In This Chapter

The Need for SecureClient  page 1
The Check Point Solution  page 1

The Need for SecureClient

Anyone who wishes to send or receive e-mail while at home, or while over the weekend, needs to do so securely. When on the road, several challenges are presented by different network environments, such as a hotel internet connection or the connection from a business partner’s network.

The Check Point Solution

VPN-1 SecuRemote/SecureClient allows you to connect to your organization in a secure manner, while at the same time protecting your machine from attacks that originate on the Internet. You can access private files over the Internet knowing that unauthorized persons cannot view the same file or alter it. With VPN-1 SecuRemote/SecureClient, remote users connect to the organization using any network adapter (including wireless adapters) or modem dialup. Once both sides are sure they are communicating with the intended party, all subsequent communication is private (encrypted) and secure. This is illustrated in FIGURE 1:

How it works

SecuRemote/SecureClient provides secure connectivity by authenticating the parties and encrypting the data that passes between them. To do this, VPN-1 SecuRemote/SecureClient takes advantage of standard Internet protocols for strong encryption and authentication. Authentication means that both parties identify themselves correctly. Encryption ensures that only the authenticated parties can read the data passed between them. In addition, the integrity of the data is maintained, which means the data cannot be altered during transit.

For more information regarding the building of Remote Access environments, see the VPN-1 book.
Configuring SecureClient

In This Chapter

Client Side Configuration  page 3
Obtaining Authentication Credentials  page 4
Connecting for the First Time Using the Connection Wizard  page 4
Creating a New Check Point Certificate  page 11
Creating an Entrust Certificate  page 18
Connecting and Authenticating  page 19
Updating a Site  page 20
Creating a New Site  page 21
Enabling Logging  page 22
Switching Between Product Views  page 23
Stopping and Starting SecureClient  page 23
Enabling and Disabling a Policy  page 24
Selecting a Different Certificate  page 25
Renewing a Certificate  page 26
Working with Profiles  page 27
Enabling Office Mode  page 30
Enabling Hub Mode  page 31
Connection Modes  page 32
Suspending Popup Messages  page 34
Secure Domain Logon (SDL)  page 35
Retrieving Status information  page 35
Understanding the Diagnostics Tool  page 38
Client Side Configuration

Once installed, SecureClient places an icon in the system tray:

The red x above the gold key means SecureClient is not currently connected to a site.
- When the mouse is placed over the icon, a balloon appears displaying SecureClient's current status, for example:

- Right-clicking the icon produces a pop-up menu:

- If a site is already defined, double-clicking the system tray icon opens the SecureClient connection screen:

Or the SecureClient connection wizard if no site is defined:
Obtaining Authentication Credentials

When you connect to a site, and supply identification details, you are supplying authentication credentials. There are many authentication methods available for SecureClient. The recommended way to authenticate is through the use of certificates. A certificate and your password (to open the certificate) are your authentication credentials.

Contact your system administrator regarding your credentials. Your system administrator will either supply you with:

- A registered certificate (on diskette, or a hardware token) and password (for opening the certificate)
- A registration code that allows you to complete the certificate creation process online.
- Alternative methods, such as a username and password, or SecurID card.

Connecting for the First Time Using the Connection Wizard

Before SecureClient connects to a site it needs to obtain information regarding the site’s structure, such as the computers and servers available within the organization. The connection wizard gathers this site information. The initial connection, which is different from all subsequent connections, obtains the site’s structure (or topology). During this process you are requested to prove who you are, either by supplying a certificate, or through some other means. If you are using certificates to authenticate yourself but have not received one from your system administrator, you will be asked to register. Registering a certificate means that you will complete a certificate creation process which was initiated by your system administrator. Once this process of defining a site is complete, regular connections can take place.

Defining a Site with the Site Creation Wizard

SecureClient needs to identify the remote party with which it is communicating. The other party is known as the Site. A new site is defined by following the site creation wizard. If no sites have been previously defined, simply double-clicking the SecureClient icon in the system tray opens the site creation wizard. If a single site or number of sites are already defined, and you wish to create another, then:

1. Double-click the SecureClient icon in the system tray:

   ![System tray](image)

   A message box appears:
2 Click Yes.

The site creation wizard opens:

Enter the name or IP address of the site.

The authentication window opens:
Select an authentication method (as specified by your system administrator), and click **Next >**

If you authenticate through the use of certificates, the certificate authentication window opens:

If your system administrator instructs you to obtain a certificate from the Gateway, select **I would like to obtain a certificate from the Gateway**, and follow the instructions in: “Registering a Certificate” on page 10”.

![Certificate Authentication Window Image]
Otherwise, click **Next >** and browse to the certificate provided by your system administrator on diskette.

Select the certificate, and click **Open**: 

Enter the password for the certificate and click **Next >**

The **Select Connectivity Settings** window opens:

Select **Standard** or **Advanced** for the connectivity settings. Try **Standard**. If experience difficulties connecting to the site, run the site creation wizard again and select **Advanced**. Click **Next >**

The connection progress window is displayed:
6 Once a connection is established successfully, the site validation window opens:

If your system administrator supplied you with the Certificate Authority’s fingerprint, compare it with the one displayed here. If they are not the same, click Cancel and contact your system administrator.

7 If the fingerprints match, Click Next >

The confirmation window opens:
8 Click Finish

The **VPN-1 SecureClient Connection** window opens:

If you authenticate using certificates, then in the certificate field the path to the certificate is displayed.

9 Enter the password for opening the certificate and click **Connect**.

The progress window is displayed:

Logging onto Policy server and updating Policy:

Followed by the connection succeeded window:
Connecting to Hot Spots

If you need to register to a hot spot, on the connection window’s Options buttons, select Register to Hot Spot/hotel.

This suspends SecureClient’s settings for several minutes. During this time, SecureClient will not attempt to connect to the site, giving you enough time to register.

Registering a Certificate

Before you can register a certificate, you first need to define a site. See: “Defining a Site with the Site Creation Wizard” on page 4.

1 After selecting I would like to obtain a certificate from the gateway, Click Next>

The Check Point Certificate window opens:

2 Enter the IP Address (or name) of the Site and registration key, as supplied by your system administrator.

The Save Certificate window opens:
Specify a name and location for the certificate file and enter a password. Later, when authenticating with this certificate, you will need to enter this password. Click **Next**

The connection progress window is displayed.

Return now to step six of: “Defining a Site with the Site Creation Wizard” on page 4”, and continue with the procedure.

### Creating a New Check Point Certificate

Your system administrator might request you to create a new Check Point certificate. Check Point certificates can be stored as either a **PKCS#12** file or as a hardware or software token (**CAPI**). Confirm with your system administrator the type of file storage you will be using.

### Creating and Storing a Check Point Certificate as a PKCS#12 File

1. In the system tray, right-click the SecureClient icon:

2. From the pop-up menu select **Settings**...

   The **VPN-1 SecureClient Settings** window opens.
3  On the **Certificates** tab click > **Create Certificate**...

The Check Point Certificate window opens:

4  Select **Store as a file (PKCS #12)** and click **Next**
5 Click Next>

The Check Point Certificate window opens:

Enter the IP Address (or name) of the Site, and registration key, as supplied by your system administrator.

The Save Certificate window opens:

6 Enter the IP Address (or name) of the Site, and registration key, as supplied by your system administrator.

The Save Certificate window opens:
Specify a name and location for the certificate file and enter a password. Later, when authenticating with this certificate, you will need to enter this password. Click **Next>**

A message window opens confirming that the certificate has been saved successfully:

Click **Finish**.

**Creating and Storing a Check Point Certificate as a Hardware or Software (CAPI) Token.**

If your system administrator has specified that the certificate should be saved as a hardware or software token:

1. Right-click the SecureClient icon in the system tray.
2. From the pop-up menu, select **Settings...** The VPN-1 SecureClient Settings window opens.
3. On the **File menu, Certificates > Check Point Certificates > Create...**

The Check Point Certificate window opens:

4. Select **Store on a hardware or software token (CAPI)**
5 Click **Next>**

The **Check Point Certificate** window opens:

Select the **Cryptographic Service Provider (CSP)** for your certificate storage. If you are not sure which to select, contact your system administrator. CAPI works with a number of Cryptographic Service Providers. Some CSPs need special hardware: a token reader/writer, others do not. SecureClient works with the CSPs supported by the Windows operating system. Each CSP produces its own unique windows. Any differences noticed from this point onwards (in terms of window design, pop up messages, authentication requirements, etc.) from that described below, are due to differences in the CSP implementation.

6 Click **Next>**

The **Create Check Point Certificate** window opens:

7 Enter the IP of the site and registration key as supplied to you by your system administrator.
8 Click **Next >**

The **Creating a new RSA signature** key window opens:

![Creating a new RSA signature window]

9 Click **Set Security Level**

![Set Security Level window]

Select the security level as specified by your system administrator.

10 Click **Next >**

A confirmation window appears:

![Confirmation window]
11 Click Finish.

The **Root Certificate Store** window opens:

12 Click **Yes**.

A confirmation message appears:

13 Click **Finish**.
Creating an Entrust Certificate

To create an entrust certificate:

1. In the system tray, right-click the SecureClient icon:

2. From the pop-up menu select Settings...
The VPN-1 SecureClient Settings window opens.

3. On the Certificates tab > Entrust Options... > Create...

   ![SecureClient Settings Window]

   The Create User window opens:

   ![Create User Window]

4. Click Browse... to select a file for the saved file and supply a name for the saved file.

5. Supply a password for your profile.
The password must comply with the following Entrust specifications:
   - At least 8 characters long
   - At least one uppercase or digit character
   - At least one lowercase
• You cannot use a long string of repeating characters.
• You cannot use a long substring of the User Name.

6 Specify your profile parameters by entering the Reference Number and Authorization code supplied by your system administrator.

7 Click OK
   A confirmation message appears:

   !Profile created successfully!

   OK

**Connecting and Authenticating**

To connect to an existing site:

1 Right-click the SecureClient icon in the system tray:

2 From the popup menu, select Connect.
   The SecureClient connection window opens:

   ![SecureClient connection window]

   If you authenticate using certificates, then in the certificate field the path to the certificate is displayed.
Enter the password for opening the certificate and click **Connect.**

The progress window is displayed:

Followed by the connection succeeded window:

### Updating a Site

SecureClient can update its site information only when disconnected from the site.

1. In the system tray right-click the SecureClient icon:

2. From the pop-up menu select **Disconnect:**

3. Again, right-click the SecureClient icon in the system tray:

4. From the pop-up menu select **Settings...**

   The SecureClient configuration window opens.

5. On the **Connections** tab, right-click the icon that represents your site:
6 Select **Update site...**

The update progress window displays:

![Update Progress Window](image)

Followed by an update successful notification:

![Update Successful Notification](image)

7 Click **OK**.

If you have not connected to the site for a certain amount of time, then the next time you connect the **SecureClient Connection** window contains an **Update** button instead of the **Connect** button:

![SecureClient Connection Window](image)

**Creating a New Site**

To create a new site:

1 In the system tray, right-click the SecureClient icon:

2 From the pop-up menu select **Settings...**

The SecureClient configuration window opens

3 On the **Connections** tab, click **New > Site**

The site creation wizard opens.
Follow the steps in “Connecting for the First Time Using the Connection Wizard”.

Enabling Logging

For trouble-shouting purposes, your system administrator may ask you to create a report log. The report log contains site-specific information and should be treated as strictly confidential. Send the report only to an authorized authority, such as your system administrator.

To enable logging:

1. In the system tray, right-click the SecureClient icon:

   From the pop-up menu, select Settings.

   The main settings window opens:

   ![SecureClient Settings Window]

2. On the advanced tab, select Enable Logging, and click Save Logs.

   Wait until the following message appears:

   ![Log Saved Successfully Message]

3. Save the logs to the default location:

   ![Log Files Table]

   NOTE: The default location is a hidden folder in windows. If you need to locate this folder, then in Control panel > Folder Options > View select Show hidden files and folders.

4. Close the location window. The file has been saved automatically.
Switching Between Product Views

SecureClient can be switched between product views. To switch between the Extended and Compact views:

1. In the system tray, right-click the SecureClient icon: From the pop-up menu, select Settings.
   The main settings window opens

2. In the Product View section of the Advanced tab, select Extended or Compact.
   Before switching from Extended to Compact View:
   • Delete all sites
   • Disable Auto Local Logon
   • Disable Secure Domain Logon

Stopping and Starting SecureClient

Stopping SecureClient

1. Right click the SecureClient icon in the system tray:
2. From the pop-up menu, select Stop VPN-1 SecureClient:

   SecureClient is now stopped, as indicated by the “x” over the SecureClient icon:
Starting SecureClient

From the Start > Programs > Check Point VPN-1 SecureClient > SecureClient:

SecureClient starts, as shown by the SecureClient icon in the system tray:

Enabling and Disabling a Policy

Desktop Security Policies can be enabled and disabled. Disabling the Desktop Security Policy leaves your machine unprotected, and is not recommended.

Disabling a Policy

A Desktop security Policy is configured by your system administrator and downloaded to your machine when you perform a site update, or when the current Policy expires. If you have a desktop security Policy, the SecureClient in the system tray consists of a yellow key with a blue padlock:

To disable the Policy:

1 Right-click the SecureClient icon in the system tray:
2 From the pop-up menu, select Tools > Disable Policy

The Desktop Security Policy is disabled.

Enabling a Policy

To enable a previously disabled desktop Security Policy:

1 Right-click the SecureClient icon in the system tray:
2 From the pop-up menu, select Tools > Disable Policy
3 Click **Disable**.

The check next to the word **Disable** is removed.

**Selecting a Different Certificate**

If your laptop acts as a terminal for other users, each user connecting to the site with their own unique certificates, then you will need to switch certificates as the need arises. To switch certificates:

1 Disconnect from the current site by right-clicking the SecureClient icon in the system tray and selecting **Disconnect** from the pop-up menu. (You cannot change certificates while connected.

2 Right click the SecureClient icon in the system tray:

3 Select **Settings...**

The VPN-1 SecureClient Settings window opens.

4 Select a site, and click **Properties**.

The Site Properties window opens:

![Site Properties Window](image)

5 Click **Browse** to select another certificate:

![Browse Certificate Window](image)

6 Click **Open**.

You return to the **Site Properties** window.

7 Click **Okay**.
Renewing a Certificate

A certificate is only valid for a certain period. From time to time you are prompted to renew the certificate. To renew a certificate:

1. Right-click the SecureClient icon in the system tray.
2. From the pop-up menu, select Settings...
   The VPN-1 Secure Client Settings window opens.
3. On the Certificates tab, click Renew Certificate...

The Renew Check Point Certificate window opens:
4 The current certificate is displayed. If you have moved the certificate to a different folder, browse to the new location. Enter the current password and click Next>

The Save Certificate window opens:

5 Enter the password and confirm the password and click Next>
   A confirmation window opens:

6 Click Finish

**Working with Profiles**

When you connect to a site, you do so with a specific connection profile. Typically, you do not need more than a single profile. However, when working in a shifting network environment (for example, from inside a partner company or from a hotel room) these sudden changes can present a number a connectivity issues. Your system administrator resolves these issues by defining a number of connection profiles. Each profile connects to the site in a slightly different way, for example using Office mode or Hub mode. Profiles are automatically downloaded to SecureClient during a site update. Which profile to work with is decided by your system administrator. Contact your system administrator for further information.
Changing Profiles

To switch profiles:

1. Disconnect from the current site by right-clicking the SecureClient icon in the system tray and selecting **Disconnect** from the pop-up menu. (You cannot change certificates while connected.)

2. Right-click the SecureClient icon in the system tray:

3. Select **Connect...**

   The **VPN-1 SecureClient Settings** window opens:

4. In the **Location Profile** drop-down menu, select the appropriate profile.

5. Enter your password.

6. Click **Connect**.
Creating a New Connection Profile

Your system administrator might require you to create a new connection profile for a particular site.

To create a new connection profile:

1. Right-click the SecureClient icon in the system tray:

2. Select Settings...

   The VPN-1 SecureClient Settings window opens.

3. On the Connections tab, click New > Profile...

   The Profile Properties window opens:

   Supply a name for the site and short description. From the Site drop-down box select the site. From the Gateway drop-down box select the appropriate Gateway.

4. Click the Advanced tab:

   Select the options as specified by your system administrator.

5. Click OK.

6. Click Close.
**Enabling Office Mode**

Office mode is used to overcome connectivity issues. For example, if your machine has been assigned an IP address that conflicts with an IP Address on the Site. Office mode resolves this issue. When Office mode is enabled, your machine receives a special “Office mode” address from the Gateway which does not conflict with any other IP address at the Site. Your system administrator will decide whether or not to use Office mode. If your system administrator has not provided with a specific profile with Office mode enabled, you might be instructed to enable Office mode manually.

To enable Office mode:

1. Right click the SecureClient icon in the system tray:
2. Select **Settings**.
   The **VPN-1 SecureClient Settings** window opens.
3. From the **Connections** tab, select the appropriate profile and click **Properties**.

   The **Profile Properties** window opens:
4. Select the name of your profile and click **Properties...**:
   The **Profile Properties** window opens:
5. Click the **Advanced** tab
6 Select **Support Office Mode**: 

7 Click **OK**.

**NOTE**: When office mode is enabled along with auto-connect mode, then the user must re-initiate the connection once the auto-connect connection has succeeded.

**Enabling Hub Mode**

Hub mode enables SecureClient to use the site's Gateway as a router. Traffic from SecureClient is not forwarded to the internal site but forwarded to another Gateway. The decision whether to use Hub mode is taken by your system administrator. You might be instructed to enable Hub mode manually. To enable Hub mode:

1 Right click the SecureClient icon in the system tray:

2 Select **Settings**...

   The **VPN-1 SecureClient Settings** window opens.

3 In the **Connections** tab, select the profile specified by your system administrator, and click **Properties**

   The **Profile Properties** window opens.

4 Click the **Advanced** tab.
5 Select **Route all traffic through gateway:**

![Profile Properties](image)

6 Click **OK**.

**Connection Modes**

SecureClient connects to the site in one of two modes:

- Connect mode
- Auto connect mode ("transparent mode" of earlier versions)

**Connect mode**

*Connect mode* means that when SecureClient detects traffic destined for the site, it connects to the site and encrypts the traffic. When SecureClient is disconnected from the site, traffic (to the site) is sent unencrypted. For example, suppose you open an FTP session with the site. If SecureClient is connected, then the FTP traffic is encrypted. If SecureClient is disconnected, the FTP traffic is still sent but not encrypted. In connect mode, you are not prompted to connect to the site.

**Auto connect Mode**

*Auto connect mode* means that SecureClient prompts you to connect to a site every time SecureClient detects certain traffic should be encrypted. That is, traffic that is destined for the site.

If you choose to connect, the traffic to the site is sent encrypted. If you choose not the connect, clicking **Cancel**, you are prompted to indicate for how long to remain disconnected without additional reminders:
During this time, traffic to the site is sent unencrypted. However, if your site is configured to drop all unencrypted traffic, you will not be able to communicate with servers behind the site’s Gateway.

**NOTE:** In auto connect mode, when traffic is detected that is destined for the site, SecureClient automatically connects. If office mode is also enabled, then the connection must be re-initiated by the user once the auto-connect connection has succeeded.

**Toggling Between Connect and Auto Connect Mode**

1. Right-click the SecureClient icon in the system tray:
2. From the pop-up menu select *Settings*....
   The VPN-1 SecureClient Settings window opens.
3. On the **Options** tab, select **Enable Auto-Connect**:
   - The **Enable Auto-Connect** option toggles between the two modes. When **Enable Auto-Connect** is not selected, you are in connect mode.
   - SecuRemote/SecureClient must now be restarted for the change to take effect.
4. Click **OK**.
   - The following message window appears:

April 2005 33
The change takes effect next your VPN-1 is relaunched. Select **Re-launch SecureClient now** or **I will relaunch SecureClient later**. If you choose to re-launch later, see: “Starting and Stop SecureClient”.

**Starting and Stop SecureClient**

- **To stop SecureClient.**
  Right-click the SecureClient icon in the system tray. From the pop-up menu select **Stop VPN-1 SecureClient**.

- **To start SecureClient.**
  From **Start > Programs > CheckPoint VPN-1 SecureClient > Select SecureClient**.

**Hot Spot Registration**

Enabling Hotspot registration can be done by either right clicking the system tray icon or by selecting the **Options** button in the **Connect** window.

Once **Register to Hot Spot/Hotel** is selected, a balloon message appears indicating the time period allowed for registration.

**Suspending Popup Messages**

When SecureClient is disconnected from the site, and **Auto-Connect** is enabled, then every time SecureClient detects traffic destined for the site, you are prompted to connect via a popup message. This popup message can be suspended.

To suspend Popup messages:

1. Right-click the SecureClient icon in the system tray.
2. From the pop-up menu select **Tools > Suspend Popup messages...**
   The Suspend Popup Messages window opens.
3. From the **File Menu**, selects **Tools > Suspend Popup Messages**.
   Select one of the options. The last option means SecureClient will prompt you to connect to the site only if it detects traffic destined for that site — in other words, traffic that should be encrypted.
4. Click **OK**.

If you choose to suspend popup messages, for example sixty minutes, then during those sixty minutes all traffic to the site is sent unencrypted. When the sixty minutes expires, you are once again prompted to connect each time SecureClient detects traffic destined for the site.
Secure Domain Logon (SDL)

In a windows environment, your account can belong to a domain controlled by the domain controller. SDL is useful when your domain controller lies behind the FireWall Gateway of your site. Your user details — name and password — belong to an account on the domain controller. When you log in, these credentials are sent to the domain controller for verification. However, SecureClient is typically launched after the login process, which means the traffic to and from the domain controller is not encrypted. SDL resolves this issue. When SDL is enabled, SecureClient launches before the login process begins, and the connection to the domain controller is encrypted. This decision is taken by our system administrator. If your system administrator decides the login process should be secure, enable SDL.

To enable SDL:

1. Right-click the SecureClient icon in the system tray:
2. From the pop-up menu select Settings...
   
The VPN-1 SecureClient Settings window opens.
   
3. On the Options tab, select Enable Secure Domain Logon
4. Click OK and reboot your computer.

Retrieving Status information

Two types of status information regarding the current status of SecureClient can be retrieved:
- General status information
- Advanced Status information
Retrieving General status information

1. Right-click the SecureClient icon in the system tray:

2. From the pop-up menu, select **Status...**:

   The **VPN-1 SecureClient Connection Status** window opens:

   ![VPN-1 SecureClient Connection Status window]

   The General tab is divided into three areas:
   - **Status**
   - **Protection**
   - **Diagnostic**

   **TABLE 2** The General tab

<table>
<thead>
<tr>
<th><strong>Section</strong></th>
<th><strong>Meaning</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Shows the current status, whether SecureClient is connected, the name of the active profile, the duration of the current connection and time remaining until the user next needs to authenticate, typically supplying a certificate and password.</td>
</tr>
<tr>
<td>Protection</td>
<td>Shows whether the Security Policy has been downloaded from the Policy server, and whether the local machine is securely configured.</td>
</tr>
<tr>
<td>Diagnostic</td>
<td>Clicking the link calls the SecureClient diagnostic utility.</td>
</tr>
</tbody>
</table>

Retrieving Advanced Status Information

1. Right-click the SecureClient icon in the system tray:

2. From the pop-up menu, select **Status**:

   The **VPN-1 SecureClient Connection Status** window opens.
Select the Advanced tab:

The advanced tab is divided into three areas:
- Activity
- Advanced
- Messages

**Activity**

Clicking Activity Viewer... opens the Activity Counters window:

This window displays information regarding:
- Encryption/decryption
- Compression/decompression ratios
- Packets accepted/rejected according to the Security Policy
Advanced

Clicking Advanced Details... displays the Advanced Status window:

When trouble-shooting, you system administrator might ask you to read the information here. A detailed explanation of each window is contained in the online help.

Messages

Clicking Message Viewer... displays the Message Viewer window:

The message viewer displays informational and warning error messages.

Understanding the Diagnostics Tool

The Diagnostic tool is a used to help trouble-shoot problem. To launch the diagnostic tool:

1. Right-click the SecureClient icon in the system tray.

2. From Tools > select Launch SecureClient Diagnostics...

The diagnostics tool covers three main areas in three views:
• Diagnostics View
• Policy View
• Logs View

**Diagnostics View**

The diagnostics view displays the current status of the machine in four categories:

- **Critical notifications.** This window displays critical notifications only.

- **SecureClient.** This window displays SecureClient's current state: information regarding active connections, location of Policy Server, secure configuration, active profile, and IKE/IPSec settings.
- **Connection.** This window displays information regarding active gateways, including encryption details.

- **Computer.** This window displays system and software information, for example: Operating system, major/minor version, service pack and build number; type of network interface card installed and current status.

**Policy View**

The Policy view displays the current Security Policy in installed on the desktop as a series of rules -- rules which apply to inbound connections, and rules which apply to outbound connections:

- **Inbound rules** - apply to connections destined for the VPN-1 SecureClient machine, initiated by an external source.
- **Outbound rules** - apply to connections destined for other machines, initiated by the VPN-1 SecureClient machine.
The direction of the rule (Inbound or Outbound) is determined by the location (source or destination) of a user group. Every rule in the Desktop Security Rule Base contains a user group, either in the Source column or in the Destination column — for example: mobile_Users@Any. This means that your system administrator created a group of remote users called mobile_users, and placed you in that group.

Inbound rules contain user groups in the Destination column and network objects in the Source column. Outbound rules contain user groups in the Source column and network objects in the Destination column:

Each rule in the Rule Base defines a specific connection in terms of source, destination, and service. When a connection matches these criteria, the action defined in the action column of the rule base is taken. The first rule that matches a connection is applied. In addition, the connection can be logged or an alert issued depending on the value in the Track field.

**NOTE:** Unless the Security Policy has been intentionally disabled, the Policy is always in effect, even when SecureClient is not connected to the VPN site.

**Log View**

The Log View enables the user to view SecureClient events, for example:

- When the Desktop Security Policy loaded
- Current connections
- Secure Configuration (SCV) state
Other events, such as the dropping of large packets.

Configuring Language Selection

A variety of languages are available to choose from to customize the interface of your SecureClient. The languages available are:

- English
- German
- Italian
- French
- Spanish

To select a language for the interface, proceed as follows:

1. Right click the SecureClient icon located in the system tray to display a pop-up menu.

2. Click Settings.

   The VPN-1 SecureClient Settings window is displayed.

3. Select the Advanced tab.

   Select a language from the drop down menu in the Language section

   Click OK.

Note - Switching languages will require restarting SecureClient for the changes to take place