2ip SPN 재택근무 Solution

March 20, 2020

2ip SPN 이란 ?

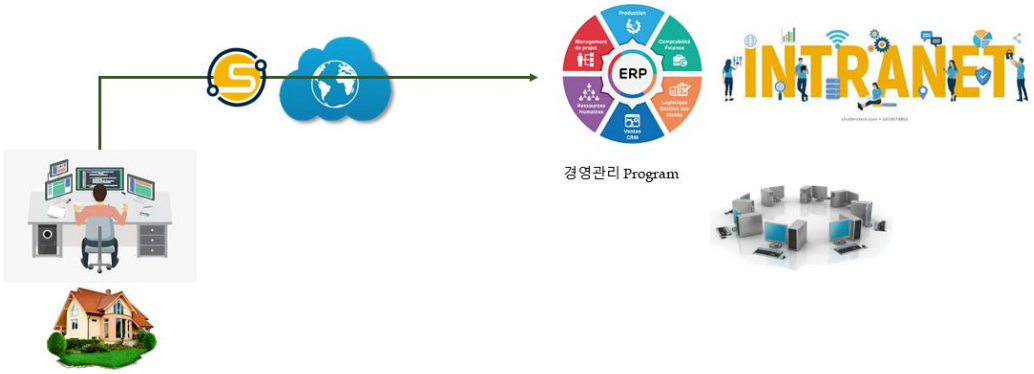
신종 코로나 바이러스 감염증(코로나19) 사태가 장기화되면서 재택근무를 시행하는 기업이 점점 늘어나고 있습니다. 재택근무는 출퇴근에 드는 비용과 시간이 절감되는 등의 장점도 있지만, 직원간 의사소통이 원활하지 않고 사생활과 업무 분리가 안 돼 힘들다는 문제가 있습니다. **2ip SPN**은 이와 같은 비상 상황에서 보다 효과적인 재택근무가 이루어질 수 있도록 도와주는 **L2 기술 기반의 가상 사설망 솔루션**입니다.

"집에 있으나, 마치 아주 긴 LAN 선을 사용하여 회사망에 직접 연결한 것과 같은 효과..."

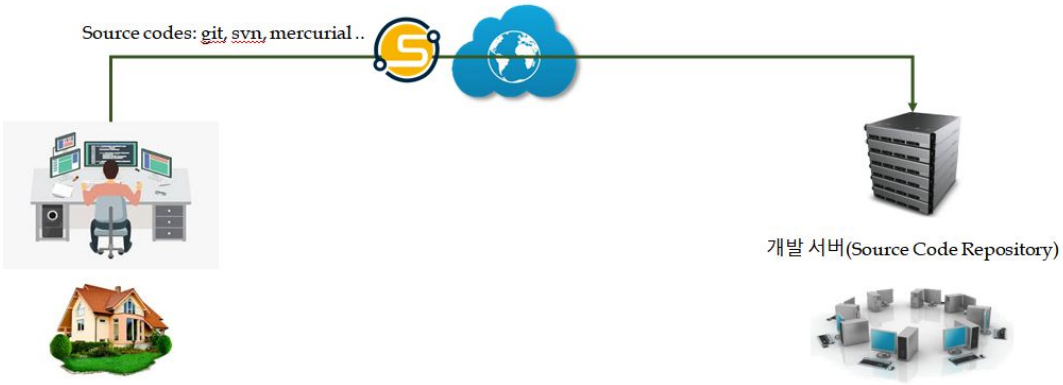
참고: SPN은 Secure Private Network, Secure Point-to-point Network을 의미함.

왜 2ip SPN을 사용해야 하나 ?

2ip SPN은 실제로는 집에 있지만, 마치 회사에 출근한 것처럼 회사망에 자유롭게 접근하도록 만들어 주는 역할을 수행합니다. 이제 집에 편하게 앉아서 사내망(Intranet)의 ERP 서버, CRM 서버, 개발 서버(git, svn, mercurial), File 서버, DBMS, 프린터 등에 안전하고 자유롭게 접근하실 수 있습니다. 모든 서버 접속시에는 사용자 인증을 거치게 되며, 인증을 통과한 패킷은 강력한 암호 알고리즘을 통해 안전하게 암호화됩니다.

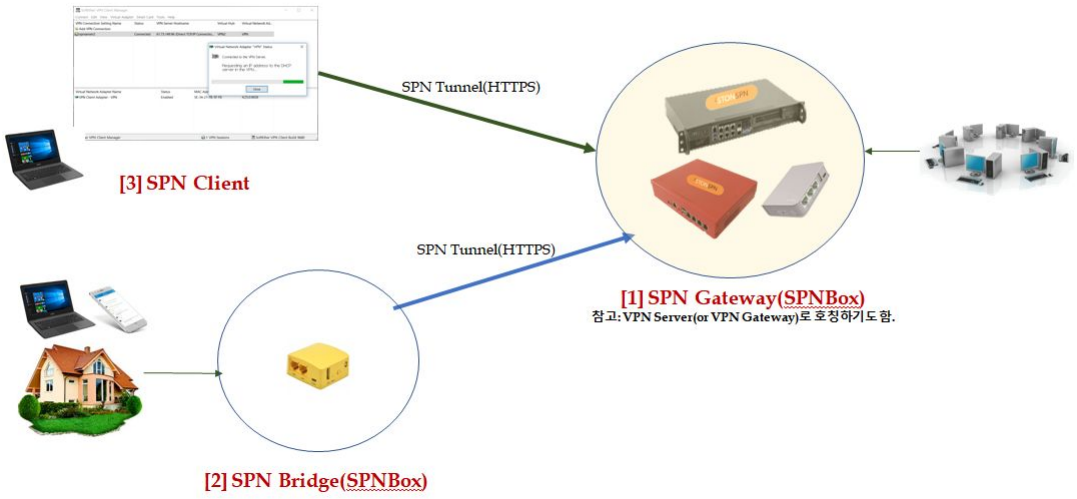


- 2ip SPN을 사용하여 사내 ERP 서버에 안전하게 접속 -



- 2ip SPN을 사용하여 사내 개발 서버에 안전하게 접속 -

2ip SPN은 사내 망의 중요 서버 앞단에 설치하는 **SPN Gateway**와 재택근무자가 사용하는 **SPN Bridge** 및 **SPN Client**로 구성되어 있습니다. SPN Bridge는 복수개의 PC(혹은 Moblie Phone)가 있는 경우에 사용하며, SPN Client는 Windows OS 상에 단독 설치하여 사용하게 됩니다.



- 2ip SPN 제품 구성 : SPN Gateway/Bridge/Client -

2ip SPN을 사용해야 하는 이유

1. 2ip SPN은 집과 사무실을 완벽히 동일한 하나의 망(사무실 LAN과 동일한 LAN으로 만들어 줌)으로 만들어 줍니다.
2. 2ip SPN은 VPN(가상 사설망) 환경을 이미 갖춘 대기업 & 금융권 보다는 중소기업을 대상으로 합니다. 따라서 기업의 규모에 맞는 합리적인 가격을 보장(제공)합니다.
3. 2ip SPN은 높은 보안성(SSL Tunnel)을 자랑하며, 빠른 속도(IPSec, OpenVPN 대비)와 안정성을 제공합니다.
4. 2ip SPN은 사용이 매우 쉽고 편리하게 설계되어 있습니다.

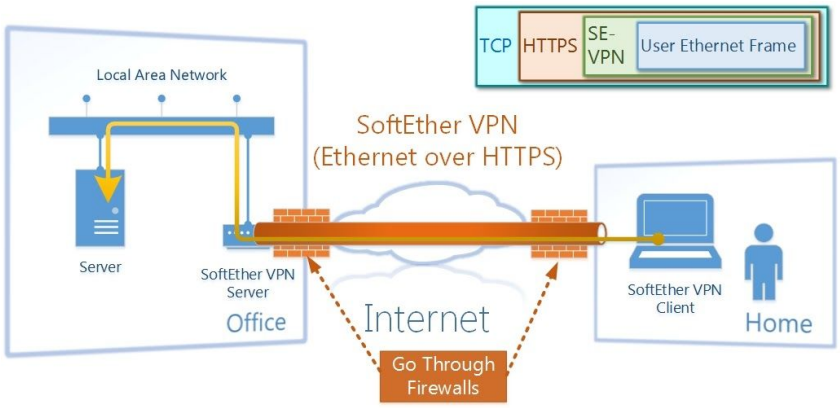
동작 원리 및 특장점

2ip SPN(L2 SPN)은 인터넷을 통해 원본 이더넷 패킷(ethernet packet)을 안전하게 실어 나를 수 있도록 설계되어 있습니다. 이는 Unicast IP protocol 만을 전달하는 방식(예: IPsec)과 비교해, 비 IP protocol(예: Windows NETBEUI, ARP packets)은 물론이고 Multicast & Broadcast IP 패킷(예: DHCP protocol)도 전달할 수 있는 이점을 제공하게 됩니다.

특장점

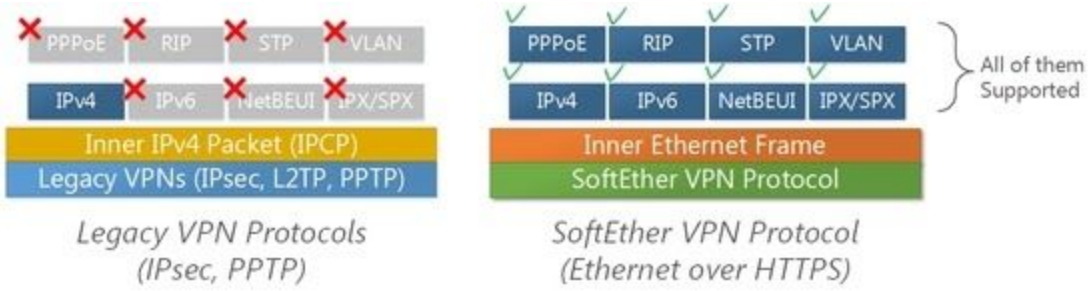
1. **쉬운 연결** : 2ip SPN은 상대편(SPN Gateway)의 IP 주소와 포트 및 사용자 계정 정보만을 입력하면 되므로, 매우 편리하고 간단하게 사내 망의 서버에 접근할 수 있습니다.

2. **SSL Tunnel 방식** : 2ip SPN은 Firewall(NAT) 장비를 쉽게 통과하기 위해 HTTPS 프로토콜에 기반한 SSL Tunnel 방식을 사용합니다.



- SSL Tunnel을 이용한 원본 이더넷 패킷 전송 -

3. **L2 Tunnel** : 2ip SPN이 터널을 통해 전달 가능한 프로토콜로는 IPv4 (TCP, UDP, ICMP, ESP, GRE etc.), IPv6, NetBEUI, IPX/SPX, PPPoE, RIP, STP, VLAN 등 모든 이더넷 기반 프로토콜과 사용자가 특수한 목적으로 정의하여 사용하는 프로토콜 까지 입니다.



- L2 Tunnel 방식이라 모든 이더넷 패킷 전달 가능 -

참고: IEEE802.1Q Tagged VLAN packet 패킷도 전송 가능함. 심지어 VLAN tag를 추가하거나 삭제할 수도 있음.

4. **다양한 암호 알고리즘** : 2ip SPN은 RC4-MD5, RC4-SHA, AES128-SHA, AES-256-SHA, DES-CBC-SHA, DES-CBC3-SHA, DHE-RSA-AES128-SHA, DHE-RSA-AES256-SHA, AES128-GCM-SHA256, AES128-SHA256, AES256-GCM-SHA384, AES256-SHA256, DHE-RSA-AES128-GCM-SHA256, DHE-RSA-AES128-SHA256, DHE-RSA-AES256-GCM-SHA384, DHE-RSA-AES256-SHA256, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES128-SHA256,

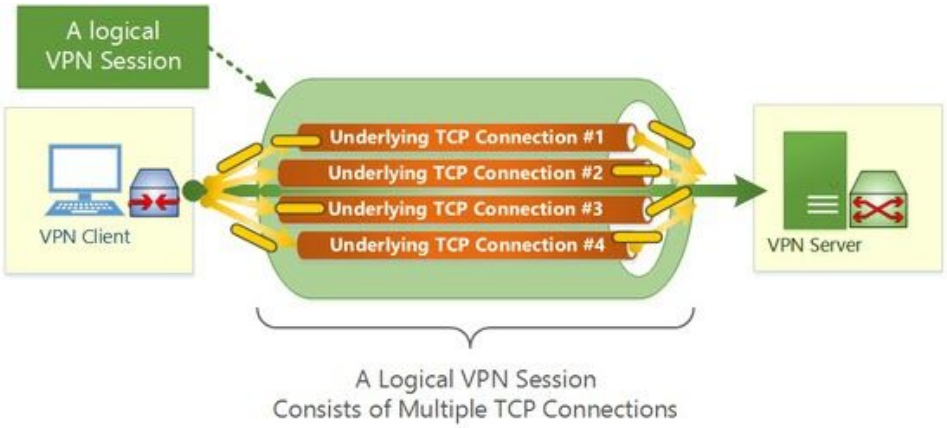
ECDHE-RSA-AES256-GCM-SHA384, ECDHE-RSA-AES256-SHA384 등의 다양한 암호/해쉬 알고리즘을 제공합니다.

5. **강력한 사용자 인증** : 2ip SPN은 단순 패스워드 인증, Radius 서버를 통한 인 증 및 X.509 인증서를 이용한 사용자 인증 기능을 지원합니다.

6. **OpenVPN & L2TP/IPsec 클론 기능** : 2ip SPN은 SPN Gateway 내부에 OpenVPN 서버 및 L2TP/IPsec 클론 기능이 포함되어 있어, OpenVPN 및 L2TP/IPsec Client를 이용하여 접근이 가능합니다. 이는 Smart Phone 사용자가 LTE 망을 통해 바로 사내망에 접근하는 것을 도와 줍니다.

7. **실시간 로그 및 접근 통제** : 2ip SPN은 실시간 로그 출력, 사용자별 접근 통제(날짜/시간대 통제 가능), 패킷 필터(IP 주소, 포트, User/Group 지정 가능) 기능 및 다양한 공격 감지 & 차단 기능 등을 제공합니다.

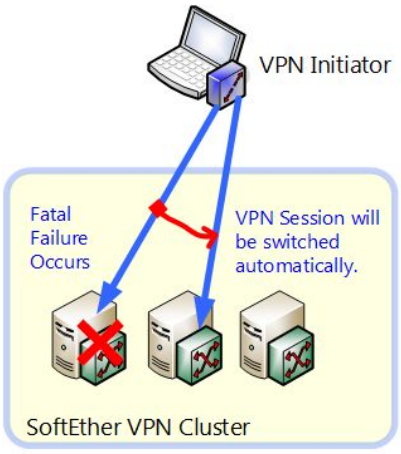
8. **빠른 성능과 안정성** : 2ip SPN은 이더넷 최대 크기(1514 bytes) 패킷 전송 시 MTU 문제로 패킷이 둘로 쪼개지는 문제를 해결하기 위해 독자적인 알고리즘을 채용한 덕택에, MTU 초과시 패킷이 쪼개지는 문제가 사라지게 되므로 빠른 성능을 보장할 수 있습니다. 또한 HTTPS Tunnel 연결이 끊길 경우, 또 다른 HTTPS connection(연결)으로 신속히 전환하여 터널의 안정성 및 성능을 확보해 줍니다.



- 하나의 논리적인 VPN 터널은 복수개의 TCP connection으로 구성 -

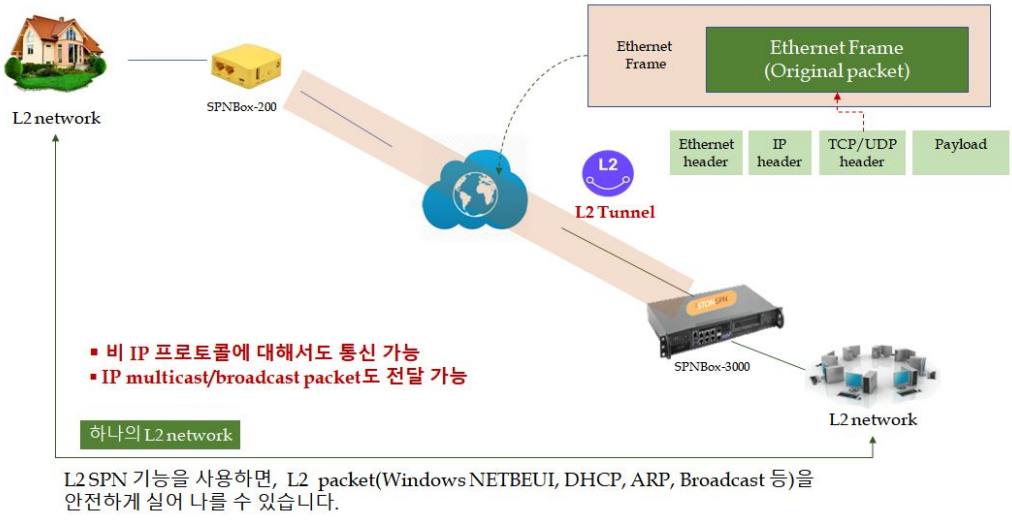
참고: MTU는 Maximum Transmission Unit의 줄임말임. 이더넷의 경우 한번에 최대 1514 bytes를 전송할 수 있음.

9. 2ip SPN은 저 사양의 SPN Gateway를 여러개 묶어 마치 하나의 커다란 SPN Gateway로 만들어 주는 Clustering 기능을 제공합니다.



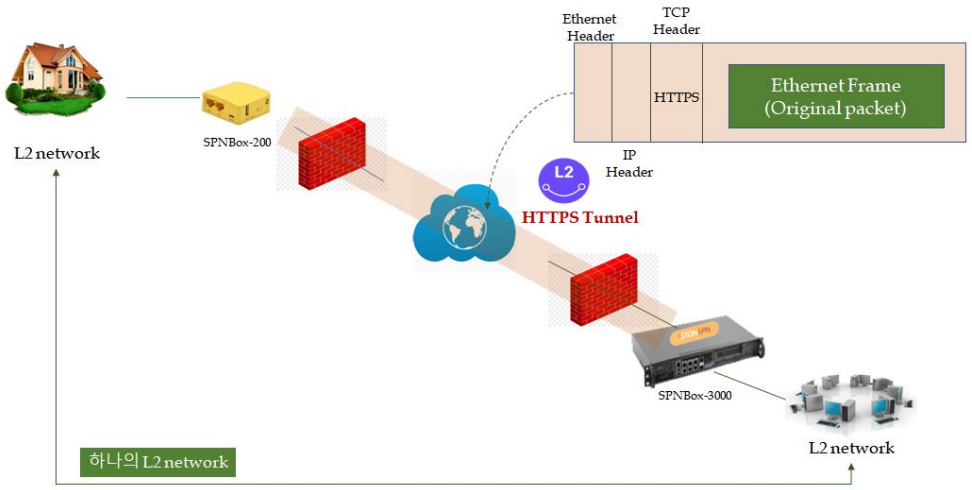
- 복수개의 VPN Server를 하나로 묶어 주는 기능 -

10. 2ip SPN(L2 SPN)은 Open Source인 **SoftEther VPN(Apache License 2.0)**을 기반으로 설계되어 있어, 높은 안정성과 신뢰성을 보장합니다.



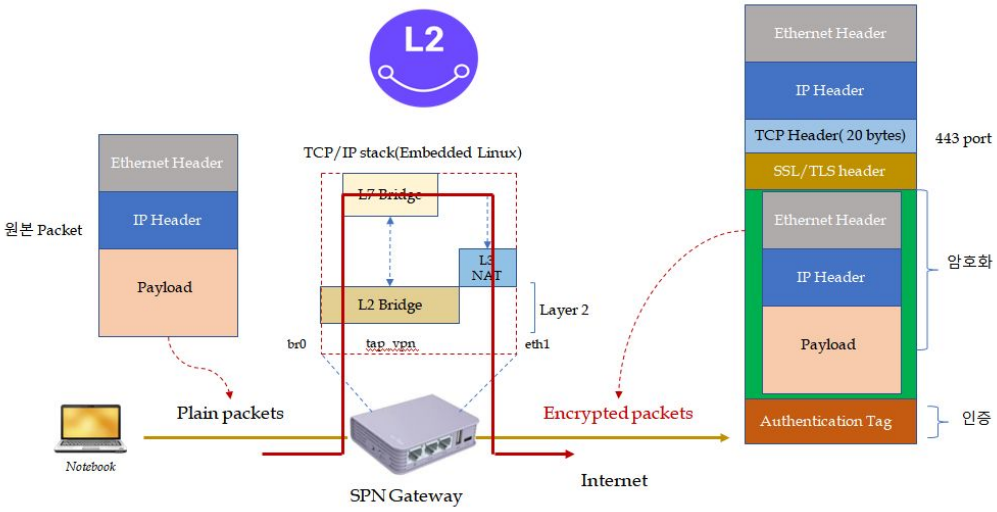
L2 SPN 기능을 사용하면, L2 packet(Windows NETBEUI, DHCP, ARP, Broadcast 등)을 안전하게 실어 나를 수 있습니다.

- 2ip SPN의 동작 원리 1 : 원본 패킷 암호화 -



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

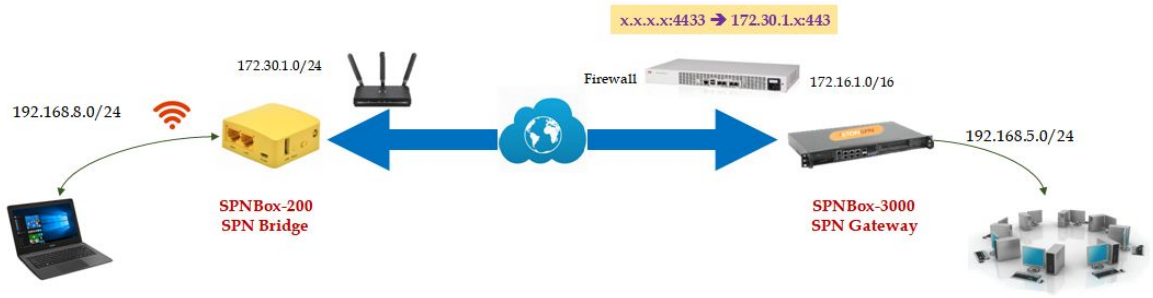
- 2ip SPN의 동작 원리 2 : SSL Tunnel 생성 1 -



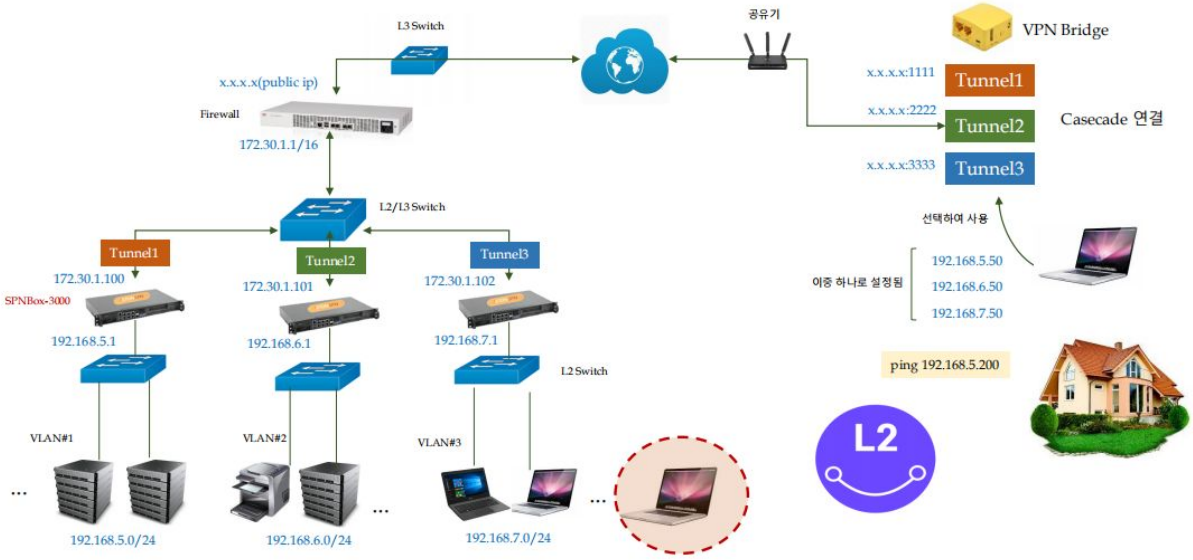
- 2ip SPN의 동작 원리 2 : SSL Tunnel 생성 2 -

네트워크 구성 방법

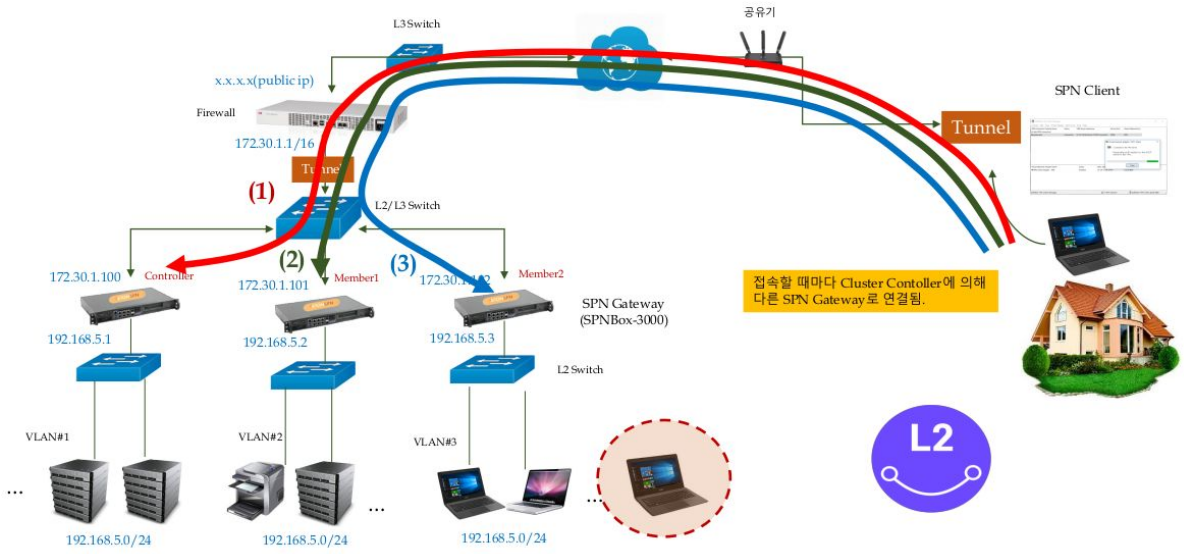
2ip SPN을 사용하기 위해서는 사무실에 SPN Gateway를 설치한 상태에서, 자택에서는 SPN Bridge 혹은 SPN Client(Windows 사용자)를 이용하여 사내망으로 원격 접속하시면 됩니다.



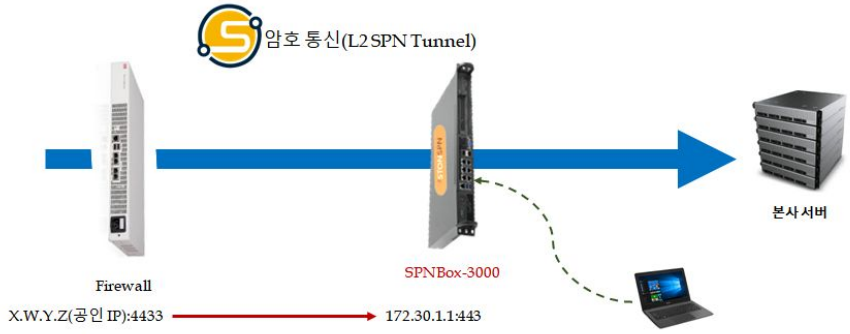
- 2ip SPN 망 구성 1 : 단일 터널 사용 예 -



- 2ip SPN 망 구성 2 : 복수개의 터널 사용(사용자가 별도의 터널 생성 방식) 예 -



- 2ip SPN 망 구성 3 : Cluster 구성(SPN Gateway가 터널을 관리하는 방식) 예 -



- 사내 망에 SPN Gateway 설치 예 -

SPN Gateway 설치 절차

1. 먼저 SPN Tunnel 연결을 위해 본사 방화벽(Firewall)에서 Port Forwarding(예: 4433 => 443) 설정을 해 줍니다.
2. 다음으로 윈도/MacOS 전용 application program인 **VPN Server Manager**를 이용하여 SPN Gateway 설정(IP 주소, Port)을 진행합니다.
3. 마지막으로 재택근무자가 접속해 오기를 기다린 후, SPN Tunnel을 생성해 줍니다.

- 자택에 SPN Bridge 설치 예 -

SPN Bridge 설치 절차

1. PC의 전원을 켜고, Windows or MacOS 관리용 tool인 **VPN Server Manager**를 설치합니다.
2. SPNBox-200에 LAN Cable을 연결하고 전원을 넣습니다(물론 Wi-Fi 연결도 가능합니다).
3. 본사에서 제공한 공인 IP 주소/포트 및 사용자 계정 정보를 입력한 후, 본사 SPN Gateway와의 SPN 연결을 시도합니다.
4. 이제 부터는 마치 자신의 PC나 Notebook이 사무실에 있는 것처럼 자유롭게 사내 망에 접속할 수 있습니다.

참고: SPN 연결이 정상적으로 진행된 상태에서 자신의 IP 주소를 확인해 보시기 바람. 본사 내부 망의 주소와 동일한 대역의 IP 주소를 할당 받았음을 알 수 있음.

- SPN Client 설치 예 -

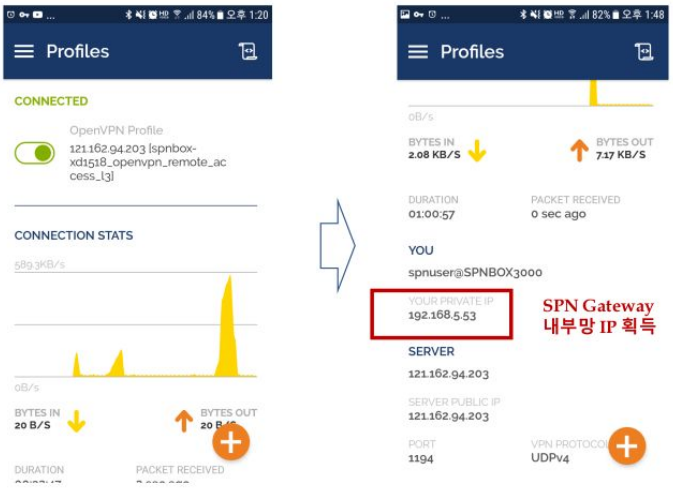
SPN Client 설치 절차

1. PC의 전원을 켜고, Windows용 **SPN Client S/W**를 설치합니다.
2. 본사에서 제공한 공인 IP 주소/포트 및 사용자 계정 정보를 입력한 후, 본사 SPN Gateway와의 SPN 연결을 시도합니다.

3. 이제 부터는 마치 자신의 PC나 Notebook이 사무실에 있는 것처럼 자유롭게 사내 망에 접속할 수 있습니다.

재택 근무 시 SPN Bridge 혹은 SPN Client를 사용해도 충분하지만, Smart Phone를 이용해 Wi-Fi가 아니라 LTE 망을 통해 사내망에 접속하고자 하는 경우라면 아래와 같이 OpenVPN을 이용할 수도 있습니다.

- OpenVPN Client를 이용하여 서버에 접속하는 예 1 -

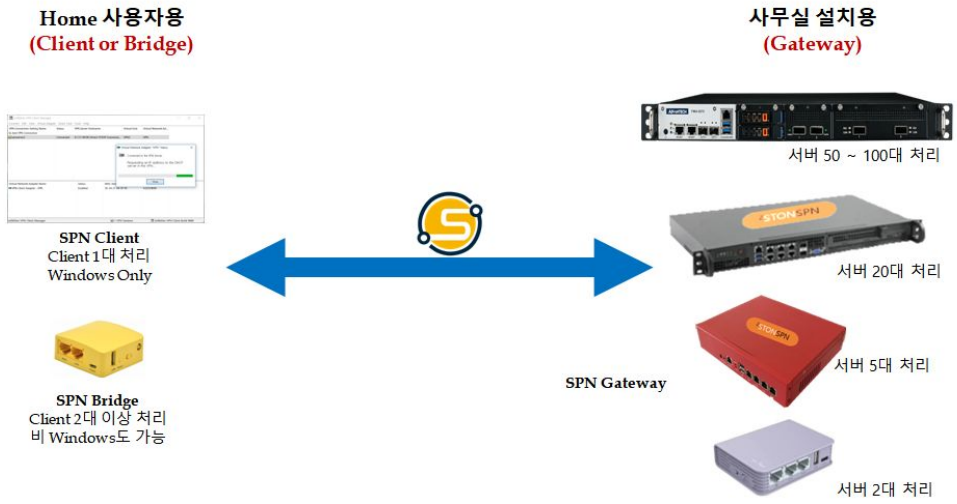


- OpenVPN Client를 이용하여 서버에 접속하는 예 2 -

참고: OpenVPN 대신에 훨씬 설정하기 편한 L2TP/IPsec client(Android, iPhone, Windows, MacOS 등에 기본 설치되어 있음)를 이용해도 접속 가능함.

제품 스펙 및 구매 정보

2ip SPN은 크게 회사 망의 중요서버 앞단에 설치하는 SPN Gateway와 가정(Home)에서 사용하는 SPN Bridge(복수개의 장치 연결 시) 및 SPN Client(Windows OS 전용)로 구성되어 있습니다.



참고: 제품 관련 자세한 스펙 및 가격은 아래 연락처로 문의 바랍니다.

지금 선택하세요.

2ip SPN이 여러분의 안전한 재택근무를 도와드릴 것입니다.

서울특별시 용산구 한남동 한남대로 80, (주)투아이피

전화: 82(2)3785-3300, 담당자: help@2ipco.com