AWS 클라우드에서 VPC의 아웃바운드 네트워크 트래픽 보호

AWS 권장 가이드

AWS 권장 가이드: AWS 클라우드에서 VPC의 아웃바운드 네트워크 트래픽 보호

Table of Contents

AWS 클라우드에서 VPC의 아웃바운드 네트워크 트래픽 보호

Kirankumar Chandrashekar 및 Abdal Garuba, Amazon Web Services(AWS)

2022년 11월(문서 기록)

이 가이드에서는 Amazon Virtual Private Cloud(VPC)를 사용할 경우 아웃바운드 네트워크 트래픽을 보호하고 모니터링하는 모범 사례를 다룹니다. 또한 탄력적 네트워크 인터페이스와 AWS 클라우드의 Virtual Private Cloud(VPCs)에서 발생하는 아웃바운드 네트워크 트래픽을 모니터링하는 데 도움이 되는 AWS 도구도 설명합니다.

> **Note**
>
> 이 가이드에서는 추가 보안 계층을 제공하기 AWS 위해와 통합할 수 있는 타사 도구에 대해서는 다루지 않습니다. 또한 클라우드 전용 아키텍처를 가정합니다. 이 가이드는 하이브리드 아키텍처에는 적용되지 않습니다.

이 가이드에는 다음과 같은 모범 사례가 요약되어 있습니다.

- 기존 트래픽 패턴을 분석하여 VPC의 보안 요구 사항 결정
- 보안 그룹을 사용하여 VPC의 아웃바운드 트래픽 제한
- AWS Network Firewall 및 DNS 호스트 이름을 사용하여 VPC의 아웃바운드 트래픽 제한
- VPC 엔드포인트를 사용하여 AWS 리소스에 액세스
- 를 사용하여 내부 애플리케이션 간에 프라이빗 연결 설정 AWS PrivateLink
- VPCs 피어링 또는 AWS 리전 를 사용하여 VPC 간 통신 AWS Transit Gateway

> **Note**
>
> 최상의 보안 태세를 위해 아웃바운드 트래픽을 전용 경로를 통해 방화벽 어플라이언스와 같은 필터링 도구로 전달할 수도 있습니다.

목표 비즈니스 성과

이 가이드는 다음을 수행하는 데 도움이 됩니다.

1. VPC의 아웃바운드 네트워크 트래픽을 제어하고 모니터링합니다.
2. AWS 리소스 간의 트래픽이 AWS 백본 네트워크에서 제어하는 안전한 프라이빗 경로를 통과하는지 확인합니다.
3. 아웃바운드 네트워크 트래픽을 지속적으로 모니터링하고 승인되지 않은 엔드포인트에 대한 요청을 중지하는 AWS 도구를 구현합니다.

VPC의 보안 요구 사항 결정

> **중요**
>
> 테스트 환경에서 VPC의 아웃바운드 트래픽 보안 아키텍처를 설계하고 테스트하는 것이 가장 좋습니다. 개발 환경에서 아키텍처 변경을 테스트하면 의도하지 않은 시스템 동작을 실시간으로 푸시할 위험을 줄일 수 있습니다.

네트워크의 아웃바운드 트래픽 패턴을 변경하기 전에 애플리케이션이 의도한 대로 작동하는 데 필요한 트래픽 패턴을 이해하는 것이 중요합니다. 이 정보는 네트워크를 재설계할 때 허용할 트래픽 패턴과 거부할 트래픽 패턴을 식별하는 데 도움이 될 수 있습니다.

VPC의 기존 아웃바운드 트래픽 패턴을 분석하려면 먼저 VPC Flow Logs를 켭니다. 그런 다음 테스트 환경을 사용하여 다양한 사용 시나리오를 통해 애플리케이션을 실행하고 흐름 로그에서 시뮬레이션된 트래픽을 분석합니다.

VPC Flow Logs는 VPC의 인바운드 및 아웃바운드 IP 트래픽을 기록합니다. 그러면 Amazon VPC가 Amazon Simple Storage Service(S3)나 Amazon CloudWatch로 로그를 보냅니다. 다음 도구 중 하나를 사용하여 로그를 보고 분석할 수 있습니다.

- (Amazon S3용) Amazon Athena
- (CloudWatch용) CloudWatch Logs Insights

자세한 내용과 예제 쿼리는 다음을 참조하세요.

- Amazon VPC Flow Logs 쿼리(Amazon Athena 사용 설명서)
- CloudWatch Logs Insights 쿼리를 VPC 흐름 로그와 함께 사용하려면 어떻게 해야 하나요? (AWS 지식 센터)
- CloudWatch Logs Insights 쿼리 구문(Amazon CloudWatch Logs 사용 설명서)

VPC Flow Logs가 캡처하는 정보 유형에 대한 자세한 내용은 Amazon VPC 사용 설명서의 Flow log record examples를 참조하세요.

> **Note**
>
> VPC Flow Logs는 DNS 호스트 이름과 같은 애플리케이션 계층(계층 7) 정보를 캡처하지 않습니다. 보안 요구 사항에 따라 애플리케이션 계층 데이터 분석이 필요한 경우 AWS Network Firewall을 배포하여 필요한 세부 정보를 캡처할 수 있습니다. 자세한 내용은이 가이드의 AWS Network Firewall 및 DNS 호스트 이름을 사용하여 VPC의 아웃바운드 트래픽 제한 섹션을 참조하세요.

VPC Flow Logs를 사용할 때 VPC의 아웃바운드 트래픽 분석 모범 사례

Amazon Athena 또는 CloudWatch Logs Insights 쿼리를 사용하여 VPC Flow Logs를 분석할 때는 다음을 수행해야 합니다.

- 애플리케이션이 사용하는 리소스에 연결된 탄력적 네트워크 인터페이스를 통해 흐르는 인바운드 및 아웃바운드 트래픽을 식별하고 분석합니다.
- NAT 게이트웨이에 연결된 네트워크 인터페이스를 통해 흐르는 애플리케이션 트래픽을 식별하고 분석합니다.
- 쿼리의 소스 주소를 네트워크 인터페이스의 사설 IP 주소로 설정하여 네트워크 인터페이스의 모든 아웃바운드 트래픽을 캡처해야 합니다.
- 예상치 못한 트래픽 패턴에만 초점을 맞추도록 쿼리를 작성합니다. (예를 들어, 애플리케이션이 HTTPS API 엔드포인트 같은 타사 엔터티와 통신하는 경우 해당 엔터티를 포함하지 않도록 쿼리를 구성할 수 있습니다.)
- 각 포트 및 대상 IP 주소의 유효성을 조사합니다. (예를 들어, 아웃바운드 대상 포트 22는 Bastion Host의 경우 정상이거나 SSH를 사용하여 Git에서 리포지토리를 복제하는 호스트일 수 있습니다.)

> **Note**
>
> Amazon Athena를 처음 사용하는 경우 쿼리 결과 위치를 구성해야 합니다. 지침은 Amazon Athena 사용 설명서의 Athena 콘솔을 사용하여 쿼리 결과 위치 지정을 참조하세요.

Amazon Athena 쿼리 예제

특정 네트워크 인터페이스에서 아웃바운드 관리자 트래픽을 반환하는 Athena 쿼리의 예

다음 Athena 쿼리는 IP 주소가 10.100.0.10인 네트워크 인터페이스에서 아웃바운드 관리 트래픽의 처음 200줄을 반환합니다.

```
SELECT * FROM "<vpc_flow_logs_table_name>"

WHERE interface_id = 'eni-1234567890000000' AND srcaddr LIKE '10.100.0.10' AND dstport
 < 1024

LIMIT 200;
```

출력 예제

#	1
version	2
account_id	<account-id>
interface_id	eni-123456789000000
srcaddr	10.32.0.10
dstaddr	11.22.33.44
srcport	36952
dstport	443
protocol	6
packets	25
bytes	5445
start	1659310200
end	1659310225
action	ACCEPT
log_status	정상

date	2022-07-16

> **Note**
>
> 이 패턴의 출력 형식은 프레젠테이션용이며 시스템에서 다르게 나타날 수 있습니다.

특정 VPC로부터 가장 많은 트래픽을 수신하는 외부 IP 주소를 반환하는 Athena 쿼리의 예

다음 Athena 쿼리는 '10.32'로 시작하는 CIDR 블록이 있는 VPC에서 가장 많은 아웃바운드 트래픽을 수신하는 외부 IP 주소와 포트를 반환합니다.

```
SELECT dstport, dstaddr,

count(*) AS count

FROM "<vpc_flow_logs_table_name>"

WHERE dstaddr not like '10.32%' AND interface_id = 'eni-1234567890000000'

GROUP BY dstport, dstaddr

ORDER BY count desc

LIMIT 200;
```

출력 예제

#	Dstport	Dstaddr	count
1	443	52.x.x.x	1442
2	443	63.x.x.x	1201
3	443	102.x.x.x	887

특정 VPC에서 거부된 아웃바운드 트래픽을 반환하는 Athena 쿼리의 예

다음 Athena 쿼리는 '10.32'로 시작하는 CIDR 블록이 있는 VPC에서 거부된 아웃바운드 트래픽을 반환합니다.

```
SELECT *

FROM "<vpc_flow_logs_table_name>"

WHERE srcaddr like '10.32%' AND action LIKE 'REJECT'
```

출력 예제

#	1
version	2
account_id	<account-id>
interface_id	eni-123456789000000
srcaddr	10.32.0.10
dstaddr	11.22.33.44
srcport	36952
dstport	443
protocol	6
packets	25
bytes	5445
start	1659310200
end	1659310225
action	REJECT
log_status	정상

date	2022-07-16

> **Note**
>
> 이 패턴의 출력 형식은 프레젠테이션용이며 시스템에서 다르게 나타날 수 있습니다.

흐름 로그 레코드에 대한 자세한 내용은 Amazon VPC 사용 설명서의 흐름 로그 레코드를 참조하세요.

CloudWatch 로그 인사이트 쿼리 예제

특정 네트워크 인터페이스에서 아웃바운드 관리자 트래픽을 반환하는 CloudWatch Logs Insights 쿼리의 예

다음 CloudWatch Logs Insights 쿼리는 IP 주소가 10.100.0.10인 네트워크 인터페이스에서 아웃바운드 관리 트래픽의 처음 200개 결과를 반환합니다.

```
fields @timestamp, @message

| filter interfaceId = 'eni-1234567890000000'

| filter srcAddr = '10.100.0.10'

| filter dstPort < 1024

| limit 200
```

출력 예제

필드	값
@ingestionTime	1659310250813
@log	<account-id>:/aws/vpc/flowlogs
@logStream	eni-123456789000000-all

@message	2 <account-id> eni-123456789000000 10.100.0.10 11.22.33.44 36952 443 6 25 5445 1659310200 1659310225 ACCEPT OK
@timestamp	1659310200000
accountId	<account-id>
작업	ACCEPT
bytes	5445
dstAddr	11.22.33.44
dstPort	443
end	1659310225
interfaceId	eni-123456789000000
logStatus	정상
packets	25
프로토콜	6
srcAddr	10.100.0.10
srcPort	36952
시작	1659310200
version	2

특정 VPC로부터 가장 많은 트래픽을 수신하는 외부 IP 주소를 반환하는 CloudWatch Logs Insights 쿼리의 예

다음 CloudWatch Logs Insights 쿼리는 '10.32'로 시작하는 CIDR 블록이 있는 VPC에서 가장 많은 아웃바운드 트래픽을 수신하는 외부 IP 주소와 포트를 반환합니다.

```
filter @logstream = 'eni-1234567890000000'
```

```
| stats count(*) as count by dstAddr, dstPort

| filter dstAddr not like '10.32'

| order by count desc

| limit 200
```

출력 예제

#	dstAddr	dstPort	count
1	52.x.x.x	443	439
2	51.79.x.x	63.x.x.x	25

특정 VPC에서 거부된 아웃바운드 트래픽을 반환하는 CloudWatch Logs Insights 쿼리의 예

다음 CloudWatch Logs Insights 쿼리는 '10.32'로 시작하는 CIDR 블록이 있는 VPC에서 거부된 아웃바운드 트래픽을 반환합니다.

```
filter @logstream = 'eni-0123456789000000'

| fields @timestamp, @message

| filter action='REJECT'
```

출력 예제

필드	값
@ingestionTime	1666991000899
@log	<account-id>:/aws/vpc/flowlogs
@logStream	eni-0123456789000000-all

@message	2 <account-id> 'eni-0123456789000000' 185.x.x.x 10.10.2.222 55116 11211 17 1 43 1666990939 1666990966 REJECT OK
@timestamp	1666990939000
accountId	<account-id>
작업	REJECT
bytes	43
dstAddr	10.10.2.222
dstPort	11211
end	1666990966
interfaceId	'eni-0123456789000000'
logStatus	정상
packets	1
프로토콜	17
srcAddr	185.x.x.x
srcPort	55116
시작	1666990939
version	2

VPC의 아웃바운드 트래픽 제한

보안 그룹을 사용하여 VPC의 아웃바운드 트래픽 제한

아키텍처의 아웃바운드 트래픽 요구 사항을 평가한 후 조직의 보안 요구 사항에 맞게 VPC의 보안 그룹 규칙을 수정하기 시작합니다. 필요한 포트, 프로토콜, 대상 IP 주소를 모두 보안 그룹의 허용 목록에 추가해야 합니다.

지침은 Amazon VPC 사용 설명서의 보안 그룹을 사용하여 리소스에 대한 트래픽 제어를 참조하세요.

> **중요**
>
> 테스트 환경에서 VPC의 보안 그룹 규칙을 업데이트한 후에는 애플리케이션이 여전히 예상대로 작동하고 있는지 확인합니다. 자세한 내용은 이 가이드의 VPC Flow Logs를 사용할 때 VPC의 아웃바운드 트래픽 분석 모범 사례를 참조하세요.

특정 AWS 서비스에 대한 주요 보안 그룹 고려 사항

Amazon Elastic Compute Cloud(Amazon EC2)

VPC를 생성할 경우 VPC는 모든 아웃바운드 트래픽을 허용하는 기본 보안 그룹과 함께 제공됩니다. Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스는 사용자 지정 보안 그룹을 생성하지 않는 한 이 기본 보안 그룹을 사용합니다.

> **중요**
>
> Amazon EC2 인스턴스가 실수로 기본 보안 그룹을 사용하는 위험을 완화하려면 그룹의 아웃바운드 규칙을 모두 제거합니다. 자세한 내용은 Amazon VPC 사용 설명서의 보안 그룹 규칙으로 작업 섹션에서 보안 그룹 규칙 삭제를 참조하세요.

Amazon Relational Database Service(RDS)

데이터베이스가 클라이언트 역할을 하지 않는 한 Amazon RDS DB 인스턴스에 대한 모든 아웃바운드 보안 그룹 규칙을 제거할 수 있습니다. 자세한 내용은 Amazon RDS 사용 설명서의 VPC 보안 그룹 개요를 참조하세요.

Amazon ElastiCache

인스턴스가 클라이언트 역할을 하지 않는 한 Amazon ElastiCache(Redis OSS) 및 Amazon ElastiCache(Memcached) 인스턴스에 대한 모든 아웃바운드 보안 그룹 규칙을 제거할 수 있습니다. 자세한 내용은 다음을 참조하세요.

- 보안 그룹: EC2-Classic(Amazon ElastiCache(Redis OSS) 사용 설명서)
- ElastiCache 및 Amazon VPCs 이해(Amazon ElastiCache(Memcached) 사용 설명서)

AWS Network Firewall 및 DNS 호스트 이름을 사용하여 VPC의 아웃바운드 트래픽 제한

애플리케이션이 동적 IP 주소를 사용하는 경우 IP 주소 대신 DNS 호스트 이름을 사용하여 VPC의 아웃바운드 트래픽을 필터링하는 것이 가장 좋습니다. 예를 들어, 애플리케이션이 Application Load Balancer를 사용하는 경우 노드가 계속 확장되므로 애플리케이션의 관련 IP 주소가 변경됩니다. 이러한 유형의 상황에서는 고정 IP 주소보다 DNS 호스트 이름을 사용하여 아웃바운드 네트워크 트래픽을 필터링하는 것이 더 안전합니다.

AWS Network Firewall을 사용하여 HTTPS 트래픽의 SNI(Server Name Indication)에서 제공하는 호스트 이름 세트에 대한 VPC 아웃바운드 인터넷 액세스를 제한할 수 있습니다.

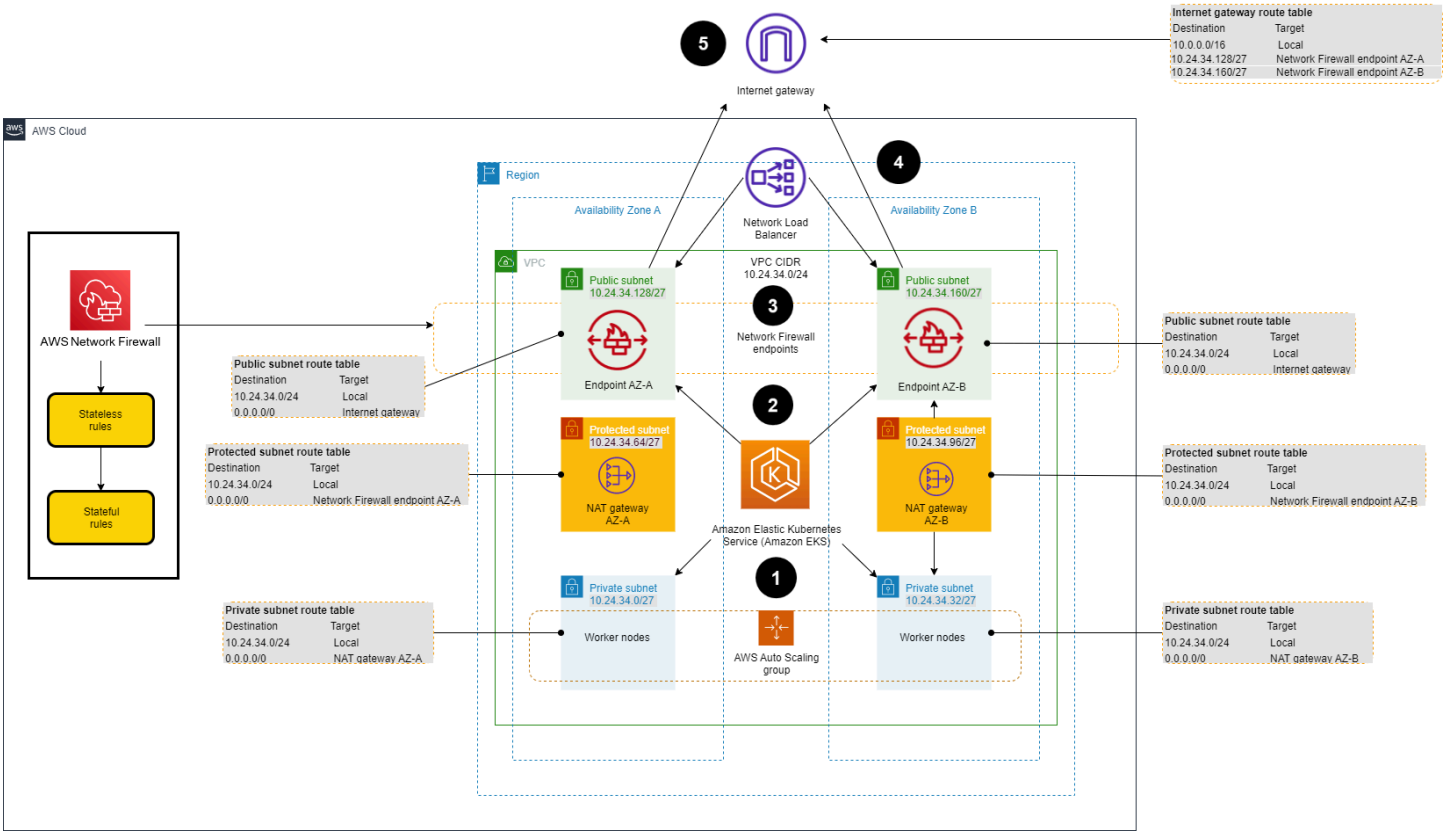
자세한 내용과 예제 Network Firewall 정책 규칙은 AWS Network Firewall Developer Guide의 Domain filtering을 참조하세요. 자세한 지침은 AWS Prescriptive Guidance(APG) 패턴, Use Network Firewall to capture the DNS domain names from the Server Name Indication (SNI) for outbound traffic을 참조하세요.

> **Note**
>
> SNI는 트래픽 흐름에서 암호화되지 않은 상태로 유지되는 TLS의 확장입니다. 클라이언트가 HTTPS를 통해 액세스를 시도하는 대상 호스트 이름을 나타냅니다.

> **중요**
>
> 테스트 환경에서 Network Firewall 상태 저장 규칙을 업데이트한 후 애플리케이션이 여전히 예상대로 작동하는지 확인합니다. SNI에서 제공하는 필수 DNS 도메인 이름이 차단되지 않았는지 확인합니다.

아키텍처 예

다음 다이어그램은를 사용하여 DNS 호스트 이름을 사용하여 VPC의 아웃바운드 트래픽을 필터링 AWS Network Firewall 하는 아키텍처의 예를 보여줍니다.



이 다이어그램은 다음 워크플로를 보여줍니다.

1. 아웃바운드 요청은 프라이빗 서브넷 내에서 시작되며 보호된 서브넷의 NAT 게이트웨이로 전송됩니다.
2. NAT 게이트웨이에서 수신한 HTTPS 트래픽은 퍼블릭 서브넷의 AWS Network Firewall 엔드포인트로 라우팅됩니다.
3. AWS Network Firewall 는 요청을 검사하고 구성된 방화벽 정책 규칙을 적용하여 인터넷 게이트웨이에 전달하기 위한 요청을 수락하거나 거부합니다.
4. 승인된 아웃바운드 요청은 인터넷 게이트웨이로 전송됩니다.
5. 인터넷 게이트웨이에서 승인된 트래픽은 인터넷으로 전송되어 의도한 URL(SNI에서 암호화되지 않은 HTTPS 헤더에 제공)에 액세스합니다.

AWS 리소스 액세스

VPC 엔드포인트는 인터넷 게이트웨이 또는 NAT 게이트웨이 없이 VPC와 지원되는 AWS 서비스 간에 프라이빗 연결을 제공합니다. 예를 들어, VPC 엔드포인트를 사용하여 Amazon Simple Storage Service(S3) 또는 Amazon Elastic Container Registry(Amazon ECR)에 VPC를 연결할 수 있습니다.

Amazon VPC는 세 가지 유형의 VPC 엔드포인트를 제공합니다.

- 인터페이스 엔드포인트VPCs를에서 지원하는 Amazon VPC 서비스에 연결합니다 AWS PrivateLink.
- 게이트웨이 엔드포인트는 특히 Amazon S3 및 Amazon DynamoDB에 대한 안정적인 연결을 제공합니다.
- Gateway Load Balancer 엔드포인트는 Gateway Load Balancer 뒤에서 호스팅되는 사용자 지정 애플리케이션에 VPC를 연결합니다.

지원되는 서비스 목록은 Amazon VPC 설명서의 AWS PrivateLink와 통합되는AWS 서비스를 참조하세요.

> **Note**
>
> Gateway Load Balancer 엔드포인트는 애플리케이션의 VPC 또는 AWS 계정 외부의 사용자에게 애플리케이션을 비공개로 공유할 때 유용합니다. 자세한 내용은 이 가이드의 내부 애플리케이션 간 프라이빗 연결 설정을 참조하세요.

내부 애플리케이션 간 프라이빗 연결 설정

클라우드 기반 애플리케이션의 엔드포인트는를 사용하여 AWS 클라우드에서 비공개로 공유할 수 있습니다 AWS PrivateLink. 자세한 내용과 예제 아키텍처는 AWS PrivateLink 설명서를 참조하세요.

더 많은 예제 아키텍처는 다음 AWS 권장 가이드 패턴을 참조하세요.

- AWS PrivateLink 및 Network Load Balancer를 사용하여 Amazon ECS에서 컨테이너 애플리케이션에 비공개로 액세스
- AWS FargateAWS PrivateLink및 Network Load Balancer를 사용하여 Amazon ECS에서 컨테이너 애플리케이션에 비공개로 액세스
- AWS PrivateLink 및 Network Load Balancer를 사용하여 Amazon EKS에서 컨테이너 애플리케이션에 비공개로 액세스

VPCs 및 간 통신 AWS 리전

다중 VPC 인프라는 조직이 워크로드를 분할하고 설치 공간을 확장하는 데 도움이 될 수 있습니다. 또한 이러한 유형의 아키텍처는 리소스가 서로 다른 VPCs AWS 리전및 AWS 계정의 AWS 서비스와 통신해야 하는 경우 문제를 일으킬 수 있습니다.

두 VPC 간의 연결을 설정하려면 VPC 피어링 또는 AWS Transit Gateway를 사용합니다. VPC 피어링 연결은 프라이빗 IPv4 또는 IPv6 주소를 사용하여 두 VPCs 간의 트래픽을 라우팅하는 두 VPC 간의 네트워킹 연결입니다.는 VPCs 단일 Transit Gateway 인스턴스에 AWS Transit Gateway 연결하여 조직의 전체 AWS 라우팅 구성을 한 곳에 통합합니다.

자세한 내용은 확장 가능하고 안전한 다중 VPC AWS 네트워크 인프라 구축 AWS 백서를 참조하세요.

> **Note**
>
> 다중 VPC AWS 네트워크 인프라를 대규모로 생성하고 관리하려면 AWS Transit Gateway을 사용하는 것이 가장 좋습니다.

VPC 피어링과AWS Transit Gateway중에서 선택 시 주요 고려 사항

VPC 피어링

- 각 VPC 간 트래픽은 각 VPC 간에 개별적으로 관리됩니다.
- VPC 피어링은 전이적 라우팅을 지원하지 않습니다. 서로 통신해야 하는 각 VPC 간에는 직접 VPC 피어링 연결이 필요합니다.

AWS Transit Gateway

- 각 VPC 간의 트래픽은 각 VPC를 연결하는 중앙 집중식 허브 역할을 하는 AWS Transit Gateway 서비스를 통해 관리됩니다.
- AWS Transit Gateway 는 전이적 라우팅을 지원합니다. 트래픽은 라우팅 테이블을 사용하여 연결된 모든 네트워크 간에 라우팅됩니다.

다음 단계

다중 VPC 관리에 대한 자세한 내용은 Amazon VPC 사용 설명서의 다른 계정과 VPC 공유하기를 참조하세요.

리소스

- VPC 흐름 로그를 사용하여 IP 트래픽 로깅(Amazon VPC 사용 설명서)
- Analyzing Logs with CloudWatch Insights(Amazon Managed Service for Apache Flink Developer Guide)
- 보안 그룹을 통한 액세스 제어(Amazon RDS 사용 설명서)

문서 기록

아래 표에 이 가이드의 주요 변경 사항이 설명되어 있습니다. 향후 업데이트에 대한 알림을 받으려면 RSS 피드를 구독하십시오.

변경 사항	설명	날짜
최초 게시	—	2022년 11월 2일

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