Authentifizierungs- und Aktivierungsfunktionen für die Cisco Secure PIX Firewall (5.2 bis 6.2)

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie AAA-authentifizierten Zugriff auf eine PIX-Firewall erstellen, die die PIX-Softwareversion 5.2 bis 6.2 ausführt. Außerdem werden Informationen zur Aktivierungsauthentifizierung, Syslogging und Zugriffsberechtigungen bereitgestellt, wenn der AAA-Server ausfällt. In PIX 5.3 und höher wird die AAA-Änderung (Authentication, Authorization, Accounting) gegenüber früheren Codeversionen durch die Möglichkeit zur Konfiguration der RADIUS-Ports ersetzt.

In PIX-Softwareversionen 5.2 und höher können Sie einen AAA-authentifizierten Zugriff auf das PIX auf fünf verschiedene Arten erstellen:

- Telnet-Authentifizierung - Innen
- Konsolenport-Authentifizierung
- Authentifizierter Cisco Secure VPN Client 1.1 - Außenbereiche
- Authentifiziertes VPN 300 2.5 - Außenbereiche
- Authentifizierte Secure Shell (SSH) - Inside oder Outside

Hinweis: DES oder 3DES müssen für die letzten drei Methoden auf dem PIX aktiviert sein (**show version**-Befehl zur Überprüfung). In der PIX Software 6.0 und höher kann der PIX Device Manager (PDM) auch geladen werden, um das GUI-Management zu aktivieren. PDM ist nicht Bestandteil dieses Dokuments.

Weitere Informationen zum Authentifizierungs- und Autorisierungsbefehl für PIX 6.2 finden Sie in PIX 6.2: Konfigurationsbeispiel für Authentifizierungs- und Autorisierungsbefehle.

Informationen zum Erstellen eines AAA-authentifizierten (Cut-Through-Proxy) Zugriffs auf eine PIX-Firewall, die die PIX-Softwareversionen 6.3 und höher ausführt, finden Sie unter PIX/ASA: Cut-Through-Proxy für Netzwerkzugriff mit TACACS+ und RADIUS-Server-Konfigurationsbeispiel.

Voraussetzungen

Anforderungen

Führen Sie diese Aufgaben aus, bevor Sie AAA-Authentifizierung hinzufügen:

- Geben Sie die folgenden Befehle ein, um ein Kennwort für das PIX hinzuzufügen:**Passwwtelnet <local_ip> [<mask>] [<if_name>]**Das PIX verschlüsselt dieses Kennwort automatisch, um eine verschlüsselte Zeichenfolge mit dem **verschlüsselten** Schlüsselwort zu bilden, wie in diesem Beispiel gezeigt:
  ```
  passwd OnTrBUG1Tp0edmkr encrypted
  ```
  Sie müssen das **verschlüsselte** Schlüsselwort nicht hinzufügen.
- Stellen Sie sicher, dass Sie Telnet vom internen Netzwerk zur internen Schnittstelle des PIX *ohne* AAA-Authentifizierung aktivieren können, nachdem Sie diese Anweisungen hinzugefügt haben.
- Stellen Sie immer eine Verbindung zum PIX her, während Sie Authentifizierungsanweisungen hinzufügen, falls ein Sichern der Befehle erforderlich ist.

Bei der AAA-Authentifizierung (außer SSH, bei der die Sequenz vom Client abhängig ist) erhält der Benutzer eine Anforderung für das PIX-Kennwort (wie in *passwd <any>*) und anschließend eine Anforderung für den RADIUS- oder TACACS-Benutzernamen und das -Kennwort.

Hinweis: Sie können kein Telnet zur externen Schnittstelle von PIX verwenden. SSH kann auf der externen Schnittstelle verwendet werden, wenn die Verbindung von einem externen SSH-Client aus erfolgt.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- PIX Software Version 5.2, 5.3, 6.0, 6.1 oder 6.2
- Cisco Secure VPN Client 1.1
- Cisco VPN 3000 Client 2.5
- Cisco VPN Client 3.0.x (PIX 6.0-Code erforderlich)

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurierbare RADIUS-Ports (5.3 und höher)

Einige RADIUS-Server verwenden andere RADIUS-Ports als 1645/1646 (in der Regel 1812/1813). In PIX 5.3 können die RADIUS-Authentifizierungs- und Accounting-Ports mithilfe der folgenden Befehle auf andere als die Standard-1645/1646 geändert werden:

aa-server radius-authport #

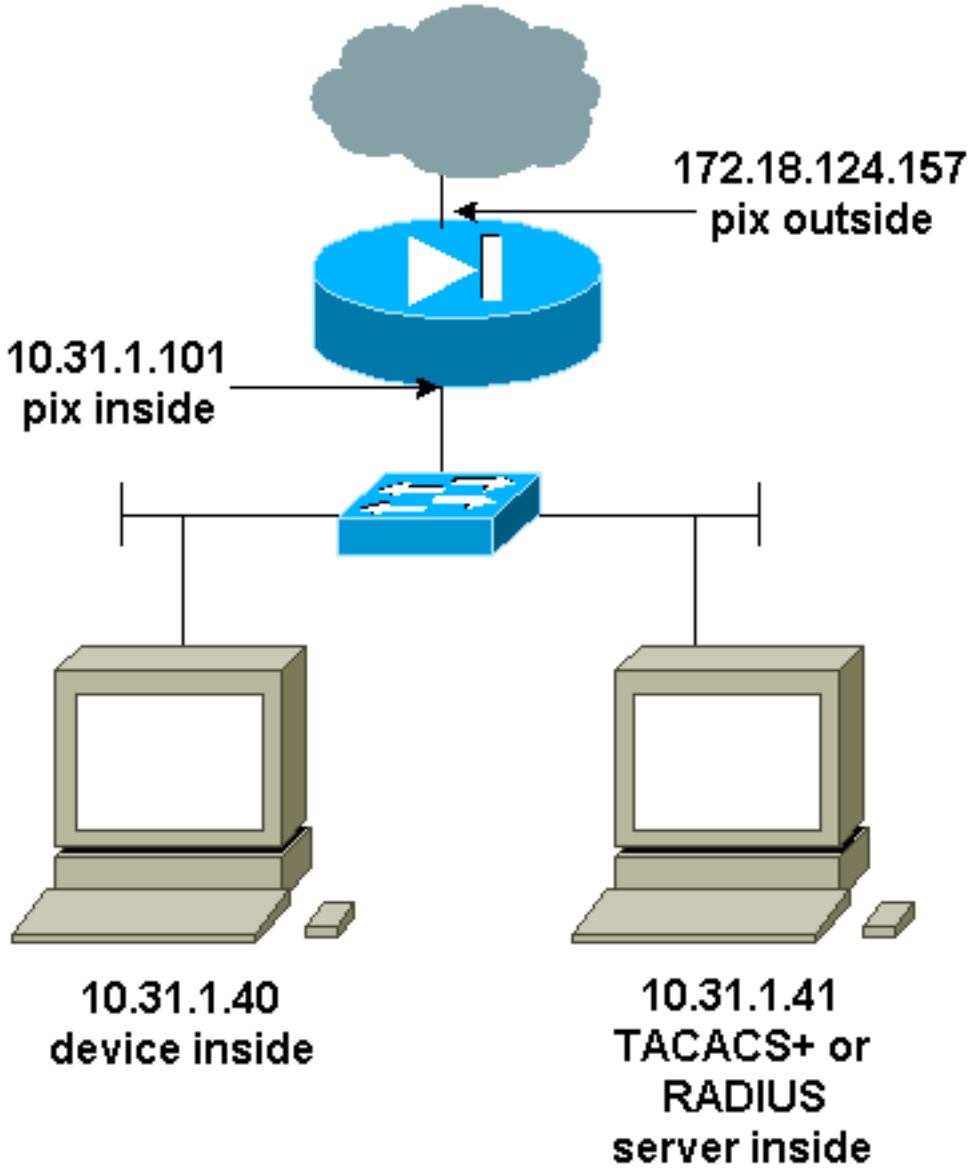
aa-server radius-acctport #

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Telnet-Authentifizierung - Innen

Netzwerkdiagramm



Zur PIX-Konfiguration hinzugefügte Befehle

Fügen Sie der Konfiguration diese Befehle hinzu:

aa-server topix protocol tacacs+

aa-server topix host 10,31,1,41 cisco timeout 5

aaa authentication Telnet-Konsolentopix

Der Benutzer erhält eine Anfrage für das PIX-Kennwort (wie in `passwd <any>`) und anschließend eine Anfrage für den RADIUS- oder TACACS-Benutzernamen und das -Kennwort (gespeichert auf dem 10.31.1.41-TACACS- oder RADIUS-Server).

Konsolenport-Authentifizierung

Fügen Sie der Konfiguration diese Befehle hinzu:

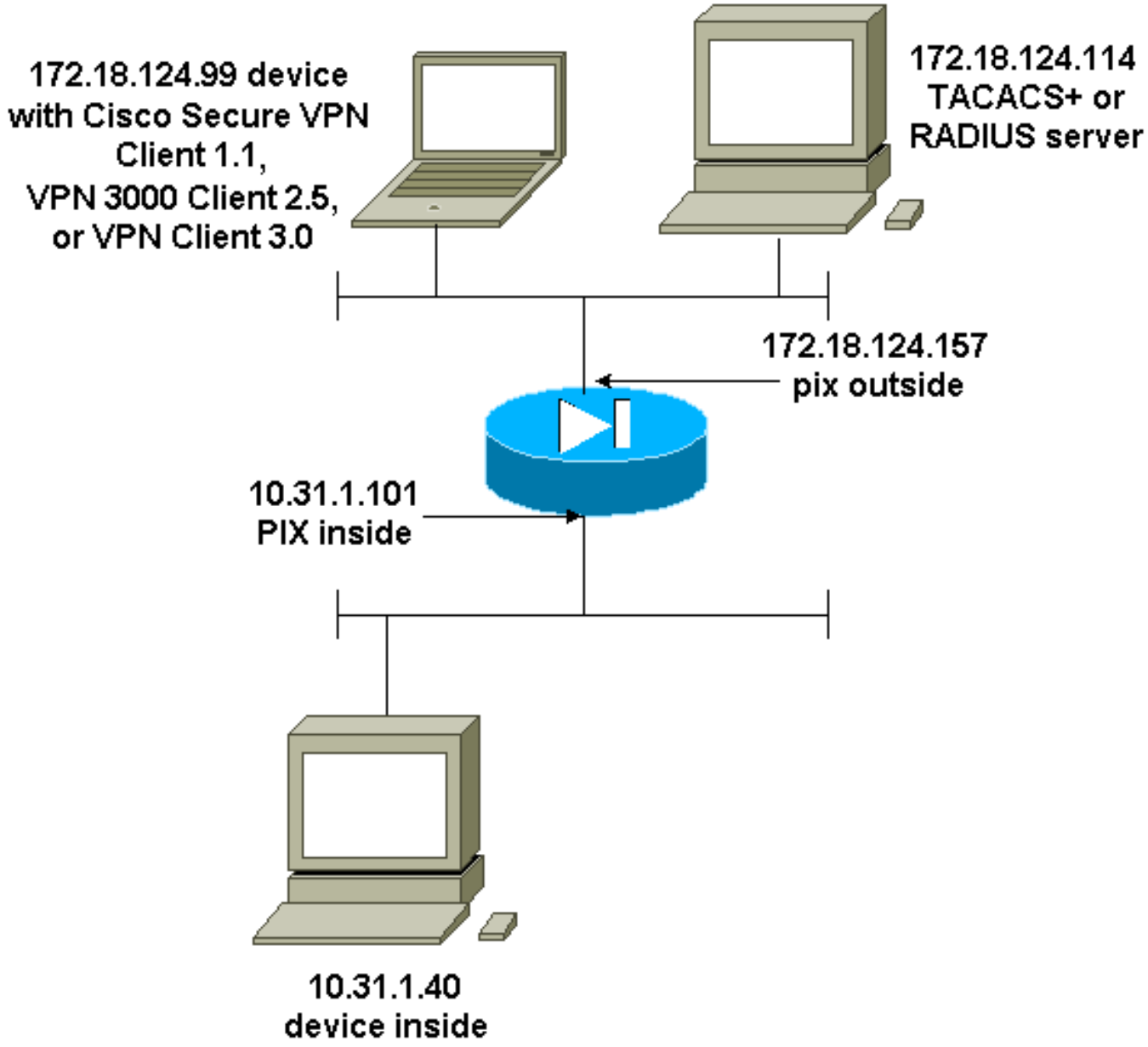
aa-server topix protocol tacacs+

aa-server topix host 10,31,1,41 cisco timeout 5

aaa authentication serielle Konsolentopix

Der Benutzer erhält eine Anfrage für das PIX-Kennwort (wie in `passwd <any>`) und anschließend eine Anfrage für den RADIUS/TACACS-Benutzernamen/das -Kennwort (gespeichert auf dem RADIUS- oder TACACS-Server 10.31.1.41).

Diagramm - VPN Client 1.1, VPN 300 2.5 oder VPN Client 3.0 - Außenbereiche



Authentifizierter Cisco Secure VPN Client 1.1 - Außenbereiche

Authentifizierter Cisco Secure VPN Client 1.1 - Außerhalb - Client-Konfiguration
1- Myconn My Identity Connection security: Secure Remote Party Identity and addressing ID Type: IP address

```
          Port all Protocol all
          Pre-shared key (matches that on PIX)

     Connect using secure tunnel
          ID Type: IP address
          172.18.124.157

     Authentication (Phase 1)
     Proposal 1

         Authentication method: Preshared key
         Encryp Alg: DES
         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

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

Authentifizierter Cisco Secure VPN Client 1.1 - Außenbereiche - Teilweise PIX-Konfiguration

```
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
```

Authentifiziertes VPN 300 2.5 oder VPN Client 3.0 - Außenbereiche

Authentifiziertes VPN 300 2.5 oder VPN Client 3.0 - Außenbereiche - Client-Konfiguration

1. Wählen Sie **VPN Dialer > Eigenschaften > Name der Verbindung** aus dem VPN 3000 aus.
2. Wählen Sie **Authentifizierung > Gruppenzugriffsinformationen aus**. Der Gruppenname und das Kennwort sollten mit dem auf dem PIX in der **vpngroup <*group_name*> password** übereinstimmen *********** Anweisung.

Wenn Sie auf **Verbinden** klicken, wird der Crypto-Tunnel aktiviert, und der PIX weist eine IP-Adresse aus dem Testpool zu (nur Modus-Konfiguration wird vom VPN 3000-Client unterstützt). Anschließend können Sie ein Terminalfenster, Telnet, auf 172.18.124.157 hochladen und AAA-authentifiziert werden. Der Befehl **telnet 192.168.1.x** auf dem PIX ermöglicht Verbindungen von Benutzern im Pool zur externen Schnittstelle.

Authentifiziertes VPN 300 2.5 - Außenbereiche - Teilweise PIX-Konfiguration

```
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
```

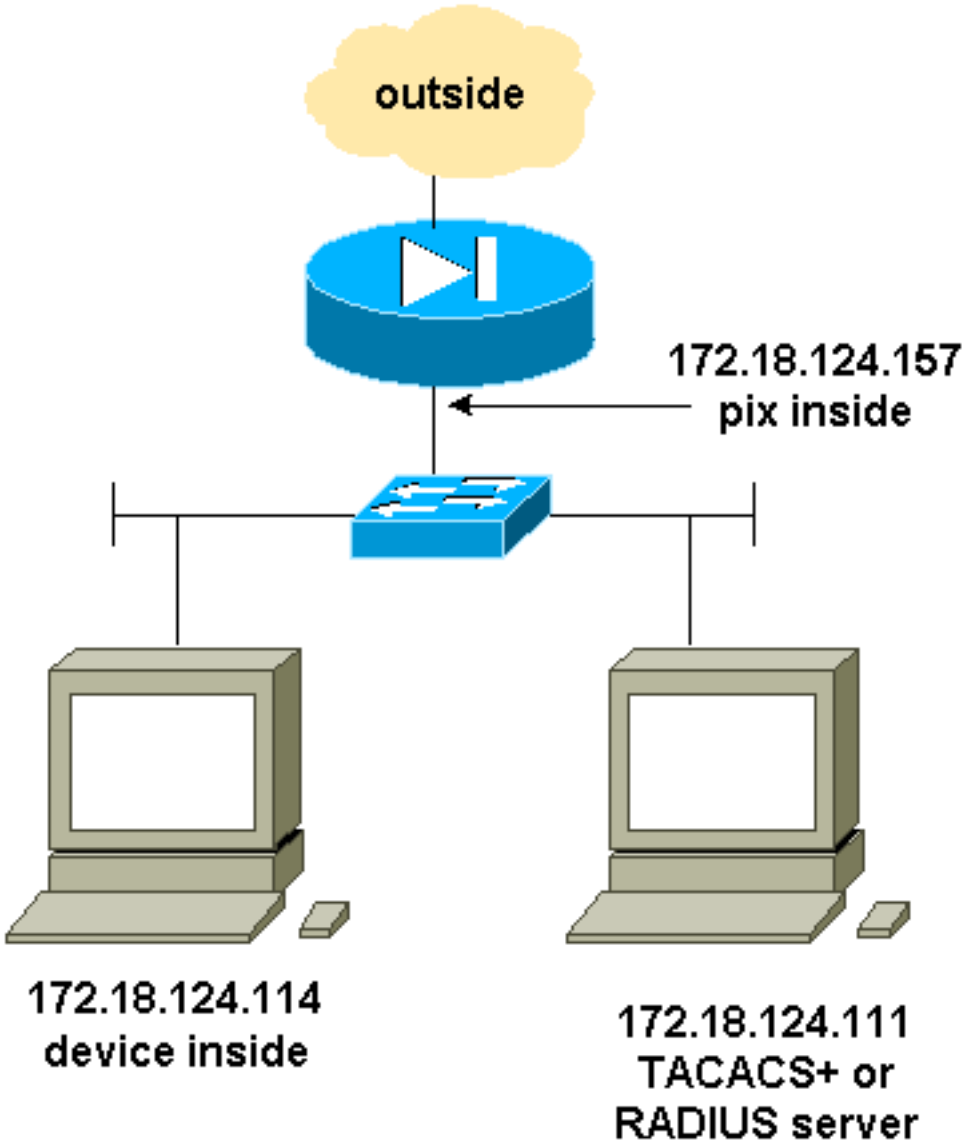
SSH - innen oder außen

PIX 5.2 hat Secure Shell (SSH) Version 1-Unterstützung hinzugefügt. SSH 1 basiert auf einem IETF-Entwurf vom November 1995. SSH-Versionen 1 und 2 sind nicht miteinander kompatibel. In den häufig gestellten Fragen zur Secure Shell (SSH) finden Sie weitere Informationen zu SSH.

Das PIX wird als SSH-Server angesehen. Datenverkehr von SSH-Clients (d. h. Boxen, auf denen SSH ausgeführt wird) zum SSH-Server (der PIX) wird verschlüsselt. Einige Clients der SSH-Version 1 sind in den Versionshinweisen zu PIX 5.2 aufgeführt. Die Tests in unserem Labor wurden mit F-sicherem SSH 1.1 unter NT und Version 1.2.26 für Solaris durchgeführt.

Hinweis: Informationen zu PIX 7.x finden Sie im Abschnitt Zulassen von SSH-Zugriff unter Verwalten des Systemzugriffs.

Netzwerkdiagramm



AAA-authentifiziertes SSH konfigurieren

Gehen Sie wie folgt vor, um AAA-authentifiziertes SSH zu konfigurieren:

1. Stellen Sie sicher, dass Telnet zu PIX mit AAA auf, aber ohne SSH:
   ```
   aaa-server AuthOutbound protocol radius (or tacacs+)
   aaa authentication telnet console AuthOutbound
   aaa-server AuthOutbound host 172.18.124.111 cisco
   ```
   Hinweis: Bei der Konfiguration von SSH wird der Befehl **telnet 172.18.124.114 255.255.255.255** nicht benötigt, da der Befehl **ssh 172.18.124.114 25.55555 255.255.255 inside** wird auf dem PIX ausgegeben. Beide Befehle sind zu Testzwecken enthalten.
2. SSH mithilfe der folgenden Befehle hinzufügen:
   ```
   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. Geben Sie den Befehl **show ca mypubkey rsa** im Konfigurationsmodus ein.

```
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
      67170674 4d5ba51e 6d020301 0001
 % 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. Testen Sie ein Telnet von der Solaris-Station:

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

Hinweis: "cisco" ist der Benutzername auf dem RADIUS/TACACS+-Server, und das Ziel ist 172.18.124.157.

Lokales SSH konfigurieren (keine AAA-Authentifizierung)

Es ist auch möglich, eine SSH-Verbindung zum PIX mit lokaler Authentifizierung und ohne AAA-Server einzurichten. Es gibt jedoch keinen separaten Benutzernamen pro Benutzer. Der Benutzername lautet immer "pix".

Verwenden Sie die folgenden Befehle, um lokales SSH auf dem PIX zu konfigurieren:

```
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
```

Da der Standardbenutzername in dieser Anordnung immer "pix" lautet, lautet der Befehl für die Verbindung mit dem PIX (dies war 3DES von einer Solaris-Box aus):

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

SSH-Debug

Debuggen ohne den Befehl debug ssh - 3DES und 512-cipher

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

Debuggen mit dem Befehl debug ssh - 3DES und 512-cipher

```
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
315002: Permitted SSH session from 172.18.124.114 on interface inside
   for user "cse"
```

Debug - 3DES und 1024-Chiffre

```
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
315002: Permitted SSH session from 172.18.124.114 on interface inside
   for user "cse"
```

Debug - DES und 1024-Chiffre

Hinweis: Diese Ausgabe stammt von einem PC mit SSH, nicht von 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
109011: Authen Session Start: user 'ssh', sid 1
315002: Permitted SSH session from 172.18.124.99 on interface outside
   for user "ssh"
```

Debug - 3DES und 2048-cipher

Hinweis: Diese Ausgabe stammt von einem PC mit SSH, nicht von 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
```

```
109011: Authen Session Start: user 'cse', Sid 2
315002: Permitted SSH session from 161.44.17.151 on interface inside
   for user "cse"
```

Was kann schief gehen?

Solaris debug - 2048-cipher und Solaris SSH

Hinweis: Solaris konnte die 2048-Chiffre nicht verarbeiten.

```
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).
```

Ungültiges Kennwort oder ungültiger Benutzername auf dem RADIUS/TACACS+-Server

```
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
109006: Authentication failed for user 'cse'
   from 0.0.0.0/0 to 161.44.17.151/0 on interface SSH
```

Der Benutzer ist mit dem Befehl nicht zulässig:

ssh 172.18.124.114 255.255.255.255 innen

Verbindungsversuche:

315001: Verweigerte SSH-Sitzung von 161.44.17.151 für die interne Schnittstelle

Schlüssel aus PIX entfernt (mit dem Befehl **ca zero rsa**) oder nicht mit dem Befehl **can save all** command

```
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"
315004: Fail to establish SSH session because PIX RSA host key retrieval failed.
315011: SSH session from 0.0.0.0 on interface outside for user ""
   disconnected by SSH server, reason: "Internal error" (0x00)
```

Der AAA-Server ist ausgefallen:

```
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"
2: Auth from 0.0.0.0/0 to 172.18.124.114/0 failed
   (server 172.18.124.111 failed) on interface outside
109002: Auth from 0.0.0.0/0 to 172.18.124.114/0 failed
   (server 172.18.124.111 failed) on interface outside
109002: Auth from 0.0.0.0/0 to 172.18.124.114/0 failed
   (server 172.18.124.111 failed) on interface outside
109006: Authentication failed for user 'cse' from 0.0.0.0/0
   to 172.18.124.114/0 on interface SSH
315003: SSH login session failed from 172.18.124.114 (1 attempts)
   on interface outside by user "cse"
315011: SSH session from 172.18.124.114 on interface outside for user "cse"
   disconnected by SSH server, reason: "status code: 0x03" (0x03)
109012: Authen Session End: user 'cse', Sid 0, elapsed 352 seconds
```

Der Client ist für 3DES konfiguriert, aber es gibt nur DES-Schlüssel in PIX:

Hinweis: Der Client war Solaris und unterstützte DES nicht.

```
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"
315011: SSH session from 172.18.124.114 on interface outside for user ""
   disconnected by SSH server, reason: "status code: 0x03" (0x03)
```

und in der Solaris-CLI:

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

Entfernen des RSA-Schlüssels aus PIX

ca Null rsa

Speichern des RSA-Schlüssels in PIX

alle

Zulassen von SSH von externem SSH-Client

ssh outside_ip *255.255.255.255* outside

Authentifizierung aktivieren

Mit dem Befehl:

aaaa authentication enable console topix

(wobei *topix* unsere Serverliste ist) wird der Benutzer zur Eingabe eines Benutzernamens und Kennworts aufgefordert, die an den TACACS- oder RADIUS-Server gesendet werden. Da das Authentifizierungspaket für enable mit dem Authentifizierungspaket für die Anmeldung übereinstimmt, kann der Benutzer, wenn er sich mit TACACS oder RADIUS beim PIX anmelden kann, über TACACS oder RADIUS mit demselben Benutzernamen/Kennwort aktivieren.

Weitere Informationen zu diesen Problemen finden Sie unter Cisco Bug ID CSCdm47044 (nur registrierte Kunden) .

Syslog-Informationen

Während die AAA-Abrechnung nur für Verbindungen über den PIX und nicht über den PIX gilt, werden bei der Einrichtung der Syslog-Protokollierung Informationen darüber, was der authentifizierte Benutzer getan hat, an den Syslog-Server (und, falls konfiguriert, an den Netzwerkverwaltungsserver über die Syslog-MIB) gesendet.

Wenn Syslog eingerichtet ist, werden Meldungen wie diese auf dem Syslog-Server angezeigt:

Protokollierungs-Trap-Benachrichtigungsebene:

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

Protokollierungs-Trap-Informationsebene (einschließlich der Benachrichtigungsebene):

307002: Zulässige Telnet-Anmeldesitzung vom 10.31.1.40

Zugriff bei Ausfall des AAA-Servers

Wenn der AAA-Server ausgefallen ist, können Sie zunächst das Telnet-Kennwort für den Zugriff auf das PIX eingeben, anschließend **pix** für den Benutzernamen und anschließend das enable-Kennwort (**Kennwort *unabhängig* von** der **Kennwortart)** für das Kennwort. Wenn Sie **das Kennwort aktivieren*, was auch immer* nicht in der PIX-Konfiguration enthalten ist**, geben Sie **pix** als Benutzernamen ein, und drücken Sie die **Eingabetaste**. Wenn das enable-Kennwort festgelegt, aber nicht bekannt ist, benötigen Sie eine Kennwortwiederherstellungsdiskette, um das Kennwort zurückzusetzen.

Informationen, die beim Öffnen eines TAC-Tickets gesammelt werden müssen

Wenn Sie nach den oben beschriebenen Schritten zur Fehlerbehebung weiterhin Hilfe benötigen und ein Ticket beim Cisco TAC erstellen möchten, geben Sie die folgenden Informationen an.
• Problembeschreibung und relevante Topologiedetails • Fehlerbehebung vor dem Öffnen des Gehäuses durchgeführt • Ausgabe des Befehls **show tech-support** • Ausgabe des Befehls **show log** nach der Ausführung mit dem Befehl **logging puffered debugging** oder Konsolenerfassungen, die das Problem veranschaulichen (falls verfügbar) Bitte fügen Sie die gesammelten Daten in einem nicht zippierten Textformat (.txt) an Ihr Ticket an. Sie können Informationen zu Ihrem Ticket hinzufügen, indem Sie es mithilfe des Case Query Tool hochladen (nur registrierte Kunden). Wenn Sie nicht auf das Fallabfrage-Tool zugreifen können, können Sie die Informationen in einem E-Mail-Anhang an attach@cisco.com senden, der Ihre Fallnummer in der Betreffzeile Ihrer Nachricht enthält.

Zugehörige Informationen

- Cisco Secure PIX Firewall - Befehlsreferenzen
- PIX RADIUS TACACS+