Using the TCNJ VPN

Updated 2/7/13

Introduction

The College has implemented Juniper Networks' VPN solution to provide an easy to use VPN for the College community. The VPN can be used to securely access on-campus resources from anywhere on the Internet.

Requirements

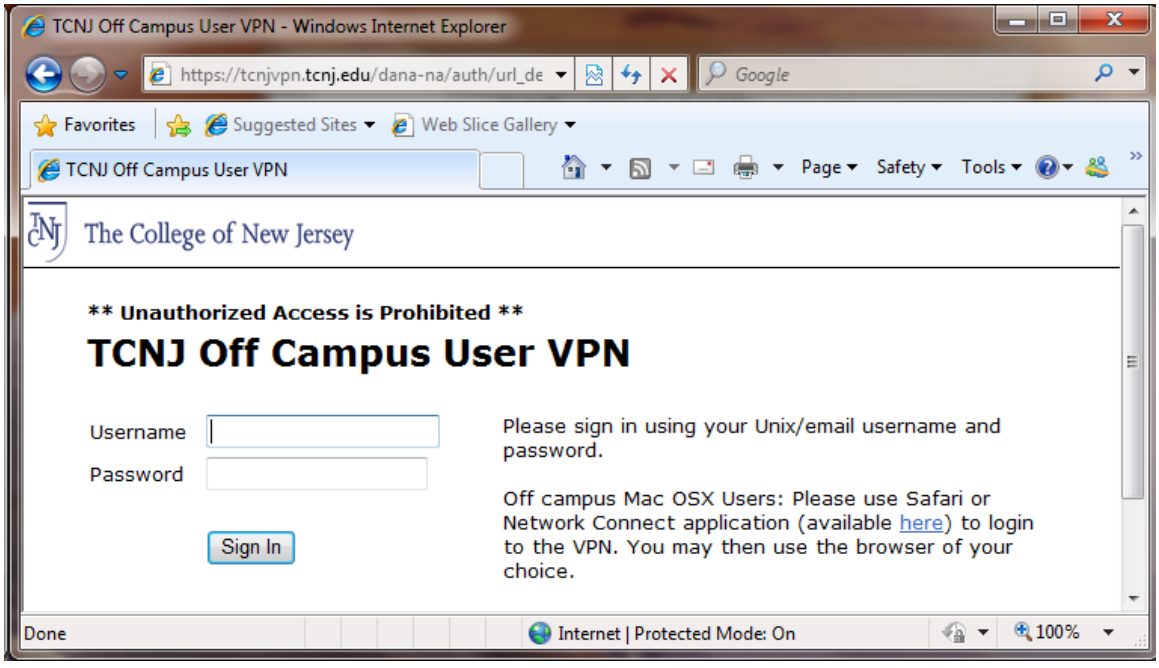
- TCNJ login and password *(e.g. your email login and password)*
- Windows 8/7/XP, MacOS X, or Linux *(while the VPN works with 32-bit Linux kernels, the College is not providing support for Linux users at this time)*
- Java Virtual Machine from www.java.com
- A web browser *(the College has tested IE and Safari)*
- Note that Windows 95/98/Me/2000 as well as Mac OS 9 are not supported.

Signing in

Open your web browser and point it to the following URL

http://tcnjvpn.tcnj.edu

You should see the login page below.

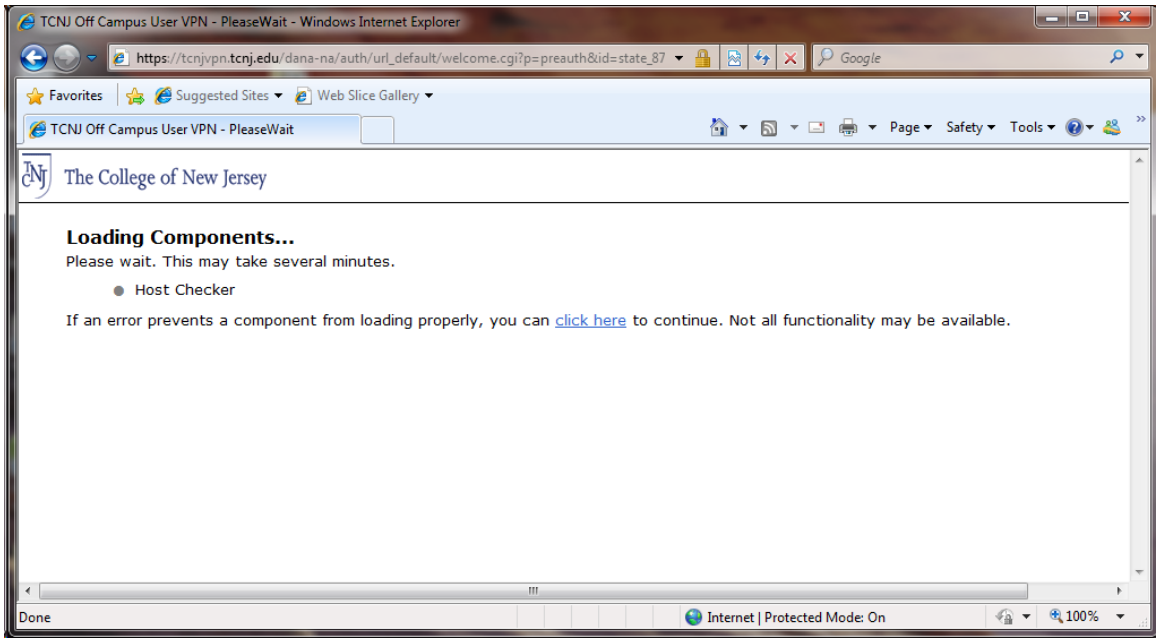


Enter your Unix/email login name and password in the respective boxes and click the "Sign In" button.

The first time you use the VPN, it will download and install a small VPN client to your computer. You may need to click through some warning boxes that pop-up. It is safe to agree to continue. The next time you use the SSL VPN from the same computer, the process will go much quicker since you won't have to install anything.

To reduce the risk of a VPN user's computer spreading malware into the campus network, IT has implemented a feature called Host Checker. Host Checker is a client side agent which is installed and run from your computer automatically when you login to the VPN that performs endpoint checks related to anti-virus software, OS patch level, host based firewalls, and services that may be responsible for sending spam. This information is checked in real time and no information about your identity or computer is permanently stored. Please see the addendum for instructions to enable your Windows XP firewall.

After successfully logging into the VPN, you will see the screen below. This is Host Checker being installed on your computer.



Host Checker uses a series of modules to check and verify different components on your computer. This may take a few moments the first time it is run. You may see the screen below appear and disappear several times.

Security checks

If your computer passes the security requirements, you will see the Junos Pulse program launch and you will be connected to the VPN. If your computer does not meet the security requirements or if the particular configuration of software you have chosen to run isn't recognized by the VPN you will see the screen below, in yellow. The specific reason your computer failed will be listed at the very bottom of the screen under the "Reasons" heading.

You will be presented with a "Continue" button that allows you to certify that your computer meets the security requirements listed above and posted within the message displayed on your screen. Only select this button if you are certain your computer meets those security requirements.

There are 4 reasons that your computer could fail the requirements:

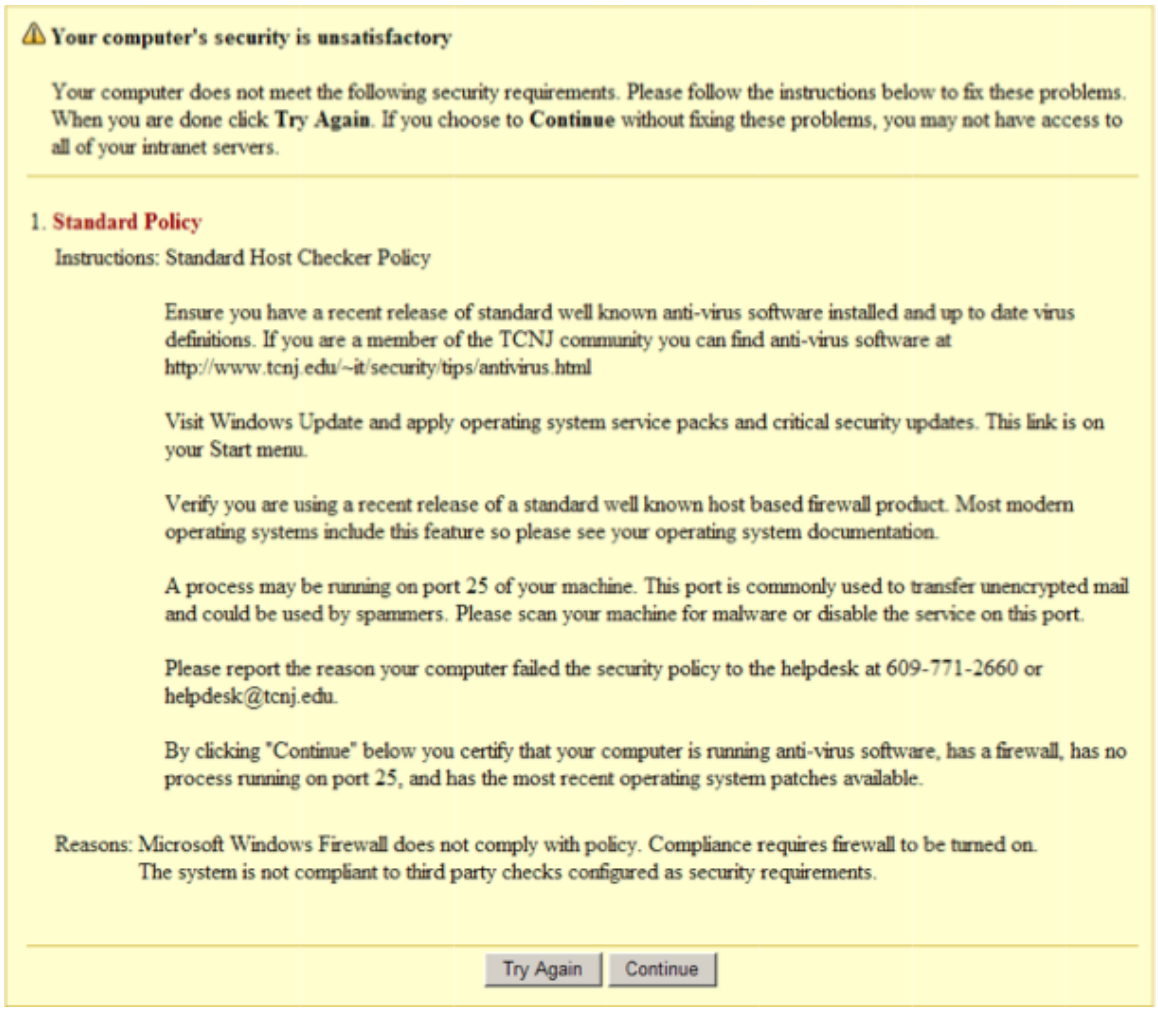
1. The error message: "[Anti-Virus Software] does not comply with policy. Compliance requires latest virus definition files." means you are not running anti-virus software, your virus definitions are very old, or you are not running well-known anti-virus software. TCNJ community members can visit http://www.tcnj.edu/~it/security/tips/antivirus.html to download anti-virus software. Otherwise, verify with your anti-virus software vendor that you have up-to-date definitions.

2. The error message: "This operating system is not allowed in accordance with security requirements." means you have not applied patches or security updates to your computer, including service packs. You must install the most recent service pack for your operating system. Please find the Windows Update link on your start menu or programs menu and apply all critical patches.

3. The error message: "[Firewall] does not comply with this policy. Compliance requires firewall to be turned on." means you are not using a firewall on your computer. Please see your operating system documentation to enable your firewall or download one from the approved vendors list.

4. You have a service running on port 25 of your computer. This port is commonly used to send email and this is unusual for end-user computers. Your machine may be infected with a virus or Trojan horse program. Please run a full virus scan on your computer and try again.

In this sample screen below, the sample computer failed for not having a firewall enabled. Please note the "Continue" button.

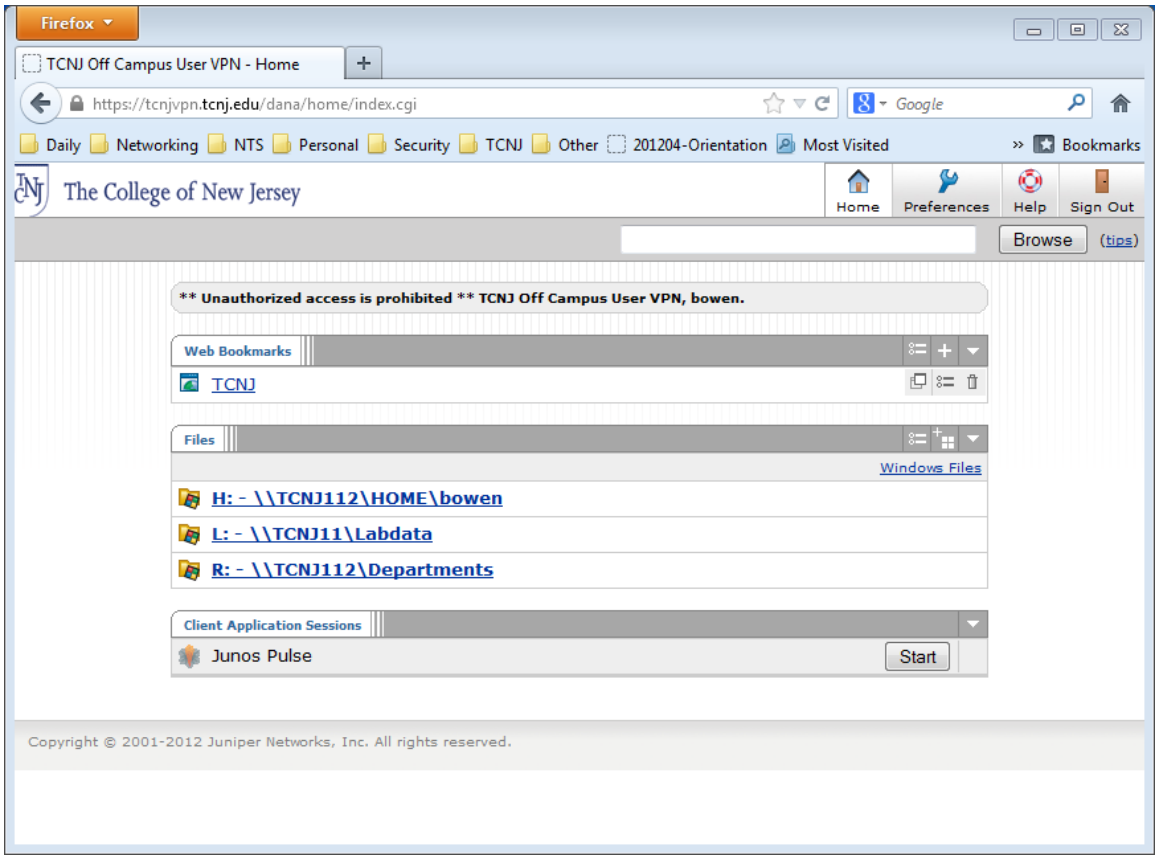


Periodic checks during your session

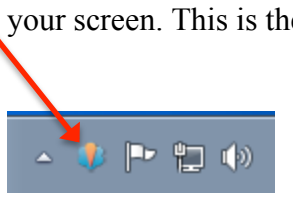
Hostchecker will report the status of your computer's security status periodically if your computer does not meet the security requirements. You may see this red icon in the lower right system tray near the clock of your Windows system. Clicking on this red icon will present a screen similar to the sample message above, in yellow. You will be presented with the option of turning off the warnings for the remainder of your session.

Once logged in

After the VPN successfully starts up, you should see the following in the web browser.



You should also see the following icon on the system tray in the lower right hand side of your screen. This is the Juniper Pulse VPN Client icon.



If you don't see this icon, you should click the "Start" button in the Junos Pulse section of the page that is currently displayed in your browser.

Once connected, you should be able to access most on-campus resources and any resource the traditional VPN was able to access. The VPN uses "split tunneling" which means that when you access TCNJ systems, it will direct the traffic over the VPN. If you are accessing a non-TCNJ system (e.g. www.google.com), your connection will not go over the VPN but will instead go directly from your computer to the site you want to visit. With split tunneling, there is no bandwidth penalty for browsing non- TCNJ sites while being connect to the TCNJ VPN. Once the VPN is started, you do not need to keep the web browser open for the VPN to continue to function.

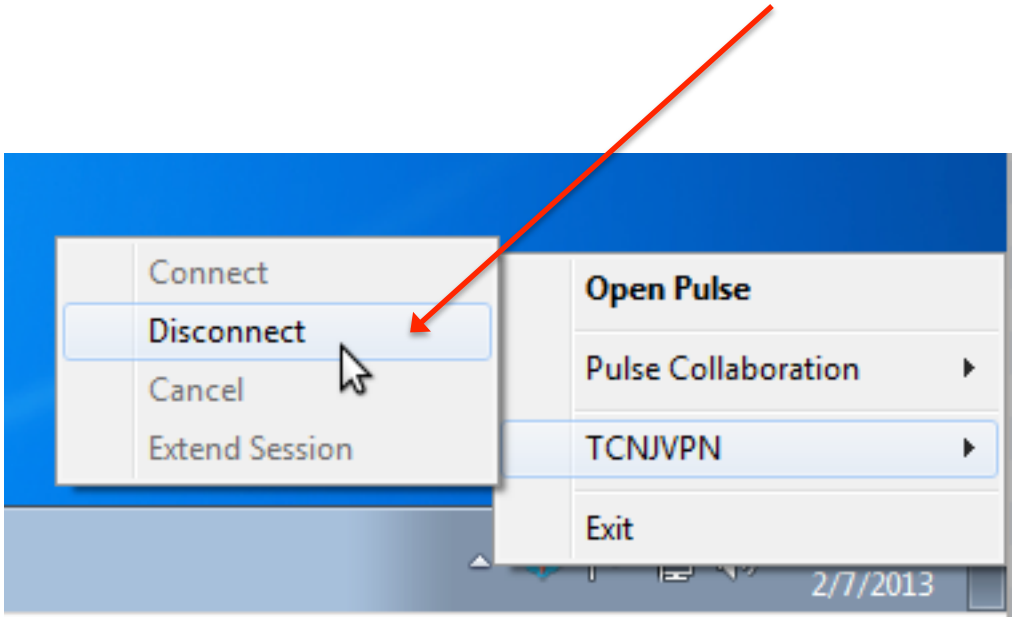
It should be noted that there are timeout values set for the VPN. If no traffic passes over the VPN for 60 minutes or more, the VPN will automatically end your session (idle timeout). In addition, the maximum amount of time you can be on the VPN in any single session is 24 hours (max session length). So, if you tend to always be connected, you will need to re-login at least once each day.

Network file access

You will see your network file shares once you login. Through this menu you can upload and download files and manage folders.

Signing out

When you are done using the VPN, you should sign out. You can click on "Sign Out" from the top right of the web browser window you used when signing in. If you closed the web browser window, you can sign out by right- clicking on the Pulse icon in the system tray and choosing "Disconnect" from the pop-up menu.



Getting Started with MacOS X and Linux

While these instructions have focused on the Microsoft Windows platform, the basic concepts should work on MacOS X and Linux 32-bit desktops. Both require a Java Runtime to be installed. Safari on the Mac should work fine. TCNJ IT is currently unable to provide support for home Linux systems.

Troubleshooting

If you run into problems getting the VPN to work, one of these solutions may solve your problem.

Problem #1: Your browser hangs after logging in, but before or while the VPN client is being installed.

Solution #1: Quit the browser and go into your Start > Control Panel > Add/Remove Programs section. Look for "Junos Pulse" and remove it if it exists. Also, remove any "Java 2 Runtime Environment" or "J2SE Runtime Environment" items. Now go to http://www.java.com/ and click on the "Download Now" icon. After you install the latest Java Runtime, restart your browser and try the SSL VPN again.

Problem #2: I still can't seem to get the VPN client to automatically download and install.

Solution #2: You can try manually downloading and installing the client. Go back to the SSL VPN web page and click on the "Manual VPN Client Install" download link. Select the Junos Pulse client appropriate for your operating system.

Problem #3: You were able to login to the VPN and the VPN client seemed to install okay, but it just doesn't work.

Solution #3: Make sure the VPN icon is in the system tray and is not greyed-out. If it isn't in the system tray, try clicking the "Start" button on the VPN web page. If that doesn't work, check to make sure you don't have any other VPN clients installed such as CheckPoint VPN client, Cisco VPN client or Netscreen VPN client. Other VPN clients may interfere with the SSL VPN client operations. Either disable them or use the Add/Remove Program option in the Control Panel to delete the other VPN clients.

Problem #4: I keep getting disconnected from the VPN after leaving my machine for a while.

Solution #4: There are two timeout values for the VPN. One is an "idle timeout" which is set for 60 minutes. If no traffic passes over the VPN for 60 minutes, it will end your session. You should get a pop-up about 5 minutes prior to warn you. The other timeout value is a "max session length." This is the maximum amount of time you can be signed onto the VPN for a given session. This is set to 24 hours. After 24 hours, the VPN will end your session, and you will need to login again. It should also warn you about 5 minutes prior.