# نيب عقوم ىلإ عقوم نم VPN ةكبش :SDM IOS ەجوم نيوكت لاتمو ASA/PIX

# المحتويات

<u>المقدمة</u> المتطلبا<u>ت الأساسية</u> المتطلبات المكونات المستخدمة <u>المنتجات ذات الصلة</u> الاصطلاحات التكوين <u>الرسم التخطيطي للشب</u>كة تكوين ASDM لنفق VPN <u>تكوين SDM للموجه</u> تكوين ASA CLI تكوين CLI للموجه التحقق من الصحة جهاز الأمان ASA/PIX - show commands <u>موجه IOS البعيد - إظهار الأوامر</u> استكشاف الأخطاء وإصلاحها معلومات ذات صلة

# <u>المقدمة</u>

يزود هذا وثيقة عينة تشكيل ل ال LAN إلى LAN (موقع إلى موقع) IPsec نفق بين cisco أمن أجهزة (ASA/PIX) و cisco ios مسحاج تخديد. يتم استخدام المسارات الثابتة للتبسيط.

ارجع إلى <u>جهاز الأمان PIX/ASA 7.x إلى مثال تكوين نفق IPsec لموجه IOS إلى شبكة LAN</u> من أجل معرفة المزيد حول نفس السيناريو حيث يقوم جهاز أمان PIX/ASA بتشغيل الإصدار Software *7.x*.

# <u>المتطلبات الأساسية</u>

#### <u>المتطلبات</u>

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

- يجب إنشاء اتصال IP الشامل قبل بدء هذا التكوين.
- يجب تمكين ترخيص جهاز الأمان لتشفير معيار تشفير البيانات (DES) (على أدنى مستوى تشفير).

#### <u>المكونات المستخدمة</u>

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

- أجهزة الأمان المعدلة x.8 والإصدارات الأحدث (Cisco Adaptive Security Appliance (ASA) مع الإصدار x.8
  - ASDM الإصدار x.6.والإصدارات الأحدث
  - cisco 1812 مسحاج تخديد مع cisco ios المرمجية إطلاق 12.3
    - Cisco Security Device Manager (SDM)، الإصدار 2.5)، الإصدار

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

**ملاحظة:** ارجع إلى <u>تكوين الموجه الأساسي باستخدام SDM</u> للسماح بتكوين الموجه بواسطة SDM.

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.

**ملاحظة:** ارجع إلى <u>محترف التكوين: الشبكة الخاصة الظاهرية (VPN) لبروتوكول IPsec من موقع إلى موقع بين</u> ASA/PIX ومثا<u>ل تكوين موجه IOS</u> لتكوين مماثل باستخدام محترف تكوين Cisco على الموجه.

#### <u>المنتجات ذات الصلة</u>

كما يمكن إستخدام هذا التكوين مع جهاز الأمان Cisco PIX 500 Series Security Appliance، والذي يشغل الإصدار x.7 والإصدارات الأحدث.

#### <u>الاصطلاحات</u>

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

# <u>التكوين</u>

#### الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة الموضح في هذا الرسم التخطيطي.



**ملاحظة:** ال ip ليس يخاطب خطة يستعمل في هذا تشكيل قانونيا routable على الإنترنت. هم <u>rfc 1918</u> عنوان، أي يتلقى يكون استعملت في مختبر بيئة.

- <u>تكوين ASDM لنفق VPN</u>
  - <u>تكوين SDM للموجه</u>
    - <u>تكوين ASA CLI</u>
    - <u>تكوين CLI للموجه</u>

#### تكوين ASDM لنفق VPN

أتمت هذا steps in order to خلقت ال VPN نفق:

1. افتح المستعرض الخاص بك وأدخل https://<IP\_Address الخاص بواجهة ASA التي تم تكوينها للوصول إلى ASDM Access>للوصول إلى ASDM 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.



- 3. بمجرد تنزيل مشغل ASDM، قم بإكمال الخطوات التي توجهها المطالبات لتثبيت البرنامج وتشغيل مشغل ASDM من Cisco.
- 4. دخلت العنوان للقارن أنت تشكل مع **ال http -** أمر، واسم مستخدم وكلمة إن يعين أنت واحد.يستعمل هذا مثال و username و **Cisco123**

| 🚰 Cisco ASDM Launc        |               |          |
|---------------------------|---------------|----------|
| 🤏 Cisco A                 | cisco         |          |
|                           |               |          |
| Device IP Address / Name: | 10.77.241.111 | <b>*</b> |
| Username:                 | cisco123      |          |
| Password:                 | *****         |          |
| 🔄 Run in Demo Mode        |               |          |
|                           | OK Close      |          |
|                           | .0            | 💼 🖆 🖆 🔒  |

5. قم بتشغيل **معالج IPsec VPN** بمجرد اتصال تطبيق ASDM ب ASA.

| 🖆 Cisco ASDM 6.1   | l for ASA - 10.77.241.111   |  |   |
|--|---|--|---|
| File View Tools  | Wizards Window Help Lo<br>Startup Wizard  | ook For:   | ahaha   |
| Home<br>Device Dast  | IPsec VPN Wizard<br>SSL VPN Wizard<br>High Availability and Scalability Wizard<br>Packet Capture Wizard   | ntion  |   |
| General License<br>Host Name:<br>ASA Version:<br>ASDM Version:<br>Firewall Mode:<br>Total Flash: | ciscoasa.default.domain.invalid<br>8.0(2) Device Uptime: 14d 3h 1m 51s<br>6.1(3) Device Type: ASA 5510<br>Routed Context Mode: Single<br>64 MB Total Memory: 256 MB | Interface IP Address/Mask<br>dm2 10.77.241.111/26<br>inside 10.10.10.1/24<br>outside 172.16.1.1/24<br>Select an interface to view input and output | Line Li<br>O up O<br>O up O<br>O up O<br>Kbps |
| VPN Tunnels<br>IKE: 0 IPSec: 0<br>System Resource<br>CPU CPU L<br>100<br>0% 50                   | Clientless SSL VPN: 0 SSL VPN Client: 0 Details<br>Ces Status<br>Jsage (percent)  | Connections Per Second Usage   | 20:44   |
|  | cisco123  | 15 🔐 🔂 🔒 4   | /6/09 8:45:42 PM UTC                          |

6. أخترت **الموقع إلى موقع** IPsec VPN نفق نوع وطقطقة **بعد ذلك** كما هو موضح هنا.

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

7. حدد عنوان IP الخارجي للنظير البعيد. أدخل معلومات المصادقة المراد إستخدامها، وهو المفتاح المشترك مسبقا في هذا المثال. المفتاح المشترك مسبقا المستخدم في هذا المثال هو Cisco123. النفق مجموعة إسم</mark> يكون ك خارجي عنوان افتراضيا إن يشكل أنت I2L VPN. انقر فوق Next (التالي).

| 🖆 VPN Wizard |   | × |
|--------------|---|---|
| VPN Wizard   | Remote Site Peer (Step 2 of 6)  |   |
| Branch       | Configure the IP address of the peer device, authentication method and the tunnel group for this site-to-site tunnel.   |   |
|              | Authentication Method   |   |
| Home         | Pre-shared key  |   |
| Corporate    | Pre-Shared Key: cisco123  |   |
| - Ar         | ◯ Certificate   |   |
| The The      | Certificate Signing Algorithm: rsa-sig  |   |
|              | Certificate Name:   |   |
| CTUTUTUT     | Challenge/response authentication (CRACK)   |   |
| THIT         | -Tunnel Group-  |   |
| B            | For site-to-site connections with pre-shared key authentication, the tunnel group name must<br>be the same as either the peer IP address or the peer hostname, whichever is used as the<br>peer's identity. |   |
|              | Tunnel Group Name: 172.17.1.1   |   |
|              |   |   |
|              | < Back Next > Finish Cancel Help  |   |

8. حدد السمات التي سيتم إستخدامها ل IKE، والمعروفة أيضا بالطور 1. يجب أن تكون هذه السمات هي نفسها على كل من ASA وموجه IOS. انقر فوق **Next** (التالي).

| 🖆 VPN Wizard                                      |  | × |
|---|--|---|
| VPN Wizard  | IKE Policy (Step 3 of 6)   |   |
| Branch<br>Branch<br>ISP<br>Corporate<br>Corporate | Select the encryption algorithm, authentication algorithm, and Diffie-Hellman group for the<br>devices to use to negotiate an Internet Key Exchange (IKE) security association between<br>them. Configurations on both sides of the connection must match exactly. |   |
| Norwork   | Encryption: DES  |   |
| A A A A A A A A A A A A A A A A A A A             | Authentication: SHA  |   |
| TTT   | DH Group:  |   |
|   |  |   |
|   | < Back Next Finish Cancel Help   | ו |

9. حدد السمات التي سيتم إستخدامها ل IPsec، المعروفة أيضا بالطور 2. يجب أن تتطابق هذه السمات على كل من ASA وموجه IOS. انقر فوق **Next** (التالي).

| 🖆 VPN Wizard   |  | × |
|--|--|---|
| VPN Wizard   | IPsec Encryption and Authentication (Step 4 of 6)  |   |
| Bandh<br>Bandh<br>Bandh<br>Hann<br>Corporatio<br>Natwork | Select the encryption and authentication algorithms for this IPsec VPN tunnel. Configurations<br>on both sides of the connection must match exactly. |   |
|  | < Back Next > Finish Cancel Help   | ) |

10. حدد البيئات المضيفة التي يجب السماح لحركة مرور البيانات الخاصة بها بالمرور من خلال نفق VPN. في هذه الخطوة، يجب عليك توفير **الشبكات المحلية** والبعيدة لنفق الشبكة الخاصة الظاهرية (VPN). انقر فوق الزر الموجود بجوار **الشبكات المحلية** كما هو موضح هنا لاختيار عنوان الشبكة المحلية من القائمة المنسدلة.

| 🖆 VPN Wizard |   |
|--------------|---|
| VPN Wizard   | Hosts and Networks (Step 5 of 6)  |
| Branch       | An IPsec tunnel protects data exchanged by selected hosts and networks at the local and<br>remote sites. Please identify hosts and networks to be used in the IPsec tunnel. |
|              | Action:   Protect  Do not Protect   |
| (Corporate)  | Local Networks: any   |
| Network      | Remote Networks: any  |
|              | ✓ Exempt ASA side host/network from address translation:  |
|              | < Back Next > Finish Cancel Help  |

11. أختر عنوان **الشبكة المحلية**، ثم انقر على **موافق** كما هو موضح هنا.

| Add      ✓ ✓ Edit      Delete     Q      Filter:     IP Address     Netmack     Description | Clear |
|---|-------|
| Filter:   | Clear |
| Name +1 IP Address Netmack Description  | CiBar |
| Name <sup>1</sup> IP Address Netmask Description  |       |
| Heno Products Houndary Costiption   |       |
| Network Objects   | _     |
| any 0.0.0.0 0.0.0.0   | _     |
| dmz-network 10.77.241.64 255.255.192  | _     |
| side-network 10.10.10.0 255.255.255.0   |       |
| outside-network 172.16.1.0 255.255.255.0  |       |
|   |       |
|   |       |
|   |       |
|   |       |
|   |       |
|   |       |
|   |       |
|   |       |
|   |       |
|   |       |
|   |       |
|   |       |
|   |       |
|   |       |
|   |       |
|   |       |
|   |       |
| Selected Local Networks   |       |
| Local Networks -> any   |       |
|   | _     |
|   | ncel  |
|   |       |

12. انقر فوق الزر الموجود بجوار **الشبكات البعيدة** كما هو موضح هنا لاختيار عنوان الشبكة البعيدة من القائمة المنسدلة.

| 🖆 VPN Wizard |   | × |
|--------------|---|---|
| VPN Wizard   | Hosts and Networks (Step 5 of 6)  |   |
| Branch       | An IPsec tunnel protects data exchanged by selected hosts and networks at the local and<br>remote sites. Please identify hosts and networks to be used in the IPsec tunnel. |   |
|              | Action:   Protect  Do not Protect   |   |
| Horne        | Local Networks: inside-network/24   |   |
| Corporate    | Remote Networks: any  |   |
|              |   |   |
|              | Exempt ASA side host/network from address translation:  | ~ |
|              | < Back Next > Finish Cancel He  | 9 |

13. أختر عنوان **الشبكة البعيدة**، ثم انقر على **موافق** كما هو موضح هنا.**ملاحظة:** إذا لم يكن لديك الشبكة البعيدة في القائمة، فيجب إضافة الشبكة إلى القائمة عن طريق النقر فوق **إضافة**.

| 🖆 Browse Remote Netwo    | irks        |                 |             |              |
|--------------------------|-------------|-----------------|-------------|--------------|
| 🗣 Add 🝷 🕝 Edit 🍿 De      | lete Q      |                 |             |              |
| Filter:                  |             |                 |             | Filter Clear |
| Name +1                  | IP Address  | Netmask         | Description |              |
| ⊡ Network Objects        |             |                 |             |              |
|                          | .0.0.0      | 0.0.0.0         |             |              |
| dmz-network 1            | 0.77.241.64 | 255.255.255.192 |             |              |
| - 🚮 inside-network 1     | 0.10.10.0   | 255.255.255.0   |             |              |
| outside-network 1        | 72.16.1.0   | 255.255.255.0   |             |              |
| i. 🛃 10.20.10.0 1        | 0.20.10.0   | 255.255.255.0   |             |              |
|                          |             |                 |             |              |
|                          |             |                 |             |              |
|                          |             |                 |             |              |
|                          |             |                 |             |              |
|                          |             |                 |             |              |
|                          |             |                 |             |              |
|                          |             |                 |             |              |
|                          |             |                 |             |              |
|                          |             |                 |             |              |
|                          |             |                 |             |              |
|                          |             |                 |             |              |
|                          |             |                 |             |              |
|                          |             |                 |             |              |
|                          |             |                 |             |              |
|                          |             |                 |             |              |
| Selected Remote Networks |             |                 |             |              |
|                          |             |                 |             |              |
| Remote Networks ->       | any         |                 |             |              |
|                          |             |                 |             |              |
|                          |             |                 | L_RK_       | Cancel       |
|                          |             |                 | Ne          |              |

14. حدد خانة الاختيار **Exception ASA Side Host/Network من ترجمة العنوان** لمنع حركة مرور النفق من الخضوع **لترجمة عنوان الشبكة**. ثم انقر فوق **التالي**.

| 🖆 VPN Wizard |   |  |
|--------------|---|--|
| VPN Wizard   | Hosts and Networks                                  | (Step 5 of 6)  |
| Bronch       | An IPsec tunnel protect<br>remote sites. Please ide | s data exchanged by selected hosts and networks at the local and<br>ntify hosts and networks to be used in the IPsec tunnel. |
|              | Action:   | Protect     O Do not Protect   |
| Home         | Local Networks:                                     | inside-network/24  |
| Network      | Remote Networks:                                    | 10.20.10.0/24  |
|              |   |  |
|              | 🗹 Exempt ASA side h                                 | ost/network from address translation:  |
|              |   | < Back Next > Finish Cancel Help   |

15. يتم عرض السمات التي تم تعريفها بواسطة معالج الشبكة الخاصة الظاهرية (VPN) في هذا الملخص. تحقق مرة أخرى من التكوين وانقر فوق **إنهاء** عندما ترضى بأن الإعدادات صحيحة.



### <u>تكوين SDM للموجه</u>

أكمل هذه الخطوات لتكوين نفق VPN من موقع إلى موقع على موجه Cisco IOS:

 افتح المستعرض وأدخل https://<IP\_Address الخاص بواجهة الموجه الذي تم تكوينه للوصول إلى إدارة قاعدة بيانات المحول (SDM)> للوصول إلى إدارة قاعدة بيانات المحول (SDM) على الموجه.تأكد من تخويل أية تحذيرات يعطيك المستعرض لها صلة بأصالة شهادة SSL. التقصير username وكلمة على حد سواء فارغ.يعرض الموجه هذه النافذة للسماح بتنزيل تطبيق إدارة قاعدة بيانات المحول (SDM). يقوم هذا المثال بتحميل التطبيق على الكمبيوتر المحلي ولا يعمل في تطبيق



2. يبدأ تنزيل إدارة قاعدة بيانات المحول (SDM) الآن. بمجرد تنزيل مشغل إدارة قاعدة بيانات المحول (SDM)، قم بإكمال الخطوات التي توجهها المطالبات لتثبيت البرنامج وتشغيل مشغل إدارة قاعدة بيانات المحول (SDM) من Cisco.

3. دخلت **ال username و كلمة** إن يعين أنت واحد وطقطقة ok.يستخدم هذا المثال Cisco123 لاسم المستخدم

| Authenticati                             | on Required 🛛 🛛 🔀                                |  |
|--|--|--|
| چ)<br>Javar                              |  |  |
| Enter login det<br>/10.77.241.10         | ails to access level_15 or view_access on<br>19: |  |
| User name:                               | cisco123   |  |
| Password:                                | •••••  |  |
| Save this password in your password list |  |  |
| OK Cancel                                |  |  |
| Authentication scheme: Basic             |  |  |

وCisco123 ككلمة المرور.

4. أخترت **تشكيل->VPN>موقع إلى موقع VPN** وطقطقت زر لاسلكي next to **خلقت VPN من موقع إلى موقع** على ال SDM صفحة الرئيسية. ثم انقر فوق **تشغيل المهمة المحددة** كما هو موضح



5. أختر **معالج خطوة بخطوة** لمتابعة التكوين:

| Site-to-Site VPN Wizard               |  |
|---------------------------------------|--|
| Site-to-Site VPN Wizard<br>VPN Wizard | Site-to-Site VPN This wizard will guide you through the necessary steps to configure one end of a site-to-site VPN tunnel on this router. The peer device must be configured with identical VPN configuration for the tunnel to work. Please select one of the following setup and click on the next button to begin. <b>Ouck setup</b> Quick setup asks for minimal information and uses SDM defaults. This is recommended if you are creating a VPN tunnel between two Cisco routers using SDM. View Defaults <b>Output: Output: Out</b> |
|                                       | < Back Next > Finish Cancel Help   |
|                                       | <pre></pre>  |

6. في الإطار التالي، توفر **معلومات اتصال VPN** في المساحات المقابلة. حدد واجهة نفق VPN من القائمة المنسدلة. هنا، يتم إختيار FastEthernet0. أخترت في **ال نظير هوية** قسم، **نظير مع ساكن إستاتيكي عنوان** ووفرت النظير بعيد عنوان. بعد ذلك، قم بتوفير **المفتاح المشترك مسبقا (Cisco123** في هذا المثال) في قسم المصادقة كما هو موضح . ثم انقر فوق **التالي**.

| Site-to-Site VPN Wizard |  |
|-------------------------|--|
| VPN Wizard              | VPN Connection Information<br>Select the interface for this VPN connection: FastEthernet0   Details  |
|                         | Peer Identity         Select the type of peer(s) used for this VPN connection:         Enter the IP address of the remote peer:  |
|                         | Authentication         Authentication ensures that each end of the VPN connection uses the same secret key.         Pre-shared Keys         pre-shared key:         *********         Re-enter Key:  |
|                         | Back Next > Finish Cancel Help     Can |

7. انقر فوق **إضافة** لإضافة اقتراحات IKE التي تحدد **خوارزمية التشفير وخوارزمية المصادقة** و**أسلوب تبادل** المفاتيح.

| Site-to-Site VPN Wizard |  |   |  |   |  |
|-------------------------|--|---|--|---|--|
| VPN Wizard              | IKE Proposals<br>IKE proposals specify the<br>method that is used by the<br>device. For the VPN con-<br>device should be config<br>Click the Add button to | ne encryption algorit<br>his router when neg<br>nection to be establi<br>ured with at least on<br>o add more policies | hm, authenticati<br>lotiating a VPN o<br>ished with the ra<br>le of the policies<br>and the Edit b | on algorithm and<br>connection with ti<br>emote device, the<br>s listed below.<br>outton to edit an e | t key exchange<br>he remote<br>e remote<br>xisting policy. |
|                         | Add Edi  | ion Hash  | D-H Group  | Authentication  | Type   |
|                         |  |   | < Back Next  | t× Finish C   | ancel Help   |

8. قم بتوفير **خوارزمية التشفير وخوارزمية المصادقة وطريقة تبادل المفاتيح** كما هو موضح هنا، ثم انقر فوق **موافق**. يجب أن تتطابق **خوارزمية التشفير وخوارزمية المصادقة وقيم طريقة تبادل المفاتيح** مع البيانات المقدمة

| Add IKE Policy       |  |
|----------------------|--|
| Configure IKE Policy |  |
| Priority:            | Authentication:  |
| Encryption:          | D-H Group:<br>group2                                   |
| Hash:<br>SHA_1       | Lifetime:<br>24 0 0 HH:MM:SS                           |
| <u> </u>             | Cancel Help  |
|                      | في ASA <b>ل</b><br>9. طقطقت <b>بعد ذلك</b> كما هو موضح |

هنا.

| Site-to-Site VPN Wizard |  |  |   |  |  |   | × |
|-------------------------|--|--|---|--|--|---|---|
| VPN Wizard              | IKE Proposal<br>IKE proposals<br>method that is<br>device. For the<br>device should<br>Click the Add | s<br>specify the en-<br>used by this ro<br>VPN connection<br>be configured to<br>button to add | ryption algorith<br>outer when nego<br>on to be establis<br>with at least on<br>more policies : | m, authenticati<br>otiating a VPN o<br>shed with the re<br>e of the policies<br>and the Edit b | on algorithm an<br>connection with t<br>emote device, th<br>s listed below.<br>outton to edit an o | d key exchange<br>he remote<br>e remote<br>existing policy. |   |
|                         | Priority   | Encryption   | Hash  | D-H Group  | Authentication   | Туре  |   |
|                         | 1  | 3DES   | SHA_1   | group2   | PRE_SHARE  | User Defined  |   |
|                         | Add  | Edit   | оня <u></u> т   | group  | РКЕ_ОПИКЕ  | Oser Delined  |   |
|                         |  | J  | 1   | < Back Nex   | t> Finish (  | Cancel Help   |   |

10. في هذه النافذة الجديدة، يجب توفير تفاصيل **مجموعة التحويل**. تحدد مجموعة التحويل خوارزميات **التشفير** و**المصادقة** المستخدمة لحماية **البيانات في نفق VPN**. ثم انقر فوق **إضافة** لتوفير هذه التفاصيل. يمكنك إضافة أي عدد من مجموعات التحويل حسب الحاجة بالنقر فوق **إضافة** وتوفير التفاصيل.

| Site-to-Site VPN Wizard |  |  |  | X   |
|-------------------------|--|--|--|---|
|                         | Transform Set<br>A transform set specifies the e<br>data in the VPN tunnel. Since to<br>communicate, the remote devi-<br>one selected below.<br>Click the Add button to add a<br>transform set.<br>Select Transform Set<br>SDM Default Transform<br>Details of the specified transform | encryption and auth<br>the two devices mo<br>ice must be config<br>new transform se<br>Set | nentication algorithm<br>ust use the same alg<br>ured with the same t<br>it and the Edit butto | is used to protect the<br>porithms to<br>transform set as the<br>in to edit the specified |
|                         | Name<br>ESP-3DES-SHA   | ESP Encryption<br>ESP_3DES   | ESP Integrity<br>ESP_SHA_HMAC  | AH Integrity  |
|                         |  | < [  | Back Next > Fini   | sh Cancel Help  |

11. قم بتوفير تفاصيل **مجموعة التحويل (خوارزمية التشفير والمصادقة**) وانقر فوق **موافق** كما هو

| Add Trans | form Set          |                   |                          | $\mathbf{X}$ |
|-----------|-------------------|-------------------|--------------------------|--------------|
| Name:     | ASA-IPSEC         |                   |                          |              |
| Dat       | ta integrity with | encryption (ES    | P)                       | _            |
| Integrity | Algorithm:        | ESP_SHA_HM        | MAC 🔽                    |              |
| Encrypti  | ion Algorithm:    | ESP_DES           | -                        |              |
|           |                   |                   | Show Advanced >          | >>           |
|           | ок                | Cancel            | Help                     |              |
| کما ھو    | القائمة المنسدلة  | يبتم استخدامها من | التحميا المطلوبة التبرير | حممكة        |

12. اختر **مجموعة التحويل** المطلوبة التي سيتم إستخدامها من القائمة المنسدلة كما هو موضح.

| Site-to-Site VPN Wizard |  |
|-------------------------|--|
|                         | Transform Set         A transform set specifies the encryption and authentication algorithms used to protect the data in the VPN tunnel. Since the two devices must use the same algorithms to communicate, the remote device must be configured with the same transform set as the one selected below.         Click the Add button to add a new transform set and the Edit button to edit the specified transform set.         Select Transform Set         SDM Default Transform Set         SDM Default Transform Set         Name         ESP Encryption         ESP Integrity         AH Integrity |
|                         | <pre>ESP-3DES-SHA ESP_3DES ESP_SHA_HMAC  Add Edit  Add Edit  Back Next &gt; Finish Cancel Help</pre>   |

. 13. انقر فوق Next (التالي).

14. في الإطار التالي، يمكنك توفير تفاصيل حول **حركة مرور البيانات التي يجب حمايتها** من خلال نفق الشبكة الخاصة الظاهرية (VPN). وفر **شبكات المصدر والوجهة** لحركة المرور أن يكون محميا بحيث تتم حماية حركة المرور بين شبكات المصدر والوجهة المحددة. في هذا المثال، شبكة المصدر هي 10.20.10.0 وشبكة الوجهة هي 10.10.10.0. ثم انقر فوق **التالي**.

| Site-to-Site VPN Wizard |   |  |
|-------------------------|---|--|
| VPN Wizard              | Traffic to protect<br>IPSec rules define the traffic, such as file trans-<br>protected by this VPN connection. Other data tra-<br>device. You can protect all traffic between a par-<br>specify an IPSec rule that defines the traffic type<br>Protect all traffic between the following subne- | fers (FTP) and e-mail (SMTP) that will be<br>affic will be sent unprotected to the remote<br>ticular source and destination subnet, or<br>es to be protected.<br>ets |
|                         | C Create/Select an access-list for IPSec traffic  | Remote Network<br>Enter the IP Address and Subnet Mask of<br>the destination Network.<br>IP Address:<br>10.10.10.0<br>Subnet Mask:<br>255.255.255.0 or 24            |
|                         |   | < Back Next > Finish Cancel Help   |

15. يبدي هذا نافذة خلاصة من الموقع إلى موقع VPN تشكيل تم. فحصت **إختبار اتصال VPN بعد تشكيل** خانة الاختيار إن أنت تريد أن إختبار اتصال VPN. هنا، يتم تحديد المربع حيث يلزم التحقق من الاتصال. ثم انقر فوق **إنهاء**.

| Site-to-Site VPN Wizard |  |  |                                    |                           |             |
|-------------------------|--|--|------------------------------------|---------------------------|-------------|
| VPN Wizard              | Summary of the   | Configuration  |                                    |                           |             |
|                         | Click Finish to de<br>Interface:FastEt<br>Peer Device:17:<br>Authentication T<br>pre-shared key:<br>IKE Policies:<br>Hash<br>SHA_1<br>SHA_1<br>Transform Sets<br>Name:<br>ESP Er<br>ESP In<br>Mode:T | eliver the configuration to the<br>hernet0<br>2.16.1.1<br>Ype : Pre-shared key<br>The Group<br>group1<br>group2<br>:<br>ASA-IPSEC<br>heryption:ESP_DES<br>tegrity:ESP_SHA_HMAC<br>TUNNEL | Authentication PRE_SHARE PRE_SHARE | Encryption<br>DES<br>3DES |             |
|                         |  |  | < Back Next>                       | Finish                    | Cancel Help |

16. انقر على **بدء** كما هو موضح للتحقق من اتصال VPN.

| VPN | Troubleshooting          |                       |           | × |
|-----|--------------------------|-----------------------|-----------|---|
|     | Tunnel Details           |                       |           |   |
|     | Interface: FastEthernet0 | Peer: 172.16.1.1      |           |   |
|     |                          |                       |           | 1 |
|     |                          |                       |           |   |
|     |                          |                       |           |   |
|     |                          | 🔳 Summany             | 🖳 Details |   |
| [   | Activity                 |                       | Status    |   |
|     |                          |                       |           |   |
|     |                          |                       |           |   |
|     |                          |                       |           |   |
|     |                          |                       |           |   |
|     |                          |                       |           |   |
|     |                          |                       |           |   |
|     | Failure Reason(s)        | Recommended Action(s) |           |   |
|     |                          |                       |           |   |
|     |                          |                       |           |   |
|     |                          |                       |           |   |
|     |                          |                       |           |   |
|     |                          |                       |           |   |
|     |                          |                       |           |   |
|     |                          |                       |           |   |
|     | Start Save Report        | Close                 | Help      |   |

17. في الإطار التالي يتم توفير نتيجة **إختبار اتصال VPN**. هنا، يمكنك أن ترى ما إذا كان النفق **أعلى** أو **أسفل**. في مثال التكوين هذا، يتم **تشغيل** النفق كما هو موضح بالأخضر.

| ٧P | N Troubl | esh  | ooting          |      |        |   |       |        |          |         |      |        |           |    | $\mathbf{X}$ |
|----|----------|------|-----------------|------|--------|---|-------|--------|----------|---------|------|--------|-----------|----|--------------|
| Г  | Tunnel   | Det  | ails            | ~    |        |   |       |        |          |         |      |        |           |    |              |
|    | Interfac | e:   | FastEthernet0   |      |        |   | Peer  | : 172  | .16.1.   | .1      |      |        |           |    |              |
|    |          |      |                 |      |        |   |       |        |          |         |      |        |           |    |              |
|    |          |      |                 |      |        |   |       |        |          |         |      |        |           |    |              |
| [  |          |      |                 |      |        |   |       |        |          | Summ    | nary | Ę      | 🖁 Details | ;  |              |
|    | Activity |      |                 |      |        |   |       |        |          |         |      | Status |           |    |              |
|    | Checkin  | g th | e tunnel status |      |        |   |       |        |          |         |      | 🔾 Up   |           |    |              |
|    |          |      |                 |      |        |   |       |        |          |         |      |        |           |    |              |
|    |          |      |                 |      |        |   |       |        |          |         |      |        |           |    |              |
|    |          |      |                 |      |        |   |       |        |          |         |      |        |           |    |              |
|    |          |      |                 |      |        |   |       |        |          |         |      |        |           |    |              |
|    | Failure  | Rea  | ason(s)         |      |        | F | Recom | mende  | n Act    | tion(s) |      |        |           | -1 |              |
|    | - unare  |      | 10011(0)        |      |        |   |       | ino na | 0.011101 | 1011(0) |      |        |           |    |              |
|    |          |      |                 |      |        |   |       |        |          |         |      |        |           |    |              |
|    |          |      |                 |      |        |   |       |        |          |         |      |        |           |    |              |
|    |          |      |                 |      |        |   |       |        |          |         |      |        |           |    |              |
|    |          |      |                 |      |        |   |       |        |          |         |      |        |           |    |              |
|    |          |      |                 |      |        |   |       |        |          |         |      |        |           |    |              |
| _  |          |      |                 |      |        |   |       |        |          |         |      |        |           |    |              |
|    |          | ş    | Start           | Save | Report |   |       | Close  | ,        |         |      | Help   |           |    |              |
|    |          |      |                 |      |        |   |       |        |          |         |      |        |           |    |              |

يؤدي هذا إلى اكتمال التكوين على موجه Cisco IOS.

## <u>تکوین ASA CLI</u>

| ASA   |
|---|
|   |
| ASA# <b>show run</b>  |
| Saved :   |
| (ASA Version 8.0(2  |
| !   |
| hostname ASA  |
| enable password 8Ry2YjIyt7RRXU24 encrypted                  |
| names   |
| !   |
| Configure the outside interface. ! interface!               |
| Ethernet0/1 nameif outside security-level 0 ip address      |
| 172.16.1.1 255.255.255.0 ! Configure the inside             |
| <pre>interface. ! interface Ethernet0/2 nameif inside</pre> |
| security-level 100 ip address 10.10.10.1 255.255.255.0      |
| <pre>! Output suppressed ! passwd 2KFQnbNIdI.2KYOU</pre>    |

encrypted ftp mode passive dns server-group DefaultDNS domain-name default.domain.invalid access-list 100 extended permit ip any any access-list inside\_nat0\_outbound extended permit ip 10.10.10.0 255.255.255.0 255.255.255.0 10.20.10.0 This access list (inside\_nat0\_outbound) is used !-- ---! - with the **nat zero** command. This prevents traffic which !--- matches the access list from undergoing network address translation (NAT). !--- The traffic specified by this ACL is traffic that is to be encrypted and !--sent across the VPN tunnel. This ACL is intentionally !--- the same as (outside\_1\_cryptomap). !--- Two separate access lists should always be used in this .configuration access-list outside\_1\_cryptomap extended permit ip 10.10.10.0 255.255.255.0 255.255.255.0 10.20.10.0 This access list (outside\_cryptomap) is used !--- ---! with the crypto map **outside\_map** !--- to determine which traffic should be encrypted and sent !--- across the tunnel. !--- This ACL is intentionally the same as (inside\_nat0\_outbound). !--- Two separate access lists .should always be used in this configuration pager lines 24 mtu inside 1500 mtu outside 1500 no failover asdm image disk0:/asdm-613.bin asdm history enable arp timeout 14400 global (outside) 1 interface nat (inside) 1 10.10.10.0 255.255.255.0 nat (inside) 0 access-list inside\_nat0\_outbound NAT 0 prevents NAT for networks specified in !--- ---! .the ACL inside\_nat0\_outbound 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 timeout mgcp-pat 0:05:00 sip 0:30:00 sip\_media 0:02:00 timeout uauth 0:05:00 absolute http server enable http 0.0.0.0 0.0.0.0 dmz no snmp-server location no snmp-server contact PHASE 2 CONFIGURATION ---! !--- The encryption ---! types for Phase 2 are defined here. crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac Define the transform set for Phase 2. crypto map ---! outside\_map 1 match address outside\_1\_cryptomap Define which traffic should be sent to the IPsec ---! peer. crypto map outside\_map 1 set peer 172.17.1.1 Sets the IPsec peer crypto map outside\_map 1 set ---!

transform-set ESP-DES-SHA Sets the IPsec transform set "ESP-AES-256-SHA" !--- ---! to be used with the crypto map entry "outside\_map". crypto map outside\_map interface outside Specifies the interface to be used with !--- the ---! settings defined in this configuration. !--- PHASE 1 CONFIGURATION ---! !--- This configuration uses isakmp policy 10. !--- The configuration commands here define the Phase !--- 1 policy parameters that are used. crypto isakmp enable outside crypto isakmp policy 10 authentication pre-share encryption des hash sha group 1 lifetime 86400 telnet timeout 5 ssh timeout 5 console timeout 0 threat-detection basic-threat threat-detection statistics access-list ! tunnel-group 172.17.1.1 type ipsec-121 In order to create and manage the database of ---! connection-specific !--- records for ipsec-121-IPsec (LAN-to-LAN) tunnels, use the command !--- tunnel-group in global configuration mode. !--- For L2L connections the name of the tunnel group **MUST** be the IP !--- address .of the IPsec peer tunnel-group 172.17.1.1 ipsec-attributes \* pre-shared-key Enter the pre-shared-key in order to configure the ---! !--- authentication method. telnet timeout 5 ssh timeout 5 console timeout 0 threat-detection basic-threat threat-detection statistics access-list ! class-map inspection\_default match default-inspection-traffic ! ! !-- Output suppressed! username cisco123 password ffIRPGpDSOJh9YLq encrypted privilege 15 Cryptochecksum:be38dfaef777a339b9e1c89202572a7d : end

#### <u>تكوين CLI للموجه</u>

#### الموجّه ...Building configuration Current configuration : 2403 bytes ! version 12.3 service timestamps debug datetime msec service timestamps log datetime msec service password-encryption ! hostname R3 !

```
boot-start-marker
                                         boot-end-marker
                                                        1
                                     no logging buffered
                                                        !
               username cisco123 privilege 15 password 7
                                      1511021F07257A767B
                                        no aaa new-model
                                          ip subnet-zero
                                                        !
                                                        !
                                                   ip cef
                                                        Т
                                                        !
                                ip ips po max-events 100
                              no ftp-server write-enable
                                                        !
   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 2
                               authentication pre-share
      Specifies the pre-shared key "cisco123" which ---!
should !--- be identical at both peers. This is a global
      !--- configuration mode command. crypto isakmp key
                             cisco123 address 172.16.1.1
                                                        I
                                                        !
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 ASA-IPSEC
                                    esp-des esp-sha-hmac
                                                        !
 Indicates that IKE is used to establish !--- ---! ---!
  the IPsec Security Association for protecting the !---
  traffic specified by this crypto map entry. crypto map
                               SDM_CMAP_1 1 ipsec-isakmp
                        description Tunnel to172.16.1.1
    Sets the IP address of the remote end. set ---! ---!
                                         peer 172.16.1.1
Configures IPsec to use the transform-set !--- ---! ---!
  "ASA-IPSEC" defined earlier in this configuration. set
                                 transform-set ASA-IPSEC
       Specifies the interesting traffic to be ---! ---!
                            encrypted. match address 100
                                                        Ţ
                                                        1
                                                        1
Configures the interface to use the !--- crypto map ---!
      "SDM_CMAP_1" for IPsec. interface FastEthernet0 ip
address 172.17.1.1 255.255.255.0 duplex auto speed auto
                                   crypto map SDM_CMAP_1
                                                        Ţ
                                 interface FastEthernet1
                    ip address 10.20.10.2 255.255.255.0
```

```
duplex auto
                                            speed auto
                                                       !
                                interface FastEthernet2
                                         no ip address
                                                      !
                                        interface Vlan1
             ip address 10.77.241.109 255.255.255.192
                                                       !
                                           ip classless
          ip route 10.10.10.0 255.255.255.0 172.17.1.2
       ip route 10.77.233.0 255.255.255.0 10.77.241.65
          ip route 172.16.1.0 255.255.255.0 172.17.1.2
                                                       !
                                                       !
        ip nat inside source route-map nonat interface
                                 FastEthernet0 overload
                                                       !
                                         ip http server
                          ip http authentication local
                                  ip http secure-server
                                                       !
   Configure the access-lists and map them to the ---!
 Crypto map configured. access-list 100 remark SDM_ACL
                                             Category=4
                     access-list 100 remark IPSec Rule
        access-list 100 permit ip 10.20.10.0 0.0.0.255
                                   10.10.10.0 0.0.0.255
                                                       !
                                                       !
                                                       T
  This ACL 110 identifies the traffic flows using -
                                                      - !
route map access-list 110 deny ip 10.20.10.0 0.0.0.255
                                   10.10.10.0 0.0.0.255
    access-list 110 permit ip 10.20.10.0 0.0.0.255 any
                              route-map nonat permit 10
                                  match ip address 110
                                                      !
                                          control-plane
                                                       !
                                                       !
                                             line con 0
                                           login local
                                             line aux 0
                                           line vty 0 4
                                    privilege level 15
                                           login local
                            transport input telnet ssh
                                                      1
                                                     end
```

# <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 .

- جهاز أمان PIX أوامر show
- <u>موجه IOS البعيد أوامر show</u>

#### جهاز الأمان ASA/PIX - show commands

• 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: 172.17.1.1 1 Type : L2L Role : initiator Rekey : no State : MM\_ACTIVE • show crypto ipSec sa— يعرض جميع معرفات فئات خدمة IPsec الحالية في نظير. ASA#show crypto ipsec sa interface: outside Crypto map tag: outside\_map, seq num: 1, local addr: 172.16.1.1 (local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0 (remote ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0 current\_peer: 172.17.1.1 pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9# pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9# pkts compressed: 0, #pkts decompressed: 0# pkts not compressed: 9, #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.: 172.16.1.1, remote crypto endpt.: 172.17.1.1 path mtu 1500, ipsec overhead 58, media mtu 1500 current outbound spi: 434C4A7F :inbound esp sas (spi: 0xB7C1948E (3082917006 transform: esp-des esp-sha-hmac none { ,in use settings ={L2L, Tunnel, PFS Group 2 slot: 0, conn\_id: 12288, crypto-map: outside\_map (sa timing: remaining key lifetime (kB/sec): (4274999/3588 IV size: 8 bytes replay detection support: Y :outbound esp sas (spi: 0x434C4A7F (1129073279 transform: esp-des esp-sha-hmac none { ,in use settings ={L2L, Tunnel, PFS Group 2 slot: 0, conn\_id: 12288, crypto-map: outside\_map (sa timing: remaining key lifetime (kB/sec): (4274999/3588 IV size: 8 bytes replay detection support: Y

### <u>موجه IOS البعيد - إظهار الأوامر</u>

show crypto isakmp sa— يعرض جميع شبكات IKE الحالية في نظير. Router#show crypto isakmp sa

| dst     | src | state    | conn-id    | slot status |
|---------|-----|----------|------------|-------------|
| QM_IDLE | 3   | 0 ACTIVE | 172.16.1.1 | 172.17.1.1  |

• show crypto ipSec sa— يعرض جميع معرفات فئات خدمة IPsec الحالية في نظير.

```
Router#show crypto ipsec sa
                                              interface: FastEthernet0
                 Crypto map tag: SDM_CMAP_1, local addr 172.17.1.1
                                              (protected vrf: (none
 (local ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0
 (remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0
                                   current_peer 172.16.1.1 port 500
                                   {,PERMIT, flags={origin_is_acl
               pkts encaps: 68, #pkts encrypt: 68, #pkts digest: 68#
             pkts decaps: 68, #pkts decrypt: 68, #pkts verify: 68#
                        pkts compressed: 0, #pkts decompressed: 0#
                   pkts not compressed: 0, #pkts compr. failed: 0#
             pkts not decompressed: 0, #pkts decompress failed: 0#
                                    send errors 0, #recv errors 0#
local crypto endpt.: 172.17.1.1, remote crypto endpt.: 172.16.1.1
                                       path mtu 1500, ip mtu 1500
                     (current outbound spi: 0xB7C1948E(3082917006
                                                  :inbound esp sas
                                     (spi: 0x434C4A7F(1129073279
                             , transform: esp-des esp-sha-hmac
                                   { ,in use settings ={Tunnel
 conn id: 2001, flow_id: C18XX_MBRD:1, crypto map: SDM_CMAP_1
     (sa timing: remaining key lifetime (k/sec): (4578719/3004
                                              IV size: 8 bytes
                                   replay detection support: Y
                                                Status: ACTIVE
                                                   inbound ah sas
                                                  :inbound pcp sas
                                                 :outbound esp sas
                                     (spi: 0xB7C1948E(3082917006
                             , transform: esp-des esp-sha-hmac
                                   { ,in use settings ={Tunnel
 conn id: 2002, flow_id: C18XX_MBRD:2, crypto map: SDM_CMAP_1
     (sa timing: remaining key lifetime (k/sec): (4578719/3002
                                              IV size: 8 bytes
                                   replay detection support: Y
                                                Status: ACTIVE
                                                  :outbound ah sas
```

:outbound pcp sas

show crypto engine connections active—يعرض الاتصالات والمعلومات الحالية حول الحزم المشفرة • وغير المشفرة (الموجه فقط).

Router#show crypto engine connections active

| ID Interface  | IP-Address | Stat | te Algorithm       | Encrypt | Decrypt |
|---------------|------------|------|--------------------|---------|---------|
| FastEthernet0 | 172.17.1.1 | set  | HMAC_SHA+DES_56_CB | 0       | 03      |
| FastEthernet0 | 172.17.1.1 | set  | DES+SHA            | 0       | 59 2001 |
| FastEthernet0 | 172.17.1.1 | set  | DES+SHA            | 59      | 0 2002  |

# <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 .

**ملاحظة:** ارجع إلى <u>معلومات مهمة حول أوامر تصحيح الأخطاء</u> و<u>أستكشاف أخطاء أمان IP وإصلاحها - فهم أوامر</u> <u>تصحيح الأخطاء واستخدامها</u> قبل أن تستخدم أوامر debug.

- debug crypto ips 7—يعرض مفاوضات IPsec للمرحلة debug crypto isakmp 7.2 للمرحلة ISakmp 7.2 ــيعرض مفاوضات المرحلة 1.
- debug crypto ipSec—يعرض مفاوضات IPsec للمرحلة debug crypto isakmp.2—يعرض مفاوضات ISAKMP للمرحلة 1.

ارجع إلى <u>حلول أستكشاف أخطاء IPSec VPN وإصلاحها الأكثر شيوعا في المستوى 2L والوصول عن بعد</u> للحصول على مزيد من المعلومات حول أستكشاف أخطاء موقع VPN وإصلاحها.

# <u>معلومات ذات صلة</u>

- <u>برنامج جدار حماية Cisco PIX</u>
- مدير أجهزة حلول الأمان المعدلة من <u>Cisco</u>
- <u>أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances</u>
- <u>محترف التكوين: شبكة VPN من موقع إلى موقع بين ASA/PIX ومثال تكوين موجه IOS</u>
  - مراجع أوامر جدار حماية PIX الآمن من Cisco
    - <u>مدير أجهزة الأمان والموجه من Cisco</u>
      - <u>طلبات التعليقات (RFCs)</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