



## Avaya Solution & Interoperability Test Lab

---

# Configuring a Juniper Networks NetScreen-Remote VPN Client to Support an Avaya IP Softphone Secure Connection to a Samsung Ubigate™ iBG3026 Gateway - Issue 1.0

### Abstract

These Application Notes describe the procedures for configuring a secure VPN connection to the Samsung Ubigate™ iBG3026 Gateway using the Juniper Networks NetScreen-Remote VPN Client to support the Avaya IP Softphone.

The Samsung iBG3026 functions as a multi-service IP switch/router. With the addition of a VPN/Internet Protocol Security (IPSec) option card, the Samsung iBG3026 provides VPN functionality to support remote users using Juniper NetScreen-Remote through the public Internet. In a mixed customer environment where both Juniper and Samsung VPN gateways are installed, the remote users can use the same Juniper NetScreen-Remote to securely connect to the office network for telephony and data access.

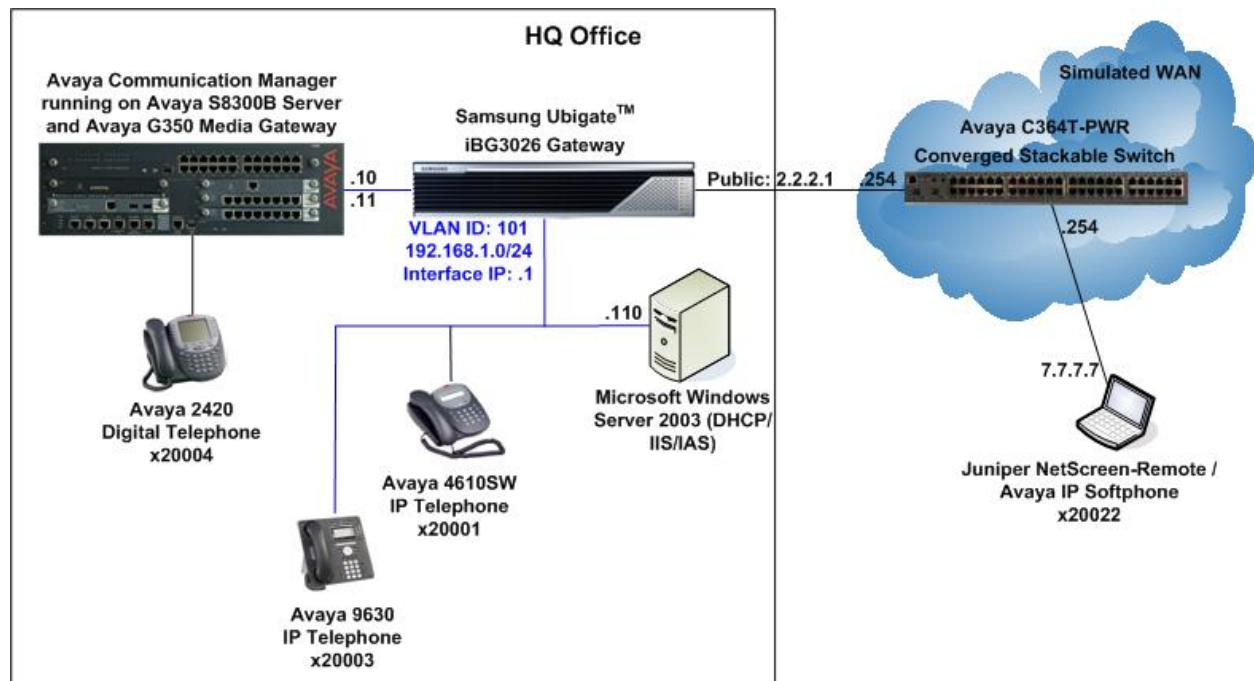
# 1. Introduction

These Application Notes describe the procedures for configuring a secure VPN connection to the Samsung Ubigate™ iBG3026 Gateway using the Juniper Networks NetScreen-Remote VPN Client to support the Avaya IP Softphone.

The Samsung iBG3026 is designed to provide WAN-connectivity such as T1, E1, T3, and metro Ethernet to a small-to-medium sized office. The Samsung iBG3026 provides VPN/firewall functionality for WAN interfaces, so remote users can build secure communication channels through the public Internet.

# 2. Test Configuration

The sample network implemented for these Application Notes is shown in Figure 1.



**Figure 1: Test Configuration**

The HQ Office consists of a Samsung iBG3026 functioning as a layer 2 Ethernet switch with Power-over-Ethernet (PoE), layer 3 router, perimeter security device and Internet Protocol Security (IPSec) VPN gateway. User authentication for remote users is done using the Microsoft Internet Authentication Service (IAS) running on a Microsoft Windows Server 2003. Avaya Communication Manager running on the Avaya S8300B Server and Avaya G350 Media Gateway provides the IP telephony platform for local and remote users.

Remote users connected to the public internet use the Juniper NetScreen-Remote for secure connection to the HQ Office and use the Avaya IP Softphone for telephony functionality.

An Avaya C364T-PWR Converged Stackable Switch simulates the WAN by routing the IP traffic between the remote user and the HQ Office.

The VPN tunnel between the Samsung iBG3026 and Juniper NetScreen-Remote is configured based on the following parameters:

**Phase 1**

Authentication Method: Pre-shared Key with extended authentication (Xauth)

Encryption: Triple Data Encryption Standard (3DES)

Authentication: Secure Hash Algorithm-1 (SHA-1)

Diffie-Hellman (DH) Group: 2

**Phase 2**

Encapsulation: Encapsulation Security Payload (ESP)

Encryption: Advanced Encryption Standard (AES) 128-bit keys

Authentication: SHA-1

Perfect Forward Secrecy: Disabled

### 3. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment	Software
Avaya S8300B Server	Avaya Communication Manager 3.1.2 (R013x.01.2.632.1) Service Pack 12714
Avaya G350 Media Gateway	25.33.0
Avaya 9630 IP Telephones	R1.1 (H.323)
Avaya 4610SW IP Telephones	R2.7 (H.323)
Avaya 2420 Digital Telephone	-
Avaya IP Softphone	R5.2 Service Pack 1
Avaya C364T-PWR Converged Stackable Switch	4.5.14
Samsung Ubigate™ iBG3026	SNOS 1.0.5.9 Advanced DSP 1.0.2 firmware
Juniper Networks NetScreen-Remote VPN Client	8.7 build 12
Microsoft Windows Server 2003	Service Pack 1

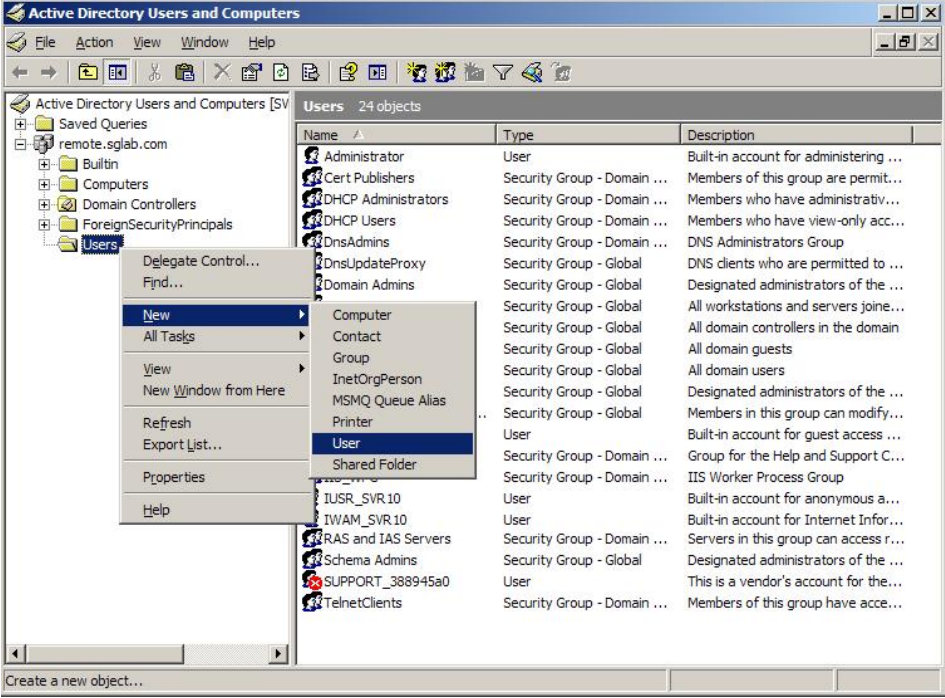
## 4. Configure Avaya Communication Manager and Avaya IP Telephones

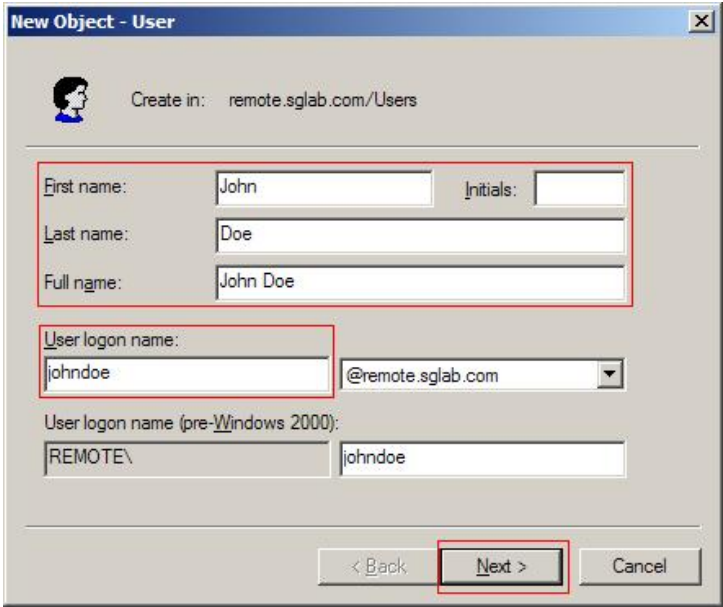

These application notes assume that the configuration of Avaya Communication Manager and the Avaya IP telephones are already in place. Refer to [1] for detail instructions on the configuration on these components.

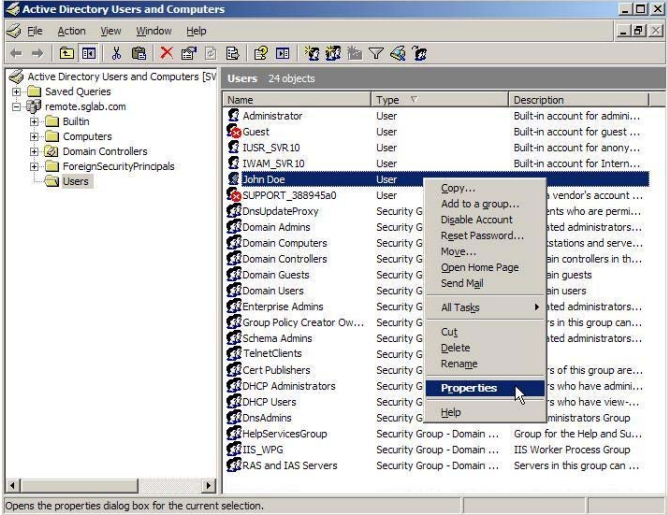
## 5. Configure Microsoft Active Directory

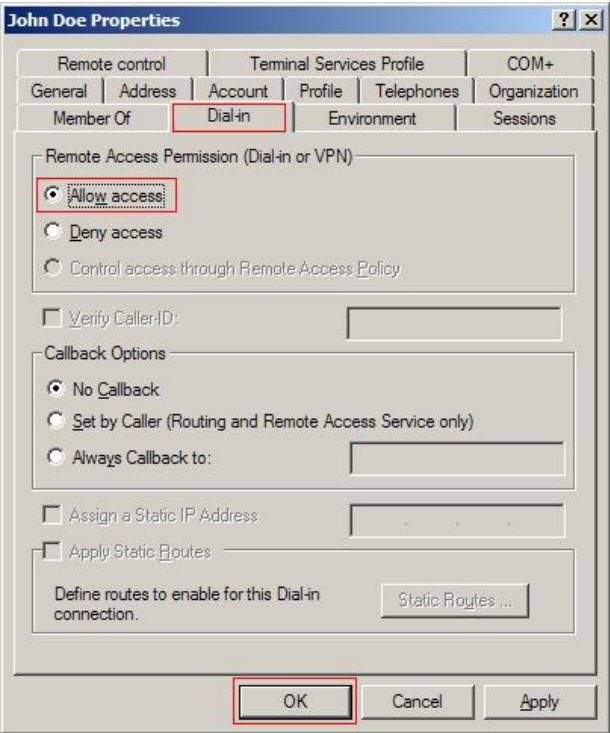
### 5.1. Create User Accounts

The steps below create a new user account for the Juniper NetScreen-Remote user shown in Figure 1. These Application Notes assume Microsoft Active Directory is installed and operational.

Step	Description																																																																					
1.	<p>On the Microsoft Windows 2003 Server running Active Directory, open the <b>Active Directory Users and Computers</b> application window by selecting <b>Start &gt; All Programs &gt; Administrative Tools &gt; Active Directory Users and Computers</b>. Right click the <b>Users</b> folder and select <b>New &gt; User</b> from the pop-up menu as shown below.</p>  <p>The screenshot shows the 'Active Directory Users and Computers' window. The left pane shows the tree structure with 'Users' selected. The right pane shows a list of 24 objects. A context menu is open over the 'Users' folder, and the 'New' option is expanded to show 'User' as the selected option.</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Type</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Administrator</td> <td>User</td> <td>Built-in account for administering ...</td> </tr> <tr> <td>Cert Publishers</td> <td>Security Group - Domain ...</td> <td>Members of this group are permit...</td> </tr> <tr> <td>DHCP Administrators</td> <td>Security Group - Domain ...</td> <td>Members who have administrativ...</td> </tr> <tr> <td>DHCP Users</td> <td>Security Group - Domain ...</td> <td>Members who have view-only acc...</td> </tr> <tr> <td>DnsAdmins</td> <td>Security Group - Domain ...</td> <td>DNS Administrators Group</td> </tr> <tr> <td>DnsUpdateProxy</td> <td>Security Group - Global</td> <td>DNS clients who are permitted to ...</td> </tr> <tr> <td>Domain Admins</td> <td>Security Group - Global</td> <td>Designated administrators of the ...</td> </tr> <tr> <td></td> <td>Security Group - Global</td> <td>All workstations and servers joine...</td> </tr> <tr> <td></td> <td>Security Group - Global</td> <td>All domain controllers in the domain</td> </tr> <tr> <td></td> <td>Security Group - Global</td> <td>All domain guests</td> </tr> <tr> <td></td> <td>Security Group - Global</td> <td>All domain users</td> </tr> <tr> <td></td> <td>Security Group - Global</td> <td>Designated administrators of the ...</td> </tr> <tr> <td></td> <td>Security Group - Global</td> <td>Members in this group can modify...</td> </tr> <tr> <td></td> <td>Security Group - Global</td> <td>Built-in account for guest access ...</td> </tr> <tr> <td></td> <td>Security Group - Domain ...</td> <td>Group for the Help and Support C...</td> </tr> <tr> <td></td> <td>Security Group - Domain ...</td> <td>IIS Worker Process Group</td> </tr> <tr> <td>IUSR_SVR.10</td> <td>User</td> <td>Built-in account for anonymous a...</td> </tr> <tr> <td>IWAM_SVR.10</td> <td>User</td> <td>Built-in account for Internet Infor...</td> </tr> <tr> <td>RAS and IAS Servers</td> <td>Security Group - Domain ...</td> <td>Servers in this group can access r...</td> </tr> <tr> <td>Schema Admins</td> <td>Security Group - Global</td> <td>Designated administrators of the ...</td> </tr> <tr> <td>SUPPORT_388945a0</td> <td>User</td> <td>This is a vendor's account for the...</td> </tr> <tr> <td>TelnetClients</td> <td>Security Group - Domain ...</td> <td>Members of this group have acce...</td> </tr> </tbody> </table>	Name	Type	Description	Administrator	User	Built-in account for administering ...	Cert Publishers	Security Group - Domain ...	Members of this group are permit...	DHCP Administrators	Security Group - Domain ...	Members who have administrativ...	DHCP Users	Security Group - Domain ...	Members who have view-only acc...	DnsAdmins	Security Group - Domain ...	DNS Administrators Group	DnsUpdateProxy	Security Group - Global	DNS clients who are permitted to ...	Domain Admins	Security Group - Global	Designated administrators of the ...		Security Group - Global	All workstations and servers joine...		Security Group - Global	All domain controllers in the domain		Security Group - Global	All domain guests		Security Group - Global	All domain users		Security Group - Global	Designated administrators of the ...		Security Group - Global	Members in this group can modify...		Security Group - Global	Built-in account for guest access ...		Security Group - Domain ...	Group for the Help and Support C...		Security Group - Domain ...	IIS Worker Process Group	IUSR_SVR.10	User	Built-in account for anonymous a...	IWAM_SVR.10	User	Built-in account for Internet Infor...	RAS and IAS Servers	Security Group - Domain ...	Servers in this group can access r...	Schema Admins	Security Group - Global	Designated administrators of the ...	SUPPORT_388945a0	User	This is a vendor's account for the...	TelnetClients	Security Group - Domain ...	Members of this group have acce...
Name	Type	Description																																																																				
Administrator	User	Built-in account for administering ...																																																																				
Cert Publishers	Security Group - Domain ...	Members of this group are permit...																																																																				
DHCP Administrators	Security Group - Domain ...	Members who have administrativ...																																																																				
DHCP Users	Security Group - Domain ...	Members who have view-only acc...																																																																				
DnsAdmins	Security Group - Domain ...	DNS Administrators Group																																																																				
DnsUpdateProxy	Security Group - Global	DNS clients who are permitted to ...																																																																				
Domain Admins	Security Group - Global	Designated administrators of the ...																																																																				
	Security Group - Global	All workstations and servers joine...																																																																				
	Security Group - Global	All domain controllers in the domain																																																																				
	Security Group - Global	All domain guests																																																																				
	Security Group - Global	All domain users																																																																				
	Security Group - Global	Designated administrators of the ...																																																																				
	Security Group - Global	Members in this group can modify...																																																																				
	Security Group - Global	Built-in account for guest access ...																																																																				
	Security Group - Domain ...	Group for the Help and Support C...																																																																				
	Security Group - Domain ...	IIS Worker Process Group																																																																				
IUSR_SVR.10	User	Built-in account for anonymous a...																																																																				
IWAM_SVR.10	User	Built-in account for Internet Infor...																																																																				
RAS and IAS Servers	Security Group - Domain ...	Servers in this group can access r...																																																																				
Schema Admins	Security Group - Global	Designated administrators of the ...																																																																				
SUPPORT_388945a0	User	This is a vendor's account for the...																																																																				
TelnetClients	Security Group - Domain ...	Members of this group have acce...																																																																				

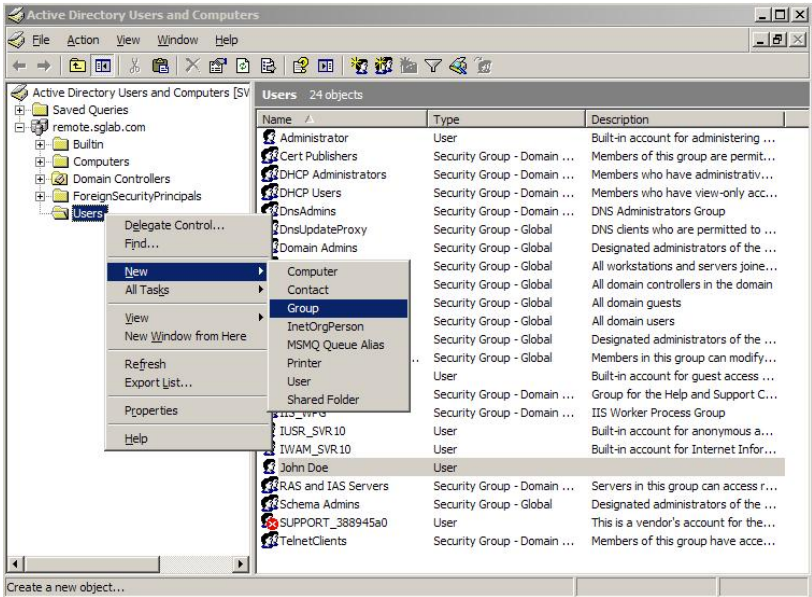
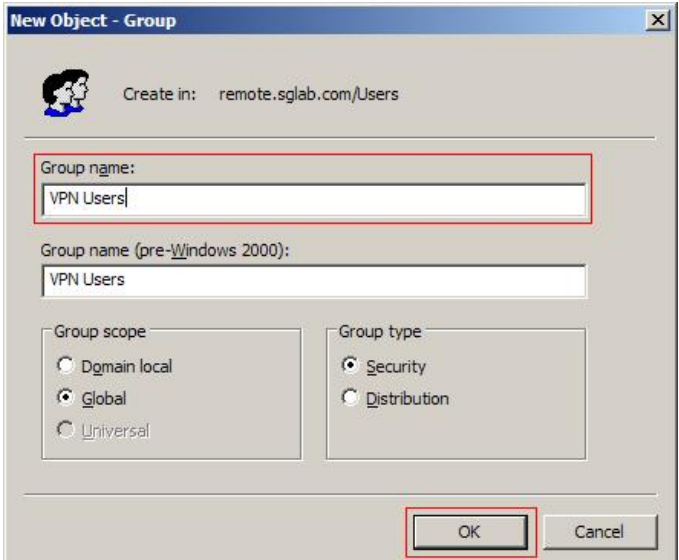
Step	Description
2.	<p>Enter the user information as highlighted below. All remaining fields may be left as the defaults. Click <b>Next</b> to continue.</p> 
3.	<p>Enter the password and the password policy options shown below. Click <b>Next</b> to continue then click <b>Finish</b> (not shown).</p> 

Step	Description
4.	<p>To allow the new account to request authentication when connecting via VPN to the Samsung iBG3026, the account's remote access permission must be enabled. From the <b>Active Directory Users and Computers</b> screen, right click the user name created in Step 2 under the <b>Users</b> folder and select <b>Properties</b> from the pop-up menu.</p>  <p>The screenshot shows the 'Active Directory Users and Computers' console. The left pane shows the tree structure with 'Users' selected. The right pane lists 24 objects, including 'John Doe' (User). A context menu is open over 'John Doe', with 'Properties' highlighted. The status bar at the bottom reads 'Opens the properties dialog box for the current selection.'</p>

5.	<p>Select the <b>Dial-in</b> tab and then select the <b>Allow access</b> option. All remaining fields can be left as the defaults. Click <b>OK</b> to save.</p>  <p>The screenshot shows the 'John Doe Properties' dialog box with the 'Dial-in' tab selected. Under 'Remote Access Permission (Dial-in or VPN)', the 'Allow access' radio button is selected. Other options include 'Deny access' and 'Control access through Remote Access Policy'. Under 'Callback Options', 'No Callback' is selected. The 'OK' button is highlighted with a red box.</p>
----	---

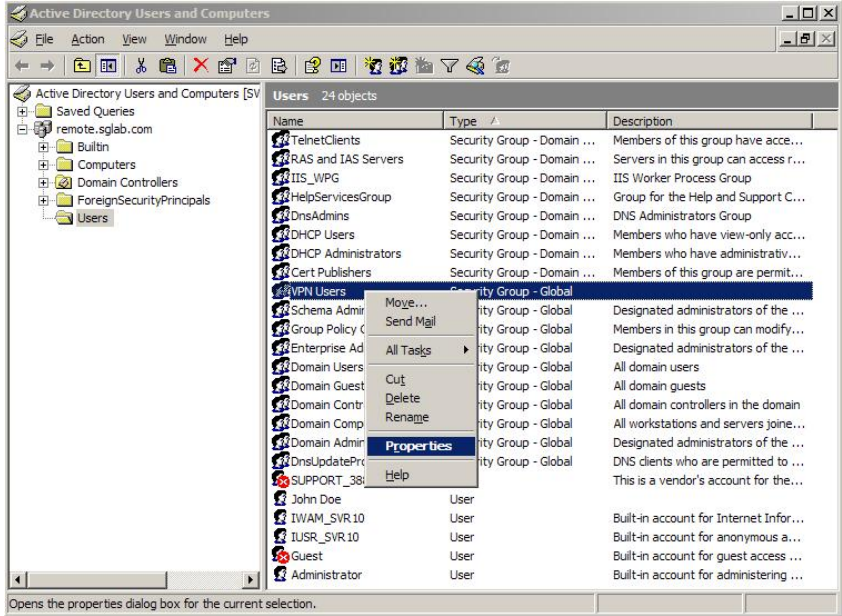
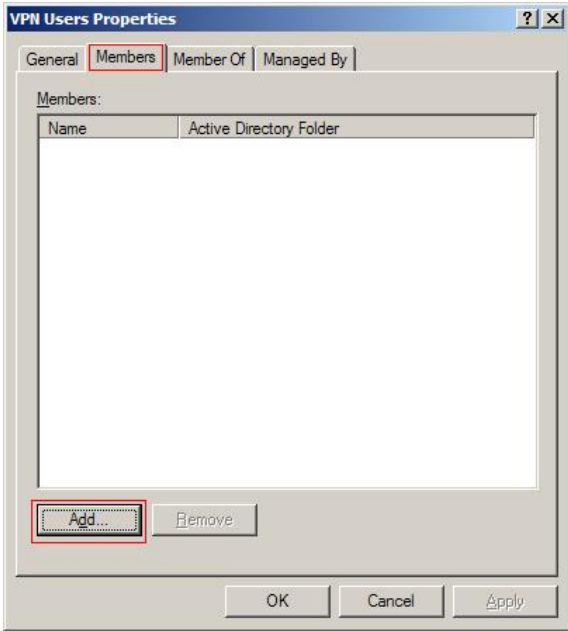
## 5.2. Create User Group

The steps below create a new user group to allow all Juniper NetScreen-Remote user accounts to be grouped together and allow Microsoft IAS to apply a consistent access policy.

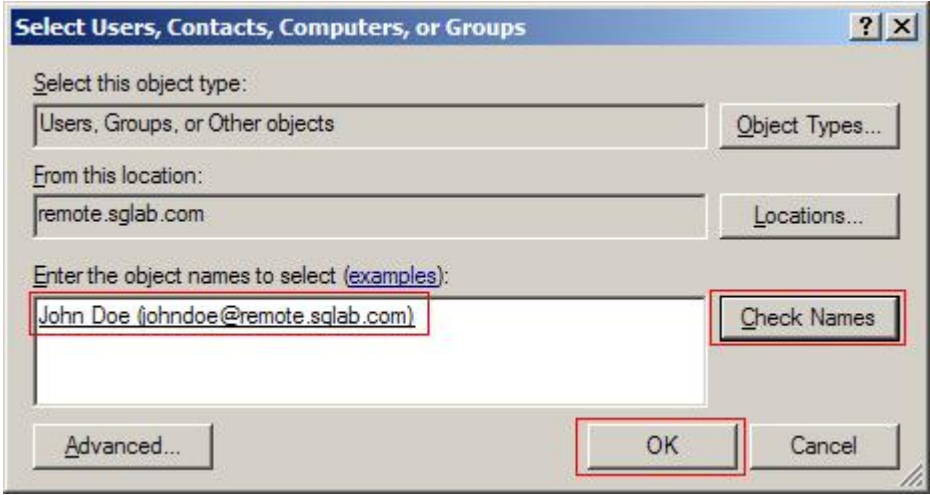
Step	Description
1.	<p>From the <b>Active Directory Users and Computers</b> screen, right click the <b>Users</b> folder and select the <b>New &gt; Group</b> from the pop-up menu as shown below.</p>  <p>The screenshot shows the 'Active Directory Users and Computers' window for the 'remote.sglab.com' domain. The 'Users' folder is selected in the left-hand tree view. A context menu is open over the 'Users' folder, with the 'New' option selected. A sub-menu is displayed, showing 'Group' as the selected option. The main window displays a list of 24 objects in the 'Users' folder, including Administrator, Cert Publishers, DHCP Administrators, and various security groups.</p>
2.	<p>Enter a descriptive name for <b>Group name</b> field as highlighted below. All remaining fields may be left as the defaults. Click <b>OK</b>.</p>  <p>The screenshot shows the 'New Object - Group' dialog box. The 'Create in' field is set to 'remote.sglab.com/Users'. The 'Group name' field is highlighted with a red box and contains the text 'VPN Users'. The 'Group name (pre-Windows 2000)' field also contains 'VPN Users'. Under 'Group scope', the 'Global' radio button is selected. Under 'Group type', the 'Security' radio button is selected. The 'OK' button is highlighted with a red box.</p>

### 5.3. Add Users to Group

The steps below add the newly created user to the newly created user group.

Step	Description
1.	<p>Edit the properties of the new user group by right clicking the group name under the <b>Users</b> folder. Select <b>Properties</b> from the pop-up menu.</p>  <p>The screenshot shows the 'Active Directory Users and Computers' console tree with 'Users' expanded. The 'VPN Users' group is selected, and a context menu is open with 'Properties' highlighted. The main pane shows a list of users and groups with columns for Name, Type, and Description.</p>
2.	<p>Select the <b>Members</b> tab then click <b>Add</b>.</p>  <p>The screenshot shows the 'VPN Users Properties' dialog box. The 'Members' tab is selected, and the 'Add...' button is highlighted with a red box. The 'Members' list is currently empty.</p>

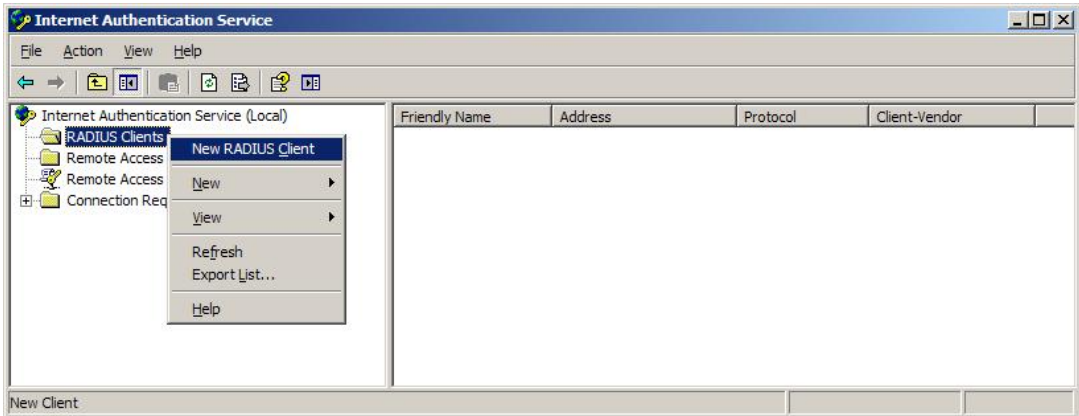


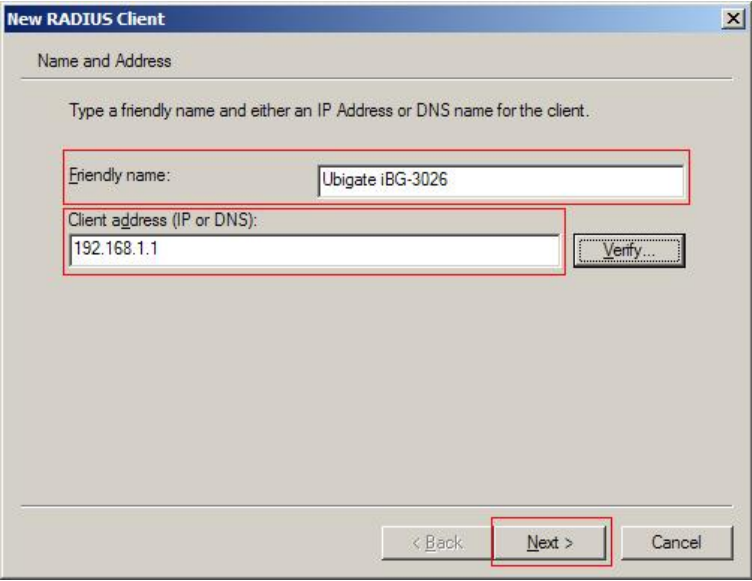
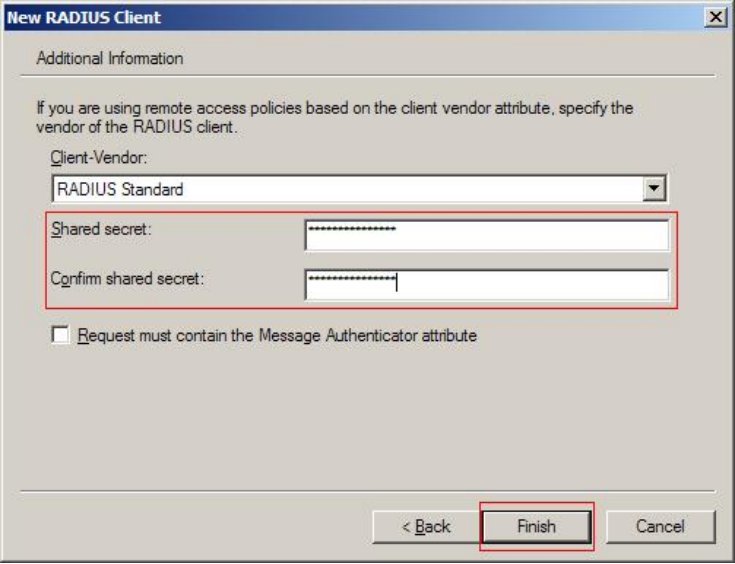
Step	Description
3.	<p>Enter the user name then click <b>Check Names</b>. The user should appear as shown below. Click <b>OK</b> to save. Then click <b>OK</b> again (not shown) to exit the <b>Group Properties</b> screen.</p> 

## 6. Configure Microsoft Internet Authentication Service

The steps below add the Samsung iBG3026 to the Microsoft IAS as a Remote Authentication Dial In User Service (RADIUS) client. This enables Microsoft IAS to exchange RADIUS messages with the Samsung iBG3026. These Application Notes assume the Microsoft IAS is installed and operational.

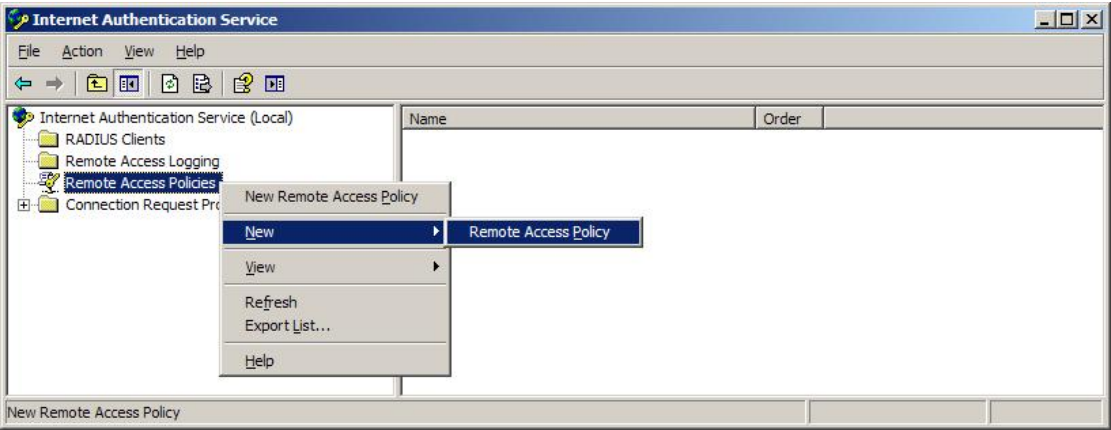
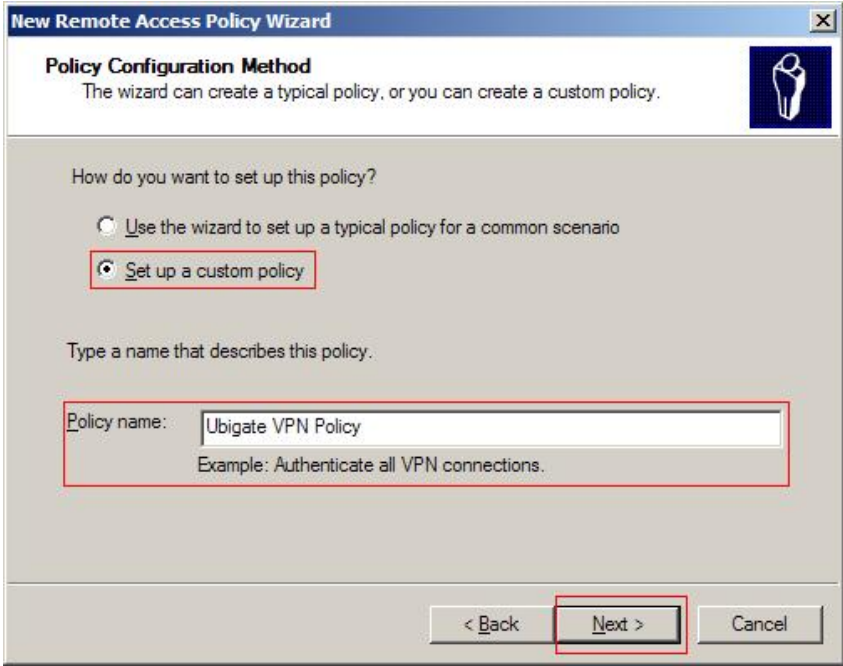
### 6.1. Add RADIUS Client

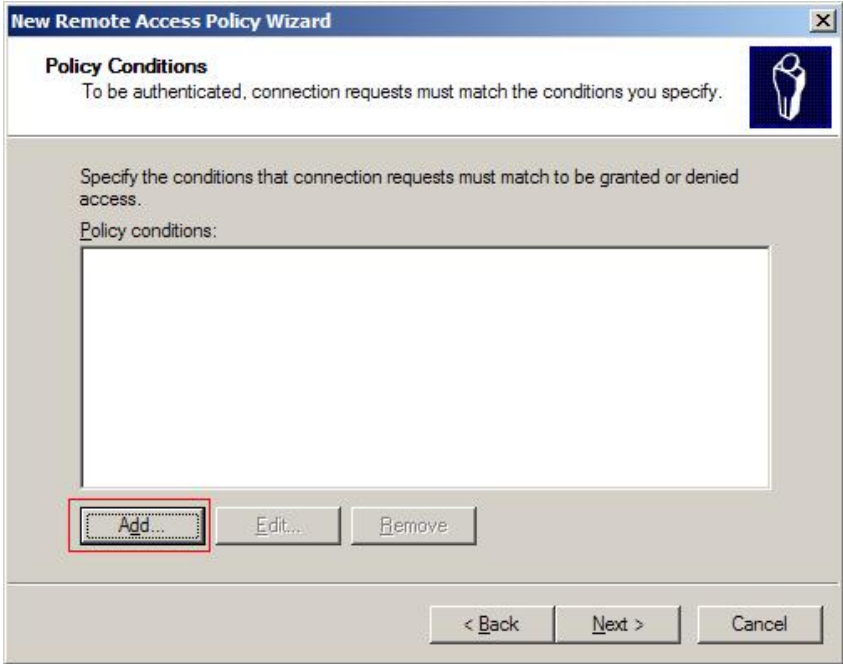
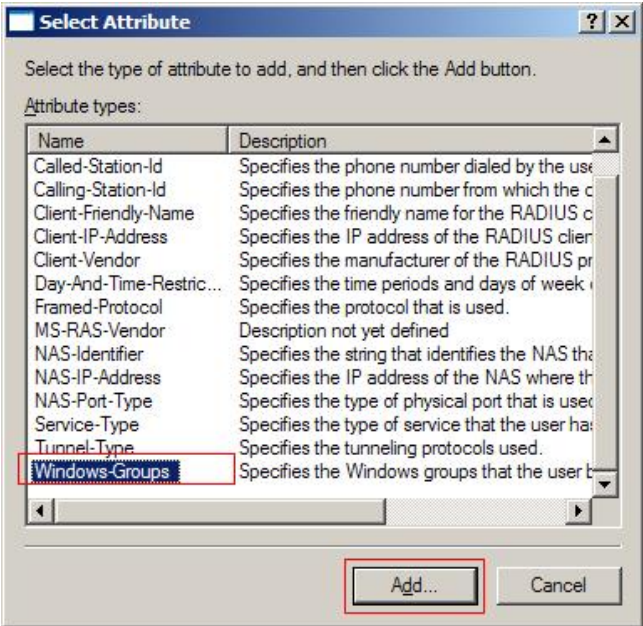
Step	Description
1.	<p>Open the <b>Internet Authentication Service</b> application by selecting <b>Start &gt; All Programs &gt; Administrative Tools &gt; IAS</b>. Right click <b>RADIUS Clients</b> and select <b>New Radius Client</b> from the pop-up menu as shown below.</p> 

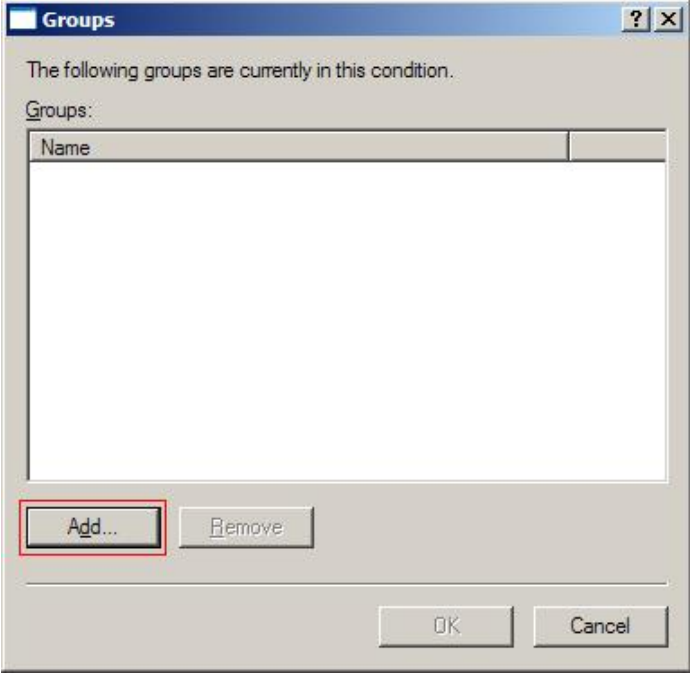
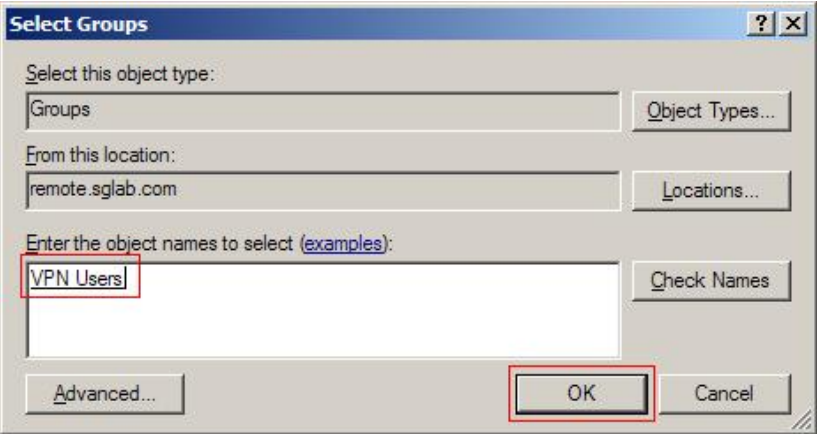
Step	Description
2.	<p>Enter a descriptive name for <b>Friendly name</b> and the IP address of the Samsung iBG3026 for <b>Client address (IP or DNS)</b>. Click <b>Next</b> to continue.</p> 
3.	<p>Enter a text string for <b>Shared secret</b>. In this configuration, the string is <i>radiussecretkey</i>. This shared secret text is used by the Samsung iBG3026 in Section 6.2 to authenticate with the Microsoft IAS for RADIUS communications. All remaining fields may be left as the defaults. Click <b>Finish</b>.</p> 

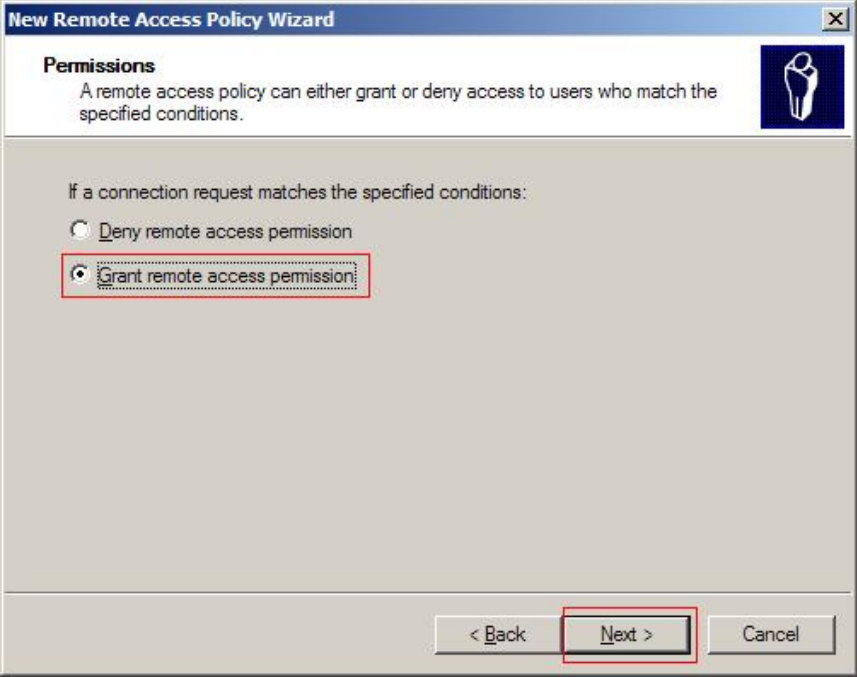
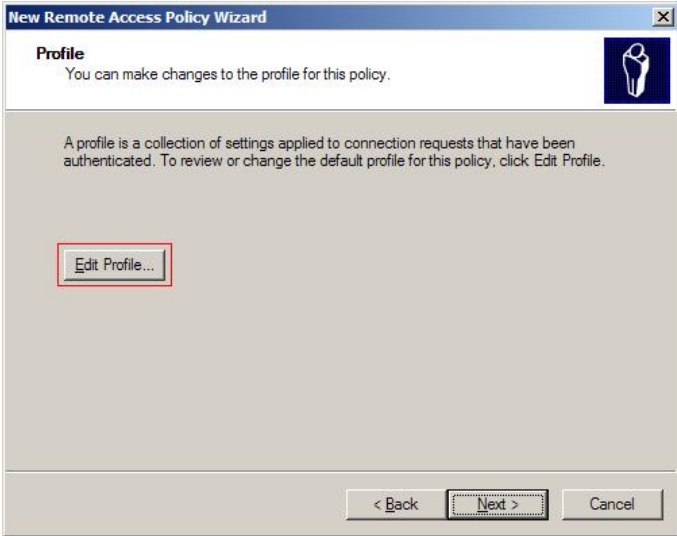
## 6.2. Configure Remote Access Policy

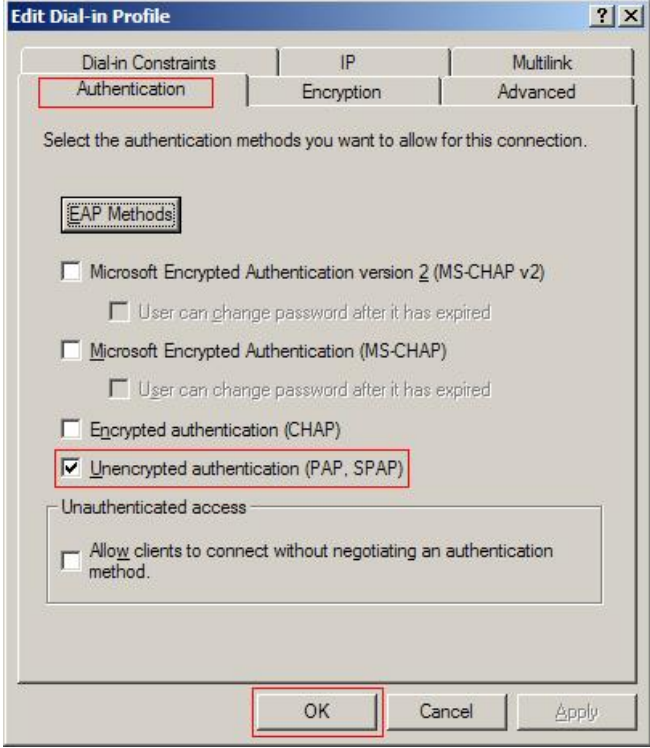
The steps below create a new access policy to be used for RADIUS requests coming from the Samsung iBG3026 on behalf of NetScreen-Remote users.

Step	Description
1.	<p>From the <b>Internet Authentication Service</b> screen, right click <b>Remote Access Policies</b> and select <b>New &gt; Remote Access Policy</b> from the pop-up menu.</p>  <p>The screenshot shows the 'Internet Authentication Service' console window. The left pane displays a tree view with 'Remote Access Policies' selected. A context menu is open over this folder, showing options: 'New Remote Access Policy', 'New', 'View', 'Refresh', 'Export List...', and 'Help'. The 'New' option is expanded, and 'Remote Access Policy' is highlighted.</p>
2.	<p>From the <b>New Remote Access Policy Wizard</b> screen, select <b>Set up a custom policy</b> and enter a descriptive name for <b>Policy name</b>. Click <b>Next</b> to continue.</p>  <p>The screenshot shows the 'New Remote Access Policy Wizard' dialog box. Under 'Policy Configuration Method', the radio button for 'Set up a custom policy' is selected and highlighted with a red box. Below, the 'Policy name' field contains 'Ubigate VPN Policy' and is also highlighted with a red box. The 'Next &gt;' button at the bottom is highlighted with a red box.</p>

Step	Description																														
3.	<p>From the <b>Policy Conditions</b> screen, click <b>Add</b>.</p>  <p>The screenshot shows the 'New Remote Access Policy Wizard' dialog box. The title bar reads 'New Remote Access Policy Wizard'. The main area is titled 'Policy Conditions' and contains the text: 'To be authenticated, connection requests must match the conditions you specify.' Below this, it says 'Specify the conditions that connection requests must match to be granted or denied access.' and 'Policy conditions:'. A large empty rectangular box is provided for listing conditions. At the bottom, there are three buttons: 'Add...', 'Edit...', and 'Remove'. The 'Add...' button is highlighted with a red rectangular box. At the very bottom of the dialog are three navigation buttons: '&lt; Back', 'Next &gt;', and 'Cancel'.</p>																														
4.	<p>From the <b>Select Attribute</b> screen, select the attribute types to be applied to this access policy. The <b>Windows-Groups</b> attribute is used in the sample configuration. Select <b>Windows-Groups</b> and click <b>Add</b>.</p>  <p>The screenshot shows the 'Select Attribute' dialog box. The title bar reads 'Select Attribute'. The main area contains the text: 'Select the type of attribute to add, and then click the Add button.' Below this, it says 'Attribute types:'. A list box contains a table of attribute types. The 'Windows-Groups' attribute is selected and highlighted with a blue background. The 'Add...' button at the bottom is highlighted with a red rectangular box.</p> <table border="1" data-bbox="558 1268 1154 1667"> <thead> <tr> <th>Name</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Called-Station-Id</td> <td>Specifies the phone number dialed by the user.</td> </tr> <tr> <td>Calling-Station-Id</td> <td>Specifies the phone number from which the call originates.</td> </tr> <tr> <td>Client-Friendly-Name</td> <td>Specifies the friendly name for the RADIUS client.</td> </tr> <tr> <td>Client-IP-Address</td> <td>Specifies the IP address of the RADIUS client.</td> </tr> <tr> <td>Client-Vendor</td> <td>Specifies the manufacturer of the RADIUS client.</td> </tr> <tr> <td>Day-And-Time-Restriction</td> <td>Specifies the time periods and days of week when access is allowed.</td> </tr> <tr> <td>Framed-Protocol</td> <td>Specifies the protocol that is used.</td> </tr> <tr> <td>MS-RAS-Vendor</td> <td>Description not yet defined.</td> </tr> <tr> <td>NAS-Identifier</td> <td>Specifies the string that identifies the NAS that is used.</td> </tr> <tr> <td>NAS-IP-Address</td> <td>Specifies the IP address of the NAS where the user is connecting.</td> </tr> <tr> <td>NAS-Port-Type</td> <td>Specifies the type of physical port that is used.</td> </tr> <tr> <td>Service-Type</td> <td>Specifies the type of service that the user has.</td> </tr> <tr> <td>Tunnel-Type</td> <td>Specifies the tunneling protocols used.</td> </tr> <tr> <td>Windows-Groups</td> <td>Specifies the Windows groups that the user belongs to.</td> </tr> </tbody> </table>	Name	Description	Called-Station-Id	Specifies the phone number dialed by the user.	Calling-Station-Id	Specifies the phone number from which the call originates.	Client-Friendly-Name	Specifies the friendly name for the RADIUS client.	Client-IP-Address	Specifies the IP address of the RADIUS client.	Client-Vendor	Specifies the manufacturer of the RADIUS client.	Day-And-Time-Restriction	Specifies the time periods and days of week when access is allowed.	Framed-Protocol	Specifies the protocol that is used.	MS-RAS-Vendor	Description not yet defined.	NAS-Identifier	Specifies the string that identifies the NAS that is used.	NAS-IP-Address	Specifies the IP address of the NAS where the user is connecting.	NAS-Port-Type	Specifies the type of physical port that is used.	Service-Type	Specifies the type of service that the user has.	Tunnel-Type	Specifies the tunneling protocols used.	Windows-Groups	Specifies the Windows groups that the user belongs to.
Name	Description																														
Called-Station-Id	Specifies the phone number dialed by the user.																														
Calling-Station-Id	Specifies the phone number from which the call originates.																														
Client-Friendly-Name	Specifies the friendly name for the RADIUS client.																														
Client-IP-Address	Specifies the IP address of the RADIUS client.																														
Client-Vendor	Specifies the manufacturer of the RADIUS client.																														
Day-And-Time-Restriction	Specifies the time periods and days of week when access is allowed.																														
Framed-Protocol	Specifies the protocol that is used.																														
MS-RAS-Vendor	Description not yet defined.																														
NAS-Identifier	Specifies the string that identifies the NAS that is used.																														
NAS-IP-Address	Specifies the IP address of the NAS where the user is connecting.																														
NAS-Port-Type	Specifies the type of physical port that is used.																														
Service-Type	Specifies the type of service that the user has.																														
Tunnel-Type	Specifies the tunneling protocols used.																														
Windows-Groups	Specifies the Windows groups that the user belongs to.																														

Step	Description
5.	<p>Click <b>Add</b> to add a new group.</p> 
6.	<p>The Active Directory Users group created in Section 5.2 is added to this access policy as shown below. Click <b>OK</b> twice to return to the <b>Policy Conditions</b> screen in Step 3 and then click <b>Next</b> to continue.</p> 

Step	Description
7.	<p>Select <b>Grant remote access permission</b> and click <b>Next</b> to continue.</p>  <p>The screenshot shows a window titled "New Remote Access Policy Wizard" with a "Permissions" section. It explains that a remote access policy can either grant or deny access. Below this, it asks "If a connection request matches the specified conditions:" and provides two radio button options: "Deny remote access permission" (unselected) and "Grant remote access permission" (selected and highlighted with a red box). At the bottom of the window, there are three buttons: "&lt; Back", "Next &gt;" (highlighted with a red box), and "Cancel".</p>
8.	<p>Click <b>Edit Profile</b>.</p>  <p>The screenshot shows a window titled "New Remote Access Policy Wizard" with a "Profile" section. It states "You can make changes to the profile for this policy." and explains that a profile is a collection of settings applied to connection requests. It instructs the user to "click Edit Profile" to review or change the default profile. A button labeled "Edit Profile..." is highlighted with a red box. At the bottom of the window, there are three buttons: "&lt; Back", "Next &gt;" (highlighted with a red box), and "Cancel".</p>

Step	Description
9.	<p>In the <b>Authentication</b> tab, ensure that the field <b>Unencrypted authentication (PAP, SPAP)</b> is checked. All other authentication methods can be unchecked. Click <b>OK</b> to return to the screen in Step 7, followed by <b>Next</b> and then <b>Finished</b> (not shown) to complete the wizard.</p> 

## 7. Configure Samsung iBG3026

The Samsung iBG3026 provides both browser-based and command-line-based (telnet or console port access) administrative interfaces. However, since the full range of necessary configuration features is supported only via the command line interface (CLI), the steps in this section use only the CLI.

## 7.1. Configure Ethernet and VLAN Interfaces

Step	Description
1.	<p>Connect to the Samsung iBG3026 command line interface via a terminal emulation program (e.g., HyperTerminal) using the serial cable provided for the console port at the back of the machine. Enter the username (samsung) and default password (see [4]) to log in. Enter <b>configure terminal</b> to access the configure mode.</p> <pre data-bbox="269 495 1429 814"> #----- # SAMSUNG ELECTRONICS CO., LTD. Login #-----  login: <b>samsung</b> password:                                  SAMSUNG ELECTRONICS CO., LTD. CLI sarak2# <b>configure terminal</b>  sarak2/configure#</pre>
2.	<p>Configure the ethernet 0/2 as an <b>untrusted</b> interface to connect to the public WAN.</p> <pre data-bbox="269 926 1429 1104"> sarak2/configure# <b>interface ethernet 0/2</b> Configuring existing Ethernet interface sarak2/configure/interface/ethernet (0/2)# <b>ip address 2.2.2.1/24</b> sarak2/configure/interface/ethernet (0/2)# <b>crypto untrusted</b> sarak2/configure/interface/ethernet (0/2)# <b>exit</b> sarak2/configure#</pre>
3.	<p>Create a VLAN for the Ethernet ports used by IP telephones and Windows 2003 server and configure the VLAN as a <b>trusted</b> interface. The configuration below is shown for Ethernet ports 1/18 and 1/19. Repeat the steps as necessary to configure other Ethernet ports.</p> <pre data-bbox="269 1331 1429 1818"> sarak2/configure# <b>vlan database</b> sarak2/configure/vlan/database# <b>vlan 101 bridge 1 name Remote</b> sarak2/configure/vlan/database# <b>exit</b> sarak2/configure# <b>interface vlan vlan1.101</b> sarak2/configure/interface/vlan vlan1.101# <b>ip address 192.168.1.1 255.255.255.0</b> sarak2/configure/interface/vlan vlan1.101# <b>crypto trusted</b> sarak2/configure/interface/vlan vlan1.101# <b>exit</b> sarak2/configure# <b>interface ethernet 1/18</b> Configuring existing Ethernet interface sarak2/configure/interface/ethernet (1/18)# <b>switchport mode access</b> sarak2/configure/interface/ethernet (1/18)# <b>switchport access vlan 101</b> sarak2/configure/interface/ethernet (1/18)# <b>exit</b> sarak2/configure# <b>interface ethernet 1/19</b> Configuring existing Ethernet interface sarak2/configure/interface/ethernet (1/19)# <b>switchport mode access</b> sarak2/configure/interface/ethernet (1/19)# <b>switchport access vlan 101</b> sarak2/configure/interface/ethernet (1/19)# <b>exit</b> sarak2/configure#</pre>



Step	Description
4.	Add a default route to the router on the public Internet.
	<pre>sarak2/configure# ip route 0.0.0.0/0 2.2.2.254 sarak2/configure#</pre>

## 7.2. Configure RADIUS

Configure the Samsung iBG3026 as a RADIUS client to the Microsoft IAS for the authentication of remote VPN users.

Step	Description
1.	Configure the Samsung iBG3026 to connect to the Microsoft IAS with the secret key as <i>radiussecretkey</i> .
	<pre>sarak2/configure# aaa sarak2/configure/aaa# radius sarak2/configure/aaa/radius# primary_server 192.168.1.110 sarak2/configure/aaa/radius# src_address 192.168.1.1 sarak2/configure/aaa/radius# shared_key radiussecretkey sarak2/configure/aaa/radius# exit sarak2/configure/aaa# enable sarak2/configure/aaa# exit sarak2/configure#</pre>

### 7.3. Configure VPN Remote Access Policy

Create the VPN Remote Access Policy to support remote users.

Step	Description
1.	<p>Configure dynamic Phase 1 IKE policy for a group of remote users. The pre-shared key is set to <i>interoptest</i> in this configuration. For dynamic policy, set the <b>mode</b> to <i>aggressive</i>. Configure the IKE phase 1 proposal as described in Section 3. Create an address pool for the Samsung iBG3026 to use for assigning IP addresses to Juniper NetScreen-Remote clients when an IPSec tunnel is successfully established. Configure the Samsung iBG3026 to use Password Authentication Protocol (PAP) to authenticate with the Microsoft Internet Authentication Service (RADIUS) for user authentication.</p> <pre> sarak2/configure# crypto sarak2/configure/crypto# dynamic sarak2/configure/crypto/dynamic# ike policy remusers modecfg-group sarak2/configure/crypto/dynamic/ike/policy remusers# local-address 2.2.2.1 sarak2/configure/crypto/dynamic/ike/policy remusers# remote-id domain-name avaya.com Default proposal created with priority1-des-shal-rsa-g1 Default ipsec policy 'remusers' of type modecfg added with proposal priority1- 3des-shal-tunnel sarak2/configure/crypto/dynamic/ike/policy remusers# key interoptest sarak2/configure/crypto/dynamic/ike/policy remusers# mode aggressive sarak2/configure/crypto/dynamic/ike/policy remusers# proposal 1 sarak2/configure/crypto/dynamic/ike/policy remusers/proposal 1# authentication- method pre-shared-key sarak2/configure/crypto/dynamic/ike/policy remusers/proposal 1# dh-group group2 sarak2/configure/crypto/dynamic/ike/policy remusers/proposal 1# encryption- algorithm 3des-cbc sarak2/configure/crypto/dynamic/ike/policy remusers/proposal 1# exit sarak2/configure/crypto/dynamic/ike/policy remusers# client configuration sarak2/configure/crypto/dynamic/ike/policy remusers/client/configuration# address-pool 1 192.168.11.101 192.168.11.120 sarak2/configure/crypto/dynamic/ike/policy remusers/client/configuration# dns- server 192.168.1.110 sarak2/configure/crypto/dynamic/ike/policy remusers/client/configuration# exit sarak2/configure/crypto/dynamic/ike/policy remusers# client authentication sarak2/configure/crypto/dynamic/ike/policy remusers/client/authentication# radius pap sarak2/configure/crypto/dynamic/ike/policy remusers/client/authentication# exit sarak2/configure/crypto/dynamic/ike/policy remusers# exit sarak2/configure/crypto/dynamic# </pre>
2.	<p>Configure dynamic Phase 2 IPSec policy for the same group of remote users. Configure the IPSec phase 2 proposal as described in Section 3.</p>

Step	Description
	<pre>sarak2/configure/crypto# <b>dynamic</b> sarak2/configure/crypto/dynamic# <b>ipsec policy remusers modecfg-group</b> sarak2/configure/crypto/dynamic/ipsec/policy remusers# <b>match address 192.168.1.0/24</b> sarak2/configure/crypto/dynamic/ipsec/policy remusers# <b>proposal 1 esp</b> sarak2/configure/crypto/dynamic/ipsec/policy remusers/proposal 1# <b>encryption-algorithm aes128-cbc</b> sarak2/configure/crypto/dynamic/ipsec/policy remusers/proposal 1# <b>hash-algorithm sha1-hmac</b> sarak2/configure/crypto/dynamic/ipsec/policy remusers/proposal 1# <b>exit</b> sarak2/configure/crypto/dynamic/ipsec/policy remusers# <b>exit</b> sarak2/configure/crypto/dynamic# <b>exit</b> sarak2/configure/crypto# <b>exit</b> sarak2/configure#</pre>

## 7.4. Configure Firewall Policies

Configure the firewall policies to allow traffic between the office network and the remote users.

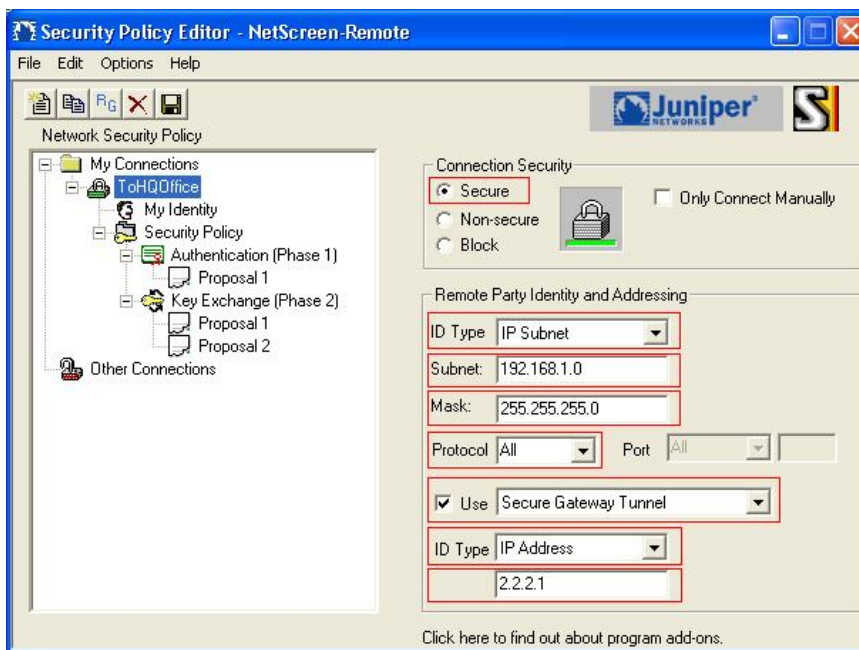
Step	Description
1.	<p>Assign the interfaces to the appropriate firewall map. By default, the Samsung iBG3026 creates two firewall maps:</p> <ul style="list-style-type: none"> <li>• internet – Untrusted interfaces connecting to the public WAN</li> <li>• corp – Trusted interfaces connected to the local LAN</li> </ul> <p>The <b>ethernet0/2</b> interface is assigned to the <b>internet</b> map while the VLAN created in Section 7.1 Step 3 is assigned to the <b>corp</b> map.</p> <pre>sarak2/configure# <b>firewall internet</b> sarak2/configure/firewall internet# <b>interface ethernet0/2</b> sarak2/configure/firewall internet# <b>exit</b> sarak2/configure# <b>firewall corp</b> sarak2/configure/firewall corp# <b>interface vlan1.101</b> sarak2/configure/firewall corp# <b>exit</b> sarak2/configure#</pre>
2.	<p>Configure firewall policies to allow IKE negotiation into the untrusted <b>ethernet0/2</b> interface.</p> <pre>sarak2/configure# <b>firewall internet</b> sarak2/configure/firewall internet# <b>policy 1000 in self</b> sarak2/configure/firewall internet/policy 1000 in# <b>exit</b> sarak2/configure/firewall internet# <b>exit</b> sarak2/configure#</pre>
3.	<p>Configure firewall policies to allow the remote users to access the office network. The remote users are assigned with the IP addresses from the address pool configured in Section 7.3 Step 1.</p>

Step	Description
	<pre>sarak2/configure# firewall corp sarak2/configure/firewall corp# policy 1000 in address 192.168.11.101 192.168.11.120 192.168.1.0 24 sarak2/configure/firewall corp/policy 1000 in# exit sarak2/configure/firewall corp# exit sarak2/configure#</pre>

## 8. Configure Juniper NetScreen-Remote

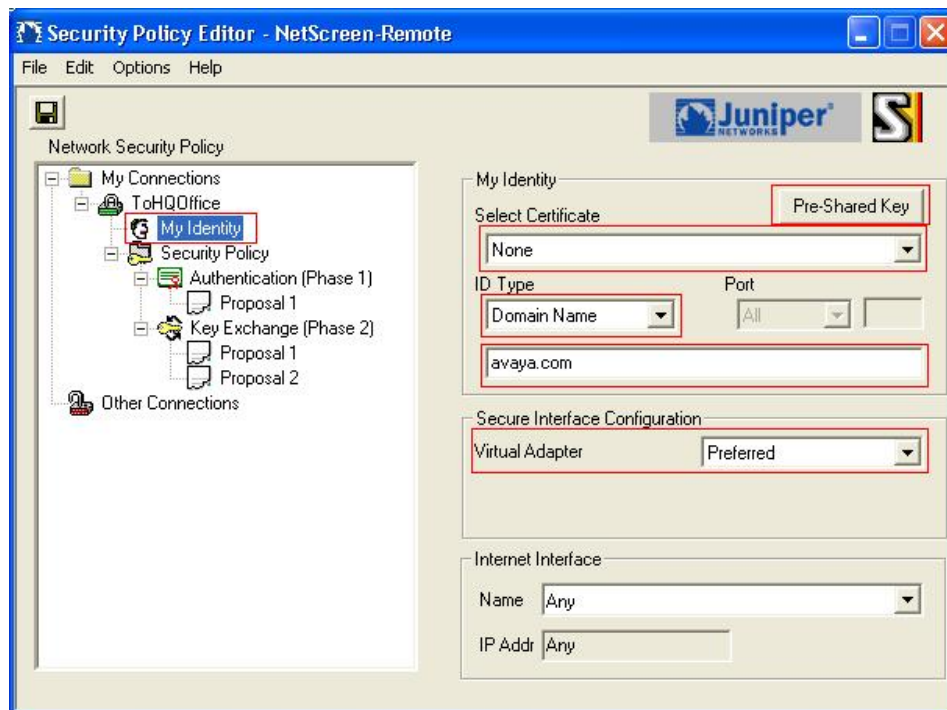
This section shows the configuration of the Juniper NetScreen-Remote on a single remote user machine.

Step	Description
1.	<p>Launch the NetScreen-Remote Security Policy Editor by selecting <b>Start &gt; Programs &gt; NetScreen-Remote &gt; Security Policy Editor</b>. Right click the folder <b>My Connections</b> and select <b>Add &gt; Connection</b> (not shown). Name the new connection as <b>ToHQOffice</b>. Configure the highlighted fields shown below.</p> <ul style="list-style-type: none"> <li>• Select <b>Secure</b> for <b>Connection Security</b>.</li> <li>• Select <b>IP Subnet</b> for <b>ID Type</b>.</li> <li>• Enter <b>192.168.1.0</b> in the field <b>Subnet</b> and <b>255.255.255.0</b> in the field <b>Mask</b>.</li> <li>• Check the <b>Use</b> box.</li> <li>• Select <b>All</b> in the <b>Protocol</b> field and <b>Secure Gateway Tunnel</b> in the <b>Use</b> field.</li> <li>• Select <b>IP Address</b> in the field <b>ID Type</b> and enter <b>2.2.2.1</b> (IP address of the Samsung iBG3026 public interface) as the tunnel endpoint IP address.</li> </ul>

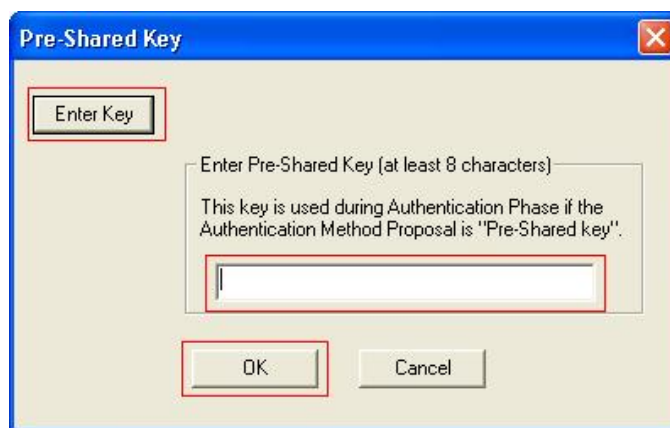


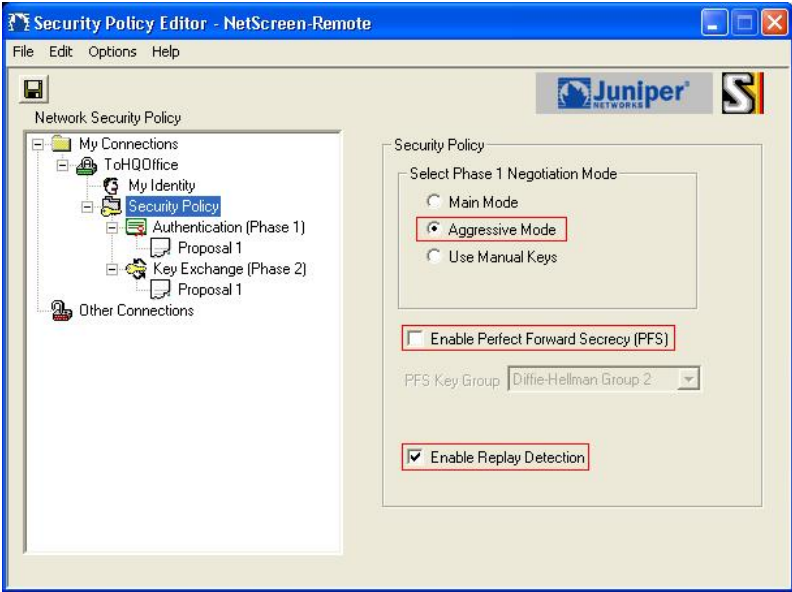
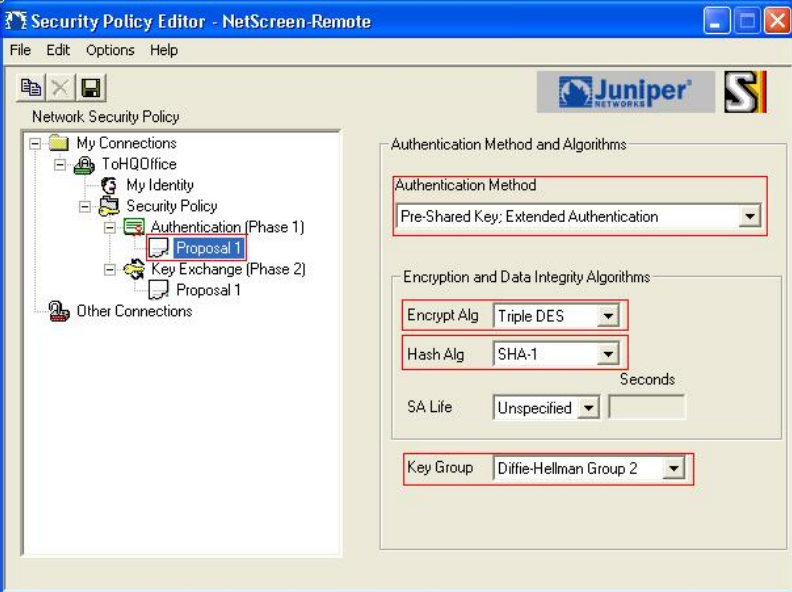
Step	Description
------	-------------

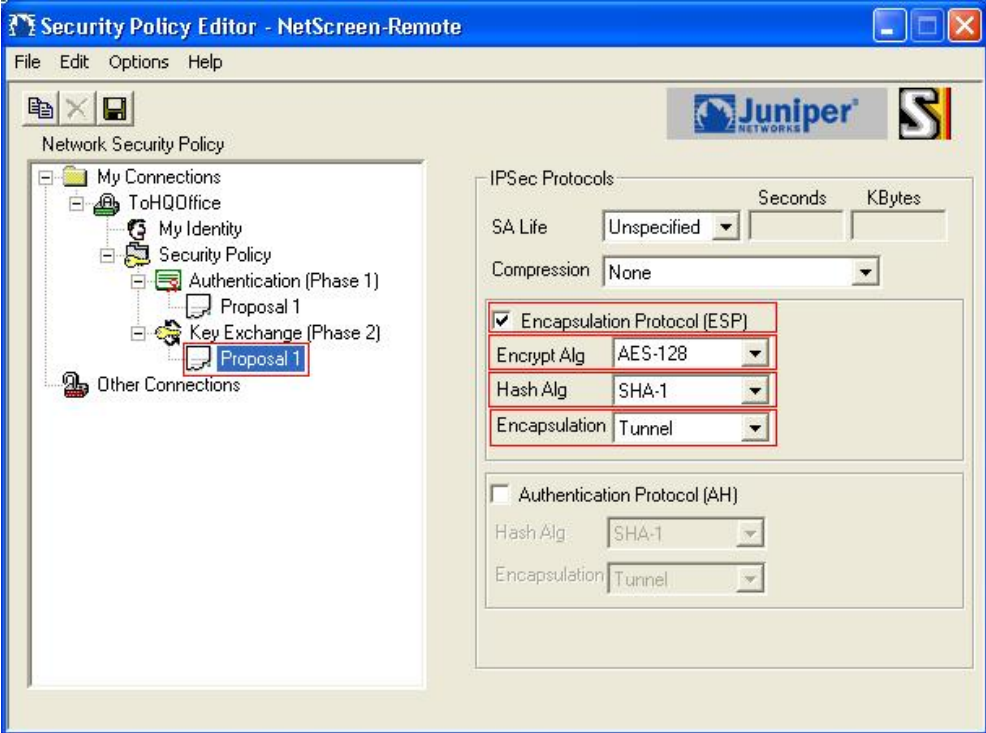
- |    |   |
|----|---|
| 2. | <p>Expand the <b>ToHQOffice</b> folder and select <b>My Identity</b>. Configure the highlighted fields shown below. Select <b>Domain Name</b> for <b>ID Type</b> field and enter <b>avaya.com</b>. Select <b>Preferred</b> for <b>Virtual Adapter</b> field. All remaining fields can be left as the defaults. Click <b>Pre-Shared Key</b> to continue.</p> |
|----|---|



- |    |  |
|----|--|
| 3. | <p>Click <b>Enter Key</b> and type the Pre-Shared Key <b>interoptest</b>. Click <b>OK</b>.</p> |
|----|--|



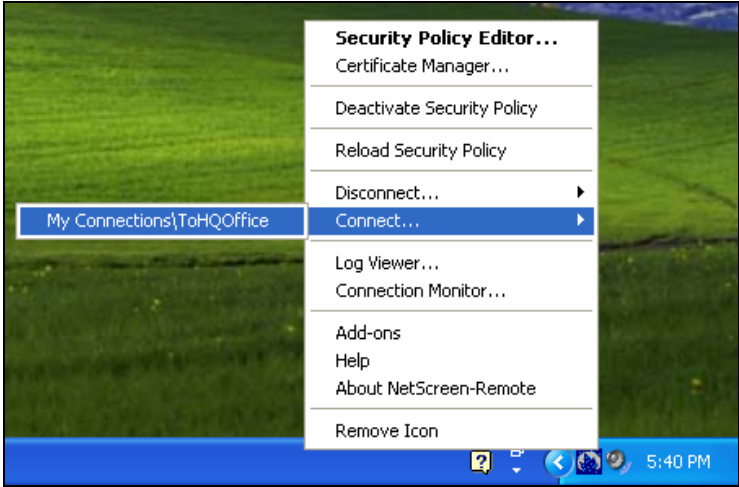
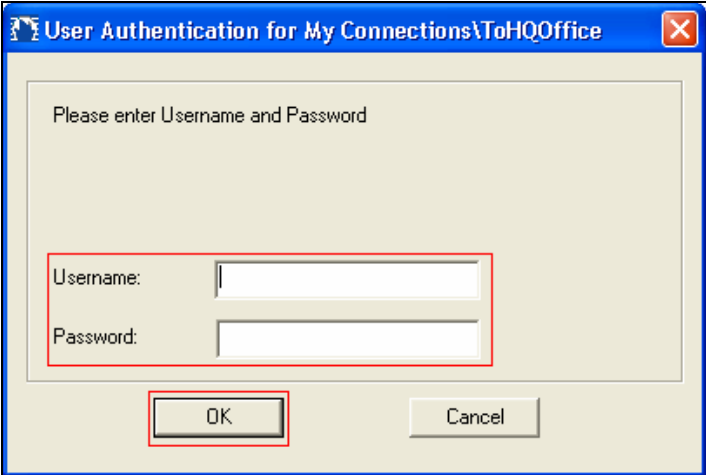
Step	Description
4.	<p>Select <b>Security Policy</b>. Configure the highlighted fields shown below. Select <b>Aggressive Mode</b> for <b>Select Phase 1 Negotiation Mode</b>. Uncheck <b>Enable Perfect Forward Secrecy (PFS)</b>. Check <b>Enable Replay Detection</b> field.</p> 
5.	<p>Expand folder <b>Security Policy &gt; Authentication (Phase 1)</b> and select <b>Proposal 1</b>. Configure the highlighted fields shown below. Select <b>Pre-Shared Key; Extended Authentication</b> for <b>Authentication Method</b> field. Select <b>Triple DES</b> for <b>Encrypt Alg</b> field, and <b>SHA-1</b> for <b>Hash Alg</b> field. Select <b>Diffie-Hellman Group 2</b> for <b>Key Group</b> field. All remaining fields can be left as the defaults.</p> 

Step	Description
6.	<p>Expand folder <b>Security Policy &gt; Key Exchange (Phase 2)</b> and select <b>Proposal 1</b>. Configure the highlighted fields shown below. All remaining fields can be left as the defaults.</p> <ul style="list-style-type: none"> <li>• Check <b>Encapsulation Protocol (ESP)</b> field.</li> <li>• Select <b>AES-128</b> for <b>Encrypt Alg</b> field.</li> <li>• Select <b>SHA-1</b> for <b>Hash Alg</b> field.</li> <li>• Select <b>Tunnel</b> for <b>Encapsulation</b> field.</li> </ul> <p>From the menu, select <b>File &gt; Save</b> to save the configuration.</p> 

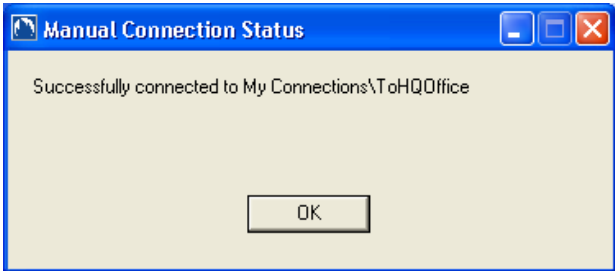
## 9. Verification Steps

The following steps can be used to verify that the configuration steps documented in these Application Notes have been done correctly.

### 9.1. Verify Juniper NetScreen-Remote

Step	Description
1.	<p>Right-click on the NetScreen-Remote icon and select <b>Connect &gt; My Connections\ToHQOffice</b>.</p> 
2.	<p>Enter the username and password created in the Microsoft Active Directory in Section 5.1.</p> 



Step	Description
3.	<p>Verify that the <b>Manual Connection Status</b> screen is displayed and shows that the connection is successful. Launch Avaya IP Softphone and verify that it can register with Avaya Communication Manager successfully.</p> <div style="text-align: center;">  </div>

## 9.2. Verify Samsung iBG3026

### 9.2.1. Verify Client Connections

Enter the command **show crypto dynamic clients** using the Samsung iBG3026 CLI. Verify that the client is connected as shown below.

```
sarak2/configure# show crypto dynamic clients
```

Client Address	Client Id	Policy	Advanced
7.7.7.7	avaya.com	remusers:192.168.11.101	ModcfgGrp-Xauth-Radius

```
sarak2/configure#
```

### 9.2.2. Verify Phase 1 Status

Enter the command **show crypto ike sa all** using the Samsung iBG3026 CLI. Verify that the **State** of the client connection shows **SA\_MATURE**.

```
sarak2/configure# show crypto ike sa all
```

Policy	Peer	State	Bytes	Transform
remusers	7.7.7.7	SA_MATURE	2052	pre-g2-3des-sha1

```
sarak2/configure#
```

### 9.2.3. Verify Phase 2 Status

Enter the command **show crypto ipsec sa all** using the Samsung iBG3026 CLI. Verify that the IPSec policies for the tunnels going to and coming from the Juniper NetScreen-Remote are created.

```
sarak2/configure# show crypto ipsec sa all

Policy      Dest IP      Spi          Packets      Transform
-----      -
INremusers  2.2.2.1     0xbb3d0e65  1121        esp-aes-sha1-tunl
remusers    7.7.7.7     0xea2383bf  1322        esp-aes-sha1-tunl

sarak2/configure#
```

## 10. Conclusion

The Samsung Ubigate™ iBG3026 is able to successfully interoperate with Juniper Networks NetScreen-Remote VPN Client to support remote users running the Avaya IP Softphone.

## 11. Additional References

The following Avaya product documentation is available from <http://support.avaya.com>.

- [1] *Configuring the Samsung Ubigate™ iBG-3026 with Avaya SIP Enablement Services and Avaya Communication Manager*, Issue 1.0, 12 Feb 2007

The following Samsung iBG3026 guides are available from Samsung for registered partner of Samsung Electronics. Visit <http://www.samsungen.com> for company and product information.

- [2] *Samsung Ubigate iBG3026 Configuration Guide*
- [3] *Samsung Ubigate iBG3026 Command Reference*
- [4] *Samsung Ubigate iBG3026 Installation Manual*
- [5] *Samsung Ubigate iBG3026 System Description*
- [6] *Samsung Ubigate iBG3026 Message Reference Manual*

The following Juniper Networks product documentations are available from <http://www.juniper.net/techpubs/>:

- [7] *Juniper Netscreen-Remote VPN Client Administrator's Guide*, Version 8.7, P/N 093-1635-000, Rev. B

---

**©2007 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at [interoplabnotes@list.avaya.com](mailto:interoplabnotes@list.avaya.com)