إجراء المصادقة والتفويض والمحاسبة للمستخدمين من خلال إصدار PIX الإصدار 5.2 والإصدارات الأحدث

المحتويات

المقدمة

يمكن إجراء مصادقة RADIUS و TACACS+ لاتصالات FTP و Telnet و HTTP من خلال جدار حماية PIX الآمن من Cisco. يتم إجراء مصادقة البروتوكولات الأخرى الأقل شيوعا للعمل. تفويض TACACS+ مدعوم. تفويض RADIUS غير مدعوم. تتضمن التغييرات في مصادقة PIX 5.2 والتفويض والمحاسبة (AAA) عبر الإصدار السابق دعم قائمة الوصول AAA للتحكم في من تمت مصادقته والموارد التي يمكن للمستخدم الوصول إليها. في المعيار PIX 5.3 والإصدارات الأحدث، يتمثل تغيير المصادقة والتفويض والمحاسبة (AAA) عبر الإصدارات السابقة من الرمز في أن منافذ RADIUS قابلة للتكوين.

ملاحظة: يمكن أن يقوم PIX 6.x بالحساب فيما يتعلق بحركة المرور العابرة ولكن ليس لحركة المرور المحددة ل PIX.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات أساسية خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج التالية:

- برنامج Cisco Secure PIX Firewall، الإصدارات 5.2.0.205 و 5.2.0.207

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

ملاحظة: إذا قمت بتشغيل الإصدار x.7 من برنامج PIX/ASA والإصدارات الأحدث، فارجع إلى تكوين خوادم AAA وقاعدة البيانات المحلية.

الاصطلاحات

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

المصادقة والتخويل والمحاسبة

فيما يلي شرح للمصادقة والتفويض والمحاسبة:

- المصادقة هي المستخدم.
- التخويل هو ما يقوم به المستخدم.
- المصادقة صالحة دون تخويل.
- التخويل غير صالح بدون مصادقة.
- المحاسبة هي ما قام به المستخدم.

ما يراه المستخدم مع المصادقة/التخويل في

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

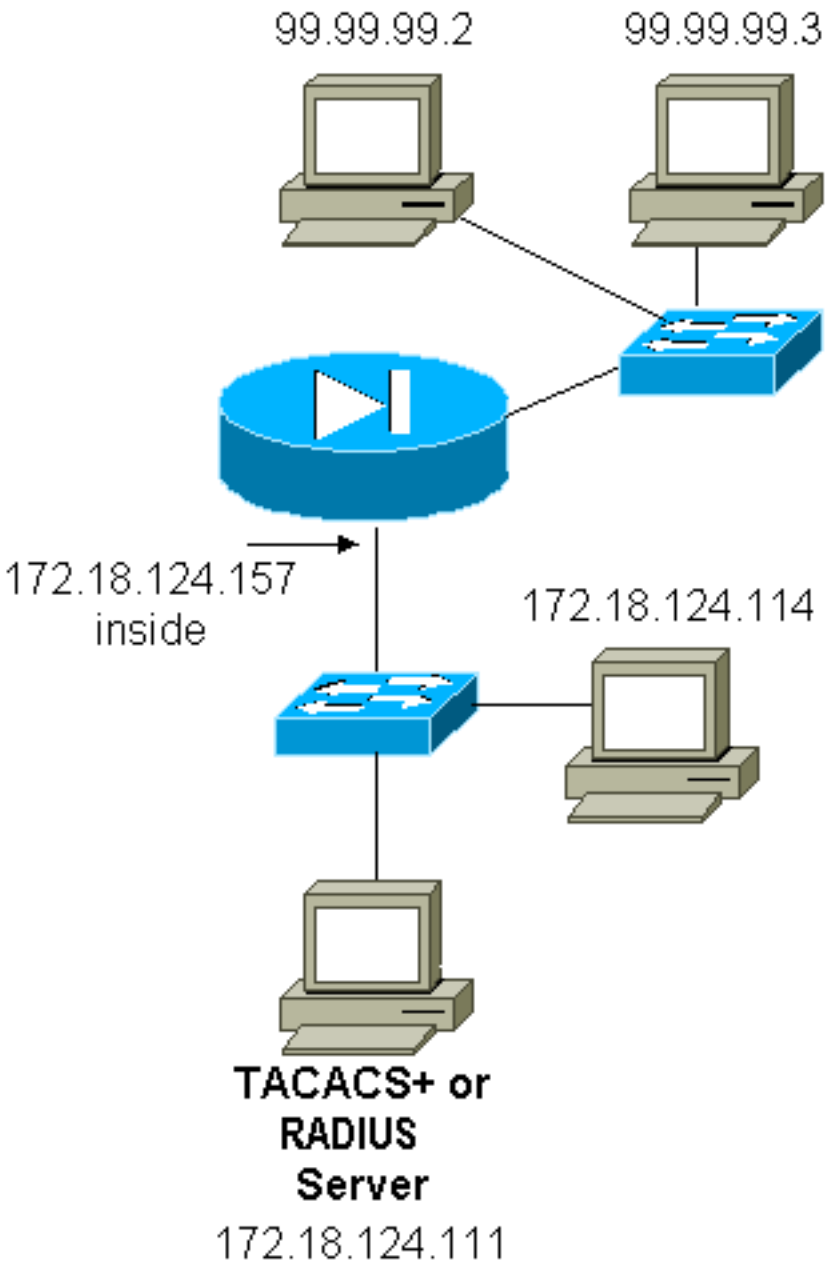
- **Telnet**— يرى المستخدم مطالبة باسم المستخدم تظهر، ثم طلبا بكلمة مرور. إذا نجحت المصادقة (والتفويض) في PIX/الخادم، فسيطلب من المستخدم اسم المستخدم وكلمة المرور بواسطة المضيف الوجهة فيما بعد.
- **FTP**—يرى المستخدم ظهور مطالبة اسم المستخدم. يحتاج المستخدم إلى إدخال "local_username@remote_username" لاسم المستخدم و"local_password@remote_password" لكلمة المرور. يرسل PIX "local_username" و "local_password" إلى خادم الأمان المحلي. إذا نجحت المصادقة (والتفويض) في PIX/الخادم، فسيتم تمرير "remote_username" و"remote_password" إلى خادم FTP الوجهة فيما 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 ينقضي وقتا لاتصال HTTP ولكنه لا يفعل ذلك، فمن المحتمل أن تتم إعادة المصادقة بالفعل مع المستعرض "إطلاق" اسم المستخدم وكلمة المرور المخزنة مؤقتا على PIX. يقوم PIX بإعادة توجيه هذا الأمر إلى خادم المصادقة. يعرض PIX syslog و/أو تصحيح أخطاء الخادم هذه الظاهرة. إذا بدا Telnet و FTP أنهما يعملان "بشكل طبيعي"، ولكن إتصالات HTTP لا تعمل، فهذا هو السبب.

خطوات التصحيح

- تأكد من عمل تكوين PIX قبل إضافة مصادقة AAA والتخويل. إذا لم تكن قادرا على تمرير حركة المرور قبل بدء المصادقة والتفويض، فلا يمكنك القيام بذلك بعد ذلك.
- تمكين نوع ما من التسجيل في PIX.قم بإصدار أمر **تصحيح أخطاء وحدة تحكم التسجيل** لتشغيل تصحيح أخطاء وحدة التحكم في التسجيل.**ملاحظة:** لا تستخدم تصحيح أخطاء وحدة تحكم التسجيل على نظام محمل بشكل كبير.أستخدم الأمر **logging monitor debug** لتسجيل جلسة عمل برنامج Telnet.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.

المصادقة فقط

الرسم التخطيطي للشبكة



إعداد الخادم - المصادقة فقط

تكوين خادم UNIX TACACS الآمن من Cisco

```
} User = cse
"password = clear "cse
default service = permit
{
```

تكوين خادم UNIX RADIUS الآمن من Cisco

ملاحظة: أضف عنوان PIX IP والمفتاح إلى قائمة خادم الوصول إلى الشبكة (NAS) بمساعدة واجهة المستخدم الرسومية (GUI) المتقدمة.

```
} user=bill
} radius=Cisco
} =check_items
```

```
"foo"=2
{
} =reply_attributes
6=6
{
{
{
```

Cisco Secure Windows RADIUS

أستخدم هذه الخطوات لإعداد خادم Cisco الآمن ل Windows RADIUS.

1. الحصول على كلمة مرور في قسم **إعداد المستخدم**.
2. من قسم **إعداد المجموعة**، قم بتعيين السمة 6 (نوع الخدمة) إلى **تسجيل الدخول** أو **Administrative**.
3. أضفت ال PIX عنوان في **ال nas تشكيل** قسم من ال gui.

بروتوكول TACACS+ الآمن من Cisco

يحصل المستخدم على كلمة مرور في قسم **إعداد المستخدم**.

تكوين خادم Liingston RADIUS

ملاحظة: إضافة عنوان PIX IP ومفتاح إلى ملف *العملاء*.

- بيل كلمة السر="foo" user-service-type = shell-user

إستحقاق تكوين خادم RADIUS

ملاحظة: إضافة عنوان PIX IP ومفتاح إلى ملف *العملاء*.

- بيل كلمة المرور="foo" نوع الخدمة = مستخدم shell

تكوين خادم TACACS+ FreeWARE

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

التكوين الأولي ل PIX - المصادقة فقط

التكوين الأولي ل PIX - المصادقة فقط
PIX Version 5.2(0)205 nameif ethernet0 outside security0 nameif ethernet1 inside security100 enable password 8Ry2YjIyt7RRXU24 encrypted passwd OnTrBUG1Tp0edmkr encrypted hostname pixfirewall fixup protocol ftp 21 fixup protocol http 80 fixup protocol h323 1720

```
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
!
These lines are necessary !--- if the new feature ---!
in 5.2 is used to define which !--- target/source IP
addresses are to be authenticated. access-list 101
permit tcp any any eq telnet
access-list 101 permit tcp any any eq ftp
access-list 101 permit tcp any any eq www
!
pager lines 24
logging on
no logging timestamp
no logging standby
logging console debugging
no logging monitor
no logging buffered
logging trap debugging
no logging history
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 10baset
mtu outside 1500
mtu inside 1500
ip address outside 99.99.99.1 255.255.255.0
ip address inside 172.18.124.157 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
arp timeout 14400
global (outside) 1 99.99.99.10-99.99.99.20 netmask
255.255.255.0
nat (inside) 1 172.18.124.0 255.255.255.0 0 0
static (inside,outside) 99.99.99.99 172.18.124.114
netmask 255.255.255.255 0 0
conduit permit tcp any any
conduit permit udp any any
conduit permit icmp any any
route inside 172.18.0.0 255.255.0.0 172.18.124.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h323 0:05:00
si p 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
!
For the purposes of illustration, the TACACS+ ---!
process is used !--- to authenticate inbound users and
RADIUS is used to authenticate outbound users. aaa-
+server TACACS+ protocol tacacs
aaa-server RADIUS protocol radius
+aaa-server AuthInbound protocol tacacs
aaa-server AuthInbound (inside) host 172.18.124.111
cisco timeout 5
aaa-server AuthOutbound protocol radius
aaa-server AuthOutbound (inside) host 172.18.124.111
cisco timeout 5
```

```
                                                                        !
   The next six statements are used to authenticate ---!
     all inbound !--- and outbound FTP, Telnet, and HTTP
 traffic. aaa authentication include ftp outside 0.0.0.0
                                        0.0.0.0 0.0.0.0 0.0.0.0
                                                 AuthInbound
       aaa authentication include telnet outside 0.0.0.0
                                        0.0.0.0 0.0.0.0 0.0.0.0
                                                 AuthInbound
  aaa authentication include http outside 0.0.0.0 0.0.0.0
                                        0.0.0.0 0.0.0.0
                                                 AuthInbound
   aaa authentication include http inside 0.0.0.0 0.0.0.0
                                        0.0.0.0 0.0.0.0
                                                AuthOutbound
 aaa authentication include telnet inside 0.0.0.0 0.0.0.0
                                        0.0.0.0 0.0.0.0
                                                AuthOutbound
    aaa authentication include ftp inside 0.0.0.0 0.0.0.0
                                        0.0.0.0 0.0.0.0
                                                AuthOutbound
                                                                        !
 OR the new 5.2 feature allows these two statements ---!
 in !--- conjunction with access-list 101 to replace the
  previous six statements. !--- Note: Do not mix the old
                                                .and new verbiage

        aaa authentication match 101 outside AuthInbound
        aaa authentication match 101 inside AuthOutbound
                                      no snmp-server location
                                       no snmp-server contact
                                  snmp-server community public
                                   no snmp-server enable traps
                                             floodguard enable
                                        no sysopt route dnat
                                    isakmp identity hostname
                                             telnet timeout 5
                                                ssh timeout 5
                                            terminal width 80
                  Cryptochecksum:5882f514247589d784a0d74c800907b8
                                                        end :
```

منافذ RADIUS القابلة للتكوين (5.3 ومتأخر)

تستخدم بعض خوادم RADIUS منافذ RADIUS بخلاف 1646/1645 (عادة 1813/1812). في PIX 5.3 والإصدارات الأحدث، يمكن تغيير منافذ مصادقة RADIUS ومحاسبته إلى شيء آخر غير الإعداد الافتراضي 1646/1645 باستخدام الأوامر التالية:

```
# aaa-server radius-authport
# aaa-server radius-acctport
```

أمثلة تصحيح أخطاء مصادقة PIX

راجع خطوات تصحيح الأخطاء للحصول على معلومات حول كيفية تشغيل تصحيح الأخطاء. هذه أمثلة لمستخدم في 99.99.99.2 الذي يبدأ حركة المرور إلى داخل 172.18.124.114 (99.99.99.99) والعكس. تتم مصادقة حركة المرور الواردة على بروتوكول TACACS، كما تتم مصادقة بروتوكول RADIUS عليها.

المصادقة الناجحة - TACACS+ (الواردة)

```
Auth start for user '???' from 99.99.99.2/11003 to 172.18.124.114/23 :109001
Authen Session Start: user 'cse', sid 2 :109011
Authentication succeeded for user 'cse' from 172.18.124.114/23 :109005
to 99.99. 99.2/11003 on interface outside
Built inbound TCP connection 4 for faddr 99.99.99.2/11003 :302001
(gaddr 99.99.99 .99/23 laddr 172.18.124.114/23 (cse
```

المصادقة غير الناجحة بسبب اسم المستخدم/كلمة المرور غير صحيحة - TACACS+ (الواردة). يرى المستخدم "خطأ: الحد الأقصى لعدد المحاولات التي تم تجاوزها."

```
Auth start for user '???' from 99.99.99.2/11004 to 172.18.1 24.114/23 :109001
Authentication failed for user '' from 172.18.124.114/23 :109006
to 99.99.99.2/1 1004 on interface outside
```

الخادم لا يتحدث إلى PIX - TACACS+ (الوارد). يرى المستخدم اسم المستخدم مرة واحدة ولا يطلب PIX أبدا كلمة مرور (هذه على Telnet). يرى المستخدم "خطأ: الحد الأقصى لعدد المحاولات التي تم تجاوزها."

```
Auth start for user '???' from 99.99.99.2/11005 to 172.18.124.114/23 :109001
Auth from 172.18.124.114/23 to 99.99.99.2/11005 failed :109002
server 172.18.12 4.111 failed) on interface outside)
Auth from 172.18.124.114/23 to 99.99.99.2/11005 failed :109002
server 172.18.12 4.111 failed) on interface outside)
Auth from 172.18.124.114/23 to 99.99.99.2/11005 failed :109002
server 172.18.12 4.111 failed) on interface outside)
Authentication failed for user '' from 172.18.124.114/23 :109006
to 99.99.99.2/1 1005 on interface outside
```

مصادقة جيدة - RADIUS (الصادر)

```
Auth start for user '???' from 172.18.124.114/35931 to 99.99.99.2/23 :109001
Authen Session Start: user 'bill', Sid 0 :109011
Authentication succeeded for user 'bill' from 172.18.124.114/35931 :109005
to 99 .99.99.2/23 on interface inside
```

مصادقة غير صحيحة (اسم المستخدم أو كلمة المرور) - RADIUS (الصادر). يرى المستخدم طلب اسم المستخدم، ثم كلمة المرور، لديه ثلاث فرص لإدخال هذه، وإذا لم ينجح، راجع "خطأ: الحد الأقصى لعدد المحاولات التي تم تجاوزها."

```
Auth start for user '???' from 172.18.124.114/35932 to 99.99.99.2/23 :109001
Auth from 172.18.124.114/35932 to 99.99.99.2/23 failed :109002
server 172.18.12 4.111 failed) on interface inside)
Authentication failed for user '' from 172.18.124.114/35932 :109006
to 99.99.99. 2/23 on interface inside
```

لن يتصل الخادم مع RADIUS - PIX (الصادر)، ولكن مع وجود برنامج تشغيل خلفي، أو الخادم غير قابل للجمع، أو عدم تطابق المفتاح/العميل. يرى المستخدم اسم المستخدم، ثم كلمة المرور، ثم "فشل خادم RADIUS"، وأخيرا "الخطأ: الحد الأقصى لعدد المحاولات التي تم تجاوزها."

```
Auth start for user '???' from 172.18.124.114/35933 to 99.99.99.2/23 :109001
Auth from 172.18.124.114/35933 to 99.99.99.2/23 failed :109002
server 172.18.12 4.111 failed) on interface inside)
Auth from 172.18.124.114/35933 to 99.99.99.2/23 failed :109002
server 172.18.12 4.111 failed) on interface inside)
```

```
Auth from 172.18.124.114/35933 to 99.99.99.2/23 failed :109002
        server 172.18.12 4.111 failed) on interface inside)
Authentication failed for user '' from 172.18.124.114/35933 :109006
        to 99.99.99. 2/23 on interface inside
```

المصادقة بالإضافة إلى التخويل

إذا كنت ترغب في السماح لجميع المستخدمين الذين تمت مصادقتهم بتنفيذ جميع العمليات (HTTP و FTP و Telnet) من خلال PIX، فإن المصادقة تكون كافية ولا تكون هناك حاجة إلى التفويض. ومع ذلك، إذا كنت ترغب في السماح ببعض مجموعة الخدمات الفرعية لمستخدمين معينين أو في الحد من وصول المستخدمين إلى مواقع معينة، فيلزمك التخويل. تفويض RADIUS غير صالح لحركة المرور عبر PIX. تفويض TACACS+ صالح في هذه الحالة.

إذا تم تمرير المصادقة وتم تشغيل التفويض، يرسل PIX الأمر الذي يقوم به المستخدم إلى الخادم. على سبيل المثال، "http 1.2.3.4." في الإصدار 5.2 من PIX، يتم إستخدام تفويض TACACS+ بالاقتران مع قوائم الوصول للتحكم في مكان توجه المستخدمين.

إذا كنت ترغب في تنفيذ تفويض HTTP (مواقع ويب التي تمت زيارتها)، أستخدم برامج مثل WebSense لأن موقع ويب واحد يمكن أن يحتوي على عدد كبير من عناوين IP المقترنة به.

إعداد الخادم - المصادقة بالإضافة إلى التخويل

تكوين خادم UNIX TACACS الآمن من Cisco

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

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

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

بروتوكول TACACS+ الآمن من Cisco

أكمل هذه الخطوات لإعداد خادم Cisco Secure Windows TACACS+.

1. انقر فوق **رفض أوامر IOS غير المتطابقة** في أسفل إعداد المجموعة.
2. طقطقة **يضيف/يحرر أمر جديد (FTP، http، telnet)**.على سبيل المثال، إذا كنت تريد السماح لبرنامج Telnet

بموقع محدد ("telnet 1.2.3.4")، فإن الأمر هو **telnet**. الوسيطة هي *1.2.3.4* . بعد ملء "command=**telnet**"، قم بتعبئة "allowed" عنوان (عناوين) IP في مستطيل الوسيطة (على سبيل المثال، "allowed 1.2.3.4"). إذا كان سيتم السماح بجميع برامج Telnet، فإن الأمر ما يزال **telnet**، ولكن انقر فوق **السماح بجميع الوسيطات غير المدرجة**. ثم انقر **أمر إنهاء التحرير**.
3. قم بإجراء الخطوة 2 لكل أمر من الأوامر المسموح بها (على سبيل المثال، Telnet و HTTP و FTP).
4. أضفت ال PIX عنوان في ال NAS تشكيل قسم مع مساعدة من ال gui.

تكوين خادم TACACS+ FreeWARE

```
      } 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
                             {
                             {
```

تكوين PIX - إضافة تخويل

إضافة أوامر لطلب التفويض:

```
aaa authorization include telnet outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
                                                                AuthInbound
  aaa authorization include http outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
                                                                AuthInbound
   aaa authorization include ftp outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
                                                                AuthInbound
```

تتيح الميزة 5.2 الجديدة لهذه العبارة بالاقتران مع قائمة الوصول 101 المحددة مسبقا لاستبدال الجمل الثلاث السابقة. لا ينبغي الخلط بين الفقرات القديمة والجديدة.

```
aaa authorization match 101 outside AuthInbound
```

أمثلة تصحيح أخطاء مصادقة PIX والتفويض

نجاح المصادقة والتفويض الجيدين - TACACS+

```
                                        Auth start for user '???' from :109001
                                      to 172.18.124.114/23 99.99.99.2/11010
                                  Authen Session Start: user 'cse', Sid 3 :109011
                                        Authentication succeeded for user :109005
                                cse' from 172.18.124.114/23 to 99.99.99.2/11010'
                                                      on interface outside
                                  Authen Session Start: user 'cse', Sid 3 :109011
                                   'Authorization permitted for user 'cse :109007
                                  from 99.99.99.2/11010 to 172.18.1  24.114/23
                                                      on interface outside
                                Built inbound TCP connection 2 for faddr :302001
                                  gaddr 99.99.99.99/23 laddr 99.99.99.2/11010
                                                     (cse) 172.18.124.114/23
```

مصادقة جيدة ولكن فشل التفويض - TACACS+. يرى المستخدم أيضا الرسالة "خطأ: تم رفض التفويض."

```
                                        Auth start for user '???' from :109001
                                      to 172.18.124.114/23 99.99.99.2/11011
                                Authen Session Start: user 'httponly', Sid 4 :109011
                                'Authentication succeeded for user 'httponly :109005
                                  from 172.18.124.114/23 to  9 9.99.99.2/11011
                                                      on interface outside
                                 'Authorization denied for user 'httponly :109008
                                    from 172.18.124.114/23 to 99.99.99.2/11011
                                                      on interface outside
```

ميزة قائمة الوصول الجديدة

في الإصدار 5.2 من برنامج PIX والإصدارات الأحدث، حدد قوائم الوصول على PIX. قم بتطبيقها على أساس كل مستخدم استنادا إلى ملف تعريف المستخدم على الخادم. يتطلب TACACS+ المصادقة والتفويض. يتطلب RADIUS المصادقة فقط. في هذا المثال، يتم تغيير المصادقة والتفويض الصادرين إلى TACACS+ . تم إعداد قائمة وصول على PIX.

ملاحظة: في الإصدار 6.0.1 من PIX والإصدارات الأحدث، إذا كنت تستخدم RADIUS، يتم تنفيذ قوائم الوصول من خلال إدخال القائمة في السمة 11 (filter-id) المعيارية IETF RADIUS [CSCdt50422]. في هذا المثال، يتم تعيين السمة 11 على 115 بدلا من تنفيذ الحكم "acl=115" الخاص بالمورد.

تكوين PIX

```
access-list 115 permit tcp any host 99.99.99.2 eq telnet
access-list 115 permit tcp any host 99.99.99.2 eq www
access-list 115 permit tcp any host 99.99.99.2 eq ftp
access-list 115 deny tcp any host 99.99.99.3 eq www
access-list 115 deny tcp any host 99.99.99.3 eq ftp
access-list 115 deny tcp any host 99.99.99.3 eq telnet
```

ملفات تعريف الخادم

ملاحظة: لا يتعرف الإصدار 2.1 من البرامج المجانية ل TACACS+ على نسخة "قائمة التحكم في الوصول".

تكوين خادم UNIX الآمن ل TACACS+ من Cisco

```
                                                      }user = pixa
                                                "*********" password = clear
```

```
} service=shell
    set acl=115
                {
                {
```

بروتوكول TACACS+ الآمن من Cisco

من أجل إضافة تفويض إلى PIX للتحكم في موقع انتقال المستخدم مع قوائم الوصول، حدد **shell/exec**، وحدد مربع **قائمة التحكم بالوصول**، وقم بتعبئة الرقم (يطابق رقم قائمة الوصول على PIX).

Cisco Secure UNIX RADIUS

```
                }user = pixa
"*********" password = clear
                } radius=Cisco
        } =reply_attributes
              "acl=115"=9,1
                {
                {
                {
```

Cisco Secure Windows RADIUS

RADIUS/Cisco هو نوع الجهاز. يحتاج المستخدم "Pixa" إلى اسم مستخدم وكلمة مرور وشيك و"acl=115" في المربع المستطيل Cisco/RADIUS حيث يقول 001\009 AV-pair (خاص بالمورد).

مردود

المستخدم الصادر "pixa" مع "acl=115" في ملف التعريف يصدق ويأذن. يقوم الخادم بتمرير قائمة التحكم في الوصول (ACL=115) إلى PIX، ويعرض PIX هذا:

```
                                pixfirewall#show uauth
        Current    Most Seen
              Authenticated Users       1          2
              Authen In Progress        0          2
user 'pixa' at 172.18.124.114, authenticated
                                  access-list 115
                        absolute   timeout: 0:05:00
                        inactivity timeout: 0:00:00
```

عندما يحاول المستخدم "pixa" الانتقال إلى 99.99.99.3 (أو أي عنوان IP باستثناء 99.99.99.2، بسبب الرفض الضمني)، يرى المستخدم هذا:

```
Error: acl authorization denied
```

قائمة وصول جديدة لكل مستخدم قابل للتنزيل مع الإصدار 6.2

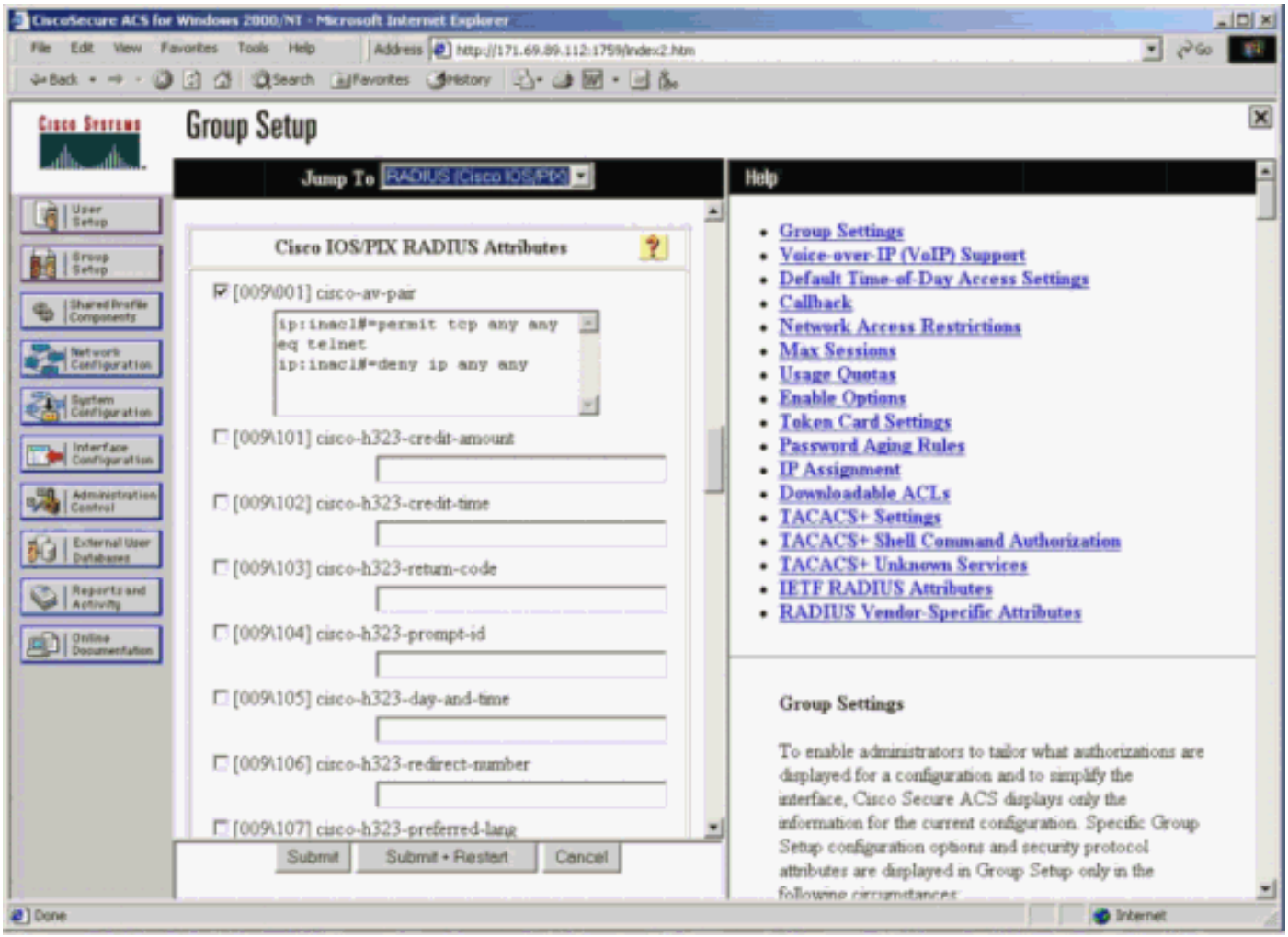
في إصدار البرنامج 6.2 والإصدارات الأحدث من جدار حماية PIX، يتم تحديد قوائم الوصول على خادم التحكم في الوصول (ACS) للتنزيل إلى PIX بعد المصادقة. لا يعمل هذا إلا مع بروتوكول RADIUS. لا توجد حاجة لتكوين قائمة الوصول على PIX نفسه. يتم تطبيق قالب مجموعة على مستخدمين متعددين.

في الإصدارات السابقة، يتم تحديد قائمة الوصول على PIX. وعند المصادقة، قام ACS بدفع اسم قائمة الوصول إلى PIX. يتيح الإصدار الجديد ل ACS دفع قائمة الوصول مباشرة إلى PIX.

ملاحظة: في حالة حدوث تجاوز الفشل، لا تتم إعادة مصادقة المستخدمين المنسوخين على جدول المصادقة. تم تنزيل قائمة الوصول مرة أخرى.

إعداد ACS

انقر فوق **إعداد المجموعة** وحدد نوع جهاز **RADIUS (Cisco IOS/PIX)** لإعداد حساب مستخدم. قم بتعيين اسم مستخدم ("cse"، في هذا المثال) وكلمة مرور للمستخدم. من قائمة السمات، حدد الخيار لتكوين **زوج *المورد*** **[001\009]**. قم بتحديد قائمة الوصول كما هو موضح في هذا المثال:



تصحيح أخطاء PIX: مصادقة صالحة وقائمة الوصول التي تم تنزيلها

- يسمح فقط ب Telnet ويرفض حركة مرور أخرى.

```
:pix# 305011: Built dynamic TCP translation from inside
   to outside:172.16.171.201/1049 172.16.171.33/11063
Auth start for user '???' from 172.16.171.33/11063 :109001
                                  to 172.16.171.202/23
      Authen Session Start: user 'cse', sid 10 :109011
       'Authentication succeeded for user 'cse :109005
                           from 172.16.171.33/11063
          to 172.16.171.202/23 on interface inside

:Built outbound TCP connection 123 for outside :302013
   :to inside (172.16.171.202/23) 172.16.171.202/23
    (cse) (172.16.171.201/1049) 172.16.171.33/11063
```

مخرجات من الأمر **show uauth**.

```
pix#show uauth
Current Most Seen
```

```
Authenticated Users 1 1
Authen In Progress 0 1
user 'cse' at 172.16.171.33, authenticated
access-list AAA-user-cse
absolute timeout: 0:05:00
inactivity timeout: 0:00:00
```

الإخراج من الأمر **show access-list**.

```
pix#show access-list
access-list AAA-user-cse; 2 elements
(access-list AAA-user-cse permit tcp any any eq telnet (hitcnt=1
(access-list AAA-user-cse deny ip any any (hitcnt=0
```

- يرفض فقط Telnet ويسمح بحركة مرور أخرى.

```
:pix# 305011: Built dynamic TCP translation from inside
to outside:172.16.171.201/1050 172.16.171.33/11064
Auth start for user '???' from 172.16.171.33/11064 to :109001
172.16.171.202/23
Authen Session Start: user 'cse', sid 11 :109011
'Authentication succeeded for user 'cse :109005
from 172.16.171.33/11064
to 172.16.171.202/23 on interface inside
'Authorization denied (acl= AAA-user-cse) for user 'cse :109015
from 172.16.171.33/11064 to 172.16.171.202/23 on interface inside
```

مخرجات من الأمر **show uauth**.

```
pix#show uauth
Current Most Seen
Authenticated Users 1 1
Authen In Progress 0 1
user 'cse' at 172.16.171.33, authenticated
access-list AAA-user-cse
absolute timeout: 0:05:00
inactivity timeout: 0:00:00
```

الإخراج من الأمر **show access-list**.

```
pix#show access-list
access-list AAA-user-cse; 2 elements
(access-list AAA-user-cse deny tcp any any eq telnet (hitcnt=1
(access-list AAA-user-cse permit ip any any (hitcnt=0
```

قائمة وصول جديدة قابلة للتنزيل لكل مستخدم باستخدام ACS 3.0

في ACS الإصدار 3.0، يسمح مكون ملف التعريف المشترك للمستخدم بإنشاء قالب قائمة وصول وتعريف اسم القالب لمستخدمين أو مجموعات معينة. يمكن إستخدام اسم القالب مع أكبر عدد من المستخدمين أو المجموعات حسب الحاجة. وهذا الأمر يقلل من الحاجة إلى تكوين قوائم وصول متطابقة لكل مستخدم.

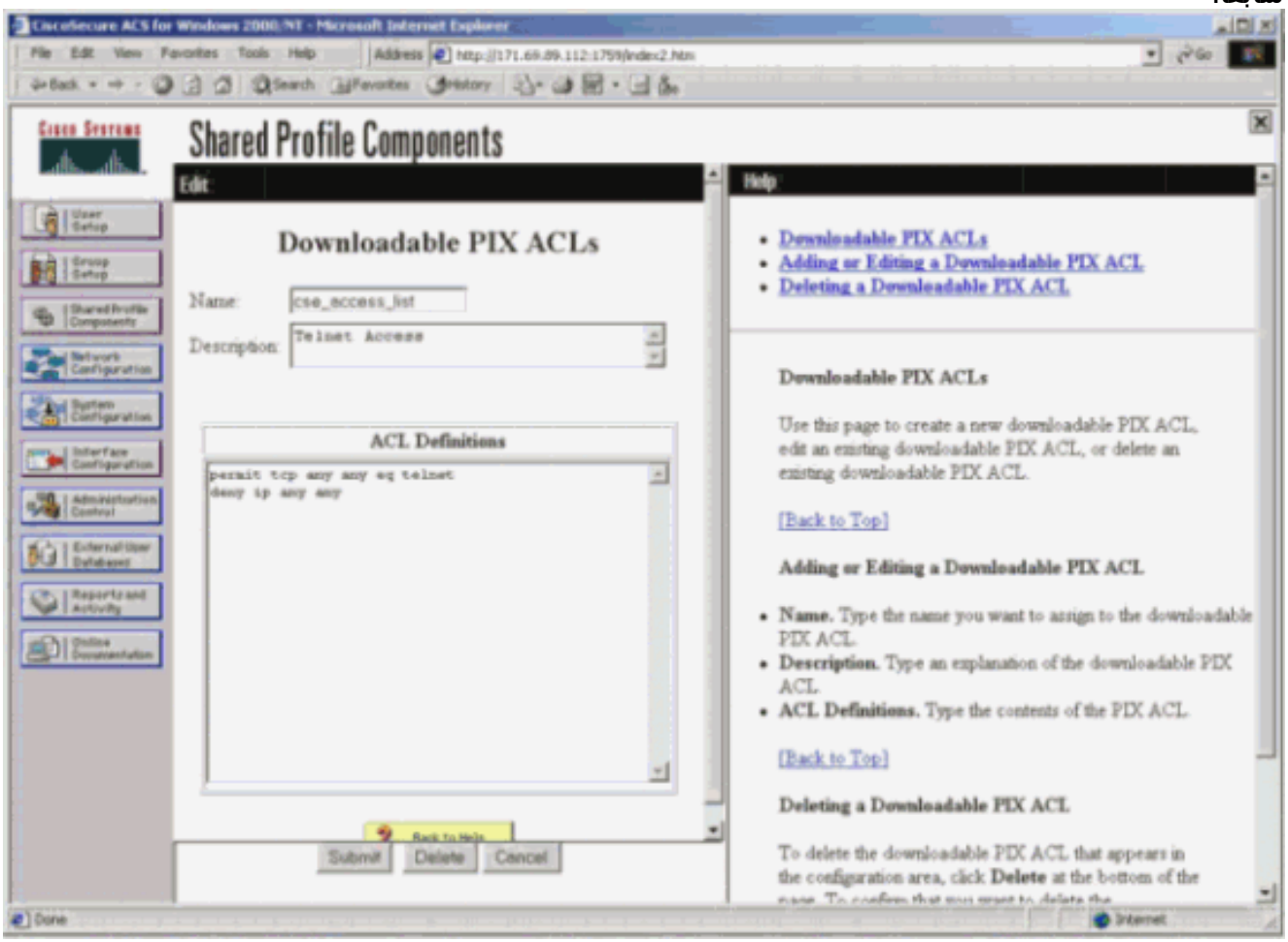
ملاحظة: في حالة حدوث تجاوز الفشل، لا يتم نسخ المصادقة إلى PIX الثانوي. في حالة تجاوز الفشل، يتم الحفاظ على الجلسة. ومع ذلك، يجب إعادة مصادقة الاتصال الجديد وتنزيل قائمة الوصول مرة أخرى.

إستخدام توصيفات مشتركة

أكمل الخطوات التالية عندما تستخدم توصيفات مشتركة.

1. طقطقة **قارن تشكيل**.
2. تحقق من **قوائم التحكم في الوصول (ACL) القابلة للتنزيل على مستوى المستخدم** و/أو **قوائم التحكم في الوصول (ACL) القابلة للتنزيل على مستوى المجموعة**.
3. انقر على **مكونات التوصيف المشترك**. انقر فوق **قوائم التحكم في الوصول (ACL) القابلة للتنزيل على مستوى المستخدم**.

4. تحديد قوائم التحكم في الوصول (ACL) القابلة للتنزيل.
5. انقر على **إعداد المجموعة**. تحت قوائم التحكم في الوصول (ACL) القابلة للتنزيل، قم بتعيين قائمة الوصول إلى PIX إلى قائمة الوصول التي تم إنشاؤها سابقا.



تصحيح أخطاء PIX: مصادقة صالحة وقائمة وصول تم تنزيلها باستخدام ملفات التعريف المشتركة

- يسمح فقط ب Telnet ويرفض حركة مرور أخرى.

```
:pix# 305011: Built dynamic TCP translation from inside
    to outside:172.16.171.201/1051 172.16.171.33/11065
Auth start for user '???' from 172.16.171.33/11065 to :109001
                                        172.16.171.202/23
      Authen Session Start: user 'cse', sid 12 :109011
   Authentication succeeded for user 'cse' from :109005
to 172.16.171.202/23 on interface inside 172.16.171.33/11065
  :Built outbound TCP connection 124 for outside :302013
    :to inside (172.16.171.202/23) 172.16.171.202/23
     (cse) (172.16.171.201/1051) 172.16.171.33/11065
```

مخرجات من الأمر **show uauth**.

```
pix#show uauth
                Current Most Seen
Authenticated Users 1 1
   Authen In Progress 0 1
user 'cse' at 172.16.171.33, authenticated
access-list #ACSACL#-PIX-cse_access_list-3cff1bb3
                absolute timeout: 0:05:00
            inactivity timeout: 0:00:00
pix# 111009: User 'enable_15' executed cmd: show uauth
                                                #pix
```

الإخراج من الأمر **show access-list**.

```
pix#show access-list
access-list #ACSACL#-PIX-cse_access_list-3cff1bb3; 2 elements
            access-list #ACSACL#-PIX-cse_access_list-3cff1bb3
                   (permit tcp any any eq telnet (hitcnt=1
            access-list #ACSACL#-PIX-cse_access_list-3cff1bb3
                                (deny ip any any (hitcnt=0
 pix# 111009: User 'enable_15' executed cmd: show access-list
```

- يرفض فقط Telnet ويسمح بحركة مرور أخرى.

```
:pix# 305011: Built dynamic TCP translation from inside
  to outside:172.16.171.201/1052 172.16.171.33/11066
Auth start for user '???' from 172.16.171.33/11066 to :109001
                                    172.16.171.202/23
          Authen Session Start: user 'cse', sid 13 :109011
           'Authentication succeeded for user 'cse :109005
                                from 172.16.171.33/11066
                    to 172.16.171.202/23 on interface inside
(Authorization denied (acl=#ACSACL#-PIX-cse_access_list-3cff1dd6 :109015
                        for user 'cse' from 172.16.171.33/11066
                    to 172.16.171.202/23 on interface inside
```

مخرجات من الأمر **show uauth**.

```
pix#show uauth
                        Current Most Seen
                Authenticated Users 1 1
                  Authen In Progress 0 1
         user 'cse' at 172.16.171.33, authenticated
      access-list #ACSACL#-PIX-cse_access_list-3cff1dd6
                          absolute timeout: 0:05:00
                        inactivity timeout: 0:00:00
 pix# 111009: User 'enable_15' executed cmd: show uauth
```

الإخراج من الأمر **show access-list**.

```
pix#show access-list
access-list #ACSACL#-PIX-cse_access_list-3cff1dd6; 2 elements
            access-list #ACSACL#-PIX-cse_access_list-3cff1dd6
                    (deny tcp any any eq telnet (hitcnt=1
            access-list #ACSACL#-PIX-cse_access_list-3cff1dd6
                         (permit ip any any (hitcnt=0
#pix# 111009: User 'enable_15' executed cmd: show access-listpix
```

إضافة محاسبة

تكوين PIX - إضافة محاسبة

(TACACS (AuthInbound=tacacs

إضافة هذا الأمر.

```
aaa accounting include any inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
AuthInbound
```

أو أستخدم الميزة الجديدة في 5.2 لتحديد ما يجب حسابه بواسطة قوائم الوصول.

```
aaa accounting match 101 outside AuthInbound
```

ملاحظة: يتم تحديد قائمة الوصول 101 بشكل منفصل.

(RADIUS (AuthOutbound=radius

إضافة هذا الأمر.

```
aaa accounting include any inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
AuthOutbound
```

أو أستخدم الميزة الجديدة في 5.2 لتحديد ما يجب حسابه بواسطة قوائم الوصول.

```
aaa accounting match 101 outside AuthOutbound
```

ملاحظة: يتم تحديد قائمة الوصول 101 بشكل منفصل.

ملاحظة: يمكن إنشاء سجلات المحاسبة لجلسات العمل الإدارية على PIX بدءا من رمز PIX 7.0.

أمثلة محاسبية

- مثال محاسبة TACACS ل Telnet من 99.99.99.2 خارج إلى 172.18.124.114 داخل (99.99.99.99).

```
pixuser PIX 99.99.99.2 start server=rtp-cherry 172.18.124.157
time=10:36:16 date=08/23/2000 task_id=0x0 foreign_ip=99.99.99.2
                                local_ip=172.18.124.114 cmd=telnet
 pixuser PIX 99.99.99.2 stop server=rtp-cherry 172.18.124.157
time=10:37:50 date=08/23/2000 task_id=0x0 foreign_ip=99.99.99.2
                                    local_ip=172.18.124.114
cmd=telnet elapsed_time=94 bytes_in=61 bytes_out=254
```

- مثال محاسبة RADIUS للاتصال من 172.18.124.114 داخل إلى 99.99.99.2 خارج (Telnet) و 99.99.99.3 خارج (HTTP).

```
                                Sun Aug  6 03:59:28 2000
                                    Acct-Status-Type = Start
                                NAS-IP-Address = 172.18.124.157
                                 Login-IP-Host = 172.18.124.114
                                           Login-TCP-Port = 23
                                  Acct-Session-Id = 0x00000004
                                              User-Name = cse
                        Vendor-Specific = Source-IP=172.18.124.114
                               Vendor-Specific = Source-Port=35937
                        Vendor-Specific = Destination-IP=99.99.99.2
                             Vendor-Specific = Destination-Port=23

                                Sun Aug  6 03:59:32 2000
                                    Acct-Status-Type = Stop
                                NAS-IP-Address = 172.18.124.157
                                 Login-IP-Host = 172.18.124.114
                                           Login-TCP-Port = 23
                                  Acct-Session-Id = 0x00000004
                                               Username = cse
                                     Acct-Session-Time = 4
                                    Acct-Input-Octets = 101
                                   Acct-Output-Octets = 143
                        Vendor-Specific = Source-IP=172.18.124.114
                               Vendor-Specific = Source-Port=35937
```

```
Vendor-Specific = Destination-IP=99.99.99.2
      Vendor-Specific = Destination-Port=23

                                  Sun Aug  6 04:05:02 2000
                         Acct-Status-Type = Start
                    NAS-IP-Address = 172.18.124.157
                     Login-IP-Host = 172.18.124.114
                               Login-TCP-Port = 80
                                    Username = cse
     Vendor-Specific = Source-IP=172.18.124.114
            Vendor-Specific = Source-Port=35949
Vendor-Specific = Destination-IP=99.99.99.3
      Vendor-Specific = Destination-Port=80

                                  Sun Aug  6 04:05:02 2000
                        Acct-Status-Type = Stop
                    NAS-IP-Address = 172.18.124.157
                     Login-IP-Host = 172.18.124.114
                               Login-TCP-Port = 80
                      Acct-Session-Id = 0x0000000a
                                    Username = cse
                           Acct-Session-Time = 0
                        Acct-Input-Octets = 1277
                        Acct-Output-Octets = 310
     Vendor-Specific = Source-IP=172.18.124.114
            Vendor-Specific = Source-Port=35949
Vendor-Specific = Destination-IP=99.99.99.3
      Vendor-Specific = Destination-Port=80
```

إستخدام أمر الاستثناء

في هذه الشبكة، إذا قررت أن مصدر أو وجهة معينة لا تحتاج إلى مصادقة أو تفويض أو محاسبة، قم بإصدار هذه الأوامر.

```
aaa authentication exclude telnet outside 172.18.124.114 255.255.255.255
                                  AuthInbound 255.255.255.255 99.99.99.3
 aaa authorization exclude telnet outside 172.18.124.114 255.255.255.255
                                  AuthInbound 255.255.255.255 99.99.99.3
    aaa accounting exclude telnet outside 172.18.124.114 255.255.255.255
                                  AuthInbound 255.255.255.255 99.99.99.3
```

ملاحظة: لديك بالفعل أوامر include.

```
aaa authentication|authorization|accounting include http|ftp|telnet
```

أو، مع الميزة الجديدة في 5.2، قم بتعريف ما تريد إستبعاده.

```
access-list 101 deny tcp host 99.99.99.3 host 172.18.124.114 eq telnet
   access-list 101 deny tcp host 99.99.99.3 host 172.18.124.114 eq ftp
   access-list 101 deny tcp host 99.99.99.3 host 172.18.124.114 eq www
                  access-list 101 permit tcp any any eq telnet
                     access-list 101 permit tcp any any eq www
                     access-list 101 permit tcp any any eq ftp
```

```
aaa authentication match 101 outside AuthInbound
aaa authorization match 101 outside AuthInbound
aaa accounting match 101 outside AuthInbound
```

ملاحظة: إذا قمت باستبعاد مربع من المصادقة وكان لديك تخويل في، فيجب أيضا إستبعاد 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 (أي أن المستخدم لديه جلسة عمل من خلال PIX). يعمل هذا بشكل جيد لاتصالات Telnet و FTP بسبب طبيعة الاتصالات. ومع ذلك، لا يعمل هذا بشكل جيد ل HTTP. في هذا المثال، يتم إستخدام تكوين شبكة مختلف، ولكن المفاهيم هي نفسها.

Telnet للمستخدم من خلال PIX، للمصادقة على الطريق.

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

نظرا لأن الخادم قد شاهد سجل "بدء" ولكن ليس سجل "إيقاف"، في هذه المرحلة من الوقت، يظهر الخادم أن مستخدم "برنامج Telnet" قد سجل الدخول. إذا حاول المستخدم إجراء اتصال آخر يتطلب مصادقة (ربما من كمبيوتر آخر)، وإذا تم تعيين الحد الأقصى لجلسات العمل على "1" على الخادم لهذا المستخدم (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 1 laddr 9.9.9.25/80
duration 0:00:00 bytes 171.68.118.100/1281
(cse) 1907
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. هنا مثال من HTTP حيث 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 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 16:35.35 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). لم يتم تسجيل دخول المستخدم إلى موقع ويب. لا يتم فتح الاتصال عندما يقوم المستخدم بقراءة صفحة ويب. الحد الأقصى لجلسات العمل أو عرض المستخدمين الذين قاموا بتسجيل الدخول لا يعملون هنا. وذلك لأن وقت الاتصال (الوقت بين "Build" و"Teardown") في HTTP قصير جدا. سجل "البدء" و"الإيقاف" هو الثاني الفرعي. لا يوجد سجل "بدء" بدون سجل "إيقاف" لأن السجلات تحدث في نفس اللحظة تقريبا. لا يزال هناك سجل "البدء" و"الإيقاف" الذي تم إرساله 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.

واجهة المستخدم

تغيير رسالة مطالبة المستخدمين

إذا كان لديك الأمر:

```
auth-prompt prompt PIX515B
```

ثم يرى المستخدمون الذين يمرون ب PIX هذه المطالبة.

```
PIX515B
```

تخصيص الرسالة التي يراها المستخدمون

إذا كانت لديك الأوامر:

```
"auth-prompt accept "GOOD_AUTHENTICATION
 "auth-prompt reject "BAD_AUTHENTICATION
```

ثم يرى المستخدمون رسالة حول حالة المصادقة عند تسجيل دخول فاشل/ناجح.

```
PIX515B
Username: junk
```

```
:Password
"BAD_AUTHENTICATION"

PIX515B
Username: cse
:Password
"GOOD_AUTHENTICATION"
```

فترات الانتظار الخاملة والمطلقة لكل مستخدم

يتحكم الأمر **timeout uauth** PIX في عدد مرات طلب إعادة المصادقة. إذا كانت مصادقة/تفويض TACACS+ قيد التشغيل، يتم التحكم في ذلك على أساس كل مستخدم. تم إعداد ملف تعريف المستخدم هذا للتحكم في المهلة (يوجد هذا على خادم TACACS+ للبرامج المجانية وتقع فترات انتهاء المهلة في دقائق).

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

بعد المصادقة/التخويل:

```
show uauth
Current    Most Seen
Authenticated Users       1          2
Authen In Progress        0          1
:user 'cse' at 99.99.99.3, authorized to
port 172.18.124.114/telnet
absolute   timeout: 0:02:00
inactivity timeout: 0:01:00
```

في نهاية دقيقتين:

المهلة المطلقة - تم تعطيل جلسة العمل:

```
Authen Session End: user 'cse', Sid 20, elapsed 122 seconds :109012
Teardown TCP connection 32 faddr 99.99.99.3/11025 :302002
gaddr 99.99.99.99/23 l addr 172.18.124.114/23 duration 0:02:26
(bytes 7547 (TCP FINs
```

الصادر ل HTTP الظاهري

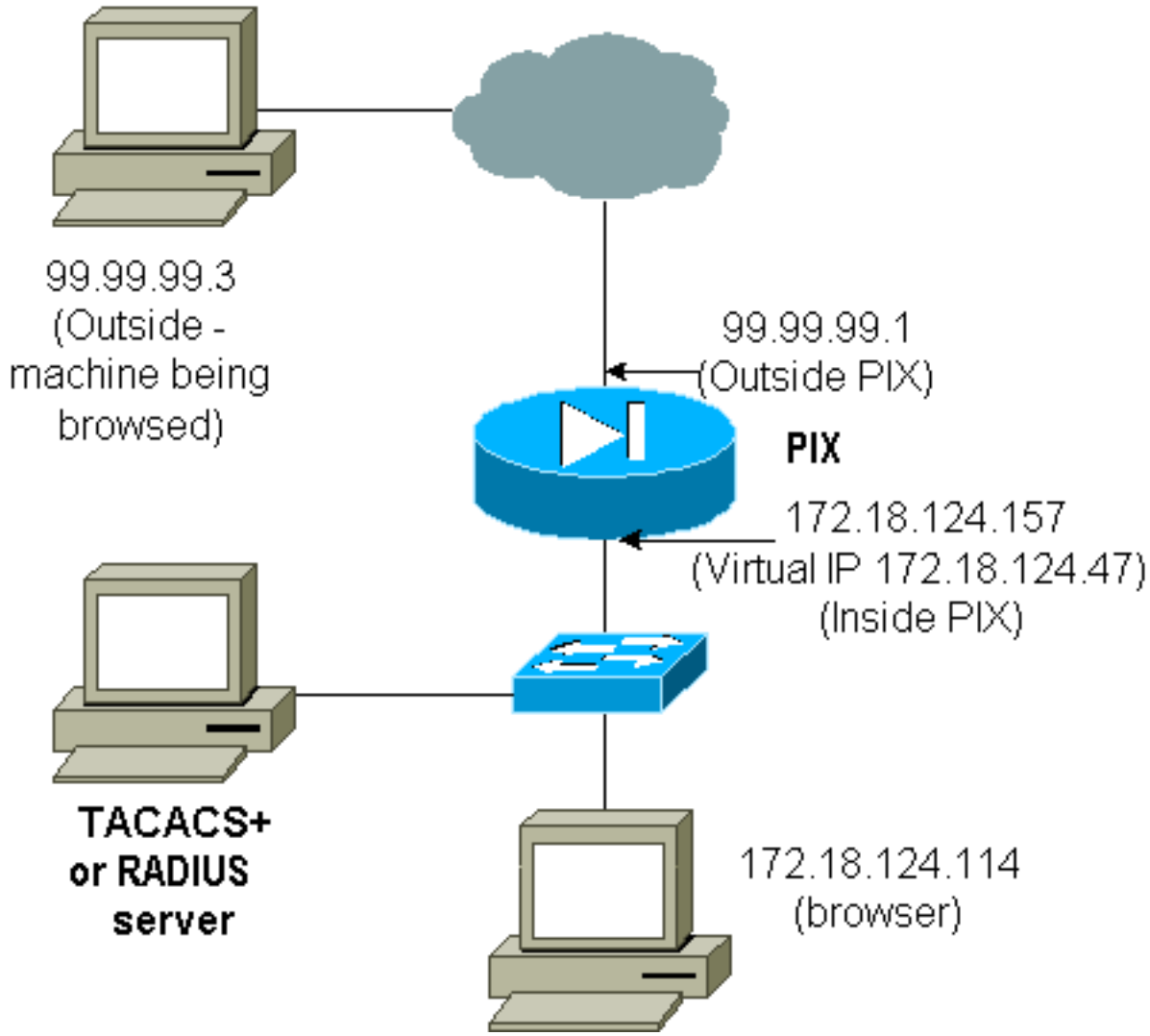
إذا كانت المصادقة مطلوبة على مواقع خارج PIX وكذلك على PIX نفسه، فيتم ملاحظة سلوك غير عادي للمستعرض في بعض الأحيان، نظرا لأن المستعرضات تخزن اسم المستخدم وكلمة المرور مؤقتا.

لتجنب هذا، قم بتنفيذ HTTP الظاهري بإضافة عنوان RFC 1918 (عنوان غير قابل للتوجيه على الإنترنت، ولكنه صالح وفريد ل PIX داخل الشبكة) إلى تكوين PIX بالتنسيق.

```
#.#.#.# virtual http
```

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.

ملاحظة: يجب تضمين عناوين HTTP الظاهرية و Telnet IP الظاهرية في عبارات **مصادقة AAA**. في هذا المثال، يتضمن تحديد 0.0.0.0 هذه العناوين.



في تكوين PIX أضف هذا الأمر.

```
virtual http 172.18.124.47
```

يشير المستخدم إلى المستعرض على 99.99.99.3. يتم عرض هذه الرسالة.

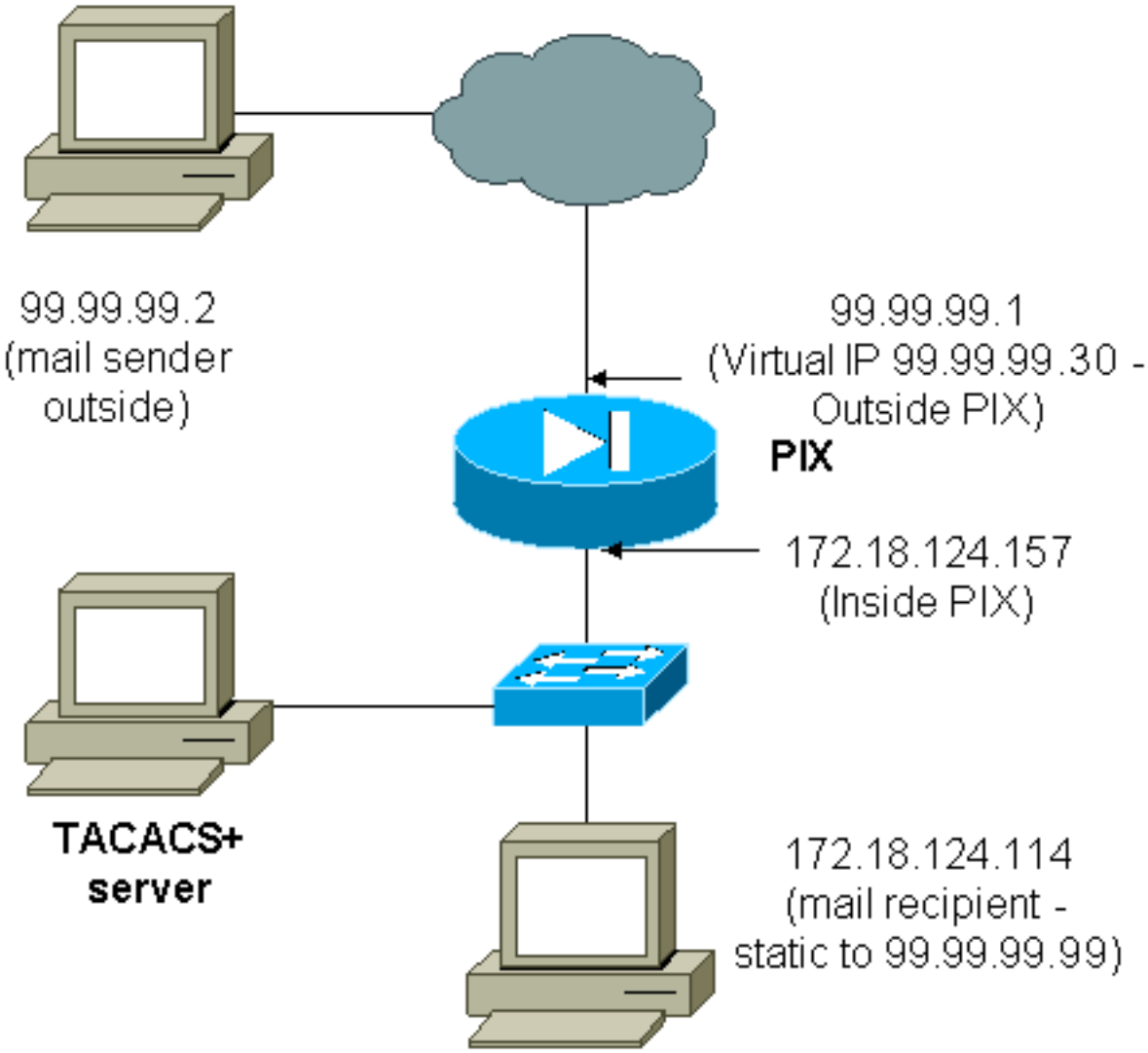
```
Enter username for PIX515B (IDXXX) at 172.18.124.47
```

بعد المصادقة، تتم إعادة توجيه حركة المرور إلى 99.99.99.3.

برنامج Telnet الظاهري

ملاحظة: يجب تضمين عناوين HTTP الظاهرية و Telnet IP الظاهرية في عبارات **مصادقة AAA**. في هذا المثال، يتضمن تحديد 0.0.0.0 هذه العناوين.

الوارد لبرنامج Telnet الظاهري



ليس من المهم مصادقة البريد الوارد نظرا لأنه لا يتم عرض إطار لإرسال البريد الوارد. أستخدم أمر **الاستبعاد** بدلا من ذلك. ولكن بهدف التوضيح، تضاف هذه الأوامر.

```
aaa authentication include tcp/25 outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
                                                                AuthInbound
 aaa authorization include tcp/25 outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
                                                                AuthInbound
OR the new 5.2 feature allows these !--- four statements to perform the same function. !--- ---!
.Note: The old and new verbiage should not be mixed

                                                access-list 101 permit tcp any any eq smtp
The "mail" was a Telnet to port 25. access-list 101 permit tcp any any eq telnet ---!
                                                aaa authentication match 101 outside AuthInbound
                                                aaa authorization match 101 outside AuthInbound
                                                                                              !
```

```
plus ! virtual telnet 99.99.99.30 ---!
static (inside,outside) 99.99.99.30 172.18.124.30
                    netmask 255.255.255.255 0 0
static (inside,outside) 99.99.99.99 172.18.124.114
                    netmask 255.255.255.255 0 0
conduit permit tcp host 99.99.99.30 eq telnet any
conduit permit tcp host 99.99.99.99 eq telnet any
  conduit permit tcp host 99.99.99.99 eq smtp any
```

المستخدمون (هذا هو البرنامج المجاني TACACS+):

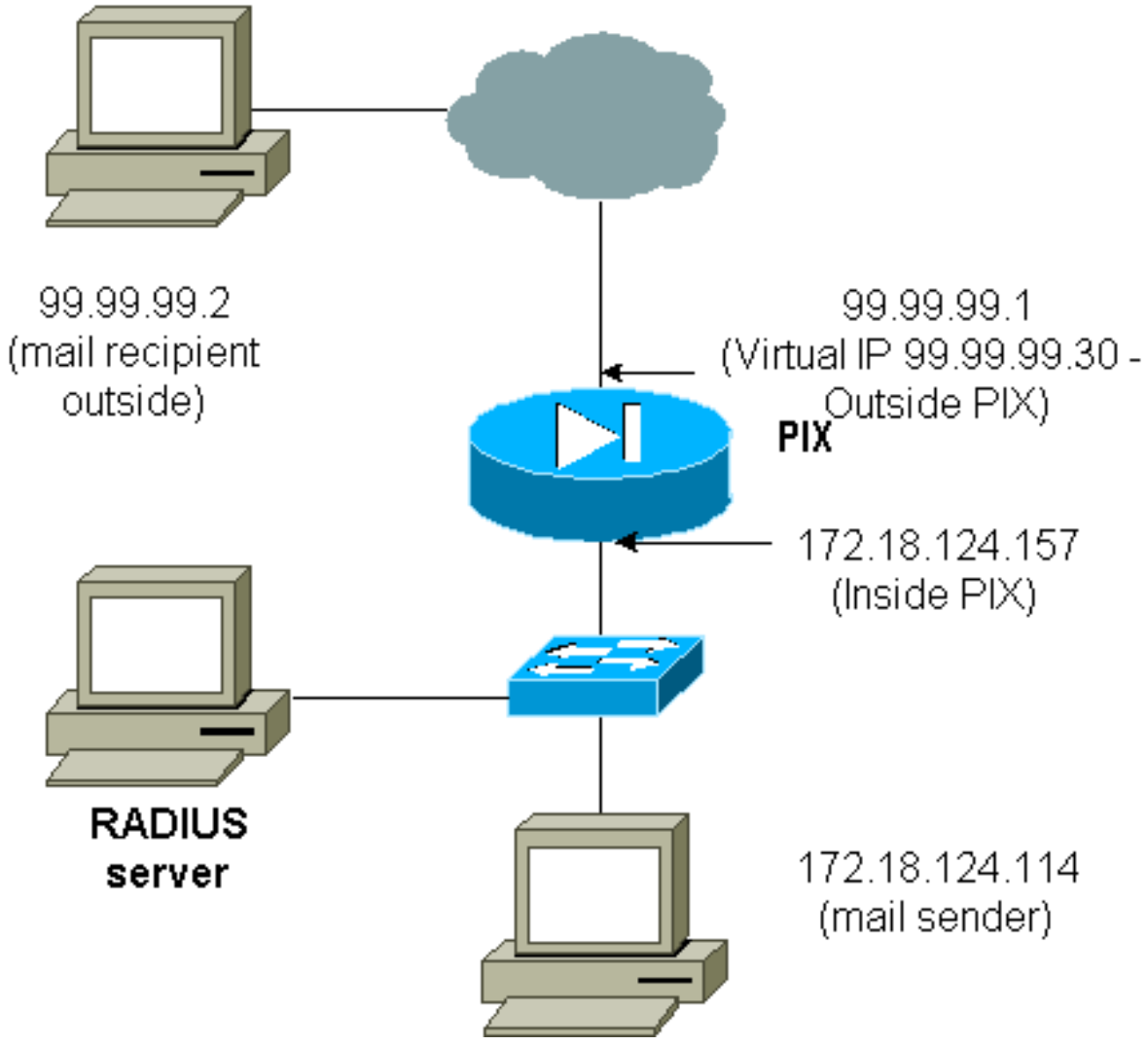
```
                                } user = cse
                          default service = permit
                       "login = cleartext "csecse
                                        {


                                } user = pixuser
                       "login = cleartext "pixuser
                                } service = exec
                                        {
                                  } cmd = telnet
                                       *. permit
                                        {
                                        {
```

في حالة تشغيل المصادقة فقط، يرسل كلا المستخدمين البريد الوارد بعد المصادقة على برنامج Telnet إلى عنوان IP 99.99.99.30. إذا تم تمكين التخويل، فإن المستخدم "Telnet "cse إلى 99.99.99.30، ويدخل اسم مستخدم/كلمة مرور TACACS+. عمليات إسقاط اتصال Telnet. وبعد ذلك يرسل المستخدم "cse" البريد إلى 99.99.99.99 (172.18.124.114). تنجح المصادقة للمستخدم "Pixuser". ومع ذلك، عندما يرسل PIX طلب التفويض ل cmd=tcp/25 و cmd-arg=172.18.124.114، يفشل الطلب، كما هو موضح في هذا الإخراج.

```
                                  Auth start for user '???' from :109001
                               to 172.18.124.114/23 99.99.99.2/11036
                            Authentication succeeded for user :109005
                                 cse' from 172.18.124.114/23 to'
                               on interface outside 99.99.99.2/11036

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

                                pixfirewall# 109001: Auth start for user '???' from
                                           to 172.18.124.30/23 99.99.99.2/11173
                                      Authen Session Start: user 'cse', sid 10 :109011
                          Authentication succeeded for user 'cse' from 99.99.99.2/23 :109005
                                to 172.18.124.30/11173 on interface outside
                                      Authen Session Start: user 'cse', sid 10 :109011
                        Authorization permitted for user 'cse' from 99.99.99.2/11173 :109007
                                   to 172.18.124.30/23 on interface outside
                                Auth start for user 'cse' from 99.99.99.2/11174 to :109001
                                                        172.18.124.114/25
                                      Authen Session Start: user 'cse', sid 10 :109011
                        Authorization permitted for user 'cse' from 99.99.99.2/11174 :109007
                                   to 172.18.124.114/25 on interface outside
                          Built inbound TCP connection 5 for faddr 99.99.99.2/11174 :302001
```

```
(gaddr 99.99.99.99/25 laddr 172.18.124.114/25 (cse

pixfirewall# 109001: Auth start for user '???' from 99.99.99.2/11175
                                                to 172.18.124.30/23
                    Authen Session Start: user 'pixuser', sid 11 :109011
Authentication succeeded for user 'pixuser' from 99.99.99.2/23 :109005
                        to 172.18.124.30/11175 on interface outside
                    Authen Session Start: user 'pixuser', sid 11 :109011
Authorization permitted for user 'pixuser' from 99.99.99.2/11175 :109007
                            to 172.18.124.30/23 on interface outside
                Auth start for user 'pixuser' from 99.99.99.2/11176 :109001
                                                to 172.18.124.114/25
        Authorization denied for user 'pixuser' from 99.99.99.2/25 :109008
                        to 172.18.124.114/11176 on interface outside
```

الصادر لبرنامج Telnet الظاهري



ليس من المهم مصادقة البريد الوارد نظرا لأنه لا يتم عرض إطار لإرسال البريد الوارد. أستخدم أمر **الاستبعاد** بدلا من ذلك. ولكن بهدف التوضيح، تضاف هذه الأوامر.

ليست فكرة عظيمة مصادقة البريد الصادر نظرا لأنه لا يتم عرض نافذة لإرسال البريد الصادر. أستخدم أمر **الاستبعاد** بدلا من ذلك. ولكن لأغراض التوضيح، تتم إضافة هذه الأوامر.

```
aaa authentication include tcp/25 inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
                                                                AuthOutbound
OR the new 5.2 feature allows these three statements !--- to replace the previous ---!
```

```
.statements. !--- Note: Do not mix the old and new verbiage

access-list 101 permit tcp any any eq smtp
access-list 101 permit tcp any any eq telnet
aaa authentication match 101 inside AuthOutbound
!
plus ! virtual telnet 99.99.99.30 ---!
.The IP address on the outside of PIX is not used for anything else ---!
```

لإرسال بريد من الداخل إلى الخارج، قم بتقديم موجه أوامر على مضيف البريد وبرنامج Telnet إلى 99.99.99.30. وهذا يفتح ثقبا للبريد ليمر به. يتم إرسال البريد من 172.18.124.114 إلى 99.99.99.2:

```
Translation built for gaddr 99.99.99.99 :305002
                    to laddr 172.18.124.114
        Auth start for user '???' from :109001
      to 99.99.99.30/23 172.18.124.114/32860
Authen Session Start: user 'cse', Sid 14 :109011
 'Authentication succeeded for user 'cse :109005
from 172.18.124.114/32860 to    99.99.99.30/23
                          on interface inside
Built outbound TCP connection 22 for faddr :302001
        gaddr 99.99.99.99/32861 99.99.99.2/25
        (laddr 172.18.124.114/32861 (cse

                          pixfirewall#show uauth
    Current    Most Seen
        Authenticated Users       1          2
        Authen In Progress        0          1
 user 'cse' at 172.18.124.114, authenticated
            absolute   timeout: 0:05:00
            inactivity timeout: 0:00:00
```

تسجيل الخروج من برنامج Telnet الظاهري

عندما يقوم المستخدمون Telnet إلى عنوان Telnet الظاهري، فإن الأمر **show uauth** يظهر الوقت الذي تكون فيه الفتحة مفتوحة. إذا كان المستخدمون يرغبون في منع حركة المرور من المرور بعد انتهاء جلسات عملهم (عندما يبقى الوقت في الوحدة)، فإنهم يحتاجون إلى برنامج Telnet إلى عنوان Telnet IP الظاهري مرة أخرى. يتم الآن تبديل جلسة العمل. وهذا ما يوضحه هذا المثال.

المصادقة الأولى

```
                '???' Auth start for user :109001
from 172.18.124.114/32862 to 99.99.99.30/23
Authen Session Start: user 'cse', Sid 15 :109011
      Authentication succeeded for user :109005
          cse' from 172.18.124.114/32862 to'
          on interface inside 99.99.99.30/23
```

بعد المصادقة الأولى

```
                          pixfirewall#show uauth
    Current    Most Seen
        Authenticated Users       1          2
        Authen In Progress        0          1
 user 'cse' at 172.18.124.114, authenticated
            absolute   timeout: 0:05:00
            inactivity timeout: 0:00:00
```

المصادقة الثانية

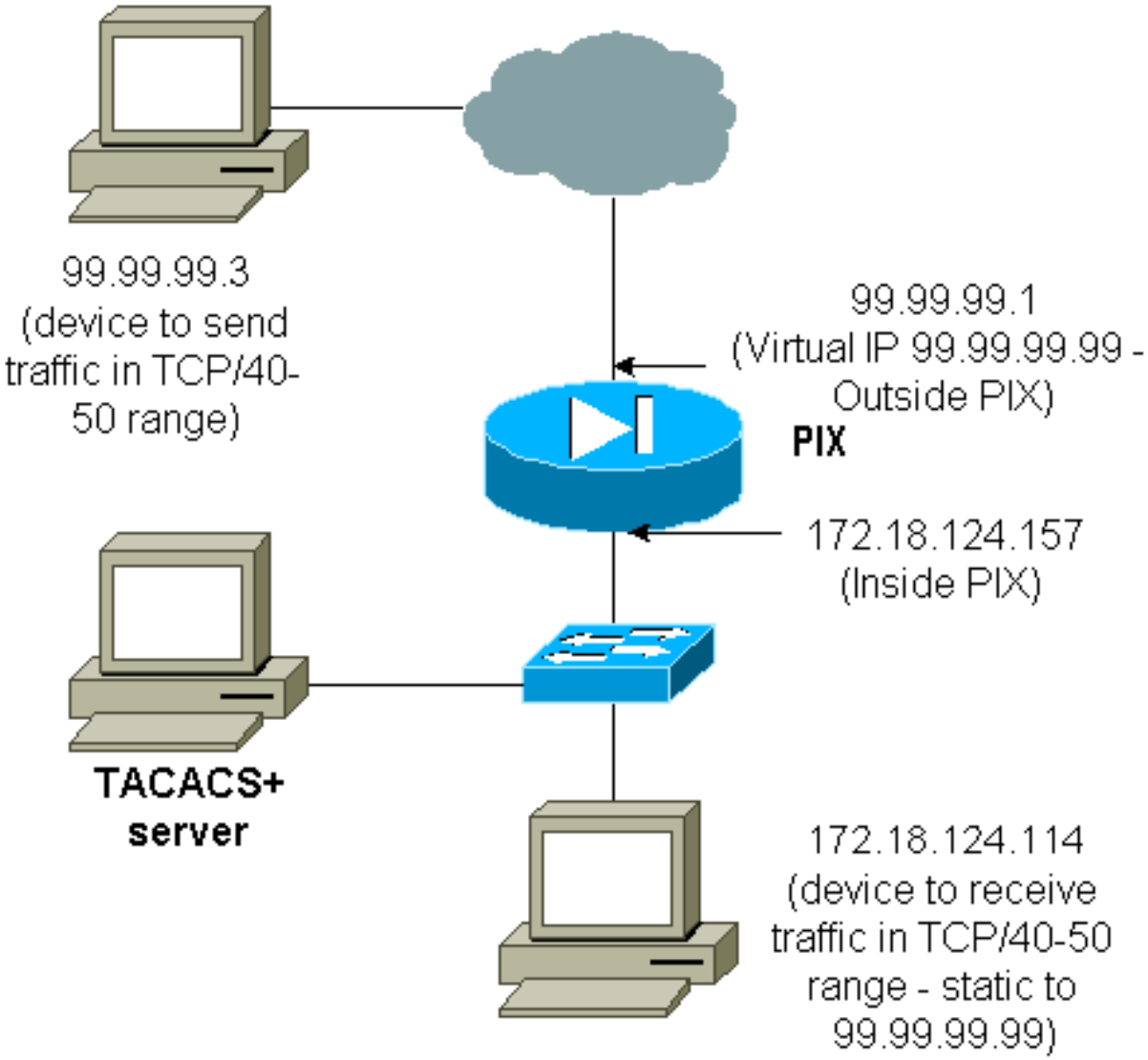
```
'pixfirewall# 109001: Auth start for user 'cse
from 172.18.124.114/32863 to    99.99.99.30/23
  'Authentication succeeded for user 'cse :109005
from 172.18.124.114/32863 to    99.99.99.30/23
                              on interface inside
```

بعد المصادقة الثانية

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

تفويض المنفذ

الرسم التخطيطي للشبكة



يسمح بالتفويض لنطاقات المنافذ. إذا تم تكوين برنامج Telnet الظاهري على برنامج PIX، وتم تكوين التفويض لنطاق من المنافذ، فإن المستخدم يقوم بفتح الثغرة باستخدام برنامج Telnet الظاهري. بعد ذلك، إذا كان تفويض نطاق منفذ قيد التشغيل وكانت حركة المرور في هذا النطاق تصل إلى PIX، فإن PIX يرسل الأمر إلى خادم TACACS+ للتفويض. يوضح هذا المثال التخويل الوارد على نطاق منفذ.

```
aaa authentication include any outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
                                                                AuthInbound
aaa authorization include tcp/40-50 outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
                                                                AuthInbound
OR the new 5.2 feature allows these three statements !--- to perform the same function as ---!
.the previous two statements. !--- Note: The old and new verbiage should not be mixed

                                                access-list 116 permit tcp any any range 40 50
                                              aaa authentication match 116 outside AuthInbound
                                               aaa authorization match 116 outside AuthInbound
                                                                                              !
                                    plus ! static (inside,outside) 99.99.99.99 172.18.124.114 ---!
                                                                  netmask 255.255.255.255 0 0
                                                                 conduit permit tcp any any
                                                                 virtual telnet 99.99.99.99
```

مثال تكوين خادم TACACS+ (مجاني):

```
                                                                                  } user = cse
                                                                "login = cleartext "numeric
                                                                        } cmd = tcp/40-50
                                                                permit 172.18.124.114
                                                                                        {
                                                                                        {
```

يجب على المستخدم إستخدام Telnet أولا إلى عنوان IP الظاهري 99.99.99.99. بعد المصادقة، عندما يحاول المستخدم دفع حركة مرور TCP في نطاق المنفذ 40-50 عبر PIX إلى 99.99.99.99 (172.18.124.114)، يتم إرسال cmd=tcp/40-50 إلى خادم TACACS+ مع cmd-arg=172.18.124.114 كما هو موضح هنا:

```
Auth start for user '???' from 99.99.99.3/11075 :109001
                                    to 172.18.124.114/23
        Authen Session Start: user 'cse', Sid 13 :109011
         'Authentication succeeded for user 'cse :109005
          from 172.18.124.114/23 to 99.99.99.3/11075
                                    on interface outside
Auth start for user 'cse' from 99.99.99.3/11077 :109001
                                    to 172.18.124.114/49
        Authen Session Start: user 'cse', Sid 13 :109011
          'Authorization permitted for user 'cse :109007
          from 99.99.99.3/11077 to 172.18.124.114/49
                                    on interface outside
```

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

بعد التأكد من عمل برنامج Telnet الظاهري للسماح لحركة مرور TCP/40-50 إلى المضيف داخل الشبكة، قم بإضافة المحاسبة لحركة المرور هذه باستخدام هذه الأوامر.

```
aaa accounting include any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
OR the new 5.2 feature allows these !--- two statements to replace the previous statement. ---!
.!--- Note: Do not mix the old and new verbiage

aaa accounting match 116 outside AuthInbound
access-list 116 permit ip any any
```

مثال على سجلات محاسبة TACACS+

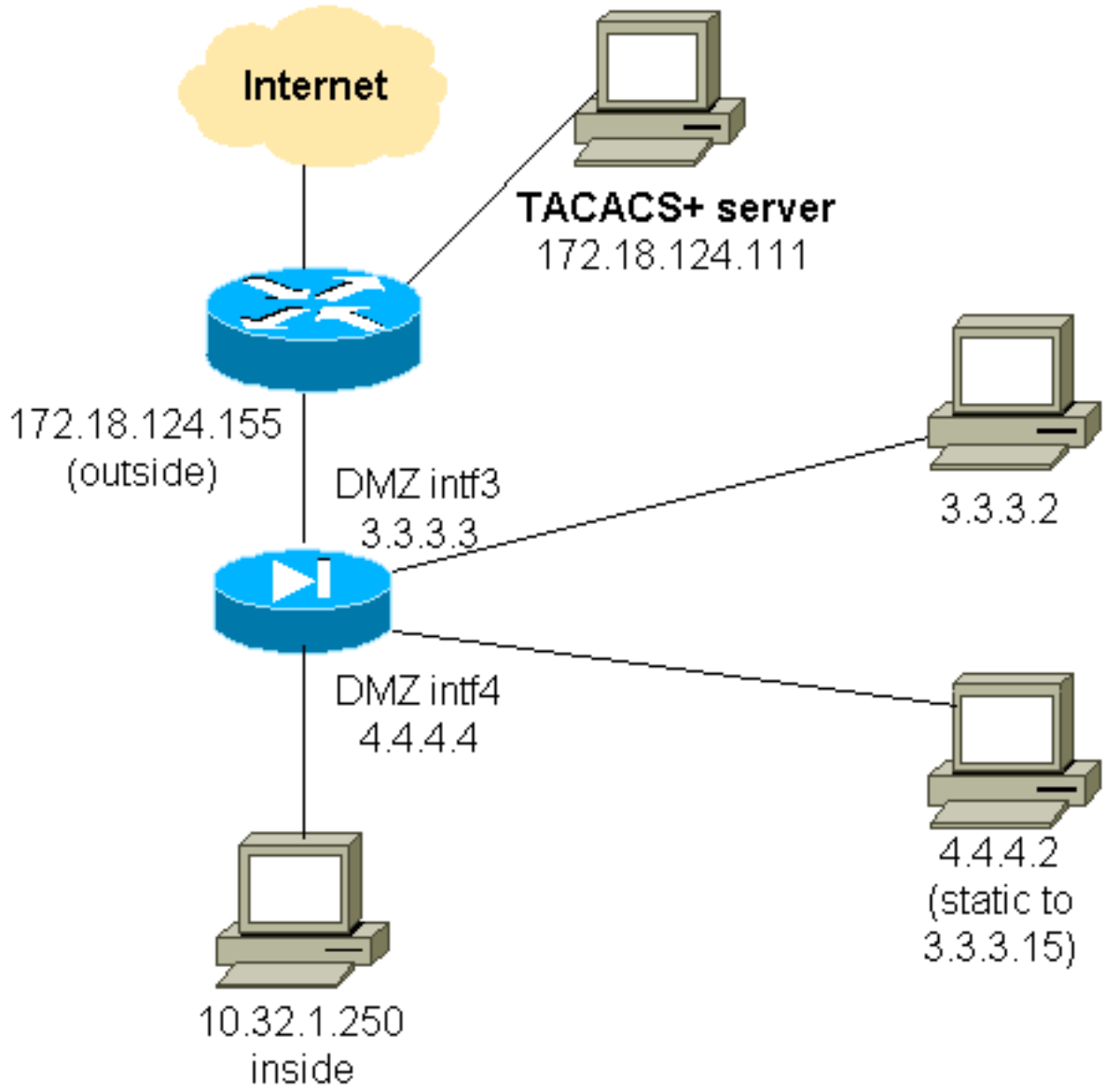
```
Thu Aug 24 08:06:09 2000 172.18.124.157 cse PIX 99.99.99.3
start task_id=0x17 foreign_ip=99.99.99.3 local_ip=172.18.124.114
                                                    cmd=tcp/40-50
Thu Aug 24 08:06:17 2000 172.18.124.157 cse PIX 99.99.99.3
stop task_id=0x17 foreign_ip=99.99.99.3 local_ip=172.18.124.114
    cmd=tcp/40-50 elapsed_time=8 bytes_in=80 bytes_out=101
```

المصادقة على DMZ

لمصادقة المستخدمين الذين ينتقلون من واجهة DMZ إلى أخرى، أخبر PIX بمصادقة حركة مرور البيانات للواجهات المسماة. على ال PIX، الترتيب مثل هذا:

```
                                                least secure
                                PIX outside (security0) = 172.18.124.155
                          pix/intf3 (DMZ - security15) = 3.3.3.3 & device 3.3.3.2
(pix/intf4 (DMZ - security20) = 4.4.4.4 & device 4.4.4.2 (static to 3.3.3.15
                                PIX inside (security100) = 10.32.1.250
                                                  most secure
```

الرسم التخطيطي للشبكة



تكوين PIX الجزئي

قم بمصادقة حركة مرور بيانات Telnet بين PIX/INTF3 و PIX/INTF4، كما هو موضح هنا.

تكوين PIX الجزئي

```
                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)
                        interface ethernet0 auto
                        interface ethernet1 auto
              (interface ethernet2 auto shutdown)
                        interface ethernet3 auto
                        interface ethernet4 auto
              (interface ethernet5 auto shutdown)
    ip address outside 172.18.124.155 255.255.255.0
        ip address inside 10.32.1.250 255.255.255.0
         ip address pix/intf3 3.3.3.3 255.255.255.0
         ip address pix/intf4 4.4.4.4 255.255.255.0
static (pix/intf4,pix/intf3) 3.3.3.15 4.4.4.2 netmask
                                  255.255.255.255 0 0
      conduit permit tcp host 3.3.3.15 host 3.3.3.2
                  +aaa-server xway protocol tacacs
aaa-server xway (outside) host 172.18.124.111 timeout
                                                    5
  aaa authentication include telnet pix/intf4 4.4.4.0
                                  255.255.255.0 3.3.3.0
            xway 255.255.255.0 3.3.3.0 255.255.255.0
  aaa authentication include telnet pix/intf3 4.4.4.0
                                  255.255.255.0 3.3.3.0
            xway 255.255.255.0 3.3.3.0 255.255.255.0
OR the new 5.2 feature allows these four statements ---!
 !--- to replace the previous two statements. !--- Note:
                    .Do not mix the old and new verbiage

    access-list 103 permit tcp 3.3.3.0 255.255.255.0
                        4.4.4.0 255.255.255.0 eq telnet
    access-list 104 permit tcp 4.4.4.0 255.255.255.0
                        3.3.3.0 255.255.255.0 eq telnet
        aaa authentication match 103 pix/intf3 xway
        aaa authentication match 104 pix/intf4 xway
```

معلومات للتجميع إذا قمت بفتح حالة مركز المساعدة الفنية

إذا كنت لا تزال بحاجة إلى المساعدة بعد اتباع خطوات أستكشاف الأخطاء وإصلاحها أعلاه وتريد فتح حالة باستخدام برنامج Cisco TAC، فتأكد من تضمين هذه المعلومات لاستكشاف أخطاء جدار حماية PIX وإصلاحها.

- وصف المشكلة وتفاصيل المخطط ذات الصلة
- أستكشاف الأخطاء وإصلاحها قبل فتح الحالة
- مخرجات من الأمر **show tech-support**
- الإنتاج من **العرض سجل** أمر بعد أن يركض أنت مع ال **logging buffered debuing** أمر، أو وحدة طرفية للتحكم على قبض أن يوضح المشكلة (إن يتوفر)

قم بإرفاق البيانات المجمعة بالحالة الخاصة بك بتنسيق نص عادي غير مضغوط (.txt). قم بإرفاق المعلومات بالحالة الخاصة بك عن

طريق تحميلها بمساعدة أداة استعلام الحالة (للعملاء المسجلين فقط). إذا لم تكن قادرا على الوصول إلى أداة استعلام الحالة، فعليك إرسال المعلومات في مرفق بريد إلكتروني إلى موقع attach@cisco.com\مع وجود رقم الحالة الخاص بك في سطر موضوع رسالتك.

معلومات ذات صلة

- برنامج جدار حماية Cisco PIX
- مراجع أوامر جدار حماية PIX الآمن من Cisco
- الإعلامات الميدانية لمنتج الأمان (بما في ذلك PIX)
- طلبات التعليقات (RFCs)
- خادم التحكم في الوصول الآمن من Cisco لأنظمة التشغيل Windows
- خادم التحكم في الوصول الآمن من Cisco ل UNIX
- نظام مراقبة الدخول إلى وحدة تحكم الوصول إلى المحطة الطرفية (TACACS+)
- خدمة مصادقة طلب اتصال المستخدم البعيد (RADIUS)
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).