사용하기 전에

Q. SSL VPN 이란 무엇인가요?

- VPN은 가상 사설망(Virtual Private Network)의 약자로, 외부에서 접근할 수 없는 사설망에 내 PC 나 네트워크를 연결시키는 방법을 말합니다.
- 사설망과의 연결은 가상 터널을 통해 이루어지며, 이 가상 터널을 SSL 암호화로 보호하는 것이 SSL VPN 입니다.
- 가상 터널을 통해 사설망과 연결된 사용자 PC는 사설망의 라우팅 및 ACL 정책에 따라 내부 서버에 접근할 수 있습니다.
- SSL VPN 서비스는 외부에서 네이버 클라우드 플랫폼 내부에 구성된 고객의 네트워크로 암호화된 보안 접속 통신을 제공하는 서비스입니다.
- SSL VPN 환경이 구축되어 있으면, 언제 어디서든 외부에서 도/감청 위협없이 내부 네트워크로 접근을 할 수 있습니다.
 Q. SSL VPN 서비스 사용 절차는 어떻게 되나요?
- 콘솔에 접속한 후에 다음 단계를 통해 간단하게 신청한 후 바로 사용할 수 있습니다.
- 1. 콘솔 접속: 네이버 클라우드 플랫폼 콘솔에 접속합니다.

Q. 네이버 클라우드 플랫폼의 SSL VPN 서비스는 무엇인가요?

- 2. SSL VPN 서비스 설정: SSL VPN 에 외부 접속을 허용할 최대 ID 수, 인증방식, VPN 아이디 정보를 등록합니다. VPN 아이디는 최대 10 개까지 등록할 수 있습니다.
- 3. SSL VPN 서비스 신청: SSL VPN 서비스를 신청합니다. 서비스 신청 즉시 이용이 가능합니다.
- 4. 클라이언트 설치: 네이버 클라우드 플랫폼 자료실에서 SSL VPN Agent 를 다운로드하여 외부 접속용 PC에 설치합니다.
- 접속: 외부 접속용 PC에 설치된 Agent 를 실행한 후 등록된 VPN 아이디를 이용해 접속합니다.
 Q. SSL VPN 에 접속하면 모든 접속은 내부 네트워크를 경유하게 되나요?
- SSL VPN 은 분할 터널링(Split Tunneling)을 지원하여 내부 사설망으로 향하는 접속에 대해서만 VPN 터널링을 수행합니다.
- 내부 사설망으로 향하지 않는 접속(인터넷 접속, 타 네트워크로의 접속 등)은 기존과 같이 사용자 PC 의 라우팅을 따릅니다.
 Q. SSL VPN 를 콘솔에서 생성했더니 SSL VPN IP pool 이라는 게 보이는데 이게 뭔가요?
- SSL VPN 은 가상의 터널을 통해 사용자의 PC 와 대상 네트워크를 연결하는 서비스로, SSL VPN IP pool 은 대상 네트워크로부터 사용자 PC 가 부여받는 IP 주소입니다.
- 사용자 PC는 28 비트의 네트워크 대역에서 비어있는 IP 주소를 자동으로 할당받습니다.
- 사용자 PC는 대상 VM에 접속할 때 해당 SSL VPN IP 주소를 사용하기 때문에, 사용자는 미리 ACG에 해당 SSL VPN IP pool을 허용 처리해 두어야 합니다.
 Q. 사용자 계정 수는 뭔가요?
- 사용자는 SSL VPN 생성 시 최대 3/5/10개의 VPN 아이디를 생성할 수 있는 상품을 선택할 수 있습니다.
- 이후 선택한 개수 내에서 자유롭게 VPN 아이디를 생성/삭제할 수 있으며, 사용자 계정 수는 이 내용을 보여주는 항목입니다.
- 예를 들어 '사용자 계정 수 (2/3)'와 같이 표기되어 있으면 사용자가 VPN 아이디 3개를 생성할 수 있는 상품을 선택했으며, 그 중 2개를 만들어 사용하고 있다는 의미입니다. 즉, 이 사용자는 1개의 VPN 아이디를 더 만들어서 사용할 수 있습니다. VPN 아이디가 더 필요한 경우, 추가로 SSL VPN 상품을 생성 후 사용하시면 됩니다.
 Q. 일차인증방식과 이차인증방식의 차이점은 뭔가요?
- SSL VPN 접속 시 인증하는 방식의 차이입니다.
- 일차인증은 ID/PW 만을 통해 인증받고 로그인할 수 있는 방식입니다.
- 이에 반해 이차인증는 MFA(Multi-Factor Authentication) 방식으로, ID/PW 를 통해 인증한 후에 OTP 를 통해 한 번 더 인증을 받아야 로그인할 수 있는 방식입니다.
- OTP 를 이용한 인증방식은 ID/PW 만을 이용한 인증방식보다 보안상 안전합니다.
- SSL VPN 의 OTP 는 사용자가 입력한 메일과 SMS 를 통해 전달됩니다.

SSL VPN 서비스 신청

Step 1. 콘솔 접속

NAVER CLOUD PLATFORM	SSL VPN
💌 한국 🗸 👻	
All Products*	
G Dashboard	SSL VPN
Bookmarks 🧿 EDIT —	
Recently Viewed	외부에서 네이버 클라우드 플랫폼 서버 접속 시 보안 통신을 제공
C SSL VPN	웹 기반의 콘솔에서 빠르고 손쉽게 접속 환경을 설정할 수 있고, 허가된 사용자는 언제 어디서든
⊟ Server +	기업 내 사설 네트워크에 보안 처리된 방식으로 안전하게 접속할 수 있습니다. < 안정적인 통신 품질 < 빠르고 편리한 사용 < 강화된 보안 장지 < 효율적인 비용 관리 2 + SSL VPN 생성 상품 더 알아보기 리 C 새로고침 ^
	아직 SSL VPN이 만들어지지 않았습니다. SSL VPN 생성 버튼을 클릭하여 SSL VPN을 생성하세요.

① 콘솔에 접속 후, Security > SSL VPN 을 클릭합니다.

② 왼쪽 상단 혹은 화면 중앙의 SSL VPN 생성을 클릭합니다.

• SSL VPN 은 필요에 따라서 2개 이상의 상품을 추가로 신청할 수 있습니다.

Step 2. 스펙 및 인증방식 선택

생성		×
	SSL VPN 를 생성합니다.	
1 상품선택 (등록가능 ID 수)	○ User ID 최대 3개 ○ User ID 최대 5개 ○ User ID 최대 10개	
2 인증방식	○ 이차인증 (ID/PW + OTP) ○ 일차인증 (ID/PW)	
3 OTP 전송 방식	SMS & Email SMS Email	
• 인증방식 및 OTP 전송 방식은 생성 후 변경을 할 수 없으니	신중하게 선택해 주세요 ★ 닫기 ✓ 적용	

① SSL VPN 생성 팝업 창이 열리면 먼저 생성 가능한 ID 수(3개/5개/10개)로 구분된 스펙을 선택합니다.

② VPN 서비스 인증방식에서 일차인증 또는 이차인증 인증을 선택합니다.

- 일차인증은 ID/PW 로 인증하는 방식입니다. 간단하지만 이차인증보다 보안성이 낮습니다.
 이차인증은 ID/PW 로 인증한 후 OTP 로 추가 인증하는 방식입니다. OTP 는 사용자 이메일 및 휴대전화번호로 전달됩니다.
 일차인증보다 보안성이 높습니다.
 - 단, 이차인증을 사용하려면 이메일 및 휴대전화번호 정보 수집을 위한 개인정보 활용에 동의해야 합니다.

• 인증방식은 SSL VPN 서비스 생성 후에는 변경할 수 없으므로 신중하게 선택해야 합니다.

(인증방식을 바꾸고 싶다면 SSL VPN 서비스 삭제 후 재생성합니다)

스펙은 **스펙 변경**을 클릭하여 언제든지 변경할 수 있습니다. 단, 스펙에 따라 요금이 변경되므로 본인에게 맞는 스펙을 선택해야 합니다.

③ 인증방식을 이차인증으로 사용하시는 경우 ID/PW 입력 이후 OTP 를 어떤 디바이스로 전송 받을지 결정합니다. SMS, Email을 선택할 수 있습니다.

④ 생성을 클릭하면 SSL VPN 상품 신청이 완료됩니다.

Step 3. 사용자 설정

인증방식에 따라 다음과 같이 사용자를 설정합니다.

일차인증

스페 병경 사용자 선정	1 				
SSL VPN IP pool	인증 방식	사용	용자 계정 수	메모	
1.1.1.0/28	일차인증	0/	3		^
	사용자 설정				×
SSL VPN IP pool	2				
인증 방식	-		SSL VPN 의 사용자	정보를 설정합니다.	
등록 가능 ID 수	Username	Password	Email	SMS	
등록 된 ID 수				한국 (+82) 🔻	+추가
생성 일시					
메모 수정					
			× 닫기	<u>√ र्व</u> 8	

• 이차인증

	1				
스펙 변경 사용자	· 설정 식제				
SSI VDN ID pool	이즈바	A	사용지 계정 수	NID	
SSE VEN IE pool	263		154 116 T	베포	
1.1.1.0/28	일자인*	6	0/3		~
2,2,2,0/28	이차인	중(SMS & Email)	0 / 5		~
3.3.3.0/28	이차인	중(SMS & Email)	1/3		^
	사용자 설정				×
SSL VPN IP pool	2		SSL VPN 의 사용자 ?	영보를 설정합니다.	
인증 방식					
등록 가능 ID 수	Username	Password	Email	SMS	
등록 된 ID 수				한국 (+82) 🔹	+추가
생성 일시					
메모 수정					
				8	
			× 닫기	✓ 적용	

① 설정할 상품을 선택한 후 사용자 설정을 클릭합니다.

② SSL VPN 을 사용할 사용자의 Username 및 부가 정보를 입력하고 추가를 클릭합니다.

- SSL VPN 생성 창에서 일차인증을 선택했다면 username, 비밀번호를 입력하고, 이차인증을 선택했다면 username, 비밀번호 외에도 메일 주소 및 휴대전화번호를 함께 입력합니다.
- 선택한 스펙에 따라 생성 가능한 username 개수도 달라집니다.
- 보안을 위해 비밀번호는 8자 이상이어야 하며, 영문자 소문자, 대문자, 특수문자, 숫자 중 3개 항목이 1자 이상씩 포함되어야 합니다.

③ 설정을 마쳤으면 적용을 클릭해 서비스에 반영합니다.

username 을 제외한 모든 설정은 수정 가능하며, username 의 추가/삭제 또한 사용자 설정에서 언제든지 가능합니다.

SSL VPN 서비스 변경

현재 선택된 스펙(등록 가능한 ID 수) 변경

Step 1. 콘솔 접속

스펙 변경 사용지	· 설정 삭제		
SSL VPN IP pool	인증 방식	사용자계정 수 메모	
1.1.1.0/28	일차인증	0/3	^
ſ	스펙 변경		×
SSL VPN IP po 인증 방식	2	SSL VPN 의 스팩을 변경합니다.	
등록 가능 ID 수 등록 된 ID 수 생성 일시	상품선택 (동록가능 ID 수) 인증방식	O User ID 최대 3개 ○ User ID 최대 5개 ○ User ID 최대 10개 일차인증	
메모 수정		× 닫기 <mark>~ 적용</mark>	

① 설정할 상품을 선택한 후 상단의 스펙 변경을 클릭합니다.

Step 2. 스펙 선택

② 변경할 스펙을 선택합니다. 현재 스펙보다 등록 가능 ID 수가 더 적은 스펙으로 변경하려면, 현재 등록된 ID 수가 변경할 스펙의 ID 수와 같거나 더 적어야 합니다.

③ 변경을 클릭합니다.

10개 이상의 ID가 필요할 때

10개 이상의 ID가 필요한 경우에는 SSL VPN 상품을 추가로 생성합니다.

등록한 ID의 정보 변경

Step 1. 콘솔 접속

SL VPN IP pool	인증 방식	사용자 계정 수	메모	
.1.1.0/28	일차인증	0/3		
.2.2.0/28	이차인증(SMS & Email)	0 / 5		
.3.3.0/28	이차인증(SMS & Email)	1/3		
인증 방식	이차인증(SM	vis & Email)		
인증 방식	이차인증(SI	/IS & Email)		
등록 가능 ID 수	3			
등록 된 ID 수	1			
생성 일시	2018-07-05	오후 1:10 (UTC+09:00)		

① 설정할 상품을 선택한 후 상단의 사용자 설정을 클릭합니다.

Step 2. 정보 변경

사용자 설정					×
		SSL VPN 의 사용자 정보를 설정합	니다.		
Username	Password	Email	SMS		
				+추가	
ncloudtest	*******	ncloudtest@naver.com	010-1234-5678	2 <mark>수정</mark> × 삭제	
		X 단기 🗸 저유			

② 변경하고 싶은 ID 오른쪽의 [수정] 버튼을 클릭한 후에 정보를 설정합니다.

×
+추가
1-2222 3 저장 취소

③ 저장을 클릭하면 정보가 저장됩니다. 변경한 정보을 저장하지 않으려면 취소를 클릭합니다.

④ 변경이 필요한 모든 ID의 정보를 저장한 후 하단의 적용을 클릭합니다.

인증방식 변경 _ 일차인증/이차인증

한 번 선택한 인증방식은 변경할 수 없습니다. 따라서 최초 SSL VPN 생성 시 인증방식을 신중하게 선택해야 합니다.

SSL VPN 서비스 삭제

스펙 변경 사용자 설정	<u>4</u> ম			
SSL VPN IP pool	인증 방식	사용자 계정 수	메모	
1.1.1.0/28	일차인증	0/3		~
2,2,2,	01#10177 (0110.0.5 V	N 015		~
3.3.3.			×	^
SSL 인증 등록 등록 컨 ID 구	선택된 SSL VPN 정 × 취소	보가 삭제됩니다. 2 ✓ 확인		
생성 일시	201	8-07-05 오후 1:10 (UTC+09:00)		
메모 수정				

① 삭제할 상품을 선택한 후 왼쪽 위의 SSL VPN 삭제를 클릭합니다.

② 경고 문구를 확인하고 확인을 클릭하면 선택한 SSL VPN 서비스가 삭제됩니다.

주의

SSL VPN 서비스를 삭제하면 해당 상품에서 등록한 모든 username 정보가 함께 삭제됩니다. 이 정보는 복구할 수 없으며, 다시 SSL VPN 서비스를 사용하려면 모든 정보를 다시 입력해야 합니다.

SSL VPN IP pool을 ACG에 등록하기

Step 1. SSL VPN IP pool 확인

스펙번경 사용자 설정 SSL VPI IP pool: 1.1.1.0 사용자계정 수 (1/3) 이쪽 박석: 01590를			
Username	Password	Email	SMS
ncloudtest	******	ncloudtest@naver.com	010-1234-5678

① SSL VPN 상품 상단에 표기된 SSL VPN IP pool을 확인합니다.

› 일반적으로 28 비트(16 개)의 IP 블록으로 할당되어 있습니다.

Step 2. 접속하고자 하는 VM의 ACG 확인

HH OLE (Instance ID)	netra dresses an(//2275)	4114 010171 017	centor 5 11-54
Viol ole (uprovice io)	ALTER	지마이미지이를	VD-4
Set	1000 1000	ZONE	
양양 될지	2017-09-19 22# 11:15	05	Lentus 5,11 (ownit)
구동 일시	2017-09-19 오후 11:15	Network Interface 제요 가는 여러	작용 불가
비공인IP			
담당자 EDIT	Account	공인 IP(Instance ID) ()	
모니터링 0	기본	서버스팩 💿	[Standard]2vCPU, 4GB Mern, 50GB Disk
민중키 이	ncioudman	포트 포워딩 정보 🗇	서버 접속용 공연 IP.: 49.236.160.23, 외부 포트 :
AEDIA 12	[HDD] onloudmannym 인 기본 스투리지 50 GB /dev.lovda	반납보호 🕜	8673
	A second s		acg-sslvpn
세모 EDIT			

② SSL VPN을 통해 접속하고자 하는 서버 VM에 어떤 ACG가 적용되어 있는지 확인합니다.

ACG 규칙 설정	형 acg-sslvpn			×
		ACG 에 적용된 상세 규칙을 표	시합니다.	
프로토콜	접근소스	허용 포트 (서비스)	메모	설정
	 ♥ ● (1) IP: 0.0.0.0/0, 192.168.1.0/24, 192.168.1.7 ● (12) ACG 이름: my-acg-1 ● Detail 	예1) 단일포트 : 22 예2) 범위지정 : 1-65535		추가
тср	1,1,1,0/28	3389	SSL VPN에 대해 윈도우 원격 접속 허용	삭제
тср	1,1,1,0/28	22	SSL VPN에 대해 ssh 접속 허용	삭제
ICMP	1,1,1,0/28		SSL VPN에 대해 ping 허용	삭제
허용할 프로	토콜 허용할 IP (SSL VPN IP pool)	허용할 포트		
• 변경사항이	아직 저장되지 않았습니다.	× 닫기 🗸 적	8	

Step 3. ACG에 등록

③ Server > ACG 메뉴에서 SSL VPN IP pool 을 등록합니다.

참고

접속 형태에 따라 아래 프로토콜 및 포트를 ACG 에 등록합니다.

- ping: ICMP 프로토콜 등록
- ssh: TCP 프로토콜의 포트 22 등록
- › 윈도우 원격 접속(RDP):TCP 프로토콜의 포트 3389 등록

SSL VPN Agent 설치

참고

다른 VPN 접속이 활성화되어 있는 상태에서는 다른 접속 환경과 충돌이 발생할 수 있으므로 VPN Agent 설치를 권장하지 않습니다.

Step 0. 네트워크 점검

SSL VPN의 원활한 사용을 위해 방화벽, NAC 등에서 sslvpn-kr-01.ncloud.com 의 443 포트로 접근이 허용되어 있는지 확인해 주세요. 접근이 허용되어 있지 않으면 Agent 설치 및 서비스 이용에 제약이 있을 수 있습니다.

Step 1. Agent 다운로드

① 설명서(Windows Agent, Mac OS Agent)에서 SSL VPN Agent 를 다운로드합니다.

Windows 사용자용 Agent 와 MAC 사용자용 Agent 가 구분되어 있습니다.

Step 2. Agent 설치

② 다운로드한 Agent를 설치합니다.

설치는 다음 그림과 같은 순서로 진행합니다.



闄 BIG-IP Edge Client Setup	×
Ready to Install The Setup Wizard is ready to begin the installation	Ð
Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.	
< Back Install Ca	ancel





SSL VPN Agent 접속

Step 1. Agent 실행

그램 (1)	
BIG-IP Edge Client	
₽ 자세한 결과 보기	
edge ×	시스템 종료 ▶

① 설치한 Agent(BIG-IP Edge Client)를 실행합니다.

설치 시와 마찬가지로, 타 VPN 연결이 활성화되어 있는 상태에서 Agent 실행은 권장하지 않습니다. 충돌의 가능성이 있습니다.

BIG-IP Edge Client	- X
■ CLOUD CL	수신 트래픽 0 b/s 송신 트래픽 2.7 Kb/s
연결 2	● 연결끊기
접속을 끊거나 자동접속 해재	
서버 변경	그래프 보기 상세 보기

Step 2. 접속

② 연결을 클릭하여 접속합니다.

Step 2-1. 옵션

BIG-IP Edge Client	
● CLOUD PLATFORM 서비: Ncloud-kr-01	수신 트래픽 0 b/s 송신 트래픽 2.7 Kb/s
연결	
<u>()</u> 연결	🧿 연결끊기
접속을 끊거나 자동접속 해재	
3 _{ин ёз} 4	그래프 보기 5 상세 보기

③ 서버 변경: 사용자가 Big-IP를 이용한 다른 SSL VPN 서비스를 사용하는 경우 이 버튼을 클릭하여 접속 경로를 변경할 수 있습니다.

④ 그래프 보기/숨기기: 트래픽 사용량을 볼 수 있습니다. 인증 후에도 열람 가능합니다.

⑤ 상세 보기: 해당 접속 경로의 세부 정보를 볼 수 있습니다. 인증 후에도 열람 가능합니다.

Step 3. 인증

Ncloud-kr-01 (https://sslvpn-kr-01.ncloud.com) - BIG-IP Edge Client	- O X
CLOUD PLATFORM	<u>^</u>
Naver Cloud Platform 6 ^아 로그온 VPN 아이디 Password	E
· · · · · · · · · · · · · · · · · · ·	
이 제품은 Naver Cloud Platform로부터 사용 허가를 받았습니다. © Naver Cloud Platform. All rights reserved.	-
	취소

⑥ ID 와 비밀번호를 입력해 인증받습니다.



인증방식으로 이차인증을 선택한 경우에 해당합니다.

ID 와 비밀번호를 입력하면 OTP 입력 창이 나타납니다. 잠시 기다린 후에 휴대전화번호 및 이메일로 전송된 OTP 를 입력합니다.

⑦ 인증에 성공하면 접속이 완료됩니다.

Step 4. 완료

그래프 보기,상세 보기 등을 클릭하면 더 자세한 정보를 확인할 수 있습니다.

SSL VPN Agent 접속 확인

네트워크 확인

콘솔 창을 실행합니다

- Windows 는 실행 창에서 cmd 입력
- macOS는 콘솔 app 실행

C:₩Users₩	>ping [VM IP]
Ping	4 IP] 32바이트 데이터 사용:
[VM IP]	의 응답: 바이트=32 시간=3ms TTL=60
[VM IP]	의 응답: 바이트=32 시간=3ms TTL=60
[VM IP]	의 응답: 바이트=32 시간=2ms TTL=60
[VM IP]	의 응답: 바이트=32 시간=5ms TTL=60
[VM IP]	에 대한 Ping 통계:
패킷: 보	보냄 = 4, 받음 = 4, 손실 = 0 (0% 손실),
왕복 시간<말	실리초):
최소 = :	2ms, 최대 = 5ms, 평균 = 3ms

① 현재 사용자의 IP 정보를 확인합니다.

- Windows 는 ipconfig 실행
- macOS 는 ifconfig 실행

② 사용자가 SSL VPN 생성 시 받은 IP pool에 포함된 IP 를 할당받았다면 정상적으로 접속이 완료된 것입니다.

ACG에 SSL VPN ip pool에 대한 규칙을 등록했다면 ping, ssh 등의 명령을 통해 해당 VM 과의 통신을 확인할 수 있습니다.

참고 사항

① SSL VPN 은 모든 글로벌 리전 서버로의 접속을 제공합니다.

- 한국 리전에서 SSL VPN 상품 가입 후 글로벌 리전 서버로 접속
 ② SSL VPN Agent 설치 및 접속 시 주의 사항
- SSL VPN 은 로그인 시뿐만 아니라 Agent 설치 시에도 네트워크 접속을 필요로 합니다.
- 원활한 Agent 설치 및 로그인을 위해 반드시 방화벽 혹은 NAC 등에서 sslvpn-kr-01.ncloud.com:443 아웃바운드 트래픽이 허용되어 있는지 확인해 주세요.

연관 정보 바로가기

- 서버 생성 가이드
- <u>ACG 사용 가이드</u>
- 글로벌 리전 사용 가이드