아키텍처 다이어그램

AWS Direct Connect의 트래픽 암호화 옵션

AWS Direct Connect의 트래픽 암호화 옵션: 아키텍처 다이어그램

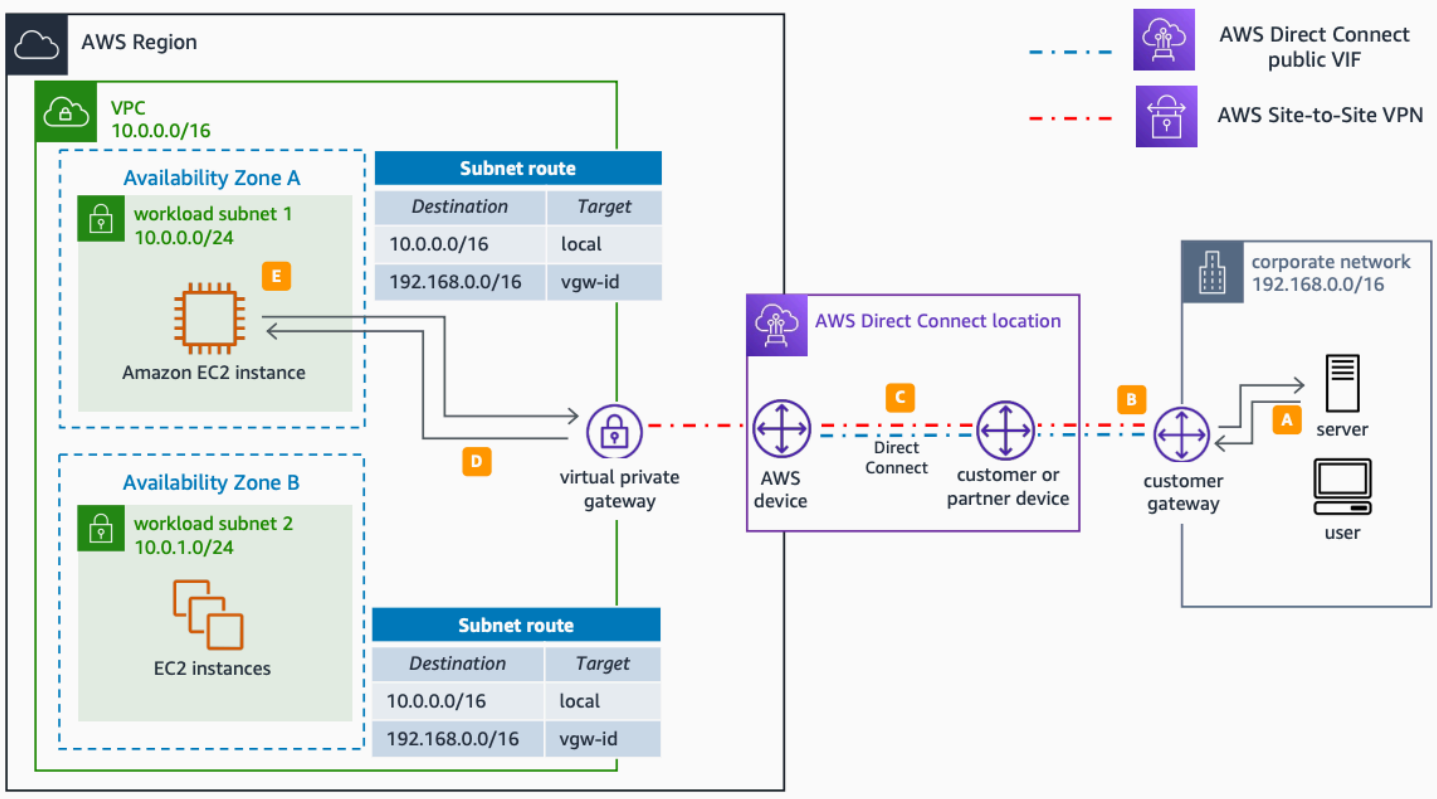
Table of Contents

Amazon VPC에 대한 AWS Site-to-Site VPN

게시 날짜: 2025년 3월 5일(다이어그램 기록)

이 방법은 Amazon VPC의 리소스에 도달할 때 end-to-end 보안 IPSec 연결의 이점과 AWS Direct Connect의 짧은 지연 시간 및 일관된 네트워크 환경을 결합하여 트래픽 암호화를 달성합니다.

VPC 아키텍처에 대한 Direct Connect 퍼블릭 VIF를 통한 Site-to-Site VPN



구성 단계:

1. AWS Direct Connect 연결을 생성합니다. 전용 연결의 경우 AWS 디바이스와 해당 위치의 디바이스(또는 파트너 디바이스) 간에 교차 연결을 설정합니다. 호스팅 연결의 경우 호스팅 연결을 사용하려면 먼저 해당 연결을 수락해야 합니다.
2. 연결이 설정되면 기존 연결을 통해 AWS Direct Connect 퍼블릭 가상 인터페이스(VIF)를 생성합니다. VIF를 가져오도록 고객 게이트웨이를 구성합니다.
3. VIF의 경계 게이트웨이 프로토콜(BGP) 피어가 설정되면는 퍼블릭 VIF를 통해 퍼블릭 IP 범위를 고객 게이트웨이 디바이스에 AWS 알립니다.

4. Amazon VPC와 연결된 가상 프라이빗 게이트웨이에 대한 AWS Site-to-Site VPN을 생성합니다.는 퍼블릭 VIF를 통해 연결할 수 있는 퍼블릭 IP 주소가 있는 가상 프라이빗 게이트웨이에 연결된 두 개의 VPN 엔드포인트를 AWS 제공합니다.
5. VPN 파라미터로 고객 게이트웨이를 구성하여 AWS Site-to-Site VPN 연결을 가져옵니다.

샘플 트래픽 흐름:

A. 회사 네트워크에 있는 클라이언트는 VPC에 있는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 IP 주소에 도달해야 하므로 트래픽은 고객 게이트웨이를 통해 라우팅됩니다.

B. 고객 게이트웨이는 VPC에 대한 최상의 경로가 AWS Site-to-Site VPN 터널을 통하는 것이라고 판단합니다. 트래픽은 IPSec 터널의 암호화 파라미터를 기반으로 암호화되며 암호화된 패킷의 대상은 VPN 엔드포인트 퍼블릭 IP 주소입니다.

C. 고객 게이트웨이는 AWS VPN 엔드포인트 퍼블릭 IP 주소로의 최상의 경로가 Direct Connect 퍼블릭 VIF를 통하는 것이라고 판단합니다.

D. AWS VPN 엔드포인트는 암호화된 IPSec 트래픽을 수신하고 해독합니다. 원래 IP 대상 주소는 VPC의 Amazon EC2 인스턴스이므로 트래픽은 VPC 패브릭을 통해 Amazon EC2 인스턴스로 라우팅됩니다.

E. Amazon EC2 인스턴스에서 회사 네트워크에 위치한 클라이언트로의 트래픽 반환은 역방향이지만 동일한 경로를 따릅니다.

참조 자료

자세한 내용은 다음 리소스를 참조하세요.

- AWS 아키텍처 아이콘
- AWS 아키텍처 센터
- AWS Well-Architected

다이어그램 기록

이 참조 아키텍처 다이어그램의 업데이트에 대한 알림을 받으려면 RSS 피드를 구독하세요.

변경 사항	설명	날짜

최초 게시	참조 아키텍처 다이어그램이 처음 게시되었습니다.	2025년 3월 5일
최초 게시	참조 아키텍처 다이어그램이 처음 게시되었습니다.	2025년 3월 5일
최초 게시	참조 아키텍처 다이어그램이 처음 게시되었습니다.	2025년 3월 5일
최초 게시	참조 아키텍처 다이어그램이 처음 게시되었습니다.	2025년 3월 5일

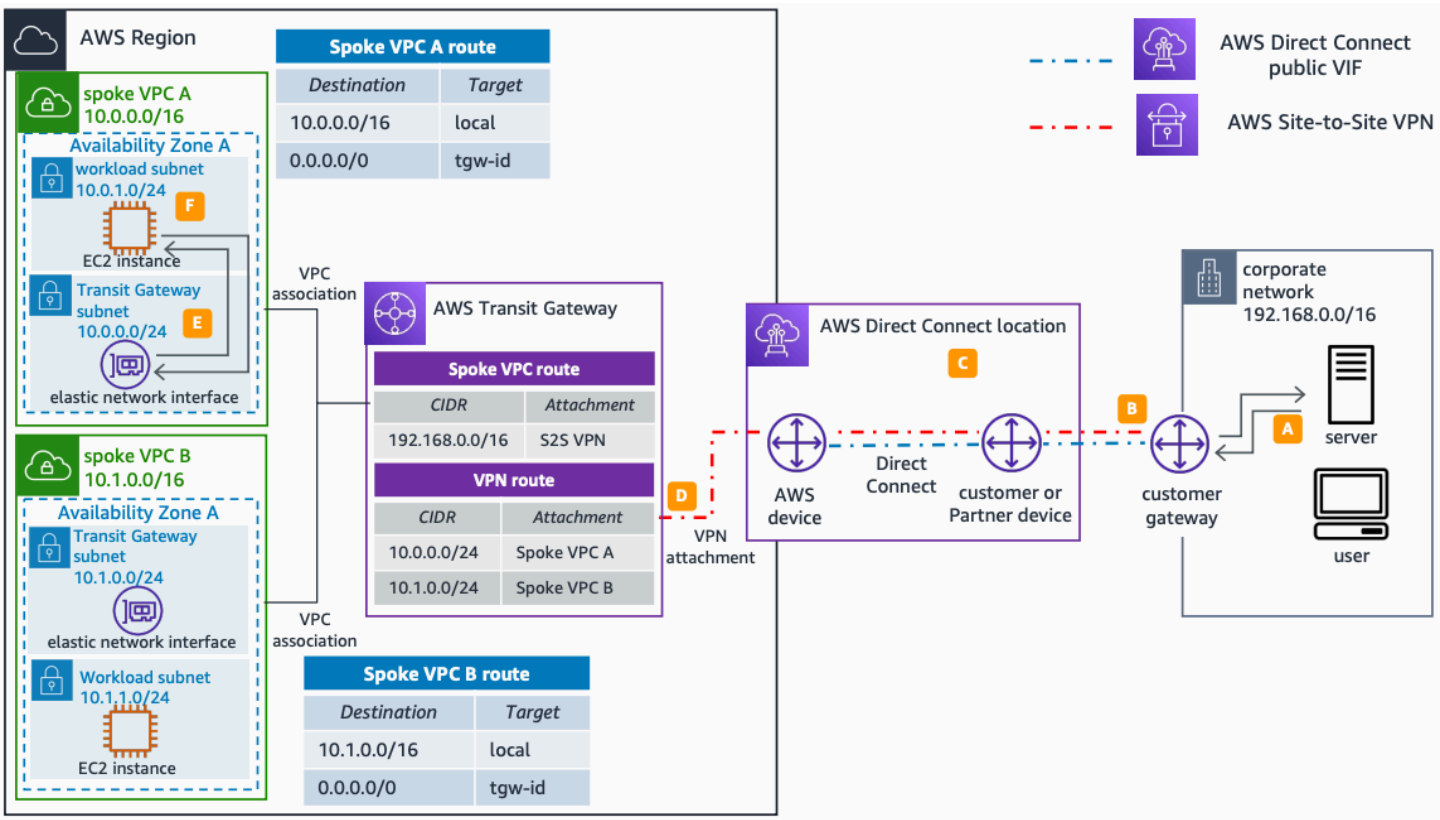
> **Note**
>
> RSS 업데이트를 구독하려면 사용 중인 브라우저에 대해 RSS 플러그인이 활성화되어 있어야 합니다.

AWS Site-to-Site VPN에서 AWS Transit Gateway로(퍼블릭 VIF)

게시 날짜: 2025년 3월 5일(다이어그램 기록)

이 방법은 end-to-end 보안 IPSec 연결의 이점을 AWS AWS Transit Gateway를 통해 Amazon VPCs의 리소스에 도달할 때 AWS Direct Connect의 짧은 지연 시간 및 일관된 네트워크 경험과 결합하여 트래픽 암호화를 달성합니다. 이 접근 방식은 AWS 환경에서 여러 VPCs에 연결해야 하는 고객에게 적합합니다.

Direct Connect 퍼블릭 VIF를 통한 Site-to-Site VPN-Transit Gateway 아키텍처



구성 단계:

1. AWS Direct Connect 연결을 생성합니다. 전용 연결의 경우 AWS 디바이스와 해당 위치의 디바이스(또는 파트너 디바이스) 간에 교차 연결을 설정합니다. 호스팅 연결의 경우 연결을 사용하려면 먼저 연결을 수락해야 합니다.

2. 연결이 설정되면 AWS Direct Connect 퍼블릭 가상 인터페이스를 생성합니다. VIF를 가져오도록 고객 게이트웨이를 구성합니다.
3. VIF의 BGP 피어가 설정되면는 퍼블릭 VIF를 통해 퍼블릭 IP 범위를 고객 게이트웨이 디바이스에 AWS 알립니다.
4. AWS Site-to-Site VPN을 생성하고 AWS Transit Gateway 인스턴스를 AWS 측의 VPN 집중기로 선택합니다.
5. AWS VPN 연결을 가져오고 AWS VPN 연결을 통해 전송 게이트웨이로 향하는 트래픽을 라우팅하도록 VPN 파라미터로 고객 게이트웨이를 구성합니다.

샘플 트래픽 흐름:

A. 회사 네트워크에 있는 클라이언트는 네트워크 트래픽을 스포크 VPC A에 있는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 IP 주소로 라우팅하고 고객 게이트웨이를 통해 트래픽을 라우팅해야 합니다.

B. 고객 게이트웨이는 VPC에 대한 최상의 경로가 AWS Site-to-Site VPN 터널을 통하는 것이라고 판단합니다. 트래픽은 IPSec 터널의 암호화 파라미터를 기반으로 암호화되며 암호화된 패킷의 대상은 AWS VPN 엔드포인트 퍼블릭 IP 주소입니다.

C. 고객 게이트웨이는 AWS VPN 엔드포인트 퍼블릭 IP 주소로의 최상의 경로가 Direct Connect 퍼블릭 VIF를 통하는 것이라고 판단합니다.

D. Transit Gateway에 연결된 AWS VPN 엔드포인트는 암호화된 IPSec 트래픽을 수신하여 Transit Gateway로 전달합니다.

E. 트래픽은 복호화되고 스포크 VPC A로 전달되며 Amazon EC2 인스턴스로 라우팅됩니다.

F. Amazon EC2 인스턴스에서 회사 네트워크로의 반환 트래픽은 역방향이지만 동일한 경로를 따릅니다.

참조 자료

자세한 내용은 다음 리소스를 참조하세요.

- AWS 아키텍처 아이콘
- AWS 아키텍처 센터
- AWS Well-Architected

다이어그램 기록

이 참조 아키텍처 다이어그램의 업데이트에 대한 알림을 받으려면 RSS 피드를 구독하세요.

변경 사항	설명	날짜
최초 게시	참조 아키텍처 다이어그램이 처음 게시되었습니다.	2025년 3월 5일
최초 게시	참조 아키텍처 다이어그램이 처음 게시되었습니다.	2025년 3월 5일
최초 게시	참조 아키텍처 다이어그램이 처음 게시되었습니다.	2025년 3월 5일
최초 게시	참조 아키텍처 다이어그램이 처음 게시되었습니다.	2025년 3월 5일

> **Note**
>
> RSS 업데이트를 구독하려면 사용 중인 브라우저에 대해 RSS 플러그인이 활성화되어 있어야 합니다.

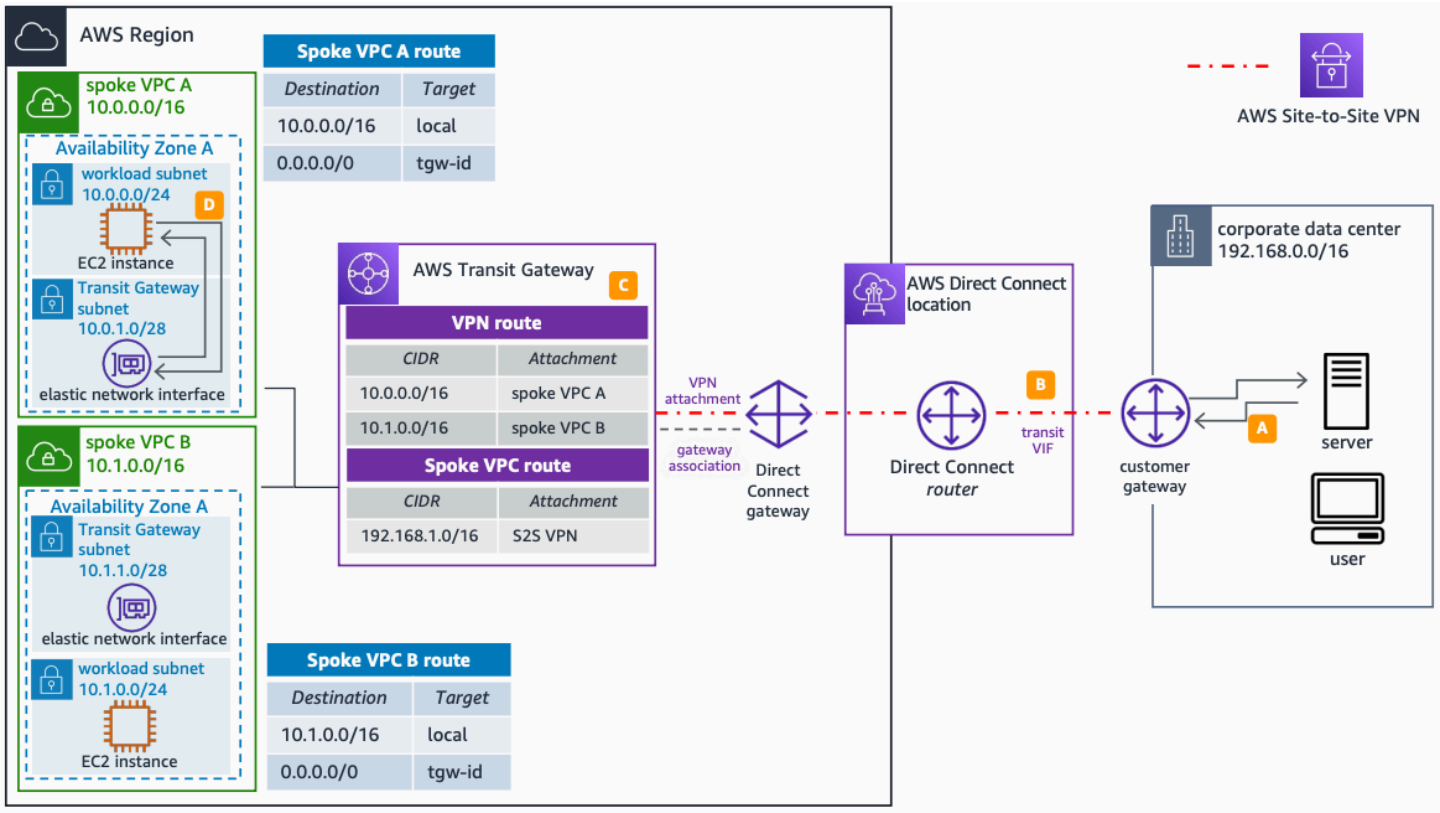
AWS Site-to-Site VPN 프라이빗 IP VPN에서 AWS Transit Gateway로

게시 날짜: 2025년 3월 5일(다이어그램 기록)

AWS Site-to-Site VPN 프라이빗 IP VPN 연결은 프라이빗 IP 주소를 사용하여 AWS Direct Connect를 통해 생성되므로 보안 및 네트워크 프라이버시가 동시에 향상됩니다. 프라이빗 IP VPNs은 전송 VIFs 및 Direct Connect 게이트웨이 위에 기본 전송으로 배포됩니다.

프라이빗 IP VPNs에 대한 자세한 내용은 AWS 블로그의 AWS Site-to-Site 프라이빗 IP VPNs 소개를 참조하세요.

Direct Connect 전송 VIF를 통해 전송 게이트웨이 아키텍처로 프라이빗 IP VPN



구성 단계:

1. AWS Direct Connect 연결을 생성합니다. 전용 연결의 경우 디바이스와 AWS 디바이스(또는 파트너 디바이스) 간의 교차 연결을 위치에 설정합니다. 호스팅 연결의 경우 호스팅 연결을 사용하려면 먼저 해당 연결을 수락해야 합니다.
2. 연결이 설정되면 Direct Connect 전송 가상 인터페이스(VIF) 및 Direct Connect 게이트웨이를 생성합니다. VIF를 가져오도록 고객 게이트웨이를 구성합니다.
3. AWS Transit Gateway를 Direct Connect 게이트웨이에 연결하여 Transit Gateway CIDR 블록을이 연결에서 허용되는 접두사로 지정합니다. 이 CIDR 블록이 Amazon VPC CIDR 블록 또는 온프레미스 CIDR 범위와 겹치지 않도록 해야 합니다.
4. Direct Connect 게이트웨이와 전송 VIF를 기본 전송으로 사용하여 AWS Site-to-Site VPN을 생성합니다.
5. AWS Site-to-Site VPN 터널을 가져오고 AWS Site-to-Site VPN 연결을 통해 전송 게이트웨이로 향하는 트래픽을 라우팅합니다.

샘플 트래픽 흐름:

A. 회사 네트워크에 있는 클라이언트는 네트워크 트래픽을 스포크 VPC A에 있는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 IP 주소로 라우팅하고 고객 게이트웨이를 통해 트래픽을 라우팅해야 합니다.

B. 고객 게이트웨이는 VPC에 대한 최상의 경로가 AWS Site-to-Site VPN 연결을 통하는 것이라고 판단합니다. 트래픽은 전송 VIF 및 Direct Connect 게이트웨이를 기본 전송 네트워크로 사용하여 선택한 암호화 방법을 사용하여 IPSec 터널을 통해 흐릅니다.

C. 트래픽은 Transit Gateway에 도착합니다. Transit Gateway VPN 라우팅 테이블에 따라 트래픽은 스포크 VPC A로 전달된 다음 Amazon EC2 인스턴스로 라우팅됩니다.

D. Amazon EC2 인스턴스에서 회사 네트워크에 위치한 클라이언트로의 반환 트래픽은 역방향이지만 동일한 경로를 따릅니다.

참조 자료

자세한 내용은 다음 리소스를 참조하세요.

- AWS 아키텍처 아이콘
- AWS 아키텍처 센터
- AWS Well-Architected

다이어그램 기록

이 참조 아키텍처 다이어그램의 업데이트에 대한 알림을 받으려면 RSS 피드를 구독하세요.

변경 사항	설명	날짜
최초 게시	참조 아키텍처 다이어그램이 처음 게시되었습니다.	2025년 3월 5일
최초 게시	참조 아키텍처 다이어그램이 처음 게시되었습니다.	2025년 3월 5일
최초 게시	참조 아키텍처 다이어그램이 처음 게시되었습니다.	2025년 3월 5일
최초 게시	참조 아키텍처 다이어그램이 처음 게시되었습니다.	2025년 3월 5일

> **Note**
>
> RSS 업데이트를 구독하려면 사용 중인 브라우저에 대해 RSS 플러그인이 활성화되어 있어야 합니다.

AWS Direct Connect의 MACsec 보안

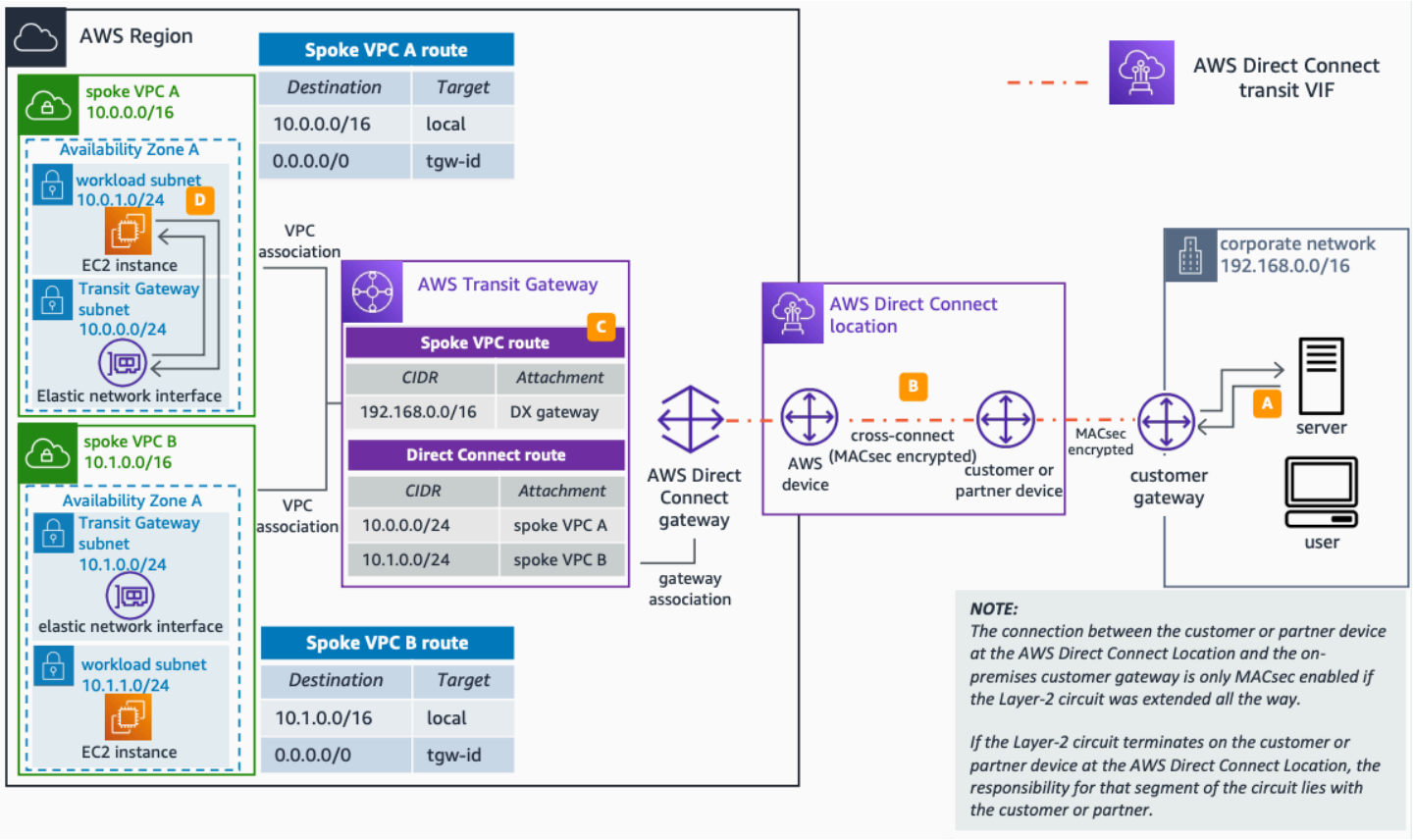
게시 날짜: 2025년 3월 5일(다이어그램 기록)

이 방법은 MACsec 보안(IEEE 802.1AE)을 사용하여 트래픽을 암호화하여 10Gbps 및 100Gbps 링크에 대해 라인에 가까운 point-to-point 암호화를 제공합니다.

AWS Direct Connect의 MACsec에 대한 자세한 내용은 AWS 블로그의 AWS Direct Connect 연결에 MACsec 보안 추가를 참조하세요.

> **Note**
>
> AWS Direct Connect 위치의 고객 또는 파트너 디바이스와 온프레미스 고객 게이트웨이 간의 연결은 Layer-2 회로가 완전히 확장된 경우에만 MACsec이 활성화됩니다. AWS Direct Connect 위치에서 고객 또는 파트너 디바이스에서 Layer-2 회로가 종료되는 경우 해당 회로 세그먼트에 대한 책임은 고객 또는 파트너에게 있습니다.

Direct Connect 아키텍처의 MACsec 암호화



구성 단계:

1. AWS Direct Connect 전용 연결에서 MACsec을 구성하려면 엔드의 디바이스가 MACsec을 지원하는지 확인합니다. 또한 Direct Connect 위치는 MACsec도 지원해야 합니다.
2. MACsec 지원 포트의 옵션을 선택하여 10G 또는 100G AWS Direct Connect 전용 연결을 생성합니다.
3. MACsec 보안 키에 대한 연결 키 이름(CKN) 및 연결 연결 키(CAK) 페어를 생성합니다. 키 페어가 디바이스(또는 파트너 디바이스)와 호환되는지 확인합니다.
4. 교차 연결을 설정하고 디바이스(또는 파트너 디바이스)에 대한 물리적 연결을 완료합니다. CKN/CAK 페어로 끝에서 디바이스를 업데이트합니다.
5. AWS 관리 콘솔, AWS 명령줄 인터페이스(CLI) 또는 API를 통해 CKN/CAK 페어를 연결에 연결합니다.
6. AWS Transit Gateway와 연결된 새 MACsec 지원 연결에서 Direct Connect 게이트웨이로 전송 VIF를 생성합니다. AWS Transit Gateway

샘플 트래픽 흐름:

A. 회사 네트워크에 있는 클라이언트는 네트워크 트래픽을 스포크 VPC A에 있는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 IP 주소로 라우팅하고 트래픽을 고객 게이트웨이로 라우팅해야 합니다.

B. 고객 게이트웨이는 VPC에 대한 최상의 경로가 전송 VIF를 통과하는 것으로 판단하여 트래픽을 Direct Connect 연결을 통해 전송해야 함을 나타냅니다.

C. Transit Gateway Direct Connect 라우팅 테이블에 따라 트래픽은 스포크 VPC A로 전달된 다음 Amazon EC2 인스턴스로 라우팅됩니다.

D. Amazon EC2 인스턴스에서 회사 네트워크에 위치한 클라이언트로의 트래픽 반환은 역방향이지만 동일한 경로를 따릅니다.

참조 자료

자세한 내용은 다음 리소스를 참조하세요.

- AWS 아키텍처 아이콘
- AWS 아키텍처 센터
- AWS Well-Architected

다이어그램 기록

이 참조 아키텍처 다이어그램의 업데이트에 대한 알림을 받으려면 RSS 피드를 구독하세요.

변경 사항	설명	날짜
최초 게시	참조 아키텍처 다이어그램이 처음 게시되었습니다.	2025년 3월 5일
최초 게시	참조 아키텍처 다이어그램이 처음 게시되었습니다.	2025년 3월 5일
최초 게시	참조 아키텍처 다이어그램이 처음 게시되었습니다.	2025년 3월 5일
최초 게시	참조 아키텍처 다이어그램이 처음 게시되었습니다.	2025년 3월 5일

> **Note**
>
> RSS 업데이트를 구독하려면 사용 중인 브라우저에 대해 RSS 플러그인이 활성화되어 있어야 합니다.

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