


Secure Access Using VPN

WHAT IS CISCO SSL VPN?

“Cisco” is the brand name of the VPN appliance  (hardware). The “SSL VPN” stands for Secure Sockets Layer Virtual Private Network. SSL VPN is a service that allows the user to connect securely to the internet via AnyConnect, Web Applications, Telnet/SSH server, Virtual Network Computing (VNC), and Terminal Servers.

Simply put SSL VPN, is a secure way to surf the web to combat internet threats that can be transparent to the user and not detected by your antivirus software. You get the benefits of security, speed and a worry free private web experience All active employee’s have access to the FSU VPN

WHAT IS SSL VPN TECHNOLOGY?

SSL VPN is technologies that allow you to build a secure “virtual” path between your computer (s), web sites, other networks, and the FSU campus network. It acts very much like a classical dialup service, except you are using a data network rather than a voice network to make your "calls". Rather than dialing into a modem on the far end, you are making a connection to a Cisco VPN appliance and to create a secure tunnel from your machine to the VPN appliance, which is located on the FSU network. Thus, everything you send and receive to/from the computer is encrypted like when you access your own personal institution records and/or e-commerce web sites that protect sensitive information. SSL VPN transmits data through an encrypted tunnel to FSU’s Cisco VPN appliance, giving the appearance that the user is on a local network, regardless of the user's actual location.

WHO CAN HAVE ACCESS TO THE CISCO SSL VPN?

NO- ACCESS FOR STUDENTS

1. Cisco SLL VPN services is not intended for FSU students.

YES -ACTIVE FACULTY, STAFF &OPS

1. You must first know that access begins with a valid FSUID.
2. You must have a web browser installed on your computer.
3. You must be part of an FSU LDAP group that has SSL VPN access or (See Attached Sheet)
4. Download the client software at <https://vpn.fsu.edu>

FLORIDA STATE UNIVERSITY SSL VPN ACCESS

YES- VENDORS, CONSULTANTS, EXTERNAL COLLABORATORS

1. You must first know that access begins with a valid FSUID.
2. You must have a web browser installed on your computer.
3. Vendors, Consultants or External Collaborators must have their FSU sponsor call the help desk technician so that they can create the guest account. At the same time ask the technician to put in a help request for "Core Networking" to create their VPN account.
4. Download the VPN client software at <https://vpn.fsu.edu> (Read ahead before you begin)

PREREQUISITE A USER MUST HAVE TO CONFIGURE SSL VPN

- A FSUID ACCOUNT (LOGIN NAME AND PASSWORD).
- AN SSL-ENABLED BROWSER (SUCH AS, INTERNET EXPLORER, NETSCAPE, MOZILLA, OR FIREFOX).
- EMAIL account

BEFORE YOU START – THINGS YOU NEED TO KNOW

- BEFORE INSTALLING - LOG OUT AND SAVE ALL OF YOUR WORK
- EXIT ALL APPLICATIONS INCLUDING VIRUS PROTECTION SOFTWARE
- AFTER THE VPN CLIENT INSTALLATION, YOUR COMPUTER MUST BE REBOOTED
- FSU VPN IDLE TIME IS 30 MINUTES
- REMEMBER TO DISCONNECT FROM VPN WHEN YOUR JOB IS COMPLETED
- USER'S GUIDE IS LOCATED AT
http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect20/administrative/guide/admin2.html#wp1001289

SYSTEM REQUIREMENTS

The following table indicates the minimum system requirements to install the Cisco AnyConnect VPN Client on each of the supported platforms.

Operating System	Computer	Requirements
<ul style="list-style-type: none">• <u>Windows 2000 SP4.</u>• <u>Windows XP SP2.</u>• <u>Windows Vista.</u> (*For optimal user experience, we recommend using this product with Vista Service Pack 1.)	Computer with a Pentium®-class processor or greater. In addition, x64 or x86 processors are supported for Windows	<ul style="list-style-type: none">• 5 MB hard disk space.• RAM: – 128 MB for Windows 2000.

FLORIDA STATE UNIVERSITY SSL VPN ACCESS

Operating System	Computer	Requirements
	XP and Windows Vista.	<ul style="list-style-type: none"> – 256 MB for Windows XP. – 512 MB for Windows Vista. • Microsoft Installer, version 3.1.
<p>AnyConnect supports Linux Kernel releases 2.4 and 2.6 on 32-bit architectures, and 64-bit architectures that support biarch (that is, that run 32-bit code). The tun module is required. All of the distributions we have tested include the tun module by default.</p> <p>The following Linux distributions have been tested and are known to work with the AnyConnect Client, while following the requirements listed in this document:</p> <ul style="list-style-type: none"> • Ubuntu 7 and 8 (32-bit only). • Red Hat Enterprise Linux 3 or 4. • Fedora Core 4 through 9¹. • Slackware 11 or 12.1. • openSuSE 10 or SuSE 10.1. 	<ul style="list-style-type: none"> • Computer with an Intel i386 or higher processor. • 32-bit processors are supported. • Biarch 64-bit - standalone mode only; web-based install/connect is not supported. 	<ul style="list-style-type: none"> • RAM: 32 MB. • About 20 MB hard disk space. • sudo access for the security appliance to download and install the AnyConnect client, or to update the AnyConnect client. • sudo: 1.6.6 or later required. • glibc users must have glibc 2.3.2 installed. For example, libc.so.6 or higher. • libstdc++ users must have libstdc++ version 3.3.2 (libstdc++.so.5) or higher, but below version 4. • Firefox: required 1.0 or later (with libnss3.so installed in /usr/local/lib, /usr/local/firefox/lib, or /usr/lib). • libcurl: required 7.10 or later. • openssl: required 0.9.7a or later. • java: required 1.5 or later.² • zlib: required 1.2.3 or later. • gtk: required 2.0.0, gdk: required 2.0.0, libpango: required 1.0. • iptables: 1.2.7a or later. • kernel: tun.o loadable module required. The tun module supplied with kernel 2.4.21 or 2.6 is required.

FLORIDA STATE UNIVERSITY SSL VPN ACCESS

Operating System	Computer	Requirements
<u>Mac OS</u> X, Version 10.4 or later	Macintosh computer	50 MB hard disk space

To use Fedora 9 with the AnyConnect client, you must first install Sun Microsystems JRE, preferably JRE 6, Update 5 or higher.

The default Java package on Fedora is an open-source GNU version, called Iced Tea on Fedora 8. The only version that works for web installation is Sun Java. You must install Sun Java and configure your browser to use that instead of the default.

ANYCONNECT CLIENT DISCONNECT BEHAVIOR

If you click Disconnect, the AnyConnect client, starting with Release 2.2, terminates the connection, as shown in the status bar at the bottom of the dialog box, and the AnyConnect GUI displays a login dialog box with a "Connect to" combo box and a Select button. To reconnect, the remote user must select a new host server to connect to or click Select. At that point, the appropriate authentication prompts are displayed.

INTERNET EXPLORER PROXY WITH THE ANYCONNECT CLIENT

If you have Internet Explorer configured with a proxy, you must activate the "Use HTTP 1.1 through proxy connections" setting to use the AnyConnect client. If this option is not set, the AnyConnect client connection does not come up.

In Internet Explorer, choose Internet Options from the Tools menu. Click the Advanced tab, and under the HTTP 1.1 Settings, check "Use HTTP 1.1 through proxy connections."

SETTING THE SECURE CONNECTION (LOCK) ICON

The Lock icon indicates a secure connection. XP automatically hides this icon among those that have not been recently used. The end user can prevent XP from hiding this icon as follows:

Step 1 Go to the XP taskbar right click.

Step 2 Select "Customize" , the screen will pop up Customize Notifications.

Step 3 Select "Cisco Systems AnyConnect VPN Client" and set to "Always Show."

FLORIDA STATE UNIVERSITY SSL VPN ACCESS

Step 4 Click on the OK button. Click on the Apply button.

This feature helps when your computer begins slowing down other application on your computer, look for the VPN icon to see if you are connected to the VPN. Disconnect if you are not using the VPN.

IN RESPONSE TO A NETSCAPE, MOZILLA, OR FIREFOX "CERTIFIED BY AN UNKNOWN AUTHORITY" WINDOW

The following procedure explains how to install a self-signed certificate as a trusted root certificate on a client in response to a "Web Site Certified by an Unknown Authority" window. This window opens when you establish a Netscape, Mozilla, or Firefox connection to a security appliance that is not recognized as a trusted site. This window shows the following text:

Unable to verify the identity of <Hostname_or_IP_address> as a trusted site.

Install the certificate as a trusted root certificate as follows:

Step 1 Click the Examine Certificate button in the "Web Site Certified by an Unknown Authority" window.

The Certificate Viewer window opens.

Step 2 Click the "Accept this certificate permanently" option.

Step 3 Click OK.

The security appliance window opens, signifying the certificate is trusted.

INSTALLING THE ANYCONNECT CLIENT ON A SYSTEM RUNNING WINDOWS

To install the AnyConnect client on a PC running Windows, follow these steps. We suggest you accept the defaults unless your system administrator has instructed otherwise.

Step 1 Exit all Windows programs, and disable any antivirus software.

Step 2 Download the AnyConnect client package file from the FSU site.

Step 3 Double-click the package file. The welcome screen for the Cisco AnyConnect VPN Client Setup Wizard displays.

FLORIDA STATE UNIVERSITY SSL VPN ACCESS

Step 4 Click **Next**. The End-User License Agreement displays. Accept the license agreement and click OK. The Select Installation Folder screen displays.

Step 5 Accept the default folder or enter a new folder and click **Next**. The Ready to Install screen displays.

Step 6 Click **Install**. The client installs and displays the status bar during installation. After installing, the Completing the Cisco AnyConnect VPN Client Setup Wizard screen displays.

Step 7 Click **Next**. The wizard disappears and the installation is complete.

Step 8 You must reboot your computer.

HELP DESK INFORMATION

HOURS M-F, 8AM-5PM

CALL HELP DESK AT 644-HELP

LOCATION

C6130 UNIVERSITY CENTER