Soroban Support Guide

Do I need a VPN?

Document summary

Unless you have a legitimate need to hide your identity, or geographic location, the short answer is you almost certainly never need a Virtual Private Network (VPN) and you may in fact be even be less protected if you attempt to use one!

This Guide explains:

- In outline how the Internet works
- How a VPN works and what a VPN actually provides
  - Explains why using the standard secure HTTPS protocol will usually provide far better security without using a VPN
- The only legal situation when it may be of benefit
  - This is when you have a well managed corporate system where the VPN extends into the corporate network, preferably using corporate owned and managed devices
- Why a VPN is a bad option if it is not actually needed

Original Author: John Steele
Revised by: John Steele
Version: Draft-01
Date: 15 Mar 2023

Copyright Notice

Revisions

Version	Date	Changed by	Summary of change
Draft-01	15/03/2023	John Steele	Initial draft

Table of Contents

1 OVERVIEW

There is a lot of misleading information available about the supposed benefits of using a Virtual Private Network or VPN.

There is one circumstance where a VPN is ESSENTIAL but unless you are using a devices that is owned and run by an organisation that has an expert, and knowledgable, IT department that also provides, or at least controls, the remote devices used to access organisation owned and run services then the supposed additional security is probably a myth and may make you less secure than not having a VPN.

The only other circumstance where a VPN can be of benefit it to access a geographically restricted resource from outside the permitted area. Such access however is typically illegal. An obvious example is to access BBC catchup services from outside the UK.

A VPN is designed to hide the location where the connection to central services is made from but this obviously makes it far more difficult, or even impossible, to determine who is attempting to access any central services. In general this is very bad news if something goes wrong and your data is leaked.

The claim that a VPN will encrypt your data as it traverses the internet is partially true but today almost all traffic is already automatically encrypted end to end so this feature of a VPN provides absolutely no benefit. A VPN will decrypt your data at some server totally outside your control and will then pass it anonymously to the service you are trying to use.

If you use a paid for VPN services, and they are not cheap, the risk of data loss or misuse is low if you use a reputable VPN service but you must be careful to choose such a VPN service and to ensure that it does not compromise any UK data protection legislation e.g. by transferring the processing and display of the data outside the UK.

There are “free” VPN services but they cost money to run. How do they operate as a business? The know who YOU are and who you are communicating with.

This document explains in hopefully simple enough terms how typical services are accessed and why using a VPN is usually a very unwise choice.

2 HOW DOES AN INTERNET SERVICE WORK?

2.1 Overview

In this document it will be assumed that someone on a computer needs to access a service from a remote supplier via a public Internet service.

Such an access may be via a Web Browser such as Microsoft Edge, Google Chrome etc. browsers when using a Microsoft Windows system or perhaps also Apple Safari If using an Apple Macintosh computer. In these cases the data being accessed is typically downloaded and displayed in the local Web Browser program.

Alternatively the service supplier may use Microsoft Terminal Services where all of the processing is done on the supplier's computers and only the data displayed on the screen is passed over the internet.

At a technical level there is actually very little difference between these two cases.

In both of these cases the data should be transferred over the Internet using the secure web protocol HTTPS which already encrypts ALL of the data passing between the local computer and the server. If this is true there is no need for additional encryption.

This document describes in some detail how the data requests are made. An attempt is made to summarise the process if the reader does not want to know the detail.

It outlines the ONLY cases that the author of this guide can identify where a VPN may be of benefit and one of these is potentially illegal!

2.2 Accessing the Internet on any computer

2.2.1 Router power on – Getting an IP address

Your router connects you to the Internet via your Internet Service Provider (ISP).

When your local router powers on, or periodically if left on, it communicates with your ISP and obtains or updates its Internet Protocol (IP) address which is a 32 bit binary number. If viewed it is conventionally displayed as four decimal numbers in the range of 0 to 255 and separated by "dots". It is referred to as "dotted decimal notation. For example 145.3.92.254.

This is the unique worldwide IP address, strictly it is an IP version 4 address, that is used to communicate from your local network and the world. Each number between the dots can be in the range of 0 to 255 which is eight binary digits (bits).

Technically this IP address is "owned" by your Internet Service Provider and they grant you a "lease" to use this address. This lease has a lifetime and will automatically be renewed before the lease expires.

There is a new numbering scheme referred to as IP version 6 which has a much larger address space (the world is running out of IP addresses) but IP version 4 is still widely used and is assumed throughout this document in the examples given.

2.2.2 On PC power on – Your local network

When you switch on your computer it will connect to your local router either via a WiFi or a direct connection and request a locally valid IP address. Typically the router will

remember the address it gave you previously but it may choose to give you another value. The address range is configured into the router and will be from one of a small number of ranges of IP addresses reserved specifically for local private use. Thousands of computers throughout the world will be using the SAME Local IP address range. Your local network is called a Subnet.

The local address depends on the router but will probably be in one of three ranges reserved for this purpose called Private Address Space. These address ranges NEVER appear on the public Internet.

The Internet standards reserve the following Private Address ranges:

- 192.168.0.0 to 192.168.255.255
- 172.16.0.0 to 172.31.255
- 10.0.0.0 to 10.255.255.255

Associated with the local IP address range is a Subnet Mask which specifies how many addresses are actually valid in your private address space which is also called a Subnet. A subnet mask is usually 255.255.255.0 which means that there are 256 addresses available (actually 254 usable ones). 255 being the largest 8 bit binary number. 256 addresses is usually more than enough for home or small business use.

In “network jargon” each of these 8 bit numbers is called an Octet.

In the private address space there is always one IP address that is the address of the router. Typically the final octet is either 1 or 254 (0 and 255 have a special meaning) depending on the make, model and configuration of your router. This is the “default route” or gateway address for your local network.

Your router will pass all necessary details to your computer when it gives your computer its IP address as it boots up.

You can usually logon to your router and look at the configuration and, with care, change it.

2.2.3 Requesting a web page – Get remote address

When requesting a web page or indeed any other web based service the request is usually made using a Uniform Resource Locator or URL. This is a text string that identifies the destination. For example soroban.co.uk

A URL needs to be converted to an IP address before it can be routed over the Internet. This process requires a lookup step that converts the URL to an IP address. The process is known as a Domain Name Service (DNS) lookup.

A URL consists of several distinct parts:

- A protocol specifier such as HTTP or HTTPS (although there are others)
  - HTTP://
    - HyperText Transfer Protocol – unencrypted data transfers to/from web server
  - HTTPS://
    - HyperText Transfer Protocol Secure – securely encrypted data transfers to/from web server
- Optional site specific server name
  - e.g. “www”
- Internet Domain Name

- e.g. “soroban.co.uk”
  - This is the part that defines the routing required over the Internet and selects the folder on the target server containing the site data or at least the first page to be processed, and a number of subfolders
  - .co.uk identifies this as a domain issued by the UK domain registrar
- Plus optional subfolder to access an inner part of the site

When your computer makes the request to your router over the local network it will forward the request to the local network Default Gateway, i.e. your router, which will use the IP address it has been given as a Domain Name Server (DNS) to use as the “first hop” to begin the name lookup process.

If the name is not understood by this hop this will have a number of other addresses to try until the domain name is recognised. Multiple searches can take place in parallel and if the domain name is discovered a “next hop” IP address will be returned with an associated “cost”.

The cost is usually the number of “hops” required to reach the destination. Your router will choose one and then pass your request to the target server. If no route is possible then an error will be returned.

Your computer will remember (cache) the IP address for a time and use it for future requests to the same server.

2.2.4 Processing the request by the server

Once the domain name has been resolved then the processing is passed to the remote server.

For a simple HTTP request the remote server will typically respond with a text string of formatted text as HTML (Hypertext Markup Language) that is interpreted and displayed by your browser. Data can then be typed into any form displayed in the browser and returned to the web server for processing and further responses returned.

If the request is for HTTPS then a further step is required.

In this case ALL data being sent to, and returned from, the browser is strongly encrypted making interception and interpretation of data in transit impossible. Such encryption is now used for ALL private communications. Encryption requires a “shared secret” to be exchanged between the browser and the server and explaining the steps involved is beyond the scope of this document. HTTPS encryption is a well proven secure method of communication where a high level of privacy is required – e.g. performing bank transactions over the Internet.

No further encryption is required.

2.3 What does a Virtual Private Network do then?

2.3.1 Introduction

HTTPS communication is already very secure by design.

There are situations however where additional protection is appropriate and in these case a Virtual Private Network (VPN) can be considered beneficial or even essential.

In all other cases the use of a VPN adds absolutely no additional security benefit and can actually make the data transactions more likely to be at risk rather than adding any additional protection.

2.3.2 What is a VPN – do I need one?

A VPN provides a secure encrypted tunnel between your computer and some server located somewhere in the Internet. When the tunnel is set up ALL traffic from your PC will typically will flow through the encrypted tunnel to the VPN server.

When the requests are made to access an external web site for example the request will appear to originate from that remote VPN server rather than from your own computer.

Your own identity therefore is untraceable. When being used for potentially sensitive data it is obviously very BAD news if the source is untraceable as it can be far more difficult to determine the original cause if data is compromised.

The IP address that would have linked any transactions to at least your home network are now linked to some third party server that may even operate outside your own legal framework.

As an example if the VPN server is located in the USA all of the data entered or displayed is subject to USA law which even varies from State to State. It is very likely to be NON compliant with UK data protection legislation DPA 2018 (was GDPR).

When being used for potentially sensitive data it is obviously very BAD news if the source is untraceable as it can be far more difficult to determine the original cause if data is compromised.

The myth of additional data privacy being provided by the encrypted VPN tunnel is totally unfounded as, if you are using HTTPS in your browser as you should be, then all data transferred is already strongly encrypted between your computer and the service you are connecting to hence no further protection is required.

If you are paying for a VPN service then you may have some contractual control over the location of the VPN server and possible some access to log data for investigation if problems arise.

If you are using a “free” service then consider how is this being paid for? They are incurring significant costs in providing the service and perhaps could be using your data for other purposes.

2.3.3 When is it appropriate to use a VPN?

2.3.3.1 Corporate environment

If you are part of an organisation that owns their own IT infrastructure, and has their own VPN servers within a corporate network, and behind a well managed firewall, then a VPN is essential for remote corporate users to work away from the office.

Managing such an environment requires specific network expertise.

This enables out of office workers to safely operate from home, or while travelling, and still access all of the corporate resources.

2.3.3.2 Accessing geographically locked services outside the geographic boundary

Using a VPN in this way is, in most cases, illegal. An obvious example is to attempt to access BBC TV video services from outside the UK which is not allowed by their license conditions.

If you access BBC catchup services they will check whether the computer is located within the UK and will reject connections where they find a device they suspect is located abroad.

A UK based VPN service MAY bypass the check and enable a connection to be made. It has been reported that certain VPN services located in the UK are also now being recognised and blocked.

