**VPN가상 사설망**

**[1.](https://mirror.enha.kr/wiki/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D" \l "toc) 개요**[**¶**](https://mirror.enha.kr/wiki/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D#s-1)

남  
영어로는 Virtual Private Network라고 하며 보통 줄여서 VPN이라고 부른다.

[기업](https://mirror.enha.kr/wiki/%EA%B8%B0%EC%97%85)이나 [군대](https://mirror.enha.kr/wiki/%EA%B5%B0%EB%8C%80)등 단체에서 내부인들만 볼 수 있는 특수목적의 [인트라넷](https://mirror.enha.kr/wiki/%EC%9D%B8%ED%8A%B8%EB%9D%BC%EB%84%B7)을 구축할 때는 보통 해당되는 [컴퓨터](https://mirror.enha.kr/wiki/%EC%BB%B4%ED%93%A8%ED%84%B0)만 전용선으로 연결해서 제3자가 함부로 접근하지 못하게 구축되는 서버를 쓴다. 그러나  사용자가 모두 회사에만 앉아있는 게 아니면 출장가서 업무에 필요한 자료를 급히 찾아야 하는 일도 생기고, 집에서 작업해야 하는 경우도 생기게 된다. 이런 경우 일일이 모든 직원의 집에 있는 컴퓨터를 전용선으로 묶을 수도 없는 노릇이고, 그렇다고 출장간 [호텔](https://mirror.enha.kr/wiki/%ED%98%B8%ED%85%94) 창문까지 전용선을 끌어오는 것은 더더욱 불가능하다.

이러한 불가피한 상황에서 인터넷 회선을 암호화된 규격을 통해 마치 개인 전용선같이 끌어쓰는 게 가상 사설망의 핵심이다. [크고 아름다운](https://mirror.enha.kr/wiki/%ED%81%AC%EA%B3%A0%20%EC%95%84%EB%A6%84%EB%8B%A4%EC%9A%B4) 전용선을 본사-지사 사이에 직접 연결하기에는 너무나 많은 비용이 들기 때문에, 비용 부담을 줄이려는 중소기업에서도 쓰이기도 한다. 아주 간단하게 설명하면 모두가 쓰는 [인터넷](https://mirror.enha.kr/wiki/%EC%9D%B8%ED%84%B0%EB%84%B7) 회선을 전용선같이 쓰는 기술이다.

원래는 저렇게 보안이 철저해야 하는 서버를 전용선으로 묶기 힘든 경우에 인터넷 회선을 빌려쓰는 기술이어서 개인이 쓸 일은 없어보이나, 이 기술을 이용하면 [프록시 서버](https://mirror.enha.kr/wiki/%ED%94%84%EB%A1%9D%EC%8B%9C%20%EC%84%9C%EB%B2%84)보다 강력한 [익명성](https://mirror.enha.kr/wiki/%EC%9D%B5%EB%AA%85%EC%84%B1)으로 더 강력한 [IP](https://mirror.enha.kr/wiki/IP)우회가 가능해진다.

[[edit](http://rigvedawiki.net/r1/wiki.php/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D?action=edit&section=2)]

[**2.**](https://mirror.enha.kr/wiki/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D#toc)**원리**[**¶**](https://mirror.enha.kr/wiki/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D#s-2)

* 간단하게 설명해서 [인터넷 공유기](https://mirror.enha.kr/wiki/%EC%9D%B8%ED%84%B0%EB%84%B7%20%EA%B3%B5%EC%9C%A0%EA%B8%B0)가 한 대 있다고 가정하자.[[1]](https://mirror.enha.kr/wiki/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D#fn1)
* 이 공유기에 연결돼있는 모든 [컴퓨터](https://mirror.enha.kr/wiki/%EC%BB%B4%ED%93%A8%ED%84%B0)는 공유기를 중심으로 [서버](https://mirror.enha.kr/wiki/%EC%84%9C%EB%B2%84)를 구성한다.
* 이 공유기는 [인터넷](https://mirror.enha.kr/wiki/%EC%9D%B8%ED%84%B0%EB%84%B7)에 연결돼있고, 공유기에 연결된 모든 컴퓨터는 공유기에게 할당받은 내부 [IP](https://mirror.enha.kr/wiki/IP)를 통해 외부 인터넷과 연결된다.
* 하지만 이 공유기는 보안기능이 있어서 [네트워크](https://mirror.enha.kr/wiki/%EB%84%A4%ED%8A%B8%EC%9B%8C%ED%81%AC)를 형성하는 컴퓨터의 내부 네트워크는 인터넷상에서 접속이 불가능하며, 오직 공유기에 연결돼있는 컴퓨터만 내부 네트워크망을 쓸 수있다.
* 그런데 공유기에서 예외로 특정 계정과 비밀번호를 가진 사용자를 내부 네트워크에 있는 것처럼 잡아줄 수 있다. 이 사용자가 가상 사설망을 사용한 사람이다.

읽어보면 알겠지만 가상 사설망으로 접속한 사람은 **내부서버로 전용선을 사용해 접속한 사용자**로 잡고 만약 서버가 인터넷에 연결돼있으면 **그 서버의 IP로 인터넷을 한다.** 특히 가상 사설망 자체가 보안이 필요한 전용선을 대신해서 쓰는 것이므로, VPN 사용자와 접속 서버간의 터널과 통신 패킷은 전부 암호화 된다. 그렇기 때문에 접속서버의 [로그](https://mirror.enha.kr/wiki/%EB%A1%9C%EA%B7%B8)를 보지 않는이상 원래 사용자를 알아내는 것은  사실상 불가능하다. [프록시 서버](https://mirror.enha.kr/wiki/%ED%94%84%EB%A1%9D%EC%8B%9C%20%EC%84%9C%EB%B2%84)에 비해 강력한 익명성이 보장된다. 아무리 외부에서 추적을 해봤자 VPN으로 접속된 서버의 내부 IP까지만 알아낼 수 있고 애초에 주소가 그렇게 할당돼있기 때문에 메인서버의 로그를 봐야만 어디서 접속해온 건지 알 수 있다.

[[edit](http://rigvedawiki.net/r1/wiki.php/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D?action=edit&section=3)]

[**3.**](https://mirror.enha.kr/wiki/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D#toc)**가상 사설망의 익명성**[**¶**](https://mirror.enha.kr/wiki/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D#s-3)

모든 과정이 암호화된다는 특성 상 [정부](https://mirror.enha.kr/wiki/%EC%A0%95%EB%B6%80)의 [검열](https://mirror.enha.kr/wiki/%EA%B2%80%EC%97%B4)을 [프록시 서버](https://mirror.enha.kr/wiki/%ED%94%84%EB%A1%9D%EC%8B%9C%20%EC%84%9C%EB%B2%84)나 [tor](https://mirror.enha.kr/wiki/tor)보다 [넘사벽](https://mirror.enha.kr/wiki/%EB%84%98%EC%82%AC%EB%B2%BD)급으로 안전하게 피할 수 있다. [프록시 서버](https://mirror.enha.kr/wiki/%ED%94%84%EB%A1%9D%EC%8B%9C%20%EC%84%9C%EB%B2%84) 항목을 보면 알겠지만 원래 사용자의 IP가 완전히 오픈되거나, 그대로 기록되는 [프록시 서버](https://mirror.enha.kr/wiki/%ED%94%84%EB%A1%9D%EC%8B%9C%20%EC%84%9C%EB%B2%84) 규격 또한 있기 때문에 모든 프록시 서버가 완벽한 [익명성](https://mirror.enha.kr/wiki/%EC%9D%B5%EB%AA%85%EC%84%B1)을 보장하지는 않고, 무엇보다 [무료](https://mirror.enha.kr/wiki/%EB%AC%B4%EB%A3%8C)로 돌아가는 [프록시 서버](https://mirror.enha.kr/wiki/%ED%94%84%EB%A1%9D%EC%8B%9C%20%EC%84%9C%EB%B2%84)들은 [**IP**](https://mirror.enha.kr/wiki/IP)**가 오픈되는 경우가 많기 때문에** 원래 사용자의 IP를 특정하는 것은 생각보다 간단한 편이다. [Tor](https://mirror.enha.kr/wiki/Tor)의 경우는 일단 접속되면 여러 IP를 거치는 루트를 이용하기 때문에 접속을 성공한 이후부터는 어느정도 안전이 보장되지만, **접속을 시도하고 터널을 확립하는 과정이 암호화가 되어있지 않다.** 실제로 이런점을 악용하여 [Tor](https://mirror.enha.kr/wiki/Tor) 접속터널을 차단하는 국가도 있다.

하지만 VPN는 서버가 해외에 있다면, 전용선과 가까운 보안을 유지해야 하는 만큼 처음 순간부터 모든 과정이 암호화되어 접속 규격 자체의 보안성이 상당히 높다. 때문에 정상적인 방법으론 메인 서버 외에는 **원래 사용자를 절대로 특정할 수 없다.** 보통 VPN으로 접속해온 실제 사용자 IP를 특정할 수 있는 경우는 무료 VPN의 자체 클라이언트 이거나, 알고보니 프록시 서버인 경우다.

또한 [온라인 게임](https://mirror.enha.kr/wiki/%EC%98%A8%EB%9D%BC%EC%9D%B8%20%EA%B2%8C%EC%9E%84)회사나 기타 인터넷 서비스를 제공하는 회사에서 VPN 계정을 막을 경우, VPN으로 접속해온 유저들을 특정하는 방법은 [IP](https://mirror.enha.kr/wiki/IP)를 역추적하여 알아내는 것이 아니라, 이미 VPN [서버](https://mirror.enha.kr/wiki/%EC%84%9C%EB%B2%84)라고 알려진 IP들의 리스트를 대조하여 일치하는 유저들만 잡는거다. 즉 알려질때로 알려진 무료 VPN IP을 사용한 유저는 당연히 잡히는 거고, 유료 VPN같이 IP를 특정인물들만 알 수 있는 VPN IP는 특정을 제대로 하지 못한다.

그런데 [천조국](https://mirror.enha.kr/wiki/%EB%AF%B8%EA%B5%AD)의 [국가안보국](https://mirror.enha.kr/wiki/NSA)은 VPN 암호코드를 해독하는데 성공하여 [**이를 패킷단위로 실시간 감시하는**](http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=105&oid=031&aid=0000300715)[**충공깽**](https://mirror.enha.kr/wiki/%EC%B6%A9%EA%B3%B5%EA%B9%BD)**을 선사하기도 했다.** 그러나 [NSA](https://mirror.enha.kr/wiki/NSA)는  외부와는 10년 이상의 기술격차를 갖고 있기에 가능한 거고, [일반인](https://mirror.enha.kr/wiki/%EC%9D%BC%EB%B0%98%EC%9D%B8) 뿐만 아니라 일반적인 국가들의 **국가기관 조차** 실제 사용자를 추적하는 것이 불가능하단 것이다. [[2]](https://mirror.enha.kr/wiki/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D#fn2)

하지만 [IP](https://mirror.enha.kr/wiki/IP) 세탁을 하면서 [막장](https://mirror.enha.kr/wiki/%EB%A7%89%EC%9E%A5)짓을 벌이는 일부 [찌질이](https://mirror.enha.kr/wiki/%EC%B0%8C%EC%A7%88%EC%9D%B4)들을 걱정할 필요는 없는게, 이들은 [프록시 서버](https://mirror.enha.kr/wiki/%ED%94%84%EB%A1%9D%EC%8B%9C%20%EC%84%9C%EB%B2%84)로만 IP를 세탁하지 가상 사설망은 잘 이용하지 않는다. 많이 알려지지 않은 수법인것도 있지만, 어느정도 속도가 나오는 가상 사설망 서비스는 기본적으로 **유료**인데다가 가격도 트롤링 하는데 쓰기엔 비싸기 때문. 무료 VPN은 체험판 성격이 강하기 때문에, 속도도 형편없고, IP 하나를 여러명이 쪼개서 쓰는것이기 때문에, 이미 [프록시 서버](https://mirror.enha.kr/wiki/%ED%94%84%EB%A1%9D%EC%8B%9C%20%EC%84%9C%EB%B2%84) 급으로 대부분의 사이트에서 밴을 먹은 상태이다.

다만 세간에서는 회사들이 체험판 VPN에 접속한 로그를 기록해 두었다가 수사기관에 가져다 바친다는 [카더라](https://mirror.enha.kr/wiki/%EC%B9%B4%EB%8D%94%EB%9D%BC)가 돌고 있는데, **말도 안되는 개소리다.**

가장 큰 이유로는 일단 상용 VPN의 기본 목적이 익명성이기 때문에 [[3]](https://mirror.enha.kr/wiki/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D#fn3) 대부분의 유저들은 타국에 위치한 서버를 통해 통신하게 된다. 대부분의 상용 VPN 클라이언트들은 전세계의 회사 서버 중 클릭 하나, 주소 입력 하나로 원하는 위치로 접근하게 해준다. 즉 자국이 수사권이 없는 위치로 통신하면 타국에 무리해서 수사협조를 요청이라도 하지 않는 이상 추적이 불가능하다. 2ch이 일본 정부에게 털리지 않은 것과 같은 이유.

또한 보안회사라는 위치상 고객 정보를 누설한다는 것이 말이 안되기도 하다. 일반적으로 VPN 회사가 내거는 운영 슬로건은 **"고객님의**[**익명성**](https://mirror.enha.kr/wiki/%EC%9D%B5%EB%AA%85%EC%84%B1)**보장."**이다. 고객이 수사권의 영향 아래인 자국 서버 VPN을 사용한 것이라면 모를까[[4]](https://mirror.enha.kr/wiki/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D#fn4), 듭보잡 나라의 사이버 모욕죄 같이 어떻게 봐도 기준이 애매한 사안 때문에 고객 보안이 생명인 회사에서 로그를 상납하면, 이들이 내걸고 있는 "고객님의 [익명성](https://mirror.enha.kr/wiki/%EC%9D%B5%EB%AA%85%EC%84%B1) 보장." 이란 정체성을 **자기 자신의 손으로 훼손하는 꼴이 된다.** 이는 트라이얼 버전이라도 동일하다. 사실 트라이얼 이라고 마구잡이로 기록하고 가져가 바치면 유료 버전이라고 안바칠 거라고 **누가 믿겠는가?**

물론 인터폴 단위로 출동할 범죄에는 가차 없다.

다만 많은 유저들이 사용하는 츠쿠바 대학교 대학원의 무료 VPN에는 **"범죄행위 방지를 위해 모든 접속로그가 자동으로 기록되고 있다."** 라는 경고문이 포함되 있다. 이는 애초에 상업적이 아닌 학술적 목적으로 운영되는 VPN 서비스이기 때문. 범죄에 악용된다는 비난을 피하기 위해 악용할 경우 대응하기 위해 게이트웨이 접속 로그를 백업해두겠다는 의미로 해석된다. 뭐 위키러들은 대개 VPN을 접속국가 속여주는 도구 이상으로 활용하지 않기에 상관없지만... 혹여나 보안이 중요하다면 유료 VPN 쓰자.

[[edit](http://rigvedawiki.net/r1/wiki.php/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D?action=edit&section=4)]

[**4.**](https://mirror.enha.kr/wiki/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D#toc)**VPN 이용**[**¶**](https://mirror.enha.kr/wiki/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D#s-4)

[[edit](http://rigvedawiki.net/r1/wiki.php/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D?action=edit&section=5)]

[**4.1.**](https://mirror.enha.kr/wiki/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D#toc)**무료 VPN**[**¶**](https://mirror.enha.kr/wiki/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D#s-4.1)

[네X버](https://mirror.enha.kr/wiki/%EB%84%A4%EC%9D%B4%EB%B2%84)와 같은 곳에서 검색하면 나오는 무료 VPN은 위에 기술된 바와같이, 일부 [트롤](https://mirror.enha.kr/wiki/%ED%8A%B8%EB%A1%A4%EB%A7%81)들의 도구로 사용되어 몇몇 국내 사이트에는 접근이 불가능한 경우가 있으며, 속도면은 아예 포기하는 것이 마음 편하다. 특히 네X버에 퍼질대로 퍼진 어느 일본대학의 무료 VPN은 [대한민국](https://mirror.enha.kr/wiki/%EB%8C%80%ED%95%9C%EB%AF%BC%EA%B5%AD) 유저 800만명이 **무려 20기가를 쓰며 1위를 찍고있다.** 2위인 [중국](https://mirror.enha.kr/wiki/%EC%A4%91%EA%B5%AD)은 3천500만명이 8기가를 쓰니 엄청난 차이. 그렇기 때문에 무료VPN은 일시적인 IP 우회로만 쓰는것을 추천한다. 그리고 제발 **트롤링 하는곳에 트래픽을 낭비하지 말자.**

무료 VPN의 속도가 마음에 안들지만, 그렇다고 유료버전을 사용하기 부담스러운 유저라면 트라이얼 버전을 사용하는 방법도 있다. 다만 일정기간동안 상용기능을 체험하는 트라이얼 버전은 사용 조건이 대부분 [**신용카드**](https://mirror.enha.kr/wiki/%EC%8B%A0%EC%9A%A9%EC%B9%B4%EB%93%9C)**정보 사전등록** 이기 때문에 트라이얼 종료기간을 잊고 있으면 폭풍 결제가 되어 눈물 쏟는 경우도 있다.

[[edit](http://rigvedawiki.net/r1/wiki.php/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D?action=edit&section=6)]

[**4.2.**](https://mirror.enha.kr/wiki/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D#toc)**유료 VPN**[**¶**](https://mirror.enha.kr/wiki/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D#s-4.2)

[대한민국](https://mirror.enha.kr/wiki/%EB%8C%80%ED%95%9C%EB%AF%BC%EA%B5%AD)에서 가상 사설망을 서비스 하는 업체들은 대부분 [기업](https://mirror.enha.kr/wiki/%EA%B8%B0%EC%97%85)을 대상으로 하기 때문에 가격 개념 자체가 다르며, 무엇보다 제공하는 IP가 대부분 국내([대한민국](https://mirror.enha.kr/wiki/%EB%8C%80%ED%95%9C%EB%AF%BC%EA%B5%AD)) IP이다. 개인을 대상으로 세계 각국의 IP를 제공해주는 업체들은 대부분 해외업체들이다. 결제수단은 [신용카드](https://mirror.enha.kr/wiki/%EC%8B%A0%EC%9A%A9%EC%B9%B4%EB%93%9C) 혹은 [페이팔](https://mirror.enha.kr/wiki/%ED%8E%98%EC%9D%B4%ED%8C%94)이다. [비자나 마스타카드를 지원하는 체크카드](https://mirror.enha.kr/wiki/%EC%B2%B4%ED%81%AC%EC%B9%B4%EB%93%9C/%ED%95%B4%EC%99%B8%EA%B2%B0%EC%A0%9C)도 받기 때문에 학생들도 어느정도 기본적인 영어실력만 있다면 크게 무리없이 결제가 가능하다. 다만 몇몇 해외 기업은 **매달 자동결제가 되므로**, 더이상 사용할 일이 없다면 반드시 해약하자.

유료로 VPN을 서비스하는 기업은 영어로 검색하면 생각보다 간단하게 찾을 수 있다. 가격대는 매달 5달러부터 20달러까지 다양한 편이지만, **같은 가격임에도** 서버 퀄리티가 심하게 차이난다. 같은돈 10달러 내면서 서버 한대에 속도마저 시망인 곳이 있다면, VPN 서버가 몇십개이면서 속도도 빵빵한 곳도 있다. 그렇기 때문에 반드시 트라이얼 버전을 통해 최종구매 전에 테스트 해봐야 한다.

하지만  [한국인](https://mirror.enha.kr/wiki/%ED%95%9C%EA%B5%AD%EC%9D%B8)들의 유료 VPN 사용률이 높아짐에 따라, VPN 시장에서 [한국인](https://mirror.enha.kr/wiki/%ED%95%9C%EA%B5%AD%EC%9D%B8) 고객들이 많아지고 있다.  이런 한국인 소비자들을 잡기위해 결제도 [대한민국 원](https://mirror.enha.kr/wiki/%EB%8C%80%ED%95%9C%EB%AF%BC%EA%B5%AD%20%EC%9B%90)으로 할 수 있게 바꾸고, 깔끔하게 번역된 [한국어](https://mirror.enha.kr/wiki/%ED%95%9C%EA%B5%AD%EC%96%B4) 홈페이지와 설명서를 지원하는 해외 VPN 업체도 생기고 있다. 다만 [대한민국 원](https://mirror.enha.kr/wiki/%EB%8C%80%ED%95%9C%EB%AF%BC%EA%B5%AD%20%EC%9B%90)으로 결제를 받는 곳들 중에는 [DCC](https://mirror.enha.kr/wiki/DCC)를 통해 [환전](https://mirror.enha.kr/wiki/%ED%99%98%EC%A0%84) 수수료 폭탄을 선사하는 곳도 있기때문에 주의해야 한다.

[[edit](http://rigvedawiki.net/r1/wiki.php/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D?action=edit&section=7)]

[**5.**](https://mirror.enha.kr/wiki/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D#toc)**통신규격**[**¶**](https://mirror.enha.kr/wiki/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D#s-5)

* **L2TP**  
  Layer 2 Tunneling Protocol. 줄여서 L2PT라고 부른다. L2F와 PPTP 프로토콜을 결합하여 만든 규격이기 때문에 PPP를 지원한다. L2PT는 터널을 확립해주기만 하며, 암호화는 [IPsec](https://mirror.enha.kr/wiki/IPsec) 기술을 사용한다. IPsec 기술에는 IKE(Internet Key Exchange)와 ESP(Encapsulation Security Payload)가 사용된다. 해당 암호화 패킷을 차단하면 L2PT 규격을 사용할 수 없다. 대부분의 [운영체제](https://mirror.enha.kr/wiki/%EC%9A%B4%EC%98%81%EC%B2%B4%EC%A0%9C)에서 기본적으로 지원하며, [iOS](https://mirror.enha.kr/wiki/iOS)에도 기본 내장되어 있다. [안드로이드](https://mirror.enha.kr/wiki/%EC%95%88%EB%93%9C%EB%A1%9C%EC%9D%B4%EB%93%9C%28%EC%9A%B4%EC%98%81%EC%B2%B4%EC%A0%9C%29)는 구글이 제작한 표준 규격에서는 기본 내장되어 있으나, 기종에 따라 내장 여부가 다르니 별도로 확인해보자.
* **OpenVPN**  
  [오픈소스](https://mirror.enha.kr/wiki/%EC%98%A4%ED%94%88%EC%86%8C%EC%8A%A4) VPN이라 OpenVPN이지, **절대로 암호화가 되어있지 않아서 OpenVPN이 아니다.** 기초규격은 L2TP를 따르지만, L2TP와 달리 세개의 레이어를 확립할 수 있다는 특징이 있다. OpenVPN의 최대 장점은 프로파일 하나만 있으면 어떤 운영체제에서도 쉽게 연결할 수 있다는 점, 또한 VPN 장비나 공유기 없이도 VPN 서버를 설정 할 수 있다는 점이 있다. 많은 OS를 지원하고 있으나 오픈소스라는 사정상 **내장되어 있지는 않다**. 허나 [안드로이드](https://mirror.enha.kr/wiki/%EC%95%88%EB%93%9C%EB%A1%9C%EC%9D%B4%EB%93%9C%28%EC%9A%B4%EC%98%81%EC%B2%B4%EC%A0%9C%29)나 [iOS](https://mirror.enha.kr/wiki/iOS) 앱스토어에 공식 앱이 올라와 있으니 설치하고 프로파일만 끼얹으면 연결 잘 된다. 기숙사나 일부 교육기관처럼 VPN의 포트를 막는 경우가 종종 있는데, OpenVPN의 경우는 포트를 자율적으로 설정할 수 있고 일단은 공식적으로 포트를 할당받은 프로토콜이 아니기 때문에 VPN 막힌 곳에서도 잘만 쓸 수 있다는 장점이 있다.
* **PPTP**  
  Point to Point Tunneling Protocol. 줄여서 PPTP라고 부른다. [PPP](https://mirror.enha.kr/wiki/PPP)(Point-to-Point Protocol) 기술을 확장하여 만든 규격이며, 위의 L2TP와 같이 PPTP도 터널을 확립해주기만 하며, 암호화는 MS-CHAP와 RC4를 합성한다. 참고로 MS-CHAP는 [마이크로소프트](https://mirror.enha.kr/wiki/%EB%A7%88%EC%9D%B4%ED%81%AC%EB%A1%9C%EC%86%8C%ED%94%84%ED%8A%B8)가 주도하여 만든 통신 규격이다. 대부분의 [운영체제](https://mirror.enha.kr/wiki/%EC%9A%B4%EC%98%81%EC%B2%B4%EC%A0%9C)에서 기본적으로 지원하며, [iOS](https://mirror.enha.kr/wiki/iOS)에도 기본 내장되어 있다. [안드로이드](https://mirror.enha.kr/wiki/%EC%95%88%EB%93%9C%EB%A1%9C%EC%9D%B4%EB%93%9C%28%EC%9A%B4%EC%98%81%EC%B2%B4%EC%A0%9C%29)는 구글이 제작한 표준 규격에서는 기본 내장되어 있으나, 기종에 따라 내장 여부가 다르니 별도로 확인해보자. 현재 보안상 결함이 발견된 바 있다.
* **SSTP**  
  Secure Socket Tunneling Protocol. 줄여서 SSTP라고 부른다. [SSL](https://mirror.enha.kr/wiki/SSL) 규격을 사용하여 만든 비교적 최근 만들어진 통신 규격이다. 자세한 사항은 [추가바람](https://mirror.enha.kr/wiki/%EC%B6%94%EA%B0%80%EB%B0%94%EB%9E%8C).

추가바람

[[edit](http://rigvedawiki.net/r1/wiki.php/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D?action=edit&section=8)]

[**6.**](https://mirror.enha.kr/wiki/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D#toc)**연결방법**[**¶**](https://mirror.enha.kr/wiki/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D#s-6)

VPN서버로 연결하는 방법은 크게 두가지로 나뉜다. 하나는 [운영체제](https://mirror.enha.kr/wiki/%EC%9A%B4%EC%98%81%EC%B2%B4%EC%A0%9C) 자체의 기능을 통해 연결하는 방식이고, 두번째는 자체 클라이언트를 통해 연결하는 방식이다. [운영체제](https://mirror.enha.kr/wiki/%EC%9A%B4%EC%98%81%EC%B2%B4%EC%A0%9C) 자체의 기능으로 이용하기 위해선 서버 주소와 서버 계정, 패스워드가 필요하다. L2PT의 경우엔 별도의 암호키나 암호 토큰이 추가로 필요하다. 경우에 따라 접속규격을 손봐줘야 하는 경우도 있다. 자체클라이언트의 경우는 클라이언트마다 전부 다르기 때문에 일일히 설명할 수 없으나, 대부분 원클릭으로 접속된다.

여기서 한가지 주의할 점은, **유료 VPN**[[5]](https://mirror.enha.kr/wiki/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D#fn5) 중에서 진짜로 VPN규격으로 접속하여 사용할 수 있는 VPN 서버는 [**운영체제**](https://mirror.enha.kr/wiki/%EC%9A%B4%EC%98%81%EC%B2%B4%EC%A0%9C)**자체의 기능으로도 연결할 수 있어야 한다.** 유료 VPN의 경우 접속할 수 있는 서버 주소와 당신의 계정이 공개되어 운영체제 자체의 규격으로도 접속할 수 있도록 한다. 만약 이러한 정보들이 하나도 공개되지 않고, 클라이언트로만 접속 가능한 유료 VPN이라면 200%의 확률로 겉에만 VPN이라고 써놓고, 까보면 [프록시 서버](https://mirror.enha.kr/wiki/%ED%94%84%EB%A1%9D%EC%8B%9C%20%EC%84%9C%EB%B2%84)거나 프록시 서버보다 못한 [짝퉁](https://mirror.enha.kr/wiki/%EC%A7%9D%ED%89%81)이다.

다만 예외로 운영체제 자체 기능이 아닌 경우 중에서 OpenVPN은 제외하도록 한다. 이는 [오픈소스](https://mirror.enha.kr/wiki/%EC%98%A4%ED%94%88%EC%86%8C%EC%8A%A4) 계열 VPN이라서 상용 OS 측에서 자체 기능으로 편입시키기 애매하기 때문에 내장되어 있지 않는거지, 분명 VPN이다. 다만 OpenVPN만 지원하는 유료 VPN은 극소수라는 점을 참고하자.

[[edit](http://rigvedawiki.net/r1/wiki.php/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D?action=edit&section=9)]

[**7.**](https://mirror.enha.kr/wiki/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D#toc)**장점**[**¶**](https://mirror.enha.kr/wiki/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D#s-7)

* 전용선을 일일이 끌어 쓸 필요가 없어서 장거리 [통신망](https://mirror.enha.kr/wiki/%ED%86%B5%EC%8B%A0%EB%A7%9D) 구축비용이 매우 저렴하다.
* 강력한 [익명성](https://mirror.enha.kr/wiki/%EC%9D%B5%EB%AA%85%EC%84%B1)이 보장된다.
* 전용선으로 연결된 [컴퓨터](https://mirror.enha.kr/wiki/%EC%BB%B4%ED%93%A8%ED%84%B0)가 아니어도 내부 네트워크에 접속할 수 있다.

[[edit](http://rigvedawiki.net/r1/wiki.php/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D?action=edit&section=10)]

[**7.1.**](https://mirror.enha.kr/wiki/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D#toc)**해외 사이트 속도 향상**[**¶**](https://mirror.enha.kr/wiki/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D#s-7.1)

* 한국 한정의 이야기인데 국내에서 일본과 경유하는 해저케이블을 제대로 계약해서 쓰는 국내 ISP는 한 곳이요 (덕분에 예전에는 일본발 지진 등으로 핑이 치솟아 해외 게임을 하다가 뒷목 잡는 게이머들이 많았다. 지금은 어떤지 [수정바람](https://mirror.enha.kr/wiki/%EC%88%98%EC%A0%95%EB%B0%94%EB%9E%8C)), 구글(유튜브)은 한국정부와 국내ISP의 병신력에 못이겨 데이터센터를 홍콩과 일본에만 지어놓은 상태에서, 갈수록 해외 컨텐츠를 찾는 국내 유저들이 기하급수적으로 늘어나고 있는 상태이기 때문에 국내업체들이 회선료를 해외ISP에 퍼다주는 상황. 그래서 국내 ISP는 암묵적으로 국내 유저의 해외 인터넷 속도를 크게 제한한다는 얘기가 있는데, 당장 유료 VPN을 쓴체 유튜브 1080p 영상만 틀어봐도... 사실 이것은 해외 사이트 접속 속도를 늘리는 것이 아니라, 일부러 국내업체들이 몰래 제한해놓은 인터넷 속도를 본래 속도로 되돌린다(...)는 것에 가깝다. 즉 원래라면 속도가 더 낮아지는게 정상인데, 국내 업체들의 속도제한을 우회하기 때문에 속도가 상승하는 것. 본래 '나왔어야 했을' 속도보다는 당연이 못나온다. 하지만 그래도 빠르다는게 함정. 프록시도 동일하다.
* 다만 나는 아무리 VPN이랑 프록시를 써봐도 느려 터지던데?! 라는 사람은 사실 그건 이미 한국 사람들이 미친듯이 쓰고 있기 때문(...) 누가 쓸만한 VPN/프록시를 찾았다! -> 소식을 들은 한국 유저들이 우르르 몰려간다 -> 트래픽 폭파(...) -> 무한루프(...). 그래서 사실상 국내 유저들끼리 네이버 따위에서 찾을 수 있는 탑10 VPN/프록시는 쓰나마나 이다. 빠른 인터넷 서비스를 신청했다고 생각하고 한달에 많아봤자 3~10달러 정도 밖에 안하니 유료 서비스를 쓰거나, 한국인들에게 아직 잘 알려지지 않은 유/무료 VPN/프록시를 찾아 쓰는게 답. 쓸만한 VPN을 찾으면 알리지 않고 혼자 쓴다는게 이기적일 수도 있지만, 사실 트래픽 폭발로 한국발 IP를 막는 서비스들이 많다는 걸 생각하면 동내방내 떠들고 다니는게 오히려 민폐일수도... VPN과 프록시가 독재에 대한 하나의 저항수단이라는 점에서 보면, 희귀 야동(...)받으려고 무료망에 트래픽폭탄 던지지 말고 그냥 오페라 브라우저의 오프로드를 사용하거나 (물론 이 경우는 IP는 한국으로 그냥 잡히기 때문에 빙신(...)은 사용 불가능하나, 차단된 해외 성인 토렌트 사이트들이 뚫리는 경우가 매우 많다), 그냥 유료 VPN을 쓰는 것을 추천한다.

[[edit](http://rigvedawiki.net/r1/wiki.php/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D?action=edit&section=11)]

[**8.**](https://mirror.enha.kr/wiki/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D#toc)**단점**[**¶**](https://mirror.enha.kr/wiki/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D#s-8)

* 전용선보다 상대적으로 보안에 취약하다.[[6]](https://mirror.enha.kr/wiki/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D#fn6)
* 전용선과 달리 [인터넷](https://mirror.enha.kr/wiki/%EC%9D%B8%ED%84%B0%EB%84%B7) 회선을 통하기 때문에 상대적으로 속도가 느리다.
* 인터넷 회선을 반드시 받아들여야 한다.(오프라인 서버 구축이 불가능하다.)

[[edit](http://rigvedawiki.net/r1/wiki.php/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D?action=edit&section=12)]

[**9.**](https://mirror.enha.kr/wiki/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D#toc)**기타**[**¶**](https://mirror.enha.kr/wiki/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D#s-9)

* 프록시 서버와 달리 가상 사설망은 개인적으로 서버를 돌리거나 단체여도 특수목적으로 쓰는 서버이기 때문에 무료로 접속이 가능한 가상 사설망은 자신의 집이 서버가 아닌 이상 거의 없다. 쉽게 접하는 무료 가상 사설망은 가상 사설망 서비스 업체가 제공하는 체험판인 경우가 대다수다.
* [리눅스](https://mirror.enha.kr/wiki/%EB%A6%AC%EB%88%85%EC%8A%A4) 등에선 [웹브라우저](https://mirror.enha.kr/wiki/%EC%9B%B9%EB%B8%8C%EB%9D%BC%EC%9A%B0%EC%A0%80)만 VPN을 연결해 쓸 수 있는 규격이 존재하지만. [윈도우](https://mirror.enha.kr/wiki/%EC%9C%88%EB%8F%84%EC%9A%B0)에선 [그런 거 없고](https://mirror.enha.kr/wiki/%EA%B7%B8%EB%9F%B0%20%EA%B1%B0%20%EC%97%86%EB%8B%A4) 컴퓨터의 모든 프로그램이 가상 사설망 회선을 써야 한다. 물론 공식적으로 지원하냐의 차이기 때문에 파워 유저라면 우회적인 방법들로 가능.
* [2012년](https://mirror.enha.kr/wiki/2012%EB%85%84), [아청법](https://mirror.enha.kr/wiki/%EC%95%84%EC%B2%AD%EB%B2%95)이 발동 한 후 VPN 업체중 한곳이 [2013년](https://mirror.enha.kr/wiki/2013%EB%85%84) 자사 서비스의 무료 사용자를 공개 했는데 30위 권 밖이던 한국이 압도적으로 1위를 찍었다. 사용자 1인당 평균 2기가 바이트를 사용했다.
* [리그베다 위키](https://mirror.enha.kr/wiki/%EB%A6%AC%EA%B7%B8%EB%B2%A0%EB%8B%A4%20%EC%9C%84%ED%82%A4)에서는 [프록시 서버](https://mirror.enha.kr/wiki/%ED%94%84%EB%A1%9D%EC%8B%9C%20%EC%84%9C%EB%B2%84)와 마찬가지로 VPN주소로 편집시 제재 대상이다. [#](http://wikibbs.net/989738)

----

* [[1]](https://mirror.enha.kr/wiki/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D#rfn1) 이 공유기를 [라우터](https://mirror.enha.kr/wiki/%EB%9D%BC%EC%9A%B0%ED%84%B0) 라고 한다. VPN은 [라우터](https://mirror.enha.kr/wiki/%EB%9D%BC%EC%9A%B0%ED%84%B0)로 가능한 기능이며 일반적인 공유기는 라우터의 NAT만 가지고 만든 거라 보통은 VPN을 지원하지 않는다. 요즘 나오는 것 중에는 지원하는 공유기도 있긴 하다.
* [[2]](https://mirror.enha.kr/wiki/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D#rfn2) 미국의 특징상 통신기기 및 암호에 백도어를 심거나 이용하기 수월한지라 그 이상 걸릴 가능성이 높다. 물론 그쯤 되면 뭔가 다른 기술이 나오겠지만.
* [[3]](https://mirror.enha.kr/wiki/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D#rfn3) 다만 보안회사들이 제공하는 VPN들의 목적이 그런것이고 VPN의 다른 기본적인 기능은 외부에서 내부 네트워크로 들어가 로컬 네트워크로 인식하여 쉽게 말하면 회사 내부에서만 할수 있는 작업들을 하게 해주는 기능들이다. 하지만 보안 회사들이 제공하는 VPN에는 대부분 로컬 네트워크의 단말기들 끼리 통신하는 기능이 없다. 사실 정말 익명성 목적으로는 필요 없기도 하고. 쉽게 말해 하마치는 일종의 VPN 서비스이면서 동시에 단말기들 끼리 서로 알아봐야 멀티를 돌리므로 로컬 네트워크를 생성하고 서로 통신한다.
* [[4]](https://mirror.enha.kr/wiki/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D#rfn4) 예를들면 한국인이 한국에 서버를 둔 VPN을 이용.
* [[5]](https://mirror.enha.kr/wiki/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D#rfn5) 무료 VPN은 대개 클라이언트로만 쓸 수 있도록 고정되어있다.
* [[6]](https://mirror.enha.kr/wiki/%EA%B0%80%EC%83%81%20%EC%82%AC%EC%84%A4%EB%A7%9D#rfn6) 다만 AES 같은 걸 쓰면 암호화를 뚫는 것이 불가능하기 때문에(...) 실용적인 범위 내에서는 충분한 보안이 유지된다. 그러나 보안은 충분하다 수준으로는 만족해서는 안되는 분야이다.