Explainer: What is a virtual private network (VPN)?

June 17 2013, by Mark A. Gregory

The ways in which we use VPNs have changed. Credit: Stephan Geyer

Have you ever wanted to exist in more than one place at the same time? The laws of physics suggest wormholes through space and time are hypothetical; but wormholes do exist in cyberspace and wonders can be found on the other side.

We call these cyberspace wormholes virtual private network (VPN) connections.

Point-to-point

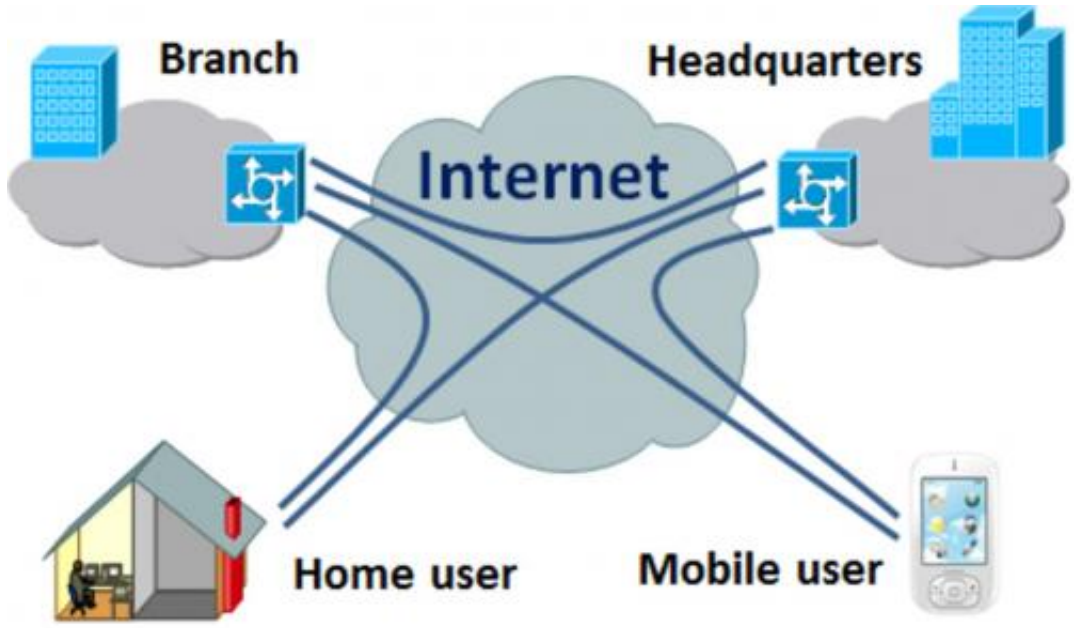
A VPN is a point-to-point connection between a VPN client and server, or a site-to-site connection between two VPN servers. In the diagram below the connection between the branch office and headquarters could be a permanent site to site VPN connection.

Home and mobile users are able to create client on-demand VPN connections to the VPN server at the branch office or the headquarters.

All internet-connected devices have a local public or private internet protocol (IP) address (eg. 192.168.1.20). When connected using a VPN the device gains access to the network at the other end of the VPN and is provided with an IP address on the remote network, even though it is not physically there.

Most devices that connect to the internet today include VPN client software that can be used to create a VPN tunnel from the client computer to the VPN server. Site-to-site VPNs are usually created between firewalls or routers that include VPN server functionality.

The most important thing to know about VPNs is that they provide security and privacy through a combination of the point-to-point tunnelling protocol used and encryption of the information sent over the point-to-point tunnel using, for example, Internet Protocol Security (IPSec), datagram transport layer security or Secure Socket Tunnelling Protocol (SSTP).



Credit: Mark Gregory

Reasons to use

As the internet has evolved so have the ways in which we use VPNs.

A VPN might be used by teleworkers as a secure connection to their office. Students can use VPNs to connect to their school or university.

We can use a VPN to connect to our home network when we're away from home to transfer photos, documents or other items to our home computer or network storage device.

But to understand what makes a VPN special we need to consider how the internet is being used today by business, government and other organisations such as law enforcement or national security agencies.

Multinationals use geo-blocking to segment the world into markets and

control access to products and pricing. The Australian government commenced an inquiry into IT pricing in May 2012, and a submission by the Australian consumer advocate Choice in July 2012 highlighted that Australian consumers are paying substantially more for IT hardware, software and digital media such as music and movies.

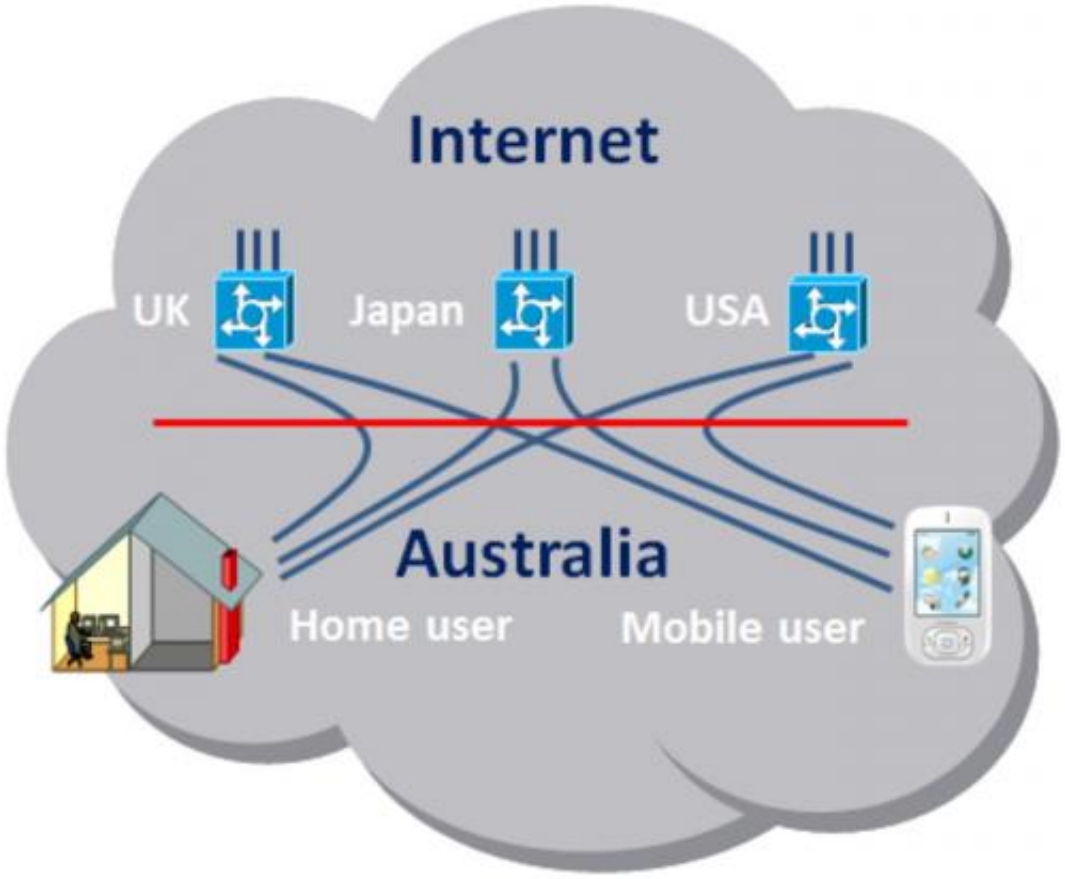
Business is learning how to identify, gather and track information about us online, and every time we use the internet we leave a trail of data that business collects, analyses and uses for targeted advertising.

Governments and their agencies are also trying – to varying degrees – to identify, track and limit what what we're doing on the internet.

Unblocking geo-blocking

The first problem that a VPN can help solve is how to get around geo-blocking.

If you want to watch a television show that is being broadcast over the internet but is only accessible by viewers in one country you can use a VPN to gain access.



Credit: Mark Gregory

If you want to buy products from a company and find those products cheaper on, say, the company's UK online store you can use a VPN to gain access to the online store.

The diagram below provides a description of how VPNs can be used to connect home and mobile users to VPN servers in other countries and be provided with public IP addresses in those countries.

Using a VPN makes it difficult for anyone to identify and track what you do on the internet.

Your traffic is encrypted until it reaches the VPN server at the other end of the VPN tunnel. If the VPN server is in another country it's not possible for your ISP to determine what is passing over the VPN tunnel.

In practice, when you connect to a VPN server in another country your home computer or mobile device will be allocated an IP address in that country, and when you disconnect the IP address would be allocated to the next VPN connection.

VPN servers being used to provide inter-country VPN connections often have large pools of IP addresses that are allocated randomly to VPN connections as they occur.

Many people, possibly thousands, share a pool of IP addresses and only the VPN service provider would know who is connected to each IP address. That said, VPN service providers that offer inter-country VPN services generally do not keep any records of which IP address was allocated to customer VPNs.

For anyone that captures traffic going to and from VPN IP addresses it would appear as a jumble of information that could be attributed to many thousands of people from countries all around the world.

Blocking VPNs

Earlier this month, Iranian authorities blocked the use of VPNs out of Iran. Iranians had been using them to bypass the government's internet filter, which prevents Iranians from accessing websites the government has deemed offensive or criminal – including Facebook, Google Mail and Yahoo.

VPN system developers including Microsoft have been working to develop VPN tunnels that pass through firewalls and internet filters by

utilising typically open internet web IP network sockets that use port 80 (HTTP) and port 443 (HTTPS) protocols.

VPN service providers

There are a large number of VPN service providers available today. When choosing one you should consider:

- whether the service includes VPN end points in one or more countries
- what protocols are provided
- the level of security
- the size of the IP address pool used for VPN connections
- whether your connection details are logged or deleted immediately after you terminate a VPN
- whether the VPN system includes anti-malware and anti-spyware protection
- support for mobile devices
- reliability and bandwidth
- price

There are a number of "free" VPN service providers that provide limited services and gain revenue by serving you with advertisements while you're connected to the VPN.

Another option is to set up VPNs to the homes of relatives or friends that live overseas.

The most important benefits of using a VPN are security, privacy and anonymity.

Why don't you use a VPN today?