사용하기 전에

Q. 네이버 클라우드 플랫폼의 Secure Zone Firewall 서비스는 무엇인가요?

- Secure Zone 내 생성한 인스턴스로의 접근에 방화벽 정책을 설정해 접근을 제어할 수 있는 기능을 제공합니다.
 Q. Secure Zone Firewall 는 어떻게 이용하나요?
- Secure Zone 이용약관 동의
- Secure Zone Fiewall 이용 신청
- Cloud Log Analytics 이용 신청 및 로그 저장소 연동
- Secure Zone VM 생성
- Secure Zone Policy 생성/Address Group 생성
- Secure Zone Firewall Network Usage 조회
- Secure Zone Firewall Log 조회
 Q. Secure Zone Firewall 서비스를 사용하지 않으면 Secure Zone VM 에 접근할 수 없나요?
- Secure Zone 내부 간을 제외한 외부 통신은 모두 차단되어 있습니다.
- 일반 Zone 또는 SSL VPN 과 Secure Zone 간에 Secure Zone Firewall 에 Policy 를 생성하여 통신 허용 정책을 생성해야 Secure Zone VM 에 접근이 가능합니다.
 Q. Secure Zone VM 에 접근 정책을 설정할 수 있는 Zone 은 어디인가요?
- SSL VPN 으로 인입되는 트래픽과 Secure zone 을 제외한 Ncloud 의 모든 Zone 간의 사설 접근입니다.
 Q. Policy 가 뭔가요?
- 정의된 Source IP 와 Destination IP 간에 특정 프로토콜 및 포트에 대한 통신을 허용하거나 차단하는 보안 정책입니다. Q. Address Group 이 뭔가요?
- 고객이 소유한 VM 을 원하는 그룹으로 묶어서 정책에서 사용할 수 있도록 하는 오브젝트입니다.
 Q. Log 는 뭔가요?
- Secure Zone Firewall 방화벽 정책에 따라 Secure Zone 의 접속 시도가 기록된 Traffic Log 입니다. Cloud Log Analytics 상품에서도 검색/조회가 가능합니다.
 Q. Excel 파일로 다운로드할 수 있나요?
- 검색 결과를 Excel 파일로 다운로드할 수 있습니다.
- 단, 전체 데이터가 아니라 검색 결과 화면에 보이는 내용만 다운로드할 수 있습니다.

Secure Zone Firewall 서비스 사용하기

Secure Zone Firewall 서비스 이용 신청

① 콘솔에 접속 후, Security > Secure Zone > Secure Zone Firewall 을 클릭합니다.

Console NAVER CLOUD PLATFORM	Secure Zone / Secure Zone Firewall / Policy
S Region 한국 / KR 한국어 ▼	Ø Secure Zone Eirewall
Dashboard	Secure Zone Filewan
My Products 🧿 EDIT — 碩 Network Traffic Monitoring 👓 +	Secure Zone 에 위지한 상비에 내한 접근 관리 개인정보 보호를 위한 보안 강화 구역 접근 관리 정해진 Source 와 Destination 서버에 필요한 포트와 프로토콜을 허용합니다.
	Stateful Inspection 기능을 제공합니다.
R Object Storage + & Cloud Search * +	+ 상품 이용 신경 상품 더 알아보기 간 ^
Belasticsearch Service +	
Secure Zone - Secure Zone Firewall	
Policy Address Group	
Log Network Usage Subscription	0

② Secure Zone Firewall 하위 메뉴 중 Policy 를 클릭합니다.

③ + 이용신청 버튼을 클릭합니다.

Clo	로그연동을 위해 Cloud Log Analytic(Cl ud Log Analytic(CLA) 상품을 미사용 중인 경	L A) 상품연동이 필수입니다. 경우, 해당 상품이 동시에 가입됩니다.
		(●필수 입력 사항입니다.
로그 저장소 연동 ®	Cloud Log Analytics(CLA)	상품 알아보기 []
	Cloud Log Analytic(CLA)는 네이버 로그를 손쉽게 저장하고 분석 데이터를	f 클라우드 플랫폼의 상품을 이용하면서 발생하는 다양한 를 제공하는 시스템입니다.
로그저장은 별도 이용요금이	발생되며 CLA의 과긍정책을 따릅니다.	
	× 취소 🗸 🗸	용 신청

• 기존 Cloud Log Analytics 가입자에게는 이 팝업 창이 노출되지 않습니다.

* 로그연동을 위해 Cloud Log Analytic(CLA) 상품가입이 필수입니다.

Secure Zone Firewall Traffic log 에 대한 저장 및 조회는 Cloud Log Analytics(CLA) 서비스 에서 제공합니다. CLA 서비스를 처음 이용하는 고객은 아래의 이용 신청 버튼을 클릭하여 서비스를 신청해주세요.

Secure Zone Firewall 가입 후 Policy 생성이 완료되면 Traffic log 발생 시 CLA 에 자동 저장되 고, Secure Zone Firewall 및 CLA 에서 로그를 조회할 수 있습니다.

저장되는 로그에 대해 CLA 정책에 따른 요금이 부과됩니다.

× 취소 ✓ Cloud Log Analytics 이용신청

⑤ Cloud Log Analytics 이용신청 버튼을 클릭하여 Cloud Log Analytics 서비스에 가입합니다.

알림		×
	Cloud Log Analytics(CLA) 이용 신청이 완료되었습니다. 확인	
알림		×
	Secure zone Firewall 이용 신청이 완료되었습니다. 확인	

• 미가입 상태일 때 Policy, Address Group, Network Usage 메뉴 선택 시 Secure Zone Firewall 이용 신청 페이지로 이동합니다.

Policy 설정

Policy 생성

Console NAVER CLOUD PLATFORM	Secure Zone / Secure Zone Firewall / Policy Policy		🔎 द 🖻 🗊 🌒 🔻
🛞 Region 한국 / KR 한국어 🗸 ▼	+ Policy 생성 ● 이용 설정 ▼ 상품 더 알아보기 亿	ᅟ	
⊖ Dashboard	Policy 삭제 🔗 스 🗸 😵 💽 Default De	eny 로깅 ⑦	20 개씩 보기 🔹
Products & Services +	Name Source IP	Destination IP	Protocol Port Action
My Products 🕦 EDIT —	test ob-stch.beta-cdb.ntruss.com	m ▼ mysql-vm(10.39.2.22) ▼	IP Allow
Secure Zone		« < 1 > »	
Secure Zone Firewall —			
Policy			
Address Group			
Log			
Network Usage			
Subscription			

① Security > Secure Zone > Secure Zone Firewall > Policy 에서 + Policy 생성 버튼을 클릭합니다.

	• 필수 입력 사항 • 경우에 따라 필	입니다. 수 입력 사항입니다.
Name *	Policy_01	
Description	Secure zone FW Rule 1	
Source IP *	Source	•
	vm-ejk02 (10.39.4.215) dmz-ejk01 (10.39.4.217)	× ×
Destination IP *	Destination	•
	sz-windows (10.39.16.74) sz-cubrid (10.39.16.77) sz-mysql01 (10.39.16.80)	× × ×
Protocol ®		
Port ®	80, 200-300, 1	
Action •	• Allow Deny	

- Name: Policy 이름
- Description: Policy 설명
- Source IP: 고객 소유의 VM / 사설 LB / SSL VPN
- Destination IP: 고객 소유의 VM
- Protocol: TCP / UDP / ICMP
- Port: destination port (0 ~ 65,535)
- Action: Allow / Deny

Source IP 와 Destination IP 중 하나는 Secure Zone 필수입니다.

② 필수 값을 입력한 후 [저장] 버튼을 클릭하여 Policy 를 생성합니다.

Policy 변경

Secure Zone / Secure Zone Firewall / Po Policy 2	licy	G 자주하는 ·	질문 🖻 .	알림 Policy 설정이 저장도	었습니다.	×
+ Policy 생성 이용 설정 ▼	상품 더 알아보기 [건 🛛 🗶 다운로드 📿	€ 새로고침 ∨				
Policy 삭제 🔗 ^ 🗸	➢ Default Deny 로깅 ⑦				20 개씩 보기	•
Name	Source IP	Destination IP	Protocol	Port	Action	
Policy_R	sz-windows(10.39.16.74), sz-cubrid(10.39	vm-ejk02(10.39.4.215), dmz-ejk01(10.39.4	TCP	10001	Allow	
Policy_01	vm-ejk02(10.39.4.215), dmz-ejk01(10.39.4	sz-windows(10.39.16.74), sz-cubrid(10.39	TCP	80, 200-300, 1	Allow	

① Security > Secure Zone > Secure Zone Firewall > Policy 에서 변경하고자 하는 Policy 의 Name 을 클릭합니다.

		● 필수 입력 사항입니다. ●경우에 따라 필수 입력 사항입니다.	
Name *	Policy_R		
Description	100자 이내		
Source IP •	Source		•
	sz-windows (10.39.16.74) sz-cubrid (10.39.16.77) sz-mysql01 (10.39.16.80)		× × ×
Destination IP •	Destination vm-ejk02 (10.39.4.215) dmz-ejk01 (10.39.4.217)	, , ,	• ×
Protocol *			
Port [•]	10001		
Action •	O Allow O Deny		

② 변경하고자 하는 값을 넣어 수정 후 저장을 클릭하여 Policy를 변경합니다.

Secure Zone / Secure Zone Firewall / Policy

-

D I!

Policy 0						
+ Policy 생성 이용 설정 ▼	상품 더 알아보기 🖸 🗶 다운로드 📿	새로고침 🗸				
Policy 삭제 🔗 🔨 🗸	≫ Default Deny 로깅 ⑦				20 개씩 보기	•
Name	Source IP	Destination IP	Protocol	Port	Action	
All_Rule	vm_all	8 sz_group	UDP	9000	Allow	
Policy_Modify	sz-windows(10.39.16.74), sz-cubrid(10.39	vm-ejk02(10.39.4.215), dmz-ejk01(10.39.4	TCP	10001	Allow	
Policy_01	vm-ejk02(10.39.4.215), dmz-ejk01(10.39.4	sz-windows(10.39.16.74), sz-cubrid(10.39	TCP	80, 200-300, 1	Allow	
		≪ < 1 > ≫				

③ Policy 우선순위를 수정하기 위해 Policy 하나를 선택하여 순서변경 버튼으로 우선순위를 조정합니다.

Policy 삭제

Secure Zone / Secure Zone Firewall / Policy 3	Policy	다 자주하는 질	실문 🖻 문의하기	[] 사용자가이드	<u>옷</u> NBP 님 ▼
+ Policy 생성 이용 설정 ▼	ㆍ 상품 더 알아보기 ☑ 🗶 다운로드 📿	새로고침 🗸			
Policy 삭제 🔗 🔨	✓ 🛛 👻 🚺 Default Deny 로깅 ⊘				20 개씩 보기 🛛 🔻
Name	Source IP	Destination IP	Protocol	Port	Action
All_Rule	Source IP	Destination IP	Protocol UDP	Port 9000	Action
Name All_Rule Policy_Modify	Source IP wm_all sz-windows(10.39.16.74), sz-cubrid(10.39	Destination IP (sz.group) vm-ejk02(10.39.4.215), dmz-ejk01(10.39.4	Protocol UDP TCP	Port 9000 10001	Action Allow Allow
Name All_Rule Policy_Modify Policy_01	Source IP vm_all sz-windows(10.39.16.74), sz-cubrid(10.39 vm-ejk02(10.39.4.215), dmz-ejk01(10.39.4	Destination IP sz.group vm-ejk02(10.39.4.215), dmz-ejk01(10.39.4 sz-windows(10.39.16.74), sz-cubrid(10.39	Protocol UDP TCP TCP	Port 9000 10001 80, 200-300, 1	Action Allow Allow Allow

Security > Secure Zone > Secure Zone Firewall > Policy 에서 삭제하고자 하는 Policy 의 콤보박스를 다중 선택 후 Policy 삭제 버튼을 클릭하여 삭제합니다.

	●필수 ●경우	입력 사항입니다. 에 따라 필수 입력 사항입니다.
Name *	Policy_R	
Description	100자 이내	
Source IP *	Source	•
	sz-windows (10.39.16.74) sz-cubrid (10.39.16.77) sz-mysql01 (10.39.16.80)	>
Destination IP •	Destination	•
	vm-ejk02 (10.39.4.215) dmz-ejk01 (10.39.4.217)	>
Protocol *		
Port [●]	10001	
Action *	• Allow Deny	

② Security > Secure Zone > Secure Zone Firewall > Policy 에서 삭제하고자 하는 Policy 의 Name 을 클릭한 후 [삭제] 버튼을 클릭합니다.

Default Deny 정책 로그 활성화/비활성화

기본적으로 방화벽에 정책 설정을 하지 않으면 All Deny 입니다. 아무 정책이 없어서 트래픽이 차단되는 경우 Default 정책에 의해 차단되고 로그가 남는데, 허용되지 않은 접속 시도가 많은 경우 Log Size 가 많이 증가하여 Cloud Log Analytics 저장소 용량을 많이 차지할 수 있습니다.

① Default Deny 로깅을 활성화/비활성화하여 Default Deny 정책에 해당하는 로그를 남기거나 남지 않도록 설정할 수 있습니다.

Default: 활성화(로그를 남김)



Address Group 설정

Address Group 생성



① Security > Secure Zone > Secure Zone Firewall > Address Group 에서 + Address Group 생성 버튼을 클릭합니다.

Address Group 생	성	×
	●필수 입력 사항입니다.	
Name •	sz_db_group	
Description	100자 이내	
Address •	Address	
	Secure Zone sz-windows (10.39.16.74) sz-cubrid (10.39.16.77) sz-mysql01 (10.39.16.80)	
	취소 🗸 저장	

② Address 를 다중 선택하고 [저장] 버튼을 클릭하여 Address Group 을 생성합니다.

Address Group 변경

Secure Zone / Secure Zone Fire	wall / Address Group		🕞 자주하는 질문	🖻 문의하기	🗊 사용자가이드	<u> 오</u> NBP 님	•
Address Group	0						
+ Address Group 생성	이용 설정 ▼ 상품 더 알0	바보기 IZ X 다운	로드 📿 새로고침 🗸				
Address Group 삭제						20 개씩 보기	•
Name	Member Count	Address		Desc	ription		
vm_all	2	vm-ejk02 (10.39.4.21	5), dmz-ejk01 (10.39.4.217)	•			
		« <	1 > >				

① Security > Secure Zone > Secure Zone Firewall > Address Group 에서 변경하고자 하는 Address Group 의 Name 을 클릭합니다.

		●필수 입력 사항입니다.
Name •	vm_all	
Description	100자 이내	
Address *	Address	•
	vm-ejk02 (10.39.4.215) dmz-ejk01 (10.39.4.217)	××
	취소 🛛 🗙 색제 🔍 저장	

② 변경하고자 하는 값을 넣어 수정 후 [저장] 버튼을 클릭하여 Address Group 을 변경합니다.

Address Group 삭제

Secure Zone /	Secure Zone Firewall / Addre	iss Group		🖓 자주하는 질문	🖻 문의하기	① 사용자가이드	<u>오</u> NBP 님	•
+ Addre	ss Group 생성 이용 설정	▼ 상품 더 알아보기 [2]	X 다운로드 C 새로고침 ∨					
Address G	roup 삭제					2	20 개씩 보기	•
	Name	Member Count	Address		Description			
	sz_all	3	sz-windows (10.39.16.74), sz-cubrid (10.39.16.77), sz-m	nysql01 (10 🔻				
	sz_db_group	2	sz-cubrid (10.39.16.77), sz-mysql01 (10.39.16.80)	•				
	vm_all	2	vm-ejk02 (10.39.4.215), dmz-ejk01 (10.39.4.217)	•				
	sz_group	3	sz-windows (10.39.16.74), sz-cubrid (10.39.16.77), sz-m	nysql01 (10 🔻				
			« < 1 > »					

① Security > Secure Zone > Secure Zone Firewall > Address Group 에서 삭제하고자 하는 Address Group 을 다중 선택한 수 Address Group 삭제버튼을 클릭합니다.

알림		×
A	ddress Group 을 삭제하시겠습니까?	
	vm_all	
	× 취소 🗸 확인	

② 삭제 대상 Address Group 체크한 후 확인 버튼을 클릭하여 삭제합니다.

Network Usage 조회

Secure Zone / Secure Zone Firewall / Network Usage	🕞 자주하는 질문	🖻 문의하기	🗊 사용자가이드	<mark>요 NBP</mark> 님	•	
Network Usage						
이용 설정 ▼ 상품 더 알아보기 [2] 🗶 다운로드 📿 새	로고침 🗸					
기간 선택 2018-02-07 📾 ~ 2018-02-08 📾 Sea	rch					
	시간대별 Traffic 2,154 Mbps 2,154					
2154	·					
	21					
	2018-02-08					
				60 개4	식보기 ▼	
일자 시	121	Traffic Pe	ak			
2018-02-08 22	1	2154 Mbp	S			
	≪ < 1 > ≫					

① Security > Secure Zone > Secure Zone Firewall > Network Usage 에서 시간대별 peak 트래픽 사용량을 조회합니다.

• 원하는 기간을 선택하여 조회할 수 있습니다.(최대 기간 설정: 1개월)

	Log 조회	
	이용 설정 ▼ 상품 더 알아보기 [2] 🗶 다운로드 📿 새로고침 >	
	Source IP Description IP Action 전체 ▼ Protocol TCP ▼ Port 20 개씩 보기 ▼	
	Receive Time 2018-03-26 11:54:36 ~ 2018-03-27 11:54:36 亩 Q Search Obfault Deny 로깅 @	Ð
	Receive Time Source IP Destination IP Protocol Port Action Policy	
•	Receive Time: 날짜 범위로 검색 가능(보관 주기 및 사이즈는 Cloud Log Analytics 상품 정책에 따름)	
•	Source IP: 고객 소유의 VM / 사설 LB / SSL VPN	
•	Destination IP: 고객 소유의 VM	
•	Protocol: TCP / UDP / ICMP	
•	Port: destination port 검색 (0 ~ 65,535)	
•	Action	
	accept: for the end of non-TCP traffic // non-TCP 의 경우(icmp, udp tcp 를 제외한) 통과를 의미, deny: for traffic blocked by a firewall policy // 정책에 의한 Block close: for the end of TCP session closed with a FIN/FIN-ACK/RST // Allow 를 의미하며, FIN or RST 에 의한 정상 종료 imeout: for the end of a TCP session which is closed because it was idle. // Allow 는 되었지만 timeout 값에 의해 결국은 Block 경우, TCP SYN 은 보냈지만 remote 에서 응답이 없는 경우에도 남음 p-conn: for IP connection failed for the session (host is not reachable) // Allow 는 되었지만 fortigate 가 어떤 reply packet 을 받기 못해 종료된 경우. ICMP request 는 있으나 reply 는 없음, UDP request 있으나 reply 없을 때 Policy: 해당 Log 가 히트된 Policy 명	된 기
	OBS 실정 ▼ Star of good J I I I I I I I I I I I I I I I I I I	Ð
	Secure Zone VM 장비 IP를 ACG에 등록	

• Secure zone 과 일반 zone 의 접근 제어를 Secure Zone Firewall 정책으로 통제하기 위해서는 각각의 VM 및 SSL VPN 을 동일한 ACG 설정 및 아래와 같은 규칙을 등록해야 합니다.(필수)

프로토콜	접근 소스	허용 포트(서비스)	메모
TCP	acggroup2(405)	1-65535	
UDP	acggroup2(405)	1-65535	
ICMP	acggroup2(405)		

Secure Zone Firewall 권한 Sub Account 적용

Sub Account 권한 상세

관리자와 사용자 권한으로 분류되고 다음과 같은 권한이 부여됩니다.

- NCP_SECURE_ZONE_FIREWALL_MANAGER
- Secure Zone Firewall 상품 내 오브젝트 조회 및 Policy, Address Group 생성/삭제/변경 권한을 가집니다.
- NCP_SECURE_ZONE_FIREWALL_VIEWER
- Secure Zone Firewall 상품 내 오브젝트 조회 권한을 가집니다.

Secure Zone Firewall 관리자 권한 부여하기

① 특정 사용자에게 Secure Zone Firewall 권한을 부여하기 위해서는 먼저 Sub Accounts 서비스를 선택합니다.

NAVER CLOUD PLATFORM	Sub Account / Sub Accounts
중 Region 한국 / KR 한국어 ▼ II All Products * + 슈 Dashboard	ุ Sub Account
My Products ② EDIT — Ø Secure Zone + ⊟ Server +	Sub Account는 서브 계정을 생성, 관리하고, 접근 권한을 제어하는 플랫폼입니다. ④ Region 통합 서비스 Sub Account를 이용해 네이버 클라우드 플랫폼의 서비스를 이용할 수 있는 서브 계정을 생성하고 서브 계정이 활용할 수 있는 상품과 권한을 관리할 수 있습니다. 서브 계정은 별도의 접속 페이지를 통해 네이버 클라우드 플랫폼에 로그인하며, 부여된 권한 안에서 상품의 기능을 사용합니다. 고객 계정 의 정보를 공유하지 않아도 서버 관리자, 개발자 등 역할에 맞는 서브 계정을 생성하고 권한을 부여해 협력 시스템을 구축할 수 있습니다.
Recently Viewed 親 Sub Account 一	 ✓ 네이버 클라우드 플랫폼의 리소스를 정책별로 세분화해 제어 ✓ 그룹 기능으로 복수의 서브 계정에 동일한 역할을 부여 ✓ API Gateway의 접근 제어와 통합
Dashboard Sub Accounts Groups Policies	11선안내 [Sub Account] 신규 정책 추가 안내 더보기 + 서브 계정 생성 상품 더 알아보기 리
행 KMS* 값 Load Balancer 행 SSL VPN 금 Cloud DB for MySQL	

② Secure Zone Firewall 권한을 부여하고자 하는 서브 계정을 선택합니다.

Sub Account / Sub Accounts				兄 🖻 🖬	•
< 서브 계정 상세					
수정 삭제 일시 정	IA 일시 정지 해지				
서브 계정 정보					
로그인 아이디	securezonefw_admin	사용자 이름 이메일	securezonefw_admin		
생성 일시	2018-05-04 15:27:17	최종 접속 일시			
접근 유형	Console Access	로그인 비밀번호	○ 비밀번호 재설정		
메모					
정책 그룹 이벤트	로그				
추가 삭제			정책 이름 ▼	검색	۹
정책 이름 🔶	정책 설명	정책 유형 ≑ 권한	허용 여부 적용대상		
		조회된 데이터가 없습니다.			

정책 추기	ŀ					×
				정책 이름 ▼	검색 Q 20개씩 보	기 🔻
	정책 이름 🔶	정책 설명	정책 유형 👙	권한 허용 여부	적용대상	
	NCP_MONITORING_MANAGER	모니터링 관리자	SYSTEM_MANAGED	 Allow 	Console, Monitoring	\sim
	NCP_NTM_VIEWER	Network Traffic Monitoring 뷰어	SYSTEM_MANAGED	 Allow 	Console, NetworkTrafficMonitoring	\sim
	NCP_SECURE_ZONE_FIREWALL _MANAGER	Secure Zone Firewall 관리자	SYSTEM_MANAGED	 Allow 	Console, SecureZone	~
	NCP_SECURE_ZONE_FIREWALL _VIEWER	Secure Zone Firewall 사용자	SYSTEM_MANAGED	 Allow 	Console, SecureZone	~
	NCP_SERVER_MANAGER	서버 관리자	SYSTEM_MANAGED	 Allow 	Server, Console, LoadBalancer, Aut oScaling	~
	NCP_SERVER_OBSERVER	서버 관찰자	SYSTEM_MANAGED	 Allow 	Server, Console	\sim
	NCP_SOURCE_COMMIT_MANA GER	SourceCommit 관리자	SYSTEM_MANAGED	 Allow 	Console, SourceCommit	~
		<	K < 1 > »			
		×	취소 🗸 추가			

④ 선택된 서브 계정의 정책에서 NCP_SECURE_ZONE_FIREWALL_MANAGER 정책 또는 NCP_SECURE_ZONE_FIREWALL_VIEWER 중 부여하고자 하는 정책을 선택하여 해당 권한을 추가합니다.

Secure Zone Firewall Advanced 업그레이드하기

Secure Zone Firewall Advanced 업그레이드 신청

① Security > Secure Zone > Secure Zone Firewall 가입된 상태에서 "이용 설정"을 클릭합니다.

Secure Zone / Secure Zone Firewall / Policy

Ø



Secure Zone Firewall

Secure Zone 에 위치한 장비에 대한 접근 관리

개인정보 보호를 위한 보안 강화 구역 접근 관리 정해진 Source 와 Destination 서버에 필요한 포트와 프로토콜을 허용합니다. Stateful Inspection 기능을 제공합니다.



Secure Zone Firewall Advanced Upgrade	×
업그레이드 상품을 이용하려면 Private Subnet 상품 연동이 필수 입니다.	
(●필수 입력 사항입니다.)	
 Private Subnet (사용중) 상품 알아보기 ☑ Advanced 로 Upgrade 하려면 Secure Zone VM 과 일반 Zone VM 및 IPSec VPN 을 연동 하는 Private Subnet 상품을 사용하여 정책 및 오브젝트를 관리해야 합니다. 	
× 취소	

Advanced 업그레이드 상품을 이용하려면 Private Subnet 상품 가입이 필수 입니다.
 ③ Advanced 로 업그레이드가 완료되면 Private Subnet 탭이 생깁니다.

Secure Zone Firewall Description of the second sec	Ø	
Secure Zone of 위치한 장비에 대한 접근 관리 개인정보 보호를 위한 보안 강화 구역 접근 관리 정례진 Source 와 Destination 서비에 필요한 포트와 프로토콜을 허용합니다. tateful Inspection 기능을 제공합니다. • Policy 생성 • 이용 성정 • 상품 더 알아보기 덥 값 다운로드 ⓒ 새로그형 andard Private Subnet 面研 생성된 Policy가 없습니다. Example Add U 바른을 클릭하여 Policy 생성을 요청하세요.	Secur	e Zone Firewall
개인정보 보호를 위한 보안 강화 구역 접근 관리 정혜진 Source 와 Destination 서버에 필요한 포트와 프로토콜을 허용합니다. Stateful Inspection 기능을 제공합니다. ▲ Policy 생성 ● 이용 설정 ▼ 상품 더 알아보기 [2]	Secure Zone 에 위	비치한 장비에 대한 접근 관리
andand Private Subnet Private Subnet @ 전쟁 생성된 Policy가 없습니다. Policy 생성] 비득을 클릭하여 Policy 생성을 요청하세요	개인정보 보호를 위한 전체진 Source 와 De	보안 강화 구역 접근 관리 stination 서버에 필요한 프로토와 프로토콜은 청용한테다
+ Policy 생성 ● 이용 설정 ▼ 상품 더 알아보기 [2] X 다운로드 ○ 새로고침 ▲ andand Private Subnet ● É ● ● ● DAT 생성된 Policy가 없습니다. ● ● ● Policy 생성! 버튼을 클릭하여 Policy 생성을 요청하세요. ● ●	장해전 Source 또 De Stateful Inspection	기능을 제공합니다.
tandand Private Subnet 한재 생성된 Policy가 없습니다. [Policy 생성] 버튼을 클릭하여 Policy 생성을 요청하세요.	+ Policy 생성	● 이용 설정 ▼ 상품 더 알아보기 [2]
한 현재 생성된 Policy가 없습니다. [Policy 생성] 버튼을 클릭하여 Policy 생성을 요청하세요.	andand Private Sul	net
● 현재 생성된 Policy가 없습니다. [Policy 생성] 버튼을 클릭하여 Policy 생성을 요청하세요.		
♥ 현재 생성된 Policy가 없습니다.		
현새 생성된 Policy가 없습니다. [Policy 생성] 버튼을 클릭하여 Policy 생성을 요청하세요.		
		현새 생성된 Policy가 없습니다. [Policy 생성] 버튼을 클릭하여 Policy 생성을 요청하세요.

• Policy / Address Grou / Log 메뉴에서 Private Subnet 탭 선택 후 Advanced 기능을 이용합니다.

Policy 설정 - Advanced

Policy 생성

Ø
Secure Zone Firewall

Secure Zone 에 위치한 장비에 대한 접근 관리

개인정보 보호를 위한 보안 강화 구역 접근 관리 정해진 Source 와 Destination 서버에 필요한 포트와 프로토콜을 허용합니다. Stateful Inspection 기능을 제공합니다.

+	Policy 생성	● 이용 설정 ▼	상품 더 알아보기 🖸	✗ 다운로드	∂ 새로고침	^	
Standand	Private Sub	onet					
				0			
			현재 생	성된 Policy가 없습	니다.		
			[Policy 생성] 버튼을	클릭하여 Policy 실	생성을 요청하세요.		

① Security > Secure Zone > Secure Zone Firewall > Policy > Private Subnet 에서 + Policy 생성 버튼을 클릭합니다.

	• 웹수 입력 사항입니다. • 경우에 따라 필수 입력 사항입니
Name •	30 자 이내 영문, 숫자 , "_"의 특수문자만 입력 가능
Description	100자 이내
Source IP •	Source
	1111
Destination IP •	VM mysql-vm (192.168.150.111) esese (192.168.150.113)
Destination IP *	VM mysql-vm (192.168.150.111) esese (192.168.150.113) TCP UDP ICMP
Destination IP • Protocol • Port •	VM mysql-vm (192.168.150.111) esese (192.168.150.113) TCP UDP ICMP IP

- Name: Policy 이름
- Description: Policy 설명
- Source IP: IPSec VPN (고객 직접 입력) / Private Subnet Network Interface 할당된 고객 소유 VM
- Destination IP: Private Subnet Network Interface 할당된 고객 소유 VM
- Protocol: TCP / UDP / ICMP
- Port: destination port (0 ~ 65,535)
- Action: Allow / Deny
- Source IP 와 Destination IP 중 하나는 Secure Zone 필수입니다.

Policy 변경

Policy **1**

+ Policy 생성 ● 이용 설정 ▼ 상품 더 알아보기 X 다운로드 C 새로고침 ✓ Standand Private Subnet 20 개씩 보기 ▼ Policy 삭제 Default Deny 로깅 ⑦ 20 개씩 보기 ▼								
Name	Source IP		Destination IP		Protocol	Port		Action
Policy_PrivateSu	mysql-vm(192.168.150.111)	• S	ejk-kr1-sz(192.168.150.112)	•	TCP	80, 443	•	Allow

① Security > Secure Zone > Secure Zone Firewall > Policy > Private Subnet 에서 변경하고자 하는 Policy 의 Name 을 클릭합니다.

Policy 변경 - Privat	e Subnet	×
	●필수 입력 사항입니다. ●경우에 따라 필수 입력 사항입니다	
Name •	Policy_PrivateSubnet	
Description	100자 이내	
Source IP *	Source	
	mysql-vm (192.168.150.111) ×	
Destination IP •	Destination	
	ejk-kr1-sz (192.168.150.112) ×	
Protocol •		
Port *	80, 443	
Action •	• Accept Deny	
	취소 × 삭제 🗸 저장	

② 변경하고자 하는 값을 넣어 수정 후 저장을 클릭하여 Policy를 변경합니다.

Policy O									
+ Policy 생성 ● 이용 설정	▼ 상품 더 알아보기 亿 🗙	다운희	은 새로고침 🗸						
Standand Private Subnet									
Policy 식제 🖹 < A 🗸 😵 🌑 Default Deny 로깅 🝸							20 개씩	보기 🔻	
Name	Source IP		Destination IP		Protocol	Port		Action	
Permit_Rule	mysql-vm(192.168.150.111) 🔻	•	ejk-kr1-sz(192.168.150.112)	,	TCP	3306	•	Allow	
PrivateSubnetPoli 💿	ejk-kr1-sz(192.168.150.112) 🔻		mysql-vm(192.168.150.111)	,	IP			Allow	
Policy_PrivateSu	mysql-vm(192.168.150.111) 🔻	5	ejk-kr1-sz(192.168.150.112)	,	TCP	80, 443	•	Allow	
		« <	1 > >						

③ Policy 우선순위를 수정하기 위해 Policy 하나를 선택하여 순서변경 버튼으로 우선순위를 조정합니다.

Policy	3
--------	---

Standand Private Subnet	✓	0			20 개씩	보기
Name	Source IP	Destination IP	Protocol	Port		Action
Permit_Rule	mysql-vm(192.168.150.111) 🔻	sik-kr1-sz(192.168.150.112) ▼	TCP	3306	•	Allow
PrivateSubnetPoli	s ejk-kr1-sz(192.168.150.112)	mysql-vm(192.168.150.111) 🔻	IP			Allow
Policy_PrivateSu	mysql-vm(192.168.150.111) 🔻	s ejk-kr1-sz(192.168.150.112) 🔻	TCP	80, 443	•	Allow
		-,,				

1 Security > Secure Zone > Secure Zone Firewall > Policy > Private Subnet 에서 삭제하고자 하는 Policy 의 콤보박스를 다중 선택 후 Policy 삭제 버튼을 클릭하여 삭제합니다.

Policy 변경	경 - Private S	Subnet	×
		● 필수 입력 사항입니다. ●경우에 따라 필수 입력 사항입니다	
Name •		Policy_PrivateSubnet	
Descrip	tion	100자 이내	
Source	IP •	Source 🗸	
		mysql-vm (192.168.150.111) ×	
Destina	tion IP •	Destination <	
		ejk-kr1-sz (192.168.150.112) ×	
Protoco	ol •		
Port *		80, 443	
Action [•]	•	O Accept O Deny	
		취소 🛛 🗙 삭제 🗸 저장	

② Security > Secure Zone > Secure Zone Firewall > Policy > Private Subnet 에서 삭제하고자 하는 Policy 의 Name을 클릭한 후 [삭제] 버튼을 클릭합니다.

Default Deny 정책 로그 활성화/비활성화

기본적으로 방화벽에 정책 설정을 하지 않으면 All Deny 입니다. 아무 정책이 없어서 트래픽이 차단되는 경우 Default 정책에 의해 차단되고 로그가 남는데, 허용되지 않은 접속 시도가 많은 경우 Log Size 가 많이 증가하여 Cloud Log Analytics 저장소 용량을 많이 차지할 수 있습니다.

① Default Deny 로깅을 활성화/비활성화하여 Default Deny 정책에 해당하는 로그를 남기거나 남지 않도록 설정할 수 있습니다.

Default: 활성화(로그를 남김)

Policy **3**

+ Policy 생성 ● 이용 실정 ◆ 상품 더 알아보기 [2] 값 대문로드 값 새로고침 Standand Private Subnet Policy 삭제 ^ ▲ ✓ Default Deny 로깅 ⑦ 20 개씩 보기 ✓							
Name	Source IP	Destination IP	Protocol	Port		Action	
Permit_Rule	mysql-vm(192.168.150.111) 🔻	s ejk-kr1-sz(192.168.150.112)	тср	3306	•	Allow	
PrivateSubnetPoli s	ejk-kr1-sz(192.168.150.112) 🔻	mysql-vm(192.168.150.111)	• IP			Allow	
Policy_PrivateSu	mysql-vm(192.168.150.111) 🔻	ejk-kr1-sz(192.168.150.112)	тср	80, 443	•	Allow	
	<	≪ < 1 > ≫					

Address Group 설정 - Advanced

Address Group 생성

Ø

Secure Zone Firewall

Secure Zone 에 위치한 장비에 대한 접근 관리

개인정보 보호를 위한 보안 강화 구역 접근 관리 정해진 Source 와 Destination 서버에 필요한 포트와 프로토콜을 허용합니다. Stateful Inspection 기능을 제공합니다.





① Security > Secure Zone > Secure Zone Firewall > Address Group > Private Subnet 에서 + Address Group 생성 버튼을 클릭합니다.

Address Group 생성		×
	• 필수 입력 사항입니다.	
Name •	vm_ps_group	
Description	100자 이내	
Address •	Address	
	Private Subnet (Secure Zone)	
	ejk-kr1-sz(192.168.150.112)	
	Private Subnet (VM)	
	mysql-vm(192.168.150.111)	
	63636(192.100.130.113)	
	취소 🗸 저장	

② Address 를 다중 선택하고 [저장] 버튼을 클릭하여 Address Group 을 생성합니다.

Address Gro	oup 변경				
Address Group	0				
+ Address Group 생성	● 상품 이용 중 ▼	상품 더 알아보기 🖸	X 다운로드 📿 새로고칭	빌 ~	
Standand Private Sub	net				
Address Group 삭제					20 개씩 보기 🛛 🔻
Name	Member Count	Address		Description	
vm_ps_group	2	mysql-vm (192.168.1	50.111) , esese (192.168.150.1	13) 🔻	
		« <	1 > >		

① Security > Secure Zone > Secure Zone Firewall > Address Group > Private Subnet 에서 변경하고자 하는 Address Group 의 Name 을 클릭합니다.

Address Group 변	3	×
	●필수 입력 사항입니	
Name *	vm_ps_group	
Description	100자 이내	
Address •	Address	•
	mysql-vm(192.168.150.111) esese(192.168.150.113)	×
	취소 🛛 🗙 삭제 🔷 저장	

② 변경하고자 하는 값을 넣어 수정 후 [저장] 버튼을 클릭하여 Address Group 을 변경합니다.

Address Group 삭제

Addres	ss Group 🏾	1						
+ Addre	ss Group 생성 🛛 ●	상품 이용 중 ▼	상품 더 알아보기 🖸	X 다운로드	€ 새로고침 ∨			
Standand	Private Subnet							
Address G	roup 삭제						20 개씩 보기	•
	Name	Member Count	Address			Description		
	vm_ps_group	2	mysql-vm (192.16	8.150.111) , esese (1	92.168.150.113) 🔻			
			« <	1 > >				

① Security > Secure Zone > Secure Zone Firewall > Address Group > Private Subnet 에서 삭제하고자 하는 Address Group 을 다중 선택한 수 Address Group 삭제버튼을 클릭합니다.

Address Group 변경		×
		●필수 입력 사항입니다.
Name •	vm_ps_group	
Description	100자 이내	
Address •	Address	•
	mysql-vm(192.168.150.111) esese(192.168.150.113)	××
	최소 > 산제 > 기자	

② Security > Secure Zone > Secure Zone Firewall > Address Group > Private Subnet 에서 삭제하고자 하는 Address Group 의 Name 을 클릭한 후 [삭제] 버튼을 클릭합니다.

Network Usage 조회

ecure Zone / Secure Zone Firewall / Network Usage		다 자주히	·는 질문 🖻 문의하기	기 🔲 사용자가이드	<mark>요 NBP</mark> 님	•
letwork Usage						
이용 설정 ▼ 상품 더 알아보기 [2] 🗶 다운로드 📿	7 새로고침 🗸					
간 선택 2018-02-07 📾 ~ 2018-02-08 📾	Search					
	<mark>시간</mark> 대 2,154	(별 Traffic Mbps 2, 154				
2154		•				
		21				
	2018	3-02-08				
				60.7#	씩 보기 ▼	
일자 2018-02-08	21		7154 Mbps			
	2.		2101 mopo			

① Security > Secure Zone > Secure Zone Firewall > Network Usage 에서 시간대별 peak 트래픽 사용량을 조회합니다.

• 원하는 기간을 선택하여 조회할 수 있습니다.(최대 기간 설정: 1개월)

Log 조회

Secure Zone > Secure Zone Firewall > Log > Private Subnet 탭에서 Private Subnet Traffic Log 확인

.og 💿	
● 상품 이용 중 ▼ 상품 더 알아보기	I [2] X 다운로드 ♂ 새로고침 ~
Standand Private Subnet	
Source IP Source IP	▼ Destination IP Destination IP ▼ Action 전체 ▼ Obfault Deny 로깅 ⑦
Protocol 전체 🔻 Port	Receive Time 2019-06-18 18:12:33 ~ 2019-06-19 18:12:33 ᇔ Q Search 20 개씩 보기

- Receive Time: 날짜 범위로 검색 가능(보관 주기 및 사이즈는 Cloud Log Analytics 상품 정책에 따름)
- Source IP: 고객 소유의 VM / 사설 LB / SSL VPN
- Destination IP: 고객 소유의 VM
- Protocol: TCP / UDP / ICMP
- Port: destination port 검색 (0 ~ 65,535)
- Action
- accept: for the end of non-TCP traffic // non-TCP 의 경우(icmp, udp.... tcp 를 제외한) 통과를 의미,
- o deny: for traffic blocked by a firewall policy // 정책에 의한 Block
- close: for the end of TCP session closed with a FIN/FIN-ACK/RST // Allow 를 의미하며, FIN or RST 에 의한 정상 종료
- o timeout: for the end of a TCP session which is closed because it was idle. // Allow 는 되었지만 timeout 값에 의해 결국은 Block 된 경우, TCP SYN 은 보냈지만 remote 에서 응답이 없는 경우에도 남음
- ip-conn: for IP connection failed for the session (host is not reachable) // Allow 는 되었지만 fortigate 가 어떤 reply packet 을 받지
 못해 종료된 경우. ICMP request 는 있으나 reply 는 없음, UDP request 있으나 reply 없을 때
- Policy: 해당 Log 가 히트된 Policy 명
- Default Deny 정책 로그 활성화/비활성화

Log 🧿

 ● 상품 이용 중 ▼ ◆ 상품 더 알아보기 	☑ 🗶 다운로드 📿 새로고침 ∨	
Standand Private Subnet		
Source IP Source IP	▼ Destination IP Destination IP ▼ Action 전체 ▼	Default Deny 로깅 ⑦

Secure Zone Firewall 이용 해지

Secure Zone Firewall Advanced 해지

① Security > Secure Zone > Secure Zone Firewall > Advanced 가입된 상태에서 "Advanced 이용해지"를 클릭합니다.

Ø **Secure Zone Firewall**

Secure Zone 에 위치한 장비에 대한 접근 관리

개인정보 보호를 위한 보안 강화 구역 접근 관리 정해진 Source 와 Destination 서버에 필요한 포트와 프로토콜을 허용합니다. Stateful Inspection 기능을 제공합니다.

+ Policy 생성	● 이용 설정 ▼ 상품 더 알아	보기 🖸 🗙 다운로드	€ 새로고침 ^			
	Advanced 이용 해지					
Standand Private	Subnet					
0						
현재 생성된 Policy가 없습니다. [Policy 생성] 버튼을 클릭하여 Policy 생성을 요청하세요.						

Advanced 상품이 해지되고 Standard 상품 가입은 유지됩니다. ② Security > Secure Zone > Secure Zone Firewall Advanced 상품이 가입되지 않은 상태에서 "이용해지"를 클릭합니다.

Secure Zone / Secure Zone Firewall / Policy



Ø

Secure Zone Firewall

Secure Zone 에 위치한 장비에 대한 접근 관리

개인정보 보호를 위한 보안 강화 구역 접근 관리 정해진 Source 와 Destination 서버에 필요한 포트와 프로토콜을 허용합니다. Stateful Inspection 기능을 제공합니다.

