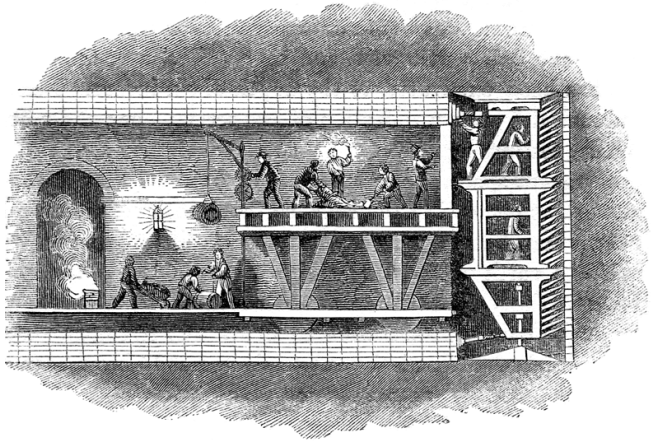
UvA-VPN onder Linux

UvA ICTS



VPN (Virtual Private Network) is een methode om een virtuele tunnel te maken tussen een afgeschermd computernetwerk en een computer buiten dat netwerk waarbij nagebootst wordt dat de computer fysiek deel uitmaakt van het netwerk. Met UvA-VPN kunt u van buiten het universitaire netwerk toch specifieke UvA-diensten benaderen, zoals Zelfbediening, fileservers of UNIX-hosts. Daarnaast verlenen sommige servers alleen toegang via UvA-VPN ook al is de client reeds verbonden met een UvA-netwerk. De onderstaande tekst legt uit hoe men UvA-VPN opzet onder (een gangbare versie van) Linux.

OpenConnect vs. Juniper's proprietary software

Om UvA-VPN te activeren op uw Linux-computer zijn er thans twee mogelijkheden. Ofwel installeren van de officiële Juniper-VPN-software voor Linux, of gebruik maken van de Juniper/Pulse-ondersteuning van OpenConnect, de opensource VPN-software die geïntegreerd zit in NetworkManager, het netwerkbeheerpakket dat door de belangrijkste Linux-distributies wordt gebruikt. Omdat de methode met OpenConnect eenvoudiger is dan die met de fabriekssoftware van Juniper —afgezien van het feit dat OpenConnect fraai geïntegreerd is in de grafische interface van de Window-Manager— behandelen wij alleen deze.

UvA-VPN stap-voor-stap opzetten

1. Installeer, zo nodig, OpenConnect. Afhankelijk van de Linux-distributie die u gebruikt kan het zo zijn dat de aanstuursoftware ontbreekt. Een kale Fedora 35-installatie bevat standaard OpenConnect, terwijl deze bij Ubuntu 18 uit de repository moet worden geïnstalleerd.

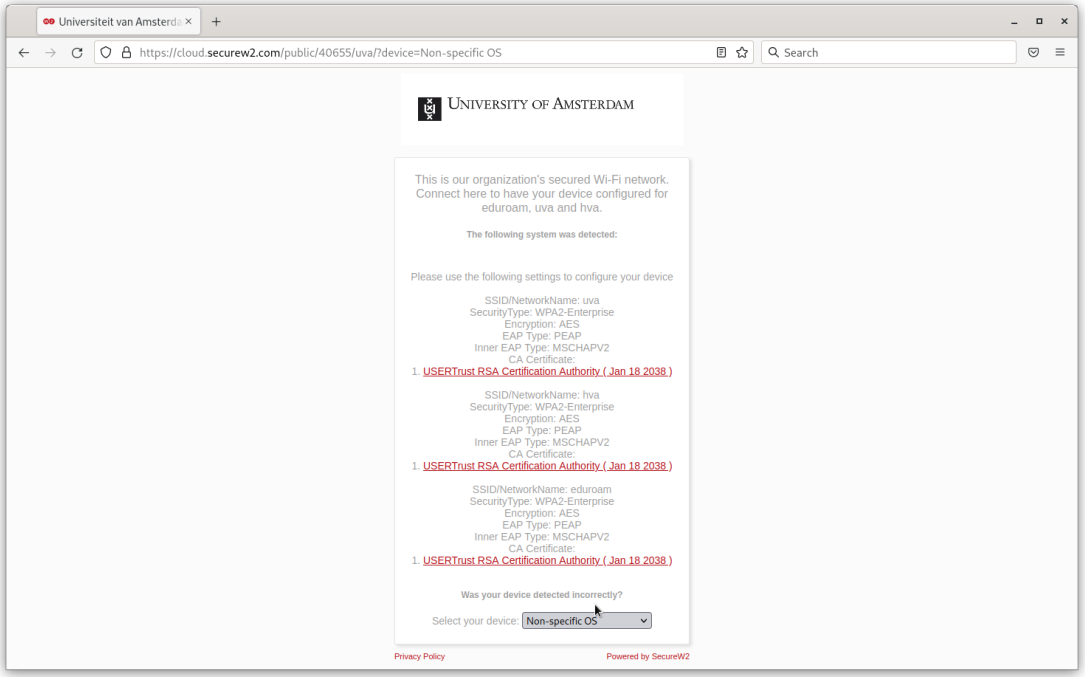
   Op rpm-systemen (Redhat EL, CentOS, SuSE) dient u als volgt te werk te gaan:

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

Voor op Debian gebaseerde systemen (Debian, Ubuntu, enz.) gelden de volgende commando's:

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

2. Haal de UvA-certificaat op vanaf de WiFi-portal: Open in de webbrowser de pagina https://cloud.securew2.com/public/40655/uva/?device=Non-specific OS of ga anders eerst naar `http://wifiportal.uva.nl` en kies bij "Select your device:" de optie "Non-specific OS" (nb. *niet* "Linux"!). U krijgt de volgende webpagina te zien:



Download de file `usertrustrsaca [jdk].cer` onder the bovenste hyperlink USERTrust RSA Certification Authority (Jan 18 2038). In feite maakt het niet uit welke link u kiest aangezien alle drie naar hetzelfde bestand wijzen.

3. Installeer de certificaat in de “trust store” van uw computer.

   Bij de Redhat-familie en SuSE gaat dit als volgt:

```
$ sudo cp usertrustrsaca\ [jdk].cer /etc/pki/ca-trust/source/anchors/
$ sudo update-ca-trust extract
```

   Na afloop kunt u het originele bestand verwijderen:

```
$ rm usertrustrsaca\ [jdk].cer
```

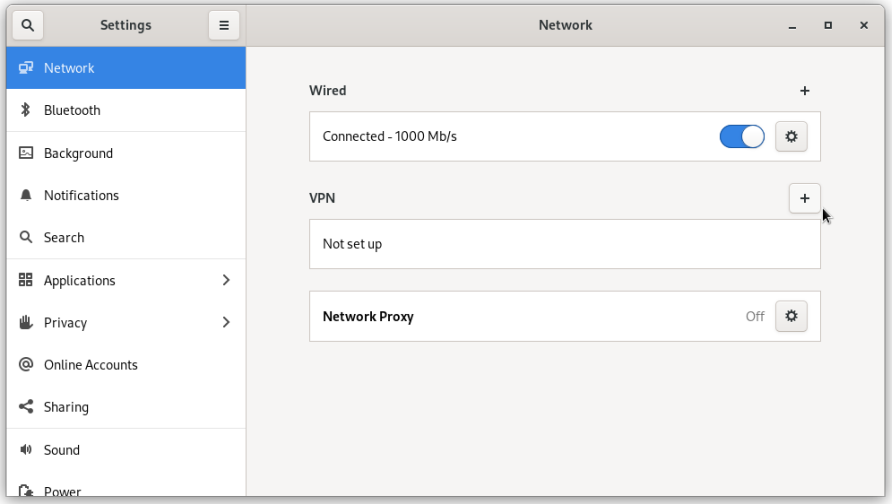
   Bij op Debian gebaseerde distributies gaat het een beetje anders. Voordat het certificaat ingevoerd kan worden dient u het te converteren naar CRT-formaat:

```
$ openssl x509 -in usertrustrsaca\ \[jdk\].cer -out usertrustrsaca\ \[jdk\].crt
$ sudo cp usertrustrsaca\ [jdk].cer /etc/pki/ca-trust/source/anchors/
$ sudo update-ca-certificates
```

   Na afloop kunt u de originele bestanden verwijderen:

```
$ usertrustrsaca\ [jdk].cer usertrustrsaca\ [jdk].crt
```

4. Open vanuit het systeem-menu het netwerk-configuratie-paneel.



5. Klik bij VPN op de "**+**" om een nieuwe VPN-configuratie te maken.
   Er verschijnt een venster genaamd **Add VPN** met een lijst opties.
6. Kies de optie **Multi-protocol VPN client (openconnect)**.
   Dit opent het OpenConnect-configuratiepaneel geopend op het tabblad **Identity**.
7. Verzin bij **Name** een gepaste naam voor de configuratie, zeg "`UvA-VPN`"
8. Selecteer bij de popup-button **VPN Protocol** de optie **Juniper Network Connect**.
9. Vul bij **Gateway** in: "`vpn.uva.nl`"
   Alle overige velden dienen ongewijzigd te blijven.
10. klik rechtsboven op de knop **Add** om de nieuwe configuratie op te slaan.
    In het netwerkpaneel is onder **VPN** een boeking genaamd **UvA-VPN** verschenen (of een door u gekozen naam).

11. Schuif de schakelaar bij **UvA-VPN** op **ON**.
    Dit doet het inlog-venstertje verschijnen genaamd **Connect to VPN "UvA-VPN"**.
12. Vul bij **username:** en **password:** uw UvAnetID resp. bijbehorende wachtwoord in.
13. Druk dan op Enter of klik op de knop **Login** (maar niet op de knop **Connect**).
    Kortstondig verschijnt de mededeling **Connecting to host** na welke, als alles goed is gegaan, het inlogvenster verdwijnt. De schuifknop bij **UvA-VPN** staat nu op toestand **ON** om aan te geven dat UvA-VPN actief is. Een actieve VPN-verbinding wordt ook in de bovenbalk weergegeven door een hangslotje: (🔒).

Hiermee is het opzetten van UvA-VPN voltooid. U kunt het netwerk-configuatie-paneel sluiten.

Gebruik

Het verbreken en opnieuw activeren van UvA-VPN gaat via het systeem-menu (resp. **VPN Off** → **Connect** en **UvA-VPN** → **Turn Off**). Bij verbinding maken moet u telkens weer uw wachtwoord invoeren in het inlog-venstertje **Connect to VPN "UvA-VPN"** en op **Login** klikken.
Om aanpassingen te maken aan een bestaande VPN-configuratie, of om de VPN-configuratie te verwijderen dient u het netwerk-configuatie-paneel weer aan te roepen (via het systeem-menu) en in het kader gelabeld **UvA-VPN** het tandwieltje (⚙) aan te klikken. De rest wijst zich vanzelf.

Commandline

U kunt OpenConnect ook vanaf de commando-prompt bedienen:

```
root$ openconnect --verbose --juniper vpn.uva.nl
```

De VPN-verbinding blijft actief totdat u in de terminal Ctrl + C geeft. Voor meer informatie verwijzen wij u naar de 'man'-pagina van OpenConnect:

```
$ man openconnect
```