**< 터널링 >**

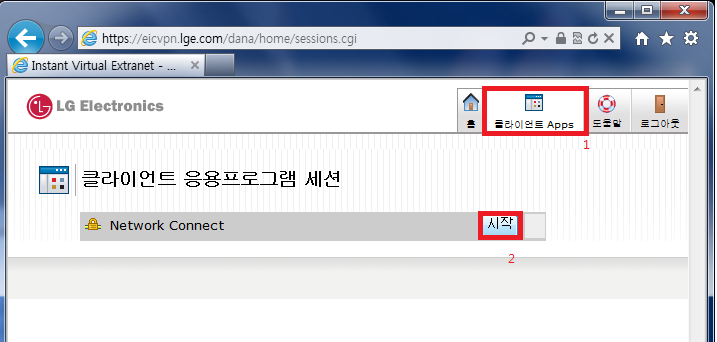
터널링이란 SSH 를 통해 원격서버의 특정 포트를 클라이언트의 특정 포트로 Port Forwarding 하는 기술이다.

\* 본 메뉴얼은 헝가리 서버를 기준으로 설명한다.

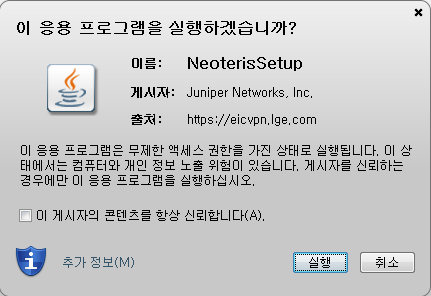
1. vpn 설치

<https://eicvpn.lge.com/> 에 접속하여 callcenter.cns / callcenter1로 로그인한다.

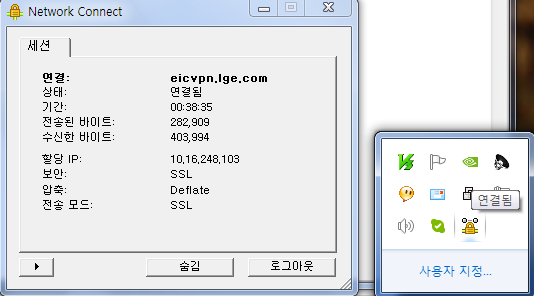
클라이언트 Apps에 Network Connect의 시작버튼을 클릭하여 응용프로그램을 설치한다.



설치가 끝난 후 프로그램 실행을 클릭한다.



실행을 누른 후 조금 기다리면 다음과 같이 연결됨이라고 뜨는걸 볼수 있다.



2. 서버 접속

57.195.129.41, 57.195.129.42 서버에 접속한다. (계정 : root / cti123)

3. 포트 포워딩

screen ssh -R 9999:localhost:22 [sshdbwj@210.121.190.210](mailto:sshdbwj@210.121.190.210) –p 62200

(ssh\_server 9999번 포트로 들어오는 데이터를 localhost의 22번 포트로 전달한다.)

명령어를 쓰고 ssh서버의 비밀번호를 입력한 후 접속이 잘 되는지 확인한다.

4. 세션 유지

ping 172.255.255.1(2) 를 입력하여 원격서버와 로컬서버의 세션을 유지시킨다.

5. detach시키기

위의 작업이 모두 끝났으면 ctrl + A + D 를 눌러 스크린으로부터 detach를 시켜준다.

6. 접속방법

ssh localhost –p 9999 를 입력하고 비밀번호를 입력한다. (cti123)

[예외상황]

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!

Someone could be eavesdropping on you right now (man-in-the-middle attack)!

It is also possible that the RSA host key has just been changed.

The fingerprint for the RSA key sent by the remote host is

xx: xx: xx: xx: xx: xx: xx: xx: xx: xx: xx: xx: xx: xx: xx:xx.

Please contact your system administrator.

Add correct host key in /home/sshdbwj/.ssh/known\_hosts to get rid of this message.

Offending key in /home/sshdbwj/.ssh/known\_hosts:00

RSA host key for localhost has changed and you have requested strict checking.

Host key verification failed.

ssh로 접속할 때 위와 같은 워닝 메시지가 뜰 경우 해결방법은

~/.ssh/known-hosts를 열고 localhost를 찾는다.

localhost를 localhost1 과 같은 방식으로 다른이름으로 만들어 둔 후에 다시 ssh명령어를 입력한다.

RSA를 등록시킬거냐고 물을때 yes를 입력하고 다시 known-hosts 파일을 열고, 다른 이름으로 저장했던 localhost의 이름을 복구시킨 후 저장하고 나와서 ssh로 접속하면 워닝메시지는 없어진다.