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

Contenu

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 du logiciel PIX 5.2 et plus tard, vous pouvez créer l'accès AAA-authentifié au PIX de cinq manières différentes :

- Authentification de telnet - À l'intérieur
- Authentification de port de console
- Cisco Secure VPN Client authentifié 1.1 - Dehors
- VPN 3000 authentifié 2.5 - Dehors
- Protocole Secure Shell (SSH) authentifié - À l'intérieur ou dehors

Remarque: Le DES ou le 3DES doit être activé sur le PIX (émettez une commande de **show version** de vérifier) pour les trois dernières méthodes. Dans la version du logiciel PIX 6.0 et plus tard, le PIX Device Manager (PDM) peut également être chargé pour activer la gestion GUI. PDM est hors de portée de ce document.

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

Afin de créer AAA-a authentifié l'accès (de proxy de cut-through) à un Pare-feu PIX qui exécute les versions du logiciel PIX 6.3 et plus tard, se rapportent à PIX/ASA : Proxy de cut-through pour l'accès au réseau utilisant l'exemple de configuration de serveur TACACS+ et RADIUS.

Conditions préalables

Conditions requises

Effectuez ces tâches avant que vous ajoutiez l'authentification d'AAA :

- Émettez ces commandes afin d'ajouter un mot de passe pour le PIX :**ww de passwd<local_ip> de telnet [<mask>] [<if_name>]**Le PIX chiffre automatiquement ce mot de passe pour former une chaîne chiffrée avec le mot clé **chiffré**, comme indiqué dans cet exemple :`passwd OnTrBUG1Tp0edmkr encrypted` Vous n'avez pas besoin d'ajouter le mot clé **chiffré**.
- Assurez-vous que vous pouvez telnet du réseau intérieur à l'interface interne du PIX *sans* authentification d'AAA après que vous ajoutiez ces déclarations.
- Ayez toujours une connexion ouverte de PIX tandis que vous ajoutez des instuctions d'authentification au cas où soutenir les commandes serait nécessaire.

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

Remarque: Vous ne pouvez pas telnet à l'interface extérieure de PIX. Le SSH peut être utilisé sur l'interface extérieure si connecté d'un client SSH extérieur.

Composants utilisés

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

- Version du logiciel PIX 5.2, 5.3, 6.0, 6.1, ou 6.2

- Cisco Secure VPN Client 1.1
- Cisco VPN 3000 Client 2.5
- Client VPN Cisco 3.0.x (code PIX 6.0 exigé)

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Le RAYON configurable met en communication (5.3 et plus tard)

Quelques serveurs de RAYON utilisent des ports de RAYON autres que 1645/1646 (habituellement 1812/1813). Dans PIX 5.3, l'authentification et les ports de traçabilité de RAYON peuvent être changés à autre que le 1645/1646 par défaut avec ces commandes :

rayon-authport d'AAA-serveur #

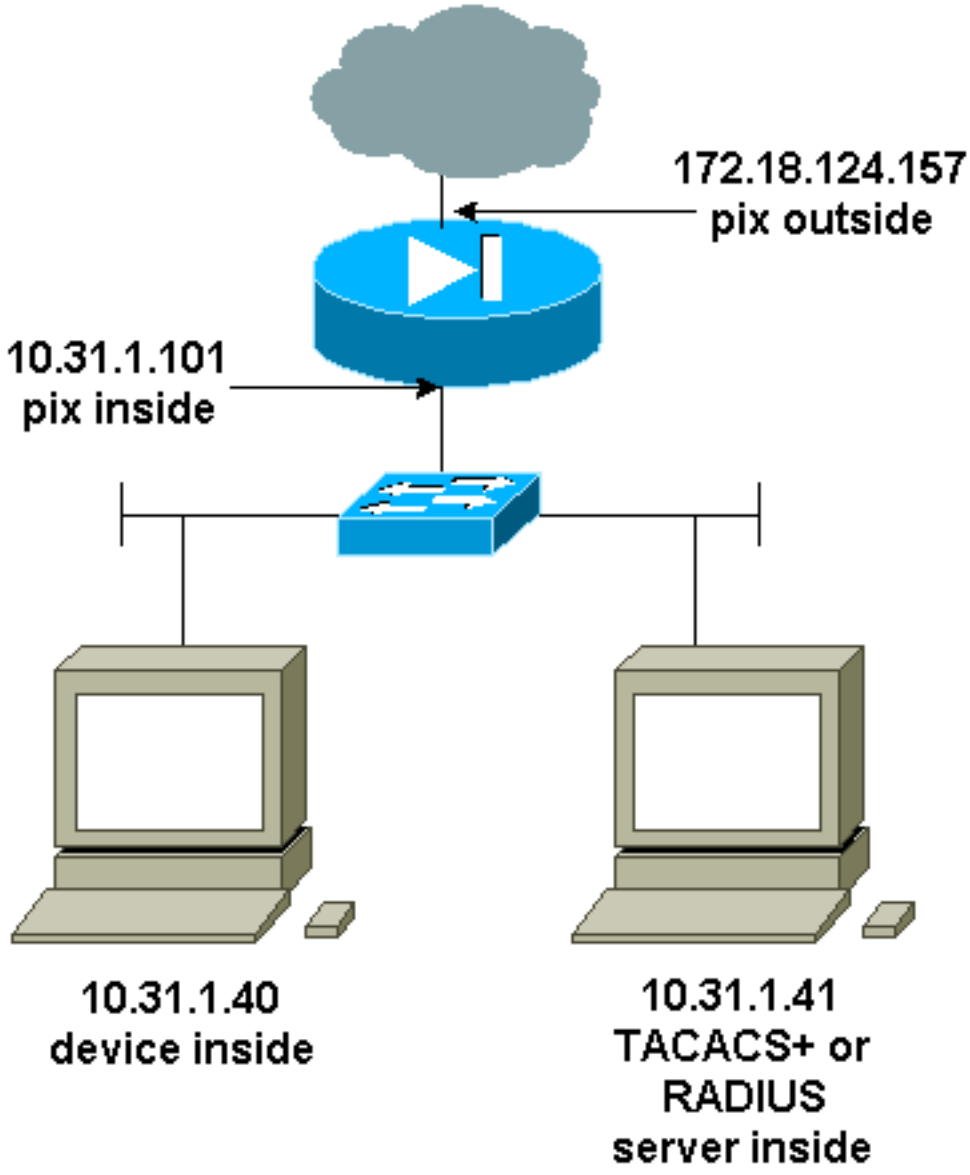
rayon-acctport d'AAA-serveur #

Conventions

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

Authentification de telnet - À l'intérieur

Diagramme du réseau



Commandes ajoutées à la configuration PIX

Ajoutez ces commandes à votre configuration :

protocole tacacs+ d'aaa-server topix

délai d'attente 5 de 10.31.1.41 Cisco d'aaa-server topix host

console topix de telnet d'authentification d'AAA

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

Authentification de port de console

Ajoutez ces commandes à votre configuration :

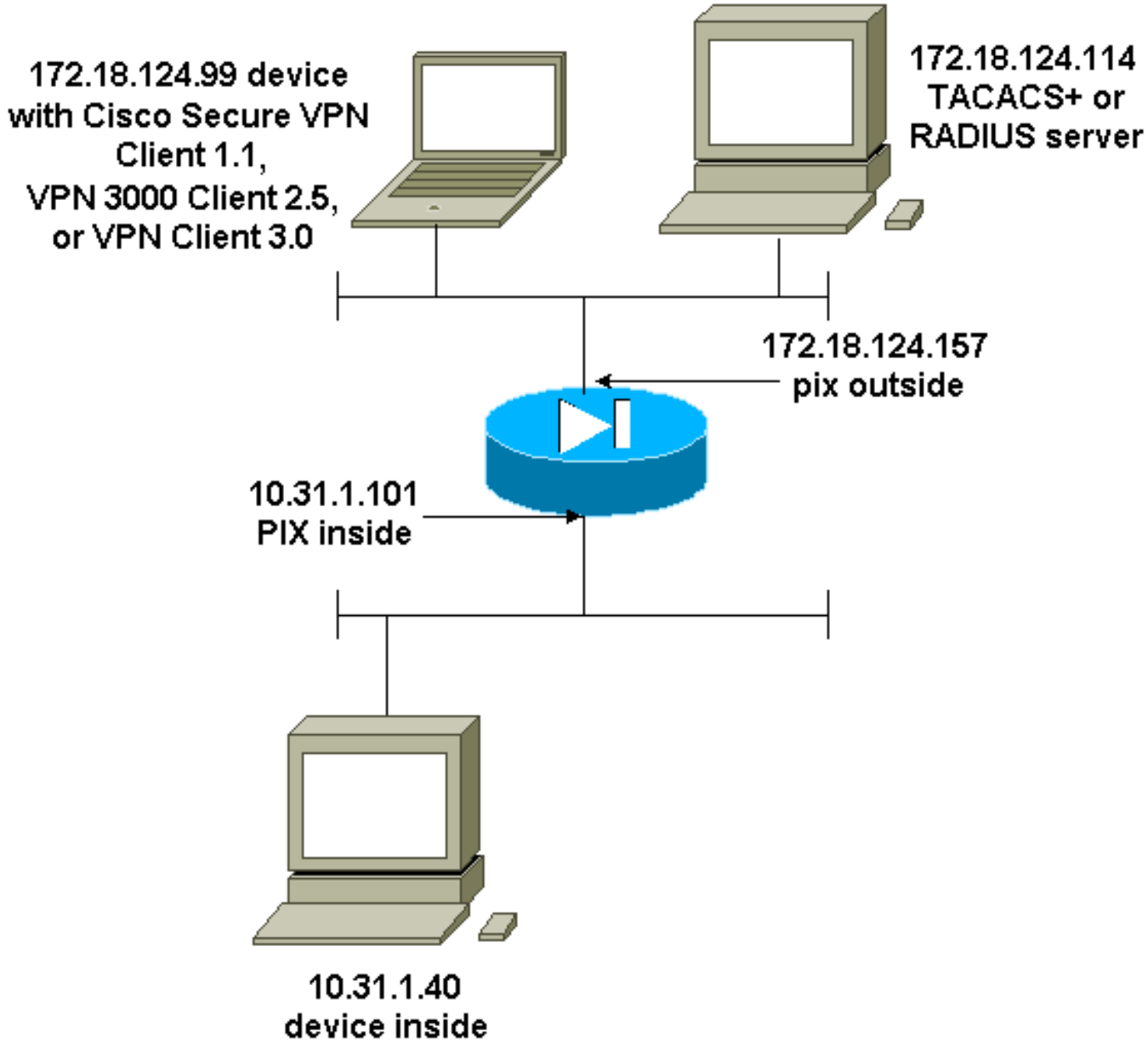
protocole tacacs+ d'aaa-server topix

délai d'attente 5 de 10.31.1.41 Cisco d'aaa-server topix host

topix de console série d'authentification d'AAA

L'utilisateur voit une demande pour le mot de passe PIX (comme dans le `<whatever> de passwd`), puis une demande du nom d'utilisateur/mot de passe RADIUS/TACACS (enregistré sur le serveur de RAYON ou TACACS 10.31.1.41).

Diagramme - Client vpn 1.1, VPN 3000 2.5, ou client vpn 3.0 - dehors



Cisco Secure VPN Client authentifié 1.1 - Dehors

Cisco Secure VPN Client authentifié 1.1 - En dehors de - Configuration de 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
```

Cisco Secure VPN Client authentifié 1.1 - En dehors de - Configuration partielle de PIX

```
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 authentifié 2.5 ou client vpn 3.0 - Dehors

VPN 3000 authentifié 2.5 ou client vpn 3.0 - En dehors de - Configuration de client

1. **Numéroteur** choisi **> Properties > nom VPN la connexion du** VPN 3000.
2. **Authentification > Group Access Information** choisis. Le nom et le mot de passe de groupe

devraient apparier ce qui est sur le PIX dans la déclaration de ********** de <group_name > de mot de passe de vpngroup**.

Quand vous clic **vous connectez**, le tunnel du chiffrement est soulevé, et le PIX assigne une adresse IP de la réserve de test (seulement le mode-config est pris en charge avec le client VPN 3000). Alors vous pouvez apporter un terminal window, telnet à 172.18.124.157, et AAA-soyez authentifié. La commande du **telnet 192.168.1.x** sur le PIX permet des connexions des utilisateurs dans le groupe à l'interface extérieure.

VPN 3000 authentifié 2.5 - En dehors de - Configuration partielle de PIX

```
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
```

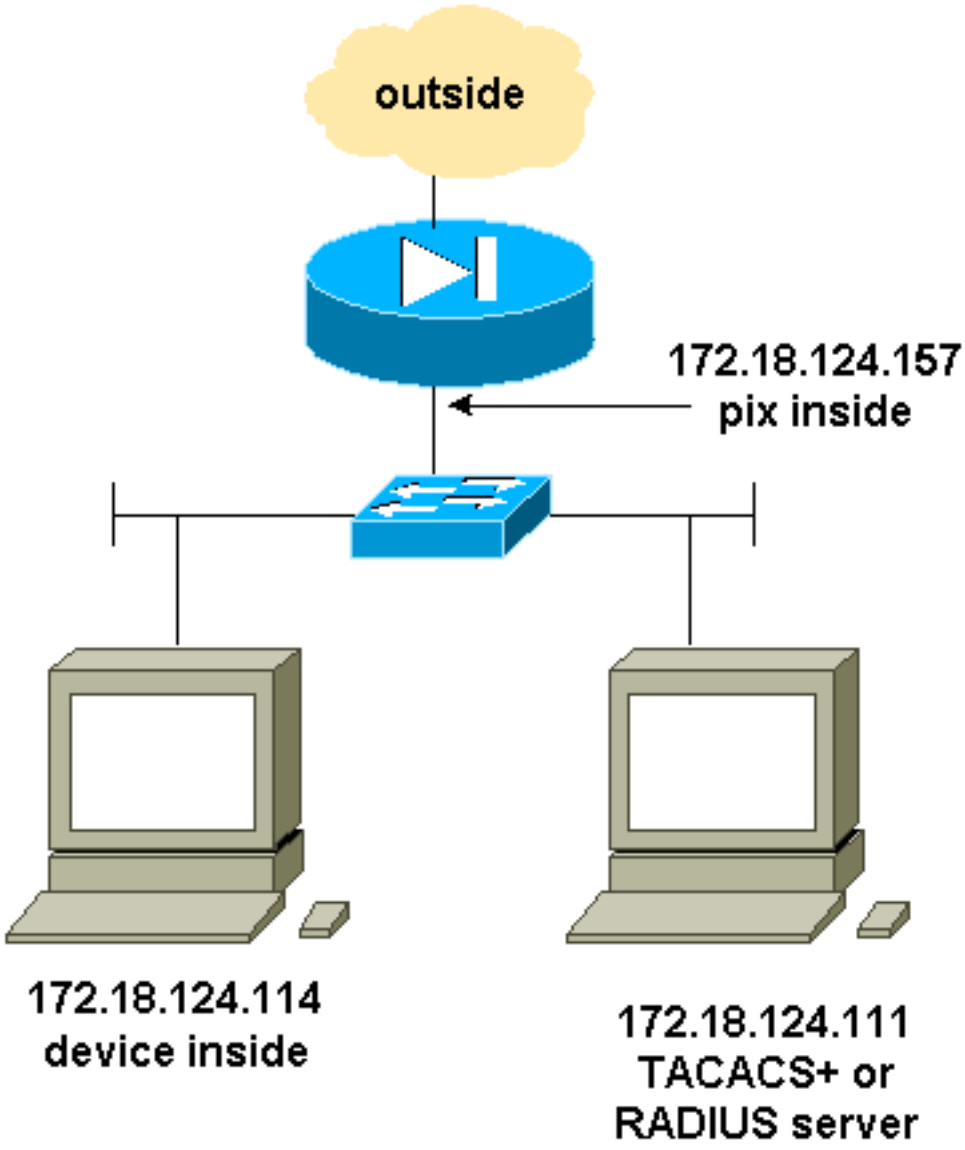
SSH - À l'intérieur ou dehors

PIX 5.2 a ajouté le support de version 1 de Protocole Secure Shell (SSH). Le SSH 1 est basé sur novembre, 1995, projet soumis à l'IETF. La version SSH 1 et 2 ne sont pas compatible avec l'un l'autre. Référez-vous aux forums aux questions de Protocole Secure Shell (SSH) pour plus d'informations sur le SSH.

Le PIX est considéré le serveur de SSH. Le trafic des clients SSH (c'est-à-dire, enferme dans une boîte le SSH courant) au serveur de SSH (le PIX) est chiffré. Quelques clients de la version SSH 1 sont répertoriés dans les notes en version PIX 5.2. Des tests dans notre laboratoire ont été faits avec le SSH F-sécurisé 1.1 sur le NT et la version 1.2.26 pour le Solaris.

Remarque: Pour PIX 7.x, référez-vous à la section laissante d'Access de SSH de gérer le système Access.

Diagramme du réseau



Configurez le SSH authentifié par AAA

Terminez-vous ces étapes pour configurer le SSH authentifié par AAA :

1. Assurez-vous que vous pouvez telnet à PIX avec l'AAA sur mais sans le SSH :`aaa-server AuthOutbound protocol radius (or tacacs+)`
   `aaa authentication telnet console AuthOutbound`
   `aaa-server AuthOutbound host 172.18.124.111 cisco` **Remarque:** Quand le SSH est configuré, la commande de **172.18.124.114 255.255.255.255 de telnet** n'est pas nécessaire parce que l'**intérieur de 172.18.124.114 255.255.255.255 de ssh** est émis sur le PIX. Les deux commandes sont incluses afin de tester.
2. Ajoutez le SSH utilisant ces commandes :`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 l'ordre de la **RSA de mypubkey de l'exposition Ca** en mode de config.`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 un telnet de la station de 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.

Configurez le SSH local (aucune authentification d'AAA)

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

Utilisez ces commandes de configurer le 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 cette organisation est toujours « pix, » puis la commande de se connecter au PIX (c'était 3DES d'un boîtier Solaris) est :

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

Debug de SSH

Debug sans commande de ssh de débogage - 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
```

Debug avec la commande de ssh de débogage - 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"
```

Debug - 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"
```

Debug - DES et 1024-cipher

Remarque: Cette sortie est d'un PC avec le SSH, pas 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 et 2048-cipher

Remarque: Cette sortie est d'un PC avec le SSH, pas 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

Solaris mettent au point - SSH 2048-cipher et de Solaris

Remarque: Solaris n'a pas pu manipuler le 2048-cipher.

```
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 incorrect ou nom d'utilisateur 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 permis par l'intermédiaire de la commande :

ssh 172.18.124.114 255.255.255.255 à l'intérieur

Tentatives de se connecter :

315001 : Session refusée de SSH de 161.44.17.151 sur l'interface à l'intérieur

La clé étant coupée de PIX (utilisant la commande **Ca zéro RSA**) ou non enregistrée avec la **sauvegarde Ca toute la** commande

```
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 d'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 installé pour 3DES mais il y a seulement clé DES dans PIX :

Remarque: Le client était Solaris ne prenant en charge pas le 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 Solaris CLI :

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

Comment retirer la clé RSA de PIX

Ca zéro RSA

Comment sauvegarder la clé RSA à PIX

sauvegarde toute Ca

Comment permettre le SSH du client SSH extérieur

outside_ip *255.255.255.255 de* **ssh dehors**

Authentification d'enable

Avec la commande :

console topix d'enable d'authentification d'AAA

(où le *topix* est notre liste de serveur), l'utilisateur est incité pour un nom d'utilisateur et mot de passe qui est envoyé au serveur TACACS ou de RAYON. Puisque le paquet d'authentification pour l'enable est identique que le paquet d'authentification pour la procédure de connexion, si l'utilisateur peut se connecter dans le PIX avec TACACS ou RAYON, ils peuvent activer par TACACS ou RAYON avec le même nom d'utilisateur/mot de passe.

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

Les informations de Syslogg

Tandis que l'aaa accounting est seulement valide pour des connexions par le PIX, pas au PIX, si syslogging est installé, les informations sur ce que l'utilisateur authentifié a fait est envoyé au serveur de Syslog (et au serveur de Gestion de réseau, si configuré, par le MIB de Syslog).

Si syslogging est installé, alors des messages de ce type sont affichés au serveur de Syslog :

Niveau d'avis de logging trap :

```
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 informatif de logging trap (qui inclut le niveau de notification) :

307002 : Session d'ouverture de connexion permise de telnet de 10.31.1.40

Accédez quand le serveur d'AAA est en panne

Si le serveur d'AAA est en panne, vous pouvez écrire l'accès de mot de passe de telnet le PIX au

commencement, alors **pix** pour le nom d'utilisateur, et puis le mot de passe d'enable (**mot de passe d'enable** *quoi que*) pour le mot de passe. Si le **mot de passe d'enable** *celui qui* ne soit pas dans la configuration PIX, écrivent le **pix** pour le nom d'utilisateur et appuyez sur **entrent**. Si le mot de passe d'enable est placé mais pas connu, vous avez besoin d'une disquette de récupération de mot de passe pour remettre à l'état initial le mot de passe.

Informations à collecter si vous ouvrez un dossier TAC

Si vous avez besoin d'assistance après avoir suivi les étapes de dépannage ci-dessus et voulez toujours ouvrir une valise avec Cisco TAC, soyez sûr d'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
- RAYON TACACS+ PIX
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems