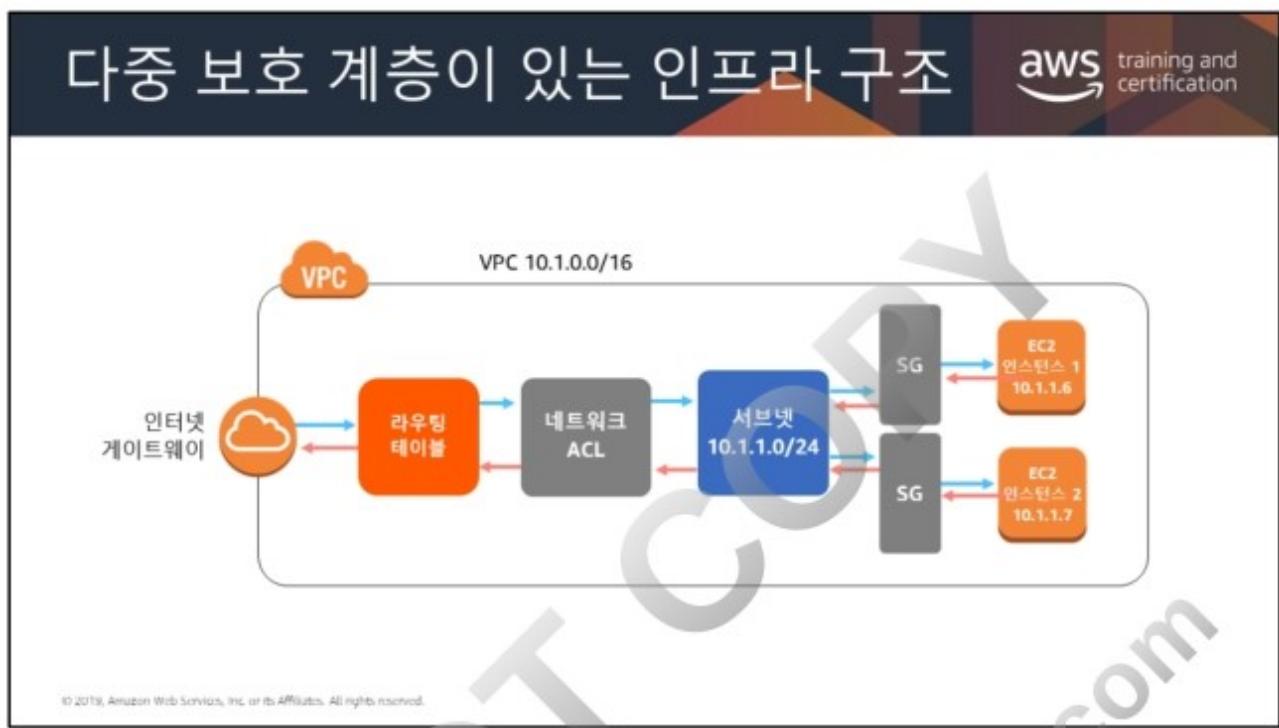


모범 사례는 다중 방어 계층으로 인프라를 보호하는 것입니다. VPC에서 인프라를 실행함으로써 어떤 인스턴스를 인터넷에 먼저 노출할지 제어할 수 있으며, 보안 그룹과 네트워크 ACL을 지정하여 인프라 및 서브넷 수준에서 인프라의 보호를 강화할 수 있습니다. 또한 운영 시스템의 수준에서 방화벽으로 인스턴스를 보호해야 하며, 다른 보안 모범 사례를 따라야 합니다.

AWS 고객은 일반적으로 보안 그룹을 네트워크 패킷 필터링의 기본적인 방법으로 활용합니다. 그 이유는 상태 저장 패킷 필터링을 수행하고 다른 보안 그룹을 참조하는 규칙을 사용할 수 있는 기능을 통해 보안 그룹을 네트워크 ACL 보다 더 다양한 용도로 활용할 수 있기 때문입니다. 그러나 네트워크 ACL은 트래픽의 특정 하위 집합을 거부하거나 서브넷에 대한 고급 수준의 가드 레일을 제공할 때 효과적인 보조 컨트롤로 활용할 수 있습니다.

네트워크 ACL과 보안 그룹을 모두 심층 방어 수단으로 구현하면 이러한 컨트롤 중 한 가지를 잘못 구성하더라도 호스트가 예기치 못한 트래픽에 노출되지 않습니다.



VPC로 트래픽 보내기

aws training and certification

VPC 서브넷의 인스턴스에 대해 인터넷 액세스를 활성화하려면 다음을 수행해야 합니다.

인터넷 게이트웨이를 VPC에 연결합니다.

라우팅 테이블을 인터넷 게이트웨이에 연결합니다.

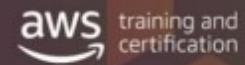
목적지	대상
10.0.0.0/16	로컬
0.0.0.0/0	<igw-id>

인스턴스에 퍼블릭 IP 또는 탄력적인 IP 주소가 있는지 확인합니다.

네트워크 ACL과 SG가 관련 트래픽 흐름을 허용하는지 확인합니다.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

지식 확인 1



VPC는 어디에 배포됩니까?

- 리전
- 가용 영역
- 서브넷
- CIDR 블록

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

DO NOT COPY
zlagusdbs@gmail.com

지식 확인 1



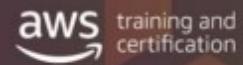
VPC는 어디에 배포됩니까?

- 리전
- 가용 영역
- 서브넷
- CIDR 블록

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

DO NOT COPY
zlagusdbs@gmail.com

지식 확인 2

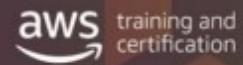


기본적으로 보안 그룹은 모든 수신 트래픽을 허용합니다. 원치 않는 트래픽을 차단하도록 규칙을 설정해야 합니다.

- 참
- 거짓

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

지식 확인 2



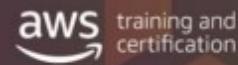
기본적으로 보안 그룹은 모든 수신 트래픽을 허용합니다. 원치 않는 트래픽을 차단하도록 규칙을 설정해야 합니다.

- 참
- 거짓

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



실습 3: Virtual Private Cloud 생성



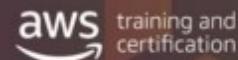
"클라우드에 프라이빗 네트워크가 필요합니다."

사용된 기술:

- Amazon VPC
- VPC 피어링
- 테스트에 Amazon EC2 및 Amazon RDS가 사용됩니다.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

실습 3: Virtual Private Cloud 생성



다음을 사용하여 VPC를 생성합니다.

- 인터넷 게이트웨이
- 퍼블릭 서브넷
- 프라이빗 서브넷
- 각 서브넷에 대한 라우팅 테이블

그런 다음 앱 서버를 실행하고 연결하여 퍼블릭 서브넷을 테스트합니다.



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

실습 3: Virtual Private Cloud 생성

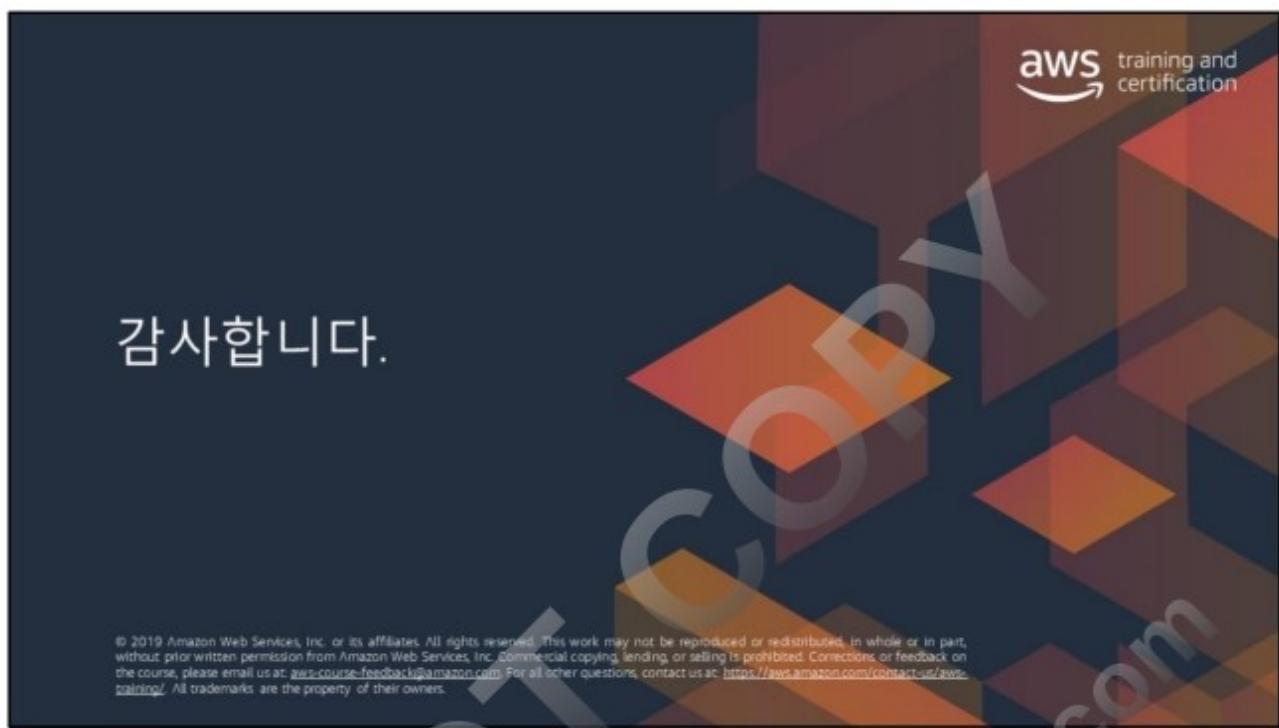
aws training and certification

선택 과제:

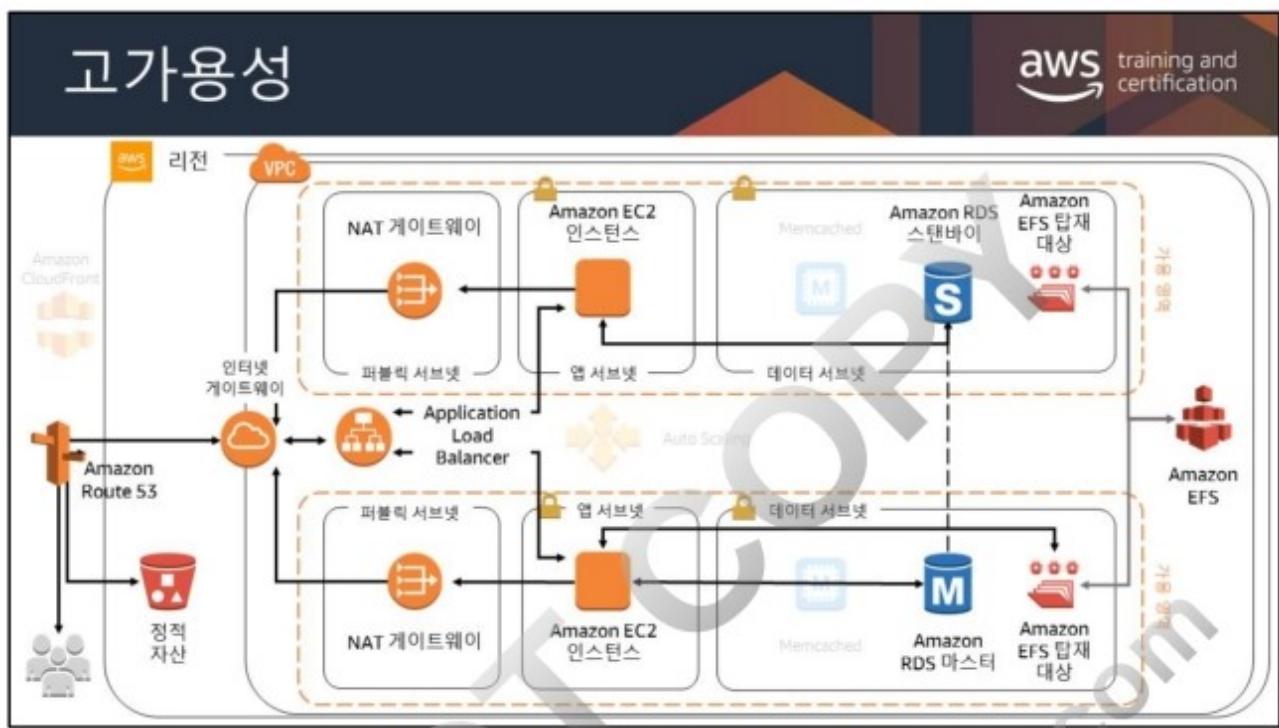
- VPC 피어링 연결 생성
- 라우팅 테이블 구성
- 애플리케이션을 데이터베이스에 연결하여 테스트

시간: 30분

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

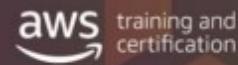






수업이 끝나면 이 아키텍처 디어그램의 모든 구성 요소를 이해할 수 있습니다.
또한 마찬가지로 규모가 크고 강력한 자체 아키텍처 솔루션을 구축할 수
있습니다.

모듈 6



아키텍처 측면에서의 필요성

애플리케이션은 훨씬 더 큰 사용자 기반 및 변동 로드를 지원해야 하며 가용 영역 수준의 장애를 처리해야 합니다.

모듈 개요

- 네트워크 연결
- VPC 엔드포인트
- 로드 밸런싱
- 고가용성

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



가상 프라이빗 게이트웨이(VGW)



Amazon VPC와 다른 네트워크 사이에 프라이빗 연결(VPN)을 설정할 수 있습니다.

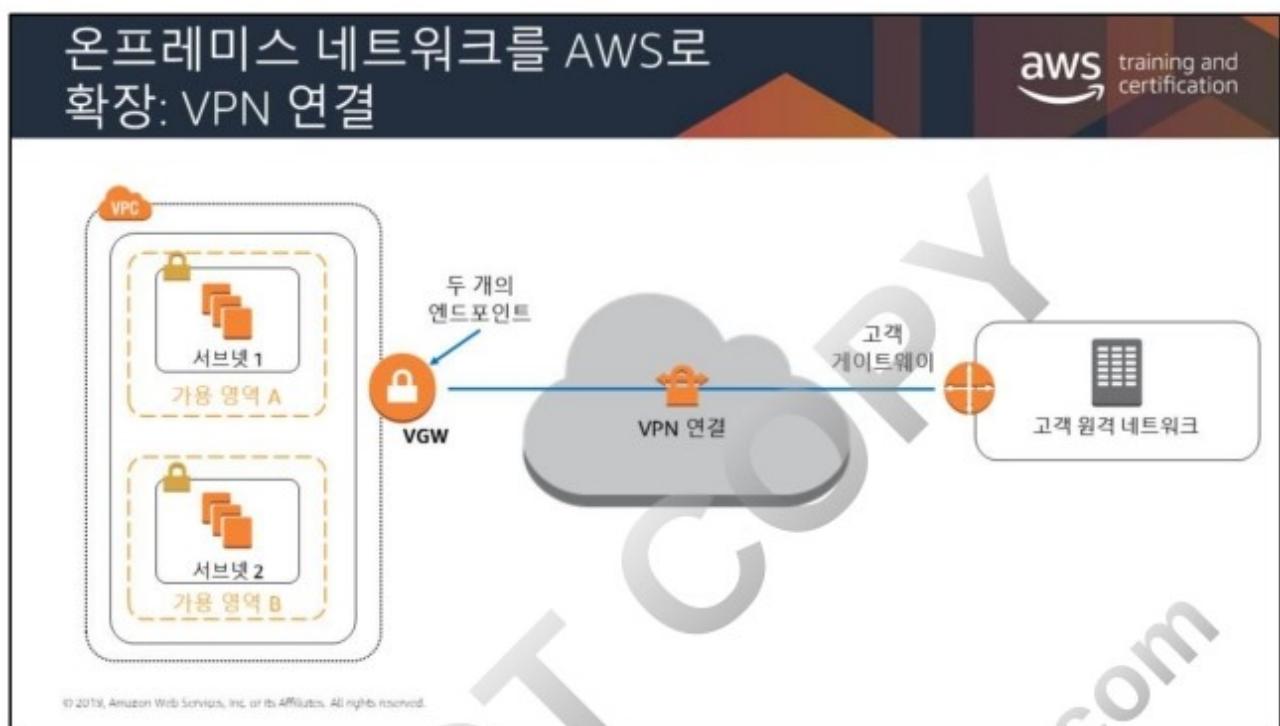
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

기본적으로 Amazon VPC에서 시작하는 인스턴스는 고객의(원격) 네트워크와 통신할 수 없습니다. VPC에 가상 프라이빗 게이트웨이(VGW)를 연결하고, 사용자 지정 라우팅 테이블을 생성하고, 보안 그룹 규칙을 업데이트하고, AWS 관리형 VPN 연결을 생성하여 VPC에서 원격 네트워크에 액세스하도록 할 수 있습니다.

VPN 연결이라는 용어는 일반적인 용어지만, Amazon VPC 설명서에서 VPN 연결은 VPC와 고객 네트워크 사이의 연결을 의미합니다. AWS는 인터넷 프로토콜 보안(IPsec) VPN 연결을 지원합니다.

VGW는 VPN 연결의 Amazon 측 VPN 집선장치입니다. VGW를 만든 후 VPN 연결을 생성할 VPC에 연결합니다.

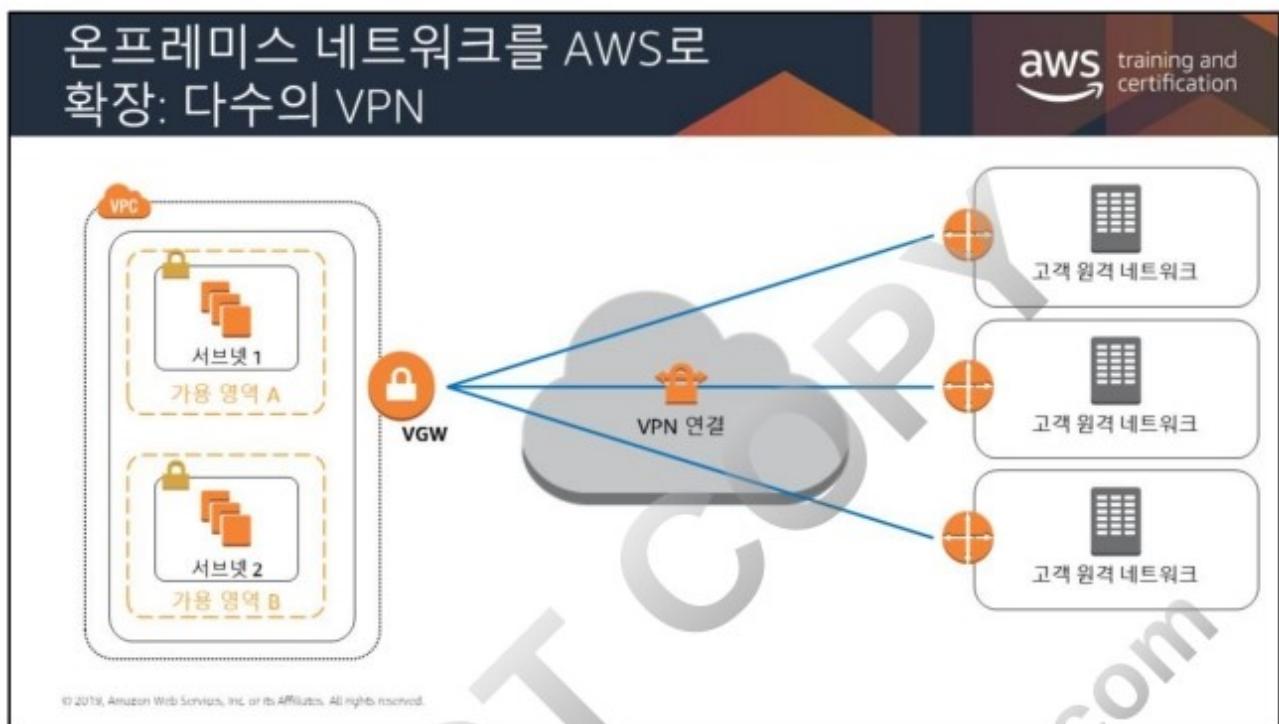
VGW를 생성할 때 Amazon 측 게이트웨이의 프라이빗 ASN(자율 시스템 번호)을 지정할 수 있습니다. ASN을 지정하지 않는 경우 VGW는 기본 ASN(64512)으로 생성됩니다. VGW를 생성한 후에는 ASN을 변경할 수 없습니다.



한 가지 방법은 VPC의 가상 게이트웨이와 데이터 센터 간에 VPN 연결을 사용하는 것입니다. AWS 하드웨어 VPN에서는 기본적인 자동 장애 조치를 지원할 수 있도록 2개의 VPN 엔드포인트가 제공됩니다. AWS 하드웨어 VPN 생성에 대한 자세한 내용은

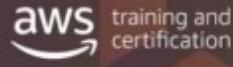
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html을 참조하십시오.

소프트웨어 VPN 어플라이언스를 실행하는 VPC의 Amazon EC2 인스턴스를 사용하여 원격 네트워크에 대한 VPN 연결을 생성할 수도 있습니다. AWS에서는 소프트웨어 VPN 어플라이언스를 제공하거나 유지 관리하지 않지만, AWS Marketplace에서 파트너 및 오픈 소스 커뮤니티가 제공하는 다양한 제품을 선택할 수 있습니다.



이 슬라이드에서 보는 것처럼 고객이 VPN 연결의 고객 측 중복성과 장애 조치를 구현할 수 있도록, AWS의 VGW는 다수의 고객 게이트웨이 연결을 지원 및 권장합니다. 라우팅 구성 시 고객에게 유연성을 제공하도록 동적 및 정적 라우팅 옵션 둘 다 제공됩니다. 동적 라우팅은 BGP 피어링을 사용하여 AWS와 해당 원격 엔드포인트 간에 라우팅 정보를 교환합니다. 또한, 동적 라우팅을 사용하면 고객이 BGP 광고의 가중치(지표), 라우팅 속성 및 정책을 지정하고 네트워크와 AWS 간의 네트워크 경로에 영향을 줄 수 있습니다.

AWS Direct Connect (DX)



AWS Direct Connect (DX)는 1 또는 10Gbps의 전용 프라이빗 네트워크 연결을 제공합니다.



AWS Direct Connect



데이터 전송 비용 감소

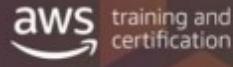


예측 가능한 지표로 애플리케이션 성능 향상

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AWS Direct Connect(DX)는 인터넷을 통한 단순한 연결을 넘어, 중요한 애플리케이션을 위해 AWS 네트워크에 규모, 속도 및 일관성을 가지고 액세스할 수 있는 고유한 솔루션입니다. DX에는 인터넷이 필요하지 않습니다. 대신 사용자의 온프레미스 솔루션과 AWS 간에 프라이빗 네트워크 연결을 사용합니다.

DX 사용 사례



AWS Direct Connect

- 하이브리드 클라우드 아키텍처
- 지속적인 대용량 데이터 세트 전송
- 네트워크 성능 예측 가능성
- 보안 및 규정 준수

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

서비스 이점

DX는 다양한 시나리오에서 유용합니다. 아래에 몇 가지 시나리오가 나와 있습니다.

대용량 데이터 세트 전송

AWS 클라우드와 데이터 센터 간에 전송해야 하는 대용량 데이터 세트에서 작동하는 HPC 애플리케이션을 예로 들어보겠습니다. 이러한 애플리케이션의 경우, DX를 사용해 AWS 클라우드에 연결하는 것이 좋은 해결책이 됩니다. 데이터 센터나 사무실 위치에서 네트워크 전송의 인터넷 대역폭을 두고 경쟁할 필요가 없습니다.

고대역폭 연결은 잠재적 네트워크 혼잡과 애플리케이션 성능 저하를 줄여줍니다.

네트워크 전송 비용 절감

대용량 데이터 세트 전송에 DX를 사용함으로써, 애플리케이션이 사용하는 인터넷 대역폭을 제한할 수 있습니다. 이를 통해 인터넷 서비스 공급자(ISP)에게 지불하는 네트워크 비용을 절감하고 인터넷 대역폭 증가 약정 또는 새로운 계약에 비용을 지불할 필요가 없습니다.

또한, DX를 통해 전송되는 모든 데이터는 인터넷 데이터 전송 요금이 아닌 저렴한 DX 데이터 전송 요금으로 부과되어 네트워크 비용을 크게 절약할 수 있습니다.

애플리케이션 성능 향상

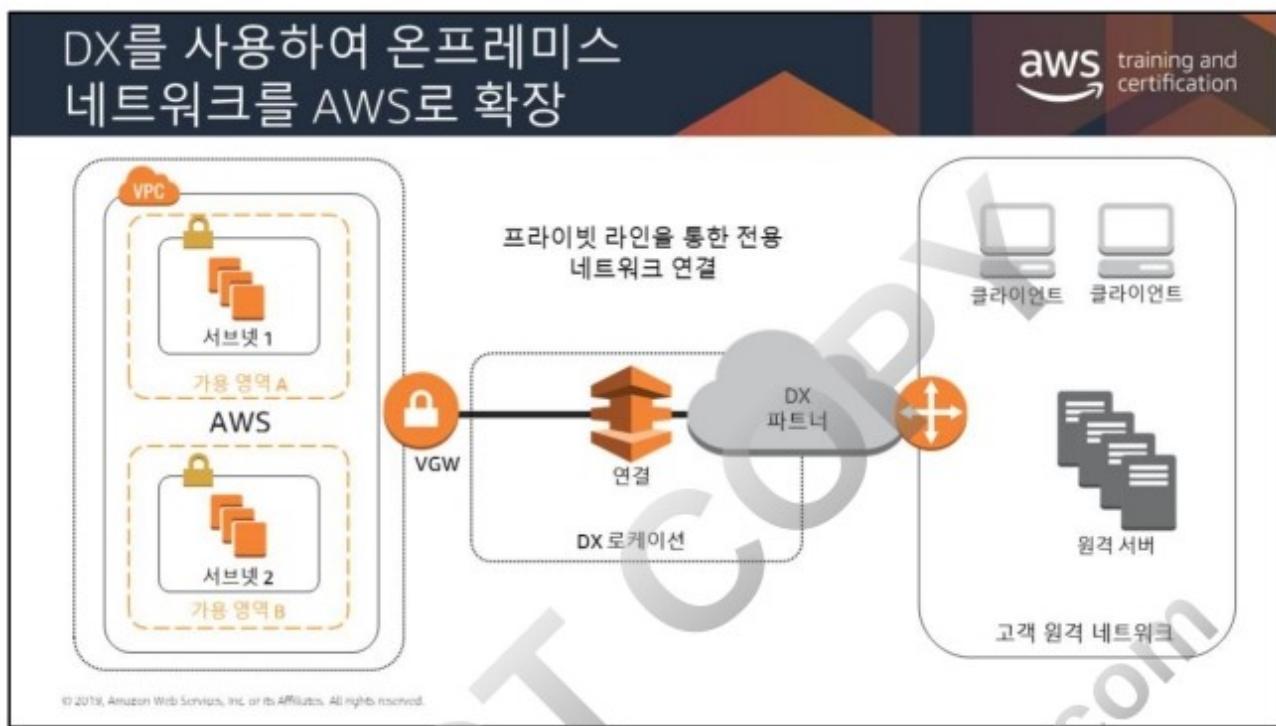
예측 가능한 네트워크 성능이 필요한 애플리케이션도 DX를 활용할 수 있습니다. 오디오 또는 동영상 스트림과 같은 실시간 데이터 피드에서 운영되는 애플리케이션이 그 예입니다. 이러한 경우, 전용 네트워크 연결이 표준 인터넷 연결보다 더 일관된 네트워크 성능을 제공할 수 있습니다.

보안 및 규정 준수

엔터프라이즈 보안 또는 규제 정책에 따라 AWS 클라우드에 호스팅된 애플리케이션이 프라이빗 네트워크 회로로만 액세스되도록 해야 할 경우가 있습니다. DX에서는 데이터 센터와 애플리케이션 간의 트래픽이 전용 프라이빗 네트워크 연결을 통해서만 전송되므로 이러한 요구 사항을 기본적으로 충족합니다.

하이브리드 클라우드 아키텍처

고객이 소유한 기존 데이터 센터 장비에 액세스해야 하는 애플리케이션도 DX를 활용할 수 있습니다. 다음 섹션에서는 이러한 사용 사례를 다루고, DX에서 지원할 수 있는 다른 시나리오도 소개합니다.



이점:

- 예측 가능한 네트워크 성능
- 대역폭 비용 감소
- 1Gbps 또는 10Gbps 프로비저닝된 연결
- BGP 피어링과 라우팅 정책 지원

AWS에서는 Equinix, Coresite, Eircom, TelecityGroup 및 Terramark와의 긴밀한 협력을 통해 전 세계 모든 AWS 리전에 대한 글로벌 DX 액세스를 구축했습니다. 일부 로케이션에서는(LA, 뉴욕 및 런던), 이 서비스의 기능을 확장하여 추가적인 IT 핫 스팟에 대한 액세스도 제공합니다.

제한 사항:

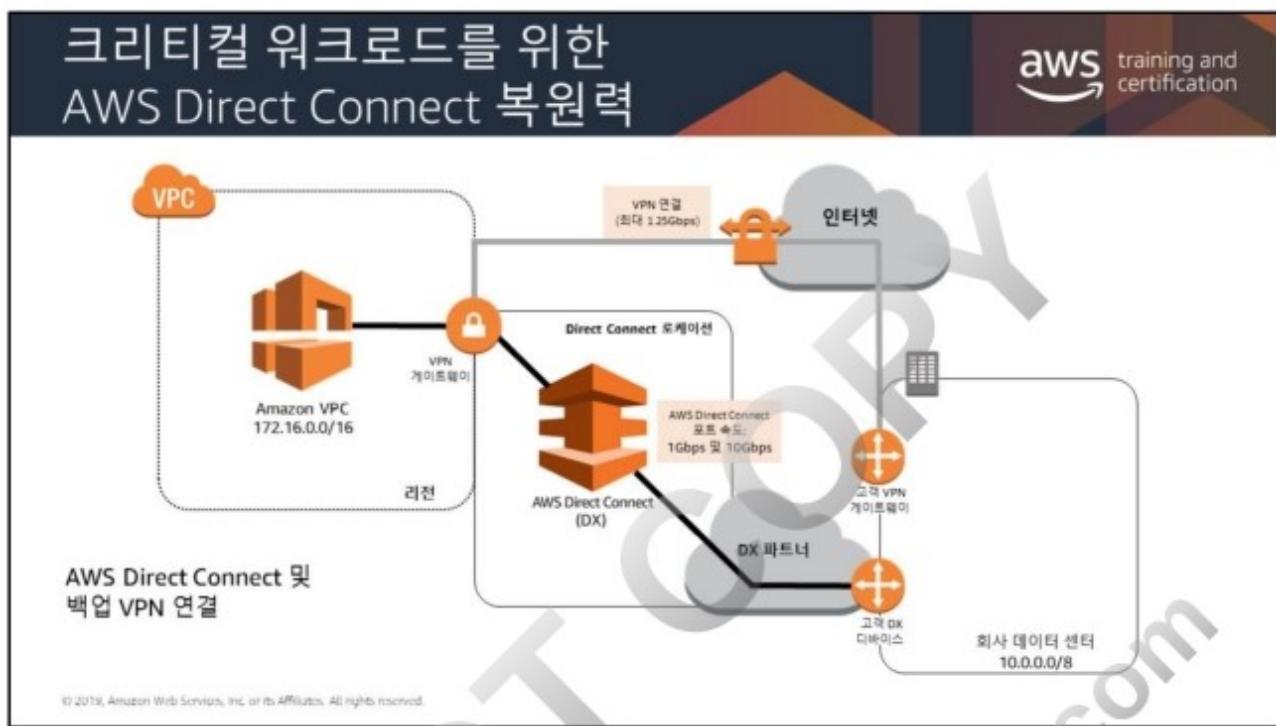
통신 및 호스팅 제공업체가 추가로 필요하거나 새로운 네트워크 회로를 프로비저닝해야 할 수도 있습니다.

DX를 사용하면 온프레미스에서 Amazon VPC로 전용 네트워크 연결을 손쉽게 구축할 수 있습니다. 고객은 DX를 사용해 AWS와 고객의 데이터 센터, 사무실 또는 코로케이션 환경 간에 프라이빗 연결을 설정할 수 있습니다. 이 프라이빗 연결은 네트워크 비용을 줄이고, 대역폭 처리량을 높이며, 인터넷 기반 연결보다 더 일관된 네트워크 환경을 제공합니다.

DX를 사용하면 고객은 DX 로케이션 중 하나와 AWS 네트워크 간에 1Gbps 또는 10Gbps 전용 네트워크 연결(또는 다수의 연결)을 구축하고, 산업 표준 VLAN을 사용하여 프라이빗 IP 주소를 사용하는 VPC 내에서 실행되는 Amazon EC2 인스턴스에 액세스할 수 있습니다. 고객은 DX 로케이션에 있는 DX 엔드포인트를 원격 네트워크와 통합하기 위해 WAN 서비스 공급자의 에코시스템을 선택할 수도 있습니다.

현재 AWS DX 로케이션의 목록은 <http://aws.amazon.com/directconnect/details/>를 참조하십시오.

크리티컬 워크로드를 위한 높은 복원력의 AWS Direct Connect 사용 방법에 대한 정보는 <https://aws.amazon.com/directconnect/resiliency-recommendation/>을 참조하십시오.



AWS 고객은 더 저렴한 백업 연결과 결합하여 하나 이상의 AWS Direct Connect(DX) 연결을 AWS에 대한 기본 연결에 사용할 수 있습니다. 이 목표를 달성하기 위해 위 다이어그램에 표시된 대로 VPN 백업을 사용하여 DX 연결을 설정할 수 있습니다.

이 예의 구성은 2개의 동적 라우팅 연결로 구성됩니다. 2개의 고객 디바이스로부터 하나는 DX 연결을 사용하고 다른 하나는 VPN 연결을 사용합니다. AWS는 DX 및 동적 라우팅 VPN 연결을 설정하는데 도움이 되는 라우터 구성 예를 제공합니다. 기본적으로 AWS는 사용자의 DX 연결을 통해 트래픽을 전송하는 것을 항상 선호합니다. 따라서 기본 및 백업 연결을 정의하기 위한 추가 AWS 관련 구성이 필요하지 않습니다. 하지만 고객은 내부 시스템이 올바른 경로를 선택하도록 DX와 VPN 전용 내부 라우팅 전파를 구성해야 합니다. 다중 데이터 센터 HA 네트워크 연결 솔루션 개요에 이 시나리오를 위한 라우팅 조작 옵션이 자세히 설명되어 있습니다. 하지만 단일 데이터 센터에서 AWS로 연결하는 대부분의 고객은 일반적으로 기본 구성이면 충분합니다.

AWS Direct Connect는 단일 모드 광섬유를 통해 다음 포트 속도를 지원합니다.
1Gbps: 1000BASE-LX(1310nm) 및 10 Gbps: 10GBASE-LR(1310nm).

AWS 관리형 VPN은 VPN 터널 당 최대 1.25Gbps의 처리량을 지원하며 동일한 VGW에 종료되는 AWS 관리형 VPN 터널이 여러 개인 경우 외부 데이터 경로에 대해 ECMP(Equal Cost Multi Path)를 지원하지 않습니다.

이 접근 방식을 통해 AWS 트래픽의 기본 네트워크 경로 및 네트워크 공급자를 선택할 수 있으며, 백업 VPN 연결에 대해 다른 공급자를 사용할 수도 있습니다. 조직의 위험 허용도, 예산 및 데이터 센터 연결 정책에 부합하는 네트워크 공급자와 AWS Direct Connect 로케이션을 선택하십시오. 예를 들어, 네트워크 공급자 가동 중단과 관련된 위험이 우려된다면 AWS Direct Connect 및 인터넷 연결에 서로 다른 네트워크 공급자를 사용할 것을 고려할 수 있습니다. 하지만 이 설계는 단일 고객 위치로부터 AWS 연결을 제공하므로 중복 네트워크 공급자 구성을 사용하더라도 모든 위치 관련 중단(예: 정전 또는 시설 외부 케이블 절단)이 여전히 AWS 연결에 영향을 미칠 수 있습니다. 또한, VPN 연결이 애플리케이션의 지연 시간 및 대역폭 요구 사항을 지원하는 데 충분한 백업이 되고 있는지 AWS Direct Connect 사용률을 모니터링해야 합니다.

VPC 연결

aws training and certification

- 일반적으로 일부 워크로드를 격리하는 것이 좋습니다.
- 그러나 둘 이상의 VPC 간에 데이터를 전송해야 할 수도 있습니다.

The diagram illustrates three separate Virtual Private Clouds (VPCs) represented by orange cloud icons. Below each icon, a white rectangular box contains the Korean word for the environment: '개발' (Development), '테스트' (Test), and '프로덕션' (Production). The boxes are arranged horizontally, separated by thin lines.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

비즈니스 또는 아키텍처 규모가 충분히 커지게 되면 보안 또는 아키텍처 측면의 필요를 위해 또는 단지 단순성을 위해 별도의 논리적 요소가 필요할 것입니다.

VPC 연결 - VPC 피어링

인스턴스는 피어링 연결을 통해 동일한 네트워크에 있는 것처럼 통신할 수 있습니다.

- 프라이빗 IP 주소 사용
- 내부 및 리전 간 지원
- IP 공간은 중복될 수 없음
- 두 VPC 간 하나의 피어링 리소스만 해당
- 전이적 피어링 관계는 지원되지 않음
- 서로 다른 AWS 계정 간에 설정 가능

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

다이어그램에서 Dev VPC와 Test VPC는 피어링되어 있습니다. 그러나 이는 Prod가 Dev와 통신할 수 있다는 것을 의미하지는 않습니다. 기본적으로 VPC 피어링에서는 명시적으로 피어로 설정되어 있지 않으면 Prod가 Dev에 연결하도록 허용하지 않습니다. 따라서 어떤 VPC가 서로 통신할 수 있는지 제어할 수 있습니다.

VPC 피어링 연결을 설정하려면, 요청자 VPC(또는 로컬 VPC)의 소유자가 피어 VPC의 소유자에게 요청을 전송하여 VPC 피어링 연결을 생성합니다. 피어 VPC는 여러분이나 다른 AWS 계정에서 소유할 수 있으며, CIDR 블록이 요청자 VPC의 CIDR 블록과 중복되어서는 안 됩니다. 피어 VPC의 소유자가 VPC 피어링 연결 요청을 수락해야 VPC 피어링 연결이 활성화됩니다. 프라이빗 IP 주소를 사용하여 피어 VPC 간에 트래픽이 전송되도록 하려면, VPC의 라우팅 테이블에 피어 VPC의 IP 주소 범위를 가리키는 하나 이상의 경로를 추가합니다. 피어 VPC의 소유자는 자신의 VPC 라우팅 테이블에 여러분의 VPC IP 주소 범위를 가리키는 하나 이상의 경로를 추가합니다. 또한, 인스턴스와 연결된 보안 그룹 규칙을 업데이트하여 피어 VPC로 송수신되는 트래픽이 제한되지 않도록 해야 할 수 있습니다.

VPC 피어링 연결은 두 VPC 간에 일대일 관계입니다. 소유한 각 VPC에 대해 여러 개의 VPC 피어링 연결을 생성할 수 있지만, 전이적 피어링 관계는 지원되지 않습니다. VPC는 직접 피어링되지 않은 VPC와는 피어링 관계를 갖지 않습니다. 자신의 VPC 사이에서, 또는 단일 리전 내에 있는 다른 AWS 계정의 VPC 사이에서 VPC 피어링 연결을 만들 수도 있습니다.

이제 서로 다른 리전에 있는 VPC 사이에서도 피어링 관계를 설정할 수 있습니다. 리전 간 VPC 피어링을 통해 서로 다른 리전에서 실행되는 Amazon EC2 인스턴스, Amazon RDS 데이터베이스, Lambda 함수 같은 VPC 리소스가 게이트웨이, VPN 연결 또는 별도의 네트워크 어플라이언스 없이 프라이빗 IP 주소를 사용하여 서로 통신할 수 있습니다. 리전 간 VPC 피어링 연결을 통해 전송되는 데이터에는 표준 리전 간 데이터 전송 요금이 부과됩니다.

VPC 피어링

aws training and certification

- 인터넷 게이트웨이 또는 가상 게이트웨이가 필요 없음
- 고가용성 연결, 단일 장애 지점 없음
- 대역폭 병목 현상 없음
- 트래픽은 항상 글로벌 AWS 백본에서 유지됨

The diagram shows two VPCs, VPC A and VPC B, connected via a central VPC Peering connection labeled 'PCX-1'. VPC A has an IP range of 10.2.0.0/16 and VPC B has an IP range of 10.1.0.0/16. Both VPCs have their own route tables:

라우팅 테이블	
목적지	대상
10.1.0.0/16	로컬
10.2.0.0/16	PCX-1

라우팅 테이블	
목적지	대상
10.1.0.0/16	로컬
10.2.0.0/16	PCX-1

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

다른 VPC와 VPC 피어링 연결을 생성하려면, 다음 제한과 규칙을 이해해야 합니다.

- VPC당 생성할 수 있는 활성 및 보류 VPC 피어링 연결의 수에는 제한이 있습니다.
- VPC 피어링은 전이적 피어링 관계를 지원하지 않습니다. VPC 피어링 연결에서 VPC는 피어 VPC가 피어링되어 있는 다른 VPC에 액세스할 권한이 없습니다. 이는 모든 것이 자신의 AWS 계정 내에 설정되어 있는 VPC 피어링 연결에도 적용됩니다.
- 동일한 2개의 VPC 간에 동시에 두 개 이상의 VPC 피어링 연결을 생성할 수 없습니다.
- VPC 피어링 연결에서 MTU(최대 전송 단위)는 1,500바이트입니다.
- 배치 그룹은 피어링된 여러 VPC를 포괄할 수 있지만, 피어링된 VPC의 인스턴스 간에는 양방향 대역폭이 제공되지 않습니다.
- VPC 피어링 연결에서는 유니캐스트 역경로 전달은 지원되지 않습니다.
- 피어링된 VPC에서 인스턴스 간에 프라이빗 DNS 값을 확인할 수 없습니다.
- 리전 간 VPC 피어링을 사용하는 트래픽은 전 세계의 AWS 백본에 항상 머무르며 퍼블릭 인터넷을 통과하지 않으므로 일반적인 도용 및 DDoS 공격 같은 위협 벡터를 줄입니다.

이제 인바운드 및 아웃바운드 규칙 모두에서 피어링된 VPC의 보안 그룹을 참조할 수 있습니다. 이 기능은 교차 계정으로 지원되므로 두 VPC가 계정이 서로 다를 수 있습니다. 피어링된 VPC 내 보안 그룹 참조에 대한 지원은 CIDR 범위 대신 보안 그룹 멤버십을 통해 피어링 트래픽을 제어하여 VPC 구성의 간소화를 줍니다. 콘솔, AWS CLI 및 SDK를 사용하여 피어링된 VPC에서 보안 그룹을 참조할 수 있습니다.

DO NOT COPY
zlagusdbs@gmail.com

여러 VPC 피어링

aws training and certification

일반 모범 사례

다음과 같이 여러 VPC를 연결할 때 고려해야 할 몇 가지 범용 네트워크 설계 원칙이 있습니다.

목적지	대상
10.1.0.0/16	로컬
10.2.0.0/16	VPC-1

중복되는 CIDR
블록 없음

VPC

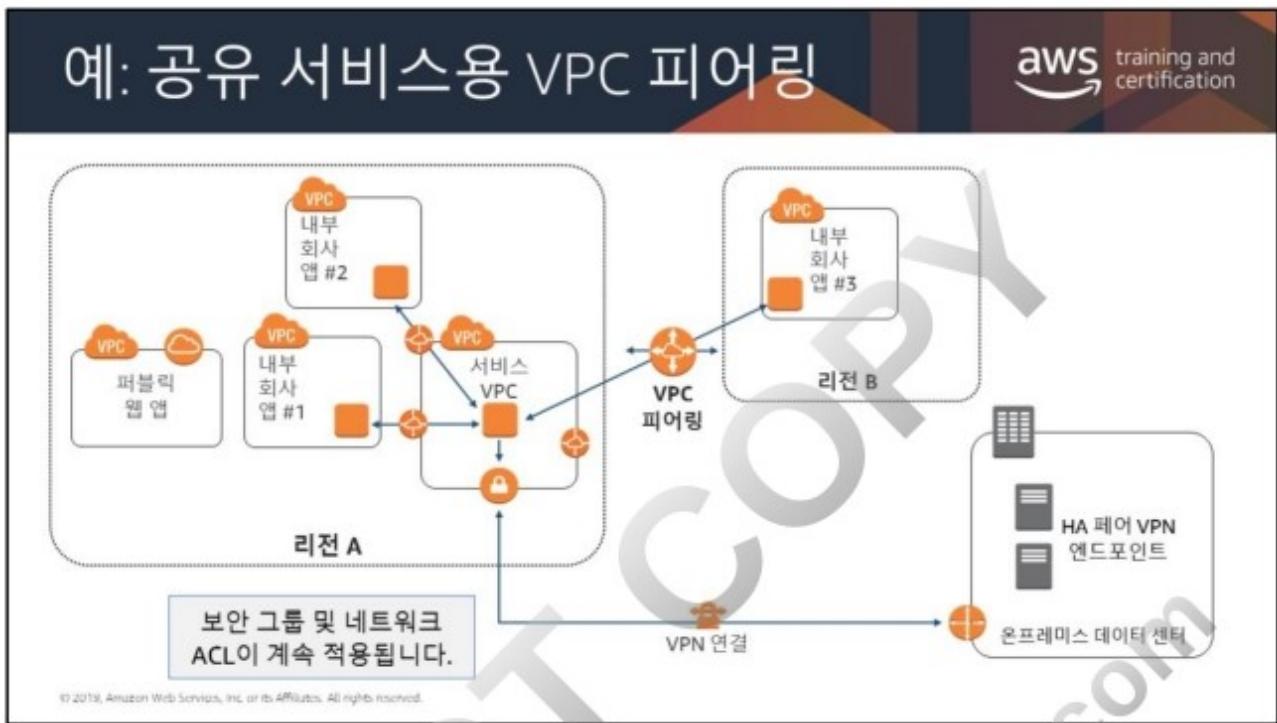
필수 VPC만 연결

솔루션을 확장할 수
있어야 함

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

단일 AWS 리전의 여러 VPC를 연결할 때 고려해야 할 몇 가지 범용 네트워크 설계 원칙이 있습니다.

- VPC 네트워크 범위(CIDR 블록)가 중복되지 않아야 합니다.
- 선택한 솔루션이 현재 및 미래의 VPC 연결 수요에 따라 확장이 가능한지 확인해야 합니다.
- 단일 장애 지점이 없는 고가용성(HA) 설계를 구현해야 합니다.
- 솔루션 선택에 영향을 미치므로 데이터 전송 요구를 고려해야 합니다. 데이터 전송량을 기준으로 어떤 솔루션은 다른 솔루션보다 비용이 높을 수 있습니다.
- 반드시 서로 통신해야 하는 VPC들만 연결해야 합니다.



이 예에서는, 맙은 책임을 이행하기 위해, 기업 IT 및 기업 정보 보안 그룹이 각 부서에서 피어링할 수 있는 "서비스 VPC"를 제공합니다. 이 VPC는 Active Directory 연결, 보안 검사 도구, 모니터링/로깅 도구 및 다양한 기타 기능을 포함하고 있습니다. 부서 VPC가 일부 온프레미스 리소스에 액세스하는 데 사용할 수 있는 프록시도 제공합니다.

VPC 피어링:

- **1 - 1 Peer** = 다른 VPC의 다른 앱으로부터 회사 앱을 분리하지만, 항상 dev/qa와 prod 사이에 임시 연결을 생성하여, 데이터를 전송하고, 연결을 제거할 수 있습니다.
- 보안 그룹 및 네트워크 ACL이 계속 적용됩니다.

다른 리전의 VPC와의 피어링 연결이 존재한다는 점을 유의하십시오. 이제 서로 다른 AWS 리전의 VPC 사이에 피어링 관계를 설정할 수 있습니다. 리전 간 VPC 피어링을 통해 서로 다른 AWS 리전에서 실행되는 EC2 인스턴스, Amazon RDS, Lambda 함수 같은 VPC 리소스가 게이트웨이, VPN 연결 또는 별도의 물리적 하드웨어 없이 프라이빗 IP 주소를 사용하여 서로 통신할 수 있습니다.

VPC 연결 - Transit Gateway



AWS Transit
Gateway

단일 게이트웨이로 최대 5,000개의 VPC와
온프레미스 환경 연결

네트워크 사이를 이동하는 모든 트래픽의 허브
역할 담당

가용성이 뛰어나고 유연한 완전 관리형 라우팅
서비스

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

17

Transit Gateway 실행 - 연결

aws training and certification

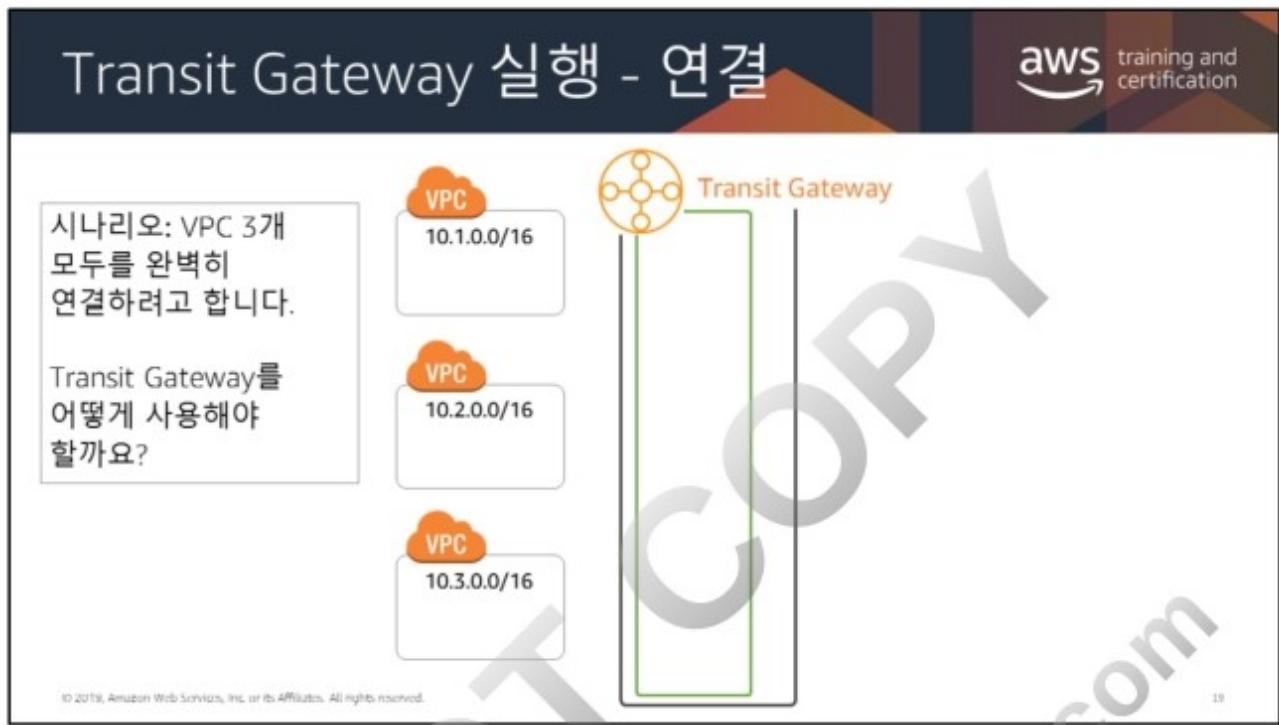
시나리오: VPC 3개 모두를 완벽히 연결하려고 합니다.

Transit Gateway를 어떻게 사용해야 할까요?

VPC 10.1.0.0/16
VPC 10.2.0.0/16
VPC 10.3.0.0/16

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved. 18

여러 VPC를 연결하는 것이 매우 바람직한 경우가 많습니다. 대규모 그룹에서 VPC 피어링 연결을 관리하는 것은 어렵고 짜증나는 일입니다. 시간 경과에 따른 환경 확장, 조정 방법, VPC 관리 방법을 염두에 두어야 합니다.



이 연결을 생성하는 첫 번째 단계는 transit gateway를 설정하는 것입니다. Amazon EC2 대시보드를 통해 이를 수행할 수 있습니다. transit gateway 사용 요금은 다양합니다. 아키텍처와 예산이 이를 지원하는지 확인하십시오.

Transit Gateway 실행 - 연결

aws training and certification

시나리오: VPC 3개 모두를 완벽히 연결하려고 합니다.

Transit Gateway를 어떻게 사용해야 할까요?

The diagram illustrates a network architecture where three separate Virtual Private Clouds (VPCs) are interconnected through a central Transit Gateway. Each VPC is represented by a cloud icon containing two orange circular icons, likely representing interfaces or endpoints. A green vertical line connects each VPC to the central orange Transit Gateway icon, which features a circular design with three points. This visual representation demonstrates how multiple VPCs can be integrated into a single, managed network fabric using the Transit Gateway service.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

20

Transit Gateway는 서브넷에 배포된 네트워크 인터페이스를 통해 작동합니다.
Transit Gateway를 효과적으로 사용하려면 대상 VPC가 있는 가용 영역마다
하나의 attachment를 배포해야 합니다.

Transit Gateway 실행 - 연결

aws training and certification

시나리오: VPC 3개 모두를 완벽히 연결하려고 합니다.

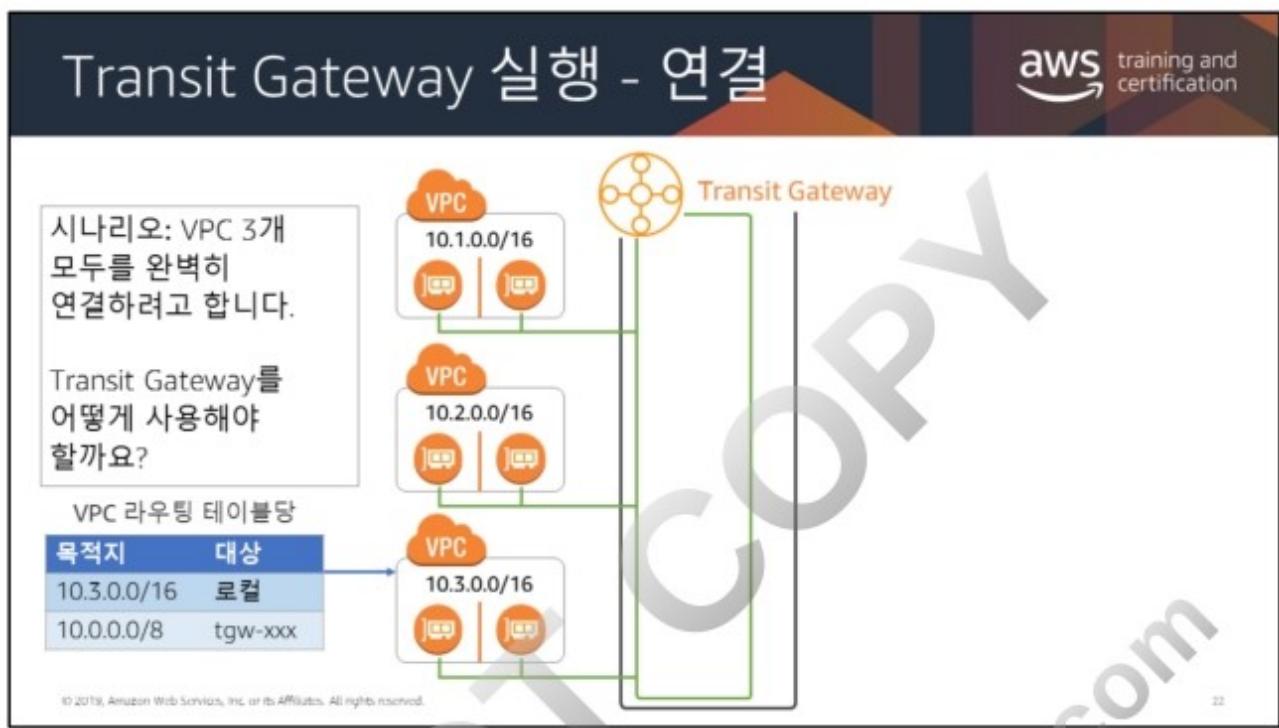
Transit Gateway를 어떻게 사용해야 할까요?

VPC 라우팅 테이블당

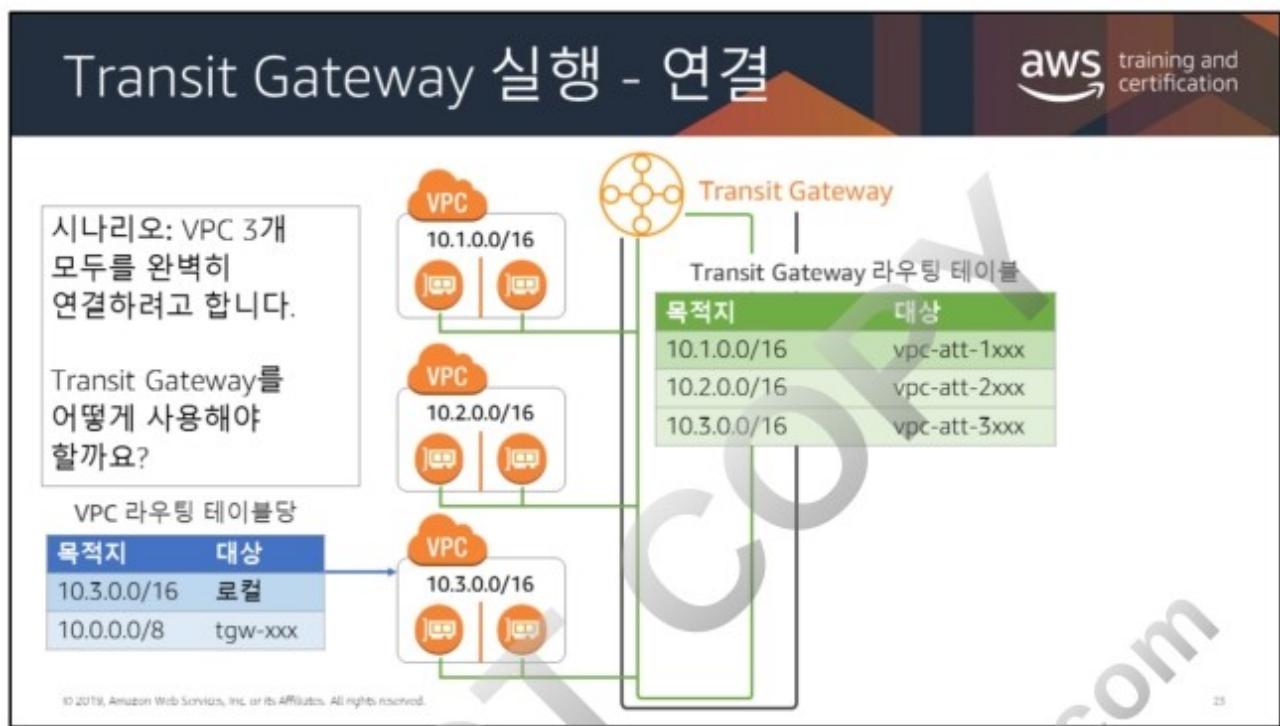
목적지	대상
10.3.0.0/16	로컬
10.0.0.0/8	tgw-xxx

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

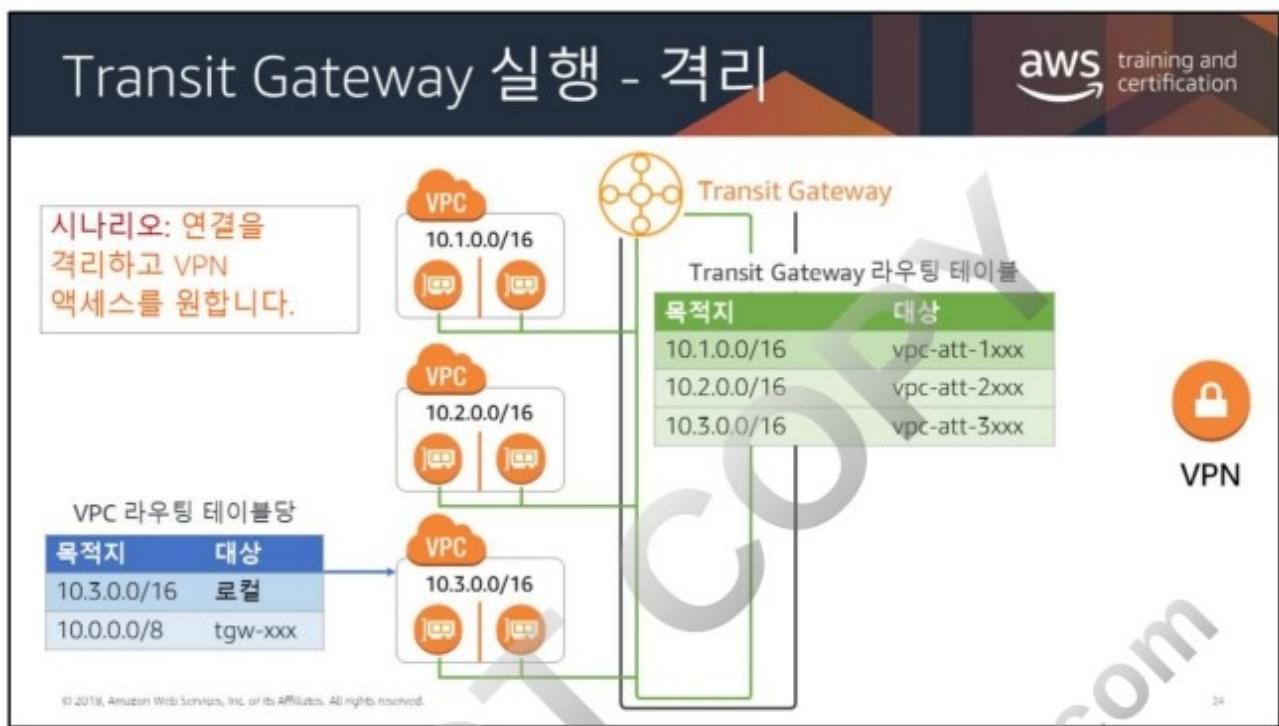
VPC의 각 라우팅 테이블에서 트래픽이 Transit Gateway attachment를 향해 외부로 라우팅되는지 확인하십시오.



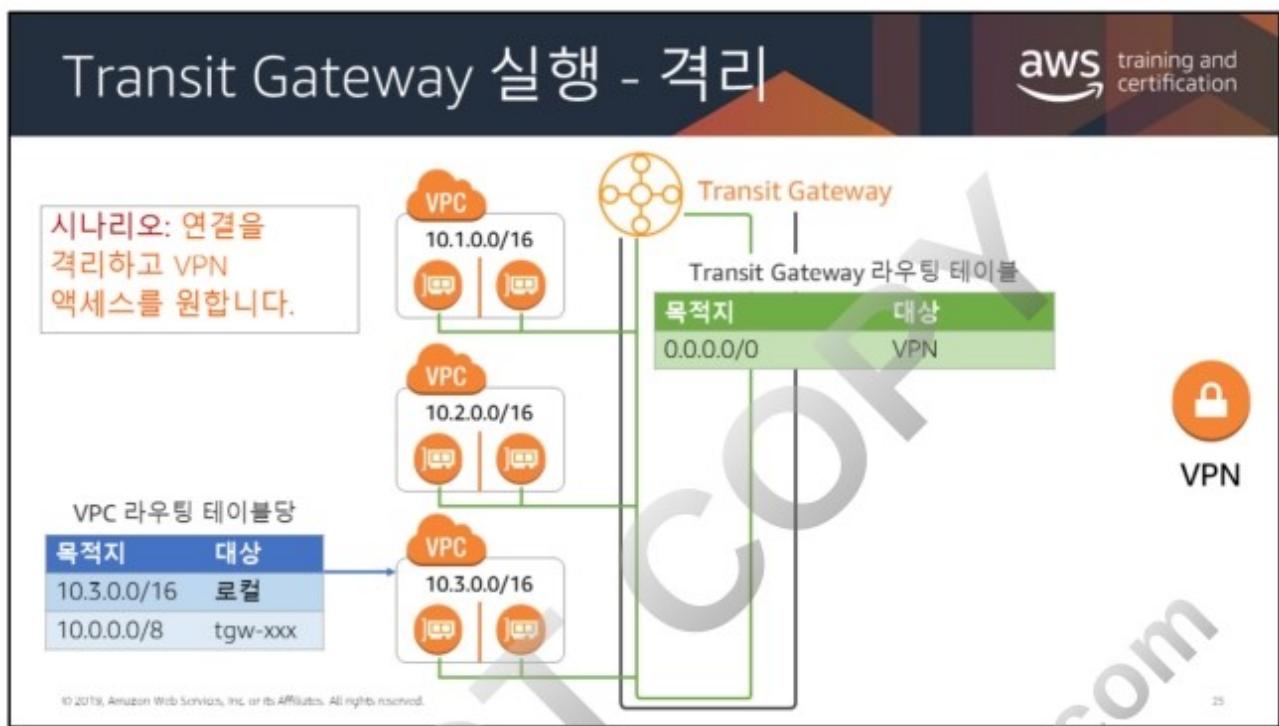
이러한 attachment는 Transit Gateway에 연결됩니다.



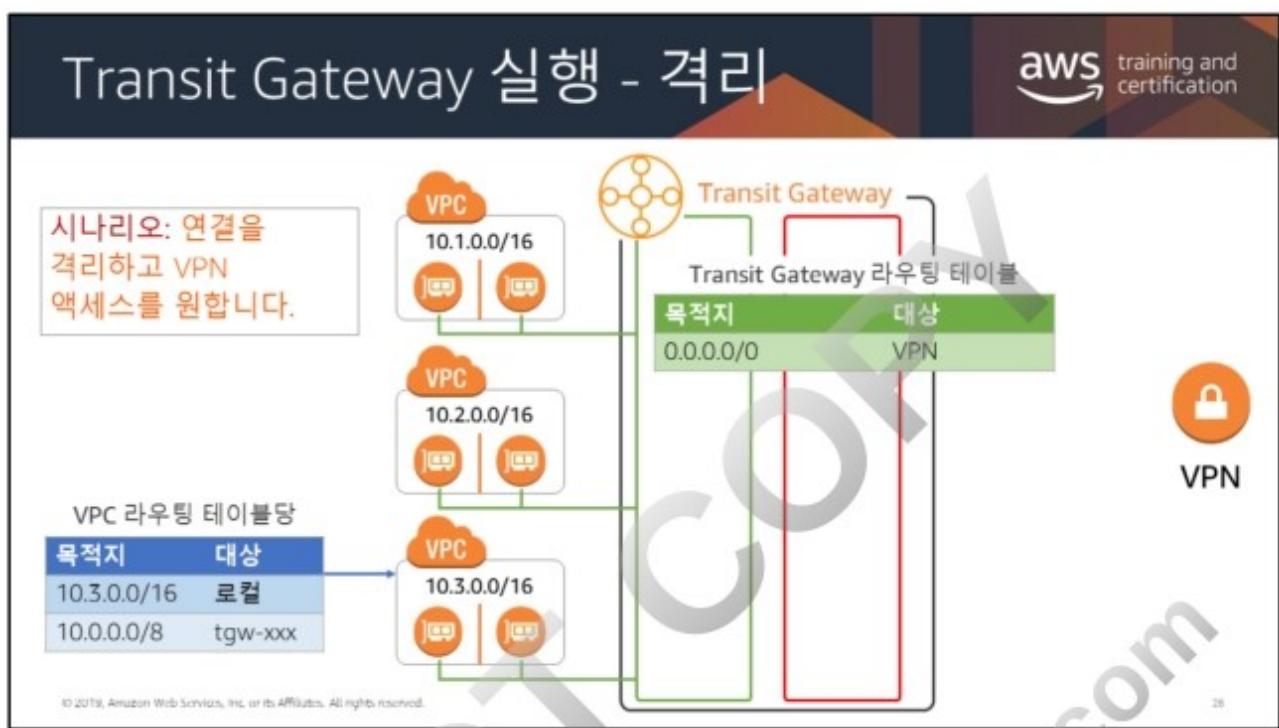
Transit Gateway 내부에서 라우팅 테이블을 생성하여 적절하게 트래픽을 전달할 수 있습니다. 매우 구체적으로 상호 작용하는 라우팅 테이블이 여러 개 있을 수 있습니다. 여기서는 하나의 라우팅 테이블로 전체 연결을 허용합니다.



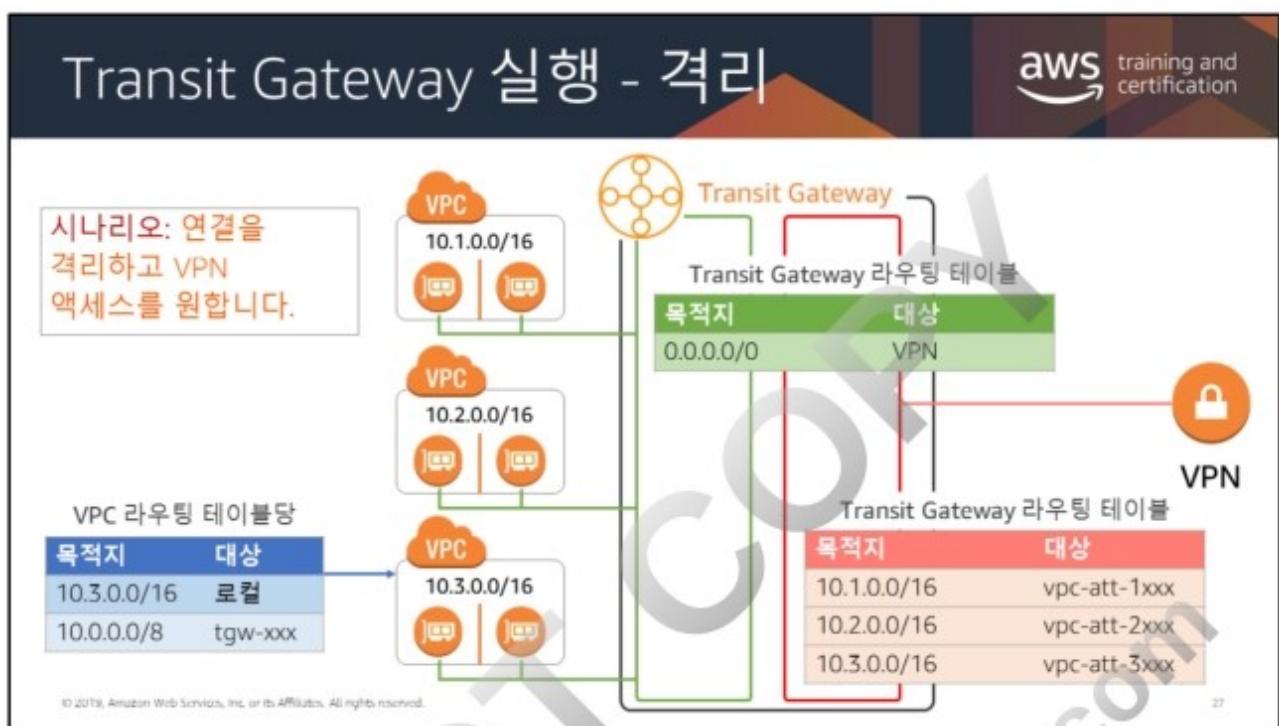
일반적인 아키텍처는 VPN 소스에서 환경에 대한 전체 액세스 권한을 갖는 것입니다. 이 시나리오에서는 또한 VPC가 서로 통신하지 않게 할 것입니다.



먼저 초기 테이블의 경로를 수정하여 VPN 연결을 향하도록 합니다. 그러면 VPC 간 통신이 중지되고 아웃바운드 액세스를 제공합니다.



이제 VPN에만 연결된 격리된 환경을 생성합니다. Transit Gateway 내에 다른 라우팅 테이블을 추가합니다.



VPN에서 대상 VPC를 향하도록 이 라우팅 테이블을 설정합니다. 이제 교차 통신이 없는 격리되고 안전한 VPN 액세스를 얻었습니다.

VPC 엔드포인트

AWS를 벗어나지 않고 EC2 인스턴스를 VPC 외부 서비스와 프라이빗하게 연결합니다.

인터넷 게이트웨이, VPN, NAT (Network Address Translation) 디바이스 또는 방화벽 프록시를 사용할 필요가 없습니다.



- 인터넷을 통해 통과할 필요가 없습니다.
- 동일한 리전에 있어야 합니다.
- 가용성이 뛰어나고, 중복적이며, 수평적으로 확장됩니다.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Amazon VPC 엔드포인트는 AWS 네트워크를 벗어나지 않고 VPC와 다른 AWS 서비스 간에 프라이빗 연결이 가능하게 합니다. 엔드포인트를 사용하면 Amazon EC2 인스턴스가 프라이빗 IP 주소로 동일한 리전의 AWS 서비스와 통신할 수 있습니다. 인터넷에서 우회하거나 NAT 인스턴스, VPN 연결 또는 DX를 통과할 필요가 없습니다. 또한 VPC 엔드포인트는 특정 VPC에서 액세스할 수 있는 Amazon S3 버킷을 제어하거나 S3 버킷을 특정 VPC로 잠그는 정책을 추가하는 등의 추가 보안 기능도 제공합니다. 현재, AWS에서는 Amazon S3 및 Amazon DynamoDB와 연결을 위한 VPC 엔드포인트만 지원합니다.

엔드포인트는 가상 디바이스입니다. 수평 확장되고 가용성이 높은 중복 VPC 구성 요소로서 가용성 위험이나 네트워크 트래픽에 대한 대역폭 제약 없이 VPC의 인스턴스와 서비스 간에 통신할 수 있습니다.

두 가지 유형의 엔드포인트



인터페이스 엔드포인트

- Amazon CloudWatch Logs
- AWS CodeBuild
- Amazon EC2 API
- Elastic Load Balancing API
- AWS Key Management Service (AWS KMS)
- Amazon Kinesis Data Streams
- AWS Service Catalog
- Amazon Simple Notification Service (Amazon SNS)
- AWS Systems Manager
- 다른 AWS 계정에서 호스팅하는 엔드포인트 서비스
- 그 외 다수

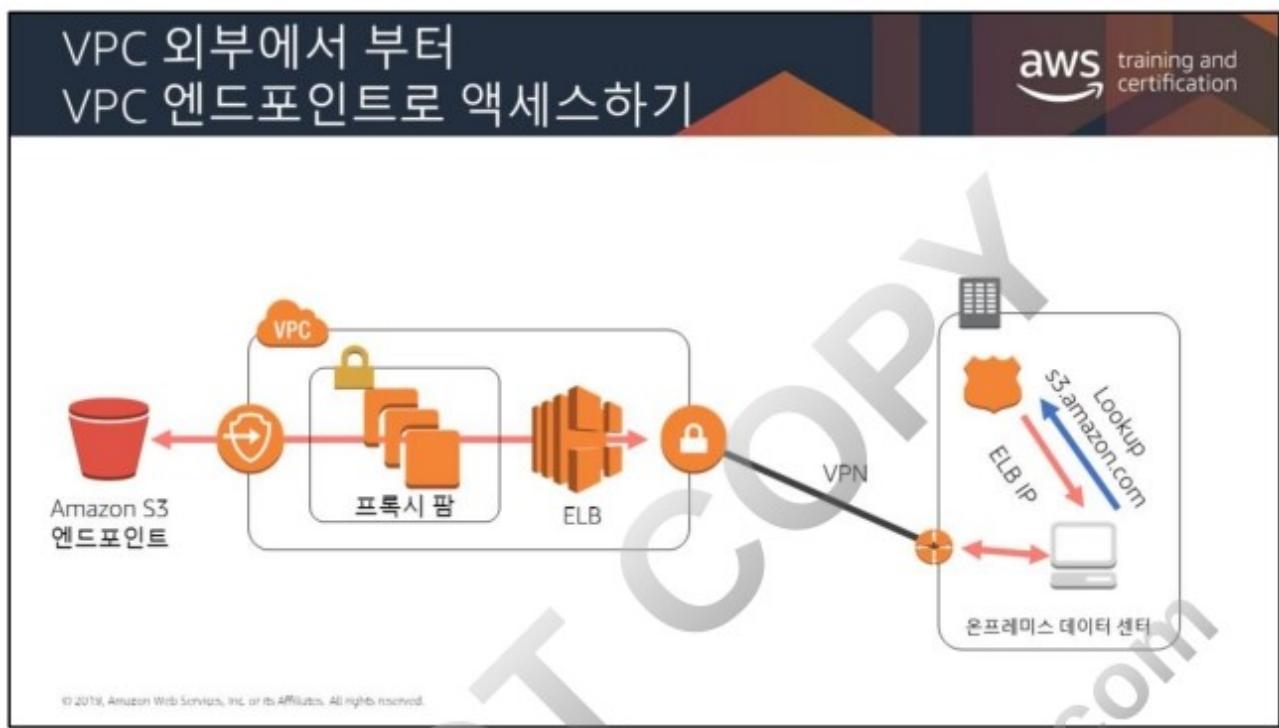
게이트웨이 엔드포인트

- Amazon Simple Storage Service(Amazon S3)
- Amazon DynamoDB

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

인터페이스 엔드포인트는 지원되는 서비스로 향하는 트래픽의 진입점 역할을 하는 프라이빗 IP 주소가 할당된 탄력적 네트워크 인터페이스입니다.

게이트웨이 엔드포인트는 라우팅 테이블의 지정된 라우팅의 대상인 게이트웨이로, 지원되는 AWS 서비스의 트래픽에 사용됩니다.



기업 도메인 이름 서비스(DNS)

원격 네트워크에서 VPC 엔드포인트를 사용하는 첫 번째 단계는 엔드포인트를 통해 리디렉션 할 트래픽을 식별하는 것입니다. 이 솔루션은 기업 DNS 서버를 사용해 VPC 엔드포인트 전용 트래픽에 대한 DNS 확인을 무시합니다. 위 예제에서 DNS 서버는 s3.amazonaws.com을 내부 ELB 로드 밸런서로 확인하도록 구성되어 있습니다. 이 로드 밸런서는 미국 표준 S3 버킷으로 향하는 트래픽을 VPC 엔드포인트로 리디렉션합니다. 그러면 기업 네트워크에서 S3 버킷으로 가는 Amazon S3 요청이 인터넷을 경유하지 않고 프라이빗 VPN 또는 DX 연결을 통해 전송됩니다.

Elastic Load Balancing (ELB)

ELB는 수신되는 Amazon S3 TCP, UDP 연결을 여러 Amazon EC2 프록시 인스턴스로 자동 분산시킵니다. 그러므로 S3 트래픽을 여러 프록시 서버로 분산하는 데 필요한 로드 밸런싱 용량을 원활하게 제공함으로써 프록시 팝의 내결합성 수준을 개선할 수 있습니다. 또한 ELB 로드 밸런서가 여러 가용 영역을 사용하여 내결합성을 최대화하도록 구성하십시오.

프록시 팜

프록시 팜은 Amazon S3 트래픽을 VPC 엔드포인트로 프록시합니다. 프록시 팜은 ACL(액세스 제어 목록)을 사용하여 VPC 엔드포인트 트래픽에 대한 추가 제어를 제공할 수 있습니다. ACL은 솔루션을 사용할 권한이 부여될 원격 사용자 또는 네트워크를 지정할 수 있으며, 클라이언트가 액세스할 수 있는 VPC 엔드포인트 또는 대상 도메인을 추가로 제한할 수 있습니다. Auto Scaling 그룹이 프록시 서비스를 관리하고 프록시 서버 로드에 따라 자동으로 필요한 인스턴스 수를 확장 또는 축소하도록 구성하십시오.

DO NOT COPY
zlagusdbs@gmail.com

