ASA 7.2(2):單臂公共網際網路VPN的SSL VPN客 戶端(SVC)配置示例

目錄

 簡介

 必要條件

 需求

 採用元件

 慣例

 背景資訊

 設定

 網路圖表

 使用ASDM 5.2(2)的ASA 7.2(2)配置

 体用SVC建立SSL VPN連線

 驗證

 疑難排解

 相關資訊

<u>簡介</u>

本文檔介紹如何設定自適應安全裝置(ASA)7.2.2以在單臂上執行SSL VPN。此設定適用於特定情況 ,其中ASA不允許分割隧道並且使用者在ASA允許進入Internet之前直接連線到ASA。

注意:在ASA 7.2.2版中,**same-security-traffic permit** configuration mode命令的 *intra-interface關 鍵字允許所有流量進入和退出同一介面(而不僅是IPsec流量)。*

必要條件

<u>需求</u>

嘗試此組態之前,請確保符合以下要求:

- 中心ASA安全裝置需要運行7.2.2版
- Cisco SSL VPN使用者端(SVC)1.x注意:從<u>Cisco Software Download</u>(僅限註冊客戶)下載 SSL VPN客戶端<u>包(sslclient-win</u>*.pkg)。將SVC複製到ASA上的快閃記憶體。SVC將下載到遠 端使用者電腦,以便與ASA建立SSL VPN連線。有關詳細資訊,請參閱*思科安全裝置命令列配 置指南7.2版*中的<u>安裝SVC軟體</u>部分。

<u>採用元件</u>

本文中的資訊係根據以下軟體和硬體版本:

- 執行軟體版本7.2(2)的Cisco 5500系列調適型安全裝置(ASA)
- 適用於Windows 1.1.4.179的Cisco SSL VPN客戶端版本
- 運行Windows 2000 Professional或Windows XP的PC
- •思科調適型安全裝置管理員(ASDM)版本5.2(2)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

<u>背景資訊</u>

SSL VPN客戶端(SVC)是一種VPN隧道技術,使遠端使用者能夠享受IPSec VPN客戶端的好處,而 無需網路管理員在遠端電腦上安裝和配置IPSec VPN客戶端。SVC使用遠端電腦上已經存在的 SSL加密以及安全裝置的WebVPN登入和身份驗證。

要建立SVC會話,遠端使用者在瀏覽器中輸入安全裝置的WebVPN介面的IP地址,瀏覽器連線到該 介面並顯示WebVPN登入螢幕。如果使用者滿足登入和身份驗證要求,且安全裝置將使用者識別為 需要SVC,則安全裝置會將SVC下載到遠端電腦。如果安全裝置確定使用者具有使用SVC的選項 ,則安全裝置將SVC下載到遠端電腦,同時在使用者螢幕上顯示連結以跳過SVC安裝。

下載後,SVC會自行安裝和配置,連線終止時,SVC會從遠端電腦保留或解除安裝自身(具體取決 於配置)。

<u>設定</u>

本節提供用於設定本文件中所述功能的資訊。

註:使用<u>Command Lookup Tool</u>(僅<u>供</u>已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

<u>網路圖表</u>

本檔案會使用以下網路設定:



注意:此配置中使用的IP編址方案在Internet上不能合法路由。它們是<u>RFC 1918</u>,已在實驗室環境 中使用。

使用ASDM 5.2(2)的ASA 7.2(2)配置

本檔案假設已建立基本設定(例如介面組態)且運作正常。

註:請參閱<u>允許ASDM進行HTTPS訪</u>問,以便允許ASDM配置ASA。

注意:除非更改埠號,否則不能在同一個ASA介面上啟用WebVPN和ASDM。有關詳細資訊,請參 閱<u>在同一介面ASA上啟用ASDM和WebVPN</u>。

完成以下步驟,以便在ASA中配置單臂上的SSL VPN:

- 1. 選擇Configuration > Interfaces,然後選中Enable traffic between two or more hosts connected to the same interface覈取方塊,以允許SSL VPN流量進入和退出同一介面。
- 2. 按一下「Apply」。

Ć	Configuration > Interfaces						
	Interface	Name	Enabled	Security Level	IP Address	Subnet Mask	
	Ethernet0/0	inside	Yes	100	10.77.241.142	255.255.255.192	
	Ethernet0/1	outside	Yes	0	172.16.1.1	255.255.255.0	
	Ethernet0/2		No				
	Ethernet0/3		No				
	Management0/0		No				
		Please wait while ASDM is delivering the command(s) to the device Parsing running configuration					
	Enable traffic between two or more interfaces which are configured with same security levels Enable traffic between two or more hosts connected to the same interface						

注意:以下是等效的CLI配置命令:

3. 選擇Configuration > VPN > IP Address Management > IP Pools > Add,以建立名為

-	付 Add IP Pool		
	Name:	vpnpool	
	Starting IP Address:	192.168.10	.1
	Ending IP Address:	192.168.10	.254
	Subnet Mask:	255.255.25	5.0 💌
		1	
vpnpool的IP地址池。	ОК	Cancel	Help

4. 按一下「**Apply**」。**注意:**以下是等效的CLI配置命令:

5. 啟用WebVPN:選擇Configuration > VPN > WebVPN > WebVPN Access,然後選擇外部介面。按一下「Enable」。選中Enable Tunnel Group Drop-down List on WebVPN Login Page覈 取方塊,以允許使用者從Login頁面中選擇其各自的組。

And working a straight state in the								
configuration > VPN > WebVPN	N > WEDVPN Access							
VPN Wizard	-WebVPN Access							
🕀 🚰 General	1							
⊞–¶N IKE	Configure access parameters for WebVPN.	Configure access parameters for Web/VPN.						
E-R IPSec								
E-Sp IP Address Management								
Assignment								
P IP Pools								
- W NAC	Interface WebVPN Enabled	Enable						
E-F WebVPN	inside No							
WebVPN Access	(outside Yes	Disable						
- Provies								
APCE								
Auto Simon								
Casha								
Cartant Paurita								
Laure Transfer of the								
Java Trustport	Port Number: 443							
Proxy Bypass	Port Number.							
Servers and URLs	Defended Transfer							
Port Forwarding	Default idle Timeout: 1100 seconds							
VVebpage Customiza								
ACLs	Max. Sessions Limit: 2							
- Incoding								
-10 SSL VPN Client	WebVPN Memory Size: 50 % of total physical memory							
SSO Servers								
🗄 🖓 E-mail Proxy	Enable Tunnel Group Drop-down List on WebVPN Login Page							
	(Arriv) Reset							
	(Servit) Incode							

按一下「**Apply**」。選擇**Configuration > VPN > WebVPN > SSL VPN Client > Add**,以便從 ASA的快閃記憶體中新增SSL VPN Client映像。

SAGO SSE YPR Clienc Image						
	Г					
Flash SVC Im	nage:				Brows	se Flash.
					Up	load
	Oł	$\langle \rangle$	Cancel		Help	
付 Browse Flash Di	alog					
Folders		Fi	les			
🖃 🤝 disk0:			FileName 🔺		Size (bytes)	Date
E log	l unto erchiu		asdm-603.bin		6,851,2	12 01/
	pto_archiv	•	asa803-k8.bin		14,635,0	108 01/
			admin.cfg		1,2	20 09/
			anyconnect-win-2.	.0.0	2,635,7	34 08/
			asdm-602.bin		6,889,7	64 01/
			asa722-k8.bin		8,312,8	32 02/
			asdm-522.bin		5,623,1	08 02/
			asa802-k8.bin		14,524,4	16 01/
		6	old_running.cfg		1,8	:41 09/
			ssiclient-win-1.1.4.	.17	418,7	65 03
File Name: sslclient-win-1.1.4.179.pkg						
		ОК	Cance		Refres	h

按一下「**OK」(確定)。**

🚎 Add SSL VPN Clier	nt Image		
Flash SVC Ima	ge: disk0:/sslo	client-win-1.1.4.179.pkg	Browse Fla
		Cancel	Help 按一下
Configuration > VPN >	WebVPN > SSL \	PN Client	
 ✓PN Wizard General General IKE IPSec IP Address Mana IP Pools NAC WebVPN NAchVPN 	agement	N Client figure SSL VPN Client pa Enable SSL VPN Client SSL VPN Client Images disk0:/sslclient-win-	arameters.

注意:以下是等效的CLI配置命令:

6. 配置組策略:選擇Configuration > VPN > General > Group Policy > Add(Internal Group Policy),以建立名為*clientgroup的內部組策略*。按一下General頁籤,然後選擇WebVPN覈取 方塊以啟用WebVPN作為隧道協定。

i 🔤 A 🔯	dd Internal Group Policy		
	Name: clientgroup		
	General IPSec Client Config	guration Client Fir	ewall Hardware Client NAC WebVPN
	Check an Inherit checkbox t	o let the correspo	nding setting take its value from the default group policy.
	Tunneling Protocols:	🗌 Inherit	□ IPSec
	Filter:	🔽 Inherit	Manage

按一下**Client Configuration**頁籤,然後按一下**General Client Parameters**頁籤。從Split Tunnel Policy下拉選單中選擇**Tunnel All Networks**,以使所有資料包從遠端PC通過安全隧道傳輸。

📷 Add Interna	al Group Policy			
Name:			Hardwara Cliant	NAC MeEVEN
Check	an Inherit checkbox to	b let the corresponding s	etting take its value	e from the default group policy.
Genera	a Cient Parameters/	Cisco Client Parameters	Microsoft Client F	'arameters
Ban	ner:		🔽 Inherit	Edit Banner
Def	ault Domain:		🔽 Inherit	
Split	Tunnel DNS Names (space delimited):	🔽 Inherit	
Spli	Tunnel Policy:		🗖 inherit	Tunnel All Networks
Split	Tunnel Network List:		🔽 Inherit	Manage
Ad	dress pools			

按一下WebVPN > SSLVPN Client頁籤,然後選擇以下選項:對於Use SSL VPN Client選項 ,取消選中Inherit覈取方塊,然後按一下Optional單選按鈕。此選項允許遠端客戶端選擇是否 下載SVC。Always選項可確保每個SSL VPN連線期間將SVC下載到遠端工作站。對於Keep Installer on Client System選項,取消選中Inherit覈取方塊,然後按一下Yes單選按鈕此選項允 許SVC軟體保留在客戶端電腦上。因此,每次建立連線時,都不需要ASA將SVC軟體下載到客 戶端。對於經常訪問公司網路的遠端使用者來說,此選項是一個不錯的選擇。對於 Renegotiation Interval選項,取消選中Inherit框,取消選中Unlimited覈取方塊,並輸入重新生 成金鑰之前的分鐘數。注意:通過對金鑰的有效時間長度設定限制來增強安全性。對於 Renegotiation Method選項,取消選中Inherit覈取方塊,然後按一下SSL單選按鈕。注意:重 新協商可以使用現有的SSL隧道或專門為重新協商建立的新隧道。SSL VPN客戶端屬性應如下 圖所示

2

j 💼 Ed	it Internal Group Po	licy: clientgroup						
Na	me: clientgroup							
Gen	Seneral IPSec Client Configuration Client Firewall Hardware Client NAC WebVPN							
Cor	nfigure Web∨PN attribu	tes using the follow	ring f	tabs.				
Che	ck an Inherit checkbox	to let the correspo	ndin	g setting ta	ake its va	lue from the	default group p	olicy.
Fu	unctions Content Filte	ring Homepage F	Port	Forwardin	ig Other	SSL VPN	Client Auto Si	gnon
	Use SSL VPN Client:			Inherit	¢	C Always	• Optional	O Never
	Keep Installer on Clien	t System:		Inherit	C	• Yes	C No	
	Compression:		V	Inherit	ć	🔿 Enable	C Disable	
	Keepalive Messages:		V	Inherit	ſ	Enable	interval:	second
ſ	Key Renegotiation Set	ttings						
	Renegotiation Inter	vat		Inherit	Г	Unlimited	30	minutes
	Renegotiation Meth	nod:		Inherit	¢	🔿 None		C New tunne
[Dead Peer Detection							
	Gateway Side Det	ection:		Inherit	Γ	Enable	interval:	second
	Client Side Detection	on:	V	Inherit	Γ	Enable	Interval:	second
		ок		Car	ncel		telp	
按一丁	<mark>≂「OK」</mark> ,然後按	<u> </u>	0					
Configu	ration > VPN > Genera	I > Group Policy						
l - ä	General	Group Policy						
ΗĿ	VPN System Options Client Update Tunnel Group Tunnel Group Manage VPN group policies. A VPN group policy is a collection of user-oriented attribute/valu may be stored internally on the device or externally on a RADIUS server. The group policy interferenced by VPN tunnel groups and user accounts						-oriented attribute/value	
							er. The group policy info	
	🙀 Group Policy 🚮 Users	Terere and a	·, ·,	re control gr	oupo unu	0001 00000110		
	+ Default Tunnel Gatev	Nan	ne		Type	Tunnel	ing Protocol	AAA Server Group
⊕-¶\	• ∠one Labs Integrity S IKE	clientgroup			Internal	webvpn		N/A
e- i ₿	PSec	DfitGrpPolicy (S	yster	m Defa	Internal	L2TP-IPSec,I	PSec	N/A
× +	N 구 E 상 사 사 이	· III III III III III III III III III I						

注意:以下是等效的CLI配置命令:

- 7. 選擇Configuration > VPN > General > Users > Add以建立新的使用者帳戶*ssluser1*。 8. 按一下「OK」,然後按一下「Apply」。

🚰 Add User Account		
Identity VPN Policy VebVPN		
Username:	ssluser1	
Password:	****	
Confirm Password:	******	
🔲 User authenti	cated using MSCHAP	
Deb die versie bewerkie werend		
Privilege level is used	with command authorization.	
Privilege Level:	2	Ŧ
ок	Cancel	Help

注意:以下是等效的CLI命令:

- 9. 選擇Configuration > Properties > AAA Setup > AAA Servers Groups > Edit。
- 10. 選擇預設伺服器組LOCAL,然後按一下Edit。
- 11. 在「編輯本地伺服器組」對話方塊中,按一下**啟用本地使用者鎖定**覈取方塊,然後在「最大 嘗試次數」文本框中輸入16。
- 12. 按一下「**OK**」(確定)。

Configuration > Properties > A	AA Setup > AAA Server Groups	
Startup Wizard	AAA Server Groups	
E & AAA Setup	1	
AAA Server Groups	AAA server groups	
Auth. Prompt	Server Group Protocol Accounting Mode Reactivation Mode	8.dd
LDAP Attribute Map		Auu
Anti-Spoofing		Edit
E-Los ARP	🔂 Edit LOCAL Server Group	
Ciert Undate		Delete
E Certificate	This feature allows to specify the maximum number of failed attempts to allow before	
E-B Device Access	locking out a user and deny access to the user. This limit is applicable only when local	
AAA Access	database is used for authentication.	
- ATTPS/ASDM		
	Enable Local User Lockout	
Teinet		Add
Virtual Access	Maximum Attempts: (16)	
Device Administration		Edit
DHCP Services		
tiene turiletiitu and Carl		Delete
Figh Availability and Scal		Move II
Fragment	OK Cancel Help	11.070 0
S rragment		Move Do

注意:以下是等效的CLI命令:

13. 配置隧道組:選擇Configuration > VPN > General > Tunnel Group > Add(WebVPN

access),以建立一個名為*sslgroup*的新隧道組。按一下General頁籤,然後按一下Basic頁籤 。從Group Policy下拉選單中選擇clientgroup。

🚺 Add	Tunnel Group
	Name: Ssigroup Type: webvpn
G	General WebVPN
(Configure general access attributes from the following sub-tabs.
	Group Policy:
	\square Strip the realm from username before passing it on to the A.A.A. server

按一下Client Address Assignment頁籤,然後按一下Add以分配可用地址池vpnpool。

度 Add Tunnel	Group		
Name:	ssigroup	Type: webvpr	1
General	WebVPN		
Configu	re general access attributes from the follo	wing sub-tabs.	
Basic	Authentication Authorization Accounting	g Client Address	Assignment Advanced
T >	o specify whether to use DHCP or addres: IP Address Management > Assignment.	s pools for addres:	s assignment, go to Configuration > VPN
	DHCP Servers		
	IP Address:	Add >>	
		Delete	
	_		
	Address Pools		
	To configure interface-specific address	pools, go to the A	dvanced tab.
	Available Pools		Assigned pools
		(Add >>	vpnpool

按一下WebVPN頁籤,然後按一下Group Aliases and URLs頁籤。在引數框中鍵入別名,然 後按一下Add將其新增到「登入」頁面上的組名清單中。

General WebVPN			
Configure WebVPN access attributes	from the following sub-t	abs.	
Basic NetBIOS Servers Group Alia	ises and URLs Web Pag	ge	
-Group Aliasas			
Oroup Allases			
		Alias	Status
Alias:	Add >>	sslgroup_users	enable
,	<< Remove		
🔽 Enable			

按一下「**OK**」,然後按一下「**Apply**」。**注意:**以下是等效的CLI配置命令:

14. 配置NAT:選擇**Configuration > NAT > Add > Add Dynamic NAT Rule**,以允許使用外部IP地 址172.16.1.5轉換來自內部網路的流量。

Real Address	
Interface:	
IP Address: 0.0.0.0	
Netmask: 0.0.0.0	
Dynamic Translation	
Interface: outside	
🖶 Add 🗹 Edit 📋 Delete	
Select Pool ID Addresses Pool	
NAT Options	
OK Cancel Help 按一下「OK」(確定	1)。選

擇**Configuration > NAT > Add > Add Dynamic NAT Rule**,以允許使用外部IP地址 172.16.1.5轉換來自外部網路192.168.10.0的流量。

付 Add Dynamic NA1	Rule				
Real Address					
Interface: outs	ide		·]		
IP Address: 192.	168.10.0	•	·		
Netmask: 255.	255.255.0	•	- <u>-</u>		
- Dynamic Translatio	n				
Interface: outsid	3		-		
💠 Add 🗹 Ed	t <u>Î</u> Delete				
Select Pool	D Addres	ses Pool			
NAT Options					
ок	Cancel	Help	按一下	、「OK」 (そ	確定)。
Configuration > NAT)				-	
Add + Add I Edit Delet)	Rule I	Diagram C Packet	Filter Gear	Dula Ouaru
Filter:]Select	Real		[Translated	Kule Query
No Type	Source	Destination	Interface	Addr	ess
inside Inside Dynamic outside	any	any	outside	₫ 172.16.1.5	
-1 Dynamic	🗗 192.168.10.0/24 🧳	any	outside	8 172.16.1.5	

按一下「**Apply**」。**注意:**以下是等效的CLI配置命令:

ASA 7.2(2)CLI配置

Cisco ASA 7.2(2)
ciscoasa# show running-config
: Saved
:
ASA Version 7.2(2)
!
hostname ciscoasa
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
1
interface Ethernet0/2
shutdown
no nameif
no security-level
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
ftp mode passive
same-security-traffic permit intra-interface
!--- Command that permits the SSL VPN traffic to enter
!--- and exit the same interface. access-list 100
extended permit icmp any any pager lines 24 mtu inside
1500 mtu outside 1500 ip local pool vpnpool
192.168.10.1-192.168.10.254
!--- The address pool for the SSL VPN Clients. no
failover icmp unreachable rate-limit 1 burst-size 1 asdm
image disk0:/asdm-522.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) 1 0.0.0.0 0.0.0.0
!--- The NAT statement to define what to encrypt !---
(the addresses from vpn-pool). nat (outside) 1
192.168.10.0 255.255.255.0
access-group 100 in interface outside
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 0:05:0
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:
timeout uauth 0:05:00 absolute
group-policy clientgroup internal
```

! Create an internal group policy "clientgroup."
group-policy clientgroup attributes
vpn-tunnel-protocol webvpn
<pre>! Enable webvpn as tunneling protocol. split-tunnel- policy tunnelall</pre>
<pre>! Encrypt all the traffic coming from the SSL VPN Clients. webvpn svc required</pre>
<pre>! Activate the SVC under webvpn mode svc keep- installer installed</pre>
<pre>! 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</pre>
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
<pre>! Command that specifies that SSL renegotiation takes place during SVC rekey. username ssluser1 password ZRhW85jZqEaVd5P. encrypted</pre>
<pre>! Create an user account "ssluser1." aaa local authentication attempts max-fail 16</pre>
<pre>! Enable the AAA local authentication. 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 tunnel- group sslgroup type webvpn</pre>
<pre>! Create a tunnel group "sslgroup" with type as WebVPN. tunnel-group sslgroup general-attributes address-pool vpnpool</pre>
<pre>! Associate the address pool vpnpool created. default-group-policy clientgroup</pre>
<pre>! Associate the group policy "clientgroup" created. tunnel-group sslgroup webvpn-attributes</pre>
group-alias sslgroup_users enable
<pre>! Configure the group alias as sslgroup-users. telnet timeout 5 ssh timeout 5 console timeout 0 ! 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</pre>
enable outside

disk0:/sslclient-win-1.1.4.179.pkg 1



使用SVC建立SSL VPN連線

完成以下步驟,以便與ASA建立SSL VPN連線。

1. 在Web瀏覽器的Address欄位中鍵入ASA WebVPN介面的URL或IP地址。例如:

WebVPN Se	rvice - Microsoft Internet Explorer
File Edit View	w Favorites Tools Help
🕒 Back 🔹 (🔊 - 🖹 🛃 🏠 🔎 Search 🤺 Favorites 🤣 😂 😓 🦓
Address 🙆 http:	s://172.16.1.1/+webvpn+/index.html
CISCO SYSTEM	™ WebVPN Service
	Login
	Please enter your username and password.
	USERNAME:
	PASSWORD:
	GROUP: sslgroup_users
	Login Clear
輸入使用者名稱	爯和密碼,然後從「組」下拉選單中選擇相應的組。 —————————————————————
	Login

	Login	
Please enter you	r username and password.	
USERNAME:	ssluser1	
PASSWORD:	•••••	
GROUP:	sslgroup_users	~
	Login Clear	



3. 建立連線後,按兩下電腦工作列中出現的黃色按鍵圖示。Cisco Systems SSL VPN Client對話 方塊顯示有關SSL連線的資訊。

🥑 Cisco Systems SSL	VPN Client		
CISCO SYSTEMS	N CLIENT for	Nebvpn	
Statistics Route Deta	ils About		
Address Information	n	SSL Information	
Server:	172.16.1.1	Cipher:	3DES SHA-1
Client:	192.168.10.1	Version:	TLSv1
Bytes		Transport Informat	ion
Sent:	5471	Local LAN:	Disabled
Received:	884	Split Tunneling:	Disabled
Frames		Connection Inform	ation
Sent:	75	Time:	00:00:35
Received:	12		
	Res	et	
	Close	Disconnect	
of Cisco Systems SSL	VPN Client		
CISCO SYSTEMS SSLVP	N CLIENT for V	VebVPN	
Statistics Route Detai	S About		
Local LAN Routes		Secure Routes	
Network Su	ibnet Mask	Network Su	bnet Mask
		0.0.0.0 0.0	0.0.0
	Close	Disconnect	





使用本節內容,確認您的組態是否正常運作。

<u>輸出直譯器工具(</u>僅供<u>已註冊</u>客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析

```
0
```

```
show webvpn svc — 顯示儲存在ASA快閃記憶體中的SVC映像。
ciscoasa#show webvpn svc
disk0:/sslclient-win-1.1.4.179.pkg 1
CISCO STC win2k+ 1.0.0
1,1,4,179
Fri 01/18/2008 15:19:49.43
1 SSL VPN Client(s) installed
show vpn-sessiondb svc — 顯示有關當前SSL連線的資訊。
ciscoasa#show vpn-sessiondb svc
```

```
Session Type: SVC
```

```
: ssluser1
Username
            : 1
Index
Assigned IP : 192.168.10.1
                                 Public IP
                                               : 192.168.1.1
Protocol : SVC
                                  Encryption : 3DES
Hashing
           : SHA1
           : 131813
Bytes Tx
                                  Bytes Rx
                                              : 5082
Client Type : Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Client Ver : Cisco Systems SSL VPN Client 1, 1, 4, 179
Group Policy : clientgroup
```

```
Tunnel Group : sslgroup
Login Time : 12:38:47 UTC Mon Mar 17 2008
Duration : 0h:00m:53s
Filter Name :
```

• show webvpn group-alias — 顯示各種組的已配置別名。 ciscoasa#show webvpn group-alias Tunnel Group: sslgroup Group Alias: sslgroup_users enabled

 在ASDM中,選擇Monitoring > VPN > VPN Statistics > Sessions以檢視有關ASA中當前 WebVPN會話的資訊。

Ronitoring > VPN > VPN Statisti	cs > Sessions	\mathbf{D}					
🖃 🛃 VPN Connection Graphs	Sessions						
PSec Tunnels	Remote				F 10		Total
Sessions	Access	LAN-to-LAN	VVebVPN	SSL VPN Client	E-mail Proxy	Total	Cumulative
VPN Statistics	0	0	1	0	0	1	12
Crypto Statistics	1						
Compression Statistic							
Clobal IVE ADS as Shat	Filter By: WebV	'PN 💌 🔤	All Sessions	*		Filter	
NAC Session Summs							
	Username	e Gi	roup Policy	Protocol		Login Time	Details
Sessions	IP Addres	s Tu	nnel Group	Encryptio	n	Duration	
E-E WebVPN	ssluser1	clientgro	oup	WebVPN	08:49:5	52 UTC Thu Mar 20	2 Logout
SSO Statistics	192.168.1.1	ssigrou	9	3DES	0h:08#	r14s	
							Ping

<u>疑難排解</u>

本節提供的資訊可用於對組態進行疑難排解。

```
    vpn-sessiondb logoff name <username> — 允許您註銷指定使用者名稱的SSL VPN會話。
ciscoasa#vpn-sessiondb logoff name ssluser1
    Called vpn_remove_uauIth: success!
    webvpn_svc_np_tear_down: no ACL
    NFO: Number of sessions with name "ssluser1" logged off : 1
```

同樣,您可以使用命令**vpn-sessiondb logoff svc**來終止所有SVC會話。**注意:**如果PC進入待機 或休眠模式,SSL VPN連線可以終止。

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, etc) Called vpn_remove_uauth: success! webvpn_svc_np_tear_down: no ACL

ciscoasa#**show vpn-sessiondb svc** INFO: There are presently no active sessions

• Debug webvpn svc <1-255> — 提供即時WebVPN事件以建立會話。

Ciscoasa#**debug webvpn svc 7**

```
ATTR_CISCO_AV_PAIR: got SVC ACL: -1
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 Systems SSL VPN Client 1, 1, 4, 179'
Processing CSTP header line: 'User-Agent: Cisco Systems SSL VPN Client 1, 1, 4,
179'
Setting user-agent to: 'Cisco Systems SSL VPN Client 1, 1, 4, 179'
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: 'Cookie: webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486
D5BC554D2 '
Processing CSTP header line: 'Cookie: webvpn=16885952@10@1205757506@D4886D33FBF1
CF236DB5E8BE70B1486D5BC554D2 '
Found WebVPN cookie: 'webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1
486D5BC554D2 '
WebVPN Cookie: 'webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486D5B
C554D2'
Validating address: 0.0.0.0
CSTP state = WAIT_FOR_ADDRESS
webvpn_cstp_accept_address: 192.168.10.1/0.0.0.0
CSTP state = HAVE_ADDRESS
No subnetmask... must calculate it
SVC: NP setup
webvpn_svc_np_setup
SVC ACL Name: NULL
SVC ACL ID: -1
SVC ACL ID: -1
vpn_put_uauth success!
SVC: adding to sessmgmt
SVC: Sending response
CSTP state = CONNECTED
```

 在ASDM中,選擇Monitoring > Logging > Real-time Log Viewer > View以檢視即時事件。這些 示例顯示了通過ASA 172.16.1.5在Internet中的SVC 192.168.10.1和Web伺服器10.2.2.2之間的 會話資訊。

Save Clear M Clear M Fiber tination IP No tran No tran No tran No tran No tran No tran	Color Settings	or udp src outs or udp src outs or udp src outs	Show Rule	Show De O 1/138 dst insid 0.1/1027 dst insid	tals ? Help e:192.168.10.255 de:10.77.244.193	Description		
tination IP No tran No tran No tran No tran 2 Built inb	Show Al Find:	or udp sno outs or udp sno outs or udp sno outs	ide 192.168.1 ide:192.168.1	0.1/138 dst insid 0.1/1027 dst insi	e:192.168.10.254 de:10.77.244.193	Description		_
Ination IP No tran No tran No tran No tran 2 Built inb	slation group found fi slation group found fi slation group found fi	or udp src outs or udp src outs or udp src outs	ide: 192.168.1 ide: 192.168.1	0.1/138 dist insid 0.1/1027 dist insi	e:192.168.10.255 de:10.77.244.193	Description		_
No tran No tran No tran No tran 2 Built inb	slation group found fi slation group found fi slation group found fi	or udp sno outs or udp sno outs or udp sno outs	ide: 192.168.1 ide: 192.168.1	0.1/138 dist insid 0.1/1027 dist insi	e:192.168.10.255 de:10.77.244.193	5/138		*
No tran No tran 2 Built inb	slation group found fi slation group found fi	or udp sno outs or udp sno outs	ide:192.168.1	0.1/1027 dst insi	de:10.77.244.193	1453		
2 Built inb	slation group found f	or udp src outs	He 100 168 1			100		
2 Built inb	a red T/CD comparties		490.102.100.1	0.1/1028 dst insi	de:10.77.244.193	3/53		
A. C	ound for connection	1902 for outsi	de:192.168.10).1/1100 (172.16	.1.5/1025) to out	, side:10.2.2.2/80 (1	0.2.2.2/80) (ssluser1	
1.5 Built dy	namic TCP translation	from outside:1	92.168.10.1/1	100 to outside:1	72.16.1.5/1025			
No tran	slation group found fo	or udp src outs	ide:192.168.1	0.1/138 dst insid	e:192.168.10.255	5/138		
No tran	slation group found fo	or udp src outs	ide:192.168.1	0.1/1027 dst insi	de:10.77.244.193	V53		
No tran	slation group found fo	or udp src outs	ide:192.168.1	0.1/1028 dist insi	de:10.77.244.193	v63		
No tran	slation aroup found fo	or udo src outs	ide:192.168.1	0.1/1027 dist insi	de:10.77.244.193	15 3		×
ry to see the expl	anation							×
Action Details								
reserving 0 Ale	ts \varTheta Critical	😣 Errors	1. Warnings	🗼 Notificatio	ns 🔒 Inform	ational 📀 Deb	sugging	
	ry to see the explanation Details	ry to see the explanation Action Details rgencies O Alerts O Critical	ry to see the explanation Action Details rgencies O Alerts @ Critical @ Errors	ry to see the explanation Action Details rgencies O Alerts @ Critical & Errors & Warnings	ry to see the explanation Action Details rgencies O Alerts @ Critical @ Errors A . Warnings A . Notificatio	ry to see the explanation Action Details rgencies O Alerts O Critical © Errors <u>A</u> Warnings <u>A</u> Notifications <u>A</u> Inform	ry to see the explanation Action Details rgencies O Alerts O Critical O Errors A Warnings A Notifications A Informational P Det	ry to see the explanation Action Details rgencies O Alerts O Critical O Errors A Warnings A Notifications A Informational P Debugging

相關資訊

- Cisco 5500系列調適型安全裝置支援頁面
- 單臂公共網際網路VPN的PIX/ASA 7.x和VPN客戶端配置示例
- 帶ASDM的ASA上的SSL VPN客戶端(SVC)配置示例
- 技術支援與文件 Cisco Systems