PIX/ASA 7.x: SSH/Telnet على مثال تكوين الواجهة الداخلية والخارجية

المحتويات

المقدمة

يقدم هذا المستند نموذجا لتكوين Secure Shell (SSH) على الواجهات الداخلية والخارجية لجهاز الأمان Cisco Series Security Appliance، الإصدار x.7 والإصدارات الأحدث. يتضمن تكوين جهاز الأمان Series Security Appliance عن بعد باستخدام سطر الأوامر إستخدام أي من Telnet أو SSH. نظرا لأنه يتم إرسال إتصالات Telnet في نص واضح، يتضمن كلمات المرور، يوصى بشدة ب SSH. يتم تشفير حركة مرور SSH في نفق وبالتالي تساعد على حماية كلمات المرور وأوامر التكوين الأخرى من الاعتراض.

يتيح جهاز الأمان إتصالات SSH بجهاز 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.

في مثال التكوين هذا، يتم إعتبار جهاز أمان PIX هو خادم SSH. يتم تشفير حركة مرور البيانات من عملاء SSH (10.1.1.2/24 و 16/172.16.1.1) إلى خادم SSH. يدعم جهاز الأمان وظائف طبقة SSH البعيدة المتوفرة في

الإصدارين 1 و 2 من SSH كما يدعم معيار تشفير البيانات (DES) وشفرات 3DES. SSH الإصدار 1 و 2 مختلفان وغير قابلين للتشغيل البيني.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى برنامج جدار حماية Cisco PIX، الإصدار 7.1 و 8.0.

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 SSHv2 في الإصدار x.7 من بروتوكول PIX/ASA والإصدارات الأحدث ولا يتم دعمه في الإصدارات السابقة على الإصدار x.7.

المنتجات ذات الصلة

كما يمكن إستخدام هذا التكوين مع جهاز الأمان Cisco ASA 5500 Series Security Appliance مع إصدارات البرنامج x.7 والإصدارات الأحدث.

الاصطلاحات

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

التكوين

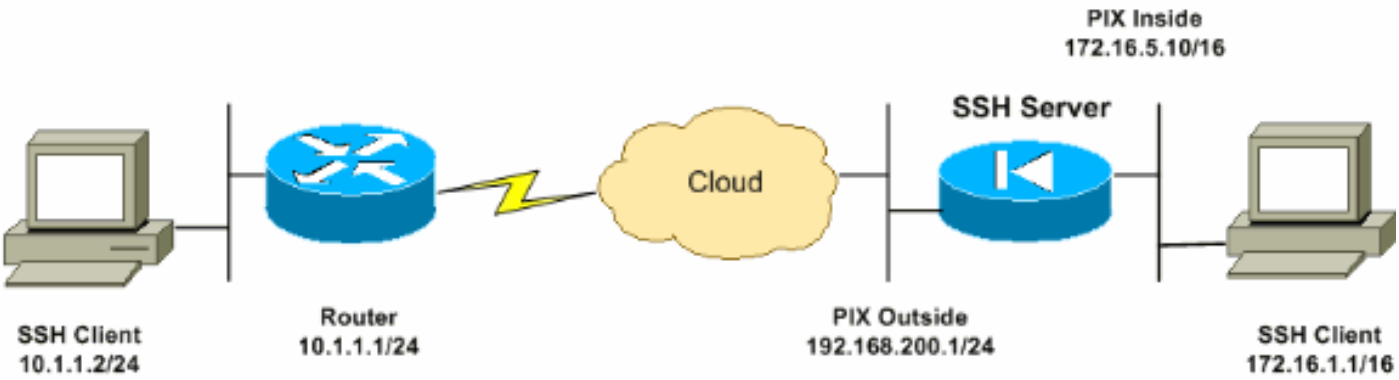
في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: يتم تقديم كل خطوة تكوين بالمعلومات اللازمة لاستخدام سطر الأوامر 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

يستخدم هذا المستند إعداد الشبكة التالي:



تكوينات SSH

يستخدم هذا المستند التكوينات التالية:

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

وصول SSH إلى جهاز الأمان

أكمل هذه الخطوات لتكوين وصول SSH إلى جهاز الأمان:

1. تتطلب جلسات SSH دائما اسم مستخدم وكلمة مرور للمصادقة. هناك طريقتان للوفاء بهذا المطلب.قم بتكوين اسم مستخدم وكلمة مرور واستخدم AAA:الصيغة:

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

ملاحظة: إذا كنت تستخدم مجموعة خوادم TACACS+ أو RADIUS للمصادقة، فيمكنك تكوين جهاز الأمان لاستخدام قاعدة البيانات المحلية كطريقة إحتياطية إذا كان خادم AAA غير متوفر. حدد اسم مجموعة الخوادم ثم محلي (محلي حساس لحالة الأحرف). من المستحسن إستخدام نفس اسم المستخدم وكلمة المرور في قاعدة البيانات المحلية كخادم AAA، لأن مطالبة جهاز الأمان لا تعطي أي إشارة إلى الطريقة التي يتم إستخدامها.**ملاحظة:** مثال :

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

ملاحظة: يمكنك بدلا من ذلك إستخدام قاعدة البيانات المحلية كطريقة أساسية للمصادقة دون إجراء نسخ إحتياطي. دخلت in order to أتمت هذا، محلي وحده.مثال:

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

أوأستخدم اسم المستخدم الافتراضي ل **pix** وكلمة مرور Telnet الافتراضية ل **Cisco**. أنت يستطيع غيرت ال telnet كلمة مع هذا أمر:

```
pix(config)#passwd password
```

ملاحظة: يمكن إستخدام الأمر **password** أيضا في هذه الحالة. كلا الأمرين يؤديان نفس الشيء.

2. أنشئ زوج مفاتيح RSA لجدار حماية PIX، والذي يكون مطلوبا ل SSH:

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

ملاحظة: يمكن أن يكون `modulus_size` (في وحدات بت) 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 1024.**ملاحظة:** الأمر المستخدم لإنشاء زوج مفاتيح RSA مختلف لإصدارات برنامج PIX التي تسبق الإصدار

x.7. في الإصدارات السابقة، يجب تعيين اسم مجال قبل أن تتمكن من إنشاء المفاتيح.**ملاحظة:** في وضع السياق المتعدد، يجب عليك إنشاء مفاتيح RSA لكل سياق. بالإضافة إلى ذلك، لا يتم دعم أوامر التشفير في وضع سياق النظام.

3. حدد البيئات المضيفة المسموح لها الاتصال بجهاز الأمان.يحدد هذا الأمر عنوان المصدر وقناع الشبكة وواجهة المضيف (الأجهزة المضيفة) المسموح لها بالاتصال ب 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.

```
pix(config)#ssh 172.16.1.1 255.255.255.255 inside
pix(config)#ssh 10.1.1.2 255.255.255.255 outside
```

4. **إختياري:** بشكل افتراضي، يسمح جهاز الأمان بكل من الإصدار 1 من SSH والإصدار 2. أدخل هذا الأمر لتقييد الاتصالات بإصدار معين:

```
pix(config)# ssh version
```

ملاحظة: يمكن أن يكون `version_number` هو 1 أو 2.

5. **إختياري:** يتم إغلاق جلسات SSH بشكل افتراضي بعد خمس دقائق من عدم النشاط. يمكن تكوين هذه المهلة بحيث تدوم لمدة تتراوح بين 1 و 60 دقيقة.

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

كيفية إستخدام عميل SSH

قم بتوفير اسم المستخدم وكلمة مرور تسجيل الدخول من جهاز الأمان PIX 500 Series Security Appliance أثناء فتح جلسة SSH. عندما تبدأ جلسة SSH، تظهر نقطة (.) على وحدة تحكم جهاز الأمان قبل أن تظهر مطالبة مصادقة مستخدم SSH:

```
. #(hostname(config
```

لا يؤثر عرض النقطة على وظائف SSH. تظهر النقطة في وحدة التحكم عند إنشاء مفتاح خادم أو فك تشفير الرسالة باستخدام مفاتيح خاصة أثناء تبادل مفاتيح SSH قبل حدوث مصادقة المستخدم. قد تستغرق هذه المهام دقيقتين أو أكثر. النقطة هي مؤشر تقدم يتحقق من أن جهاز الأمان مشغول ولم يعلق.

يعد الإصداران x.1 و 2 من SSH بروتوكولين مختلفين تماما وغير متوافقين. تنزيل عميل متوافق. راجع قسم الحصول على عميل SSH من التكوينات المتقدمة للحصول على مزيد من المعلومات.

تكوين PIX

يستعمل هذا وثيقة هذا تشكيل:

تكوين PIX

```
(PIX Version 7.1(1
!
hostname pix
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 192.168.200.1 255.255.255.0
!
```

```
                                    interface Ethernet1
                                         nameif inside
                                    security-level 100
                            ip address 172.16.5.10 255.255.0.0
                                                    !
                              passwd 2KFQnbNIdI.2KYOU encrypted
                                        ftp mode passive
                                          pager lines 24
                                       mtu outside 1500
                                        mtu inside 1500
                                            no failover
                                   icmp permit any outside
                                    no asdm history enable
                                         arp timeout 14400
          route outside 10.1.1.0 255.255.255.0 192.168.200.1 1
                                      timeout xlate 3:00:00
          timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
                                                icmp 0:00:02
        timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
                                                    0:05:00
       timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
                               timeout uauth 0:05:00 absolute

        AAA for the SSH configuration username ciscouser ---!
                            password 3USUcOPFUiMCO4Jk encrypted
                          aaa authentication ssh console LOCAL

                                        http server enable
                         http 172.16.0.0 255.255.0.0 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 10.1.1.2 255.255.255.255 outside

        Allows the users on the host 172.161.1.1 !--- to ---!
            access the security appliance !--- on the inside
            interface. ssh 172.16.1.1 255.255.255.255 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
```

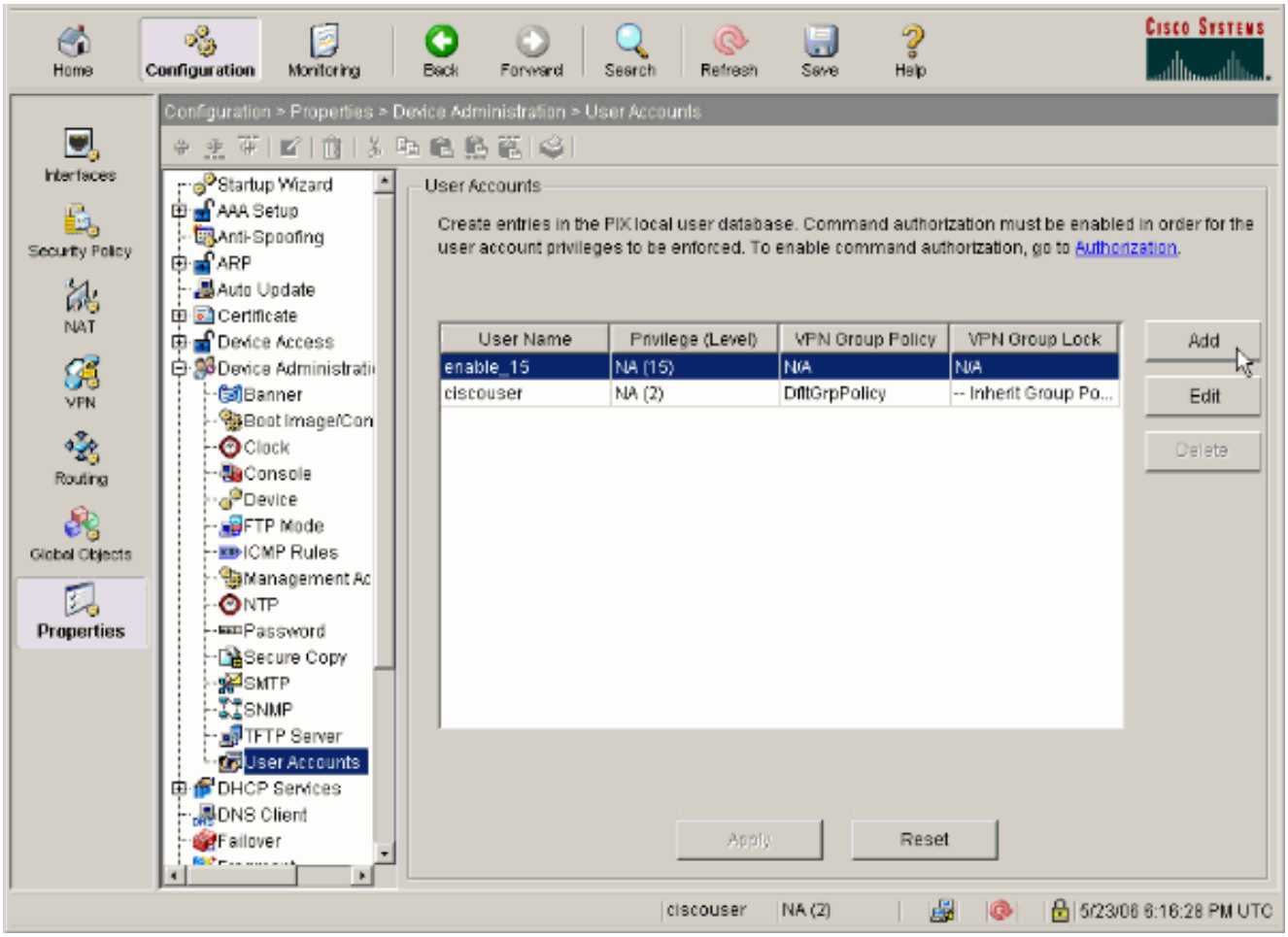
```
                                                inspect rtsp
                                               inspect skinny
                                                inspect esmtp
                                               inspect sqlnet
                                               inspect sunrpc
                                                 inspect tftp
                                                  inspect sip
                                                inspect xdmcp
                                                           !
                                       service-policy global_policy global
                                    Cryptochecksum:a6b05fd04f9fbd0a39f1ca7328de91f7
                                                        end :
```

ملاحظة: للوصول إلى واجهة إدارة ASA/PIX باستخدام SSH، قم بإصدار هذا الأمر: `SSH 172.16.16.160 255.255.255.255`

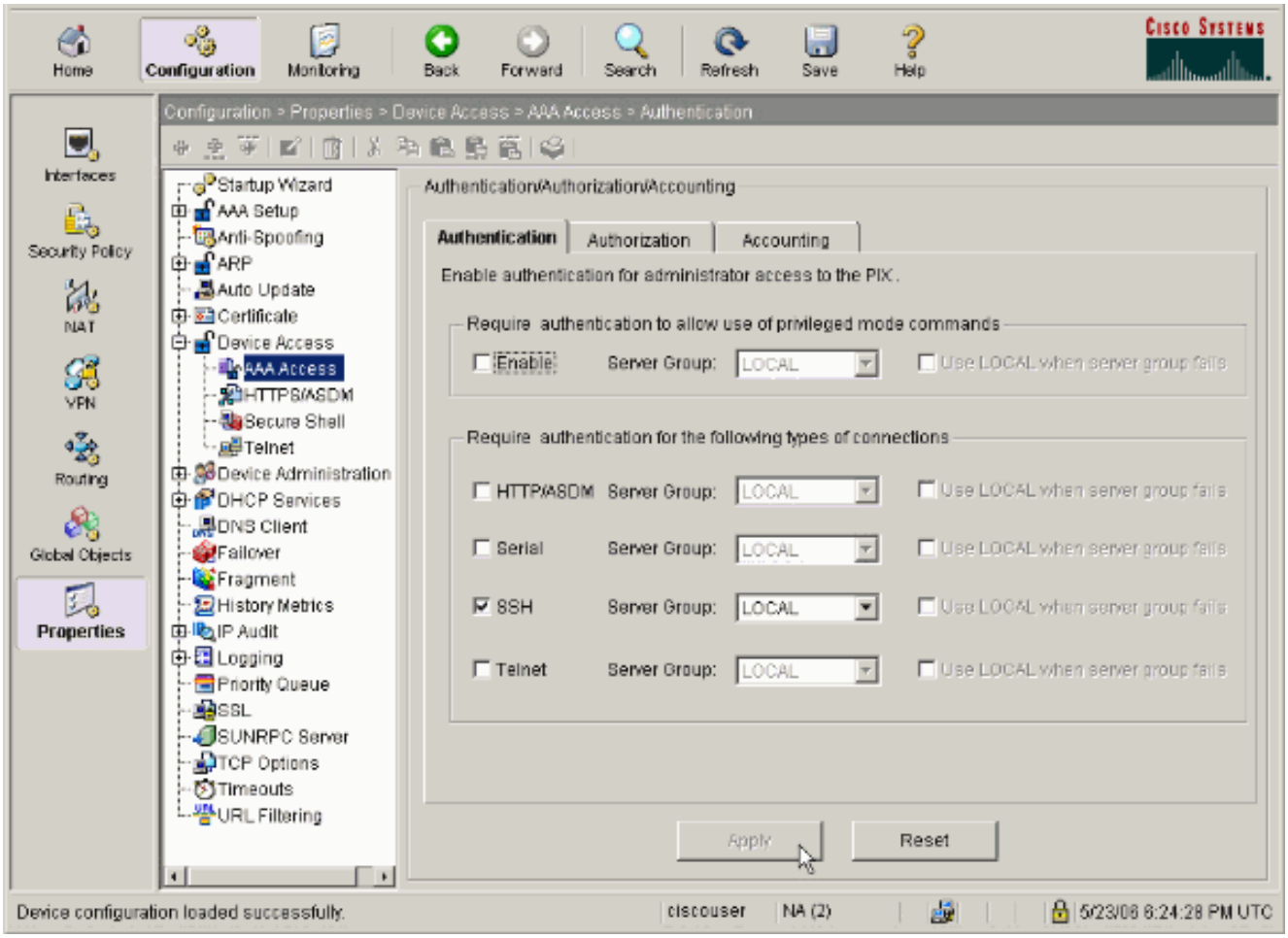
التكوين باستخدام ASDM 5.x

أكمل هذه الخطوات لتكوين الجهاز ل SSH باستخدام ASDM:

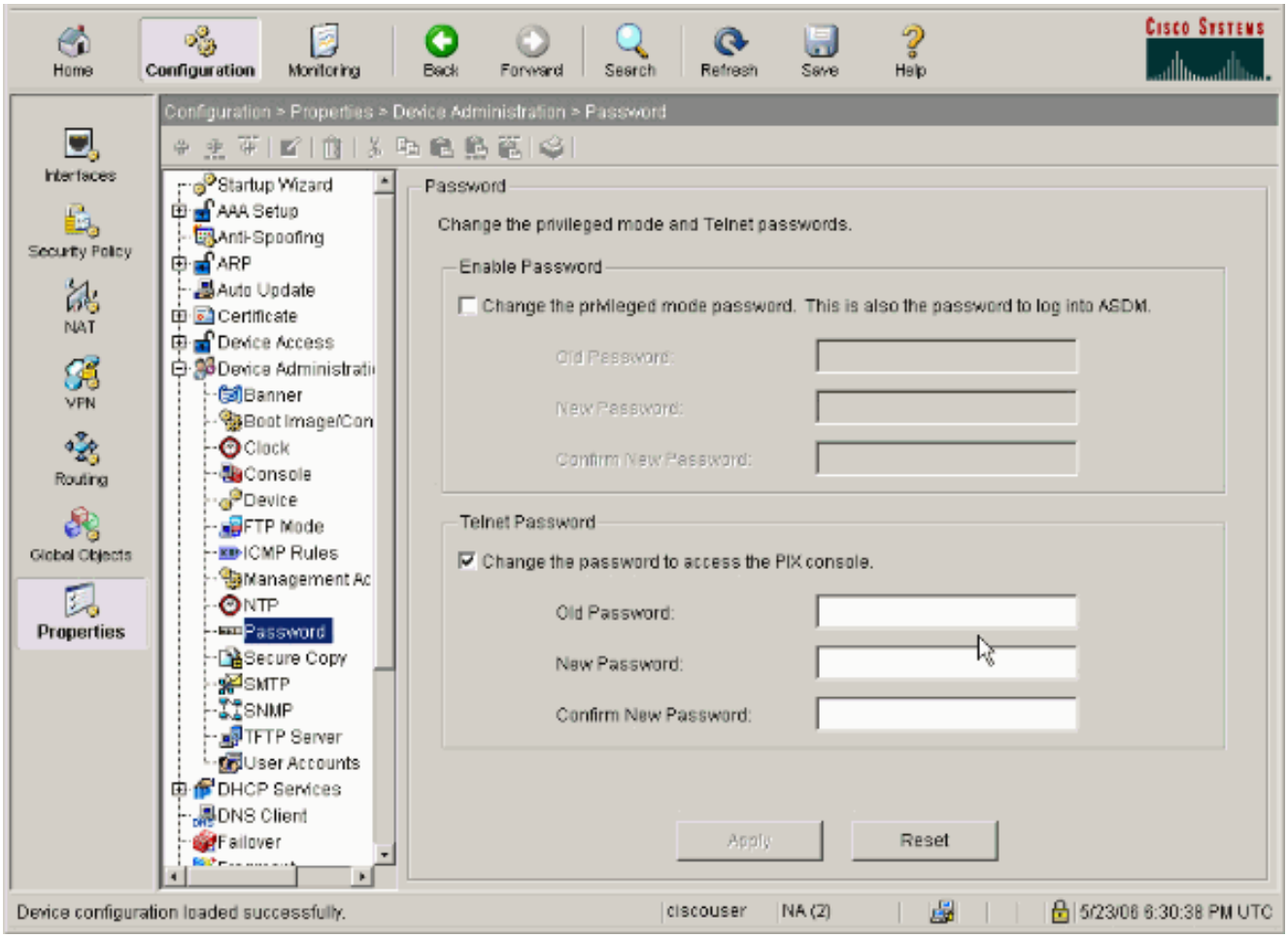
1. أخترت **تشكيل>خصائص>أداة إدارة>مستعمل حساب** in order to أضفت مستعمل مع ASDM.



2. أختر **تكوين > خصائص > وصول الجهاز > وصول AAA > مصادقة** لإعداد مصادقة AAA ل SSH باستخدام ASDM.

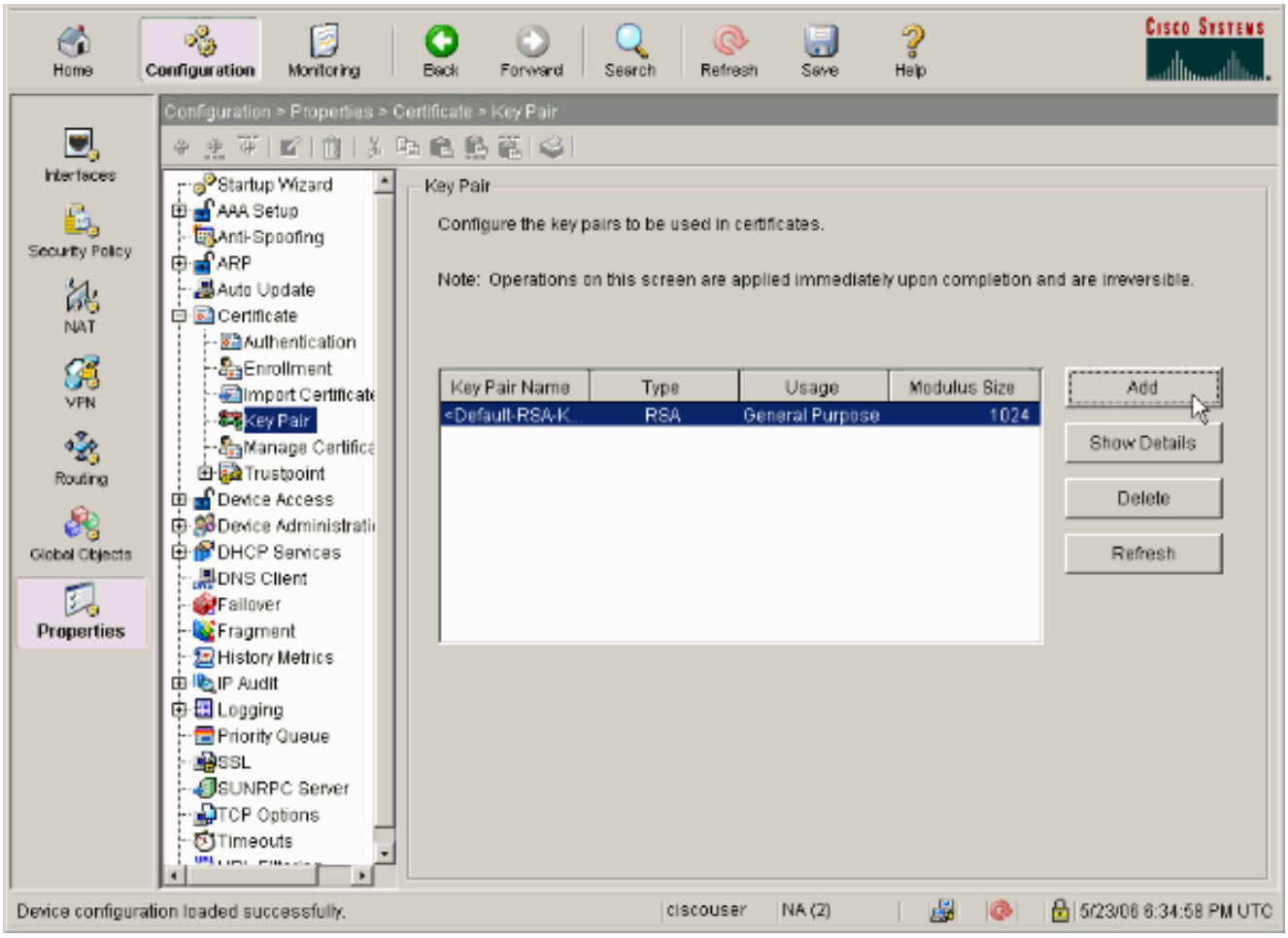


3. أخترت **تشكيل>خصائص>أداة إدارة>كلمة** in order to غيرت ال telnet كلمة مع ASDM.

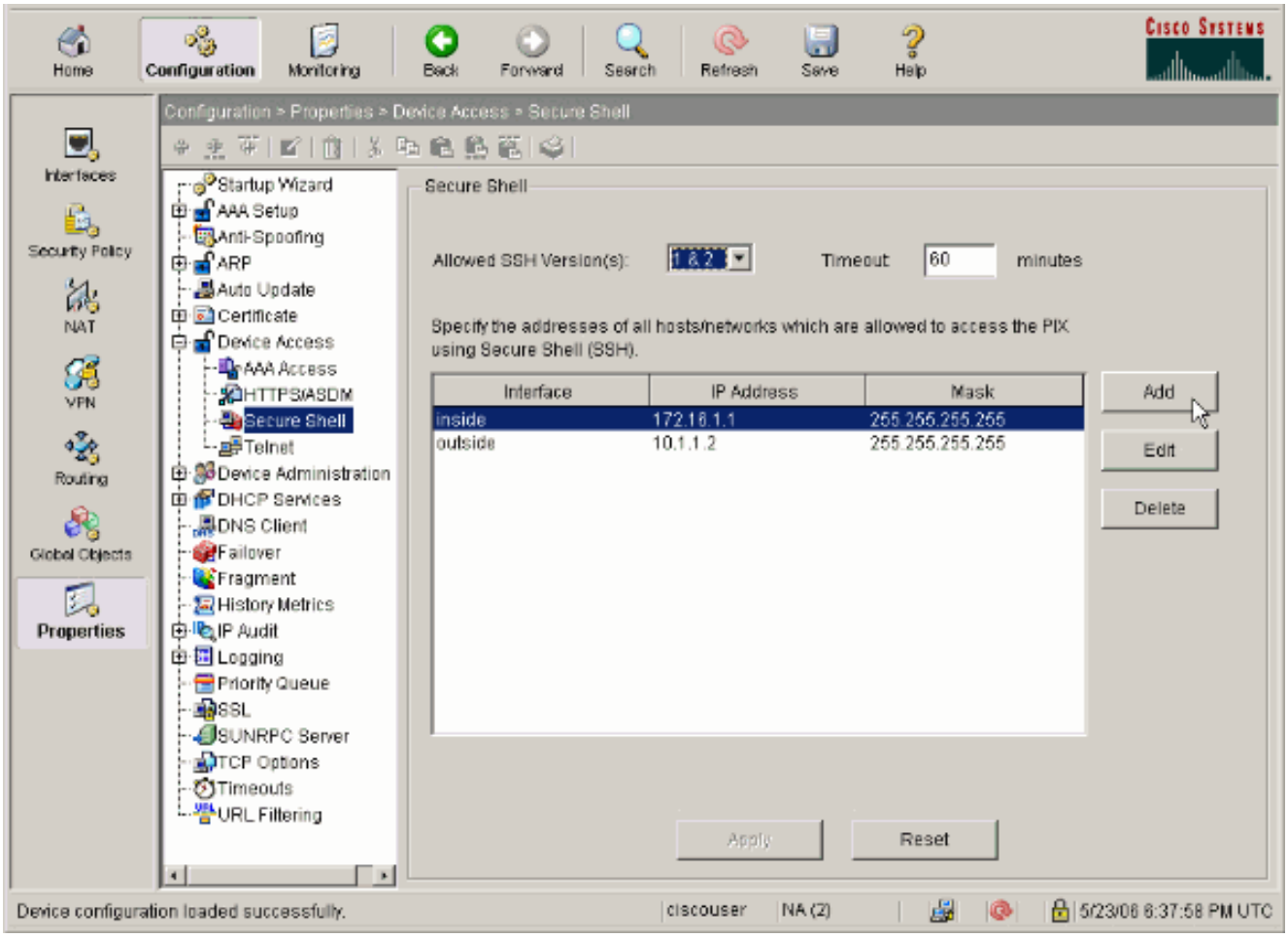


4. أختر **تكوين > خصائص > شهادة > زوج مفاتيح**، انقر فوق **إضافة** واستخدم الخيارات الافتراضية المقدمة لإنشاء

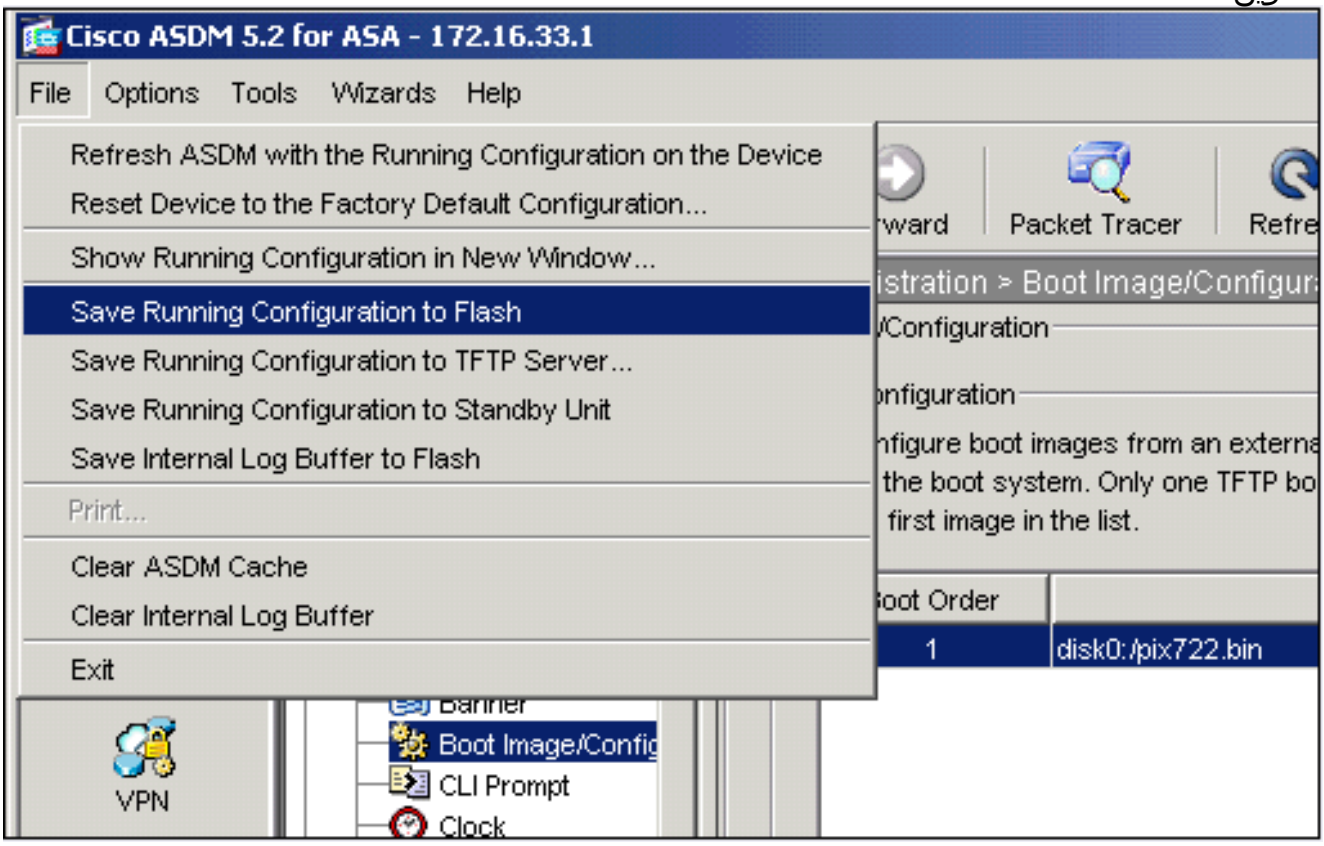
نفس مفاتيح RSA مع
.ASDM



5. أختر **تكوين > خصائص > الوصول إلى الجهاز > طبقة الأمان** لاستخدام ASDM لتحديد البيئات المضيفة المسموح لها بالاتصال ب SSH ولتحديد الإصدار وخيارات المهلة.



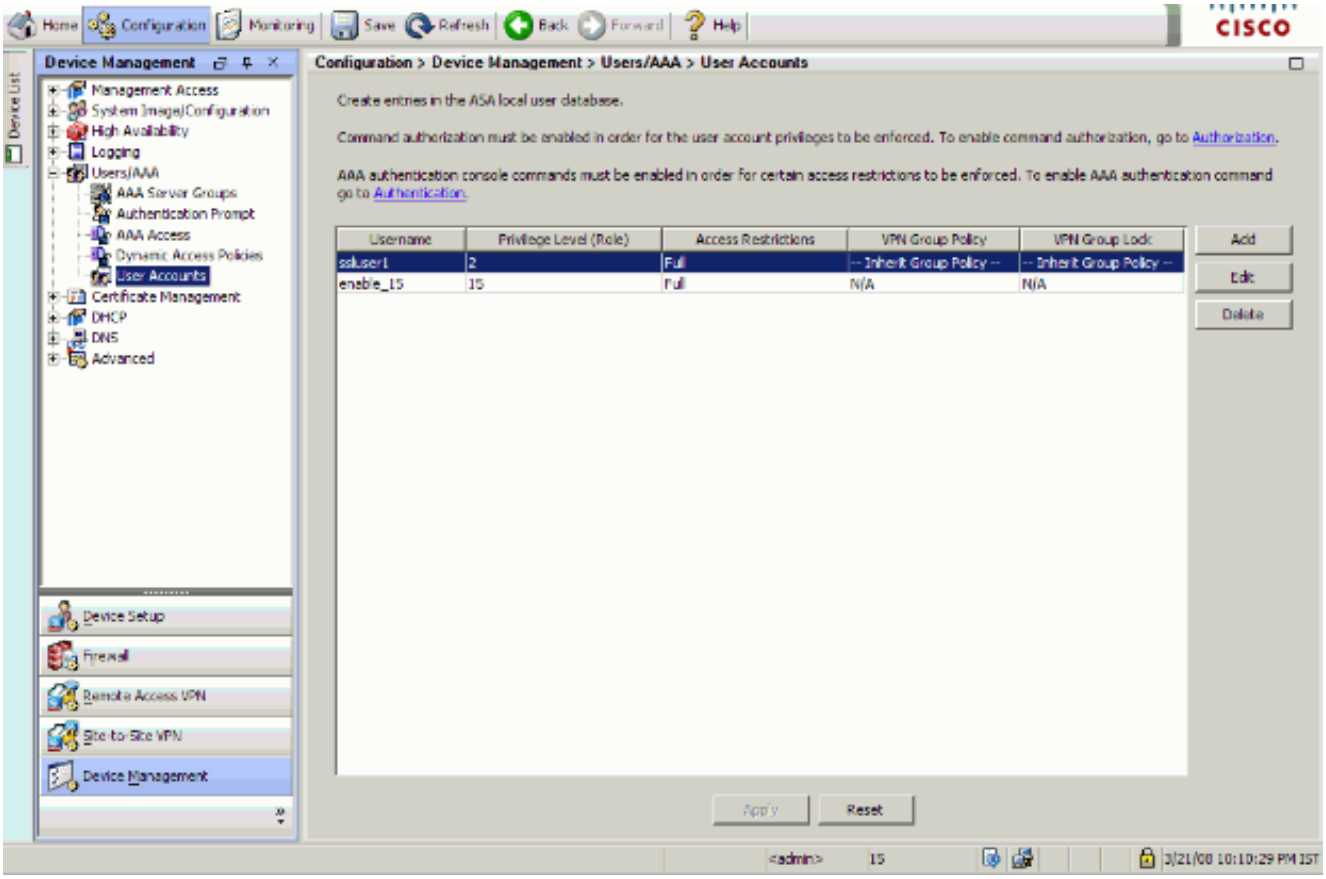
6. انقر فوق **ملف > حفظ التكوين الجاري تشغيله في Flash** لحفظ التكوين.



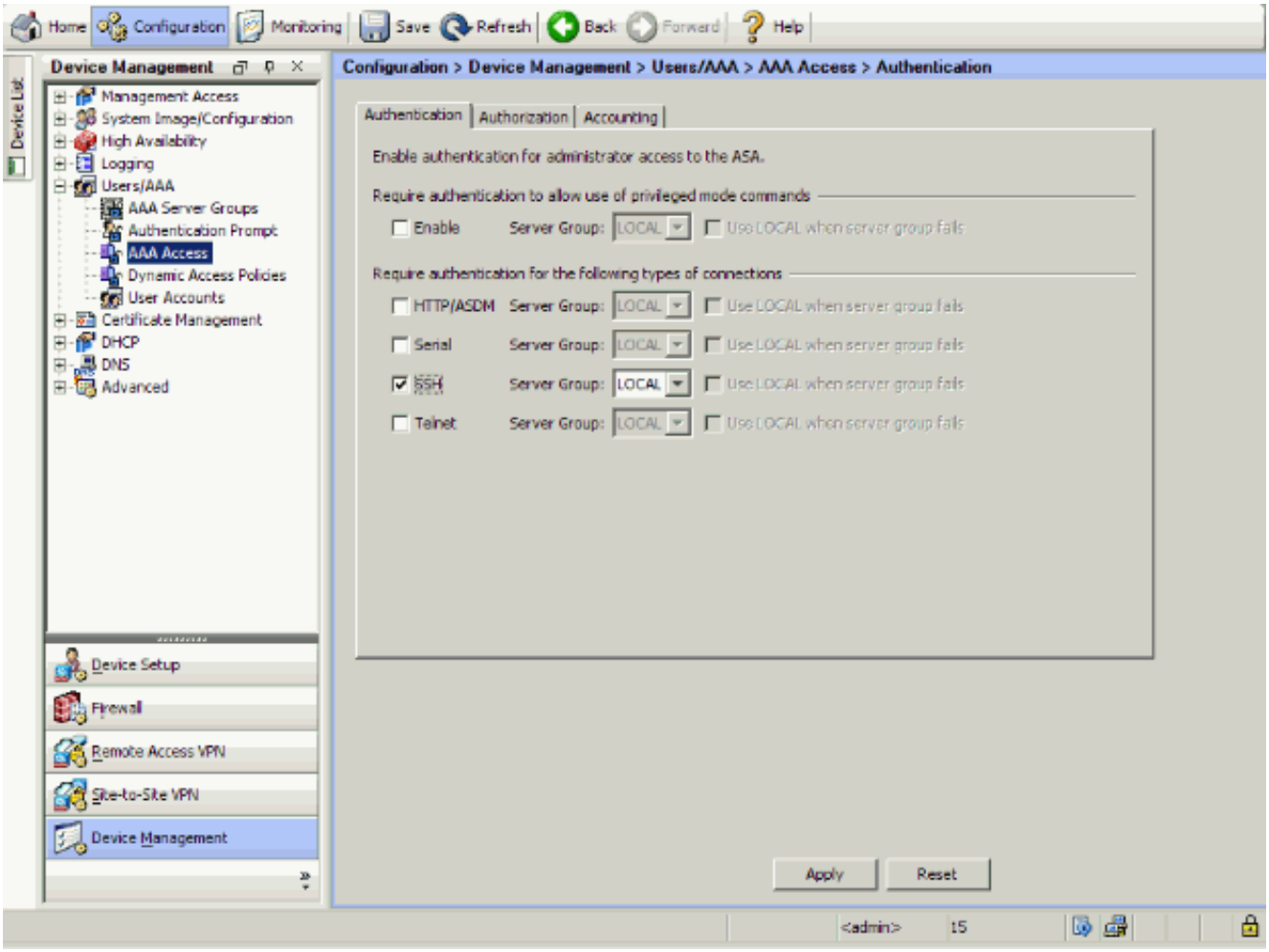
[التكوين باستخدام ASDM 6.x]

أكمل الخطوات التالية:

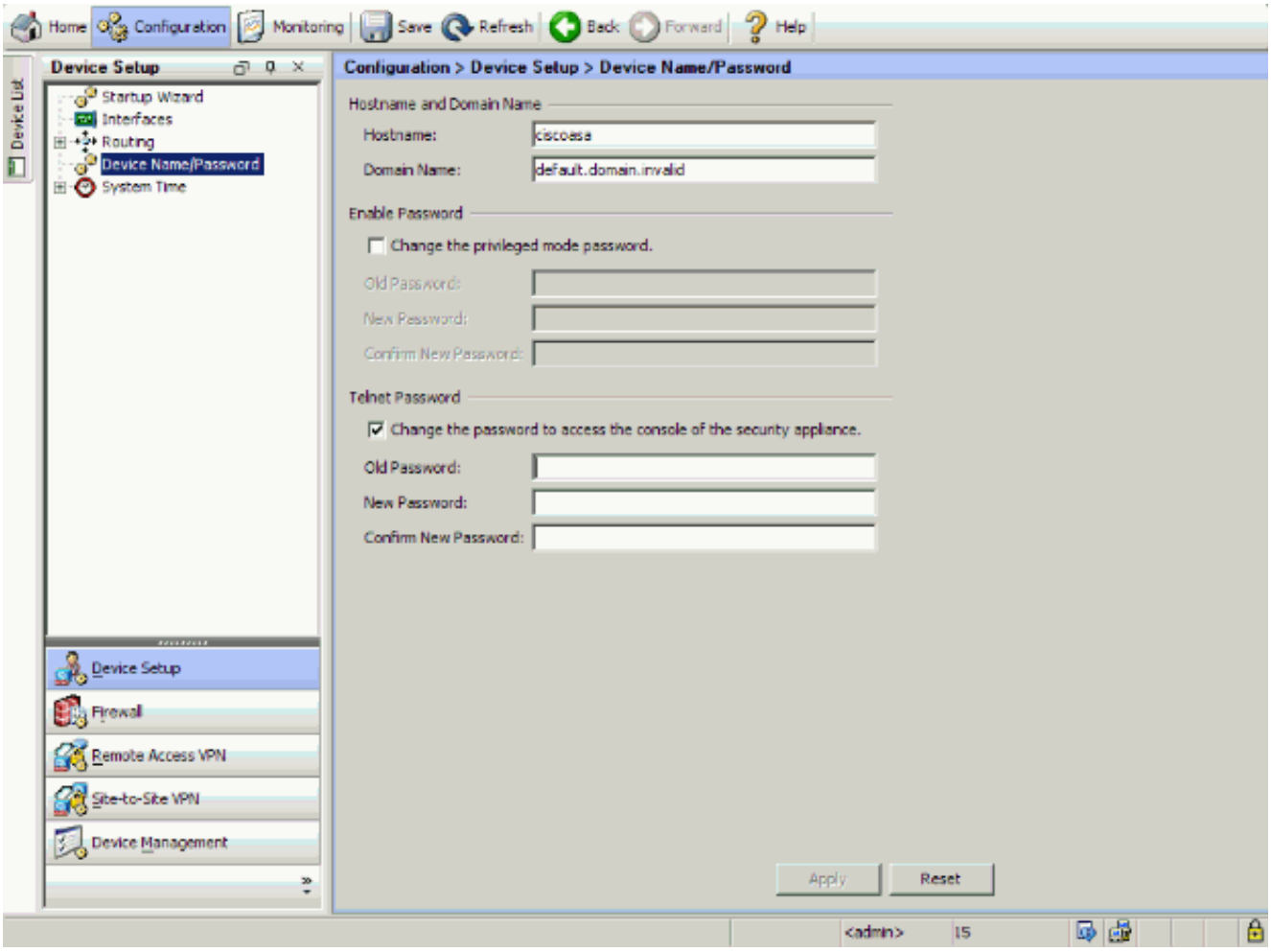
1. أخترت **تشكيل>أداة إدارة>مستعمل/AAA>مستعمل حساب** in order to أضفت مستعمل مع ASDM.



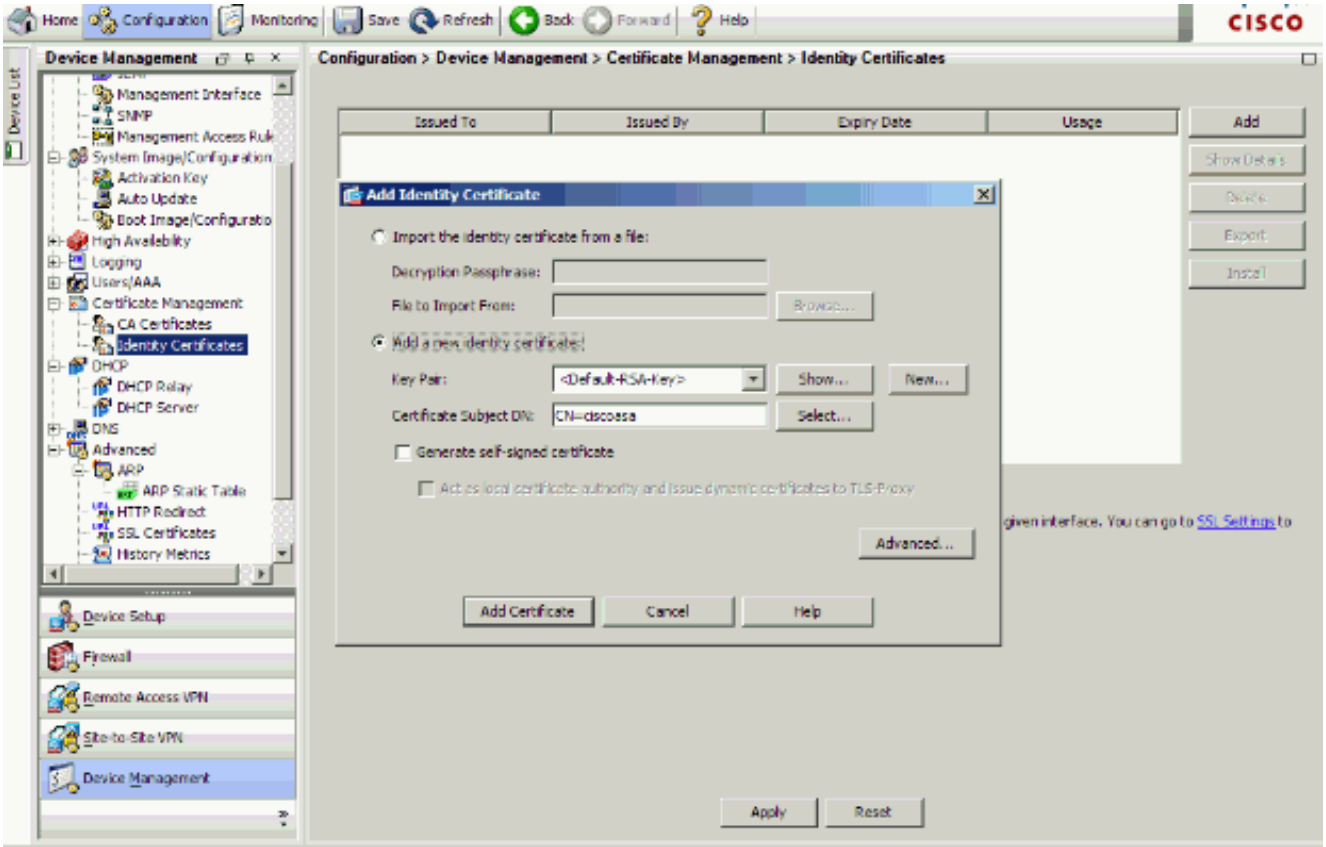
2. أختر **تكوين > إدارة الأجهزة > Users/AAA > الوصول إلى AAA > المصادقة** لإعداد مصادقة AAA ل SSH باستخدام ASDM.



3. أخترت **تشكيل>أداة setup>أداة إسم/كلمة** in order to غيرت ال telnet كلمة مع ASDM.

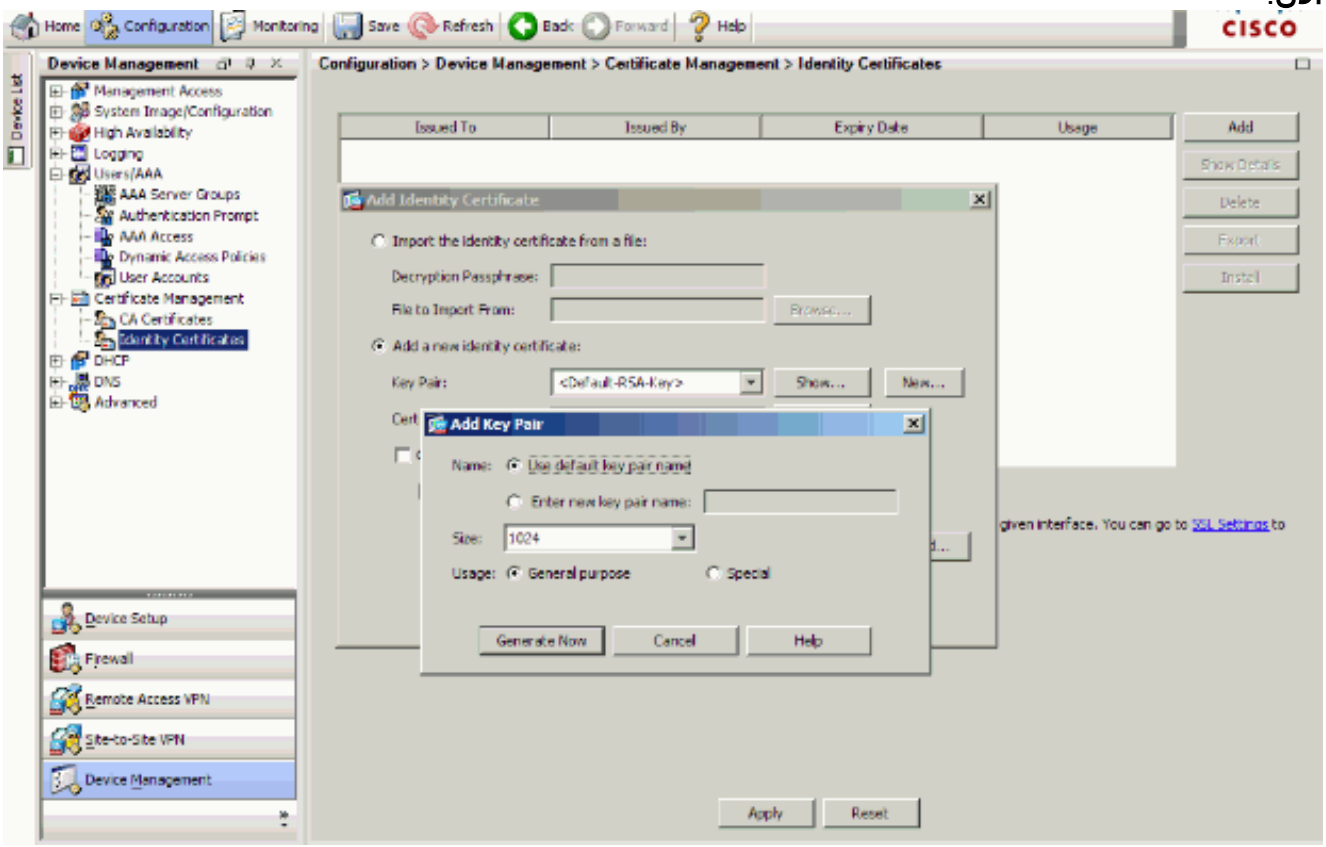


4. أختر **تكوين > إدارة الأجهزة > إدارة الشهادات > شهادات الهوية**، انقر فوق **إضافة** واستخدم الخيارات الافتراضية المقدمة لإنشاء نفس مفاتيح RSA مع ASDM.

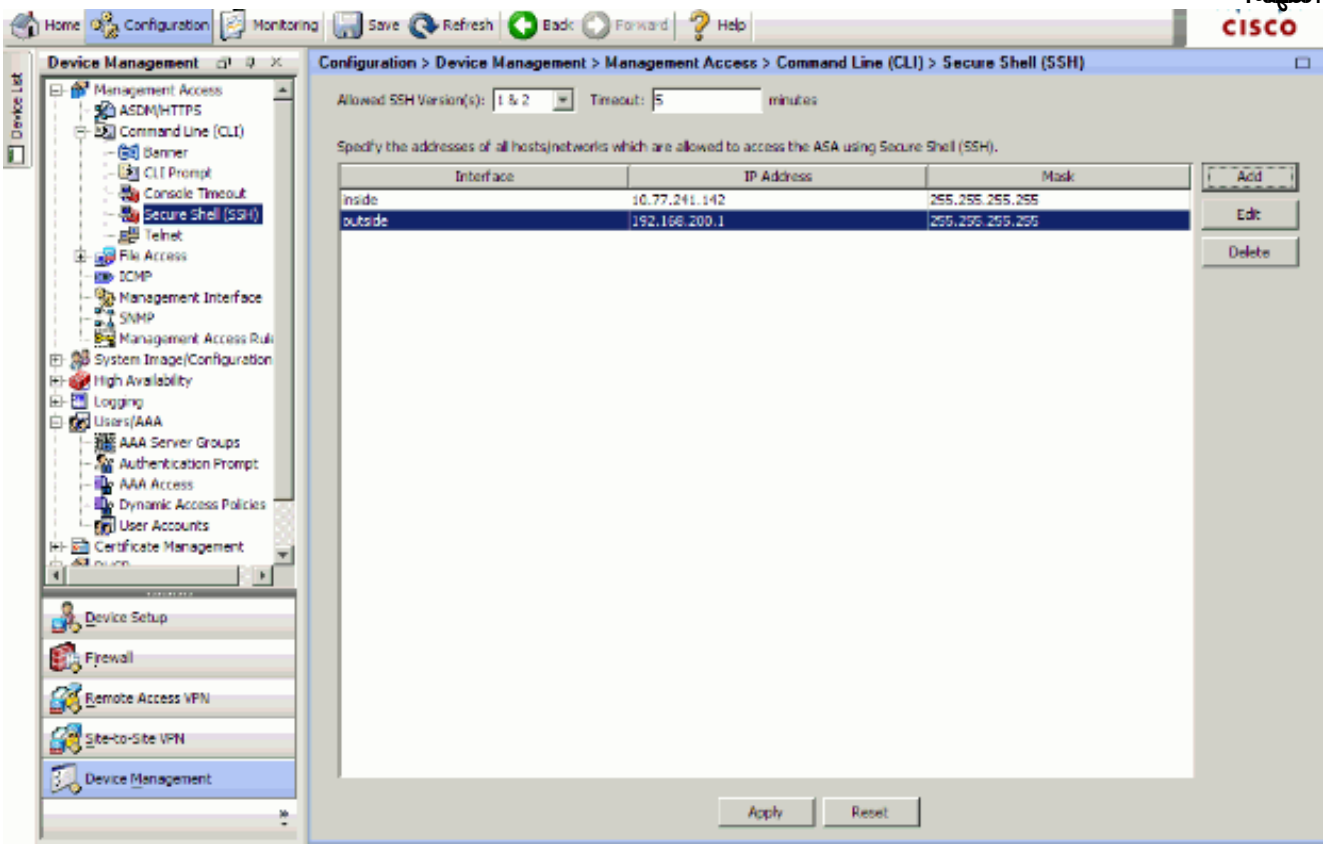


5. تحت **إضافة شهادة هوية جديدة** انقر على **جديد** لإضافة زوج مفاتيح افتراضي إذا لم يكن واحدا موجودا. بعد ذلك، انقر فوق **إنشاء**.

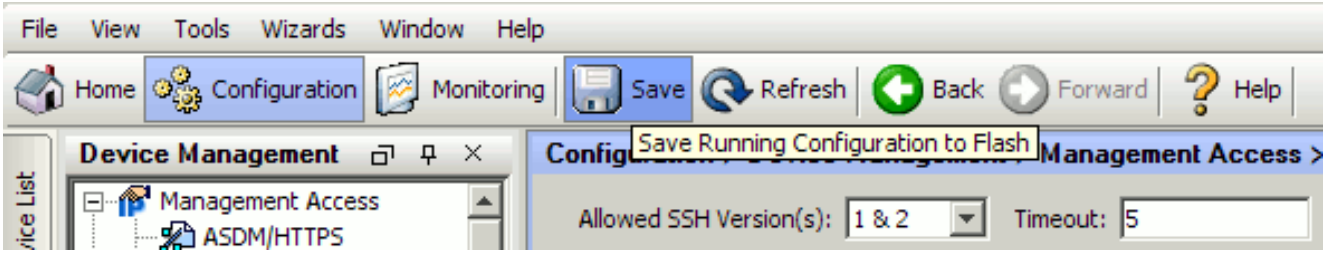
الآن.



6. أختر **تكوين > إدارة الأجهزة > الوصول إلى الإدارة > سطر الأوامر (CLI) > طبقة الأمان (SSH)** لاستخدام ASDM لتحديد البيئات المضيفة المسموح بها للاتصال ب SSH ولتحديد الإصدار وخيارات المهلة.



7. طقطقة **حفظ** فوق النافذة in order to أنقذت التشكيل.



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

تكوين Telnet

من أجل إضافة وصول Telnet إلى وحدة التحكم وتعيين مهلة الخمول، قم بإصدار الأمر **telnet** في وضع التكوين العام. 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
```

يتيح لك الأمر **telnet** تحديد البيئات المضيفة التي يمكنها الوصول إلى وحدة تحكم جهاز الأمان باستخدام برنامج Telnet.

ملاحظة: يمكنك تمكين Telnet على جهاز الأمان على جميع الواجهات. ومع ذلك، يفرض جهاز الأمان حماية جميع حركات مرور برنامج Telnet إلى الواجهة الخارجية بواسطة IPsec. لتمكين جلسة عمل برنامج Telnet إلى الواجهة الخارجية، قم بتكوين IPsec على الواجهة الخارجية لتضمين 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 0 أو أقل من أي واجهة أخرى، فلا يسمح PIX/ASA ل Telnet بهذه الواجهة.

ملاحظة: لا يوصى بالوصول إلى جهاز الأمان من خلال جلسة عمل على برنامج Telnet. يتم إرسال معلومات بيانات اعتماد المصادقة، مثل كلمة المرور، كنص واضح. لا يحدث اتصال خادم Telnet والعميل إلا مع النص الواضح. توصي Cisco باستخدام SSH لاتصال البيانات الأكثر أمانا.

إذا قمت بإدخال عنوان IP، فيجب عليك أيضا إدخال قناع الشبكة. لا يوجد قناع شبكة افتراضي. لا تستخدم قناع الشبكة الفرعية للشبكة الداخلية. قناع الشبكة هو قناع بت فقط لعنوان IP. لتحديد الوصول إلى عنوان IP واحد، أستخدم 255 في كل نظام ثماني؛ على سبيل المثال، 255.255.255.255.

إذا عمل IPsec، فيمكنك تحديد اسم واجهة غير آمن، وهو عادة الواجهة الخارجية. على الأقل، يمكنك تكوين الأمر **crypto map** لتحديد اسم واجهة باستخدام الأمر **telnet**.

أصدرت **الكلمة** أمر in order to ثبتت كلمة ل telnet منفذ إلى الوحدة طرفية للتحكم. الافتراضي هو Cisco. قم بإصدار الأمر **who** لعرض عناوين IP التي تصل حاليا إلى وحدة تحكم جهاز الأمان. قم بإصدار الأمر **kill** لإنهاء جلسة عمل لوحدة تحكم Telnet نشطة.

لتمكين جلسة عمل Telnet إلى الواجهة الداخلية، راجع الأمثلة التالية:

مثال 1

يسمح هذا المثال للمضيف 10.1.1.1 فقط بالوصول إلى وحدة تحكم جهاز الأمان من خلال برنامج Telnet:

```
pix(config)#telnet 10.1.1.1 255.255.255.255 inside
```

مثال 2

يسمح هذا المثال للشبكة 8/10.0.0.0 فقط بالوصول إلى وحدة تحكم جهاز الأمان من خلال برنامج Telnet:

```
pix(config)#telnet 10.0.0.0 255.0.0.0 inside
```

مثال 3

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

```
pix(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** للمطالبة بمصادقة وصول وحدة تحكم Telnet الأمنية ومهلة خروج 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 ثبت 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
```

دعم SSH/Telnet في ACS 4.x

إذا نظرت إلى وظائف RADIUS، فيمكنك إستخدام RADIUS لوظيفة SSH.

عند إجراء محاولة للوصول إلى جهاز الأمان باستخدام اتصال Telnet أو SSH أو HTTP أو اتصال وحدة تحكم تسلسلية ومطابقة حركة مرور البيانات لبيان المصادقة، يطلب جهاز الأمان اسم المستخدم وكلمة المرور. ثم يرسل بيانات الاعتماد هذه إلى خادم (ACS RADIUS)، ويمنح أو يرفض وصول CLI بناء على الاستجابة من الخادم.

راجع قسم خادم AAA ودعم قاعدة البيانات المحلية في تكوين خوادم AAA وقاعدة البيانات المحلية للحصول على مزيد من المعلومات.

على سبيل المثال، يحتاج جهاز أمان ASA 7.0 إلى عنوان IP يقبل جهاز الأمان منه الاتصالات، مثل:

```
hostname(config)#ssh source_IP_address mask source_interface
```

راجع قسم السماح بوصول SSH من تكوين خوادم AAA وقاعدة البيانات المحلية للحصول على مزيد من المعلومات.

ارجع إلى PIX/ASA: وكيل التوصيل البيني للوصول إلى الشبكة باستخدام TACACS+ ومثال تكوين خادم RADIUS للحصول على مزيد من المعلومات حول كيفية تكوين وصول SSH/Telnet إلى PIX باستخدام مصادقة ACS.

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استعملت ال OIT in order to شاهدت تحليل من **عرض** أمر إنتاج.

debug ssh

قم بإصدار الأمر **debug ssh** لتشغيل تصحيح أخطاء SSH.

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

يوضح هذا الإخراج أن طلب المصادقة من المضيف 10.1.1.2 (خارج إلى PIX) إلى "PIX" ناجح:

```
                                                                #pix
                                                .Device ssh opened successfully
                                  SSH0: SSH client: IP = '10.1.1.2' interface # = 1
                                                     SSH: host key initialised
                                               SSH0: starting SSH control process
                                    SSH0: Exchanging versions - SSH-1.99-Cisco-1.25
                                                SSH0: send SSH message: outdata is NULL
(server version string:SSH-1.99-Cisco-1.25SSH0: receive SSH message: 83 (83
   SSH0: client version is - SSH-1.99-3.2.0 SSH Secure Shell for Windows
     :client version string:SSH-1.99-3.2.0 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 receivedSSH(pix): user authen method is
                                                      no AAA', aaa server group ID = 0'
                      SSH(pix): user authen method is 'no AAA', aaa server group ID = 0
                                                SSH2 0: authentication successful for pix
Authentication for the PIX 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 أعطى مستخدم اسم مستخدم غير صحيح، على سبيل المثال، "PIX1" بدلا من "PIX"، فإن جدار حماية PIX يرفض المصادقة. يظهر إخراج تصحيح الأخطاء هذا المصادقة الفاشلة:

```
#pix
.Device ssh opened successfully
SSH0: SSH client: IP = '10.1.1.2' interface # = 1
SSH: host key initialised
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-1.99-Cisco-1.25
SSH0: send SSH message: outdata is NULL
(server version string:SSH-1.99-Cisco-1.25SSH0: receive SSH message: 83 (83
SSH0: client version is - SSH-1.99-3.2.0 SSH Secure Shell for Windows client version
string:SSH-1.99-3.2.0 SSH Secure Shell for WindowsSSH0: begin server key generation
SSH0: complete server key generation, elapsed time = 1960 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 receivedSSH(pix1): user authen method is
no AAA', aaa server group ID = 0'
SSH(pix1): user authen method is 'no AAA', aaa server group ID = 0
SSH2 0: authentication failed for pix1
.Authentication for pix1 was not successful due to the wrong username ---!
```

بالمثل، إذا قدم المستخدم كلمة المرور الخطأ، فإن مخرج تصحيح الأخطاء هذا يوضح لك المصادقة الفاشلة.

```
#pix
.Device ssh opened successfully
SSH0: SSH client: IP = '10.1.1.2'  interface # = 1
SSH: host key initialised
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-1.99-Cisco-1.25
:SSH0: send SSH message: outdata is NULL server version string
(SSH-1.99-Cisco-1.25SSH0: receive      SSH message: 83 (83
SSH0: client version is - SSH-1.99-3.2.0 SSH Secure Shell for
Windows client version string:SSH-1.99-3.2.0
SSH Secure Shell for WindowsSSH0: begin server key generation
SSH0: complete server key generation, elapsed time = 1920 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 receivedSSH(pix): user authen method
is 'no AAA', aaa server group ID = 0
SSH(pix): user authen method is 'no AAA', aaa server group ID = 0
SSH2 0: authentication failed for pixSSH(pix): user authen method
is 'no AAA', aaa server group ID = 0
SSH2 0: authentication failed for pix
.Authentication for PIX was not successful due to the wrong password ---!
```

عرض جلسات SSH النشطة

قم بإصدار هذا الأمر للتحقق من عدد جلسات عمل SSH المتصلة وحالة الاتصال ب PIX:

```
pix#show ssh session

SID Client IP       Version Mode Encryption Hmac     State            Username
     IN   aes128-cbc md5      SessionStarted   pix    1.99        10.1.1.2   0
     OUT  aes128-cbc md5      SessionStarted   pix
```

أختر **مراقبة > خصائص > الوصول إلى الجهاز > جلسات عمل Secure Shell** لعرض الجلسات باستخدام ASDM.

عرض مفتاح RSA العام

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

```
pix#show crypto key mypubkey rsa

Key pair was generated at: 19:36:28 UTC May 19 2006
<Key name: <Default-RSA-Key
Usage: General Purpose Key
 Modulus Size (bits): 1024
:Key Data

    30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00c172f4
    95f66c34 2c2ced37 aa3442d8 12158c93 131480dd 967985ab 1d7b92d9 5290f695
    8e9b5b0d d88c0439 6169184c d8fb951c 19023347 d6b3f939 99ac2814 950f4422
    69b67328 f64916b1 82e15341 07590da2 390fbefd 38758888 7319196c de61aef1
165c4bab 03d081d5 ddaf15cc c9ddb204 c2b451e0 f19ce0f3 485b1d69 8b020301 0001
```

أختر **تكوين > خصائص > شهادة > زوج مفاتيح**، وانقر فوق **إظهار التفاصيل** لعرض مفاتيح RSA مع ASDM.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

كيفية إزالة مفاتيح RSA من PIX

قد تتطلب حالات معينة، مثل عند ترقية برامج PIX أو تغيير إصدار SSH في PIX، إزالة مفاتيح RSA وإعادة إنشائها. أصدرت هذا أمر in order to أزلت ال RSA مفتاح زوج من ال PIX:

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

أختر **تكوين > خصائص > شهادة > زوج مفاتيح**، وانقر **حذف** لإزالة مفاتيح RSA مع ASDM.

فشل اتصال SSH

رسالة خطأ على PIX/ASA:

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

رسالة الخطأ المقابلة على جهاز عميل SSH:

```
Selected cipher type
```

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

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

أصدرت هذا أمر in order to خلقت المفتاح جديد:

```
ASA(config)# crypto key generate rsa modulus 1024
```

يتعذر الوصول إلى ASA مع SSH

رسالة الخطأ:

```
ssh_exchange_identification: read: Connection reset by peer
```

لحل هذه المشكلة، أكمل الخطوات التالية:

1. قم بإعادة تحميل ASA أو إزالة جميع التكوين المرتبط SSH ومفاتيح RSA.
2. قم بإعادة تكوين أوامر SSH وإعادة إنشاء مفاتيح RSA.

يتعذر الوصول إلى ASA الثانوي باستخدام SSH

عندما يكون ASA في وضع تجاوز الفشل، لا يمكن إستخدام SSH إلى ASA في وضع الاستعداد من خلال نفق VPN. وذلك لأن حركة مرور الرد على SSH تأخذ الواجهة الخارجية من ASA الاحتياطي.

معلومات ذات صلة

- أجهزة الأمان Cisco PIX 500 Series Security Appliances
- أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances
- برنامج جدار حماية Cisco PIX
- مراجع أوامر جدار حماية PIX الآمن من Cisco
- تكوين إتصالات SSH - موجهات Cisco ومحركات Cisco
- 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).