

VIII. 네트워크

2. hybrid cloud - VPN

목차

- 2.1 VPN 서비스 소개
- 2.2 VPN FAQ
- 2.3 Public Cloud 공용 VPN 상품 신청 방법
- 2.4 Enterprise Cloud VPN 상품 신청 방법
- 2.5 G-Cloud VPN 상품 신청 방법
- 2.6 VPN 기타 가이드

2.1 VPN 서비스 소개

2.1.1 목적/특징

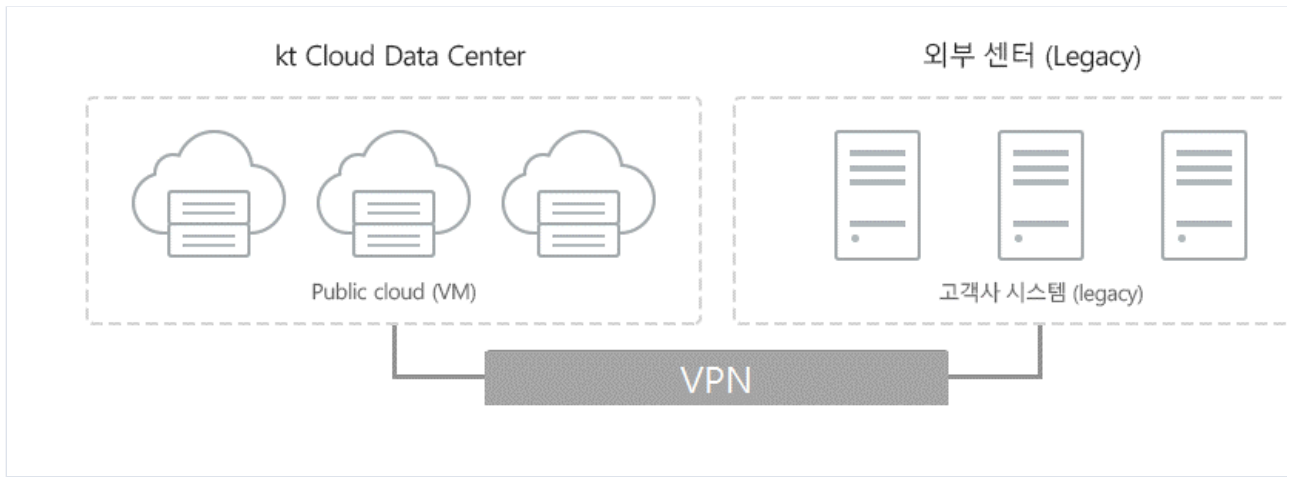
Cloud 환경 외부에 위치한 고객사 Site와 고객의 Cloud 환경을 사설망으로 연결하여, 고객의 Data Center 유연성 확장 및 Hybrid cloud 환경을 제공합니다.

□ 서비스 특·장점

- 보안성
 - IPSec-VPN을 통한 터널링 기술을 이용하여 다양한 고객들의 트래픽을 분리하고, 변환된 특정 패킷 사용
 - 특정 사용자끼리 전용망처럼 안전하게 통신 가능(보안성 강화)
- 비용 절감
 - 고객의 별도의 네트워크 구성이 필요 없으며, 이에 따른 기업의 통신 비용 절감 효과

2.1.2 구조/원리

□ 서비스 구조



VPN 구성으로 공중망을 통한 터널링(IP-Sec) 연동 구조로, 외부의 고객 시스템과 Site-to-site VPN(IP-Sec)으로 공중망을 통해 cloud와 연결이 가능합니다.

2.1.3 유의사항/제약사항

□ ucloud VPN 연동 지원 유형

- Public Cloud, Enterprise Cloud, G-Cloud(Private Zone) 간 VPN 연동이 가능합니다.

연동 Zone	
Public Cloud VPN 연동	Public cloud 공용 VPN 연동 2장
Enterprise Cloud 의 Public Zone 연동 Enterprise Cloud 의 Private Zone 연동	Enterprise Cloud 공용 VPN 연동 3장
G-Cloud 의 Private Zone 연동	G-Cloud 공용 VPN 장비 연동 4장

□ IPSec-VPN 방식

- Public Cloud, Enterprise Cloud, G-Cloud 공히 IPSec-VPN 을 지원하며, SSL-VPN은 지원하지 않습니다.

2.2 VPN FAQ

□ VPN 설정 작업 소요 시간은 어느정도 걸리나요?

○ VPN 연동작업은 고객사 사내 네트워크 환경과 정합을 맞추는 작업 및 방화벽 작업 등 적지 않은 시간이 걸리는 작업으로 개통 요청부터 개통완료까지 업무일 기준 최소 3 일이상 소요될 수 있으므로 일정을 지나치게 촉박하게 잡지 않는 것이 좋습니다.

□ 고객사 VPN 장비는 이중화 구성을 꼭 해야 하나요?

○ 고객사 VPN 장비는 되도록 이중화를 권고합니다. Kt Cloud VPN 은 자체적으로 이중화되어 있으나 고객사 VPN 이 이중화되어 있지 않은 경우 단일 장애지점 (SPoF) 가 될 수 있습니다.

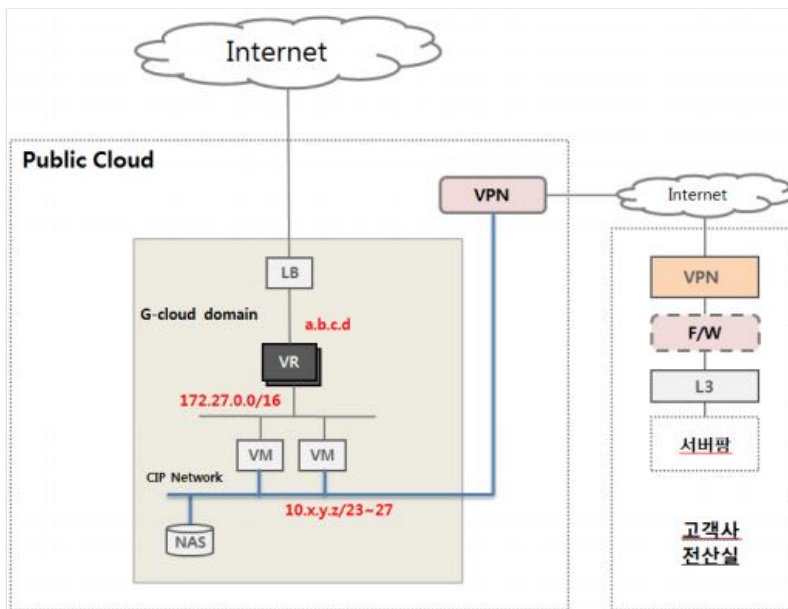
□ VPN 관련 문의는 어디로 해야 하나요?

	전화번호	온라인 문의 및 요청
G-Cloud VPN 구성 협력사	031-622-5891	mss1@wins21.co.kr
ucloud biz 고객센터 (테크센터)	080-2580-005	서비스포탈 > 고객센터 > 문의하기

2.3 Public Cloud 공용 VPN 서비스

2.3.1 Public Cloud VPN 구조

□ 서비스 구조



고객사 전산실의 시스템은 VPN 이용, Public Cloud VM 과 CIP 를 이용하여 연동

고객사 전산실내에는 일반적으로 방화벽으로 내부망으로 보호하도록 구성

연동경로 : 고객사 서버팜 <-> 고객사 F/W <-> 고객사 VPN 장비 <-> 인터넷 <-> kt CDC VPN 장비 <-> Public Cloud VM

고객사로부터 kt CDC 로 라우팅되는 IP 는 VM 의 CIP Network (10.x.y.z/23~27)

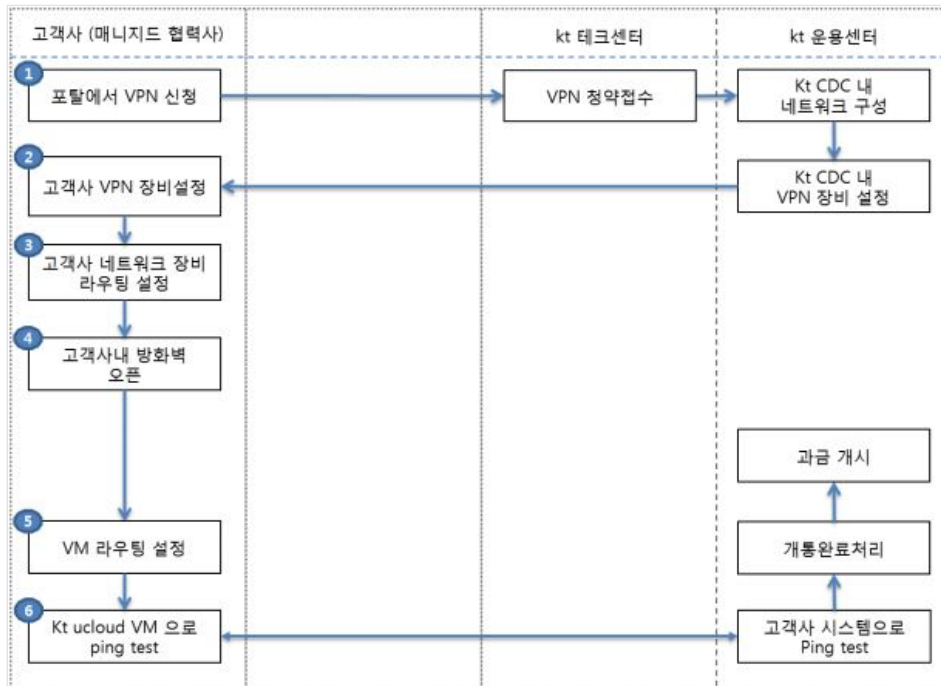
고객사로부터 VPN 으로 연동하는 경우 ucloud LB 에 연동하는 것은 불가

Public Cloud 연동 VPN 장비

Public Cloud 의 공용 VPN 장비는 Cisco 장비로 대국측 (고객사) 도 Cisco 호환 장비로 구성 권고.

2.3.2 개통 프로세스 및 체크리스트

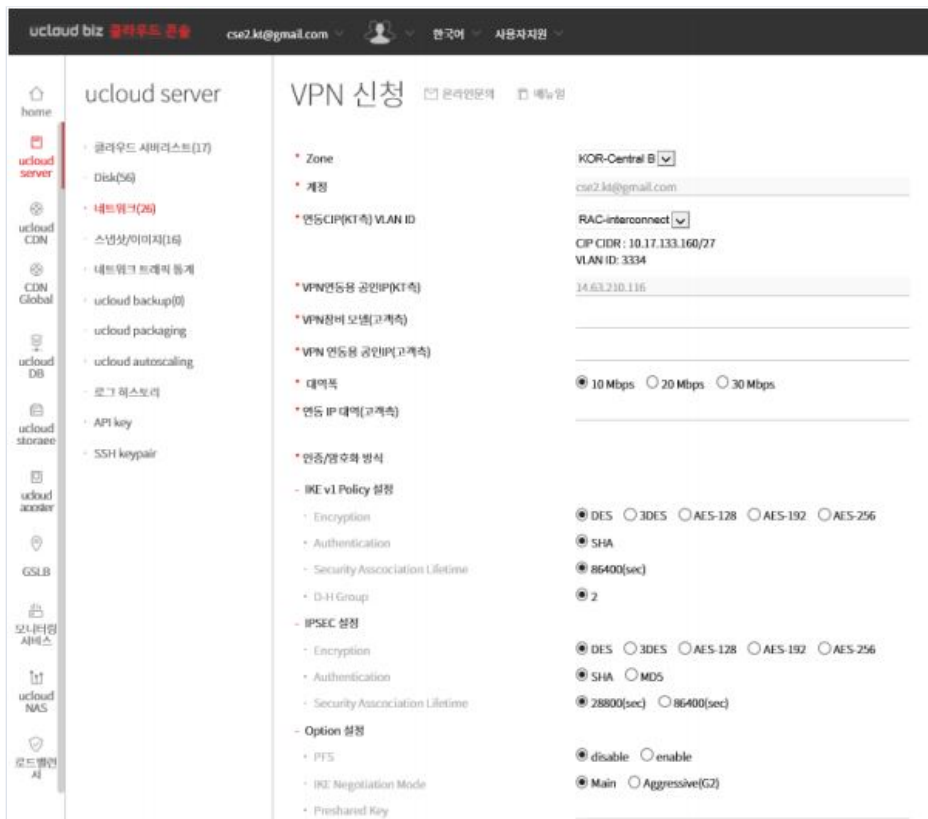
개통 프로세스



2.3.3 Public Cloud VPN 신청 방법

ucloud biz 포탈에서 VPN 신청

ucloudbiz 서비스 포탈 로그인후 > 클라우드 콘솔 > ucloud server > 네트워크 > VPN > VPN 신청



zone : VPN 을 구성하려는 Public Cloud 의 Zone 을 선택

계정 : 자동입력

연동 CIP(KT 측) VLAN ID : VPN 을 연동하려는 CIP 를 선택 (CIP 가 없는 경우 CIP 를 먼저 구성 (클라우드 콘솔 > ucloud server > 네트워크 > CIP)

VPN 연동용 공인 IP (KT 측) : 자동입력

VPN 장비모델 (고객측) : 고객사에 설치된 VPN 장비 모델명 입력

VPN 연동용 공인 IP (고객측) : VPN 을 연동하기 위한 공인 IP 입력

대역폭 : 10/20/30Mbps 중에서 선택

연동 IP 대역(고객측) : 고객사 네트워크 대역, 보통 사설 IP 대역

인증/암호화 방식
IKE 정책 설정 : Encryption 만 고객사가 선호하는 방식으로 선택 IPSEC 설정 : Encryption, Authentication,

Security Association Lifetime 을 고객사가 선호하는 방식으로 설정

Option 설정 : 선호하는 방식으로 설정

VPN 담당자 연락처 : 고객사의 VPN 설정작업 실무를 담당할 담당자 연락처를 기재

□ 고객사 VPN 장비 설정

고객사의 VPN 담당자는 Public VPN 방식과 정합을 위해 위 신청화면에 기재한 내용과 같이 VPN 장비를 설정합니다.

고객사 VPN 장비가 Proxy 모드로 설정된 경우 로컬 Network 을 여러 개 등록이 불가능한 경우가 있으므로 이 경우 any address 로 등록합니다

□ 고객사 네트워크 장비 라우팅 설정

kt cloud 와 연동하려는 고객사 네트워크를 VPN 을 통해 연동할 수 있도록 고객사 라우터에서 라우팅을 설정합니다.

하나의 고객사 네트워크를 VPN 방향으로 라우팅하지 않고 개별 시스템별로 라우팅 처리를 하고자하는 경우 개별 시스템상에서 VPN으로 향하

는 라우팅 테이블이 추가되어야 합니다.

□ 고객사 방화벽 오픈

Public Cloud 와 고객사 전산실간 VPN 연결 구성도에서 보는 것 처럼 고객사 전산실에서 외부로 나가는 내부 방화벽이 있는 경우 방화벽에 대한 오픈 작업을 진행합니다.

라우터를 VPN endpoint 로 사용하는 경우 라우터의 ACL (Access Control List) 에 로컬 네트워크 및 리모트 네트워크가 모두 허용이 되었는지 확인합니다.

□ VM 라우팅 설정

위 모든 과정에 문제가 없으면 VM 에서는 VPN 으로 가기 위한 Routing Table 을 추가합니다. Linux 를 기준으로 하면 아래와 같이 될 것입니다.

```
# route add <remote network> gw <gwip>
```

위에서 gateway IP는 VPN 연동 신청후, Techcenter 를 통해 안내됩니다. (CIP 네트워크 IP Plan 에 따라 할당)

□ Ping Test

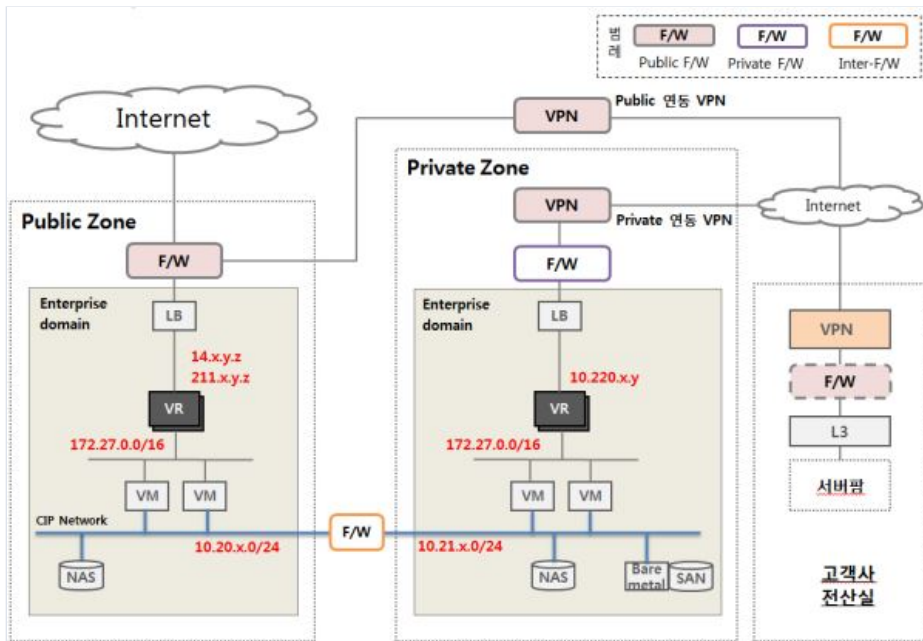
모든 작업이 완료되면 단계적으로 ping test 를 수행하여 점검합니다.

ex) 10.x.y.z/23~27 로 ping

2.4 Enterprise Cloud VPN 서비스

2.4.1 Enterprise Cloud VPN 구조

□ 서비스 구조



고객사 전산실의 시스템은 VPN 이용, Public Zone VM 또는 Private Zone VM 과 연동, Private Zone VM 과 연동이 Default.

고객사 전산실내에는 일반적으로 방화벽으로 내부망으로 보호하도록 구성

연동경로 : 고객사 서버팜 <-> 고객사 F/W <-> 고객사 VPN 장비 <-> 인터넷 <-> kt CDC VPN 장비 <-> Public Zone F/W 또는 Private Zone F/W <-> Public Zone VR 또는 Private Zone VR <-> VM

Private 연동 VPN : 고객사에서 kt CDC 로 라우팅되는 IP 는 Private IP (10.220.x.y)

Public 연동 VPN: 고객사에서 kt CDC 로 라우팅되는 IP 는 Public IP (14.x.y.z 또는 211.x.y.z)

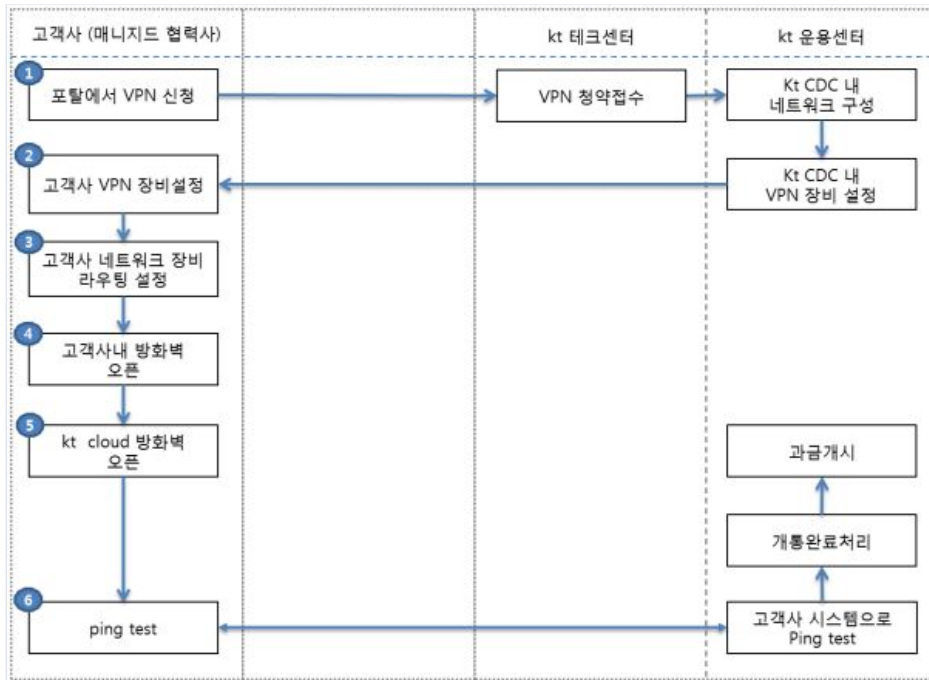
Public 연동 VPN 의 경우는 VPN 을 경유하여 Public LB 에 연동하는 것은 불가

▣ Public Cloud 연동 VPN 장비

Enterprise 의 공용 VPN 장비는 Cisco 장비 (Cisco ASA 5585) 로 고객사측 VPN 장비도 가능한한 Cisco 호환 장비로 구성 권고.

2.4.2 개통 프로세스 및 체크리스트

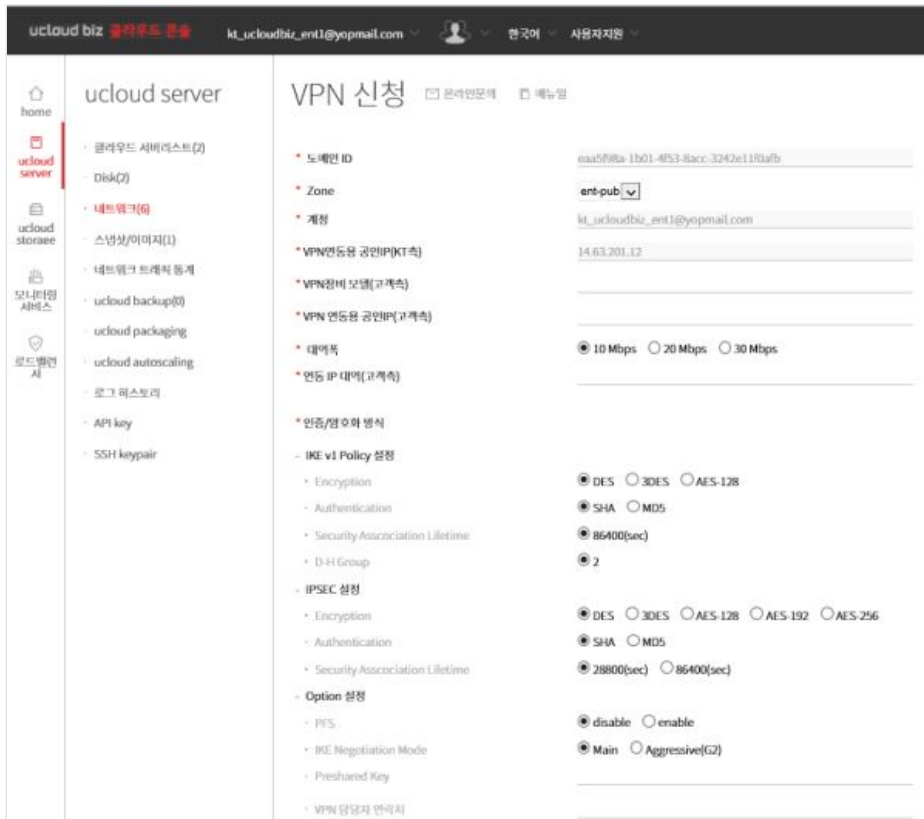
개통 프로세스



2.4.3 Enterprise Cloud VPN 신청 방법

□ ucloud biz 포털에서 VPN 신청

ucloudbiz 서비스 포털 로그인후 > 클라우드 콘솔 > ucloud server > 네트워크 > VPN > VPN 신청



도메인 ID : 고객사가 포함된 도메인 ID (자동 입력)

zone : VPN 을 구성하려는 Enterprise Cloud 의 Zone 을 선택 (Public/Private)

계정 : 자동입력

VPN 연동용 공인 IP (KT 측) : 자동입력

VPN 장비모델 (고객측) : 고객사에 설치된 VPN 장비 모델명 입력

VPN 연동용 공인 IP (고객측) : VPN 을 연동하기 위한 공인 IP 입력

대역폭 : 10/20/30Mbps 중에서 선택

연동 IP 대역(고객측) : 고객사 네트워크 대역, 보통 사설 IP 대역

인증/암호화 방식 IKE 정책 설정 : Encryption 만 고객사가 선호하는 방식으로 선택 IPSEC 설정 : Encryption, Authentication 을 고객사가 선호하는 방식으로 설정

Option 설정 : 선호하는 방식으로 설정

VPN 담당자 연락처 : 고객사의 VPN 설정작업 실무를 담당할 담당자 연락처를 기재

▣ 고객사 네트워크 장비 라우팅 설정

kt cloud 와 연동하려는 고객사 네트워크를 VPN 을 통해 연동할 수 있도록 고객사 라우터에서 라우팅을 설정합니다.

하나의 고객사 네트워크를 VPN 방향으로 라우팅하지 않고 개별 시스템별로 라우팅 처리를 하고자하는 경우 개별 시스템상에서 VPN으로 향하

는 라우팅 테이블이 추가되어야 합니다.

▣ 고객사 방화벽 오픈

Enterprise-Cloud 와 고객사 전산실간 VPN 연결 구성도에서 보는 것 처럼 고객사 전산실에서 외부로 나가는 내부 방화벽이 있는 경우 방화벽에 대한 오픈 작업을 진행합니다.

라우터를 VPN endpoint 로 사용하는 경우 라우터의 ACL (Access Control List) 에 로컬 네트워크 및 리모트 네트워크가 모두 허용이 되었는지 확인합니다.

▣ kt cloud 방화벽 오픈

Enterprise-Cloud 와 고객사 전산실간 VPN 연결 구성도에서 VPN 이 연동되는 포인트가 Public 연동 VPN 이라면 Public Zone의 F/W 과 Public Zone 의 계정별 VR 에서 방화벽을 오픈합니다.

Enterprise-Cloud 와 고객사 전산실간 VPN 연결 구성도에서 VPN 이 연동되는 포인트가 Private 연동 VPN 이라면 Private Zone 의 F/W 과 Private Zone 의 계정별 VR 에서 방화벽을 오픈합니다.

Public F/W 이나 Private F/W 에 대한 오픈 및 Public F/W 과 VPN 간 연결은 윈스텍으로 첨부 2. 방화벽 정책신청서를 작성하여 윈스로 전달하여 오픈합니다.

Public Zone 의 VR 이나 Private Zone 의 VR 은 ucloudbiz 서비스 포털 (<http://ucloudbiz.olleh.com>) 을 이용하여 오픈 작업을 수행합니다.

▣ Ping Test

모든 작업이 완료되면 단계적으로 ping test 를 수행하여 점검합니다.

Public 연동 VPN 인 경우 Legacy -> VM ping test: VR 의 공인 IP (14.x.y.z 또는 211.x.y.z) 로 ping

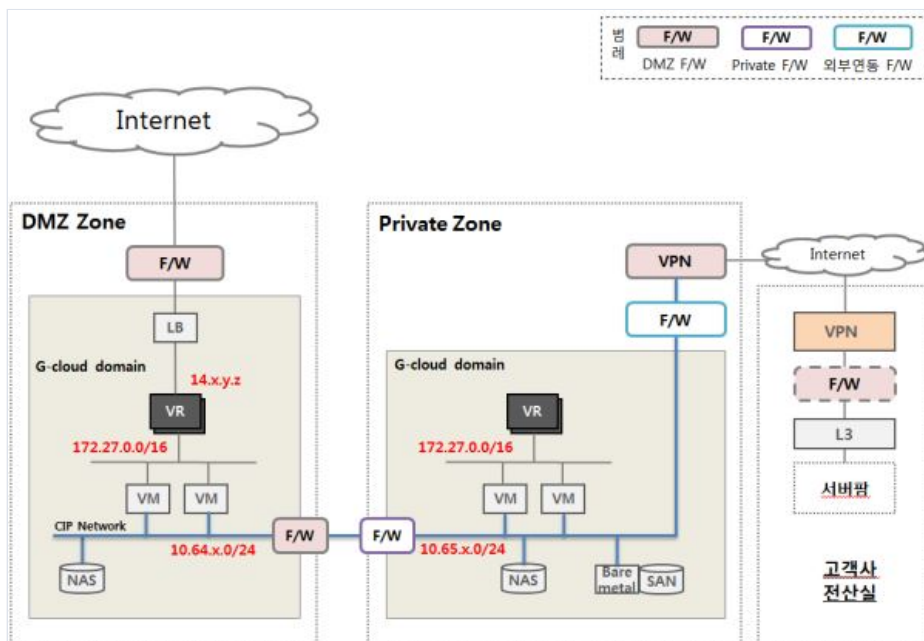
Private 연동 VPN 인 경우 Legacy -> VM ping test : VR 의 사설 IP (10.220.x.y) 로 ping

VM -> Legacy : VM 에서 Legacy 시스템 (Remote Network) 으로 ping 을 확인합니다

2.5 G-Cloud VPN 서비스

2.5.1 G-Cloud VPN 구조

□ 서비스 구조



고객사 전산실의 시스템은 VPN 이용, Private Zone VM 과 연동

고객사 전산실내에는 일반적으로 방화벽으로 내부망으로 보호하도록 구성

연동경로 : 고객사 서버팜 <-> 고객사 F/W <-> 고객사 VPN 장비 <-> 인터넷 <-> kt CDC VPN 장비 <-> Private Zone F/W

□ Private Zone VM

Enterprise Zone 의 경우 Private Zone VR 을 경유하나 G-Cloud 의 경우 CIP network 으로 직접 연동

고객사에서 kt CDC 로 라우팅되는 IP 는 Public IP (14.x.y.z 또는 211.x.y.z)

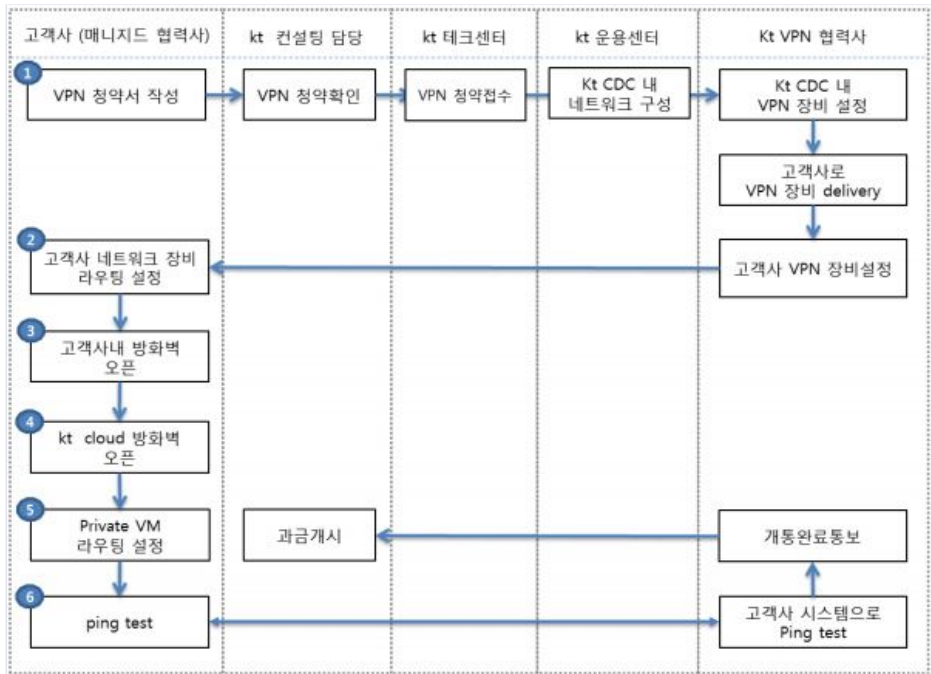
G-Cloud 에서는 Enterprise-Cloud 와는 다르게 CIP 로 DMZ 와 Private 을 연결할 때 두 개의 F/W 을 경유

□ Public Cloud 연동 VPN 장비

G-Cloud VPN 장비는 대국측 장비도 kt 에서 delivery 하여 설치하는 것을 기본 정책으로 합니다. 이 때 kt cloud CDC 에 있는 VPN 장비와 호환되는 장비를 설치합니다.

2.5.2 개통 프로세스 및 체크리스트

개통 프로세스



2.5.3 G-Cloud VPN 신청 방법

□ G-Cloud VPN 신청

첨부 1. G-Cloud VPN 신청양식을 작성하여 kt 컨설팅 담당자에게 이메일로 신청서를 제출합니다.
 이후 kt 컨설팅 담당자가 kt VPN 협력사로 VPN 개통요청이 가게 되며 신청서에 기재된 구성정보에 따라 VPN 장비를 설정합니다.
 그리고 기재된 고객사 연락처로 연락을 하여 연동작업에 대한 협의를 진행하면서 개통작업을 진행합니다.

□ 고객사 네트워크 장비 라우팅 설정

kt cloud 와 연동하려는 고객사 네트워크를 VPN 을 통해 연동할 수 있도록 고객사 라우터에서 라우팅을 설정합니다.

하나의 고객사 네트워크를 VPN 방향으로 라우팅하지 않고 개별 시스템별로 라우팅 처리를 하고자하는 경우 개별 시스템상에서 VPN 으로

향하는 라우팅 테이블이 추가되어야 합니다.

□ 고객사 방화벽 오픈

G-Cloud 와 고객사 전산실간 VPN 연결 구성도에서 보는 것 처럼 고객사 전산실에서 외부로 나가는 내부 방화벽이 있는 경우 방화벽에 대한 오픈 작업을 진행합니다.

라우터를 VPN endpoint 로 사용하는 경우 라우터의 ACL (Access Control List) 에 로컬 네트워크 및 리모트 네트워크가 모두 허용이 되었는지 확인합니다

□ kt cloud 방화벽 오픈

VPN 연동 방화벽에 대한 오픈 정책요청은 서비스 포탈 (<https://gov.ucloudbiz.olleh.com>) > email 계정 > 개인 정보 > F/W 정책신청에서 요청하거나 윈스테크로 첨부 2. 방화벽 정책신청서를 작성하여 윈스로 전달하여 오픈 합니다.

□ VM 라우팅 설정

위 모든 과정에 문제가 없으면 Private VM 에서는 VPN 으로 가기 위한 Routing Table 을 추가해야 합니다. 추가 된 라우팅테이블은 다음과 같은 형태입니다.

```
# route add -net 10.66.x.0/24 gw 10.65.x.1
```

10.66.x.0/24 네트워크는 VPN 네트워크입니다. 이로 가기 해서는 10.65x.1 의 G/W 를 경유하도록 설정해야 합니다. 또한 고객사 네트워크로 가기위한 경로도 추가해줍니다.

```
Destination Gateway Genmask Flags Iface10.66.x.0 10.65.x.1 255.255.255.0 UG eth1Remote Network 10.65.x.1 Remote Subnet UG eth1
```

10.66.x.0/24 네트워크는 VPN 네트워크입니다. 이로 가기위해서는 10.66.x.1 의 G/W 를 경유하도록 설정해야 합니다. 또한 고객사 네트워크로 가기위한 경로도 추가해줍니다.

□ Ping Test

모든 작업이 완료되면 단계적으로 ping test 를 수행하여 점검합니다.

Legacy -> VM : VM 의 CIP Network IP (10.65.x.0/24) 로 ping 을 확인합니다.

VM -> Legacy : VM 에서 Legacy 시스템 (Remote Network) 으로 ping 을 확인합니다.

2.9 VPN 기타 가이드

문의

	전화번호	온라인 문의 및 요청
G-Cloud VPN 구성 협력사	031-622-5891	mss1@wins21.co.kr

유의사항

VPN 연동작업은 고객사 사내 네트워크 환경과 정합을 맞추는 작업 및 방화벽 작업 등 적지 않은 시간이 걸리는 작업으로 개통 요청부터 개통완료까지 업무일 기준 최소 3 일이상 소요될 수 있으므로 일정을 지나치게 촉박하게 잡지 않는 것이 좋습니다.

고객사 VPN 장비는 되도록 이중화를 권고합니다. Kt Cloud VPN 은 자체적으로 이중화되어 있으나 고객사 VPN 이 이중화되어 있지 않은 경우 단일 장애지점 (SPoF) 가 될 수 있습니다.

첨부1. G-Cloud VPN 구성 및 관제 신청양식

[다운로드](#)

첨부2. 방화벽 정책 신청서

[다운로드](#)