Fortinet SSL-VPN under Linux

Stand: b’29. Mai 2020’

1 Preamble

To use Fortinet SSL-VPN according to this guide you need:

• a working Internet connection on your computer (e.g. via WLAN) and
• an account at the CMS or at the Institute for Computer Science, Mathematics or Physics

2 Installation

For the distributions Ubuntu, Debian, Fedora, Centos, openSUSE, Arch Linux, Gentoo, NixOS and Solus the package openfortivpn is available. This is how you can install it:

Ubuntu/Debian:
sudo apt install openfortivpn

Fedora:
sudo dnf install openfortivpn

openSUSE:
sudo zypper install openfortivpn

Arch Linux:
sudo pacman -S openfortivpn

If there is no package available for your system, you have to build one. there is a manual for it.
3 Configuration

Please use a text editor of your choice (vim, nano, gedit, etc.) to create the file “hu-berlin” under /etc/openfortivpn/ with the following content:

host = forti-ssl.vpn.hu-berlin.de
port = 443
trusted-cert = e5a7d56543002ffe1e8962caa5fd6d94053aa702381458247b670877a66f3c6f
username = <HU-Account>

4 Establish Fortinet SSL-VPN connection

Now you can start the VPN connection from a terminal window as follows

sudo openfortivpn -c /etc/openfortivpn/hu-berlin

If openfortivpn should also be used for non-sudo users, please add openfortivpn to /etc/sudoers/.

visudo -f /etc/sudoers.d/openfortivpn