Amazon Virtual Private Cloud 를 이용한 IT 인프라의 확장

최초작성일: 2010 년 1 월

최종수정일: 2012 년 9 월

목차

서론

Amazon Virtual Private Cloud(VPC) 기능은 사용자가 Amazon Web Services(AWS) 클라우드를 분리해 사적인 공간을 프로비저닝할 수 있도록 해 주며, 이 격리된 공간 안에서는 사용자가 정의한 가상 네트워크를 기반으로 AWS 서비스를 사용할 수 있습니다. Amazon VPC 를 이용하면 사용자의 데이터 센터에서 운영하는 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.

- 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. AWS 가 획득한 인증 및 승인에 대한 전체 목록은 AWS 보안 및 규정 준수 센터[1]에서 확인하실 수 있습니다.

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

[1] http://aws.amazon.com/ko/security/

Amazon Virtual Private Cloud에 대한 이해

개요

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. 그리고 이 주소를 Classless Inter-Domain Routing[2](CIDR) 블록 형태로 지정합니다 (예시> 10.0.0.0/16). /28 (16 IP 주소)과 /16 (65,536 IP 주소) 사이에서 네트워크의 블록 크기를 지정할 수도 있습니다.

Amazon VPC 에서 각각의 Amazon EC2 인스턴스는 Amazon VPC 네트워크에서 주 사설 IP 주소로 지정된 기본 네트워크 인터페이스를 갖습니다. 사용자는 추가적인 Elastic Network Interfaces(ENI)를 생성해 VPC 내의 모든 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 인스턴스가 지원하는 ENI 와 사설 IP 주소의 총 개수는 인스턴스 유형[3]에 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. 다중 IP 및 EIP 지원의 가장 큰 장점은 단일 서버에 다중 SSL 인증서를 사용하고 각 인증서를 특정 IP 주소에 연결할 수 있다는 것입니다.

Amazon Virtual Private Cloud 사용 설명서[4]에 기록된 대로 VPC 에 배포할 수 있는 많은 구성 요소에 대한 기본적인 제한이 있습니다. 이러한 제한을 강화하려면 Amazon VPC Limits form[5]을 작성하십시오.

---

2 http://ko.wikipedia.org/wiki/%EC%82%AC%EC%9D%B4%EB%8D%94_(%EB%84%A4%ED%8A%B8%EC%9B%8C%ED%82%B9)

3 http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/instance-types.html

4 http://docs.amazonwebservices.com/AmazonVPC/latest/UserGuide/VPC_Appendix_Limits.html

5 http://aws.amazon.com/contact-us/vpc-request/

다양하게 지원되는 네트워크 구성

VPC 에서는 서브넷을 목적에 따라 공개, 사설, 또는 VPN 전용으로 설정할 수 있습니다. 공개 서브넷을 설정하려면 해당 서브넷에서 인터넷으로 연결되는 트래픽이 VPC 와 연결된 인터넷 게이트웨이를 통해 라우팅되도록 라우팅 테이블을 구성해야 합니다. EIP 주소를 서브넷의 인스턴스에 지정하면 인터넷에서 인스턴스로 연결되도록 할 수 있습니다. 하지만 가장 좋은 방법은 해당 서브넷의 Network ACL[6] (네트워크 접근 통제 목록, Network Access Control List)과 인스턴스들의 보안 그룹[7]을 설정해 이 인스턴스들에 대한 ingress 및 egress 트래픽을 모두 제한하는 것입니다.

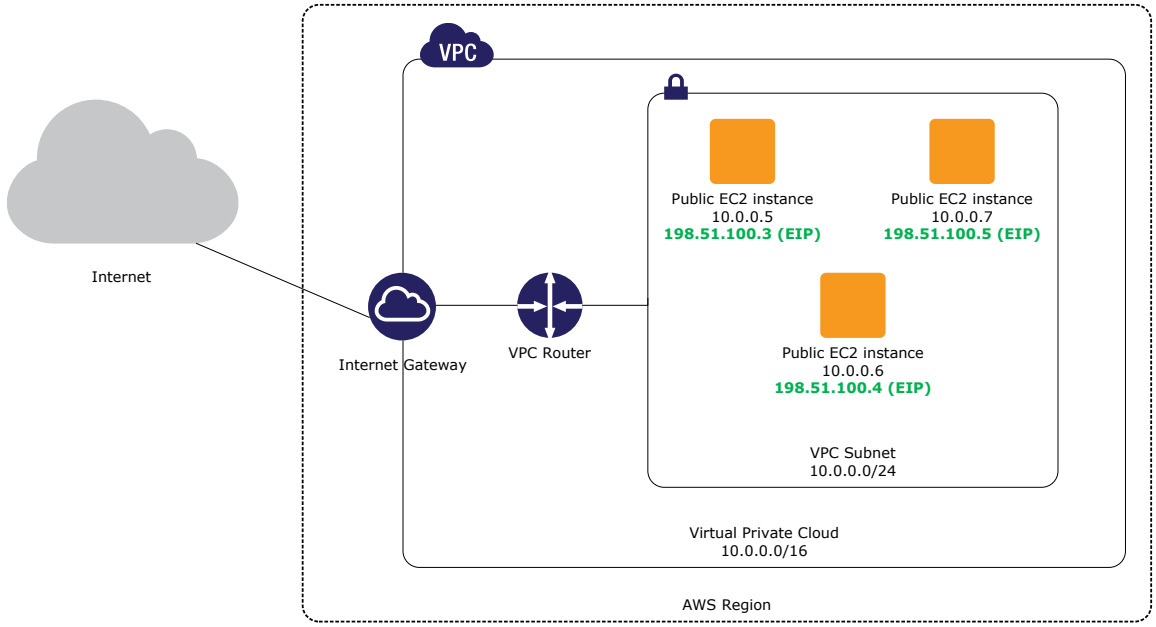

그림 1 – 공인 서브넷만 사용하는 VPC 의 예

사설 서브넷을 구축하는 경우, 해당 서브넷에서 인터넷으로 나가는 트래픽은 공인 EIP 를 사용하는 공개 서브넷 내의 특수 NAT(Network Address Translation) 인스턴스를 통해 라우팅되어야 합니다. 이 구성은 사설 서브넷의 리소스가 EIP 를 할당하거나 직접 인바운드 연결을 수용하지 않고도 아웃바운드 트래픽을 인터넷에 연결하도록 해 줍니다. AWS 는 미리 구성된 NAT 서버 AMI 를 제공하므로 사용자가 이를 쉽게 사용할 수 있습니다.

[6] http://docs.amazonwebservices.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html

[7] http://docs.amazonwebservices.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

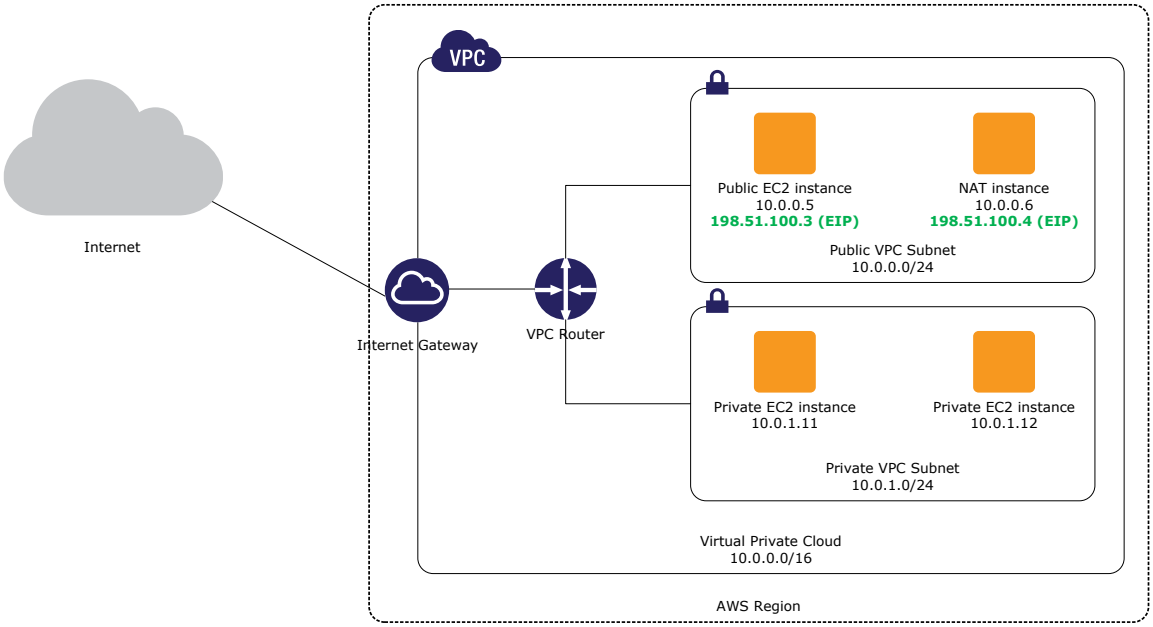

그림 2 - 공개 및 사설 서브넷을 사용하는 VPC 의 예

VPC 에 virtual private gateway 를 연결하면 VPN 과 사용자의 자체 데이터 센터 사이를 VPN 으로 연결할 수 있습니다. 이 VPN 연결은 뮤추얼 게이트웨이 인증 기능을 제공하고 데이터가 전송되는 동안 도청되거나 변경될 가능성을 막기 위해 산업 표준 IPsec 을 터널 모드 (IKEv1-PSK, AES-128, HMAC-SHA-1, PFS)로 사용합니다. IPsec 은 추가적으로 최소화된 캡슐화 기능을 제공하기도 합니다. VPN 구성에서 이중화가 가능하도록 각각의 VPN 연결은 두 개의 터널로 구성되며, 이 터널들은 각각 고유의 virtual private gateway 공개 IP 주소를 사용합니다.

VPN 연결, Border Gateway Protocol[8](BGP) 또는 정적 라우팅을 설정하는 두 가지 라우팅 옵션이 있습니다. BGP 의 경우, IP 주소와 VPN 에 연결할 고객 게이트웨이의 Autonomous System Number(ASN)가 필요합니다. 사용자가 VPN 구성에 이 정보를 제공하면, 지원되는 고객 게이트웨이 하드웨어 또는 어플라이언스의 설정 파일을 다운로드하여 고객 게이트웨이와 VPC 사이의 VPN 터널을 구성할 수 있습니다. BGP 를 지원하지 않는 디바이스의 경우에는 VPC 연결을 구성할 때 해당 CIDR 범위를 제공함으로써 하나 이상의 정적 라우터를 온-프레미스 네트워크에 설치합니다. 그리고 나서 IPSec 터널을 통해 VPC 로 트래픽을 라우팅하기 위해 고객의 VPN 게이트웨이와 다른 내부 네트워크 디바이스에 정적 라우터를 구성합니다.

8 http://en.wikipedia.org/wiki/Border_Gateway_Protocol

온-프레미스 네트워크에 연결된 virtual private gateway 만을 선택할 경우, 인터넷-바운드 트래픽을 VPN 으로 라우팅하여 기존 온-프레미스에 연결된 인터넷 연결을 사용하여 조직의 보안 규정 및 방화벽으로아웃바운드 트래픽을 통제할 수 있습니다.

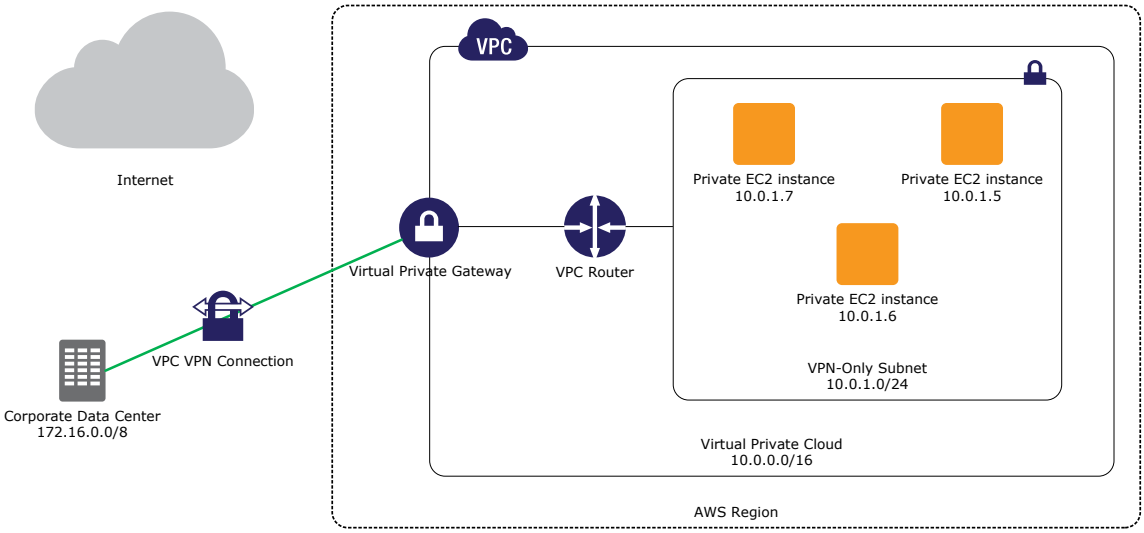

그림 3 - 인터넷에서 격리된 VPC 및 VPN 을 통해 기업 데이터 센터에 연결된 VPC 의 예

AWS Direct Connect 를 사용하면 온-프레미스 네트워크에서 Amazon VPC 로 직접 사설 논리 연결을 구축할 수 있습니다. AWS Direct Connect 는 네트워크와 VPC 간의 사설, 고대역폭 네트워크 연결을 제공합니다. Multiple logical connections 을 통해 격리된 네트워크를 유지하면서도 다중 VPC 에 대해 private 연결망을 구축할 수 있습니다.

AWS Direct Connect 를 사용하면 AWS 와 모든 AWS Direct Connect locations[9] 사이에 1Gbps 또는 10Gbps 의 전용 네트워크 연결망을 구축할 수 있습니다. 전용 연결망은 산업 표준 802.1q VLAN 를 이용하여 Multiple logical connections 로 분할할 수 있습니다. 이렇게 하면, 공개 IP 주소 공간을 사용하는 Amazon Simple Storage Service(Amazon S3)에 저장된 객체와 같은 AWS 의 다른 공개 리소스와 더불어, 사설 IP 공간을 사용하여 VPC 내에서 작동하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스와 같은 사설 리소스에 접근하는데 동일한 연결망을 사용할 수 있는데, 이는 하나의 연결을 사용하면서도 공개 환경과 사설 환경 간의 네트워크 독립성을 유지하는것을 가능하게 합니다. WAN 서비스 제공업체[10]의 에코시스템에서 원격 네트워크를 사용하여 AWS Direct Connect endpoint 를 AWS Direct Connect location 에 통합하도록 선택할 수 있습니다. Figure 4 그림 4 는 일반적인 AWS Direct Connect 설치를 나타냅니다.

---

[9] 지원되는 Direct Connect locations 및 서비스 제공업체에 대한 자세한 내용은 http://aws.amazon.com/ko/directconnect/를 참조하십시오.

[10] http://aws.amazon.com/ko/directconnect/#details

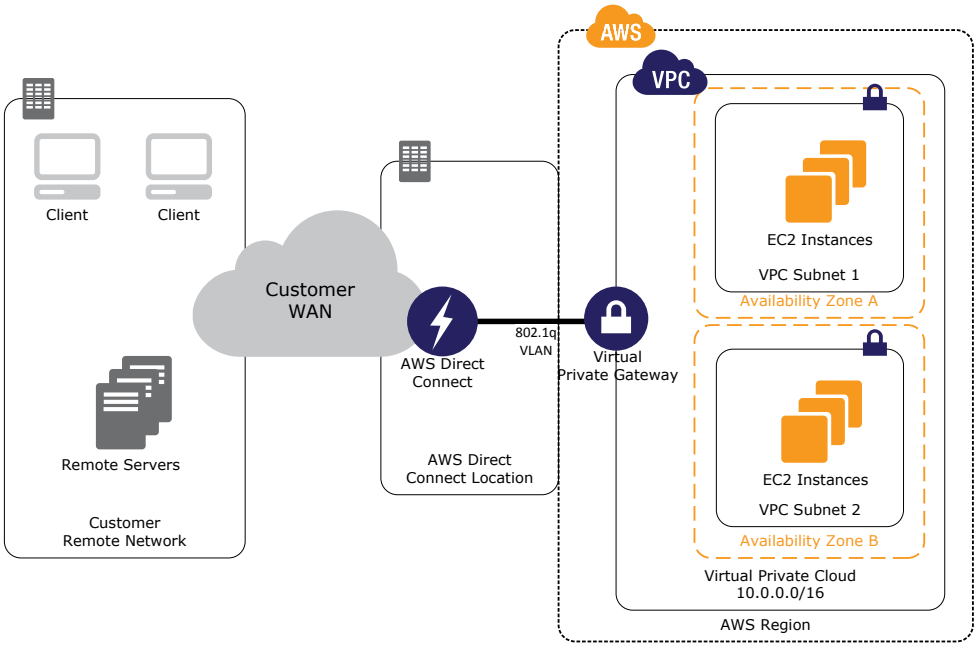

그림 4 - 고객 원격 네트워크를 이용한 VPC Direct Connect

사용자는 이렇게 구성된 환경에 다른 모든 시설 및 AWS 의 서비스를 결합할 수 있습니다. 예를 들어, virtual private gateway 를 이용하여 VPC 를 기존 데이터 센터에 연결하고 Amazon S3, Amazon Simple Queue Service (Amazon SQS) 또는 Amazon Simple Notification Service(Amazon SNS) 등 VPC 내에서 실행되지 않는 다른 AWS 서비스 제공업체에 추가 공인 서브넷을 설치할 수 있습니다. 이 경우, 이러한 서비스에 대한 AWS Identity and Access Management(IAM) 전용 사용자를 구성하고 NAT 서버의 엘라스틱 IP 주소만 수용하도록 그들에 대한 IAM 규정을 설정해야 합니다.

예제 시나리오

Amazon VPC 의 탁월한 유연성은 다양한 상황에서의 비즈니스 및 IT 보안 요구조건에 정확히 부합하는 가상 네트워크 토폴로지를 설계할 수 있도록 해 줍니다. Amazon VPC 의 진정한 가능성을 이해하기 위해 일반적인 사용 사례를 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
- 가상 데스크톱 인프라 생성

PCI 호환 전자 상거래 웹사이트 호스팅

전자 상거래 웹사이트는 대개 신용 카드 정보, 사용자 정보 및 구매 내역 등의 민감한 데이터를 처리합니다. 이렇게 민감한 고객 데이터를 보호하기 위해서는 PCI DSS (Payment Card Industry Data Security Standard) 호환 인프라가 필수적입니다.

AWS 는 Payment Card Industry Data Security Standard (PCI DSS) Level 1 서비스 제공업체로 인증받았기 때문에 클라우드에서 신용 카드 정보를 저장, 처리 및 전송할 수 있는 PCI 호환 기술 인프라 상에서 애플리케이션을 실행할 수 있습니다. 전자 상거래 웹사이트의 운영자는 여전히 서비스의 PCI 인증을 관리해야 하지만, AWS 와 같은 인증된 인프라 서비스 제공업체를 이용하면 인프라 수준에서 PCI 규정 준수에 따른 별도의 노력을 할 필요가 없습니다. PCI 규정 준수에 대한 자세한 내용은 AWS 보안 센터[11]를 참조하십시오.

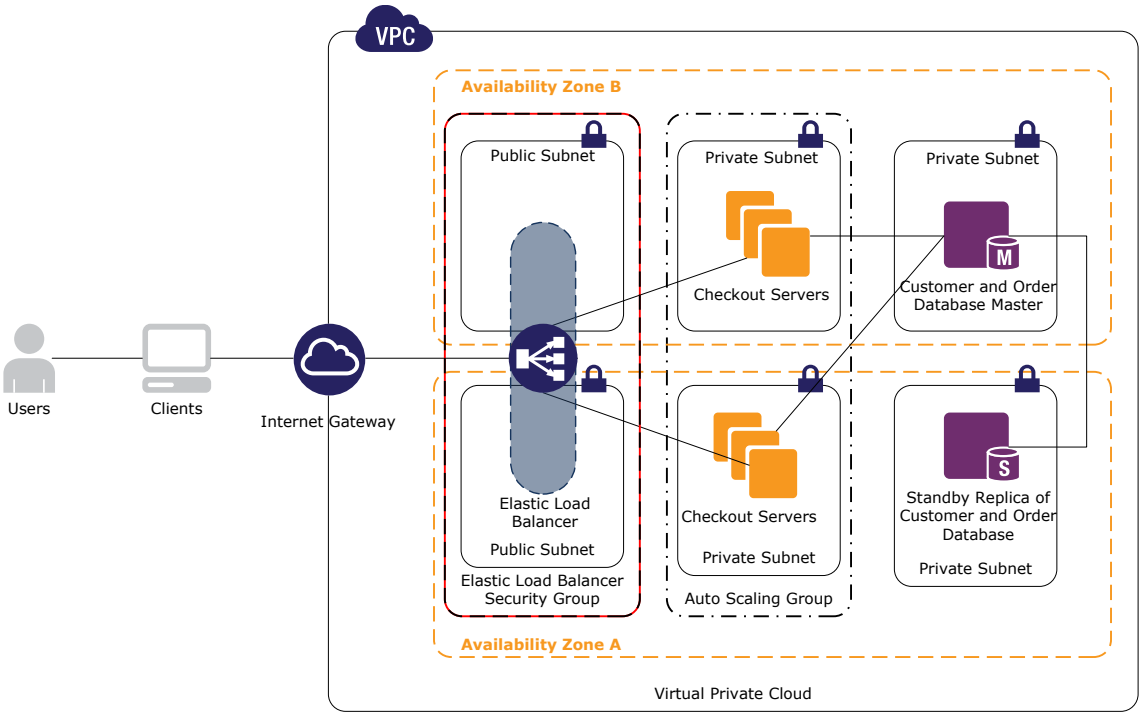

그림 5 – 체크아웃 아키텍처의 예

11 http://aws.amazon.com/ko/security/#certifications

예를 들어, 사용자는 VPC 를 생성해 고객 데이터베이스를 호스팅하고 전자 상거래 웹사이트의 체크아웃 프로세스를 관리할 수 있습니다. 고가용성을 확보하기 위해서는 동일한 지역 내의 가용 영역 여러 곳에 사설 서브넷을 설치하고 각각의 가용 영역에 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 결합함으로써 사용자는 AWS 인프라 액세스를 정교하게 제어할 수 있으며 전자 상거래 웹사이트에서 가장 민감한 부분인 확장성, 보안, 탄력성 및 가용성과 관련한 문제에 대비할 수 있습니다.

개발 및 테스팅 환경 구축

소프트웨어 환경은 새로운 버전, 추가 기능, 패치 및 업데이트로 계속 변화합니다. 소프트웨어 변화는 짧은 시간 내에 회귀 검사를 마치고 신속히 배포되어야 합니다. 개발 환경을 완벽히 복제하면 업데이트를 적용하고 평소의 워크로드 패턴을 테스트해 볼 수 있는 이상적인 실험공간이 될 것입니다. 업데이트 또는 새로운 버전이 모든 테스트를 통과하면 해당 버전에 대한 신뢰를 가지고 실제 개발에 투입할 수 있을 것입니다.

이런 실습 환경을 자체적으로 구축하려면 다른 때는 사용되지도 않는 많은 양의 하드웨어를 프로비저닝해야 합니다. 이 하드웨어들이 실습 및 테스트 환경에만 쓰이기보다는 개발용 하드웨어로 그 용도가 변경되는 경우가 많습니다. Amazon VPC 는 사용자가 실제 개발 환경을 시뮬레이션할 수 있는 경제적이고 기능적인 실습 환경을 구축하여 개발 환경에 영향을 미치지 않고 새로운 기능을 테스트할 수 있도록 지원합니다. 필요하면 즉시 테스트 환경을 만들 수 있고, 테스트가 끝나면 제거할 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 완전히 자동화되어 소프트웨어 개발 단계에 통합될 수도 있습니다.

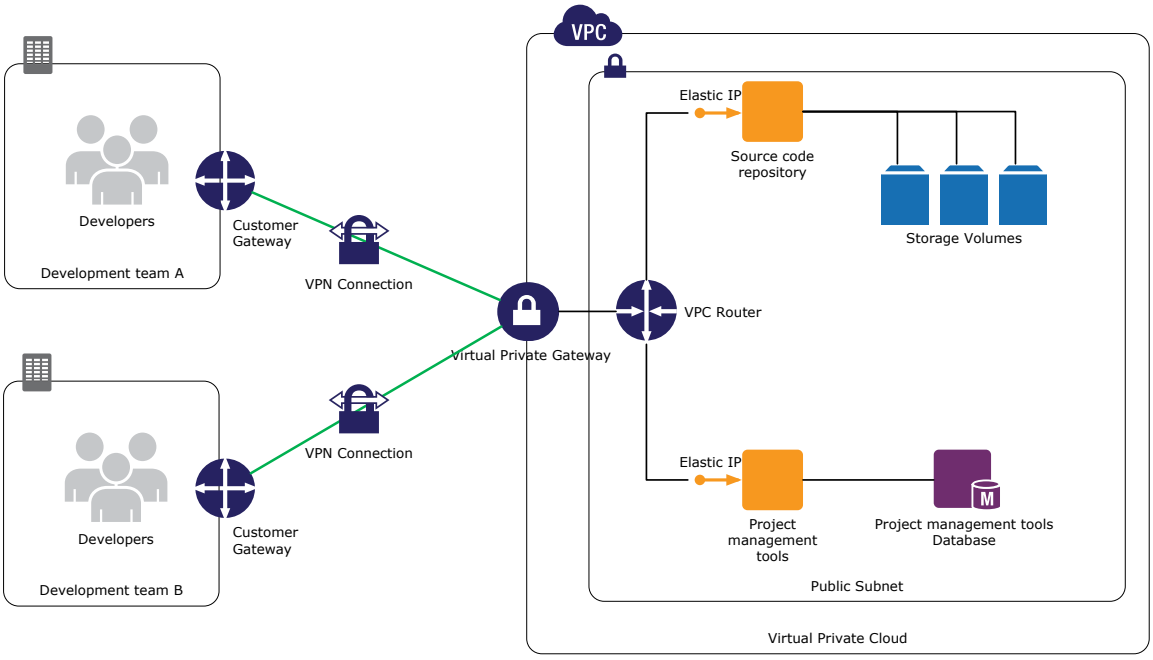

그림 6 - 개발 및 테스트 환경 사례

애플리케이션 테스트도 비슷하게 진행할 수 있습니다. 개발 환경에서 분리된 공간에서 새로운 소프트웨어 패키지를 평가하고 싶다면 VPC 에 테스트 환경을 구축하고 Amazon EC2 인스턴스 몇 대에 해당 소프트웨어를 나누어 설치하고 여기 접근할 필요가 있는 내부 사용자들에게 접근 권한을 부여하면 됩니다. 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 일어날 수도 있습니다. 자연 재해가 비즈니스 운영에 미치는 영향을 최소화하기 위한 전략 수립에는 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 리소스가 요구량이 갑자기 폭증하는 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 사용하면 생산 데이터를 Amazon EBS 볼륨 또는 Amazon S3 버킷으로 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.

더 자세한 내용은 "Amazon Web Services 를 이용한 재해 복구" 를 참조하십시오. 해당 문서는 AWS 아키텍처 센터[12]에서 확인할 수 있습니다.

데이터 센터를 클라우드로 확장

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.

중요한 것은 클라우드 리소스가 안전해야 하고, 그 구성과 작동이 모두 사용자의 온-프레미스 환경과 동일한 방식이어야 한다는 한다는 것입니다. 온-프레미스 환경과 AWS 클라우드를 잘 연결하면 이런 요건들을 모두 충족시킬 수 있습니다. 사용자는 온-프레미스 네트워크를 VPC 에 있는 AWS 리소스에 연결하기 위해 데이터 센터에 고객 게이트웨이를 생성하고 VPC 상에 virtual private gateway 를 생성할 수 있습니다. 이 게이트웨이들은 VPN 으로 연결됩니다. VPC 를 인터넷에서 격리하고자 할 경우 인터넷 게이트웨이를 사용하지 않으면 됩니다.

이런 방법 외에도 AWS Direct Connect 기능을 사용하면 VPC 에 대한 사설 연결을 구축해 지연시간을 낮추고 고대역폭을 확보할 수 있습니다. 기업의 지사에 IP 주소를 할당하듯 VPC 에도 자체 IP 주소 범위를 지정해 줄 수 있습니다. 데이터 센터에 물리적인 하드웨어를 추가하지 않고도 기업 애플리케이션을 VPC 로 이전할 수 있으며,

[12] http://aws.amazon.com/ko/architecture/

사용자의 네트워크에 웹 서버나 컴퓨팅 파워를 추가할 수 있습니다. VPC 를 기업의 방화벽 뒤에서 호스팅할 수 있으므로, 애플리케이션의 사용자들이 애플리케이션에 접근하던 기존 방식을 바꾸지 않고도 IT 리소스를 클라우드에 원활하게 이전할 수 있습니다. 본 문서의 앞쪽에 있는 F 그림 3 에서 VPC 로 데이터 센터를 확장하는 방법의 예시를 확인할 수 있습니다.

지사 및 사업부 네트워크의 생성

기업의 지사들이 상호 연결된 개별 로컬 네트워크를 필요로 한다면, Amazon VPC 를 통해 리소스를 배포하고 각 지점에 자체 서브넷을 지정하는 방법을 고려해 볼 수 있습니다. VPC 에서 제공하는 보안 그룹을 설정하면 VPC 서브넷 내의 애플리케이션들이 서로 통신할 수 있습니다. 혹은 가상 라우터를 통해 각기 다른 서브넷에 존재하는 애플리케이션들끼리 통신하게 해 줄 수도 있습니다. 한 서브넷 내부, 혹은 각기 다른 서브넷 사이의 흐름을 제한해야 할 경우엔 VPC 에서 제공하는 보안 그룹 또는 네트워크 ACL 을 구성해 어떤 서버들끼리의 통신이 가능한지의 허용 여부를 설정할 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.

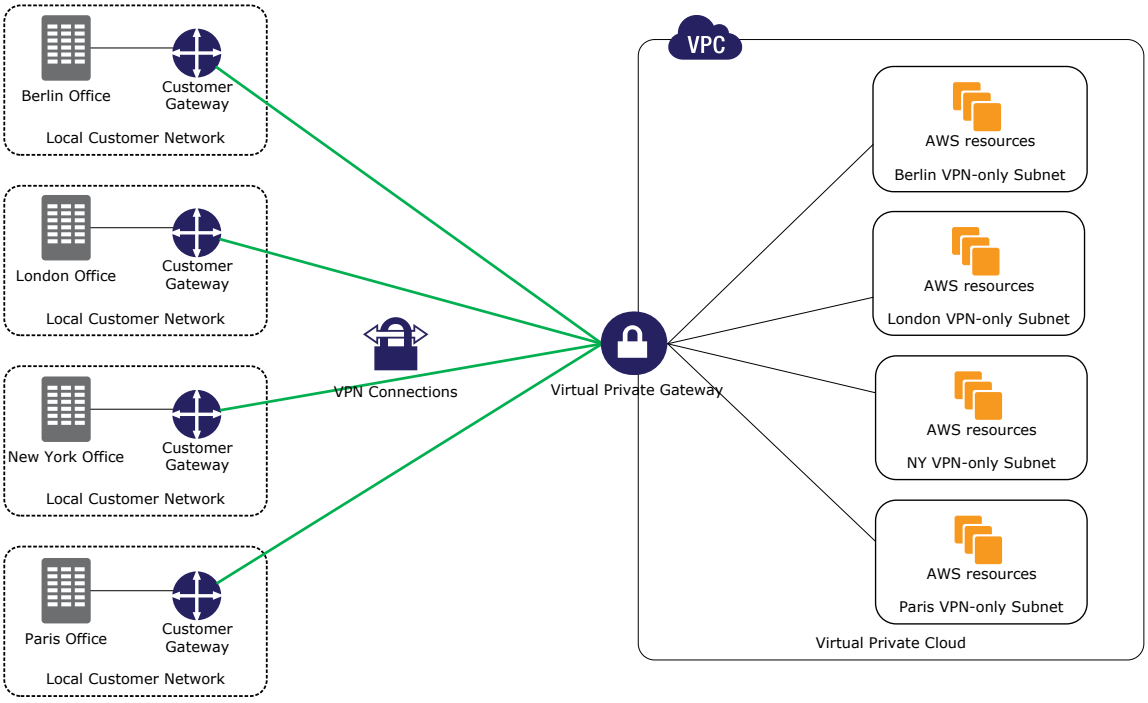

그림 7 - 지점 시나리오에 대한 VPC 및 VPN 의 사용

지사별로 프로비저닝된 온-프레미스 하드웨어와 VPC 를 병용하는 방식의 주요 이점은 다른 사용사례에서 언급한 것들과 크게 다르지 않습니다. 리소스를 신축적으로 확장 및

축소해 수요를 맞출 수 있기에 과도하거나 부족한 프로비저닝으로 위험을 초래하지 않을 수 있다는 것이죠. 용량을 추가하는 것은 매우 쉽습니다. 사용자 지정 Amazon Machine Images(AMIs)에서 Amazon EC2 인스턴스를 추가로 시작하기만 하면 됩니다. 용량을 줄여야 할 때에도 간단히 불필요한 인스턴스를 수동으로 종료시키거나 Auto Scaling 정책을 설정해 자동으로 종료시킬 수 있습니다. 이러한 운영 작업은 기존 하드웨어 자산의 유지와 별다를 바 없지만 기존의 방식에서 그러했듯 원격으로 이런 일을 맡아 하던 전담 인력이 더 이상은 필요하지 않다는 것과 쓰는 만큼 지불하는 과금 구조로 비용을 절약할 수 있다는 것이 다릅니다.

가상 데스크톱 인프라 생성

Amazon EC2 에서 호스팅할 수 있는 클라이언트 가상화 및 애플리케이션 스트리밍 솔루션 (Citrix, XenApp 등)을 제공하는 벤더들이 있습니다. VPC 로 가상 데스크탑을 호스팅하거나 클라이언트 애플리케이션을 스트리밍할 경우 이런 솔루션들을 사용해 온사이트 계약자가 기업 표준에 부합하는 가상 데스크탑을 운영하도록 하거나 회사 VPN 에 연결된 원격 직원 및 개인 사용자들에게 사무실과 동일한 환경을 제공하는 것이 가능합니다.

예를 들어 내부 세미나에서 참석자들이 사용할 다수의 클라이언트 PC 를 배포할 필요가 있는 경우, 씬 클라이언트 컴퓨터를 대여해 VPC 에서 사용자 지정 가상 데스크탑을 불러오도록 함으로써 비용을 최소화할 수 있습니다. 짧은 기간 동안만 데스크탑 PC 를 쓸 필요가 있는 프로젝트들과 프로그램에는 가상 데스크탑이나 애플리케이션 활용이 매우 적합합니다. 예를 들어, 새로운 혹은 업데이트된 클라이언트 애플리케이션을 배포 전에 테스트해보고 싶다면 가상 데스크톱 인프라(VDI)를 사용할 수 있습니다. 비즈니스상 특정 애플리케이션을 다른 환경에서 분리해 실행해 볼 필요가 있다면 VDI 가 효율적인 샌드박스 역할을 해 줄 것입니다.

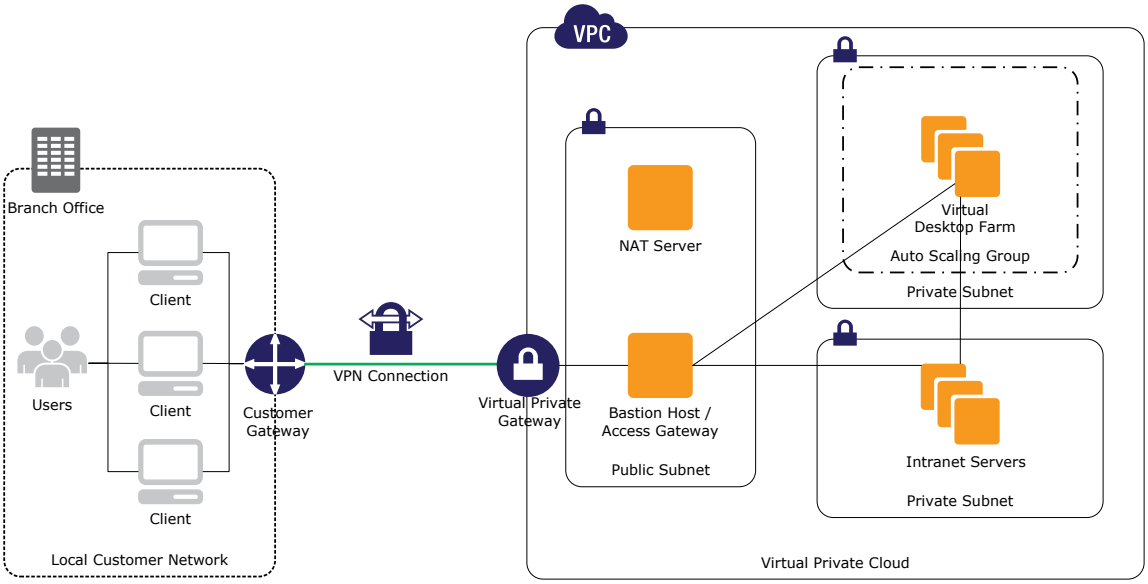

그림 8 - 간소화된 VDI 아키텍처 사례

가상 데스크톱 인프라를 쓰는 것은 영구적인 사용 면에서도 많은 이점이 있습니다. 컴퓨팅 워크로드를 Amazon VPC 로 이전함으로써 기존 클라이언트 하드웨어의 수명을 연장할 수 있으며, 불필요한 자금의 지출도 피할 수 있습니다. 중앙집중식으로 관리되는 VDI 솔루션의 특성 덕분에 운영 시스템의 업데이트 및 패칭과 새로운 클라이언트 애플리케이션의 배포를 간소화할 수 있습니다. 또한, 내부 직원에 대해 까다로운 규정을 적용하는 산업에서도 중앙 관리식 VDI 솔루션으로 데이터 유실 및 멜웨어 감염의 위험을 대폭 줄일 수 있습니다.

Amazon VPC를 이용하는 모범 사례

인프라 배포의 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 helper scripts 을 통해 표준 Amazon Machine Images(AMIs)를 사용하면 Amazon EC2 인스턴스의 시작에 앞서 배포 단계에 요구되는 모든 하드웨어를 설치할 수 있습니다.

프로세스에 자동화된 인프라 배포를 완전히 통합하는 것이 좋습니다.. 자동화 스크립트를 표준 및 규정에 따라 테스트하고 유지해야 하는 소프트웨어로 생각해야 합니다. 훌륭한 자동화 전략은 대부분의 VPC 사용 사례에 이득이 됩니다. 철저하게 테스트된 자동화 프로세스는 대부분의 경우 복잡한 수동 작업에 의존하는 프로세스보다 빠르고 저렴하며 더 안정적입니다.

VPC 에서 사용하는 다중 AZ 배포와 고가용성

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 Multi-AZ Amazon RDS DB Instance 를 배포하기 위해서는 먼저 데이터베이스 인스턴스가 시작될 지역 내의 각 가용 영역에 VPC 서브넷을 구성해 둬야 합니다. Auto Scaling 그룹 및 Elastic Load balancer 들이 각 가용 영역의 서브넷에 배포됨으로써 여러 가용 영역을 사용하는 효용을 발휘할 것입니다.

보안 그룹 및 Network ACL 의 사용

Amazon VPC 는 사설 AWS 클라우드에 걸쳐 추가적인 보안 기능을 제공합니다. 사용자는 EC2 보안 그룹에 걸쳐 추가적인 기능을 지원하는 네트워크 ACL 및 VPC 보안 그룹을 지정할 수 있습니다. 예를 들어, VPC 보안 그룹은 사용자가 인바운드 트래픽 및 아웃바운드 트래픽 (EC2 보안 그룹은 ingress 만 통제)을 통제하고, 모든 프로토콜 및 포트에 대한 규칙을 정의할 수 있도록 합니다. (EC2 보안 그룹은 TCP, UDP, 및 ICMP 에 대해서만 규칙을 정의합니다.) Amazon EC2 와 Amazon VPC 의 보안 그룹 간 차이점에

대한 전체 개요는 Amazon Virtual Private Cloud 사용 설명서[13]를 참조하십시오. Amazon EC2 및 Amazon VPC 보안 그룹 모두 보전형 방화벽입니다.

네트워크 ACL 은 서브넷을 드나드는 트래픽을 통제하기 위해 방화벽처럼 작동하는 추가적인 보안 계층입니다. 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 인바운드 및 아웃바운드 트래픽 모두에 지정할 수 있습니다. 네트워크 ACL 또는 NACL 는 stateless 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. 또한, 운영 시스템의 수준에서 방화벽으로 인스턴스를 보호해야 하며, AWS 보안 및 규정 준수 센터[14]에 기록된 다른 보안 모범 사례를 따라야 합니다.

IAM Users 를 이용한 역할 분담

AWS Identity and Access Management(IAM)을 통해 계정을 생성하고 관리할 수 있습니다. 사용자는 사람 또는 AWS 와 소통해야 하는 애플리케이션일 수 있습니다. IAM 으로 계정 사용자, 액세스 자격 증명과 같은 보안 자격 증명, 그리고 사용자가 액세스할 수 있는 AWS 리소스에 대한 허가를 중앙집중식으로 관리할 수 있습니다. 일반적으로 사용자에 대해서는 IAM User accounts 를 생성할 것이며, 애플리케이션에 대해서는 IAM roles 를 사용합니다.

IAM 은 최소 권한의 보안 전략을 구현할 때 사용하기를 권장합니다. 예를 들어, 모든 AWS 인프라를 관리하기 위해 주 AWS 사용자 계정을 사용하는 방법은 별로 좋지 않습니다. 그 대신 AWS 에서 수행되어야 하는 각 태스크에 대한 사용자 그룹을 지정하고, 각 사용자가 수행해야 하는 기능만을 허용하도록 정확히 제한하기를 권장합니다. 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 제한적 규정을 지정하여 각 사용자가 필요한 서비스에만 액세스할 수 있도록 할 수도 있습니다. 조직 내에서 자격 증명이 된 사람만이 이 사용자 계정에 대한 액세스를 갖도록 해야하며, 주기적으로 자격 증명을 변경해 인프라에 대한 리스크를 줄이는 것이 좋습니다.

---

13 http://docs.amazonwebservices.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

14 http://aws.amazon.com/ko/security/

IAM 사용자 및 규정 정의 방법에 대한 자세한 내용은 Amazon Virtual Private Cloud 사용 설명서[15]를 참조하십시오.

VPC 인스턴스 및 VPN 링크의 상태 모니터링을 위한 Amazon CloudWatch 의 사용

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 CloudWatch API 를 통해서도 확인할 수 있어 기존 관리 도구에 통합할 수 있습니다.

AWS Management Console 또는 vgw-telemetry API 작업을 사용하여 VPN 연결을 모니터링할 수 있습니다. 이러한 도구들은 VPN 연결 상태를 표시하는데, 각각의 VPN 터널 상태(연결/비연결) 및 터널이 '비연결' 상태일 때에 오류 메시지 등이 표시됩니다.

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 의 유연성과 확장성, 탄력성, 성능 및 가용성을 비롯해 "사용한 만큼만 비용을 지불한다"는 과금 구조의 이점을 모두 누리면서도 AWS 상의 리소스를 쉽게 보호하도록 해 줍니다.

[15] http://docs.amazonwebservices.com/AmazonVPC/latest/UserGuide/VPC_IAM.html

참고 문헌

1. **Amazon VPC 제품 페이지**: http://aws.amazon.com/ko/vpc/
2. **Amazon VPC 문서:** http://aws.amazon.com/ko/documentation/vpc/
3. **AWS Direct Connect 제품 페이지:** http://aws.amazon.com/ko/directconnect/
4. **AWS Direct Connect 문서:** http://aws.amazon.com/ko/documentation/directconnect/
5. **AWS 아키텍처 센터:** http://aws.amazon.com/ko/architecture/
6. **AWS 보안 및 준수 센터:** http://aws.amazon.com/ko/security/
7. **AWS 를 사용한 재해 복구**: http://media.amazonwebservices.com/AWS_Disaster_Recovery.pdf
8. **클라우드를 위한 설계: 모범 사례**
   http://media.amazonwebservices.com/AWS_Cloud_Best_Practices.pdf

수정 내역

최신 버전 이후의 변경 사항(2010 년 1 월)

- Amazon VPC 의 새로운 기능을 반영하는 주요 수정 사항
- VPC 의 새로운 사용 사례가 추가됨
- "Amazon Virtual Private Cloud 에 대한 이해" 섹션이 추가됨
- "Amazon VPC 를 사용한 모범 사례" 섹션이 추가됨