تكوين PIX 5.0.x: TACACS+ و RADIUS

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. تفويض RADIUS غير صحيح. تتضمن التغييرات في مصادقة PIX 5.0 والتفويض والمحاسبة (AAA) عبر الإصدار السابق محاسبة AAA لحركة المرور بخلاف HTTP و FTP و Telnet.

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.

على سبيل المثال، افترض أن لديك مائة مستخدم بالداخل وتريد فقط أن يكون ستة من هؤلاء المستخدمين قادرين على 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. وباستخدام *مصادقة* بسيطة، يمكن مصادقة هؤلاء المستخدمين الستة باستخدام اسم المستخدم وكلمة المرور، ثم الخروج. أما المستخدمين الأربعة والتسعون الآخرون فلا يستطيعون الخروج. يطلب PIX من المستخدمين اسم المستخدم/كلمة المرور، ثم يقوم بتمرير اسم المستخدم وكلمة المرور إلى خادم أمان TACACS+/RADIUS. اعتمادا على الاستجابة، فإنه يفتح الاتصال أو ينفيه. يمكن لهؤلاء المستخدمين الستة تنفيذ بروتوكول FTP أو Telnet أو HTTP.

ومن ناحية أخرى، افترض أن *واحدا* من هؤلاء المستخدمين الثلاثة، "تيري"، ليس محل ثقة. تود أن تسمح لتيري بعمل FTP، ولكن ليس HTTP أو Telnet إلى الخارج. هذا يعني أنك تحتاج إلى إضافة *التفويض*. أي، تخويل *ما* يمكن للمستخدمين القيام به بالإضافة إلى المصادقة *من* هم. عند إضافة *التفويض* إلى PIX، يرسل PIX أولا اسم مستخدم وكلمة مرور تيري إلى خادم الأمان، ثم يرسل طلب تفويض يخبر خادم الأمان بما يحاول *تيري* القيام به *الأمر*". 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** - نافذة معروضة 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 UNIX TACACS الآمن من Cisco

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 UNIX RADIUS الآمن من Cisco

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

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

نظام التشغيل Windows 2.x RADIUS الآمن من Cisco

اتبع 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 **أمر 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 أو HTTP أو FTP).
7. قم بإضافة PIX IP في قسم تكوين NAS.

Cisco Secure 2.x TACACS+

يتلقى المستعمل كلمة في المستعمل setup gui قسم.

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 **أمر إضافة/تحرير جديد** لكل أمر تريد السماح به (على سبيل المثال، Telnet).
4. إذا كنت ترغب في السماح ب Telnet لمواقع معينة، فأدخل تصريح IP (عناوين) IP 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 السابقة لكل من الأوامر المسموح بها (على سبيل المثال، Telnet و/أو HTTP و/أو FTP).
7. قم بإضافة PIX IP في قسم تكوين NAS.

تكوين خادم Liingston RADIUS

إضافة 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

"key = "cisco

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

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

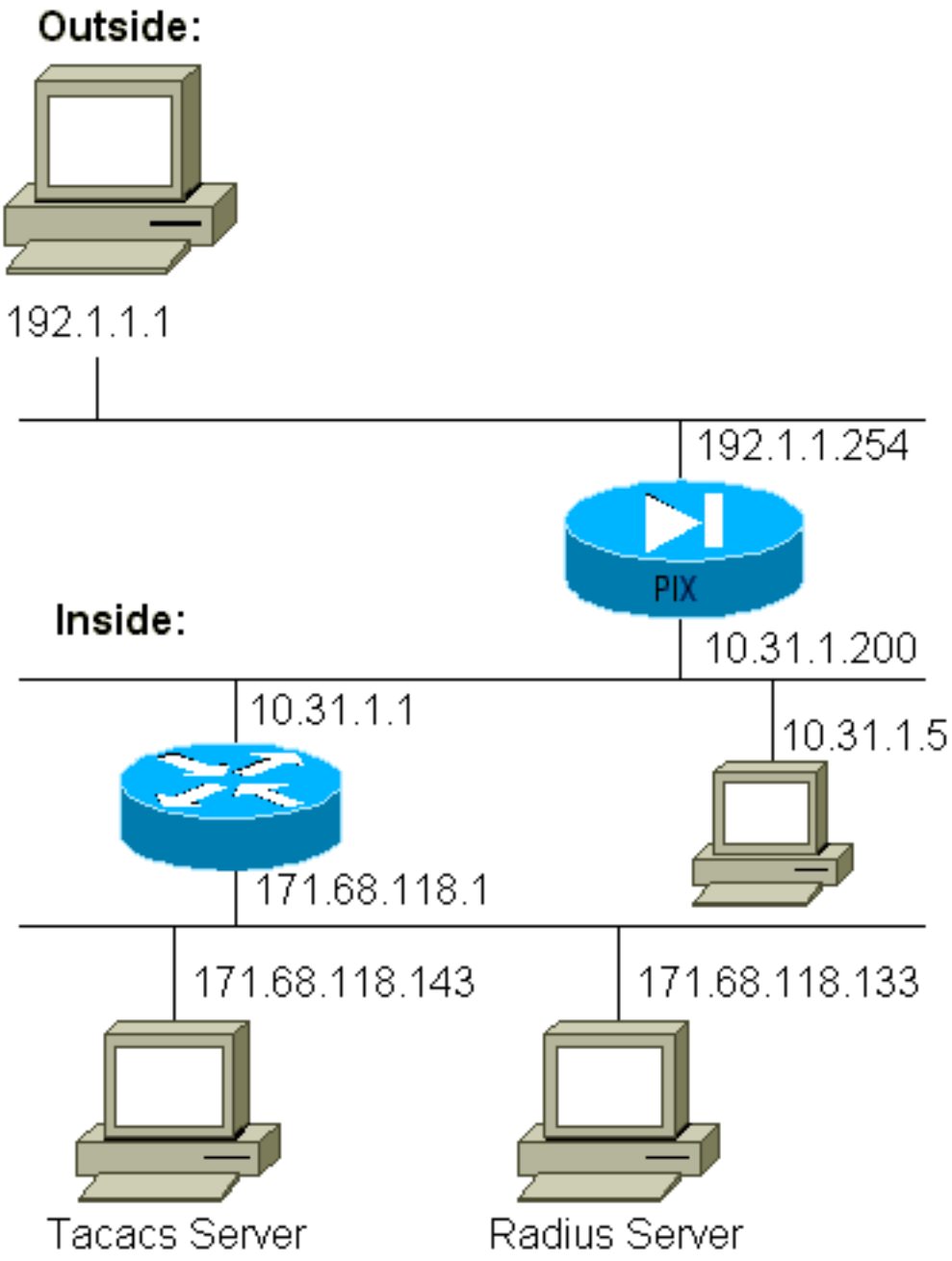
```
                                                } user = httponly
                                    "login = cleartext "httponly
                                                    } cmd = http
                                                       *. permit
                                   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

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

خطوات التصحيح

- تأكد من عمل تكوينات PIX قبل إضافة AAA.إذا تعذر عليك تمرير حركة المرور قبل إنشاء المصادقة والتفويض، فلن تتمكن من القيام بذلك بعد ذلك.
- تمكين تسجيل الدخول إلى PIXيجب *عدم* إستخدام أمر تصحيح أخطاء **وحدة تحكم التسجيل** على نظام محمل بشكل ثقيل.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
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
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
name 1.1.1.1 abcd
name 1.1.1.2 a123456789
name 1.1.1.3 a123456789123456
pager lines 24
logging timestamp
no logging standby
```

```
                                logging console debugging
                                       no logging monitor
                                logging buffered debugging
                                           no logging trap
                                      logging facility 20
                                        logging queue 512
                                 interface ethernet0 auto
                                 interface ethernet1 auto
                                         mtu outside 1500
                                          mtu inside 1500
          ip address outside 192.1.1.254 255.255.255.0
           ip address inside 10.31.1.200 255.255.255.0
                                               no failover
                                 failover timeout 0:00:00
                     failover ip address outside 0.0.0.0
                      failover ip address inside 0.0.0.0
                                       arp timeout 14400
       global (outside) 1 192.1.1.10-192.1.1.20 netmask
                                                255.255.255.0
     static (inside,outside) 192.1.1.25 171.68.118.143
                                 netmask 255.255.255.255 0 0
  static (inside,outside) 192.1.1.30 10.31.1.5 netmask
                                         255.255.255.255 0 0
                                 conduit permit tcp any any
                                conduit permit icmp any any
                                 conduit permit udp any any
                                     no rip outside passive
                                     no rip outside default
                                      no rip inside passive
                                      no rip inside default
    route inside 171.68.118.0 255.255.255.0 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
                  +aaa-server AuthInbound protocol tacacs
    aaa-server AuthInbound (inside) host 171.68.118.143
                                             cisco timeout 5
                  aaa-server AuthOutbound protocol radius
   aaa-server AuthOutbound (inside) host 171.68.118.133
                                             cisco timeout 5
     aaa authentication telnet outbound 0.0.0.0 0.0.0.0
                                 0.0.0.0 0.0.0.0 AuthOutbound
      aaa authentication telnet inbound 0.0.0.0 0.0.0.0
                                 0.0.0.0 0.0.0.0 AuthInbound
       aaa authentication http outbound 0.0.0.0 0.0.0.0
                                 0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication http inbound 0.0.0.0 0.0.0.0 0.0.0.0
                                          0.0.0.0 AuthInbound
aaa authentication ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0
                                         0.0.0.0 AuthOutbound
 aaa authentication ftp inbound 0.0.0.0 0.0.0.0 0.0.0.0
                                          0.0.0.0 AuthInbound
                                    no snmp-server location
                                     no snmp-server contact
                                snmp-server community public
                                 no snmp-server enable traps
                                           telnet timeout 5
                                       terminal width 80
        Cryptochecksum:fef4bfc9801d7692dce0cf227fe7859b
                                                    end :
```

أمثلة تصحيح أخطاء المصادقة من 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 192.1.1.1 ويتم مصادقته من خلال TACACS+. تستخدم حركة المرور الصادرة قائمة الخوادم "AuthOutbound" التي تتضمن خادم RADIUS 171.68.118.133.

داخل

يقوم المستخدم الخارجي في 192.1.1.1 ببدء حركة المرور إلى داخل 10.31.1.5 (192.1.1.30) وتتم مصادقته من خلال TACACS. تستخدم حركة المرور الواردة قائمة الخادم "AuthInbound" التي تتضمن خادم TACACS (171.68.118.143).

تصحيح أخطاء PIX - مصادقة جيدة - TACACS+

يوضح هذا المثال تصحيح أخطاء PIX بمصادقة جيدة:

```
pixfirewall# 109001: Auth start for user "???" from 192.1.1.1/13155
                                                    to 10.31.1.5/23
                        Authen Session Start: user 'pixuser', sid 6 :109011
Authentication succeeded for user 'pixuser' from 10.31.1.5/23 :109005
                                                  to 192.1.1.1/13155
 Authen Session End: user 'pixuser', Sid 6, elapsed 1 seconds :109012
    Built inbound TCP connection 6 for faddr 192.1.1.1/13155 :302001
                    (gaddr 192.1.1.30/23 laddr 10.31.1.5/23 (pixuser
```

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

يوضح هذا المثال تصحيح أخطاء PIX بمصادقة غير صحيحة (اسم المستخدم أو كلمة المرور). يرى المستخدم أربع مجموعات اسم مستخدم/كلمة مرور والرسالة : .

```
pixfirewall# 109001: Auth start for user '???' from 192.1.1.1/13157
                                                    to 10.31.1.5/23
      Authentication failed for user '' from 10.31.1.5/23 :109006
                                                  to 192.1.1.1/13157
```

تصحيح أخطاء PIX - خادم إختبار الاتصال Can Ping، دون إستجابة - TACACS+

يوضح هذا المثال تصحيح أخطاء PIX حيث يمكن تقسيم الخادم ولكنه لا يتحدث إلى PIX. يرى المستخدم اسم المستخدم مرة واحدة، ولكن PIX لا يطلب كلمة مرور (هذه على Telnet). يرى المستخدم : ".

```
                    Auth start for user '???' from 192.1.1.1/13159 to
                                                        10.31.1.5/23
 pixfirewall# 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13159
                              (failed (server 171.68.118.143 failed
      Auth from 10.31.1.5/23 to 192.1.1.1/13159 failed :109002
                                  (server 171.68.118.143 failed)
      Auth from 10.31.1.5/23 to 192.1.1.1/13159 failed :109002
                                  (server 171.68.118.143 failed)
```

```
Authentication failed for user '' from 10.31.1.5/23 :109006
                                                to 192.1.1.1/13159
```

تصحيح أخطاء PIX - يتعذر إختبار اتصال الخادم - TACACS+

يوضح هذا المثال تصحيح أخطاء PIX حيث يكون الخادم غير قابل للجلب. يرى المستخدم اسم المستخدم مرة واحدة، ولكن PIX لا يطلب كلمة مرور (هذه على Telnet). يتم عرض هذه الرسائل: TACACS+" و": " (تم تبديلها في خادم وهمي في التكوين).

```
Auth start for user '???' from 192.1.1.1/13158 :109001
                                                to 10.31.1.5/23
Auth from 10.31.1.5/23 to 192.1.1.1/13158 failed :109002
                                (server 171.68.118.143 failed)
Auth from 10.31.1.5/23 to 192.1.1.1/13158 failed :109002
                                (server 171.68.118.143 failed)
Auth from 10.31.1.5/23 to 192.1.1.1/13158 failed :109002
                                (server 171.68.118.143 failed)
Authentication failed for user '' from 10.31.1.5/23 :109006
                                                to 192.1.1.1/13158
```

تصحيح أخطاء PIX - مصادقة جيدة - RADIUS

يوضح هذا المثال تصحيح أخطاء PIX بمصادقة جيدة:

```
Auth start for user '???' from 10.31.1.5/11074 :109001
                                                to 192.1.1.1/23
  Authen Session Start: user 'pixuser', Sid 7 :109011
  'Authentication succeeded for user 'pixuser :109005
                    from 10.31.1.5/11074 to 192.1.1.1/23
   ,Authen Session End: user 'pixuser', Sid 7 :109012
                                      elapsed 1 seconds
Built outbound TCP connection 7 for faddr 192.1.1.1/23 :302001
     (gaddr 192.1.1.30/11074 laddr 10.31.1.5/11074 (pixuser
```

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

يوضح هذا المثال تصحيح أخطاء PIX بمصادقة غير صحيحة (اسم المستخدم أو كلمة المرور). يرى المستخدم طلبا لاسم المستخدم وكلمة المرور. للمستخدم ثلاث فرص لإدخال اسم المستخدم/كلمة المرور الناجح.

```
                                'Error: max number of tries exceeded' -
  pixfirewall# 109001: Auth start for user '???' from
                                   to 10.31.1.5/23 192.1.1.1/13157
Auth start for user '???' from 10.31.1.5/11075 :109001
                                                to 192.1.1.1/23
Auth from 10.31.1.5/11075 to 192.1.1.1/23 failed :109002
                                (server 171.68.118.133 failed)
Auth from 10.31.1.5/11075 to 192.1.1.1/23 failed :109002
                                (server 171.68.118.133 failed)
Auth from 10.31.1.5/11075 to 192.1.1.1/23 failed :109002
                                (server 171.68.118.133 failed)
Authentication failed for user '' from 10.31.1.5/11075 :109006
                                                to 192.1.1.1/23
```

تصحيح أخطاء إختبار الاتصال - يمكن إختبار اتصال الخادم، إيقاف البرنامج الخفي - RADIUS

يوضح هذا المثال تصحيح أخطاء PIX حيث يكون الخادم قابلا للانقسام، ولكن الأداة المساعدة متوقفة ولن تتصل ب PIX. يرى المستخدم اسم المستخدم وكلمة المرور والرسائل RADIUS" و": ".

```
'???' pixfirewall# 109001: Auth start for user
                     from 10.31.1.5/11076 to 192.1.1.1/23
Auth from 10.31.1.5/11076 to 192.1.1.1/23 failed :109002
                          (server 171.68.118.133 failed)
Auth from 10.31.1.5/11076 to 192.1.1.1/23 failed :109002
                          (server 171.68.118.133 failed)
Auth from 10.31.1.5/11076 to 192.1.1.1/23 failed :109002
                          (server 171.68.118.133 failed)
Authentication failed for user '' from 10.31.1.5/11076 :109006
                                                to 192.1.1.1/23
```

تصحيح أخطاء PIX - غير قادر على إختبار اتصال الخادم أو المفتاح/العميل غير المتطابق - RADIUS

في هذا المثال، يتم ضبط تصحيح أخطاء PIX حيث يكون الخادم غير قابل للجلب أو يوجد عدم تطابق في المفتاح/العميل. يرى المستخدم اسم المستخدم وكلمة المرور والرسائل RADIUS" و": " (تم تبديل خادم وهمي في التكوين).

```
Auth start for user '???' from 10.31.1.5/11077 :109001
                                                to 192.1.1.1/23
Auth from 10.31.1.5/11077 to 192.1.1.1/23 failed :109002
                          (server 100.100.100.100 failed)
Auth from 10.31.1.5/11077 to 192.1.1.1/23 failed :109002
                          (server 100.100.100.100 failed)
Auth from 10.31.1.5/11077 to 192.1.1.1/23 failed :109002
                          (server 100.100.100.100 failed)
Authentication failed for user '' from 10.31.1.5/11077 :109006
                                                to 192.1.1.1/23
```

إضافة تخويل

إذا قررت إضافة تخويل، فستحتاج إلى تخويل لنفس نطاق المصدر والوجهة (نظرا لأن التخويل غير صالح بدون مصادقة):

```
aaa authorization telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authorization HTTP inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authorization ftp inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

لاحظ أنه لا تتم إضافة التخويل ل "الصادر" لأنه تتم مصادقة حركة المرور الصادرة باستخدام RADIUS، وأن تخويل RADIUS غير صالح.

أمثلة تصحيح أخطاء المصادقة والتفويض من PIX

تصحيح أخطاء PIX - المصادقة الجيدة والتفويض الناجح - TACACS+

يوضح هذا المثال تصحيح أخطاء PIX بمصادقة جيدة وتفويض ناجح:

```
Authen Session Start: user 'pixuser', Sid 8 :109011
'Authorization permitted for user 'pixuser :109007
          from 192.1.1.1/13160 to 10.31.1.5/23
,Authen Session End: user 'pixuser', Sid 8 :109012
                                  elapsed 1 seconds
Built inbound TCP connection 8 for faddr 192.1.1.1/13160 :302001
        (gaddr 192.1.1.30/23 laddr 10.31.1.5/23 (pixuser
```

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

يوضح هذا المثال تصحيح أخطاء PIX بمصادقة جيدة ولكن بتخويل فاشل. هنا يرى المستخدم أيضا الرسالة : ".

```
Auth start for user '???' from 192.1.1.1/13162 :109001
                                    to 10.31.1.5/23
Authen Session Start: user 'userhttp', Sid 10 :109011
 'Authentication succeeded for user 'userhttp :109005
             from 10.31.1.5/23 to 192.1.1.1/13162
    'Authorization denied for user 'userhttp :109008
             from 10.31.1.5/23 to 192.1.1.1/13162
 ,Authen Session End: user 'userhttp', Sid 10 :109012
                                  elapsed 1 seconds
                        in use, 2 most used 0 :302010
```

إضافة محاسبة

TACACS+

```
aaa accounting any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

تصحيح الأخطاء نفس النظرة سواء كانت المحاسبة قيد التشغيل أو قيد الإيقاف. ومع ذلك، يتم إرسال سجل محاسبة "البدء" في وقت "الإنشاء". في وقت "التيردون"، يتم إرسال سجل محاسبة "إيقاف".

تبدو سجلات محاسبة TACACS+ مثل هذا الإخراج (هذا من Cisco Secure NT، وبالتالي التنسيق المحدد بفاصلة):

```
,pixuser,Default Group,192.1.1.1,04/26/2000,01:31:22
      ,start,,,,,,,0x2a,,PIX,10.31.1.200,telnet,6
,Login,1,,,1,,,,,,,,,,,local_ip=10.31.1.5 foreign_ip=192.1.1.1
                    ^,,,,,,,,zekie,,,,,,,,, ,,
,pixuser,Default Group,192.1.1.1,stop,4,04/26/2000,01:31:26
                  ,0x2a,,PIX,10.31.1.200,telnet,6,,,36,82,
,Login,1,,,1,,,,,,,,,,,local_ip=10.31.1.5 foreign_ip=192.1.1. 1
                    ,,,,,,,,zekie,,,,,,,,,,,
```

RADIUS

```
aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
```

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

تبدو سجلات محاسبة RADIUS بهذا الإخراج (وهذه من Cisco Secure UNIX؛ وقد تكون هناك سجلات في Cisco Secure NT مفصولة بفاصلة بدلا من ذلك):

```
radrecv: Request from host a1f01c8 code=4, id=18, length=65
                        Acct-Status-Type = Start
                         Client-Id = 10.31.1.200
                          Login-Host = 10.31.1.5
                             Login-TCP-Port = 23
```

```
"Acct-Session-Id = "0x0000002f
"User-Name = "pixuser
(Sending Accounting Ack of id 18 to a1f01c8 (10.31.1.200
radrecv: Request from host a1f01c8 code=4, id=19, length=83
Acct-Status-Type = Stop
Client-Id = 10.31.1.200
Login-Host = 10.31.1.5
Login-TCP-Port = 23
"Acct-Session-Id = "0x0000002f
"Username = "pixuser
Acct-Session-Time = 7
```

أمر إستخدام EXCEPT

في شبكتنا، إذا قررنا أن مصدر و/أو وجهة معينة لا تحتاج إلى مصادقة أو تفويض أو محاسبة، فيمكننا القيام بشيء مثل هذا الإخراج:

```
aaa authentication except inbound 192.1.1.1 255.255.255.255
AuthInbound 0.0.0.0 0.0.0.0
```

إذا كنت تقوم "باستثناء" مربع من المصادقة وكان لديك تخويل عليه، فيجب أيضا إستثناء المربع من التخويل.

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 (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 هذا المثال إخراج الإخراج، يتم إستخدام تكوين شبكة مختلف، ولكن المفاهيم هي نفسها.

برنامج Telnet للمستخدم 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 171.68.118.100/12 00 to 9.9.9.25/23
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
```

بما أن الخادم قد شاهد سجل "بدء" ولكن ليس سجل "إيقاف" (في هذه المرحلة من الوقت)، يظهر الخادم أن مستخدم "برنامج Telnet" قد قام بتسجيل 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)، يتم رفض الاتصال من قبل الخادم.

يستمر المستخدم في عمل Telnet أو FTP على المضيف الهدف، ثم يخرج (يقضي 10 دقائق هناك):

```
pix) 302002: Teardown TCP connection 5 faddr)
                                    gaddr 9.9.9.10/128 1 9.9.9.25/80
(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 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.

يعمل HTTP بشكل مختلف نظرا لطبيعة البروتوكول. يوضح هذا الإخراج مثالا 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 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
                                                (bytes 1907 (cse 0:00:00
                                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، فإن الحد الأقصى لجلسات العمل وعرض المستخدمين الذين تم تسجيل دخولهم لا يعملان بسبب طبيعة إتصالات HTTP.

المصادقة والتمكين على PIX نفسه

وصفت المناقشة السابقة مصادقة حركة مرور Telnet (و HTTP و FTP) *من خلال* PIX. نتأكد من أن Telnet *إلى* PIX يعمل *دون* مصادقة على:

```
telnet 10.31.1.5 255.255.255.255 passwd ww
```

```
aaa authentication telnet console AuthInbound
```

عندما يستعمل Telnet إلى ال PIX، هم حضضت ل ال telnet كلمة (**ww**). ثم يطلب PIX أيضا TACACS+ (في هذه الحالة، نظرا لاستخدام قائمة خادم "AuthInbound") أو اسم مستخدم وكلمة مرور RADIUS. إذا كان الخادم معطلا، فيمكنك الوصول إلى PIX عن طريق إدخال **PIX** لاسم المستخدم، ثم كلمة مرور **enable** (enable **password** مهما كان) للحصول على الوصول.

باستخدام هذا الأمر:

```
aaa authentication enable console AuthInbound
```

تتم مطالبة المستخدم باسم مستخدم وكلمة مرور، والتي يتم إرسالها إلى TACACS (في هذه الحالة، نظرا لاستخدام قائمة خادم "AuthInbound"، ينتقل الطلب إلى خادم TACACS) أو خادم RADIUS. بما أن حزمة المصادقة للتمكين هي نفسها حزمة المصادقة لتسجيل الدخول، إذا إستطاع المستخدم تسجيل الدخول إلى PIX باستخدام TACACS أو RADIUS، فيمكنه التمكين من خلال TACACS أو RADIUS باستخدام نفس اسم المستخدم/كلمة المرور. عينت هذا مشكلة cisco بق CSCdm47044 id (يسجل زبون فقط).

المصادقة على وحدة التحكم التسلسلية

يتطلب الأمر **AAA authentication serial console AuthInbound** التحقق من المصادقة للوصول إلى وحدة التحكم التسلسلية ل PIX.

عندما يقوم المستخدم بتنفيذ أوامر التكوين من وحدة التحكم، يتم قطع رسائل syslog (بافتراض تكوين PIX لإرسال syslog على مستوى تصحيح الأخطاء إلى مضيف syslog). هذا مثال من ما يعرض على ال syslog نادل:

```
logmsg: pri 245, flags 0, from [10.31.1.200.2.2], msg Nov 01 1999
.PIX-5-111008: User 'pixuser' executed the 'logging' command% :03:21:14
```

تغيير المطالبة التي يراها المستخدمون

إذا كان لديك الأمر **auth-prompt PIX_PIX_PIX**، فإن المستخدمين الذين يتنقلون عبر PIX يرون هذا التسلسل:

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

عند الوصول إلى مربع الوجهة النهائية، يتم عرض نافذة مطالبة "username:" و"password:". تؤثر هذه المطالبة فقط على المستخدمين الذين *يمرون* ب PIX، وليس *على* PIX.

ملاحظة: لا توجد سجلات محاسبة مقطوعة للوصول إلى PIX.

تخصيص الرسالة التي يراها مستخدمو الرسالة على النجاح/الفشل

إذا كانت لديك الأوامر:

```
"auth-prompt accept "GOOD_AUTH
"auth-prompt reject "BAD_AUTH
```

يرى المستخدمون هذا التسلسل عند تسجيل دخول فشل/ناجح من خلال PIX:

```
PIX_PIX_PIX
Username: asjdkl
:Password
"BAD_AUTH"
"PIX_PIX_PIX"
Username: cse
:Password
"GOOD_AUTH"
```

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 بحاجة إلى أجهزة مختلفة لكل مستخدم، فاستمر في القراءة.

في هذا المثال، يتم إستخدام الأمر **timeout** auth 3:00:00. بمجرد أن يقوم الشخص بالتصديق، لا يتعين عليه إعادة المصادقة لمدة ثلاث ساعات. ومع ذلك، إذا قمت بإعداد مستخدم باستخدام ملف التعريف هذا وكان لديك *تفويض* TACACS AAA قيد التشغيل في PIX، فإن حالات انتهاء المهلة الخاملة والمطلقة في ملف تعريف المستخدم تتجاوز المهلة الواردة في PIX لذلك المستخدم. لا يعني ذلك أن جلسة عمل Telnet من خلال PIX تم قطع إتصالها بعد المهلة الخاملة/المطلقة. إنها فقط تتحكم في ما إذا كانت تتم إعادة المصادقة.

يأتي ملف التعريف هذا من البرنامج المجاني TACACS+:

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

بعد المصادقة، قم بتنفيذ 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
```

يجب على المستخدم إعادة المصادقة عند إرجاعه إلى المضيف الهدف نفسه أو إلى مضيف مختلف.

HTTP الظاهري

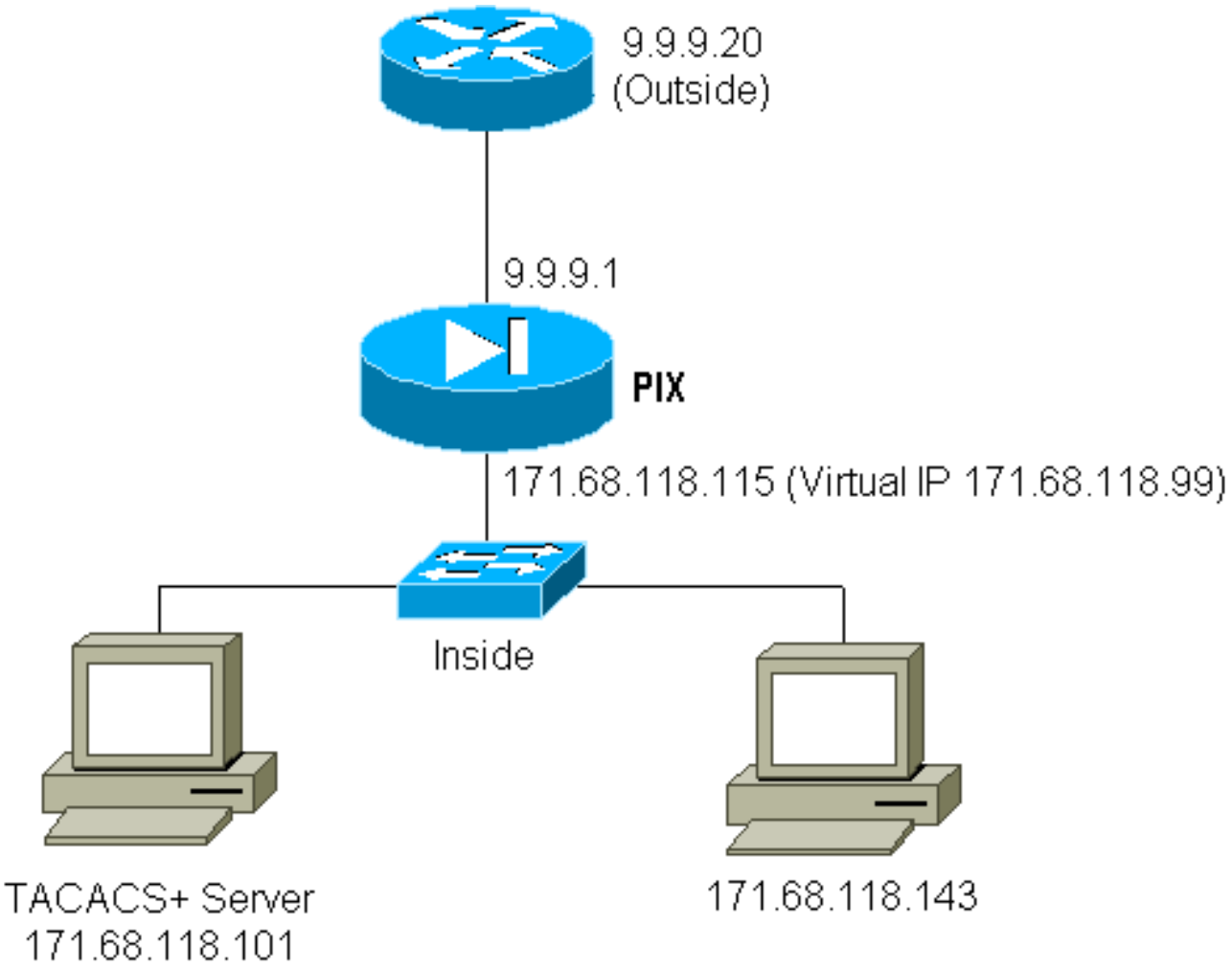
إذا كانت المصادقة مطلوبة على مواقع خارج PIX، وكذلك على PIX نفسه، فيمكن ملاحظة سلوك غير عادي للمستعرض في بعض الأحيان نظرا لأن المستعرضات تخزن اسم المستخدم وكلمة المرور مؤقتا.

لتجنب هذا، يمكنك تنفيذ HTTP ظاهري بإضافة عنوان RFC 1918 (عنوان غير قابل للتوجيه على الإنترنت، ولكنه صالح وفريد ل PIX داخل الشبكة) إلى تكوين PIX باستخدام هذا الأمر:

```
[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 يؤدي إلى منع إتصالات HTTP بخادم ويب الحقيقي.

الرسم التخطيطي الظاهري ل HTTP Outbound



خرج PIX Configuration Virtual HTTP

```
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 AuthOutbound protocol tacacs
aaa-server AuthOutbound (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 AuthOutbound
virtual http 171.68.118.99
```

```
auth-prompt THIS_IS_PIX_5
```

برنامج Telnet الظاهري

من الممكن تكوين PIX لمصادقة جميع حركة المرور الواردة والصادرة، ولكن ليس من الأفضل القيام بذلك. وذلك نظرا لأنه ليس من السهل مصادقة بعض البروتوكولات، مثل "mail". عندما يحاول خادم بريد وعميل الاتصال من خلال PIX عندما تتم مصادقة جميع حركات مرور البيانات عبر PIX، فإن PIX syslog للبروتوكولات غير القابلة للمصادقة تظهر رسائل مثل:

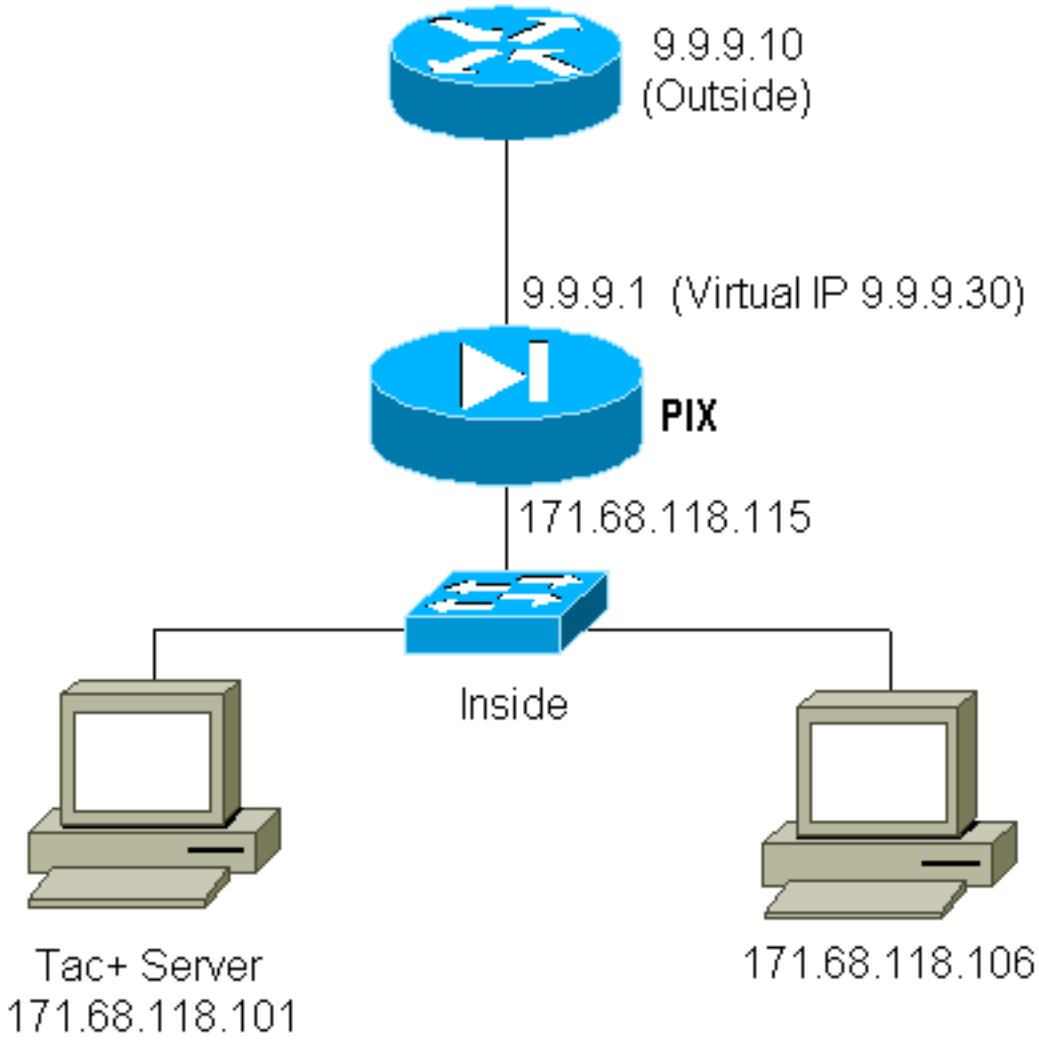
```
Auth start for user '???' from 9.9.9.10/11094 :109001
                                  to 171.68.118.106/25
Authorization denied from 171.68.118.106/49 to :109009
                        not authenticated) 9.9.9.10/11094
```

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).

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.

في هذا المثال، نريد تدفق حركة مرور منفذ TCP رقم 49 من المضيف الخارجي 9.9.9.10 إلى المضيف الداخلي 171.68.118.106. بما أن حركة المرور هذه ليست حقا قابلة للمصادقة، فقد قمنا بإعداد برنامج Telnet ظاهري. بالنسبة ل Telnet الظاهرية الواردة، يجب أن يكون هناك ثابت مقترن. هنا، كل من 9.9.9.20 و 171.68.118.20 هي عناوين افتراضية.

الرسم التخطيطي 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) 9.9.9.20 171.68.118.20 netmask 255.255.255.255 0 0
static (inside,outside) 9.9.9.30 171.68.118.106 netmask 255.255.255.255 0 0
conduit permit tcp host 9.9.9.20 eq telnet any
conduit permit tcp host 9.9.9.30 eq tacacs any
+aaa-server TACACS+ protocol tacacs
+aaa-server AuthInbound protocol tacacs
aaa-server AuthInbound (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 AuthInbound
virtual telnet 9.9.9.20
```

حزمة Telnet الظاهرية لتكوين مستخدم خادم TACACS+

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

الوارد لبرنامج Telnet الظاهري لتصحيح أخطاء PIX

يجب على المستخدم في 9.9.9.10 المصادقة أولا بواسطة Telnet على عنوان 9.9.9.20 على PIX:

```
pixfirewall# 109001: Auth start for user '???' from 9.9.9.10/11099
                                                to 171.68.118.20/23
                    Authen Session Start: user 'pinecone', Sid 13 :109011
                     'Authentication succeeded for user 'pinecone :109005
                               from 171.68.118.20/23 to 9.9.9.10/1470
```

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

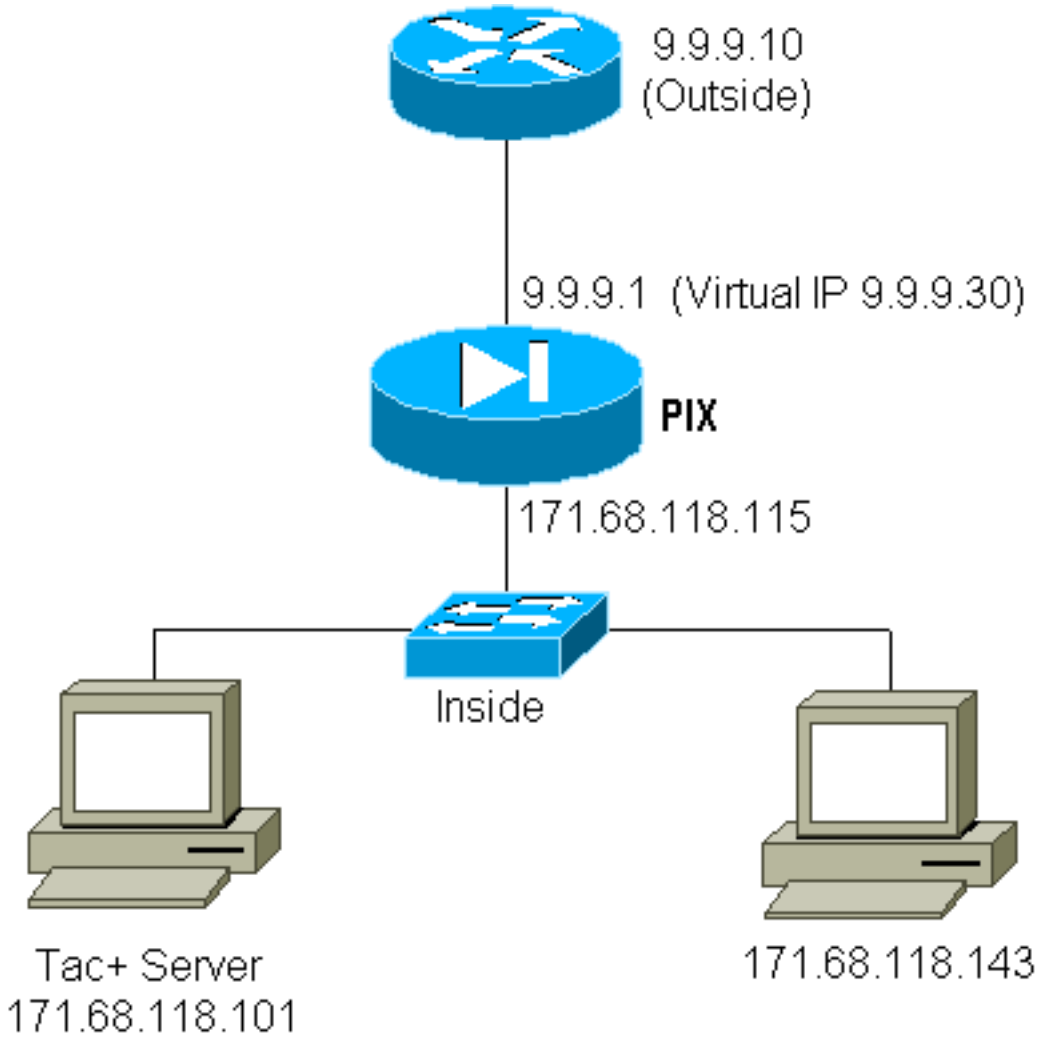
```
                                        pixfirewall# show uauth
                                Current    Most Seen
                                     Authenticated Users       1          1
                                     Authen In Progress        0          1
                           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

هنا، يريد الجهاز على 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 171.68.118.20/23
                    Authen Session Start: user 'pinecone', Sid 14 :109011
Authentication succeeded for user 'pinecone' from 171.68.118.20/23 :109005
                                                  to 9.9.9.10/1470
Built TCP connection 23 for faddr 9.9.9.10/11104 gaddr 9.9.9.30/49 :302001
                                        (laddr 171.68.118.106/49 (pinecone
 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 هذا المثال، المستخدم الداخلي في 171.68.118.143 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:



الصادر لتكوين PIX Virtual Telnet

```
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 AuthOutbound protocol tacacs
aaa-server AuthOutbound (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 AuthOutbound
virtual telnet 9.9.9.30
```

الصادر عن برنامج PIX Debug Virtual Telnet

```
Auth start for user '???' from 171.68.118.143/1536 :109001
to 9.9.9.30/23
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 :302001
(laddr 171.68 .118.143/1537 (timeout_143 9.9.9.30/1537
/: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 :302001
(laddr 171.68 .118.143/1538 (timeout_143 9.9.9.30/1538
Teardown TCP connection 46 faddr 9.9.9.10/80 gaddr :302002
laddr 171.68. 118.143/1537 duration 0:00:03 9.9.9.30/1537
```

```
(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 :302002
laddr 171.68. 118.143/1538 duration 0:00:01 9.9.9.30/1538
(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 المصادقة.

إذا أراد المستخدم منع حركة مرور البيانات من المرور بعد انتهاء جلسة العمل (عندما يكون هناك وقت متبقي في الوحدة)، فسيحتاج المستخدم إلى إرسال Telnet إلى برنامج Telnet الظاهري IP مرة أخرى. يتم الآن تبديل جلسة العمل.

تفويض المنفذ

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

تكوين PIX

```
AAA authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
AAA authorization tcp/23-49 outbound 0.0.0.0 0.0.0.0
AuthOutbound 0.0.0.0 0.0.0.0
```

عندما تم تنفيذ Telnet من 171.68.118.143 إلى 9.9.9.10، حدثت المصادقة والتفويض لأن منفذ Telnet 23 هو في النطاق 23-49.

عند إجراء جلسة HTTP من 171.68.118.143 إلى 9.9.9.10، ما يزال يتعين عليك 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+.

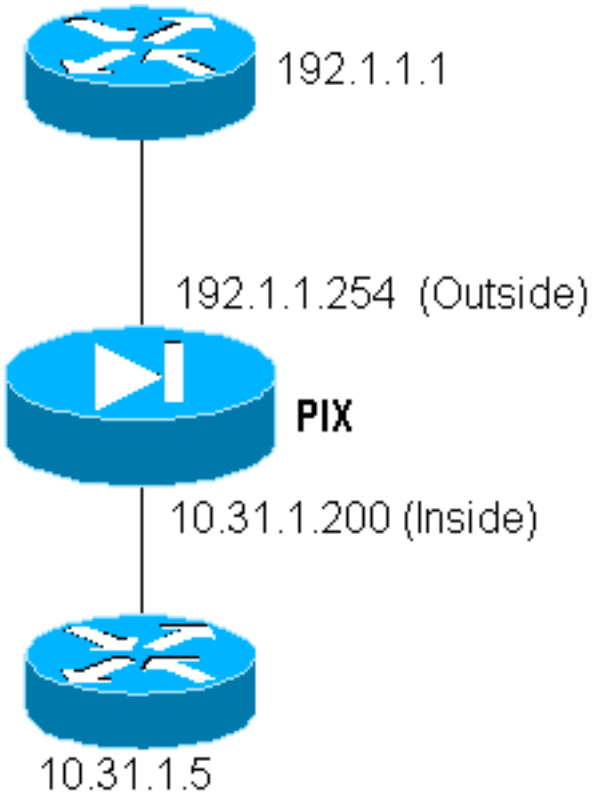
تصحيح الأخطاء على PIX

```
Auth start for user '???' from 171.68.118.143/1051 :109001
to 9.9.9.10/23
Authen Session Start: user 'telnetrange', Sid 0 :109011
'Authentication succeeded for user 'telnetrange :109005
from 171.68.118.143/1051 to 9. 9.9.10/23
Authen Session Start: user 'telnetrange', Sid 0 :109011
```

```
'Authorization permitted for user 'telnetrange :109007
                    from 171.68.118.143/1051 to 9.9 .9.10/23
          Built TCP connection 0 for faddr 9.9.9.10/23 :302001
(gaddr 9.9.9.5/1051 laddr 171.68.1 18.143/1051 (telnetrange
    Auth start for user '???' from 171.68.118.143/1105 :109001
                                                to 9.9.9.10/80
    Auth start for user '???' from 171.68.118.143/1110 :109001
                                                to 9.9.9.10/80
       Authen Session Start: user 'telnetrange', Sid 1 :109011
        'Authentication succeeded for user 'telnetrange :109005
                    from 171.68.118.143/1110 to 9. 9.9.10/80
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 :302002
 (laddr 171.68.11 8.143/1111 duration 0:00:01 bytes 2329 (telnetrange
```

محاسبة AAA لحركة المرور الأخرى من غير HTTP و FTP و Telnet

يغير الإصدار 5. 0 من برنامج PIX وظيفة محاسبة حركة المرور. يمكن قطع سجلات المحاسبة الآن لحركة المرور بخلاف HTTP و FTP و Telnet، بمجرد اكتمال المصادقة.



لنسخ ملف من الموجه الخارجي (192.1.1.1) إلى الموجه الداخلي (10.31.1.5)، أضف برنامج Telnet الظاهري لفتح فتحة لعملية TFTP:

```
virtual telnet 192.1.1.30
static (inside,outside) 192.1.1.30 10.31.1.5 netmask 255.255.255.255 0 0
conduit permit udp any any
AAA authentication udp/69 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

```
AAA authorization udp/69 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
AAA accounting udp/0 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

بعد ذلك، يعمل برنامج Telnet من الموجه الخارجي في 192.1.1.1 إلى 192.1.1.30 IP الافتراضي ويصادق على العنوان الظاهري الذي يسمح ل UDP باجتياز PIX. في هذا المثال، تم بدء عملية **copy tftp flash** من الخارج إلى الداخل:

```
Teardown UDP connection for faddr 192.1.1.1/7680 :302006
    gaddr 192.1.1.30/69 laddr 10.31.1.5/69
```

مقابل كل **نسخة tftp flash** على PIX (كانت هناك ثلاث مرات خلال نسخة IOS هذه)، يتم قص سجل محاسبة وإرساله إلى خادم المصادقة. فيما يلي مثال على سجل TACACS على Cisco Secure Windows):

```
,Date,Time,Username,Group-Name,Caller-Id,Acct-Flags,elapsed_time
,service,bytes_in,bytes_out,paks_in,paks_out
task_id,addr,NAS-Portname,NAS-IP-Address,cmd
,,,,,,,pixuser,Default Group,192.1.1.1,start,04/28/2000,03:08:26
0x3c,,PIX,10.31.1.200,udp/69
```

معلومات ذات صلة

- مرجع أوامر PIX
- صفحة دعم منتج PIX

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).