UvA-VPN for Linux
UvA ICTS

UvA-VPN is a device to establish a shielded connection between your personal computer residing outside the UvA and the internal network of the UvA, enabling you to access restricted university facilities (e.g. file servers, UNIX hosts, Zelfbediening, etc.) as if the remote computer were physically part of the UvA network. Additionally a few services require access through UvA-VPN even for hosts already connected to a UvA network.

The following text explains how to set up UvA-VPN on a modern Linux computer.

OpenConnect vs. Juniper’s proprietary software
To set up UvA-VPN on your Linux computer one can choose to either use Juniper’s proprietary VPN software or utilize the Juniper/Pulse capability of OpenConnect, an open-source VPN program used by NetworkManager—the network control package used by most Linux distributions. We will limit ourselves to discussing the latter since the OpenConnect solution is more straightforward and better integrated into the Linux system.

The command prompt
Those not familiar with UNIX might want to consider the following. The instructions discussed below involve using a command prompt. The green frames with fixed-width font, as shown below, represent user-computer interaction through the prompt. For clarity the blue text stands for user input while the black text corresponds to your computer’s output. User input is only submitted after pressing the Enter key so you may imagine all blue lines ending with an invisible Enter character. To open a command prompt call the application named Terminal. Some commands require administrator privileges. This is indicated by the black string “root$” preceding the blue-colored text. To issue a command as root type sudo + space before the command, after which you will be prompted for your user password. Alternatively you can become user root with the su command. For the latter you will need your computer’s root password:

```
$ su
Password: ******
root$
```

Commands preceded by just a black “$” may be issued with common user rights. To leave root-mode press Ctrl+d at the beginning of the prompt or type the command exit.
Step by step instruction

1. If necessary install OpenConnect. Depending on your Linux distro you might need to install the OpenConnect software. Fedora 27 comes with it out of the box, while a bare Ubuntu 17 installation lacks the binaries. On rpm-based systems (Redhat EL, CentOS, SuSE) you would proceed as follows:

```bash
root$ yum -y install NetworkManager-openconnect-gnome
(....)
root$ systemctl restart NetworkManager.service
```

For Debian-based systems (Debian, Ubuntu, etc.) issue the following command:

```bash
root$ apt-get install network-manager-openconnect network-manager-openconnect-gnome
(....)
root$ systemctl restart network-manager
root$ systemctl daemon-reload
```

2. Install the UvA root certificate in your computer's so-called “trust store”:

Open your favourite internet browser and fetch UvA's CA certificate at [http://wifiportal.uva.nl](http://wifiportal.uva.nl) by downloading the “.cer” file associated with the generic or unknown device (not Linux!) and with WiFi network “uva” (on the website it says “SSID/NetworkName: uva”). At the time of this writing the file name was: afe5d244a8d1194230ff479fe2f897bbcd7a8cb4.cer. We will use this name in our example but keep in mind it may change in the future.

With Redhat-based systems this goes as follows:

```bash
root$ cp afe5d244a8d1194230ff479fe2f897bbcd7a8cb4.cer /etc/pki/ca-trust/source/anchors/
root$ update-ca-trust extract
```

On Debian-based systems the procedure is slightly different. Notably the certificate requires a conversion.

```bash
$ openssl x509 -in afe5d244a8d1194230ff479fe2f897bbcd7a8cb4.cer -outform PEM -out certificate-uvavpn.crt
root$ cp certificate-uvavpn.crt /usr/local/share/ca-certificates/
root$ update-ca-certificates
```

Afterwards there is no need to keep the original files.

```bash
$ rm afe5d244a8d1194230ff479fe2f897bbcd7a8cb4.cer certificate-uvavpn.crt
```
3. Open the network configuration panel from the system menu.

4. On the VPN row click on “+” to create a new VPN configuration.
   This will open a new window titled Add VPN and featuring a list of options.

5. Click option Cisco AnyConnect Compatible VPN (openconnect).
   This will open the configuration panel. The tab labeled Identity will be displayed.

6. In the Name text box enter an appropriate name for the VPN configuration such as “UvA-VPN”

7. In the pop-up button labeled VPN Protocol choose option Juniper/Pulse Network Connect.

8. In the Gateway text box enter: uvavpn.uva.nl All the remaining fields should be left unchanged.

9. Click the Add button at the top-right side of the window to save the new configuration.
   In the network configuration panel under VPN we will see a box symbolizing to the newly created configuration UvA-VPN (or whatever name you chose to give it).

10. In the UvA-VPN box toggle the switch to ON.
    This will open the login frame Connect to VPN “UvA-VPN”.

11. Enter your UvAnetID and associated password.

12. Press Enter or click the Login button (not the Connect or Close button).
    Briefly the login frame will display Connecting to host and, if all went well, disappear uncovering the network configuration panel. The slide button for UvA-VPN will be set to ON indicating that your VPN connection to the UvA is up and running. An active VPN is also indicated by a padlock (🔒) in the top bar.

This about sums it up for setting-up UvA-VPN. You may now close the network configuration panel.

Usage

Disconnecting and reconnecting is done through the system menu (i.e. VPN Off → Connect and UvA-VPN → Turn Off). For each time you start UvA-VPN you will be presented the Connect to VPN “UvA-VPN” window asking you to enter your UvA password.

To make adjustments to the existing VPN configuration, or either to delete it, open the network configuration panel (NetworkManager) through the system menu and under VPN click the “cog” button (⚙️) in the UvA-VPN box. The rest should be self-explanatory.