

Configuring SSL VPN on the Cisco ISA500 Security Appliance

This application note describes how to configure SSL VPN on the Cisco ISA500 security appliance. This document includes these topics:

- Overview
- Prerequisites
- Configuring the ISA500 for SSL VPN
- Connecting the AnyConnect Client to the ISA500
- Verifying the SSL VPN Connection
- Troubleshooting
- For More Information

Overview

Secure Socket Layer (SSL) Virtual Private Network (VPN) technology allows a remote user to connect securely from anywhere on the Internet to an internal corporate network by using an SSL VPN client. In this document, the SSL VPN client used is the Cisco AnyConnect client.

With SSL VPN and the AnyConnect client, personal computers, Cisco SPA525G phones, and handheld devices (such as IPhone, iPad, and so forth) can connect to the SSL VPN gateway (ISA500) for remote access.

This document uses the network configuration described in Figure 1. As illustrated, the remote user connects to the ISA500 IP address with the AnyConnect client. After the user successfully authenticates to the ISA500, they can then use an encrypted secure session for full access to all permitted resources on the corporate network.

Figure 1 ISA500 Network Configuration with AnyConnect Client



Prerequisites

To securely access resources on a private network behind the ISA500, the remote user of the SSL VPN service must have the following:

- User account (login name and password) to access the ISA500 Configuration Utility
- Administrative access to the ISA500 (to initially install the AnyConnect client and to use the full tunnel client feature)
- AnyConnect VPN client (also referred to as the Cisco AnyConnect Secure Mobility client) installed on their workstations. To download the latest client, see: http://www.cisco.com/cisco/software/navigator.html?mdfid=281268793&i=rm.
- Operating system support for the AnyConnect client
 - Microsoft Windows 7, Windows 2000, Windows XP, or Windows Vista
 - Macintosh OS
 - Linux

NOTE You must configure the SSL VPN configuration and the SSL VPN group policies on the ISA500 before a remote user can access resources on the private network.

Configuring the ISA500 for SSL VPN

This section describes how to configure the ISA500 for SSL VPN by using the Remote Access VPN Wizard and how to connect it to the AnyConnect client.

SSL VPN uses tunneling to establish private connections through public networks such as the Internet. VPN supports two types of tunneling modes. Choose one of these modes to configure the ISA500:

- Configuring SSL VPN Full Tunnelling
- Configuring SSL VPN Split Tunneling

We recommend that you use the Remote Access VPN Wizard the first time that you configure SSL VPN. Afterwards, if you want to modify the SSL VPN configuration and group policies, you can configure them from the **VPN > SSL Remote User Access** pages.

Configuring SSL VPN Full Tunnelling

Full tunnel mode allows remote clients to access both corporate network resources and the Internet through the ISA500. In this mode, all network traffic is routed to the ISA500 through a secure tunnel.

To configure full tunnel mode, follow these steps:

Step 1. From the ISA500 Configuration Utility, choose Configuration Wizards > Remote Access VPN Wizard.

Setup Wizard Dual WAN Wizard	Remote Access VPN Wiza	Ind
Remote Access VPN Wuard Site-5-Site VPN V/Land DAZ/Wland Wireless Wizard	Getting Started IPsec Remote Access SSL Remote Access	Getting Started Help The Remote Access VPN Without helps you configure your secunity appliance as a IPsec Remote Access server or as a SSL Remote Access or SSL Remote Access as the VPN tunnel type and then click Next to proceed. VPN Tunnel Type: Psec Remote Access Startende users can secure access or SSL

Step 2. Choose SSL Remote Access from VPN Tunnel Type drop-down menu and click Next.

Getting Started	Getting Started	Help
Psec Remote Access SSL Remote Access	Getting Started The Remote Access VPN Ward helps you configure your security appliance as a IPsec Remote Access server or as a SSL Remote Access or Remote Access as the VPN tunnel type and then click Next to proceed. VPN Tunnel Type: SSL Remote Access :	Help SSL

The SSL VPN Configuration window opens and displays the default SSL VPN settings. From this page you can enable or disable the SSL VPN service, and edit or customize the settings.

In this example, the **Client Domain**, **Login Banner**, and **Session Timeout** values were modified. The session timeout value (shown as 43200 seconds) is equivalent to 12 hours. For detailed descriptions of these fields, see <u>Basic Configuration Settings</u>, page 14.

Getting Started SSL Remote Access	SSL VPN - Configuration Gateway(Basic)	Help
Configuration Group Policy User Group Summary	Gateway Interface: WANT • Gateway Port: 443 (Range: 1-65535) Certificate File: Gefault • Client Address Pool: 192.168 200.0 Client Netmask: 255.255.255.0 Client Intermet Access: Image: Create NAT rule allowing intermet access to remote users Client Domain: Cisco.com	
	Login Banner:	
	Keep Alive: 30 seconds (Range: 0-600) Lease Duration: 43200 seconds (Range: 600-1209600)	
	1406 bytes (Range: 256-1406)	

Step 3. Click **Next** to continue to the Group Policy configuration page.

0.00

By default, the ISA500 uses the default policy **SSLVPNDefaultPolicy**. You can also create and customize your own policy by clicking **Add**.

etting Started SL Remote Access	Grou	p Policy		Help
Configuration		Add 🗙 Delete		1
Jser Group Summary	P S	olicy Name SLVPNDefaultPo	Configure icy /X	

Step 4. Click the pencil icon next to the default policy to open the Group Policy configuration settings.

As shown here, the Primary DNS value is automatically populated with the default ISA500 IP address (this field is required). When the ISA500 IP address uses the Primary DNS, the remote clients sets this IP address as the DNS server address on its outgoing SSL VPN interface and sends any DNS queries to the ISA500. The ISA500 resolves these queries by using the DNS server IP address configured on the WAN settings.

If desired, you can change the Primary DNS value to the DNS IP address of the corporate network. Optionally, you can configure a secondary DNS server and a primary and secondary WIN server.

Basic Settings	E Proxy Settings	Split Tunneling Settings	Zone-based Firew all Settings	
olicy Name:	SSLVPNDefau	ItPolicy	(Length: 1 to 49 characters)	
rimary DNS:	192.168.200.1			
econdary DNS:				
rimary WINS:				

Step 5. Configure the IE Proxy, Split Tunneling, and Zone based Firewall settings.

In this example, the IE Proxy Policy and Split Tunneling settings are disabled. If desired, you can enable the proxy and specify several Internet Explorer (MSIE) proxies for the client's computers. When enabled, Internet Explorer on the client computer is automatically configured with these settings.

Setting Started	Group Policy		н	elp
Configuration	Add XDelete		Group Policy - Add/Edit	Help
Jser Group Summary	Policy Name SSLVPNDefaultPolicy	Configure	re Bask Settings IEProny Settings Sett Tunneting Settings Zone-based Frew all Settings IE Prony Policy. None Auto Bypass-Local O Disable Address: (IP Address or Domain Name) Port (Range: 1-65535) IE Prony Exception: (IP Address or Domain Name) Add S	
			Deete	Cancel

Getting Started SSL Remote Access	Group Policy		Help
Configuration Group Policy		Group Policy - Add/Edit	Hel
User Group Summary	Policy Name Configure SSLVPNDefaultPolicy		ings
		Ectude Local LANS	OK Cancel

By default, the remote clients can access all resources on all ISA500 interfaces. However, if desired, you can control user access by permitting or denying access to a particular zone.

asic Settings	IE Proxy Settings	Split Tunneling Settings	Zone-based Firewall Settings	
Access Conti	ol			
Zone	Access Set	tting		
LAN	Permit	ODeny		
WAN	Permit	ODeny		
DMZ	Permit	ODeny		
VPN	Permit	ODeny		
GUEST	Permit	ODeny		
VOICE	Permit	ODeny		

- Step 6. Click **OK** when you are finished.
- Step 7. From the Group Policy page, click **Next** to configure the users and user groups for the SSL VPN remote clients on the local database. In this example, we used the default user group **admin** and created user accounts under that group on the local database.

To add your own user groups, click **Add**. You can also configure user accounts on an Active Directory or RADIUS server. For more information see the "Configuring the ISA500 for Active Directory/LDAP and RADIUS Authentication" application note at: www.cisco.com/go/isa500resources.

tting Started L Remote Access	User Group					Help
onfiguration	-Add 🗙 De	liete				
ser Group	Sequence	Name	User Membership List	SSL VPN	Configure	
immary		admin		SSLVPNDefaultPolicy	10	

er Group - Add/Edi		Help
Group Settings	lembership admin	
iervices Veb Login: SSL VPN: Cisco IPsec VPN: Captive Portal:	 Disable Read Only Administrator SSLVPNDefaultPolicy Enable Disable Enable Disable 	
		Ok Cancel

a. Click the **Membership** tab to create a new user account for the remote client. Enter the **User Name** and **Password** and then click **Create**. In this example, we created a user named **jdoe**.

Group Settings	mbership	
User	Membership	
Create new membe Jser Name:	er:	
^D assword:	••••••	

		Help
Group Settings Me	mbership	
Jser doe	e Membership	
	ar ·	
Create new membe	····	
Create new membe Jser Name:		
Create new membe User Name: Password:		
Create new membe User Name: Password: Password Confirm:		

Group Settings Member	ship	
User	Membership Idoe	
Create new member :		
User Name:		
User Name:	reate	

Step 8. Click the right arrow to add **jdoe** as a member to the user group **admin**.

- Step 9. Create more user accounts as needed and then click **OK** to save your settings.
- Step 10. Click **Next** to continue to the SSL VPN summary page. Verify that the information is correct and then click **Finish** to save the configuration.

Getting Started	SSL VPN summa		Help
SL Remote Access			
Group Policy User Group	SSL VPN Server Setting Gateway Interface Gateway Port	9 WAN1 443	
Summary	Client Address pool Client Netmask Client Internet Access Client Domain	default 192168.200.0 255.255.255.0 Enabled cisco.com Welcome to Cisco	
	Login Banner	Systems Network For further assistance please contact admin@cisco.com.	
	Policy Name SSL\PNDefaultPolicy	Applied Group List admin	

Configuring SSL VPN Split Tunneling

SSL VPN split tunnelling allows specific traffic to be routed outside of the AnyConnect client tunnel. You can configure network traffic to be either included (resolved by the SSL VPN tunnel), or excluded (resolved through the ISP or the WAN connection).

To configure split tunneling mode, follow these steps:

- For steps 1 though 5, follow the same steps as those in Configuring SSL VPN Full Tunnelling, page 2. In this example the IE Proxy settings are left unchanged. For more about the proxy settings feature see page 6.
- Step 2. Click the Split Tunneling Settings tab to configure the policy.
 - a. Check the box to enable Split Tunneling.

In this example, the **Exclude Traffic** option is enabled. With this option all network traffic on the remote client (except for those networks added to exclude traffic) is routed to the ISA500 and the excluded traffic is routed to the ISP.

If you select **Include Traffic**, all network traffic on the remote client (except for those networks added to include traffic) is routed to the ISP and the included traffic is routed to the ISA500.

NOTE You can select either the Include Traffic or Exclude Traffic option for the group policy but not both.

Basic Settings IE	Proxy Settings Split	Tunneling Settings	Zone-based Firewall Settings	
Enable Split Split Selection: Address:	Tunneling 🔵 Include Traffic 🖲	Exclude Traffic		^
Split Table				
🗙 Delete				
IP IP	Netmask			
	No data a			
Exclude Local				
Exclude Local	0.040	(A 4 4		~

b. Enter the **Address** and **Netmask** for the traffic that you want to exclude when routing traffic to the ISA500 and then click **Add**.

lasic Sattings	IE Drovy Sattings	Solit Tuppeling Settinge	Zone hased Firewall Settings	
	a lit Turne a line	opik runneing sexings	Zone-based in email cettings	~
Enable a Split Coloctic	spint i uninening sp: Include Tr	offic 💽 Evoludo Troffic		
s i i	128 107 0.0			
Address:	120.101.0.0			
vetmask:	255.255.0.0		Add	
Colit Notes	ork			11
Split Netwo				
XDelete				
IP	Netm	ask		
	No	data available		
				-
				0 1

- c. Check the Exclude Local LANs box to exclude the remote clients local LAN from traffic that is resolved by ISA500. When enabled, traffic routed to the hosts on the same LAN as the remote client is routed directly to the hosts (instead of sent to the ISA500 to route back on same secure tunnel).
- d. Enter the **DNS server IP address** in the Split DNS field and click **Add**. The DNS server resolves domain names when traffic is sent to the excluded networks.
- Step 3. Click **OK** to save your settings.
- Step 4. Click the **Zone-based Firewall Settings** tab.

By default, the remote clients can access resources on all of the ISA500 interfaces. You can control this access by changing the Access Setting for a particular zone to Permit or Deny. In this example, the firewall is configured to deny LAN and VPN access to the remote client.

asic Settings	IE Proxy Settings	Split Tunneling Settings	Zone-based Firewall Settings	
Access Con	trol			
Zone	Access Set	ting		
LAN	Permit	Oeny		
WAN	Permit	Deny		
DMZ	Permit	ODeny		
VPN	Permit	Oeny		
GUEST	Permit	ODeny		
VOICE	Permit	Deny		

- Step 5. Click **OK** when you are finished.
- Step 6. Configure the user accounts for the SSL VPN remote clients on the local database. Follow the same steps as those for configuring full tunnel mode on page 7.

Basic Configuration Settings

This section describes the basic settings required for an SSL VPN Configuration. You can configure these settings from the Remote Access VPN Wizard or from the **VPN > SSL Remote User Access > SSL VPN Configuration** page.

- Gateway Interface: The WAN port through which SSL VPN connection requests are sent to the ISA500. By default, WAN1 (mandatory) is the only available interface and is the only option that appears in the Gateway Interface drop-down menu.
 - For a WAN load balancing configuration, choose either WAN1 or WAN2 depending on your network.
 - For a WAN failover configuration, always choose the primary WAN (WAN1) as the gateway interface.

NOTE If a failover occurs, the SSL VPN service restarts and uses the standby WAN as the gateway interface.

Gateway Port: By default, SSL VPN operates on port number 443. If desired, you can change the port number to a user-defined value. When configuring the port, the SSL VPN client must enter the entire address pair as *Gateway IP Address:Gateway Port Number* to connect to the ISA500.

In this example, the AnyConnect client uses the default SSL VPN port and the ISA500 IP address 220.0.0.1.



In this example, the ISA500 IP address 220.0.0.1 is the same as before, but the SSL VPN port was changed to 10000.

cisco	AnyCo Secure Mo	onnect obility Clier	
VPN: Re	eady to conn	nect.	
220.0.0.1:10	0000	-	Connect

- Certificate file: File used to authenticate remote users who try to access the corporate network through the SSL VPN tunnels. You can choose either the default certificate file or import one of your choice.
- Client Address Pool: Private network address from which the host IP address is assigned to the remote access client. The IP address range must not overlap with other IP addresses on the local network.
- **Client Netmask**: Netmask address for the network address chosen for the client's address pool. Valid netmask addresses are 255.255.255.0, 255.255.255.128 and 255.255.255.192.

The following table shows the network address range for different network addresses. This example assumes that the maximum number of clients connected to the ISA500 is 50.

Network IP Address	Netmask	Beginning Host Address	Ending Host Address	SSL VPN Gateway IP Address
10.10.10.0	255.255.255.0	10.10.10.2	10.10.10.51	10.10.10.1
172.16.10.0	255.255.255.128	172.16.10.130	172.16.10.179	172.16.10.129
192.168.10.0	255.255.255.192	192.168.10.194	192.168.10.243	192.168.10.193

- Client Internet Access: Automatically creates advanced NAT rules to allow SSL VPN clients to
 access the Internet over the SSL VPN tunnels. This option is enabled by default.
- Client Domain: Changes the default text to the domain name of choice given to the SSL VPN address space.
- Login Banner: Text entered in the login banner field that appears after a remote user authenticates to the SSL VPN server. You can change the default banner text to whatever you want. For example: Welcome to xyz company. For assistance contact admin@xyz.com.

Connecting the AnyConnect Client to the ISA500

After you configure the ISA500 for SSL VPN, you can set up the connection to the AnyConnect client. This client establishes the SSL VPN tunnels and provides users with a secure VPN connection to the ISA500.

Make sure that the user has already installed the AnyConnect client installed on their workstations. To download the latest client, see: http://www.cisco.com/cisco/software/ navigator.html?mdfid=281268793&i=rm.

Follow these steps to connect the client to the ISA500. In this example, we used the Cisco AnyConnect Secure Mobility Client v3.0.2052 on a Windows 7 computer.

- Step 1. Launch the AnyConnect client.
- Step 2. From the AnyConnect Secure Mobility Client window, click the **Advanced** link.



- Step 3. Under Preferences, check the Enable local LAN access box. You must select this option if you enabled it in the Split Tunneling settings as described on page 11. If this option is disabled, the local LAN to which the remote client belongs will not be excluded from routing packets to the ISA500.
- Step 4. Choose the ISA500 WAN address in the AnyConnect dialog box and click Connect.

cisco	AnyConnec Secure Mobility Cl No Network Conn	ct lient nectivity
VPN: Ve	erify your network co	nnection.
220.0.0.1	-	Connect
	Advanced	

Step 5. Enter the remote client's **Username** and **Password** and click **OK**.

Please enter	your username and password.
Username:	jdoe
Password:	******
	W.P.

The banner text message appears and prompts the remote user to **Accept** the connection. The SSL VPN connection is then established.

NOTE If you receive an error message or if the connection fails, see Troubleshooting, page 26 for more information.

Welcome to Cisco Systems Network. Fo contact admin@cisco.com.	r further assistance please	*
		Ŧ

You can view the connection status and other details about the VPN from the AnyConnect VPN status pages. These pages show the status, routing, and client connection information for the VPN.

	- 11	V 11 2000	10			
Virtual Pr	ivate Ne	twork (VPN	1)			
Preferences	Statistics	Route Details	Firewall	Message History		100
Connection	Information	1		Address Informa	ation	
State:			Connecte	d Client (IPv4):	192.168.200.3	
Mode:			All Traffi	c Client (IPv6):	Not Available	
Duration	:		00:01:3	9 Server:	220.0.0.1	
Bytes				Transport Inform	nation	
Sent:			1791	3 Protocol:	TLS	
Received	i:		60	9 Cipher:	RSA_AES_256_SHA1	
Frames				Compression:	None	
Sent:			22	9 Proxy Addres	s: No Proxy	
Received	l:			4 Feature Configu	ration	
Control Era	mar			FIPS Mode:	Disabled	
Sent:	inco			Trusted Netw	ork Detection: Disabled	
Received	i:			Always On:	Disabled	
Client Mana	nement			Secure Mobility S	Solution	
Administr	rative Domai	in:	220.0.0	1 Status:	Unconfirmed	
muniii 115 U	Save Dollig			Appliance:	Not Available	

Preferences	Statistics	Route Details	Firewall	Message	History	
Non-Sec	ured Route	25			Secured Routes	
Destinat	on	Subnet Mask			Destination	Subnet Mask



Verifying the SSL VPN Connection

You can use the ISA500 SSL VPN Status page to view the information for all active VPN sessions. This page is automatically updated every 10 seconds.



cisco ISA	Business	Configur	ation Utili	ty					
Configuration Wi	zards	SS	VPN Stat	us					
Networking		Ref	resh						
Networking		Acti	ve Sessions S	SL VPN Statistics					
Firewall		Ac	tive Sessions						
Security Services	k	3	Disconnect						
VPN			Session ID	Liser Name	Client IP (Actu	al) Client IP	(APN) Cor	nect Time	Configure
 VPN Status IPsec VPN S 	Status		5	jdoe	220.0.0.2	192.168	200.7 00:0	08:46	N.
SSL VPN Sta Site-to-Site	Access								
 SSL Remote L SSL VPN Co SSL VPN Go 	User Access onfiguration oup Policies								
Lazo Const	N Client								
VPN Passthroi	ugh								
SSL VPN Stat	tus								
Refresh									
Active Sessions	R VPN Statistics								
Gobal Status Active Users In CSTP Frames. In CSTP Data In CSTP Data In CSTP Control. Out CSTP Frames: Out CSTP Pata: Out CSTP Data Out CSTP Control. Oesc.	1 4433 310492 4372 61 308 26128 306 0								
Session Statistics									
- Clear									
Session ID	In CSTP Frames	In CSTP Bytes	In CSTP Data	In CSTP Control	Out CSTP Fra. O	t CSTP Bytes	Out CSTP Data	Out CSTP C	Configure
5	85	5682	74	11	72 75	60	72	0	Clear

Step 2. Click the SSL VPN Statistics tab to view the traffic statistics.

Refresh									
Active Sessions	it. VPN Statistics								
Global Status Active Users: In CSTP Frames: In CSTP Bytes: In CSTP Data: In CSTP Control: Out CSTP Control: Out CSTP Data: Out CSTP Data: Out CSTP Control: Otes:	1 551 41466 549 2 30 2360 30 0								
Session Statistics	1								
Clear									
Session ID	In CSTP Frames	In CSTP Bytes	In CSTP Data	In CSTP Control	Out CSTP Fra	Out CSTP Bytes	Out CSTP Data	Out CSTP Co	Configure
		1.12.2.2	2743 A. 201						(Creater Han)

After the SSL VPN session is established, a dynamic access control list (ACL) is added to the ISA500 firewall based on the Zone-based Firewall settings that you configured on page 12.

() (C)			9				_				
trol List											
Delete	🖓 Reset 🛛 😚 Re	efresh									
Enable	From Zone	To Zone	Services	Source Address	Destination Address	Hit Count	Log	Action	Detail	Configure	
	SSLVPN	LAN		sslvpnSession0	Any			Deny 👻	0		
	SSLVPN	WAN		sslvpnSession0	Any			Permit -	0		
	SSLVPN	DMZ		sslvpnSession0	Any			Permit 👻	0		
	SSLVPN	VPN		sslvpnSession0	Any			Deny -	0		
	SSLVPN	GUEST		sslvpnSession0	Any			Permit 👻	0		
	SSLVPN	VOICE		sslvpnSession0	Any			Permit 👻	0		
	LAN	WAN						Permit -	0		
	LAN	DMZ						Permit 👻	0		
	LAN	VPN						Permit 👻	0		
	LAN	GUEST						Permit 👻	0		
	LAN	SSLVPN						Permit +	0		
	LAN	VOICE						Deny -	0		
	rtrol List Delete Enable V V V V V V V V V V V V V	Control List Control	Rest Refersh Enable From Zone To Zone SSLVPN LAN SSLVPN VAN SSLVPN VAN SSLVPN VAN SSLVPN VAN SSLVPN VAN SSLVPN VOLE SSLVPN VOLE LAN VAN LAN VAN LAN VAN LAN VAN LAN VAN LAN VAN LAN GUEST LAN GUEST LAN GUEST LAN GUEST LAN GUEST LAN SUEVPN	Rest Refresh Enable Form Zone To Zone Services SSLVPN LAN SSLVPN VAN SSLVPN MAZ SSLVPN VAZ SSLVPN VMA SSLVPN VAZ SSLVPN VDCE SSLVPN VOICE LAN VAX VOICE LAN LAN VAX VAX VAX	No Lone No Lone No Lone No Lone No Lone Date From Lone To Zone Services Source Address Call From Zone To Zone Services Source Address SILVPN LAN SstypRession0 SstypRession0 SILVPN MAN sstypRession0 SILVPN VPN sstypRession0 SILVPN VDEST sstypRession0 SILVPN VOICE sstypRession0 SILVPN VOICE sstypRession0 LAN VAN VAN LAN VAN VAN LAN LAN VPN LAN VPN LAN LAN SSUPN VICE	Number Number Number Date: Reset Referation Enable From Zone To Zone Services Source Address Image: Services Source Address Destination Address Image: Services Source Address Any Image: Services Sourc	Number Number Context Reset Context Reset Enable From Zone To Zone Services StuPrn LAN SSLVPN VAN SSLVPN VOICE SSLVPN VOICE SSLVPN VOICE SSLVPN VOICE SSLVPN VOICE LAN DMZ UAN VAN UAN UAN UAN OUEST LAN OUEST	Result Result Result Code: Result Result Enable From Zone To Zone SSLVPN LAN sshpn2esion0 X SSLVPN MAN SSLVPN DMX sshpn2esion0 X SSLVPN MAN SSLVPN DMX sshpn2esion0 X SSLVPN VMN SSLVPN VMN SSLVPN VMN SSLVPN VMN SSLVPN VOICE LAN DMZ ILAN OUEST LAN OUEST LAN OUEST LAN OUEST LAN OUEST LAN OUEST	Rest Rest Services SUPPN LAN SshynDession0 Any Destination Address Hit Count Log Action Imable From Zone To Zone Services Source Address Destination Address Hit Count Log Action Image: Signature SsluPN LAN sshynDession0 Any Derry Derry Derry Derry SsluPN Derry SsluPN Derry Derry Derry Derry SsluPN VDMZ SshynDession0 Any Derry Derry Derry SsluPN VDMZ SshynDession0 Any Derry Derry Derry Derry Derry SsluPN VDICE SshynDession0 Any Derry Derry Derry Derry Derry Derry Derry Derry SsluPN Derry Derry SsluPN Derry Derry Derry Derry Derry Derry Derry Derry SsluPN Derry Derry Derry Derry Derry	Name Rest Rest Coste: Ray Rest Enable From Zone To Zone Services SSLVPN LAN SstynnBession0 Any 2 SSLVPN VAN SstynnBession0 2 SSLVPN MAX SstynnBession0 2 SSLVPN VAN SstynnBession0 2 SSLVPN VAN SstynnBession0 2 SSLVPN VAN SstynnBession0 2 SSLVPN VAN SstynnBession0 2 SSLVPN VOICE SstynnBession0 3 SSLVPN VOICE SstynnBession0 2 LAN DMZ Permit 0 2 LAN QUEST SstynnBession0 Permit 2 LAN QUEST Permit 0 2 LAN QUEST Permit 0 2 LAN QUEST Permit 0 2 LAN	Province Province Source Address Destination Address Hit Count Log Action Detail Configure Enable From Zone To Zone Services Source Address Destination Address Hit Count Log Action Detail Configure Image: Status in Address Status in Address Hit Count Log Action Detail Configure Image: Status in Address Image: Status

Configuring Advanced Settings

This section provides information on using the advanced features on the ISA500. It includes the following:

- Advanced Configuration Settings
- Configuring the Cisco SPA525G with the ISA500
- Configuring Content Filtering Policies

Advanced Configuration Settings

These are the advanced (optional) configuration settings that are available for SSL VPN. You can configure these settings from the **Remote Access VPN Wizard** or from the **VPN > SSL Remote User Access > SSL VPN Configuration** page.

- Idle Timeout: Timeout value in seconds that the SSL VPN session remains idle after the ISA500 terminated the session. The default value is 2100 seconds.
- Session Timeout: Timeout value in seconds that a SSL VPN session can remain active. Set this value to a larger value to avoid terminating the session. The default value is 0 seconds, which keeps the SSL VPN session always active.
- Client DPD Timeout: Dead Peer Detection (DPD) allows detection and termination of inactive SSL VPN sessions. This timeout is configured on the remote client during the SSL VPN tunnel set up. If the session is nonresponsive for the period of the timeout value, the remote client will terminate the session. The default value is 300 seconds.
- Gateway DPD Timeout: If the SSL VPN session is unresponsive more than twice the amount of the DPD timeout value, the ISA500 will terminate the session. The default value is 300 seconds.
- **Keep Alive**: Timeout set on the remote client. A timeout interval periodically sends the Keep Alive packets to the ISA500 to indicate that it is active. The default value is 30 seconds.
- Lease Duration: Amount of time after which the SSL VPN client must send an IP address lease renewal request to the server. The default value is 43200 seconds.
- Max MTU: Maximum transmission unit for the session. The default value is 1406 bytes.
- **Rekey Interval**: Time interval for which the remote client negotiates with the ISA500 to rekey the session key. The default value is 3600 seconds

Configuring the Cisco SPA525G with the ISA500

You can create a secure VPN connection between the ISA500 and the Cisco SPA525G phone. The SPA525G has an embedded SSL VPN client that can be used to establish SSL VPN connections to the ISA500.

- Step 1. Log on to the SPA525G configuration utility.
- Step 2. Click the Information and Settings button.
- Step 3. Choose number 3 Network Configuration.



Step 4. Click the **VPN** option.



Step 5. Enter the **VPN Server**, **User Name**, and **Password** under VPN Settings. Leave the Tunnel Group field blank.



- Step 6. Check the **Connect on Bootup** box to establish a VPN connection every time that the phone boots up.
- Step 7. Click Set to save your settings.
- Step 8. Check the Enable Connection box to establish the SSL VPN connection.

The VPN connection is successful.

2 20	UPN
PN Status	States of the local division of the local di
VPN Connected	Yes
IP Address	192.168.200.7
Subnet Mask	255.255.255.255
Bytes Send	3786
Bytes Recv	5040
ownloading:SEP0025	84060DCC.enf.xml
Refresh	Back

You can also verity the connection from the ISA500 Configuration Utility by choosing **VPN > VPN Status** > **SSL VPN Status**. This example shows that the SSL VPN session is now active.



Configuring Content Filtering Policies

You can configure content filtering policies on the ISA500 to specify which websites to block or allow on your network.

Step 1. Choose Firewall > Content Filtering > Content Filtering Policies.

Configuration Wizards	Content Filtering	Policies		
Status	Content Fillering Policies			
Frewall	- the Add			
Access Control	Policy Profile	Description		Tas
ACL Rules	Detault_Profile	Default profile - apply to all zone	es by default	1
Detault Policies	SSLVPN_Profile	Policy for SSL VPN users.		13
Content Filtering Content Filtering Policies Policy to Zone Mapping		Content Filtering Policies - Add/Edit Policy Profile SSLVPN_Profile	Help	1
Advanced Settings		Description : Policy for SSL VPN	Website Access Control List - Add/Edit	Help
Attack Protection		Website Access Control List	Enable content filter urt: On Off 	
Session Limits		nde Add X Delate All	URL: badsite.com	
Application Level Gateway		Number Enable 1101	Match Type: Domain 💌	
		Transie Linker Sta	Action:	
	Save Cancel		Deny C	
				Cox Cancel
Security Services		(a) (b)	until them. (1) Para them	
VPN		For URLS not specified above : Pe	mmit mem O neny mem	
lisers			CK Cose	

- Step 2. Click **Add** to create a new policy profile.
- Step 3. In the Content Filtering Policies page, click Add
- Step 4. Under the Website Access Control List, specify the website URLs that you want to allow or block.
- Step 5. Click **OK** to save the new profile.
- Step 6. To map the content filtering policy profile to the SSL VPN zone, choose Content Filtering > Policy to Zone Mapping. Choose the content filtering policy for the SSL VPN zone and click Save.

Troubleshooting

The following is a list of problems that might occur when AnyConnect client fails to connect to the ISA500:

- WAN Connection is Down
- Remote Client Cannot Reach the ISA500 WAN Interface
- Wrong Username and Password Combination
- Active Directory or RADIUS Server is Unresponsive
- Accessibility Issues

NOTE If logging is enabled on the ISA500, you can use the information in the syslogs for troubleshooting purposes. See Troubleshooting Using Log Files, page 28.

WAN Connection is Down

Verify that your ISA500 is securely connected, or contact your Internet Service Provider (ISP) to resolve the issue.

Remote Client Cannot Reach the ISA500 WAN Interface

Step 1. Uncheck the Block Ping WAN Interface option from the Firewall > MAC Filtering > Attack Protection. This option is typically used to prevent attackers from discovering your network through ICMP Echo (ping) requests.

Configuration Wizards	Attack Protection					
Status	MRN Country Charles					
Networking	WAN Security Checks	~				
Firewall	Block Ping WAN Interface					
Access Control	Stealth Mode					
ACL Rules Default Policies	Block TCP Flood					
NAT	LAN Security Checks	WAN Security Checks				
Content Filtering MAC Filtering	Block UDP Flood					
Attack Protection Session Limits	Firewall Settings					
Application Level Gateway	Block ICMP Notification					
	Block Fragmented Packs	its				
	Block Multicast Packets					
	DoS Attacks					
	SYN Flood Detect Rate:	128	max/sec (Range: 0-10000, Default: 128)			
	Echo Storm:	15	ping pkts/sec (Range: 0~10000, Default 15)			
	ICMP Flood	100	ICMP pkts/sec (Range: 0~10000, Default: 100)			

Step 2. Use the Diagnostic Utilities (**Device Management >Diagnostic Utilities > Ping**) to check the network connectivity between the remote client and the ISA500. Enter the client's **IP Address** and **Number of Pings** and click **Start**. The results appear in the pane below.

Configuration Wizards	Ping	
Status	Dira Cattinus	
Networking	Ping Settings	
Wireless	* IP Address or URL: 128.107.229.220	
Firewall	Packet Size: 32 bytes (Range: 32-65500)	
Security Services		
VPN		
Users	Start Stop	
Device Management	Baselita	
oysenin status Processes Resource Utilization Administration Backup/Restore Certificate Management Cisco Services & Support Date and Time Device Properties Diagnostic Utilities Ping Traceroute DNS Lookup Packet Capture Discovery Protocols Firmware	PING 128.107.229.220 (128.107.229.220) 32(60) bytes of data. From 172.16.100.10 icmp_seq=1 Destination Host Unreachable From 172.16.100.10 icmp_seq=2 Destination Host Unreachable From 172.16.100.10 icmp_seq=3 Destination Host Unreachable From 172.16.100.10 icmp_seq=4 Destination Host Unreachable From 172.16.100.10 icmp_seq=4 Destination Host Unreachable From 172.16.100.10 icmp_seq=4 Destination Host Unreachable From 172.16.100.10 icmp_seq=5 Destination Host Unreachable From 172.16.100.10 icmp_seq=6 Destination Host Unreachable From 172.16.100.10 icmp_seq=6 Destination Host Unreachable From 172.16.100.10 icmp_seq=6 Destination Host Unreachable	
License Management		
Logs		

Wrong Username and Password Combination

Check the local database, Active Directory server, or RADIUS server to retrieve or update the username and password.

Active Directory or RADIUS Server is Unresponsive

Check the connectivity between the Active Directory or RADIUS server and the ISA500. Check the logs for more information. See Troubleshooting Using Log Files, page 28.

SSL VPN Session Terminated Due to Idle Timeout or Session Timeout

Increase the idle timeout and session timeout values from the VPN > Remote User Access > SSL VPN Configuration page.

Accessibility Issues

These problems might happen if the remote client is unable to reach the resources on ISA500 LAN after the SSL VPN connection is established.

Resources on the ISA500 LAN Not Accessible

Check the connectivity of the hosts on the ISA500 LAN by using the Ping option form the **Device Management >Diagnostic Utilities > Ping** page.

Wrong DNS is Configured

Make sure that the ISA500 IP address is configured as the primary DNS in the Basic Settings tab under **VPN > SSL Remote User Access > SSL VPN Group Policies**. Otherwise, resolve any DNS server issues with the DNS IP address configured on the WAN settings.

Troubleshooting Using Log Files

You can turn on specific VPN logs for more details if problems occur when establishing a VPN connection.

Step 1. To enable logging, choose **Device Management > Logs > Log Settings** and then click **On** to enable the Log feature.

	a Cottinga		
LO	g settings		
	Log Settings		
	Log: On O) Off	
*	Log Buffer: 409600	bytes (Range:100000-10000000, I	Default 409600)
	System Logs		
	Unicast Traffic:	🔿 On 💿 Off	Log Settings
	Broadcast/Multicast Tr	raffic: 🔿 On 💿 Off	
	Local Log		
1	Severity: Critical		
1			
	Email Server		
		Set Email Alert	
	Email Alert:	On Off	
	From Email Address:		
	To Email Address:		
	SMTP Server:		
	SMTP Authentication:	🔘 On 🖲 Off	
*	Mail Subtitle:	[Syslog]	Range:0-127
	Severity:	Warning 💌	
	Email Schedule		
	Frequency: Hourly	¥	
	Day: Monday		
		hear (

- Step 2. Choose the **Severity** level for the events that you want to log and click **Save**. For example: If you select Critical, all logs listed under the Critical, Emergency, and Alert categories are saved to the local syslog.
- Step 3. Choose **Log Facilities** and verify that the SSL VPN option is enabled under Local Log. If the syslog server is configured, click the **Remote Log** box.
- Step 4. Click **Save** to apply your settings.

Log Facilities			
Name	🗌 Email Alert	🗌 Remote Log	🔲 Local Log
Kernel	V		V
System	1	V	
Firewall			
NAT			
Network			
Site-to-Site VPN			
IPsec Remote Access			
Teleworker VPN Client			
SSL VPN			
User			
License			
Intrusion Prevention (IPS)			
Application Control			
Anti-Virus			
Web URL Filtering			
Web Reputation			
Network Reputation			
Spam Filter			

Step 5. From the View Logs page, choose **Debug** and **SSL VPN** from the drop-down menus and click **Query**. The log output appears in the Logs table which can then be used for troubleshooting purposes.

select Logs to View					
.og Severity:	Debug 💌				
og Facility.	SSL VPN				
Serword:					
ing in the second second					
Jource IP Address:					
Jestination IP Addres	s:				
Query Cancel					
.ogs					
Lons					
Clear 🔗 Refre	sh 👔 Export				
- Clear 🔗 Refre	severity	Facility	Log Data	Source IP Address	Destination IP Ad
Clear 🔗 Refe Date 2012-05-04	Ceverity Information	Facility SSL VPN	Log Data msg-INFO ssilven, tuni, main c 994 A tunnel established	Source IP Address	Destination IP Ad.
	Copert Seventy Information	Facility SSL VPN SSL VPN	Log Data msg=NPC sslopn_tuni _main c 944 Atunnel established successtully Tunnel IP[192:168 200 8]; msg=NPC sslopn_appl c 295 Received user credentials. User:	Source IP Address	Destination IP Ad.
Clear Refre Date 2012-05-04 00:48:42 2012-05-04 00:48:08 2012-05-04 00:45:08	Ceventy Seventy Information Information Information	Facility SSL VPN SSL VPN SSL VPN	Log Data msg=NPO sshpn_binl_main c 994 Atunnel established successfully. Tunnel IP 1192.168.200.8): msg=NPO sshpn_appic 2.058 Received user credentials. User: jdoe. Sent for authentication. msg=NPO sshpomprc. 198 User jdoe authenticated successfully.	Source IP Address	Destination IP Ad
Clear Refre Date 2012-05-04 00:48:42 2012-05-04 00:48:08 2012-05-04 00:48:08 2012-05-04 00:48:08 2012-05-04	Content of the second of	Facility SSL VPN SSL VPN SSL VPN SSL VPN	Log Data msg-iNFO eshon, Lini, main c 994 A turnel established successfully. Turnel IP 1192 168 200 a), msg-iNFO solyon, zept c 205 Received user credentials. User: jobo. Sent for authentication msg-iNFO solyonmjrc. 198 User jobe authenticated successfully. Sending confirmation.; usersrides from=220.0 0 2 Jobin. resultSUCCESS.	Source IP Address	Destination IP Ad
Clear Roho Date 2012-05-04 0048/34 2012-05-04 0048/38 2012-05-04 0048/38 2012-05-04 0048/38 2012-05-04	Export Seventy Information Information Information Information Information	Facility SSL VPN SSL VPN SSL VPN SSL VPN SSL VPN	Log Data msg-sNRO rshpm, tinl ,main: c.964 A turnel established mspestNRO rshpm, pinl: 2158 200 (3); msg-sNRO rshpm, zept c.958 Review user credentials. User: jdop. Sent for authentication; msg-sNRO sshpm; zer, 198 User jdoe authenticated successfully. Sending confirmation; user=jdoe, from =220 0.0.2 jogin_result=SUCCESS; msg-sNRO sshpm; zer, 155 Client ik Aw/conset;	Source IP Address	Destination IP Ad

For More Information

Product Resources	Location
Product Documentation	www.cisco.com/go/isa500resources
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Cisco Small Business Support and Resources	www.cisco.com/go/smallbizhelp
Phone Support Contacts	www.cisco.com/go/sbsc
Firmware Downloads	www.cisco.com/go/isa500software
Cisco Partner Central for Small Business (Partner Login Required)	www.cisco.com/web/partners/sell/smb
Cisco Small Business Home	www.cisco.com/smb

Cisco, Cisco Systems, the Cisco logo, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. All other trademarks mentioned in this document or Website 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. (0705R)

© 2012 Cisco Systems, Inc. All rights reserved. 78-21034-01