Using OpenConnect to preserve PF configurations

Using OpenConnect to preserve PF configurations

Introduction

OpenConnect is not an ITS-supported VPN client. Use it at your own risk.

The Cisco AnyConnect Secure Mobility Client (hereafter referred to as "AnyConnect") is the only ITS-supported application for establishing a connection to the UT Virtual Private Network (VPN). However, the AnyConnect client on macOS modifies the system's built-in PF firewall configuration upon establishing a VPN connection, and fails to restore the system's PF configuration after disconnecting from a VPN session. This is annoying, and—for those who have implemented custom rules for the system's PF firewall—dangerous.

In order to maintain your customized PF configuration but keep convenient access to the UT VPN, you may use OpenConnect in place of AnyConnect. OpenConnect runs at the command line, supports Cisco AnyConnect VPN connections such as the one used by the UT VPN, and integrates with UT's Duo-based two-factor authentication mechanism.

Installation

OpenConnect can be downloaded from its homepage and compiled. Alternatively, an easier method (should you have it installed) is to use Homebrew:

```bash
$ brew install openconnect
```

Connecting

Connections are established at the command prompt. OpenConnect must be run as root. If your everyday user account does not have sudo privileges, use su to switch to a local account that does. Then, run:

```bash
$ sudo openconnect -u eid@vpn-group vpn.utexas.edu
```

This initiates a connection to the UT VPN as user eid. If you connect to the UT VPN using a particular VPN group, include that.

When connecting, OpenConnect will ask for your password twice; enter your UT EID password at the first password prompt, then enter push (or your preferred Duo two-factor authentication method) at the second password prompt.

Disconnecting

Issuing a SIGINT (by pressing Ctrl-C) disconnects gracefully from the UT VPN and removes any network routes that were put in place to allow for VPN connectivity.

Usage tips

Keep OpenConnect open and visible in your terminal to verify that your VPN connection remains active; at least one user has reported that it disconnects with some regularity.

Support
OpenConnect is not an ITS-supported VPN client. Use it at your own risk.