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 computers to 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.

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 before you install a new VPN Client.
- You must uninstall any VPN 5000 Client before you install a VPN Client. Refer to the Cisco VPN 5000 Client documentation for more information.

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

To uninstall the VPN Client for Linux:

Step 1 Run the following command:

```
sudo /usr/local/bin/vpn_uninstall
```

Step 2 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.

Gathering Information You Need

To configure and use the VPN Client, you might be required to have the following information.

This information is normally obtained from the system administrator of the private network you want to access. The system administrator might preconfigure much of this data.

- Hostname or IP address of the secure gateway you are connecting to
- Your IPSec Group Name (for preshared keys)
- Your IPSec Group Password (for preshared keys)
- The name of the certificate, if authenticating with a digital certificate
- Your username and password, if authenticating through:
  - The secure gateway's internal server
  - A RADIUS server
  - An NT Domain server
- Your username and PIN, if authenticating through a token vendor
- The hostnames or IP addresses of the backup servers, if you should configure backup server connections

Verifying 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 prior to VPN Client Release 4.0.1.A and does not support SMP (multiprocessor) kernels in any release of the VPN Client.

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
- NAT-T (Standards-Based NAT Transparency) port 4500

Troubleshooting Tip

The following two lines might be added by default with your Linux installation in the /etc/sysconfig/ipchains directory. For Red Hat, 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, try one of the following solutions:

- First delete the above two reject lines, then enter the following two commands:

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

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

- Add the following rule to the default ipchains firewall configuration, or add it above any UDP reject line.

  ```
  -A input -p udp -s 0/0 -d 0/0 500 -j ACCEPT
  ```

  This rule allows UDP port 500, which is required for the VPN Client connection.

Bundling a Root Certificate with the Installation Package—Linux

To use mutual authentication, the VPN Client system must have a root certificate installed. You can bundle a root certificate with the installation package so that the root certificate is installed automatically during installation. The following commands place a root certificate with the installation package. The root certificate is contained in a file. The name of the file must be rootcert with no extension.

```
zcat vpnclient-linux-<version>-K9.tar.gz | tar xf -
rm -f vpnclient-linux-<version>-K9.tar.gz
cp -f <path_to_root_cert>/<root_cert_filename> vpnclient/rootcert
tar czf vpnclient-linux-<version>-K9.tar.gz vpnclient
```

Bundling a Root Certificate with the Installation Package—Solaris

To use mutual authentication, the VPN Client computer must have a root certificate installed. You can bundle a root certificate with the installation package so that the root certificate is installed automatically. The following commands place a root certificate with the installation package. The root certificate is contained in a file. The name of the file must be rootcert with no extension.

```
zcat vpnclient-solaris-<version>-K9.tar.Z | tar xf -
rm -f vpnclient-solaris-<version>-K9.tar.Z
cp -f <path_to_root_cert>/<root_cert_filename> vpnclient/rootcert
tar cf - vpnclient | compress -c > vpnclient-solaris-<version>-K9.tar.Z
```

Solaris System Requirements

The VPN Client for Solaris runs on any UltraSPARC computer running a 32-bit or 64-bit Solaris kernel OS Version 2.6 or later.

Changing a Kernel Version

You can install the VPN Client running the 32-bit or 64-bit version of the kernel (referred to as 32-bit mode and 64-bit mode). If you experience problems installing or running the VPN Client in one mode, try the other one.

To see which mode the system is running in, enter this command:

```
isainfo -kv
```

If the cipsec module is loaded correctly, the dmesg log displays a message similar to the following:

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

Note If the dmesg log does not show the cipsec log message, you should switch to the other mode.

To switch to 32-bit mode:

- Temporarily—Enter the following command (ok is the system prompt):

  ```
  ok boot kernel/unix
  ```

- Permanently—Enter the following command as root, then restart your computer:

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

To switch to 64-bit mode:

- Temporarily—Enter the following command (ok is the system prompt):

  ```
  ok boot kernel/sparcv9/unix
  ```

- Permanently—Enter the following command as root, then restart your computer:

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

Unpacking the VPN Client Files

The VPN Client is shipped as a compressed tar file.

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-3.7.xxx-K9.tar.gz | tar xvf -
```

The command for Solaris is:

```
zcat vpnclient-solaris-3.7.xxx-K9.tar.Z | 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.

Installing the VPN Client for Linux

Before you install a new version of the VPN Client, or before you reinstall 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
```

The default directories for the binaries, kernel, VPN modules, and profiles are listed during the installation process.

You receive the following prompts during the installation:

- Directory where binaries will be installed [/lib/modules/<kernel version>/build/]
- Automatically start the VPN service at boot time [yes]
- Directory containing linux kernel source code [/usr/src/linux]
- Is the above correct [y]

Step 3 Press **Enter** to choose the default response. At the directory prompts, if you do not choose the default, you must enter another directory in your user's path.

Step 4 If the installer cannot auto detect these settings, you might receive the following prompts:

- Directory containing init scripts:
  - The directory where scripts that are run at boot time are kept. Typically this is /etc/init.d or /etc/rc.d/init.d

- Directory containing run level directories (rcX.d):
  - The directory that contains init's run level directories. Typically this is /etc or /etc/rc.d

Step 5 Enable the VPN service by using one of the following methods:

- Restart your computer.
- Enable the service without restarting. Enter the following command:

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

Kernel Source Requirements

To install the VPN Client, you must have the kernel source that was used to build the kernel that is running on the system. If the system is using a kernel that came as part of the Linux distribution, or a custom built kernel, the kernel code can be obtained in different ways:

- For users running kernels that came with their distribution—You must install the corresponding kernel-source rpm. The vpn_install script should be able to automatically find the kernel source.
- For users running a custom-built kernel—You must use the same copy of the kernel source that was used to build the kernel you are running. Unpacking the source code for the version of the kernel you are using is insufficient. There are several files generated when the kernel is compiled that the VPN Client uses. These files must exactly match with the kernel you are running. Otherwise, the VPN Client installation might fail.

Note If you install a patch on the workstation kernel, you must reinstall the VPN Client using these guidelines.

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.
4. 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 reinstall your current version, you must uninstall the old VPN Client. See the "Uninstalling an Old Client" section on page 2-1 for more information.

Note If you are installing the VPN Client for Solaris, Release 3.7 or later on a Version 2.6 Solaris platform, you receive the following message during the VPN Client installation: "Patch 105181 version 29 (or higher) to Solaris 2.6 is required for the client to function properly. Installing without this patch will cause the kernel to crash as soon as the client kernel module is loaded. This patch is available from Sun as part of the "Recommended Solaris Patch Cluster". If you proceed with installation, the kernel module will not be enabled. After you have installed the patch, you may enable the kernel module by uncommenting all lines in /etc/iu.ap that contain 'cipsec'."

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
```

The default directories for the binaries, kernel, VPN modules, and profiles are listed during the installation process.

You receive the following prompts during the installation:

- Directory where binaries will be installed [/usr/local/bin]
- Is the above correct [y]
- If the installer finds a conflict with the VPN Client files and another application, you receive this message:

  The following files are already installed on the system and are being used by another package:<installer lists files> Do you want to install these conflicting files [y,n,?,q]
- The following files are being installed with setuid and/or setgid permissions:<installer lists files>Do you want to install these as setuid/setgid files [y,n,?,q]
- This package contains scripts which will be executed with super-user permission during the process of installing this package. Do you want to continue with the installation of <vpnclient> [y,n,?]

Step 3 Press **Enter** to choose the default response. At the directory prompts, if you do not choose the default, you must enter another directory in your user's path.

Step 4 Restart your computer.

VPN Client for Solaris Install Script Notes

During the installation process:

1. The following line is added to the /etc/iu.ap file to enable the autopush facility at startup:

   ```
   <dev_name> -1 0 cipsec
   ```

   where dev_name is the name of the interface without the trailing numbers (for example ipdtp, le, or hme). A line is added for every supported network device detected.

2. 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
```