

Choosing the Right VPN

Locating the perfect solution for the home user

Richard Bach

Contents

Abstract	3
Introduction	4
Background	4
Research Description and Results.....	6
OpenVPN.....	6
HotSpotVPN	6
Hamachi	7
iPIG.....	8
Summary and Conclusions.....	8
References	10

Abstract

This paper contains an analysis of various Virtual Private Networking solutions and attempts to compare and contrast them with the goal of singling out one or two choices that would be appropriate for the security-conscious computer user. To come to these conclusions, several products were compared based on product reviews and information available from vendor web sites. After completing this research, I've settled on a product named HotSpotVPN thanks to its wide compatibility across computer operating systems, ease of use, and relatively low price compared to other options.

Introduction

As technology (namely computers and the Internet) has become a larger and larger part of people's daily lives the threat that this technology poses to our safety has increased tremendously. More and more people use computers to help manage their finances, file tax returns, and purchase products online. Needless to say, there is a large amount of very sensitive data on our computers just waiting to be stolen by malicious people. The Internet serves as a conduit for much of the information as we conduct business online and being a public network it has the potential to leave our valuable data out in the open for others to view as they please. One way to protect this information as it passes through the various relays on the Internet is to encrypt the data while it travels between your computer and the trusted party at the other end. One tool that can accomplish this for us is a virtual private network, or VPN.

With this in mind, I set out to collect a list of VPN solutions that could possibly serve the needs of average users—specifically, people who travel a lot or use a variety of (potentially dangerous) wireless hotspots like those in a Starbucks or airport. I wanted to find something that could protect the information they send out over these relatively open networks and keep it safe from anyone running, for example, a packet sniffer on the network. Of course, average users aren't computer experts, so the solution(s) I would eventually recommend would need to be fairly easy to get setup and use. Also, the cost of a solution would need to be fairly small—we aren't dealing with a company who can afford to pay some consultants to setup a VPN provided by Cisco, after all. The VPN must also be reliable, a requirement that would apply to any person, group, or organization that happened to be looking into a VPN, not just my target demographic. Clearly, console-based programs with long, obscure command lines and a high price tag would not be anywhere near appropriate here.

To be completely honest, I would have had absolutely no idea where to begin such research were it not for a podcast available from <http://twit.tv> known as *Security Now*. It is a weekly program that covers a wide variety of topics related to computer security (usually one topic per episode) with a focus on making the information discussed as easy to understand as possible. Indeed, their target audience isn't all that different from the one I hoped to target with this research project. In any case, in the tail end of 2005 a number of VPN solutions were discussed and reviewed over several episodes and this served as an excellent starting point for my own research. From there it was simply a matter of looking into each product they covered in more detail as well as doing a little research of my own to find anything the creators of *Security Now* might have missed.

Background

It continues to amaze me how much power the consumer has been given by advances in technology over the past decade. Once, servers, routers, switches, and other networking equipment were much too expensive for anyone other than businesses to afford. Today I can buy a router with built-in firewall and wireless networking for less than \$40. I can create a server to store and backup data from all my computers for just a few hundred dollars. I can apply for loans, manage my bank account, and purchase just about anything (even food!) online. However, all of this power comes with significant

risks. Now we have to be careful not to open suspicious e-mail messages or run strange executables and monitor what software installs spyware and adware on our machines and we have to be observant enough to spot phishing scams when they arrive in our inbox and the list goes on and on. We even have to protect ourselves on public networks! It's all too much work for people! For most people it feels like you have to be a security expert just to use a computer and the Internet safely and most people seem to just not bother. Part of that is simply ignorance of the risks, but some truly comes from the sheer number of things people need to remember to protect themselves from the legion of threats on the Internet. Hopefully I can ease the pain of wading through the myriad of computer security options by narrowing the list of VPN candidates a little—every little bit helps, after all.

So what exactly is a VPN going to do to protect people, anyway? Why bother with it at all? Mainly, I picture users employing them mainly in places where open wireless networks are available or in cases where the wired network can't be trusted. For example, I consider the previously-mentioned Starbucks wireless network to be a risky place. The same holds true for most of the municipal wireless networks that are beginning to appear in some cities and even Ball State's own wireless network. On the wired side of things, I would see VPNs employed in, for example, a hotel room where the wired network is connected together with a bunch of cheap hubs—in practice, however, I'd recommend their use regardless of how the hotel's wired network is setup. After all, I doubt you can ask the employees what technologies they're using for the network (assuming they even know that information in the first place). Basically, any time your computer may be sending out information over a medium that may be easily monitored by someone (or something) malicious I would strongly suggest using a VPN. Even if you don't do anything "important" on-the-go and aren't that concerned with privacy, it is better to be safe than sorry.

As I stated previously, I have had little difficulty finding information with which to conduct my research and evaluation. The *Security Now* podcasts were an excellent starting point and, helpfully, transcripts were available to facilitate information gathering. Of course, from there individual product pages also provided valuable information although, naturally, one must be wary of the bias that is undoubtedly in such pages.

As it stands, there are several VPN products available for people to choose from. Most use similar technology to encrypt traffic and have versions in one form or another for all major operating systems. There is a strong Windows-centric focus in these products, but that is to be expected given the various versions of Windows have the largest market share by a very, very large margin. Fortunately most options have free versions in addition to less limited paid versions, but I feel most people would be perfectly happy with the free versions. If that isn't the case, there are completely free solutions (including source code) available as well, but this comes at the price of ease-of-use.

Research Description and Results

OpenVPN

Of the solutions covered here, OpenVPN is the one I personally find the most interesting, but it is also the worst choice for most people. It is completely free and open source (hence the name) and has versions for just about any operating system you can think of from Windows (2000 or later) to Mac OSX to Linux to the BSDs. Even a PocketPC version is in the works (OpenVPN Solutions LLC). OpenVPN is also scalable—anyone from individual user to large corporations can use it and tailor it to their needs. All it needs to work is for ports 80 and 443 to be open (with one exception—it can't work through a proxy) and compared to other solutions it tends to be faster thanks to its ability to reduce packet fragmentation (Leo Laporte, *VPNs Three: Hamachi, iPig, and OpenVPN*). Unfortunately, this flexibility comes at the expense of usability. Basically, the issue is that there are simply a lot of options to choose from when configuring it. From *Security Now*:

“The downside, and of course there is one, is it is anything but one click...OpenVPN is a much more complex product. I would consider it the Swiss army knife of VPN solutions. You configure whether you want TCP or UDP protocol, what port you want to run on, and, I mean, well, that's just the beginning.” (Leo Laporte, *VPNs Three: Hamachi, iPig, and OpenVPN*)

Fortunately, some of the pain of setting up OpenVPN can be alleviated with the help of other products. Some models of consumer routers (most notably the Linksys WRT54G/WRT54GL) can be flashed with custom firmware such as OpenWRT (<http://openwrt.org>) or DD-WRT (<http://www.dd-wrt.com/dd-wrtv2/index.php>). These firmware replacements support OpenVPN. My favorite of the two, DD-WRT has a version available that includes the OpenVPN server. Configuring it is as simple as opening the DD-WRT administration page and clicking a checkbox. Configuring its many settings is still a bit of a pain, but at least some of the work is done for you. Fortunately, there is an even better solution: HotSpotVPN

HotSpotVPN

You can think of HotSpotVPN as OpenVPN with all the hard work done for you. No, honestly, it's a repackaging of OpenVPN that handles much of the configuration. Again, from *Security Now*:

HotSpotVPN uses just the OpenVPN system, right out of the box. What they provide is about a \$10-a-month service where they provide the Internet connectivity for anyone using OpenVPN out on the road... It installs exactly the same stuff as if you were to download it from SourceForge, except that they've done all the work of pre-preparing your asymmetric public key certificates. It's all part of the bundle. So you sign up for HotSpotVPN, you get a link in a return email, you click the link, download a package, install it on your machine, and you literally click an icon on your taskbar, and you're connected securely to their servers. (Leo Laporte, *VPNs Three: Hamachi, iPig, and OpenVPN*)

So how much does this service cost? Well, that depends on which encryption scheme you choose to go with. For Blowfish encryption, you will pay \$10.88 a month. For AES-192 you'll pay \$11.88/month. AES-

256 will cost you \$13.88 every month. These subscription fees give you access to the HotSpotVPN software, the HotSpotVPN server, and subscription to the older version of HotspotVPN, HotSpotVPN1 (HotSpotVPN). Why would you want HotSpotVPN1? It is there purely for devices that may support IPSEC and the like, but not the HotSpotVPN software. Their product page claims support for Palm and most PocketPC devices (HotSpotVPN), so I'm not quite sure what they'd be referring to. I guess they're looking out for the poor Windows 95/98/ME user, which OpenVPN/HotSpotVPN don't support. Either way, it seems like a nice bonus feature. Shorter term subscriptions (HotSpotVPN1 only) are available for 1, 3, and 7 days, "for only \$3.88, \$5.88, and \$6.88 respectively." (HotSpotVPN) Some may complain that it may not be wise to trust the HotSpotVPN servers with all your traffic, but I figure you're taking even greater risks by installing their software in the first place. Instead, I consider this an advantage. You don't have to run a server at home, open ports on your router/firewall, or leave any machines on at home to get your secure connection to the net. Overall, I'd say this is a pretty strong competitor.

Hamachi

Another impressive entry in this battle-royal of VPNs is Hamachi. It creates networks in an interesting way compared to other solutions discussed here. Basically, the Hamachi servers act only as a go-between for your client computer and your server back home. It negotiates the connection between the two, avoiding any trouble with having to open router/firewall ports (your server apparently always has a connection with the Hamachi server) (Leo Laporte, "Hamachi" Rocks!). It creates a virtual network which you then decide which machines can be part of that network. You could mix and match computers from several different locations into a single virtual network this way. In fact, I've even heard of gamers using Hamachi to create a LAN with which geographically separate players can game together without having to go through online servers, but that is not a concern of ours here.

Unfortunately, Hamachi's operating system support is nowhere near as complete as OpenVPN or HotSpotVPN. It only supports Windows, Mac OSX, and Linux and the Mac and Linux versions currently are command line only (Hamachi : Stay Connected). With that said, the Windows support is excellent and the software is very easy to install. One *Security Now* listener had it running before he'd even finished listening to episode 18 of the podcast:

"I've got one posting here that someone sent a few hours ago, who posted to our site saying, I do a lot of traveling and have always had issues with using the wireless connections at hotels. I was so happy to have heard about Hamachi that I had it installed and running before I finished listening to your podcast." (Leo Laporte, VPNs Three: Hamachi, iPig, and OpenVPN)

Hamachi comes in two flavors: free and paid. The free version limits your network to one administrator, 16 clients, and it must run as a user application as opposed to a system service. The paid version allows you to have up to 256 clients, multiple administrators, ban users, and run as a service (Hamachi : Stay Connected). Comparing the feature sets of each version, I'd almost say don't bother paying the \$4.95 a month for the paid version, but there's one major problem with the free version: I doesn't act as a relay between your computers. If a NAT router on one end of your connection doesn't handle NAT traversal well for some reason, you may find yourself in a bit of a bind (Leo Laporte,

"Hamachi" Rocks!). For that reason alone I would suggest paying the monthly fee. It is still cheaper than HotSpotVPN, after all.

It would seem that Hamachi is an excellent, easy to use, option as long as you're running Windows. The only significant issues with it are issues with NAT traversal and dealing with closed ports, and the former can be dealt with by paying that monthly fee and the latter probably isn't a problem all that often. Even so, it's something to keep in mind.

iPIG

Rounding out the contenders is the unfortunately-named iPIG (iOpus Private Internet Gateway). It strikes me as a sort of middle-ground between the almost completely do-it-yourself OpenVPN and the easier to setup HotSpotVPN and Hamachi. You can use their client software and either connect to their own servers or setup your own server to connect to, removing the iPIG servers from the equation altogether. The client software is free and there is a free version of the server software. If you use the iPIG server instead of setting up your own, you are limited to 10MB/month, which isn't much data at all. Fortunately, for \$29.95/month that cap can be increased to 30GB. The only limitation on the free server is that only 5 users are allowed—a limit I see few people reaching. For those who need or want unlimited users, a "pro" version of the iPIG server is available for \$99. Also, e-mail support comes with this purchase (iPIG - iOpus Private Internet Gateway). Naturally, running your own server requires that you open some ports on your router and leave a computer running all the time when you're travelling. Unfortunately, this software is only available on Windows. There aren't even command line versions for other operating systems.

Summary and Conclusions

While each product reviewed is a fine solution on its own, there are clearly some that are better than others. While OpenVPN gets the job done, I wouldn't recommend it to anyone unless they were specifically looking for something to tinker with or absolutely didn't want to spend any money or were strongly against closed source solutions. OpenVPN is also notable for its flexibility, but I consider much of that flexibility to be outside the scope of what average users would care to deal with. I would rank it fourth if I were forced to do such a ranking.

Assuming the user is a "do-it-yourself" type of person, I might recommend iPIG. The ability to choose to run your own server is a nice feature to have. Unfortunately, it's only an option for Windows users, so Linux & Mac users don't have this option at all. The price to use the iPIG servers as your VPN server is a more expensive than the alternatives, so I don't think I'd recommend it to someone who only wanted to connect to the iPIG servers. At least it is easy to use and setup, putting it ahead of OpenVPN in my hypothetical rankings even with its own flaws.

Hamachi is the first of these options I feel I could recommend to just about anybody. It's Mac and Linux support is somewhat lacking, but it at least works on these platforms. Windows users, of course, have it easy. The free version is certainly adequate and the paid edition is very reasonably

priced in my opinion. If you don't need the added compatibility of HotSpotVPN's services, I would probably recommend this over it. Following the pattern I've established, I'd rank this second.

HotSpotVPN, as you've undoubtedly guessed given I've saved it for last, is my favorite of these VPN solutions. From a security standpoint, it benefits from the theoretical advantage of open source. It is easy to install and use on Windows and fairly easy to get running on OSX. It is compatible with every OS OpenVPN is and runs on Palm devices. It is over twice as expensive as Hamachi, but remember that HotSpotVPN1 is part of the overall package and that HotSpotVPN1 is the only option for users of the 9x/ME versions of Windows. Its compatibility is unmatched by any other options considered. For these reasons it earns a place as my VPN solution of choice.

References

- Hamachi : Stay Connected. 2007. <<http://www.hamachi.cc/>>.
- HotSpotVPN. <<http://www.hotspotvpn.com/>>.
- Leo Laporte, Steve Gibson. "'Hamachi' Rocks!" 15 December 2005. GRC | Security Now! <<http://www.grc.com/sn/SN-018.txt>>.
- . "PPTP and IPsec VPN Technology." 8 December 2005. GRC | Security Now! <<http://www.grc.com/sn/SN-017.txt>>.
- . "Virtual Private Networks (VPN): Theory." 17 November 2005. GRC | Security Now! <<http://www.grc.com/sn/SN-014.txt>>.
- . "VPN Secure Tunneling Solutions." 24 November 2005. GRC | Security Now! <<http://www.grc.com/sn/SN-015.txt>>.
- . "VPNs Three: Hamachi, iPig, and OpenVPN." 22 December 2005. GRC | Security Now! <<http://www.grc.com/sn/SN-019.txt>>.
- OpenVPN Solutions LLC. OpenVPN - An Open Source SSL VPN Solution. 2006. <<http://openvpn.net/>>.
- Project VOLANS: Comparison Chart. <<http://mia.ece.uic.edu/~papers/volans/table.html>>.
- Ricciardi, Fulvio. Zeroshell. 2007. <<http://www.zeroshell.net/eng/>>.
- Security and VPN Case Studies. 2007. <http://www.cisco.com/web/about/ciscoitwork/case_studies/security.html>.
- Tyson, Jeff. How Virtual Private Networks Work. 2007. <<http://computer.howstuffworks.com/vpn.htm>>.