Virtual Private Network (VPN) Service

TABLE OF CONTENTS

User Documentation Wiki Space

The root page NetEng:User Documentation could not be found in space NCSA Cybersecurity.

NOTE : Connectivity options to use the NCSA VPN have changed recently. Please read through the page and follow instructions below to use the new SSL VPN.

Introduction

A Virtual Private Network (VPN) is designed to give users the privacy of a separate network over public lines by substituting encryption and other security measures for the physically separated network lines of traditional private networks. Hardware and/or software that encrypts and decrypts transmissions sent over already-installed network cabling is usually a much less expensive proposition than installing new network cable for the purpose of keeping information private. Also, in the case of wireless networking, no amount of new cabling would serve to make wireless communication private in any way other than the encrypted approach VPN solutions take.

Who should use the VPN system?

- Anyone who needs to use NCSA services configured to deny remote (non NCSAnet) connections. For example: SMTP and some file sharing services.
- Anyone who needs access to an NCSA system that is on a protected subnet, and therefore unreachable when off-site.
- Anyone who needs access to a UIUC system that is on a protected subnet, and therefore unreachable when off-site.
- Anyone who needs to use Windows shares that are filtered at the NCSA border.
- Anyone who wants to make sure that what they are sending to or receiving from the NCSA network over a wired or wireless network is encrypted.
- We **STRONGLY** encourage people who travel and use other wireless/campus/hotel networks to use the VPN service as a security mechanism.

Connecting to the VPN System

To use the NCSA SSL VPN system users will need to setup Duo and install **DUO mobile for two-factor authentication.** The NCSA DUO instance is separate from the campus instance and will need to be setup separately. After this has been completed, users can use the **Cisco AnyConnect VPN Client**, which can be installed and connected to with little to no effort on the user's part. This is the officially supported VPN client both by NCSA and by Cisco.

Using the Cisco AnyConnect VPN Client (Required)

In order to connect to the NCSA network using the Cisco AnyConnect option, you must first install Duo and then the AnyConnect client. Installation of the AnyConnect client is done through your operating system's native web browser the first time that you connect to the VPN server. After the initial connection, you will be able to connect to the NCSA network by launching the Cisco AnyConnect VPN Client application directly. The Cisco AnyConnect VPN Client supports Microsoft Windows, Apple OS X, and Linux. The client auto-download works better on some operatings systems /browser combinations than others. If you cannot download the client from the VPN concentrator, the client are linked in the next section below.

1. To download the AnyConnect client login to https://sslvpn.ncsa.illinois.edu/ and using your kerberos username and password. *Enter push as your second password.*
   a. Most users should leave ncsa-vpn-default as the group selection.
   b. Windows users should connect using Internet Explorer.
   c. Mac users should connect using Safari.
2. Your browser will start the Cisco AnyConnect VPN Client automated installation process. You might need to enable Java in your browser to automatic download and install the client software. One or more times during the installation process, you will need to grant permission for the software to make changes to your system. Linux users may be sent to a client download link and required to perform a manual installation.
3. When the installation completes, the Cisco AnyConnect VPN Client will likely ask for a second password or will ask you to select either push, SMS or phone. ***Enter push as your second password***. This should send a push on your phone/tablet where you have NCSA DUO installed. Once you approve the DUO login request you should be able to connect to the NCSA network. At this point, you can close your web browser.
4. You can disconnect from the VPN at any time by using the Cisco AnyConnect icon in the system tray (Windows) or the menu bar (OS X).

VPN Profiles

The NCSA VPN provides multiple profiles for users in order to provide the best service for a given use case. All profiles require NCSA credentials and Duo 2FA.

- ncsa-vpn-default
  - Default split-tunnel profile that is the best fit for most users. Only traffic destined for NCSA resources will be tunneled.
- ncsa-vpn-tunnelall
  - All traffic from your device will be tunneled over the VPN. This is the best option for those who are traveling and want the additional security of having their traffic tunneled to a known endpoint. As all traffic is tunneled to the VPN this will cause a loss of access to resources on the local network and increased latency for connections as all traffic will traverse the VPN.
- ncsa-vpn-cerberus
  - This VPN profile has similar behavior to the tunnelall profile and can be accessed by users within the Cerberus group. This profile uses the 141.142.146.128/25 IP range and some services that are locked down to the Cerberus bastion hosts will be accessible from the VPN profile. Please contact your local administrator to ask about access to resources through this VPN profile.

Cisco AnyConnect VPN Client Downloads

In many cases, the VPN client will automatically download and install to your machine while following the instructions in this Wiki page. More detailed process for various operating systems is described in the below section. Should you need (or prefer) to manually download the client, they are provided here:

- Client Downloads

Using the Apple IOS - Cisco AnyConnect Client app

Use the following instructions to configure Cisco AnyConnect client software on Apple iPhone to connect to the NCSA VPN system.

1. Go to the Apple App Store on your iPhone and download Cisco AnyConnect app.
2. On the Home tab select Connections.
3. Then select 'Add a VPN connection'
4. Under the Server Address field enter **sslvpn.ncsa.illinois.edu**
5. Go back to your home tab and toggle the AnyConnect VPN switch.
6. The app will now as you for the following details
   a. Group : *ncsa-vpn-default*
   b. Username : *Your NCSA NetID*
   c. *Password : Your NCSA Kerberos password*
   d. *Second Password : "push" or your Duo Passcode*
7. You will now receive a push notification on your DUO mobile app. Click on the green button to allow VPN connection to be made.
8. You should now have VPN connectivity. You can also verify as you see a small VPN tab on the top corner of your iOS display.

Using the Android - Cisco AnyConnect Client App

NOTE: these instructions may vary from Android version to Android version, but the following are instructions that should hopefully be able to be used broadly. Use the following instructions to configure Android to connect to the NCSA VPN system using the native client.

1. Download the Cisco AnyConnect app from the Google Playstore
2. Open the AnyConnect app and sign up for the end user license agreement
3. To configure you NCSA VPN connection, tap on the **Connect** button.
4. On the **Advanced Preferences** screen, tap **Add New VPN Connection**
5. On the **Connection Editor** screen, fill in the following information:
   a. In the **Description** field, type SSLVPN.
   b. In the **Server Address** field, type sslvpn.ncsa.illinois.edu and then tap **Done**
6. Select the **AnyConnect VPN** icon from your device and then tap **AnyConnect VPN**.
7. On the **AnyConnect** screen:
   a. Choose the ncsa-vpn-default VPN Group Authentication Profile for your location from the **Group** pull-down menu.
   b. In the **Username** and password field, enter your NCSA Kerberos credentials.
   c. If prompted for the **Second Password** field, enter *"push" or your Duo Passcode***.** If you enter "push", this will send a DUO login push on your phone. Accept the push from DUO.
   d. At this point you should have your VPN connection all setup.

Additional Technical Details

Kerberos Authentication
Authentication on the NCSA VPN System is handled by the NCSA kerberos system. When authenticating to the VPN, be sure to use your kerberos username and password.

IP Address Assignments
After connecting to the NCSA VPN System, your machine will be assigned an IP address from the 141.142.146.0/24 network.

Split Tunneling

The default VPN profiles are configured with split tunneling. This means that only traffic being sent to specific IP networks is selected for encryption and transport over the VPN tunnel. In our configuration, these protected networks are 141.142.0.0/16 and 10.142.0.0/16. In some special cases you may need to send all of your traffic over the VPN tunnel such that your system behaves as if it is directly attached to the NCSA network. If this is the case, please contact the Network Engineering team for further information on this setup.

Split DNS

In addition to split tunneling, the NCSA VPN system is also configured with Split DNS. When your system connects to a VPN system that is configured with split DNS, the VPN-specific DNS suffixes are added into your system DNS suffix search list. This aids the VPN client when trying to find network resources on the remote network by DNS name. It is worth noting that this functionality can cause problems when trying to find network resources that are local to the client. If this happens, try connecting to the local resource using the fully-qualified domain name (FQDN).

Cisco AnyConnect VPN Client Automatic Updates

Each time that the Cisco AnyConnect VPN Client connects to the VPN system, it checks to see if any client updates are available for download. If any are available, they will be automatically downloaded and the client on your system will be upgraded.