Comment assurer l'authentification et l'activation sur le pare-feu Cisco Secure PIX Firewall (versions 5.2 à 6.2)

Contenu

Introduction
Conditions préalables
Conditions requises
Components Used
Ports RADIUS configurables (5.3 et versions ultérieures)
Conventions
Authentification Telnet - Interne
Diagramme du réseau
Commandes ajoutées à la configuration PIX
Authentification du port de console
Client VPN sécurisé Cisco authentifié 1.1 - Externe
VPN 3000 2.5 ou Client VPN 3.0 authentifié - Externe
VPN 3000 2.5 ou Client VPN 3.0 authentifié - Externe - Configuration du client
SSH : interne ou externe
Diagramme du réseau
Configurer AAA Authenticated SSH
Configurer SSH local (pas d'authentification AAA)
Débogage SSH
Causes de problèmes potentiels
Comment supprimer la clé RSA de PIX
Comment enregistrer la clé RSA sur PIX
Comment autoriser SSH à partir d'un client SSH externe
Activer l'authentification
Informations Syslogan
Gagner l'accès en cas de panne du serveur AAA
Informations à collecter si vous ouvrez un dossier TAC
Informations connexes

Introduction

Ce document décrit comment créer un accès authentifié AAA à un pare-feu PIX fonctionnant sous un logiciel PIX de versions 5.2 à 6.2, et fournit également des renseignements sur l'authentification, la création d'un journal de système et l'accès lorsque le serveur AAA est en panne. Dans PIX 5.3 ou une version ultérieure, les modifications apportées à AAA

(authentification, autorisation et traçabilité) permettent la configuration de ports RADIUS.

Dans les versions 5.2 et ultérieures du logiciel PIX, vous pouvez créer un accès AAA authentifié au PIX de cinq manières différentes :

- Authentification Telnet - Interne
- Authentification du port de console
- Client VPN sécurisé Cisco authentifié 1.1 - Externe
- VPN authentifié 3000 2.5 - Externe
- SSH (Authenticated Secure Shell) - Intérieur ou Externe

Remarque : DES ou 3DES doivent être activés sur le PIX (émettez une commande **show version** pour vérifier) pour les trois dernières méthodes. Dans les versions 6.0 et ultérieures du logiciel PIX, PIX Device Manager (PDM) peut également être chargé pour activer la gestion de l'interface utilisateur graphique. Le PDM n'est pas inclus dans ce document.

Pour plus d'informations sur la commande d'authentification et d'autorisation pour PIX 6.2, référez-vous à PIX 6.2 : Exemple de configuration des commandes d'authentification et d'autorisation.

Afin de créer un accès AAA authentifié (Proxy Cut-through) à un pare-feu PIX qui exécute le logiciel PIX versions 6.3 et ultérieures, référez-vous à PIX/ASA : Exemple de configuration d'un proxy à coupure pour l'accès réseau à l'aide d'un serveur TACACS+ et RADIUS.

Conditions préalables

Conditions requises

Effectuez ces tâches avant d'ajouter l'authentification AAA :

- Émettez ces commandes afin d'ajouter un mot de passe pour PIX :**passwd wwtelnet <ip_local> [<masque>] [<nom_if>]**Le PIX chiffre automatiquement ce mot de passe pour former une chaîne chiffrée avec le mot clé **chiffré**, comme dans cet exemple :
  ```
  passwd OnTrBUG1Tp0edmkr encrypted
  ```
  Vous n'avez pas besoin d'ajouter le mot clé **chiffré**.
- Assurez-vous que vous pouvez établir une connexion Telnet entre le réseau interne et l'interface interne du PIX *sans* authentification AAA après avoir ajouté ces instructions.
- Ayez toujours une connexion ouverte au PIX pendant que vous ajoutez des instructions d'authentification au cas où la suppression des commandes est nécessaire.

Sur l'authentification AAA (autre que SSH où la séquence dépend du client), l'utilisateur voit une demande pour le mot de passe PIX (comme dans *passwd <any>*), puis une demande pour le nom d'utilisateur et le mot de passe RADIUS ou TACACS.

Remarque : Vous ne pouvez pas établir de connexion Telnet avec l'interface externe de PIX. SSH peut être utilisé sur l'interface externe si connecté à partir d'un client SSH externe.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Logiciel PIX version 5.2, 5.3, 6.0, 6.1 ou 6.2
- Client VPN sécurisé Cisco 1.1
- Client VPN Cisco 3000 2.5
- Client VPN Cisco 3.0.x (code PIX 6.0 requis)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Ports RADIUS configurables (5.3 et versions ultérieures)

Certains serveurs RADIUS utilisent des ports RADIUS autres que 1645/1646 (généralement 1812/1813). Dans PIX 5.3, les ports d'authentification et de comptabilité RADIUS peuvent être remplacés par d'autres ports que le 1645/1646 par défaut avec les commandes suivantes :

aaa-server radius-authport #

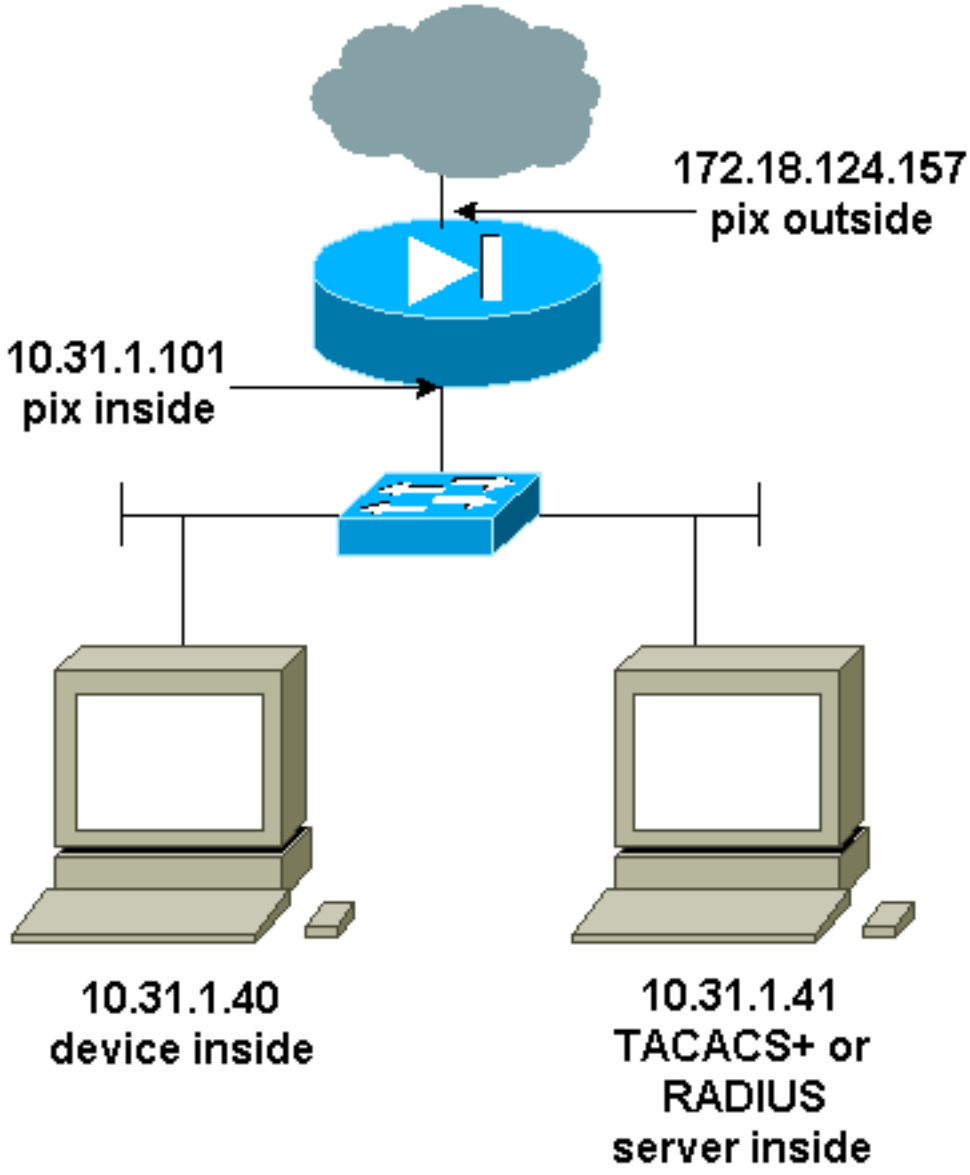
aaa-server radius-acctport n°

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Authentification Telnet - Interne

Diagramme du réseau



Commandes ajoutées à la configuration PIX

Ajoutez ces commandes à votre configuration :

aaa-server topix protocol tacacs+

aaa-server topix host 10.31.1.41 cisco timeout 5

aaa authentication telnet console topix

L'utilisateur voit une demande pour le mot de passe PIX (comme dans `passwd <any>`), puis une demande pour le nom d'utilisateur et le mot de passe RADIUS ou TACACS (stockés sur le serveur 10.31.1.41 TACACS ou RADIUS).

Authentification du port de console

Ajoutez ces commandes à votre configuration :

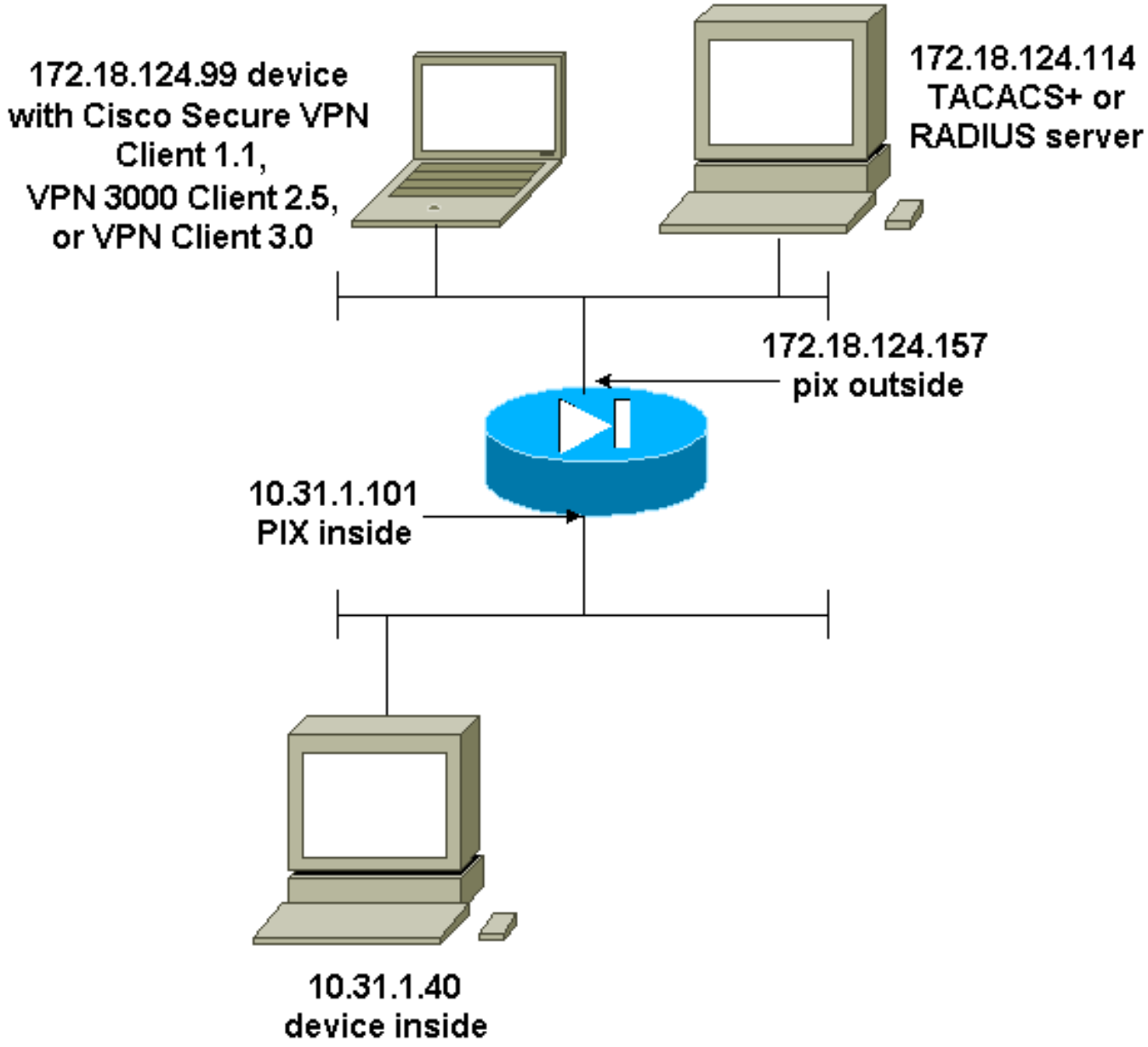
aaa-server topix protocol tacacs+

aaa-server topix host 10.31.1.41 cisco timeout 5

aaa authentication serial console topix

L'utilisateur voit une requête pour le mot de passe PIX (comme dans `passwd <any>`), puis une requête pour le nom d'utilisateur/mot de passe RADIUS/TACACS (stocké sur le serveur RADIUS ou TACACS 10.31.1.41).

Schéma - Client VPN 1.1, VPN 3000 2.5 ou Client VPN 3.0 - Externe



Client VPN sécurisé Cisco authentifié 1.1 - Externe

Client VPN sécurisé Cisco authentifié 1.1 - Externe - Configuration du client
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
```

Client VPN sécurisé Cisco authentifié 1.1 - Externe - Configuration PIX partielle

```
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 ou Client VPN 3.0 authentifié - Externe

VPN 3000 2.5 ou Client VPN 3.0 authentifié - Externe - Configuration du client

1. Sélectionnez **VPN Dialer > Properties > Name > Name the connection** from the VPN 3000.
2. Sélectionnez **Authentication > Group Access Information**. Le nom et le mot de passe du groupe doivent correspondre à ceux du PIX dans l'instruction **vpngroup <*group_name*> password ********.

Lorsque vous cliquez sur **Connect**, le tunnel de chiffrement s'active et le PIX attribue une adresse IP à partir du pool de tests (seul le mode-config est pris en charge avec le client VPN 3000). Ensuite, vous pouvez afficher une fenêtre de terminal, Telnet à 172.18.124.157, et être authentifié AAA. La commande **telnet 192.168.1.x** sur le PIX autorise les connexions des utilisateurs du pool à l'interface externe.

VPN authentifié 3000 2.5 - Externe - Configuration PIX partielle

```
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
```

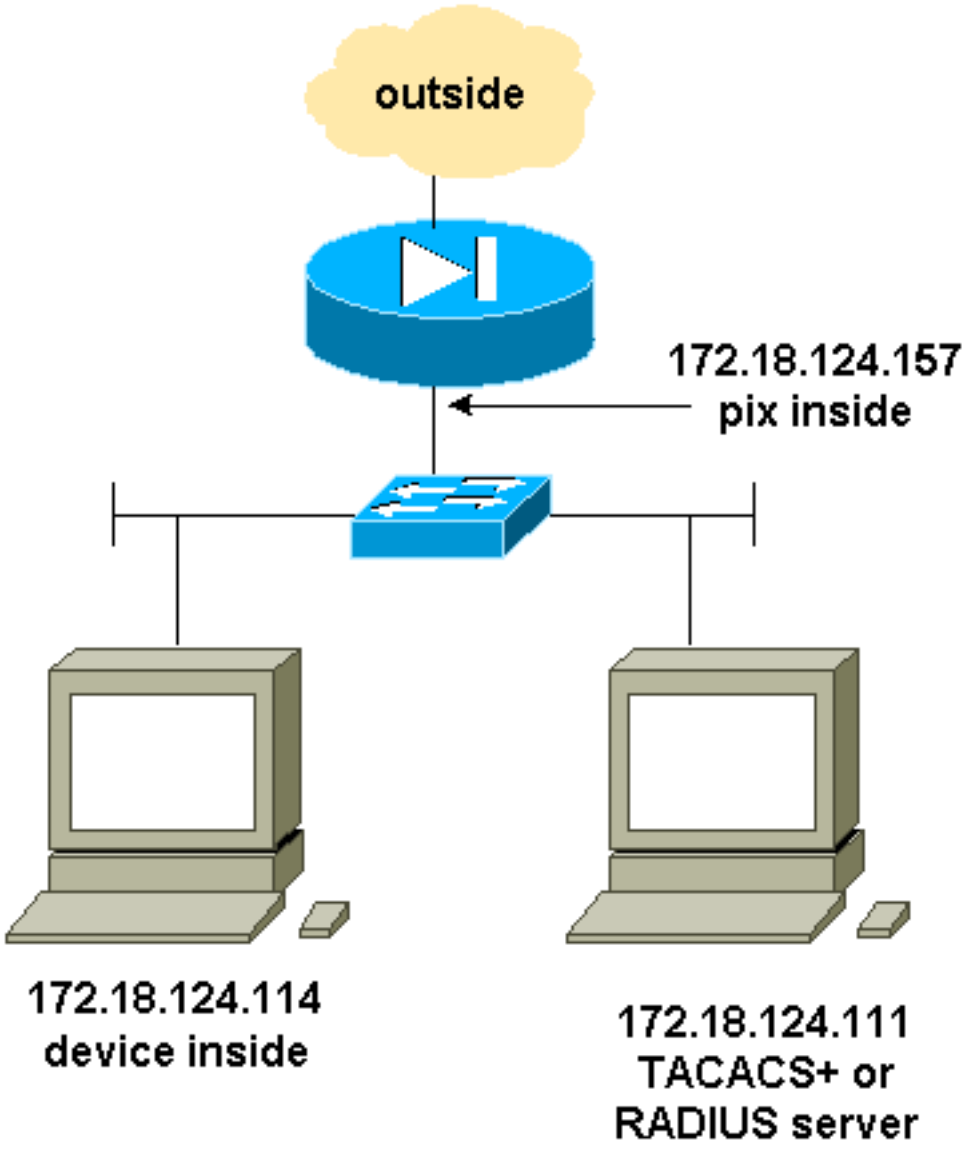
SSH : interne ou externe

PIX 5.2 a ajouté la prise en charge de Secure Shell (SSH) version 1. SSH 1 est basé sur une ébauche de novembre 1995 de l'IETF. Les versions 1 et 2 de SSH ne sont pas compatibles entre elles. Référez-vous à la Foire aux questions Secure Shell (SSH) pour plus d'informations sur SSH.

Le PIX est considéré comme le serveur SSH. Le trafic des clients SSH (c'est-à-dire des boîtes exécutant SSH) vers le serveur SSH (le PIX) est chiffré. Certains clients SSH version 1 sont répertoriés dans les notes de version de PIX 5.2. Les tests de nos travaux pratiques ont été réalisés avec F-secure SSH 1.1 sur NT et la version 1.2.26 pour Solaris.

Remarque : pour PIX 7.x, reportez-vous à la section Autoriser l'accès SSH de Gestion de l'accès au système.

Diagramme du réseau



Configurer AAA Authenticated SSH

Complétez ces étapes pour configurer AAA authentifié SSH :

1. Assurez-vous que vous pouvez établir une connexion Telnet avec PIX avec AAA sur mais sans SSH :
   ```
   aaa-server AuthOutbound protocol radius (or tacacs+)
   aaa authentication telnet console AuthOutbound
   aaa-server AuthOutbound host 172.18.124.111 cisco
   ```
   Remarque : lorsque SSH est configuré, la commande **telnet 172.18.124.114 255.255.255.255** n'est pas nécessaire car **ssh 172.18.124.1142555 255.255.255 à l'intérieur** est émis sur le PIX. Les deux commandes sont incluses à des fins de test.
2. Ajoutez SSH à l'aide des commandes suivantes :
   ```
   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. Émettez la commande **show ca mypubkey rsa** en mode de configuration.

```
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. Essayez une connexion Telnet à partir de la station Solaris :

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

Remarque : « cisco » est le nom d'utilisateur sur le serveur RADIUS/TACACS+ et 172.18.124.157 est la destination.

Configurer SSH local (pas d'authentification AAA)

Il est également possible de configurer une connexion SSH au PIX avec une authentification locale et aucun serveur AAA. Cependant, il n'y a pas de nom d'utilisateur distinct par utilisateur. Le nom d'utilisateur est toujours « pix ».

Utilisez ces commandes pour configurer le protocole SSH local sur le 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
```

Puisque le nom d'utilisateur par défaut dans cet arrangement est toujours « pix », alors la commande pour se connecter au PIX (il s'agissait de 3DES à partir d'une zone Solaris) est :

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

Débogage SSH

Déboguer sans la commande debug ssh - 3DES et 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
```

Déboguer avec la commande debug ssh - 3DES et 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"
```

Débogage - 3DES et 1024-cipher

```
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"
```

Débogage - DES et 1024-cipher

Remarque : cette sortie provient d'un PC avec SSH, et non de 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"
```

Débogage - 3DES et 2048-cipher

Remarque : cette sortie provient d'un PC avec SSH, et non de 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"
```

Causes de problèmes potentiels

Débogage Solaris - 2048-cipher et SSH Solaris

Remarque : Solaris n'a pas pu gérer le chiffrement 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).
```

Mot de passe ou nom d'utilisateur incorrect sur le serveur 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
109006: Authentication failed for user 'cse'
   from 0.0.0.0/0 to 161.44.17.151/0 on interface SSH
```

Utilisateur non autorisé via la commande :

ssh 172.18.124.114 255.255.255.255 à l'intérieur

Tentatives de connexion :

315001: Session SSH refusée de 161.44.17.151 sur l'interface interne

Avec la touche supprimée de PIX (à l'aide de la commande **ca zéro rsa**) ou non enregistrée avec la commande **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"
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)
```

Le serveur AAA est en panne :

```
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
```

Le client est configuré pour 3DES mais il n'y a que la clé DES dans PIX :

Remarque : Solaris ne prenait pas en charge 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"
315011: SSH session from 172.18.124.114 on interface outside for user ""
   disconnected by SSH server, reason: "status code: 0x03" (0x03)
```

et sur notre CLI Solaris :

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

Comment supprimer la clé RSA de PIX

ca zéro rsa

Comment enregistrer la clé RSA sur PIX

peut enregistrer tout

Comment autoriser SSH à partir d'un client SSH externe

ssh outside_ip *255.255.255.255* externe

Activer l'authentification

Avec la commande :

aaa authentication enable console topix

(où *topix* est notre liste de serveurs), l'utilisateur est invité à fournir un nom d'utilisateur et un mot de passe qui sont envoyés au serveur TACACS ou RADIUS. Puisque le paquet d'authentification pour enable est identique au paquet d'authentification pour la connexion, si l'utilisateur peut se connecter au PIX avec TACACS ou RADIUS, il peut activer via TACACS ou RADIUS avec le même nom d'utilisateur/mot de passe.

Plus d'informations sur ces problèmes sont disponibles dans l'ID de bogue Cisco CSCdm47044 (clients enregistrés uniquement).

Informations Syslogan

Alors que la comptabilité AAA est uniquement valide pour les connexions via le PIX, pas pour le PIX, si syslogging est configuré, les informations sur ce que l'utilisateur authentifié a fait sont envoyées au serveur syslog (et au serveur de gestion de réseau, si configuré, via la MIB syslog).

Si syslogging est configuré, les messages tels que ceux-ci s'affichent sur le serveur syslog :

Niveau de notification de déroutement de journalisation :

```
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.
```

Niveau d'informations de déroutement de journalisation (qui inclut le niveau de notification) :

307002: Session de connexion Telnet autorisée à partir de 10.31.1.40

Gagner l'accès en cas de panne du serveur AAA

Si le serveur AAA est arrêté, vous pouvez entrer le mot de passe Telnet pour accéder au PIX initialement, puis **pix** pour le nom d'utilisateur, puis le mot de passe enable (**enable password *any***) pour le mot de passe. Si **enable password *quoi qu'*** il ne soit pas dans la configuration PIX, entrez **pix** pour le nom d'utilisateur et appuyez sur **Entrée**. Si le mot de passe enable est défini mais n'est pas connu, vous devez disposer d'un disque de récupération de mot de passe pour réinitialiser le mot de passe.

Informations à collecter si vous ouvrez un dossier TAC

Si vous avez toujours besoin d'assistance après avoir suivi les étapes de dépannage ci-dessus et que vous souhaitez ouvrir un dossier auprès du centre d'assistance technique Cisco, veillez à inclure les informations suivantes.
• Description du problème et des détails topologiques pertinents • Dépannage exécuté avant d'ouvrir le cas • Sortie de la commande **show tech-support** • Sortie de la commande **show log après l'exécution avec la commande logging buffered debugging , ou les captures de console qui expliquent le problème (si disponible)** Veuillez attacher les données rassemblées à votre cas en format texte décompressé (.txt). Vous pouvez joindre des informations à votre dossier en les téléchargeant à l'aide du Case Query Tool (clients enregistrés uniquement). Si vous ne pouvez pas accéder au Case Query Tool, vous pouvez envoyer les informations en pièce-jointe dans un e-mail à attach@cisco.com avec votre numéro de dossier dans l'objet du message.

Informations connexes

- Références des commandes du pare-feu Cisco Secure PIX
- PIX RADIUS TACACS+