Amazon Virtual Private Cloud 를 이용한 IT 인프라의 확장

2013 년 12 월

(본 문서의 최신 버전을 보려면 **http://aws.amazon.com/whitepapers/** 를 참조하십시오.)

목차

서론

Amazon Virtual Private Cloud(VPC)는 사용자가 Amazon Web Services(AWS) 클라우드의 격리 프라이빗 영역을 프로비저닝할 수 있도록 해 주며, 이 영역 안에서 사용자는 정의한 가상 네트워크에서 AWS 리소스를 시작할 수 있습니다. Amazon VPC 를 이용하여 사용자의 자체 데이터 센터에서 운영 중인 기존 네트워크와 매우 유사한 가상 네트워크 토폴로지를 정의할 수 있습니다. IP 주소 범위, 서브넷 생성, 라우팅 테이블 및 네트워크 게이트웨이 구성 선택 등 가상 네트워킹 환경을 완벽하게 제어할 수 있습니다. VPC 를 사용해 구현할 수 있는 것들의 예는 다음과 같습니다. 예를 들어, VPC 를 사용하면 다음을 구현할 수 있습니다.

- 기존 온 프레미스 인프라의 용량 확장
- 재해 복구용 환경에 대한 백업 스택 구축
- 보안 결제를 지원하는 PCI DSS(Payment Card Industry Data Security Standard) 규제 준수 웹사이트 구축
- 격리된 개발 및 테스트 환경 마련
- 기업 네트워크 내 가상 데스크톱 애플리케이션 제공

기존의 방식으로 이런 환경을 조성하려면, 엄청난 규모의 선행 투자로 자체 데이터 센터를 구축하고 필요한 하드웨어를 구비함은 물론 필요한 보안 인증을 획득하고 시스템 관리자를 채용해야 하는 등 필요한 조건들을 모두 충족시켜야 합니다. AWS 의 VPC 를 사용하면 필요할 때마다 작은 규모의 투자로 인프라를 확장 및 축소할 수 있습니다. 안전한 환경의 혜택을 추가 비용 없이 모두 온전히 누릴 수 있습니다. AWS 보안 컨트롤, 인증, 승인 및 기능은 보안에 굉장히 민감한 대형 고객사는 물론 정부 기관의 보안 기준에도 부합하는 수준입니다. 자격증 및 승인에 대한 전체 목록은 AWS 규정 준수 센터에서 확인하실 수 있습니다.

본 문서는 Amazon VPC 와 관련 서비스에 대한 일반 사용 사례 및 모범 사례를 다루고 있습니다.

Amazon Virtual Private Cloud 에 대한 이해

Amazon VPC 는 AWS 클라우드 내의 분리된 공간으로, 안전한 사설형 클라우드라고 할 수 있습니다. 사용자는 이 공간 내에서 가상 네트워크 구성을 정의해 AWS 서비스를 사용할 수 있습니다. VPC 를 생성하면 사용자는 VPC 의 인스턴스가 사용할 사설 IP 주소를 직접 제공할 수 있습니다. 이 주소를 CIDR(Classless Inter-Domain Routing) 블록 형태로 지정합니다(예: 10.0.0.0/16). 또한, /28 (16 IP 주소)과 /16 (65,536 IP 주소) 사이에서 네트워크의 블록 크기를 지정할 수도 있습니다.

Amazon VPC 에서 각각의 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스는 Amazon VPC 네트워크에서 기본 프라이빗 IP 주소로 지정된 기본 네트워크 인터페이스를 갖습니다. 사용자는 추가적인 Elastic Network Interfaces(ENI)를 생성해 VPC 내의 모든 Amazon EC2 인스턴스에 첨부할 수 있습니다. 각각의 ENI 는 자체 MAC 주소를 갖습니다. 다수의 사설 IP 주소 할당이 가능하며, 특정 보안 그룹에 지정할 수도 있습니다. 개개의 인스턴스에 지정할 수 있는 ENI 와 프라이빗 IP 주소의 총 개수는 인스턴스 유형에 따라 다릅니다. 동일한 가용 영역 내의 각기 다른 서브넷에서 ENI 를 생성해 단일 인스턴스에 첨부하는 방식으로 저렴한 관리용 네트워크 또는 네트워크 및 보안 어플라이언스 등을 구축할 수 있습니다. 보조 ENI 및 사설 IP 주소를 동일한 서브넷 내의 다른 인스턴스로 옮겨 비용이 낮은 고가용성 솔루션을 확보하는 것도 가능합니다. 각각의 사설 IP 주소에 공인 엘라스틱 IP 주소(EIP)를 연결할 수 있어 인터넷에서 인스턴스에 접근할 수도 있습니다. 또한 시작 시에 퍼블릭 IP 주소를 할당받도록 Amazon EC2 인스턴스를 구성할 수도 있습니다. 퍼블릭 IP 주소는 Amazon 의 퍼블릭 IP 주소 풀에서 사용자 인스턴스로 할당되며 AWS 계정과는 관련이 없습니다. 다중 IP 및 EIP 지원의 가장 큰 장점은 단일 서버에 다중 SSL 인증서를 사용하고 각 인증서를 특정 IP 주소에 연결할 수 있다는 것입니다.

Amazon VPC 제한에 기록된 대로 VPC 에 배포할 수 있는 구성 요소의 수에는 기본 한도가 있습니다. 한도 상향을 신청하려면 Amazon VPC 제한 양식을 작성하십시오.

다양한 수준의 네트워크 격리

VPC 서브넷은 *퍼블릭*, *프라이빗*, 또는 *VPN 전용으로 설정할 수 있습니다.*퍼블릭 서브넷을 설정하려면 그림 1 처럼 해당 서브넷에서 인터넷으로 나가는 트래픽이 VPC 와 연결된 인터넷 게이트웨이를 통해 라우팅되도록 라우팅 테이블을 구성해야 합니다. EIP 주소를 서브넷의 인스턴스에 지정함으로써 인터넷에서도 연결되도록 할 수 있습니다. 상태 저장 보안 그룹 규칙을 활용하여 해당 인스턴스에 대한 인바운드 트래픽과 아웃바운드 트래픽을 모두 제한하는 것이 모범 사례입니다. 해당 서브넷에 대한 네트워크 ACL(액세스 제어 목록)을 설정하면 서브넷에 상태 비저장 네트워크 필터링도 적용할 수 있습니다.

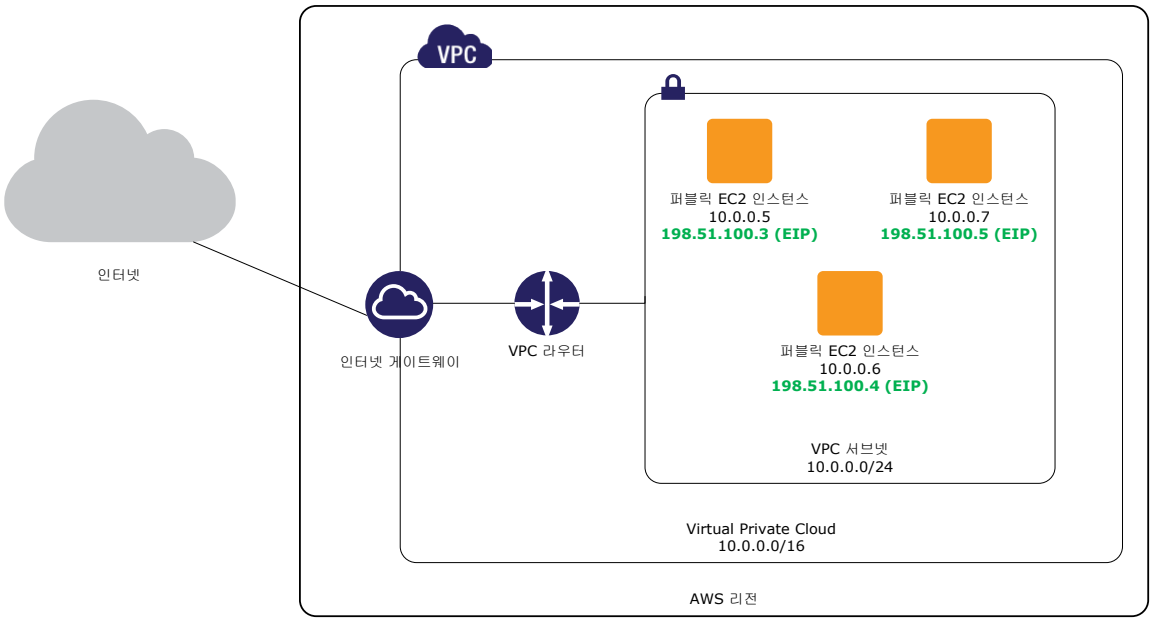

그림 1: 퍼블릭 서브넷 하나만 사용하는 VPC 의 예

프라이빗 서브넷의 경우, 해당 서브넷에서 인터넷으로 나가는 트래픽은 퍼블릭 EIP 를 사용하는 퍼블릭 서브넷 내의 특수 NAT(Network Address Translation) 인스턴스를 통해 라우팅할 수 있습니다. 이 구성은 프라이빗 서브넷의 리소스가 EIP 를 할당하거나 직접 인바운드 연결을 수용하지 않고도 아웃바운드 트래픽을 인터넷에 연결하도록 해 줍니다. AWS 는 미리 구성된 NAT 서버 이미지를 제공하며, NAT 를 지원하는 사용자 지정 AMI 를 사용할 수도 있습니다. 그림 2 에서 퍼블릭 및 프라이빗 서브넷을 모두 사용하는 VPC 의 예를 확인할 수 있습니다.

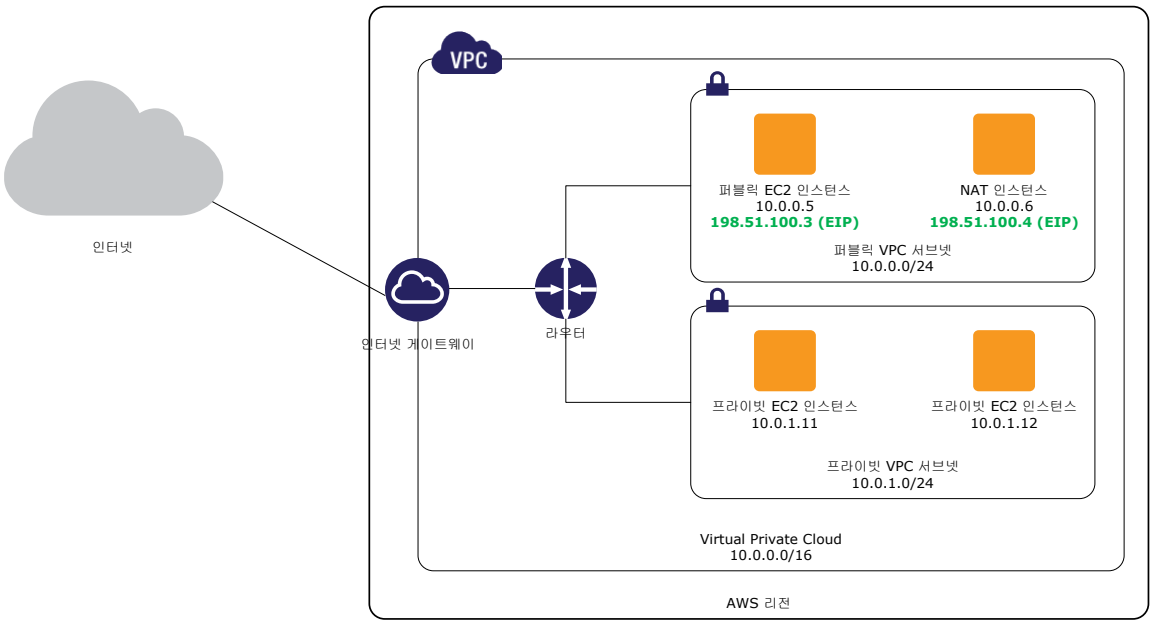

그림 2: 퍼블릭 및 프라이빗 서브넷을 사용하는 VPC 의 예

그림 3 에서 확인할 수 있는 바와 같이, VPC 에 가상 프라이빗 게이트웨이를 연결하면 VPN 과 사용자의 자체 데이터 센터 사이를 VPN 으로 연결할 수 있습니다. VPN 연결은 업계 표준 IPsec 터널(IKEv1-PSK, AES-128, HMAC-SHA-1, PFS)을 사용하여 각 게이트웨이를 상호 인증하고 데이터 전송 중의 도청 또는 훼손을 방지합니다. VPN 구성에서 이중화가 가능하도록 각각의 VPN 연결은 두 개의 터널로 구성되며, 터널은 각각 고유의 가상 프라이빗 게이트웨이 퍼블릭 IP 주소를 사용합니다.

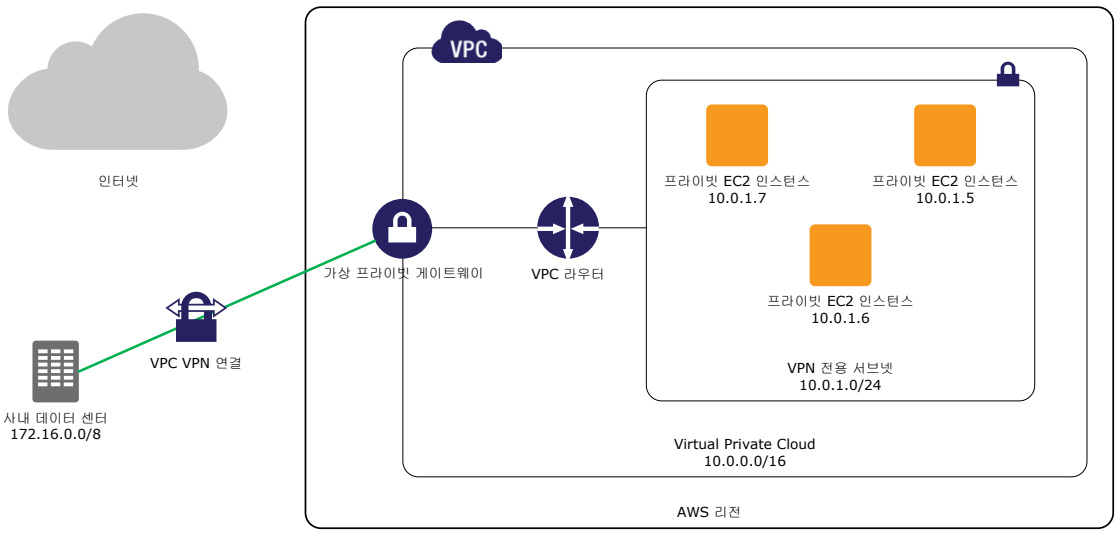

그림 3: 인터넷에서 격리되어 VPN 을 통해 기업 데이터 센터에 연결된 VPC 의 예

VPN 연결 설정에는 두 가지 라우팅 옵션이 있습니다. BGP(Border Gateway Protocol) 또는 정적 라우팅입니다. BGP 의 경우, VPC 에 연결하기 전 IP 주소와 고객 게이트웨이의 BGP ASN(자율 시스템 번호)가 필요합니다. 이 정보를 제공하고 나면, 각종 VPN 디바이스에 대한 구성 템플릿을 다운로드하여 VPN 터널 두 개를 구성할 수 있습니다. BGP 를 지원하지 않는 디바이스의 경우에는 VPN 연결을 구성할 때 해당 CIDR 범위를 제공함으로써 하나 이상의 정적 라우터를 온-프레미스 네트워크에 설치할 수 있습니다. 그러고 나서 IPsec 터널을 통해 VPC 로 트래픽을 라우팅하기 위해 VPN 고객 게이트웨이와 기타 내부 네트워크 디바이스에 정적 라우터를 구성합니다.

온-프레미스 네트워크에 연결된 가상 프라이빗 게이트웨이 하나만 선택할 경우, 인터넷 바운드 트래픽을 VPN 으로 라우팅하여 기존 보안 정책 및 네트워크 컨트롤로 아웃바운드 트래픽을 통제할 수 있습니다.

또한 AWS Direct Connect 를 사용해 온-프레미스 네트워크에서 Amazon VPC 로 직접 프라이빗 논리적 연결을 구축할 수 있습니다. AWS Direct Connect 를 사용하면 온 프레미스 네트워크에서 Amazon VPC 로 직접 사설 논리 연결을 구축할 수 있습니다. Multiple logical connections 을 통해 격리된 네트워크를 유지하면서도 다중 VPC 에 대해 private 연결망을 구축할 수 있습니다.

AWS Direct Connect 를 사용하면 AWS 와 아무 AWS Direct Connect 위치 사이에 1Gbps 또는 10Gbps 의 전용 네트워크 연결을 구축할 수 있습니다. 전용 연결은 업계 표준 802.1Q VLAN 을 사용해 여러 논리적 연결로 분할할 수 있습니다. 이렇게 하면 퍼블릭 리소스(예: 퍼블릭 IP 주소 공간을 사용하는 Amazon Simple Storage Service(Amazon S3)에 저장된 객체)와 프라이빗 리소스(예: 프라이빗 IP 공간을 사용하는 VPC 내에서 실행 중인 Amazon EC2 인스턴스)를 액세스할 때 동일한 연결을 사용하면서도, 퍼블릭 환경과 프라이빗 환경 사이의 네트워크 분리를 유지할 수 있습니다. 사용자는 AWS Partner Network(APN)에서 파트너를 선택하여 AWS Direct Connect 위치 내의 AWS Direct Connect 엔드포인트를 원격 네트워크에 연결할 수 있습니다. 그림 4 에서 일반적인 AWS Direct Connect 구성을 확인할 수 있습니다.

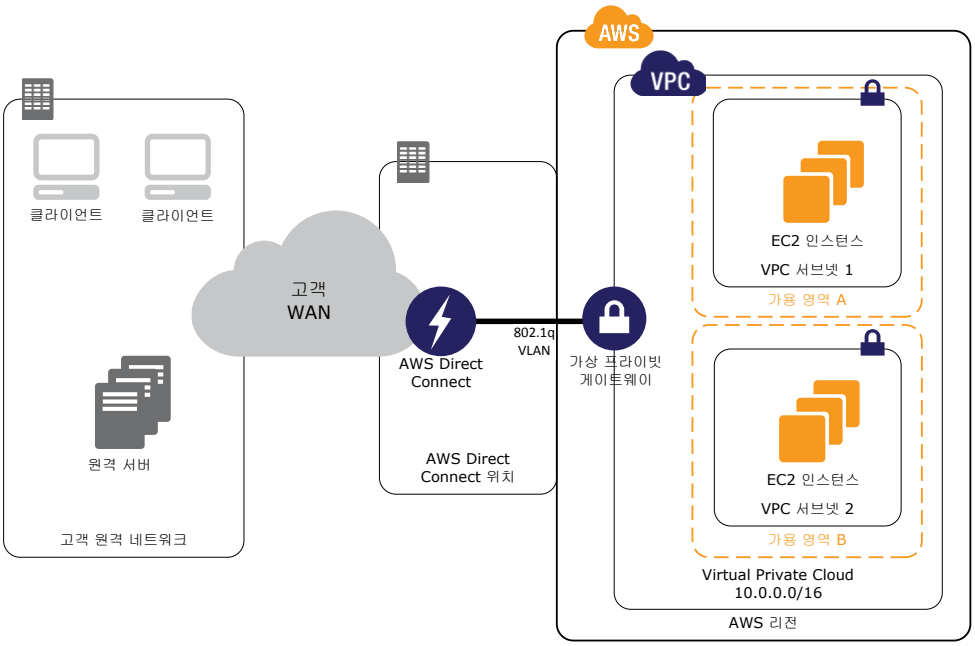

그림 4: VPC 와 AWS Direct Connect 를 고객 원격 네트워크와 함께 사용하는 예

마지막으로, 사용자의 비즈니스 및 보안 정책에 적합하도록 각종 옵션을 자유롭게 조합할 수 있습니다. 예를 들어, 가상 프라이빗 게이트웨이를 이용하여 VPC 를 기존 데이터 센터에 연결하고, 추가 퍼블릭 서브넷을 설정하여 Amazon S3, Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(Amazon SNS) 등 VPC 내에서 실행되지 않는 다른 AWS 서비스에 연결할 수 있습니다. 이때 Amazon EC2 의 IAM 역할을 활용하여 서비스에 액세스할 수 있고, IAM 정책을 구성하여 해당 NAT 서버의 엘라스틱 IP 주소에서의 액세스만 허용할 수도 있습니다.

예제 시나리오

Amazon VPC 는 매우 유연하므로, 다양한 사용 사례에서의 비즈니스 및 IT 보안 요건에 정확히 부합하는 가상 네트워크 토폴로지를 설계할 수 있습니다. Amazon VPC 의 진정한 잠재력을 이해하기 위해 가장 흔한 일반 사용 사례를 몇 가지 살펴보겠습니다.

- PCI 호환 전자 상거래 웹사이트 호스팅
- 개발 및 테스팅 환경 설계
- 재해 복구 및 비즈니스 연속성 계획
- 데이터 센터를 클라우드로 확장
- 비즈니스 유닛 네트워크 및 지점 생성

PCI 표준 준수 전자 상거래 웹사이트 호스팅

전자 상거래 웹사이트는 대개 신용카드 정보, 사용자 정보 및 구매 내역 등의 민감한 데이터를 취급합니다. 민감한 고객 데이터를 보호하기 위해서는 PCI DSS(Payment Card Industry Data Security Standard)를 준수하는 인프라가 필수적입니다.

AWS 는 PCI DSS(Payment Card Industry Data Security Standard) 레벨 1 서비스 제공업체로 인증받았으므로, 사용자가 클라우드상의 신용카드 정보를 저장, 처리 및 전송할 수 있는 PCI 준수 기술 인프라에서 애플리케이션을 실행할 수 있습니다. 전자 상거래 웹사이트 운영자는 자체 PCI 자격증을 관리해야 하지만, AWS 와 같은 인증된 인프라 서비스 제공업체를 이용하면 인프라 수준의 PCI 표준 준수를 위해 별도로 노력할 필요가 없습니다. PCI 표준 준수에 대한 자세한 내용은 AWS 규정 준수 센터를 참조하십시오.

예를 들어, 사용자는 VPC 를 생성해 고객 데이터베이스를 호스팅하고 전자 상거래 웹사이트의 체크아웃 프로세스를 관리할 수 있습니다. 고가용성을 확보하기 위해서는 동일한 리전 내의 각 가용 영역에 프라이빗 서브넷을 설치하고 고객 및 주문 관리 데이터베이스를 배포하면 됩니다. 이 경우 체크아웃 서버는 각 가용 영역의 사설 서브넷에 걸쳐 있는 Auto Scaling 그룹에 속하게 됩니다. 이 서버는 각 가용 영역에 자리잡은 공개 서브넷들을 망라하는 Elastic Load Balancer 뒤에 위치합니다. VPC, 서브넷, 네트워크 ACL, 보안 그룹을 결합하여 AWS 인프라에 대한 액세스를 세밀하게 제어할 수 있습니다. 전자 상거래 웹사이트에서 가장 민감한 부분에 대한 주요 과제, 즉 확장성, 보안, 탄력성 및 가용성 문제에 대비할 수 있습니다. 그림 5 에서 체크아웃 아키텍처의 예를 확인할 수 있습니다.

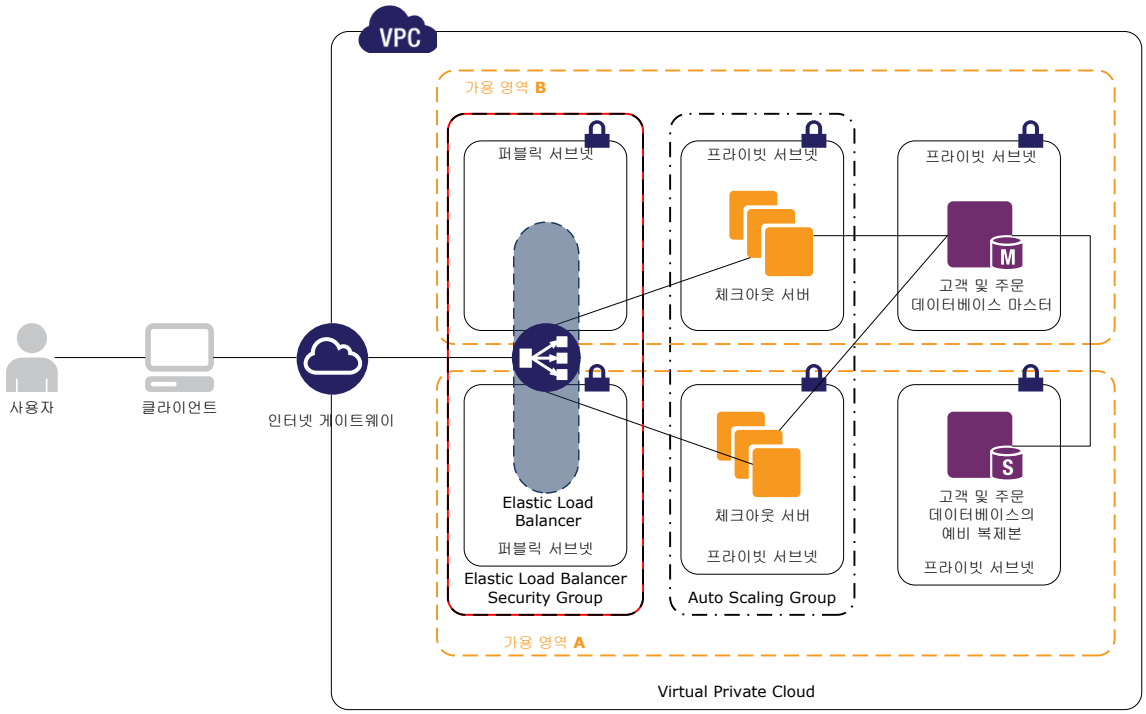

그림 5: 체크아웃 아키텍처의 예

개발 및 테스팅 환경 구축

소프트웨어 환경은 새로운 버전, 추가 기능, 패치 및 업데이트로 계속 변화합니다. 소프트웨어에 변화가 있을 경우 빠르게 배포해야 하므로, 회귀 검사를 실시할 시간이 부족합니다. 이상적인 테스트 환경은, 프로덕션 환경을 정확하게 복제하여 업데이트를 적용하고 평소의 워크로드를 테스트하는 것입니다. 업데이트 또는 신규 버전이 모든 테스트를 통과하면, 확신을 가지고 프로덕션 단계로 넘길 수 있을 것입니다.

이런 테스트 환경을 자체적으로 구축하려면 평소에는 거의 사용할 일이 없는 하드웨어를 대량으로 프로비저닝해야 합니다. 때로는 이 미사용 하드웨어의 용도로 변경하기도 하는데, 그러면 정작 필요할 때 테스트 환경을 사용할 수 없습니다. Amazon VPC 를 사용하면 프로덕션 환경과 유사한 테스트 환경을 경제적이고 효과적으로 구축할 수 있습니다. 테스트 환경은 필요할 때만 실행하고 테스트를 완료한 후에는 닫을 수 있습니다. 고가의 하드웨어를 구매할 필요가 없기 때문에 급변하는 소프트웨어 및 비지니스 환경에 더 유연하고 민첩하게 대응할 수 있습니다, 사용자가 만든 테스트 환경은 LDAP, 메시징 및 모니터링 등을 통해 사용자의 온-프레미스 네트워크 내에서 투명하게 상호작용합니다. 그리고 사용자는 실제 사용한 만큼만 비용을 지불하면 됩니다. 이 프로세스는 전체적으로 자동화되어 소프트웨어 개발 단계에 통합될 수도 있습니다. 그림 6 에서 개발 및 테스트 환경의 예를 확인할 수 있습니다.

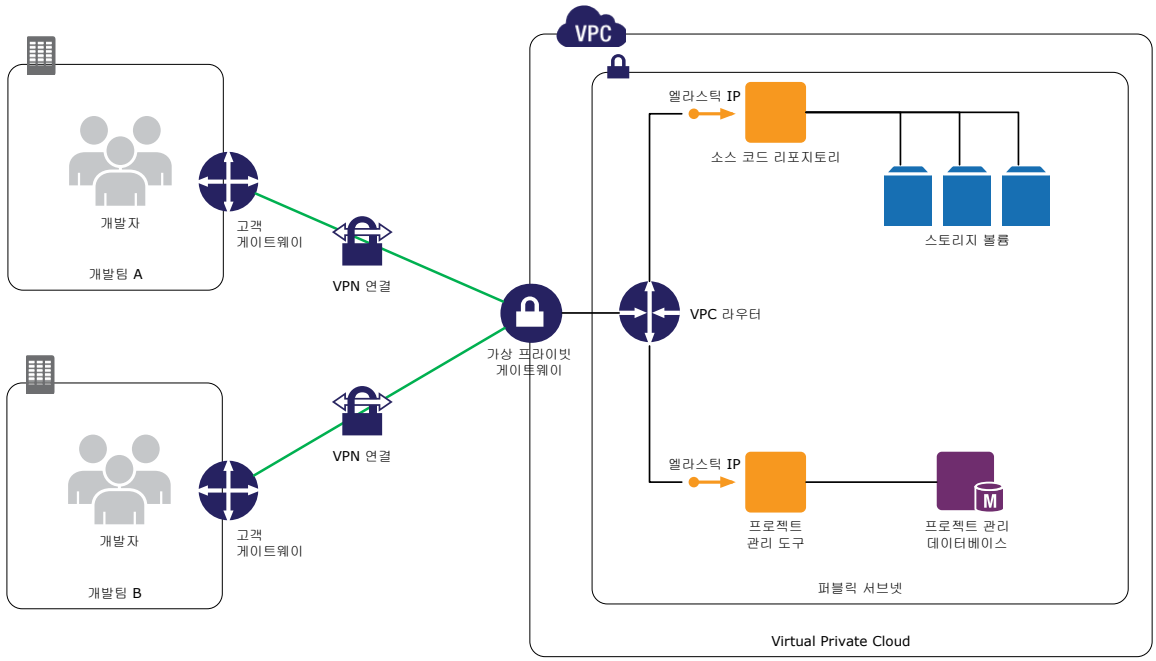

그림 6: 개발 및 테스트 환경의 예

실험 애플리케이션에는 동일한 로직이 적용됩니다. 생산 환경에서 분리하고자 하는 새로운 소프트웨어 패키지를 평가할 경우, 이를 PVC 의 테스팅 환경 내 몇 개의 Amazon EC2 인스턴스에 설치하고 선택된 내부 사용자 세트에 액세스를 부여할 수 있습니다. 새로운 소프트웨어의 테스트가 성공적이라면, 해당 이미지를 개발 환경으로 옮기고 불필요한 리소스를 중단할 수 있습니다.

재해 복구 및 비즈니스 연속성 계획

데이터 센터에 영향을 미치는 자연 재해에 미리 대비하지 않으면 비즈니스에 막대한 손실이 발생할 수 있습니다. 자연 재해가 비즈니스 운영에 미치는 영향을 최소화하기 위한 전략을 수립하는 데는 시간을 투자할 가치가 있습니다. 재해 복구에 대한 기존의 접근방식은 보통 노동집약적인 백업 및 고가의 예비 장비를 필요로 합니다. 이제는 이 대신 재해 복구 계획에 Amazon VPC 의 활용을 고려할 수 있습니다. AWS 의 탄력적이고도 역동적인 특성은 리소스 요구 사항에 갑작스러운 요청 급증 현상 생길 수 있는 자연 재해 상황에 적합합니다.

비즈니스에 가장 중요한 IT 자산을 파악하는 것부터 시작하십시오. 본 문서에서 테스트 환경에 대해 설명한 대로, 사용자는 중요한 자산의 기능을 복제하기 위해 서비스에 사용되는 개발 환경을 자동으로 복제할 수 있습니다. 자동화 프로세스를 통해 프로덕션 데이터를 Amazon Elastic Block Store(EBS) 볼륨 또는 Amazon S3 버킷에 백업할 수 있습니다. 또한, 사전 정의가 가능한 AWS CloudFormation 템플릿을 작성해 기존 온-프레미스 환경과 동일하게 구성된 VPC 인프라 스택을 정의할 수 있으며 필요시 어떤 AWS 리전 혹은 가용 영역에든 이를 자동으로 구축할 수 있습니다.

자연 재해가 발생하면 신속하게 서비스 환경을 그대로 복제한 VPC 환경을 구축할 수 있으며, 이후 재해가 발생한 지역에 연결되는 비즈니스 트래픽을 이 VPC 환경으로 리다이렉션할 수 있습니다. 자연 재해로 인해 자체 서비스 환경에서 데이터 부분만 유실될 경우, VPC 에서 백업 스토리지로 쓰고 있던 Amazon EBS 데이터 볼륨에서 그 부분을 불러와 복구할 수 있습니다.

자세한 내용은 Using Amazon Web Services for Disaster Recovery(Amazon Web Services 를 이용한 재해 복구) 를 참조하십시오. AWS 아키텍처 센터에서 확인할 수 있습니다.

데이터 센터를 클라우드로 확장하기

자체 데이터 센터 구축에 투자를 했다면, 계속해서 변하는 서비스 용량의 요구사항에 대응하기가 힘들 것입니다. 가끔은 서비스 용량에 대한 이런 수요가 현재 보유한 전체 용량을 초과하는 경우도 있습니다. 비즈니스가 성공을 거둔다면 일반적인 운영에 필요한 용량조차 계속 커져 결국 데이터 센터의 용량 한계에 도달하게 되고, 이 경우 용량을 늘릴 방법을 결정해야 할 것입니다. 새로운 데이터 센터를 구축하는 것도 하나의 방법이지만, 이 방법은 느리고 비용이 많이 드는 것은 물론 적절한 프로비저닝에 실패해 위험을 초래할 가능성이 높습니다. Amazon VPC 는 이러한 위험 없이 기존 데이터 센터에 부족한 용량을 추가로 프로비저닝할 수 있어 데이터 센터를 확장하는 도구 역할을 합니다.

Amazon VPC 에서는 IP 주소 범위를 직접 지정할 수 있으므로, 기존 네트워크를 신규 데이터 센터 또는 지사로 확장할 때와 마찬가지 방법으로 네트워크를 AWS 로 확장할 수 있습니다. VPN 과 AWS Direct Connect 연결 옵션을 통해 여러 네트워크를 매끄럽고 안전하게 통합하여, 물리적 위치와 무관하게 사용자와 애플리케이션을 지원하는 하나의 기업 네트워크를 구축할 수 있습니다. 또한 데이터 센터를 통해 물리적으로 확장할 때와 마찬가지로, 사용자 또는 시스템 관리자의 애플리케이션 액세스 및 관리 방식을 변경하지 않아도 VPC 에서 호스팅하는 IT 리소스가 사용자 인증, 모니터링, 로깅, 변화 관리, 배포 서비스 등 기존의 중앙 IT 시스템을 활용할 수 있습니다.

확장 가상 데이터 센터의 외부 연결도 고객이 자유롭게 설정할 수 있습니다. VPC 트래픽이 모두 기존 네트워크 인프라를 통과하도록 설정하여, 기존의 내외부 네트워크에 대한 Amazon EC2 인스턴스의 액세스 권한을 제어할 수 있습니다. 이 방법을 택하면 예컨대 기존의 인터넷 기반 네트워크 컨트롤을 네트워크 전체에 그대로 활용할 수 있습니다. 그림 7 에서 AWS 로 확장한 데이터 센터의 예를 확인할 수 있습니다.

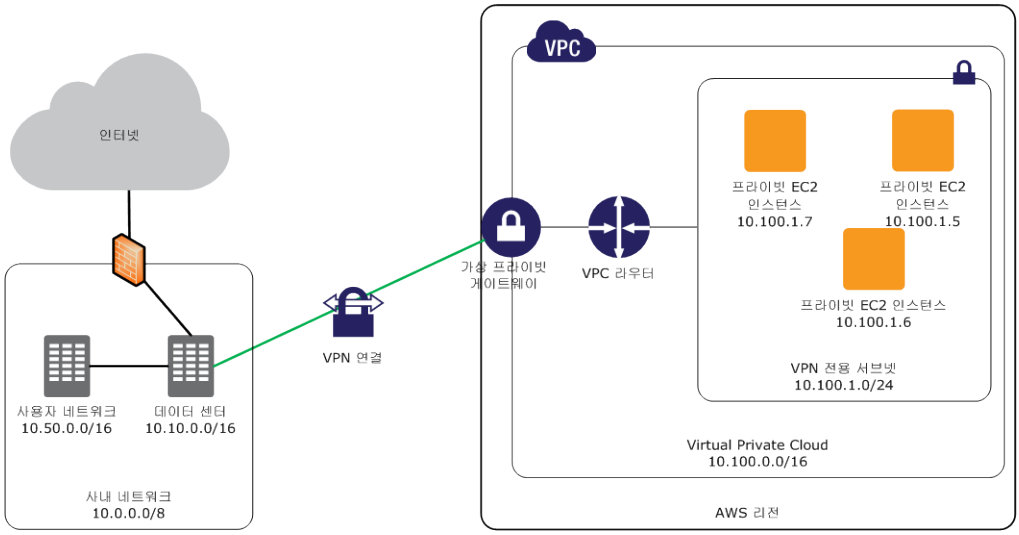

그림 7: 고객의 기존 인터넷 연결을 활용하는 AWS 확장 데이터 센터의 예

또한 그림 8 에서처럼 필요에 따라 VPC 에서 고객에게 직접 제공하고자 하는 인터넷 방면 트래픽의 하위 집합에 대해 AWS 인터넷 파이프를 활용하는 한편으로, 백엔드 리소스에 VPN 으로 연결하여 매끄러운 최종 사용자 경험을 제공할 수 있습니다.

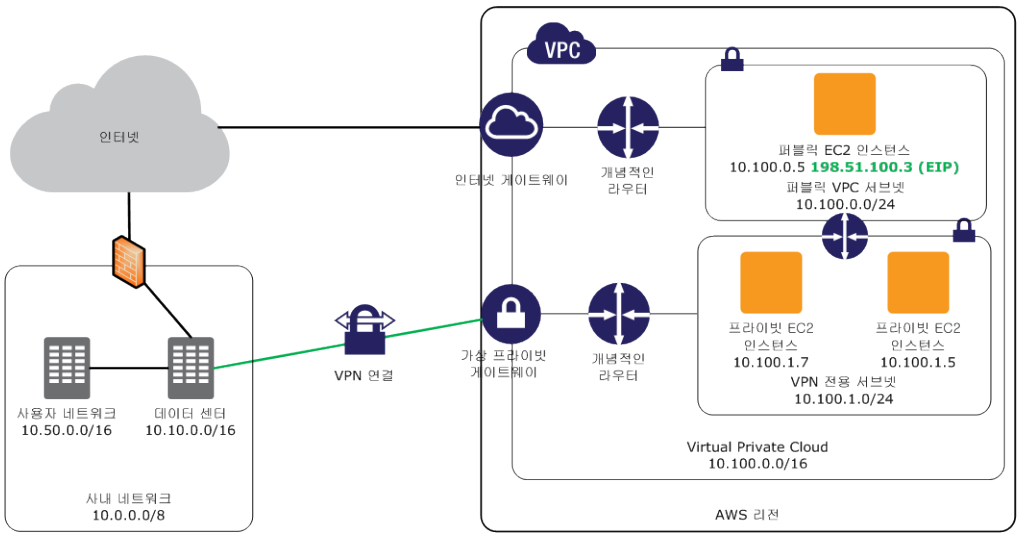

그림 8: 다중 인터넷 연결을 활용하는 AWS 확장 데이터 센터의 예

지사 및 사업 부문 네트워크 생성하기

기업의 지사에 별도 로컬 네트워크를 구축한 후 이를 서로 연결해야 하는 경우에는, Amazon VPC 내부에서 리소스를 배포하고 각 지사에 자체 서브넷을 할당하는 방법을 고려해 볼 수 있습니다. VPC 서브넷 내의 애플리케이션은 고객이 지정하는 VPC 보안 그룹 규칙에 따라 서로 통신할 수 있습니다. 또한 가상 라우터를 통해 각기 다른 서브넷에 존재하는 애플리케이션끼리 통신할 수도 있습니다. 서브넷 내부, 혹은 여러 서브넷 사이의 네트워크 통신을 제한해야 할 경우에는 보안 그룹 또는 네트워크 ACL 규칙을 구성하여 통신을 허용할 인스턴스를 지정할 수 있습니다. 사용할 수 있는 기능을 사업부마다 각기 다르게 구성해야 하는 경우에도 그룹 애플리케이션간의 통신에 이러한 방식의 제한을 가할 수 있습니다. 각 사업부별 애플리케이션을 각기 다른 별도의 서브넷에 설치해 두면 됩니다. 그림 9: 지사 시나리오에서의 VPC 및 VPN 의 활용 예에서 지사 시나리오에서 VPC 및 VPC 를 활용하는 예를 확인할 수 있습니다.

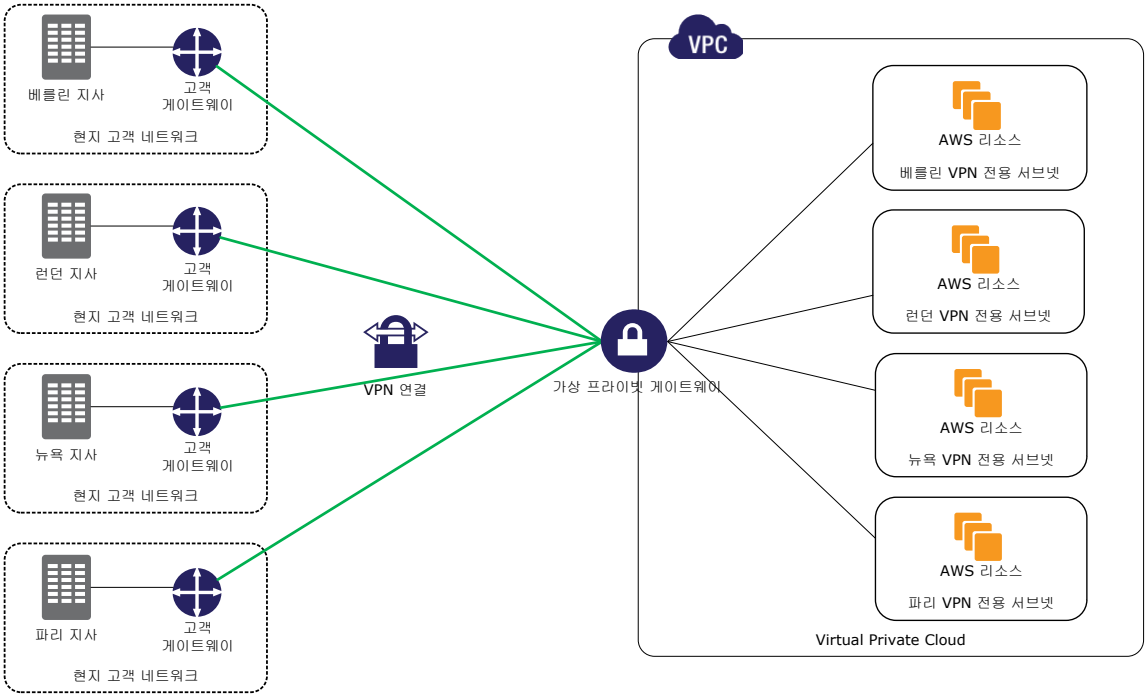

그림 9: 지사 시나리오에서의 VPC 및 VPN 의 활용 예

지사별로 프로비저닝된 온-프레미스 하드웨어와 VPC 를 병용하는 방식의 주요 이점은 다른 사용사례에서 언급한 것들과 크게 다르지 않습니다. 언더프로비저닝 또는 오버프로비저닝하지 않음을 보장하며 요구 사항에 따라 탄력적으로 리소스를 확장 축소하여 할 수 있습니다. 용량을 추가하는 것은 아주 쉽습니다. 사용자 지정 Amazon Machine Images(AMIs)에서 Amazon EC2 인스턴스를 추가로 시작하기만 하면 됩니다. 용량을 줄여야 할 때에는 불필요한 인스턴스를 수동으로 종료하거나 Auto Scaling 정책을 설정해 자동으로 종료할 수 있습니다. 이러한 운영 작업은 자산이 정상적으로 작동하도록 관리한다는 점에서는 마찬가지지만, 원격 전담 인력이 필요 없고 쓰는 만큼만 요금을 지불하므로 비용을 절약할 수 있습니다.

Amazon VPC 활용 모범 사례

Amazon VPC 사용 시에 참고할 수 있는 모범 사례를 몇 가지 소개합니다.

- 인프라 배포 자동화
- VPC 내 다중 AZ 배포를 통한 고가용성 확보
- 보안 그룹 및 네트워크 ACL 활용
- IAM 사용자 및 정책을 통한 액세스 제어
- Amazon CloudWatch 를 통한 VPC 인스턴스 및 VPN 링크의 상태 모니터링

인프라 배포 자동화

인프라를 수동으로 관리하는 일은 대부분 지겹고 오류 발생도 잦으며, 느린 데다 비용도 많이 듭니다. 예를 들어 재해 복구 계획을 수립할 때는 수동 작업을 최대한 배제해야 합니다. 수동 작업은 복구 프로세스의 속도를 늦추기 때문이죠. 개발 및 테스트 환경 등 그 중요성이 덜한 경우에도 실제 서비스 환경과 똑같은 예비 환경을 갖춰 두는 것이 좋습니다. 서비스 환경을 수동으로 복제하는 것은 굉장히 어려운 일이며, 배포 단계에서 종속성과 관련된 문제를 초래하거나 이미 존재하는 그러한 문제들을 발견하지 못하고 지나칠 위험이 높습니다.

AWS CloudFormation 로 배포를 자동화하면 템플릿을 기록함으로써 필요 인프라를 사전 정의 방식으로 기술할 수 있습니다. 이 템플릿을 활용하면 어떤 AWS 지역으로든 사전 지정된 스택을 매우 빠른 속도로 배포할 수 있습니다. 템플릿을 사용해 AWS 리소스의 서브넷 생성, 라우팅 정보, 보안 그룹, 프로비저닝을 완전 자동화해 언제든 필요할 때 활용할 수 있습니다. AWS CloudFormation 헬퍼 스크립트를 사용하면, Amazon EC2 인스턴스 시작 시에 표준 Amazon 머신 이미지(AMI)로 배포에 적합한 버전의 소프트웨어를 한꺼번에 설치할 수 있습니다.

자동 인프라 배포를 프로세스에 완전히 통합하는 것이 바람직합니다. 자동화 스크립트를 표준 및 정책에 따라 테스트하며 관리해야 하는 소프트웨어와 마찬가지로 취급해야 합니다. 훌륭한 자동화 전략은 대부분의 VPC 사용 사례에 이득이 됩니다. 철저하게 테스트된 자동화 프로세스는 대부분의 경우 복잡한 수동 단계에 의존하는 프로세스 보다 빠르고 저렴하며 더 안정적입니다.

VPC 내 다중 AZ 배포를 통한 고가용성 확보

고가용성을 기반으로 한 설계는 일반적으로 AWS 리소스를 동일한 지역 내 여러 가용 영역에 걸쳐 다중으로 배포합니다. 한 가용 영역에서 서비스 중단이 일어날 경우, 사용자는 트래픽을 다른 가용 영역으로 리다이렉션해 장애의 영향을 최소화할 수 있습니다. 이는 일반적으로 많이 활용되는 모범적 접근법이며 Amazon VPC 를 포함한 설계에도 적용됩니다.

VPC 가 여러 가용 영역을 사용하고 있다고 해도, VPC 내 각각의 서브넷은 하나의 가용 영역에 제한됩니다. 예를 들어 다중 AZ Amazon RDS DB 인스턴스를 배포하기 위해서는, 먼저 데이터베이스 인스턴스를 시작할 리전 내의 각 가용 영역에 VPC 서브넷을 구성해야 합니다. 마찬가지로 Auto Scaling 그룹 및 Elastic Load Balancer 를 각 가용 영역의 서브넷에 배포하면 여러 가용 영역을 아우를 수 있습니다.

보안 그룹 및 네트워크 ACL 활용

Amazon VPC 는 Amazon EC2-Classic 환경에 추가적인 보안 기능을 제공합니다. 예를 들어, VPC 보안 그룹을 통해 인바운드 트래픽 및 아웃바운드 트래픽(Amazon EC2 보안 그룹은 인바운드만 통제)을 통제하고, 모든 IP 프로토콜 및 포트에 대한 규칙을 정의할 수 있습니다. (Amazon EC2 보안 그룹은 TCP, UDP, ICMP 에 대해서만 규칙을 정의합니다.) Amazon EC2 와 Amazon VPC 보안 그룹의 차이점을 모두 확인하려면 VPC 의 보안 그룹을 참조하십시오. Amazon EC2 및 Amazon VPC 보안 그룹 모두 상태 저장 방화벽입니다.

네트워크 ACL 의 경우, 허용 및 거절 규칙을 ingress 및 egress 트래픽 모두에 지정할 수 있습니다. 각각의 서브넷에 대해 액세스 콘트롤 규칙을 정의할 수 있습니다. VPC 보안 그룹이 인스턴스 레벨에서 작동할지라도 네트워크 ACL 은 서브넷 레벨에서 작동합니다. 네트워크 ACL 의 경우, *허용* 및 *거절* 규칙을 ingress 및 egress 모두에 지정할 수 있습니다. 네트워크 ACL 은 상태 비저장 방화벽입니다.

이들을 사용한 모범 사례는 다중 보호 계층으로 인프라를 보호하는 것입니다. VPC 에서 인프라를 실행함으로써 어떤 인스턴스를 인터넷에 먼저 노출할 지 제어할 수 있으며, 보안 그룹과 네트워크 ACL 을 지정하여 인프라 및 서브넷 수준에서 인프라의 보호를 강화할 수 있습니다. 추가로 운영 시스템 수준에서 방화벽으로 인스턴스를 보호해야 하며, AWS 보안 리소스에서 소개하는 기타 보안 모범 사례를 따라야 합니다.

IAM 사용자 및 정책을 통한 액세스 제어

AWS Identity and Access Management(IAM)를 통해 AWS 계정에 사용자를 생성하고 관리할 수 있습니다. 사용자는 사람일 수도 있고, AWS 와 상호작용해야 하는 애플리케이션일 수도 있습니다. IAM 으로 사용자, 액세스 자격 증명 등의 보안 자격 증명, 그리고 AWS 리소스에 대한 사용자의 액세스 권한을 중앙집중식으로 관리할 수 있습니다. 일반적으로 사용자의 경우에는 IAM 사용자를 생성하며, 애플리케이션의 경우에는 IAM 역할을 생성합니다.

*최소 권한*의 보안 전략을 구현할 때 IAM 을 사용하기를 권장합니다. 예를 들어, 기본 AWS 계정으로 AWS 인프라의 모든 측면을 관리하는 것은 바람직하지 않습니다. AWS 에서 수행해야 하는 개별 태스크에 대해 사용자 그룹을 지정하고, 각 사용자가 해당 역할을 수행하는 데 필요한 기능만 사용할 수 있도록 제한하는 것이 좋습니다. 그 예로, IAM 에 *네트워크 관리자* 그룹을 생성할 수 있는데, 해당 그룹에게만 VPC 를 생성 및 수정할 수 있는 권한을 줄 수 있습니다. 각 사용자 그룹에 대해서 제한적인 *규정*을 지정하여 각 사용자가 필요한 서비스에만 액세스할 수 있도록 합니다. 조직 내 자격 증명이 된 사람만이 이 사용자 계정에 대한 액세스를 갖도록 해야하며, 주기적으로 자격 증명을 변경해 인프라에 대한 리스크를 줄이는 것이 좋습니다.

IAM 사용자 및 정책 정의에 대한 자세한 정보는 Amazon VPC 리소스 액세스 권한 제어를 참고하십시오.

Amazon CloudWatch 를 통한 VPC 인스턴스 및 VPN 링크의 상태 모니터링

일반적인 Amazon EC2 인스턴스처럼 VPC 에서 실행되는 인스턴스의 성능도 Amazon CloudWatch 로 모니터링할 수 있습니다. Amazon CloudWatch 는 리소스 활용도, 운영 성능 및 전반적인 수요 패턴을 가시적으로 보여주며, 이는 CPU 사용율과 디스크 읽기 및 쓰기, 네트워크 트래픽 등을 포함합니다. 이 정보는 AWS Management Console 에 표시되며 Amazon CloudWatch API 를 통해서도 확인할 수 있어 기존 관리 도구에 통합할 수 있습니다.

AWS Management Console 을 사용하거나 API 를 호출하여 VPN 연결 정보를 확인할 수도 있습니다. VPN 터널 정보에서는 해당 VPN 터널의 상태(가동/미가동)를 확인할 수 있고, 미가동인 경우 관련 오류 메시지를 볼 수 있습니다.

결론

Amazon VPC 는 다양한 도구를 제공해 사용자가 AWS 인프라를 더 세밀하게 제어할 수 있도록 해 줍니다. VPC 내에서는 서브넷 및 라우팅 테이블을 지정함으로써 자체 네트워크 토폴로지를 구성할 수 있으며 서브넷 수준에서는 네트워크 ACL 로, 리소스 수준에서는 VPC 보안 그룹으로 액세스를 제한할 수 있습니다. 리소스를 Internet 으로부터 격리하고 VPN 을 통해 이를 자체 데이터 센터에 연결할 수 있습니다. 일부 인스턴스에만 엘라스틱 IP 주소를 지정하고 인터넷 게이트웨이를 통해 이를 공개 Internet 으로 연결하는 동시에 나머지 인프라는 사설 서브넷 내에만 유지하는 것도 가능합니다. VPC 는 AWS 가 제공하는 유연성, 확장성, 탄력성, 성능, 가용성, 사용량에 따라 지불하는 요금 모델의 이점을 모두 누리면서도 AWS 리소스를 쉽게 보호하도록 해 줍니다.

참조 자료

- Amazon VPC 제품 페이지: http://aws.amazon.com/vpc/
- Amazon VPC 문서: http://aws.amazon.com/ko/documentation/vpc/
- AWS Direct Connect 제품 페이지: http://aws.amazon.com/directconnect/
- AWS Direct Connect 문서: http://aws.amazon.com/documentation/directconnect/
- AWS 아키텍처 센터: http://aws.amazon.com/architecture/
- AWS 규정 준수 센터: http://aws.amazon.com/compliance/
- AWS 보안 센터: http://aws.amazon.com/security/
- AWS 보안 리소스: http://aws.amazon.com/security/security-resources/
- Amazon VPC 연결 옵션: http://media.amazonwebservices.com/AWS_Amazon_VPC_Connectivity_Options.pdf
- AWS 보안 모범 사례: http://media.amazonwebservices.com/AWS_Security_Best_Practices.pdf
- AWS 를 이용한 재해 복구: http://media.amazonwebservices.com/AWS_Disaster_Recovery.pdf
- 클라우드에서의 아키텍처 설계: 모범 사례: http://media.amazonwebservices.com/AWS_Cloud_Best_Practices.pdf

버전 기록

2013 년 12 월

- Amazon VPC 의 새로운 기능을 반영하는 주요 수정 사항
- VPC 사용 사례 추가
- “Amazon Virtual Private Cloud 에 대한 이해” 섹션 추가
- “Amazon VPC 활용 모범 사례” 섹션 추가

2010 년 1 월

- 최초 릴리스