네이버클라우드플랫폼 VPC 상품소개

NAVER
CLOUD PLATFORM

Network - VPC

고객 전용 네트워크를 클라우드에서 구현하실 수 있습니다.

논리적으로 격리된 네트워크를 리전 전체에 걸쳐 제공하여 다른 사용자의 간섭 없이 IT인프라 환경을 안전하게 클라우드 상에서 구현하실 수 있습니다. 또한 네트워크 서브넷(Subnet) 기능을 통해 용도에 따라 네트워크를 세분화하여 고객 맞춤형 네트워크를 구성하실 수 있습니다.

논리적으로 완벽하게 격리된 네트워크

타사용자와 논리적으로 분리된 네트워크 환경 제공하여 안전하고 안정적인 IT시스템 구축이 가능합니다.

강력한 보안

접근제어를 위한 ACG외에도 네트워크 서브넷에 적용가능한 NACL을 제공하여 다양한 접근제어 정책 수립이 가능합니다.

용도별 다양한 네트워크 구성

인터넷 연결이 가능한 네트워크와 연결이 불가능한 네트워크를 몇 번의 클릭 만으로 VPC 상에서 동시에 구성하실 수 있습니다. 외부 연결이 필수인 웹 서버는 Front-end 서브넷에 배치를 하고, 제한적으로 외부 연결이 필요한 서버는 오직 NAT 게이트웨이 통해 접속할 수 있는 서브넷에 배치하여 고객 내부 비즈니스 요구사항을 충족시킬 수 있습니다.

안정적인 하이브리드 솔루션

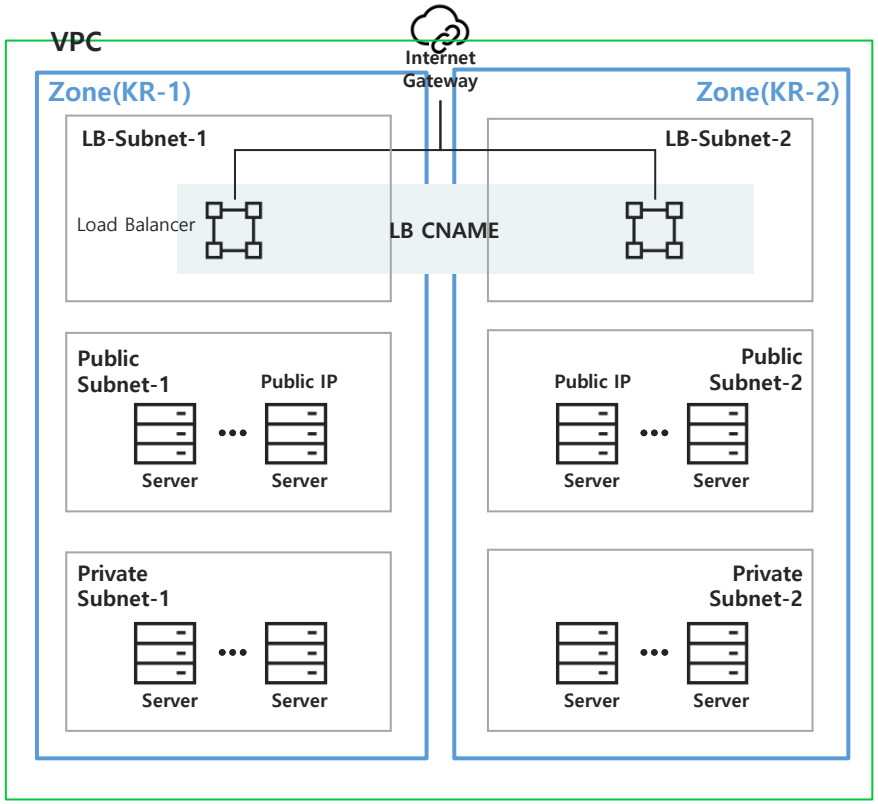
전용회선 서비스인 Cloud Connect와 네트워크 보안 서비스인 IPsec VPN을 이용하여 고객의 데이터센터와 네이버클라우드의 퍼블릭 클라우드를 연결하실 수 있습니다. 또한 Virtual Private Gateway 서비스를 통해 Cloud Connect와 IPsec VPN을 이중화 하여 안정성을 제고할 수 있습니다.

Key Features

- **VPC Subnet** – 고객 맞춤형 네트워크 구성 가능
- **ACG, NACL** – 네트워크와 서버를 보호하기 위한 보안 환경 제공
- **Peering** – VPC 간 사설 IP 기반의 통신
- **VGW** – IPsec VPN과 Cloud Connect 연결을 위한 게이트웨이
- **Route Table** – VPC 내에서 동작하는 고유의 라우팅 기능
- **NAT Gateway**, **Internet Gwateway** – 외부 인터넷 연결을 위한 게이트웨이
- **VPC Flowlog** - 서버 네트워크 인터페이스에서 송수신되는 네트워크 트래픽에 대해 ACG 룰 기반으로 정보를 수집하는 기능

VPC Subnet

VPC(Virtual Private Cloud)는 퍼블릭 클라우드 상에서 제공되는 고객 전용 사설 네트워크를 의미합니다. 고객의 계정마다 최대 3개의 VPC를 생성할 수 있으며, 각 VPC는 최대 넷마스크 255.255.0.0 /16 (IP 65,536개) 크기의 네트워크 주소 공간을 제공합니다. VPC는 다른 VPC 네트워크와 논리적으로 분리되어 있으며, 기존 고객 데이터센터 네트워크와 유사하게 구현할 수 있습니다.
IP 주소범위는 (10.0.0.0/16, 172.16.0.0/12, 192.168.0.0/16) 내에서 선택하여 입력 가능하며 200개의 서브넷 생성이 가능합니다.



서브넷은 Zone을 지정할 수 있으며, 4개 종류의 서브넷을 선택할 수 있습니다.

Public 서브넷
- 공인 IP 할당이 가능한 서브넷이며, 외부에서 직접 접근하거나 외부에 노출되는 서버들을 위치시킬 수 있습니다.

Private 서브넷
- 제한적인 외부 연결이 필요한 서버들이 위치하는 프라이빗 서브넷이며, 외부 연결을 위하여 NAT 게이트웨이를 통해 연결할 수 있습니다.

Loadbalancer 서브넷
- Public / Priavte Loadbalancer를 생성할 수 있는 서브넷이며, Loadbalancer는 오직 해당 서브넷에서만 생성이 가능합니다.

Baremetal 전용 서브넷
- 가상화 되지 않은 물리서버를 단독으로 제공하는 베어메탈 서버를 생성할 수 있는 서브넷입니다. 베어메탈 서버는 오직 해당 서버에서 생성이 가능합니다.

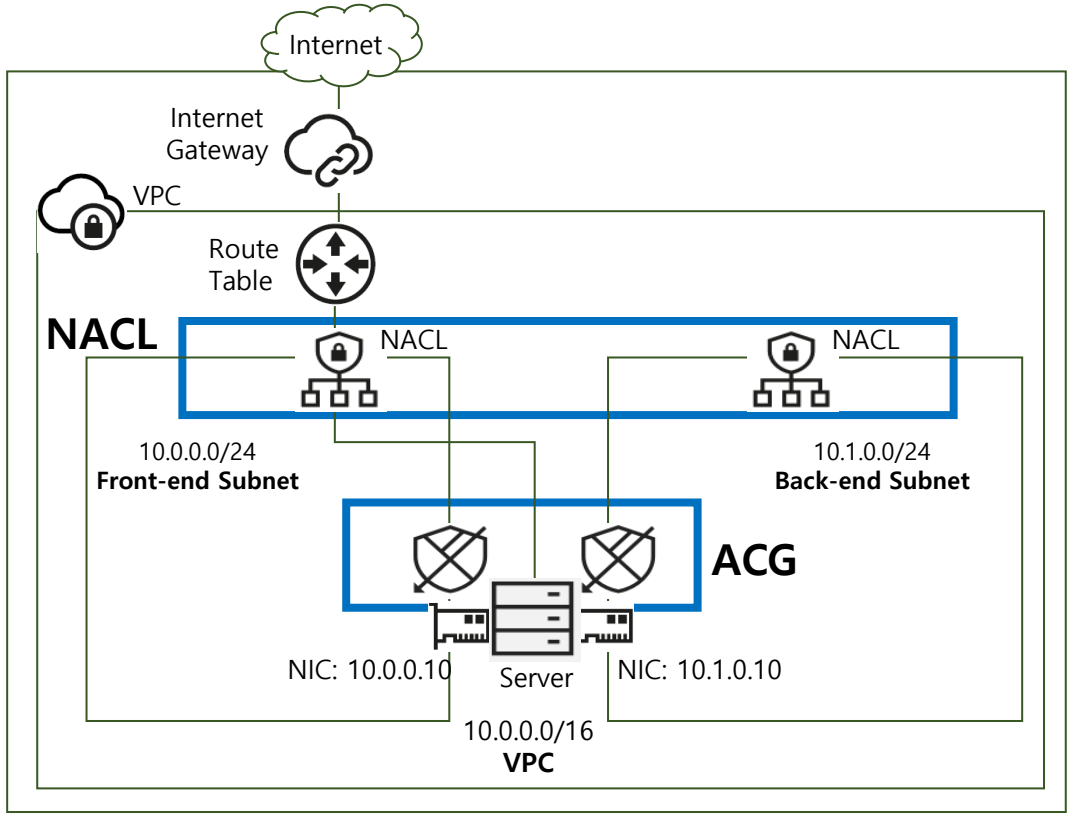
ACG, NACL

네이버 클라우드 플랫폼는 VPC의 보안을 강화하기 위해 사용할 수 있는 ACG와 Network ACL 두 가지 기능을 제공합니다.

ACG는 Inbound / Outbound 트래픽에 허용 규칙을 설정하여 서버의 트래픽을 제어합니다. 반면에 Network ACL은 Subnet 레벨에서 작동하며 Inbound 및 Outbound 트래픽에 대하여 허용 또는 차단 규칙을 적용할 수 있습니다.
Network ACL을 이용하여 각 Subnet을 독립적인 네트워크로 구분 짓고, Subnet 내 통신의 보안은 ACG로 제어함으로써 강력한 네트워크 보안체계를 구성할 수 있습니다.

ACG는 "stateful", Network ACL은 "Stateless" 방식으로 각각 동작합다. Stateful 은 트래픽 상태를 저장한다는 의미로 Inbound 규칙에 의해 허용된 트래픽은 Outbound 규칙에 상관없이 응답할 수 있습니다. 반면에 Stateless 방식은 트래픽 상태를 저장하고 있지 않으므로 Inbound 규칙에 의해 허용된 트래픽의 응답도 Outbound 규칙에 의해 필터링됩니다. 따라서 Network ACL 규칙 설정은 각별한 주의와 충분한 검증 테스트가 요구됩니다.

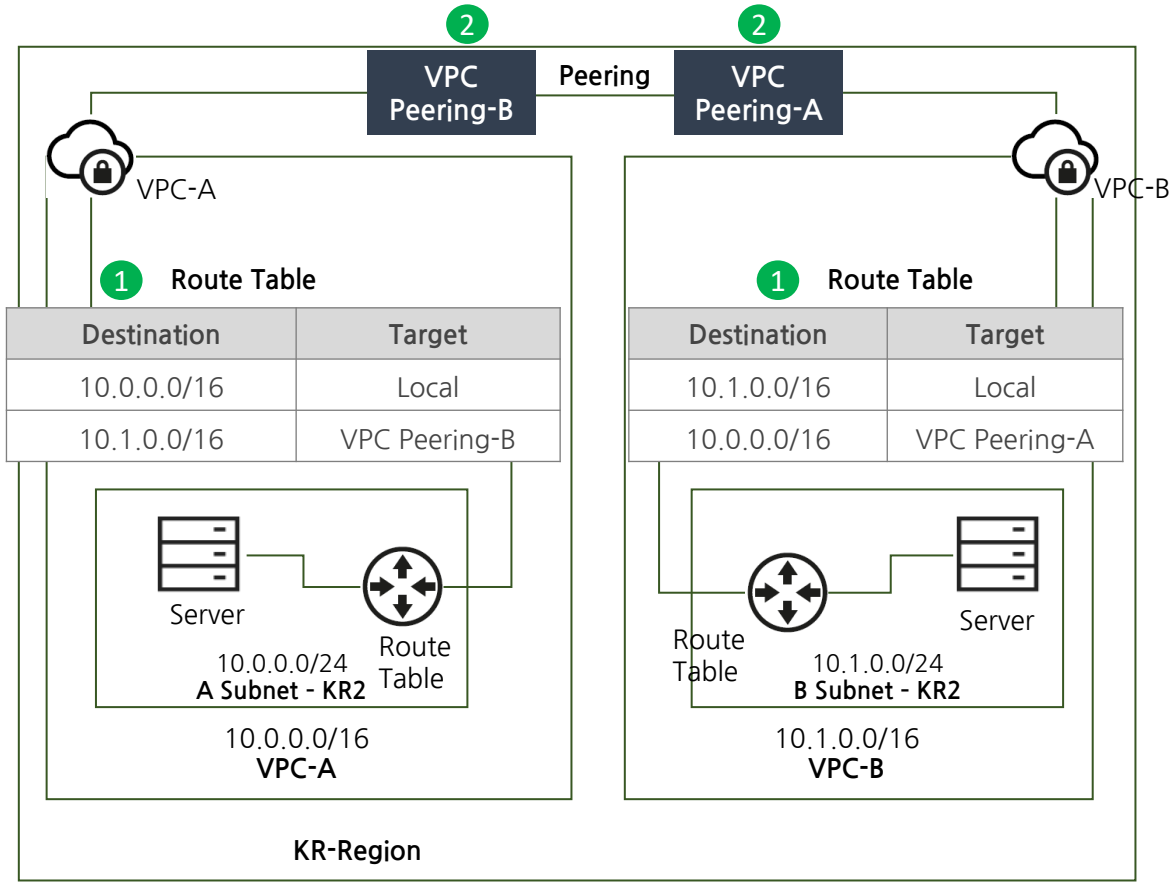
구분	ACG	NACL
적용 대상	서버의 접근 제어	Subnet의 접근 제어
지원 규칙	허용 (Allow)	허용 및 거부 (Allow/Deny)
상태 저장 여부	상태 저장 (규칙에 관계없이 반환 트래픽이 자동으로 허용됨)	상태 비저장 (반환 트래픽이 규칙에 의해 명시적으로 허용되어야 함)
적용 방법	서버의 NIC에 ACG 정책 적용	Subnet 단위로 적용 (Subnet 별 1개만 허용)



① **ACG(Access Control Group)**은 서버의 인터페이스별 Inbound 및 Outbound 트래픽을 제어
② **NACL(Network Access Control List)**은 Subnet의 Inbound 및 Outbound 트래픽을 제어

1 Route Table

네트워크 경로를 설정할 수 있는 기능을 제공합니다.
Route Table은 Destination과 Target으로 구성되어 있습니다.
VPC 내부 통신을 위한 Local은 기본적으로 설정되어 있습니다.
단, 공인 Route Table을 생성할 시에는 인터넷 통신을 위한 규칙이 자동으로 추가됩니다.

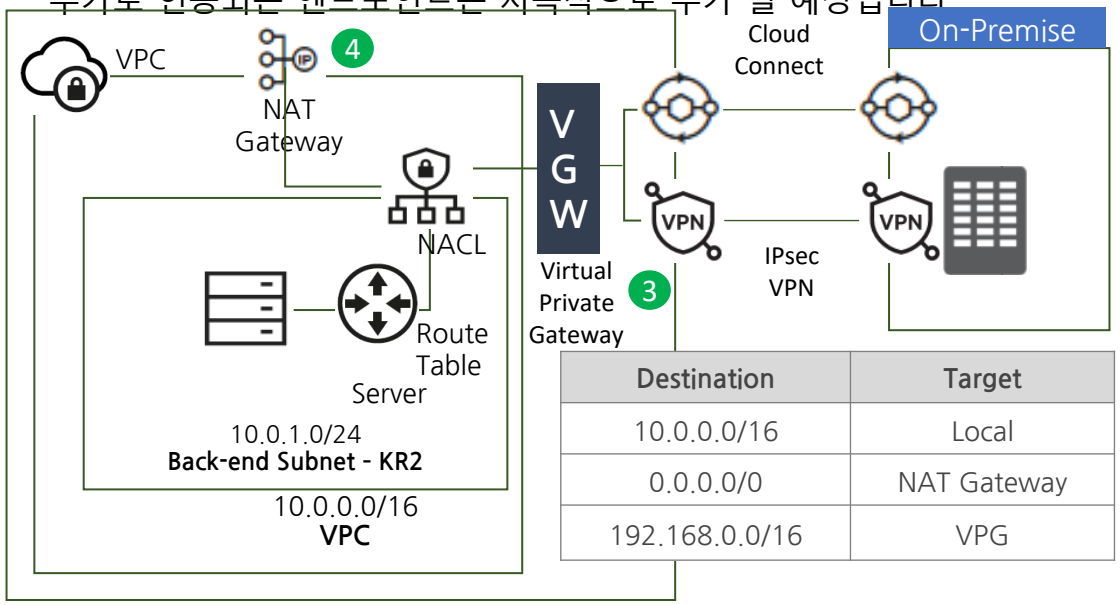


2 Peering

VPC간 사설 연결을 보장하는 기능입니다. 기본적으로 단방향 통신을 제공하므로
양방향 통신 시 Source와 Destination이 뒤바뀐 2개의 VPC Peering을 생성하셔야 합니다.

3 VGW(Virtual Private Gateway)

VGW는 VPC와 외부 연결 네트워크 장치 간 연결 접점으로서 외부 연결을 위해서 반드시 생성해야 하며, IPsec VPN과 클라우드 커넥트가 연결됩니다.
추가로 연동되는 엔드포인트는 지속적으로 추가 될 예정입니다.



4 NAT Gateway

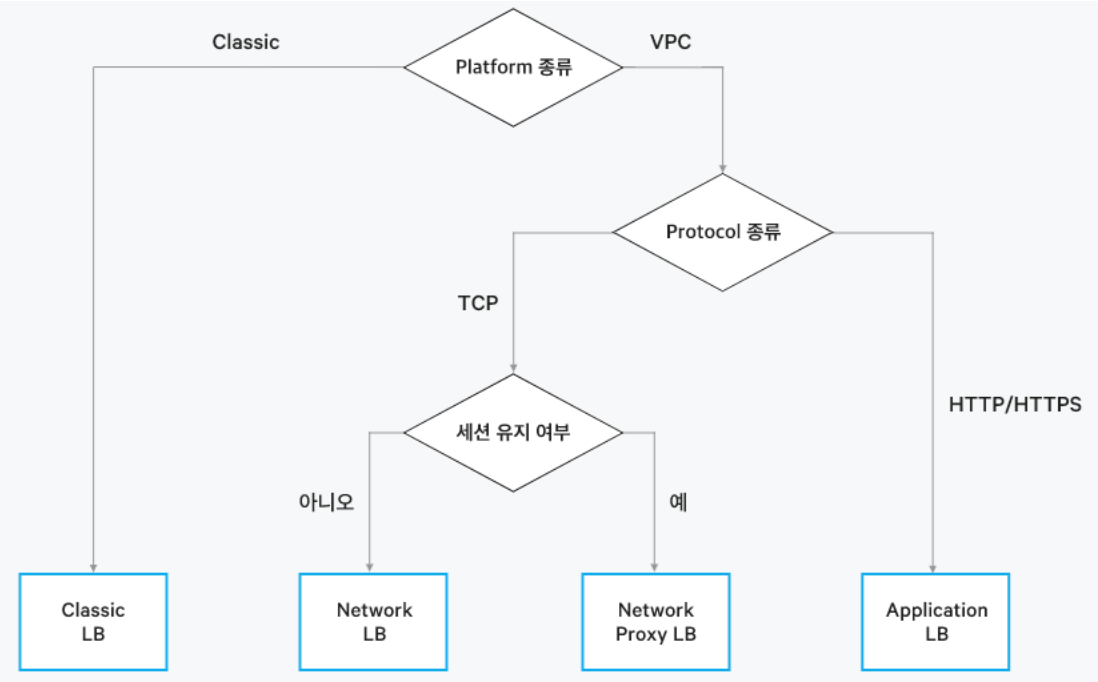
인터넷 접속이 제한된 네트워크에서 외부와의 통신을 위해 사용하는 게이트웨이(Gateway)로서 IP 노출을 최소화하는 효과를 얻을 수 있습니다.

VPC 적용으로 변경되는 네트워크 상품

- 로드밸런서
- 클라우드 커넥트
- IPsec VPN

VPC 로드밸런서

네트워크 로드밸런서, 네트워크 프록시 로드밸런서, 어플리케이션 로드밸런서를 제공하며 고객 서비스 특성에 최적화된 로드밸런서 타입을 다양하게 선택할 수 있습니다.



네트워크 로드밸런서

네트워크 로드밸런서는 초당 연결 수 기준 최소100,000개에서 최대 400,000개까지 성능을 보장하는 단계별 상품을 제공하여 고객 서비스 규모에 최적화된 분산처리 성능을 제공합니다. 또한 네트워크 로드밸런서는 트래픽 분배만 수행하고 고객 서버에서 직접 응답하는 기능(DSR)을 구현하여 보다 빠르고 효율적인 서비스를 이용하실 수 있습니다.

네트워크 프록시 로드밸런서

네트워크 프록시 로드밸런서는 프록시 방식의 통신을 제공하여 세션 유지가 필요한 TCP 기반 애플리케이션에 이용할 수 있습니다. 또한 애플리케이션 로드밸런서와 동일한 부하 분산 알고리즘을 적용할 수 있습니다.
웹 기반의 콘솔에서 SSL 인증서를 추가할 수 있습니다. TLSv1, TLSv1.1, TLSv1.2 등 SSL 프로토콜 중 가능한 버전을 선택해 사용할 수 있으며, 적용된 SSL Ciphers를 설정할 수 있습니다. SSL 인증서는 Certificate Manager와 연동하여 편리하게 관리됩니다

어플리케이션 로드밸런서

HTTP/HTTPS 트래픽에 대해서 패킷 헤더를 확인하여 Application 레벨에서의 분기처리를 제공합니다. 로드밸런서의 리스너에 Host Header기반 분기처리, URL Path Pattern 기반 분기처리, 가중치 기반 분기처리, Redirection 응답처리와 같은 규칙이 지원되어 보다 상세한 고급 서비스 구성이 가능합니다.

로드밸런서 타입별 기능 비교

VPC 네트워크 로드밸런서와 애플리케이션 로드밸런서의 제공 기능을 요약하면 아래와 같습니다.

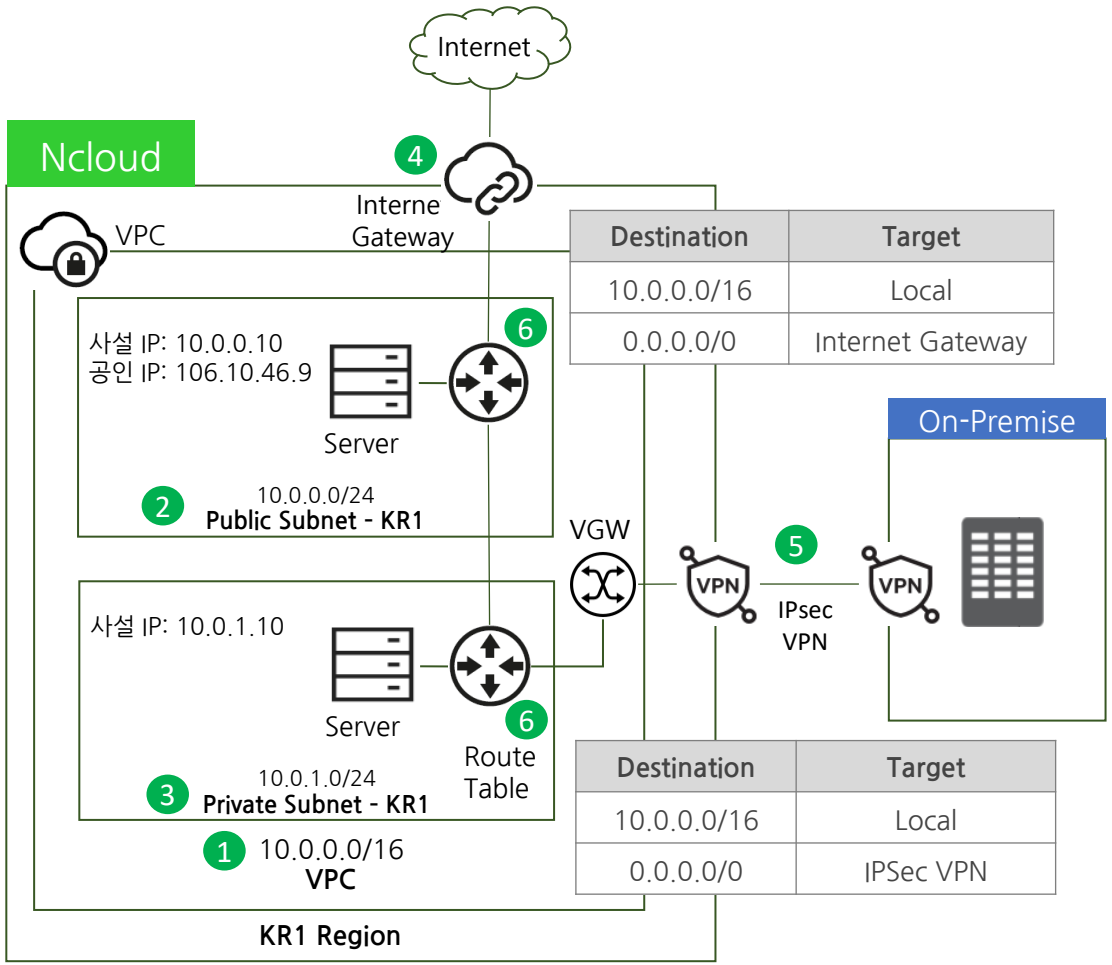
기능	Network LoadBalancer	Network Proxy LoadBalancer	Application LoadBalancer
프로토콜	TCP	TCP, TLS	HTTP, HTTPS
상태 확인	O	O	O
로깅	X	O	O
DSR(Direct Server Return)	O	X	X
같은 인스턴스의 여러 포트로 로드 밸런싱	X	X	O
HTTP 2.0 지원	N/A	N/A	O
경로 기반 라우팅	N/A	N/A	O (출시예정)
SSL 오프로드	X	O	O
고정 세션	X	O	O

Cloud Connect 및 IPsec VPN

현재 Managed 형태로 제공되며, 추후 Self Managed 상품 출시 예정입니다.

【 참고 아키텍처 】 Public Subnet과 IPSec VPN 연결 Subnet

이 시나리오 구성에는 Public Subnet 및 VPN-Only Subnet이 있는 Virtual Private Cloud(VPC)와 IPSec VPN 터널을 통해 고객사의 네트워크와 통신하기 위한 가상 IPSec VPN Gateway가 포함됩니다.



1 VPC
- IPv4 CIDR 블록의 크기가 /16(예: 10.0.0.0/16)으로 제공되며 65,536 개의 주소 공간을 제공

2 Public Subnet
- Subnet의 크기가 최대 /24(예: 10.0.0.0/24) 으로 제공되며, 256개의 주소 공간을 제공
- Public Subnet 내의 서버는 인터넷과 연결이 필요한 서버 (공인 IP 보유 가능)

3 Private Subnet
- Subnet의 크기가 최대 /24(예: 10.0.0.0/24) 으로 제공되며, 256개의 주소 공간을 제공
- Private Subnet 내의 서버는 인터넷과 연결이 필요없으며, 고객 사업장과 연결이 필요한 서버의 집합

4 Internet Gateway
- VPC를 인터넷 및 다양한 네이버 클라우드 플랫폼 서비스에 연결

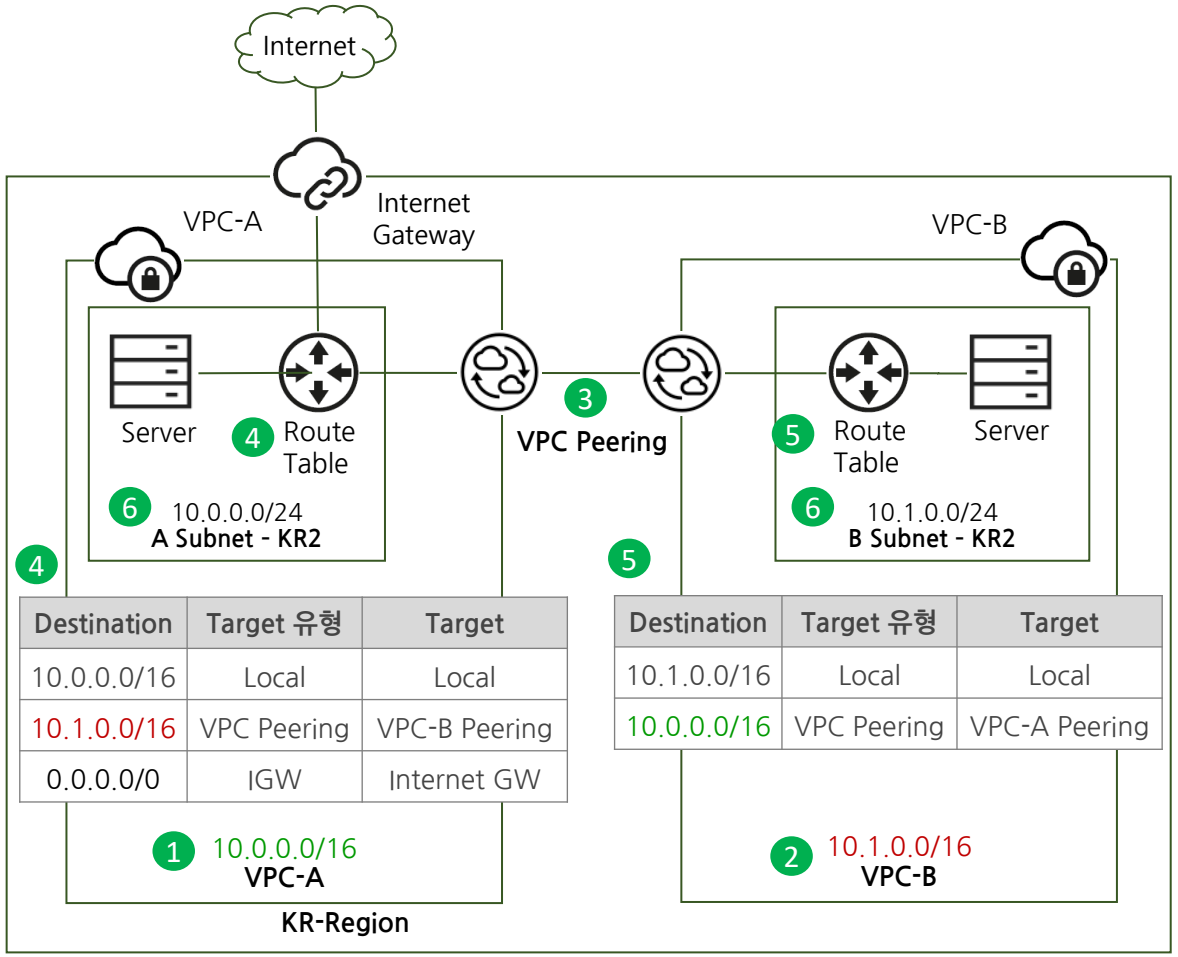
5 IPSec VPN
- 네이버 클라우드와 고객사 네트워크 사이의 VPN 연결을 지원

6 Route Table
- Public Subnet: 서버가 VPC 내의 다른 인스턴스와 통신할 수 있게 하는 항목(local)과 인터넷과 직접 통신할 수 있게 하는 항목(IQW-ID)이 저장됩니다.
- VPN-Only Subnet: 서버가 VPC 내의 다른 인스턴스와 통신할 수 있게 하는 항목(local)과 IPSec VPN Gateway를 통해 고객의 네트워크와 통신할 수 있게 하는 항목이 저장됩니다.

※ 참고 링크:
설명서: https://guide.ncloud-docs.com/docs/networking-vpc-vpcuserscenario3
소개: https://www.ncloud.com/product/networking/vpc

【 참고 아키텍처 】 VPC 간 사설 통신(Peering 구성)

하나의 사용자에게 최대 3개(주1)의 VPC를 제공합니다. 기본 적으로 VPC 간 통신은 공인 IP를 이용하나 보안과 안정성을 고려하면 사설 IP 통신을 권장합니다. VPC Peering 은 VPC 간 사설 IP 통신을 지원하는 통신 도구입니다.



1 VPC-A
- VPC-A는 Public 망과 연결된 VPC로 IP 대역을 10.0.0.0/16 대역을 사용

2 VPC-B
- VPC-B는 Private 망에만 연결된 VPC로 IP 대역을 10.1.0.0/16 대역을 사용

3 VPC Peering
- VPC 간 연결을 제공하는 가상 네트워크 도구로 1:1 단방향 통신을 제공하고, VPC Peering 요청 및 수락 절차 필요.
- 양방향 통신을 하기 위해서는 상호간 VPC 요청/수락하여 VPC Peering 2개를 생성

4
- VPC-A Route Table
  - VPC-A는 Local과 Public 망 접근을 위한 2개의 정책에 VPC-B로 나가는 Traffic에 대한 VPC-B(10.1.0.0/16) Peering Route정책 추가

5
- VPC-B Route Table
  - VPC-B는 Public 망 접근이 필요 없으므로 Local 접근을 위한 1개의 정책에 VPC-A로 나가는 Traffic에 대한 VPC-A(10.0.0.0/16) Peering Route정책 추가

6
- 보안
  - **ACG**(서버의 Inboud/Outbound 트래픽 제어)와 **Network ACL**(Subnet의 Inbound/Outbound 트래픽 제어)에 VPC Peering에 의해 발생하는 트래픽에 대해 적절한 정책을 추가

※ 참고 링크:
설명서: https://guide.ncloud-docs.com/docs/networking-vpc-vpcuserscenario4

(주1) 계정 당 VPC 3개 제공 항목은 고객과 협의를 통해 조정 가능합니다.

Thank you

NAVER
CLOUD PLATFORM