Juniper™ NetScreen™ IPSec Dial Client

Installation Guide for Windows 2000® Windows XP®

Revision 1.0

1 Overview

This document gives detailed procedures including captured screen shots for end users to install and uninstall IPSec Dial Client on their PC. The final section of the document includes the instructions required to import the customer-specific security policy that contains the VPN connectivity information. Contact your company's contact to obtain your SafeNet security policy.

2 System Requirements

Operating system:	Juniper NetScreen Version 8.7 build 12 will be used for: Windows 2000* Windows XP*
Disk space:	10 MB
RAM:	64MB for Windows 2000 and Windows XP
Minimum CPU:	Pentium 200

Warning:
All other IPSec clients (e.g., Nortel Contivity or Cisco Unity clients) should be removed prior to installation of the SafeNet client. Any previous versions of SafeNet should be removed before starting the installation of the new version. Multiple IPSec clients existing on the same PC may cause serious problems, including system crash.

In the event of a third party personal firewall software is used in the Windows XP environment instead of the Windows firewall, it is recommended that the Windows firewall be turned off to avoid a possible conflict. It also allows the proper operation of the third party personal firewall.

Also after uninstalling the previous version of SafeNet SoftRemote client software the system must be rebooted. In Windows XP with Service Pack 2, ensure that the Windows firewall is turned off prior to installing the new release of the SafeNet SoftRemote client software. Then enable it after the installation completes. This applies to the case where there is no third party personal firewall enabled or active.

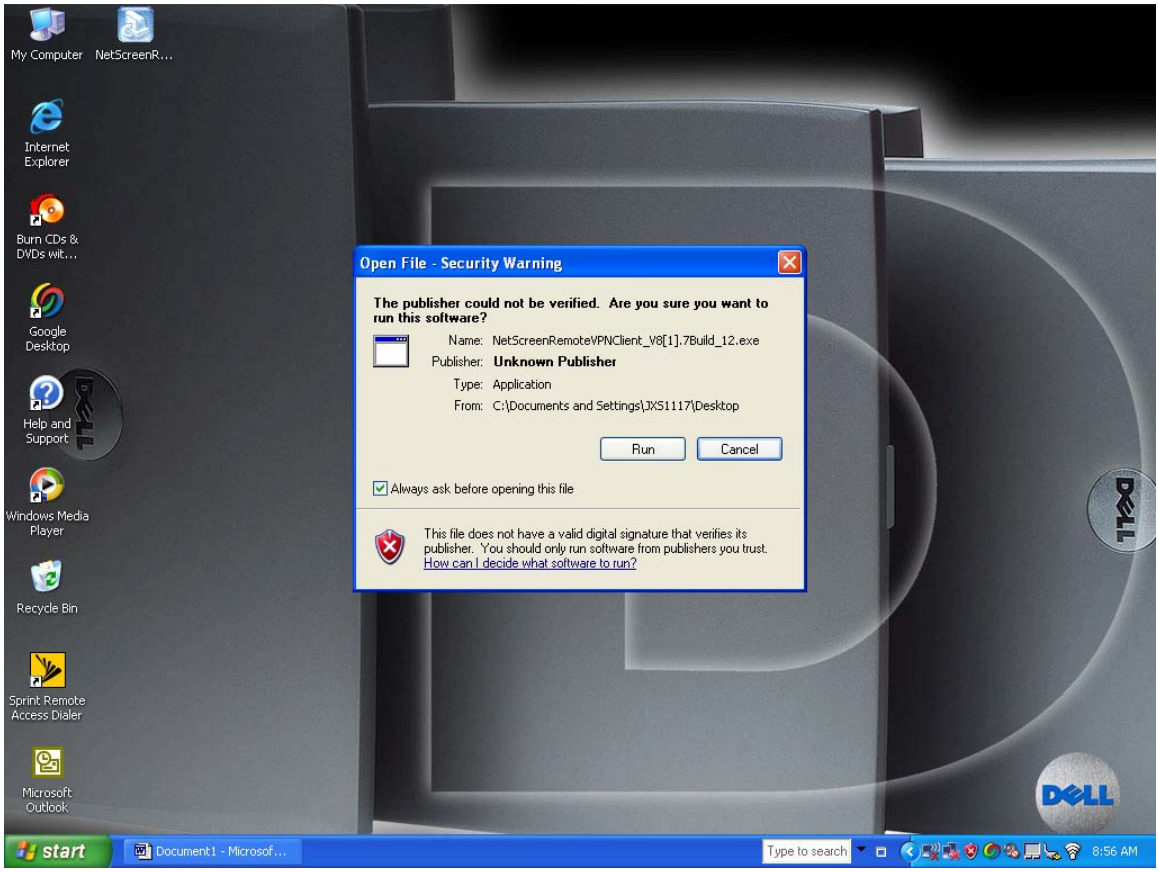
3 Installing the Client

Download and save the "Netscreen Remote VPN Client for Windows 2000 Professional, XP Home and XP Professional SP2" file to your PC Desktop. The file will be provided to you by your network contact or may be downloaded from the Internet at the following URL with pop-up enabled:

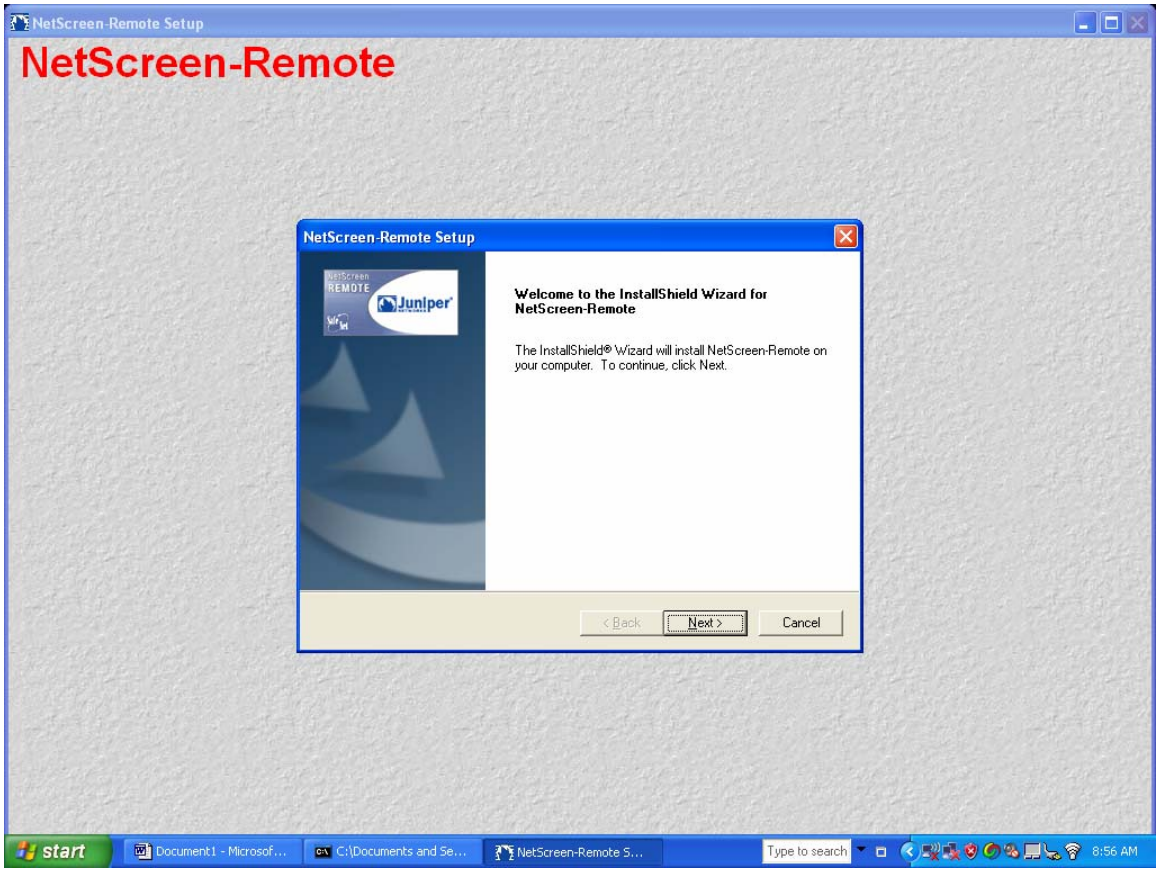
http://www.sprint.com/business/products/products/popup/popupVpnIndex.html

This self-extracting file contains all the components for installation.

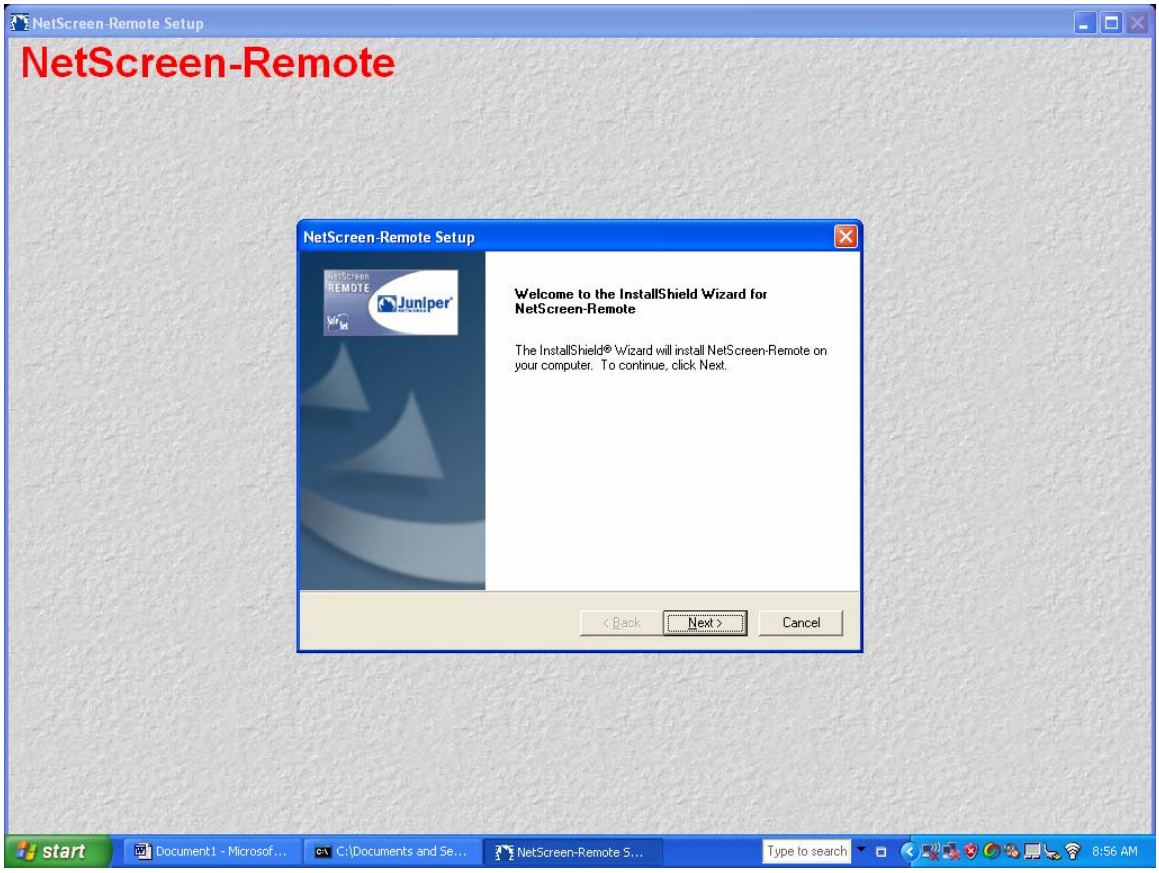
Step 1: Select "RUN" on the "NetScreenRemoteVPNClient_V8[1].7Build_12.exe" icon to execute the installation process.



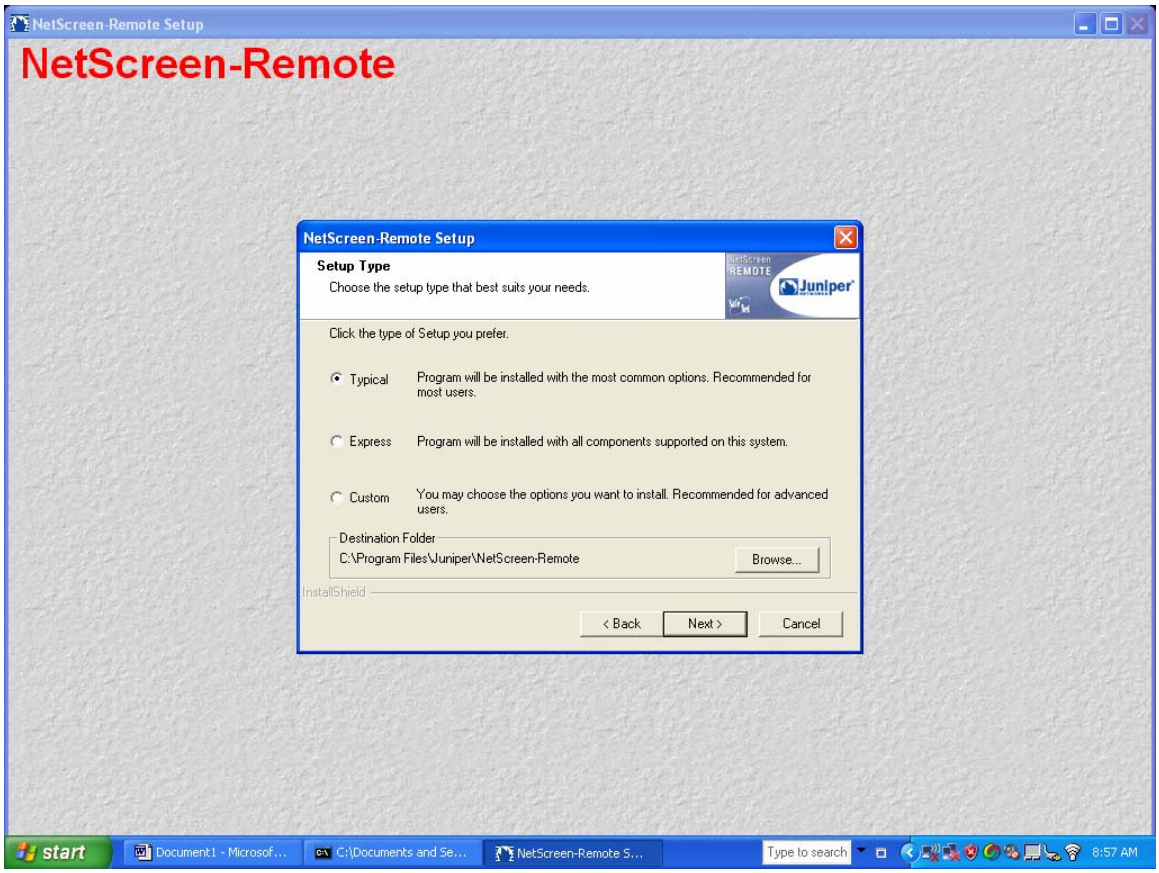
Step 2: Click on **NEXT** to continue on the following screen.



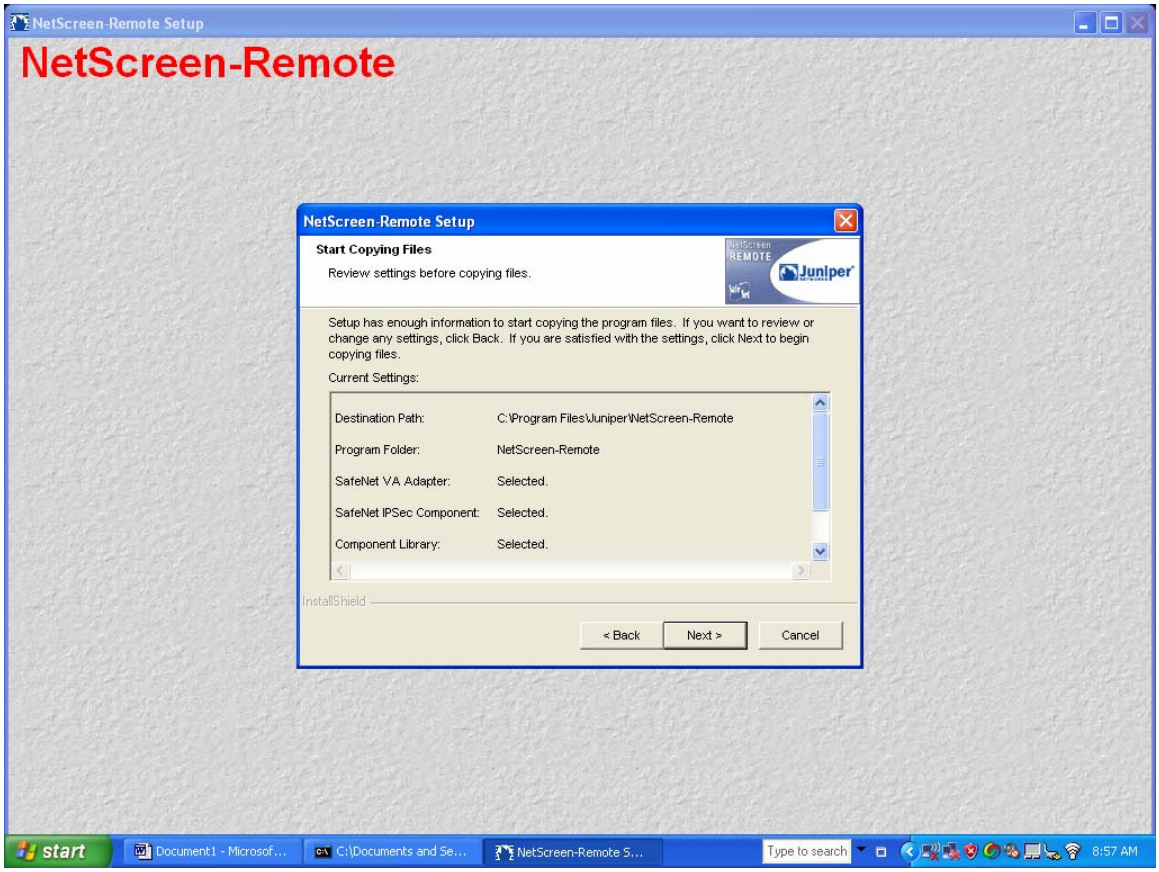
Step 3: When license agreement screen appears, select "YES" to continue.

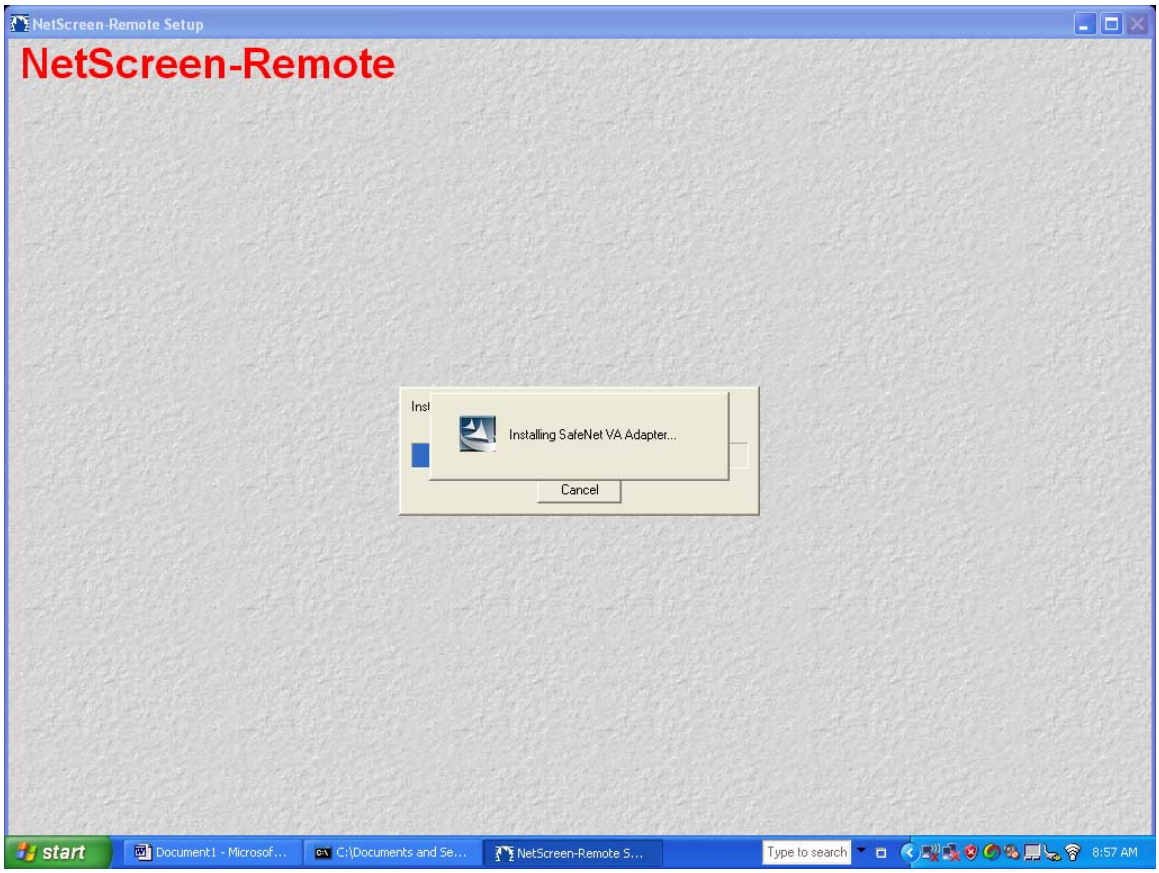


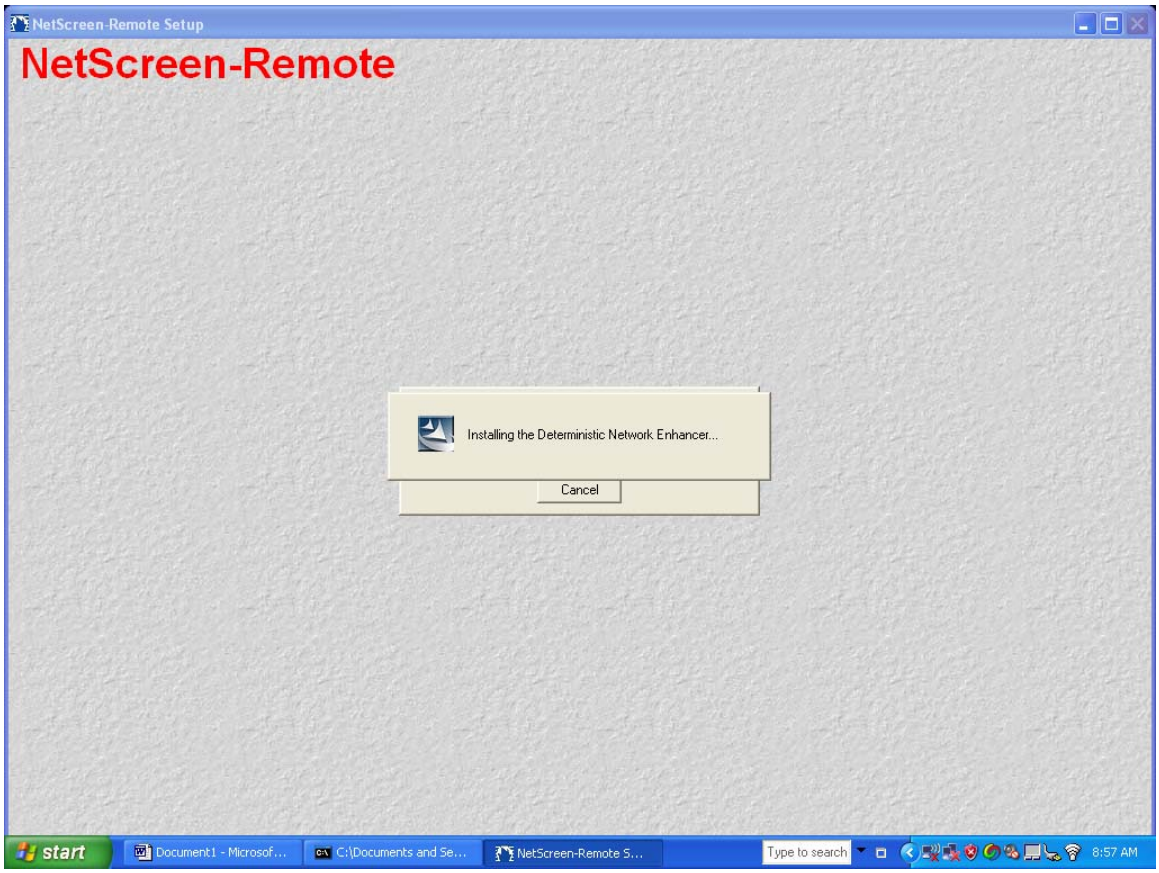
Step 4: Select "TYPICAL" in the NetScreen-Remote Setup screen and then select "NEXT"



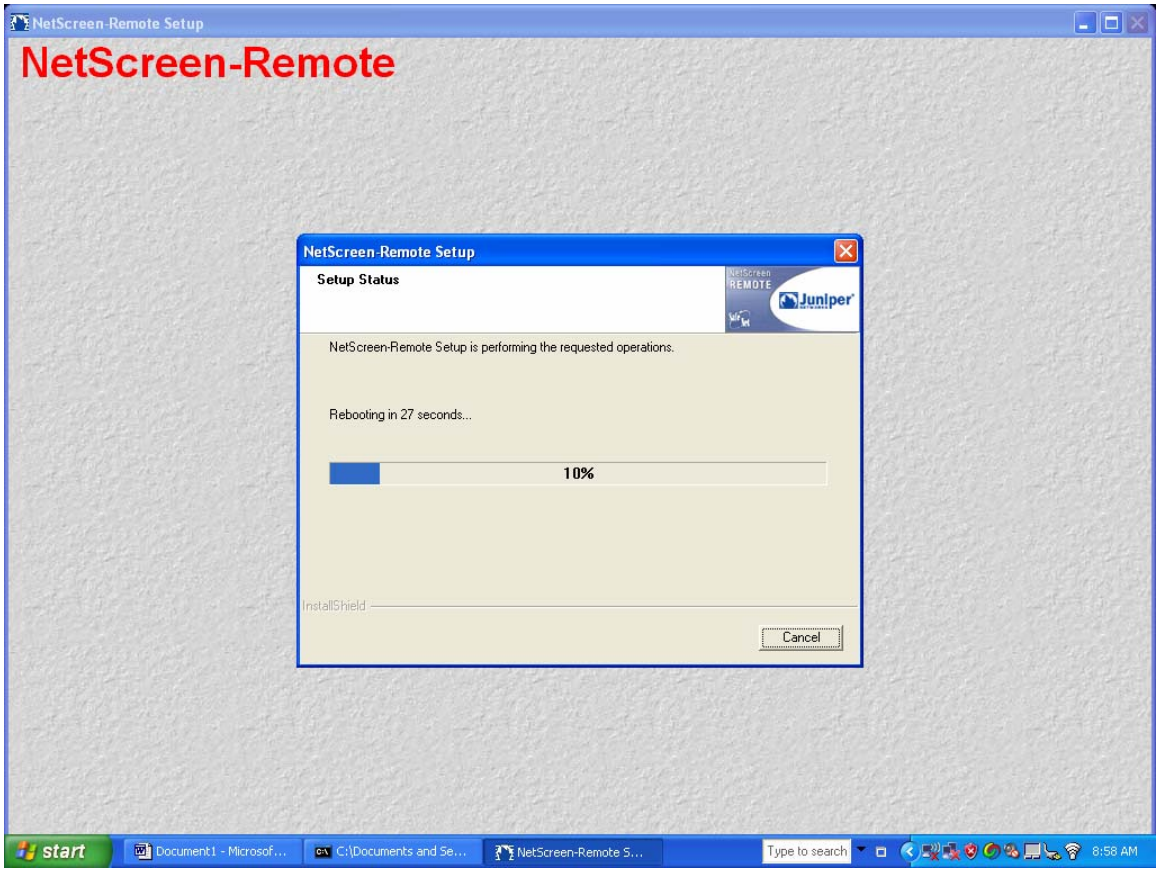
Step 5: At the InstallShield Wizard window, click **Next**.




NetScreen-Remote Setup
NetScreen-Remote
Installing SafeNet VA Adapter...
Cancel
start
Document1 - Microsof...
C:\Documents and Se...
NetScreen-Remote S...
Type to search
8:57 AM

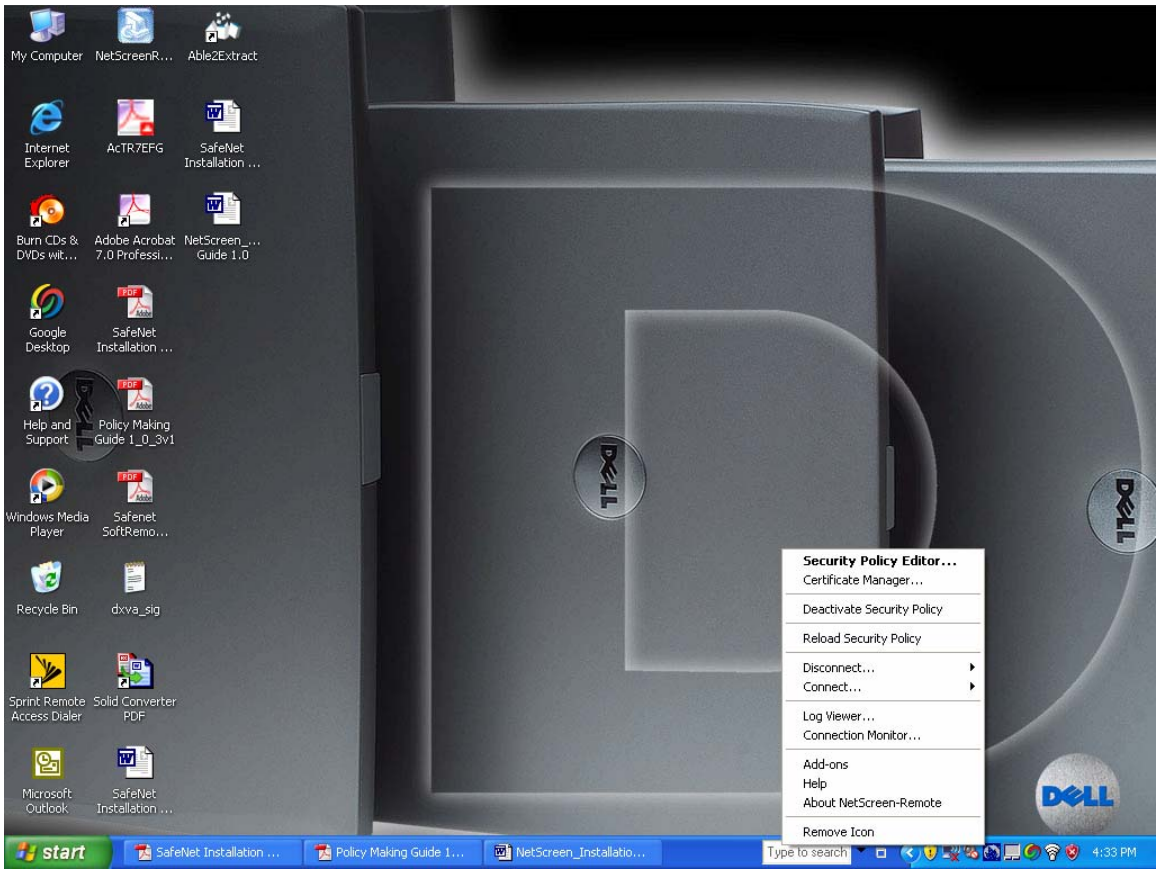

NetScreen-Remote Setup
NetScreen-Remote
Installing the Deterministic Network Enhancer...
Cancel
start
Document1 - Microsof...
C:\Documents and Se...
NetScreen-Remote S...
Type to search
8:57 AM

Step 6: Once Wizard has completed installation of files, the PC will automatically reboot.

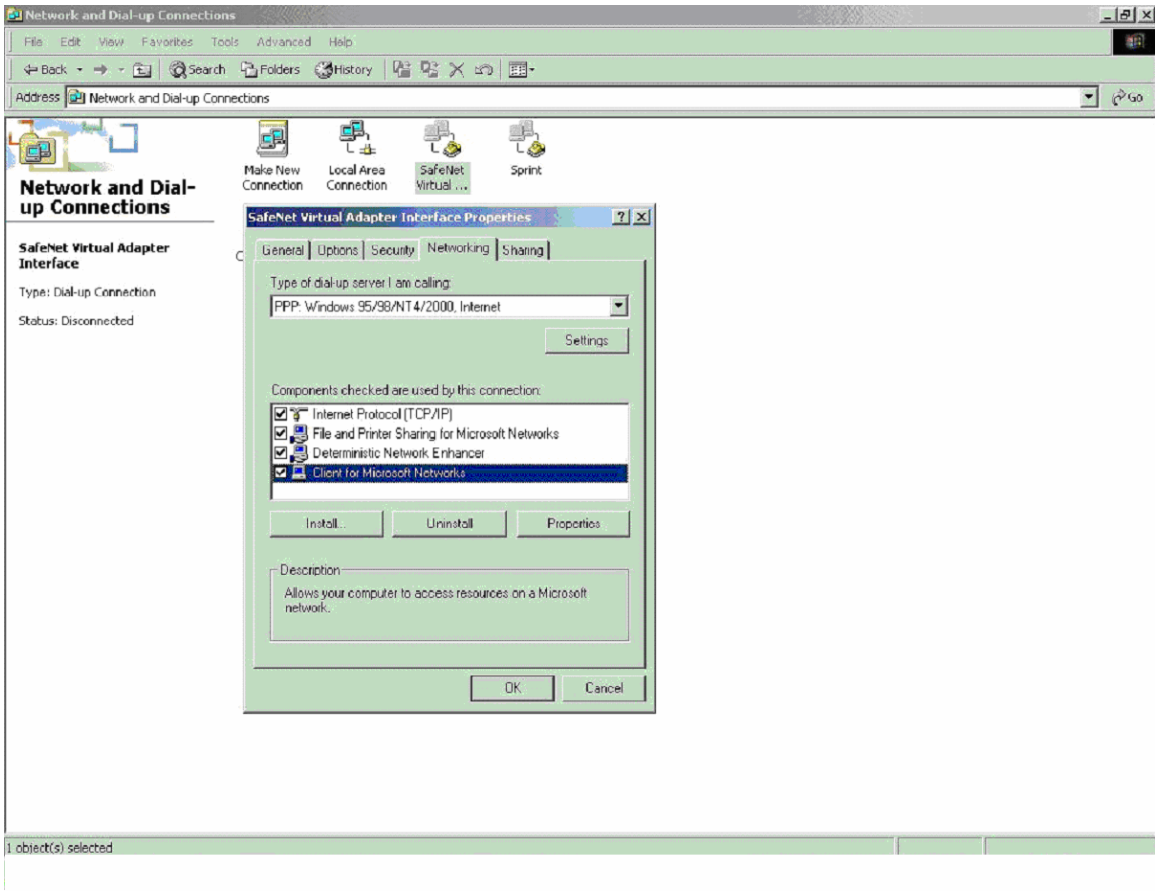


Step 7: When PC boots up, the NetScreen IPSec Dial Client icon should appear in the Windows System Tray. The IPSec Dial Client can be switched on and off by right clicking on the icon in the System Tray and selecting **Activate** or **Deactivate** from the menu. The IPSec Dial Client should be deactivated until the Security Policy has been imported.

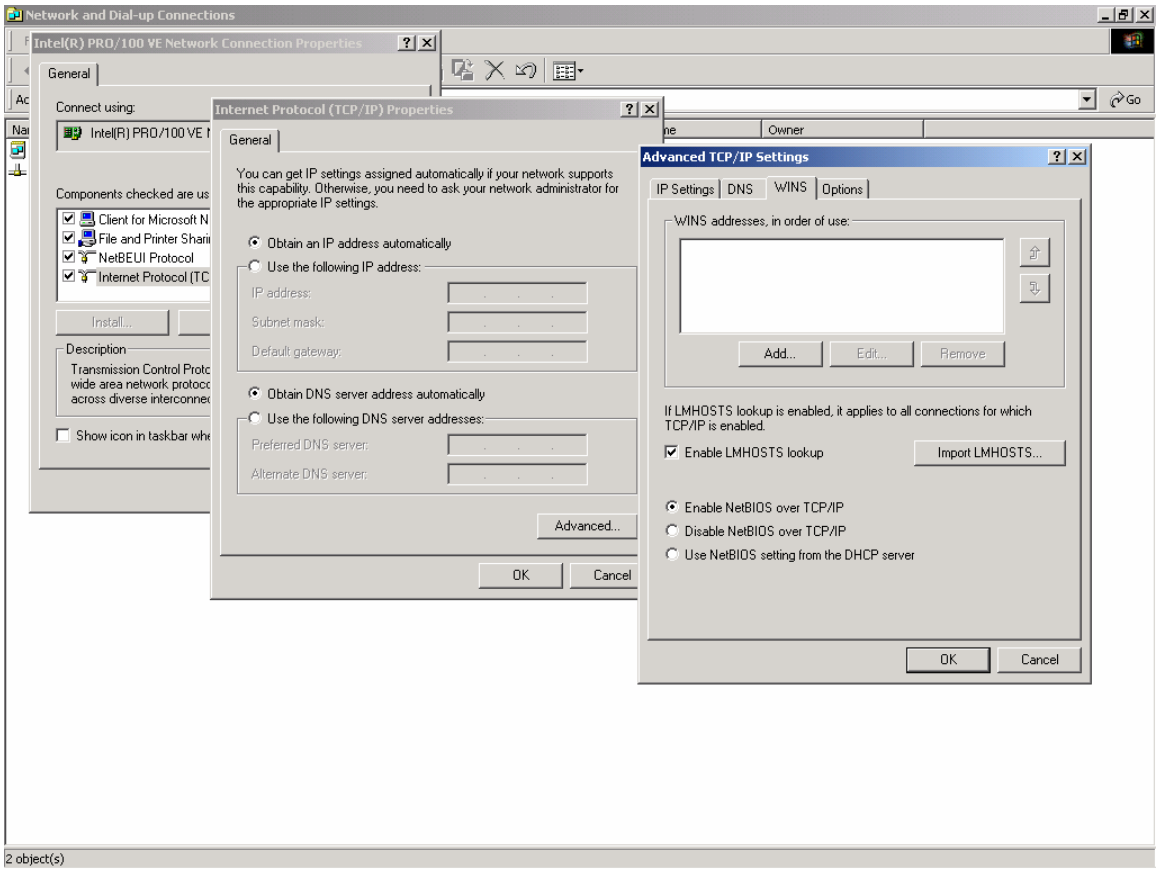
The IPSec Dial Client is now successfully installed.



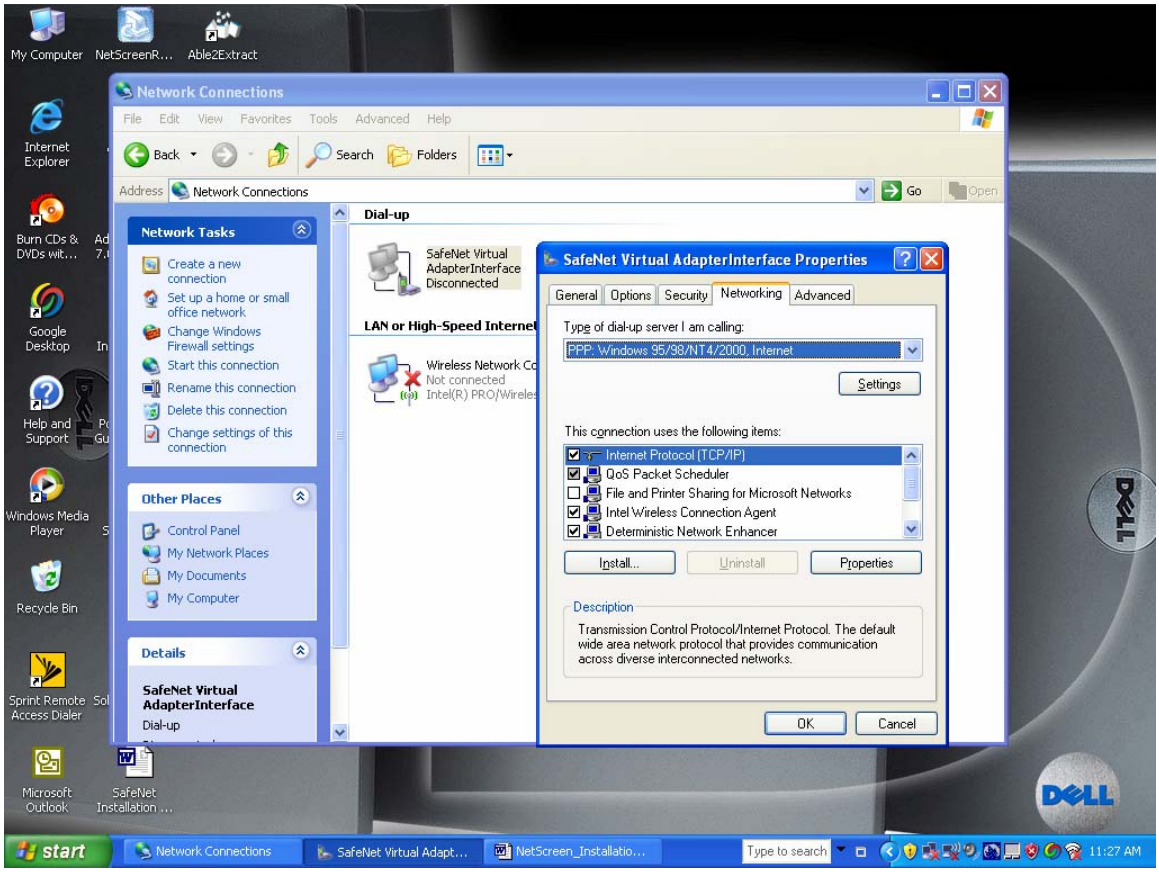
Step 8: In order to access Windows network resources (WINS resolution, file sharing), NetBIOS protocol may need to be enabled on the NetScreen virtual adaptor. This applies to all Windows operating systems. For most versions of Windows 2000, go to your "Network and Dial-up Connections" and select "properties' on the NetScreen virtual adaptor using right-click button on the mouse and then select "Networking**."** The virtual adaptor might not appear until a VPN connection is attempted. **If installed, check "File and Print Sharing for Microsoft Networks" and "Client for Microsoft Networks."**



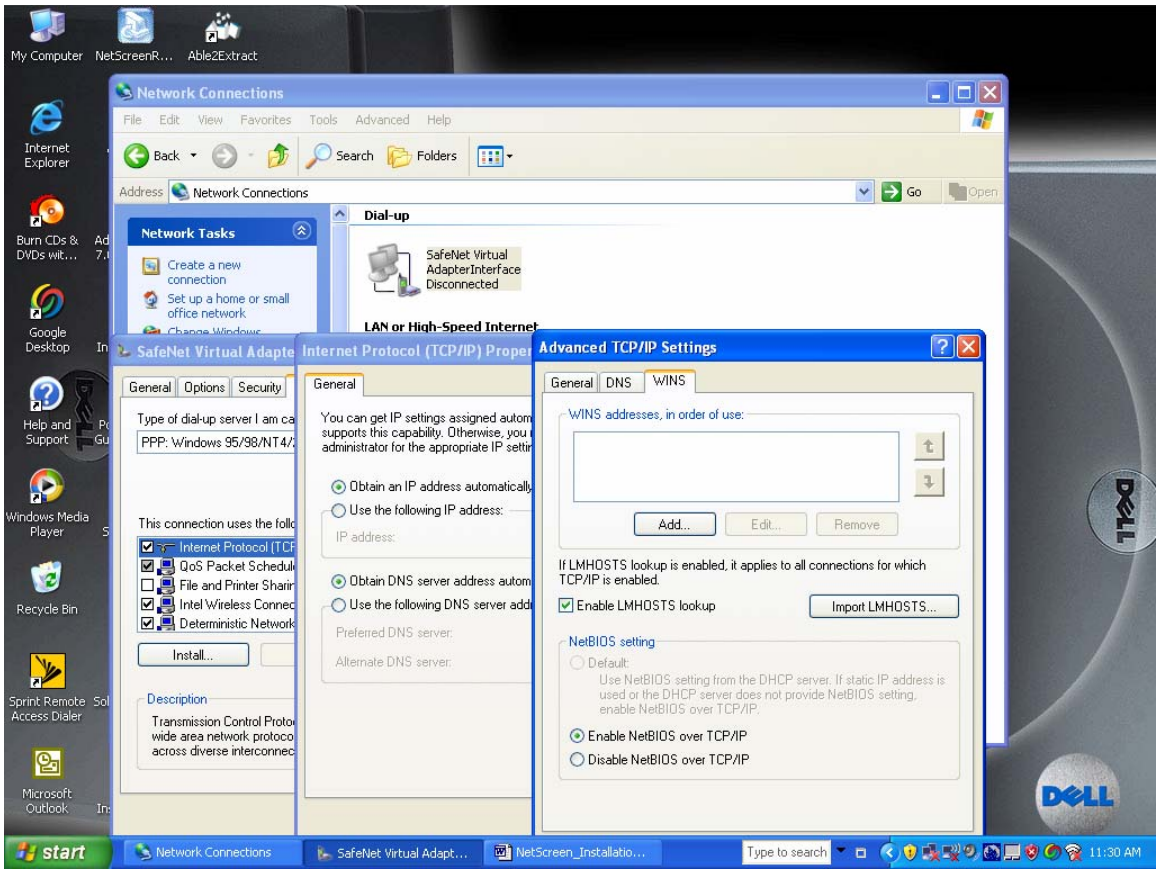
Highlight "Internet Protocol (TCP/IP)" and select "Properties." Then select "Advanced" and you should see the screen capture depicted on the next page. Select the Tab "WINS" and check the appropriate boxes shown. Then select OK and exit back out completely.



For most versions of Windows XP, go to "Network Connections" and highlight the NetScreen Virtual Adaptor and select "properties" using the right-click button on the mouse then select the "Networking" Tab. The virtual adaptor might not appear until a VPN connection is attempted. **If installed, check "File and Print Sharing for Microsoft Networks" and "Client for Microsoft Networks."**

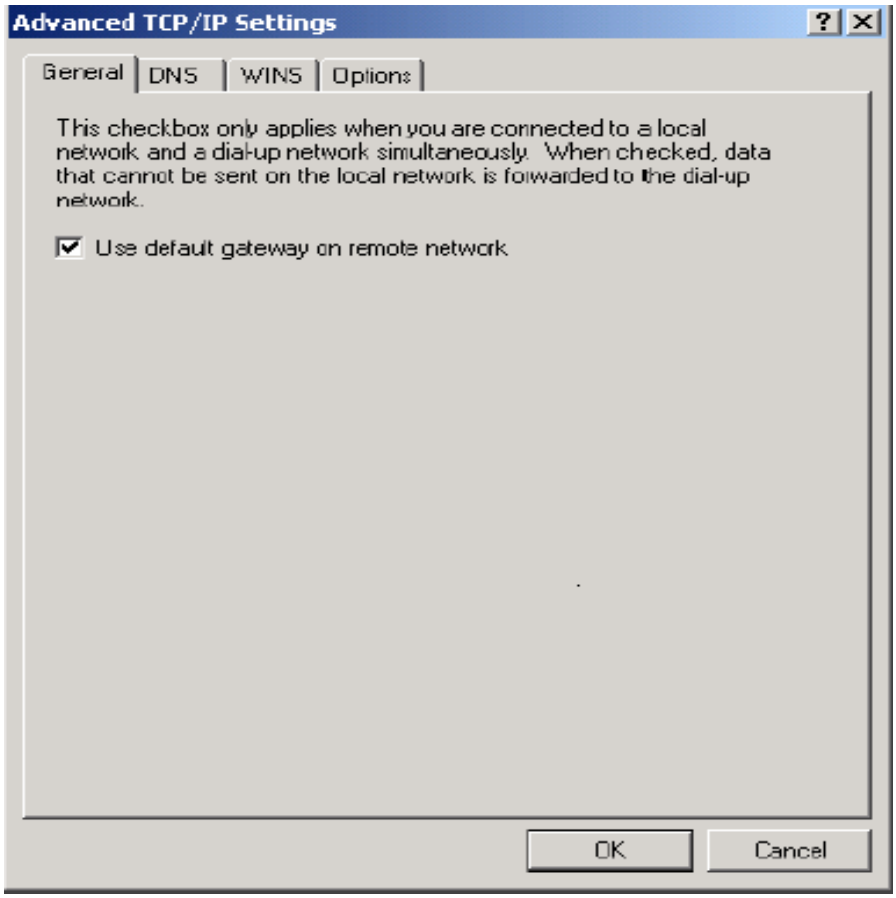


Highlight "Internet Protocol (TCP/IP)" and select "Properties." Then select "Advanced" and you should see the screen capture depicted below. Select the tab "WINS" and check the appropriate boxes shown. Then select OK and exit back out completely.

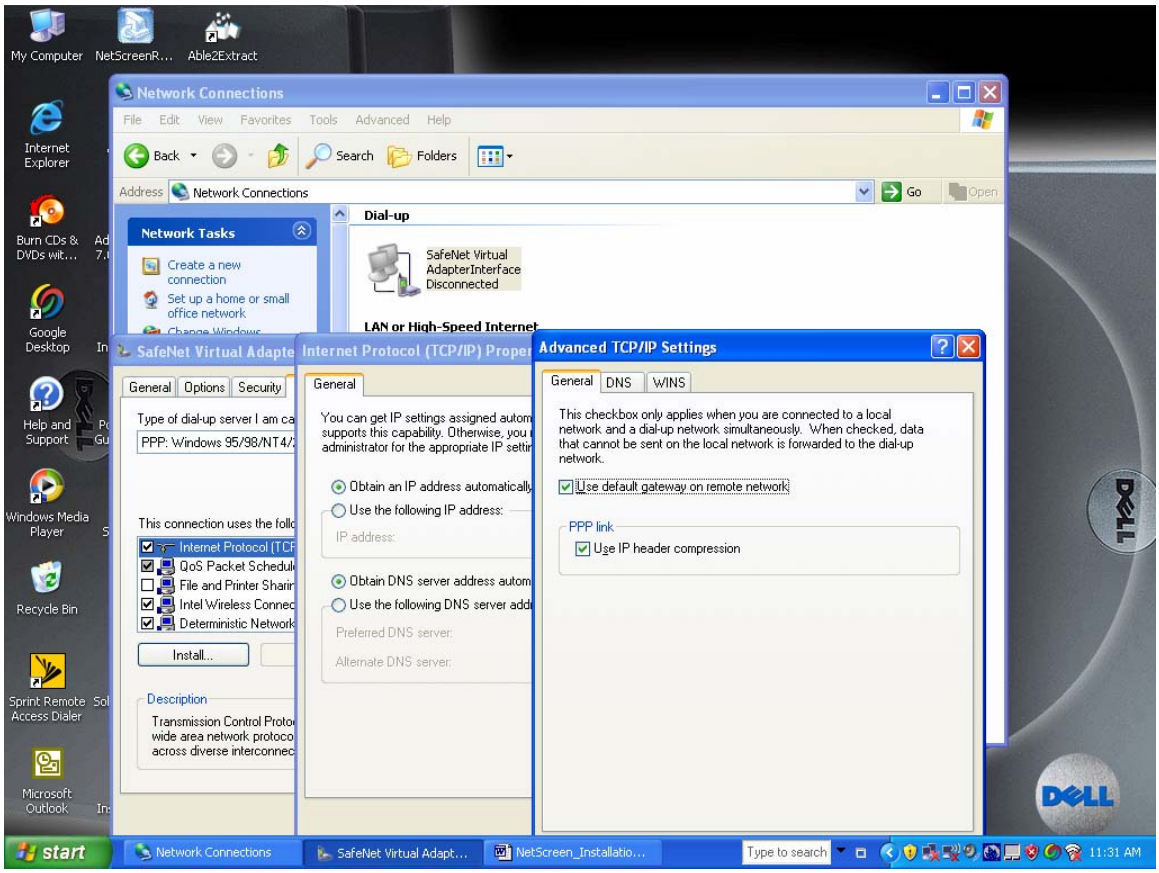


Step 9: Enable the default route option on the NetScreen virtual adaptor (it should be disabled if the user needs Split Tunneling option). By checking this option, all traffic is forced to go over the VPN client. It renders the local LAN resources inaccessible to the user until the VPN session is disconnected and the policy is de-activated.

To enable the default route on Windows 2000, go to your "Network and Dial-up Connections" and select "properties" on the SafeNet virtual adaptor using the right-click button on the mouse and choose "Networking." The virtual adaptor might not appear until a VPN connection is attempted. Highlight Internet Protocol (TCP/IP) and select "Properties" and choose the Tab "Advanced." Then select the "General" tab and check **Use default gateway on remote network.**



For most versions of Windows XP, go to your "Network and Dial-up Connections" and select "properties" on the SafeNet virtual adaptor and choose "Networking." Highlight Internet Protocol (TCP/IP) and select "Properties" and choose the Tab "Advanced." Then select the "General" tab and check **Use default gateway on remote network.**



Step 10: Import the NetScreen Security Policy into your VPN client. It contains your VPN-specific configuration which will establish a secure connection from the PC to your VPN. Obtain the security policy from your security administrator and follow the steps in the NetScreen Client Policy Import Guide contained below.

Caution! When not using your connection to the VPN, the session should be properly disconnected and de-activated. Using "right-click" mouse button on NetScreen icon  , select "disconnect all" and then "deactivate security policy", both in the same menu. If you shut down the PC without deactivating the policy, the session would stay active and you may not be able to use the Windows login at the next start up.

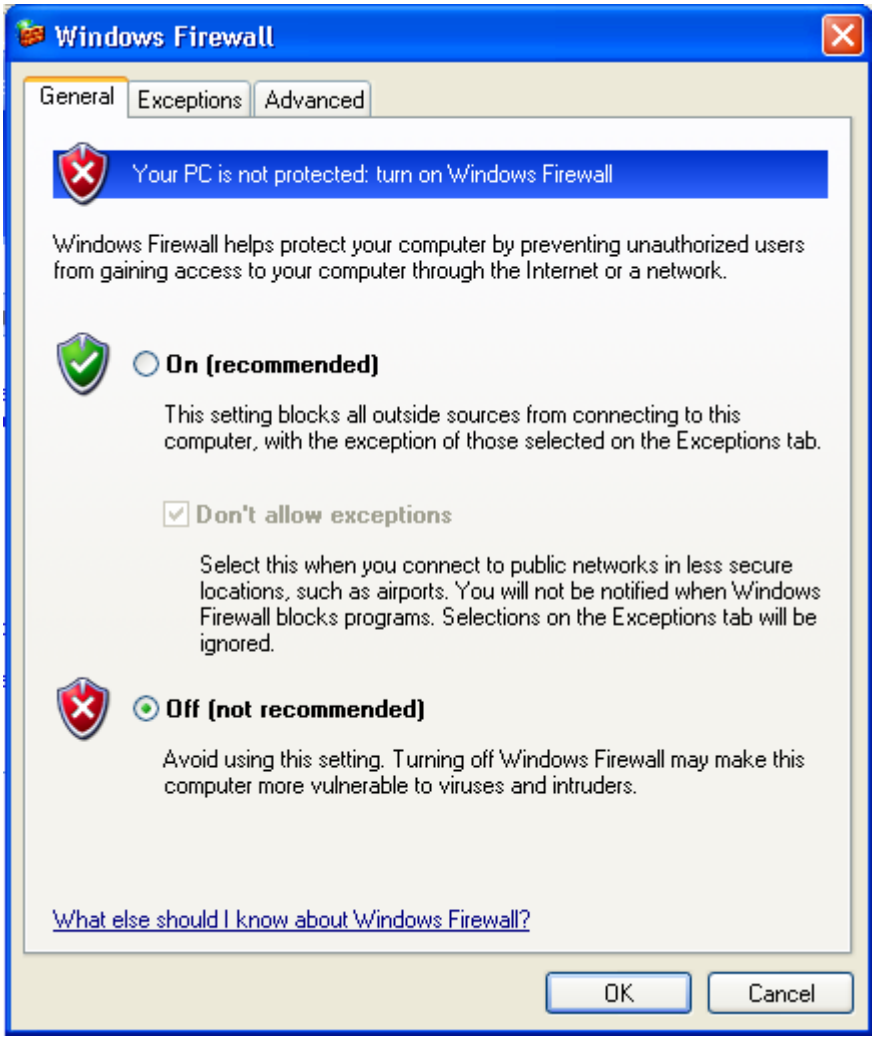
4 Verifying and Disabling Windows Firewall

In the client PC, a personal firewall can be active at a time to avoid a possible conflict. In the event of a third party personal firewall is used instead of the Windows XP firewall, the Windows firewall should be disabled. It also allows the proper operation of the third party personal firewall. The following are steps needed to verify to state of the Windows firewall.

Step 1: Go to Start
Step 2: Select Control Panel from the pop-up menu
Step 3: Click on Security Center
Step 4: If a personal firewall is active, the Security Center shows the following state


Windows Security Center
Security Center
Help protect your PC
Resources
Get the latest security and virus information from Microsoft
Check for the latest updates from Windows Update
Get support for security-related issues
Get help about Security Center
Change the way Security Center alerts me
Security essentials
Security Center helps you manage your Windows security settings. To help protect your computer, make sure the three security essentials are marked ON. If the settings are not ON, follow the recommendations. To return to the Security Center later, open Control Panel.
What's new in Windows to help protect my computer?
Firewall
ON
Automatic Updates
ON
Virus Protection
ON
ZoneAlarm Security Suite Antivirus reports that it is up to date and virus scanning is on. Antivirus software helps protect your computer against viruses and other security threats. How does antivirus software help protect my computer?
Note: You now have antivirus software that Windows can monitor. Click Recommendations to find out how.
Recommendations...
Manage security settings for:
Internet Options
Automatic Updates
Windows Firewall
At Microsoft, we care about your privacy. Please read our privacy statement.

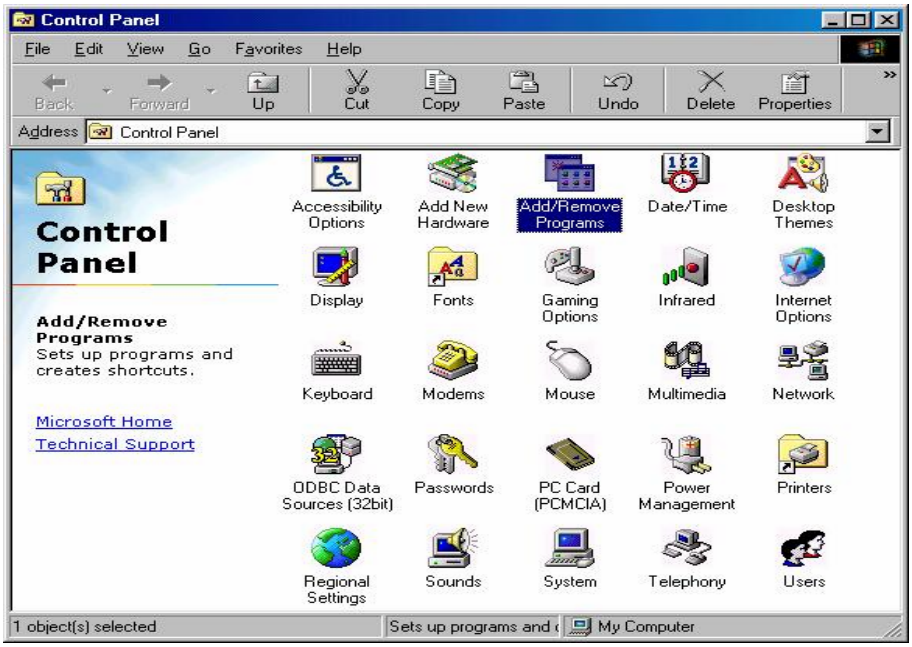
Step 5: Click on Windows Firewall to verify if it is disabled or not



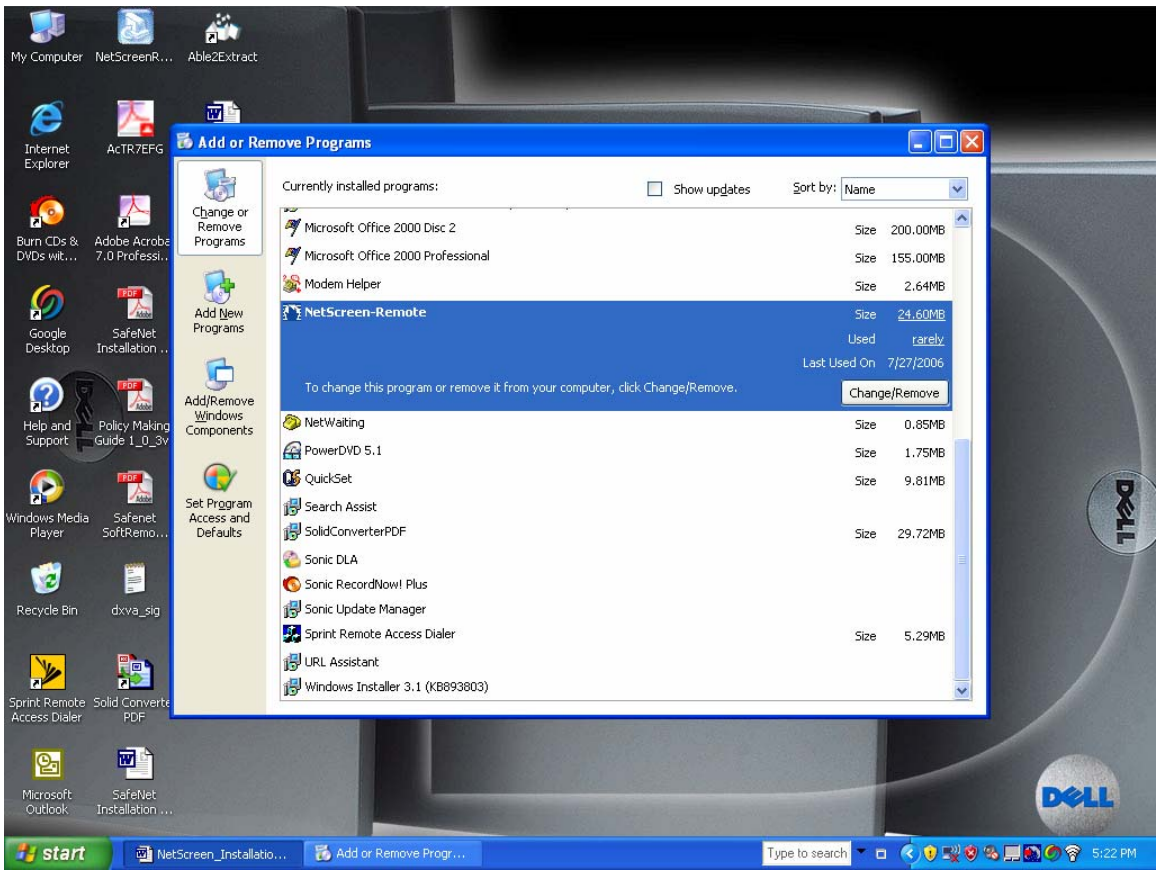
It should be turned off if a third party personal firewall is present and active.

5 Uninstalling the Client

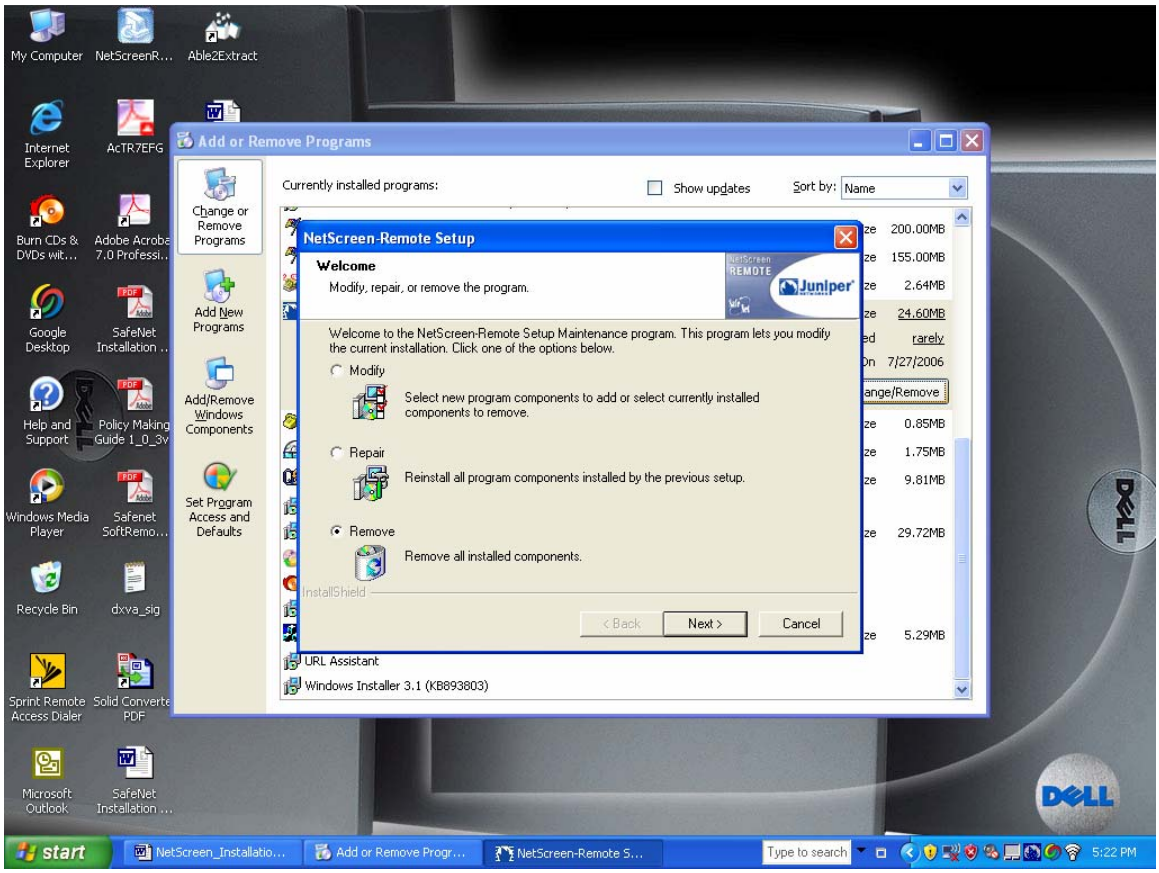
Step 1: Open up the Windows Control Panel by clicking **Start → Settings → Control Panel.** Double-click the **Add/Remove Programs** icon.



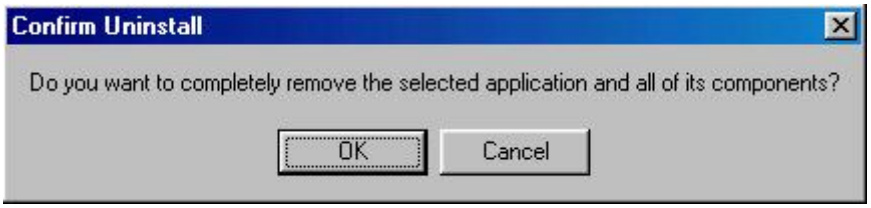
Step 2: For **Windows 2000 and Windows XP**, the following window is shown. Click on the **Change or Remove** icon in the Add/Remove Programs Window, Click to highlight *IPSec Dial Client*, and then click on **Change/Remove** to uninstall.



Step 3: Check the *Remove* option when the InstallShield Wizard window is displayed, then click **Next** to continue the uninstall process.

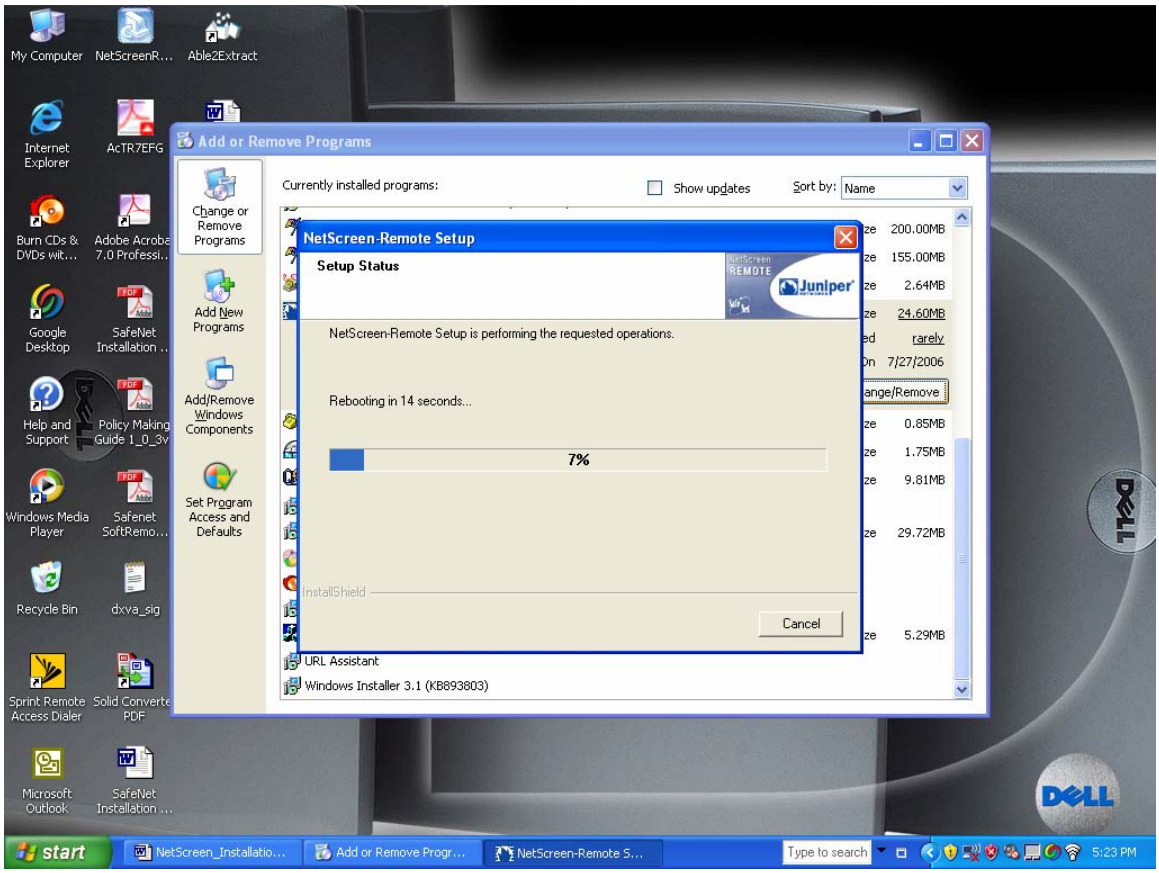


Step 4: Click **OK** when prompted with the following message to confirm the uninstall.



Click **Yes** when prompted with the following message box to completely remove the client. Click No is you are upgrading to a new version of the SafeNet IPSec Dial Client since you will need to re-import the security policy.

Step 5: When the Maintenance Complete window is shown, click **Finish** to restart the PC and complete uninstalling the IPSec Dial Client.



Step 6: When the PC boots up, the IPSec Dial Client icon should not appear in the Windows System Tray. The IPSec Dial client has been removed from the PC.

6 Importing a Policy

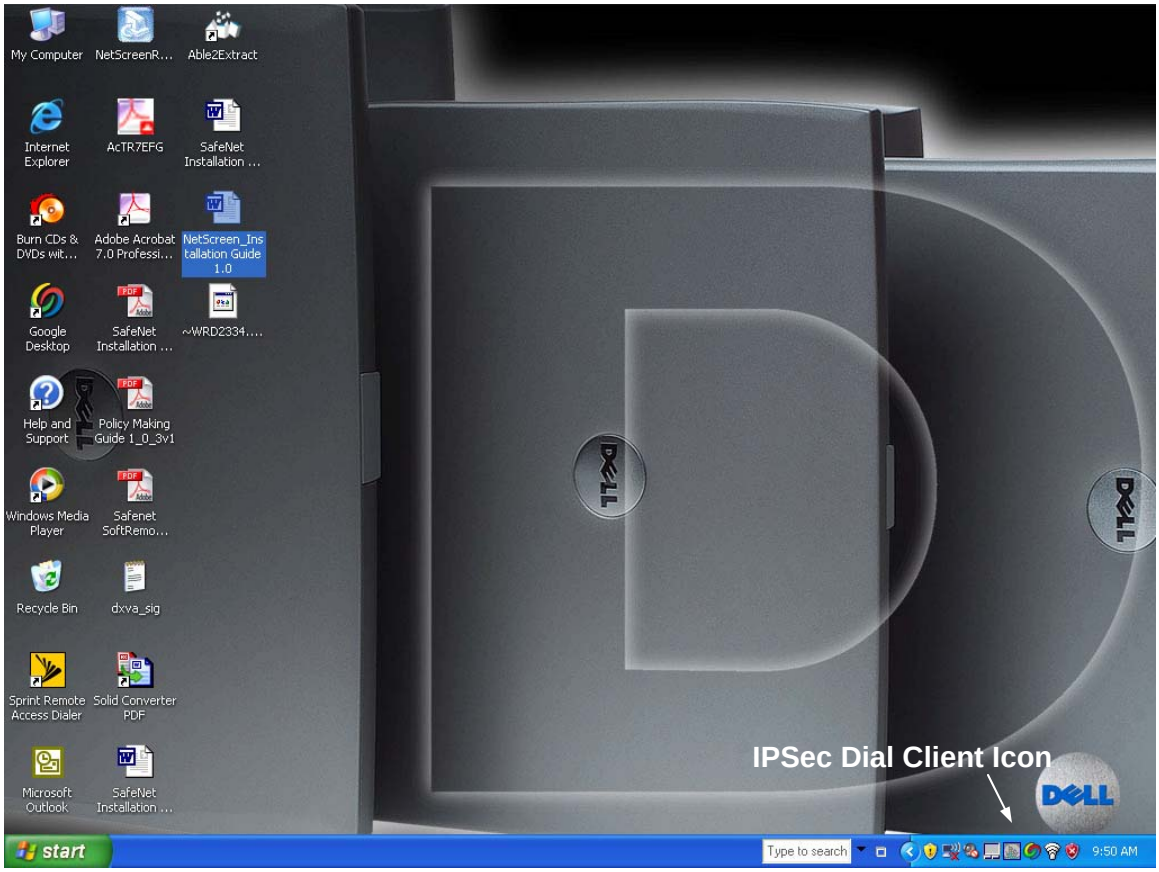
In order to connect to your company's network, you must instruct the IPSec Dial client how to establish this connection. This information is contained in a policy that is imported into the Dial Client.

Confirm that the SafeNet SoftRemote IPSec Dial Client is installed on your PC. The IPSec Dial Client icon (either if it's activated or if it's deactivated) will appear in the Windows System Tray if the client is installed. If the client has not been installed, refer to the Installation Guide for Windows 98/NT/2000/XP users.

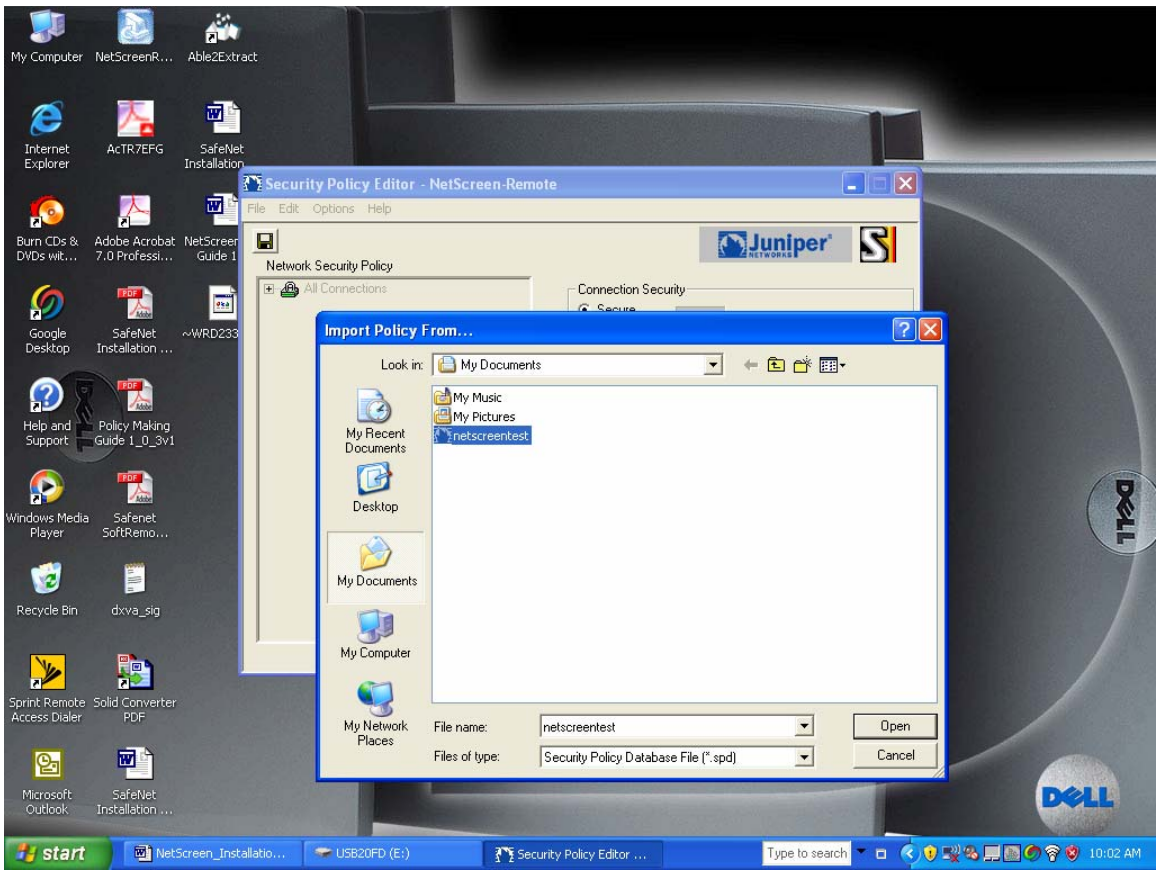
You will need to obtain a policy from your company's administrator. The policy file will have the extension ".spd" (e.g., NewPolicy.spd). Note the directory where you save the policy file (e.g., C:\Data, C:\My Documents, or the Windows Desktop).

Before importing a policy, the client needs to be activated. It is already activated if the Dial Client icon looks like  . If it does not, right click on the  icon and select **Activate Security Policy** from the menu.

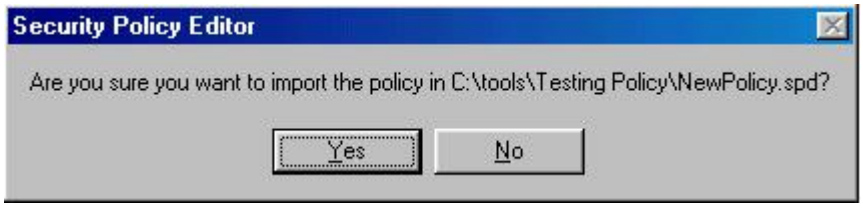
Step 1: Double-click on the activated IPSec Dial Client icon  located in the Windows System Tray to open up the IPSec Dial Client's "Security Policy Editor" window. Choose **File** from the Menu Bar and select **Import Security Policy**.



Step 2: From the "Import policy from…" window, locate the policy file in the directory where you saved it (e.g., C:\Data, C:\My Documents, or the Windows Desktop). Highlight the policy file then click **Open** to import the policy.



Step 3: Click **Yes** to confirm selection of the policy and continue the importation process.



Step 4: Click **OK** to complete the policy importation process. The policy is now loaded into the IPSec Dial Client.

Step 5: Click **File** on the Menu Bar and select **Save Changes** to put policy in effect or generate interesting traffic using a web browser or ping.