تكوين الكشف عن التهديدات للوصول عن بعد إلى خدمات VPN على الدفاع الآمن عن التهديد باستخدام جدار الحماية

المحتويات

المقدمة

يصف هذا المستند عملية تكوين اكتشاف التهديد للوصول عن بعد إلى خدمات VPN على الدفاع ضد تهديد جدار الحماية الآمن (FTD) من Cisco.

المتطلبات الأساسية

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- الدفاع الآمن عن تهديد جدار الحماية (FTD) من Cisco.
- مركز إدارة جدار الحماية الآمن (FMC) من Cisco.
- شبكة VPN للوصول عن بعد (RAVPN) على FTD.

المتطلبات

يتم دعم ميزات اكتشاف التهديدات هذه في إصدارات الدفاع ضد تهديد جدار الحماية الآمن من Cisco المدرجة في القائمة التالية:

- قطار الإصدار 7.0 -> مدعوم في 7.0.6.3

المكونات المستخدمة

أسست المعلومة يصف في هذا وثيقة على هذا جهاز وبرمجية صيغة:

- الإصدار الظاهري للدفاع ضد تهديد جدار الحماية الآمن من Cisco 7.0.6.3.

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 قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

تتيح لك ميزات اكتشاف التهديدات الخاصة بخدمات الشبكة الخاصة الظاهرية (VPN) للوصول عن بعد إمكانية الحماية ضد أي من السيناريوهات التالية:

1. محاولات الاتصال لإلغاء صلاحية خدمات VPN للوصول عن بعد. أي محاولة الاتصال بالخدمات المخصصة للاستخدام الداخلي فقط.
2. هجمات بدء العميل، حيث يقوم المهاجم بتشغيل محاولات الاتصال للوصول عن بعد إلى وحدة الاستقبال والبث الخاصة بشبكة VPN مرات متكررة من مضيف واحد ولكنه لا يكمل هذه المحاولات.
3. محاولات المصادقة الفاشلة المتكررة للوصول عن بعد إلى خدمات VPN (هجمات المسح الضوئي لاسم مستخدم/كلمة المرور بالقوة).

يمكن لهذه الهجمات، حتى عند فشلها في محاولة الوصول، إستهلاك موارد حسابية ومنع المستخدمين الحقيقيين من الاتصال بخدمات VPN للوصول عن بعد.

عند تمكين هذه الخدمات، يتجنب جدار الحماية الآمن المضيف (عنوان IP) الذي يتجاوز الحدود التي تم تكوينها تلقائيا، لمنع مزيد من المحاولات حتى تقوم بإزالة فجوة عنوان IP يدويا.

ملاحظة: يتم تعطيل جميع خدمات اكتشاف التهديدات للوصول عن بعد إلى VPN بشكل افتراضي.

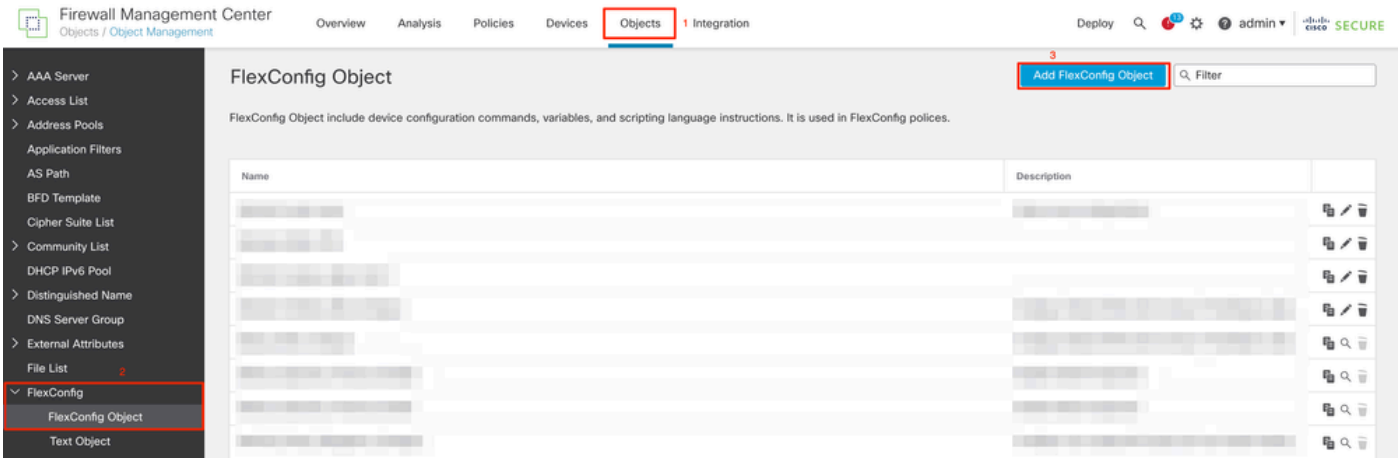
التكوين

ملاحظة: لا يتم دعم تكوين هذه الميزات على "الحماية الآمنة من تهديدات جدار الحماية" حاليا إلا عبر FlexConfig.

---

1. سجل الدخول إلى مركز إدارة جدار الحماية الآمن.

2. لتكوين كائن FlexConfig، انتقل إلى الكائنات > إدارة الكائنات > FlexConfig > FlexConfig Object، ثم انقر فوق إضافة كائن FlexConfig.



3. بمجرد فتح نافذة إضافة كائن FlexConfig، أضف التكوين المطلوب لتمكين ميزات اكتشاف التهديدات الخاصة بشبكة VPN للوصول عن بعد:

- اسم كائن FlexConfig: enable-threat-detection-range
- وصف كائن FlexConfig: تمكين اكتشاف التهديدات لخدمات VPN للوصول عن بعد.
- النشر: مرة واحدة
- الكتابة: إلحاق.
- مربع النص: أضف أوامر "خدمة اكتشاف التهديدات" استنادا إلى الميزات المتاحة الموضحة لاحقا.

ملاحظة: يمكنك تمكين ميزات اكتشاف التهديدات الثلاث المتوفرة لشبكة VPN الخاصة بالوصول عن بعد باستخدام كائن FlexConfig نفسه، أو يمكنك إنشاء كائن FlexConfig واحد بشكل فردي لكل ميزة ليتم تمكينها.

الميزة 1: اكتشاف التهديدات لمحاولات الاتصال بخدمات VPN الداخلية (غير الصالحة) فقط

لتمكين هذه الخدمة، قم بإضافة الأمر invalid-vpn-access لخدمة اكتشاف التهديدات في مربع نص كائن FlexConfig.

الميزة 2: اكتشاف التهديدات لهجمات بدء عميل شبكة VPN للوصول عن بعد

لتمكين هذه الخدمة، أضف أمر خدمة اكتشاف التهديدات من بعد-access-client-initiations <دقيقة>حد <count> في مربع نص كائن FlexConfig، حيث:

- يحدد الإيقاف المؤقت <minutes> الفترة بعد آخر محاولة بدء يتم خلالها حساب محاولات الاتصال المتتالية. إذا كان عدد محاولات الاتصال المتتالية في بالعتبة التي تم تكوينها خلال هذه الفترة، فسيتم تجنب عنوان IPv4 الخاص بالمهاجم. يمكنك تعيين هذه الفترة بين 1 و 1440 دقيقة.
- Threshold <count> هو عدد محاولات الاتصال المطلوبة خلال فترة الانتظار لتشغيل تجنب. يمكنك تعيين الحد الفاصل بين 5 و 100.

على سبيل المثال، إذا كانت فترة التعليق هي 10 دقائق والعتبة هي 20، فسيتم تجنب عنوان IPv4 تلقائيا إذا كانت هناك 20 محاولة توصيل متتالية في أي مدى 10 دقائق.

ملاحظة: عند تعيين قيم التعليق والحد، ضع إستخدام NAT في الاعتبار. إن يستعمل أنت ضرب، أي يسمح كثير طلب من ال نفس عنوان، راعي قيمة أعلى. وهذا يضمن حصول المستخدمين الصحيحين على وقت كاف للاتصال. على سبيل المثال، في الفندق، يمكن للعديد من المستخدمين محاولة الاتصال في فترة قصيرة.

الميزة 3: اكتشاف التهديدات لفشل مصادقة VPN للوصول عن بعد

لتمكين هذه الخدمة، أضف أمر تقييد الوصول عن بعد لخدمة اكتشاف التهديدات<دقيقة>الحد <count>في مربع نص كائن FlexConfig، حيث:

- يحدد الإيقاف المؤقت <minutes> الفترة بعد آخر محاولة فاشلة يتم خلالها حساب حالات الفشل المتتالية. وإذا كان عدد حالات فشل المصادقة المتتالية يستوفي الحد الذي تم تكوينه خلال هذه الفترة، فسيتم تجنب عنوان IPv4 للمهاجم. يمكنك تعيين هذه الفترة بين 1 و 1440 دقيقة.
- Threshold <count> هو عدد محاولات المصادقة الفاشلة المطلوبة خلال فترة الانتظار لتشغيل تجنب. يمكنك تعيين الحد الفاصل بين 1 و 100.

على سبيل المثال، إذا كانت فترة التعليق هي 10 دقائق والعتبة هي 20، فسيتم تجنب عنوان IPv4 تلقائيا إذا كان هناك 20 فشل مصادقة متتابع في أي مدى 10 دقائق.

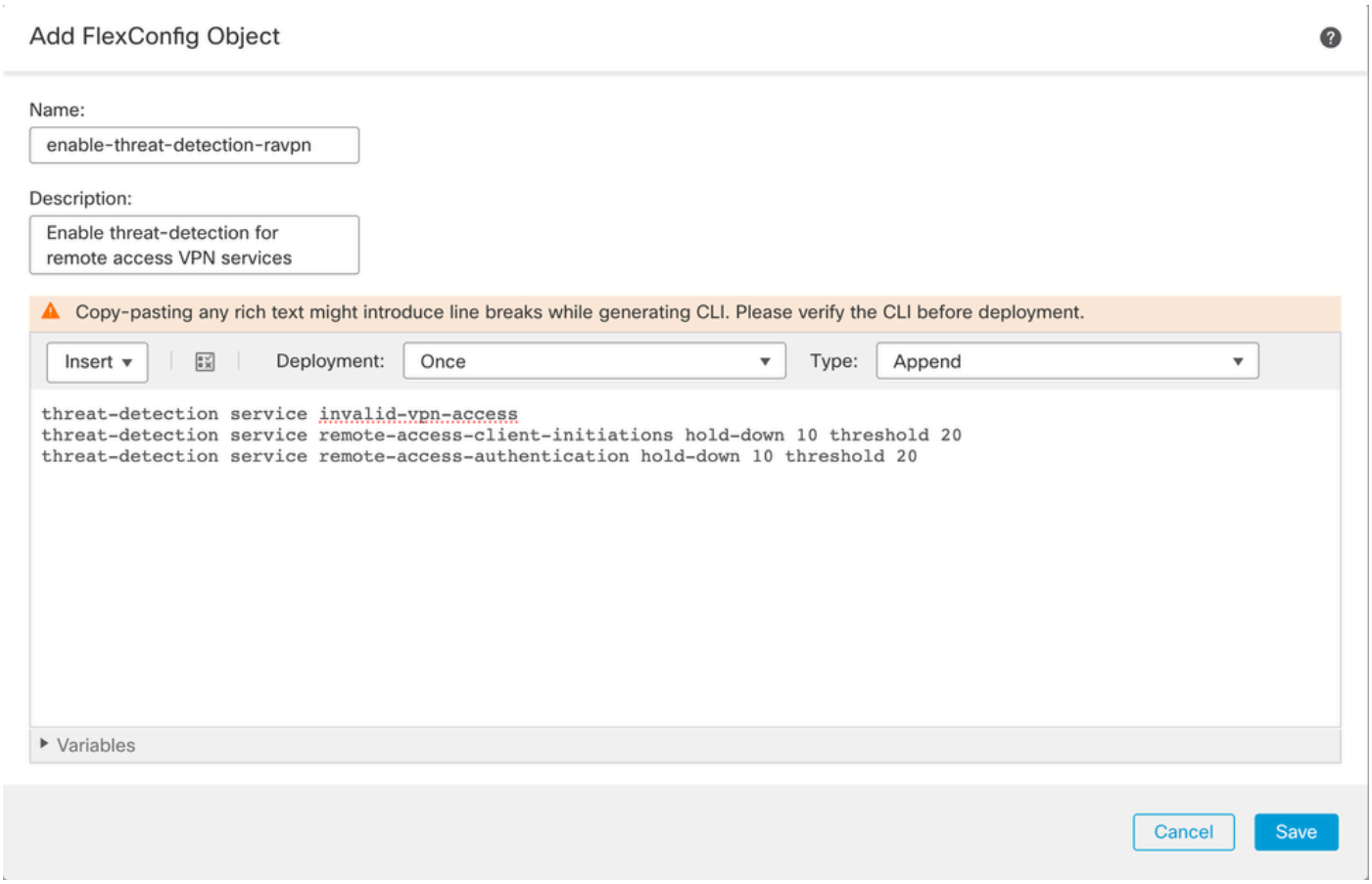
ملاحظة: عند تعيين قيم التعليق والحد، ضع إستخدام NAT في الاعتبار. إن يستعمل أنت ضرب، أي يسمح كثير طلب من ال نفس عنوان، راعي قيمة أعلى. وهذا يضمن حصول المستخدمين الصحيحين على وقت كاف للاتصال. على سبيل المثال، في الفندق، يمكن للعديد من المستخدمين محاولة الاتصال في فترة قصيرة.

ملاحظة: حالات فشل المصادقة عبر SAML غير مدعومة حتى الآن.

ويتيح مثال التكوين التالي خدمات اكتشاف التهديدات الثلاثة المتوفرة لشبكة VPN الخاصة بالوصول عن بعد مع فترة توقف تبلغ 10 دقائق وعتبة تبلغ 20 لبدء العميل ومحاولات المصادقة الفاشلة. قم بتكوين قيم الإيقاف والحد وفقا لمتطلبات البيئة الخاصة بك.

يستخدم هذا المثال كائن FlexConfig واحدا لتمكين الميزات الثلاث المتاحة.

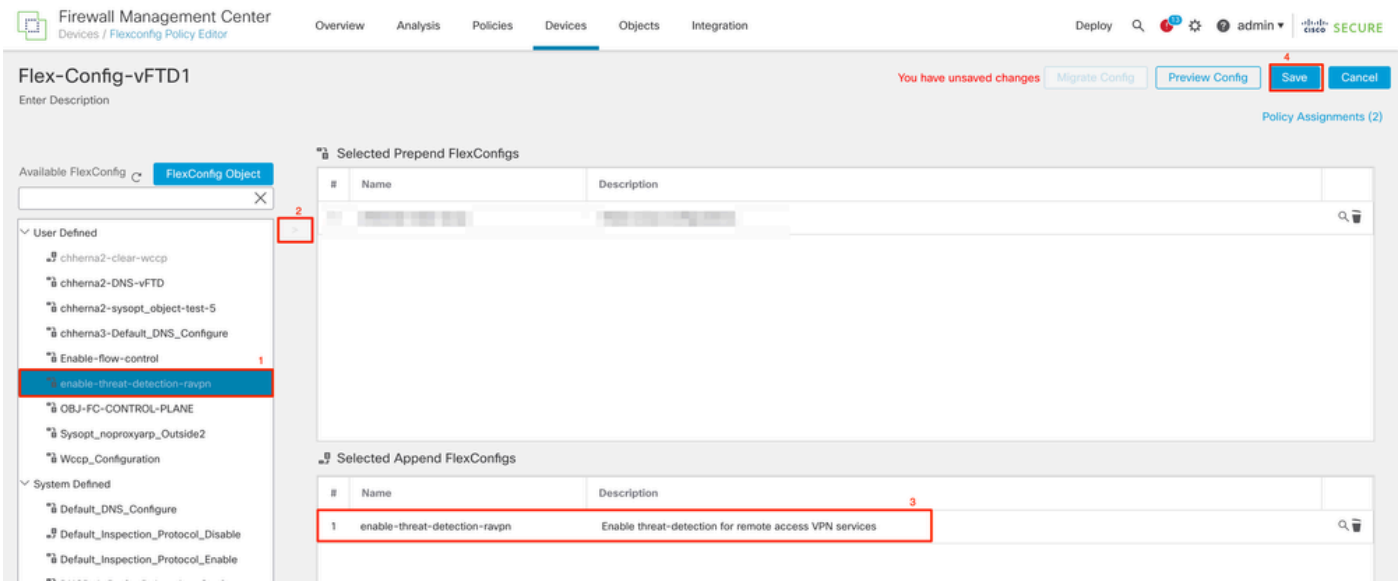
```
threat-detection service invalid-vpn-access
threat-detection service remote-access-client-initiations hold-down 10 threshold 20
threat-detection service remote-access-authentication hold-down 10 threshold 20
```



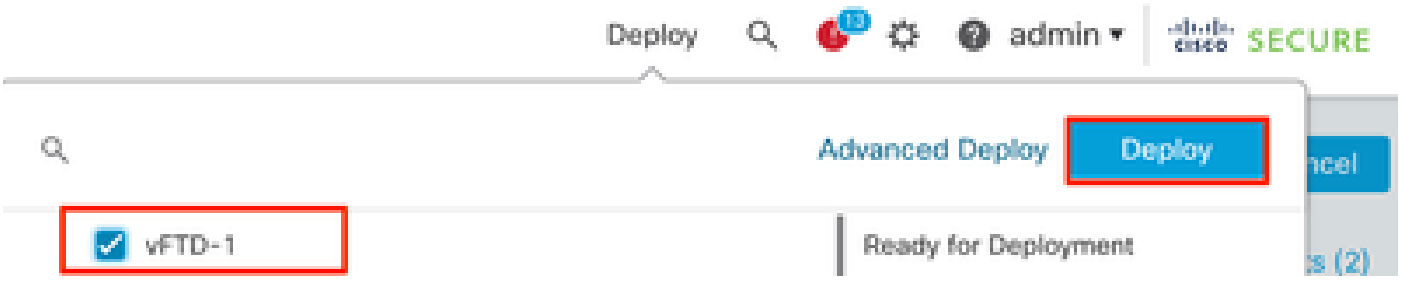
4. احفظ كائن FlexConfig.

5. انتقل إلى الأجهزة > FlexConfig وحدد سياسة FlexConfig المعينة لجدار الحماية الآمن الخاص بك.

6. من كائنات FlexConfig المتاحة المعروضة في الجزء الأيسر، حدد كائن FlexConfig الذي قمت بتكوينه في الخطوة 3، وانقر فوق ">، واحفظ التغييرات.



7. قم بنشر التغييرات والتحقق.



التحقق من الصحة

من أجل عرض إحصائيات لخدمات WAPN الخاصة بكشف التهديدات، قم بتسجيل الدخول إلى CLI الخاص ب FTD وقم بتشغيل الأمر show threat-detection service [service] [entries|details]. حيث يمكن أن تكون الخدمة: مصادقة الوصول عن بعد أو بدء الوصول عن بعد إلى العميل أو الوصول إلى VPN غير صالح.

يمكنك الحد من طريقة العرض عن طريق إضافة هذه المعلمات:

- الإدخالات — عرض الإدخالات التي يتم تعقبها فقط من خلال خدمة كشف التهديدات. على سبيل المثال، عناوين IP التي فشلت محاولات المصادقة.
- التفاصيل — عرض كل من تفاصيل الخدمة وإدخالات الخدمة.

قم بتشغيل الأمر show threat-detection service لعرض إحصائيات جميع خدمات اكتشاف التهديدات التي تم تمكينها.

```
<#root>

ciscoftd# show threat-detection service

Service: invalid-vpn-access State : Enabled

    Hold-down : 1 minutes
    Threshold : 1
    Stats:
        failed      :          0
        blocking    :          0
        recording   :          0
        unsupported :          0
        disabled    :          0
    Total entries: 0

Service: remote-access-authentication State : Enabled

    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          1
        recording   :          4
        unsupported :          0
        disabled    :          0
```

```
    Total entries: 2

Name: remote-access-client-initiations State : Enabled

    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          0
        recording   :          0
        unsupported :          0
        disabled    :          0
    Total entries: 0
```

لعرض مزيد من تفاصيل المهاجمين المحتملين الذين يتم تعقبهم لخدمة مصادقة الوصول عن بعد، قم بتشغيل الأمر show threat-detection service <service> entries.

```
ciscoftd# show threat-detection service remote-access-authentication entries
Service: remote-access-authentication
    Total entries: 2

Idx Source              Interface            Count          Age        Hold-down
--- ------------------- -------------------- -------------- ---------- ---------
  1 192.168.100.101/ 32              outside              1        721         0
  2 192.168.100.102/ 32              outside              2        486       114
Total number of IPv4 entries: 2

NOTE: Age is in seconds since last reported. Hold-down is in seconds remaining.
```

لعرض الإحصاءات العامة والتفاصيل الخاصة بخدمة وصول عن بعد للكشف عن التهديدات المحددة إلى VPN، قم بتشغيل الأمر show threat-detection service <service> details.

```
ciscoftd# show threat-detection service remote-access-authentication details
Service: remote-access-authentication
    State     : Enabled
    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          1
        recording   :          4
        unsupported :          0
        disabled    :          0
     Total entries: 2

Idx Source              Interface            Count          Age        Hold-down
--- ------------------- -------------------- -------------- ---------- ---------
  1 192.168.100.101/ 32              outside              1        721         0
  2 192.168.100.102/ 32              outside              2        486       114
Total number of IPv4 entries: 2

NOTE: Age is in seconds since last reported. Hold-down is in seconds remaining.
```

ملاحظة: تعرض الإدخالات عناوين IP التي تمت تعقبها بواسطة خدمة اكتشاف التهديدات فقط. إذا كان عنوان IP قد استوفى الشروط المطلوب تجنبها، يزداد عدد الحظر والتي تم عرض عنوان IP كإدخال.

وبالإضافة إلى ذلك، أنت يستطيع راقبت رفض يطبق ب VPN خدمة، وأزال رفض لعنوان وحيد أو كل عنوان ال IP مع الأمر التالي:

- [عرض تجاهل [ip_address

يظهر البيئات المضيفة المبعدة، بما في ذلك تلك التي تم تجاهلها تلقائيا بواسطة كشف التهديد لخدمات VPN، أو يدويا باستخدام أمر الإحجام. يمكنك تحديد طريقة العرض إختياريا إلى عنوان IP محدد.

- ال يوجد تجاهل ip_address [interface if_name]

إزالة تجنب عنوان IP المحدد فقط. أنت يستطيع إختياريا عينت القارن إسم ل للعنة، إن العنوان يكون نبذت على أكثر من واحد قارن وأنت تريد أن يترك ال ينشق في مكانه على بعض قارن.

- تجاهل واضح

إزالة التجاوز من جميع عناوين IP وجميع الوجهات.

ملاحظة: ال تظهر عناوين IP التي تم تجنبها بواسطة اكتشاف التهديدات لخدمات VPN في الأمر show threat-detection"، والذي ينطبق على مسح اكتشاف التهديدات فقط.

من أجل قراءة جميع التفاصيل لكل إخراج أمر ورسائل syslog المتاحة المتعلقة بخدمات اكتشاف التهديدات الخاصة ب VPN للوصول عن بعد، الرجاء الرجوع إلى مستند مرجع الأوامر.

معلومات ذات صلة

- للحصول على مساعدة إضافية، يرجى الاتصال بمركز المساعدة التقنية (TAC). يلزم عقد دعم صالح: جهات اتصال الدعم العالمية من Cisco.
- يمكنك أيضا زيارة مجتمع Cisco VPN هنا.
- الدعم الفني والتنزيلات من Cisco

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).