# تصفية قواعد التطفل استناداً إلى إصدار SRU و LSP لأجهزة FirePOWER التي تتم إدارتها بواسطة FMC

## المحتويات



## المقدمة

يوضح هذا المستند كيفية تصفية قواعد الشبكة استناداً إلى إصدار حزمة حالة الارتباط (LSP) من Cisco Secure Rule Update (SRU) ومن أجهزة FirePOWER التي يديرها مركز إدارة FirePOWER (FMC).

## المتطلبات الأساسية

### المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة الشيخ مفتوح المصدر
- مركز إدارة Firepower (FMC)
- Firepower Threat Defense (FTD)

### المكونات المستخدمة

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

- تنطبق هذه المقالة على جميع منصات Firepower
- برنامج الدفاع ضد تهديد FirePOWER (FTD) من Cisco الذي يشغل الإصدار 7.0.0 من البرنامج
- Firepower Management Center Virtual (FMC) الذي يشغل الإصدار 7.0.0 من البرنامج

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

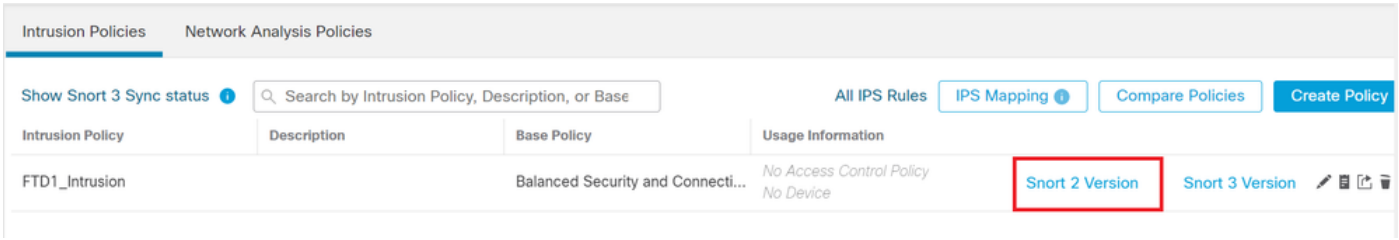
في سياق أنظمة كشف التسلل (IDS) وأنظمة منع التسلل (IPS)، يعني مصطلح "SID" "معرف التوقيع" أو "معرف توقيع الشورت".

معرف توقيع الشورت (SID) هو معرف فريد يتم تعيينه لكل قاعدة أو توقيع ضمن مجموعة القواعد الخاصة به. يتم إستخدام هذه القواعد لاكتشاف الأنماط أو السلوكيات المحددة في حركة مرور الشبكة التي يمكن أن تشير إلى نشاط ضار أو تهديدات أمان. تقترن كل قاعدة بمعرف الأمان (SID) للسماح بسهولة الرجوع والإدارة.

وللحصول على معلومات عن شركة Snort مفتوحة المصدر، يرجى زيارة موقع SNORT على الويب.

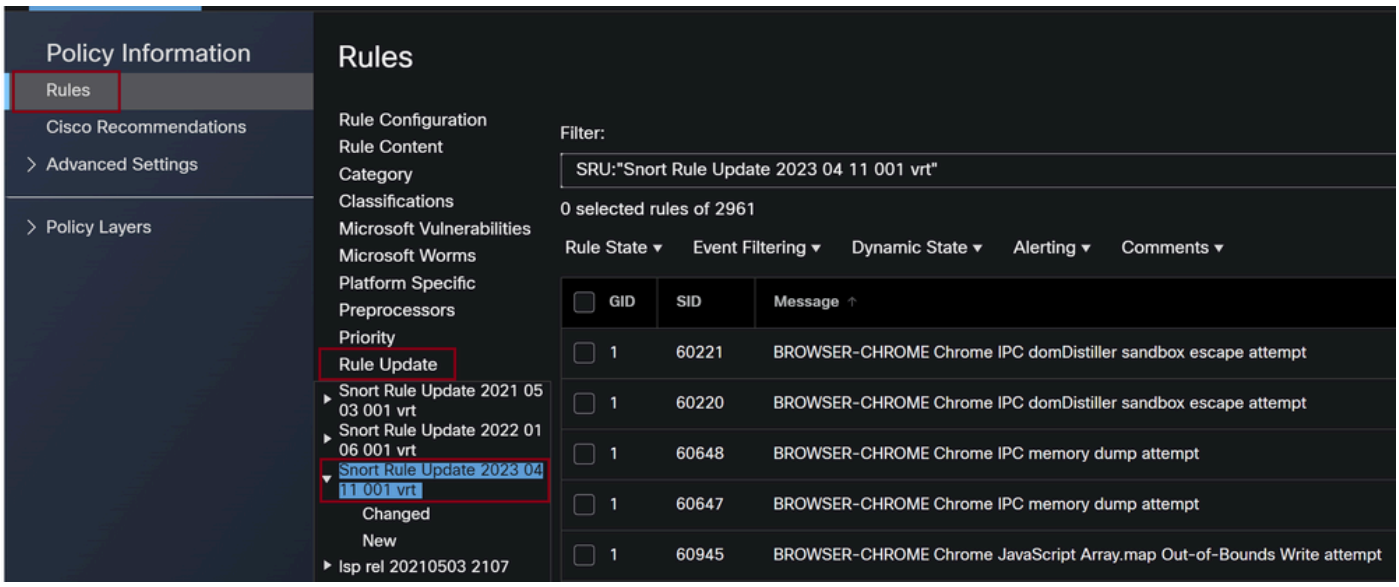
# إجراء تصفية قواعد الشخير

لعرض مجموعات توصيل قاعدة Snort 2، انتقل إلى FMC Policies > Access Control > Intrusion, بعد ذلك انقر خيار snort2 في الزاوية العليا اليمنى، كما هو موضح في الصورة:

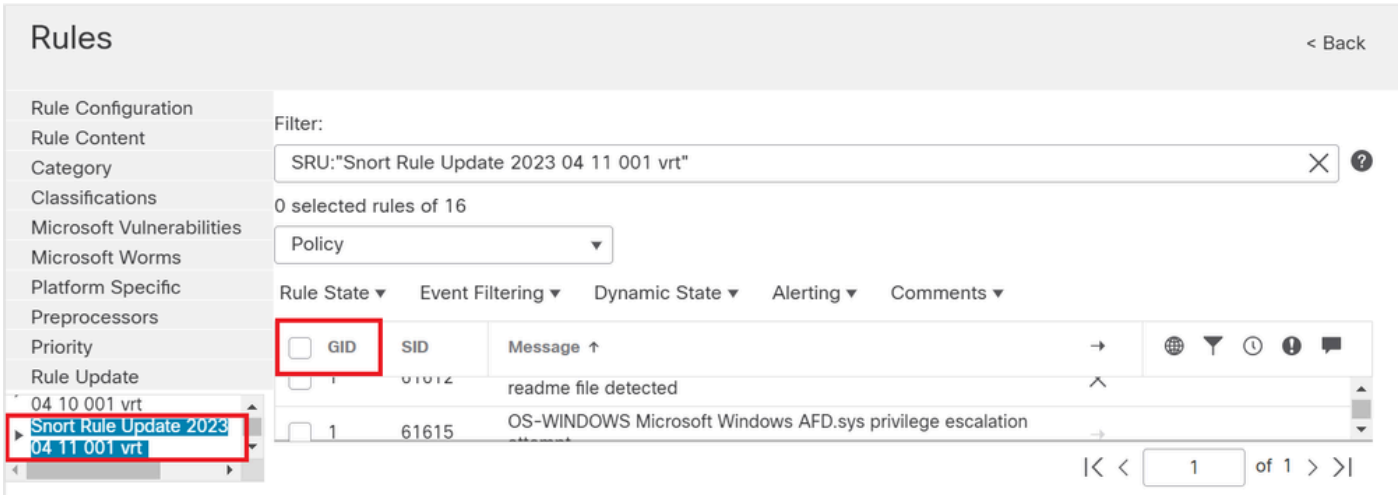



نورت 2

انتقل إلى Rules > Rule Update وحدد آخر تاريخ لتصفية معرف الأمان (SID).

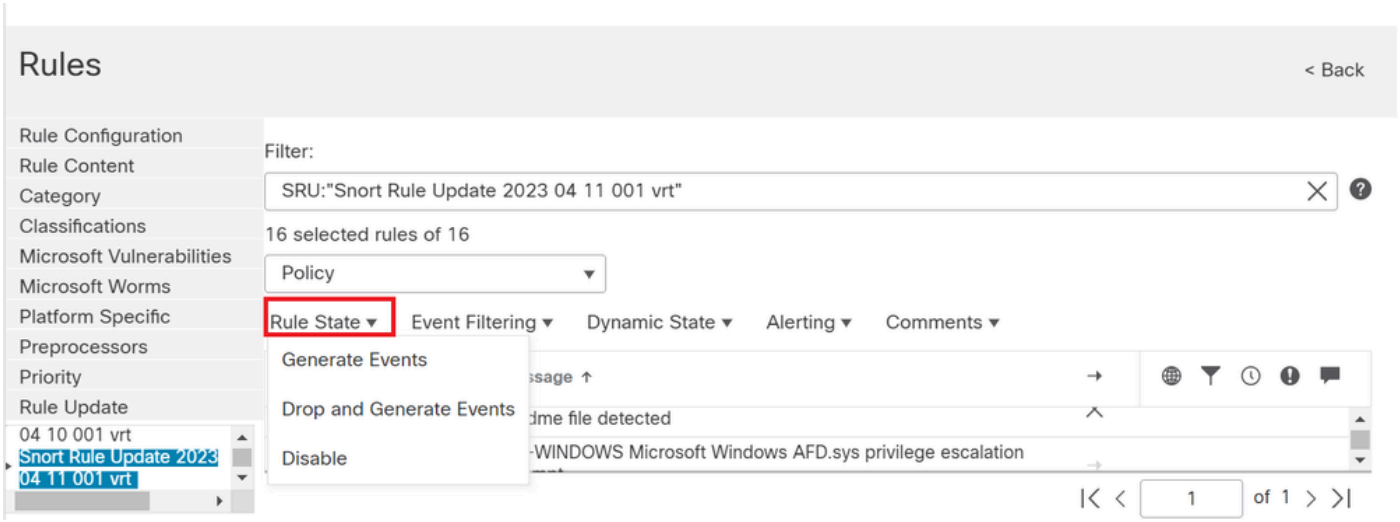



تحديث القاعدة



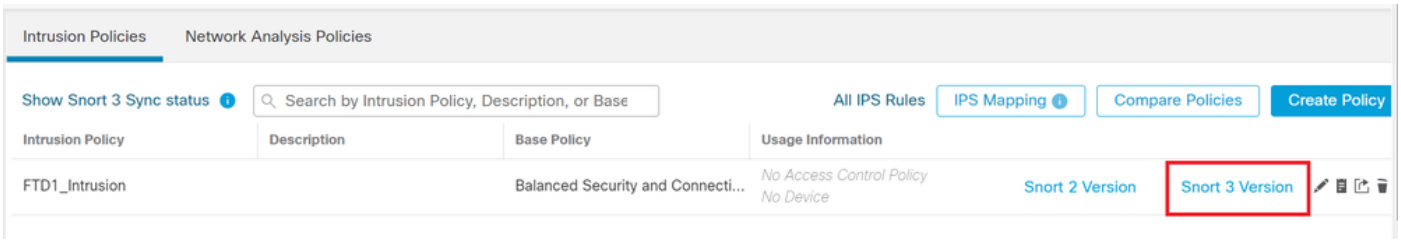

Sid المتاحة تحت قواعد الشخير

تحديد خيار مطلوب تحت Rule State كما هو موضح في الصورة.



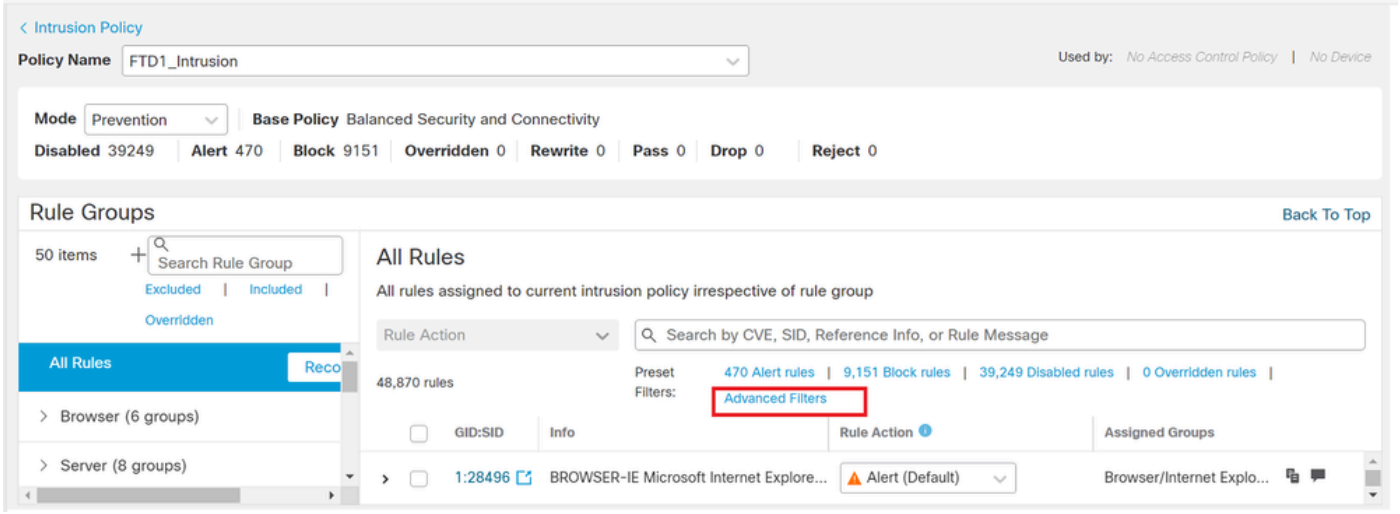

تحديد حالات القاعدة

لعرض مجموعات توصيل قاعدة Snort 3، انتقل إلى FMC Policies > Access Control > Intrusion ، ثم انقر خيار snort3 في الزاوية العليا اليمنى، كما هو موضح في الصورة:

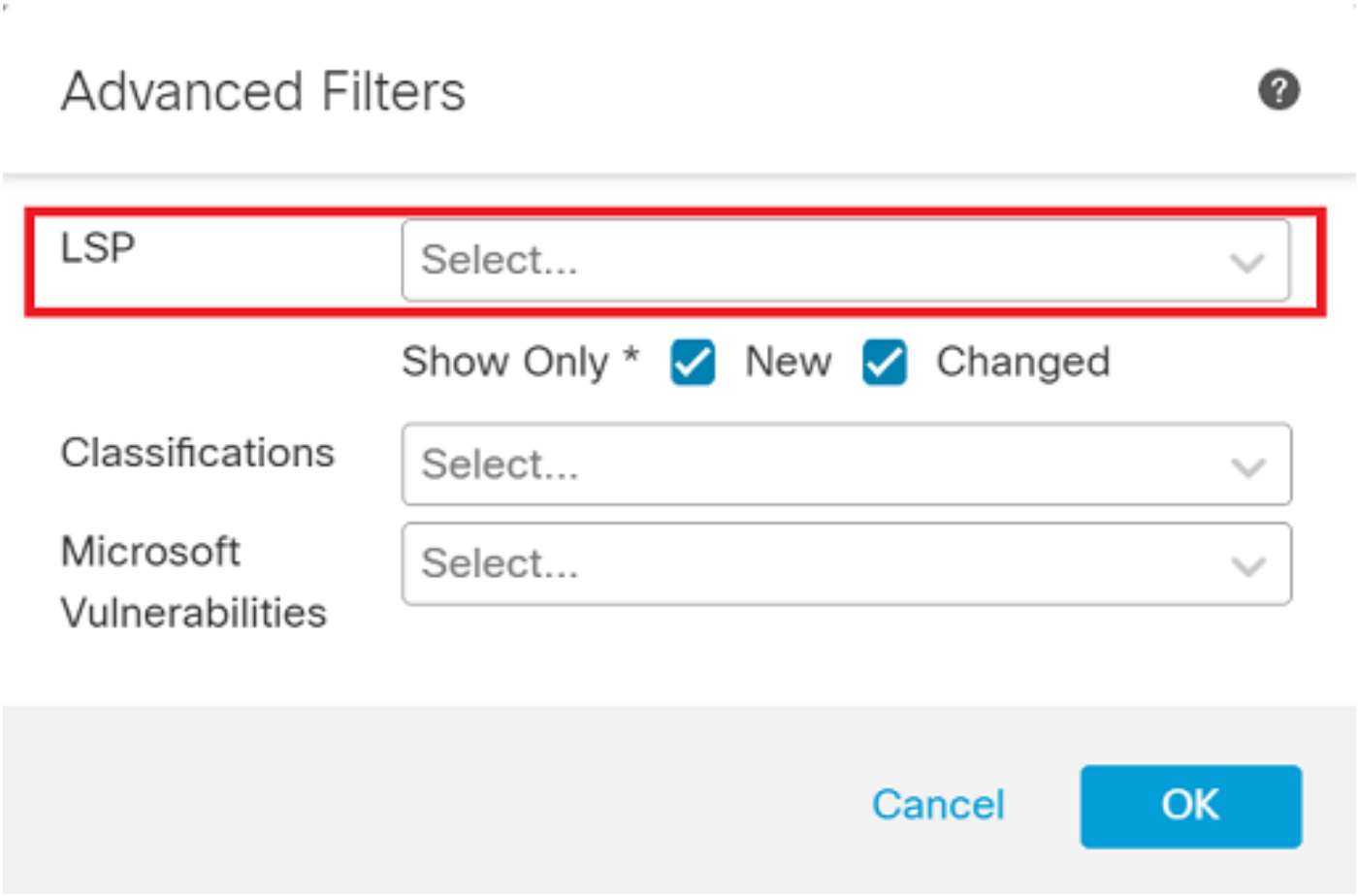



ورت 3

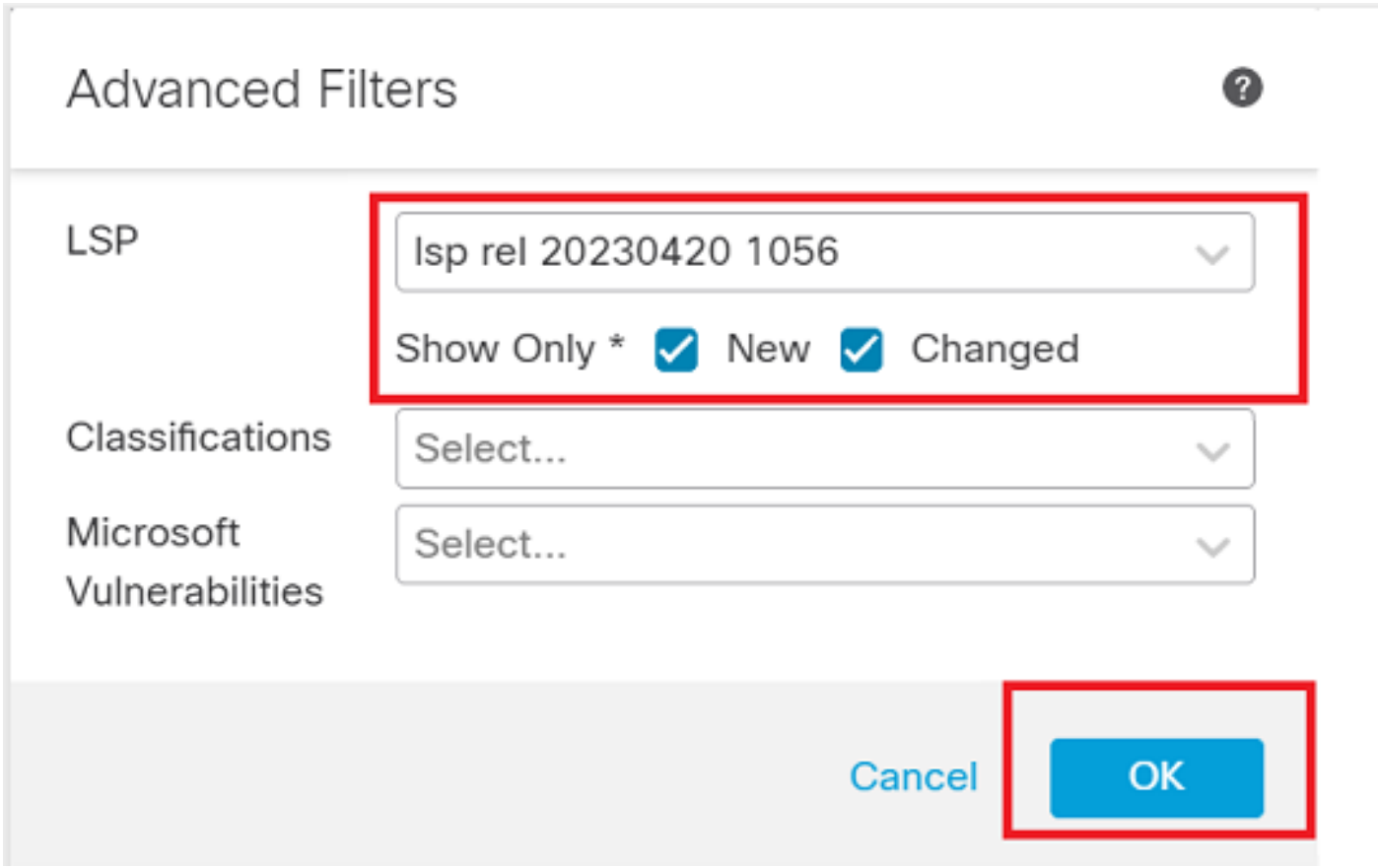
انتقل إلى Advanced Filters وحدد آخر تاريخ لتصفية SID كما هو موضح في الصورة.




عوامل تصفية Snort 3



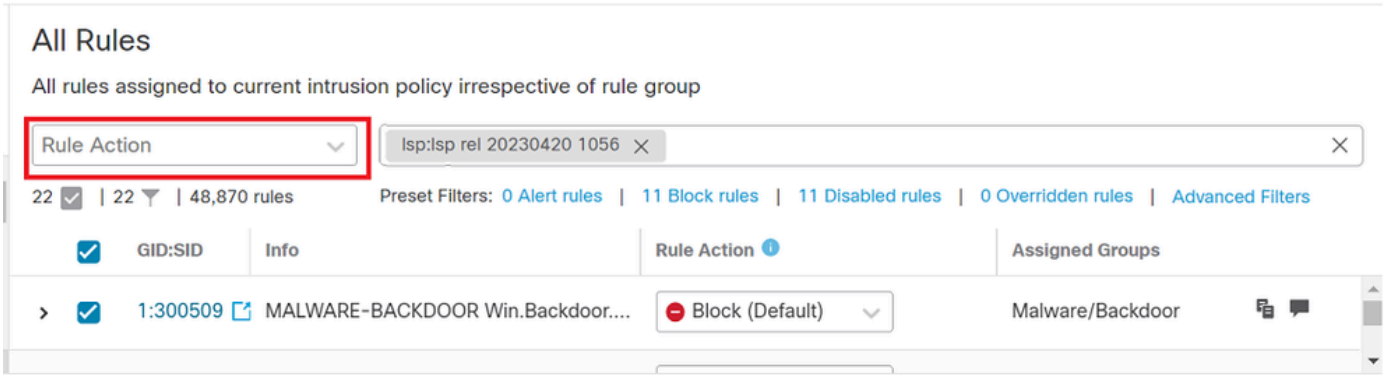

عامل تصفية متقدم تحت LSP




إصدار LSP


عامل تصفية مجموعة مسبقة ل Sid's

تحديد خيار مطلوب تحت Rule state كما هو موضح في الصورة.



إجراء القاعدة

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).