إستخدام خادم RSA المميز و بروتوكول SDI ل ACS و ASA

المحتويات

المقدمة

يصف هذا المستند إجراءات أستكشاف الأخطاء وإصلاحها الخاصة بمدير مصادقة RSA، والتي يمكن دمجها مع جهاز الأمان القابل للتكيف (ASA) من Cisco وخادم التحكم في الوصول الآمن (ACS) من Cisco.

يعد مدير مصادقة RSA حلا يوفر كلمة مرور المرة الواحدة (OTP) للمصادقة. يتم تغيير كلمة المرور هذه كل 60 ثانية ويمكن إستخدامها مرة واحدة فقط. وهو يدعم كلا من الأجهزة والبرامج المميزة.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة أساسية بالمواضيع التالية:

- تكوين ASA CLI من Cisco
- تكوين ACS من Cisco

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج التالية:

- برنامج Cisco ASA، الإصدار 8.4 والإصدارات الأحدث
- Cisco Secure ACS، الإصدار 5.3 والإصدارات الأحدث

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

نظرية

يمكن الوصول إلى خادم RSA باستخدام بروتوكول RADIUS أو بروتوكول RSA الخاص: SDI. يمكن أن يستخدم كل من ASA و ACS البروتوكولين (RADIUS، SDI) للوصول إلى RSA.

تذكر أنه يمكن دمج RSA مع Cisco AnyConnect Secure Mobility Client عند إستخدام رمز مميز للبرنامج. يركز هذا المستند فقط على دمج ASA و ACS. لمزيد من المعلومات حول AnyConnect، ارجع إلى قسم إستخدام مصادقة SDI من دليل مسؤول Cisco AnyConnect Secure Mobility Client، الإصدار 3.1.

RSA عبر RADIUS

يتمتع RADIUS بميزة واحدة كبيرة مقارنة ب SDI. في RSA، من الممكن تعيين توصيفات معينة (تسمى مجموعات على ACS) للمستخدمين. هذه التوصيفات لها سمات RADIUS محددة معرفة. بعد المصادقة الناجحة، تحتوي رسالة قبول RADIUS التي تم إرجاعها من RSA على هذه السمات. واستنادا إلى هذه الخصائص، يتخذ ال ACS قرارات اضافية. السيناريو الأكثر شيوعا هو قرار إستخدام تعيين مجموعة ACS لتعيين سمات RADIUS المحددة، المتعلقة بملف التعريف على RSA، إلى مجموعة معينة على ACS. باستخدام هذا المنطق، من الممكن نقل عملية الاعتماد بالكامل من RSA إلى ACS مع الحفاظ على المنطق متعدد المستويات كما هو الحال على RSA.

RSA عبر SDI

يتمتع SDI بميزتين رئيسيتين عبر RADIUS. الأول هو أن كل الجلسة مشفرة. والثاني هو الخيارات المثيرة للاهتمام التي يوفرها عميل SDI: وهو قادر على تحديد ما إذا كان قد تم إنشاء الفشل بسبب فشل المصادقة أو التفويض أو بسبب عدم العثور على المستخدم.

يستخدم ACS هذه المعلومات أثناء العمل للهوية. على سبيل المثال، يمكن أن يستمر ل "لم يتم العثور على المستخدم" ولكن رفض ل "فشلت المصادقة."

هناك فرق آخر بين RADIUS و SDI. عندما يستخدم جهاز وصول إلى الشبكة مثل ASA SDI، يقوم ACS بتنفيذ المصادقة فقط. عندما يستخدم RADIUS، ينفذ ACS المصادقة والتخويل والمحاسبة (AAA). ومع ذلك، هذا ليس فارقا كبيرا. من الممكن تكوين SDI للمصادقة و RADIUS لمحاسبة نفس الجلسات.

بروتوكول SDI

بشكل افتراضي، يستخدم SDI بروتوكول مخطط بيانات المستخدم (UDP) 5500. يستخدم SDI مفتاح تشفير متماثل، مماثل لمفتاح RADIUS، من أجل تشفير الجلسات. يتم حفظ هذا المفتاح في ملف سري للعقدة ويختلف عن كل عميل SDI. يتم نشر هذا الملف يدويا أو تلقائيا.

ملاحظة: لا يدعم ACS/ASA النشر اليدوي.

بالنسبة لعقدة النشر التلقائي، يتم تنزيل الملف السري تلقائيا بعد أول مصادقة ناجحة. يتم تشفير سر العقدة باستخدام مفتاح مشتق من رمز مرور المستخدم ومعلومات أخرى. وهذا يخلق بعض مشاكل الأمان المحتملة، لذلك يجب تنفيذ المصادقة الأولى محليا واستخدام البروتوكول المشفر (طبقة الأمان [SSH]، وليس برنامج Telnet) لضمان عدم قدرة المهاجم على اعتراض ذلك الملف وفك تشفيره.

التكوين

ملاحظات:

استخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المُستخدمة في هذا القسم.

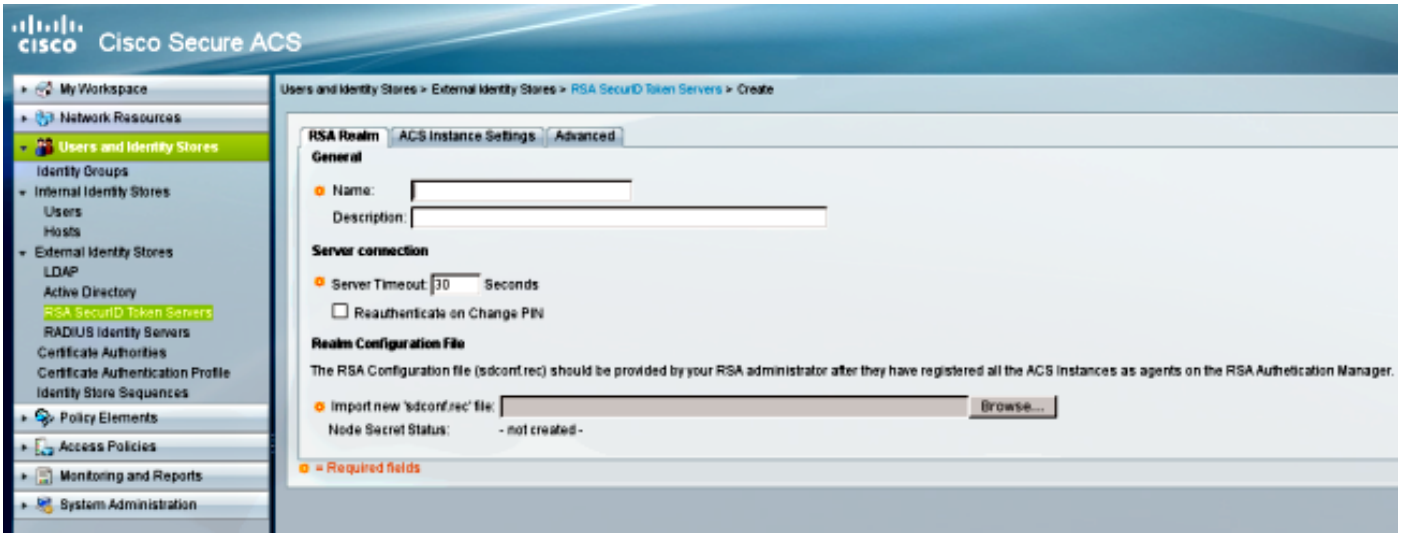
تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم "أداة مترجم الإخراج" لعرض تحليل لمُخرَج الأمر **show**.

ارجع إلى معلومات مهمة عن أوامر تصحيح الأخطاء قبل أن تستخدم أوامر **debug**.

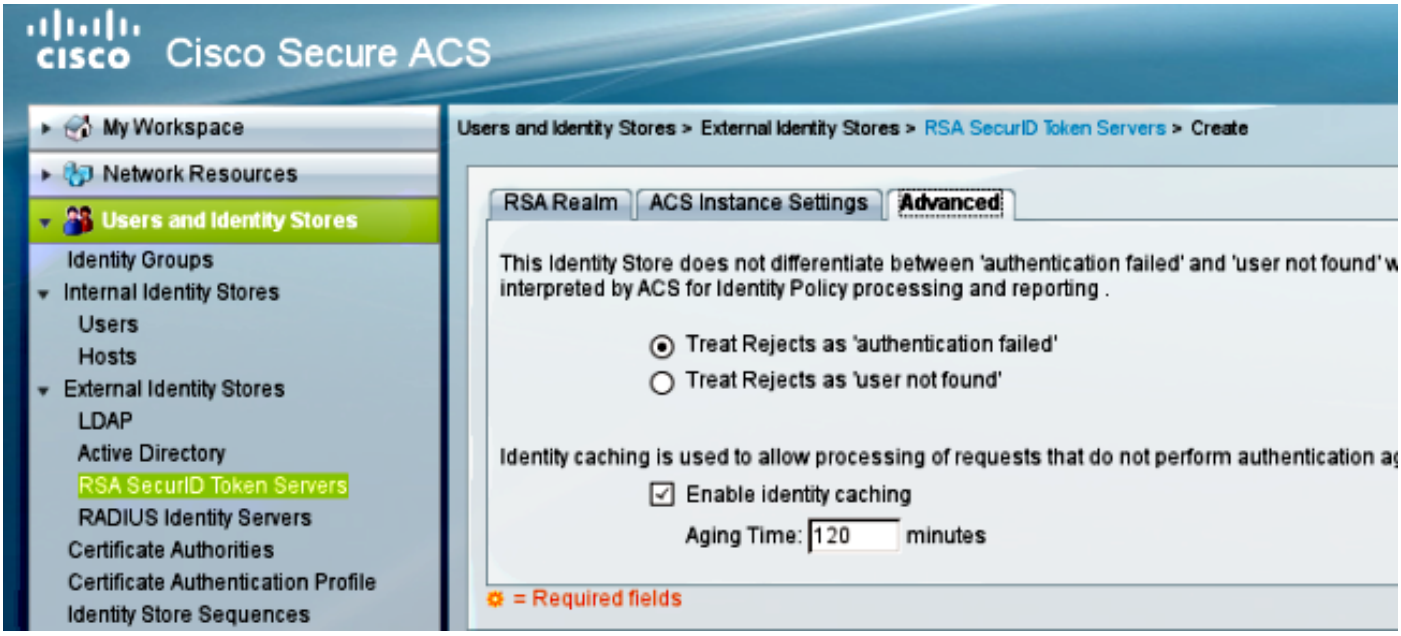
SDI على ACS

ويتم تكوينها في **المستخدمين ومخازن الهوية > مخزن الهوية الخارجية > خوادم رمز معرف RSA الآمن**.

يحتوي RSA على خوادم نسخ متماثلة متعددة، مثل الخوادم الثانوية ل ACS. لا توجد حاجة لوضع جميع العناوين هناك، فقط ملف **sdconf.rec** الذي يقدمه مسؤول RSA. يتضمن هذا الملف عنوان IP الخاص بخادم RSA الأساسي. بعد أول عقدة مصادقة ناجحة، يتم تنزيل الملف السري مع عناوين IP لجميع النسخ المتماثلة ل RSA.



لتمييز "لم يتم العثور على المستخدم" عن "فشل المصادقة"، أختر الإعدادات في علامة التبويب **خيارات متقدمة**:



من الممكن أيضا تغيير آليات التوجيه الافتراضية (موازنة التحميل) بين خوادم RSA المتعددة (الأساسية والنسخ المتماثلة). قم بتغييره باستخدام ملف **sdopts.rec** المتوفر من قبل مسؤول RSA. في ACS، يتم تحميلها في **Users and Identity Stores (المستخدمين ومتاجر الهوية) > مخزن الهوية الخارجية > خوادم رمز معرف RSA الآمن > إعدادات مثيل ACS**.

بالنسبة لنشر نظام المجموعة، يجب نسخ التكوين نسخا متماثلا. بعد أول مصادقة ناجحة، تستخدم كل عقدة من عقد ACS سر العقدة الخاص بها الذي تم تنزيله من خادم RSA الأساسي. من المهم تذكر تكوين RSA لجميع عقد ACS في نظام المجموعة.

SDI على ASA

لا يسمح ال ASA بتحميل من ال **sdconf.rec** مبرد. ومثلها كمثل ACS، فإنها تسمح بالنشر التلقائي فقط. يلزم تكوين ASA يدويا للإشارة إلى خادم RSA الأساسي. لا توجد حاجة إلى كلمة مرور. بعد أول عقدة مصادقة ناجحة، يتم تثبيت الملف السري (.sdi file على flash) ويتم حماية جلسات المصادقة الإضافية. كما يتم تنزيل عنوان IP الخاص بخوادم RSA الأخرى.

فيما يلي مثال:

```
aaa-server SDI protocol sdi
aaa-server SDI (backbone) host 1.1.1.1
debug sdi 255
test aaa auth SDI host 1.1.1.1 user test pass 321321321
```

بعد المصادقة الناجحة، يعرض الأمر **show aaa-server protocol sdi** أو **show aaa-server <aaa-server-group>** جميع خوادم RSA (إذا كان هناك أكثر من واحد)، بينما يعرض الأمر **show run** عنوان IP الأساسي فقط:

```
bsns-asa5510-17# show aaa-server RSA
                Server Group:    RSA
                Server Protocol: sdi
            Server Address:  10.0.0.101
                Server port:     5500
Server status:   ACTIVE (admin initiated), Last transaction at
                 UTC Sat Jul 27 2013 10:13:55
    Number of pending requests              0
Average round trip time                 706ms
    Number of authentication requests       4
```

```
Number of authorization requests        0
Number of accounting requests           0
Number of retransmissions               0
Number of accepts                       1
Number of rejects                       3
Number of challenges                    0
Number of malformed responses           0
Number of bad authenticators            0
Number of timeouts                      0
Number of unrecognized responses        0


                                :SDI Server List
      Active Address:           10.0.0.101
      Server Address:           10.0.0.101
            Server port:              5500
               Priority:                 0
               Proximity:                2
             Status:                    OK
Number of accepts                       0
Number of rejects                       0
Number of bad next token codes          0
Number of bad new pins sent             0
Number of retries                       0
Number of timeouts                      0

      Active Address:           10.0.0.102
      Server Address:           10.0.0.102
            Server port:              5500
               Priority:                 8
               Proximity:                2
             Status:                    OK
Number of accepts                       1
Number of rejects                       0
Number of bad next token codes          0
Number of bad new pins sent             0
Number of retries                       0
Number of timeouts                      0
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

لا يوجد تكوين وكيل على RSA

في العديد من الحالات بعد تثبيت ASA جديد أو تغيير عنوان ASA IP، من السهل نسيان إجراء نفس التغييرات على RSA. يلزم تحديث عنوان IP للوكيل على RSA لجميع العملاء الذين يصلون إلى RSA. ثم يتم إنشاء سر العقدة الجديدة. وينطبق الأمر نفسه على ACS، وخاصة العقد الثانوية لأن لها عناوين IP مختلفة ويلزم أن يثق RSA بها.

العقدة السرية التالفة

في بعض الأحيان، يصبح ملف العقدة السرية على ASA أو RSA تالفا. بعد ذلك، من الأفضل إزالة تكوين الوكيل على RSA وإضافته مرة أخرى. أنت تحتاج أيضا إلى تنفيذ العملية نفسها على ASA/ACS - أزلت وأضفت تشكيل مرة أخرى. احذف أيضا ملف .sdi على ذاكرة Flash (الذاكرة المؤقتة)، حتى يتم تثبيت ملف .sdi جديد في المصادقة التالية. يجب أن يحدث النشر التلقائي لسر العقدة بمجرد اكتمال ذلك.

العقدة في الوضع المعلق

في بعض الأحيان، تكون إحدى العقد في وضع إيقاف مؤقت، وهو ما لا ينتج عن إستجابة من الخادم:

```
asa# show aaa-server RSA
"output ommited.....>
:SDI Server List
Active Address: 10.0.0.101
Server Address: 10.0.0.101
Server port: 5500
Priority: 0
Proximity: 2
Status: SUSPENDED
```

في الوضع المعلق، لا يحاول ASA إرسال أي حزم إلى تلك العقدة، بل يحتاج إلى حالة **OK** لذلك. يتم وضع الخادم الذي فشل في الوضع النشط مرة أخرى بعد المؤقت المعطل. أحلت ل كثير معلومة، [ال reactivation-mode أمر](#) قسم في [ال cisco ASA sery أمر مرجع](#)، 9.1 مرشد.

في مثل هذه السيناريوهات، من الأفضل إزالة تكوين AAA-server وإضافته لتلك المجموعة من أجل تشغيل هذا الخادم إلى الوضع النشط مرة أخرى.

تم تأمين الحساب

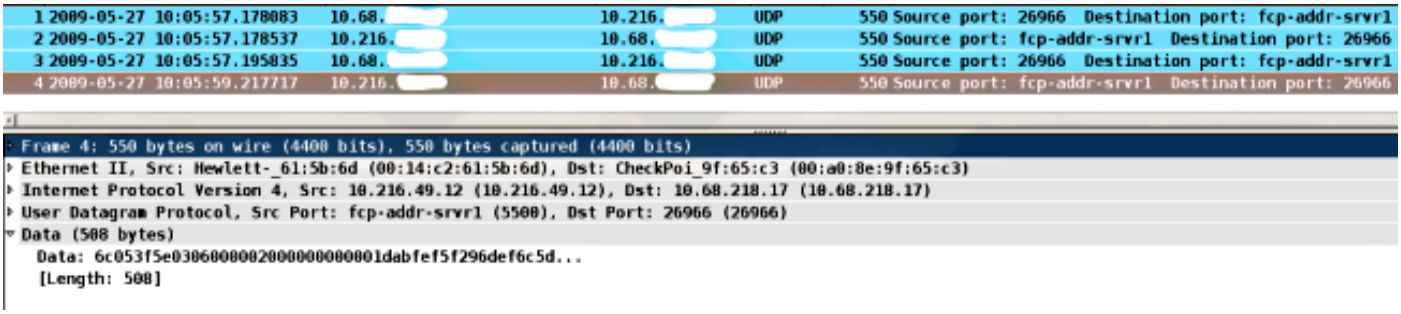
بعد عمليات إعادة المحاولة المتعددة، قد يتم قفل RSA من الحساب. يمكن فحصه بسهولة على RSA مع التقارير. في ASA/ACS، تظهر التقارير فقط "المصادقة الفاشلة".

الحد الأقصى لمشكلات الوحدة الانتقالية (MTU) والتجزئة

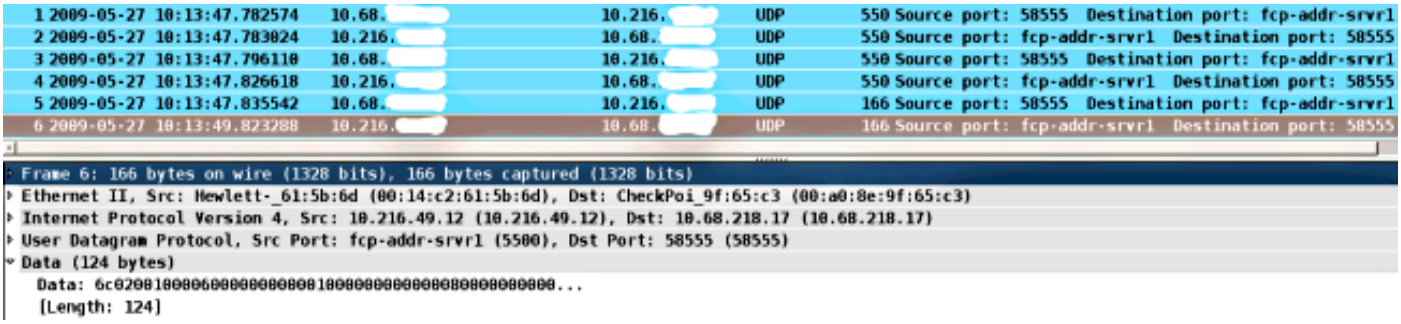
يستخدم SDI بروتوكول UDP كنقل، وليس اكتشاف مسار MTU. أيضا لا يوجد لحركة مرور UDP بت عدم التجزئة (DF) مضبوطة بشكل افتراضي. في بعض الأحيان للحزم الأكبر، قد تكون هناك مشاكل تجزئة. من السهل شم حركة المرور على RSA (يستخدم كل من الجهاز والجهاز الظاهري [Windows VM] ويستخدم Wireshark). أكمل نفس العملية على ASA/ACS وقارن. أيضا، اختبر RADIUS أو WebAuthentication على RSA لمقارنته مع SDI (in order to قللت المشكلة).

الحزم وتصحيح الأخطاء ل ACS

نظرا لأنه يتم تشفير حمولة SDI، فإن الطريقة الوحيدة لاستكشاف أخطاء عمليات الالتقاط وإصلاحها هي مقارنة حجم الاستجابة. إذا كان حجمه أقل من 200 بايت، فقد تكون هناك مشكلة. يتضمن تبادل SDI النموذجي أربع حزم، كل منها 550 بايت، ولكن قد يتغير ذلك مع إصدار خادم RSA:



وفي حالة حدوث مشاكل، يكون عادة أكثر من أربع حزم يتم تبادلها وأحجام أصغر:



كما أن سجلات ACS واضحة تماما. فيما يلي سجلات SDI النموذجية على ACS:

```
EventHandler,11/03/2013,13:47:58:416,DEBUG,3050957712,Stack: 0xa3de560
Calling backRSAIDStore: Method MethodCaller<RSAIDStore, RSAAgentEvent> in
thread:3050957712,EventStack.cpp:242

,AuthenSessionState,11/03/2013,13:47:58:416,DEBUG,3050957712,cntx=0000146144
sesn=acs-01/150591921/1587,user=mickey.mouse,[RSACheckPasscodeState
onEnterState],RSACheckPasscodeState.cpp:23::

EventHandler,11/03/2013,13:47:58:416,DEBUG,3002137488,Stack: 0xa3de560
:Calling RSAAgent:Method MethodCaller<RSAAgent, RSAAgentEvent> in thread
EventStack.cpp:204,3002137488

=RSAAgent,11/03/2013,13:47:58:416,DEBUG,3002137488,cntx=0000146144,sesn
,[acs-01/150591921/1587,user=mickey.mouse,[RSAAgent::handleCheckPasscode
RSAAgent.cpp:319

::RSASessionHandler,11/03/2013,13:47:58:416,DEBUG,3002137488,[RSASessionHandler
checkPasscode] call AceCheck,RSASessionHandler.cpp:251

EventHandler,11/03/2013,13:48:00:417,DEBUG,2965347216,Stack: 0xc14bba0
Create newstack, EventStack.cpp:27

EventHandler,11/03/2013,13:48:00:417,DEBUG,3002137488,Stack: 0xc14bba0 Calling
RSAAgent: Method MethodCaller<RSAAgent, RSAServerResponseEvent> in
thread:3002137488,EventStack.cpp:204

RSAAgent,11/03/2013,13:48:00:417,DEBUG,3002137488,cntx=0000146144,sesn=acs-01
user=mickey.mouse,[RSAAgent::handleResponse] operation completed,150591921/1587/
with ACM_OKstatus,RSAAgent.cpp:237

EventHandler,11/03/2013,13:48:00:417,DEBUG,3002137488,Stack: 0xc14bba0
EventStack.cpp:37

EventHandler,11/03/2013,13:48:00:417,DEBUG,3049905040,Stack: 0xa3de560 Calling
:back RSAIDStore: Method MethodCaller<RSAIDStore, RSAAgentEvent> in thread
EventStack.cpp:242,3049905040

=AuthenSessionState,11/03/2013,13:48:00:417,DEBUG,3049905040,cntx=0000146144,sesn
[acs-01/150591921/1587,user=mickey.mouse,[RSACheckPasscodeState::onRSAAgentResponse
Checkpasscode succeeded, Authentication passed,RSACheckPasscodeState.cpp:55
```

معلومات ذات صلة

- موارد مدير مصادقة RSA
- قسم دعم خادم RSA/SDI من دليل تكوين سلسلة Cisco ASA 5500 باستخدام CLI، 8.4 و 8.6
- قسم خادم SecureID الخاص ب RSA في دليل المستخدم لنظام التحكم في الوصول الآمن من Cisco 5.4

- 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).