

2ip 2STON SPN

- L2 SPN Setup Guide -

2ip, Inc.

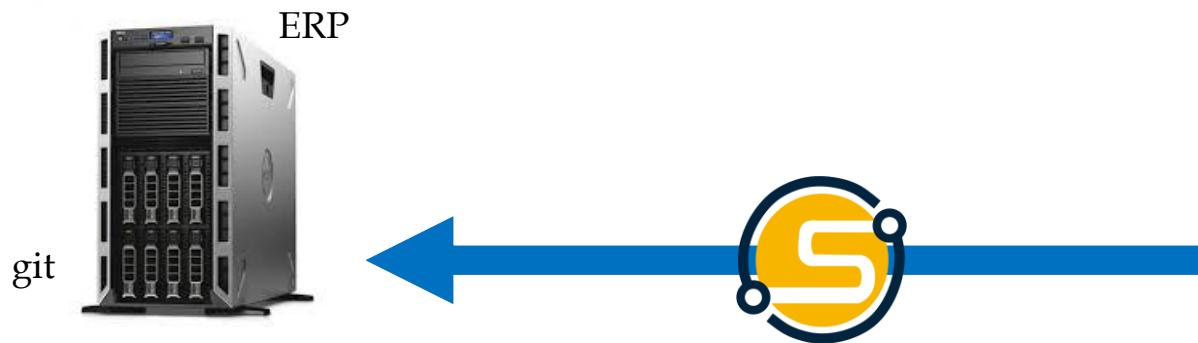
Doc. Revision: 1.2

Copyright© 2018-2020, 2ip Inc. All Rights Reserved.



Contents(1)

- 1. 2ip SPNBox 소개
- 2. VPN 네트워크 구성 : [VPN 망 구성 예](#)
- 3. SPN Gateway & SPN Bridge : [상세 Setup Guide](#)
- 4. SPN Gateway & SPN Client : [상세 Setup Guide](#)
- 5. SPN Gateway & Mobile Phone1 : [OpenVPN Setup Guide](#)
- 6. SPN Gateway & Mobile Phone2 : [L2TP/IPsec Setup Guide](#)
- 7. SPN Gateway Cluster : [상세 Setup Guide](#)

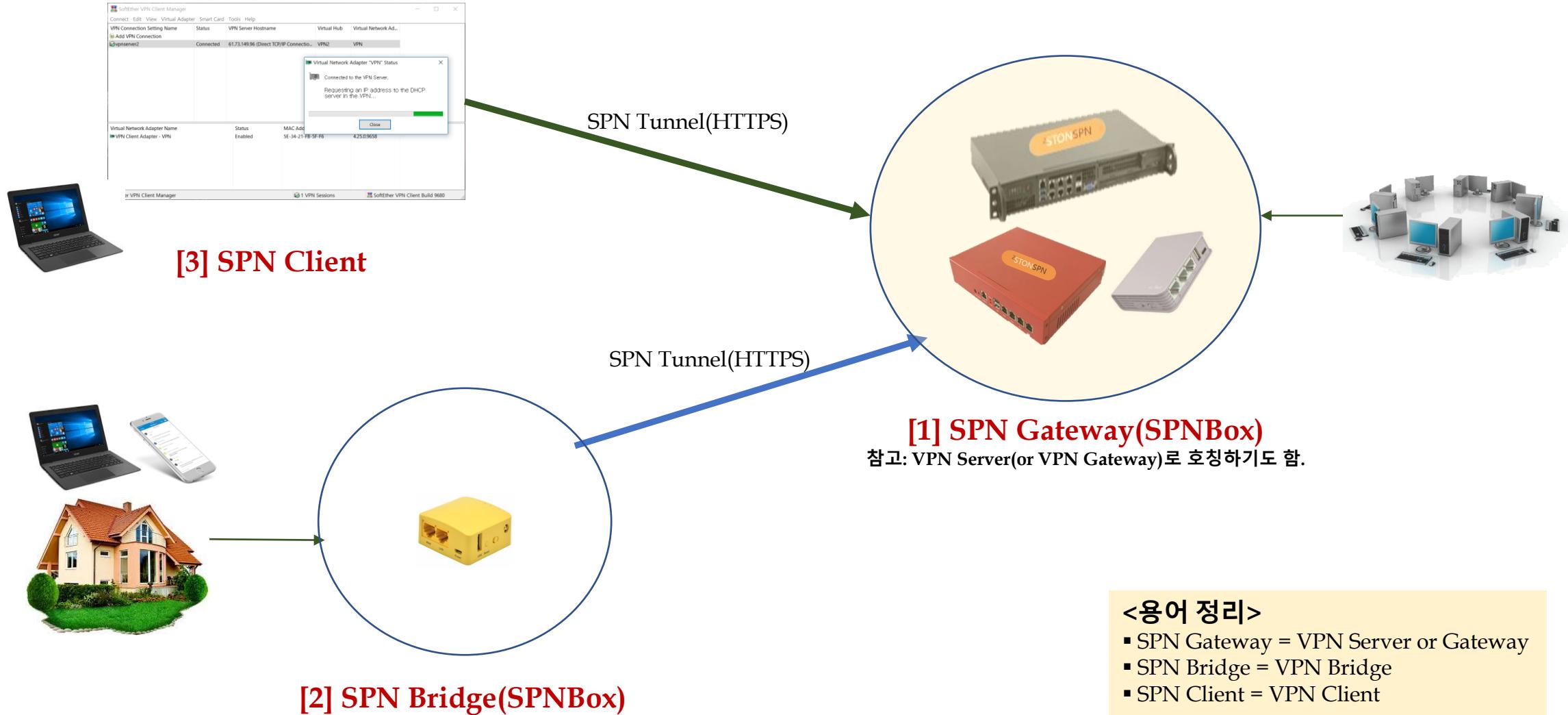


Contents(2)

- 8. Internet 접속 차단 : [상세 Setup Guide](#)
- 9. Standalone Server : [상세 Setup Guide](#)
- 10. L2 SPN Internal Architecture

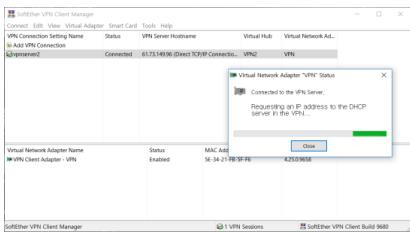
1. 2ip SPNBox 소개(1)

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



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



서버 5대 처리

SPN Gateway



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

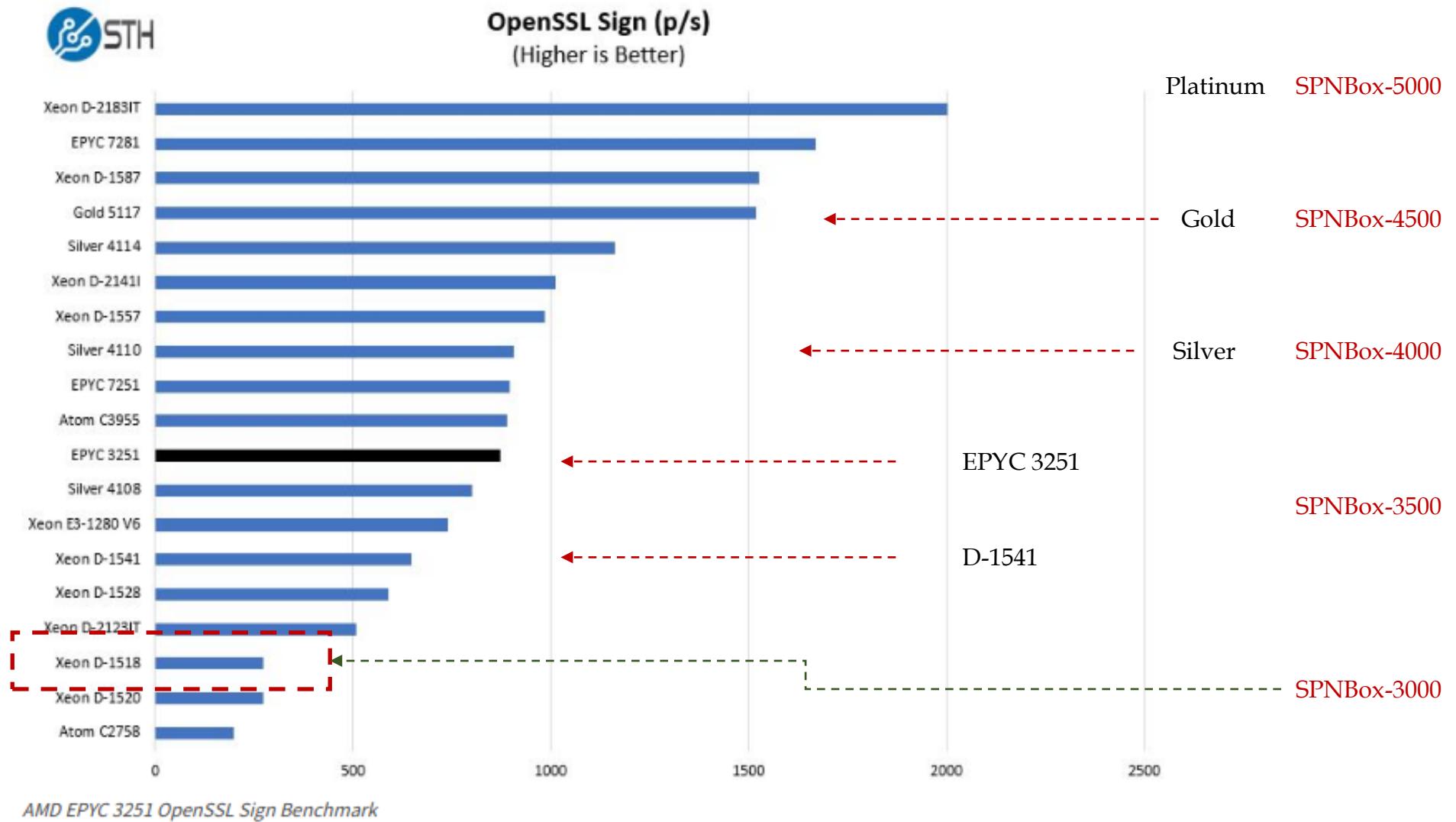
Robust storage options with 2x internal 2.5" SATA, 1x mSATA, plus up to 8 x SSD/HDD or PCIe SSD via NMC modules

IPMI 2.0 compliant Remote Management

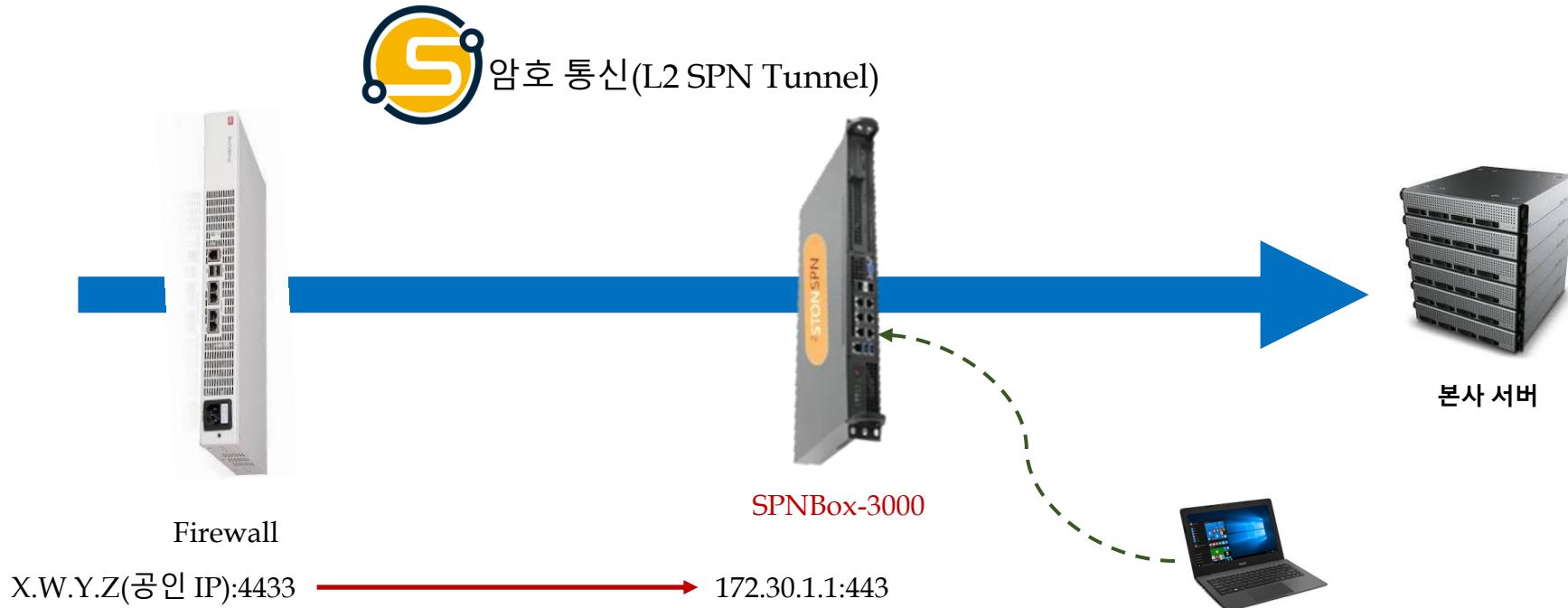
System management features include 2 x RJ45 management ports & BMC AST2500
Operating Temperature: 0 ~ 40 °C (32 ~ 104 °F) via advanced thermal design

Linux 지원(CentOS, Ubuntu)

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



1. 2ip SPNBox 소개(3) – SPN Gateway



1. L2 SPN Tunnel 연결을 위해 본사 방화벽(Firewall)에서 Port Forwarding($4433 \rightarrow 443$) 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.



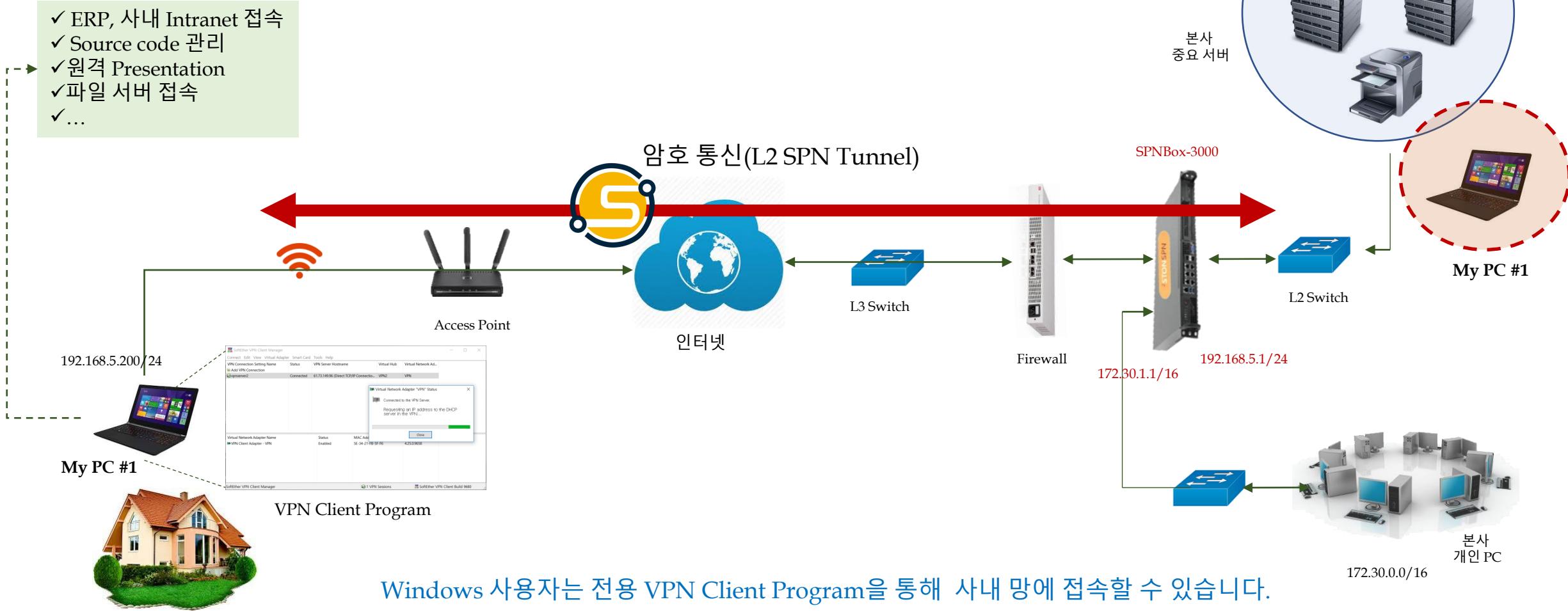
3. 본사에서 제공한 외부 공인 IP 주소 & 포트 및 사용자 계정 정보를 입력한 후, VPN 연결을 시도한다.

4. 이제부터는 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.

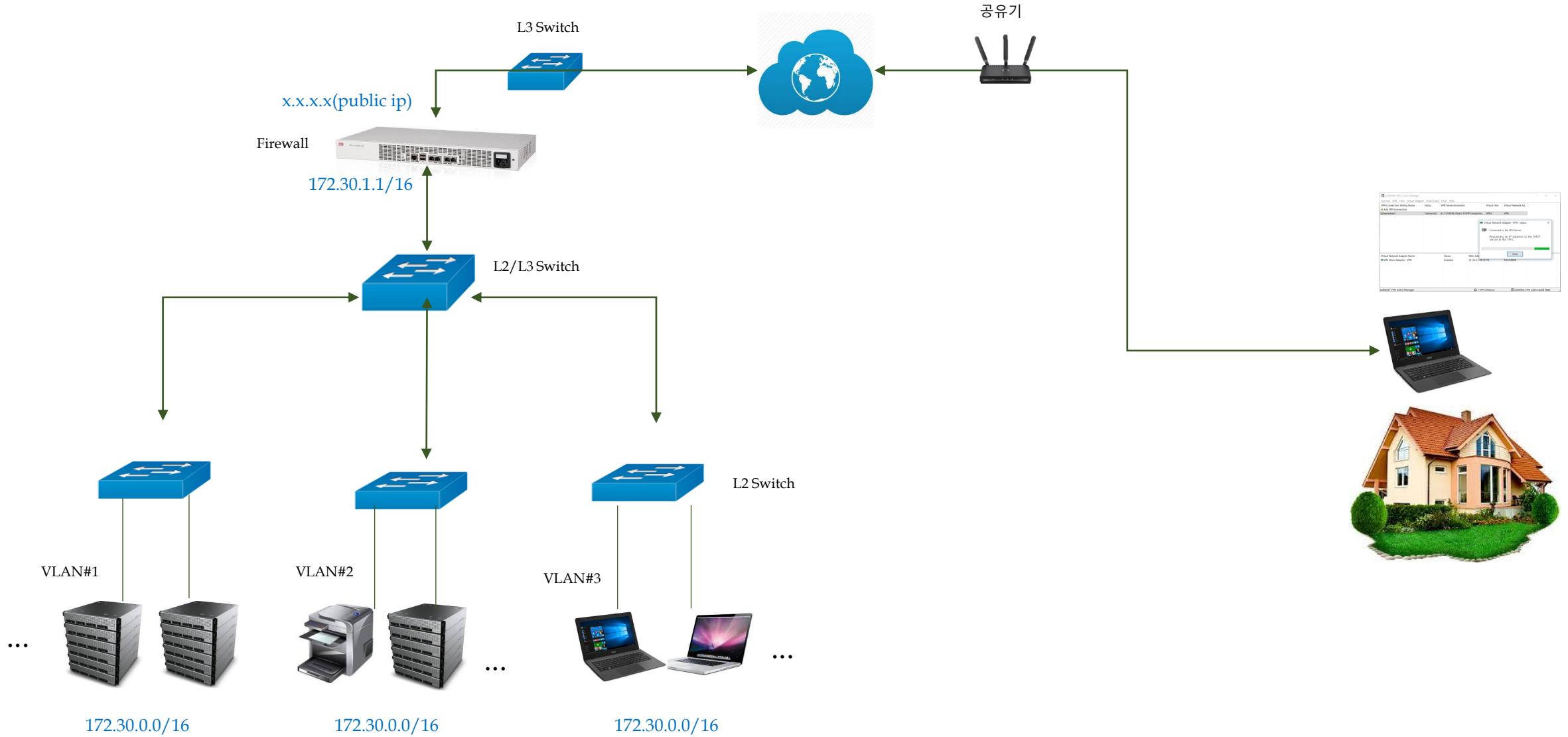
1. 2ip SPNBox 소개(5) - SPN Client

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

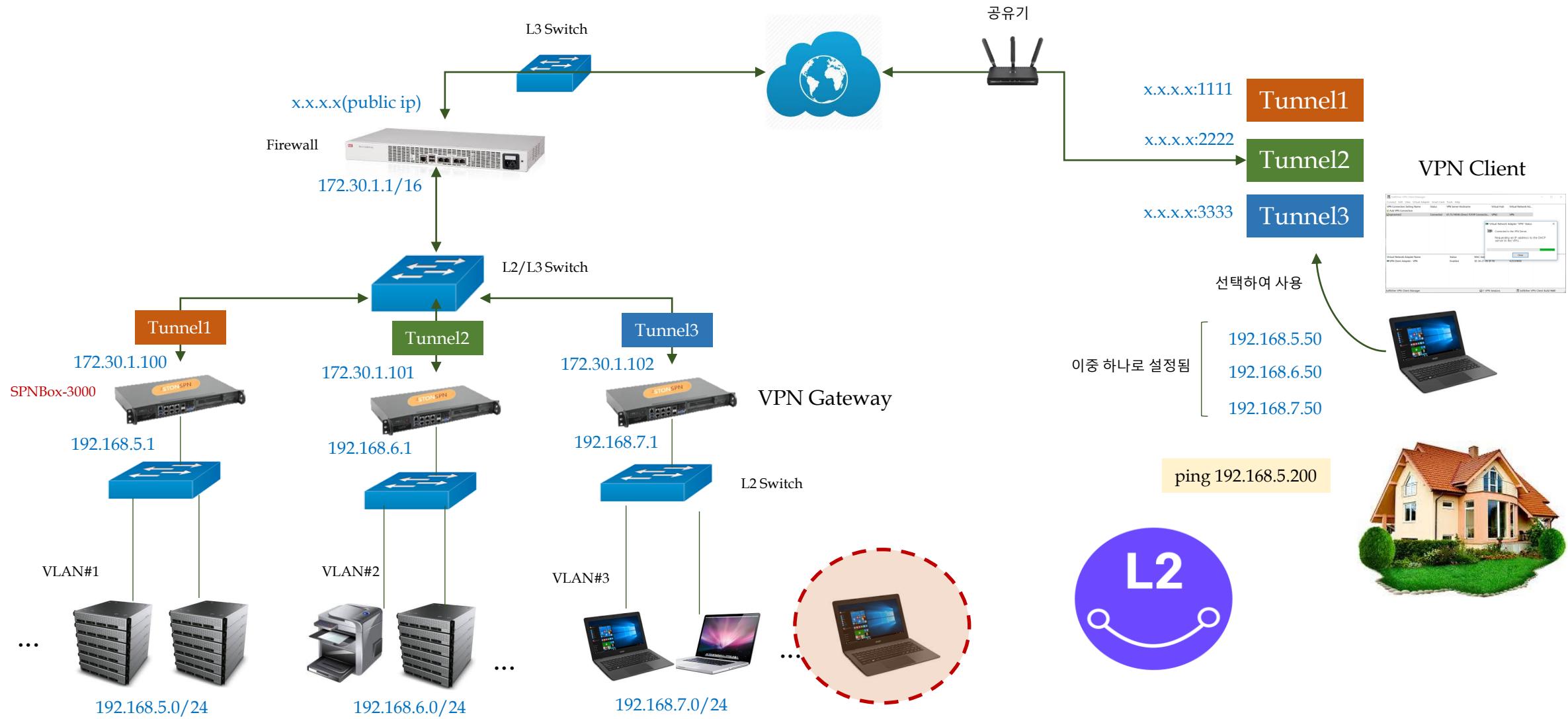


2. VPN 네트워크 구성 : VPN망 구성 예

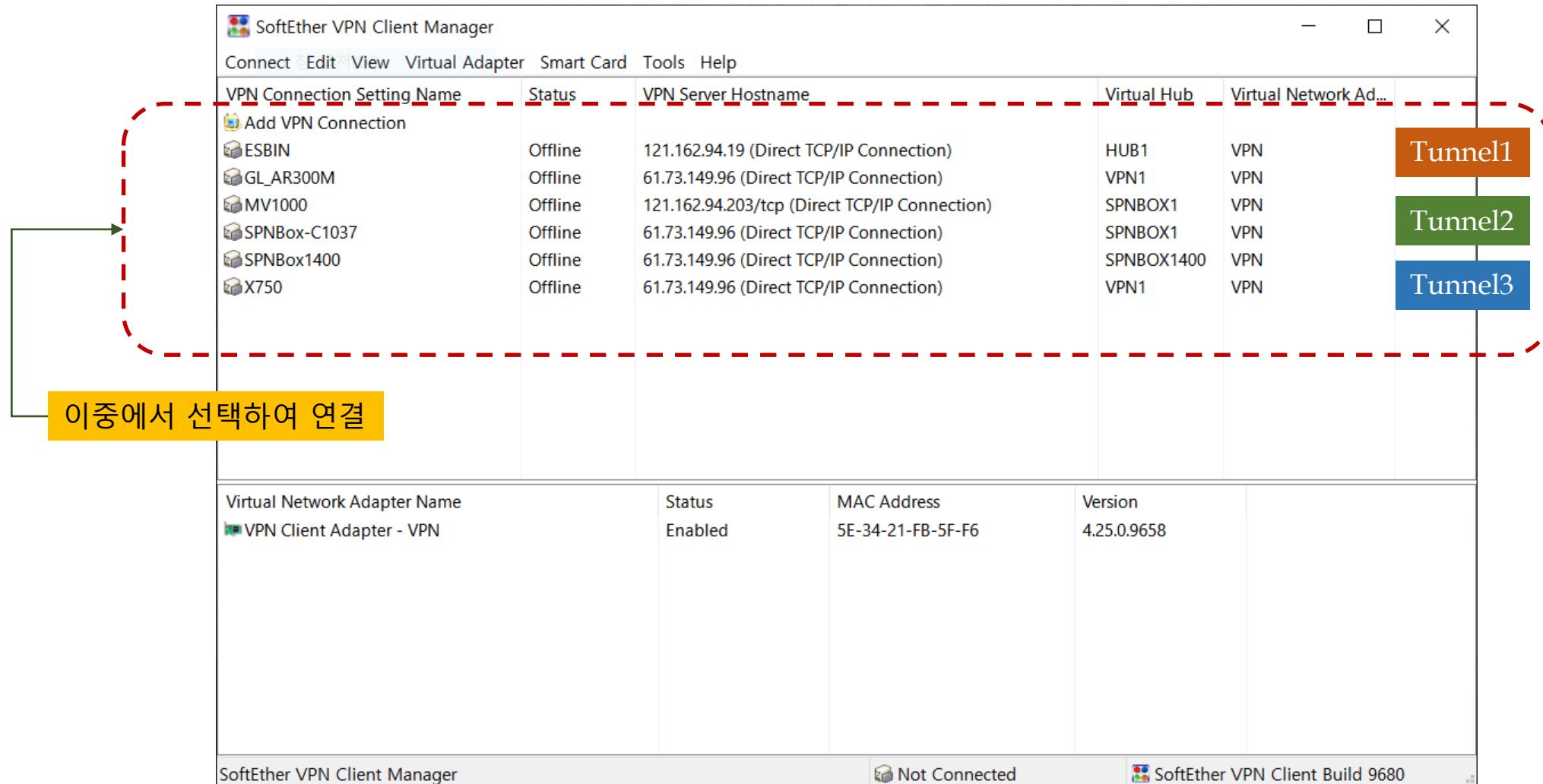
2. VPN 네트워크 구성(1)



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

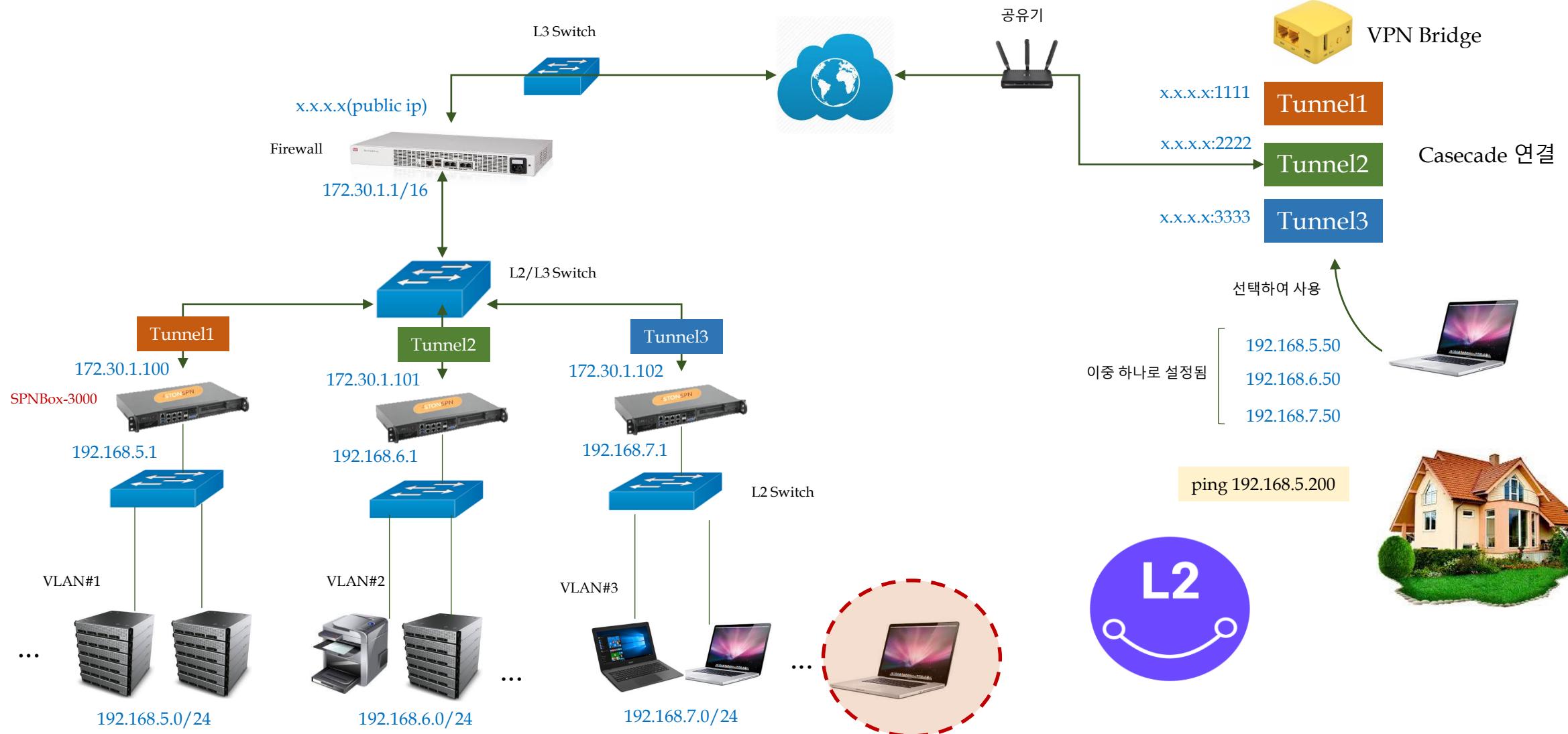


2. VPN 네트워크 구성(2) - SPN Gateway & SPN Client(2)

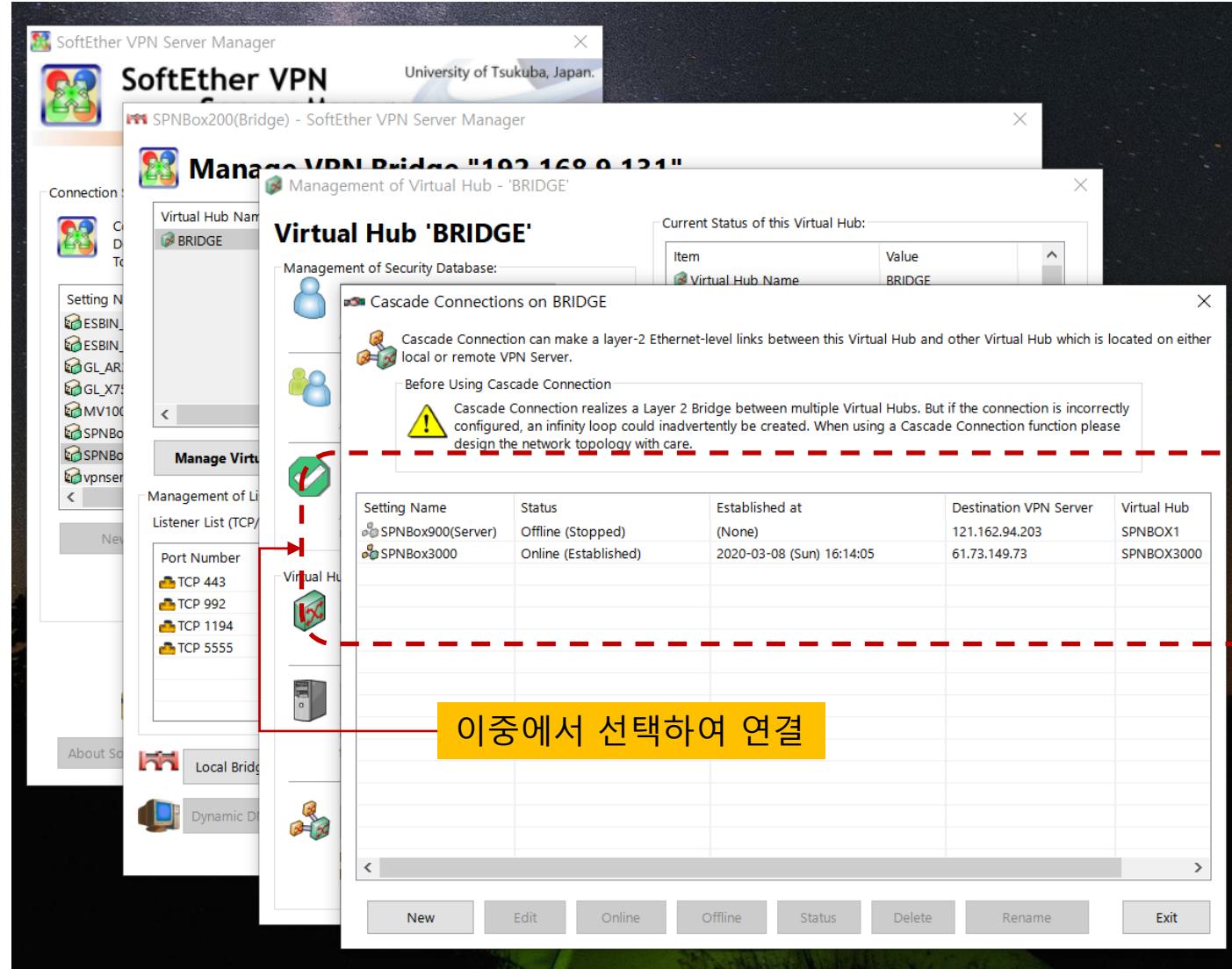


L2 SPN Client

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



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



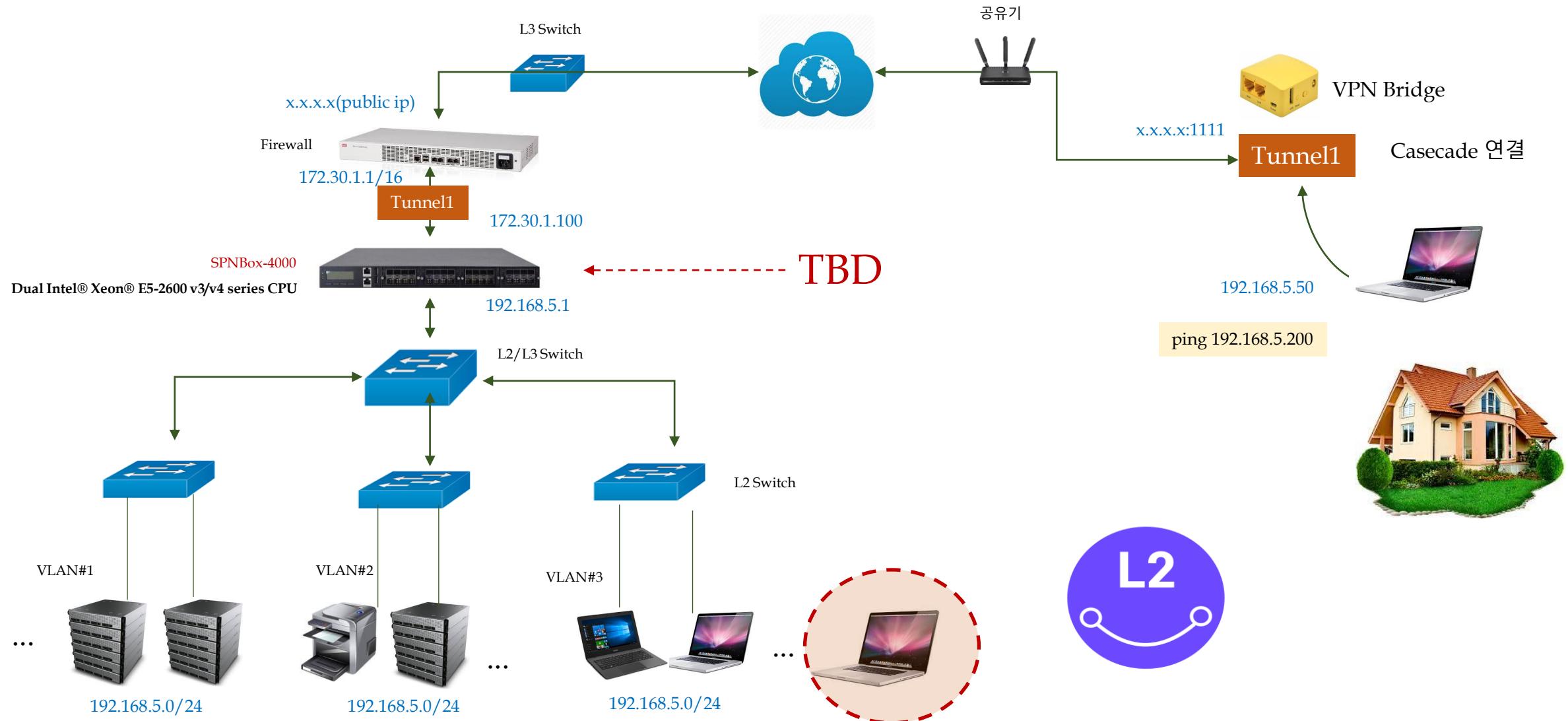
L2 SPN Bridge

Tunnel1

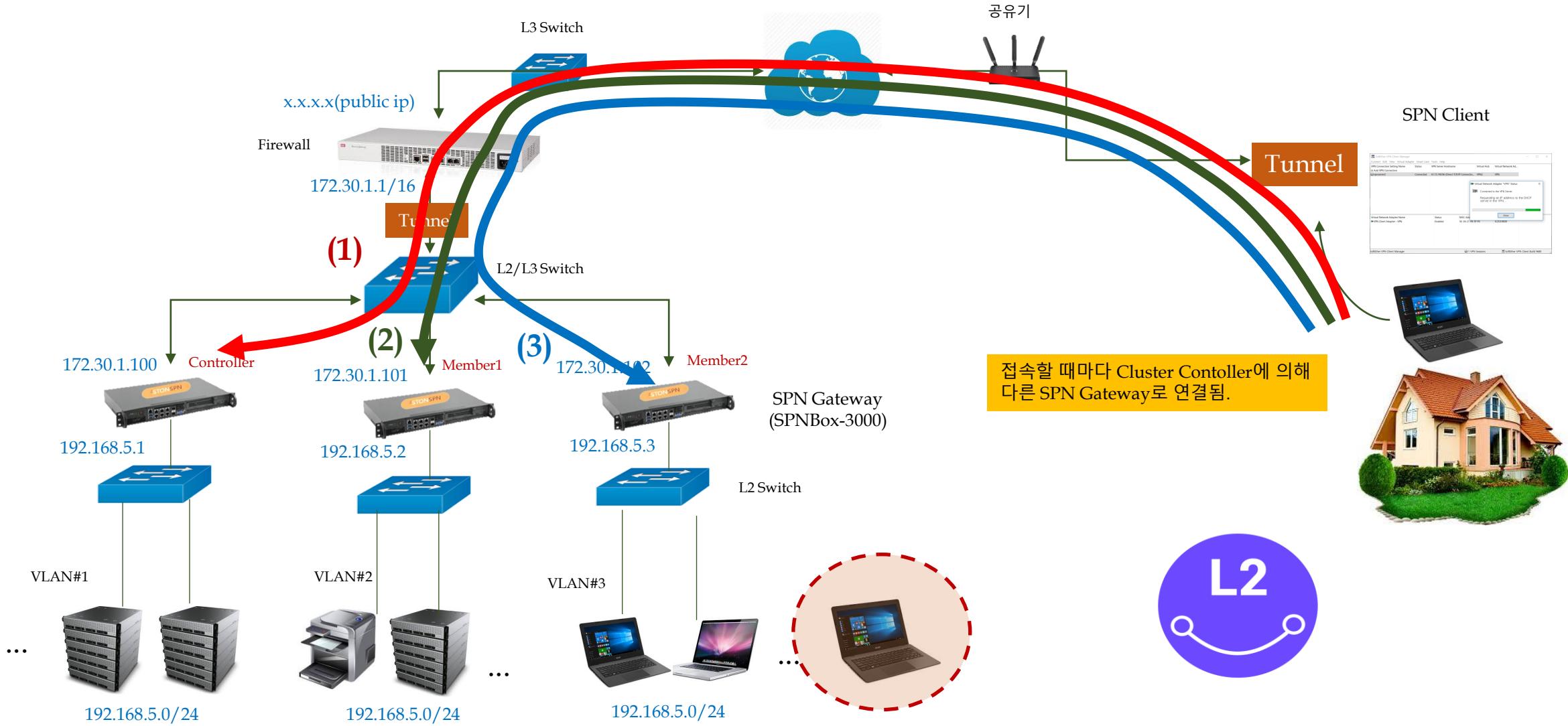
Tunnel2

Tunnel3

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

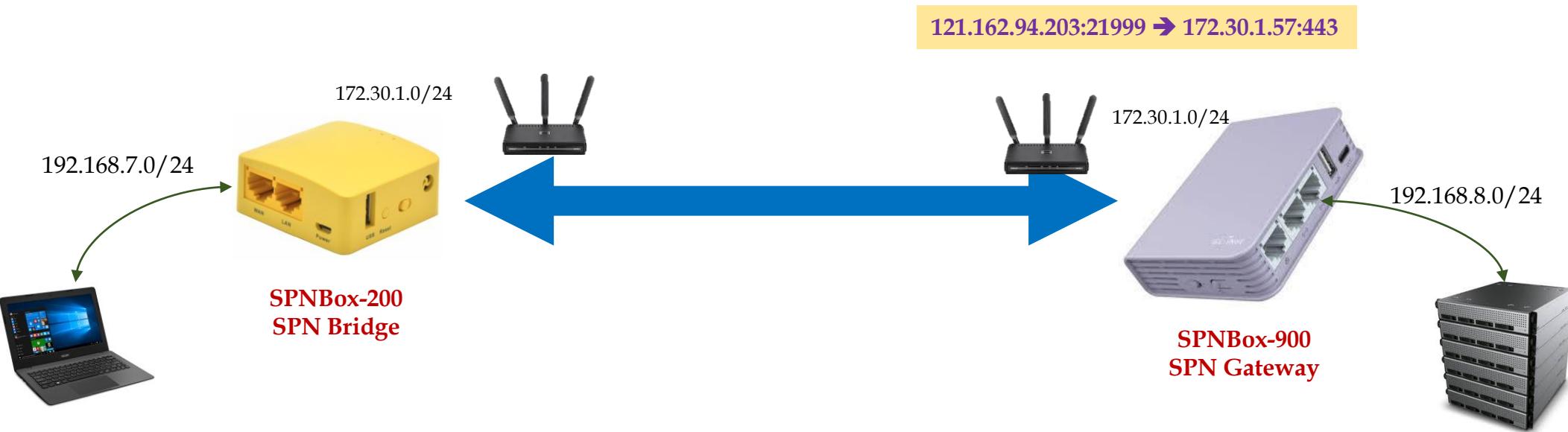


2. VPN 네트워크 구성(5) - SPN Gateway Cluster



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).

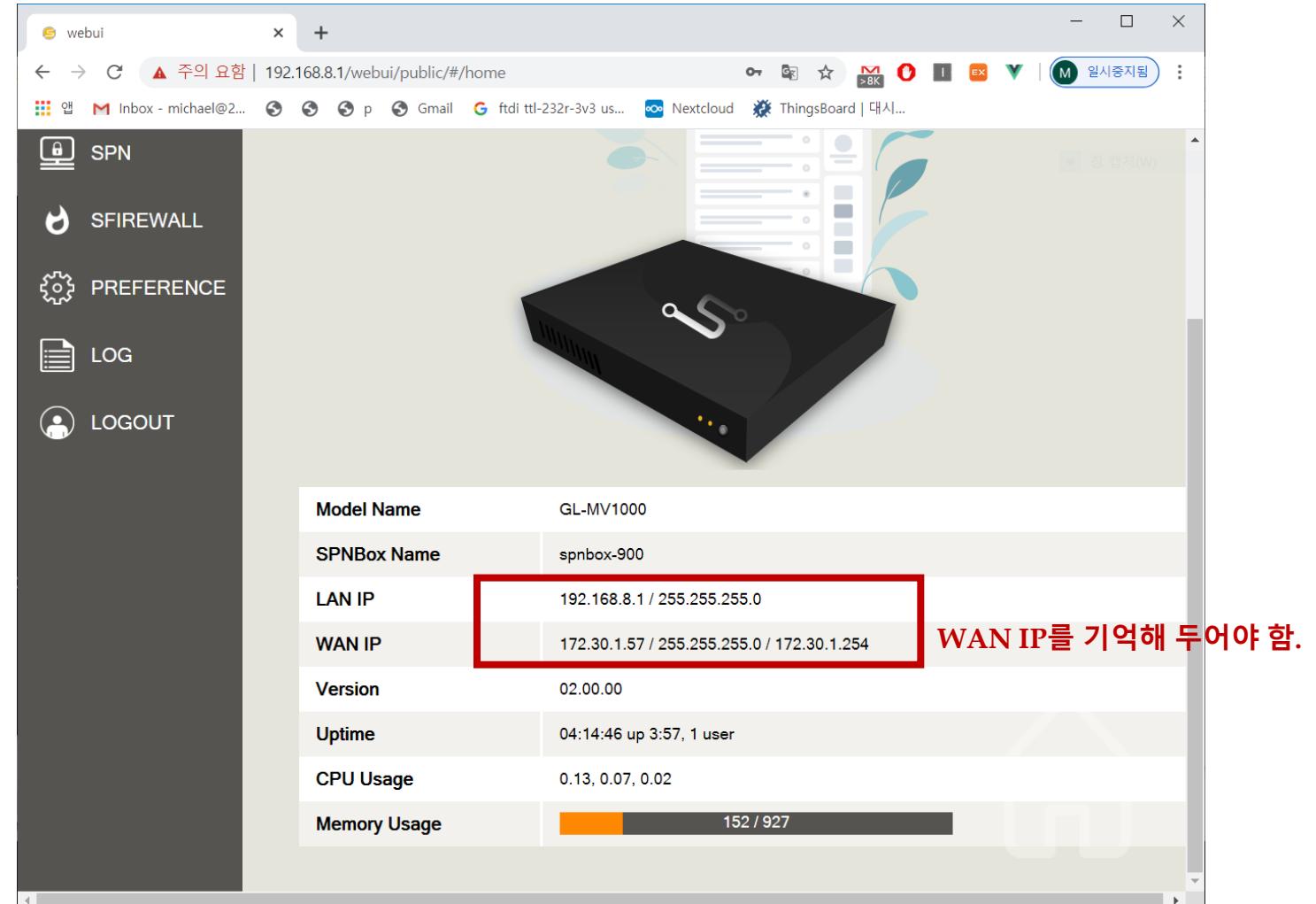
SPN Bridge	전체 설정 절차 요약
a)	VPN Bridge를 구동시키고, vpncmd로 admin password를 설정한다(SPNBox CLI에서 수행)
b)	Windows PC에서 VPN Server Manager로 VPN Bridge에 접속한 후, 가장 기본적인 서버 설정(local ip address, port, admin password 입력)을 한다.
c)	Virtual Hub은 새로 추가할 수 없으며, 기 등록되어 있는 녀석(BRIDGE)을 그대로 사용한다.
d)	나머지는 수행할 필요가 없으며, VPN Server와의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

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



SPNBox-900
VPN Gateway

LAN: 192.168.8.0/24



The screenshot shows the web-based user interface (webui) of the SPNBox-900. The URL in the browser is 192.168.8.1/webui/public/#/home. The page features a sidebar with icons for SPN, SFIREWALL, PREFERENCE, LOG, and LOGOUT. The main area displays a 3D rendering of the black SPNBox-900 device. Below the device, there is a table with various system statistics. The WAN IP field is highlighted with a red border, and a red box surrounds both the LAN IP and WAN IP fields. A red text annotation to the right of the WAN IP field reads "WAN IP를 기억해 두어야 함." (Remember to save the WAN IP).

Model Name	GL-MV1000
SPNBox Name	spnbox-900
LAN IP	192.168.8.1 / 255.255.255.0
WAN IP	172.30.1.57 / 255.255.255.0 / 172.30.1.254
Version	02.00.00
Uptime	04:14:46 up 3:57, 1 user
CPU Usage	0.13, 0.07, 0.02
Memory Usage	152 / 927

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
  VPN Command Line Management Utility (vpncmd command)
  edition
  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.

```
2. Management of VPN Server or VPN Bridge
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 port number 443 of localhost (this computer).
Hostname of IP Address of Destination: <Enter> 입력

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: <Enter> 입력

Connection has been established with VPN Server "localhost" (port 443).

You have administrator privileges for the entire VPN Server.
```

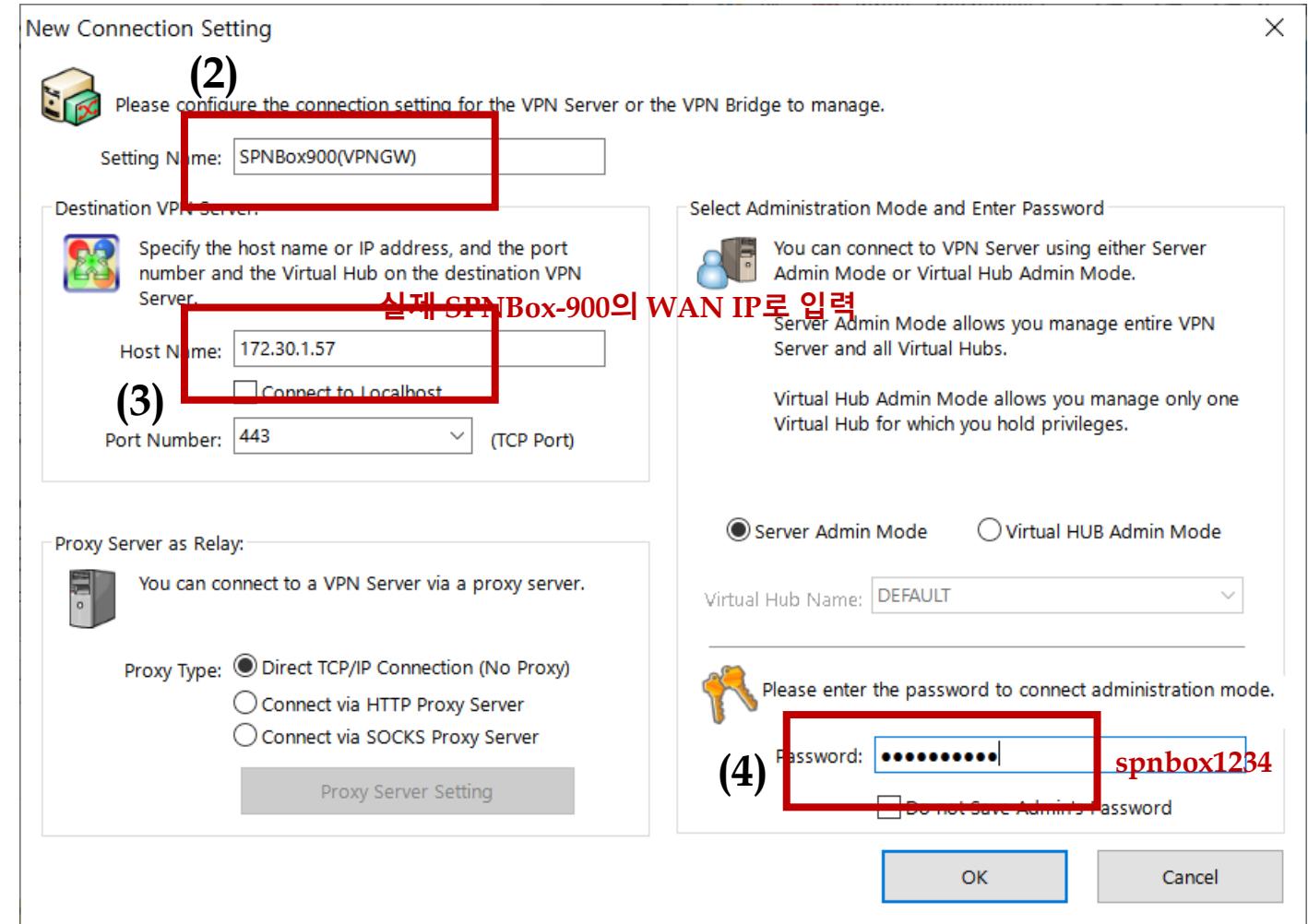
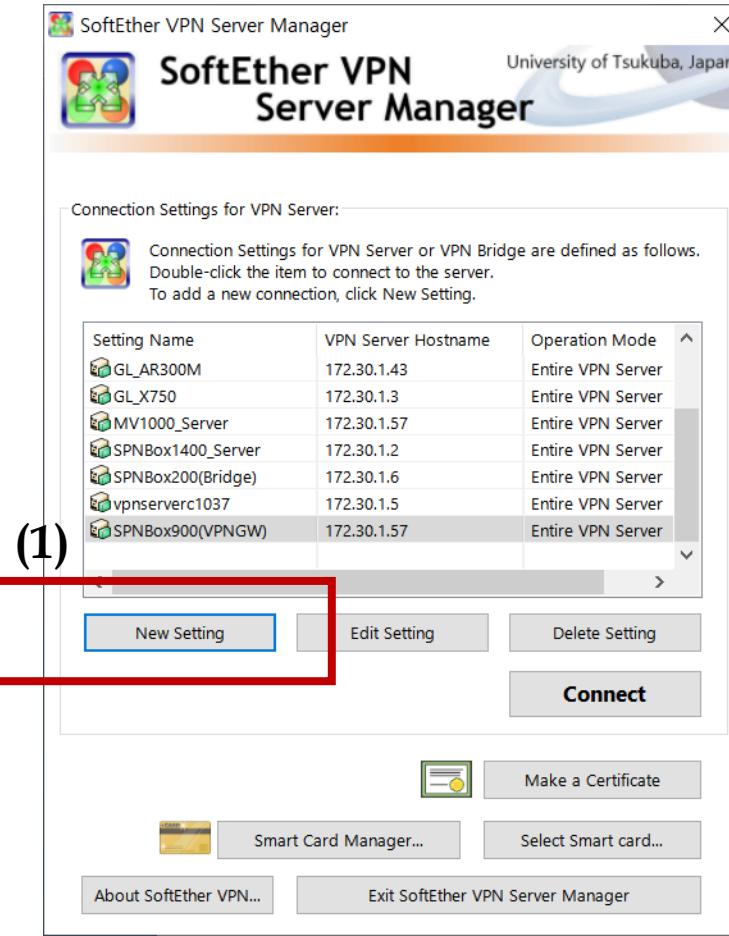
```
VPN Server>ServerPasswordSet
ServerPasswordSet command - Set VPN Server Administrator Password
Please enter the password. To cancel press the Ctrl+D key.
```

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

The command completed successfully.

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)

SoftEther VPN Server / Bridge Easy Setup

By using this setup you can easily setup a SoftEther VPN Server or VPN Bridge for the following use and purpose. After exiting the setup, you can use the VPN Server Manager to freely configure more advanced settings.

Select the type of VPN server you want to build. Multiple types can be selected together.

Remote Access VPN Server

The Remote Access VPN Server allows VPN Client computers in remote locations to access to the existing Ethernet segments, for example company LAN.

Any VPN Clients who is connecting to the VPN Server will be able to access to the network as if they are connected directly and physically to the network.

Site-to-site VPN Server or VPN Bridge

Site-to-site VPN is a VPN configuration to connect between two or more remote Ethernet segments.

Each of the sites are connected together, and become the same segment at Layer-2 level. It enables any computers of each sites to communicate to each other as if there is a single network.

Select the role of this VPN Server:

VPN Server that Accepts Connection from Other Sites (Center)
 VPN Server or VPN Bridge access Site (Edge)

Other Advanced Configuration of VPN

Select this if you are planning to build a VPN system that provides advanced functions such as a clustering function and a Virtual Layer 3 Switch function.

Click Next > to start Setup. Click Close if you want to exit the setup and manually configure all settings.

Next > **Close**

SPNBox900(VPNGW) - SoftEther VPN Server Manager

Manage VPN Server "172.30.1.57"

Virtual Hub Name	Status	Type	Users	Groups	Sessions	MAC Tables	IP Tables
DEFAULT	Online	Standalone	0	0	0	0	0

Manage Virtual Hub **Online** **Offline** **View Status** **Create a Virtual Hub** **Properties** **Delete**

Management of Listeners:

Listener List (TCP/IP port):

Port Number	Status	Create
TCP 443	Listening	
TCP 992	Listening	
TCP 1194	Listening	
TCP 5555	Listening	

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: vpn433471537.softether.n

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

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

New Virtual Hub

Virtual Hub Name: SPNBOX900

Security Settings:

Administration password for this Virtual Hub.

Password: **pass: hub1234**

Confirm:

No Enumerate to Anonymous Users

Virtual Hub Status:

Set the Virtual Hub status.

Online Offline

Virtual Hub Options:

Limit Max VPN Sessions

Max Number of Sessions: sessions
(Will not count sessions on server side that are generated by Local Bridge, Virtual NAT or Cascade Connection.)

You can configure more advanced settings on the Virtual Hub Extended Option List.

[Edit Virtual Hub Extended Option List](#)

OK Cancel

SPNBox900(VPNGW) - SoftEther VPN Server Manager

Manage VPN Server "172.30.1.57"

Virtual Hub Name	Status	Type	Users	Groups	Sessions	MAC Tables	IP T
DEFAULT	Online	Standalone	0	0	0	0	0
SPNBOX900	Online	Standalone	0	0	0	0	0

Manage Virtual Hub

Management of Listeners:

Listener List (TCP/IP port):

Port Number	Status
TCP 443	Listening
TCP 992	Listening
TCP 1194	Listening
TCP 5555	Listening

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**

Dynamic DNS Setting **VPN Azure Setting**

IPsec / L2TP Setting **OpenVPN / MS-SSTP Setting**

Refresh Exit

Current DDNS Hostname: vpn433471537.softether.n

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

Management of Virtual Hub - 'SPNBOX900'

Virtual Hub 'SPNBOX900'

Management of Security Database:

- Manage Users** (highlighted with a red box)
Add, delete or edit user accounts.
- Manage Groups
Add, delete or edit groups.
- Manage Access Lists
Add or delete access lists (Packet filtering rules).

Virtual Hub Settings:

- Virtual Hub Properties
Configure this Hub.
- Authentication Server Setting
Use external RADIUS authentication server for user authentication.
- Manage Cascade Connections
Establish Cascade Connection to Hubs on local or remote VPN Servers.

Current Status of this Virtual Hub:

Item	Value
Virtual Hub Name	SPNBOX900
Status	Online
Type	Standalone
SecureNAT	Disabled
Sessions	0
Access Lists	0
Users	0
Groups	0
MAC Tables	0
IP Tables	0

Other Settings:

- Log Save Setting
Configure settings of log saving function.
- Trusted CA Certificates
Manage trusted CA certificates.
- Virtual NAT and Virtual DHCP Server (SecureNAT)
Secure NAT is available on this Virtual Hub. You can run Virtual NAT and Virtual DHCP.

VPN Sessions Management:

- Manage Sessions
- Exit

Manage Users

Virtual Hub "SPNBOX900" has the following users.

User Name	Full Name	Group Name	Description	Auth Method	Num Logins	Last Login

New (highlighted with a red box) Edit View User Info Remove Refresh Exit

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

Create New User

User Name: spnuser
Full Name: SPN User
Note: SPN User

Group Name (Optional): Browse Groups...

Set the Expiration Date for This Account
2020-03-11 오전 12:00:00

Auth Type: Anonymous Authentication
 Password Authentication
 Individual Certificate Authentication
 Signed Certificate Authentication
 RADIUS Authentication
 NT Domain Authentication

RADIUS or NT Domain Authentication Settings:
Login attempts by password will be verified by the external RADIUS server, Windows NT domain controller, or Active Directory controller.
 Specify User Name on Authentication Server
User Name on Authentication Server:

Security Policy

Set Security Policy Security Policy

pass: spnuser1234

Manage Users

Virtual Hub "SPNBOX900" has the following users.

User Name	Full Name	Group Name	Description	Auth Method	Next Login	Last Login
spnuser	SPN User	-	SPN User	Password Authen...	0	(None)

OK **Cancel**

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

SPNBox900(VPNGW) - SoftEther VPN Server Manager

Manage VPN Server "172.30.1.57"

Virtual Hub Name	Status	Type	Users	Groups	Sessions	MAC Tables	IP Tables
DEFAULT	Online	Standalone	0	0	0	0	0

Management of Listeners:

Listener List (TCP/IP port):

Port Number	Status
TCP 443	Listening
TCP 992	Listening
TCP 1194	Listening
TCP 5555	Listening

Buttons: Create, Delete, Start, Stop, Local Bridge Setting, Layer 3 Switch Setting, IPsec / L2TP Setting, OpenVPN / MS-SSTP Setting, Dynamic DNS Setting, VPN Azure Setting.

Current DDNS Hostname: vpn433471537.softether.n

Local Bridge Settings

Local Bridge can establish a Layer 2 bridge connection between a Virtual Hub on this VPN server and a physical Ethernet Device (Network Adapter). It is also possible to create a tap device (virtual network interface) and establish a bridge connection with a Virtual Hub. (Tap is supported on Linux versions only)

Number	Virtual Hub Name	Network Adapter or Tap Device Name	Status

Delete Local Bridge

New New Local Bridge Definition:

Select the Virtual Hub to bridge.

Virtual Hub: SPNBOX900

Type to Create: Bridge with Physical Existing Network Adapter Bridge with New Tap Device

Enter a name of the new tap device to create.

LAN Adapter: Bond0

New Tap Device Name: vpn (Maximum 11 Characters)

Note: Although it is possible to establish a bridge using any operating network adapter, in high load environments, you should prepare a network adapter dedicated for bridging.

Create Local Bridge

If a network adapter doesn't appear which is recently added on the system, reboot the computer and re-open this screen.

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

Instructions for Local Bridge on VM

Using Local Bridge Function on VM

It has been detected that the VPN Server might be running on a VM (Virtual Machine) suchlike VMware or Hyper-V. Read the following instructions carefully. If you are not using a VM, please ignore this message.

Instructions

Some VMs prohibit the "Promiscuous Mode" (MAC Address Spoofing) on the network adapters by default.

If the Promiscuous Mode (MAC Address Spoofing) is administratively disabled, the Local Bridge function between a Virtual Hub on the VPN Server and a physical network adapter on the physical computer does not work well. You should allow the Promiscuous Mode (MAC Address Spoofing) by using the configuration tool of the VM.

For details please refer the documents of your VM. If it is a shared-VM and administrated by other person, please request the administrator to permit the use of the Promiscuous (MAC Address Spoofing) Mode to your VM.

OK

Virtual Hub의 동작 원리

Local Bridge Settings

Local Bridge can establish a Layer 2 bridge connection between a Virtual Hub on this VPN server and a physical Ethernet Device (Network Adapter). It is also possible to create a tap device (virtual network interface) and establish a bridge connection with a Virtual Hub. (Tap is supported on Linux versions only)

Number	Virtual Hub Name	Network Adapter or Tap Device Name	Status
1	SPNBOX900	vpn	Operating

Delete Local Bridge

New Local Bridge Definition:

Select the Virtual Hub to bridge.

Virtual Hub:

Type to Create: Bridge with Physical Existing Network Adapter Bridge with New Tap Device

Enter a name of the new tap device to create.

LAN Adapter: bond0

New Tap Device Name: (Maximum 11 Characters)

Note: Although it is possible to establish a bridge using any operating network adapter, in high load environments, you should prepare a network adapter dedicated for bridging.

Create Local Bridge

If a network adapter doesn't appear which is recently added on the system, reboot the computer and re-open this screen.

Exit

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

SPNBox-900 CLI 설정 변경

```
tap_vpni: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
          inet6 fe80::5cc5:b5ff:fe13:986f prefixlen 64 scopeid 0x20<link>
          ether 5e:c5:b5:13:98:6f txqueuelen 1000 (Ethernet)
            RX packets 14 bytes 1204 (1.2 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 43 bytes 3546 (3.5 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wan: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 172.30.1.57 netmask 255.255.255.0 broadcast 172.30.1.255
      inet6 fe80::9683:c4ff:fe00:bf8c prefixlen 64 scopeid 0x20<link>
          ether 94:83:c4:00:bf:8c txqueuelen 1000 (Ethernet)
            RX packets 7993 bytes 2257039 (2.2 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 1914 bytes 261568 (261.5 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

spnbox-900(config)# se localbridge tap_vpni
spnbox-900(config)# wr
Configuration saved SUCCESS
```

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 이용 할 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_vpn이라는 virtual interface가 생성된다. 반드시 위의 명칭을 사용하기 바란다.

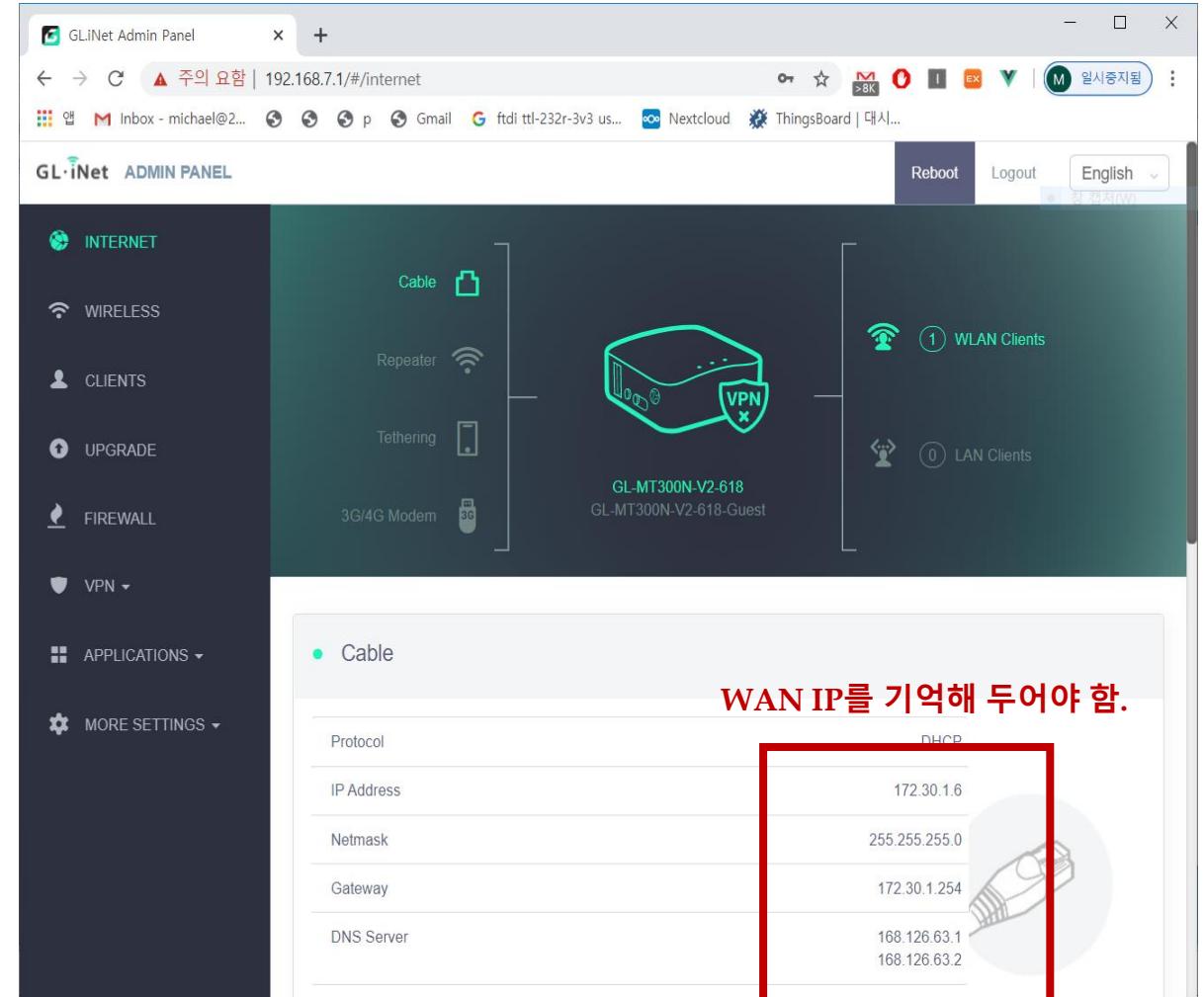
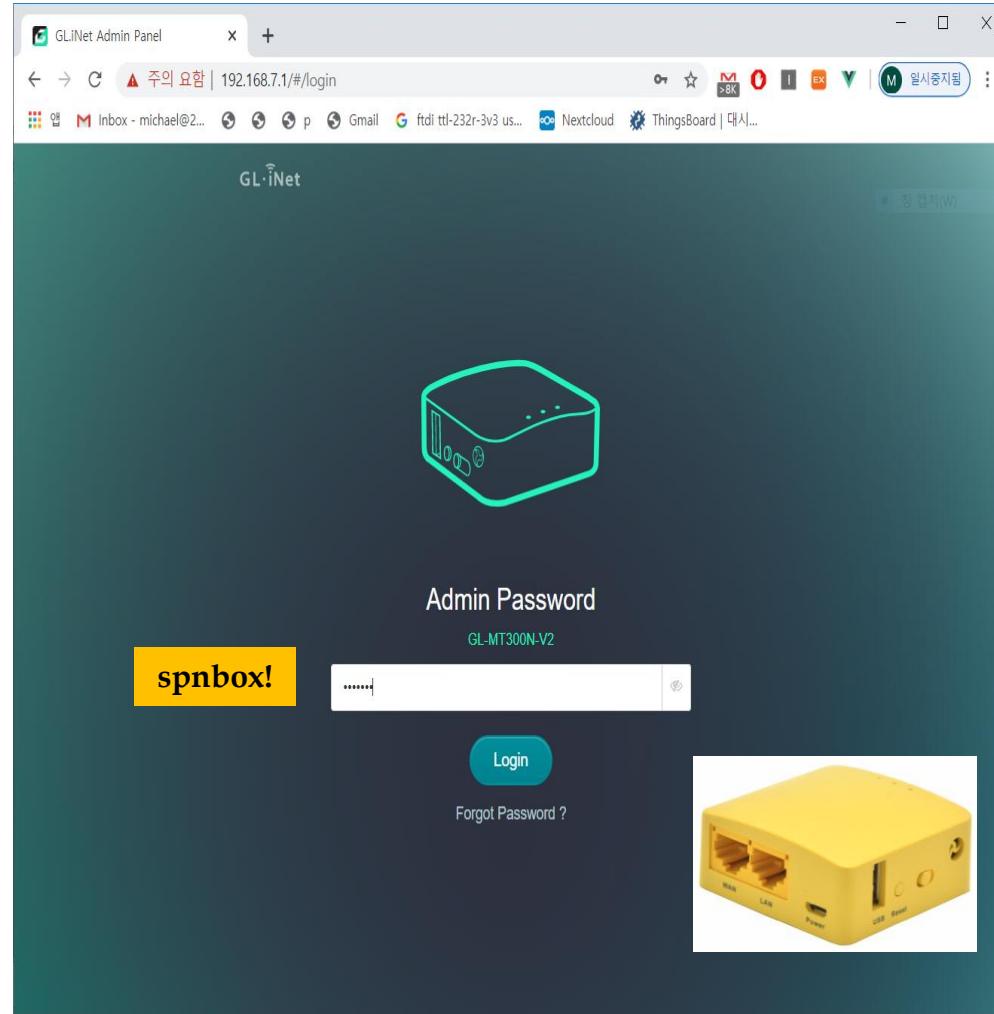
참고: 위의 설정 중 고객이 실제 field 상황에 맞게 재 수정해 주어야 하는 부분은 Local IP address 뿐이다.

- 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)



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: <Enter> 입력

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: <Enter> 입력
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.

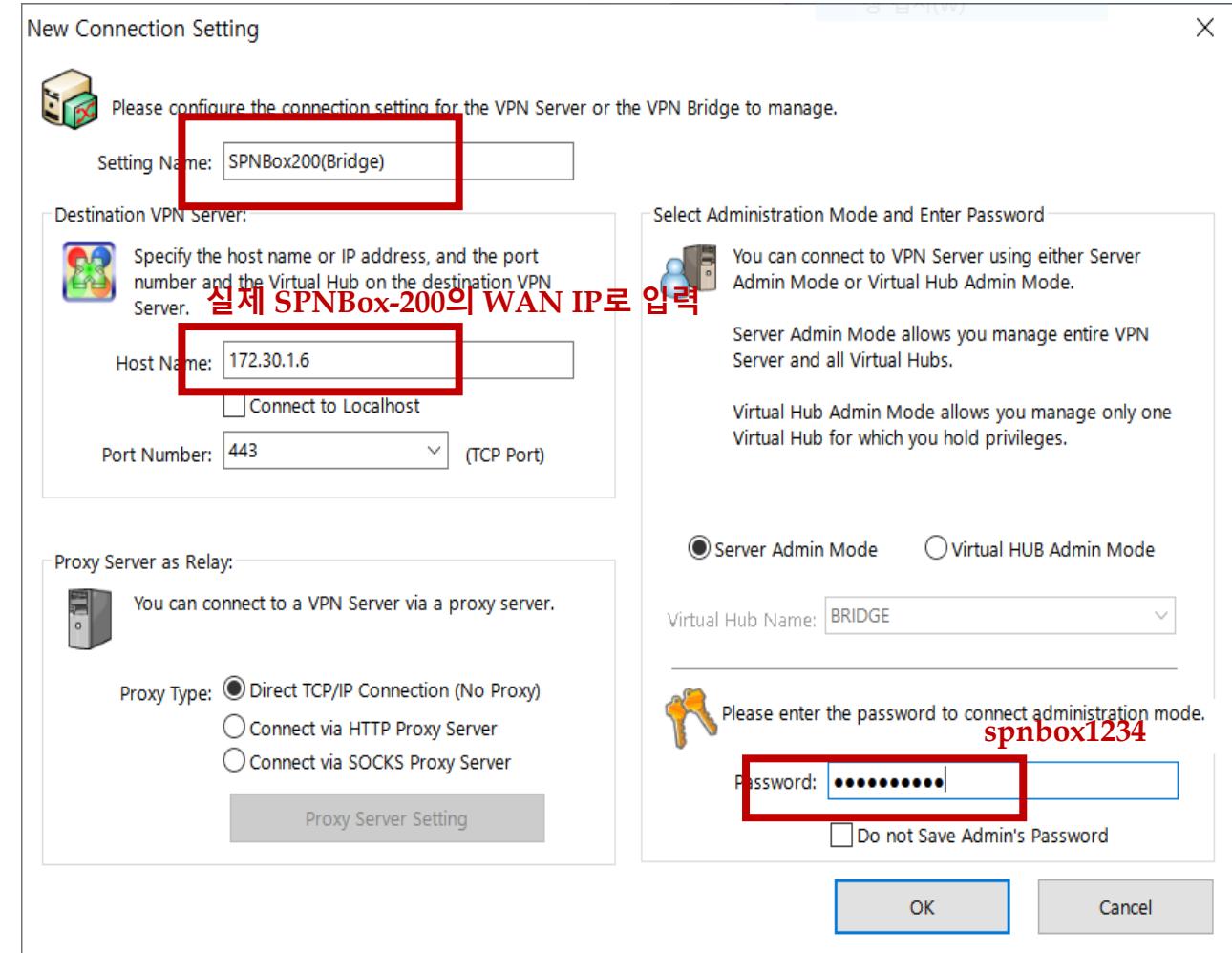
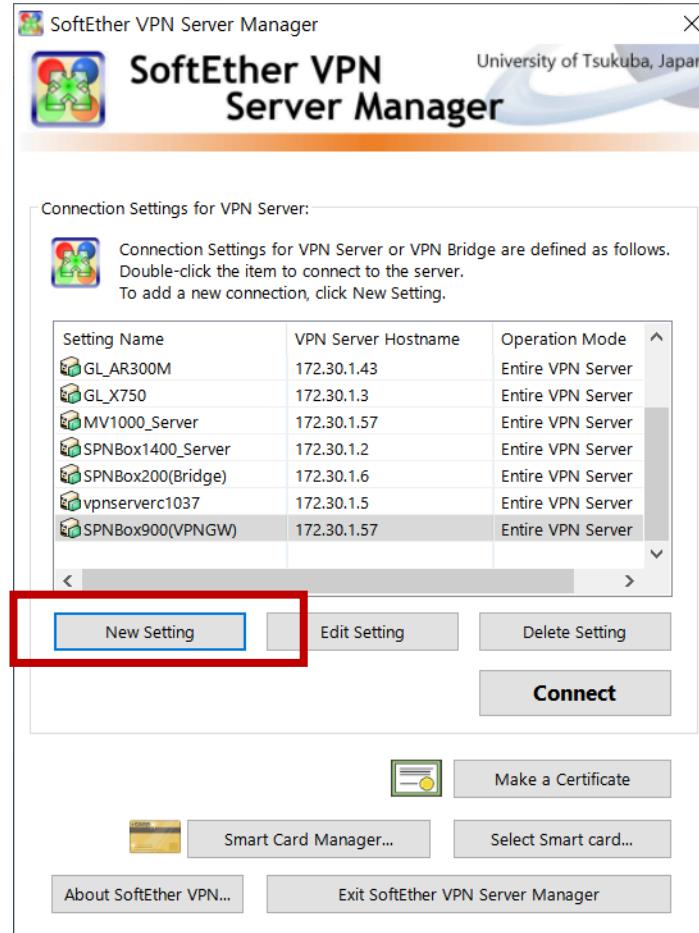
Password: *****
Confirm input: *****

The command completed successfully.

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

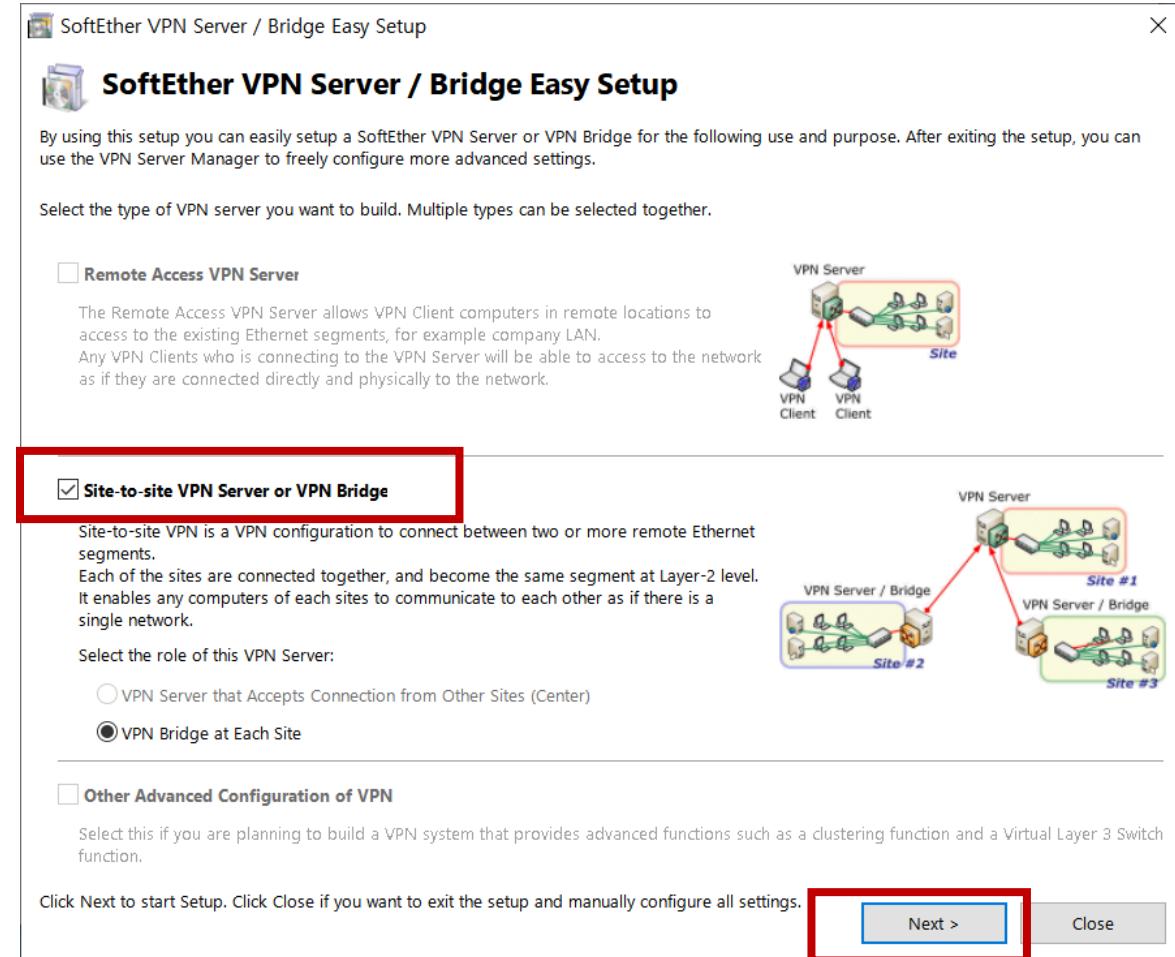
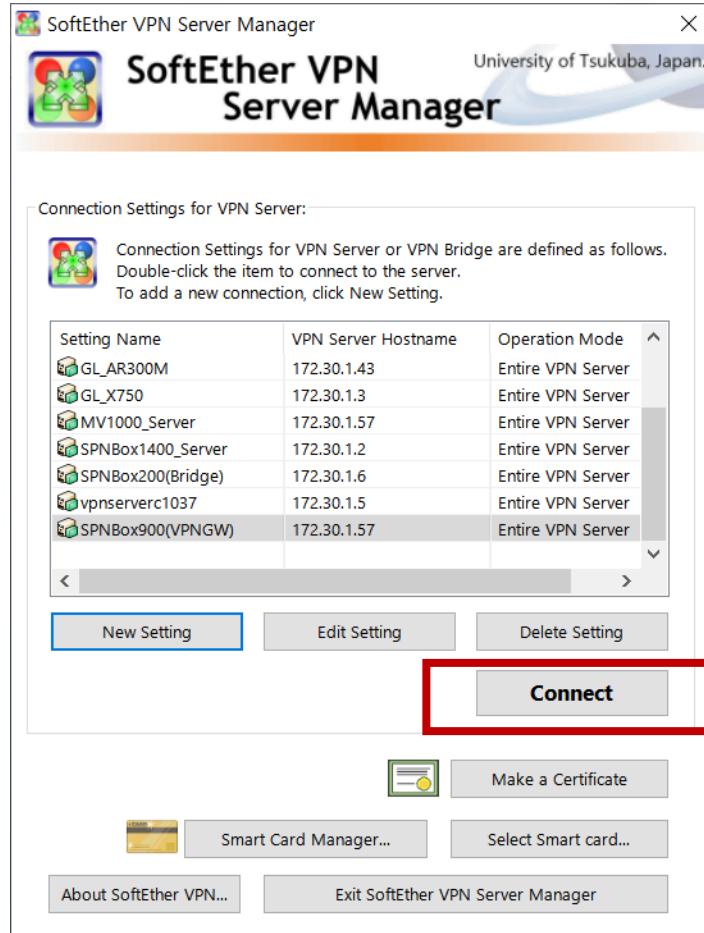
2) VPN Bridge admin 패스워드 설정 (pass: spnbox1234)

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)

VPN Easy Setup Tasks

To complete the setup of this VPN Server / VPN Bridge, you must complete the following tasks.

Step 1. Create a User to Accept VPN Connection

When this VPN Server accepts a remote access VPN, or becomes the central site-to-site VPN server that accepts connections from other sites, create users to accept the VPN connection.

Create Users

Step 2. Define a Connection to Destination VPN Server

When this VPN Server is installed on a particular site (edge) of a site-to-site VPN, you have to specify the address of the center VPN Server that accepts the connections, and establish a connection to that central VPN Server.

Configure Connection Setting

Step 3. Set Local Bridge

For an site-to-site VPN, use the Local Bridge Function to connect a bridge between the virtual Ethernet segment on the VPN side and the physical Ethernet segment on the local side. Select an existing Ethernet device (Network Adapter) that will be provide the bridge connection to the VPN.

Select the Ethernet device to establish the bridge connection.

Once the required settings are configured, click Close. An advanced management tool for VPN Server / VPN Bridge will be appeared. You can then configure any advanced settings as you wish.

Close

SPNBox200(Bridge) - SoftEther VPN Server Manager

Manage VPN Bridge "172.30.1.6"

Virtual Hub Name	Status	Type	Users	Groups	Sessions	MAC Tables	IP Tables
BRIDGE	Online	Standalone	0	0	2	2	1

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

Local Bridge Setting

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
- Layer 3 Switch Setting
- IPsec / L2TP Setting
- OpenVPN / MS-SSTP Setting

Dynamic DNS Setting **VPN Azure Setting** **Refresh** **Exit**

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

Local Bridge Settings

Local Bridge can establish a Layer 2 bridge connection between a Virtual Hub on this VPN server and a physical Ethernet Device (Network Adapter). It is also possible to create a tap device (virtual network interface) and establish a bridge connection with a Virtual Hub. (Tap is supported on Linux versions only)

Number	Virtual Hub Name	Network Adapter or Tap Device Name	Status
1	BRIDGE	br-lan	Operating

New Local Bridge Definition:

Select the Virtual Hub to bridge.

Virtual Hub: BRIDGE

Type to Create:

Bridge with Physical Existing Network Adapter
 Bridge with New Tap Device

Select the Ethernet device (network adapter) for the bridge destination.

LAN Adapter: apcli0

New Tap Device Name: (Maximum 11 Characters)

Note: Although it is possible to establish a bridge using any operating network adapter, in high load environments, you should prepare a network adapter dedicated for bridging.

Create Local Bridge

If a network adapter doesn't appear which is recently added on the system, reboot the computer and re-open this screen.

Exit

이 화면은 변경할 필요가 없는 화면임.

SPNBox200(Bridge) - SoftEther VPN Server Manager

Manage VPN Bridge "172.30.1.6"

Virtual Hub Name	Status	Type	Users	Groups	Sessions	MAC Tables	IP Tables
BRIDGE	Online	Standalone	0	0	2	2	1

Manage Virtual Hub

Management of Listeners:

Listener List (TCP/IP port):

Port Number	Status
TCP 443	Listening
TCP 992	Listening
TCP 1194	Listening
TCP 5555	Listening

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

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

Management of Virtual Hub - 'BRIDGE'

Virtual Hub 'BRIDGE'

Management of Security Database:

- Manage Users
- Add, delete or edit user accounts.

Manage Groups

- Add, delete or edit groups.

Manage Access Lists

- Add or delete access lists (Packet filtering rules).

Virtual Hub Settings:

- Virtual Hub Properties
- Configure this Hub.

Authentication Server Setting

- Use external RADIUS authentication server for user authentication.

Manage Cascade Connections

- Establish Cascade Connection to Hubs on local or remote VPN Servers.

Current Status of this Virtual Hub:

Item	Value
Virtual Hub Name	BRIDGE
Status	Online
Type	Standalone
SecureNAT	Disabled
Sessions	2
Access Lists	0
Users	0
Groups	0
MAC Tables	2
IP Tables	1

Other Settings:

- Log Save Setting
- Log File List
- Configure settings of log saving function.

Trusted CA Certificates

- Manage trusted CA certificates.

Virtual NAT and Virtual DHCP Server (SecureNAT)

- Secure NAT is available on this Virtual Hub. You can run Virtual NAT and Virtual DHCP.

VPN Sessions Management:

- Manage Sessions
- Exit

Cascade Connections on BRIDGE

Cascade Connection can make a layer-2 Ethernet-level links between this Virtual Hub and other Virtual Hub which is located on either local or remote VPN Server.

Before Using Cascade Connection

⚠ Cascade Connection realizes a Layer 2 Bridge between multiple Virtual Hubs. But if the connection is incorrectly configured, an infinity loop could inadvertently be created. When using a Cascade Connection function please design the network topology with care.

Setting Name	Status	Established at	Destination VPN Server	Virtual Hub
SPNBox3000	Online (Established)	2020-03-10 (Tue) 14:15:35	61.73.149.73	SPNBOX3000

New Edit Online Offline Status Delete Rename Exit

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

New VPN Connection Setting Properties

Please configure the VPN Connection Setting for VPN Server.

Setting Name: SPNBox200_SPNBox900_Tunnel

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: 21999 Disable NAT-T

Virtual Hub Name: SPNBOX900

Proxy Server as Relay:

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

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

Cascade Connection Setting

You can configure the security policy which will be applied to the Cascade Connection on this Virtual Hub's side.

Security Policy

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: *****

Advanced Setting of Communication:

Reconnects Automatically After Disconnected

Reconnect Count: times

Reconnect Interval: seconds

Infinite Reconnects (Keep VPN Always Online)

Use SSL 3.0 (1)

Advanced Settings...

OK Cancel

VPN Gateway의 endpoint 정보 및 Virtual Hub 명 입력

Id/pass: spnuser, spnuser1234

(VPN) 장치설정																																																																																																																																																	
포드 포워딩 설정																																																																																																																																																	
장치설정		포드 포워딩 설정																																																																																																																																															
<ul style="list-style-type: none"> 네트워크 관리 무선 관리(2.4GHz) 무선 관리(5GHz) 스위치 관리 트래픽 관리 보안 기능 부가 기능 시스템 관리 		<p>소스 IP 주소: <input type="text"/></p> <p>소스 포트: <input type="text"/> ~ <input type="text"/></p> <p>외부 포트: <input type="text"/> ~ <input type="text"/></p> <p>내부 IP 주소: <input type="text"/></p> <p>내부 포트: <input type="text"/> ~ <input type="text"/></p> <p>프로토콜: TCP</p> <p>설명: <input type="text"/></p>																																																																																																																																															
<table border="1"> <thead> <tr> <th>선택</th> <th>소스IP 주소</th> <th>소스포트</th> <th>외부포트</th> <th>내부 IP 주소</th> <th>내부 포트</th> <th>프로토콜</th> <th>설명</th> <th>플래그</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>-</td> <td>443-4433</td> <td>172.30.1.37</td> <td>443-443</td> <td>TCP</td> <td>nextcloud</td> <td>KT</td> </tr> <tr> <td><input type="checkbox"/></td> <td>-</td> <td>59200-59200</td> <td>172.30.1.27</td> <td>59200-59200</td> <td>UDP</td> <td>ebay-200</td> <td>KT</td> </tr> <tr> <td><input type="checkbox"/></td> <td>-</td> <td>47147-47147</td> <td>172.30.1.14</td> <td>47147-47147</td> <td>UDP</td> <td>CSRT-1200</td> <td>KT</td> </tr> <tr> <td><input type="checkbox"/></td> <td>-</td> <td>51820-51820</td> <td>172.30.1.21</td> <td>51820-51820</td> <td>UDP</td> <td>spn</td> <td>KT</td> </tr> <tr> <td><input type="checkbox"/></td> <td>-</td> <td>59760-59760</td> <td>172.30.1.44</td> <td>59760-59760</td> <td>UDP</td> <td>spn</td> <td>KT</td> </tr> <tr> <td><input type="checkbox"/></td> <td>-</td> <td>443-443</td> <td>172.30.1.34</td> <td>443-443</td> <td>TCP</td> <td>2ipforum</td> <td>KT</td> </tr> <tr> <td><input type="checkbox"/></td> <td>-</td> <td>50600-50600</td> <td>172.30.1.45</td> <td>50600-50600</td> <td>UDP</td> <td>NFDemo-600</td> <td>KT</td> </tr> <tr> <td><input type="checkbox"/></td> <td>-</td> <td>7195-7195</td> <td>172.30.1.5</td> <td>8080-8080</td> <td>TCP</td> <td>thingsbrd</td> <td>KT</td> </tr> <tr> <td><input type="checkbox"/></td> <td>-</td> <td>57195-57195</td> <td>172.30.1.5</td> <td>57195-57195</td> <td>UDP</td> <td>spncloud</td> <td>KT</td> </tr> <tr> <td><input type="checkbox"/></td> <td>-</td> <td>59990-59990</td> <td>172.30.1.50</td> <td>59990-59990</td> <td>UDP</td> <td>spnbox900</td> <td>KT</td> </tr> <tr> <td><input type="checkbox"/></td> <td>-</td> <td>55704-55704</td> <td>172.30.1.52</td> <td>55704-55704</td> <td>TCP</td> <td>LeoOpenvpn</td> <td>KT</td> </tr> <tr> <td><input type="checkbox"/></td> <td>-</td> <td>52002-52002</td> <td>172.30.1.36</td> <td>52002-52002</td> <td>UDP</td> <td>200-08f</td> <td>KT</td> </tr> <tr> <td><input type="checkbox"/></td> <td>-</td> <td>0443-0443</td> <td>172.30.1.27</td> <td>443-443</td> <td>TCP</td> <td>L2SPN(900)</td> <td>KT</td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>-</td> <td>21999-21999</td> <td>172.30.1.57</td> <td>443-443</td> <td>TCP</td> <td>L2 SPN</td> <td>KT</td> </tr> <tr> <td><input type="checkbox"/></td> <td>-</td> <td>7777-7777</td> <td>172.30.1.112</td> <td>8080-8080</td> <td>TCP</td> <td>nyr1000</td> <td>KT</td> </tr> <tr> <td><input type="checkbox"/></td> <td>-</td> <td>51400-51400</td> <td>172.30.1.112</td> <td>51400-51400</td> <td>UDP</td> <td>spnbox1000</td> <td>KT</td> </tr> </tbody> </table>									선택	소스IP 주소	소스포트	외부포트	내부 IP 주소	내부 포트	프로토콜	설명	플래그	<input type="checkbox"/>	-	443-4433	172.30.1.37	443-443	TCP	nextcloud	KT	<input type="checkbox"/>	-	59200-59200	172.30.1.27	59200-59200	UDP	ebay-200	KT	<input type="checkbox"/>	-	47147-47147	172.30.1.14	47147-47147	UDP	CSRT-1200	KT	<input type="checkbox"/>	-	51820-51820	172.30.1.21	51820-51820	UDP	spn	KT	<input type="checkbox"/>	-	59760-59760	172.30.1.44	59760-59760	UDP	spn	KT	<input type="checkbox"/>	-	443-443	172.30.1.34	443-443	TCP	2ipforum	KT	<input type="checkbox"/>	-	50600-50600	172.30.1.45	50600-50600	UDP	NFDemo-600	KT	<input type="checkbox"/>	-	7195-7195	172.30.1.5	8080-8080	TCP	thingsbrd	KT	<input type="checkbox"/>	-	57195-57195	172.30.1.5	57195-57195	UDP	spncloud	KT	<input type="checkbox"/>	-	59990-59990	172.30.1.50	59990-59990	UDP	spnbox900	KT	<input type="checkbox"/>	-	55704-55704	172.30.1.52	55704-55704	TCP	LeoOpenvpn	KT	<input type="checkbox"/>	-	52002-52002	172.30.1.36	52002-52002	UDP	200-08f	KT	<input type="checkbox"/>	-	0443-0443	172.30.1.27	443-443	TCP	L2SPN(900)	KT	<input checked="" type="checkbox"/>	-	21999-21999	172.30.1.57	443-443	TCP	L2 SPN	KT	<input type="checkbox"/>	-	7777-7777	172.30.1.112	8080-8080	TCP	nyr1000	KT	<input type="checkbox"/>	-	51400-51400	172.30.1.112	51400-51400	UDP	spnbox1000	KT
선택	소스IP 주소	소스포트	외부포트	내부 IP 주소	내부 포트	프로토콜	설명	플래그																																																																																																																																									
<input type="checkbox"/>	-	443-4433	172.30.1.37	443-443	TCP	nextcloud	KT																																																																																																																																										
<input type="checkbox"/>	-	59200-59200	172.30.1.27	59200-59200	UDP	ebay-200	KT																																																																																																																																										
<input type="checkbox"/>	-	47147-47147	172.30.1.14	47147-47147	UDP	CSRT-1200	KT																																																																																																																																										
<input type="checkbox"/>	-	51820-51820	172.30.1.21	51820-51820	UDP	spn	KT																																																																																																																																										
<input type="checkbox"/>	-	59760-59760	172.30.1.44	59760-59760	UDP	spn	KT																																																																																																																																										
<input type="checkbox"/>	-	443-443	172.30.1.34	443-443	TCP	2ipforum	KT																																																																																																																																										
<input type="checkbox"/>	-	50600-50600	172.30.1.45	50600-50600	UDP	NFDemo-600	KT																																																																																																																																										
<input type="checkbox"/>	-	7195-7195	172.30.1.5	8080-8080	TCP	thingsbrd	KT																																																																																																																																										
<input type="checkbox"/>	-	57195-57195	172.30.1.5	57195-57195	UDP	spncloud	KT																																																																																																																																										
<input type="checkbox"/>	-	59990-59990	172.30.1.50	59990-59990	UDP	spnbox900	KT																																																																																																																																										
<input type="checkbox"/>	-	55704-55704	172.30.1.52	55704-55704	TCP	LeoOpenvpn	KT																																																																																																																																										
<input type="checkbox"/>	-	52002-52002	172.30.1.36	52002-52002	UDP	200-08f	KT																																																																																																																																										
<input type="checkbox"/>	-	0443-0443	172.30.1.27	443-443	TCP	L2SPN(900)	KT																																																																																																																																										
<input checked="" type="checkbox"/>	-	21999-21999	172.30.1.57	443-443	TCP	L2 SPN	KT																																																																																																																																										
<input type="checkbox"/>	-	7777-7777	172.30.1.112	8080-8080	TCP	nyr1000	KT																																																																																																																																										
<input type="checkbox"/>	-	51400-51400	172.30.1.112	51400-51400	UDP	spnbox1000	KT																																																																																																																																										
<input type="button" value="삭제"/> <input type="button" value="삭제"/>																																																																																																																																																	

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

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

Cascade Connections on BRIDGE

Cascade Connection can make a layer-2 Ethernet-level links between this Virtual Hub and other Virtual Hub which is located on either local or remote VPN Server.

Before Using Cascade Connection

! Cascade Connection realizes a Layer 2 Bridge between multiple Virtual Hubs. But if the connection is incorrectly configured, an infinity loop could inadvertently be created. When using a Cascade Connection function please design the network topology with care.

Setting Name	Status	Established at	Destination VPN Server	Virtual Hub
SPNBox3000	Online (Established)	2020-03-10 (Tue) 14:15:35	61.73.149.73	SPNBOX3000
SPNBox200_SPNBo...	Offline (Stopped)	(None)	121.162.94.203	SPNBOX900

< >

New Edit **Online** Offline Status Delete Rename Exit

Cascade Connections on BRIDGE

Cascade Connection can make a layer-2 Ethernet-level links between this Virtual Hub and other Virtual Hub which is located on either local or remote VPN Server.

Before Using Cascade Connection

! Cascade Connection realizes a Layer 2 Bridge between multiple Virtual Hubs. But if the connection is incorrectly configured, an infinity loop could inadvertently be created. When using a Cascade Connection function please design the network topology with care.

Setting Name	Status	Established at	Destination VPN Server	Virtual Hub
SPNBox3000	Online (Established)	2020-03-10 (Tue) 14:15:35	61.73.149.73	SPNBOX3000
SPNBox200_SPNBo...	Online (Established)	2020-03-10 (Tue) 14:42:54	121.162.94.203	SPNBOX900

< >

New Edit Offline Status **Online** Delete Rename **Exit**

VPN Tunnel(VPN Bridge ⇄ VPN Gateway) 연결 성공

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

SPNBox200(Bridge) - SoftEther VPN Server Manager

Manage VPN Bridge "172.30.1.6"

Virtual Hub Name	Status	Type	Users	Groups	Sessions	MAC Tables	IP Tables
BRIDGE	Online	Standalone	0	0	2	2	1

Manage Virtual Hub (highlighted with a red box)

Management of Listeners:

Port Number	Status	Action
TCP 443	Listening	Create
TCP 992	Listening	Delete
TCP 1194	Listening	Start
TCP 5555	Listening	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

Management of Virtual Hub - 'BRIDGE'

Virtual Hub 'BRIDGE'

Current Status of this Virtual Hub:

Item	Value
Virtual Hub Name	BRIDGE
Status	Online
Type	Standalone
SecureNAT	Disabled
Sessions	2
Access Lists	0
Users	0
Groups	0
MAC Tables	2
IP Tables	1

Refresh

Other Settings:

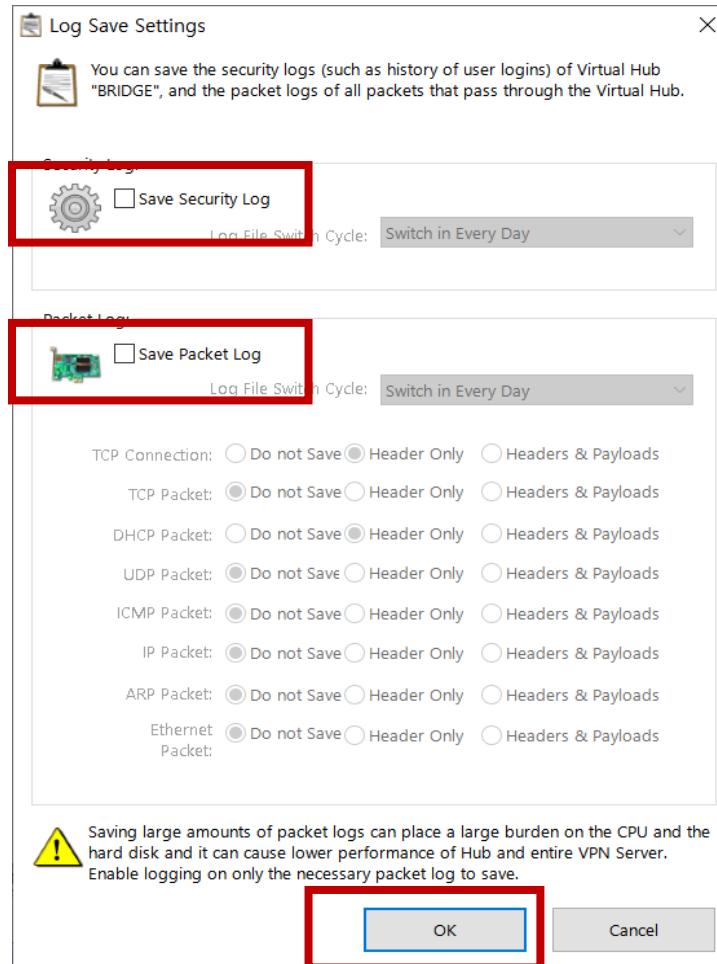
- Log Save Setting (highlighted with a red box)
- Log File List
- Configure settings of log saving function.
- Trusted CA Certificates
- Revoked Certs
- Manage trusted CA certificates.
- Virtual NAT and Virtual DHCP Server (SecureNAT)
- Secure NAT is available on this Virtual Hub. You can run Virtual NAT and Virtual DHCP.

VPN Sessions Management:

- Manage Sessions

Exit

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



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

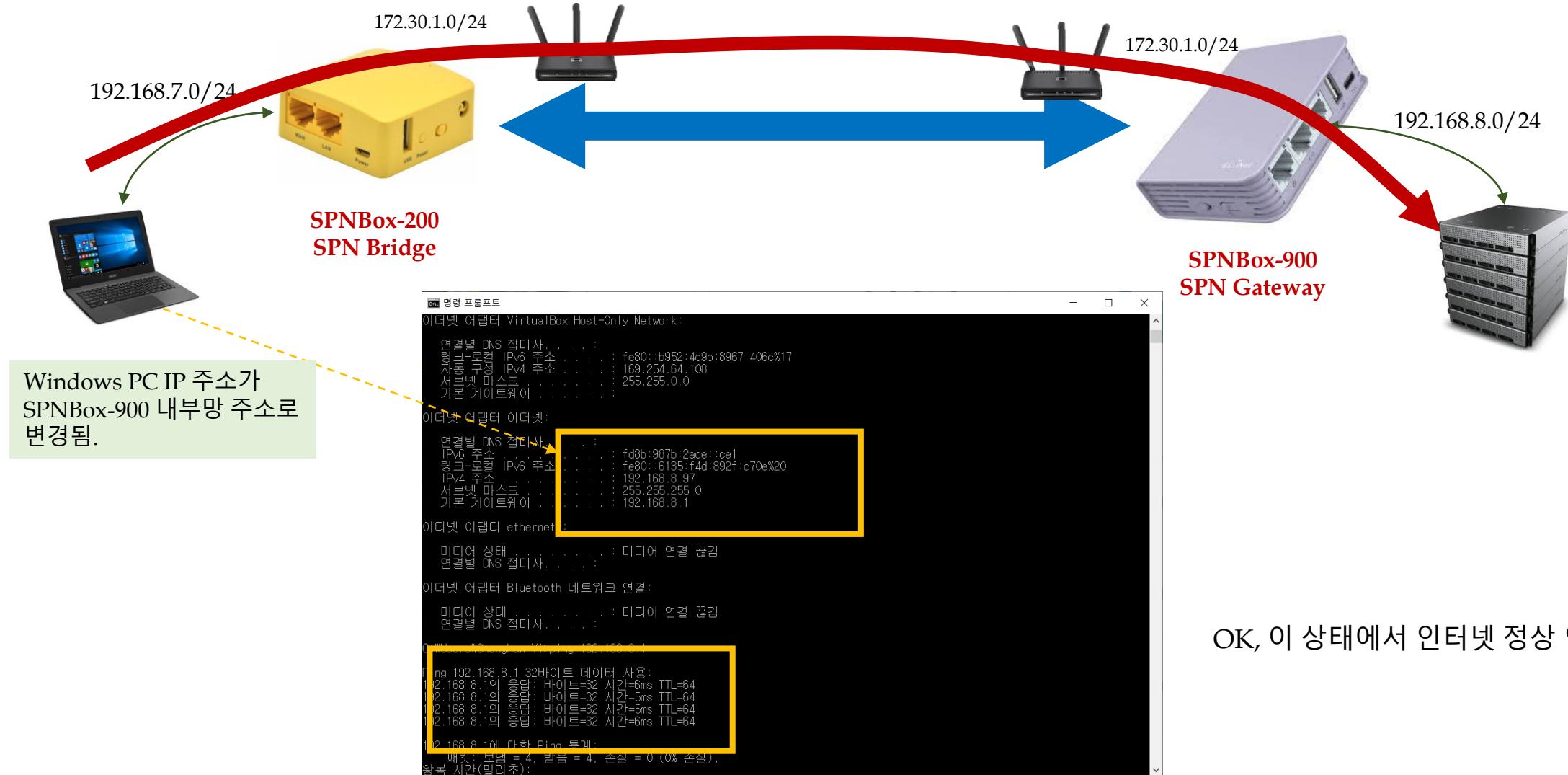
3. SPN Gateway & Bridge(3) - Bridge 설정(12)

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

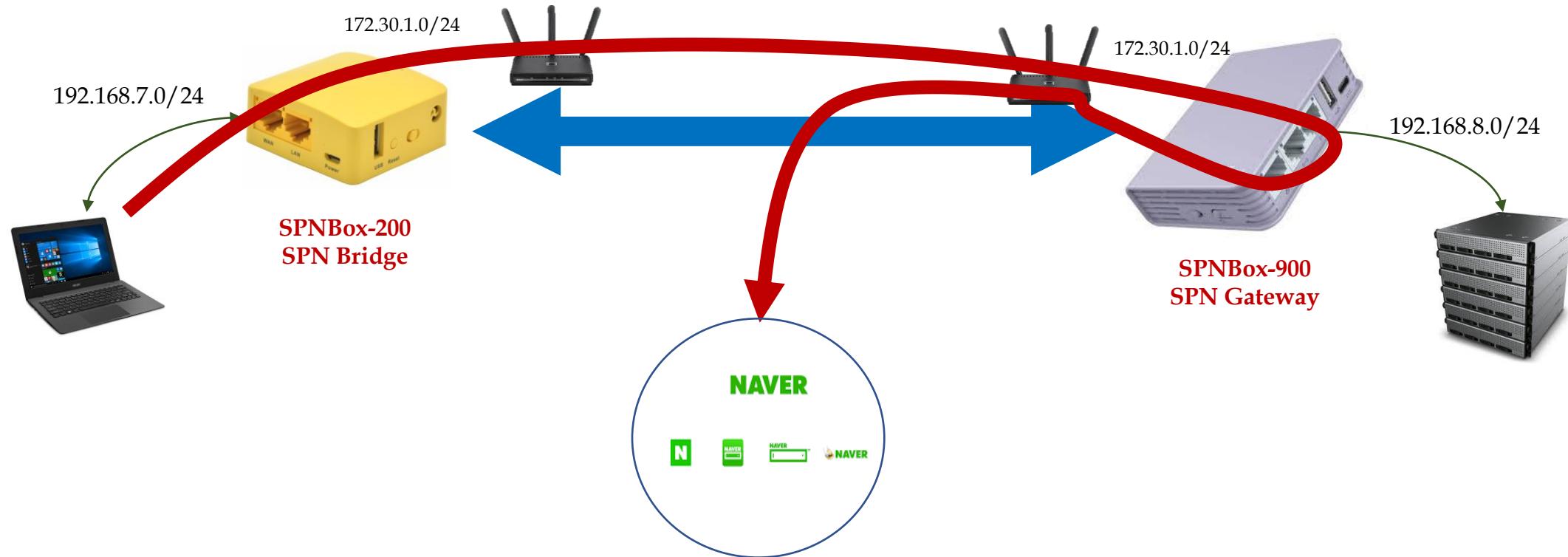
<참고>

- 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)



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

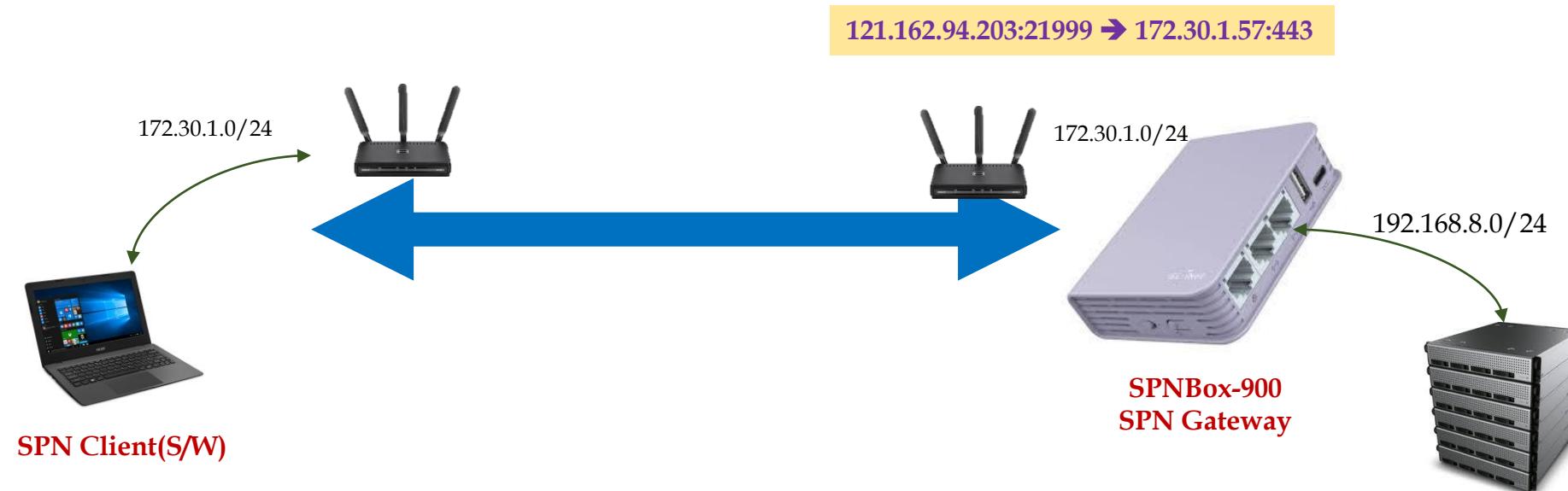


참고: L2 SPN을 사용하여 인터넷을 접속할 경우, 위와 같이 패킷이 SPN Gateway를 경유하게 된다(느리다).
해법 1: 인터넷 접속이 목적이라면 Home AP에 직접 붙으면 된다.

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) 버전을 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 Setting ... 선택
(Ct+G + N)

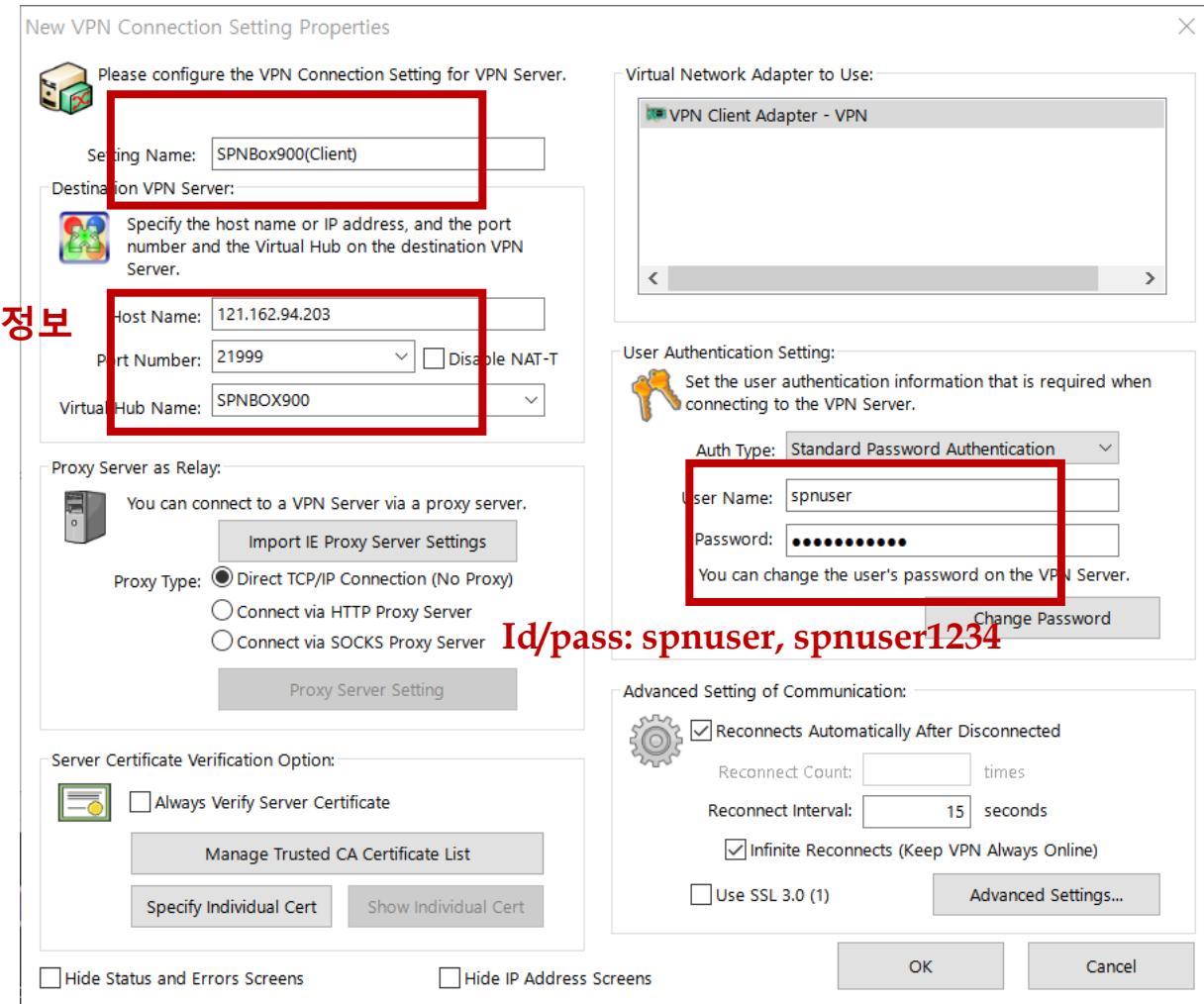
VPN Connection Setting Name	Status	VPN Server Hostname	Virtual Hub	Virtual Network Ad...
Add VPN Connection	Offline	121.162.94.19 (Direct TCP/IP Connection)	HUB1	VPN
ESBIN	Offline	61.73.149.96 (Direct TCP/IP Connection)	VPN1	VPN
GL_AR300M	Offline	121.162.94.203 (Direct TCP/IP Connection)	SPNBOX900	VPN
MV1000_James	Offline	61.73.149.96 (Direct TCP/IP Connection)	SPNBOX1	VPN
SPNBox-C1037	Offline	61.73.149.96 (Direct TCP/IP Connection)	SPNBOX1400	VPN
SPNBox1400	Offline	61.73.149.96 (Direct TCP/IP Connection)	VPN1	VPN
X750	Offline	61.73.149.96 (Direct TCP/IP Connection)		

Virtual Network Adapter Name	Status	MAC Address	Version
VPN Client Adapter - VPN	Enabled	5E-34-21-FB-5F-F6	4.25.0.9658

SoftEther VPN Client Manager Not Connected SoftEther VPN Client Build 9680

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

VPN Gateway의 endpoint 정보



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

SoftEther VPN Client Manager

Connect Edit View Virtual Adapter Smart Card Tools Help

VPN Connection Setting Name	Status	VPN Server Hostname	Virtual Hub	Virtual Network Ad...
Add VPN Connection				
ESBIN	Offline	121.162.94.19 (Direct TCP/IP Connection)	HUB1	VPN
GL_AR300M	Offline	61.73.149.96 (Direct TCP/IP Connection)	VPN1	VPN
MV1000_James	Offline	121.162.94.203 (Direct TCP/IP Connection)	SPNBOX900	VPN
SPNBox-C1037	Offline	61.73.149.96 (Direct TCP/IP Connection)	SPNBOX1	VPN
SPNBox1400	Offline	61.73.149.96 (Direct TCP/IP Connection)	SPNBOX1400	VPN
X750	Offline	61.73.149.96 (Direct TCP/IP Connection)	VPN1	VPN
SPNBox900(Client)	Connected	121.162.94.203 (Direct TCP/IP Connection)	SPNBOX900	VPN

1) 오른쪽 마우스 클릭 후, Connect 선택

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

Network Adapter Name	Status	MAC Address	Version
Client Adapter - VPN	Enabled	5E-34-21-FB-5F-F6	4.25.0.9658

SoftEther VPN Client Manager

1 VPN Sessions

SoftEther VPN Client Build 9680

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)

```
C:\Users\Chunghan Yi>
C:\Users\Chunghan Yi>
C:\Users\Chunghan Yi>
C:\Users\Chunghan Yi>ipconfig

Windows IP 구성

알 수 없는 어댑터 VPN - VPN Client:
  연결별 DNS 접미사 . . . . . : 
  링크-로컬 IPv6 주소 . . . . . : fe80::e512:fe76:533b:d01%13
  IPv4 주소 . . . . . : 192.168.8.67
  서브넷 마스크 . . . . . : 255.255.255.0
  기본 게이트웨이 . . . . . : 192.168.8.1

이더넷 어댑터 VirtualBox Host-Only Network:
  연결별 DNS 접미사 . . . . . : 
  링크-로컬 IPv6 주소 . . . . . : fe80::b952:4c9b:8967:406c%17
  자동 구성 IPv4 주소 . . . . . : 169.254.64.108
  서브넷 마스크 . . . . . : 255.255.0.0
  기본 게이트웨이 . . . . . : 

무선 LAN 어댑터 로컬 영역 연결* 5:
  미디어 상태 . . . . . : 미디어 연결 끊김
  연결별 DNS 접미사 . . . . . : 

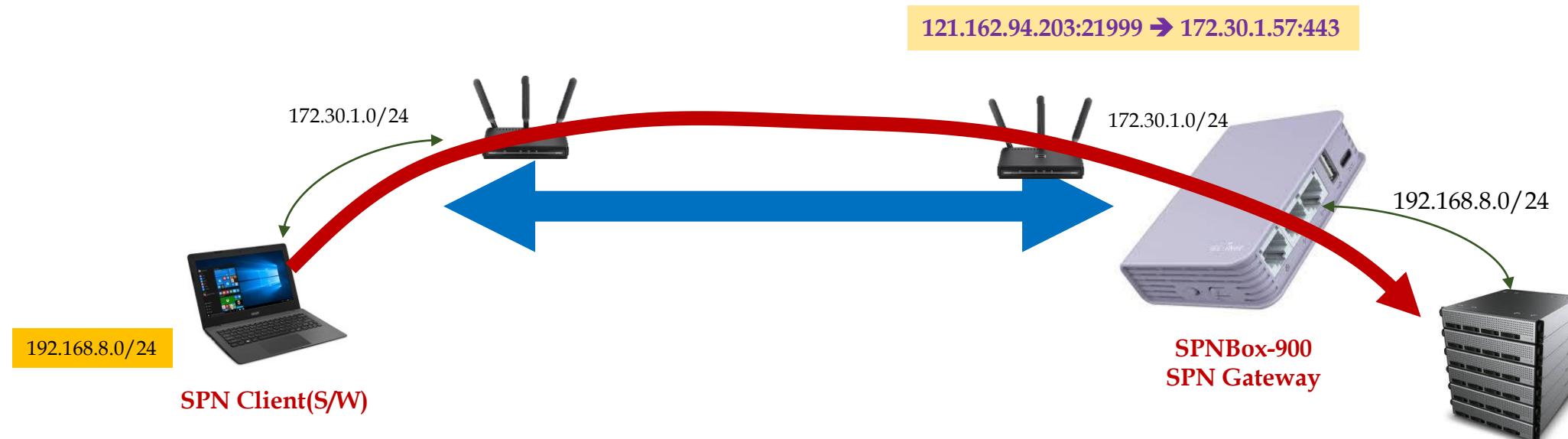
무선 LAN 어댑터 로컬 영역 연결* 7:
  미디어 상태 . . . . . : 미디어 연결 끊김
  연결별 DNS 접미사 . . . . . : 

이더넷 어댑터 ethernet2:
  미디어 상태 . . . . . : 미디어 연결 끊김
  연결별 DNS 접미사 . . . . . : 
```

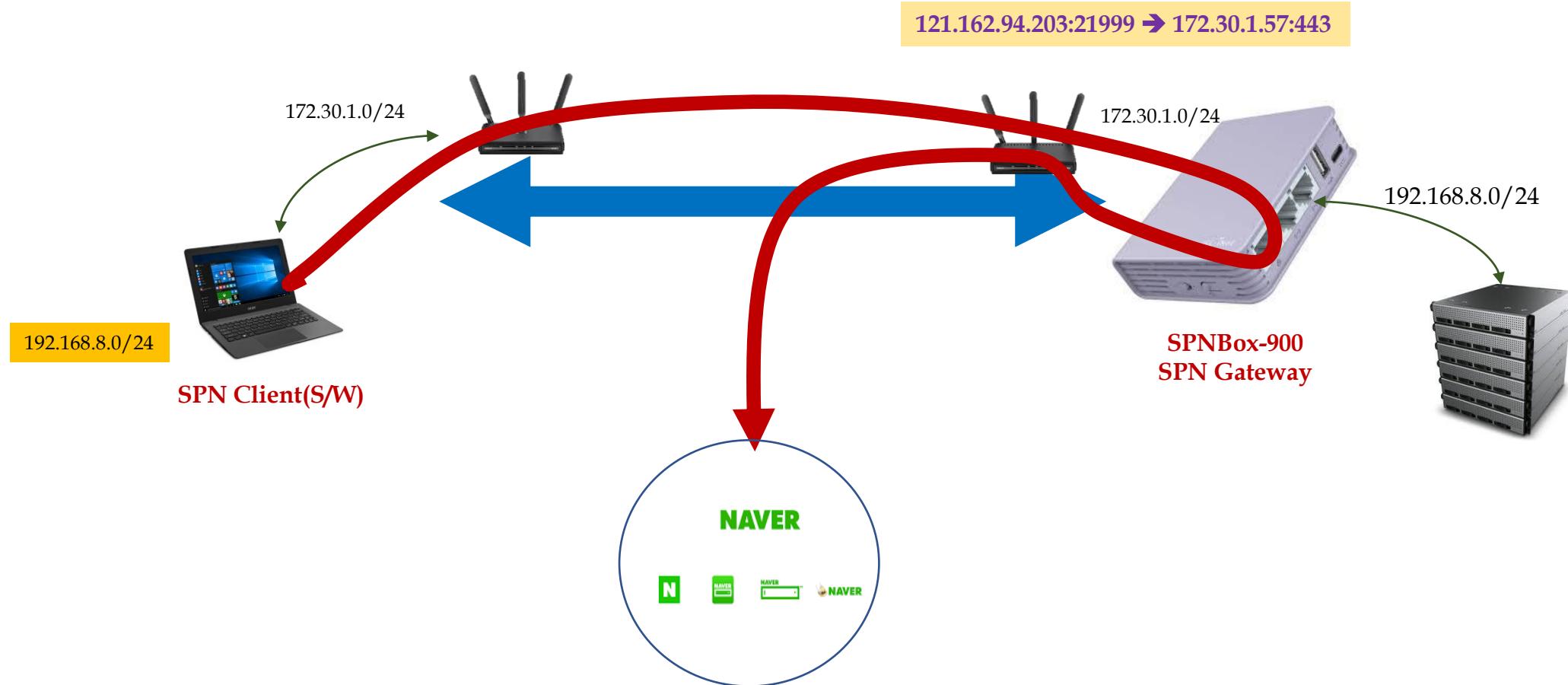
Windows PC IP 주소가
SPNBox-900 내부망 주소로
변경됨.

OK, 이 상태에서 인터넷 정상 연결

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



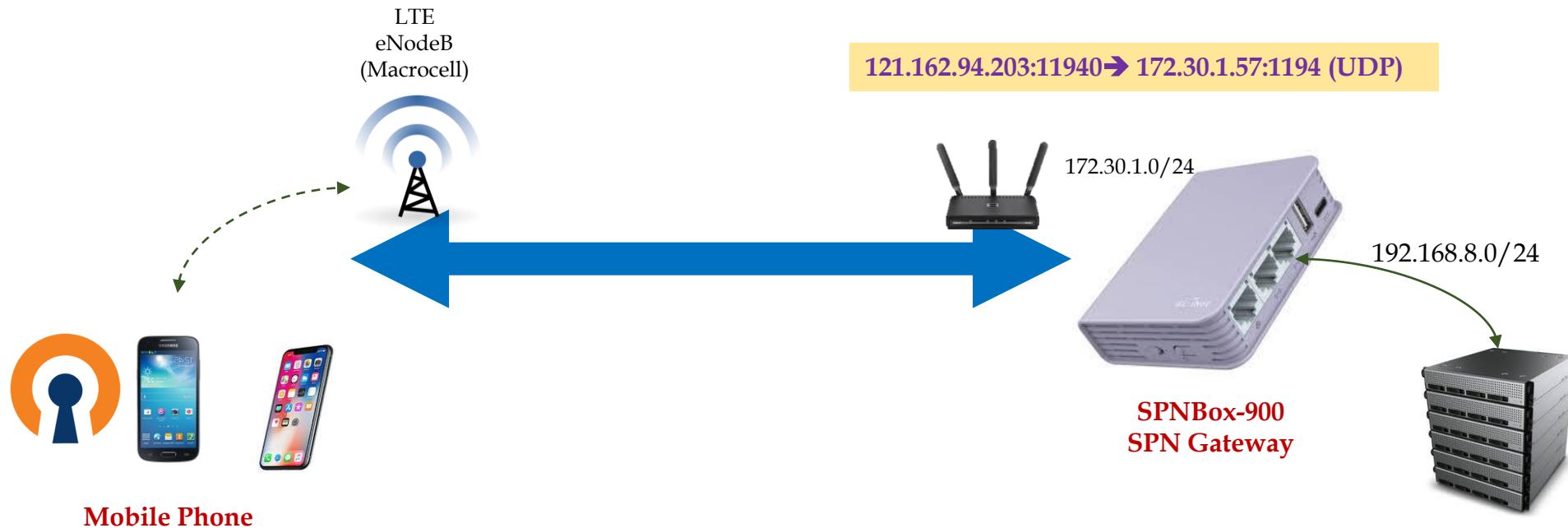
4. SPN Gateway & Client(3) - VPN 연결 시험(3)



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)



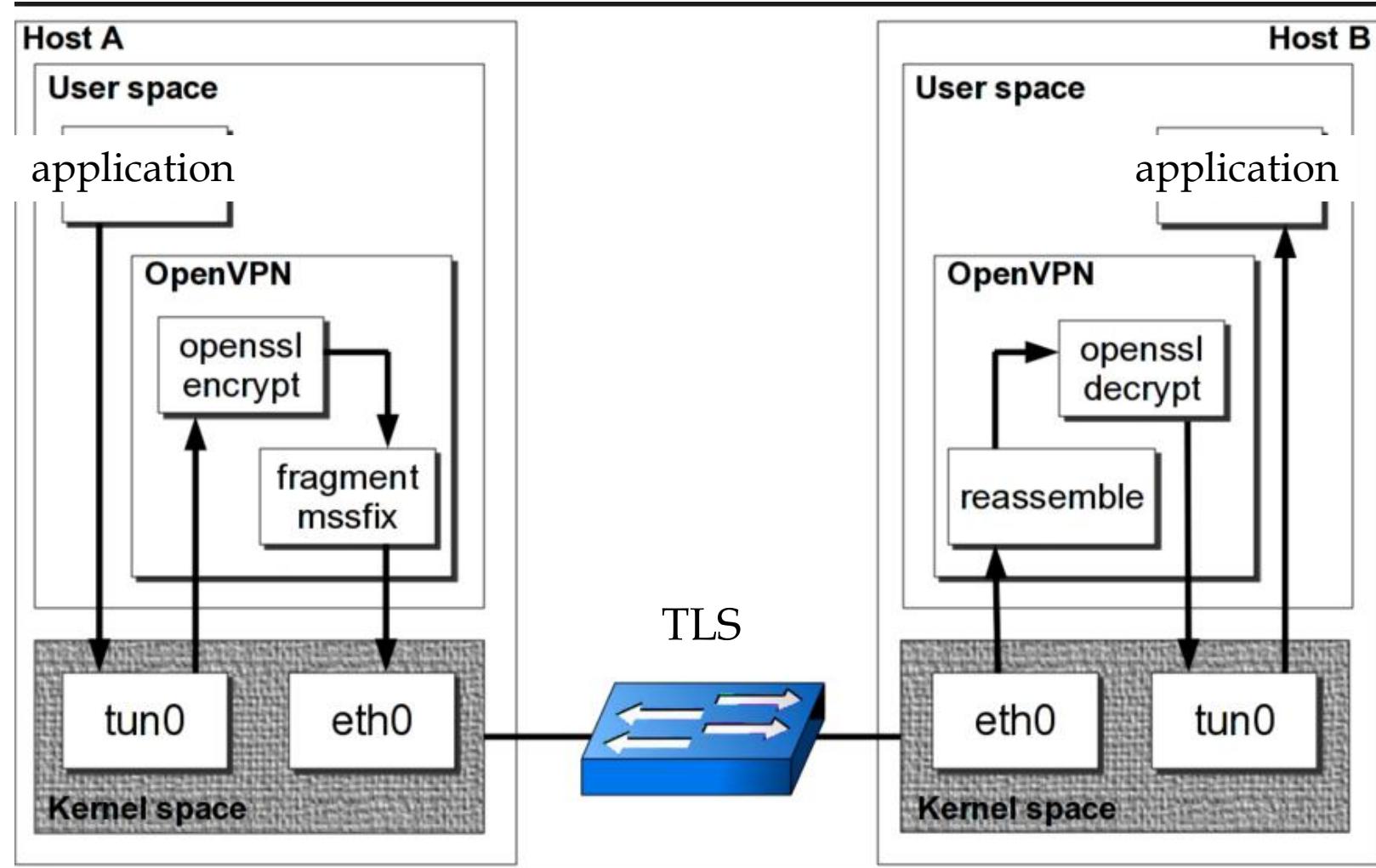
이 장에서는 위의 네트워크(테스트베드) 환경에서 VPN 연결 시험을 진행하도록 하겠습니다.
SPN Gateway는 OpenVPN, L2TP/IPsec Clone 서버 기능을 제공합니다.

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

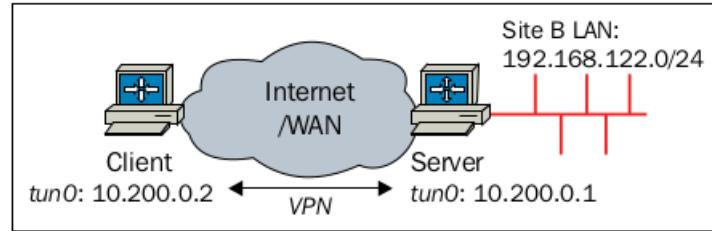
SPN Gateway	전체 설정 절차 요약
a)	VPN Server를 구동시키고, vpncmd(CLI: se vcmd run 명령)로 admin password를 설정한다(SPNBox CLI에서 수행)
b)	Windows PC에서 VPN Server Manager로 VPN Server에 접속한 후, 가장 기본적인 서버 설정(local ip address, port, admin password 입력)을 한다.
c)	Virtual Hub을 하나 추가한다. Default Virtual Hub을 사용해도 됨.
d)	Virtual Hub 사용을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

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

Server's config

```
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
```

SPN Gateway는 OpenVPN Clone 서버 기능을 제공합니다.

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

Manage VPN Server "172.30.1.127"

Virtual Hub Name	Status	Type	Users	Groups	Sessions	MAC Tables	IP Tables
DEFAULT	Online	Standalone	0	0	0	0	0
SPNBOX3000	Online	Standalone	1	0	3	4	6

Management of Listeners:

Port Number	Status
TCP 443	Listening
TCP 992	Listening
TCP 1194	Listening
TCP 5555	Listening

Buttons: Manage Virtual Hub, Online, Offline, View Status, Create a Virtual Hub, Properties, Delete.

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
- OpenVPN / MS-SSTP Setting

Buttons: Local Bridge Setting, Layer 3 Switch Setting, IPsec / L2TP Setting, Dynamic DNS Setting, VPN Azure, VPN Azure Setting.

여기서 생성한 ovpn 파일을 mobile phone에 설치하면 됨.

OpenVPN / MS-SSTP Settings

OpenVPN / MS-SSTP VPN Clone Server Function Settings

OpenVPN Clone Server Function
This VPN Server has the clone functions of OpenVPN software products by OpenVPN Technologies, Inc.

Any OpenVPN Clients can connect to this VPN Server.

Enable OpenVPN Clone Server Function

UDP Ports to Listen for OpenVPN:
1194

Multiple UDP ports can be specified with splitting by space or comma letters.
OpenVPN Server Function also runs on TCP port. Any TCP ports which are defined as listeners on the VPN Server accepts OpenVPN Protocol respectively and equally.

ovpn(OpenVPN client profile) 파일 생성

Sample File Generating Tool for OpenVPN Clients
Making a OpenVPN Client configuration file is a very difficult job. You can use this tool to generate an appropriate OpenVPN Client configuration file. The generated configuration sample can be used immediately.

Microsoft SSTP VPN Clone Server Function
This VPN Server has the clone functions of MS-SSTP VPN Server which is on Windows Server 2008 / 2012 by Microsoft Corporation. Built-in MS-SSTP clients on Windows Vista / 7 / 8 / RT / 10 can connect to this VPN Server.

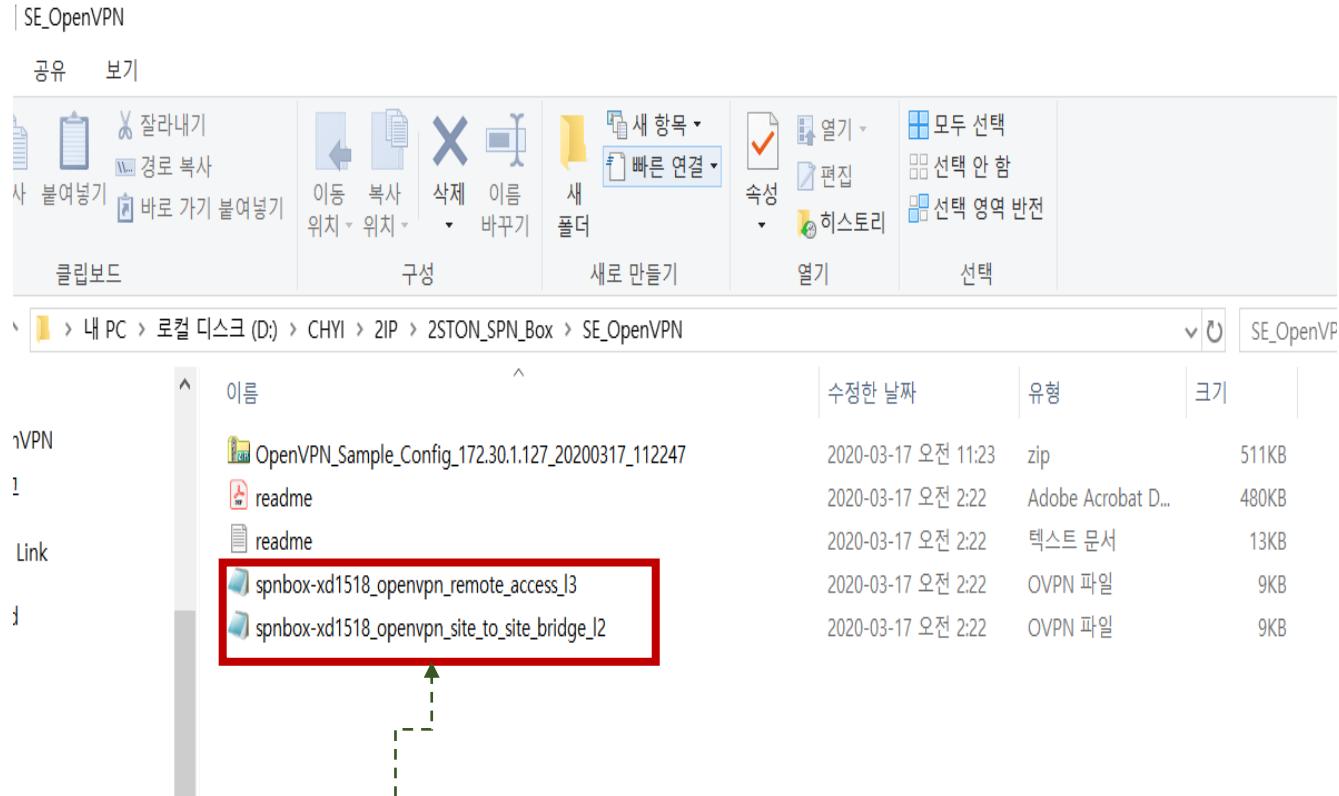
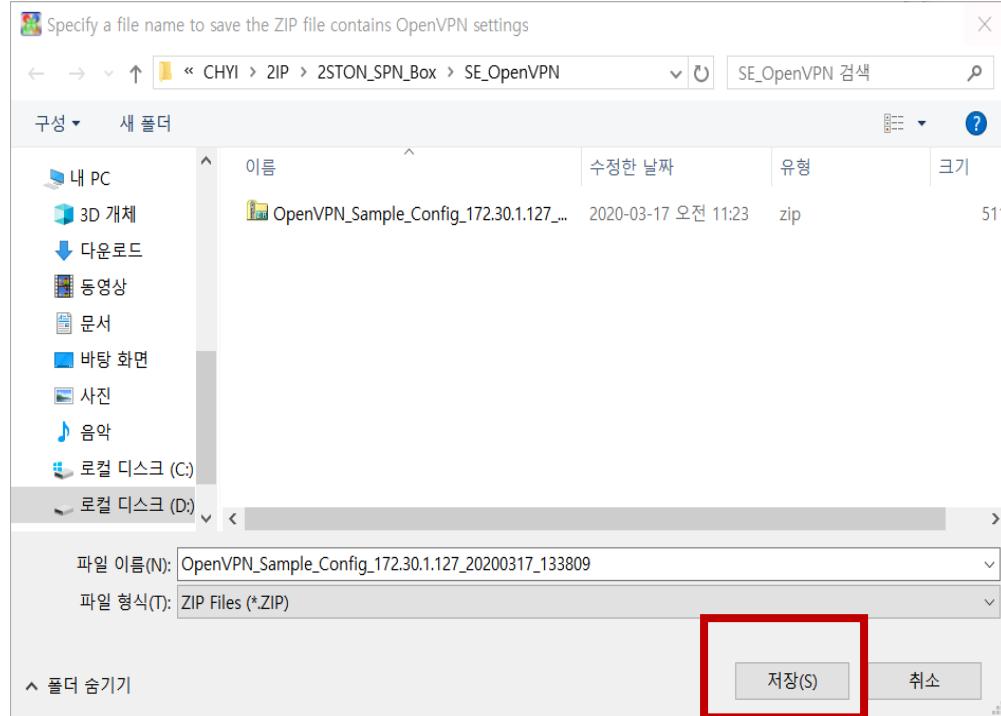
Enable MS-SSTP VPN Clone Server Function

The value of CN (Common Name) on the SSL certificate of VPN Server must match to the hostname specified on the client, and that certificate must be in the trusted list on the client. For details refer the Microsoft's documents.

The manner to specify a username to connect to the Virtual Hub, and the selection rule of default Hub by using these clone server functions are same to the IPsec Server functions.

Buttons: IPsec Server Configuration, OK, Cancel.

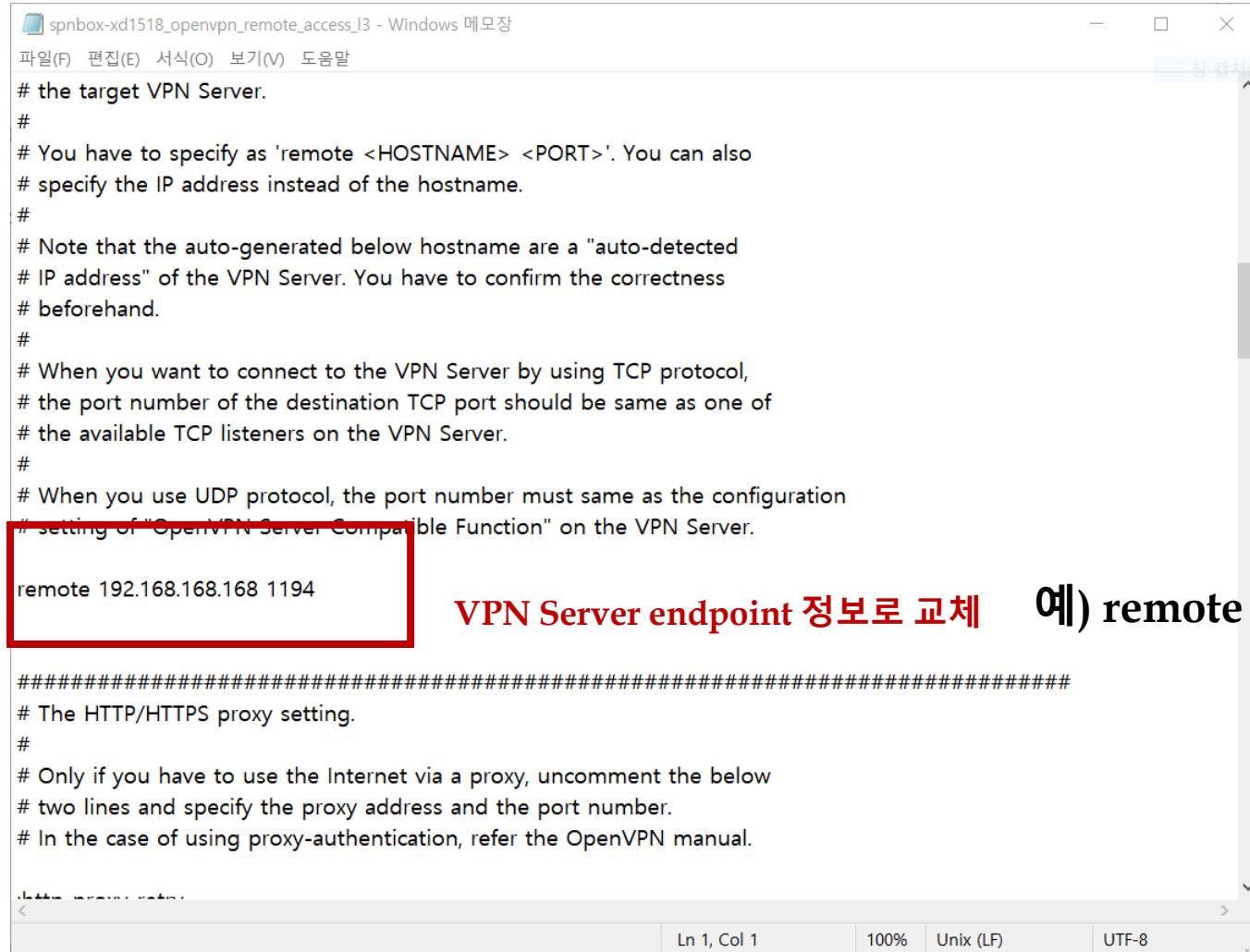
5. SPN Gateway & Mobile Phone(3) - Gateway 설정(2)



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.

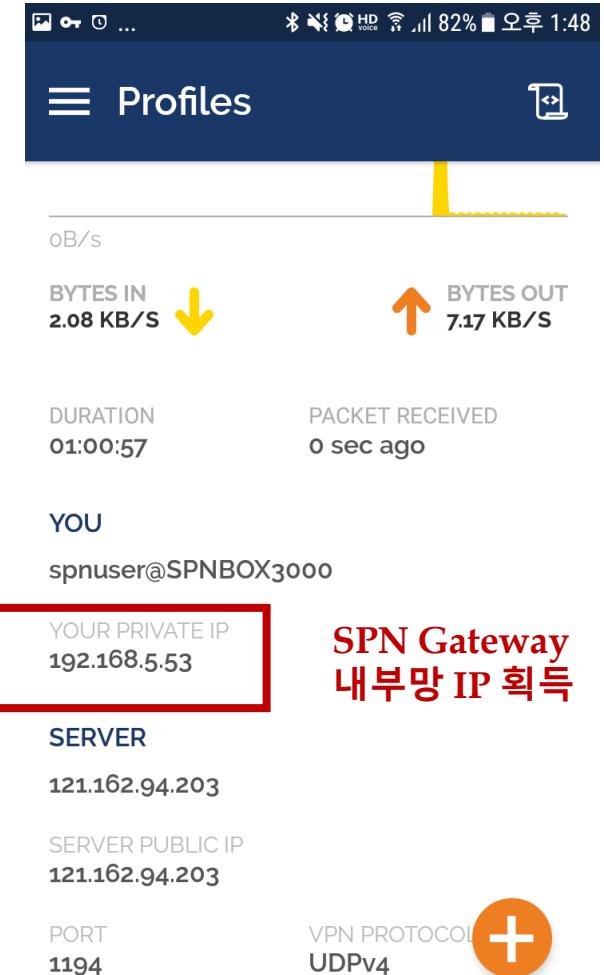
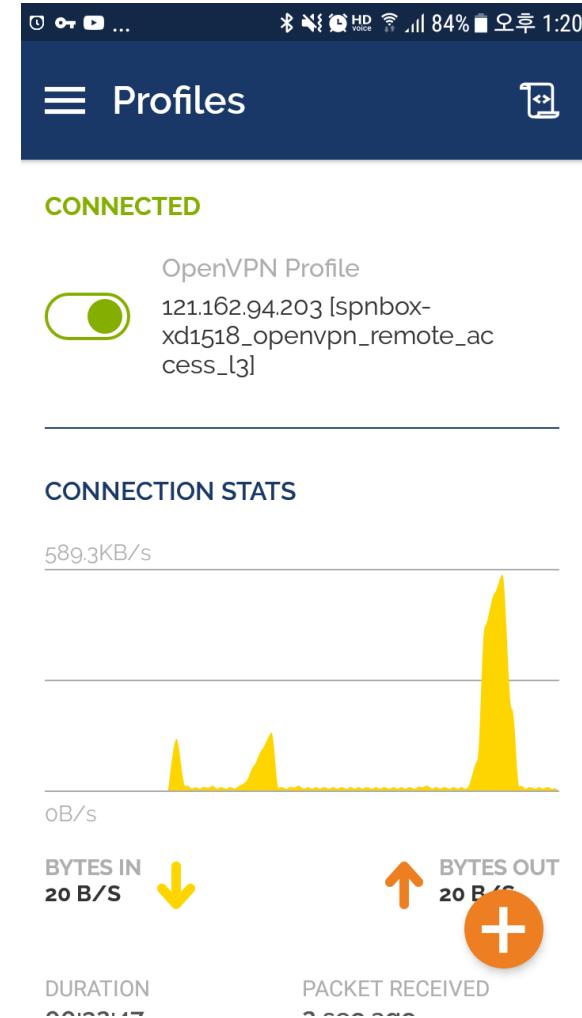
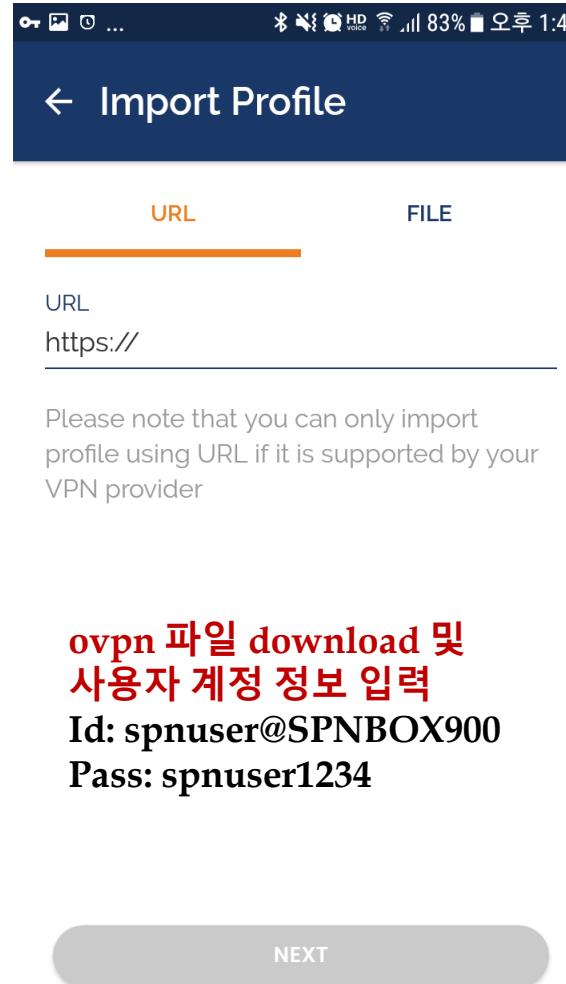
5. SPN Gateway & Mobile Phone(3) - Gateway 설정(3)



The screenshot shows a Windows Notepad window titled "spnbox-xd1518_openvpn_remote_access_3 - Windows 메모장". The content of the file is an OpenVPN configuration script. A red box highlights the line "remote 192.168.168.168 1194", which is the VPN server endpoint. To the right of this highlighted line, the text "VPN Server endpoint 정보로 교체 예) remote 121.162.94.203 1940" is displayed in red, indicating that the user should replace the highlighted line with their own endpoint information.

```
# the target VPN Server.  
#  
# You have to specify as 'remote <HOSTNAME> <PORT>'. You can also  
# specify the IP address instead of the hostname.  
#  
# Note that the auto-generated below hostname are a "auto-detected  
# IP address" of the VPN Server. You have to confirm the correctness  
# beforehand.  
#  
# When you want to connect to the VPN Server by using TCP protocol,  
# the port number of the destination TCP port should be same as one of  
# the available TCP listeners on the VPN Server.  
#  
# When you use UDP protocol, the port number must same as the configuration  
# setting of "OpenVPN Server Compatible Function" on the VPN Server.  
  
remote 192.168.168.168 1194  
  
#####  
# The HTTP/HTTPS proxy setting.  
#  
# Only if you have to use the Internet via a proxy, uncomment the below  
# two lines and specify the proxy address and the port number.  
# In the case of using proxy-authentication, refer the OpenVPN manual.  
  
#<>  
Ln 1, Col 1 100% Unix (LF) UTF-8
```

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



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

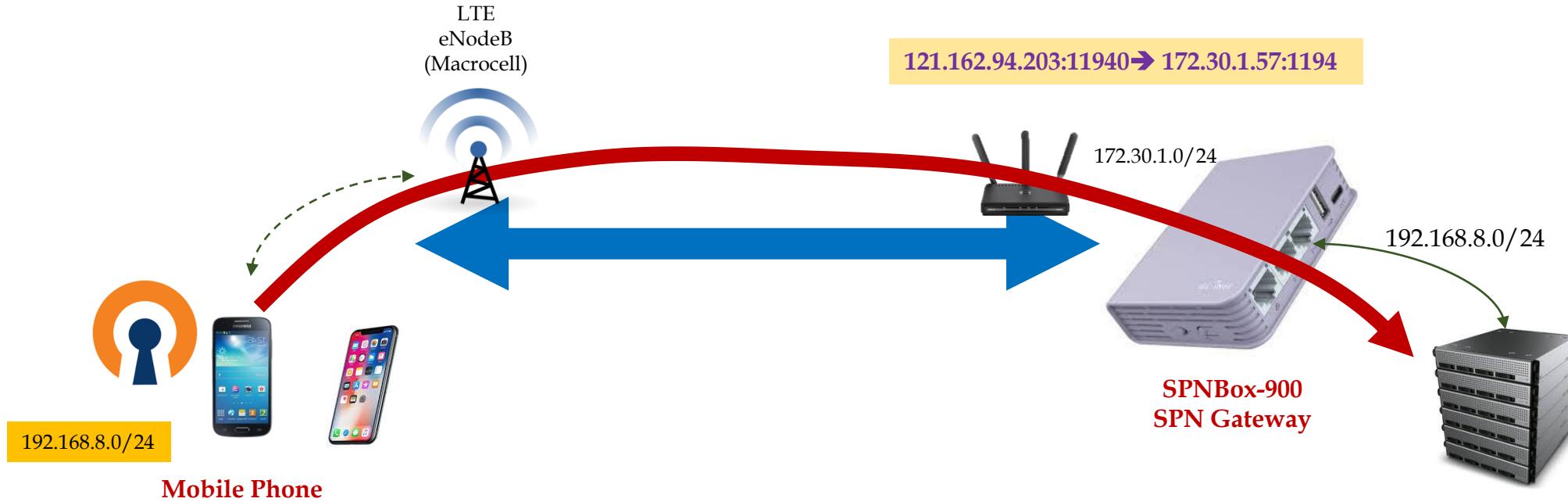
5. SPN Gateway & Mobile Phone(4) - OpenVPN 설정(2)

- 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, import 해 주면 된다.*

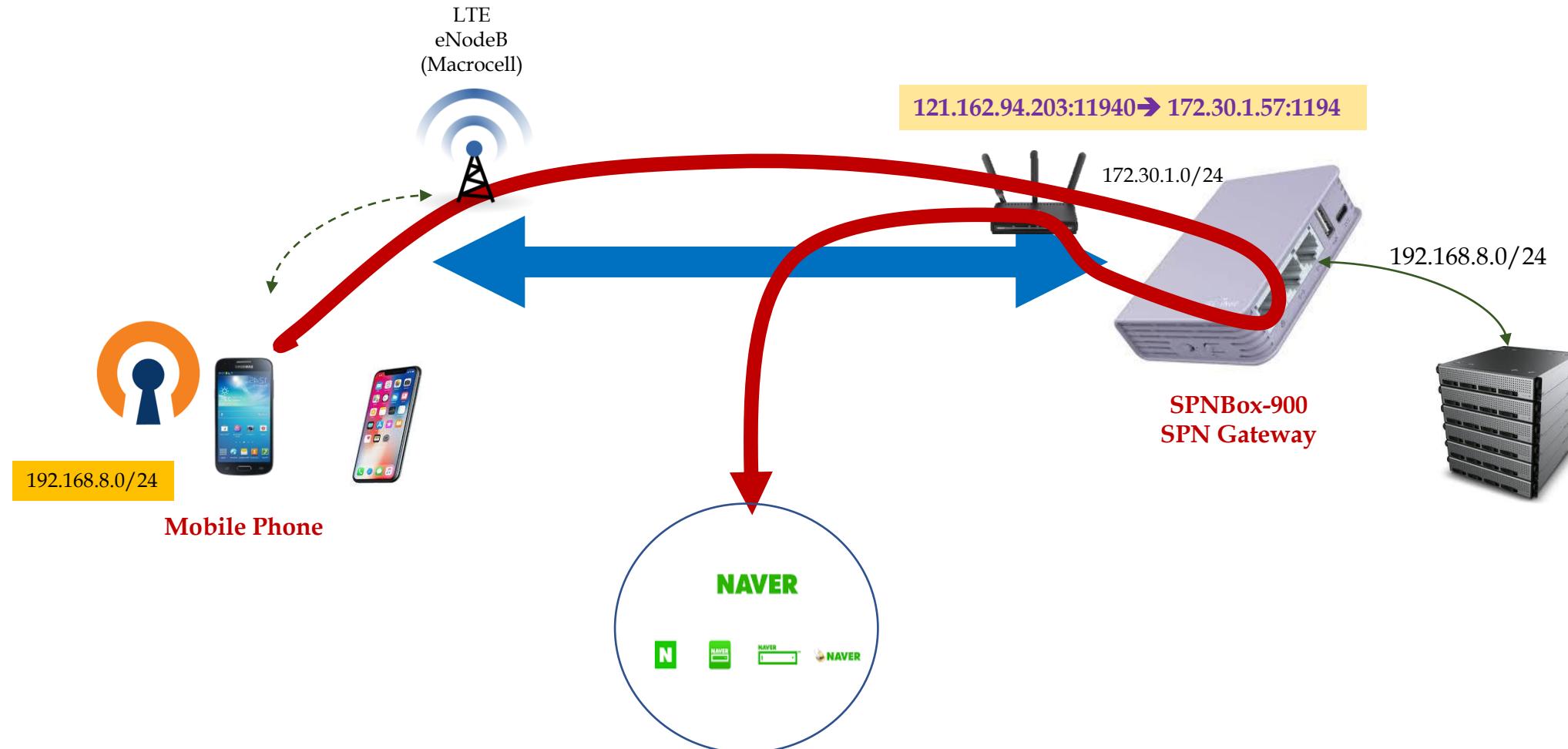
```
chyi@mars:~/workspace/test/03172020$ sudo adb push ./spnbox-xd1518_openvpn_remote_access_l3.ovpn /storage/emulated/0/Music  
./spnbox-xd1518_openvpn_remote_access_l3.ovpn: 1 file pushed. 0.4 MB/s (9085 bytes in 0.025s)
```

- 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)

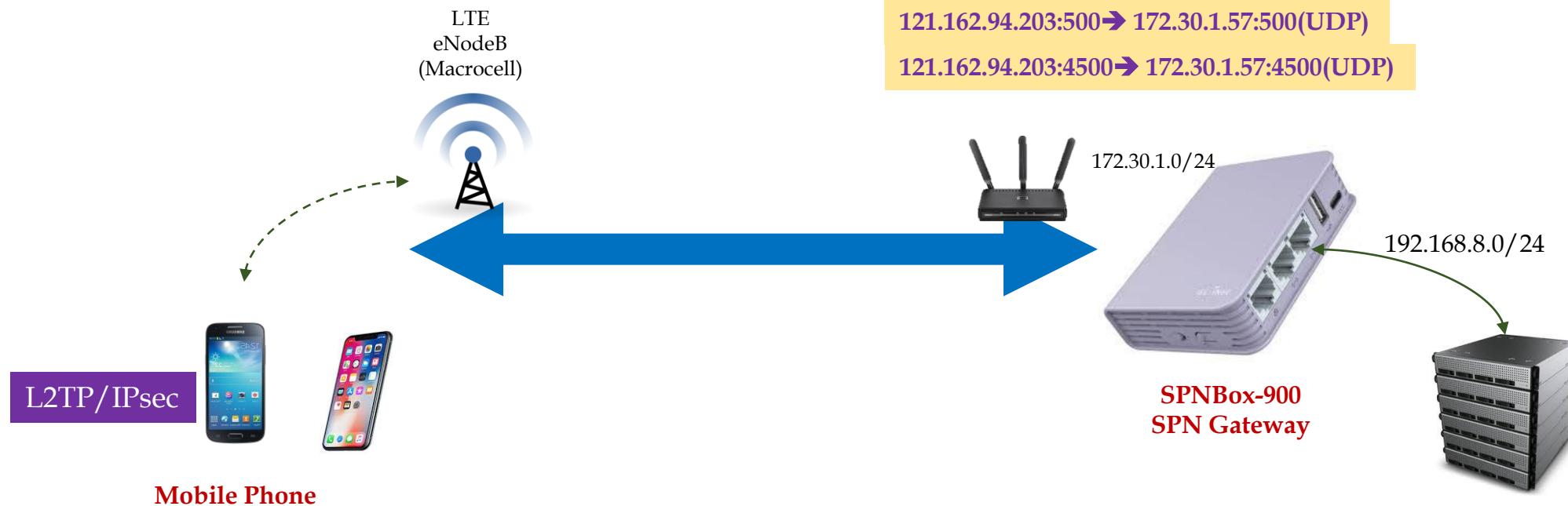


6. SPN Gateway & Mobile Phone 2 : L2TP/IPsec Setup Guide

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.

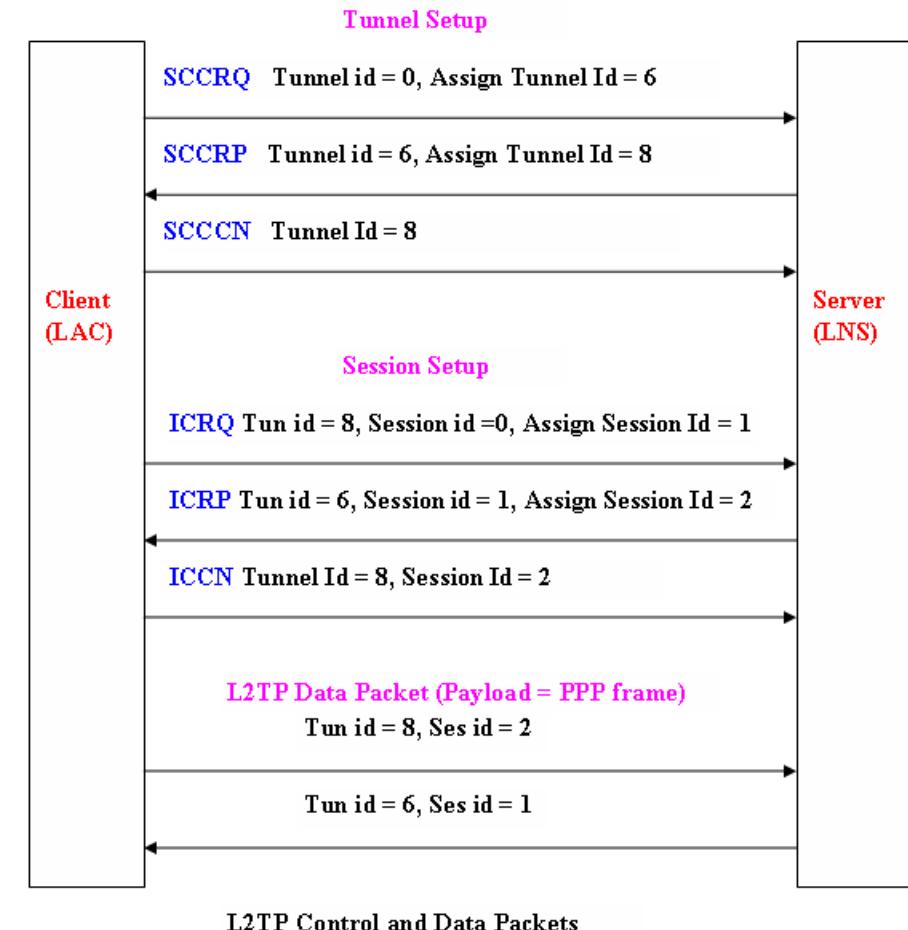
L2TP는 일부 방화벽이 차단하는 것으로 알려진 UDP 포트 500을 사용하기 때문에 때때로 방화벽 관련 문제를 겪을 수 있습니다.

장점

✓ PPTP보다 안전함

단점

- ✗ OpenVPN보다 느림
- ✗ 때때로 방화벽에 의해 차단됨



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

Benefits of L2TP VPN?

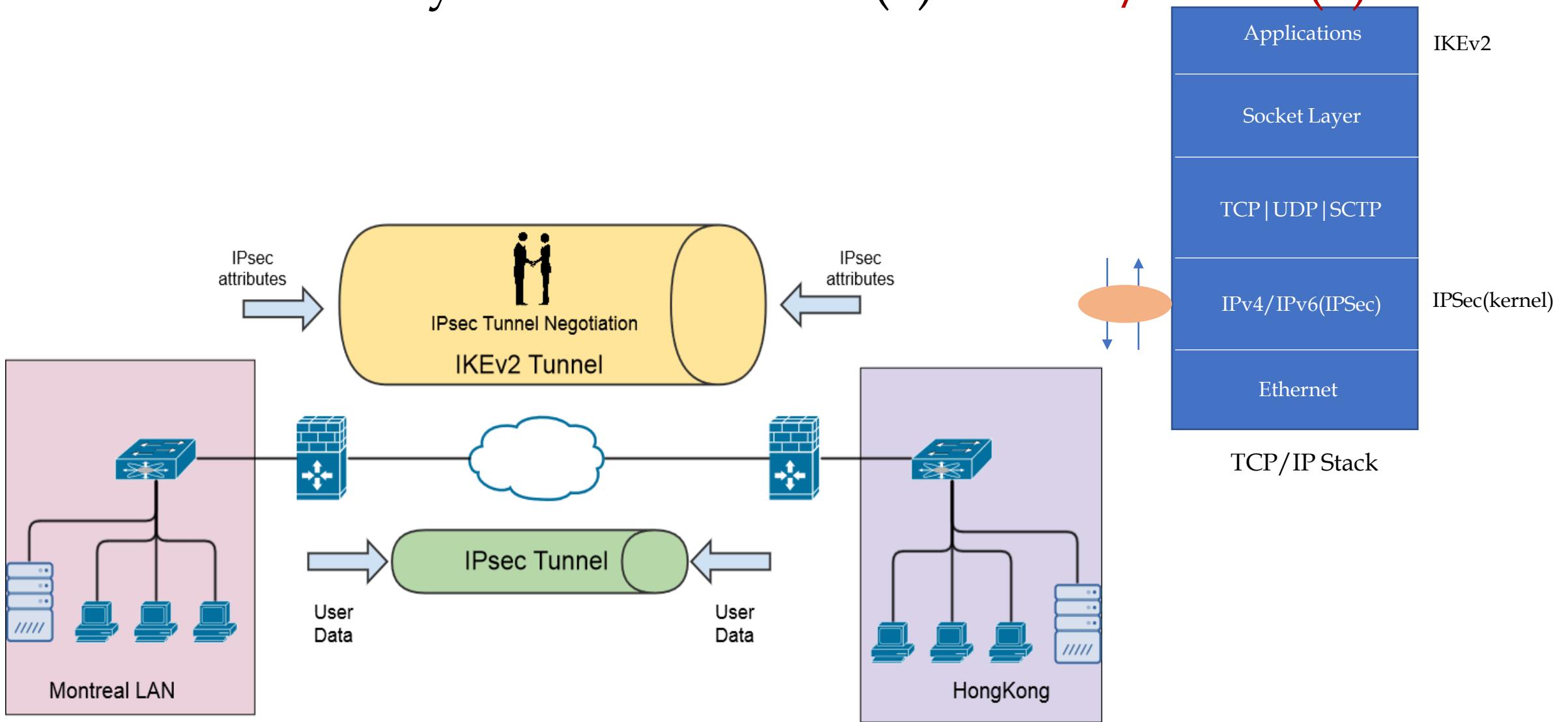
Advantages

- ☒ 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.

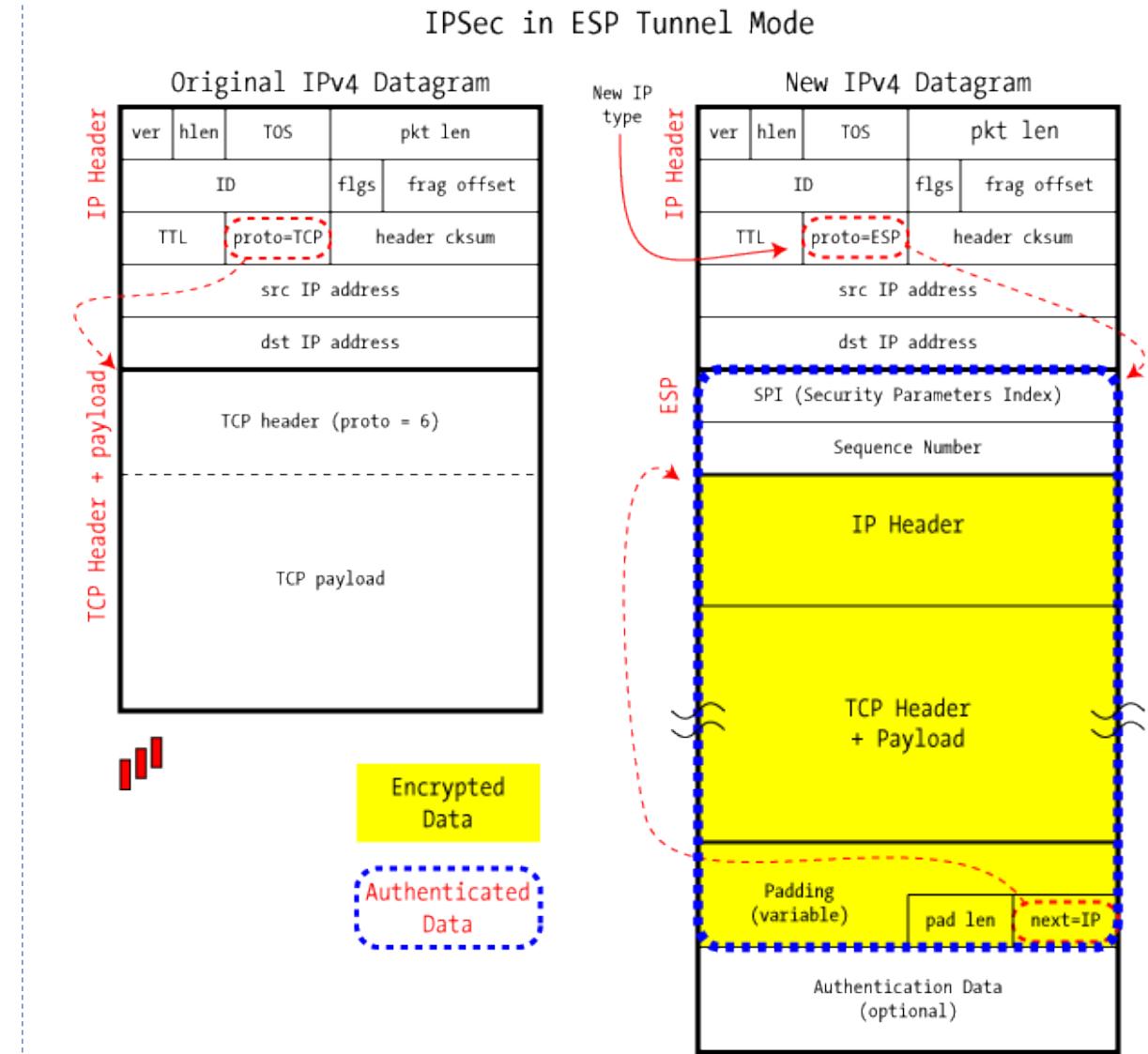
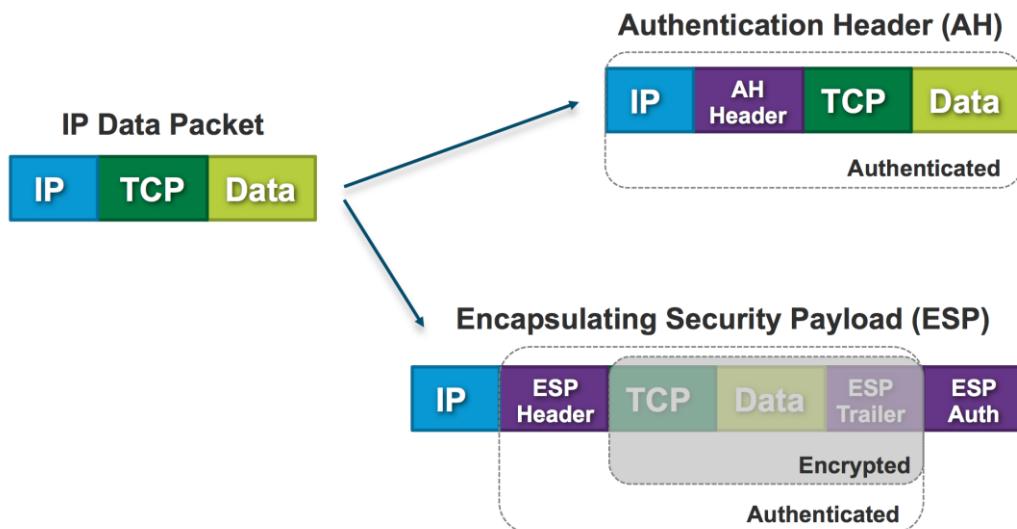
Disadvantages

- ☒ 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.

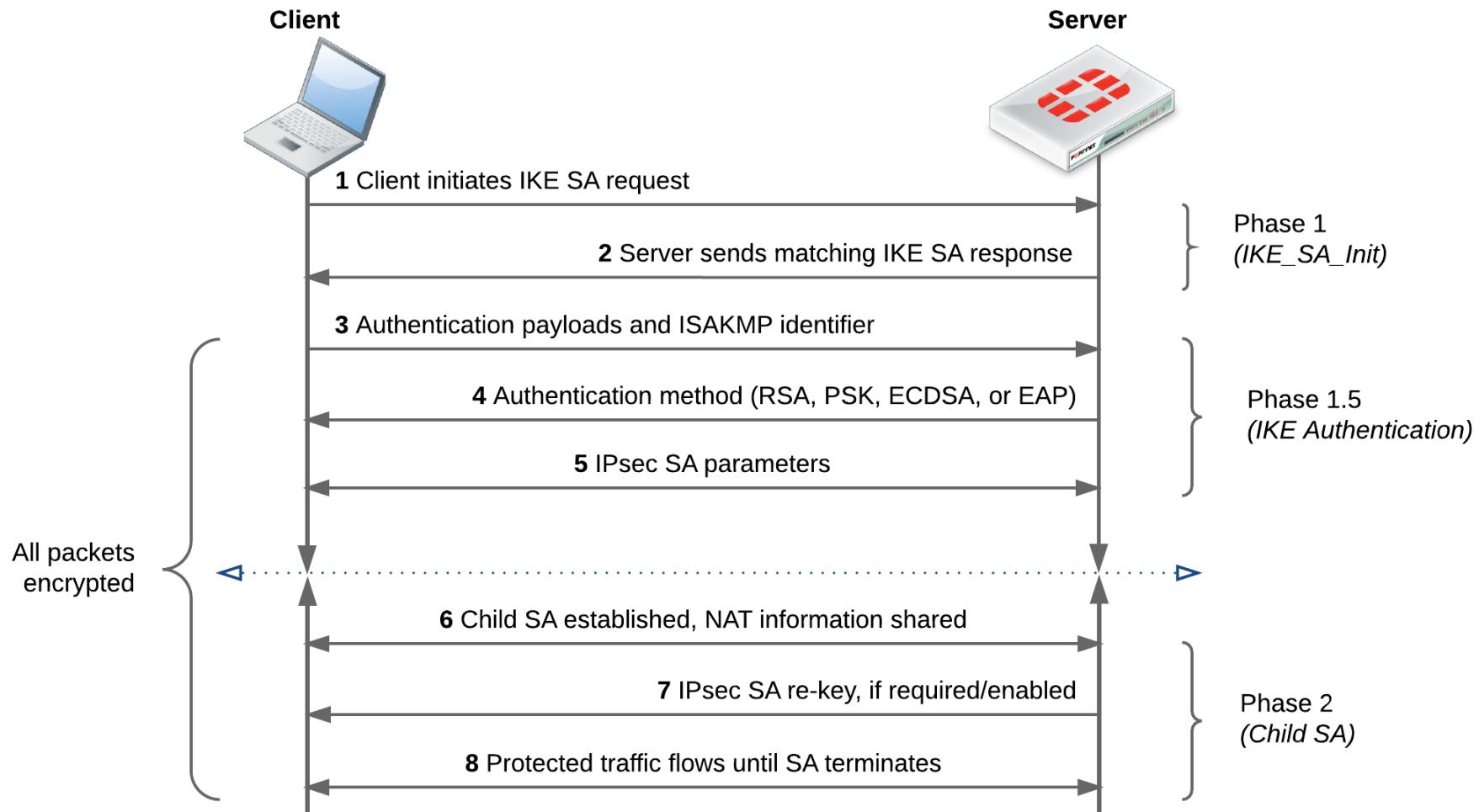
6. SPN Gateway & Mobile Phone(3) - IPsec/IKEv2(1)



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)

SPNBox3000 - SoftEther VPN Server Manager

Manage VPN Server "172.30.1.127"

Virtual Hub Name	Status	Type	Users	Groups	Sessions	MAC Tables	IP Tables
DEFAULT	Online	Standalone	0	0	0	0	0
SPNBOX3000	Online	Standalone	1	0	3	4	6

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

Local Bridge Setting Layer 3 Switch Setting IPsec / L2TP Setting OpenVPN / MS-SSTP Setting Refresh Exit

Dynamic DNS Setting VPN Azure VPN Azure Setting

IPsec / L2TP / EtherIP / L2TPv3 Settings

IPsec / L2TP / EtherIP / L2TPv3 Server Settings

Virtual Hubs on the VPN Server can accept Remote-Access VPN connections from L2TP-compatible PCs, Mac OS X and Smartphones, and also can accept EtherIP / L2TPv3 Site-to-Site VPN Connection.

L2TP Server (Remote-Access VPN Server Function)

VPN Connections from Smartphones suchlike iPhone, iPad and Android, and also from built-in VPN Clients on Mac OS X and Windows can be accepted.

Enable L2TP Server Function (L2TP over IPsec)
Make VPN Connections from iPhone, iPad, Android, Windows, and Mac OS X acceptable.

Enable L2TP Server Function (Raw L2TP with No Encryptions)
It supports special VPN Clients which uses L2TP with no IPsec encryption.

VPN Server Hub 명 선택

Default Virtual Hub in a case of omitting a name of Hub on the Username: SPNBOX3000

EtherIP Server Function (Site-to-Site VPN Connection)

Router products which are compatible with EtherIP / L2TPv3 over IPsec can connect to Virtual Hub on the VPN Server and establish Layer-2 (Ethernet) Bridging.

Enable EtherIP / L2TPv3 over IPsec Server Function

EtherIP / L2TPv3 Detail Settings

IPsec Common Settings

IPsec Pre-Shared Key: **VPN**

IPsec Pre-Shared Key is also called "PSKs" or "Secrets". Specify it with around eight ASCII characters, and let all VPN users know.

IPsec pre-shared key 값 입력(default: vpn)

OK Cancel

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
<input type="checkbox"/>		-						
<input type="checkbox"/>		-						
<input type="checkbox"/>		-						
<input type="checkbox"/>		-						
<input type="checkbox"/>		-						
<input type="checkbox"/>		-						
<input type="checkbox"/>		-						
<input type="checkbox"/>		-						
<input type="checkbox"/>		-						
<input type="checkbox"/>		-						
<input type="checkbox"/>		-						
<input type="checkbox"/>		-						
<input type="checkbox"/>		-						
<input type="checkbox"/>		-						
<input type="checkbox"/>		-	500-500	172.30.1.127	500-500	UDP	I2tp/ipsec	KT
<input type="checkbox"/>		-	4500-4500	172.30.1.127	4500-4500	UDP	I2tp/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)

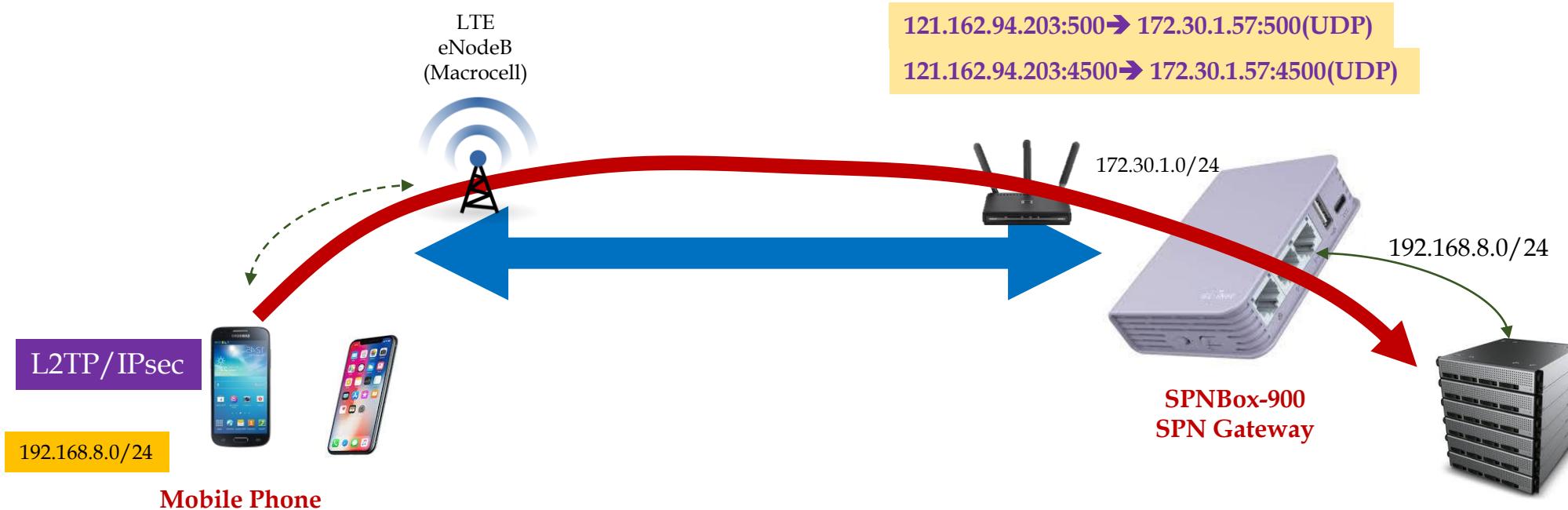


L2TP/IPsec 설정은 매우 간단하다. 즉, 서버 IP 주소, 사전 공유 키 및 사용자 정보만 입력하면 바로 연결 가능하다.

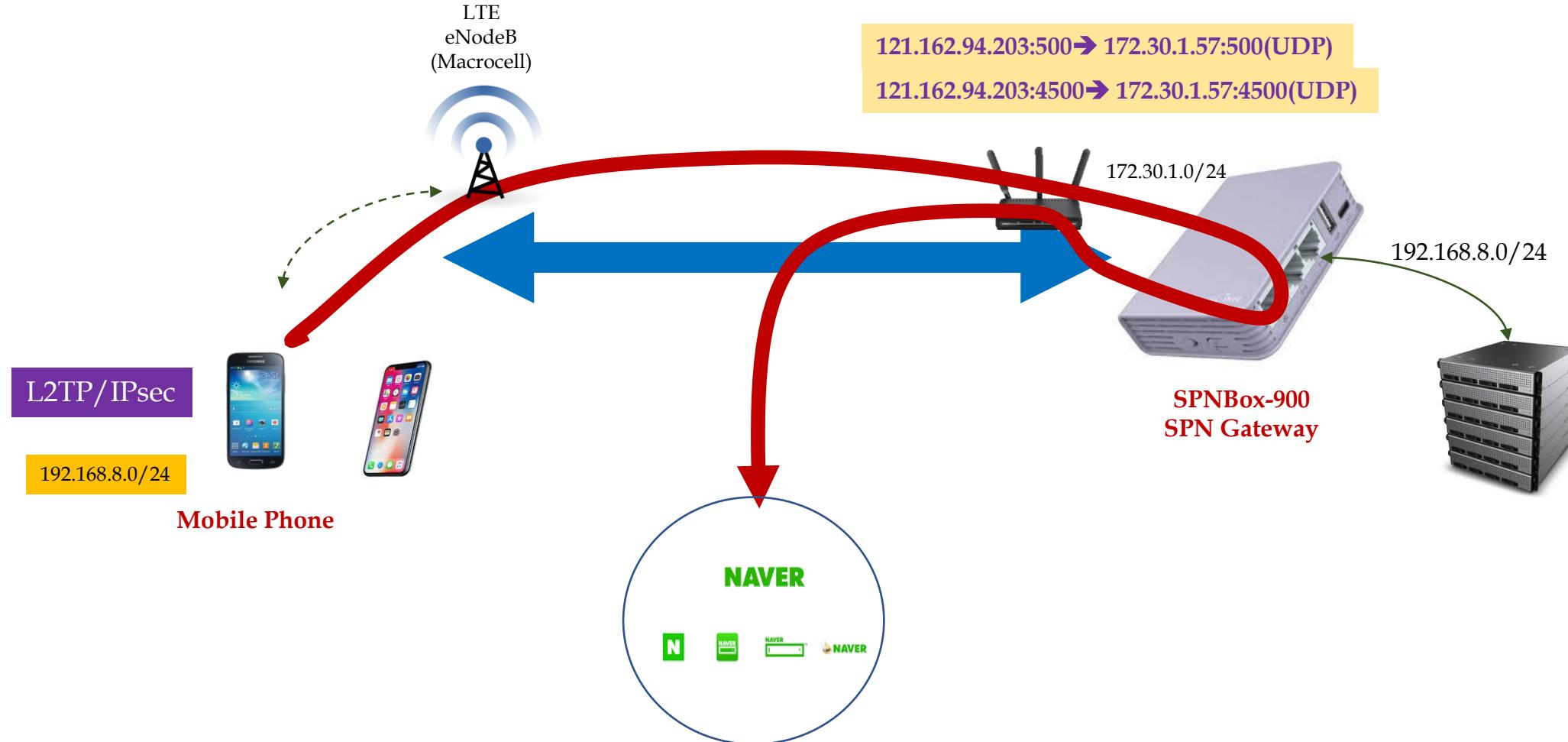
6. SPN Gateway & Mobile Phone(5) - Android 설정(2)

- <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)

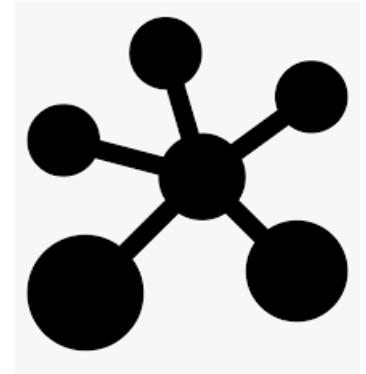


6. SPN Gateway & Mobile Phone(6) - VPN 연결 시험(2)

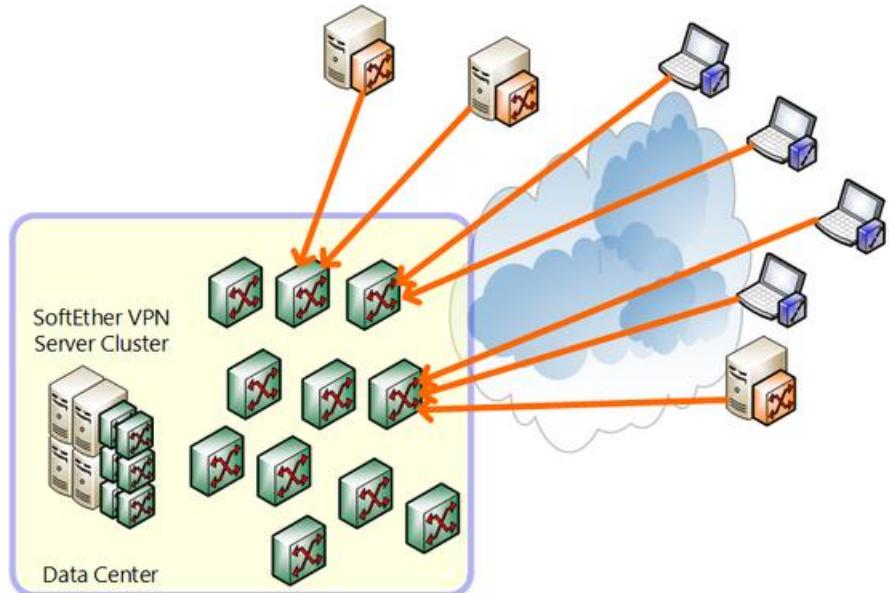


7. SPN Gateway Cluster : Setup Guide

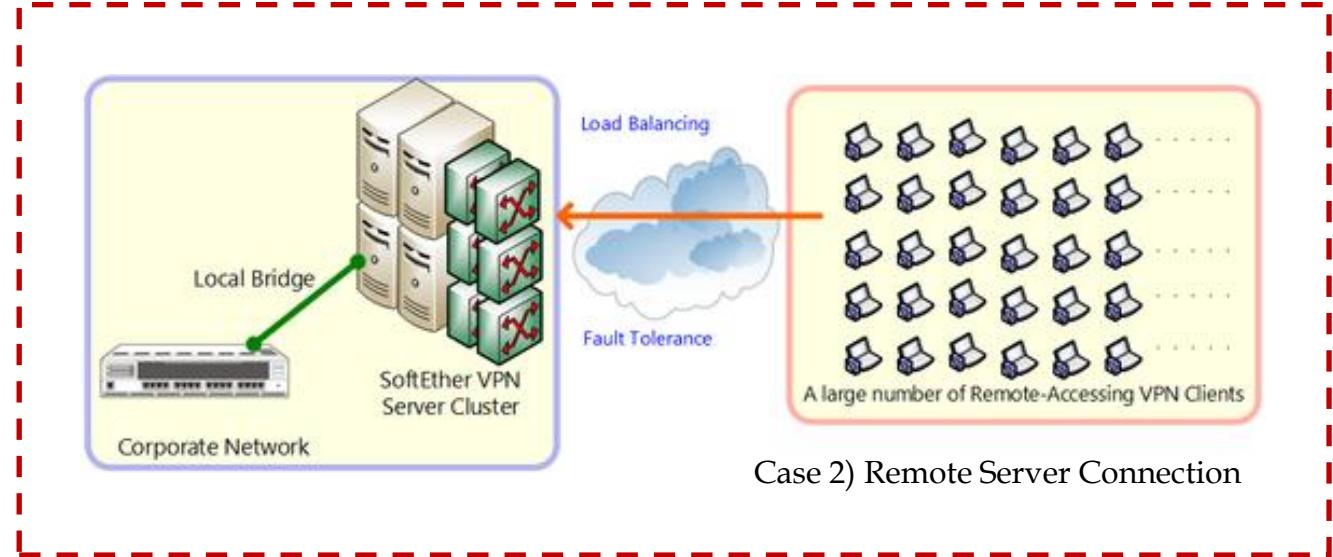
수십(최대 64) 개의 SPN Gateway를 묶어 하나의 SPN Gateway 처럼 사용하는 기능



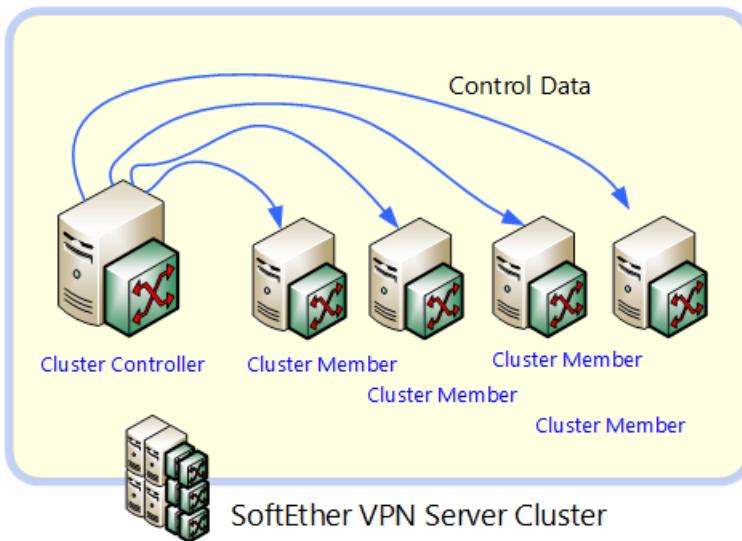
7. SPN Gateway Cluster(1) - SE Clustering 개요(1)



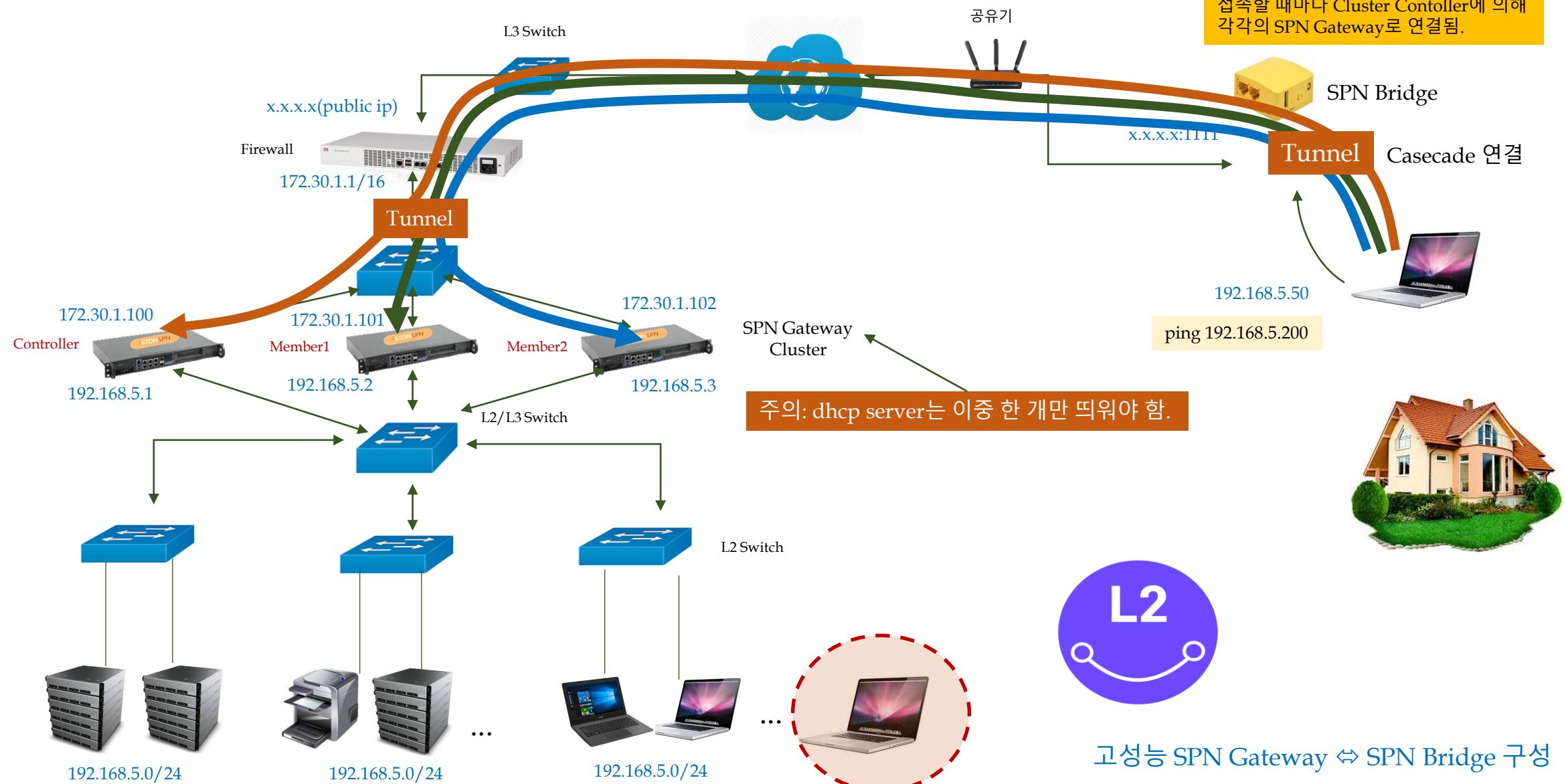
Case 1) Virtual Server Hosting



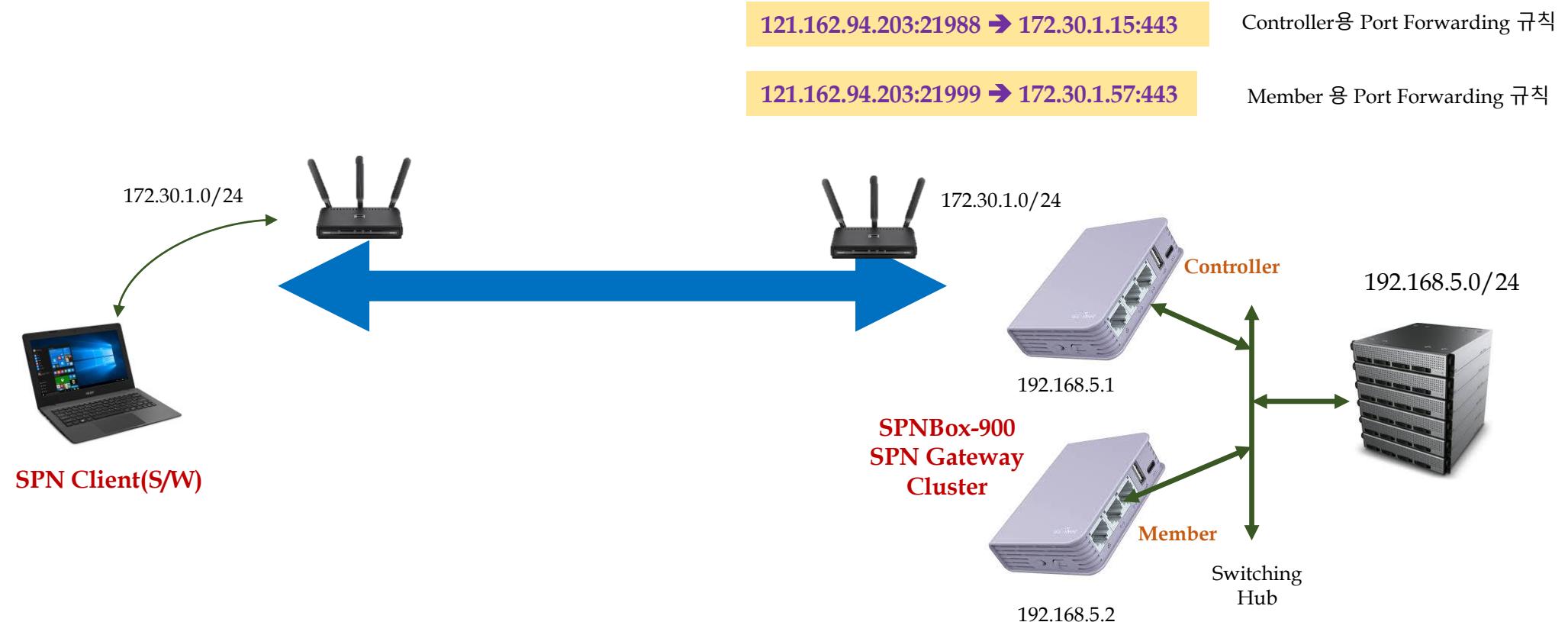
Case 2) Remote Server Connection



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



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



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.

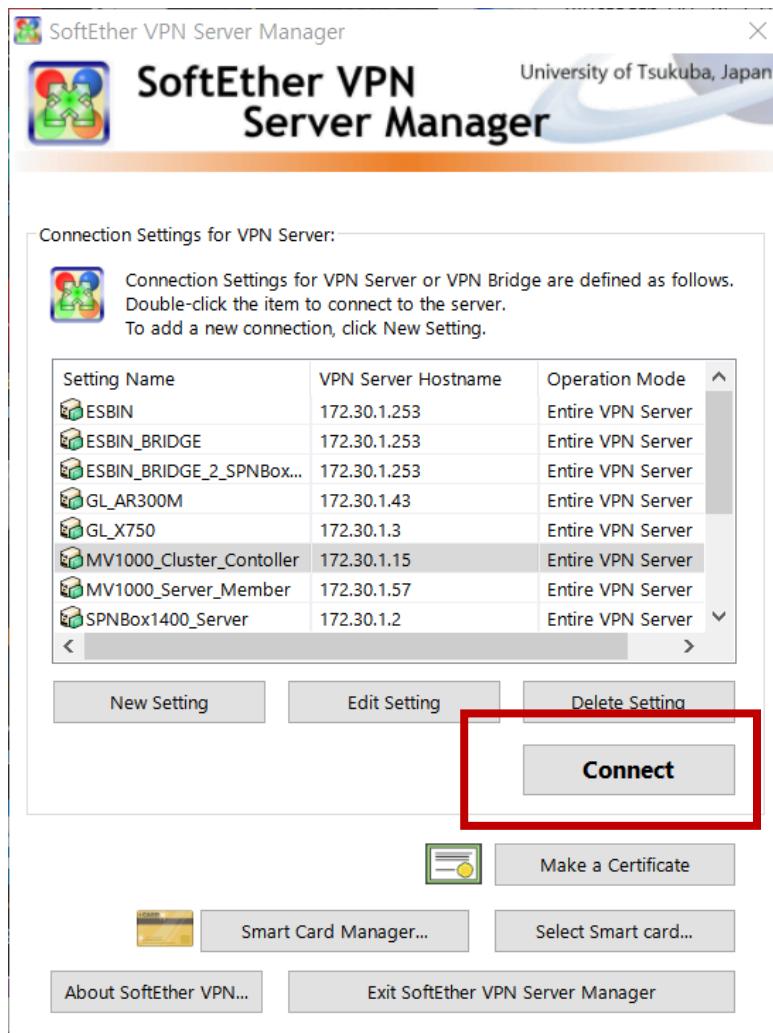
7. SPN Gateway Cluster(2) - Testbed(2)

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> <ul style="list-style-type: none">▪ 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_vpni br-lan bridge에 통합되었는지 확인하도록 하자.
c)	<Cluster Member 용 SPN Gateway 설정> <ul style="list-style-type: none">▪ 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_vpni br-lan bridge에 통합되었는지 확인하도록 하자.

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

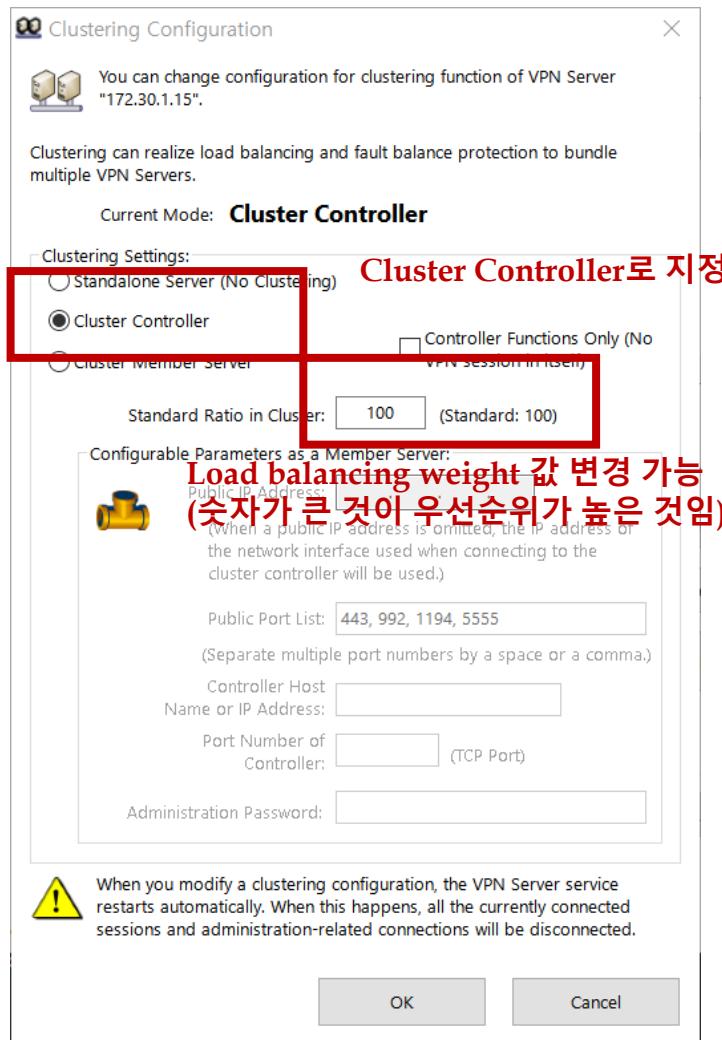
SPN Client	전체 설정 절차 요약
a)	VPN Client Manager를 실행한 후, VPN 설정을 한다. 이때 아래 정보가 필요하다. <ul style="list-style-type: none">▪ VPN Server에서 추가한 Virtual Hub 이름 및 사용자 계정 정보▪ Firewall or AP 안쪽에 VPN Server가 있을 경우, port forwarding 설정 및 이와 관련된 정보(Firewall External IP, port)

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



The screenshot shows the 'Manage VPN Server' window for '172.30.1.15'. It features a table with columns for 'Virtual Hub Name', 'Status', 'Type', 'Users', 'Groups', 'Sessions', 'MAC Tables', and 'IP T'. A row for 'SPNBOXCLUSTER' is highlighted with a red box. Below the table is a note in Korean: '이 부분은 나중에 생성한 것임(화면 capture를 나중에 한 것임)'. The window also includes tabs for 'Manage Virtual Hub', 'Online', 'Offline', 'View Status', 'Create a Virtual Hub', 'Properties', and 'Delete'. On the right, there's a section for 'Management of Listeners:' with a table for 'Listener List (TCP/IP port)' and buttons for 'Create', 'Delete', 'Start', and 'Stop'. The right side contains various configuration buttons, with 'Clustering Configuration' being specifically highlighted by a red box. At the bottom, it shows the current DDNS Hostname: 'vpn290370780.softether.n'.

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



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

New Virtual Hub

Virtual Hub Name: SPNBOXCLUSTER

Security Settings:
Administration password for this Virtual Hub.
Password: hub1234
Confirm: hub1234

No Enumerate to Anonymous Users

Virtual Hub Status:
Set the Virtual Hub status.
Online (radio button selected) Offline

Virtual Hub Options:
 Limit Max VPN Sessions
Max Number of Sessions: sessions
(Will not count sessions on server side that are generated by Local Bridge, Virtual NAT or Cascade Connection.)

You can configure more advanced settings on the Virtual Hub Extended Option List.

Edit Virtual Hub Extended Option List

OK Cancel

Static으로 지정해야 함.

MV1000_Cluster_Controller - SoftEther VPN Server Manager

Manage VPN Server "172.30.1.15"

Virtual Hub Name	Status	Type	Users	Groups	Sessions	MAC Tables	IP T
SPNBOXCLUSTER	Online	Static Hub	1	0	3	10	8

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

Manage Virtual Hub

Management of Listeners:

Port Number	Status
TCP 443	Listening
TCP 992	Listening
TCP 1194	Listening
TCP 5555	Listening

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

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

Management of Virtual Hub - 'SPNBOXCLUSTER'

Virtual Hub 'SPNBOXCLUST...

Management of Security Database:

- Manage Users** (highlighted with a red box)
- Add, delete or edit user accounts.

Virtual Hub Settings:

- Virtual Hub Properties**
- Configure this Hub.

- Authentication Server Setting**
- Use external RADIUS authentication server for user authentication.

- Manage Cascade Connections**
- Establish Cascade Connection to Hubs on local or remote VPN Servers.

Current Status of this Virtual Hub:

Item	Value
Virtual Hub Name	SPNBOXCLUSTER
Status	Online
Type	Static Hub
Sessions	3
Sessions (Client)	1
Sessions (Bridge)	0
Access Lists	0
Users	1
Groups	0
MAC Tables	10

Other Settings:

- Log Save Setting**
- Configure settings of log saving function.
- Trusted CA Certificates**
- Manage trusted CA certificates.
- Virtual NAT and Virtual DHCP Server (SecureNAT)**
- Secure NAT is available on this Virtual Hub. You can run Virtual NAT and Virtual DHCP.

VPN Sessions Management:

- Manage Sessions**
- Exit

Manage Users

Virtual Hub "SPNBOXCLUSTER" has the following users.

User Name	Full Name	Group Name	Description	Auth Method	Num Logins	Last Login
cuser	cluster user	-	cluster user	Password Authen...	4	2020-03-19

New Edit View User Info Remove Refresh Exit

사용자를 하나 등록: cuser/cuser1234

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

MV1000_Cluster_Controller - SoftEther VPN Server Manager

Manage VPN Server "172.30.1.15"

Virtual Hub Name	Status	Type	Users	Groups	Sessions	MAC Tables	IP Tables
SPNBOXCLUSTER	Online	Static Hub	1	0	3	10	8

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

Management of Listeners:

Listener List (TCP/IP port):

Port Number	Status	Action
TCP 443	Listening	Create
TCP 992	Listening	Delete
TCP 1194	Listening	Start
TCP 5555	Listening	Stop

Local Bridge Setting

Layer 3 Switch Setting

IPsec / L2TP Setting

OpenVPN / MS-SSTP Setting

Dynamic DNS Setting

VPN Azure Setting

Current DDNS Hostname: vph290370780.softether.n

Local Bridge Settings

Local Bridge can establish a Layer 2 bridge connection between a Virtual Hub on this VPN server and a physical Ethernet Device (Network Adapter). It is also possible to create a tap device (virtual network interface) and establish a bridge connection with a Virtual Hub. (Tap is supported on Linux versions only)

Number	Virtual Hub Name	Network Adapter or Tap Device Name	Status
1	SPNBOXCLUSTER	vpn	Operating

기존에 하던 대로 tap_vpn local bridge interface 생성

New Local Bridge Definition:

Select the Virtual Hub to bridge.

Virtual Hub:

Type to Create:

Bridge with Physical Existing Network Adapter

Bridge with New Tap Device

Select the Ethernet device (network adapter) for the bridge destination.

LAN Adapter: bond0

New Tap Device Name: (Maximum 11 Characters)

Note: Although it is possible to establish a bridge using any operating network adapter, in high load environments, you should prepare a network adapter dedicated for bridging.

Create Local Bridge

If a network adapter doesn't appear which is recently added on the system, reboot the computer and re-open this screen.

Exit

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

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

MV1000_Cluster_Controller - SoftEther VPN Server Manager

Manage VPN Server "172.30.1.15"

Virtual Hub Name	Status	Type	Users	Groups	Sessions	MAC Tables	IP T
SPNBOXCLUSTER	Online	Static Hub	1	0	3	10	8

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:

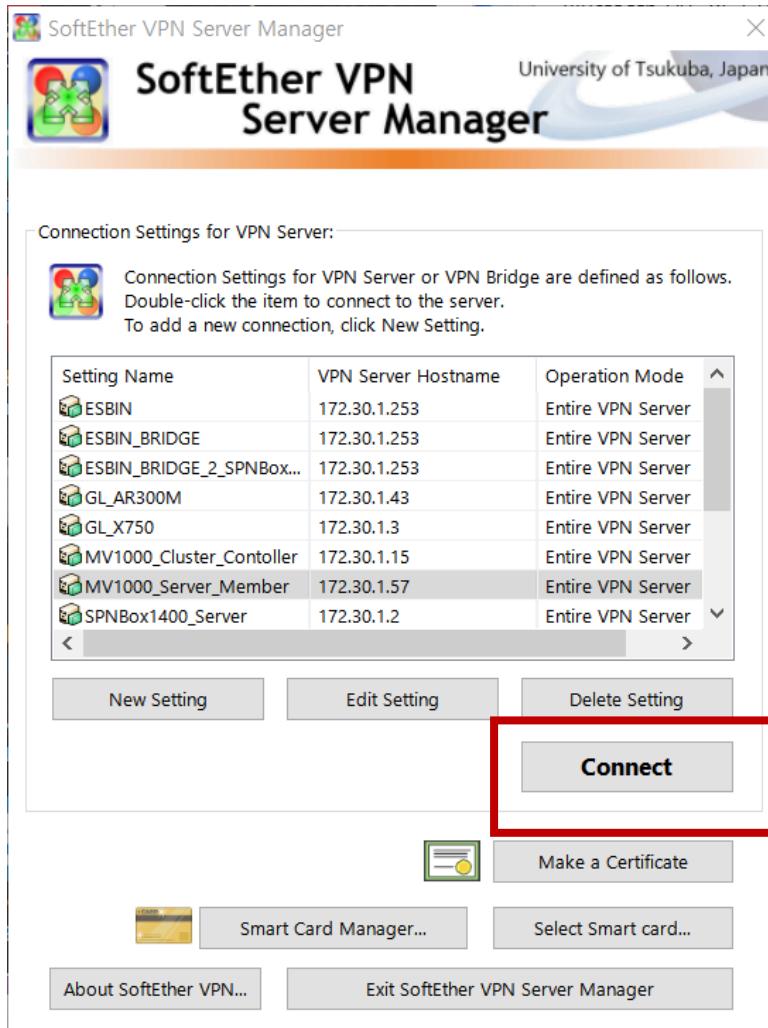
- Encryption and Network Clustering Configuration
- View Server Status Clustering Status
- About this VPN Server Show List of TCP/IP Connections
- Edit Config

Local Bridge Setting Layer 3 Switch Setting IPsec / L2TP Setting OpenVPN / MS-SSTP Setting

Dynamic DNS Setting VPN Azure Setting Refresh Exit

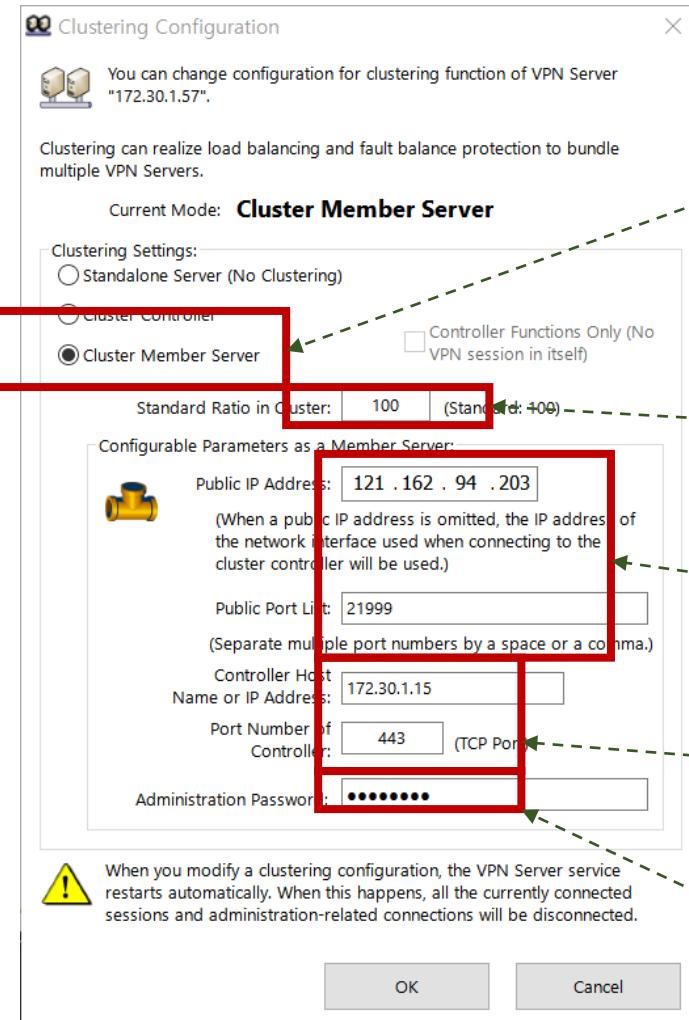
Current DDNS Hostname: vpn290370780.softether.n

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



This screenshot shows the 'Manage VPN Server "172.30.1.57"' window. It displays a table of virtual hubs, with one named 'SPNBOXCLUSTER' highlighted by a red box. Below the table are tabs for 'Manage Virtual Hub', 'Online', 'Offline', 'View Status', 'Create a Virtual Hub', 'Properties', and 'Delete'. A section for 'Management of Listeners' shows a table of TCP ports (443, 992, 1194, 5555) all in 'Listening' state. To the right, under 'VPN Server and Network Information and Settings', several options are listed: 'Encryption and Network', 'Clustering Configuration' (which is also highlighted with a red box), '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', and 'Exit'. At the bottom, it shows the current DDNS hostname: 'vpn433471537.softether.n'.

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)

Management of Virtual Hub - 'SPNBOXCLUSTER'

Virtual Hub 'SPNBOXCLUST...'

Management of Security Database:

- Manage Users
- Manage Groups
- Manage Access Lists

Virtual Hub Settings:

- Virtual Hub Properties
- Authentication Server Setting
- Manage Cascade Connections

Current Status of this Virtual Hub:

Item	Value
Virtual Hub Name	SPNBOXCLUSTER
Status	Online
Type	Static Hub
Sessions	2
Sessions (Client)	1
Sessions (Bridge)	0
Access Lists	0
MAC Tables	5
IP Tables	7
Num Logins	6

Other Settings:

- Log Save Setting
- Log File List
- Trusted CA Certificates
- Revoked Certs
- Virtual NAT and Virtual DHCP Server (SecureNAT)

VPN Sessions Management:

- Manage Sessions

Exit

Local Bridge Settings

Local Bridge can establish a Layer 2 bridge connection between a Virtual Hub on this VPN server and a physical Ethernet Device (Network Adapter). It is also possible to create a tap device (virtual network interface) and establish a bridge connection with a Virtual Hub. (Tap is supported on Linux versions only)

Number	Virtual Hub Name	Network Adapter or Tap Device Name	Status
1	SPNBOXCLUSTER	vpn	Operating

기존에 하던 대로 tap_vpn local bridge interface 생성

New New Local Bridge Definition:

Select the Virtual Hub to bridge.

Virtual Hub:

Type to Create:

Bridge with Physical Existing Network Adapter

Bridge with New Tap Device

Select the Ethernet device (network adapter) for the bridge destination.

LAN Adapter: bond0

New Tap Device Name: (Maximum 11 Characters)

Note: Although it is possible to establish a bridge using any operating network adapter, in high load environments, you should prepare a network adapter dedicated for bridging.

Create Local Bridge

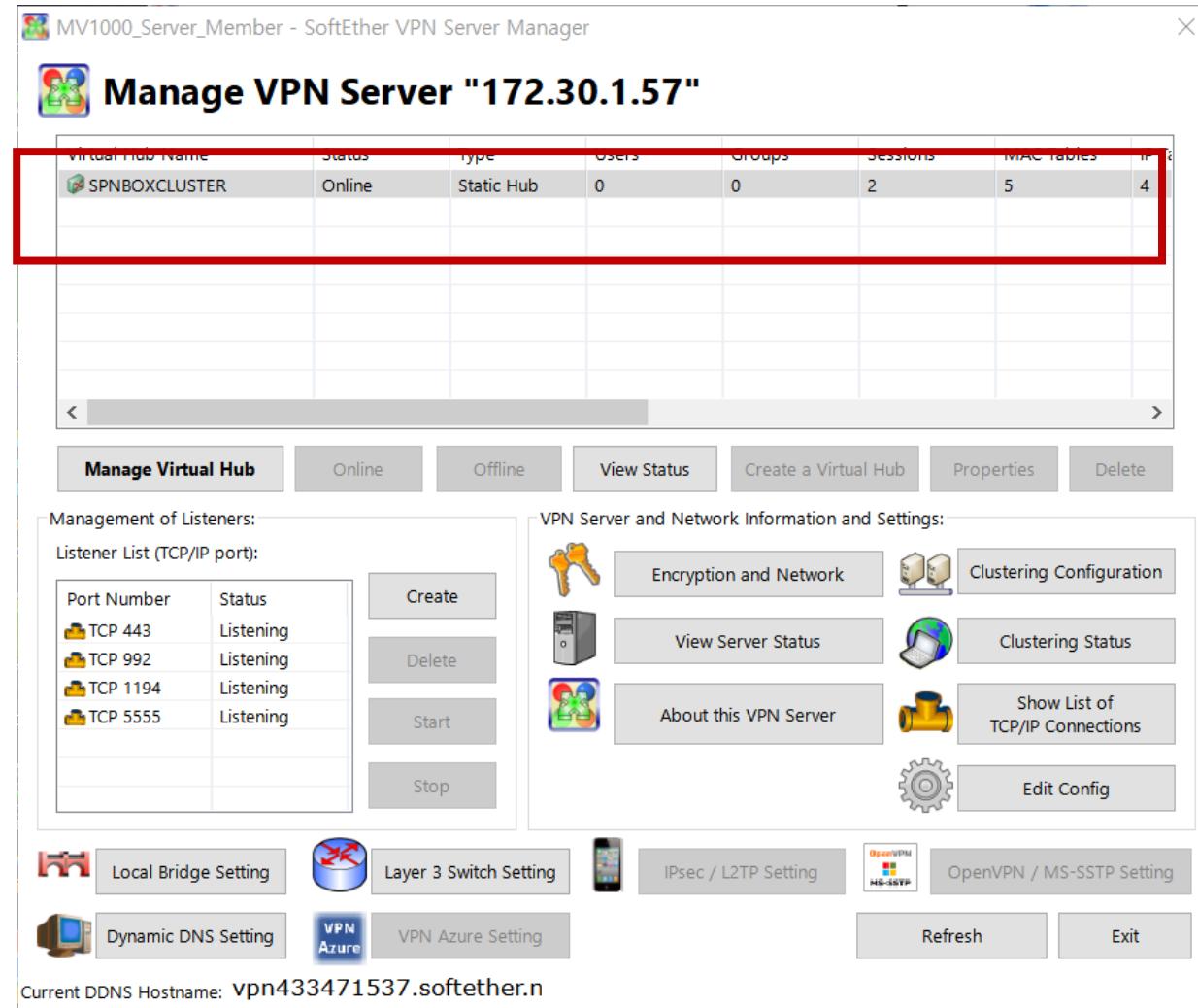
If a network adapter doesn't appear which is recently added on the system, reboot the computer and re-open this screen.

Exit

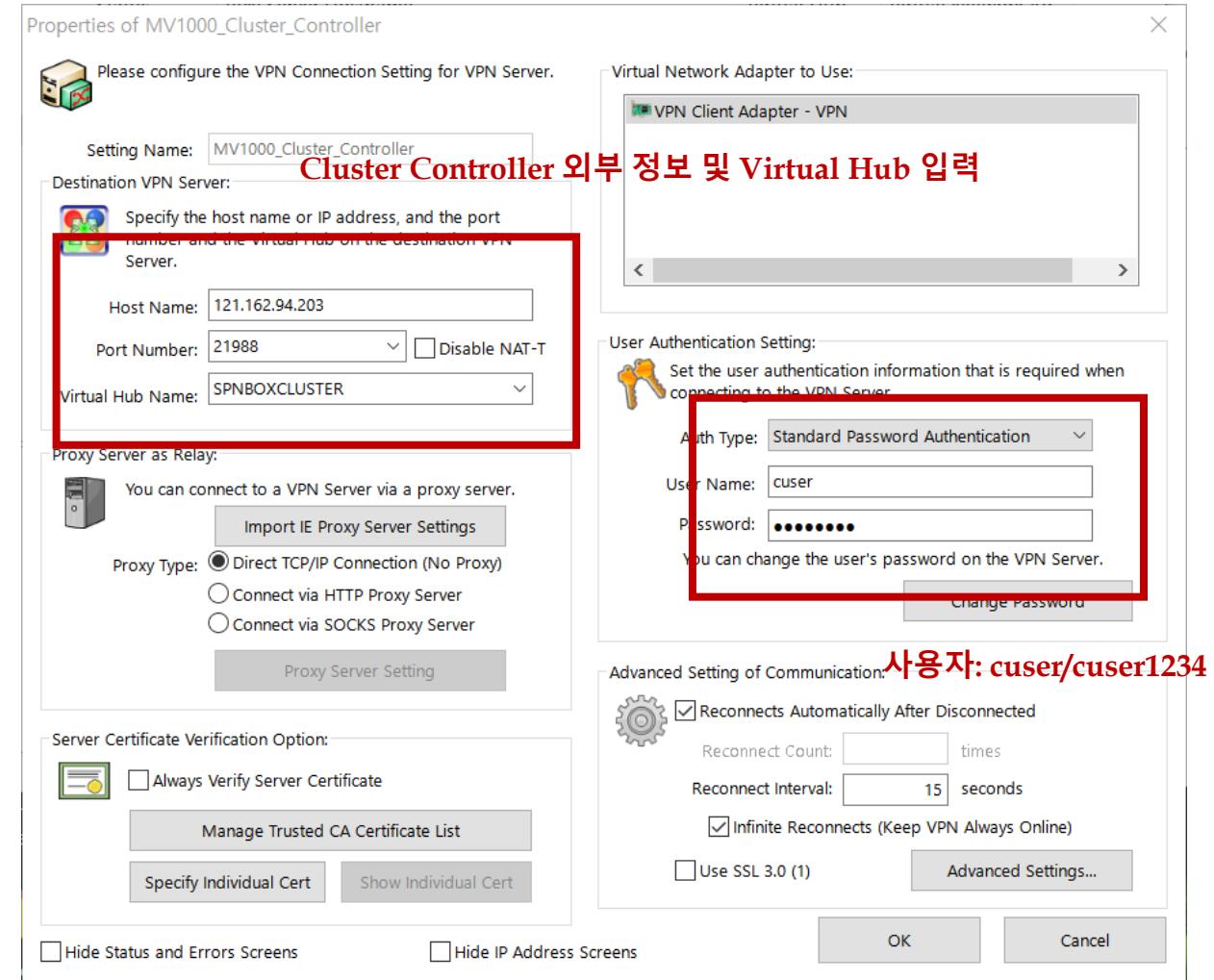
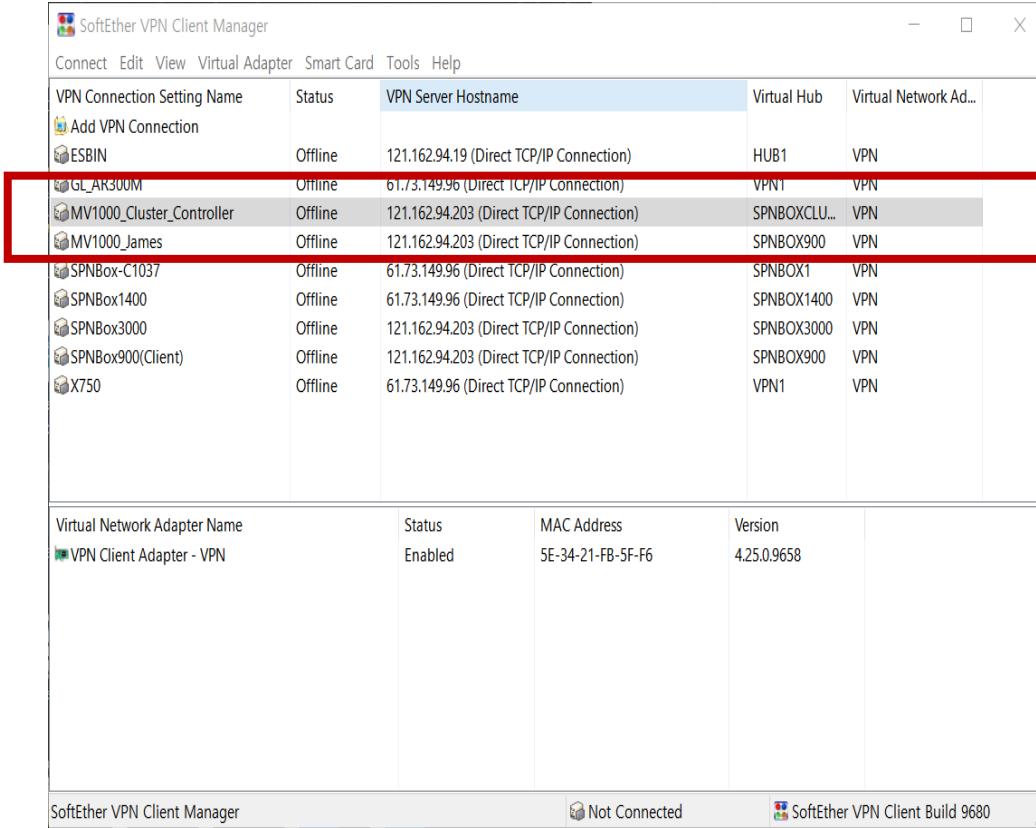
VirtualHub은 별도로 생성할 필요 없음. Controller에서 생성한 내용을 공통으로 사용함.

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

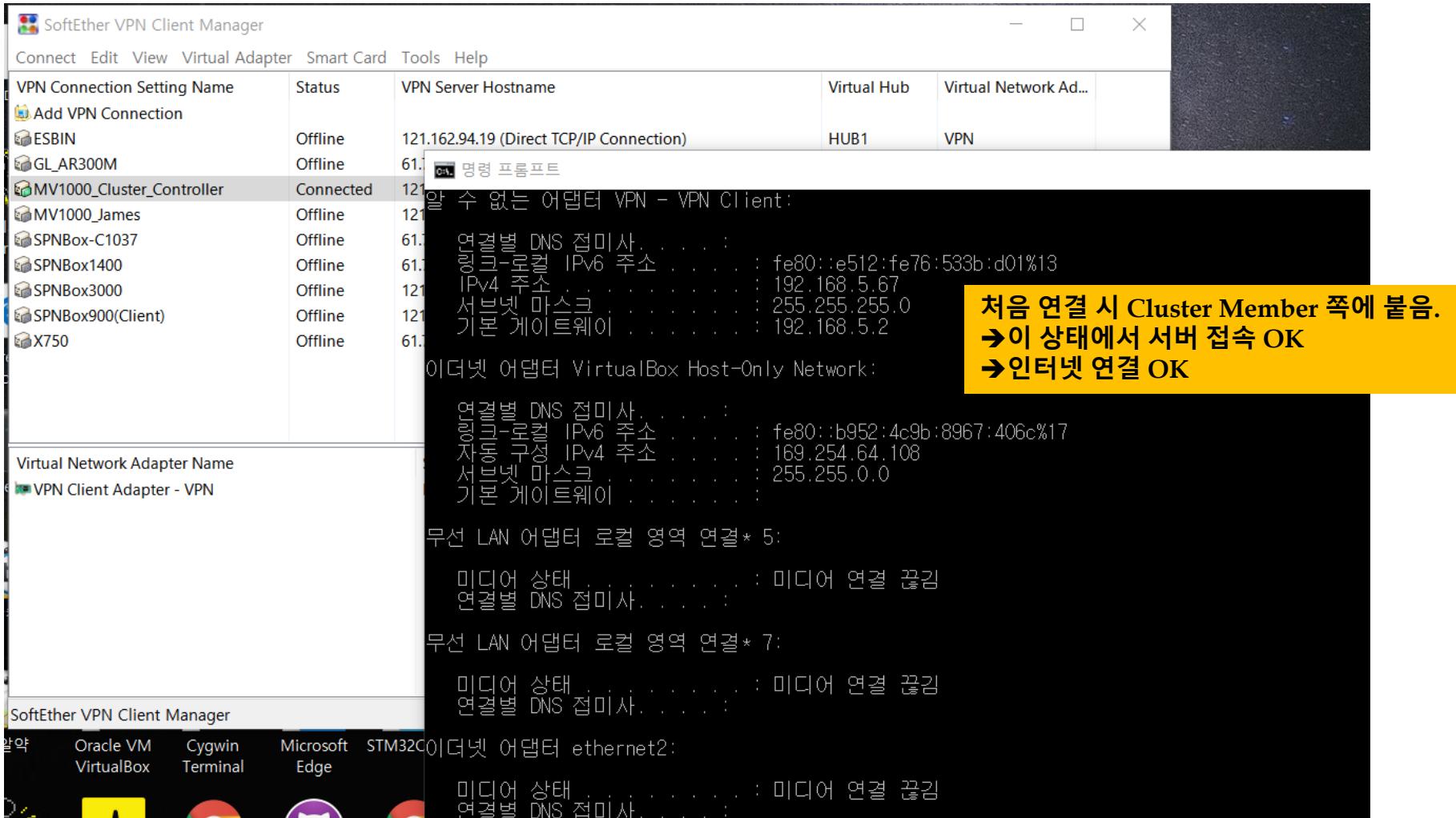
7. SPN Gateway Cluster(4) - Cluster Member 설정(4)



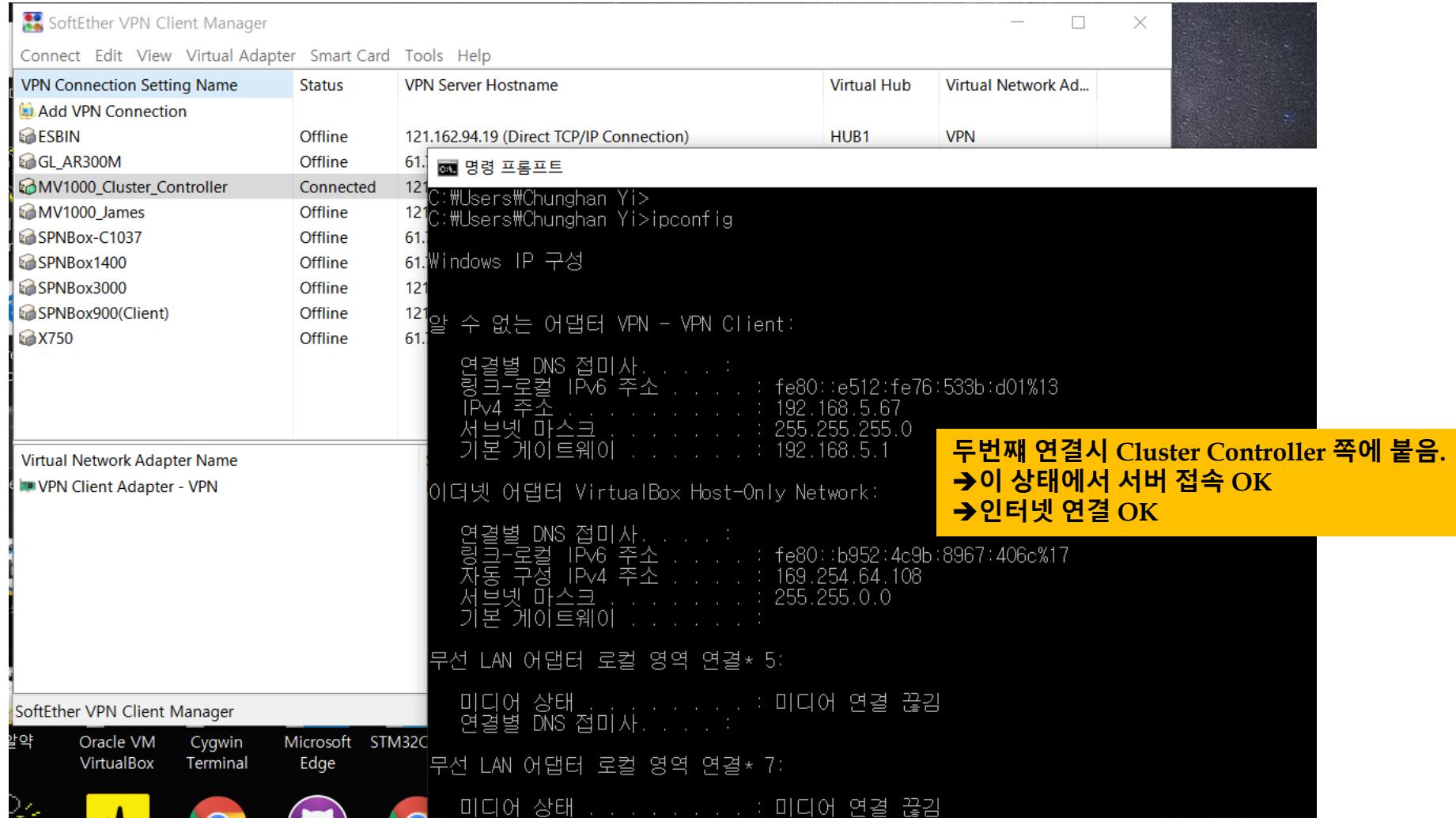
7. SPN Gateway Cluster(5) - SPN Client 설정(1)



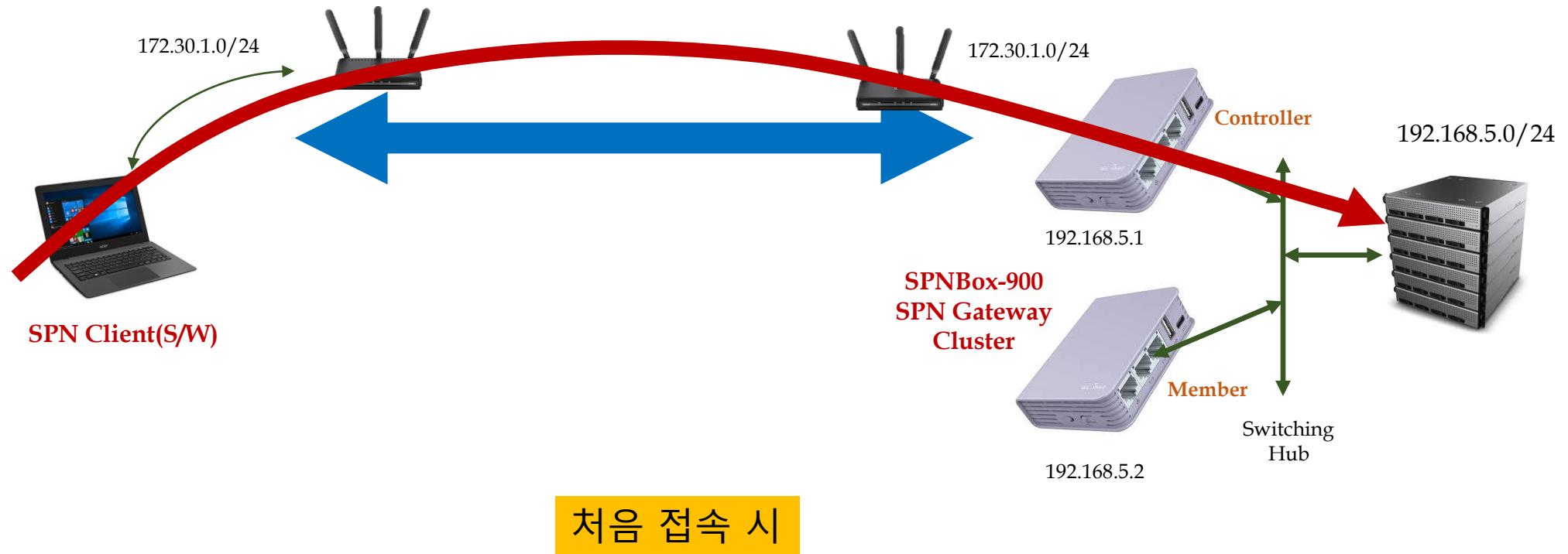
7. SPN Gateway Cluster(5) - SPN Client 설정(2)



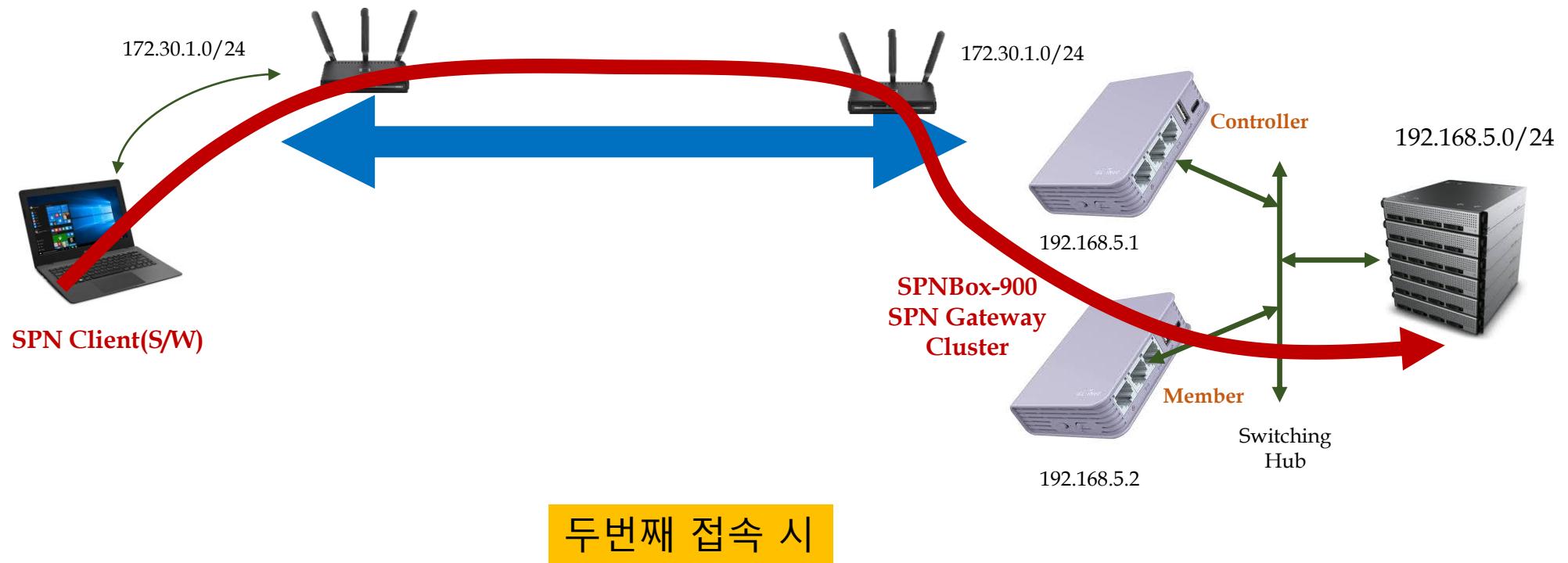
7. SPN Gateway Cluster(5) - SPN Client 설정(3)



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



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



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)

```
root@spnbox-900: ~
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 탭(B) 도움말(H)
chyi@mars: ~/workspace/spn/2ston_spnbox_prj x root@spnbox-900: ~ x
top - 06:58:37 up 4:03, 1 user, load average: 0.06, 0.04, 0.00
Tasks: 116 total, 1 running, 115 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.5 us, 1.3 sy, 0.0 ni, 98.0 id, 0.0 wa, 0.0 hi, 0.2 si, 0.0 st
KiB Mem : 949752 total, 647124 free, 79324 used, 223304 buff/cache
KiB Swap: 0 total, 0 free, 0 used. 807940 avail Mem

PID USER PR NI VIRT RES %CPU %MEM TIME+ COMMAND
3527 root 20 0 7684 3384 2776 R 2.6 0.4 1:56.24 top
1934 root 0 -20 1011964 22700 5420 S 0.3 2.4 2:16.79 vpnserver
3729 root 20 0 0 0 0 S 0.3 0.0 0:05.16 kworker/1:1
1 root 20 0 0 0 0 S 0.0 0.0 0:07.72 systemd
2 root 20 0 0 0 0 S 0.0 0.0 0:00.01 kthreadd
3 root 20 0 0 0 0 S 0.0 0.0 0:00.34 ksoftirqd/0
5 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 kworker/0:0H
7 root 20 0 0 0 0 S 0.0 0.0 0:01.64 rcu_preempt
8 root 20 0 0 0 0 S 0.0 0.0 0:00.00 rcu_sched
9 root 20 0 0 0 0 S 0.0 0.0 0:00.00 rcu_bh
10 root rt 0 0 0 0 S 0.0 0.0 0:00.22 migration/0
11 root rt 0 0 0 0 S 0.0 0.0 0:00.04 watchdog/0
12 root rt 0 0 0 0 S 0.0 0.0 0:00.03 watchdog/1
13 root rt 0 0 0 0 S 0.0 0.0 0:00.22 migration/1
14 root 20 0 0 0 0 S 0.0 0.0 0:00.14 ksoftirqd/1
16 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 kworker/1:0H
17 root 20 0 0 0 0 S 0.0 0.0 0:00.00 kdevtmpfs
18 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 netns
21 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 perf
377 root 20 0 0 0 0 S 0.0 0.0 0:00.02 khungtaskd
378 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 writeback
380 root 25 5 0 0 0 S 0.0 0.0 0:00.00 ksmd
381 root 39 19 0 0 0 S 0.0 0.0 0:00.79 khugepaged
382 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 crypto
383 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 bioset
385 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 kblockd
396 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 ata_sff
419 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 md
515 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 rpciod
```

SPN Gateway1(Cluster Controller)

```
root@spnbox-900: ~
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 탭(B) 도움말(H)
chyi@mars: ~/workspace/spn/2ston_spnbox_prj x root@spnbox-900: ~ x
top - 06:58:36 up 4:03, 1 user, load average: 0.21, 0.08, 0.01
Tasks: 114 total, 1 running, 113 sleeping, 0 stopped, 0 zombie
%Cpu(s): 4.1 us, 5.1 sy, 0.0 ni, 87.7 id, 0.0 wa, 0.7 hi, 2.5 si, 0.0 st
KiB Mem : 949752 total, 695780 free, 77504 used, 176468 buff/cache
KiB Swap: 0 total, 0 free, 0 used. 809872 avail Mem

PID USER PR NI VIRT RES %CPU %MEM TIME+ COMMAND
1931 root 0 -20 1012164 22796 5440 S 15.0 2.4 3:27.66 vpnservice
11959 root 20 0 7684 3404 2768 R 1.3 0.4 1:59.99 top
3 root 20 0 0 0 0 S 0.3 0.0 0:00.34 ksoftirqd/0
1822 systemd+ 20 0 10680 5500 4668 S 0.3 0.6 0:01.96 systemd-resolve
12391 root 20 0 0 0 0 S 0.3 0.0 0:00.52 kworker/0:1
1 root 20 0 95112 7732 5716 S 0.0 0.8 0:07.36 systemd
2 root 20 0 0 0 0 S 0.0 0.0 0:00.01 kthreadd
5 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 kworker/0:0H
7 root 20 0 0 0 0 S 0.0 0.0 0:01.79 rcu_preempt
8 root 20 0 0 0 0 S 0.0 0.0 0:00.00 rcu_sched
9 root 20 0 0 0 0 S 0.0 0.0 0:00.00 rcu_bh
10 root rt 0 0 0 0 S 0.0 0.0 0:00.00 migration/0
11 root rt 0 0 0 0 S 0.0 0.0 0:00.04 watchdog/0
12 root rt 0 0 0 0 S 0.0 0.0 0:00.04 watchdog/1
13 root rt 0 0 0 0 S 0.0 0.0 0:00.19 migration/1
14 root 20 0 0 0 0 S 0.0 0.0 0:00.10 ksoftirqd/1
16 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 kworker/1:0H
17 root 20 0 0 0 0 S 0.0 0.0 0:00.00 kdevtmpfs
18 root 20 0 0 0 0 S 0.0 0.0 0:00.00 netns
21 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 perf
377 root 20 0 0 0 0 S 0.0 0.0 0:00.02 khungtaskd
378 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 writeback
380 root 25 5 0 0 0 S 0.0 0.0 0:00.00 ksmd
381 root 39 19 0 0 0 S 0.0 0.0 0:00.86 khugepaged
382 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 crypto
383 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 bioset
385 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 kblockd
396 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 ata_sff
419 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 md
```

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)

```
root@spnbox-900:/sbin/vpnserver/server_log
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 탭(B) 도움말(H)
chyi@mars:~/workspace/spn/2ston_spnbox_prj x root@spnbox-900:/sbin/vpnserver/server_log x
02:21:09.632399 IP 172.30.1.15.https > spnbox-900.49520: Flags [.], ack 94530, win 1429, options [nop, nop, TS val 1777077 ecr 1777047], length 0
02:21:09.692483 IP spnbox-900.https > 61.73.149.73.57300: Flags [P.], seq 6760:7021, ack 8510, win 628, options [nop,nop,TS val 1777062 ecr 1983526046], length 261
02:21:09.694036 IP 61.73.149.73.57300 > spnbox-900.https: Flags [.], ack 7021, win 3949, options [nop, nop, TS val 1983528334 ecr 1777062], length 0
02:21:09.859433 IP spnbox-900.https > 61.73.149.73.57298: Flags [P.], seq 11218:11671, ack 12813, win 682, options [nop,nop,TS val 1777104 ecr 1983525029], length 453
02:21:09.861144 IP 61.73.149.73.57298 > spnbox-900.https: Flags [.], ack 11671, win 5085, options [nop ,nop,TS val 1983528501 ecr 1777104], length 0
02:21:11.010078 IP 91.108.56.104.https > spnbox-900.49379: Flags [P.], seq 11583:11688, ack 2895, win 2534, options [nop,nop,TS val 3290932617 ecr 807622813], length 105
02:21:11.011153 IP spnbox-900.49379 > 91.108.56.104.https: Flags [.], ack 11688, win 4092, options [no p,nop,TS val 807624358 ecr 3290932617], length 0
02:21:11.462105 IP 91.108.56.104.https > spnbox-900.49379: Flags [P.], seq 11688:11793, ack 2895, win 2534, options [nop,nop,TS val 3290932730 ecr 807624358], length 105
02:21:11.463146 IP spnbox-900.49379 > 91.108.56.104.https: Flags [.], ack 11793, win 4092, options [no p,nop,TS val 807624810 ecr 3290932730], length 0
02:21:11.469379 IP 61.73.149.73.57300 > spnbox-900.https: Flags [P.], seq 8510:8867, ack 7021, win 3949, options [nop,nop,TS val 1983530109 ecr 1777062], length 357
02:21:11.469645 IP spnbox-900.https > 61.73.149.73.57300: Flags [.], ack 8867, win 651, options [nop,nop,TS val 1777506 ecr 1983530109], length 0
02:21:11.663822 IP 61.73.149.73.57298 > spnbox-900.https: Flags [P.], seq 12813:13074, ack 11671, win 5085, options [nop,nop,TS val 1983530304 ecr 1777104], length 261
02:21:11.664077 IP spnbox-900.https > 61.73.149.73.57298: Flags [.], ack 13074, win 704, options [nop, nop, TS val 1777555 ecr 1983530304], length 0
02:21:13.670664 IP 192.168.5.84.49362 > 91.108.56.118.https: Flags [R], seq 1211259880, win 0, length 0
02:21:13.774918 IP spnbox-900.https > 61.73.149.73.57300: Flags [P.], seq 7021:7298, ack 8867, win 651, options [nop,nop,TS val 1778082 ecr 1983530109], length 277
02:21:13.776524 IP 61.73.149.73.57300 > spnbox-900.https: Flags [.], ack 7298, win 4078, options [nop, nop, TS val 1983532416 ecr 1778082], length 0
```

```
# tcpdump -i wan port 443
```

SPN Gateway1(Cluster Controller)

```
root@spnbox-900:/sbin/vpnserver
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 탭(B) 도움말(H)
chyi@mars:~/workspace/spn/2ston_spnbox_prj/spnbox/sy... x root@spnbox-900:/sbin/vpnserver x
02:21:09.584950 IP 52.114.32.6.https > spnbox-900.55900: Flags [P.], seq 5237:6047, ack 253, win 1027, leng th 810
02:21:09.631310 IP spnbox-900.https > 172.30.1.57.49520: Flags [P.], seq 36780:37649, ack 92589, win 1432, options [nop,nop,TS val 1777075 ecr 1774543], length 869
02:21:09.632724 IP 172.30.1.57.49520 > spnbox-900.https: Flags [.], seq 92589:94037, ack 37649, win 1424, o ptions [nop,nop,TS val 1777047 ecr 1777075], length 1448
02:21:09.637392 IP 172.30.1.57.49520 > spnbox-900.https: Flags [P.], seq 94037:94530, ack 37649, win 1424, options [nop,nop,TS val 1777047 ecr 1777075], length 493
02:21:09.637573 IP spnbox-900.https > 172.30.1.57.49520: Flags [.], ack 94037, win 1432, options [nop,nop,T S val 1777077 ecr 1777047], length 0
02:21:09.637673 IP spnbox-900.https > 172.30.1.57.49520: Flags [.], ack 94530, win 1429, options [nop,nop,T S val 1777077 ecr 1777047], length 0
02:21:09.641703 IP spnbox-900.55900 > 52.114.32.6.https: Flags [.], ack 6047, win 1024, length 0
02:21:09.644584 IP spnbox-900.55900 > 52.114.32.6.https: Flags [P.], seq 253:346, ack 6047, win 1024, leng ht 93
02:21:09.663594 IP 52.114.32.6.https > spnbox-900.55900: Flags [P.], seq 4738:6047, ack 253, win 1027, leng th 1309
02:21:09.671063 IP spnbox-900.55900 > 52.114.32.6.https: Flags [.], ack 6047, win 1024, options [nop,nop,sa ck 1 {4738:6047}], length 0
02:21:09.696281 IP 52.114.32.6.https > spnbox-900.55900: Flags [P.], seq 6047:6098, ack 346, win 1027, leng th 51
02:21:09.752106 IP spnbox-900.55900 > 52.114.32.6.https: Flags [.], ack 6098, win 1023, length 0
02:21:09.753915 IP spnbox-900.55900 > 52.114.32.6.https: Flags [P.], seq 346:936, ack 6098, win 1023, leng ht 590
02:21:09.754114 IP spnbox-900.55900 > 52.114.32.6.https: Flags [P.], seq 936:2097, ack 6098, win 1023, leng ht 1161
02:21:09.785807 IP 52.114.32.6.https > spnbox-900.55900: Flags [.], ack 2097, win 1027, length 0
02:21:09.864000 IP 52.114.32.6.https > spnbox-900.55900: Flags [P.], seq 6098:6524, ack 2097, win 1027, len ght 426
02:21:09.877409 IP spnbox-900.55900 > 52.114.32.6.https: Flags [.], ack 6524, win 1022, length 0
02:21:13.675111 IP 91.108.56.118.https > spnbox-900.49362: Flags [.], ack 1, win 7508, options [nop,nop,TS val 3280390144 ecr 806423544], length 0
```

```
# tcpdump -i wan port 443
```

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

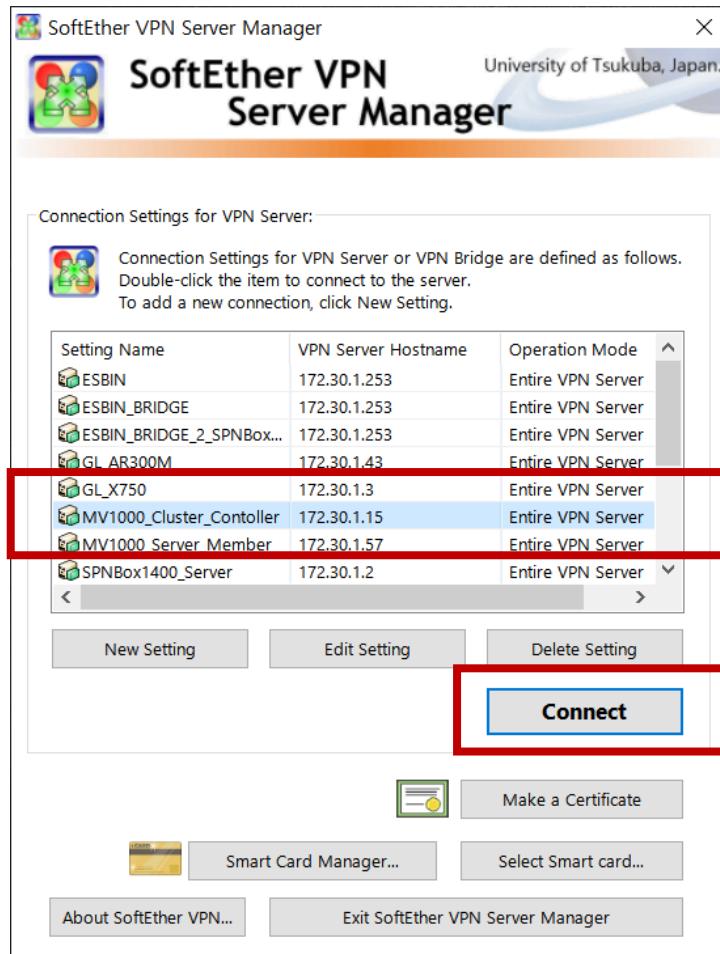
8. 인터넷 접속 차단 : Setup Guide

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)



The screenshot shows the 'Manage VPN Server' interface for '172.30.1.15'. It includes a table for a 'Virtual Hub' named 'SPNBOXCLUSTER' and various management options.

Virtual Hub Name	Status	Type	Users	Groups	Sessions	MAC Tables	IP Ta
SPNBOXCLUSTER	Online	Static Hub	1	0	3	11	11

Below the table are buttons: 'Manage Virtual Hub' (highlighted with a red box), 'Online', 'Offline', 'View Status', 'Create a Virtual Hub', 'Properties', and 'Delete'.

The interface also includes sections for 'Management of Listeners' (Listener List (TCP/IP port)) and 'VPN Server and Network Information and Settings' (with icons for 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, and VPN Azure Setting).

At the bottom, it shows the current DDNS Hostname: `vpn290370780.softether.n`.

8. 인터넷 접속 차단(3)

Management of Virtual Hub - 'SPNBOXCLUSTER'

Virtual Hub 'SPNBOXCLUST...'

Management of Security Database:

- Manage Users**: Add, delete or edit user accounts.
- Manage Groups**: Add, delete or edit groups.
- Manage Access Lists**: Add or delete access lists (Packet filtering rules). **(Red Box)**

Current Status of this Virtual Hub:

Item	Value
Virtual Hub Name	SPNBOXCLUSTER
Status	Online
Type	Static Hub
Sessions	3
Sessions (Client)	0
Sessions (Bridge)	1
Access Lists	1
Users	1
Groups	0
MAC Tables	11

Virtual Hub Settings:

- Virtual Hub Properties**: Configure this Hub.
- Authentication Server Setting**: Use external RADIUS authentication server for user authentication.
- Manage Cascade Connections**: Establish Cascade Connection to Hubs on local or remote VPN Servers.

Other Settings:

- Log Save Setting**: Configure settings of log saving function.
- Trusted CA Certificates**: Manage trusted CA certificates.
- Virtual NAT and Virtual DHCP Server (SecureNAT)**: Secure NAT is available on this Virtual Hub. You can run Virtual NAT and Virtual DHCP.
- VPN Sessions Management**:

Exit

Edit Access List Item (IPv4)

Configure the access list settings. The access list that is defined here will be applied to all IP packets passing through the Virtual Hub.

Basic Settings

Memo:	Internet_Blocking
Action:	<input type="radio"/> Pass <input checked="" type="radio"/> Discard
Priority:	1000 (Smaller number has higher priority.)

Filtering Options for IP Headers

Source IP Address:	<input checked="" type="checkbox"/> Applies to All Source Addresses
IPv4 Address:	. . .
Subnet Mask:	. . .

(255.255.255.255 means a single host)

Destination IP Address: Applies to All Destination Addresses

IPv4 Address:	. . .
Subnet Mask:	. . .

(255.255.255.255 means Specified host only)

Protocol Type: 6 (TCP/IP Protocol)

Filtering Options for MAC Headers

Source MAC Address:	<input type="checkbox"/> Applies to any Source Addresses
MAC Address:	5E-34-21-FB-5F-F6
Mask:	FF-FF-FF-FF-FF-FF

Destination MAC Address: Applies to any Destination Addresses

MAC Address:	
Mask:	

You can use hexadecimal number with two separators, "-" or ":" , and without the separators.
(FF-FF-FF-FF-FF-FF means a specified host)

Filtering Options for TCP Headers and UDP Headers

Source Port:	-
Destination Port:	443 - 443

The blank port number field is also supported.
It will apply to packets that match only the minimum value when the minimum value is specified but the maximum value is not.

Verify TCP Connection State (Only TCP Packets)
 Established Packet Unestablished Packet

Redirect HTTP Request to Specific URL Delay and Packet Loss...

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

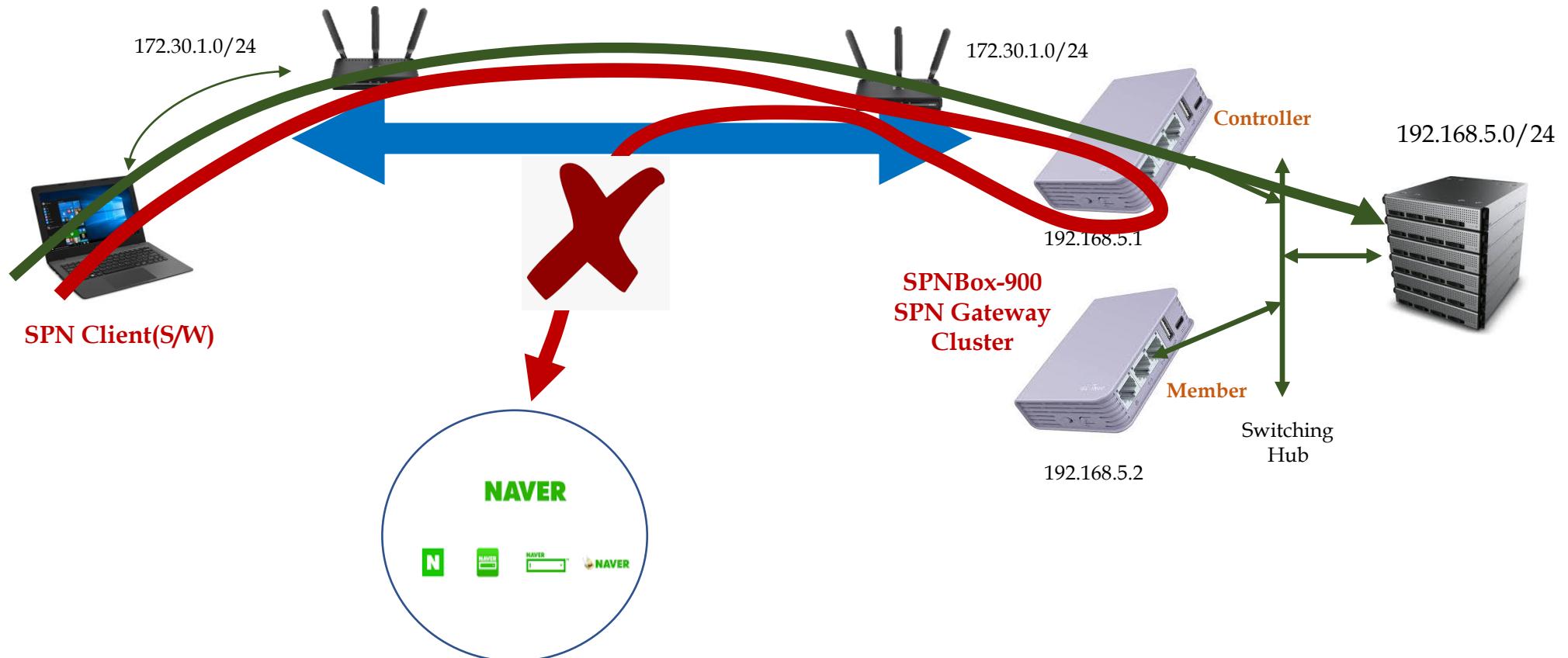
Items with higher priority appear higher in the list.

< >

Note: IP packets that did not match any access list items can pass.

Save **Cancel**

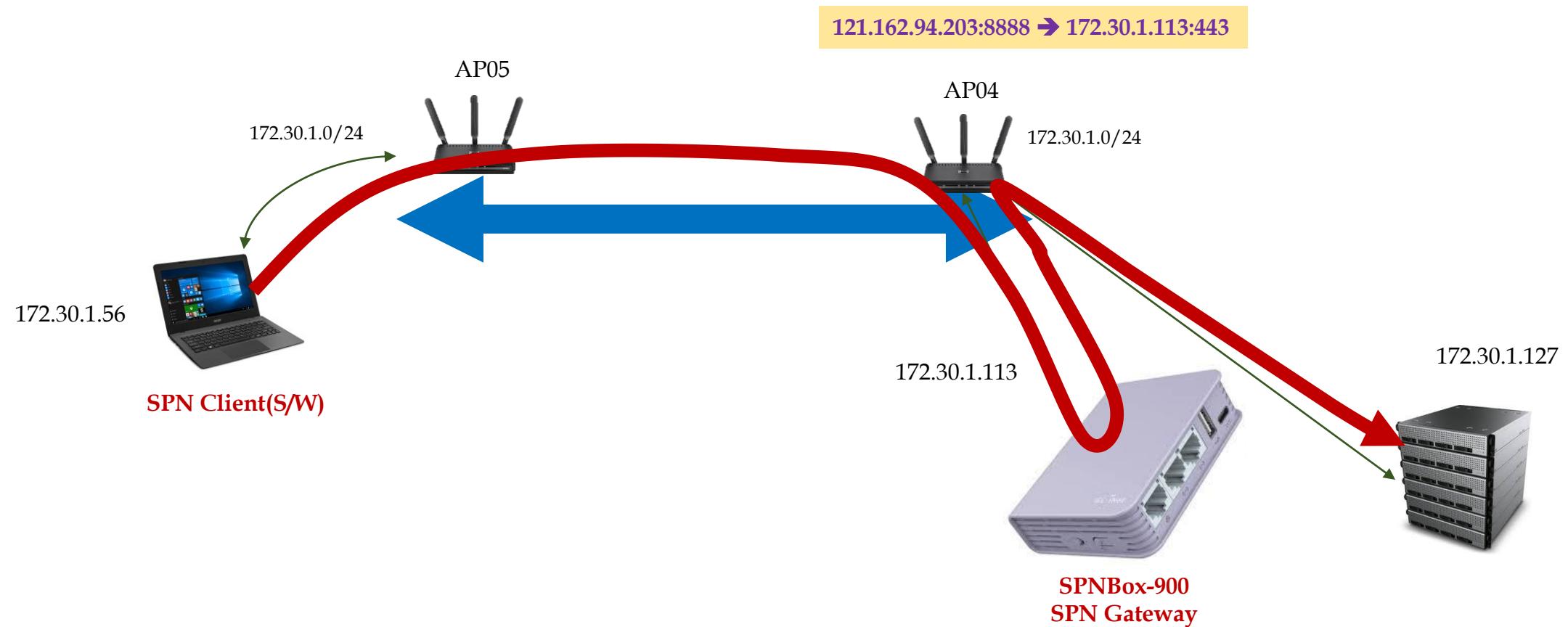
8. 인터넷 접속 차단(5)



9. Standalone Server : Setup Guide

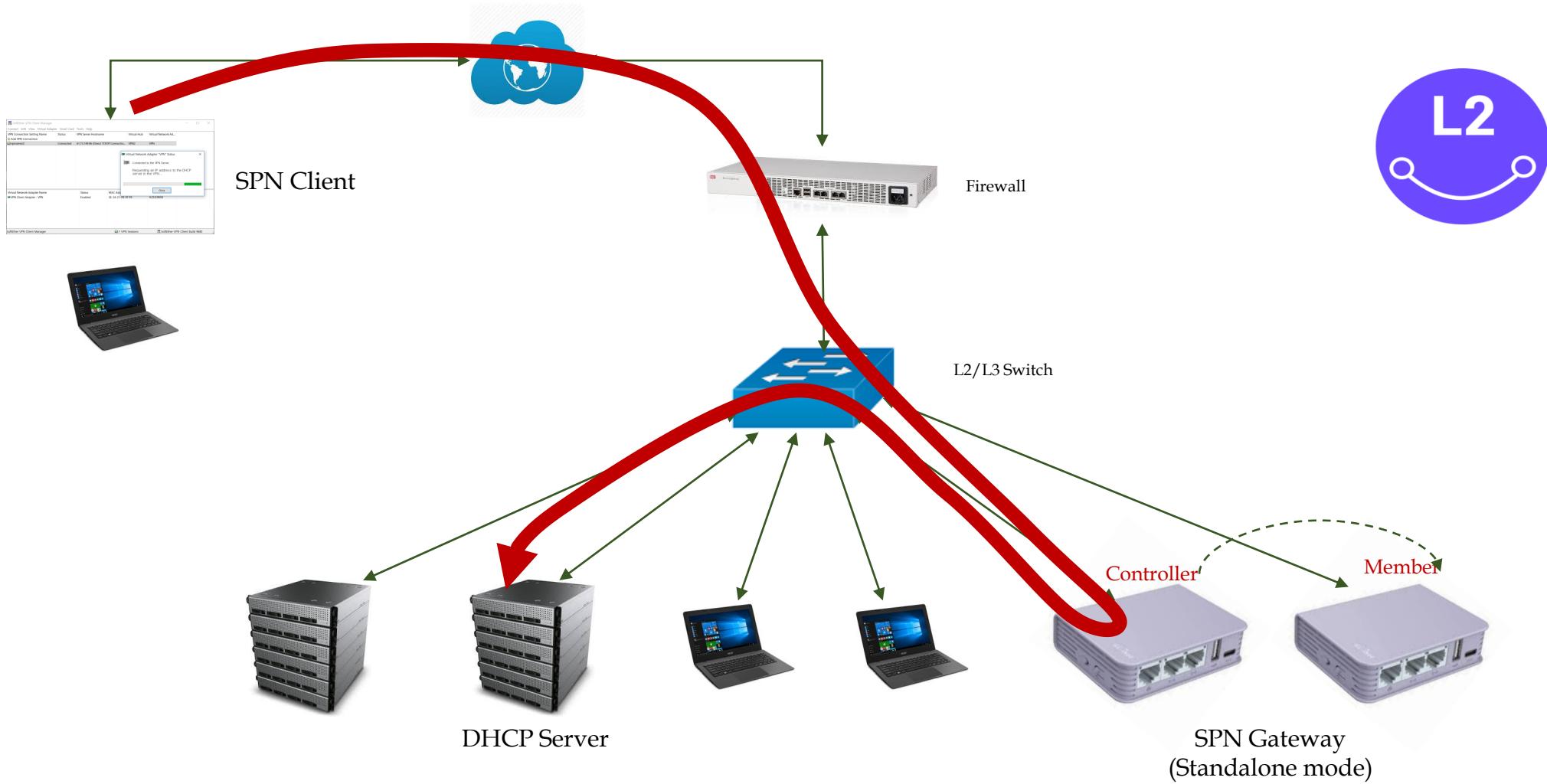
네트워크 관리 담당자가 네트워크 구성 변경에 난색을 표한다면

9. Standalone Server(1) - Testbed(1)



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

9. Standalone Server(1) - Testbed(2)

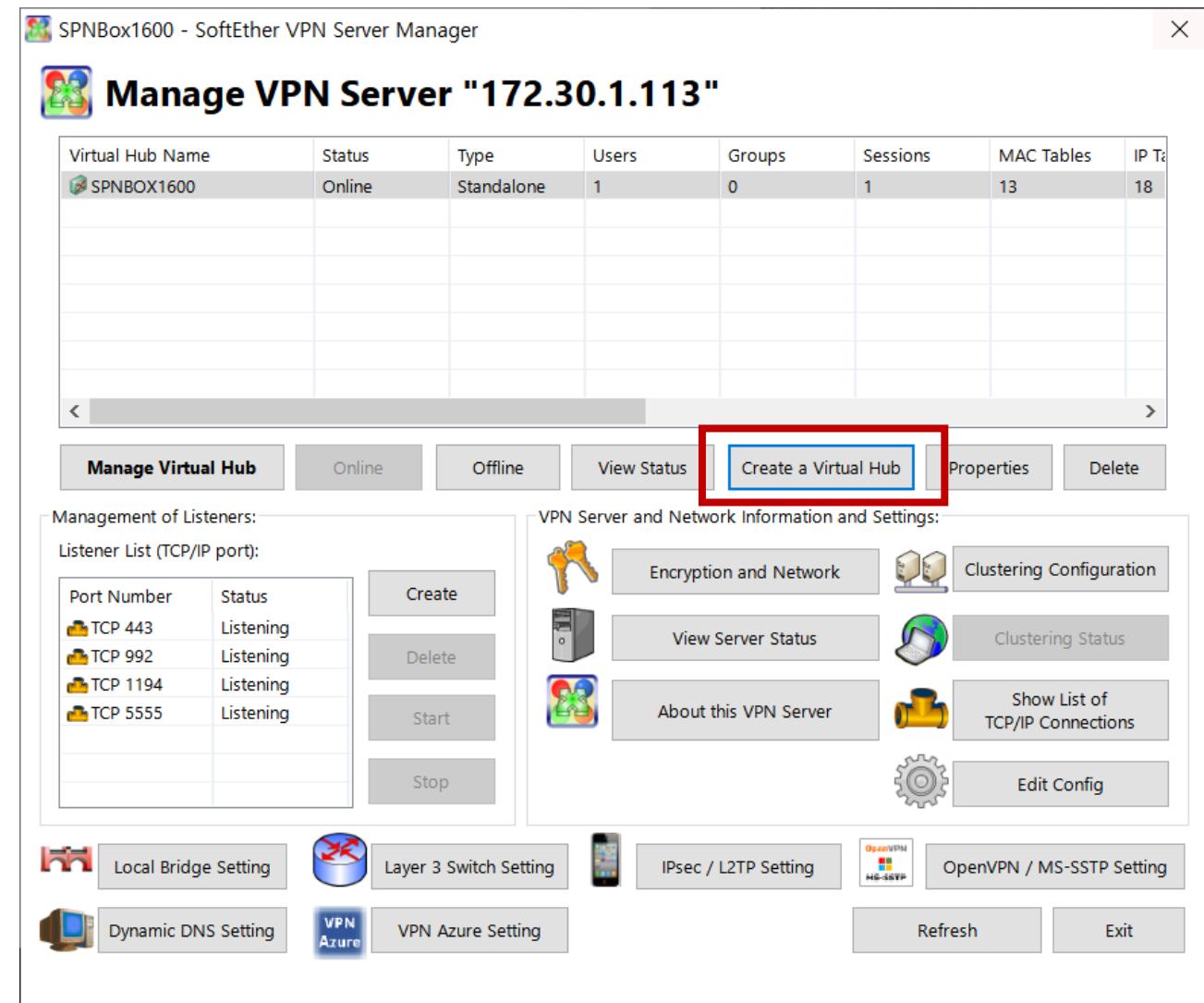
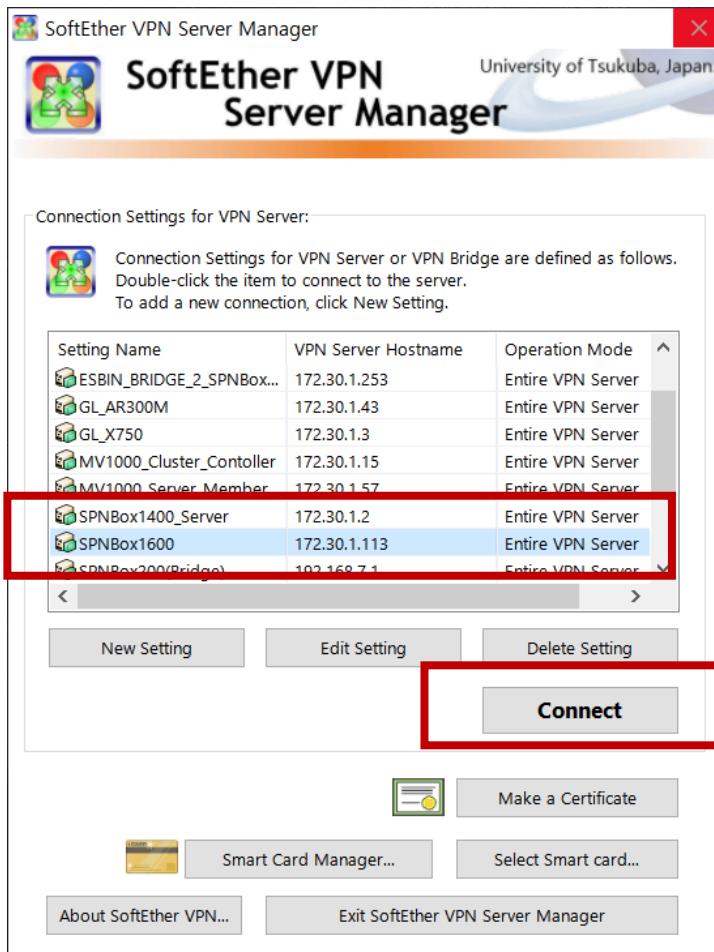


WAN Port만 사용하여 사내망에 연결

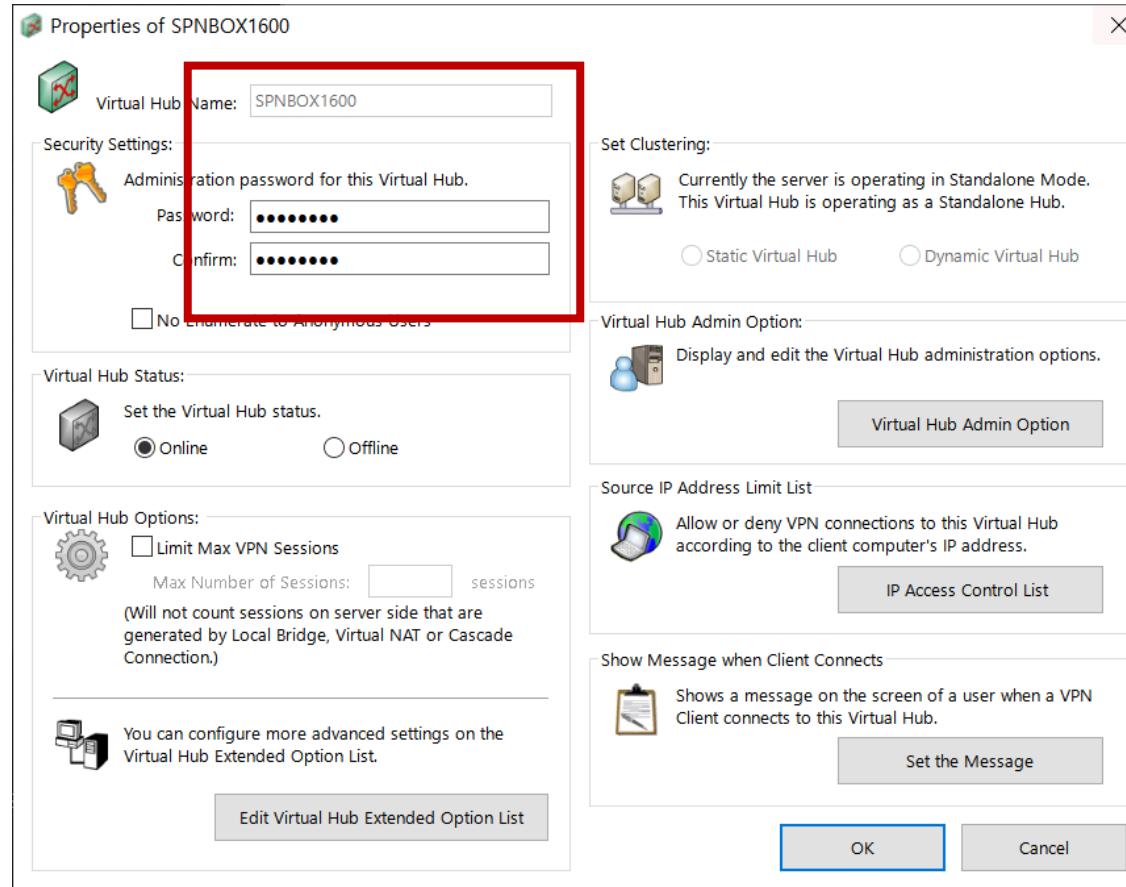
9. Standalone Server(2) - SPN Gateway 설정(1)

- <Standalone Server 설정 요약>
 - 1) SPN Gateway의 LAN port는 더 이상 사용하지 않으며, WAN port만을 사용하여 사무실 내부망에 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)



This interface shows the management of the Virtual Hub 'SPNBOX1600'. It features a sidebar with icons for managing users, groups, access lists, and cascade connections. A central panel displays the current status of the hub, including its name, status (Online), type (Standalone), and various statistics like session counts and user counts. On the right, there are sections for other settings like log saving and trusted CA certificates, and a 'VPN Sessions Management' section with a 'Manage Sessions' button.

Item	Value
Virtual Hub Name	SPNBOX1600
Status	Online
Type	Standalone
SecureNAT	Disabled
Sessions	1
Access Lists	0
Users	1
Groups	0
MAC Tables	13
IP Tables	18

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

The image displays three windows from a network management interface:

- Properties of User spnuser**: Shows basic user information (User Name: spnuser, Full Name: spn user, Note: spn user) highlighted with a red box. It also shows password authentication settings (Password: [REDACTED], Confirm Password: [REDACTED]) and individual certificate authentication settings.
- Security Policy**: A modal window showing the "Set Security Policy" button and a "Security Policy" button.
- Manage Users**: A table listing users in the Virtual Hub "SPNBOX1600". The table includes columns: User Name, Full Name, Group Name, Description, Auth Method, Num Logins, and Last Login. One row is highlighted with a red box, showing "spnuser" as the User Name, "spn user" as the Full Name, and "spn user" as the Description. The "Auth Method" column shows "Password Authen..." and "1" logins.

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

Local Bridge Settings

Local Bridge can establish a Layer 2 bridge connection between a Virtual Hub on this VPN server and a physical Ethernet Device (Network Adapter). It is also possible to create a tap device (virtual network interface) and establish a bridge connection with a Virtual Hub. (Tap is supported on Linux versions only)

Number	Virtual Hub Name	Network Adapter or Tap Device Name	Status
< 1 >	SPNBOX1600	ens37	Operating

New New Local Bridge Definition:

Select the Virtual Hub to bridge.
Virtual Hub: SPNBOX1600

Type to Create: Bridge with Physical Existing Network Adapter
 Bridge with New Tap Device

Select the Ethernet device (network adapter) for the bridge destination.
LAN Adapter: ens37

Note: Although it is possible to establish a bridge using any operating network adapter, in high load environments, you should prepare a network adapter dedicated for bridging.

If a network adapter doesn't appear which is recently added on the system, reboot the computer and re-open this screen.

Create Local Bridge

Exit

Local Bridge Settings

Local Bridge can establish a Layer 2 bridge connection between a Virtual Hub on this VPN server and a physical Ethernet Device (Network Adapter). It is also possible to create a tap device (virtual network interface) and establish a bridge connection with a Virtual Hub. (Tap is supported on Linux versions only)

Number	Virtual Hub Name	Network Adapter or Tap Device Name	Status
< 1 >	SPNBOX1600	ens37	Operating

New New Local Bridge Definition:

Select the Virtual Hub to bridge.
Virtual Hub: [empty]

Type to Create: Bridge with Physical Existing Network Adapter
 Bridge with New Tap Device

Select the Ethernet device (network adapter) for the bridge destination.
LAN Adapter: ens37

New Tap Device Name: [empty] (Maximum 11 Characters)

Note: Although it is possible to establish a bridge using any operating network adapter, in high load environments, you should prepare a network adapter dedicated for bridging.

If a network adapter doesn't appear which is recently added on the system, reboot the computer and re-open this screen.

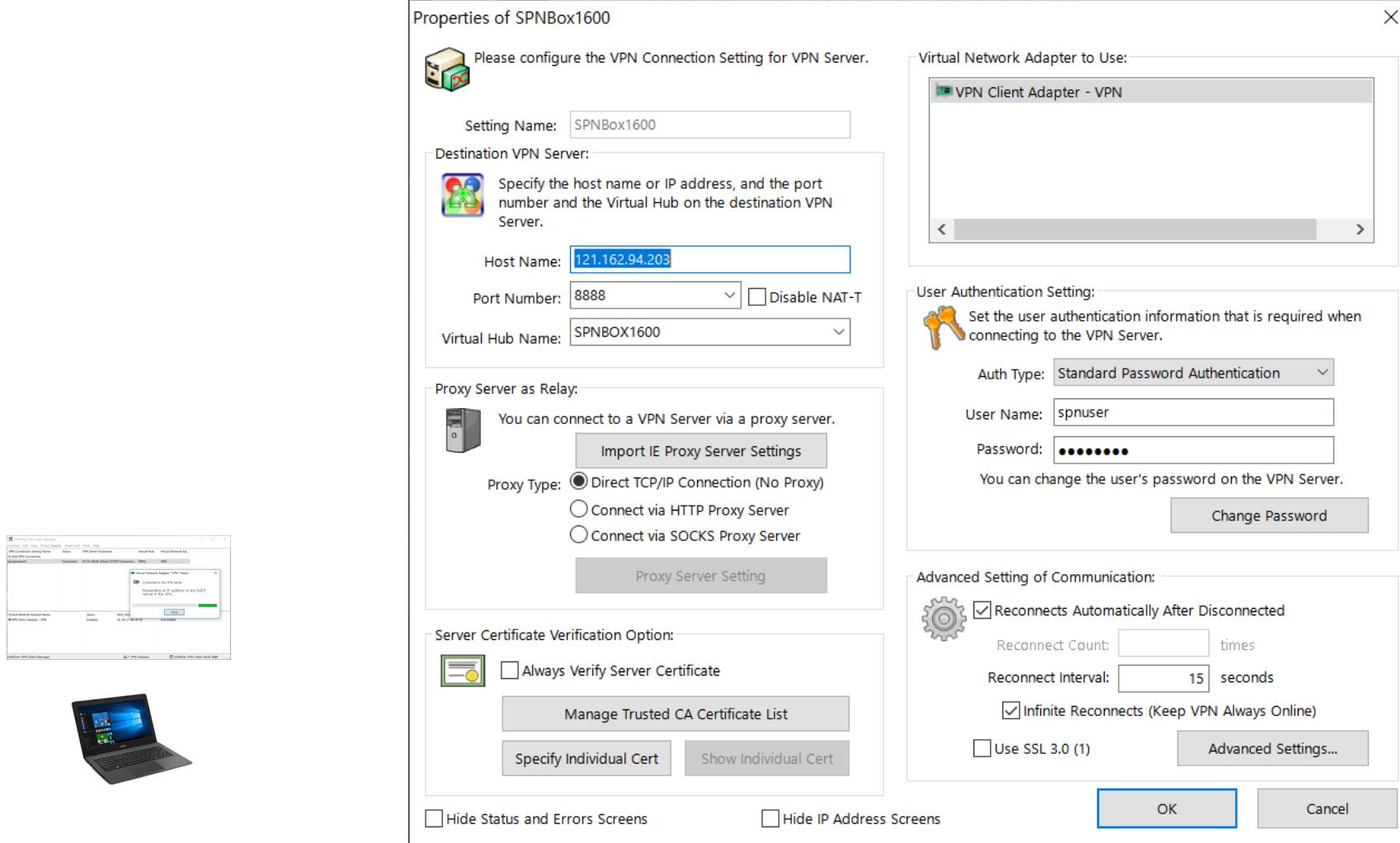
Create Local Bridge

Exit

WAN Port 선택

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

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



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

```
C:\ 명령 프롬프트

알 수 없는 어댑터 VPN - VPN Client:

연결별 DNS 접미사 . . . . . : 미디어 상태 . . . . . : 미디어 연결 끊김
링크-로컬 IPv6 주소 . . . . . : fe80::e512:fe76:533b:d01%13
IPv4 주소 . . . . . : 172.30.1.56
서브넷 마스크 . . . . . : 255.255.255.0
기본 게이트웨이 . . . . . : 172.30.1.254

이더넷 어댑터 VirtualBox Host-Only Network:

연결별 DNS 접미사 . . . . . : 미디어 상태 . . . . . : 미디어 연결 끊김
링크-로컬 IPv6 주소 . . . . . : fe80::b952:4c9b:8967:406c%17
자동 구성 IPv4 주소 . . . . . : 169.254.64.108
서브넷 마스크 . . . . . : 255.255.0.0
기본 게이트웨이 . . . . . :

무선 LAN 어댑터 로컬 영역 연결* 5:

미디어 상태 . . . . . : 미디어 연결 끊김
연결별 DNS 접미사 . . . . . :

무선 LAN 어댑터 로컬 영역 연결* 7:

미디어 상태 . . . . . : 미디어 연결 끊김
연결별 DNS 접미사 . . . . . :

이더넷 어댑터 ethernet2:

미디어 상태 . . . . . : 미디어 연결 끊김
연결별 DNS 접미사 . . . . . :
```

```
C:\ 명령 프롬프트

미디어 상태 . . . . . : 미디어 연결 끊김
연결별 DNS 접미사 . . . . . :

무선 LAN 어댑터 Wi-Fi:

연결별 DNS 접미사 . . . . . : 미디어 상태 . . . . . : 미디어 연결 끊김
링크-로컬 IPv6 주소 . . . . . : fe80::241e:c18:8949:1b58%10
IPv4 주소 . . . . . : 172.30.1.2
서브넷 마스크 . . . . . : 255.255.255.0
기본 게이트웨이 . . . . . :

이더넷 어댑터 Bluetooth 네트워크 연결:

미디어 상태 . . . . . : 미디어 연결 끊김
연결별 DNS 접미사 . . . . . :

C:\#Users\Chunghan Yi>
C:\#Users\Chunghan Yi>ping 172.30.1.254

Ping 172.30.1.254 32바이트 데이터 사용:
172.30.1.254의 응답: 바이트=32 시간=7ms TTL=64
172.30.1.254의 응답: 바이트=32 시간=3ms TTL=64
172.30.1.254의 응답: 바이트=32 시간=2ms TTL=64
172.30.1.254의 응답: 바이트=32 시간=3ms TTL=64

172.30.1.254에 대한 Ping 통계:
패킷: 보낸 = 4, 받음 = 4, 손실 = 0 (0% 손실),
왕복 시간(밀리초):
최소 = 2ms, 최대 = 7ms, 평균 = 3ms

C:\#Users\Chunghan Yi>
```

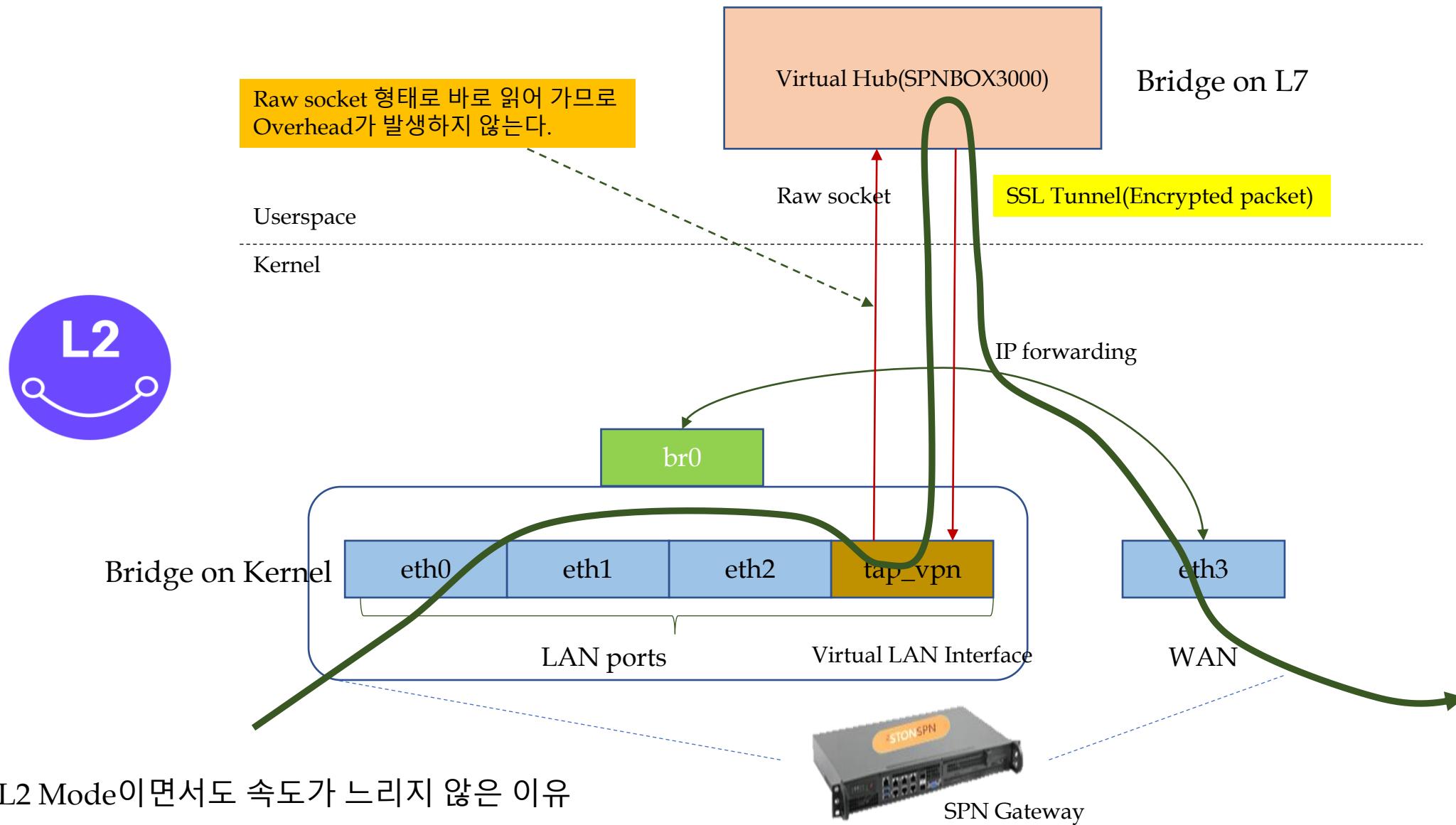
- VPN 연결 결과, Windows PC의 IP 주소가 AP04 망의 172.30.1.56를 할당 받았으며, 같은 망 내의 다른 IP 주소와도 통신에 무리가 없음을 알 수 있다.

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

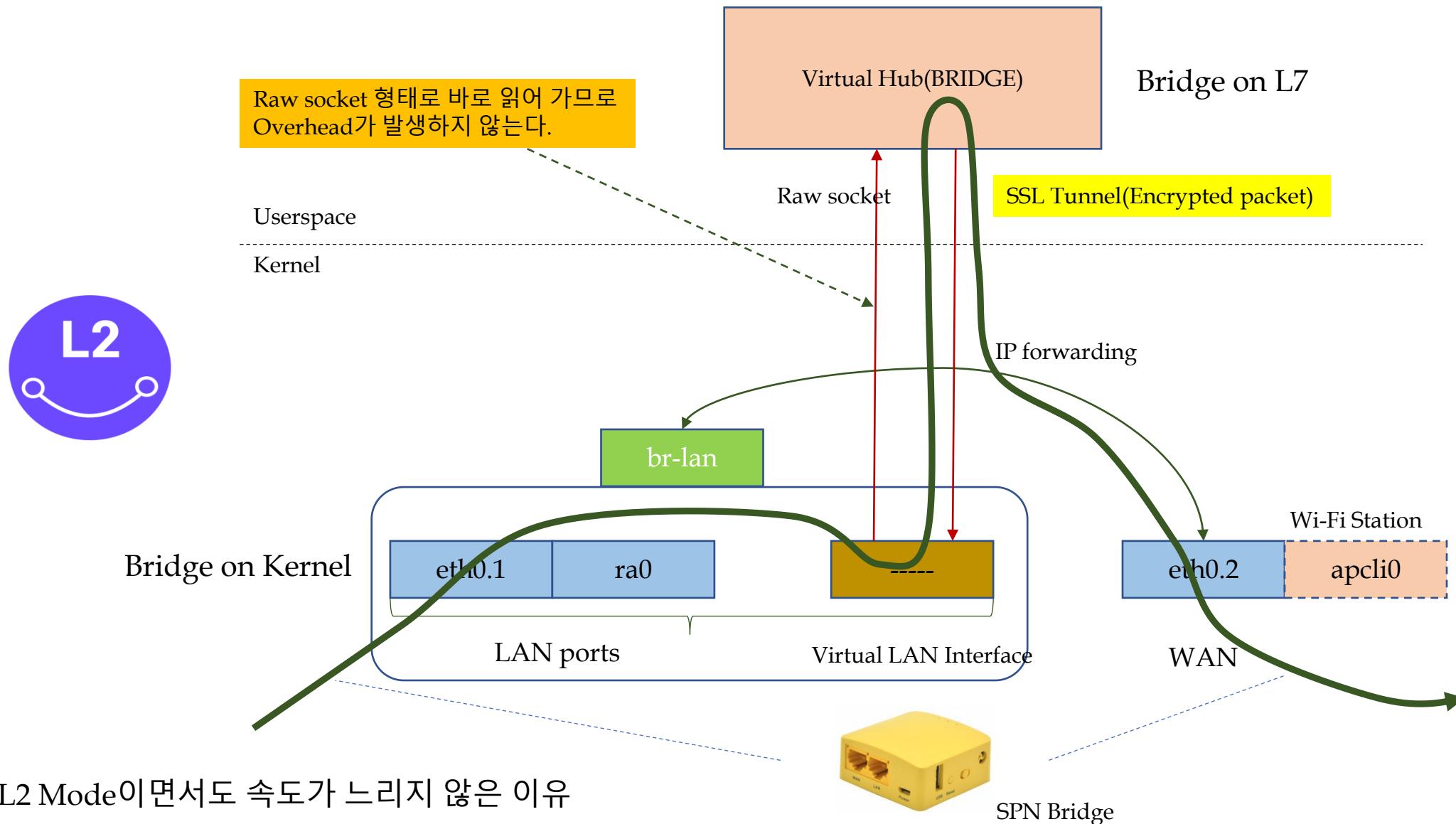
- <인터넷 연결 속도>
 - 역시 예상했던 대로, 인터넷 접속시 약간의 delay가 있는 것으로 보인다.

10. L2 SPN Internal Architecture

10. L2 SPN Internal Architecture(1)

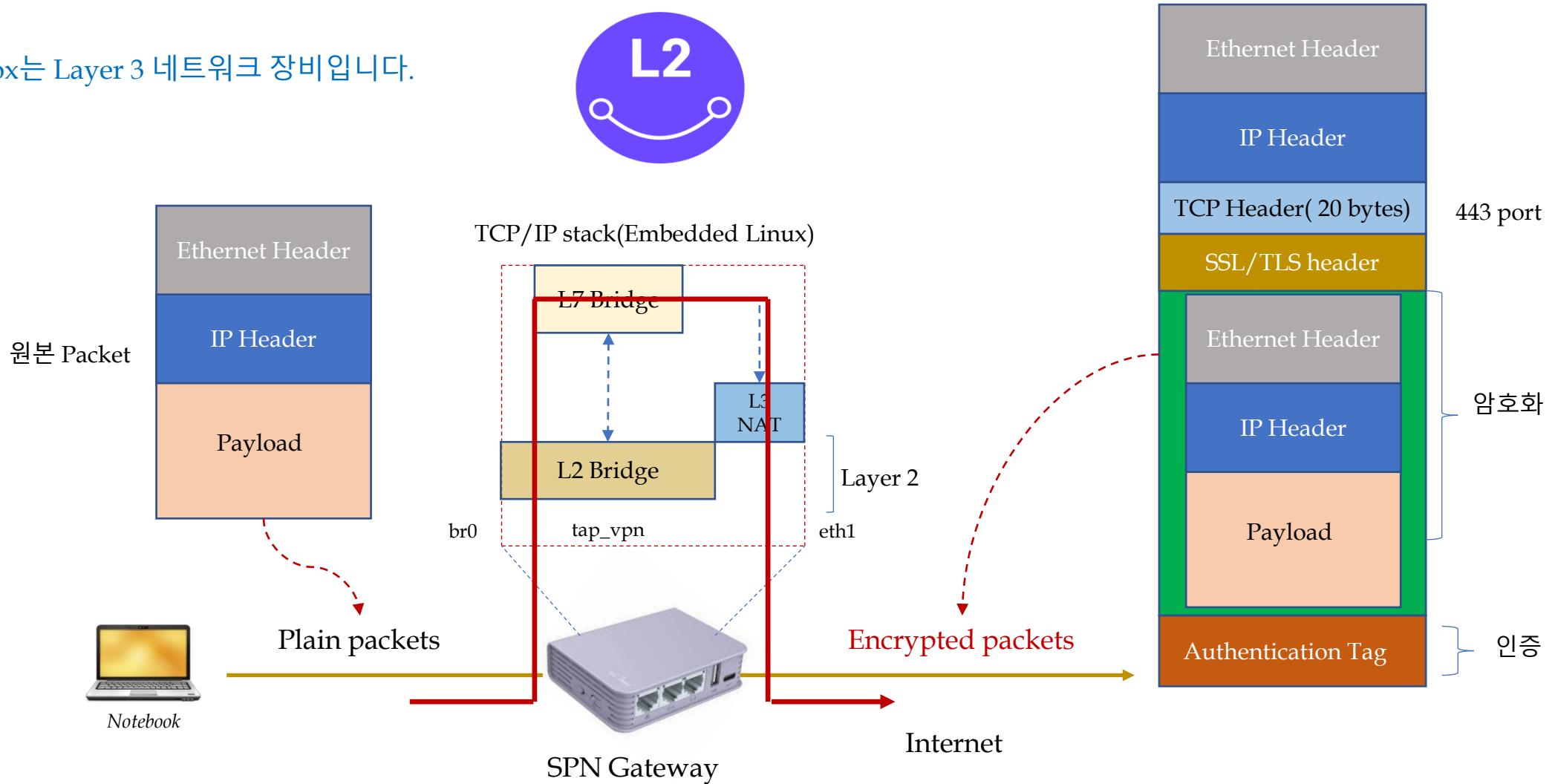


10. L2 SPN Internal Architecture(2)

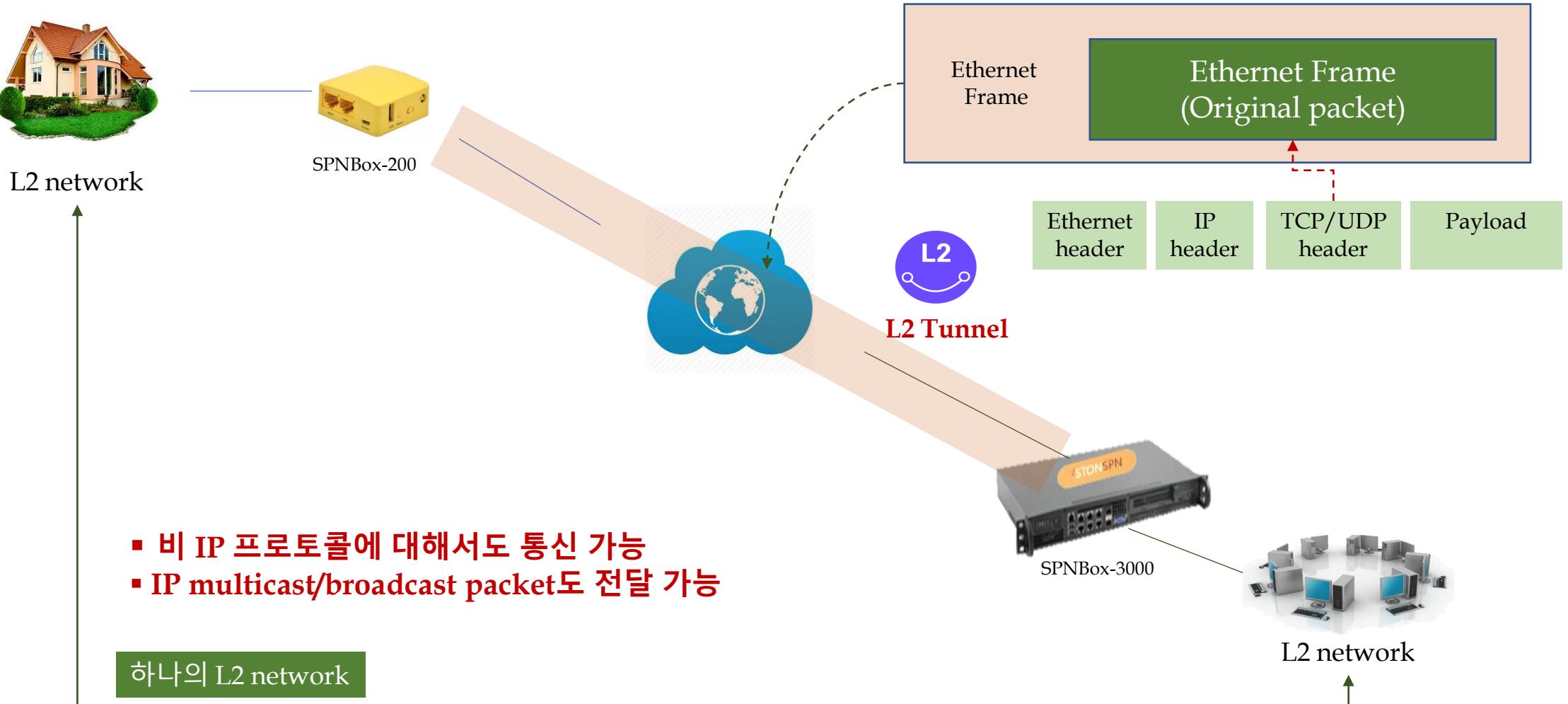


10. L2 SPN Internal Architecture(3)

SPNBox는 Layer 3 네트워크 장비입니다.

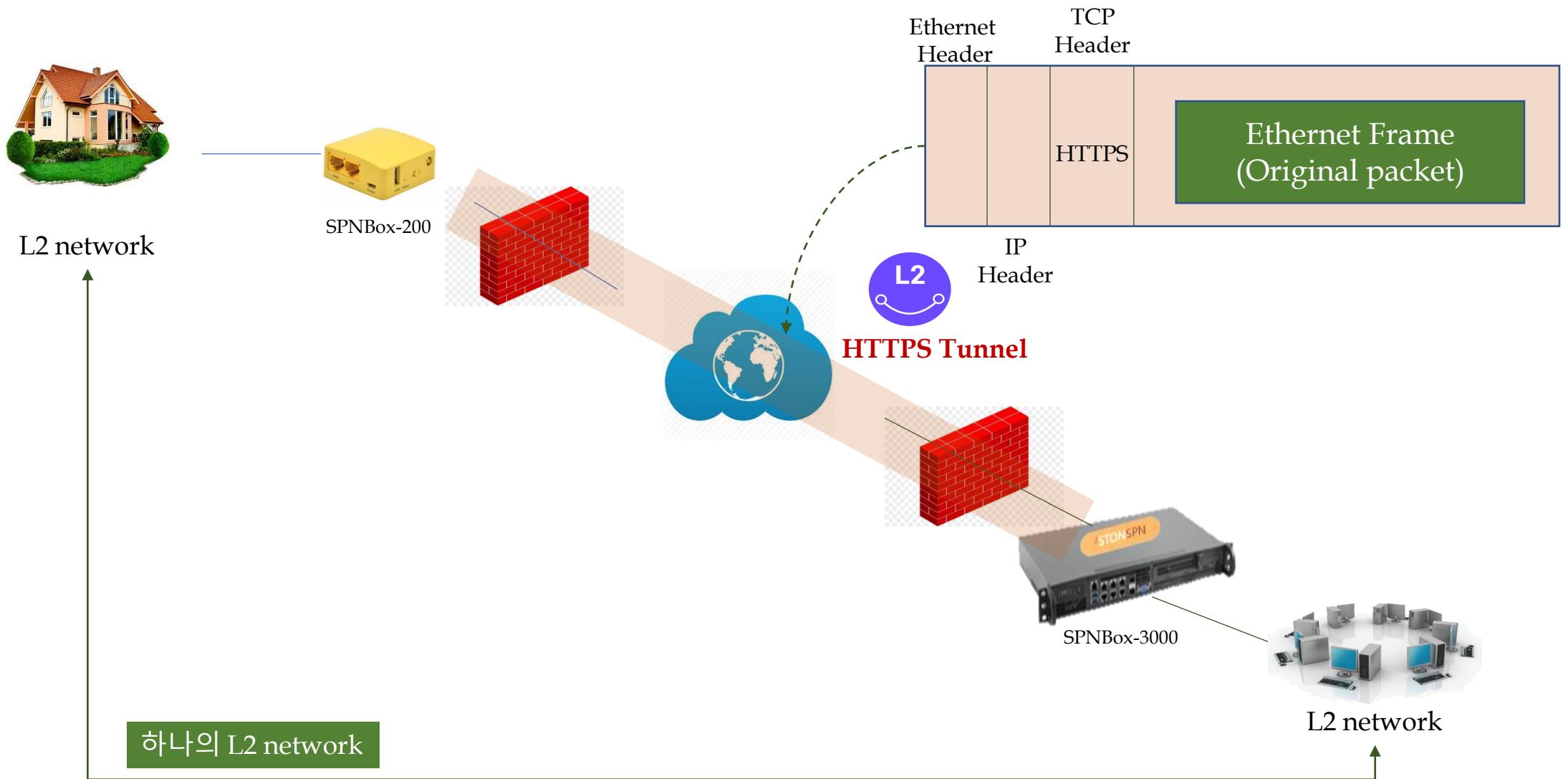


10. L2 SPN Internal Architecture(4)



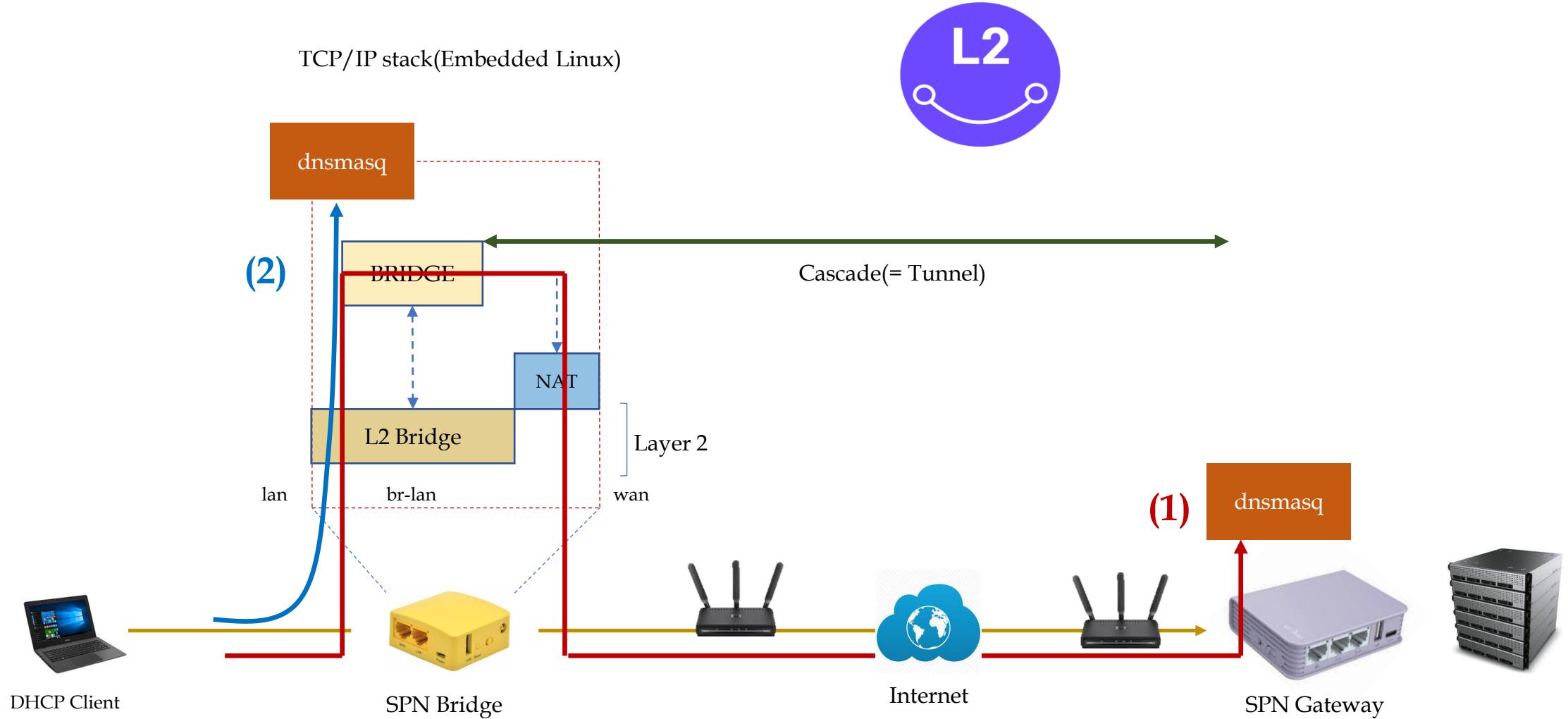
L2 SPN 기능을 사용하면, L2 packet(Windows NETBEUI, DHCP, ARP, Broadcast 등)을 안전하게 실어 나를 수 있습니다.

10. L2 SPN Internal Architecture(5)



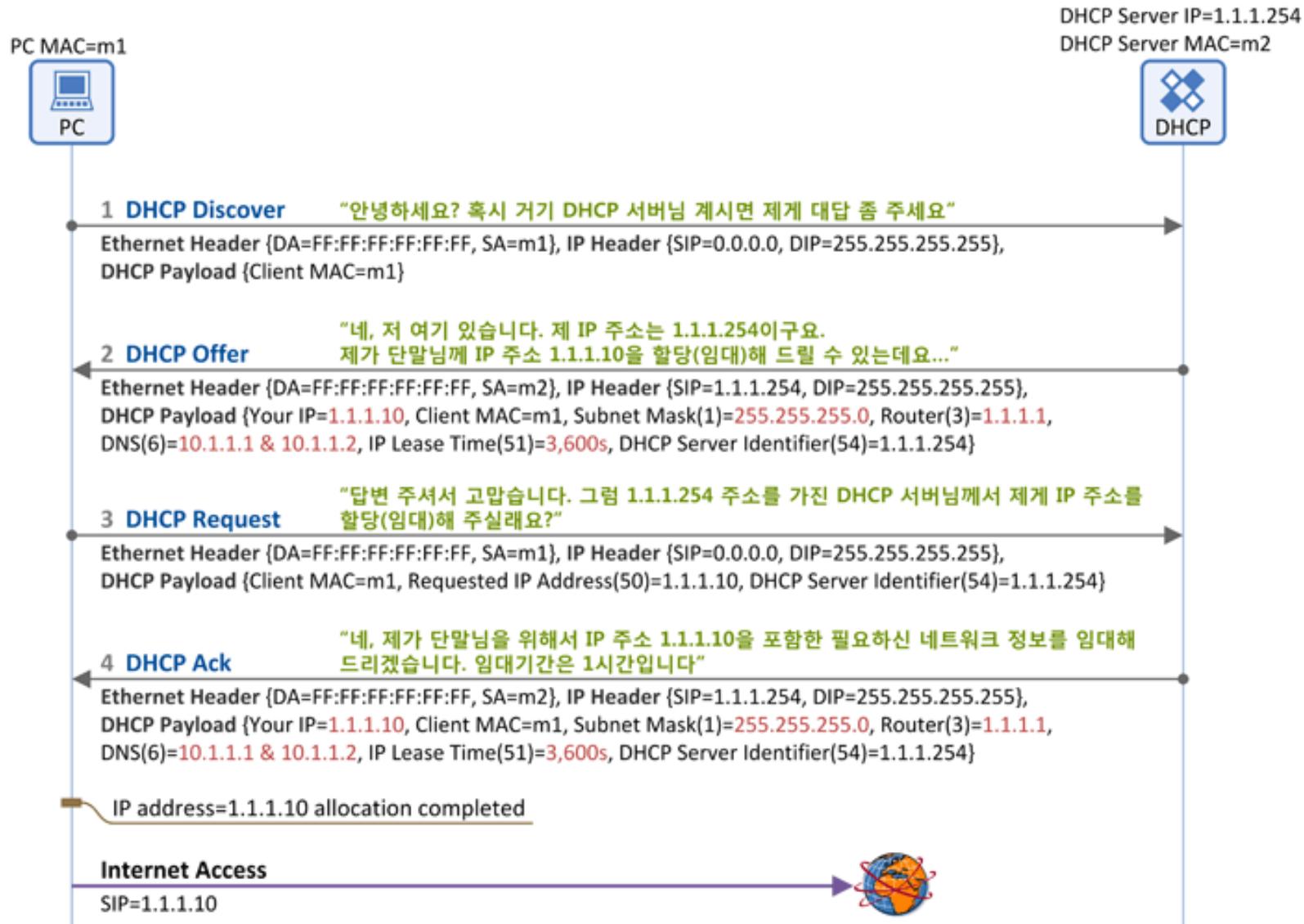
HTTPS Tunnel(a.k.a SSL Tunnel)은 방화벽을 통과하는데 있어 자유롭습니다.

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

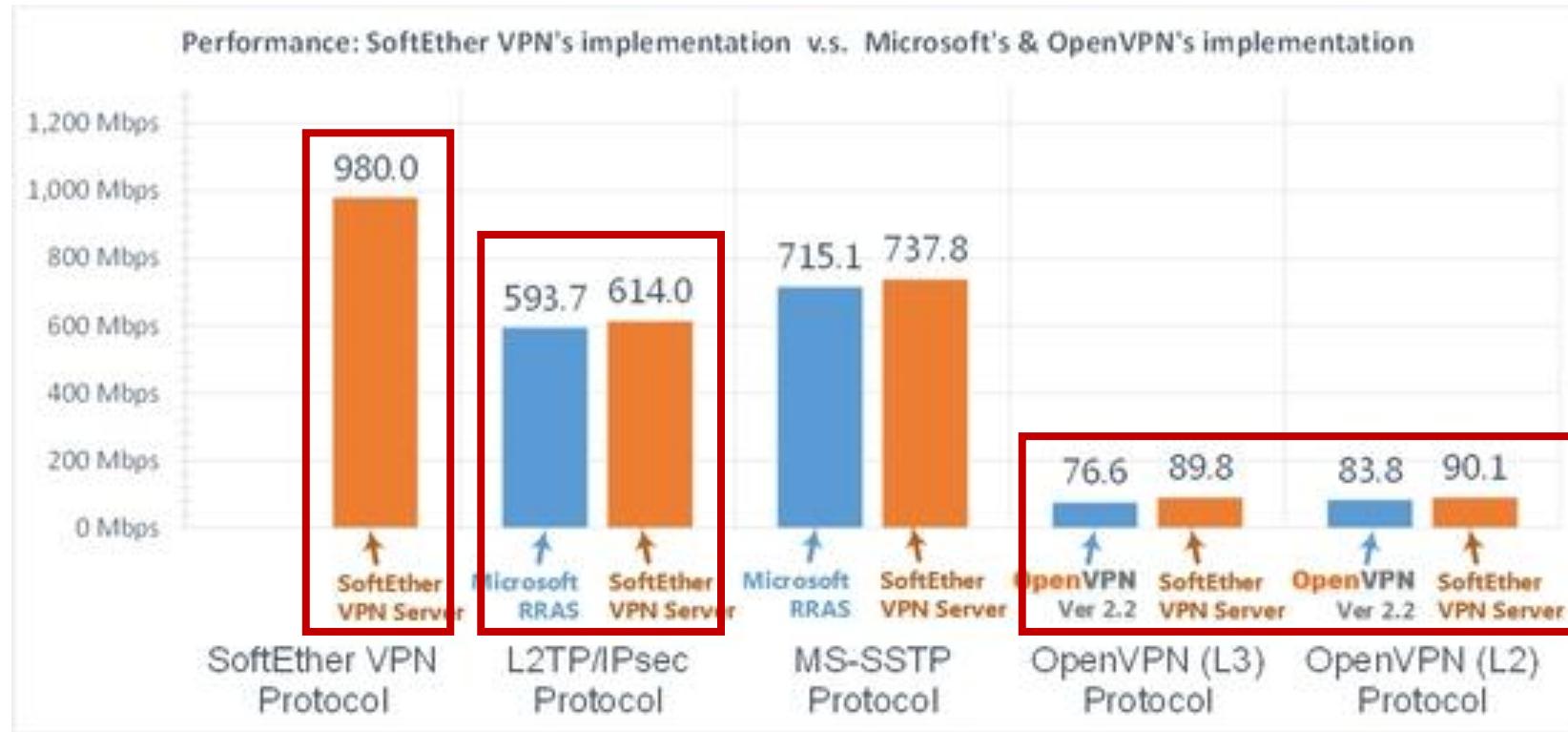


(1), (2) 부분에서 race condition이 발생할 수 있다. 이 경우 static ip 설정을 해 주면 VPN 사용에 문제가 없다.

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™