Configuring a Cisco SA 500 to Accept a VPN Connection from a Shrew Soft VPN Client

The Cisco SA 500 is a small business security router that provides SSL VPN connections and VPN connections through Cisco Quick VPN Client. If a different IPSec client is required for compatibility reasons, you will need to configure the SA 500 to work with a third-party client such as the Shrew Soft VPN Client.

This application note document provides information on how to configure a SA 500 security router to work with the Shrew Soft VPN client.

Contents

Scope and Assumptions

The procedures and guidelines in this Application Note assume that your SA 500 is set up for Internet connectivity and has a basic configuration. It applies to an SA 500 running firmware version 1.1.21 and Shrew Soft Client version 2.1.15. Using different versions might display slightly different screens and configurations that what is described in this document. Administrators working on this system should have a basic working knowledge of IPSec VPNs.

Before proceeding, make sure you know the preshared key, list of users, and user passwords.

Configuring the SA 500 with the VPN Wizard

The SA 500 configuration utility includes a VPN Wizard you use to configure the SA 500. This section describes how to configure the router to allow the Shrew Soft VPN Client to connect to your network with minimal changes to the configuration.

To run the VPN Wizard, you must have administrator access to the SA 500.

Running the Wizard

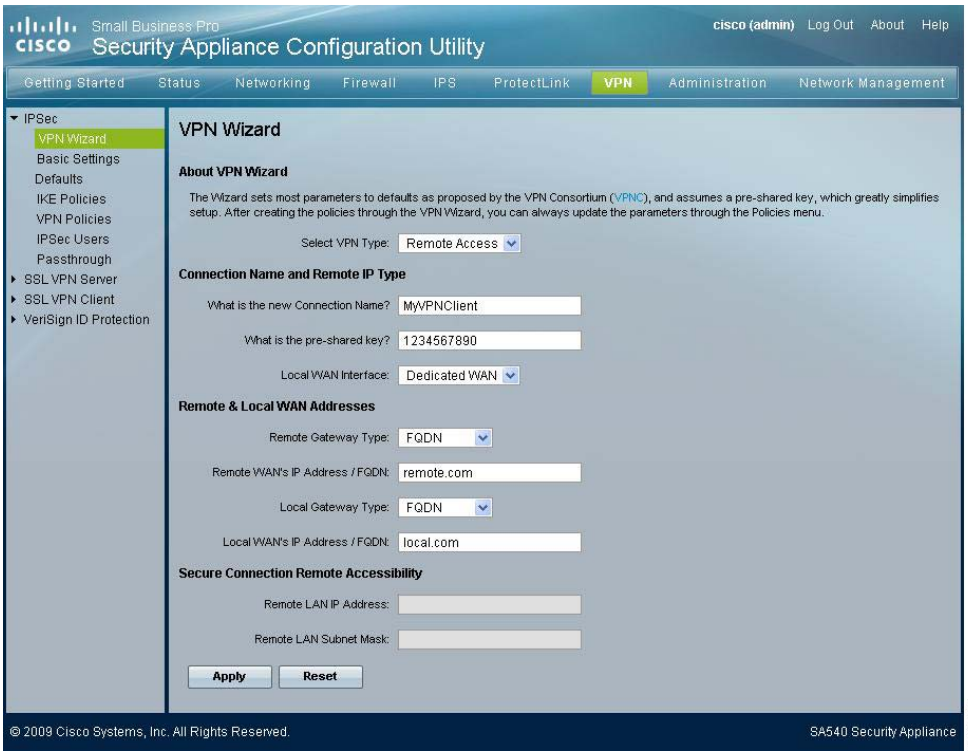
To run the VPN Wizard:

Step 1. To access the wizard, login to the SA 500 as administrator by entering this address: **192.168.75.1.**

Step 2. The default username and password is **cisco/cisco**.

Step 3. Click **VPN** on the menu bar, and then click **IPSec > VPN Wizard** in the navigation tree.

This is an example configuration of the VPN Wizard page.



Step 4. From the Select VPN Type drop-down menu, select **Remote Access**.

Step 5. In the **Connection Name and Remote IP Type** area, enter this information:

- **VPN Connection Name**: Enter a name to help you identify the VPN that you are setting up. For example: MyVPNClient.
- **Preshared Key**: Enter the preshared key for the VPN Clients. For example: 1234567890.

  The length of the preshared key is between 8 characters and 49 characters and must be entered exactly the same on this page and on the client.
- **Local WAN Interface**: From the drop-down menu, select **Dedicated WAN**.

Step 6. In the Remote & Local WAN Addresses area, enter this information:

- **Remote Gateway Type**: From the drop-down menu, select **FQDN**.

  We recommend that you do not select IP address as the gateway type when configuring IPSec clients. This option only allows a single user from that IP address to connect to the network at once.
- **Remote WAN's IP Address/FQDN**: Enter a domain name. For example: remote.com.

  This is an identifier that IPSec uses to verify the identity of the other IPSec device. For this configuration, the identifier is the IPSec client.
- **Local Gateway Type**: From the drop-down menu, select **FQDN** or **IP Address**.

  If you select IP Address, you must configure a static IP address on the SA 500 Dedicated WAN interface.
- **Local WAN's IP Address/FQDN**: Enter a domain name. For example: local.com.

  This is an identifier that IPSec uses to verify this IPSec device. If you selected **IP Address** as the gateway type, you must also enter the WAN IP Address of the Dedicated WAN.

NOTE The domain names that you specify for the Remote and Local WAN IP Address are the same ones that you will use when configuring the client. See "Configuring the Shrew Soft Client" on page 7.

Step 7. Click **Apply** to save your changes. A VPN policy and IKE policy are created.

Changing the IKE Policy

NOTE The name of the IKE policy that you are changing must match the **Connection Name** that you entered on the VPN Wizard page. For example: MyVPNClient.

Follow these steps to change the IKE policy:

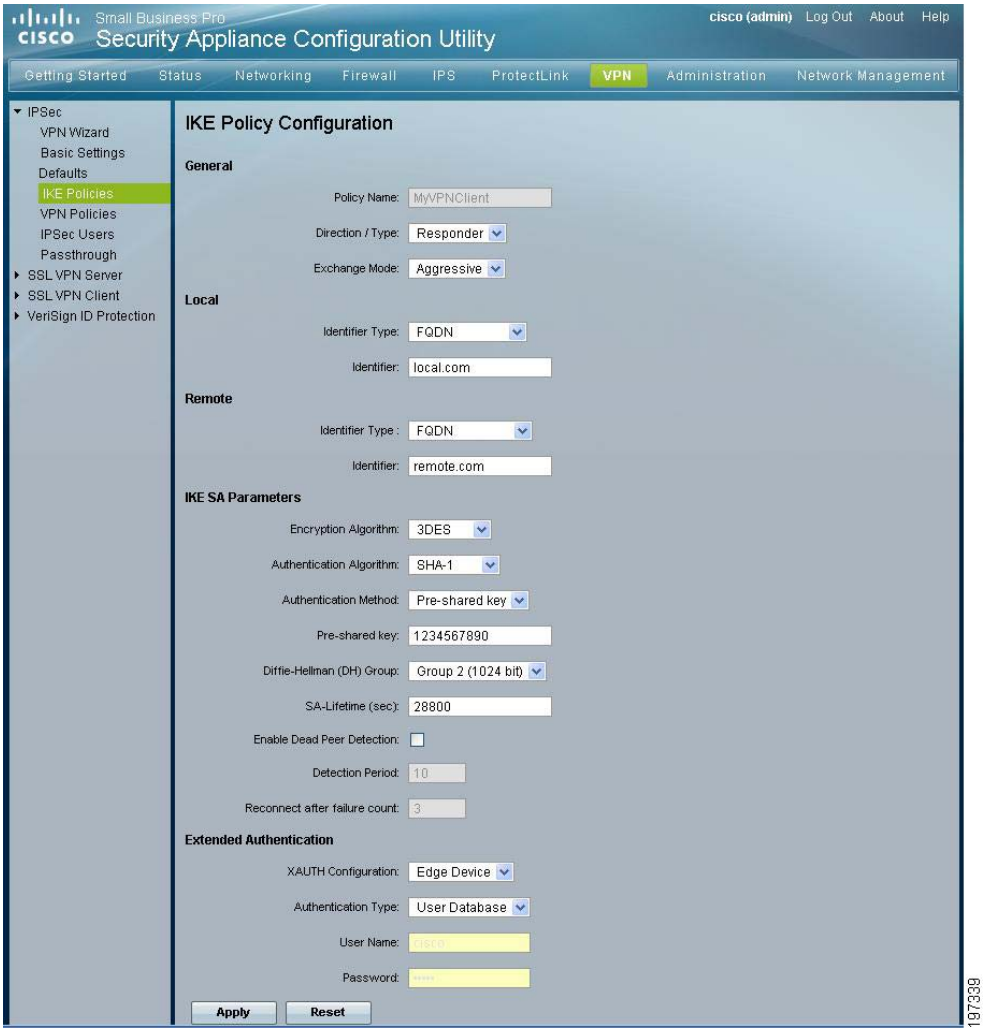
Step 1. Select **VPN Policies** in the navigation tree.

Step 2. Select the newly created policy from the VPN policies table and click **Disable**.

Step 3. Select **IKE Policies** in the navigation tree.

Step 4. Select the newly created policy from the IKE policies table and click the **Edit** button.

The IKE Policy Configuration window appears.



Step 5. In the Extended Authentication area (at the bottom of the page), select **Edge Device** from the XAUTH Configuration drop-down menu.

This option requires individual users to login to the system.

Step 6. From the Authentication Type drop-down menu, select **User Database**.

This option allows the users to authenticate locally to the system. To view the user list, select **IPSec Users** from the navigation tree.

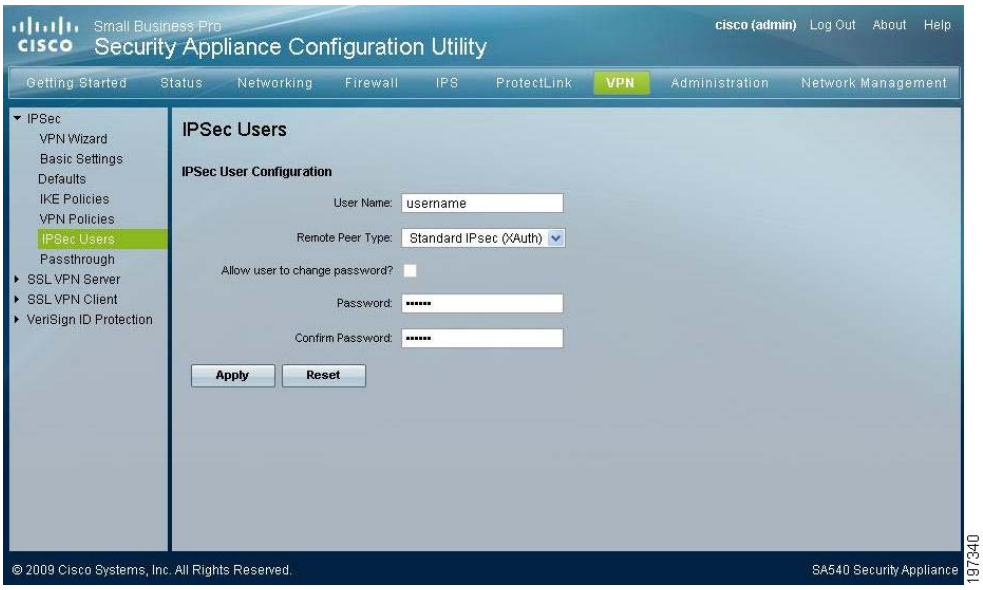
Step 7. Click **Apply** to save your changes.

Adding IPSec Users

Step 1. Select **IPSec Users** in the navigation tree.

Step 2. Click **Add** to add an IPSec VPN user.

The IPSec Users window appears.



Step 3. For **User Name**, enter the name of the user you are adding.

Step 4. From the Remote Peer Type drop-down menu, select **Standard IPSec (XAuth)**.

Step 5. Enter the user password and then confirm it.

Step 6. Click **Apply** to save the user.

Step 7. Select **VPN Policies** in the navigation tree. Select the VPN Policy that you disabled when you changed the IKE Policy and re-enable it.

- If you are only using a single subnet, go to Configuring the Shrew Soft Client, page 7.
- If you need to add more subnets, proceed to the next section, Adding Additional Subnets on the SA 500.

Adding Additional Subnets on the SA 500

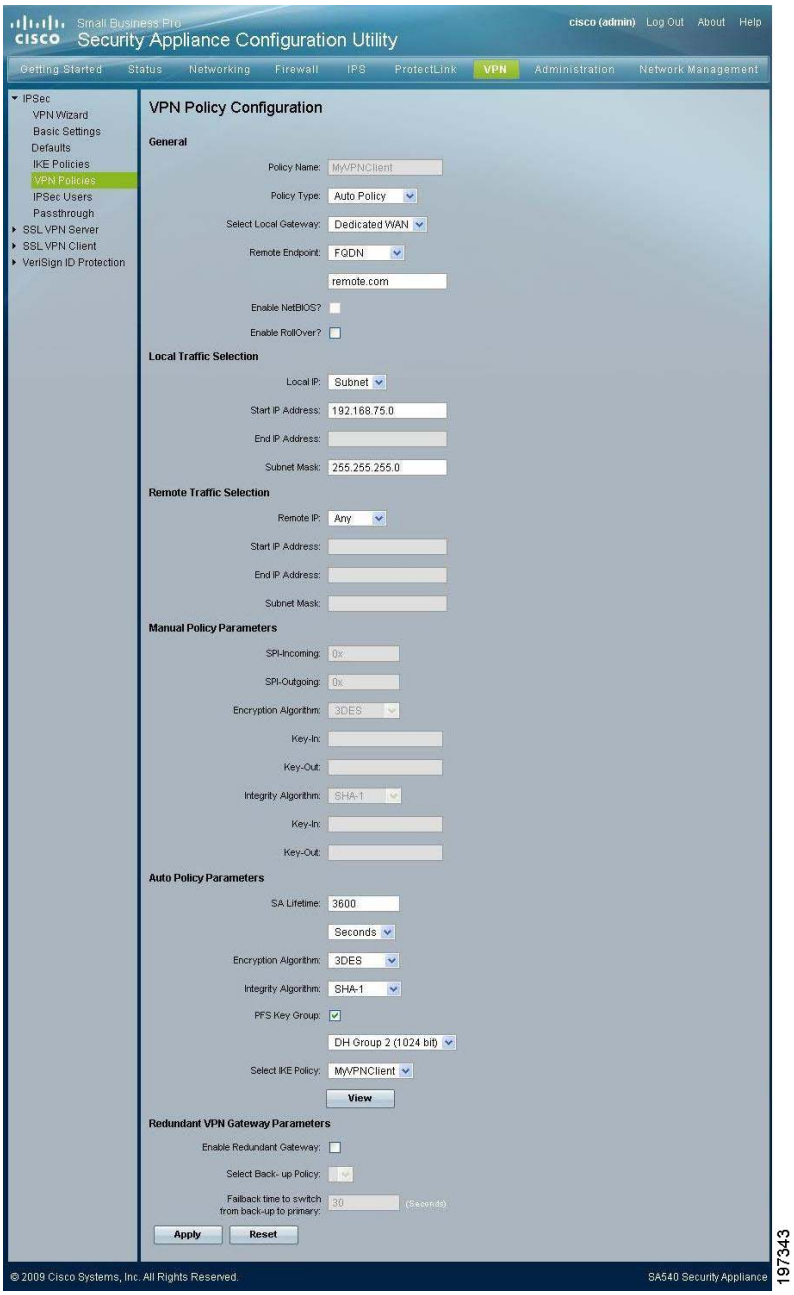
If the SA 500 has additional subnets that are configured as VLANs on the device, or has routes to local subnets, you might want to make these subnets available to the IPSec VPN users. To do so, you must have a list of subnets for users to have access to from the VPN. If different users require access to different subnets, new IKE and VPN Policies are required for different types of access.

To add an additional subnet, you must configure a VPN Policy for that subnet. Each additional subnet will require another VPN Policy.

Step 1. Select **VPN Policies** in the navigation tree.

Step 2. Click **Add** to add another VPN policy.

The VPN Policy Configuration page appears.



Step 3. In the **General** area, enter this information:

- **Policy Name**: Enter the name of the VPN policy.
- **Policy Type**: Select **Auto Policy**.
- **Select Local Gateway**: Select the interface you chose in the VPN Wizard. For example: Dedicated WAN.
- **Remote Endpoint**: Select **FQDN** and enter the domain you specified in the VPN Wizard for the Remote WAN's IP Address/FQDN. For example: remote.com.

Step 4. In the **Local Traffic Selection** area, enter this information:

- **Local IP**: Select **Subnet** from the drop-down menu.

  You can also use other options, such as host. The VPN client must have the same configuration of subnets and hosts that are entered on the VPN Policies.
- **Start IP Address**: Enter the subnet to add to the IPSec VPN. For example: 192.168.75.0.
- **Subnet Mask**: Enter the subnetmask of the subnet you are adding. For example: 255.255.255.0.

Step 5. In the **Remote Traffic Selection** area, select **Any** from the Remote IP drop-down menu.

Step 6. In the **Auto Policy Parameters** area, enter the name of the VPN Client IKE policy that you created in the VPN Wizard. For example: MyVPNClient.

Step 7. Click **Apply** to save your changes.

Configuring the Shrew Soft Client

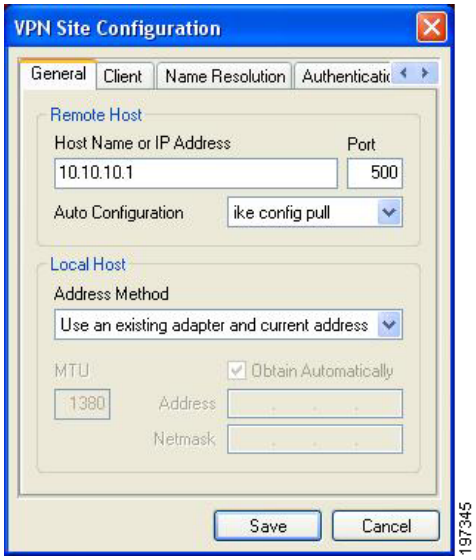
This section describes how to configure the Shrew Soft Client to work with the SA 500. The Shrew Soft client is a free IPSec VPN Client available for download at: http://www.shrew.net.

Step 1. Install Shrew Soft on the client and then launch the **Shrew Soft VPN Access Manager**.

Step 2. Click **Add** to add a new site.

The VPN Configuration window appears. It contains configuration tabs for General, Client, Name Resolution, Authentication, Phase 1, Phase 2, Policy, and Network.

Step 3. Configure the **General** tab settings.

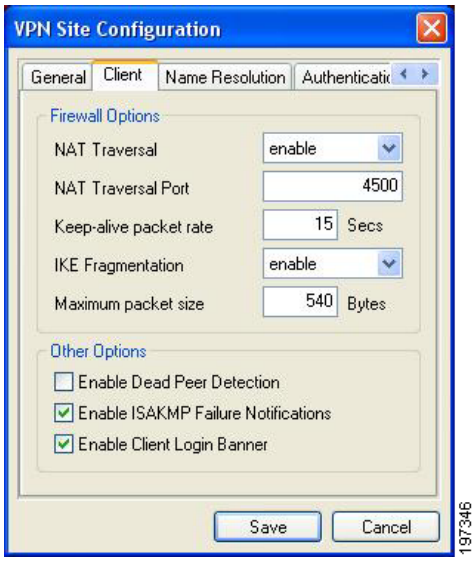


a. In the **Remote Host** area, enter the IP address of the SA 500.

b. In the **Local Host Area**, select **Use an existing adapter and current address** from the Address Method drop-down menu.

c. Click **Save** to apply your changes.

Step 4. Configure the **Client** tab settings.

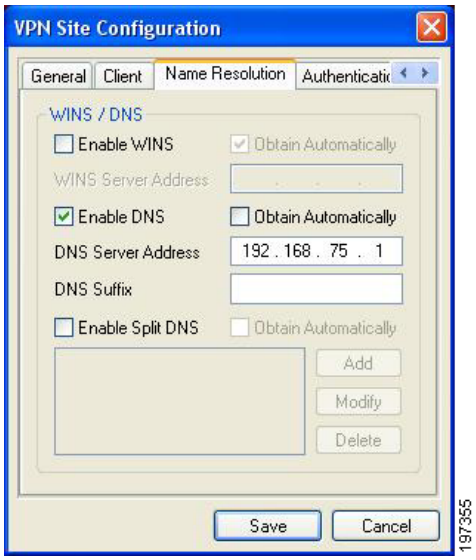


a. Uncheck **Enable Dead Peer Detection** to disable peer detection.

Even though you can enable dead peer detection on the system, it is not required and is not shown in the example configuration.

b. Click **Save** to apply your changes.

Step 5. Configure the **Name Resolution** tab settings.

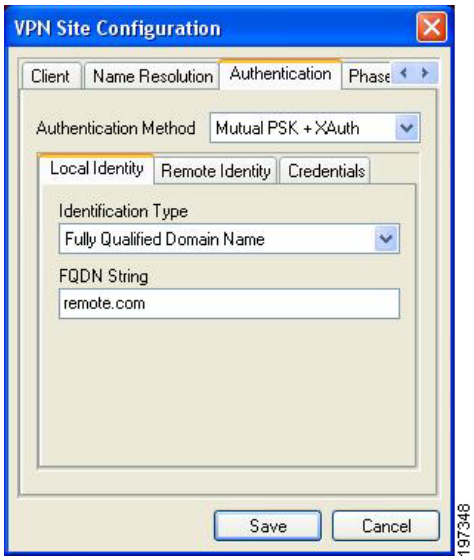


a. Uncheck the **Obtain Automatically** box.

b. Check **Enable DNS** and then enter the DNS server IP address.

c. Click **Save** to apply your changes.

Step 6. Configure the **Authentication Local Identity** tab settings.



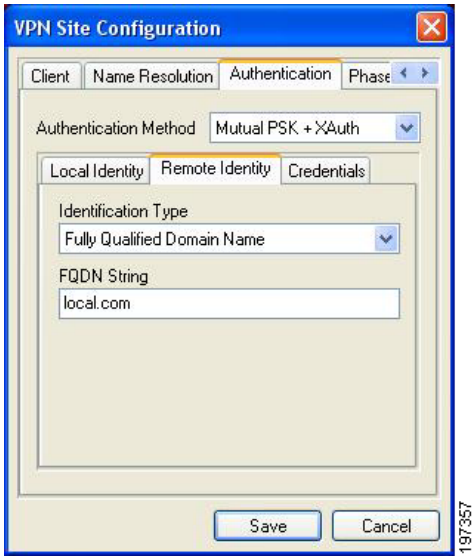
a. From the Authentication Method drop-down menu, select **Mutual PSK + XAuth**.

b. From the Identification Type drop-down menu, select **Fully Qualified Domain Name**.

c. For the FQDN String, enter the Remote FQDN that you entered in the VPN Wizard. For example, **remote.com**.

d. Click **Save** to apply your changes.

Step 7. Configure the **Authentication Remote Identity** tab settings.

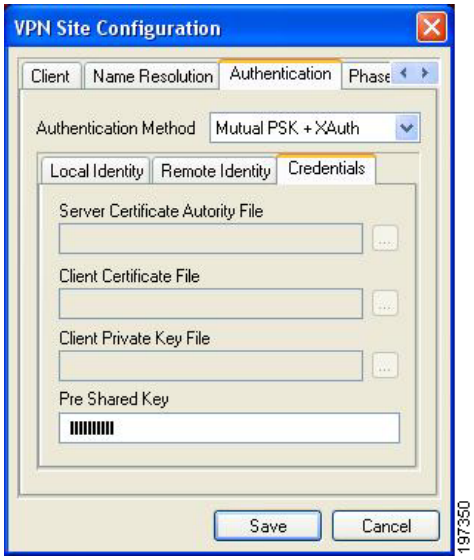


a. From the Identification Type drop-down menu, select **Fully Qualified Domain Name**.

b. For the FQDN String, enter the Local FQDN that you entered on the VPN Wizard page. For example: local.com.

c. Click **Save** to apply your changes.

Step 8. Configure the **Authentication Credentials** tab settings.

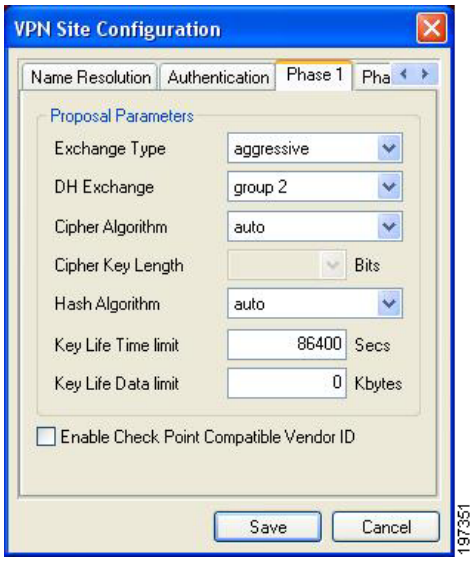


a. Enter the preshared key that you entered on the VPN Wizard page. In the example, **1234567890** is used as the key.

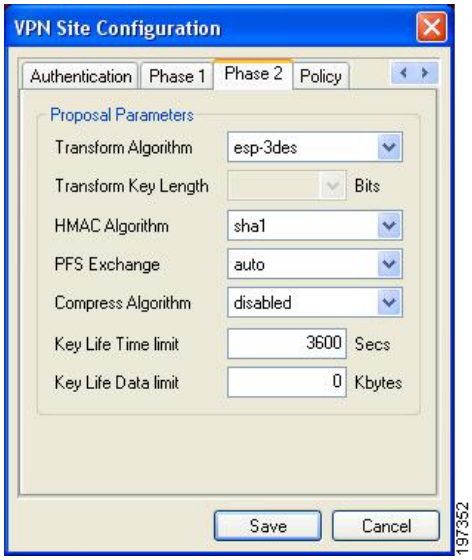
   For testing, this key is acceptable, but should be changed for a production environment.

b. Click **Save** to apply your changes.

Step 9. Verify that the **Phase 1** default settings are set to those shown below. If the settings match, no changes are needed.



Step 10. Configure the **Phase 2** tab settings.

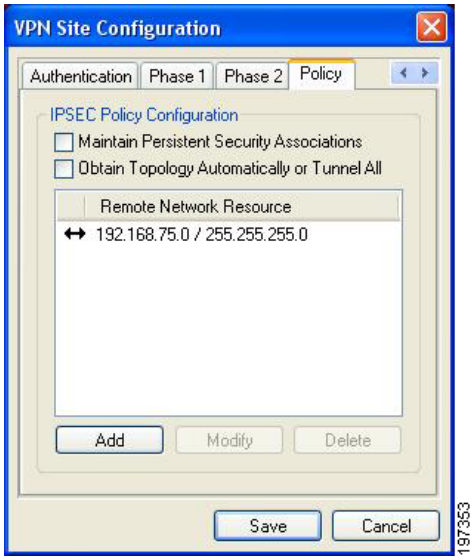


a. From the Transform Algorithm drop-down menu, select **esp-3des.**

b. From the HMAC Algorithm drop-down menu, select **sha1.**

c. Click **Save** to apply your changes.

Step 11. Configure the **Policy** tab settings.

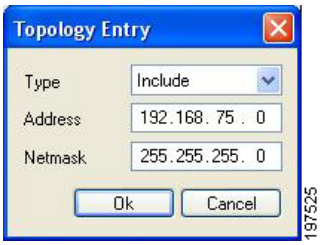


a. Verify that **Maintain Persistent Security Associations** is unchecked.

   In this example, **Obtain Topology Automatically or Tunnel All** is unchecked. If you do not want to allow split tunneling, check this box. However, disabling this option will not allow you to add a network.

b. Click **Add**.

   The Topology Entry window appears.



c. From the Type drop-down menu, select **Include**.

d. For the Address and Netmask, select **192.168.75.0** and **255.255.255.0**.

   If you changed the network to a different one, use those network settings for this configuration.

e. Repeat steps b through d to add additional networks if needed.

Step 12. From Screw Soft VPN Access Manager, open the site that you created.

In the Shrew Soft VPN Connect window, the example site appears as:Example VPN.

Step 13. Enter the username and password that you entered in "Adding IPSec Users" on page 5.

Step 14. Click **Connect**.

The VPN is now connected.

For More Information

Product and Support Resources	Location
SA 500 Technical Documentation	www.cisco.com/go/sa500resources
Cisco Partner tools	www.cisco.com/go/partners
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Cisco.com Technical Support page	http://www.cisco.com/en/US/support/index.html