는 Direct Connect 연결을 전송 연결로 지정할 수 있습니다.

콘솔을 사용하여 Connect 연결 생성

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway Attachment를 선택합니다.
3. Transit Gateway Attachment 생성을 선택합니다.
4. (선택 사항) 이름 태그(Name tag)에 연결의 이름 태그를 지정합니다.
5. Transit gateway ID에서 연결에 사용할 Transit Gateway를 선택합니다.
6. 연결 유형(Attachment type)에서 Connect를 선택합니다.
7. 전송 연결 ID(Transport Attachment ID)에서 기존 연결(전송 연결)의 ID를 선택합니다.
8. Transit Gateway Attachment 생성을 선택합니다.

AWS CLI를 사용하여 Connect 연결 생성

[create-transit-gateway-connect](#) 명령을 사용합니다.

Connect 피어(GRE 터널) 생성

기존 Connect 연결에 대한 Connect 피어(GRE 터널)를 생성할 수 있습니다. 시작하기 전에 Transit Gateway CIDR 블록을 구성했는지 확인합니다. Transit Gateway를 [생성](#)하거나 [수정](#)할 때 Transit Gateway CIDR 블록을 구성할 수 있습니다.

Connect 피어를 생성할 때 Connect 피어의 어플라이언스 측에서 GRE 외부 IP 주소를 지정해야 합니다.

콘솔을 사용하여 Connect 피어를 생성하려면

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway Attachment를 선택합니다.
3. Connect 연결을 선택하고 작업(Actions), Connect 피어 생성(Create Connect peer)을 선택합니다.
4. (선택 사항) 이름 태그(Name tag)에 Connect 피어의 이름 태그를 지정합니다.
5. (선택 사항) Transit Gateway GRE 주소(Transit gateway GRE Address)에 Transit Gateway의 GRE 외부 IP 주소를 지정합니다. 기본적으로 Transit Gateway CIDR 블록에서 사용 가능한 첫 번째 주소가 사용됩니다.
6. 피어 GRE 주소(Peer GRE Address)에 Connect 피어의 어플라이언스 측에 대한 GRE 외부 IP 주소를 지정합니다.
7. BGP 내부 CIDR 블록 IPv4(BGP Inside CIDR blocks IPv4)에 BGP 피어링에 사용되는 내부 IPv4 주소의 범위를 지정합니다. 169.254.0.0/16 범위에서 /29 CIDR 블록을 지정합니다.
8. (선택 사항) BGP 내부 CIDR 블록 IPv6(BGP Inside CIDR blocks IPv6)에 BGP 피어링에 사용되는 내부 IPv6 주소의 범위를 지정합니다. fd00::/8 범위에서 /125 CIDR 블록을 지정합니다.
9. (선택 사항) 피어 ASN(Peer ASN)에 어플라이언스의 경계 게이트웨이 프로토콜(BGP) 자율 시스템 번호(ASN)를 지정합니다. 네트워크에 할당된 기존 ASN을 사용할 수 있습니다. 해당 ASN이 없는 경우에는 64512–65534(16비트 ASN) 또는 4200000000–4294967294(32비트 ASN) 범위의 프라이빗 ASN을 사용할 수 있습니다.

기본값은 Transit Gateway와 동일한 ASN입니다. 피어 ASN을 Transit Gateway ASN(eBGP)과 다르게 구성하는 경우 TTL(Time-to-Live) 값이 2인 ebgp-multihop을 구성해야 합니다.

10. 커넥트 피어 생성(Create connect peer)을 선택합니다.

AWS CLI을(를) 사용하여 Connect 피어를 생성

[create-transit-gateway-connect-peer](#) 명령을 사용합니다.

Connect 연결 및 Connect 피어 보기

Connect 연결 및 Connect 피어를 볼 수 있습니다.

콘솔을 사용하여 Connect 연결 및 Connect 피어를 보려면

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway Attachment를 선택합니다.

3. Connect 연결을 선택합니다.
4. 연결의 Connect 피어를 보려면 Connect 피어(Connect Peers) 탭을 선택합니다.

AWS CLI을(를) 사용하여 Connect 연결 및 Connect 피어를 보려면

[describe-transit-gateway-connects](#) 및 [describe-transit-gateway-connect-peers](#) 명령을 사용합니다.

Connect 연결 및 Connect 피어 태그 수정

Connect 연결의 태그를 수정할 수 있습니다.

콘솔을 사용하여 Connect 연결 태그 수정

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway Attachment를 선택합니다.
3. Connect 연결을 선택한 다음 Actions(작업), 태그 관리(Manage tags)를 선택합니다.
4. 태그를 추가하려면 새 태그 추가(Add new tag)를 선택하고 키 이름 및 키 값을 지정합니다.
5. 태그를 제거하려면 제거(Remove)를 선택합니다.
6. 저장(Save)을 선택합니다.

Connect 피어의 태그를 수정할 수 있습니다.

콘솔을 사용하여 Connect 피어 태그를 수정하려면

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway Attachment를 선택합니다.
3. Connect 연결을 선택한 다음 Connect 피어(Connect peers)를 선택합니다.
4. Connect 피어를 선택한 다음 작업(Actions), 태그 관리(Manage tags)를 선택합니다.
5. 태그를 추가하려면 새 태그 추가(Add new tag)를 선택하고 키 이름 및 키 값을 지정합니다.
6. 태그를 제거하려면 제거(Remove)를 선택합니다.
7. 저장(Save)을 선택합니다.

AWS CLI을(를) 사용하여 Connect 연결 및 Connect 피어 태그를 수정하려면

[create-tags](#) 및 [delete-tags](#) 명령을 사용합니다.

Connect 피어 삭제

Connect 피어가 더 이상 필요하지 않으면 삭제할 수 있습니다.

콘솔을 사용하여 Connect 피어를 삭제하려면

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway Attachment를 선택합니다.
3. Connect 연결을 선택합니다.
4. Connect 피어(Connect Peers) 탭에서 Connect 피어를 선택하고 작업(Actions), Connect 피어 삭제>Delete Connect peer)를 선택합니다.

AWS CLI을(를) 사용하여 Connect peer 삭제

[delete-transit-gateway-connect-peer](#) 명령을 사용합니다.

Connect 연결을 삭제합니다

Connect 연결이 더 이상 필요하지 않으면 삭제할 수 있습니다. 먼저 연결의 Connect 피어를 삭제해야 합니다.

콘솔을 사용하여 Connect 연결 삭제

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway Attachment를 선택합니다.
3. Connect 연결을 선택한 다음 작업(Actions), Transit Gateway Attachment 삭제>Delete transit gateway attachment)를 선택합니다.
4. **delete**를 입력한 다음 삭제>Delete)를 선택합니다.

AWS CLI를 사용하여 Connect 연결 삭제

[delete-transit-gateway-connect](#) 명령을 사용합니다.

Transit Gateway 라우팅 테이블

전송 게이트웨이 라우팅 테이블을 사용하여 Transit Gateway Attachment의 라우팅을 구성합니다.

Transit Gateway 라우팅 테이블 생성

콘솔을 사용하여 Transit Gateway 라우팅 테이블 생성

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway Route Tables(전송 게이트웨이 라우팅 테이블)를 선택합니다.
3. Transit Gateway 라우팅 테이블 생성(Create Transit Gateway route table)을 선택합니다.
4. (선택 사항) 이름 태그에 전송 게이트웨이 라우팅 테이블의 이름을 입력합니다. 태그 키 '이름'이 있는 태그가 생성됩니다. 여기서 태그 값은 지정한 이름입니다.
5. Transit Gateway ID에서 라우팅 테이블에 대한 Transit Gateway를 선택합니다.
6. Transit Gateway 라우팅 테이블 생성(Create Transit Gateway route table)을 선택합니다.

를 사용하여 트랜짓 게이트웨이 라우팅 테이블을 만들려면 AWS CLI

[create-transit-gateway-route-table](#) 명령어를 사용합니다.

Transit Gateway 라우팅 테이블 보기

콘솔을 사용하여 Transit Gateway 라우팅 테이블 보기

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway Route Tables(전송 게이트웨이 라우팅 테이블)를 선택합니다.
3. (선택 사항) 특정 라우팅 테이블 또는 테이블 집합을 찾으려면 필터 필드에 이름, 키워드 또는 속성의 전체 또는 일부를 입력합니다.
4. 라우팅 테이블의 확인란을 선택하거나 해당 ID를 선택하여 연결, 전파, 경로 및 태그에 대한 정보를 표시합니다.

를 사용하여 트랜짓 게이트웨이 라우팅 테이블을 보려면 AWS CLI

[describe-transit-gateway-route-tables](#) 명령어를 사용하세요.

를 사용하여 트랜짓 게이트웨이 라우팅 테이블의 경로를 보려면 AWS CLI

[search-transit-gateway-routes](#) 명령어를 사용합니다.

를 사용하여 트랜짓 게이트웨이 라우팅 테이블의 경로 전파를 보려면 AWS CLI

[get-transit-gateway-route-table-propagations](#) 명령어를 사용하세요.

를 사용하여 트랜짓 게이트웨이 라우팅 테이블에 대한 연결을 보려면 AWS CLI

[get-transit-gateway-route-table-sociations](#) 명령어를 사용하세요.

Transit Gateway 라우팅 테이블 연결

전송 게이트웨이 라우팅 테이블에 Transit Gateway Attachment를 연결할 수 있습니다.

콘솔을 사용하여 Transit Gateway 라우팅 테이블 연결

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway Route Tables(전송 게이트웨이 라우팅 테이블)를 선택합니다.
3. 라우팅 테이블을 선택합니다.
4. 페이지의 하단에서 연결 탭을 선택합니다.
5. 연결 생성을 선택합니다.
6. 원하는 연결을 선택하고 연결 생성을 선택합니다.

를 사용하여 트랜짓 게이트웨이 라우팅 테이블을 연결하려면 AWS CLI

[associate-transit-gateway-route-table](#) 명령어를 사용합니다.

Transit Gateway 라우팅 테이블에 대한 연결 삭제

Transit Gateway Attachment와 전송 게이트웨이 라우팅 테이블의 연결을 해제할 수 있습니다.

콘솔을 사용하여 Transit Gateway 라우팅 테이블의 연결 해제

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway Route Tables(전송 게이트웨이 라우팅 테이블)를 선택합니다.
3. 라우팅 테이블을 선택합니다.
4. 페이지의 하단에서 연결 탭을 선택합니다.
5. 해제할 연결을 선택하고 연결 삭제를 선택합니다.
6. 확인 메시지가 나타나면 연결 삭제를 선택합니다.

를 사용하여 트랜짓 게이트웨이 라우팅 테이블의 연결을 끊으려면 AWS CLI

[disassociate-transit-gateway-route-table](#) 명령어를 사용합니다.

Transit Gateway 라우팅 테이블에 라우팅 전파

경로 전파를 사용하여 연결의 경로를 라우팅 테이블에 추가합니다.

Transit Gateway Attachment 라우팅 테이블에 경로 전파

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway Route Tables(전송 게이트웨이 라우팅 테이블)를 선택합니다.
3. 전파를 생성할 라우팅 테이블을 선택합니다.
4. 작업, Create propagation(전파 생성)을 선택합니다.
5. Create propagation(전파 생성) 페이지에서 연결을 선택합니다.
6. Create propagation(전파 생성)을 선택합니다.

를 사용하여 경로 전파를 활성화하려면 AWS CLI

[enable-transit-gateway-route-table-propagation](#) 명령을 사용합니다.

경로 전파 비활성화

라우팅 테이블 연결에서 전파 경로를 제거합니다.

콘솔을 사용하여 경로 전파 비활성화

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway Route Tables(전송 게이트웨이 라우팅 테이블)를 선택합니다.
3. 전파를 삭제할 라우팅 테이블을 선택합니다.
4. 페이지의 하단에서 Propagations(전파) 탭을 선택합니다.
5. 연결을 선택한 다음 Delete propagation(전파 삭제)을 선택합니다.
6. 확인 메시지가 나타나면 Delete propagation(전파 삭제)을 선택합니다.

를 사용하여 경로 전파를 비활성화하려면 AWS CLI

[disable-transit-gateway-route-table-propagation](#) 명령을 사용하십시오.

정적 경로 생성

VPC, VPN 또는 Transit Gateway 피어링 연결에 대한 정적 경로를 생성하거나 해당 경로와 일치하는 트래픽을 삭제하는 블랙홀 경로를 생성할 수 있습니다.

VPN 연결을 대상으로 하는 Transit Gateway 라우팅 테이블의 정적 경로는 Site-to-Site VPN을 기준으로 필터링되지 않습니다. 이렇게 하면 BGP-기반 VPN을 사용할 때 의도하지 않은 아웃바운드 트래픽 흐름이 허용될 수 있습니다.

콘솔을 사용하여 정적 경로 생성

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway Route Tables(전송 게이트웨이 라우팅 테이블)를 선택합니다.
3. 경로를 생성할 라우팅 테이블을 선택합니다.
4. Actions(작업), 정적 경로 생성(Create static route)을 선택합니다.
5. 정적 경로 생성(Create static route) 페이지에 라우팅을 생성할 CIDR 블록을 입력한 다음 활성(Active)을 선택합니다.
6. 경로에 대한 연결을 선택합니다.
7. 정적 경로 생성(Create static route)을 선택합니다.

콘솔을 사용하여 블랙홀 경로 생성

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway Route Tables(전송 게이트웨이 라우팅 테이블)를 선택합니다.
3. 경로를 생성할 라우팅 테이블을 선택합니다.
4. Actions(작업), 정적 경로 생성(Create static route)을 선택합니다.
5. 정적 경로 생성(Create static route) 페이지에 라우팅을 생성할 CIDR 블록을 입력한 다음 블랙홀(Blackhole)을 선택합니다.
6. 정적 경로 생성을 선택합니다.

를 사용하여 고정 경로 또는 블랙홀 경로를 만들려면 AWS CLI

[create-transit-gateway-route](#) 명령을 사용합니다.

정적 경로 삭제

Transit Gateway 라우팅 테이블에서 정적 경로를 삭제할 수 있습니다.

콘솔을 사용하여 정적 경로 삭제

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway Route Tables(전송 게이트웨이 라우팅 테이블)를 선택합니다.
3. 경로를 삭제할 라우팅 테이블을 선택하고 경로(Routes)를 선택합니다.
4. 삭제할 경로를 선택합니다.
5. 정적 경로 삭제>Delete static route)를 선택합니다.
6. 확인 상자에서 정적 경로 삭제>Delete static route)를 선택합니다.

를 사용하여 고정 경로를 삭제하려면 AWS CLI

[delete-transit-gateway-route](#) 명령을 사용합니다.

정적 경로 바꾸기

전송 게이트웨이 라우팅 테이블의 정적 경로를 다른 고정 경로로 바꿀 수 있습니다.

콘솔을 사용하여 정적 경로 바꾸기

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway Route Tables(전송 게이트웨이 라우팅 테이블)를 선택합니다.
3. 라우팅 테이블에서 교체하려는 경로를 선택합니다.
4. 세부 정보 섹션에서 라우팅(Routes) 탭을 선택합니다.
5. 작업, 정적 경로 바꾸기를 선택합니다.
6. 유형에서 활성 또는 블랙홀을 선택합니다.
7. 첨부 파일 선택(Choose attachment) 드롭다운에서 라우팅 테이블의 현재 게이트웨이를 대체할 전송 게이트웨이를 선택합니다.
8. 정적 경로 바꾸기를 선택합니다.

를 사용하여 고정 경로를 바꾸려면 AWS CLI

[replace-transit-gateway-route](#) 명령을 사용합니다.

Amazon S3에 라우팅 테이블 내보내기

Transit Gateway 라우팅 테이블의 라우팅을 Amazon S3 버킷으로 내보낼 수 있습니다. 라우팅은 JSON 파일의 지정된 Amazon S3 버킷에 저장됩니다.

콘솔을 사용하여 Transit Gateway 라우팅 테이블 내보내기

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway Route Tables(전송 게이트웨이 라우팅 테이블)를 선택합니다.
3. 내보낼 경로가 포함된 라우팅 테이블을 선택합니다.
4. 작업, 경로 내보내기(Export routes)를 선택합니다.
5. 경로 내보내기(Export routes) 페이지에서 S3 버킷 이름에 대해 S3 버킷의 이름을 입력합니다.
6. 내보낸 경로를 필터링하려면 페이지의 필터 섹션에서 필터 파라미터를 지정합니다.
7. 경로 내보내기(Export routes)를 선택합니다.

내보낸 라우팅에 액세스하려면 <https://console.aws.amazon.com/s3/>에서 Amazon S3 콘솔을 열고 지정한 버킷으로 이동합니다. 파일 이름에는 AWS 계정 ID, AWS 지역, 라우팅 테이블 ID, 타임스탬프가 포함됩니다. 파일을 선택하고 다운로드를 선택합니다. 다음은 VPC 연결에 대한 두 개의 전파 경로 정보를 포함한 JSON 파일의 예입니다.

```
{
  "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"
  }
]
}

```

Transit Gateway 라우팅 테이블 삭제

콘솔을 사용하여 Transit Gateway 라우팅 테이블 삭제

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway Route Tables(전송 게이트웨이 라우팅 테이블)를 선택합니다.
3. 삭제할 라우팅 테이블을 선택합니다.
4. 작업(Actions), Transit Gateway 라우팅 테이블 삭제>Delete Transit Gateway route table)를 선택합니다.
5. **delete**를 입력하고 삭제>Delete)를 선택하여 삭제를 확인합니다.

를 사용하여 트랜짓 게이트웨이 라우팅 테이블을 삭제하려면 AWS CLI

[delete-transit-gateway-route-table](#) 명령어를 사용합니다.

접두사 목록 참조

Transit Gateway 라우팅 테이블에서 접두사 목록을 참조할 수 있습니다. 접두사 목록은 사용자가 정의하고 관리하는 하나 이상의 CIDR 블록 항목 세트입니다. 접두사 목록을 사용하면 리소스에서 네트워크 트래픽을 라우팅하기 위해 참조하는 IP 주소의 관리를 간소화할 수 있습니다. 예를 들어 여러

Transit Gateway 라우팅 테이블에서 동일한 대상 CIDR을 자주 지정하는 경우 각 라우팅 테이블에서 동일한 CIDR을 반복해서 참조하는 대신 단일 접두사 목록에서 이러한 CIDR을 관리할 수 있습니다. 대상 CIDR 블록을 제거해야 하는 경우 영향을 받는 모든 라우팅 테이블에서 경로를 제거하는 대신 접두사 목록에서 해당 항목을 제거할 수 있습니다.

Transit Gateway 라우팅 테이블에서 접두사 목록 참조를 생성하면 접두사 목록의 각 항목이 Transit Gateway 라우팅 테이블에 경로로 표시됩니다.

접두사 목록에 대한 자세한 내용을 알아보려면 Amazon VPC 사용 설명서의 [접두사 목록](#)을 참조하세요.

접두사 목록 참조 생성

Transit Gateway 라우팅 테이블에서 접두사 목록에 대한 참조를 생성할 수 있습니다.

콘솔을 사용하여 접두사 목록 참조를 생성하려면

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway 라우팅 테이블(Transit Gateway Route Tables)을 선택합니다.
3. Transit Gateway 라우팅 테이블을 선택합니다.
4. Actions(작업), Create prefix list reference(접두사 목록 참조 생성)를 선택합니다.
5. Prefix list ID(접두사 목록 ID)에서 접두사 목록의 ID를 선택합니다.
6. 유형(Type)에서 이 접두사 목록에 대한 트래픽을 허용(활성(Active))할지, 아니면 삭제(블랙홀(Blackhole))할지를 선택합니다.
7. Transit Gateway 연결 ID(Transit gateway attachment ID)에서 트래픽을 라우팅할 연결의 ID를 선택합니다.
8. Create prefix list reference(접두사 목록 참조 생성)를 선택합니다.

AWS CLI를 사용하여 접두사 목록 참조 생성

[create-transit-gateway-prefix-list-reference](#) 명령을 사용합니다.

접두사 목록 참조 보기

Transit Gateway 라우팅 테이블에서 접두사 목록 참조를 볼 수 있습니다. 또한 접두사 목록의 각 항목을 Transit Gateway 라우팅 테이블에서 개별 경로로 볼 수 있습니다. 접두사 목록 라우팅의 라우팅 유형은 propagated입니다.

콘솔을 사용하여 접두사 목록 참조 보기

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway 라우팅 테이블(Transit Gateway Route Tables)을 선택합니다.
3. Transit Gateway 라우팅 테이블을 선택합니다.
4. 아래쪽 창에서 Prefix list references(접두사 목록 참조)를 선택합니다. 접두사 목록 참조가 나열됩니다.
5. 경로(Routes)를 선택합니다. 각 접두사 목록 항목은 라우팅 테이블에 경로로 나열됩니다.

AWS CLI를 사용하여 접두사 목록 참조 보기

[get-transit-gateway-prefix-list-references](#) 명령을 사용합니다.

접두사 목록 참조 수정

트래픽이 라우팅되는 연결을 변경하거나 해당 경로와 일치하는 트래픽을 삭제할지 여부를 지정하여 접두사 목록 참조를 수정할 수 있습니다.

경로(Routes) 탭에서는 접두사 목록의 개별 경로를 수정할 수 없습니다. 접두사 목록의 항목을 수정하려면 Managed Prefix Lists(관리형 접두사 목록) 화면을 사용합니다. 자세한 내용을 알아보려면 Amazon VPC 사용 설명서의 [접두사 목록 수정](#)을 참조하세요.

콘솔을 사용하여 접두사 목록 참조 수정

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway 라우팅 테이블(Transit Gateway Route Tables)을 선택합니다.
3. Transit Gateway 라우팅 테이블을 선택합니다.
4. 아래쪽 창에서 Prefix list references(접두사 목록 참조)를 선택합니다.
5. 접두사 목록 참조를 선택하고 참조 수정(Modify reference)를 선택합니다.
6. 유형(Type)에서 이 접두사 목록에 대한 트래픽을 허용(활성(Active))할지, 아니면 삭제(블랙홀(Blackhole))할지를 선택합니다.
7. Transit Gateway 연결 ID(Transit gateway attachment ID)에서 트래픽을 라우팅할 연결의 ID를 선택합니다.
8. Modify prefix list reference(접두사 목록 참조 수정)를 선택합니다.

AWS CLI를 사용하여 접두사 목록 참조 수정

[modify-transit-gateway-prefix-list-reference](#) 명령을 사용합니다.

접두사 목록 참조 삭제

접두사 목록 참조가 더 이상 필요하지 않은 경우 Transit Gateway 라우팅 테이블에서 삭제할 수 있습니다. 참조를 삭제해도 접두사 목록은 삭제되지 않습니다.

콘솔을 사용하여 접두사 목록 참조를 삭제하려면

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 Transit Gateway 라우팅 테이블(Transit Gateway Route Tables)을 선택합니다.
3. Transit Gateway 라우팅 테이블을 선택합니다.
4. 접두사 목록 참조를 선택하고 참조 삭제>Delete references)를 선택합니다.
5. 참조 삭제>Delete references)를 선택합니다.

AWS CLI를 사용하여 접두사 목록 참조 삭제

[delete-transit-gateway-prefix-list-reference](#) 명령을 사용합니다.

Transit Gateway 정책 테이블

전송 게이트웨이 동적 라우팅은 정책 테이블을 사용하여 AWS Cloud WAN에 대한 네트워크 트래픽을 라우팅합니다. 테이블에는 정책 속성별로 네트워크 트래픽을 일치시키는 정책 규칙이 포함되어 있으며 규칙과 일치하는 트래픽을 대상 라우팅 테이블에 매핑합니다.

전송 게이트웨이에 대한 동적 라우팅을 사용하여 피어링된 전송 게이트웨이 유형과 라우팅 및 연결 가능성 정보를 자동으로 교환할 수 있습니다. 정적 경로와 달리 트래픽은 경로 장애 또는 정체와 같은 네트워크 조건에 따라 다른 경로를 따라 라우팅될 수 있습니다. 또한 동적 라우팅은 네트워크 침해 또는 침입이 발생한 경우 트래픽을 더 쉽게 재라우팅한다는 점에서 추가적인 보안 계층을 추가합니다.

Note

전송 게이트웨이 정책 테이블은 현재 전송 게이트웨이 피어링 연결을 생성할 때 Cloud WAN에서만 지원됩니다. 피어링 연결을 생성할 때 이 연결과 해당 테이블을 연결할 수 있습니다. 그러면 이 연결이 정책 규칙으로 테이블을 자동으로 채웁니다.

Cloud WAN에서 피어링 연결에 대한 자세한 정보는 AWS Cloud WAN 사용 설명서의 [피어링](#)을 참조하세요.

Transit Gateway 정책 테이블 생성

콘솔을 사용하여 전송 게이트웨이 정책 테이블 생성

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 여세요.
2. 탐색 창에서 전송 게이트웨이 정책 테이블(Transit Gateway Policy Tables)을 선택합니다.
3. Transit Gateway 정책 테이블 생성(Create Transit Gateway policy table)을 선택합니다.
4. (선택 사항) 이름 태그(Name tag)에 Transit Gateway 정책 테이블의 이름을 입력합니다. 그러면 태그 값이 지정한 이름인 태그가 생성됩니다.
5. 전송 게이트웨이 ID에서 정책 테이블에 대한 전송 게이트웨이를 선택합니다.
6. 전송 게이트웨이 정책 테이블 생성(Create transit gateway policy table)을 선택합니다.

를 사용하여 트랜짓 게이트웨이 정책 테이블을 만들려면 AWS CLI

[create-transit-gateway-policy-table](#) 명령을 사용합니다.

전송 게이트웨이 정책 테이블 삭제

전송 게이트웨이 정책 테이블을 삭제합니다. 테이블이 삭제되면 해당 테이블 내의 모든 정책 규칙이 삭제됩니다.

콘솔을 사용하여 전송 게이트웨이 정책 테이블 삭제

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 여세요.
2. 탐색 창에서 전송 게이트웨이 정책 테이블(Transit Gateway Policy Tables)을 선택합니다.
3. 삭제할 Transit Gateway 정책 테이블을 선택합니다.
4. 작업(Actions)을 선택한 후 정책 테이블 삭제>Delete policy table)를 선택합니다.
5. 테이블을 삭제하려 한다는 것을 확인합니다.

를 사용하여 트랜짓 게이트웨이 정책 테이블을 삭제하려면 AWS CLI

[delete-transit-gateway-policy-table](#) 명령을 사용합니다.

Transit Gateway의 멀티캐스트

멀티캐스트는 데이터의 단일 스트림을 여러 수신 컴퓨터에 동시에 전달하는 데 사용되는 통신 프로토콜입니다. Transit Gateway는 연결된 VPC의 서브넷 간에 멀티캐스트 트래픽 라우팅을 지원하며 여러 수신 인스턴스로 향하는 트래픽을 보내는 인스턴스에 대한 멀티캐스트 라우터 역할을 합니다.

멀티캐스트 개념

다음은 멀티캐스트의 핵심 개념입니다.

- 멀티캐스트 도메인 — 멀티캐스트 네트워크를 여러 도메인으로 분할할 수 있으며 Transit Gateway를 여러 멀티캐스트 라우터로 사용할 수 있습니다. 서브넷 수준에서 멀티캐스트 도메인 멤버십을 정의합니다.
- 멀티캐스트 그룹 — 동일한 멀티캐스트 트래픽을 보내고 받을 호스트 집합을 식별합니다. 멀티캐스트 그룹은 그룹 IP 주소로 식별됩니다. 멀티캐스트 그룹 멤버십은 EC2 인스턴스에 연결된 개별 탄력적 네트워크 인터페이스에 의해 정의됩니다.
- 인터넷 그룹 관리 프로토콜(IGMP) - 호스트와 라우터가 멀티캐스트 그룹 멤버십을 동적으로 관리할 수 있도록 하는 인터넷 프로토콜입니다. IGMP 멀티캐스트 도메인에는 IGMP 프로토콜을 사용하여 메시지를 연결, 탈퇴 및 전송하는 호스트가 포함됩니다. AWS IGMPv2 프로토콜과 IGMP 및 정적(API 기반) 그룹 멤버십 멀티캐스트 도메인을 모두 지원합니다.
- 멀티캐스트 소스 — 멀티캐스트 트래픽을 전송하도록 정적으로 구성된 지원되는 EC2 인스턴스와 연결된 탄력적 네트워크 인터페이스입니다. 멀티캐스트 소스는 정적 소스 구성에만 적용됩니다.

정적 소스 멀티캐스트 도메인에는 메시지의 가입, 종료 및 전송을 처리하는 데 IGMP 프로토콜을 사용하지 않는 호스트가 포함됩니다. 를 사용하여 소스 및 그룹 AWS CLI 구성원을 추가합니다. 정적으로 추가된 소스는 멀티캐스트 트래픽을 전송하고 멤버는 멀티캐스트 트래픽을 수신합니다.

- 멀티캐스트 그룹 멤버 — 멀티캐스트 트래픽을 수신하는, 지원되는 EC2 인스턴스와 연결된 탄력적 네트워크 인터페이스입니다. 멀티캐스트 그룹에는 여러 그룹 멤버가 있습니다. 정적 소스 그룹 멤버십 구성에서 멀티캐스트 그룹 멤버는 트래픽을 수신할 수만 있습니다. IGMP 그룹 구성에서 멤버는 트래픽을 보내고 받을 수 있습니다.

고려 사항

- 지원되는 리전에 대한 자세한 내용은 [AWS Transit Gateway FAQ](#)를 참조하세요.
- 멀티캐스트를 지원하려면 새 Transit Gateway를 생성해야 합니다.

- 멀티캐스트 그룹 멤버십은 OR AWS CLI, Amazon Virtual Private Cloud Console 또는 IGMP를 사용하여 관리합니다.
- 서브넷은 하나의 멀티캐스트 도메인에만 있을 수 있습니다.
- Nitro 인스턴스가 아닌 인스턴스를 사용하는 경우 소스/대상 확인을 비활성화해야 합니다. 확인 비활성화에 대한 자세한 내용은 Amazon EC2 사용 [설명서의 원본 또는 대상 확인 변경을](#) 참조하십시오.
- Nitro 인스턴스가 아닌 인스턴스는 멀티캐스트 발신자가 될 수 없습니다.
- Site-to-Site VPN AWS Direct Connect, 피어링 첨부 파일 또는 트랜짓 게이트웨이 Connect 첨부 파일을 통한 멀티캐스트 라우팅은 지원되지 않습니다.
- Transit Gateway는 멀티캐스트 패킷의 조각화를 지원하지 않습니다. 조각화된 멀티캐스트 패킷은 삭제됩니다. 자세한 정보는 [최대 전송 단위\(MTU\)](#)을 참조하세요.
- 시작할 때 IGMP 호스트는 멀티캐스트 그룹에 가입하기 위해 IGMP JOIN 메시지를 여러 번 보냅니다(일반적으로 2~3회 재시도). 가능성은 낮지만 모든 IGMP JOIN 메시지가 손실되는 경우 호스트는 전송 게이트웨이 멀티캐스트 그룹의 멤버가 되지 않습니다. 이러한 시나리오에서는 애플리케이션별 방법을 사용하여 호스트에서 IGMP JOIN 메시지를 다시 트리거해야 합니다.
- 그룹 멤버십은 Transit Gateway에 의한 IGMPv2 JOIN 메시지 수신으로 시작되어 IGMPv2 LEAVE 메시지의 수신으로 종료됩니다. Transit Gateway는 그룹에 성공적으로 조인한 호스트를 추적합니다. 클라우드 멀티캐스트 라우터로서 Transit Gateway는 2분마다 IGMPv2 QUERY 메시지를 모든 멤버에게 보냅니다. 각 멤버는 응답으로 IGMPv2 JOIN 메시지를 전송하고, 이 메시지는 멤버가 해당 멤버십을 갱신하는 방법을 나타냅니다. 멤버가 연속 세 번 쿼리에 응답하지 못하면 Transit Gateway가 조인된 모든 그룹에서 이 멤버십을 제거합니다. 하지만 구성원을 목록에서 영구적으로 제거하기 전에 12시간 동안 이 구성원에게 계속 쿼리를 보냅니다. to-be-queried 명시적 IGMPv2 LEAVE 메시지는 이후의 모든 멀티캐스트 처리에서 호스트를 즉시 영구적으로 제거합니다.
- Transit Gateway는 그룹에 성공적으로 조인한 호스트를 추적합니다. Transit Gateway는 중단이 발생한 경우 IGMP JOIN 메시지가 마지막으로 성공한 시점부터 7분(420초) 동안 호스트로 멀티캐스트 데이터를 보냅니다. 전송 게이트웨이는 최대 12시간 동안 또는 호스트에서 IGMP LEAVE 메시지를 받을 때까지 호스트에 멤버십 쿼리를 계속 보냅니다.
- Transit Gateway는 멀티캐스트 그룹 멤버십을 추적할 수 있도록 모든 IGMP 멤버에게 멤버십 쿼리 패킷을 보냅니다. 이러한 IGMP 쿼리 패킷의 소스 IP는 0.0.0.0/32이고 대상 IP는 224.0.0.1/32이며 프로토콜은 2입니다. IGMP 호스트(인스턴스)의 보안 그룹 구성과 호스트 서브넷의 모든 ACL 구성은 이러한 IGMP 프로토콜 메시지를 허용해야 합니다.
- 멀티캐스트 소스와 대상이 동일한 VPC에 있는 경우 보안 그룹 참조를 사용하여 소스 보안 그룹의 트래픽을 허용하도록 대상 보안 그룹을 설정할 수 없습니다.

- 정적 멀티캐스트 그룹 및 소스의 경우 Amazon VPC Transit Gateway는 더 이상 존재하지 않는 ENI의 정적 그룹과 소스를 자동으로 제거합니다. 이는 정기적으로 [Transit Gateway 서비스 연결 역할](#)을 맡아 계정의 ENI를 설명함으로써 수행됩니다.
- 정적 멀티캐스트만 IPv6을 지원합니다. 동적 멀티캐스트는 그렇지 않습니다.

Windows Server의 멀티캐스트

Windows Server 2019 또는 2022에서 전송 게이트웨이와 함께 작동하도록 멀티캐스트를 설정할 때는 추가 단계를 수행해야 합니다. PowerShell를 사용하여 다음 명령을 실행합니다.

1. TCP/IP 스택에 IGMPv3 대신 IGMPv2를 사용하도록 윈도우 서버를 변경하세요.

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

Note

New-ItemPropertyIGMP 버전을 지정하는 속성 인덱스입니다. IGMP v2는 멀티캐스트에 지원되는 버전이므로 속성은 Value 다음과 같아야 합니다. 3 Windows 레지스트리를 편집하는 대신 다음 명령을 실행하여 IGMP 버전을 2로 설정할 수 있습니다. :

```
Set-NetIPv4Protocol -IGMPVersion Version2
```

2. Windows 방화벽은 기본적으로 대부분의 UDP 트래픽을 삭제합니다. 먼저 멀티캐스트에 사용되는 연결 프로필을 확인해야 합니다.

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

NetworkCategory
-----
                Public
```

3. 필수 UDP 포트에 액세스할 수 있도록 이전 단계의 연결 프로필을 업데이트하세요.

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

4. EC2 인스턴스를 재부팅합니다.
5. 멀티캐스트 애플리케이션을 테스트하여 트래픽이 예상대로 흐르고 있는지 확인하세요.

멀티캐스트 라우팅

Transit Gateway에서 멀티캐스트를 활성화하면 Transit Gateway는 멀티캐스트 라우터 역할을 합니다. 서브넷을 멀티캐스트 도메인에 추가하면 해당 멀티캐스트 도메인과 연결된 Transit Gateway로 모든 멀티캐스트 트래픽을 보냅니다.

네트워크 ACL

네트워크 ACL 규칙은 서브넷 수준에서 작동합니다. Transit Gateway는 서브넷 외부에 있기 때문에 이는 멀티캐스트 트래픽에 적용됩니다. 자세한 내용을 알아보려면 Amazon VPC 사용 설명서의 [네트워크 ACL](#)을 참조하세요.

인터넷 그룹 관리 프로토콜(IGMP) 멀티캐스트 트래픽의 경우 다음과 같은 최소 인바운드 규칙이 있습니다. 원격 호스트는 멀티캐스트 트래픽을 보내는 호스트입니다.

유형	프로토콜	소스	설명
사용자 지정 프로토콜	IGMP(2)	0.0.0.0/32	IGMP 쿼리
사용자 지정 UDP 프로토콜	UDP	원격 호스트 IP 주소	인바운드 멀티캐스트 트래픽

다음은 IGMP용 최소 아웃바운드 규칙입니다.

유형	프로토콜	대상 주소	설명
사용자 지정 프로토콜	IGMP(2)	224.0.0.2/32	IGMP 나가기
사용자 지정 프로토콜	IGMP(2)	멀티캐스트 그룹 IP 주소	IGMP 가입
사용자 지정 UDP 프로토콜	UDP	멀티캐스트 그룹 IP 주소	아웃바운드 멀티캐스트 트래픽

보안 그룹

보안 그룹 규칙은 인스턴스 수준에서 작동합니다. 인바운드 및 아웃바운드 멀티캐스트 트래픽 모두에 적용할 수 있습니다. 이 동작은 유니캐스트 트래픽과 동일합니다. 모든 그룹 멤버 인스턴스에 대해 그

룹 소스로부터의 인바운드 트래픽을 허용해야 합니다. 자세한 내용을 알아보려면 Amazon VPC 사용 설명서의 [보안 그룹](#)을 참조하세요.

IGMP 멀티캐스트 트래픽의 경우 최소한 다음과 같은 인바운드 규칙이 있어야 합니다. 원격 호스트는 멀티캐스트 트래픽을 보내는 호스트입니다. 보안 그룹을 UDP 인바운드 규칙의 소스로 지정할 수 없습니다.

유형	프로토콜	소스	설명
사용자 지정 프로토콜	2	0.0.0.0/32	IGMP 쿼리
사용자 지정 UDP 프로토콜	UDP	원격 호스트 IP 주소	인바운드 멀티캐스트 트래픽

IGMP 멀티캐스트 트래픽의 경우 최소한 다음과 같은 아웃바운드 규칙이 있어야 합니다.

유형	프로토콜	대상 주소	설명
사용자 지정 프로토콜	2	224.0.0.2/32	IGMP 나가기
사용자 지정 프로토콜	2	멀티캐스트 그룹 IP 주소	IGMP 가입
사용자 지정 UDP 프로토콜	UDP	멀티캐스트 그룹 IP 주소	아웃바운드 멀티캐스트 트래픽

멀티캐스트 작업

Amazon VPC 콘솔 또는 AWS CLI를 사용하여 전송 게이트웨이에서 멀티캐스트를 구성할 수 있습니다.

멀티캐스트 도메인을 생성하기 전에 호스트가 멀티캐스트 트래픽에 대해 인터넷 그룹 관리 프로토콜 (IGMP) 프로토콜을 사용하는지 여부를 알아야 합니다.

내용

- [멀티캐스트 도메인 속성](#)
- [IGMP 구성 관리](#)
- [정적 소스 구성 관리](#)

- [정적 그룹 멤버 구성 관리](#)
- [멀티캐스트 도메인 관리](#)
- [멀티캐스트 그룹 관리](#)
- [공유 멀티캐스트 도메인 작업](#)

멀티캐스트 도메인 속성

다음 표에 멀티캐스트 도메인 속성에 대해 자세히 설명되어 있습니다. 두 가지 속성을 동시에 사용할 수 없습니다.

속성	설명
IgmPV2Support (AWS CLI) IGMPv2 지원(IGMPv2 support)(콘솔)	<p>이 속성은 그룹 멤버가 멀티캐스트 그룹에 조인하거나 나가는 방법을 결정합니다.</p> <p>이 속성을 사용하지 않도록 설정한 경우 도메인에 수동으로 그룹 멤버를 추가해야 합니다.</p> <p>하나 이상의 멤버가 IGMP 프로토콜을 사용하면 이 속성을 사용하도록 설정합니다. 멤버는 다음 방법 중 하나로 멀티캐스트 그룹에 조인합니다.</p> <ul style="list-style-type: none"> • IGMP를 지원하는 멤버는 JOIN 및 LEAVE 메시지를 사용합니다. • IGMP를 지원하지 않는 멤버는 Amazon VPC 콘솔 또는 AWS CLI를 사용하여 그룹에 추가하거나 그룹에서 제거해야 합니다. <p>멀티캐스트 그룹 멤버를 등록한 경우 멤버 등록 취소도 직접 해야 합니다. Transit Gateway는 수동으로 추가된 그룹 멤버가 보낸 IGMP LEAVE 메시지를 무시합니다.</p>
StaticSourcesSupport (AWS CLI) 정적 소스 지원(Static sources support)(콘솔)	<p>이 속성은 그룹에 대한 정적 멀티캐스트 소스가 있는지 여부를 결정합니다.</p> <p>이 속성이 활성화되면 register-transit-gateway-multicast-group-sources를 사용하여 멀티캐스트 도메인의 소스를 추가해야 합니다. 멀티캐스트 소스만 멀티캐스트 트래픽을 보낼 수 있습니다.</p>

속성	설명
	이 속성이 사용하도록 설정되어 있지 않으면 지정된 멀티캐스트 소스가 없습니다. 멀티캐스트 도메인과 연결된 서브넷에 있는 모든 인스턴스는 멀티캐스트 트래픽을 보낼 수 있으며 그룹 멤버는 멀티캐스트 트래픽을 받을 수 있습니다.

IGMP 구성 관리

멀티캐스트 트래픽에 IGMP 프로토콜을 사용하는 호스트가 하나 이상 있는 경우 AWS 는 인스턴스로부터 IGMP JOIN 메시지를 수신할 때 멀티캐스트 그룹을 자동으로 생성한 다음 해당 인스턴스를 이 그룹의 멤버로 추가합니다. 를 사용하여 IGMP가 아닌 호스트를 그룹에 정적으로 구성원으로 추가할 수도 있습니다. AWS CLI 멀티캐스트 도메인과 연결된 서브넷에 있는 모든 인스턴스는 트래픽을 보낼 수 있으며 그룹 멤버는 멀티캐스트 트래픽을 받을 수 있습니다.

다음 단계에 따라 구성을 완료합니다.

1. VPC를 만듭니다. VPC 생성에 대한 자세한 내용은 Amazon VPC 사용 설명서의 [VPC 생성](#)을 참조하세요.
2. VPC에서 서브넷을 만듭니다. 서브넷 생성에 대한 자세한 내용을 알아보려면 Amazon VPC 사용 설명서의 [VPC에서 서브넷 생성](#)을 참조하세요.
3. 멀티캐스트 트래픽에 대해 구성된 Transit Gateway를 만듭니다. 자세한 설명은 [the section called “Transit Gateway 생성”](#) 섹션을 참조하세요.
4. VPC 연결을 만듭니다. 자세한 설명은 [the section called “VPC에 대한 Transit Gateway Attachment 생성”](#) 섹션을 참조하세요.
5. IGMP 지원을 위해 구성된 멀티캐스트 도메인을 만듭니다. 자세한 설명은 [the section called “IGMP 멀티캐스트 도메인 생성”](#) 섹션을 참조하세요.

다음 설정을 사용합니다.

- IGMPv2 지원(IGMPv2 support)을 사용하도록 설정합니다.
 - 정적 소스 지원(Static sources support)을 사용하지 않도록 설정합니다.
6. Transit Gateway VPC 연결의 서브넷과 멀티캐스트 도메인 간에 연결을 생성합니다. 자세한 내용을 알아보려면 [the section called “VPC 연결 및 서브넷을 멀티캐스트 도메인과 연결”](#) 섹션을 참조하세요.

7. EC2의 기본 IGMP 버전은 IGMPv3입니다. 모든 IGMP 그룹 멤버의 버전을 변경해야 합니다. 다음 명령을 실행할 수 있습니다.

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

8. IGMP 프로토콜을 사용하지 않는 멤버를 멀티캐스트 그룹에 추가합니다. 자세한 설명은 [the section called “멀티캐스트 그룹에 멤버 등록”](#) 섹션을 참조하세요.

정적 소스 구성 관리

이 구성에서는 그룹에 멀티캐스트 소스를 정적으로 추가해야 합니다. 호스트는 IGMP 프로토콜을 사용하여 멀티캐스트 그룹에 조인하거나 나가지 않습니다. 멀티캐스트 트래픽을 수신하는 그룹 멤버를 정적으로 추가해야 합니다.

다음 단계에 따라 구성을 완료합니다.

1. VPC를 만듭니다. VPC 생성에 대한 자세한 내용은 Amazon VPC 사용 설명서의 [VPC 생성](#)을 참조하세요.
2. VPC에서 서브넷을 만듭니다. 서브넷 생성에 대한 자세한 내용을 알아보려면 Amazon VPC 사용 설명서의 [VPC에서 서브넷 생성](#)을 참조하세요.
3. 멀티캐스트 트래픽에 대해 구성된 Transit Gateway를 만듭니다. 자세한 설명은 [the section called “Transit Gateway 생성”](#) 섹션을 참조하세요.
4. VPC 연결을 만듭니다. 자세한 설명은 [the section called “VPC에 대한 Transit Gateway Attachment 생성”](#) 섹션을 참조하세요.
5. IGMP 지원 없이 구성된 멀티캐스트 도메인을 만들고 소스를 정적으로 추가할 수 있도록 지원합니다. 자세한 설명은 [the section called “정적 소스 멀티캐스트 도메인 생성”](#) 섹션을 참조하세요.

다음 설정을 사용합니다.

- IGMPv2 지원(IGMPv2 support)을 사용하지 않도록 설정합니다.
- 소스를 수동으로 추가하려면 정적 소스 지원(Static sources support)을 사용하도록 설정합니다.

이 소스가 이 속성이 사용하도록 설정된 경우 멀티캐스트 트래픽을 전송할 수 있는 유일한 리소스입니다. 그렇지 않으면 멀티캐스트 도메인과 연결된 서브넷에 있는 모든 인스턴스가 멀티캐스트 트래픽을 보낼 수 있으며 그룹 멤버는 멀티캐스트 트래픽을 받을 수 있습니다.

6. Transit Gateway VPC 연결의 서브넷과 멀티캐스트 도메인 간에 연결을 생성합니다. 자세한 내용은 [the section called “VPC 연결 및 서브넷을 멀티캐스트 도메인과 연결”](#) 섹션을 참조하세요.

7. 정적 소스 지원(Static sources support)을 사용하도록 설정한 경우 소스를 멀티캐스트 그룹에 추가합니다. 자세한 설명은 [the section called “멀티캐스트 그룹에 소스 등록”](#) 섹션을 참조하세요.
8. 멀티캐스트 그룹에 멤버를 추가합니다. 자세한 설명은 [the section called “멀티캐스트 그룹에 멤버 등록”](#) 섹션을 참조하세요.

정적 그룹 멤버 구성 관리

이 구성에서는 그룹에 멀티캐스트 멤버를 정적으로 추가해야 합니다. 호스트는 IGMP 프로토콜을 사용하여 멀티캐스트 그룹에 조인하거나 나갈 수 없습니다. 멀티캐스트 도메인과 연결된 서브넷에 있는 모든 인스턴스는 멀티캐스트 트래픽을 보낼 수 있으며 그룹 멤버는 멀티캐스트 트래픽을 받을 수 있습니다.

다음 단계에 따라 구성을 완료합니다.

1. VPC를 만듭니다. VPC 생성에 대한 자세한 내용은 Amazon VPC 사용 설명서의 [VPC 생성](#)을 참조하세요.
2. VPC에서 서브넷을 만듭니다. 서브넷 생성에 대한 자세한 내용을 알아보려면 Amazon VPC 사용 설명서의 [VPC에서 서브넷 생성](#)을 참조하세요.
3. 멀티캐스트 트래픽에 대해 구성된 Transit Gateway를 만듭니다. 자세한 설명은 [the section called “Transit Gateway 생성”](#) 섹션을 참조하세요.
4. VPC 연결을 만듭니다. 자세한 설명은 [the section called “VPC에 대한 Transit Gateway Attachment 생성”](#) 섹션을 참조하세요.
5. IGMP 지원 없이 구성된 멀티캐스트 도메인을 만들고 소스를 정적으로 추가할 수 있도록 지원합니다. 자세한 설명은 [the section called “정적 소스 멀티캐스트 도메인 생성”](#) 섹션을 참조하세요.

다음 설정을 사용합니다.

- IGMPv2 지원(IGMPv2 support)을 사용하지 않도록 설정합니다.
 - 정적 소스 지원(Static sources support)을 사용하지 않도록 설정합니다.
6. Transit Gateway VPC 연결의 서브넷과 멀티캐스트 도메인 간에 연결을 생성합니다. 자세한 내용을 알아보려면 [the section called “VPC 연결 및 서브넷을 멀티캐스트 도메인과 연결”](#) 섹션을 참조하세요.
 7. 멀티캐스트 그룹에 멤버를 추가합니다. 자세한 설명은 [the section called “멀티캐스트 그룹에 멤버 등록”](#) 섹션을 참조하세요.

멀티캐스트 도메인 관리

Transit Gateway와 함께 멀티캐스트를 사용하려면 멀티캐스트 도메인을 생성한 다음 서브넷을 도메인에 연결합니다.

목차

- [IGMP 멀티캐스트 도메인 생성](#)
- [정적 소스 멀티캐스트 도메인 생성](#)
- [VPC 연결 및 서브넷을 멀티캐스트 도메인과 연결](#)
- [멀티캐스트 도메인 연결 보기](#)
- [멀티캐스트 도메인에서 서브넷 연결 해제](#)
- [멀티캐스트 도메인에 태그 추가](#)
- [멀티캐스트 도메인 삭제](#)

IGMP 멀티캐스트 도메인 생성

아직 수행하지 않은 경우 사용 가능한 멀티캐스트 도메인 속성을 검토합니다. 자세한 설명은 [the section called “멀티캐스트 작업”](#) 섹션을 참조하세요.

Console

콘솔을 사용하여 IGMP 멀티캐스트 도메인 생성

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 여세요.
2. 탐색 창에서 Transit Gateway Multicast(전송 게이트웨이 멀티캐스트)를 선택합니다.
3. Transit Gateway 멀티캐스트 도메인 생성(Create Transit Gateway multicast domain)을 선택합니다.
4. 이름 태그(Name tag)에 서브넷의 이름을 입력합니다.
5. Transit gateway ID에서 멀티캐스트 트래픽을 처리하는 Transit Gateway를 선택합니다.
6. IGMPv2 지원(IGMPv2 support)의 경우 확인란을 선택합니다.
7. 정적 소스 지원(Static sources support)의 경우 확인란을 선택 취소합니다.
8. 이 멀티캐스트 도메인에 대한 교차 계정 서브넷 연결을 자동으로 수락하려면 공유 연결 자동 수락(Auto accept shared associations)을 선택합니다.
9. Transit Gateway 멀티캐스트 도메인 생성(Create Transit Gateway multicast domain)을 선택합니다.

Command line

를 사용하여 IGMP 멀티캐스트 도메인을 만들려면 AWS CLI

[create-transit-gateway-multicast-domain](#) 명령을 사용합니다.

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

정적 소스 멀티캐스트 도메인 생성

아직 수행하지 않은 경우 사용 가능한 멀티캐스트 도메인 속성을 검토합니다. 자세한 설명은 [the section called “멀티캐스트 작업”](#) 섹션을 참조하세요.

Console

콘솔을 사용하여 정적 멀티캐스트 도메인 생성

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 여세요.
2. 탐색 창에서 Transit Gateway Multicast(전송 게이트웨이 멀티캐스트)를 선택합니다.
3. Transit Gateway 멀티캐스트 도메인 생성(Create Transit Gateway multicast domain)을 선택합니다.
4. 이름 태그(Name tag)에 도메인을 식별하는 이름을 입력합니다.
5. Transit gateway ID에서 멀티캐스트 트래픽을 처리하는 Transit Gateway를 선택합니다.
6. IGMPv2 지원(IGMPv2 support)의 경우 확인란을 선택 취소합니다.
7. 정적 소스 지원(Static sources support)의 경우 확인란을 선택합니다.
8. 이 멀티캐스트 도메인에 대한 교차 계정 서브넷 연결을 자동으로 수락하려면 공유 연결 자동 수락(Auto accept shared associations)을 선택합니다.
9. Transit Gateway 멀티캐스트 도메인 생성(Create Transit Gateway multicast domain)을 선택합니다.

Command line

를 사용하여 정적 멀티캐스트 도메인을 만들려면 AWS CLI

[create-transit-gateway-multicast-domain](#) 명령을 사용합니다.

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

VPC 연결 및 서브넷을 멀티캐스트 도메인과 연결

VPC 연결을 멀티캐스트 도메인과 연결하려면 다음 절차를 따릅니다. 연결을 생성할 때 멀티캐스트 도메인에 포함할 서브넷을 선택할 수 있습니다.

시작하기 전에 Transit Gateway에 VPC 연결을 생성해야 합니다. 자세한 설명은 [VPC에 대한 Transit Gateway Attachment](#) 섹션을 참조하세요.

Console

콘솔을 사용하여 VPC 연결을 멀티캐스트 도메인과 연결

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 여세요.
2. 탐색 창에서 Transit Gateway Multicast(전송 게이트웨이 멀티캐스트)를 선택합니다.
3. 멀티캐스트 도메인을 선택한 다음 작업(Actions), 연결 생성(Create association)을 선택합니다.
4. 연결할 연결 선택(Choose attachment to associate)에서 Transit Gateway Attachment를 선택합니다.
5. 연결할 서브넷 선택(Choose subnets to associate)에서 멀티캐스트 도메인에 포함할 서브넷을 선택합니다.
6. 연결 생성을 선택합니다.

Command line

를 사용하여 VPC 연결을 멀티캐스트 도메인과 연결하려면 AWS CLI

[associate-transit-gateway-multicast-domain](#) 명령을 사용합니다.

멀티캐스트 도메인 연결 보기

멀티캐스트 도메인을 보고 사용 가능 여부와 적절한 서브넷 및 연결이 포함되어 있는지를 확인할 수 있습니다.

Console

콘솔을 사용하여 멀티캐스트 도메인을 보려면

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 여세요.
2. 탐색 창에서 Transit Gateway Multicast(전송 게이트웨이 멀티캐스트)를 선택합니다.
3. 멀티캐스트 도메인을 선택합니다.
4. 연결 탭을 선택합니다.

Command line

를 사용하여 멀티캐스트 도메인을 보려면 AWS CLI

[describe-transit-gateway-multicast-domain](#) 명령을 사용합니다.

멀티캐스트 도메인에서 서브넷 연결 해제

멀티캐스트 도메인에서 서브넷을 연결 해제하려면 다음 절차를 따릅니다.

Console

콘솔을 사용하여 서브넷의 연결 해제

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 여세요.
2. 탐색 창에서 Transit Gateway Multicast(전송 게이트웨이 멀티캐스트)를 선택합니다.
3. 멀티캐스트 도메인을 선택합니다.
4. 연결 탭을 선택합니다.
5. 서브넷을 선택한 후 작업(Actions), 연결 삭제>Delete association)를 선택합니다.

Command line

를 사용하여 서브넷 연결을 끊으려면 AWS CLI

[disassociate-transit-gateway-multicast-domain](#) 명령을 사용합니다.

멀티캐스트 도메인에 태그 추가

리소스에 태그를 추가하면 용도, 소유자 또는 환경과 같은 기준으로 태그를 구성하고 식별할 수 있습니다. 각 멀티캐스트 도메인에 여러 태그를 추가할 수 있습니다. 태그 키는 각 멀티캐스트 도메인에 대해 고유해야 합니다. 멀티캐스트 도메인에 이미 연결된 키를 통해 태그를 추가하면 해당 태그의 값이 업데이트됩니다. 자세한 내용은 [Amazon EC2 리소스에 태깅](#)을 참조하세요.

Console

콘솔을 사용하여 멀티캐스트 도메인에 태그를 추가하려면

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 여세요.
2. 탐색 창에서 Transit Gateway Multicast(전송 게이트웨이 멀티캐스트)를 선택합니다.
3. 멀티캐스트 도메인을 선택합니다.
4. 작업(Actions), 태그 관리(Manage tags)를 선택합니다.
5. 각 태그에 대해 새 태그 추가(Add new tag)를 선택하고 태그의 키(Key) 및 값(Value)을 입력합니다.
6. 저장(Save)을 선택합니다.

Command line

를 사용하여 멀티캐스트 도메인에 태그를 추가하려면 AWS CLI

[create-tags](#) 명령을 사용합니다.

멀티캐스트 도메인 삭제

멀티캐스트 도메인을 삭제하려면 다음 절차를 따릅니다.

Console

콘솔을 사용하여 멀티캐스트 도메인 삭제

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 여세요.
2. 탐색 창에서 Transit Gateway Multicast(전송 게이트웨이 멀티캐스트)를 선택합니다.
3. 멀티캐스트 도메인을 선택한 다음 작업(Actions), 멀티캐스트 도메인 삭제>Delete multicast domain)를 선택합니다.
4. 확인 메시지가 나타나면 **delete**을 입력한 다음 삭제를 선택합니다.

Command line

를 사용하여 멀티캐스트 도메인을 삭제하려면 AWS CLI

[delete-transit-gateway-multicast-domain](#) 명령을 사용합니다.

멀티캐스트 그룹 관리

목차

- [멀티캐스트 그룹에 소스 등록](#)
- [멀티캐스트 그룹에 멤버 등록](#)
- [멀티캐스트 그룹에서 소스 등록 취소](#)
- [멀티캐스트 그룹에서 멤버 등록 취소](#)
- [멀티캐스트 그룹 보기](#)

멀티캐스트 그룹에 소스 등록

Note

이 절차는 정적 소스 지원(Static sources support) 속성을 활성화(enable)로 설정한 경우에만 필요합니다.

멀티캐스트 그룹에 소스를 등록하려면 다음 절차를 따릅니다. 소스는 멀티캐스트 트래픽을 전송하는 네트워크 인터페이스입니다.

소스를 추가하려면 다음 정보가 필요합니다.

- 멀티캐스트 도메인의 ID
- 소스의 네트워크 인터페이스 ID
- 멀티캐스트 그룹 IP 주소

Console

콘솔을 사용하여 소스를 등록하려면

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 여세요.

2. 탐색 창에서 Transit Gateway Multicast(전송 게이트웨이 멀티캐스트)를 선택합니다.
3. 멀티캐스트 도메인을 선택한 다음 작업(Actions), 그룹 소스 추가(Add group sources)를 선택합니다.
4. Group IP address(그룹 IP 주소)에 멀티캐스트 도메인에 할당할 IPv4 CIDR 블록 또는 IPv6 CIDR 블록을 입력합니다.
5. Choose network interfaces(네트워크 인터페이스 선택)에서 멀티캐스트 발신자의 네트워크 인터페이스를 선택합니다.
6. Add sources(소스 추가)를 선택합니다.

Command line

를 사용하여 소스를 등록하려면 AWS CLI

[register-transit-gateway-multicast-group-sources](#) 명령을 사용합니다.

멀티캐스트 그룹에 멤버 등록

멀티캐스트 그룹에 그룹 멤버를 등록하려면 다음 절차를 따릅니다.

멤버를 추가하려면 다음 정보가 필요합니다.

- 멀티캐스트 도메인의 ID
- 그룹 멤버의 네트워크 인터페이스 ID
- 멀티캐스트 그룹 IP 주소

Console

콘솔을 사용하여 멤버 등록

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 여세요.
2. 탐색 창에서 Transit Gateway Multicast(전송 게이트웨이 멀티캐스트)를 선택합니다.
3. 멀티캐스트 도메인을 선택한 다음 작업(Actions), 그룹 멤버 추가(Add group members)를 선택합니다.
4. Group IP address(그룹 IP 주소)에 멀티캐스트 도메인에 할당할 IPv4 CIDR 블록 또는 IPv6 CIDR 블록을 입력합니다.

5. Choose network interfaces(네트워크 인터페이스 선택)에서 멀티캐스트 수신자의 네트워크 인터페이스를 선택합니다.
6. Add members(멤버 추가)를 선택합니다.

Command line

를 사용하여 멤버를 등록하려면 AWS CLI

[register-transit-gateway-multicast-group-members](#) 명령을 사용합니다.

멀티캐스트 그룹에서 소스 등록 취소

멀티캐스트 그룹에 소스를 수동으로 추가하지 않은 경우 이 절차를 따르지 않아도 됩니다.

Console

콘솔을 사용하여 소스 제거

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 여세요.
2. 탐색 창에서 Transit Gateway Multicast(전송 게이트웨이 멀티캐스트)를 선택합니다.
3. 멀티캐스트 도메인을 선택합니다.
4. 그룹 탭을 선택합니다.
5. 소스를 선택한 다음 Remove source(소스 제거)를 선택합니다.

Command line

를 사용하여 소스를 제거하려면 AWS CLI

[deregister-transit-gateway-multicast-group-sources](#) 명령을 사용합니다.

멀티캐스트 그룹에서 멤버 등록 취소

멀티캐스트 그룹에 멤버를 수동으로 추가하지 않은 경우 이 절차를 따르지 않아도 됩니다.

Console

콘솔을 사용하여 멤버 등록 취소

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 여세요.

2. 탐색 창에서 Transit Gateway Multicast(전송 게이트웨이 멀티캐스트)를 선택합니다.
3. 멀티캐스트 도메인을 선택합니다.
4. 그룹 탭을 선택합니다.
5. 멤버를 선택한 다음 Remove member(멤버 제거)를 선택합니다.

Command line

를 사용하여 구성원 등록을 취소하려면 AWS CLI

[deregister-transit-gateway-multicast-group-members](#) 명령을 사용합니다.

멀티캐스트 그룹 보기

멀티캐스트 그룹에 대한 정보를 보고 IGMPv2 프로토콜을 사용하여 멤버가 검색되었는지 확인할 수 있습니다. 멤버 유형 (콘솔) 또는 MemberType (내) 프로토콜로 멤버가 AWS CLI AWS 검색되면 IGMP가 표시됩니다.

Console

콘솔을 사용하여 멀티캐스트 그룹 보기

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 여세요.
2. 탐색 창에서 Transit Gateway Multicast(전송 게이트웨이 멀티캐스트)를 선택합니다.
3. 멀티캐스트 도메인을 선택합니다.
4. 그룹 탭을 선택합니다.

Command line

를 사용하여 멀티캐스트 그룹을 보려면 AWS CLI

[search-transit-gateway-multicast-groups](#) 명령을 사용합니다.

다음 예제에서는 IGMP 프로토콜이 멀티캐스트 그룹 멤버를 검색한 것을 보여 줍니다.

```
aws ec2 search-transit-gateway-multicast-groups --transit-gateway-multicast-domain tgw-mcast-domain-000fb24d04EXAMPLE
{
  "MulticastGroups": [
    {
```



```

    "GroupIdAddress": "224.0.1.0",
    "TransitGatewayAttachmentId": "tgw-attach-0372e72386EXAMPLE",
    "SubnetId": "subnet-0187aff814EXAMPLE",
    "ResourceId": "vpc-0065acced4EXAMPLE",
    "ResourceType": "vpc",
    "NetworkInterfaceId": "eni-03847706f6EXAMPLE",
    "MemberType": "igmp"
  }
]
}

```

공유 멀티캐스트 도메인 작업

멀티캐스트 도메인 공유를 사용하면 멀티캐스트 도메인 소유자가 해당 도메인을 조직 내, 또는 AWS의 여러 조직에 걸쳐 다른 AWS Organizations 계정과 공유할 수 있습니다. 멀티캐스트 도메인 소유자는 멀티캐스트 도메인을 중앙에서 생성하고 관리할 수 있습니다. 소비자는 공유 멀티캐스트 도메인에서 다음 작업을 수행할 수 있습니다.

- 멀티캐스트 도메인의 그룹 멤버 또는 그룹 소스 등록 및 등록 취소
- 멀티캐스트 도메인에 서브넷 연결 및 멀티캐스트 도메인에서 서브넷 연결 해제

멀티캐스트 도메인 소유자는 멀티캐스트 도메인을 다음과 공유할 수 있습니다.

- 조직 내부 또는 AWS Organizations의 조직에 걸친 AWS 계정
- AWS Organizations에서 조직 내부의 조직 단위
- AWS Organizations의 전체 조직
- AWS Organizations 외부의 AWS 계정.

조직 외부의 AWS 계정과 멀티캐스트 도메인을 공유하려면 AWS Resource Access Manager을 사용해 리소스 공유를 만든 다음, 해당 멀티캐스트 도메인을 공유할 보안 주체를 선택할 때 Allow sharing with anyone(모든 사용자와 공유 허용)을 선택해야 합니다. 리소스 공유 생성에 관한 자세한 정보는 AWS RAM 사용 설명서의 [AWS RAM에서 리소스 공유 생성](#)을 참조하세요.

목차

- [멀티캐스트 도메인 공유를 위한 사전 조건](#)
- [관련 서비스](#)
- [여러 가용 영역 공유](#)

- [멀티캐스트 도메인 공유](#)
- [공유 멀티캐스트 도메인 공유 해제](#)
- [공유 멀티캐스트 도메인 식별](#)
- [공유 멀티캐스트 도메인 권한](#)
- [결제 및 측정](#)
- [할당량](#)

멀티캐스트 도메인 공유를 위한 사전 조건

- 멀티캐스트 도메인을 공유하려면 AWS 계정에서 해당 접두사 목록을 소유해야 합니다. 다른 사용자가 자신과 공유한 멀티캐스트 도메인은 공유할 수 없습니다.
- AWS Organizations의 조직 또는 조직 단위와 접두사 목록을 공유하려면 AWS Organizations와의 공유를 활성화해야 합니다. 자세한 내용은 AWS RAM 사용 설명서의 [AWS Organizations를 사용하여 공유 사용](#)을 참조하세요.

관련 서비스

멀티캐스트 도메인 공유는 AWS Resource Access Manager(AWS RAM)과 통합됩니다. AWS RAM은 모든 AWS 계정 또는 AWS Organizations를 통해 AWS 리소스를 공유할 수 있는 서비스입니다. AWS RAM을 사용하여 리소스 공유로 생성한 사용자 소유 리소스를 공유할 수 있습니다. 리소스 공유는 공유할 리소스와 공유 대상 소비자를 지정합니다. 소비자는 AWS의 개별 AWS Organizations 계정, 조직 단위 또는 전체 조직일 수 있습니다.

AWS RAM에 대한 자세한 내용은 [AWS RAM 사용 설명서](#)를 참조하세요.

여러 가용 영역 공유

리전의 가용 영역에 걸쳐 리소스가 배포될 수 있도록 각 계정의 이름에 가용 영역을 독립적으로 매핑합니다. 이로 인해 계정 전체에서 가용 영역 이름의 차이가 발생할 수 있습니다. 예를 들어 AWS 계정의 us-east-1a 가용 영역은 다른 AWS 계정에 대한 us-east-1a로 위치가 동일하지 않을 수 있습니다.

계정과 관련된 멀티캐스트 도메인의 위치를 확인하려면 가용 영역 ID(AZ ID)를 사용해야 합니다. AZ ID는 모든 AWS 계정의 가용 영역에 대한 고유하고 일관된 식별자입니다. 예를 들어, use1-az1은 us-east-1 리전의 AZ ID이고, 모든 AWS 계정에서 위치가 동일합니다.

계정의 가용 영역에 대한 AZ ID 보는 방법

1. <https://console.aws.amazon.com/ram>에서 콘솔을 엽니다.

2. 현재 지역의 AZ ID는 화면의 오른쪽에 있는 사용자 AZ ID 패널에 표시됩니다.

멀티캐스트 도메인 공유

소유자가 멀티캐스트 도메인을 소비자와 공유하는 경우 소비자는 다음을 수행할 수 있습니다.

- 그룹 멤버 또는 그룹 소스 등록 및 등록 취소
- 서브넷 연결 및 연결 해제

멀티캐스트 도메인을 공유하려면 리소스 공유에 추가해야 합니다. 리소스 공유는 여러 AWS 계정에서 리소스를 공유할 수 있게 해주는 AWS RAM 리소스입니다. 리소스 공유는 공유할 리소스와 공유 대상 소비자를 지정합니다. Amazon Virtual Private Cloud Console을 사용하여 멀티캐스트 도메인을 공유하면 기존 리소스 공유에 추가합니다. 새 리소스 공유에 멀티캐스트 도메인을 추가하려면 먼저 [AWS RAM 콘솔](#)을 사용하여 리소스 공유를 만들어야 합니다.

AWS Organizations의 조직에 속해 있고 조직 내의 공유가 활성화되어 있으면 조직의 소비자에게 공유 접두사 목록에 대한 액세스 권한이 자동으로 부여됩니다. 그렇지 않은 경우 리소스 공유에 가입하라는 초대를 받은 소비자가 초대를 수락하면 공유 멀티캐스트 도메인에 대한 액세스 권한이 부여됩니다.

*Amazon Virtual Private Cloud Console, AWS RAM 콘솔 또는 AWS CLI를 사용하여 자신이 소유한 멀티캐스트 도메인을 공유할 수 있습니다.

*Amazon Virtual Private Cloud Console을 사용하여 사용자가 소유한 멀티캐스트 도메인을 공유하려면

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 멀티캐스트 도메인(Multicast Domains)을 선택합니다.
3. 멀티캐스트 도메인을 선택한 다음 작업(Actions), 멀티캐스트 도메인 공유(Share multicast domain)를 선택합니다.
4. 리소스 공유를 선택하고 멀티캐스트 도메인 공유(Share multicast domain)를 선택합니다.

AWS RAM 콘솔을 사용하여 자신이 소유한 멀티캐스트 도메인 공유

AWS RAM 사용 설명서에서 [리소스 공유 생성](#)을 참조하세요.

AWS CLI를 사용하여 자신이 소유한 멀티캐스트 도메인 공유

[create-resource-share](#) 명령을 사용합니다.

공유 멀티캐스트 도메인 공유 해제

공유 멀티캐스트 도메인이 공유 해제되면 소비자 멀티캐스트 도메인 리소스에 다음과 같은 상황이 발생합니다.

- 소비자 서브넷이 멀티캐스트 도메인에서 연결 해제됩니다. 서브넷은 소비자 계정에 남아 있습니다.
- 소비자 그룹 소스 및 그룹 멤버가 멀티캐스트 도메인에서 연결 해제된 다음 소비자 계정에서 삭제됩니다.

멀티캐스트 도메인을 공유 해제하려면 리소스 공유에서 제거해야 합니다. AWS RAM 콘솔 또는 AWS CLI에서 이 작업을 수행할 수 있습니다.

자신이 소유한 공유 멀티캐스트 도메인을 공유 해제하려면 리소스 공유에서 제거해야 합니다.

*Amazon Virtual Private Cloud Console, AWS RAM 콘솔 또는 AWS CLI를 사용하여 이 작업을 수행할 수 있습니다.

*Amazon Virtual Private Cloud Console을 사용하여 사용자가 소유한 공유 멀티캐스트 도메인의 공유를 해제하려면

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 멀티캐스트 도메인(Multicast Domains)을 선택합니다.
3. 멀티캐스트 도메인을 선택한 다음 작업(Actions), 공유 중지(Stop sharing)를 선택합니다.

AWS RAM 콘솔을 사용하여 자신이 소유한 공유 멀티캐스트 도메인의 공유 해제

AWS RAM 사용 설명서에서 [리소스 공유 업데이트](#)를 참조하세요.

AWS CLI를 사용하여 자신이 소유한 공유 멀티캐스트 도메인 공유 해제

[disassociate-resource-share](#) 명령을 사용합니다.

공유 멀티캐스트 도메인 식별

소유자와 소비자는 *Amazon Virtual Private Cloud Console 및 AWS CLI를 사용하여 공유 멀티캐스트 도메인을 식별할 수 있습니다.

*Amazon Virtual Private Cloud Console을 사용하여 공유 멀티캐스트 도메인을 식별하려면

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.

2. 탐색 창에서 멀티캐스트 도메인(Multicast Domains)을 선택합니다.
3. 멀티캐스트 도메인을 선택합니다.
4. 전송 멀티캐스트 도메인 세부 정보(Transit Multicast Domain Details) 페이지에서 Owner ID(소유자 ID)를 확인하여 멀티캐스트 도메인의 AWS 계정 ID를 식별합니다.

AWS CLI를 사용하여 공유 멀티캐스트 도메인 식별

[describe-transit-gateway-multicast-domains](#) 명령을 사용합니다. 이 명령은 사용자가 소유한 멀티캐스트 도메인과 사용자에게 공유된 멀티캐스트 도메인을 반환합니다. OwnerId에는 멀티캐스트 도메인 소유자의 AWS 계정 ID가 표시됩니다.

공유 멀티캐스트 도메인 권한

소유자에 대한 권한

소유자는 멀티캐스트 도메인과 자신이 도메인에 등록하거나 연결한 멤버 및 연결을 관리할 책임이 있습니다. 소유자는 언제든지 공유 액세스를 변경하거나 취소할 수 있습니다. 소유자는 AWS Organizations를 사용하여 소비자가 공유 멀티캐스트 도메인에서 생성하는 리소스를 보고, 수정하고, 삭제할 수 있습니다.

소비자에 대한 권한

소비자는 자신이 생성한 멀티캐스트 도메인과 동일한 방식으로 공유 멀티캐스트 도메인에 대해 다음 작업을 수행할 수 있습니다.

- 멀티캐스트 도메인의 그룹 멤버 또는 그룹 소스 등록 및 등록 취소
- 멀티캐스트 도메인에 서브넷 연결 및 멀티캐스트 도메인에서 서브넷 연결 해제

소비자는 자신이 공유 멀티캐스트 도메인에 생성한 리소스를 관리할 책임이 있습니다.

소비자는 다른 소비자나 멀티캐스트 도메인 소유자가 소유한 리소스를 보거나 수정할 수 없으며, 자신에게 공유된 멀티캐스트 도메인을 수정할 수 없습니다.

결제 및 측정

소유자 또는 소비자에 대한 멀티캐스트 도메인 공유에는 추가 요금이 없습니다.

할당량

공유 멀티캐스트 도메인은 소유자 및 소비자의 멀티캐스트 도메인 할당량에 포함됩니다.

Transit Gateway 공유 고려 사항

AWS Resource Access Manager(RAM)를 사용하여 VPC 연결용 Transit Gateway를 계정 전체 또는 AWS Organizations의 조직 전체에서 공유할 수 있습니다. RAM을 활성화하고 리소스를 조직과 공유해야 합니다. 자세한 내용은 AWS RAM 사용 설명서에서 [AWS Organizations을\(를\) 사용하여 공유 사용을 참조하세요](#).

Transit Gateway를 공유할 때는 다음 사항을 고려하세요.

- AWS Site-to-Site VPN Site-to-Site VPN 연결은 Transit Gateway를 소유한 AWS 계정에서 생성되어야 합니다.
- Direct Connect 게이트웨이 연결이 Transit Gateway Attachment를 사용하고, Direct Connect 게이트웨이와 동일한 AWS 계정 또는 Direct Connect 게이트웨이와 다른 계정에 있을 수 있습니다.

기본적으로 사용자는 AWS RAM 리소스를 생성 또는 수정할 수 있는 권한이 없습니다. 사용자에게 리소스 생성 또는 수정 및 작업 수행을 허용하려면 특정 리소스 및 API 작업을 사용할 권한을 부여하는 IAM 정책을 생성해야 합니다. 그런 다음 해당 권한이 필요한 IAM 사용자 또는 그룹에 이러한 정책을 연결합니다.

리소스 소유자만 다음 작업을 수행할 수 있습니다.

- 리소스 공유를 생성할 수 있습니다.
- 리소스 공유를 업데이트할 수 있습니다.
- 리소스 공유를 볼 수 있습니다.
- 귀하의 계정이 공유한 리소스를 모든 리소스 공유에 걸쳐 볼 수 있습니다.
- 귀하와 리소스를 공유 중인 보안 주체를 모든 리소스 공유에 걸쳐 볼 수 있습니다. 귀하와 공유 중인 보안 주체를 볼 수 있다면 귀하의 공유 리소스에 누가 액세스할 수 있는지 확인할 수도 있습니다.
- 리소스 공유를 삭제할 수 있습니다.
- 모든 Transit Gateway, Transit Gateway Attachment 및 Transit Gateway 라우팅 테이블 API를 실행합니다.

공유되는 리소스에 대해 다음 작업을 수행할 수 있습니다.

- 리소스 공유 초대를 수락하거나 거부할 수 있습니다.
- 리소스 공유를 볼 수 있습니다.

- 액세스 가능한 공유 리소스를 볼 수 있습니다.
- 귀하와 리소스를 공유 중인 모든 보안 주체의 목록을 볼 수 있습니다. 귀하와 보안 주체가 공유한 리소스와 리소스 공유를 볼 수 있습니다.
- DescribeTransitGateways API를 실행할 수 있습니다.
- VPC에서 연결을 생성 및 설명하는 API(예: CreateTransitGatewayVpcAttachment 및 DescribeTransitGatewayVpcAttachments)를 실행할 수 있습니다.
- 리소스 공유를 나갈 수 있습니다.

Transit Gateway가 공유되면 Transit Gateway 라우팅 테이블 또는 Transit Gateway 라우팅 테이블 전파 및 연관을 생성, 수정 또는 삭제할 수 없습니다.

Transit Gateway를 생성할 때 Transit Gateway는 계정에 매핑되며 다른 계정과는 별도의 가용 영역에서 생성됩니다. Transit Gateway와 연결 개체가 서로 다른 계정에 있는 경우에는 가용 영역 ID를 사용하여 가용 영역을 고유하고 지속적으로 식별합니다. 예를 들어 use1-az1은 us-east-1 리전의 AZ ID이고, 모든 AWS 계정에서 동일한 위치에 매핑됩니다.

Transit Gateway 공유 해제

공유 소유자가 Transit Gateway를 공유 해제하면 다음 규칙이 적용됩니다.

- Transit Gateway Attachment는 계속 작동합니다.
- 공유 계정은 Transit Gateway를 설명할 수 없습니다.
- Transit Gateway 소유자 및 공유 소유자는 Transit Gateway Attachment를 삭제할 수 있습니다.

전송 게이트웨이가 다른 AWS 계정과 공유되지 않거나 전송 게이트웨이가 공유되는 AWS 계정이 조직에서 제거될 경우, 전송 게이트웨이 자체는 영향을 받지 않습니다.

공유 서브넷

VPC 소유자는 공유 VPC 서브넷에 전송 게이트웨이를 연결할 수 있습니다. 참가자는 선택할 수 없습니다. 참여자의 리소스에서 오는 트래픽은 VPC 소유자가 공유 VPC 서브넷에 설정한 경로에 따라 첨부 파일을 사용할 수 있습니다.

자세한 내용은 Amazon VPC 사용 설명서의 [다른 계정과 VPC 공유하기](#)를 참조하세요.

Transit Gateway 흐름 로그를 사용하여 네트워크 트래픽 로깅

전송 게이트웨이 흐름 로그는 전송 게이트웨이로 들어오고 나가는 IP 트래픽에 대한 정보를 캡처할 수 있는 기능입니다. 플로우 로그 데이터는 Amazon CloudWatch Logs, Amazon S3 또는 Firehose에 게시할 수 있습니다. 흐름 로그를 생성한 다음 선택된 대상의 데이터를 가져와 확인할 수 있습니다. 흐름 로그 데이터는 네트워크 트래픽 경로 외부에서 수집되므로 네트워크 처리량이나 지연 시간에 영향을 주지 않습니다. 네트워크 성능에 영향을 주지 않고 흐름 로그를 생성하거나 삭제할 수 있습니다. 전송 게이트웨이 흐름 로그는 [the section called “전송 게이트웨이 흐름 로그 레코드”](#)에 설명된 대로 전송 게이트웨이에 관련된 정보만 캡처합니다. VPC의 네트워크 인터페이스에서 송수신되는 IP 트래픽에 대한 정보를 캡처하려면 VPC 흐름 로그를 사용합니다. 자세한 내용은 Amazon VPC 사용 설명서의 [VPC 흐름 로그를 사용하여 IP 트래픽 로깅](#)을 참조하세요.

Note

전송 게이트웨이 흐름 로그를 생성하려면 전송 게이트웨이의 소유자여야 합니다. 소유자가 아닌 경우 트랜짓 게이트웨이 소유자가 권한을 부여해야 합니다.

모니터링된 전송 게이트웨이의 흐름 로그 데이터는 트래픽 흐름을 설명하는 필드로 구성된 로그 이벤트인 흐름 로그 레코드로 기록됩니다. 자세한 정보는 [전송 게이트웨이 흐름 로그 레코드](#)을 참조하세요.

흐름 로그를 생성하려면 다음을 지정합니다.

- 흐름 로그를 생성할 리소스
- 흐름 로그 데이터를 게시할 대상

흐름 로그를 생성한 후에는, 데이터를 수집하여 선택된 대상에 게시하는 데 몇 분의 시간이 소요될 수 있습니다. 흐름 로그는 전송 게이트웨이에 대한 실시간 로그 스트림을 캡처하지 않습니다. 자세한 정보는 [흐름 로그 생성](#)을 참조하세요.

흐름 로그에 태그를 적용할 수 있습니다. 각 태그는 사용자가 정의하는 키와 선택적 값으로 구성됩니다. 태그는 흐름 로그를 용도나 소유자별로 구성하는 데 도움이 될 수 있습니다.

흐름 로그가 더 이상 필요하지 않을 경우 삭제할 수 있습니다. 흐름 로그를 삭제하면 리소스에 대한 흐름 로그 서비스가 비활성화되고 새 흐름 로그 레코드가 생성되거나 CloudWatch Logs 또는 Amazon S3에 게시되지 않습니다. 흐름 로그를 삭제해도 전송 게이트웨이의 기존 흐름 로그 레코드 또는 로그 스트림 (CloudWatch 로그용) 또는 로그 파일 객체 (Amazon S3의 경우) 는 삭제되지 않습니다. 기존 로그 스트림을 삭제하려면 CloudWatch Logs 콘솔을 사용하십시오. 기존 로그 파일 객체를 삭제하려면

Amazon S3 콘솔을 사용합니다. 흐름 로그를 삭제한 후 데이터 수집이 중단되기까지 몇 분 정도 시간이 걸릴 수 있습니다. 자세한 정보는 [흐름 로그 삭제](#)를 참조하세요.

제한 사항

Transit Gateway 흐름 로그에는 다음과 같은 제한이 적용됩니다.

- 멀티캐스트 트래픽은 지원되지 않습니다.
- 연결 연결은 지원되지 않습니다. 모든 Connect 흐름 로그는 전송 첨부 파일 아래에 표시되므로 전송 게이트웨이 또는 Connect 전송 첨부 파일에서 활성화해야 합니다.

전송 게이트웨이 흐름 로그 레코드

흐름 로그 레코드는 전송 게이트웨이에 네트워크 흐름을 나타냅니다. 각 레코드는 필드가 공백으로 구분되어 있는 문자열입니다. 레코드에는 소스, 대상, 프로토콜 등 트래픽 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

흐름 로그를 생성할 때 흐름 로그 레코드의 기본 형식을 사용하거나 사용자 지정 형식을 지정할 수 있습니다.

내용

- [기본 형식](#)
- [사용자 지정 형식](#)
- [사용 가능한 필드](#)

기본 형식

기본 형식의 흐름 로그 레코드에는 [사용 가능한 필드](#) 테이블에 표시되는 순서대로 모든 버전 2~6 필드가 포함됩니다. 기본 형식을 사용자 정의하거나 변경할 수 없습니다. 추가 필드 또는 다른 필드 하위 세트를 캡처하려면 사용자 지정 형식을 지정합니다.

사용자 지정 형식

사용자 지정 형식을 사용하면 흐름 로그 레코드에 포함되는 필드와 그 순서를 지정할 수 있습니다. 이를 통해 요구 사항에 맞는 흐름 로그를 만들고 관련이 없는 필드를 생략할 수 있습니다. 사용자 지정 형식을 사용하면 게시된 흐름 로그에서 특정 정보를 추출하기 위해 별도의 프로세스가 필요하지 않습니다. 사용 가능한 흐름 로그 필드를 얼마든지 지정할 수 있지만 하나 이상을 지정해야 합니다.

사용 가능한 필드

다음 표는 전송 게이트웨이 흐름 로그 레코드에 사용 가능한 모든 필드를 설명합니다. 버전 열은 필드가 도입된 버전을 나타냅니다.

Amazon S3 흐름 로그 데이터를 게시할 때 필드의 데이터 유형은 흐름 로그 형식에 따라 다릅니다. 형식이 일반 텍스트인 경우 모든 필드는 STRING 유형입니다. 형식이 Parquet 인 경우 필드 데이터 유형에 대한 표를 참조하십시오.

필드를 적용할 수 없거나 특정 레코드에 대해 계산할 수 없는 경우 레코드는 해당 항목에 대해 '.' 기호를 표시합니다. 패킷 헤더에서 직접 제공되지 않는 메타데이터 필드는 최선의 작업 수준 근사값이며 해당 값이 누락되거나 정확하지 않을 수 있습니다.

필드	설명	버전
version	해당 필드가 도입된 버전을 나타냅니다. 기본 형식에는 모든 버전 2 필드가 테이블에 표시되는 순서와 동일하게 포함됩니다. Parquet 데이터 유형: INT_32	2
resource-type	구독이 생성되는 리소스 유형입니다. Transit Gateway 플로우 로그의 경우 다음과 같습니다TransitGateway. Parquet 데이터 유형: 문자열	6
account-id	소스 트랜짓 게이트웨이 소유자의 AWS 계정 ID. Parquet 데이터 유형: 문자열	2
tgw-id	트래픽이 기록되는 전송 게이트웨이의 ID입니다. Parquet 데이터 유형: 문자열	6
tgw-attachment-id	트래픽이 기록되는 Transit Gateway Attachment의 ID입니다. Parquet 데이터 유형: 문자열	6
tgw-src-vpc-account-id	소스 VPC 트래픽의 AWS 계정 ID입니다. Parquet 데이터 유형: 문자열	6

필드	설명	버전
tgw-dst-vpc-account-id	대상 VPC 트래픽의 AWS 계정 ID입니다. Parquet 데이터 유형: 문자열	6
tgw-src-vpc-id	전송 게이트웨이에 대한 소스 VPC의 ID Parquet 데이터 유형: 문자열	6
tgw-dst-vpc-id	전송 게이트웨이에 대한 대상 VPC의 ID입니다. Parquet 데이터 유형: 문자열	6
tgw-src-subnet-id	전송 게이트웨이 소스 트래픽의 서브넷 ID입니다. Parquet 데이터 유형: 문자열	6
tgw-dst-subnet-id	전송 게이트웨이 대상 트래픽의 서브넷 ID입니다. Parquet 데이터 유형: 문자열	6
tgw-src-eni	흐름에 대한 소스 Transit Gateway Attachment ENI의 ID. Parquet 데이터 유형: 문자열	6
tgw-dst-eni	해당 흐름에 대한 대상 Transit Gateway Attachment ENI의 ID입니다. Parquet 데이터 유형: 문자열	6
tgw-src-az-id	트래픽이 기록되는 소스 전송 게이트웨이가 포함된 가용 영역의 ID입니다. 하위 위치에서 트래픽이 발생한 경우 레코드는 이 필드에 대해 '-' 기호를 표시합니다. Parquet 데이터 유형: 문자열	6
tgw-dst-az-id	트래픽이 기록되는 대상 전송 게이트웨이가 포함된 가용 영역의 ID입니다. Parquet 데이터 유형: 문자열	6

필드	설명	버전
tgw-pair-attachment-id	흐름 방향에 따라 흐름의 송신 또는 수신 연결 ID가 됩니다. Parquet 데이터 유형: 문자열	6
srcaddr	수신 트래픽의 소스 주소입니다. Parquet 데이터 유형: 문자열	2
dstaddr	발신 트래픽의 대상 주소입니다. Parquet 데이터 유형: 문자열	2
srcport	트래픽의 소스 포트 Parquet 데이터 유형: INT_32	2
dstport	트래픽의 대상 포트 Parquet 데이터 유형: INT_32	2
protocol	트래픽의 IANA 프로토콜 번호. 자세한 정보는 지정된 인터넷 프로토콜 번호 단원을 참조하십시오. Parquet 데이터 유형: INT_64	2
packets	흐름 중 전송된 패킷 수. Parquet 데이터 유형: INT_64	2
bytes	흐름 중 전송된 바이트 수. Parquet 데이터 유형: INT_64	2
start	흐름의 첫 번째 패킷이 집계 간격 내에서 수신된 시간(단위: Unix 초)입니다. 전송 게이트웨이에서 패킷을 전송하거나 수신한 후 최대 60 초일 수 있습니다. Parquet 데이터 유형: INT_64	2

필드	설명	버전
end	<p>집계 간격 내에서 흐름의 마지막 패킷을 수신한 시간(단위: Unix 초)입니다. 전송 게이트웨이에서 패킷을 전송하거나 수신한 후 최대 60 초일 수 있습니다.</p> <p>Parquet 데이터 유형: INT_64</p>	2
log-status	<p>흐름 로그의 상태:</p> <ul style="list-style-type: none"> • OK — 데이터가 선택된 대상에 정상적으로 로깅됩니다. • NODATA — 집계 간격 중 네트워크 인터페이스에서 전송되거나 수신된 네트워크 트래픽이 없습니다. • SKIPDATA — 집계 간격 중 일부 흐름 로그 레코드를 건너뛰었습니다. 내부 용량 제한 또는 내부 오류가 원인일 수 있습니다. <p>Parquet 데이터 유형: 문자열</p>	2
type	<p>트래픽 유형입니다. 가능한 값은 IPv4, IPv6 및 EFA입니다. 자세한 내용은 Amazon EC2 사용 설명서의 엘라스틱 패브릭 어댑터를 참조 하십시오.</p> <p>Parquet 데이터 유형: 문자열</p>	3
packets-lost-no-route	<p>경로가 지정되지 않아 패킷이 손실되었습니다.</p> <p>Parquet 데이터 유형: INT_64</p>	6
packets-lost-blackhole	<p>블랙홀로 인해 패킷이 손실되었습니다.</p> <p>Parquet 데이터 유형: INT_64</p>	6
packets-lost-mtu-exceeded	<p>크기가 MTU를 초과하여 패킷이 손실되었습니다.</p> <p>Parquet 데이터 유형: INT_64</p>	6
packets-lost-ttl-expired	<p>의 만료로 인해 패킷이 손실되었습니다. time-to-live</p> <p>Parquet 데이터 유형: INT_64</p>	6

필드	설명	버전
tcp-flags	<p>다음 TCP 플래그의 비트 마스크 값:</p> <ul style="list-style-type: none"> • FIN — 1 • SYN — 2 • RST — 4 • PSH — 8 • ACK — 16 • SYN-ACK — 18 • URG — 32 <div style="border: 1px solid #f08080; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p>⚠ Important</p> <p>흐름 로그 항목이 ACK 패킷으로만 구성된 경우 플래그 값은 16이 아닌 0입니다.</p> </div> <p>TCP 플래그에 대한 일반 정보(예: FIN, SYN 및 ACK와 같은 플래그의 의미)는 Wikipedia에서 TCP 세그먼트 구조를 참조하십시오.</p> <p>TCP 플래그는 집계 간격 동안 OR일 수 있습니다. 짧은 연결의 경우 SYN-ACK 및 FIN에 대해 19, SYN 및 FIN에 대해 3과 같이 흐름 로그 레코드의 동일한 행에 플래그가 설정될 수 있습니다.</p> <p>Parquet 데이터 유형: INT_32</p>	3
region	<p>트래픽이 기록되는 전송 게이트웨이를 포함하는 리전입니다.</p> <p>Parquet 데이터 유형: 문자열</p>	4
flow-direction	<p>트래픽이 캡처되는 인터페이스에 대한 흐름 방향입니다. 가능한 값: ingress egress</p> <p>Parquet 데이터 유형: 문자열</p>	5

필드	설명	버전
pkt-src-aws-service	<p>IP 주소 하위 집합의 이름은 소스 IP 주소가 서비스용인 srcaddr AWS 경우에 사용됩니다. 가능한 값: AMAZON AMAZON_AP FLOW AMAZON_CONNECT API_GATEWAY CHIME_MEE TINGS CHIME_VOICECONNECTOR CLOUD9 CLOUDFRON T CODEBUILD DYNAMODB EBS EC2 EC2_INSTA NCE_CONNECT GLOBALACCELERATOR KINESIS_V IDEO_STREAMS ROUTE53 ROUTE53_HEALTHCHECKS ROUTE53_HEALTHCHECKS_PUBLISHING ROUTE53_R ESOLVER S3 WORKSPACES_GATEWAYS.</p> <p>Parquet 데이터 유형: 문자열</p>	5
pkt-dst-aws-service	<p>대상 IP 주소가 서비스용인 경우 dstaddr 필드의 IP 주소 범위 하위 집합 이름. AWS 가능한 값 목록은 pkt-src-aws-service 필드를 참조 하십시오.</p> <p>Parquet 데이터 유형: 문자열</p>	5

Transit Gateway 흐름 로그 요금

Transit Gateway 흐름 로그를 게시하면 벤딩 로그에 대한 데이터 모으기 및 스토리지 요금이 적용됩니다. 벤딩 로그를 게시할 때의 요금에 대한 자세한 내용을 보려면 [Amazon CloudWatch Pricing](#)을 열고 유료 티어에서 로그를 선택하고 벤딩 로그를 찾으십시오.

Logs에 게시하는 흐름 로그를 생성하십시오. CloudWatch

흐름 로그는 흐름 로그 데이터를 Amazon에 직접 게시할 수 CloudWatch 있습니다.

CloudWatch Logs에 게시되면 흐름 로그 데이터가 로그 그룹에 게시되고 각 트랜짓 게이트웨이는 로 그 그룹에 고유한 로그 스트림을 가집니다. 로그 스트림에는 흐름 로그 레코드가 포함됩니다. 여러 개 의 흐름 로그를 생성하여, 그 데이터를 같은 로그 그룹에 게시할 수 있습니다. 같은 로그 그룹의 하나 이 상의 흐름 로그에 동일한 전송 게이트웨이가 있는 경우 하나의 결합된 로그 스트림이 있습니다. 한 흐 름 로그에서는 거부된 트래픽을 캡처하고, 다른 흐름 로그에서는 허용된 트래픽을 캡처하도록 지정한 경우, 병합된 로그 스트림은 모든 트래픽을 캡처합니다.

흐름 로그를 Logs에 게시할 때는 벤디드 로그의 데이터 수집 및 보관 요금이 적용됩니다. CloudWatch 자세한 내용은 [Amazon CloudWatch 요금을](#) 참조하십시오.

CloudWatch 로그에서 타임스탬프 필드는 흐름 로그 레코드에 캡처된 시작 시간에 해당합니다. IngestionTime 필드는 로그에서 흐름 로그 레코드를 수신한 날짜 및 시간을 제공합니다. CloudWatch 타임스탬프는 흐름 로그 레코드에 캡처된 종료 시간보다 이후입니다.

CloudWatch 로그에 대한 자세한 내용은 Amazon Logs 사용 설명서의 [CloudWatch 로그로 전송된 CloudWatch 로그를](#) 참조하십시오.

내용

- [플로우 로그를 로그에 게시하기 CloudWatch 위한 IAM 역할](#)
- [IAM 사용자가 역할을 전달할 수 있는 권한](#)
- [Logs에 게시하는 흐름 로그를 생성하십시오. CloudWatch](#)
- [로그에서 흐름 로그 기록을 처리합니다. CloudWatch](#)

플로우 로그를 로그에 게시하기 CloudWatch 위한 IAM 역할

흐름 로그와 관련된 IAM 역할에는 Logs의 지정된 로그 그룹에 흐름 로그를 게시할 수 있는 충분한 권한이 있어야 합니다. CloudWatch IAM 역할은 사용자의 역할이어야 합니다. AWS 계정

IAM 역할에 연결된 IAM 정책에는 최소한 다음과 같은 권한이 포함되어야 합니다.

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


또한 귀하의 역할에 흐름 로그 서비스의 역할 수임을 허용하는 신뢰 관계가 포함되어 있는지 확인해야 합니다.

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

[혼동된 대리자 문제](#)로부터 자신을 보호하기 위하여 `aws:SourceAccount` 및 `aws:SourceArn` 조건 키를 사용할 것을 권장합니다. 예를 들어 이전 신뢰 정책에 다음 조건 블록을 추가할 수 있습니다. 소스 계정은 흐름 로그의 소유자이고 소스 ARN은 흐름 로그 ARN입니다. 흐름 로그 ID를 모르는 경우 ARN의 해당 부분을 와일드카드(*)로 바꾼 다음 흐름 로그를 만든 후 정책을 업데이트할 수 있습니다.

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

흐름 로그에 대한 IAM 역할 생성 또는 업데이트

이미 존재하는 역할을 업데이트하거나 흐름 로그를 사용할 수 있도록 새로운 역할을 만들기 위해서 다음 절차를 따라하실 수 있습니다.

흐름 로그에 대한 IAM 역할 생성

1. <https://console.aws.amazon.com/iam/>에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 Roles(역할), Create role(역할 생성)을 선택합니다.
3. 신뢰할 수 있는 엔터티 유형 선택(Select type of trusted entity)에서 AWS 서비스(service)를 선택합니다. 사용 사례(Use case)에서 EC2를 선택합니다. 다음을 선택합니다.

4. Add permissions(권한 추가) 페이지에서 Next: Tags(다음: 태그)를 선택하고 선택 사항으로써 태그를 추가합니다. 다음을 선택합니다.
5. 이름, 검토 및 작성 페이지에 역할 이름을 입력하고 선택적으로 Description(설명)을 제공합니다. 역할 생성을 선택합니다.
6. 역할 이름을 선택합니다. Add permissions(권한 추가) 탭에서 Create inline policy(인라인 정책 생성)을 선택하고 JSON 탭을 선택합니다.
7. [플로우 로그를 로그에 게시하기 CloudWatch 위한 IAM 역할](#)에서 첫 번째 정책을 복사한 후 창에 붙여 넣습니다. 정책 검토(Review policy)를 선택합니다.
8. 정책 이름을 입력하고 정책 생성(Create policy)을 선택합니다.
9. 역할 이름을 선택합니다. 신뢰 관계(Trust Relationships)로 들어가려면 신뢰 관계 편집(Edit Trust Relationship)을 선택합니다. 기존 정책 문서의 서비스 항목을 `ec2.amazonaws.com`에서 `vpc-flow-logs.amazonaws.com`로 바꾸어 주십시오. 신뢰 정책 업데이트(Update Trust Policy)를 선택합니다.
10. 요약 페이지에서 사용자 역할에 대한 ARN을 확인합니다. 사용자의 흐름 로그를 만들 때 이 ARN이 필요합니다.

IAM 사용자가 역할을 전달할 수 있는 권한

또한 사용자에게 해당 흐름 로그와 연결된 IAM 역할에 대한 `iam:PassRole` 작업의 사용 권한이 있어야 합니다.

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

Logs에 게시하는 흐름 로그를 생성하십시오. CloudWatch

전송 게이트웨이에 대한 흐름 로그를 생성할 수 있습니다. IAM 사용자로 이러한 단계를 수행하는 경우 `iam:PassRole` 작업을 사용할 수 있는 권한이 있는지 확인하십시오. 자세한 정보는 [IAM 사용자가 역할을 전달할 수 있는 권한](#)을 참조하세요.

콘솔을 사용하여 전송 게이트웨이 생성

1. AWS Management Console [로그인하고 https://console.aws.amazon.com/vpc/](https://console.aws.amazon.com/vpc/) 에서 [Amazon VPC 콘솔을 엽니다.](#)
2. 탐색 창에서 Transit Gateway를 선택합니다.
3. 하나 이상의 전송 게이트웨이의 확인란을 선택하고 작업(Actions), 흐름 로그 생성(Create flow log)을 선택합니다.
4. [대상] 에서 [CloudWatch로그로 보내기] 를 선택합니다.
5. 대상 로그 그룹에서 현재 대상 로그 그룹의 이름을 선택합니다.

Note

대상 로그 그룹이 아직 없는 경우 이 필드에 새 이름을 입력하면 새 대상 로그 그룹이 생성됩니다.

6. IAM 역할의 경우 로그를 로그에 게시할 권한이 있는 역할의 이름을 지정합니다. CloudWatch
7. 로그 레코드 형식(Log record format)에서 흐름 로그 레코드의 형식을 선택합니다.
 - 기본 형식을 사용하려면 AWS 기본 형식(default format)을 선택하세요.
 - 사용자 지정 형식을 사용하려면 사용자 지정 형식(Custom format)을 선택하고 로그 형식(Log format)에서 필드를 선택합니다.
8. (선택 사항) 새 태그 추가(Add new tag)를 선택하여 흐름 로그에 태그를 적용합니다.
9. 흐름 로그 생성(Create flow log)을 선택합니다.

명령줄을 사용하여 흐름 로그를 만들려면 다음을 수행합니다.

다음 명령 중 하나를 사용합니다.

- [create-flow-logs](#)(AWS CLI)
- [New-EC2FlowLogs](#) (AWS Tools for Windows PowerShell)
- [CreateFlow로그](#) (아마존 EC2 쿼리 API)

다음 AWS CLI 예제는 트랜짓 게이트웨이 정보를 캡처하는 흐름 로그를 생성합니다. 흐름 로그는 IAM 역할을 사용하여 계정 123456789101이라는 CloudWatch my-flow-logs 로그의 로그 그룹에 전달됩니다. 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
```

로그에서 흐름 로그 기록을 처리합니다. CloudWatch

CloudWatch Logs에서 수집한 다른 로그 이벤트와 마찬가지로 흐름 로그 레코드로 작업할 수 있습니다. 로그 데이터 및 지표 필터 모니터링에 대한 자세한 내용은 Amazon CloudWatch User Guide의 [로그 데이터 검색 및 필터링](#)을 참조하십시오.

예: 흐름 로그에 대한 CloudWatch 지표 필터 및 경고 생성

이 예에서는 tgw-123abc456bca에 대한 흐름 로그를 사용합니다. TCP 포트 22(SSH)를 거쳐 인스턴스에 연결하려는 시도가 한 시간 내에 10번 이상 거부된 경우 이를 알려 주는 알림을 만들 수 있습니다. 우선 경보를 만들려는 트래픽의 패턴과 일치하는 지표 필터를 만들어야 합니다. 그런 다음 지표 필터에 대한 경보를 만듭니다.

거부된 SSH 트래픽에 대한 지표 필터와 필터에 대한 경보를 만들려면

1. <https://console.aws.amazon.com/cloudwatch/>에서 CloudWatch 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 로그, 로그 그룹을 선택합니다.
3. 로그 그룹에 대한 확인란을 선택한 다음 작업(Actions), 지표 필터 생성(Create metric filter)을 선택합니다.
4. 필터 패턴(Filter Pattern)에 다음을 입력합니다.

```
[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. 테스트할 로그 데이터 선택(Select log data to test)에서 전송 게이트웨이에 대한 로그 스트림을 선택합니다. (선택 사항) 필터 패턴과 일치하는 로그 데이터 행을 보려면 패턴 테스트를 선택합니다. 준비가 되면 다음을 선택합니다.
6. 필터 이름, 지표 네임스페이스 및 지표 이름을 입력합니다. 지표 값을 **1**로 설정합니다. 완료되면 다음을 선택하고 지표 필터 생성을 선택합니다.

7. 탐색 창에서 경보, 모든 경보를 선택합니다.
8. Create alarm(경보 생성)을 선택하세요.
9. 앞에서 생성한 지표 필터에 대한 네임스페이스를 선택합니다.

새로운 지표가 콘솔에 표시될 때까지 몇 분 정도 걸릴 수 있습니다.

10. 생성한 지표 이름을 선택한 후 지표 선택을 선택합니다.
11. 경보를 다음과 같이 구성한 다음 다음(Next)을 선택합니다.
 - Statistic(통계)에서 Sum(합계)를 선택합니다. 이것으로 지정된 기간 동안 데이터 포인트의 총 수를 캡처할 수 있습니다.
 - 기간에서 1시간을 선택합니다.
 - 항상에서 초과/같음을 선택하고 임계값으로 **10**을 입력합니다.
 - 추가 구성(Additional configuration)에서 경보에 대한 데이터 포인트(Datapoints to alarm)를 기본값 **1**로 남겨둡니다.
12. 알림(Notification)에서 기존 SNS 주제를 선택하거나 새 주제 생성(Create new topic)을 선택하여 새로 생성합니다. 다음(Next)을 선택합니다.
13. 경보의 이름과 설명을 입력하고 다음을 선택합니다.
14. 경보 구성이 완료되면 경보 생성을 선택합니다.

Amazon S3에 게시하는 흐름 로그 생성

흐름 로그는 흐름 로그 데이터를 Amazon S3에 게시할 수 있습니다.

Amazon S3에 게시하는 경우 흐름 로그 데이터가 지정해 놓은 기존 Amazon S3 버킷에 게시됩니다. 모니터링되는 모든 전송 게이트웨이에 대한 흐름 로그 레코드는 버킷에 저장된 일련의 로그 파일 객체에 게시됩니다.

Amazon S3에 흐름 로그를 게시할 때 벤드 Amazon CloudWatch 로그에 데이터 수집 및 보관 요금이 적용됩니다. 판매 로그의 CloudWatch 요금에 대한 자세한 내용을 보려면 [Amazon CloudWatch Pricing](#)을 열고 로그를 선택한 다음 Vended Logs를 찾으십시오.

흐름 로그와 함께 사용할 Amazon S3 버킷을 만드는 방법은 Amazon Simple Storage Service 사용 설명서의 [버킷 생성](#)을 참조하세요.

다중 계정 로깅에 대한 자세한 내용은 AWS 솔루션 라이브러리의 [중앙 로깅](#)을 참조하세요.

CloudWatch 로그에 대한 자세한 내용은 Amazon Logs 사용 설명서의 [Amazon S3로 전송된 CloudWatch 로그](#)를 참조하십시오.

내용

- [흐름 로그 파일](#)
- [Amazon S3에 플로우 로그를 게시하는 IAM 보안 주체에 대한 IAM 정책](#)
- [Amazon S3 버킷의 흐름 로그에 대한 권한](#)
- [SSE-KMS를 사용할 경우 필요한 키 정책](#)
- [Amazon S3 로그 파일 권한](#)
- [Amazon S3에 게시하는 흐름 로그 생성](#)
- [Amazon S3에서 흐름 로그 레코드 처리](#)

흐름 로그 파일

VPC 흐름 로그는 흐름 로그 레코드를 수집하여 로그 파일로 통합한 다음 해당 로그 파일을 5분 간격으로 Amazon S3 버킷에 게시하는 기능입니다. 각 로그 파일에는 이전 5분 동안 기록된 IP 트래픽에 대한 흐름 로그 레코드가 포함됩니다.

로그 파일의 최대 크기는 75MB입니다. 로그 파일이 5분 내에 파일 크기 제한에 도달하면 흐름 로그가 흐름 로그 레코드 추가를 중지합니다. 그런 다음 흐름 로그를 Amazon S3 버킷에 게시하고 새 로그 파일을 만듭니다.

Amazon S3에서 흐름 로그 파일의 마지막 수정(Last modified) 필드는 파일이 Amazon S3 버킷에 업로드된 날짜와 시간을 나타냅니다. 파일 이름의 타임스탬프보다 이후이며 파일을 Amazon S3 버킷에 업로드하는 데 걸리는 시간에 따라 다릅니다.

로그 파일 형식

로그 파일에 대해 다음 형식 중 하나를 지정할 수 있습니다. 각 파일은 단일 Gzip 파일로 압축됩니다.

- 텍스트(Text) – 일반 텍스트. 이것은 기본 형식입니다.
- Parquet – Apache Parquet은 열 기반 데이터 형식입니다. Parquet 형식의 데이터에 대한 쿼리는 일반 텍스트 데이터에 대한 쿼리에 비해 10배에서 100배 빠릅니다. Gzip 압축을 사용하는 Parquet 형식 데이터는 Gzip 압축을 사용하는 일반 텍스트보다 스토리지 공간을 20% 적게 사용합니다.

로그 파일 옵션

필요한 경우 다음과 같은 옵션을 지정할 수 있습니다.

- Hive 호환 S3 접두사 – 분할을 Hive 호환 도구로 가져오는 대신 Hive 호환 접두사를 활성화합니다. 쿼리 실행 전에 MSCK REPAIR TABLE 명령을 사용합니다.
- 시간당 분할 – 대량의 로그가 있고 일반적으로 특정 시간까지 쿼리를 타겟팅하는 경우 로그를 시간 별로 분할하여 더 결과를 빠르게 얻고 쿼리 비용을 절감할 수 있습니다.

로그 파일 S3 버킷 구조

로그 파일은 흐름 로그의 ID, 리전, 생성된 날짜 및 대상 옵션에 따라 폴더 구조를 사용하여 지정된 Amazon S3 버킷에 저장됩니다.

기본적으로 파일은 다음 위치로 전달됩니다.

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

Hive 호환 S3 접두사를 사용하도록 설정하면 파일이 다음 위치로 전달됩니다.

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

시간별 분할을 사용하도록 설정하면 파일이 다음 위치로 전달됩니다.

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

Hive 호환 분할을 사용하도록 설정하고 시간당 흐름 로그를 분할하면 파일이 다음 위치로 전달됩니다.

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

로그 파일 이름

로그 파일의 파일 이름은 흐름 로그 ID, 리전 및 생성 날짜 및 시간을 기반으로 합니다. 파일 이름은 다음 형식을 사용합니다.

```
aws_account_id_vpcflowlogs_region_flow_log_id_YYYYMMDDTHHmmZ_hash.log.gz
```

예를 들어, 다음은 June 20, 2018, 16:20 UTC에 us-east-1 리전의 리소스에 대해 AWS 계정 123456789012에서 생성한 흐름 로그에 대한 로그 파일의 예를 보여 줍니다. 종료 시간이 16:20:00에서 16:24:59 사이인 흐름 로그 레코드가 파일에 포함됩니다.

```
123456789012_vpcflowlogs_us-east-1_f1-1234abcd_20180620T1620Z_fe123456.log.gz
```

Amazon S3에 플로우 로그를 게시하는 IAM 보안 주체에 대한 IAM 정책

흐름 로그를 생성하는 IAM 보안 주체에는 대상 Amazon S3 버킷에 흐름 로그를 게시하는 데 필요한 다음 권한이 있어야 합니다.

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

Amazon S3 버킷의 흐름 로그에 대한 권한

기본적으로 Amazon S3 버킷과 버킷에 포함된 객체는 비공개입니다. 버킷 소유자만이 해당 버킷과 그 안에 저장된 객체에 액세스할 수 있습니다. 그러나 버킷 소유자는 액세스 정책을 작성하여 다른 리소스 및 사용자에게 액세스 권한을 부여할 수 있습니다.

흐름 로그를 생성하는 사용자가 버킷을 소유하고 해당 버킷에 대한 PutBucketPolicy 및 GetBucketPolicy 권한을 소유한 경우, 다음 정책을 해당 버킷에 자동으로 연결합니다. 이 정책은 버킷에 연결된 모든 기존 정책을 덮어씁니다.

그렇지 않으면 버킷 소유자가 이 정책을 버킷에 추가하고 흐름 로그 작성자의 AWS 계정 ID 지정 또는 흐름 로그 생성이 실패합니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 [버킷 정책 사용](#)을 참조하세요.

```
{
```



```

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

```

*my-s3-arn*에 지정한 ARN은 Hive 호환 S3 접두사를 사용하는지 여부에 따라 다릅니다.

- 기본 접두사

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

- Hive 호환 S3 접두사

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

모범 사례로서 개별 AWS 계정 ARN 대신 로그 전송 서비스 보안 주체에 이러한 권한을 부여하는 것이 좋습니다. 또한 [혼동된 대리자 문제](#)로부터 보호하려면 `aws:SourceAccount` 및 `aws:SourceArn` 조건 키를 사용하는 것 좋습니다. 소스 계정은 흐름 로그의 소유자이고 원본 ARN은 로그 서비스의 와일드카드(*) ARN입니다.

SSE-KMS를 사용할 경우 필요한 키 정책

Amazon S3-관리형 키(SSE-S3)를 사용한 서버 측 암호화 또는 KMS 키(SSE-KMS)를 사용한 서버 측 암호화를 활성화하여 Amazon S3 버킷의 데이터를 보호할 수 있습니다. 자세한 내용은 Amazon S3 사용 설명서의 [서버 측 암호화를 사용하여 데이터 보호](#)를 참조하세요.

SSE-KMS에서는 AWS 관리 키 또는 고객 관리 키를 사용할 수 있습니다. AWS 관리형 키의 경우 계정 간 전송을 사용할 수 없습니다. 흐름 로그는 로그 배달 계정에서 전달되므로 교차 계정 전달에 대한 액세스 권한을 부여해야 합니다. S3 버킷에 대한 교차 계정 액세스 권한을 부여하려면 버킷 암호화를 활성화할 때 고객 관리형 키를 사용하고 고객 관리형 키의 Amazon 리소스 이름(ARN)을 지정합니다. 자세한 내용은 Amazon S3 사용 설명서의 [AWS KMS를 사용한 서버 측 암호화 지정](#)을 참조하세요.

고객 관리형 키에서 SSE-KMS를 사용할 때는 S3 버킷의 버킷 정책이 아니라 키의 키 정책에 다음을 추가해야 VPC 흐름 로그가 S3 버킷에 쓸 수 있습니다.

```
{
  "Sid": "Allow Transit Gateway Flow Logs to use the key",
  "Effect": "Allow",
  "Principal": {
    "Service": [
      "delivery.logs.amazonaws.com"
    ]
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "*"
}
```

Amazon S3 로그 파일 권한

필요한 버킷 정책 외에도, Amazon S3는 ACL(액세스 제어 목록)을 사용하여 흐름 로그에서 생성한 로그 파일에 대한 액세스를 관리합니다. 기본적으로 버킷 소유자는 각 로그 파일에 대한 FULL_CONTROL 권한을 보유하고 있습니다. 로그 전송 소유자가 버킷 소유자와 다른 경우에는 권한이 없습니다. 로그 전송 계정에는 READ 및 WRITE 권한이 부여됩니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 [액세스 제어 목록\(ACL\) 개요](#)를 참조하십시오.

Amazon S3에 게시하는 흐름 로그 생성

Amazon S3 버킷을 생성하고 구성한 후에는 전송 게이트웨이에 대한 흐름 로그를 생성할 수 있습니다.

콘솔을 사용하여 Amazon S3에 게시하는 전송 게이트웨이 흐름 로그 생성

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 여세요.
2. 탐색 창에서 전송 게이트웨이(Transit Gateway), 전송 게이트웨이 연결(Transit Gateway Attachment)을 선택합니다.
3. 하나 이상의 전송 게이트웨이 혹은 전송 게이트웨이 연결의 확인란을 선택합니다.
4. 작업(Actions), 흐름 로그 생성(Create flow log)을 선택합니다.
5. 흐름 로그 설정을 구성합니다. 자세한 정보는 [흐름 로그 설정을 구성하려면](#) 내용을 참조하십시오.

콘솔을 사용하여 흐름 로그 설정을 구성하려면

1. 대상(Destination)에서 S3 버킷으로 전송(Send to an S3 bucket)을 선택합니다.
2. S3 버킷 ARN(S3 bucket ARN)의 경우 기존 Amazon S3 버킷의 Amazon 리소스 이름(ARN)을 지정합니다. 필요한 경우 하위 폴더를 포함할 수 있습니다. 예를 들어 my-bucket이란 이름의 버킷에 my-logs이란 이름의 하위 폴더를 지정하려면 다음 ARN을 사용하십시오.

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

버킷에 AWSLogs를 하위 폴더 이름으로 사용할 수 없습니다. 이것은 예약된 용어입니다.

버킷을 소유한 경우, 자동으로 리소스 정책을 생성하여 버킷에 연결합니다. 자세한 정보는 [Amazon S3 버킷의 흐름 로그에 대한 권한](#)을 참조하세요.

3. 로그 레코드 형식에서 흐름 로그 레코드의 형식을 지정합니다.
 - 기본 흐름 로그 레코드 형식을 사용하려면 AWS 기본 형식을 선택하세요.

- 사용자 지정 형식을 만들려면 사용자 지정 형식을 선택하십시오. 로그 형식(Log format)에 대해 흐름 로그 레코드에 포함할 필드를 선택하세요.
4. 로그 파일 형식의 경우 로그 파일의 형식을 지정합니다.
 - Text – 일반 텍스트. 이것은 기본 형식입니다.
 - Parquet – Apache Parquet은 열 기반 데이터 형식입니다. Parquet 형식의 데이터에 대한 쿼리는 일반 텍스트 데이터에 대한 쿼리에 비해 10배에서 100배 빠릅니다. Gzip 압축을 사용하는 Parquet 형식 데이터는 Gzip 압축을 사용하는 일반 텍스트보다 스토리지 공간을 20% 적게 사용합니다.
 5. (선택 사항) Hive 호환 S3 접두사를 사용하려면 Hive 호환 S3 접두사,활성화를 선택합니다.
 6. (선택 사항) 흐름 로그를 시간당 분할하려면 1시간마다 (60분)을 선택합니다.
 7. (선택 사항) 흐름 로그에 태그를 추가하려면 새 태그 추가를 선택하여 태그 키와 값을 지정하십시오.
 8. 흐름 로그 생성(Create flow log)을 선택합니다.

명령줄 도구를 사용하여 Amazon S3에 게시하는 흐름 로그를 만들려면

다음 명령 중 하나를 사용합니다.

- [create-flow-logs](#)(AWS CLI)
- [New-EC2FlowLogs](#) (AWS Tools for Windows PowerShell)
- [CreateFlow로그](#) (아마존 EC2 쿼리 API)

다음 AWS CLI 예제에서는 VPC의 모든 전송 게이트웨이 트래픽을 tgw-00112233344556677 캡처하고 이라는 Amazon S3 버킷으로 흐름 로그를 전송하는 흐름 로그를 생성합니다. flow-log-bucket --log-format 파라미터는 흐름 로그 레코드의 사용자 지정 형식을 지정합니다.

```
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/'
```

Amazon S3에서 흐름 로그 레코드 처리

로그 파일은 압축된 상태입니다. Amazon S3 콘솔을 사용해 로그 파일을 열면 압축이 해제되고 흐름 로그 레코드가 표시됩니다. 파일을 다운로드하는 경우, 압축을 해제해야 흐름 로그 레코드를 볼 수 있습니다.

Firehose에 플로우 로그 게시

주제

- [교차 계정 전송에 대한 IAM 역할](#)
- [Firehose에 게시하는 흐름 로그 만들기](#)

흐름 로그는 흐름 로그 데이터를 Firehose에 직접 게시할 수 있습니다. 같은 계정을 리소스 모니터로 하여 흐름 로그를 게시하거나 다른 계정에 흐름 로그를 게시하기로 선택할 수 있습니다.

사전 조건

Firehose에 게시할 때 흐름 로그 데이터는 Firehose 전송 스트림에 일반 텍스트 형식으로 게시됩니다. 먼저 Firehose 전송 스트림을 생성해야 합니다. 전송 스트림을 생성하는 단계는 Amazon Data Firehose [개발자 안내서의 Amazon Data Firehose 전송 스트림 생성](#)을 참조하십시오.

요금

표준 모으기 및 전송 요금이 적용됩니다. 자세한 내용은 [Amazon CloudWatch Pricing](#)을 열고 로그를 선택한 다음 벤디드 로그를 찾으십시오.

교차 계정 전송에 대한 IAM 역할

Kinesis Data Firehose에 게시할 때 모니터링할 리소스와 동일한 계정(소스 계정) 또는 상이한 계정(대상 계정)에 있는 전송 스트림을 선택할 수 있습니다. Firehose에 흐름 로그의 계정 간 전송을 활성화하려면 원본 계정에서 IAM 역할을 만들고 대상 계정에서 IAM 역할을 만들어야 합니다.

역할

- [소스 계정 역할](#)
- [대상 계정 역할](#)

소스 계정 역할

소스 계정에서 다음과 같은 권한을 부여하는 역할을 생성합니다. 이 예시에서는 역할 이름이 mySourceRole이지만, 이 역할에 대해 다른 이름을 선택할 수 있습니다. 마지막 명령문에서는 대상 계정의 역할에 이 역할 수임을 허용합니다. 조건문에서는 지정된 리소스를 모니터링할 때만 이 역할이 로그 전송 서비스에만 전달되도록 합니다. 정책을 생성할 때 모니터링 중인 VPC, 네트워크 인터페이스 또는 서브넷을 조건 키(iam:AssociatedResourceARN)로 지정합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::source-account:role/mySourceRole",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "delivery.logs.amazonaws.com"
        },
        "StringLike": {
          "iam:AssociatedResourceARN": [
            "arn:aws:ec2:region:source-account:transit-gateway/
            tgw-0fb8421e2da853bf"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs>DeleteLogDelivery",
        "logs>ListLogDeliveries",
        "logs:GetLogDelivery"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::destination-account:role/
      AWSLogDeliveryFirehoseCrossAccountRole"
    }
  ]
}
```

로그 전송 서비스에서 역할을 수임할 수 있는 다음과 같은 신뢰 정책이 이 역할에 있는지 확인하세요.

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

```

{
  "Effect": "Allow",
  "Principal": {
    "Service": "delivery.logs.amazonaws.com"
  },
  "Action": "sts:AssumeRole"
}
]
}

```

소스 계정에서 다음과 같은 절차를 사용하여 역할을 생성합니다.

소스 계정 역할을 생성하는 방법

1. AWS Management Console [로그인하고 https://console.aws.amazon.com/iam/](https://console.aws.amazon.com/iam/) 에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 정책을 선택합니다.
3. [정책 생성(Create policy)]을 선택합니다.
4. [정책 생성(Create policy) 페이지에서 다음을 수행합니다.
 1. JSON을 선택합니다.
 2. 이 창의 내용을 이 섹션의 시작 부분에 있는 권한 정책으로 대체합니다.
 3. Next: Tags(다음: 태그)와 Next: Review(다음: 검토)를 선택합니다.
 4. 정책의 이름과 설명(선택 사항)을 입력한 다음에 Create policy(정책 생성)를 선택합니다.
5. 탐색 창에서 역할을 선택합니다.
6. 역할 생성을 선택합니다.
7. 신뢰할 수 있는 엔터티 유형(Trusted entity type)에 사용자 지정 신뢰 정책(Custom trust policy)을 선택합니다. 사용자 지정 신뢰 정책(Custom trust policy)에서 로그 전송 서비스를 지정하는 다음으로 "Principal": {}, 을 대체합니다. 다음을 선택합니다.

```

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

```

8. Add permissions(권한 추가) 페이지에서 이 절차의 앞부분에서 생성한 정책의 확인란을 선택한 후 Next(다음)를 선택합니다.
9. 역할 이름을 입력하고 선택적으로 설명을 제공합니다.
10. 역할 생성(Create role)을 선택합니다.

대상 계정 역할

대상 계정에서 로 시작하는 이름으로 역할을 생성합니다.

AWSLogsDeliveryFirehoseCrossAccountRole 이 역할에서는 다음과 같은 권한을 부여해야 합니다.

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

이 역할을 수임할 수 있도록 소스 계정에서 생성한 역할이 허용되는 다음과 같은 신뢰 정책이 이 역할에 있는지 확인하세요.

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

대상 계정에서 다음과 같은 절차를 사용하여 역할을 생성합니다.

대상 계정 역할을 생성하는 방법

1. 에 AWS Management Console 로그인하고 <https://console.aws.amazon.com/iam/> 에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 정책을 선택합니다.

3. [정책 생성(Create policy)]을 선택합니다.
4. [정책 생성(Create policy)] 페이지에서 다음을 수행합니다.
 1. JSON을 선택합니다.
 2. 이 창의 내용을 이 섹션의 시작 부분에 있는 권한 정책으로 대체합니다.
 3. 다음: 태그(Next: Tags)와 다음: 검토(Next: Review)를 선택합니다.
 4. 로 AWSLogDeliveryFirehoseCrossAccountRole시작하는 정책 이름을 입력한 다음 Create policy (정책 생성) 를 선택합니다.
5. 탐색 창에서 역할을 선택합니다.
6. 역할 생성을 선택합니다.
7. 신뢰할 수 있는 엔터티 유형(Trusted entity type)에 사용자 지정 신뢰 정책(Custom trust policy)을 선택합니다. 사용자 지정 신뢰 정책(Custom trust policy)에서 로그 전송 서비스를 지정하는 다음으로 "Principal": {}, 을 대체합니다. 다음을 선택합니다.


```
"Principal": {
  "AWS": "arn:aws:iam::source-account:role/mySourceRole"
},
```
8. Add permissions(권한 추가) 페이지에서 이 절차의 앞부분에서 생성한 정책의 확인란을 선택한 후 Next(다음)를 선택합니다.
9. 역할 이름을 입력하고 선택적으로 설명을 제공합니다.
10. 역할 생성(Create role)을 선택합니다.

Firehose에 게시하는 흐름 로그 만들기

콘솔을 사용하여 Firehose에 게시하는 전송 게이트웨이 흐름 로그를 만들려면

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 여세요.
2. 탐색 창에서 전송 게이트웨이(Transit Gateway), 전송 게이트웨이 연결(Transit Gateway Attachment)을 선택합니다.
3. 하나 이상의 전송 게이트웨이 혹은 전송 게이트웨이 연결의 확인란을 선택합니다.
4. 작업(Actions), 흐름 로그 생성(Create flow log)을 선택합니다.
5. 대상(Destination)에 Firehose 전송 시스템으로 전송(Send to a Firehose Delivery System)을 선택합니다.

6. Firehose 전송 스트림 ARN(Firehose Delivery Stream ARN)으로는, 흐름 로그를 게시하려고 생성한 전송 스트림의 ARN을 선택합니다.
7. 로그 레코드 형식에서 흐름 로그 레코드의 형식을 지정합니다.
 - 기본 흐름 로그 레코드 형식을 사용하려면 AWS 기본 형식을 선택하세요.
 - 사용자 지정 형식을 만들려면 사용자 지정 형식을 선택하십시오. 로그 형식(Log format)에 대해 흐름 로그 레코드에 포함할 필드를 선택하세요.
8. (선택 사항) 흐름 로그에 태그를 추가하려면 새 태그 추가를 선택하여 태그 키와 값을 지정하십시오.
9. 흐름 로그 생성(Create flow log)을 선택합니다.

명령줄 도구를 사용하여 Firehose에 게시하는 흐름 로그를 만들려면

다음 명령 중 하나를 사용합니다.

- [플로우 로그 생성 \(CLI\)](#) AWS
- [New-EC2FlowLogs](#) (AWS Tools for Windows PowerShell)
- [CreateFlow로그](#) (아마존 EC2 쿼리 API)

다음 AWS CLI 예제는 전송 게이트웨이 정보를 캡처하고 지정된 Firehose 전송 스트림에 흐름 로그를 전달하는 흐름 로그를 생성합니다.

```
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
```

다음 AWS CLI 예제는 전송 게이트웨이 정보를 캡처하고 원본 계정의 다른 Firehose 전송 스트림으로 흐름 로그를 전송하는 흐름 로그를 만듭니다.

```
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
```

Transit Gateway 흐름 로그 작업

Amazon EC2, CloudWatch 아마존 VPC 및 Amazon S3 콘솔을 사용하여 Transit Gateway 플로우 로그를 처리할 수 있습니다.

Tasks

- [흐름 로그 사용 제어](#)
- [흐름 로그 생성](#)
- [흐름 로그 보기](#)
- [흐름 로그에 대한 태그 추가 또는 제거](#)
- [흐름 로그 레코드 보기](#)
- [흐름 로그 레코드 검색](#)
- [흐름 로그 삭제](#)
- [API 및 CLI 개요 및 제한](#)

흐름 로그 사용 제어

기본적으로 사용자에게는 흐름 로그 사용 권한이 없습니다. 사용자 정책을 만들어 사용자에게 흐름 로그를 생성, 설명, 삭제할 수 있는 권한을 부여할 수 있습니다. 자세한 내용은 Amazon EC2 API 참조의 [IAM 사용자에게 Amazon EC2 리소스에 대한 필요 권한 부여](#)를 참조하세요.

다음은 사용자에게 흐름 로그를 생성, 설명 및 삭제할 수 있는 전체 권한을 부여하는 정책의 예입니다.

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

```

    "Resource": "*"
  }
]
}

```

CloudWatch Logs 또는 Amazon S3에 게시하는지 여부에 따라 몇 가지 추가 IAM 역할 및 권한 구성이 필요합니다. 자세한 내용은 [Logs에 게시하는 흐름 로그를 생성하십시오. CloudWatch](#) 및 [Amazon S3에 게시하는 흐름 로그 생성](#) 섹션을 참조하세요.

흐름 로그 생성

로그, Amazon S3 또는 Firehose에 데이터를 게시할 수 있는 전송 게이트웨이의 흐름 CloudWatch 로그를 생성할 수 있습니다.

자세한 내용은 다음 자료를 참조하세요.

- [Logs에 게시하는 흐름 로그를 생성하십시오. CloudWatch](#)
- [Amazon S3에 게시하는 흐름 로그 생성](#)
- [Firehose에 게시하는 흐름 로그 만들기](#)

흐름 로그 보기

특정 리소스에 대한 흐름 로그(Flow Logs) 탭을 보면 Amazon VPC 콘솔에서 흐름 로그에 대한 정보를 볼 수 있습니다. 리소스를 선택하면 해당 리소스의 모든 흐름 로그가 나열됩니다. 흐름 로그의 ID, 흐름 로그 구성, 흐름 로그 상태에 대한 정보 등이 표시됩니다.

전송 게이트웨이의 흐름 로그 정보 보기

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 여세요.
2. 탐색 창에서 전송 게이트웨이(Transit Gateway), 전송 게이트웨이 연결(Transit Gateway Attachment)을 선택합니다.
3. 전송 게이트웨이 또는 Transit Gateway Attachment를 선택하고 흐름 로그를 선택합니다. 흐름 로그에 대한 정보가 탭에 표시됩니다. 대상 유형(Destination type) 열은 흐름 로그를 게시할 대상을 표시합니다.

흐름 로그에 대한 태그 추가 또는 제거

Amazon EC2 및 Amazon VPC 콘솔에서 흐름 로그의 태그를 추가하거나 제거할 수 있습니다.

전송 게이트웨이 흐름 로그에 대한 태그를 추가 혹은 제거

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 여세요.
2. 탐색 창에서 전송 게이트웨이(Transit Gateway), 전송 게이트웨이 연결(Transit Gateway Attachment)을 선택합니다.
3. 전송 게이트웨이 또는 Transit Gateway Attachment를 선택
4. 필요한 흐름 로그에 대해 태그 관리(Manage Tags)를 선택합니다.
5. 새 태그를 추가하려면 태그 생성(Create Tag)을 선택합니다. 태그를 제거하려면 삭제 버튼(x)을 선택합니다.
6. 저장(Save)을 선택합니다.

흐름 로그 레코드 보기

선택한 대상 유형에 따라 CloudWatch 로그 콘솔 또는 Amazon S3 콘솔을 사용하여 흐름 로그 기록을 볼 수 있습니다. 흐름 로그를 생성한 후 콘솔에서 흐름 로그를 보려면 몇 분 정도 지나야 할 수 있습니다.

CloudWatch Logs에 게시된 흐름 로그 레코드를 보려면

1. <https://console.aws.amazon.com/cloudwatch/>에서 CloudWatch 콘솔을 엽니다.
2. 탐색 창에서 로그(Logs)를 선택하고 흐름 로그가 포함된 로그 그룹을 선택합니다. 각 전송 게이트웨이의 로그 스트림 목록이 표시됩니다.
3. 흐름 로그 레코드를 보려는 전송 게이트웨이의 ID를 포함하는 로그 스트림을 선택합니다. 자세한 정보는 [전송 게이트웨이 흐름 로그 레코드](#)을 참조하세요.

Amazon S3에 게시된 플로우 로그 레코드를 보려면

1. <https://console.aws.amazon.com/s3/>에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름(Bucket name)에서 흐름 로그를 게시할 버킷을 선택합니다.
3. 이름(Name)에서 로그 파일 옆의 확인란을 선택합니다. 객체 개요 패널에서 다운로드(Download)를 선택합니다.

흐름 로그 레코드 검색

Logs 콘솔을 사용하여 CloudWatch Logs에 게시된 흐름 로그 레코드를 검색할 수 있습니다.

CloudWatch [지표 필터](#)를 사용하여 흐름 로그 레코드를 필터링할 수 있습니다. 흐름 로그 레코드는 공백으로 구분됩니다.

로그 콘솔을 CloudWatch 사용하여 흐름 로그 기록을 검색하려면

1. <https://console.aws.amazon.com/cloudwatch/> 에서 CloudWatch 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 로그(Logs)를 선택한 다음, 로그 그룹(Log groups)을 선택합니다.
3. 흐름 로그가 포함된 로그 그룹을 선택합니다. 각 전송 게이트웨이의 로그 스트림 목록이 표시됩니다.
4. 검색 중인 전송 게이트웨이를 알고 있는 경우 개별 로그 스트림을 선택합니다. 또는 로그 그룹 검색을 선택하여 전체 로그 그룹을 검색합니다. 로그 그룹에 전송 게이트웨이가 많거나 선택한 시간 범위에 따라 시간이 다소 걸릴 수 있습니다.
5. 이벤트 필터에 다음 문자열을 입력합니다. 여기서는 흐름 로그 레코드가 [기본 형식](#)을 사용한다고 가정합니다.

```
[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. 필드의 값을 지정하여 필요에 따라 필터를 수정합니다. 다음 예제에서는 특정 원본 IP 주소를 기준으로 필터링합니다.

```
[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]
```

다음 예제는 전송 게이트웨이 ID tgw-123abc456bca, 대상 포트, 바이트 수를 기준으로 필터링됩니다.

```
[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]
```

흐름 로그 삭제

Amazon VPC 콘솔을 사용하여 전송 게이트웨이를 삭제할 수 있습니다.

이러한 절차는 리소스의 흐름 로그 서비스를 비활성화합니다. 흐름 로그를 삭제해도 Amazon S3의 로그 또는 로그 파일의 기존 로그 스트림은 삭제되지 않습니다. CloudWatch 각 서비스의 콘솔을 사용해 기존 흐름 로그 데이터를 삭제해야 합니다. 또한 Amazon S3에 게시되는 플로우 로그를 삭제해도 버킷 정책과 로그 파일 액세스 제어 목록(ACL)은 삭제되지 않습니다.

전송 게이트웨이 흐름 로그 삭제

1. <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 여세요.
2. 탐색 창에서 Transit Gateway를 선택합니다.
3. 하나의 Transit gateway ID를 선택합니다.
4. 흐름 로그 섹션에서 삭제하려는 흐름 로그를 선택합니다.
5. 작업(Actions)을 선택한 다음 흐름 로그 삭제>Delete flow logs)를 선택합니다.
6. 삭제>Delete)를 선택하여 흐름을 삭제할 것인지 확인합니다.

API 및 CLI 개요 및 제한

이 페이지에서 설명한 작업은 명령줄이나 API를 사용하여 수행할 수 있습니다.

[CreateFlowLogs](#) API 또는 [create-flow-logs](#) CLI를 사용할 때는 다음 제한 사항이 적용됩니다.

- `--resource-ids`의 최대 제약 조건은 25개의 TransitGateway 또는 TransitGatewayAttachment 리소스 유형입니다.
- `--traffic-type`는 기본적으로 필수 필드가 아닙니다. 전송 게이트웨이 리소스 유형에 이 값을 제공하면 오류가 반환됩니다. 이 제한은 전송 게이트웨이 리소스 유형에만 적용됩니다.
- `--max-aggregation-interval`의 기본값인 60은 전송 게이트웨이 리소스 유형에 유일하게 허용되는 값입니다. 다른 값을 전달하려고 하면 오류가 반환됩니다. 이 제한은 전송 게이트웨이 리소스 유형에만 적용됩니다.
- `--resource-type`은 두 가지 새로운 리소스 유형 TransitGateway 및 TransitGatewayAttachment를 지원합니다.
- `--log-format`은 포함할 필드를 설정하지 않은 경우 전송 게이트웨이 리소스 유형에 대한 모든 로그 필드를 포함합니다. 이는 전송 게이트웨이 리소스 유형에만 적용됩니다.

흐름 로그 생성

- [create-flow-logs](#)(AWS CLI)
- [New-EC2FlowLog](#) (AWS Tools for Windows PowerShell)
- [CreateFlow로그](#) (아마존 EC2 쿼리 API)

흐름 로그 설명

- [describe-flow-logs](#)(AWS CLI)
- [Get-EC2FlowLog](#) (AWS Tools for Windows PowerShell)
- [DescribeFlow로그](#) (아마존 EC2 쿼리 API)

흐름 로그 레코드 확인(로그 이벤트)

- [get-log-events](#)(AWS CLI)
- [Get-CWL \(\) LogEvent](#) AWS Tools for Windows PowerShell
- [GetLog이벤트](#) (API) CloudWatch

흐름 로그 삭제

- [delete-flow-logs](#)(AWS CLI)
- [Remove-EC2FlowLog](#) (AWS Tools for Windows PowerShell)
- [DeleteFlow로그](#) (아마존 EC2 쿼리 API)

Transit Gateway 모니터링

다음 기능을 사용하여 전송 게이트웨이를 모니터링하고 트래픽 패턴을 분석하며 전송 게이트웨이의 문제를 해결할 수 있습니다.

CloudWatch 지표

Amazon CloudWatch를 사용하면 전송 게이트웨이의 데이터 요소에 대한 통계를 지표라고 하는 정렬된 시계열 데이터 세트로 검색할 수 있습니다. 이러한 지표를 사용하여 시스템이 예상대로 수행되고 있는지 확인할 수 있습니다. 자세한 내용은 [전송 게이트웨이용 CloudWatch 지표](#) 섹션을 참조하세요.

전송 게이트웨이 흐름 로그

전송 게이트웨이 흐름 로그를 사용하여 전송 게이트웨이의 네트워크 트래픽에 대한 자세한 정보를 캡처할 수 있습니다. 자세한 내용은 [전송 게이트웨이 흐름 로그](#) 섹션을 참조하세요.

VPC 흐름 로그

VPC 흐름 로그를 사용하여 전송 게이트웨이에 연결된 VPC로 들어오고 나가는 트래픽에 대한 세부 정보를 캡처할 수 있습니다. 자세한 내용은 Amazon VPC 사용 설명서의 [VPC 흐름 로그](#)를 참조하세요.

CloudTrail 로그

AWS CloudTrail을 사용하여 전송 게이트웨이 API에 보낸 요청에 대한 자세한 정보를 캡처하고 Amazon S3에 로그 파일로 저장할 수 있습니다. 이러한 CloudTrail 로그를 사용하여 어떤 요청이 이루어졌는지, 어떤 소스 IP 주소에서 요청을 했는지, 누가 언제 요청했는지 등을 확인할 수 있습니다. 자세한 내용은 [AWS CloudTrail을 사용하여 전송 게이트웨이에 대한 API 호출 로깅](#) 섹션을 참조하세요.

Network Manager를 사용한 CloudWatch 이벤트

AWS Network Manager를 사용하여 이벤트를 CloudWatch로 전달한 다음 해당 이벤트를 대상 함수 또는 스트림으로 라우팅할 수 있습니다. Network Manager는 토폴로지 변경, 라우팅 업데이트 및 상태 업데이트에 대한 이벤트를 생성하며, 이 모든 이벤트는 전송 게이트웨이의 변경 사항을 알리는 데 사용될 수 있습니다. 자세한 내용은 전송 게이트웨이를 위한 AWS 글로벌 네트워크 사용 설명서에서 [CloudWatch 이벤트를 통한 글로벌 네트워크 모니터링](#)을 참조하세요.

전송 게이트웨이용 CloudWatch 지표

Amazon VPC는 Transit Gateway 및 Transit Gateway Attachment를 위해 Amazon CloudWatch에 데이터 포인트를 게시합니다. CloudWatch를 사용하면 이러한 데이터 요소에 대한 통계를 정렬된 시계열 데이터 세트로 검색할 수 있습니다. 이러한 통계를 지표라고 합니다. 지표를 모니터링할 변수로 생각하면 데이터 요소는 시간에 따른 변수의 값을 나타냅니다. 각 데이터 포인트에는 연결된 타임스탬프와 측정 단위(선택 사항)가 있습니다.

지표를 사용하여 시스템이 예상대로 수행되고 있는지 확인할 수 있습니다. 예를 들어 CloudWatch 경보를 생성하여 지정된 지표를 모니터링할 수 있으며, 지표가 허용 범위를 벗어난다고 간주되는 경우 작업(예: 이메일 주소로 알림 전송)을 시작할 수 있습니다.

Amazon VPC는 60초 간격으로 지표를 측정하고 CloudWatch에 전송합니다.

자세한 내용은 [Amazon CloudWatch 사용 설명서](#)를 참조하세요.

목차

- [Transit Gateway 지표](#)
- [전송 게이트웨이의 지표 차원](#)

Transit Gateway 지표

AWS/TransitGateway 네임스페이스에는 다음 지표가 포함되어 있습니다.

지표	설명
BytesDropCountBlackhole	blackhole 경로와 일치하여 삭제된 바이트 수입니다.
BytesDropCountNoRoute	경로와 일치하지 않아 삭제된 바이트 수입니다.
BytesIn	전송 게이트웨이에서 수신한 바이트 수입니다.
BytesOut	전송 게이트웨이에서 보낸 바이트 수입니다.
PacketsIn	전송 게이트웨이에서 수신한 패킷 수입니다.
PacketsOut	전송 게이트웨이에서 보낸 패킷 수입니다.

지표	설명
PacketDropCountBlackhole	blackhole 경로와 일치하여 삭제된 패킷 수입니다.
PacketDropCountNoRoute	경로와 일치하지 않아 삭제된 패킷 수입니다.

연결 수준 지표

Transit Gateway Attachment에 사용할 수 있는 지표는 다음과 같습니다. 모든 연결 지표는 전송 게이트웨이 소유자의 계정에 게시됩니다. 개별 연결 지표는 연결 소유자의 계정도 게시됩니다. 연결 소유자는 자체 연결에 대한 지표만 볼 수 있습니다. 지원되는 첨부 파일 유형에 대한 자세한 내용은 [the section called “리소스 연결”](#) 섹션을 참조하세요.

지표	설명
BytesDropCountBlackhole	Transit Gateway Attachment의 blackhole 경로와 일치하여 삭제된 바이트 수입니다.
BytesDropCountNoRoute	Transit Gateway Attachment의 경로와 일치하지 않아 삭제된 바이트 수입니다.
BytesIn	전송 게이트웨이가 연결에서 수신한 바이트 수입니다.
BytesOut	전송 게이트웨이에서 연결로 보낸 바이트 수입니다.
PacketsIn	전송 게이트웨이가 연결에서 수신한 패킷 수입니다.
PacketsOut	전송 게이트웨이가 연결로 보낸 패킷 수입니다.
PacketDropCountBlackhole	Transit Gateway Attachment의 blackhole 경로와 일치하여 삭제된 패킷 수입니다.
PacketDropCountNoRoute	Transit Gateway Attachment의 경로와 일치하지 않아 삭제된 패킷 수입니다.

전송 게이트웨이의 지표 차원

전송 게이트웨이의 지표를 필터링하려면 다음 차원을 사용합니다.

차원	설명
TransitGateway	전송 게이트웨이를 기준으로 지표 데이터를 필터링합니다.
TransitGatewayAttachment	Transit Gateway Attachment를 기준으로 지표 데이터를 필터링합니다.

AWS CloudTrail을 사용하여 전송 게이트웨이에 대한 API 호출 로깅

AWS CloudTrail은 사용자, 역할 또는 AWS 서비스가 수행한 작업 기록을 제공하는 서비스입니다. CloudTrail은 모든 전송 게이트웨이 API 호출을 이벤트로 캡처합니다. 캡처되는 호출에는 AWS Management Console의 호출과 전송 게이트웨이 API 작업에 대한 코드 호출이 포함됩니다. 추적을 생성하면 전송 게이트웨이 이벤트를 포함한 CloudTrail 이벤트를 지속적으로 Amazon S3 버킷에 배포할 수 있습니다. 추적을 구성하지 않은 경우에도 CloudTrail 콘솔의 Event history(이벤트 기록)에서 최신 이벤트를 볼 수 있습니다. CloudTrail에서 수집한 정보를 사용하여 게이트웨이 API에 수행된 요청, 요청이 수행된 IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

전송 게이트웨이 API에 대한 자세한 내용은 [Amazon EC2 API Reference](#)의 AWS 전송 게이트웨이 작업을 참조하세요.

CloudTrail에 대한 자세한 내용은 [AWS CloudTrail 사용 설명서](#)를 참조하세요.

CloudTrail의 전송 게이트웨이 정보

CloudTrail은 계정 생성 시 AWS 계정에서 사용되도록 설정됩니다. Amazon API Gateway에서 활동이 발생하면 해당 활동은 이벤트 기록에 있는 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트에 기록됩니다. AWS 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용은 [CloudTrail 이벤트 기록을 사용하여 이벤트 보기](#)를 참조하세요.

전송 게이트웨이 API의 이벤트를 포함한 AWS 계정 이벤트를 지속적으로 기록하려면 추적을 생성해야 합니다. CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에

서 추적을 생성하면 기본적으로 모든 리전에 추적이 적용됩니다. 추적은 AWS 파티션에 있는 모든 리전의 이벤트를 로깅하고 지정된 Amazon S3 버킷으로 로그 파일을 전송합니다. 또는 CloudTrail 로그에서 수집된 이벤트 데이터를 추가 분석 및 처리하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하세요.

- [추적 생성 개요](#)
- [CloudTrail 지원 서비스 및 통합](#)
- [CloudTrail에 대한 Amazon SNS 알림 구성](#)
- [여러 리전에서 CloudTrail 로그 파일 받기 및 여러 계정에서 CloudTrail 로그 파일 받기](#)

Transit Gateway 작업에 대한 모든 호출은 CloudTrail에서 기록합니다. 예를 들어 CreateTransitGateway 작업을 호출하면 CloudTrail 로그 파일에 항목이 생성됩니다.

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에게 대한 정보가 들어 있습니다. 자격 증명 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청을 루트로 했는지 아니면 AWS Identity and Access Management 사용자 자격 증명으로 했는지 여부
- 역할 또는 페더레이션 사용자에게 대한 임시 보안 자격 증명을 사용하여 요청이 생성되었는지 여부.
- 다른 AWS 서비스에서 요청했는지 여부.

자세한 내용은 [CloudTrail userIdentity 요소](#)를 참조하세요.

Transit Gateway 로그 파일 항목 이해

추적이란 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 입력할 수 있게 하는 구성입니다.

CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함될 수 있습니다. 이벤트는 모든 소스의 단일 요청을 나타내며 요청된 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보를 포함합니다. CloudTrail 로그 파일은 퍼블릭 API 호출의 주문 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

로그 파일에는 전송 게이트웨이 API 호출 외에 AWS 계정의 모든 API 호출 이벤트도 포함되어 있습니다. eventSource 값이 있는 ec2.amazonaws.com 요소를 확인하여 전송 게이트웨이 API에 대한 호출의 위치를 찾을 수 있습니다. CreateTransitGateway 같은 특정 작업에 대한 레코드를 보려면 작업 이름이 있는 eventName 요소를 확인합니다.

다음은 콘솔을 사용하여 전송 게이트웨이를 생성한 사용자의 전송 게이트웨이 API에 대한 CloudTrail 로그 레코드의 예입니다. userAgent 요소를 사용하여 콘솔을 식별할 수 있습니다. eventName

요소를 사용하여 요청된 API 호출을 식별할 수 있습니다. 그리고 사용자(Alice)에 대한 정보는 `userIdentity` 요소를 보면 알 수 있습니다.

Example 예: `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"
}
```


전송 게이트웨이의 Identity and Access Management

AWS는 보안 자격 증명을 사용하여 사용자를 식별하고 AWS 리소스에 대한 액세스 권한을 부여합니다. AWS Identity and Access Management(IAM)의 기능을 사용하면 보안 자격 증명을 공유하지 않고도 다른 사용자, 서비스 및 애플리케이션이 AWS 리소스를 완전히 또는 제한된 방식으로 사용할 수 있습니다.

기본적으로 IAM 사용자는 AWS 리소스를 생성, 확인 또는 수정할 수 있는 권한이 없습니다. 사용자에게 Transit Gateway 같은 리소스에 액세스하여 작업을 수행하도록 허용하려면 사용자에게 필요한 특정 리소스 및 API 작업을 사용할 권한을 부여하는 IAM 정책을 생성하고, 해당 사용자가 속한 그룹에 정책을 연결해야 합니다. 사용자 또는 사용자 그룹에 정책을 연결하면 지정된 리소스에 대해 지정된 작업을 수행할 권한이 허용되거나 거부됩니다.

예를 들어 Transit Gateway의 경우 다음 AWS 관리형 정책 중 하나가 적합할 수 있습니다.

- [AmazonEC2FullAccess](#)
- [AmazonEC2ReadOnlyAccess](#)
- [PowerUserAccess](#)
- [ReadOnlyAccess](#)

Transit Gateway를 관리하는 정책의 예

다음은 Transit Gateway 작업에 대한 IAM 정책의 예입니다.

필수 태그를 사용하여 Transit Gateway 생성

다음 예제에서는 사용자가 Transit Gateway를 생성할 수 있도록 합니다. `aws:RequestTag` 조건 키를 사용하려면 사용자가 `stack=prod` 태그를 사용하여 Transit Gateway에 태그를 지정해야 합니다. `aws:TagKeys` 조건 키는 `ForAllValues` 한정자를 사용하여 요청에 `stack` 키만 허용됨을 나타냅니다(다른 어떤 태그도 지정할 수 없음). 사용자가 Transit Gateway를 생성할 때 이 태그를 전달하지 않거나 태그를 전혀 지정하지 않으면 요청이 실패합니다.

두 번째 문은 `ec2:CreateAction` 조건 키를 사용하여 사용자가 `CreateTransitGateway`의 컨텍스트에서만 태그를 생성하도록 허용합니다.

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

```

    {
      "Sid": "AllowCreateTaggedTGWs",
      "Effect": "Allow",
      "Action": "ec2:CreateTransitGateway",
      "Resource": "arn:aws:ec2:region:account-id:transit-gateway/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/stack": "prod"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "stack"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:region:account-id:transit-gateway/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction": "CreateTransitGateway"
        }
      }
    }
  ]
}

```

Transit Gateway 라우팅 테이블 작업

다음 예제에서는 사용자가 특정 Transit Gateway(tgw-11223344556677889)에 대해서만 Transit Gateway 라우팅 테이블을 생성하고 삭제할 수 있도록 합니다. 또한 사용자는 모든 Transit Gateway 라우팅 테이블에서 라우팅을 생성하고 바꿀 수 있지만 network=new-york-office 태그가 있는 연결에 대해서만 가능합니다.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",

```

```

    "Action": [
      "ec2:DeleteTransitGatewayRouteTable",
      "ec2:CreateTransitGatewayRouteTable"
    ],
    "Resource": [
      "arn:aws:ec2:region:account-id:transit-gateway/tgw-11223344556677889",
      "arn:aws:ec2:*:*:transit-gateway-route-table/*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:CreateTransitGatewayRoute",
      "ec2:ReplaceTransitGatewayRoute"
    ],
    "Resource": "arn:aws:ec2:*:*:transit-gateway-attachment/*",
    "Condition": {
      "StringEquals": {
        "ec2:ResourceTag/network": "new-york-office"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:CreateTransitGatewayRoute",
      "ec2:ReplaceTransitGatewayRoute"
    ],
    "Resource": "arn:aws:ec2:*:*:transit-gateway-route-table/*"
  }
]
}

```

AWS Network Manager를 관리하는 정책 예

정책 예는 Transit Gateway에 대한 AWS 글로벌 네트워크 사용 설명서의 [Network Manager 관리를 위한 예시 정책](#)을 참조하십시오.

전송 게이트웨이에 대해 서비스 연결 역할 사용

Amazon VPC는 다른 AWS 서비스를 자동으로 호출하는 데 필요한 권한에 서비스 연결 역할을 사용합니다. 자세한 내용은 IAM 사용 설명서의 [서비스 연결 역할 사용](#)을 참조하세요.

Transit Gateway 서비스 연결 역할

Amazon VPC는 Transit Gateway에서 작업할 때 귀하를 대신 다른 AWS 서비스를 호출하는 데 필요한 권한에 서비스 연결 역할을 사용합니다.

서비스 연결 역할에 의해 부여된 권한

Amazon VPC는 전송 게이트 웨이에서 작업할 때 `AWSServiceRoleForVPCTransitGateway`라는 서비스 연결 역할을 사용하여 자동으로 다음 작업을 호출합니다.

- `ec2:CreateNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2:ModifyNetworkInterfaceAttribute`
- `ec2>DeleteNetworkInterface`
- `ec2:CreateNetworkInterfacePermission`
- `ec2:AssignIpv6Addresses`
- `ec2:UnAssignIpv6Addresses`

`AWSServiceRoleForVPCTransitGateway` 역할은 역할을 수입하기 위해 다음 서비스를 신뢰합니다.

- `transitgateway.amazonaws.com`

`AWSServiceRoleForVPCTransitGateway`는 관리형 정책 [AWSVPCTransitGatewayServiceRolePolicy](#)을(를) 사용합니다.

IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 연결 역할을 작성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 [서비스 연결 역할 권한](#)을 참조하세요.

서비스 연결 역할 생성

`AWSServiceRoleForVPCTransitGateway` 역할은 수동으로 생성할 필요가 없습니다. Amazon VPC는 계정의 VPC를 Transit Gateway에 연결할 때 사용자를 대신해 이 역할을 생성합니다.

Amazon VPC가 서비스 연결 역할을 자동으로 생성하려면 사용자에게 필수 권한이 있어야 합니다. 자세한 내용은 IAM 사용 설명서의 [서비스 연결 역할 권한](#)을 참조하세요.

서비스 연결 역할 편집

IAM을 사용하여 `AWSServiceRoleForVPCTransitGateway`의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 [서비스 연결 역할 편집](#)을 참조하세요.

서비스 연결 역할 삭제

Transit Gateway를 사용할 필요가 없다면 `AWSServiceRoleForVPCTransitGateway`를 삭제하는 것이 좋습니다.

이 서비스 연결 역할은 AWS 계정에서 모든 Transit Gateway VPC 연결을 삭제한 후에만 삭제할 수 있습니다. 이렇게 하면 VPC 연결에 대한 액세스 권한을 실수로 제거할 수 없습니다.

IAM 콘솔, IAM CLI 또는 IAM API를 사용하여 서비스 연결 역할을 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 [서비스에 연결 역할 삭제](#) 단원을 참조하세요.

`AWSServiceRoleForVPCTransitGateway`를 삭제한 후 계정에 있는 VPC를 Transit Gateway에 연결하면 Amazon VPC가 다시 역할을 만듭니다.

전송 게이트웨이에 대한 AWS 관리형 정책

AWS 관리형 정책은 AWS에 의해 생성되고 관리되는 독립 실행형 정책입니다. AWS 관리형 정책은 사용자, 그룹 및 역할에 권한 할당을 시작할 수 있도록 많은 일반 사용 사례에 대한 권한을 제공하도록 설계되었습니다.

AWS 관리형 정책은 모든 AWS 고객이 사용할 수 있기 때문에 특정 사용 사례에 대해 최소 권한을 부여하지 않을 수 있습니다. 사용 사례에 고유한 [고객 관리형 정책](#)을 정의하여 권한을 줄이는 것이 좋습니다.

AWS 관리형 정책에서 정의한 권한은 변경할 수 없습니다. AWS에서 AWS 관리형 정책에 정의된 권한을 업데이트할 경우 정책이 연결되어 있는 모든 보안 주체 엔터티(사용자, 그룹 및 역할)에도 업데이트가 적용됩니다. 새로운 AWS 서비스를 시작하거나 새로운 API 작업을 기존 서비스에 이용하는 경우 AWS가 AWS 관리형 정책을 업데이트할 가능성이 높습니다.

자세한 내용은 IAM 사용 설명서의 [AWS 관리형 정책](#)을 참조하세요.

예를 들어 Transit Gateway의 경우 다음 AWS 관리형 정책 중 하나가 적합할 수 있습니다.

- [AmazonEC2FullAccess](#)
- [AmazonEC2ReadOnlyAccess](#)
- [PowerUserAccess](#)

- [ReadOnlyAccess](#)

AWS 관리형 정책: AWSVPCTransitGatewayServiceRolePolicy

이 정책은 [AWSServiceRoleForVPCTransitGateway](#) 역할에 연결됩니다. 이를 통해 Amazon VPC는 Transit Gateway Attachment에 대한 리소스를 생성하고 관리할 수 있습니다.

이 정책의 권한을 보려면 AWS 관리형 정책 참조의 [AWSVPCTransitGatewayServiceRolePolicy](#)를 확인하세요.

전송 게이트웨이를 AWS 관리형 정책으로 업데이트

Amazon VPC가 2021년 3월에 이러한 변경 사항을 추적하기 시작한 이후 전송 게이트웨이용 AWS 관리형 정책 업데이트에 대한 세부 정보를 확인합니다.

변경 사항	설명	날짜
Amazon VPC에서 변경 사항 추적 시작	Amazon VPC AWS관리형 정책에 대한 변경 사항 추적을 시작했습니다.	2021년 3월 1일

네트워크 ACL과 Transit Gateway를 함께 사용하는 방법

네트워크 액세스 제어 목록(NACL)은 선택적 보안 계층입니다.

네트워크 액세스 제어 목록(NACL) 규칙은 시나리오에 따라 다르게 적용됩니다.

- [the section called “EC2 인스턴스 및 Transit Gateway 연결에 동일한 서브넷 사용”](#)
- [the section called “EC2 인스턴스 및 Transit Gateway 연결에 다른 서브넷 사용”](#)

EC2 인스턴스 및 Transit Gateway 연결에 동일한 서브넷 사용

동일한 서브넷을 이용하는 EC2 인스턴스 및 Transit Gateway 연결 구성을 고려합니다. EC2 인스턴스에서 Transit Gateway로 이동하는 트래픽과 Transit Gateway에서 인스턴스로 이동하는 트래픽 모두에 동일한 네트워크 ACL이 사용됩니다.

NACL 규칙은 인스턴스에서 Transit Gateway로 이동하는 트래픽에 대해 다음과 같이 적용됩니다.

- 아웃바운드 규칙은 평가를 위해 대상 IP 주소를 사용합니다.
- 인바운드 규칙은 평가를 위해 소스 IP 주소를 사용합니다.

NACL 규칙은 Transit Gateway에서 인스턴스로 이동하는 트래픽에 대해 다음과 같이 적용됩니다.

- 아웃바운드 규칙은 평가되지 않습니다.
- 인바운드 규칙은 평가되지 않습니다.

EC2 인스턴스 및 Transit Gateway 연결에 다른 서브넷 사용

한 서브넷에 EC2 인스턴스가 있고 다른 서브넷에 Transit Gateway 연결이 있으며 각 서브넷이 다른 네트워크 ACL과 연결된 구성을 고려합니다.

네트워크 ACL 규칙은 EC2 인스턴스 서브넷에 대해 다음과 같이 적용됩니다.

- 아웃바운드 규칙은 대상 IP 주소를 사용하여 인스턴스에서 Transit Gateway로 이동하는 트래픽을 평가합니다.
- 인바운드 규칙은 소스 IP 주소를 사용하여 Transit Gateway에서 인스턴스로 이동하는 트래픽을 평가합니다.

NACL 규칙은 Transit Gateway 서브넷에 대해 다음과 같이 적용됩니다.

- 아웃바운드 규칙은 대상 IP 주소를 사용하여 Transit Gateway에서 인스턴스로 이동하는 트래픽을 평가합니다.
- 아웃바운드 규칙은 인스턴스에서 Transit Gateway로의 트래픽을 평가하는 데 사용되지 않습니다.
- 인바운드 규칙은 소스 IP 주소를 사용하여 인스턴스에서 Transit Gateway로 이동하는 트래픽을 평가합니다.
- 인바운드 규칙은 Transit Gateway에서 인스턴스로 이동하는 트래픽을 평가하는 데 사용되지 않습니다.

모범 사례

각 Transit Gateway VPC 첨부 파일에 대해 별도의 서브넷을 사용합니다. 서브넷별로 작은 CIDR(예: /28)을 사용하여 EC2 리소스를 위한 주소를 더 많이 확보하십시오. 별도의 서브넷을 사용하는 경우 다음을 구성할 수 있습니다.

- Transit Gateway 서브넷과 연결된 인바운드 및 아웃바운드 NACL을 그대로 열어 둡니다.
- 트래픽 흐름에 따라 NACL을 워크로드 서브넷에 적용할 수 있습니다.

VPC 연결의 작동 방식에 대한 자세한 내용은 [the section called “리소스 연결”](#) 단원을 참조하세요.

Transit Gateway에 대한 할당량

환승 게이트웨이와 관련된 할당량 (이전에는 한도라고 함) AWS 계정은 다음과 같습니다. 다르게 표시되지 않는 한 리전별로 각 할당량이 적용됩니다.

Service Quotas 콘솔이 계정의 할당량에 관한 정보를 제공합니다. Service Quotas 콘솔을 사용하면 기본 할당량을 확인하고 조정 가능한 할당량에 대한 [할당량 증가를 요청](#)할 수 있습니다. 자세한 내용은 Service Quotas 사용 설명서의 [할당량 증가 요청](#)을 참조하십시오.

Service Quotas에서 조정 가능한 할당량을 아직 사용할 수 없는 경우 지원 사례를 열 수 있습니다.

일반

명칭	기본값	조정 가능
계정당 Transit Gateway 수	5	예
전송 게이트웨이당 CIDR 블록 수	5	아니요

CIDR 블록은 [the section called “Connect 연결 및 Connect 피어”](#) 기능에서 사용됩니다.

라우팅

명칭	기본값	조정 가능
전송 게이트웨이당 전송 게이트웨이 라우팅 테이블 수	20	예
단일 전송 게이트웨이의 모든 라우팅 테이블(동적 및 정적)을 합친 총 경로	10,000개	예
가상 라우터 어플라이언스에서 Connect 피어로 공개된 동적 라우팅	1,000	예
전송 게이트웨이의 Connect 피어에서 가상 라우터 어플라이언스로 공개된 라우팅	5,000	아니요

명칭	기본값	조정 가능
단일 연결에 대한 접두사의 정적 경로 수	1	아니요

공개된 경로는 Connect 연결에 연결된 라우팅 테이블에서 가져옵니다.

Transit Gateway Attachment

전송 게이트웨이는 동일한 VPC에 둘 이상의 VPC 연결을 가질 수 없습니다.

명칭	기본값	조정 가능
전송 게이트웨이당 연결 수	5,000	아니요
VPC당 Transit Gateway 수	5	아니요
전송 게이트웨이당 피어링 연결 수	50	예
전송 게이트웨이당 보류 중인 피어링 연결 수	10	예
두 트랜짓 게이트웨이 간 또는 하나의 트랜짓 게이트웨이와 클라우드 WAN 코어 네트워크 에지 (CNE) 간의 피어링 어태치먼트	1	아니요
Connect 연결당 Connect 피어(GRE 터널)	4	아니요

대역폭

Site-to-Site VPN 연결을 통해 실현된 대역폭에 영향을 줄 수 있는 요인은 패킷 크기, 트래픽 혼합(TCP/UDP), 중간 네트워크의 셰이핑 또는 제한 정책, 인터넷 날씨 및 특정 애플리케이션 요구 사항을 포함 하되 이에 국한되지 않습니다. VPC 연결, AWS Direct Connect 게이트웨이 또는 피어링된 Transit Gateway Attachment의 경우 기본값 이상으로 추가 대역폭을 제공하려고 합니다.

명칭	기본값	조정 가능
가용 영역별 VPC 연결당 대역폭	최대 100Gbps	추가 지원 필요 시 솔루션스 아키텍트(SA)

명칭	기본값	조정 가능
		또는 기술 계정 관리자 (TAM)에게 문의하세요.
가용 영역별 전송 게이트웨이 VPC 연결당 초당 패킷 수	최대 7,500,000	추가 지원 필요 시 솔루션스 아키텍트(SA) 또는 기술 계정 관리자 (TAM)에게 문의하세요.
지역 내 사용 가능한 가용 영역별 AWS Direct Connect 게이트웨이 또는 피어링된 트랜짓 게이트웨이 연결 대역폭	최대 100Gbps	추가 지원 필요 시 솔루션스 아키텍트(SA) 또는 기술 계정 관리자 (TAM)에게 문의하세요.
지역 내 사용 가능한 가용 영역별 전송 게이트웨이 연결 (AWS Direct Connect 및 피어링 첨부 파일) 당 초당 패킷 수	최대 7,500,000	추가 지원 필요 시 솔루션스 아키텍트(SA) 또는 기술 계정 관리자 (TAM)에게 문의하세요.
VPN 터널당 최대 대역폭	최대 1.25Gbps	아니요
VPN 터널당 초당 최대 패킷 수	최대 140,000	아니요
Connect 연결마다 Connect 피어(GRE 터널)당 최대 대역폭	최대 5Gbps	아니요
Connect 피어당 초당 최대 패킷 수	최대 300,000	아니요

등가 다중 경로 라우팅(ECMP)을 사용하면 여러 개의 VPN 터널을 집계하여 더 높은 VPN 대역폭을 얻을 수 있습니다. ECMP를 사용하려면 동적 라우팅에 대해 VPN 연결을 구성해야 합니다. 정적 라우팅을 사용하는 VPN 연결에서는 ECMP가 지원되지 않습니다.

기본 전송 (VPC 또는) 연결이 필요한 대역폭을 지원하는 경우 Connect 연결당 최대 4개의 Connect 피어를 생성할 수 있습니다 (Connect 연결당 총 대역폭은 최대 20Gbps AWS Direct Connect). 동일한 전

송 게이트웨이의 다중 Connect 연결에서 또는 동일한 Connect 연결의 다중 Connect 피어에서 수평 확장을 통해 ECMP를 사용하여 더 높은 대역폭을 얻을 수 있습니다. 전송 게이트웨이는 동일한 Connect 피어의 BGP 피어링 사이에서 ECMP를 사용할 수 없습니다.

AWS Direct Connect 게이트웨이

명칭	기본값	조정 가능
AWS Direct Connect 트랜짓 게이트웨이당 게이트웨이	20	아니요
게이트웨이당 트랜짓 게이트웨이 AWS Direct Connect	6	아니요

최대 전송 단위(MTU)

- 네트워크 연결의 MTU는 연결을 통해 전달될 수 있는 최대 허용 패킷의 크기 (바이트)입니다. 연결의 MTU가 클수록 하나의 패킷으로 전달할 수 있는 데이터의 양이 늘어납니다. 트랜짓 게이트웨이는 VPC, Transit Gateway Connect 및 피어링 첨부 파일 간의 트래픽에 대해 8500바이트의 MTU를 지원합니다. AWS Direct Connect VPN 연결을 통한 트래픽은 1,500바이트의 MTU를 가질 수 있습니다.
- Transit Gateway를 사용하기 위해 VPC 피어링에서 마이그레이션할 때 VPC 피어링과 Transit Gateway 간에 MTU 크기가 일치하지 않으면 일부 비대칭 트래픽 패킷이 삭제될 수 있습니다. 크기 불일치로 인해 정보 패킷이 삭제되지 않도록 두 VPC를 동시에 업데이트합니다.
- 8,500바이트보다 큰 패킷이 Transit Gateway에 도착하면 삭제됩니다.
- Transit Gateway는 ICMPv4 패킷의 FRAG_NEEDED 또는 ICMPv6 패킷의 PTB(Packet Too Big)를 생성하지 않습니다. 따라서 PMTUD(경로 MTU 검색)가 지원되지 않습니다.
- Transit Gateway는 모든 패킷에 대해 MSS(최대 세그먼트 크기) 클램핑을 적용합니다. 자세한 내용은 [RFC879](#)를 참조하세요.
- MTU의 Site-to-Site VPN 할당량에 대한 자세한 내용을 알아보려면 AWS Site-to-Site VPN 사용 설명서의 [최대 전송 단위\(MTU\)](#)를 참조하세요.

멀티캐스트

명칭	기본값	조정 가능
전송 게이트웨이당 멀티캐스트 도메인 수	20	예
전송 게이트웨이당 멀티캐스트 네트워크 인터페이스 수	10,000개	예
VPC당 멀티캐스트 도메인 연결 수	20	예
전송 게이트웨이 멀티캐스트 그룹당 소스 수	1	예
전송 게이트웨이당 정적 및 IGMPv2 멀티캐스트 그룹 멤버 수 및 소스 수	10,000개	아니요
전송 게이트웨이 멀티캐스트 그룹당 정적 및 IGMPv2 멀티캐스트 그룹 멤버 수	100	아니요
흐름 당 최대 멀티캐스트 처리량	1Gbps	아니요
가용 영역당 최대 집계 멀티캐스트 처리량	20Gbps	아니요

AWS 네트워크 관리자

이름	기본값	조정 가능
글로벌 네트워크 (PR) AWS 계정	5	예
글로벌 네트워크당 디바이스 수	200	예
글로벌 네트워크당 링크 수	200	예
글로벌 네트워크당 사이트 수	200	예
글로벌 네트워크당 연결 수	500	아니요

추가 할당량 리소스

자세한 내용은 다음 자료를 참조하세요.

- AWS Site-to-Site VPN 사용 설명서의 [Site-to-Site VPN 할당량](#)
- Amazon VPC 사용 설명서의 [Amazon VPC 할당량](#)
- AWS Direct Connect 사용 설명서의 [AWS Direct Connect 할당량](#)

전송 게이트웨이의 문서 기록

다음 표에서는 전송 게이트웨이 릴리스를 설명합니다.

변경 사항	설명	날짜
AWS Transit Gateway 할당량	대역폭 제한이 추가되었습니다.	2023년 8월 14일
AWS Transit Gateway 흐름 로그	전송 게이트웨이는 이제 전송 게이트웨이 흐름 로그를 지원하므로 전송 게이트웨이 간의 네트워크 트래픽을 모니터링하고 기록할 수 있습니다.	2022년 7월 14일
전송 게이트웨이 정책 테이블	정책 테이블을 사용하여 피어링된 전송 게이트웨이 유형과 라우팅 및 연결 가능성 정보를 자동으로 교환하기 위해 전송 게이트웨이에 대한 동적 라우팅을 설정합니다.	2022년 7월 13일
Network Manager 사용 설명서	Network Manager는 독립적인 사용 설명서로 분리되었으며 더 이상 AWS Transit Gateway 사용 설명서에 포함되지 않습니다.	2021년 12월 2일
피어링 연결	동일한 리전에서 전송 게이트웨이를 사용하여 피어링 연결을 생성할 수 있습니다.	2021년 12월 1일
전송 게이트웨이 연결	전송 게이트웨이와 VPC에서 실행하는 서드 파티 가상 어플라이언스 간에 연결을 설정할 수 있습니다.	2020년 12월 10일

어플라이언스 모드	VPC 연결에서 어플라이언스 모드를 활성화하면 연결에서 양방향 트래픽이 동일한 가용 영역을 통과하게 할 수 있습니다.	2020년 10월 29일
접두사 목록 참조	전송 게이트웨이 라우팅 테이블에서 접두사 목록을 참조할 수 있습니다.	2020년 8월 24일
전송 게이트웨이 수정	전송 게이트웨이에 대한 구성 옵션을 수정할 수 있습니다.	2020년 8월 24일
Transit Gateway Attachment에 대한 CloudWatch 지표	개별 Transit Gateway Attachment에 대한 CloudWatch 지표를 볼 수 있습니다.	2020년 7월 6일
Network Manager Route Analyzer	글로벌 네트워크의 전송 게이트웨이 라우팅 테이블에 있는 라우팅을 분석할 수 있습니다.	2020년 5월 4일
피어링 연결	다른 리전에서 전송 게이트웨이를 사용하여 피어링 연결을 생성할 수 있습니다.	2019년 12월 3일
멀티캐스트 지원	전송 게이트웨이는 연결된 VPC의 서브넷 간에 멀티캐스트 트래픽 라우팅을 지원하며 여러 수신 인스턴스로 향하는 트래픽을 보내는 인스턴스에 대한 멀티캐스트 라우터 역할을 합니다.	2019년 12월 3일
AWS Network Manager	전송 게이트웨이를 중심으로 구축된 글로벌 네트워크를 시각화하고 모니터링할 수 있습니다.	2019년 12월 3일

AWS Direct Connect 지원	AWS Direct Connect 게이트웨이를 사용하여 전송 가상 인터페이스를 통해 Transit Gateway에 연결된 VPC 또는 VPN에 AWS Direct Connect를 연결할 수 있습니다.	2019년 3월 27일
최초 릴리스	이 릴리스에서는 전송 게이트웨이가 도입되었습니다.	2018년 11월 26일

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.