AWS 백서

Amazon Virtual Private Cloud 연결 옵션

Amazon Virtual Private Cloud 연결 옵션: AWS 백서

Table of Contents

Amazon Virtual Private Cloud 연결 옵션

발행일: 2023년 4월 5일 () 문서 수정

요약

Amazon VPC (Virtual Private Cloud) 를 사용하면 고객이 Amazon Web Services (AWS) 클라우드의 격리된 프라이빗 섹션을 프로비저닝하여 고객이 정의한 IP 주소 범위를 사용하여 가상 네트워크에서 AWS 리소스를 시작할 수 있습니다. Amazon VPC는 고객에게 AWS 가상 네트워크를 다른 원격 네트워크에 연결할 수 있는 여러 옵션을 제공합니다. 이 문서에서는 고객이 사용할 수 있는 몇 가지 일반적인 네트워크 연결 옵션에 대해 설명합니다. 여기에는 원격 고객 네트워크를 Amazon VPC와 통합하고 여러 Amazon VPC를 인접한 가상 네트워크에 연결하는 연결 옵션이 포함됩니다.

이 백서는 사용 가능한 연결 옵션을 검토하려는 기업 네트워크 설계자와 엔지니어 또는 Amazon VPC 관리자를 대상으로 합니다. 이 백서는 네트워크 연결 논의를 촉진하기 위한 다양한 옵션에 대한 개요를 제공하고 더 자세한 정보 또는 예제가 포함된 추가 설명서 및 리소스를 안내합니다.

소개

Amazon VPC는 현재 네트워크 설계 및 요구 사항에 따라 사용할 수 있는 여러 네트워크 연결 옵션을 제공합니다. 이러한 연결 옵션에는 인터넷 또는 AWS Direct Connect 연결을 네트워크 백본으로 사용하는 것과 AWS 또는 사용자 관리형 네트워크 엔드포인트에 대한 연결을 종료하는 것이 포함됩니다. 또한 AWS에서는 AWS 서비스 또는 사용자 관리 네트워크 장비 및 경로를 활용하여 Amazon VPC와 네트워크 간에 네트워크 라우팅을 제공하는 방법을 선택할 수 있습니다. 이 백서에서는 다음 옵션에 대한 개요와 각 옵션에 대한 개괄적인 비교를 제공합니다.

- 네트워크와 아마존 VPC 연결 옵션
  - AWS Site-to-Site VPN — 원격 네트워크의 네트워크 장비에서 Amazon VPC로 관리형 IPsec VPN 연결을 설정하는 방법을 설명합니다.
  - AWS Transit Gateway + AWS 사이트 간 VPN — 를 사용하여 원격 네트워크의 네트워크 장비에서 Amazon VPC용 지역 네트워크 허브로 관리형 IPsec VPN 연결을 설정하는 방법을 설명합니다. AWS Transit Gateway
  - AWS Direct Connect- 를 사용하여 원격 네트워크에서 Amazon VPC로 비공개적이고 논리적인 연결을 설정하는 방법을 설명합니다. AWS Direct Connect
  - AWS Direct Connect + AWS Transit Gateway— AWS Direct Connect 및 AWS Transit Gateway 를 사용하여 Amazon VPC용 원격 네트워크에서 지역 네트워크 허브로 논리적으로 사설 연결을 설정하는 방법을 설명합니다.
  - AWS Direct Connect+ AWS Site-to-Site VPN — AWS AWS Direct Connect Site-to-Site VPN을 사용하여 원격 네트워크에서 Amazon VPC로 암호화된 프라이빗 연결을 설정하는 방법을 설명합니다.
  - AWS Direct ConnectAWS Transit Gateway + AWS 사이트 간 VPN— AWS Direct Connect 및 AWS Transit Gateway 를 사용하여 원격 네트워크에서 Amazon VPC용 지역 네트워크 허브로 암호화된 개인 연결을 설정하는 방법을 설명합니다.
  - AWS VPN CloudHub— 원격 지사 연결을 위한 hub-and-spoke 모델 수립에 대해 설명합니다.
  - 소프트웨어 VPN— 원격 네트워크의 장비에서 Amazon VPC 내에서 실행되는 사용자 관리형 소프트웨어 VPN 어플라이언스로 VPN 연결을 설정하는 방법을 설명합니다.
  - AWS Transit Gateway + SD-WAN 솔루션- AWS 백본 또는 인터넷을 전송 네트워크로 사용하여 여러 원격 위치를 Amazon VPC용 지역 네트워크 허브에 상호 연결하는 소프트웨어 정의 광역 네트워크 (SD-WAN) 솔루션의 통합에 대해 설명합니다.
- 아마존 VPC와 아마존 VPC 연결 옵션

  - VPC 피어링— Amazon VPC 피어링 기능을 사용하여 지역 내부 및 지역 간에 Amazon VPC를 연결하는 방법을 설명합니다.
  - AWS Transit Gateway— hub-and-spoke 모델을 사용하여 AWS Transit Gateway 지역 내 및 지역 간에 Amazon VPC를 연결하는 방법을 설명합니다.
  - AWS PrivateLink— Amazon VPC를 VPC 인터페이스 엔드포인트 및 VPC 엔드포인트 서비스와 연결하는 방법을 설명합니다.
  - 소프트웨어 VPN— 각 Amazon VPC 내에서 실행되는 사용자 관리 소프트웨어 VPN 어플라이언스 간에 설정된 VPN 연결을 사용하여 Amazon VPC를 연결하는 방법을 설명합니다.
  - 소프트웨어 VPN-AWS 사이트 간 VPN— 한 Amazon VPC의 사용자 관리 소프트웨어 VPN 어플라이언스와 다른 Amazon VPC에 연결된 AWS 사이트 간 VPN 간에 설정된 VPN 연결을 사용하여 Amazon VPC를 연결하는 방법을 설명합니다.
- Amazon VPC에 대한 소프트웨어 원격 액세스 연결 옵션
  - AWS 클라이언트 VPN— AWS Client VPN을 활용하여 Amazon VPC에 소프트웨어 원격 액세스를 연결하는 방법을 설명합니다.
  - 소프트웨어 클라이언트 VPN— 사용자 관리 소프트웨어 VPN 어플라이언스를 활용하여 Amazon VPC에 소프트웨어 원격 액세스를 연결하는 방법을 설명합니다.
- 트랜짓 VPC— 소프트웨어 VPN과 AWS 관리형 VPN을 함께 사용하여 AWS에 글로벌 전송 네트워크를 구축하는 방법을 설명합니다.
- AWS 클라우드 WAN- Amazon VPC, 데이터 센터 및 원격 지점의 리소스 간 글로벌 상호 연결을 쉽게 구축, 관리 및 모니터링할 수 있는 관리형 광역 네트워크 (WAN) 구축에 대해 설명합니다.

네트워크와 아마존 VPC 연결 옵션

이 섹션에서는 원격 네트워크를 Amazon VPC 환경에 연결하기 위한 설계 패턴을 제공합니다. 이러한 옵션은 내부 네트워크를 AWS 클라우드로 확장하여 AWS 리소스를 기존 현장 서비스 (예: 모니터링, 인증, 보안, 데이터 또는 기타 시스템) 와 통합하는 데 유용합니다. 또한 이 네트워크 확장을 통해 내부 사용자는 다른 내부 리소스처럼 AWS에 호스팅된 리소스에 원활하게 연결할 수 있습니다.

원격 고객 네트워크에 대한 VPC 연결은 연결 중인 각 네트워크에 대해 중복되지 않는 IP 범위를 사용할 때 가장 잘 이루어집니다. 예를 들어, 하나 이상의 VPC를 기업 네트워크에 연결하려면 VPC가 고유한 CIDR (클래스 없는 도메인 간 라우팅) 범위로 구성되어 있어야 합니다. 각 VPC에서 사용할 연속적이고 중복되지 않는 단일 CIDR 블록을 할당하는 것이 좋습니다. Amazon VPC 라우팅 및 제약 조건에 대한 추가 정보는 Amazon VPC 자주 묻는 질문을 참조하십시오.

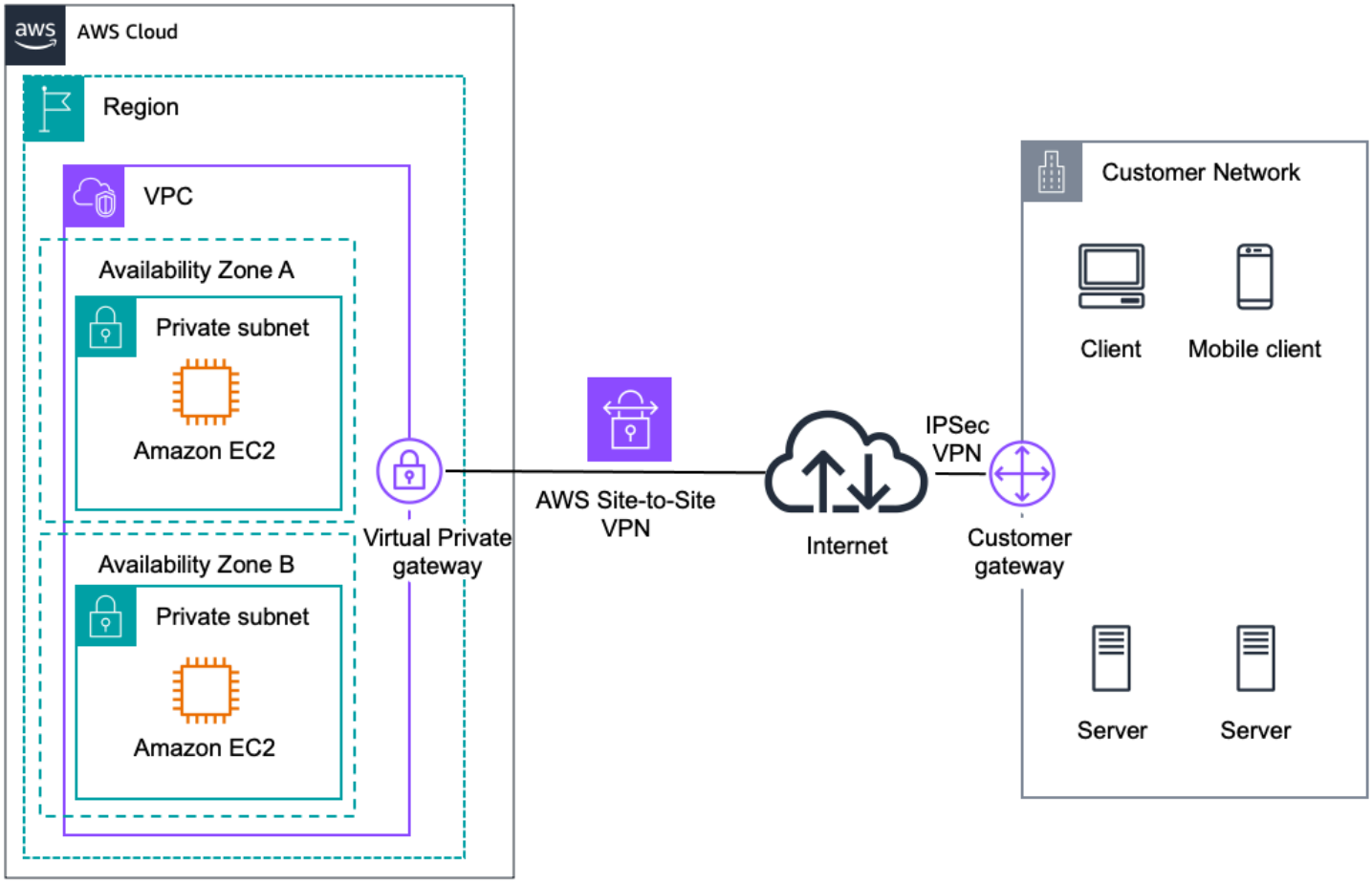
옵션	사용 사례	장점	제한 사항
AWS Site-to-Site VPN	인터넷을 통해 개별 VPC에 대한 AWS의 관리형 IPsec VPN 연결	기존 VPN 장비 및 프로세스 재사용 기존 인터넷 연결 재사용 AWS 관리형 고가용성 VPN 서비스 고정 경로 또는 동적 BGP (보더 게이트웨이 프로토콜) 피어링 및 라우팅 정책을 지원합니다.	네트워크 지연 시간, 변동성 및 가용성은 인터넷 상태에 따라 달라집니다. 이중화 및 페일오버를 구현할 책임은 귀하에게 있습니다 (필요한 경우). 원격 장치는 단일 홉 BGP를 지원해야 합니다 (동적 라우팅에 BGP를 활용하는 경우)
AWS Transit Gateway + AWS 사이트 간 VPN	인터넷을 통한 여러 VPC의 지역 라우터로의 AWS 관리형 IPsec VPN 연결	이전 옵션과 동일합니다. 최대 5,000개의 첨부 파일을 위한 AWS 관	이전 옵션과 동일

옵션	사용 사례	장점	제한 사항
		리형 고가용성 및 확장성 지역 네트워크 허브	
AWS Direct Connect	전용 회선을 통한 전용 네트워크 연결	보다 예측 가능한 네트워크 성능 대역폭 비용 감소 BGP 피어링 및 라우팅 정책 지원	추가 통신 및 호스팅 제공자 관계가 필요하거나 새 네트워크 회로를 프로비저닝해야 할 수 있음
AWS Direct Connect + AWS Transit Gateway	전용 회선을 통해 여러 VPC의 지역 라우터에 전용 네트워크 연결	이전 옵션과 동일 최대 5,000개의 첨부 파일을 위한 AWS 관리형 고가용성 및 확장성 지역 네트워크 허브	이전 옵션과 동일
AWS Direct Connect + AWS 사이트 간 VPN	전용 회선을 통한 IPsec VPN 연결	보다 예측 가능한 네트워크 성능 대역폭 비용 감소 에 대한 BGP 피어링 및 라우팅 정책 지원 AWS Direct Connect 기존 VPN 장비 및 프로세스 재사용 AWS 관리형 고가용성 VPN 서비스 VPN 연결에서 고정 경로 또는 동적 BGP (보더 게이트웨이 프로토콜) 피어링 및 라우팅 정책을 지원합니다.	추가 통신 및 호스팅 제공자 관계가 필요하거나 새 네트워크 회로를 프로비저닝해야 할 수 있음 이중화 및 페일오버를 구현할 책임은 귀하에게 있습니다 (필요한 경우). 원격 장치는 단일 홉 BGP를 지원해야 합니다 (동적 라우팅에 BGP를 활용하는 경우)

옵션	사용 사례	장점	제한 사항
AWS Direct ConnectAWS Transit Gateway + AWS 사이트 간 VPN	여러 VPC의 경우 사설 회선을 통한 지역 라우터에 IPsec VPN 연결	이전 옵션과 동일 최대 5,000개의 첨부 파일을 위한 AWS 관리형 고가용성 및 확장성 지역 네트워크 허브	이전 옵션과 동일
AWS VPN CloudHub	기본 또는 백업 연결을 위한 hub-and-spoke 모델로 원격 지사를 연결합니다.	기존 인터넷 연결 및 AWS VPN 연결 재사용 AWS 관리형 고가용성 VPN 서비스 경로 및 라우팅 우선순위 교환을 위한 BGP 지원	네트워크 지연 시간, 가변성 및 가용성은 인터넷에 따라 다릅니다. 사용자 관리형 지사 엔드포인트는 이중화 및 장애 조치 (필요한 경우) 구현을 담당합니다.
AWS Transit Gateway + SD-WAN 솔루션	AWS 백본 또는 인터넷을 트랜짓 네트워크로 사용하여 소프트웨어 정의 광역 네트워크로 원격 지사와 사무실을 연결합니다.	다양한 SD-WAN 공급업체, 제품 및 프로토콜을 지원합니다. 일부 공급업체 솔루션은 AWS 네이티브 서비스와 통합되어 있습니다.	Amazon VPC에 SD-WAN 어플라이언스를 배치하는 경우 해당 어플라이언스의 HA (고가용성) 를 구현할 책임은 사용자에게 있습니다.
소프트웨어 VPN	인터넷을 통한 소프트웨어 어플라이언스 기반 VPN 연결	다양한 VPN 공급업체, 제품 및 프로토콜 지원 완전 고객 관리형 솔루션	모든 VPN 엔드포인트에 HA (고가용성) 솔루션을 구현할 책임은 귀하에게 있습니다 (필요한 경우).

AWS Site-to-Site VPN

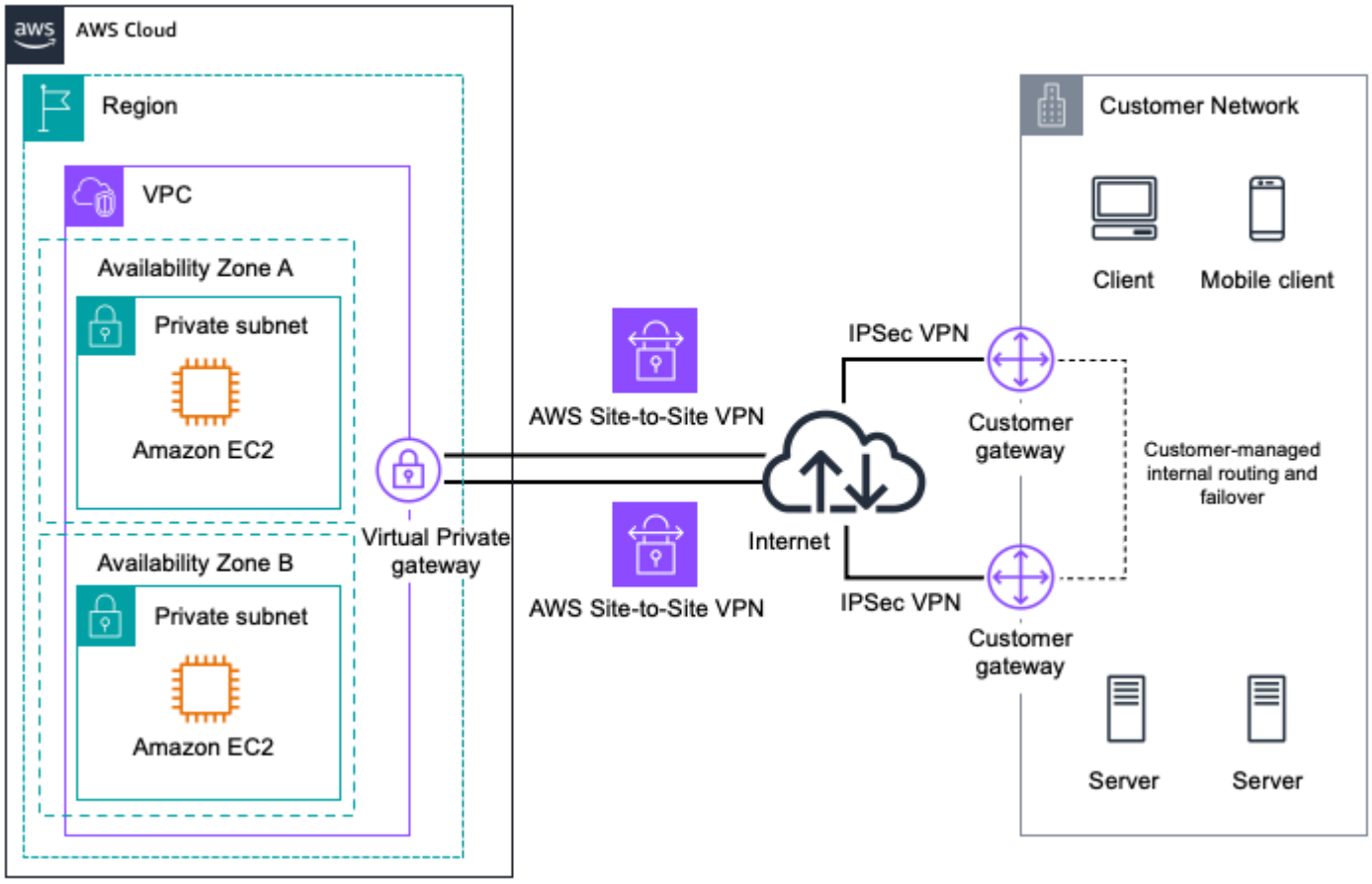
Amazon VPC는 다음 그림과 같이 인터넷을 통해 원격 네트워크와 Amazon VPC 간에 IPsec VPN 연결을 생성하는 옵션을 제공합니다.



AWS Managed VPN

AWS 측 VPN 연결에 내장된 자동 중복성 및 장애 조치가 포함된 AWS 관리형 VPN 엔드포인트를 활용하려는 경우 이 접근 방식을 사용하는 것이 좋습니다.

또한 가상 프라이빗 게이트웨이는 다중 사용자 게이트웨이 연결을 지원하고 권장하므로, 다음 그림과 같이 VPN 연결 측면에서 이중화 및 장애 조치를 구현할 수 있습니다.



Redundant AWS Site-to-Site VPN Connections

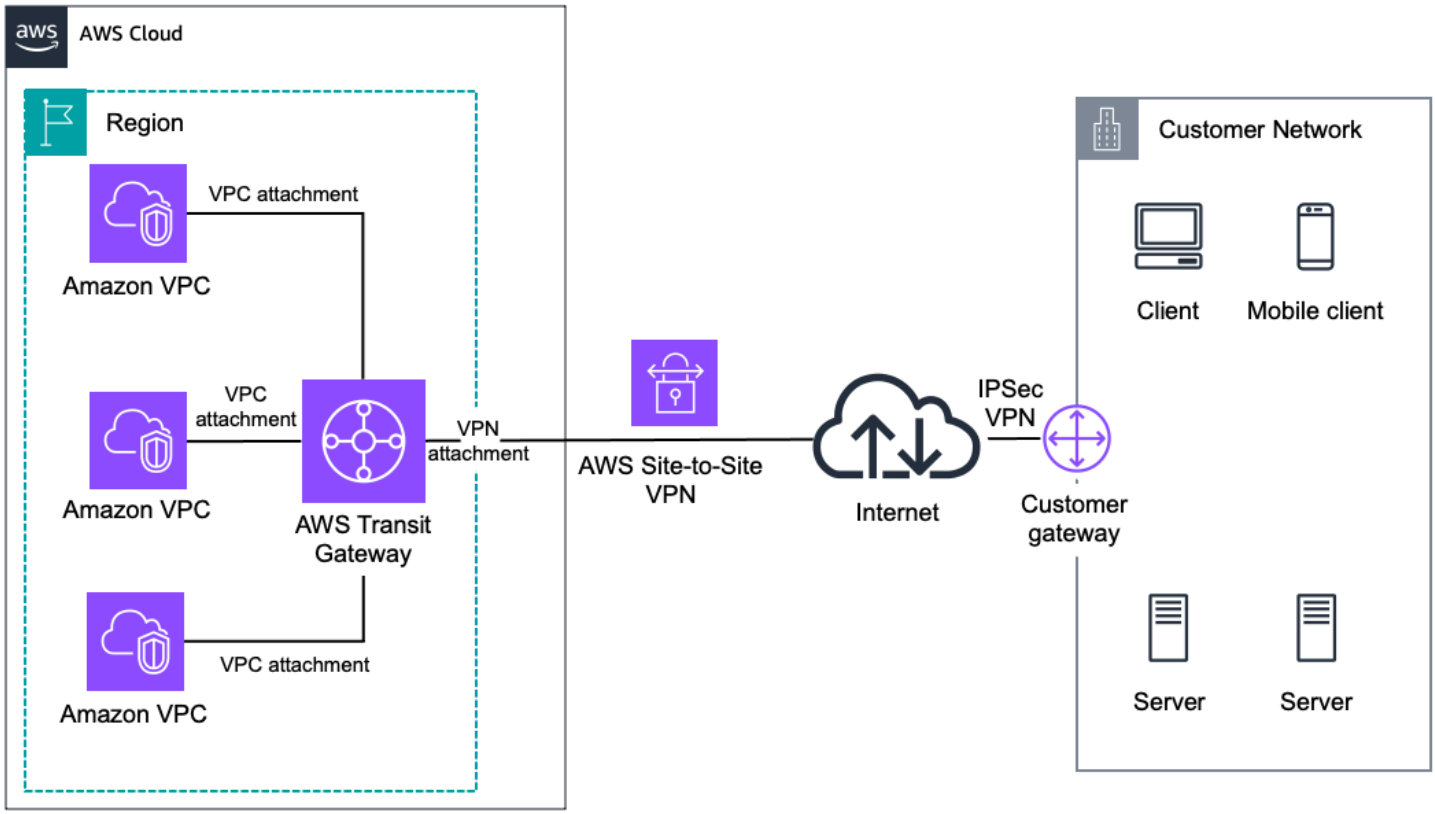
동적 및 정적 라우팅 옵션이 모두 제공되므로 라우팅 구성의 유연성을 높일 수 있습니다. 동적 라우팅은 BGP 피어링을 사용하여 AWS와 이러한 원격 엔드포인트 간에 라우팅 정보를 교환합니다. 동적 라우팅을 사용하면 BGP 광고의 라우팅 우선 순위, 정책 및 가중치 (지표) 를 지정하고 네트워크와 AWS 간의 네트워크 경로에 영향을 미칠 수도 있습니다. BGP를 사용할 때는 IPsec과 BGP 세션 모두 동일한 사용자 게이트웨이 디바이스에서 종료되어야 하므로 IPsec 및 BGP 세션을 모두 종료할 수 있어야 한다는 점에 유의해야 합니다.

추가적인 리소스

- AWS Site-to-Site VPN 사용 설명서
- 고객 게이트웨이 디바이스 요구 사항
- Amazon VPC로 테스트한 고객 게이트웨이 디바이스

AWS Transit Gateway + AWS 사이트 간 VPN

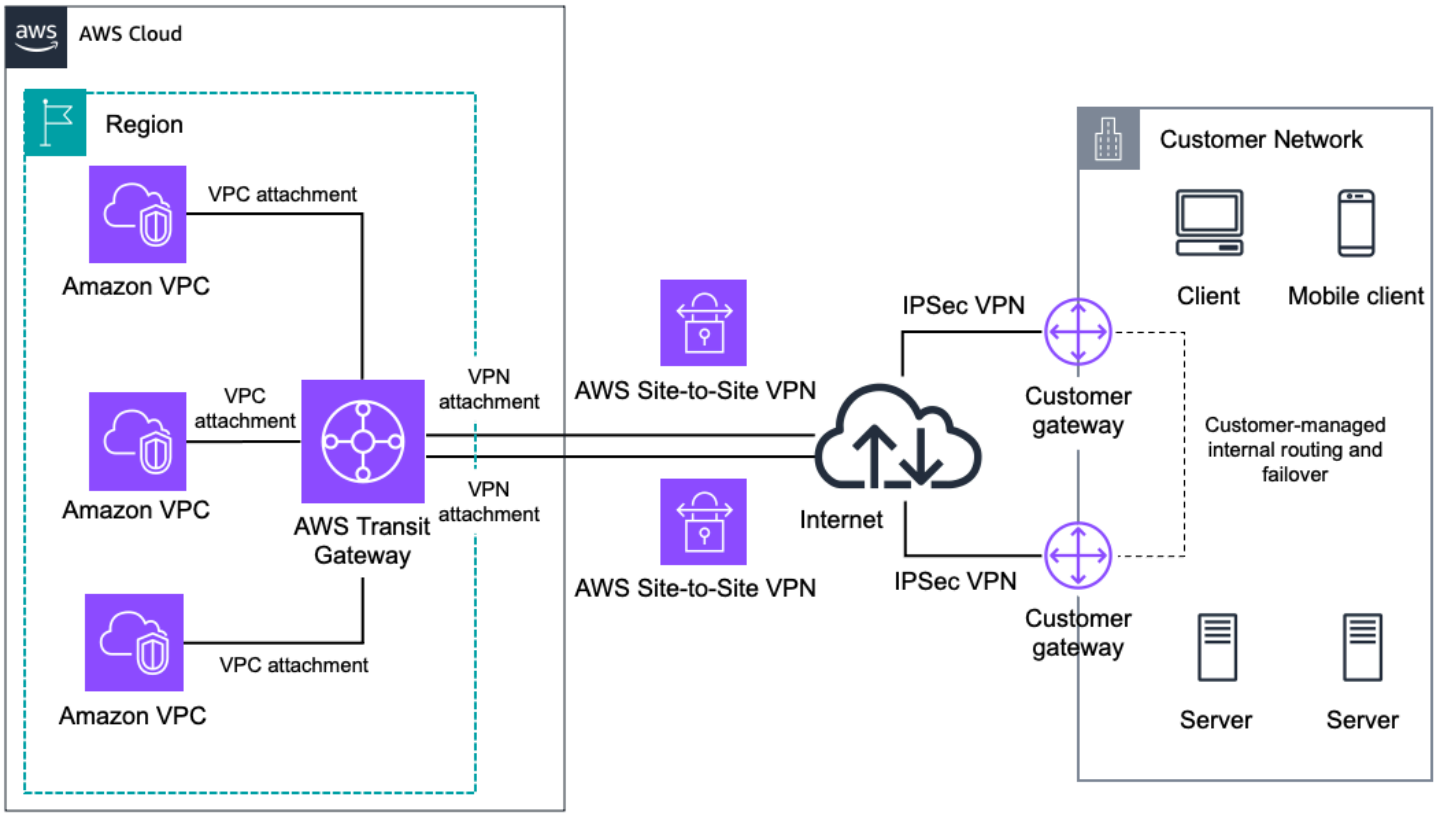
AWS Transit Gateway는 VPC와 고객 네트워크를 상호 연결하는 데 사용되는 AWS 관리형 고가용성 및 확장성 지역 네트워크 전송 허브입니다. Transit Gateway VPN 연결을 사용하는 AWS Transit Gateway + VPN은 다음 그림과 같이 인터넷을 통해 원격 네트워크와 Transit Gateway 사이에 IPsec VPN 연결을 생성하는 옵션을 제공합니다.



AWS Transit Gateway and AWS Site-to-Site VPN

AWS 관리형 VPN 엔드포인트를 활용하여 여러 Amazon VPC에 대한 여러 IPsec VPN 연결을 추가 비용 및 관리 없이 동일한 지역의 여러 VPC에 연결하려는 경우 이 접근 방식을 사용하는 것이 좋습니다.

또한 AWS Transit Gateway는 다중 사용자 게이트웨이 연결을 지원하고 장려하므로 다음 그림과 같이 VPN 연결 측에서 중복성 및 장애 조치를 구현할 수 있습니다.

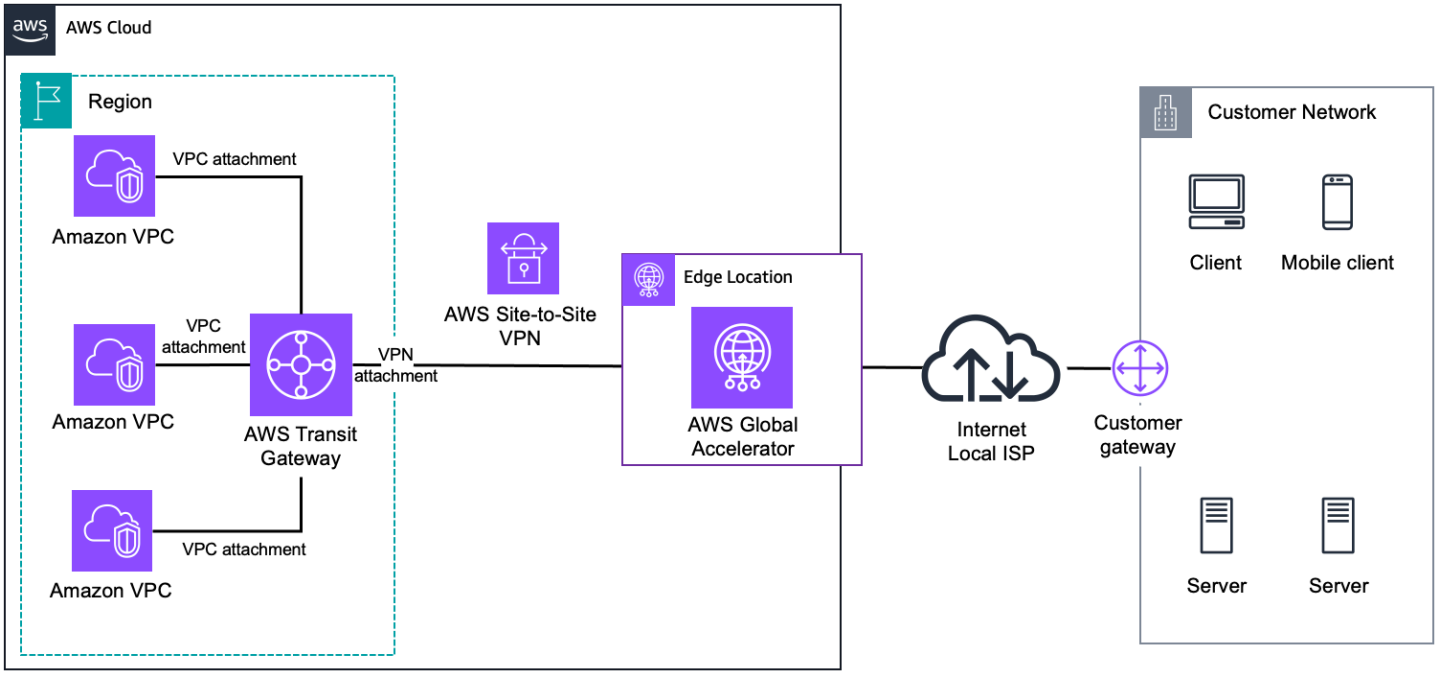


AWS Transit Gateway and Redundant VPN

동적 및 정적 라우팅 옵션이 모두 제공되므로 Transit Gateway VPN IPsec 첨부 파일의 라우팅 구성을 유연하게 수행할 수 있습니다. 동적 라우팅은 BGP 피어링을 사용하여 AWS와 이러한 원격 엔드포인트 간에 라우팅 정보를 교환합니다. 동적 라우팅을 사용하면 BGP 광고의 라우팅 우선 순위, 정책 및 가중치 (지표) 를 지정하고 네트워크와 AWS 간의 네트워크 경로에 영향을 미칠 수도 있습니다. BGP를 사용할 때는 IPsec과 BGP 세션 모두 동일한 사용자 게이트웨이 디바이스에서 종료되어야 하므로 IPsec 및 BGP 세션을 모두 종료할 수 있어야 한다는 점에 유의해야 합니다.

VPN 연결당 1.25Gbps의 처리량과 초당 14만 패킷을 달성할 수 있습니다. Transit Gateway에서 VPN 연결을 종료할 때 균등 비용 다중 경로 (ECMP) 라우팅을 사용하여 여러 VPN 터널을 집계하여 더 높은 VPN 대역폭을 확보할 수 있습니다. ECMP를 사용하려면 VPN 연결에서 동적 라우팅을 구성해야 합니다. 정적 라우팅을 사용하는 ECMP는 지원되지 않습니다.

또한 AWS 사이트 간 VPN 연결에서 가속화를 활성화할 수 있습니다. 가속화된 VPN 연결은 AWS Global Accelerator를 사용하여 네트워크에서 고객 게이트웨이 디바이스와 가장 가까운 AWS 엣지 로케이션으로 트래픽을 라우팅합니다. 이 옵션을 사용하면 트래픽이 퍼블릭 인터넷을 통해 라우팅될 때 발생할 수 있는 네트워크 중단을 방지할 수 있습니다. 가속은 다음 그림과 같이 Transit Gateway에 연결된 VPN 연결에만 지원됩니다.



Accelerated AWS Site-to-Site VPN

마지막으로 IP 주소 지정과 관련하여 사이트 간 VPN 연결은 IPv4 및 IPv6 AWS Transit Gateway 트래픽을 모두 지원합니다. 다음 규칙이 적용됩니다.

- IPv6는 VPN 터널의 내부 IP 주소에만 지원됩니다. AWS 엔드포인트의 외부 IP 주소는 퍼블릭 IPv4 주소입니다. 고객 게이트웨이 IP 주소는 퍼블릭 IPv4 주소여야 합니다.
- Site-to-Site VPN 연결은 IPv4 트래픽과 IPv6 트래픽을 모두 지원할 수 없습니다. 하이브리드 연결에 이중 스택 통신이 필요한 경우 IPv4 및 IPv6 트래픽에 대해 서로 다른 VPN 터널을 생성해야 합니다.

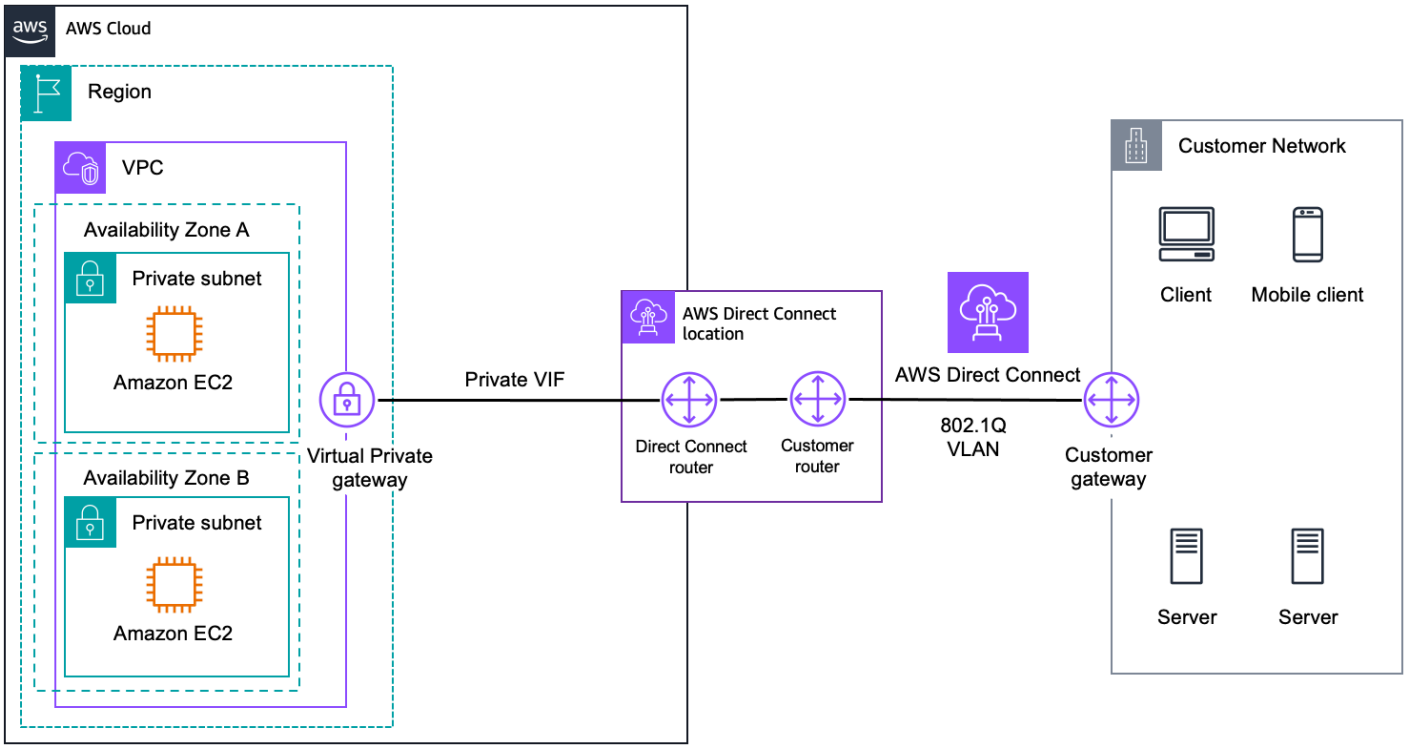
추가적인 리소스

- 트랜짓 게이트웨이 VPN 첨부 파일
- 고객 게이트웨이
- 사이트-투-사이트 VPN 사용
- 사이트-사이트 간 VPN 연결 가속화

AWS Direct Connect

AWS Direct Connect온프레미스 네트워크에서 하나 이상의 VPC로 전용 연결을 쉽게 설정할 수 있습니다. AWS Direct Connect 네트워크 비용을 줄이고, 대역폭 처리량을 늘리고, 인터넷 기반 연결보다 더 일관된 네트워크 경험을 제공할 수 있습니다. 업계 표준 802.1Q VLAN을 사용하여 사설 IP 주소를 사용하여 Amazon VPC에 연결합니다. VLAN은 가상 인터페이스 (VIF) 를 사용하여 구성되며 다음과 같은 세 가지 유형의 VIF를 구성할 수 있습니다.

- 퍼블릭 가상 인터페이스 - AWS 퍼블릭 엔드포인트와 데이터 센터, 사무실 또는 코로케이션 환경 간의 연결을 설정합니다.
- 전송 가상 인터페이스 - 데이터 센터, 사무실 또는 코로케이션 환경 간에 AWS Transit Gateway 사설 연결을 설정합니다. 이 연결 옵션은 섹션에서 ??? 다룹니다.
- 프라이빗 가상 인터페이스 - Amazon VPC 리소스와 데이터 센터, 사무실 또는 코로케이션 환경 간에 프라이빗 연결을 설정합니다. 프라이빗 VIF의 사용은 다음 그림에 나와 있습니다.



AWS Direct Connect

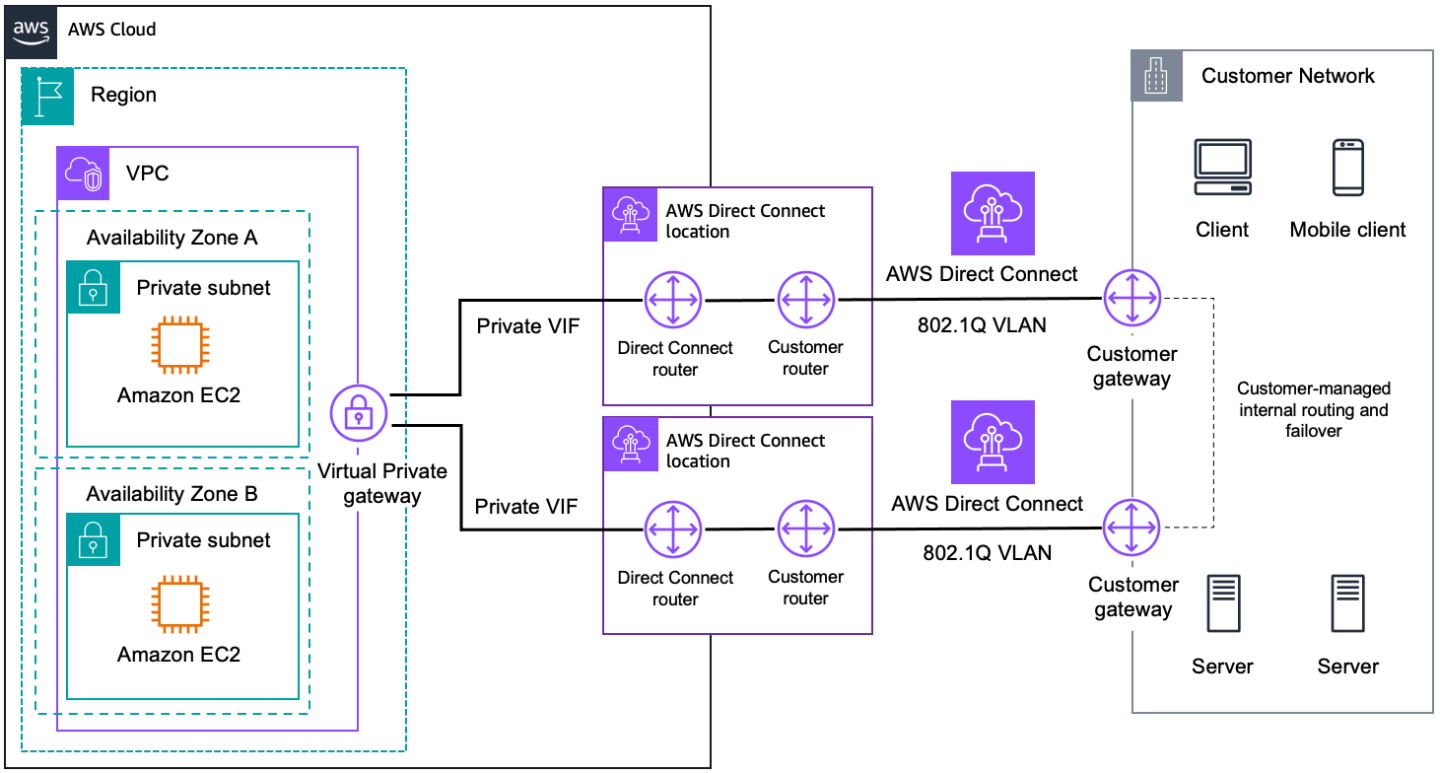
Direct Connect 위치에 있는 AWS 장치에 교차 연결을 AWS Direct Connect 설정하여 를 사용하여 AWS 백본에 대한 연결을 설정할 수 있습니다. 모든 Direct Connect 위치 (중국 제외) 에서 모든 AWS 지역에 액세스할 수 있습니다. 특정 위치에 장비가 없는 경우 WAN 서비스 제공업체 에코시스템 중에서 선택하여 특정 AWS Direct Connect 위치의 AWS Direct Connect 엔드포인트를 원격 네트워크와 통합할 수 있습니다.

에는 두 가지 유형의 연결이 있습니다. AWS Direct Connect

- 전용 연결: 물리적 이더넷 연결이 단일 고객과 연결되는 경우 포트 속도는 1, 10 또는 100Gbps로 주문할 수 있습니다. AWS Direct Connect 파트너 프로그램의 파트너와 협력하여 AWS Direct Connect 연결과 데이터 센터, 사무실 또는 코로케이션 환경 간에 네트워크 회로를 설정하는 데 도움을 받아야 할 수도 있습니다.
- 호스트형 연결: AWS Direct Connect 파트너가 물리적 이더넷 연결을 제공하고 사용자와 공유하는 방식. 포트 속도는 50Mbps에서 10Gbps 사이로 주문할 수 있습니다. 파트너가 설정한 연결과 AWS Direct Connect 연결과 데이터 센터, 사무실 또는 AWS Direct Connect 코로케이션 환경 간의 네트워크 회로에서 파트너와 협력합니다.

전용 연결의 경우 LAG (링크 어그리게이션 그룹) 를 사용하여 단일 엔드포인트에서 여러 연결을 집계할 수도 있습니다. AWS Direct Connect 이들을 단일 관리형 연결로 취급합니다. 최대 4개의 1Gbps 또는 10Gbps 연결과 최대 2개의 100Gbps 연결을 집계할 수 있습니다.

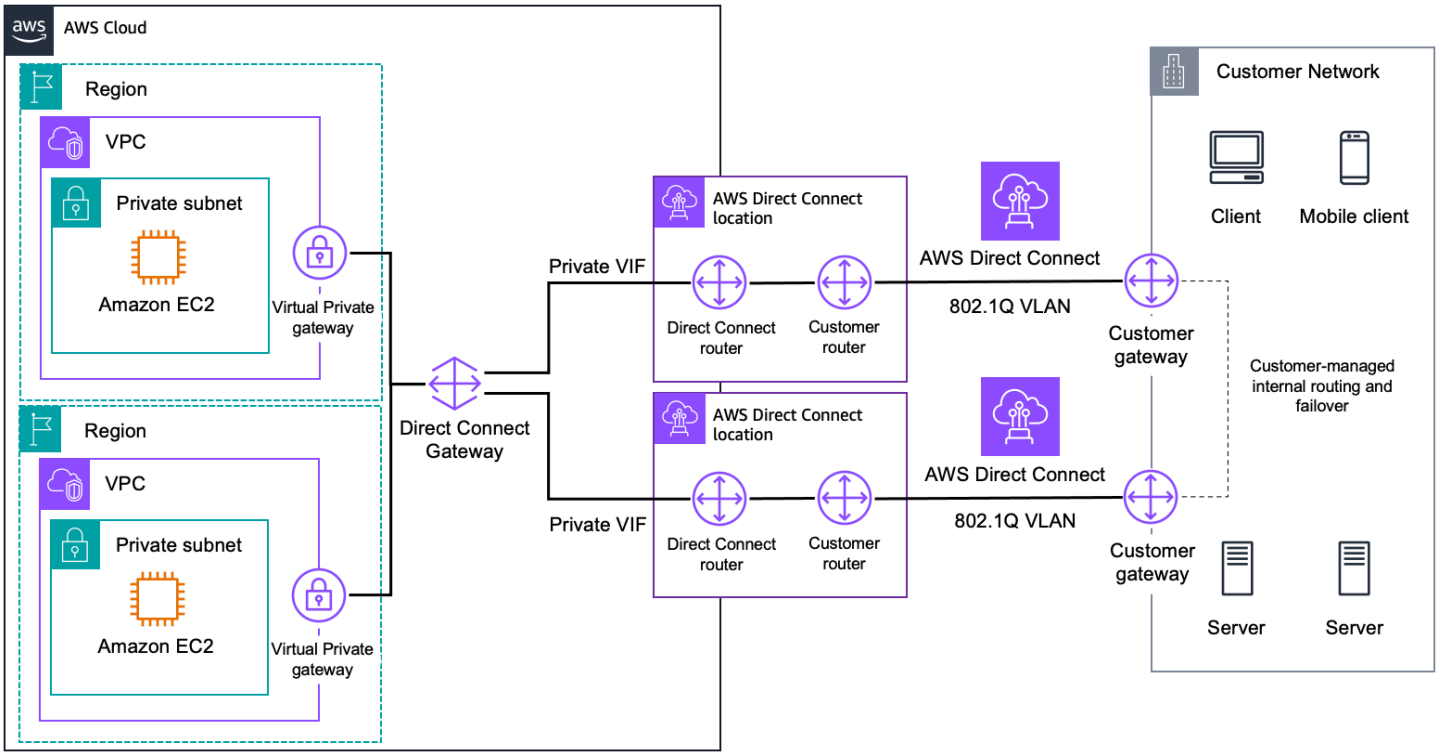
에서 고가용성을 논할 때는 추가 연결을 사용하는 것이 AWS Direct Connect좋습니다. AWS Direct Connect AWS Direct Connect Resiliency Toolkit은 데이터 센터, 사무실 또는 코로케이션 환경 간에 AWS 복원력이 뛰어난 네트워크 연결을 구축하는 데 필요한 지침을 제공합니다. 다음 그림은 서로 다른 두 위치에서 두 AWS Direct Connect 개의 연결이 종료되는 고복원력 연결 옵션의 예를 보여줍니다. AWS Direct Connect



리던던트 AWS Direct Connect

AWS Direct Connect 기본적으로 암호화되지 않습니다. 10Gbps 또는 100Gbps 전용 연결의 경우 MAC 보안 (MACsec) 을 암호화 옵션으로 사용할 수 있습니다. 1Gbps 이하 연결의 경우 연결 위에 VPN 터널을 만들 수 있습니다. 이 옵션은 및 섹션에서 다릅니다. AWS Direct Connect + AWS 사이트 간 VPN AWS Direct ConnectAWS Transit Gateway + AWS 사이트 간 VPN

에서 AWS Direct Connect 중요한 리소스 중 하나는 Direct Connect 게이트웨이입니다. Direct Connect 게이트웨이는 전 세계에서 사용할 수 있는 리소스로서 여러 지역 또는 계정에 걸쳐 여러 Amazon VPC 또는 트랜짓 게이트웨이에 연결할 수 있습니다. AWS 또한 이 리소스를 사용하면 다음 그림과 같이 하나의 프라이빗 VIF 또는 트랜짓 VIF에서 참여 VPC 또는 Transit Gateway에 연결할 수 있으므로 AWS Direct Connect 관리 작업이 줄어듭니다.



AWS Direct Connect Gateway

IP 주소 지정과 관련하여 AWS Direct Connect 가상 인터페이스는 이중 스택 작업을 위해 IPv4 및 IPv6 BGP 세션을 모두 지원합니다.

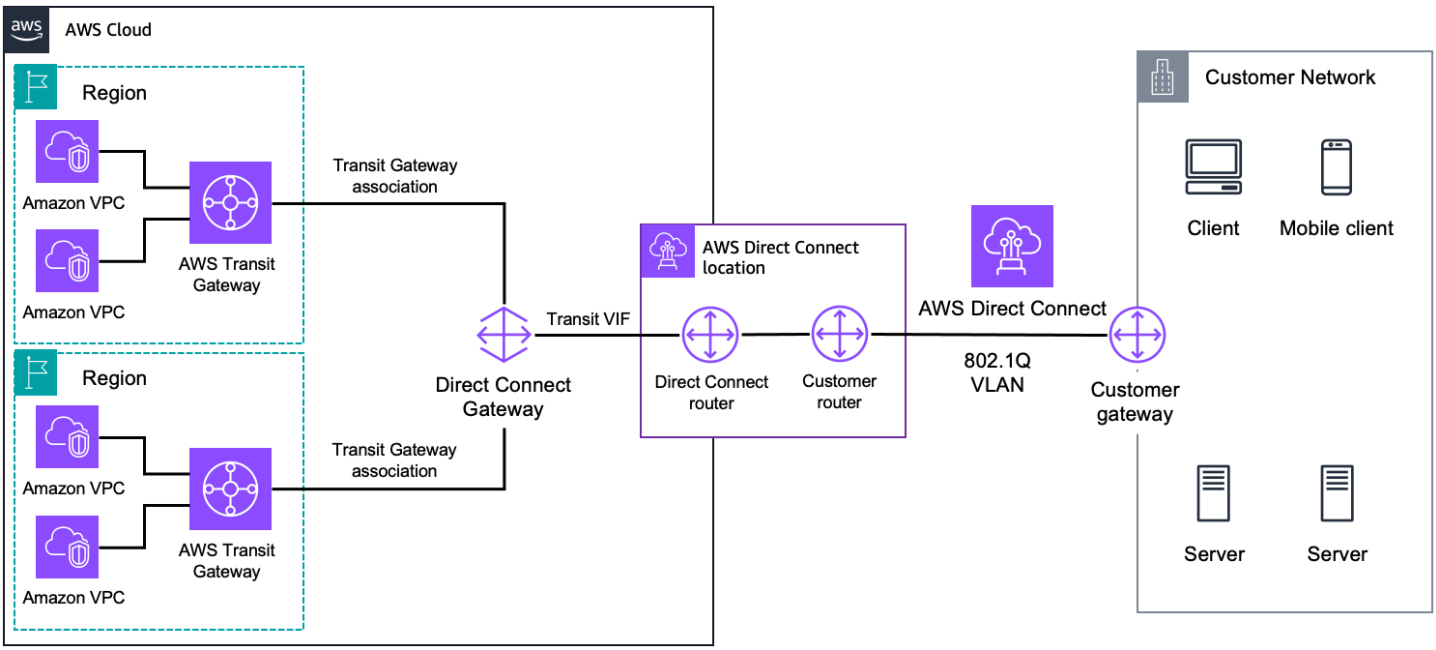
- 프라이빗 및 트랜짓 VIF IPv4 구성은 AWS에서 생성한 IPv4 주소 또는 사용자가 구성한 주소를 사용합니다. 퍼블릭 VIF IPv4 BGP 피어링의 경우 소유하고 있는 고유한 퍼블릭 /31 IPv4 CIDR을 지정하거나 CIDR 블록을 할당하도록 요청을 제출해야 합니다.
- 모든 유형의 VIF IPv6 BGP 피어링에 대해 AWS는 /125 CIDR을 할당하며, 이는 구성할 수 없습니다.

추가적인 리소스

- AWS Direct Connect 사용 설명서
- AWS Direct Connect 가상 인터페이스
- AWS Direct Connect 게이트웨이
- AWS Direct Connect 레질리언스 툴킷
- AWS Direct Connect MAC 보안
- AWS Direct Connect 위치
- AWS Direct Connect 배송 파트너

AWS Direct Connect + AWS Transit Gateway

AWS Direct Connect+ AWS Transit Gateway, Direct Connect 게이트웨이에 대한 트랜짓 VIF 연결을 사용하면 네트워크에서 사설 전용 연결을 통해 여러 지역의 중앙 집중식 라우터를 연결할 수 있습니다. 다음 다이어그램은 두 라우터에 연결하는 것을 보여줍니다.



AWS Direct Connect and AWS Transit Gateway

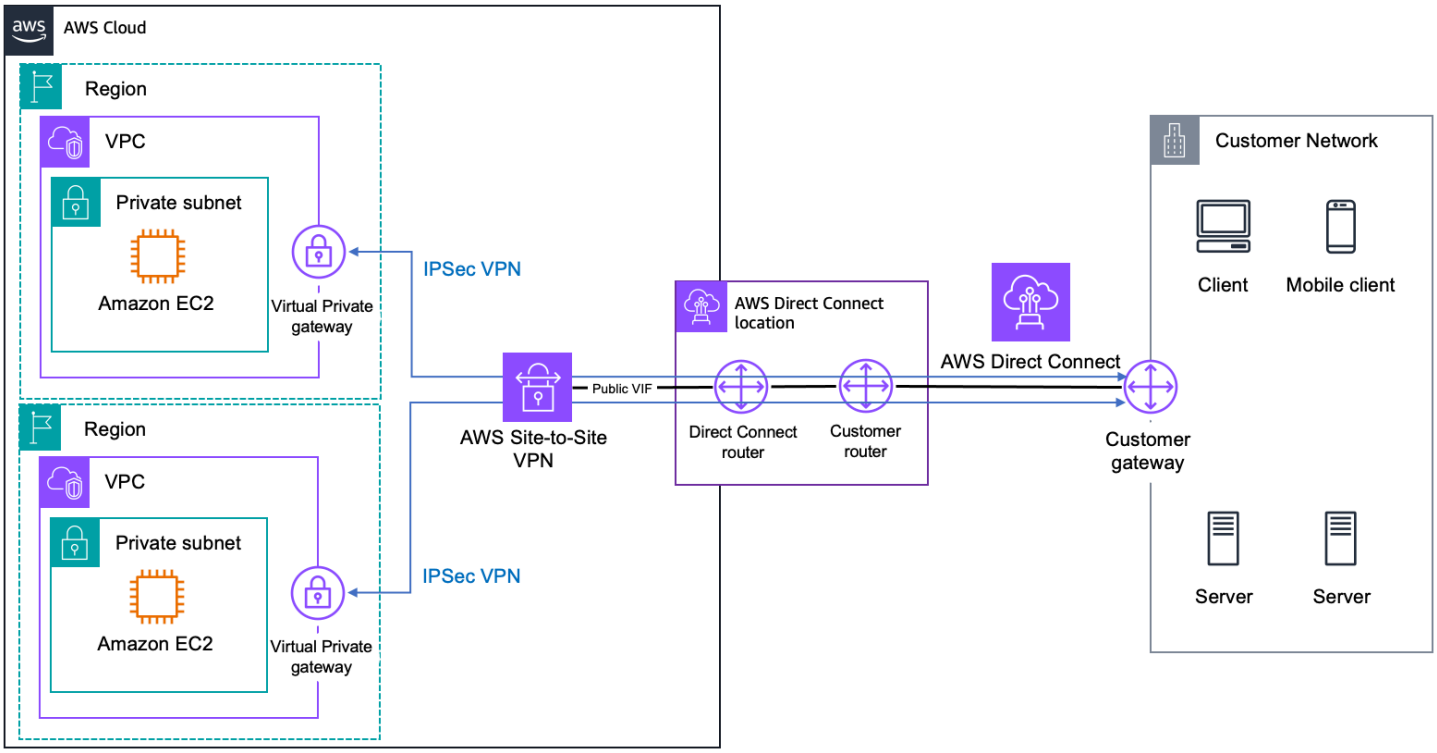
AWS Transit Gateway 각각은 동일한 지역의 VPC를 상호 연결하는 네트워크 전송 허브로서 Amazon VPC 라우팅 구성을 한 곳에서 통합합니다. 이 솔루션은 사설 연결을 통한 Amazon VPC와 네트워크 간 연결 관리를 단순화하여 네트워크 비용을 줄이고, 대역폭 처리량을 늘리고, 인터넷 기반 연결보다 더 일관된 네트워크 경험을 제공할 수 있습니다.

추가적인 리소스

- AWS Direct Connect 사용 설명서
- 링크 어그리게이션 그룹은 AWS Direct Connect
- 블로그 게시물: 1Gbps 미만의 호스팅 연결을 AWS Transit Gateway와 통합

AWS Direct Connect + AWS 사이트 간 VPN

AWS Direct Connect+ AWS Site-to-Site VPN을 사용하면 AWS Direct Connect 연결을 AWS 관리형 VPN 솔루션과 결합할 수 있습니다. AWS Direct Connect 퍼블릭 VIF는 네트워크와 퍼블릭 AWS 리소스 (예: AWS Site-to-Site VPN 엔드포인트) 간에 전용 네트워크 연결을 설정합니다. 서비스에 대한 연결을 설정하고 나면 해당 Amazon VPC 가상 사설 게이트웨이에 IPsec 연결을 생성할 수 있습니다. 다음 그림은 이 옵션을 보여줍니다.



AWS Direct Connect and AWS Site-to-Site VPN

이 솔루션은 end-to-end 보안 IPsec 연결의 이점과 짧은 대기 시간 및 증가된 대역폭을 결합하여 인터넷 기반 VPN 연결보다 더 일관된 네트워크 환경을 제공합니다. AWS Direct Connect BGP 연결 세션은 퍼블릭 VIF의 라우터 간에 AWS Direct Connect 설정됩니다. 가상 프라이빗 게이트웨이와 IPsec VPN 터널의 라우터 사이에 또 다른 BGP 세션 또는 고정 경로가 설정됩니다.

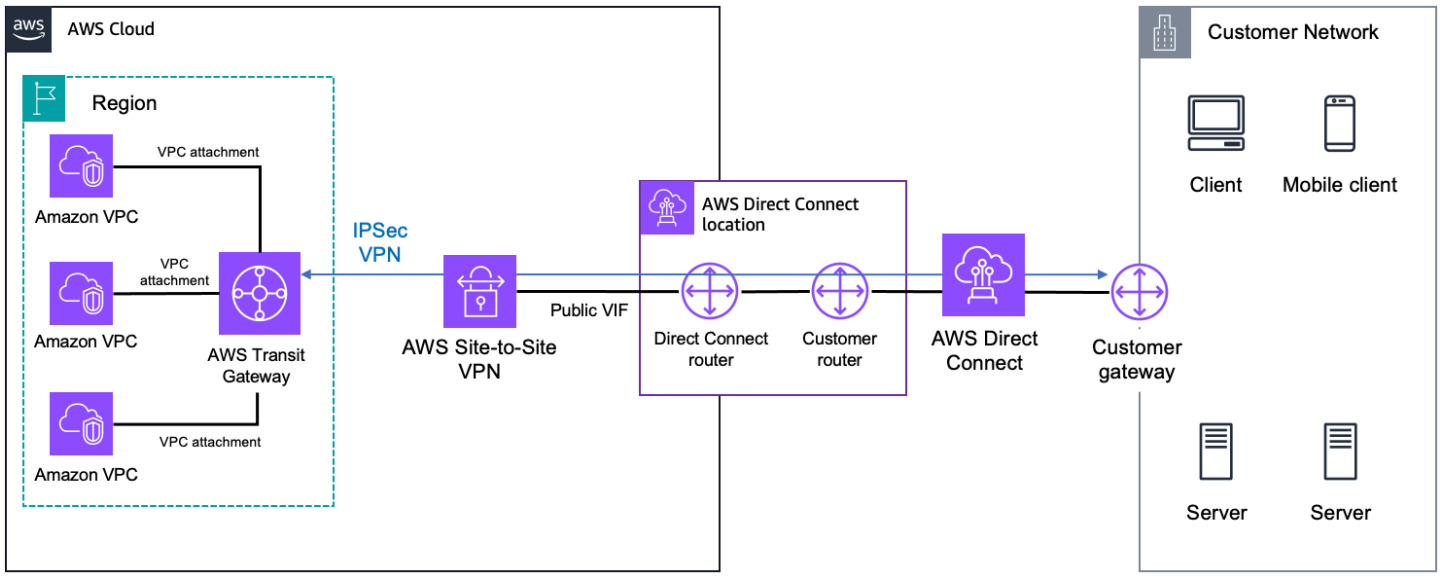
추가적인 리소스

- AWS Direct Connect
- AWS Direct Connect 가상 인터페이스
- AWS Site-to-Site VPN 사용 설명서

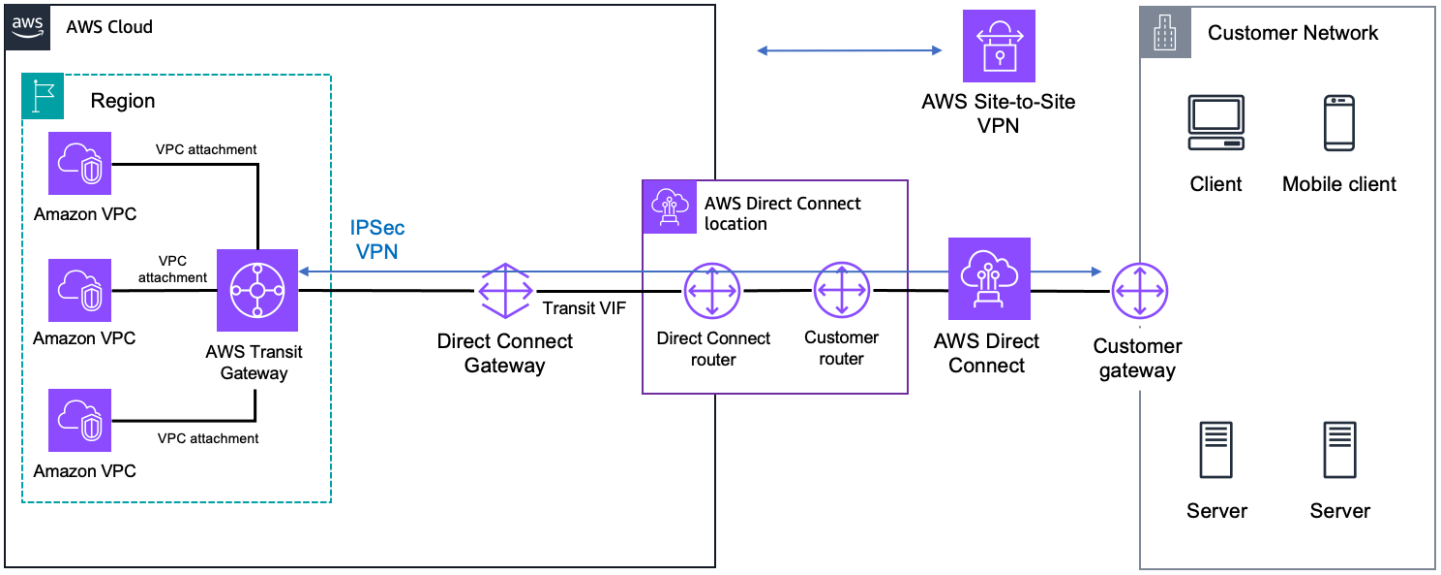
AWS Direct ConnectAWS Transit Gateway + AWS 사이트 간 VPN

AWS Direct Connect+ AWS Transit Gateway+ AWS Site-to-Site VPN을 사용하면 프라이빗 전용 연결을 통해 네트워크와 Amazon VPC용 지역 중앙 집중식 라우터 간에 end-to-end IPsec으로 암호화된 연결을 활성화할 수 있습니다.

먼저 AWS Direct Connect 퍼블릭 VIF를 사용하여 네트워크와 퍼블릭 AWS 리소스 (예: AWS Site-to-Site VPN 엔드포인트) 간에 전용 네트워크 연결을 설정할 수 있습니다. 이 연결이 설정되면 IPsec 연결을 생성할 수 있습니다. AWS Transit Gateway다음 그림은 이 옵션을 보여줍니다.



AWS Direct Connect, AWS Transit Gateway, and AWS Site-to-Site VPN (public VIF)



AWS Direct Connect, AWS Transit Gateway, and AWS Site-to-Site VPN (transit VIF)

인터넷 기반 VPN을 통한 프라이빗 전용 연결의 지연 시간이 짧고 일관된 네트워크 경험의 이점을 활용하여 관리를 간소화하고 동일한 지역의 여러 Amazon VPC에 대한 IPsec VPN 연결 비용을 최소화하려는 경우 이 접근 방식을 사용하는 것이 좋습니다. BGP 세션은 퍼블릭 또는 트랜짓 AWS Direct Connect VIF를 사용하여 라우터 간에 설정됩니다. IPsec VPN 터널의 라우터 간에 AWS Transit Gateway 또 다른 BGP 세션 또는 고정 경로가 설정됩니다.

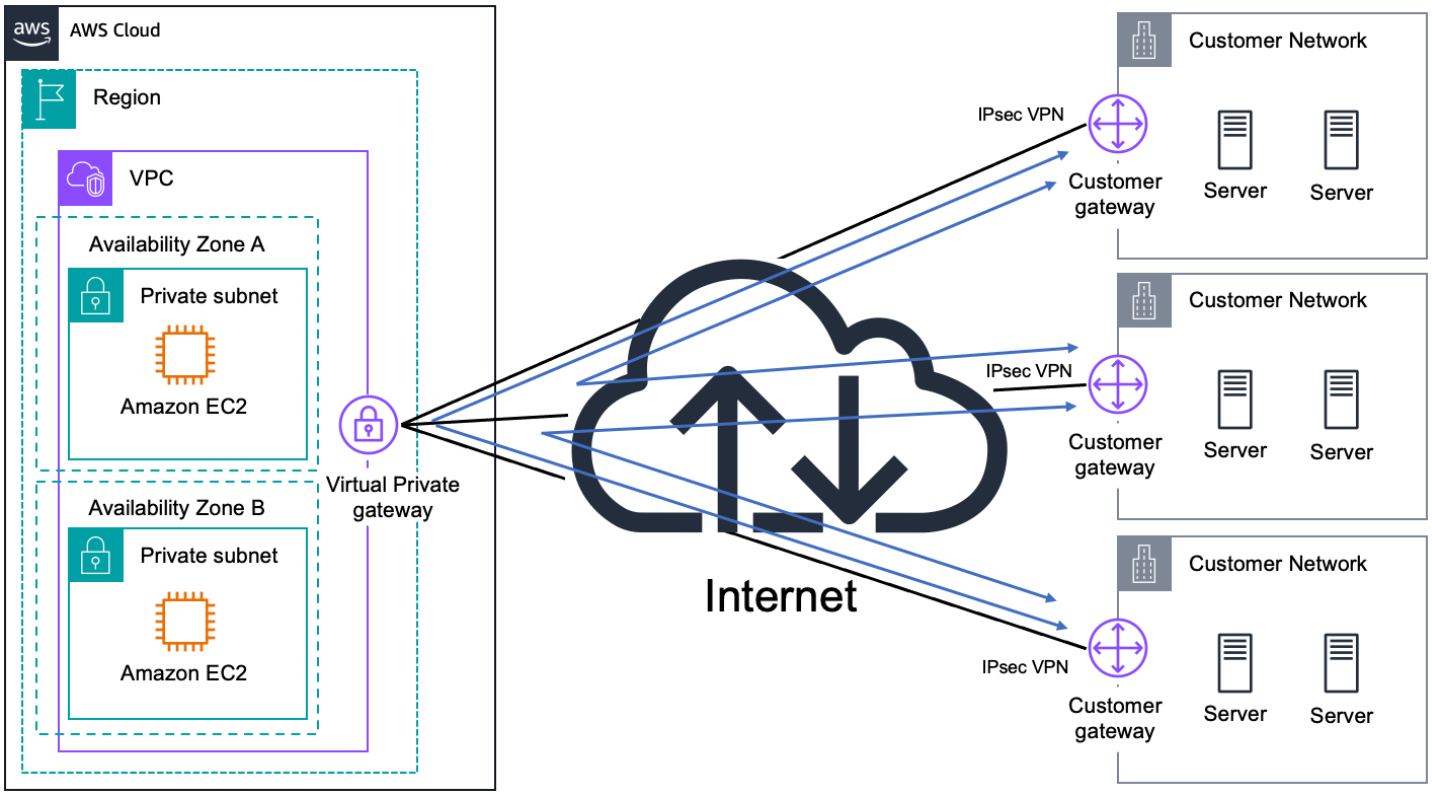
추가적인 리소스

- AWS Direct Connect 가상 인터페이스
- 트랜짓 게이트웨이 VPN 첨부 파일
- 고객 게이트웨이 디바이스 요구 사항
- Amazon VPC로 테스트한 고객 게이트웨이 디바이스
- AWS 사이트-사이트 간 VPN — 프라이빗 IP VPN을 사용하는 AWS Direct Connect

AWS VPN CloudHub

앞서 설명한 AWS 관리형 VPN 옵션을 기반으로 구축하면 를 사용하여 한 사이트에서 다른 사이트로 안전하게 통신할 수 AWS VPN CloudHub 있습니다. 는 VPC와 함께 또는 VPC 없이 사용할 수 있는 간단한 hub-and-spoke 모델에서 AWS VPN CloudHub 작동합니다. 여러 지사와 기존 인터넷 연결이 있고 이러한 원격 사무실 간의 기본 또는 백업 연결을 위한 편리하고 잠재적으로 저렴한 hub-and-spoke 모델을 구현하려는 경우 이 접근 방식을 사용하십시오.

다음 그림은 AWS VPN CloudHub 아키텍처를 보여줍니다. 선은 연결을 통해 라우팅되는 원격 사이트 간의 네트워크 트래픽을 나타냅니다. AWS VPN



AWS VPN CloudHub

AWS VPN CloudHub 는 각각 고유한 BGP 자율 시스템 번호 (ASN) 를 사용하는 여러 고객 게이트웨이가 있는 Amazon VPC 가상 프라이빗 게이트웨이를 사용합니다. 원격 사이트의 IP 범위가 중복되어서는 안 됩니다. 게이트웨이는 VPN 연결을 통해 적절한 경로 (BGP 접두사) 를 알립니다. 이러한 라우팅 알림은 각 BGP 피어에 수신되고 다시 광고되므로 각 사이트가 다른 사이트와 데이터를 주고 받을 수 있습니다.

추가적인 리소스

- VPN을 사용하여 사이트 간 보안 통신 제공 CloudHub
- AWS Site-to-Site VPN 사용 설명서
- 고객 게이트웨이 장치 요구 사항
- Amazon VPC로 테스트한 고객 게이트웨이 디바이스

AWS Transit Gateway + SD-WAN 솔루션

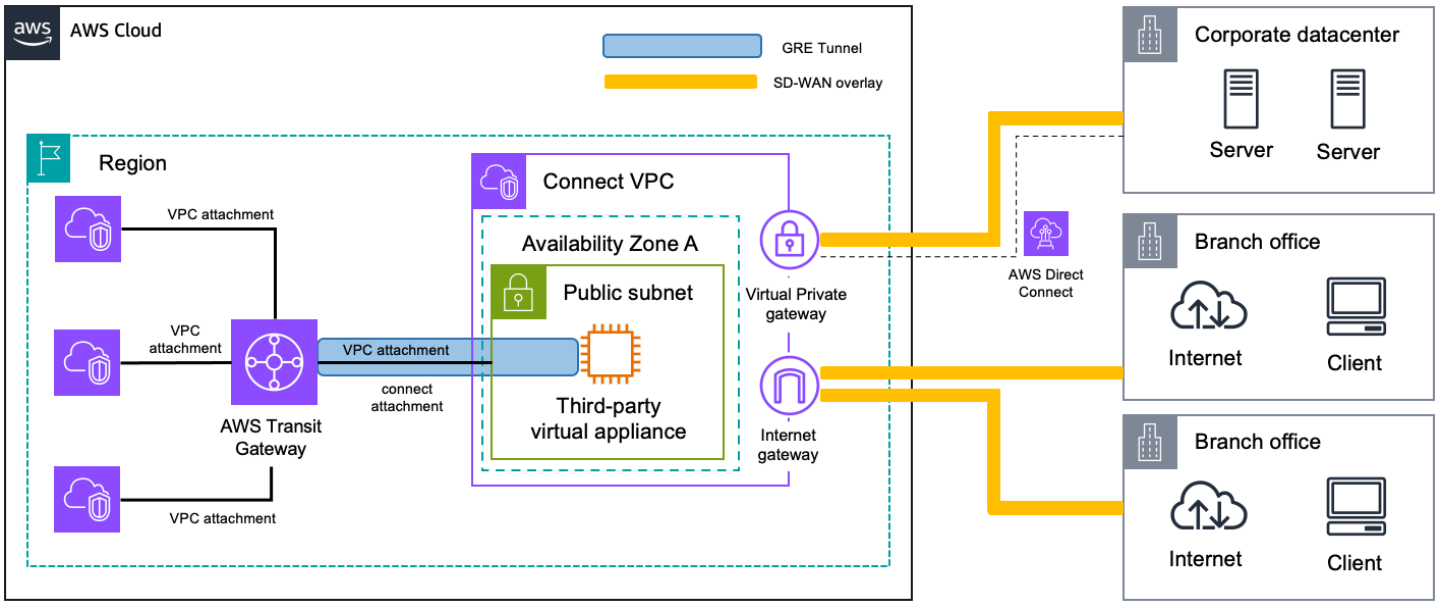
소프트웨어 정의 광역 네트워크 (SD-WAN) 는 다양한 전송 네트워크 (예: 공용 인터넷, MPLS 네트워크 또는 AWS 백본 사용 AWS Direct Connect) 를 통해 데이터 센터, 사무실 또는 코로케이션 환경을 연결하는 데 사용되며, 네트워크 상태, 애플리케이션 유형 또는 QoS (서비스 품질) 요구 사항에 따라 가장 적절하고 효율적인 경로에서 트래픽을 자동으로 동적으로 관리합니다.

여러 데이터 센터, 사무실 또는 코로케이션 환경 간에 또는 AWS와 통신해야 하는 복잡한 네트워크 토폴로지가 있는 경우 이 접근 방식을 사용하십시오. SD-WAN 솔루션은 이러한 유형의 네트워크를 효율적으로 관리하는 데 도움이 될 수 있습니다.

SD-WAN 네트워크를 AWS에 연결하는 경우 VPC와 SD-WAN 네트워크를 상호 연결할 수 있는 가용성과 확장성이 뛰어난 관리형 지역 네트워크 전송 허브를 AWS Transit Gateway 제공합니다. Transit Gateway 연결 첨부 파일은 SD-WAN 인프라 및 어플라이언스를 AWS와 연결하는 기본 방법을 제공합니다. 따라서 IPsec VPN을 설정하지 않고도 SD-WAN을 AWS로 쉽게 확장할 수 있습니다.

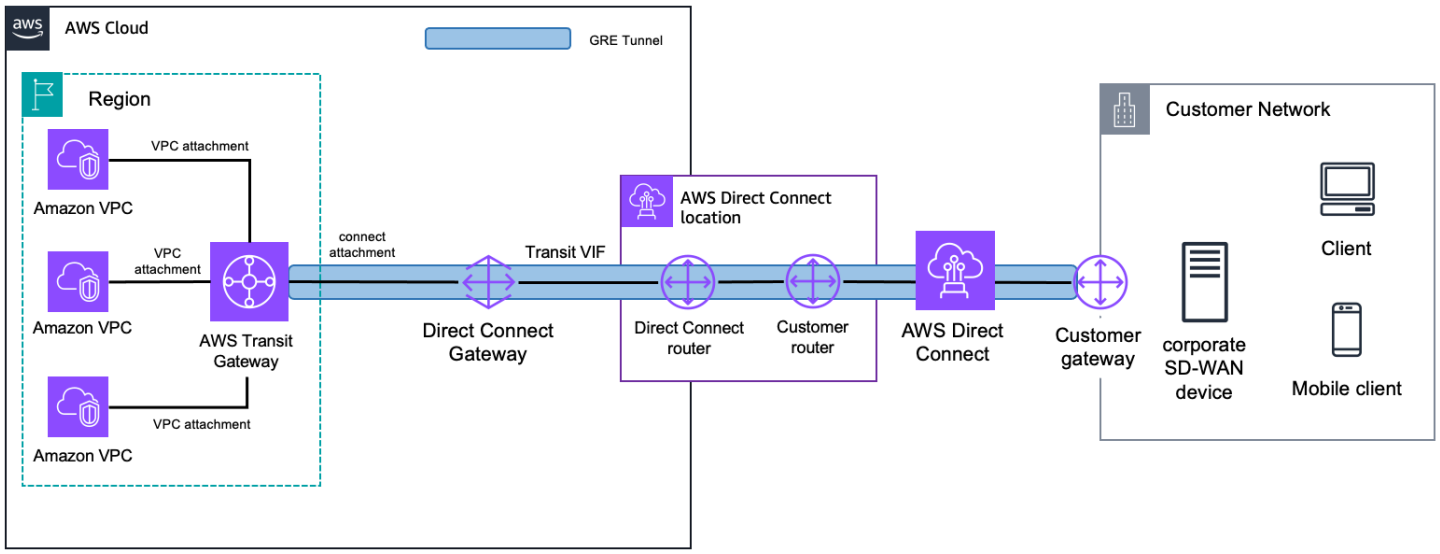
Transit Gateway 연결 연결은 VPN 연결에 비해 더 높은 대역폭 성능을 위해 일반 라우팅 캡슐화 (GRE) 를 지원합니다. 동적 라우팅을 위한 BGP (보더 게이트웨이 프로토콜) 를 지원하므로 고정 경로를 구성할 필요가 없습니다. 이를 통해 네트워크 설계가 단순화되고 관련 운영 비용이 절감됩니다. 또한 Transit Gateway Network Manager와의 통합은 글로벌 네트워크 토폴로지, 첨부 파일 수준 성능 지표 및 원격 측정 데이터를 통해 고급 가시성을 제공합니다.

연결 연결을 사용하여 SD-WAN 네트워크를 Transit Gateway에 통합할 때는 두 가지 일반적인 패턴이 있습니다. 첫 번째는 SD-WAN 네트워크의 가상 어플라이언스를 AWS 내 VPC에 배치하는 것입니다. 그런 다음 다음 그림과 같이 VPC 연결을 가상 어플라이언스와 Transit Gateway 간의 Transit Gateway 연결 연결을 위한 기본 전송으로 사용합니다.



SD-WAN connectivity with AWS Transit Gateway (virtual appliance in AWS)

또는 추가 인프라를 추가하지 않고도 SD-WAN 트래픽을 AWS로 확장하고 분할할 수 있습니다. 다음 그림에 표시된 것처럼 AWS Direct Connect 연결을 기본 전송으로 사용하여 Transit Gateway 연결 첨부 파일을 생성할 수 있습니다.



SD-WAN connectivity with AWS Transit Gateway (Direct Connect as transport)

Transit Gateway 연결 첨부 파일을 사용할 때는 다음과 같은 몇 가지 고려 사항을 숙지해야 합니다.

- 기존 트랜짓 게이트웨이에 연결 첨부 파일을 만들 수 있습니다.

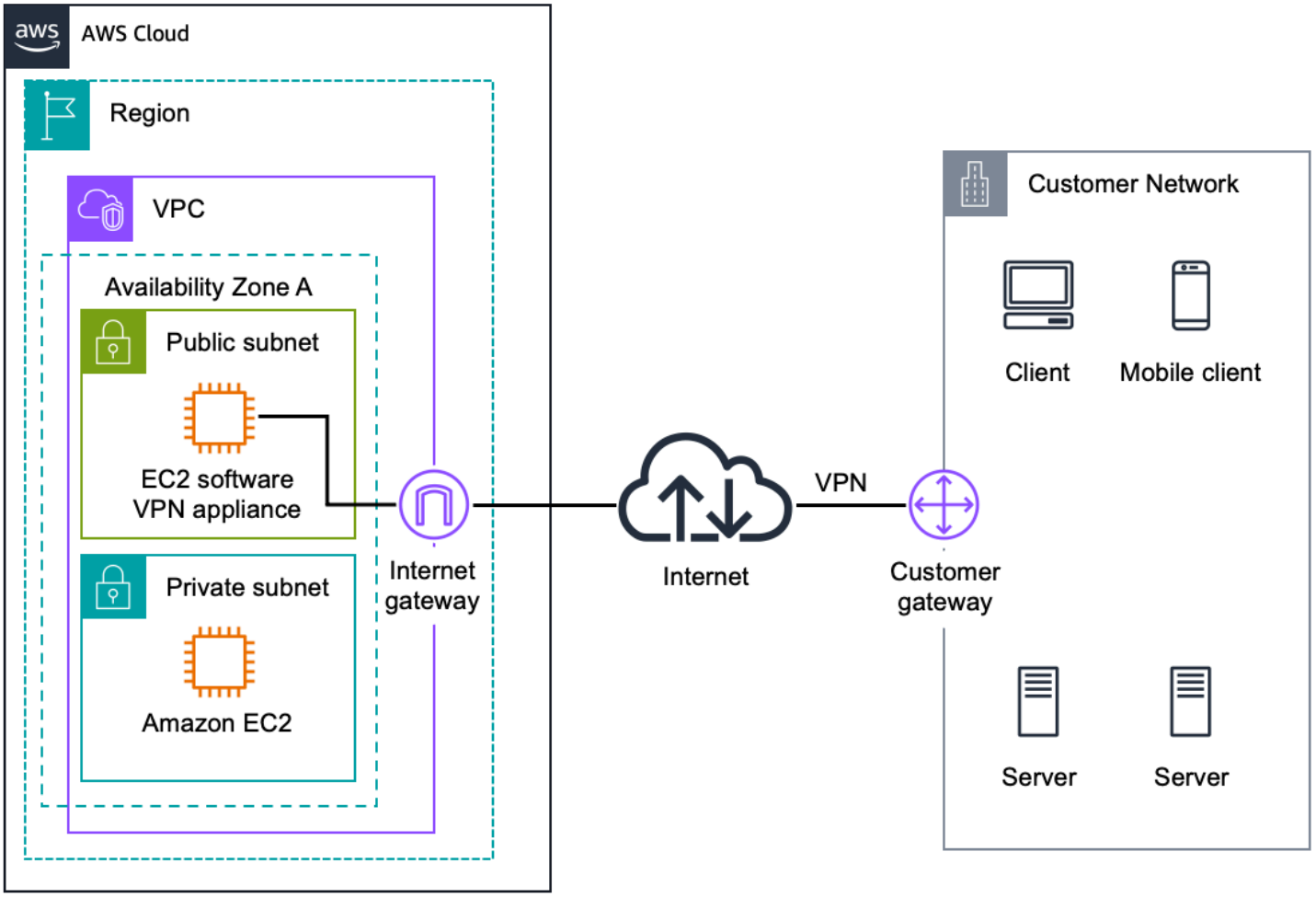
- 연결 첨부 파일을 사용하여 Transit Gateway에서 트래픽을 보내고 받으려면 타사 어플라이언스를 GRE 터널로 구성해야 합니다. 동적 경로 업데이트 및 상태 확인을 위해 어플라이언스를 BGP로 구성해야 합니다.
- Connect 어태치먼트는 고정 경로를 지원하지 않습니다.
- Transit Gateway 연결 어태치먼트는 GRE 터널당 최대 5Gbps의 대역폭을 지원합니다. 동일한 Connect 연결에 대해 여러 Connect 피어 (GRE 터널) 에 동일한 접두사를 광고함으로써 5Gbps를 초과하는 대역폭을 확보할 수 있습니다.
- 각 연결 연결에 대해 최대 4개의 Connect 피어가 지원됩니다.
- Transit Gateway 연결 첨부 파일은 BGP (MBGP 또는 MP-BGP) 용 멀티프로토콜 확장을 통해 IPv6 및 동적 경로 알림을 지원합니다.

추가적인 리소스

- Transit Gateway 피어링 연결
- 요구 사항 및 고려 사항
- 블로그 게시물: AWS Transit Gateway Connect를 사용하여 SD-WAN 연결을 단순화하십시오

소프트웨어 VPN

Amazon VPC는 원격 네트워크와 Amazon VPC 네트워크에서 실행되는 소프트웨어 VPN 어플라이언스 간에 VPN 연결을 생성하여 Amazon VPC 연결의 양쪽을 모두 완벽하게 관리할 수 있는 유연성을 제공합니다. 규정 준수를 위해 또는 현재 Amazon VPC의 VPN 솔루션에서 지원하지 않는 게이트웨이 디바이스를 활용하기 위해 VPN 연결의 양쪽 끝을 모두 관리해야 하는 경우 이 옵션을 사용하는 것이 좋습니다. 다음 그림은 이 옵션을 보여줍니다.



소프트웨어 사이트-투-사이트 VPN

Amazon EC2에서 실행되는 소프트웨어 VPN 어플라이언스를 제작한 여러 파트너 및 오픈 소스 커뮤니티로 구성된 에코시스템 중에서 선택할 수 있습니다. 이러한 선택과 함께 구성, 패치, 업그레이드를 비롯한 소프트웨어 어플라이언스를 관리해야 하는 책임도 따릅니다.

소프트웨어 VPN 어플라이언스가 단일 Amazon EC2 인스턴스에서 실행되기 때문에 이 설계에서는 네트워크 설계에 잠재적인 단일 장애 지점이 발생할 수 있습니다. 자세한 내용은 소프트웨어 VPN 인스턴스용 부록 A: 소프트웨어 VPN 인스턴스를 위한 고수준 HA 아키텍처 아키텍처를 참조하십시오.

추가적인 리소스

- 에서 사용할 수 있는 VPN 어플라이언스 AWS Marketplace
- 테크 브리프 - Cisco ASA를 VPC EC2 인스턴스 (IPsec) 에 연결
- 기술 요약 - 여러 VPC를 EC2 인스턴스 (IPsec) 로 연결
- 테크 브리프 - 여러 VPC를 EC2 인스턴스 (SSL) 로 연결

아마존 VPC와 아마존 VPC 연결 옵션

여러 Amazon VPC를 대규모 가상 네트워크에 통합하려는 경우 이러한 디자인 패턴을 사용하십시오. 이는 보안, 청구, 여러 지역에서의 입지 또는 내부 차지백 요구 사항 등으로 인해 여러 VPC가 필요한 경우 Amazon VPC 간에 AWS 리소스를 더 쉽게 통합하는 데 유용합니다. 또한 이러한 패턴을 Amazon VPC 네트워크 연결 옵션과 결합하여 원격 네트워크 및 여러 VPC에 걸친 기업 네트워크를 구축할 수 있습니다.

VPC 간 VPC 연결은 연결 중인 각 VPC에 대해 중복되지 않는 IP 범위를 사용할 때 가장 잘 이루어집니다. 예를 들어 여러 VPC를 연결하려는 경우 각 VPC가 고유한 CIDR (클래스 없는 도메인 간 라우팅) 범위로 구성되어 있어야 합니다. 따라서 각 VPC에서 사용할 연속적이고 중복되지 않는 단일 CIDR 블록을 할당하는 것이 좋습니다. Amazon VPC 라우팅 및 제약 조건에 대한 추가 정보는 Amazon VPC 자주 묻는 질문을 참조하십시오.

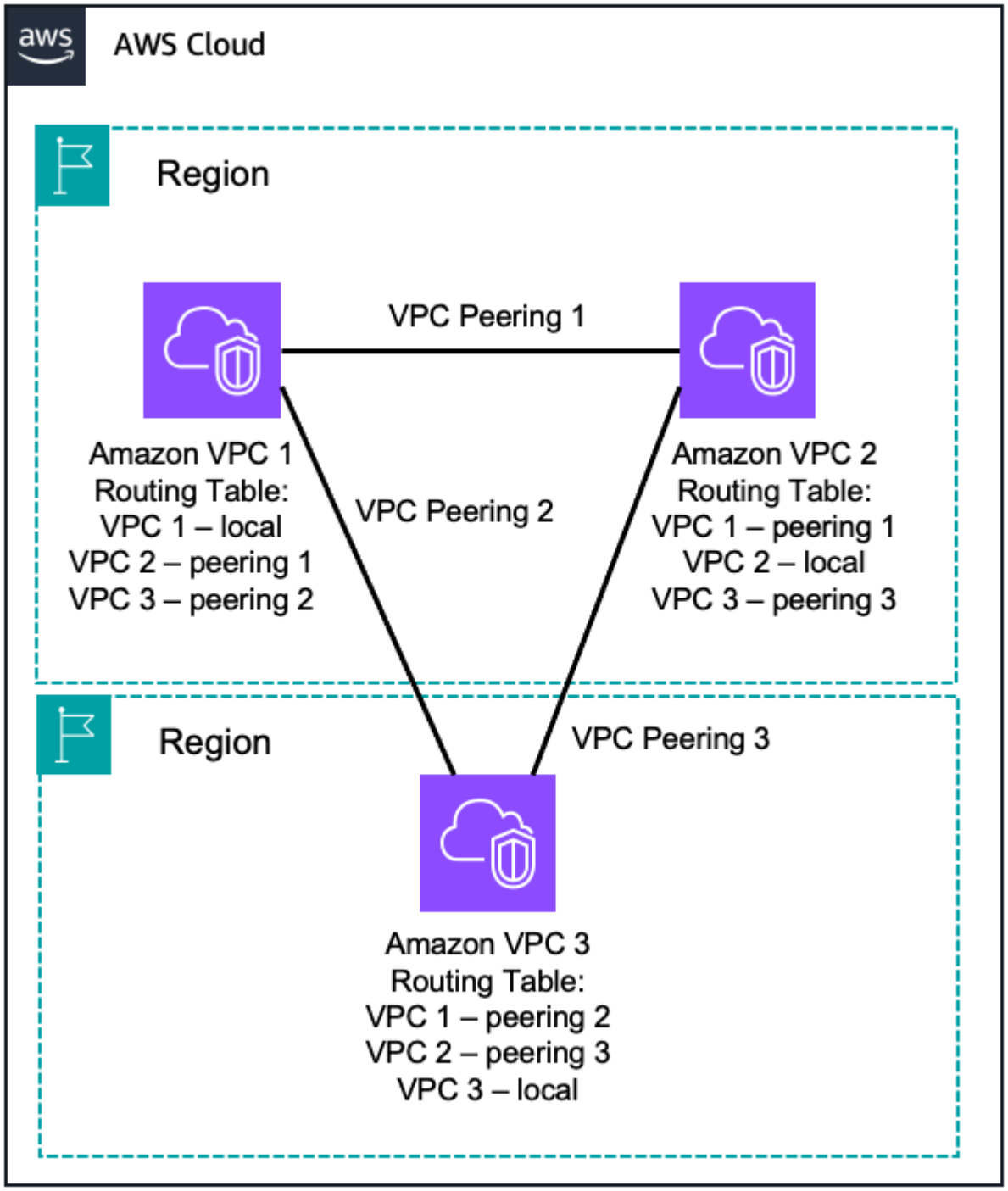
옵션	사용 사례	장점	제한 사항
VPC 피어링	AWS에서 제공하는 두 VPC 간 네트워크 연결.	AWS의 관리형 확장 가능한 네트워킹 인프라 활용	VPC 피어링은 전이적 피어링 관계를 지원하지 않습니다. 대규모 관리가 어려움
AWS Transit Gateway	AWS에서 제공하는 VPC용 지역 라우터 연결	AWS 관리형 고가용성 및 확장성 서비스 최대 5,000개의 첨부 파일을 위한 지역 네트워크 허브	Transit Gateway 피어링은 고정 경로만 지원합니다.
AWS PrivateLink	인터페이스 엔드포인트를 사용하는 두 VPC 간 AWS 제공 네트워크 연결	AWS의 관리형 확장 가능한 네트워킹 인프라 활용	VPC 엔드포인트 서비스는 서비스가 생성된 AWS 지역에서만 사용할 수 있습니다.
소프트웨어 VPN	VPC 간 소프트웨어 어플라이언스 기반 VPN 연결	다양한 VPN 공급업체, 제품 및 프로토콜 지원	모든 VPN 엔드포인트에 HA 솔루션을 구현할 책임은 귀하에게 있습니다 (필요한 경우).

옵션	사용 사례	장점	제한 사항
		전적으로 사용자가 관리합니다.	VPN 인스턴스는 네트워크 병목 현상이 될 수 있습니다.
소프트웨어 VPN-AWS 사이트 간 VPN	VPC 간 소프트웨어 어플라이언스-VPN 연결	AWS 관리형 고가용성 VPC VPN 연결 사용자가 관리하는 다양한 VPN 공급업체 및 제품을 지원합니다. 고정 경로와 동적 BGP 피어링 및 라우팅 정책을 지원합니다.	소프트웨어 어플라이언스 VPN 엔드포인트(필요한 경우)를 위한 HA 솔루션을 구현할 책임은 귀하에게 있습니다. VPN 인스턴스는 네트워크 병목 현상이 될 수 있습니다. IPsec VPN 프로토콜은 AWS 관리형 VPN 전용입니다.

VPC 피어링

[VPC peering] 연결은 두 VPC가 동일한 네트워크에 있는 것처럼 각 VPC의 프라이빗 IP 주소를 사용하여 라우팅을 지원하는 두 VPC 간 네트워크 연결입니다. VPC 피어링 연결은 자체 VPC 간에 생성하거나 다른 AWS 계정의 VPC와 함께 생성할 수 있습니다. VPC 피어링은 리전 간 피어링도 지원합니다.

리전 간 VPC 피어링을 사용하는 트래픽은 항상 글로벌 AWS 백본에 머물며 퍼블릭 인터넷을 통과하지 않으므로 일반적인 익스플로잇 및 DDoS 공격과 같은 위협 벡터가 줄어듭니다.



VPC-to-VPC Peering

AWS는 VPC의 기존 인프라를 사용하여 VPC 피어링 연결을 생성하며 별도의 물리적 하드웨어를 사용하지 않습니다. 따라서 VPC 간에 잠재적인 단일 장애 지점이나 네트워크 대역폭 병목 현상이 발생하지 않습니다. 또한 VPC 라우팅 테이블, 보안 그룹 및 네트워크 액세스 제어 목록을 활용하여 VPC 피어링 연결을 사용할 수 있는 서브넷 또는 인스턴스를 제어할 수 있습니다.

Amazon VPC는 전이적 피어링을 지원하지 않습니다. 즉, 세 번째 VPC를 전송으로 사용하여 직접 피어링되지 않은 두 VPC를 통신할 수 없습니다. 모든 VPC가 VPC 피어링을 사용하여 서로 통신하도록 하려면 각 VPC 간에 1:1 VPC 피어링 연결을 만들어야 합니다. AWS Transit Gateway또는 AWS Cloud WAN을 사용하여 네트워크 전송 허브 역할을 할 수도 있습니다.

IPv4 트래픽과 IPv6 트래픽 모두 VPC 피어링 연결에서 지원됩니다. 하지만 기본 IPv4 CIDR 블록이 겹치는 경우 사용된 보조 IPv4 또는 IPv6 CIDR 블록과 상관없이 두 VPC를 피어링할 수 없습니다. VPC 간에 VPC 피어링을 사용하려는 경우 VPC에 기본 CIDR 블록을 할당할 때 이 점을 고려하십시오.

추가적인 리소스

- 아마존 VPC 피어링
- VPC 피어링이란 무엇입니까?

AWS Transit Gateway

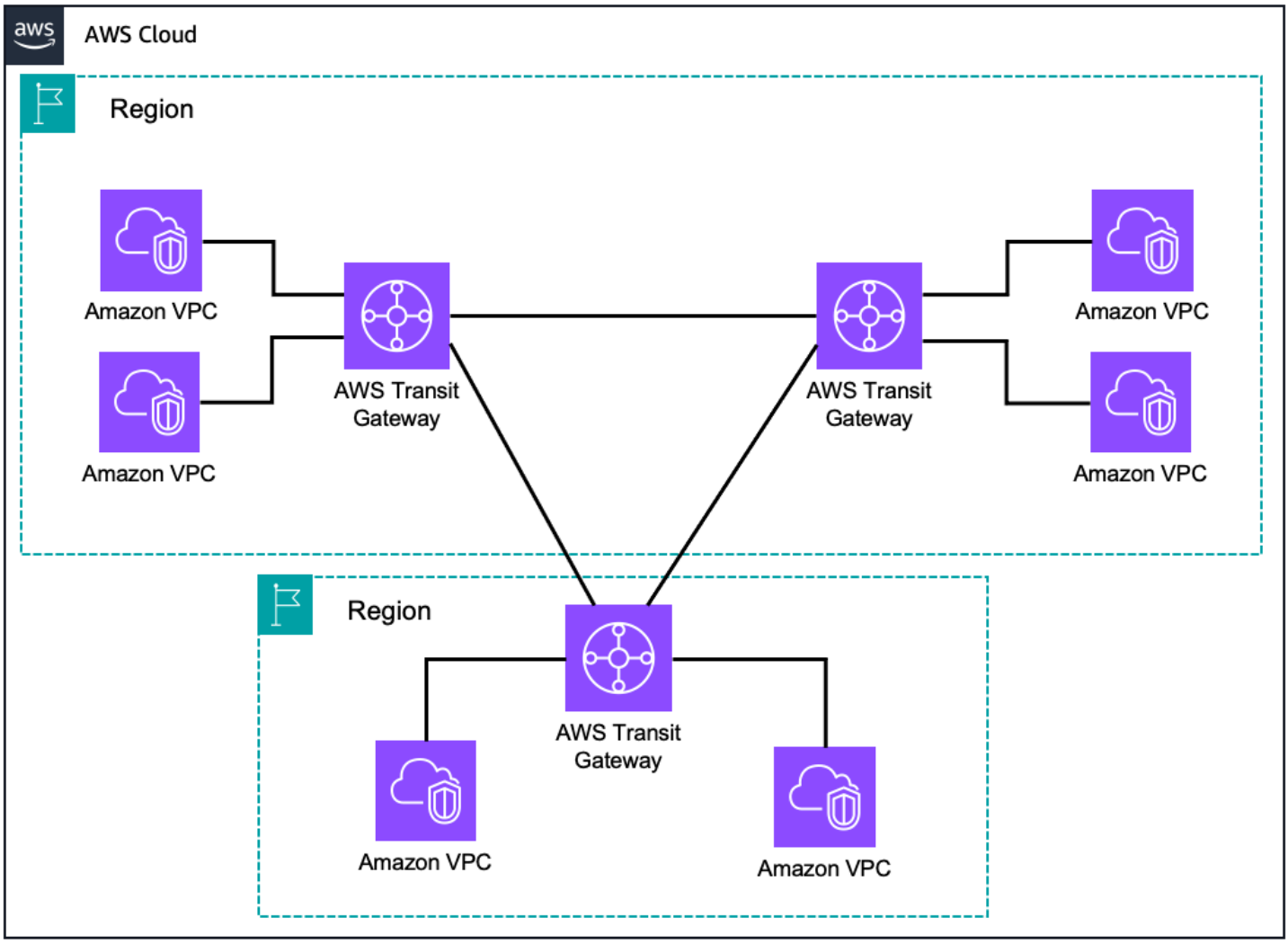
AWS Transit Gateway는 리전용 AWS VPC 라우팅 구성을 아키텍처와 통합하는 가용성과 확장성이 뛰어난 서비스입니다. hub-and-spoke 각 스포크 VPC는 Transit Gateway에 연결하기만 하면 연결된 다른 VPC에 액세스할 수 있습니다. 에서는 IPv4 트래픽과 IPv6 트래픽이 모두 지원됩니다. AWS Transit Gateway

여러 Transit Gateway 라우팅 테이블, 연결 및 전파를 활용하여 동일한 Transit Gateway 내에서 트래픽을 분류할 수 있습니다. 단일 관리 지점에서 서로 다른 라우팅 도메인 (예: 프로덕션 및 비프로덕션 트래픽) 을 관리하여 이러한 라우팅 도메인이 서로 통신할 수 없도록 할 수 있습니다.

또한 Transit Gateway에서 만든 hub-and-spoke 아키텍처를 활용하여 트래픽 검사, 인터페이스 VPC 엔드포인트 액세스 또는 NAT 게이트웨이 또는 NAT 인스턴스를 통한 송신 트래픽과 같은 공유 서비스에 대한 액세스를 중앙 집중화할 수 있습니다. 이러한 중앙 집중화는 여러 VPC에서 이러한 리소스를 관리하는 복잡성을 단순화하고 AWS에서 사용 공간을 확장함에 따라 더 나은 제어를 가능하게 합니다.

트랜짓 게이트웨이는 동일한 AWS 지역 내에서 또는 다른 AWS 지역 간에 서로 피어링될 수 있습니다. AWS Transit Gateway트래픽은 항상 글로벌 AWS 백본에 머물며 퍼블릭 인터넷을 통과하지 않으므로 일반적인 익스플로잇 및 DDoS 공격과 같은 위협 벡터가 줄어듭니다.

VPC가 많은 경우 Transit Gateway는 다음 그림과 같이 VPC 피어링을 통해 보다 간단한 VPC 간 통신 관리를 제공합니다.



AWS Transit Gateway

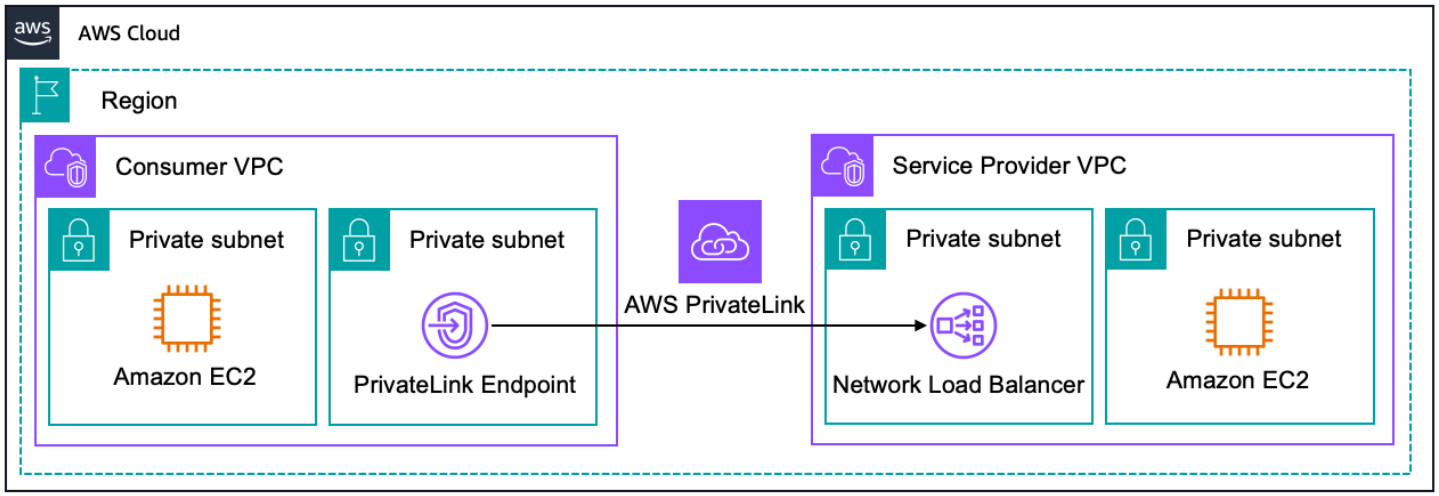
트랜짓 게이트웨이로 들어오고 나가는 IP 트래픽을 중앙에서 파악하기 위해 Transit Gateway 플로우 로그를 Amazon Logs 및 Amazon CloudWatch S3에 게시할 수 있습니다. 흐름 로그 데이터는 네트워크 트래픽 경로 외부에서 수집되므로 네트워크 처리량이나 지연 시간에 영향을 주지 않습니다.

추가적인 리소스

- 아마존 VPC 트랜짓 게이트웨이
- Transit Gateway 피어링 연결
- 트랜짓 게이트웨이 사용
- Transit Gateway 흐름 로그를 사용하여 네트워크 트래픽 로깅

AWS PrivateLink

AWS PrivateLinkVPC의 사설 IP 주소를 통해 일부 AWS 서비스, 다른 AWS 계정에서 호스팅하는 서비스 (엔드포인트 서비스라고 함) 및 지원되는 AWS Marketplace 파트너 서비스에 연결할 수 있습니다. 인터페이스 엔드포인트는 VPC 서브넷의 엘라스틱 네트워크 인터페이스와 IP 주소를 사용하여 VPC 내에서 직접 생성됩니다. 즉, VPC 보안 그룹을 사용하여 엔드포인트에 대한 액세스를 관리할 수 있습니다.



AWS PrivateLink

사설 IP 주소를 사용하여 AWS 네트워크 내에서 다른 VPC가 제공하는 서비스를 안전하게 사용하려는 경우 이 방법을 사용하는 것이 좋습니다. 또는 VPC의 IP 주소가 겹치는 경우 좋은 AWS PrivateLink 해결책입니다.

AWS PrivateLinkIPv6를 완벽하게 지원하지만 이중 스택을 사용하려면 대상 VPC, VPC 서브넷, Network Load Balancer 및 DNS 이름을 모두 활성화하거나 수정해야 합니다. 이러한 사전 요구 사항이 충족되면 엔드포인트의 서비스 구성에서 IPv6를 활성화할 수 있습니다.

액세스 제어: AWS PrivateLink

인터페이스 엔드포인트는 VPC 서브넷의 엘라스틱 네트워크 인터페이스와 IP 주소를 사용하여 VPC 내에서 직접 생성됩니다. 즉, VPC 보안 그룹을 사용하여 엔드포인트에 대한 네트워크 액세스를 관리할 수 있습니다.

인터페이스 엔드포인트 또는 게이트웨이 엔드포인트를 생성할 때 엔드포인트 정책도 연결할 수 있습니다. 엔드포인트 정책은 VPC 엔드포인트를 사용하여 엔드포인트 서비스에 액세스할 수 있는 AWS 보안 주체 (AWS 계정, IAM 사용자 및 역할) 를 제어합니다.

하나의 엔드포인트에 둘 이상의 정책을 연결할 수 없습니다. 그러나 언제든 엔드포인트 정책을 수정할 수 있습니다.

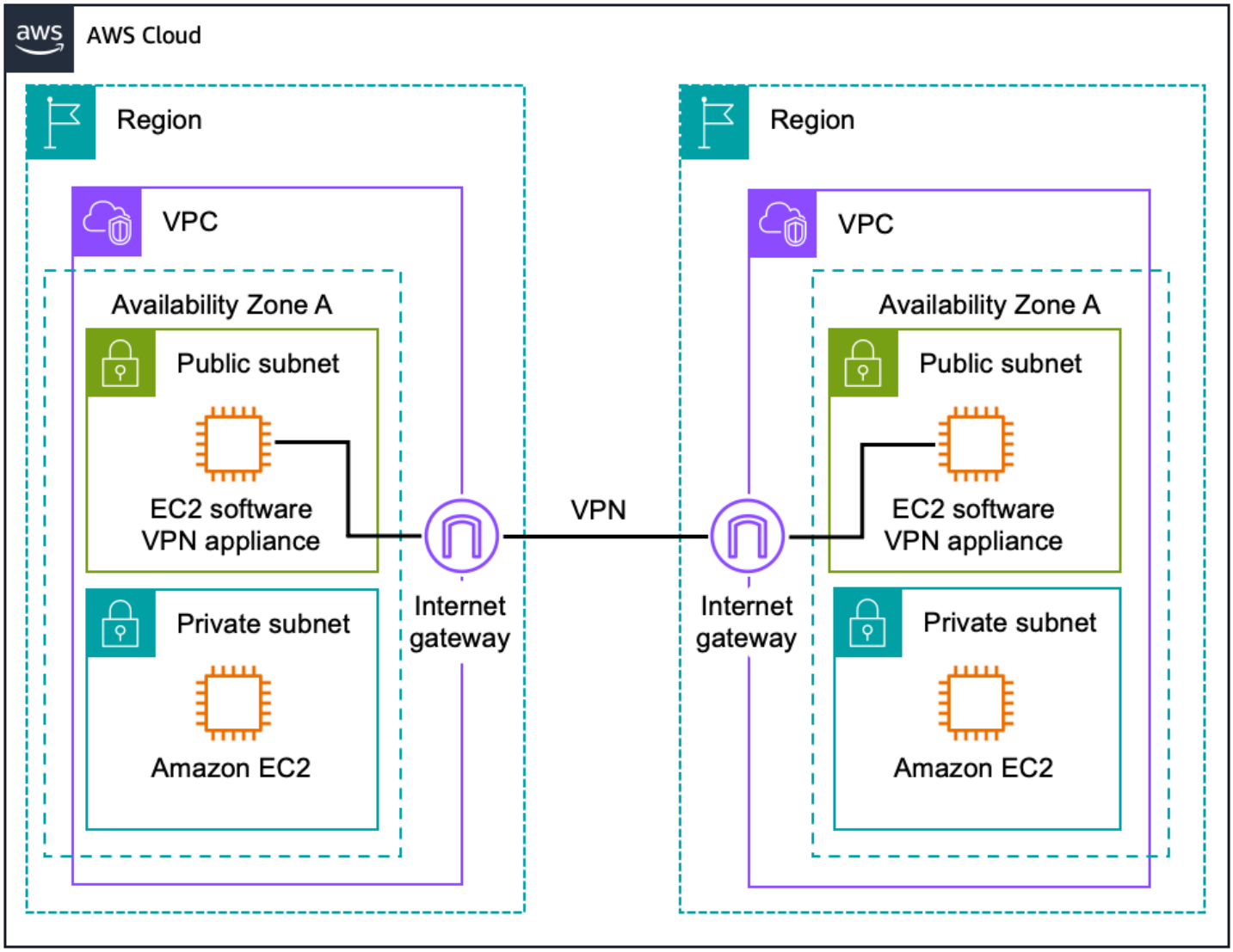
엔드포인트 정책은 IAM 사용자 정책 또는 서비스별 정책 (예: Amazon S3 버킷 정책) 을 재정의하거나 대체하지 않습니다. 인터페이스 엔드포인트를 사용하여 Amazon S3에 연결하는 경우, Amazon S3 버킷 정책을 사용하여 특정 엔드포인트 또는 특정 VPC의 버킷에 대한 액세스를 제어할 수도 있습니다.

추가적인 리소스

- 인터페이스 VPC 엔드포인트 () AWS PrivateLink
- VPC 엔드포인트 서비스 () AWS PrivateLink
- 블로그 게시물: 서비스 및 엔드포인트로 IPv6 채택을 가속화하세요. PrivateLink
- 블로그 게시물: IP 범위가 겹치는 네트워크 연결
- AWS PrivateLink 파트너

소프트웨어 VPN

Amazon VPC는 네트워크 라우팅 유연성을 제공합니다. 여기에는 두 개 이상의 소프트웨어 VPN 어플라이언스 간에 보안 VPN 터널을 생성하여 여러 VPC를 대규모 가상 사설망에 연결하여 각 VPC의 인스턴스가 사설 IP 주소를 사용하여 서로 원활하게 연결할 수 있도록 하는 기능이 포함됩니다. 이 옵션은 선호하는 VPN 소프트웨어 공급자를 사용하여 VPN 연결의 양쪽 끝을 관리하려는 경우에 권장됩니다. 이 옵션은 각 VPC에 연결된 인터넷 게이트웨이를 사용하여 소프트웨어 VPN 어플라이언스 간의 통신을 용이하게 합니다.



Software Site-to-Site VPN VPC-to-VPC Routing

Amazon EC2에서 실행되는 소프트웨어 VPN 어플라이언스를 제작한 여러 파트너 및 오픈 소스 커뮤니티로 구성된 에코시스템 중에서 선택할 수 있습니다. 이러한 선택과 함께 구성, 패치 및 업그레이드를 포함한 소프트웨어 어플라이언스를 관리할 책임도 따릅니다.

단, 소프트웨어 VPN 어플라이언스가 단일 Amazon EC2 인스턴스에서 실행되므로 이 설계에서는 네트워크 설계에 잠재적인 단일 장애 지점이 발생할 수 있습니다. 자세한 내용은 부록 A: 소프트웨어 VPN 인스턴스를 위한 고수준 HA 아키텍처 섹션을 참조하세요.

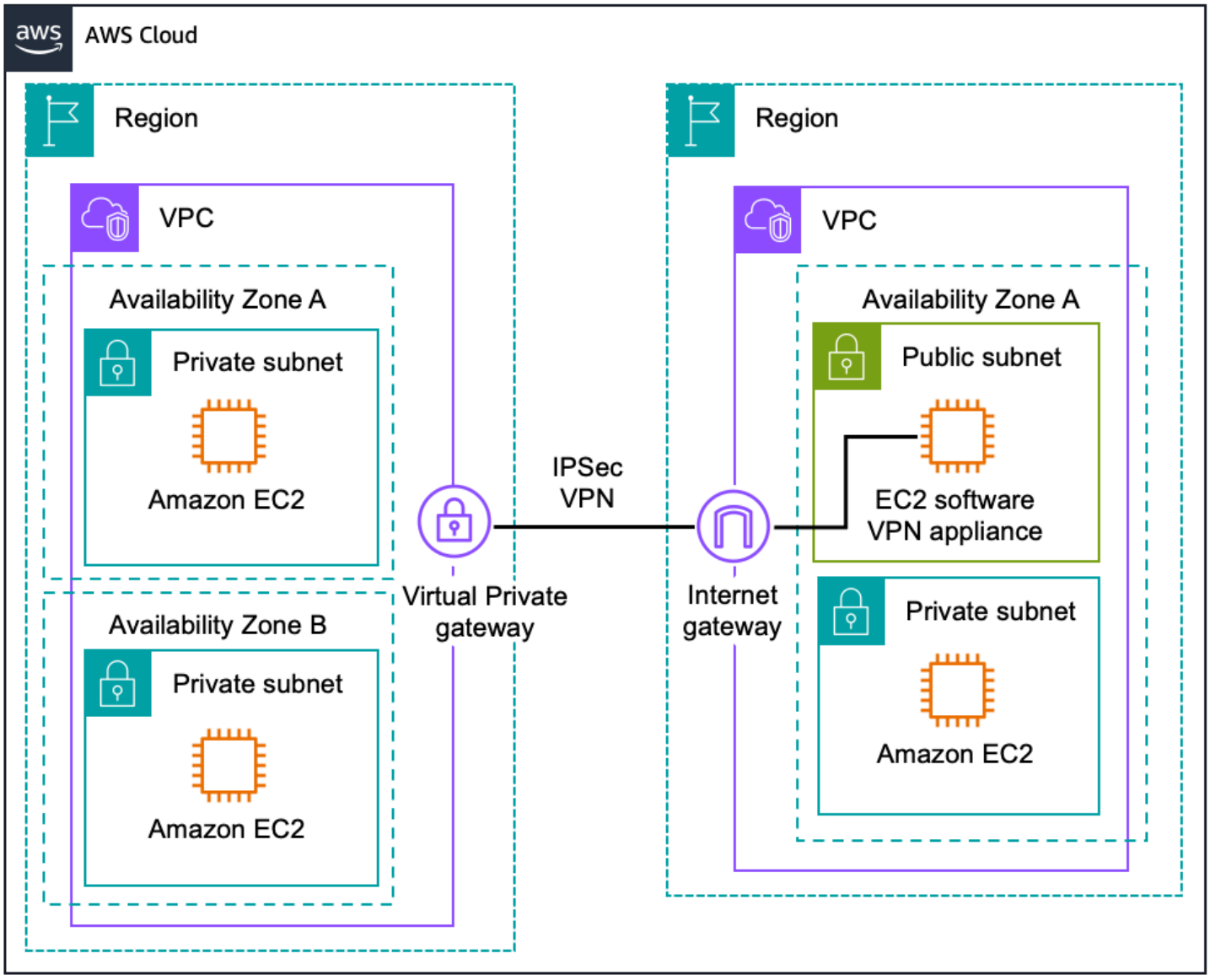
추가적인 리소스

- VPN 어플라이언스는 에서 사용할 수 있습니다. AWS Marketplace
- 기술 요약 - 여러 VPC를 EC2 인스턴스 (IPsec) 에 연결

- 테크 브리프 - 여러 VPC를 EC2 인스턴스 (SSL) 로 연결

소프트웨어 VPN-AWS 사이트 간 VPN

Amazon VPC는 AWS 관리형 VPN과 소프트웨어 VPN 옵션을 결합하여 여러 VPC를 연결할 수 있는 유연성을 제공합니다. 이 설계를 통해 소프트웨어 VPN 어플라이언스와 가상 프라이빗 게이트웨이 사이에 보안 VPN 터널을 생성하여 각 VPC의 인스턴스가 프라이빗 IP 주소를 사용하여 서로 원활하게 연결되도록 할 수 있습니다. 이 옵션은 다음 그림과 같이 한 Amazon VPC에서는 가상 프라이빗 게이트웨이를 사용하고 다른 Amazon VPC에서는 인터넷 게이트웨이와 소프트웨어 VPN 어플라이언스의 조합을 사용합니다.



Software VPN to AWS Site-to-Site VPN VPC-to-VPC Routing

참고로 이 설계에서는 네트워크 설계에 잠재적인 단일 장애 지점이 발생할 수 있습니다. 자세한 내용은 부록 A: 소프트웨어 VPN 인스턴스를 위한 고수준 HA 아키텍처 섹션을 참조하세요.

추가적인 리소스

- 에서 사용할 수 있는 VPN 어플라이언스 AWS Marketplace
- AWS Site-to-Site VPN 사용 설명서
- 고객 게이트웨이 장치 요구 사항

Amazon VPC에 대한 소프트웨어 원격 액세스 연결 옵션

소프트웨어 원격 액세스 VPN을 사용하면 저렴하고 탄력적이며 안전한 서비스를 활용하여 원격 액세스 솔루션을 구현하는 동시에 AWS 호스팅 리소스에 원활하게 연결할 수 있습니다. 이 옵션은 일반적으로 원격 네트워크가 광범위하지 않거나 직원을 위한 원격 액세스 솔루션을 아직 구축 및 배포하지 않은 소규모 회사에서 선호합니다.

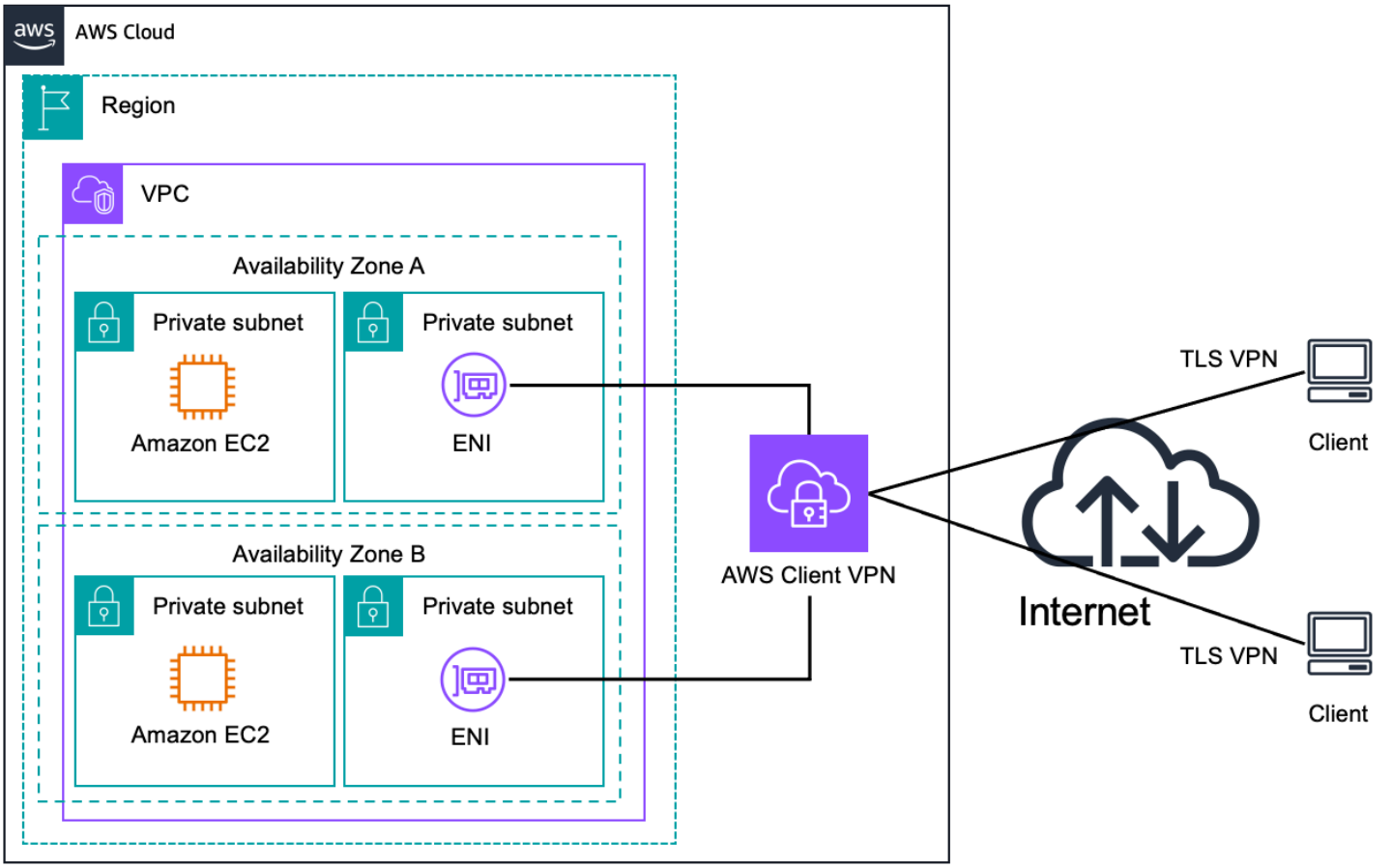
이러한 패턴을 네트워크와 아마존 VPC 연결 옵션 연결 옵션과 결합하여 원격 네트워크와 아마존 VPC와 아마존 VPC 연결 옵션 여러 VPC를 아우르는 네트워크를 만들 수 있습니다.

다음 표에는 이러한 옵션의 장점과 한계가 요약되어 있습니다.

옵션	사용 사례	장점	제한 사항
AWS 클라이언트 VPN	Amazon VPC 및/또는 내부 네트워크에 대한 AWS 관리형 원격 액세스 솔루션	AWS 관리형 고가용성 및 확장성 서비스	OpenVPN 클라이언트 전용
소프트웨어 클라이언트 VPN	Amazon VPC 및/또는 내부 네트워크에 대한 소프트웨어 VPN 어플라이언스 원격 액세스 솔루션	다양한 VPN 공급업체, 제품 및 프로토콜을 지원합니다. 완전 고객 관리형 솔루션	HA 솔루션 구현은 귀사의 책임입니다.

AWS 클라이언트 VPN

AWS Client VPN은 안전한 소프트웨어 원격 액세스를 지원하는 AWS 관리형 고가용성 및 확장성 서비스입니다. 다음 그림과 같이 인터넷을 통해 AWS 리소스 및 온프레미스에 안전하게 액세스할 수 있도록 원격 클라이언트와 Amazon VPC 간에 보안 TLS 연결을 생성하는 옵션을 제공합니다.



AWS Client VPN Remote Access

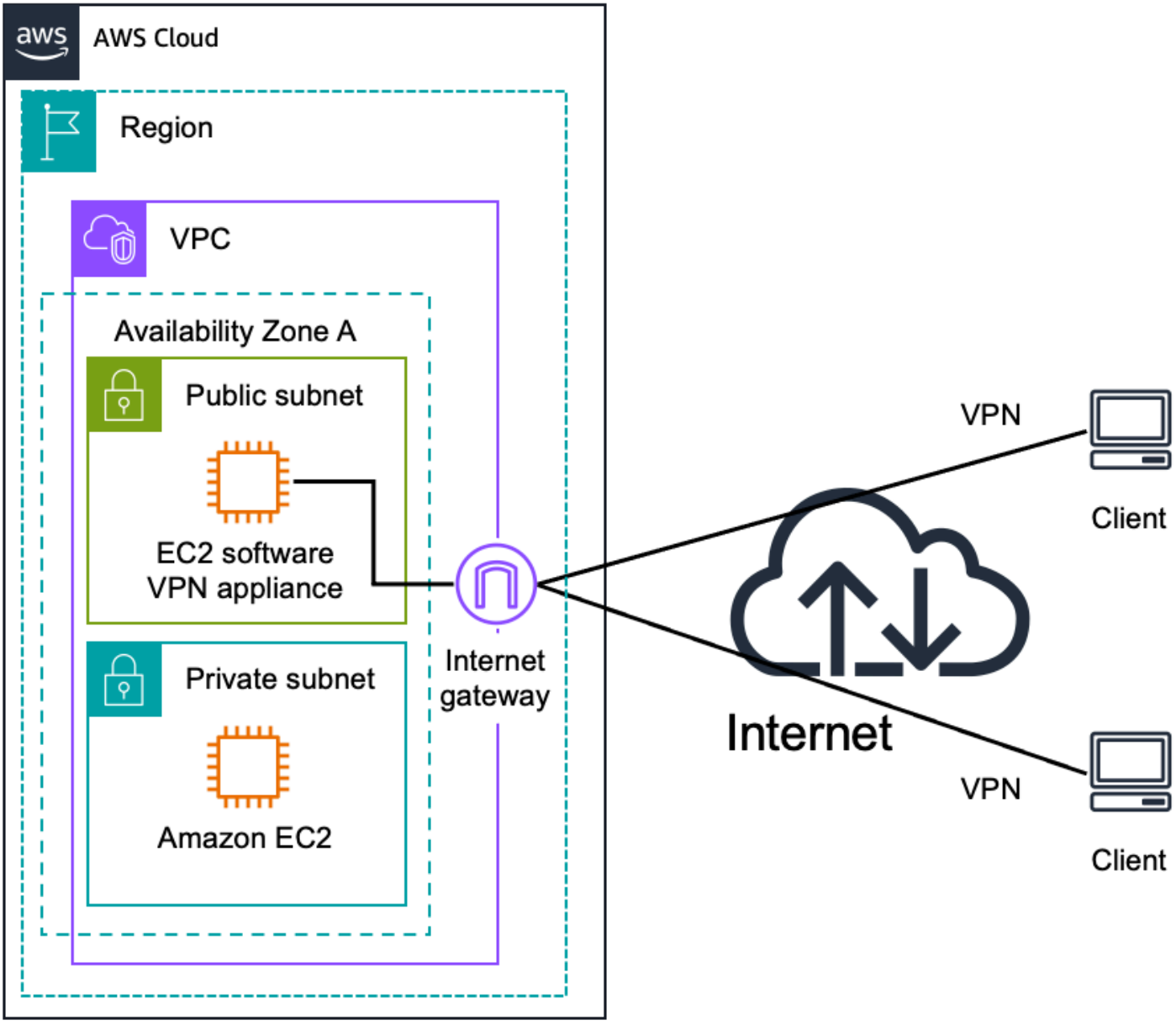
원격 클라이언트는 데스크톱용 AWS Client VPN 또는 Active Directory 또는 상호 인증서 인증을 통한 인증을 사용하는 타사 OpenVPN 클라이언트일 수 있습니다.

추가적인 리소스

- AWS Client VPN 관리자 안내서

소프트웨어 클라이언트 VPN

Amazon EC2에서 실행되는 원격 액세스 솔루션을 만든 여러 파트너 및 오픈 소스 커뮤니티로 구성된 에코시스템 중에서 선택할 수 있습니다. 다음 그림과 같이 이러한 솔루션은 Amazon VPC에 원격으로 액세스하여 인터넷을 통해 AWS 리소스 및 온프레미스에 안전하게 액세스하는 데 사용할 수 있는 보안 프로토콜을 매우 유연하게 제공합니다.



Software Client VPN Remote Access

원격 액세스 솔루션은 복잡성이 다양하고 여러 클라이언트 인증 옵션 (다단계 인증 포함) 을 지원하며 Amazon VPC 또는 Microsoft Active Directory 또는 기타 LDAP/다단계 인증 솔루션과 같은 원격 호스팅된 ID 및 액세스 관리 솔루션 (네트워크-Amazon VPC 옵션 중 하나 활용) 과 통합할 수 있습니다.

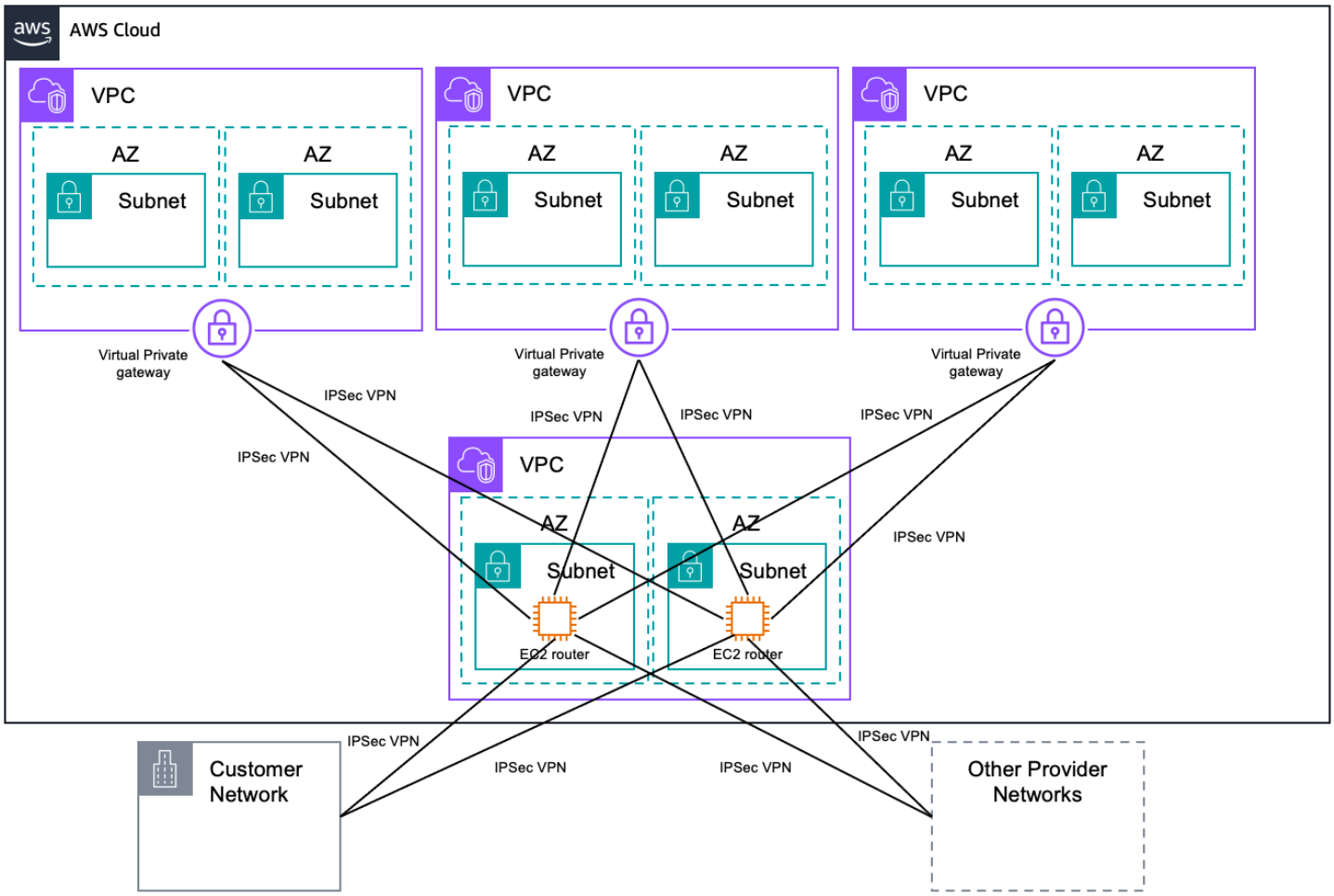
사용자 관리, 구성, 패치 및 업그레이드를 포함한 원격 액세스 소프트웨어 관리는 고객의 책임입니다. 원격 액세스 서버가 단일 Amazon EC2 인스턴스에서 실행되므로 이 설계는 네트워크 설계에 잠재적인 단일 장애 지점을 도입합니다. 자세한 내용은 부록 A: 소프트웨어 VPN 인스턴스를 위한 고수준 HA 아키텍처 섹션을 참조하세요.

추가적인 리소스

- VPN 어플라이언스는 에서 사용할 수 있습니다. AWS Marketplace
- OpenVPN 액세스 서버 퀵 스타트 가이드

트랜짓 VPC

위에서 언급한 소프트웨어 VPN 설계를 기반으로 AWS에서 글로벌 전송 네트워크를 생성할 수 있습니다. 전송 VPC는 글로벌 네트워크 전송 센터를 구축하기 위해 지리적으로 분산된 여러 VPC와 원격 네트워크를 연결하는 일반적인 전략입니다. 전송 VPC는 네트워크 관리를 간소화하고 여러 VPC와 원격 네트워크를 연결하는 데 필요한 연결 수를 최소화합니다. 다음 그림은 이 설계를 보여줍니다.



Transit VPC

이 설계를 통해 VPC와 온프레미스 네트워크 간에 직접 네트워크 라우팅을 제공할 뿐만 아니라 전송 VPC는 중복되는 네트워크 범위 간의 네트워크 주소 변환과 같은 더 복잡한 라우팅 규칙을 구현하거나 네트워크 수준의 패킷 필터링 또는 검사를 추가할 수 있습니다. 전송 VPC 디자인은 프라이빗 네트워킹, 공유 연결 및 계정 간 AWS 사용과 같은 중요한 사용 사례를 지원하는 데 사용할 수 있습니다.

추가적인 리소스

- AWS Transit Gateway

- SD-WAN 및 라우팅 인용 시스코 카탈리스트 8000V AWS Marketplace

AWS 클라우드 WAN

AWS Cloud WAN은 인텐트 기반 관리형 광역 네트워크 (WAN) 로서, 데이터 센터, 지사 및 AWS 네트워크를 통합하도록 사용자가 정의한 정책에 따라 설명됩니다. 여러 지역에 걸쳐 여러 Transit Gateway를 상호 연결하여 자체 글로벌 네트워크를 만들 수 있지만, 클라우드 WAN은 핵심 네트워크 정책을 기반으로 글로벌 네트워크를 구축하고 운영하기 위해 특별히 설계된 자동화, 세분화 및 구성 관리 기능을 내장하고 있습니다. Cloud WAN에는 자동화된 VPC 연결, 통합 성능 모니터링, 중앙 집중식 구성과 같은 기능이 추가되었습니다.

핵심 네트워크 정책은 세그먼트, AWS 리전 라우팅, 첨부 파일이 세그먼트에 매핑되는 방식을 정의하는 선언적 언어로 작성되었습니다. 핵심 네트워크 정책을 사용하면 액세스 제어 및 트래픽 라우팅에 대한 의도를 설명할 수 있으며, AWS Cloud WAN은 네트워크 구성 세부 정보를 처리합니다.

클라우드 WAN은 AWS 네트워크 관리자 내에서 관리되므로 AWS 계정, 지역 및 온프레미스 위치에서 클라우드 WAN 코어 네트워크와 Transit Gateway 네트워크를 중앙에서 관리하고 시각화할 수 있습니다. Network Manager는 글로벌 네트워크의 모든 측면을 보고 모니터링하는 데 도움이 되는 몇 가지 대시보드 시각화를 제공합니다. 일부 대시보드에는 다음이 포함됩니다.

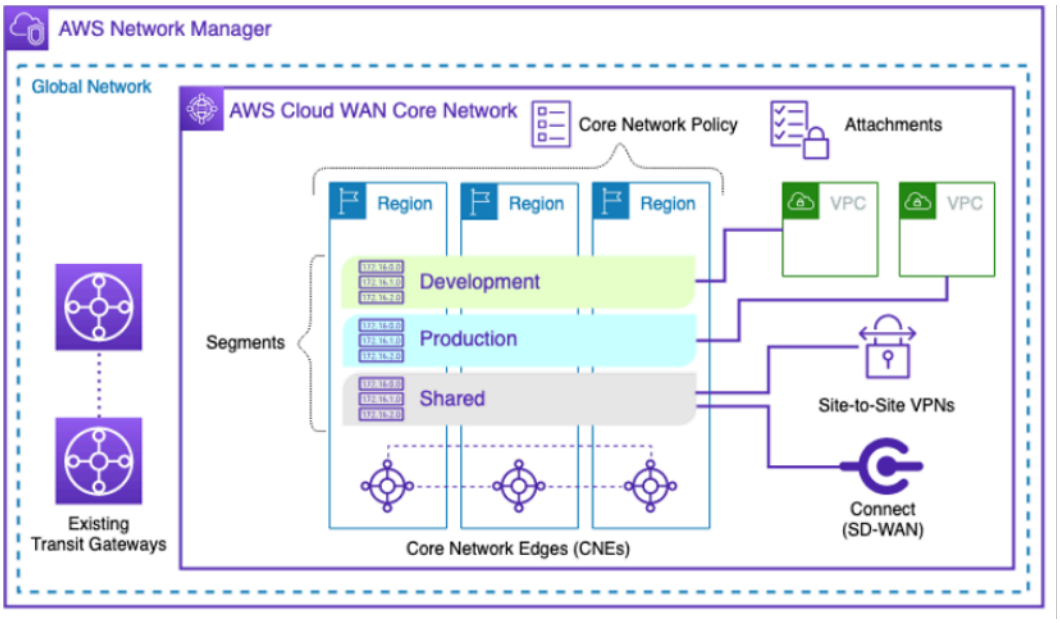
- 네트워크 리소스 (예: 엣지 로케이션, 디바이스, 첨부 파일) 의 위치를 정확히 알려주는 세계 지도.
- 모니터링은 CloudWatch 이벤트를 사용하여 15개월 분량의 통계를 추적하여 네트워크 성능을 더 잘 파악할 수 있도록 합니다.
- 실시간 이벤트를 이벤트 대시보드로 스트리밍하는 이벤트 추적.
- 트랜짓 게이트웨이 네트워크 및 트랜짓 게이트웨이의 토폴로지 및 논리적 다이어그램.

Transit Gateway와 클라우드 WAN 모두 VPC와 온프레미스 위치 간의 중앙 집중식 연결을 허용합니다. Transit Gateway는 지역 네트워크 연결 허브로서 일부 AWS 지역에서 사업을 운영하거나 자체 피어링 및 라우팅 구성을 관리하고자 하거나 자체 자동화 사용을 선호하는 고객에게 적합합니다. 클라우드 WAN은 정책을 통해 글로벌 네트워크를 정의하고 서비스가 기본 구성 요소를 자동으로 구현하도록 하려는 고객에게 적합합니다.

알아야 할 것들

- CNE (코어 네트워크 에지) 는 VPC 연결당 처리량과 같은 많은 Transit Gateway 특성을 상속합니다.
- 클라우드 WAN은 IPv4와 IPv6를 모두 지원합니다.

- 현재 클라우드 WAN은 첨부 파일을 기본적으로 지원하지 않습니다. AWS Direct Connect 클라우드 AWS Direct Connect WAN과 함께 사용하려면 Transit Gateway를 게이트웨이에 연결한 다음 Transit AWS Direct Connect Gateway를 클라우드 WAN에 피어링해야 합니다.
- 변경 사항이 많은 대규모 네트워크의 경우 변경 사항을 검증할 수 있는 별도의 개발 및 테스트 글로벌 네트워크를 만드는 것이 좋습니다.



AWS Cloud WAN

추가적인 리소스

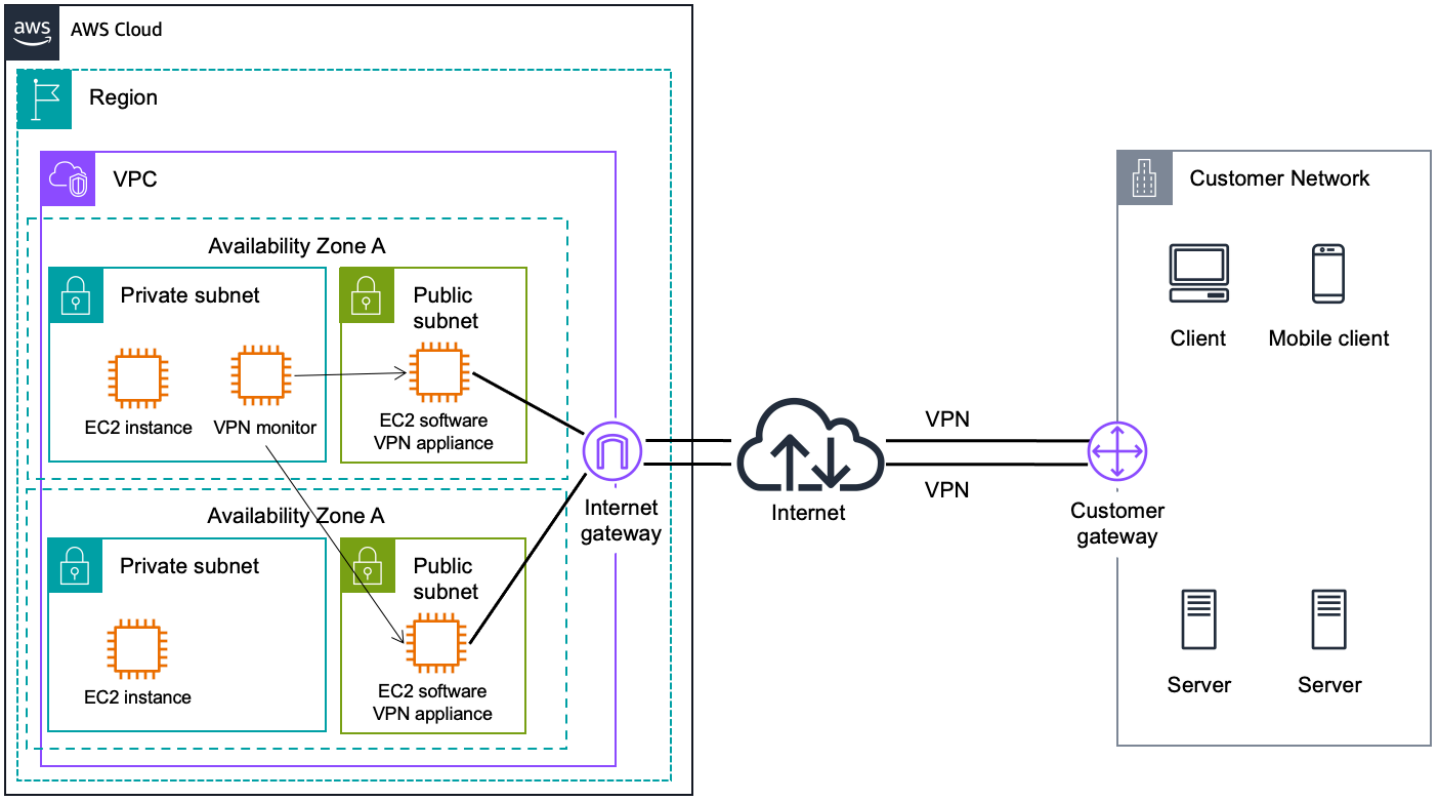
- AWS 클라우드 WAN 설명서
- 블로그 게시물: AWS 클라우드 WAN 및 AWS Transit Gateway 마이그레이션 및 상호 운용성 패턴

결론

AWS는 사용자의 원격 네트워크를 Amazon VPC와 통합할 때 사용자가 AWS를 최대한 활용할 수 있도록 여러 가지 효율적이고 안전한 연결 옵션을 제공합니다. 이 백서에서 설명하는 옵션에서는 고객이 자신의 원격 네트워크 또는 여러 Amazon VPC 네트워크를 성공적으로 통합하는 데 사용한 몇 가지 연결 옵션 및 패턴을 강조합니다. 여기에 제공된 정보를 사용하여 물리적 위치 또는 호스팅되는 위치에 관계없이 비즈니스를 운영하는 데 필요한 인프라를 연결하는 데 가장 적합한 메커니즘을 결정할 수 있습니다.

부록 A: 소프트웨어 VPN 인스턴스를 위한 고수준 HA 아키텍처

소프트웨어 VPN 인스턴스에 대해 완전히 복원력이 뛰어난 VPC 연결을 생성하려면 여러 VPN 인스턴스의 설정 및 구성과 VPN 연결 상태를 모니터링하기 위한 모니터링 인스턴스가 필요합니다.



고수준 소프트웨어 VPN HA

한 가용 영역의 모든 서브넷에서 들어오는 트래픽을 동일한 가용 영역의 해당 VPN 인스턴스를 통해 전달하여 모든 VPN 인스턴스를 동시에 활용하도록 VPC 라우팅 테이블을 구성하는 것이 좋습니다. 그러면 각 VPN 인스턴스가 동일한 가용 영역을 공유하는 인스턴스에 VPN 연결을 제공합니다.

VPN 모니터링

소프트웨어 기반 VPN 어플라이언스를 모니터링하려면 VPN 모니터를 만들 수 있습니다. VPN 모니터는 VPN 모니터링 스크립트를 실행해야 하는 사용자 지정 인스턴스입니다. 이 인스턴스는 VPN 연결 및 VPN 인스턴스의 상태를 실행하고 모니터링하기 위한 것입니다. VPN 인스턴스 또는 연결이 중단되는 경우 모니터는 VPN 인스턴스를 중지, 종료 또는 다시 시작해야 하며 두 연결이 모두 다시 작동할 때까지 영향을 받는 서브넷의 트래픽을 작동 중인 VPN 인스턴스로 다시 라우팅해야 합니다. 고객 요구 사

항이 다양하기 때문에 AWS는 현재 이 모니터링 인스턴스 설정에 대한 규범적 지침을 제공하지 않습니다. 하지만 NAT 인스턴스 간 HA를 활성화하기 위한 예제 스크립트는 소프트웨어 VPN 인스턴스용 HA 솔루션을 만들기 위한 출발점으로 사용할 수 있습니다. VPN 연결 실패 시 필요한 비즈니스 로직을 숙고하여 알림을 제공하거나 네트워크 연결을 자동으로 복구하도록 시도하는 것이 좋습니다.

또한 Amazon 메트릭을 사용하여 AWS Managed VPN 터널을 모니터링할 수 있습니다. Amazon CloudWatch 메트릭은 VPN 서비스에서 데이터 포인트를 읽을 수 있는 거의 실시간 지표로 수집합니다. 각 VPN 연결은 다양한 터널 메트릭을 수집하여 CloudWatch Amazon에 게시합니다. 이러한 지표를 통해 터널 상태, 활동을 모니터링하고 자동화된 작업을 생성할 수 있습니다.

기여자

다음은 이 문서의 기여자입니다.

- 다니엘 유, AWS 엔터프라이즈 지원 수석 기술 계정 관리자
- 가빗 싱, 솔루션 빌더, AWS 솔루션 아키텍처
- 스티브 모라드, 시니어 매니저, 솔루션 빌더, AWS 솔루션 아키텍처
- 소하비 타히르, 솔루션스 아키텍트, AWS 솔루션 아키텍처
- 피오나 아르마다, 수석 솔루션 아키텍트, AWS 솔루션 아키텍처
- 파블로 산체스 카르모나, 네트워킹 전문가 솔루션 아키텍트, AWS 솔루션 아키텍처
- Tony Hawke, 수석 네트워킹 전문가 기술 계정 관리자, AWS 엔터프라이즈 지원

문서 수정

이 백서에 대한 업데이트 알림을 받으려면 RSS 피드를 구독하면 됩니다.

변경 사항	설명	날짜
백서 업데이트	AWS 클라우드 WAN 및 Transit Gateway 연결 연결 옵션이 추가되었고, 전체적으로 다이어그램과 정보가 업데이트되었습니다.	2023년 4월 5일
백서 업데이트	AWS Transit Gateway 및 AWS Client VPN 옵션을 추가하고 전체적으로 다이어그램과 정보를 업데이트했습니다.	2020년 6월 6일
마이너 업데이트	소프트웨어 VPN 어플라이언스에 대한 참조를 수정하기 위한 사소한 변경.	2020년 5월 20일
백서 업데이트	전체 정보가 업데이트되었습니다. 트랜짓 VPC, Direct Connect 게이트웨이 등의 디자인/기능에 중점을 둡니다. AWS PrivateLink	2018년 1월 1일
최초 게시	Amazon Virtual Private 클라우드 연결 옵션이 게시되었습니다.	2014년 7월 1일

고지 사항

고객은 본 문서에 포함된 정보를 독자적으로 평가할 책임이 있습니다. 본 문서는 (a) 정보 제공만을 위한 것이며, (b) 사전 고지 없이 변경될 수 있는 현재의 AWS 제품 제공 서비스 및 사례를 보여 주며, (c) AWS 및 자회사, 공급업체 또는 라이선스 제공자로부터 어떠한 약정 또는 보증도 하지 않습니다. AWS 제품 또는 서비스는 명시적이든 묵시적이든 어떠한 종류의 보증, 진술 또는 조건 없이 '있는 그대로' 제공됩니다. 고객에 대한 AWS의 책임과 법적 책임은 AWS 계약서에 준하며 본 문서는 AWS와 고객 간의 계약에 포함되지 않고 계약을 변경하지도 않습니다.

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