دجوي ال - ةردانصلا ةقداصملا لكيو ةقداصم NAT نيوكت وأ Cisco IOS ةيامح رادج

المحتويات

المقدمة

تسمح ميزة وكيل المصادقة للمستخدمين بتسجيل الدخول إلى الشبكة أو الوصول إلى الإنترنت عبر HTTP، مع إسترداد ملفات تعريف الوصول الخاصة بهم وتطبيقها تلقائيا من خادم RADIUS أو TACACS+. لا تكون ملفات تعريف المستخدم نشطة إلا في حالة وجود حركة مرور نشطة من المستخدمين المصادق عليهم.

يقوم نموذج التكوين هذا بحظر حركة مرور البيانات من الجهاز المضيف (على 40.31.1.47) على الشبكة الداخلية إلى جميع الأجهزة الموجودة على الإنترنت حتى يتم إجراء مصادقة المستعرض باستخدام وكيل المصادقة. تضيف قائمة التحكم في الوصول (ACL) التي تم تمريرها من الخادم (**السماح ب tcp|ip|icmp any**) تفويض ما بعد للإدخالات الديناميكية إلى قائمة الوصول 116 التي تسمح مؤقتا بالوصول من الكمبيوتر المضيف إلى الإنترنت.

ارجع إلى تكوين وكيل المصادقة للحصول على مزيد من المعلومات حول وكيل المصادقة.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- برنامج IOS® الإصدار 12.2(15)T من Cisco

- موجّه Cisco 7206

ملاحظة: تم إدخال الأمر **ip auth-proxy** في برنامج جدار حماية Cisco IOS الإصدار T.12.0.5.

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.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

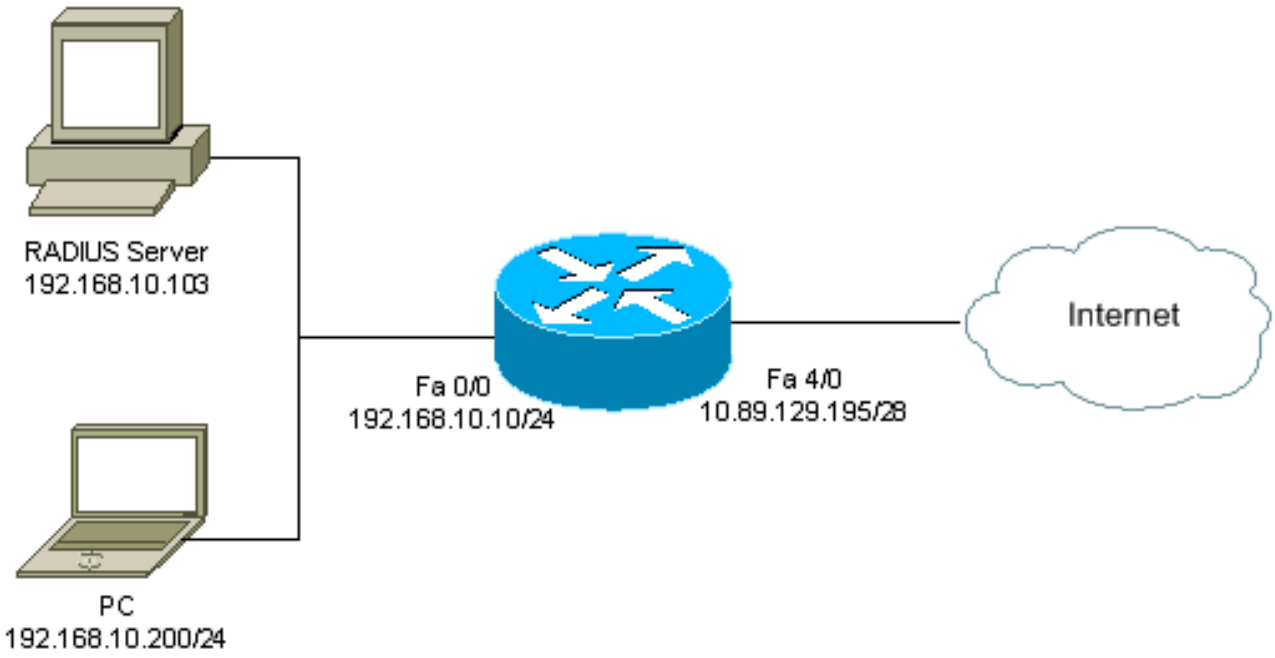
التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للعثور على مزيد من المعلومات حول الأوامر المستخدمة في هذا المستند.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



التكوين

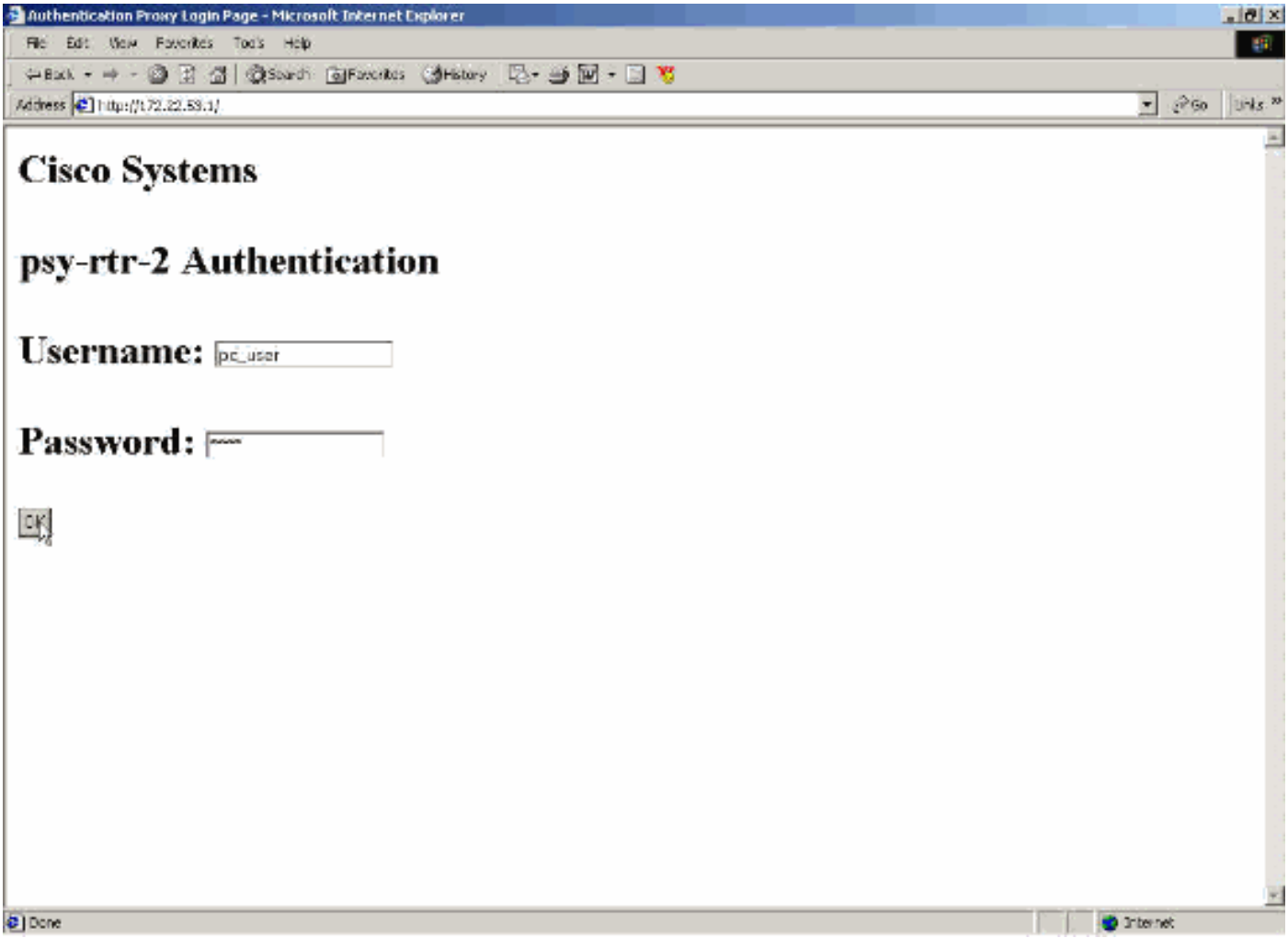
يستعمل هذا وثيقة هذا تشكيل:

الموجه 7206
version 12.2 service timestamps debug datetime msec service timestamps log datetime msec

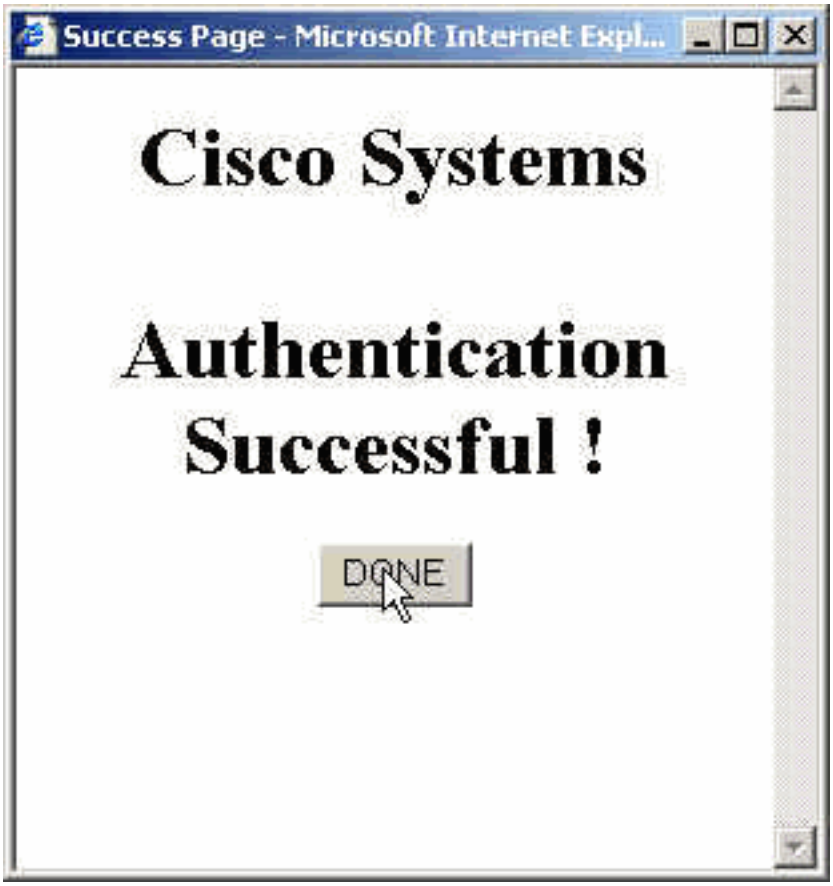
```
service password-encryption
!
hostname psy-rtr-2
!
logging queue-limit 100
!
<username admin password 7 <deleted
aaa new-model

Enable AAA. aaa authentication login default group ---!
  radius none !--- Use RADIUS to authenticate users. aaa
       authorization exec default group radius none aaa
     authorization auth-proxy default group radius !---
       Utilize RADIUS for auth-proxy authorization. aaa
    session-id common ip subnet-zero ! ip cef ! ip auth-
   proxy auth-proxy-banner !--- Displays the name of the
   firewall router !--- in the Authentication Proxy login
     page. ip auth-proxy auth-cache-time 10 !--- Sets the
   global Authentication Proxy idle !--- timeout value in
        minutes. ip auth-proxy name restrict_pc http !---
   Associates connections that initiate HTTP traffic with
     !--- the "restrict_pc" Authentication Proxy name. ip
  audit notify log ip audit po max-events 100 ! no voice
    hpi capture buffer no voice hpi capture destination !
          mta receive maximum-recipients 0 ! ! interface
  FastEthernet0/0 ip address 192.168.10.10 255.255.255.0
ip access-group 116 in !--- Apply access list 116 in the
  inbound direction. ip auth-proxy restrict_pc !--- Apply
       the Authentication Proxy list !--- "restrict_pc"
            configured earlier. duplex full ! interface
FastEthernet4/0 ip address 10.89.129.195 255.255.255.240
  duplex full ! ip classless ip http server !--- Enables
   the HTTP server on the router. !--- The Authentication
  Proxy uses the HTTP server to communicate !--- with the
   client for user authentication. ip http authentication
   aaa !--- Sets the HTTP server authentication method to
    AAA. ! access-list 116 permit tcp host 192.168.10.200
host 192.168.10.10 eq www !--- Permit HTTP traffic (from
     the PC) to the router. access-list 116 deny tcp host
         192.168.10.200 any access-list 116 deny udp host
        192.168.10.200 any access-list 116 deny icmp host
 192.168.10.200 any !--- Deny TCP, UDP, and ICMP traffic
   from the client by default. access-list 116 permit tcp
    192.168.10.0 0.0.0.255 any access-list 116 permit udp
  192.168.10.0 0.0.0.255 any access-list 116 permit icmp
     192.168.10.0 0.0.0.255 any !--- Permit TCP, UDP, and
              ICMP traffic from other !--- devices in the
            192.168.10.0/24 network. ! radius-server host
       192.168.10.103 auth-port 1645 acct-port 1646 key 7
<deleted> !--- Specify the IP address of the RADIUS !---
   server along with the key. radius-server authorization
 permit missing Service-Type call rsvp-sync ! ! line con
    0 stopbits 1 line aux 0 stopbits 1 line vty 0 4 ! end
```

المصادقة على الكمبيوتر الشخصي

يوفر هذا القسم لقطات للشاشة مأخوذة من الكمبيوتر الشخصي الذي يعرض إجراء المصادقة. يظهر الالتقاط الأول الإطار حيث يدخل المستخدم اسم المستخدم وكلمة المرور للمصادقة ويضغط **موافق**.



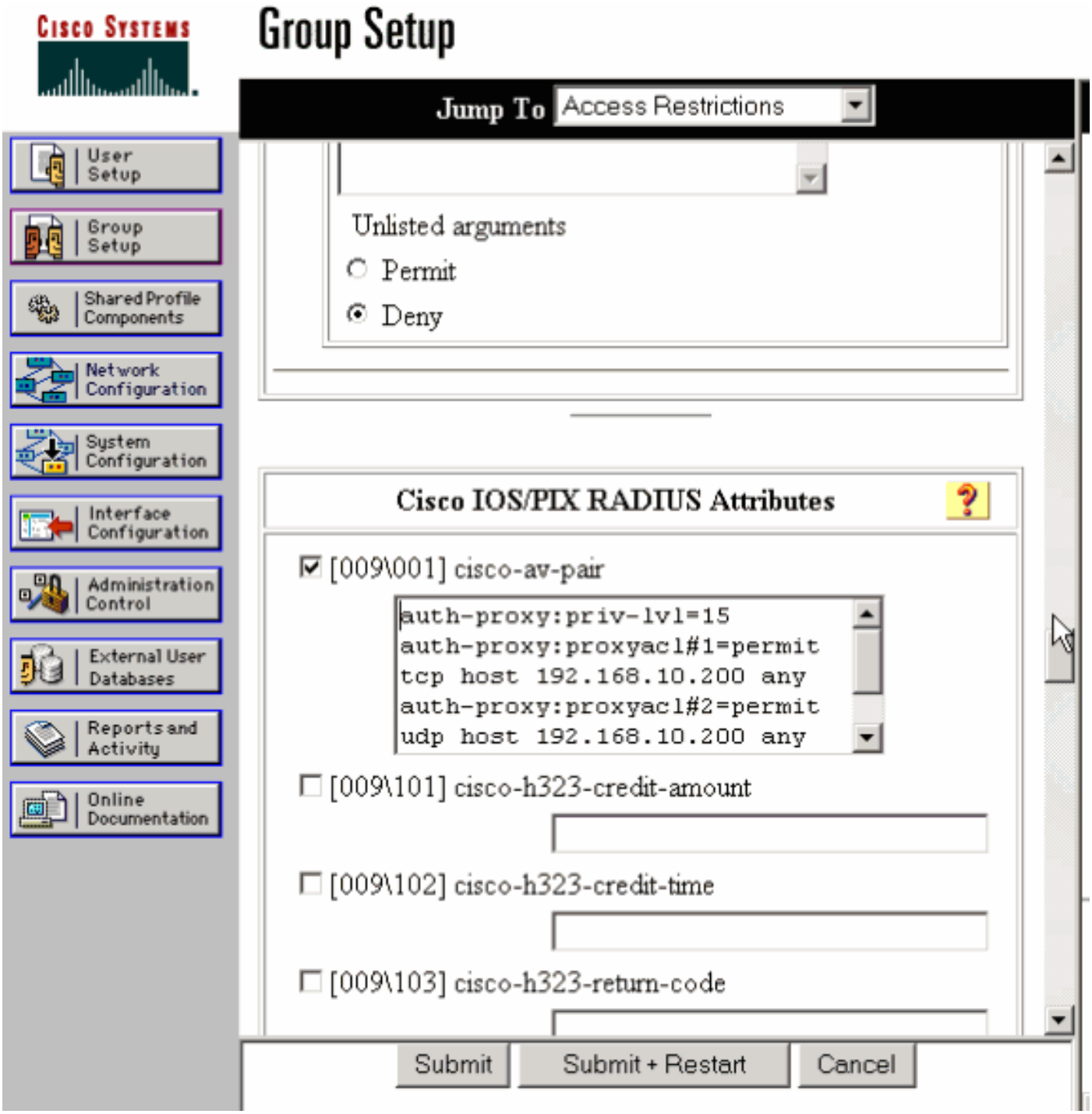
إذا نجحت المصادقة، يظهر هذا الإطار.



يجب تكوين خادم RADIUS باستخدام قوائم التحكم في الوصول (ACL) للوكيل التي يتم تطبيقها. في هذا المثال، يتم تطبيق إدخالات قائمة التحكم في الوصول (ACL) هذه. وهذا يسمح للكمبيوتر بالاتصال بأي جهاز.

```
permit tcp host 192.168.10.200 any
permit udp host 192.168.10.200 any
permit icmp host 192.168.10.200 any
```

تظهر نافذة Cisco ACS هذه مكان إدخال قوائم التحكم في الوصول (ACL) للوكيل.



ملاحظة: ارجع إلى تكوين وكيل المصادقة للحصول على مزيد من المعلومات حول كيفية تكوين خادم RADIUS/TACACS+.

التحقق من الصحة

يوفر هذا القسم معلومات يمكنك إستخدامها للتأكد من أن التكوين يعمل بشكل صحيح.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

- **show ip access lists** — يعرض قوائم التحكم في الوصول (ACL) القياسية والموسعة التي تم تكوينها على جدار الحماية (يتضمن إدخالات قائمة التحكم في الوصول (ACL) الديناميكية). تتم إضافة إدخالات قائمة التحكم في الوصول (ACL) الديناميكية وإزالتها بشكل دوري استنادا إلى ما إذا كان المستخدم يصدق أو لا.
- **show ip auth-proxy cache**—يعرض إما إدخالات وكيل المصادقة أو تكوين وكيل المصادقة الجاري تشغيله. الكلمة الأساسية ذاكرة التخزين المؤقت لسرد عنوان IP للمضيف، ورقم منفذ المصدر، وقيمة المهلة لوكيل المصادقة، وحالة الاتصالات التي تستخدم وكيل المصادقة. إذا كانت حالة وكيل المصادقة HTTP_ESTAB، تكون مصادقة المستخدم ناجحة.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

بالنسبة لهذه الأوامر، ارجع إلى وكيل مصادقة أستكشاف الأخطاء وإصلاحها، إلى جانب معلومات أستكشاف الأخطاء وإصلاحها الأخرى.

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر **debug**.

معلومات ذات صلة

- صفحة دعم جدار حماية IOS
- صفحة دعم TACACS/TACACS+
- TACACS+ في وثائق IOS
- صفحة دعم RADIUS
- وثائق RADIUS في IOS
- طلبات التعليقات (RFCs)
- الدعم التقني والمستندات - Cisco Systems

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).