تكوين PIX 5.1.x: TACACS+ و RADIUS

المحتويات

المقدمة

قد تتم مصادقة RADIUS و TACACS+ لاتصالات FTP و Telnet و HTTP. يمكن عادة إجراء المصادقة للبروتوكولات الأخرى الأقل شيوعا لتعمل. تفويض TACACS+ مدعوم، أما تفويض RADIUS فهو غير مدعوم. تتضمن التغييرات في مصادقة PIX 5.1 والتفويض والمحاسبة (AAA) عبر الإصدار السابق المصادقة الموسعة (xauth)— مصادقة أنفاق IPSec من عميل Cisco Secure VPN Client 1.1.

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، راجع اصطلاحات تلميحات Cisco التقنية.

معلومات أساسية

المصادقة مقابل التخويل

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

افترض أن لديك 100 مستخدم بالداخل وتريد فقط أن يتمكن ستة من هؤلاء المستخدمين من تنفيذ FTP أو Telnet أو HTTP خارج الشبكة. يمكنك مطالبة PIX بمصادقة حركة المرور الصادرة ومنح معرفات المستخدمين الستة جميعها على خادم أمان TACACS+/RADIUS. وبمصادقة بسيطة، يمكن مصادقة هؤلاء المستخدمين الستة باسم المستخدم وكلمة المرور، ثم الخروج. أما المستخدمين الأربعة والتسعون الآخرون فلم يتمكنوا 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 الستة، "فستوس"، لا يجب الوثوق به. تريد السماح ل Festus بتنفيذ FTP، ولكن ليس HTTP أو Telnet إلى الخارج. وهذا يعني ضرورة إضافة *التفويض*، أي تفويض *ما* يمكن للمستخدمين القيام به بالإضافة إلى المصادقة على من هم. ولا يكون ذلك صحيحا إلا مع TACACS+. عند إضافة *التفويض* إلى PIX، يرسل PIX أولا اسم مستخدم وكلمة مرور Festus إلى خادم الأمان، ثم يرسل طلب تفويض يخبر خادم الأمان بما يحاول *Festus* القيام به *الأمر*. مع إعداد الخادم بشكل صحيح، يمكن السماح ل Festus بالوصول

إلى "FTP 1.2.3.4" ولكن سيتم 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 مطالبة باسم المستخدم تظهر، ثم طلبا بكلمة 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 المستعمل أن يدخل **local_username@remote_username** لاسم مستخدم و**local_password@remote_password** لكلمة. يرسل ال PIX ال local_username و local_password إلى المحلي أمن نادل، وإن كانت المصادقة (تفويض) ناجح في ال PIX/نادل، ال remote_username و remote_password يتم تمريرها إلى الغاية FTP نادل بعد ذلك.
- **HTTP** - يتم عرض نافذة في المستعرض تطلب 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 يكون في الوقت المحدد لاتصال HTTP ولكنه لا يفعل ذلك، فمن المحتمل أن تتم إعادة المصادقة في الواقع باستخدام المستعرض الذي يقوم بطرح اسم المستخدم وكلمة المرور المخزنة مؤقتا على PIX، والذي يقوم بعد ذلك بإعادة توجيهه إلى خادم المصادقة. يعرض PIX syslog و/أو تصحيح أخطاء الخادم هذه الظاهرة. إذا بدا أن Telnet و FTP يعملان بشكل طبيعي، ولكن إتصالات HTTP لا تعمل، فهذا هو السبب.
- **Tunnel** - عند محاولة إدخال حركة مرور IPSec إلى الشبكة باستخدام عميل VPN و xauth على، يتم عرض مربع رمادي ل "مصادقة المستخدم للاتصال الجديد" لاسم المستخدم/كلمة المرور.**ملاحظة:** يتم دعم هذه المصادقة بدءا من عميل Cisco Secure VPN Client 1.1. إذا كانت القائمة **تعليمات > حول** لا تظهر الإصدار x.2.1 أو الأحدث، فإن ذلك لا يعمل.

تكوينات خادم الأمان المستخدمة لجميع السيناريوهات

تكوين خادم UNIX TACACS الآمن من Cisco

في هذا القسم، تقدم لك معلومات تكوين خادم الأمان.

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 عنوان PIX IP والمفتاح إلى قائمة خادم الوصول إلى الشبكة (NAS).

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

مصدر المحتوى الإضافي الآمن من Cisco لنظام التشغيل Windows 2.x RADIUS

أستخدم هذه الخطوات لتكوين مصدر المحتوى الإضافي الآمن من Cisco ل Windows 2.x RADIUS.

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 **الإداري**.
3. قم بإضافة عنوان PIX IP في واجهة المستخدم الرسومية (GUI) لقسم تكوين 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، **برنامج Telnet**.
4. إذا تم السماح بالتوصيل إلى مواقع معينة، قم بتعبئة عنوان (عناوين) IP في قسم الوسيطة بالشكل "allowed #.#. #.^". وإلا، للسماح بالتعليق عن بعد، 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+

يحصل المستخدم على كلمة مرور في قسم إعداد المستخدم لواجهة المستخدم الرسومية.

1. في قسم المجموعة، انقر فوق **Shell EXEC** لمنح امتيازات EXEC.
2. لإضافة تفويض إلى PIX، في أسفل إعداد المجموعة، انقر فوق **رفض أوامر IOS غير المتطابقة**.
3. حدد **أمر إضافة/تحرير جديد** لكل أمر تريد السماح به (على سبيل المثال، **Telnet**).
4. للسماح بالتوصيل إلى مواقع معينة، أدخل عنوان IP في قسم الوسيطة في النموذج "السماح #.#. #.#". للسماح بالتعليق عن بعد لأي موقع، 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. تأكد من إضافة عنوان PIX IP في قسم واجهة المستخدم الرسومية (GUI) لتكوين 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

إضافة عنوان PIX IP والمفتاح إلى ملف العملاء.

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

تكوين خادم TACACS+ FreeWARE

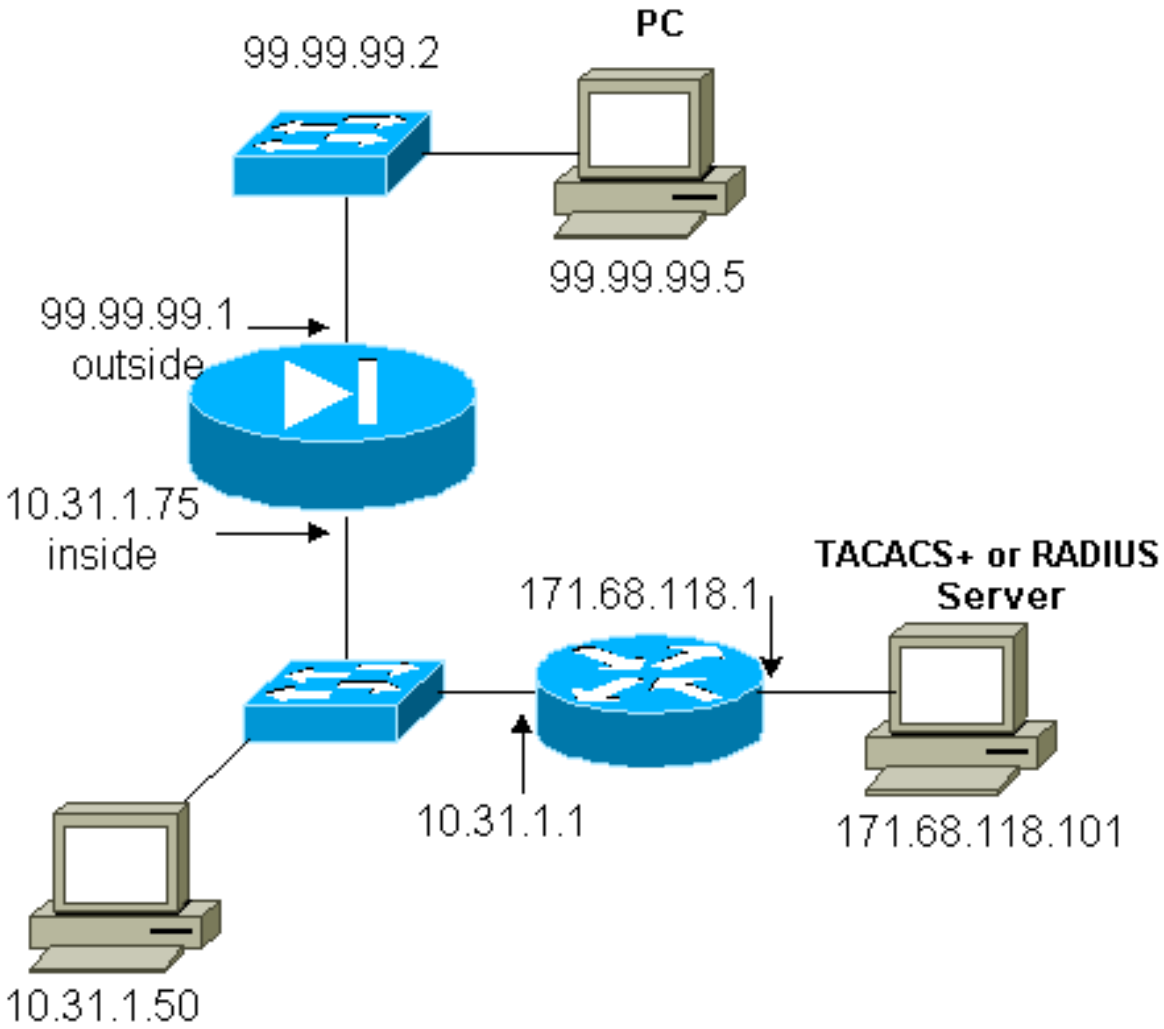
```
                                "key = "cisco
                             } user = adminuser
                          "login = cleartext "all
                        default service = permit
                                                {

                           } 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

ملاحظة: يتم دعم بعض أوامر **العرض** بواسطة أداة مترجم الإخراج (العملاء المسجلون فقط)، والتي تتيح لك عرض تحليل إخراج أمر **العرض**.

- تأكد من أن تكوين PIX يعمل قبل إضافة 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 تصحيح أخطاء وحدة التحكم في التسجيل على نظام محمل بشكل كبير.يمكن إستخدام تصحيح الأخطاء المخزن مؤقتا للتسجيل، ثم تنفيذ الأمر **show logging**.يمكن أيضا إرسال التسجيل إلى خادم syslog وفحصه هناك.
- قم بتشغيل تصحيح الأخطاء على خوادم TACACS+ أو RADIUS (تحتوي جميع الخوادم على هذا الخيار).

الرسم التخطيطي للشبكة



تكوين PIX
(PIX Version 5.1(1 nameif ethernet0 outside security0 nameif ethernet1 inside security100 nameif ethernet2 pix/intf2 security10 enable password 8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU encrypted hostname pix3 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
no logging standby
logging console debugging
no logging monitor
no logging buffered
no logging trap
no logging history
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
mtu outside 1500
mtu inside 1500
mtu pix/intf2 1500
ip address outside 99.99.99.1 255.255.255.0
ip address inside 10.31.1.75 255.255.255.0
ip address pix/intf2 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
arp timeout 14400
global (outside) 1 99.99.99.7-99.99.99.10 netmask
255.255.255.0
nat (inside) 1 10.31.1.0 255.255.255.0 0 0
static (inside,outside) 99.99.99.99 10.31.1.50 netmask
255.255.255.255 0 0
conduit permit icmp any any
conduit permit tcp any any
conduit permit udp any any
route outside 0.0.0.0 0.0.0.0 99.99.99.2 1
route inside 171.68.118.0 255.255.255.0 10.31.1.1 1
route inside 171.68.120.0 255.255.255.0 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 0:05:00 absolute
+aaa-server TACACS+ protocol tacacs
aaa-server RADIUS protocol radius
+aaa-server AuthInbound protocol tacacs
aaa-server AuthInbound (inside) host 171.68.118.101
cisco timeout 5
aaa-server AuthOutbound protocol radius
aaa-server AuthOutbound (inside) host 171.68.118.101
cisco timeout 5
aaa authentication include telnet outbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication include telnet inbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authentication include http outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication include http inbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthInbound
aaa authentication include ftp outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication include 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
floodguard enable
telnet timeout 5
terminal width 80
Cryptochecksum:b26b560b20e625c9e23743082484caca
end :
[OK]
```

أمثلة تصحيح أخطاء المصادقة من PIX

يعرض هذا القسم نماذج من تصحيح أخطاء المصادقة لسيناريوهات مختلفة.

داخل

يقوم المستخدم الخارجي في 99.99.99.2 ببدء حركة المرور إلى داخل 10.31.1.50 (99.99.99.99) وتتم مصادقته من خلال TACACS (أي، تستخدم حركة المرور الواردة قائمة الخادم "AuthInbound" والتي تتضمن خادم TACACS 171.68.118.101).

تصحيح أخطاء PIX - مصادقة جيدة - TACACS+

يوضح المثال التالي تصحيح أخطاء PIX بمصادقة جيدة:

```
Auth start for user '???' from :109001
to 10.31.1.50/23 99.99.99.2/11008
Authen Session Start: user 'cse', sid 4 :109011
'Authentication succeeded for user 'cse :109005
from 10.31.1.50/23 to 99.99.99.e
Built inbound TCP connection 10 for :302001
(.faddr 99.99.99.2/11008 gaddr 99.99
```

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 المستخدم ثلاث مجموعات اسم مستخدم/كلمة مرور، متبوعة بهذه الرسالة: : .

```
Auth start for user '???' from :109001
to 10.31.1.50/23 99.99.99.2/11010
Authentication failed for user '' from :109006
to 99.99.99.2/11010 on 10.31.1.50/23
interface outside
```

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

يوضح المثال التالي تصحيح أخطاء PIX حيث يكون الخادم قابلا للجمع، ولكن دون التحدث إلى PIX. يرى المستخدم اسم المستخدم مرة واحدة، ولكن PIX لا يطلب كلمة مرور (هذا على Telnet). يرى المستخدم : .

```
Auth start for user '???' from 99.99.99.2/11011 :109001
```

```
                                                    to 10.31.1.50/23
                Auth from 10.31.1.50/23 to 99.99.99.2/11011 failed :109002
                    server 171.68.118.101 failed) on interface outside)
                Auth from 10.31.1.50/23 to 99.99.99.2/11011 failed :109002
                    server 171.68.118.101 failed) on interface outside)
                Auth from 10.31.1.50/23 to 99.99.99.2/11011 failed :109002
                    server 171.68.118.101 failed) on interface outside)
            Authentication failed for user '' from 10.31.1.50/23 :109006
                                to 99.99.99.2/11011 on interface outside
```

تصحيح أخطاء PIX - يتعذر إختبار اتصال الخادم - TACACS+

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

```
                                   console end configuration: OK :111005
                                Auth start for user '???' from :109001
                                  to 10.31.1.50/23 99.99.99.2/11012
                           Auth from 10.31.1.50/23 to 99.99.99.2/11012 :109002
                        failed (server 1.1.1.1 failed) on interface outside
                           Auth from 10.31.1.50/23 to 99.99.99.2/11012 :109002
                        failed (server 1.1.1.1 failed) on interface outside
                           Auth from 10.31.1.50/23 to 99.99.99.2/11012 :109002
                        failed (server 1.1.1.1 failed) on interface outside
                                Authentication failed for user '' from :109006
                             to 99.99.99.2/11012 on interface 10.31.1.50/23
                                                                  outside
```

تصحيح أخطاء PIX - مصادقة جيدة - RADIUS

يوضح المثال التالي تصحيح أخطاء PIX بمصادقة جيدة:

```
                                Auth start for user '???' from :109001
                                  to 99.99.99.2/23 10.31.1.50/11008
                   Authen Session Start: user 'pixuser', sid 8 :109011
                                Authentication succeeded for user :109005
                                    pixuser' from 10.31.1.50/11008 to'
                                  on interface inside 99.99.99.2/23
                    Built outbound TCP connection 16 for faddr :302001
                                  gaddr 99.99.99.99/11008 99.99.99.2/23
                                       (laddr 10.31.1.50/11008 (pixuser
```

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 طلب اسم مستخدم وكلمة مرور، ولديه ثلاث فرص لإدخال هذين. عندما يكون الإدخال غير ناجح، يتم عرض الرسالة التالية: : .

```
            Auth start for user '???' from 10.31.1.50/11010 :109001
                                            to 99.99.99.2/23
                        '' Authentication failed for user :109006
                        from 10.31.1.50/11010 to 99.99.99.2/23
                                          on interface inside
```

تصحيح أخطاء PIX - يمكن إختبار اتصال الخادم مع الجهاز المساعد - RADIUS

يوضح المثال التالي تصحيح أخطاء PIX حيث يكون الخادم قابلا للانقسام، ولكن الأداة المساعدة متوقفة ولن تتصل ب PIX. يرى المستخدم اسم المستخدم، ثم كلمة المرور، RADIUS في الرسالة، : . رسالة الخطأ.

```
Auth start for user '???' from 10.31.1.50/11011 :109001
                                      to 99.99.99.2/23
ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
1ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
   Auth from 10.31.1.50/11011 to 99.99.99.2/23 :09002
failed (server 171.68.118.101 failed) on interface inside
Auth from 10.31.1.50/11011 to 99.99.99.2/23 failed :109002
     server 171.68.118.101 failed) on interface inside)
Auth from 10.31.1.50/11011 to 99.99.99.2/23 failed :109002
     server 171.68.118.101 failed) on interface inside)
Authentication failed for user '' from 10.31.1.50/11011 :109006
                          to 99.99.99.2/23 on interface inside
```

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

يوضح المثال التالي تصحيح أخطاء PIX حيث يكون الخادم غير قابل للجلب أو يوجد عدم تطابق في العميل/المفتاح. يرى المستخدم اسم مستخدم وكلمة مرور ورسالة RADIUS و: رسالة تم تبديل خادم وهمي في التكوين).

```
Auth start for user '???' from 10.31.1.50/11012 :109001
                                      to 99.99.99.2/23
Auth from 10.31.1.50/11012 to 99.99.99.2/23 failed :109002
          server 1.1.1.1 failed) on interface inside)
Auth from 10.31.1.50/11012 to 99.99.99.2/23 failed :109002
          server 1.1.1.1 failed) on interface inside)
Auth from 10.31.1.50/11012 to 99.99.99.2/23 failed :109002
          server 1.1.1.1 failed) on interface inside)
Authentication failed for user '' from 10.31.1.50/11012 :109006
                          to 99.99.99.2/23 on interface inside
```

إضافة التخويل

إذا قررت إضافة التفويض، نظرا لأن التخويل غير صالح بدون مصادقة، فأنت بحاجة إلى طلب تخويل لنفس نطاق المصدر والوجهة.

```
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 أنك لا تضيف تخويل للصادر لأن حركة المرور الصادرة تتم مصادقتها مع RADIUS، وتخويل RADIUS غير صالح.

أمثلة تصحيح أخطاء المصادقة والتفويض من PIX

تصحيح أخطاء PIX - المصادقة الجيدة والتفويض الناجح - TACACS+

يوضح المثال التالي تصحيح أخطاء PIX بمصادقة جيدة وتفويض ناجح:

```
Auth start for user '???' from 99.99.99.2/11016 :109001
                                        to 10.31.1.50/23
        Authen Session Start: user 'cse', Sid 11 :109011
         'Authentication succeeded for user 'cse :109005
from 10.31.1.50/23 to 99.99.99.2/11016 on interface outside
        Authen Session Start: user 'cse', Sid 11 :109011
      Authorization permitted for user 'cse' from :109007
to 10.31.1.50/23 on interface outside 99.99.99.2/11016
Built inbound TCP connection 19 for faddr 99.99.99.2/11016 :302001
          (gaddr 99.99.99.99/23 laddr 10.31.1.50/23 (cse
```

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

يوضح المثال التالي تصحيح أخطاء PIX بمصادقة جيدة ولكن فشل التفويض. هنا يرى المستخدم أيضا الرسالة : .

```
Auth start for user '???' from :109001
  to 10.31.1.50/23 99.99.99.2/11017
,'Authen Session Start: user 'httponly :109011
                                    Sid 12
'Authentication succeeded for user 'httponly :109005
  from 10.31.1.50/23 to 99.99.99.2/11017 on
                              interface outside
Authorization denied for user 'httponly' from :109008
to 99.99.99.2/11017 on interface outside 10.31.1.50/23
```

إضافة محاسبة

TACACS+

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

إخراج البرنامج المجاني TACACS+:

```
Tue Feb 22 08:52:20 2000  10.31.1.75 cse PIX
        start task_id=0x14 99.99.99.2
foreign_ip=99.99.99.2 local_ip=10.31.1.50
                              cmd=telnet
Tue Feb 22 08:52:25 2000  10.31.1.75 cse PIX
         stop task_id=0x14 99.99.99.2
foreign_ip=99.99.99.2 local_ip=10.31.1.50
           cmd=telnet elapsed_time=5
           bytes_in=39 bytes_out=126
```

RADIUS

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

خرج Merit RADIUS:

```
Tue Feb 22 08:56:17 2000
```

```
        Acct-Status-Type = Start
    NAS-IP-Address = 10.31.1.75
     Login-IP-Host = 10.31.1.50
            Login-TCP-Port = 23
Acct-Session-Id = 0x00000015
            User-Name = pixuser

   Tue Feb 22 08:56:24 2000
        Acct-Status-Type = Stop
    NAS-IP-Address = 10.31.1.75
     Login-IP-Host = 10.31.1.50
            Login-TCP-Port = 23
Acct-Session-Id = 0x00000015
             Username = pixuser
      Acct-Session-Time = 6
    Acct-Input-Octets = 139
    Acct-Output-Octets = 36
```

أمر إستخدام الاستبعاد

إذا أضفنا مضيف آخر خارج (في 99.99.99.100) إلى شبكتنا، وكان هذا المضيف موثوقا به، فيمكنك إستبعادهم من المصادقة والتخويل باستخدام الأوامر التالية:

```
aaa authentication exclude telnet inbound 0.0.0.0 0.0.0.0 99.99.99.100
AuthInbound 255.255.255.255

aaa authorization exclude telnet inbound 0.0.0.0 0.0.0.0 99.99.99.100 255.255.255.255
AuthInbound
```

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 المستخدم 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.

Telnet للمستخدم من خلال PIX، للمصادقة على الطريقة:

```
    to 9.9.9.25 /23 171.68.118.100/1200
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)
        gaddr 9.9.9.10/12 00 9.9.9.25/23
        (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 بدء ولكن ليس سجل توقف، 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 (بافتراض أن الخادم يدعم الحد الأقصى لجلسات العمل)، يتم رفض الاتصال من قبل الخادم.

يقوم المستخدم بتنفيذ عمله في برنامج Telnet أو FTP على المضيف الهدف، ثم يخرج (يقضي عشر دقائق هناك):

```
pix) 302002: Teardown TCP connection 5 faddr
                gaddr 9.9.9.10/128 9.9.9.25/80
laddr 171.68.118.100/1281 duration 0:00:00 1
                        (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 (أي المصادقة في كل مرة) أو أكثر (المصادقة مرة واحدة وليس مرة أخرى خلال فترة المصادقة)، يتم قطع سجل محاسبة لكل موقع يتم الوصول إليه.

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)
            to 9.9.9.25 /80 171.68.118.100/1281
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)
        gaddr 9.9.9.10/12 81 laddr 9.9.9.25/80
                    (cse) 171.68.118.100/1281
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)
                gaddr 9.9.9.10/128 9.9.9.25/80
laddr 171.68.118.100/1281 duration 0:00:00 1
                        (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 الويب التي تم تنزيلها.

يتم نشر سجل البداية في 16:35:34 وسجل التوقف 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 يقوم المستخدم بقراءة 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 والتوقف هو ثانية فرعية. لا يوجد سجل بدء بدون سجل توقف لأن السجلات تحدث في نفس اللحظة تقريبا. سيظل هناك سجل بدء وإيقاف مرسلة 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

وتتعلق المناقشة السابقة بمصادقة حركة مرور Telnet (و HTTP و FTP) من خلال PIX. ضمان عمل برنامج Telnet إلى PIX دون مصادقة على:

```
telnet 10.31.1.5 255.255.255.255
passwd ww
```

ثم قم بإضافة الأمر لمصادقة المستخدمين الذين يتصلون ب Telnet إلى PIX:

```
aaa authentication telnet console AuthInbound
```

عندما يستعمل Telnet إلى ال PIX، هم حضضت ل ال telnet كلمة (**WW**). كما يطلب PIX اسم مستخدم وكلمة مرور TACACS+ أو RADIUS. في هذه الحالة، حيث أنه يتم إستخدام قائمة خادم AuthInbound، يطلب PIX اسم مستخدم وكلمة مرور TACACS+.

إذا كان الخادم معطلا، فيمكنك الوصول إلى PIX عن طريق إدخال **PIX** لاسم المستخدم، ثم كلمة مرور enable (**enable password**) أيا كان). باستخدام الأمر:

```
aaa authentication enable console AuthInbound
```

تتم مطالبة المستخدم باسم مستخدم وكلمة مرور يتم إرسالها إلى خادم TACACS أو RADIUS. في هذه الحالة، حيث أنه يتم إستخدام قائمة خادم AuthInbound، يطلب PIX اسم مستخدم وكلمة مرور TACACS+.

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. تم تعيين هذه المشكلة لمعرف تصحيح الأخطاء من Cisco CSCdm47044 (العملاء المسجلون فقط).

إذا كان الخادم معطلا، فيمكنك الوصول إلى وضع تمكين PIX عن طريق إدخال **PIX** لاسم المستخدم وكلمة مرور التمكين العادية من PIX (**تمكين كلمة المرور** أيا كان). إن **يمكن كلمة** أي كان ليس في ال PIX تشكيل، دخلت PIX ل ال username واضغط **يدخل**. في حالة تعيين كلمة مرور enable ولكن غير معروفة، يلزم إنشاء قرص إسترداد كلمة المرور لإعادة ضبط كلمة المرور.

تغيير رسالة مطالبة المستخدمين

إذا كان لديك الأمر:

```
auth-prompt PIX_PIX_PIX
```

يرى المستخدمون الذين يمرون ب PIX التسلسل التالي:

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

عند الوصول إلى الوجهة النهائية، سيرى المستخدمون اسم المستخدم: وكلمة المرور: مطالبة معروضة بواسطة مربع الوجهة. يؤثر هذا موجه الأمر 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 لديك الأوامر:

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

ثم سيرى المستخدمون التسلسل التالي عند تسجيل دخول فاشل/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

لا تعمل هذه الوظيفة حاليا وقد تم تعيين المشكلة إلى معرف تصحيح الأخطاء من CSCdp93492 Cisco (العملاء المسجلون فقط).

HTTP الظاهري

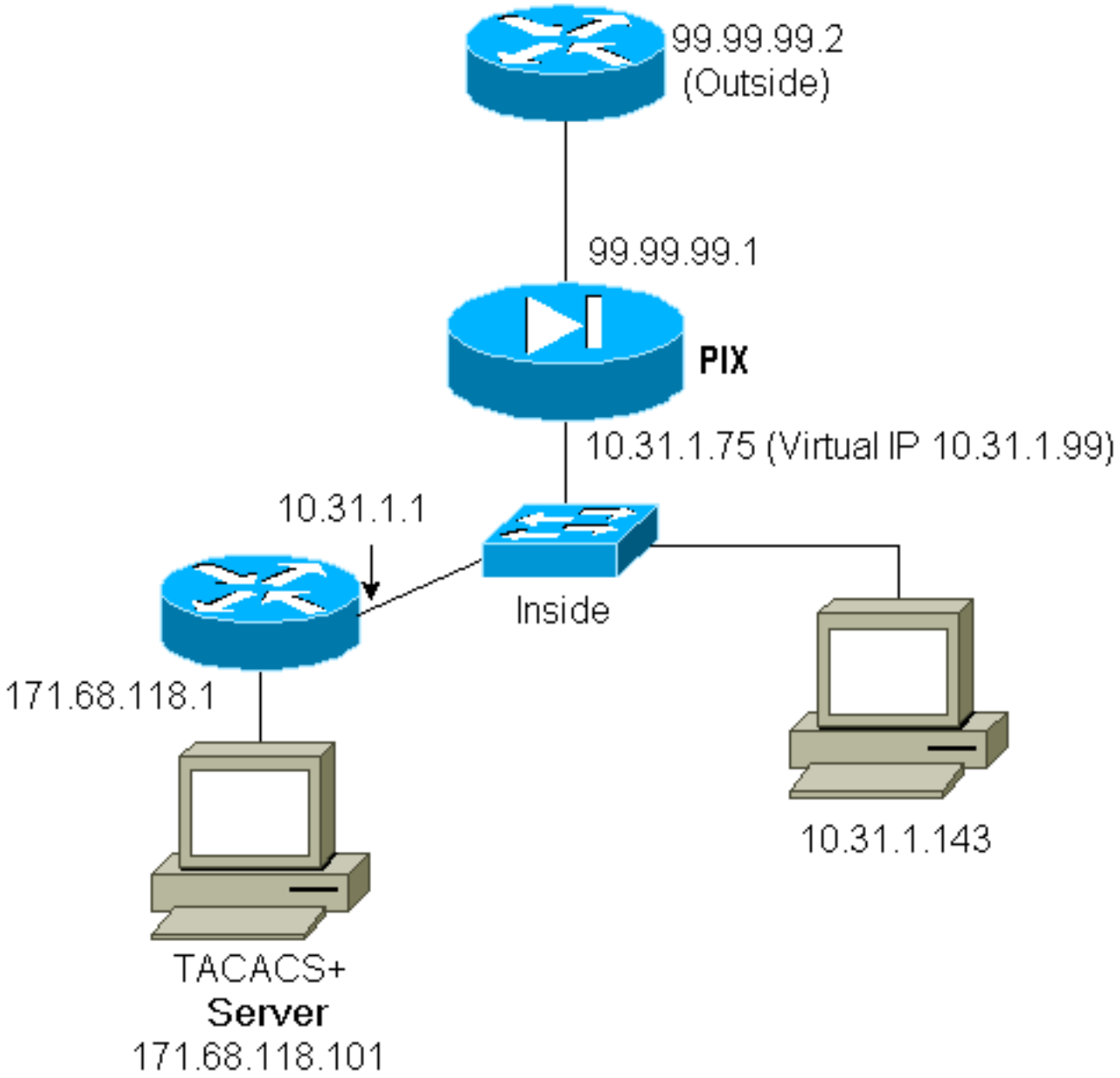
إذا كانت المصادقة مطلوبة على مواقع خارج PIX وكذلك على PIX نفسه، فيمكن ملاحظة سلوك غير عادي للمستعرض في بعض الأحيان، نظرا لأن المستعرضات تخزن اسم المستخدم وكلمة المرور مؤقتا.

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 99.99.99.1 255.255.255.0
ip address inside 10.31.1.75 255.255.255.0
global (outside) 1 99.99.99.7-99.99.99.10 netmask 255.255.255.0
timeout uauth 01:00:00
aaa authentication include http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
aaa-server RADIUS protocol radius
aaa-server AuthOutbound protocol radius
aaa-server AuthOutbound (inside) host 171.68.118.101 cisco timeout 5
virtual http 10.31.1.99
```

برنامج Telnet الظاهري

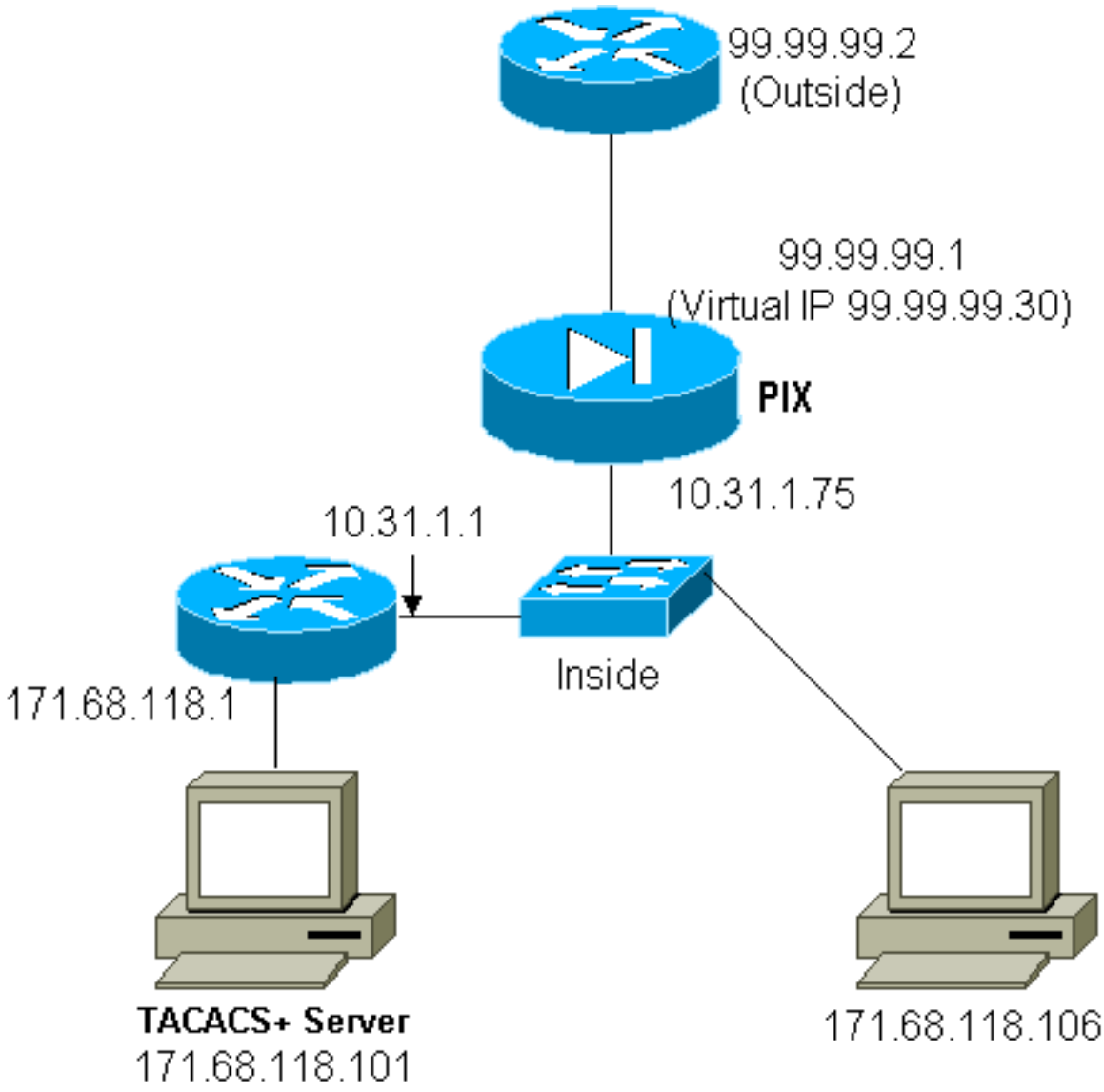
من الممكن تكوين PIX لمصادقة جميع البروتوكولات الواردة والصادرة، ولكنها ليست فكرة جيدة نظرا لأنه لا يمكن مصادقة بعض البروتوكولات، مثل البريد، بسهولة. عندما يحاول خادم بريد وعميل الاتصال من خلال PIX عندما تتم مصادقة جميع حركات مرور البيانات عبر PIX، فإن PIX syslog للبروتوكولات غير القابلة للمصادقة يظهر رسائل مثل:

```
User must authenticate before using :109013
                                        this service
Authorization denied from 171.68.118.106/49 :109009
                (to 9.9.9.10/11094    (not authenticated
```

ومع ذلك، إذا كانت هناك حاجة حقيقية إلى مصادقة نوع ما من الخدمات غير العادية، يمكن القيام بذلك باستخدام الأمر **virtual telnet**. يسمح هذا أمر أن تحدث المصادقة إلى عنوان Telnet IP الظاهري. بعد هذه المصادقة، يمكن لحركة مرور الخدمة غير العادية الانتقال إلى الخادم الحقيقي.

في هذا المثال، تريد حركة مرور منفذ TCP رقم 49 أن تتدفق من المضيف الخارجي 99.99.99.2 إلى المضيف الداخلي 171.68.118.106. بما أن حركة المرور هذه ليست حقا قابلة للمصادقة، قم بإعداد برنامج Telnet ظاهري. بالنسبة لبرنامج Telnet الظاهري، يجب أن يكون هناك ثابت مرتبط. هنا، كل من 99.99.99.20 و 171.68.118.20 هي عناوين افتراضية.

الوارد لبرنامج Telnet الظاهري



PIX Configuration Virtual Telnet Inbound

```
ip address outside 99.99.99.1 255.255.255.0
ip address inside 10.31.1.75 255.255.255.0
```

```
static (inside,outside) 99.99.99.20 171.68.118.20 netmask 255.255.255.255 0 0
static (inside,outside) 99.99.99.30 171.68.118.106 netmask 255.255.255.255 0 0
conduit permit tcp host 99.99.99.20 eq telnet any
conduit permit tcp host 99.99.99.30 eq tacacs any
+aaa-server TACACS+ protocol tacacs
+aaa-server Incoming protocol tacacs
aaa-server Incoming (inside) host 171.68.118.101 cisco timeout 5
aaa authentication include telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
Incoming
aaa authentication include tcp/49 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
Incoming
virtual telnet 99.99.99.20
```

الوارد لبرنامج Telnet الظاهري لتصحيح أخطاء PIX

يجب على المستخدم في 99.99.99.2 المصادقة أولا بواسطة Telnet على عنوان 99.99.99.20 على PIX:

```
Auth start for user '???' from :109001
to 171.68.118.20/23 99.99.99.2/22530
Authen Session Start: user 'cse', Sid 13 :109011
Authentication succeeded for user :109005
cse' from 171.68.118.20/23 to'
on interface outside 99.99.99.2/22530
```

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

```
pixfirewall# show uauth
Current    Most Seen
Authenticated Users       1          2
Authen In Progress        0          1
user 'cse' at 99.99.99.2, authenticated
absolute   timeout: 0:05:00
inactivity timeout: 0:00:00
```

وعندما يريد الجهاز على 99.99.99.2 إرسال حركة مرور TCP/49 إلى الجهاز على 171.68.118.106:

```
Built inbound TCP connection 16 :302001
for faddr 99.99.99.2/11054 gaddr
(laddr 171.68.118.106/49 (cse 99.99.99.30/49
```

يمكن إضافة التفويض:

```
aaa authorization include tcp/49 inbound
AuthInbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
```

بحيث أنه عندما يتم محاولة حركة مرور TCP/49 من خلال PIX، يرسل PIX أيضا استعلام التفويض إلى الخادم:

```
'Authorization permitted for user 'cse :109007
from 99.99.99.2/11057 to 171.68.118.106/49
on interface outside
```

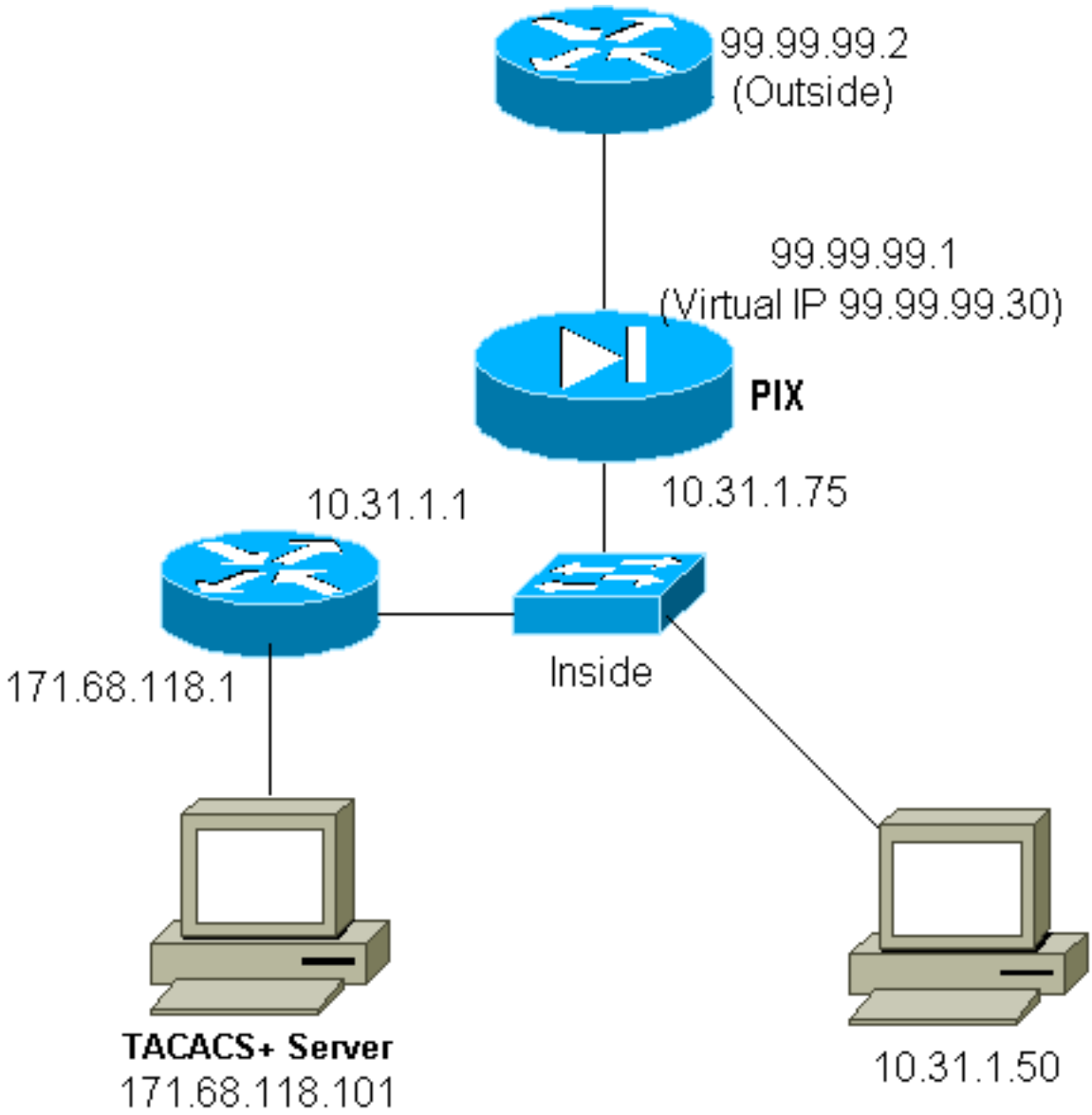
على خادم TACACS+، يظهر هذا على أنه:

```
,service=shell
,cmd=tcp/49
```

```
cmd-arg=171.68.118.106
```

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، المستخدم الداخلي في 10.31.1.50 من Telnet إلى الإصدار 99.99.99.30 الظاهري والمصادقة، يتم إسقاط اتصال Telnet على الفور. بمجرد المصادقة، يتم السماح بحركة مرور TCP من 10.31.1.50 إلى الخادم على 99.99.99.2:



خرج Telnet الظاهري لتكوين PIX:

```
ip address outside 99.99.99.1 255.255.255.0
ip address inside 10.31.1.75 255.255.255.0
global (outside) 1 99.99.99.7-99.99.99.10 netmask 255.255.255.0
timeout uauth 0:05:00 absolute
aaa-server RADIUS protocol radius
aaa-server AuthOutbound protocol radius
aaa-server AuthOutbound (inside) host 171.68.118.101 cisco timeout 5
aaa authentication include telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication include tcp/49 outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
virtual telnet 99.99.99.30
```

ملاحظة: لا يوجد تفويض نظرا لأن هذا RADIUS.

الصادر عن برنامج PIX Debug Virtual Telnet:

```
Auth start for user '???' from 10.31.1.50/11034 :109001
                                    to 99.99.99.30/23
  Authen Session Start: user 'pixuser', Sid 16 :109011
   'Authentication succeeded for user 'pixuser :109005
from 10.31.1.50/11034 to 99.99.99.30/23 on interface
                                          inside
    Built outbound TCP connection 18 for faddr :302001
         gaddr 99.99.99.8/11036 laddr 99.99.99.2/49
                        (pixuser) 10.31.1.50/11036
Teardown TCP connection 18 faddr 99.99.99.2/49 :302002
      gaddr 99.99.99.8/11036 laddr 10.31.1.50/11036
                (duration 0:00:02 bytes 0 (pixuser
```

تسجيل الخروج من برنامج Telnet الظاهري

عندما يعرض المستخدمون Telnet إلى عنوان Telnet IP الظاهري، فإن الأمر **show uauth** يعرض مستواهم. إذا كان المستخدمون يرغبون في منع حركة المرور من المرور بعد انتهاء جلسات عملهم عندما يكون هناك وقت متبقي في الوحدة، فإنهم يحتاجون إلى برنامج Telnet إلى عنوان IP الظاهري مرة أخرى. يتم الآن تبديل جلسة العمل.

بعد المصادقة الأولى:

```
                                    pix3# show uauth
        Current    Most Seen
              Authenticated Users       1          2
              Authen In Progress        0          1
         user 'pixuser' at 10.31.1.50, authenticated
                        absolute   timeout: 0:05:00
                        inactivity timeout: 0:00:00
   pix3# 109001: Auth start for user 'pixuser' from
                    to 99.99.99.30/23 10.31.1.50/11038
 'Authentication succeeded for user 'pixuser :109005
      from 10.31.1.50/11038 to 99.99.99.30/23 on
                                interface inside
```

بعد المصادقة الثانية (أي يتم تغيير الثقب ليتم إغلاقه):

```
                                    pix3# show uauth
        Current    Most Seen
              Authenticated Users       0          2
              Authen In Progress        0          1
```

تفويض المنفذ

يسمح بالتفويض لنطاقات المنافذ (مثل TCP/30-100). إذا تم تكوين برنامج Telnet الظاهري على برنامج PIX والتخويل لمجموعة من المنافذ، بمجرد فتح الثقب باستخدام برنامج Telnet الظاهري، يصدر برنامج PIX الأمر **tcp/30-100** إلى خادم TACACS+ للتخويل:

```
static (inside,outside) 99.99.99.75 10.31.1.50 netmask 255.255.255.255 0 0
conduit permit tcp host 99.99.99.75 host 99.99.99.2
static (inside,outside) 99.99.99.75 10.31.1.50 netmask 255.255.255.255 0 0
virtual telnet 99.99.99.75
aaa authentication include any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authorization include tcp/30-100 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
virtual telnet 99.99.99.30
```

تكوين خادم TACACS+ FreeWare:

```
} user = anyone
"login = cleartext "anyone
} cmd = tcp/30-100
permit 10.31.1.50
{
{
```

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

بعد التأكد من أن برنامج Telnet الظاهري يعمل للسماح لحركة مرور TCP/49 إلى المضيف داخل الشبكة، قررنا أننا نريد معرفة سبب ذلك، لذا قمنا بإضافة ما يلي:

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

ينتج عن ذلك خفض سجل محاسبة عند مرور حركة مرور TCP/49 (هذا المثال من البرامج المجانية TACACS+):

```
Sun Feb 27 05:24:44 2000 10.31.1.75 cse PIX
start task_id=0x14 foreign_ip=99.99.99.2 local_ip=171.68.118.106 99.99.99.2
cmd=tcp/49
```

المصادقة الموسعة (Xauth)

نموذج للتكوينات

- إنهاء أنفاق IPSec على الواجهات المتعددة لجدار حماية PIX الآمن من Cisco باستخدام Xauth
- IPSec بين جدار حماية PIX الآمن من Cisco وعميل VPN مع مصادقة موسعة

المصادقة على DMZ

لمصادقة المستخدمين المتنقلين من واجهة DMZ إلى أخرى، اطلب من PIX مصادقة حركة مرور البيانات للواجهات المسماة. على ال PIX لدينا الترتيب هو:

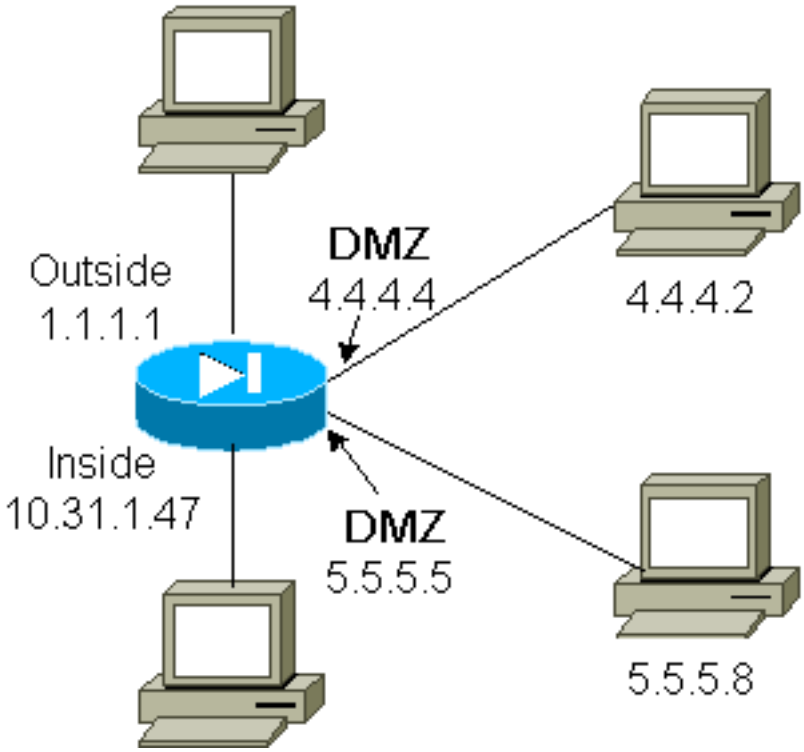
```
least secure

PIX outside (security0) = 1.1.1.1

pix/intf4 (DMZ - security20) = 4.4.4.4 & device 4.4.4.2

pix/intf5 (DMZ - security25) = 5.5.5.5 & device 5.5.5.8
```

(static to 4.4.4.15)

PIX inside (security100) = 10.31.1.47

most secure

الرسم التخطيطي للشبكة



تكوين PIX

نريد مصادقة حركة مرور Telnet بين PIX/INTF4 و PIX/INTF5:

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 pix/intf2 security10)
(nameif ethernet3 pix/intf3 security15
nameif ethernet4 pix/intf4 security20
nameif ethernet5 pix/intf5 security25
ip address outside 1.1.1.1 255.255.255.0
ip address inside 10.31.1.47 255.255.255.0
ip address pix/intf2 127.0.0.1 255.255.255.255)
(ip address pix/intf3 127.0.0.1 255.255.255.255
ip address pix/intf4 4.4.4.4 255.255.255.0
ip address pix/intf5 5.5.5.5 255.255.255.0
static (pix/intf5,pix/intf4) 4.4.4.15 5.5.5.8 netmask 255.255.255.255 0 0
aaa authentication telnet pix/intf4 5.5.5.0 255.255.255.0
AuthInbound 255.255.255.0 4.4.4.0
aaa authentication telnet pix/intf5 5.5.5.0 255.255.255.0
AuthInbound 255.255.255.0 4.4.4.0
+aaa-server TACACS+ protocol tacacs
+aaa-server AuthInbound protocol tacacs
aaa-server AuthInbound (inside) host 171.68.118.101 cisco timeout 5
```

محاسبة Xauth

إذا تم تكوين الأمر **sysopt connection permit-ipPSec**، وليس الأمر **sysopt ipSec متوافق مع**، في PIX باستخدام xauth، تكون المحاسبة صالحة لاتصالات TCP، ولكن ليس ICMP أو UDP.

معلومات ذات صلة

- صفحة دعم منتج PIX
- مرجع أوامر PIX
- صفحة دعم RADIUS
- طلبات التعليقات (RFCs)
- صفحة دعم UNIX الآمن من Cisco
- مصدر المحتوى الإضافي الآمن من Cisco لصفحة دعم Windows
- الدعم الفني - 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).