# ASA 8.x : Allow Split Tunneling for AnyConnect VPN Client on the ASA Configuration Example

## Contents

Introduction Prerequisites Requirements Components Used Conventions Background Information Configure Network Diagram ASA Configuration Using ASDM 6.0(2) ASA CLI Configuration Establish the SSL VPN Connection with SVC Verify Troubleshoot Related Information

# **Introduction**

This document provides step-by-step instructions on how to allow Cisco AnyConnect VPN client access to the Internet while they are tunneled into a Cisco Adaptive Security Appliance (ASA) 8.0.2. This configuration allows the client secure access to corporate resources via SSL while giving unsecured access to the Internet using split tunneling.

# **Prerequisites**

## **Requirements**

Ensure that you meet these requirements before you attempt this configuration:

- ASA Security Appliance needs to run version 8.x
- Cisco AnyConnect VPN Client 2.x**Note:** Download the AnyConnect VPN Client package (anyconnect-win\*.pkg) from the Cisco <u>Software Download</u> (<u>registered</u> customers only). Copy the AnyConnect VPN client to the ASA's flash memory, which is to be downloaded to the remote user computers in order to establish the SSL VPN connection with the ASA. Refer to the <u>Installing the AnyConnect Client</u> section of the ASA configuration guide for more information.

## **Components Used**

The information in this document is based on these software and hardware versions:

- Cisco 5500 Series ASA that runs software version 8.0(2)
- Cisco AnyConnect SSL VPN Client version for Windows 2.0.0343
- PC which runs Microsoft Visa, Windows XP SP2 or Windows 2000 Professional SP4 with Microsoft Installer version 3.1
- Cisco Adaptive Security Device Manager (ASDM) version 6.0(2)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

### **Conventions**

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

## **Background Information**

The Cisco AnyConnect VPN Client provides secure SSL connections to the security appliance for remote users. Without a previously installed client, remote users enter the IP address in their browser of an interface configured to accept SSL VPN connections. Unless the security appliance is configured to redirect http:// requests to https://, users must enter the URL in the form https://<address>.

After entering the URL, the browser connects to that interface and displays the login screen. If the user satisfies the login and authentication, and the security appliance identifies the user as requiring the client, it downloads the client that matches the operating system of the remote computer. After downloading, the client installs and configures itself, establishes a secure SSL connection and either remains or uninstalls itself (depending on the security appliance configuration) when the connection terminates.

In the case of a previously installed client, when the user authenticates, the security appliance examines the revision of the client and upgrades the client as necessary.

When the client negotiates an SSL VPN connection with the security appliance, it connects using Transport Layer Security (TLS), and optionally, Datagram Transport Layer Security (DTLS). DTLS avoids latency and bandwidth problems associated with some SSL connections, and improves the performance of real-time applications that are sensitive to packet delays.

The AnyConnect client can be downloaded from the security appliance, or it can be installed manually on the remote PC by the system administrator. Refer to <u>Cisco AnyConnect VPN Client</u> <u>Administrator Guide</u> for more information on how to install the client manually.

The security appliance downloads the client based on the group policy or username attributes of the user establishing the connection. You can configure the security appliance to automatically download the client, or you can configure it to prompt the remote user about whether to download the client. In the latter case, if the user does not respond, you can configure the security appliance to either download the client after a timeout period or present the login page.

# **Configure**

In this section, you are presented with the information to configure the features described in this document.

**Note:** Use the <u>Command Lookup Tool</u> (<u>registered</u> customers only) to obtain more information on the commands used in this section.

#### **Network Diagram**

This document uses this network setup:



**Note:** The IP addressing schemes used in this configuration are not legally routable on the Internet. They are <u>RFC 1918</u> addresses which have been used in a lab environment.

### ASA Configuration Using ASDM 6.0(2)

This document assumes that the basic configuration, such as interface configuration, is already made and works properly.

**Note:** Refer to <u>Allowing HTTPS Access for ASDM</u> in order to allow the ASA to be configured by the ASDM.

**Note:** WebVPN and ASDM cannot be enabled on the same ASA interface unless you change the port numbers. Refer to <u>ASDM and WebVPN Enabled on the Same Interface of ASA</u> for more information.

Complete these steps in order to configure the SSL VPN on ASA with split tunneling:

1. Choose Configuration > Remote Access VPN > Network (Client) Access > Address Management > Address Pools > Add in order to create an IP address pool

	🔂 Add IP Pool	
	Name:	vpnpool
	Starting IP Address:	192.168.10.1
	Ending IP Address:	192.168.10.254
	Subnet Mask:	255.255.255.0
vpnpool.	ок	Cancel Help

- 2. Click Apply.Equivalent CLI Configuration:
- 3. Enable WebVPN.Choose Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles and under Access Interfaces, click the check boxes Allow Access and Enable DTLS for the outside interface. Also, check the Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interface selected in the table below check box in order to enable SSL VPN on the outside interface.

Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles

The security appliance automatically deploys the Cisco AnyConnect VPN Client or legacy SSL VPN Client to client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports the Layer Security (DTLS) tunneling options.

(More client-related parameters, such as client images and client profiles, can be found at <u>Client Settings</u>

Access Interfaces								
Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interfaces selected in the								
Interface	Allow Access	Require Client Certificate	Enable DTLS					
outside								
inside								
Access Port: 443 DTLS Port: 443								
Click here to <u>Assign</u>	Certificate to Interface.							

Click Apply.Choose Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings > Add in order to add the Cisco AnyConnect VPN

# client image from the flash memory of ASA as shown.

🕵 Add SSL YPN Client Image		X SSL VPN > Clie	ent Settings
Flash SVC Image:	Browse Flash	2	
	Upload	buntered operat	ion system to the top of the
🚰 Browse Flash			×
Folders	Files		
E- e disk0:	FileName 🗡	Size (bytes)	Date Modified
🔄 🕂 🔁 log	Crypto archive		07/24/07 05:21:48
			07/24/07 05:21:36
	asdm-603.bin	6,851,212	01/04/08 18:07:02
	asa803-k8.bin	14,635,008	01/04/08 17:49:50
	admin.cfg	1,220	09/20/07 09:51:38
	anyconnect-win-2.0.03	2,635,734	08/13/07 04:14:50
	asdm-602.bin	6,889,764	01/03/08 21:38:26
	asa722-k8.bin	8,312,832	02/13/07 04:16:30
	asdm-522.bin	5,623,108	02/12/07 05:53:48
	asa802-k8.bin	14,524,416	01/03/08 21:24:42
	old_running.cfg	1,841	09/20/07 09:51:38
	sslclient-win-1.1.4.179	418,765	03/14/08 13:47:58
File Name:	anyconnect-win-2.0.0343-k9.p	kg	
	Client Image		
Auu SSL TPN	chencimaye		Í
Flash SVC Image	ct-win-2.0.0343-k9.pkg	Browse Flash	
		Upload	
	-	opiodarii	-
	Cancel	Help	
Click OK.			Click
Add.			

Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings							
Identify SSL VPN Client (SVC) related files.							
SSL VPN Client Images							
Minimize connection setup time by moving the image used by the most commonly encountered operation system to t							
Add Replace 🗊 Delete 🛧 Move UP 🗲 Move Down							
disk0: /apvcoppect-wip-2.0.0343-k9.pkg							

#### **Equivalent CLI Configuration:**

4. Configure Group Policy.Choose Configuration > Remote Access VPN > Network (Client) Access > Group Policies in order to create an internal group policy clientgroup. Under the General tab, select the SSL VPN Client check box in order to enable the WebVPN as tunneling

pr	otocol.	
	Add Internal Group Policy	
	(Seneral) Servers	Name: Clientgroup
Ē	⊟—Advanced —Split Tunneling	Banner: 🔽 Inherit
	E Browser Proxy	Address Pools: 🔽 Inherit
	IPsec Client	More Options
		Tunneling Protocols: 🔲 Inherit 📄 Clientless SSL VPN 🔽 SSL VPN Client 📄 IPsec

In the **Advanced > Split Tunneling** tab, uncheck the **Inherit** check box for Split Tunnel Policy and chose **Tunnel Network List Below** from the drop down



Uncheck the Inherit check box for Split Tunnel Network List and then click Manage in order to launch the ACL

Manager. 📬 Edit Internal Group Policy: hivalleyvpn Split tunneling network lists distinguish networks that require traffic to go through the tunnel and those that do not General require tunneling. The security appliance makes split tunneling decisions on the basis of a network list, which is an Servers ACL that consists of list of addresses on the private network. -Advanced Split Tunneling DNS Names: 🔽 Inherit IE Browser Proxy € -SSL VPN Client Inherit Tunnel Network List Below Policy: -- IPsec Client Client Access Rule Network List: [ Inherit -- None --¥ (Manage...) Client Firewall Hardware Client

Within the ACL Manager, choose **Add > Add ACL...** in order to create a new access list.

<u>1</u>	ACL Manager				
ſ	Standard ACL Extended	ACL			
	🔂 Add 🕞 📝 Edit 📋	Delete 🛧 🗲	* * * ®	*	
🔂 Add ACL					
	🔂 Add ACL	dress	Action	Description	
	<ul> <li>Add ACL</li> <li>Add ACE</li> </ul>	dress	Action	Description	
	<ul> <li>Add ACL</li> <li>Add ACE</li> <li>Insert</li> </ul>	dress	Action	Description	

#### Provide a name for the ACL and click

OK.							
🔂 ACL Mar	ager						
Standard	ACL Extended ACL	]					
🔂 Add	💠 Add 👻 🗹 Edit: 📋 Delete 🛧 🗲 🕉 🐚 🛍 👻						
No	Address	s Action	Description				
🔂 Ade	I ACL						
ACL	Name: split-tunnel						
	ок	Cancel Hel	ql				

Once the ACL name is created, choose Add > Add ACE in order to add an Access Control Entry (ACE).Define the ACE that corresponds to the LAN behind the ASA. In this case, the network is 10.77.241.128/26 and select **Permit** as the Action.Click **OK** in order to exit the ACL

Manager.

No	Address	Action	Description	
split-tunnel				
🔄 Add ACE				
Host/Netw	/ork			
IP Addre	ss: 10.77.241.128			<b>•</b>
Netmask	: 255.255.255.192			<b>v</b>
Description				
Description:				

Make sure that the ACL you just created is selected for the split-tunnel Network List. Click **OK** in order to return to the Group Policy

configuration.

📸 Add Internal Group Policy				X
General Servers Advanced <u>Splt Tunneling</u> IE Browser Proxy E-SSL VPN Client F-IPsec Client	Split tunneling network lists require tunneling. The secu ACL that consists of list of a DNS Names: I Inherit Policy: Inherit	s distinguish networks that req urity appliance makes split tunn addresses on the private netw	uire traffic to go through th eling decisions on the basis ork.	e tunnel and those that do not of a network list, which is an
	Network List: 🥅 Inherit	split-tunnel		Manage
	Intercept DHCP Config	guration Message from Mi	cosoft Clients	*

On the main page, click **Apply** and then Send (if required) in order to send the commands to the ASA.Configure the **SSL VPN** settings under Group policy mode.For the Keep Installer on Client System option, uncheck the **Inherit** check box, and click the **Yes** radio button.This action allows the SVC software to remain on the client machine. Therefore, the ASA is not required to download the SVC software to the client each time a connection is made. This option is a good choice for remote users who often access the corporate network.

🚘 Edit Internal Group Policy: clientgroup						
General	Keep Installer on Client System:	🔲 Inherit	• Yes	C No		
-Servers	Compression:	🔽 Inherit	C Enable	C Disab		
	Datagram TLS:	🔽 Inherit	C Enable	C Disab		
Cogin Setting	Keepalive Messages:	🔽 Inherit	🗖 Disable	Interval:		

Click Login Setting in order to set the Post Login Setting and Default Post Login Selection as

shown.

J		
	General	<ul> <li>After successfully logging in, user can have the choice to download the client software, or g portal page. The following settings decides what will happen.</li> </ul>
	-Servers -Advanced	
	-Split Tunneling	
	IE Browser Proxy	Post Login Setting —
	-SSL VPN Client -SSL VPN Client -Login Setting	Do not prompt user to choose
Key Regeneration Dead Peer Detecti		C Prompt user to choose
		User has seconds to choose, or Default Post Login Selection below is take
		Default Post Login Selection
		C Go to Clientless SSL VPN portal
		Download SSL VPN Client

For the Renegotiation Interval option, uncheck the **Inherit** box, uncheck the **Unlimited** check box, and enter the number of minutes until rekey.Security is enhanced by setting limits on the length of time a key is valid.For the Renegotiation Method option, uncheck the **Inherit** check box, and click the **SSL** radio button.Renegotiation can use the present SSL tunnel or a new tunnel created expressly for

renegotiation.

General	Renegotiation Interval:	🔲 Inherit	🔲 Unlimited	30	minutes
-Servers			-		
🖻 - Advanced	Renegotiation Method:	🔲 Inherit	O None	💿 SSL )	🔘 New Tunnel
-Split Tunneling					
-IE Browser Proxy					
🖨 SSL VPN Client					
Login Setting Key Regeneration	)				
Click OK and then					

Apply.

Co	nfiguration > Remote Access VPN	> Net	work (Client) Access	• Group Policies					
	Manage VPN group policies. A VPN grou externally on a RADIUS/LDAP server. T	riented attribute/val eferenced by VPN tu	ue pairs that may be sto nnel groups and user acc	red inter counts.					
	🗣 Add 🔻 🗹 Edit 📋 Delete	Add 🗸 🗹 Edit 📋 Delete							
	Name		Туре	Tunneling Protocol					
	clientgroup	$\overline{)}$	Internal	svc		N/A -			
	DfltGrpPolicy (System Default)		Internal	L2TP-IPSec, IPSec, w	ebvpn	N/A -			

### Equivalent CLI Configuration:

5. Choose **Configuration > Remote Access VPN > AAA Setup > Local Users > Add** in order to create a new user account **ssluser1**. Click **OK** and then

Apply. Add User Account	
Untity → VPN Policy	Username: ssluser1 Password: ******* Confirm Password: ******
	User authenticated using MSCHAP
	Member-of
	Member-of: Add >> Delete
	Access Restriction
	Select one of the options below to restrict ASDM, SSH, Telnet and Console access.
	Eull access(ASDM_SSH_Telpet and Console)
	Privilege level is used with command authorization
	Privilege Level: 2
	CLI login prompt for SSH, Telnet and console (no ASDM access)
	This setting is effective only if AAA authenticate console command is configured.
	No ASDM, SSH, Telnet or Console access
	This setting is effective only if AAA authenticate console command is configured.

#### Equivalent CLI Configuration:

 Choose Configuration > Remote Access VPN > AAA Setup > AAA Servers Groups > Edit in order to modify the default server group LOCAL by checking the Enable Local User Lockout check box with maximum attempts value as 16.

Configurati	on > Remote /	Access VPN > AA	A Setup > AAA Server	Groups	
AAA Serve	er Groups —				
Ser	ver Group	Protocol	Accounting Mode	Reactivation Mode	
LOCAL		LOCAL			
	This feature before lockin when the loc Enable Lo Maximum	L Server Group allows you to speci g out and denying al database is used ocal User Lockout Attempts: 16	fy the maximum number of access to the user. This I for authentication.	of failed attempts to allov imit is applicable only Help	×

- 7. Click **OK** and then **Apply.Equivalent CLI Configuration:**
- 8. Configure Tunnel Group.Choose Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles Connection Profiles > Add in order to create a new tunnel group sslgroup.In the Basic tab, you can perform the list of configurations as shown:Name the Tunnel group as sslgroup.Under Client Address Assignment, choose the address pool vpnpool from the drop down list.Under Default Group Policy, choose the group policy clientgroup from the drop down list

inc				
	Add SSL VPN Connection	Profile		
	<mark>⊕Basid)</mark> ⊡–Advanced	Name: Aliases:	ssigroup	
		Authentication ——		
		Method:	👁 AAA 🔿 Certificate 🔿 Both	
		AAA Server Group:	LOCAL	Manag
			Use LOCAL if Server Group fails	
		Client Address Assign	ment	
		DHCP Servers:		
		Client Address Pools:	vpnpool	Select
		Default Group Policy		
		Group Policy:	clientgroup	Manag
		SSL VPN Client Protoco	ol: 🔽 Enabled	
		OK	Cancel Help	

Under the **SSL VPN > Connection Aliases** tab, specify the group alias name as **sslgroup\_users** and click

Add SSL VPN Connection	Profile
Basic	Portal Page Customization: DfltCustomization
General	CSD Alternate Group Policy: DfltGrpPolicy
Client Addressing Authentication	Enable the display of Radius Reject-Message on the
-Authorization -Accounting	Connection Aliases
	🔁 Add 🗹 Delete
	Add Connection Alias
	Alias: sslgroup_users
	Enabled
	OK Cancel Help
	🕂 Add 🗹 Delete

OK.

- OK and then Apply.Equivalent CLI Configuration:
- 9. Configure NAT.Choose **Configuration > Firewall > NAT Rules > Add Dynamic NAT Rule** so the traffic that comes from the inside network can be translated with outside IP address 172.16.1.5.

¢,	Add D	ynamic	NAT Ru	e												
C	Driginal	I —														
	Interfa	ace: linsi	de						-	]						
	Source	e: Jany							-	]						
1	ransla	ted —														
	Select	a global j	pool for d	lynamic tra	nslatior	٦.										
	Po	ool ID		Interf	ace						Addres	sses Poo	bl			
	0		(outbou	nd)				Same a	s oriç	ginal a	address	(identit	y)			
	-0-		(inbound	<del>1) (t</del>				<del>Same a</del>	s orig	<del>jina</del> l i	address	(identit	y)			
	1		outside					📙 172	2,16,	1.5				Click		
OI OI	<b>∢</b> .Click <b>∢</b> .													onon		
Co	onfigura	tion > Fire	ewali > N/	AT Rules												
	🔂 Add	🝷 📝 Ed	lit <u> î</u> De	elete 🛉 🛧	4	¥			Q	Find	👥 Diag	gram 🥰	🛛 Pacł	ket Tra	асе	
Γ		т.					Origin	nal								
	*	ڊ ا ا	he	So	urce		De	estination	า	Se	ervice	Int	erface			
I	∃ inside (	(1 Dynamic	: rules)													
	1	📲 Dynar	mic	🏈 any								outside				

#### Click Apply.Equivalent CLI Configuration:

10. Configure the nat-exemption for the return-traffic from inside network to the VPN

Client.ciscoasa(config)#access-list nonat permit ip 10.77.241.0 192.168.10.0
ciscoasa(config)#access-list nonat permit ip 192.168.10.0 10.77.241.0 ciscoasa(config)#nat
(inside) 0 access-list nonat

### **ASA CLI Configuration**

#### Cisco ASA 8.0(2)

ciscoasa(config)#**show running-config** : Saved : ASA Version 8.0(2) ! hostname ciscoasa domain-name default.domain.invalid enable password 8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0/0 nameif inside security-level 100 ip address 10.77.241.142 255.255.255.192 ! interface Ethernet0/1 nameif outside security-level 0 ip address 172.16.1.1 255.255.255.0 ! interface Ethernet0/2 shutdown no nameif no securitylevel no ip address ! interface Ethernet0/3 shutdown no nameif no security-level no ip address ! interface Management0/0 shutdown no nameif no security-level no ip address ! passwd 2KFQnbNIdI.2KYOU encrypted boot system disk0:/asa802-k8.bin ftp mode passive clock timezone IST 5 30 dns server-group DefaultDNS domain-name default.domain.invalid access-list split-tunnel standard permit 10.77.241.128 255.255.255.192 !--- ACL for Split Tunnel network list for encryption. access-list nonat permit ip 10.77.241.0 192.168.10.0 access-list nonat permit ip 192.168.10.0 10.77.241.0 !--- ACL to define the traffic to be exempted from NAT. pager lines 24 logging enable logging asdm informational mtu inside 1500 mtu outside 1500 ip local pool vpnpool 192.168.10.1-192.168.10.254 mask 255.255.255.0 !--- The address pool for the Cisco AnyConnect SSL VPN Clients no failover icmp unreachable rate-limit 1 burst-size 1 asdm image disk0:/asdm-602.bin no asdm history enable arp timeout 14400 global (outside) 1 172.16.1.5 !--- The global address for Internet access used by VPN Clients. !--- Note: Uses an RFC 1918 range for lab setup. !---Apply an address from your public range provided by your ISP. nat (inside) 0 access-list nonat !--- The traffic permitted in "nonat" ACL is exempted from NAT. nat (inside) 1 0.0.0.0 0.0.0.0 route outside 0.0.0.0 0.0.0.0 172.16.1.2 1 timeout xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip\_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute dynamic-access-policy-record DfltAccessPolicy http server enable http 0.0.0.0 0.0.0.0 inside no snmp-server location no snmp-server contact snmp-server enable traps snmp authentication linkup linkdown coldstart no crypto isakmp nat-traversal telnet timeout 5 ssh timeout 5 console timeout 0 threatdetection basic-threat threat-detection statistics access-list ! class-map inspection\_default match default-inspection-traffic ! ! policy-map type inspect dns preset\_dns\_map parameters message-length maximum 512 policy-map global\_policy class inspection\_default inspect dns preset\_dns\_map inspect ftp inspect h323 h225 inspect h323 ras inspect netbios inspect rsh inspect rtsp inspect skinny inspect esmtp inspect sqlnet inspect

```
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
policy global_policy global webvpn enable outside !---
Enable WebVPN on the outside interface svc image
disk0:/anyconnect-win-2.0.0343-k9.pkg 1 !--- Assign an
order to the AnyConnect SSL VPN Client image svc enable
!--- Enable the security appliance to download SVC
images to remote computers tunnel-group-list enable !---
Enable the display of the tunnel-group list on the
WebVPN Login page group-policy clientgroup internal !---
Create an internal group policy "clientgroup" group-
policy clientgroup attributes vpn-tunnel-protocol svc !-
-- Specify SSL as a permitted VPN tunneling protocol
split-tunnel-policy tunnelspecified split-tunnel-
network-list value split-tunnel !--- Encrypt the traffic
specified in the split tunnel ACL only webvpn svc keep-
installer installed !--- When the security appliance and
the SVC perform a rekey, they renegotiate !--- the
crypto keys and initialization vectors, increasing the
security of the connection. svc rekey time 30 !---
Command that specifies the number of minutes from the
start of the !--- session until the rekey takes place,
from 1 to 10080 (1 week). svc rekey method ssl !---
Command that specifies that SSL renegotiation takes
place during SVC rekey. svc ask none default svc
username ssluser1 password ZRhW85jZqEaVd5P. encrypted !-
-- Create a user account "ssluser1" tunnel-group
sslgroup type remote-access !--- Create a tunnel group
"sslgroup" with type as remote access tunnel-group
sslgroup general-attributes address-pool vpnpool !---
Associate the address pool vpnpool created default-
group-policy clientgroup !--- Associate the group policy
"clientgroup" created tunnel-group sslgroup webvpn-
attributes group-alias sslgroup_users enable !--
Configure the group alias as sslgroup-users prompt
hostname context
Cryptochecksum:af3c4bfc4ffc07414c4dfbd29c5262a9 : end
ciscoasa(config)#
```

## Establish the SSL VPN Connection with SVC

Complete these steps in order to establish a SSL VPN connection with ASA:

1. Enter the URL or IP address of the ASA's WebVPN interface in your web browser in the format as shown.https://urlORhttps://<IP address of the ASA WebVPN interface>

WebVPN Service - Microsoft	Internet Explorer						
File Edit View Favorites Tool	s Help						
🚱 Back 🔹 🐑 🔹 🛃	🏠 🔎 Search 🤺 Favorites 🤣 🎯 - 🌺 🔜 🦓						
Address 🕘 https://172.16.1.1/+web	vpn+/index.html						
Cisco Systems webVPN	CISCO SYSTEMS WebVPN Service						
	Login						
	Please enter your username and password.						
	USERNAME:						
	PASSWORD:						
	GROUP: sslgroup_users						
	Login Clear						

2. Enter your username and password. Also, choose your respective group from the drop down

		Login	
	Please enter your	r username and password.	
	USERNAME:	ssluser1	
	PASSWORD:	••••••	
	GROUP:	sslgroup_users 🔽	
list as shown.		Login Clear	This

window appears before the SSL VPN connection is established.

Cisco	AnyConnect VPN Client
VPN Client Download Please w	der vait while the VPN connection is established.
	Cancel
🔄 - Microsoft Java	
🗌 - Download	
Connected	Help Cancel N

**ote:** ActiveX software must be installed in your computer before you download the SVC.You receive this window once the connection is established.



3. Click the lock which appears in the task bar of your

	🔏 Cisco AnyCo	nnect VPN Client		
	K Connection	🚯 Statistics 🚕 About		
		cisco		
	Connect to:	172.16.1.1	~	
		Disconnect		
computer.	PN session establi	shed.		This window appears

and provides information about the SSL connection. For example, **192.168.10.1** is the assigned IP by the ASA,

Cisco AnyConnect VPN C	lient 📃 🗖 🔀								
🗞 Connection 🚺 Statistics)	🙈 About								
cisco									
Tunnel State:	Connected								
Client Address: Server Address:	192.168.10.1 172.16.1.1								
Bytes Sent: Bytes Received:	23461 1111								
Time Connected:	00:04:51								
Details.									

etc. VPN session established. Cisco AnyConnect VPN Client Version

This window shows the



information. VPN session established

# **Verify**

Use this section to confirm that your configuration works properly.

The <u>Output Interpreter Tool</u> (<u>registered</u> customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- show webvpn svc—Displays the SVC images stored in the ASA flash memory.ciscoasa#show webvpn svc 1. disk0:/anyconnect-win-2.0.0343-k9.pkg 1 CISCO STC win2k+ 2,0,0343 Mon 04/23/2007 4:16:34.63 1 SSL VPN Client(s) installed
- show vpn-sessiondb svc—Displays the information about the current SSL

CONNECTIONS.ciscoasa#show vpn-sessiondb svc Session Type: SVC Username : ssluser1 Index : 12 Assigned IP : 192.168.10.1 Public IP : 192.168.1.1 Protocol : Clientless SSL-Tunnel DTLS-Tunnel Encryption : RC4 AES128 Hashing : SHA1 Bytes Tx : 194118 Bytes Rx : 197448 Group Policy : clientgroup Tunnel Group : sslgroup Login Time : 17:12:23 IST Mon Mar 24 2008 Duration : 0h:12m:00s NAC Result : Unknown VLAN Mapping : N/A VLAN : none

- show webvpn group-alias—Displays the configured alias for various groups.ciscoasa#show webvpn group-alias Tunnel Group: sslgroup Group Alias: sslgroup\_users enabled
- In ASDM, choose Monitoring > VPN > VPN Statistics > Sessions in order to know the current WebVPN sessions in the ASA.

0	onitoring > VF	N > VPN S	tatistic	s > Sessions	)				
Г	Sessions								
	Remote	City by City			SSL VPN		E-mail Provid	VPN Load Balancin	
	Access	Sile-lu-	Site	Clientless	With Client	Total	E-mail Proxy	VPN LUdu Dalahui	' <sup>9</sup>
	0	0 0 0		0	0	0	0	0	
	Filter By: SSL VPN Client All Sessions Filter								
	Username Group Policy			Group Policy	Proto	col	Log	in Time	Byt
	IP Address clientgr ssluser1 clientgr 192.168.10.1 sslgrou			Connection	Encry	ption	Du	ration	Byt
			roup Ip	Clientless SSL RC4 AES128	-Tunnel DT	17:12:23 IST Mor 0h:03m:31s	194118 192474		

## **Troubleshoot**

This section provides information you can use to troubleshoot your configuration.

1. vpn-sessiondb logoff name <username> —Command to logoff the SSL VPN session for the particular username.ciscoasa#vpn-sessiondb logoff name ssluser1 Do you want to logoff the VPN session(s)? [confirm] Y INFO: Number of sessions with name "ssluser1" logged off : 1 ciscoasa#Called vpn\_remove\_uauth: success! webvpn\_svc\_np\_tear\_down: no ACL

webvpn\_svc\_np\_tear\_down: no IPv6 ACL np\_svc\_destroy\_session(0xB000) Similarly, you can use the **vpn-sessiondb logoff svc** command in order to terminate all the SVC sessions.

2. **Note:** If the PC goes to standby or hibernate mode, then the SSL VPN connection can be terminated.

webvpn\_rx\_data\_cstp webvpn\_rx\_data\_cstp: got message SVC message: t/s=5/16: Client PC is going into suspend mode (Sleep, Hibernate, e tc) Called vpn\_remove\_uauth: success! webvpn\_svc\_np\_tear\_down: no ACL webvpn\_svc\_np\_tear\_down: no IPv6 ACL np\_svc\_destroy\_session(0xA000) ciscoasa#show vpn-sessiondb svc INFO: There are presently no active sessions

#### 3. debug webvpn svc <1-255> — Provides the real time webvpn events in order to establish

```
the session.Ciscoasa#debug webvpn svc 7 webvpn_rx_data_tunnel_connect CSTP state =
HEADER_PROCESSING http_parse_cstp_method() ...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
webvpn_cstp_parse_request_field() ...input: 'Host: 172.16.1.1' Processing CSTP header line:
'Host: 172.16.1.1' webvpn_cstp_parse_request_field() ...input: 'User-Agent: Cisco
AnyConnect VPN Client 2, 0, 0343' Processing CSTP header line: 'User-Agent: Cisco
AnyConnect VPN Client 2, 0, 0343 ' Setting user-agent to: 'Cisco AnyConnect VPN Client 2,
0, 0343' webvpn_cstp_parse_request_field() ...input: 'Cookie:
webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B08B 7D75F4EDEF26' Processing CSTP
header line: 'Cookie: webvpn=16885952@12288@1206098825@D251883E8
625B92C1338D631B08B7D75F4EDEF26' Found WebVPN cookie:
'webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B 08B7D75F4EDEF26' WebVPN Cookie:
'webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B08B7D7 5F4EDEF26'
webvpn_cstp_parse_request_field() ...input: 'X-CSTP-Version: 1' Processing CSTP header
line: 'X-CSTP-Version: 1' Setting version to '1' webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Hostname: tacweb' Processing CSTP header line: 'X-CSTP-Hostname: tacweb'
Setting hostname to: 'tacweb' webvpn_cstp_parse_request_field() ...input: 'X-CSTP-Accept-
Encoding: deflate;q=1.0' Processing CSTP header line: 'X-CSTP-Accept-Encoding:
deflate;q=1.0' webvpn_cstp_parse_request_field() ...input: 'X-CSTP-MTU: 1206' Processing
CSTP header line: 'X-CSTP-MTU: 1206' webvpn_cstp_parse_request_field() ...input: 'X-CSTP-
Address-Type: IPv4' Processing CSTP header line: 'X-CSTP-Address-Type: IPv4'
webvpn_cstp_parse_request_field() ...input: 'X-DTLS-Master-Secret:
CE151BA2107437EDE5EC4F5EE6AEBAC12031550B1812D40
642E22C6AFCB9501758FF3B7B5545973C06F6393C92E59693' Processing CSTP header line: 'X-DTLS-
Master-Secret: CE151BA2107437EDE5EC4F5EE6AE
BAC12031550B1812D40642E22C6AFCB9501758FF3B7B5545973C06F6393C92E59693 '
webvpn_cstp_parse_request_field() ...input: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-
```

CBC3-SHA:DES-CBC-SHA' Processing CSTP header line: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3 -SHA:DES-CBC-SHA' Validating address: 0.0.0.0 CSTP state = WAIT\_FOR\_ADDRESS webvpn\_cstp\_accept\_address: 192.168.10.1/0.0.0 CSTP state = HAVE\_ADDRESS No subnetmask... must calculate it SVC: NP setup np\_svc\_create\_session(0x3000, 0xD41611E8, TRUE) webvpn\_svc\_np\_setup SVC ACL Name: NULL SVC ACL ID: -1 SVC ACL ID: -1 vpn\_put\_uauth success! SVC IPv6 ACL Name: NULL SVC IPv6 ACL ID: -1 SVC: adding to sessmgmt SVC: Sending response Unable to initiate NAC, NAC might not be enabled or invalid policy CSTP state = **CONNECTED** webvpn\_rx\_data\_cstp webvpn\_rx\_data\_cstp: got internal message Unable to initiate NAC, NAC might not be enabled or invalid policy

#### In ASDM, choose Monitoring > Logging > Real-time Log Viewer > View in order to see the real time

#### events.

🔂 Cisco ASDM 6.0 for ASA - 10.77.241.142									
File	<u>V</u> iew <u>T</u> ools Wi <u>z</u> ards <u>W</u> indow <u>H</u> e	p	Look For:						
	Home 🦓 Configuration 🔯 Monitori	9 🔚 Save 🔇 Refresh 🔇 Back 🚫 Forward 🦓 Help							
	Logging 🗗 🕂 🗡	Monitoring > Logging > Real-Time Log Viewer							
ice List	Real-Time Log Viewer	Real-Time Log Viewer							
Dev									
		Click the View button below to start displaying syslog messages in real time. Select the desired logging level to see messages at that severity or higher.							
		Logging Level: Deougging							
		Buffer Limit: 1000							
		View							
		Lanana and a second sec							

This example shows that the SSL session has been established with the head end device.

💼 Real-Time Log Viewer - 10.77.241.142									
Eie Iools Window Help									
💷 Payse   🖹 Copy 🎧 Save 🏭 Clear   🞬 Color Settings   🜓 Create Rule 📷 Show Rule   🔞 Show Details   🦿 Help									
Fiker By: Filter 🗐 Show All Find:									
Severity	Date	Time	Syslog ID	Source IP	Destination IP				
<u>k</u> 6	Mar 21 2008	20:03:36	725007	10.77.233.74		SSL session with client inside:10.77.233.74/1026 terminated.			
A 6	Mar 21 2008	20:03:35	106015	10.77.233.74	10.77.241.142	Deny TCP (no connection) from 10.77.233.74/1026 to 10.77.241.142/44			
<u>4</u> 6	Mar 21 2008	20:03:35	302014	10.77.233.74	10.77.241.142	Teardown TCP connection 700 for inside:10.77.233.74/1026 to NP Identi			
<u>4</u> 6	Mar 21 2008	20:03:35	605005	0.0.0.0	0.0.0.0	Login permitted from 0.0.0.0/1026 to inside:0.0.0.0/https for user "enable			
<u>A</u> 6	Mar 21 2008	20:03:35	725002	10.77.233.74		Device completed SSL handshake with client inside:10.77.233.74/1026			
🔺 6	Mar 21 2008	20:03:35	725003	10.77.233.74		SSL client inside:10.77.233.74/1026 request to resume previous session.			
A 6	Mar 21 2008	20:03:35	725001	10.77.233.74		Starting SSL handshake with client inside: 10.77.233.74/1026 for TLSv1 se			
🔺 6	Mar 21 2008	20:03:35	302013	10.77.233.74	10.77.241.142	Built inbound TCP connection 700 for inside:10.77.233.74/1026 (10.77.23			
1	▲								
%ASA-6 723002 Device completed SSL handshake with remote_device interface_name:IP_address/port The SSL handshake has completed successfully with the remote device.									

## **Related Information**

Cisco 5500 Series Adaptive Security Appliance Support Page

- <u>Release Notes for AnyConnect VPN Client, Release 2.0</u>
- ASA/PIX: Allow Split Tunneling for VPN Clients on the ASA Configuration Example
- <u>Router Allows VPN Clients to Connect IPsec and Internet Using Split Tunneling</u>
   <u>Configuration Example</u>
- PIX/ASA 7.x and VPN Client for Public Internet VPN on a Stick Configuration Example
- <u>SSL VPN Client (SVC) on ASA with ASDM Configuration Example</u>
- <u>Technical Support & Documentation Cisco Systems</u>