عمليات تكوين العينة PIX و TACACS+ و RADIUS: 4.4.x

المحتويات

المقدمة

قد تتم مصادقة RADIUS و TACACS+ لاتصالات FTP و Telnet و HTTP. يمكن عادة إجراء المصادقة لبروتوكولات TCP الأخرى الأقل شيوعا للعمل.

تفويض TACACS+ مدعوم، أما تفويض RADIUS فهو غير مدعوم. تتضمن التغييرات في مصادقة PIX 4.4.1 والتفويض والمحاسبة (AAA) عبر الإصدار السابق: مجموعات خوادم AAA وتجاوز الأعطال، والمصادقة لتمكين الوصول إلى وحدة التحكم التسلسلية والوصول إليها، وقبول الرسائل الفورية ورفضها.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

الاصطلاحات

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

المصادقة مقابل التخويل

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

افترض أن لديك 100 مستخدم بالداخل وتريد فقط أن يتمكن 6 من هؤلاء المستخدمين من تنفيذ FTP أو Telnet أو HTTP خارج الشبكة. يمكنك مطالبة PIX بمصادقة حركة المرور الصادرة ومنح جميع معرفات المستخدمين الستة على خادم أمان TACACS+/RADIUS. وبمصادقة بسيطة، يمكن مصادقة هؤلاء المستخدمين الستة باستخدام اسم المستخدم وكلمة المرور، ثم الخروج. ولم يتمكن المستخدمون ال 94 الآخرون من الخروج. يطلب PIX من المستخدمين اسم المستخدم/كلمة المرور، ثم يقوم بتمرير اسم المستخدم وكلمة المرور إلى خادم أمان TACACS+/RADIUS، وبناء على الاستجابة، يفتح الاتصال أو يرفضه. يمكن لهؤلاء المستخدمين الستة تنفيذ بروتوكول FTP أو Telnet أو HTTP.

ولكن لنفترض 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 ضرورة إضافة التفويض، أي تخويل ما يمكن للمستخدمين القيام به بالإضافة إلى مصادقة من هم. عندما نقوم بإضافة تفويض إلى PIX، يقوم PIX أولا بإرسال 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 رفض القدرة إلى HTTP أو Telnet في أي مكان.

ما يراه المستخدم مع المصادقة/التخويل في

عند محاولة 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 تطلب اسم المستخدم وكلمة المرور. 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 المخزن مؤقتا على PIX، والذي يقوم بعد ذلك بإعادة توجيه هذا إلى خادم المصادقة. سيقوم PIX syslog و/أو تصحيح أخطاء الخادم بعرض هذه الظاهرة. إذا بدا أن Telnet و FTP يعملان "بشكل طبيعي"، ولكن إتصالات HTTP لا تعمل، فهذا هو السبب.

تكوينات خادم الأمان المستخدمة لجميع السيناريوهات

تكوين خادم Cisco Secure UNIX TACACS

تأكد من أن لديك عنوان PIX IP أو اسم المجال والمفتاح المؤهلان بالكامل في ملف CSU.cfg.

```
                } user = ddunlap
          "password = clear "rtp
        default service = permit
                               {

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

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

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

تكوين خادم Cisco الآمن من UNIX RADIUS

أستخدم واجهة المستخدم الرسومية المتقدمة (GUI) لإضافة PIX IP والمفتاح إلى قائمة خادم الوصول إلى الشبكة (NAS).

```
} user=adminuser
  } radius=Cisco
  } =check_items
        "all"=2
              {
} =reply_attributes
              6=6
                {
                {
```

Cisco Secure NT 2.x RADIUS

أكمل الخطوات التالية.

1. الحصول على كلمة مرور في قسم إعداد المستخدم لواجهة المستخدم الرسومية.
2. من قسم واجهة المستخدم الرسومية لإعداد المجموعة، قم بتعيين السمة 6 (نوع الخدمة) إلى تسجيل الدخول أو الإجراء الإداري.
3. قم بإضافة PIX IP في واجهة المستخدم الرسومية (GUI) لتكوين NAS.

EasyACS TACACS+

تصف وثائق EasyACS 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 الأمر **إضافة/تحرير** جديد لكل أمر تريد السماح به (على سبيل المثال، Telnet).
4. إذا كنت ترغب في السماح لبرنامج Telnet بمواقع معينة، فأدخل عنوان (عناوين) IP في قسم الوسيطة في النموذج "السماح #.#. #.#". 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. قم بإضافة PIX IP في قسم تكوين NAS.

بروتوكول TACACS+ الآمن من Cisco

يتلقى المستعمل كلمة في المستعمل setup قسم من ال gui.

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 لبرنامج Telnet بمواقع معينة، فأدخل عنوان (عناوين) IP المسموح بها في مستطيل الوسيطة (على سبيل المثال، "السماح 1.2.3.4"). 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 أو HTTP أو FTP).
7. قم بإضافة PIX IP في قسم تكوين NAS.

تكوين خادم Liingston RADIUS

قم بإضافة عنوان PIX IP والمفتاح إلى ملف العملاء.

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

إستحقاق تكوين خادم RADIUS

قم بإضافة عنوان PIX IP والمفتاح إلى ملف العملاء.

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

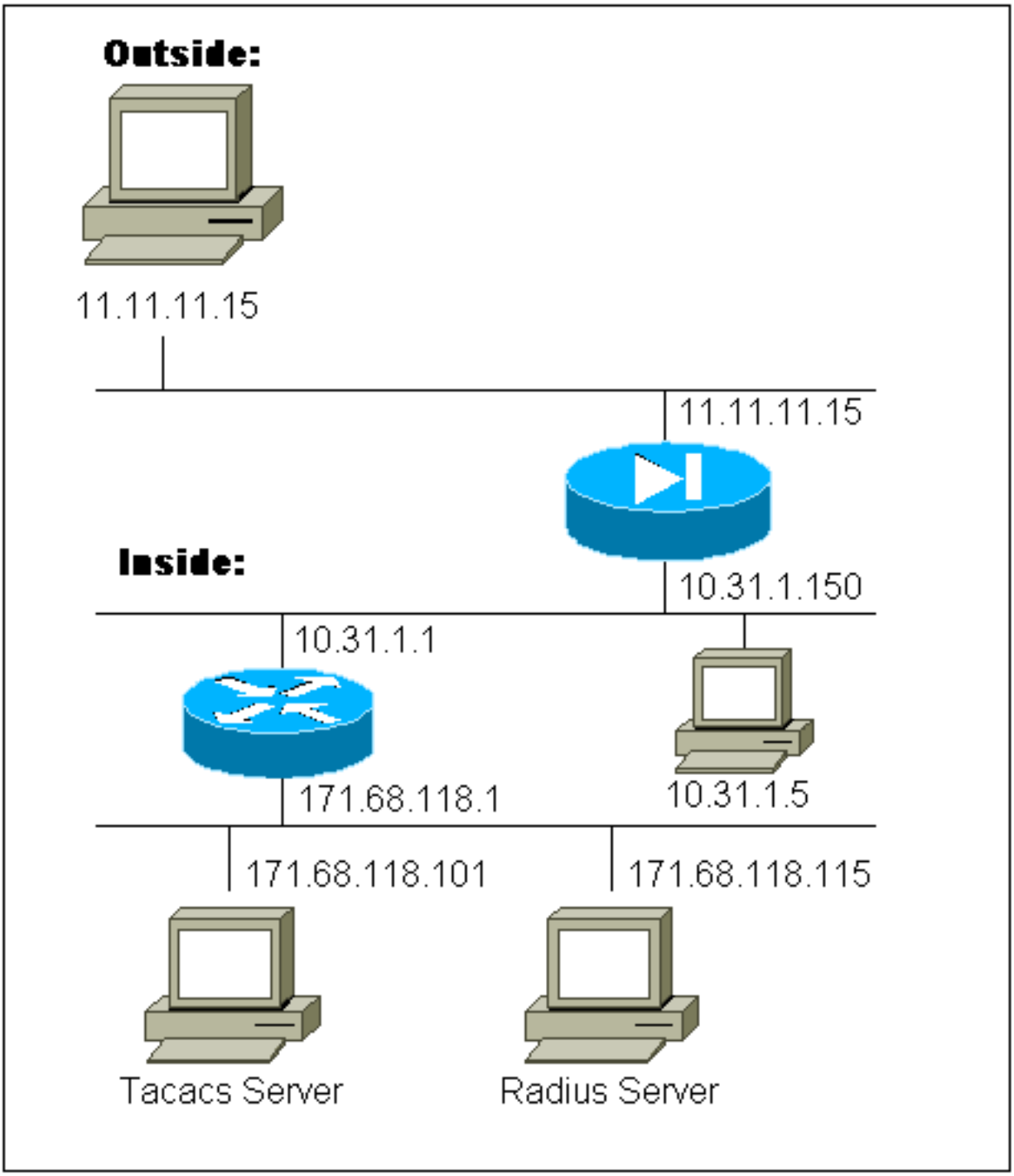
تكوين خادم TACACS+ FreeWARE

```
"key = "cisco

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

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

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

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

خطوات التصحيح

- تأكد من أن تكوينات PIX تعمل قبل إضافة المصادقة والتفويض والمحاسبة (AAA).إذا تعذر عليك تمرير حركة المرور قبل إنشاء المصادقة والتفويض، 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 أمر **logging buffered debuing**. يمكن 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.

الرسم التخطيطي للشبكة



تكوين PIX

```
pix-5# write terminal
...Building configuration
Saved :
:
(PIX Version 4.4(1
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 pix/intf2 security10
nameif ethernet3 pix/intf3 security15
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix-5
fixup protocol ftp 21
fixup protocol http 80
fixup protocol smtp 25
fixup protocol h323 1720
```

```
                                    fixup protocol rsh 514
                                fixup protocol sqlnet 1521
                                                    names
                                          pager lines 24
                                    no logging timestamp
                                logging console debugging
                                       no logging monitor
                                     no logging buffered
                                  logging trap debugging
                                     logging facility 20
                                 interface ethernet0 auto
                                 interface ethernet1 auto
                                 interface ethernet2 auto
                                 interface ethernet3 auto
                                         mtu outside 1500
                                          mtu inside 1500
                                       mtu pix/intf2 1500
                                       mtu pix/intf3 1500
            ip address outside 11.11.11.1 255.255.255.0
            ip address inside 10.31.1.150 255.255.255.0
         ip address pix/intf2 127.0.0.1 255.255.255.255
         ip address pix/intf3 127.0.0.1 255.255.255.255
                                                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 pix/intf2 0.0.0.0
                    failover ip address pix/intf3 0.0.0.0
                                        arp timeout 14400
     global (outside) 1 11.11.11.10-11.11.11.14 netmask
                                                255.255.255.0
     static (inside,outside) 11.11.11.20 171.68.118.115
                                 netmask 255.255.255.255 0 0
     static (inside,outside) 11.11.11.21 171.68.118.101
                                 netmask 255.255.255.255 0 0
  static (inside,outside) 11.11.11.22 10.31.1.5 netmask
                                         255.255.255.255 0 0
                              conduit permit icmp any any
                               conduit permit tcp any any
                                   no rip outside passive
                                   no rip outside default
                                    no rip inside passive
                                    no rip inside default
                                 no rip pix/intf2 passive
                                 no rip pix/intf2 default
                                 no rip pix/intf3 passive
                                 no rip pix/intf3 default
                 route inside 0.0.0.0 0.0.0.0 10.31.1.1 1
 timeout xlate 3:00:00 conn 1:00:00 half-closed 0:10:00
                                                udp 0:02:00
                          timeout rpc 0:10:00 h323 0:05:00
                            timeout uauth 0:00:00 absolute
                       +aaa-server TACACS+ protocol tacacs
                         aaa-server RADIUS protocol radius
                                                         !
  For any given list, multiple AAA servers can !--- ---!
  be configured. They will be !--- tried sequentially if
 any one of them is down. ! aaa-server Outgoing protocol
tacacs+ aaa-server Outgoing (inside) host 171.68.118.101
    cisco timeout 10 aaa-server Incoming protocol radius
  aaa-server Incoming (inside) host 171.68.118.115 cisco
      timeout 10 aaa authentication ftp outbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 Outgoing aaa authentication http
   outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing aaa
```

```
authentication telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 Outgoing aaa authentication ftp inbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa authentication http
inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa
authentication telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 Incoming no snmp-server location no snmp-server
contact snmp-server community public no snmp-server
enable traps telnet timeout 5 terminal width 80
Cryptochecksum:b287a37a676262275a4201cac52399ca : end
```

أمثلة تصحيح أخطاء المصادقة من PIX

في أمثلة تصحيح الأخطاء هذه:

صادر

يقوم المستخدم الداخلي في 10.31.1.5 ببدء حركة المرور إلى خارج 11.11.11.15 وتتم مصادقته من خلال TACACS+ (حركة المرور الصادرة تستخدم قائمة الخادم "الصادرة" التي تتضمن خادم TACACS 171.68.118.101).

داخل

يقوم المستخدم الخارجي في 11.11.11.15 ببدء حركة المرور إلى داخل 10.31.1.5 (11.11.22) وتتم مصادقته من خلال RADIUS (تستخدم حركة المرور الواردة قائمة الخادم "الواردة" التي تتضمن خادم RADIUS 171.68.118.115).

تصحيح أخطاء PIX - مصادقة جيدة - TACACS+

يوضح المثال التالي تصحيح أخطاء PIX بمصادقة جيدة:

```
Auth start for user '???' from 10.31.1.5/11004 to 11.11.11.15/23 :109001
Authen Session Start: user 'ddunlap', sid 3 :109011
'Authentication succeeded for user 'ddunlap :109005
from 10.31.1.5/11004 to 11.11.11.15/23
Authen Session End: user 'ddunlap', sid 3, elapsed 1 seconds :109012
Built outbound TCP connection 4 for faddr 11.11.11.15/23 gaddr :302001
laddr 10.31.1.5/11004 11.11.11.22/11004
```

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

يوضح المثال التالي تصحيح أخطاء PIX بمصادقة غير صحيحة (اسم المستخدم أو كلمة المرور). يرى المستعمل أربعة username/كلمة مجموعة. تعرض الرسالة التالية: "خطأ: الحد الأقصى لعدد المحاولات التي تم تجاوزها".

```
Auth start for user '???' from 10.31.1.5/11005 to 11.11.11.15/23 :109001
Authentication failed for user '' from 10.31.1.5/11005 to 11.11.11.15/23 :109006
```

تصحيح أخطاء PIX - إمكانية إختبار الاتصال، ولكن دون إستجابة - TACACS+

يوضح المثال التالي تصحيح أخطاء PIX لخادم قابل للجمع لا يتحدث إلى PIX. يرى المستخدم اسم المستخدم مرة واحدة، ولا يطلب PIX أبدا كلمة مرور (هذه على Telnet).

```
'Error: Max number of tries exceeded'
```

```
Auth start for user '???' from 10.31.1.5/11006 to 11.11.11.15/23 :109001
                Auth from 10.31.1.5/11006 to 11.11.11.15/23 failed :109002
                                          (server 171.68.118.101 failed)
                Auth from 10.31.1.5/11006 to 11.11.11.15/23 failed :109002
                                          (server 171.68.118.101 failed)
 URL Server 171.68.118.101 not responding, trying 171.68.118.101 :304006
                Auth from 10.31.1.5/11006 to 11.11.11.15/23 failed :109002
                                          (server 171.68.118.101 failed)
Authentication failed for user '' from 10.31.1.5/11006 to 11.11.11.15/23 :109006
```

تصحيح أخطاء PIX - لا يمكن إختيار اتصال الخادم - TACACS+

يوضح المثال التالي تصحيح أخطاء PIX لخادم غير قابل للجلب. يرى المستعمل ال username مرة. لا يطلب PIX كلمة مرور (هذا على Telnet). تعرض الرسالة التالية: "المهلة إلى خادم TACACS+" و"الخطأ: الحد الأقصى لعدد المحاولات التي تم تجاوزها" (يعكس التكوين الموجود في هذا المثال خادما زائفا).

```
Auth start for user '???' from 10.31.1.5/11007 to 11.11.11.15/23 :109001
                Auth from 10.31.1.5/11007 to 11.11.11.15/23 failed :109002
                                          (server 171.68.118.199 failed)
                Auth from 10.31.1.5/11007 to 11.11.11.15/23 failed :109002
                                          (server 171.68.118.199 failed)
 URL Server 171.68.118.199 not responding, trying 171.68.118.199 :304006
                Auth from 10.31.1.5/11007 to 11.11.11.15/23 failed :109002
                                          (server 171.68.118.199 failed)
Authentication failed for user '' from 10.31.1.5/11007 to 11.11.11.15/23 :109006
```

تصحيح أخطاء PIX - مصادقة جيدة - RADIUS

يوضح المثال التالي تصحيح أخطاء PIX بمصادقة جيدة:

```
Auth start for user '???' from 11.11.11.15/11003 to 10.31.1.5/23 :109001
                  Authen Session Start: user 'adminuser', sid 4 :109011
                  'Authentication succeeded for user 'adminuser :109005
                                  from 10.31.1.5/23 to 11.11.11.15/11003
  Authen Session End: user 'adminuser', sid 4, elapsed 1 seconds :109012
                      Built inbound TCP connection 5 for faddr :302001
 gaddr 11.11.11.22/23 laddr 10.31.1.5/23 11.11.11.15/11003
```

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

يوضح المثال التالي تصحيح أخطاء PIX بمصادقة غير صحيحة (اسم المستخدم أو كلمة المرور). يرى المستخدم طلبا لاسم المستخدم وكلمة المرور. إذا كان أي منهما خطأ، تعرض الرسالة "كلمة مرور غير صحيحة" أربع مرات. ثم يتم قطع اتصال المستخدم. تم تعيين معرف الخطأ CSCdm46934# لهذه المشكلة.

```
                                'Error: Max number of tries exceeded'
                Auth start for user '???' from 11.11.11.15/11007 to 10.31.1.5/23 :109001
Authentication failed for user '' from 10.31.1.5/23 to 11.11.11.15/11007 :109006
```

تصحيح أخطاء PIX - النسيان لأسفل، لن يتصل ب PIX - RADIUS

يوضح المثال التالي تصحيح أخطاء PIX باستخدام خادم قابل للانقسام، ولكن البرنامج الخفي قد تعطل. لن يتصل الخادم ب PIX. يرى المستخدم اسم المستخدم، متبوعا بكلمة مرور. تظهر الرسائل التالية: "فشل خادم RADIUS" و"خطأ: تجاوز الحد الأقصى لعدد المحاولات".

```
Auth start for user '???' from 11.11.11.15/11008 to 10.31.1.5/23 :109001
```

```
Auth from 10.31.1.5/23 to 11.11.11.15/11008 failed :109002
                                        (server 171.68.118.115 failed)
Auth from 10.31.1.5/23 to 11.11.11.15/11008 failed :109002
                                        (server 171.68.118.115 failed)
URL Server 171.68.118.115 not responding, trying 171.68.118.115 :304006
Auth from 10.31.1.5/23 to 11.11.11.15/11008 failed :109002
                                        (server 171.68.118.115 failed)
Authentication failed for user '' from 10.31.1.5/23 to 11.11.11.15/11008 :109006
```

تصحيح أخطاء PIX - لا يمكن إختبار اتصال الخادم أو المفتاح/العميل غير المتطابق - RADIUS

يوضح المثال التالي تصحيح أخطاء PIX لخادم غير قابل للجمع أو حيث يوجد عدم تطابق في المفتاح/العميل. يرى المستعمل username وكلمة. تظهر الرسائل التالية: "المهلة إلى خادم RADIUS" و"الخطأ: الحد الأقصى لعدد المحاولات التي تم تجاوزها" (الخادم في التكوين لأغراض معينة فقط).

```
Auth start for user '???' from 11.11.11.15/11009 to 10.31.1.5/23 :109001
Auth from 10.31.1.5/23 to 11.11.11.15/11009 failed :109002
                                        (server 171.68.118.199 failed)
Auth from 10.31.1.5/23 to 11.11.11.15/11009 failed :109002
                                        (server 171.68.118.199 failed)
URL Server 171.68.118.199 not responding, trying 171.68.118.199 :304006
Auth from 10.31.1.5/23 to 11.11.11.15/11009 failed :109002
                                        (server 171.68.118.199 failed)
Authentication failed for user '' from 10.31.1.5/23 to 11.11.11.15/11009 :109006
```

إضافة التخويل

بما أن التخويل غير صالح دون مصادقة، فإننا سنحتاج إلى التخويل لنفس نطاق المصدر والوجهة:

```
aaa authorization ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
aaa authorization http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
aaa authorization telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
```

صادر

لاحظ أننا لا نقوم بإضافة تخويل ل "الوارد" لأن حركة المرور الواردة تتم مصادقتها باستخدام RADIUS، وترخيص RADIUS غير صالح

أمثلة تصحيح أخطاء المصادقة والتفويض من PIX

تصحيح أخطاء PIX بمصادقة جيدة وتفويض ناجح - TACACS+

يوضح المثال التالي تصحيح أخطاء PIX باستخدام المصادقة الجيدة والتفويض الناجح:

```
Auth start for user '???' from 10.31.1.5/11002 to 11.11.11.15/23 :109001
        Authen Session Start: user 'can_only_do_telnet', sid 7 :109011
        'Authentication succeeded for user 'can_only_do_telnet :109005
                                from 10.31.1.5/11002 to 11.11.11.15/23
        Authen Session Start: user 'can_only_do_telnet', sid 7 :109011
         'Authorization permitted for user 'can_only_do_telnet :109007
                                from 10.31.1.5/11002 to 11.11.11.15/23
          ,Authen Session End: user 'can_only_do_telnet', sid 7 :109012
                                                    elapsed 1 seconds
```

```
Built outbound TCP connection 6 for faddr 11.11.11.15/23 :302001
(gaddr 11.11.11.22/11002 laddr 10.31.1.5/11002 (can_only_do_telnet
```

تصحيح أخطاء PIX - مصادقة جيدة، تفويض فشل - TACACS+

يوضح المثال التالي تصحيح أخطاء PIX بمصادقة جيدة، ولكنه فشل في التفويض:

هنا يرى المستخدم أيضا الرسالة "خطأ: تم رفض التخويل"

```
Auth start for user '???' from 10.31.1.5/11000 to 11.11.11.15/23 :109001
            Authen Session Start: user 'can_only_do_ftp', sid 5 :109011
             'Authentication succeeded for user 'can_only_do_ftp :109005
                                  from 10.31.1.5/11000 to 11.11.11.15/23
              Authorization denied for user 'can_only_do_ftp' from :109008
                                          to 11.11.11.15/23 10.31.1.5/11000
Authen Session End: user 'can_only_do_ftp', sid 5, elapsed 33 seconds :109012
```

إضافة محاسبة

TACACS+

```
aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing
```

سيبدو تصحيح الأخطاء بنفس الطريقة سواء كانت عملية المحاسبة قيد التشغيل أو قيد الإيقاف. ومع ذلك، في وقت "الإنشاء"، سيتم إرسال سجل محاسبة "البدء". وفي وقت "التيرداون"، سيرسل سجل محاسبي "الإيقاف".

تبدو سجلات محاسبة TACACS+ كما يلي (هذه من CiscoSecure UNIX؛ وقد تكون السجلات الموجودة في CiscoSecure NT محددة بفاصلة بدلا من ذلك):

```
Thu Jun  3 10:41:50 1999 10.31.1.150 can_only_do_telnet
PIX 10.31.1.5 start task_id=0x7 foreign_ip=11.11.11.15
                                local_ip=10.31.1.5  cmd=telnet
Thu Jun  3 10:41:55 1999 10.31.1.150 can_only_do_telnet PIX 10.31.1.5
                                stop task_id=0x7 foreign_ip=11.11.11.15
local_ip=10.31.1.5 cmd=telnet elapsed_time=4 bytes_in=74 bytes_out=27
```

RADIUS

```
aaa accounting any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming
```

سيبدو تصحيح الأخطاء بنفس الطريقة سواء كانت عملية المحاسبة قيد التشغيل أو قيد الإيقاف. ومع ذلك، يتم إرسال سجل محاسبة "البدء" في وقت "الإنشاء". عند "التيردون"، يتم إرسال سجل محاسبة "إيقاف":

تبدو سجلات محاسبة RADIUS كما يلي: (هذه من CiscoSecure UNIX؛ وقد تكون السجلات الموجودة في CiscoSecure NT محددة بفاصلة بدلا من ذلك):

```
10.31.1.150adminuser -- start server=rtp-evergreen.rtp.cisco.com
                time=14:53:11 date=06/3/1999 task_id=0x00000008
                                    Thu Jun  3 15:53:11 1999
                            Acct-Status-Type = Start
```

```
                                        Client-Id = 10.31.1.150
                                         Login-Host = 10.31.1.5
                                            Login-TCP-Port = 23
                                  "Acct-Session-Id = "0x00000008
                                         "User-Name = "adminuser
adminuser -- stop server=rtp-evergreen.rtp.cisco.com 10.31.1.150
                      time=14:54:24 date=06/ 3/1999 task_id=0x00000008
                                               Thu Jun  3 15:54:24 1999
                                        Acct-Status-Type = Stop
                                        Client-Id = 10.31.1.150
                                         Login-Host = 10.31.1.5
                                            Login-TCP-Port = 23
                                  "Acct-Session-Id = "0x00000008
                                         "User-Name = "adminuser
                                          Acct-Session-Time = 73
                                          Acct-Input-Octets = 27
                                        Acct-Output-Octets = 73
```

أمر إستخدام EXCEPT

في شبكتنا، إذا قررنا أن المصدر و/أو الوجهة لا تحتاج إلى المصادقة، التخويل، أو المحاسبة، يمكننا القيام بشيء مثل التالي:

```
aaa authentication except outbound 10.31.1.60 255.255.255.255
                                Outgoing 255.255.255.255 11.11.11.15
aaa authorization except outbound 10.31.1.60 255.255.255.255
                                Outgoing 255.255.255.255 11.11.11.15
```

إذا كنت تقوم "باستثناء" عناوين IP من المصادقة وكان لديك تفويض عليها، فيجب عليك أيضا إستثنائها من التفويض!

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. عندما يكون هناك سجل "بدء" محاسبة تم إنشاؤه ولكن لم يتم "إيقاف"، يفترض خادم TACACS+ أو RADIUS أن الشخص لا يزال قيد تسجيل الدخول (أي أن لديه جلسة عمل من خلال PIX).

يعمل هذا بشكل جيد لاتصالات Telnet و FTP بسبب طبيعة الاتصالات. لا يعمل هذا بشكل جيد ل HTTP بسبب طبيعة الاتصال. في المثال التالي، يتم إستخدام تكوين شبكة مختلف ولكن المفاهيم هي نفسها.

يقوم المستخدم بالتوصيل من خلال PIX، للمصادقة 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)
                                        to 9.9.9.25/23 00 171.68.118.100/12
               pix) 302001: Built TCP connection 5 for faddr 9.9.9.25/23)
                     (gaddr 9.9.9.10/12 00 laddr 171.68.118.100/1200 (cse
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 "البدء" ولكن ليس سجل "إيقاف" (في هذه المرحلة من الوقت)، سيظهر 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 (بافتراض أن الخادم يدعم الحد الأقصى لجلسات العمل)، فسيرفض الخادم الاتصال.

تواصل المستخدم عملها في برنامج Telnet أو FTP على المضيف الهدف، ثم تخرج (تقضي 10 دقائق هناك):

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

server stop account) Sun Nov 8 16:41:17 1998 rtp-pinecone.rtp.cisco.com cse)

PIX 171.68.118.100 stop task_id=0x3 foreign_ip=9.9.9.25 local_ip=171.68.118.100
cmd=telnet elapsed_time=5 bytes_in=98 bytes_out=36
```

سواء كانت المصادقة هي 0 (المصادقة كل مرة) أو أكثر (المصادقة مرة واحدة وليس مرة أخرى خلال فترة المصادقة)، يتم خفض سجل محاسبة لكل موقع يتم الوصول إليه.

ومع ذلك، يعمل HTTP بشكل مختلف نظرا لطبيعة البروتوكول. فيما يلي مثال على HTTP.

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)
to 9.9.9.25/80 81 171.68.118.100/12
pix) 302001: Built TCP connection 5 for faddr 9.9.9.25/80 gaddr)
(laddr 171.68.118.100/1281 (cse 81 9.9.9.10/12
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)
(laddr 171.68.118.100/1281 duration 0:00:00 bytes 1907 (cse 1 9.9.9.10/128
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 الويب التي تم تنزيلها.

سجل البداية المنشور في 16:35:34، وسجل التوقف المنشور في 16:35:35. استغرق هذا التنزيل ثانية واحدة (أي أنه كان هناك أقل من ثانية واحدة بين سجل البداية وسجل التوقف). هل لا يزال المستخدم يسجل الدخول إلى موقع ويب ولا يزال الاتصال مفتوحا عندما يقرأ صفحة ويب؟ لا. هل سيعمل الحد الأقصى لجلسات العمل أو عرض المستخدمين الذين تم تسجيل دخولهم هنا؟ لا، لأن وقت الاتصال (الوقت بين "Build" و"Teardown") في HTTP قصير جدا. سجل "البدء" و"الإيقاف" هو الثاني الفرعي. 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.

المصادقة والتمكين على PIX نفسه

كانت المناقشة السابقة حول مصادقة حركة مرور Telnet (و FTP، HTTP) من خلال PIX. في المثال التالي، نتأكد من أن Telnet إلى PIX يعمل دون مصادقة على:

```
telnet 10.31.1.5 255.255.255.255
passwd ww
```

بعد ذلك، نقوم بإضافة الأمر لمصادقة المستخدمين الذين يتصلون ب Telnet إلى PIX:

```
aaa authentication telnet console Outgoing
```

عند مطالبة المستخدمين Telnet إلى PIX، بكلمة مرور برنامج ww") Telnet"). كما يطلب PIX اسم مستخدم وكلمة مرور TACACS+ في هذه الحالة (نظرا لاستخدام قائمة خادم "الصادر") أو اسم مستخدم وكلمة مرور RADIUS.

```
aaa authentication enable console Outgoing
```

باستخدام هذا الأمر، تتم مطالبة المستخدم باسم مستخدم وكلمة مرور يتم إرسالها إلى خادم TACACS أو RADIUS. في هذه الحالة، حيث أنه يتم إستخدام قائمة الخادم "الصادرة"، يذهب الطلب إلى خادم TACACS. بما أن حزمة المصادقة للتمكين هي نفسها حزمة المصادقة لتسجيل الدخول، فيمكن للمستخدم التمكين من خلال TACACS أو RADIUS بنفس اسم المستخدم/كلمة المرور، بافتراض أنه يمكن للمستخدم تسجيل الدخول إلى PIX باستخدام TACACS أو RADIUS. تم تعيين معرف الخطأ #CSCdm47044 لهذه المشكلة.

في حالة تعطل الخادم، يمكن للمستخدم الوصول إلى وضع تمكين PIX بإدخال "PIX" لاسم المستخدم وكلمة مرور التمكين العادية من enable password any") PIX"). إذا لم يكن "enable password any" في تكوين PIX، فيجب على المستخدم إدخال "PIX" لاسم المستخدم والضغط على مفتاح Enter. في حالة تعيين كلمة مرور enable ولكن غير معروفة، يلزم وجود قرص إسترداد كلمة المرور لإعادة ضبطه.

المصادقة على وحدة التحكم التسلسلية

يتطلب الأمر **مصادقة وحدة التحكم التسلسلية AAA** التحقق من المصادقة للوصول إلي وحدة التحكم التسلسلية الخاصة ب PIX. عندما يقوم المستخدم بتنفيذ أوامر التكوين من وحدة التحكم، سيتم قطع رسائل syslog (إذا تم تكوين PIX لإرسال syslog على مستوى تصحيح الأخطاء إلى مضيف syslog). أدناه مثال من ال syslog نادل:

```
Jun  5 07:24:09 [10.31.1.150.2.2] %PIX-5-111008: User 'cse' executed
.the 'hostname' command
```

تغيير رسالة مطالبة المستخدمين

إذا كان لدينا الأمر:

```
auth-prompt THIS_IS_PIX_5
```

المستخدمون الذين يمرون ب PIX يرون التسلسل:

```
[THIS_IS_PIX_5 [at which point one would enter the username
    [Password:[at which point one would enter the password
```

وبعد ذلك، عند الوصول إلى مربع الوجهة النهائية، "username:" و "كلمة المرور:" مطالبة الغاية قدمت صندوق.

تؤثر هذه المطالبة فقط على المستخدمين الذين يمرون ب PIX، وليس ب PIX.

ملاحظة: لا توجد سجلات محاسبة مقطوعة للوصول إلى PIX.

تخصيص الرسالة التي يراها مستخدمو الرسالة عند النجاح/الفشل

إذا كانت لدينا الأوامر:

```
"auth-prompt accept "You're allowed through the pix
"auth-prompt reject "You blew it
```

سيرى المستخدمون ما يلي عند تسجيل الدخول الفاشل/الناجح من خلال PIX:

```
THIS_IS_PIX_5
Username: asjdkl
:Password
"You blew it"
"THIS_IS_PIX_5"
Username: cse
:Password
"You're allowed through the pix"
```

فترات الانتظار الخاملة والمطلقة لكل مستخدم

يمكن إرسال فترات الانتظار الخاملة والمطلقة من خادم TACACS+ على أساس كل مستخدم. إذا كان لكافة المستخدمين في شبكتك نفس "المهلة"، فلا تقم بتنفيذ هذا! ولكن إذا كنت تحتاج إلى أجهزة مختلفة لكل مستخدم، فقراءة على.

في المثال الخاص بنا على PIX، نستخدم الأمر **timeout** من **النوع** 3:00:00. وهذا يعني أنه بمجرد مصادقة الشخص، لن يتعين عليه إعادة المصادقة لمدة 3 ساعات. ولكن إذا قمنا بإعداد مستخدم بملف التعريف التالي وكان لدينا تفويض TACACS AAA قيد التشغيل في PIX، فإن المهلة الخاملة والمطلقة في ملف تعريف المستخدم تتجاوز المهلة في PIX لذلك المستخدم. لا يعني ذلك أن جلسة عمل Telnet من خلال PIX يتم قطع إتصالها بعد انتهاء المهلة الخاملة/المطلقة. إنها فقط تتحكم فيما إذا كانت تتم إعادة المصادقة أم لا.

```
} user = timeout
default service = permit
"login = cleartext "timeout
} service = exec
timeout = 2
idletime = 1
{
{
```

بعد المصادقة، قم بإصدار أمر **show uauth** على PIX:

```
pix-5# show uauth
Current    Most Seen
Authenticated Users       1          1
Authen In Progress        0          1
:user 'timeout' at 10.31.1.5, authorized to
port 11.11.11.15/telnet
absolute   timeout: 0:02:00
inactivity timeout: 0:01:00
```

بعد أن يجلس المستخدم في وضع الخمول لمدة دقيقة واحدة، يظهر تصحيح الأخطاء الموجود على PIX:

```
Authen Session End: user 'timeout', sid 19, elapsed 91 seconds :109012
```

سيتعين على المستخدم إعادة المصادقة عند الرجوع إلى المضيف الهدف نفسه أو مضيف مختلف.

HTTP الظاهري

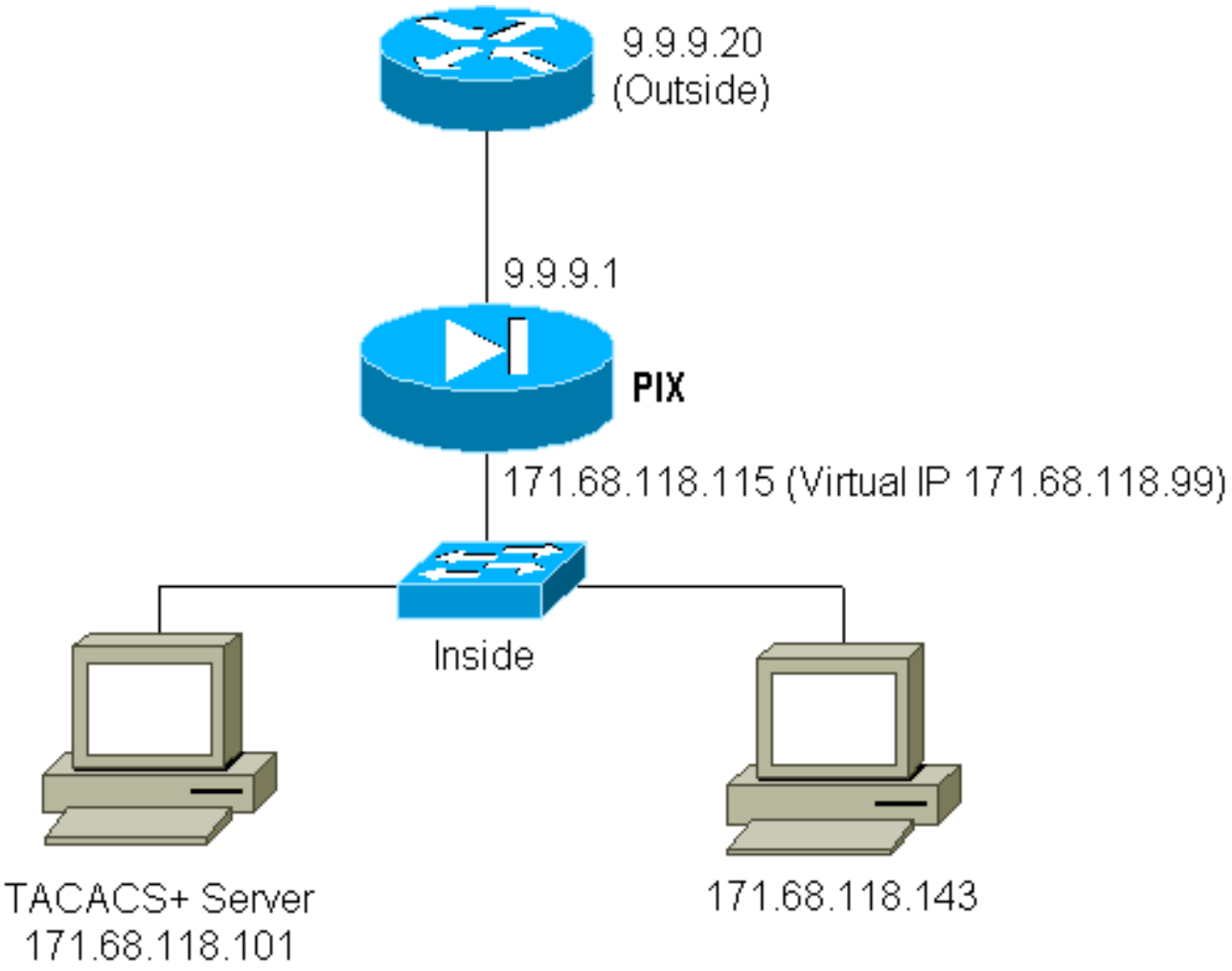
إذا كانت المصادقة مطلوبة على مواقع خارج PIX، وكذلك على PIX نفسه، فيمكن ملاحظة سلوك غير عادي للمستعرض في بعض الأحيان نظرا لأن المستعرضات تخزن اسم المستخدم وكلمة المرور مؤقتا.

لتجنب هذا، يمكنك تنفيذ HTTP ظاهري بإضافة عنوان RFC 1918 (وهو عنوان غير قابل للتوجيه على الإنترنت، ولكنه صالح وفريد لشبكة PIX الداخلية) إلى تكوين PIX باستخدام الأمر التالي:

```
[virtual http #.#.#.# [warn
```

عندما يحاول المستخدم الخروج من PIX، تكون المصادقة مطلوبة. إذا كانت المعلمة WARN موجودة، يتلقى المستخدم رسالة إعادة توجيه. تعد المصادقة جيدة لطول الوقت في الوحدة. كما هو موضح في التوثيق، لا تقم بتعيين مدة الأمر uth **timeout** إلى 0 ثوان مع HTTP الظاهري، وهذا يمنع إتصالات HTTP بخادم الويب الحقيقي.

مثال HTTP Outbound الظاهري:



:PIX Configuration Virtual HTTP Outbound

```
ip address outside 9.9.9.1 255.255.255.0
```

```
ip address inside 171.68.118.115 255.255.255.0
global (outside) 1 9.9.9.5-9.9.9.9 netmask 255.0.0.0
timeout uauth 01:00:00
+aaa-server TACACS+ protocol tacacs
+aaa-server Outgoing protocol tacacs
aaa-server Outgoing (inside) host 171.68.118.101 cisco timeout 10
aaa authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing
virtual http 171.68.118.99
auth-prompt THIS_IS_PIX_5
```

برنامج Telnet الظاهري

تكوين PIX لمصادقة جميع حركة المرور الواردة والصادرة ليست فكرة جيدة نظرا لأنه لا يمكن مصادقة بعض البروتوكولات، مثل "mail"، بسهولة. عندما يحاول خادم بريد وعميل الاتصال من خلال PIX عندما تتم مصادقة جميع حركات مرور البيانات عبر PIX، سيقوم PIX syslog للبروتوكولات غير القابلة للمصادقة بإظهار رسائل مثل:

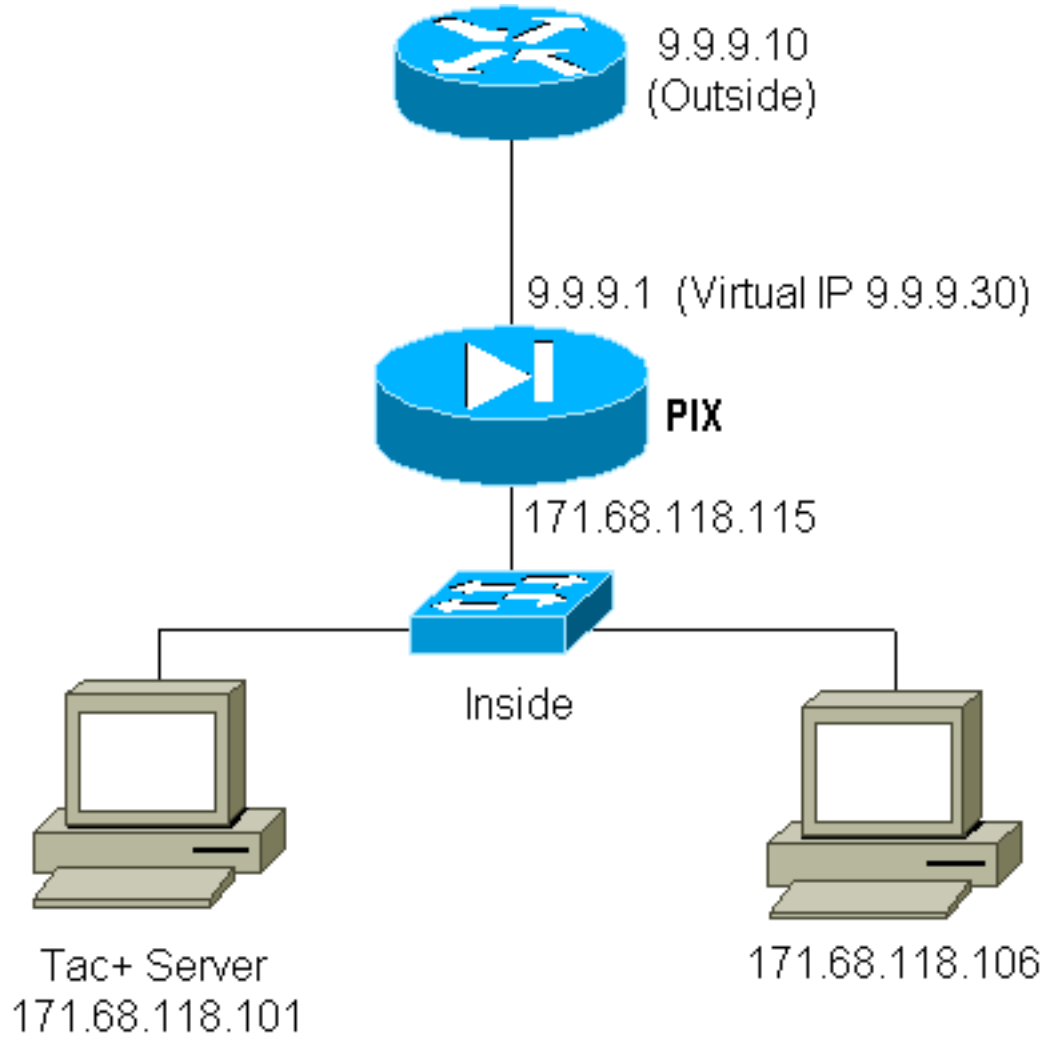
```
Auth start for user '???' from 9.9.9.10/11094 to 171.68.118.106/25 :109001
Authorization denied from 171.68.118.106/49 to 9.9.9.10/11094 :109009
not authenticated)
```

نظرا لأن البريد وبعض الخدمات الأخرى ليست تفاعلية بشكل كاف للمصادقة، فإن أحد الحلول هو إستخدام الأمر **except** للمصادقة/التفويض (مصادقة الكل باستثناء مصدر/وجهة خادم/عميل البريد).

ولكن إذا كانت هناك حاجة حقيقية لمصادقة نوع ما من الخدمة غير العادية، يمكن القيام بذلك باستخدام الأمر **virtual telnet**. يسمح هذا الأمر بظهور المصادقة إلى Telnet IP الظاهري. بعد هذه المصادقة، يمكن لحركة مرور الخدمة غير العادية الانتقال إلى الخادم الحقيقي المرتبط ب IP الظاهري.

في مثالنا، نريد السماح لحركة مرور منفذ TCP رقم 49 بالتدفق من المضيف الخارجي 9.9.9.10 إلى المضيف الداخلي 171.68.118.106. حيث أن حركة المرور هذه ليست حقا قابلة للمصادقة، فقد قمنا بإعداد برنامج Telnet ظاهري.

الوارد لبرنامج Telnet الظاهري:



:PIX Configuration Virtual Telnet Inbound

```
ip address outside 9.9.9.1 255.255.255.0
ip address inside 171.68.118.115 255.255.255.0
static (inside,outside) 9.9.9.30 171.68.118.106 netmask 255.255.255.255 0 0
conduit permit tcp host 9.9.9.30 host 9.9.9.10
+aaa-server TACACS+ protocol tacacs
+aaa-server Incoming protocol tacacs
aaa-server Incoming (inside) host 171.68.118.101 cisco timeout 5
aaa authentication any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming
virtual telnet 9.9.9.30
```

تكوين مستخدم خادم TACACS+ الوارد الظاهري ل Telnet:

```
} user = pinecone
default service = permit
"login = cleartext "pinecone
} service = exec
timeout = 10
idletime = 10
{
{
```

الوارد لبرنامج Telnet الظاهري لتصحيح أخطاء PIX:

يجب أن يقوم المستخدم في 9.9.9.10 بالمصادقة أولا عن طريق الاتصال بالشبكة إلى عنوان 9.9.9.30 على PIX:

```
pixfirewall# 109001: Auth start for user '???' from 9.9.9.10/11099
                                                to 171.68.118.106/23
            Authen Session Start: user 'pinecone', sid 13 :109011
  Authentication succeeded for user 'pinecone' from :109005
                                  to 9.9.9.10/11099 171.68.118.106/23
```

بعد المصادقة الناجحة، يظهر الأمر **show uauth** أن المستخدم لديه "الوقت على العداد":

```
                                        pixfirewall# show uauth
                        Current    Most Seen
                              Authenticated Users       1          1
                              Authen In Progress        0          1
                        user 'pinecone' at 9.9.9.10, authenticated
                                        absolute   timeout: 0:10:00
                                        inactivity timeout: 0:10:00
```

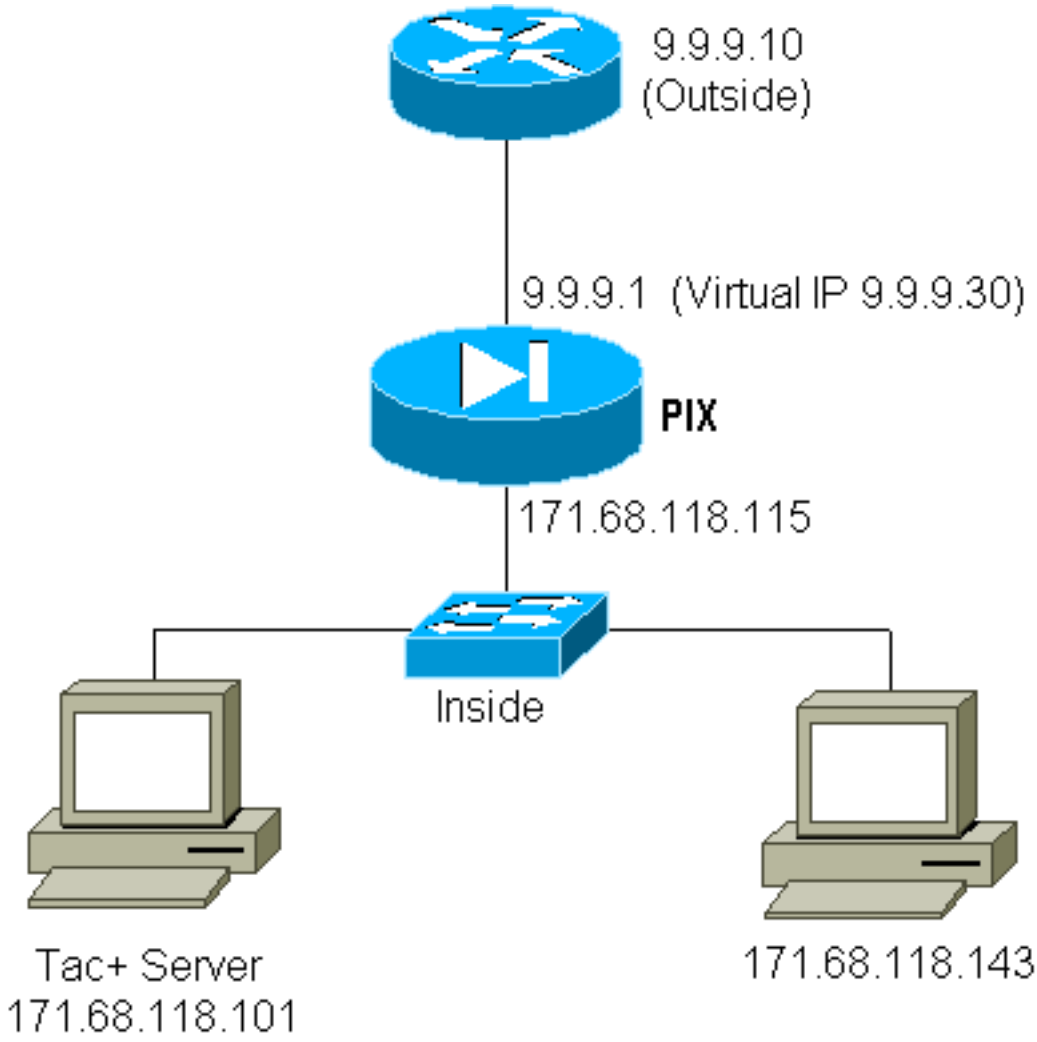
وعندما يريد الجهاز في 9.9.9.10 إرسال حركة مرور TCP/49 إلى الجهاز على 171.68.118.106:

```
'pixfirewall# 109001: Auth start for user 'pinecone
                          from 9.9.9.10/11104 to 171.68.118.106/49
            Authen Session Start: user 'pinecone', sid 14 :109011
  Authorization permitted for user 'pinecone' from 9.9.9.10/11104 :109007
                                                to 171.68.118.106/49
      Built TCP connection 23 for faddr 9.9.9.10/11104 gaddr :302001
                                    (laddr 171.68.118.106/49 (pinecone 9.9.9.30/49
Teardown TCP connection 23 faddr 9.9.9.10/11104 gaddr 9.9.9.30/49 :302002
                    (laddr 171.68.118.106/49 duration 0:00:10 bytes 179 (pinecone
```

الصادر لبرنامج Telnet الظاهري:

بما أن حركة المرور الصادرة مسموح بها بشكل افتراضي، فلا حاجة إلى وجود حركة مرور ثابتة لاستخدام الصادر الظاهري لبرنامج Telnet. في المثال التالي، سيقوم المستخدم الداخلي في 171.68.118.143 باستخدام برنامج Telnet إلى الإصدار Virtual 9.9.9.30 والمصادقة. تم إسقاط اتصال برنامج Telnet على الفور.

بمجرد التصديق، يتم السماح بحركة مرور TCP من 171.68.118.143 إلى الخادم على 9.9.9.10:



خرج Telnet الظاهري لتكوين PIX:

```
ip address outside 9.9.9.1 255.255.255.0
ip address inside 171.68.118.115 255.255.255.0
global (outside) 1 9.9.9.5-9.9.9.9 netmask 255.0.0.0
timeout uauth 00:05:00
+aaa-server TACACS+ protocol tacacs
+aaa-server Outgoing protocol tacacs
aaa-server Outgoing (inside) host 171.68.118.101 cisco timeout 10
aaa authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing
virtual telnet 9.9.9.30
```

الصادر عن برنامج PIX Debug Virtual Telnet:

```
Auth start for user '???' from 171.68.118.143/1536 to 9.9.9.30/23 :109001
Authen Session Start: user 'timeout_143', sid 25 :109011
Authentication succeeded for user 'timeout_143' from :109005
to 9.9.9.30/23 171.68.118.143/1536
Built TCP connection 46 for faddr 9.9.9.10/80 gaddr 9.9.9.30/1537 :302001
(laddr 171.68 .118.143/1537 (timeout_143
/:timeout_143@171.68.118.143 Accessed URL 9.9.9.10 :304001
Built TCP connection 47 for faddr 9.9.9.10/80 gaddr 9.9.9.30/1538 :302001
(laddr 171.68 .118.143/1538 (timeout_143
Teardown TCP connection 46 faddr 9.9.9.10/80 gaddr 9.9.9.30/1537 :302002
(laddr 171.68. 118.143/1537 duration 0:00:03 bytes 625 (timeout_143
/:timeout_143@171.68.118.143 Accessed URL 9.9.9.10 :304001
Teardown TCP connection 47 faddr 9.9.9.10/80 gaddr 9.9.9.30/1538 :302002
```

```
(laddr 171.68. 118.143/1538 duration 0:00:01 bytes 2281 (timeout_143
in use, 1 most used 0 :302009
```

تسجيل الخروج من برنامج Telnet الظاهري

عندما يقوم المستخدم Telnet إلى Telnet IP الظاهري، فإن الأمر **show uauth** يعرض حالته. إذا أراد المستخدم منع حركة المرور بعد انتهاء جلسة عمله (عندما يكون هناك وقت متبقي في الوحدة)، فإنه يحتاج إلى Telnet إلى برنامج Telnet الظاهري IP مرة أخرى. يتم الآن تبديل جلسة العمل.

تفويض المنفذ

يمكنك طلب تفويض على نطاق من المنافذ. في المثال التالي، كانت المصادقة لا تزال مطلوبة لجميع المنافذ الصادرة، ولكن يكون التخويل مطلوبا فقط لمنافذ TCP 23-49.

تهيئة PIX:

```
aaa authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing
aaa authorization tcp/23-49 outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing
```

لذلك، عندما نحن Telnet من 171.68.118.143 إلى 9.9.9.10، حدثت المصادقة والتفويض لأن Telnet port 23 هو في النطاق 23-49. عند إجراء جلسة عمل HTTP من 171.68.118.143 إلى 9.9.9.10، ما يزال يتعين علينا المصادقة، ولكن لا يطلب PIX من خادم TACACS+ تخويل HTTP لأن 80 ليست في النطاق 23-49.

تكوين خادم TACACS+ FreeWARE

```
                                } user = telnetrange
                    "login = cleartext "telnetrange
                                } cmd = tcp/23-49
                                  permit 9.9.9.10
                                                {
                                                {
```

لاحظ أن PIX يرسل "cmd=tcp/23-49" و"cmd-arg=9.9.9.10" إلى خادم TACACS+.

تصحيح الأخطاء على PIX:

```
Auth start for user '???' from 171.68.118.143/1051 to 9.9.9.10/23 :109001
                Authen Session Start: user 'telnetrange', sid 0 :109011
            Authentication succeeded for user 'telnetrange' from :109005
                                  to 9. 9.9.10/23 171.68.118.143/1051
                Authen Session Start: user 'telnetrange', sid 0 :109011
             Authorization permitted for user 'telnetrange' from :109007
                                  to 9.9 .9.10/23 171.68.118.143/1051
  Built TCP connection 0 for faddr 9.9.9.10/23 gaddr 9.9.9.5/1051 :302001
                                (laddr 171.68.1 18.143/1051 (telnetrange
Auth start for user '???' from 171.68.118.143/1105 to 9.9.9.10/80 :109001
Auth start for user '???' from 171.68.118.143/1110 to 9.9.9.10/80 :109001
                Authen Session Start: user 'telnetrange', sid 1 :109011
            Authentication succeeded for user 'telnetrange' from :109005
                                  to 9. 9.9.10/80 171.68.118.143/1110
  Built TCP connection 1 for faddr 9.9.9.10/80 gaddr 9.9.9.5/1110 :302001
                                (laddr 171.68.1 18.143/1110 (telnetrange
  Built TCP connection 2 for faddr 9.9.9.10/80 gaddr 9.9.9.5/1111 :302001
```

```
(laddr 171.68.1 18.143/1111 (telnetrange
Teardown TCP connection 1 faddr 9.9.9.10/80 gaddr 9.9.9.5/1110 :302002
(laddr 171.68.11 8.143/1110 duration 0:00:08 bytes 338 (telnetrange
/:timeout_143@171.68.118.143 Accessed URL 9.9.9.10 :304001
Teardown TCP connection 2 faddr 9.9.9.10/80 gaddr 9.9.9.5/1111 laddr :302002
(duration 0:00:01 bytes 2329 (telnetrange 8.143/1111 171.68.11
```

معلومات ذات صلة

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

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).