My Experience with a subscriber VPN
Advantages, costs, pitfalls, workarounds
Part 1 of a 2-part article series

Author: John Krout, Member, Potomac Area Technology and Computer Society (PATACS)
www.patacs.org
jkrout75 (at) yahoo.com

This article is based on a lot of research, several years of use of a corporate VPN at work, and a few months of using a subscriber VPN at home.

VPN is an acronym for Virtual Private Network. The idea is that your use of a VPN provides a secure method of data communication, through strong encryption. The encryption hides the info in your communication, such as content of emails and URLs of web sites, from your Internet Service Provider (ISP) and any other **Man in the Middle**.

WHY VPNS EXIST
That phrase Man in the Middle is important. Your communication with your email server or any Web site may pass through half a dozen or more servers in between. For any one of those in-between servers, any bored or underpaid system administrator, and any hacker breaking in, might install message trapping software to capture info passing through, such as your IDs and passwords for your stockbroker or bank. Those snooping activities are called Man in the Middle attacks. Encryption makes it almost impossible for them to make use of that info.

Originally, when local area networks (LANs) first became available, the only networks were inside a single building where all the computers were connected on the local network, with no connection to anything outside the building.
Later, secure direct circuits, and modems, allowed communication between computers on the inside and the outside.

A very entertaining book, **The Cuckoo's Egg**, written by Clifford Stoll, describes the Bad Old Days before VPNs, when networks were insecure. It is a fascinating read. The author, an astronomer, was given the task of tracking down a 75-cent discrepancy in billing for use of a university local area network. His investigation led him to identify peoples who broke into the network. He found the same people also broke into military computers. He tracked the people to Europe, where they were tried and convicted based on his testimony and a huge pile of printed computer logs as physical documentary evidence. Stoll was a good guy in the middle.

Because of experiences like that, corporations and the federal government have used their own VPNs for many years. VPNs have enabled greater automated data movement, ensuring privacy of the data due to the use of strong encryption.
And, now, VPNs are available to the rest of us.

While using a VPN, the encryption is based on two *digital certificates*. The VPN server provides one to your computer, tablet, and smart phone. Additionally, the VPN server itself has another one. The encryption using those two certificates is based on some very creative research done in the early 1980s by three MIT professors, Rivest, Shamir and Adelman, who founded RSA and Verisign, two companies now at the heart of modern digital security efforts.

A second result of the two-certificate approach is that your account is known to be valid by the VPN server, and the VPN server is known to you to be valid as well.
Without using a VPN, web sites and other internet services get access to the internet protocol address (IP address) of your home router, computer, phone or tablet. This is important because those IP addresses let web sites figure out where you are located. When you use a VPN, the web sites see only the IP address of the VPN server. In this way, a VPN server acts as your proxy, and are sometimes called **Proxy servers**.
Take a look at **Illustration 1**. This shows how a VPN server fits in the overall path of servers between your computer, phone or tablet and the world of the internet. Inevitably, your VPN-encrypted communications pass through your ISP servers, and then possibly through other intermediary servers until it reaches the VPN server. Using a VPN server severely limits any snooping not only by your ISP but also by any servers between the ISP servers and your VPN server. So the Man in the Middle is stymied in that part of the path.

Beyond the VPN server, the communication is unencrypted by the VPN, or *in the clear*, and at that point reaches the destination, which might be for instance a video streaming server, or a credit card company's web server. Of course, that leg of the path also involves intermediate servers.

Because that leg of the overall communications path is not depicted as encrypted, you might think that a Man in the Middle attack would succeed there.

However, these days most of those destination servers use HTTP-Secure protocol (https), which also employs encryption done in a different way, by your Web browser and by the destination server. That's right, a second encryption. As a result, the communication remains secure all the way through the entire path.

But I want to digress for a moment and suggest that your ISP might also behave as a Man in the Middle.

When you use a VPN, the fact that the servers of your ISP see only encrypted data is very significant. Your ISP is always in the best position to snoop, effectively a Man in the Middle for all the web sites you browse, the streaming services you use, and so forth. All of your browsing and other use of the Internet goes through those ISP servers.

Your ISP has a strong economic incentive to take advantage of that best position: data on the web sites you visit and the downloads you select can be quite valuable to third parties. And don’t think ISPs will ignore that incentive simply because you are a

customer of the ISP; the big ISPs convinced the FCC to eliminate Net Neutrality rules so that the ISPs could solicit money from the likes of Netflix and CNN to accelerate delivery of those sites to your computer.
So use of a VPN consistently protects you from snooping by your ISP.

MORE ADVANTAGES OF A VPN

I have been using a VPN and HTTPS from my work site for more than a decade. I have seen no significant impact on communications speed. Computers do the encryption and decryption quite quickly these days.

An advantage of subscriber VPN services is that you have access to hundreds or thousands of VPN servers, in many cases spread around the world. If one is busy or down, you can easily use another. Redundancy is a very valuable advantage.
Another advantage is that you can choose a VPN server located in a country where a local web site or video streaming service is of interest to you. For instance, the BBC streaming service is open only to users located in the UK. When the BBC servers detect a request from a US IP address, the servers ignore it. if you use a VPN Proxy server in the UK, the UK IP address of the VPN Proxy server tells the BBC that you are local, and you then get to use that streaming service.

A third advantage is far less clear. According to PC Magazine, many VPN users in the US subscribe specifically because the federal government has eliminated the Net Neutrality rules. The idea is the ISP cannot throttle back what it cannot decrypt, meaning what it cannot recognize. NordVPN, for one example, actively promotes that idea on their company’s web site.

I am not convinced that idea is correct.

COUNT YOUR VPN-READY DEVICES

Another advantage is that subscriber VPN services let you connect more than one of your devices (computer, phone, tablet) to the VPN *at the same time*. This is important if you use two or more internet-connected devices, like I do. And it is a major convenience factor, allowing you to leave all your devices connected all the time, not just when you actively use each one.

Snoopers can monitor the web browser on your phone or tablet just as readily as they can on your computer. A VPN can and should protect all of those devices.
Several VPN services that I reviewed set a ceiling on the number of concurrent uses by a single account, and that limit varies from 3 to 10.

Because of that, before you select a VPN service, you need to make a realistic assessment of the number of concurrent connections you may need.
For example, in my case: I have two Windows computers, two Android tablets, and one Android smart phone, a total of five devices. My son has a Windows computer, a Linux computer, one android tablet, and one Android smart phone, a total of four devices.
So our grand total is nine.

COMPARISON SHOPPING FOR VPNS

When I was shopping for a VPN service, I came across a review of public subscriber VPNs on **TechRadar.com**, published in March 2019. **Illustration 2** is a table comparing the top three VPN services according to TechRadar's ratings system, and some details about them. The number of servers and countries will likely continue to grow for each of the public subscriber VPNs.

The column labeled ceiling of devices per account indicates the ceiling on the number of computers, tablets, and smart phones on which you run the VPN client software simultaneously.

The column labeled # proxy servers is especially valuable for redundancy purposes. If one VPN proxy server happens to be down, or malfunctioning, then you can try many others. Generally, more is better.

Concerning the number of countries, although the overall situation worldwide is improving all the time, to some extent I think there are diminishing returns beyond about 50 countries. This is because smaller countries have fewer localized streaming services, and often do not have high bandwidth connections to the internet, so VPN servers in many smaller cannot work as rapidly as VPN servers in say the US or Canada or western Europe or Japan or South Korea.

I chose to subscribe to the **IPvanish VPN service**. Its ceiling on the number of concurrent connections is 10.That was the most important factor for me.

Later on, I found that VPN services are now so popular that PC Magazine reviews the services and provides Editor's Choice awards, their long-coveted recommendation. In 2019, the Editor's Choice awards went to three VPN services:

- TunnelBear (www.tunnelbear.com),
- Private Internet Access (www.privateinternetaccess.com),
- NordVPN (www.nordvpn.com).

NordVPN was the one service that was top rated by both TechRadar and PC Magazine.

PRICING

The VPN services have a monthly rate, usually less than $10, and offer discounts if you pay in advance for say 3 months or for a year. Some even offer further discounts if you pay in advance for three years.

Some VPN services have their business offices outside of the US and may charge your credit card to a bank outside of the US. You may wish to let your credit card company know in advance, so that the charges are not automatically blocked by your card company.

This ends Part 1. In Part 2, you will learn about some difficulties encountered on VPNs, and some workarounds.

ABOUT THE AUTHOR: John Krout is a former president of the Washington Area Computer User Group (WAC), one of two groups that merged to become the Potomac Area Technology and Computer Society (PATACS). He has been writing about personal computer uses since he joined WAC in the early 1980s. He is a frequent contributor to PATACS Posts, and occasionally provides presentations on tech issues at PATACS meetings. He lives in Arlington VA and is a writer for the Thales Group, a major maker of automated fingerprint identification hardware, supporting the use of that hardware in the computer system of a major federal government agency.

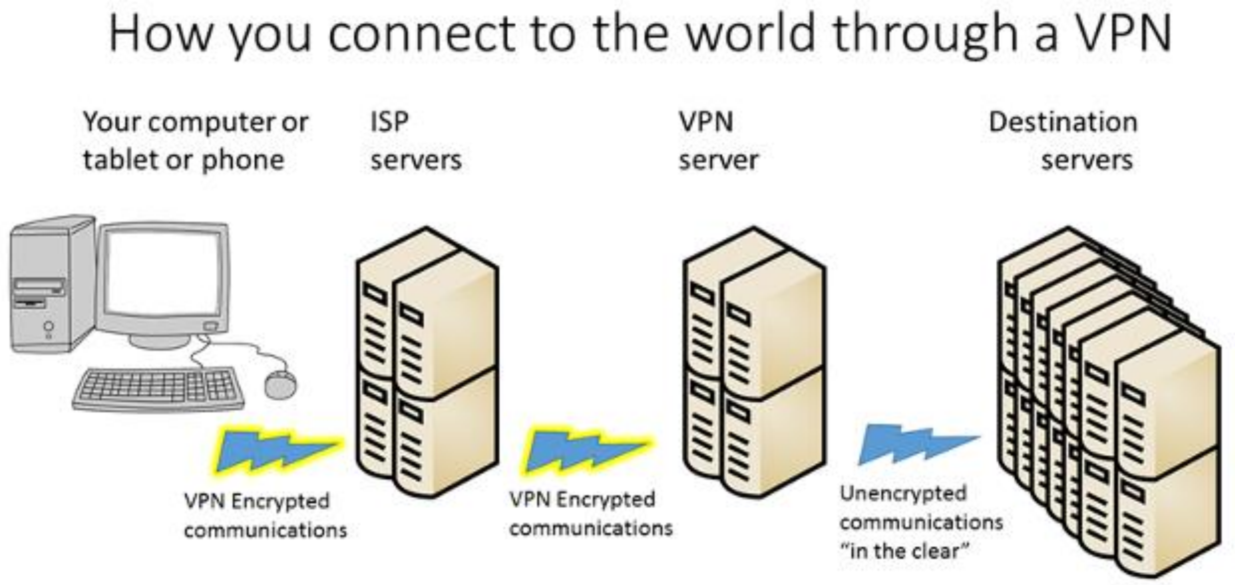
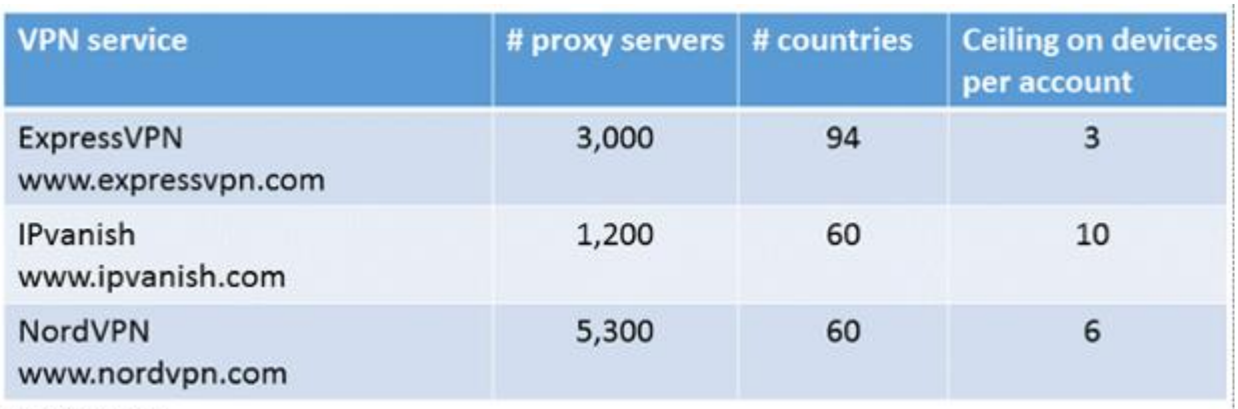

How you connect to the world through a VPN
Your computer or tablet or phone
ISP servers
VPN server
Destination servers
VPN Encrypted communications
VPN Encrypted communications
Unencrypted communications "in the clear"

Illustration 1.



VPN service	# proxy servers	# countries	Ceiling on devices per account
ExpressVPN www.expressvpn.com	3,000	94	3
IPvanish www.ipvanish.com	1,200	60	10
NordVPN www.nordvpn.com	5,300	60	6

Illustration 2.