يداحأ لوخد ليجستو WebVPN عم ASA و ASDM نيوكت لاثم مادختساب

المحتويات

المقدمة المتطلبات الأساسية المتطلبات المكونات المستخدمة الاصطلاحات التكوين إضافة خادم AAA لمصادقة مجال Windows انشاء شهادة موقعة ذاتيا تمكين WebVPN على الواجهة الخارجية تكوين قائمة عناوين URL للخادم (الخوادم) الداخلي تكوين نهج مجموعة داخلي <u>تكوين مجموعة نفق</u> تكوين الموقع التلقائي للخادم تكوين ASA النهائي التحقق من الصحة إختبار تسجيل دخول WebVPN جلسات المراقبة تصحيح أخطاء جلسة WebVPN استكشاف الأخطاء واصلاحها معلومات ذات صلة

<u>المقدمة</u>

يصف هذا المستند كيفية تكوين جهاز الأمان القابل للتكيف (ASA) من Cisco لتمرير بيانات اعتماد تسجيل دخول مستخدم WebVPN تلقائيا، بالإضافة إلى المصادقة الثانوية، إلى الخوادم التي تتطلب التحقق من تسجيل الدخول الإضافي مقابل Windows Active Directory الذي يشغل الإصدار 1 من مدير شبكة LAN NT (NTLMv1). تعرف هذه الميزة باسم تسجيل الدخول الأحادي (SSO). وهو يمنح الارتباطات التي تم تكوينها لمجموعة WebVPN معينة القدرة على تمرير معلومات مصادقة المستخدم هذه، وبالتالي تقليل مطالبات المصادقة المتحدم هذه الميزة على مستوى التكوين العام أو مستوى تكوين المستخدم.

<u>المتطلبات الأساسية</u>

<u>المتطلبات</u>

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

• تأكد من تكوين أذونات NTLMv1 و Windows لمستخدمي VPN الهدف. راجع وثائق Microsoft للحصول على مزيد من المعلومات حول حقوق الوصول إلى مجال Windows.

<u>المكونات المستخدمة</u>

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

- (Cisco ASA 7.1(1 •
- مدير أجهزة حلول الأمان المعدلة (ASDM) 5.1(2) من Cisco
 - خدمات معلومات الإنترنت (IIS) من Microsoft

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>التكوين</u>

في هذا القسم، تقدم لك معلومات تكوين ASA كخادم WebVPN مع SSO.

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

إضافة خادم AAA لمصادقة مجال Windows

أكمل هذه الخطوات لتكوين ASA لاستخدام وحدة تحكم بالمجال للمصادقة.

1. حدد **تكوين > خصائص > إعداد AAA > خوادم AAA** وانقر **إضافة**. قم بتوفير اسم لمجموعة الخوادم، مثل Windows_NT، واختر **مجال NT** كبروتوكول.

🔂 Claco ASDM !	5.1 for ASA -	172.16.172.57							2				
File Rules Be	arch Options	Tools Wizards	: Help		~	-	-		Cesto	Sector			
Hone (Configuration	Nonitoring	Back	Forward	Search	C+ Refresh	Save -	2 Help	ally				
Hone (Interfaces Security Policy NAT VINI CSD Viens per PS Reading Reading Gibbal Caperts	Configuration	Monitoring Proceediess - Al Proceediess - Al Proceediess - Al Proceediess Access Access Access Stervices Stervic	Beck	Forward I	Protoc Los	Refresh of Az CAL Interface	Sove counting M	Holp ode Reactiva Timeo	ton Mode Add Edit Detel X Add Edit Detel Miros J View co				
Projectics	-∰TCF 0 -ॐTimed ⊏∰URL P ∎	ptions ute litering			c e	Apply cc 1		Reset	Configure AAA Serve Configure AAA serve applicable for RAD Server Group:	r Group Kergroup The Ar IUE and TACACI Windows	counting Mod E+ protocols. NT	e attribute is only	
_									Perment	NT Doord			
									Protocol Accounting Mode.	⊖ Smul≿	ueore S) Single	
									Reactivation Mode:	: Opplet	on (Timed	
									Dead	Time. 10		minutes	
									Na: Failed Attempt	8: 3			
									DX		ancel	Help	

2. إضافة خادم Windows.حدد المجموعة التي تم إنشاؤها حديثا وانقر فوق **إضافة**. حدد الواجهة التي يوجد بها الخادم وأدخل عنوان IP واسم وحدة التحكم بالمجال. تأكد من إدخال اسم وحدة التحكم بالمجال في كافة الأحرف الكبيرة. انقر فوق موافق عند الانتهاء.

🔂 Cisco ASDM 5	5.1 for ASA - 172.16.172.52		
File Prinss da	And Options Tools Wizards		Gisco Systems
Home C	Configuration Montoring	Back Forward Search Refresh Save Help	ավիստվիսե
Interfaces Becurity Policy NAT Security Policy NAT CSD Monager CSD Monager Ins Rodrig Gladed Objects	Configuration > Properties > AV	Wetup > AAA Beners Am Servers Server Groups Server Structure Dock Server Server Name or IP Address Interface	Note Add Edit Delete Note Edit Delete Note Edit Delete Note Edit Delete
Properties	- 3월TCP Options 이Timeouls - 양URL Filtering	Apply Rest Server (AA Server 🔀 Group: Windows_NT
		cisco NA (15) 🔯 🕼 interfac	e Name: inside 💌
		Server I Timeou NT Dan Serve Dema	Name or IP Address: 10.1.1.200 it: 10 seconds nain Parameters er Port: 138 an Dontroller: ESO-&I-7800 OK Cancel Help

تعرض هذه النافذة تكوين AAA المكتمل:

📬 Cisco ASDM 5	i.1 for ASA - 172.16.171.51		
File Rules Ser	arch Options Tools Wizards	Help	
Home C	Sonfiguration Monitoring	C C C C C C C C C C C C C C C C C C C	CISCO SYSTEMS
	Configuration > Properties > A#	A Setup > AAA Servers	
	●金革 ■ 前 湯風	a @ 魚 篇 今	
Interfaces	- Startup Wizard	AAA Servers	
<u>6</u> ,	AAA Setup	Server Groups	
Security Policy	Auth. Prompt	Server Group Protocol Accounting Mode Reactivation Mode	Add
20	- Sa LDAP Attribute N	LOCAL LOCAL	
1010	- BAnti-Spoofing	Windows_NT NT Domain Depletion	Edit
	⊞ ∎ ARP		Delete
<u>84</u>	- Auto Update		
YPN -	Authentication	8	
A	Enrollment		
CSD Manager		Servers in Selected Group	
rta -	- 🍀 Key Pair	Pener Name or IP Address Interface Timeoud	Add
9	Hanage Certific:	10.1.1.200 incide 10	
IPS		10.1.1.200 Inside 10	Edit
4 <u>₹</u> 4	Device Administrati		Delete
Routing	DHCP Services		
8			Move up
67 8	- @Failover		Move down
Global Objects	Fragment		
5	History Metrics		Test
Properties	E P Audit		
	👜 🖽 Logging		
	- 🚍 Priority Queue 🔹	Apply Reset	
Configuration cha	inges saved successfully.	cisco NA (15) 📑 🔂 3/3	0/06 1:57:40 PM UTC

إنشاء شهادة موقعة ذاتيا

أكمل هذه الخطوات لتكوين ASA لاستخدام شهادة موقعة ذاتيا.

ملاحظة: في هذا المثال، يتم إستخدام شهادة موقعة ذاتيا لتحقيق البساطة. لخيارات تسجيل الشهادة الأخرى، مثل التسجيل مع مرجع شهادة خارجي، راجع <u>تكوين الشهادات</u>.

- 1. حدد **تشکیل > خصائص > ترخیص > TrustPoint > تشکیل** وانقر **إضافة**.
- 2. في النافذة التي تظهر أدخل اسم TrustPoint مثل Local-TP وحدد **إنشاء شهادة موقعة ذاتيا على التسجيل**. يمكن ترك الخيارات الأخرى مع إعداداتها الافتراضية. انقر فوق موافق عند الانتهاء.



تعرض هذه النافذة تكوين TrustPoint المكتمل:



<u>تمكين WebVPN على الواجهة الخارجية</u>

أكمل هذه الخطوات للسماح للمستخدمين خارج الشبكة بالاتصال باستخدام WebVPN.

- 1. حدد **تكوين > VPN > WebVPN > وصول WebVPN**.
- 2. حدد الواجهة المطلوبة، وانقر فوق تمكين، ثم حدد تمكين القائمة المنسدلة لمجموعة النفق في صفحة تسجيل الدخول إلى WebVPN و ASDM و MebVPN ، فيجب عليك الدخول إلى WebVPN و ASDM ما ستخدام نفس الواجهة للوصول إلى 8080، ويتم القيام بذلك ضمن تغيير المنفذ الافتراضي للوصول إلى ASDM من المنفذ 80 إلى منفذ جديد مثل 8080، ويتم القيام بذلك ضمن التكوين > الخصائص > الوصول إلى HTTPS/ASDM من المنفذ 80 إلى منفذ جديد مثل 8080، ويتم القيام بذلك ضمن التكوين > الخصائص > الوصول إلى HTTPS/ASDM من المنفذ 90 إلى منفذ جديد مثل 8080، ويتم القيام بذلك ضمن التكوين > الخصائص > الوصول إلى الجهاز > http://sip_address. ملاحظة: يمكنك إعادة توجيه مستخدم إلى المنفذ 40 إلى منفذ جديد مثل 4000، ويتم القيام بذلك ضمن التكوين > الخصائص > الوصول إلى الجهاز > http://sip_address. يمكنك إعادة توجيه مستخدم إلى المنفذ 40 إلى الجهاز > http://sip_address. يمكنك إعادة توجيه مستخدم إلى المنفذ 200 المنفذ 443 يرمن خطة: يمكنك إعادة توجيه مستخدم إلى المنفذ 200 المنفذ 240 بدلا من حدير من 4000. حدد المنفذ 240 تلوبي الجهاز > https://eip_address بدلا من حدة إلى الجهاز > https://eip_address. بدلا من حدة من 400 المنفذ 443 تلوبي المنفذ 443 تلوبي المنفذ 443 تلوبي الجهاز > https://eip_address بدلا من 500 التكرابي الجهاز > https://eip_address. وحدذ إعادة توجيه 400 إلى الحما إلى تكوين > خصائص > الوصول إلى الحما إلى الحما إلى واجهة المطلوبة، وانقر تحرير وحدد إعادة توجيه 400 إلى HTTPS.

🖆 Cisco ASDM 5	i.1 for ASA - 172.16.171.51			
File Rules Se	arch Options Tools Wizards	Help		
G Home C	onfiguration Montering	Back Forward Search Refres	h Save Help	Cisco Systems
	Configuration > VPN > WebVPN	I > WebVPN Access		
	● 坐 革 ■ 前 湯 暭	1 ili 💁 🛍 🗳 i		
Interfaces	🔁 📲 E-mail Proxy 📃 🛌	WebVPN Access		
<u>6</u> ,	General			
Security Policy	- Default Tunnel G	 Configure access parameters for WebYF currently provided as a free trial, and future 	PN. (Note: The WebVPN features in this re major software releases will require (software release are the purchase and
34,	Group Policy	installation of a WebVPN feature license)	ne parenezo ano
NAT	- Tunnel Group			
	A System Opt	Interface	WebVPN Enabled	Enable
<u>84</u>	THE Sale Address Manager	nutside	Ves	Dieshla
VPN		bacarde.	103	Disania
A				
CSD Manager	E WebVPN			
12				
IPS	- CSD Setup	Port Number 443		
.7.	😹 Cache			
ಿಷ್ಟೆ	- Content Rewrite	Default Idle Timeout: 1800	seconds	
Routing	- Encoding	Max Sectional limit: 2		
<u>&</u>	- Proxies			
Global Objects	- Proxy Bypass	WebVPN Memory Size: 50	% of total physical memory 🛛 👻	
	- 38 SSL VPN Client	Enable Tuppel Group Dron-down Lis	t on WebVPN Login Page	
Properties	SSO Servers			
Properties	- Egiservers and URI			
	Webpage Custor -	Ар	ply Reset	
Configuration cha	inges saved successfully.	cisco	NA (15) 🛛 🚔 🔂 🔹 🔒	3/30/06 2:37:41 PM UTC

<u>تكوين قائمة عناوين URL للخادم (الخوادم) الداخلي</u>

أكمل الخطوات التالية لإنشاء قائمة تحتوي على الخوادم التي تريد منح مستخدمي WebVPN الوصول إليها.

- 1. حدد **تشكيل > VPN > WebVPN > خوادم و URLs** وانقر **إضافة**.
- 2. أدخل اسما لقائمة URL. هذا الاسم غير مرئي للمستخدمين النهائيين. انقر فوق **إضافة (Add)**.
- 3. أدخل اسم عرض عنوان URL كما سيتم عرضه للمستخدمين. أدخل معلومات عنوان URL الخاص بالخادم. يجب أن تكون هذه هي الطريقة التي تصل بها عادة إلى الخادم.

Cisco ASDM 5	.1 for ASA - 172.16.172.52 min. Online. Toole. Minerie	Liela	
Сонцикана и сон	onfiguration Nonitoring	Back Forward Search Refresh Save Hep	Cisco Systems
Interfaces	Contiguitation > VPN > WebYPN	Servers and URLs Servers and URLs Servers and URLs Configure lists of servers and URLs for access over WebVPN.	
	Acdress Manageme Acdress Manageme Pac Pac	List Name URL Display Name URL	Edit
CSD Manager PS PS Routing	- ACSD Betup Cache Content Rewrite Pet Forwarding Proxies Proxies SEL VPN Client	List Name: Webserver	×
Global Objects	- 13880 Servers Servers and URLS Webpage Customi Add Ser	Ver or URL	URL Add Edit
	URLDI	splay Name: Internal Server	Mova Up Move Down
	URL:	https i g 10.1.1.200	antel Help

4. طقطقت **ok، ok، و**بعد ذلك **طبقت**.

🖆 Cisco ASDM 5	.1 for ASA - 172.16.171.51				
File Rules Sea	arch Options Tools Wizards	Help			
Home C	onfiguration Monitoring	Back Forward	Q Search Refresh	Save Help	Cisco Systems
	Configuration > VPN > WebVPN >	Servers and URLs			
	●金革 ■ 前 炎陥	6666			
Interfaces	🗧 🚰 🕒 🛌	Servers and URLs			
Es Security Policy	⊕ 않E-mail Proxy 호텔General 문화 및 Client Update	Configure lists of se	rvers and URLs for acc	cess over WebYPN.	
24		List Name	URL Display Name	URL	Add
NAT	- Croup Policy	webserver	Internal Server	https://10.1.1.200	
SK VPN	Souther Group				Delete
CSD Manager	Super Address Hanager				
IPS					
Routing	- MCSD Setup - MCSC Setup - MCSC Setup - MCSC Setup				
Right Chiefts	- The Encoding - The Port Forwarding				
5	- Proxy Bypass				
Properties	Servers Servers and URL WebVPN Access		Apply	Reset	
Configuration cha	nges saved successfully.		cisco	NA (15) 🛛 🛃 🔂	🔒 3/30/06 1:54:10 PM UTC

تكوين نهج مجموعة داخلي

أكمل هذه الخطوات لتكوين نهج مجموعة لمستخدمي WebVPN.

- 1. حدد **تشكيل > VPN > عام > نهج المجموعة**، انقر **إضافة**، وحدد **نهج المجموعة الداخلي**.
- 2. في علامة التبويب "عام"، حدد أسَّم نهج، مثل Internal-Group_POL_WEBVPN. ثمَّ قم بإلغاء تحديد Inherit بجوار بروتوكولات الاتصال النفقي وفحص WebVPN.

🔂 Ad	d Internal Group Policy		
Ν	ame: nal-GRP_POL_	WEBVPN	
Ge	neral IPSec Client Confi	guration Clie	nt Firewall Hardware Client WebVPN
0	Check an Inherit checkbox t	o let the corres	sponding setting take its value from the default group policy.
1	Funneling Protocols:	📃 Inherit	IPSec VebVPN
F	Filter:	🗹 Inherit	Manage
Γ	Connection Settings	D lake site	
	Access Hours:	🕑 innerit	New
	Simultaneous Logins:	🗹 Inherit	
	Maximum Connect Time:	🖌 Inherit	Unlimited minutes
	Idle Timeout:	🗹 Inherit	Unlimited minutes
	Servers		
	DNS Servers:	🖌 Inherit	Primary: Secondary:
	WINS Servers:	🖌 Inherit	Primary: Secondary:
	DHCP Scope:	🗹 Inherit	
		OK	Cancel Help

3. في علامة التبويب WebVPN حدد علامة التبويب الفرعية **أخرى**. قم بإلغاء تحديد **توريث** بجوار الخوادم وقوائم عناوين URL وحدد قائمة عناوين URL التي قمت بتكوينها من القائمة المنسدلة. انقر فوق موافق عند الانتهاء.

🕵 Add Intern	al Group Policy					×
Name:	mal-GRP_POL_W	EBVPN				
General IF	Sec Client Config	uration Clien	t Firewall Hardware Clie	nt WebVPN		
Configura	Alah)/DN attributor i	cing the fello	wing take			
Check an li	nherit checkbox to le	t the correspo	unding setting take its valu	e from the de	efault group policy.	
					inaan groap ponoj.	
Functions	Content Filtering	Homepage	Port Forwarding Other	SSL VPN CI	ient	
Serve	rs and URL Lists:	📃 Inherit	webserver	<u> </u>	New	
Web-	Type ACL ID:	🗹 Inherit			Manage	
SSO	Server:	🗹 Inherit			New	
нттр	Compression:	🗹 Inherit	⊖ Enable ⊖ D	isable		
-Keep	oalive Ignore					
Spe	cify upper limit of the	HTTP/HTTP	S traffic, per transaction to	ignore.		
Tra	neartion Size: 🔽	Inherit	LUR.			
1 an		, millione				
-Dem	Message					
	Inherit					
		OK	leaned	Help		
				Treip		

<u>تكوين مجموعة نفق</u>

أكمل هذه الخطوات لتكوين مجموعة نفق لمستخدمي WebVPN لديك.

1. حدد **تكوين > VPN > عام > مجموعة أنفاق**، انقر فوق **إضافة** وحدد **وصول** WebVPN...

🖆 Cisco ASDM 5	.1 for ASA - 172.16.172.52				
File Rules Sea	ach Options Tools Wizards	Help			
ổ наме С	onfiguration Manifering	Back Forwerd Seerch	Retresh Save	? Нер	Cisco Systems
	Configuration > VPN > General >	Tunnel Group			
	●金革 ■ 菌 蒸勉	■ 爲 邕 ♀			
Interfaces	- 🚰 YPN Wizard 👘	Tunnel Group			
Security Policy	표 역을 E-mail Proxy 한 33 General - 글 Client Update - 같 Default Tunnel Gat	Manage VPN tunnel groups. IPSec or WebVPN connectio	A VPN tunnel group re. n.	presents a connection sp	ecific record for a
NAT	- Group Policy	Name 1	Type	Group Policy	Add 🔻
03	- WPN System Option	DefaulfWEBVPNGroup w	ebypn	DftGrpPolicy	IPSec for Remote Access
	B-%IKE	DefaultRAGroup ip	sec-ra	DftOrpPolicy DftOrpPolicy	IPSec for LAN to LAN Access
CSD Manager	- Policy - PRules - Rules - Policies - Policies - Policies - Policies - Policies - Policies - Policies - Policies - Policies - Provincies - Policy - Policies - Poli				
Routing Routing Global Objects	} NebvPN	Specify the delimeter to be u are received when tunnels a Group Delimiter: Noni	sed when parsing turn re being negotiated. a V	el group names from the	user name that
Properties			Apply	Reset	
Configuration cha	nges saved successfully.	lei	sco NA (15)	12 - 2 - 2	4/13/06 10:56:08 AM PBT
			1		

2. أدخل اسم لمجموعة النفق، مثل WEB_VPN-GRP. في علامة التبويب "أساسي" حدد "نهج المجموعة" الذي أنشأته وتحقق من أن "نوع المجموعة" هو WebVPN.

📧 Edit Tunnel Group 🛛 🛛 🔀
Name: WEB_VPN-GRP Type: webvpn
General WebVPN
Configure general access attributes from the following sub-tabs.
Basic AAA Client Address Assignment Advanced
Group Policy: Internal-GRP_POL
Internal-GRP_POL_WEBV
Strip the realm from username before passing it on to the AAA server
Strip the group from username before passing it on to the AAA server
OK Cancel Help

3. انتقل إلى علامة التبويب AAA.بالنسبة لمجموعة خوادم المصادقة، أختر المجموعة التي قمت بتكوينها لتمكين مصادقة NTLMv1 باستخدام وحدة التحكم في المجال الخاصة بك.**إختياري:** حدد **إستخدام محلي إذا فشلت مجموعة الخوادم** في تمكين إستخدام قاعدة بيانات المستخدم المحلية في حالة فشل مجموعة AAA التي تم تكوينها. يمكن أن يساعدك ذلك على أستكشاف الأخطاء وإصلاحها في وقت لاحق.

🖆 Edit Tunnel Group	×
Name: WEB_VPN-GRP Type: webvpn	
General WebVPN	
Configure general access attributes from the following sub-tabs.	
Racic AAA Client address Assignment Advanced	
Dasit And Cilent Address Assignment Advanced	
To set authentication server group per interface, go to the Advanced tab.	
Authentication Server Group: Windows_NT	
Use LOCAL if Server Gra None	
Authorization Server Group: LOCAL	
Users must exist in the authorization database to connect	
Accounting Server Group:	
Authorization Settings	
O Use the entire DN as the username	
 Specify individual DN fields as the username 	
Primary DN Field: CN (Common Name)	
Secondary DN Field: OU (Organization Unit)	
-Password Management	
Override account-disabled indication from AAA server	
Enable notification upon password expiration to allow user to change password	
Enable notification prior to expiration Notify days prior to expiration	
OK Cancel Help	

- 4. انتقل إلى علامة التبويب WebVPN ثم انتقل إلى علامة التبويب الفرعية **أسماء المجموعات المستعارة وعناوين** URL.
 - 5. أدخل اسما مستعارا ضمن الأسماء المستعارة للمجموعة وانقر فوق **إضافة**. يظهر هذا الاسم المستعار في القائمة المنسدلة المقدمة إلى مستخدمي WebVPN عند تسجيل الدخول.

🖆 Edit Tunnel Group	
Name: WEB_VPN-GRP Type: webvpn	
Conorol WebVPN	
General Weberna	
Configure WebVPN access attributes from the following sub-tabs.	
Basic NetBIOS Servers Group Aliases and URLs Web Page	
Group Aliases	
Alias	Status
Add >> Group-Selection	enable
<< Remove	
- Oraun LIDL -	
URL	Status
URL (http or https): Add >>	
<< Remove	
Enable	
OK Concel Hein	
Cancer Help	

6. طقطقت **ok** وبعد ذلك **يطبق**.

<u>تكوين الموقع التلقائي للخادم</u>

قم بالتبديل إلى سطر الأوامر لتمكين SSO للخادم (الخوادم) الداخلية لديك.

ملاحظة: لا يمكن إكمال هذه الخطوة في ASDM ويجب إنجازها باستخدام سطر الأوامر. راجع <u>الوصول إلى واجهة</u> <u>سطر الأوامر</u> للحصول على مزيد من المعلومات.

أستخدم الأمر **auto-signon** لتحديد مورد الشبكة، مثل الخادم، الذي تريد منح المستخدمين إمكانية الوصول إليه. يتم تكوين عنوان IP لخادم واحد هنا، ولكن يمكن أيضا تحديد نطاق شبكة مثل 10.1.10 /24. راجع أمر <mark>الموقع التلقائي</mark> للحصول على مزيد من المعلومات. في إخراج هذا المثال، يتم تكوين الأمر **auto-signon** ل WebVPN بشكل عام. كما يمكن إستخدام هذا الأمر في وضع تكوين مجموعة WebVPN أو وضع تكوين اسم مستخدم WebVPN. يحد إستخدام هذا الأمر في وضع تكوين مجموعة WebVPN هذا الأمر على مجموعة معينة. وعلى نحو مماثل، يحد إستخدام هذا الأمر في وضع تكوين اسم مستخدم WebVPN هذا الأمر على مستخدم واحد. راجع أمر <u>الموقع التلقائي</u> للحصول على مزيد من المعلومات.

تكوين ASA النهائي

يستعمل هذا وثيقة هذا تشكيل:

1	ASA الإصدار 7.1(ا
ASA# sho	w running-config
	Saved :
	:
(A	SA Version 7.1(1 !
te	rminal width 200
	hostname ASA
domai	n-name cisco.com
enable password 8Rv2YiIvt7	RRXII24 encrypted
	names
	11211105
interface Ci	·
Incertace GI	yabitetiletilet///
	nameri outside
S	ecurity-level 0
ip address 172.16.171.5	1 255.255.255.0
	!
interface Gi	gabitEthernet0/1
	nameif inside
sec	urity-level 100
ip address 10.1.1.	1 255.255.255.0
	!
interface Gi	gabitEthernet0/2
	shutdown
	no nameif
no	security-level
	no ip address
	!
interface Gi	gabitEthernet0/3
	shutdown
	no nameif
no	security-level
-	no ip address
	!!
interfa	ce Management0/0
	shutdown
	no nameif
no	security-level
110	no in address
	TO TH GOULERS
Second Otherstat	2KVOU on amount of
passwa ZKFQNDNIAI	.ZKIUU encrypted
	Lup mode passive
dns server-	group DefaultDNS
domain	-name cisco.com

pager lines 24 mtu inside 1500 mtu outside 1500 no failover asdm image disk0:/asdm512.bin no asdm history enable arp timeout 14400 route outside 0.0.0.0 0.0.0.0 172.16.171.1 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 timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute AAA server configuration aaa-server Windows_NT ---! protocol nt aaa-server Windows_NT host 10.1.1.200 ntauth-domain-controller ESC-SJ-7800 !--- Internal group policy configuration group-policy Internal-GRP_POL_WEBVPN internal group-policy Internal-GRP_POL_WEBVPN attributes vpn-tunnel-protocol webvpn webvpn url-list value webserver username cisco password Q/odgwmtmVIw4Dcm encrypted privilege 15 aaa authentication http console LOCAL aaa authentication ssh console LOCAL aaa authentication enable console LOCAL http server enable 8181 http 0.0.0.0 0.0.0.0 outside no snmp-server location no snmp-server contact snmp-server enable traps snmp authentication linkup linkdown coldstart !--- Trustpoint/certificate configuration crypto ca trustpoint Local-TP enrollment self crl configure crypto ca certificate chain Local-TP certificate 31 308201b0 30820119 a0030201 02020131 300d0609 2a864886 f70d0101 04050030 1e311c30 1a06092a 864886f7 0d010902 160d4153 412e6369 73636f2e 636f6d30 1e170d30 36303333 30313334 3930345a 170d3136 30333237 31333439 30345a30 1e311c30 1a06092a 864886f7 0d010902 160d4153 412e6369 73636f2e 636f6d30 819f300d 06092a86 4886f70d 01010105 0003818d 00308189 02818100 e47a29cd 56becf8d 99d6d919 47892f5a 1b8fc5c0 c7d01ea6 58f3bec4 a60b2025 03748d5b 1226b434 561e5507 5b45f30e 9d65a03f 30add0b5 81f6801a 766c9404 9cabcbde 44b221f9 b6d6dc18 496fe5bb 4983927f adabfb17 68b4d22c cddfa6c3 d8802efc ec3af7c7 749f0aa2 3ea2c7e3 776d6d1d 6ce5f748 e4cda3b7 4f007d4f 02030100 01300d06 092a8648 86f70d01 01040500 03818100 c6f87c61 534bb544 59746bdb 4e01680f 06a88a15 e3ed8929 19c6c522 05ec273d 3e37f540 f433fb38 7f75928e 1b1b6300 940b8dff 69eac16b af551d7f 286bc79c e6944e21 49bf15f3 c4ec82d8 8811b6de 775b0c57 e60a2700 fd6acc16 a77abee6 34cb0cad 81dfaf5a f544258d cc74fe2d 4c298076 294f843a edda3a0a 6e7f5b3c quit !--- Tunnel group configuration tunnel-group WEB_VPN-GRP type webvpn tunnel-group WEB_VPN-GRP general-attributes authentication-server-group Windows_NT default-grouppolicy Internal-GRP_POL_WEBVPN tunnel-group WEB_VPN-GRP webvpn-attributes group-alias Group-Selection enable telnet timeout 5 ssh timeout 5 console timeout 0 ! class-map inspection_default match default-inspectiontraffic ! ! policy-map global_policy class inspection_default inspect dns maximum-length 512 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

<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 .

إختبار تسجيل دخول WebVPN

قم بتسجيل الدخول كمستخدم لاختبار التكوين الخاص بك.

1. حاول تسجيل الدخول إلى ASA مع معلومات المستخدم من مجال NT الخاص بك. حدد الاسم المستعار للمجموعة الذي تم تكوينه في الخطوة 5 ضمن <u>تكوين مجموعة</u>

	يعق.
3 WebVPN Service - Microsoft Internet Explorer	
Ele Edit View Figvorites Icols Help	an 🕸 🛛
😋 Back 🔹 😥 🔹 🌠 🖉 🔎 Search 🤸 Favorites 🤣 🎯 - 🌺 🚍 🦓	
Address 🕘 https://172.16.171.51/+webvpr+/index.html	💙 🄂 Go Unks 🎽
CISCO SYSTEMS wellinger WebVPN Service	
Login	
Please enter your usemame and password.	1
USERNAME: test	
PASSWORD:	
GROUP: Group-Selection	
Login Clear	
	-
a Done	🔒 🔮 Internet

2. ابحث عن الارتباط (الارتباطات) الذي تم تكوينه للخادم (الخوادم) الداخلي. انقر فوق الارتباط للتحقق.

🖻 WebVPN Service - Microsoft Internet Explorer				
Ele Edit Yew Favorites Icols Help		R		
🕒 Back + 🕗 - 🖹 🗟 🏠 🔎	🔎 Search 🤺 Favorites 🚱 😥 - 🌺 🚍 🦓			
Address 🙆 https://172.16.171.51/+webvpn+/p	ipoetal.html 💌 🛃 Go 🛛 Lini	з ж		
🛐 Pop-up blocked. To see this pop-up or additional options dick here 🗙				
Cisco Systems WebVPN Servi	ice			
	Click here to open the Floating Toolbar 🖓 🎑 🔀			
WEB APPLICATIONS	Web Bookmarks			
Enter Web Address (URL)	Internal Server			
Go				
Web Bookmarks 🛛 👻				
		Ξ.		
		-		
javascript:top.doWebUH("https://10.1.1.200")) S 🔒 🔮 Internet			

جلسات المراقبة

حدد **مراقبة > VPN > إحصائيات VPN > جلسات العمل** وابحث عن جلسة عمل WebVPN التي تنتمي إلى المجموعة التي تم تكوينها في هذا المستند.

🖆 Cisco ASDM 5.1 for ASA - 172.16.171.51					
File Rules Sea	arch Options Tools Wizards	: Help			
G Home C	Sontiguration Monitoring	O O Q O O Cisco Systems Back Forward Search Refresh Save Help			
	Monitoring > VPN > VPN Statist	ica > Sessiona			
Interfaces	P 2 VPN Connection Grapi	Sessions Remote LAN-to-LAN WebVPN SSL VPN Client E-mail Proxy Total Total			
VPN	Cluster Loads				
PS S	Compression Stat	Filter By: WebVPN All Sessions Filter			
Routing	Protocol Statistics	IP Address Tunnel Group Encryption Duration			
Properties	Ġ· 몰 WebVPN └─ 王 SSO Statistics	test Internal-ORP_POL WebVPN 15:03:38 UTC Thu t Cogour 171.69.89.116 WEB VPN-GRP 3DES 0h:01m:18s Ping			
Logging					
		To solt VPN sessions, righ-click on the above table and select Table Solt Order from popup menu.			
		Logout By: All Sessions Logout Sessions			
		Refresh			
Data Refreshed S	accessfully.	cisco NA (15) 🔡 🚮 🐼 🔒 3/30/06 3:05:21 PM UTC			

تصحيح أخطاء جلسة WebVPN

هذا الإخراج هو نموذج تصحيح أخطاء لجلسة عمل WebVPN ناجحة.

ملاحظة: ارجع إلى <u>معلومات مهمة حول أوامر التصحيح</u> قبل إستخدام أوامر debug.

```
ASA#debug webvpn 255
                                                         INFO: debug webvpn enabled at level 255
                                                                                             #ASA
                                            [ASA# webvpn_portal.c:ewaFormServe_webvpn_login[1570
                                                    [webvpn_portal.c:http_webvpn_kill_cookie[385
                                                                   [webvpn_auth.c:webvpn_auth[286
                                                                      !!WebVPN: no cookie present
                                                [webvpn_portal.c:ewaFormSubmit_webvpn_login[1640
                                                    [webvpn_portal.c:http_webvpn_kill_cookie[385
                                              [webvpn_auth.c:http_webvpn_pre_authentication[1782
Begin AAA WebVPN: calling AAA with ewsContext (78986968) and nh (78960800)! WebVPN: started ---!
                                                                           ... user authentication
                                                         [webvpn_auth.c:webvpn_aaa_callback[3422
                                                                    (WebVPN: AAA status = (ACCEPT
                                                [webvpn_portal.c:ewaFormSubmit_webvpn_login[1640
                                             [webvpn_auth.c:http_webvpn_post_authentication[1095
                                                              .WebVPN: user: (test) authenticated
                                        End AAA webvpn_auth.c:http_webvpn_auth_accept[2093] ---!
webvpn_session.c:http_webvpn_create_session[159] webvpn_session.c:http_webvpn_find_session[136]
                                                                          !WebVPN session created
```

```
[webvpn_session.c:http_webvpn_find_session[136
                                                 [webvpn_db.c:webvpn_get_server_db_first[161
                                                  [webvpn_db.c:webvpn_get_server_db_next[202
                                                                 (traversing list: (webserver
                                            [webvpn_portal.c:ewaFormServe_webvpn_cookie[1421
                                                              [webvpn_auth.c:webvpn_auth[286
                                              [webvpn_session.c:http_webvpn_find_session[136
                                               [webvpn_session.c:webvpn_update_idle_time[924
                                                      .WebVPN: session has been authenticated
                                                              [webvpn_auth.c:webvpn_auth[286
                                              [webvpn_session.c:http_webvpn_find_session[136
                                               [webvpn_session.c:webvpn_update_idle_time[924
                                                      .WebVPN: session has been authenticated
                                        Output supressed webvpn_auth.c:webvpn_auth[286] ---!
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
                      WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
                      WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn session.c:http webvpn find session[136] webvpn session.c:webvpn update idle time[924]
                      WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
                      WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
      WebVPN: session has been authenticated. webvpn_session.c:http_webvpn_find_session[136]
                                               [webvpn_session.c:webvpn_update_idle_time[924
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

- إذا لم يكن المربع المنسدل الخاص بالمجموعة موجودا في صفحة تسجيل الدخول إلى WebVPN، فتأكد من إكمال الخطوة 2 ضمن <u>تمكين WebVPN على الواجهة الخارجية</u> والخطوة 5 ضمن <u>تكوين مجموعة نفق</u>. إذا لم يتم إكمال هذه الخطوات وكانت القائمة المنسدلة مفقودة، تقع المصادقة ضمن المجموعة الافتراضية ومن المحتمل أن تفشل.
- على الرغم من أنه لا يمكنك تعيين حقوق الوصول للمستخدم في ASDM أو في ASA، إلا أنه يمكنك تقييد المستخدمين بحقوق الوصول إلى Microsoft Windows على وحدة التحكم بالمجال الخاصة بك. قم بإضافة أذونات مجموعة NT الضرورية لصفحة الويب التي يصادق المستخدم عليها. بمجرد أن يقوم المستخدم بتسجيل الدخول إلى WebVPN باستخدام أذونات المجموعة، يتم منح حق الوصول إلى الصفحات المحددة أو رفضه وفقا لذلك. يعمل ASA فقط كمضيف مصادقة وكيل نيابة عن وحدة التحكم في المجال وجميع الاتحام بعد م
- لا يمكنك تكوين SSO ل SharePoint عبر WebVPN لأن خادم SharePoint لا يدعم المصادقة المستندة إلى النماذج. ونتيجة لذلك، فإن الإشارات المرجعية التي لها عملية مادة النشر أو إجراء إضافة مادة النشر غير قابلة للتطبيق هنا.

<u>معلومات ذات صلة</u>

- أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances
 - <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