VPN Overview

The path for wireless VPN users

First, the user's computer (the blue computer) connects to an access point in the uiuc-wireless-net network and is assigned an IP address in that range (172.21.0.0 /20). Machines on this subnet are not allowed to access anything outside that network without authenticating through the VPN server.

Next, when the user runs the VPN client, the computer makes a VPN connection request which is routed to the VPN server (the blue path in the diagram). The router sends VPN connection requests from the uiuc-wireless-net to the VPN server, but drops any requests for other campus locations or the Internet from uiuc-wireless-net.

The VPN server takes the user's authentication request and communicates with the Radius server and the Kerberos server to determine whether the user is authenticating correctly. If so, the VPN server establishes an encrypted tunnel with the wireless computer over the blue path (using the computer's real ID). The VPN server takes the encrypted communications the client computer sends to it, unencrypts the information, and forwards the information along to its destination with its identity represented as a part of the VPN-assigned network address range (shown as the orange block above).

Requests from computers in the uiuc-vpn-net address range (orange) are allowed access to both campus resources and the Internet. Requests that would not be permitted if the router received them unencrypted from uiuc-wireless-net (blue) are permitted after the VPN server has begun representing the computer's identity as part of the uiuc-vpn-net address range (orange). The VPN server is the only machine which knows the blue computer's true identity and location; it exchanges information over the encrypted tunnel it established with that machine, and redirects the data as though it originated in an unencrypted form from a machine with a uiuc-vpn-net (orange) IP address.
The path for remote wired VPN users

The path for remote wired users is the same as that described above for wireless users, with one exception. Rather than coming from an access point and using an original IP in the wireless network range, the machine is coming from a third-party ISP before making its VPN connection request and being routed to the VPN server. For the diagram above to represent the remote wired users' path, all that changes is the network name and IP range assigned to the cloud around the blue computer.

Security basics

Note that from the blue computer to the VPN server and back, all transmissions are encrypted. From the VPN server out to the rest of the world, communications are NOT encrypted. The goal of the VPN server is not to make wireless transmissions end-to-end secure; the goal is to permit wireless users to access resources on the UIUC network without revealing sensitive data such as login names and passwords to anyone close enough to "overhear" it.

Without the VPN server, a hacker could overhear and interpret a wireless computer's transmissions by standing close enough to connect to the same access point. (Wired systems start off a little more secure. It's more difficult for a hacker to intercept communication traveling across a series of wires than to intercept everything passing through the air around an access point.)

In banking terms, wireless "security" without a VPN server would be roughly equivalent to storing money on a table in the middle of a room and expecting passers-by not to walk off with it. The VPN server effectively puts your valuables (password and data) in a safety deposit box (encryption), and each person communicating with the VPN server is given a key which accesses only one safety deposit box (the data sent to and from their own machine).

The VPN server carries the transmissions securely into the wired part of the UIUC network. From that point on, however, the wireless users' communications are subject to the same protections and vulnerabilities as any wired computer on the UIUC network.

VPN Installation

Installation and configuration for Windows

Before beginning this process, make sure you have downloaded and saved the identification certificate on your hard drive in a location you can find (http://www-commeng.cso.uiuc.edu/software/vpnclient.html). Store the certificate in a place where you can keep it permanently on your hard drive.

1. Double-click on the downloaded .exe file (http://www-commeng.cso.uiuc.edu/software/vpnclient.html) to start the installation process, and follow the prompts as given.

   (In most cases, the installation utility will automatically locate and install the correct networking drivers. If it cannot do so automatically, see the "Manually Installing the Network Driver" section on http://www.cisco.com/univercd/cc/td/doc/product/aggr/vpn5000/client/index.htm for your platform.)

2. Restart your machine when prompted.
3. After the restart, run the VPN client. A window like the following will appear:

![VPN Client Window]

4. In the Configuration tab (shown above), click the "Add..." button.

5. In the Login Properties box which appears, select the Certificate radio button, and select "Manual" from the drop box (as shown). Your login name will be your Network ID (in lower case) followed by @UIUC.EDU (in upper case), like the example shown. The Primary VPN Server's IP address is 128.174.1.98; there is no Secondary VPN Server. When you have entered this information, click OK.

![Login Properties Window]

6. Next, you will be prompted for a root certificate. Click the Browse button and navigate to where you saved the certificate. It will appear in the Root Certificates list (as shown). (Note: Do not move or delete the certificate after directing the VPN client to use this location, unless you also change the
configuration to recognize a new location or new certificate.)

You're now finished with initial configuration. You can exit the VPN client now.

**Starting a new VPN session**

1. When you want to make a VPN connection, you'll need to have *established your regular network connection first*. If your network connection is not established first, the VPN system will not know what IP address to communicate with.
   
   o For cable modem, DSL, and Ethernet users, you'll already be connected.
   
   o For dialup users, you'll need to follow your usual dialup procedure and log in to your ISP.

2. *After this connection has been established*, double-click the VPN client icon to start it again.

3. Return to the Configuration tab, select the login configuration you want to use from the list of configurations available, and click the Connect button to establish a connection. The system will prompt you with a "RADIUS login" screen (as shown). Enter your Network ID (NetID/Kerberos) password in the Password box. Then click OK.

4. You should receive a message at the bottom of the main window indicating that you have successfully connected to the VPN server. Clicking the General tab will give you connection information.

5. When you are finished working through the VPN connection:
1. Click the Configuration tab
2. Then click the Disconnect button
3. Then click the Exit button.

(If you're using a dialup connection, you'll need to disconnect it separately using your normal disconnect procedure.)

**UIUCLIBRARY Specific Settings**

*Note: Access to the Library’s network shares (G:\ or H:\ drives, etc.) is limited to machines running Windows 2000, Windows NT, and Windows XP. Operating systems such as Windows 95, 98, and ME, will not be able to connect to network shares.*

**Settings to change**

Under your TCP/IP properties, there will be an option such as below to enable NetBIOS over TCP/IP. Depending on the OS version, the setting may be in several places. Typically you will need to right click on your Network Neighborhood (My Network Places) icon and choose the properties option.

![Advanced TCP/IP Settings](image)

---

Set NetBIOS over TCP/IP to Enable

The Client for Microsoft Networks also must be installed under your network connection properties.
Connecting to network shares

Note: Access to the Library’s network shares is limited to machines running Windows 2000, Windows NT, and Windows XP. Operating systems such as Windows 95, 98, and ME, will not be able to connect to network shares.

The network shares you most commonly have available to you are as follows:
- Groupfiles, also the G drive \libsys5.library.uiuc.edu\groupfiles
- Home directory, also the H drive \libsys5.library.uiuc.edu\username$
- Web pages, also the W drive on libgrenlil \www.library.uiuc.edu\deptwebshare

To connect to a network drive, click on the start menu and choose run. Type in the above bold line depending on the share you wish to connect to. You should get a prompt for your username and password. For your username, type in your NT domain account as follows: UIUC\username your password is your NT domain password.

*note* the italicized items need to be replaced with your pertinent information

Further security issues

Since Enable NetBIOS over TCP/IP is needed to connect to network shares on the library servers, any drives you have shared on your computer can also be accessed over a TCP/IP connection. This poses a problem if you have File and Printer Sharing enabled on your computer. If you do not need to share a file or printer from your computer, uninstall or disable this service.