Using the ROE VPN

Introduction

This document describes the ROE VPN service for users.

A VPN is a virtually direct network link, either from a roving salesperson's laptop to the company site, or between company sites. Although STFC has an inter-site VPN, this document is about a VPN service of the roving-salesperson type. Hence the client end is your laptop or home computer, and the VPN makes it virtually connected to the LAN at ROE.

One major use of the ROE VPN is from ROE's own Staff wireless network, and perhaps in some cases even from its Guest wireless network.

An important limitation of the ROE VPN is that on Windows the client software has to be run with administrator privileges. This rules out Windows laptops managed by IT Group for ROE staff. For such laptops, ATC staff can instead use the STFC VPN, while IfA staff and postgrads can use the University's VPN.

Applying for access to the VPN

Ask for this through the help desk.

You will be given a login name and password for access to the VPN. Please keep the login name and password safe and do not disclose it to others.

You will be given an SSL certificate to install in the VPN client software of your computer. Keep this certificate also safe and do not allow others to copy it. Should your certificate be stolen, e.g. along with your laptop, please inform IT Support at ROE so that the certificate can be revoked. The certificate is valid for one year, please make sure you get a replacement before it expires.

The computer that you use to join the ROE VPN must be used exclusively by yourself and other members of ROE, at least at those times when the VPN is connected. Your computer must not share its Internet connection or act as a router, NAT gateway, etc. Your computer must also be up to date in terms of security, with the latest operating system patches and suitable measures against viruses, malware etc.

You will be given three configuration files for your OpenVPN client software:

all.conf or all.ovpn
: With this configuration, all your Internet access will be through the VPN. This configuration is necessary

- if you use the Staff wireless network at ROE, or
- if you need access to Internet resources - such as e-Journals or UK SBS - that are accessible only from ROE.

roe.conf or roe.ovpn
: With this configuration, the VPN will access only ROE, STFC and the University of Edinburgh. This is in general the better choice, as it is less likely to interfere with local connectivity, such as communicating with other computers in your home. It will also be more efficient in using the Internet in general. Use this configuration

- if you are not at ROE, or
- at ROE on eduroam, or
- at ROE on the Guest wireless network.

tcp.conf or tcp.ovpn
: This configuration is equivalent to roe.conf, but uses the TCP protocol instead of UDP. By activating one commented line in this configuration it becomes equivalent to all.conf. UDP is more suited to the purpose of a VPN. However, TCP can in some cases help your connectivity. For example, the firewall at a site you visit may allow your TCP traffic but block your UDP traffic. Another example, Android and iOS apps for OpenVPN tend not to support the smaller traffic fragmentation that our server requires; this sabotages UDP for these apps, but using TCP they may work.

You will be given the certificate and configuration files as an archive file, either in ZIP format (for Windows), or in .tgz format for Linux and Unix-style operating systems, including OS X.

Installing the client software

The VPN software used is OpenVPN. How you download and install it depends on your operating system. Below are described three cases:

1. The Debian Linux 7 (wheezy) case would apply on ROE Linux laptops. If you run Debian or a derivative Linux distribution like Ubuntu, the process should be very similar. For other Linux distributions, explore what the package names are and install them as you install other packages from the Linux distro.
2. The OS X 10.9 (Mavericks) case should also work for 10.7 (Lion) upwards.
3. The Windows 7 case may also work for Windows 8.

If there is no pre-built OpenVPN package for your Linux distro, you will have to build from source, which can be obtained from http://www.openvpn.net. Click on "Community Software", then on "Downloads". The ROE server runs version 2.2.

Debian 9 or Ubuntu 18.04

Install OpenVPN from the Debian or Ubuntu distribution. Reboot afterwards so that the Network-Manager becomes aware of the possibility of OpenVPN-type VPNs.

```
apt-get install openvpn \
  network-manager-openvpn network-manager-openvpn-gnome
reboot
```

OS X 10.9 & 10.10

As an admin user go to http://code.google.com/p/tunnelblick. Download the appropriate version .dmg file and install it. Do not launch the application yet.

Windows 7

Note that this applies only to your own laptop. OpenVPN cannot be used on laptops managed for you by IT Group.

Using and administrator account, take your web browser to http://www.openvpn.net. Click on "Community Software", then on "Downloads". Download and run the binary Windows installer for your platform (32 bit or 64 bit).

Configuring the client software

When you were granted access to the VPN, a ZIP archive and a .tgz archive were created for you. These contain an SSL certificate, which expires after one year. Remember to have it renewed in time. It is split into two files, the private `client.key` and the "public" `client.cert`. The archive also contains the necessary configuration files.

For Windows, use the ZIP archive. For other operating systems, use the .tgz archive. You can download these from the world-wide web, using the same login name and password as you will later use to run the VPN.

Debian 9 and Ubuntu 18.04

Create a suitable, permanent, protected directory and unpack the .tgz archive into it. The certificate is security-sensitive information, so don't let copies of it or the .tgz archive lie around.

```
mkdir        $HOME/openvpn
chmod go-rwx $HOME/openvpn
tar -zxvf /tmp/YourName.tgz -C $HOME/openvpn
rm        /tmp/YourName.tgz
```

In the desktop graphical user interface find out, how to add a VPN. You do not select a VPN type and set up everything from scratch. Rather, you import almost everything from the unpacked files. You will point the setup utility at one of the configuration files (`roe.conf` or `all.conf`) and the utility will learn from this most of the settings. There are a few settings you have to make:

- Enter the username, enter the password, next to the password choose to store this only for this user.
- For the private key there is no password; say so next to the field for entering this password.
- Somewhere the setter-upper has ticked the box that you want to allow all users to use your VPN. Find this tick box and un-tick it.
- Under "IPv4", possibly further down under "Routes" the setter-upper has ignored what the imported configuration file says. For `roe.conf` you must tick to use the VPN only for resources on its network. For `all.conf` you must un-tick this so that the whole Internet is reached through the VPN as if you were at work.
- It is possible that the configuration importer also ignored the compression setting that the file stipulates. Find where the relevant tick box is and make sure LZO compression is turned on.

Repeat for the other configuration file. The profiles will be named "roe" and "all" similar to the imported configuration files. Do not delete the unpacked data; it has not been copied by the configuration importer.

When it comes to replacing the certificate after a year, all you need to do is extract the `client.cert` and `client.key` files and move them into `$HOME/openvpn` to replace the expired files.

OS X 10.9 & 10.10

The Tunnelblick configuration folder is `~/Library/Application Support/Tunnelblick/Configurations`. Unpack the tgz archive into this directory.

```
cd ~/Library/Application\ Support/Tunnelblick/Configurations
tar -zxvf /tmp/YourName.tgz
```

If the folder does not yet exist, run the Tunnelblick application to open it, then unpack the tgz archive into it.

There is a strange interaction between Tunnelblick and the OS X implementation of the Domain Name Service. It is therefore necessary to add Windows-specific settings for DNS servers to the configuration. Edit each `*.conf` file to add the following lines:

```
dhcp-option DNS 195.194.120.2
dhcp-option DNS 195.194.120.1
```

In rare cases this can cause problems with the roe.conf configuration relating to host names used in the local network where you are connected.

When Tunnelblick is run after placing and editing the configuration files, it will convert these into per-configuration subdirectories. This will cause you headaches when, after a year, you have to replace the certificate files, because you have not been told where the used copies are. This is the file tree after configuration conversion:

```
Configurations/
  all.tblk/Contents/Resources/
    ca.cert
    client.cert
    client.key
    config.ovpn
  roe.tblk/Contents/Resources/
    ca.cert
    client.cert
    client.key
    config.ovpn
  tcp.tblk/Contents/Resources/
    ca.cert
    client.cert
    client.key
    config.ovpn
```

When it comes to fixing the configuration or replacing the certificate, those are the files to edit or replace.

Windows 7

Unpack the ZIP archive into `C:\Program Files\OpenVPN\config\`

There is an oddity in the Windows 7 (and later) implementation of the Domain Name Service. It is therefore necessary to add Windows-specific settings for DNS servers to the configuration. Edit each `*.ovpn` file to add the following lines:

```
dhcp-option DNS 195.194.120.2
dhcp-option DNS 195.194.120.1
```

In rare cases this can cause problems with the roe.conf configuration relating to host names used in the local network where you are connected.

Using the VPN

Debian 9 and Ubuntu 18.04

In the desktop graphical interface find the place to turn on and off the VPN. You will normally have a choice of "roe" or "all".

OS X 10.9 & 10.10

First time you have to run Tunnelblick from the Applications folder. From then on it is in the system menu bar, where you can connect or disconnect a particular configuration. Usually, you can use an unprivileged account. If Tunnelblick has to convert or fix configurations or certificates, you may need to give the name and password of a privileged account to get through that hurdle.

Do disconnect the VPN before moving to a different local network (before going to work or going home). Also be sure the VPN is not connected automatically.

Windows 7

You have to use a privileged account. Double-clicking the desktop icon brings a small icon into the system tray. With this you can connect or disconnect a particular configuration.

Topic history

- 2014-03-17 - HorstMeyerdierks - Re-write / conversion from HTML on Intranet.
- 2014-08-08 - HorstMeyerdierks - Add some more info for OS X.
- 2015-07-13 - HorstMeyerdierks - Review the configuration choice after eduroam arrives at ROE.
- 2016-10-05 - HorstMeyerdierks - On Linux rename the .conf files to less harmful .konf.
- 2019-02-15 - HorstMeyerdierks - Rewrite for Linux, where the Gnome GUI is now preferred over a sudo command line.
- 2019-03-26 - HorstMeyerdierks - Add the compression gotcha for more recent Linux GUI configurators (Ubuntu 18.04, Debian 10, ...).

This topic: ITSupport > WebHome > UsingTheRoeVPN
Topic revision: r11 - 2019-03-26 - HorstMeyerdierks