عمليات تهيئة نموذج PIX و TACACS+ و RADIUS: 4.2.x

المحتويات

المقدمة

قد تتم مصادقة RADIUS و TACACS+ لاتصالات FTP و Telnet و HTTP. تفويض TACACS+ مدعوم، أما تفويض RADIUS فهو غير مدعوم.

تغيرت الصياغة للمصادقة بشكل طفيف في برنامج PIX 4.2.2. يستخدم هذا المستند الصياغة لإصدارات البرامج

.4.2.2

المتطلبات الأساسية

المتطلبات

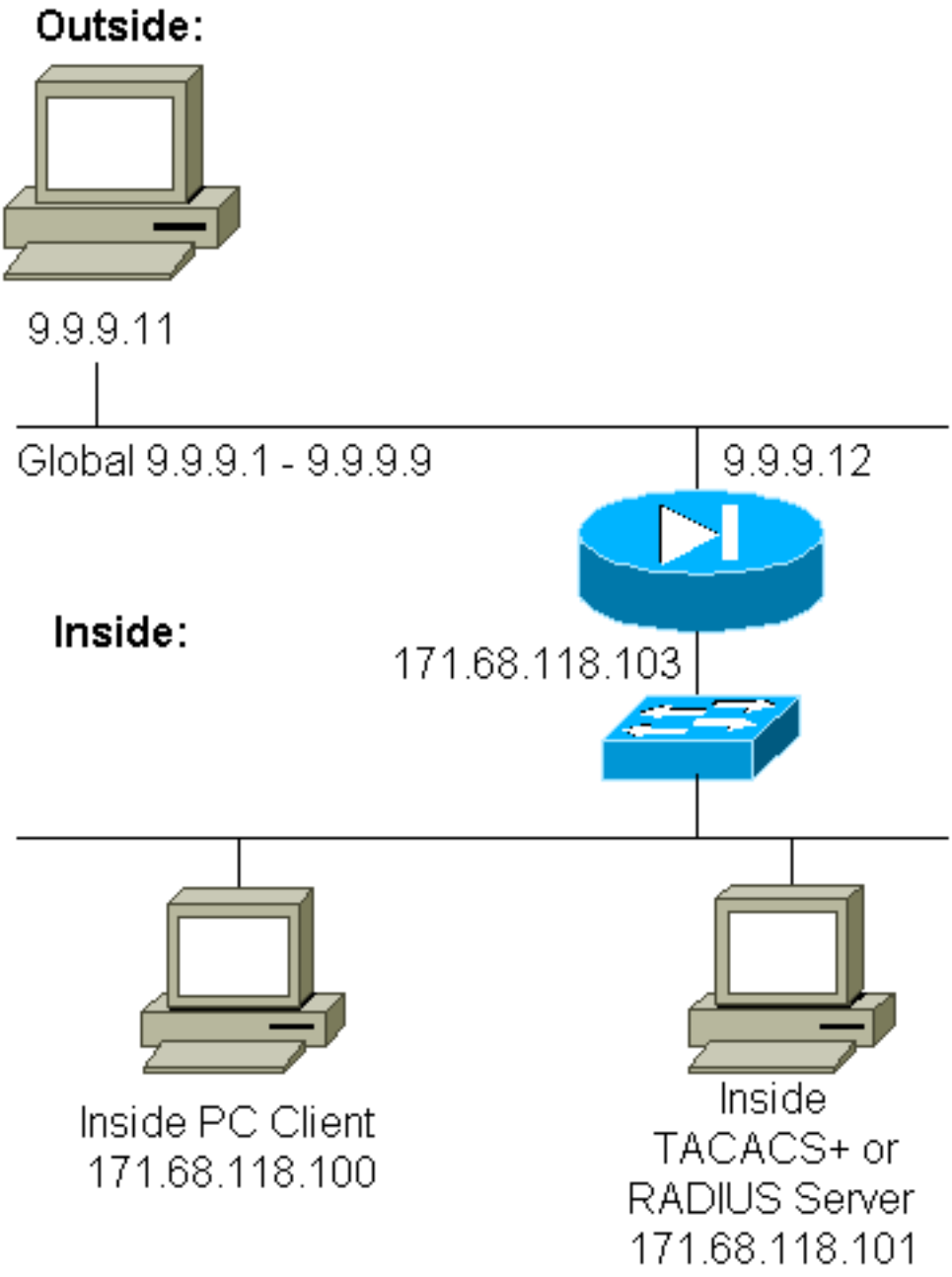
لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



تكوين PIX

```
pix2# write terminal
Building configuration
Saved :
:
(PIX Version 4.2(2
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd OnTrBUG1Tp0edmkr encrypted
hostname pix2
fixup protocol http 80
fixup protocol smtp 25
no fixup protocol ftp 21
no fixup protocol h323 1720
no fixup protocol rsh 514
no fixup protocol sqlnet 1521
no failover
failover timeout 0:00:00
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address  0.0.0.0
names
pager lines 24
logging console debugging
no logging monitor
logging buffered debugging
logging trap debugging
logging facility 20
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
ip address outside 9.9.9.12 255.255.255.0
ip address inside 171.68.118.103 255.255.255.0
ip address  0.0.0.0 0.0.0.0
arp timeout 14400
global (outside) 1 9.9.9.1-9.9.9.9 netmask 255.0.0.0
static (inside,outside) 9.9.9.10 171.68.118.100 netmask
255.255.255.255 0 0
conduit permit icmp any any
conduit permit tcp host 9.9.9.10 eq telnet any
no rip outside passive
no rip outside default
no rip inside passive
no rip inside default
timeout xlate 3:00:00 conn 1:00:00 udp 0:02:00
timeout rpc 0:10:00 h323 0:05:00
timeout uauth 0:00:00 absolute
!
The next entry depends on whether TACACS+ or RADIUS ---!
   is used. ! tacacs-server (inside) host 171.68.118.101
cisco timeout 5
radius-server (inside) host 171.68.118.101 cisco timeout
10
!
   The focus of concern is with hosts on the inside ---!
 network !--- accessing a particular outside host. ! aaa
  authentication any outbound 171.68.118.0 255.255.255.0
9.9.9.11
tacacs+|radius 255.255.255.255
!
It is possible to be less granular and authenticate ---!
```

```
!--- all outbound FTP, HTTP, Telnet traffic with: aaa
  authentication ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 tacacs+|radius aaa authentication http outbound
   0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tacacs+|radius aaa
 authentication telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0
  0.0.0.0 tacacs+|radius ! !--- Accounting records are
sent for !--- successful authentications to the TACACS+
or RADIUS server. ! aaa accounting any outbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 tacacs+|radius ! no snmp-server
  location no snmp-server contact snmp-server community
public no snmp-server enable traps telnet 171.68.118.100
   255.255.255.255 mtu outside 1500 mtu inside 1500 mtu
1500 Smallest mtu: 1500 floodguard 0 tcpchecksum silent
  Cryptochecksum:be28c9827e13baf89a937c617cfe6da0 : end
                                                    [[OK
```

الاصطلاحات

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

المصادقة مقابل التخويل

- المصادقة هي *من* يكون المستخدم.
- التفويض هو *ما* يمكن للمستخدم القيام به.
- المصادقة *صالحة* دون تخويل.
- التخويل غير صالح بدون مصادقة.

على سبيل المثال، افترض أن لديك مائة مستخدم بالداخل وتريد فقط أن يتمكن ستة من هؤلاء المستخدمين من تنفيذ FTP أو Telnet أو HTTP خارج الشبكة. اطلب من PIX مصادقة حركة المرور الصادرة ومنح معرفات المستخدمين الستة جميعها على خادم أمان TACACS+/RADIUS. باستخدام مصادقة بسيطة، يمكن مصادقة هؤلاء المستخدمين الستة باستخدام اسم المستخدم وكلمة المرور، ثم الخروج. أما المستخدمين الأربعة والتسعون الآخرون فلا يمكنهم الخروج. يطلب PIX من المستخدمين اسم المستخدم/كلمة المرور، ثم يقوم بتمرير اسم المستخدم وكلمة المرور إلى خادم أمان TACACS+/RADIUS. أيضا، اعتمادا على الاستجابة، يفتح الاتصال أو ينفيه. يمكن لهؤلاء المستخدمين الستة تنفيذ بروتوكول FTP أو Telnet أو HTTP.

ومع ذلك، فلنفترض أن واحدا من هؤلاء المستخدمين الثلاثة، "تيري"، ليس محل ثقة. تود أن تسمح لتيري بعمل FTP، ولكن ليس HTTP أو Telnet إلى الخارج. وهذا يعني أنك بحاجة إلى إضافة التفويض. أي، تفويض ما يمكن للمستخدمين القيام به بالإضافة إلى مصادقة من هم. عند إضافة تفويض إلى PIX، يرسل PIX أولا اسم مستخدم وكلمة مرور تيري إلى خادم الأمان، ثم يرسل طلب تفويض يخبر خادم الأمان بما يحاول "الأمر" تيري القيام به. ومع إعداد الخادم بشكل صحيح، يمكن السماح لتيري بالوصول إلى "FTP 1.2.3.4" ولكنه يحرم من القدرة على إستخدام "HTTP" أو "Telnet" في أي مكان.

ما يراه المستخدم مع المصادقة/التخويل في

عندما تحاول الانتقال من الداخل إلى الخارج (أو العكس) باستخدام المصادقة/التخويل على:

- **Telnet** - يرى المستخدم نافذة مطالبة باسم المستخدم، يتبعها طلب كلمة مرور. إذا نجحت المصادقة (والتفويض) في PIX/الخادم، فسيطلب من المستخدم اسم المستخدم وكلمة المرور بواسطة المضيف الوجهة فيما بعد.
- **FTP** - يرى المستخدم ظهور مطالبة اسم المستخدم. يحتاج المستخدم إلى إدخال "local_username@remote_username" لاسم المستخدم و"local_password@remote_password" لكلمة المرور. يرسل ال PIX ال "local_username" و "local_password" إلى الأمن نادل محلي، وإن كانت المصادقة (والتخويل) ناجح في ال PIX/نادل، ال "remote_username" و "remote_password" يكون مررت

إلى الغاية FTP نادل بعد.

- **HTTP** - يتم عرض نافذة في المستعرض الذي يطلب اسم مستخدم وكلمة مرور. في حالة نجاح المصادقة (والتفويض)، يصل المستخدم إلى موقع ويب الوجهة فيما بعد. تذكر أن **المستعرضات تخزن أسماء المستخدمين وكلمات المرور مؤقتا**. إذا بدا أن PIX يجب أن يقوم بتوقيت اتصال HTTP ولكنه لا يفعل ذلك، فمن المحتمل أن تتم إعادة المصادقة بالفعل مع المستعرض "إطلاق" اسم المستخدم وكلمة المرور المخزنة مؤقتا على PIX. ثم يعيد توجيه هذا إلى خادم المصادقة. يعرض PIX syslog و/أو تصحيح أخطاء الخادم هذه الظاهرة. إذا بدا Telnet و FTP أنهما يعملان بشكل طبيعي، ولكن إتصالات HTTP لا تعمل، فهذا هو السبب.

تكوينات الخادم المستخدمة لجميع السيناريوهات

في أمثلة تكوين خادم TACACS+، إذا كانت المصادقة فقط قيد التشغيل، يعمل المستخدمون "all" و"telnetOnly" و"httponly" و"ftponly" جميعا. في أمثلة تكوين خادم RADIUS، يعمل المستخدم "all".

عند إضافة التفويض إلى PIX، يرسل PIX، بالإضافة إلى إرسال اسم المستخدم وكلمة المرور إلى خادم مصادقة TACACS+، أوامر (Telnet أو HTTP أو FTP) إلى خادم TACACS+. ثم يتحقق خادم TACACS+ لمعرفة ما إذا كان ذلك المستخدم مخولا لهذا الأمر.

في مثال لاحق، يصدر المستخدم في 171.68.118.100 الأمر **telnet 9.9.9.11**. عند تلقي هذا الأمر في PIX، يقوم PIX بتمرير اسم المستخدم وكلمة المرور والأمر إلى خادم TACACS+ للمعالجة.

لذلك مع تشغيل التخويل بالإضافة إلى المصادقة، يمكن للمستخدم "telnetOnly" إجراء عمليات Telnet من خلال PIX. ومع ذلك، لا يمكن للمستخدمين "httponly" و"ftponly" تنفيذ عمليات Telnet من خلال PIX.

(مرة أخرى، لا يتم دعم التخويل مع RADIUS بسبب طبيعة مواصفات البروتوكول).

تكوين خادم UNIX الآمن ل TACACS+ من Cisco

Cisco Secure 2.x

- يتم عرض إستمارات المستخدم هنا.
- قم بإضافة عنوان PIX IP أو اسم المجال والمفتاح المؤهلان بالكامل إلى CSU.cfg.

```
                                                } user = all
                                          "password = clear "all
                                       default service = permit
                                                              {

                                                  } user = telnetonly
                                          "password = clear "telnetonly
                                                    } service = shell
                                                       } cmd = telnet
                                                            *. permit
                                                                    {
                                                                    {
                                                                    {

                                                   } user = ftponly
                                             "password = clear "ftponly
                                                  } service = shell
                                                       } cmd = ftp
                                                         *. permit
                                                                    {
                                                                    {
                                                                    {
```

```
} user = httponly
"password = clear "httponly
} service = shell
} cmd = http
*. permit
{
{
{
```

تكوين خادم UNIX RADIUS الآمن من Cisco

أستخدم واجهة المستخدم الرسومية المتقدمة (GUI) لإضافة PIX IP والمفتاح إلى قائمة خادم الوصول إلى الشبكة (NAS). يظهر المستعمل ستانزا كما هو موضح هنا:

```
"all Password="all
User-Service-Type = Shell-User
```

Cisco Secure NT 2.x RADIUS

يصف قسم نماذج التكوينات في CiscoSecure 2.1 عبر الإنترنت ووثائق الويب الإعداد؛ وتكون السمة 6 (نوع الخدمة) هي تسجيل الدخول أو Administrative.

أضفت ال ip من ال PIX في ال nas تشكيل قسم يستعمل ال gui.

+EasyACS TACACS

توفر وثائق EasyACS معلومات الإعداد.

1. في قسم المجموعة، انقر فوق **Shell EXEC** (لإعطاء امتيازات EXEC).
2. لإضافة تفويض إلى PIX، انقر فوق **رفض أوامر IOS غير المتطابقة** في أسفل إعداد المجموعة.
3. حدد **إضافة/تحرير** لكل أمر تريد السماح به (على سبيل المثال، Telnet).
4. إذا كنت ترغب في السماح ب Telnet إلى مواقع معينة، فأدخل IP(s) في قسم الوسيطة. للسماح لبرنامج Telnet بجميع المواقع، انقر فوق **السماح بجميع الوسيطات غير المدرجة**.
5. طقطقة **إنجاز تحرير أمر**.
6. قم بإجراء الخطوات من 1 إلى 5 لكل من الأوامر المسموح بها (على سبيل المثال، Telnet و/أو HTTP و/أو FTP).
7. أضفت ال ip من ال PIX في ال nas تشكيل قسم يستعمل ال gui.

بروتوكول TACACS NT 2.x+ الآمن من Cisco

توفر وثائق Cisco Secure 2.x معلومات الإعداد.

1. في قسم المجموعة، انقر فوق **Shell EXEC** (لإعطاء امتيازات EXEC).
2. لإضافة تفويض إلى PIX، انقر فوق **رفض أوامر IOS غير المتطابقة** في أسفل إعداد المجموعة.
3. حدد خانة إختيار **الأمر** في الأسفل وأدخل الأمر الذي تريد السماح به (على سبيل المثال، Telnet).
4. إذا كنت ترغب في السماح لبرنامج Telnet بمواقع معينة، فأدخل IP في قسم الوسيطة (على سبيل المثال، "السماح 1.2.3.4"). للسماح لبرنامج Telnet بجميع المواقع، انقر فوق **السماح بالوسيطات غير المدرجة**.
5. انقر على **إرسال**.
6. قم بإجراء الخطوات من 1 إلى 5 لكل من الأوامر المسموح بها (على سبيل المثال، Telnet و/أو FTP و/أو HTTP).
7. أضفت ال ip من ال PIX في ال nas تشكيل قسم يستعمل ال gui.

تكوين خادم Liingston RADIUS

إضافة عنوان PIX IP والمفتاح إلى ملف العملاء.

```
"all Password="all
User-Service-Type = Shell-User
```

إستحقاق تكوين خادم RADIUS

قم بإضافة عنوان PIX IP والمفتاح إلى ملف العملاء.

```
"all Password="all
Service-Type = Shell-User
```

تكوين خادم TACACS+ FreeWARE

```
:'Handshake with router--PIX needs 'tacacs-server host #.#.#.# cisco #
"key = "cisco

} user = all
default service = permit
"login = cleartext "all
{

} user = telnetonly
"login = cleartext "telnetonly
} cmd = telnet
*. permit
{
{

} user = httponly
"login = cleartext "httponly
} cmd = http
*. permit
{
{

} user = ftponly
"login = cleartext "ftponly
} cmd = ftp
*. permit
{
{
```

خطوات التصحيح

- تأكد من أن تكوينات PIX تعمل قبل إضافة المصادقة والتفويض والمحاسبة (AAA).إذا لم تتمكن من تمرير حركة المرور قبل إنشاء المصادقة والتفويض والمحاسبة (AAA)، فلن تتمكن من القيام بذلك بعد ذلك.
- تمكين تسجيل الدخول إلى PIX:يجب عدم إستخدام أمر **تصحيح أخطاء وحدة تحكم التسجيل** على نظام محمل بشكل كبير.يمكن إستخدام الأمر **logging buffered debuing** . يمكن بعد ذلك إرسال الإخراج من أوامر **show logging** أو **logging** إلى خادم syslog وفحصه.
- تأكد من تشغيل تصحيح الأخطاء لخوادم TACACS+ أو RADIUS. كافة الخوادم لها هذا الخيار.

أمثلة تصحيح أخطاء المصادقة من PIX

تصحيح أخطاء PIX - مصادقة جيدة - RADIUS

هذا مثال على تصحيح أخطاء PIX بمصادقة جيدة:

```
Auth start for user '???' from 171.68.118.100/1116 to 9.9.9.11/23 :109001
                        Authen Session Start: user 'bill', sid 1 :109011
                        'Authentication succeeded for user 'bill :109005
                              from 171.68.118.100/1116 to 9.9.9.11/23
      Authen Session End: user 'bill', sid 1, elapsed 1 seconds :109012
Built TCP connection 1 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1116 :302001
                                    (laddr 171.68.118.100/1116 (bill
```

تصحيح أخطاء PIX - مصادقة غير صحيحة (اسم المستخدم أو كلمة المرور) - RADIUS

هذا مثال على تصحيح أخطاء PIX بمصادقة غير صحيحة (اسم المستخدم أو كلمة المرور). يرى المستعمل أربعة username/كلمة مجموعة. يتم عرض الرسالة "خطأ: الحد الأقصى لعدد مرات إعادة المحاولة التي تم تجاوزها".

ملاحظة: إذا كانت هذه محاولة FTP، يتم السماح بمحاولة واحدة. بالنسبة ل HTTP، يتم السماح بعمليات إعادة المحاولة غير المحدودة.

```
Auth start for user '???' from 171.68.118.100/1132 to 9.9.9.11/23 :109001
                        Authentication failed for user '' from :109006
                              to 9.9.9.11/23 171.68.118.100/1132
```

تصحيح أخطاء PIX - خادم لأسفل - RADIUS

هذا مثال على تصحيح أخطاء PIX مع تنزيل الخادم. يرى المستعمل ال username مرة. ثم "يعلق" الخادم ويطلب كلمة مرور (ثلاث مرات).

```
Auth start for user '???' from 171.68.118.100/1151 to 9.9.9.11/23 :109001
            Auth from 171.68.118.100/1151 to 9.9.9.11/23 failed :109002
                                  (server 171.68.118.101 failed)
            Auth from 171.68.118.100/1151 to 9.9.9.11/23 failed :109002
                                  (server 171.68.118.101 failed)
```

تصحيح أخطاء PIX - مصادقة جيدة - TACACS+

هذا مثال على تصحيح أخطاء PIX بمصادقة جيدة:

```
Auth start for user '???' from 171.68.118.100/1200 to 9.9.9.11/23 :109001
                        Authen Session Start: user 'cse', sid 3 :109011
                        'Authentication succeeded for user 'cse :109005
                              from 171.68.118.100/1200 to 9.9.9.11/23
      Authen Session End: user 'cse', sid 3, elapsed 1 seconds :109012
Built TCP connection 3 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1200 :302001
                                    (laddr 171.68.118.100/1200 (cse
```

تصحيح أخطاء PIX - مصادقة غير صحيحة (اسم المستخدم أو كلمة المرور) - TACACS+

هذا مثال على تصحيح أخطاء PIX بمصادقة غير صحيحة (اسم المستخدم أو كلمة المرور). يرى المستعمل أربعة username/كلمة مجموعة. يتم عرض الرسالة "خطأ: الحد الأقصى لعدد مرات إعادة المحاولة التي تم تجاوزها".

ملاحظة: إذا كانت هذه محاولة FTP، يتم السماح بمحاولة واحدة. بالنسبة ل HTTP، يتم السماح بعمليات إعادة

المحاولة غير المحدودة.

```
Auth start for user '???' from 171.68.118.100/1203 to 9.9.9.11/23 :109001
                                  '' Authentication failed for user :109006
                                 from 171.68.118.100/1203 to 9.9.9.11/23
```

تصحيح أخطاء PIX - خادم لأسفل - TACACS+

هذا مثال على تصحيح أخطاء PIX مع تنزيل الخادم. يرى المستعمل ال username مرة. وعلى الفور، يتم عرض رسالة "الخطأ: الحد الأقصى لعدد المحاولات التي تم تجاوزها".

```
Auth start for user '???' from 171.68.118.100/1212 to 9.9.9.11/23 :109001
            Auth from 171.68.118.100/1212 to 9.9.9.11/23 failed :109002
                                  (server 171.68.118.101 failed)
            Auth from 171.68.118.100/1212 to 9.9.9.11/23 failed :109002
                                  (server 171.68.118.101 failed)
            Auth from 171.68.118.100/1212 to 9.9.9.11/23 failed :109002
                                  (server 171.68.118.101 failed)
Authentication failed for user '' from 171.68.118.100/1212 to 9.9.9.11/23 :109006
```

إضافة التخويل

نظرا لأن التخويل غير صالح دون مصادقة، يلزم توفر التخويل لنفس المصدر والوجهة:

```
aaa authorization any outbound 171.68.118.0 255.255.255.0 9.9.9.11
                                  tacacs+|radius 255.255.255.255
```

أو، إذا كانت الخدمات الصادرة الثلاث قد تمت مصادقتها في الأصل:

```
aaa authorization http outbound 0.0.0.0 0.0.0.0 0.0.0.0
                                  tacacs+|radius 0.0.0.0
 aaa authorization ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0
                                  tacacs+|radius 0.0.0.0
aaa authorization telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0
                                  tacacs+|radius 0.0.0.0
```

أمثلة تصحيح أخطاء المصادقة والتفويض من PIX

تصحيح أخطاء PIX - المصادقة والتفويض الجيدين - TACACS+

هذا مثال على تصحيح أخطاء PIX بمصادقة وتفويض جيدين:

```
Auth start for user '???' from 171.68.118.100/1218 to 9.9.9.11/23 :109001
                    Authen Session Start: user 'telnetonly', sid 5 :109011
                Authentication succeeded for user 'telnetonly' from :109005
                                  to 9.9.9.11/23 171.68.118.100/1218
                    Authen Session Start: user 'telnetonly', sid 5 :109011
                 Authorization permitted for user 'telnetonly' from :109007
                                  to 9.9.9.11/23 171.68.118.100/1218
 Authen Session End: user 'telnetonly', sid 5, elapsed 1 seconds :109012
```

```
Built TCP connection 4 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1218 :302001
                                (laddr 171.68.118.100/1218 (telnetonly
```

تصحيح أخطاء PIX - مصادقة جيدة، ولكن فشل في التفويض - TACACS+

هذا مثال على تصحيح أخطاء PIX بمصادقة جيدة ولكن فشل في التفويض:

```
Auth start for user '???' from 171.68.118.100/1223 to 9.9.9.11/23 :109001
                        Authen Session Start: user 'httponly', sid 6 :109011
                        'Authentication succeeded for user 'httponly :109005
                                  from 171.68.118.100/1223 to 9.9.9.11/23
                           'Authorization denied for user 'httponly :109008
                                  from 171.68.118.100/1223 to 9.9.9.11/23
```

تصحيح أخطاء PIX - مصادقة غير صحيحة، تفويض غير مجرب - TACACS+

هذا مثال على تصحيح أخطاء PIX بالمصادقة والتخويل، ولكن لم تتم محاولة التخويل بسبب المصادقة غير الصحيحة (اسم المستخدم أو كلمة المرور). يرى المستعمل أربعة username/كلمة مجموعة. تم عرض الرسالة "خطأ: الحد الأقصى لعدد مرات إعادة المحاولة"

ملاحظة: إذا كانت هذه محاولة FTP، يتم السماح بمحاولة واحدة. بالنسبة ل HTTP، يتم السماح بعمليات إعادة المحاولة غير المحدودة.

```
Auth start for user '???' from 171.68.118.100/1228 to 9.9.9.11/23 :109001
      Authentication failed for user '' from 171.68.118.100/1228 :109006
                                                  to 9.9.9.11/23
```

تصحيح أخطاء PIX - المصادقة/التفويض، تعطل الخادم - TACACS+

هذا مثال على تصحيح أخطاء PIX بالمصادقة والتفويض. الخادم معطل. يرى المستعمل username مرة واحدة. وعلى الفور، يتم عرض "الخطأ: الحد الأقصى لعدد المحاولات التي تم تجاوزها."

```
Auth start for user '???' from 171.68.118.100/1237 to 9.9.9.11/23 :109001
             Auth from 171.68.118.100/1237 to 9.9.9.11/23 failed :109002
                                        (server 171.68.118.101 failed)
             Auth from 171.68.118.100/1237 to 9.9.9.11/23 failed :109002
                                        (server 171.68.118.101 failed)
             Auth from 171.68.118.100/1237 to 9.9.9.11/23 failed :109002
                                        (server 171.68.118.101 failed)
      Authentication failed for user '' from 171.68.118.100/1237 :109006
                                                  to 9.9.9.11/23
```

إضافة محاسبة

TACACS+

```
+aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0: tacacs
```

يبدو التصحيح نفسه سواء كانت المحاسبة قيد التشغيل أو إيقاف التشغيل. ومع ذلك، يتم إرسال سجل محاسبة "البدء" في وقت "الإنشاء". كما يتم إرسال سجل محاسبة "إيقاف" في وقت "التيردون":

```
Authen Session Start: user 'telnetonly', sid 13 :109011
'Authentication succeeded for user 'telnetonly :109005
```

```
                                    from 171.68.118.100/1299 to 9.9.9.11/23
                          Authen Session Start: user 'telnetonly', sid 13 :109011
                            'Authorization permitted for user 'telnetonly :109007
                                    from 171.68.118.100/1299 to 9.9.9.11/23
                   Authen Session End: user 'telnetonly', sid 13, elapsed 1 seconds :109012
                Built TCP connection 11 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1299 :302001
                                      (laddr 171.68.118.100/1299 (telnetonly
                   Teardown TCP connection 11 faddr 9.9.9.11/23 gaddr 9.9.9.10/1299 :302002
                                  laddr 171.68.118.100/1299 duration 0:00:02 bytes 112
```

تبدو سجلات محاسبة TACACS+ مثل هذا الإخراج (وهذه من CiscoSecure UNIX؛ وقد تكون السجلات الموجودة في Cisco Secure Windows محددة بفاصلة بدلا من ذلك):

```
                  Tue Sep 29 11:00:18 1998 redclay cse PIX 171.68.118.103
                                    start task_id=0x8 foreign_ip=9.9.9.11
                                        local_ip=171.68.118.100 cmd=telnet
                  Tue Sep 29 11:00:36 1998 redclay cse PIX 171.68.118.103
                                     stop task_id=0x8 foreign_ip=9.9.9.11
                       local_ip=171.68.118.100 cmd=telnet elapsed_time=17
                                             bytes_in=1198 bytes_out=62
               Tue Sep 29 11:02:08 1998 redclay telnetonly PIX 171.68.118.103
                                    start task_id=0x9 foreign_ip=9.9.9.11
                                        local_ip=171.68.118.100 cmd=telnet
               Tue Sep 29 11:02:27 1998 redclay telnetonly PIX 171.68.118.103
                                     stop task_id=0x9 foreign_ip=9.9.9.11
                       local_ip=171.68.118.100 cmd=telnet elapsed_time=19
                                             bytes_in=2223 bytes_out=64
```

تنهار الحقول كما يظهر هنا:

```
DAY MO DATE TIME YEAR NAME_OF_PIX USER SENDER PIX_IP START/STOP
                                        UNIQUE_TASK_ID DESTINATION SOURCE
                                    <SERVICE <TIME> <BYTES_IN> <BYTES_OUT
```

RADIUS

```
aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 radius
```

يبدو التصحيح نفسه سواء كانت المحاسبة قيد التشغيل أو إيقاف التشغيل. ومع ذلك، يتم إرسال سجل محاسبة "البدء" في وقت "الإنشاء". كما يتم إرسال سجل محاسبة "إيقاف" في وقت "التيردون":

```
          Auth start for user '???' from 171.68.118.100/1316 to 9.9.9.11/23 :109001
                                Authen Session Start: user 'bill', sid 16 :109011
                                 'Authentication succeeded for user 'bill :109005
                                        from 171.68.118.100/1316 to 9.9.9.11/23
                      Authen Session End: user 'bill', sid 16, elapsed 1 seconds :109012
                   Built TCP connection 14 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1316 :302001
                                          (laddr 171.68.118.100/1316 (bill
                   Teardown TCP connection 14 faddr 9.9.9.11/23 gaddr 9.9.9.10/1316 :302002
                                  laddr 171.68.118.100/1316 duration 0:00:03 bytes 112
```

سجلات محاسبة RADIUS تبدو مثل هذا المخرج (هذه من Cisco Secure UNIX؛ تلك الموجودة في Cisco Secure Windows مفصولة بفاصلة):

```
                                        Mon Sep 28 10:47:01 1998
                                      Acct-Status-Type = Start
                                    Client-Id = 171.68.118.103
```

```
Login-Host = 171.68.118.100
Login-TCP-Port = 23
"Acct-Session-Id = "0x00000004
"User-Name = "bill

Mon Sep 28 10:47:07 1998
Acct-Status-Type = Stop
Client-Id = 171.68.118.103
Login-Host = 171.68.118.100
Login-TCP-Port = 23
"Acct-Session-Id = "0x00000004
"User-Name = "bill
Acct-Session-Time = 5
```

تنهار الحقول كما يظهر هنا:

```
Acct-Status-Type = START or STOP
Client-ID = IP_OF_PIX
Login_Host = SOURCE_OF_TRAFFIC
# = Login-TCP-Port
Acct-Session-ID = UNIQUE_ID_PER_RADIUS_RFC
<User-name = <whatever
<# = Acct-Session-Time>
```

الحد الأقصى لجلسات العمل وعرض المستخدمين الذين تم تسجيل دخولهم

تحتوي بعض خوادم TACACS و RADIUS على ميزات "الحد الأقصى لجلسة العمل" أو "عرض المستخدمين الذين تم تسجيل دخولهم". تعتمد إمكانية تنفيذ الحد الأقصى لجلسات العمل أو فحص المستخدمين الذين تم تسجيل دخولهم على سجلات المحاسبة. عند وجود سجل "بدء" محاسبة تم إنشاؤه ولكن لم يتم تسجيل "إيقاف"، يفترض خادم TACACS أو RADIUS أن الشخص لا يزال قيد تسجيل الدخول (أي لديه جلسة عمل من خلال PIX). يعمل هذا بشكل جيد لاتصالات Telnet و FTP بسبب طبيعة الاتصالات. كمثال:

المستخدم Telnet من 171.68.118.100 إلى 9.9.9.25 من خلال PIX، يصدق على الطريقة:

```
pix) 109001: Auth start for user '???' from 171.68.118.100/1200)
to 9.9.9.25/23
pix) 109011: Authen Session Start: user 'cse', sid 3)
pix) 109005: Authentication succeeded for user 'cse' from 171.68.118.100/12)
to 9.9.9.25/23 00
pix) 302001: Built TCP connection 5 for faddr 9.9.9.25/23 gaddr 9.9.9.10/12)
(laddr 171.68.118.100/1200 (cse 00
server start account) Sun Nov 8 16:31:10 1998 rtp-pinecone.rtp.cisco.com)
cse PIX 171.68.118.100 start task_id=0x3 foreign_ip=9.9.9.25
local_ip=171.68.118.100 cmd=telnet
```

نظرا لأن الخادم قد شاهد سجل "بدء" ولكن ليس سجل "إيقاف" (في هذه المرحلة من الوقت)، يظهر الخادم أن مستخدم "برنامج Telnet" قد سجل الدخول. إذا حاول المستخدم إجراء اتصال آخر يتطلب مصادقة (ربما من كمبيوتر آخر) وإذا تم تعيين الحد الأقصى لجلسات العمل على "1" على الخادم لهذا المستخدم، فسيرفض الخادم الاتصال.

يقوم المستخدم بإنجاز الأعمال في المضيف الهدف، ثم يخرج (يقضي 10 دقائق هناك).

```
pix) 302002: Teardown TCP connection 5 faddr 9.9.9.25/80 gaddr 9.9.9.10/128 1)
(laddr 171.68.118.100/1281 duration 0:00:00 bytes 1907 (cse

server stop account) Sun Nov 8 16:41:17 1998)
rtp-pinecone.rtp.cisco.com cse PIX
stop task_id=0x3 foreign_ip=9.9.9.25 171.68.118.100
local_ip=171.68.118.100
```

```
cmd=telnet elapsed_time=5  bytes_in=98 bytes_out=36
```
سواء كانت المصادقة هي 0 (أي؛ مصادقة كل مرة) أو أكثر (مصادقة مرة واحدة وليس مرة أخرى خلال فترة المصادقة)، فسيكون هناك خفض لسجل المحاسبة لكل موقع يتم الوصول إليه.

ولكن HTTP يعمل بشكل مختلف نظرا لطبيعة البروتوكول. وفيما يلي مثال على هذا:

يستعرض المستخدم من 171.68.118.100 إلى 9.9.9.25 من خلال PIX.

```
pix) 109001: Auth start for user '???' from 171.68.118.100/1281)
to 9.9.9.25 /80 (pix) 109011: Authen Session Start: user 'cse', sid 5

'pix) 109005: Authentication succeeded for user 'cse)
from 171.68.118.100/12 81 to 9.9.9.25/80

pix) 302001: Built TCP connection 5 for faddr 9.9.9.25/80 gaddr 9.9.9.10/12 81)
(laddr 171.68.118.100/1281 (cse

server start account) Sun Nov  8 16:35:34 1998 rtp-pinecone.rtp.cisco.com)
cse PIX     171.68.118.100  start   task_id=0x9     foreign_ip=9.9.9.25
local_ip=171.68.118.100     cmd=http

pix) 302002: Teardown TCP connection 5 faddr 9.9.9.25/80 gaddr 9.9.9.10/128 1)
(laddr 171.68.118.100/1281 duration 0:00:00 bytes 1907 (cse

server stop account) Sun Nov  8 16:35.35 1998 rtp-pinecone.rtp.cisco .com)
cse     PIX     171.68.118.100  stop  task_id=0x9   foreign_ip =9.9.9.25

local_ip=171.68.118.100 cmd=http   elapsed_time=0
bytes_ in=1907   bytes_out=223
```
يقرأ المستخدم صفحة ويب تم تنزيلها.

لاحظ الوقت. استغرقت عملية التنزيل هذه ثانية واحدة (كانت هناك أقل من ثانية واحدة بين سجل البداية وسجل التوقف). هل لا يزال المستخدم يسجل الدخول إلى موقع ويب ولا يزال الاتصال مفتوحا؟ م

هل سيعمل الحد الأقصى لجلسات العمل أو عرض المستخدمين الذين تم تسجيل دخولهم هنا؟ لا، لأن وقت الاتصال في HTTP قصير جدا. الفترة بين سجل "Build" و"Teardown" (سجل "Start" و"Stop") هي الثانية. لن يكون هناك سجل "بدء" بدون سجل "إيقاف"، لأن السجلات تحدث في نفس اللحظة تقريبا. سيظل هناك سجل "البدء" و"الإيقاف" مرسلا إلى الخادم لكل معاملة سواء تم تعيينها ل 0 أو أي شيء أكبر. ومع ذلك، لن يعمل الحد الأقصى لجلسات العمل وعرض المستخدمين الذين تم تسجيل دخولهم بسبب طبيعة إتصالات HTTP.

إستخدام أمر EXCEPT

في شبكتنا، إذا قررنا أن مستخدم واحد صادر (171.68.118.100) لا يحتاج إلى مصادقة، فيمكننا القيام بذلك:

```
aaa authentication any outbound 171.68.118.0 255.255.255.0 9.9.9.11
+tacacs 255.255.255.255
aaa authentication except outbound 171.68.118.100 255.255.255.255 9.9.9.11
+tacacs 255.255.255.255
```

المصادقة ل PIX نفسه

تتعلق المناقشة السابقة بمصادقة حركة مرور Telnet (و HTTP و FTP) من خلال PIX. باستخدام 4.2.2، قد تتم

أيضا مصادقة إتصالات Telnet ب PIX. هنا، نحدد عناوين IP الخاصة بالمربعات التي يمكن أن تصل Telnet إلى PIX:

```
telnet 171.68.118.100 255.255.255.255
```

ثم قم بإمداد كلمة مرور برنامج Telnet: **كلمة المرور ww**.

إضافة الأمر الجديد لمصادقة المستخدمين الذين يتصلون إلى PIX:

```
aaa authentication telnet console tacacs+|radius
```

عند مطالبة المستخدمين Telnet إلى PIX، بكلمة مرور برنامج ww") Telnet"). كما يطلب PIX اسم مستخدم وكلمة مرور TACACS+ أو RADIUS.

تغيير المطالبة التي يراها المستخدمون

إذا قمت بإضافة الأمر: **المطالبة التلقائية ل YOU_ARE_AT_PIX**، فسيرى المستخدمون الذين يمرون عبر PIX التسلسل:

```
YOU_ARE_AT_THE_PIX [at which point you enter the username] Password:[at which point you enter
[the password
```

عند الوصول إلى الوجهة النهائية، سيتم عرض المطالبات "username:" و"password:". تؤثر هذه المطالبة فقط على المستخدمين الذين يمرون ب PIX، وليس ب PIX.

ملاحظة: لا توجد سجلات محاسبة مقطوعة للوصول إلى PIX.

معلومات ذات صلة

- دعم منتج برنامج جدار حماية Cisco PIX
- مراجع أوامر جدار حماية PIX الآمن من 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).