1. Introduction

VPN (Virtual Private Network) is used to provide a secure connection between the client machine and the host network. The traffic between the client and the VPN is encrypted. This means that the information is not available in clear text across the Internet. The VPN that ASU uses is Check Point. Client software is required on the client machine. This software is called SecuRemote. The SecuRemote software is pre-configured and does not require any intervention once installed. The software will authenticate the user and allow access if approved. This write-up goes step-by-step through the installation of the VPN client software.

This VPN software is used for remote access to the ASU Network as well as access to systems protected by CheckPoint firewalls.

2. Where to get the software

The VPN software is available for use by the entire ASU community. The web site for VPN at ASU is http://www.asu.edu/vpn. This site provides information for installation, download the software, and an FAQ with information that users might need.

3. Installation of the Secure Client software

Begin by downloading the software to the workstation from the web site listed in the above section.

After the software is downloaded to the workstation, double click the executable to begin the installation. The software self-extracts and begins the installation program. The first window to appear is the License Agreement screen. Click the Yes button to continue.

The VPN software now begins installation. It will take several minutes for the installation to complete. There might be flashes of the screen and the cursor might change icons, but basically it is just running. Be patient.
The setup will then complete and the following screen is displayed. The computer needs to be restarted for the software to finish installation. Click the **Finish** key to restart the machine.

By default the software is bound to all network adapters. In other words if you are using PPP, Ethernet, DSL, or Cable modem the software will be attached to all those network interfaces automatically.

4. **Authentication**

   The ASURITE userid and password are used to authenticate the user. The first start after installation the following window will appear. It needs to update the topology of the network in order to function correctly. Click **Update Now** to update the topology.

The window below will pop up whenever authentication needs to occur. The software will authenticate when the software is first loaded when the machine is turned on and when the user is trying to reach a different resource behind a different firewall.

Finally, the software will inform the user if they are authenticated or not. The screen below displays an authenticated session. If you receive an error try typing in your ASURITE userid and password again.
5. **Off Campus Connections (DSL, Cable Modem, or Other ISPs)**

Some users have non-routable IP addresses configured for their home or other business networks. This provides a greater amount of security. A small change needs to be made to the VPN software to account for this situation.

- Right click on the icon in the taskbar with the golden key.
- Select **Setting** on the menu and the following screen will pop open
- On the right side, select **Properties**. You will now see the following window:

![Profile Properties](image1)

- Go under the **Advanced** tab on the top and select **IKE over TCP** and **UDP encapsulation** as seen in the window below.

![Profile Properties](image2)

6. **Further Information**

For further information on installation of the Secure Client, please call the IT Help Desk at 480-965-6500 or submit a trouble ticket to the [Submit Problem web site](#).