

FireSIGHT ةمظنأل ةيلوالا نيوكتلا تاوطخ

المحتويات

[المقدمة](#)

[المتطلبات الأساسية](#)

[التكوين](#)

[الخطوة 1: الإعداد الأولي](#)

[الخطوة 2: تثبيت التراخيص](#)

[الخطوة 3: تطبيق سياسة النظام](#)

[الخطوة 4: تطبيق السياسة الصحية](#)

[الخطوة 5: تسجيل الأجهزة المدارة](#)

[الخطوة 6: تمكين التراخيص المثبتة](#)

[الخطوة 7: تكوين واجهات الاستشعار](#)

[الخطوة 8: تكوين سياسة التسلل](#)

[الخطوة 9: تكوين سياسة التحكم في الوصول وتطبيقها](#)

[الخطوة 10: التحقق مما إذا كان FireSIGHT Management Center يستقبل الأحداث](#)

[توصية إضافية](#)

المقدمة

بعد إعادة تكوين مركز إدارة FireSIGHT أو جهاز FirePOWER، تحتاج إلى إكمال عدة خطوات لجعل النظام يعمل بشكل كامل ولإنشاء تبيهاات لأحداث التسلل، مثل تثبيت التراخيص وتسجيل الأجهزة وتطبيق سياسة الصحة وسياسة النظام وسياسة التحكم في الوصول وسياسة التسلل، وما إلى ذلك. هذا المستند هو ملحق لدليل تثبيت نظام FireSIGHT.

المتطلبات الأساسية

يفترض هذا الدليل أنك قرأت بعناية دليل تثبيت نظام FireSIGHT.

التكوين

الخطوة 1: الإعداد الأولي

في مركز إدارة FireSIGHT الخاص بك، يجب عليك إكمال عملية الإعداد من خلال تسجيل الدخول إلى واجهة الويب وتحديد خيارات التكوين الأولية على صفحة الإعداد الموضحة أدناه. في هذه الصفحة، يجب عليك تغيير كلمة مرور المسؤول، كما يمكنك تحديد إعدادات الشبكة مثل خوادم Domain و DNS، وتكوين الوقت.

Change Password

Use these fields to change the password for the admin account. Sourcefire recommends that you use a password that has at least eight alphanumeric characters of mixed case and includes at least one numeric character. Avoid using words that appear in a dictionary.

New Password	<input type="password"/>
Confirm	<input type="password"/>

Network Settings

Use these fields to specify network-related information for the management interface on the appliance.

Protocol	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 <input type="radio"/> Both
IPv4 Management IP	<input type="text"/>
Netmask	<input type="text"/>
IPv4 Default Network Gateway	<input type="text"/>
Hostname	<input type="text"/>
Domain	<input type="text"/>
Primary DNS Server	<input type="text"/>
Secondary DNS Server	<input type="text"/>
Tertiary DNS Server	<input type="text"/>

Time Settings

Use these fields to specify how you want to set the time for the Defense Center.

Set My Clock	<input checked="" type="radio"/> Via NTP from <input type="text"/>
	<input type="radio"/> Manually <input type="text" value="2013"/> / <input type="text" value="July"/> / <input type="text" value="19"/> : <input type="text" value="9"/> : <input type="text" value="25"/>
Current Time	2013-07-19 09:25
Set Time Zone	America/New York

يمكنك بشكل إختياري تكوين تحديثات القواعد المتكررة والموقع الجغرافي بالإضافة إلى النسخ الاحتياطية التلقائية. يمكن أيضا تثبيت أي تراخيص ميزات عند هذه النقطة.

Recurring Rule Update Imports

Use these fields to schedule recurring rule updates.

- Install Now
- Enable Recurring Rule Update Imports

Recurring Geolocation Updates

Use these fields to schedule recurring weekly geolocation updates. Note that updates may be large and can take up to 45 minutes.

- Install Now
- Enable Recurring Weekly Updates

Automatic Backups

Use this field to schedule automatic configuration backups.

- Enable Automatic Backups

License Settings

To obtain your license, navigate to _____ where you will be prompted for the license key _____ and the activation key, which was emailed to the contact person on your support contract. Follow the on-screen instructions to generate a license, which will be emailed to you. Paste the license below and click Add/Verify. If your browser cannot access the Internet, switch to a host that can.

License Key

Add/Verify

Type	Description	Expires
------	-------------	---------

في هذه الصفحة، يمكنك أيضا تسجيل جهاز إلى مركز إدارة FireSIGHT وتحديد وضع اكتشاف. يحدد وضع الكشف والخيارات الأخرى التي تختارها أثناء التسجيل الواجهات الافتراضية والمجموعات المضمنة والمناطق التي ينشئها النظام، بالإضافة إلى النهج التي يطبقها في البداية على الأجهزة التي تتم إدارتها.

Device Registration

Use this section to add, license, and apply initial access control policies to pre-registered devices. Note that you do not need to add devices to the secondary Defense Center in a high availability pair. If you enable the Apply Default Access Control Policies option, the applied policy for each device depends on the detection mode (Inline, Passive, Access Control, or Network Discovery) you configured for the device.

Click Add to add each device.

Apply Default Access Control Policies

Hostname/IP Address	Registration Key	Protection	Control	URL Filtering	Malware	VPN	
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	Add				

End User License Agreement

IF YOU DO NOT AGREE TO ALL OF THE TERMS AND CONDITIONS CONTAINED IN THIS AGREEMENT, THEN SOURCEFIRE IS UNWILLING TO LICENSE THE LICENSED MATERIALS TO YOU, IN WHICH CASE YOU MAY NOT DOWNLOAD, INSTALL OR USE ANY OF THE LICENSED MATERIALS.

IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT DO NOT INITIATE USE OF THE PRODUCT. BY SELECTING "I ACCEPT," "OK," "CONTINUE," "YES," "NEXT" OR BY INSTALLING OR USING THE LICENSED MATERIALS IN ANY WAY, YOU ARE INDICATING YOUR COMPLETE UNDERSTANDING AND ACCEPTANCE OF THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT INSTALL OR USE THE PRODUCT.

If You are located outside of the United States, then Sourcefire International GmbH, a subsidiary located in Switzerland, shall be a party to this Agreement with You and the party licensing the Licensed Materials to You hereunder. This Agreement governs Your access and use of the Sourcefire Products, except to the extent there is a separate written agreement signed by both You and Sourcefire that expressly states that it governs Your use of the Sourcefire Products. In the event of a conflict between the provisions of such a written agreement and this Agreement, the order of precedence shall be (1) the separate signed agreement, and (2) this Agreement.

1. DEFINITIONS

The following capitalized terms shall have the following meanings in this EULA:

1.1. "Appliance" means any Sourcefire-branded network security appliance made available to You, consisting of Hardware and pre-installed Sourcefire Software and/or

I have read and agree to the END USER LICENSE AGREEMENT

الخطوة 2: تثبيت التراخيص

إذا لم تقم بتثبيت التراخيص أثناء صفحة الإعداد الأولي، فيمكنك إكمال المهمة باتباع الخطوات التالية:

- انتقل إلى الصفحة التالية: النظام < التراخيص.
- انقر على إضافة ترخيص جديد.

Add Feature License

License Key

License

Get License

Verify License

Submit License

If your web browser cannot access the Internet, you must switch to a host with Internet access and navigate to

Using the license key, follow the on-screen instructions to generate a license.

Return to License Page

إذا لم تكن قد حصلت على ترخيص، فاتصل بمندوب المبيعات في حسابك.

الخطوة 3: تطبيق سياسة النظام

يحدد نهج النظام تكوين ملفات تعريف المصادقة ومزامنة الوقت بين FireSIGHT Management Center والأجهزة المدارة. لتكوين سياسة النظام أو تطبيقها، انتقل إلى النظام < محلي > نهج النظام. يتم توفير نهج افتراضي للنظام ولكن يجب تطبيقه على أي أجهزة مدارة.

الخطوة 4: تطبيق السياسة الصحية

يتم استخدام "نهج الحماية" لتكوين كيفية قيام الأجهزة المدارة بالإبلاغ عن حالتها الصحية إلى "مركز إدارة FireSIGHT". لتكوين النهج الصحي أو تطبيقه، انتقل إلى الصحة < النهج الصحي >. يتم توفير نهج صحة افتراضي ولكن يجب تطبيقه على أي أجهزة مدارة.

الخطوة 5: تسجيل الأجهزة المدارة

إذا لم تقم بتسجيل الأجهزة أثناء صفحة الإعداد الأولية، فقم بقراءة [هذا المستند](#) للحصول على تعليمات حول كيفية

الخطوة 6: تمكين التراخيص المثبتة

قبل أن تتمكن من استخدام أي ترخيص ميزة على الجهاز الخاص بك، يلزمك تمكينه لكل جهاز تتم إدارته.

1. انتقل إلى الصفحة التالية: **إدارة الأجهزة**.
2. انقر فوق الجهاز الذي تريد تمكين التراخيص له وإدخال علامة التبويب "الجهاز".
3. انقر فوق أيقونة تحرير (قلم رصاص) الموجودة بجوار الترخيص.

License



Protection:	Yes
Control:	Yes
Malware:	Yes
URL Filtering:	Yes
VPN	Yes

قم بتمكين التراخيص المطلوبة لهذا الجهاز وانقر فوق حفظ.

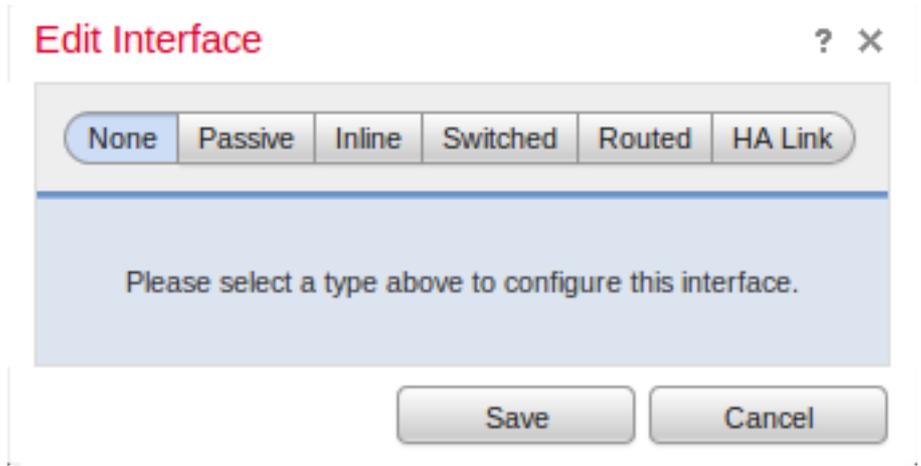
لاحظ الرسالة لديك تغييرات غير مطبقة " في الركن الأيمن العلوي. يبقى هذا التحذير نشطا حتى إذا قمت بالتنقل بعيدا عن صفحة إدارة الأجهزة حتى تقوم بالنقر فوق الزر تطبيق التغييرات.

Health System Help admin

You have unapplied changes Apply Changes

الخطوة 7: تكوين واجهات الاستشعار

1. انتقل إلى أجهزة الصفحة التالية < إدارة الأجهزة.
2. انقر أيقونة تحرير (القلم الرصاص) للمستشعر الذي تختاره.
3. تحت علامة التبويب الواجهات، انقر فوق أيقونة تحرير للواجهة التي تختارها.



حدد تكوين واجهة خاملة أو مضمنة. الواجهات المحولة والموجهة خارج نطاق هذه المقالة.

الخطوة 8: تكوين سياسة التسلل

- انتقل إلى الصفحة التالية: السياسات < الاقتحام < سياسة الاقتحام.
- انقر على إنشاء سياسة ويتم عرض الشاشة التالية:

يجب تعيين اسم وتحديد النهج الأساسي المراد استخدامه. على حسب عملية النشر الخاصة بك، يمكنك اختيار خيار الإسقاط عند تمكين الخط الداخلي. قم بتعريف الشبكات التي تريد حمايتها لتقليل الإيجابيات الخاطئة وتحسين أداء النظام.

سيؤدي النقر فوق إنشاء نهج إلى حفظ الإعدادات وإنشاء نهج IPS. إذا كنت ترغب في إجراء أي تعديل على نهج التطفل، يمكنك اختيار إنشاء نهج وتحديثه بدلا من ذلك.

ملاحظة: يتم تطبيق سياسات التسلل كجزء من سياسة التحكم بالوصول. بعد تطبيق سياسة التطفل، يمكن

تطبيق أي تعديلات دون إعادة تطبيق سياسة التحكم بالوصول بالكامل عن طريق النقر فوق الزر إعادة التطبيق.

الخطوة 9: تكوين سياسة التحكم في الوصول وتطبيقها

1. انتقل إلى السياسات < التحكم في الوصول.

2. انقر فوق نهج جديد.

New Access Control Policy ? X

Name:

Description:

Default Action: Block all traffic Intrusion Prevention Network Discovery

Targeted Devices

Available Devices

Search

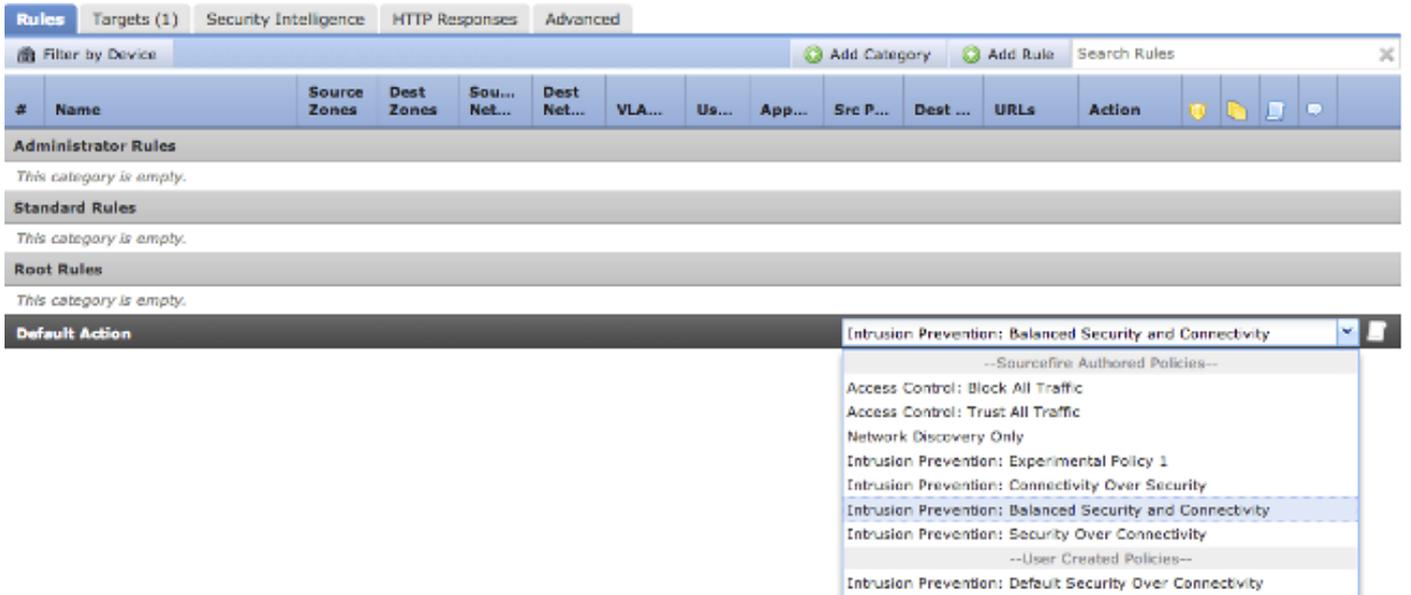
Selected Devices

3. قم بتوفير اسم للنهج والوصف.

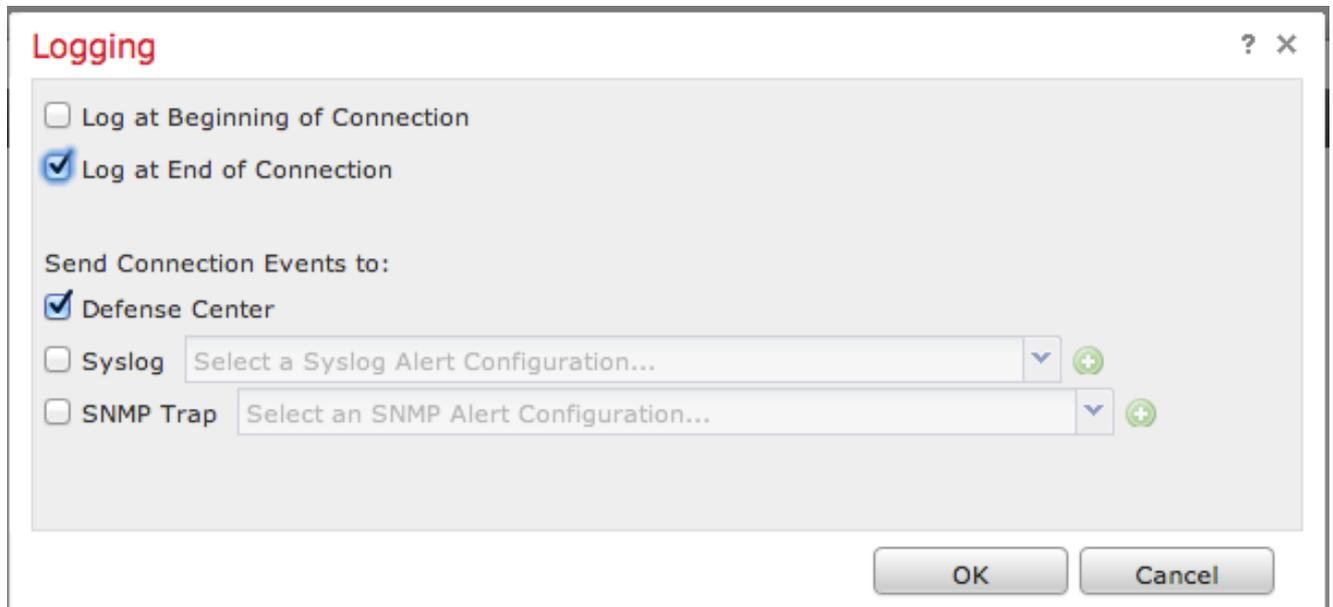
4. حدد منع التسلسل على أنه الإجراء الافتراضي لسياسة التحكم بالوصول.

5. حدد أخيرا الأجهزة المستهدفة التي تريد تطبيق نهج التحكم في الوصول عليها، وانقر فوق حفظ.

6. حدد سياسة التطفل الخاصة بك للإجراء الافتراضي.



7. يجب تمكين تسجيل الاتصال لإنشاء أحداث الاتصال. انقر فوق القائمة المنسدلة التي تقع على يمين الإجراء الافتراضي.



8. أختار تسجيل الاتصالات في بداية الاتصال أو نهايته. يمكن تسجيل الأحداث على FireSIGHT Management Center، أو موقع syslog، أو من خلال SNMP.

ملاحظة: لا يوصى بتسجيل الدخول في طرفي الاتصال لأن كل اتصال (باستثناء الاتصالات المحظورة) سيتم تسجيله مرتين. التسجيل في البداية مفيد للاتصالات التي سيتم حظرها، والتسجيل في النهاية مفيد لجميع الاتصالات الأخرى.

9. انقر فوق OK. لاحظ أن لون أيقونة التسجيل قد تغير.

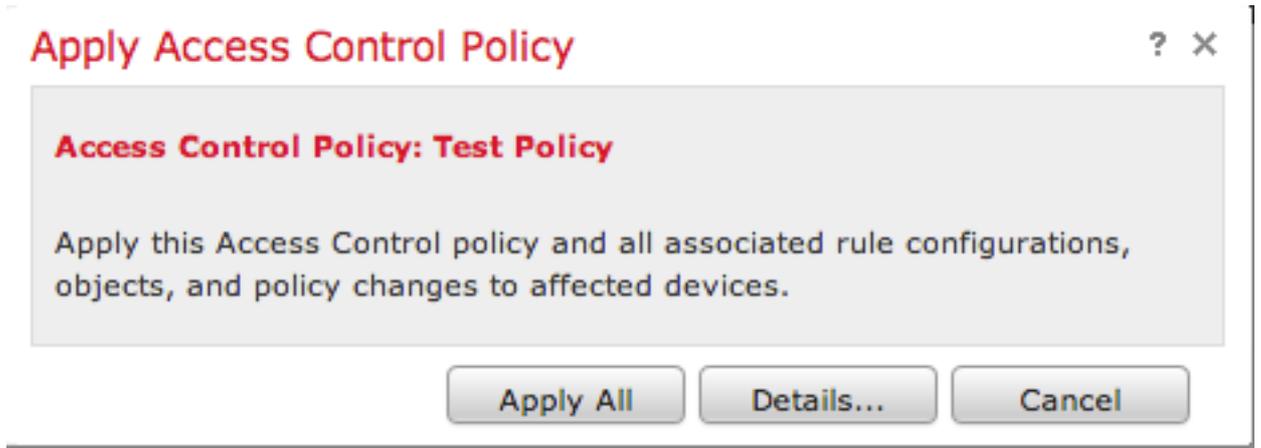
10. يمكنك إضافة قاعدة التحكم بالوصول في الوقت الحالي. تعتمد الخيارات التي يمكنك استخدامها على نوع التراخيص التي قمت بتثبيتها.

11. عند الانتهاء من إجراء التغييرات. انقر فوق الزر **حفظ وتطبيق**. ستلاحظ رسالة تشير إلى أن لديك تغييرات غير محفوظة في النهج الخاص بك في الزاوية العلوية اليمنى حتى يتم النقر فوق الزر.

You have unsaved changes



يمكنك إختيار **حفظ** التغييرات فقط أو النقر فوق **حفظ وتطبيق**. تظهر النافذة التالية إذا أخترت الأخيرة.



12. سيقوم **تطبيق الكل** بتطبيق سياسة التحكم في الوصول وأي سياسة (سياسات) إفتحام مرتبطة على الأجهزة المستهدفة.

ملاحظة: في حالة تطبيق سياسة التطفل لأول مرة، لا يمكن إلغاء تحديدها.

13. يمكنك مراقبة حالة المهمة التي تنقر فوق إرتباط **حالة المهمة** في الإعلام الموضح في أعلى الصفحة، أو بالانتقال إلى: **نظام < مراقبة > حالة المهمة**



14. انقر فوق الارتباط "حالة المهمة" لمراقبة تقدم تطبيق نهج التحكم بالوصول.

Job Summary

[Remove Completed Jobs](#)[Remove Failed Jobs](#)

Running	0
Waiting	0
Completed	7
Retrying	0
Failed	0

Jobs

Task Description	Message	Creation Time	Last Change	Status	
Health Policy apply tasks 0 Running 0 Waiting 1 Completed 0 Retrying 0 Failed					
Health policy apply to appliance Health Policy Apply	Health Policy applied successfully	2013-07-19 18:25:39	2013-07-19 18:26:42	Completed	
Policy apply tasks 0 Running 0 Waiting 3 Completed 0 Retrying 0 Failed					
Apply Default Access Control to Access Control Policy	Access Control Policy applied successfully	2013-07-19 18:26:04	2013-07-19 18:27:12	Completed	

الخطوة 10: التحقق مما إذا كان FireSIGHT Management Center يستقبل الأحداث

بعد اكتمال تطبيق سياسة التحكم بالوصول، يجب أن تبدأ في رؤية أحداث الاتصالات وتبعاً لأحداث أختراق حركة المرور.

توصية إضافية

يمكنك أيضاً تكوين الميزات الإضافية التالية على النظام الخاص بك. يرجى الرجوع إلى دليل المستخدم للحصول على تفاصيل التنفيذ.

- النسخ الاحتياطية المجدولة
- التنزيل/التثبيتات التلقائية للبرامج و SRU و VDB و GeoLocation.
- مصادقة خارجية من خلال LDAP أو RADIUS

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسمل اذ ه Cisco ت مچرت
ملاعلاء ن أ عي مچ ي ف ن ي م دخت سمل ل معد ي و تح م مي دقت ل ة يرش ب ل و
امك ة ق ي قد ن و ك ت ن ل ة ي ل أ ة مچرت ل ض ف أ ن أ 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 (رف و ت م ط بار ل ا) ي ل ص أ ل ا ي ز ي ل ج ن ا ل ا دن تسمل ا