업데이트일 : 2018-11-01

IV. 엔터프라이즈

1. Enterprise Security

목차

- 1.1 Enterprise Security 서비스 소개
- 1.2 Enterprise Security FAQ
- o 1.3 Enterprise Security 상품 신청 방법
- 1.4 Enterprise Security 서비스 이용 방법
- 1.5 Enterprise Security 기타 가이드

1.1 Enterprise security 서비스소개

1.1.1 목적/용도

Enterprise Security 서비스는 일반 클라우드에 비해 H/W 보안장비 기반으로 강화된 보안을 제공하는 기업특화 클라우드로, 기업 중요 시스템, 금융, 의료 등 높은 수준의 보안을 요구하는 분야에 더욱 적합합니다. 자동화 기반의 방화벽 서비스로 사용자가 방화벽 정책을 직접 관리할 수 있습니다(매니지드 옵션 선택) 사용자는 자신이 네트워크 및 방화벽 정책을 설정하고 이를 기반으로 ucloud biz 서비스를 사용할 수 있습니다.

ㅁ 서비스 특·장점

ㅇ 보안성, 고성능

- 침입탐지시스템(IPS), 방화벽, VPN 등 물리 보안장비로 구현 되어 보안 안정성 제공
- 인바운드 및 아웃바운드 트래픽 필터링을 통하여 보안기능을 강화 하였습니다.
- DMZ존과 private존을 분리하여 중요 데이터 보호 구조

ㅇ 유연성

- DMZ 및 private 네트워크를 유연하게 생성/변경 할 수 있습니다(추가적인 네트워크 생성은 별도 요청으로 가능합니다).

- 변화하는 비즈니스 환경에 따라, 사용자가 직접 방화벽 정책을 정의할 수 있습니다.

- 물리서버(베어메탈), 전용회선 연동이 가능합니다

ㅇ 효율성, 신속성

- 모든 네트워크/방화벽 정책은 ucloud biz 포탈 콘솔을 사용하여 손쉽게 설정 가능합니다.

- 고객이 설정한 정책은 바로 사용자의 네트워크/방화벽에 적용 되며 고객의 업무 효율성을 극대화 할 수 있 습니다.

	Enterprise Security	기존 Enterprise Cloud
제공 Zone	Seoul-M2 (목동) - 신규 고성능 server.g2 제공 - M2존내 public VM과 계정 이동성	천안 enterprise 전용존
망분리	DMZ / private 분리	DMZ / private 분리
IPS	Enterprise 전용 물리장비(CC인증)	Enterprise 전용 물리장비(CC인증)
방화벽	Enterprise 전용 물리장비(CC인증) 고객 도메인별 최대 40만 세션 제공	Enterprise 전용 물리장비(CC인증) 고객 도메인별 최대 10만 세션 제공
매니지드	- 보안 매니지드 서비스 - 방화벽은 self 보안관제 선택(저비용)	보안 매니지드 서비스
기타	- 단일 NIC 연결 - Static routing, 고정 지정 IP 부가기능	- Multi NIC 연결

1.1.2 구조/원리

ㅁ 시스템 구성도

다.



Tier는 고객 계정 전용의 가상 L2 네트워크로 여러 개의 Tier(기본으로 제공하는 Tier 포함 총 15개)를 생성할 수 있습니다. 고객은 방화벽, NAT 를 통해 포트포워딩이나 Static NAT를 설정할 수 있고 방화벽 Rule도 직접 설정이 가능합니

1.1.3 유의사항/제약사항

ㅁ 셀프 서비스/ 보안 매니지드 서비스

- Enterprise Security에서는 방화벽 셀프 서비스를 사용하시는 경우에 포탈 콘솔을 이용하여 고객이 직접 방화 벽 정책 설정을 할 수 있고, 설정 후에는 바로 적용 된 것을 확인할 수 있습니다. 그러나 보안 매니지드 서비스를 받으시는 경우에는 직접 설정을 하지 마시고, 보안 매니지드사로 설정을 요청 하셔야 합니다.

□ Enterprise Cloud / Enterprise Security 구분

- 기존 Enterprise cloud는 천안 zone에 위치 하며, Enterprise security는 목동 M2 zone에서 사용 가능합니다.

1.2 Enterprise Security FAQ

- 방화벽은 도메인당 세션 수 제한이 어떻게 되나요?

o Enterprise Security 방화벽은 도메인당 40만 세션까지 지원 됩니다.

□ 기존 public zone에서 사용중인 VM을 Enterprise Security Zone으로 옮길 수 있나요?

o 존간 및 계정간 이미지 copy 이동은 가능하나, 운영팀과 고객간의 사전 협의가 필요합니다.

□ Tier는 몇 개까지 생성 가능한가요?

o Tier는 L2 가상 네트워크로 기본으로 제공하는 2개의 Tier 네트워크를 포함하여 총 15개의 Tier를 생성할 수 있습니다.

1.3 Enterprise security 상품 신청 방법

1.3.1 컨설팅 신청

고객은 포탈을 통하여 서비스 컨설팅을 요청합니다. Enterprise security는 컨설팅을 통해서만 서비스가 활성화 됩니다.



위 화면 오른쪽에 컨설팅 신청 버튼을 눌러 컨설팅을 신청합니다.

* 사업자 유행	 개인 · 개인사업 · 법인사업
사업자등록변호	사업자등록만호는 ^ 업데 업데
• 12418I	ଅ ମ ାର ଅମ
* 8 8248	
* #128/22	(010 2)
. 8469448	(62 E)
*e-mail 卒土	최신 2011일 주소 일적
*소페티	এমান হাম
	ଏଖ ଲ ନ୍ତ ଅସ
• PARE AN UR	

위 화면에서 각각의 항목을 입력하고 신청버튼을 누르시면 기재된 연락번호로 컨설팅 담당자가 고객께 연락하 여 컨설팅을 진행합니다.

1.3.2 고객 컨설팅

컨설팅 담당자의 오프라인으로 시스템 수요 및 서비스 이용 프로세스에 대한 가이드를 제공합니다. 고객사에서 서비스 이용을 희망하실 경우 고객사 전용의 도메인생성 및 계정생성 단계로 넘어갑니다.

1.3.3 고객 도메인 생성 (KT 운영센터) 및 고객 계정 생성 (고객사)

Enterprise Security 상품은 별도의 내부 도메인 규정이 있습니다. 컨설팅 담당자는 일정한 양식에 맞춘 도메인 네임을 고객과 협의한 후, 그 이름으로 도메인 네임을 만들어 이를 고객사에 전달합니다.

그룹사 : ent2_kt_xxx 일반고객 : ent2_xxx 혹은 ent2_xxx_xxx

고객사는 전달받은 도메인 명을 기준으로 회원가입을 수행합니다. ucloudbiz portal (https://ucloudbiz.olleh.com) 에서 회원가입 시 도메인입력란에 전달받은 도메인 명을 입력합니다.

도메인 정보 입력	확인
* Domain을 이용 중인 고객의 경우 입력해 주시기 바랍니 * Secure Zone을 이용하시는 경우 Domain을 SecureZon 랍니다.	l다. (옵션) ne으로 입력해 주시기 바

회원가입신청이 완료되면 등록하신 이메일 계정으로 인증메일이 발송됩니다. 접속하시어 '회원가입 완료하러 가 기'를 클릭합니다.

전달 받은 도메인 명으로 최초 가입한 계정이 admin의 권한을 갖게 됩니다. 동일한 도메인 명으로 추가 회원가 입을 할 경우 admin으로부터의 승인이 필요하며, 이 때에 생성된 계정은 일반 user의 권한을 가지게 됩니다.

1.3.4 Enterprise security의 계정 관리

고객은 동일 도메인 내 복수 개의 계정을 가질 수 있습니다. 도메인 내 최초 생성된 계정은 admin 권한을 가지 며, 추가로 생성되는 계정들은 admin 계정으로부터 별도의 승인이 필요하고, 승인 후에는 user권한을 갖게 됩니 다.



admin 계정은 방화벽 정책 및 포트포워딩 설정, StaticNAT IP 할당 등의 네트워크 설정이 가능합니다. 추가로 생성된 user 계정은 설정된 네트워크에 VM을 생성할 수 있습니다.

Enterprise 2.0 개청 관리						로그아운
요금 및 이용 내역	사용자 정보				문의 현황	장기구동서버
베어메달 사용현황	계정	1916	29239	상태	문의 0 달년 0	게칭 0 VM 0
나의 문의 내역	test.@test.com	테스트	2017-06-23 14:08:47.0	0.899.6	मंडम र	비 바로가기
할인 정보 등록						_
그룹 계정 관리					< 1840.884	
결제 정보 관리						985
개인 정보 관리						
치원 달치						1941 1944
F/W정책신청						TOP

포탈 메인화면 - 계정 아이콘 - 내 정보 관리 바로가기

위 왼쪽 메뉴의 'Enterprise 2.0 계정 관리' 에서 계정 승인을 진행합니다.

1.3.5 상품 신청

회원가입이 완료되면 포탈 로그인 진행 후 아래 페이지에서 server 상품을 신청합니다.



상품 신청 후에는 기본 인프라 자원이 자동으로 생성되며, 클라우드 콘솔을 통해 서버 및 자원 생성이 가능합니 다.

1.4 Enterprise security 서비스 이용 방법

1.4.1 Server 이용 방법

ㅁ VM 생성

상품 신청이 완료되면 다음과 같은 ucloudbiz 서비스 포탈의 클라우드 콘솔 화면을 보실 수 있습니다.

hame ucloud server	ucloud server - क्रम्पर- मनग스=200 - ग्रह्मम्बर - मन्द्रम्मन्द्रक	클라우드 콘 ucloud blaff4 선생 가방영	·	· 특인하실 수 있으며, 원하는 상품	의 신왕 및 해지가 3	가동합니다.		시스템 아키텍처 System Architecture는 사용 중적 사용및 출우선 등 전체 서 비스의 연관관계를 양눈에 파 역할 수 있도록 구도도를 제공 하는 ucload bla 2만의 특衡된 시비스입니다.
CDN	· 스냅쉿/이미자(31)	이용충인 상품 및 관	8면 자원 현 1	y				০সপম হস
CON Global	· 네트워크 트라티 통계 · ucloud backup(1)	ucloud server		ucloud NAS		로드별런서		추천 상품
8	· ucloud packaging	· 시비대수	20	 首長 개수 	1	- 로드별린시 설정	1	사용용인 영웅과 영제 고인 등 은 상품을 추천 해트립니다.
ucloud	· ucloud autoscaling	· 추가 디스크 개수	5	- 查望哲乐仪		- 山田県江 初合留	0GB	수건 영향으로 운영표를을 줄 이세요.
	· 로그 히스토리	· 非计10 개令	11	1000G8				
E ucloud	· API key	· CIP XED	1	- 스냅샷 캐수	0			웹방화벽(WIWAF- VE) 상품선형
storage	 SSH keypair 	웹방화벽		ucloud storage		ucloud CDN		범상의석
E Zaclara		· 웹방학력 다수	2	- 스토리지 용량	37168	- 시티스 개수	12	WWW-VEE 블라믹인 별 탑 하세 시스템 구축 많이 몰라무
storage				- 스토리지 용량 (ec)	1058	· 다운로드 전송량	OGB	는 환경에서 구순이 용가야는 다양한 웹 공격에 대해 담지 및
8				- 다운코드 환송양	168	· 스트레팅 전송량	0GB	차단하는 보안 서비스입니다.
ucloud appriler				- 폭입박스 개수	35			ChallManitas
		ucloud DB		GSLR				MB NBUN

ucloud server 메뉴에서 '서버 신청'을 이용하여 필요한 VM을 생성합니다.

ucloud server	서버생성 🖻) 온라인문의 📋	1117 <u>1</u> 1	
· 클라우드 서버리스트(3)	* 표시는 필수 입력사항입니다	8.		
· Disk(4) · 네트워크(2)	• 서비명			중복확인
- 스냅샷/이미치(2)	호스트명			중복확인
• 네트워크 트레직 통계	• 위치	KOR-Secul M2		
 ucloud backup(0) ucloud packaging 	* 운영체제	<u>서버종류/운영체제</u>	선택하기	
ucloud autoscaling	• MH	요금제/서비 사양 선	<u>ष्ण्ठी ७ ।</u>	
ucloud windows HPC pack	• Tier	ent2_portal01_F	Private_tier \$	
로그 히스토리	분산 배치 대상 선택(옵션)	분산 배치 대상 선택	<u>하기</u>	
API key SSH keypair	* 생생할 서비 수	1	(2대이상 생성 시 동일그룹에 지정한 서버명, 호스트명에 일린번호 주	가)
	* 그름명	♀그룹 미 적용		
		○기존 그룹 선택	•	
		○새로운 그룹 생성		중비확인
			*서버명, 호스트명, 그룹명은 영문, 숫자, *-* 문자로 63자 까지 입력 가 단, 첫 글자는 영문, 마지막 글자는 영문, 숫자만 입력 가능합니다.	8합니다.

VM을 생성할 tier를 선택하여 VM을 생성합니다. tier는 계정 전용의 가상 네트워크입니다.

포탈상으로는 기본적으로 두 개의 tier(DMZ, private)를 제공하며, 2개 이상의 tier 생성을 원할 때에는 컨설팅 담 당자에게 별도의 요청을 주시기 바랍니다.

DMZ tier의 IP 대역은 172.16.0.0/24, Private tier는 172.16.1.0/24 입니다. 실제 VM에 할당되는 IP 범위는 .6~.180 입니다.

VM을 생성한 후, 서버리스트에서 생성된 VM의 상세 정보를 확인하면, 내부주소 항목에 선택한 tier 대역의 IP가 설정 된 것을 확인 할 수 있습니다.(고정 IP)

글다우.	드 서버리스트 👓 🕫	라인문의 🛅 매뉴업				 ucloud server 	/ 클라우드 세버리스
이용 중인 클라우:	E 시비 리스트를 확인할 수 있으며, 시비 정보 !	전경 및 상태를 컨트롤 할 수 있	습니다.				
시바영성	위치 > KOR-Seoul M2 〇 · 항육엔깅	? Q				Action	역설저장
	√ালাপ্ত ♦	茶祥 	위치 🕈	상대 Φ	£প্রথায় ♦	스펙수	口田中
	edutestPRIV	王委	KOR-Seoul M2	사용	centos64-64-161228	1 vCore, 1 GB	
	edutest0MZ	표준	KOR-Seoul M2	● 사용	centos65-64-161228	1 vCore, 1 GB	
√ 선택된 서비 :	edutestPRV						
[╱] ॳॺॾॳॺः 상세정보	■ edusesPRV 서버 모니터링						
✓ 선택된 서비 : 상세정보 · 서비영	edutestPRV 서버 모니터링 edutestPRV 신번호범			J¥₽¢	172.16.1.56 efresh	모드 모위일 살림	
✓ 선택된 서비: 상세정보 · 시비명 · 시비D	edutestPRV 서버 모니터링 edutestPRV 신비호명 01a36897-3a56-4596-697	1 3-c8ed1a1b52es		내부주소 운영지제	172.16.1.56 efresh centos44-64-161228	포트 포위당 성정	

D VM의 외부 DNS 사용을 위한 방화벽 설정

VM을 생성한 후, 외부 DNS를 사용하기 위해서는 방화벽 설정이 필요합니다. 네트워크 메뉴에서 방화벽 정책을 추가할 수 있습니다. 외부 DNS IP는 /etc/resolv.conf 에서 확인 가능합니다.

Source Network에 원하는 tier 네트워크를 선택하고, UDP프로토콜과 Destination Network에는 DNS IP 대역 (168.126.63.0/24)을 입력합니다. 해당 방화벽 정책을 추가하면 외부 DNS 사용이 가능해집니다.

D VM의 인터넷 접속

Enterprise의 VM들은 기본적으로 인바운드, 아웃바운드 트래픽이 차단되어 있습니다. 따라서 같은 tier내에 있는 VM들은 서로 통신할 수는 있지만, 기본적으로 외부와의 연결이 차단되어 인터넷에 접속할 수는 없습니다. 또한 tier간 통신도 차단되어 있습니다. 네트워크 리스트에서 보여지는 SRCNAT type의 IP가 VM에서 인터넷 접근을 위하여 사용되는 source NAT IP인 데, 이에 대한 설정 방법은 3.6에서 설명합니다.

ㅁ IP 추가 신청

VM에서 인터넷 접근을 위한 SRCNAT type의 공인 IP외에, 추가적인 공인 IP를 할당 받아 사용할 수 있습니다. 기본적으로 공인 IP는 31개를 제공하며, 기본 SRCNAT용 1개를 제외하고 고객이 추가로 30개를 사용할 수 있습 니다.

네트워	📑 🖸 පිස්තිසික් 🖻 ශ්ල 🖬	- ucloud server / I	4693/ <u>46933</u> 22		
신형 네트워크 IPI	를 관리할 수 있으며, Cloud Internal Path를 성	성하고 관리할 수 있습니다.			
네트워크 리스트	Tier 가상IP CIP-Hybrid VPN				
IP 추가 신형	위치 > KOR-Secul M2 Q : 영	बलब : C		,	Action 역설자장
	공인만◆	유(지) 문	ТуреФ	Static NAT Ø	기분IP 🕈
	211.252.82.225	KOR-Seoul M2	PORTFORWARDING		YES
	211.252.82.224	KOR-Seoul M2	SRCNAT		YES
	211.252.82.226	KOR-Seoul M2	ASSOCIATE		YES

네트워크 메뉴에서 'IP 추가 신청'이라는 빨간 버튼을 클릭하면 뜨는 팝업 창에서 확인을 클릭합니다. 생성된 공 인 IP는 목록에서 조회 가능하며, 아직 사용 중이지 않은 상태로 type은 ACCOCIATE 상태 입니다.

1.4.2 외부에서 VM 접속 방법

ㅁ 포트포워딩

외부 -> DMZ/Private tier 연결 구성



네트워크 리스트 중에 VM 접속을 위해 사용할 공인 IP를 선택하고 '포트포워딩' 탭을 조회 합니다.

기존 할당 받은 SRCNAT IP 주소를 사용하거나, 또는 IP 추가 신청을 통해 공인 IP를 받을 수 있습니다.

	321	ΡΦ	引入 Φ	Туре Ф	Static NAT Ø 71世纪 Ø
	211.252	82.226	KOR-Seoul M2	ASSOCIATE	- YES
√ 선택된 네트워크	211.252	82.226			
상세정보	방화벽	포트포워딩			
· 포트포워딩 추가					泰7/約2
	પ્રામ		28 I.I.	사설 포트	프로토콜
cloudDMZ			22 · 22	22 · 22	TCP \$

포트포워딩에 사용할 IP를 선택 후에, 포트포워딩 탭에서 외부로부터 접속하려는 서버를 선택하고, 접속 정보를 입력합니다.

[중요] 포트포워딩 추가 시, 해당 포트포워딩에 대한 방화벽 정책이 자동으로 설정되지 않기 때문에(모두 DENY 상태) 3.5 장을 통해 별도의 방화벽 허용(ALLOW) 정책을 추가해야 합니다.

ㅁ 방화벽 정책 설정

방화벽 self 서비스를 사용하시는 경우에는, 포탈 콘솔을 이용하여 고객이 직접 방화벽 정책을 설정할 수 있으며, 바로 적용 된 것을 확인할 수 있습니다. 그러나 보안 매니지드 서비스를 받으시는 경우에는, 보안 매니지드사로 설정을 요청해야 합니다.

포트포워딩 설정 후, 해당 공인 IP의 방화벽 허용 정책을 추가해야 합니다. '방화벽' 탭에서 설정 가능합니다.

상세정보	방화벽 포트	포워딩					
- 방화벽 추가							추가하기
Action	Source Network	Source IP	프로도랑	Destination Network	Destination IP	Start Port	End Port
Allow 0	external 0		ALL	ent2_portal01_Private_ti 8	PortForwarding_211.2	52.82.225_TCP_	22

Source network를 external로 설정하고, Source IP에는 네트워크 대역을 입력합니다. Source IP를 공란으로 둘 경우 ANY로 입력 됩니다.

Destination Network를 선택합니다. 원하는 프로토콜을 선택하며, 여기에서는 TCP 로 선택하였습니다.

Destination IP 목록에서, 포트포워딩 설정한 IP가 표시되는 것을 확인할 수 있습니다. 해당 포트포워딩 구성을 선택하고 '추가하기'를 누릅니다.

포트포워딩 설정에 대한 방화벽 허용 정책이 추가 되어, 외부에서 VM으로의 접근이 가능합니다.

특정 Port를 지정하여 정책 적용 시 Start Port와 End Port는 포트포워딩 된 서버의 Port를 입력하여 주시면 됩니다. 공인 IP의 Port가 아닌 사설 IP의 port를 입력합니다.

ex) start port = 8080, end port = 8082

영화역 리스트										
Priority No	Action	Source Network	Source IP	Protocol	Destination Network	Destinantion IP	Start Port	End Port	ধম দ্ব	015
1	allow	ent2_portal01_Private_tier	all	ALL	external	all			018	48
2	allow	external	all	ALL	ent2_portal01_Private_tie	PortForwarding_211.252.82.225_TCP_22			015	412

1.4.3 VM에서 외부 접속 방법

ㅁ 방화벽 정책 설정

생성한 VM 에서 인터넷 접근을 하기 위해서는 방화벽 정책을 허용해 주어야합니다.

DMZ/Private tier → 외부 연결 설정



아래 ucloud server의 메뉴 중 네트워크 항목을 조회하면, 특정 IP의 TYPE이 SRCNAT로 설정되어 있는 것을 확 인할 수 있습니다.

ucloud server	네트워	네트워크 전 RANDER 전 Res						
· 플라우드 세미리스트(3)	신청 네트워크 (P	를 관리할 수 있으며, Cloud Internal Path를 영	성하고 관리할 수 있습니다.					
- Disk[4)	네트워크 리스트	Tier 7Hal IP CIP-Hybrid VPN						
· 네트웨크(2) - 스냅보/0(0(3)(2)	IP 추가 신청	위치 > KOR-Secul M2 Q : 왕기	बलब ? O			Action 역행저장		
· 네트워크 트라믹 들게		금인무◆	9(3) Φ	ТуреФ	Static NAT 0	7)원(문•		
 ucloud backup(0) 		211 252 82 224	WOR-Secul M2	SRENAT		YES		
· ucloud packaging		211.252.82.226	KOR-Seoul M2	ASSOCIATE		YES		
 ucloud autoscaling 								
· ucloud windows HPC pack								
· 보그 히스토리	√ 선택된 네트용	13 211.252.82.224						
- API key	상세정보	방화벽 포트포워	5					

네트워크 리스트에서 방화벽 탭을 선택합니다.

인터넷 접근을 가능하게 할 tier대역을 선택하고 Destination Network를 external(외부)로 선택하고 '추가하기'를 클릭합니다. 해당 방화벽 설정을 통해 해당 tier의 VM은 인터넷에 접근할 수 있습니다.

아래의 예제는 프로토콜-TCP만 허용한 예제이며, 필요에 따라 ICMP, UDP, TCP, ALL 로 지정 가능합니다.

	공인IPΦ		위치 Φ	Type	0	Static NAT	rθ	기본IP 0
~	211.252.82.224		KOR-Seoul M2	SRCN	AT			YES
	211.252.82.226		KOR-Seoul M2	ASSOC	IATE			YES
 ✓ 선택된 네트워 상세정보 - 방화비추가 	³ 211.252.82.224 방화벽 포트:	포워딩						⊼ - ⊻ 추가하기
Action	Source Netowrk	Source IP	프로토콜	Destination Net	owrk	Destination IP	Start Port	End Port
Allow \$	ent2_portal01_DMZ_tier \$		TCP	\$ external	•			
• 방화벽 리스트								

1.4.4 Tier 이용 방법

□ Tier 추가 생성

Tier는 L2 가상 네트워크로 기본으로 제공하는 2개의 Tier 네트워크를 포함하여 총 15개의 Tier를 생성할 수 있습니다.

네트워크 🗆 8러인문의 🗈 배뉴일 · ucloud server / 네트워크 /									
신청 네트워크 IP	신청 네트워크 IP를 견리할 수 있으며, Cloud Internal Path를 생성하고 관리할 수 있습니다.								
네트워크 리스트	네트워크리스트 Tier 가상 IP CIP-Hybrid VPN								
Tier 생성	위치 > KOR-Seoul M2 〇 항목변경	? I Q			Action > 역설저장				
	이름 Φ	위치호	VLAN Ø	CIDR Ø	생성일 🏼				
	ent2_portal01_DMZ_tier	KOR-Seoul M2	2044	172.16.0.0/24	06/23/2017 02:10				
	ent2_portal01_Private_tier	KOR-Seoul M2	2045	172.16.1.0/24	06/23/2017 02:10				
	lbtest_tier3	KOR-Seoul M2	2074	172.16.2.0/24	07/30/2017 13:16				
	aa_tier4	KOR-Seoul M2	2119	172.16.3.0/24	08/30/2017 13:57				
	ent_ent2_portal01_jinsu12_tier7	KOR-Seoul M2	1	172.16.6.0/24	0				
	177916_jin12_tier6	KOR-Seoul M2	2124	172.16.8.0/24	08/30/2017 19:22				
	177916_jin31_tier7	KOR-Seoul M2	2125	172.16.9.0/24	08/31/2017 09:36				

ucloud server – 네트워크의 상위 항목 중 Tier 탭에서 Tier를 관리할 수 있습니다.

네트워크 ☆ 온라인문의 집 매뉴얼 · ucloud server /네트워크 / ፲년						
현황 테드워크 IF를 한테일 두 있으며, Cloud Internal Pa						
네트워크리스트 <u>Tier</u> 가상 IP CIP-Hybrid	VPN					
Tier 생성 위치 > KOR-Seoul M2 Q 이 항	목변경 ? 이			Action > 역셾저장		
이름 令	위치�	VLAN \$	CIDR 🗢	생성일¢		
ent2_portal01_DMZ_tier	KOR-Seoul M2	2044	172.16.0.0/24	06/23/2017 02:10		
_{ent} Tier 생성			172.16.1.0/24	06/23/2017 02:10		
			172.16.2.0/24	07/30/2017 13:16		
Availability Zone	KOR-Seoul M2		172.16.3.0/24	08/30/2017 13:57		
ent_er . 이름]		172.16.6.0/24			
* 입력하신 이름뒤(계 "_tier" + 총 갯수가 추가되	어 생성됩니다.	172.16.8.0/24	08/30/2017 19:22		
· IP4정			172.16.9.0/24	08/31/2017 09:36		
- Super CIDR: 1	72.16.0.0/16					
	c 100					
- IP range :172.16	6 ~ 180					
디스드늘 선택애주세요.						
취소		확인				

Tier 생성을 클릭하면 Tier를 생성하기 위한 팝업창에 이름과 설정할 IP를 입력할 수 있습니다. 확인을 누르면 Tier가 생성됩니다.

며 서로 다른 Tier 간 통신

DMZ ← → Private tier 연결 설정



tier간의 통신은 간단한 방화벽 정책 설정으로 가능합니다. 아래와 같이 source network와 destination network 로 원하는 tier의 네트워크를 선택합니다. 그 밖의 항목은 역시 공란으로 둘 경우 ANY로 입력 됩니다.

상세정보	방화벽 포	트포워딩						
• 영화백 추가								추가하기
Action	Source Netowrk	Source IP	프로토콜		Destination Netowrk	Destination IP	Start Port	End Port
Allow \$	ent2_portai01_Private_ti	•	TCP	+	ent2_portal01_DMZ_tier \$			

마 방화벽 정책 우선순위 설정

방화벽 정책들의 우선순위를 설정하여 보다 효율적으로 네트워크 자원들을 관리할 수 있습니다.

포탈 콘솔에서 방화벽 탭을 조회하면, 방화벽 정책들을 우선순위 순으로 조회 가능합니다. 방화벽 정책은 기본 적으로 DENY로 설정 됩니다.

두 tier내 VM들의 방화벽 정책을 예로 들겠습니다.

아래와 같이 방화벽을 설정하면 DMZ VM □ Private VM 방향으로 11~8090 port까지 TCP 통신이 가능합니다.

Priority No.	Action	Source Network	Source IP	Protocol	Destination Network	Destinantion IP	Start Port	End Port	44192.018
1	allow	ent2_portal01_DMZ_tier	al	КМР	ent2_portal01_Private_tie	al			গদ্র ধ্য
2	allow	esternal	al	TCP	ent2_portal01_0M7_tier	PortForwarding_211.252.82.226_TCP_22			গম্ভ : ধ্যম
3	aliew	ent2_portal01_DM2_tier	al	TCP	ent2_portal01_Private_tier	al.	11	8090	918 A[4]
4	alow	ent2_portal01_DMZ_tier	al .	ALL	external	al.			415 444
5	allow	external	al	ALL	ent2_portal01_DMZ_tier	211.252.82.230_temp			이동 석제

여기에 700~800 port의 TCP 통신을 Deny 하는 방화벽 정책을 설정하였습니다.

 영화학 리스트 	2019 ALT										
Priority No	Action	Source Network	Source IP	Protocol	Destination Network	Destinantion IP	Start Port	End Port	석제 및 이동		
1	allow	ent2_portal01_DM2_tier	al	KMP	ent2_portal01_Private_tier				পম্ব গ্ৰহ		
2	allow	external	all	TOP	ent2_portal01_0MZ_tier	PortForwarding_211.252.82.226_TOP_22			গন্থ ধ্য		
3	allow	ent2_portal01_DMZ_tier	al	TCP	ent2_portal01_Private_tier	al	11	8090	পদ্র ব্যয		
4	allow	eet2_portal01_DM2_tier	al	ALL	esternal	at			গম নাম		
5	allow	external	al	ALL	ent2_portal01_0M2_tier	211.252.82.230_temp			ণন্দ্র ধ্যম		
6	deny	ent2_portal01_DMZ_tier	al	TCP	ent2_portal01_Private_tier	al	700	800	이동 : 석제		

Deny 정책의 우선순위가 가장 낮기 때문에(3번의 allow 정책보다 낮음) 700~800 port의 TCP 통신은 여전히 가 능한 상태입니다.

오른쪽 '이동'을 클릭하고, 3번의 allow 정책보다 높은 우선순위로 deny 정책을 이동할 수 있습니다.

Deny 정책의 우선순위가 높아져, 이 때에는 설정한 700~800port의 TCP 통신이 차단됩니다.

방화벽 정책을 보다 효율적으로 설정하기 위해서는, 구체적이고 범위가 좁은 rule을 우선순위가 높게 설정하고, 더 넓은 범위의 allow/deny 정책 rule을 우선순위가 낮게 설정하는 것을 권고합니다.

1.4.5 로드밸런서 이용 방법

D Enterprise Security 로드밸런서 서비스 구조

로드밸런서는 트래픽에 대한 분산처리를 합니다. Enterprise Security의 로드밸런서는 일반형과 다른 구조를 가 지고 있습니다.

로드밸런서는 서버와 같은 사설 네트워크(L2)에 위치하고, IPS와 NAT/FW내부인 Trust구간에 위치한 보안 강화 구조입니다.



ㅁ 서비스 설정

서버 구성 후 로드밸런서 메뉴에서 부하분산을 위한 설정을 할 수 있습니다.

1) 로드밸런서 신청 (메뉴 : 로드밸런서 - 로드밸런서 리스트)

로드밸런서 구성에 필요한 IP(신규/기존)/포트, 로드밸런서 타입(프로토콜), 로드밸런서 옵션(메소드), Health Check,

그리고 적용 서버를 등록할 수 있습니다.

(상세 설정값 구성은 일반 로드밸런서와 동일하며, '네트워크-Load Balancer 사용자 가이드'에서 확인 하실 수 있습니다)

_ 	모드밸런,	서 신청 ⊠ 온라인문의 茴 매뉴얼	
	로드밸런서 적용 서	버등록	
	Availability Zone	KOR-Seoul M2	
	Tier	ent2_portal01_DMZ_tier	
	로드밸런서명	중복검사	
		- 로드밸런서명은 영문, 숫자, 특수문자(, -, -, @,, #,, =, :)만 입력 가능합니다. - 로드밸런서명은 최대 32자 이상 입력하실수 없습니다.	
	서비스 IP / PORT	신규할당 IP ▼	
	로드밸런서 타입	●HTTP OTCP OHTTPS(bridge) OHTTPS OFTP	
	로드밸런서 옵션	Round robin Src IP Hash Least Response Least connection Src IP Hash+Port	
	Health Check	Protocol TCP Path	
	-	서버 Public Port	
	dnstest (dnstest)	· · · · · · · · · · · · · · · · · · ·	
	<u>3</u> 취소 신청		

2) Static NAT 설정 : 외부 통신이 필요한 경우에만 설정 (메뉴 : ucloudserver - 네트워크)

로드밸런서 신청 후 VIP(로드밸런서 IP)는 해당 Tier 사설 네트워크에서 정해진 범위에서 할당됩니다.

Tier네트워크내에서의 부하분산과 Tier네트워크간 부하분산에서는 Static NAT는 불필요하며(이경우 방화벽 허용 정책은 필요합니다),

웹서버와 같이 외부에서 접속을 위한 공인 구간 접속을 위해서 Static NAT작업이 필요합니다.

네트워크 메뉴에서 'IP 추가 신청'을 통해 <ASSOCIATE: IP추가 후 미사용 상태> 상태 인 공인IP만 가능합니다.

네트워크 🛛	>~ 온라인문의 📑 메뉴얼		· ucloud server/네트워크/ 네트워크리스트					
신청 네트워크 IP를 관리할 수	신청네트워크 IP를 관리할 수 있으며, Cloud Internal Path를 생성하고 관리할 수 있습니다.							
네트워크리스트 Tier 7	가상 IP CIP-Hybrid VPN							
IP 추가 신청 IP I	IP 추가 신청 IP PCOL 추가 신청 위치 > KOR-Seoul M2 Q : 항목변경 : ? : Q Action : 역설저							
	공인마수	위치◆	Type⇔					
	211.252.82.231	KOR-Seoul M2	ASSOCIATE					

<ASSOCIATE>상태의 공인IP 선택 후 'Action'버튼으로 로드밸런서를 외부 연동이 되도록 설정할 수 있습니다.

Static NAT 설정	102 201			
●서버선택 ●Load Balancer	skim∨mFromGi TESTM20831b	roupImg3		•
취소			확인	

이후 일반 서버와 같이 방화벽에서 'Static NAT'를 설정한 IP에 대한 허용 정책을 설정하면 서비스를 위한 준비 가 완료됩니다.

1.6 Enterprise security 기타 가이드

1.6.1 방화벽 정책 self 가이드

며 복수개의 방화벽 정책 설정

Source IP, Destination IP, 프로토콜 3개 항목에 대해서 복수개 입력이 가능합니다. (Source Network, Destination Network는 정책상 복수개 불가능)

- 복수개 입력 시 ,(콤마) 로 구분하여 수동 입력
- 프로토콜 입력의 경우는 단일 입력, 복수개 입력 text가 다릅니다.(TCP,UDP만 다르며, 나머지는 동일합니다) ex) 단일 입력 : TCP, UDP
 - 복수개 입력 : ALL_TCP, ALL_UDP



방화벽 정책 예시) Source IP : 172.16.0.1, 172.16.0.2 프로토콜 : ALL_TCP, ALL_UDP Destination IP : 10.10.2.3, 10.10.2.10, 10.10.2.15