Hoe u verificatie kunt uitvoeren en de Cisco Secure PIX-firewall (5.2 tot en met 6.2) kunt inschakelen

Inhoud

Inleiding

Dit document beschrijft hoe u AAA-geauthentiseerde toegang kunt creëren tot een PIX-firewall die PIX-softwareversie 5.2 tot en met 6.2 draait en tevens informatie biedt over het mogelijk maken van verificatie, syslogging en het verkrijgen van toegang wanneer de AAA-server uitvalt. In PIX 5.3 en later is de verificatie, autorisatie en accounting (AAA) verandering in vergelijking met eerdere

versies van code dat de RADIUS poorten configureerbaar zijn.

In PIX-softwarereleases 5.2 en hoger kunt u op vijf verschillende manieren AAA-geauthentiseerde toegang tot de PIX creëren:

- Telnet-verificatie - binnen
- Console poortverificatie
- Geautomatiseerde Cisco Secure VPN-client 1.1 - buiten
- Geautomatiseerde VPN 3000 2.5 - buiten
- Secure Shell (SSH) - binnen of buiten

Opmerking: DES of 3DES moeten op de PIX (geef een **show versie** opdracht om te controleren) zijn ingeschakeld voor de laatste drie methoden. In PIX-softwareversie 6.0 en hoger kan PIX-apparaatbeheer (PDM) ook worden geladen om GUI-beheer mogelijk te maken. PDM valt buiten het toepassingsgebied van dit document.

Zie PIX 6.2 voor meer informatie over de authenticatie en autorisatie opdracht voor PIX 6.2: Configuratievoorbeeld van verificatie- en autorisatieopdracht.

Om voor AAA-echt bevonden (Cut-through Proxy) toegang te creëren tot een PIX-firewall die PIX-softwarereleases 6.3 en hoger uitvoert, raadpleegt u PIX/ASA: Snijd-door proxy voor netwerktoegang met behulp van TACACS+ en RADIUS-serverconfiguratievoorbeeld.

Voorwaarden

Vereisten

Voer deze taken uit voordat u AAA-verificatie toevoegt:

- Geef deze opdrachten uit om een wachtwoord voor de PIX toe te voegen:**zwabbertelnet <local_ip> [<mask>] [<if_name>]**PIX versleutelt automatisch dit wachtwoord om een versleutelde string te vormen met het sleutelwoord **versleuteld**, zoals in dit voorbeeld:
  ```
  passwd OnTrBUG1Tp0edmkr encrypted
  ```
  U hoeft het **gecodeerde** trefwoord niet toe te voegen.
- Zorg ervoor dat u van het binnennetwerk aan de binnenkant interface van de PIX kunt tellen *zonder* AAA authenticatie nadat u deze verklaringen toevoegt.
- Heb altijd een verbinding open voor PIX terwijl u authenticatie verklaringen toevoegt in het geval dat het terugdraaien van de opdrachten nodig is.

Op AAA-verificatie (anders dan SSH waar de sequentie afhankelijk is van de client) ziet de gebruiker een aanvraag voor het PIX-wachtwoord (zoals in *doorgestuurd <wat>*), dan een verzoek voor de RADIUS- of TACACS-gebruikersnaam en -wachtwoord.

Opmerking: U kunt niet tellen naar de externe interface van PIX. SSH kan op de externe interface worden gebruikt indien aangesloten vanaf een externe SSH-client.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- PIX-softwarerelease 5.2, 5.3, 6.0, 6.1 of 6.2

- Cisco Secure VPN-client 12.1
- Cisco VPN 3000 client 2.5
- Cisco VPN-client 3.0.x (PIX 6.0 code vereist)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureerbare RADIUS-poorten (5.3 en later)

Sommige RADIUS-servers gebruiken RADIUS-poorten anders dan 1645/1646 (gewoonlijk 1812/1813). In PIX 5.3 kunnen de RADIUS-verificatie en de accounting-poorten worden gewijzigd in andere dan standaard 1645/1646 met deze opdrachten:

Straal autorisatie per server #

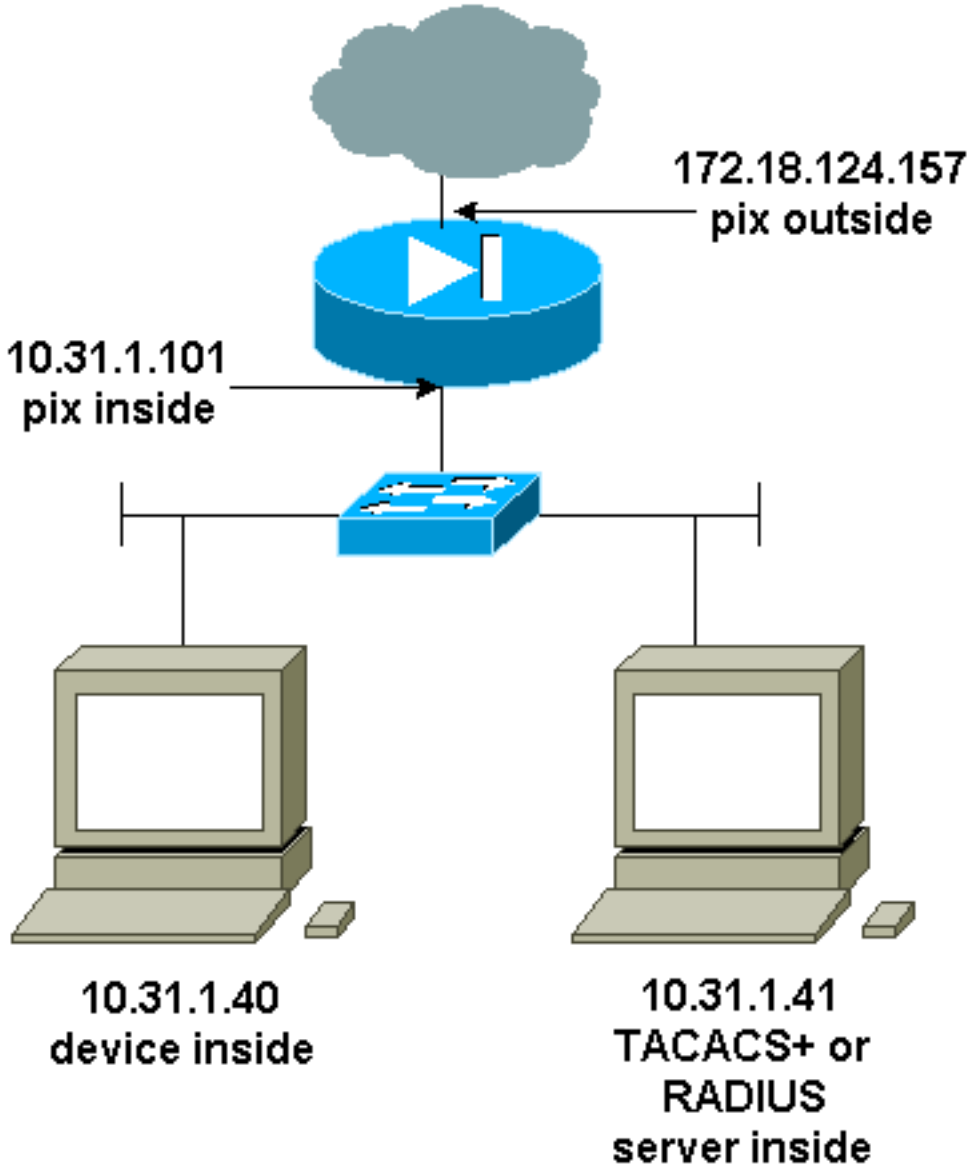
Straal van een server #-ondersteuning

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Telnet-verificatie - binnen

Netwerkdiagram



Opdrachten toegevoegd aan PIX-configuratie

Voeg deze opdrachten aan de configuratie toe:

Auto server topix protocol tacs+

AAA-server topix host 10.31.1.41 cisco timeout 5

AAA-verificatie telnet-topix

De gebruiker ziet een verzoek om het PIX-wachtwoord (zoals in `doorgevoerd <wat>`) en vervolgens een verzoek om de RADIUS- of TACACS-gebruikersnaam en het wachtwoord (opgeslagen op de 10.31.1.41 TACACS- of RADIUS-server).

Console poortverificatie

Voeg deze opdrachten aan de configuratie toe:

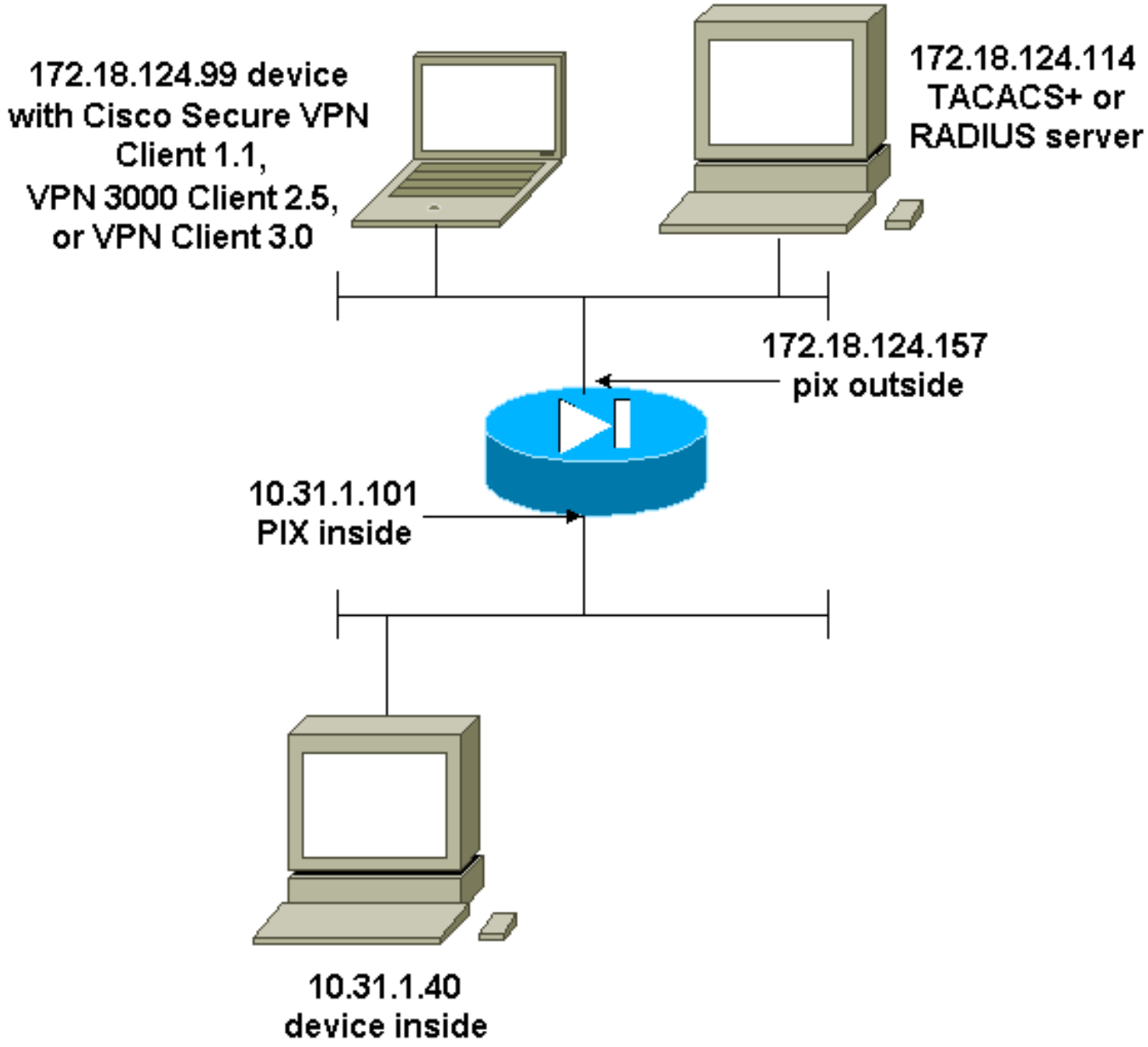
Auto server topix protocol tacs+

AAA-server topix host 10.31.1.41 cisco timeout 5

AAA authenticatie seriële console topix

De gebruiker ziet een verzoek om het PIX-wachtwoord (zoals in `doorgevoerd <wat>`), dan een verzoek om de RADIUS/TACACS-gebruikersnaam/wachtwoord (opgeslagen op de RADIUS- of TACACS-server 10.31.1.41).

Diagram - VPN-client 1.1, VPN 3000 2.5 of VPN-client 3.0 - buiten



Geautomatiseerde Cisco Secure VPN-client 1.1 - buiten

Geautomatiseerde Cisco Secure VPN-client 1.1 - Clientconfiguratie
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
```

Cisco Secure VPN-client 1.1 - buiten - partiële PIX-configuratie

```
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
```

Geautomatiseerde VPN-client 3000 2.5 of VPN-client 3.0 - buiten

Geautomatiseerde VPN-client 3000 2.5 of VPN-client 3.0 - Clientconfiguratie

1. Selecteer **VPN Kiezer > Eigenschappen > Naam van de verbinding** vanuit VPN 3000.
2. Selecteer **Verificatie > Groepstoegangsinformatie**. De naam en het wachtwoord van de groep moeten overeenkomen met wat er op de PIX staat in de verklaring **van** de **groep** <*group_name*> ******.

Wanneer u op **Connect** klikt, komt de crypto tunnel op, en PIX wijst een IP adres toe van de testpool (slechts mode-configuratie wordt ondersteund met de VPN 3000 client). Dan kunt u een eindvenster, telnet aan 172.18.124.157 omhoog brengen, en AAA-echt zijn. De opdracht **telnet 192.168.1.x** op de PIX maakt verbindingen mogelijk van gebruikers in de pool naar de externe interface.

Geautomatiseerde VPN-configuratie 3000 2.5 - Buiten - PIX-configuratie

```
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
```

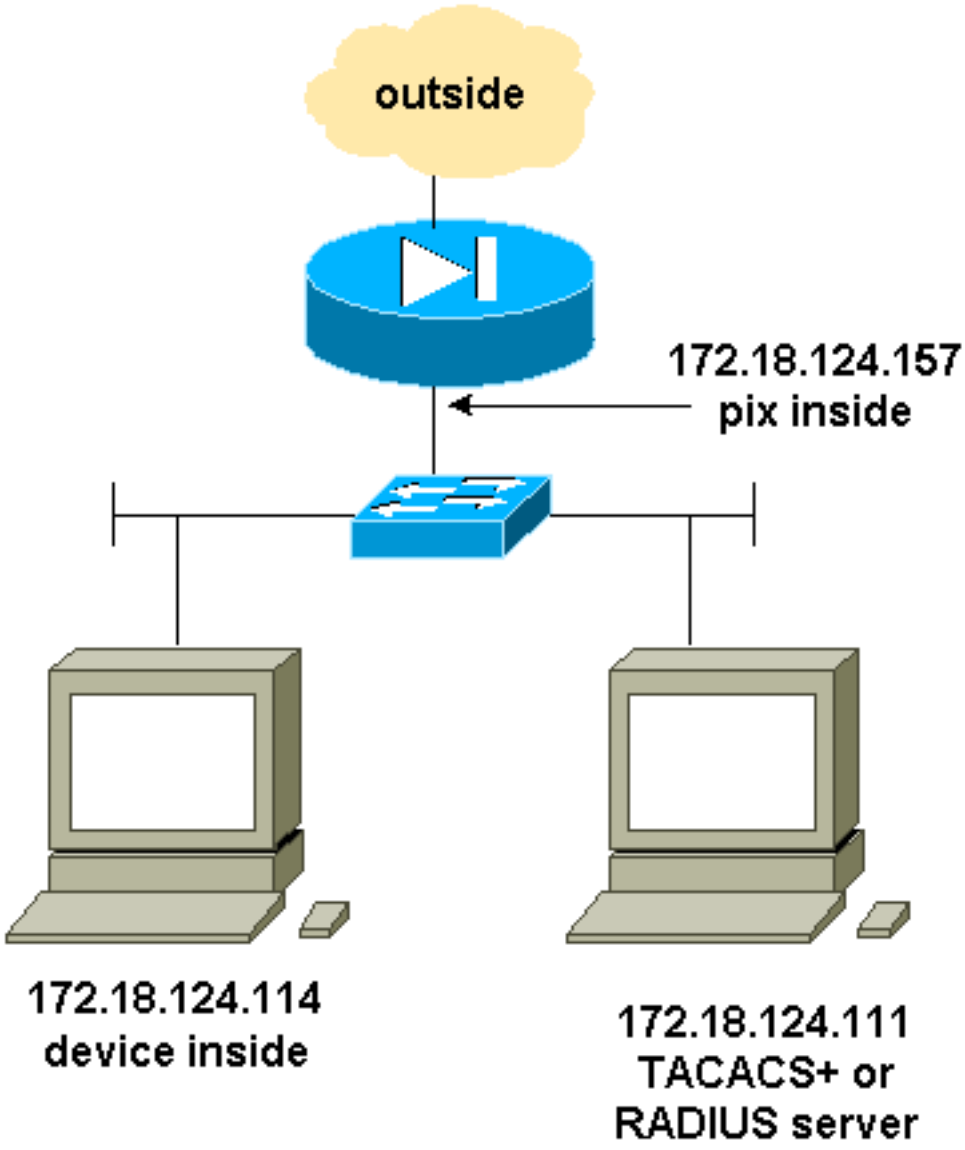
SSH - In of buiten

Ondersteuning van PIX 5.2 Secure Shell (SSH), versie 1. SSH 1 is gebaseerd op een IETF - ontwerp van november 1995. SSH versie 1 en 2 zijn niet compatibel met elkaar. Raadpleeg de Secure Shell (SSH), waar vragen vaak zijn gesteld voor meer informatie over SSH.

De PIX wordt beschouwd als de SSH-server. Verkeer van SSH-clients (dat wil zeggen, boxen die SSH's draaien) naar de SSH-server (de PIX) is versleuteld. Sommige klanten van SSH versie 1 zijn opgenomen in de PIX 5.2 release notes. De testen in ons laboratorium werden uitgevoerd met F-veilige SSH 1.1 op NT en versie 1.2.26 voor Solaris.

Opmerking: Raadpleeg voor PIX 7.x het gedeelte Toegang tot SSH van het beheersysteem.

Netwerkdiagram



AAA geverifieerd SSH configureren

Voltooi deze stappen om AAA echt bevonden SSH te configureren:

1. Zorg ervoor dat u met AAA op maar zonder SSH kunt tellen naar PIX:
   ```
   aaa-server AuthOutbound protocol radius (or tacacs+)
   aaa authentication telnet console AuthOutbound
   aaa-server AuthOutbound host 172.18.124.111 cisco
   ```
   Opmerking: Als SSH is geconfigureerd is de opdracht **telnet 172.18.124.114 255.255.255** niet nodig omdat **SH 172.18.124.114 25.5 255.255.255 binnenin** wordt afgegeven op de PIX. Beide opdrachten zijn opgenomen voor testdoeleinden.
2. Voeg SSH toe met deze opdrachten:
   ```
   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. Geef de **show ca mypubkey rsa** opdracht in **de** configuratie modus uit.

```
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. Probeer een telnet van het Solaris station:

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

Opmerking: "cisco" is de gebruikersnaam voor RADIUS/TACACS+ server en 172.18.124.157 is de bestemming.

Local SSH configureren (geen AAA-verificatie)

Het is ook mogelijk een SSH-verbinding naar de PIX op te zetten met lokale authenticatie en geen AAA-server. Er is echter geen afzonderlijke gebruikersnaam voor de gebruiker. De gebruikersnaam is altijd 'pix'.

Gebruik deze opdrachten om een lokale SSH op de PIX te configureren:

```
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
```

Aangezien de standaardgebruikersnaam in dit arrangement altijd "pix" is, is de opdracht om verbinding te maken met de PIX (dit was 3DES uit een Solaris box):

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

SSH-debug

Debug zonder debug Sh-opdracht - 3DES en 512-algoritme

```
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
```

Debug met de debug Sh-opdracht - 3DES en 512-algoritme

```
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 en een 1024-algoritme

```
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 en een 1024-algoritme

Opmerking: deze output komt van een PC met SSH, niet van 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 en een 2048-algoritme

Opmerking: deze output komt van een PC met SSH, niet van 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"
```

Wat er kan misgaan

Solaris debug - 2048-algoritme en Solaris SSH

Opmerking: Solaris kon het 2048-algoritme niet aan.

```
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).
```

Slecht wachtwoord of gebruikersnaam op 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
```

Gebruiker niet toegestaan via de opdracht:

ssh 172.18.124.114 255.255.255.255 binnenin

Probeert aan te sluiten:

315001: Geontheerde SSH-sessie van 16.4.17.151 op interface binnen

Met een toets die is verwijderd van PIX (met de opdracht **ca nul** instellen) of niet opgeslagen is met de **opdracht alle** opdracht **opslaan**

```
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)
```

AAA-server is uitgeschakeld:

```
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
```

Client is ingesteld voor 3DES, maar er is alleen DES-toets in PIX:

Opmerking: Cliënt was Solaris die geen DES ondersteunde.

```
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)
```

en op onze Solaris CLI:

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

RSA-toets verwijderen van PIX

A nul rsa

RSA-toets opslaan op PIX

alles opslaan

SSH van buitenzijde naar SSH-client toestaan

ssh buitenkant_ip *255.255.255.255* buiten

Verificatie inschakelen

Met deze opdracht:

AAA-verificatie maakt console topix mogelijk

(waar *topix* onze serverlijst is), wordt de gebruiker gevraagd om een gebruikersnaam en wachtwoord die naar de TACACS- of RADIUS-server worden verzonden. Aangezien het verificatiepakket waarmee u een verbinding kunt maken hetzelfde is als het authenticatiepakket voor inloggen, kunnen de gebruikers, als ze met TACACS of RADIUS in de PIX kunnen inloggen, TACACS of RADIUS met dezelfde gebruikersnaam/wachtwoord invoeren.

Meer informatie over deze kwesties is beschikbaar in Cisco bug-ID CSCdm47044 (alleen geregistreerde klanten).

Systeemloginformatie

Terwijl AAA-accounting alleen geldig is voor verbindingen door de PIX, niet voor de PIX als syslogging is ingesteld, wordt informatie over wat de geauthenticeerde gebruiker deed verzonden naar de syslog server (en naar de netwerkbeheerserver, indien geconfigureerd, door de standaard MIB).

Als syslogging is ingesteld, worden er berichten zoals deze weergegeven op de syslogserver:

Meldingsniveau van de Logingvanger:

```
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.
```

Informatieniveau van de vangnetten (inclusief meldingsniveau):

307002: Toegestane Telnet-sessie van 10.31.1.40

Toegang verkrijgen wanneer de AAA-server is uitgeschakeld

Als de AAA-server uitvalt, kunt u eerst het Telnet-wachtwoord invoeren dat toegang heeft tot de PIX, dan **PIX** voor de gebruikersnaam en vervolgens het wachtwoord inschakelen (**Wachtwoord *inschakelen* wat dan ook) voor het wachtwoord.** Als u *het **wachtwoord invoert wat*** niet in de PIX-configuratie voorkomt, voert u **pix** in voor de gebruikersnaam en drukt u op **ENTER**. Als het wachtwoord wordt ingesteld maar niet bekend, moet u een wachtwoordherstelschijf hebben om het wachtwoord te herstellen.

Te verzamelen informatie als u een TAC-case opent

Als u nog steeds hulp nodig hebt nadat u de bovenstaande stappen voor het oplossen van problemen hebt gevolgd en u een case wilt openen met Cisco TAC,

zorg er dan voor dat u de volgende informatie bevat.
• Probleembeschrijving en relevante topologgegevens • Probleemoplossing uitgevoerd voordat u de case opent • Uitvoer vanuit de opdracht **Tech-support** • Uitvoer van het bevel van het **showlogbestand** na het lopen met de **het registreren gebufferde** het bevel, of console vangt die het probleem (indien beschikbaar) aantoont Hang de verzamelde gegevens aan uw case in een niet-zipped, onbewerkte tekstindeling (.txt). U kunt informatie aan uw case toevoegen door deze te uploaden met behulp van de Case Query Tool (alleen geregistreerde klanten). Als u geen toegang hebt tot de Case Query Tool, kunt u de informatie in een e-mailbijlage naar attach@cisco.com met uw casenummer in de onderwerpregel of uw bericht verzenden.

Gerelateerde informatie

- Opdrachtreferenties van Cisco Secure PIX-firewall
- PIX RADIUS TACACS+