AWS 백서

하이브리드 연결

하이브리드 연결: AWS 백서

Table of Contents

하이브리드 연결

발행일: 2023년 7월 6일(문서 수정)

많은 조직에서 온프레미스 데이터 센터, 원격 사이트, 클라우드를 연결해야 합니다. 하이브리드 네트워크는 이러한 다양한 환경을 연결합니다. 이 백서는 적합한 하이브리드 연결 모델을 결정할 때 고려해야 할 AWS 구성 요소와 주요 요구 사항을 설명합니다. 비즈니스 및 기술 요구 사항에 가장 적합한 솔루션을 결정하는 데 도움이 되도록 논리적 선택 프로세스를 안내하는 의사 결정 트리를 제공합니다.

소개

현대 조직은 광범위한 IT 리소스를 사용합니다. 과거에는 이러한 리소스를 온프레미스 데이터 센터나 콜로케이션 시설에서 호스팅하는 것이 일반적이었습니다. 클라우드 컴퓨팅 채택이 증가함에 따라 조직은 네트워크 연결을 통해 클라우드 서비스 공급자로부터 IT 리소스를 제공하고 소비합니다. 조직은 기존 IT 리소스의 일부 또는 전체를 클라우드로 마이그레이션할 수 있습니다. 어느 경우든 온프레미스와 클라우드 리소스를 연결하려면 공통 네트워크가 필요합니다. 온프레미스와 클라우드 리소스가 공존하는 것을 하이브리드 클라우드라고 하고, 이들을 연결하는 공용 네트워크를 하이브리드 네트워크라고 합니다. 조직이 모든 IT 리소스를 클라우드에 보관하더라도 원격 사이트에 대한 하이브리드 연결이 필요할 수 있습니다.

여러 연결 모델 중에서 선택할 수 있습니다. 옵션이 있으면 유연성이 향상되지만 최적의 옵션을 선택하려면 비즈니스 및 기술 요구 사항을 분석하고 적합하지 않은 옵션을 제거해야 합니다. 보안, 배포 시간, 성능, 신뢰성, 통신 모델, 확장성 등과 같은 고려 사항을 기준으로 요구 사항을 그룹화할 수 있습니다. 요구 사항을 신중하게 수집, 분석 및 고려한 후에는 네트워크 및 클라우드 설계자가 적용 가능한 AWS 하이브리드 네트워크 구성 요소 및 솔루션을 식별할 수 있습니다. 최적의 모델을 식별하고 선택하려면 설계자가 각 모델의 장단점을 이해해야 합니다. 또한 기술적인 한계로 인해 다른 적합한 모델이 제외될 수 있습니다.

선택 프로세스를 단순화하기 위해 이 백서는 각 주요 고려 사항을 논리적인 순서로 안내합니다. 각 고려 사항에는 요구 사항을 수집하는 데 사용되는 질문이 있습니다. 잠재적 솔루션과 함께 각 설계 결정의 영향을 식별합니다. 이 백서는 의사 결정 프로세스를 지원하고 옵션을 제거하며 각 결정의 결과를 이해하는 방법으로 일부 고려 사항에 대한 의사 결정 트리를 제시합니다. 종단 간 연결 모델 선택 및 설계를 적용하여 하이브리드 사용 사례를 다루는 시나리오로 결론을 맺습니다. 이 예시를 사용하여 실제 예시에서 이 백서에 설명된 프로세스를 실행하는 방법을 확인할 수 있습니다.

이 백서는 최적의 하이브리드 연결 모델을 선택하고 설계하는 데 도움을 주기 위한 것입니다. 이 백서의 구조는 다음과 같습니다.

- 하이브리드 연결 구성 요소 - 하이브리드 연결에 사용되는 AWS 서비스에 대한 개요입니다.
- 연결 선택 및 설계 고려 사항 - 각 연결성 모델의 정의, 각 모델이 설계 결정에 미치는 영향, 요구 사항 식별 질문, 솔루션 및 의사 결정 트리에 대한 설명입니다.
- 고객 사용 사례 - 고려 사항 및 의사 결정 트리를 실제로 적용하는 방법에 대한 예시입니다.

귀사는 Well-Architected입니까?

AWS Well-Architected 프레임워크는 클라우드에서 시스템을 구축할 때 내리는 결정의 장단점을 이해하는 데 도움이 됩니다. 이 프레임워크를 사용하여 클라우드에서 안정적이고 안전하며 효율적이고 비용 효율적인 시스템을 설계하고 운영하기 위한 아키텍처 모범 사례를 살펴볼 수 있습니다. AWS Management Console에서 무료로 제공되는 AWS Well-Architected Tool을 사용하면 각 요소에 대한 일련의 질문에 답하여 모범 사례와 비교하여 워크로드를 검토할 수 있습니다.

참조 아키텍처 배포, 다이어그램, 백서 등 클라우드 아키텍처에 대한 더 많은 전문가 지침과 모범 사례를 보려면 AWS 아키텍처 센터를 참조하세요.

AWS 하이브리드 연결 구성 요소

하이브리드 네트워크 연결 아키텍처에는 세 가지 구성 요소가 있습니다.

- 하이브리드 네트워크 연결: AWS 연결 서비스와 온프레미스 고객 게이트웨이 디바이스 간의 연결 유형입니다.
- AWS 하이브리드 연결 서비스: 고객 인프라와 AWS 사이의 연결과 라우팅을 제공하는 AWS 서비스입니다.
- 온프레미스 고객 게이트웨이 디바이스: 고객의 기존 네트워크 내에 있는 디바이스로, 하이브리드 네트워크 연결을 위한 온프레미스 엔드포인트입니다. 연결 유형마다 이러한 디바이스에 대한 기술적 요구 사항이 다릅니다. 이에 대해서는 다음 섹션에서 설명하겠습니다.

하이브리드 네트워크 연결

온프레미스 장비와 AWS를 연결하는 방법에는 여러 가지가 있습니다. 이 백서는 이러한 다양한 방법을 전체 아키텍처에 결합하는 방법에 초점을 맞추고 있지만, 다양한 옵션(AWS Direct Connect, Site-to-Site VPN, Transit Gateway Connect)에 대한 간략한 개요를 제공합니다.

AWS Direct Connect

AWS Direct Connect는 구내에서 AWS로 전용 네트워크 연결을 설정하는 서비스입니다. 자세한 내용은 AWS Direct Connect를 참조하세요.

AWS Direct Connect 연결에는 전용 연결과 호스팅 연결의 두 가지 유형이 있습니다. 전용 연결은 AWS 디바이스와 온프레미스 디바이스 간의 직접 연결인 반면, 호스팅 연결은 연결 세부 정보를 처리할 수 있는 AWS 파트너가 지원합니다. 자세한 내용은 AWS Direct Connect 연결을 참조하세요.

Direct Connect 링크는 가상 인터페이스(VIF)를 사용하여 다양한 트래픽 흐름을 분리합니다. 여러 VIF가 동일한 Direct Connect 링크를 사용할 수 있으며, VLAN(802.1q) 태그로 구분할 수 있습니다. AWS 네트워크 연결을 제공하는 VIF에는 세 가지 유형이 있습니다. 자세한 내용은 AWS Direct Connect 가상 인터페이스를 참조하세요. 세 가지 유형은 다음과 같습니다.

- 프라이빗 VIF: 프라이빗 VIF는 디바이스와 AWS 내부 리소스 간의 프라이빗 연결입니다. 이는 AWS 내부의 가상 프라이빗 게이트웨이(VGW)에서 직접(단일 VPC를 지원) 또는 Direct Connect 게이트웨이를 통해 여러 VGW에 연결되는 방식으로 종료됩니다.
- 퍼블릭 VIF: 퍼블릭 VIF를 사용하면 S3, DynamoDB, 퍼블릭 EC2 IP 범위와 같은 모든 퍼블릭 AWS 리소스에 연결할 수 있습니다. 퍼블릭 VIF는 인터넷에 직접 액세스할 수 없지만 다른 고객의 퍼블릭

EC2 인스턴스를 포함한 모든 Amazon 퍼블릭 리소스에 연결할 수 있으므로 고객은 보안 계획 시 이를 고려해야 합니다.

- 전송 VIF: 전송 VIF는 Direct Connect 게이트웨이를 통한 디바이스와 AWS Transit Gateway 사이의 프라이빗 연결입니다. 이제 전송 VIF는 속도가 1Gbps 미만인 링크에서 지원됩니다. 자세한 내용은 출시 발표를 참조하세요.

> **Note**
>
> 호스팅 가상 인터페이스(호스팅 VIF)는 프라이빗 VIF의 한 유형으로, VIF가 AWS Direct Connect 연결을 소유한 AWS 계정가 아닌 다른 AWS 계정에 할당됩니다(AWS Direct Connect 파트너를 포함할 수 있음). AWS는 더 이상 신규 파트너가 이 모델을 제공하는 것을 허용하지 않습니다. 자세한 내용은 Creating a hosted virtual interface를 참조하세요.

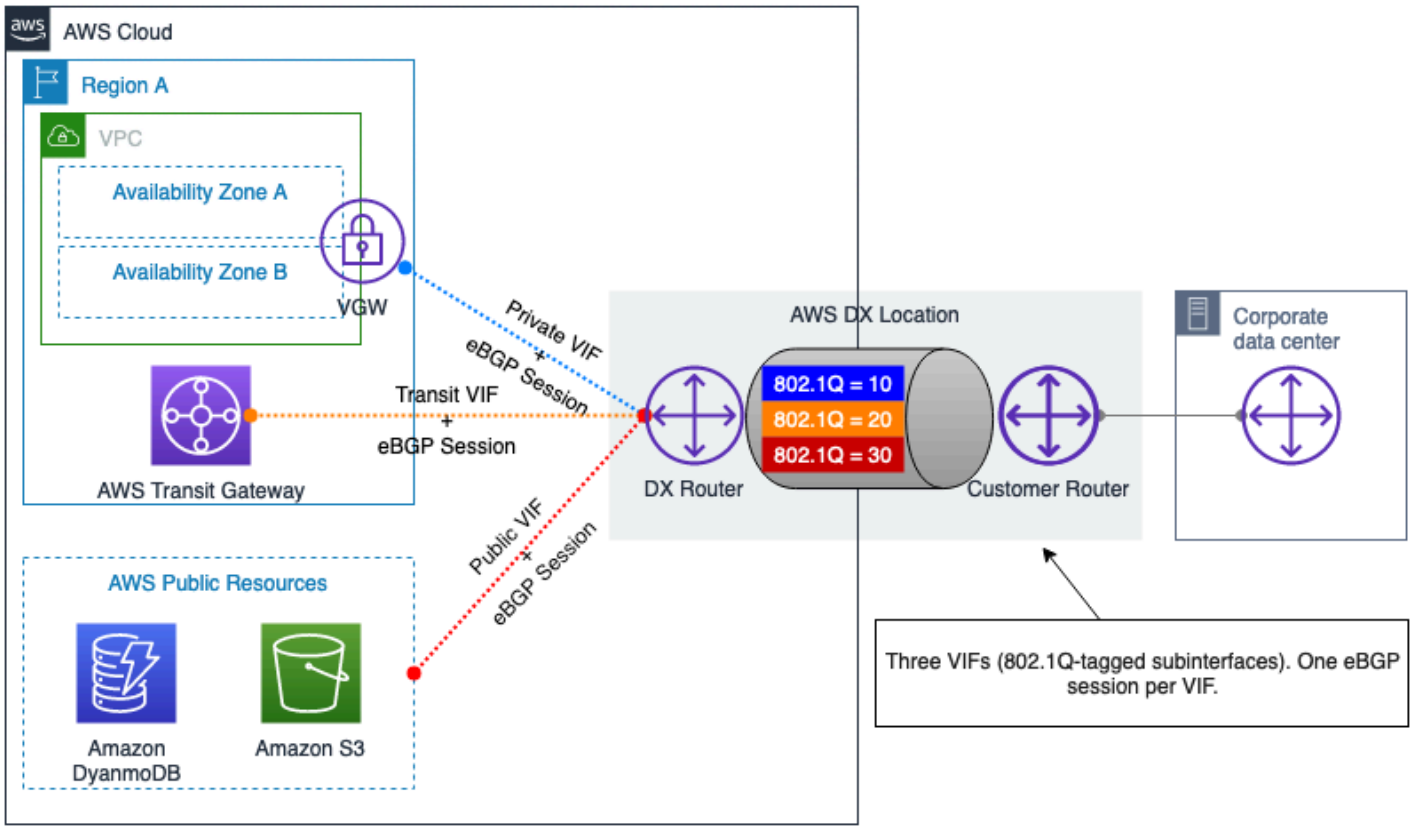

그림 1 - AWS Direct Connect 프라이빗 및 퍼블릭 VIF

Site-to-Site 가상 프라이빗 네트워크(VPN)

Site-to-Site VPN을 사용하면 두 네트워크가 안전하게 통신할 수 있으며 인터넷과 같은 신뢰할 수 없는 전송을 통해 사용할 수 있습니다. 고객은 다음 두 가지 옵션을 통해 온프레미스 사이트와 Amazon Virtual Private Cloud(Amazon VPC) 간에 VPN 연결을 설정할 수 있습니다.

- AWS 관리형 Site-to-Site VPN(AWS S2S VPN): IPsec을 사용하는 완전 관리형 고가용성 VPN 서비스입니다. 자세한 내용은 AWS Site-to-Site VPN란 무엇인가요?를 참조하세요. 선택적으로 Site-to-Site VPN 연결에 가속을 활성화할 수 있습니다. 자세한 내용은 Accelerated Site-to-Site VPN 연결을 참조하세요. 또한 S2S VPN은 Direct Connect 전송 VIF를 사용하여 트래픽이 인터넷을 통과하지 않도록 하여 비용을 절감하고 프라이빗 IP 주소를 사용할 수 있습니다. 자세한 내용은 AWS Direct Connect를 통한 프라이빗 IP VPN을 참조하세요.
- 소프트웨어 Site-to-Site VPN(고객 관리형 VPN): 이 VPN 연결 옵션을 사용하면 일반적으로 EC2 인스턴스에서 VPN 소프트웨어를 실행하여 전체 VPN 솔루션을 프로비저닝하고 관리할 책임이 있습니다. 자세한 내용은 소프트웨어 Site-to-Site VPN을 참조하세요.

두 옵션 모두 온프레미스 VPN 터널을 종료하려면 고객 게이트웨이 디바이스에 대한 지원이 필요합니다. 이 디바이스는 물리적 디바이스일 수도 있고 소프트웨어 어플라이언스일 수도 있습니다. AWS에서 테스트한 네트워크 디바이스에 대한 자세한 내용은 고객 게이트웨이 디바이스 목록을 참조하세요.

Transit Gateway Connect(TGW Connect)

Transit Gateway Connect는 AWS Transit Gateway와 온프레미스 게이트웨이 디바이스 사이에 GRE 터널을 사용합니다. BGP는 동적 라우팅을 활성화하기 위해 TGW Connect 위에 사용됩니다. TGW Connect는 암호화되지 않았습니다. 자세한 내용은 Transit Gateway Connect를 참조하세요.

AWS 하이브리드 연결 서비스

AWS 하이브리드 연결 서비스는 확장성과 가용성이 뛰어난 네트워킹 구성 요소를 제공합니다. 이러한 구성 요소는 하이브리드 네트워킹 솔루션 구축에 필수적인 역할을 합니다. 본 백서 작성 시점에는 다음과 같은 세 가지 주요 서비스 엔드포인트가 있습니다.

- AWS 가상 프라이빗 게이트웨이(VGW)는 VPC 수준에서 IP 라우팅 및 전달을 제공하는 고도로 다중화된 리전별 서비스로서, VPC가 고객 게이트웨이 디바이스와 통신하기 위한 게이트웨이 역할을 합니다. VGW는 AWS S2S VPN 연결 및 AWS Direct Connect 프라이빗 VIF를 종료할 수 있습니다.
- AWS Transit Gateway(TGW)는 단일 중앙 집중식 게이트웨이를 사용하여 Site-to-Site VPN 및/또는 Direct Connect를 통해 여러 VPC를 서로 연결하고 온프레미스 네트워크를 연결할 수 있는 가용

성이 뛰어나고 확장 가능한 리전별 서비스입니다. 개념적으로 AWS Transit Gateway는 고가용성의 다중화 가상 클라우드 라우터 역할을 합니다. AWS Transit Gateway는 여러 Direct Connect 연결, VPN 터널 또는 TGW Connect 피어를 통한 등가 다중 경로(ECMP) 라우팅을 지원합니다. Transit Gateway는 같은 리전과 다른 리전 모두에서 서로 피어링할 수 있으며, 연결된 리소스가 피어링 링크를 통해 통신할 수 있습니다. 자세한 내용은 AWS Transit Gateway 시나리오를 참조하세요.

- AWS 클라우드 WAN은 지사, 데이터 센터, Amazon VPC를 연결할 수 있는 중앙 대시보드를 제공하여 클릭 몇 번으로 글로벌 네트워크를 구축할 수 있습니다. 네트워크 정책을 사용하여 한 위치에서 네트워크 관리 및 보안 작업을 자동화할 수 있습니다. 자세한 내용은 AWS 클라우드 WAN 설명서를 참조하세요.
- Direct Connect Gateway(DXGW)는 연결 전반에 걸쳐 라우팅 정보를 배포하는 전 세계적으로 사용 가능한 서비스로, 기존 네트워크의 BGP 경로 리플렉터와 유사하게 작동합니다. 데이터는 DXGW를 통과하지 않고 라우팅 정보만 처리합니다. 모든 AWS 리전에서 DXGW를 생성하고 다른 모든 AWS 리전에서 액세스할 수 있습니다. Direct Connect VIF를 DXGW에 연결한 다음, DXGW를 VGW(프라이빗 VIF 사용) 또는 AWS Transit Gateway(전송 VIF 사용)와 연결할 수 있습니다. 자세한 정보는 Direct Connect 게이트웨이를 참조하세요. 전 세계적으로 이용 가능한 서비스이므로 이중화를 위해 여러 개의 DXGW를 만들 필요가 없습니다. 그러나 완전히 격리된 상태로 유지하려는 프로덕션 네트워크와 테스트 네트워크와 같이 라우팅 도메인을 분리하기 위해 여러 DXGW를 사용할 수도 있습니다.

하이브리드 연결 유형 및 설계 고려 사항

백서의 이 섹션에서는 온프레미스 환경을 AWS에 연결하기 위해 하이브리드 네트워크를 선택할 때 선택에 영향을 미치는 고려 사항을 다룹니다. 논리적 사고 프로세스를 따라 최적의 하이브리드 연결 솔루션을 선택할 수 있도록 지원합니다. 설계에 영향을 미치는 고려 사항은 연결 유형에 영향을 미치는 고려 사항과 연결 설계에 영향을 미치는 고려 사항으로 분류됩니다. 연결 유형 고려 사항은 인터넷 기반 VPN 또는 Direct Connect를 사용할지 결정하는 데 도움이 됩니다. 연결 설계 고려 사항은 연결 설정 방법을 결정하는 데 도움이 됩니다.

연결 유형에 영향을 미치는 고려 사항에는 확장성, 통신 모델, 신뢰성, 타사 SD-WAN 통합 등이 있습니다. 이러한 고려 사항과 이러한 고려 사항이 설계 선택에 미치는 영향을 검토한 후 요구 사항을 충족하기 위해 인터넷 기반 연결을 사용하는 것이 좋은지 Direct Connect를 사용하는 것이 좋은지 결정할 수 있습니다.

연결 설계에 영향을 미치는 고려 사항에는 확장성, 통신 모델, 신뢰성, 타사 SD-WAN 통합 등이 있습니다. 이러한 고려 사항과 이것이 디자인 선택에 어떤 영향을 미치는지 검토한 후 요구 사항을 충족하는 데 권장되는 최적의 논리적 디자인을 결정할 수 있습니다.

다음 구조는 각 선택 및 설계 고려 사항을 논의하고 분석하는 데 사용됩니다.

- 정의 - 고려 사항에 대한 간략한 정의입니다.
- 핵심 질문 - 고려 사항과 관련된 요구 사항을 수집할 수 있는 일련의 질문을 제공합니다.
- 고려해야 할 기능 - 고려 사항과 관련된 요구 사항을 해결하는 솔루션입니다.
- 의사 결정 트리 - 일부 고려 사항 또는 고려 사항 그룹의 경우 최적의 하이브리드 네트워크 솔루션을 선택하는 데 도움이 되는 의사 결정 트리가 제공됩니다.

하이브리드 네트워크 설계에 영향을 미치는 고려 사항은 한 가지 고려 사항의 결과가 후속 고려 사항의 입력에 포함되는 순서대로 다루어집니다. 그림 2에서 볼 수 있듯이 첫 번째 단계는 연결 유형을 결정한 다음 설계 선택 고려 사항을 적용하여 연결 유형을 구체화하는 것입니다.

그림 2는 두 가지 고려 사항 범주, 개별 고려 사항과 후속 하위 섹션에서 고려 사항을 다루는 논리적 순서를 보여줍니다. 이는 하이브리드 네트워크 설계 결정을 내릴 때 반드시 고려해야 할 사항입니다. 대상 설계에 이러한 모든 고려 사항이 필요하지 않은 경우 요구 사항에 적용되는 고려 사항에 집중할 수 있습니다.

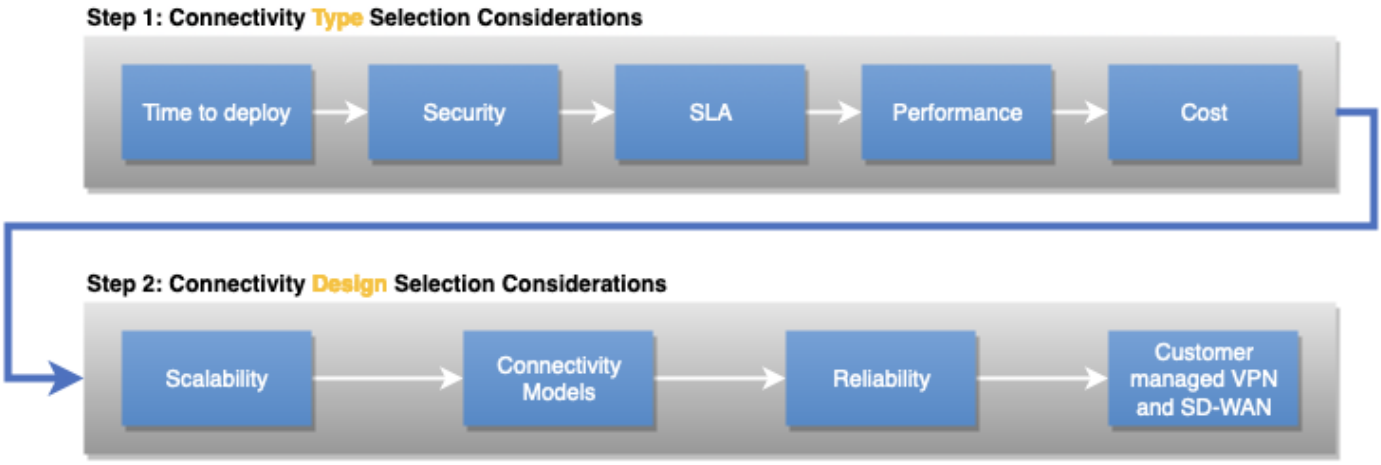

그림 2 - 고려 사항 범주, 개별 고려 사항, 고려 사항 간의 논리적 순서

연결 유형 선택

이 섹션에서는 워크로드에 대해 선택한 연결 유형에 영향을 미치는 고려 사항을 다룹니다. 여기에는 배포 시간, 보안, SLA, 성능 및 비용이 포함됩니다.

고려 사항

- 배포 시간
- 보안
- 서비스 수준에 관한 계약(SLA)
- 성능
- 비용

배포 시간

정의

배포 시간은 워크로드에 적합한 연결 유형을 선택하는 데 중요한 요소가 될 수 있습니다. 연결 유형과 온프레미스 위치에 따라 몇 시간 내에 연결을 설정할 수 있지만 추가 회로를 설치해야 하는 경우 몇 주 또는 몇 달이 걸릴 수 있습니다. 이는 인터넷 기반 연결, 프라이빗 전용 연결 또는 AWS Direct Connect 파트너가 관리 서비스로 제공하는 프라이빗 호스팅 연결을 사용할지 결정하는 데 영향을 미칩니다.

핵심 질문

- 배포에 필요한 타임라인이 어떻게 됩니까? 몇 시간, 며칠, 몇 주 또는 몇 달입니까?
- 연결이 얼마나 오래 필요합니까? 수명이 짧은 프로젝트입니까, 아니면 영구적인 인프라입니까?

고려해야 할 기능

몇 시간 또는 며칠 내에 AWS 연결이 필요한 경우 대부분 기존 네트워크 연결을 사용해야 합니다. 이는 종종 공용 인터넷을 통해 AWS에 대한 VPN 연결을 설정하는 것을 의미합니다. 기존 AWS DX 파트너가 프라이빗 AWS 연결을 제공하는 경우 몇 시간 내에 호스팅된 새 연결을 프로비저닝할 수 있습니다.

며칠에서 몇 주가 걸린다면 AWS Direct Connect 파트너와 협력하여 AWS에 대한 프라이빗 연결을 설정할 수 있습니다. AWS Direct Connect 파트너는 AWS Direct Connect 위치와 데이터 센터, 사무실 또는 콜로케이션 환경 간의 네트워크 연결을 설정하는 데 도움을 줍니다. 일부 AWS Direct Connect파트너는 Direct Connect 호스팅 연결을 제공하도록 승인되었습니다. 호스팅된 연결은 종종 전용 연결보다 더 빠르게 프로비저닝될 수 있습니다. AWS Direct Connect 파트너는 AWS 백본에 연결된 기존 인프라를 사용하여 각 호스팅 연결을 프로비저닝합니다.

몇 주에서 몇 달이 있다면 AWS와의 전용 프라이빗 연결을 설정하는 방안을 검토해 볼 수 있습니다. 서비스 제공업체 및 AWS Direct Connect 파트너는 AWS Direct Connect 전용 연결을 지원합니다. 서비스 공급업체는 Direct Connect 전용 연결을 용이하게 하기 위해 고객의 구내에 네트워킹 장비를 설치하는 것이 일반적입니다. 서비스 제공업체, 사이트 위치 및 기타 물리적 요인에 따라 Direct Connect 전용 연결 설치에는 몇 주에서 몇 개월까지 걸릴 수 있습니다.

위치가 있는 동일한 콜로케이션 시설에 네트워크 장비를 이미 설치한 경우 AWS Direct Connect 코로케이션 사이트에서 교차 연결을 통해 AWS Direct Connect 전용 연결을 신속하게 설정할 수 있습니다. 연결을 요청한 후 AWS는 다운로드할 수 있는 Letter of Authorization and Connecting Facility Assignment(LOA-CFA)를 제공하거나 추가 정보를 요청하는 이메일을 보냅니다. LOA-CFA는 AWS 연결에 대한 승인이며, 네트워크 공급자가 사용자 대신 교차 연결을 주문하는 데 필요합니다.

표 1 - 비용 효율성 비교

	인터넷 기반 연결	DX 전용 연결 (DX 위치 내 기존 장비)	DX 전용 연결 (네트워크 신규)	DX 호스팅 연결(DX 파트너의 기존 포트)	DX 호스팅 연결(네트워크 신규)
프로비저닝 시간	몇 시간에서 며칠까지	일	몇 주에서 몇 달까지	몇 시간에서 며칠까지	며칠에서 몇 주, 몇 달

> **Note**
>
> 제공된 제공 시간 지침은 실제 관찰을 기반으로 하며 예시용으로만 제공됩니다. 사이트 위치, 직접 연결 위치와의 근접성, 기존 인프라를 고려할 때는 모두 프로비저닝 시간에 영향을 미칩니다. AWS Direct Connect 파트너가 정확한 프로비저닝 시간을 알려줄 것입니다.

보안

정의

보안 요구 사항은 하이브리드 연결 유형에 영향을 미칩니다. 주요 고려 사항은 다음과 같습니다.

- 전송 유형 - 인터넷 또는 프라이빗 네트워크 연결
- 암호화 요구 사항

핵심 질문

- 보안 요구 사항 및 정책에 따라 인터넷을 통한 암호화된 연결을 사용하여 AWS에 연결할 수 있습니까? 아니면 프라이빗 네트워크 연결 사용을 의무화하고 있습니까?
- 프라이빗 네트워크 연결을 활용할 때 네트워크 계층이 전송 중 암호화를 제공해야 합니까?

기술 솔루션

보안 요구 사항 및 정책에 따라 인터넷 사용이 허용되거나 AWS와 회사 네트워크 간의 프라이빗 네트워크 연결 사용이 필요할 수 있습니다. 또한 네트워크가 전송 중에 암호화를 제공해야 하는지 또는 애플리케이션 계층에서 암호화를 수행할 수 있는지 여부를 결정하는 데에도 영향을 미칩니다.

인터넷을 활용할 수 있는 경우, AWS Site-to-Site VPN VPN을 사용하여 인터넷을 통해 네트워크와 Amazon VPC 또는 AWS Transit Gateway 사이에 암호화된 터널을 생성할 수 있습니다. 인터넷 기반 연결을 활용하는 경우 인터넷을 통해 SD-WAN 솔루션을 AWS 로 확장할 수도 있습니다. 이 백서 뒷부분의 고객 관리형 VPN 및 SD-WAN 섹션에서는 SD-WAN에 대한 구체적인 고려 사항을 다룹니다.

AWS와 회사 네트워크 간에 프라이빗 네트워크 연결이 필요한 경우, AWS는 AWS Direct Connect 전용 연결 또는 호스트 연결을 사용할 것을 권장합니다. 프라이빗 네트워크 연결을 통해 전송 중 암호화가 필요한 경우 Direct Connect를 통한 VPN을 설정하거나(퍼블릭 VIF 또는 전송 VIF) 10Gbps 또는 100Gbps 전용 연결에서 MACsec을 사용하는 것을 고려해야 합니다.

표 2 - 자동차 회사 연결 유형 요구 사항 예시

	Site-to-Site VPN	Direct Connect
운송	인터넷	프라이빗 네트워크 연결
전송 중 데이터 암호화	예	DX를 통한 S2S VPN, 트랜짓 VIF를 통한 S2S VPN 또는 10Gbps 또는 100Gbps 전용 연결의 MACsec이 필요합니다.

서비스 수준에 관한 계약(SLA)

정의

기업 조직에서는 대개 서비스 공급자에게 조직이 소비하는 각 서비스에 대한 SLA를 충족하도록 요구합니다. 조직은 이를 기반으로 자체 서비스를 구축하고 자체 소비자에게 SLA를 제공할 수 있습니다. SLA는 서비스 제공 및 운영 방식을 설명하므로 중요하며 가용성과 같은 측정 가능한 특정 특성을 포함하는 경우가 많습니다. 서비스가 정의된 SLA를 위반할 경우 일반적으로 서비스 공급업체는 계약에 명시된 금전적 보상을 제공합니다. SLA는 측정 유형, 요구 사항 및 측정 기간을 정의합니다. AWS Direct Connect SLA에 따른 가동 시간 목표 정의를 예시로 참조하세요.

핵심 질문

- 하이브리드 연결 SLA와 서비스 크레딧이 필요합니까?
- 전체 하이브리드 네트워크가 가동 시간 목표를 준수해야 합니까?

고려해야 할 기능

연결 유형: 인터넷 연결은 예측할 수 없습니다. AWS는 다양한 ISP와의 여러 링크를 통해 세심한 주의를 기울이고 있지만, 인터넷 관리는 AWS 또는 단일 제공업체의 관리 도메인 외부에 있습니다. 트래픽이 네트워크 경계를 벗어나면 클라우드 제공업체가 할 수 있는 라우팅 엔지니어링 및 트래픽 영향력에는 한계가 있습니다. 하지만 AWS Site-to-Site VPN 엔드포인트에 대한 가용성 목표를 제공하는 AWS Site-to-Site VPN SLA가 있습니다.

AWS Direct Connect는 공식적인 SLA를 제공하며, 서비스 크레딧은 SLA가 충족되지 않은 월간 청구 주기 동안 사용 불가능했던 해당 연결에 대해 사용자가 지불한 총 AWS Direct Connect 포트 시간 요금

의 백분율로 계산됩니다. SLA가 필요한 경우 이 방법을 사용하는 것이 좋습니다. AWS Direct Connect는 AWS Direct Connect 위치 수, 연결 수, 기타 구성 세부 정보 등 각 가동 시간 목표에 대한 구체적인 최소 구성 요구 사항을 나열합니다. 요구 사항을 충족하지 못하면 서비스가 정의된 SLA를 위반하는 경우 서비스 크레딧을 제공할 수 없습니다.

중요한 점은 하이브리드 연결을 제공하도록 선택한 서비스가 SLA 요구 사항을 충족하도록 구성되어 있더라도 나머지 네트워크가 동일한 수준의 SLA를 제공하지 않을 수 있다는 것입니다. AWS의 책임은 AWS Direct Connect 포트의 AWS Direct Connect 위치에서 끝납니다. AWS가 트래픽을 조직의 네트워크로 넘기면 더 이상 AWS의 책임이 아닙니다. AWS와 온프레미스 네트워크 사이에 서비스 제공업체를 사용하는 경우, 연결은 사용자와 서비스 제공업체 간의 SLA(해당되는 경우)의 적용을 받습니다. 하이브리드 연결을 설계할 때는 전체 하이브리드 네트워크가 가장 취약한 부분만큼이나 중요하다는 점을 명심하세요.

AWS Direct Connect 파트너는 AWS Direct Connect 연결을 제공합니다. 파트너는 AWS와의 경계 지점까지 제품 제공을 기반으로 서비스 크레딧이 포함된 SLA를 제공할 수 있습니다. 이 옵션은 APN 파트너와 직접 평가하고 추가 조사를 해야 합니다. AWS는 검증된 제공 파트너 목록을 게시합니다.

논리적 설계: 전체 설계의 일부로 연결 유형 외에도 다른 구성 요소도 고려해야 합니다. 예를 들어, AWS Transit Gateway에는 AWS S2S VPN과 마찬가지로 자체 SLA가 있습니다. 보안상의 이유로 AWS Transit Gateway 확장용 VPN과 AWS S2S VPN을 사용할 수도 있지만, 각 서비스에서 서비스 크레딧을 받을 수 있으려면 두 VPN 모두를 각 SLA에 맞게 설계해야 합니다.

AWS Direct Connect Resiliency Recommendations와 Resiliency Toolkit을 검토하세요.

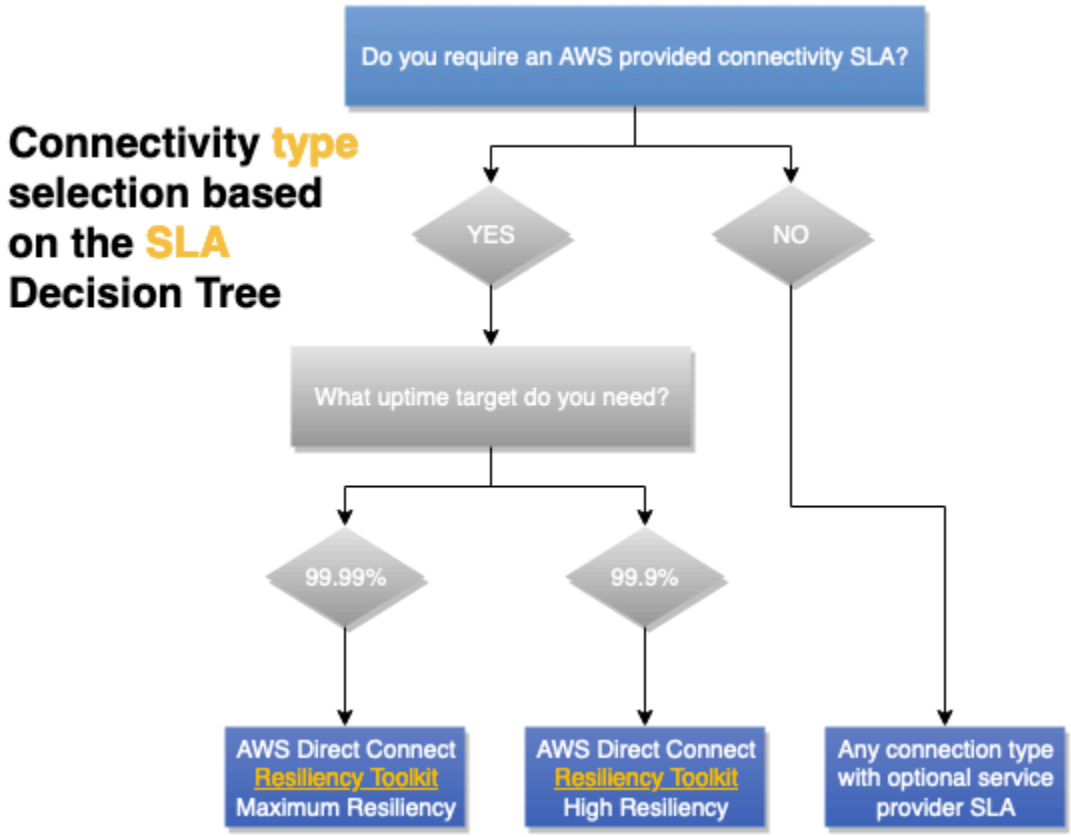

그림 3 - SLA 고려 사항 의사 결정 트리

성능

정의

네트워크 성능에 영향을 미치는 요인은 지연 시간, 패킷 손실, 지터, 대역폭 등 여러 가지가 있습니다. 애플리케이션 요구 사항에 따라 이러한 각 요소의 중요도가 달라질 수 있습니다.

핵심 질문

애플리케이션 요구 사항에 따라 애플리케이션 동작 및 사용자 경험에 영향을 미치는 네트워크 성능 요소를 식별하고 우선 순위를 정해야 합니다.

대역폭

대역폭은 연결의 데이터 전송 속도를 의미하며 일반적으로 초당 비트 수(bps)로 측정됩니다. 초당 메가비트(Mbps) 및 초당 기가비트(Gbps)는 일반적인 스케일링이며, 다른 곳에서 볼 수 있는 기본 2(2^10)와 달리 기본 10(초당 1,000,000비트 = 1Mbps)입니다.

애플리케이션의 대역폭 요구 사항을 평가할 때는 시간이 지남에 따라 대역폭 요구 사항이 변할 수 있다는 점을 염두에 두십시오. 클라우드로의 초기 배포, 정상 운영, 새 워크로드 및 장애 조치 시나리오는 모두 대역폭 요구 사항이 다를 수 있습니다.

애플리케이션마다 고유한 대역폭 고려 사항이 있을 수 있습니다. 일부 애플리케이션은 고대역폭 연결에서 결정적 성능이 필요한 반면, 결정적 성능과 고대역폭이 모두 필요한 애플리케이션도 있습니다. 애플리케이션이 트래픽 흐름당 대역폭 제한에 도달하는 경우, 연결 대역폭을 더 많이 사용할 수 있도록 여러 트래픽 흐름(스트림 또는 소켓이라고도 함)을 병렬로 사용하려면 특별한 구성이 필요할 수 있습니다. VPN은 터널링 오버헤드, 낮은 MTU 제한 또는 하드웨어 대역폭 제한으로 인해 처리량을 제한할 수 있습니다.

지연 시간

지연 시간은 네트워크 연결을 통해 패킷이 소스에서 대상으로 이동하는 데 필요한 시간으로, 일반적으로 밀리초(ms) 단위로 측정되며, 지연 시간이 짧은 요구 사항은 마이크로초(µs)로 표시되기도 합니다. 지연 시간은 빛의 속도에 따라 달라지므로 거리에 따라 지연 시간도 증가합니다.

애플리케이션 지연 요구 사항은 다양한 형태를 취할 수 있습니다. 가상 데스크톱과 같은 고도의 대화형 애플리케이션은 사용자가 입력을 수행한 시점부터 가상 데스크톱이 입력에 반응하는 것을 볼 때까지의 지연 시간 목표를 측정할 수 있습니다. Voice over IP(VoIP) 애플리케이션의 요구 사항도 비슷할 수 있습니다. 고려해야 할 두 번째 유형의 워크로드는 트랜잭션이 많아 작업을 계속하려면 서버의 응답이 필요한 유형입니다. 데이터베이스 또는 기타 형태의 키/값 저장소는 네트워크 지연 시간 증가로 인해 큰 영향을 받을 수 있습니다.

Jitter

Jitter는 네트워크 대기 시간의 일관성을 측정하며 대기 시간과 마찬가지로 일반적으로 밀리초(ms) 단위로 측정됩니다.

애플리케이션 Jitter 요구 사항은 일반적으로 비디오 및 음성 전송을 포함한 실시간 스트리밍 애플리케이션에서 찾을 수 있습니다. 이러한 애플리케이션은 일정한 속도와 지연으로 데이터 흐름을 유지하고 소량의 Jitter를 보정하기 위한 작은 버퍼를 사용해야 하는 경향이 있습니다.

패킷 손실

패킷 손실은 전달되지 않은 네트워크 트래픽의 비율을 측정한 것입니다. 모든 네트워크에는 높은 트래픽 버스트, 용량 감소, 네트워크 장비 오류 및 기타 이유로 인해 때때로 어느 정도의 패킷 손실이 발생합니다. 따라서 애플리케이션은 어느 정도 패킷 손실을 허용해야 하지만 허용 가능한 정도는 애플리케이션마다 다를 수 있습니다.

TCP를 사용하여 트래픽을 전송하는 애플리케이션은 재전송을 통해 패킷 손실을 수정할 수 있습니다. IP 위에 UDP 또는 자체 프로토콜을 사용하는 애플리케이션은 패킷 손실을 처리하는 자체 수단을 구현해야 하며 이에 매우 민감할 수 있습니다. VoIP 응용 프로그램에서는 재전송을 시도하는 대신 단순히 패킷이 손실된 통화 부분에 무음을 삽입할 수 있습니다. 일부 VPN 솔루션에는 트래픽을 전달하는 데 사용하는 네트워크의 패킷 손실을 복구하기 위한 자체 메커니즘이 포함되어 있습니다.

고려해야 할 기능

예측 가능한 지연 시간과 처리량이 필요한 경우 결정적인 성능을 제공하는 AWS Direct Connect를 선택하는 것이 좋습니다. 처리량 요구 사항에 따라 대역폭을 선택할 수 있습니다. AWS는 인터넷 기반 연결이 제공할 수 있는 것보다 더 일관된 네트워크 경험이 필요한 경우 AWS Direct Connect를 사용할 것을 권장합니다. 프라이빗 VIF 및 전송 VIF는 네트워크를 통한 패킷 수를 줄이고 오버헤드 감소로 인해 처리량을 향상시킬 수 있는 점보 프레임을 지원합니다. AWS Direct Connect SiteLink를 사용하면 AWS 백본을 사용하여 위치 간 연결을 제공할 수 있으며 요청 시 활성화할 수 있습니다. Direct Connect 대역폭을 선택할 때는 SiteLink에 사용되는 대역폭을 고려해야 합니다.

AWS Direct Connect를 통해 VPN을 사용하면 암호화가 추가됩니다. 하지만 MTU 크기가 줄어들어 처리량이 줄어들 수 있습니다. AWS 관리형 Site-to-Site(S2S) VPN 기능은AWS Site-to-Site VPNVPN 설명서에서 확인할 수 있습니다. 연결을 통한 암호화가 기본 암호화 요구 사항인 경우 대부분의 직접 연결 위치에서 MACsec을 지원합니다. MACsec에는 Site-to-Site VPN 연결과 동일한 MTU 또는 잠재적 처리량 고려 사항이 없습니다. AWS Transit Gateway를 사용하면 고객은 VPN 연결 수를 수평적으로 확장하고 등가 다중 경로(ECMP)를 통해 그에 따라 처리량을 높일 수 있습니다. AWS의 관리형 Site-to-Site VPN은 프라이빗 연결을 위해 Direct Connect 전송 VIF 사용을 지원합니다. 자세한 내용은AWS Direct Connect를 통한 프라이빗 IP VPN을 참조하세요.

또 다른 옵션은 인터넷을 통해 AWS 관리형 Site-to-Site VPN을 사용하는 것입니다. 비용이 저렴하고 널리 사용 가능하기 때문에 매력적인 옵션이 될 수 있습니다. 그러나 인터넷을 통한 성능은 최선의 노력이라는 점을 명심하십시오. 인터넷 기상 상황, 혼잡, 대기 시간 증가 등은 예측할 수 없습니다. AWS는 AWS Accelerated S2S VPN을 통해 인터넷 경로 사용의 일부 단점을 완화할 수 있는 솔루션을 제공합니다. Accelerated S2S VPN은 AWS Global Accelerator를 사용합니다. 글로벌 액셀러레이터를 사용하면 VPN 트래픽이 최대한 빨리 고객 게이트웨이 디바이스에 가깝게 AWS 네트워크에 유입될 수 있습니다. 정체가 없는 AWS 글로벌 네트워크를 사용해 최상의 성능을 제공하는 엔드포인트로 트래픽을 라우팅하여 네트워크 경로를 최적화합니다. 가속 VPN 연결을 사용하여 트래픽이 퍼블릭 인터넷을 통해 라우팅될 때 발생할 수 있는 네트워크 중단을 방지할 수 있습니다.

비용

정의

클라우드에서 하이브리드 연결 비용에는 프로비저닝된 리소스 및 사용 비용이 포함됩니다. 프로비저닝된 리소스의 비용은 시간 단위(일반적으로 시간당)로 측정됩니다. 사용량은 기가바이트(GB)로 측정되는 데이터 전송 및 처리에 사용됩니다. 기타 비용에는 AWS 네트워크 접속 지점으로의 연결 비용이 포함됩니다. 네트워크가 동일한 콜로케이션 시설 내에 있는 경우 교차 연결 비용만큼 적을 수 있습니다. 네트워크가 다른 위치에 있는 경우 서비스 공급업체 또는 APN Direct Connect 파트너 비용이 발생합니다.

핵심 질문

- 시설 및 인터넷을 통해 AWS로 매월 전송되는 데이터의 양은 어느 정도일 것으로 예상하십니까?
- AWS에서 시설 및 인터넷으로 매월 전송되는 데이터의 양은 어느 정도일 것으로 예상하십니까?
- 이 금액은 얼마나 자주 변경됩니까?
- 장애 시나리오에는 어떤 변화가 있습니까?

고려해야 할 기능

AWS에서 대역폭을 많이 사용하는 워크로드를 실행하려는 경우 AWS를 사용하면 두 가지 방법으로 AWS Direct Connect 내부 및 외부의 네트워크 비용을 줄일 수 있습니다. 첫째, AWS와 직접 데이터를 주고받음으로써 인터넷 서비스 공급자에 지불하는 대역폭 비용을 줄일 수 있습니다. 둘째, 전용 연결을 통해 전송된 모든 데이터에는 인터넷 데이터 전송 요금이 아닌 할인된 AWS Direct Connect 데이터 전송 요금이 부과됩니다. 자세한 내용은 Direct Connect 요금 페이지를 참조하세요.

AWS Direct Connect를 사용하면 AWS Direct Connect SiteLink를 사용하여 AWS 백본을 사용하는 사이트를 상호 연결할 수 있습니다. SiteLink 출시 블로그를 참조하세요. 이 기능을 활용하면 일반적인 Direct Connect 데이터 전송 비용이 발생하며 SiteLink가 활성화된 경우 시간당 요금이 부과됩니다. SiteLink는 온디맨드로 활성화 및 비활성화할 수 있으며, 인터넷 또는 프라이빗 네트워크 연결과 관련된 장애 시나리오에 적합한 옵션일 수 있습니다.

온프레미스와 Direct Connect 위치 간의 연결을 위해 네트워크 서비스 공급자를 사용하는 경우 대역폭 약정을 변경하는 데 필요한 능력과 시간은 서비스 공급자와의 계약에 따라 결정됩니다.

AWS 백본은 모든 AWS 리전 네트워크 거점에서 중국을 제외한 모든 AWS 리전으로 트래픽을 전송할 수 있습니다. 이 기능은 인터넷을 사용하여 원격 AWS 리전 리전에 액세스하는 것보다 많은 기술적 이

점이 있지만 비용이 발생합니다. 자세한 내용은 EC2 데이터 전송 가격 페이지를 참조하세요. 트래픽 경로에 AWS Transit Gateway가 있는 경우 GB당 데이터 처리 비용이 추가되지만 두 Transit Gateway 간에 지역 간 피어링을 사용하는 경우 Transit Gateway 데이터 처리에 대해 한 번만 요금이 청구됩니다.

최적의 애플리케이션 설계로 데이터 처리를 AWS 내에서 유지하고 불필요한 데이터 송신 요금을 최소화하세요. AWS로의 데이터 수신은 무료입니다.

> **Note**
>
> 전체 연결 솔루션의 일환으로 AWS 연결 비용 외에도 서비스 공급업체 비용, 교차 연결, 랙, DX 위치 내 장비(필요한 경우)를 포함한 종단 간 연결 비용도 고려해야 합니다.

인터넷을 사용해야 할지 프라이빗 연결을 사용해야 할지 잘 모르겠다면, AWS Direct Connect를 사용하는 것이 인터넷을 사용하는 것보다 저렴해지는 손익분기점을 계산해 보세요. 데이터 볼륨으로 인해 AWS Direct Connect 비용이 더 저렴하고 영구적인 연결이 필요한 경우라면 AWS Direct Connect가 최적의 연결 옵션입니다.

연결이 일시적이고 인터넷이 다른 요구 사항을 충족하는 경우 인터넷의 탄력성 때문에 인터넷을 통한 AWS S2S VPN을 사용하는 것이 더 저렴할 수 있습니다. 단, 온프레미스 네트워크의 인터넷 연결이 충분해야 합니다.

AWS Direct Connect가 있는 시설(목록은 Direct Connect 웹 사이트에서 확인 가능) 내에 있는 경우 AWS에 대한 교차 연결을 설정할 수 있습니다. 즉, 1,10 또는 100Gbps의 전용 연결을 사용한다는 의미입니다. AWS Direct Connect 파트너는 더 많은 대역폭 옵션과 더 작은 용량을 제공하므로 연결 비용을 최적화할 수 있습니다. 예를 들어 50Mbps 호스팅 연결과 1Gbps 전용 연결 중 하나로 시작할 수 있습니다.

AWS Transit Gateway를 사용하면 VPN 및 Direct Connect 연결을 여러 VPC와 공유할 수 있습니다. 시간당 AWS Transit Gateway에 연결하는 연결 수와 AWS Transit Gateway를 통해 흐르는 트래픽 양에 따라 요금이 부과되지만, 관리가 간소화되고 필요한 VPN 연결과 VIF의 수가 줄어듭니다. 운영 오버헤드 감소로 인한 이점과 비용 절감은 데이터 처리에 드는 추가 비용을 쉽게 능가할 수 있습니다. 선택적으로, AWS Transit Gateway가 대부분의 VPC로 향하는 트래픽 경로에 있는 설계를 고려할 수 있습니다(전부는 아님). 이 접근 방식은 대량의 데이터를 AWS로 전송해야 하는 사용 사례에 대해 AWS Transit Gateway 데이터 처리 수수료를 피할 수 있습니다. 이 설계에 대한 자세한 내용은 연결 모델 섹션을 참조하세요. 또 다른 접근 방식은 AWS Direct Connect를 기본 경로로 사용하고 인터넷을 통한 AWS S2S VPN을 백업/장애 조치 경로로 결합하는 것입니다. 이 솔루션은 기술적으로 실현 가능하고

비용 효율적이지만, 기술적 단점(이 백서의 신뢰성 섹션에서 설명)이 있으며 관리가 더 어려울 수 있습니다. AWS는 매우 중요하거나 중요한 워크로드에는 이 방법을 권장하지 않습니다.

마지막 접근 방식은 Amazon EC2 인스턴스에 배포된 고객 관리형 VPN 또는 SD-WAN입니다. 사이트가 수십 개에서 수백 개일 경우 AWS S2S VPN과 비교하면 규모가 더 저렴할 수 있습니다. 하지만 각 가상 어플라이언스마다 고려해야 할 관리 오버헤드, 라이선스 비용, EC2 리소스 비용이 있습니다.

의사결정 매트릭스

표 3 - Example Corp. Automotive 연결 설계 입력

범주	고객 관리형 VPN 또는 SD-WAN	AWS S2S VPN	AWS Accelerated S2S VPN	AWS Direct Connect 호스팅 연결	AWS Direct Connect 전용 연결
인터넷 연결 필요	예	예	예	아니요	아니요
프로비저닝된 리소스 비용	EC2 인스턴스 및 소프트웨어 라이선싱	AWS S2S VPN	AWS S2S VPN 및 AWS Global Accelerator	포트 비용 중 적용 가능한 용량 부분	전용 포트 비용
데이터 전송 비용	인터넷 요금	인터넷 요금 또는 Direct Connect 요금	데이터 전송 프리미엄이 적용되는 인터넷	Direct Connect 속도	Direct Connect 속도
전송 게이트웨이	선택	선택	필수	선택	선택
AWS 데이터 처리 비용	해당 사항 없음	AWS Transit Gateway에서만 발생	예	AWS Transit Gateway에서만 발생	AWS Transit Gateway에서만 발생
AWS Direct Connect를 통해 사용할 수 있나요?	예	예	아니요	해당 사항 없음	해당 사항 없음

연결 설계 선택

백서의 이 섹션에서는 연결 설계 선택에 영향을 미치는 고려 사항을 다룹니다. 연결 설계에는 논리적 측면뿐만 아니라 하이브리드 연결 신뢰성을 설계하고 최적화하는 방법도 포함됩니다.

확장성, 연결 모델, 안정성, 고객 관리VPN형 및 SD-와 같은 고려 사항이 적용됩니다WAN.

고려 사항

- 확장성
- 연결 모델
- 신뢰성
- 고객 관리형 VPN 및 SD-WAN

확장성

정의

확장성이란 요구 사항이 변경되고 시간이 지남에 따라 연결 솔루션이 성장하고 발전할 수 있는 능력을 말합니다.

솔루션을 설계할 때는 현재 규모뿐만 아니라 예상 성장률도 고려해야 합니다. 이러한 성장은 유기적인 성장일 수도 있고, 인수합병과 같은 급격한 확장과 관련이 있을 수도 있습니다.

참고: 대상 솔루션 아키텍처에 따라 앞의 모든 요소를 고려하지는 않아도 될 수도 있습니다. 그러나 이는 가장 일반적인 하이브리드 네트워크 솔루션의 확장성 요구 사항을 식별하는 기본 요소가 될 수 있습니다. 이 백서는 하이브리드 연결 선택 및 설계에 중점을 둡니다. 또한 VPC 네트워킹 아키텍처와 관련된 하이브리드 연결의 규모를 고려하는 것이 좋습니다. 자세한 내용은 확장 가능하고 안전한 다중 VPC AWS 네트워크 인프라 구축 백서를 참조하세요.

핵심 질문

- 온프레미스 사이트 또는 사이트에 연결해야 VPCs 하는 현재 및 예상 수는 몇 개입니까?
- 단일 AWS 리전 또는 여러 리전에 VPCs 배포됩니까?
- AWS에 연결해야 하는 온프레미스 사이트는 몇 개입니까?
- AWS에 연결해야 하는 사이트당 고객 게이트웨이 디바이스(일반적으로 라우터 또는 방화벽)는 몇 개입니까?

- Amazon에 광고될 것으로 예상되는 경로는 몇 VPCs개이며 AWS 측면에서 수신될 것으로 예상되는 경로 수는 몇 개입니까?
- 시간 AWS 경과에 따라 대역폭을 늘려야 하는 요구 사항이 있나요?

고려해야 할 기능

규모는 하이브리드 연결 설계에서 중요한 요소입니다. 이를 위해 다음 섹션에서는 대상 연결 모델 설계의 일부에 규모를 포함할 것입니다.

다음은 하이브리드 네트워크 연결 설계의 규모 복잡성을 최소화하기 위한 권장 모범 사례입니다.

- 경로 요약을 사용하여 에 광고되고 에서 수신되는 경로 수를 줄여야 합니다 AWS. 따라서 IP 주소 지정 체계는 경로 요약의 사용을 극대화하도록 설계되어야 합니다. 트래픽 엔지니어링은 전반적으로 중요한 고려 사항입니다. 트래픽 엔지니어링에 대한 자세한 내용은 신뢰성 섹션의 트래픽 엔지니어링 하위 섹션을 참조하세요.
- 단일 세션이 여러 에 대한 연결을 제공할 수 AWS Transit Gateway있는 VGW 또는 DXGW를 사용하여 BGP 피어링 BGP 세션 수를 최소화합니다VPCs.
- 여러 AWS 리전 및 온프레미스 사이트를 함께 연결해야 하는 WAN 경우 클라우드를 고려하세요.

연결 모델

정의

연결 모델은 온프레미스 네트워크와 AWS클라우드 리소스 간의 통신 패턴을 말합니다. Amazon S3 및 DynamoDB AWS 리전와 같이 단일 AWS 리전 또는 다중 에 퍼블릭 엔드포인트가 있는 서비스뿐만 AWS 아니라 여러 리전VPCs에 걸쳐 단일 또는 다중 VPC 내에서 Amazon 내에 클라우드 리소스를 배포할 수 있습니다. Amazon S3

핵심 질문

- 리전 내 및 리전 간 인터VPC 커뮤니케이션에 대한 요구 사항이 있나요?
- 온프레미스에서 직접 AWS 퍼블릭 엔드포인트에 액세스해야 하는 요구 사항이 있나요?
- 온프레미스에서 VPC 엔드포인트를 사용하여 AWS 서비스에 액세스해야 하는 요구 사항이 있나요?

고려해야 할 기능

다음은 가장 일반적인 연결 모델 시나리오의 일부입니다. 각 연결 모델에는 요구 사항, 특성, 고려 사항이 포함됩니다.

참고: 앞서 강조한 바와 같이 이 백서는 온프레미스 네트워크와 AWS사이의 하이브리드 연결에 초점을 맞추고 있습니다. 상호 연결 설계에 대한 자세한 내용은 확장 가능하고 안전한 다중 VPC AWS 네트워크 인프라 구축 백서를 VPCs참조하세요.

모델

- AWS 가속 Site-to-SiteVPN- AWS Transit Gateway, 단일 AWS 리전
- AWS DX - VGW, 단일 리전 DXGW 포함
- AWS DX - VGW, 다중 리전 및 AWS 퍼블릭 피어링 DXGW 포함
- AWS DX - AWS Transit Gateway, 다중 리전 및 AWS 퍼블릭 피어링 DXGW 포함
- AWS DX - AWS Transit Gateway, 다중 리전(3개 이상) DXGW 포함

AWS 가속 Site-to-SiteVPN- AWS Transit Gateway, 단일 AWS 리전

이 모델은 다음과 같이 구성됩니다.

- 단일 AWS 리전.
- AWS 와의 관리형 Site-to-Site VPN 연결 AWS Transit Gateway.
- 가속VPN이 활성화되었습니다.

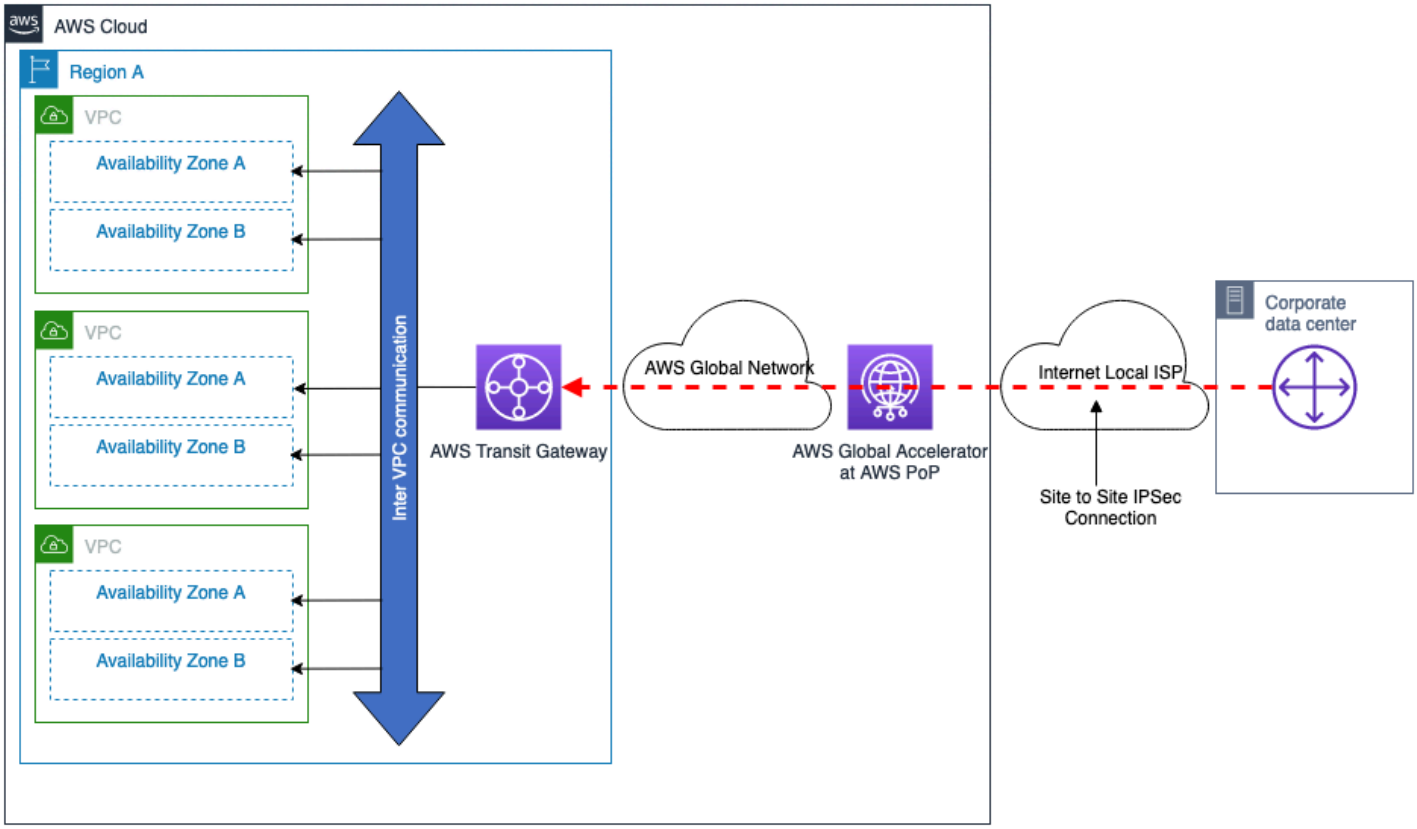

그림 4 - AWS 관리형 VPN - AWS Transit Gateway, 단일 AWS 리전

연결 모델 속성:

- 가속 VPN 연결 을 사용하여 퍼블릭 인터넷을 통해 최적화된 연결을 설정할 수 있는 기능을 제공합니다. AWS Site-to-Site VPN
- 를 사용하여 여러 VPN 터널을 구성하여 더 높은 VPN 연결 대역폭을 달성할 수 있는 기능을 제공합니다ECMP.
- 여러 원격 사이트에서 연결하는 데 사용할 수 있습니다.
- 동적 라우팅()을 사용하여 자동 장애 조치를 제공합니다BGP.
- 에 AWS Transit Gateway 연결된 를 사용하면 연결된 VPCs모든 가 동일한 VPN 연결을 사용할 VPCs 수 있습니다. 에서 원하는 통신 모델을 제어할 수도 있습니다. VPCs자세한 내용은 Transit Gateways 작동 방식 을 참조하세요.
- 타사 보안 및 SD-WAN 가상 어플라이언스를 와 통합할 수 있는 유연한 설계 옵션을 제공합니다 AWS Transit Gateway. 및 온프레미스에서 VPC 트래픽 에 대한 VPC-to-VPC 중앙 집중식 네트워크 보안을 참조하세요.

규모 고려 사항:

- IPsec 터널이 여러 개 있고 ECMP 구성된 최대 50Gbps의 대역폭(각 트래픽 흐름은 VPN 터널당 최대 대역폭으로 제한됨).
- 에 따라 수천 개의 를 연결할 VPCs 수 있습니다 AWS Transit Gateway.
- 경로 수와 같은 다른 규모 한도는 Site-to-Site VPN 할당량을 참조하세요.

기타 고려 사항:

- 온프레미스 데이터 센터와 간의 데이터 전송에 대한 추가 AWS Transit Gateway 처리 비용입니다 AWS.
- 원격 의 보안 그룹은 에서 참조할 수 VPC 없습니다. 하지만 VPC 피어링을 통해 지원 AWS Transit Gateway 됩니다.

AWS DX - VGW, 단일 리전 DXGW 포함

이 모델은 다음과 같이 구성됩니다.

- 단일 AWS 리전.
- 독립 DX 위치에 이중 AWS Direct Connect 연결.
- AWS DXGW 를 VPCs 사용하여 에 직접 연결됩니다VGW.
- 상호VPC 통신을 AWS Transit Gateway 위한 의 선택적 사용.

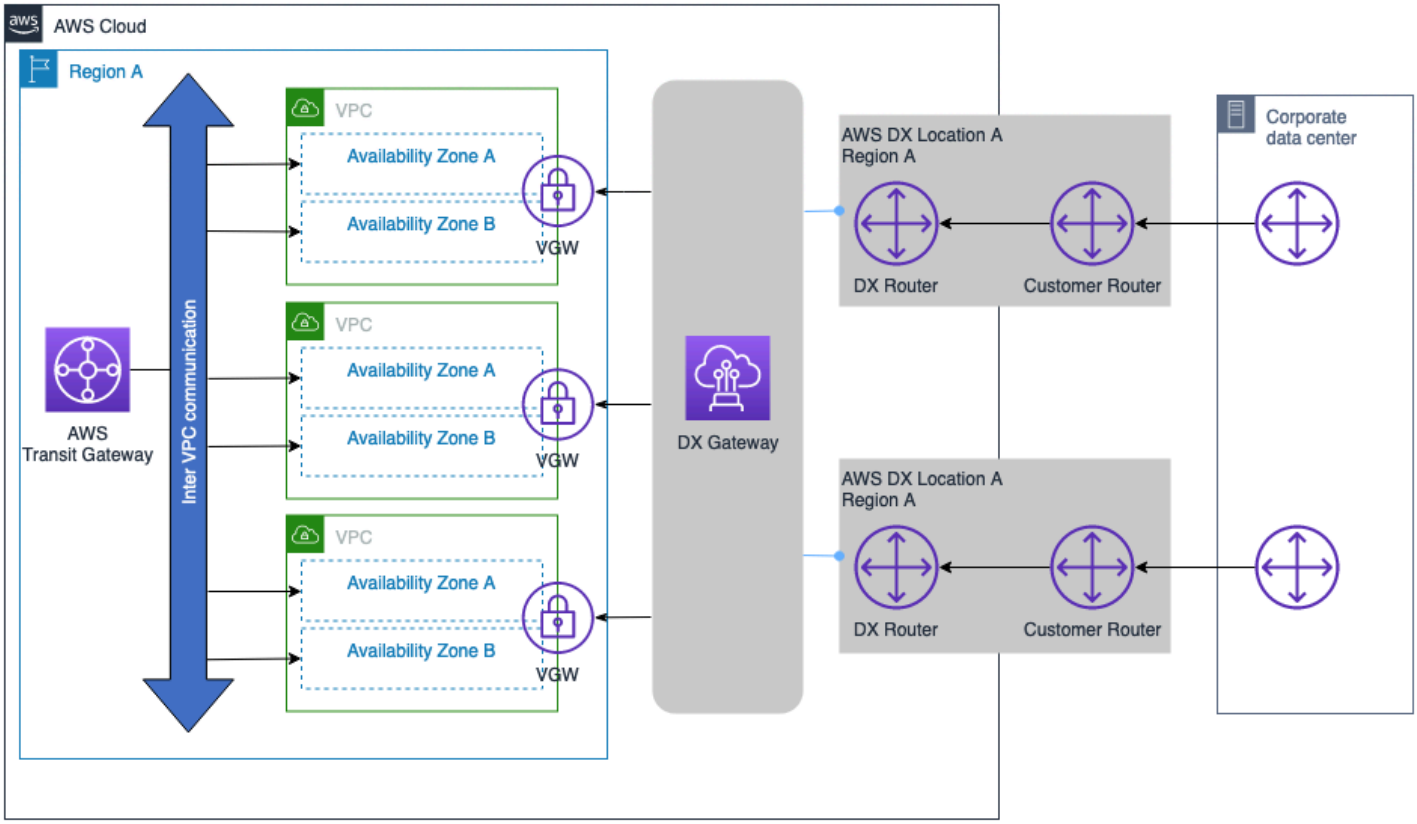

그림 5 – AWS DX – DXGW VGW, 단일 AWS 리전

연결 모델 속성:

- 향후 다른 리전의 VPCs 및 DX 연결에 연결할 수 있는 기능을 제공합니다.
- 동적 라우팅()을 사용하여 자동 장애 조치를 제공합니다BGP.
- 를 AWS Transit Gateway 사용하면 에서 원하는 통신 모델을 제어할 수 있습니다VPCs. 자세한 내용은 Transit Gateway 작동 원리를 참조하세요.

규모 고려 사항:

지원되는 접두사 수, DX 연결 유형VIFs당 수(전용, 호스팅)와 같은 다른 스케일 제한에 대한 자세한 내용은 AWS Direct Connect 할당량을 참조하세요. 몇 가지 주요 고려 사항:

- 프라이빗의 BGP 세션은 IPv4 및 에 대해 각각 최대 100개의 경로를 광고할 VIF 수 있습니다IPv6.
- 단일 BGP 세션당 최대 20DXGW개까지 연결할 VPCs 수 있습니다. 20개 이상이 VPCs 필요한 경우 대규모 연결을 용이하게 하기 위해 추가하거나 Transit Gateway 통합 사용을 고려할 DXGWs 수 있습니다.

- 필요에 따라 AWS Direct Connect를 추가할 수 있습니다.

기타 고려 사항:

- 및 온프레미스 네트워크 간의 AWS 데이터 전송에 대한 AWS Transit Gateway 관련 처리 비용이 발생하지 않습니다.
- 원격 의 보안 그룹은 AWS Transit Gateway (피VPC어링 필요)를 통해 참조할 수 VPC 없습니다.
- VPC 피어링은 간의 통신을 용이하게 AWS Transit Gateway 하는 대신 사용할 수 VPCs있지만, 이로 인해 대규모로 대규모 VPC point-to-point 피어링을 구축하고 관리하기 위한 운영 복잡성이 추가됩니다.
- 상호VPC 통신이 필요하지 않은 경우 이 연결 모델에서는 피VPC어링 AWS Transit Gateway 도 필요하지 않습니다.

AWS DX - VGW, 다중 리전 및 AWS 퍼블릭 피어링 DXGW 포함

이 모델은 다음과 같이 구성됩니다.

- 에 이중으로 연결된 여러 온프레미스 데이터 센터 AWS.
- 독립 DX 위치에 이중 AWS Direct Connect 연결.
- AWS DXGW 를 VPCs 사용하여 10개 이상VGW, 를 VPCs 사용하여 최대 20개에 직접 연결됩니다 VGW.
- 리전 간VPC 및 리전 간 통신을 AWS Transit Gateway 위한 의 선택적 사용.

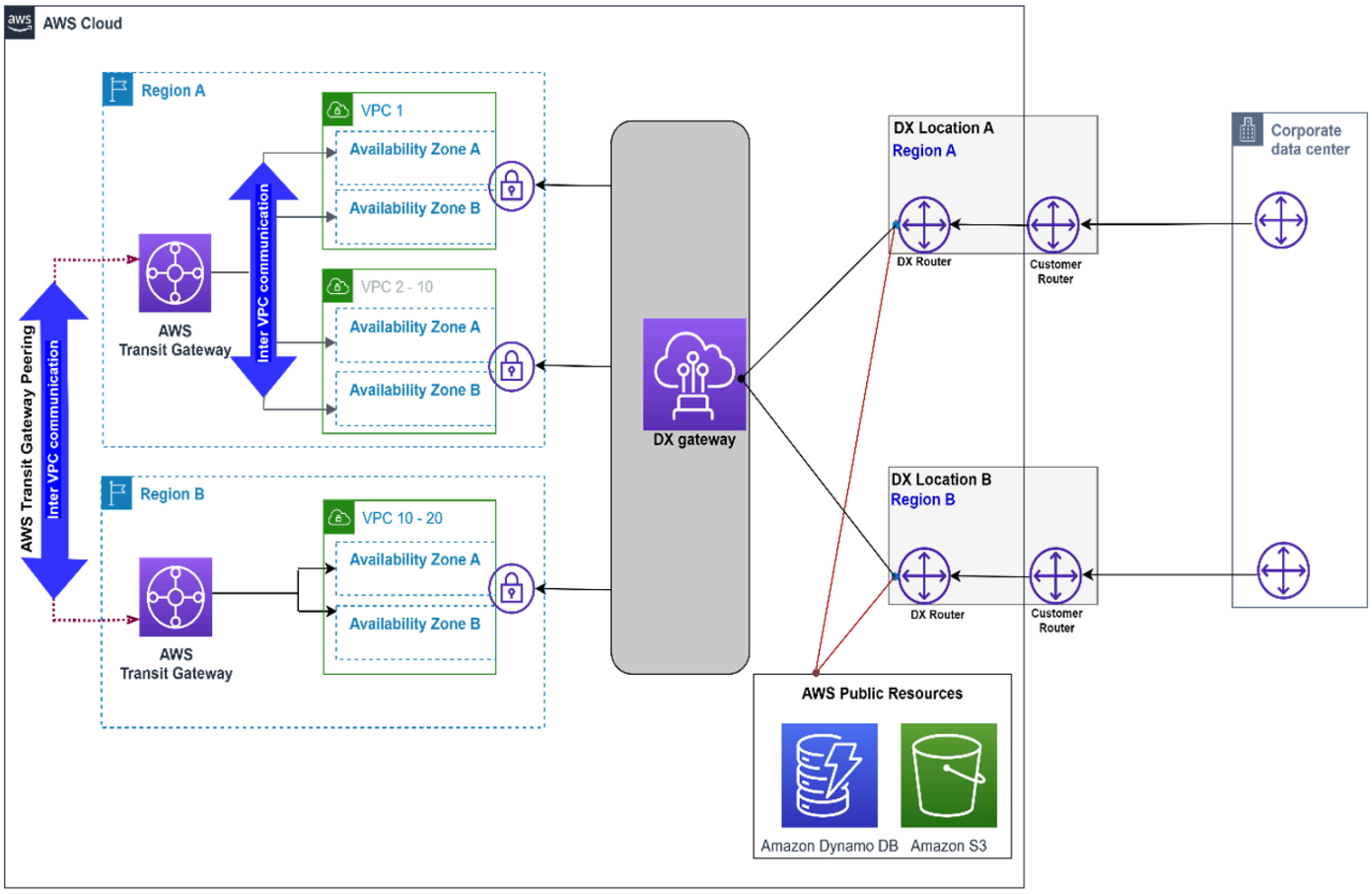

그림 6 – AWS DX – VGW, 다중 리전 및 퍼블릭 DXGW 포함 VIF

연결 모델 속성:

- AWS DXGW 를 사용하여 VGW 최대 20개를 VPCs 사용하여 10개 이상에 직접 연결됩니다 VPCsVGW.
- AWS DX 퍼블릭VIF은 AWS DX 연결을 통해 Amazon S3와 같은 AWS 퍼블릭 서비스에 직접 액세스하는 데 사용됩니다.
- 향후 다른 리전의 VPCs 및 DX 연결에 연결할 수 있는 기능을 제공합니다.
- AWS Transit Gateway 및 Transit Gateway 피어링이 용이하게 하는 리전 간VPC 및 리전 간 VPC 통신입니다.

규모 고려 사항:

지원되는 접두사 수, DX 연결 유형VIFs당 수(전용, 호스팅)와 같은 다른 스케일 제한에 대한 자세한 내용은 AWS Direct Connect 할당량을 참조하세요. 몇 가지 주요 고려 사항:

- 프라이빗 BGP 세션은 IPv4 및 에 대해 각각 최대 100개의 경로를 광고할 VIF 수 있습니다IPv6.
- 각 프라이빗 에서 DXGW 단일 BGP 세션당 최대 20개VIF까지 연결할 VPCs 수 있으며, VIFs 마다 최대 30개의 프라이빗 를 연결할 수 있습니다DXGW.
- 필요에 따라 AWS Direct Connect를 추가할 수 있습니다.

기타 고려 사항:

- 및 온프레미스 네트워크 간의 AWS 데이터 전송에 대한 AWS Transit Gateway 관련 처리 비용이 발생하지 않습니다.
- 원격 의 보안 그룹은 AWS Transit Gateway (피VPC어링 필요)에서 참조할 수 VPC 없습니다.
- VPC 피어링은 간의 통신을 용이하게 AWS Transit Gateway 하는 대신 사용할 수 VPCs있지만, 이로 인해 대규모로 대규모 VPC point-to-point 피어링을 구축하고 관리하기 위한 운영 복잡성이 가중될 것입니다.
- 상호VPC 통신이 필요하지 않은 경우 이 연결 모델에서는 피VPC어링 AWS Transit Gateway 도 필요하지 않습니다.

AWS DX - AWS Transit Gateway, 다중 리전 및 AWS 퍼블릭 피어링 DXGW 포함

이 모델은 다음과 같이 구성됩니다.

- 여러 AWS 리전.
- 독립 DX 위치에 이중 AWS Direct Connect 연결.
- 에 이중으로 연결된 단일 온프레미스 데이터 센터입니다 AWS.
- AWS DXGW 를 사용합니다 AWS Transit Gateway.
- 리전VPCs당 높은 규모.

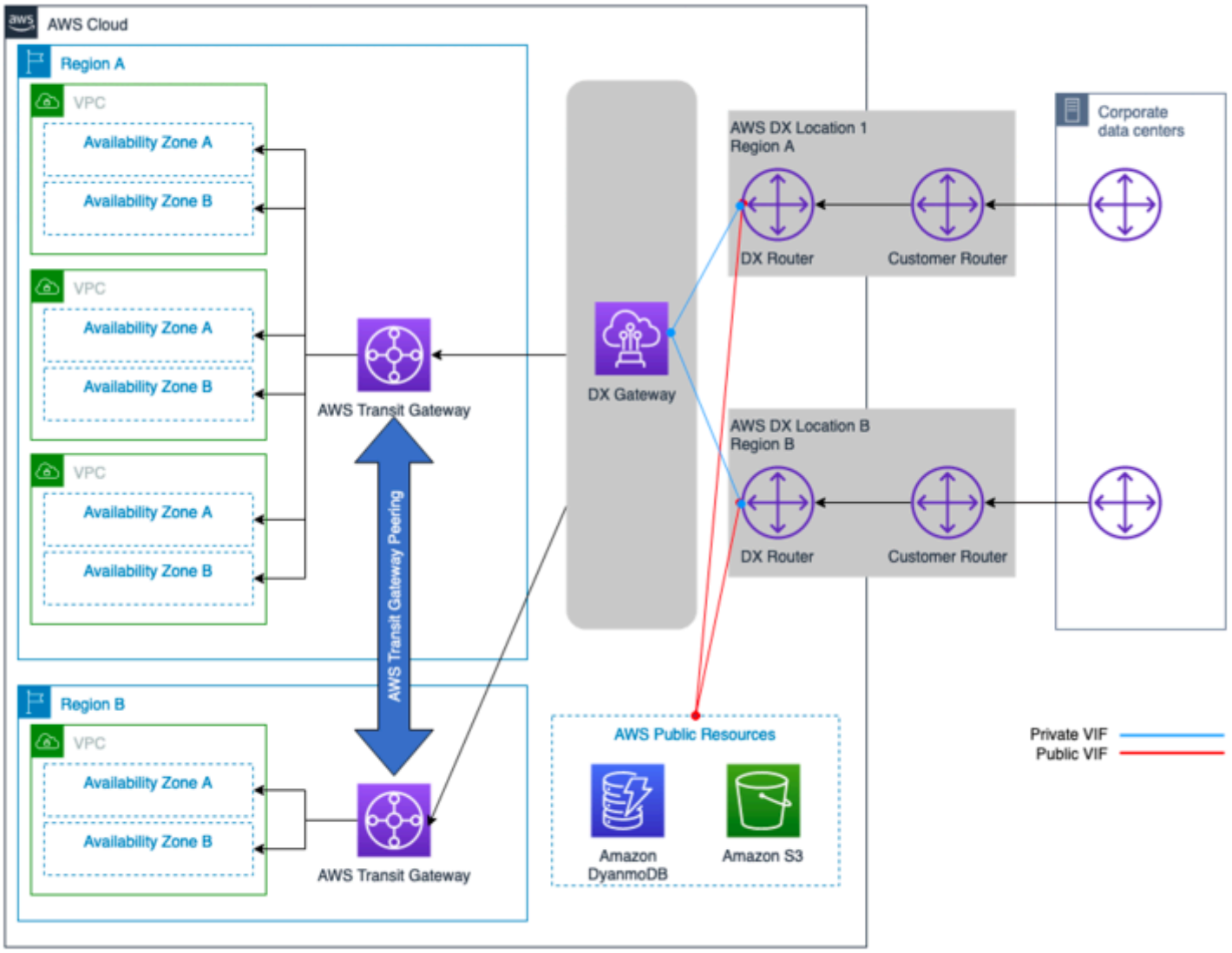

그림 7 – AWS DX – AWS Transit Gateway, 다중 리전 및 AWS 퍼블릭 DXGW 포함 VIF

연결 모델 속성:

- AWS DX 퍼블릭VIF은 AWS DX 연결을 통해 S3와 같은 AWS 퍼블릭 리소스에 직접 액세스하는 데 사용됩니다.
- 향후 다른 리전의 VPCs 및/또는 DX 연결에 연결할 수 있는 기능을 제공합니다.
- 에 AWS Transit Gateway 연결하면 간에 VPCs전체 또는 부분 메시 연결을 달성할 수 있습니다 VPCs.
- AWS Transit Gateway 피어링을 통한 리전 간VPC 및 리전 간 VPC 통신이 용이합니다.

- 타사 보안 및 SDWAN 가상 어플라이언스를 와 통합할 수 있는 유연한 설계 옵션을 제공합니다 AWS Transit Gateway. 및 온프레미스에서 VPC 트래픽 에 대한 VPC-to-VPC 중앙 집중식 네트워크 보안을 참조하세요.

규모 고려 사항:

- 송수신 경로 수는 전송을 통해 지원되는 최대 경로 수로 AWS Transit Gateway 제한됩니다VIF(인바운드 및 아웃바운드 수는 다양함). 규모 제한 및 지원되는 경로 및 수에 대한 자세한 내용은 AWS Direct Connect 할당량을 참조하세요VIFs.
- 단일 BGP 세션VPCs당 최대 수천 개까지 확장할 AWS Transit Gateway 수 있습니다.
- AWS DXVIF당 단일 전송.
- 필요에 따라 추가 AWS DX 연결을 추가할 수 있습니다.

기타 고려 사항:

- AWS 및 온프레미스 사이트 간 데이터 전송에 대한 추가 AWS Transit Gateway 처리 비용이 발생합니다.
- 원격 의 보안 그룹은 AWS Transit Gateway (피VPC어링 필요)에서 참조할 수 VPC 없습니다.
- VPC 피어링은 간의 통신을 용이하게 AWS Transit Gateway 하는 대신 사용할 수 VPCs있지만, 이로 인해 대규모로 대규모 VPC point-to-point 피어링을 구축하고 관리하기 위한 운영 복잡성이 가중될 것입니다.

AWS DX - AWS Transit Gateway, 다중 리전(3개 이상) DXGW 포함

이 모델은 다음과 같이 구성됩니다.

- 다중 AWS 리전 (3개 이상).
- 이중 온프레미스 데이터 센터.
- 리전당 독립 DX 위치에 대한 이중 AWS Direct Connect 연결입니다.
- AWS DXGW 를 사용합니다 AWS Transit Gateway.
- 리전VPCs당 높은 규모.
- 간의 피어링의 전체 메시 AWS Transit Gateway입니다.

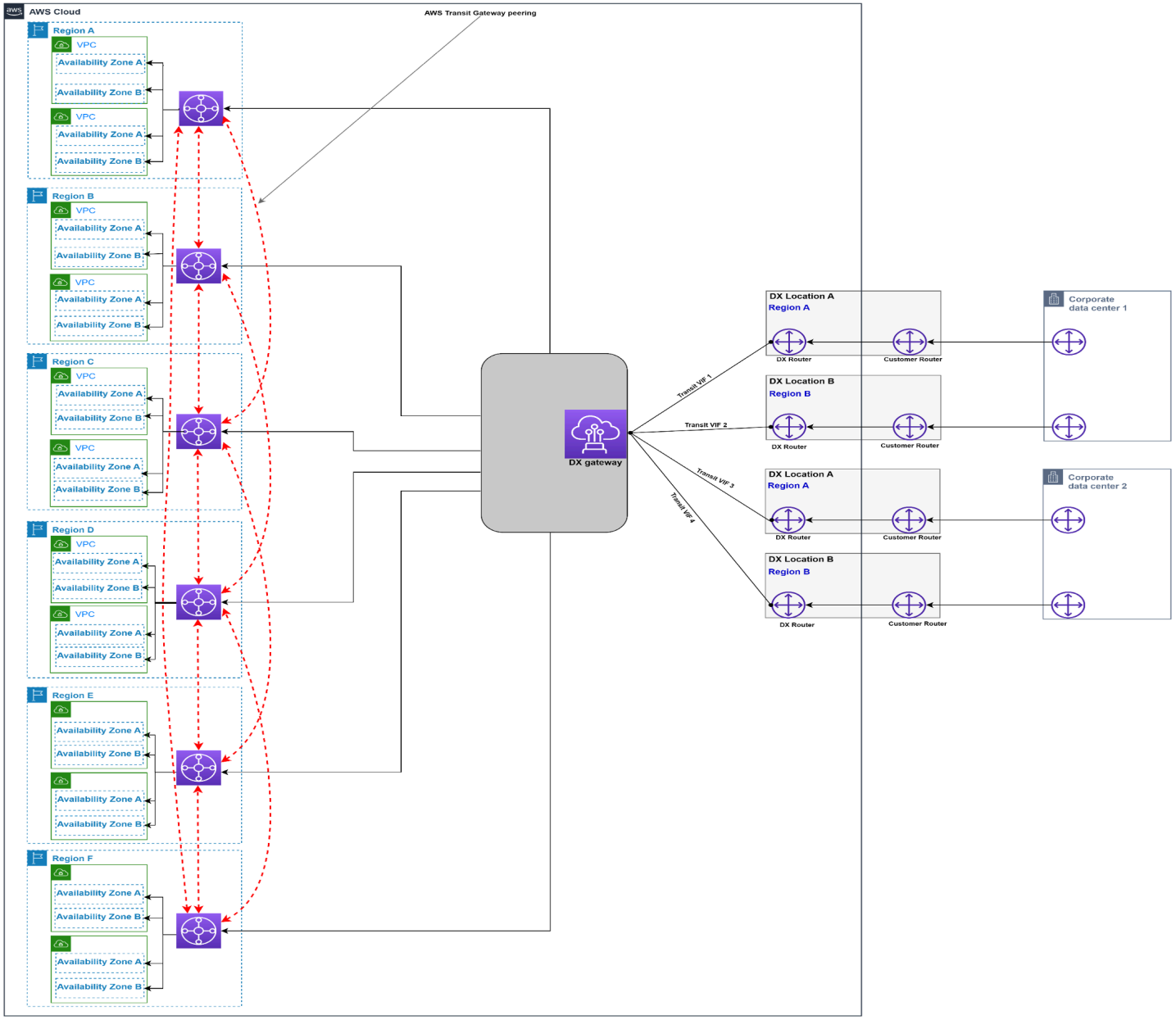

그림 8 – AWS DX – AWS Transit Gateway, 다중 리전(3개 이상) DXGW 포함

연결 모델 속성:

- 운영 오버헤드가 가장 낮습니다.
- AWS DX 퍼블릭VIF은 AWS DX 연결을 통해 S3와 같은 AWS 퍼블릭 리소스에 직접 액세스하는 데 사용됩니다.
- 향후 다른 리전의 VPCs 및 DX 연결에 연결할 수 있는 기능을 제공합니다.

- 에 AWS Transit Gateway 연결하면 간에 VPCs전체 또는 부분 메시 연결을 달성할 수 있습니다 VPCs.
- 리전 간 VPC 통신은 AWS Transit Gateway 피어링을 통해 촉진됩니다.
- 타사 보안 및 SDWAN 가상 어플라이언스를 와 통합할 수 있는 유연한 설계 옵션을 제공합니다 AWS Transit Gateway. 및 온프레미스에서 VPC 트래픽 에 대한 VPC-to-VPC 중앙 집중식 네트워크 보안을 참조하세요.

규모 고려 사항:

- 송수신 경로 수는 전송을 통해 지원되는 최대 경로 수로 AWS Transit Gateway 제한됩니다VIF(인바운드 및 아웃바운드 수는 다양함). 규모 제한에 대한 자세한 내용은 AWS Direct Connect 할당량을 참조하세요. 경로 수를 줄이기 위해 필요한 경우 경로 요약을 고려하세요.
- VPCs 에 따라 AWS Transit Gateway 단일 BGP 세션당 최대 수천 개까지 확장합니다DXGW(프로비저닝된 AWS DX 연결로 제공된 성능이 충분하다고 가정).
- 당 최대 6개의 AWS Transit Gateway를 연결할 수 있습니다DXGW.
- 를 사용하여 리전을 3개 이상 연결해야 하는 AWS Transit Gateway경우 추가DXGWs가 필요합니다.
- AWS DXVIF당 단일 전송.
- 필요에 따라 추가 AWS DX 연결을 추가할 수 있습니다.

기타 고려 사항:

- 온프레미스 사이트와 간의 데이터 전송에 대한 추가 AWS Transit Gateway 처리 비용이 발생합니다 AWS.
- 원격 의 보안 그룹은 AWS Transit Gateway (피VPC어링 필요)에서 참조할 수 VPC 없습니다.
- VPC 피어링은 간의 통신을 용이하게 AWS Transit Gateway 하는 대신 사용할 수 VPCs있지만, 이로 인해 대규모로 대규모 VPC point-to-point 피어링을 구축하고 관리하기 위한 운영 복잡성이 가중될 것입니다.

다음 의사 결정 트리는 확장성 및 통신 모델 고려 사항을 다룹니다.

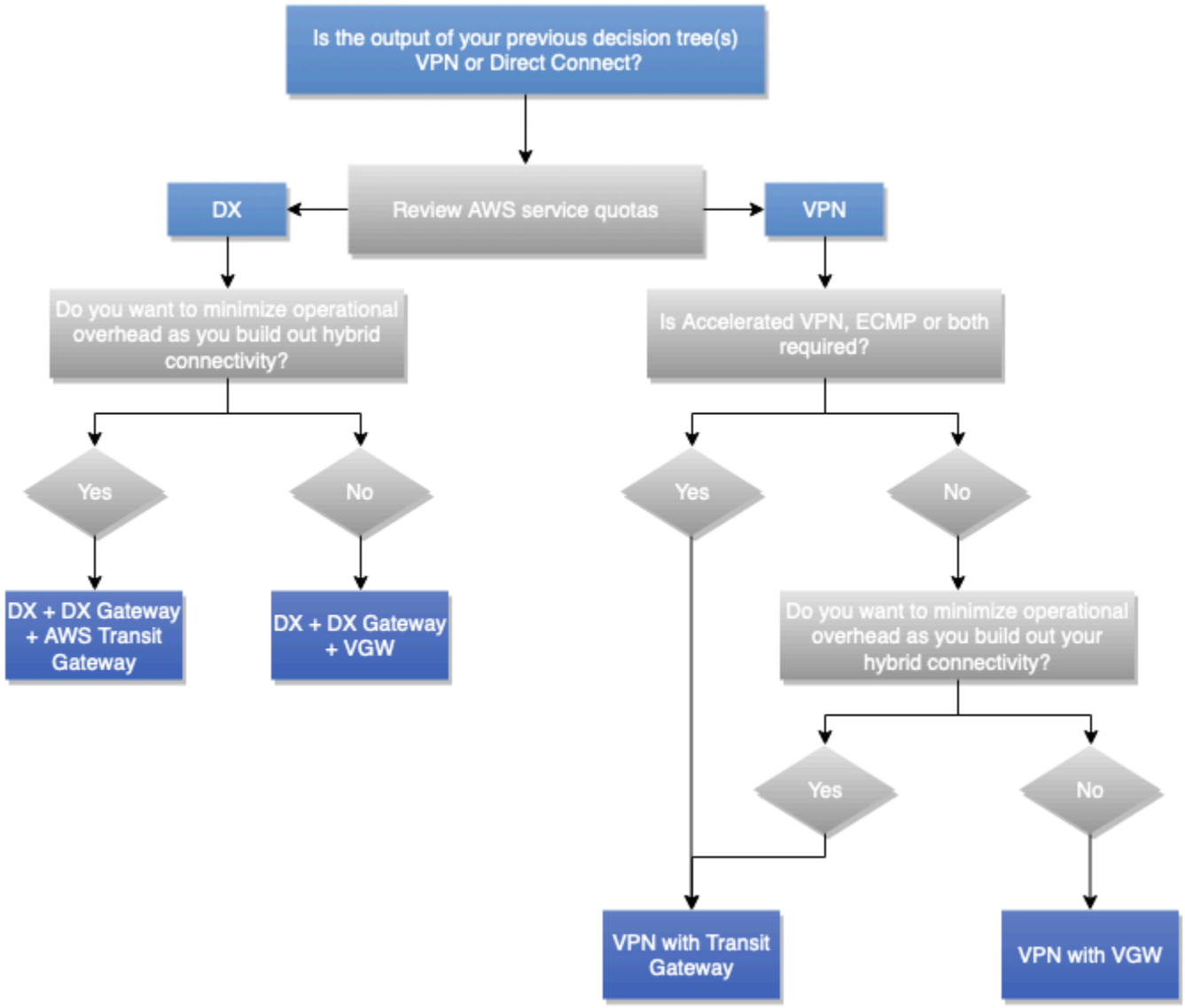

그림 9 - 확장성 및 통신 모델 의사 결정 트리

> **Note**
>
> 선택한 연결 유형이 인 경우 VPN일반적으로 성능 고려 사항에서 VPN 종료 시점이 AWS VGW S AWS Transit Gateway AWS S2S VPN 연결인지 여부를 결정해야 합니다. 아직 수행하지 않은 경우, 결정에 도움이 되도록 VPN 연결(들)에 연결하는 VPC 데 필요한 수와 VPC 함께 간의 필수 통신 모델을 고려할 수 있습니다.

신뢰성

정의

신뢰성이란 필요할 때 서비스 또는 시스템이 예상 기능을 수행할 수 있는 능력을 말합니다. 시스템의 신뢰성은 주어진 기간 내의 운영 품질 수준으로 측정할 수 있습니다. 이는 인프라 또는 서비스 중단으로부터 동적이며 안정적으로 복구할 수 있는 시스템의 능력을 의미하는 복원성과 대조됩니다.

가용성과 복원력을 사용하여 신뢰성을 측정하는 방법에 대한 자세한 내용은 AWS Well-Architected Framework의 신뢰성 요소를 참조하세요.

핵심 질문

가용성

가용성은 워크로드를 사용할 수 있는 시간의 비율입니다. 일반적인 목표에는 99%(연간 허용되는 가동 중지 시간 3.65일), 99.9%(8.77시간), 99.99%(52.6분)가 포함되며, 백분율의 9는 줄여서 표현합니다(99%는 '9 2개', 99.9%는 '9 3개' 등). AWS 와 온프레미스 데이터 센터 간의 네트워킹 솔루션 가용성은 전체 솔루션 또는 애플리케이션 가용성과 다를 수 있습니다.

네트워킹 솔루션의 가용성에 대한 핵심 질문은 다음과 같습니다.

- AWS 내 리소스가 온프레미스 리소스와 통신할 수 없는 경우에도 계속 작동할 수 있나요? 그 반대도 마찬가지인가요?
- 계획된 유지 관리에 대한 예정된 가동 중지 시간은 가용성 지표에 포함시켜야 합니까, 아니면 제외시켜야 합니까?
- 전체 애플리케이션 상태와 별도로 네트워킹 계층의 가용성을 측정하려면 어떻게 해야 합니까?

Well-Architected Framework의 신뢰성 원칙의 가용성 섹션에 가용성 계산을 위한 제안과 공식이 수록되어 있습니다.

복원력

복원력은 인프라 또는 서비스 중단을 복구하고, 수요에 따라 컴퓨팅 리소스를 탄력적으로 확보하고, 구성 오류나 일시적 네트워크 문제 같은 중단 사태를 완화할 수 있는 워크로드의 능력입니다. 다중화 네트워크 구성 요소(링크, 네트워크 디바이스 등)가 자체적으로 예상되는 기능을 제공할 만큼 충분한 가용성을 갖지 못한다면 장애에 대한 복원력이 낮은 것입니다. 그 결과 사용자 경험이 열악해지고 저하됩니다.

네트워킹 솔루션의 복원력에 대한 핵심 질문은 다음과 같습니다.

- 동시에 발생하는 개별 장애는 몇 개까지 허용해야 합니까?
- 연결 솔루션과 내부 네트워크 모두에서 단일 장애 지점을 줄이려면 어떻게 해야 합니까?
- 분산 서비스 거부(DDoS) 이벤트에 대한 취약성은 무엇입니까?

기술 솔루션

먼저, 모든 하이브리드 네트워크 연결 솔루션에 높은 수준의 신뢰성이 필요한 것은 아니며 신뢰성 수준이 높아지면 그에 따라 비용도 증가한다는 점에 유의해야 합니다. 일부 시나리오에서는 다운타임이 비즈니스에 미치는 영향이 더 크기 때문에 기본 사이트에 신뢰할 수 있는 (다중화되어 있으며 복원력이 뛰어난) 연결이 필요할 수 있지만, 지역 사이트는 장애 발생 시 비즈니스에 미치는 영향이 낮기 때문에 동일한 수준의 신뢰성이 필요하지 않을 수 있습니다. AWS Direct Connect 설계에 대한 AWS Direct Connect 높은 복원력을 보장하는 모범 사례를 설명하므로 복원력 권장 사항을 참조하는 것이 좋습니다. AWS

복원력 측면에서 신뢰할 수 있는 하이브리드 네트워크 연결 솔루션을 구현하려면 설계에서 다음 측면을 고려해야 합니다.

- 이중화: 네트워크 연결, 엣지 네트워크 디바이스, 가용 영역 간 이중화, DX 위치 AWS 리전, 디바이스 전원, 광케이블 경로, 운영 체제를 포함하되 이에 국한되지 않는 하이브리드 네트워크 연결 경로의 단일 장애 지점을 제거하는 것을 목표로 합니다. 이 백서의 목적 및 범위를 위해 중복성은 네트워크 연결, 엣지 디바이스(예: 고객 게이트웨이 디바이스), AWS DX 위치 및 AWS 리전 (다수 리전 아키텍처의 경우)에 중점을 둡니다.
- 신뢰할 수 있는 장애 조치 구성 요소: 일부 시나리오에서는 시스템이 작동하지만 필요한 수준에서 기능을 수행하지 못할 수 있습니다. 이러한 상황은 계획된 다중 구성 요소가 중복되지 않은 상태로 작동하는 단일 장애 이벤트 중에 흔히 발생합니다. 즉, 사용량 때문에 네트워킹 부하가 다른 곳으로 갈 곳이 없어 전체 솔루션을 위한 용량이 충분하지 않게 됩니다.
- 장애 조치 시간: 장애 조치 시간은 보조 구성 요소가 기본 구성 요소의 역할을 완전히 인계하는 데 걸리는 시간입니다. 장애 조치 시간에는 장애를 감지하는 데 걸리는 시간, 보조 연결을 활성화하는 데 걸리는 시간, 나머지 네트워크에 변경 사항을 알리는 데 걸리는 시간 등 여러 요소가 있습니다. 링크의 경우 데드 피어 감지(DPD)를 사용하고 VPN 링크의 경우 양방향 전달 감지(BFD)를 사용하여 장애 감지를 개선할 수 있습니다 AWS Direct Connect . 보조 연결을 활성화하는 데 걸리는 시간은 매우 짧거나(이러한 연결이 항상 활성 상태인 경우), 짧은 기간이거나(사전 구성된 VPN 연결을 활성화해야 하는 경우), 더 길 수 있습니다(물리적 리소스를 이동하거나 새 리소스를 구성해야 하는 경우). 나머지 네트워크에 대한 알림은 일반적으로 고객 네트워크 내의 라우팅 프로토콜을 통해 이루어지며, 각 프로토콜의 수렴 시간과 구성 옵션이 다릅니다. 이러한 구성은 본 백서의 범위를 벗어납니다.

- 트래픽 엔지니어링: 복원력이 뛰어난 하이브리드 네트워크 연결 설계의 맥락에서의 트래픽 엔지니어링은 정상 및 장애 시나리오에서 사용 가능한 여러 연결을 통해 트래픽이 어떻게 흘러야 하는지를 해결하는 것을 목표로 합니다. 다양한 장애 시나리오에서 솔루션이 어떻게 작동하는지, 비즈니스에서 수용할 수 있는지 여부를 살펴봐야 하는 design for failure 개념을 따르는 것이 좋습니다. 이 섹션에서는 하이브리드 네트워크 연결 솔루션의 전반적인 복원력 수준을 향상시키는 것을 목표로 하는 몇 가지 일반적인 트래픽 엔지니어링 사용 사례에 대해 설명합니다. AWS Direct Connect 라우팅 및 BGP 트래픽 흐름에 영향을 미치는 여러 트래픽 엔지니어링 옵션(커뮤니티, BGP 로컬 기본 설정, AS 경로 길이)에 대해 설명합니다. 효과적인 트래픽 엔지니어링 솔루션을 설계하려면 각 AWS 네트워킹 구성 요소가 라우팅 평가 및 선택 측면에서 IP 라우팅을 처리하는 방법과 라우팅 선택에 영향을 미칠 수 있는 메커니즘을 잘 이해해야 합니다. 이에 대한 자세한 내용은 이 문서에서 다루지 않습니다. 자세한 내용은 Transit Gateway Route Evaluation Order , Site-to-Site VPN Route Priority , Direct Connect Routing 및 BGP 필요한 경우 설명서를 참조하세요.

> **Note**
>
> VPC 라우팅 테이블에서 추가 라우팅 선택 규칙이 있는 접두사 목록을 참조할 수 있습니다. 이 사용 사례에 대한 자세한 내용은 접두사 목록의 라우팅 우선 순위를 참조하세요. AWS Transit Gateway 라우팅 테이블은 접두사 목록도 지원하지만 적용되면 특정 라우팅 항목으로 확장됩니다.

더 구체적인 경로를 사용한 이중 Site-to-Site VPN 연결 예제

이 시나리오는 인터넷을 통해 에 대한 중복 VPN 연결을 통해 단일 AWS 리전 에 연결하는 소규모 온프레미스 사이트를 기반으로 합니다 AWS Transit Gateway. 그림 10에 나와 있는 트래픽 엔지니어링 설계에서는 트래픽 엔지니어링을 통해 경로 선택에 영향을 주어 하이브리드 연결 솔루션 신뢰성을 높이는 다음과 같은 이점을 얻을 수 있음을 보여줍니다.

- 복원력 있는 하이브리드 연결: 중복 VPN 연결은 각각 동일한 성능 용량을 제공하고, 동적 라우팅 프로토콜(BGP)을 사용하여 자동 장애 조치를 지원하며, VPN 데드 피어 감지를 사용하여 연결 장애 감지 속도를 높입니다.
- 성능 효율성: 전체 VPN 연결 대역폭을 최대화하는 데 도움이 되도록 AWS Transit Gateway 두 VPN 연결ECMP에 걸쳐 를 구성합니다. 또는 사이트 요약 경로와 함께 서로 다른 보다 구체적인 경로를 광고하여 두 VPN 연결에서 부하를 독립성으로 관리할 수 있습니다.

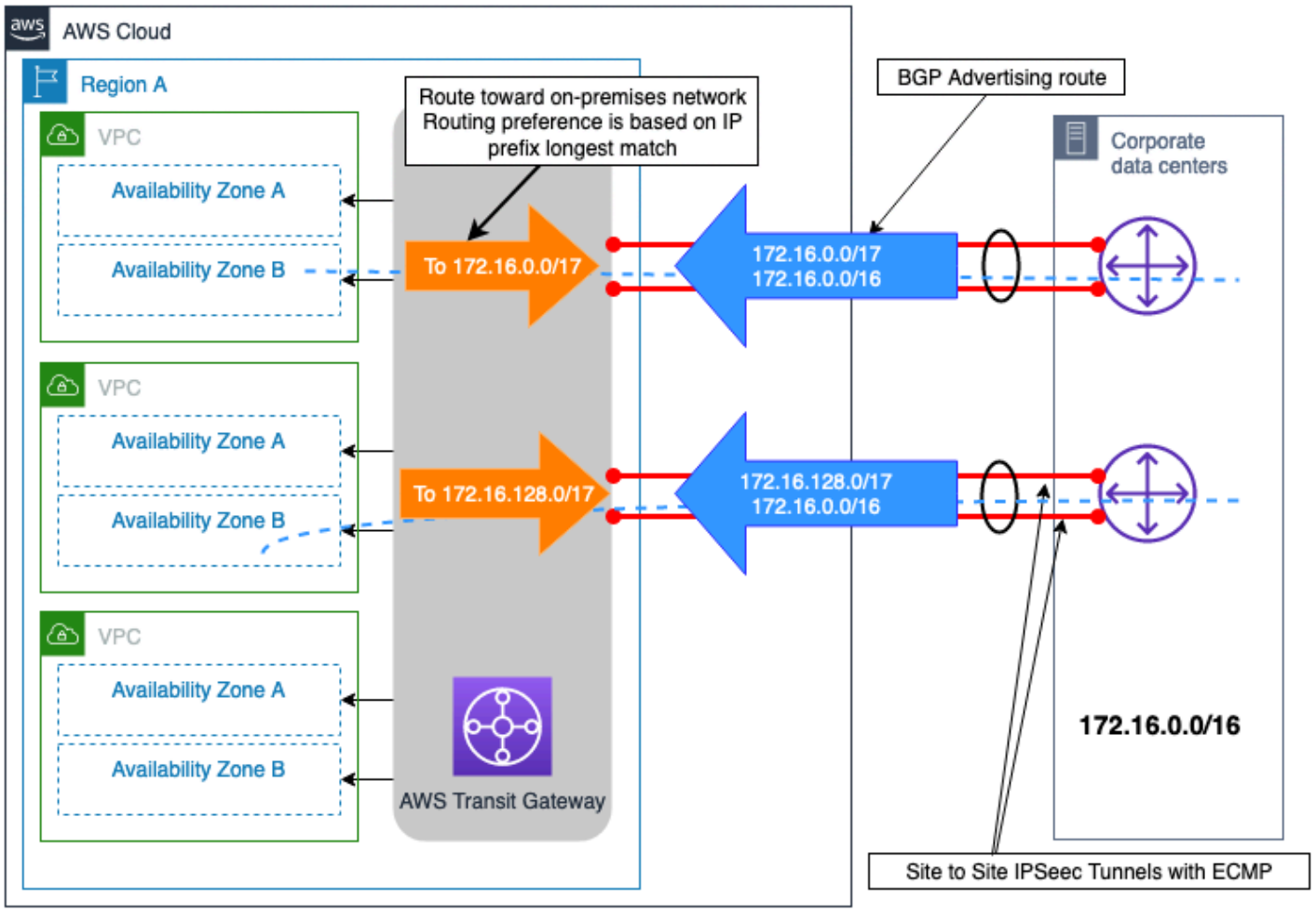

그림 10 - 더 구체적인 경로를 사용한 이중 Site-to-Site VPN 연결 예제

다중 DX 연결이 있는 이중 온프레미스 사이트 예시

그림 11에 나와 있는 시나리오는 서로 다른 지리적 리전에 위치하고 DXGW 및 와 AWS Direct Connect 함께 AWS 를 사용하여 최대 복원력 연결 모델(AWS Direct Connect 복원력 권장 사항 에 설명됨)을 사용하는 에 연결된 두 개의 온프레미스 데이터 센터 사이트를 보여줍니다VGW. 이 두 온프레미스 사이트는 데이터 센터 상호 연결(DCI) 링크를 통해 서로 상호 연결됩니다. 원격 지사 사이트에 속하는 온프레미스 IP 접두사(192.168.0.0/16)는 두 온프레미스 데이터 센터 사이트 모두에서 광고됩니다. 이 접두사의 기본 경로는 데이터 센터 1이어야 합니다. 원격 지사 사이트를 오가는 트래픽은 데이터 센터 1 또는 두 DX 위치 모두에 장애가 발생할 경우 데이터 센터 2로 장애 조치됩니다. 또한 각 데이터 센터에는 사이트별 IP 접두사가 있습니다. 이러한 접두사는 두 DX 위치 모두에 장애가 발생할 경우를 대비하여 다른 데이터 센터 사이트를 통해 직접 연결해야 합니다.

BGP 커뮤니티 속성을 에 보급된 경로와 연결하면 측면에서 AWS DXGW 송신 경로 선택에 영향을 미칠 AWS DXGW수 있습니다. 이러한 커뮤니티 속성은 광고된 경로에 할당된 AWS의 BGP 로컬 기본 설정 속성을 제어합니다. 자세한 내용은 AWS DX 라우팅 정책 및 BGP 커뮤니티 를 참조하세요.

AWS 리전 수준에서 연결의 신뢰성을 극대화하기 위해 각 AWS DX 연결 쌍은 각 온프레미스 사이트와 간의 데이터 전송에 동시에 둘 다를 사용할 수 ECMP 있도록 를 구성합니다 AWS.

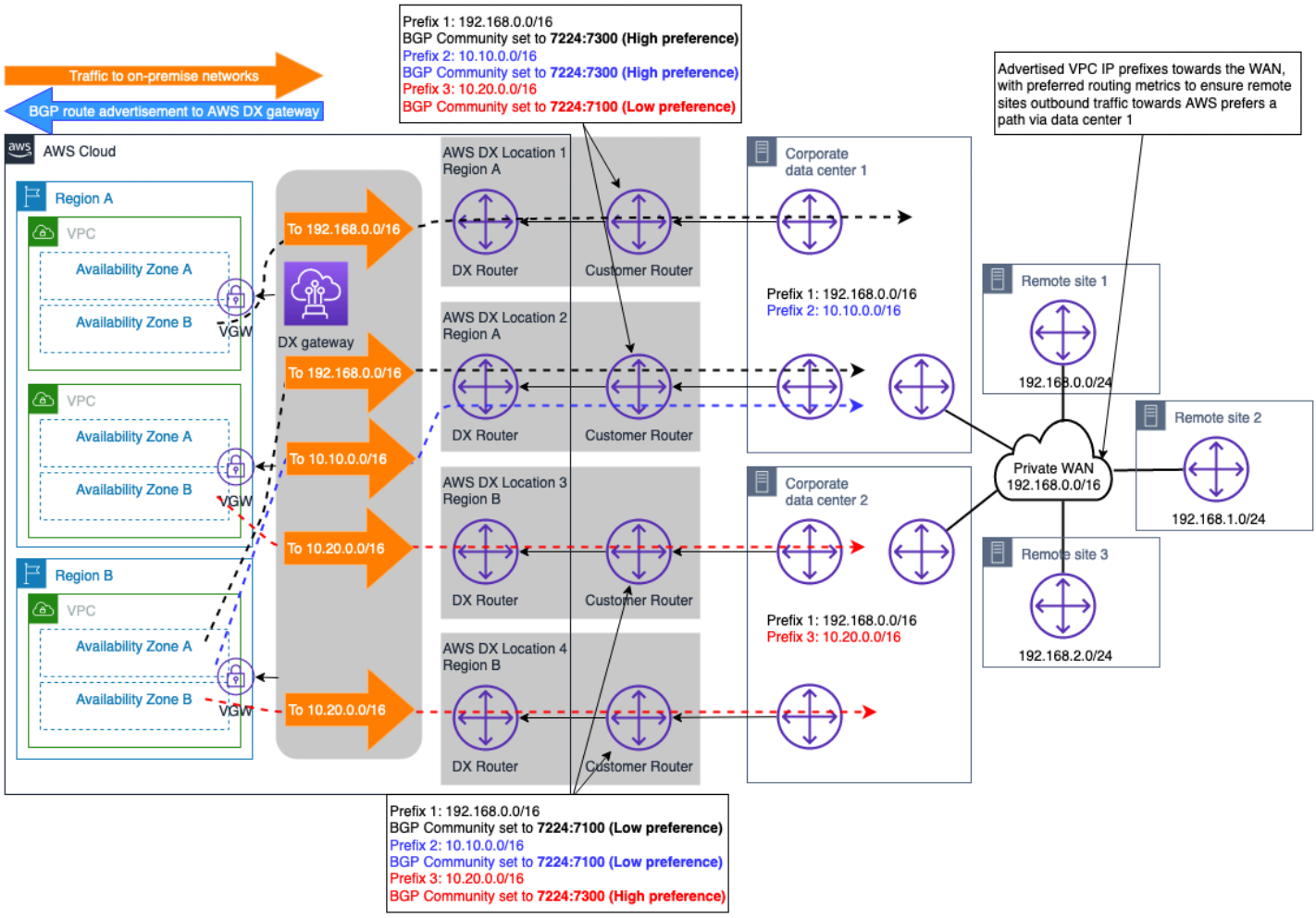

그림 11 - 다중 DX 연결이 있는 이중 온프레미스 사이트 예시

이 설계를 사용하면 온프레미스 네트워크(광고된 접두사 길이와 BGP 커뮤니티가 동일한)로 향하는 트래픽 흐름이 를 사용하여 사이트당 듀얼 DX 연결에 분산됩니다ECMP. 그러나 ECMP가 DX 연결 전반에 걸쳐 필요하지 않은 경우 앞서 논의되고 라우팅 정책 및 BGP 커뮤니티 설명서에 설명된 것과 동일한 개념을 사용하여 DX 연결 수준에서 경로 선택을 추가로 엔지니어링할 수 있습니다.

참고: 온프레미스 데이터 센터 내의 경로에 보안 디바이스가 있는 경우 이러한 디바이스는 하나의 DX 링크를 통해 나가고 동일한 데이터 센터 사이트 내의 다른 DX 링크(두 링크 모두 에서 사용됨ECMP)에서 들어오는 트래픽 흐름을 허용하도록 구성해야 합니다.

VPN AWS DX 연결에 대한 백업으로서의 연결 예제

VPN 는 연결에 백업 네트워크 연결을 제공하도록 선택할 수 있습니다 AWS Direct Connect . 일반적으로 이러한 유형의 연결 모델은 인터넷을 통한 예측 불가능한 성능으로 인해 전체 하이브리드 연결 솔루션에 더 낮은 수준의 안정성을 제공하고 퍼블릭 인터넷을 통한 연결에 대해 얻을 SLA 수 있는 것은 없기 때문에 비용에 의해 구동됩니다. 유효하고 비용 효율적인 연결 모델이므로 비용이 최우선 고려 사항이고 예산이 제한적일 때 사용하거나 보조 DX를 프로비저닝할 수 있을 때까지 임시 솔루션으로 사용해야 합니다. 그림 12는 이 연결 모델의 설계를 보여줍니다. VPN 와 DX 연결이 모두 에서 종료되는 이 설계의 한 가지 주요 고려 AWS Transit Gateway사항은 VPN 연결이 에 연결된 DX 연결을 통해 광고할 수 있는 경로에 비해 더 많은 수의 경로를 광고할 수 있다는 것입니다 AWS Transit Gateway. 이로 인해 라우팅이 최적화되지 않는 상황이 발생할 수 있습니다. 이 문제를 해결하기 위한 옵션은 VPN 연결에서 수신한 경로에 대해 고객 게이트웨이 디바이스(CGW)에서 경로 필터링을 구성하여 요약 경로만 수락할 수 있도록 하는 것입니다.

참고: 에서 요약 경로를 생성하려면 요약이 더 구체적인 경로를 따라 전송되도록 라우팅 AWS Transit Gateway 테이블의 임의의 연결에 대한 정적 경로를 지정 AWS Transit Gateway해야 합니다.

AWS Transit Gateway 라우팅 테이블의 관점에서 온프레미스 접두사에 대한 경로는 접두사 길이VPN가 동일한 AWS DX 연결(를 통해DXGW)과 에서 모두 수신됩니다. 의 라우팅 우선 순위 로직 AWS Transit Gateway에 따라 Direct Connect를 통해 수신된 경로는 를 통해 Site-to-Site 수신된 경로보다 선호도가 높VPN으므로 를 통한 경로 AWS Direct Connect 가 온프레미스 네트워크(들)에 도달하는 것이 선호됩니다.

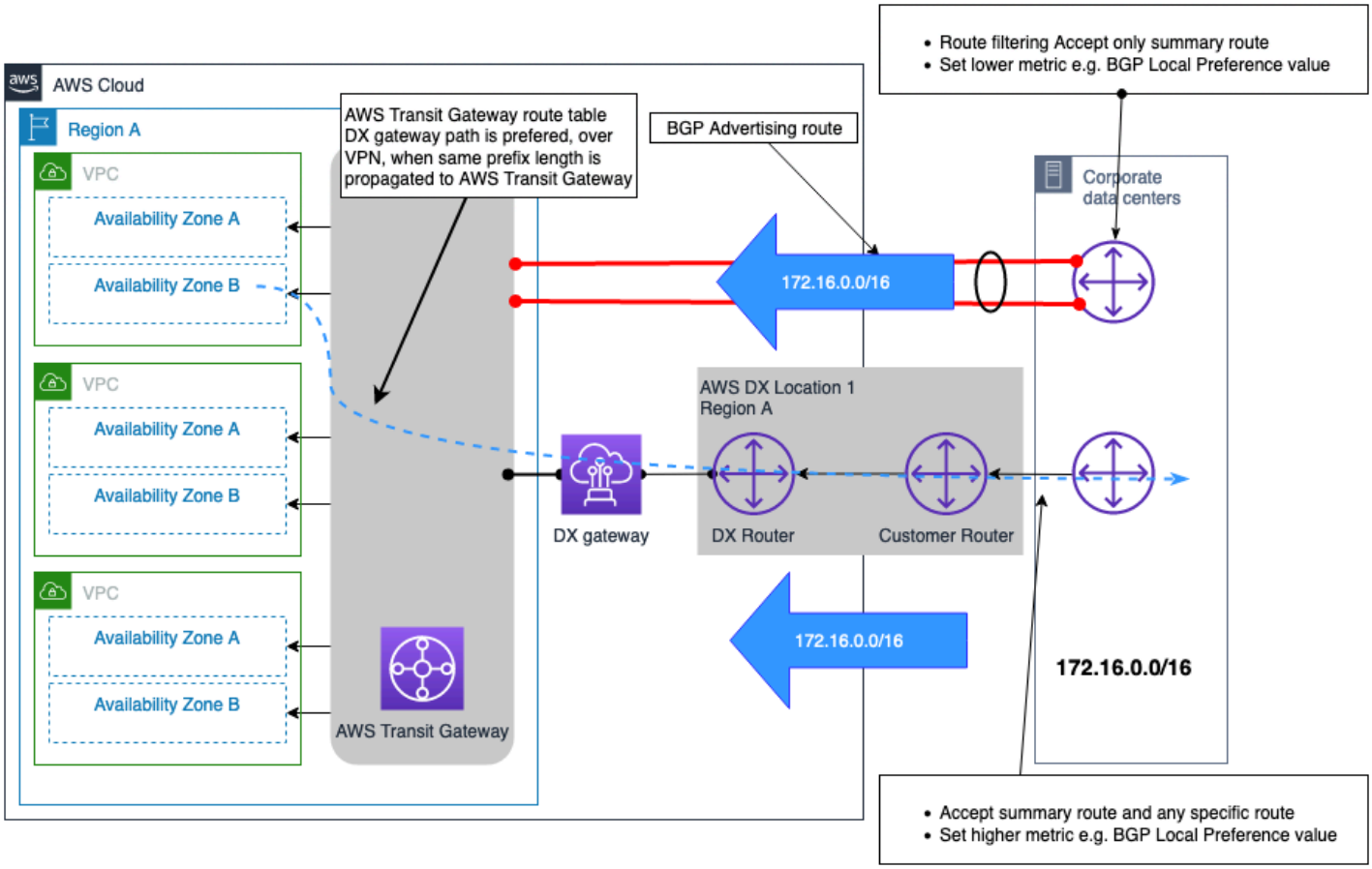

그림 12 - AWS DX VPN 연결에 대한 백업으로서의 연결 예제

다음 의사 결정 트리는 복원력이 뛰어나고 안정적인 하이브리드 네트워크 연결을 달성하기 위해 원하는 결정을 내리는 과정을 안내합니다. 자세한 내용은 AWS Direct Connect Resiliency Toolkit을 참조하세요.

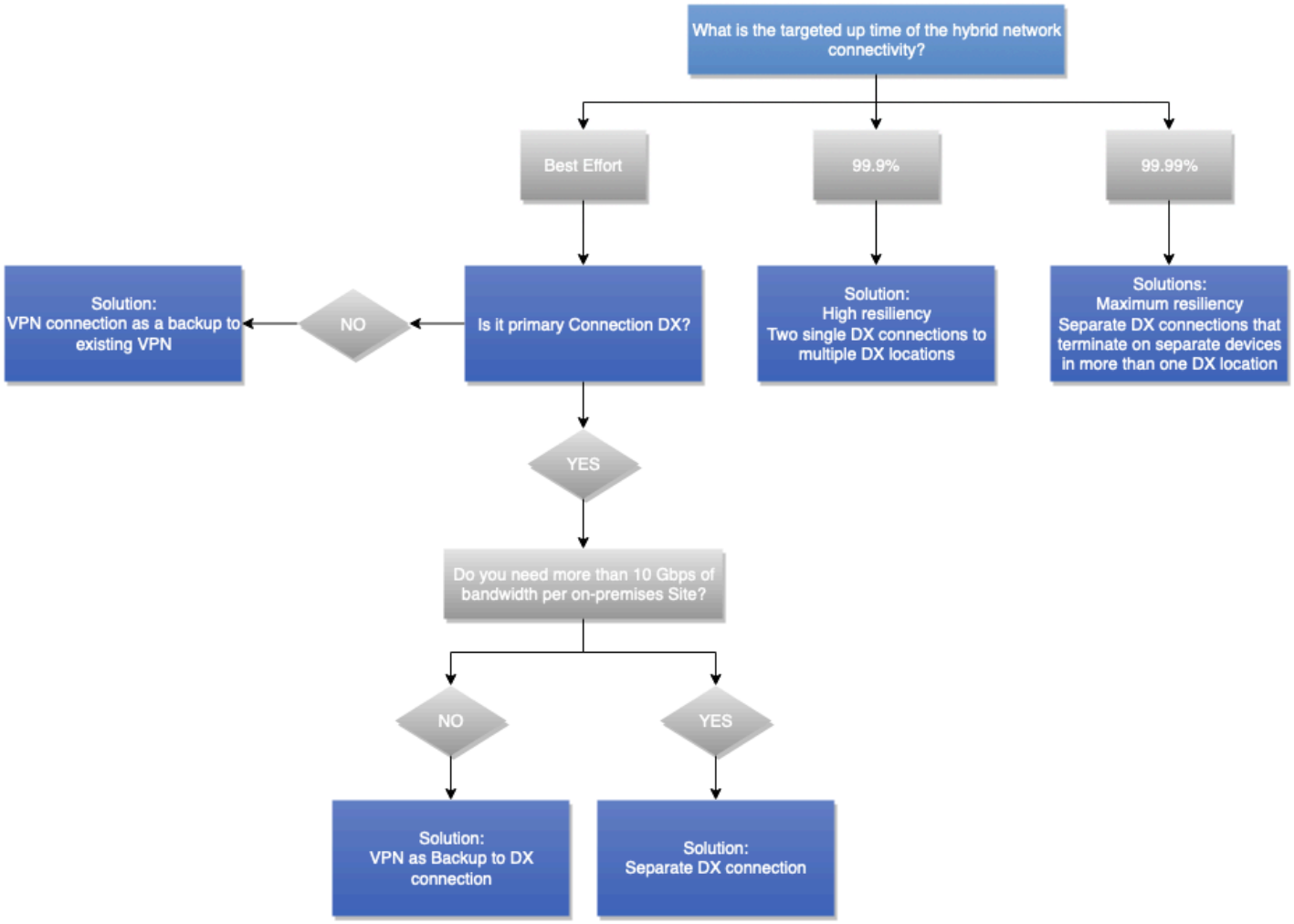

그림 13 - 신뢰성 의사 결정 트리

고객 관리형 VPN 및 SD-WAN

정의

인터넷 연결은 필수이며 사용 가능한 대역폭은 매년 계속 증가하고 있습니다. 일부 고객은 프라이빗 를 구축하고 운영하는 대신 인터넷 WAN 위에 가상 를 빌드하기로 선택합니다WAN. 소프트웨어 정의 광역 네트워크(SD-WAN)를 통해 기업은 소프트웨어를 WAN 스마트하게 사용하여 이 가상을 중앙에서 신속하게 프로비저닝하고 관리할 수 있습니다. 다른 고객은 사이트 에 기존 자체 관리형 사이트를 채택하기로 선택합니다VPNs.

설계 결정에 미치는 영향

SDWAN 및 고객 관리형 는 인터넷 또는 를 통해 실행할 VPNs 수 있습니다 AWS Direct Connect. SD-WAN(또는 소프트웨어 VPN 오버레이)는 기본 네트워크 전송만큼 안정적입니다. 따라서 이 백서의 앞

부분에서 설명한 신뢰성과 SLA 고려 사항은 여기에 적용됩니다. 예를 들어 인터넷을 통해 SD 오버레이WAN를 구축해도 를 통해 구축된 경우와 동일한 안정성을 제공하지 않습니다 AWS Direct Connect.

요구 사항 정의

- 온프레미스 네트워크에서 SD-WAN를 사용하십니까?
- VPN 종료에 사용되는 특정 가상 어플라이언스에서만 사용할 수 있는 특정 기능이 필요합니까?

기술 솔루션

AWS 는 SD-WAN를 와 통합하는 것을 권장하며 AWS Transit Gateway통합을 지원하는 AWS Transit Gateway 공급업체 목록을 게시합니다. AWS 는 SD-WAN 사이트의 허브 또는 스포크 사이트 역할을 할 수 있습니다. 백본은 AWS 에 배포된 다양한 SD 허브WAN를 매우 안정적이고 성능이 뛰어난 네트워크 AWS 와 연결하는 데 사용할 수 있습니다. SD-WAN 솔루션은 단일 관리 창에서 사용 가능한 경로, 추가 모니터링 및 관찰 기능을 통해 자동 장애 조치를 지원합니다. 자동 구성 및 자동화를 폭넓게 사용하면 기존 에 비해 신속한 프로비저닝 및 가시성이 가능합니다WANs. 그러나 터널링 및 암호화 오버헤드의 사용은 프라이빗 연결에 사용되는 전용 고속 파이버 링크와 비교할 수 없습니다.

경우에 따라 VPN 기능이 있는 가상 어플라이언스를 사용하도록 선택할 수 있습니다. 자체 관리형 가상 어플라이언스를 선택하는 이유에는 기술적 특징 및 나머지 네트워크와의 호환성 등이 있습니다. EC2 인스턴스에 배포된 가상 어플라이언스를 사용하는 자체 관리형 VPN 또는 SD-WAN 솔루션을 선택하면 해당 어플라이언스를 관리할 책임이 있습니다. 또한 가상 어플라이언스 간의 고가용성 및 장애 조치도 사용자 책임입니다. 이러한 설계는 운영 책임을 증가시키지만 더 많은 유연성을 제공할 수 있습니다. 솔루션의 특징과 기능은 선택한 가상 어플라이언스에 따라 달라집니다.

AWS Marketplace 에는 고객이 Amazon 에 배포할 수 있는 많은 VPN 가상 어플라이언스가 포함되어 있습니다EC2. AWS 는 AWS 관리형 S2S로 시작하고 요구 사항을 충족하지 않는 경우 다른 옵션을 VPN 살펴볼 것을 권장합니다. 가상 어플라이언스의 관리 오버헤드는 고객의 책임입니다.

Example Corp. Automotive에서의 사용 사례

백서의 이 섹션에서는 최적의 하이브리드 네트워크 설계를 결정하는 데 도움이 되는 고려 사항, 요구 사항 정의 질문 및 의사 결정 트리를 사용하는 방법을 보여줍니다. 요구 사항은 의사 결정 트리의 입력으로 사용되므로 요구 사항을 식별하고 파악하는 것이 중요합니다. 요구 사항을 미리 파악하면 추가 설계 반복을 피할 수 있습니다. 설계를 다시 검토해야 하는 경우 프로젝트를 완전히 중단하고 귀중한 리소스를 보류하는 것을 최소화할 수 있으며, 요구 사항을 미리 이해하면 이상적으로는 이러한 상황을 피할 수 있습니다.

Example Corp. Automotive는 이 섹션 전체에서 예시 고객으로 사용될 것입니다. 이 회사는 처음에 AWS에서 첫 번째 분석 프로젝트를 배포하려고 합니다. 이 분석 프로젝트는 회사에서 제조하는 자동차의 데이터와 회사 데이터 센터에 이미 존재하는 기타 데이터 세트를 분석하는 데 중점을 두고 있습니다. 처음에 이 회사의 아키텍처 그룹은 프로덕션 및 개발 환경을 호스팅하기 위해 AWS 계정 계정과 Amazon VPC, 그리고 몇 개의 서브넷이 필요할 것이라고 생각했습니다. 프로젝트 팀은 빨리 시작하고 싶어서 가능한 한 빨리 개발 환경 액세스를 요청했습니다. 이들은 지금부터 3개월 후에 프로덕션에 들어가는 것을 목표로 하고 있습니다.

Example Corp. Automotive는 또한 향후 6개월 동안 ERP 시스템, 가상 데스크톱 인프라(VDI) 및 기타 20개 애플리케이션을 온프레미스에서 AWS로 마이그레이션하는 등 여러 추가 프로젝트에 AWS를 사용할 계획입니다. 추가 프로젝트에 대한 일부 요구 사항은 아직 정의 중이지만 AWS 클라우드 사용량이 증가할 것이라는 점은 분명합니다.

아키텍처 팀은 이 백서에 설명된 접근 방식을 활용하기로 결정했습니다. 각 고려 사항 아래에 설명된 요구 사항 정의 질문을 사용하여 설계 결정을 내리는 데 필요한 정보를 수집했습니다.

이러한 요구 사항은 다음 표에 요약되어 있는 연결 유형과 관련된 요구 사항부터 시작합니다.

표 4 - Example Automotive Corp의 신뢰성 입력

연결 유형 선택 고려 사항	요구 사항 정의 질문	답변
배포 시간	배포에 필요한 일정은 어떻게 됩니까? 몇 시간, 며칠, 몇 주 또는 몇 달입니까?	• 개발 및 테스트: 1개월 • 프로덕션: 3개월
보안	보안 요구 사항 및 정책에 따라 인터넷을 통한 암호화된 연결을 사용하여 AWS에 연결하도	• 개발 및 테스트: Site-to-Site VPN 허용

연결 유형 선택 고려 사항	요구 사항 정의 질문	답변
	록 허용합니까, 아니면 프라이빗 네트워크 연결 사용을 의무화합니까?	• 프로덕션: 프라이빗 네트워크 필요
	프라이빗 네트워크 연결을 활용할 때 네트워크 계층이 전송 중 암호화를 제공해야 합니까?	아니요. 애플리케이션 계층 암호화가 사용됩니다.
SLA	하이브리드 연결 SLA와 서비스 크레딧이 필요합니까?	• 개발 및 테스트: 아니요 • 프로덕션: 예
	가동 시간 목표는 어떻게 됩니까?	• 개발 및 테스트: N/A • 프로덕션: 99.99%
	전체 하이브리드 네트워크가 가동 시간 목표를 준수하고 있습니까?	• 개발 및 테스트: N/A • 프로덕션: 예
성능	필요한 처리량은 얼마입니까?	• 개발 및 테스트: 100Mbps • 프로덕션: 500Mbps, 2Gbps로 성장
	온프레미스 네트워크와 AWS 간의 허용 가능한 최대 지연 시간은 얼마입니까?	• 개발 및 테스트: 까다로운 요구 사항 없음 • 프로덕션: 30ms 미만
	허용 가능한 최대 네트워크 Jitter는 얼마입니까?	• 개발 및 테스트: 까다로운 요구 사항 없음 • 프로덕션: 최소 Jitter 필요
비용	한 달에 얼마나 많은 데이터를 AWS로 전송하시겠습니까?	• 개발 및 테스트: 2TB • 프로덕션: 20TB에서 50TB로 확장

연결 유형 선택 고려 사항	요구 사항 정의 질문	답변
	한 달에 얼마나 많은 데이터를 AWS에서 전송하시겠습니까?	• 개발 및 테스트: 1TB • 프로덕션: 10TB에서 25TB로 확장
	이 연결은 영구적입니까?	예

접수된 요구 사항에 따라 아키텍처 팀은 그림 9의 연결 유형 결정 트리를 따랐습니다. 이를 통해 아키텍처 팀은 개발, 테스트 및 프로덕션 환경의 연결 유형을 결정할 수 있었습니다. 프로덕션 환경의 경우 즉각적인 요구 사항과 향후 요구 사항을 고려했습니다. 개발 및 테스트를 위해 Example Corp. Automotive는 인터넷을 통해 사이트 간 VPN을 구축할 예정입니다. 프로덕션의 경우 서비스 공급자와 협력하여 기업 네트워크를 AWS Direct Connect에 연결할 예정입니다. Example Corp. Automotive는 처음에 Direct Connect 호스팅 연결 사용을 고려했지만, AWS가 제공한 SLA에 대한 요구 사항 때문에 Direct Connect 전용 연결을 선택했습니다.

연결 유형을 결정한 후 다음 단계는 연결 설계 선택에 영향을 미치는 요구 사항을 파악하는 것입니다. 이는 연결을 구성하는 방법, 비즈니스 및 기술 요구 사항을 지원하는 데 사용할 AWS 서비스 등과 같은 논리적 설계와 관련이 있습니다.

확장성 및 통신 모델 요구 사항을 파악하기 위해 아키텍처 팀은 이 백서의 관련 섹션에 있는 요구 사항 정의 질문을 사용했습니다. 이러한 두 고려 사항과 관련된 요구 사항은 다음 표에 요약되어 있습니다.

표 5 - 요구 사항 정의 질문

연결 설계 선택 고려 사항	요구 사항 정의 질문	답변
확장성	온프레미스 사이트에 연결해야 하는 VPC의 현재 또는 예상 수는 몇 개입니까?	처음에는 2개였다가 6개월 만에 30개로 증가
	이러한 VPC는 단일 AWS 리전 리전에 배포됩니까, 아니면 여러 리전에 배포됩니까?	단일 리전
	AWS에 연결해야 하는 온프레미스 사이트는 몇 개입니까?	데이터 센터 2개

연결 설계 선택 고려 사항	요구 사항 정의 질문	답변
	AWS에 연결해야 하는 고객 게이트웨이 디바이스는 사이트당 몇 개 있습니까?	데이터 센터당 라우터 2개
	AWS VPC에 광고될 것으로 예상되는 경로의 수와 AWS측에서 수신될 것으로 예상되는 경로의 수는 몇 개입니까?	• AWS에 광고할 경로: 20개 경로 • AWS에서 수신할 경로: /16 경로 1개
	가까운 장래에 AWS 연결의 대역폭 증가를 고려할 계획이 있습니까?	• 개발 및 테스트: 100Mbps • 프로덕션: 500Mbps, 2Gbps로 성장
연결 디자인 모델	(리전 내 및/또는 리전 간)VPC 간 통신을 활성화해야 하는 요구 사항이 있습니까?	예, AWS 리전 내에 있음
	온프레미스에서 직접 AWS 퍼블릭 엔드포인트 서비스에 액세스해야 합니까?	예
	온프레미스에서 VPC 엔드포인트를 사용하여 AWS 서비스에 액세스해야 합니까?	아니요

아키텍처 팀은 의견을 바탕으로 연결 설계 섹션의 의사 결정 트리를 따랐습니다. 향후 6개월 내에 VPC 수가 2개에서 30개로 증가할 것으로 예상한 후 아키텍처 팀은 연결 및 VPC 간 라우팅을 위한 종료 게이트웨이로 AWS Transit Gateway를 사용하기로 결정했습니다. 독립적인 AWS Transit Gateway는 개발 및 테스트와 AWS Direct Connect와의 프로덕션 연결에 사용되는 VPN 연결을 종료합니다. 분리된 AWS Transit Gateway를 사용하면 변경 관리가 단순해지고 개발 및 테스트 환경과 프로덕션 환경을 명확하게 구분할 수 있습니다. 프로덕션에는 AWS Transit Gateway 때문에 AWS Direct Connect 게이트웨이가 필요합니다. 퍼블릭 VIF는 AWS 퍼블릭 엔드포인트 서비스에 액세스하는 데 사용됩니다. 그림 14는 수집된 요구 사항을 기반으로 의사 결정 트리에서 선택되는 경로를 보여줍니다.

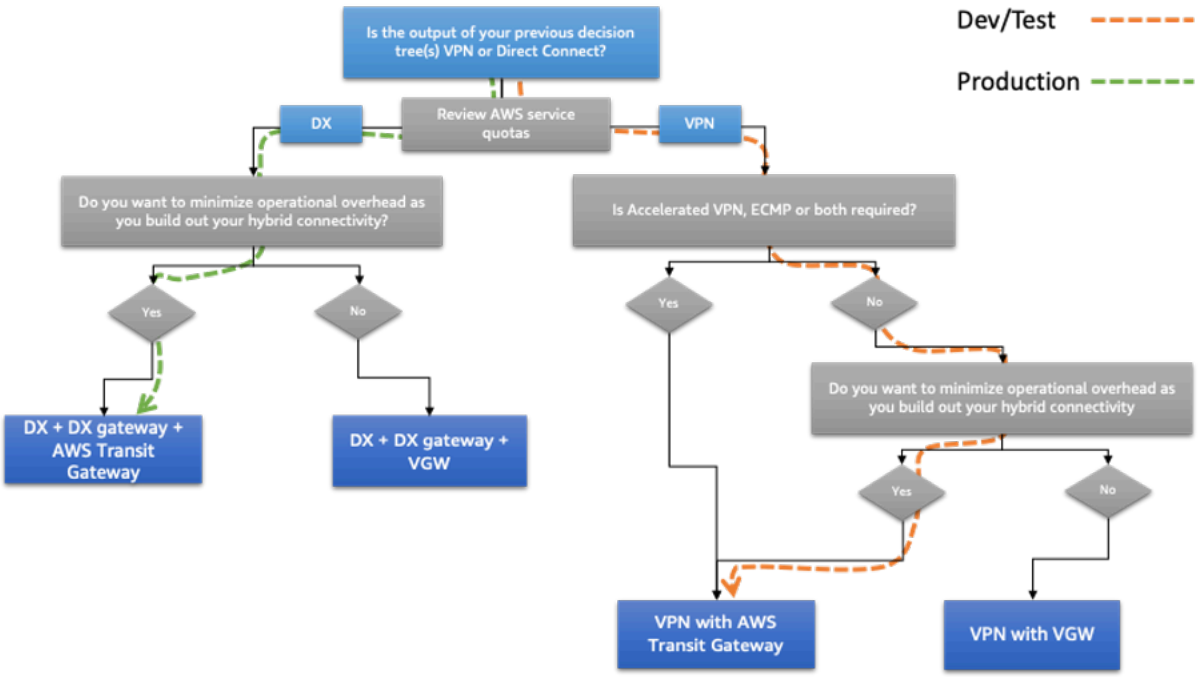

그림 14 - Example Corp. Automotive 연결 설계 의사 결정 트리

확장성 및 통신 모델 요구 사항을 충족하는 솔루션을 결정한 후 다음 단계는 신뢰성과 관련된 요구 사항을 파악하는 것입니다. 이는 필요한 가용성 및 복원력 수준과 관련이 있습니다.

신뢰성 요구 사항을 파악하기 위해 아키텍처 팀은 이 백서의 관련 섹션에 있는 요구 사항 정의 질문을 사용했습니다. 요구 사항은 다음 표에 요약되어 있습니다.

표 6 - 신뢰성 요구 사항 질문

연결 설계 선택 고려 사항	요구 사항 정의 질문	답변
신뢰성	AWS에 대한 연결 장애가 발생할 경우 비즈니스에 미치는 영향은 어느 정도입니까?	• 개발 및 테스트: 낮음 • 프로덕션: 높음
	비즈니스 관점에서 AWS에 대한 연결 실패에 따른 비용이 매우 안정적인 연결 모델을 AWS에 배포하는 데 드는 비용보다 큽니까?	• 개발 및 테스트: 아니요 • 프로덕션: 예

접수된 의견을 바탕으로 아키텍처 팀은 이 백서에서 이전에 다룬 신뢰성 고려 사항 섹션의 의사 결정 트리를 따랐습니다. 아키텍처 팀은 프로덕션 연결의 가동 시간 목표인 99.99% 와 서비스 중단이 발생할 경우 비즈니스에 미치는 영향이 크다는 점을 고려한 후 2개의 Direct Connect 위치를 사용하고 각 온프레미스 데이터 센터에서 각 Direct Connect 위치로 연결되는 2개의 링크를 설치하기로 결정했습니다(총 4개 링크). 개발 및 테스트에 사용되는 VPN 연결에도 추가 이중화를 위해 두 개의 VPN 연결이 사용됩니다. 신뢰성 섹션에서 설명하는 경로 엔지니어링 기술을 사용하여 연결은 다음과 같이 구성됩니다.

- 개발 및 테스트를 위해 기본 데이터 센터로 향하는 2개의 터널을 통해 ECMP를 사용하여 트래픽을 로드 밸런싱할 예정입니다. 이를 통해 처리량을 높일 수 있습니다. 보조 데이터 센터로 연결되는 터널은 기본 터널에 장애가 발생할 경우를 대비해 사용될 예정입니다.
- 프로덕션의 경우 Direct Connect 위치 중 하나를 통한 온프레미스와 AWS 간의 지연 시간은 매우 유사합니다. 이 경우 기본 데이터 센터에 배포된 온프레미스 시스템의 경우 기본 데이터 센터로 가는 두 연결을 통해 AWS와 온프레미스 간의 트래픽을 로드 밸런싱하기로 결정했습니다. 마찬가지로 보조 데이터 센터에서 실행되는 온프레미스 시스템의 경우 보조 데이터 센터로 연결되는 두 연결 간에 트래픽이 로드 밸런싱됩니다. 연결이 실패하는 경우 BGP는 자동 장애 조치를 용이하게 합니다.

그림 15는 수집된 요구 사항을 기반으로 의사 결정 트리에서 선택되는 경로를 보여줍니다.

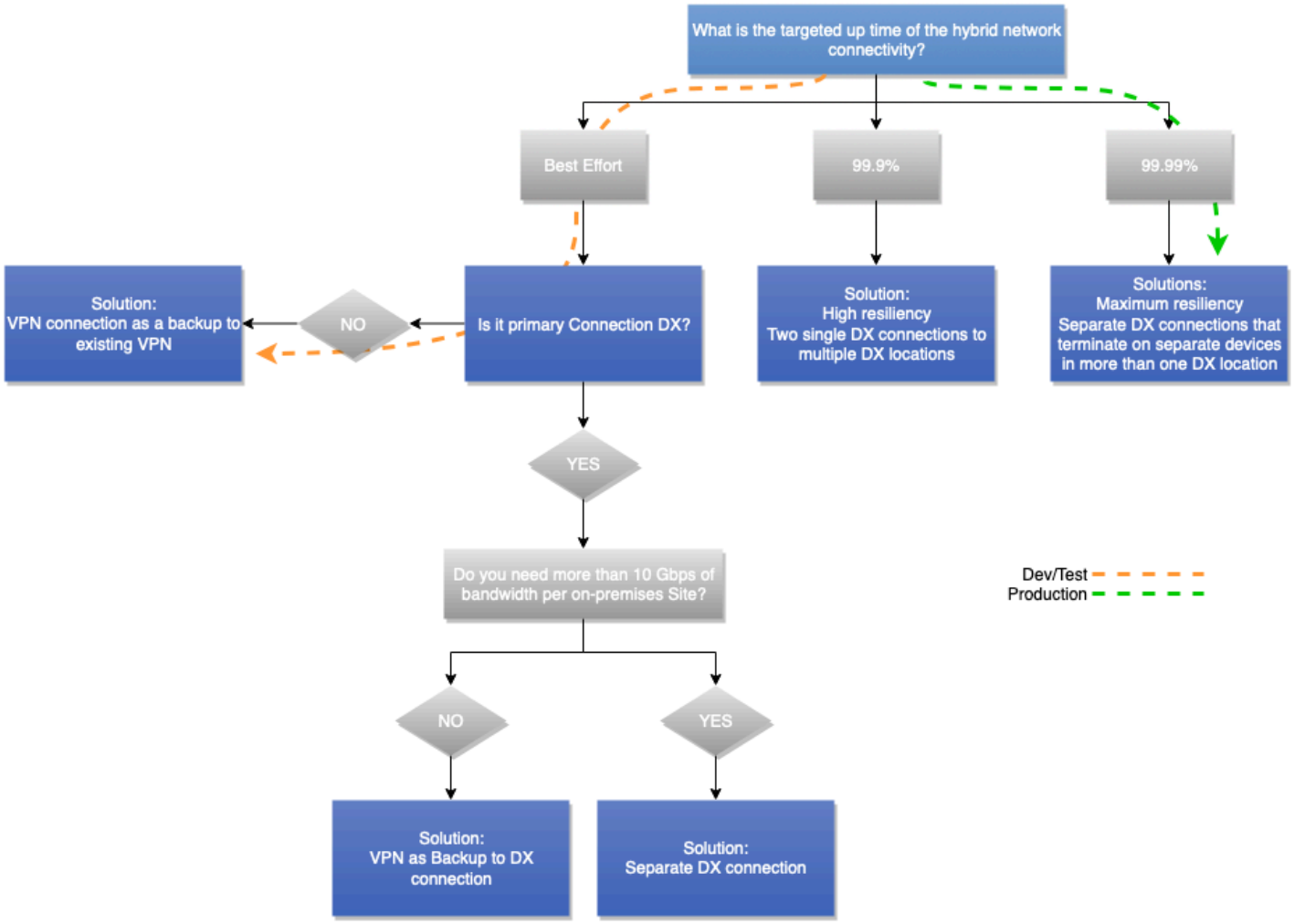

그림 15 - Example Corp. Automotive 신뢰성 의사 결정 트리

Example Corp. Automotive가 선택한 아키텍처

다음 다이어그램은 Example Corp. Automotive가 요구 사항을 수집하고 이 백서의 이전 섹션에서 다룬 의사 결정 트리를 탐색한 후 선택한 아키텍처를 보여줍니다.

아키텍처는 개발 및 테스트를 위해 AWS에서 종료되는 인터넷을 통해 AWS Transit Gateway S2S VPN을 사용합니다. 그런 다음 Direct Connect 게이트웨이와 함께 AWS Direct Connect를 사용하고 프로덕션 트래픽을 위해 두 번째 AWS Transit Gateway를 사용합니다. AWS Transit Gateway는 VPC 간 라우팅에 사용됩니다. 데이터 경로 관점에서 보면 기본 데이터 센터의 VPN 터널은 개발 및 테스트를 위한 기본 경로로 사용되고 보조 데이터 센터의 터널은 장애 조치 경로로 사용됩니다. 프로덕션 트래픽의 경우 모든 연결이 동시에 사용됩니다. AWS 의 트래픽은 온프레미스 시스템이 위치한 데이터 센터를 기반으로 하는 가장 선택적인 네트워크 연결을 선호합니다. Example Corp. Automotive는 유사한 경

로 엔지니어링 기술을 사용하여 트래픽이 AWS로 전송될 때 적절한 경로를 선호하여 대칭적인 트래픽 경로를 사용하여 온프레미스 기본 데이터 센터와 보조 데이터 센터 간의 회사 네트워크 사용을 최소화합니다.

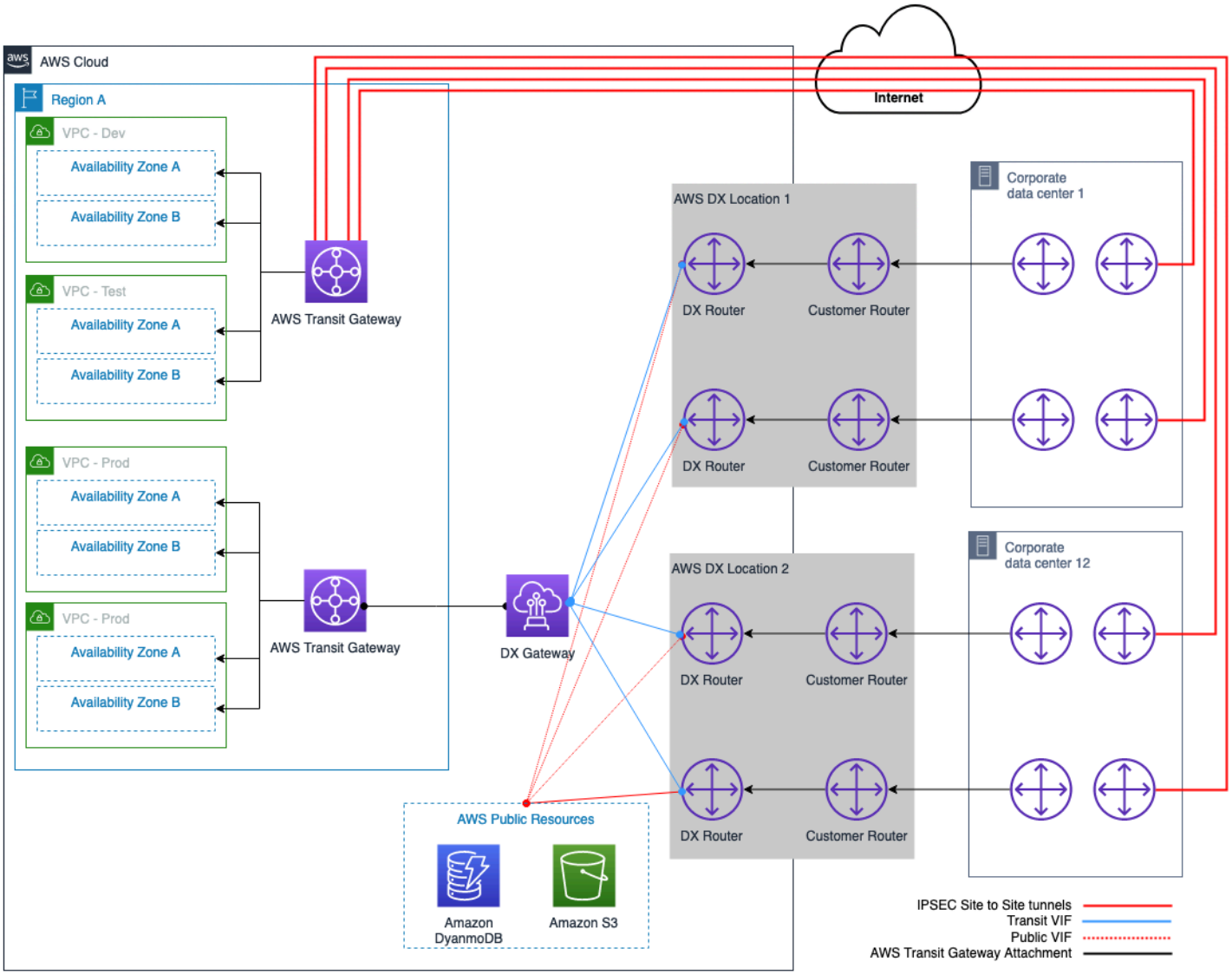

그림 16 - Example Corp. Automotive가 선택한 하이브리드 연결 모델 예시

결론

하이브리드 연결 모델은 클라우드 컴퓨팅 채택을 위한 기본 출발점 중 하나입니다. 이 백서에 설명된 연결 모델 선택 프로세스에 따라 최적의 아키텍처로 하이브리드 네트워크를 구축할 수 있습니다.

프로세스는 논리적인 순서로 정렬된 고려 사항으로 구성됩니다. 이 순서는 노련한 네트워크 및 클라우드 아키텍트가 따르는 멘탈 모델과 매우 비슷합니다. 각 고려 사항 그룹 내에서 의사 결정 트리를 사용하면 입력 요구 사항이 제한적인 경우에도 신속한 연결 모델을 선택할 수 있습니다. 일부 고려 사항과 그에 따른 영향이 서로 다른 솔루션을 가리킬 수도 있습니다. 이러한 경우 의사 결정권자는 일부 요구 사항을 타협하여 비즈니스 및 기술 요구 사항을 충족하는 최적의 솔루션을 선택해야 할 수도 있습니다.

기여자

다음은 이 문서의 기여자입니다.

- James Devine, Principal Solutions Architect, Amazon Web Services
- Andrew Gray, Principal Solutions Architect – Networking, Amazon Web Services
- Maks Khomutskyi, Senior Solutions Architect, Amazon Web Services
- Marwan Al Shawi, Solutions Architect, Amazon Web Services
- Santiago Freitas, Head of Technology, Amazon Web Services
- Evgeny Vaganov, Specialist Solutions Architect – Networking, Amazon Web Services
- Tom Adamski, Specialist Solutions Architect – Networking, Amazon Web Services
- Armstrong Onaiwu, Solutions Architect, Amazon Web Services

참조 자료

- 확장 가능하고 안전한 다중 VPC AWS 네트워크 인프라 구축
- Amazon VPC용 하이브리드 클라우드 DNS 옵션
- Amazon Virtual Private Cloud 연결 옵션
- Amazon Virtual Private Cloud 설명서
- AWS Direct Connect 설명서
- 가상 인터페이스(VIF) 호스팅과 호스팅 연결의 차이점은 무엇인가요?

문서 수정

이 백서에 대한 업데이트 알림을 받으려면 RSS 피드를 구독하면 됩니다.

변경 사항	설명	날짜
마이너 업데이트	DX 할당량 한도 증가를 반영하도록 업데이트되었습니다.	2023년 7월 10일
메이저 업데이트	최신 모범 사례, 서비스 및 기능을 통합하도록 업데이트되었습니다.	2023년 7월 6일
마이너 업데이트	DX 할당량 변경을 반영하도록 참조 아키텍처 다이어그램을 업데이트했습니다.	2023년 6월 27일
마이너 업데이트	끊어진 링크를 수정했습니다.	2022년 3월 22일
최초 게시	백서가 처음 게시되었습니다.	2020년 9월 22일

고지 사항

고객은 본 문서의 정보를 독립적으로 평가할 책임이 있습니다. 본 문서는 (a) 정보 제공의 목적으로만 제공되고, (b) 사전 통지 없이 변경될 수 있는 현재 AWS 제품 및 관행을 나타내고, (c) AWS 및 그 계열사, 공급업체 또는 라이선스 제공자로부터 어떠한 약속이나 보증도 하지 않습니다. AWS 제품 또는 서비스는 명시적이든 묵시적이든 어떠한 종류의 보증, 진술 또는 조건 없이 '있는 그대로' 제공됩니다. 고객에 대한 AWS의 책임 및 채무는 AWS 계약에 준거합니다. 본 문서는 AWS와 고객 간의 어떠한 계약도 구성하지 않으며 이를 변경하지도 않습니다.

AWS 용어집

최신 AWS 용어는 AWS 용어집 참조의 AWS 용어집을 참조하세요.

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