



Installing the VPN Client

This chapter describes how to install the VPN client software on your workstation. You should be familiar with software installation on UNIX or Macintosh computers before you perform this procedure.

The VPN client consists of:

- A driver, which is a loadable module.
- A set of commands accessible through your shell, which is used to access the applications.

The commands and some parts of the driver are distributed in binary form only.

Contents

This chapter contains the following sections:

- [Uninstalling an Old Client, page 2-2](#)
- [System Requirements, page 2-3](#)
- [Unpacking the VPN Client Files, page 2-5](#)
- [Installing the Software, page 2-6](#)

Uninstalling an Old Client

This section describes how to uninstall the VPN client.

- You *must* uninstall an old VPN client for Solaris before you install a new VPN client.
- You are *not required* to uninstall an old VPN client for Linux or for Mac OS X before you install a new VPN client.

Uninstalling a VPN Client for Solaris

If a VPN client for Solaris was previously installed, you must remove the old VPN client before you install a new one.

To uninstall a package, use the **pkgrm** command. For example:

```
pkgrm vpnclient
```

Uninstalling a VPN Client for Linux or Mac OS X

To uninstall the VPN client for Linux or Mac OS X:

- a. Locate the script `vpn_uninstall`.
This file must be run as root.
- b. You are prompted to remove all profiles and certificates.
 - If you answer yes, all binaries, startup scripts, certificates, profiles, and any directories that were created during the installation process are removed.
 - If you answer no, all binaries and startup scripts are removed, but certificates, profiles, and the `vpnclient.ini` file remain.

System Requirements

This section describes system requirements for the VPN client for each operating system.

Linux System Requirements

The VPN client for Linux supports Red Hat Version 6.2 Linux (Intel), or compatible libraries with glibc Version 2.1.1-6 or later, using kernel Versions 2.2.12 or later.



Note

The VPN client for Linux does not support kernel Version 2.5.

Firewall Issues

If you are running a Linux firewall (for example, ipchains or iptables), be sure that the following types of traffic are allowed to pass through:

- UDP port 500
- UDP port 10000 (or any other port number being used for IPSec/UDP)
- IP protocol 50 (ESP)
- TCP port configured for IPSec/TCP

Troubleshooting Tip

The following two lines might be added by default with your Linux installation in the `/etc/sysconfig/ipchains` directory. For Redhat, this might be written to the `/etc/sysconfig/ipchains` directory. These two commands might prevent UDP traffic from passing through.

```
-A input -p udp -s 0/0 -d 0/0 0:1023 -j REJECT  
-A input -p udp -s 0/0 -d 0/0 2049 -j REJECT
```

If you have problems with UDP traffic, first delete the above two lines, then enter the following two commands:

```
/etc/init.d/ipchains stop
/etc/init.d/ipchains start
```



Note Ipchains might be replaced by iptables or it might be located in a different directory on your Linux distribution.

Solaris System Requirements

The VPN client for Solaris runs on any ultraSPARC computer running a 32-bit Solaris kernel OS Version 2.6 or later.

Using the 32-Bit Kernel

Some Solaris machines run a 64-bit kernel by default. To use the VPN client, run the 32-bit version of the kernel.

There are several ways to run in 32-bit mode.

- Specify the kernel/unix as the boot file. Enter the following command:

```
ok boot kernel/unix
```

This command immediately reboots the system in 32-bit mode. 32-bit mode is only valid for this boot. When you reboot again, the system switches back to its default mode.

- Switch to 32-bit mode permanently. Enter the following command:

```
eeeprom boot-file=/platform/sun4u/kernel/unix
```

You must reboot after you issue this command.

- Switch back to 32-bit mode permanently. Enter the following command:

```
eeeprom boot-file=/platform/sun4u/kernel/sparcv9/unix
```

You must reboot after you issue this command.

To confirm that your system is running in 32-bit mode:

- a. Issue the following command:

```
isainfo -kv
```

- b. When the Solaris system boots up, a message in the **dmesg** event log similar to the following appears:

```
Oct 29 11:09:54 sol-2062 cipsec: [ID 952494 kern.notice] Cisco  
Unity IPsec Module Load OK
```

If you do not receive this message, the IPsec module did not load properly and you need to switch to the 32-bit kernel.

Mac OS X System Requirements

The VPN client for Mac OS X runs on any Macintosh computer running OS X Version 10.1.0 or later.



Note

Classic Mac applications do not make use of the VPN tunnel.

Unpacking the VPN Client Files

The VPN client is shipped as a compressed tar file.

For Solaris, there are two available VPN client files. Make sure that you have the correct installation file for your operating system.

- The installation file for Solaris 5.6 and Solaris 7 is named:

```
vpnclient-solaris5.6-3.5.xxx-K9.tar.Z
```

- The installation file for Solaris 8 is named:

```
vpnclient-solaris5.8-3.5.xxx-K9.tar.Z
```

To unpack the files

-
- Step 1** Download the packed files, either from your internal network or the Cisco website, to a directory of your choice.
 - Step 2** Copy the VPN client file to a selected directory.
 - Step 3** Unpack the file using the **zcat** and **tar** commands.

For example, the command for Linux is:

```
zcat vpnclient-linux-3.5.xxx-k9.tar.gz | tar xvf -
```

The command for SPARC Solaris is:

```
zcat vpnclient-solaris5.8-3.5.xxx-k9.tar.Z | tar xvf -
```

The command for Mac OS X is:

```
zcat vpnclient-macosx-3.5.xxx-k9.tar.gz | tar xvf -
```

This command creates the vpnclient directory in the current directory.

Installing the Software

The following sections describe the installation procedure for the VPN client for each operating system.



Note

You cannot have both a VPN 5000 client and a Unified VPN client installed on your workstation. You must uninstall one before you use the other. Refer to the [“Uninstalling an Old Client”](#) section on page 2-2 for more information.

Installing the VPN Client for Linux

Before you install a new version of the VPN client, or before you re-install your current version, you must use the **stop** command to disable VPN service.

If you are upgrading from the VPN 5000 client to the VPN client, use the following **stop** command:

```
/etc/rc.d/init.d/vpn stop
```

If you are upgrading from the VPN 3000 client to the VPN client, use the following **stop** command:

```
/etc/rc.d/init.d/vpnclient_init stop
```

To install the VPN client for Linux

Step 1 Obtain superuser privileges to run the install script.

Step 2 Enter the following commands:

```
cd vpnclient
./vpn_install
```

Step 3 At the prompt, choose a directory in which to install the VPN client.

Use the default directory (by pressing **Enter**), or choose a directory in your user's path.

Step 4 Enable the VPN service by using one of the following methods:

- Reboot your computer.
- Enable the service without rebooting. Enter the following command:

```
/etc/rc.d/init.d/vpnclient_init start
```

VPN Client for Linux Install Script Notes

During the installation process:

1. The module is compiled, linked, and copied to either the directory `/lib/modules/preferred/CiscoVPN`, if it exists, or to `/lib/modules/system/CiscoVPN`, where *system* is the kernel version.
2. The application binaries are copied to the specified destination directory.
3. The startup file `/etc/rc.d/init.d/vpnclient_init` is created to enable and disable the VPN service.

- The links `/etc/rc3.d/s85vpnclient` and `/etc/rc5.d/s85vpnclient` are added to run level 3 and level 5 if startup at boot time is requested.

These links allow the tunnel server to start at boot time and run in levels 3 and 5.

Installing the VPN Client for Solaris

Before you install a new version of the VPN client, or before you re-install your current version, you must uninstall the old VPN client. See the [“Uninstalling an Old Client” section on page 2-2](#) for more information.

To install the VPN client for Solaris

-
- Step 1** Obtain superuser privileges to run the install script.
 - Step 2** Enter the following command:

```
pkgadd -d . vpnclient
```
 - Step 3** At the prompt, choose a directory in which to install the VPN client applications. Use the default directory (by pressing **Enter**), or choose a directory in your user’s path.
 - Step 4** Respond **Yes** to any other prompts to complete the installation.
 - Step 5** Reboot your computer.
-

VPN Client for Solaris Install Script Notes

During the installation process:

- The following line is added to the `/etc/uu.ap` file to enable the autopush facility at startup:

```
hme -1 0 cipsec
```
- The VPN module is copied to the `/kernel/strmod` directory, which is in the system’s module search path.

The **pkginfo** command provides information about the installed packages. For more information on other package-related commands, enter:

```
man pkgadd
```

Installing the VPN Client for Mac OS X



Note

You must have root privileges to install the VPN client for Mac OS X.

To install the VPN client for Mac OS X

Step 1 Activate the root account.

The root account is disabled by default. Open the application NetInfo Manager in the Utilities folder, which is in the Applications folder. Click the button with the lock and enter your password. In the menu choose **Domain > Security > Authenticate** and then **Domain > Security > Enable Root User**. You are prompted for a password.

Step 2 Obtain superuser privileges to run the install script.

Step 3 Enter the following commands:

```
cd vpnclient
./vpn_install
```

Step 4 At the prompt, choose a directory in which to install the VPN client.

Use the default directory (by pressing Enter), or choose a directory in your user's path.

Step 5 Respond to the question about automatically loading the VPN NKE at boot time.

- If you answer **Yes**, use the following commands to control the NKE:

```
/System/Library/StartupItems/CiscoVPN/CiscoVPN start
/System/Library/StartupItems/CiscoVPN/CiscoVPN stop
/System/Library/StartupItems/CiscoVPN/CiscoVPN restart
```

- If you answer **No**, use the following commands to control the NKE:

```
kmodload  
/System/Library/Extensions/CiscoVPN.kext/Contents/MacOS/CiscoVPN  
  
kmodunload com.cisco.nke.ipsec
```

VPN Client for Mac OS X Install Script Notes

During the installation process:

1. The application binaries are copied to the specified destination directory.
2. Use the following commands to start, stop, and restart VPN service:
 - `/System/Library/StartupItems/CiscoVPN/CiscoVPN start`
 - `/System/Library/StartupItems/CiscoVPN/CiscoVPN stop`
 - `/System/Library/StartupItems/CiscoVPN/CiscoVPN restart`