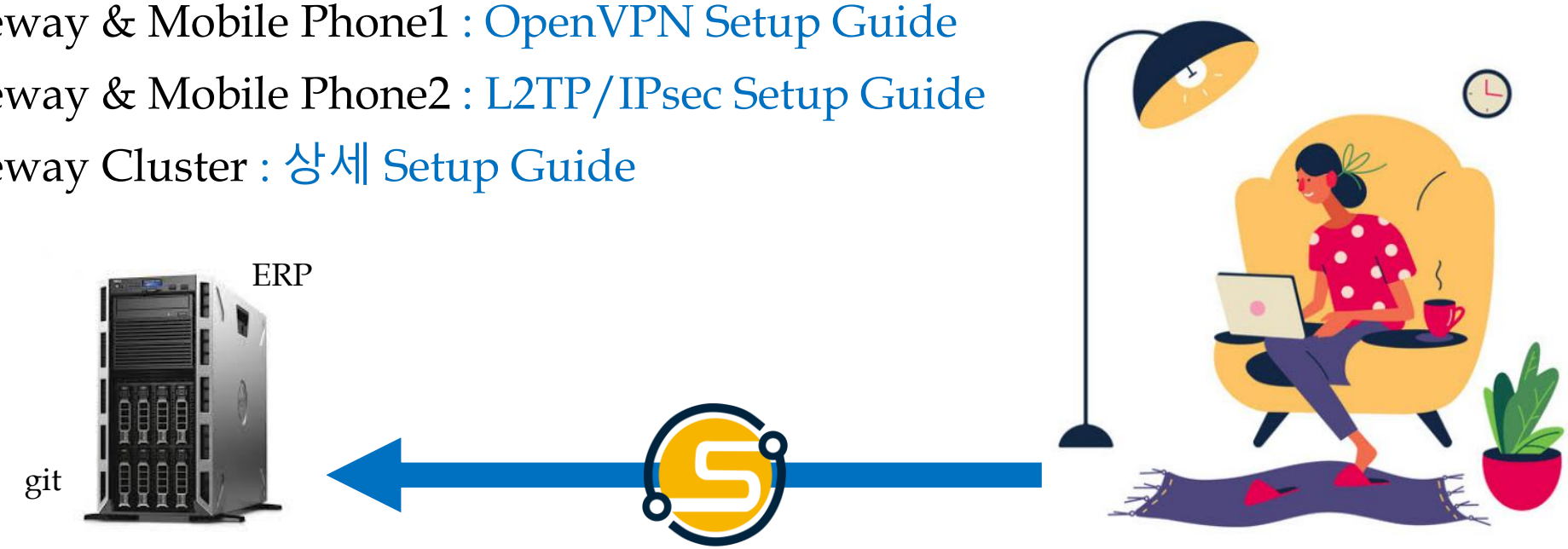
2ip 2STON SPN

- L2 SPN Setup Guide -

2ip, Inc.
Doc. Revision: 1.2

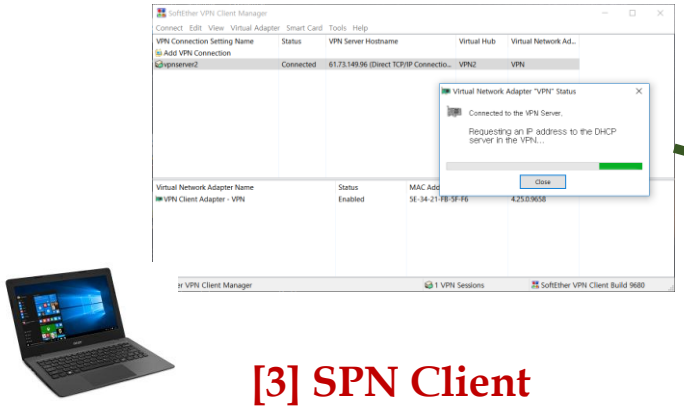
Contents(1)



Contents(2)

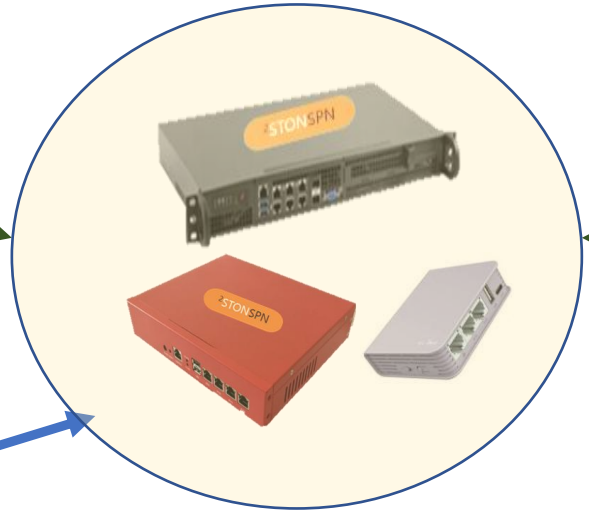
1. 2ip SPNBox 소개(1)

L2 SPN은 3개의 구성 요소(SPN Client, Bridge, Gateway)로 이루어져 있습니다.



[3] SPN Client

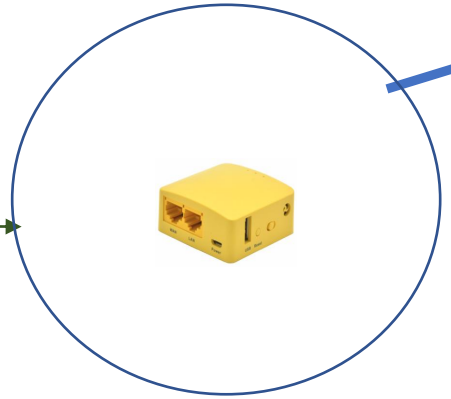
SPN Tunnel(HTTPS)



SPN Tunnel(HTTPS)

[1] SPN Gateway(SPNBox)

참고: VPN Server(or VPN Gateway)로 호칭하기도 함.



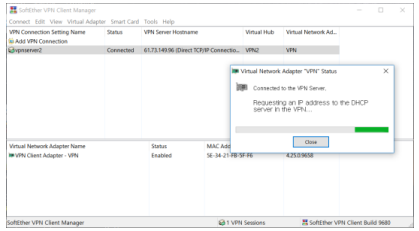
[2] SPN Bridge(SPNBox)

<용어 정리>

- SPN Gateway = VPN Server or Gateway
- SPN Bridge = VPN Bridge
- SPN Client = VPN Client

1. 2ip SPNBox 소개(2-1)

Home 사용자용
(Client or Bridge)



SPN Client
Client 1대 처리
Windows Only

SPN Bridge
Client 2대 이상 처리
비 Windows도 가능

사무실 설치용
(Gateway)

서버 50 ~ 100대 처리

서버 20대 처리

SPN Gateway

서버 5대 처리

서버 2대 처리

1. 2ip SPNBox 소개(2-2)

(2) VPN Server Manager

Model Name	VPN Type	Admin id/pass	Default LAN IP
SPNBox-4000 **[개발 중]**	VPN Gateway(Server)	spnbox/spnbox!	192.168.5.1/24
SPNBox-3000	VPN Gateway(Server)	spnbox/spnbox!	192.168.5.1/24
SPNBox-1400	VPN Gateway(Server)	spnbox/spnbox!	192.168.5.1/24
SPNBox-900	VPN Gateway(Server)	spnbox/spnbox!	192.168.5.1/24
SPNBox-200	VPN Bridge	root/spnbox! WiFi SSID: goodlife	192.168.8.1/24

SPNBox는 Web browser를 통해 기본 설정을 하며, VPN Server Manager를 이용하여 상세 VPN 설정을 하게 됩니다.

(1) Web browser

1. 2ip SPNBox 소개(2-3) – New SPNBoxes(1)

Supermicro AS-5019D-FT41 1U
(Single AMD **EPYC 3251** SoC Processor)

Supermicro SYS-5018D-FN4T Tower Server Barebone
(Intel Xeon processor **D-1541**, 8-Core 16 threads)

SPNBox-3500

1. 2ip SPNBox 소개(2-3) – New SPNBoxes(2)

https://buy.advantech.com/Rackmount-Systems/Network-Computer-Platforms-Single-Xeon-Network-Computer-Platforms/FWA-5070-1/system-22020.htm

(서버 style로 뒤 쪽이 긴 장비)

Advantech FWA-5070
(2 x Intel Xeon E5-8100/6100/5100/4100)

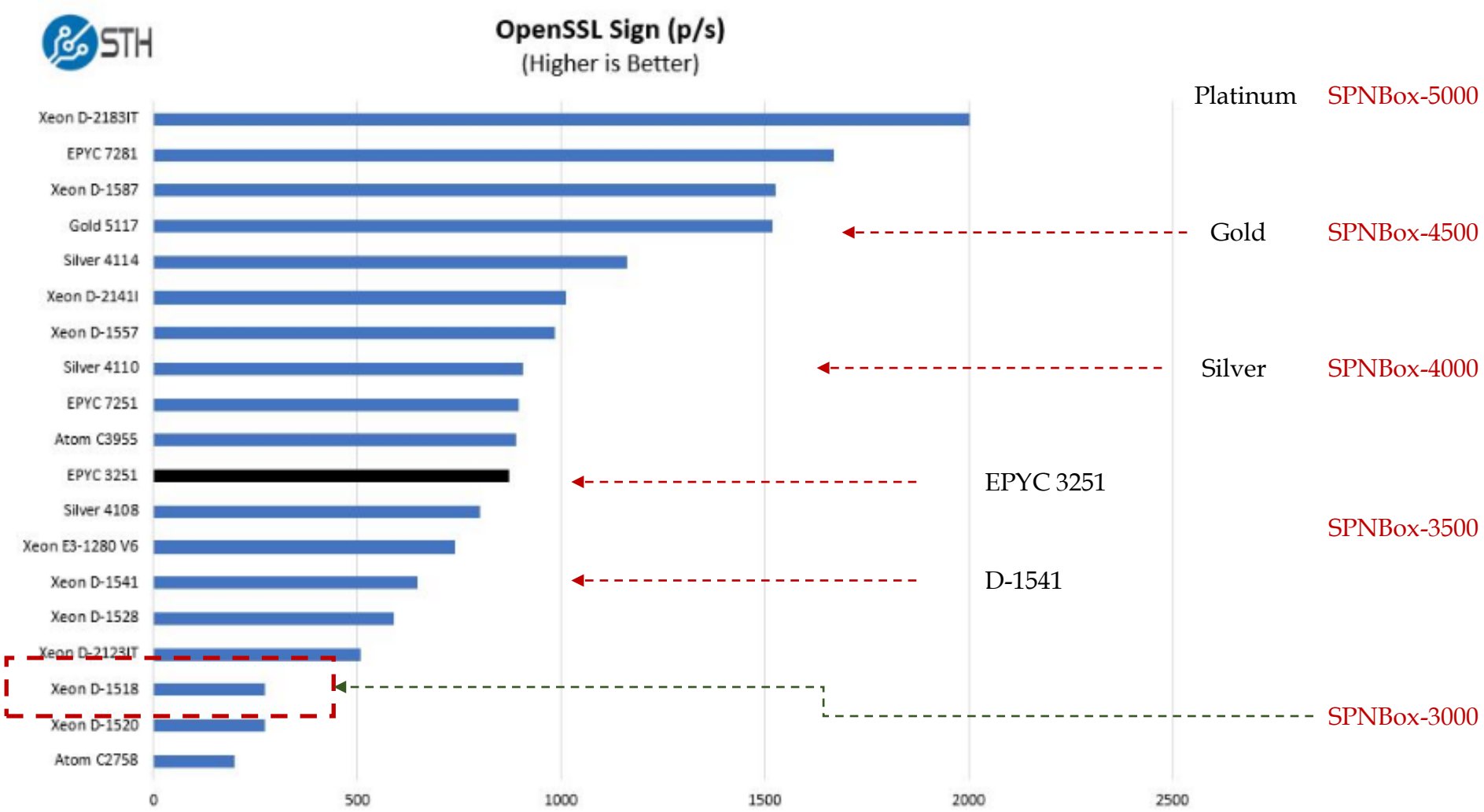
$2,285.00 ~ $4,000.00

SPNBox-4000, 4500, 5000

1 x Intel® Xeon® Scalable Processors Platinum 8100, Gold 6100 & 5100, Silver 4100 and Bronze 3100, up to 28 cores
DDR4 2133/2400/2666 ECC registered memory, 12x RDIMM
4 x NMC (Network Mezzanine Card) slots for a wide range of GbE, 10GbE, 40GbE and 100GbE NMCs with or without Advanced LAN bypass.
1 x internal PCIe x8 or x16 slots support for FH/HL add-on card
Robust storage options with 2x internal 2.5" SATA, 1x mSATA, plus up to 8 x SSD/HDD or PCIe SSD via NMC modules
IPMI 2.0 compliant Remote Management
System management features include 2 x RJ45 management ports & BMC AST2500
Operating Temperature: 0 ~ 40 °C (32 ~ 104 °F) via advanced thermal design

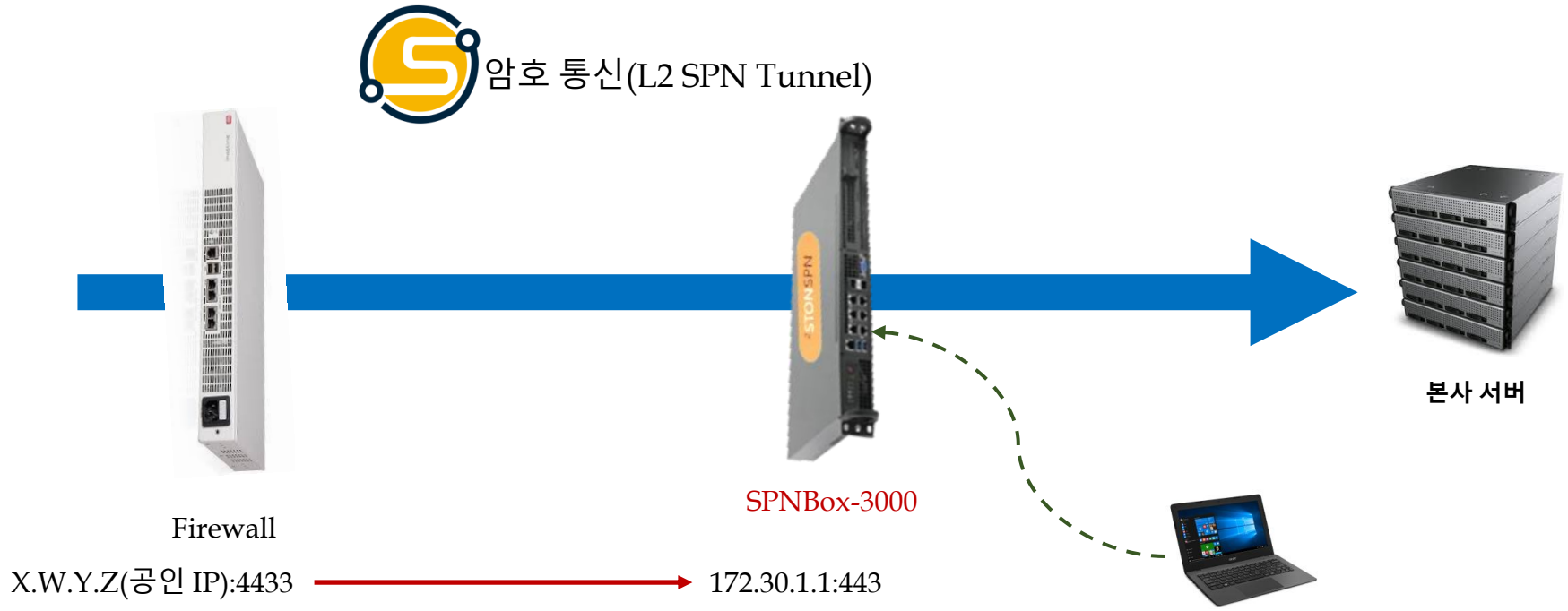
Linux 지원(CentOS, Ubuntu)

1. 2ip SPNBox 소개(2-3) – New SPNBoxes(3)



AMD EPYC 3251 OpenSSL Sign Benchmark

1. 2ip SPNBox 소개(3) – SPN Gateway



---

1. L2 SPN Tunnel 연결을 위해 본사 방화벽(Firewall)에서 Port Forwarding(4433 ➔ 443) 설정을 해 준다.
2. VPN Server Manager를 이용하여 L2 SPN Server 설정을 한다. 참고: IP 주소, Port 등의 값을 설정해 주면 된다.
3. 재택근무자가 VPN 연결을 해 오기를 기다린다.

1. 2ip SPNBox 소개(4) – SPN Bridge

1. PC의 전원을 켜고, Widows or MAC의 경우 VPN Server Manager를 설치한다.
   참고: 그 밖의 OS 사용자는 SPNBox-200에 접속하여 CLI 명령을 사용할 수 있다.

2. SPNBox-200에 LAN Cable을 연결하고 전원을 넣는다. 물론 Wi-Fi 설정도 가능하다.

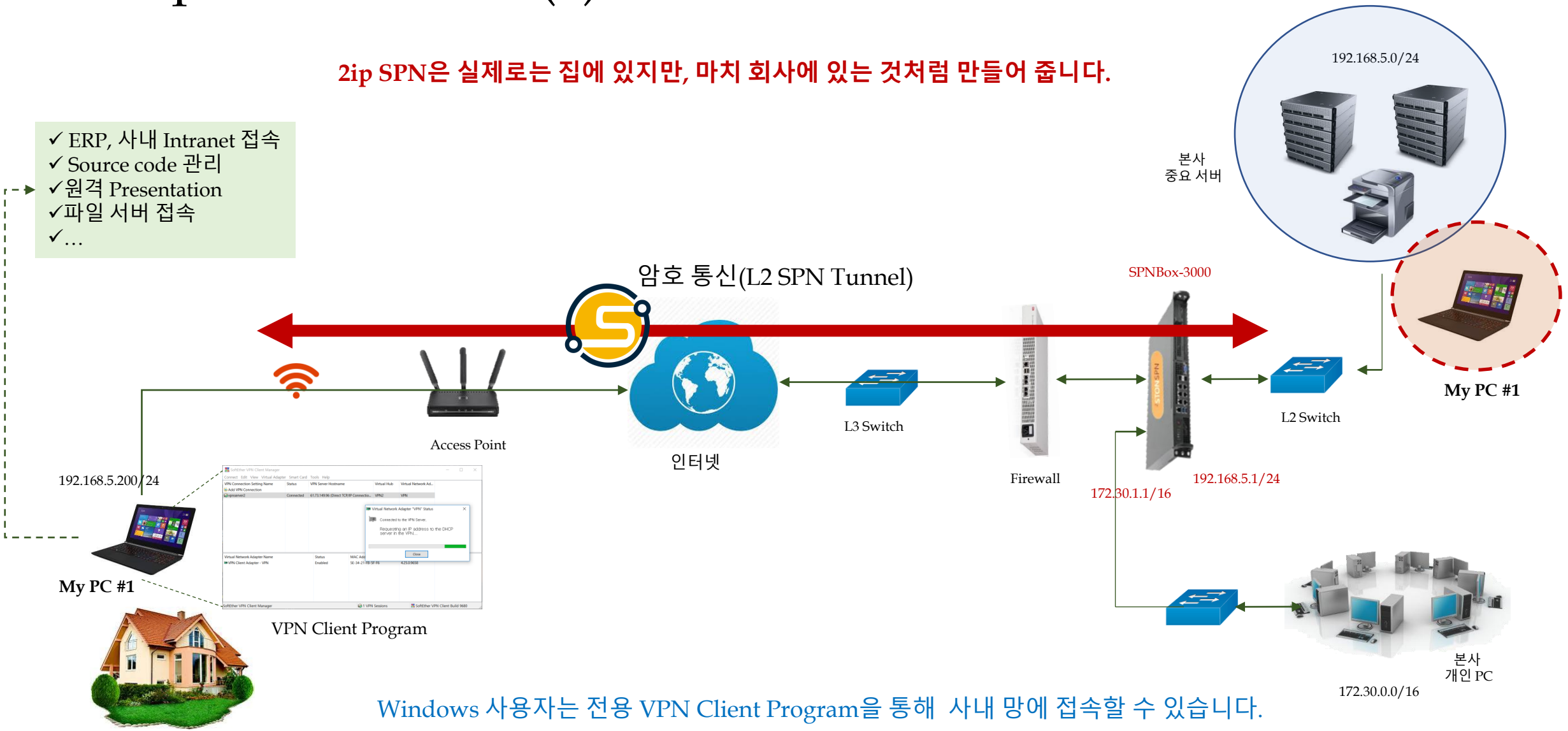
3. 본사에서 제공한 외부 공인 IP 주소 & 포트 및 사용자 계정 정보를 입력한 후, VPN 연결을 시도한다.

4. 이제 부터는 마치 자신의 Notebook이 사무실에 있는 것처럼 자유롭게 사내 서버에 접속할 수 있다.
   참고: 자신의 IP 주소를 확인해 보라. 본사 내부 망의 주소와 동일한 대역임을 알 수 있다.

1. 2ip SPNBox 소개(5) – SPN Client

2ip SPN은 실제로는 집에 있지만, 마치 회사에 있는 것처럼 만들어 줍니다.

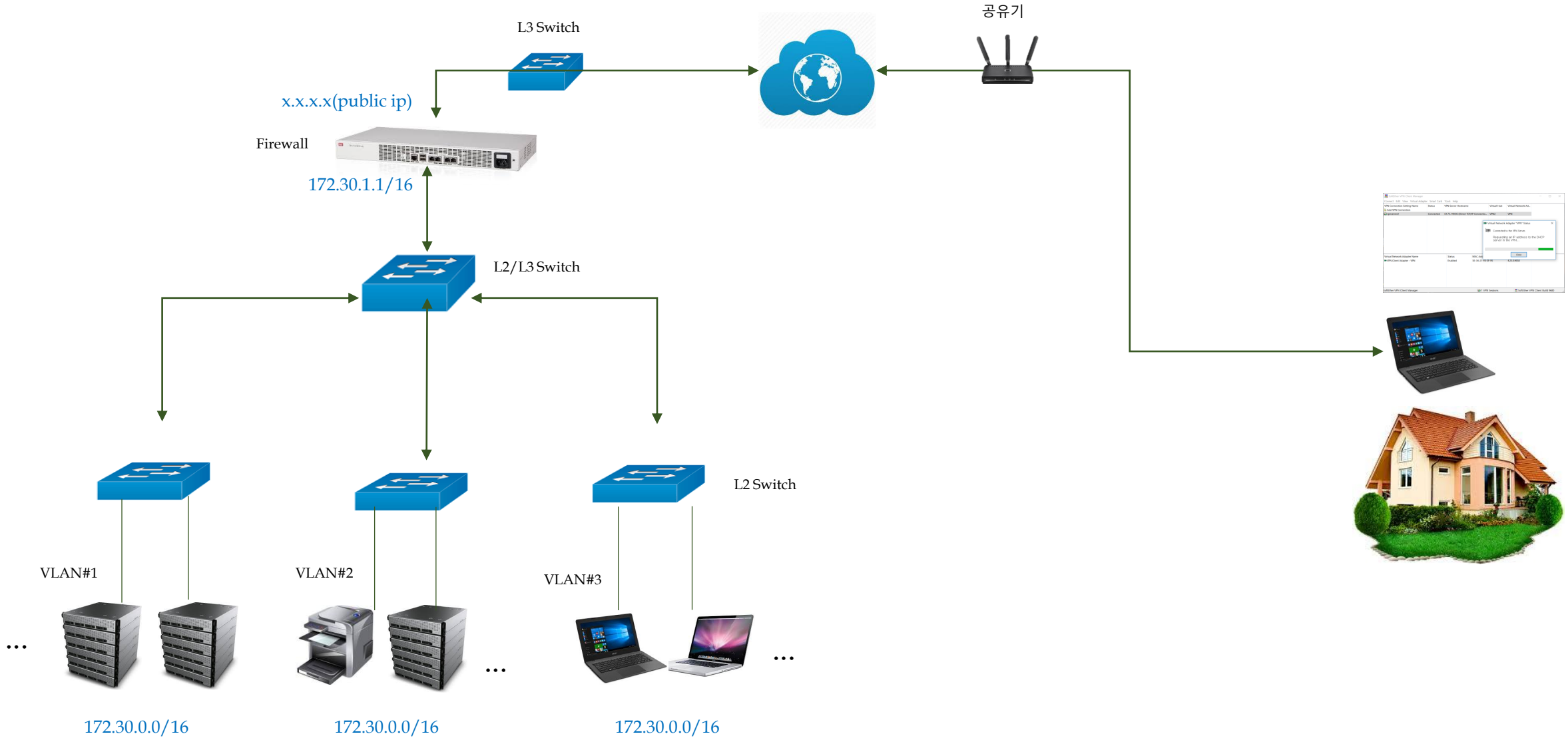
- ✓ ERP, 사내 Intranet 접속
- ✓ Source code 관리
- ✓원격 Presentation
- ✓파일 서버 접속
- ✓…



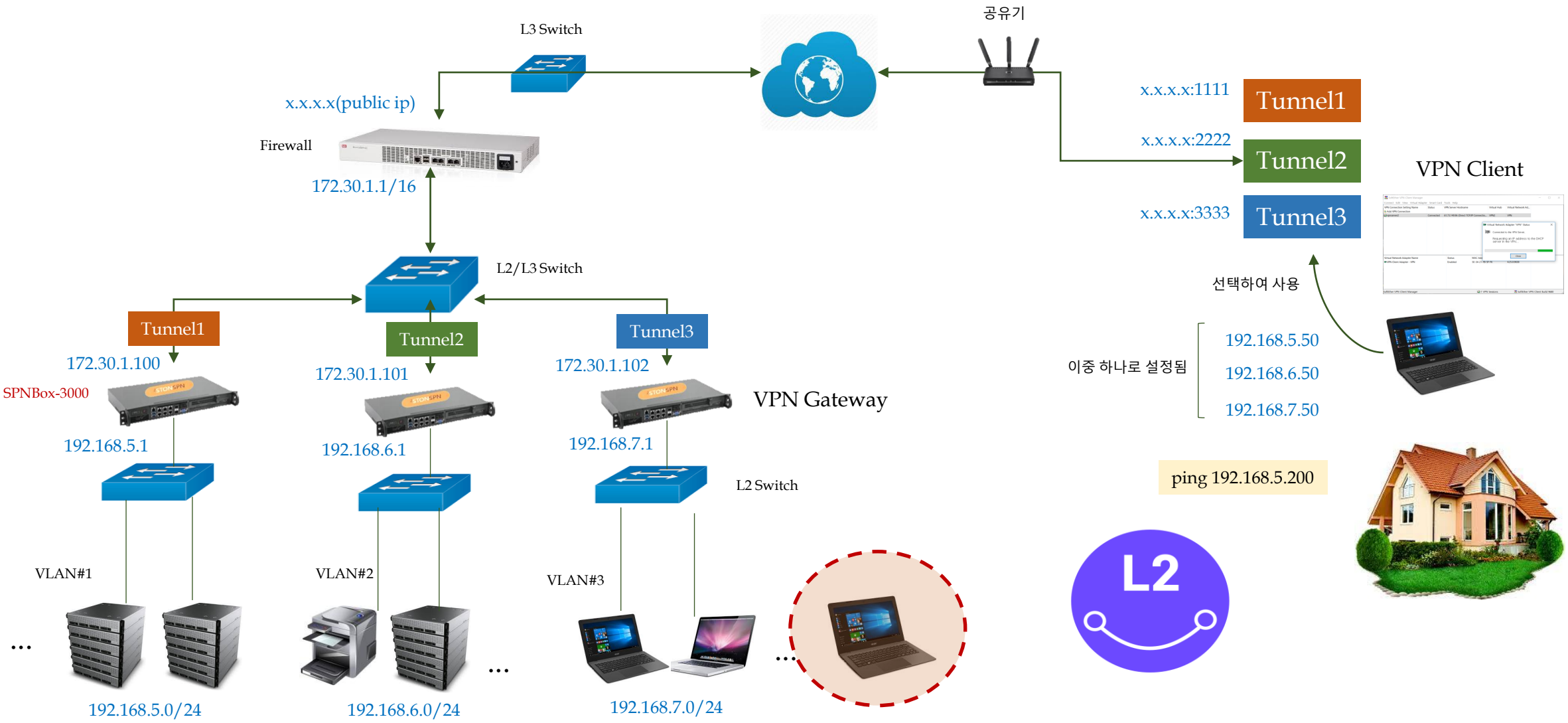
Windows 사용자는 전용 VPN Client Program을 통해 사내 망에 접속할 수 있습니다.

2. VPN 네트워크 구성
: VPN망 구성 예

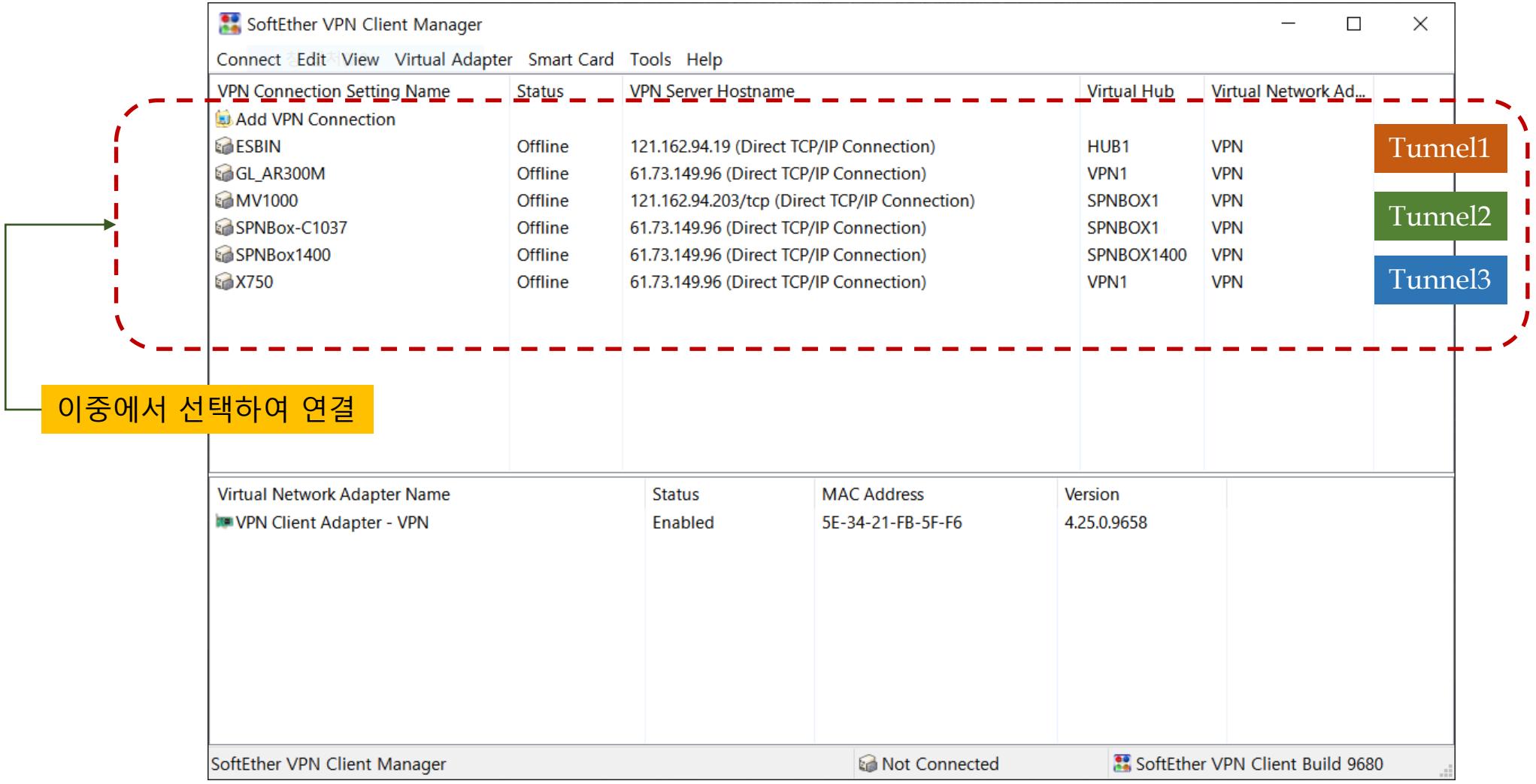
2. VPN 네트워크 구성(1)



2. VPN 네트워크 구성(2) – SPN Gateway & SPN Client(1)

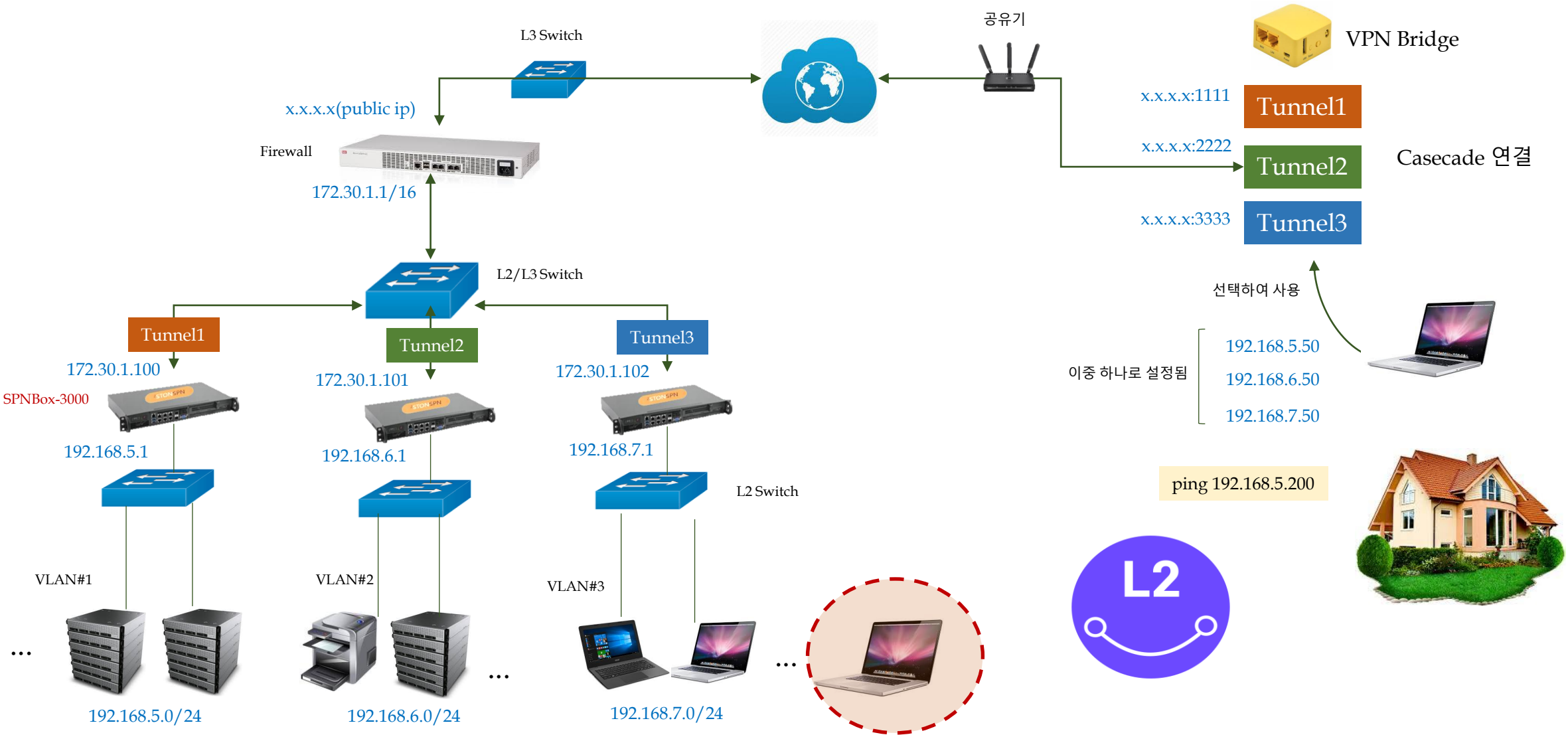


2. VPN 네트워크 구성(2) – SPN Gateway & SPN Client(2)

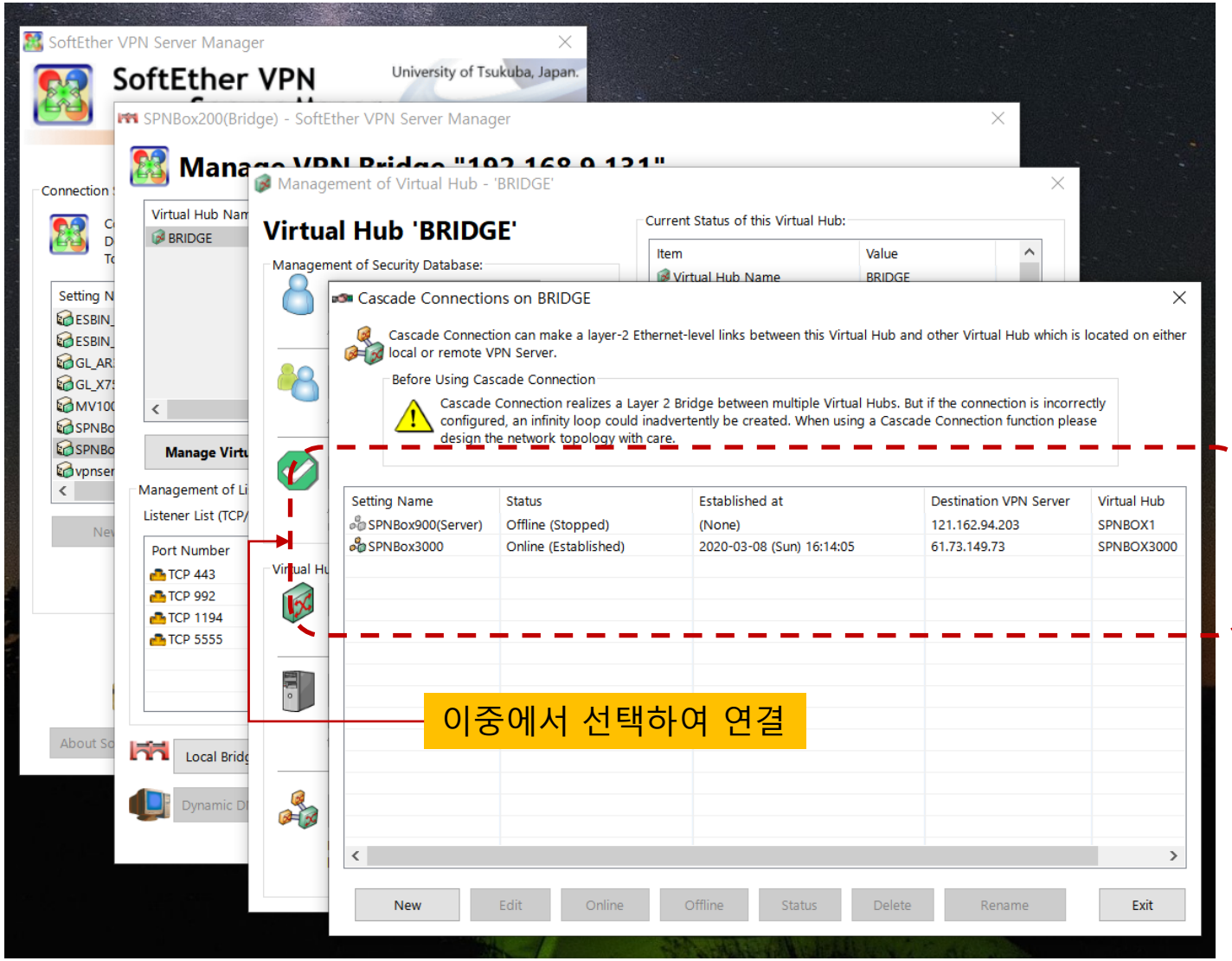


L2 SPN Client

2. VPN 네트워크 구성(3) – SPN Gateway & SPN Bridge(1)

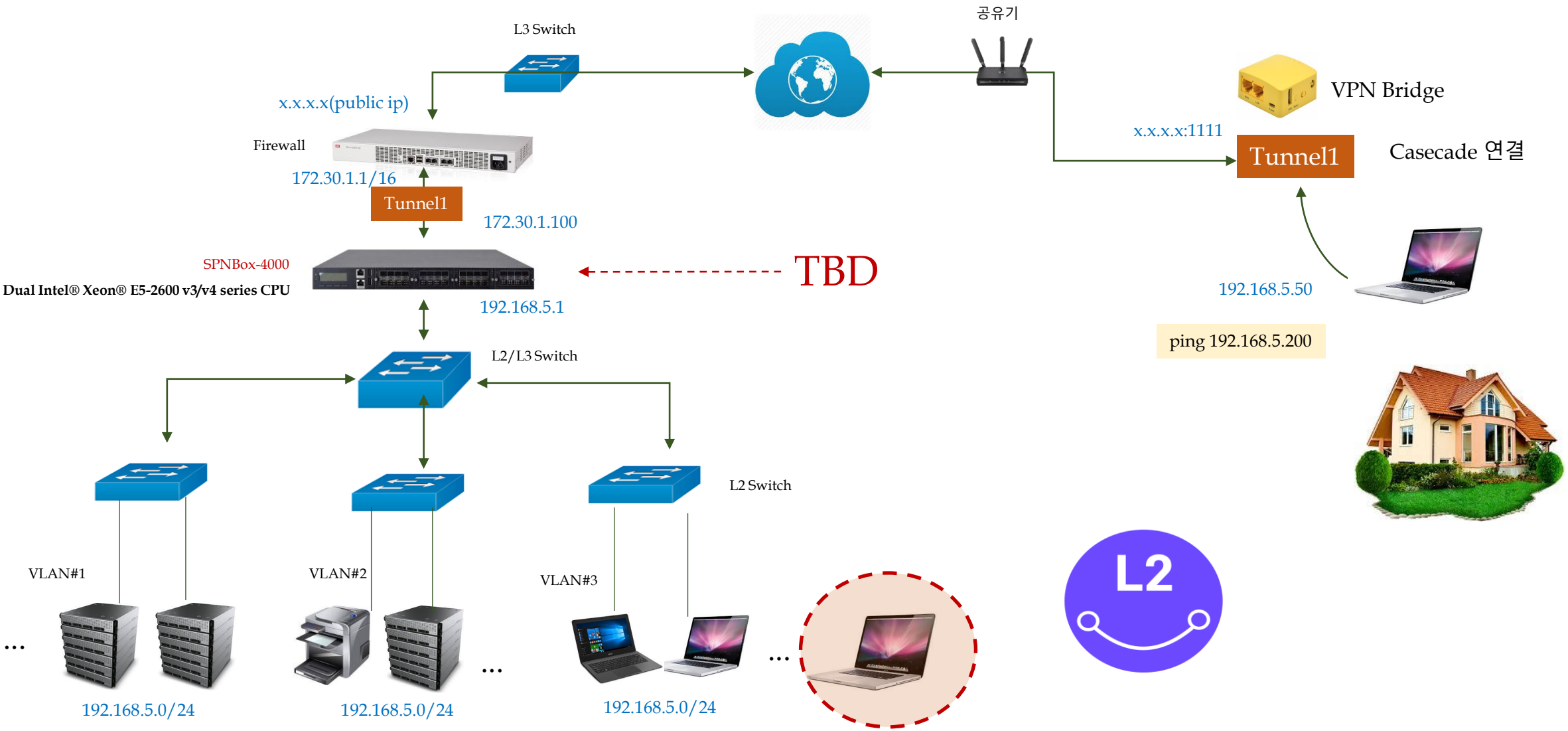


2. VPN 네트워크 구성(3) – SPN Gateway & SPN Bridge(2)

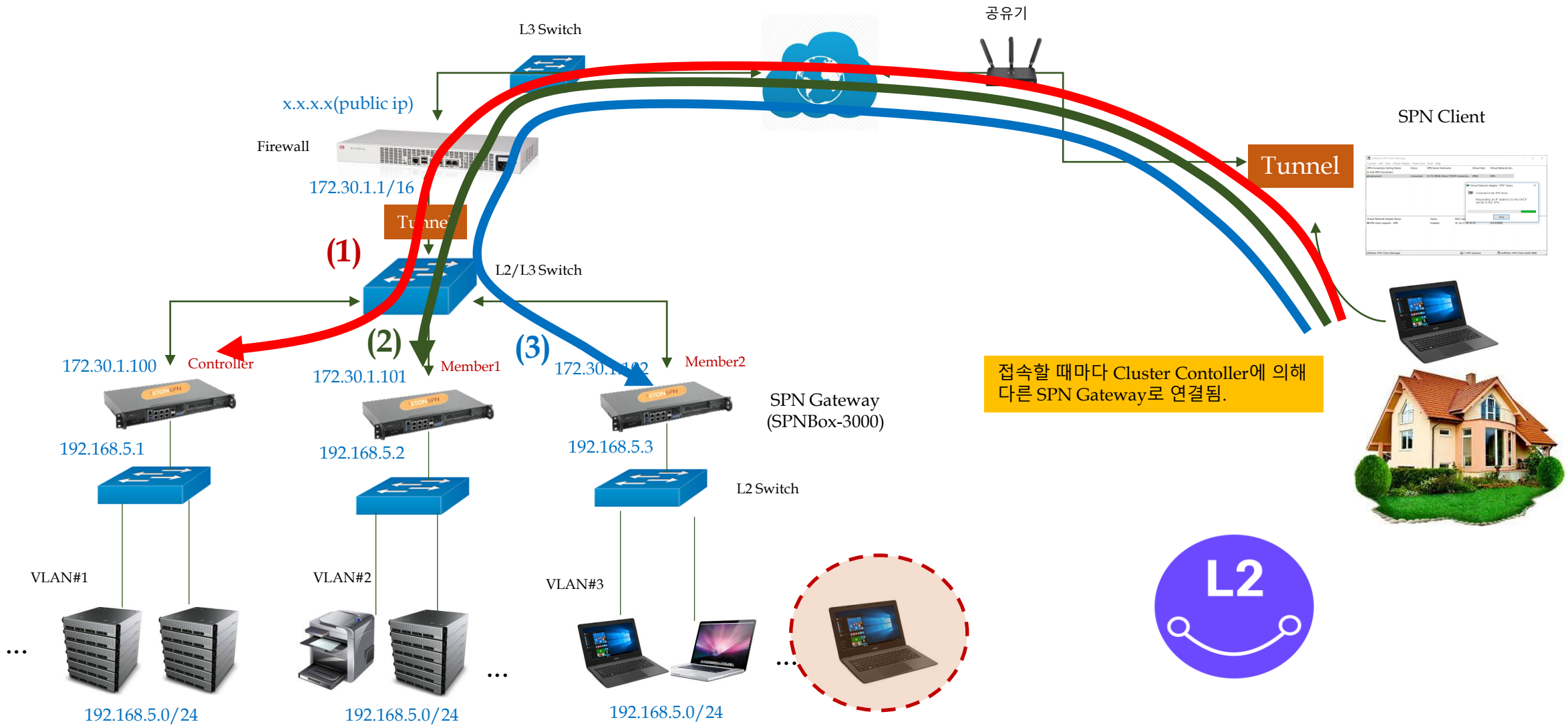


L2 SPN Bridge

2. VPN 네트워크 구성(4) – SPN Gateway & SPN Bridge

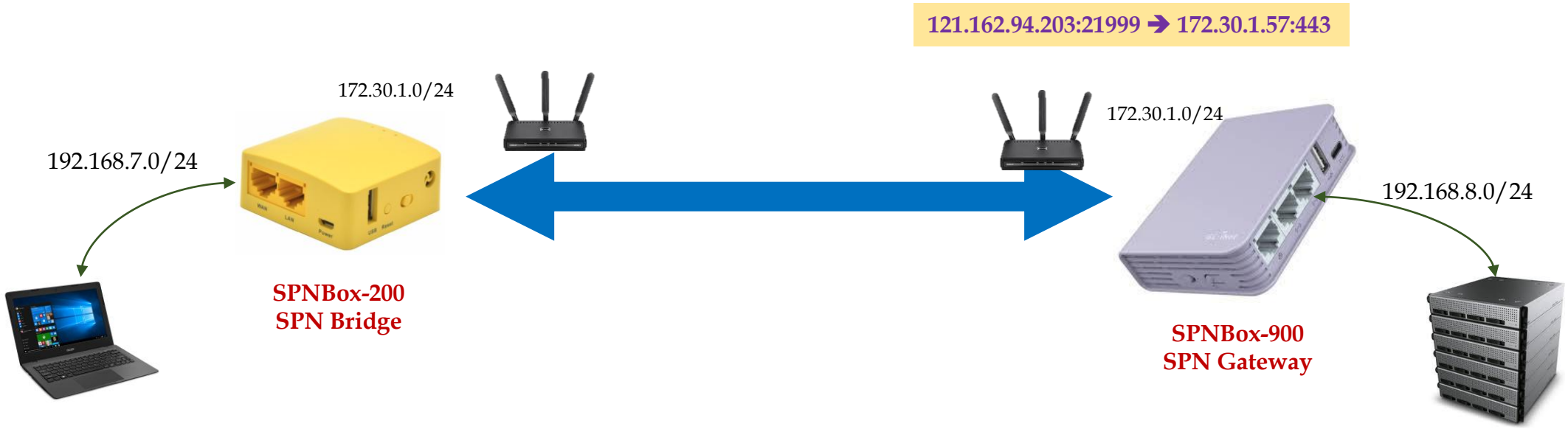


2. VPN 네트워크 구성(5) – SPN Gateway Cluster



3. SPN Gateway & SPN Bridge
: 상세 Setup Guide

3. SPN Gateway & Bridge(1) – Testbed(1)



이 장에서는 위의 네트워크(테스트베드) 환경에서 VPN 연결 시험을 진행하도록 하겠습니다.

3. SPN Gateway & Bridge(1) - Testbed(2)

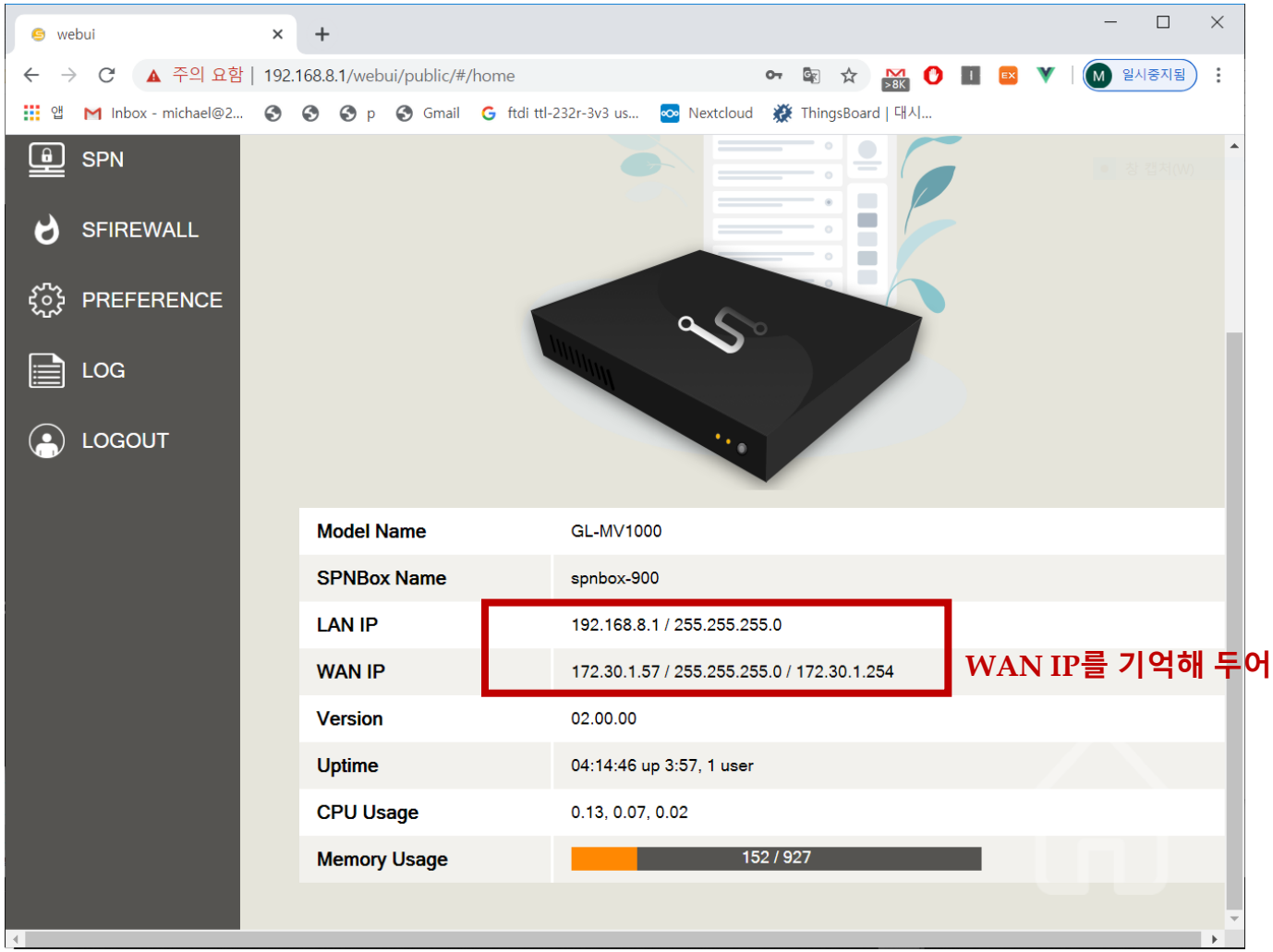
SPN Gateway	전체 설정 절차 요약
a)	VPN Server를 구동시키고, vpncmd(CLI: se vcmd run 명령)로 admin password를 설정한다(SPNBox CLI에서 수행)
b)	Windows PC에서 VPN Server Manager로 VPN Server에 접속한 후, 가장 기본적인 서버 설정(local ip address, port, admin password 입력)을 한다.
c)	Virtual Hub을 하나 추가한다. Default Virtual Hub을 사용해도 됨.
d)	Virtual Hub 사용을 위한 client 계정을 하나 등록한다.
e)	Local bridge를 하나 생성하고 SPNBox LAN bridge와 연결한다(SPNBox CLI에서 수행).

SPN Bridge	전체 설정 절차 요약
a)	VPN Bridge를 구동시키고, vpncmd로 admin password를 설정한다(SPNBox CLI에서 수행)
b)	Windows PC에서 VPN Server Manager로 VPN Bridge에 접속한 후, 가장 기본적인 서버 설정(local ip address, port, admin password 입력)을 한다.
c)	Virtual Hub은 새로 추가할 수 없으며, 기 등록되어 있는 녀석(BRIDGE)을 그대로 사용한다.
d)	나머지는 수행할 필요가 없으며, VPN Server와의 연결을 위한 Cascade 설정을 진행한다.

3. SPN Gateway & Bridge(2) – Gateway 설정(1)

SPNBox-900
VPN Gateway

LAN: 192.168.8.0/24



WAN IP를 기억해 두어야 함.

3. SPN Gateway & Bridge(2) – Gateway 설정(2)

```
spnbox-900(config)# se
  enable       Start the softether daemon
  localbridge  Add tap interface to kernel bridge(ex: br0 interface)
  vcmd         Execute SE vpncmd
spnbox-900(config)# se enable  vserver
spnbox-900(config)# show se vserver
SE daemon(pid=2144 2143) is alive.
================================================================================
root      2143  0.0  0.1   7764  1868 ?        S<s  04:14   0:00 /sbin/vpnserver/vpnserver execsvc
root      2144  9.3  2.0 1013008 19140 ?       S<l  04:14   0:01 /sbin/vpnserver/vpnserver execsvc
================================================================================
spnbox-900(config)# wr
Configuration saved SUCCESS
spnbox-900(config)#
```

1) VPN Server 구동

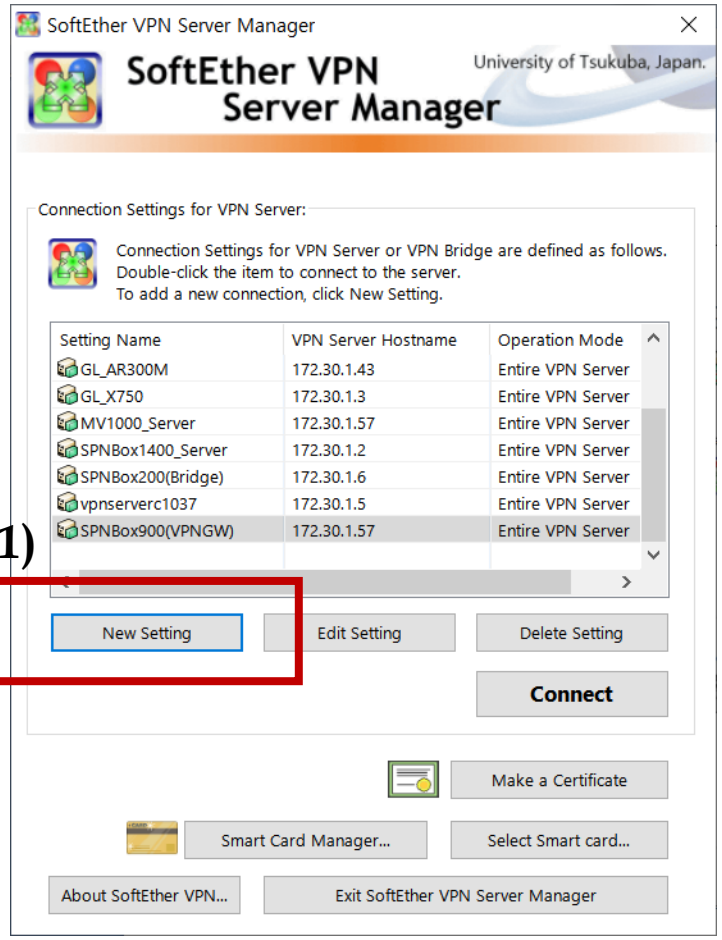
```
config)# se vcmd run
and - SoftEther VPN Command Line Management Utility Developer Edition
PN Command Line Management Utility (vpncmd command)
dition
2 Build 9731   (English)
20/01/01 17:54:10 by buildsan at crosswin
c) all contributors on SoftEther VPN project in GitHub.
c) Daiyuu Nobori, SoftEther Project at University of Tsukuba, and SoftEther Corporation.
reserved.

ncmd program, the following can be achieved.

nt of VPN Server or VPN Bridge
2. Management of VPN Client
3. Use of VPN Tools (certificate creation and Network Traffic Speed Test Tool)

Select 1, 2 or 3: 1

Specify the host name or IP address of the computer that the destination VPN Server or VPN Bridge is oper
ating on.
By specifying according to the format 'host name:port number', you can also specify the port number.
(When the port number is unspecified, 443 is used.)
If nothing is input and the Enter key is pressed, the connection will be made to the port number 443 of l
ocalhost (this computer).
Hostname of IP Address of Destination:

If connecting to the server by Virtual Hub Admin Mode, please input the Virtual Hub name.
If connecting by server admin mode, please press Enter without inputting anything.
Specify Virtual Hub Name:
Connection has been established with VPN Server "localhost" (port 443).

You have administrator privileges for the entire VPN Server.

VPN Server>ServerPasswordSet
ServerPasswordSet command - Set VPN Server Administrator Password
Please enter the password. To cancel press the Ctrl+D key.

Password: **********
Confirm input: **********


The command completed successfully.
```

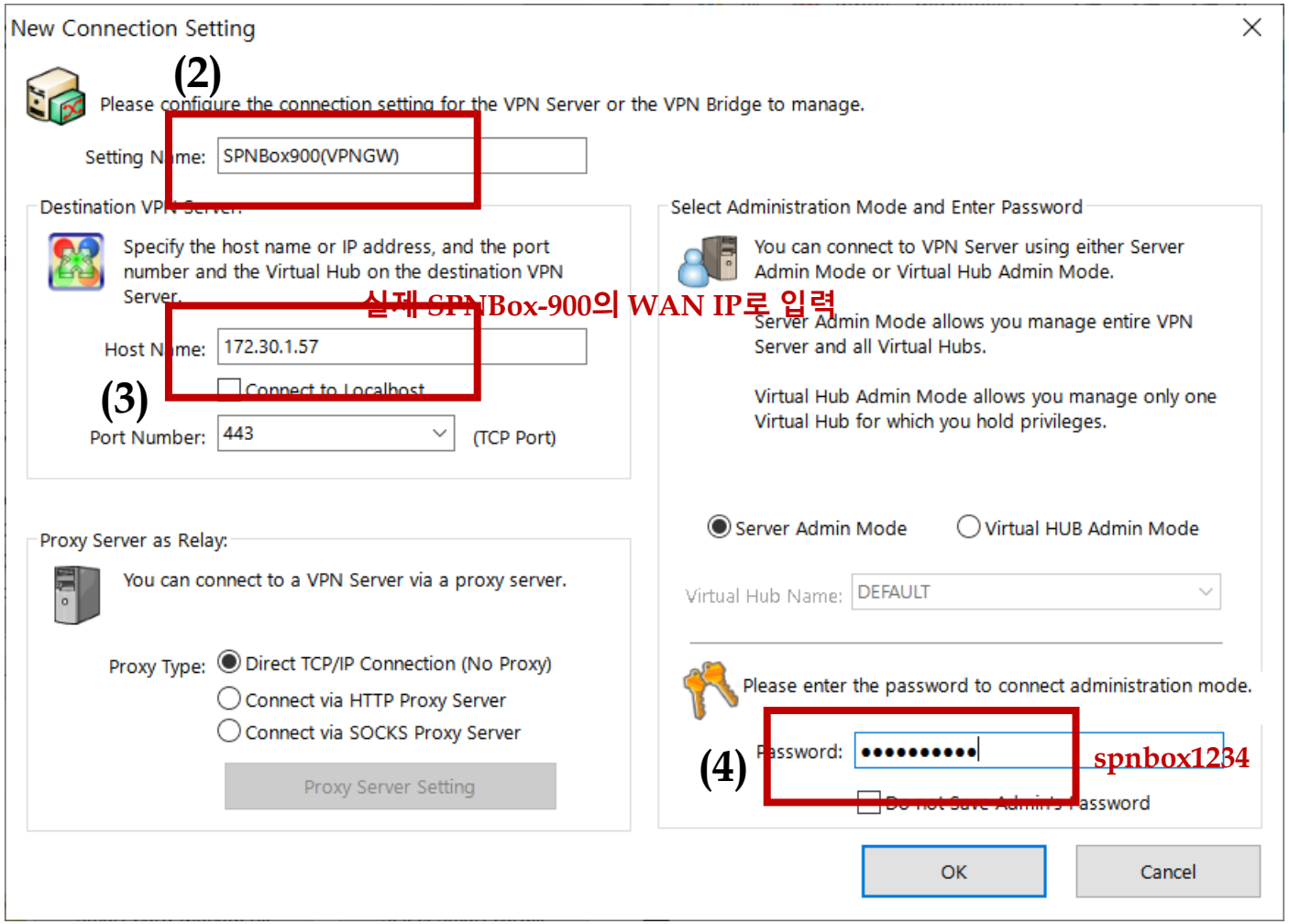
<Enter> 입력

<Enter> 입력

2) VPN Server admin 패스워드 설정
(pass: spnbox1234)

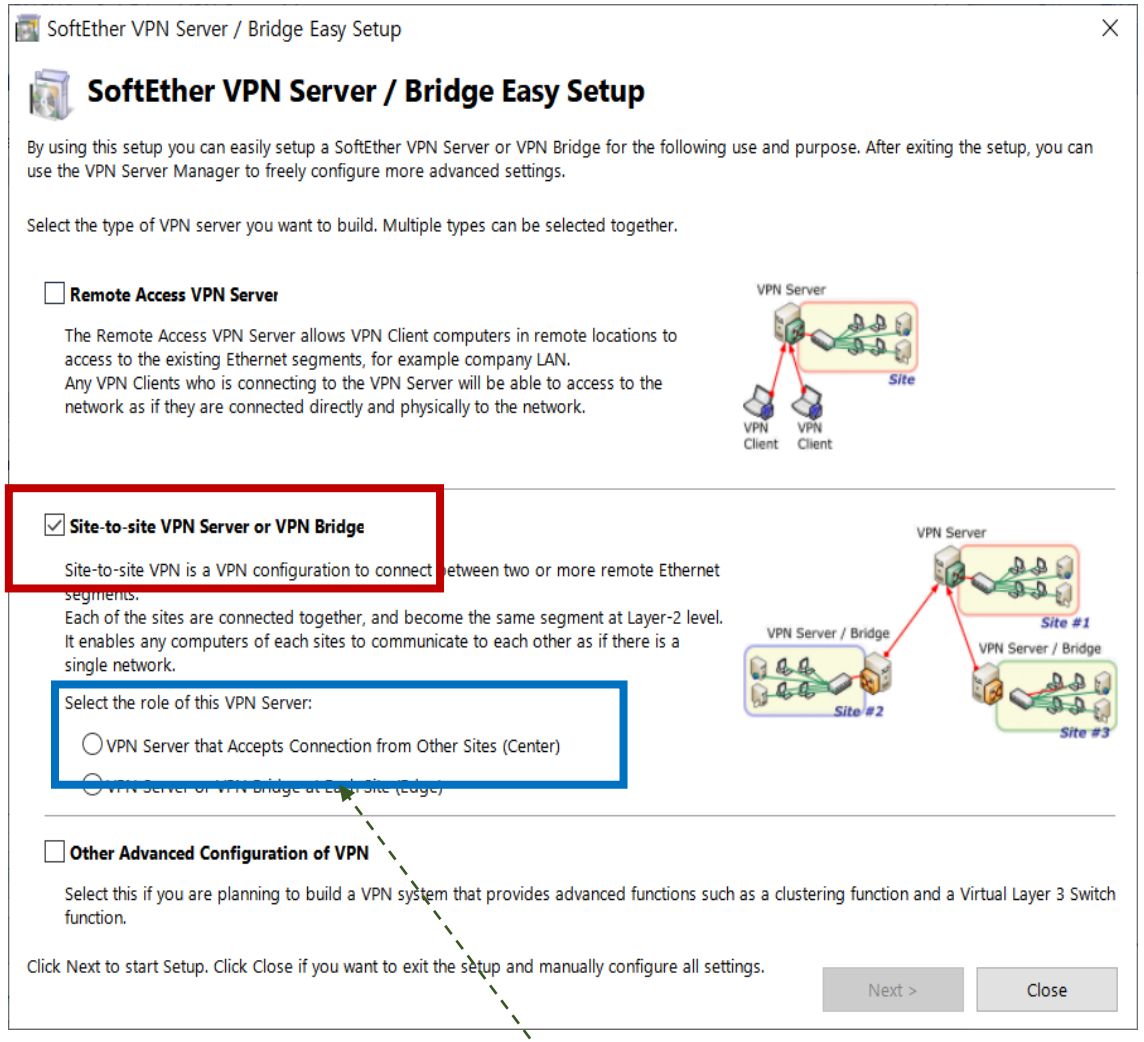
3. SPN Gateway & Bridge(2) – Gateway 설정(3)

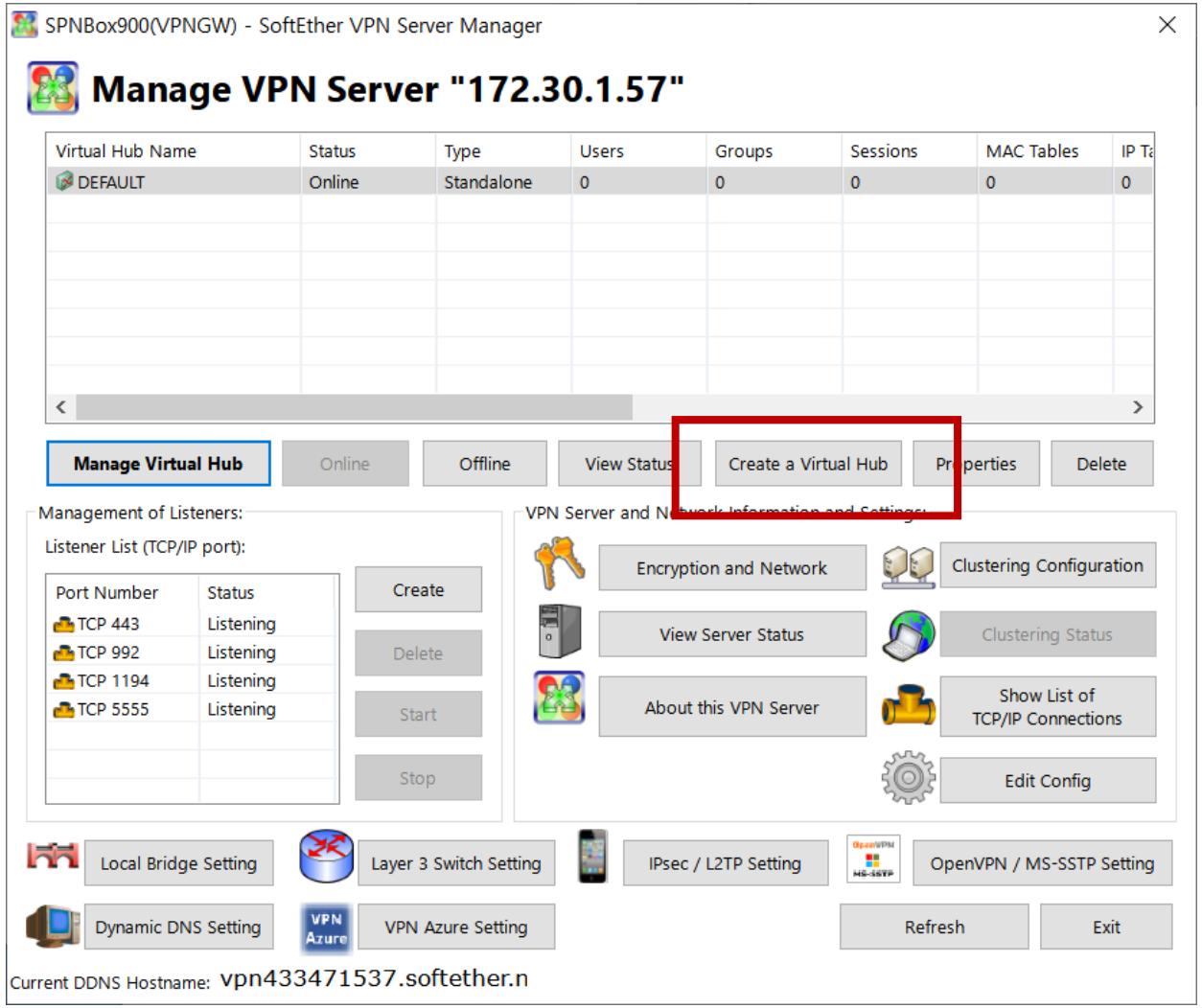




주의: 위의 설정을 하기 위해서는 notebook PC가 SPNBox-900과 동일한 네트워크 환경(예: 같은 무선 AP에 연결)에 있어야 한다.

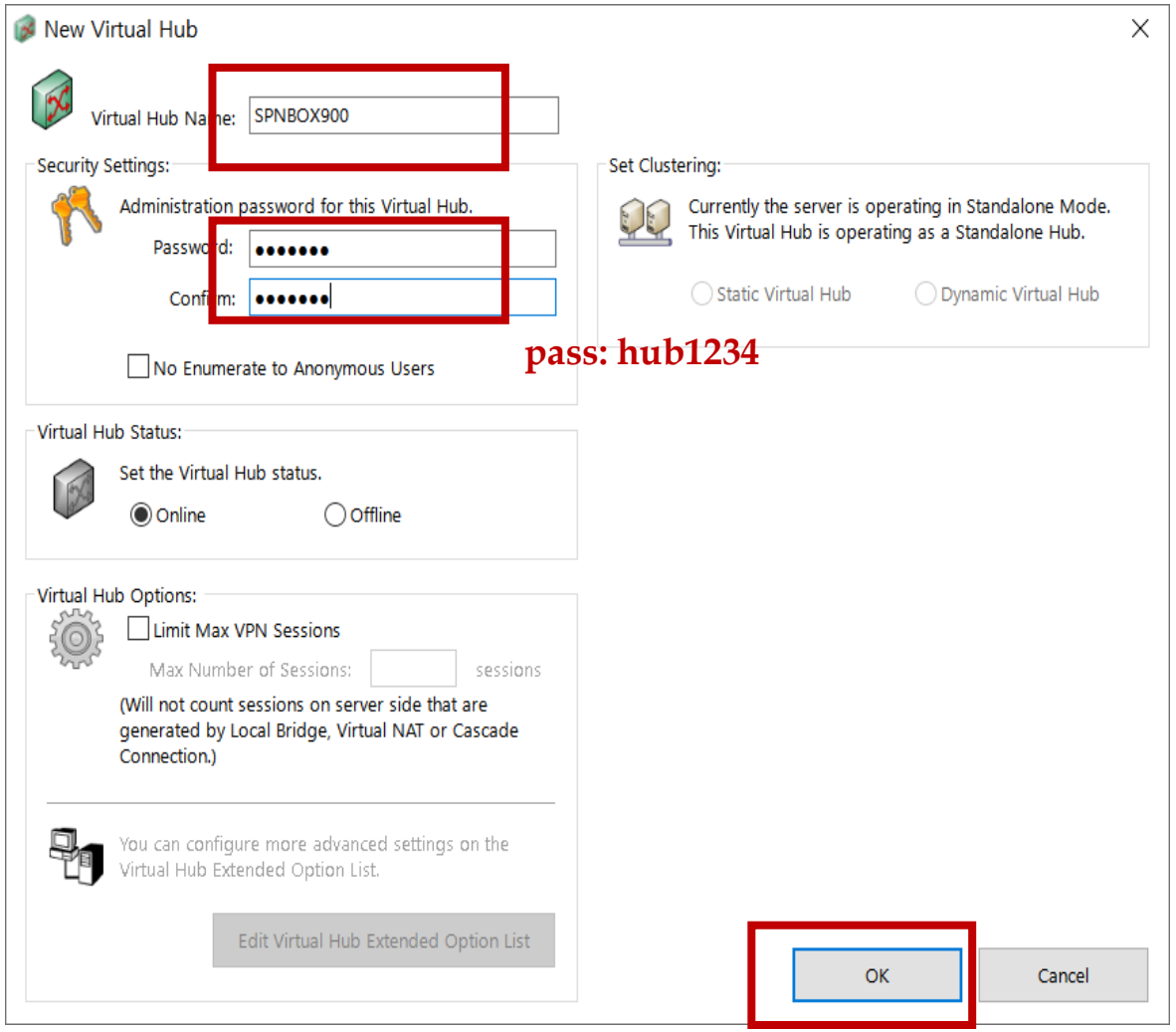
3. SPN Gateway & Bridge(2) – Gateway 설정(4)

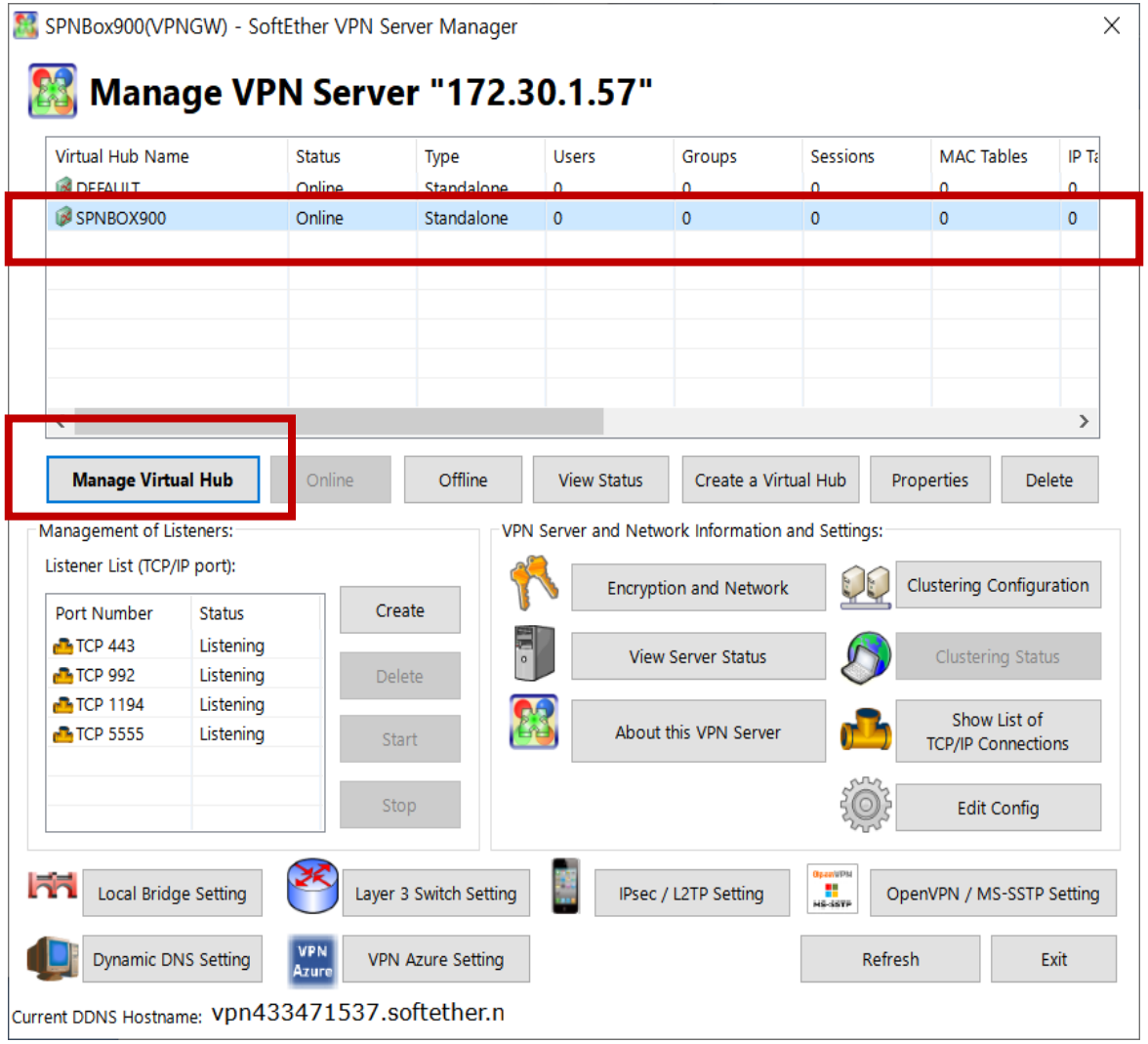




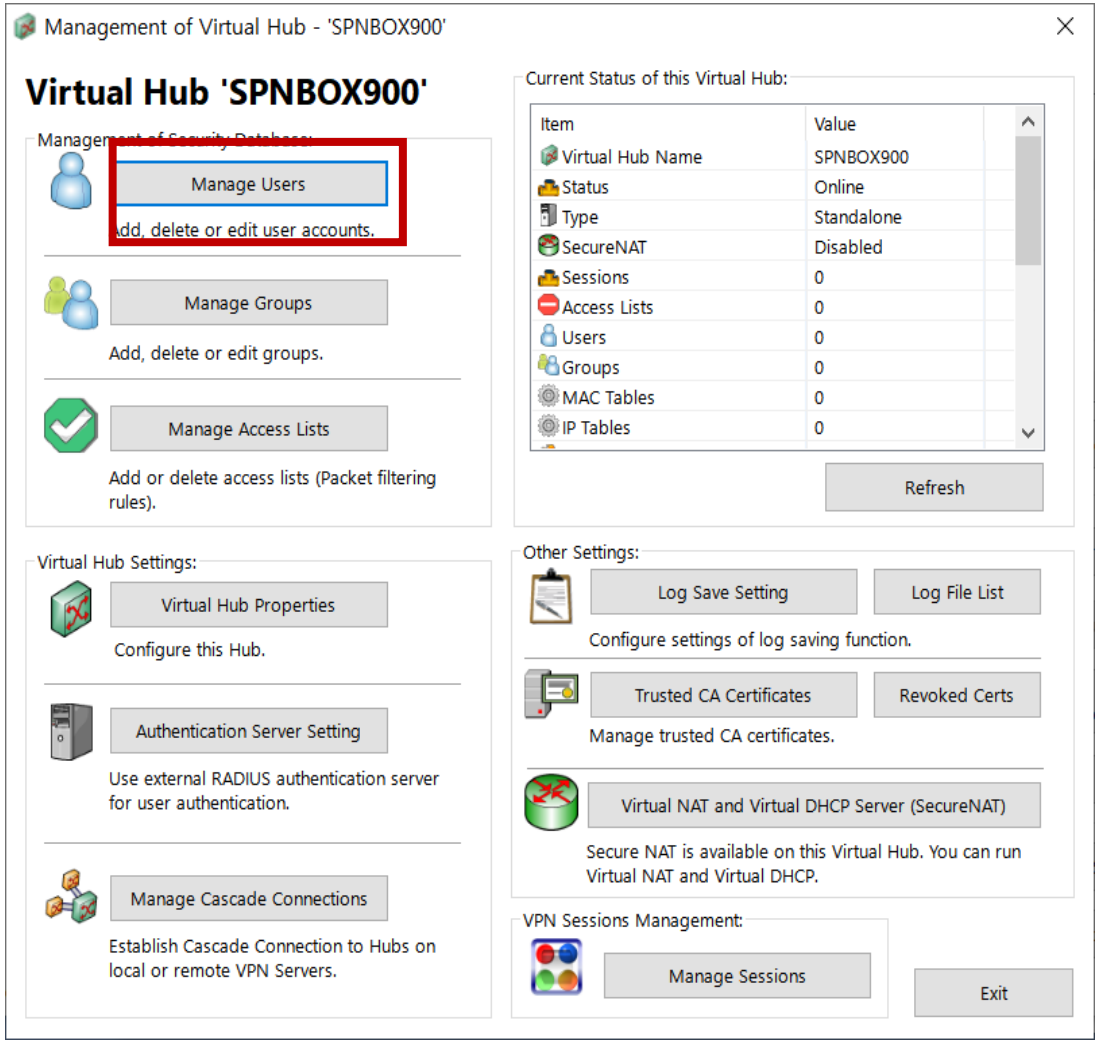
참고로, 이걸 enable하면 이후, wizard 형태로 주요 설정 절차를 진행할 수 있다.

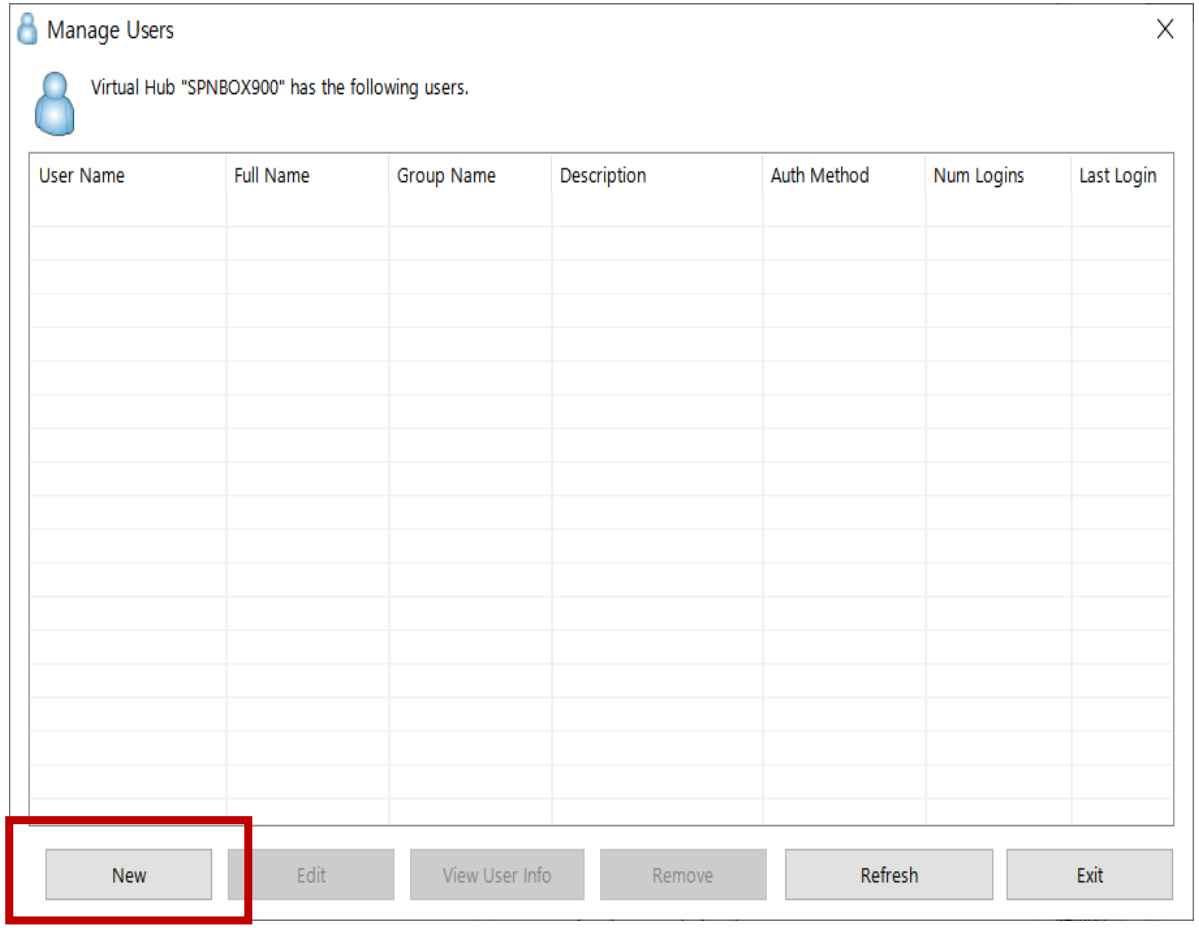
3. SPN Gateway & Bridge(2) – Gateway 설정(5)



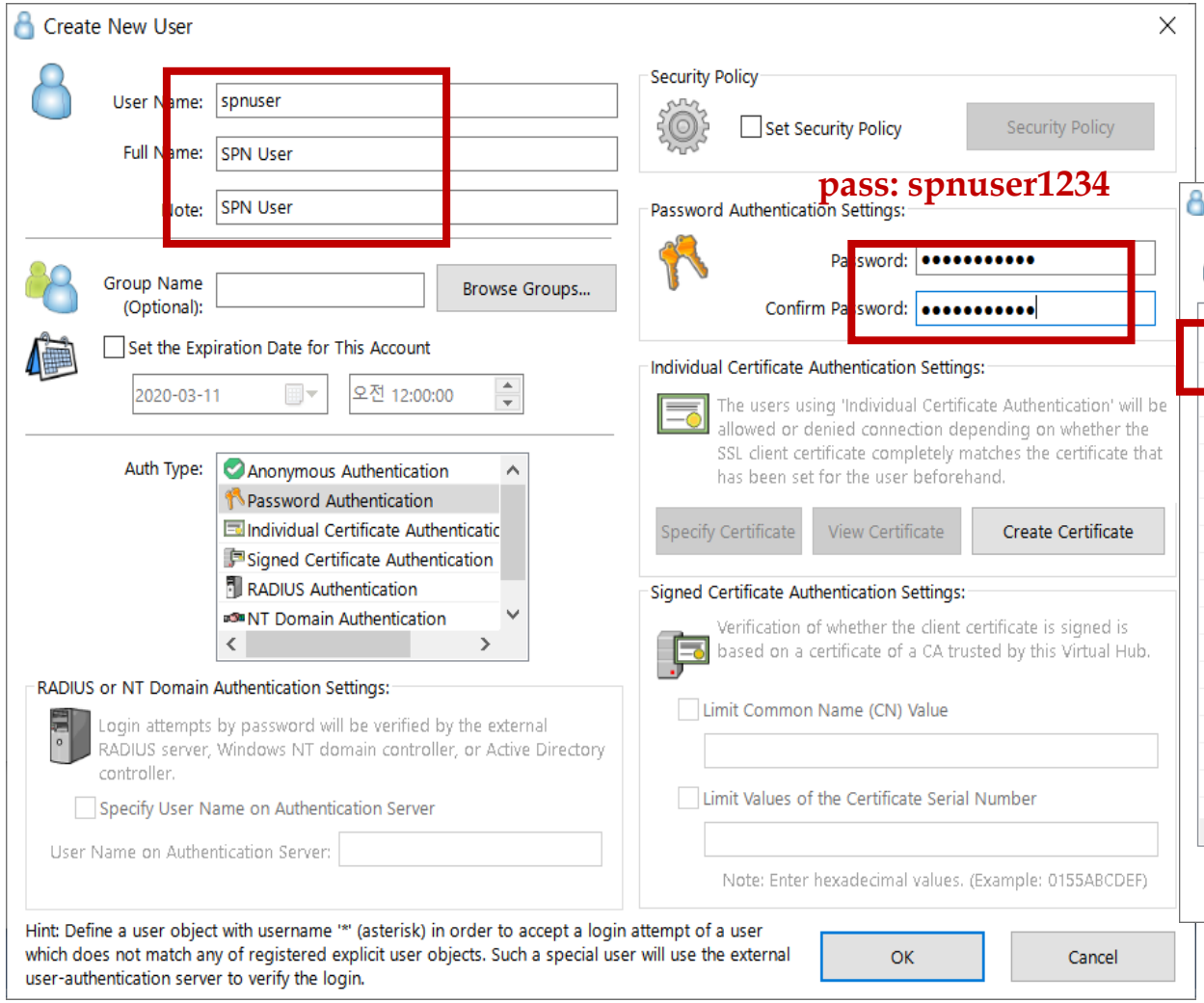


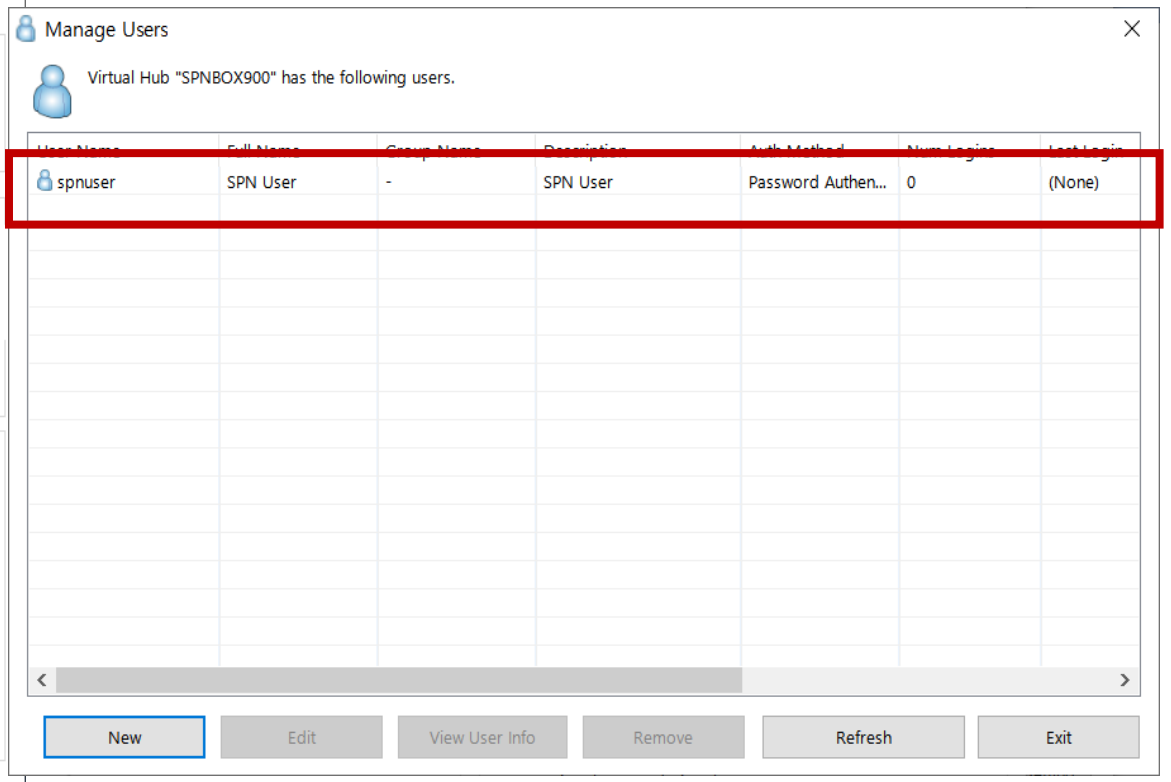
3. SPN Gateway & Bridge(2) – Gateway 설정(6)



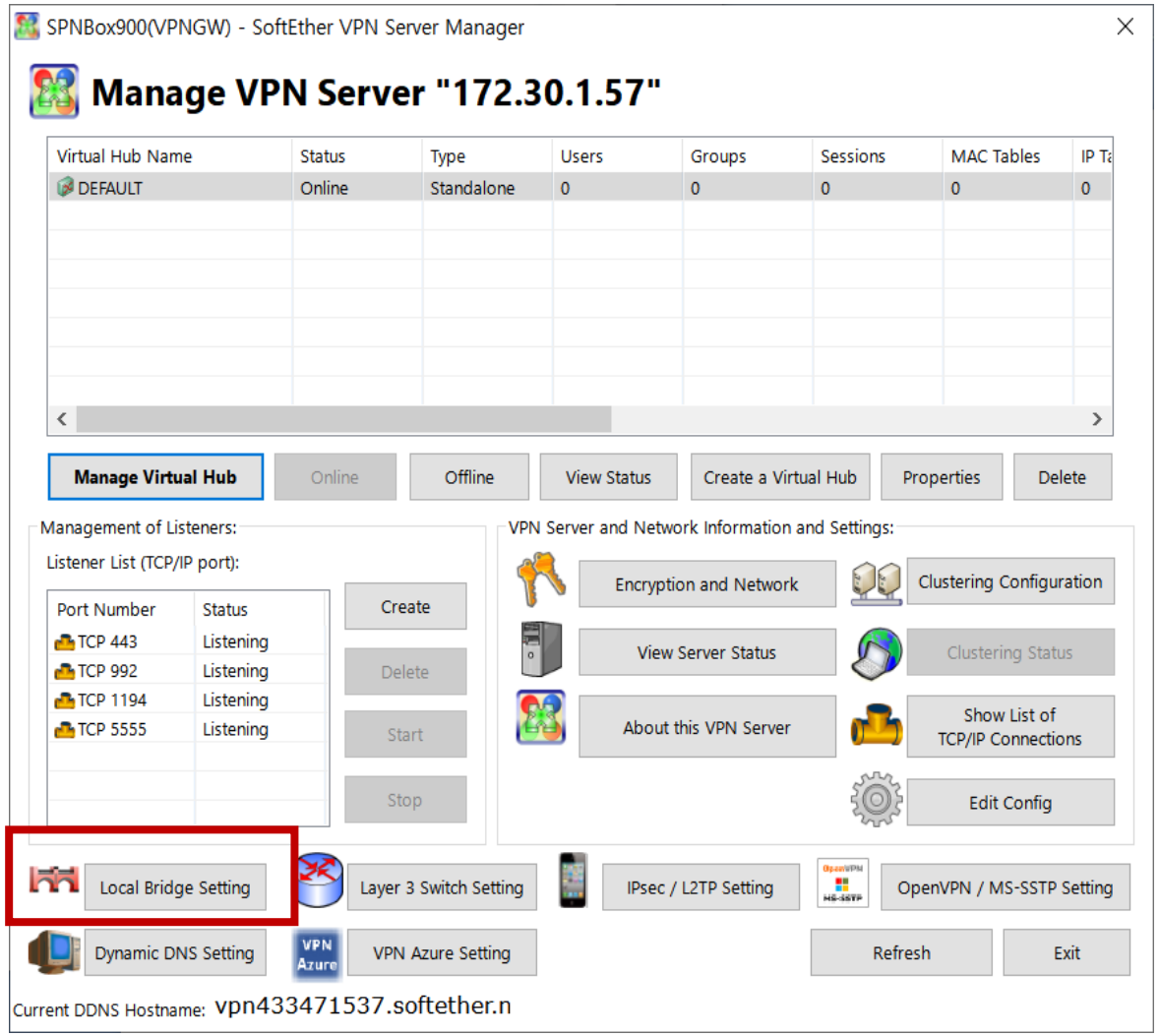


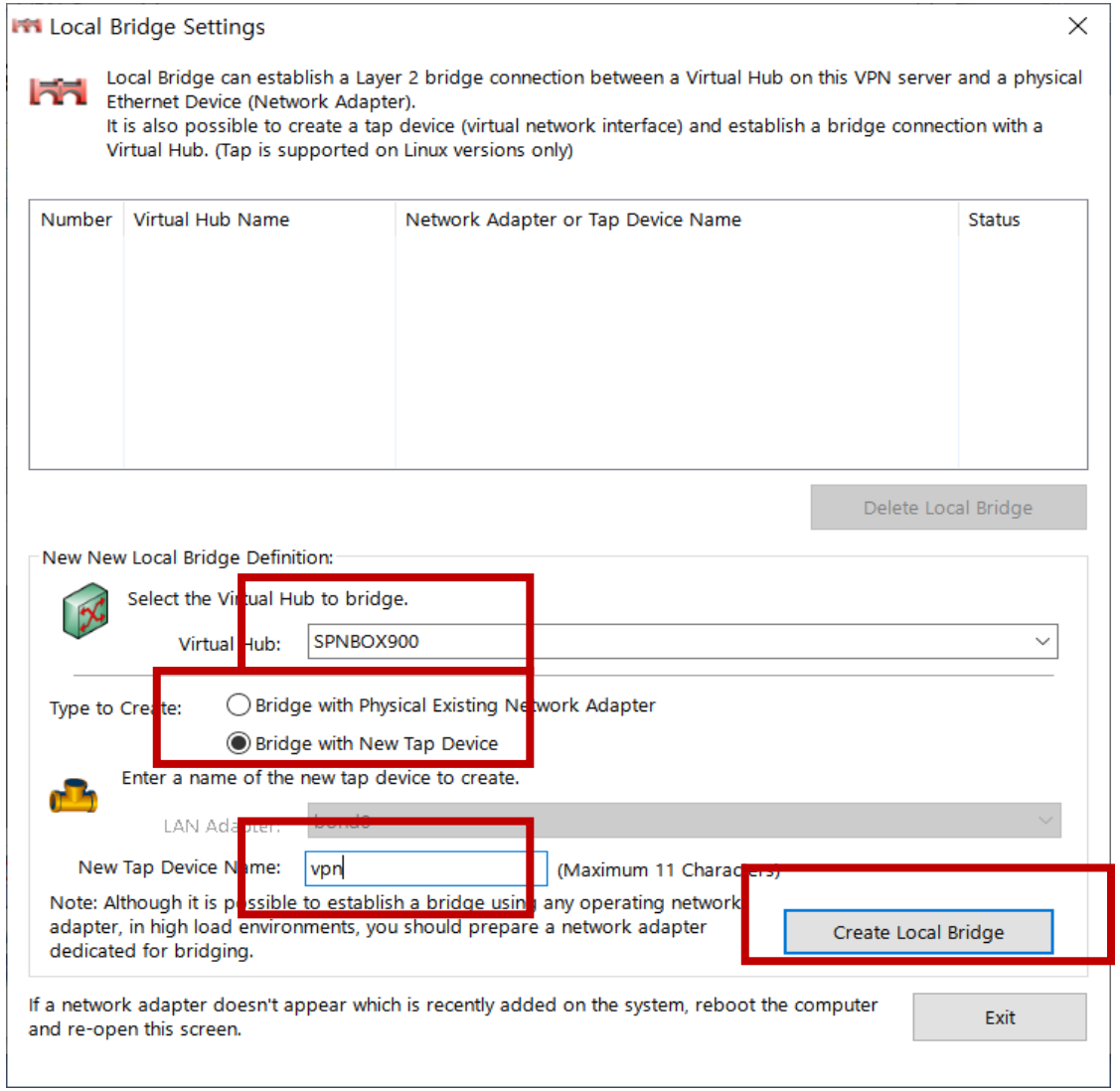
3. SPN Gateway & Bridge(2) – Gateway 설정(7)



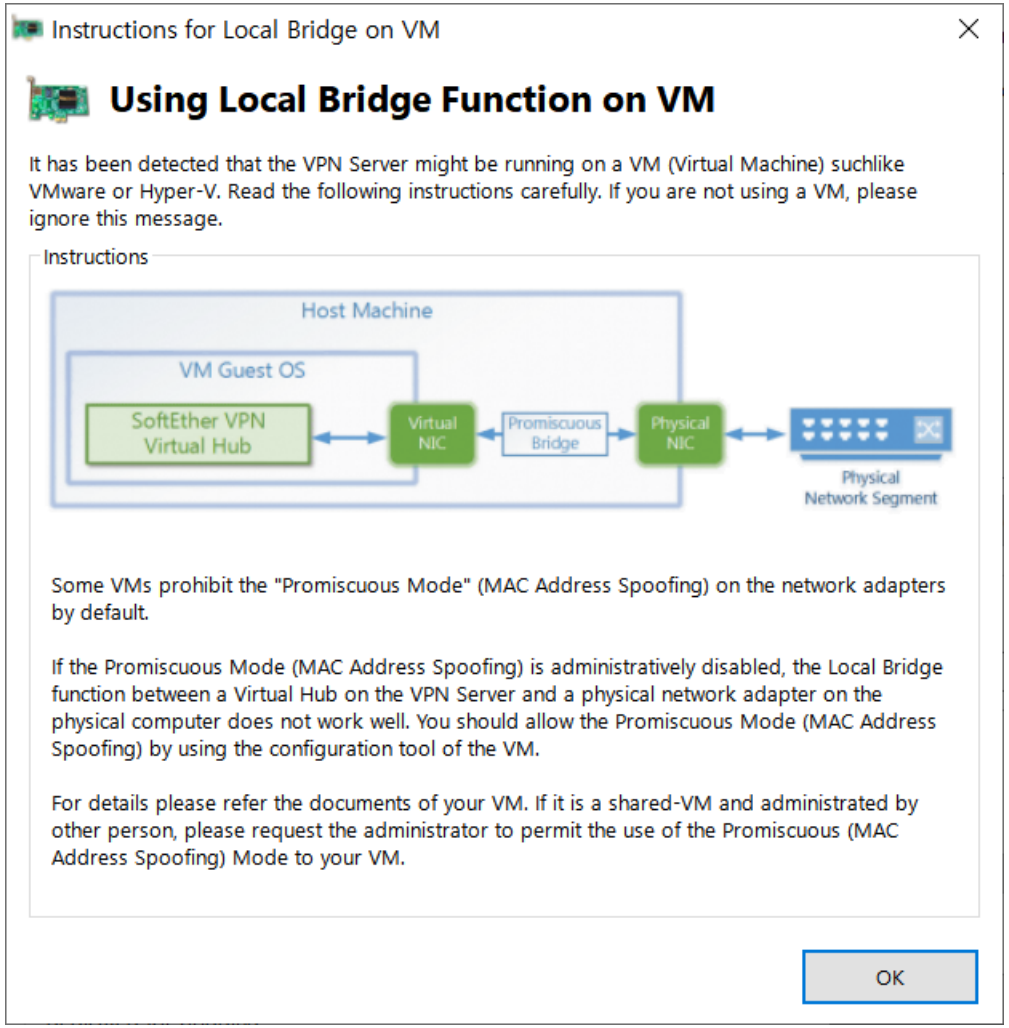


3. SPN Gateway & Bridge(2) – Gateway 설정(8)

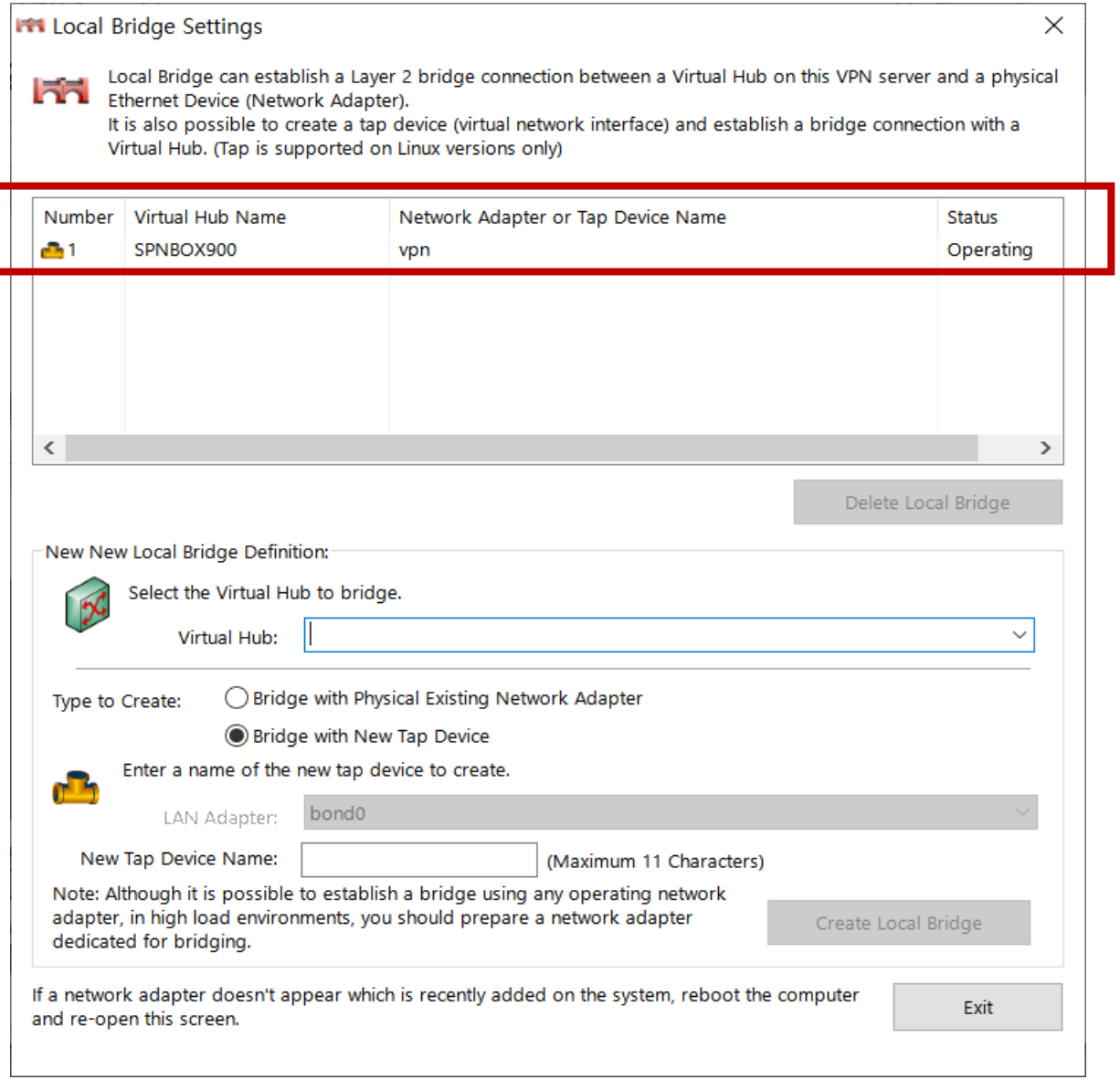




3. SPN Gateway & Bridge(2) – Gateway 설정(9)

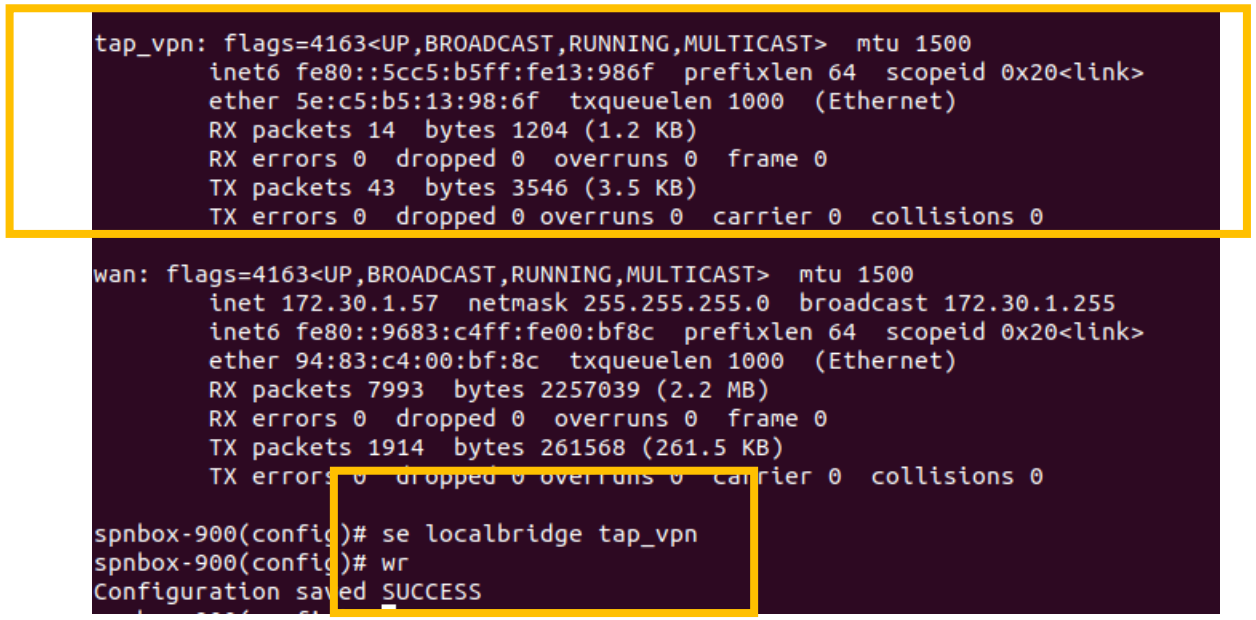


Virtual Hub의 동작 원리



3. SPN Gateway & Bridge(2) – Gateway 설정(10)

SPNBox-900 CLI 설정 변경



참고 : SPNBox-900 WebUI에서도 이 설정을 해 줄 수 있다[TBD].

3. SPN Gateway & Bridge(2) – Gateway 설정(11)

SPN Gateway	중요 설정 정보 요약
a) Admin password	**spnbox1234**
b) Local IP address	**172.30.1.57** (이 정보는 실제로 망에 연결된 VPN Gateway WAN IP를 입력해 주어야 함) **[정정] 192.168.8.1 즉 LAN IP를 입력하도록 하자.**
c) Virtual Hub	**SPNBOX900** 참고: Virtual Hub Name은 **SPNBOX$model_number** 형태로 입력한다. Hub password: **hub1234**
d) Virutla Hub을 이용할 사용자 정보	Id: **spnuser** Pass: **spnuser1234** 참고: 복수의 VPN 사용자가 VPN Server에 붙을 경우 각각의 사용자 id가 필요할 것이나, 일단은 단순화 차원에서 같은 id/password를 사용하는 것으로 하자.
e) Local Bridge interface 명	**vpn** 참고: SPNBox 내에서는 tap_vpn 이라는 virtual interface가 생성된다. 반드시 위의 명칭을 사용하기 바란다.

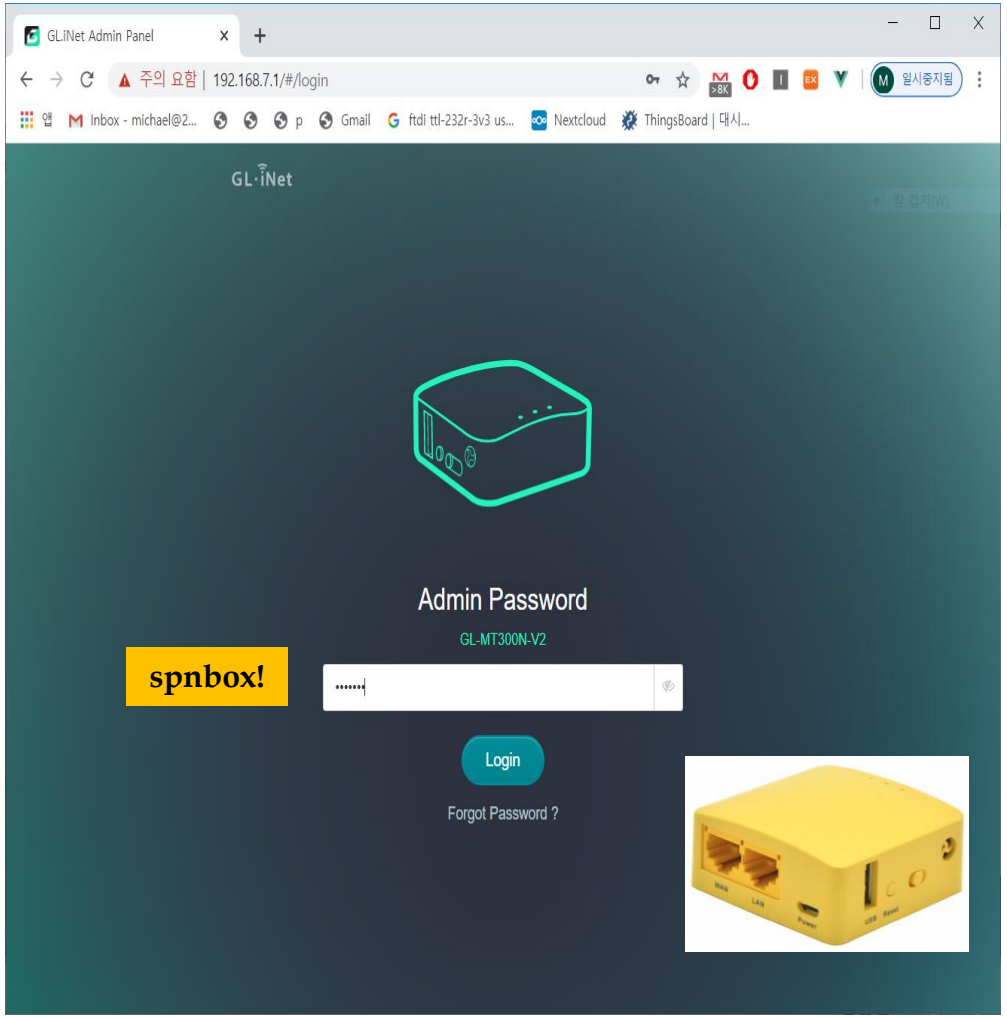
참고: 위의 설정 중 고객이 실제 field 상황에 맞게 재 수정해 주어야 하는 부분은 Local IP address 뿐이다.

- 아니다. 아무것도 없다.

3. SPN Gateway & Bridge(2) – Gateway 설정(12)

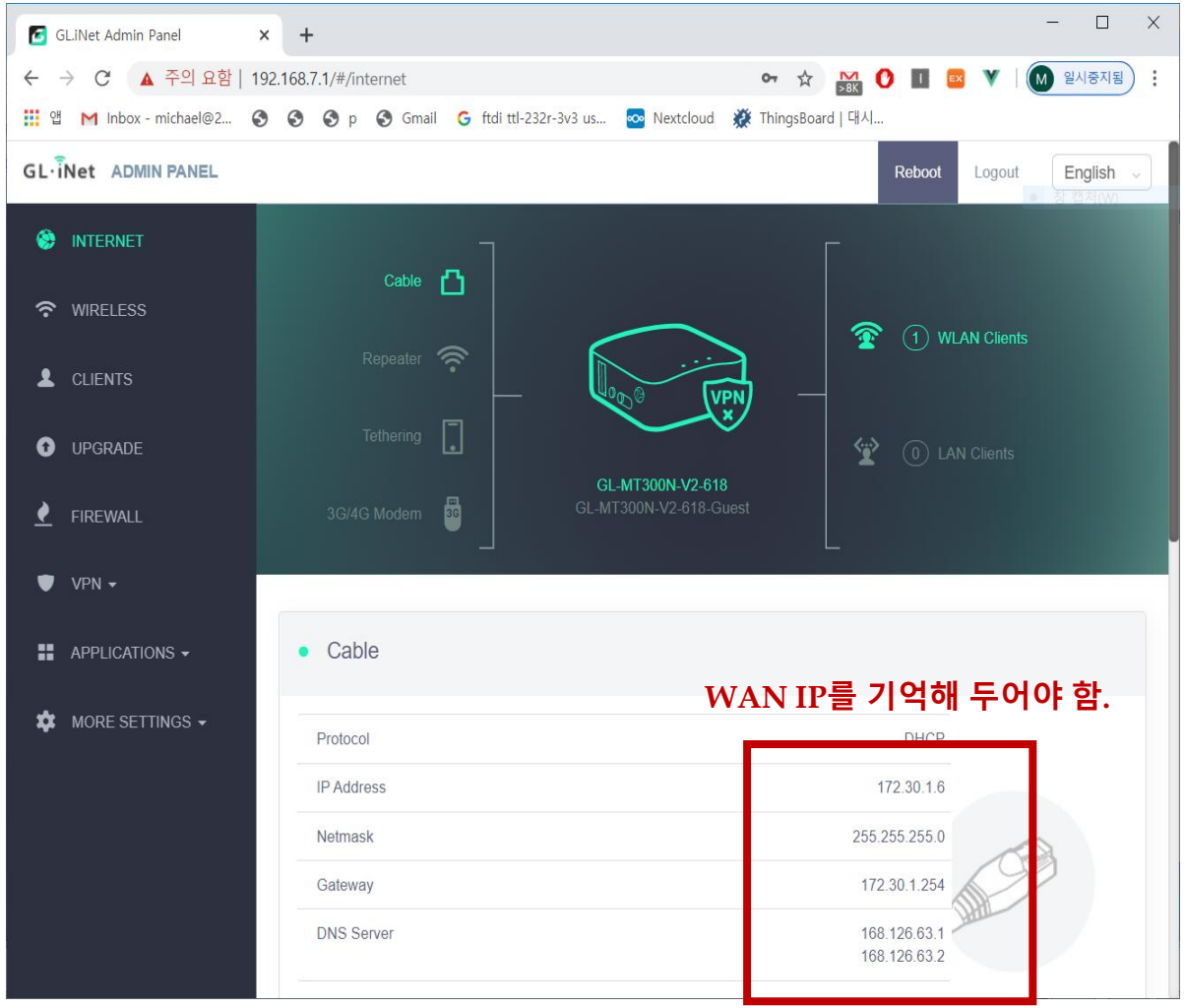
SPN Gateway	추가 변경 사항
a) Keepalive server	Keepalive.softether.org => www.2ipco.com
b) Encryption Algorighm Name	AES256-SHA => AES256-GCM-SHA256
c) Number of TCP Connections	1 => 8
d) 사용자 계정	개별 생성하는게 맞겠다. Id: email_id(@ 앞 string), pass: email_id1234

3. SPN Gateway & Bridge(3) – Bridge 설정(1)



LAN: 192.168.7.0/24

SPNBox-200
SPN Bridge



WAN IP를 기억해 두어야 함.

3. SPN Gateway & Bridge(3) – Bridge 설정(2)

```
SPNBox-200(config)# se enable  vbridge
SPNBox-200(config)# wr
Configuration saved SUCCESS
SPNBox-200(config)# show se  vbridge
SE daemon(pid 15352 15351) is alive.
================================================================================
15351 root      4512 S<   /usr/libexec/softethervpn/vpnbridge execsvc
15352 root     19244 S<   /usr/libexec/softethervpn/vpnbridge execsvc
================================================================================
SPNBox-200(config)#
```

1) VPN Bridge 구동

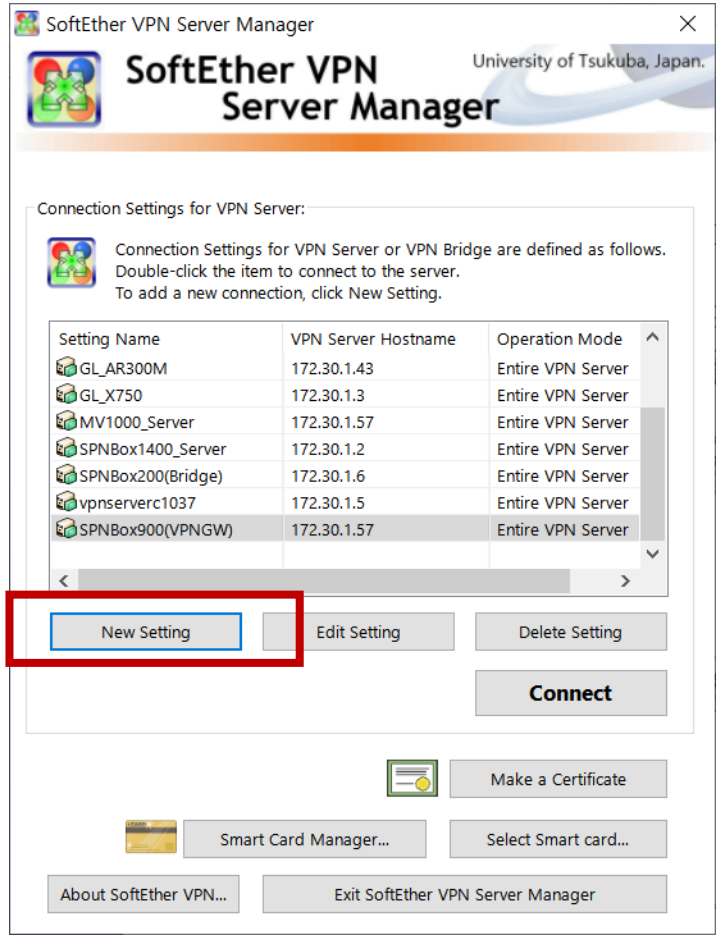
```
SPNBox-200(config)# se vcmd run
vpncmd command - SoftEther VPN Command Line Management Utility
SoftEther VPN Command Line Management Utility (vpncmd command)
Version 4.25 Build 9656   (English)
Compiled 2018/01/15 09:33:22 by yagi at pc33
Copyright (c) SoftEther VPN Project. All Rights Reserved.

By using vpncmd program, the following can be achieved.

1. Management of VPN Server or VPN Bridge
2. Management of VPN Client
3. Use of VPN Tools (certificate creation and Network Traffic Speed Test Tool)

Select 1, 2 or 3: 1

Specify the host name or IP address of the computer that the destination VPN Server or
VPN Bridge is operating on.
By specifying according to the format 'host name:port number', you can also specify the
 port number.
(When the port number is unspecified, 443 is used.)
If nothing is input and the Enter key is pressed, the connection will be made to the po
rt number 8888 of localhost (this computer).
Hostname of IP Address of Destination:

If connecting to the server by Virtual Hub Admin Mode, please input the Virtual Hub nam
e.
If connecting by server admin mode, please press Enter without inputting anything.
Specify Virtual Hub Name:
Connection has been established with VPN Server "localhost" (port 443).

You have administrator privileges for the entire VPN Server.

VPN Server>ServerPasswordSet
ServerPasswordSet command - Set VPN Server Administrator Password
Please enter the password. To cancel press the Ctrl+D key.

Password: **********
Confirm input: **********

The command completed successfully.

VPN Server>exit
SPNBox-200(config)#
```

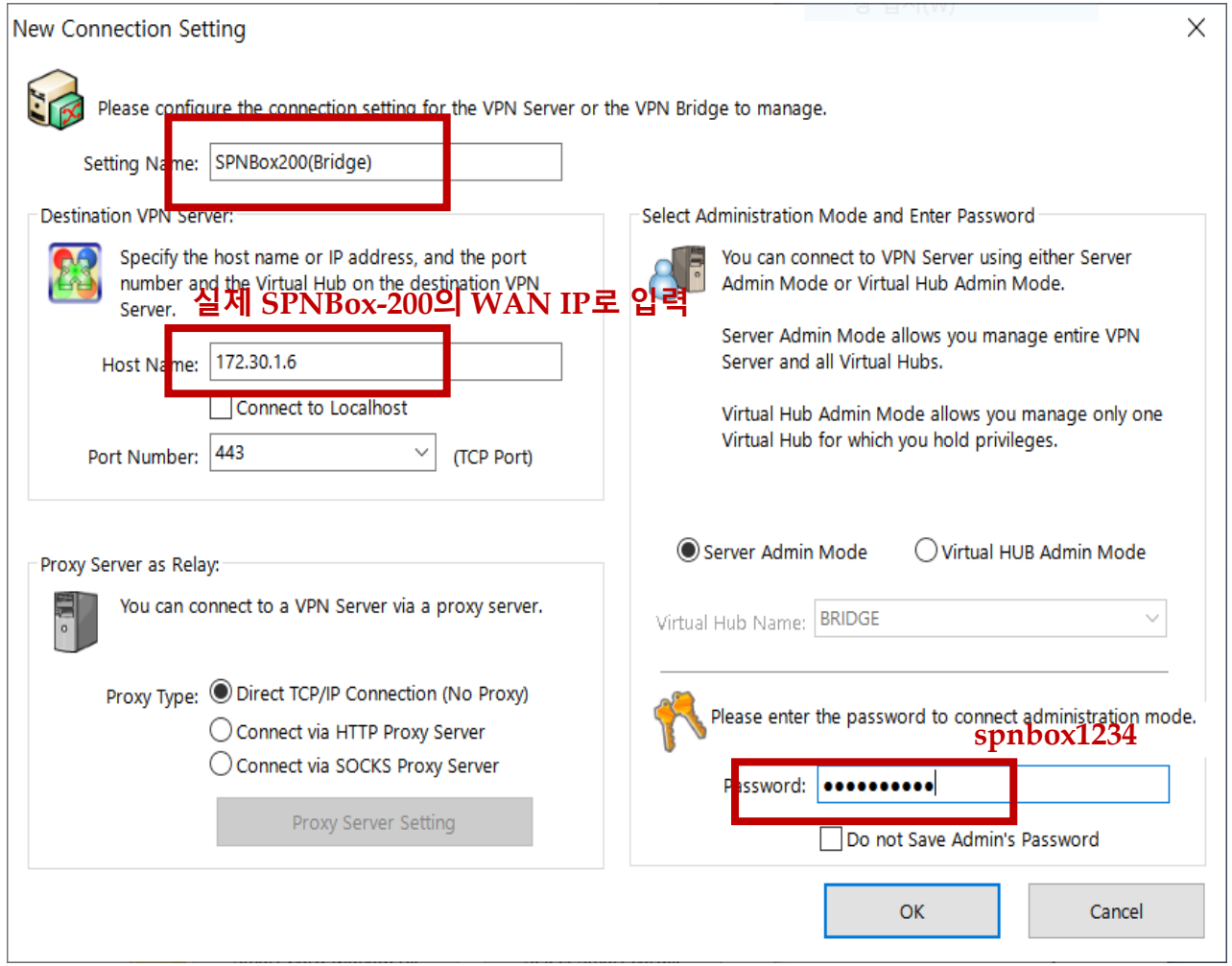
<Enter> 입력

<Enter> 입력

2) VPN Bridge admin 패스워드 설정
(pass: spnbox1234)

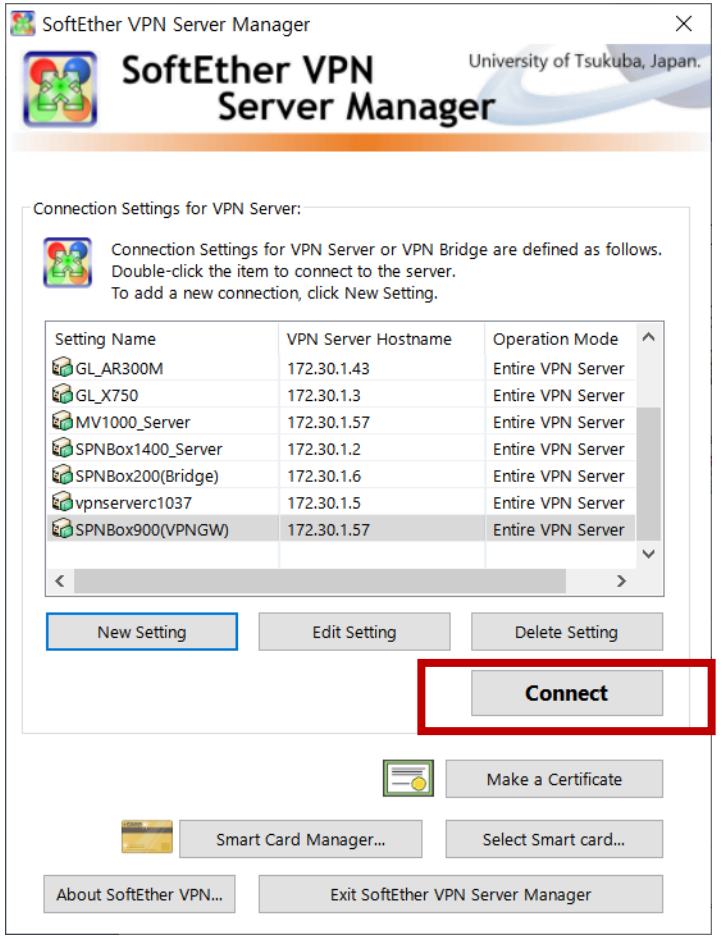
3. SPN Gateway & Bridge(3) – Bridge 설정(3)

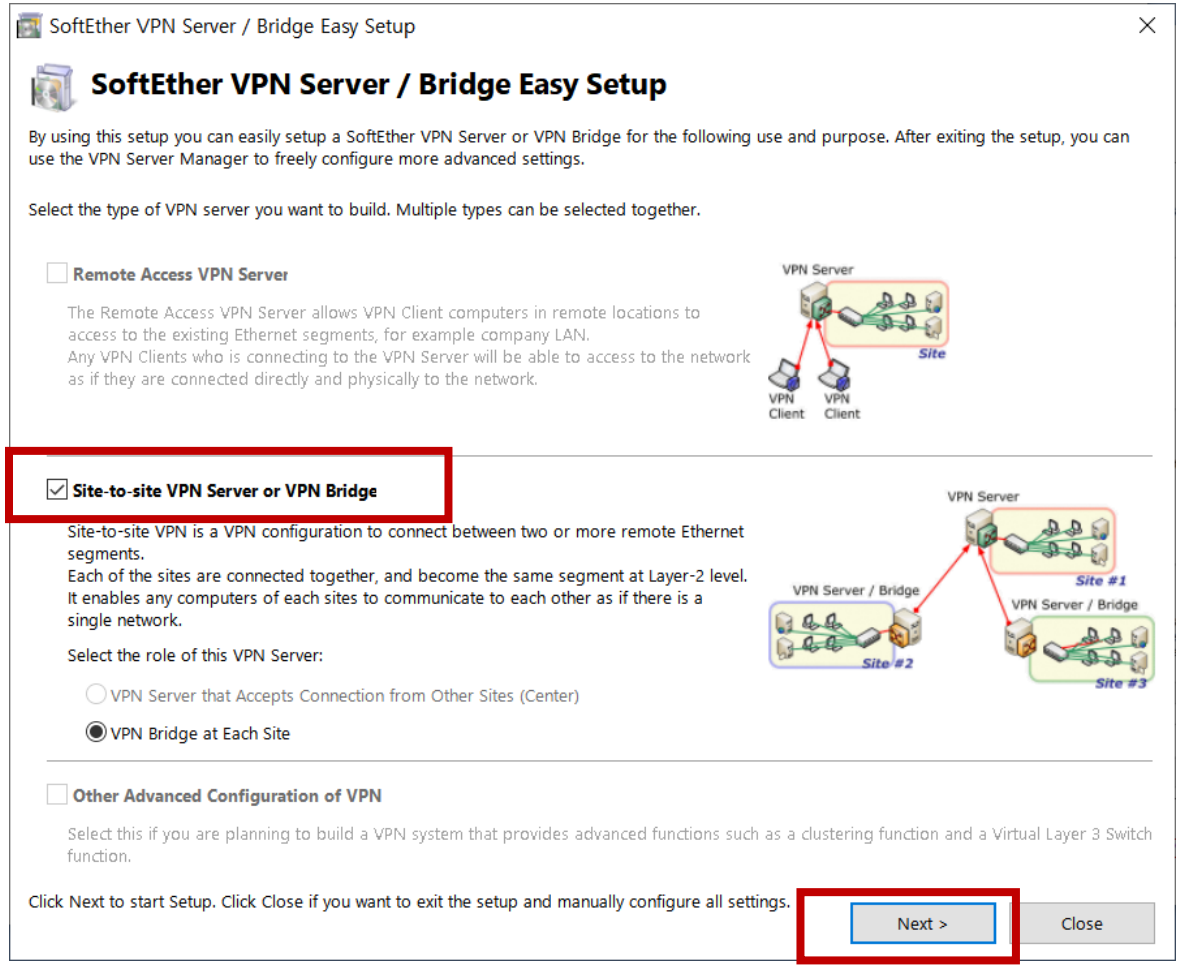




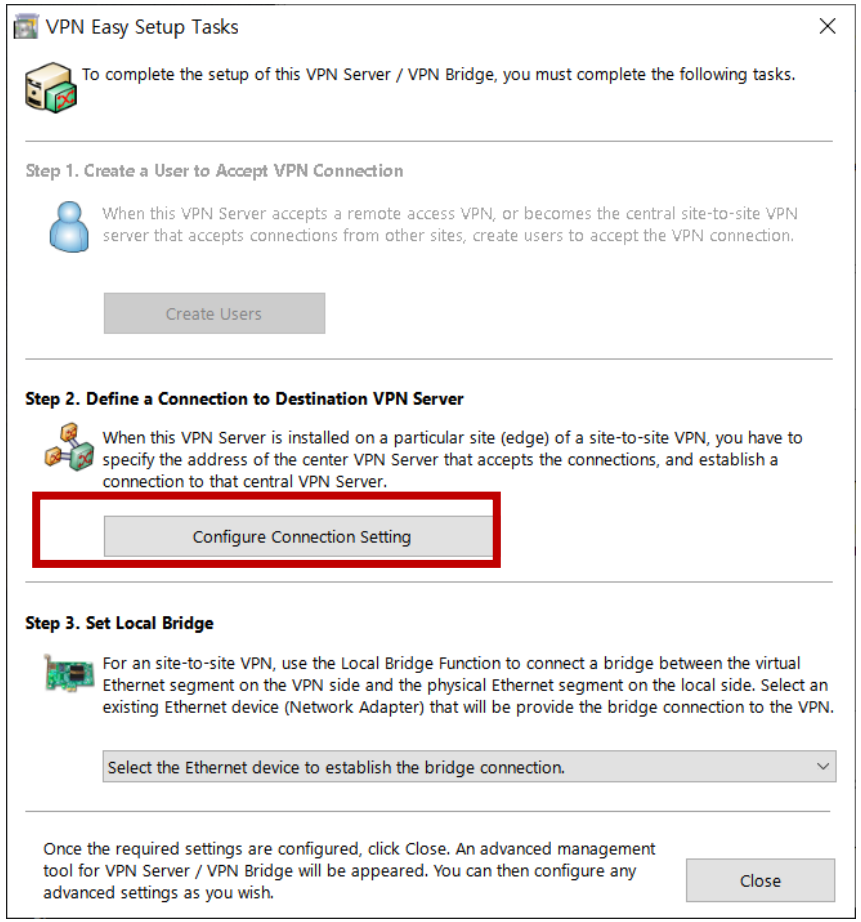
주의: 위의 설정을 하기 위해서는 notebook PC가 SPNBox-200과 동일한 네트워크 환경(예: 같은 무선 AP에 연결)에 있어야 한다.

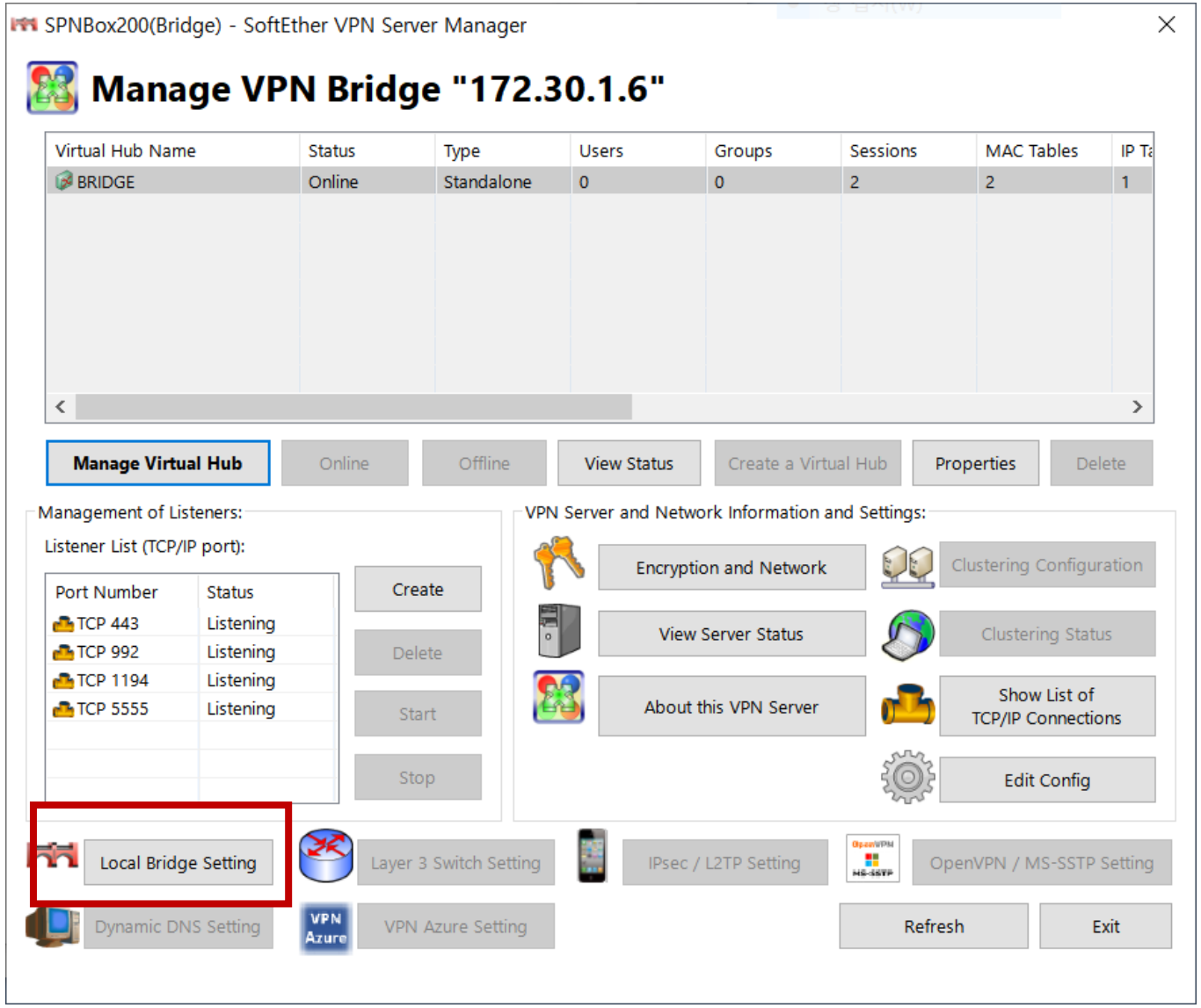
3. SPN Gateway & Bridge(3) – Bridge 설정(4)



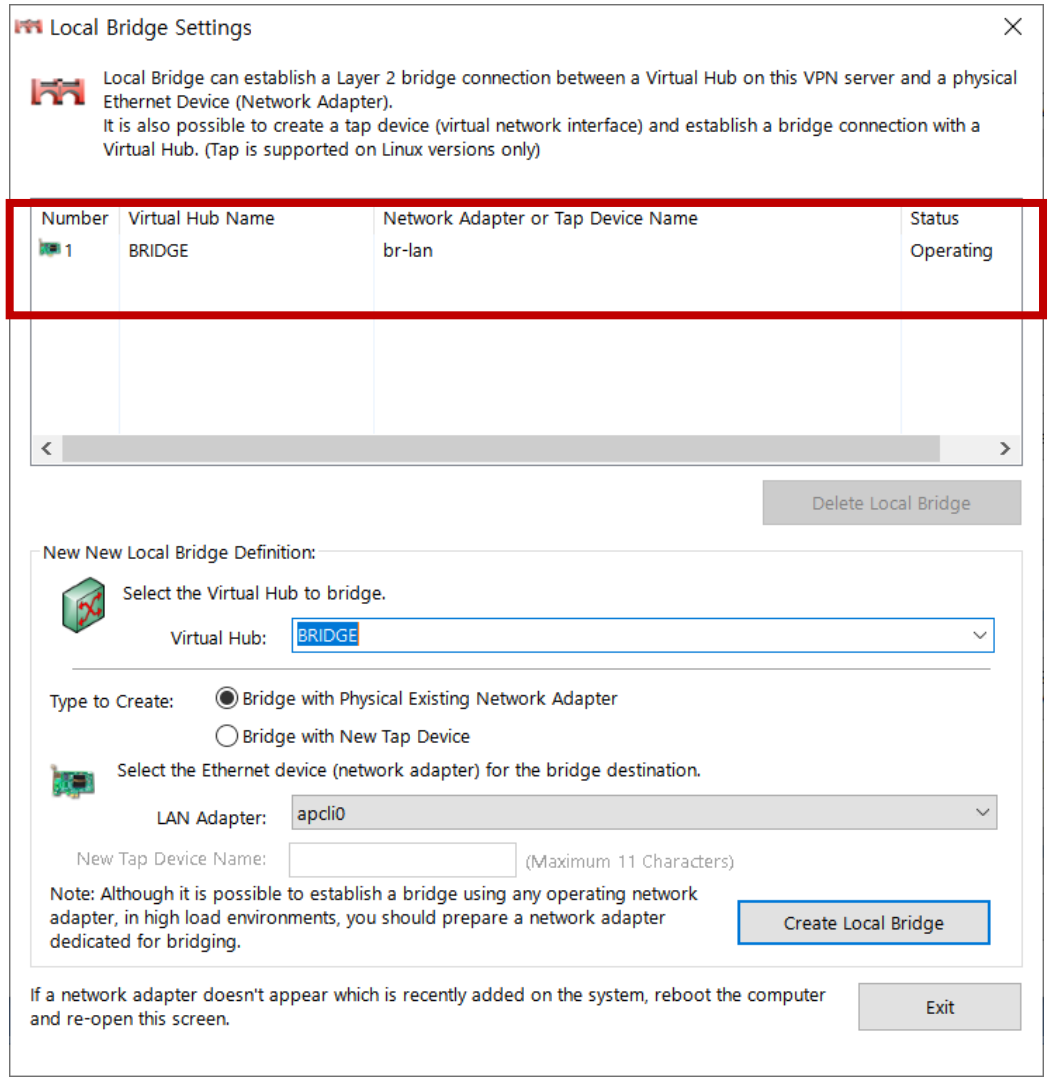


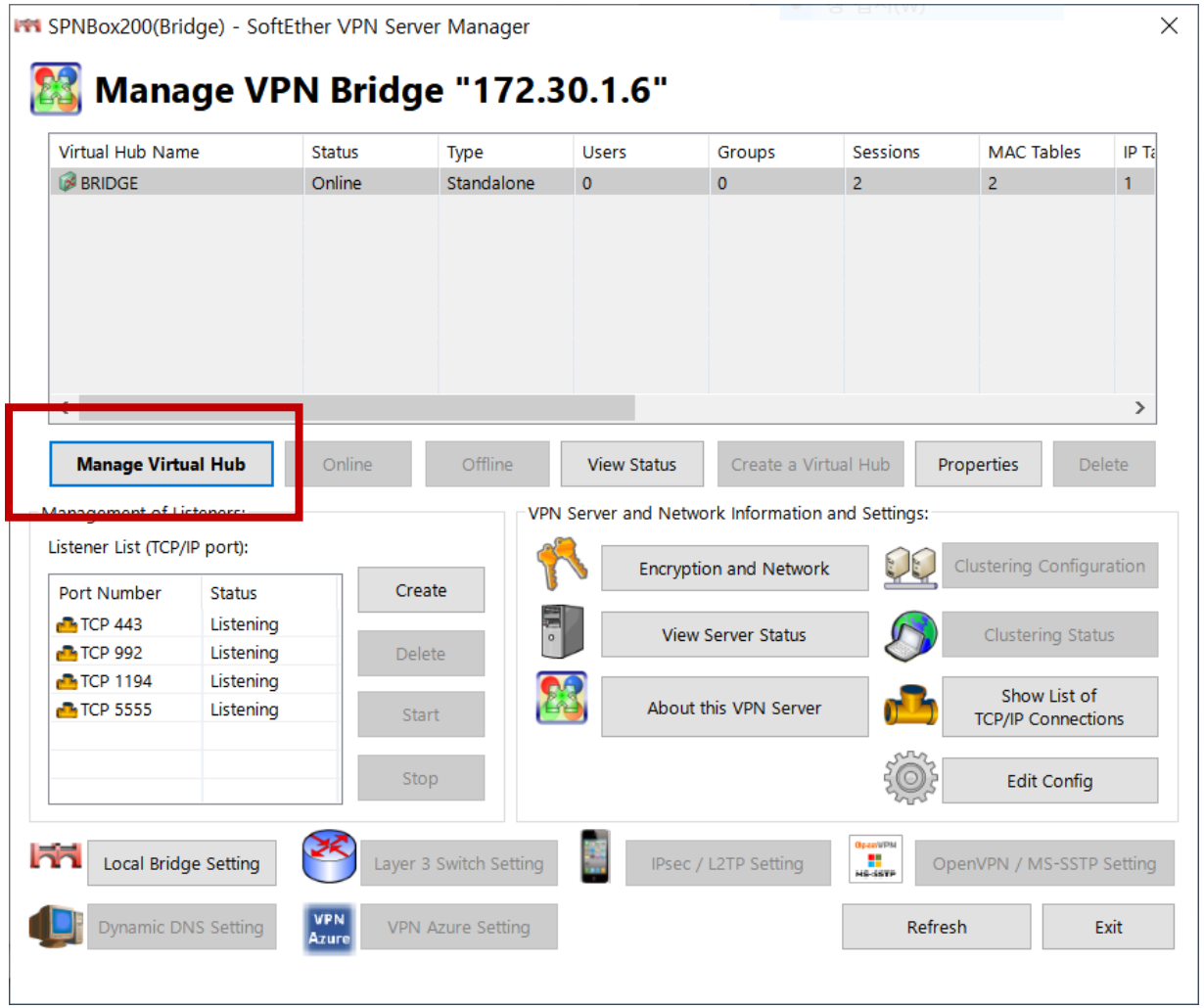
3. SPN Gateway & Bridge(3) – Bridge 설정(5)





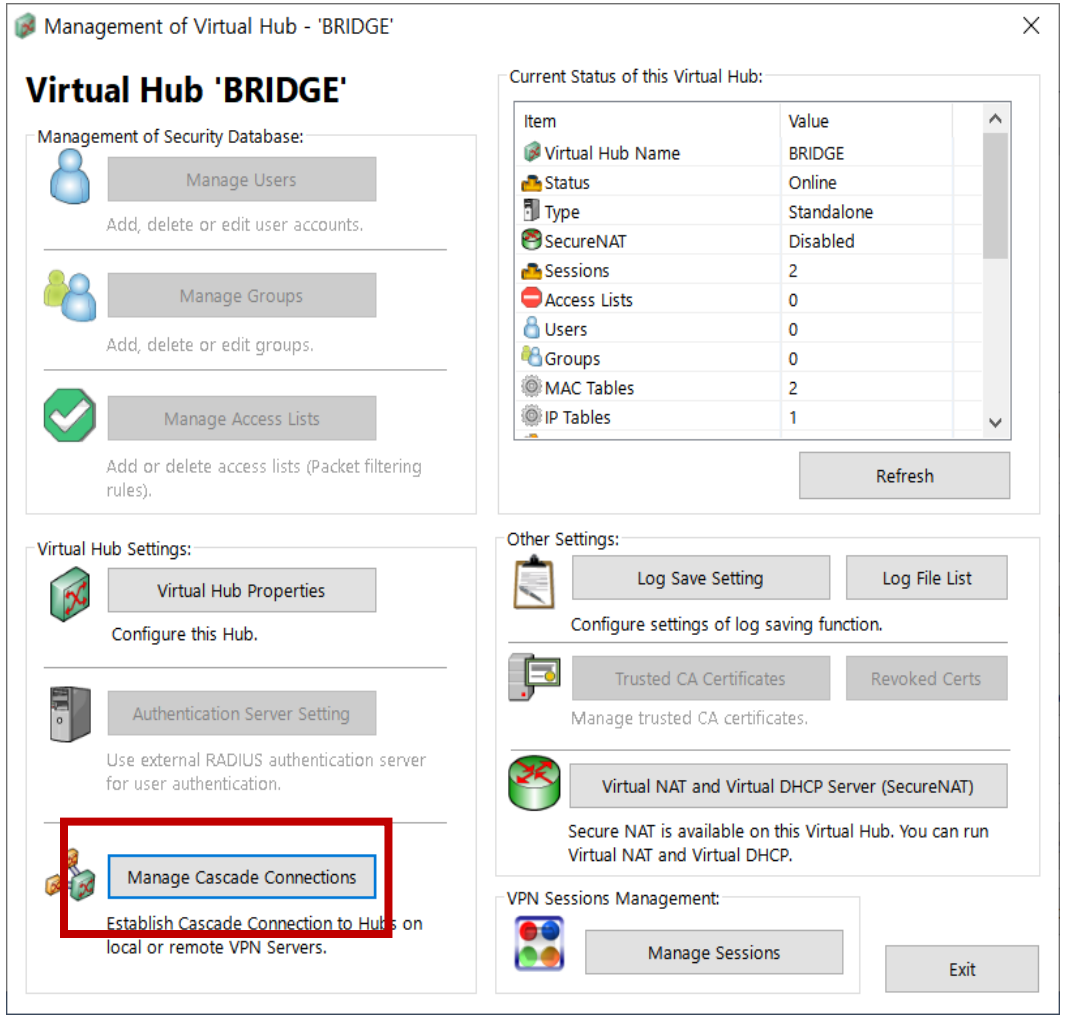
3. SPN Gateway & Bridge(3) – Bridge 설정(6)

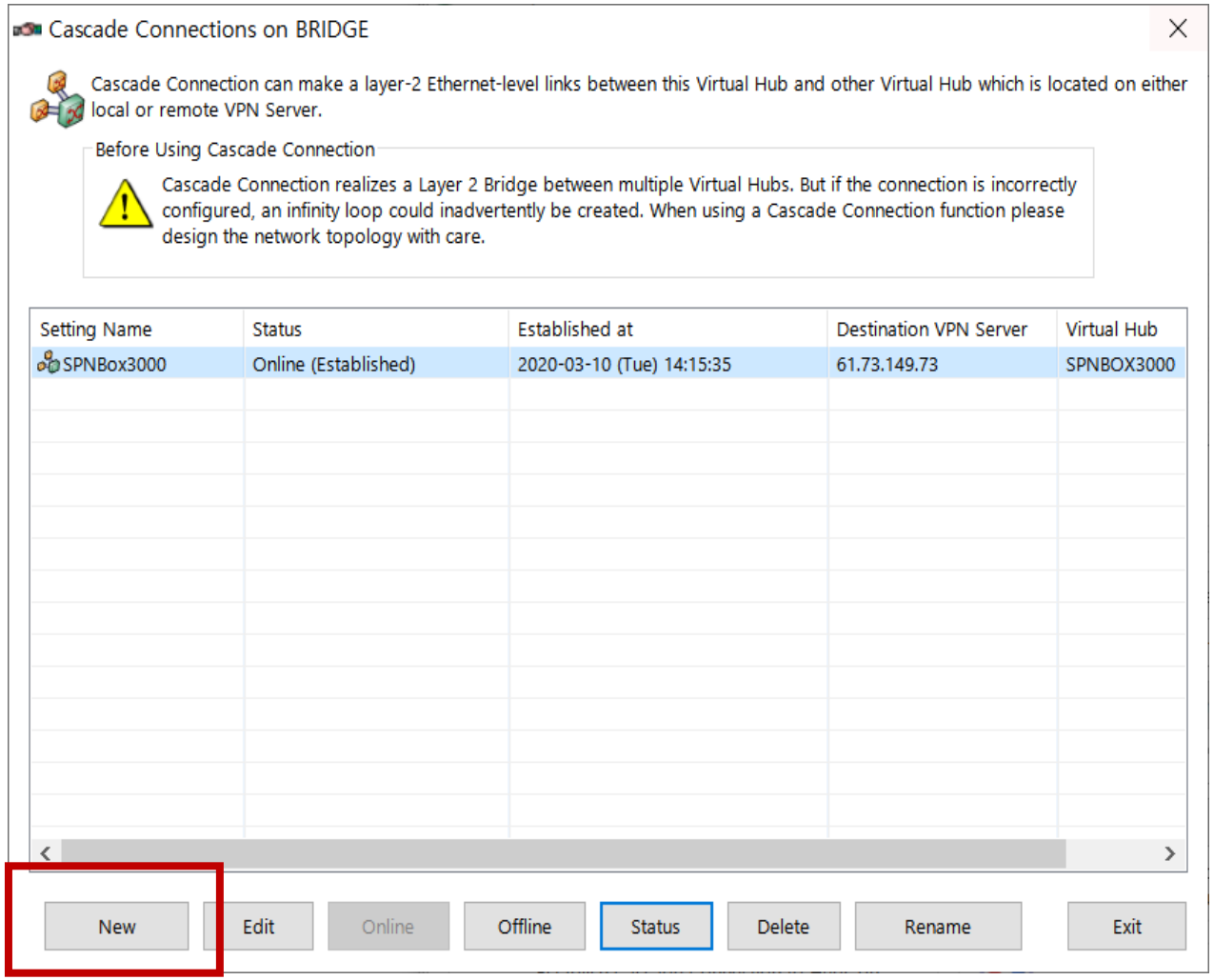




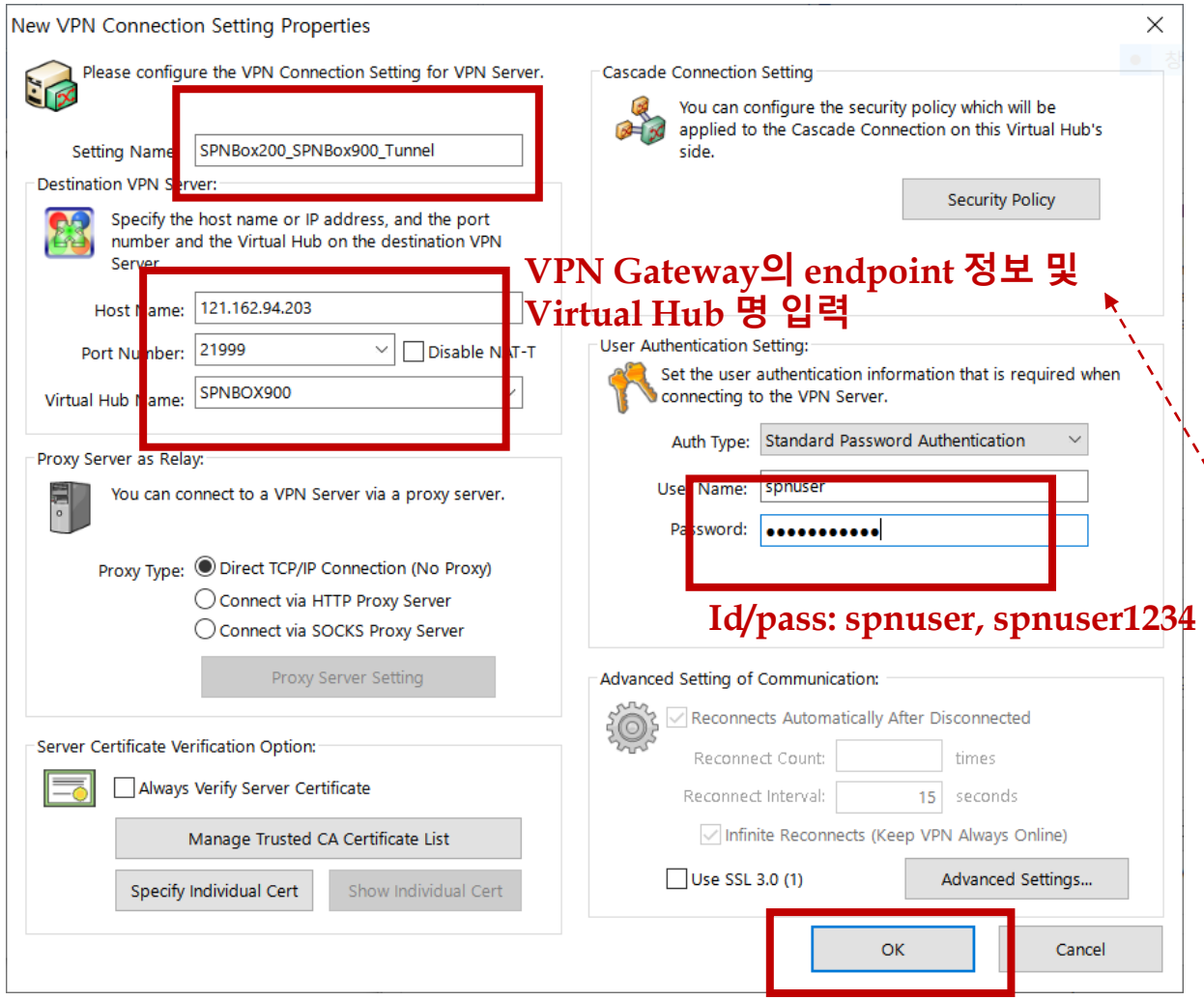
이 화면은 변경할 필요가 없는 화면임.

3. SPN Gateway & Bridge(3) – Bridge 설정(7)



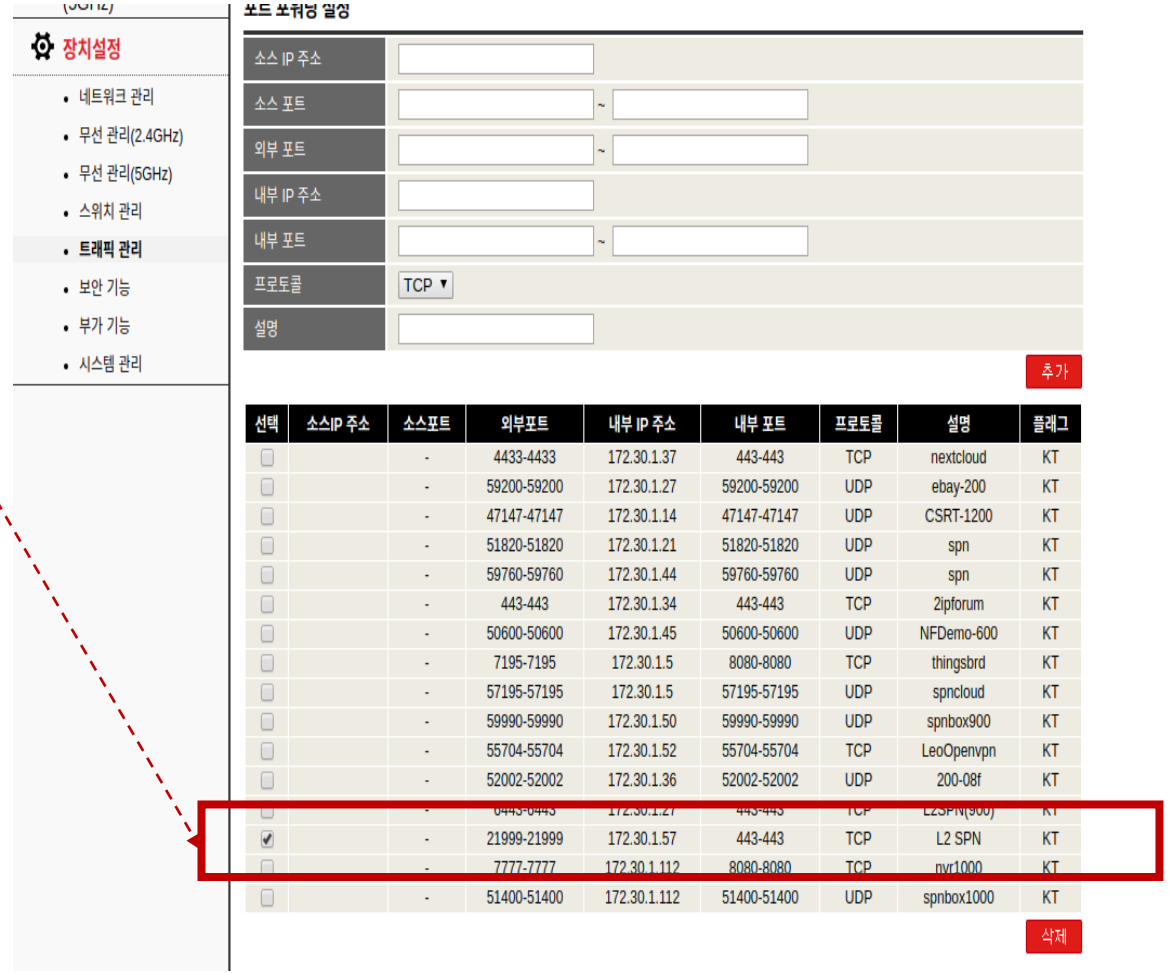


3. SPN Gateway & Bridge(3) – Bridge 설정(8)



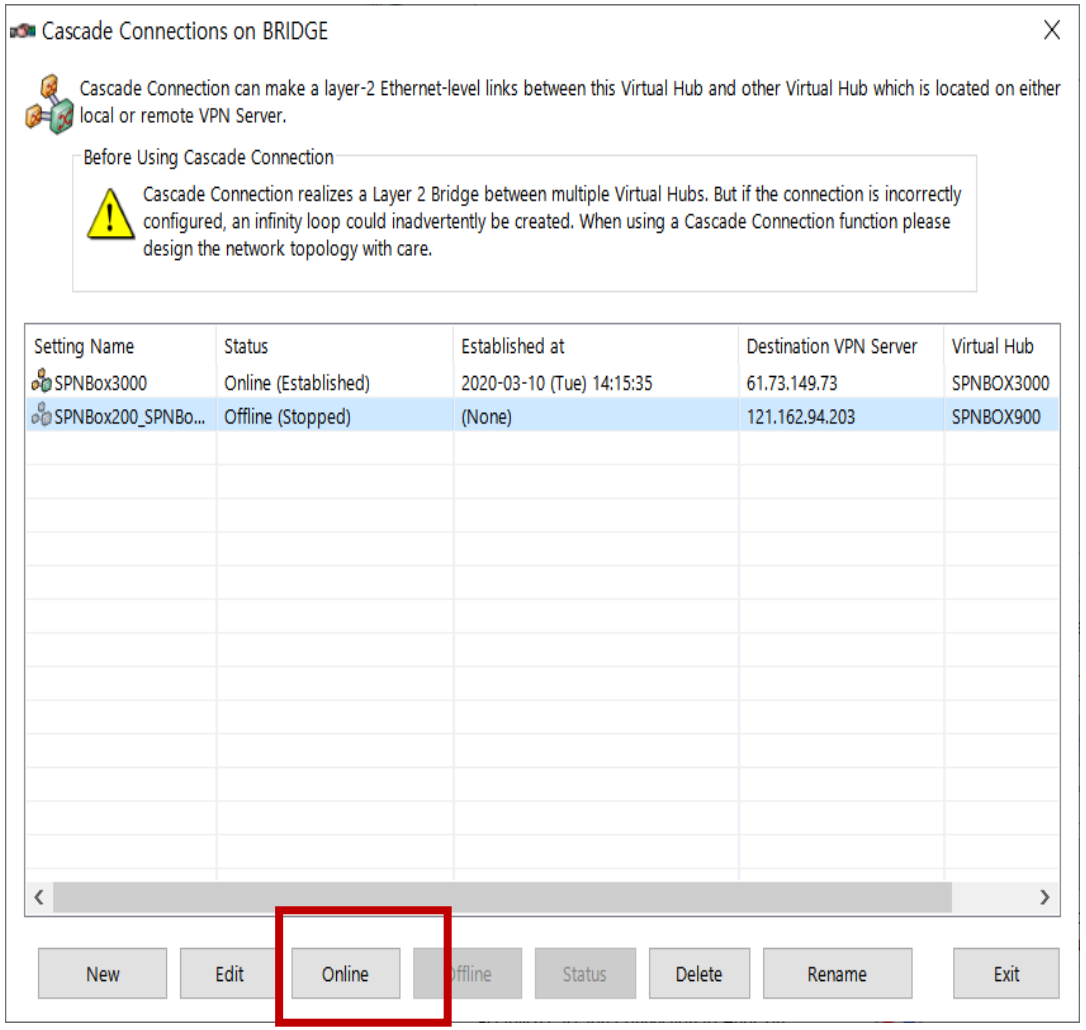
VPN Gateway의 endpoint 정보 및 Virtual Hub 명 입력

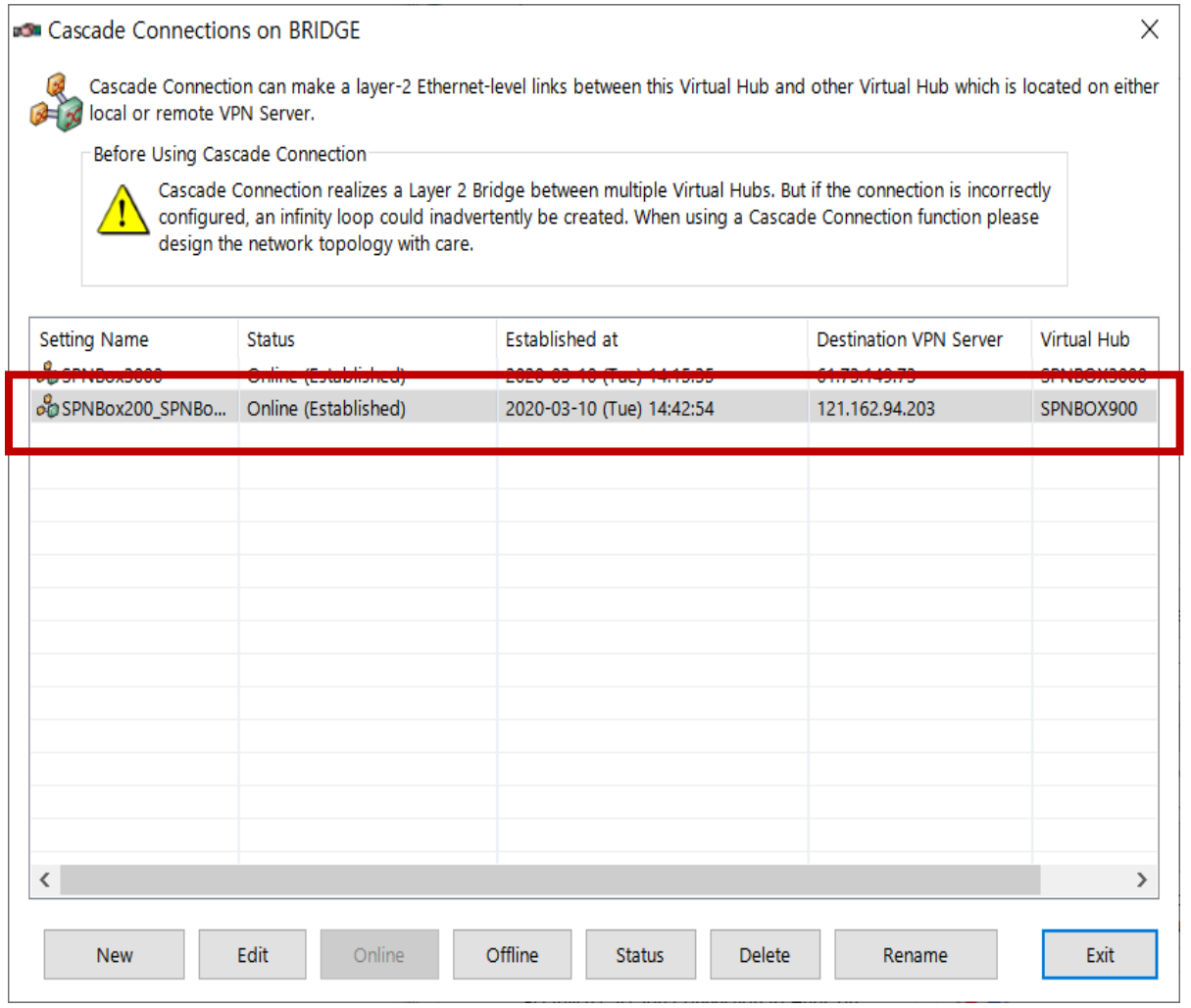
Id/pass: spnuser, spnuser1234



VPN Gateway 앞단의 Firewall or AP 등에서 Port Forwarding 설정을 해 주어야 한다.

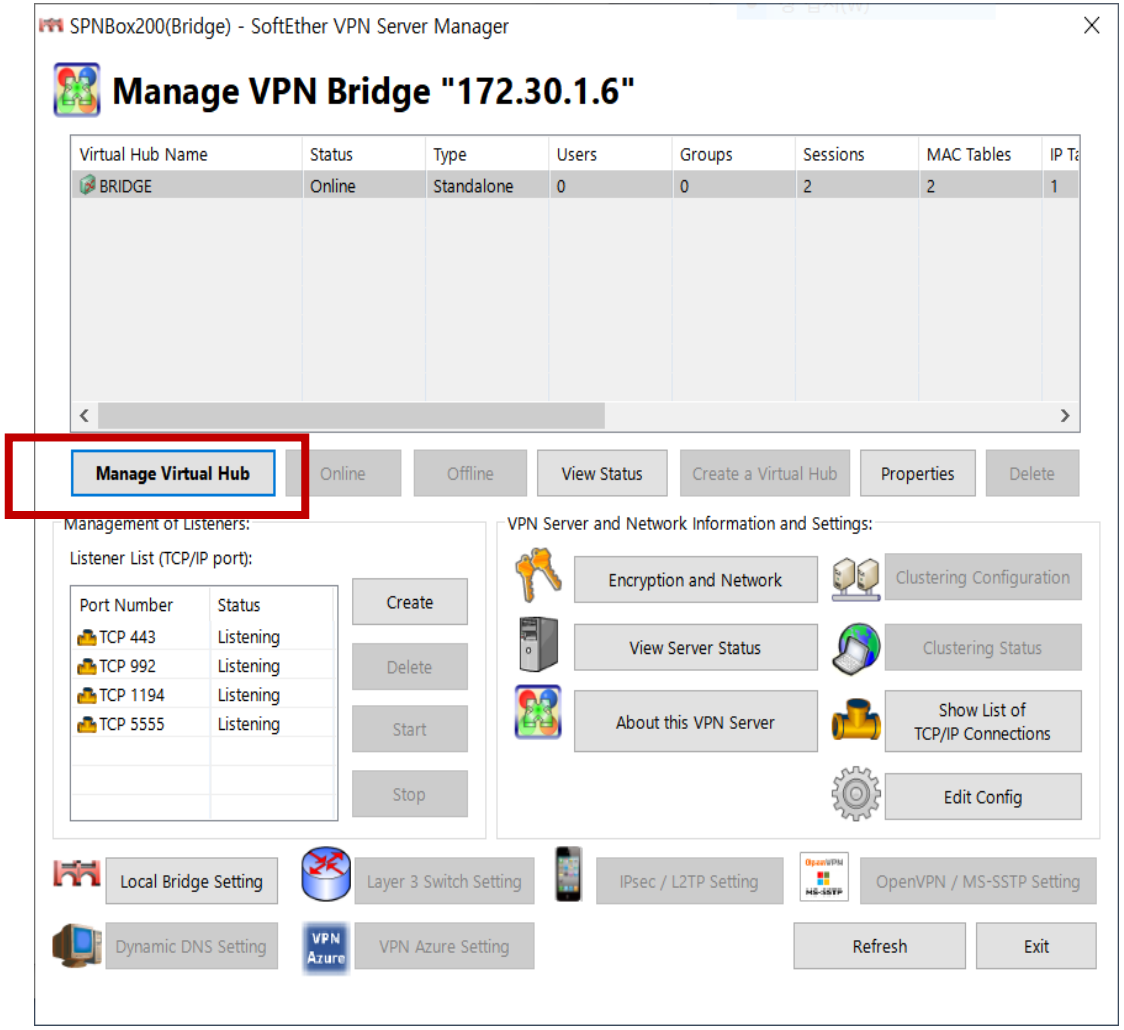
3. SPN Gateway & Bridge(3) – Bridge 설정(9)

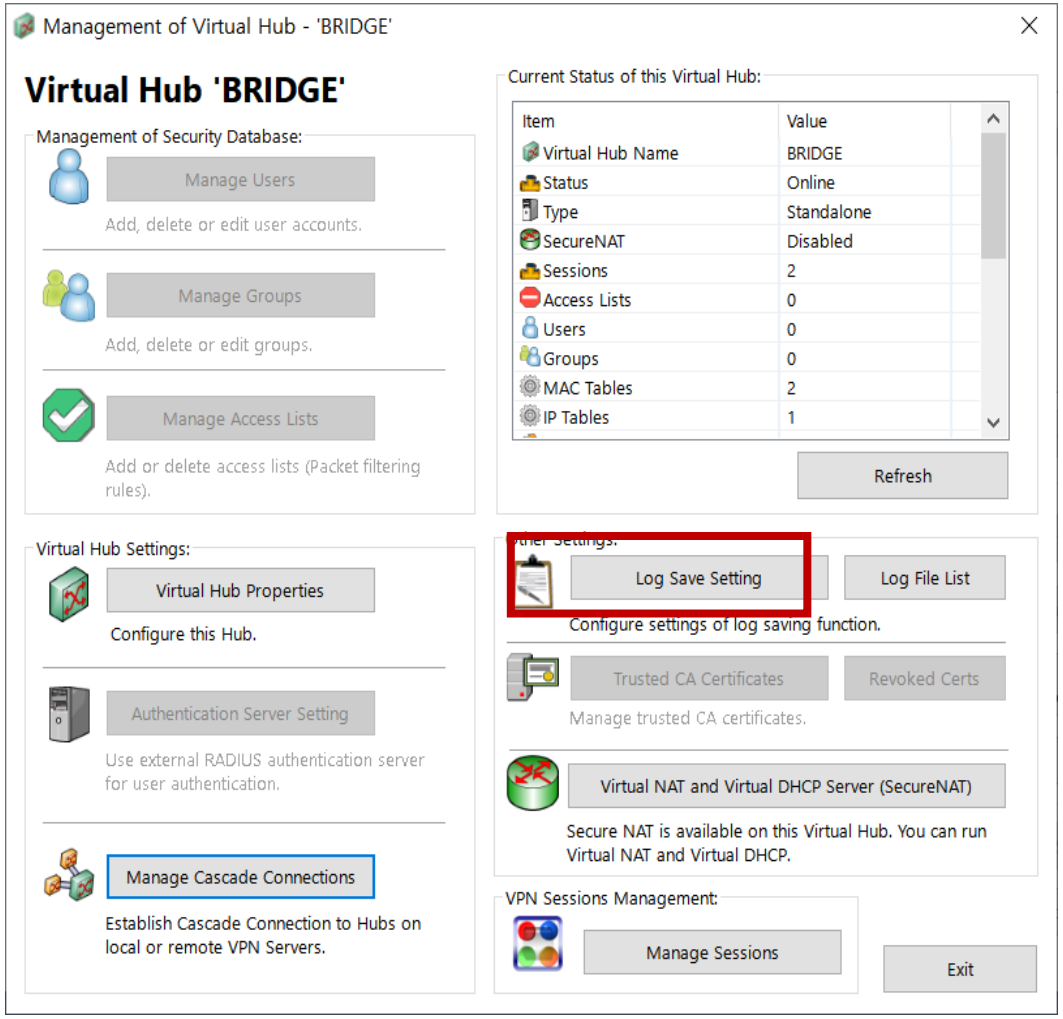




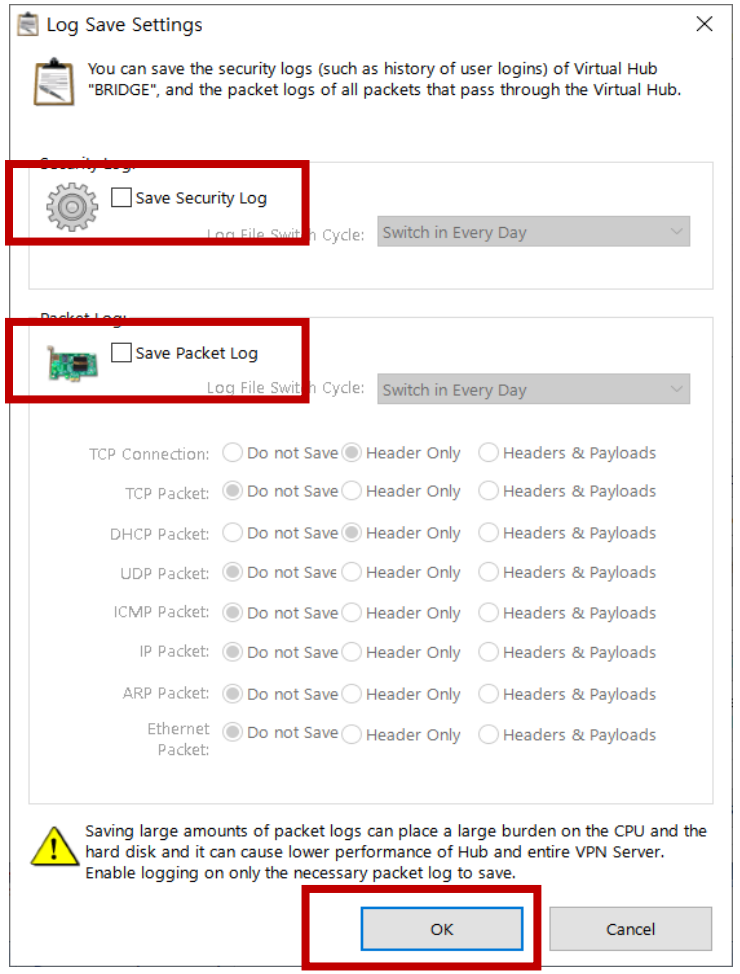
VPN Tunnel(VPN Bridge ⇔ VPN Gateway) 연결 성공

3. SPN Gateway & Bridge(3) – Bridge 설정(10)





3. SPN Gateway & Bridge(3) – Bridge 설정(11)



SPNBox-200은 disk(NOR flash) 공간이 매우 부족하니 반드시 Log 출력을 disable하도록 하자.

3. SPN Gateway & Bridge(3) – Bridge 설정(12)

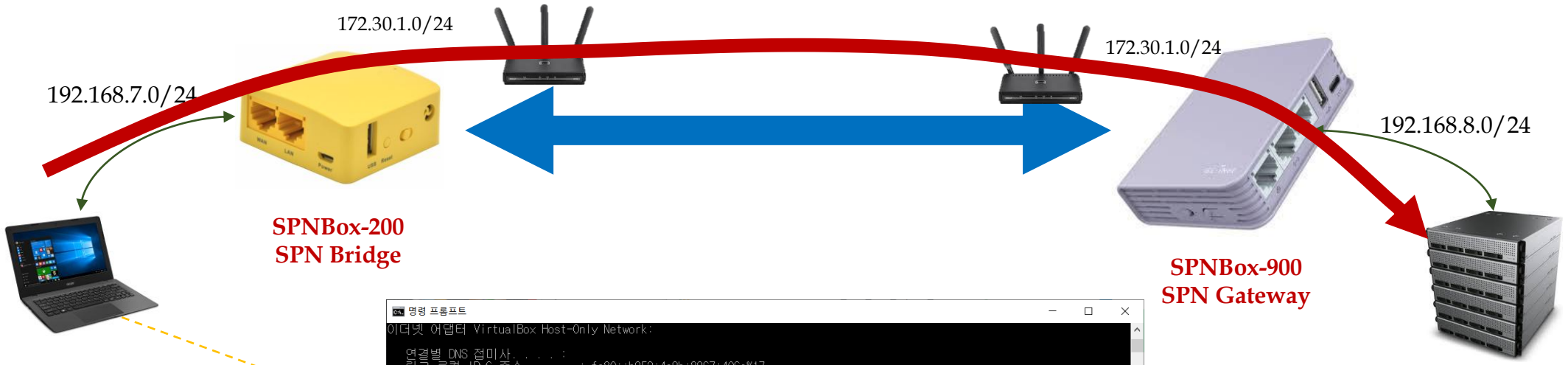
SPN Bridge	중요 설정 정보 요약
a) Admin password	**Spnbox1234** (SPN Bridge의 admin password 임)
b) Local IP address	**172.30.1.6** (이 정보는 실제로 망에 연결된 VPN Bridge 장비의 WAN IP를 입력해 주어야 함) **[정정] 192.168.7.1 즉 LAN IP를 입력하도록 하자.**
c) Virtual Hub	**BRIDGE** (default로 이미 생성되어 있음)
d) Cascade 연결	VPN Server endpoint IP address(공유기 WAN IP): **121.162.94.203** VPN Server endpoint Port: **21999** (포트 포워딩 설정 참조) User id/passwd: **spnuser/spnuser1234**
e) Log disable	**Security & Packet log 출력 제한**

<참고>

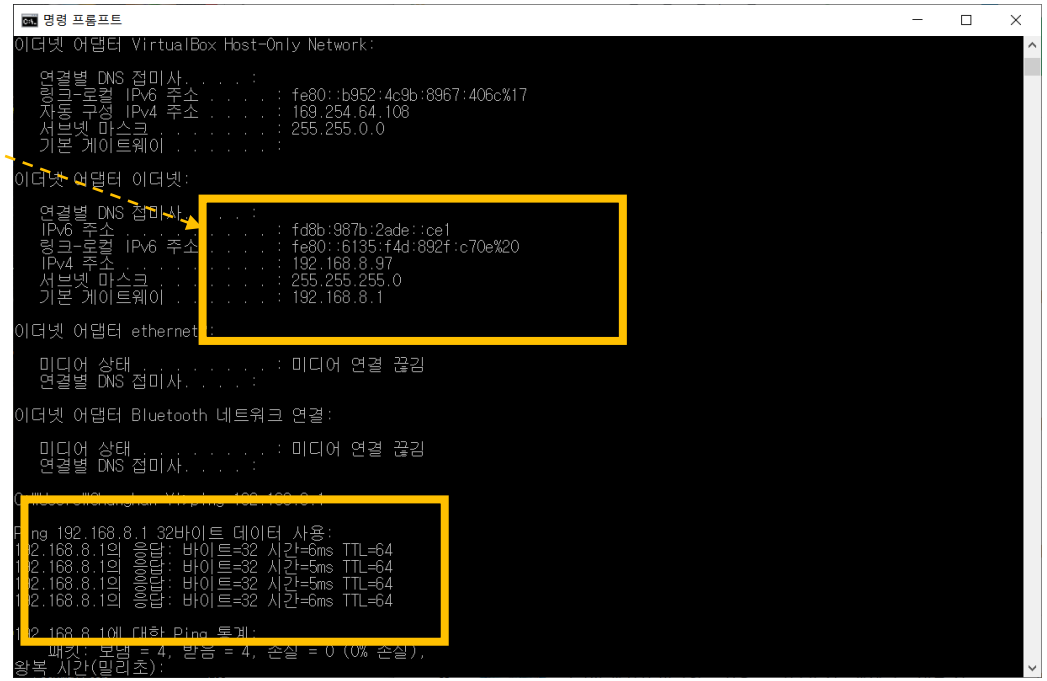
▪ 위의 설정 중 실제 고객이 field 상황에 맞게 재 수정해 주어야 하는 부분은 Cascade 연결 정보(VPN Server의 IP, Port) 뿐이다.

▪ Cascade 설정을 위해서는 사전에 VPN Gateway가 위치(사무실)한 Firewall(or AP)에서 Port forwarding 설정을 해 주어야만 한다.

3. SPN Gateway & Bridge(4) – VPN 연결 시험(1)

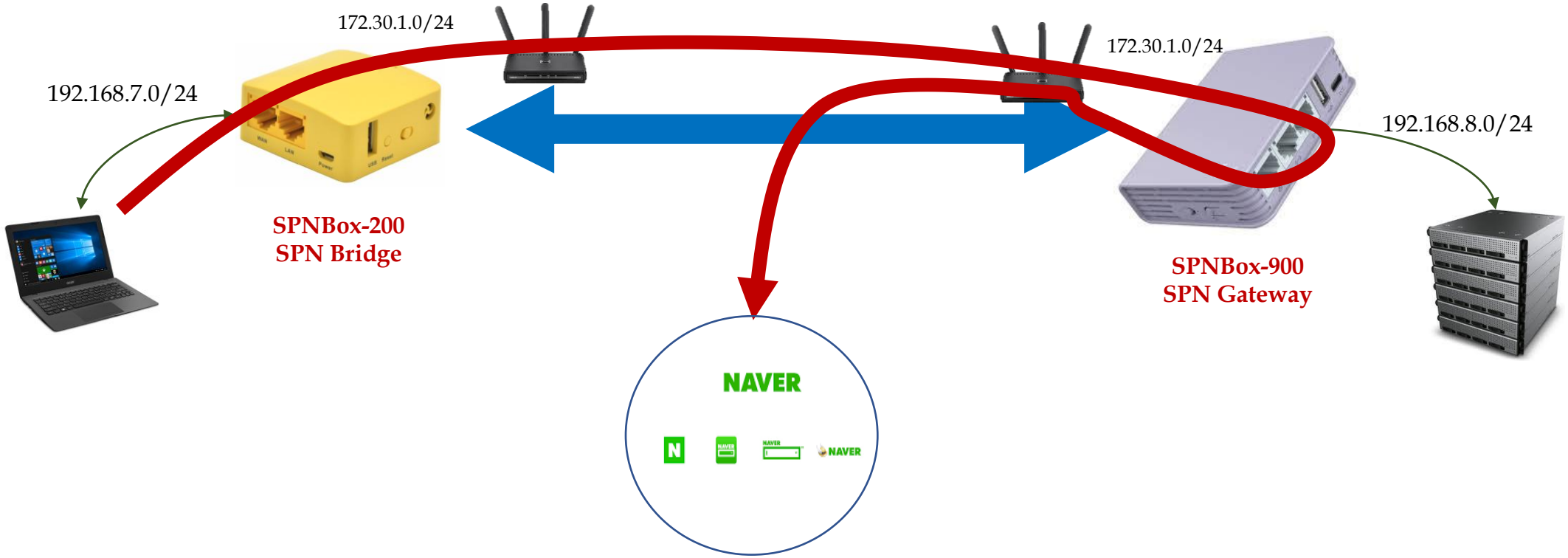


Windows PC IP 주소가 SPNBox-900 내부망 주소로 변경됨.



OK, 이 상태에서 인터넷 정상 연결

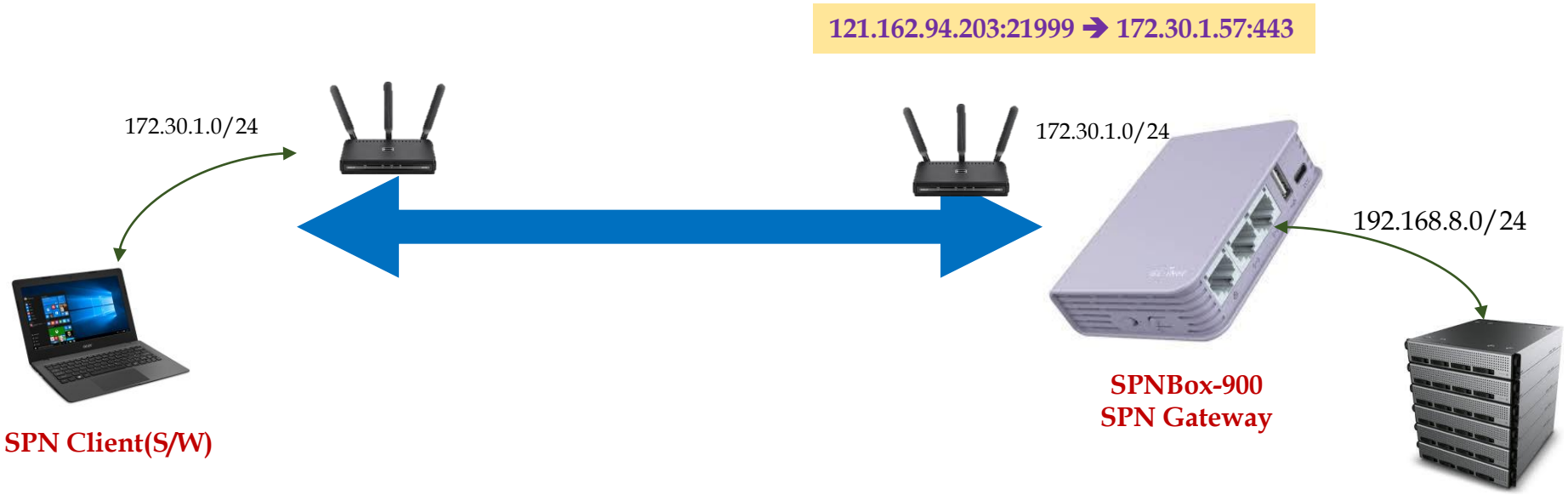
3. SPN Gateway & Bridge(4) – VPN 연결 시험(2)



참고: L2 SPN을 사용하여 인터넷을 접속할 경우, 위와 같이 패킷이 SPN Gateway를 경유하게 된다(느리다).
해법 1: 인터넷 접속이 목적이라면 Home AP에 직접 붙으면 된다.
해법 2: Windows PC의 IP 주소를 SPNBox-200의 LAN IP 대역(예: 192.168.7.100)으로 설정(static)해 준다.
이 경우, VPN 접속을 위해서는 다시 DHCP 설정으로 변경해주면 된다.

4. SPN Gateway & SPN Client
: 상세 Setup Guide

4. SPN Gateway & Client(1) – Testbed(1)



이 장에서는 위의 네트워크(테스트베드) 환경에서 VPN 연결 시험을 진행하도록 하겠습니다.

4. SPN Gateway & Client(1) – Testbed(2)

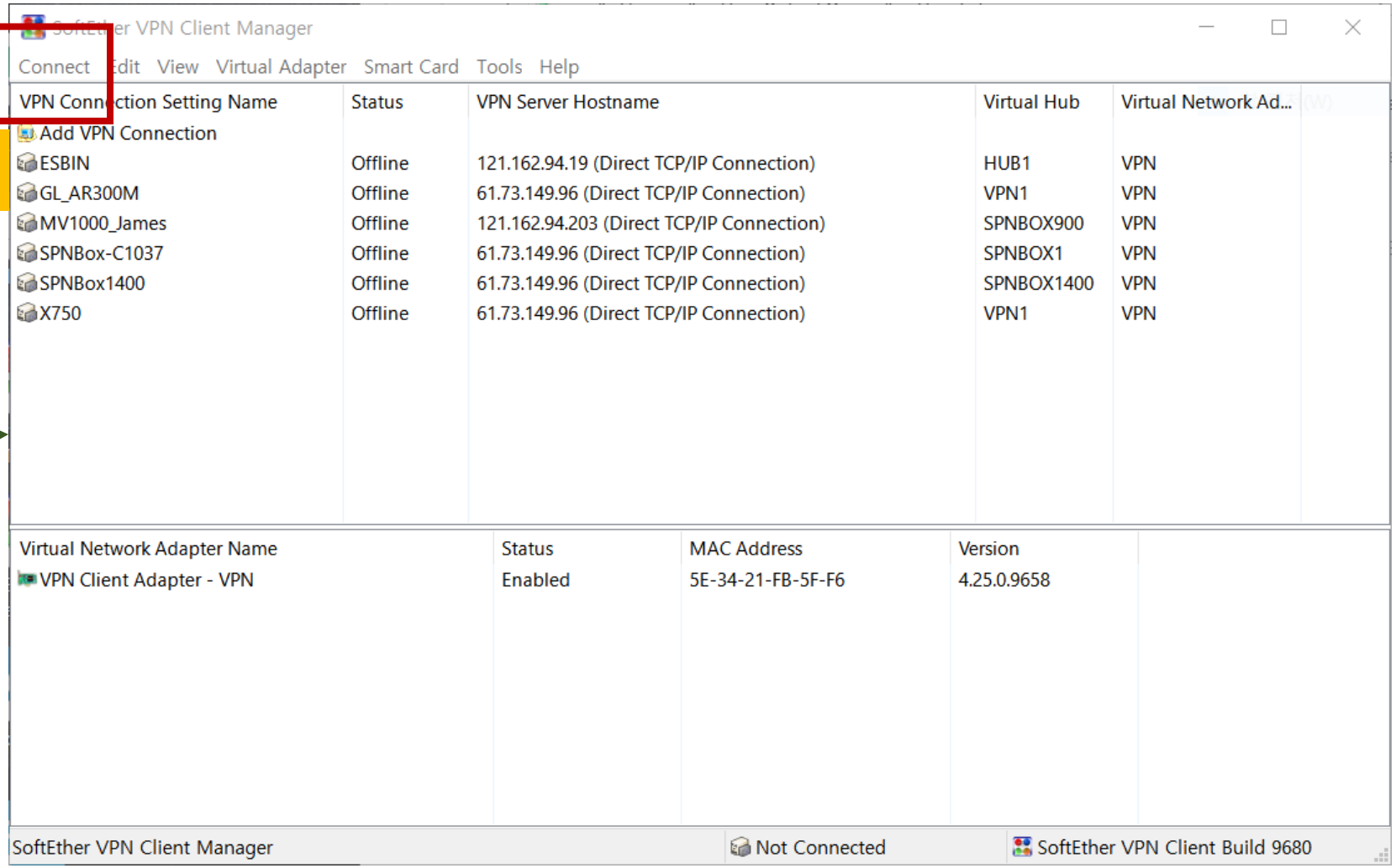
SPN Gateway	전체 설정 절차 요약
a)	VPN Server를 구동시키고, vpncmd(CLI: se vcmd run 명령)로 admin password를 설정한다(SPNBox CLI에서 수행)
b)	Windows PC에서 VPN Server Manager로 VPN Server에 접속한 후, 가장 기본적인 서버 설정(local ip address, port, admin password 입력)을 한다.
c)	Virtual Hub을 하나 추가한다. Default Virtual Hub을 사용해도 됨.
d)	Virtual Hub 사용을 위한 client 계정을 하나 등록한다.
e)	Local bridge를 하나 생성하고 SPNBox LAN bridge와 연결한다(SPNBox CLI에서 수행).

VPN Gateway 설정은 3장의 내용과 동일하므로, 여기서는 생략하기로 하자.

SPN Client	전체 설정 절차 요약
a)	SoftEther VPN home page에서 VPN Client Manager(for Windows) 버젼을 내려 받아 설치한다.
b)	Windows PC를 공유기에 연결한다.
c)	VPN Client Manager를 실행한 후, VPN 설정을 한다. 이때 아래 정보가 필요하다. ▪ VPN Server에서 추가한 Virtual Hub 사용을 위한 **사용자 계정 정보** ▪ Firewall or AP 안쪽에 VPN Server가 있을 경우, port forwarding 설정 및 이와 관련된 정보(**Firewall External IP, port**)

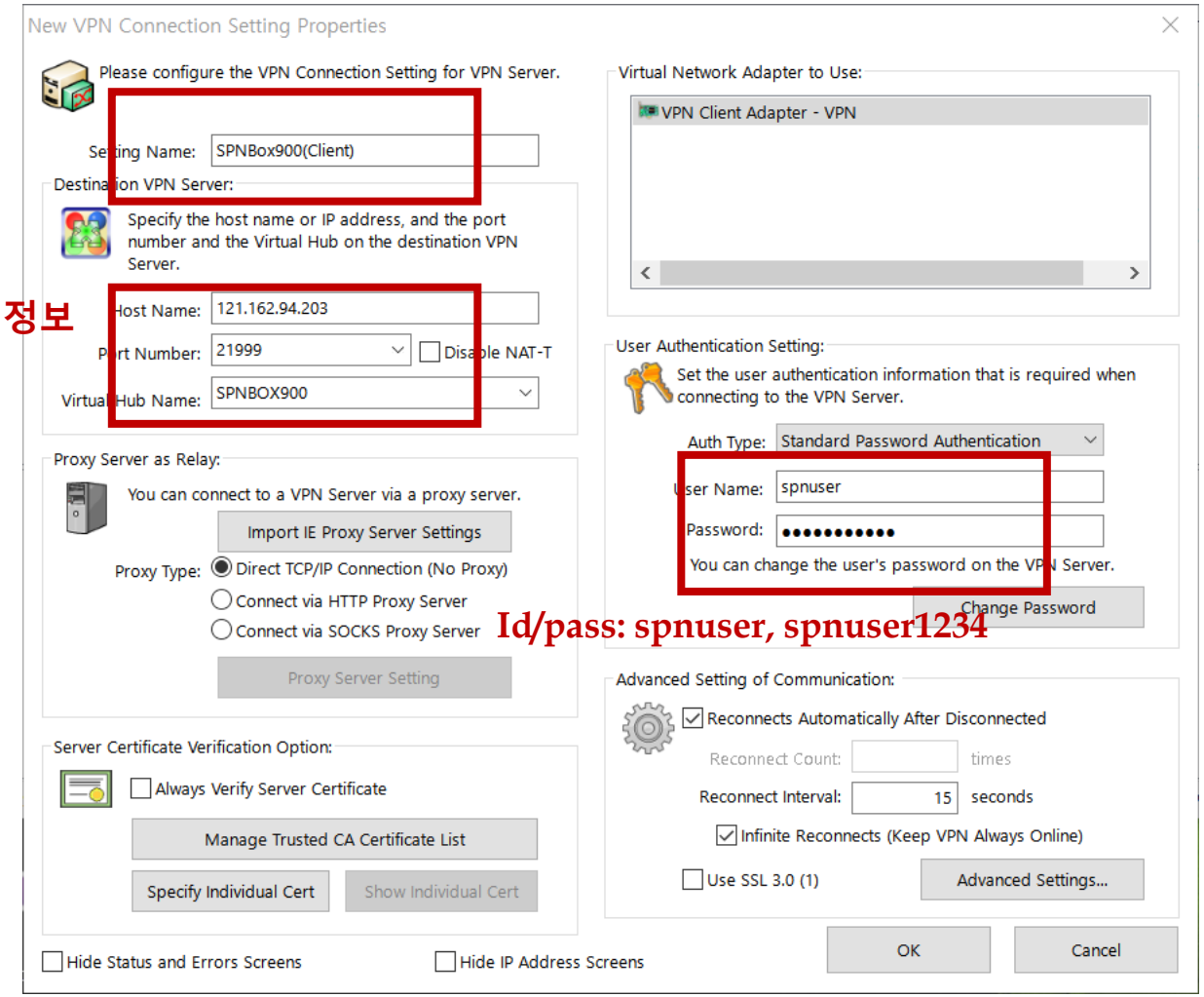
4. SPN Gateway & Client(2) – Client 설정(1)

New VPN Connection Settting … 선택
(Ctrl + N)

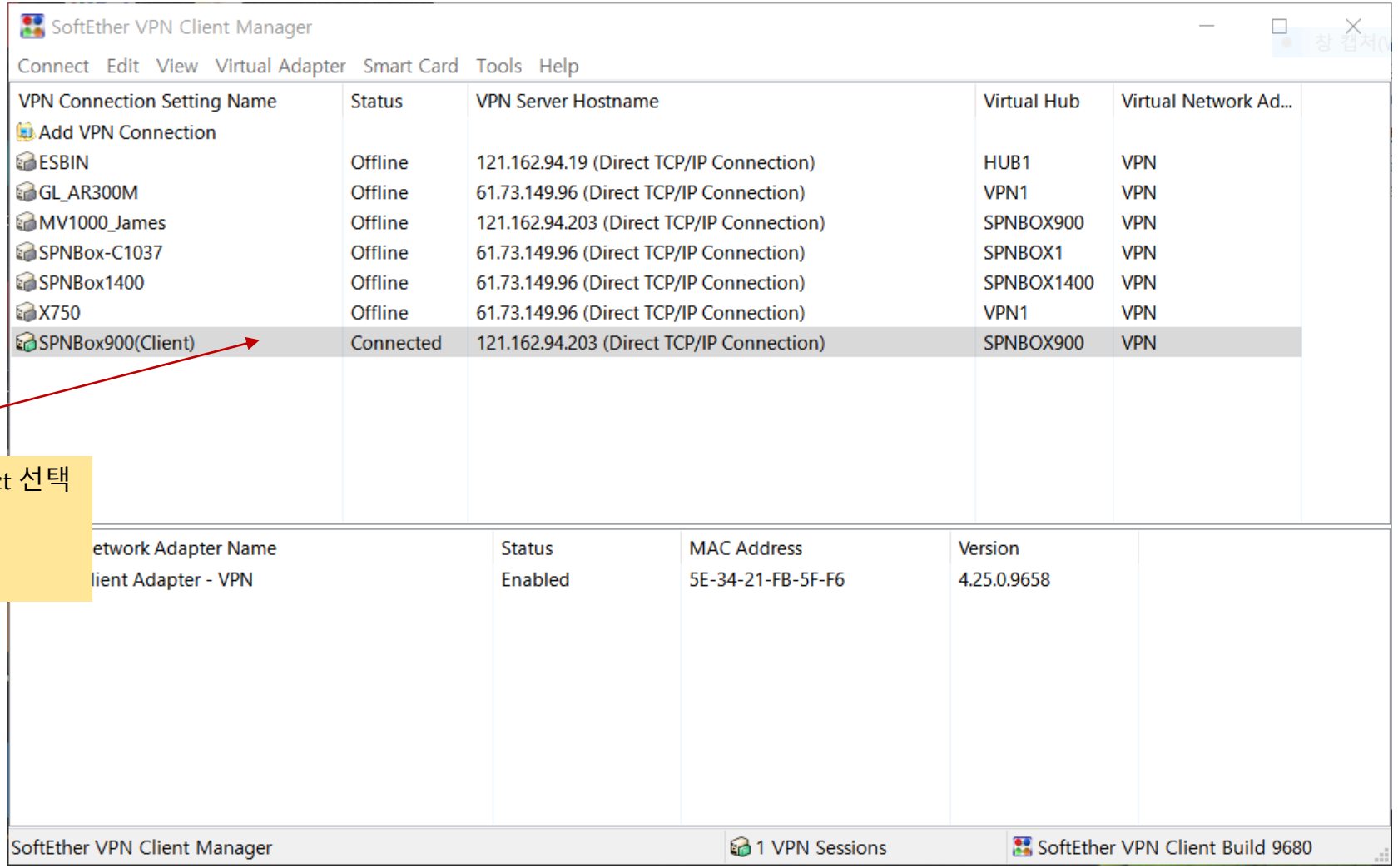


4. SPN Gateway & Client(2) – Client 설정(2)

VPN Gateway의 endpoint 정보



4. SPN Gateway & Client(2) – Client 설정(3)



1) 오른쪽 마우스 클릭 후, Connect 선택

2) Connected 표시 후,
DHCP popup 창 뜨면 연결 성공

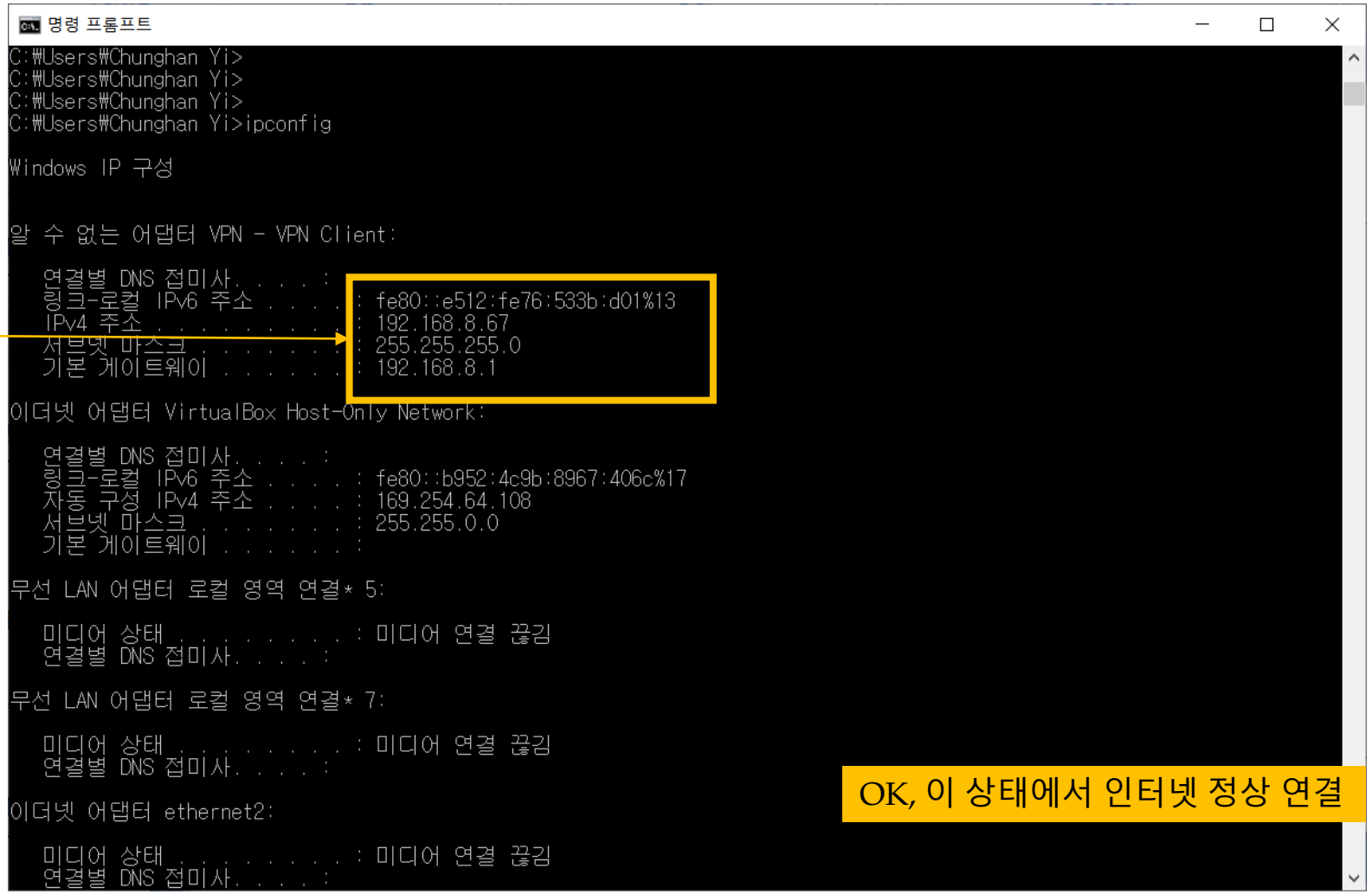
4. SPN Gateway & Client(2) – Client 설정(4)

SPN Client	중요 설정 정보 요약
a) VPN Server(Gateway) 정보	VPN Server endpoint IP address(VPN Server 쪽 공유기 WAN IP): **121.162.94.203** VPN Server endpoint Port: **21999** (포트 포워딩 설정 참조)
b) Virtual Hub 사용자 계정 정보	User id/passwd: **spnuser/spnuser1234**

참고: 위의 설정 중 VPN Server 정보는 실제 field 상황에 맞게 입력해 주어야 한다.

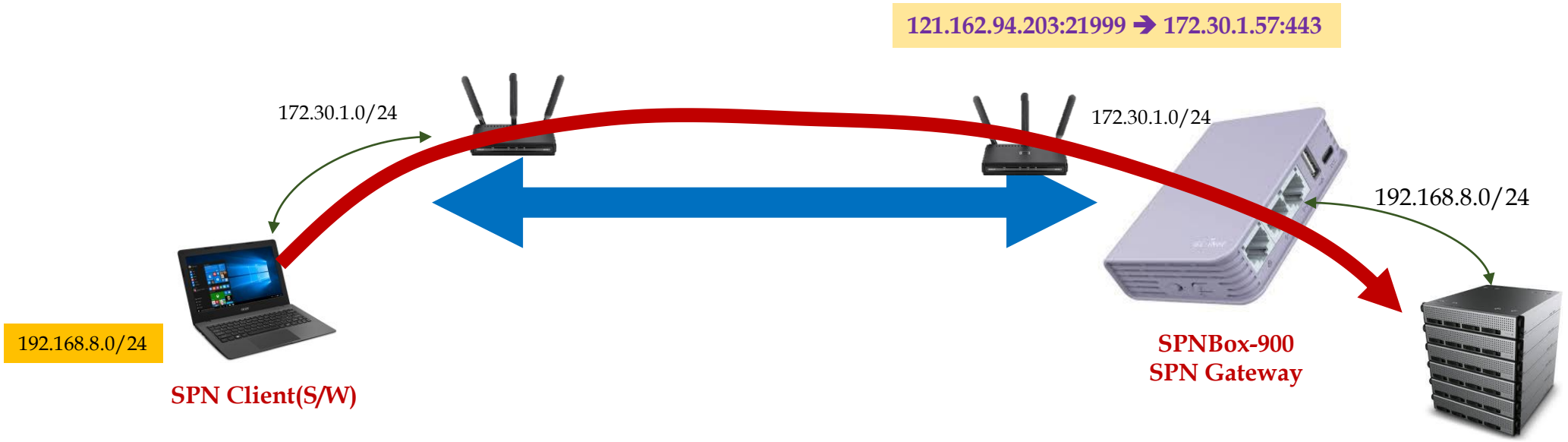
4. SPN Gateway & Client(3) – VPN 연결 시험(1)

Windows PC IP 주소가 SPNBox-900 내부망 주소로 변경됨.

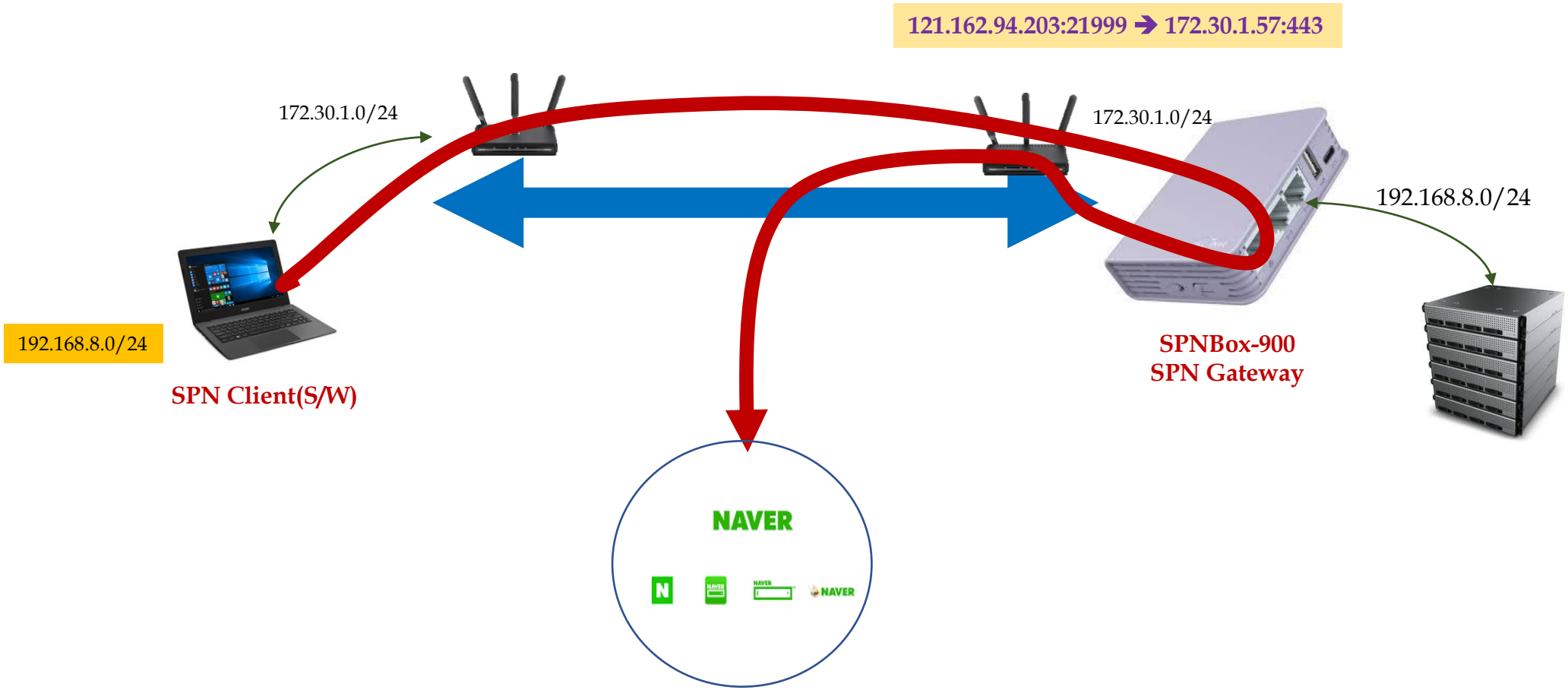


OK, 이 상태에서 인터넷 정상 연결

4. SPN Gateway & Client(3) – VPN 연결 시험(2)



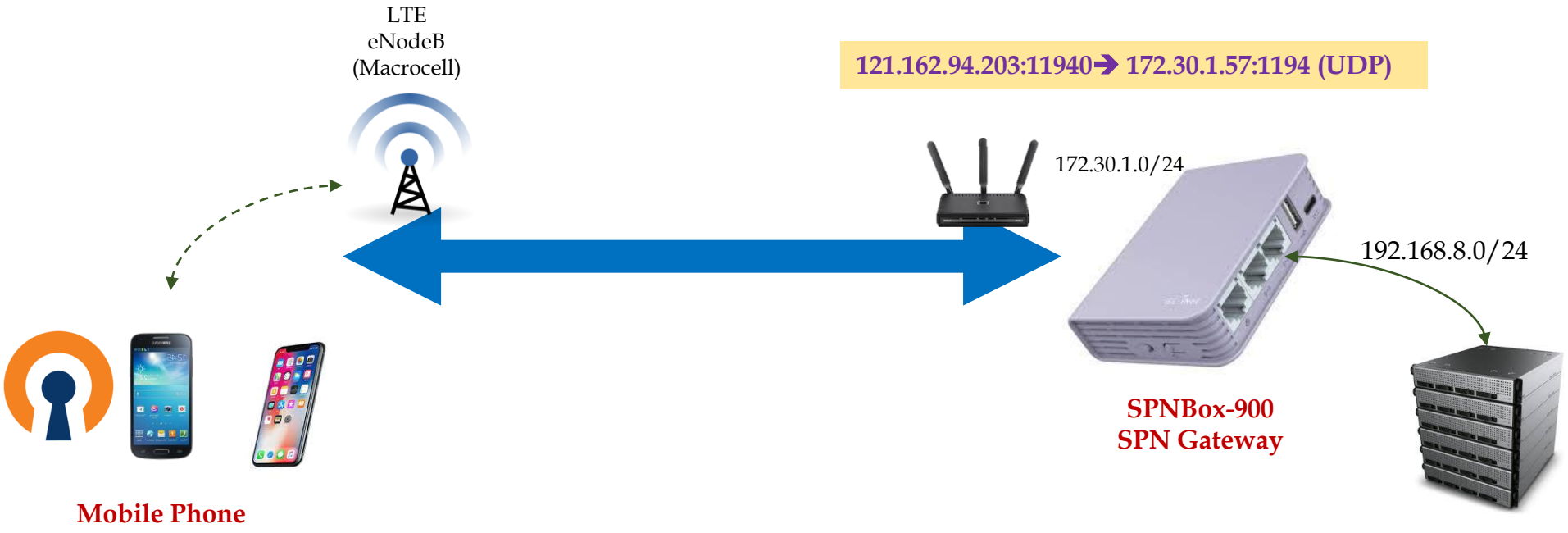
4. SPN Gateway & Client(3) – VPN 연결 시험(3)



참고: L2 SPN을 사용하여 인터넷을 접속할 경우, 위와 같이 패킷이 VPN Gateway를 경유하게 된다(느리다).
해법: VPN 접속이 아니라 인터넷 접속이 목적이라면 Home AP에 직접 붙으면 된다.

5. SPN Gateway & Mobile Phone 1
: OpenVPN Setup Guide

5. SPN Gateway & Mobile Phone(1) – Testbed(1)



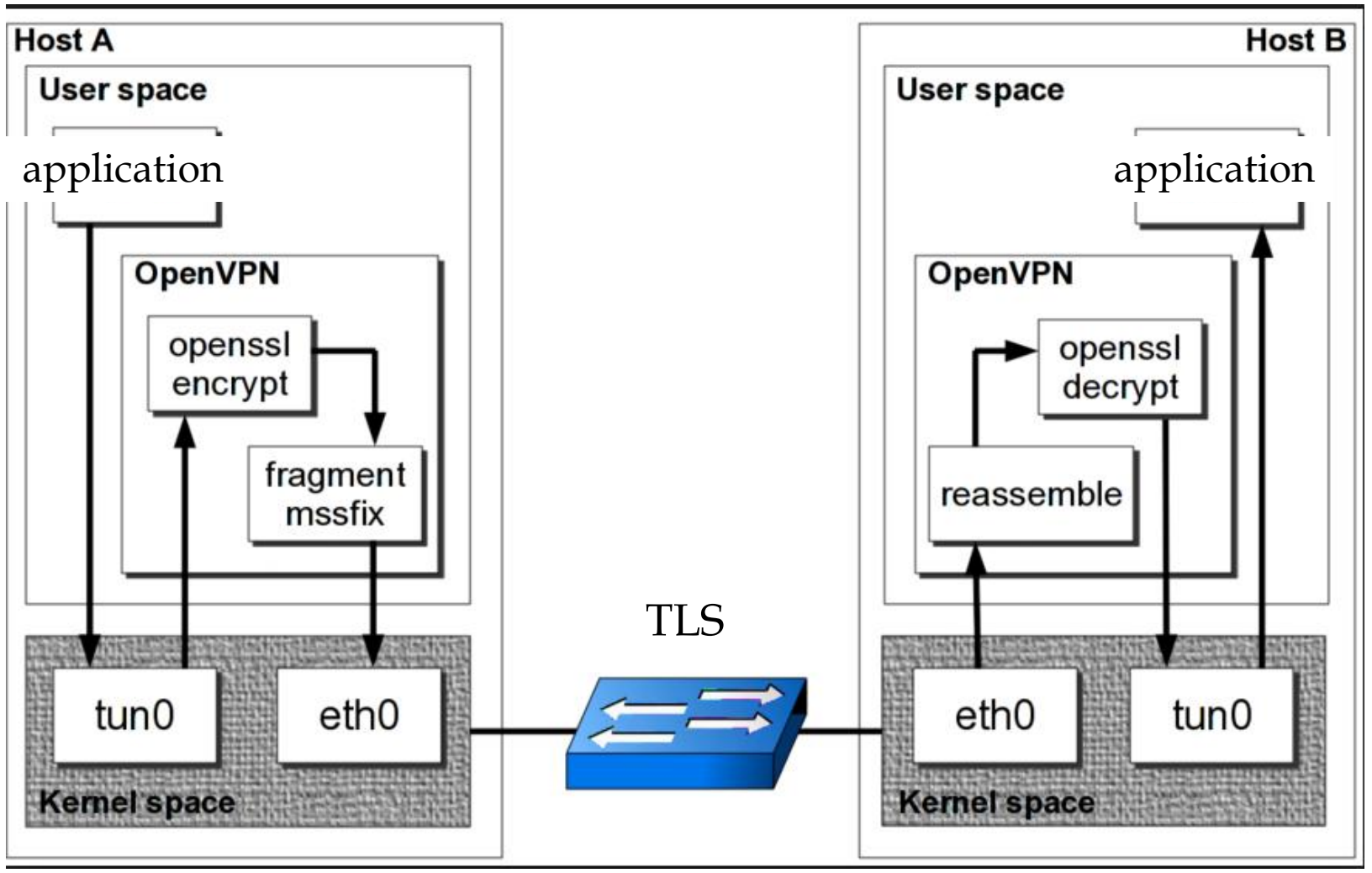
이 장에서는 위의 네트워크(테스트베드) 환경에서 VPN 연결 시험을 진행하도록 하겠습니다.
SPN Gateway는 **OpenVPN**, L2TP/IPsec Clone 서버 기능을 제공합니다.

5. SPN Gateway & Mobile Phone(1) – Testbed(2)

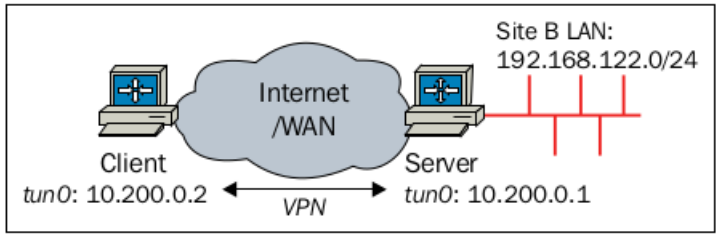
SPN Gateway	전체 설정 절차 요약
a)	VPN Server를 구동시키고, vpncmd(CLI: se vcmd run 명령)로 admin password를 설정한다(SPNBox CLI에서 수행)
b)	Windows PC에서 VPN Server Manager로 VPN Server에 접속한 후, 가장 기본적인 서버 설정(local ip address, port, admin password 입력)을 한다.
c)	Virtual Hub을 하나 추가한다. Default Virtual Hub을 사용해도 됨.
d)	Virtual Hub 사용을 위한 client 계정을 하나 등록한다.
e)	Local bridge를 하나 생성하고 SPNBox LAN bridge와 연결한다(SPNBox CLI에서 수행).
f)	**OpenVPN 접속을 허용(1194 port에 대한 port forwarding 설정 추가)하도록 한다. 이후 OpenVPN Client profile(.ovpn)을 자동 생성하여, PC에 저장한다.**

Mobile Phone	전체 설정 절차 요약(OpenVPN Connect 설정 절차)
a)	Google Play Store나 Apple AppStore로 부터 OpenVPN Connect App을 내려 받아 자신의 Phone에 설치한다.
b)	VPN Server에서 생성해 준 ovpn 파일을 편집한다. 즉, VPN 서버 endpoint IP & port 정보를 수정한다. 주의: VPN Server 외부 방화벽(or 공유기)에서는 Port Forwarding 규칙을 사전에 생성해 두어야 한다(예: 11940 -> 1194)
c)	OpenVPN app을 실행한 후, ovpn 파일을 내려 받는다(이건 https로 내려 받거나, mobile phone local folder로 부터).
d)	username@Virtual_Hub_Name 형태로 사용자 계정 정보를 입력한다. 예를 들어, spnuser@SPNBOX900 이후 잠시 기다리면, SPN Gateway(VPN Server)와의 연결에 성공할 것이다.

5. SPN Gateway & Mobile Phone(2) – OpenVPN 소개(1)



5. SPN Gateway & Mobile Phone(2) – OpenVPN 소개(2)



Client's config

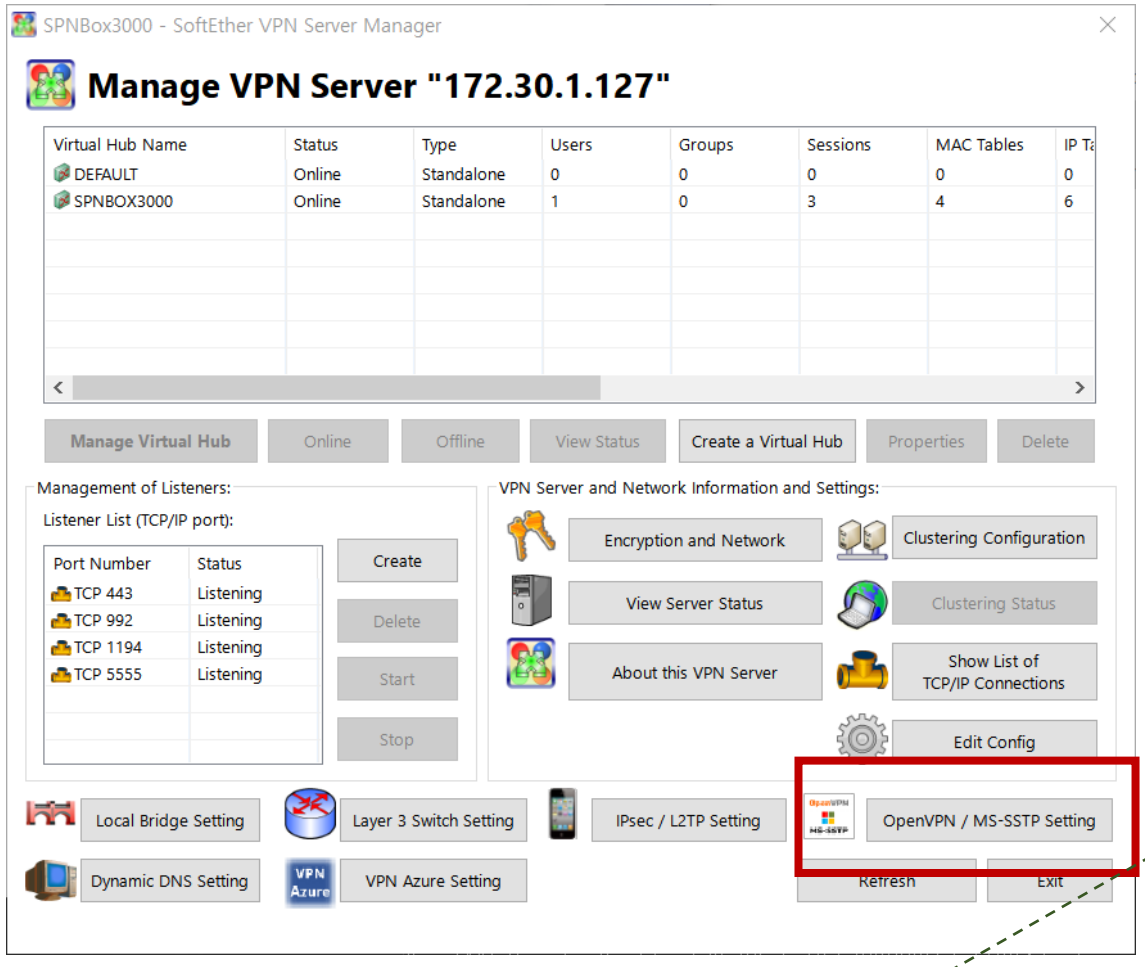
```
client
proto udp
remote openvpnserver.example.com
port 1194
dev tun
nobind
ca   /etc/openvpn/movpn/movpn-ca.crt
cert /etc/openvpn/movpn/client1.crt
key  /etc/openvpn/movpn/client1.key
```

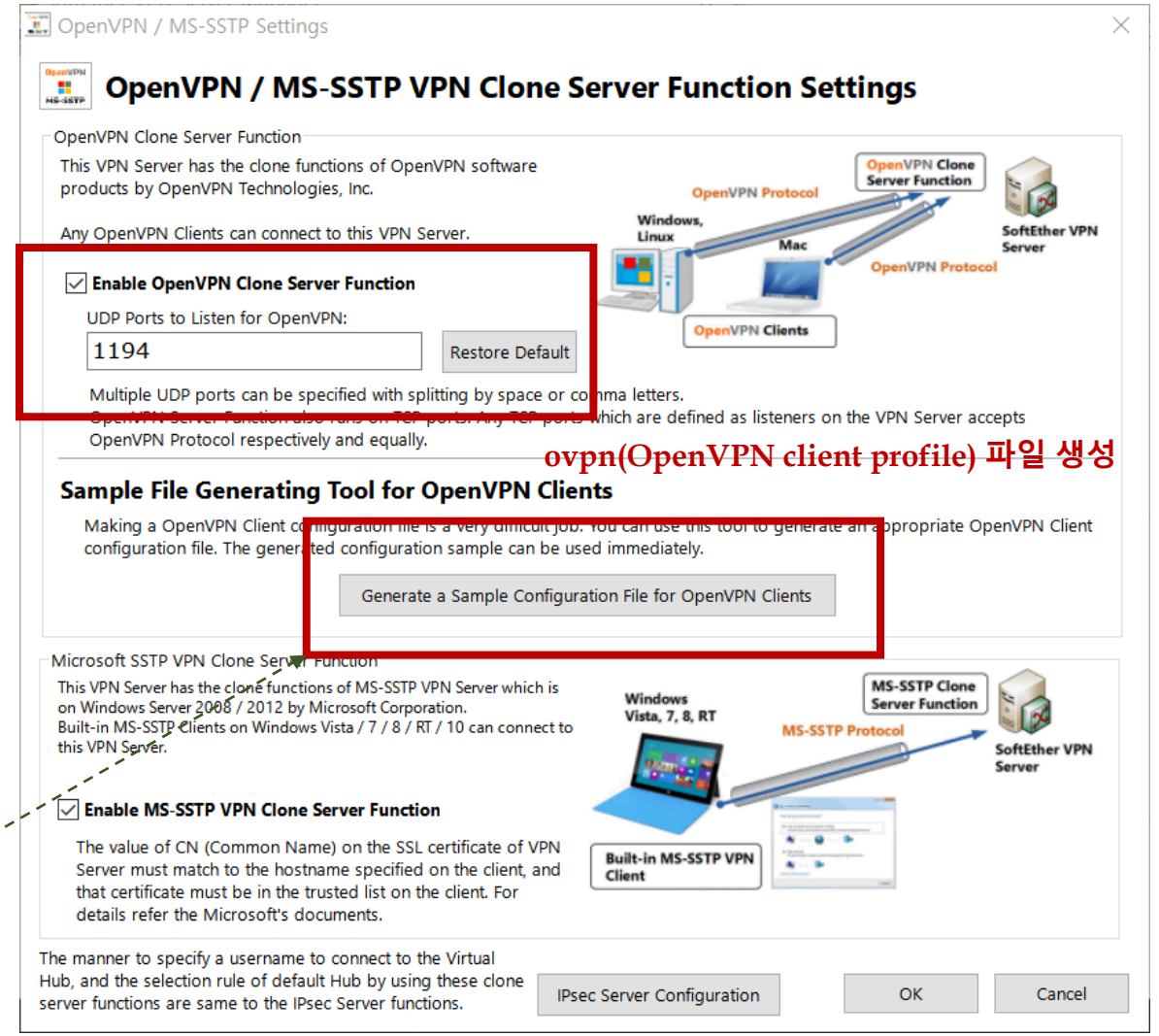
SPN Gateway는 OpenVPN Clone 서버 기능을 제공합니다.

Server's config

```
proto udp
port 1194
dev tun
server 10.200.0.0 255.255.255.0
topology subnet
persist-key
persist-tun
keepalive 10 60

dh      /etc/openvpn/movpn/dh2048.pem
ca      /etc/openvpn/movpn/movpn-ca.crt
cert    /etc/openvpn/movpn/server.crt
key     /etc/openvpn/movpn/server.key

user  nobody
group nobody  # use 'group nogroup' on Debian/Ubuntu

verb 3
daemon
log-append /var/log/openvpn.log
```

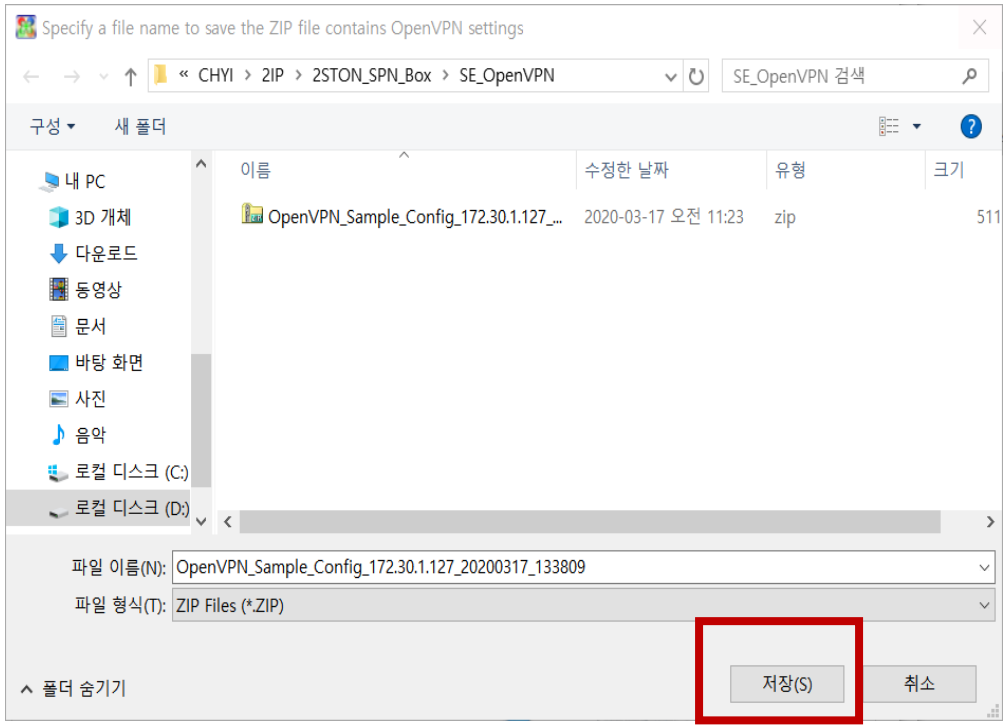
5. SPN Gateway & Mobile Phone(3) - Gateway 설정(1)

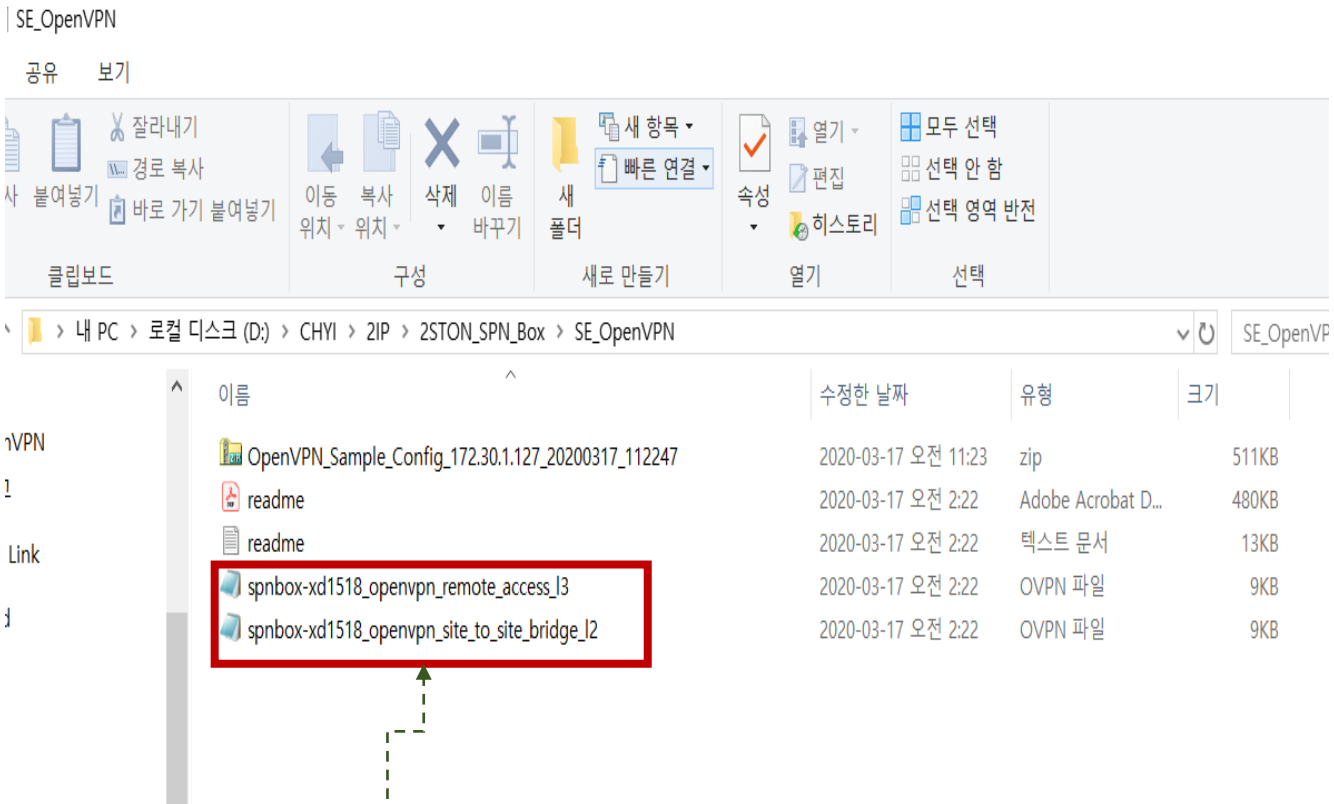




여기서 생성한 ovpn 파일을 mobile phone에 설치하면 됨.

5. SPN Gateway & Mobile Phone(3) - Gateway 설정(2)

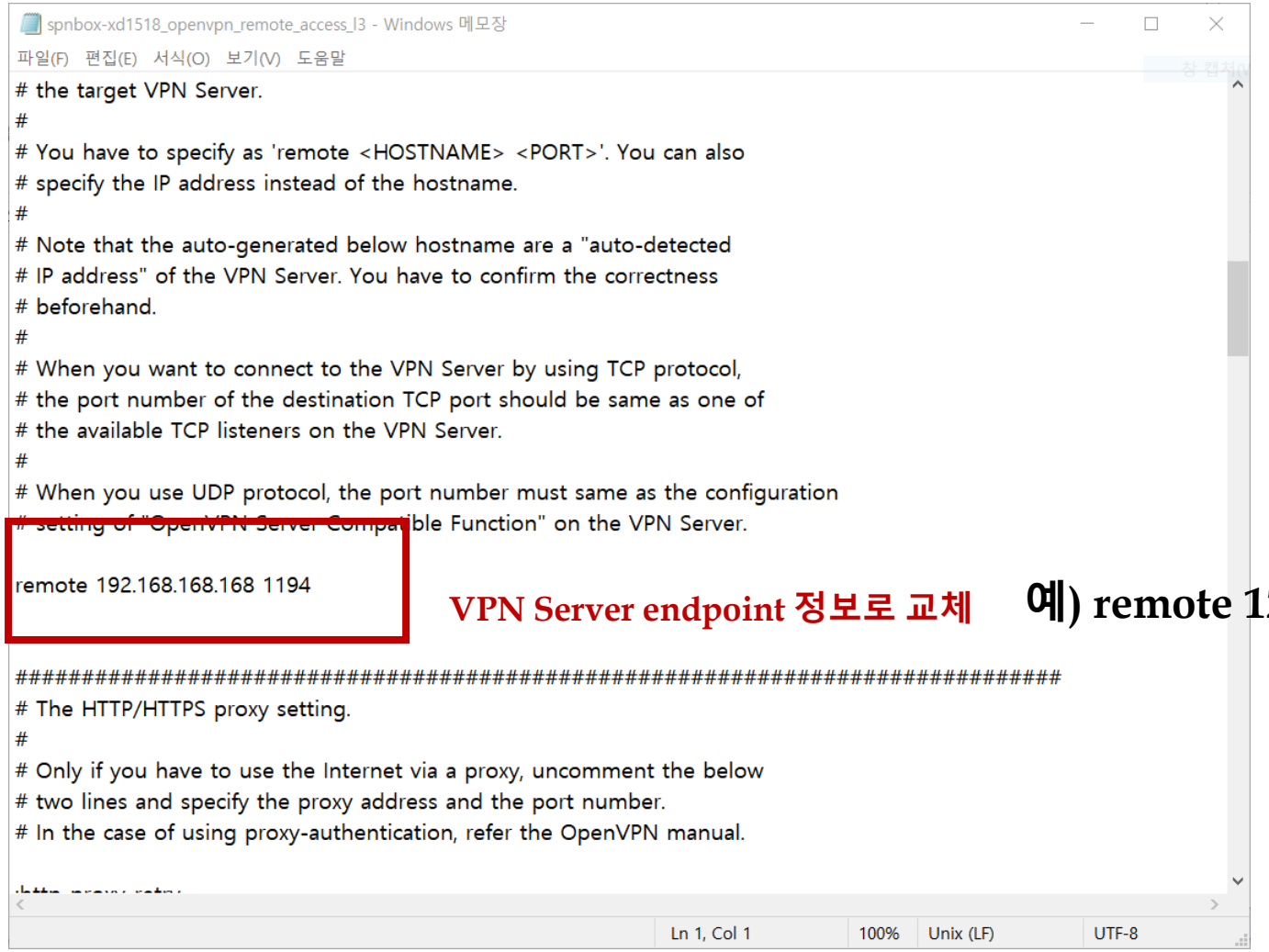




ovpn(OpenVPN client profile) 파일 편집하여 사용

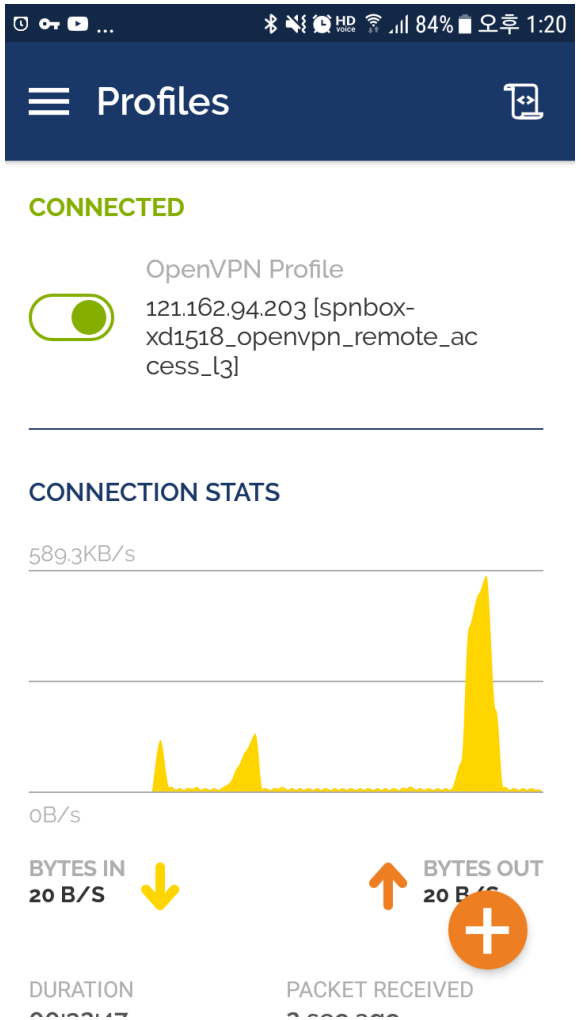
- **13, 12의 정확한 의미를 파악하기 위해서는 위의 readme 파일을 읽어 보시기 바람.**
- **잘 모르겠으면 13 파일을 사용하면 됨.**

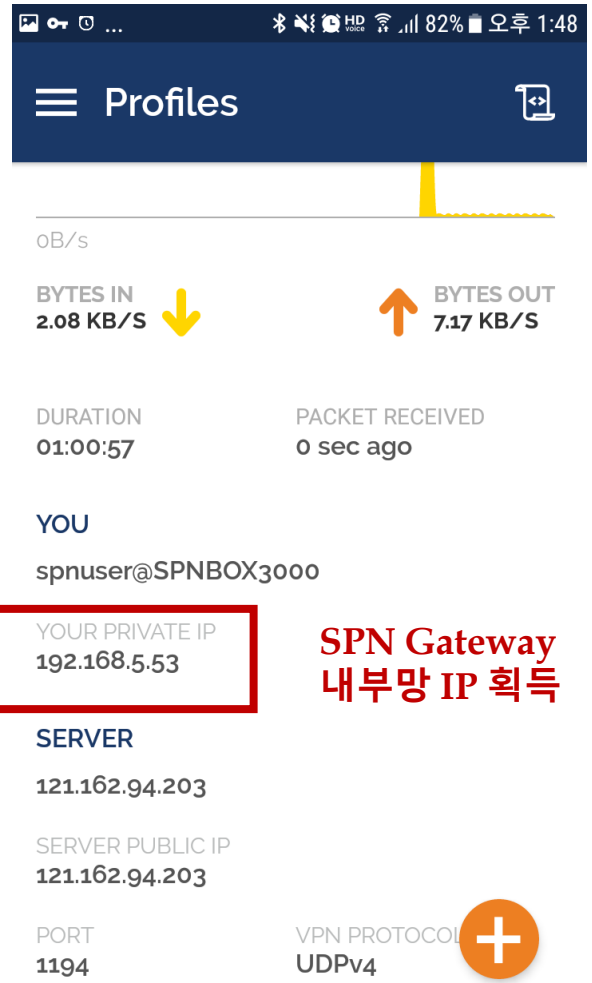
5. SPN Gateway & Mobile Phone(3) - Gateway 설정(3)



5. SPN Gateway & Mobile Phone(4) – OpenVPN 설정(1)

ovpn 파일 download 및 사용자 계정 정보 입력
Id: spnuser@SPNBOX900
Pass: spnuser1234





SPN Gateway 내부망 IP 획득

참고: 위의 snapshot은 실제 Testbed의 내용과는 다르게 SPNBox3000과의 연결 내용을 정리한 것이다.

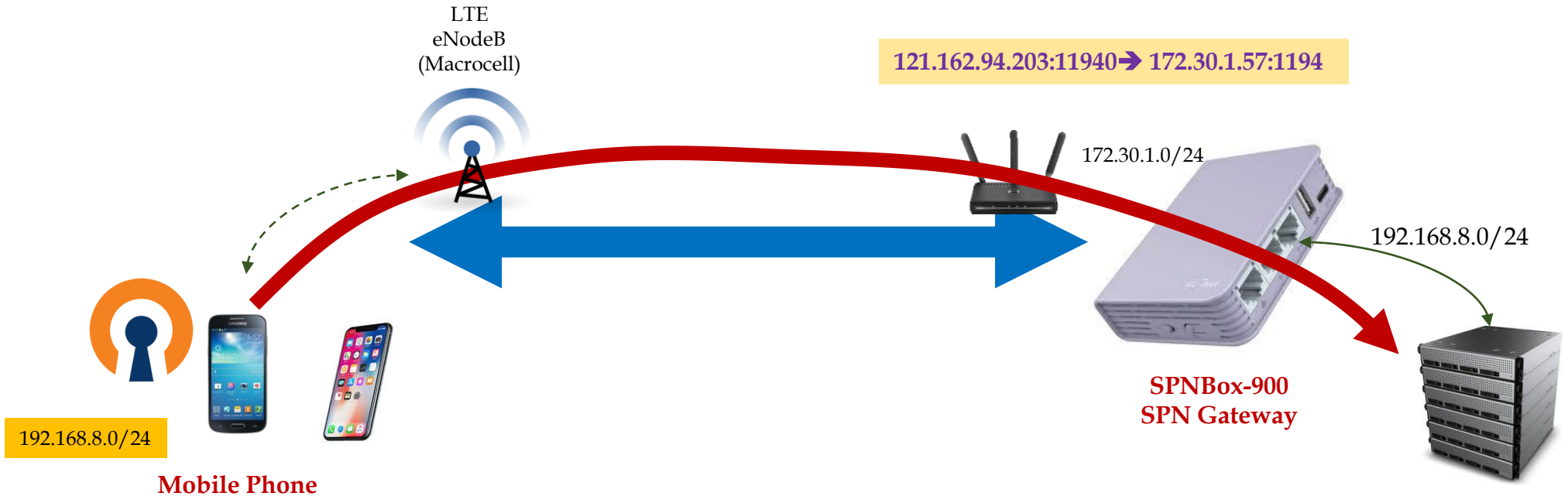
5. SPN Gateway & Mobile Phone(4) – OpenVPN 설정(2)

- 1) App store에서 OpenVPN app을 download 받아 설치한다.
- 2) SPN Gateway(VPN Server)로 부터 생성해 둔, ovpn 파일(l3 or l2)을 편집한다.
  - ✓ *SPN Gateway 쪽 endpoint 정보만 변경해 주면 됨.*
- 3) OpenVPN app을 실행한 후, ovpn 파일(OpenVPN Client profile)을 import 한다.
  - ✓ *관련 서버가 마련되어 있다면, https를 통해 내려 받거나, 다른 기법(예: adb)을 통해 적당한 위치로 복사 후, import해 주면 된다.*

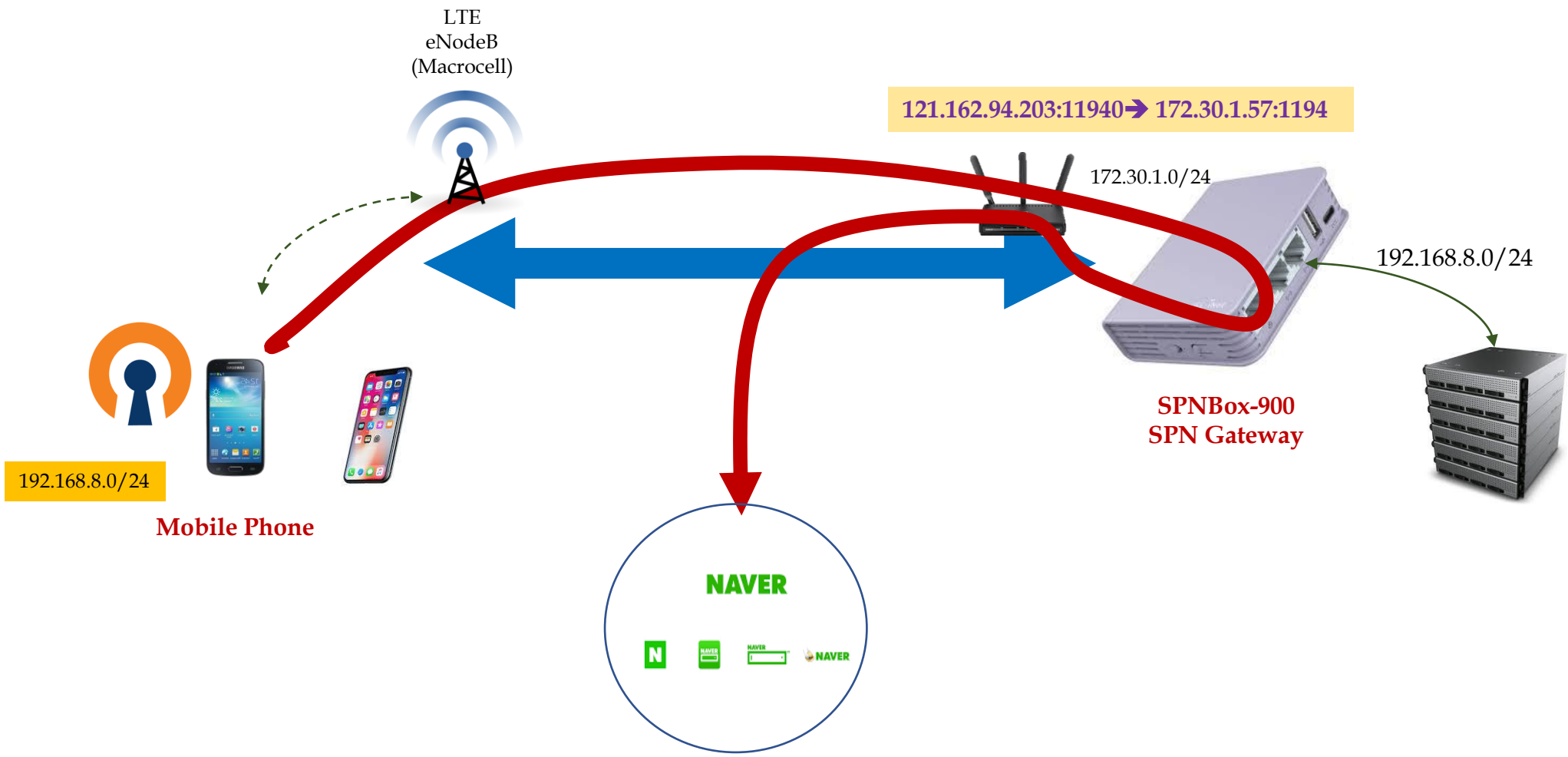
```
chyi@mars:~/workspace/test/03172020$ sudo adb push ./spnbox-xd1518_openvpn_remote_access_l3.ovpn /storag
e/emulated/0/Music
./spnbox-xd1518_openvpn_remote_access_l3.ovpn: 1 file pushed. 0.4 MB/s (9085 bytes in 0.025s)
```

- 4) 사용자 계정 정보를 입력한다.
  - ✓ *Id: spnuse@SPNBOX900, pass: spnuser1234*
- 5) 잠시 기다리면 정상적으로 VPN 연결이 이루어질 것이다. 이후, 내부 서버에 접속 시도해 본다.

5. SPN Gateway & Mobile Phone(5) – VPN 연결 시험(1)



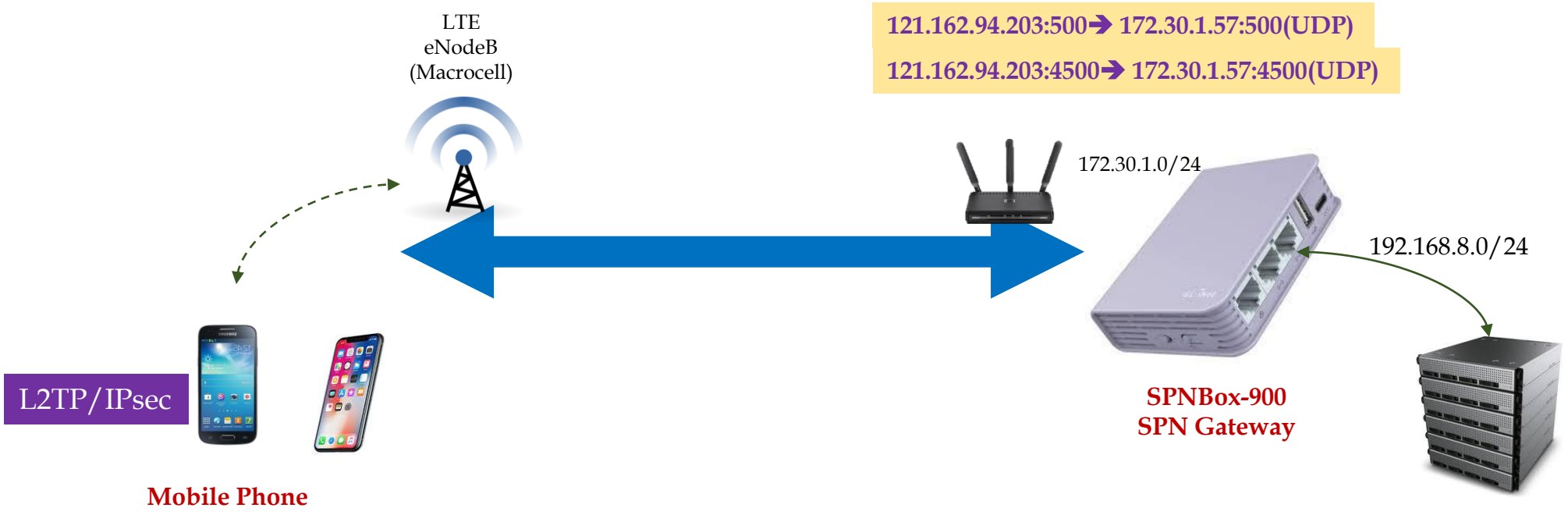
5. SPN Gateway & Mobile Phone(5) – VPN 연결 시험(2)



6. SPN Gateway & Mobile Phone 2
: L2TP/IPsec Setup Guide

6. SPN Gateway & Mobile Phone(1) – Testbed(1)

<참고>
- **UDP 500**: IKE가 사용하는 Port
- **UDP 4500**: IPsec NAT Traversal Port



이 장에서는 위의 네트워크(테스트베드) 환경에서 VPN 연결 시험을 진행하도록 하겠습니다.
SPN Gateway는 OpenVPN, **L2TP/IPsec** Clone 서버 기능을 제공합니다.

6. SPN Gateway & Mobile Phone(1) – Testbed(2)

SPN Gateway	전체 설정 절차 요약
a)	VPN Server를 구동시키고, vpncmd(CLI: se vcmd run 명령)로 admin password를 설정한다(SPNBox CLI에서 수행)
b)	Windows PC에서 VPN Server Manager로 VPN Server에 접속한 후, 가장 기본적인 서버 설정(local ip address, port, admin password 입력)을 한다.
c)	Virtual Hub을 하나 추가한다. Default Virtual Hub을 사용해도 됨.
d)	Virtual Hub 사용을 위한 client 계정을 하나 등록한다.
e)	Local bridge를 하나 생성하고 SPNBox LAN bridge와 연결한다(SPNBox CLI에서 수행).
f)	**L2TP over IPsec 접속을 허용하도록 한다. Firewall에서 UDP 500, 4500 port를 열어 준다(Port Forwarding 설정)**

Mobile Phone	전체 설정 절차 요약(L2TP/IPsec 설정 절차)
a)	L2TP/IPsec은 Android, iPhone, Windows, MacOS에서 이미 포함되어 있다(별도로 설치할 필요 없음).
b)	Android 기준: 설정 ➔ 연결 => 기타 연결 설정 => VPN => VPN 추가 => {이름, 종류: L2TP/IPSec PSK, 서버 주소: VPN Server endpoint ip 주소, IPsec 사전 공유키: vpn, 사용자 이름: spnuser, 비밀번호: spnuser1234 }
c)	연결 선택, 이후 잠시 기다리면, SPN Gateway(VPN Server)와의 연결에 성공할 것이다.

6. SPN Gateway & Mobile Phone(2) – L2TP/IPsec(1)

L2TP/IPsec이란?

L2TP는 Layer 2 Tunneling Protocol(계층 2 터널링 프로토콜)의 약자입니다. L2TP는 L2F(계층 2 포워딩 프로토콜)와 PPTP(지점간 터널링 프로토콜)가 결합된 프로토콜로 1999년에 처음 제안되었습니다. L2TP는 자체적으로 강력한 암호화 또는 인증을 제공하지 않기 때문에 IPsec이라는 또다른 프로토콜이 L2TP와 함께 사용되는 경우가 많습니다.

IPsec은 Internet Protocol security(인터넷 프로토콜 보안)의 약자입니다. IPsec은 주어진 통신에서 각각의 개별 IP 패킷을 인증 및 암호화하는 종단간 보안을 위한 매우 유연한 프로토콜입니다. IPsec은 다양한 애플리케이션의 인터넷 프로토콜 슈트의 인터넷 계층에 사용됩니다.

L2TP와 IPsec을 함께 사용하면 PPTP(지점간 터널링 프로토콜)보다 훨씬 안전하지만 보안보다 익명화에 더 적합합니다.

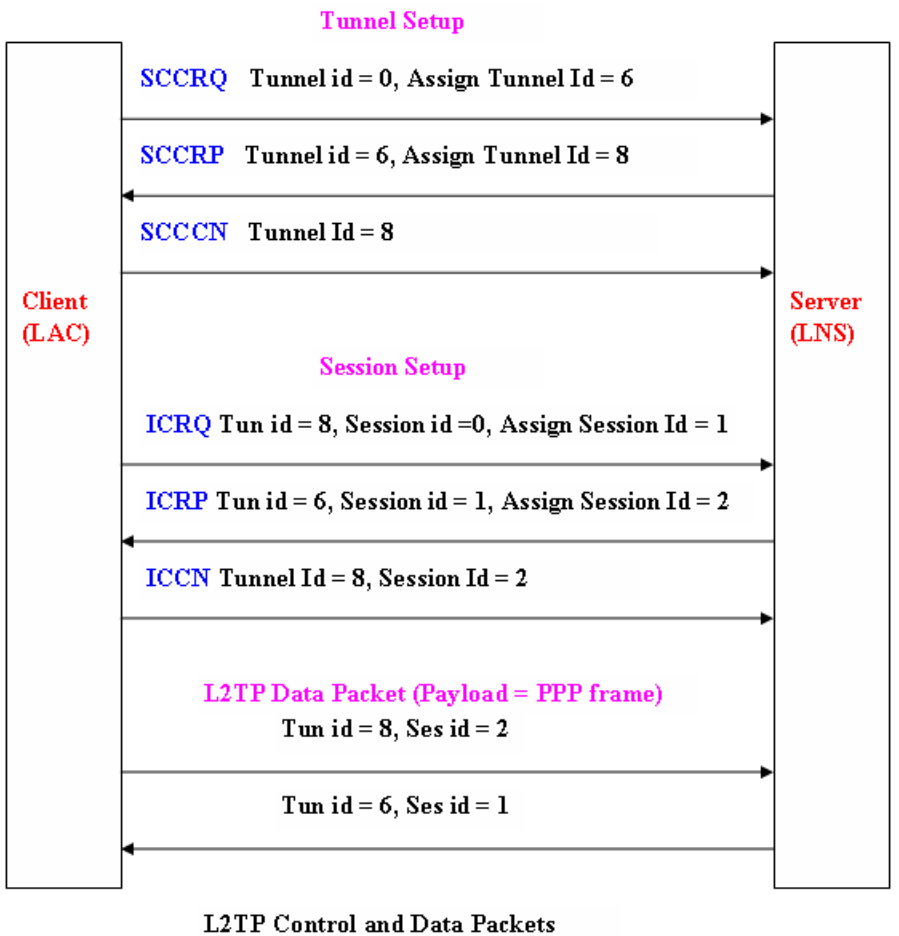
L2TP는 일부 방화벽이 차단하는 것으로 알려진 UDP 포트 500을 사용하기 때문에 때때로 방화벽 관련 문제를 겪을 수 있습니다.

장점

✔ PPTP보다 안전함

단점

✖ OpenVPN보다 느림
✖ 때때로 방화벽에 의해 차단됨



L2TP Control and Data Packets

6. SPN Gateway & Mobile Phone(2) – L2TP/IPsec(2)

Benefits of L2TP VPN?

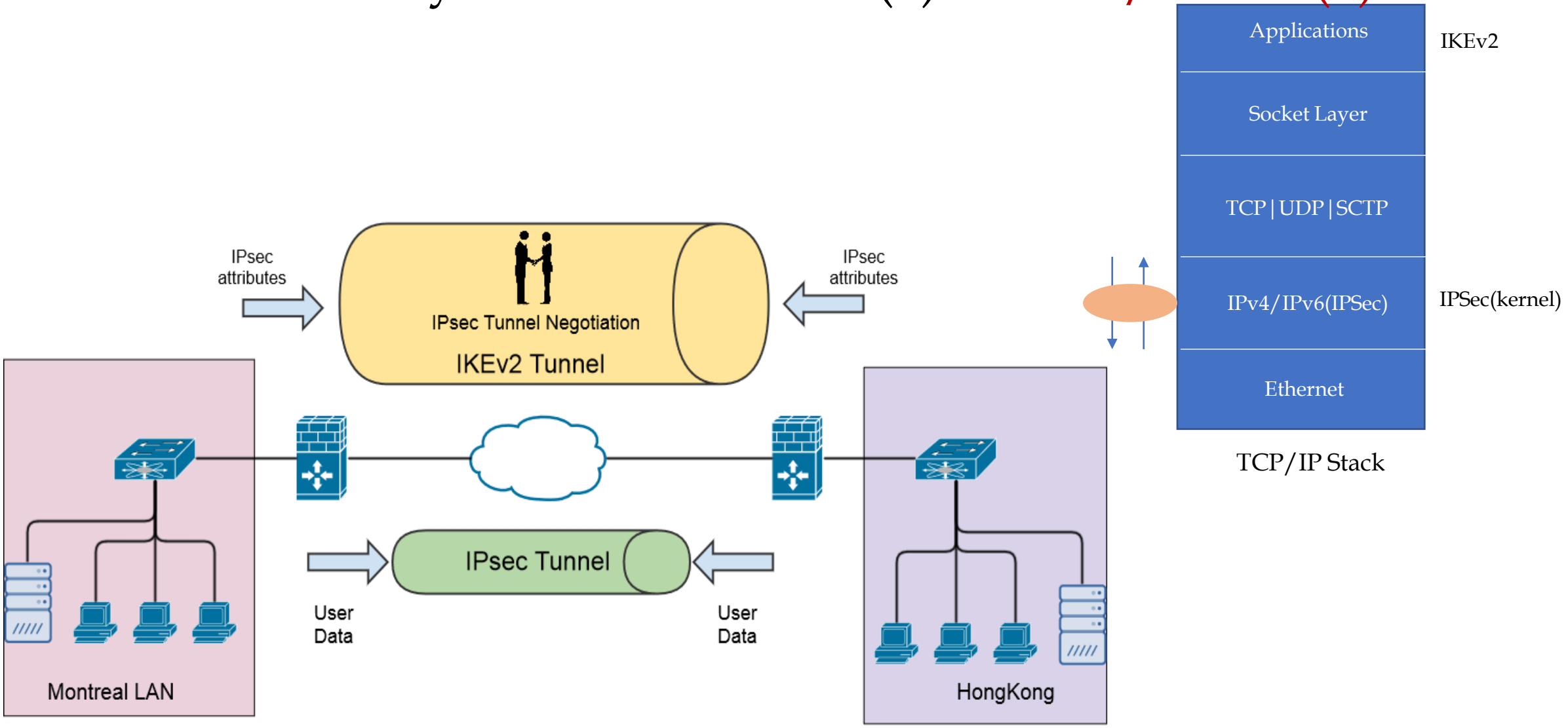
Advantages

- Unlike PPTP, it offers excellent level of encryption and security
- The protocol encapsulates the data twice, which means double data verification.
- The protocol is available on not only desktop but also mobile operating systems.
- L2TP is quite easy to configure on all the operating systems it supports.

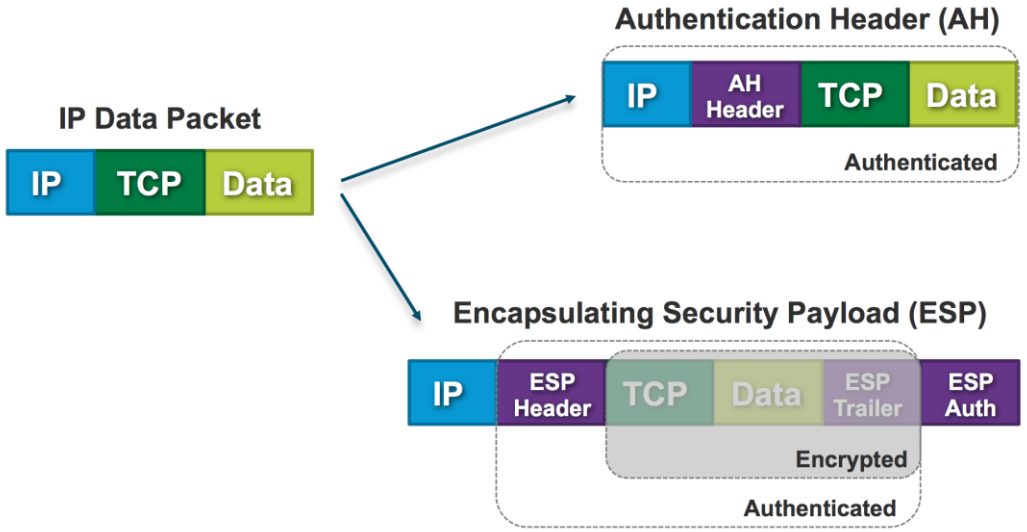
Disadvantages

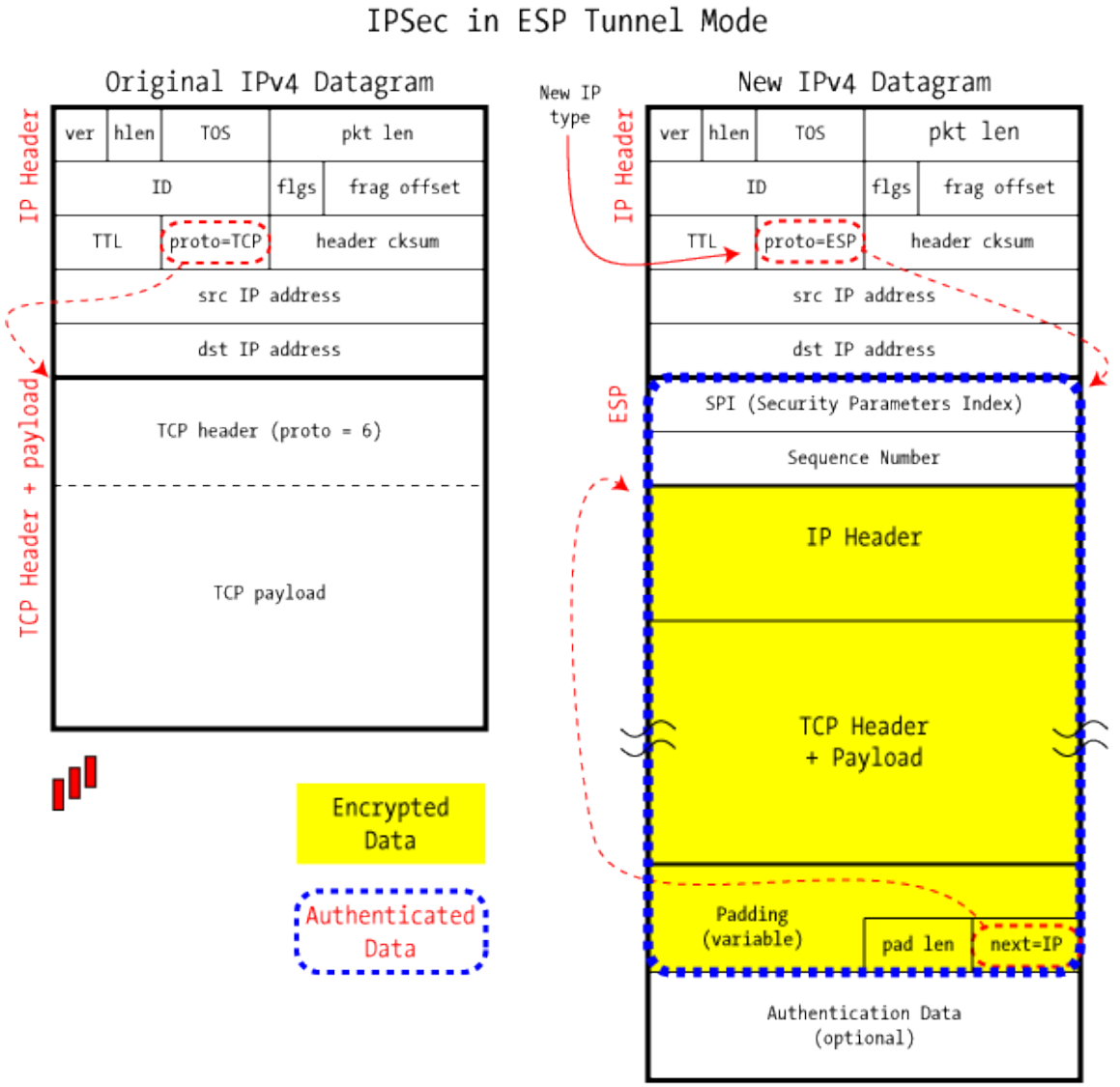
- It offers slow performance because of double authentication (encapsulation).
- There are some firewalls that can block the L2TP protocol ports.
- The protocol is difficult to configure on devices that run on NAT routers.

6. SPN Gateway & Mobile Phone(3) – IPsec/IKEv2(1)

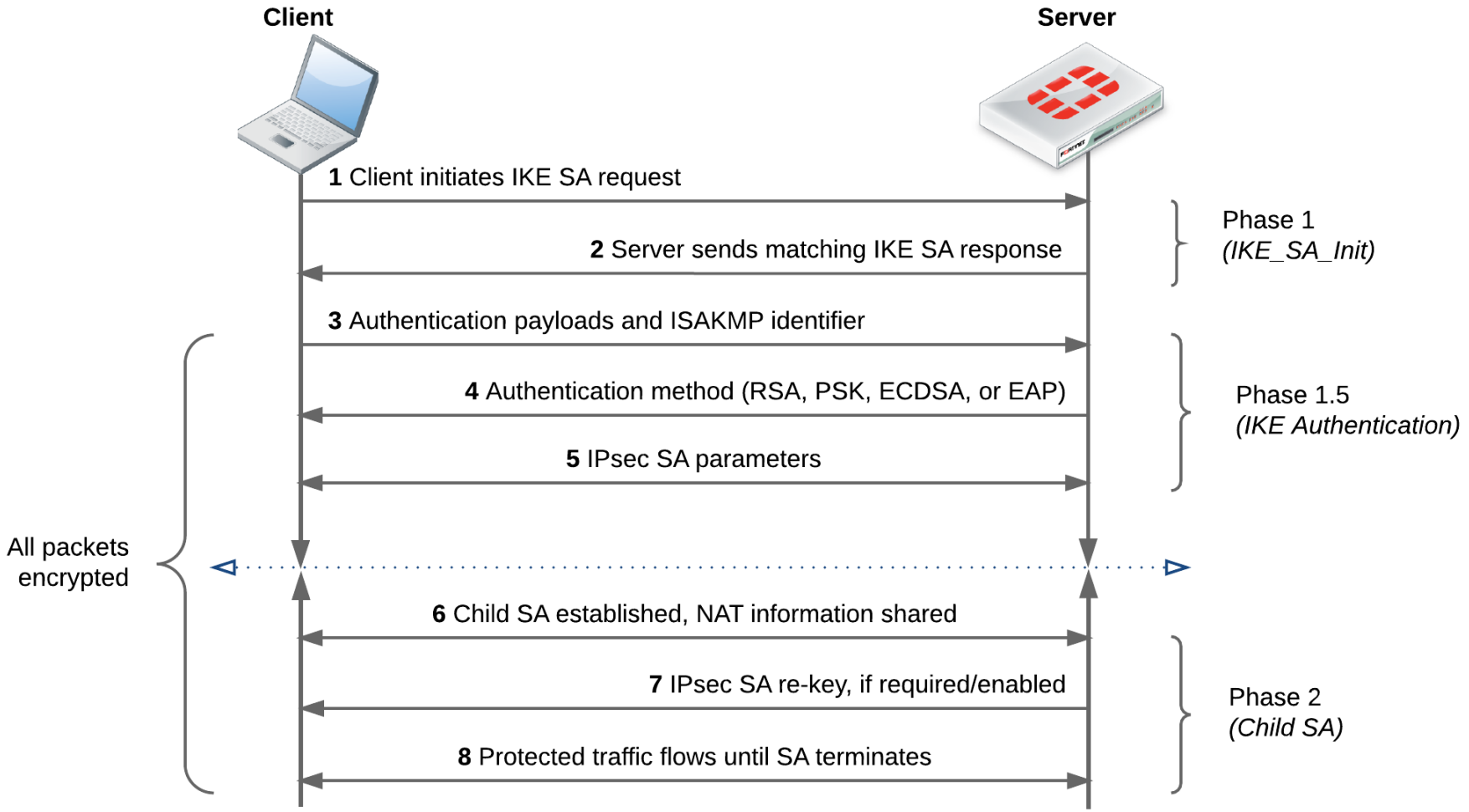


6. SPN Gateway & Mobile Phone(3) – IPsec/IKEv2(2)

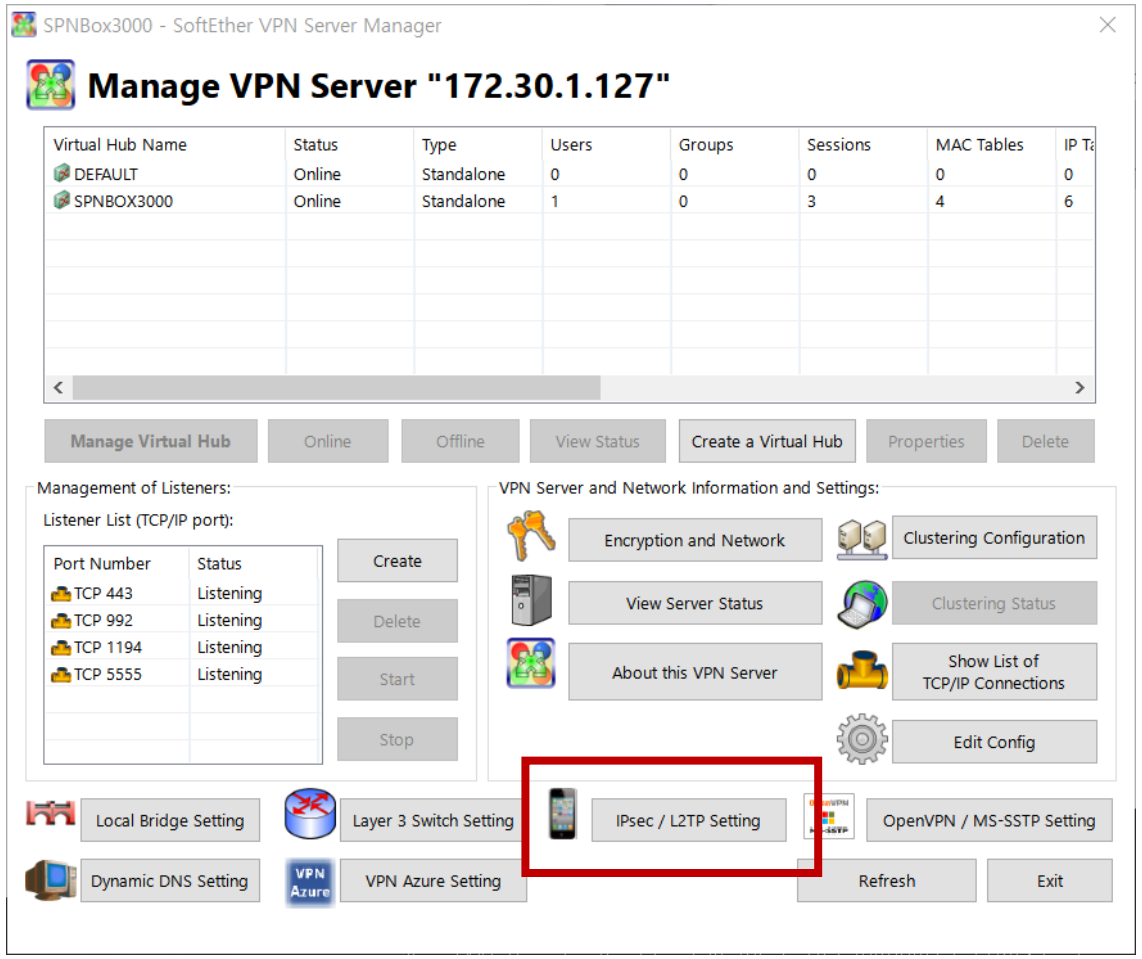




6. SPN Gateway & Mobile Phone(3) – IPsec/IKEv2(3)



6. SPN Gateway & Mobile Phone(4) - Gateway 설정(1)



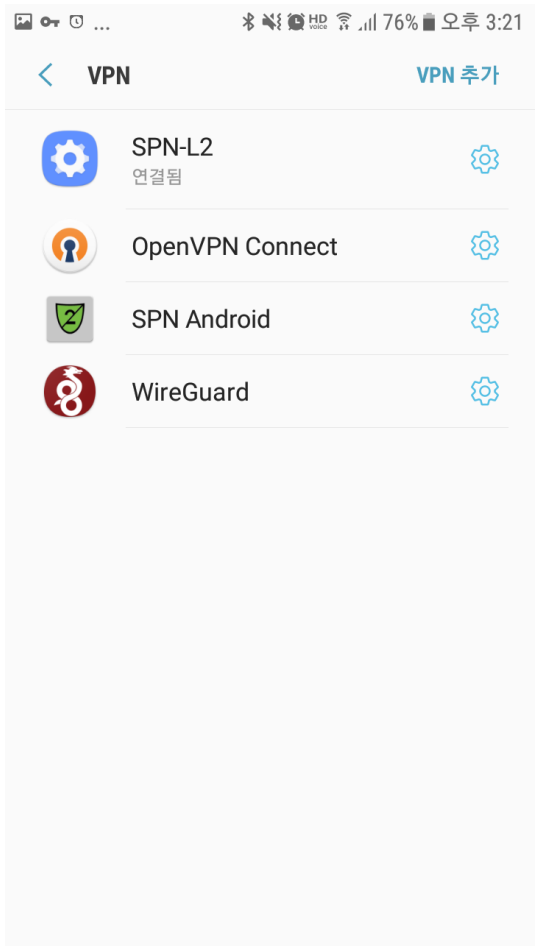
6. SPN Gateway & Mobile Phone(4) - Gateway 설정(2)

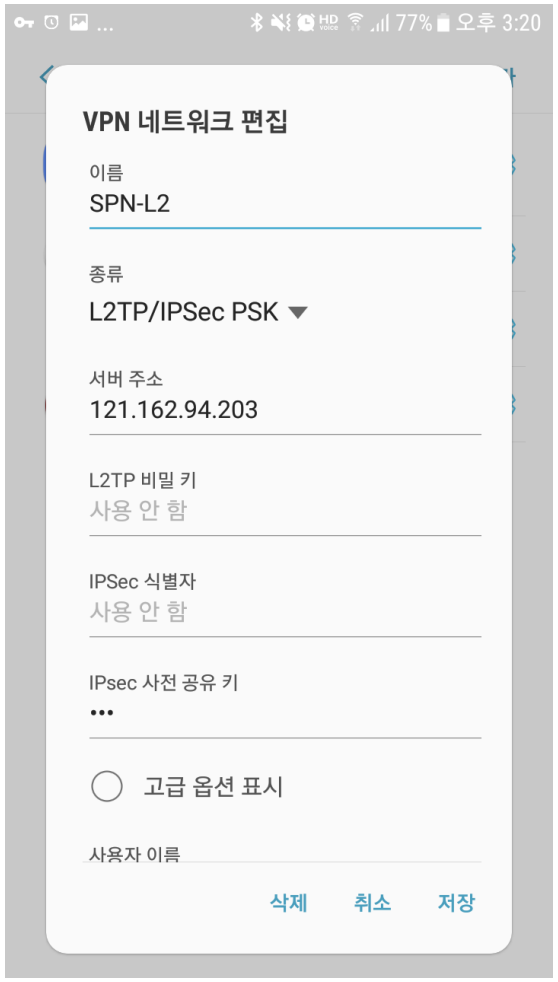
AP04 Port Forwarding 설정

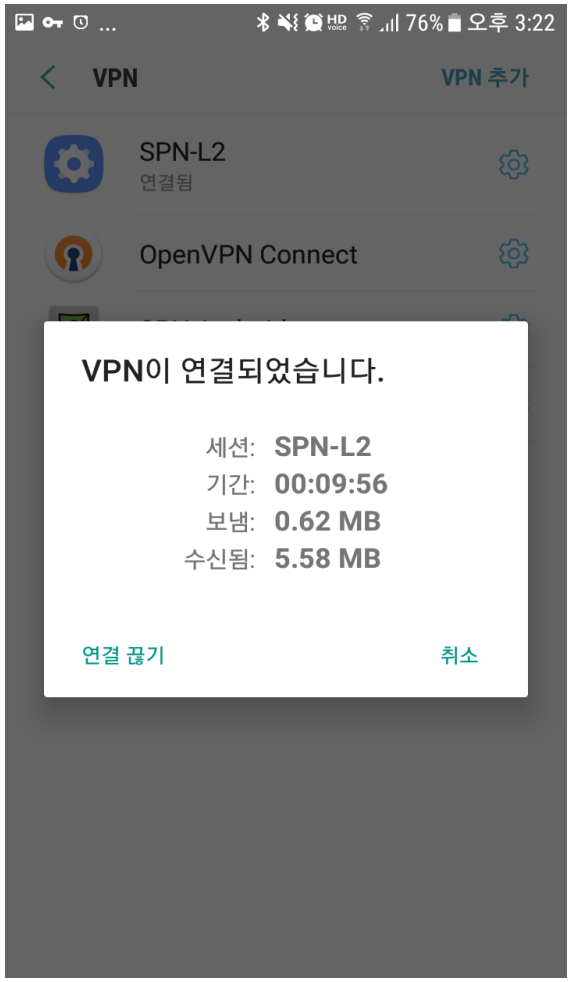
선택	소스IP 주소	소스포트	외부포트	내부 IP 주소	내부 포트	프로토콜	설명	플래그
☐		-						
☐		-						
☐		-						
☐		-						
☐		-						
☐		-						
☐		-						
☐		-						
☐		-						
☐		-						
☐		-						
☐		-						
☐		-						
☐		-						
☐		-						
☐		-						
☐		-	500-500	172.30.1.127	500-500	UDP	l2tp/ipsec	KT
☐		-	4500-4500	172.30.1.127	4500-4500	UDP	l2tp/ipsec	KT

<참고>
- **UDP 500**: IKE(Internet Key Exchange)가 사용하는 Port
- **UDP 4500**: IPsec NAT Traversal Port (UDP 500이 Firewall/NAT에 의해 막힐 경우 사용)

6. SPN Gateway & Mobile Phone(5) – Android 설정(1)





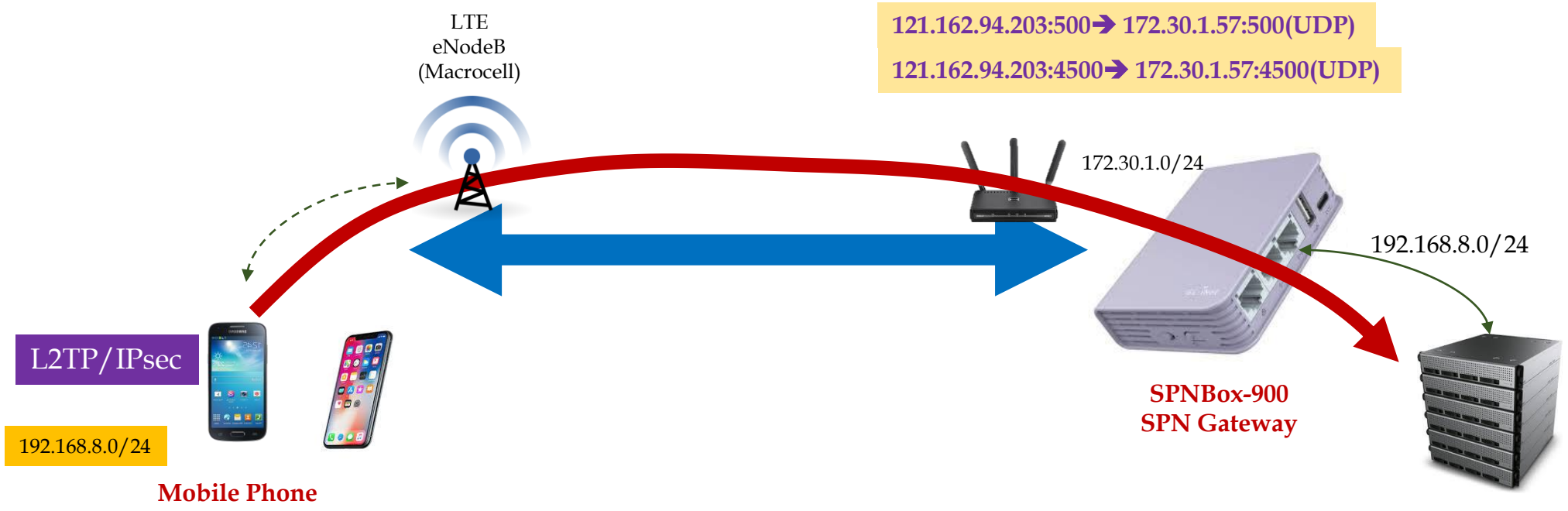


L2TP/IPsec 설정은 매우 간단하다. 즉, 서버 IP 주소, 사전 공유 키 및 사용자 정보만 입력하면 바로 연결 가능하다.

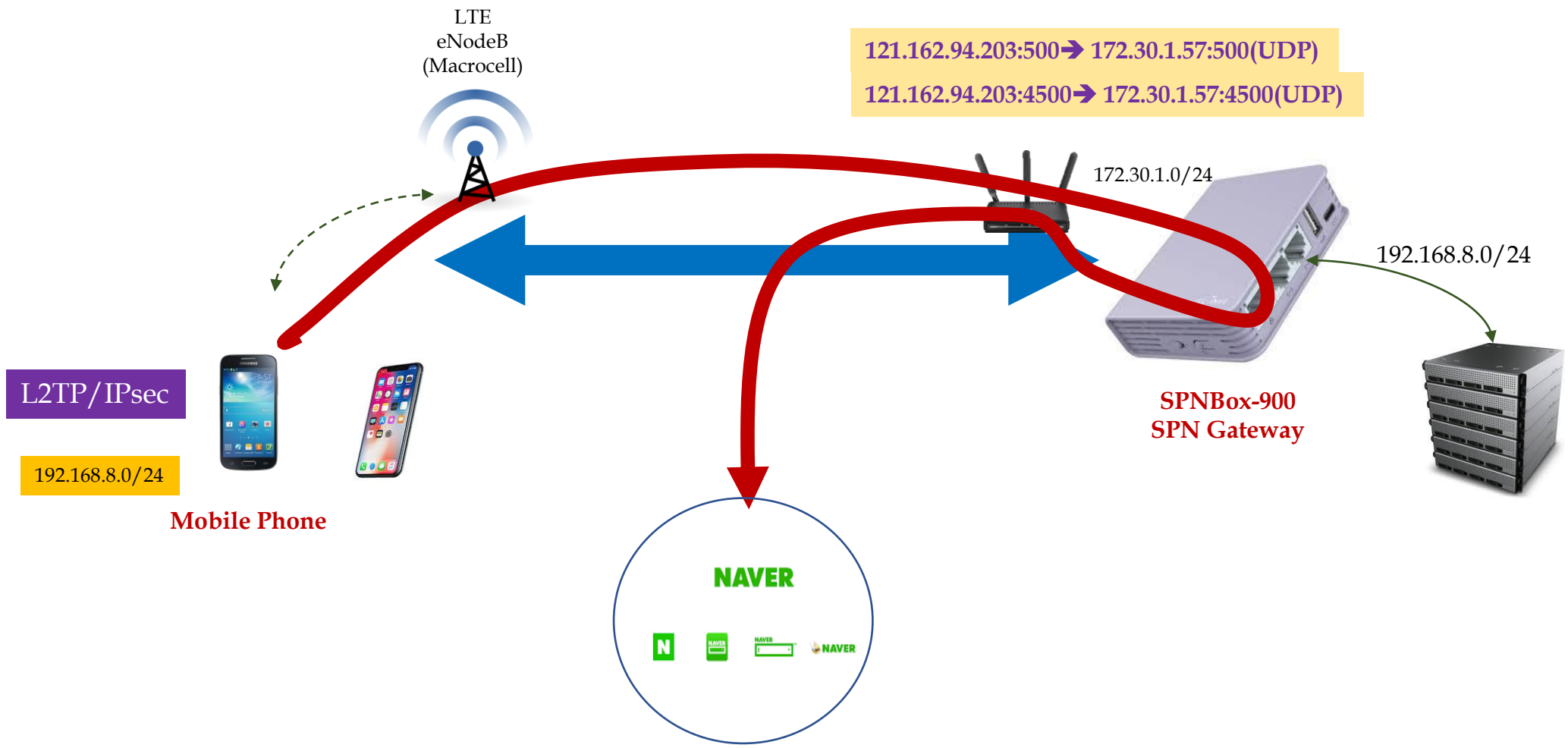
6. SPN Gateway & Mobile Phone(5) – Android 설정(2)

- <L2TP/IPsec 설정 참고 Site>
- https://www.softether.org/4-docs/2-howto/9.L2TPIPsec_Setup_Guide_for_SoftEther_VPN_Server
- Android, iPhone, Windows, MacOS에서의 L2TP/IPsec 설정 방법이 잘 정리되어 있음.

6. SPN Gateway & Mobile Phone(6) – VPN 연결 시험(1)

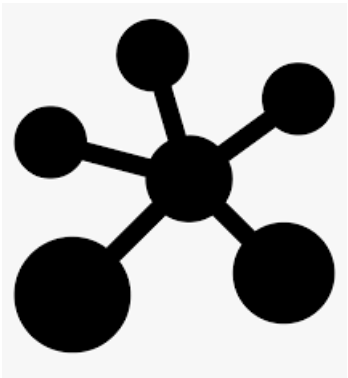


6. SPN Gateway & Mobile Phone(6) – VPN 연결 시험(2)

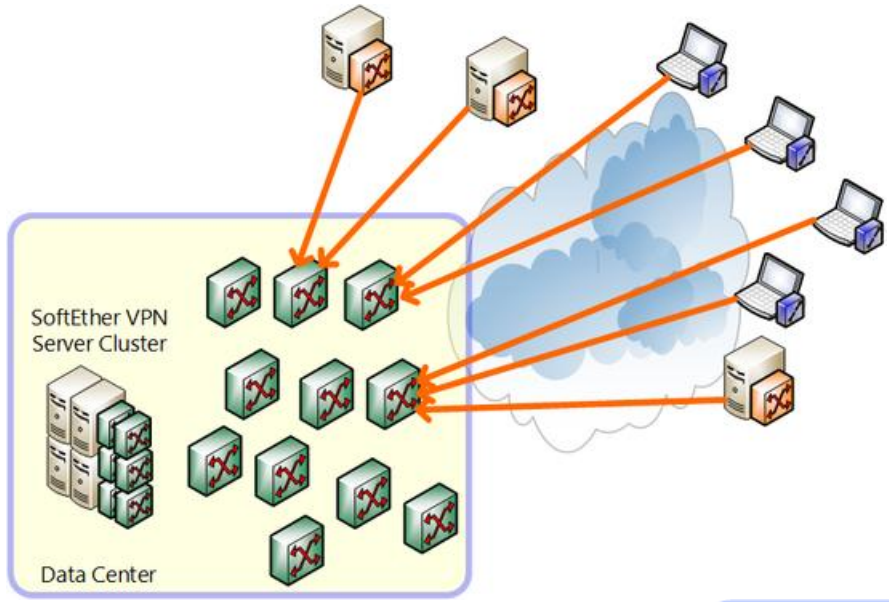


7. SPN Gateway Cluster
: Setup Guide

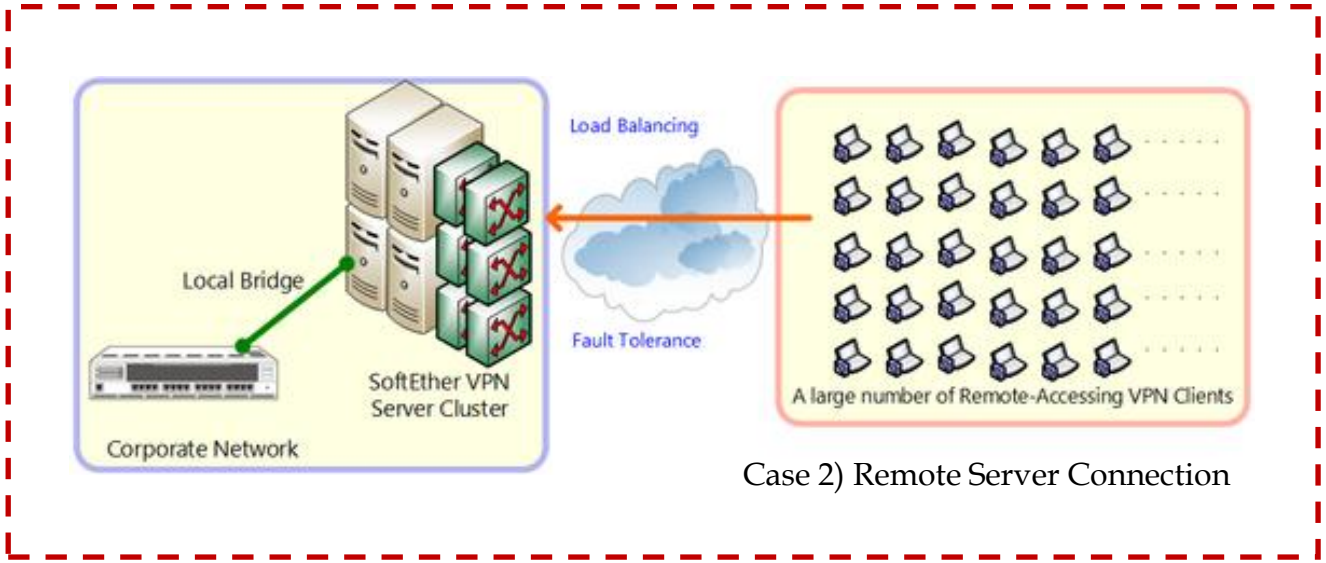
수십(최대 64) 개의 SPN Gateway를 묶어 하나의 SPN Gateway 처럼 사용하는 기능



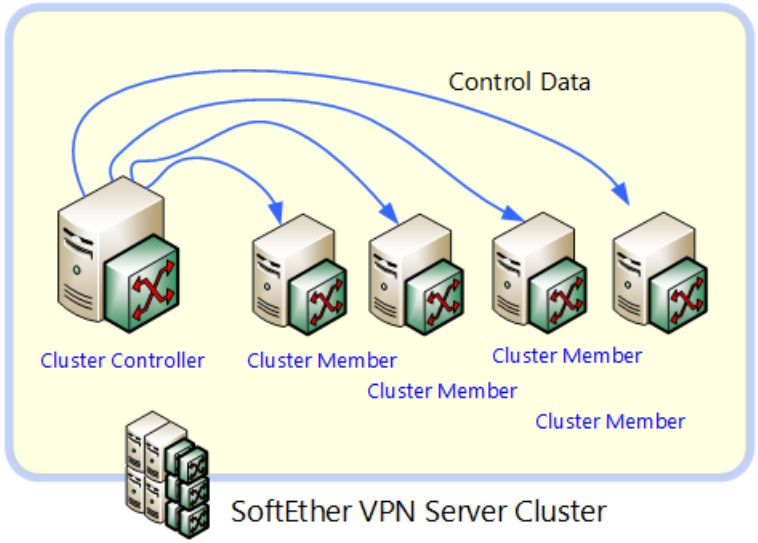
7. SPN Gateway Cluster(1) – SE Clustering 개요(1)



Case 1) Virtual Server Hosting

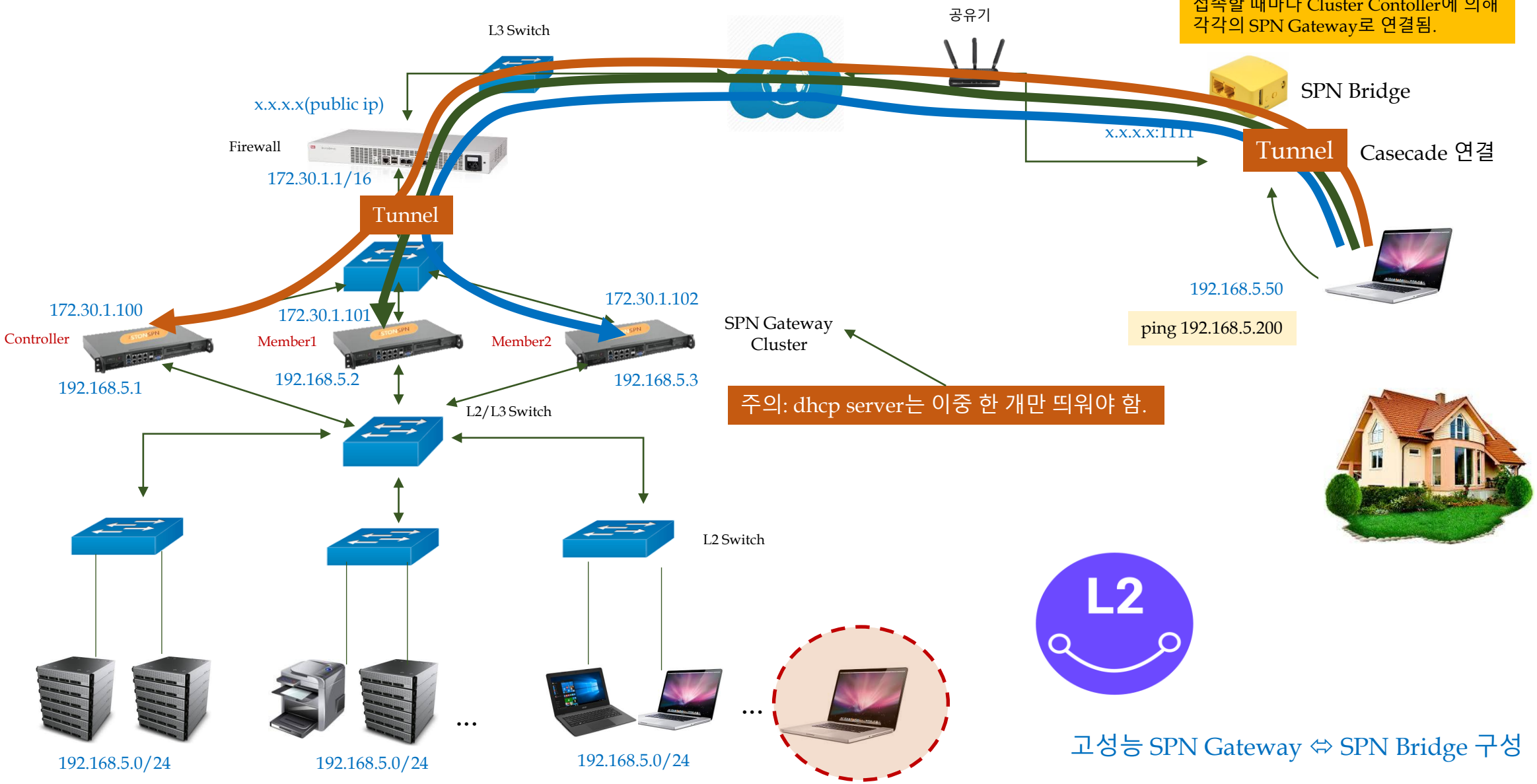


Case 2) Remote Server Connection



7. SPN Gateway Cluster(1) – SE Clustering 개요(2)

접속할 때마다 Cluster Contoller에 의해 각각의 SPN Gateway로 연결됨.

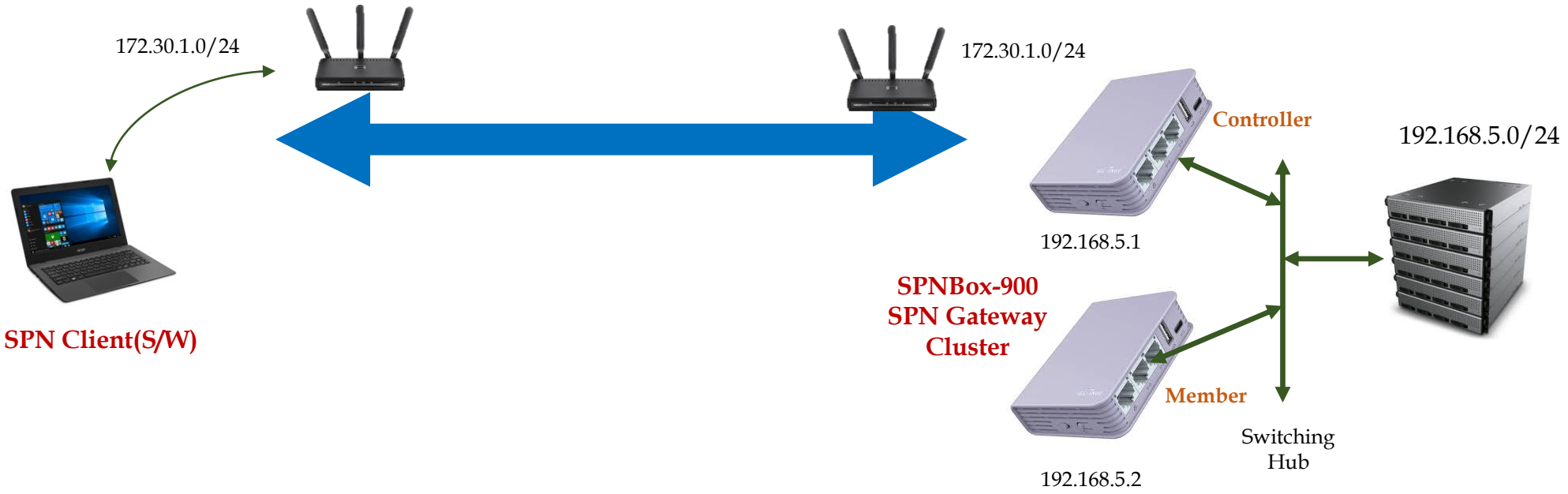


고성능 SPN Gateway ⇔ SPN Bridge 구성

7. SPN Gateway Cluster(2) – Testbed(1)

121.162.94.203:21988 ➔ 172.30.1.15:443 Controller용 Port Forwarding 규칙

121.162.94.203:21999 ➔ 172.30.1.57:443 Member 용 Port Forwarding 규칙



주의: dhcp server는 SPN Gateway 중에서 오직 1개만 구동시켜야 함. 안그러면 네트워크가 이상하게 동작함.

이 장에서는 위의 네트워크(테스트베드) 환경에서 VPN 연결 시험을 진행하도록 하겠습니다.

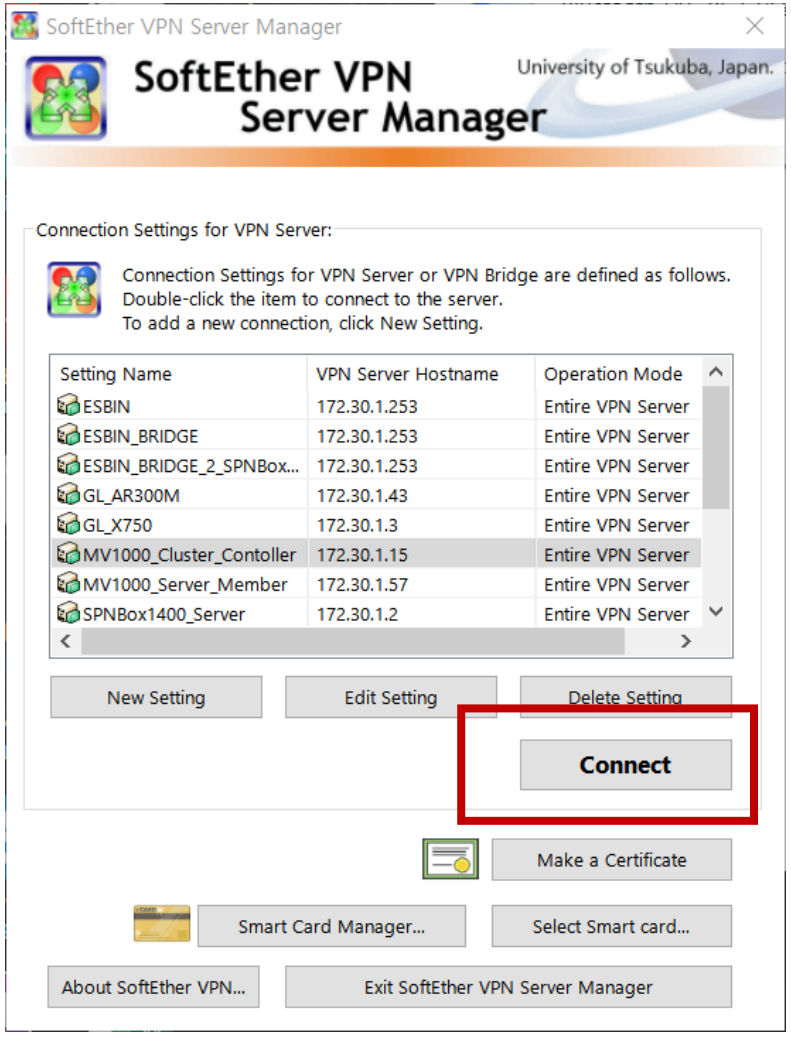
7. SPN Gateway Cluster(2) – Testbed(2)

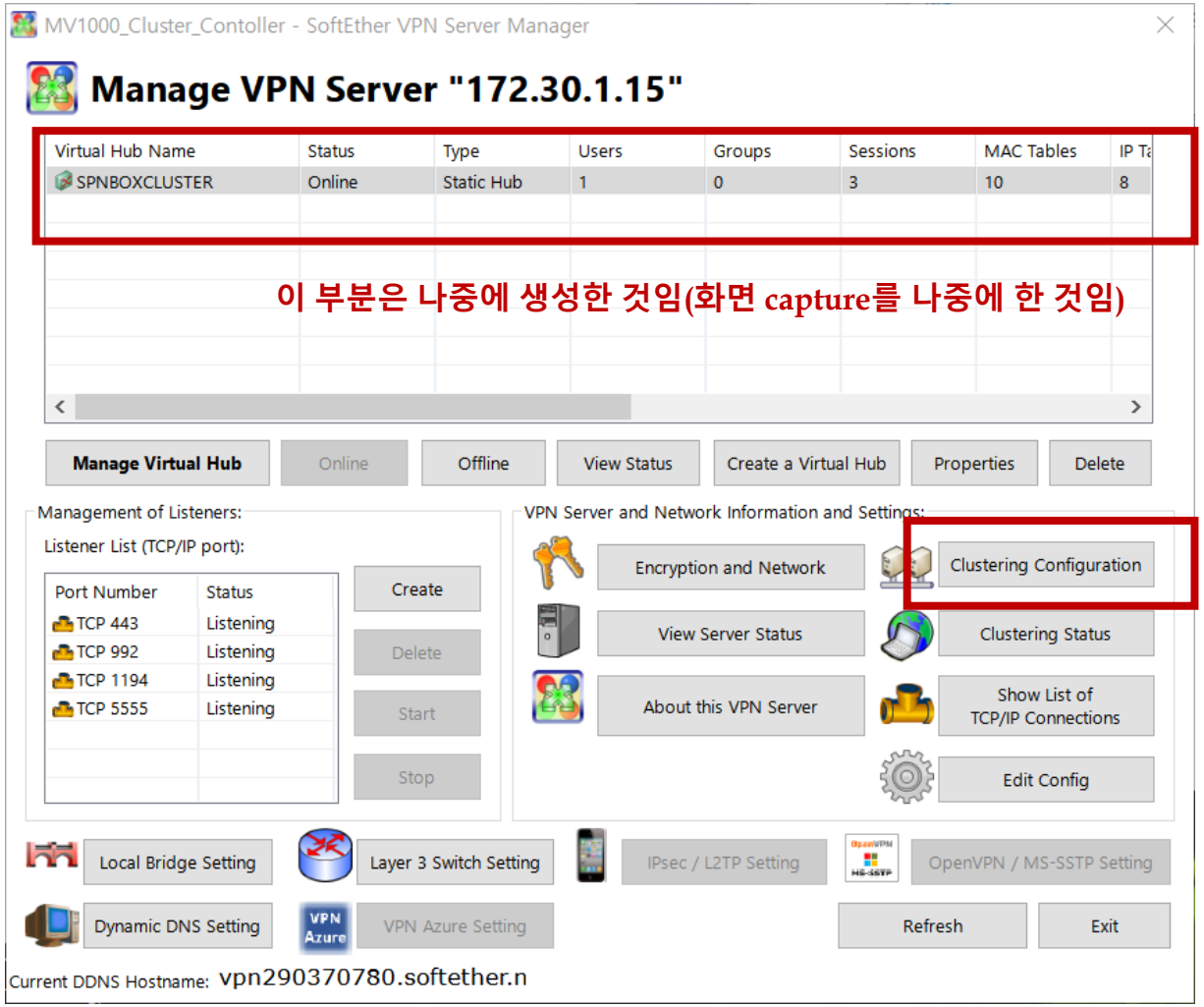
SPN Gateway	전체 설정 절차 요약
a)	VPN Server 2개 (이상)를 구동시키고, 각각 vpncmd(CLI: se vcmd run 명령)로 admin password를 설정한다(SPNBox CLI에서 수행)
b)	**<Cluster Controller용 SPN Gateway 설정>** ▪ Windows PC에서 VPN Server Manager로 VPN Server 1에 접속한 후, VPN Server1을 Cluster Controller로 지정한다. ▪ 이후 Virtual Hub(예: SPNBOXCLUSTER)를 하나 생성한 후, Static으로 지정한다. 물론 새로운 Virtual Hub을 신규로 생성했으니, 이를 사용하는 사용자도 새로 추가해야 한다(예: cuser/cuser1234). ▪ 끝으로, Local Bridge를 하나 생성하여 Physical network과 연결한다(이것은 기존 방식과 동일). 주의: CLI에서 tap_vpn이 br-lan bridge에 통함되었는지 확인하도록 하자.
c)	**<Cluster Member 용 SPN Gateway 설정>** ▪ Windows PC에서 VPN Server Manager로 VPN Server 2에 접속한 후, VPN Server2을 Cluster Member로 지정한다. Cluster Member는 자신의 정보와 Cluster Controller 정보를 알 필요가 있으므로, 이를 설정시 입력해 준다. ▪ 이후 Virtual Hub은 별도로 생성할 필요가 없다(사용자도 새로 추가할 필요 없음). ▪ 하지만, Local Bridge를 하나 생성하여 Physical network과 연결해 주어야 한다(이것은 기존 방식과 동일). 주의: CLI에서 tap_vpn이 br-lan bridge에 통함되었는지 확인하도록 하자.

주의: Firewall에서 SPN Gateway1, SPN Gateway2 각각에 대해 Port Forwarding 설정을 해 주어야 함.

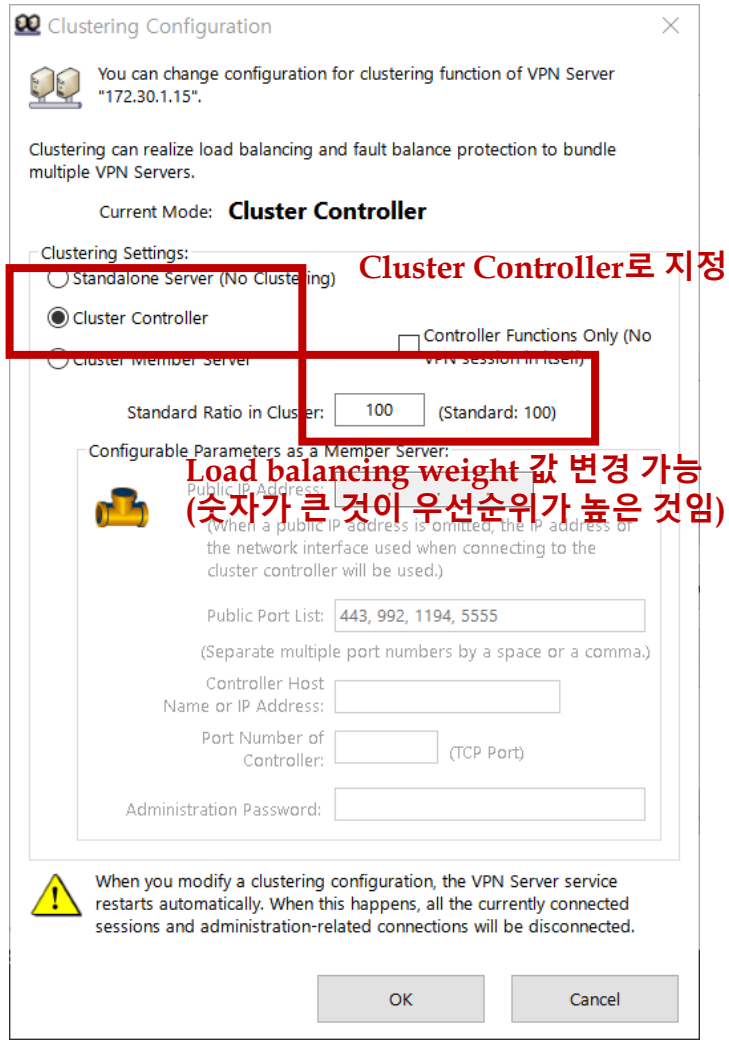
SPN Client	전체 설정 절차 요약
a)	VPN Client Manager를 실행한 후, VPN 설정을 한다. 이때 아래 정보가 필요하다. ▪ VPN Server에서 추가한 **Virtual Hub 이름** 및 **사용자 계정 정보** ▪ Firewall or AP 안쪽에 VPN Server가 있을 경우, port forwarding 설정 및 이와 관련된 정보(**Firewall External IP, port**)

7. SPN Gateway Cluster(3) – Cluster Controller 설정(1)



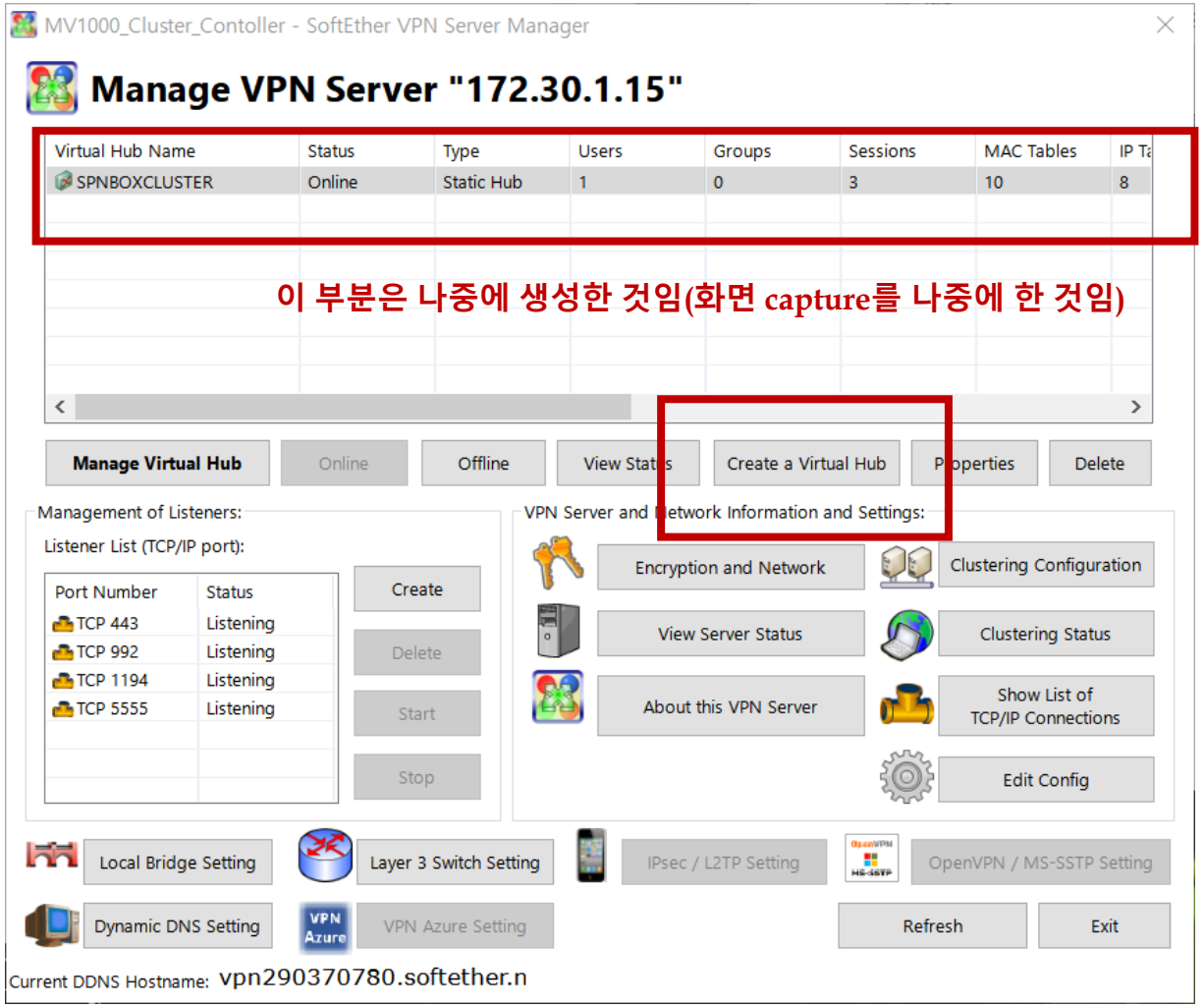


7. SPN Gateway Cluster(3) – Cluster Controller 설정(2)



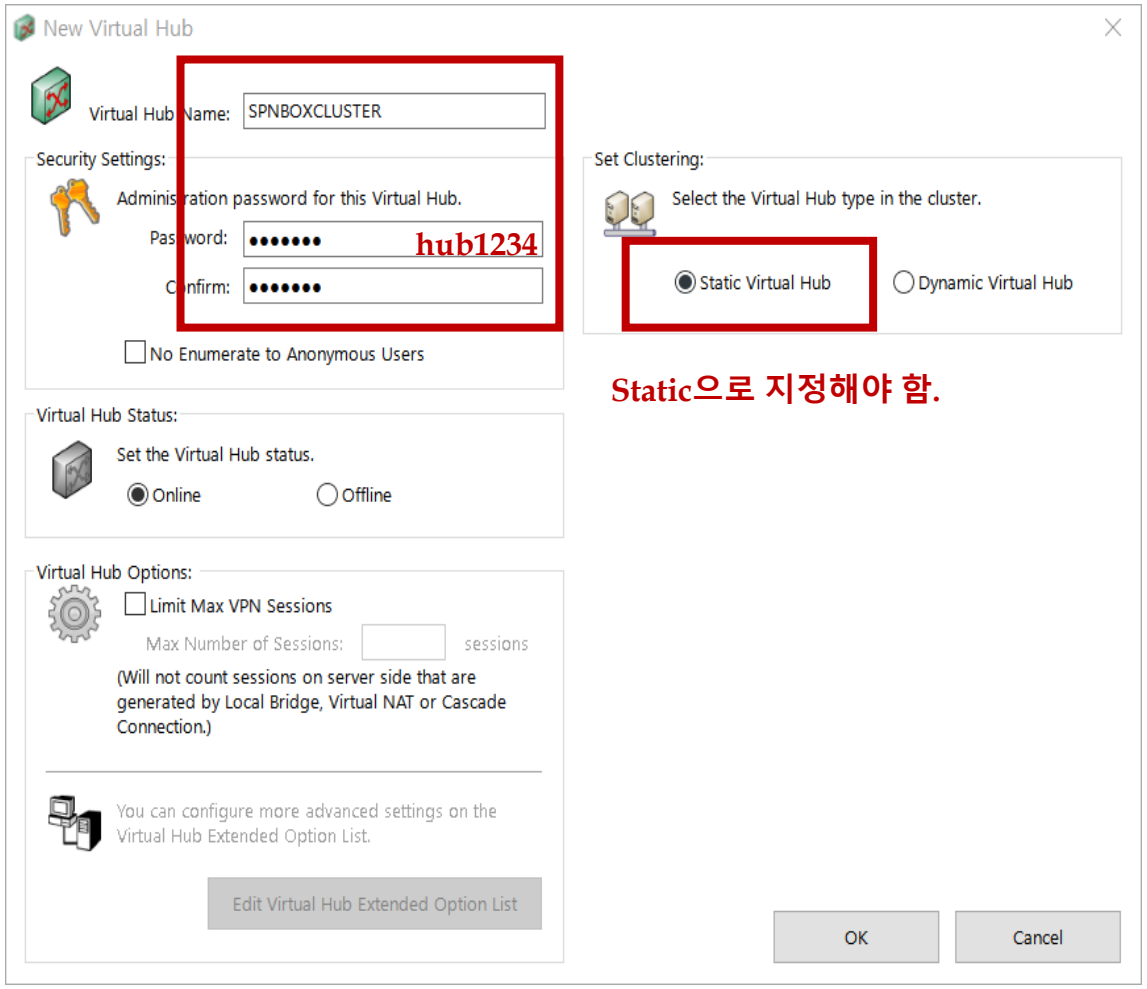
Cluster Controller로 지정

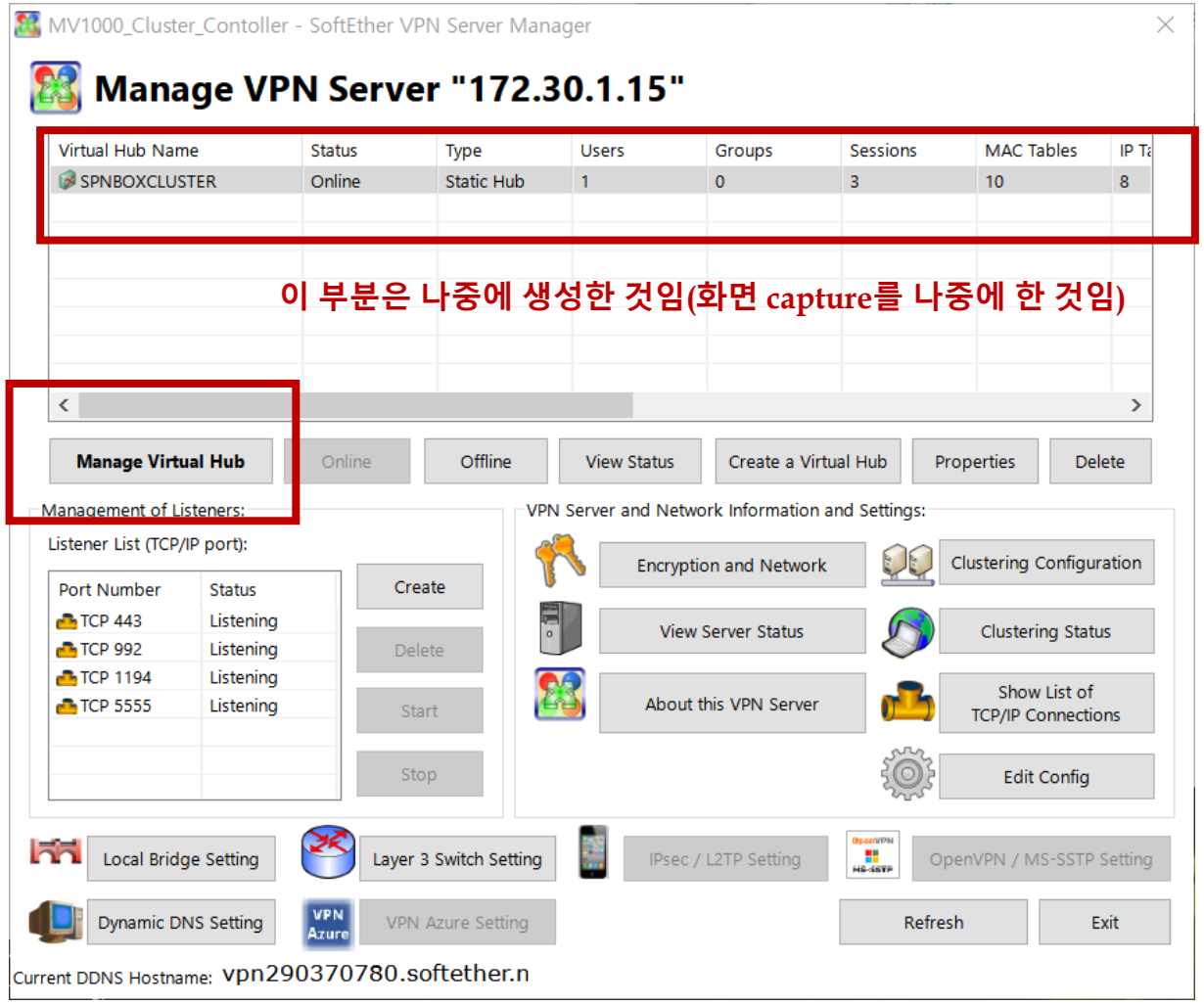
Load balancing weight 값 변경 가능
(숫자가 큰 것이 우선순위가 높은 것임)



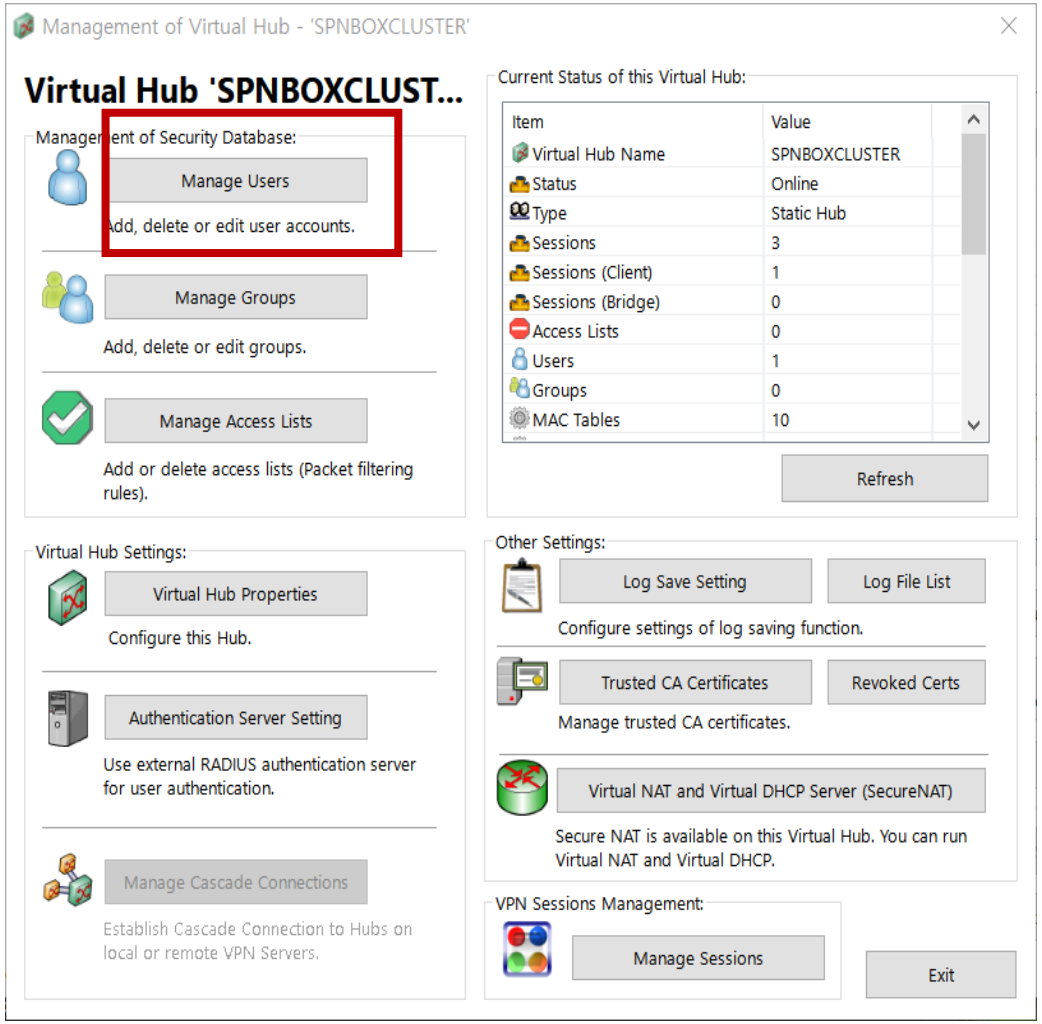
이 부분은 나중에 생성한 것임(화면 capture를 나중에 한 것임)

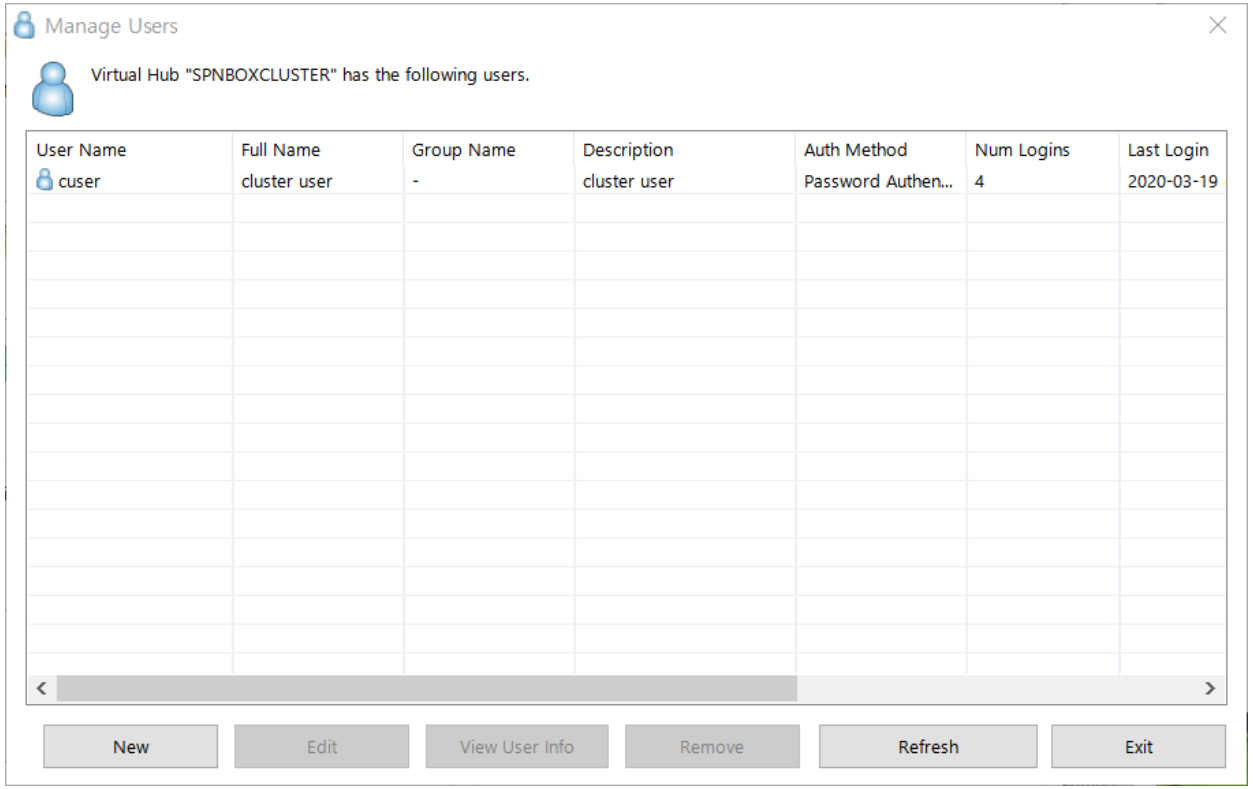
7. SPN Gateway Cluster(3) – Cluster Controller 설정(3)





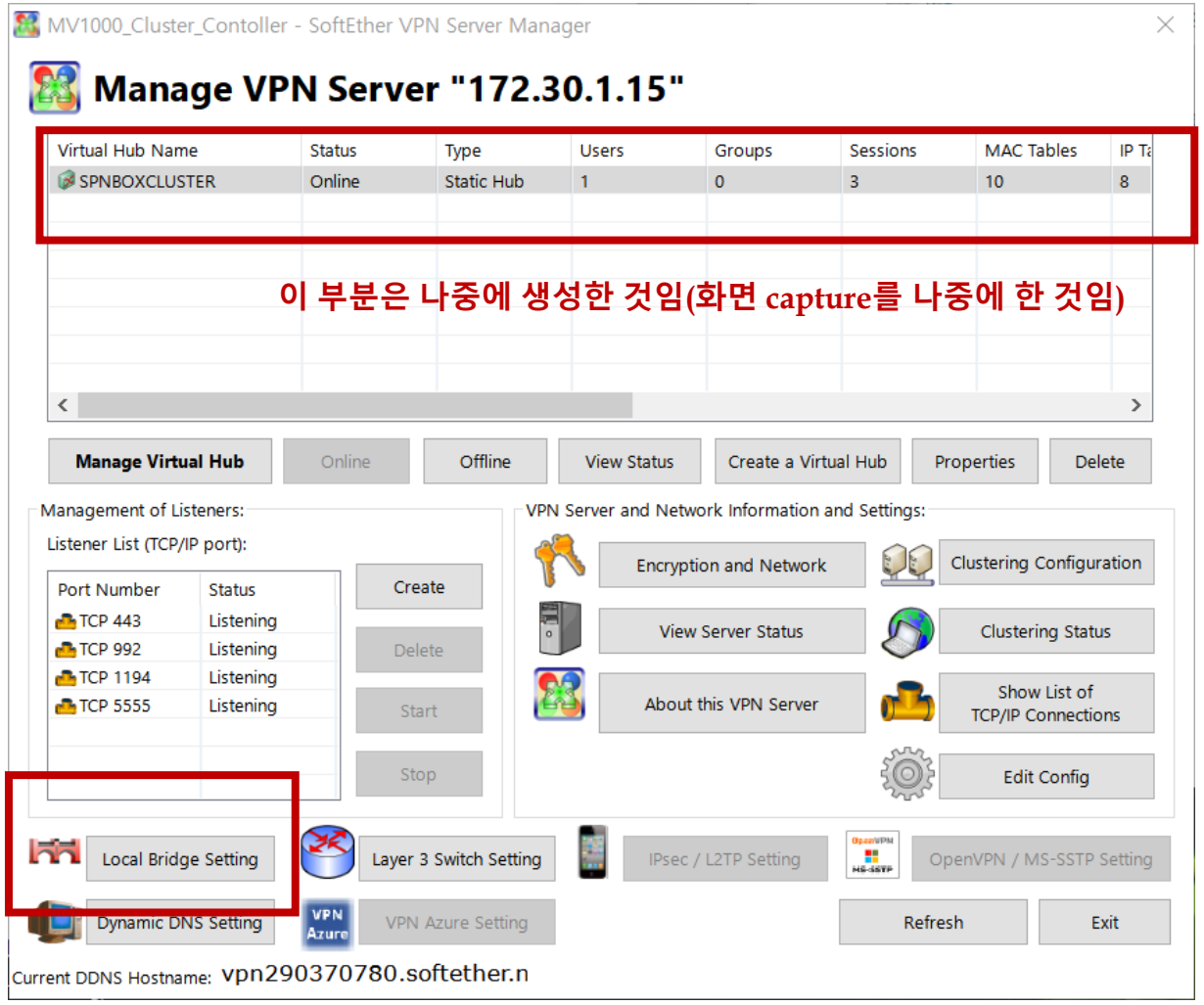
7. SPN Gateway Cluster(3) – Cluster Controller 설정(4)

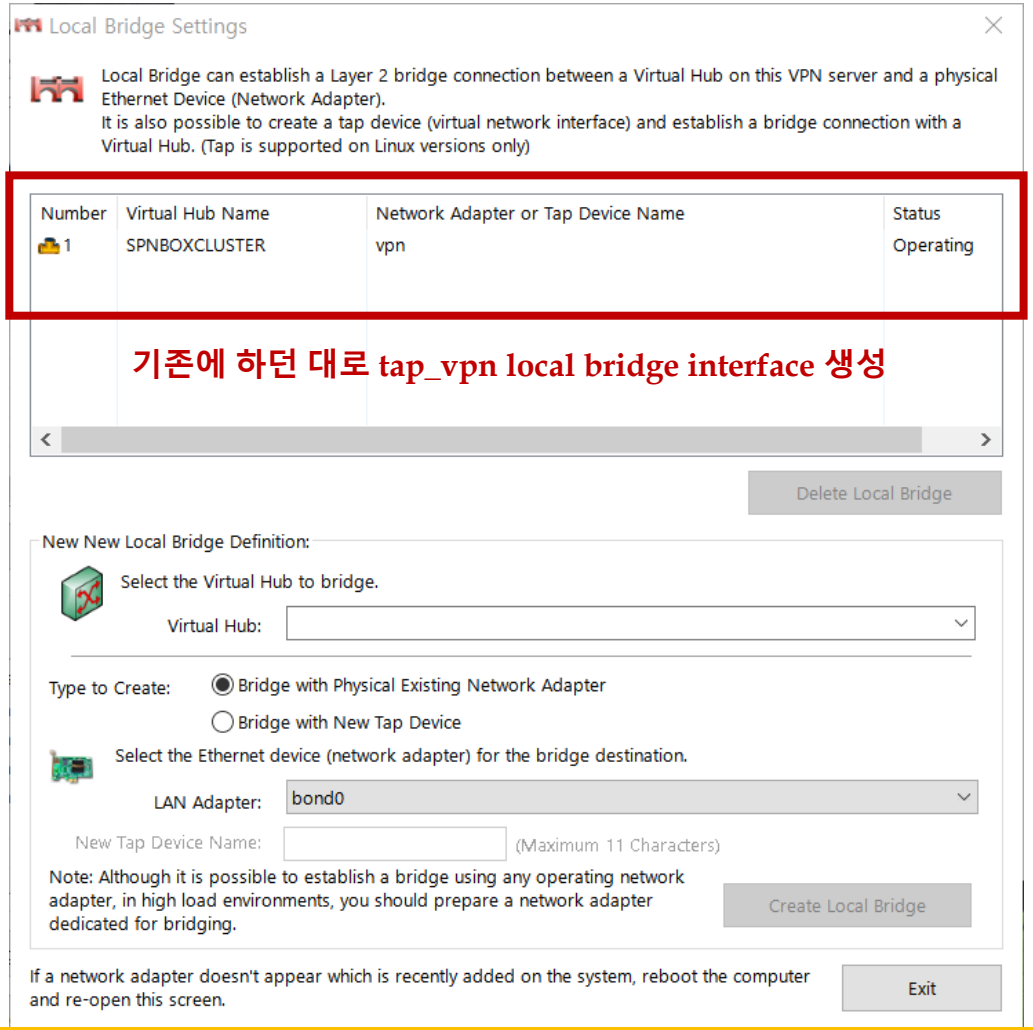




사용자를 하나 등록: cuser/cuser1234

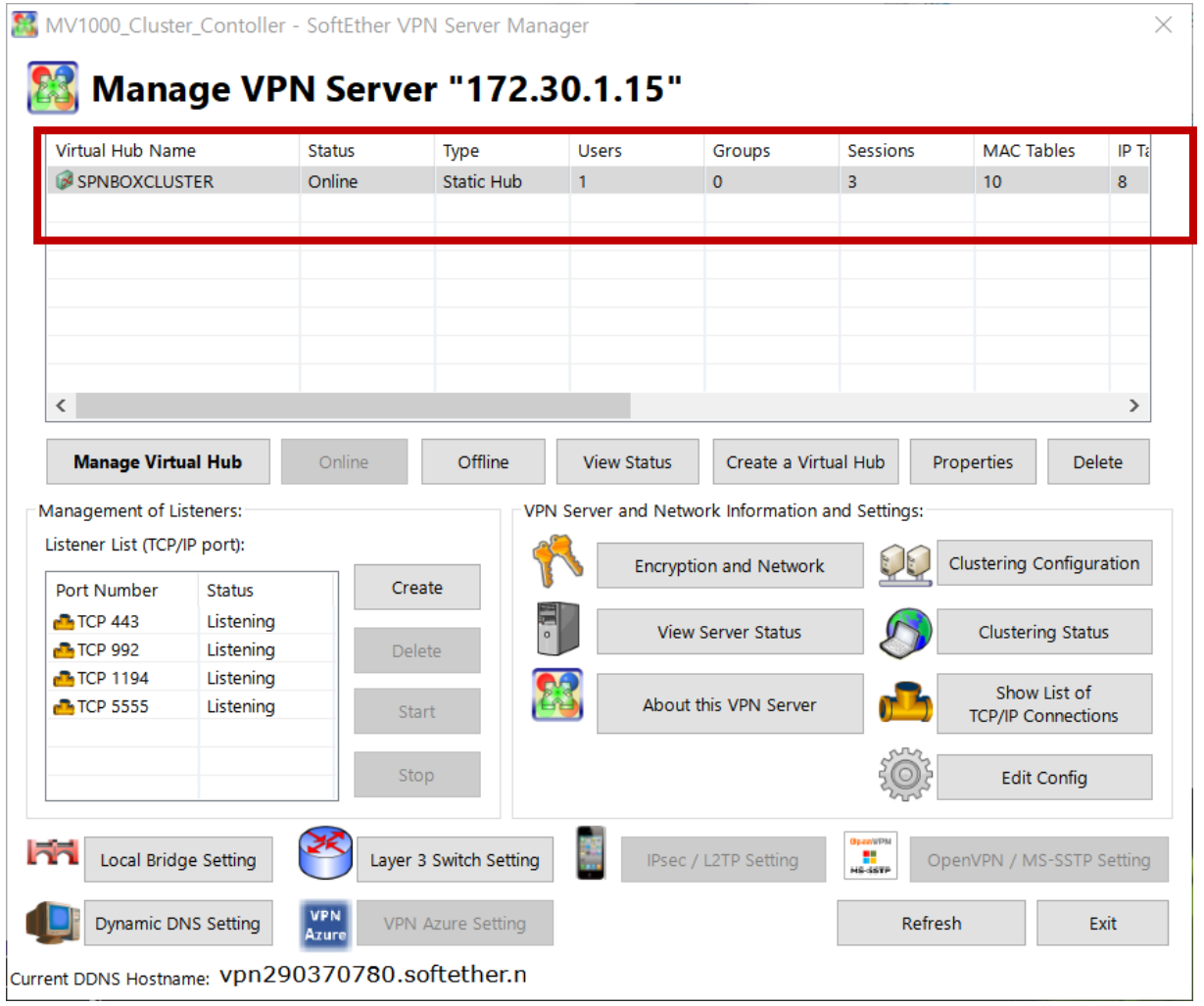
7. SPN Gateway Cluster(3) – Cluster Controller 설정(5)



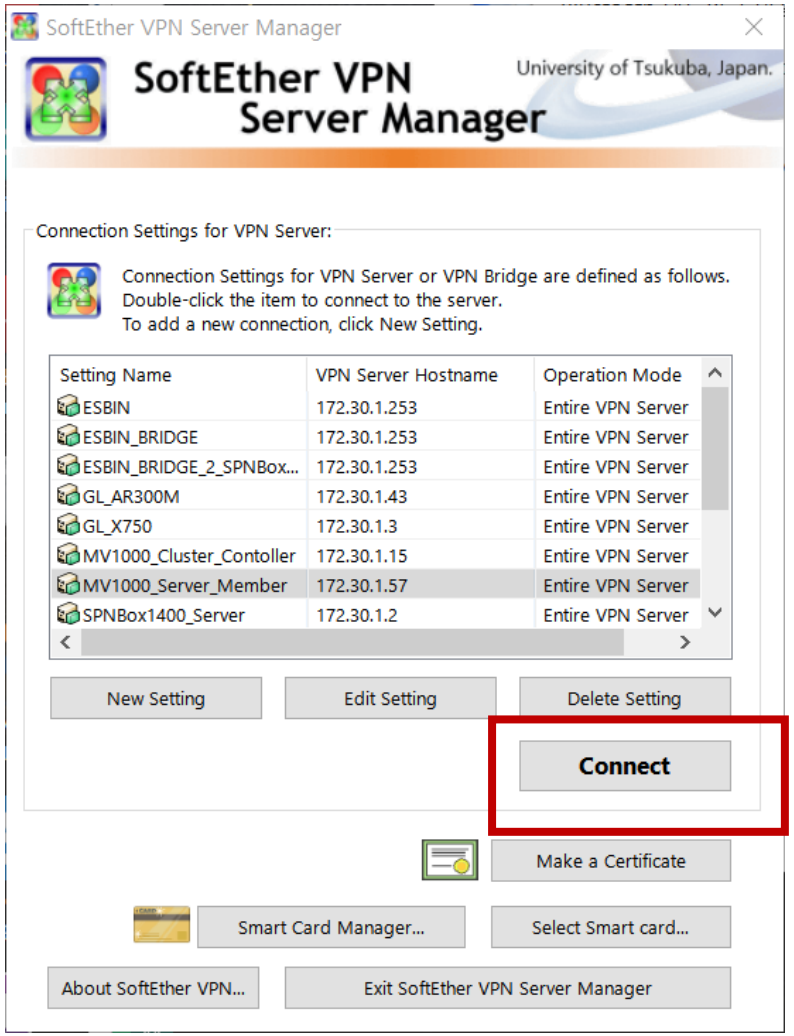


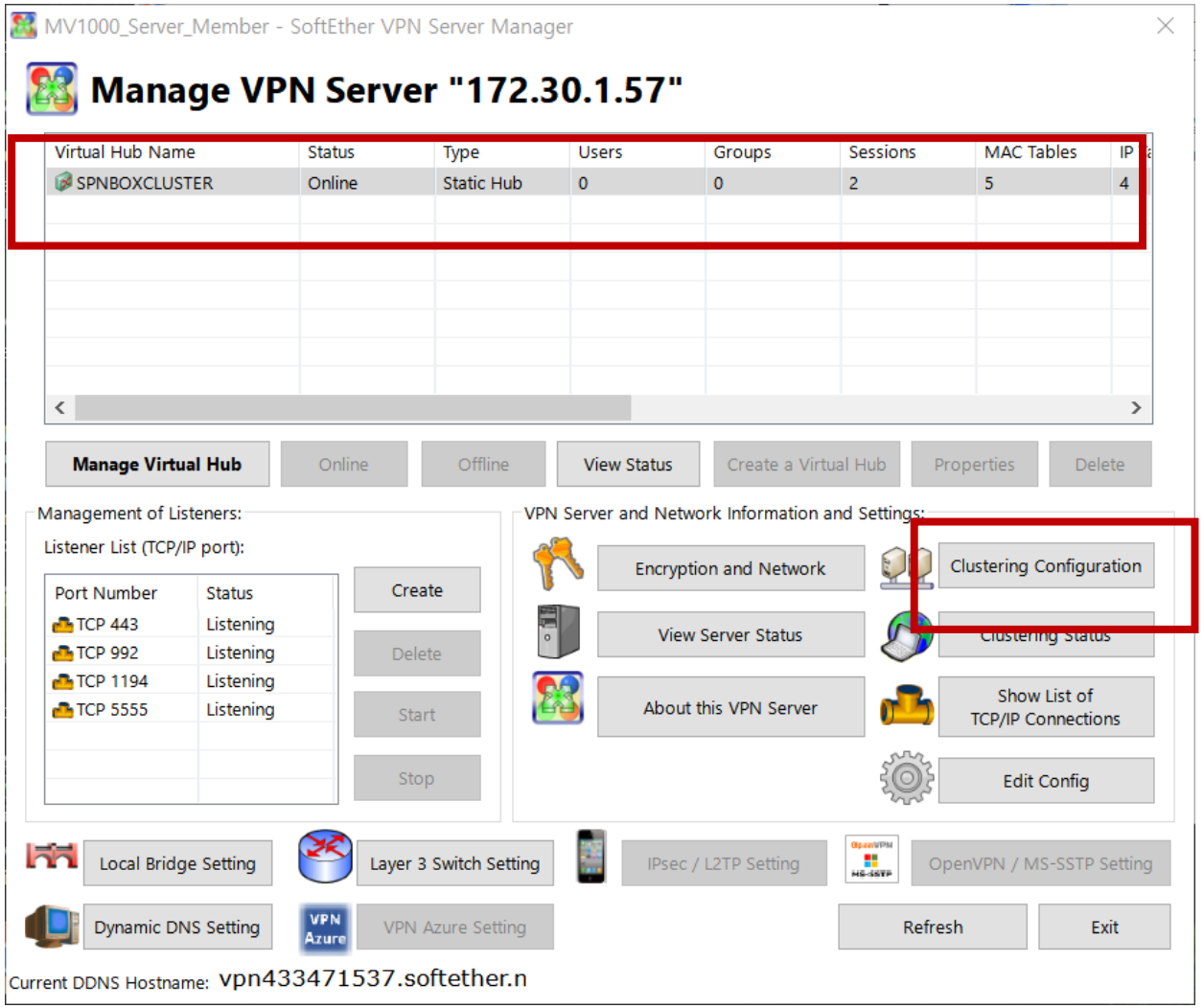
주의: 이 상태에서 CLI로 tap_vpn이 bridge br-lan에 통합되었는지 확인 요망

7. SPN Gateway Cluster(3) – Cluster Controller 설정(6)

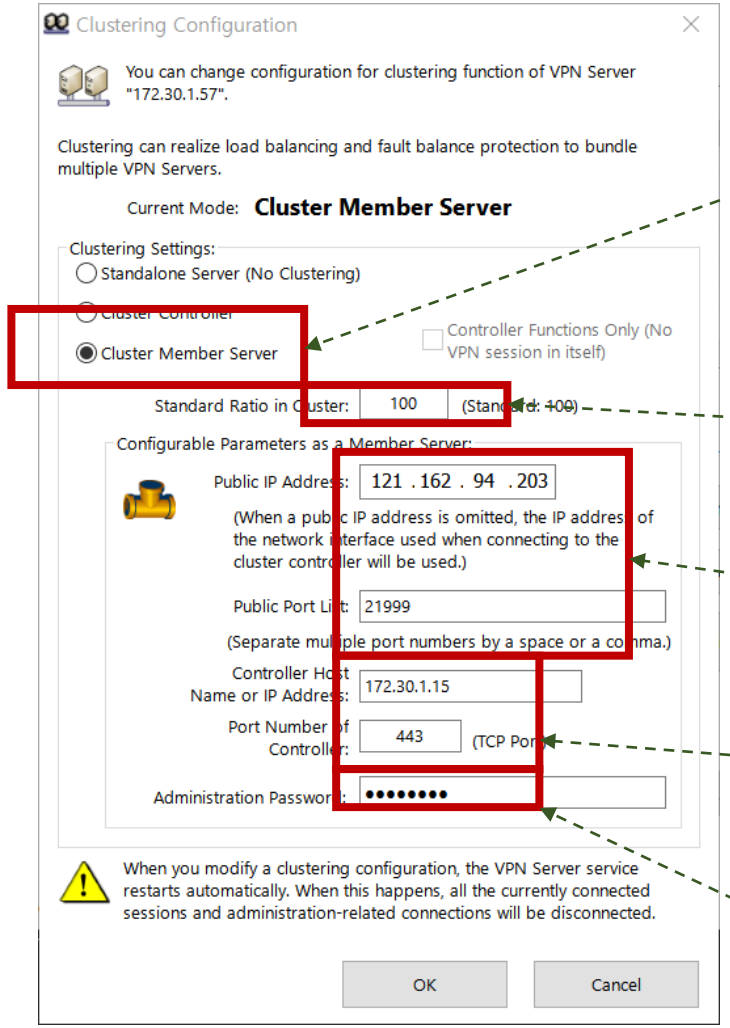


7. SPN Gateway Cluster(4) – Cluster Member 설정(1)





7. SPN Gateway Cluster(4) – Cluster Member 설정(2)



Cluster Member로 설정

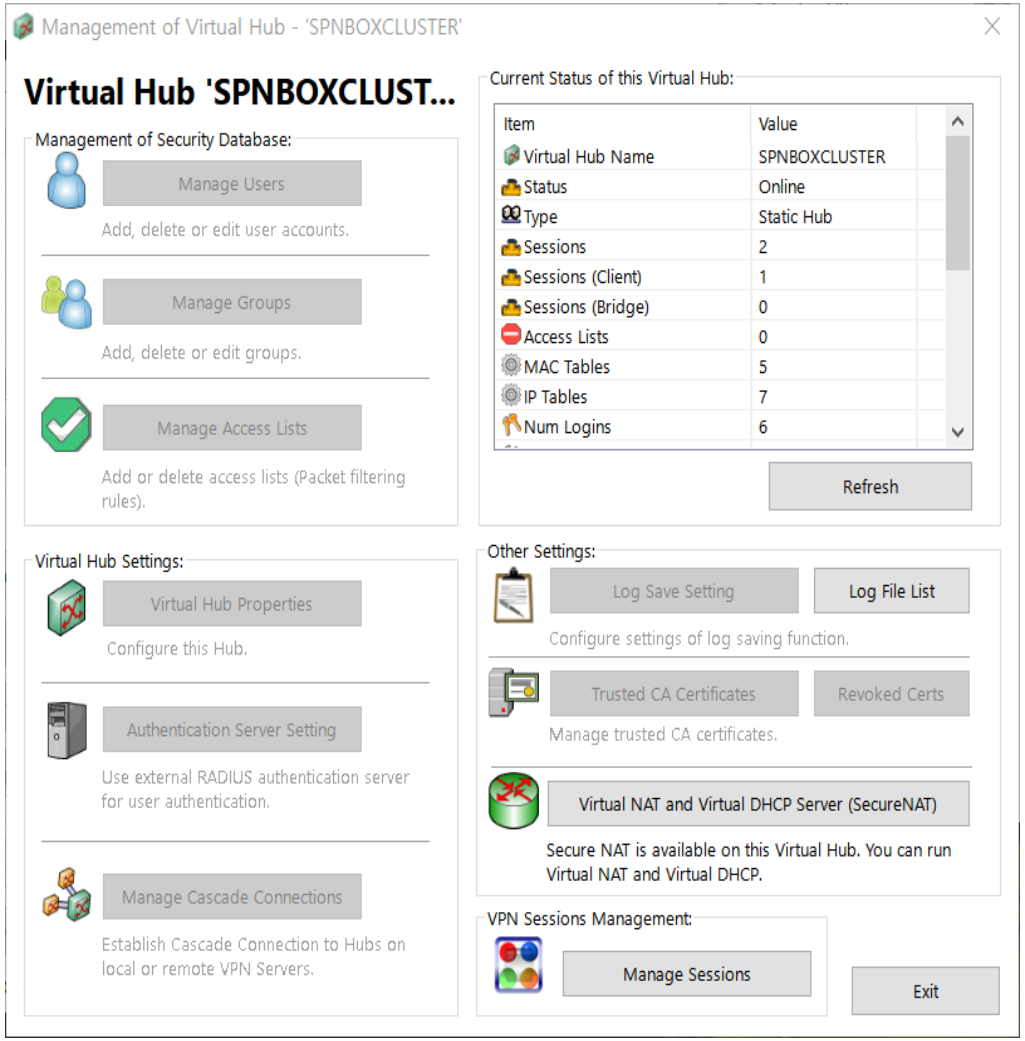
Load balancing weight 값 변경 가능
(숫자가 큰 것이 우선순위가 높은 것임)

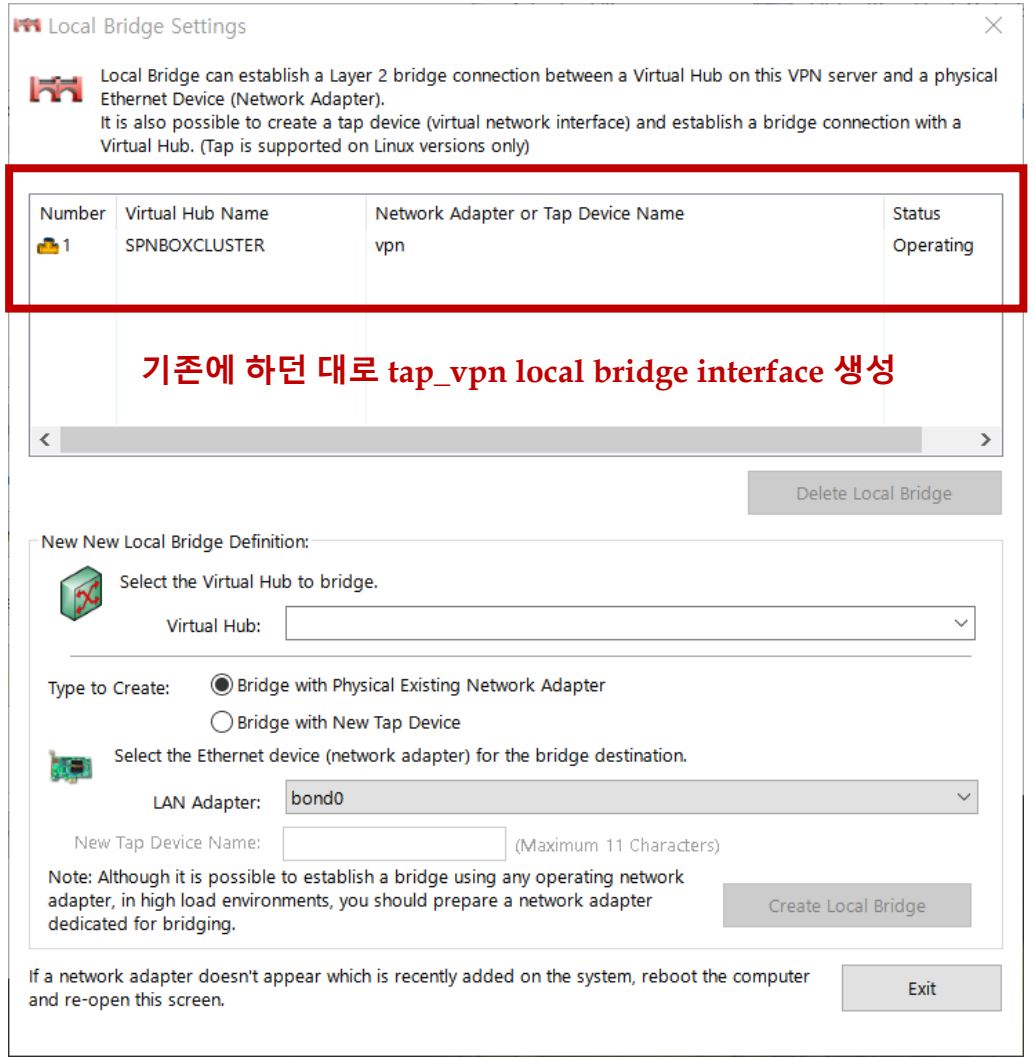
Cluster Member용 SPN Gateway 외부 endpoint 정보

Cluster Controller WAN 정보
Port는 443 이외에도 1194, 992, 5555 등 열려 있는 포트 사용 가능

spnbox1234

7. SPN Gateway Cluster(4) – Cluster Member 설정(3)

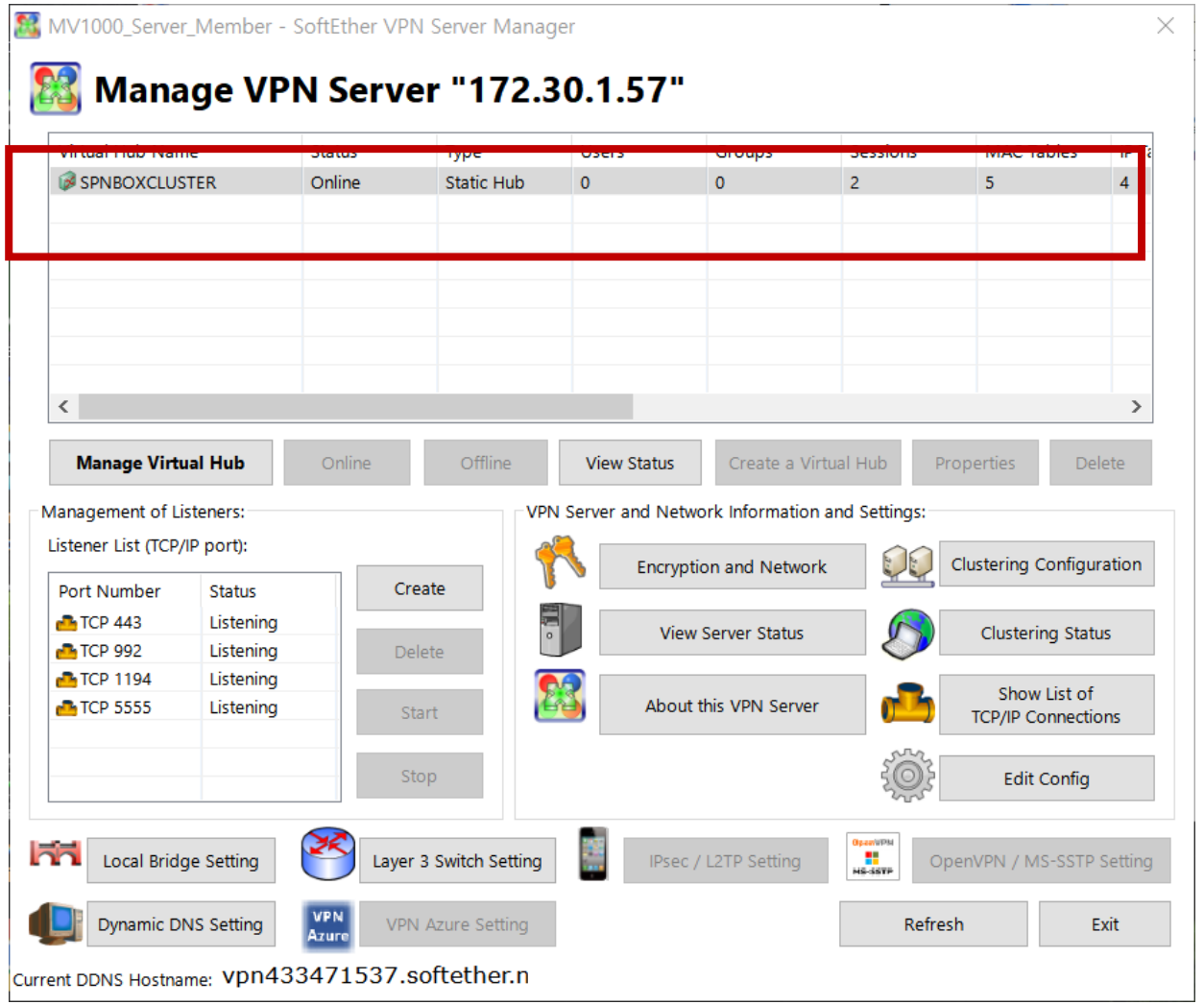




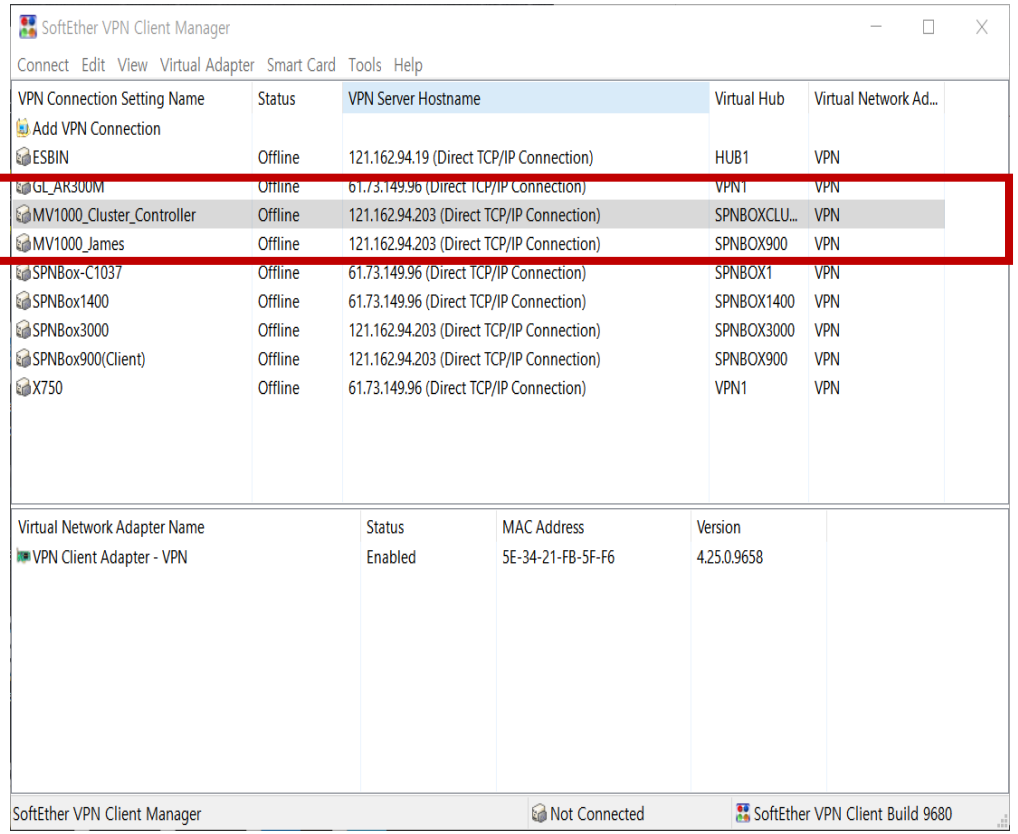
VirtualHub은 별도로 생성할 필요 없음. Controller에서 생성한 내용을 공통으로 사용함.

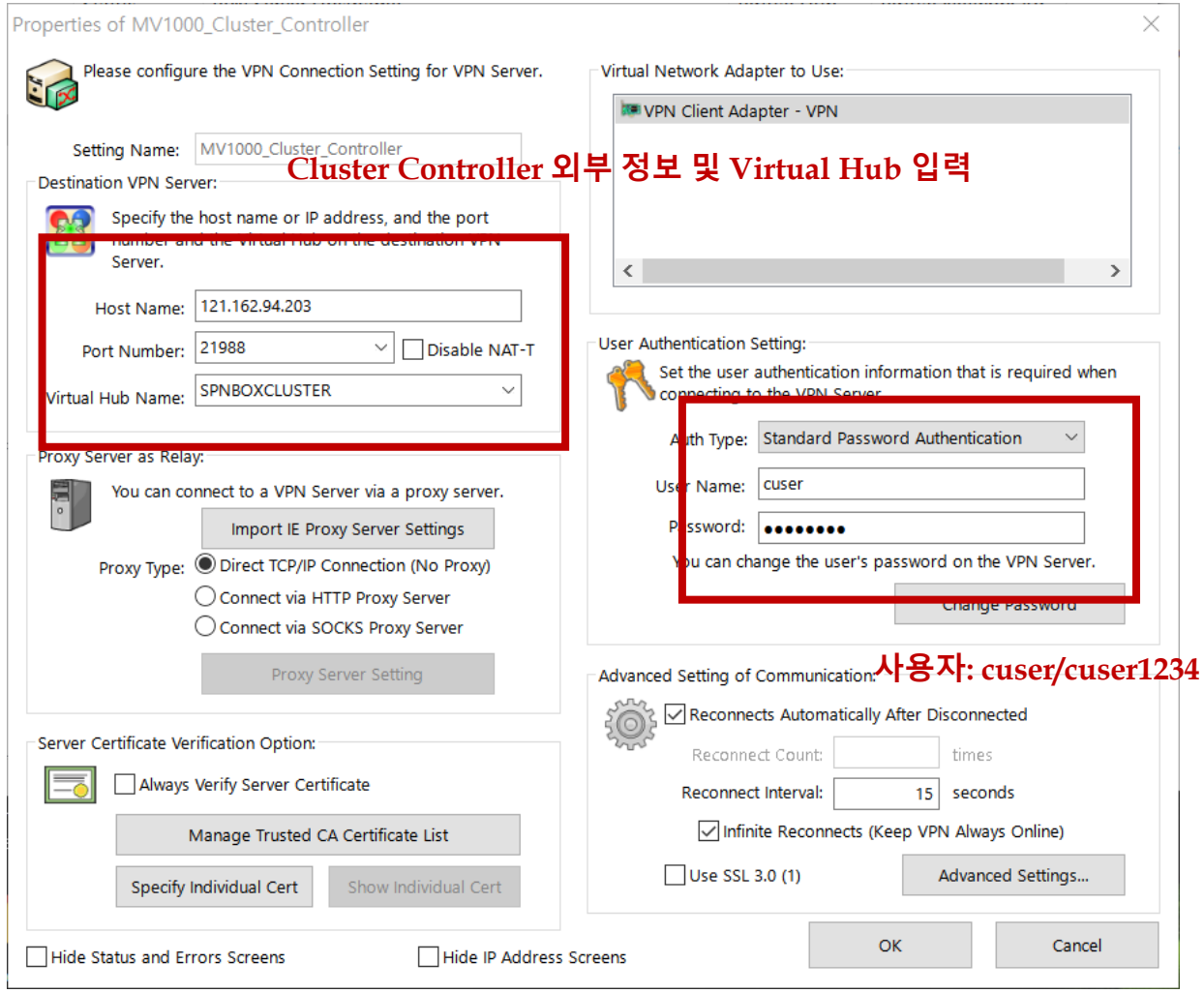
주의: 이 상태에서 CLI로 tap_vpn이 bridge br-lan에 통합되었는지 확인 요망

7. SPN Gateway Cluster(4) – Cluster Member 설정(4)

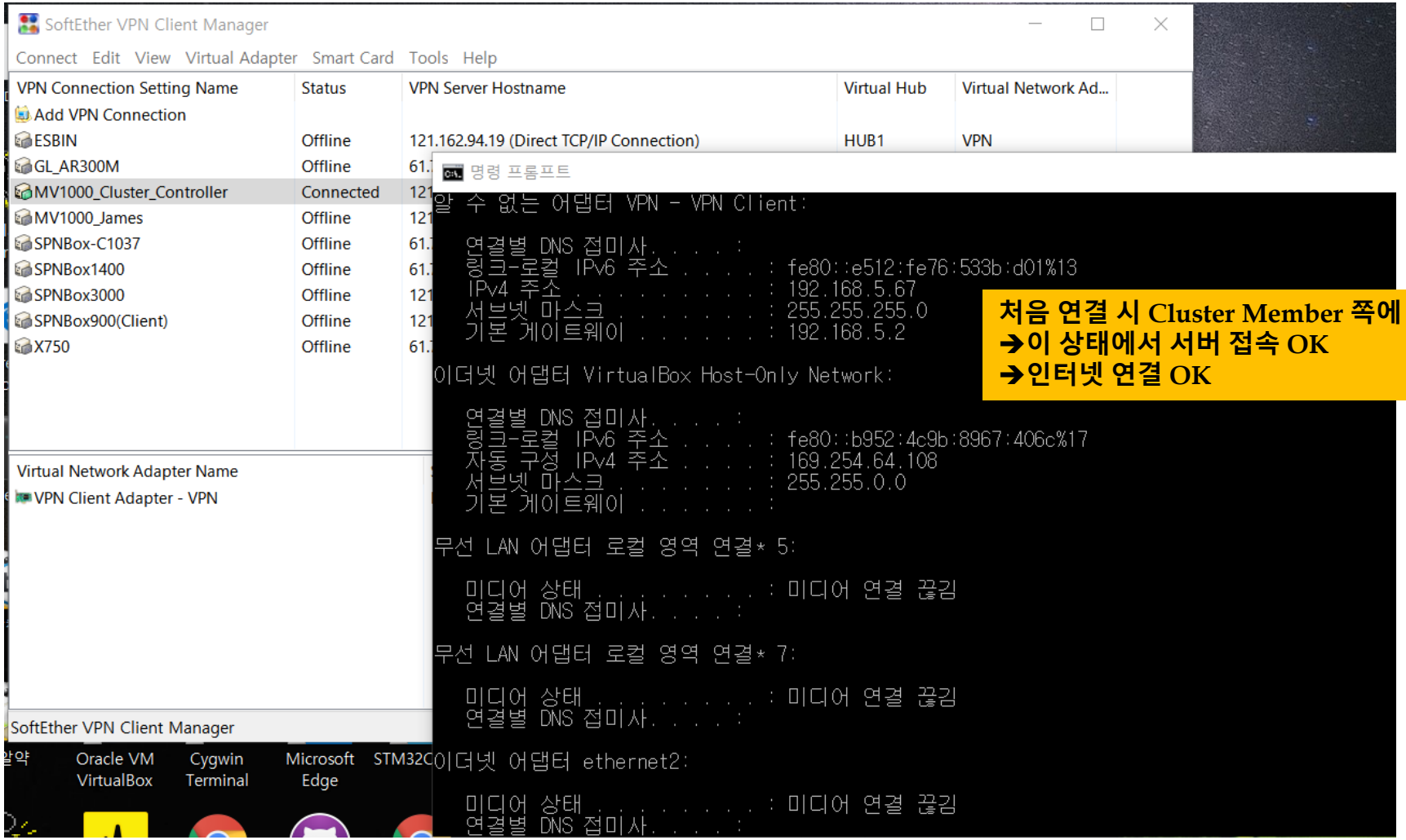


7. SPN Gateway Cluster(5) – SPN Client 설정(1)

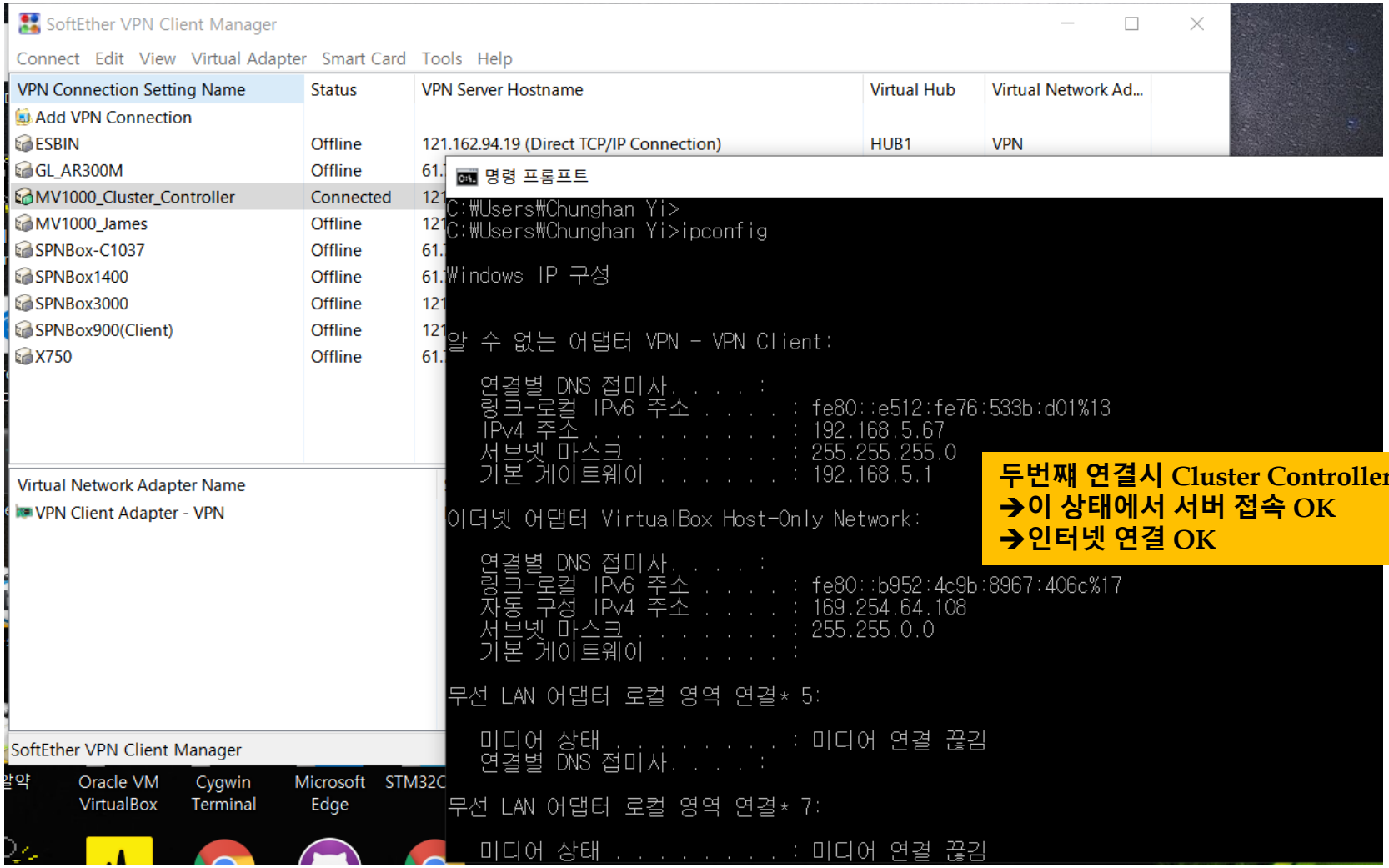




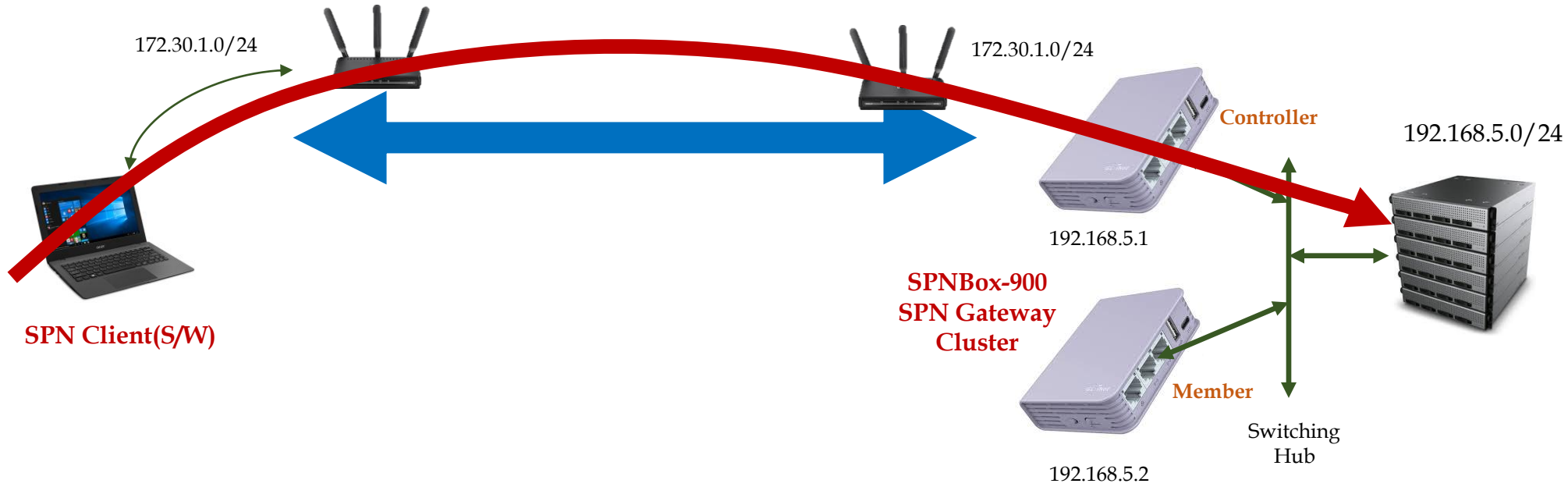
7. SPN Gateway Cluster(5) – SPN Client 설정(2)



7. SPN Gateway Cluster(5) – SPN Client 설정(3)

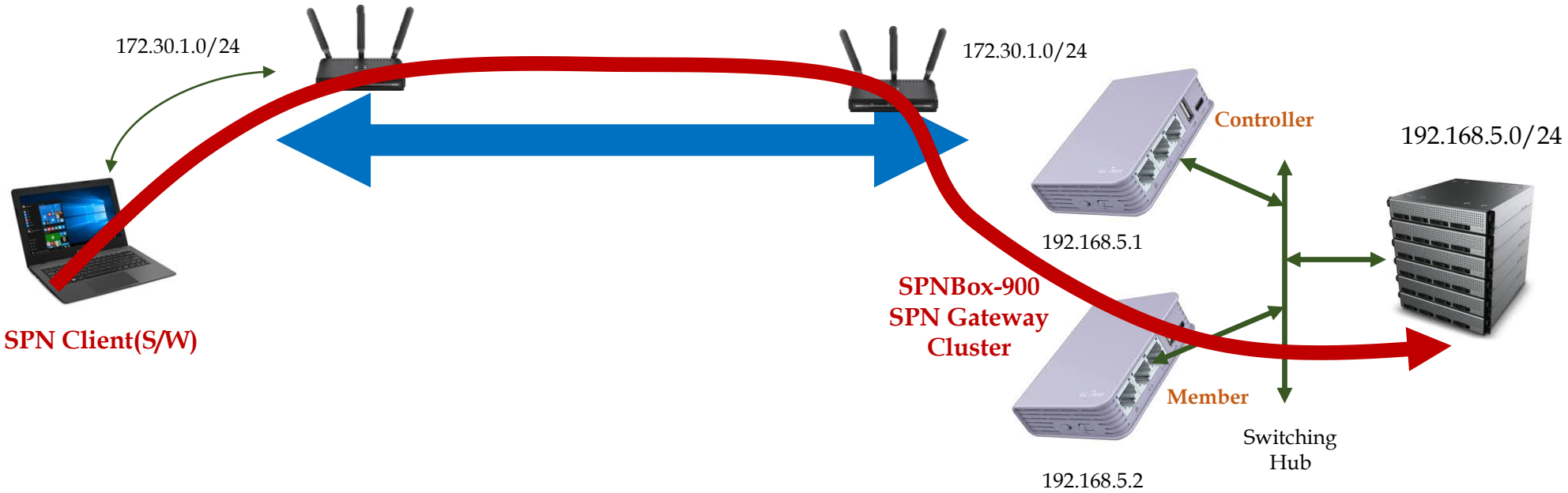


7. SPN Gateway Cluster(6) – VPN 연결 시험(1)



처음 접속 시

7. SPN Gateway Cluster(6) – VPN 연결 시험(2)



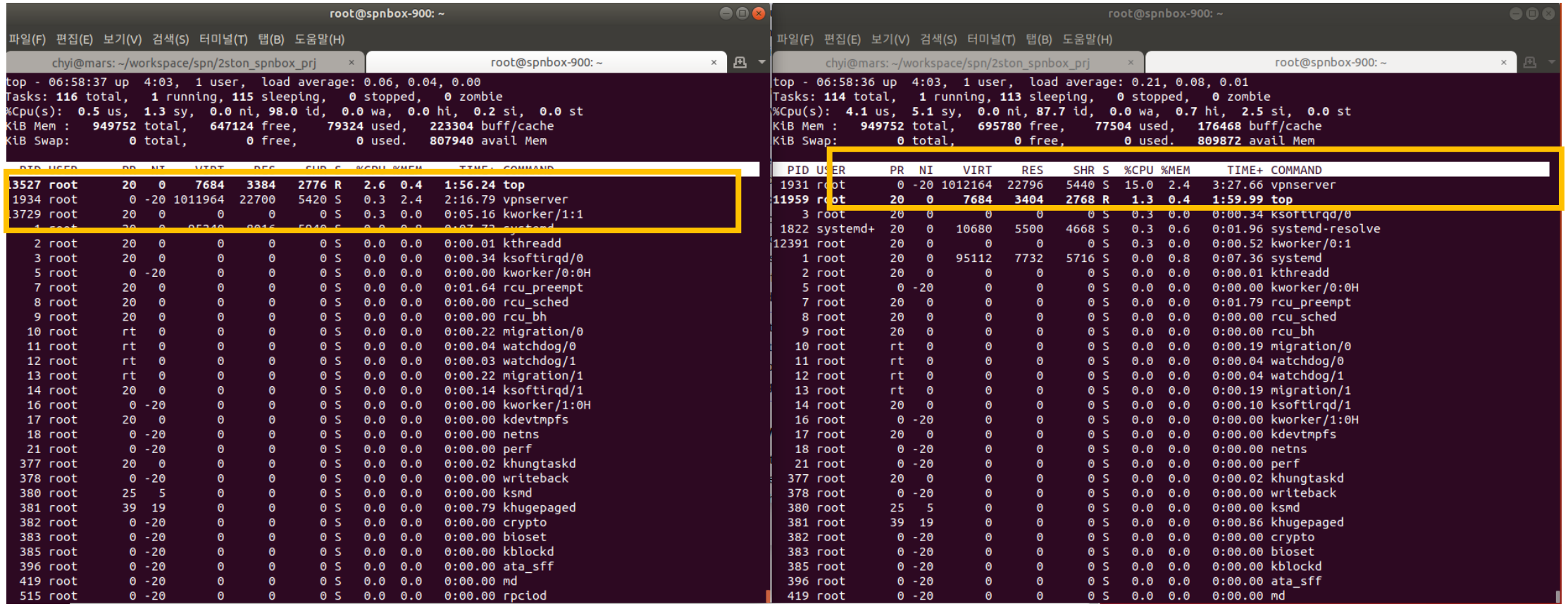
두번째 접속 시

현재 Standard Ratio 값을 100:100으로 지정했기 때문에 순차적(round-robin fashion)으로 연결됨.

7. SPN Gateway Cluster(6) – VPN 연결 시험(3)

SPN Gateway2(Cluster Member)

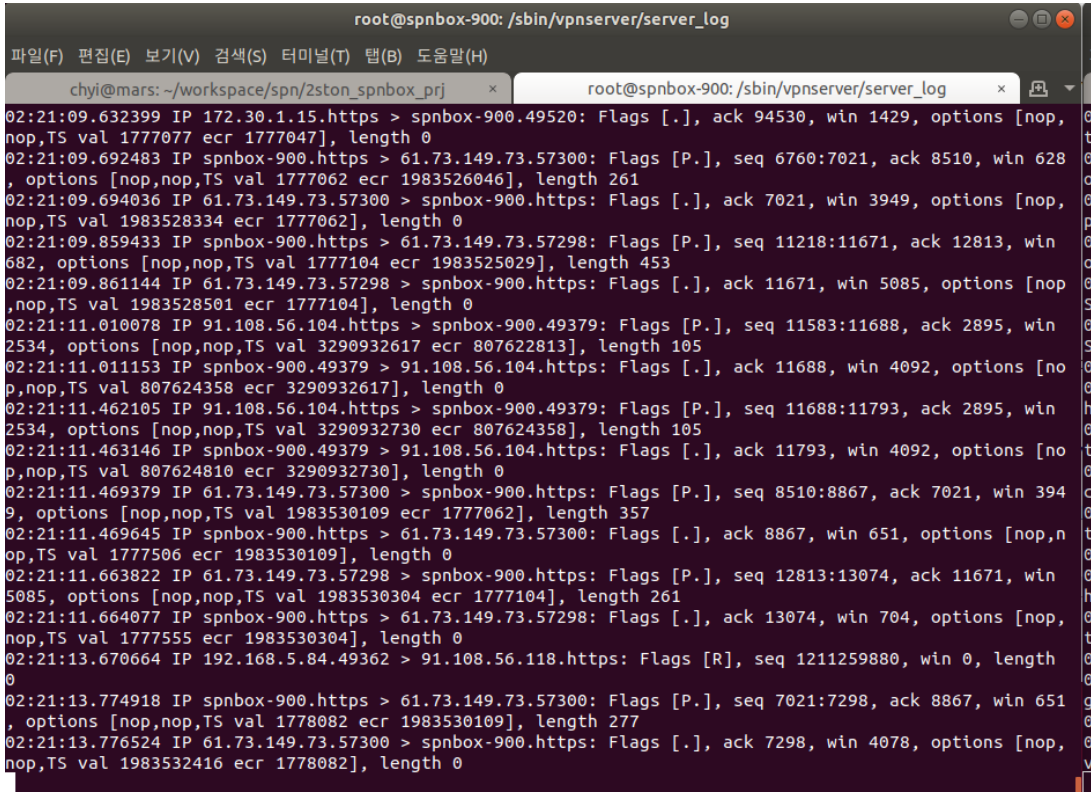
SPN Gateway1(Cluster Controller)



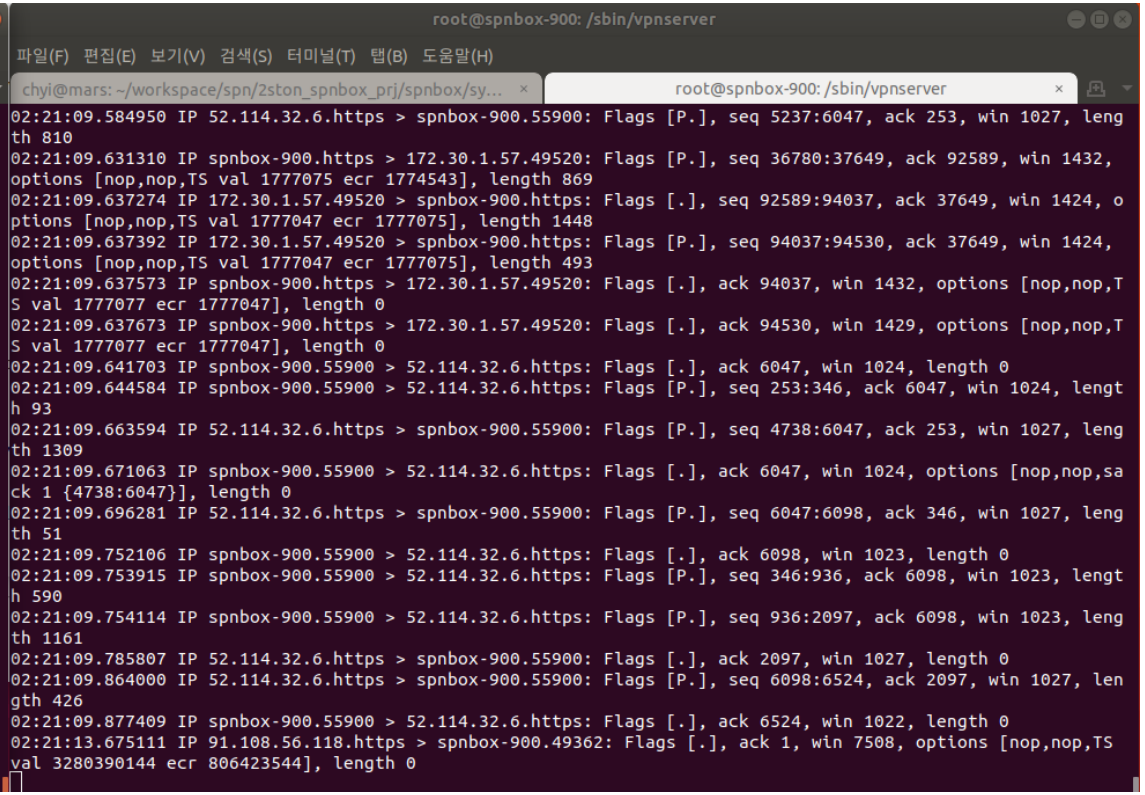
Cluster Controller에 붙은 상태에서 CPU 사용량 측정. 반대의 경우 역시 제대로 출력됨(단, 화면 캡쳐 안함).

7. SPN Gateway Cluster(6) – VPN 연결 시험(4)

SPN Gateway2(Cluster Member)



SPN Gateway1(Cluster Controller)



tcpdump –i wan port 443

tcpdump –i wan port 443

Cluster Member(좌측)에 붙거나 Controller(우측)에 붙을 경우, WAN 구간의 HTTPS 패킷이 확실히 구분되어 출력된다.

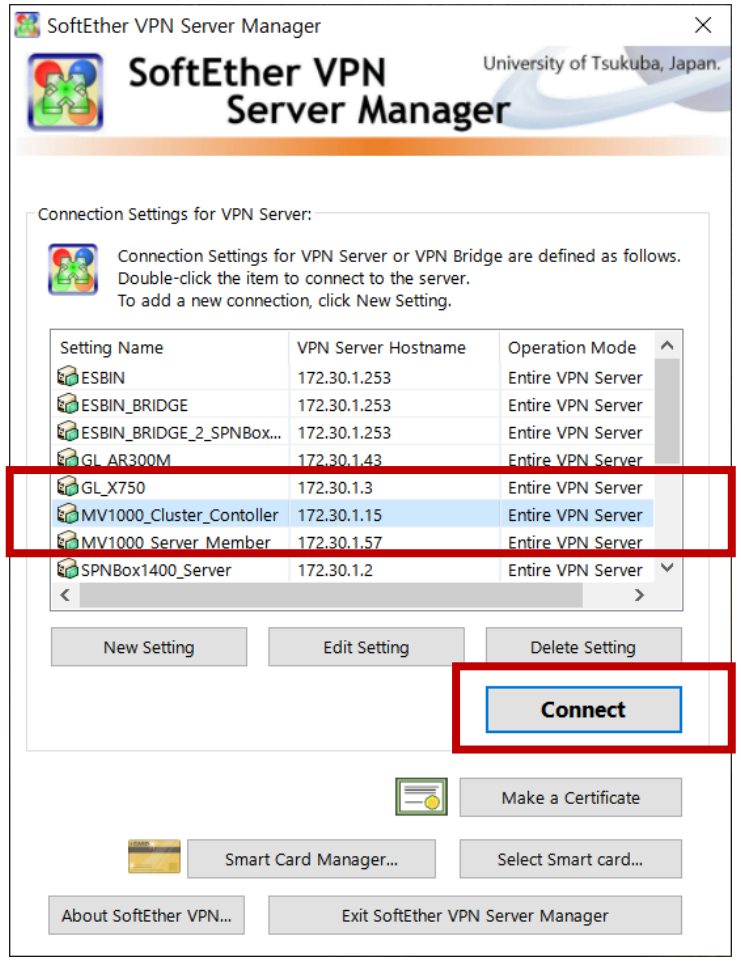
8. 인터넷 접속 차단
: Setup Guide

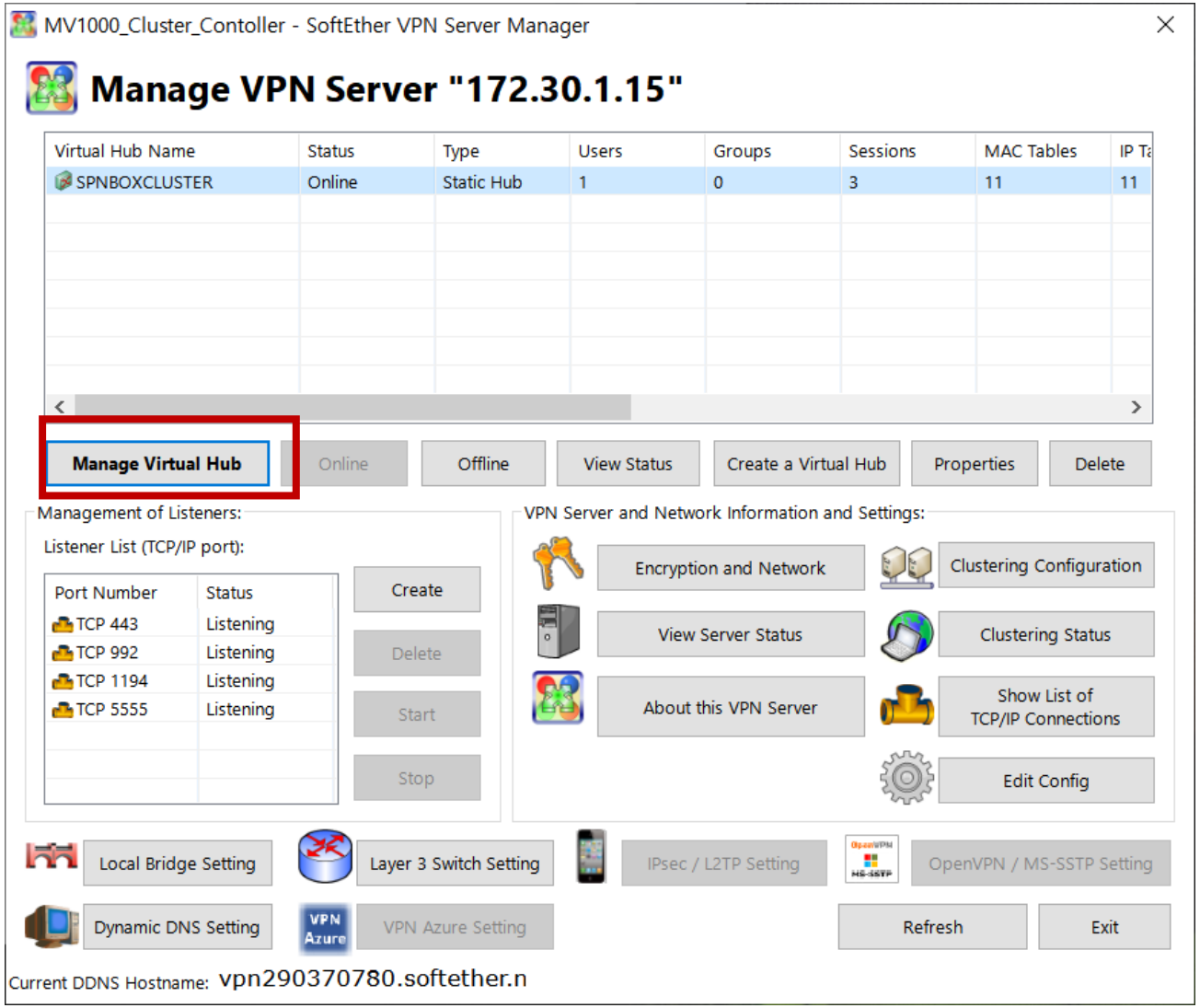
재택근무자가 사무실 망으로는 진입 가능하나, 인터넷을 차단하고 싶다면 …

8. 인터넷 접속 차단(1)

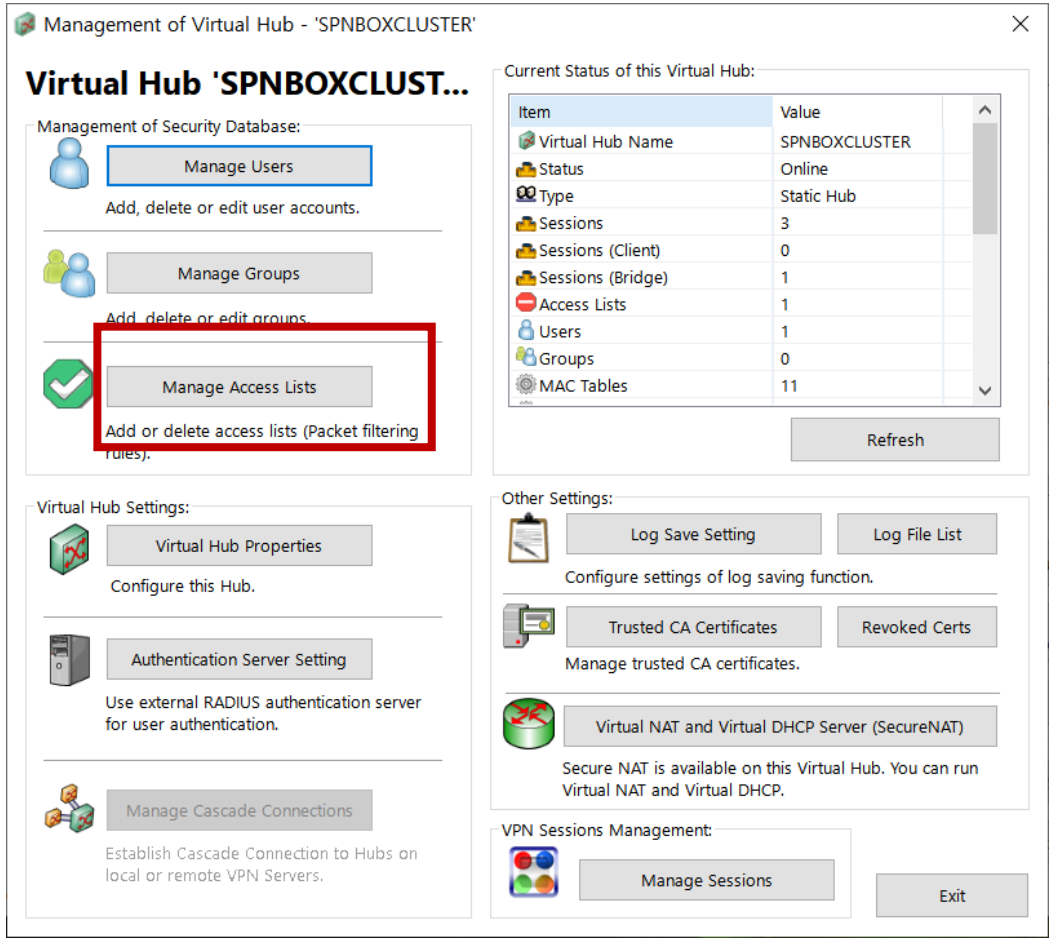
- **<요구 사항>**
  - 재택 근무자가 본사망에 접근하는 것은 허용하고, SPN Gateway를 통해 인터넷으로 나가는 것은 차단하고 싶다.
- **<해법>**
  - L2 SPN의 경우, 재택근무자(Home)의 IP 주소 대역이 본사 사무실의 그것과 동일해 지는 관계로 static IP 주소를 사용하는 경우가 아니라면 사실상 차단하기가 쉽지 않다. ➔ IP 주소를 가지고 차단하는 것은 가능함.
  - 따라서, 여기에서는 SPN Bridge의 WAN port MAC 주소 혹은 Windows Client의 Virtual Adapter의 MAC 주소를 기반으로 인터넷 트래픽을 차단하는 설정을 소개하도록 하겠다.

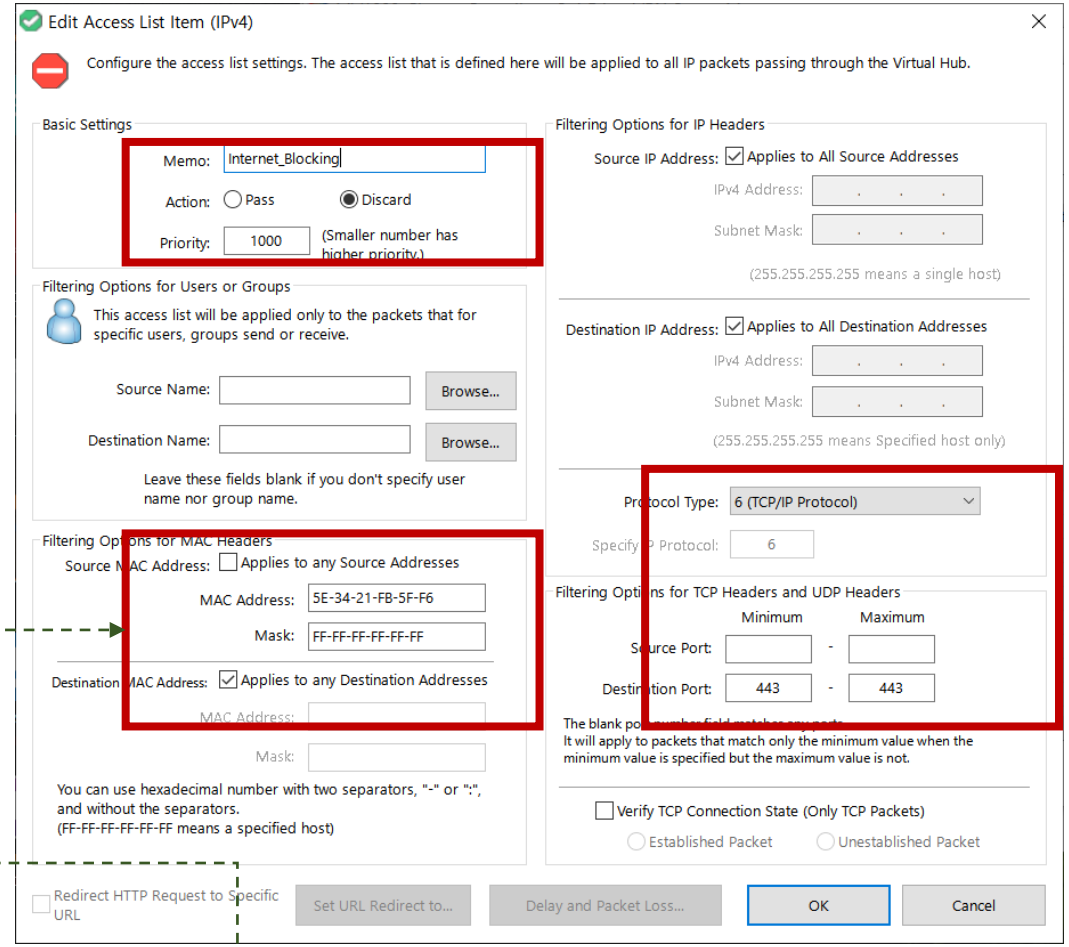
8. 인터넷 접속 차단(2)


SoftEther VPN Server Manager
SoftEther VPN Server Manager
University of Tsukuba, Japan.
Connection Settings for VPN Server:
Connection Settings for VPN Server or VPN Bridge are defined as follows.
Double-click the item to connect to the server.
To add a new connection, click New Setting.
Setting Name
VPN Server Hostname
Operation Mode
ESBIN
172.30.1.253
Entire VPN Server
ESBIN_BRIDGE
172.30.1.253
Entire VPN Server
ESBIN_BRIDGE_2_SPNBox...
172.30.1.253
Entire VPN Server
GL_AR300M
172.30.1.43
Entire VPN Server
GL_X750
172.30.1.3
Entire VPN Server
MV1000_Cluster_Contoller
172.30.1.15
Entire VPN Server
MV1000_Server_Member
172.30.1.57
Entire VPN Server
SPNBox1400_Server
172.30.1.2
Entire VPN Server
New Setting
Edit Setting
Delete Setting
Connect
Make a Certificate
Smart Card Manager...
Select Smart card...
About SoftEther VPN...
Exit SoftEther VPN Server Manager


MV1000_Cluster_Contoller - SoftEther VPN Server Manager
Manage VPN Server "172.30.1.15"
Virtual Hub Name
Status
Type
Users
Groups
Sessions
MAC Tables
IP Ta
SPNBOXCLUSTER
Online
Static Hub
1
0
3
11
11
Manage Virtual Hub
Online
Offline
View Status
Create a Virtual Hub
Properties
Delete
Management of Listeners:
Listener List (TCP/IP port):
Port Number
Status
TCP 443
Listening
TCP 992
Listening
TCP 1194
Listening
TCP 5555
Listening
Create
Delete
Start
Stop
VPN Server and Network Information and Settings:
Encryption and Network
Clustering Configuration
View Server Status
Clustering Status
About this VPN Server
Show List of TCP/IP Connections
Edit Config
Local Bridge Setting
Layer 3 Switch Setting
IPsec / L2TP Setting
OpenVPN / MS-SSTP Setting
Dynamic DNS Setting
VPN Azure Setting
Refresh
Exit
Current DDNS Hostname: vpn290370780.softether.n

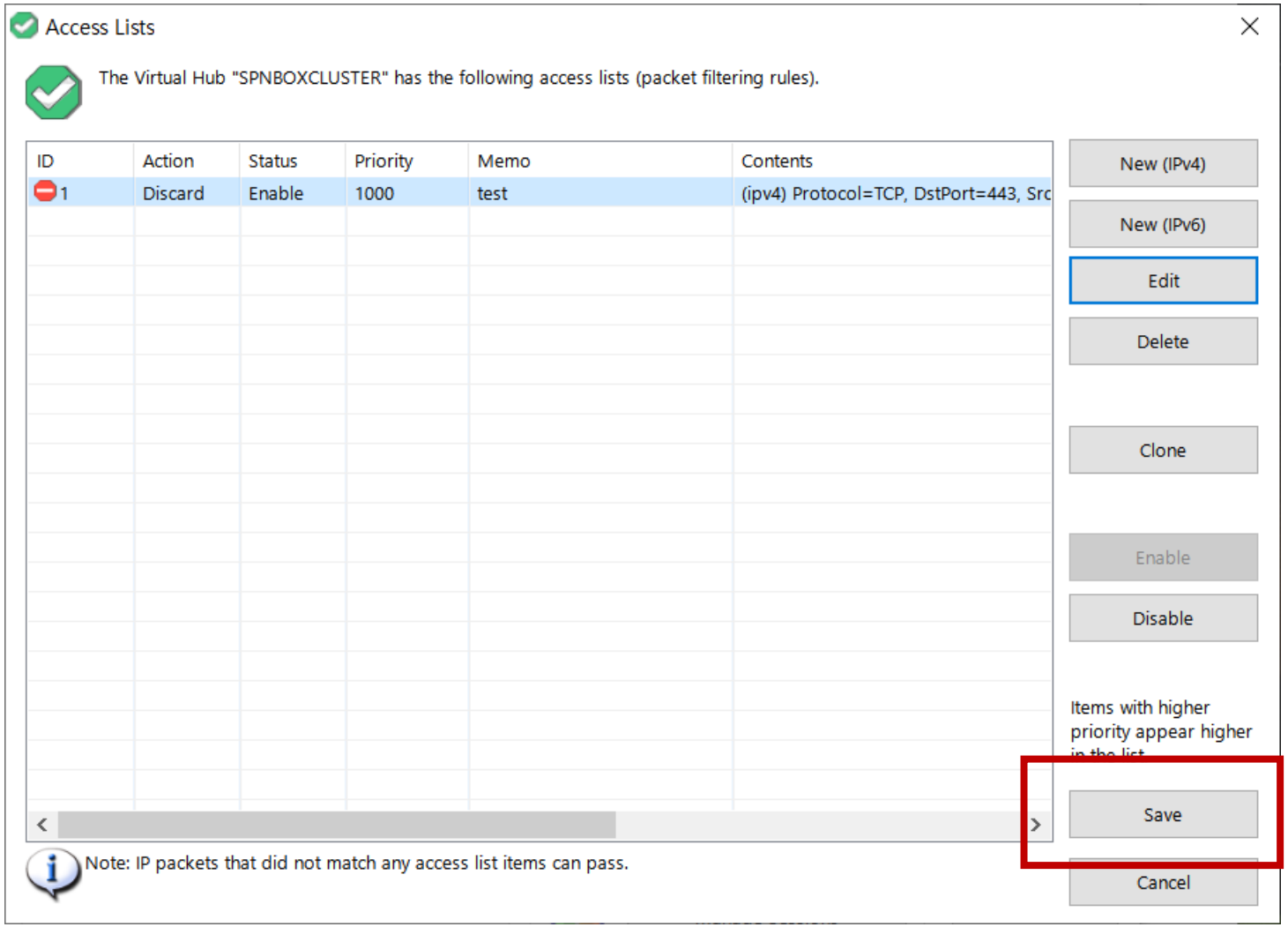
8. 인터넷 접속 차단(3)



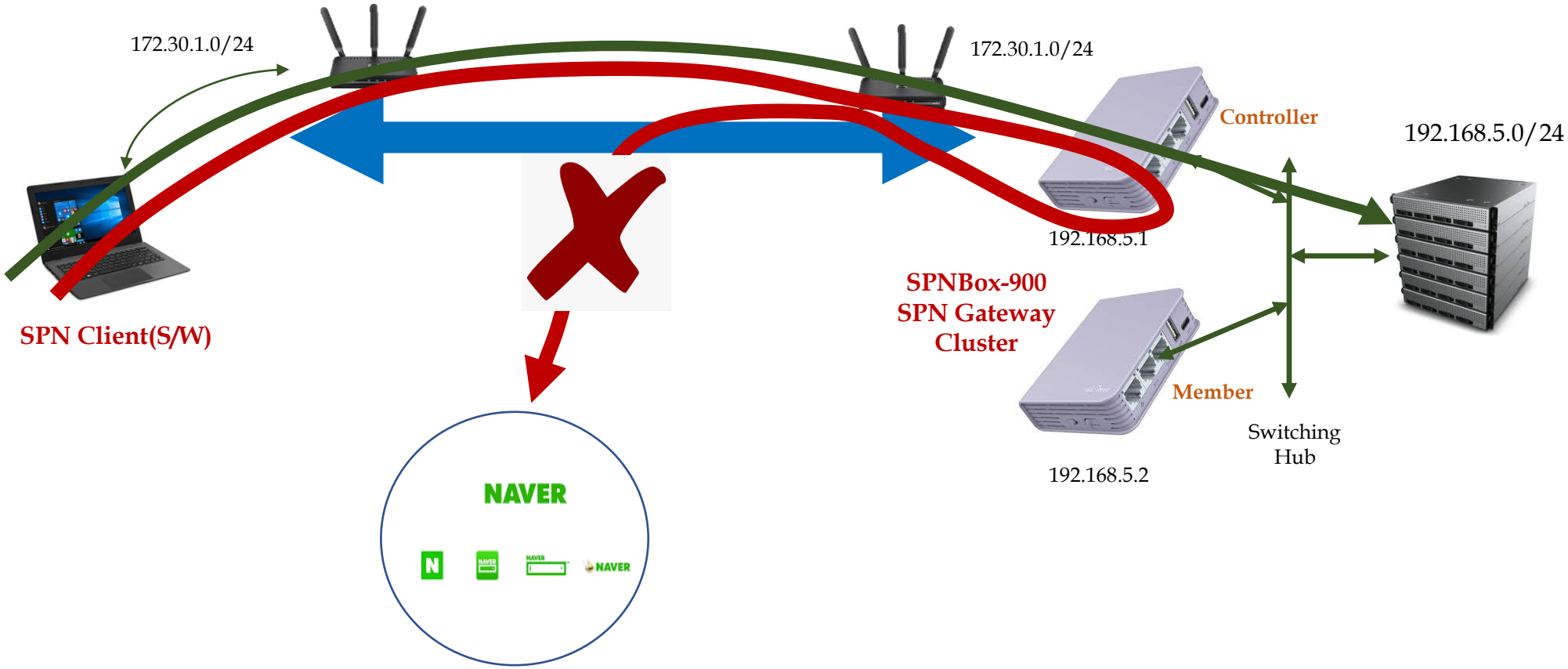


이 MAC 주소는 Windows PC의 MAC 주소임. 혹은 SPN Bridge WAN Port의 MAC 주소임.

8. 인터넷 접속 차단(4)


Access Lists
The Virtual Hub "SPNBOXCLUSTER" has the following access lists (packet filtering rules).
ID
Action
Status
Priority
Memo
Contents
1
Discard
Enable
1000
test
(ipv4) Protocol=TCP, DstPort=443, Src
New (IPv4)
New (IPv6)
Edit
Delete
Clone
Enable
Disable
Items with higher priority appear higher
Save
Cancel
Note: IP packets that did not match any access list items can pass.

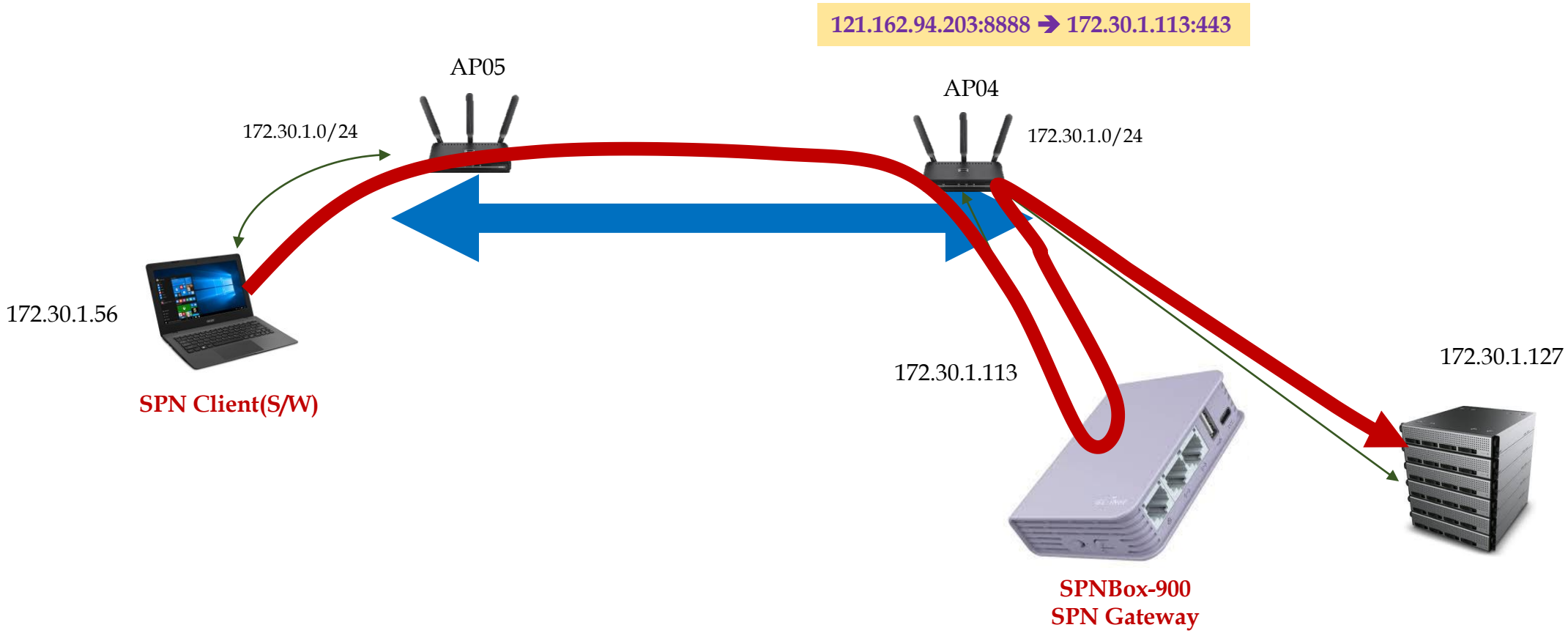
8. 인터넷 접속 차단(5)


172.30.1.0/24
172.30.1.0/24
Controller
192.168.5.0/24
192.168.5.1
SPNBox-900
SPN Gateway
Cluster
SPN Client(S/W)
Member
Switching
Hub
192.168.5.2
NAVER

9. Standalone Server
: Setup Guide

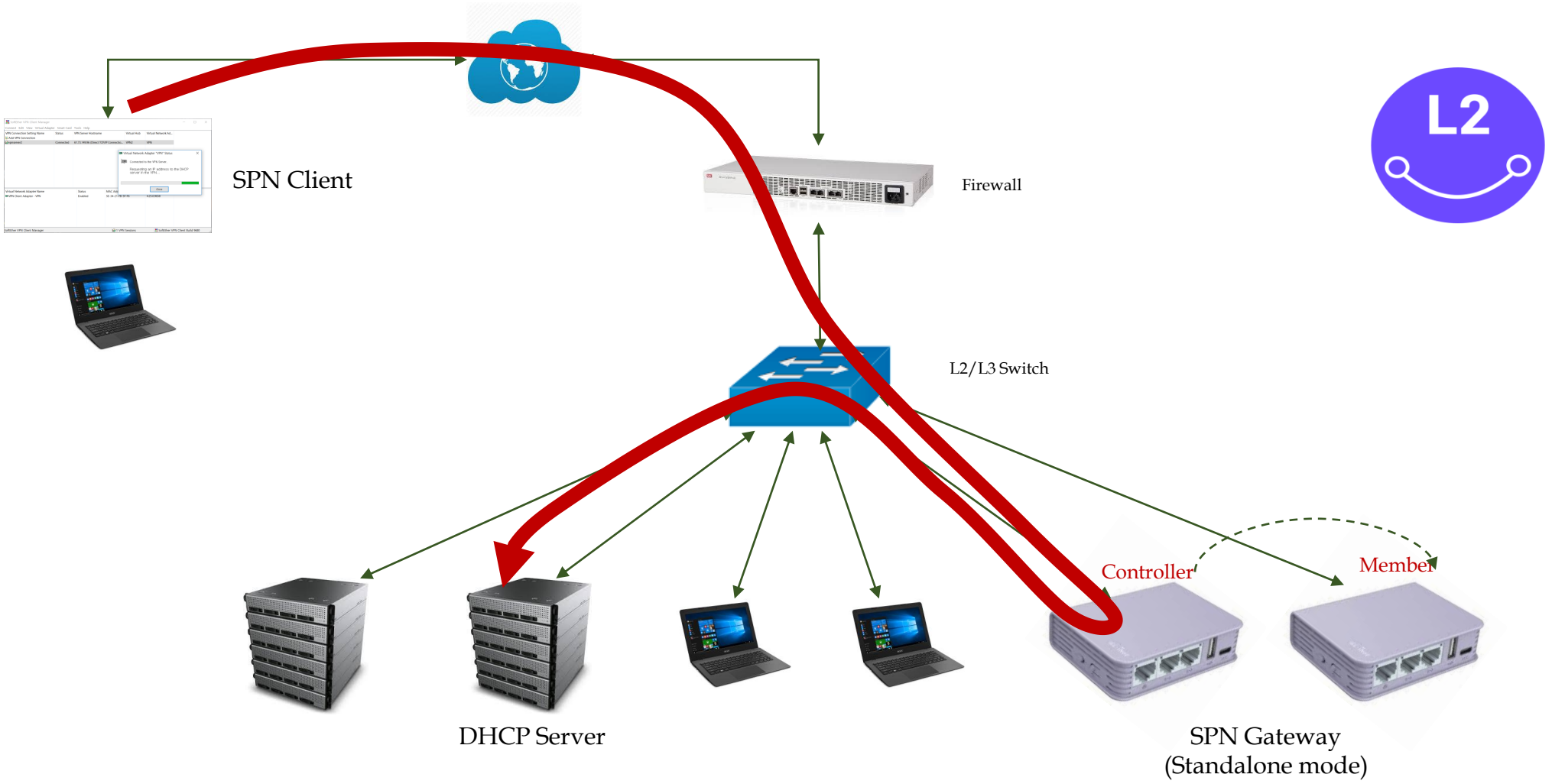
네트워크 관리 담당자가 네트워크 구성 변경에 난색을 표한다면 ....

9. Standalone Server(1) – Testbed(1)



Gateway mode가 아니라 WAN Port만 이용하여 Server mode로 동작시킬 수 있습니다.

9. Standalone Server(1) – Testbed(2)

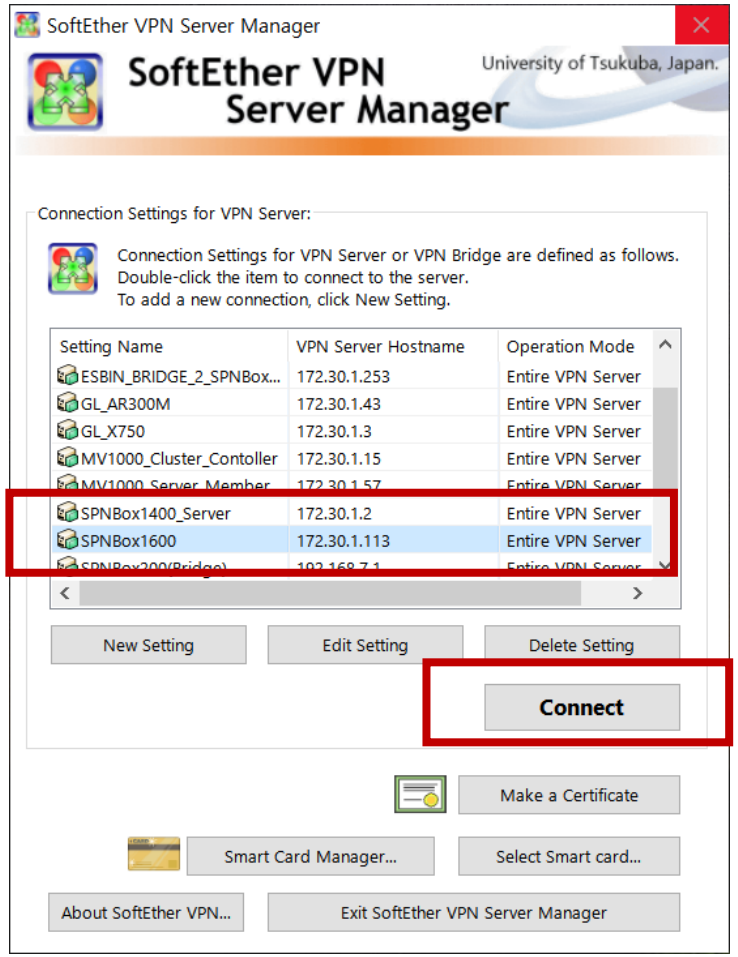


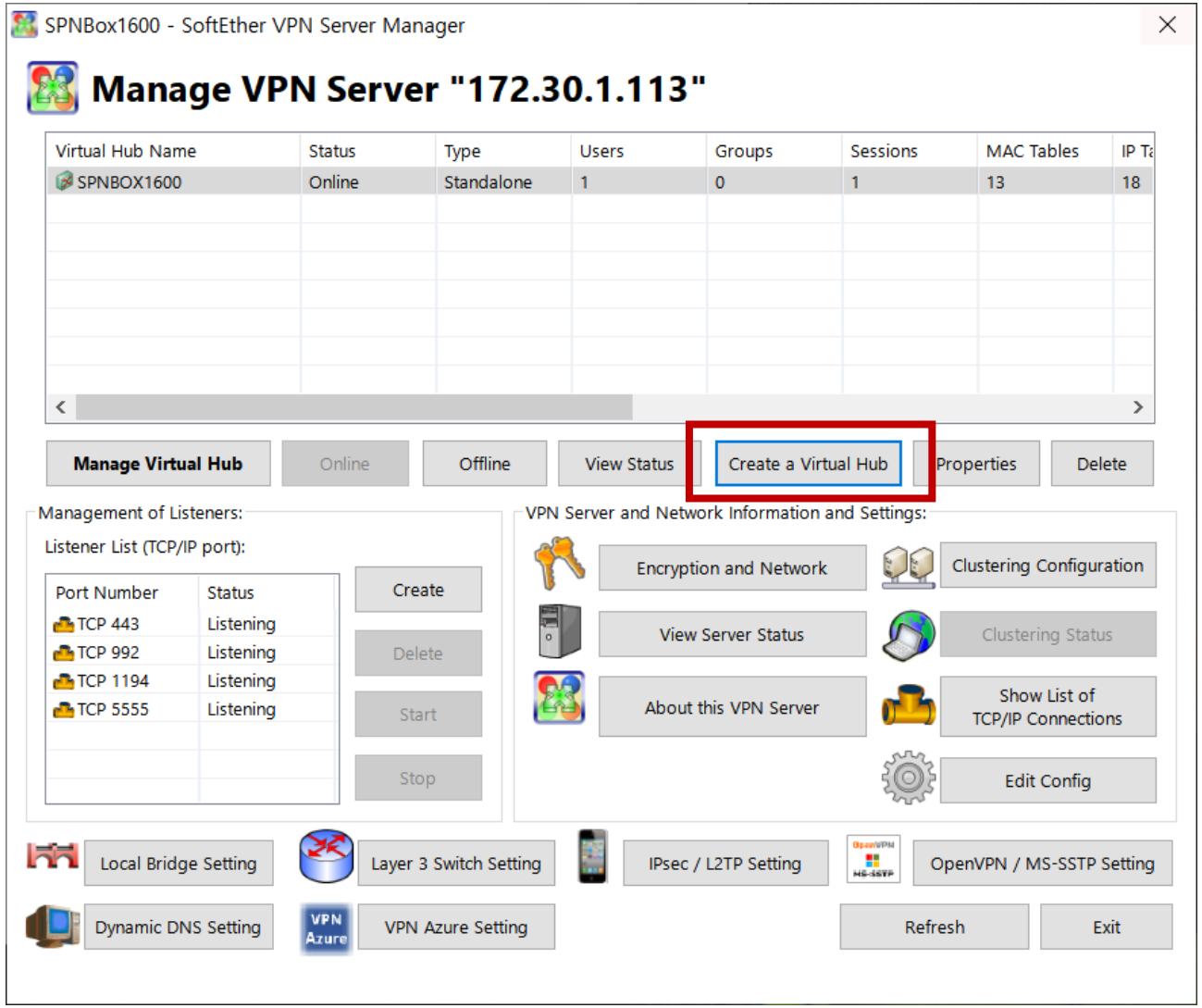
WAN Port만 사용하여 사내망에 연결

9. Standalone Server(2) – SPN Gateway 설정(1)

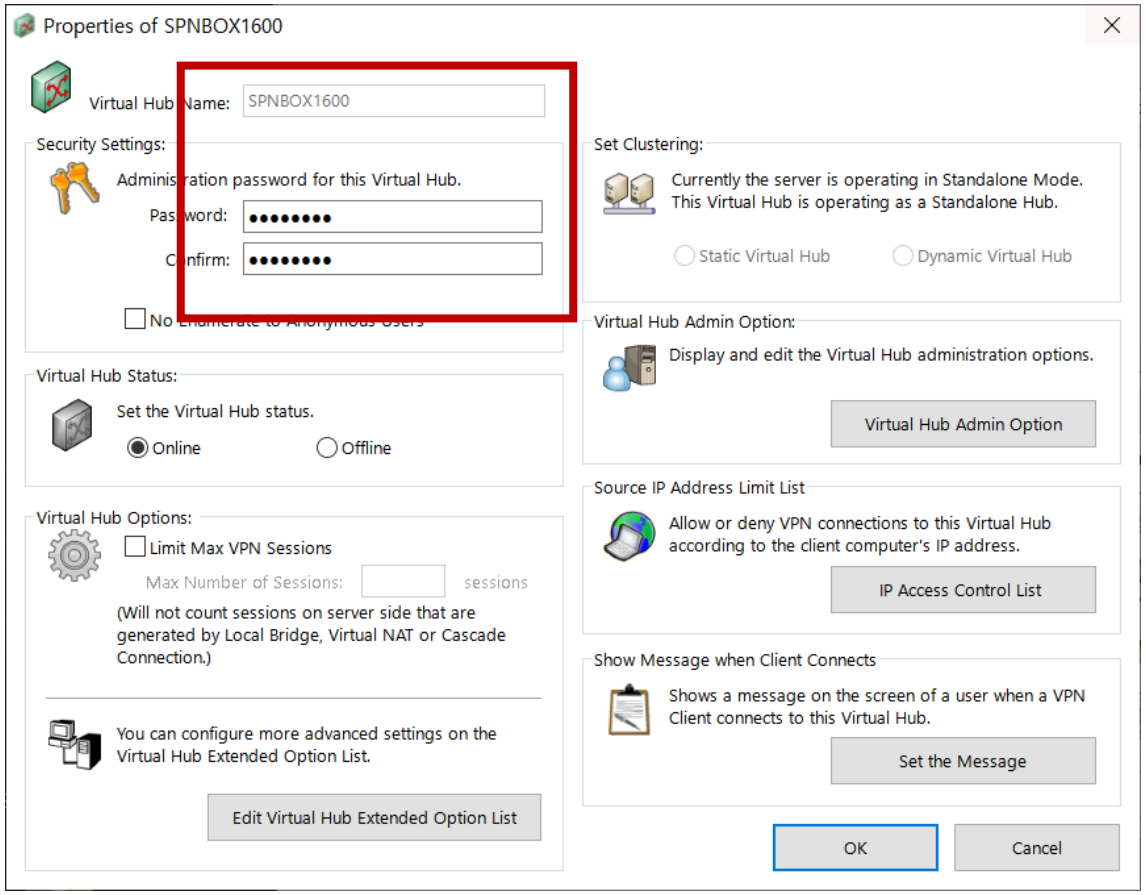
- **<Standalone Server 설정 요약>**
  - 1) SPN Gateway의 LAN port는 더 이상 사용하지 않으며, WAN port만을 사용하여 사무실 내부 망에 연결한다.
  - 2) 다른 부분(Virtual Hub 설정 관련)은 모두 동일하며, Local Bridge 설정 부분만 다르다.
  - 3) 즉, Gateway mode의 경우에는 tap_vpn interface를 생성하였다면, Standalone mode에서는 Physical WAN interface를 선택한 후, Virtual Hub에 연결해 주면 된다.
  - 4) 따라서, CLI에서 “se localbridge tap_vpn” 명령을 더 이상 실행해 주지 않아도 된다. 실행해 주어도 LAN port가 연결되어 있지 않으므로, 아무런 영향을 주지 않는다.

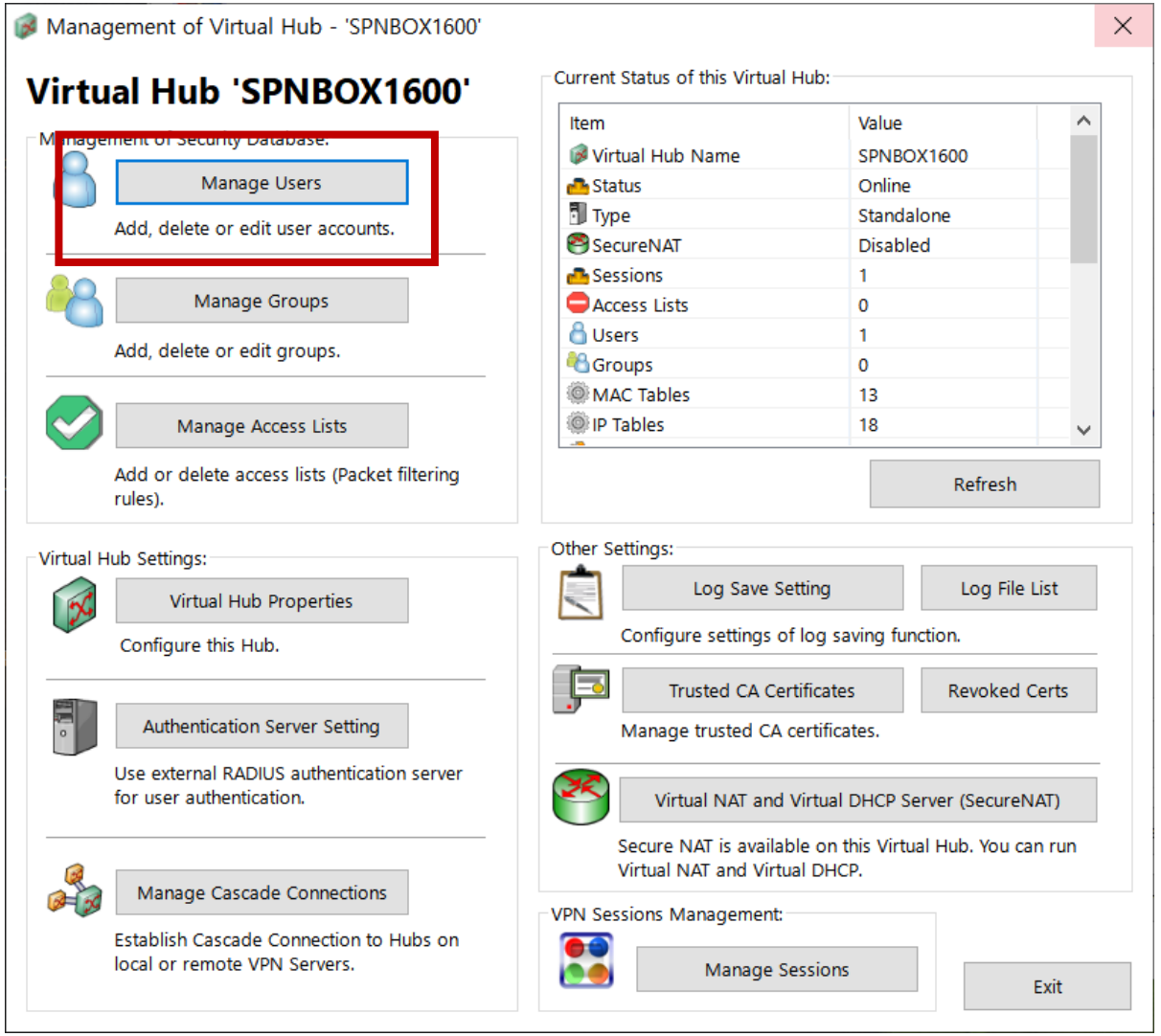
9. Standalone Server(2) – SPN Gateway 설정(2)



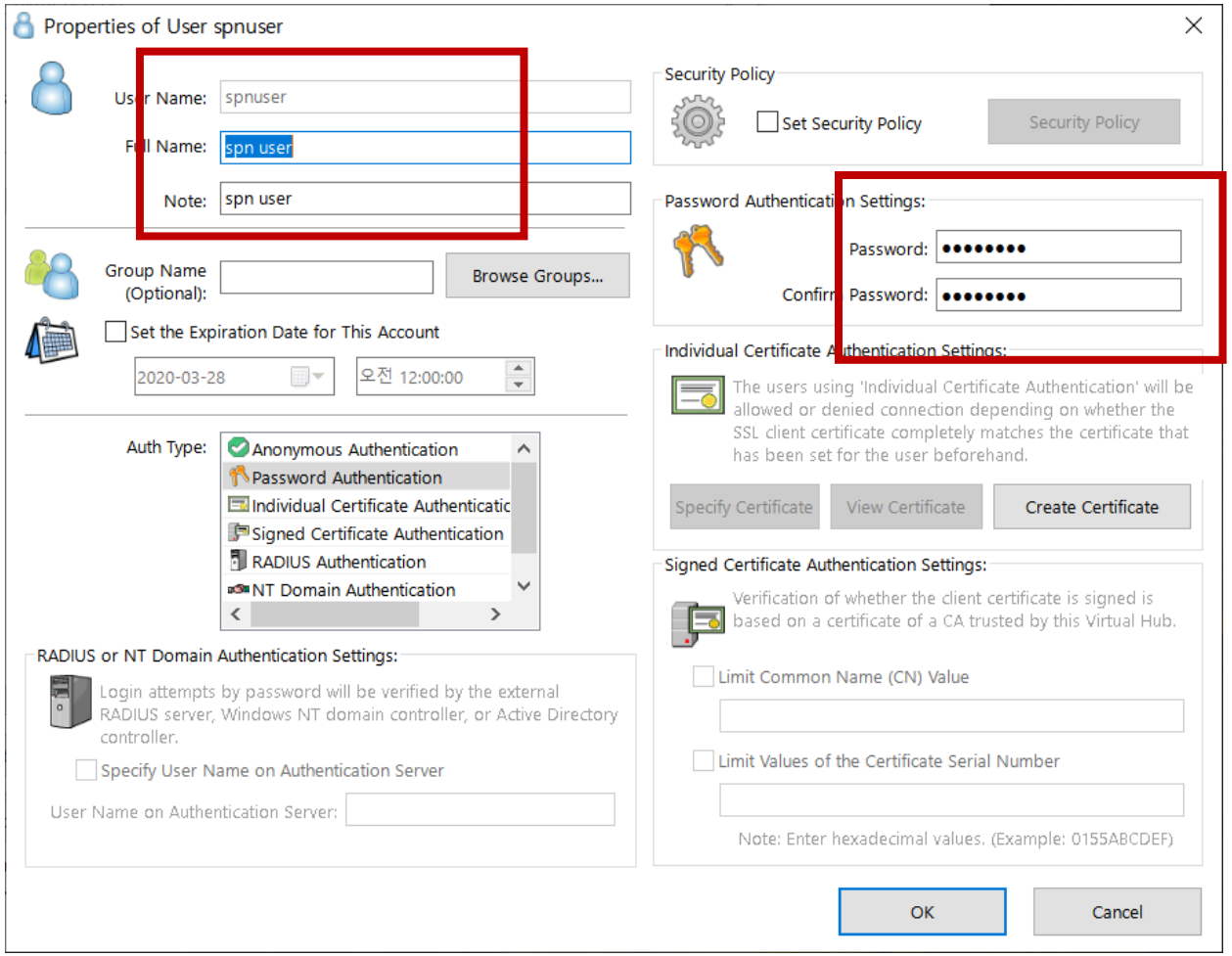


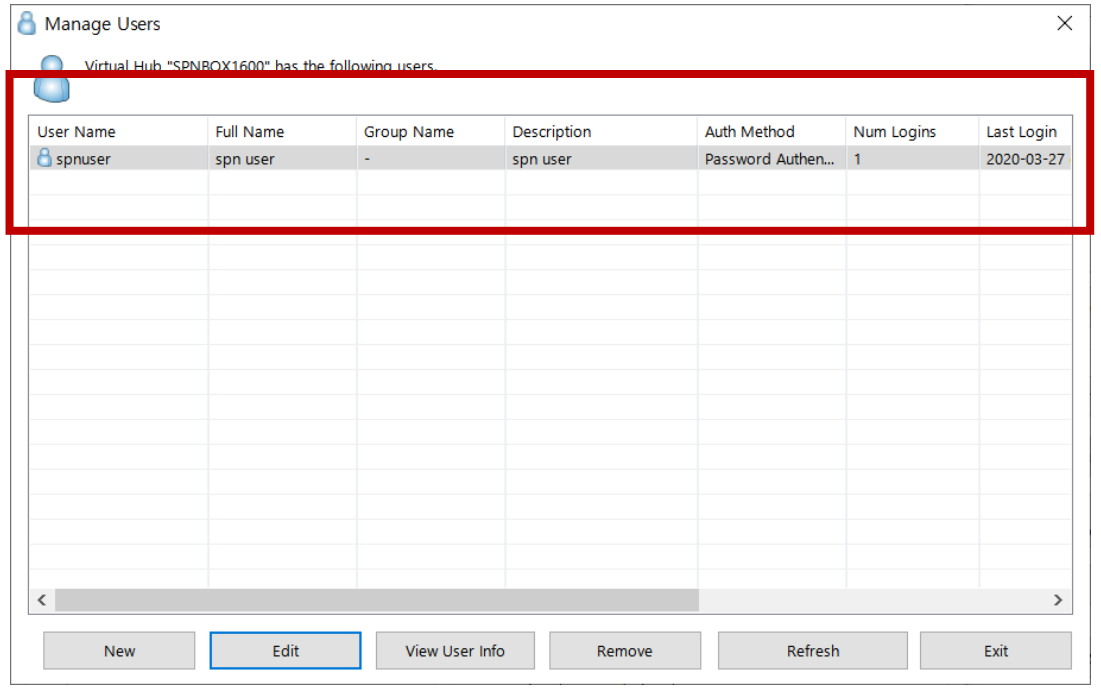
9. Standalone Server(2) – SPN Gateway 설정(3)



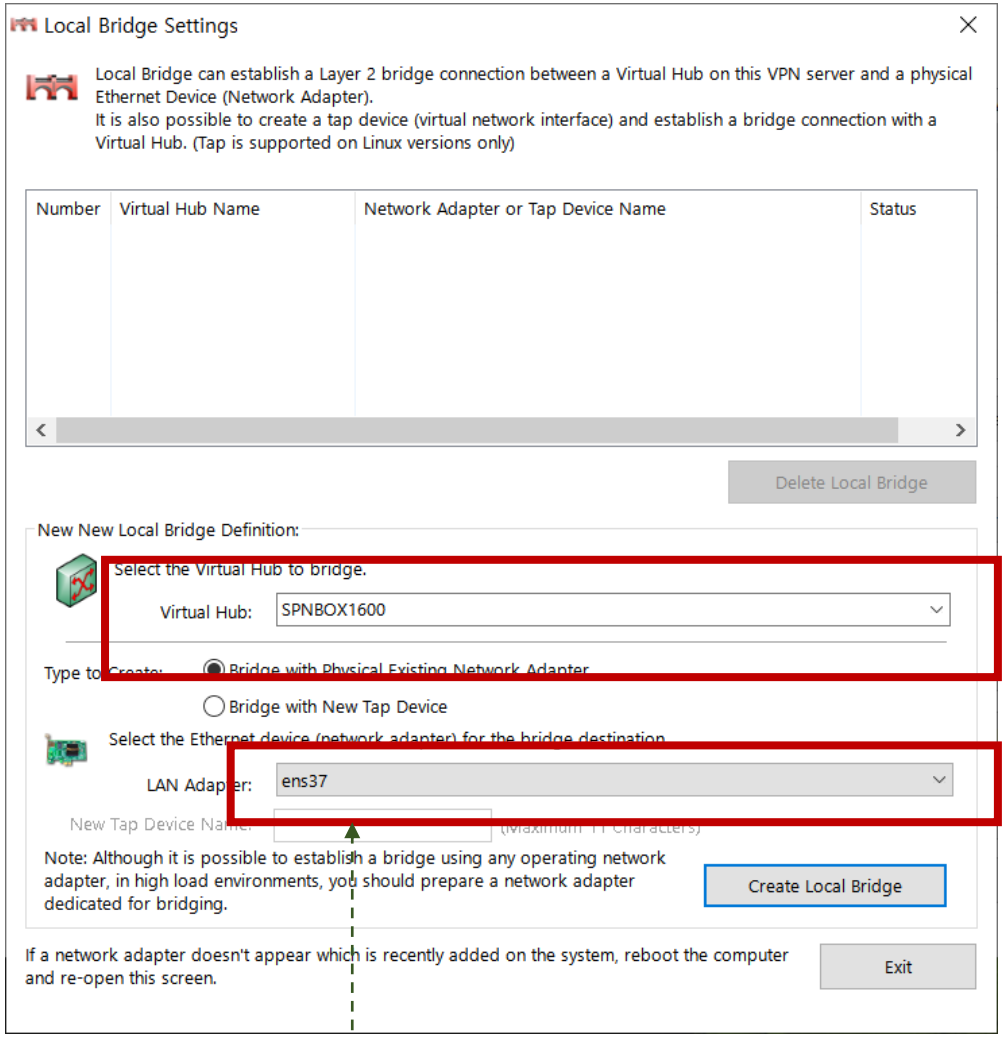


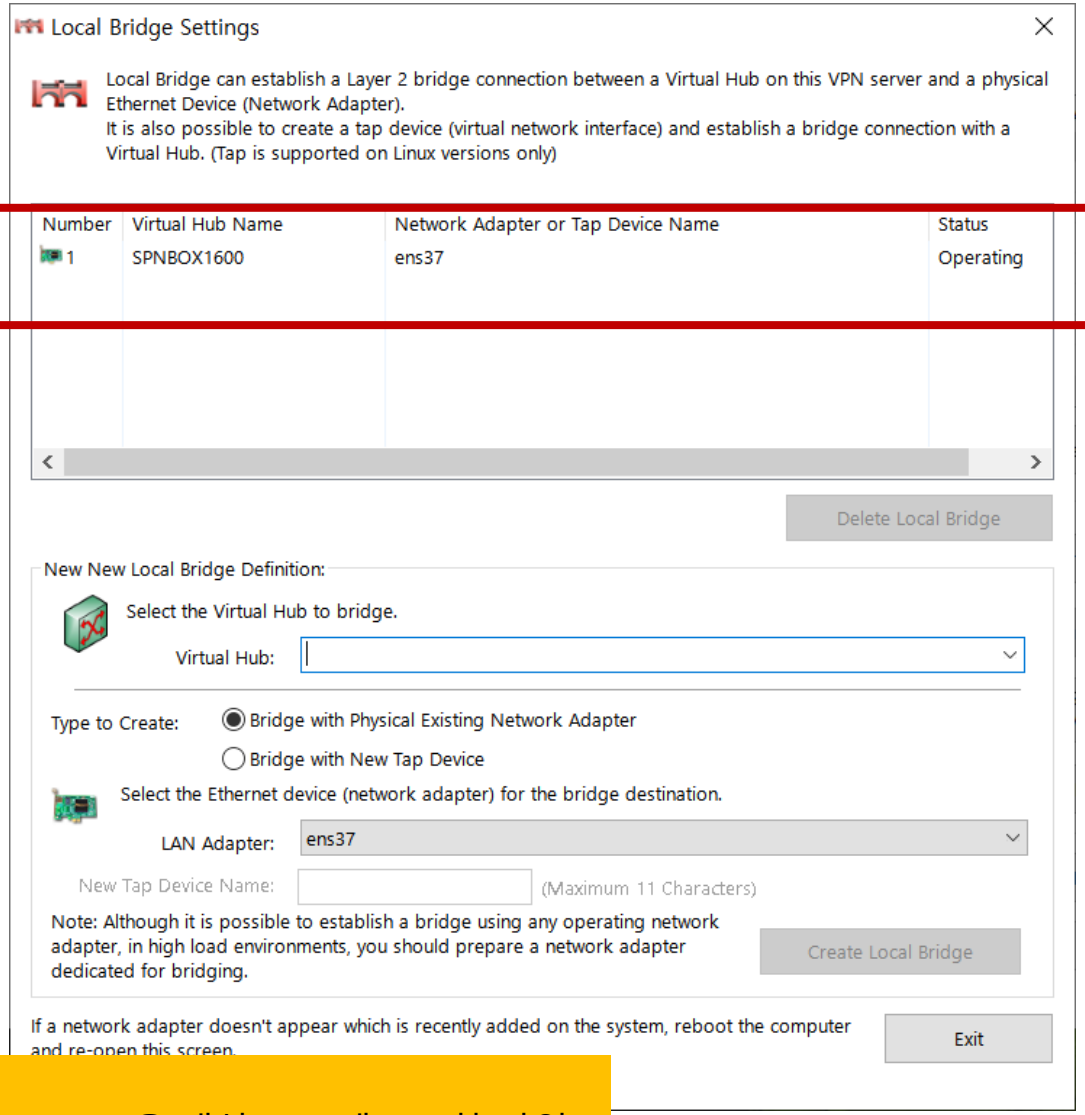
9. Standalone Server(2) – SPN Gateway 설정(4)





9. Standalone Server(2) – SPN Gateway 설정(5)

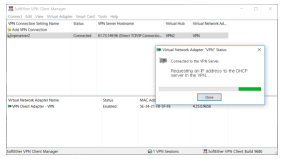




WAN Port 선택

주의: 위의 내용은 SPNBox-900이 아니라, SPNBox-1600을 대상으로 테스트한 것임.

9. Standalone Server(3) – SPN Client 설정(1)



Properties of SPNBox1600

Please configure the VPN Connection Setting for VPN Server.

Setting Name: SPNBox1600

Destination VPN Server:

Specify the host name or IP address, and the port number and the Virtual Hub on the destination VPN Server.

Host Name: 121.162.94.203

Port Number: 8888 Disable NAT-T

Virtual Hub Name: SPNBOX1600

Proxy Server as Relay:

You can connect to a VPN Server via a proxy server.

Import IE Proxy Server Settings

Proxy Type: Direct TCP/IP Connection (No Proxy)

Connect via HTTP Proxy Server

Connect via SOCKS Proxy Server

Proxy Server Setting

Server Certificate Verification Option:

Always Verify Server Certificate

Manage Trusted CA Certificate List

Specify Individual Cert Show Individual Cert

Hide Status and Errors Screens Hide IP Address Screens

Virtual Network Adapter to Use:

VPN Client Adapter - VPN

User Authentication Setting:

Set the user authentication information that is required when connecting to the VPN Server.

Auth Type: Standard Password Authentication

User Name: spnuser

Password: ••••••••

You can change the user's password on the VPN Server.

Change Password

Advanced Setting of Communication:

Reconnects Automatically After Disconnected

Reconnect Count: times

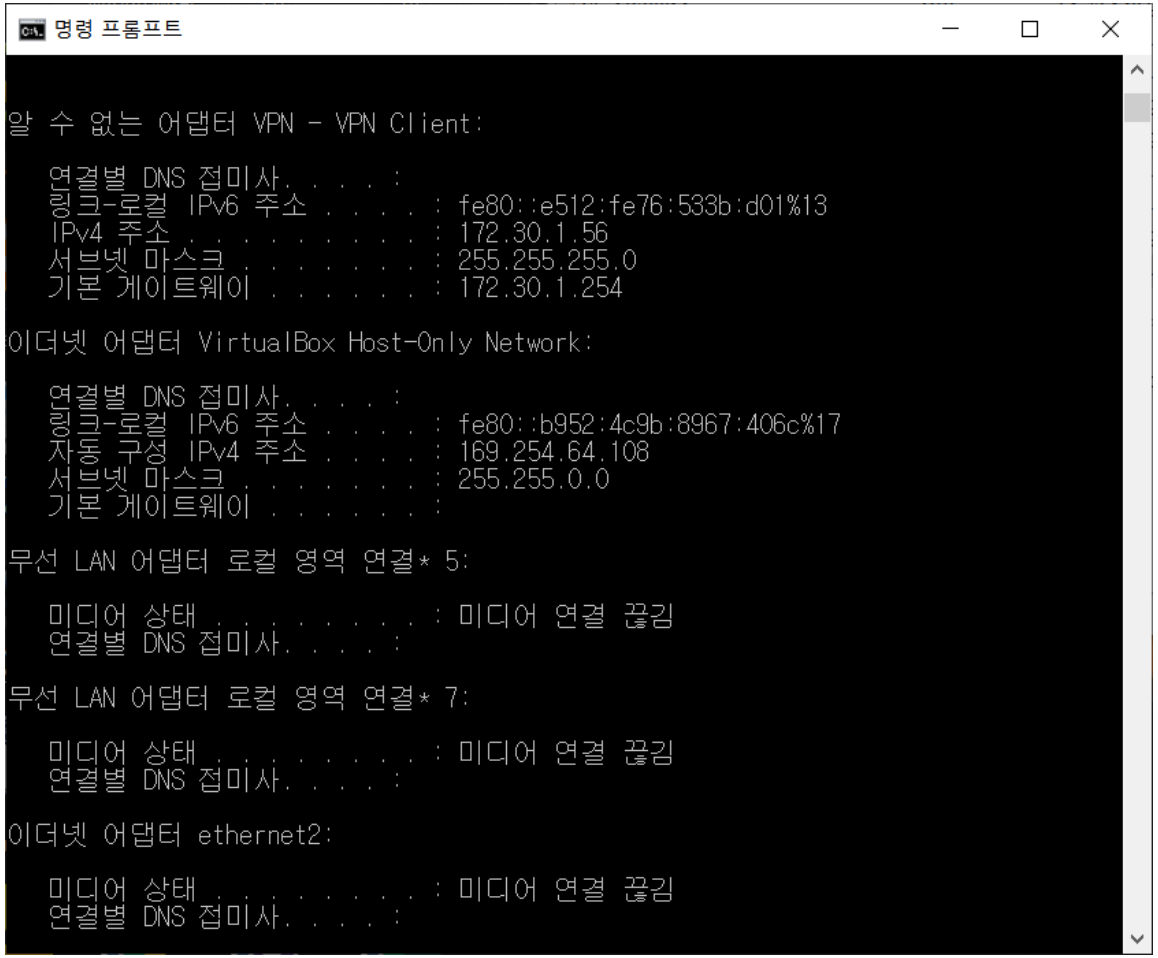
Reconnect Interval: 15 seconds

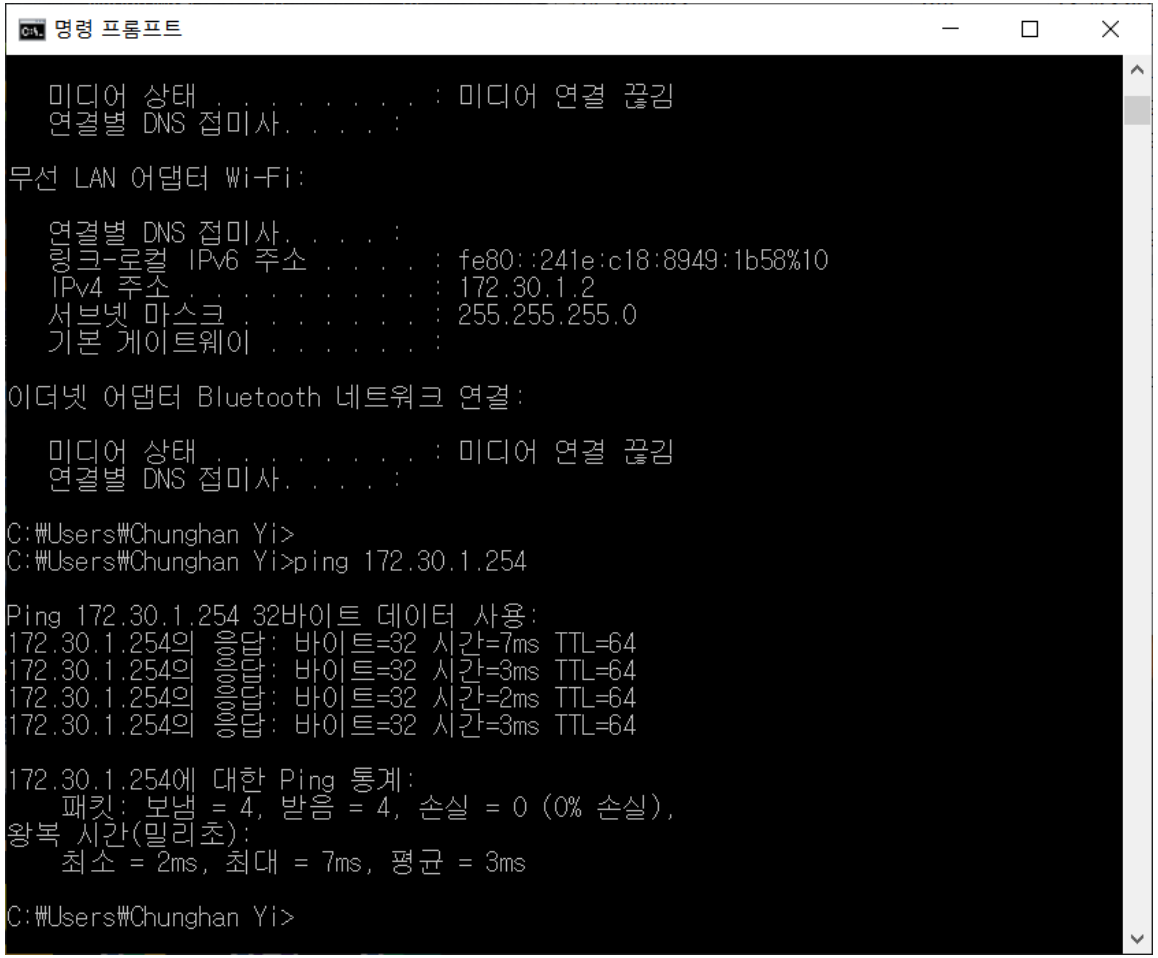
Infinite Reconnects (Keep VPN Always Online)

Use SSL 3.0 (1) Advanced Settings...

OK Cancel

9. Standalone Server(3) – SPN Client 설정(2)





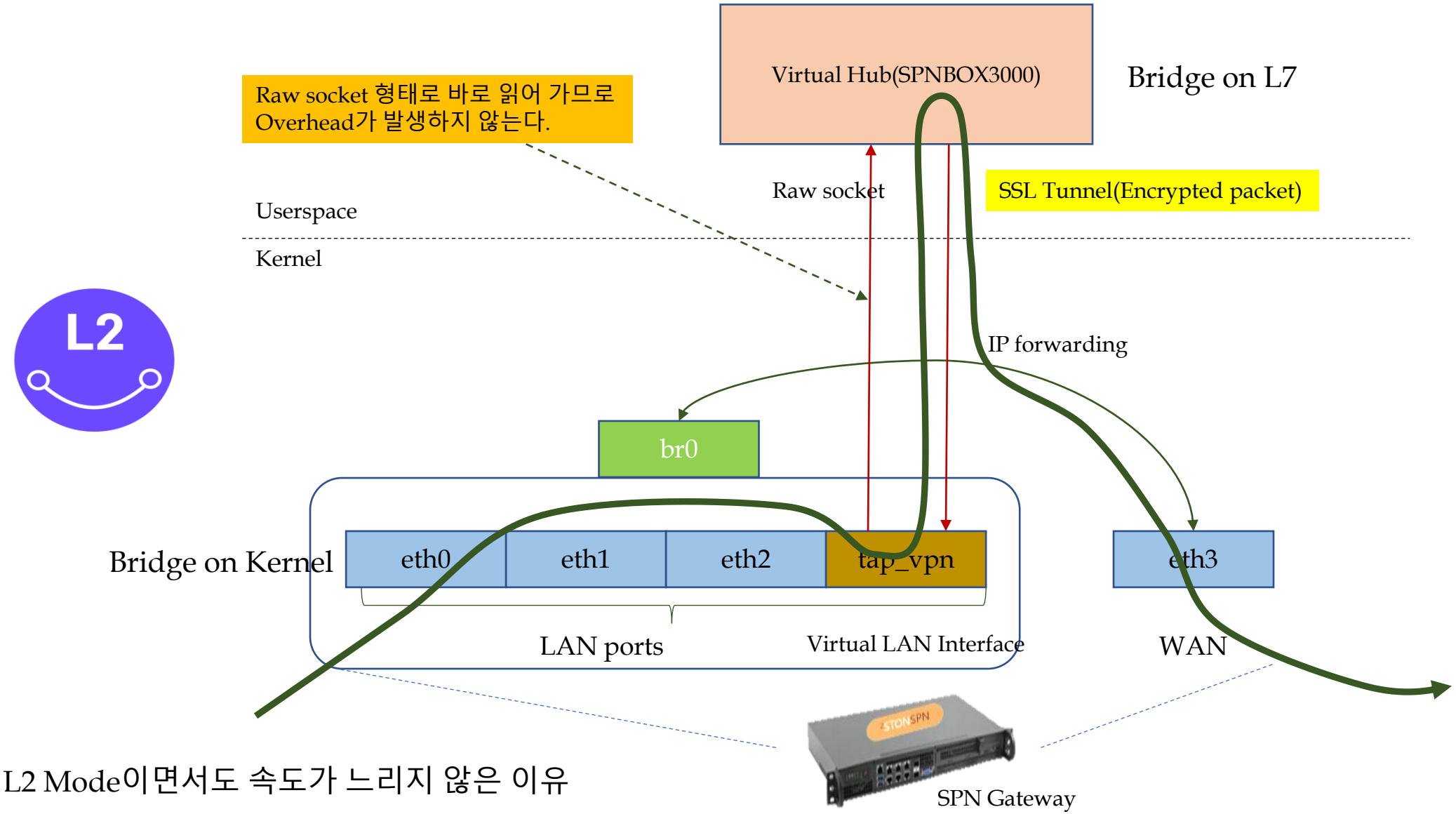
▪ VPN 연결 결과, Windows PC의 IP 주소가 AP04 망의 172.30.1.56를 할당 받았으며, 같은 망 내의 다른 IP 주소와도 통신에 무리가 없음을 알 수 있다.

9. Standalone Server(3) – SPN Client 설정(3)

- **<인터넷 연결 속도>**
  - 역시 예상했던 대로, 인터넷 접속시 약간의 delay가 있는 것으로 보인다.

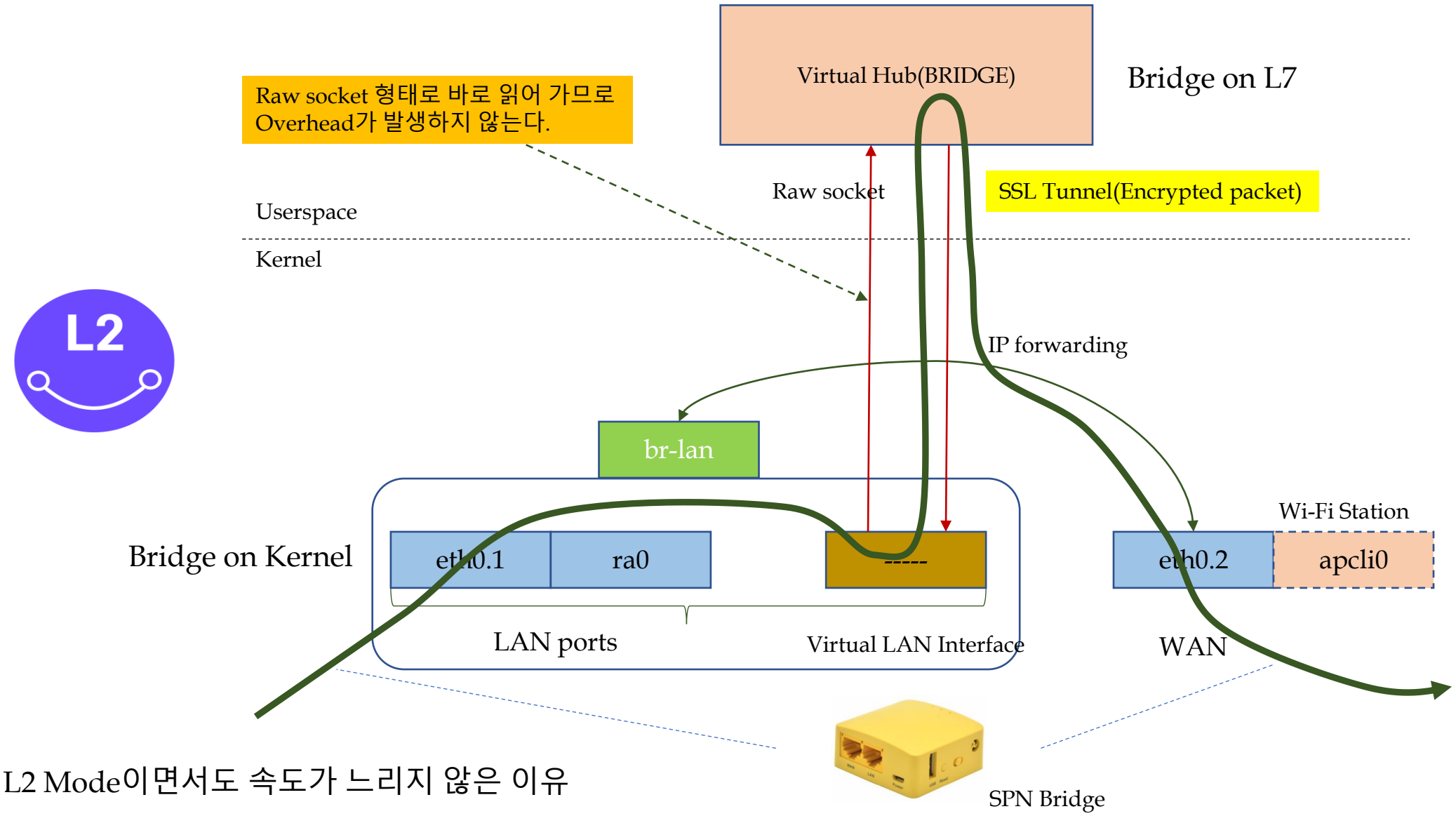
10. L2 SPN Internal Architecture

10. L2 SPN Internal Architecture(1)



L2 Mode이면서도 속도가 느리지 않은 이유

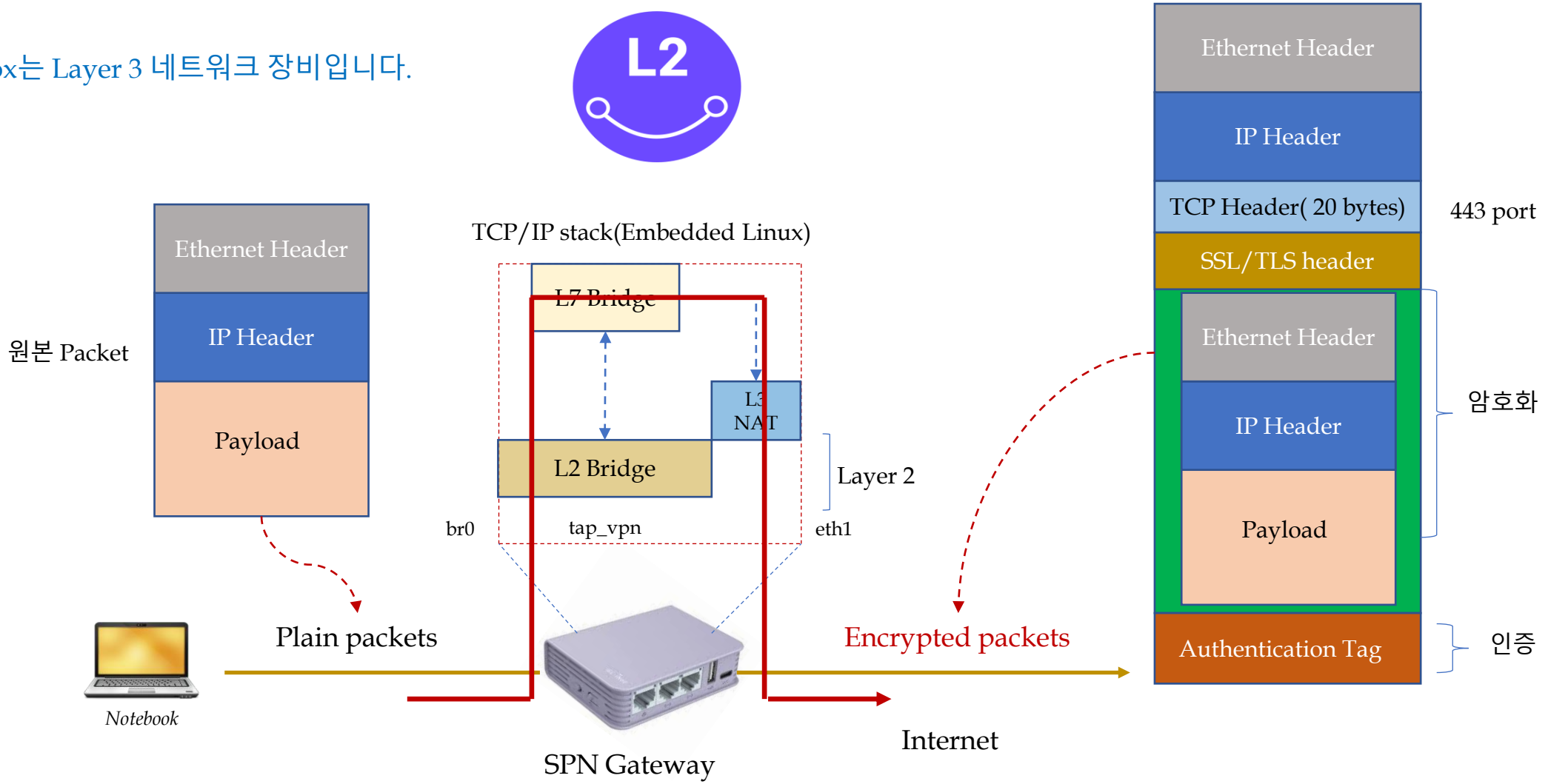
10. L2 SPN Internal Architecture(2)



L2 Mode이면서도 속도가 느리지 않은 이유

10. L2 SPN Internal Architecture(3)

SPNBox는 Layer 3 네트워크 장비입니다.



10. L2 SPN Internal Architecture(4)

L2 network

SPNBox-200

Ethernet Frame

Ethernet Frame (Original packet)

Ethernet header | IP header | TCP/UDP header | Payload

L2

L2 Tunnel

SPNBox-3000

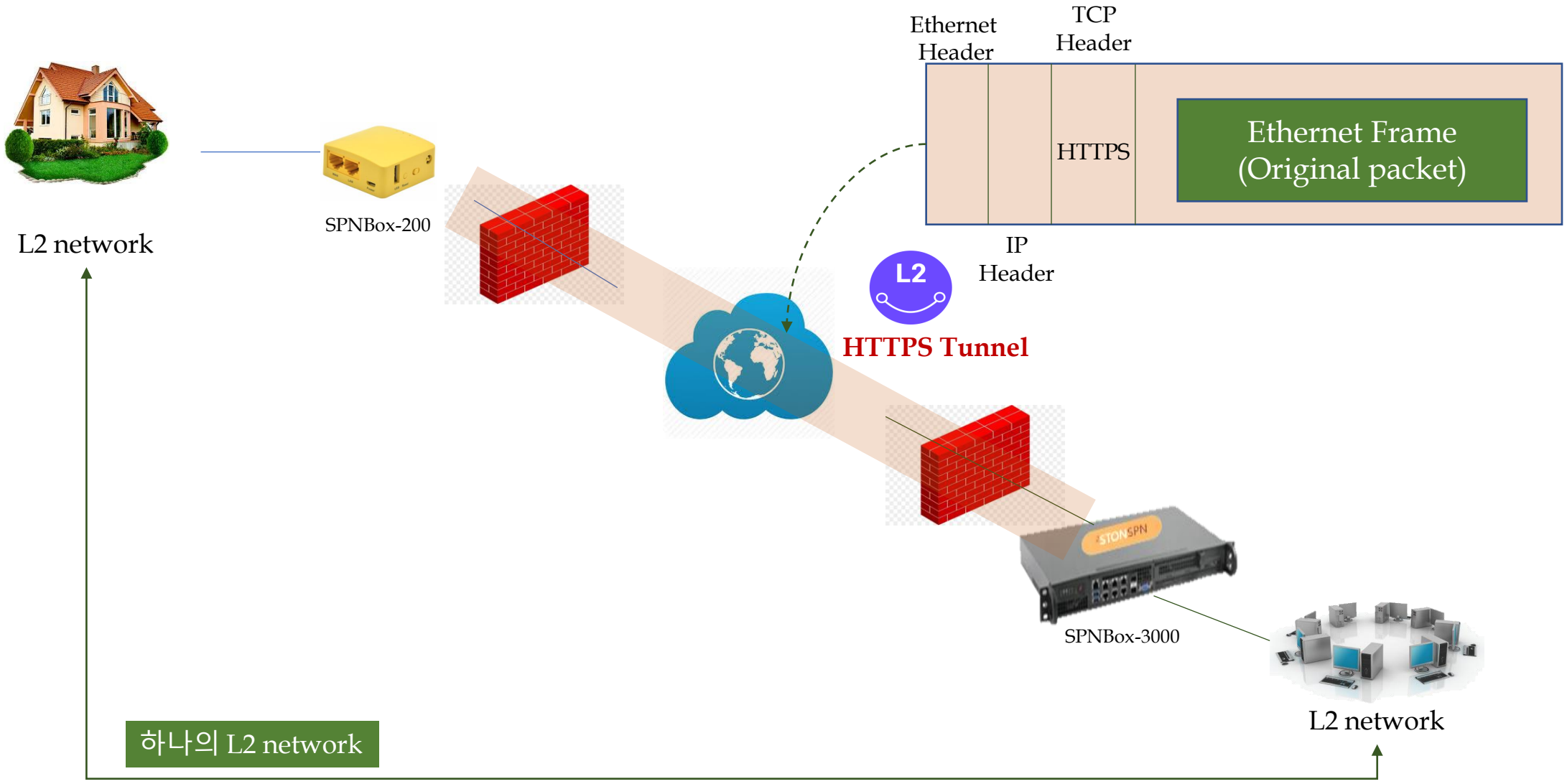
L2 network

- **비 IP 프로토콜에 대해서도 통신 가능**
- **IP multicast/broadcast packet도 전달 가능**

하나의 L2 network

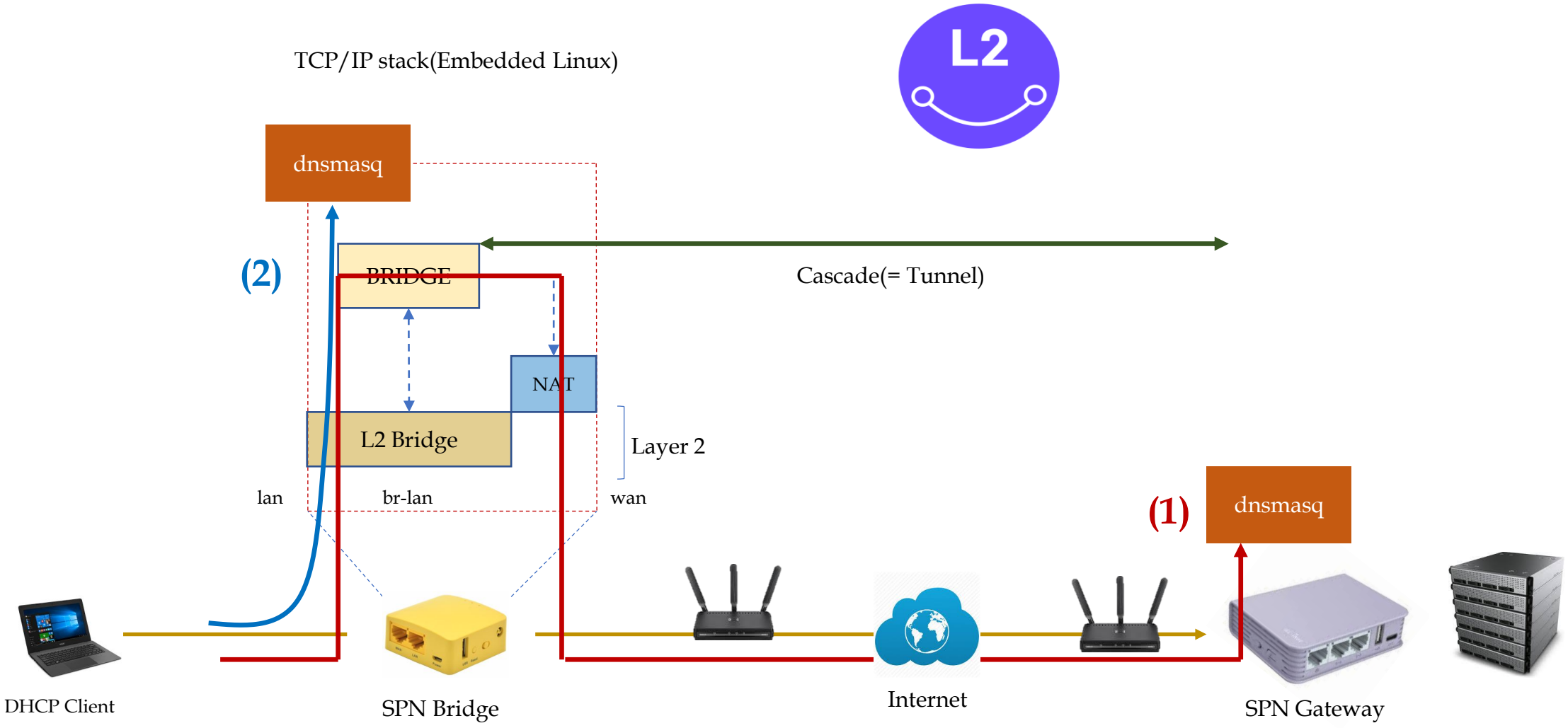
L2 SPN 기능을 사용하면, L2 packet(Windows NETBEUI, DHCP, ARP, Broadcast 등)을 안전하게 실어 나를 수 있습니다.

10. L2 SPN Internal Architecture(5)



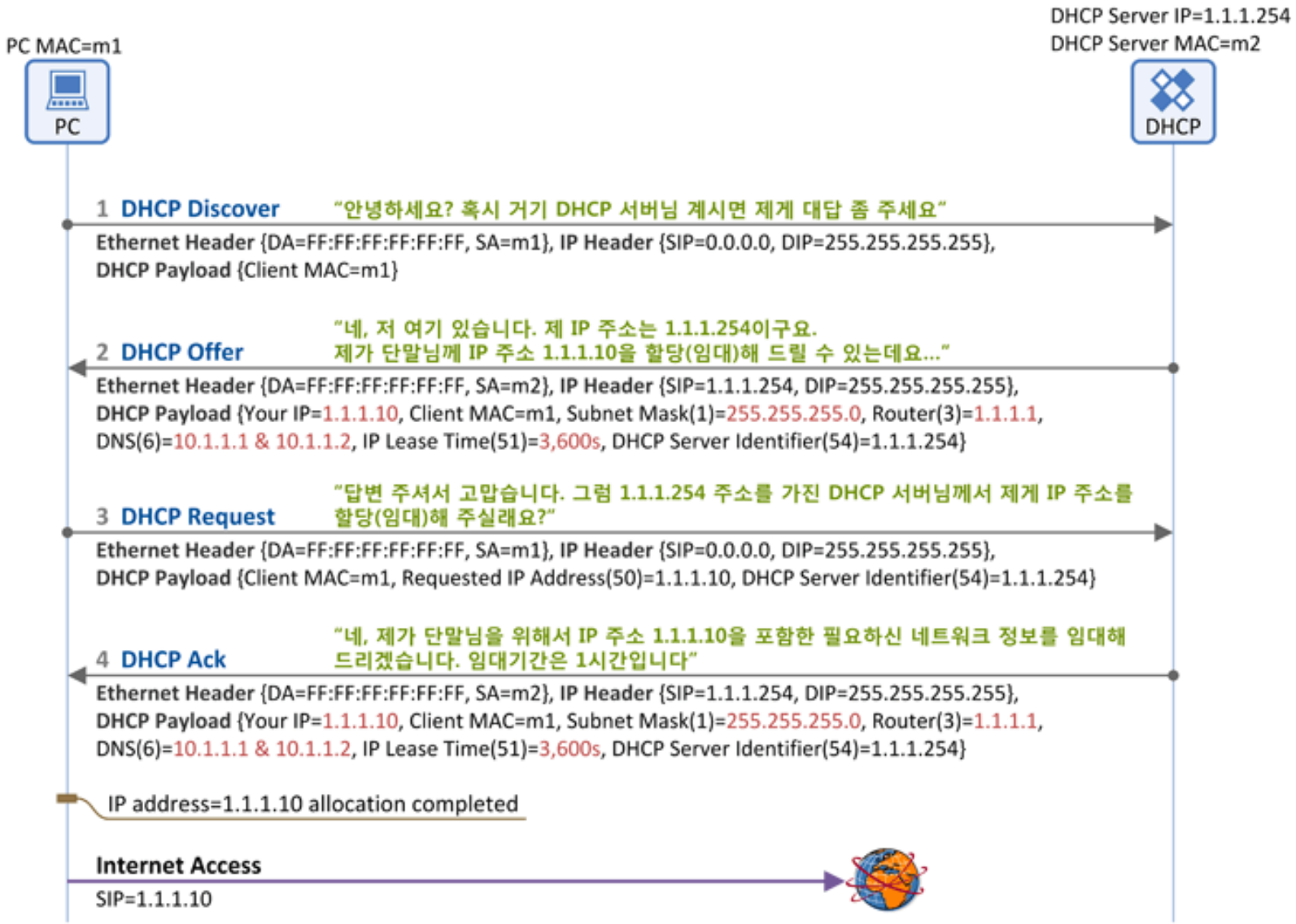
HTTPS Tunnel(a.k.a SSL Tunnel)은 방화벽을 통과하는데 있어 자유롭습니다.

10. L2 SPN Internal Architecture(6) – DHCP(1)

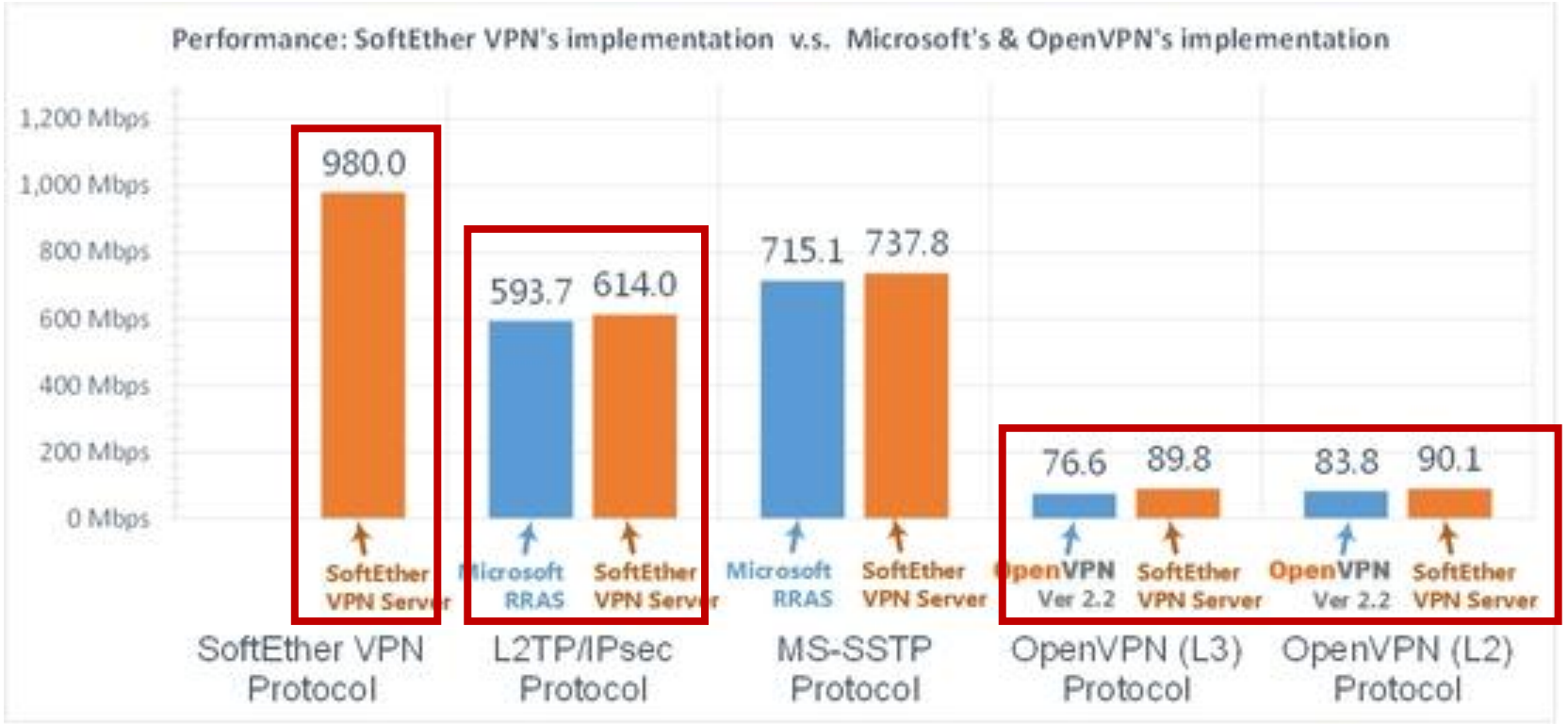


(1), (2) 부분에서 race condition이 발생할 수 있다. 이 경우 static ip 설정을 해 주면 VPN 사용에 문제가 없다.

10. L2 SPN Internal Architecture(6) – DHCP(2)



10. L2 SPN Internal Architecture(7) – Performance



Windows Server 2008 R2 x64 on Intel Xeon E3-1230 3.2GHz and Intel 10 Gigabit CX4 Dual Port Server Adapter.
Microsoft RRAS: L2TP and SSTP VPN Server of Routing and Remote Access Service.
OpenVPN: OpenVPN Technologies OpenVPN 2.2 (open-source version).
Performance Test by Daiyuu Nobori at University of Tsukuba. Japan.

Thank You

We Secure the Internet of Things with 2STON™