Ira A. Fulton Schools of Engineering
Arizona State University

CSE 543: Information Assurance and Security

VPN Configuration

Setup

Most assignments in CSE 543 take part in a virtualized networking environment to prevent any accidental damage to the Internet or any real-world environments from happening. We provide an OpenVPN-based setup for this course. Students **must** use OpenVPN client (not OpenVPN Connect Client or any other VPN solutions) to connect to the virtualized networking environment. Students cannot work on Networking or Web assignments without first connecting to the CSE 543 VPN.

Installing OpenVPN client

If the student is using Ubuntu or Debian, they may install OpenVPN client using the apt package manager:

```
sudo apt install openvpn
```

If the student is using other Linux OS, they may install OpenVPN client using the default package manager that comes with their Linux install.

If the student is using Windows, they may install OpenVPN client by downloading and installing the "Windows 64-bit MSI Installer" from this page: https://openvpn.net/community-downloads/

If the student is using MacOS (which we recommend against), they may install TunnelBlick by downloading it from https://tunnelblick.net/downloads.html

Using the VPN

At the beginning of the course, the TA will distribute an .ovpn file to each student.
If the student is using Linux (including Ubuntu/Debian), they may simply run the following command:

```
sudo openvpn --config the_ovpn_filename.ovpn
```

If the student is using Windows, they should first copy the provided .ovpn file into the "config" directory under where OpenVPN client is installed (usually C:\Program Files\OpenVPN\), and then restart the OpenVPN client. After, they may connect to the VPN by right-clicking the OpenVPN client icon in the tray area, and then clicking the new VPN item.

If the student is using MacOS and TunnelBlick, they must contact the TA for getting a special version of the config file, since TunnelBlick has special requirements.