Amazon Virtual Private Cloud(VPC) 연결 옵션

Steve Morad
2012년 10월

(이 문서의 최신 버전은 http://aws.amazon.com/whitepapers/를 참조하십시오.)

목차

요약

Amazon Virtual Private Cloud(VPC)를 사용하면 고객이 정의하는 IP 주소 범위를 사용하여 가상 네트워크에서 AWS(Amazon Web Services) 리소스를 시작할 수 있는 AWS 클라우드의 프라이빗 격리 섹션을 프로비저닝할 수 있습니다. Amazon VPC는 고객에게 AWS 가상 네트워크와 기타 원격 네트워크를 상호 연결할 수 있는 여러 옵션을 제공합니다. 이 문서에는 고객이 사용할 수 있는 몇 가지 일반적인 네트워크 연결 옵션이 설명되어 있습니다. 원격 고객 네트워크를 Amazon VPC와 통합할 수 있는 연결 옵션뿐 아니라 여러 Amazon VPC를 연속적인 가상 네트워크와 상호 연결할 수 있는 연결 옵션도 포함되어 있습니다.

이 백서는 기업 네트워크 설계자 및 엔지니어 또는 사용 가능한 연결 옵션을 검토하는 Amazon VPC 관리자를 대상으로 합니다. 이 문서는 네트워크 연결 논의를 원활히 진행할 수 있는 다양한 옵션에 대한 개요를 제공하며 더 자세한 정보나 예제를 제공하는 추가 설명서 및 리소스에 대한 포인터도 제공합니다.

소개

Amazon VPC는 고객에게 현재 네트워크 디자인 및 요구 사항에 맞춰 활용할 수 있는 여러 가지 네트워크 연결 옵션을 제공합니다. 이러한 연결 옵션에는 인터넷 또는 AWS Direct Connect 연결을 네트워크 "백본"으로 활용하고 AWS 또는 고객이 관리하는 네트워크 엔드포인트로의 연결을 종료할 수 있는 기능이 포함되어 있습니다. 또한, AWS는 고객이 AWS 또는 고객이 관리하는 네트워크 장비 및 라우팅 중 하나를 활용하여 Amazon VPC 및 고객 네트워크 간에 네트워크 라우팅을 전달하는 방식을 선택할 수 있게 해 줍니다. 이 백서는 다음 섹션 및 하위 섹션에서 이러한 옵션에 대해 자세히 설명합니다. 각 섹션은 개요로 시작되며, 각 옵션에 대한 대략적인 비교가 포함되어 있습니다.

고객 네트워크-Amazon VPC 연결 옵션	
하드웨어 VPN	원격 네트워크에 있는 고객의 네트워크 장비에서 고객의 Amazon VPC에 연결된 AWS 관리형 네트워크 장비로 하드웨어 VPN 연결을 설정하는 데 대한 내용을 설명합니다.
AWS Direct Connect	AWS Direct Connect를 사용하여 고객의 원격 네트워크에서 Amazon VPC로 프라이빗 논리적 연결을 설정하는 데 대한 내용을 설명합니다.
AWS Direct Connect + VPN	AWS Direct Connect를 사용하여 고객의 원격 네트워크에서 Amazon VPC로 프라이빗 암호화된 연결을 설정하는 데 대한 정보가 나와 있습니다.
AWS VPN CloudHub	원격 지사를 연결하기 위해 허브 앤 스포크 모델을 설정하는 데 대한 내용을 설명합니다.
소프트웨어 VPN	원격 네트워크에 있는 고객의 네트워크 장비에서 Amazon VPC를 내부에서 실행 중인 고객이 관리하는 소프트웨어 VPN 어플라이언스로 VPN 연결을 설정하는 데 대한 내용을 설명합니다.
Amazon VPC–Amazon VPC 연결 옵션	
소프트웨어 VPN	각각의 Amazon VPC 내부에서 실행 중인 고객 관리형 소프트웨어 VPN 어플라이언스 간에 설정된 VPN 연결을 사용하여 여러 Amazon VPC를 상호 연결하는 데 대한 정보가 나와 있습니다.
하드웨어-소프트웨어 VPN	Amazon VPC의 고객 관리형 소프트웨어 VPN 어플라이언스와 다른 Amazon VPC에 연결된 AWS 관리형 네트워크 장비 간에 설정된 VPN 연결을 사용하여 여러 Amazon VPC를 상호 연결하는 데 대한 정보가 나와 있습니다.
하드웨어 VPN	고객의 원격 네트워크와 각 Amazon VPC 간에 설정된 여러 개의 하드웨어 VPN 연결을 사용하여 여러 Amazon VPC를 상호 연결하는 데 대한 정보가 나와 있습니다.
AWS Direct Connect	고객이 관리하는 AWS Direct Connect 라우터에서 논리적 연결을 사용하여 여러 Amazon VPC를 상호 연결하는 데 대한 내용을 설명합니다.
내부 사용자-Amazon VPC 연결 옵션	
소프트웨어 원격 액세스 VPN	이 섹션에서는 VPC 리소스에 원격 사용자를 연결하기 위한 고객 네트워크-Amazon VPC 연결 옵션 외에도, 최종 사용자에게 Amazon VPC로의 VPN 액세스 권한을 제공하기 위한 원격 액세스 솔루션 사용 관련 내용이 나와 있습니다.

고객 네트워크-Amazon VPC 연결 옵션

이 섹션에서는 Amazon VPC 환경과 원격 네트워크를 상호 연결하려는 고객을 위한 디자인 패턴을 제공합니다. 이러한 옵션은 내부 네트워크를 AWS 클라우드로 확장하여 고객의 기존 현장 서비스(예: 모니터링, 인증, 보안, 데이터 또는 기타 시스템)와 AWS 리소스를 통합하는 경우 유용합니다. 또한, 이 네트워크 확장을 수행하면 내부에서 리소스를 사용할 때와 같이 내부 사용자가 AWS에서 호스트하는 리소스에 원활하게 연결할 수 있습니다.

상호 연결되는 각각의 네트워크에 중첩되지 않는 IP 범위를 사용하는 경우 원격 고객 네트워크에 대한 VPC 연결이 가장 효율적으로 설정됩니다. 예를 들어 하나 이상의 VPC를 홈 네트워크에 상호 연결하려는 경우 고유 CIDR (클래스 없는 도메인 간 라우팅) 범위로 구성되었는지 확인하십시오. 따라서 각 VPC에서 사용할 연속되는 비중첩 CIDR 블록 하나를 할당하는 것이 좋습니다. Amazon VPC 라우팅 및 제약 조건에 대한 자세한 내용은 Amazon VPC FAQ를 참조하십시오. http://aws.amazon.com/vpc/faqs/.

옵션	사용 사례	장점	제한
하드웨어 VPN	인터넷을 통한 하드웨어 기반 IPsec VPN 연결	• 기존 VPN 장비 및 프로세스를 재사용합니다. • 기존 인터넷 연결을 재사용합니다. • AWS 관리형 엔드포인트에는 다중 데이터 센터 중복성 및 자동화된 장애 조치가 포함되어 있습니다. • 정적 라우터 또는 동적 BGP(Border Gateway Protocol) 피어링 및 라우팅 정책을 지원합니다.	• 네트워크 지연 시간, 가변성 및 가용성은 인터넷 조건에 따라 다릅니다. • 고객 관리형 엔드포인트는 필요한 경우 중복성 및 장애 조치를 구현해야 합니다. • 동적 라우팅을 위해 BGP를 활용하는 경우 고객 장치가 단일 홉 BGP를 지원해야 합니다.
AWS Direct Connect	전용 회선을 통한 전용 네트워크 연결	• 네트워크 성능을 더 쉽게 예측할 수 있습니다. • 대역폭 비용이 절감됩니다. • 1Gbps 또는 10Gbps 프로비저닝 연결을 제공합니다. • BGP 피어링 및 라우팅 정책을 지원합니다.	• 추가되는 통신 및 호스팅 공급자 관계나 새 네트워크 회로를 프로비저닝해야 할 수도 있습니다.
AWS Direct Connect + VPN	전용 회선을 통한 하드웨어 기반 IPsec VPN 연결	• 이전 옵션과 동일하며 보안 IPsec VPN 연결이 추가됩니다.	• 이전 옵션과 동일하며 VPN 추가가 약간 복잡합니다.
AWS VPN CloudHub	기본 또는 백업 연결을 위해 허브 앤 스포크 모델의 원격 지사 연결	• 기존 인터넷 연결 및 AWS VPN 연결을 재사용합니다(예: CloudHub를 타사 MPLS 네트워크에 대한 백업 연결로 사용). • AWS 관리형 가상 프라이빗 게이트웨이에는 다중 데이터 센터 중복성 및 자동화된 장애 조치가 포함되어 있습니다. • 라우팅 및 라우팅 우선 순위 교환을 위해 BGP를 지원합니다(예: 백업 AWS VPN 연결을 통한 MPLS 연결 선호).	• 네트워크 지연 시간, 가변성 및 가용성은 인터넷에 따라 다릅니다. • 고객 관리형 지사 엔드포인트는 필요한 경우 중복성 및 장애 조치를 구현해야 합니다.
소프트웨어 VPN	인터넷을 통한 소프트웨어 어플라이언스 기반 VPN 연결	• 다양한 VPN 공급 업체, 제품 및 프로토콜을 지원합니다. • 완전한 고객 관리형 솔루션입니다.	• 필요한 경우 고객이 모든 VPN 엔드포인트에 대한 HA 솔루션을 구현해야 합니다.

하드웨어 VPN

Amazon VPC는 그림 1에 나와 있는 것처럼 IPsec, 원격 고객 네트워크 간 하드웨어 VPN 연결 및 인터넷을 통한 Amazon VPC 생성 옵션을 제공합니다. VPN 연결의 AWS 측에 구축된 자동화된 다중 데이터 센터 중복성 및 장애 조치를 포함하는 AWS 관리형 VPN 엔드포인트를 활용하려는 고객은 이 접근 방식을 사용하는 것이 좋습니다. 표시되어 있지는 않지만 Amazon VGW(가상 프라이빗 게이트웨이)는 VPN 연결 가용성을 확대하기 위해 별도의 데이터 센터에 물리적으로 위치하고 있는 고유 VPN 엔드포인트 두 개를 제공합니다.

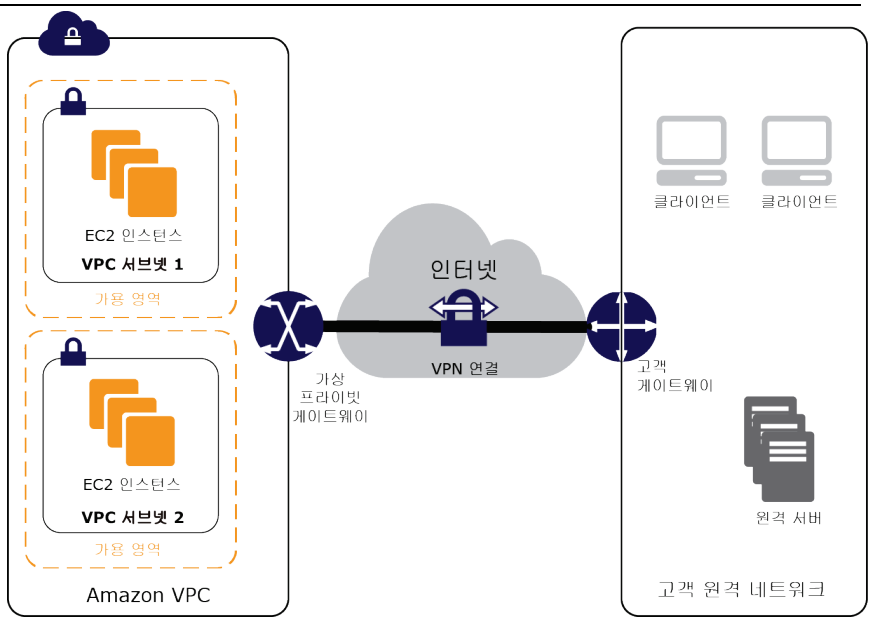

그림 1 – 하드웨어 VPN

Amazon VGW는 여러 개의 고객 게이트웨이 연결을 지원하고 권장하므로 그림 2에 나와 있는 것처럼 고객이 VPN 연결 시 중복성 및 장애 조치를 구현할 수도 있습니다. 고객이 유연하게 라우팅 구성을 수행할 수 있도록 동적 및 정적 라우팅 옵션이 모두 제공됩니다. 동적 라우팅에서는 BGP 피어링을 이용하여 AWS와 이러한 원격 엔드포인트 간에 라우팅 정보를 교환합니다. 또한, 동적 라우팅을 사용하면 고객이 BGP 공급에 라우팅 우선순위, 정책 및 가중치(측정치)를 지정할 수 있으며 네트워크와 AWS 간의 네트워크 경로에 영향을 미칠 수 있습니다.

BGP를 사용할 경우 동일한 고객 게이트웨이 디바이스에서 IPSec와 BGP 연결을 모두 종료해야 하므로, IPSec와 BGP 연결을 모두 종료할 수 있는 상태여야 한다는 점에 유의하십시오.

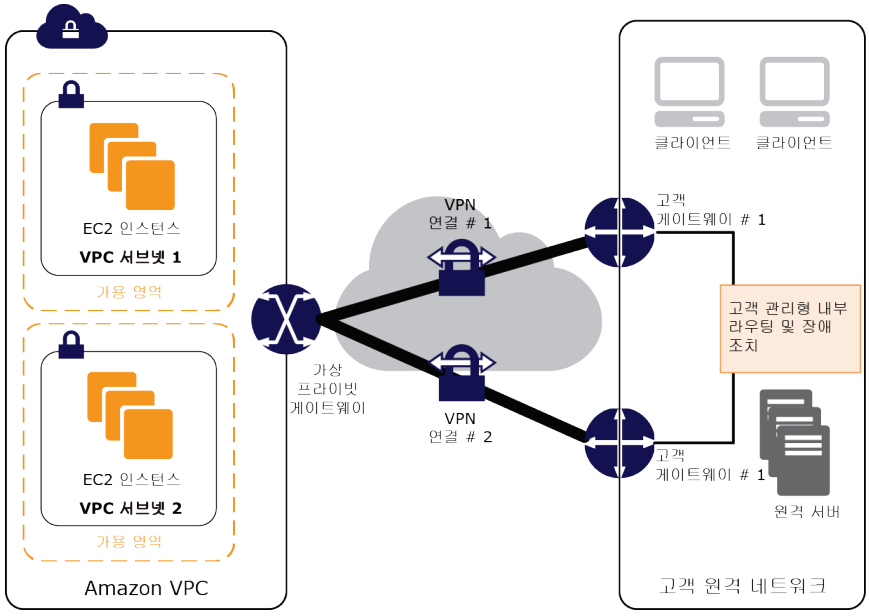

그림 2 – 중복 하드웨어 VPN 연결

추가 리소스

- VPC에 하드웨어 가상 프라이빗 게이트웨이 추가
- 고객 게이트웨이 장치 최소 요구 사항
- Amazon VPC와 작동하는 것으로 알려진 고객 게이트웨이 장치

AWS Direct Connect

AWS Direct Connect를 사용하면 온프레미스에서 Amazon VPC로 전용 네트워크 연결을 쉽게 설정할 수 있습니다. 고객은 AWS Direct Connect를 사용하여 AWS와 데이터 센터, 사무실 또는 코로케이션 환경 사이의 프라이빗 연결을 설정할 수 있습니다. 이러한 프라이빗 연결을 통해 네트워크 비용을 절감하고 대역폭 처리량을 늘리며, 인터넷 기반 연결보다 더욱 일관된 네트워크 환경을 제공할 수 있습니다.

AWS Direct Connect를 사용하면 고객이 AWS Direct Connect 위치 중 하나와 AWS 네트워크 간에 1Gbps 또는 10Gbps 전용 네트워크 연결 또는 다중 연결을 설정할 수 있으며, 산업 표준 VLAN을 사용하여 Amazon VPC 내에서 프라이빗 IP 주소를 통해 실행되는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 액세스할 수 있습니다. 고객은 AWS Direct Connect 위치에 있는 AWS Direct Connect 엔드포인트를 원격 네트워크와 통합하기 위해 WAN 서비스 공급자의 에코시스템을 선택할 수도 있습니다. 그림 3에는 이 패턴이 설명되어 있습니다.

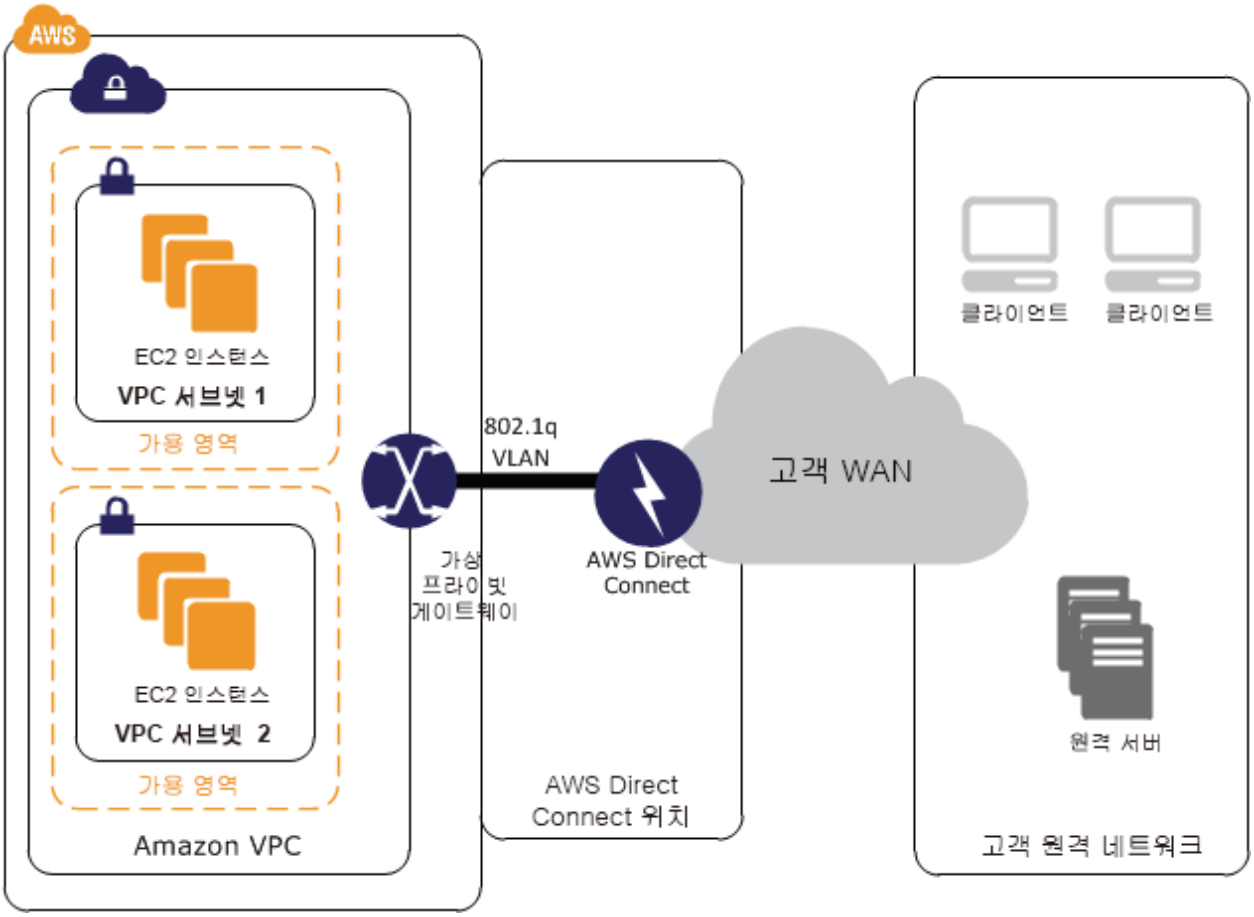

그림 3 - AWS Direct Connect

추가 리소스

- AWS Direct Connect 제품 페이지
- AWS Direct Connect 위치
- AWS Direct Connect FAQ
- AWS Direct Connect 시작하기

AWS Direct Connect + VPN

AWS Direct Connect + VPN을 통해 고객은 하나 이상의 AWS Direct Connect 전용 네트워크 연결을 Amazon VPC 하드웨어 VPN과 결합할 수 있습니다. 이러한 결합은 IPsec 암호화된 프라이빗 연결을 제공하여 네트워크 비용을 절감하고 대역폭 처리량을 늘리며, 인터넷 기반 VPN 연결보다 더욱 일관된 네트워크 환경을 제공합니다.

AWS Direct Connect를 사용하면 고객이 AWS Direct Connect 위치 중 하나와 고객 네트워크 간에 전용 네트워크 연결을 설정할 수 있으며, 산업 표준 VLAN을 사용하여 Amazon VGW IPsec 엔드포인트와 같은 퍼블릭 AWS 리소스에 대한 논리적 연결을 생성할 수 있습니다. 이 솔루션은 하드웨어 VPN 솔루션의 AWS 관리형 이점을 결합하여 지연 시간이 적고 대역폭이 증가되며, AWS Direct Connect의 장점인 더욱 일관적인 네트워크 환경을 제공할 수 있게 되고 종단 간 안전한 IPsec 연결을 제공할 수 있습니다. 그림 4에는 이 옵션이 나와 있습니다.

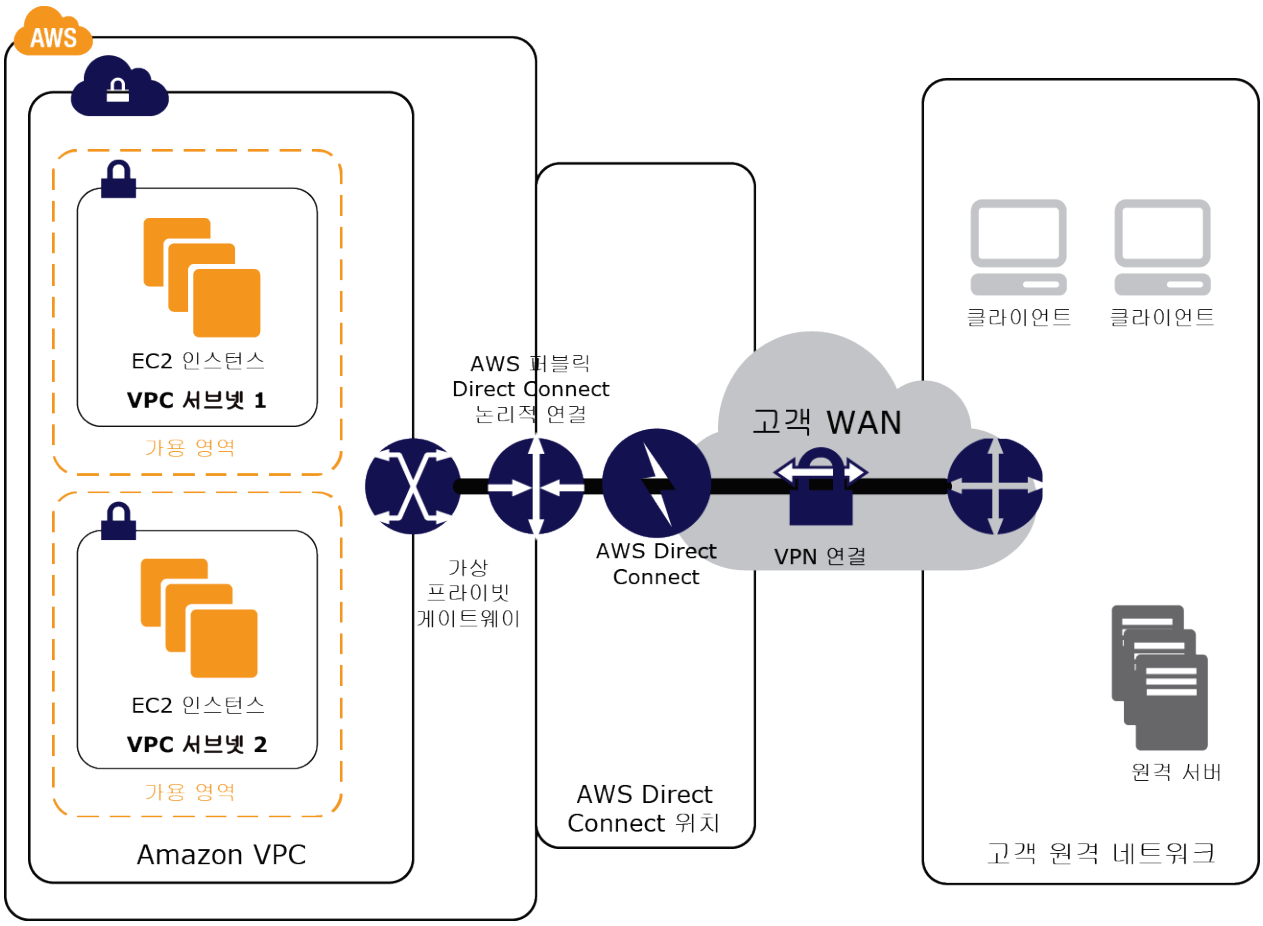

그림 4 - AWS Direct Connect + VPN

추가 리소스

- AWS Direct Connect 제품 페이지
- AWS Direct Connect FAQ
- VPC에 하드웨어 가상 프라이빗 게이트웨이 추가

AWS VPN CloudHub

위에서 설명한 하드웨어 VPN 및 AWS Direct Connect 옵션을 기반으로 하므로 고객은 AWS VPN CloudHub를 사용하여 안전하게 사이트 간 통신을 수행할 수 있습니다. VPN CloudHub는 VPC와 함께 또는 VPC 없이 사용할 수 있는 간단한 허브 앤 스포크 모델에서 작동합니다. 이러한 디자인은 여러 지사가 있고 기존 인터넷 연결을 사용하는 고객이 원격 지사 간에 기본 또는 백업 연결을 위해 편리하고도 경제적인 허브 앤 스포크 모델을 구현하고자 할 때 적합합니다. 그림 5는 AWS VPN CloudHub 아키텍처를 보여 주며, 파란색 점선은 AWS VPN 연결을 통해 라우팅되는 원격 사이트 간의 네트워크 트래픽을 나타냅니다.

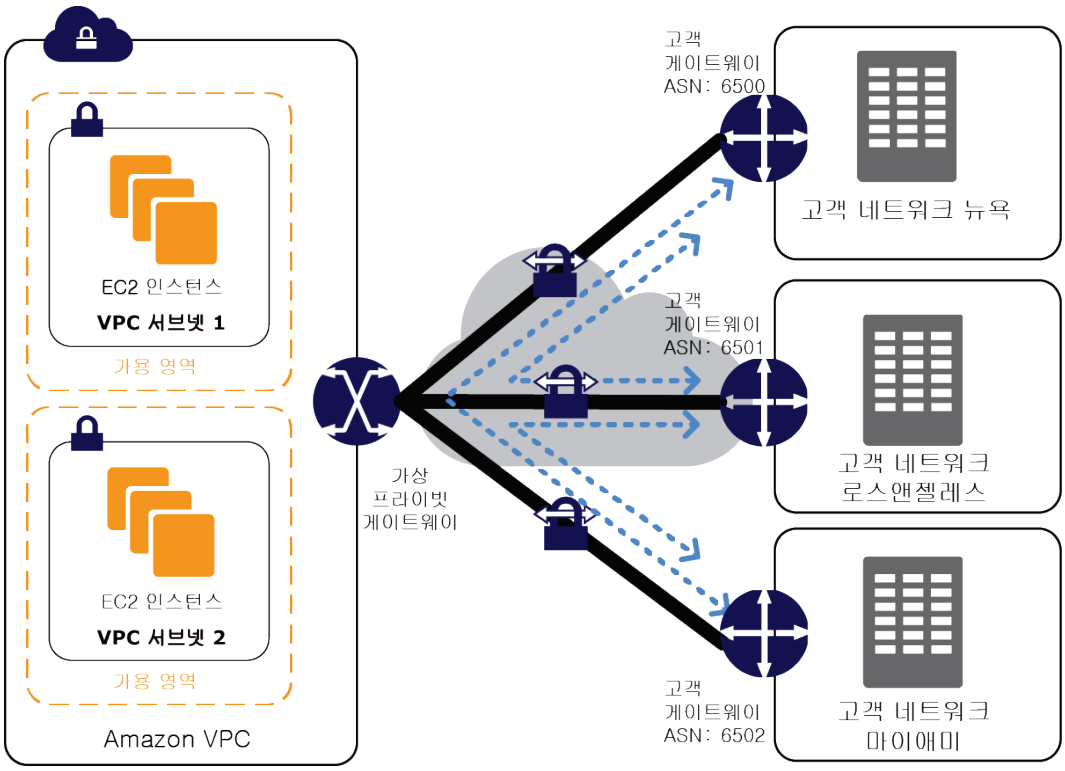

그림 5 – AWS VPN CloudHub

AWS VPN CloudHub는 고유의 BGP ASN(자율 시스템 번호)을 각각 사용하는 여러 고객 게이트웨이가 있는 VPC 가상 프라이빗 게이트웨이를 활용합니다. 고객 게이트웨이는 VPN 연결을 통해 적절한 라우팅(BGP 접두사)을 공급합니다. 이처럼 라우팅을 공급하면 각 BGP 피어에서 이를 수신하여 다시 공급함으로써 각 사이트는 다른 사이트와 데이터를 주고받을 수 있습니다. 각 스포크의 원격 네트워크 접두사는 고유 ASN이 있어야 하며 사이트의 IP 범위는 중복되지 않아야 합니다. 각 사이트는 스탠다드 VPN 연결을 사용하는 것처럼 VPC에서 데이터를 송수신할 수도 있습니다.

이 옵션은 고객 요구 사항에 따라 AWS Direct Connect 또는 기타 하드웨어 VPN 옵션(예: 고객 측 중복성 또는 고객 백본 라우팅을 위한 사이트별 여러 고객 게이트웨이)을 결합할 수 있습니다.

추가 리소스

- AWS VPN CloudHub
- Amazon VPC VPN 가이드
- 고객 게이트웨이 장치 최소 요구 사항
- Amazon VPC와 작동하는 것으로 알려진 고객 게이트웨이 장치
- AWS Direct Connect 제품 페이지

소프트웨어 VPN

Amazon VPC는 원격 네트워크와 Amazon VPC 네트워크에서 실행 중인 소프트웨어 VPN 어플라이언스 간 VPN 연결을 생성하여 고객이 Amazon VPC 연결 양쪽을 완전히 관리할 수 있는 유연성을 제공합니다. 이 옵션은 규정 준수를 위해 또는 Amazon VPC 하드웨어 VPN 솔루션에서 현재 지원되지 않는 고객 게이트웨이 장치를 활용하기 위해 VPN 연결 양쪽을 관리해야 하는 고객이 사용하는 것이 좋습니다. 그림 6에는 이 옵션이 나와 있습니다.

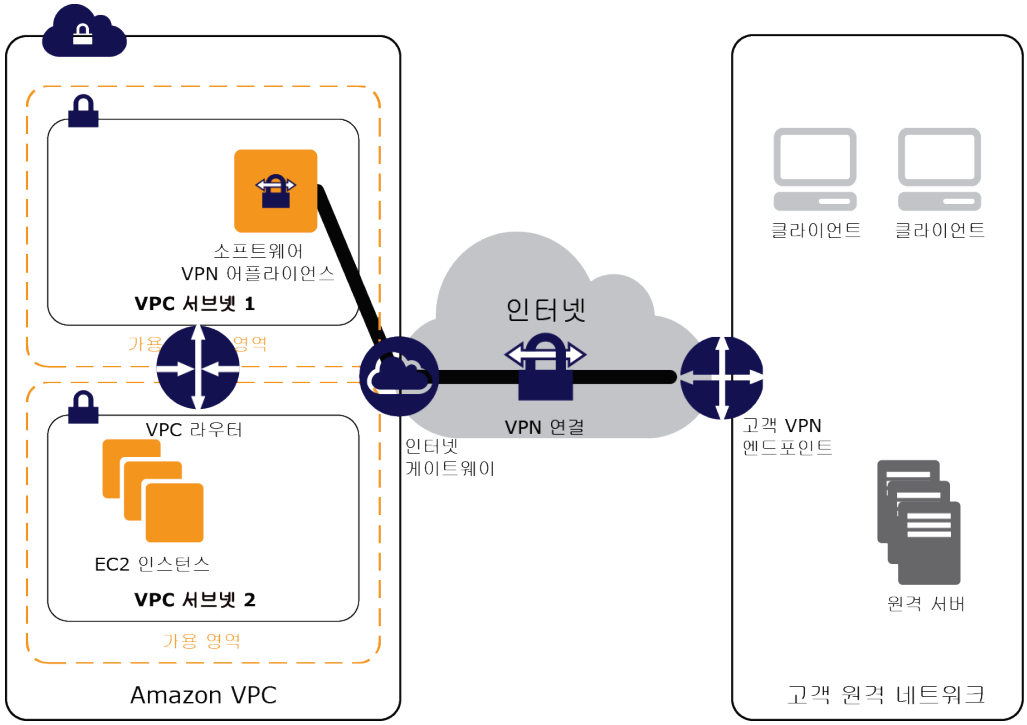

그림 6 – 소프트웨어 VPN

AWS 고객은 Amazon EC2에서 실행되는 소프트웨어 VPN 어플라이언스를 만든 여러 파트너와 오픈 소스 커뮤니티의 에코시스템에서 선택할 수 있습니다. 여기에는 Checkpoint, Astaro, OpenVPN Technologies 및 Microsoft와 같이 잘 알려진 보안 회사의 제품과 OpenVPN, OpenSWAN 및 IPsec-Tools와 같이 인기 있는 오픈 소스 도구가 포함됩니다. 이러한 제품 및 도구를 사용하면 고객이 구성, 패치, 업그레이드를 포함하여 소프트웨어 어플라이언스를 관리해야 합니다.

이 디자인의 경우 소프트웨어 VPN 어플라이언스가 단일 Amazon EC2 인스턴스에서 실행되므로 네트워크 디자인으로의 잠재적인 단일 실패 지점이 발생한다는 점에 유의하십시오. 추가 정보는 부록 A: 소프트웨어 VPN 인스턴스에 대한 상위 수준 HA 아키텍처를 참조하십시오.

추가 리소스

- AWS Marketplace의 VPN 어플라이언스
- 문서 - Cisco ASA를 VPC EC2 인스턴스에 연결(IPSec)
- 문서 - 여러 VPC를 EC2 인스턴스와 연결(IPSec) [1]
- 문서 - 여러 VPC를 EC2 인스턴스와 연결(SSL) [1]

---

[1] 이 문서에서 특히 여러 Amazon VPC 연결에 대해 설명했지만 IPsec 또는 Amazon VPC 에서 실행 중인 SSL 소프트웨어 VPN 어플라이언스에 연결되는 온프레미스 VPN 장치로 VPC 중 하나를 대체하여 이 네트워크 구성을 지원하도록 조정할 수 있습니다.

Amazon VPC–Amazon VPC 연결 옵션

이 디자인 패턴은 여러 Amazon VPC를 더 큰 가상 네트워크에 통합하려는 고객에게 적용할 수 있습니다. 이 옵션은 보안, 결제, 여러 리전에 존재 유무 또는 내부 차지백 요구 사항으로 인해 여러 VPC가 필요한 고객에게 유용한 옵션으로, Amazon VPC 간 AWS 리소스를 더욱 쉽게 통합할 수 있습니다. 이 패턴은 원격 네트워크 및 여러 VPC를 포괄하는 회사 네트워크를 생성하기 위해 고객 네트워크-Amazon VPC 연결 옵션과 결합될 수도 있습니다.

상호 연결되는 각각의 VPC에 중첩되지 않는 IP 범위를 사용하는 경우 VPC 간에 각각의 VPC 연결이 가장 효율적으로 설정됩니다. 예를 들어 여러 VPC를 상호 연결하려는 경우 각각의 VPC가 고유 CIDR(클래스 없는 도메인 간 라우팅) 범위로 구성되었는지 확인하십시오. 따라서 각 VPC에서 사용할 연속되는 비중첩 CIDR 블록 하나를 할당하는 것이 좋습니다. Amazon VPC 라우팅 및 제약 조건에 대한 자세한 내용은 Amazon VPC FAQ를 참조하십시오. http://aws.amazon.com/vpc/faqs/

옵션	사용 사례	장점	제한
소프트웨어 VPN	VPC 간 소프트웨어 어플라이언스 기반 VPN 연결	• 리전 내 AWS 네트워킹 장비 및 리전 간 인터넷 파이프를 활용합니다. • 다양한 VPN 공급 업체, 제품 및 프로토콜을 지원합니다. • 완전한 고객 관리형 솔루션입니다.	• 필요한 경우 고객이 모든 VPN 엔드포인트에 대한 HA 솔루션을 구현해야 합니다.
하드웨어-소프트웨어 VPN	VPC 간 소프트웨어 어플라이언스-하드웨어 VPN 연결	• 리전 내 AWS 네트워킹 장비 및 리전 간 인터넷 파이프를 활용합니다. • AWS 관리형 엔드포인트에는 다중 데이터 센터 중복성 및 자동화된 장애 조치가 포함되어 있습니다.	• 고객은 필요한 경우 소프트웨어 어플라이언스 VPN 엔드포인트에 대한 HA 솔루션을 구현해야 합니다.
하드웨어 VPN	고객 장비 및 인터넷을 사용하여 하드웨어 기반 IPsec VPN 연결을 통해 고객이 관리하는 VPC-VPC 라우팅	• 기존 Amazon VPC VPN 연결을 재사용합니다. • AWS 관리형 엔드포인트에는 다중 데이터 센터 중복성 및 자동화된 장애 조치가 포함되어 있습니다. • 정적 라우팅, 동적 BGP 피어링 및 라우팅 정책을 지원합니다.	• 네트워크 지연 시간, 가변성 및 가용성은 인터넷 조건에 따라 다릅니다. • 고객 관리형 엔드포인트는 필요한 경우 중복성 및 장애 조치를 구현해야 합니다.
AWS Direct Connect	AWS Direct Connect 위치 및 전용 회선의 고객 장비를 사용하여 고객이 관리하는 VPC-VPC 라우팅	• 네트워크 성능이 일관적으로 유지됩니다. • 대역폭 비용이 절감됩니다. • 1Gbps 또는 10Gbps 프로비저닝 연결을 제공합니다. • 정적 라우팅, BGP 피어링 및 라우팅 정책을 지원합니다.	• 추가 통신 및 호스팅 공급자 관계가 필요할 수 있습니다.

소프트웨어 VPN

Amazon VPC는 고객에게 네트워크 라우팅 유연성을 제공합니다. 이 유연성은 둘 이상의 소프트웨어 VPN 어플라이언스 사이에 안전한 VPN 터널을 생성하여 여러 VPC를 더 큰 가상 프라이빗 네트워크에 연결할 수 있게 해 주므로, 각 VPC의 인스턴스가 프라이빗 IP 주소를 사용하여 서로 원활하게 접속할 수 있게 됩니다. 이 옵션은 선호하는 VPN 소프트웨어 공급자를 사용하여 VPN 연결의 양쪽 끝을 관리하려는 고객에게 권장됩니다. 이 옵션은 VPC 두 개에 연결된 "인터넷" 게이트웨이[2]를 사용하여 소프트웨어 VPN 어플라이언스 간 통신을 원활하게 해 줍니다.

AWS 고객은 Amazon EC2에서 실행되는 소프트웨어 VPN 어플라이언스를 만든 여러 파트너와 오픈 소스 커뮤니티의 에코시스템에서 선택할 수 있습니다. 여기에는 Checkpoint, Sophos, OpenVPN Technologies 및 Microsoft와 같이 잘 알려진 보안 회사의 제품과 OpenVPN, OpenSWAN 및 IPsec-Tools와 같이 인기 있는 오픈 소스 도구가 포함됩니다. 이러한 제품 및 도구를 사용하면 고객이 구성, 패치, 업그레이드를 포함하여 소프트웨어 어플라이언스를 관리해야 합니다.

이 디자인의 경우 소프트웨어 VPN 어플라이언스가 단일 Amazon EC2 인스턴스에서 실행되므로 네트워크 디자인으로의 잠재적인 단일 실패 지점이 발생한다는 점에 유의하십시오. 추가 정보는 "부록 A: 소프트웨어 VPN 인스턴스에 대한 상위 수준 HA 아키텍처"를 참조하십시오.

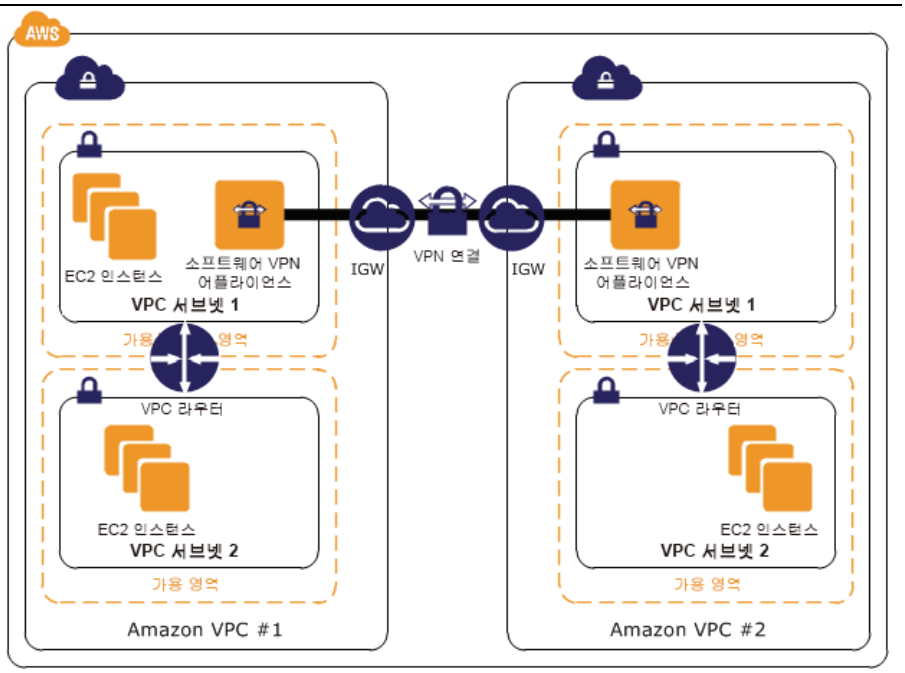

그림 7 - 리전 내 VPC-VPC 라우팅

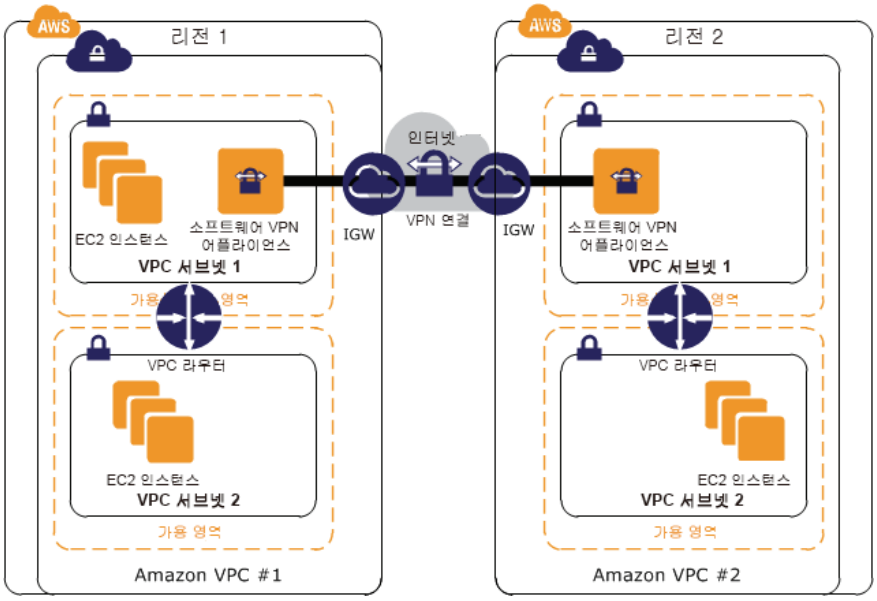

그림 8 - 리전 간 VPC-VPC 라우팅

추가 리소스

- AWS Marketplace의 VPN 어플라이언스
- 문서 - 여러 VPC를 EC2 인스턴스와 연결(IPSec)
- 문서 - 여러 VPC를 EC2 인스턴스와 연결(SSL)

---

[2] "인터넷"을 따옴표로 묶은 이유는 Amazon VPC 가 별도 리전에 있는 경우 인터넷 게이트웨이가 인터넷을 통해 VPN 연결만 라우팅하기 때문입니다(그림 7). 동일한 AWS 리전에 있는 VPC 간에 통신하는 경우 IGW 가 AWS 네트워크를 사용하여 VPC 간에 트래픽을 직접 라우팅합니다(그림 6).

하드웨어-소프트웨어 VPN

Amazon VPC는 고객에게 하드웨어 VPN과 소프트웨어 VPN 옵션을 결합하여 여러 VPC를 상호 연결할 수 있는 유연성을 제공합니다. 이 디자인을 사용하면 고객은 소프트웨어 VPN 어플라이언스와 가상 프라이빗 게이트웨이 사이에 안전한 VPN 터널을 생성하여 여러 VPC를 더 큰 가상 프라이빗 네트워크에 연결할 수 있게 해 주므로, 각 VPC의 인스턴스가 프라이빗 IP 주소를 사용하여 서로 원활하게 접속할 수 있게 됩니다. 이 옵션은 VPN 연결의 VGW 측에 구축된 자동화된 다중 데이터 센터 중복성 및 장애 조치를 포함하여 AWS 관리형 하드웨어 VPN 엔드포인트를 활용하려는 고객이 사용하는 것이 좋습니다. 이 옵션은 그림 9에 나와 있는 것처럼 Amazon VPC의 가상 프라이빗 게이트웨이 하나와 "인터넷" 게이트웨이[3] 및 다른 Amazon VPC의 소프트웨어 VPN 어플라이언스를 결합하여 사용합니다.

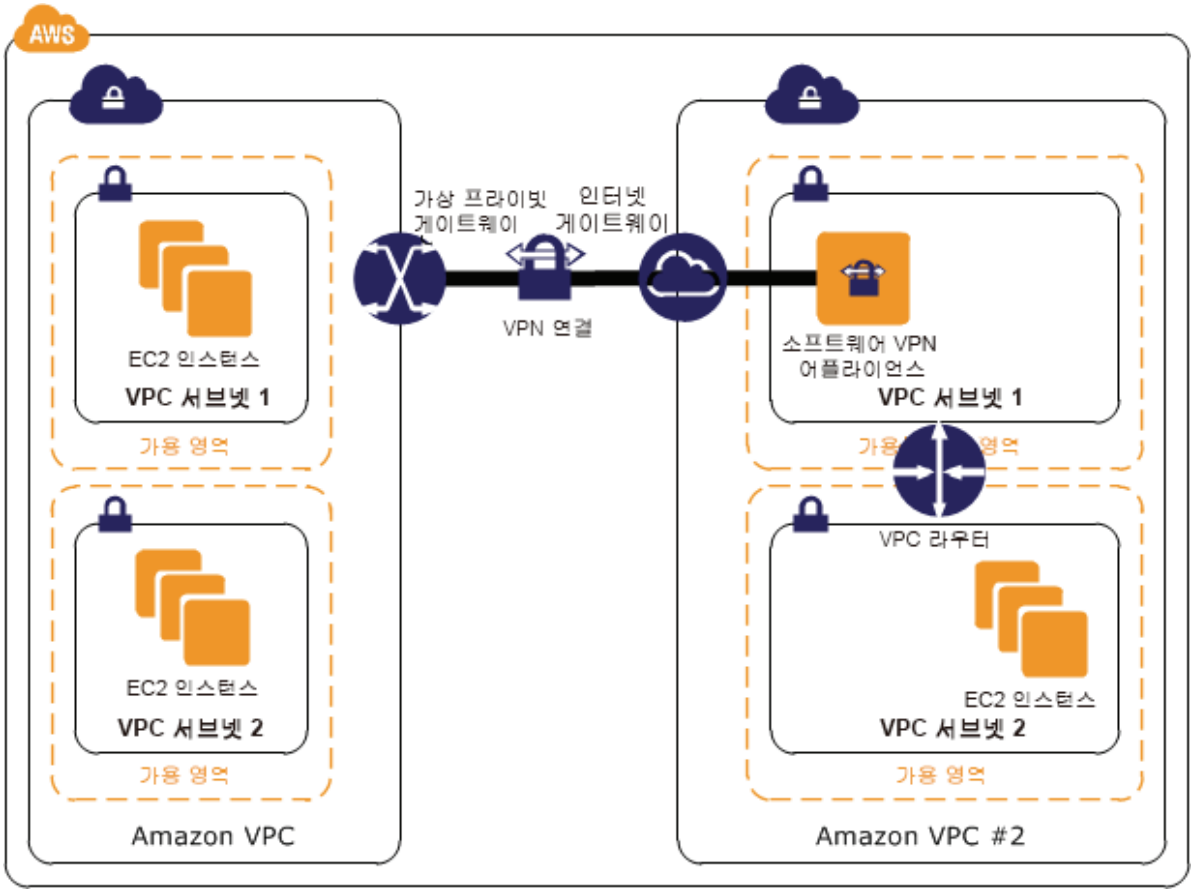

그림 9 - 리전 내 VPC-VPC 라우팅

이 디자인의 경우 ASG 어플라이언스가 단일 Amazon EC2 인스턴스에서 실행되므로 네트워크 디자인으로의 잠재적인 단일 실패 지점이 발생한다는 점에 유의하십시오. 추가 정보는 "부록 A: 소프트웨어 VPN 인스턴스에 대한 상위 수준 HA 아키텍처"를 참조하십시오.

추가 리소스

- 문서 - 여러 VPC를 Astaro 보안 게이트웨이와 연결
- Windows Server 2008 R2를 Amazon Virtual Private Cloud의 고객 게이트웨이로 구성

[3] "인터넷"을 따옴표로 묶은 이유는 Amazon VPC 가 별도 리전에 있는 경우 인터넷 게이트웨이가 인터넷을 통해 VPN 연결만 라우팅하기 때문입니다. 추가 정보는 이전 섹션의 바닥글을 참조하십시오.

하드웨어 VPN

Amazon VPC는 인터넷을 통해 원격 고객 네트워크를 Amazon VPC와 연결할 수 있는 하드웨어 IPsec VPN 생성 옵션을 제공합니다. 그림 10에 나와 있는 것처럼 고객은 여러 하드웨어 VPN 연결을 사용하여 Amazon VPC 간 트래픽을 라우팅할 수 있습니다.

각 VPN 연결의 AWS 측에 구축된 자동화된 다중 데이터 센터 중복성 및 장애 조치를 포함하여 AWS 관리형 VPN 엔드포인트를 활용하려는 고객은 이 접근 방식을 사용하는 것이 좋습니다. 표시되어 있지는 않지만 Amazon VGW는 각각의 VPN 연결 가용성을 확대하기 위해 별도의 데이터 센터에 물리적으로 위치하고 있는 고유 VPN 엔드포인트 두 개를 제공합니다.

Amazon VGW는"고객 네트워크-Amazon VPC 연결 옵션" - 하드웨어 VPN 섹션 및 그림 2에 설명되어 있는 것과 같이 여러 고객 게이트웨이 연결을 지원하므로 고객이 VPN 연결 시 중복성 및 장애 조치를 구현할 수도 있습니다. 또한, 이 솔루션은 BGP 피어링을 이용하여 AWS와 이러한 원격 엔드포인트 간에 라우팅 정보를 교환할 수 있습니다. 고객은 BGP 공급에 라우팅 우선 순위, 정책 및 가중치(측정치)를 지정할 수 있으며 네트워크와 AWS 간의 네트워크 경로 트래픽에 영향을 미칠 수 있습니다.

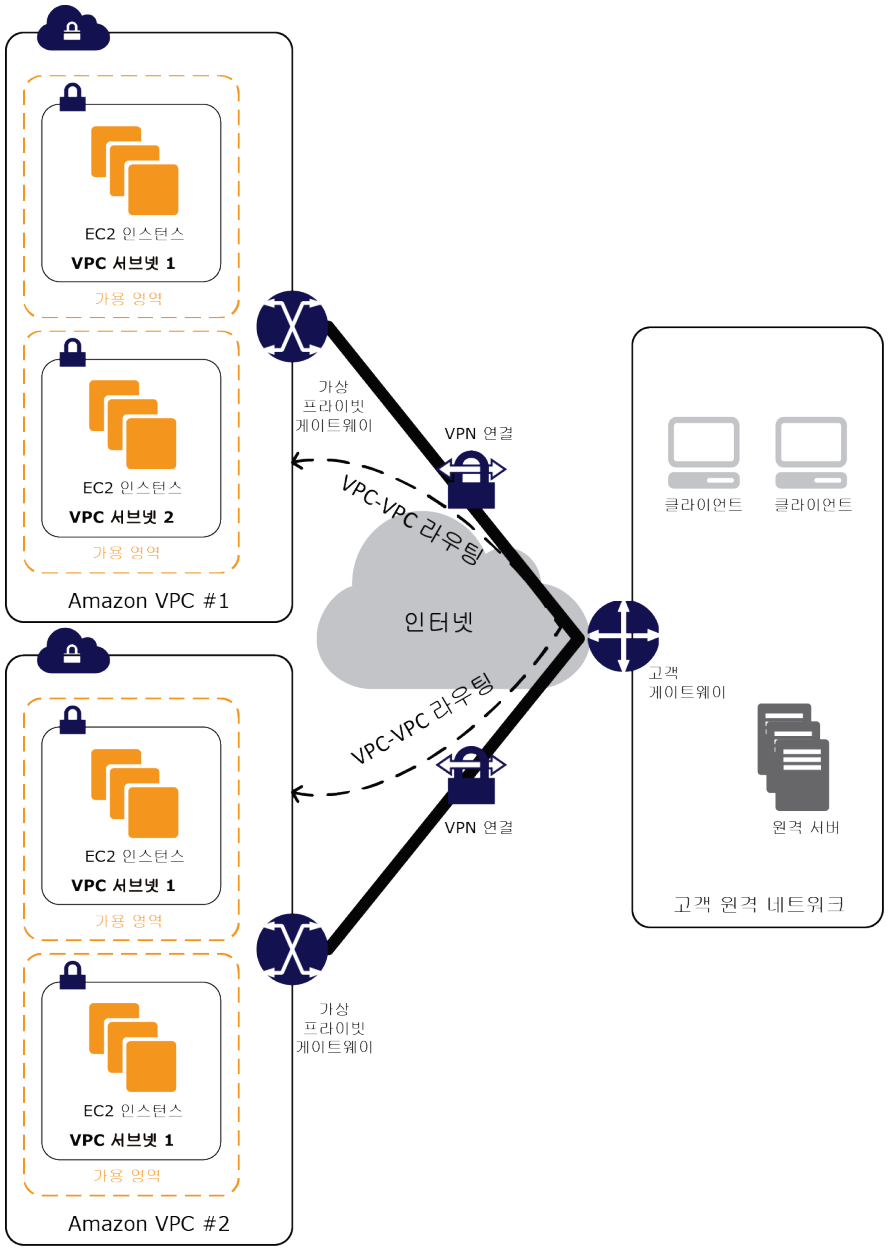

그림 10 – VPC 간 트래픽 라우팅

트래픽이 인터넷을 통과하여 고객 네트워크를 오고 가야 하지만, 로컬 및 원격 네트워크에서 라우팅을 제어하고 관리할 수 있도록 고객에게 많은 유연성을 제공할 뿐 아니라 하드웨어 VPN 연결을 재사용할 수도 있게 해 주기 때문에 이 접근 방식은 라우팅 관점에서 차선책입니다.

추가 리소스

- Amazon VPC 사용 설명서
- 고객 게이트웨이 장치 최소 요구 사항
- Amazon VPC와 작동하는 것으로 알려진 고객 게이트웨이 장치
- 문서 - 여러 VPC에 단일 라우터 연결

AWS Direct Connect

AWS Direct Connect를 사용하면 고객의 자체 환경에서 Amazon VPC로의 전용 네트워크 연결 또는 Amazon VPC 간의 전용 네트워크 연결을 쉽게 설정할 수 있습니다. 이 옵션을 통해 잠재적으로 네트워크 비용을 절감하고 대역폭 처리량을 늘리며, 다른 VPC-VPC 연결 옵션보다 더욱 일관된 네트워크 환경을 제공할 수 있습니다.

물리적 AWS Direct Connect 연결을 각 VPC에 대해 하나씩 여러 논리적 연결로 분할할 수 있습니다. 그림 11에 나와 있는 것처럼 이러한 논리적 연결을 각 VPC 간 트래픽 라우팅에 사용할 수 있습니다. 지역 내 라우팅 외에도 고객이 기존 WAN 공급자를 사용하여 다른 리전에서 AWS Direct Connect 위치를 연결하고, AWS Direct Connect를 활용하여 WAN 백본 네트워크를 통해 리전 간의 트래픽을 라우팅할 수 있습니다.

기존 AWS Direct Connect 고객 또는 AWS Direct Connect의 네트워크 비용 감소, 대역폭 처리량 증가 및 더욱 일관된 네트워크 환경 이점을 활용하고자 하는 고객은 이 접근 방식을 사용하는 것이 좋습니다. 이 접근 방식을 사용하면 트래픽이 각 리전의 AWS 네트워크에 물리적으로 연결된 1GB 또는 10GB 광연결을 이용할 수 있기 때문에 매우 효율적으로 라우팅을 수행할 수 있습니다. 또한, 고객이 로컬 및 원격 네트워크에서 가장 유연하게 라우팅을 제어 및 관리하고, 잠재적으로 AWS Direct Connect 연결을 재사용할 수도 있습니다.

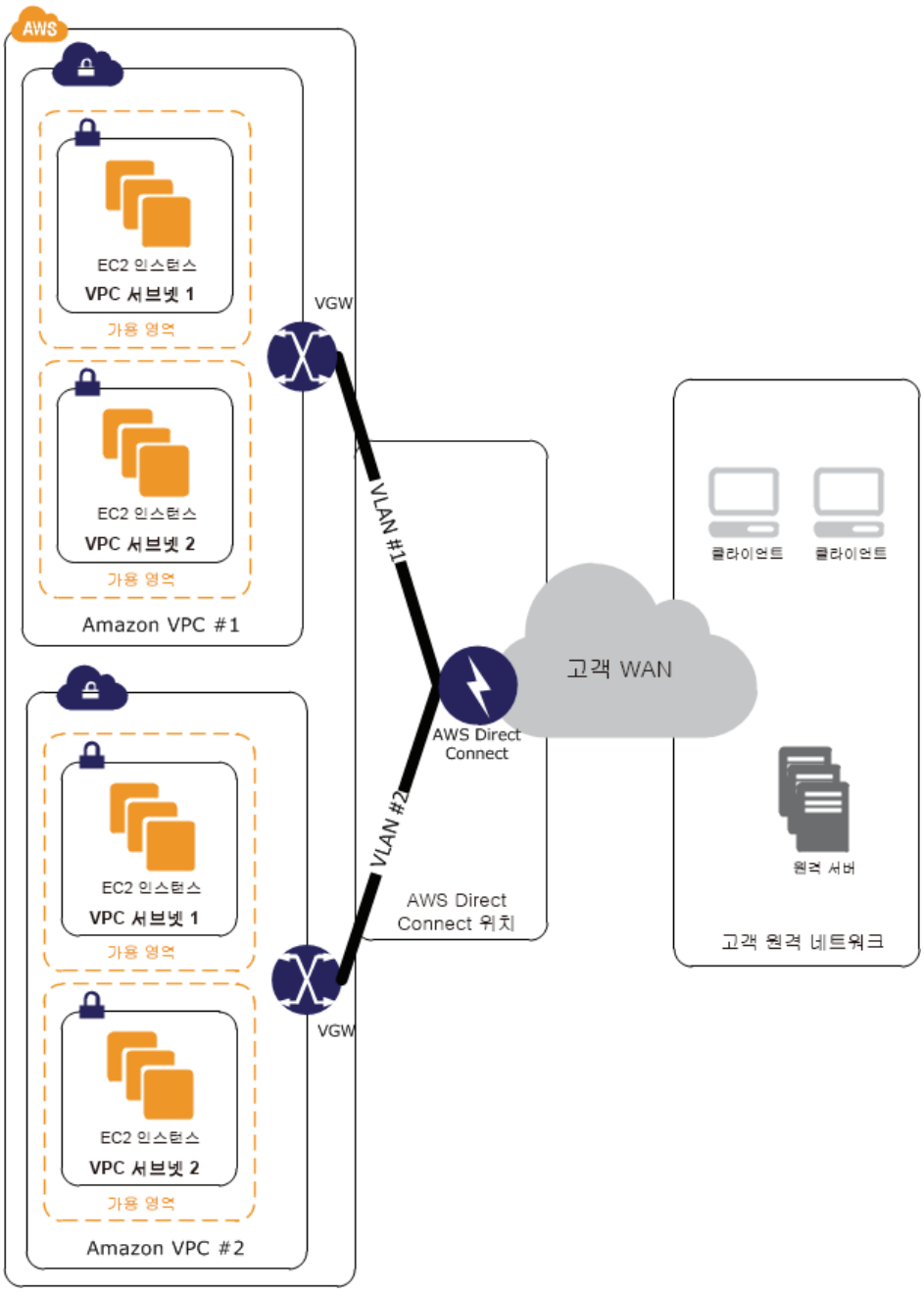

그림 11 – AWS Direct Connect 를 사용하여 리전 내 VPC-VPC 라우팅

추가 리소스

- AWS Direct Connect 제품 페이지
- AWS Direct Connect 위치
- AWS Direct Connect FAQ
- AWS Direct Connect 시작하기

내부 사용자-Amazon VPC 연결 옵션

내부 사용자는 일반적으로 고객 네트워크-Amazon VPC 연결 옵션을 통하거나 내부 사용자를 VPC 리소스에 연결하기 위한 소프트웨어 원격 액세스 VPN을 사용하여 Amazon VPC 리소스에 액세스할 수 있습니다. 첫 번째 옵션을 사용하면 고객이 최종 사용자 액세스 관리에 기존 온프레미스 및 원격 액세스 솔루션을 재사용할 수 있으며, AWS에서 호스트하는 리소스에 원활하게 연결할 수 있는 환경이 제공됩니다. 이 문서에서는 온프레미스 내부 및 원격 액세스 솔루션에 대해 "고객 네트워크-Amazon VPC 연결 옵션" 섹션에 설명되어 있는 내용보다 더 자세히 설명하지 않습니다.

소프트웨어 원격 액세스 VPN 접근 방식을 사용하면 고객이 비용이 저렴하고 탄력적이며 안전한 Amazon Web Services를 사용하여 원격 액세스 솔루션을 구현할 수 있으며, AWS에서 호스트하는 리소스에 원활하게 연결할 수 있는 환경도 제공됩니다. 또한, 소프트웨어 원격 액세스 VPN을 고객 네트워크-Amazon VPC 옵션과 결합하여 원하는 경우 내부 네트워크에 대한 원격 액세스를 제공할 수 있습니다. 이 옵션은 일반적으로 덜 광범위한 원격 네트워크를 갖춘 더 작은 규모의 회사에서 주로 사용하거나, 직원이 사용할 수 있는 원격 액세스 솔루션을 이미 구축 및 배포하지 않은 사용자가 주로 사용합니다.

다음 표에는 이러한 옵션과 관련된 장점 및 제한 사항이 요약되어 있습니다.

옵션	사용 사례	장점	제한
고객 네트워크-Amazon VPC 옵션	고객의 데이터 센터를 AWS로 가상 확장	• 기존 최종 사용자 내부, 원격 액세스 정책 및 기술을 활용합니다.	• 기존 최종 사용자 내부 및 원격 액세스를 구현해야 합니다.
소프트웨어 원격 액세스 VPN	Amazon VPC 및/또는 내부 네트워크에 대한 클라우드 기반 원격 액세스 솔루션	• 원격 액세스 솔루션 구현을 위해 AWS에서 제공하는 비용이 저렴하고 탄력적이며 안전한 웹 서비스를 활용합니다.	• 내부 및 원격 액세스가 이미 구현되어 있는 경우 중복될 수 있습니다.

소프트웨어 원격 액세스 VPN

AWS 고객은 Amazon EC2에서 실행되는 원격 액세스 솔루션을 만든 여러 파트너와 오픈 소스 커뮤니티의 에코시스템에서 선택할 수 있습니다. 여기에는 Checkpoint, Sophos, OpenVPN Technologies 및 Microsoft와 같이 잘 알려진 보안 회사의 제품이 포함됩니다. 그림 12에는 내부 원격 사용자 데이터베이스를 활용하는 단순 원격 액세스 솔루션이 나와 있습니다.

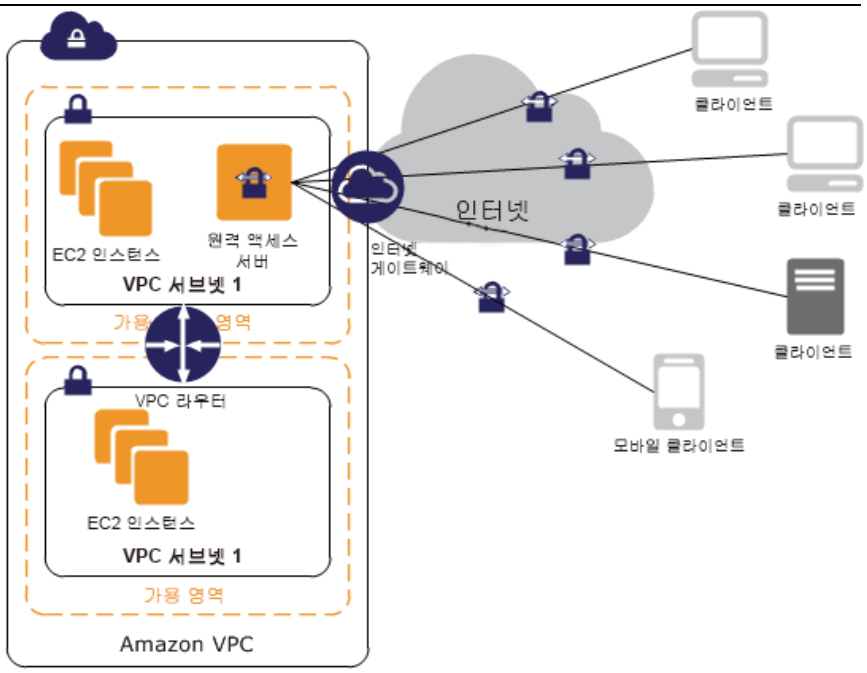

그림 12 – 원격 액세스 솔루션

복잡한 원격 액세스 솔루션 범위는 여러 클라이언트 인증 옵션(멀티 팩터 인증 포함)을 지원하며 Amazon VPC 또는 Microsoft Active Directory 혹은 기타 LDAP/멀티 팩터 인증 솔루션과 같이 원격으로 호스트되는 Identity and Access Management 솔루션(고객 네트워크-Amazon VPC 연결 옵션 중 하나 사용)으로 통합할 수 있습니다. 그림 13에는 원하는 경우 원격 액세스 서버가 내부 액세스 관리 솔루션을 사용하도록 허용할 수 있는 이 결합이 나와 있습니다.

VPN 옵션을 사용하면 고객이 사용자 관리, 구성, 패치 및 업그레이드를 포함하여 원격 액세스 소프트웨어를 관리해야 합니다. 또한, 이 디자인의 경우 원격 액세스 서버가 단일 Amazon EC2 인스턴스에서 실행되므로 네트워크 디자인으로의 잠재적인 단일 실패 지점이 발생한다는 점에 유의하십시오. 추가 정보는 “부록 A: 소프트웨어 VPN 인스턴스에 대한 상위 수준 HA 아키텍처”를 참조하십시오.

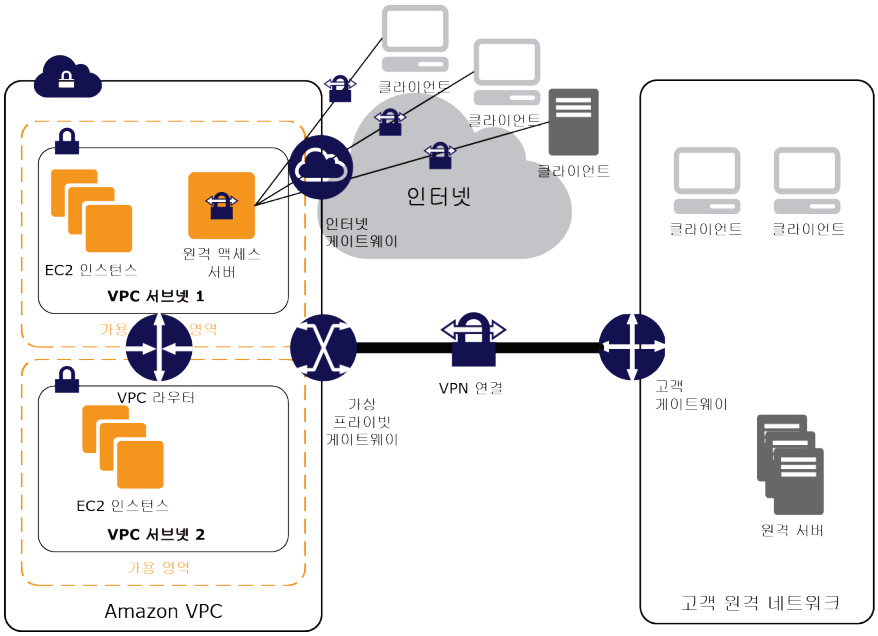

그림 13 – 결합 원격 액세스 솔루션

추가 리소스

- AWS Marketplace의 VPN 어플라이언스
- OpenVPN 액세스 서버 빠른 사용 설명서

결론

AWS는 고객이 원격 네트워크를 Amazon VPC와 통합할 때 AWS를 최대한 활용할 수 있도록 효율적이고 안전한 연결 옵션을 다양하게 제공합니다. 이 백서에 나와 있는 옵션은 고객이 원격 네트워크 또는 여러 Amazon VPC 네트워크를 성공적으로 통합하는 데 사용해 온 연결 옵션 및 패턴 몇 가지를 강조해서 설명합니다. 이러한 옵션을 통해 물리적으로 존재하거나 호스트되는 위치와 관계없이 기업 운영에 필요한 인프라에 연결할 수 있는 가장 적절한 메커니즘을 효율적으로 결정할 수 있기를 바랍니다.

부록 A: 소프트웨어 VPN 인스턴스에 대한 상위 수준 HA 아키텍처

소프트웨어 VPN 인스턴스의 탄력적인 VPC 연결을 만들려면 VPN 연결 상태를 모니터할 수 있는 모니터링 인스턴스 및 여러 VPN 인스턴스를 설정하고 구성해야 합니다.

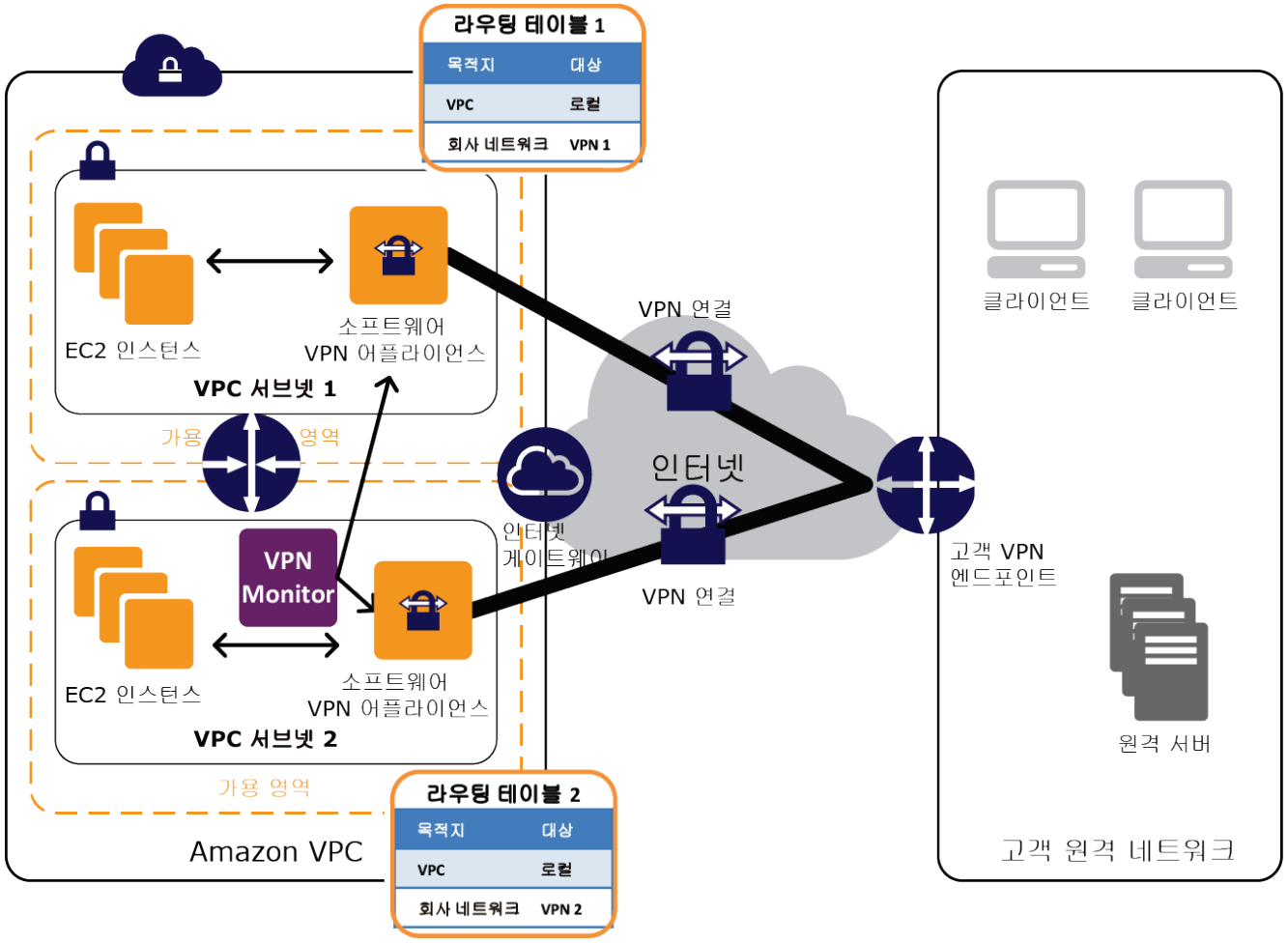

그림 14 – 상위 수준 HA 디자인

동일한 가용 영역에 있는 각각의 VPN 인스턴스를 통해 가용 영역 하나의 모든 서브넷 트래픽을 전달하여 모든 VPN 인스턴스를 동시에 활용하도록 VPC 라우팅 테이블을 구성하는 것이 좋습니다. 그러면 각 VPN 인스턴스가 동일한 가용 영역을 공유하는 인스턴스에 대한 VPN 연결을 제공합니다.

VPN 모니터링 인스턴스

VPN 모니터는 실행되는 모니터링 스크립트를 생성하고 개발해야 하는 사용자 지정 인스턴스입니다. 이 인스턴스는 VPN 연결 및 VPN 인스턴스 상태를 실행하고 모니터하도록 마련되었습니다. VPN 인스턴스 또는 연결이 작동 중지되면 모니터는 VPN을 정지, 종료하거나 다시 시작해야 하며, 모든 연결이 다시 작동될 때까지 영향을 받는 서브넷의 트래픽을 작동하는 VPN 인스턴스로 다시 라우팅해야 합니다. 고객 요구 사항이 다양하기 때문에 AWS는 현재 이 모니터링 인스턴스를 설정하는 데 사용할 수 있는 설명서 또는 스크립트를 제공하지 않습니다. 알림을 제공하고 VPN 연결 오류가 발생하는 경우 자동으로 네트워크 연결을 복구할 수 있도록 필요한 비즈니스 로직을 충분히 생각해 보십시오.