ماعل (SVC): SSL VPN Client (SVC) تنرتنإلا اصعلا نيوكت لاثم ىلع VPN تنرتنإلا

المحتويات

<u>المقدمة</u> المتطلبات الأساسية <u>المكونات المستخدمة</u> <u>المكونات المستخدمة</u> معلومات أساسية <u>الرسم التخطيطي للشبكة</u> <u>الرسم التخطيطي للشبكة</u> <u>تكوينات 2)ASA 7.2 (2) (ASDM 2) استخدام 2)SV (ASDM 2)</u> <u>تكوينا 2)SSL VPN باستخدام SVC 2001</u> إنشاء اتصال SSL VPN باستخدام SVC التحقق من الصحة معلومات ذات صلة

<u>المقدمة</u>

يوضح هذا المستند كيفية إعداد جهاز أمان قابل للتكيف (ASA (ASA لإجراء SSL VPN على جهاز تثبيت. ينطبق هذا الإعداد على حالة محددة لا يسمح فيها ASA بنفق التقسيم ويتصل المستخدمون مباشرة ب ASA قبل السماح لهم بالانتقال إلى الإنترنت.

ملاحظة: في الإصدار 7.2.2 من ASA، تسمح الكلمة الأساسية *intra-interface* لأمر وضع التكوين **نفسه--security** بأن تدخل جميع حركة المرور الواجهة نفسها وتخرج منها (ليس فقط حركة مرور IPsec).

<u>المتطلبات الأساسية</u>

<u>المتطلبات</u>

تأكد من استيفاء المتطلبات التالية قبل أن تحاول إجراء هذا التكوين:

- يحتاج جهاز أمان Hub ASA إلى تشغيل الإصدار 7.2.2
- SSL VPN Client (SVC) (sslclient-win*.pkg**ملاحظة:** قم بتنزيل حزمة عميل SSL VPN (sslclient-win*.pkg) من <u>تنزيل برامج Cisco</u> (للعملاء المسجلين فقط). انسخ SVC إلى ذاكرة Flash (الذاكرة المؤقتة) على ASA. يجب تنزيل SVC إلى أجهزة كمبيوتر المستخدم البعيدة لإنشاء اتصال SSL VPN مع ASA. راجع <u>تثييت</u> قسم <u>برنامج</u> SVC من *دليل تكوين سطر أوامر Cisco Security Appliance، الإصدار 7.2* للحصول على مزيد من المعلومات.

<u>المكونات المستخدمة</u>

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- جهاز الأمان القابل للتكيف (ASA) من Cisco 5500 Series الذي يشغل الإصدار 2.7(2) من البرنامج
 - إصدار عميل Cisco SSL VPN ل Windows 1.1.4.179
 - كمبيوتر يعمّل بنظام التشغيل Windows 2000 Professional أو Windows XP
 - (Cisco Adaptive Security Device Manager (ASDM •

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

<u>الاصطلاحات</u>

راجع <u>اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.</u>

<u>معلومات أساسية</u>

ال SSL VPN Client (SVC) هو تقنية VPN tunneling التي تمنح المستخدمين البعيدين فوائد IPSec VPN) وال Client دون الحاجة إلى مسؤولي الشبكة لتثبيت وتكوين عملاء IPSec VPN على أجهزة الكمبيوتر البعيدة. يستخدم SVC تشفير SSL الموجود بالفعل على الكمبيوتر البعيد بالإضافة إلى تسجيل دخول WebVPN ومصادقة جهاز الأمان.

لإنشاء جلسة SVC، يدخل المستخدم البعيد عنوان IP الخاص بواجهة WebVPN الخاصة بجهاز الأمان في المستعرض، ويتصل المستعرض بتلك الواجهة ويعرض شاشة تسجيل الدخول إلى WebVPN. إذا استوفى المستخدم تسجيل الدخول والمصادقة، وقام جهاز الأمان بتعريف المستخدم على أنه يتطلب SVC، يقوم جهاز الأمان بتنزيل SVC إلى الكمبيوتر البعيد. إذا كان جهاز الأمان يحدد أن المستخدم لديه خيار إستخدام SVC، فإن جهاز الأمان يقوم بتنزيل SVC إلى الكمبيوتر البعيد أثناء عرض إرتباط على شاشة المستخدم لحيم لتخطي تشييت

بعد التنزيل، يقوم SVC بتثبيت نفسه وتكوينه، ومن ثم يبقى SVC أو يقوم بإلغاء تثبيت نفسه (حسب التكوين) من الكمبيوتر البعيد عند إنهاء الاتصال.

<u>التكوين</u>

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم <u>أداة بحث الأوامر</u> (للعملاء <u>المسجلين</u> فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

<u>الرسم التخطيطي للشبكة</u>

يستخدم هذا المستند إعداد الشبكة التالي:



ملاحظة: ال ip ليس يخاطب خطة يستعمل في هذا تشكيل قانونيا routable على الإنترنت. وهي عناوين<u>RFC 1918</u> التي تم استخدامها في بيئة مختبرية.

<u>تكوينات 2)ASA 7.2 (ASDM 5.2) باستخدام 2)ASDM 5.2 (</u>

يفترض هذا المستند أن التكوينات الأساسية، مثل تكوين الواجهة، قد تم إنشاؤها بالفعل وتعمل بشكل صحيح.

ملاحظة: ارجع إلى <u>السماح بوصول HTTPS إلى ASDM</u> للسماح بتكوين ASA بواسطة ASDM.

ملاحظة: لا يمكن تمكين WebVPN و ASDM على واجهة ASA نفسها ما لم تقم بتغيير أرقام المنافذ. راجع <u>ASDM</u> <u>و WebVPN الذي تم تمكينه على نفس واجهة ASA</u> للحصول على مزيد من المعلومات.

أتمت هذا steps in order to شكلت ال SSL VPN على a stick في ASA:

- 1. أخترت **تشكيل>قارن**، وفحصت ال **يمكن حركة مرور بين إثنان أو أكثر مضيف يربط إلى ال نفسه قارن** تدقيق in سمحت SSL VPN حركة مرور أن يدخل ويخرج ال نفسه قارن.
 - 2. طقطقة

يطبق.

onfiguration > 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				
/lanagement0/0		No				
Please wait Please wait while ASDM is delivering the command(s) to the device Parsing running configuration Image: Please wait while ASDM is delivering the command(s) to the device Parsing running configuration Image: Please wait while ASDM is delivering the command(s) to the device Parsing running configuration Image: Please wait while ASDM is delivering the command(s) to the device Parsing running configuration Image: Please wait while ASDM is delivering the command(s) to the device Parsing running configuration Image: Please wait while ASDM is delivering the command(s) to the device Parsing running configuration Image: Please wait wait was an event of the same interface with the same interface. Image: Please wait was an event was an event of the same interface.						
			Appl	y	Reset	
بركة يعين	in ord خلقت عنوان Add IP Pool Name: Starting IP Ending IP /	der to فيف Address: Address:	فئ: IF بركة>يم vpnp 192.1 192.1	تكوين CLI المكار VF عنوان إدارة> 68.10.1 68.10.254	لاحظة: فيما يلي امر خترت تشكيل>N IP<	
	Subnet Ma	ask:	255.2	55.255.0	-	

ок

Help

.VPNPOOL

Cancel

^{4.} طقطقة **يطبق.ملاحظة:** فيما يلي أمر تكوين CLI المكافئ:

5. تمكين WebVPN:أخترت **تشكيل>VPN>WebVPN>WebVPN**:أخترت **تشكيل>WebVPN منفذ**، وعينت القارن خارجي.طقطقة **يمكن**.حدد خانة الاختيار **تمكين القائمة المنسدلة لمجموعة النفق على صفحة تسجيل الدخول إلى WebVPN** للسماح للمستخدمين باختيار مجموعاتهم الخاصة من صفحة تسجيل الدخوا.

					الدمون.
Configuration > VPN > WebVPN >	> WebVPN Access)				
VPN Wizard	WebVPN Access				
🗄 🚰 General					
E-N KE	Configure access parame	sters for WebVPN.			
E-R IPSec					
E-Sp IP Address Management					
Assignment					
- IP Pools	Interde		Manager Countries		C C C C C C C C C C C C C C C C C C C
- 🞀 NAC	Interna	ce	VVebVPN Enabled		criatre
E- 🕞 WebVPN	inside		No	_	
WebVPN Access	outside		Yes		Disable
- Proxies					
Proxy Bypass	Port Number:	443			
- In Servers and URLs					
- Port Forwarding	Default Idle Timeout:	1800	seconds		
ACLs	Max. Sessions Limit:	2			
Encoding					
SSL VPN Client	WebVPN Memory Size:	50	% of total physical memory		
SSO Servers	(=				
E-mail Proxy	I Enable Tunnel Group	Drop-down List on	WebVPN Login Page		
		0	koply Reset		
- I I I I I I I I I I I I					
				2	

طقطقة **يطبق**.أخترت **تشكيل>VPN>WebVPN>SSL VPN زبون>إضافة** in order to أضفت ال SSL VPN زبون صورة من ال flash ذاكرة من ASA.

🔚 AGO SSL YPN LII	ent Image					
					(
Flash SVC In	nage:				Browse	Flash.
					Uploa	id
				1	1	
	ОК		Cancel		Help	
付 Browse Flash Di	alog					
Folders		Fi	les			
diskU:			FileName 🔺		Size (bytes)	Date
	} vnto archive		asdm-603.bin		6,851,212	01/0
	pto_arenive		asa803-k8.bin		14,635,008	01/0
			admin.cfg		1,220	09/2
			anyconnect-win-2	2.0.0	2,635,734	08/1
			asdm-602.bin		6,889,764	01/0
			asa722-k8.bin		8,312,832	02/1
			asdm-522.bin		5,623,108	02/1
			asa802-k8.bin		14,524,416	01/0
			old_running.cfg		1,841	09/2
			ssiclient-win-1.1.4	4.17	418,765	03 <mark>1</mark>
		_				
	File Name:	s	slolient-win-1.1.4.179	9.pkg		
				1		1
		OK	Canc	el	Refresh	

وانقر فوق

	🇯 Add SSL VPN CI	ient Image					
	Flash SVC I	mage: disk	0:/sslclient-win-	-1.1.4.179.pkg		Brows	se Fla
						Up	load.
وانق		OK		Cancel	I	Help	ок

ر

C	li	e	r	1	t
_	_	_	_		

Configuration > VPN > WebVPN > SSL VPN Client					
- 🚰 VPN Wizard	SSL VPN Client				
⊕ General ⊕ ¶ IKE	Configure SSL VPN Client parameters.				
🕀 📲 IPSec	Enable SSL VPN Client				
🖻 🏭 IP Address Management					
Assignment IP Pools	SSL VPN Client Images				
	disk0:/sslclient-win-1.1.4.179.pkg				

ملاحظة: فيما يلي أوامر تكوين CLI المكافئة:

6. تكوين نهج المجمَّوعةُ:أُخترت**ُ تَشكيل>VPN>عام>مجموعة سياسة>إضافة (داخلي مجموعة سياسة) in order** to خلقت داخلي مجموعة سياسة يعين *زبونGroup*.انقر فوق علامة التبويب **عام**، وحدد خانة الاختيار WebVPN لتمكين WebVPN كبروتوكول اتصال

				نفقي.
📬 A	dd Internal Group Policy			
	Name: clientgroup			
	General IPSec Client Conf	iguration Client Fir	ewall Hardware Clier	t NAC WebVPN
	Check an Inherit checkbox	to let the correspor	nding setting take its va	lue from the default group policy.
	Tunneling Protocols:	🗖 Inherit	🗆 IPSec 🔽 🕅	bVPN
	Filter:	🔽 Inherit		Manage

انقر فوق علامة التبويب **تكوين العميل**، ثم انقر فوق علامة التبويب **معلمات العميل العامة**.أختر Tunnel all Networks من القائمة المنسدلة لسياسة النفق المقسم لجعل جميع الحزم تنتقل من الكمبيوتر الشخصي البعيد من خلال نفق آم .

فوق OK.انقر فوق خانة الاختيار OK.

📬 A c	id Internal Group Policy		
	Name: clientgroup		
	General IPSec Client Configuration Client Firewall	Hardware Client	NAC WebVPN
	Check an Inherit checkbox to let the corresponding s	etting take its valu	e from the default group policy.
	General Client Parameters Cisco Client Parameters	Microsoft Client	Parameters
	Banner:	🔽 Inherit	Edit Banner
	Default Domain:	🔽 Inherit	
	Split Tunnel DNS Names (space delimited):	🔽 Inherit	
	Split Tunnel Policy:	🗆 İnherit	Tunnel All Networks
	Split Tunnel Network List:	🔽 Inherit	Manage
	Address pools		

انقر فوق علامة التبويب Inherit (توريث)، وانقر فوق زر الاختيار التالية:لخيار إستخدام SSL VPN (انعتار، قم بإلغاء تحديد خانة الاختيار الموريث)، وانقر فوق زر الاختيار الاختياري. يسمح هذا الخيار للعميل البعيد باختيار ما إذا كان سيتم تنزيل SVC أم لا. يضمن الاختيار الدائم تنزيل SVC إلى محطة العمل البعيدة أثناء كل اتصال SSL VPN للحصول على خيار إبقاء المثبت على نظام العميل، قم بإلغاء تحديد خانة الاختيار **توريث**، وانقر فوق الزر **نعم** للانتقاءيتيح هذا الخيار لبرنامج SVC البقاء على جهاز العميل. لذلك، لا يتطلب ASA تنزيل برنامج SVC إلى العميل في كل مرة يتم فيها الاتصال. يعد هذا الخيار خيارا جيدا يتطلب ASA تنزيل برنامج SVC إلى العميل في كل مرة يتم فيها الاتصال. يعد هذا الخيار خيارا جيدا يتم يتم ينه ASA تنزيل برنامج SVC إلى العميل في كل مرة يتم فيها الاتصال. يعد هذا الخيار خيارا جيدا يتم يتم ينه ASA تنزيل مرنامج SVC إلى العميل في كل مرة يتم فيها الاتصال. يعد هذا الخيار خيارا جيدا يتم يتم ين المعيدين الذين غالبا ما يصلون إلى شبكة الشركة.لخيار الفاصل الزمني لإعادة التفاوض، قم بإلغاء تحديد خانة الاختيار المادة الاليا ما يصلون إلى شبكة الشركة.لخيار الفاصل الزمني لإعادة التفاوض، قم بإلغاء يتم تحديد نانة الاختيار Inherit، وإلغاء تحديد خانة الاختيار DNI وأدخل عدد الدقائق حتى المفتاح. المستخدمين المان من خلال تعيين حدود لطول المدة التي يكون فيها المفتاح صالحا.لخيار طريقة إعادة يتم تحديد الذمان من خلال تعيين حدود لطول المدة التي يكون فيها المفتاح صالحا.لخيار طريقة إعادة التفاوض، قم بإلغاء تحديد خانة الاختيار Inherit، وانقر فوق زر انتقاء SSL ملاحظة: يمكن لإعادة التفاوض التفاوض، قم بالغاء تحديد خانة الاختيار SSL الفول المدة التي يكون فيها المفتاح صالحا.لخيار طريقة إعادة المورة. الالمان من خلال تعيين حدود لطول المدة التي يكون فيها المفتاح صالحا.لخيار طريقة إعادة التفاوض المورض، قم بالغاء تحديد خانة الاختيار Inherit، وانقر فوق زر انتقاء SSL ملاحظة: يمكن لإعادة التفاوض المورة. والم الحاصة بك كما هو موضح في هذه

💼 Edit Internal Group Po	licy: clientgroup				
Name: clientgroup					
Seneral IPSec Client Co	nfiguration Client Fir	rewall Hardv	ware Client NAC 🛛	VebVPN	
Configure WebVPN attribut	tes using the followir	ng tabs .			
Check an Inherit checkbox	to let the correspon	ding setting ta	ke its value from the	default group poli	cy.
Functions Content Filter	ring Homepage Po	ort Forwarding	g Other SSL VPN	Client Auto Sign	on
Use SSL VPN Client:		🗖 Inherit	C Always	• Optional	C Never
Keep Installer on Clien	t System:	🗌 Inherit	(Yes	C No	
Compression:		🔽 Inherit	C Enable	C Disable	
Keepalive Messages:		🔽 Inherit	Enable	interval:	second
Key Renegotiation Set	tings				
Renegotiation Inter	val:	🗌 Inherit	🗌 Unlimited	30	minutes
Renegotiation Meth	od:	🗌 Inherit	C None	© 55L	C New tunne
Dead Peer Detection					
Gateway Side Dete	ection:	🔽 Inherit	🗖 Enable	interval:	second
Client Side Detection	on:	🔽 Inherit	🗖 Enable	Interval:	second
	ок	Can	cel H	telp	
				، ثم انقر فوق	انقر فوق موافق ،
Configuration > VPN > General	I > Group Policy)				تطبيق.

Configuration > VPN > General > Group Policy)						
- 🚰 VPN Wizard	Group Policy					
🖻 🚰 General						
- 📆 VPN System Options	Manage VPN group policies. A VPN group policy is a collection of user-oriented attribute/value may be stored internally on the device or externally on a RADIUS server. The group policy info					
Client Update						
Tunnel Group						
Group Policy	referenced by vrivialities g	reterenced by VPN tunnel groups and user accounts.				
- 🙀 Users						
	Nama	Turne	Transling Destand	0.0.0 Someon Crown		
-+2+ Zone Labs Integrity S	Iname	туре	Tunneling Protocol	AAA Server Group		
E-N KE	clientgroup	Internal	webvpn	N/A		
E-1 B IPSec	DfitGrpPolicy (System Defa	Internal	L2TP-IPSec JPSec	N/A		
1.22						

- ملاحظة: فيما يلي أوامر تكوين CLI المكافئة:
- 7. أخترت **تشكيل>VPN عام>مستعمل>يضيف** in order to خلقت جديد مستعمل حساب *ssluser1*.
 - 8. انقر فوق **موافق**، ثم انقر فوق

	تطبيق.
🕵 Add User Account	
Identity VPN Policy WebVPN	
Username:	ssluser1
Password:	*****
Confirm Password:	******
User authenti	cated using MSCHAP
Privilege level is used	with command authorization.
Privilege Level:	2
ок	Cancel Help

لاحظة: فيما يلي أمر CLI المكافئ:

- 9. أختر **التكوين > الخصائص > إعداد AAA > مجموعات خوادم AAA > تحرير**.
 - 10. حدد مجموعة الخوادم الافتراضية *المحلية*، وانقر فوق **تحرير**.
- 11. في شاشة تحرير مجموعة الخوادم المحلية، انقر خانة الاختيار **تمكين تأمين المستخدم المحلي**، وأدخل 16 في مربع النص الحد الأقصى للمحاولات.
 - 12. وانقر فوق

.OK

Configuration > Properties > A	AA Setup > AAA Server Groups	
Startup Wizard	AAA Server Groups	
E- 🖬 AAA Setup		
AAA Server Groups	AAA server groups	
	Server Group Protocol Accounting Mode Reactivation Mode	ê alal
LDAP Attribute Map		Add
	LOCAL	Edit
E-B ARP	🔂 Edit LOCAL Server Group	Con
—🛃 Auto Update		Delete
-B Client Update		
🐑 🔁 Certificate	This feature allows to specify the maximum number of failed attempts to allow before	
E-P Device Access	locking out a user and deny access to the user. This limit is applicable only when local	
	database is used for authentication.	
	Enable Local User Lockout	
- E Teinet		Add
Virtual Access	Maximum Attempts: (16)	0.000
🖅 🥮 Device Administration		Edit
E-17 DHCP Services		
🕀 📲 DNS		Delete
High Availability and Scal		
- 健 Failover		Move U
-W Fragment	OK Cancel Help	
		Mourp Floor

ملاحظة: فيما يلي أمر CLI المكافئ:

.vpnPool

13. تكوين مجموعة النفق:أخترت **تشكيلً>VPN>عام>نفق مجموعة>إضافة(WebVPN منفذ)** in order to خلقت جديد نفق مجموعة يعين *sslgroup*.انقر صفحة **عام**، ثم انقر صفحة **أساسي**.أختر ClientGroup من القائمة المنسدلة "نهج

مجموعه".
🚰 Add Tunnel Group
Name: Sslgroup Type: webvpn
General WebVPN
Configure general access attributes from the following sub-tabs. Basic Authentication Authorization Accounting Client Address Assignment Advanced Group Rolicy: Client group Image: Client Address Assignment Advanced
Strip the realm from username before passing it on to the AAA server
فر فوق علامة التبويب تعيين عنوان العميل ، ثم انقر فوق إضافة لتعيين تجمع العناوين المتوفر

in Add Tunnel	Group		
Name:	ssigroup	Type: webvpn	
General			
General	VVeb VPN		
Configu	re general access attributes from the	following sub-tabs.	
Regio	Authentication Authorization Acco	unting Client Address Assignment Advanced	
Dasie -	Ramenacation Admonization Acco	aning Colore transcer transcer and Autonced	
т	o specify whether to use DHCP or ad	dress pools for address assignment, go to Configuration	i > VPN
>	IP Address Management > Assignme	nt.	
	DHCP Servers		
	IP Address:		
		Add >>	
		Delete	
	-Address Pools		
	To configure interface-specific add	ress pools, go to the Advanced tab.	
	Available Pools	Assigned pools	
		vpnpool	
		(Add >>)	

انقر فوق علامة التبويب WebVPN، ثم انقر فوق علامة التبويب **أسماء مستعارة للمجموعة وعناوين** URL.اكتب اسم الاسم المستعار في مربع المعلمة، وانقر فوق **إضافة** لإضافته إلى قائمة أسماء المجموعات في صفحة تسجيل الدخما

				الدخون.
Ge	neral (WebVPN)			
0	onfigure WebVPN access attributes	from the following sub-t	abs.	
В	asic NetBIOS Servers Group Alias	ses and URLs VVeb Pag	je	
	-Croup Aliases			
	Group Allases			
			Alias	Status
	Alias:	Add >>	ssigroup_users	enable
		<< Remove		
	I⊻ Enable			

انقر فوق **موافق**، ثم انقر فوق **تطبيق**.**ملاحظة:** فيما يلي أوامر تكوين CLI المكافئة:

14. تكوين NAT:أخترت **تشكيل>nat>إضافة>إضافة>قاعدة nat حُركي** أن يسمح الحركة مرور أن يأتي من الشبكة الداخلية أن يكون ترجمت مع الإستعمالمن الخارجي عنوان

8	🗯 Add Dynamic	NAT R	ule			
	Real Address					
	Interface:	inside			•	
	IP Address:	0.0.0.0			•	
	Netmask:	0.0.0.0			_	
	Dynamic Tran	slation				
	Interface:	utside			-	
	🔂 Add 🖪	🖞 Edit	<u>î</u> Delete			
	Select	Pool ID	Addre	sses Pool		
			💾 172.16.1.5			
	NAT Options					
_وانقر فوق	ок		Cancel	Н	lelp	.172.16.1.5

OK.أخترت **تشكيل>nat>يضيف>إضافة قاعدة nat حركي** أن يسمح الحركة مرور أن يأتي من الشبكة الخارجية 192.168.10.0 أن يكون ترجمت مع الإستعمالمن العنوان الخارجي

	1	Add Dynamic	NAT Rule			
		-Real Address				
		Interface:	outside			•
		IP Address:	192.168.10).0		 ✓ …
		Netmask:	255.255.25	5.0		
		-Dynamic Tran:	slation			
		Interface: o	utside			-
		🔂 Add 🖸	f Edit 📋	Delete		
		Select	Pool ID	Addre	esses Pool	
		⊡ 1		172.16.1.5		
		NAT Options				
		ок		Cancel	Не	al
وق	اوانقر فو					.172.16.1.5
onfiguratio	on > NAT)					.0N
💠 Add 👻	🗹 Edit 📋 🕻	Delete 🛧 🐇	🖻 🛍 🔹	🔍 Find 📴 Rule I	Diagram 🥰 Packet 1	Trace
Filter:Sele	ect 💌					Filter Clear Rule Query
No	Туре		Real			Translated
-inside		Sourc	e	Destination	Interface	Address
4	Dynamic	🍳 any	ې 🏈 د	iny	outside	172.16.1.5
⊡outside	Li Damania	192 169 10	0/24	1012	outside	172464 5
	E.L. Oynamic	182.160.10.	0/24	ату	outoluo	a 172.16.1.5

طقطقة **يطبق.ملاحظة:** فيما يلي أوامر تكوين CLI المكافئة:

<u> تكوين ASA 7.2(2) CLI تكوين ا</u>

(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
                                                        !
                                   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 2KFOnbNIdI.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
```

I

Create an internal group policy "clientgroup."! group-policy clientgroup attributes vpn-tunnel-protocol webvpn
Enable webvpn as tunneling protocol. split-tunnel- ! policy tunnelall
Encrypt all the traffic coming from the SSL VPN! Clients. webvpn svc required
Activate the SVC under webvpn mode 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. username ssluser1 password ZRhW85jZqEaVd5P. encrypted
Create an user account "ssluser1." aaa local! authentication attempts max-fail 16
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
Create a tunnel group "sslgroup" with type as! WebVPN. 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. 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 enable outside
Enable WebVPN on the outside interface. svc image !

disk0:/sslclient-win-1.1.4.179.pkg 1

Assign an order to the SVC 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. prompt hostname context Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end #ciscoasa

إنشاء اتصال SSL VPN باستخدام SVC

أكمل هذه الخطوات لإنشاء اتصال SSL VPN مع ASA.

1. اكتب في حقل العنوان لمستعرض الويب الخاص بك عنوان URL أو عنوان IP لواجهة WebVPN الخاصة ب ASA.على سبيل المثال:

	<pre><https: <ip="" address="" asa="" interface<="" of="" pre="" the="" webvpn=""></https:></pre>
WebVPN Server	vice - Microsoft Internet Explorer
File Edit View	Favorites Tools Help
G Back 🝷 🤅	🕽 - 📓 💰 🔎 Search 🤺 Favorites 🤣 🎯 - 🌺 🔜 🦓
Address 🕘 https:,	//172.16.1.1/+webvpn+/index.html
CISCO SYSTEMS	• WebVPN Service
	Login
	Please enter your username and password.
	USERNAME:
	PASSWORD:
	GROUP: sslgroup_users
	Login Clear

2. أدخل اسم المستخدم وكلمة المرور، ثم أختر المجموعة الخاصة بك من القائمة المنسدلة الخاصة



3. بمجرد تأسيس الاتصال، انقر نقرا مزدوجا على رمز المفتاح الأصفر الذي يظهر في شريط المهام على

	ال حول المقال	CISCO Systel معلوم	IIS SSE VEN Client	وتربيعتر عن تتربع الأعوار	الحمبيا		
🥑 Cisco Systems SSL VPN Client 🛛 🛛 🔀							
CISCO SYSTEMS AILING SSLVPN CLIENT for WEBVPN							
Statistics Route Details About							
Addre	ess Informati	on	SSL Information				
Se	erver:	172.16.1.1	Cipher:	3DES SHA-1			
Cli	ent:	192.168.10.1	Version:	TLSv1			
Bytes			Transport Inform	nation			
Se	ent:	5471	Local LAN:	Disabled			
Re	eceived:	884	Split Tunneling:	: Disabled			
Frame	25		Connection Info	rmation			
Se	ent:	75	Time:	00:00:35			
Re	eceived:	12					
		Res	et				
		Close	Disconnect		.SSL		
4	Cisco Sys	tems SSL VPN C	lient				
CISCO SYSTEMS SSLVPN CLIENT for WEBVPN							
	adduced duce	SSL VPN CUE	INT for WEBVPN	N			
	Statistics	SSLVPN CLI	ENT for WEBVPN	N			
	Statistics	SSLVPN CLI Route Details Abo	UNT for WEBVPN	N Routes			
	Statistics Local LA	SSLVPN CLI Route Details Abo N Routes Subnet Ma	INT for WEBVPN	N Routes	sk		
	Statistics Local LA Network	SSLVPN CLI Route Details Abo N Routes Subnet Ma	INT for WEBVPN	Routes Subnet Mas 0.0.0.0	sk		
	Statistics Local LA	SSLVPN CLI Route Details Abo N Routes Subnet Ma	INT for WEBVPN	Routes Subnet Mas	sk		
	Statistics Local LA	SSLVPN CLI Route Details Abo N Routes Subnet Ma	INT for WEBVPN	Routes Subnet Mas 0.0.0.0	sk		
	Statistics Local LA	SSLVPN CLI Route Details Abo N Routes Subnet Ma	INT for WEBVPN	Routes Subnet Mas 0.0.0.0	sk		
	Statistics Local LA	SSLVPN CLI Route Details Abo N Routes Subnet Ma	INT for WEBVPN	Routes Subnet Mas 0.0.0.0	sk		
	Statistics Local LA	SSLVPN CLI Route Details Abo N Routes Subnet Ma	INT for WEBVPN	Routes Subnet Mas 0.0.0.0	sk		
	Statistics Local LA Network	SSLVPN CLI Route Details Abo N Routes Subnet Ma	INT for WEBVPN	Routes Subnet Mas 0.0.0.0	sk		
	Statistics Local LA Network	SSLVPN CLI Route Details Abo N Routes Subnet Ma	INT for WEBVPN	Routes Subnet Mas 0.0.0.0	sk		

🥑 Cisco Systems SS	L VPN Client			
CISCO SYSTEMS SSLVF	N CLIENT for WEBVPN			
Statistics Route Det	ails About			
CISCO SYSTEMS	SSL VPN CLIENT for WEBVPN Version 1.1.4.179			
6	Create a fully secure connection anywhere anytime SECURE REMOTE ACCESS.NOW.			
© Copyright 2004-2006 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems and the Cisco Systems Logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.				
	Close Disconnect			

<u>التحقق من الصحة</u>

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم <u>أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر</u> show. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر show .

.

```
show webVPN svc. يعرض صور SVC المخزنة في ذاكرة ASA المؤقتة.
دiscoasa#show webvpn svc
disk0:/sslclient-win-1.1.4.179.pkg 1 .1
CISCO STC win2k+ 1.0.0
1,1,4,179
Fri 01/18/2008 15:19:49.43
SSL VPN Client(s) installed 1
```

• show vpn-sessiondb svc – يعرض المعلومات حول إتصالات SSL الحالية. ciscoasa#show vpn-sessiondb svc

Session Type: SVC

: ssluser1 Username Index : 1 Assigned IP : 192.168.10.1 Public IP : 192.168.1.1 : SVC Protocol Encryption : 3DES Hashing : SHA1 : 131813 : 5082 Bytes Tx Bytes Rx (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
ciscoasa#show webvpn group-alias
Tunnel Group: sslgroup Group Alias: sslgroup_users enabled
```

.

• في ASDM، أخترت **monitore>VPN>VPN، أحسائيات>VPN>جلسة** in order to شاهدت معلومة حول الحالي WebVPN جلسة في ال

							.ASA
Nonitoring > VPN > VPN Statisti	cs > Sessions)					
P-E VPN Connection Graphs	Sessions						
PSec Tunnels	Remote Access	LAN-to-LAN	WebVPN	SSL VPN Client	E-mail Proxy	Total	Total Cumulative
Crypto Statistics	0	0	1	0	0	1	12
Compression Statistic Encryption Statistics Global IKE/IPSec Stat	Filter By: WebV	'PN 💌 🚥	All Sessions			Filter	
NAC Session Summa Protocol Statistics	Username IP Addres	Gr Gr Tu	roup Policy nnel Group	Protocol Encryptio	n	Login Time Duration	Details
Sessions WebVPN SS0 Statistics	ssluser1 192.168.1.1	clientgro ssigrou;	oup o	WebVPN 3DES	08:49:5 0h:08n	52 UTC Thu Mar 20 ແ14s	Logout
							Ping

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

• VPN-sessionDB logoff name <*username*/ يسمح أنت أن يدون خارج ال SSL VPN جلسة ل ال يعين

```
مستعمل إسم.
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
```

بالمثل، أنت يستطيع استعملت الأمر **vpn-sessiondb logoff svc** in order to أنهيت all the SVC جلسة.**ملاحظة:** إذا انتقل الكمبيوتر إلى وضع الاستعداد أو الإسبات، يمكن إنهاء اتصال SSL VPN.

```
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>** يوفر أحداث WebVPN في الوقت الفعلي لإنشاء الجلسة. 7 ^{Ciscoasa#debug} webvpn svc

> 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;g=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
```

• في ASDM، أختر **مراقبة > تسجيل > عارض السجل في الوقت الفعلي > عرض** لعرض الأحداث في الوقت الفعلي. تظهر هذه الأمثلة معلومات الجلسة بين SVC 192.168.10.1 و WebServer 10.2.2.2 في الإنترنت عبر ASA 172.16.1.5.

💼 Real-time Log Viewer			
👂 Resume 🗈 Copy 🎧 Save 🆓 Clear 🥂 Color Settings 🜓 Create Rule 📸 Show Rule 🝈 Show Details 💡 Help			
Filter By: Filter III Show Al Find:			
a ID	Source IP	Destination IP	Description
	192.168.10.255 10.77.244.193		No translation group found for udp src outside:192.168.10.1/138 dst inside:192.168.10.255/138 No translation group found for udp src outside:192.168.10.1/1027 dst inside:10.77.244.193/53
ſ	192.168.10.1 192.168.10.1	10.2.2.2	Built inbound TCP connection 1902 for outside:192.168.10.1/1000 (172.16.1.5/1025) to outside:10.2.2.2/80 (10.2.2.2/80) (ssluser1) Built dynamic TCP translation from outside:192.168.10.1/1100 to outside:172.16.1.5/1025
	192.168.10.255 10.77.244.193 10.77.244.193		No translation group found for udp src outside:192.168.10.1/138 dst inside:192.168.10.255/138 No translation group found for udp src outside:192.168.10.1/1027 dst inside:10.77.244.193/53 No translation group found for udp src outside:192.168.10.1/1028 dst inside:10.77.244.193/53
I	10.77.244.193		No translation arous found for udo arc outside:192.168.10.1/1027 dist inside:10.77.244.193/53
Please select a syslog entry to see the explanation			
Explanation Recommended Action Details			
U Emergencies U Alerts 🐠 Critical 😝 Errors 🙏 Warnings 🚊 Notifications 🗼 Informational 🔌 Debugging			

<u>معلومات ذات صلة</u>

- <u>صفحة دعم جهاز الأمان القابل للتكيف طراز Series 5500 من Cisco</u>
- عميل PIX/ASA 7.x و VPN لشبكة VPN العامة عبر الإنترنت على مثال تكوين العصا
 - <u>ASDM مع مثال تكوين ASA) على ASA مع مثال تكوين ASDM) •</u>
 - <u>الدعم التقني والمستندات Cisco Systems</u>

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما