ASA/PIX: ةكرحل دراولا NAT عم ديعب VPN مداخ نيوكت لاثمو CLI عم VPN ليمع رورم ASDM

المحتويات

<u>المقدمة</u> المتطلبات الأساسية المكونات المستخدمة المكونات المستخدمة معلومات أساسية معلومات أساسية تكوين حركة مرور عميل VPN بعيد باستخدام ASDM تكوين حركة مرور عميل VPN بعيد و ل ASA/PIX إلى NAT باستخدام ASDM شكلت ال ASA/PIX كنادل VPN بعيد و ل ASA/PIX إلى NAT باستخدام ASDM شكلت ال ASA/PIX كنادل VPN بعيد و ل ASA/N إلى NAT باستخدام شكلت ال ASA/PIX كنادل VPN بعيد و ل ASA/N المان مع ال التحقق من الصحة جهاز الأمان ASA/PIX - show commands استكشاف الأخطاء وإصلاحها معلومات ذات صلة

<u>المقدمة</u>

يصف هذا المستند كيفية تكوين جهاز الأمان القابل للتكيف (ASA) من السلسلة Cisco 5500 للعمل كخادم VPN بعيد باستخدام مدير أجهزة الأمان القابل للتكيف (ASDM) أو CLI (واجهة سطر الأوامر (CLI) وبطاقة واجهة الشبكة الخاصة (NAT) الواردة إلى حركة مرور عميل VPN. يوفر برنامج إدارة قاعدة بيانات المحول (ASDM) إدارة ومراقبة أمان على مستوى عالمي من خلال واجهة إدارة سهلة الاستخدام قائمة على الويب. بمجرد اكتمال تكوين Cisco ASA، يمكن التحقق منه من خلال عميل VPN.

<u>المتطلبات الأساسية</u>

<u>المتطلبات</u>

يفترض هذا المستند أن ASA قيد التشغيل الكامل وتم تكوينه للسماح ل Cisco ASDM أو CLI بإجراء تغييرات التكوين. كما يفترض أنه تم تكوين ASA ل NAT الصادر. أحلت <u>يسمح داخلي مضيف منفذ إلى شبكة خارجي مع</u> <u>الإستعمالمن ضرب</u> ل كثير معلومة على كيف أن يشكل NAT صادر.

ملاحظة: ارجع إلى <u>السماح بوصول HTTPS ل ASDM</u> أو <u>PIX/ASA 7.x: SSH على مثال تكوين الواجهة الداخلية</u> <u>والخارجية</u> للسماح بتكوين الجهاز عن بعد بواسطة ASDM أو Secure Shell (SSH).

<u>المكونات المستخدمة</u>

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

- برنامج جهاز الأمان القابل للتكيف الإصدار x.7 من Cisco والإصدارات الأحدث
 - Adaptive Security Device Manager الإصدار x.5 والإصدارات الأحدث
 - Cisco VPN Client الإصدار x.4 والإصدارات الأحدث

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>المنتجات ذات الصلة</u>

كما يمكن إستخدام هذا التكوين مع جهاز الأمان Cisco PIX الإصدار x.7 والإصدارات الأحدث.

<u>الاصطلاحات</u>

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

<u>معلومات أساسية</u>

توفر تكوينات الوصول عن بعد الوصول الآمن عن بعد لعملاء Cisco VPN، مثل المستخدمين كثيري التنقل. تتيح الشبكة الخاصة الظاهرية (VPN) للوصول عن بعد للمستخدمين البعيدين إمكانية الوصول الآمن إلى موارد الشبكة المركزية. يتوافق عميل شبكة VPN من Cisco مع بروتوكول IPSec وتم تصميمه خصيصا للعمل مع جهاز الأمان. ومع ذلك، يمكن أن يقوم جهاز الأمان بإنشاء إتصالات IPSec مع العديد من العملاء المتوافقين مع البروتوكول. ارجع إلى <u>أدلة تكوين ASA</u> للحصول على مزيد من المعلومات حول IPSec.

المجموعات والمستخدمين هم المفاهيم الأساسية في إدارة أمان الشبكات الخاصة الظاهرية (VPN) وفي تكوين جهاز الأمان. هم يعين شعار أن يحدد مستعمل منفذ إلى واستخدام ال VPN. المجموعة هي مجموعة من المستخدمين الذين يتم التعامل معهم ككيان واحد. يحصل المستخدمون على خصائصهم من نهج المجموعة. تحدد مجموعات النفق نهج المجموعة للاتصالات المحددة. في حالة عدم تعيين نهج مجموعة معين للمستخدمين، يتم تطبيق نهج المجموعة الافتراضي للاتصال.

تتكون مجموعة النفق من مجموعة سجلات تحدد نهج اتصال النفق. تحدد هذه السجلات الخوادم التي تتم مصادقة مستخدمي النفق عليها، بالإضافة إلى خوادم المحاسبة، إن وجدت، التي يتم إرسال معلومات الاتصال إليها. كما أنها تحدد نهج مجموعة افتراضي للاتصالات، وهي تحتوي على معلمات اتصال خاصة بالبروتوكول. تتضمن مجموعات الأنفاق عددا صغيرا من السمات المتعلقة بإنشاء النفق نفسه. تتضمن مجموعات النفق مؤشر لنهج المجموعة الذي يعرف السمات الموجهة للمستخدم.

<u>التكوينات</u>

تكوين ASA/PIX كخادم VPN بعيد باستخدام ASDM

أتمت هذا steps in order to شكلت ال cisco ASA كنادل VPN بعيد مع ASDM:

1. افتح المستعرض وأدخل https://**<IP_Address الخاص بواجهة ASA التي تم تكوينها للوصول إلى ASDM**كللوصول إلى ASDM>للوصول إلى ASDN على ASA.تأكد من تخويل أية تحذيرات يعطيك المستعرض لها صلة بأصالة شهادة SSL. التقصير username وكلمة على حد سواء فارغ.يقدم ASA هذا الإطار للسماح بتنزيل تطبيق ASDM. يقوم هذا المثال بتحميل التطبيق على الكمبيوتر المحلي ولا يعمل في تطبيق Java.





Cisco ASDM 6.1(3) provides an intuitive graphical user interface that makes it easy to set up, configure and manage your Cisco Security Appliances.

Cisco ASDM runs as either a local application or Java Web Start.

 Running Cisco ASDM as a local Application

 When you run Cisco ASDM as a local application, it connects to your Security Appliance from your desktop via SSL. Running Cisco ASDM as an application has these advantages:

 • You can invoke ASDM from desktop shortcuts. No browser is required.

 • One desktop shortcut allows you to connect to multiple Security Appliances.

 Install ASDM Launcher and Run ASDM

 Running Cisco ASDM as Java Web Start

 You can run Cisco ASDM as Java Web Start that is dynamically downloaded from the device to which you connect.

 • Click Run ASDM to run Cisco ASDM.

 • Click Run Startup Wizard to run Startup Wizard.Startup Wizard walks you through, step by step, the initial configuration of your security appliance.

 Run ASDM
 Run Startup Wizard

- 2. انقر على **تنزيل مشغل ASDM وابدأ ASDM** لتنزيل المثبت الخاص بتطبيق ASDM.
- 3. بمجرد تنزيل مشغل ASDM، قم بإكمال الخطوات التي توجهها المطالبات لتثبيت البرنامج وتشغيل مشغل من Cisco.
- 4. دخلت العنوان للقارن أنت تشكل مع **ال http -** أمر، واسم مستخدم وكلمة إن يعين أنت واحد.يستخدم هذا المثال **Cisco123** كاسم مستخدم و**Cisco123** ككلمة

🕵 Cisco ASDM Launch	er v1.5(30)		
	SDM Launcher	cisco	
Device IP Address / Name:	10.77.241.111	•	
Username:	cisco123		
Password:	* * * * * * *		
🔲 Run in Demo Mode			
		i i 🗳 🔂	م
	IPse من الإطار	دد المعالجات > معالج C VPN	, 5. ح
🛸 Cisco ASDM 6.1	for ASA - 10.77.241.111		
File View Tools V	Wizards Window Help		
Home 3 Cor	Startup Wizard		
Device List	IPsec VPN Wizard		
	SSL VPN Wizard		
	High Availability and Scalab	ility Wizard	
10.77.241.10	Packet Capture Wizard	رئيسي.	الر

6. حدد نوّع نفق VPN **للوصول عن بعد** وتأكد من تعيين واجهة نفق VPN على النحو المطلوب، وانقر فوق **التالي** كما هو موضح هنا.

🖆 VPN Wizard	
VPN Wizard	VPN Tunnel Type (Step 1 of)
Branch Branch ISP Home	Use this wizard to configure new site-to-site VPN tunnels or new remote access VPN tunnels. A tunnel between two devices is called a site-to-site tunnel and is bidirectional. A tunnel established by calls from remote users such as telecommuters is called remote access tunnel. This wizard creates basic tunnel configurations that you can edit later using the ASDM.
Corporate Network	VPN Tunnel Type: Site-to-Site VPN
	⊖ Site-to-Site
	Remote Access
	VPN Tunnel Interface: Outside Image: Enable inbound IPsec sessions to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic.
	< Back Next > Finish Cancel Help

7. يتم إختيار نوع عميل شبكة VPN، كما هو موضح. يتم إختيار **عميل شبكة VPN من Cisco** هنا. انقر فوق **Next** (التالي).

🖆 VPN Wizard	
VPN Wizard	Remote Access Client (Step 2 of)
Brandh	Remote access users of various types can open VPN tunnels to this ASA. Select the type of VPN client for this tunnel.
	VPN Client Type:
Corporate Notwork	⊙ Cisco VPN Client, Release 3.x or higher,
North	or other Easy VPN Remote product
The Ital	Microsoft Windows client using L2TP over IPsec
	Specify the PPP authentication protocol. If a protocol is not specified on the remote client, do not specify it.
- THUM	PAP V CHAP V MS-CHAP-V1 MS-CHAP-V2 EAP-PROXY
	Specify if the client will send tunnel group name as - username@tunnelgroup.
	Client will send tunnel group name as username@tunnelgroup.
	If pre-shared authentication is used with this option then DefaultRAGroup's pre-shared key and ppp authentication are also modified.
	< Back Next > Finish Cancel Help

8. أدخل اسما **لاسم مجموعة النفق**. أدخل معلومات المصادقة التي سيتم إستخدامها، وهي **المفتاح المشترك مسبقا** في هذا المثال. المفتاح المشترك مسبقا المستخدم في هذا المثال هو Cisco123. اسم مجموعة النفق المستخدم في هذا المثال هو Cisco. انقر فوق Next

-					
	.((.	٦	لتا	I

🖆 VPN Wizard	
VPN Wizard	VPN Client Authentication Method and Tunnel Group Name (Step 3 of)
Branch Branch Honse Norworks	The ASA allows you to group remote access tunnel users based on common connection parameters and clent attributes configured in the subsequent screens. Configure authentication method and tunnel group for this remote connection. Use the same tunnel group name for the device and the remote clent. Authentication Method Pre-shared key clscol23 Certificate Certificate Signing Algorithm: rsa-sig Certificate Name: Challenge/response authentication (CRACK) Tunnel Group Name:
	< Back Next > Finish Cancel Help

9. أختر ما إذا كنت تريد مصادقة المستخدمين عن بعد إلى قاعدة بيانات المستخدم المحلية أو إلى مجموعة خوادم AAA خارجية.**ملاحظة:** يمكنك إضافة مستخدمين إلى قاعدة بيانات المستخدم المحلية في الخطوة 10.**ملاحظة:** ارجع إلى <u>مجموعات خوادم المصادقة والتفويض الخاصة ب PIX/ASA 7.x لمستخدمي VPN عبر مثال تكوين</u> <u>ASDM</u> للحصول على معلومات حول كيفية تكوين مجموعة خوادم AAA الخارجية مع ASDM.

VPN Wizard Client Authentication (Step 4 of) Image: Client Authenticate remote users using local device user database, select the first option below. You can create user accounts in the next step. Image: Client Authenticate remote users using local device user database, select the first option below. You can create a new one using the New button below. Image: Client Authenticate remote users using local device user database, select the first option below. Image: Client Authenticate remote users accounts in the next step. Image: Client Authenticate remote users accounts in the next step. Image: Client Authenticate user accounts in the next step. Image: Client Authenticate user accounts in the next step. Image: Client Authenticate user anew one using the New button below. Image: Client Authenticate using an AAA settings, go to Configuration > Device Management > Users/AAA in the main ASDM window. Image: Authenticate using the local user database: Image: Authenticate using an AAA server group AAA Server Group Name: Image: New Image: New New	🖆 VPN Wizard		×
 Constructions Constructions	VPN Wizard	Client Authentication (Step 4 of)	
	Branch Branch Branch Home Corporate Network	To authenticate remote users using local device user database, select the first option below. You can create user accounts in the next step. To use external AAA servers instead, select the second option. You can select an existing AAA server group or create a new one using the New button below. To manage all other AAA settings, go to Configuration > Device Management > Users/AAA in the main ASDM window.	
SBack Next > Finish Cancel Help		Sack Next > Finish Cancel Hel	

10. توفر **اسم مستخدم** و**كلمة مرور** إختيارية وانقر فوق **إضافة** لإضافة مستخدمين جدد إلى قاعدة بيانات مصادقة المستخدم. انقر فوق Next (**التالي).ملاحظة:** لا تقم بإزالة المستخدمين الحاليين من هذا الإطار. حدد **تكوين >** إدارة الأجهزة > Users/AAA > حسابات المستخدمين في نافذة ASDM الرئيسية لتحرير الإدخالات الموجودة في قاعدة البيانات أو إزالتها من قاعدة البيانات.

🖆 VPN Wizard		\times
VPN Wizard	User Accounts (Step 5 of 11)	
Brands Brand Brand Brands Brand Brands Brands Brand	Add new users into the user authentication database. To edit existing entries in the database or to remove them from the database, go to Configuration > Device Management > Users/AAA > User Accounts in the main ASDM window.	
Home	User to Be Added	
Corporate Network	Username: dsco123	
The states and the	cisco Add >>	
	Password (optional): Delete	
-T-HIIIII		
THIT	Confirm Password (optional):	
	< Back Next > Finish Cancel Help	

11. طقطقت in order to عينت بركة من محلي أن يكون عينت ديناميكيا إلى VPN زبون بعيد، **جديد** أن يخلق جديد IP ب**ركة**.

🖆 VPN Wizard	
VPN Wizard	Address Pool (Step 6 of 11)
Branch Branch ISP Horne	Enter a pool of local addresses to be used for assigning dynamic IP addresses to remote VPN clients.
Corporate	Tunnel Group Name : Cisco
THE THE	Pool Name:
	Pool Settings
Terthelin	Range Start Address:
TTT	Range End Address:
	Subnet Mask:
	< Back Next > Finish Cancel Help

12. في الإطار الجديد بعنوان **إضافة تجمع I**P وفر هذه المعلومات، وانقر **موافق.اسم تجمع Pاعنوان IP** الأولينهاية عنوان Pاقناع الشبكة

1	dd IP Pool		
Ι.			_
	Name:	vpnpool	
	Starting IP Address:	192.168.1.1	
	Ending IP Address:	192.168.1.254	
	Subnet Mask:	255.255.255.0]
	OK R	ancel Help	اخ مة

13. بعد تحديد تجمع العناوين المحلية التي سيتم تعيينها ديناميكيا لعملاء VPN البعيدة عند إتصالهم، انقر فوق **التالي.**

🖆 VPN Wizard		×
VPN Wizard	Address Pool (Step 6 of 11)	
Branch Branch Fisp Home	Enter a pool of local addresses to be used for assigning dynamic IP addresses to remote VPN clients.	
Corporate Natwork	Tunnel Group Name : cisco	
THE IN	Pool Name: vpnpool V New	
	Pool Settings	
THUIL	Range Start Address: 192.168.1.1	
- Carlotte	Range End Address: 192.168.1.254	
THE REAL	Subnet Mask: 255.255.255.0	
	< Back Next > Finish Cancel Help)

14. *إختياري:* حدد معلومات خادم DNS و WINS واسم مجال افتراضي ليتم دفعه إلى عملاء VPN البعيدة.

		البعيدة.
🖆 VPN Wizard		\mathbf{X}
VPN Wizard	Attributes Pushed to Client (Optional)	(Step 7 of 11)
Brands Br	Attributes you configure below are push ASA. If you do not want an attribute pu	ed to the VPN client when the client connects to the shed to the client, leave the corresponding field blank.
Corporate	Tunnel Group:	cisco
Notwo ka	Primary DNS Server:	I
	Secondary DNS Server:	
	Primary WINS Server:	
THE	Secondary WINS Server:	
	Default Domain Name:	
		< Back Next > Finish Cancel Help

15. حدد معلمات IKE، المعروفة أيضا بالمرحلة 1 من IKE.يجب أن تتطابق التكوينات الموجودة على كلا جانبي النفق تماما. ومع ذلك، يحدد عميل شبكة VPN من Cisco التكوين المناسب تلقائيا لنفسه. لذلك، لا يلزم تكوين IKE على جهاز الكمبيوتر السيا

	میل.	الع
🖆 VPN Wizard		×
VPN Wizard	IKE Policy (Step 8 of 11)	
Branch Branch F ISP Home Home	Select the encryption algorithm, authentication algorithm, and Diffie-Hellman group for the devices to use to negotiate an Internet Key Exchange (IKE) security association between them. Configurations on both sides of the connection must match exactly.	
Contwork Natwork	Encryption: DES	
	Authentication: MDS	
1911	Diffie-Helman Group: 2	
	< Back Next Finish Cancel Help]

16. تعرض هذه النافذة ملخصا للإجراءات التي اتخذتها. انقر فوق **إنهاء** إذا كنت راضيا عن التكوين الخاص بك.



<u>تكوين حركة مرور عميل VPN الواردة ل ASA/PIX إلى NAT باستخدام ASDM</u>

أتمت هذا steps in order to شكلت ال cisco ASA أن nat داخل VPN زبون حركة مرور مع ASDM:

1. أخترت **تشكيل>جدار حماية>nat قاعدة**، وطقطقة **يضيف**. في القائمة المنسدلة، حدد **إضافة قاعدة NAT**. Configuration > Firewall > NAT Rules



2. في نافذة **قاعدة إضافة شبكة (NAT) الديناميكية**، أختر **خارجي** كواجهة، وانقر زر الاستعراض الموجود بجوار المربع **المصدر**.

🖆 Add Dyn	amic NAT Rule		
Original	Outside	tion.	
Pool ID 0	Interface (outbound) (inbound)	Addresses Pool Same as original address (identity) Same as original address (identity)	Manage
Connectio	n Settings	OK Cancel Help	*

3. في نافذة تصفح المصدر، حدد كائنات الشبكة المناسبة واختر أيضا **المصدر** تحت قسم المصدر المحدد، وانقر **موافق**. هنا يتم إختيار كائن الشبكة 192.168.1.0.

📥 add. 📨 Ed	it 🗊 Delet							
iter:		e 9					F	ilter Clear
Name	÷1	IP Addres	55	Netmask		Description		
Network Obie	ects					Description.		_
any	1	0.0.0.0		0.0.0.0				
🕞 📠 inside	-network	172.16.1.0	D	255.255.255	0			- 1
- 🙀 Outsid	de-network	10.10.10.0	D	255.255.255	0			
192.1	68.1.0	192.168.1	.0	255.255.255.	0	1		
elected Source								
elected Source	192.168	3.1.0/24						

إدارة.

C	Add Dyna	amic NAT Rule		
O. Tr	riginal — Interface: Source: anslated — Select a glo	Outside 192.168.0.0 Ibal pool for dynamic tr	anslation.	
	Pool ID	Interface	Addresses Pool	
	0	(outbound)	Same as original address (identity)	
	0	(inbound)	Same as original address (identity)	Manage
	Connectio	n Settings		*
			OK Cancel Help	

5. في نافذة "إدارة التجمع العام"، انقر فوق

🛓 Manage Glo	obal Pool		
😫 Add 🗹 E	dit 🍿 Delete		
Pool ID	Interface	Addresses Pool	
	ОК	Cancel Help	

6. في نافذة "إضافة تجمع عناوين عمومي"، أختر Inside كواجهة و2 كمعرف **التجمع**. تأكدت أيضا أن **انتقيت** زر لاسلكي بجوار **ضرب يستعمل عنوان من القارن**. طقطقة **يضيف>**، وبعد ذلك يطقطق ok.

🖆 Add Global Address Pool	
Interface: inside Pool ID: 2	
IP Addresses to Add Range Starting IP Address: Ending IP Address: Netmask (optional): IP Address Translation (PAT) IP Address: Netmask (optional): Det Address Translation (PAT)	Addresses Pool Add >> Add >>
Address of the interface	Cancel Help

7. انقر فوق **موافق** بعد تحديد التجمع العام باستخدام **معرف التجمع 2** الذي تم تكوينه في الخطوة السابقة.

🕵 Add Dyna	amic NAT Rule		×
Original			
Interface:	Outside	~	
Source:	192.168.1.0/24		
Translated			
Select a glo	bal pool for dynamic transla	tion.	
Pool ID	Interface	Addresses Pool	
0	(outbound)	Same as original address (identity)	
0	(inbound)	Same as original address (identity)	n I
-	i i ide		
Connection	n Settings	(6	8
	[OKN Cancel Help	
	Ľ		

8. انقر الآن فوق **تطبيق** حتى يتم تطبيق التكوين على ASA.يؤدي هذا إلى اكتمال التكوين.

Configura	onfiguration > Firewall > NAT Rules						
💠 Add	🝷 📑 Edit 🏦 Dele	te 🛧 🗲 🕉 ங	💼 - 🛛 🔍 Find 🗄	🔁 Diagram 🗐	Packet Trace		
	Turne	Original			Translated		
*	туре	Source	Destination	Service	Interface	Addre:	
🔳 Outsid	le (1 Dynamic rules)						
1	Dynamic	192.168.1.0/24			inside	🛲 insid	
inside	(1 Exempt rules, 1 Dy	/namic rules)					
1	= Exempt	🇳 any	192.168.1.0/24		(outbound)		
2	📊 Dynamic	🏈 any			Outside	🔤 Out	
<						>	
Eacht	a traffic through the l	Frowall without address h	randation				
C C I I ADM	e trainc through the l	ni ewait without audress ti	ansiduuti				
		Apply	Reset				

<u>شكلت ال ASA/PIX كنادل VPN بعيد و ل inbound NAT مع ال CLI</u>



nameif inside security-level 100 ip address 172.16.1.2 255.255.255.0 ! I. passwd 2KFQnbNIdI.2KYOU encrypted boot system disk0:/asa803-k8.bin ftp mode passive access-list inside_nat0_outbound extended permit ip any 192.168.1.0 255.255.255 0 pager lines 24 logging enable mtu Outside 1500 mtu inside 1500 ip local pool vpnpool 192.168.1.1-192.168.1.254 mask 255.255.255.0 no failover icmp unreachable rate-limit 1 burst-size 1 asdm image disk0:/asdm-615.bin asdm history enable arp timeout 14400 nat-control global (Outside) 1 interface global (inside) 2 interface nat (Outside) 2 192.168.1.0 255.255.255.0 outside nat (inside) 0 access-list inside_nat0_outbound nat (inside) 1 0.0.0.0 0.0.0.0 route Outside 0.0.0.0 0.0.0.0 10.10.10.3 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 no snmp-server location no snmp-server contact Configuration for IPsec policies. !--- Enables the ---! crypto transform configuration mode, !--- where you can specify the transform sets that are used !--- during an IPsec negotiation. crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5hmac crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set pfs group1 crypto dynamic-map SYSTEM DEFAULT CRYPTO MAP 65535 set transform-set ESP-DES-SH ESP-DES-MD5 crypto map Outside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP crypto map Outside_map interface Outside crypto isakmp enable Outside Configuration for IKE policies. !--- Enables the ---! IKE policy configuration (config-isakmp) !--- command mode, where you can specify the parameters that !--- are used during an IKE negotiation. Encryption and !---

Policy details are hidden as the default values are

chosen. crypto isakmp policy 10 authentication pre-share encryption des hash sha group 2 lifetime 86400 crypto isakmp policy 30 authentication pre-share encryption des hash md5 group 2 lifetime 86400 telnet timeout 5 ssh timeout 60 console timeout 0 management-access inside threat-detection basic-threat threat-detection statistics access-list group-policy cisco internal group-policy cisco attributes vpn-tunnel-protocol IPSec Specifies the username and password with their !--- ---! respective privilege levels username cisco123 password ffIRPGpDSOJh9YLq encrypted privilege 15 username cisco password ffIRPGpDSOJh9YLq encrypted privilege 0 username cisco attributes vpn-group-policy cisco tunnel-group cisco type remote-access tunnel-group cisco general-attributes address-pool vpnpool default-group-policy cisco Specifies the pre-shared key "cisco123" which must ---! !--- be identical at both peers. This is a global !--configuration mode command. tunnel-group cisco ipsecattributes * pre-shared-key 1 class-map inspection_default match default-inspection-traffic ! ! policy-map type inspect dns migrated_dns_map_1 parameters message-length maximum 512 policy-map global_policy class inspection_default inspect dns migrated_dns_map_1 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 prompt hostname context Cryptochecksum:f2ad6f9d5bf23810a26f5cb464e1fdf3 end : #ciscoasa

<u>التحقق من الصحة</u>

حاول الاتصال ب Cisco ASA من خلال عميل Cisco VPN للتحقق من تكوين ASA بنجاح.

1. طقطقت

!

			جديد.
VPN Client - Version 5.0.03.0530			
Connection Entries Status Certificates Log Options	s Help		
Connect News Import Modify	Delete		diadia cisco
Connection Entry	Host	Transport	
Not connected.			

2. املأ تفاصيل إتصالك الجديد.يجب أن يحتوي حقل المضيف على عنوان IP أو اسم المضيف الخاص ب Cisco ASA الذي تم تكوينه مسبقا. يجب أن تتوافق معلومات مصادقة المجموعة مع تلك المستخدمة في **الخطوة 4**. انقر فوق **حفظ** عند

🤌 VPN Client 🕴 🤇	Create New VPN Conne	ction Entry	
Connection Entry: MyV	/PNClient		
Description:			
Host: 10.1	0.10.2		cisco
Authentication Tr	ansport Backup Servers	Dial-Up	
Group Authentica	tion	O Mutual Group	Authentication
Name:	cisco		
Password:	*****		
Confirm Password:	******		
C Certificate Auther	ntication		
🗖 Send CA Certif	icate Chain		
		-	
Erase User Password]	Save 💦	Cancel

3. حدد[ّ] الاتصال الذي تم إنشاؤه حديثا، وانقر فوق **توصيل**.

Status: Disconnected VPN Client - Version	ion 5.0.03.0530		
Connection Entries Status Certificates Log Option	is Help		
Confect New Import Modify Connection Entries Certificates Log) Delete		cisco
Connection Entry	Host	Transport	
MyVPNClient	10.10.10.2	IPSec/UDP	
Not connected.			

4. أدخل اسم مستخدم وكلمة مرور للمصادقة الموسعة. يجب أن تطابق هذه المعلومات المعلومات المعلومات المحددة في **الخطوتين 5 و**

🤌 VPN Client User Authen	tication for "MyVPNC	lient" 🛛 🔀
The server has requested the followin authentication.	ng information to complete t	ne user
CISCO Password: *******		
	ОК	Cancel

5. بمجرد تأسيس الاتصال بنجاح، أختر **إحصائيات** من قائمة الحالة للتحقق من تفاصيل النفق.

🥔 status: Connected V	PN Client - Version	5.0.03.0530		
Connection Entries Status O	ertificates Log Options	s Help		
Statis	tics Ctrl+S			
Connection Entries Reset	t Stats	Delete		
Connection Entry	\triangle	Host	Transport	
MyVPNClient		10.10.10.2	IPSec/UDP	
Connected to "MyVPNClient".			Connected Time: 0 day(s), 00:00.36	▼ //
			لذة حركة مرور و تشفير	یدی هذا ناد

Tunnel Details	Firewall		
Address Information	Connection Information		
Client: 192.168.1.1	Entry:	MyVPNClient	
Server: 10.10.10.2	Time:	0 day(s), 00:01.13	
Bytes	Crypto		
Received: 5412	Encryption:	56-bit DES	
Sent: 5416	Authentication:	HMAC-MD5	
Packets	Transport		
Encrypted: 39	Transparent Tunneling:Inactive		
Decrypted:31	Local LAN:	Disabled	
Discarded: 8	Compression:	None	
Bypassed: 22			
		Beset	
		11636(
		~	
		Close	



VPN Client	Statistics			×
Tunnel Details	Route Details Firev	vall		
Local LAN Routes		Secured Routes		
Network	Subnet Mask	Network	Subnet Mask	
		0.0.0.0	0.0.0.0	
1		1		
			Close	1

<u>جهاز الأمان ASA/PIX - show commands</u>

• show crypto isakmp sa— يعرض جميع شبكات IKE الحالية في نظير. ASA#show crypto isakmp sa Active SA: 1 (Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey Total IKE SA: 1 IKE Peer: 10.10.10.1 1 Type : user Role : responder Rekey : no State : AM_ACTIVE show crypto ipSec sa— يعرض جميع معرفات فئات خدمة IPsec الحالية في نظير. ASA#show crypto ipsec sa interface: Outside Crypto map tag: SYSTEM_DEFAULT_CRYPTO_MAP, seq num: 65535, local addr: 10.10 10.2. (local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0 (remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0 current_peer: 10.10.10.1, username: cisco123 dynamic allocated peer ip: 192.168.1.1 pkts encaps: 20, #pkts encrypt: 20, #pkts digest: 20# pkts decaps: 74, #pkts decrypt: 74, #pkts verify: 74# pkts compressed: 0, #pkts decompressed: 0# pkts not compressed: 20, #pkts comp failed: 0, #pkts decomp failed: 0# pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0# PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0# send errors: 0, #recv errors: 0#

local crypto endpt.: 10.10.10.2, remote crypto endpt.: 10.10.10.1

```
path mtu 1500, ipsec overhead 58, media mtu 1500
                                               current outbound spi: F49F954C
                                                               :inbound esp sas
                                                 (spi: 0x3C10F9DD (1007745501
                                      transform: esp-des esp-md5-hmac none
                                           { ,in use settings ={RA, Tunnel
            slot: 0, conn id: 24576, crypto-map: SYSTEM DEFAULT CRYPTO MAP
                            sa timing: remaining key lifetime (sec): 27255
                                                          IV size: 8 bytes
                                               replay detection support: Y
                                                              :outbound esp sas
                                                 (spi: 0xF49F954C (4104099148
                                      transform: esp-des esp-md5-hmac none
                                           { ,in use settings ={RA, Tunnel
            slot: 0, conn_id: 24576, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP
                            sa timing: remaining key lifetime (sec): 27255
                                                          IV size: 8 bytes
                                               replay detection support: Y
                                                  ciscoasa(config)#debug icmp trace
Inbound Nat Translation is shown below for Outside to Inside ICMP echo request ---!
                         translating Outside:192.168.1.1/768 to inside:172.16.1.2/1
   ICMP echo reply from inside:172.16.1.3 to Outside:172.16.1.2 ID=1 seq=7936 len=3
                                                                                   2
  Inbound Nat Translation is shown below for Inside to Outside ICMP echo reply ---!
                       untranslating inside:172.16.1.2/1 to Outside:192.168.1.1/768
   ICMP echo request from Outside:192.168.1.1 to inside:172.16.1.3 ID=768 seq=8192
                                                                              len=32
       ICMP echo request translating Outside:192.168.1.1/768 to inside:172.16.1.2/1
  ICMP echo reply from inside:172.16.1.3 to Outside:172.16.1.2 ID=1 seq=8192 len=3
                                                                                   2
       ICMP echo reply untranslating inside:172.16.1.2/1 to Outside:192.168.1.1/768
            ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8448 len=32
             ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8448 len=32
            ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8704 len=32
              ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8704 len=32
            ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8960 len=32
              ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8960 len=32
```

<u>استكشاف الأخطاء وإصلاحها</u>

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

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

ارجع إلى <u>حلول أستكشاف أخطاء IPSec VPN وإصلاحها للمستوى2L والوصول عن بعد</u> للحصول على مزيد من المعلومات حول كيفية أستكشاف أخطاء شبكة VPN الخاصة بالموقع وإصلاحها.

<u>معلومات ذات صلة</u>

- أجهزة الأمان المعدلة <u>Cisco ASA 5500 Series Adaptive Security Appliances</u>
 - مدير أجهزة حلول الأمان المعدلة من <u>Cisco</u>
- <u>أستكشاف أخطاء أجهزة الأمان المعدلة وإصلاحها وتنبيهات سلسلة Cisco ASA 5500</u>
 - الدعم التقني والمستندات Cisco Systems

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