

# VPN ريظن تامولعم ةفاضل: ASA 8.x/ASDM 6.x ىلإ عقوم نم ةدوجوم VPN ةكبش يف ةديج ASDM مادختساب عقوم

## المحتويات

[المقدمة](#)

[المتطلبات الأساسية](#)

[المتطلبات](#)

[المكونات المستخدمة](#)

[الاصطلاحات](#)

[معلومات خلفية](#)

[تكوين ASDM](#)

[إنشاء ملف تعريف اتصال جديد](#)

[تحرير تكوين VPN الموجود](#)

[التحقق من الصحة](#)

[استكشاف الأخطاء وإصلاحها](#)

[تعذر على بادئ IKE العثور على النهج: SRC: 172.16.1.103، DST: 10.1.4.251، INTF test\\_ext](#)

[معلومات ذات صلة](#)

## المقدمة

يقدم هذا المستند معلومات حول تغييرات التكوين التي يتم إجراؤها عند إضافة نظير شبكة VPN جديد إلى تكوين شبكة VPN الموجود من موقع إلى موقع باستخدام مدير أجهزة الأمان القابل للتكيف (ASDM). وهذا مطلوب في هذه السيناريوهات:

- تم تغيير موفر خدمة الإنترنت (ISP) ويتم استخدام مجموعة جديدة من نطاق IP العام.
  - إعادة تصميم كاملة للشبكة في موقع ما.
  - يتم ترحيل الجهاز المستخدم كبوابة VPN في موقع ما إلى جهاز جديد باستخدام عنوان IP عام مختلف.
- يفترض هذا المستند أن شبكة VPN من الموقع إلى الموقع تم تكوينها بالفعل بشكل صحيح وتعمل بشكل صحيح. يزود هذا وثيقة ال steps أن يتبع in order to غيرت VPN نظير معلومة في ال L2L VPN تشكيل.

## المتطلبات الأساسية

### المتطلبات

Cisco يوصي أن يتلقى أنت معرفة من هذا موضوع:

- [مثال تكوين VPN من موقع ASA إلى موقع](#)

### المكونات المستخدمة

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

- سلسلة أجهزة الأمان المعدلة Cisco 5500 مع إصدار البرنامج 8.2 والإصدارات الأحدث
- مدير أجهزة حلول الأمان المعدلة من Cisco مع الإصدار 6.3 من البرنامج والإصدارات الأحدث

## الاصطلاحات

راجع [اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.](#)

## معلومات خلفية

تعمل الشبكة الخاصة الظاهرية (VPN) من موقع إلى موقع بشكل جيد بين الحقاصة والبقاصة. بافتراض أن BKASA لديه إعادة تصميم شبكة كاملة وتم تعديل مخطط IP على مستوى ISP، ولكن تبقى جميع تفاصيل الشبكة الفرعية الداخلية كما هي.

يستخدم نموذج التكوين هذا عناوين IP التالية:

• BKASA موجود خارج عنوان 200.200.200.200 - IP

• BKASA جديد خارج عنوان 209.165.201.2 - IP

**ملاحظة:** هنا، سيتم تعديل معلومات النظير فقط. نظرا لعدم وجود تغيير آخر في الشبكة الفرعية الداخلية، تظل قوائم الوصول الخاصة بالشفرة كما هي.

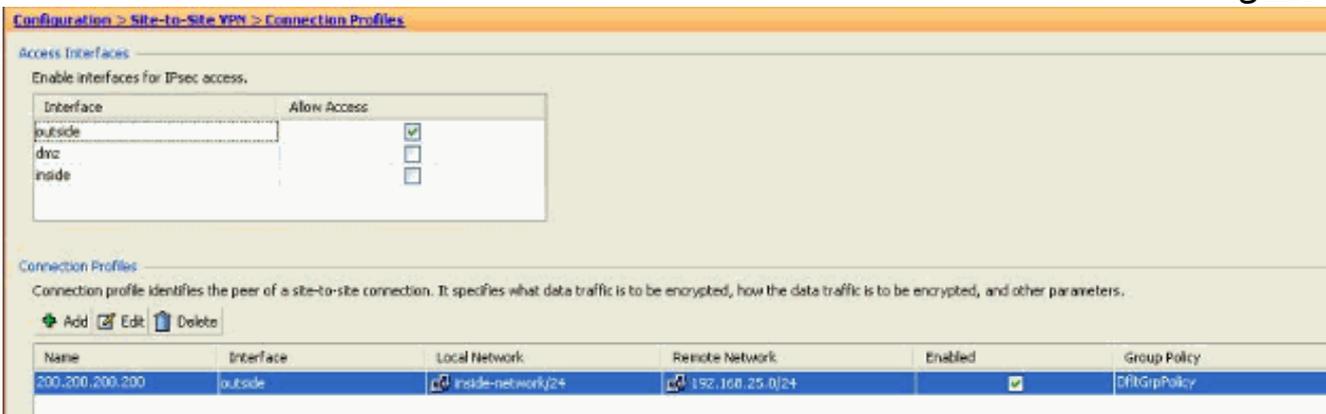
## تكوين ASDM

يوفر هذا القسم معلومات حول الطرق المحتملة المستخدمة لتغيير معلومات نظير VPN على HKASA باستخدام ASDM.

### إنشاء ملف تعريف اتصال جديد

يمكن أن يكون هذا هو الطريقة الأسهل لأنه لا يزعج تكوين VPN الموجود ويمكن أن يخلق ملف تعريف اتصال جديد باستخدام المعلومات الجديدة ذات الصلة بنظير VPN.

1. انتقل إلى التكوين < VPN من موقع إلى موقع > ملفات تعريف الاتصال وانقر فوق إضافة ضمن منطقة ملفات تعريف الاتصال.



يظهر إطار إضافة ملف تعريف اتصال من موقع إلى موقع IPsec. 2. تحت علامة التبويب "أساسي"، قم بتوفير تفاصيل عنوان IP للنظير والمفتاح المشترك مسبقا والشبكات المحمية. استعملت كل ال نفسه معلم بما أن ال VPN موجود، ماعدا النظير معلومة. وانقر فوق

**Add IPsec Site-to-Site Connection Profile**

Peer IP Address:  Static 209.165.201.2

Connection Name:  Same as IP Address 209.165.201.2

Interface: outside

**IKE Authentication**

Pre-shared Key: .....

Identity Certificate: -- None --

**Protected Networks**

Local Network: inside-network/24

Remote Network: 192.168.25.0/24

**Encryption Algorithms**

IKE Proposal: pre-share-des-sha, pre-share-3des-sha

IPsec Proposal: :S-256-MD5, ESP-3DES-SHA, ESP-3DES-MD5, ESP-DES-SHA, ESP-DES-MD5

Find:   Next  Previous

3. تحت قائمة متقدمة، انقر فوق إدخال خريطة التشفير. ارجع إلى علامة التبويب الأولوية. هذه الأولوية مساوية للرقم التسلسلي في تكوين CLI المكافئ الخاص بها. عند تعيين رقم أقل من إدخال خريطة التشفير الحالي، يتم تنفيذ ملف التعريف الجديد هذا أولاً. كلما زاد رقم الأولوية، كلما قلت القيمة. يستخدم هذا لتغيير ترتيب التسلسل الذي سيتم تنفيذ خريطة تشفير معينة به. انقر على موافق لإكمال إنشاء توصيف توصيل جديد.

**Add IPsec Site-to-Site Connection Profile**

Priority: 20

Perfect Forward Secrecy:  Disable  Enable

Diffie-Hellman Group:

NAT-T:  Enable

Reverse Route Injection:  Enable

**Security Association Lifetime**

Time: 8 : 0 : 0 hh:mm:ss

Traffic Volume: 4608000 KBytes

**Static Crypto Map Entry Parameters**

Connection Type: bidirectional

CA Certificate: -- None --

Send CA Certificate Chain

IKE Negotiation Mode:  Main  Aggressive

Diffie-Hellman Group:

Find:   Next  Previous

يؤدي هذا تلقائياً إلى إنشاء مجموعة نفق جديدة مع خريطة تشفير مقترنة. تأكد من إمكانية الوصول إلى BKASA باستخدام عنوان IP الجديد قبل استخدام ملف تعريف الاتصال الجديد هذا.

## تحرير تكوين VPN الموجود

هناك طريقة أخرى لإضافة نظير جديد وهي تعديل التكوين الموجود. لا يمكن تحرير ملف تعريف الاتصال الموجود لمعلومات النظير الجديدة لأنه مرتبط بنظير معين. in order to حررت التشكيل حالي، أنت تحتاج أن ينجز هذا steps:

1. إنشاء مجموعة نفق جديدة
2. تحرير خريطة التشفير الموجودة

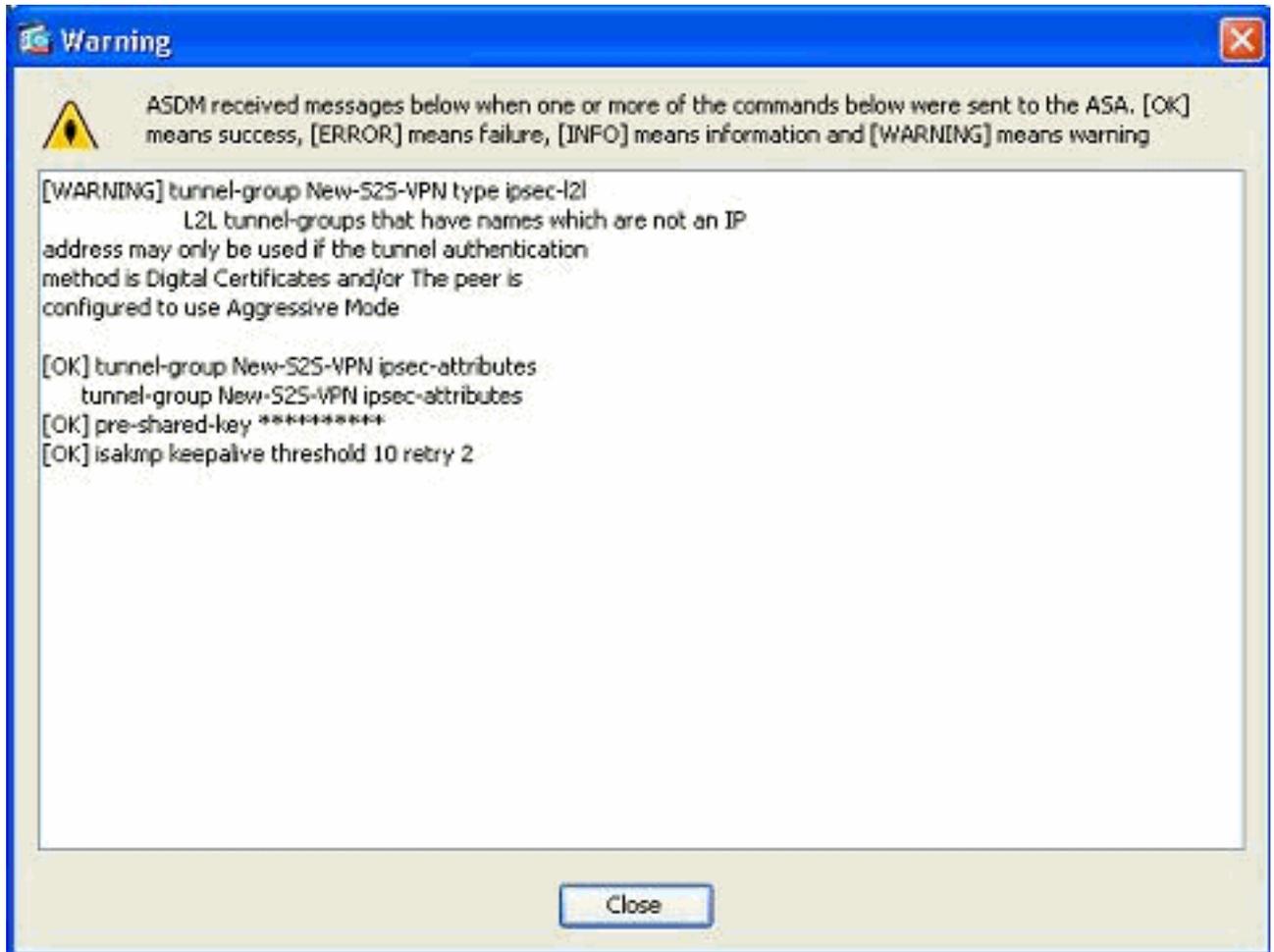
## إنشاء مجموعة نفق جديدة

انتقل إلى التكوين < VPN من موقع إلى موقع < متقدم < مجموعات النفق وانقر فوق إضافة لإنشاء مجموعة نفق جديدة تحتوي على معلومات نظير VPN الجديدة. حدد حقل الاسم والمفتاح المشترك مسبقاً، ثم انقر على موافق.

ملاحظة: تأكد من تطابق المفتاح المشترك مسبقاً مع الطرف الآخر من شبكة VPN.

The screenshot shows the 'Add IPsec Site-to-site Tunnel Group' dialog box. The 'Name' field is set to '209.165.201.2'. Under 'IKE Authentication', the 'Pre-shared Key' is masked with '\*\*\*\*\*', 'Identity Certificate' is set to '-- None --', 'Send Certificate Chain' is 'Enable', and 'IKE Peer ID Validation' is 'Required'. Under 'IKE Keepalive', 'Disable keepalives' is selected, with 'Confidence Interval' and 'Retry Interval' fields. Under 'Default Group Policy', 'Group Policy' is 'DfltGrpPolicy' and 'IPsec Protocol' is 'Enabled'. Buttons for 'OK', 'Cancel', and 'Help' are at the bottom.

ملاحظة: في حقل "الاسم"، يجب إدخال عنوان IP فقط للنظير البعيد عندما يكون وضع المصادقة مفاتيح مشتركة مسبقاً. يمكن استخدام أي اسم فقط عندما تكون طريقة المصادقة من خلال الشهادات. يظهر هذا خطأ عندما تتم إضافة اسم في حقل الاسم ويتم مشاركة طريقة المصادقة مسبقاً:

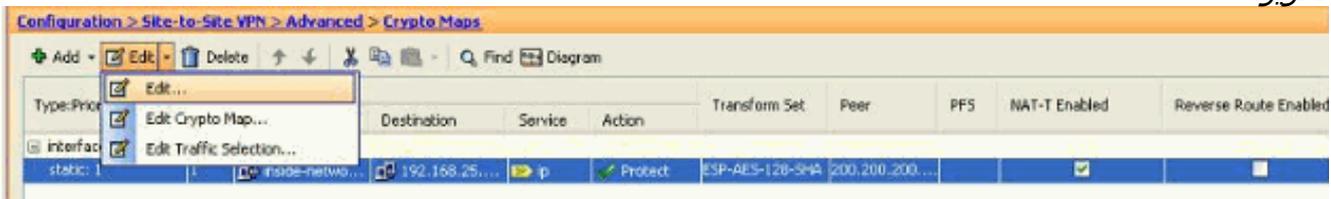


### تحرير خريطة التشفير الموجودة

يمكن تحرير خريطة التشفير الموجودة لإقران معلومات النظير الجديدة.

أكمل الخطوات التالية:

1. انتقل إلى التكوين < VPN < موقع إلى موقع < متقدم < خرائط التشفير، ثم حدد خريطة التشفير المطلوبة وانقر فوق تحرير.



تظهر نافذة تحرير قاعدة IPsec.

2. تحت علامة التبويب سياسة النفق (أساسي)، في منطقة إعدادات النظير، حدد النظير الجديد في حقل عنوان IP الخاص بالنظير المراد إضافته. بعد ذلك، انقر فوق إضافة.

**Edit IPsec Rule**

Tunnel Policy (Crypto Map) - Basic | Tunnel Policy (Crypto Map) - Advanced | Traffic Selection

Interface: outside      Policy Type: static      Priority: 1

**Transform Sets**

Transform Set to Be Added:

ESP-AES-128-MD5      Add >>      ESP-AES-128-SHA      Move Up

Remove      Move Down

**Peer Settings - Optional for Dynamic Crypto Map Entries**

The Connection Type is applicable to static tunnel policies only. Uni-directional connection type policies are used for LAN-to-LAN redundancy. Tunnel policies of the 'Originate Only' connection type may specify up to 10 redundant peers.

Connection Type: bidirectional

IP Address of Peer to Be Added:

209.165.201.2      Add >>      200.200.200.200      Move Up

Remove      Move Down

Enable Perfect Forwarding Secrecy

Diffie-Hellman Group: [ ]

OK      Cancel      Help

3. حدد عنوان IP للنظير الموجود وانقر فوق إزالة للاحتفاظ بمعلومات النظير الجديدة فقط. وانقر فوق .OK

**Edit IPsec Rule**

Tunnel Policy (Crypto Map) - Basic | Tunnel Policy (Crypto Map) - Advanced | Traffic Selection

Interface: outside      Policy Type: static      Priority: 1

**Transform Sets**

Transform Set to Be Added:

ESP-AES-128-MD5      Add >>      ESP-AES-128-SHA      Move Up

Remove      Move Down

**Peer Settings - Optional for Dynamic Crypto Map Entries**

The Connection Type is applicable to static tunnel policies only. Uni-directional connection type policies are used for LAN-to-LAN redundancy. Tunnel policies of the 'Originate Only' connection type may specify up to 10 redundant peers.

Connection Type: bidirectional

IP Address of Peer to Be Added:

200.200.200.200      Add >>      209.165.201.2      Move Up

Remove      Move Down

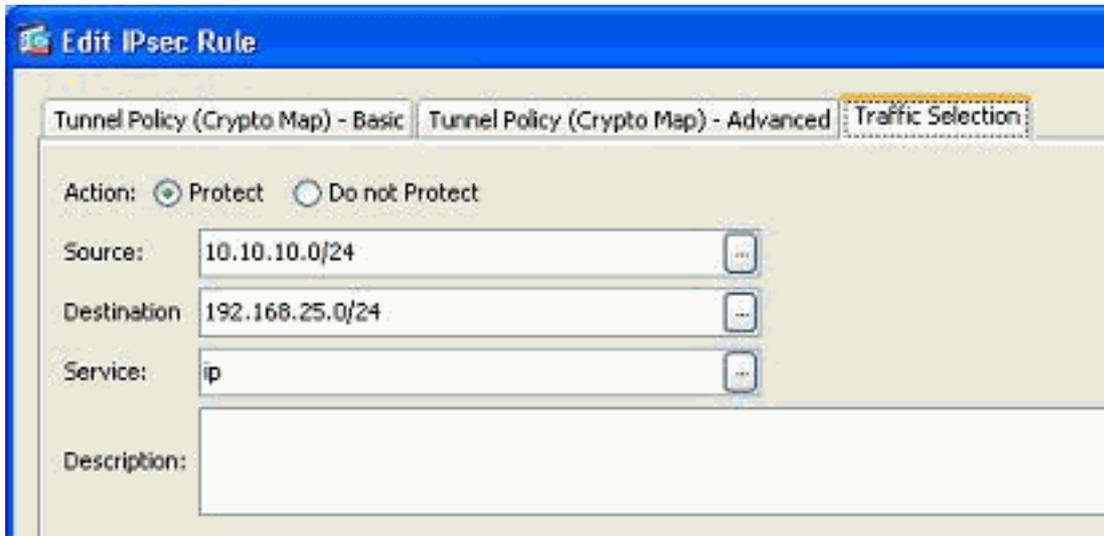
Enable Perfect Forwarding Secrecy

Diffie-Hellman Group:     

OK      Cancel      Help

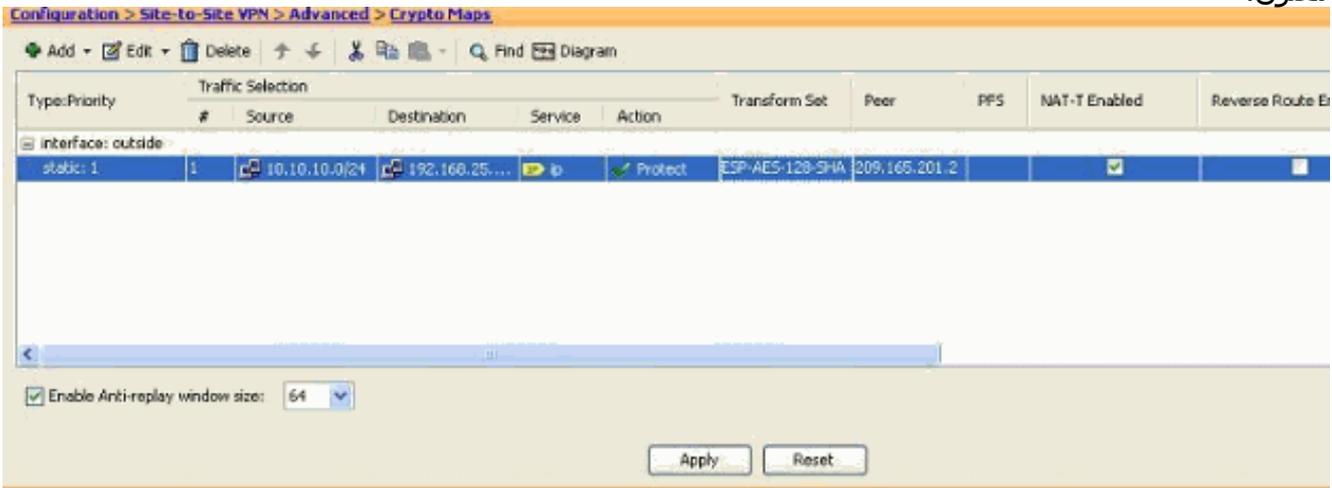
**ملاحظة:** بعد تعديل معلومات النظير في خريطة التشفير الحالية، يتم حذف ملف تعريف الاتصال المرتبط بخريطة التشفير هذه فوراً في نافذة ASDM.

4. تبقى تفاصيل الشبكات المشفرة كما هي. إذا كنت بحاجة إلى تعديل هذه العناصر، فانتقل إلى علامة التبويب تحديد حركة مرور



البيانات.

5. انتقل إلى التكوين < VPN من موقع إلى موقع > متقدم < جزء خرائط التشفير لعرض خريطة التشفير المعدلة. ومع ذلك، لا تحدث هذه التغييرات حتى تنقر فوق تطبيق. بعد النقر فوق تطبيق، انتقل إلى التكوين < شبكة VPN من موقع إلى موقع > متقدم < مجموعات النفق للتحقق من وجود مجموعة أنفاق مقترنة أو عدم وجودها. إذا كانت الإجابة نعم، سيتم إنشاء ملف تعريف اتصال مقترن.



## التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم أداة مترجم الإخراج (للعلماء المسجلين فقط) بعض أوامر show. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مخرج الأمر **show**.

• استخدم هذا الأمر لعرض معلمات اقتران الأمان المحددة لنظير واحد: عرض نظير IPsec للتشفير > عنوان IP للنظير

## استكشاف الأخطاء وإصلاحها

استخدم هذا القسم لاستكشاف أخطاء التكوين وإصلاحها.

تعذر على بادئ IKE العثور على النهج: DST: 172.16.1.103، SRC: INTF test\_ext، 10.1.4.251

يعرض هذا الخطأ في رسائل السجل عند محاولة تغيير نظير VPN من مركز VPN إلى ASA.

**الحل:**

قد يكون هذا نتيجة لخطوات التكوين غير الصحيحة التي تم اتباعها أثناء الترحيل. تأكد من إزالة ربط التشفير بالواجهة قبل إضافة نظير جديد. تأكدت أيضا، أن أنت استعملت العنوان من النظير في النفق-مجموعة، غير أن ليس الاسم.

## معلومات ذات صلة

- [موقع إلى موقع \(VPN L2L\) مع ASA](#)
- [أكثر مشاكل الشبكات الخاصة الظاهرية \(VPN\) شيوعا](#)
- [صفحة الدعم الفني ل ASA](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن مة و مچم مادخت ساب دن تسمل اذ ه Cisco ت مچرت  
ملاعلاء ان أ عي مچ ي ف ن ي م دخت سمل ل معد ي و تح م مي دقت ل ي رش ب ل و  
امك ة ق ي قد ن و ك ت ن ل ة ل آل ة مچرت ل ض ف أن ة ظ حال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب  
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه  
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco  
Systems ( ر ف و ت م ط ب ا ر ل ا ) ي ل ص أ ل ا ي ز ي ل ج ن إ ل ا دن تسمل ا