PIX 6.2: المصادقة أو الترخيص أو المحاسبة (AAA) مثال تكوين

المحتويات

المقدمة

تم إدخال تفويض أوامر PIX والتوسع في المصادقة المحلية في الإصدار 6.2. يقدم هذا المستند مثالا لكيفية إعداد هذا على PIX. لا تزال ميزات المصادقة المتوفرة مسبقا متوفرة ولكنها غير قابلة للمناقشة في هذا المستند (على سبيل المثال، Secure Shell (SSH) واتصال عميل IPsec من كمبيوتر شخصي وما إلى ذلك). قد يتم التحكم في الأوامر التي يتم تنفيذها محليا على PIX أو عن بعد من خلال TACACS+. تفويض أوامر RADIUS غير مدعوم، هذا حد لبروتوكول RADIUS.

يتم تفويض الأوامر المحلية عن طريق تعيين أوامر ومستخدمين إلى مستويات الامتيازات.

يتم تفويض الأوامر عن بعد من خلال خادم مصادقة TACACS+ والتخويل والمحاسبة (AAA). يمكن تعريف خوادم AAA المتعددة في حالة تعذر الوصول إلى واحد.

تعمل المصادقة أيضا مع إتصالات IPSec و SSH التي تم تكوينها مسبقا. تتطلب مصادقة SSH إصدار هذا الأمر:

```
aaa authentication ssh console <LOCAL | server_tag>
```

ملاحظة: إذا كنت تستخدم مجموعة خوادم TACACS+ أو RADIUS للمصادقة، فيمكنك تكوين PIX لاستخدام قاعدة البيانات المحلية كطريقة **إحتياطي** إذا كان خادم AAA غير متوفر.

على سبيل المثال

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

يمكنك بدلا من ذلك إستخدام قاعدة البيانات المحلية كطريقة أساسية للمصادقة (دون نسخ إحتياطي) إذا قمت بإدخال LOCAL وحده.

على سبيل المثال، قم بإصدار هذا الأمر لتحديد حساب مستخدم في قاعدة البيانات المحلية ولإجراء مصادقة محلية لاتصال SSH:

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

ارجع إلى كيفية إجراء المصادقة والتمكين على جدار حماية PIX الآمن من Cisco (من 5.2 إلى 6.2) للحصول على مزيد من المعلومات حول كيفية إنشاء وصول مصدق من قبل المصادقة والتفويض والمحاسبة (AAA) إلى جدار حماية PIX الذي يشغل برنامج PIX الإصدار 5.2 إلى 6.2 للحصول على مزيد من المعلومات حول تمكين المصادقة والتسلسل واكتساب الوصول عند تعطل خادم AAA.

ارجع إلى PIX/ASA: وكيل التوصيل البيني للوصول إلى الشبكة باستخدام TACACS+ ومثال تكوين خادم RADIUS للحصول على مزيد من المعلومات حول كيفية إنشاء وصول (وكيل التوصيل البيني (AAA) المصادق (Cut-through) إلى جدار حماية PIX الذي يشغل إصدارات برنامج PIX 6.3 والإصدارات الأحدث.

إذا تم إجراء التكوين بشكل صحيح، فيجب ألا تكون مؤمنا على PIX. إذا لم يتم حفظ التكوين، فيجب أن تقوم إعادة تمهيد PIX بإعادته إلى حالة التكوين المسبق الخاصة به. إذا لم يتم الوصول إلى PIX بسبب عدم التكوين، فارجع إلى إجراء إسترداد كلمة المرور واسترداد تكوين AAA ل PIX.

قبل البدء

الاصطلاحات

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

المتطلبات الأساسية

لا توجد متطلبات أساسية خاصة لهذا المستند.

المكونات المستخدمة

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

- برنامج PIX الإصدار 6.2
- مصدر المحتوى الإضافي الآمن من Cisco لنظام التشغيل Windows الإصدار 3.0 (ACS)
- Cisco Secure ACS ل CSUnix) UNIX)، الإصدار 2.3.6

تم إنشاء المعلومات المُقدمة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كنت تعمل في شبكة مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر قبل استخدامه.

الاختبار قبل إضافة المصادقة/التخويل

قبل تنفيذ ميزات المصادقة/التفويض الجديدة 6.2، تأكد من أنك قادر حاليا على الوصول إلى PIX باستخدام هذه الأوامر:

```
IP range allowed to Telnet to the PIX (values depend on network). telnet 172.18.124.0 ---!
255.255.255.0
<Telnet password. passwd <password ---!
<Enable password. enable password <password ---!
```

يفهم امتياز عملية إعداد

توجد معظم الأوامر في PIX في المستوى 15، على الرغم من أن بعضها في المستوى 0. لعرض الإعدادات الحالية لكل الأوامر، أستخدم هذا الأمر:

```
show privilege all
```

تكون معظم الأوامر في المستوى 15 بشكل افتراضي، كما هو موضح في هذا المثال:

```
privilege configure level 15 command route
```

توجد بعض الأوامر في المستوى 0، كما هو موضح في هذا المثال:

```
privilege show level 0 command curpriv
```

يمكن أن يعمل PIX في أوضاع التمكين والتكوين. تتوفر بعض الأوامر، مثل **show logging** ، في كلا الوضعين. لتعيين امتيازات على هذه الأوامر، يجب عليك تحديد الوضع الذي يوجد فيه الأمر، كما هو موضح في المثال. الآخر أسلوب خيار **enable**. تحصل على رسالة خطأ . إن لا يشكل أنت الأسلوب، استعملت **الأسلوب [enable|configure]** أمر:

```
privilege show level 5 mode configure command logging
```

تعالج هذه الأمثلة أمر **الساعة**. أستخدم هذا الأمر لتحديد الإعدادات الحالية لأمر **الساعة**:

```
show privilege command clock
```

يظهر إخراج أمر ساعة **أمر عرض الامتيازات** أن أمر **الساعة** موجود في هذه التنسيقات الثلاثة:

```
.Users at level 15 can use the show clock command ---!
```

```
privilege show level 15 command clock
.Users at level 15 can use the clear clock command ---!

Privilege clear level 15 command clock
Users at level 15 can configure the clock !--- (for example, clock set 12:00:00 Jan 01 ---!
.(2001

privilege configure level 15 command clock
```

المصادقة/التفويض - أسماء المستخدمين المحليين

قبل تغيير مستوى الامتياز لأمر **الساعة**، يجب الانتقال إلى منفذ وحدة التحكم لتكوين مستخدم إداري وتشغيل مصادقة تسجيل الدخول المحلية، كما هو موضح في هذا المثال:

```
GOSS(config)# username poweruser password poweruser privilege 15
GOSS(config)# aaa-server LOCAL protocol local
GOSS(config)# aaa authentication telnet console LOCAL
```

يؤكد PIX إضافة المستخدم، كما هو موضح في هذا المثال:

```
:GOSS(config)# 502101: New user added to local dbase
Uname: poweruser Priv: 15 Encpass: Nimjl8wRa7VAmpm5
```

يجب أن يكون المستخدم "poweruser" قادرا على إستخدام Telnet في PIX والتمكين باستخدام كلمة مرور تمكين PIX المحلي الموجود (الكلمة من الأمر **enable password <*password*>**).

يمكنك إضافة المزيد من الأمان بإضافة مصادقة للتمكين، كما هو موضح في هذا المثال:

```
GOSS(config)# aaa authentication enable console LOCAL
```

يتطلب هذا من المستخدم إدخال كلمة المرور لكل من تسجيل الدخول والتمكين. في هذا مثال، استعملت الكلمة "poweruser" لكل من login وتمكين. يجب أن يكون المستخدم "poweruser" قادرا على إستخدام Telnet في PIX كما يجب تمكينه باستخدام كلمة مرور PIX المحلية.

إذا كنت تريد أن يتمكن بعض المستخدمين من إستخدام أوامر معينة فقط، فعليك إعداد مستخدم بامتيازات أقل، كما هو موضح في هذا المثال:

```
GOSS(config)# username ordinary password ordinary privilege 9
```

بما أن كل الأوامر الخاصة بك تقريبا هي في المستوى 15 بشكل افتراضي، يجب عليك نقل بعض الأوامر إلى المستوى 9 حتى يتمكن المستخدمون "العاديون" من إصدارها. في هذا المثال، تريد أن يكون مستخدم المستوى 9 قادرا على إستخدام الأمر **show clock**، ولكن ليس لإعادة تكوين الساعة، كما هو موضح في هذا المثال:

```
GOSS(config)# privilege show level 9 command clock
```

تحتاج أيضا إلى أن يكون المستخدم قادرا على تسجيل الخروج من PIX (قد يكون المستخدم في المستوى 1 أو 9 عند رغبته في القيام بذلك)، كما هو موضح في هذا المثال:

```
GOSS(config)# privilege configure level 1 command logout
```

أنت تحتاج أن يكون المستخدم قادرا على إستخدام الأمر **enable** (المستخدم في المستوى 1 عند محاولة هذا)، كما هو موضح في هذا المثال:

```
GOSS(config)# privilege configure level 1 mode enable command enable
```

بنقل الأمر **disable** إلى المستوى 1، يمكن لأي مستخدم بين المستويات 2-15 الخروج من وضع التمكين، كما هو موضح في هذا المثال:

```
GOSS(config)# privilege configure level 1 command disable
```

إن يستعمل أنت Telnet ك المستعمل "عادي" ويمكن بما أن ال نفسه مستعمل (الكلمة يكون أيضا "عادي")، أنت سوفت استعملت **الامتياز يشكل مستوى 1 أمر يعجز**، كما هو موضح في هذا مثال:

```
GOSS# show curpriv
Username : ordinary
Current privilege level : 9
Current Mode/s : P_PRIV
```

إذا كان لا يزال لديك جلسة العمل الأصلية مفتوحة (الجلسة السابقة لإضافة أي مصادقة)، فقد لا يعرف PIX من تكون لأنك لم تقم بتسجيل الدخول باستخدام اسم المستخدم في البداية. إذا كان هذا هو الحال، فاستخدم الأمر **debug** لعرض رسائل حول المستخدم "enable_15" أو "enable_1" إذا لم يكن هناك اسم مستخدم مقترن. لذلك، يدخل Telnet في PIX على أنه المستخدم "poweruser" (المستخدم "المستوى 15") قبل تكوين تفويض الأوامر، لأنك بحاجة إلى التأكد من أن PIX يمكن أن يربط اسم مستخدم بالأوامر التي يتم محاولة القيام بها. أنت جاهز لاختبار تفويض الأوامر باستخدام هذا الأمر:

```
GOSS(config)# aaa authorization command LOCAL
```

يجب أن يكون المستخدم "poweruser" قادرا على إستخدام Telnet في جميع الأوامر وتمكينها وتنفيذها. يجب أن يكون المستخدم "عادي" قادرا على إستخدام أوامر **show clock** و**enable** و**disable** و**تسجيل الخروج**، ولكن لا يوجد آخرون، كما هو موضح في هذا المثال:

```
GOSS# show xlate
Command authorization failed
```

المصادقة/التفويض باستخدام خادم AAA

يمكنك أيضا مصادقة المستخدمين وتخويلهم باستخدام خادم AAA. يعمل TACACS+ بشكل أفضل لأن تفويض الأوامر ممكن، ولكن يمكن إستخدام RADIUS أيضا. تحقق لمعرفة ما إذا كانت هناك أوامر AAA Telnet/Console سابقة على PIX (في حالة إستخدام أمر **AAA المحلي** مسبقا)، كما هو موضح في هذا المثال:

```
GOSS(config)# show aaa
AAA authentication telnet console LOCAL
AAA authentication enable console LOCAL
AAA authorization command LOCAL
```

إذا كانت هناك أوامر AAA Telnet/وحدة التحكم السابقة، فقم بإزالتها باستخدام الأوامر التالية:

```
GOSS(config)# no aaa authorization command LOCAL
GOSS(config)# no aaa authentication telnet console LOCAL
GOSS(config)# no aaa authentication enable console LOCAL
```

كما هو الحال مع تكوين المصادقة المحلية، قم بالاختبار للتأكد من أنه يمكن للمستخدمين إستخدام Telnet في PIX باستخدام هذه الأوامر.

```
telnet 172.18.124.0 255.255.255.0
<IP range allowed to telnet to the PIX (values would depend on network). passwd <password ---!
<Telnet password. Enable password <password ---!
.Enable password ---!
```

وفقا للخادم الذي تستخدمه، قم بتكوين PIX للمصادقة/التفويض باستخدام خادم AAA.

ACS - TACACS+

قم بتكوين ACS للاتصال ب PIX عن طريق تحديد PIX في تكوين الشبكة باستخدام "المصادقة باستخدام" TACACS+ (لبرنامج Cisco IOS®). يعتمد تكوين مستخدم ACS على تكوين PIX. يجب على مستخدم ACS إعداد اسم مستخدم وكلمة مرور كحد أدنى.

على ال PIX، استعملت هذا أمر:

```
GOSS(config)# enable password cisco123
+GOSS(config)# aaa-server TACSERVER protocol tacacs
GOSS(config)# aaa-server TACSERVER (inside) host   timeout 10
GOSS(config)# aaa authentication telnet console TACSERVER
```

عند هذه النقطة، يجب أن يكون مستخدم ACS قادرا على إستخدام Telnet في PIX، وتمكينه باستخدام كلمة مرور التمكين الموجودة على PIX، وتنفيذ جميع الأوامر. أكمل الخطوات التالية:

1. إذا كانت هناك حاجة إلى تمكين مصادقة PIX باستخدام ACS، أختر **تكوين الواجهة > إعدادات TACACS+ المتقدمة**.
2. حدد **ميزات TACACS+ المتقدمة في** مربع **خيارات التكوين المتقدمة**.
3. انقر على **إرسال**. تظهر الآن إعدادات TACACS+ المتقدمة تحت تكوين المستخدم.
4. تعيين الحد الأقصى للامتياز لأي عميل AAA إلى المستوى 15.
5. أخترت ال enable كلمة نظام للمستخدم (أي يستطيع تضمنت يشكل منفصل enable كلمة).
6. انقر على **إرسال**.

لتشغيل تمكين المصادقة من خلال TACACS+ في PIX، أستخدم هذا الأمر:

```
GOSS(config)# aaa authentication enable console TACSERVER
```

عند هذه النقطة، يجب أن يكون مستخدم ACS قادرا على إستخدام Telnet في PIX والتمكين باستخدام كلمة مرور enable التي تم تكوينها في ACS.

قبل إضافة تفويض أوامر PIX، يجب تصحيح ACS 3.0. يمكنك تنزيل التصحيح من مركز البرامج (للعملاء المسجلين فقط). يمكنك أيضا عرض معلومات إضافية حول هذا التصحيح بالوصول إلى معرف تصحيح الأخطاء من Cisco CSCdw78255 (للعملاء المسجلين فقط).

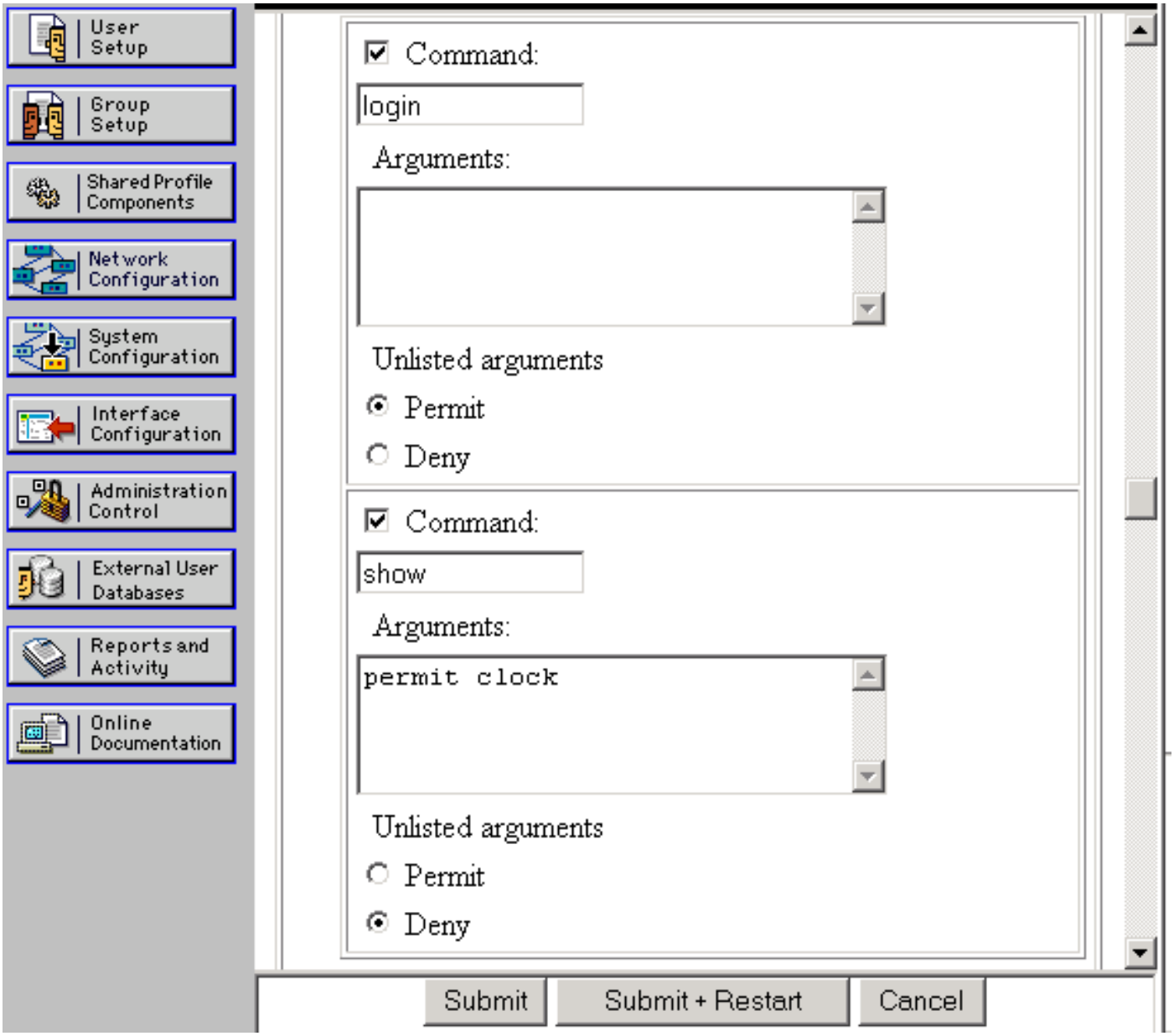
يجب أن تعمل المصادقة قبل القيام بتفويض الأوامر. إذا كانت هناك حاجة لتنفيذ تفويض الأوامر باستخدام ACS، أختر **تكوين الواجهة > Shell (EXEC) (TACACS+ (Cisco) للمستخدم و/أو المجموعة** وانقر فوق **إرسال**. تظهر إعدادات تفويض أمر shell الآن ضمن تكوين المستخدم (أو المجموعة).

من الأفضل إعداد مستخدم ACS واحد فعال على الأقل لتفويض الأوامر والسماح بأوامر Cisco IOS غير المتطابقة.

يمكن إعداد مستخدمي ACS الآخرين باستخدام تفويض الأوامر عن طريق السماح بمجموعة فرعية من الأوامر. يستخدم هذا المثال الخطوات التالية:

1. أختر إعدادات المجموعة للعثور على المجموعة المطلوبة من المربع المنسدل.
2. طقطقة **يحرر عملية إعداد**.
3. أختر **مجموعة تفويض أوامر Shell**.
4. انقر زر **الأمر**.
5. أدخل **تسجيل الدخول**.
6. أختر السماح تحت الوسيطات غير المدرجة.
7. كرر هذه العملية لأوامر **تسجيل الخروج** و**enable** و**disable**.
8. أختر مجموعة تخويل أوامر Shell.
9. انقر زر **الأمر**.
10. **برنامج Entershow**.
11. تحت الوسيطات ، أدخل **ساعة السماح**.
12. أختر رفض للوسيطات غير المدرجة.
13. انقر على **إرسال**.

فيما يلي مثال على هذه الخطوات:



إذا كان لا يزال لديك جلسة عمل أصلية مفتوحة (جلسة العمل السابقة لإضافة أي مصادقة)، فقد لا يعرف PIX من تكون لأنك لم تقم بتسجيل الدخول في البداية باستخدام اسم مستخدم ACS. إذا كان هذا هو الحال، فاستخدم الأمر **debug** لعرض رسائل حول المستخدم "enable_15" أو "enable_1" إذا لم يكن هناك اسم مستخدم مقترن. تحتاج إلى التأكد من أنه يمكن ل PIX إرفاق اسم مستخدم بالأوامر التي يتم محاولة تنفيذها. يمكنك تنفيذ هذا الإجراء من خلال إنشاء شبكة عن بعد في PIX كمستخدم مستوى 15 ACS قبل تكوين تفويض الأوامر. أنت جاهز لاختبار تفويض الأوامر باستخدام هذا الأمر:

```
aaa authorization command TACSERVER
```

عند هذه النقطة، يجب أن يكون لديك مستخدم واحد يمكنه إستخدام كافة الأوامر من Telnet وتمكينها واستخدامها، ومستخدم ثان يمكنه تنفيذ خمسة أوامر فقط.

+CSUnix - TACACS

قم بتكوين CSUnix للاتصال ب PIX كما تفعل مع أي جهاز شبكة آخر. يعتمد تكوين مستخدم CSUnix على تكوين PIX. يجب إعداد مستخدم CSUnix على أقل تقدير باستخدام اسم مستخدم وكلمة مرور. في هذا المثال، تم إعداد ثلاثة مستخدمين:

```
        This is our "poweruser" who can enable, use all commands, and log in. !--- The login ---!
      password is in the 'clear "*********"' statement. !--- The enable password is in the 'clear
          "*********" 15' statement. user = pixtest{ password = clear "*********" privilege = clear
"*********" 15 service=shell { default cmd=permit default attribute=permit } } !--- This user can
Telnet in, enable, and use four commands !--- (such as show clock, logout, exit, and enable). !-
-- The login password is in the 'clear "*********"' statement. !--- The enable password is in the
                                                          .'clear "*********" 15' statement

                                                                        }user = limitpix
                                                             "*********" password = clear
                                                          privilege = clear "*********" 15
                                                                        } service=shell
                                                                             } cmd=show
                                                                      "permit "clock
                                                                                    {
                                                                        } cmd=logout
                                                                         "*." permit
                                                                                    {
                                                                        } cmd=enable
                                                                         "*." permit
                                                                                    {
                                                                         } cmd=exit
                                                                        "*." permit
                                                                                    {
                                                                                    {
                                                                                    {

 This user can Telnet in, but not enable. This user can use any !--- show commands in non- ---!
                                                                  .? enable mode as well as logout, exit, and

                                                                         }user = oneuser
                                                                "*********" password = clear
                                                                         } service=shell
                                                                              } cmd=show
                                                                         "*." permit
                                                                                    {
                                                                        } cmd=logout
                                                                         "*." permit
                                                                                    {
                                                                          } "?"=cmd
                                                                         "*." permit
                                                                                    {
                                                                         } cmd=exit
                                                                        "*." permit
                                                                                    {
                                                                                    {
                                                                                    {
```

على ال PIX، استعملت هذا أمر:

```
                                                        GOSS(config)# enable password cisco123
                                                    +GOSS(config)# aaa-server TACSERVER protocol tacacs
                                                       GOSS(config)# aaa-server TACSERVER (inside) host
```

```
                                                    GOSS(config)# aaa authentication telnet console TACSERVER
```

عند هذه النقطة، يجب أن يكون أي من مستخدمي CSUnix قادرا على إستخدام Telnet في PIX، والتمكين باستخدام كلمة مرور التمكين الموجودة على PIX، واستخدام جميع الأوامر.

تمكين المصادقة من خلال TACACS+ في PIX:

```
GOSS(config)# aaa authentication enable console TACSERVER
```

عند هذه النقطة، يجب أن يتمكن مستخدمو CSUnix الذين لديهم كلمات مرور "الامتياز 15" من إستخدام Telnet في PIX والتمكين باستخدام كلمات المرور "enable" هذه.

إذا كانت جلسة العمل الأصلية ما زالت مفتوحة (جلسة قبل إضافة أي مصادقة)، فقد لا يعرف PIX من أنت لأنه لم تقم بتسجيل الدخول باستخدام اسم المستخدم في البداية. إذا كان هذا هو الحال، فإن إصدار الأمر **debug** قد يظهر رسائل حول المستخدم "enable_15" أو "enable_1" إذا لم يكن هناك اسم مستخدم مقترن. يدخل Telnet في PIX كمستخدم "pixtest" (المستخدم "من المستوى 15") قبل تكوين تفويض الأوامر، لأننا نحتاج إلى التأكد من أن PIX يمكن أن يربط اسم مستخدم بالأوامر التي يتم تجربتها. يجب أن يكون تمكين المصادقة قيد التشغيل قبل إجراء تفويض الأوامر. إذا كانت هناك حاجة لتنفيذ تفويض الأوامر باستخدام CSUnix، فقم بإضافة هذا الأمر:

```
GOSS(config)# aaa authorization command TACSERVER
```

من بين المستخدمين الثلاثة، يمكن ل "Pixtest" عمل كل شيء، ويمكن للمستخدمين الآخرين عمل مجموعة فرعية من الأوامر.

ACS - RADIUS

تفويض أوامر RADIUS غير مدعوم. يمكن إستخدام Telnet وتمكين المصادقة مع ACS. يمكن تكوين ACS للاتصال ب PIX بتعريف PIX في تكوين الشبكة ب "مصادقة إستخدام" RADIUS (أي تنوع). يعتمد تكوين مستخدم ACS على تكوين PIX. يجب على مستخدم ACS إعداد اسم مستخدم وكلمة مرور كحد أدنى.

على ال PIX، استعملت هذا أمر:

```
GOSS(config)# enable password cisco123
(GOSS(config)# aaa-server RADSERVER protocol radius GOSS(config
(aaa-server RADSERVER (inside #
host
```

```
GOSS(config)# aaa authentication telnet console RADSERVER
```

عند هذه النقطة، يجب أن يكون مستخدم ACS قادرا على إرسال برنامج Telnet إلى PIX والتمكين باستخدام كلمة مرور التمكين الموجودة على PIX واستخدام جميع الأوامر (لا يقوم PIX بإرسال الأوامر إلى خادم RADIUS؛ تفويض أوامر RADIUS غير مدعوم).

إن يريد أنت أن يمكن مع ACS و RADIUS على PIX، أضفت هذا أمر:

```
aaa authentication enable console RADSERVER
```

بخلاف TACACS+، يتم إستخدام نفس كلمة المرور لتمكين RADIUS مثل تسجيل دخول RADIUS.

CSUnix - RADIUS

قم بتكوين CSUnix للتحدث إلى PIX كما تفعل مع أي جهاز شبكة آخر. يعتمد تكوين مستخدم CSUnix على تكوين PIX. يعمل هذا التوصيف على المصادقة والتمكين:

```
}user = pixradius
  profile_id = 26
profile_cycle = 1
The login password is in the 'clear "********"' statement; !--- this is used for the login, ---!
.enable, and non-enable commands

password = clear "********" < pixradius
{
```

على ال PIX، استعملت هذا أمر:

```
GOSS(config)# enable password cisco123
GOSS(config)# aaa-server RADSERVER protocol radius
GOSS(config)# aaa-server RADSERVER (inside) host
```

إن يريد أنت أن يمكن مع ACS و RADIUS على PIX، استعملت هذا أمر:

```
GOSS(config)# aaa authentication enable console RADSERVER
```

بخلاف TACACS+، يتم إستخدام نفس كلمة المرور لتمكين RADIUS مثل تسجيل دخول RADIUS.

قيود الوصول إلى الشبكة

يمكن إستخدام تقييدات الوصول إلى الشبكة في كل من ACS و CSUnix لتحديد من قد يتصل ب PIX لأغراض إدارية.

- **ACS**— سيتم تكوين PIX في منطقة "قيود الوصول إلى الشبكة" من إعدادات المجموعة. إن تكوين PIX إما "مواقع الاتصال/نقطة الوصول المرفوضة" أو "مواقع الاتصال/نقطة الوصول المسموح بها" (حسب خطة الأمان).
- **CSUnix**—هذا مثال لمستخدم يسمح له بالوصول إلى PIX، وليس الأجهزة الأخرى:

```
}user = naruser
profile_id = 119
profile_cycle = 1
"********" password = clear
privilege = clear "********" 15
} service=shell
"*." "*." "allow "10.98.21.50
"*." "*." "*." refuse
default cmd=permit
default attribute=permit
```

{
{

تصحيح الأخطاء

لتشغيل تصحيح الأخطاء، أستخدم الأمر التالي:

```
logging on
logging
```

هذه أمثلة لتصحيح الأخطاء الجيدة والسيئة:

- **تصحيح جيد**—يمكن للمستخدم إستخدام **أوامر تسجيل الدخول والتمكين والتنفيذ**.

```
Permitted Telnet login session from 172.18.124.111 :307002
Console Login from pixpartial at console :111006
User priv level changed: Uname: pixpartial From: 1 To: 15 :502103
User 'pixpartial' executed cmd: show clock :111009
```

- **تصحيح الأخطاء** — يفشل التفويض للمستخدم، كما هو موضح في هذا المثال:

```
Authorization failed: Cmd: uauth Cmdtype: show :610101
```

- **يتعذر الوصول إلى خادم AAA البعيد:**

```
AAA server host machine not responding
```

محاسبة

لا توجد عملية محاسبة أوامر فعلية متوفرة، ولكن من خلال تنشيط syslog على PIX، يمكنك مشاهدة الإجراءات التي تم تنفيذها، كما هو موضح في هذا المثال:

```
Permitted Telnet login session from 172.18.124.111 :307002
Console Login from pixtest at console :111006
User logged out: Uname: pixtest :611103
Permitted Telnet login session from 172.18.124.111 :307002
Console Login from pixtest at console :111006
User priv level changed: Uname: pixtest From: 1 To: 15 :502103
.User 'pixtest' executed the 'enable' command :111008
Begin configuration: 172.18.124.111 reading from terminal :111007
.User 'pixtest' executed the 'configure t' command :111008
.User 'pixtest' executed the 'write t' command :111008
```

معلومات للتجميع إذا قمت بفتح حالة مركز المساعدة الفنية

إذا كنت لا تزال بحاجة إلى المساعدة بعد اتباع خطوات أستكشاف الأخطاء وإصلاحها أعلاه وتريد فتح حالة باستخدام برنامج Cisco TAC، فتأكد من تضمين المعلومات التالية لاستكشاف أخطاء جدار حماية PIX وإصلاحها.
• وصف المشكلة وتفاصيل المخطط ذات الصلة

- تم إجراء أستكشاف الأخطاء وإصلاحها قبل فتح الحالة
- مخرجات من الأمر **show tech-support**
- الإخراج من الأمر **show log** بعد التشغيل باستخدام الأمر **logging buffered debugging**، أو التقاط وحدة التحكم التي توضح المشكلة (إذا كانت متاحة)

الرجاء إرفاق البيانات المجمعة بالحالة الخاصة بك بتنسيق نص عادي غير مضغوط (.txt). يمكنك إرفاق المعلومات بالحالة الخاصة بك عن طريق تحميلها باستخدام أداة استعلام الحالة (للعملاء المسجلين فقط). إذا تعذر عليك الوصول إلى "أداة استعلام الحالة"، فيمكنك إرسال المعلومات في مرفق بريد إلكتروني إلى موقع attach@cisco.com مع وجود رقم الحالة الخاص بك في سطر موضوع رسالتك.

معلومات ذات صلة

- مرجع أوامر PIX
- برنامج جدار حماية Cisco PIX - الدعم التقني والمستندات
- خادم التحكم في الوصول الآمن من Cisco لأنظمة التشغيل Windows - الدعم التقني والمستندات
- خادم التحكم في الوصول الآمن من Cisco ل UNIX - الدعم التقني والمستندات

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).