ucloud 공용 VPN 연동가이드

2015-10-20

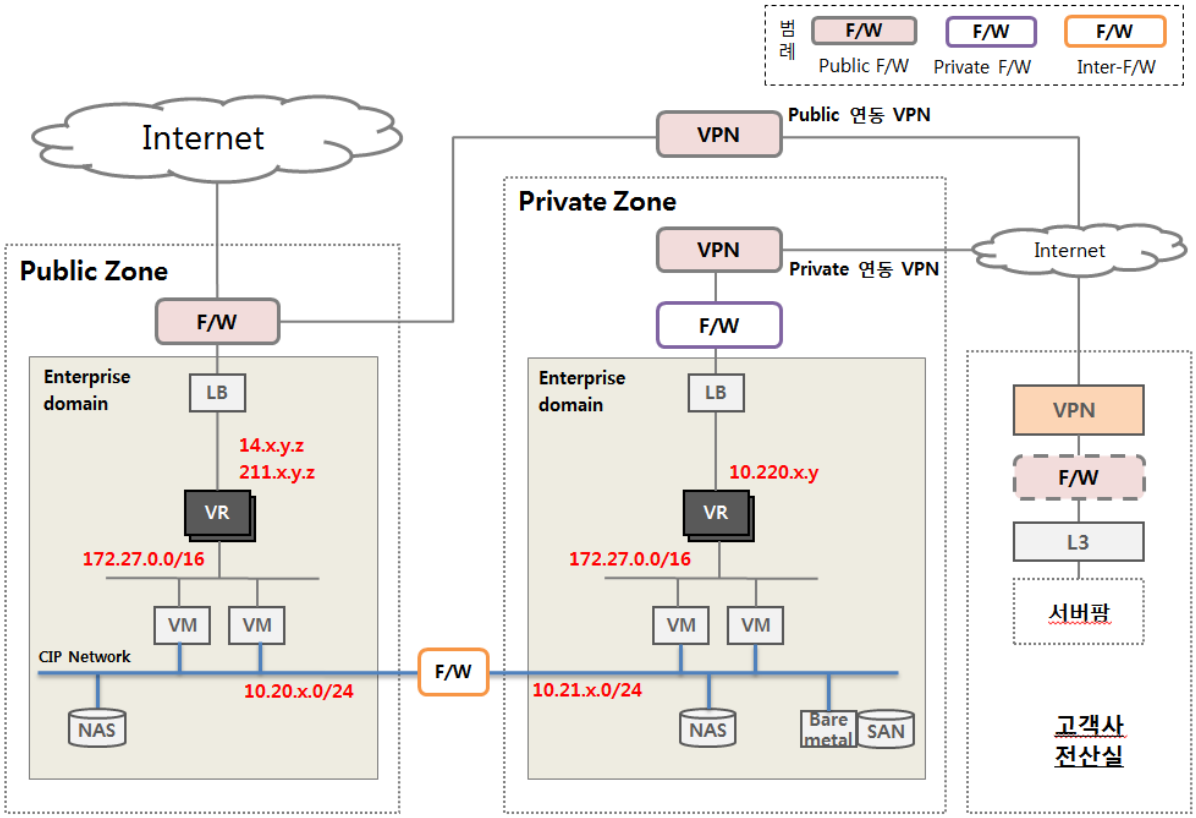
1. ucloud VPN 연동 지원 유형

연동 Zone	IPSec-VPN
Enterprise Cloud 의 Public Zone 연동 Enterprise Cloud 의 Private Zone 연동	공용 VPN 장비연동 2.1)
G-Cloud 의 Private Zone 연동	공용 VPN 장비연동 2.2)

2. 유형별 구성도 및 지원장비

2.1) Enterprise Cloud 와 Legacy 간 공용 VPN (IPSec-VPN) 을 이용한 연동

2.1.1) 구성도



- 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

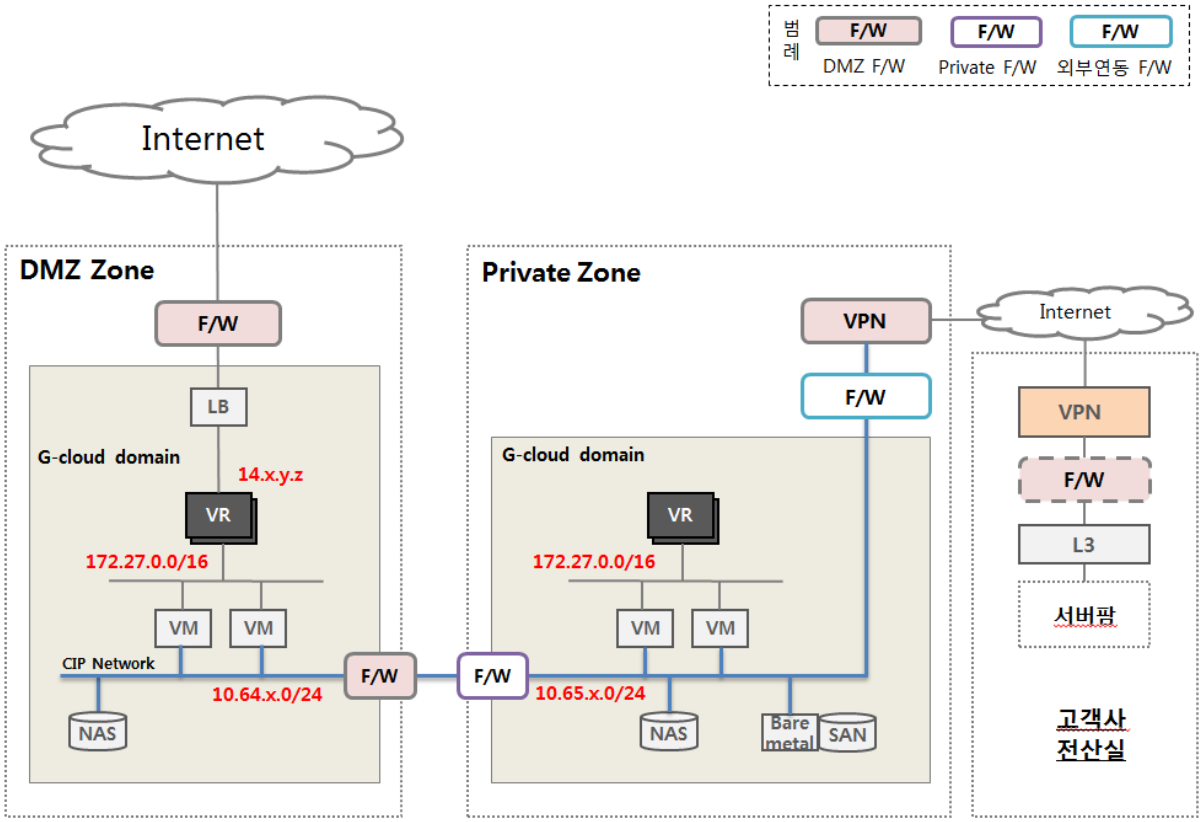
- Private 연동 VPN 은 고객사에서 kt CDC 로 라우팅되는 IP 는 Private IP (10.220.x.y)
- Public 연동 VPN 은 고객사에서 kt CDC 로 라우팅되는 IP 는 Public IP (14.x.y.z 또는 211.x.y.z)
- Public 연동 VPN 의 경우는 VPN 을 경유하여 Public LB 에 연동하는 것은 불가

2.1.2) 지원장비

- Enterprise 의 공용 VPN 장비는 Cisco 장비 (Cisco ASA 5585) 로 대국측 (Enterprise Legacy VPN 장비) 도 되도록 Cisco 호환 장비로 구성 권고.

2.2) G-Cloud 의 Private Zone 과 Legacy 간 공용 VPN (IPSec-VPN) 을 이용한 연동

2.2.1) 구성도

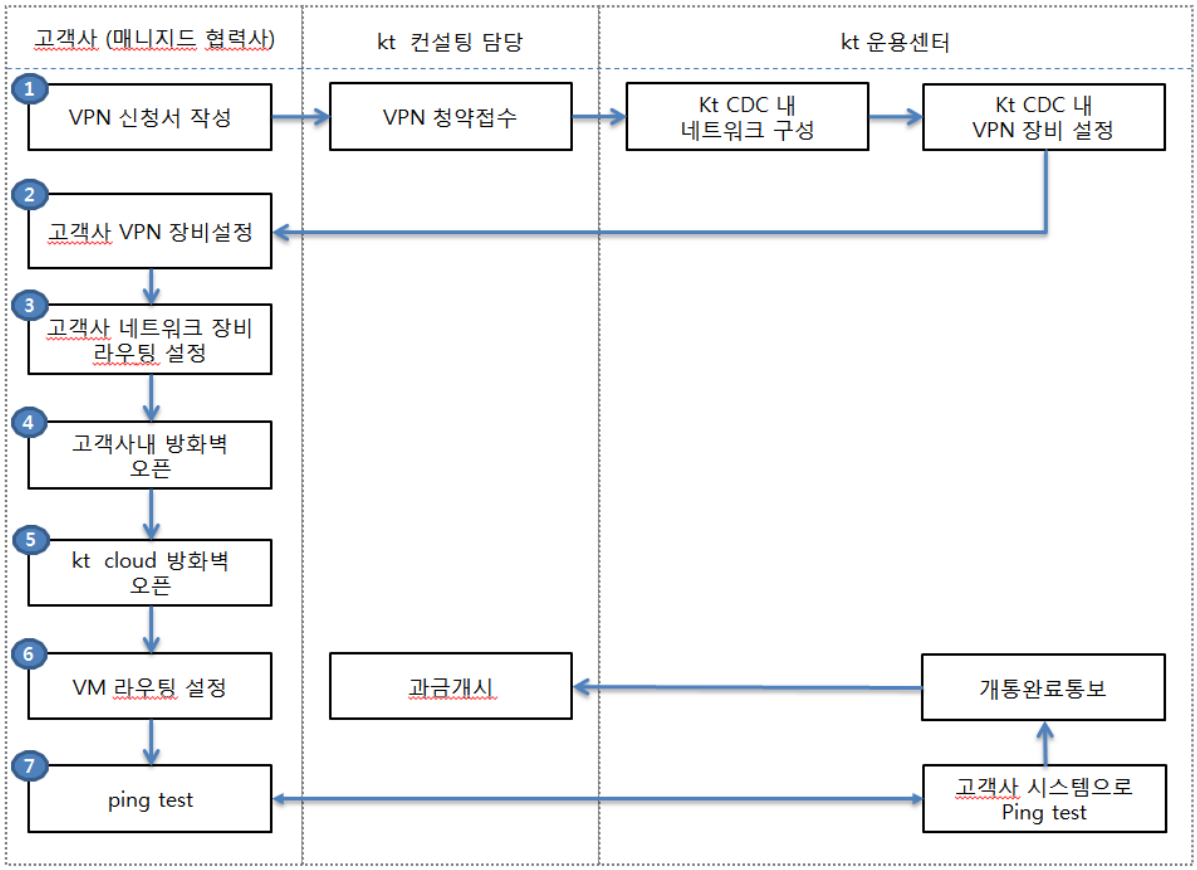


- 고객사 전산실의 시스템은 VPN 이용, Private Zone VM 과 연동
- 고객사 전산실내에서는 일반적으로 방화벽으로 내부망으로 보호하도록 구성
- 연동경로 : 고객사 서버팜 → 고객사 F/W → 고객사 VPN 장비 → 인터넷 → kt CDC VPN 장비 → Private Zone F/W → Private Zone VM
- Enterprise Zone 의 경우 Private Zone VR 을 경유하나 G-Cloud 의 경우 CIP network 으로 직접 연동
- 고객사에서 kt CDC 로 라우팅되는 IP 는 CIP (10.65.x.0/24)
- G-Cloud 에서는 Enterprise-Cloud 와는 다르게 CIP 로 DMZ 와 Private 을 연결할 때 두 개의 F/W 을 경유

2.2.2) 지원장비 : 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 설치

3. 개통 프로세스 및 체크리스트

3.1) Enterprise-Cloud VPN 개통 프로세스



3.2) Enterprise-Cloud VPN 개통을 위한 고객사 단계별 작업 사항 및 점검사항

3.2.1) VPN 신청서 작성

- 첨부 1. Enterprise Cloud 공용 VPN 신청양식을 작성하여 kt 컨설팅 담당자에게 이메일로 신청서를 제출합니다.

- 이후 kt 컨설팅 담당자가 kt 운용센터로 VPN 개통요청이 가게 되며 신청서에 기재된 구성정보에 따라 VPN 장비를 설정합니다. 그리고 기재된 고객사 연락처로 연락을 하여 연동작업에 대한 협의를 진행하면서 개통작업을 진행합니다.

3.2.2) 고객사 VPN 장비 설정

- 고객사의 VPN 담당자는 Enterprise VPN 방식과 정합을 위해 신청서에 기재한 방식대로 VPN 장비를 설정합니다.
  이 때 remote VPN (kt cloud VPN) 의 IP 는 kt 운용센터와 협의후 설정합니다.
- 키 교환을 위한 IKE 파라미터 및 IPSec 파라미터에 유의하여 설정합니다.
- 고객사 VPN 장비가 Proxy 모드로 설정된 경우 로컬 Network 을 여러개 등록이

불가한 경우가 있으므로 이 경우 any address 로 등록합니다.

3.2.3) 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.
- 라우터를 VPN endpoint 로 사용하는 경우 위 3.2.2) 절의 과정이 라우터상에서 설정되어야 합니다.

3.2.4) 고객사 방화벽 오픈

- 2.1.1) 의 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.

3.2.5) kt cloud 방화벽 오픈

- 2.1.1) 의 구성도에서 VPN 이 연동되는 포인트가 Public 연동 VPN 이라면 Public Zone 의 F/W 과 Public Zone 의 계정별 VR 에서 방화벽을 오픈합니다.
- 2.1.1) 의 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 윈스테크로 첨부 3. 방화벽 정책신청서를 작성하여 윈스로 전달하여 오픈합니다.
- Public Zone 의 VR 이나 Private Zone 의 VR 은 ucloudbiz 서비스 포탈 (http://ucloudbiz.olleh.com) 을 이용하여 오픈 작업을 수행합니다..

3.2.6) VM Routing 설정 (옵션)

- 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 172.27.0.1
```

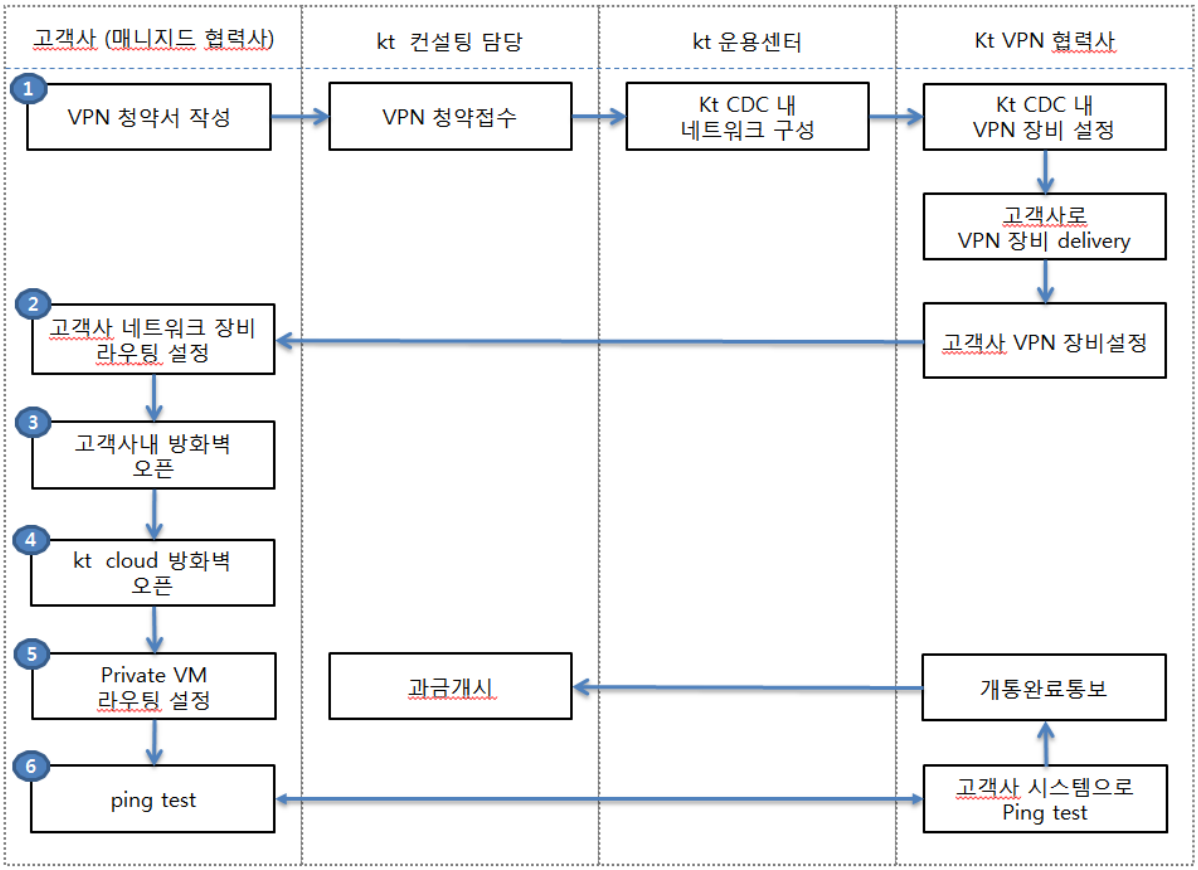
- 위에서 gateway IP 는 VR 의 IP (172.27.0.1) 입니다. VM 의 default GW 가 VR 이기 때문에 Remote Network 으로 가는 별도의 경로를 찾지 못하게 되면 자동적으로 VR 로 갈 것이기 필수 사항은 아닙니다.

3.2.7) 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

3.3) G-Cloud VPN 개통 프로세스



3.4) G-Cloud VPN 개통을 위한 고객사 단계별 작업 사항 및 점검사항

3.4.1) VPN 신청서 작성

- 첨부 2. 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.

3.4.2) 고객사 VPN 장비 설정

- VPN 장비는 kt 협력사가 delivery 할 수도 있고 (default) 고객사 자체적으로 준비할 수 있습니다. 되도록 정합성을 위해 kt 협력사가 delivery 하는 장비를 사용할 것을 권고합니다.
- kt VPN 협력사가 delivery 한 장비의 경우 고객사 네트워크 담당자와의 협의를 통해 협력사가 직접 VPN 설정작업을 진행합니다.

3.4.3) 고객사 네트워크 장비 라우팅 설정

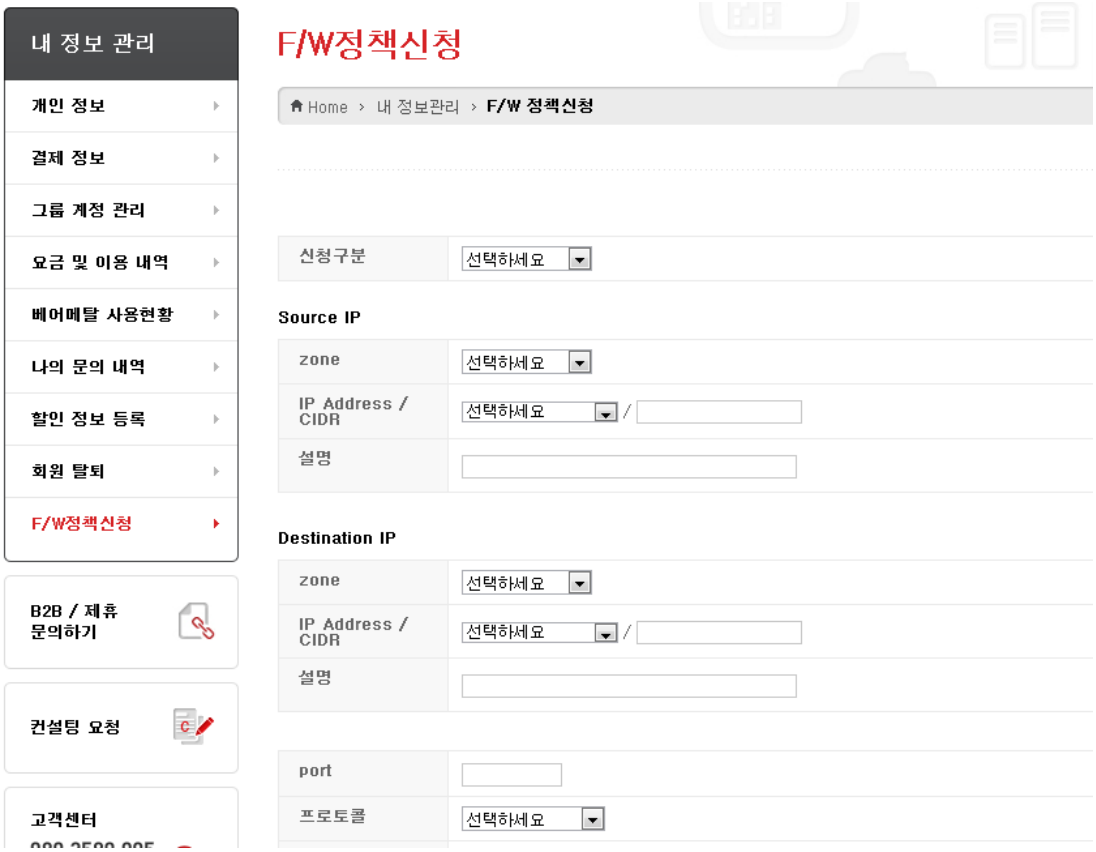
- kt cloud 와 연동하려는 고객사 네트워크를 VPN 을 통해 연동할 수 있도록 고객사 라우터에서 라우팅을 설정합니다.
- 하나의 고객사 네트워크를 VPN 방향으로 라우팅하지 않고 개별 시스템별로 라우팅 처리를 하고자하는 경우 개별 시스템상에서 VPN 으로 향하는 라우팅 테이블이 추가되어야 합니다.
- 라우터를 VPN endpoint 로 사용하는 경우 위 3.4.2) 절의 과정이 라우터상에서 설정되어야 합니다.

3.4.4) 고객사 방화벽 오픈

- 2.2.1) 의 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.

3.4.5) kt cloud 방화벽 오픈

- 2.2.1) 의 구성도에서 VPN 연동 방화벽을 오픈합니다.
- VPN 연동 방화벽에 대한 오픈 정책요청은 서비스 포탈 (https://gov.ucloudbiz.olleh.com) > email 계정 > 개인정보 > F/W 정책신청에서 요청하거나 윈스테크로 첨부 3. 방화벽 정책신청서를 작성하여 윈스로 전달하여 오픈합니다.



3.4.6) VM Routing 설정

- 위 모든 과정에 문제가 없으면 Private VM 에서는 VPN 으로 가기 위한 Routing Table 을 추가해야 합니다. 추가된 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	Iface
10.66.x.0	10.65.x.1	255.255.255.0	UG	eth1
Remote 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.

3.4.7) 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.

4. 문의 및 요청 연락처

	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

5. 유의사항

- VPN 연동작업은 고객사 사내 네트워크 환경과 정합을 맞추는 작업 및 방화벽 작업등 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.

첨부 1. Enterprise Cloud 공용 VPN 신청양식

<table>
<tr><th>구분</th><th>내용</th></tr>
<tr><td>VPN 장비 모델</td><td>(예) Cisco ASA</td></tr>
<tr><td>VPN IP</td><td>(예) 200.10.200.10</td></tr>
<tr><td>VPN bandwidth</td><td>(예)10Mbps ~ [xxx]Mbps</td></tr>
<tr><td>연동 IP 대역</td><td>(예) 30.10.0.1 ~ 30.10.0.10</td></tr>
<tr><td>인증/암호화 방식</td><td>
Phase 1 : IKE 파라미터
IKEv1 (default)의 경우 아래 조합중 선택
<table>
<tr><th>Priority</th><th>Encryption</th><th>Hash</th><th>D-H group</th><th>Authentication</th><th>Lifetime</th></tr>
<tr><td>1</td><td>Aes-128</td><td>Sha</td><td>2</td><td>Pre-share</td><td>86400</td></tr>
<tr><td>2</td><td>3des</td><td>Sha</td><td>2</td><td>Pre-share</td><td>86400</td></tr>
<tr><td>3</td><td>Aes-128</td><td>Md5</td><td>2</td><td>Pre-share</td><td>86400</td></tr>
<tr><td>4</td><td>3des</td><td>Md5</td><td>2</td><td>Pre-share</td><td>86400</td></tr>
<tr><td>5</td><td>Des</td><td>Sha</td><td>2</td><td>Pre-share</td><td>86400</td></tr>
<tr><td>6</td><td>Des</td><td>Md5</td><td>2</td><td>Pre-share</td><td>86400</td></tr>
</table>
IKE2v2 의 경우 아래 조합중 선택
<table>
<tr><th>Priority</th><th>Encryption</th><th>Hash</th><th>D-H group</th><th>Authentication</th><th>Lifetime</th></tr>
<tr><td>1</td><td>AES-256</td><td>Sha</td><td>2 or 5</td><td>Pre-share</td><td>86400</td></tr>
<tr><td>10</td><td>Aes-192</td><td>Sha</td><td>2</td><td>Pre-share</td><td>86400</td></tr>
<tr><td>20</td><td>Aes</td><td>Sha</td><td>2</td><td>Pre-share</td><td>86400</td></tr>
<tr><td>30</td><td>3des</td><td>Sha</td><td>2</td><td>Pre-share</td><td>86400</td></tr>
<tr><td>40</td><td>Des</td><td>Sha</td><td>2</td><td>Pre-share</td><td>86400</td></tr>
</table>
Phase 2 : IPSEC Parameter
IPsec Proposal : Mode(Tunnel / Transparent)
Encryption : DES, 3DES, AES-128, AES-192, AES-256
Authentication : SHA, MD5
Secyrity Association Lifetime : 28800(sec) / 4608000(Kbytes)

Options 설정
PFS(Perfect Forward Secrecy) : disable (default) / enable
IKE Negotiation Mode : Main (default) / Aggressive
</td></tr>
<tr><td>Preshared Key</td><td>Key 값은 VPN 연동 작업 시 알려주시면 맞춰서 설정할 예정입니다.</td></tr>
<tr><td>VPN 담당자 연락처</td><td>(예) 홍길동, 010-1234-5678</td></tr>
</table>

첨부2. G-Cloud VPN 구성 신청양식

서비스 신청 정보

1. 설치 기본정보

설치 요청일	년 월 일 오전 시
설치 주소	
NIC TYPE	☐ UTP ☐ Multi Fiber ☐ Single Fiber
장비 관리 공인 IP	x.x.x.x/x
내부 IP 대역 / 서브넷	y.y.y.y/y
Gateway IP	z.z.z.z (Default G/W : k.k.k.k)
Link speed,	☐ Auto ☐ 100M Full ☐ 1G Full ☐ 기타 ( )

2. 위험 단계별 담당자 연락처

	직책	담당자명	TEL	H.P	E-mail
관심, 주의					
경계					
심각					

첨부3. 방화벽 정책 신청서

방화벽 정책 신청서

고객정보					
고객사 명		신청일		신청자	
일반전화		휴대전화		E-mail	
작업희망일시	년 월 일 시 분	작업내용			

접근 제어규칙 변경사항									
	Src-IP			Dst-IP			서비스 (포트번호)	프로토콜	허용/ 차단
신규/변경/ 삭제	Zone	IP Address	설명	Zone	IP Address	설명			
		/			/				