إعادة توجيه حركة مرور ISE على المحول Catalyst 3750 Series Switch

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
معلومات أساسية
استكشاف الأخطاء وإصلاحها
سيناريو الاختبار
لا تصل حركة المرور إلى قائمة التحكم في الوصول (ACL) الخاصة بإعادة التوجيه
تصل حركة المرور إلى قائمة التحكم في الوصول (ACL) المعاد توجيهها
سيناريو 1 - مضيف الوجهة في نفس شبكة VLAN، موجود، و SVI 10 up
سيناريو 2 - مضيف الوجهة في شبكة VLAN نفسها، غير موجود، و SVI 10 up
سيناريو 3 - مضيف الوجهة في شبكة VLAN مختلفة، يتواجد، و SVI 10 up
سيناريو 4 - مضيف الوجهة في شبكة VLAN مختلفة، غير موجود، و SVI 10 up
سيناريو 5 - مضيف الوجهة في شبكة VLAN مختلفة، يتواجد، و SVI 10 لأسفل
سيناريو 6 - مضيف الوجهة في شبكة VLAN مختلفة، غير موجود، و SVI 10 لأسفل
السيناريو 7 - خدمة HTTP معطلة
قائمة التحكم في الوصول (ACL) المعاد توجيهها - المنافذ والبروتوكولات غير الصحيحة، بدون إعادة التوجيه
معلومات ذات صلة

المقدمة

يصف هذا مادة كيف مستعمل حركة مرور redirection والشروط أن يكون ضروري in order to أعدت الربط بالمفتاح.

المتطلبات الأساسية

المتطلبات

cisco يوصي أن يتلقى أنت خبرة مع ال cisco هوية خدمة محرك (ISE) تشكيل ومعرفة الأساسية من هذا موضوع:

- عمليات نشر ISE وتدفقات مصادقة الويب المركزية (CWA)
- CLI تشكيل من cisco مادة حفازة مفتاح

المكونات المستخدمة

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

- نظام التشغيل Microsoft Windows 7
- برامج المحول Cisco Catalyst 3750X Series Switch، الإصدارات 15.0 والإصدارات الأحدث
- برنامج ISE، الإصدارات 1.1.4 والإصدارات الأحدث

معلومات أساسية

يعد إعادة توجيه حركة مرور بيانات المستخدم على المحول مكونا هاما لمعظم عمليات النشر مع ISE. تتضمن كل هذه التدفقات إستخدام إعادة توجيه حركة مرور البيانات بواسطة المحول:

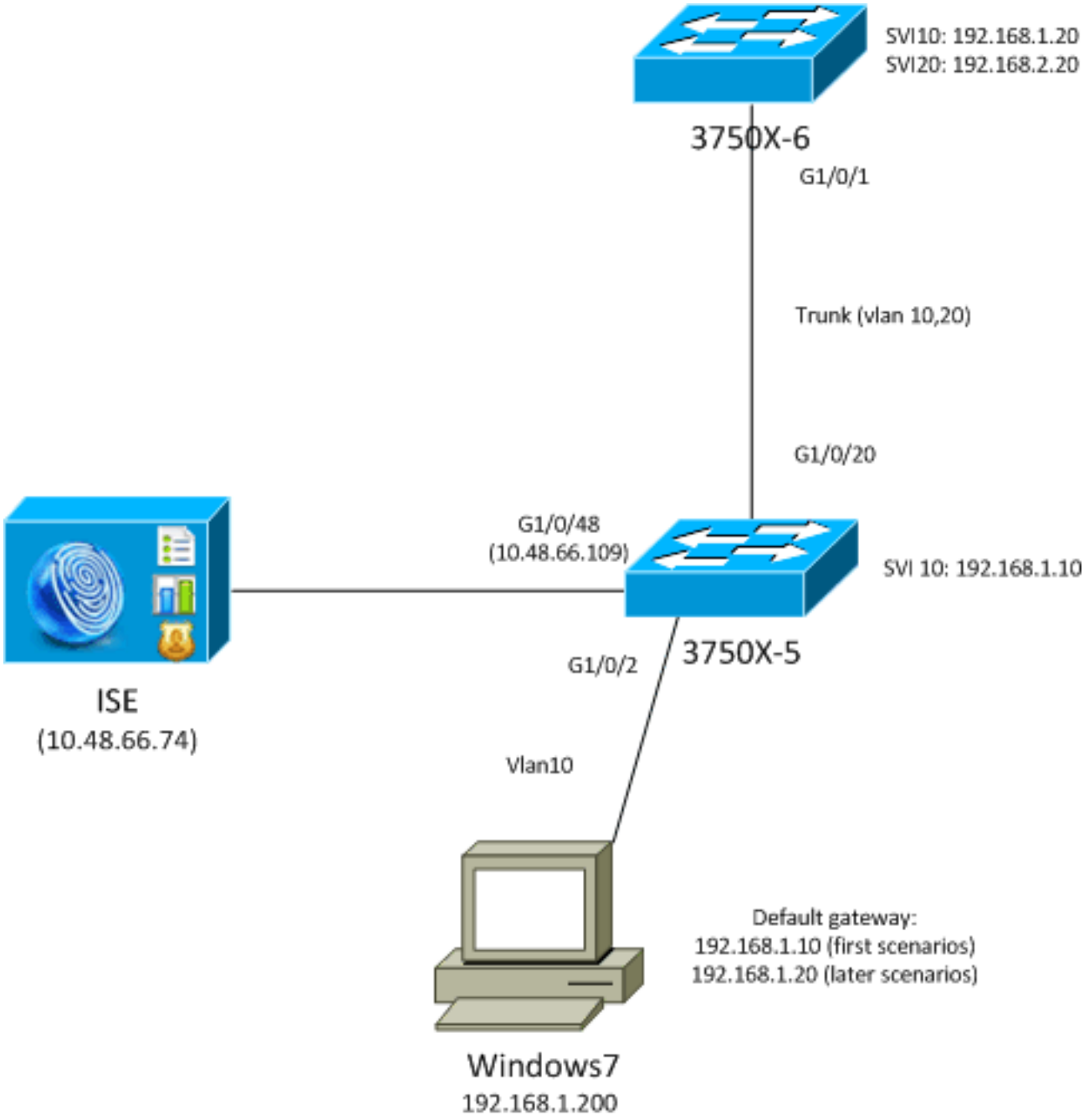
- مصادقة الويب المركزية (CWA)
- إمداد العميل (CPP)
- تسجيل الأجهزة (DRW)
- توفير الطالب الأصلي (NSP)
- إدارة الأجهزة المحمولة (MDM)

إعادة التوجيه التي تم تكوينها بشكل غير صحيح هي السبب في حدوث مشاكل متعددة أثناء النشر. تتمثل النتيجة النموذجية في عامل التحكم في الدخول إلى الشبكة (NAC) الذي لا يظهر بشكل صحيح أو عدم القدرة على عرض مدخل Guest.

للسيناريوهات التي لا يحتوي فيها المحول على نفس واجهة المحول الظاهرية (SVI) كشبكة VLAN الخاصة بالعميل، ارجع إلى الأمثلة الثلاثة الأخيرة.

استكشاف الأخطاء وإصلاحها

سيناريو الاختبار



يتم إجراء الاختبارات على العميل، والتي يجب إعادة توجيهها إلى ISE للإمداد (CPP). تتم مصادقة المستخدم من خلال تجاوز مصادقة MAC (MAB) أو 802.1x. تقوم ISE بإرجاع ملف تعريف التخويل باسم قائمة التحكم في الوصول (ACL) المعاد توجيهها (REDIRECT_POSTURE) وعنوان URL المعاد توجيهه (عمليات إعادة التوجيه إلى ISE):

```
bsns-3750-5#show authentication sessions interface g1/0/2
            Interface:  GigabitEthernet1/0/2
              MAC Address:  0050.5699.36ce
               IP Address:  192.168.1.201
                User-Name:  cisco
                   Status:  Authz Success
                   Domain:  DATA
           Security Policy:  Should Secure
           Security Status:  Unsecure
            Oper host mode:  single-host
          Oper control dir:  both
       Authorized By:  Authentication Server
                Vlan Policy:  10
ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-51ef7db1
```

```
URL Redirect ACL:  REDIRECT_POSTURE
=URL Redirect:  https://10.48.66.74:8443/guestportal/gateway?sessionId
C0A8000100000D5D015F1B47&action=cpp
Session timeout:  N/A
Idle timeout:  N/A
Common Session ID:  C0A8000100000D5D015F1B47
Acct Session ID:  0x00011D90
Handle:  0xBB000D5E

:Runnable methods list
Method   State
dot1x    Authc Success
```

تسمح قائمة التحكم في الوصول (DACL) القابلة للتنزيل بجميع حركات المرور في هذه المرحلة:

```
bsns-3750-5#show ip access-lists xACSACLx-IP-PERMIT_ALL_TRAFFIC-51ef7db1
(Extended IP access list xACSACLx-IP-PERMIT_ALL_TRAFFIC-51ef7db1 (per-user
permit ip any any 10
```

تسمح قائمة التحكم في الوصول (ACL) المعاد توجيهها لحركة المرور هذه دون إعادة التوجيه:

- جميع حركات المرور إلى ISE (10.48.66.74)
- نظام اسم المجال (DNS) وحركة مرور بروتوكول رسائل التحكم في الإنترنت (ICMP)

يجب إعادة توجيه جميع حركات المرور الأخرى:

```
bsns-3750-5#show ip access-lists REDIRECT_POSTURE
Extended IP access list REDIRECT_POSTURE
(deny ip any host 10.48.66.74 (153 matches 10
deny udp any any eq domain 20
(deny icmp any any (10 matches 30
(permit tcp any any eq www (78 matches 40
permit tcp any any eq 443 50
```

المفتاح يتلقى SVI في ال نفسه VLAN بما أن المستعمل:

```
interface Vlan10
ip address 192.168.1.10 255.255.255.0
```

في الأقسام التالية، يتم تعديل هذا الأمر من أجل عرض التأثير المحتمل.

لا تصل حركة المرور إلى قائمة التحكم في الوصول (ACL) الخاصة بإعادة التوجيه

عند محاولة إختبار اتصال أي مضيف، يجب أن تستلم إستجابة لأن حركة المرور هذه لا يتم إعادة توجيهها. للتأكيد، قم بتشغيل تصحيح الأخطاء هذا:

```
debug epm redirect
```

لكل حزمة ICMP يتم إرسالها بواسطة العميل، يجب أن تظهر تصحيح الأخطاء:

```
Jan 9 09:13:07.861: epm-redirect:IDB=GigabitEthernet1/0/2: In
... epm_host_ingress_traffic_qualify
:Jan 9 09:13:07.861: epm-redirect:epm_redirect_cache_gen_hash
IP=192.168.1.201 Hash=562
Jan 9 09:13:07.861: epm-redirect:IP=192.168.1.201: CacheEntryGet Success
Jan 9 09:13:07.861: epm-redirect:IP=192.168.1.201: Ingress packet on
[idb= GigabitEthernet1/0/2] didn't match with [acl=REDIRECT_POSTURE]
```

للتأكد، راجع قائمة التحكم في الوصول (ACL):

```
bsns-3750-5#show ip access-lists REDIRECT_POSTURE
        Extended IP access list REDIRECT_POSTURE
 (deny ip any host 10.48.66.74 (153 matches 10
             deny udp any any eq domain 20
          (deny icmp any any (4 matches 30
(permit tcp any any eq www (78 matches 40
             permit tcp any any eq 443 50
```

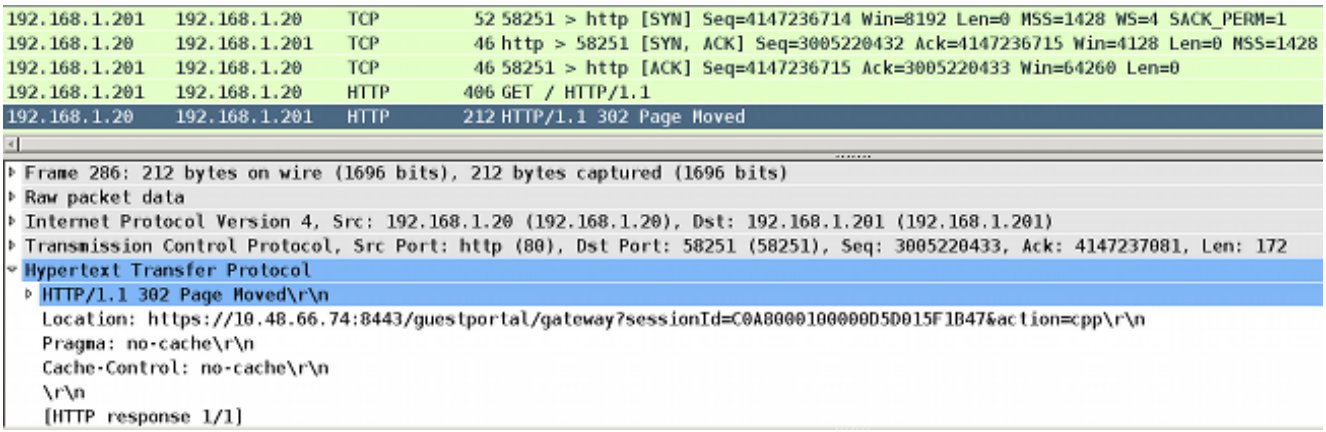
تصل حركة المرور إلى قائمة التحكم في الوصول (ACL) المعاد توجيهها

سيناريو 1 - مضيف الوجهة في نفس شبكة VLAN، موجود، و SVI 10 up

عندما يبدأ أنت الحركة مرور إلى العنوان أن يكون مباشرة طبقة 3 (reachable (L3 بالمفتاح (الشبكة للمحول لها واجهة SVI)، هنا ما يحدث:

1. يبدأ العميل طلب تحليل بروتوكول تحليل العنوان (ARP) لمضيف الوجهة (192.168.1.20) في شبكة VLAN 1. نفسها ويستلم إستجابة (لا يتم إعادة توجيه حركة مرور ARP).

2. يعترض المفتاح أن جلسة، even when الغاية عنوان لا يشكل على أن مفتاح. انتهت عملية تأكيد اتصال TCP. بين العميل والمحول. في هذه المرحلة، لا يتم إرسال حزم أخرى خارج المحول. في هذا السيناريو، بدأ العميل (192.168.1.201) جلسة عمل TCP مع المضيف الآخر الموجود في شبكة VLAN هذه (192.168.1.20) والتي يحتوي المحول على واجهة SVI لأعلى (مع عنوان IP 192.168.1.10):



3. بعد إنشاء جلسة TCP وإرسال طلب HTTP، يقوم المحول بإرجاع إستجابة HTTP مع إعادة التوجيه إلى ISE (رأس الموقع).

يتم تأكيد هذه الخطوات بواسطة تصحيح الأخطاء. هناك العديد من عمليات الوصول إلى قائمة التحكم في الوصول (ACL):

```
[epm-redirect:IP=192.168.1.201: Ingress packet on [idb= GigabitEthernet1/0/2
                                    [matched with [acl=REDIRECT_POSTURE
=epm-redirect:Fill in URL=https://10.48.66.74:8443/guestportal/gateway?sessionId
                                    C0A8000100000D5D015F1B47&action=cpp for redirection
                    :epm-redirect:IP=192.168.1.201: Redirect http request to https
guestportal/gateway?sessionId=C0A8000100000D5D015F1B47&action=cpp/10.48.66.74:8443//
```

```
epm-redirect:EPM HTTP Redirect Daemon successfully created
```

كما يمكن تأكيد ذلك من خلال تصحيح الأخطاء الأكثر تفصيلا:

```
debug ip http all

http_epm_http_redirect_daemon: got redirect request
'HTTP: token len 3: 'GET
http_proxy_send_page: Sending http proxy page
... http_epm_send_redirect_page: Sending the Redirect page to
```

4. يتصل العميل بجلسة عمل طبقة مآخذ التوصيل الآمنة (SSL) مباشرة إلى 10.48.66.74:8443). لا يطلق هذا ربط redirection:

```
epm-redirect:IP=192.168.1.201: Ingress packet on [idb= GigabitEthernet1/0/2] didn't
[match with [acl=REDIRECT_POSTURE
```

ملاحظة: يتم اعتراض الجلسة بواسطة المحول، وبالتالي يمكن التقاط حركة مرور البيانات على المحول باستخدام التقاط الحزمة المضمنة (EPC). تم الالتقاط السابق مع EPC على المحول.

سيناريو 2 - مضيف الوجهة في شبكة VLAN نفسها، غير موجود، و SVI 10 up

إذا كان المضيف الوجهة 192.168.1.20 معطلا (لا يستجيب)، فلن يتلقى العميل ردا على ARP (لا يعترض المحول ARP)، ولا يرسل العميل نظام TCP. إعادة التوجيه لا تحدث أبدا.

هذا هو السبب في أن وكيل NAC يستخدم بوابة افتراضية لاكتشاف ما. يجب أن تستجيب البوابة الافتراضية دائما وتطلق عمليات إعادة التوجيه.

سيناريو 3 - مضيف الوجهة في شبكة VLAN مختلفة، يتواجد، و SVI 10 up

هنا ما يحدث في هذا سيناريو:

1. يحاول العميل الوصول إلى HTTP://8.8.8.8.

2. أن شبكة ليس على أي SVI على المفتاح.
3. يرسل العميل نظام TCP لجلسة العمل تلك إلى البوابة الافتراضية 192.168.1.10 (عنوان MAC للوجهة معروف).

4. يتم تشغيل إعادة التوجيه بنفس الطريقة تماما كما في المثال الأول.

5. يعترض المحول تلك الجلسة ويعيد إستجابة HTTP التي تعيد التوجيه إلى خادم ISE.

6. يقوم العميل بالوصول إلى خادم ISE دون حدوث مشاكل (لم تتم إعادة توجيه حركة مرور البيانات).

ملاحظة: لا يهم ما إذا كانت العبارة الافتراضية موجودة على المحول نفسه أو على جهاز تدفق البيانات من

الخادم. من الضروري فقط تلقي إستجابة ARP من تلك البوابة لتشغيل عملية إعادة التوجيه. وبالإضافة إلى ذلك، من الضروري السماح بوصول ISE عبر البوابة الافتراضية. منح اهتمام خاص إذا كان هناك جدار حماية على التصحيح، وخاصة إذا كان جدار حماية من الطبقة 2 (L2) وكانت حزم L2 تجتاز إرتباطات مختلفة (بعد ذلك قد يكون تجاوز حالة TCP ضروريا على جدار الحماية).

سيناريو 4 - مضيف الوجهة في شبكة VLAN مختلفة، غير موجود، و SVI 10 up

وهذا السيناريو هو نفسه تماما للسيناريو 3. لا يهم ما إذا كان المضيف الوجهة في شبكة VLAN بعيدة موجودا أم لا.

سيناريو 5 - مضيف الوجهة في شبكة VLAN مختلفة، يتواجد، و 10 SVI لأسفل

إن لا يتلقى المفتاح SVI up في ال نفسه VLAN بما أن الزبون، هو يستطيع بعد أنجزت redirection لكن فقط عندما شرط خاص قارن.

المشكلة للمفتاح كيف أن يرجع الإستجابة إلى الزبون من SVI مختلف. من الصعب تحديد مصدر عنوان MAC الذي يجب إستخدامه.

يختلف التدفق عن عندما يكون SVI قيد التشغيل:

1. يرسل الزبون TCP syn إلى المضيف في VLAN مختلف (192.168.2.20) مع غاية {mac address{upper يثبت إلى تقصير مدخل أي يكون عينت على ال upstream مفتاح. تصل هذه الحزمة إلى قائمة التحكم في الوصول (ACL) المعاد توجيهها، والتي يتم عرضها بواسطة تصحيح الأخطاء.
2. يتحقق المحول من توفر توجيه مرة أخرى إلى العميل. تذكر أن 10 SVI قد تعطل.
3. إذا لم يكن المحول يحتوي على SVI آخر يحتوي على توجيه مرة أخرى إلى العميل، فإن الحزمة لا يتم اعتراضها أو إعادة توجيهها، حتى عندما تشير سجلات Enterprise Policy Manager (EPM) إلى الوصول إلى قائمة التحكم في الوصول. قد يرجع المضيف البعيد SYN ACK، ولكن المحول لا يتلقى توجيه مرة أخرى إلى العميل (VLAN10) ويسقط الحزمة. لا يمكن تبديل الحزمة (L2) فقط، لأنها وصلت إلى قائمة التحكم في الوصول (ACL) المعاد توجيهها.
4. إن لا يتلقى المفتاح تحشد إلى الزبون VLAN عن طريق SVI مختلف، هو يعترض أن ربط وينفذ ال redirect كمعتاد. لا تنتقل الاستجابة باستخدام إعادة توجيه URL مباشرة إلى العميل، ولكن عبر محول/موجه مختلف استنادا إلى قرار التوجيه.

لاحظوا عدم التناظر هنا:

- يتم اعتراض حركة المرور المستلمة من العميل محليا بواسطة المحول.
- ويتم إرسال الاستجابة لذلك، والتي تتضمن إعادة توجيه HTTP، عبر محول الخادم استنادا إلى التوجيه.
- هذا هو الوقت الذي قد تحدث فيه مشاكل نموذجية مع جدار الحماية، ويتطلب تجاوز TCP.
- حركة المرور إلى ISE، والتي لا يتم إعادة توجيهها، متماثلة. وإعادة التوجيه ذاتها هي الوحيدة غير المتماثلة.

سيناريو 6 - مضيف الوجهة في شبكة VLAN مختلفة، غير موجود، و 10 SVI لأسفل

وهذا السيناريو هو نفسه تماما للسيناريو 5. لا يهم أن المضيف البعيد موجود. يعد التوجيه الصحيح هو المهم.

السيناريو 7 - خدمة HTTP معطلة

كما هو موضح في السيناريو 6، تلعب عملية HTTP على المحول دورا مهما. إذا تم تعطيل خدمة HTTP، فإن EPM يوضح أن الحزمة تصل إلى قائمة التحكم في الوصول (ACL) المعاد توجيهها:

```
epm-redirect:IP=192.168.1.201: Ingress packet on [idb= GigabitEthernet1/0/2] matched
[with [acl=REDIRECT_POSTURE
```

ومع ذلك، فإن إعادة التوجيه لا تحدث أبدا.

خدمة HTTPS على المحول غير مطلوبة لإعادة توجيه HTTP، ولكنها مطلوبة لإعادة توجيه HTTPS. يمكن أن يستخدم وكيل NAC كلا لاكتشاف ISE. لذلك، ينصح بتمكين كليهما.

قائمة التحكم في الوصول (ACL) المعاد توجيهها - المنافذ والبروتوكولات غير الصحيحة، بدون إعادة التوجيه

لاحظت أن المفتاح يستطيع فقط اعترضت HTTP أو HTTPS حركة مرور أن يعمل على ميناء معياري (TCP/80 و TCP/443). إذا كان HTTP/HTTPS يعمل على منفذ غير قياسي، يمكن تكوينه باستخدام الأمر **ip port-map http**. أيضا، المفتاح ينبغي يتلقى HTTP نادل على أن ميناء (**ip http ميناء**).

معلومات ذات صلة

- المصادقة المركزية للويب مع محول ومثال تكوين محرك خدمات الهوية
- دليل مستخدم محرك خدمات الهوية من Cisco، إصدار 1.2
- 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).