Configuring an IPSec VPN Tunnel Between a Cisco SA 500 and a Mac IPSecuritas Client

This application note provides information about how to set up a tunnel between a Cisco SA 500 Series security appliance and the IP Securitas client for Mac OS X.

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. Administrators working on this system should have a working knowledge of IPSec VPNs.

Requirements

Before you begin the configuration, make sure that you have the following information:

- Administrator access and preshared key information for the SA 500.
- MAC IPSecuritas client software. To download this client, go to: http://www.lobotomo.com

Configuring the SA 500

The SA 500 has a configuration utility that you use to set up an IPSec VPN tunnel between the SA 500 and the IPSecuritas client,

Follow the steps provided in these sections to set up the tunnel:

- Configuring the VPN Tunnel Settings
- Verifying the IKE Policy
- Verifying the IPSec VPN Policy

NOTE The values that you specify for the SA 500 must be the same for the IPSecuritas client. For information about configuring the client, see Configuring the IPSecuritas Client, on page 7.

Configuring the VPN Tunnel Settings

Use the VPN Wizard to set up the VPN tunnel. The wizard automatically creates an IKE and IPSec VPN Policy for the tunnel based on the settings that you enter on the VPN Wizard page.

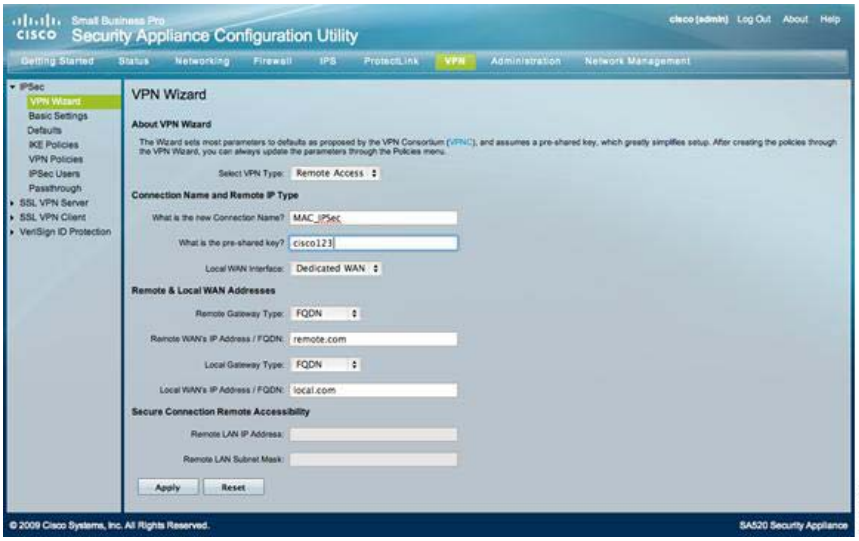
To configure the tunnel settings:

Step 1. Login to the SA 500 as administrator by entering this address: **192.168.75.1.**

- The default username is **cisco**.
- The default password is **cisco**.

Step 2. Click **VPN** in the menu bar, and then click **IPSec > VPN Wizard** in the navigation tree.

The VPN Wizard page appears.



Step 3. In the **About VPN Wizard** area, select **Remote Access** as the VPN Type.

Step 4. 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. In this example, the connection name is **MAC_IPSec**.
- **Preshared Key**: Enter the desired value, which the peer device must provide to establish a connection. In this example, the key is **cisco123**.

  The length of the preshared key is between 8–49 characters and must be entered exactly the same on this page and on the IP Securitas client.
- **Local WAN Interface**: Select **Dedicated WAN** as the interface to use for this VPN tunnel.

Step 5. In the **Remote & Local WAN Addresses** area, enter this information:

- **Remote Gateway Type**: Select **FQDN**.
- **Remote WANs IP Address / FQDN**: Enter remote.com
- **Local Gateway Type:** Select **FQDN**.
- **Local WANs IP Address / FQDN:** Enter local.com.

Step 6. Click **Apply** to save your changes. A VPN policy and an IKE policy are created.

Verifying the IKE Policy

An IKE policy is automatically created after you run the VPN Wizard. The IKE policy establishes a secure tunnel over which the SA 500 and IPSecuritas client can exchange tunnel and key information.

Before you connect the tunnel, verify that the parameters for the newly created IKE policy match those that you entered in the VPN Wizard. You can also edit the IKE policies to something else; however, in most cases the values that you specified in the wizard are sufficient.

NOTE The IKE attributes need to be the same on both the SA 500 router and the IPSecuritas client.The IKE policy name must also match the **Connection Name** that you entered on the VPN Wizard page (for example: **MAC_IPSec**).

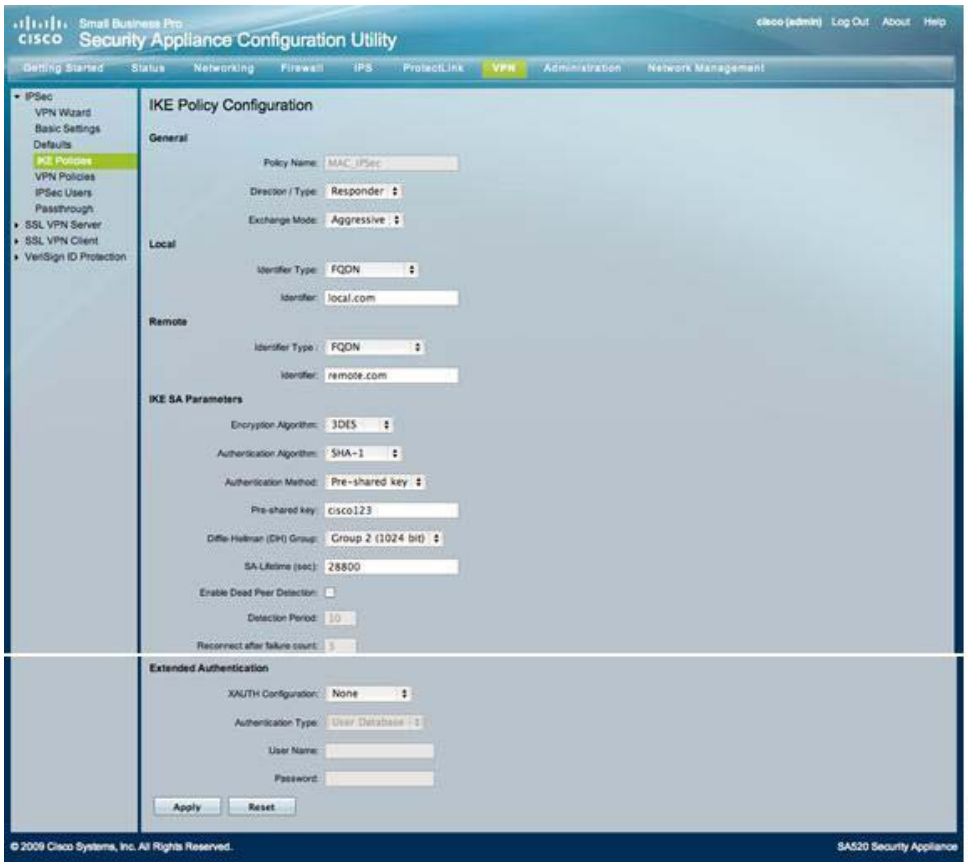
To verify or edit the IKE policy settings:

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

The IKE Policies window appears.

Step 2. Select the newly created policy from the IKE policies table and click **Edit**.

The IKE Policy Configuration window appears.



Verify the following settings.

Step 3. **General** settings.

- **Direction/Type**: Responder.
- **Exchange Mode**: Aggressive.
- **Local Identifier Type**: FQDN
- **Identifier**: local.com

Step 4. **Remote** settings

- **Remote Identifier Type**: FQDN.
- **Identifier**: remote.com

Step 5. **IKE SA Parameters** settings.

- **Encryption Algorithm**: 3DES. Algorithm used to negotiate the SA.
- **Authentication Algorithm**: SHA-1. Authentication algorithm for the VPN header.
- **Authentication Method**: Pre-shared key.
- **Pre-Shared Key**: cisco123
- **Diffie-Hellman (DH) Group**: Group 2 (1024 bit). Algorithm used when exchanging keys.
- **SA Lifetime (seconds)**: 28800. Number of seconds for the SA to remain valid.
- **Enable Dead Peer Detection**: Check the box to enable.

Step 6. **Extended Authentication** > **XAUTH Configuration**: None.

Continue to the next section Verifying the IPSec VPN Policy, or click **Apply** to save your changes.

Verifying the IPSec VPN Policy

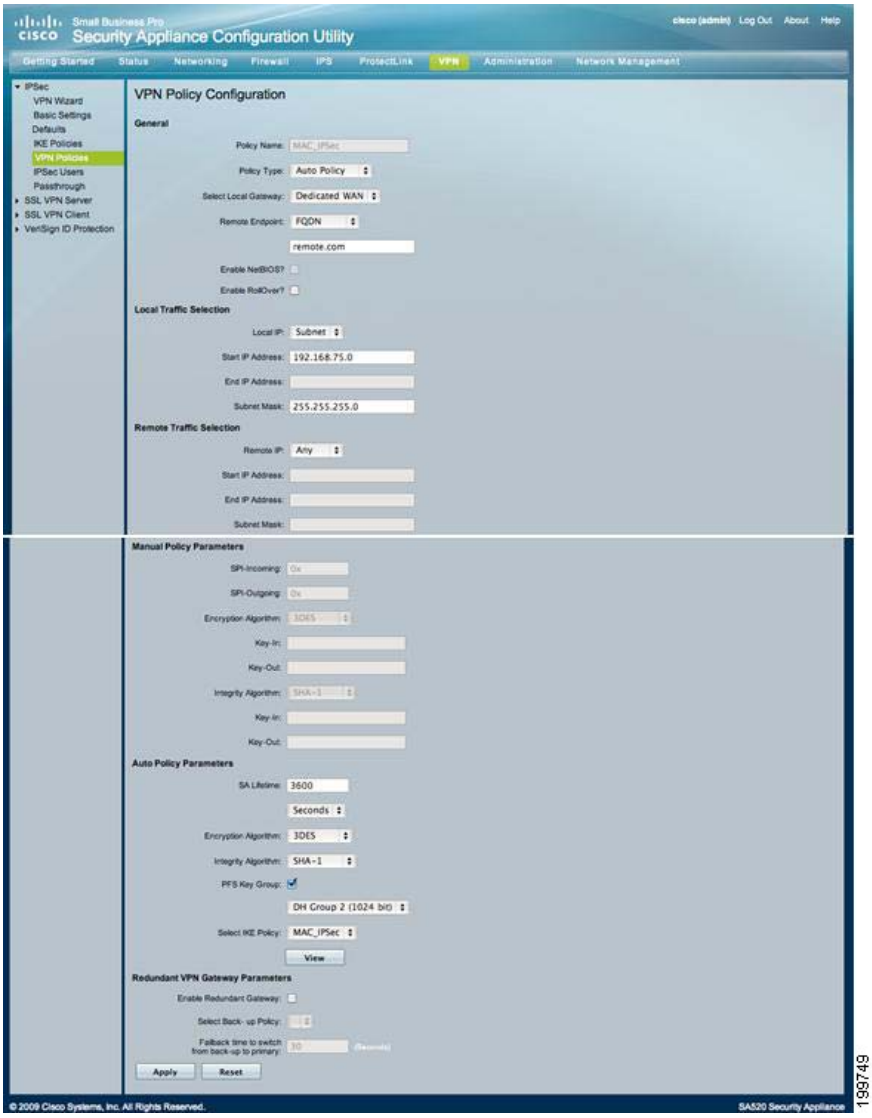
To verify or edit the IPSec VPN policy:

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

The VPN Policy window appears.

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

The VPN Policy Configuration window appears.



Verify the following settings:

Step 3. **General** settings.

- **Policy Type**: Auto Policy.
- **Select Local Gateway**: Dedicated WAN.
- **Remote Endpoint**: FQDN.

Verify that the information matches the domain that you specified in the VPN Wizard for the FQDN. In this example, the FQDN is remote.com. When you select FQDN, the Exchange Mode used is “Aggressive.”

Step 4. **Local Traffic** selection.

- **Local IP**: Subnet.
- **Start IP Address**: Subnet that you want to add to the IPSec VPN. In this example, the starting IP address of the local subnet is:192.168.75.0.
- **Subnet Mask**: Subnet mask of the subnet you are adding. For example: 255.255.255.0

Step 5. **Remote Traffic Selection**: Any.

Step 6. **Auto Policy Parameters** settings.

The SA Lifetime and Algorithm settings should match the IKE SA parameters for this tunnel. See Verifying the IKE Policy, on page 4.

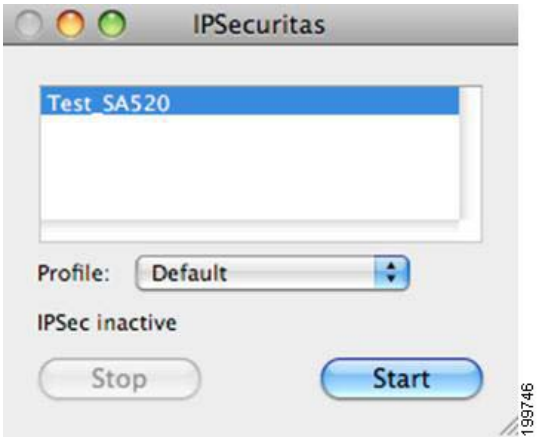
Step 7. Click **Apply** to save your changes if needed.

Configuring the IPSecuritas Client

This section describes how to configure the Mac IPSecuritas client to work with the SA 500. To download this client, go to: http://www.lobotomo.com

Step 1. Install and open the IPSecuritas client.

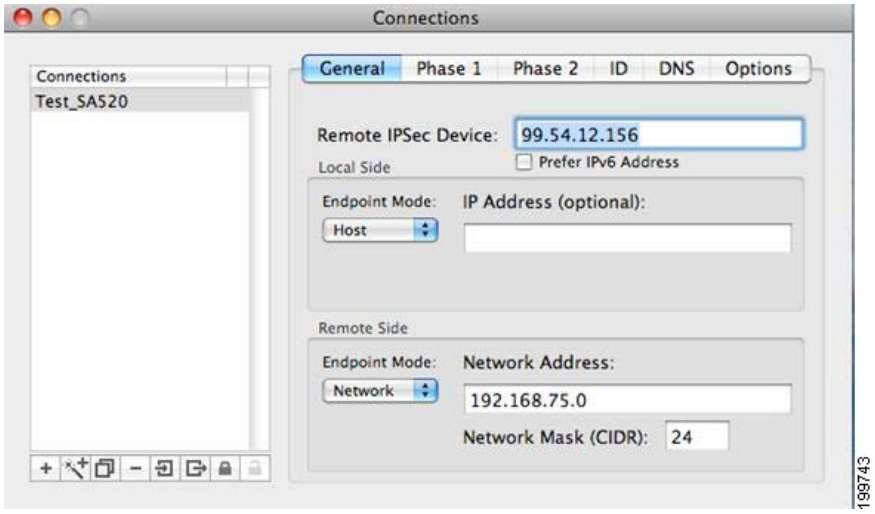
The IPSecuritas window opens.



The SA 500 appears in the window. In this example, the device appears as Test_SA520.

Step 2. From the menu bar, click **Connections > Edit Connections**.

The Connections window opens.

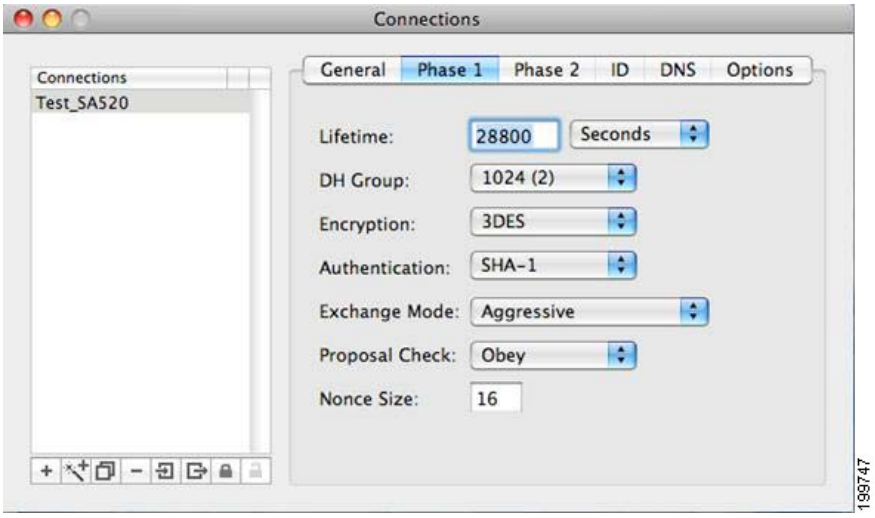


a. Cick the **+** icon on the bottom left of the page.

b. For the **Remote IPSec device**, enter the SA 500 WAN IP address. Leave **Local Side Endpoint** point as blank.

c. For the **Remote Site Endpoint Mode**, select **Network**, and enter the IP addresses for all VLANs used on the LAN of the SA 500.

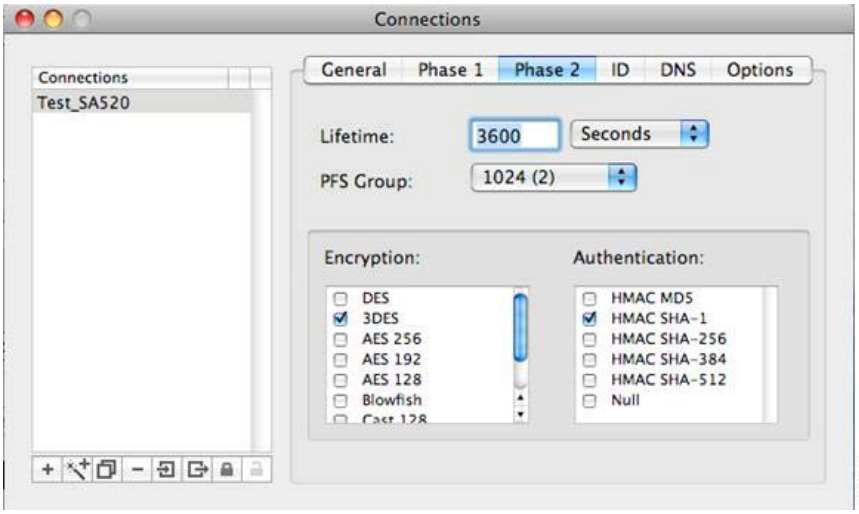
Step 3. Click the **Phase 1** tab.



Verify the follow settings. These values must match the ones that you entered for the SA 500.

- **Lifetime**: 28800
- **DH Group**: 1024 (2)
- **Encryption**: 3DES
- **Authentication**: SHA-1
- **Exchange Mode**: Aggressive
- **Proposal Check**: Obey
- **Nonce Size**: 16

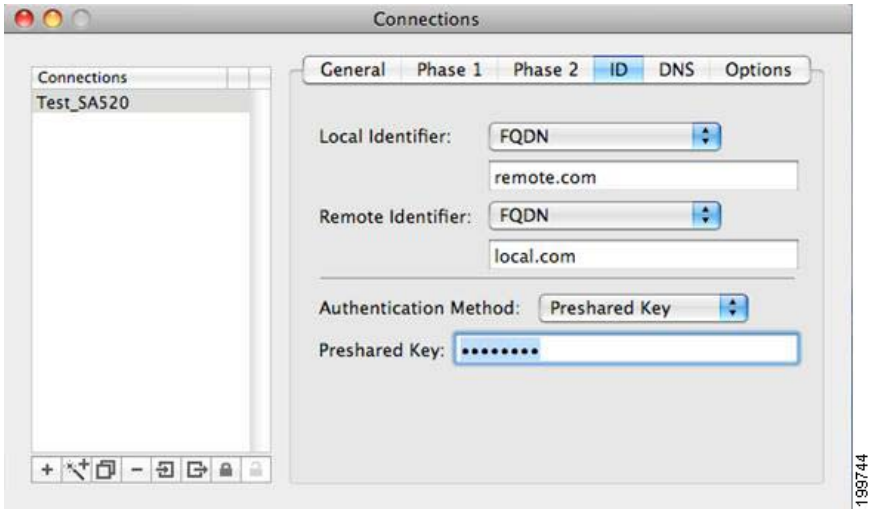
Step 4. Click the **Phase 2** tab.



a. Verify that the **Lifetime** and **PFS** group settings are the same as the ones you specified for the SA 500.

b. Check the boxes for the **Encryption** and **Authentication** methods that you want to use.

Step 5. Click the **ID** tab.



a. For **Local Identifier**, select FQDN. Enter the identifier name as remote.com.

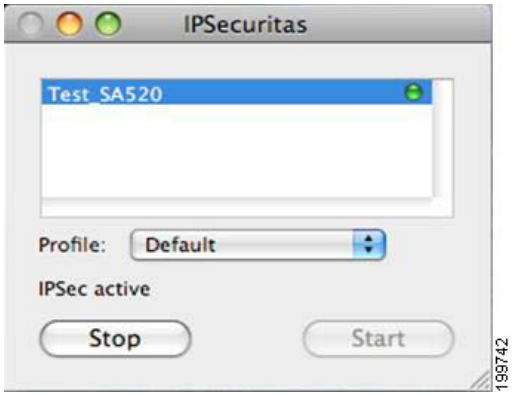
b. For **Remote Identifier**, select FQDN. Enter the identifier name as local.com.

c. Select Preshared Key for the **Authentication Method**. For the **Preshared Key**, enter the same key

Step 6. Close the **Connections** window.

The settings are automatically saved.

Step 7. Click **Start** from the IPSecuritas window.



When the VPN is connected “IPSec active” appears in the window, and the green status icon lights up.

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