ASA الإصدار 9.x SSH و Telnet على مثال تكوين الواجهات الداخلية والخارجية

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
المنتجات ذات الصلة
الاصطلاحات
التكوين
الرسم التخطيطي للشبكة
تكوينات SSH
وصول SSH إلى جهاز الأمان
تكوين ASA
تكوين ASDM الإصدار 7.2.1
تكوين Telnet
سيناريوهات مثال Telnet
التحقق من الصحة
debug ssh
عرض جلسات SSH النشطة
عرض مفاتيح RSA العامة
استكشاف الأخطاء وإصلاحها
إزالة مفاتيح RSA من ASA
فشل اتصال SSH

المقدمة

يصف هذا المستند كيفية تكوين "طبقة الأمان" (SSH) على الواجهات الداخلية والخارجية ل Cisco Series Security Appliance، الإصدار x.9 والإصدارات الأحدث. عندما يجب تكوين جهاز الأمان القابل للتكيف (ASA) من Cisco ومراقبته عن بعد باستخدام واجهة سطر الأوامر، يلزم إستخدام أي من برنامج Telnet أو بروتوكول SSH. نظرا لأنه يتم إرسال إتصالات Telnet في نص واضح، والذي يمكن أن يتضمن كلمات المرور، يوصى بشدة بوجود بروتوكول SSH. يتم تشفير حركة مرور SSH في نفق وبالتالي تساعد على حماية كلمات المرور وأوامر التكوين الحساسة الأخرى من الاعتراض.

يسمح ASA باتصالات SSH إلى جهاز الأمان لأغراض الإدارة. يسمح جهاز الأمان بخمسة إتصالات SSH متزامنة كحد أقصى لكل سياق أمان، إذا كان متوفرا، وبحد أقصى عالمي يبلغ 100 اتصال لكل السياقات مجتمعة.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى برنامج جدار حماية Cisco ASA، الإصدار 9.1.5.

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.

ملاحظة: يتم دعم الإصدار 2 من SSH (SSHv2) في إصدارات ASA 7.x والإصدارات الأحدث.

المنتجات ذات الصلة

كما يمكن إستخدام هذا التكوين مع جهاز الأمان Cisco ASA 5500 Series Security Appliance مع إصدارات البرنامج x.9 والإصدارات الأحدث.

الاصطلاحات

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

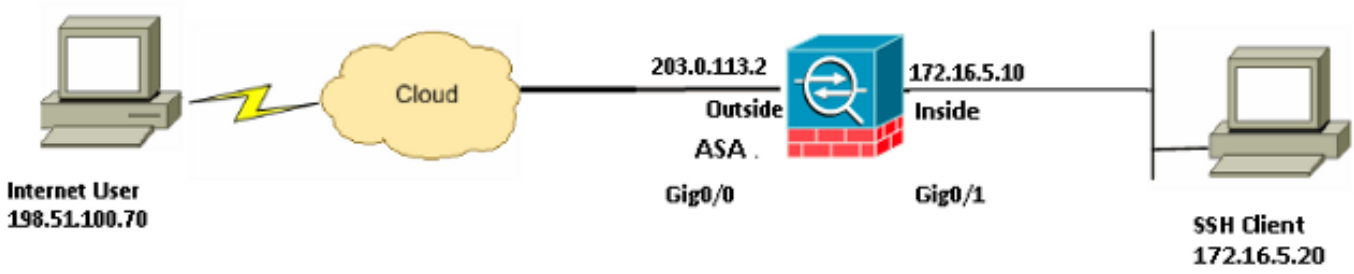
التكوين

أستخدم المعلومات المقدمة في هذا القسم لتكوين الميزات الموضحة في هذا المستند.

ملاحظة: توفر كل خطوة تكوين يتم وصفها المعلومات اللازمة لاستخدام إما CLI أو مدير أجهزة الأمان المعدلة (ASDM).

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

الرسم التخطيطي للشبكة



في مثال التكوين هذا، يعتبر ASA خادم SSH. يتم تشفير حركة مرور البيانات من عملاء SSH (198.51.100.70/32 و 24/172.16.5.20) إلى خادم SSH. يدعم جهاز الأمان وظيفة طبقة SSH البعيدة التي يتم توفيرها في الإصدارين 1 و 2 من SSH كما يدعم معيار تشفير البيانات (DES) وشفرات 3DES. SSH تختلف الإصداران 1 و 2 وهي غير قابلة للتشغيل البيني.

تكوينات SSH

يستخدم هذا المستند التكوينات التالية:

- وصول SSH إلى جهاز الأمان
- كيفية إستخدام عميل SSH
- تكوين ASA

وصول SSH إلى جهاز الأمان

أكمل هذه الخطوات لتكوين وصول SSH إلى جهاز الأمان:

1. تتطلب جلسات SSH دائما نموذج مصادقة مثل اسم المستخدم وكلمة المرور. هناك طريقتان يمكنك إستخدامهما للوفاء بهذا المتطلب.

   الطريقة الأولى التي يمكنك إستخدامها لتلبية هذا المتطلب هي تكوين اسم مستخدم وكلمة مرور باستخدام المصادقة والتفويض والمحاسبة (AAA):

```
ASA(config)#username username password password
ASA(config)#aaa authentication {telnet | ssh | http | serial} console
{[LOCAL | server_group [LOCAL]}
```

   ملاحظة: إذا كنت تستخدم مجموعة خادم TACACS+ أو RADIUS للمصادقة، فيمكنك تكوين جهاز الأمان بحيث يستخدم قاعدة البيانات المحلية كطريقة إحتياطية إذا كان خادم AAA غير متوفر. حدد اسم مجموعة الخادم ثم **محلي** (**محلي** هو حالة حساس). توصي Cisco باستخدام نفس اسم المستخدم وكلمة المرور في قاعدة البيانات المحلية وخادم AAA، لأن موجه أمر جهاز الأمان لا يعطي أي إشارة إلى الطريقة التي يتم إستخدامها.لتحديد نسخ إحتياطي **محلي** ل **TACACS+**، أستخدم هذا التكوين لمصادقة SSH:

```
ASA(config)#aaa authentication ssh console TACACS+ LOCAL
```

   يمكنك بدلا من ذلك إستخدام قاعدة البيانات المحلية كطريقة أساسية للمصادقة دون تعيين الطريقة الاحتياطية. دخلت in order to أتمت هذا، **محلي** فقط:

```
ASA(config)#aaa authentication ssh console LOCAL
```

   الطريقة الثانية التي يمكنك إستخدامها لتلبية هذا المتطلب هي إستخدام اسم المستخدم الافتراضي **ل ASA** وكلمة مرور Telnet الافتراضية من **Cisco**. أنت يستطيع غيرت ال telnet كلمة مع هذا أمر:

```
ASA(config)#passwd password
```

ملاحظة: يمكن **إستخدام** الأمر **password** أيضا في هذه الحالة، حيث أن كلا الأمرين يعملان بشكل متماثل.
2. أنشئ زوج مفاتيح RSA لجدار حماية ASA، والذي يكون مطلوبا ل SSH:

```
ASA(config)#crypto key generate rsa modulus modulus_size
```

ملاحظة: يمكن أن يكون **modulus_size** (في وحدات بت) هو 512 أو 768 أو 1024 أو 2048. كلما كبر حجم معامل المفاتيح الذي تحدده، كلما طال الوقت الذي يستغرقه إنشاء زوج مفاتيح RSA. يوصى بقيمة 2048. يختلف الأمر الذي يتم إستخدامه لإنشاء زوج مفاتيح RSA لإصدارات برنامج ASA الأقدم من الإصدار x.7. في الإصدارات السابقة، يجب تعيين اسم مجال قبل أن تتمكن من إنشاء المفاتيح. في وضع سياق متعدد، يجب عليك إنشاء مفاتيح RSA لكل سياق.
3. حدد البيئات المضيفة المسموح لها بالتوصيل بجهاز الأمان. يحدد هذا الأمر عنوان المصدر وقناع الشبكة وواجهة المضيف (الأجهزة المضيفة) المسموح لها بالاتصال مع SSH. ويمكن إدخاله عدة مرات للعديد من البيئات المضيفة أو الشبكات أو الواجهات. في هذا المثال، يتم السماح بمضيف واحد من الداخل ومضيف واحد من الخارج:

```
ASA(config)#ssh 172.16.5.20 255.255.255.255 inside
ASA(config)#ssh 198.51.10.70 255.255.255.255 outside
```

4. هذه الخطوة إختيارية. بشكل افتراضي، يسمح جهاز الأمان لكل من الإصدار 1 من SSH والإصدار 2. أدخل هذا الأمر لتقييد الاتصالات بإصدار معين:

```
ASA(config)# ssh version
```

ملاحظة: يمكن أن يكون **version_number** إما **1** أو **2**.
5. هذه الخطوة إختيارية. بشكل افتراضي، يتم إغلاق جلسات عمل SSH بعد خمس دقائق من عدم النشاط. يمكن تكوين هذه المهلة بحيث تدوم بين 1 و 60 دقيقة:

```
ASA(config)#ssh timeout minutes
```

تكوين ASA

أستخدم هذه المعلومات لتكوين ASA:

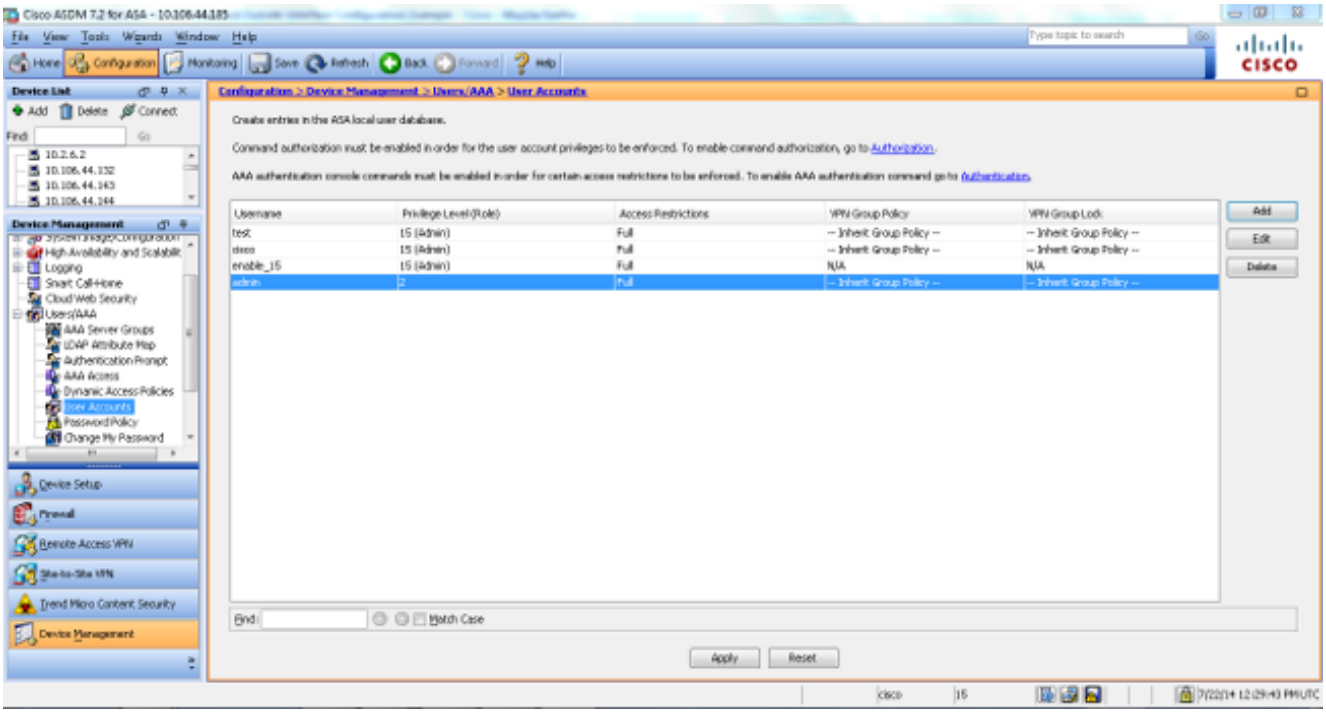
```
ASA Version 9.1(5)2
!
hostname ASA
domain-name cisco.com

interface GigabitEthernet0/0
nameif inside
security-level 100
ip address 172.16.5.10 255.255.255.0
!
interface GigabitEthernet0/1
nameif outside
security-level 0
ip address 203.0.113.2 255.255.255.0

AAA for the SSH configuration ---!

username ciscouser password 3USUcOPFUiMCO4Jk encrypted
aaa authentication ssh console LOCAL

http server enable
http 172.16.5.0 255.255.255.0 inside
no snmp-server location
no snmp-server contact
```

```
snmp-server enable traps snmp authentication linkup linkdown coldstar
telnet timeout 5

Enter this command for each address or subnet ---!
to identify the IP addresses from which ---!
.the security appliance accepts connections ---!
.The security appliance accepts SSH connections from all interfaces ---!

ssh 172.16.5.20 255.255.255.255 inside
ssh 198.51.100.70 255.255.255.255 outside

Allows the users on the host 172.16.5.20 on inside ---!
Allows SSH access to the user on internet 198.51.100.70 on outside ---!
to access the security appliance ---!
.on the inside interface ---!

ssh 172.16.5.20 255.255.255.255 inside

Sets the duration from 1 to 60 minutes ---!
,default 5 minutes) that the SSH session can be idle) ---!
.before the security appliance disconnects the session ---!

ssh timeout 60

console timeout 0
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map global_policy
class inspection_default
inspect dns maximum-length 512
inspect ftp
inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
!
service-policy global_policy global
```

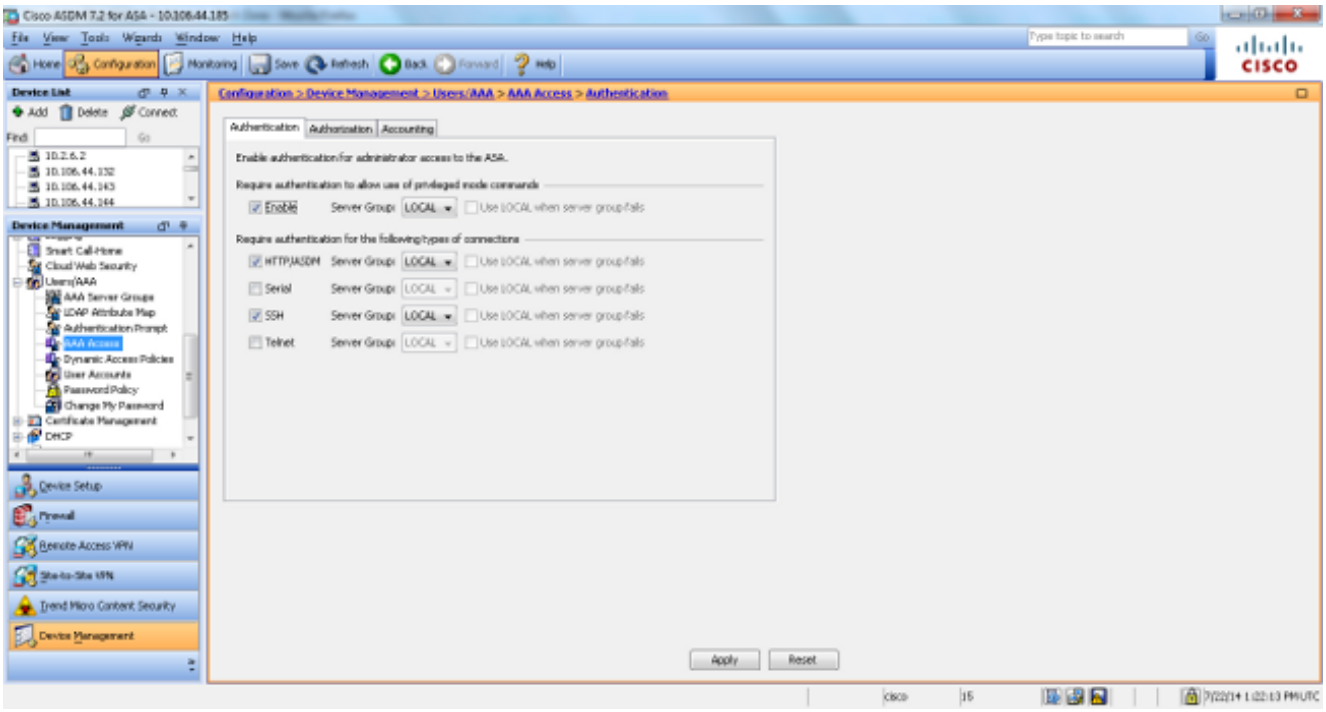
تكوين ASDM الإصدار 7.2.1

أتمت هذا steps in order to شكلت ال ASDM صيغة 7.2.1:

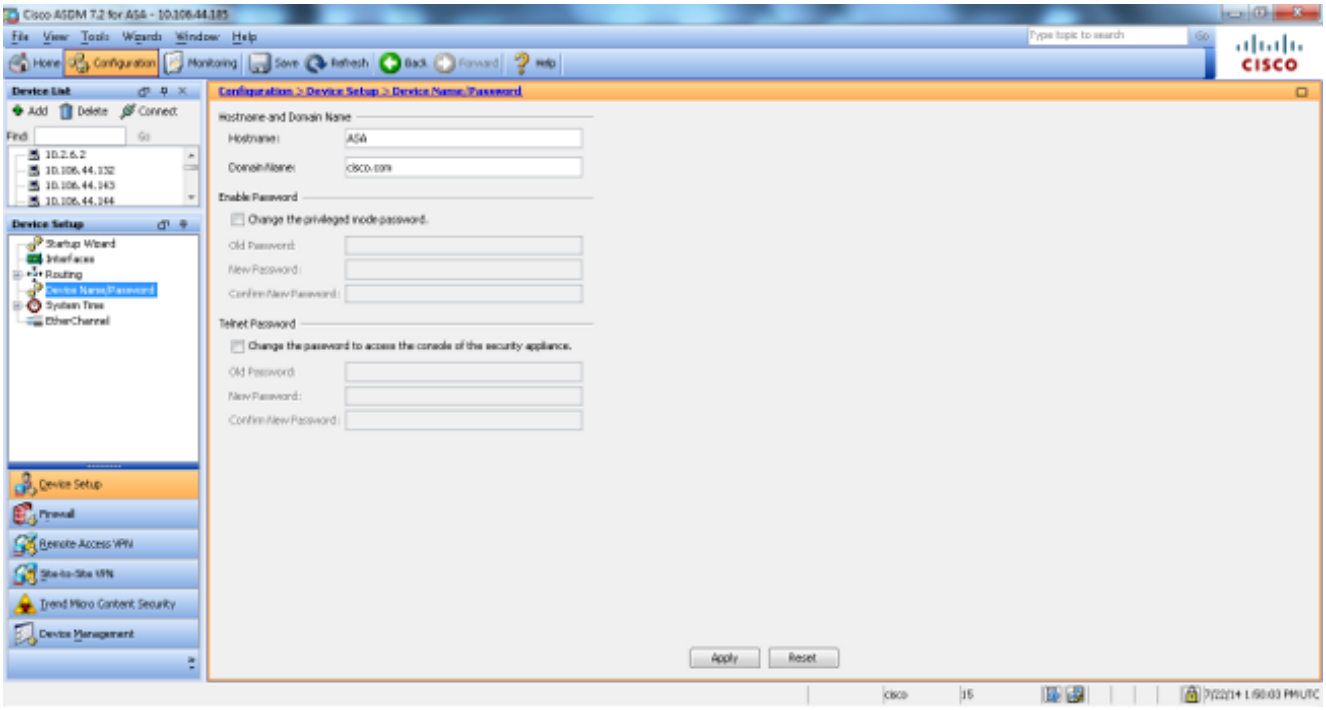
انتقل إلى **التكوين > إدارة الأجهزة > Users/AAA > حسابات المستخدمين** لإضافة مستخدم باستخدام ASDM.



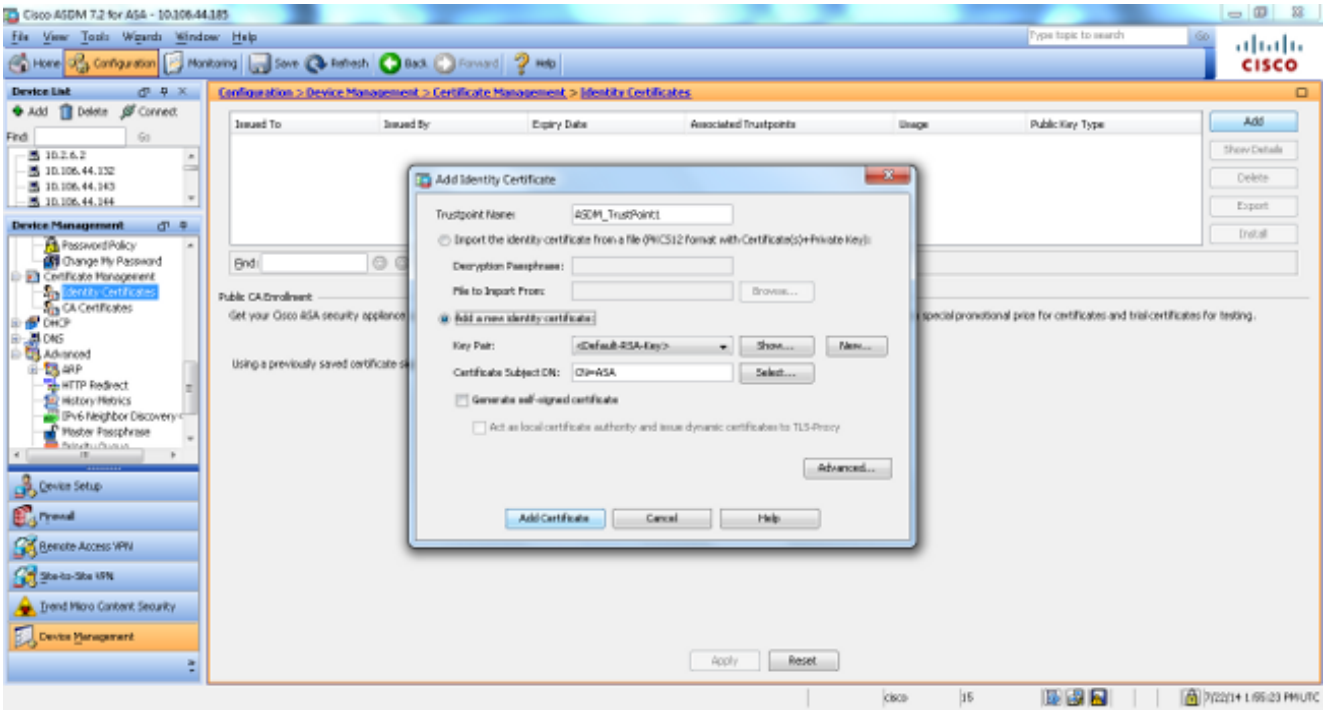
انتقل إلى **التكوين > إدارة الأجهزة > Users/AAA > الوصول إلى AAA > المصادقة** لإعداد مصادقة AAA لـ2. SSH باستخدام ASDM.



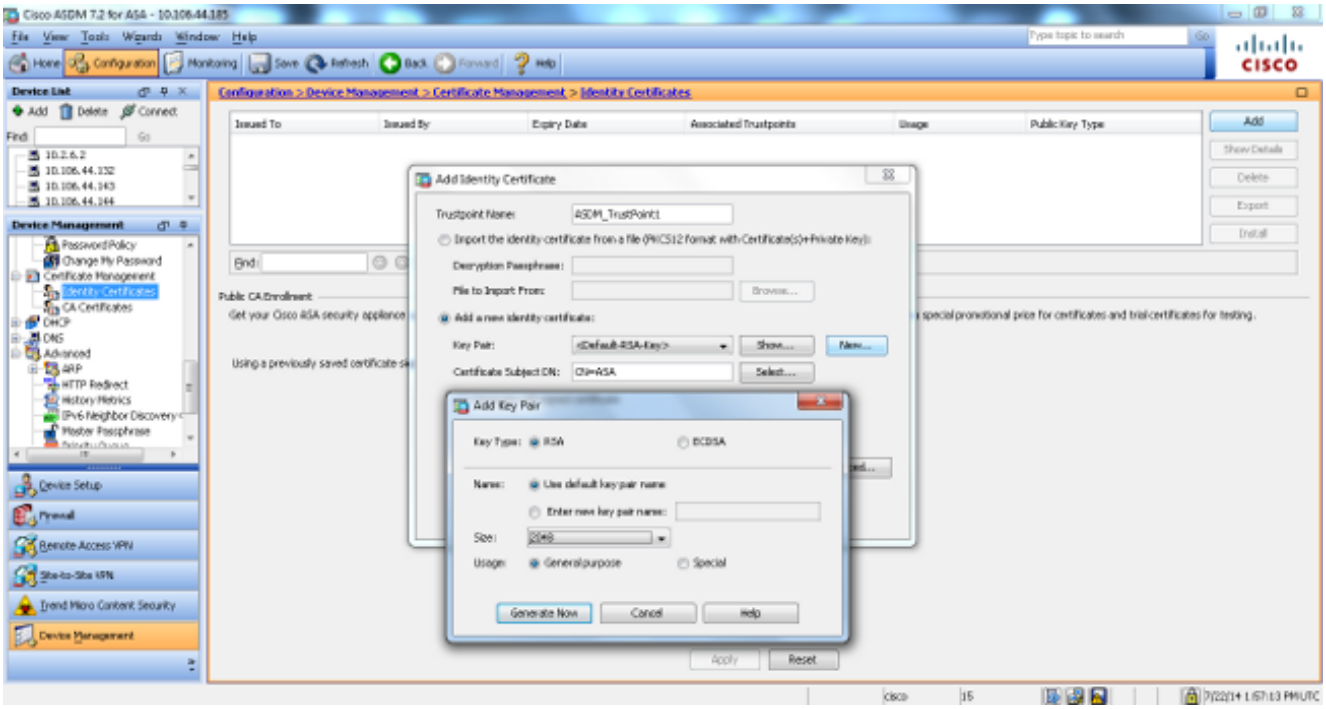
انتقل إلى **التكوين > إعداد الجهاز > اسم الجهاز/كلمة المرور** لتغيير كلمة مرور Telnet باستخدام ASDM. .3



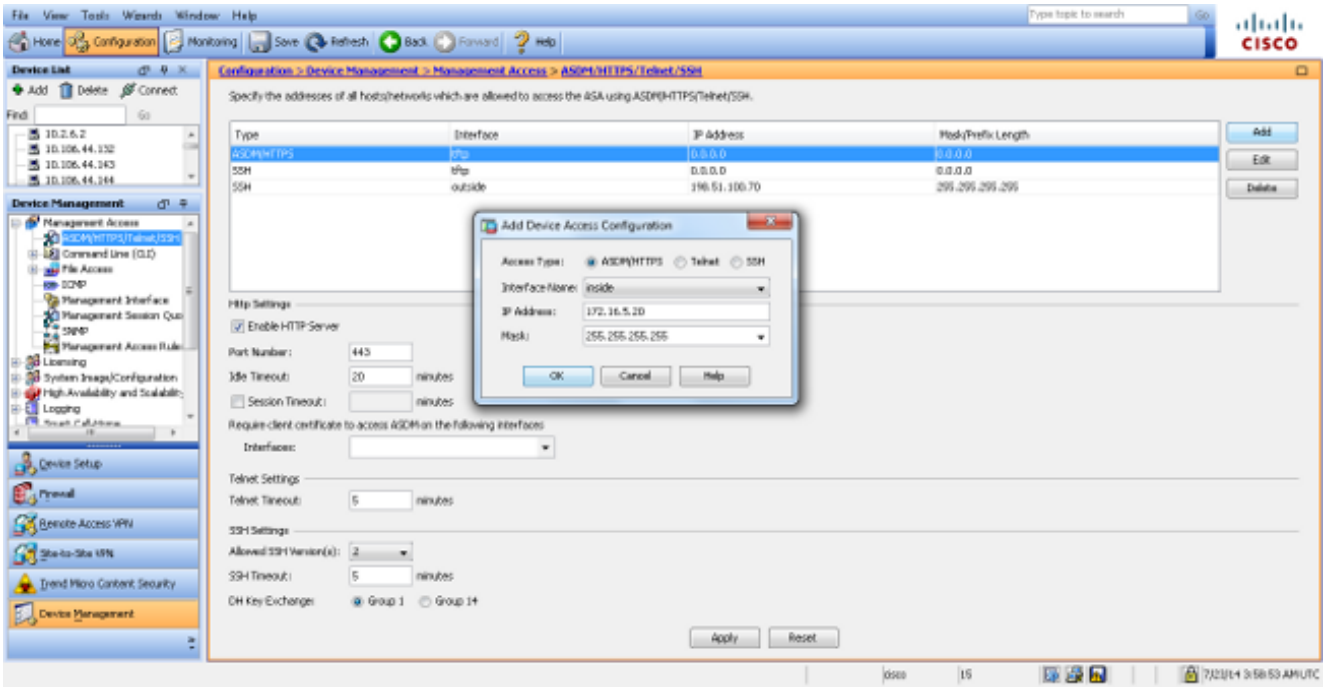
4. انتقل إلى **التكوين > إدارة الأجهزة > إدارة الشهادات > شهادات الهوية**، انقر فوق **إضافة**، واستخدم الخيارات الافتراضية المتوفرة لإنشاء نفس مفاتيح RSA مع ASDM.



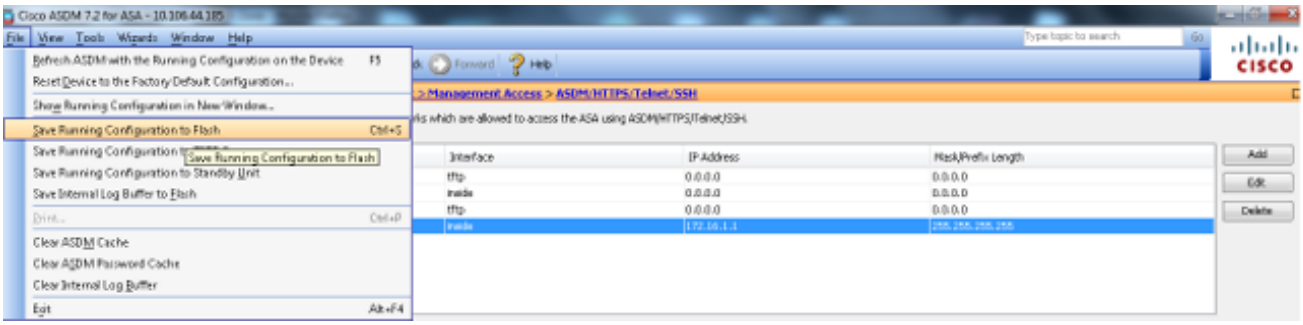
5. انقر على زر **إضافة شهادة هوية جديدة** وانقر فوق **جديد** لإضافة زوج مفاتيح افتراضي، إذا لم يكن واحدا موجودا. بعد اكتمال العملية، انقر فوق **إنشاء الآن**.



6. انتقل إلى **التكوين > إدارة الأجهزة > الوصول إلى الإدارة > سطر الأوامر (CLI) > طبقة الأمان (SSH)** لاستخدام ASDM حتى يمكنك تحديد البيئات المضيفة المسموح لها بالاتصال ب SSH ولتحديد الإصدار وخيارات المهلة.



7. طقطقة **حفظ** من النافذة pop-up in order to أنقذت التشكيل.



8. عند مطالبتك بحفظ التكوين على ذاكرة Flash (الذاكرة المؤقتة)، أختر **تطبيق** لحفظ التكوين.

تكوين Telnet

دخلت in order to أضفت telnet منفذ إلى الوحدة طرفية للتحكم وعينت الخمول مهلة، **ال telnet** أمر في شامل تشكيل أسلوب. بشكل افتراضي، يتم إغلاق جلسات عمل Telnet التي يتم تركها في وضع الخمول لمدة خمس دقائق بواسطة جهاز الأمان. لإزالة وصول Telnet من عنوان IP محدد مسبقا، أستخدم الصيغة **no** من هذا الأمر.

```
telnet {{hostname | IP_address mask interface_name} | {IPv6_address
                                        {{interface_name} | {timeout number
no telnet {{hostname | IP_address mask interface_name} | {IPv6_address
                                        {{interface_name} | {timeout number
```

يسمح لك الأمر **telnet** بتحديد الأجهزة المضيفة التي يمكنها الوصول إلى وحدة تحكم جهاز الأمان عبر برنامج Telnet.

ملاحظة: يمكنك تمكين Telnet على جهاز الأمان على جميع الواجهات. ومع ذلك، يتطلب جهاز الأمان حماية جميع حركات مرور بيانات Telnet إلى الواجهة الخارجية بواسطة IPsec. لتمكين جلسة عمل برنامج Telnet إلى الواجهة الخارجية، قم بتكوين IPsec على الواجهة الخارجية حتى تتضمن حركة مرور IP التي يتم إنشاؤها بواسطة جهاز الأمان وتمكين Telnet على الواجهة الخارجية.

ملاحظة: بشكل عام، إذا كان هناك أي واجهة تحتوي على مستوى أمان صفر أو أقل من أي واجهة أخرى، فإن ASA لا يسمح ل Telnet بهذه الواجهة.

ملاحظة: لا توصي Cisco بالوصول إلى جهاز الأمان من خلال جلسة عمل على برنامج Telnet. يتم إرسال معلومات بيانات اعتماد المصادقة، مثل كلمة المرور، كنص واضح. توصي Cisco باستخدام SSH لاتصال البيانات الأكثر أمانا.

دخلت **الكلمة** أمر in order to ثبتت كلمة ل telnet منفذ إلى الوحدة طرفية للتحكم. كلمة المرور الافتراضية هي **cisco**. دخلت **ال**who أمر in order to شاهدت العنوان أن حاليا ينفذ ال security جهاز وحدة طرفية للتحكم. أدخل الأمر **kill** لإنهاء جلسة عمل لوحدة تحكم Telnet نشطة.

سيناريوهات مثال Telnet

in order to مكنت telnet جلسة إلى القارن داخلي، راجعت الأمثلة أن يكون زودت في هذا قسم.

مثال 1

يسمح هذا المثال للمضيف فقط **172.16.5.20** بالوصول إلى وحدة تحكم جهاز الأمان من خلال برنامج Telnet:

```
ASA(config)#telnet 172.16.5.20 255.255.255.255 inside
```

مثال 2

يتيح هذا المثال للشبكة **24/172.16.5.0** فقط الوصول إلى وحدة تحكم جهاز الأمان من خلال برنامج Telnet:

```
ASA(config)#telnet 172.16.5.0 255.255.255.0 inside
```

مثال 3

يتيح هذا المثال لجميع الشبكات إمكانية الوصول إلى وحدة تحكم جهاز الأمان من خلال برنامج Telnet:

```
ASA(config)#telnet 0.0.0.0 0.0.0.0 inside
```

إذا كنت تستخدم الأمر **aaa** مع الكلمة الأساسية وحدة التحكم، فيجب مصادقة وصول وحدة تحكم Telnet باستخدام خادم مصادقة.

ملاحظة: إذا قمت بتكوين الأمر **AAA** لطلب مصادقة جهاز الأمان والوصول إلى وحدة تحكم Telnet، ومهلة طلب تسجيل دخول وحدة التحكم، فيمكنك الوصول إلى جهاز الأمان من وحدة التحكم التسلسلية. دخلت in order to أتمت هذا، ال security جهاز username وكلمة أن يكون ثبتت مع **ال enable كلمة** أمر.

قم بإصدار الأمر **telnet timeout** لتعيين الحد الأقصى للوقت الذي يمكن أن تكون فيه جلسة عمل برنامج Telnet لوحدة التحكم خاملة قبل أن يتم تسجيل خروجها بواسطة جهاز الأمان. لا يمكنك إستخدام الأمر **no telnet** باستخدام الأمر **telnet timeout**.

يوضح هذا المثال كيفية تغيير الحد الأقصى لمدة خمول جلسة العمل:

```
hostname(config)#telnet timeout 10

hostname(config)#show running-config telnet timeout

telnet timeout 10 minutes
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

ملاحظة: الإنتاج مترجم يساند أداة (يسجل زبون فقط) (OIT) مؤكد **عرض** أمر. استعملت ال OIT in order to شاهدت تحليل من **عرض** أمر إنتاج.

debug ssh

أدخل الأمر **debug ssh** لتمكين تصحيح أخطاء SSH:

```
ASA(config)#debug ssh
SSH debugging on
```

يعرض هذا الإخراج محاولة SSH من عنوان IP داخلي (172.16.5.20) إلى الواجهة الداخلية ل ASA. تصف هذه الأخطاء اتصالا ومصادقة ناجحين:

```
.Device ssh opened successfully
SSH0: SSH client: IP = '172.16.5.20' interface # = 1
SSH: host key initialised
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-2.0-Cisco-1.25
SSH0: send SSH message: outdata is NULL
server version string:SSH-2.0-Cisco-1.25
(SSH0: receive SSH message: 83 (83
SSH0: client version is - SSH-2.0-PuTTY_Release_0.62
```

```
                                                SSH Secure Shell for Windows
                                  client version string:SSH-2.0-PuTTY_Release_0.62
                                SSH Secure Shell for WindowsSSH0: begin ser ver key generation
                                  SSH0: complete server key generation, elapsed time = 1760 ms
                                                      SSH2 0: SSH2_MSG_KEXINIT sent
                                                  SSH2 0: SSH2_MSG_KEXINIT received
                                  SSH2: kex: client->server aes128-cbc hmac-md5 none
                                  SSH2: kex: server->client aes128-cbc hmac-md5 none
                                                SSH2 0: expecting SSH2_MSG_KEXDH_INIT
                                                SSH2 0: SSH2_MSG_KEXDH_INIT received
                                                        SSH2 0: signature length 143
                                                    SSH2: kex_derive_keys complete
                                                          SSH2 0: newkeys: mode 1
                                                    SSH2 0: SSH2_MSG_NEWKEYS sent
                                                SSH2 0: waiting for SSH2_MSG_NEWKEYS
                                                          SSH2 0: newkeys: mode 0
                                                SSH2 0: SSH2_MSG_NEWKEYS received
                                  SSH(cisco): user authen method is 'use AAA', aaa server group ID = 1
                                                  SSH2 0: authentication successful for cisco

                                  .Authentication for the ASA was successful ---!

                                                        SSH2 0: channel open request
                                                             SSH2 0: pty-req request
                                                SSH2 0: requested tty: vt100, height 25, width 80
                                                                SSH2 0: shell request
                                                        SSH2 0: shell message received
```

إذا تم إدخال اسم مستخدم خطأ، مثل **Cisco1** بدلا من **Cisco**، يرفض جدار حماية ASA المصادقة. يظهر إخراج تصحيح الأخطاء هذا المصادقة الفاشلة:

```
                                                  .Device ssh opened successfully
                                  SSH0: SSH client: IP = '172.16.5.20' interface # = 1
                                                        SSH: host key initialised
                                                    SSH0: starting SSH control process
                                  SSH0: Exchanging versions - SSH-2.0-Cisco-1.25
                                                SSH0: send SSH message: outdata is NULL
                                  server version string:SSH-2.0-Cisco-1.25
                                                (SSH0: receive SSH message: 83 (83
                                  SSH0: client version is - SSH-2.0-PuTTY_Release_0.62
                                                SSH Secure Shell for Windows
                                  client version string:SSH-2.0-PuTTY_Release_0.62
                                SSH Secure Shell for WindowsSSH0: begin ser ver key generation
                                  SSH0: complete server key generation, elapsed time = 1760 ms
                                                      SSH2 0: SSH2_MSG_KEXINIT sent
                                                  SSH2 0: SSH2_MSG_KEXINIT received
                                  SSH2: kex: client->server aes128-cbc hmac-md5 none
                                  SSH2: kex: server->client aes128-cbc hmac-md5 none
                                                SSH2 0: expecting SSH2_MSG_KEXDH_INIT
                                                SSH2 0: SSH2_MSG_KEXDH_INIT received
                                                        SSH2 0: signature length 143
                                                    SSH2: kex_derive_keys complete
                                                          SSH2 0: newkeys: mode 1
                                                    SSH2 0: SSH2_MSG_NEWKEYS sent
                                                SSH2 0: waiting for SSH2_MSG_NEWKEYS
                                                          SSH2 0: newkeys: mode 0
                                                SSH2 0: SSH2_MSG_NEWKEYS received
                                  SSH(cisco): user authen method is 'use AAA', aaa server group ID = 1
                                                SSH2 0: authentication failed for cisco1

                                  .Authentication for ASA1 was not successful due to the wrong username ---!
```

وبالمثل، إذا تم توفير كلمة المرور غير الصحيحة، فإن المصادقة تفشل. يظهر إخراج تصحيح الأخطاء هذا المصادقة

الفاشلة:

```
.Device ssh opened successfully
SSH0: SSH client: IP = '172.16.5.20' interface # = 1
SSH: host key initialised
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-2.0-Cisco-1.25
SSH0: send SSH message: outdata is NULL
server version string:SSH-2.0-Cisco-1.25
(SSH0: receive SSH message: 83 (83
SSH0: client version is - SSH-2.0-PuTTY_Release_0.62
SSH Secure Shell for Windows
client version string:SSH-2.0-PuTTY_Release_0.62
SSH Secure Shell for WindowsSSH0: begin ser ver key generation
SSH0: complete server key generation, elapsed time = 1760 ms
SSH2 0: SSH2_MSG_KEXINIT sent
SSH2 0: SSH2_MSG_KEXINIT received
SSH2: kex: client->server aes128-cbc hmac-md5 none
SSH2: kex: server->client aes128-cbc hmac-md5 none
SSH2 0: expecting SSH2_MSG_KEXDH_INIT
SSH2 0: SSH2_MSG_KEXDH_INIT received
SSH2 0: signature length 143
SSH2: kex_derive_keys complete
SSH2 0: newkeys: mode 1
SSH2 0: SSH2_MSG_NEWKEYS sent
SSH2 0: waiting for SSH2_MSG_NEWKEYS
SSH2 0: newkeys: mode 0
SSH2 0: SSH2_MSG_NEWKEYS received
SSH(cisco): user authen method is 'use AAA', aaa server group ID = 1
SSH2 0: authentication failed for cisco1

.Authentication for ASA was not successful due to the wrong password ---!
```

عرض جلسات SSH النشطة

دخلت هذا أمر in order to دققت الرقم من SSH جلسة أن يكون ربطت (والتوصيل دولة) إلى ال ASA:

```
ASA(config)# show ssh sessions

SID Client IP    Version Mode Encryption Hmac State          Username
    IN   aes256-cbc sha1 SessionStarted  cisco     2.0 172.16.5.20   0
    OUT  aes256-cbc sha1 SessionStarted  cisco
```

انتقل إلى **المراقبة > خصائص > الوصول إلى الجهاز > جلسات عمل Secure Shell** لعرض الجلسات باستخدام ASDM.

أدخل الأمر **show asp table socket** للتحقق من إنشاء جلسة عمل TCP:

```
ASA(config)# show asp table socket

Protocol Socket State Local Address Foreign Address

*:SSL 02444758 LISTEN 203.0.113.2:443 0.0.0.0
 *:TCP 02448708 LISTEN 203.0.113.2:22 0.0.0.0
*:SSL 02c75298 LISTEN 172.16.5.10:443 0.0.0.0
 *:TCP 02c77c88 LISTEN 172.16.5.10:22 0.0.0.0
TCP      02d032d8  ESTAB    172.16.5.10:22     172.16.5.20:52234
```

عرض مفاتيح RSA العامة

أدخل هذا الأمر لعرض الجزء العام من مفاتيح RSA على جهاز الأمان:

```
ASA(config)# show crypto key mypubkey rsa
Key pair was generated at: 23:23:59 UTC Jul 22 2014
<Key name: <Default-RSA-Key
Usage: General Purpose Key
Modulus Size (bits): 2048
:Key

300d0609 2a864886 f70d0101 01050003 82010f00 3082010a 02820101 30820122
00aa82d1 f61df1a4 7cd1ae05 c92322c1 1ce490e3 c9db00fd d75afe77 1ea0b2c2
3325576f a7dc5ffe a6166bf5 7f0f2551 25b8cb23 a8908b49 81c42618 c98e3aea
ce6f9e42 367974d1 5c2ea6b1 e7aac40b 44a6c0a5 23c4d845 a57d4c04 6de49dbb
2c6f074e 25e3b19e 7c5da809 ac7d775c 0c01bb9d 211b7078 741094b4 94056e75
72d5e938 c59baaec 12285005 ee6abf81 90822610 cf7ee4c1 ae8093d9 6943bde3
16d8748c d86b5f66 1a6ccf33 9cde0432 b3cabab5 938b1874 c3d7c13e 43a95a8f
ed36db2e f9ca5d2c 0c65858e 3e513723 2d362b47 7984d845 faf22579 654113d1
24d59f27 55d2ddf3 20af3b65 62f039cb a3aafc31 d92a3d9b 14966eb3 cb6ca249
0001 55020301
```

انتقل إلى **التكوين > خصائص > شهادة > زوج المفاتيح** وانقر فوق **إظهار التفاصيل** لعرض مفاتيح RSA مع ASDM.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

إزالة مفاتيح RSA من ASA

في حالات معينة، على سبيل المثال، عند ترقية برنامج ASA أو تغيير إصدار SSH في ASA، قد يكون مطلوبا إزالة مفاتيح RSA وإعادة إنشائها. أدخل هذا الأمر لإزالة زوج مفاتيح RSA من ASA:

```
ASA(config)#crypto key zeroize rsa
```

انتقل إلى **التكوين > خصائص > شهادة > زوج المفاتيح** وانقر فوق **حذف** لإزالة مفاتيح RSA مع ASDM.

فشل اتصال SSH

أنت تستلم هذا خطأ رسالة على ال ASA:

```
.ASA-3-315004: Fail to establish SSH session because RSA host key retrieval failed%
```

هذه هي رسالة الخطأ التي تظهر على جهاز عميل SSH:

```
Selected cipher type
```

لحل هذه المشكلة، قم بإزالة مفاتيح RSA وإعادة إنشائها. أدخل هذا الأمر لإزالة زوج مفاتيح RSA من ASA:

```
ASA(config)#crypto key zeroize rsa
```

دخلت هذا أمر in order to خلقت المفتاح جديد:

```
ASA(config)# crypto key generate rsa modulus 2048
```

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).