# كيفية إجراء المصادقة والتمكين على جدار الحماية PIX الآمن من Cisco (من 5.2 إلى 6.2)

## المحتويات



## المقدمة

يوضح هذا المستند كيفية إنشاء وصول مصدق بواسطة AAA إلى جدار حماية PIX يشغل برنامج PIX الإصدار 5.2 من خلال 6.2، كما يوفر معلومات حول تمكين المصادقة وsyslogging واكتساب الوصول عند تعطل خادم AAA. في المعيار PIX 5.3 والإصدارات الأحدث، يتمثل تغيير المصادقة والتفويض والمحاسبة (AAA) عبر الإصدارات السابقة من الرمز في أن منافذ RADIUS قابلة للتكوين.

في إصدارات برنامج PIX 5.2 والإصدارات الأحدث، يمكنك إنشاء وصول مصدق بواسطة AAA إلى PIX بخمس طرق

مختلفة:

- مصادقة Telnet - الداخل
- مصادقة منفذ وحدة التحكم
- Cisco Secure VPN Client 1.1 - خارج
- شبكة VPN 3000 مصدق عليها 2.5 - خارج
- القشرة الآمنة (SSH) التي تمت مصادقتها - داخل أو خارج

**ملاحظة:** يجب تمكين DES أو 3DES على PIX (قم بإصدار أمر **show version** للتحقق) للطرق الثلاث الأخيرة. في الإصدار 6.0 من برنامج PIX والإصدارات الأحدث، يمكن أيضا تحميل مدير أجهزة PIX (PDM) لتمكين إدارة واجهة المستخدم الرسومية (GUI). خارج نطاق PDM لهذا المستند.

لمزيد من المعلومات حول أمر المصادقة والتفويض ل PIX 6.2، ارجع إلى PIX 6.2: مثال تكوين أمر المصادقة والتفويض.

من أجل إنشاء وصول مصدق من قبل المصادقة والتفويض والمحاسبة (AAA) إلى جدار حماية PIX يشغل إصدارات برنامج PIX 6.3 والإصدارات الأحدث، ارجع إلى PIX/ASA: وكيل التوصيل للوصول إلى الشبكة باستخدام مثال تكوين خادم TACACS+ و RADIUS.

# المتطلبات الأساسية

## المتطلبات

قم بأداء هذه المهام قبل إضافة مصادقة AAA:

- أصدرت هذا أمر in order to أضفت كلمة ل ال PIX:**باسود دبليو<if_name> [<mask>] [<local_ip>**]يقوم PIX بتشفير كلمة المرور هذه تلقائيا لتكوين سلسلة مشفرة باستخدام الكلمة الأساسية **المشفرة**، كما هو الحال في هذا المثال:
  ```
  passwd OnTrBUG1Tp0edmkr encrypted
  ```
  لا تحتاج إلى إضافة الكلمة الأساسية **المشفرة**.
- تأكد من أنه يمكنك إستخدام Telnet من الشبكة الداخلية إلى الواجهة الداخلية ل PIX *دون* مصادقة AAA بعد إضافة هذه الجمل.
- قم دائما بفتح اتصال ب PIX أثناء إضافة عبارات المصادقة في حالة ضرورة نسخ الأوامر إحتياطيا.

في مصادقة AAA (بخلاف SSH حيث يعتمد التسلسل على العميل)، يرى المستخدم طلبا لكلمة مرور PIX (كما هو الحال في *كلمة المرور* <any>)، ثم طلبا لاسم مستخدم وكلمة مرور RADIUS أو TACACS.

**ملاحظة:** لا يمكنك إستخدام Telnet إلى الواجهة الخارجية ل PIX. يمكن إستخدام SSH على الواجهة الخارجية إذا تم إتصاله من عميل SSH الخارجي.

## المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- برنامج PIX الإصدار 5.2 أو 5.3 أو 6.0 أو 6.1 أو 6.2
- Cisco Secure VPN Client 1.1
- Cisco VPN 3000 Client 2.5
- عميل شبكة VPN 3.0.x من Cisco (يلزم وجود رمز PIX 6.0)

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.

### منافذ RADIUS القابلة للتكوين (5.3 ومتأخر)

تستخدم بعض خوادم RADIUS منافذ RADIUS بخلاف 1646/1645 (عادة 1813/1812). في PIX 5.3، يمكن تغيير منافذ مصادقة RADIUS ومحاسبته إلى خلاف المنافذ الافتراضية 1646/1645 باستخدام الأوامر التالية:

**خادم AAA-radius-authport #**

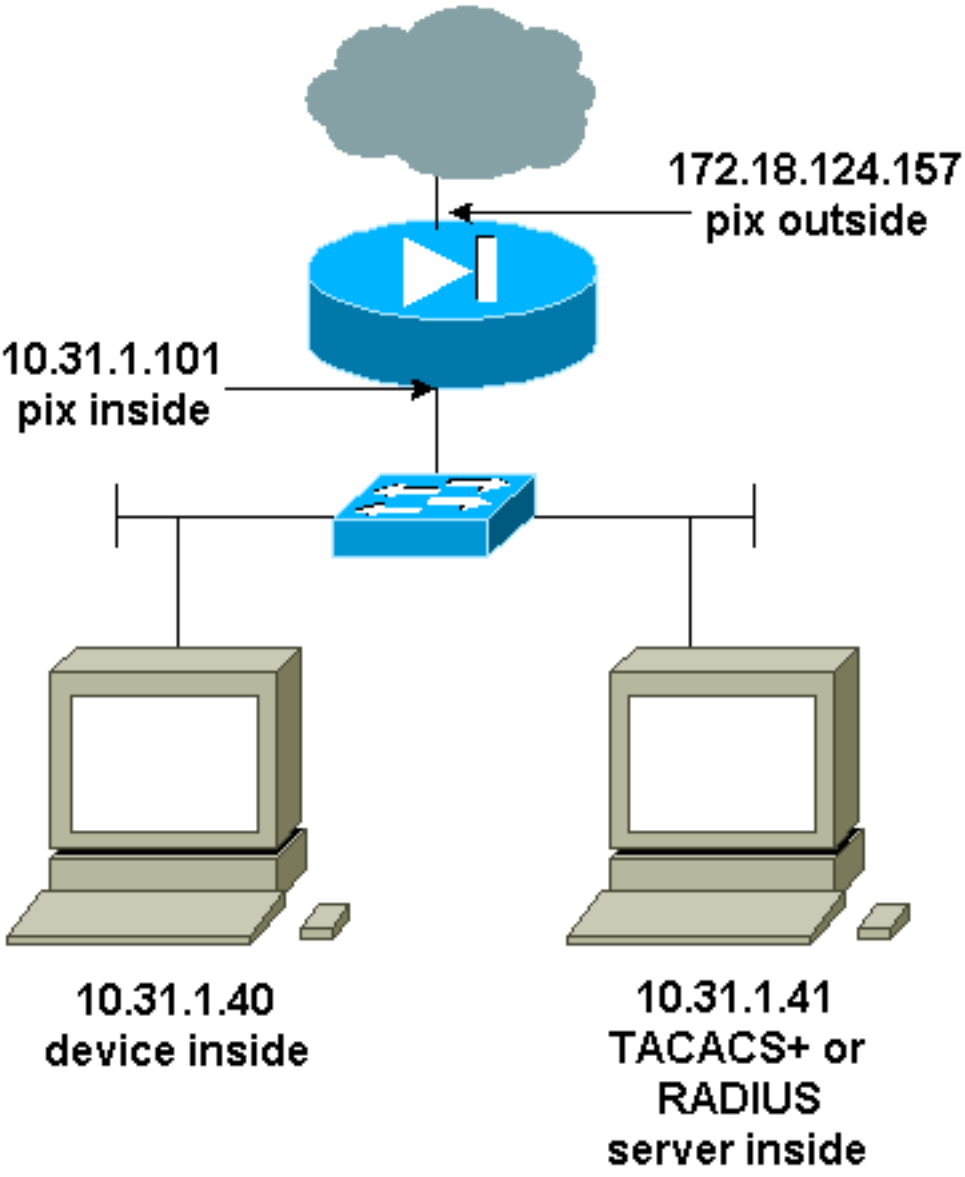
**منفذ AAA-server radius #**

## الاصطلاحات

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

# مصادقة Telnet - الداخل

## الرسم التخطيطي للشبكة




## الأوامر المضافة إلى تكوين PIX

إضافة هذه الأوامر إلى التكوين الخاص بك:

**بروتوكول مخطط خوادم TACACS +AAA**

**AAA-server topix مضيف 10.31.1.41 cisco مهلة 5**

**AAA مصادقة telnet وحدة تحكم موضوع**

يرى المستخدم طلبا لكلمة مرور PIX (كما في <any>)، ثم طلبا لاسم مستخدم وكلمة مرور RADIUS أو TACACS (المخزن على خادم TACACS 10.31.1.41 أو RADIUS).

## مصادقة منفذ وحدة التحكم

إضافة هذه الأوامر إلى التكوين الخاص بك:

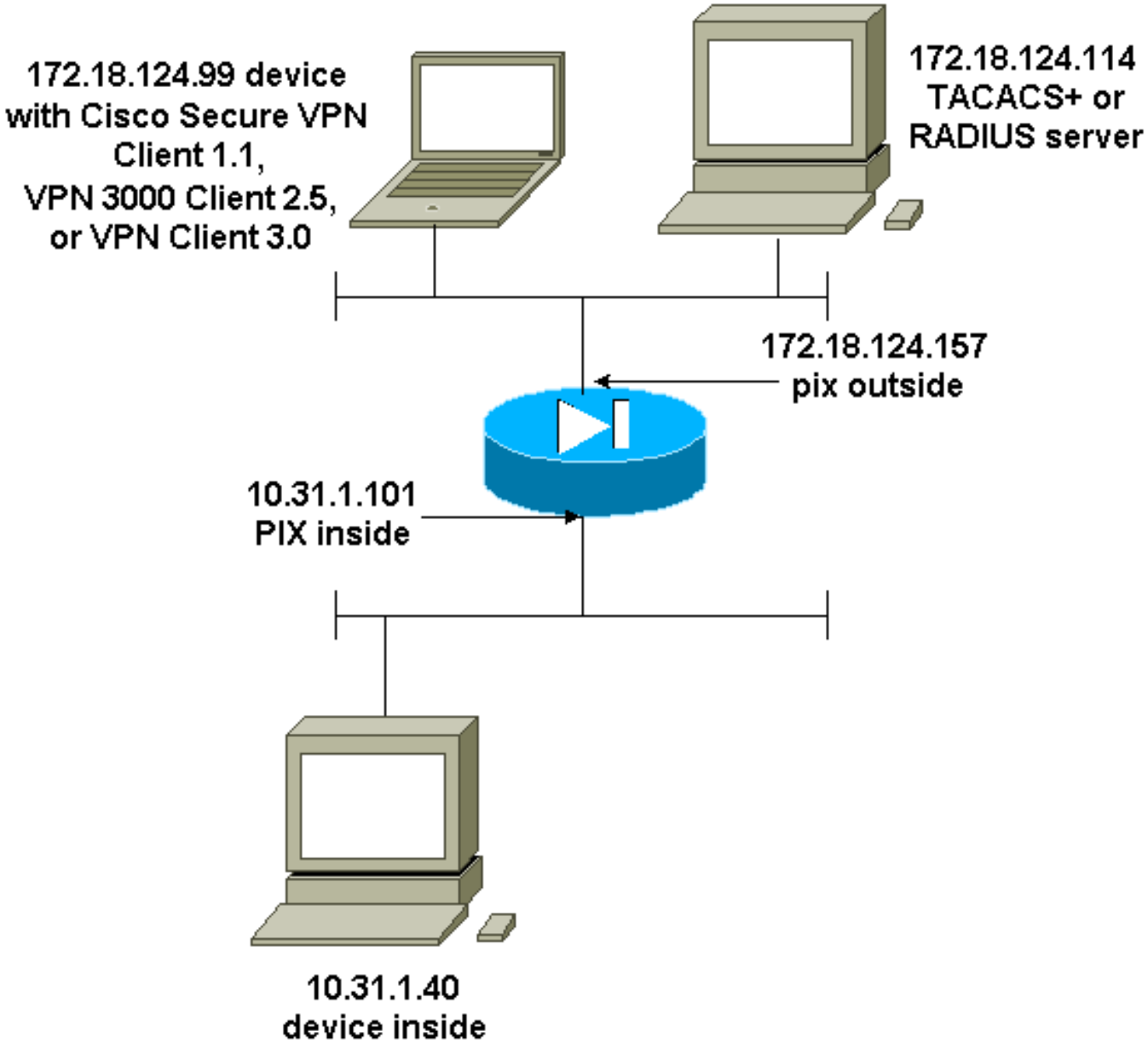
**بروتوكول مخطط خوادم TACACS +AAA**

**AAA-server topix مضيف 10.31.1.41 cisco مهلة 5**

**محور وحدة التحكم التسلسلية لمصادقة AAA**

يرى المستخدم طلبا لكلمة مرور PIX (كما في <any>)، ثم طلبا لاسم مستخدم/كلمة مرور RADIUS/TACACS (المخزن على خادم RADIUS أو TACACS 10.31.1.41).

**الرسم التخطيطي - عميل VPN 1.1 أو VPN 3000 2.5 أو VPN Client 3.0 - خارج**




## خارج - Cisco Secure VPN Client 1.1

| Cisco Secure VPN Client 1.1 - خارجي - تكوين العميل |
| --- |
| Myconn 1-<br>My Identity<br>Connection security: Secure<br>Remote Party Identity and addressing<br>ID Type: IP address<br>Port all Protocol all<br>(Pre-shared key (matches that on PIX<br><br>Connect using secure tunnel<br>ID Type: IP address<br>172.18.124.157<br><br>(Authentication (Phase 1<br>Proposal 1<br><br>Authentication method: Preshared key<br>Encryp Alg: DES<br>Hash Alg: MD5 |

```
                                SA life:  Unspecified
                                      Key Group: DH 1

                                   (Key exchange (Phase 2
                                                 Proposal 1
                                    Encapsulation ESP
                                     Encrypt Alg: DES
                                        Hash Alg: MD5
                                        Encap: tunnel
                                  SA life: Unspecified
                                                no AH

                                          Other Connections 2-
                          Connection security: Non-secure
                                  Local Network Interface
                                               Name: Any
                                           IP Addr: Any
                                               Port: All
```

**Cisco Secure VPN Client 1.1 - خارجي - تكوين PIX جزئي**

```
ip address outside 172.18.124.157 255.255.255.0
aaa-server topix (outside) host 172.18.124.114 cisco
                                                timeout 5
aaa authentication telnet console topix
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap interface outside
isakmp enable outside
If you know the IP address of the outside client, ---!
use that !--- IP address in this statement. isakmp key
******** address 0.0.0.0 netmask 0.0.0.0 ! isakmp
identity address isakmp policy 10 authentication pre-
share isakmp policy 10 encryption des isakmp policy 10
hash md5 isakmp policy 10 group 1 isakmp policy 10
lifetime 86400 !--- We knew our client would access the
PIX from this !--- network. If you know the IP address
of the client, use that IP address !--- in this
statement. telnet 172.18.124.0 255.255.255.0 outside
```

# VPN 3000 2.5 أو VPN Client 3.0 المصدق - خارج

## VPN 3000 2.5 أو VPN Client 3.0 المصدق - خارج - تكوين العميل

1. حدد **متصل VPN > خصائص > تسمية الاتصال** من ال VPN 3000.
2. حدد **المصادقة > معلومات الوصول الجماعي**. يجب أن يتطابق اسم المجموعة وكلمة المرور مع ما يوجد على PIX في بيان **password <*group_name*> VPNgroup ***********.

عند النقر فوق **Connect**، يظهر نفق التشفير، ويقوم PIX بتعيين عنوان IP من تجمع الاختبار (يتم دعم وضع config- فقط مع عميل VPN 3000). بعد ذلك، يمكنك إحضار نافذة طرفية، ويتصل Telnet ب 172.18.124.157، ويمكن مصادقته عبر المصادقة والتفويض والمحاسبة (AAA). يسمح الأمر **telnet 192.168.1.x** على PIX بالاتصال من المستخدمين في المجموعة إلى الواجهة الخارجية.

**شبكة VPN 3000 مصدق عليها 2.5 - خارجي - تكوين PIX جزئي**

```
ip address outside 172.18.124.157 255.255.255.0
```

```
                ip address inside 10.31.1.101 255.255.255.0
    aaa-server topix (outside) host 172.18.124.114 cisco
                                                  timeout 5
                aaa authentication telnet console topix
                        sysopt connection permit-ipsec
                                    no sysopt route dnat
   crypto ipsec transform-set myset esp-des esp-md5-hmac
    crypto dynamic-map dynmap 10 set transform-set myset
         crypto map mymap 10 ipsec-isakmp dynamic dynmap
  crypto map mymap client configuration address initiate
   crypto map mymap client configuration address respond
                      crypto map mymap interface outside
                                  isakmp enable outside
                               isakmp identity address
  ISAKMP Policy for VPN 3000 Client runs 2.5 code. ---!!
 isakmp policy 10 authentication pre-share isakmp policy
10 encryption des isakmp policy 10 hash md5 !--- The 2.5
 client uses group 1 policy (PIX default). isakmp policy
 10 group 1 isakmp policy 10 lifetime 86400 !--- ISAKMP
  Policy for VPN Client runs 3.0 code. isakmp policy 20
authentication pre-share isakmp policy 20 encryption des
  isakmp policy 20 hash md5 !--- The 3.0 clients use D-H
 group 2 policy and require PIX 6.0 code. isakmp policy
  20 group 2 isakmp policy 20 lifetime 86400 ! vpngroup
   vpn3000 address-pool test vpngroup vpn3000 idle-time
         1800 vpngroup vpn3000 password ******** telnet
                      192.168.1.0 255.255.255.0 outside
```

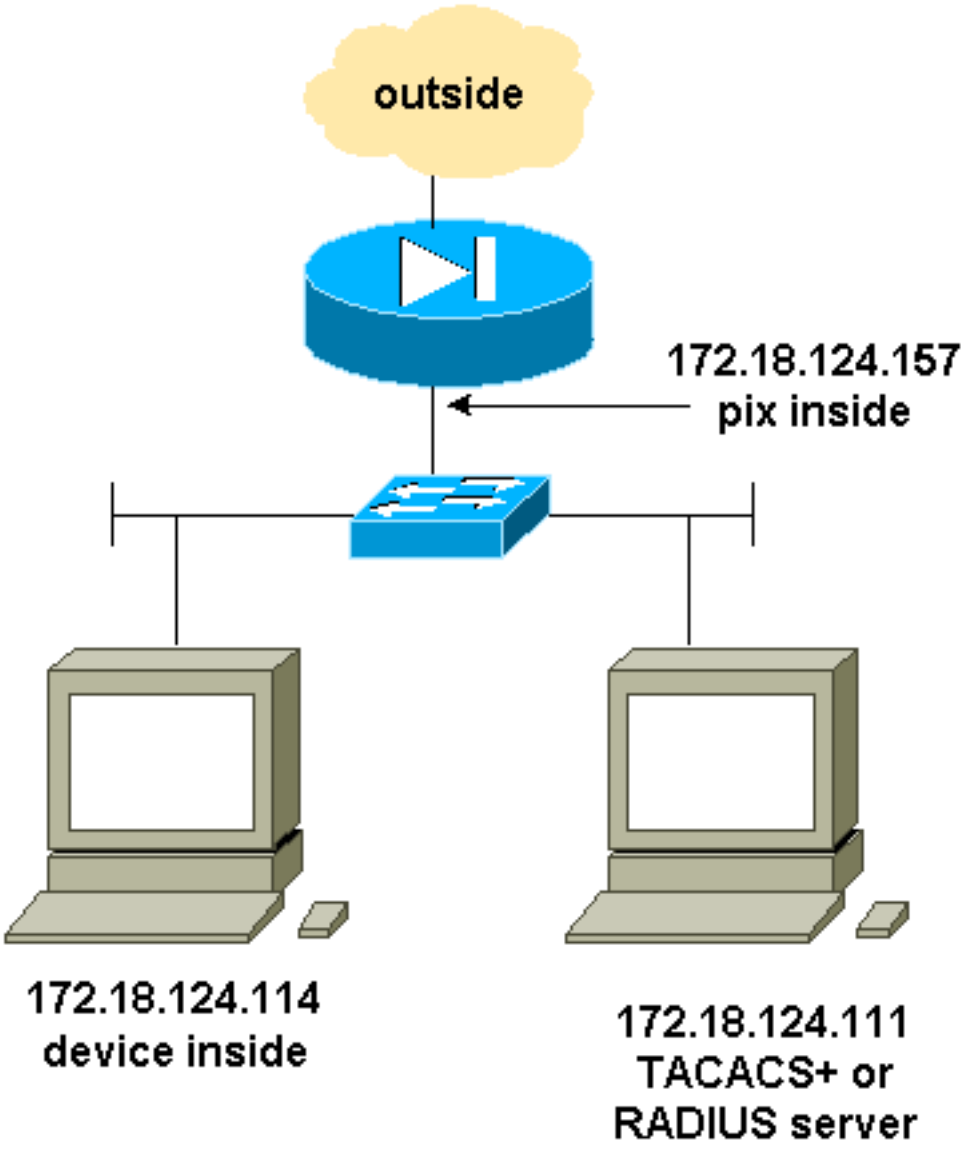
## SSH - داخل أو خارج

أضاف PIX 5.2 دعم طبقة الأمان (SSH) الإصدار 1. يعتمد بروتوكول SSH 1 على مسودة من IETF تم التوصل إليها في نوفمبر 1995. لا يكون الإصداران 1 و 2 من SSH متوافقين مع بعضهما البعض. ارجع إلى الأسئلة المتكررة حول طبقة الأمان (SSH) للحصول على مزيد من المعلومات حول SSH.

يعتبر PIX خادم SSH. يتم تشفير حركة مرور البيانات من عملاء SSH (أي المربعات التي تشغل SSH) إلى خادم SSH (ال PIX). يتم سرد بعض عملاء SSH الإصدار 1 في ملاحظات إصدار PIX 5.2. تم إجراء الاختبارات في مختبرنا باستخدام بروتوكول SSH 1.1 الآمن من المستوى الثاني (NT) والإصدار 1.2.26 لنظام التشغيل Solaris.

**ملاحظة:** بالنسبة للطراز PIX 7.x، ارجع إلى قسم السماح بوصول SSH في إدارة الوصول إلى النظام.

## الرسم التخطيطي للشبكة




## تكوين SSH الذي تمت مصادقة AAA

أكمل الخطوات التالية لتكوين SSH الذي تم مصادقة AAA:

1. تأكد من إمكانية إستخدام برنامج Telnet إلى PIX باستخدام المصادقة والتفويض والمحاسبة (AAA) مع عدم وجود بروتوكول SSH:

```
(+aaa-server AuthOutbound protocol radius (or tacacs
aaa authentication telnet console AuthOutbound
aaa-server AuthOutbound host 172.18.124.111 cisco
```

**ملاحظة:** عند تكوين بروتوكول SSH، لا يلزم الأمر **telnet 172.18.124.114 255.255.255.255** لأن الأمر **SSH 172.18.124.114 255.255.255.255** داخلي يتم إصداره على PIX. يتم تضمين كلا الأمرين لأغراض الاختبار.

2. إضافة SSH باستخدام هذه الأوامر:

```
hostname goss-d3-pix515b
domain-name rtp.cisco.com
ca gen rsa key 1024!--- Caution: The RSA key is not be saved without !--- the ca save all
   command. !--- The write mem command does not save it. !--- In addition, if the PIX has
  undergone a write erase !--- or has been replaced, then cutting and pasting !--- the old
configuration does not generate the key. !--- You must re-enter the ca gen rsa key command.
  !--- If there is a secondary PIX in a failover pair, the write standby !--- command does
  not copy the key from the primary to the secondary. !--- You must also generate and save
.the key on the secondary device
```

```
ssh 172.18.124.114 255.255.255.255 inside
ssh timeout 60
aaa authen ssh console AuthOutbound
logging trap debug
logging console debug
```

3. قم بإصدار الأمر **show ca mypubkey rsa** في وضع التكوين.

```
goss-d3-pix(config)#show ca mypubkey rsa
Key pair was generated at: 08:22:25 Aug 14 2000 %
Key name: goss-d3-pix.rtp.cisco.com
Usage: General Purpose Key
:Key Data
30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00ad4bcb
e9c174d5 0657a0f3 c94e4b6d 32ac8500 6b84e754 59e20df4 f28c257d 131af21d
4c0a8f4c e79d8b6d a3520faa 1a42d577 c6adfe51 9d96fa62 f3be07fb 01e082d7
133cecff bf24f653 bc690b11 ee222070 413c1920 d02321f8 4fc3c5f1 f0c6e077
81e93184 af55438b dcdcda34 c0a5f5ad 87c435ef
4d5ba51e 6d020301 0001 67170674
Key pair was generated at: 08:27:18 Aug 14 2000 %
Key name: goss-d3-pix.rtp.cisco.com.server
Usage: Encryption Key
:Key Data
307c300d 06092a86 4886f70d 01010105 00036b00 30680261 00d4f61b ec45843a
4ad9266d b125ee26 efc63cc4 e5e9cda4 9418ee53 6e4d16cf 3d0dc864 4d4830c8
fa7f110e 8a5761ed 4ca73ea7 5d405862 6f3150df 9eb0d11e 9c4d3563 95ff51ae
6711d60b 9a1415e4 19201d3f 03b455ea c1df9a41 b3a5a73f 4f020301 0001
```

4. جرب برنامج Telnet من محطة Solaris:

```
rtp-evergreen#./ssh -c 3des -l cisco -v 172.18.124.157
```

**ملاحظة:** "cisco" هو اسم المستخدم على خادم RADIUS/TACACS+ والوجهة 172.18.124.157.

## تكوين SSH المحلي (لا توجد مصادقة AAA)

كما يمكن إعداد اتصال SSH ب PIX باستخدام المصادقة المحلية وبدون خادم AAA. ومع ذلك، لا يوجد اسم مستخدم منفصل لكل مستخدم. اسم المستخدم هو دائما "pix".

أستخدم هذه الأوامر لتكوين SSH المحلي على PIX:

```
hostname goss-d3-pix515b
domain-name rtp.cisco.com
ca gen rsa key 1024!--- Caution: The RSA key is not saved without !--- the ca save all command.
!--- The write mem command does not save it. !--- In addition, if the PIX has undergone a write
erase !--- or has been replaced, then cutting and pasting !--- the old configuration does not
generate the key. !--- You must re-enter the ca gen rsa key command. !--- If there is a
secondary PIX in a failover pair, a write standby !--- command does not copy the key from the
.primary to the secondary. !--- You must also generate and save the key on the secondary device
ssh 172.18.124.114 255.255.255.255 inside
ssh timeout 60
passwd cisco123
```

بما أن اسم المستخدم الافتراضي في هذا الترتيب هو دائما "pix"، ثم الأمر للاتصال ب PIX (هذا كان 3DES من مربع Solaris) هو:

```
<ssh -c 3des -1 pix -v <ip_of_pix/.
```

## تصحيح أخطاء SSH

### تصحيح الأخطاء بدون الأمر debug ssh - 3DES و cipher-512

```
Authentication succeeded for user 'cse' from 0.0.0.0/0 :109005
                                to 172.18.124.114/0 on interface SSH
                            Authen Session Start: user 'cse', sid 0 :109011
  Permitted SSH session from 172.18.124.114 on interface inside :315002
                                                    "for user "cse
            SSH session from 172.18.124.114 on interface inside :315011
                                 for user "cse" terminated normally
```

### تصحيح الأخطاء باستخدام الأمر debug ssh - 3DES و cipher-512

```
                                                goss-d3-pix#debug ssh
                                                     SSH debugging on
                                        .goss-d3-pix# Device opened successfully
                                                    .SSH: host key initialised
                        SSH: SSH client: IP = '172.18.124.114' interface # = 1
                                         SSH1: starting SSH control process
                                SSH1: Exchanging versions - SSH-1.5-Cisco-1.25
                                       SSH1: client version is - SSH-1.5-1.2.26
              SSH1: declare what cipher(s) we support: 0x00 0x00 0x00 0x0c
                                     SSH1: SSH_SMSG_PUBLIC_KEY message sent
SSH1: SSH_CMSG_SESSION_KEY message received - msg type 0x03, length 112
                                      SSH1: client requests 3DES cipher: 3
                                     SSH1: keys exchanged and encryption on
                                SSH1: authentication request for userid cse
        SSH(cse): user authen method is 'use AAA', aaa server group ID = 3
                                ,SSH(cse): starting user authentication request
                                       and waiting for reply from AAA server
                                   SSH(cse): user 'cse' is authenticated
                                SSH(cse): user authentication request completed
                                 :SSH1: authentication successful for cse109005
          'SSH1: starting exec shellAuthentication succeeded for user 'cse
                    from 0.0.0.0/0 to 172.18.124.114/0 on interface SSH
  Permitted SSH session from 172.18.124.114 on interface inside :315002
                                                    "for user "cse
```

### cipher-1024 و debug - 3DES

```
                                        .goss-d3-pix# Device opened successfully
                                                    .SSH: host key initialised
                        SSH: SSH client: IP = '172.18.124.114' interface # = 1
                                         SSH1: starting SSH control process
                                SSH1: Exchanging versions - SSH-1.5-Cisco-1.25
                                       SSH1: client version is - SSH-1.5-1.2.26
              SSH1: declare what cipher(s) we support: 0x00 0x00 0x00 0x0c
                                     SSH1: SSH_SMSG_PUBLIC_KEY message sent
SSH1: SSH_CMSG_SESSION_KEY message received - MSG type 0x03, length 144
                                      SSH1: client requests 3DES cipher: 3
                                     SSH1: keys exchanged and encryption on
                                SSH1: authentication request for userid cse
        SSH(cse): user authen method is 'use AAA', aaa server group ID = 3
                                ,SSH(cse): starting user authentication request
                                       and waiting for reply from AAA server
                                   SSH(cse): user 'cse' is authenticated
                                SSH(cse): user authentication request completed
                                 :SSH1: authentication successful for cse109005
          'SSH1: starting exec shellAuthentication succeeded for user 'cse
                    from 0.0.0.0/0 to 172.18.124.114/0 on interface SSH
  Permitted SSH session from 172.18.124.114 on interface inside :315002
                                                    "for user "cse
```

### cipher-1024 و debug - DES

**ملاحظة:** هذا الإخراج من جهاز كمبيوتر مزود ببروتوكول SSH، وليس بنظام Solaris.

```
.Device opened successfully
.SSH: host key initialised
SSH: SSH client: IP = '172.18.124.99' interface # = 0
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-1.5-Cisco-1.25
SSH0: client version is - SSH-1.5-W1.0
SSH0: declare what cipher(s) we support: 0x00 0x00 0x00 0x04
SSH0: SSH_SMSG_PUBLIC_KEY message sent
SSH0: SSH_CMSG_SESSION_KEY message received - MSG type 0x03, length 144
SSH0: client requests DES cipher: 2
SSH0: keys exchanged and encryption on
SSH0: authentication request for userid ssh
SSH(ssh): user authen method is 'use AAA', aaa server group ID = 4
,SSH(ssh): starting user authentication request
and waiting for reply from AAA server
SSH(ssh): user 'ssh' is authenticated
SSH(ssh): user authentication request completed
SSH0: authentication successful for ssh109
SSH0: invalid request - 0x2500
'SSH0: starting exec shell5: Authentication succeeded for user 'ssh
from 0.0.0.0/0 to 172.18.124.99/0 on interface SSH
Authen Session Start: user 'ssh', sid 1 :109011
Permitted SSH session from 172.18.124.99 on interface outside :315002
"for user "ssh
```

### debug - 3DES و cipher-2048

**ملاحظة:** هذا الإخراج من جهاز كمبيوتر مزود ببروتوكول SSH، وليس بنظام Solaris.

```
.goss-d3-pix# Device opened successfully
.SSH: host key initialised
SSH: SSH client: IP = '161.44.17.151' interface # = 1
SSH1: starting SSH control process
SSH1: Exchanging versions - SSH-1.5-Cisco-1.25
SSH1: client version is - SSH-1.5-W1.0
SSH1: declare what cipher(s) we support: 0x00 0x00 0x00 0x0c
SSH1: SSH_SMSG_PUBLIC_KEY message sent
SSH1: SSH_CMSG_SESSION_KEY message received - MSG type 0x03, length 272
.SSH1: client requests 3DES cipher: 3
SSH1: keys exchanged and encryption on
SSH1: authentication request for userid cse
SSH(cse): user authen method is 'use AAA', aaa server group ID = 3
,SSH(cse): starting user authentication request
and waiting for reply from AAA server
SSH(cse): user 'cse' is authenticated
SSH(cse): user authentication request completed
SSH1: authentication successful for cse10900
:SSH1: invalid request - 0x255
'SSH1: starting exec shellAuthentication succeeded for user 'cse
from 0.0.0.0/0 to 161.44.17.151/0 on interface SSH
Authen Session Start: user 'cse', Sid 2 :109011
Permitted SSH session from 161.44.17.151 on interface inside :315002
"for user "cse
```

## ما الذي يمكن أن يحدث بشكل خاطئ

### تصحيح أخطاء Solaris - 2048-cipher و Solaris SSH

**ملاحظة:** تعذر على Solaris معالجة تشفير 2048.

```
;rtp-evergreen.cisco.com: Initializing random
  seed file /export/home/cse/.ssh/random_seed
.(RSA key has too many bits for RSAREF to handle (max 1024
```

### كلمة المرور غير صحيحة أو اسم المستخدم على خادم RADIUS/TACACS+

```
.Device opened successfully
.SSH: host key initialised
SSH: SSH client: IP = '161.44.17.151' interface # = 1
SSH1: starting SSH control process
SSH1: Exchanging versions - SSH-1.5-Cisco-1.25
SSH1: client version is - SSH-1.5-W1.0
SSH1: declare what cipher(s) we support: 0x00 0x00 0x00 0x0c
SSH1: SSH_SMSG_PUBLIC_KEY message sent
SSH1: SSH_CMSG_SESSION_KEY message received - MSG type 0x03, length 272
SSH1: client requests 3DES cipher: 3
SSH1: keys exchanged and encryption on
SSH1: authentication request for userid cse
SSH(cse): user authen method is 'use AAA', aaa server group ID = 3
,SSH(cse): starting user authentication request
  #and waiting for reply from AAA serverss-d3-pix
SSH(cse): user authentication for 'cse' failed
SSH(cse): user authentication request completed
SSH1: password authentication failed for cse
'Authentication failed for user 'cse :109006
from 0.0.0.0/0 to 161.44.17.151/0 on interface SSH
```

غير مسموح للمستخدم عبر الأمر:

### ssh 172.18.124.114 255.255.255.255 داخل

محاولات الاتصال:

315001: رفض جلسة SSH من 161.44.17.151 على الواجهة داخل

مع إزالة المفتاح من PIX (باستخدام الأمر **ca zero rsa**) أو عدم حفظه باستخدام الأمر **ca save all**

```
.Device opened successfully
,'SSH: unable to retrieve host public key for 'goss-d3-pix.rtp.cisco.com
.terminate SSH connection
"SSH-2145462416: Session disconnected by SSH server - error 0x00 "Internal error
.Fail to establish SSH session because PIX RSA host key retrieval failed :315004
"" SSH session from 0.0.0.0 on interface outside for user :315011
(disconnected by SSH server, reason: "Internal error" (0x00
```

خادم AAA معطل:

```
.SSH: host key initialised
SSH: SSH client: IP = '172.18.124.114' interface # = 0
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-1.5-Cisco-1.25
SSH0: client version is - SSH-1.5-1.2.26
SSH0: declare what cipher(s) we support: 0x00 0x00 0x00 0x0c
SSH0: SSH_SMSG_PUBLIC_KEY message sent302010: 0 in use, 0 most used
SSH0: SSH_CMSG_SESSION_KEY message received - MSG type 0x03, length 144
SSH0: client requests 3DES cipher: 3
```

```
                                    SSH0: keys exchanged and encryption on
                                SSH0: authentication request for userid cse
        SSH(cse): user authen method is 'use AAA', aaa server group ID = 3
                            ,SSH(cse): starting user authentication request
                               and waiting for reply from AAA server1090
                             SSH(cse): user authentication for 'cse' failed
                            SSH(cse): user authentication request completed
                              SSH0: password authentication failed for cse0
                                        SSH0: authentication failed for cse
  "SSH0: Session disconnected by SSH server - error 0x03 "status code: 0x03
                                Auth from 0.0.0.0/0 to 172.18.124.114/0 failed :2
                        server 172.18.124.111 failed) on interface outside)
                        Auth from 0.0.0.0/0 to 172.18.124.114/0 failed :109002
                        server 172.18.124.111 failed) on interface outside)
                        Auth from 0.0.0.0/0 to 172.18.124.114/0 failed :109002
                        server 172.18.124.111 failed) on interface outside)
                  Authentication failed for user 'cse' from 0.0.0.0/0 :109006
                                      to 172.18.124.114/0 on interface SSH
           (SSH login session failed from 172.18.124.114 (1 attempts :315003
                                       "on interface outside by user "cse
"SSH session from 172.18.124.114 on interface outside for user "cse :315011
           (disconnected by SSH server, reason: "status code: 0x03" (0x03
          Authen Session End: user 'cse', Sid 0, elapsed 352 seconds :109012
```

تم إعداد العميل ل 3DES ولكن يوجد مفتاح DES فقط في PIX:

**ملاحظة:** لم يكن Solaris يدعم DES.

```
                                    .GOSS-PIX# Device opened successfully
                                                SSH: host key initialised
                                        .SSH: license supports DES: 1
                    SSH: SSH client: IP = '172.18.124.114' interface # = 0
                                        SSH0: starting SSH control process
                                SSH0: Exchanging versions - SSH-1.5-Cisco-1.25
                                      SSH0: client version is - SSH-1.5-1.2.26
                SSH0: declare what cipher(s) we support: 0x00 0x00 0x00 0x04
                                      SSH0: SSH_SMSG_PUBLIC_KEY message sent
  "SSH0: Session disconnected by SSH server - error 0x03 "status code: 0x03
   "" SSH session from 172.18.124.114 on interface outside for user :315011
           (disconnected by SSH server, reason: "status code: 0x03" (0x03
```

وعلى واجهة سطر الأوامر (CLI) لنظام Solaris:

```
.Selected cipher type 3DES not supported by server
```

## كيفية إزالة مفتاح RSA من PIX

**ca zero rsa**

## كيفية حفظ مفتاح RSA في PIX

**إمكانية حفظ الكل**

## كيفية السماح ل SSH من خارج عميل SSH

**SSH خارج_*255.255.255.255* IP خارج**

## تمكين المصادقة

باستخدام الأمر:

**مصادقة AAA تمكن مخطط وحدة التحكم**

(حيث *topix* هو قائمة الخوادم الخاصة بنا)، تتم مطالبة المستخدم باسم مستخدم وكلمة مرور يتم إرسالها إلى خادم TACACS أو RADIUS. بما أن حزمة المصادقة للتمكين هي نفسها حزمة المصادقة لتسجيل الدخول، إذا يمكن للمستخدم تسجيل الدخول إلى PIX باستخدام TACACS أو RADIUS، فيمكنه التمكين من خلال TACACS أو RADIUS باستخدام نفس اسم المستخدم/كلمة المرور.

يتوفر المزيد من المعلومات حول هذه المشاكل في معرف تصحيح الأخطاء من Cisco CSCdm47044 (العملاء المسجلون فقط).

## معلومات SyllLog

بينما تكون محاسبة AAA صالحة فقط للاتصالات من خلال PIX، وليس إلى PIX، وفي حالة إعداد syslog، يتم إرسال المعلومات حول ما قام به المستخدم المصدق عليه إلى خادم syslog (وإلى خادم إدارة الشبكة، إذا تم تكوينه، من خلال قاعدة معلومات الإدارة (MIB) syslog).

إن setup syslog يكون، بعد ذلك رسالة مثل هذا يعرض في ال syslog نادل:

*مستوى إعلام ملائمة التسجيل:*

```
Console Login from pixuser at console :111006
Begin configuration: 10.31.1.40 reading from terminal :111007
.User 'pixuser' executed the 'conf' command :111008
.User 'pixuser' executed the 'hostname' command :111008
```

*مستوى معلومات ملائمة التسجيل (والذي يتضمن مستوى الإعلام):*

307002: جلسة تسجيل الدخول المسموح بها إلى Telnet من 10.31.1.40

## اكتساب الوصول عند تعطل خادم AAA

إن ال aaa نادل يكون معطل، أنت يستطيع دخلت ال telnet كلمة منفذ ال PIX مبدئيا، بعد **PIX** ل ال username، وبعد ذلك ال enable كلمة (**كلمة enable** مهما ) ل الكلمة. 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، تحتاج إلى قرص إسترداد كلمة المرور لإعادة ضبط كلمة المرور.

## 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 Cisco TAC، فتأكد من تضمين المعلومات التالية.** |
| --- |
| • وصف المشكلة وتفاصيل المخطط ذات الصلة<br>• تم إجراء أستكشاف الأخطاء وإصلاحها قبل فتح الحالة<br>• مخرجات من الأمر **show tech-support**<br>• الإخراج من الأمر **show log** بعد التشغيل باستخدام الأمر |

logging buffered debugging، أو التقاط وحدة التحكم التي توضح المشكلة (إذا كانت متاحة)
الرجاء إرفاق البيانات المجمعة بالحالة الخاصة بك بتنسيق نص عادي غير مضغوط (.txt). يمكنك إرفاق المعلومات بالحالة الخاصة بك عن طريق تحميلها باستخدام أداة استعلام الحالة (للعملاء المسجلين فقط). إذا تعذر عليك الوصول إلى "أداة استعلام الحالة"، فيمكنك إرسال المعلومات في مرفق بريد إلكتروني إلى موقع attach@cisco.com مع وجود رقم الحالة الخاص بك في سطر موضوع رسالتك.

## معلومات ذات صلة

- مراجع أوامر جدار حماية PIX الآمن من Cisco
- TACACS RADIUS PIX+

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