



Enterprise System & Services — Telecommunications Division

Rutgers University VPN Access

Introduction

Virtual Private Network (VPN) is technology that allows remote users to gain access to Private Enterprise Network resources over the Internet. Rutgers has VPN solutions that allow users of high speed Internet and personal ISP accounts access to Rutgers' private network resources such as printing, file sharing and locally restricted websites. VPN provides authenticated access to RUNet resources that require the user to maintain a valid NetID (account on the RCI and ICI systems, eden, rci, pegasus, andromeda, clam and/or crab). See <http://netid.rutgers.edu/>.

WebVPN, PC Client VPN and SSL Client VPN are the three available VPN access solutions available to the University community.

Requirements

In order to establish a WebVPN or SSL Client VPN session, a SSL capable web browser is required. A VPN session requires that the PC client support the PPTP or IPSEC protocols. The client then has to be configured with the name of the VPN server, **vpn.rutgers.edu**. The account and password to be used for authentication is the NetID. Configuration guides are available for Windows9x, and Windows2000. Other 3rd Party VPN client software may also work, but are not supported. [CiscoVPN Client](#) (NETID required) and [configuration](#) compatible with Windows9x, WindowsNT, Windows2000 is available.

WebVPN

WebVPN enables a single SSL capable web browser instance to be authenticated as part of the Rutgers Network. All other data and other web browser instances will maintain communication through the user's ISP. This allows the flexibility of having a normal Internet connection available while web based RUNet resources are being simultaneously accessed. This version of VPN is simple to use, but offers limited functionality. If you encounter problems or require a larger feature set, please use SSL VPN Client or download the Cisco VPN Client.

SSL VPN Client

SSL VPN (Secure Socket Layer - Virtual Private Network) requires no local installation of software. It provides the same access as a PC Client VPN (see below). **NOTE: SSL VPN Client works only with Windows 2000 and Windows XP.** A Secure connection can be created with the VPN from any Internet terminal by connecting to the VPN from a SSL capable browser. To access the VPN SSL VPN Client, point your browser at <https://vpn.rutgers.edu> and log in using your Rutgers NetID. After logging in, a self-installing package (requires **Active X be installed**) will install software on the target PC. Once completed, the PC will be "virtually" on the Rutgers network (RUNet). **NOTE: Administrator privileges are required for this installation.**

PC Client VPN

[VPN Client software](#) can be loaded directly onto a workstation. Microsoft Windows Platforms usually come bundled with a VPN Client. **NOTE: Use of this client is discouraged because the connection created with the VPN is not secure.** Cisco VPN client software is available for download for each of the following operating systems, [Microsoft Windows 9x-XP](#), [Linux](#) version 2.2 or higher and [Macintosh](#), MAC 10.x or higher. (A valid ICI or RCI account is needed to download the software). Once the client has been properly configured and launched, a tunnel is created between the PC and the VPN concentrator. Once completed, the workstation will be “virtually” on the Rutgers network (RUNet).

VPN Server Notes

- The Microsoft VPN bundled client uses the PPTP tunneling protocol to set up a connection to the VPN server, due to current technological limitations at this time an encrypted connection using PPTP is not supported on the VPN. Please turn off all encryption before attempting to connect to the VPN. If encryption is desired, please see the above instructions on how to download and install the Cisco VPN software.
- Only one ‘simultaneous logon’ is permitted. Therefore, only one connection per user is permitted.
- There is a 10-hour absolute limit and a 4-hour idle timeout on all VPN connections.
- When a connection is established with the Rutgers VPN a new IP address in the Rutgers private address space will be assigned to your PC. All data communications will go through the Rutgers tunnel connection. Therefore, please disconnect when Rutgers specific work is complete.

Implementation

The VPN Server is a Cisco 3030 VPN concentrator. The tunnels created by the following protocols make it possible to use Public Networks to view / change private information over secure connections made between the VPN client loaded on the users workstation and the VPN Server.

The supported tunneling protocols are:

IPSEC

The Internet Protocol Security Protocol (IPSec) is available with the Cisco VPN clients, and it support secure connections.

The secure tunnels provide the following features:

- Negotiate tunnel parameters between the VPN client and the concentrator.
- Establish tunnels
- Authenticate users and data
- Manage security keys
- Encrypt data

PPTP

Point-to-Point Tunneling Protocol (without encryption)

The PPTP protocol is the tunneling protocol used by the Microsoft Windows platforms. At this time encryption is not supported. All security has to be turned off before connecting to the VPN.

*****Use of this client is discouraged because the connection created with the VPN is not secure**

Getting Help

Please refer to the troubleshooting guide prior to reporting problems.

Reporting Problems

When reporting problems with the University's remote access systems, it is best to include as much information about the problem as possible to assist the maintenance staff in timely and accurate diagnosis and resolution of the problem. Please be sure to include the following in all problem reports. **At no time should you volunteer your password to anyone.**

1. Your name, daytime and evening phone numbers and email address.
2. Type of machine (PC, Macintosh, etc.)
3. Whether you are using PPTP or the Cisco IPSEC client
4. A brief, specific description of the nature of the problem, include all error messages
5. Some indication as to when problems first began. Indicate if you have successfully connected in the past, did anything change?

The table below lists the organizational contact information for the access numbers listed above.

OIT Information Centers		
OIT Camden	856/225-6274	All Camden users: help@camden.rutgers.edu
OIT Newark	973/353-5083	Students: help@pegasus.rutgers.edu Fac / Staff: help@andromeda.rutgers.edu
OIT New Brunswick	732/445-HELP	Students: help@eden.rutgers.edu Fac / Staff: help@rci.rutgers.edu

Caveats

1. Many VPN clients are available to establish a connection with the VPN server, however we only support those listed in this document.
2. When using the PPTP client, all encryption must be turned off.
3. When using the IPSEC client, if your local Internet Service Provider assigned you a "private" IP address that is conflict with our IP address range which is 172.16.8.x, you will have problems using the VPN after a connection has been made. All your network traffic may prefer to go out the ISP connection.
4. When using WebVPN, only the web browser instance used to connect to the Rutgers VPN will be configured to be part of Rutgers. All other browser instances will not be able to connect to the same Rutgers private documents.
5. SSL VPN Client requires Administrative privileges the first use.
6. WebVPN and SSL VPN Client require a SSL capable web browser.
7. SSL VPN requires Active X.
8. SSL VPN Client works only with Windows 2000 and Windows XP.

VPN Configuration and Setup Guides in PDF format

- [VPN Troubleshooting Guide](#)
- [SSL VPN Guide](#)
- [Web VPN Guide](#)
- [Cisco VPN Client Setup Guide](#)
- [Windows 98 VPN Setup guide](#)
- [Windows 2000 VPN Setup Guide](#)

VPN Client Download References

- [All VPN Clients](#)
- [Microsoft Windows 9x-XP](#)
- [Linux](#)
- [Macintosh](#)