# 

# Configuring an IPSec Tunnel Between a Cisco SA500 and the Cisco VPN Client

This application note document provides information on how to configure an SA500 IPSec VPN Tunnel for remote access with the Cisco VPN Client. The Cisco VPN Client allows the security appliance to securely connect to small branch offices, teleworkers, and mobile workers. It provides ease-of-use, scalability, and reduces the need for individual PC-based client applications.

- Scope and Assumptions 2
- Requirements, page 2
- Cisco VPN Client Compatibility, page 2
- Configuring the SA500 for the Cisco VPN Client 2
- Configuring the Cisco VPN Client 8
- Verifying the Client Connection 11
- Viewing the IPSec VPN Connection 12
- For More Information 13

#### Scope and Assumptions

The procedures and guidelines in this Application Note assume that your SA500 is set up for Internet connectivity and has a basic configuration. It applies to an SA500 running firmware v2.1.12 or later with the Cisco VPN Client v4.0 or later. Administrators working on this system must have a basic working knowledge of IPSec VPNs.

#### **Requirements**

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

- An SA500 running firmware version 2.1.12 or later.
- Administrator access to the SA500.
- Preshared key, list of users, and user passwords.
- Cisco VPN Client software (version 4.x or later). To download this client go to: www.cisco.com/go/sa500software.

**Note.** A 3-year Cisco Small Business Support Service Contract (CON-SBS-SVC2) is required to download the client software. If you do not have a support contract, contact your partner or reseller for more information.

# **Cisco VPN Client Compatibility**

The Cisco VPN Client is compatible with the following:

- Windows XP, Vista (x86/32-bit only), Windows 7 (x86/32-bit only), and Windows x64 (64-bit).
- Mac OS X 10.4, 10.5, and 10.6.

# Configuring the SA500 for the Cisco VPN Client

This section describes how to set up an IPSec VPN tunnel on the SA500 to allow workers to connect to your network from remote locations with the Cisco VPN Client. To configure the SA500, you need to create a VPN policy and then add users so they can authenticate to the device. Follow the tasks described in following sections:

- Configuring the VPN Policy using the VPN Wizard
- Adding IPSec Users

#### Configuring the VPN Policy using the VPN Wizard

You configure the VPN policy by using the VPN Wizard. After creating the policy, you can update any of the parameters by using the other options in the Configuration Utility. After the Wizard completes, you will need to add VPN users through the IPSec VPN Users page to complete the SA500 configuration.

**Note.** The Wizard sets most parameters to the defaults proposed by the VPN Consortium (VPNC). For information about the VPNC recommendations, see: http://www.vpnc.org/vpn-standards.html.

- Step 1. Login to the SA500 as administrator by entering: **192.168.75.1.** The default username and password is **cisco/cisco**.
- Step 2. From the Configuration Utility, click VPN > IPSec > VPN Wizard, or from the Getting Started (Advanced) page, click VPN Wizard (Select Remote Access).

The VPN Wizard window appears.

Getting Started	Status	Networking	Wireles		Firewall	IPS	ProtectLink			Network Managemen
Getting Started IFSec VPN Wisard Basic Settings Defaults IKE Policies VPN Policies VPN Policies VPN Policies VPN Server SSL VPN Server SSL VPN Server SSL VPN Server SSL VPN Server VeriSign ID Protection	VPN 1 About V The Wi always Connec Wh Remote Re	Networking Wizard PH Wizard zard sets most para suddate the parame Selec Enable Cisci tion Name and Re at is the new Conne Unat is the pre- Local WA & Local WA Remote Ga Remote WAN'S IP Addi Local WAN'S IP Addi Local WAN'S IP Addi	Wireles meters to defe ters through th ct VPN Type: 5 VPN Client: arrote IP Typ ction Name? shared key? AN interface: dresses teway Type: reas / FQDN: teway Type: reas / FQDN: te Accessit IP Address:	sis as point in the second sec	roposed by th menu. Access v N ed_Key*2010 d WAN v H	e VPN Cons	ProtectLink	VPN	Administration	Network Managemen
		Remote LAN S	ubnet Mask							
	An	Ne Rese	4							

- Step 3. In the **About VPN Wizard** area, choose **Remote Access** to allow the security appliance to be accessed by remote PCs that are running the Cisco VPN Client software.
- Step 4. Check Enable Cisco VPN Client.
- Step 5. In the Connection Name and Remote IP Type area, enter the following information:
  - What is the new connection name?: Enter a name for the connection. This name is used for management and identification purposes. For example: Cisco\_VPN.
  - What is the pre-shared Key?: Enter the desired value, which the peer device must provide to establish a connection. For example: Pre\$h@red\_Key\*20!0.

The length of the pre-shared key is between 8 characters and 49 characters and must be entered exactly the same here and on the VPN remote client. This key is used as the Group Authentication password on the Cisco VPN Client. The preshared key must be the same for both the SA500 and the client.

Note. Do not use the double-quote character (") in the pre-shared key.

- Local WAN Interface: If you have only one WAN configured, choose Dedicated WAN. If you have two WANs configured, choose the interface that you want to use for this VPN tunnel.
- In the Remote & Local WAN Addresses area, use the default (FQDN) for the Local Gateway Type. Note that the fields for Remote LAN IP Address and Subnet Mask are disabled.
- Step 6. Click **Apply** to save your settings.

The VPN policy is added to the "List of VPN Policies" under VPN > IPSec > VPN Policies and the IKE policy is added to the "List of IKE Policies" under VPN > IPSec > IKE Policies.

Step 7. Continue to the next section, "Adding IPSec Users."

#### Adding IPSec Users

You can enable the SA500 to authenticate users from the local user database or to an external RADIUS server. When adding IPSec users, choose one of the following methods:

- Authenticating IPsec Users from the Local User Database
- Authenticating IPSec Users using a RADIUS Server

#### Authenticating IPsec Users from the Local User Database

Step 1. Click VPN > IPSec > IPSec Users.

The IPSec Users window opens. Any existing users are listed in the List of IPSec Users table.

Step 2. Click Add.

The IPSec User Configuration window opens.

Getting Started St	atus Networking Wireless	s Firewall IPS		ProtectLink	VPN
IPSec VPN Wizard	IPSec Users				
Basic Settings Defaults	IPSec User Configuration				
IKE Policies	User Name:	vpnuser1	Ĵ		
IPSec Users	Remote Peer Type:	Standard IPsec (XAuth)	\$		
Passthrough Dynamic IP Range	Allow user to change password?				
SSL VPN Server	Password:	•••••			
VeriSign ID Protection	Confirm Password:	••••••	]		
	Local IP Address:				
	Subnet Mask:				
	Apply Reset				

- Step 3. Enter the following information:
  - User Name: Enter a unique identifier for the XAuth user. For example: vpnuser1.
  - Remote Peer Type: Choose Standard IPsec (XAuth). Note. Do not select Cisco QuickVPN.

The VPN gateway authenticates users in this list when XAuth is used in an IKE policy. XAuth is used when additional client security is required with IPSec clients such the Cisco VPN Client.

**Note.** When XAuth is selected, the **Allow user to change password**, **Local IP Address**, and **Subnet Mask** fields are disabled. The user has access to all the VLANs and not a particular VLAN.

- Password: Enter an alphanumeric password for the user.
- Confirm Password: Enter the exact same characters you entered in the Password field above.
- Step 4. Click Apply to save your changes.

The user is added to the List of IPSec Users table under VPN > IPSec > IPSec Users.

**Note.** The IP address of the remote client is defined by the Dynamic IP Range and is automatically set (default). If you want to manually change this range, you must modify it "before" the VPN policy is created. Otherwise, the changes will not take affect. To change the range, go to **VPN > IPSec > Dynamic IP Range**.

#### Authenticating IPSec Users using a RADIUS Server

Step 1. Click VPN > IPSec > IKE Policies.

The IKE Policies window opens.



- Step 2. Select the user policy you created in the previous step from the List of IKE Policies table and click **Edit**. For example: Cisco\_VPN.
- Step 3. From the IKE Policy Configuration window, under Extended Authentication, enter the following:
  - Choose Edge Device from the XAUTH Config drop-down list.
  - Choose a RADIUS option from the Authentication Type drop-down list. You can choose from RADIUS CHAP or RADIUS PAP.

Extended Authentication		
XAUTH Configuration:	Edge Device	¢
Authentication Type:	Radius - CHA	P ;

- Step 4. Click Apply to save your changes.
- Step 5. To specify the RADIUS Server settings, click Administration > RADIUS Server.

The Radius Server window opens.

Getting Started	Status	Networkin	g Wir	eless	Firewall	IPS	Pro	tectLink		VPN	Administration
Users Firmware & Configuration Diagnostics Traffic Meter	Rad	ius Server Of Configur Authenticatio	ed Radius n Server IP	Server Address	Authentication	Port	Timeout	Retries	Edit		
Logging     Authentication     RADIUS Server     License Managemen	it	Add	Delete								



The Radius Server Configuration window opens.

Getting Started S	tatus Networking Wir	eless F	Firewall	IPS	ProtectLink	VPN	Administration
<ul><li>Users</li><li>Firmware &amp;</li></ul>	Radius Server						
Configuration Diagnostics	Radius Server Configuration						
<ul> <li>Traffic Meter</li> <li>Time Zone</li> </ul>	Authentication Server IP Add	ress: 192.1	68.75.50				
Logging	Authentication	Port: 1812					
RADIUS Server	Se	ecret: •••••	•••				
License Management	Tim	eout: 180	(Seconds				
	Re	tries: 3					

Step 7. Enter the following information:

- Authentication Server IP Address: Enter the IP address of the authenticating RADIUS server.
- Authentication Port: Enter the port number on the RADIUS server that is used to send the RADIUS traffic.
- Secret: Enter the shared key that is configured on the RADIUS server. The secret can contain all characters except for single quote, double quote and space.
- Timeout: Enter the number of seconds that the connection can exist before reauthentication is required.
- Retries: Enter the number of retries for the device to re-authenticate with the RADIUS server.
- Step 8. Click **Apply** to save your settings.

The new server appears in the "List of Configured Radius Server" table.

Getting Started	Status	Networking	Wireless	Firewall IPS	S Pro	otectLink	VPN	Administration
<ul> <li>Firmware &amp; Configuration Diagnostics</li> <li>Traffic Meter</li> </ul>	Copera List	ius Server ation succeeded Of Configured R	adius Server	Authoritanian Dart	Timeout	Patrias	Edia	
Time Zone Logging Authentication RADIUS Server License Manageme	nt	192.168.	75.50 te	1812	180	3		

# **Configuring the Cisco VPN Client**

This section describes how to configure the Cisco VPN Client to work with the SA500. For information about downloading this client, see Requirements, page 2.

Step 1. Install the VPN Client client and launch it.

On a PC, you can launch the client by clicking **Start > Programs> Cisco Systems VPN Client > VPN Client**, or by clicking the VPN Client icon on your desktop.

The VPN Client window appears.

Connect New Import Modify	Delete		ili.ili. cisco
Connection Entry /	Host	Transport	

Step 2. Click New to add a new VPN connection.

onnection Entries Status Certific	ates Log Options Help		
Connect New Impo	a Modify Delete		cisco
Connection Entry	Host	Transport	
	Stephene   Create New VPN Con	nnection Entry	
	Connection Entry: Cisco_VPN Description: Cisco_VPN Host: 39.109.206.124 Authentication Transport Backup Serve	ers Dial-Up	cisco
	Group Authentication	C Mutual Gr	oup Authentication
ot connected.	Name:         Cisco_VPN           Password:         XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX		
	Certificate Authentication Name: Send CA Certificate Chain	T	
	Erase User Password	Save	Cancel

The Create New VPN Connection Entry window opens.

- Step 3. Enter a name and description for the new connection. For example: Cisco\_VPN.
- Step 4. In the Host field enter the WAN IP address of the VPN Server (SA500). For example: 99.109.206.124.
- Step 5. Specify the Group Authentication information.
  - a. Enter the name for the Group Authentication policy. For example: Cisco\_VPN.
  - b. Enter the password and confirm it. The password must be the same as the preshared key configured for the SA500. See Configuring the SA500 for the Cisco VPN Client, page 2.
  - c. Click Save.

The new connection entry appears in the VPN Client page.

Connection Entries Status Certificates Log Option	is Help Delete	cisco
Connection Entries Certificates Log	Host	Transport
Cisco VPN	99 109 206 124	IPSec/IIDP
1		

Step 6. Select the new entry and click **Connect**.

Cancel Connect New Import	Modify Delete	cisco
Connection Entries Certificates Log	Host	Transport
Cisco_VPN	99.109.206.124	IPSec/UDP
	VPN Client   User Authentic	cation for "Cisco_VPN"
	VPN Client User Authentic The server has requested the following in authentication. Username: vpnuser1 CISCO Password: VPNUSER1	cation for "Cisco_VPN"

- Step 7. In the User Authentication window, enter the Username and Password and click **OK**. These must match the username and password configured in the SA500 List of IPSec Users or on the RADIUS server. See Adding IPSec Users, page 4.
- Step 8. After the VPN tunnel is established, the status shows as **Connected** on the VPN Client page and displays the **IP Address** assigned to the remote user from the VPN server (SA500).

Connec Z Disco	tion Entries Status Certificates Log C	Diptions Help	ululu cisco
Conne	ction Entries Certificates Log	Host	Transport
3	Cisco_VPN	99.109.206.124	IPSec/UDP
4			

# Verifying the Client Connection

Step 1. To verify the client connection, make sure the that the connected (lock) icon is displayed on the taskbar on the remote VPN Client as shown below.



Step 2. Enter **ipconfig** from the Windows Command Prompt to view the IP Address for the VPN remote client. In this example, the remote IP address is 192.168.11.50.



Step 3. Verify that the remote user can ping the hosts on the LAN of the SA500.



#### **Viewing the IPSec VPN Connection**

Use this page to view the connection status of the remote client connected to the SA500. To access this page, click **Status > VPN Status > IPSec Status** from the Configuration Utility.

This page shows the statistics for the connection including the policy name, endpoint, data and number of IP packets transmitted, and the current status of the IKE policies. You can also use the buttons on the page to start or stop the connection. This page also refreshes automatically to display the most current status for the security association (SA).

Getting Started	Status Networkii	ng Wireles	s Firewal	II IPS P	rotectLink	VPN	Network Managemen
Device Status     VPN Status     IPSec Status     SSL VPN Status     QuickVPN Status	IPSec VPN Co The page will auto	onnection St o-refresh in 7 si	atus econds				
Active Users	Policy Name En	dpoint Tx (KB	Tx (Packets)	State	Action		
<ul> <li>View Logs</li> <li>CDP Neighbor</li> </ul>	99.54.12.155* 99.5	4.12.155 0.00	0	IPsec SA Establis	hed Drop		
LAN Devices	Poll Interval: 10		Start	Stop			

# For More Information

Product and Support Resources	Location
SA500 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

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

© 2010 Cisco Systems, Inc. All rights reserved. OL-24043-01