PIX/ASA 7.x : exemple de configuration de SSH/Telnet sur l'interface interne et externe

Table des matières

Introduction

Ce document fournit un exemple de configuration de Secure Shell (SSH) sur les interfaces internes et externes du dispositif de sécurité de la gamme Cisco version 7.x et ultérieure. La configuration à distance de la gamme Appliance de sécurité avec la ligne de commande implique l'utilisation de Telnet ou SSH. Puisque les communications Telnet sont envoyées en texte clair, qui inclut les mots de passe, SSH est fortement recommandé. Le trafic SSH est crypté dans un tunnel et aide à protéger de ce fait les mots de passe et autre commandes de configuration contre une interception.

L'appliance de sécurité permet les connexions SSH à l'appliance de sécurité pour la gestion. L'appliance de sécurité permet un maximum de cinq connexions simultanées de SSH pour chaque contexte de sécurité, si disponible, et un maximum global de 100 connexions pour tous les

contextes combinés.

Dans cet exemple de configuration, l'appliance de sécurité PIX est considérée être le serveur SSH. Le trafic des clients SSH (10.1.1.2/24 et 172.16.1.1/16) au serveur SSH est crypté. L'appliance de sécurité prend en charge la fonctionnalité SSH remote shell fournie dans les versions 1 et 2 de SSH et prend en charge le Data Encryption Standard (DES) et le cryptage 3DES. Les versions SSH 1 et 2 sont différentes et ne sont pas interopérables.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations de ce document sont basées sur le logiciel pare-feu Cisco PIX version 7.1 et 8.0.

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.

Remarque : SSHv2 est pris en charge dans PIX/ASA version 7.x et ultérieures et non pris en charge dans les versions antérieures à 7.x.

Produits connexes

Cette configuration peut également être utilisée avec le logiciel Security Appliance de la gamme Cisco ASA 5500 versions 7.x et ultérieures.

Conventions

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

Configurer

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : chaque étape de configuration est présentée avec les informations nécessaires pour utiliser la ligne de commande ou l'ASDM (Adaptive Security Device Manager).

Remarque : Utilisez l'outil de recherche de commandes (clients enregistrés seulement) pour en savoir plus sur les commandes employées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Configurations SSH

Ce document utilise les configurations suivantes :

- Accès SSH à l'appliance de sécurité
- Comment utiliser un client SSH
- Configuration PIX

Accès SSH à l'appliance de sécurité

Complétez ces étapes afin de configurer l'accès SSH à l'appliance de sécurité :

1. Les sessions SSH exigent toujours un nom utilisateur et un mot de passe pour l'authentification. Il y a deux manières de répondre à cette exigence.

   Configurez un nom utilisateur et un mot de passe et utilisez AAA :

   Syntaxe:

   <#root>

   ```
   pix(config)#
   username username password password
   pix(config)#
   aaa authentication {telnet | ssh | http | serial} console {LOCAL |
   server_group [LOCAL]}
   ```

   Remarque : si vous utilisez un groupe de serveurs TACACS+ ou RADIUS pour l'authentification, vous pouvez configurer l'appliance de sécurité pour utiliser la base de données locale comme méthode de secours si le serveur AAA n'est pas disponible. Spécifiez le nom du groupe de serveurs et puis LOCAL (LOCAL distingue les majuscules et minuscules). Nous recommandons que vous utilisez les mêmes nom utilisateur et mot de passe dans la base de données locale que le serveur AAA, parce que la demande de l'appliance de sécurité ne donne aucune indication sur quelle méthode est utilisée.

   Remarque : exemple :

   <#root>

   ```
   pix(config)#
   aaa authentication ssh console TACACS+ LOCAL
   ```

Remarque : vous pouvez également utiliser la base de données locale comme principale méthode d'authentification sans reprise. Afin de faire ceci, entrez LOCAL seul.

Exemple :

<#root>

```
pix(config)#
aaa authentication ssh console LOCAL
```

OU

Utilisez le nom d'utilisateur par défaut de pix et le mot de passe Telnet par défaut cisco. Vous pouvez changer le mot de passe Telnet avec cette commande :

<#root>

```
pix(config)#
passwd password
```

Remarque : la commande password peut également être utilisée dans cette situation. Les deux commandes font la même chose.

2. Produisez une paire de clés RSA pour le pare-feu PIX, qui est requis pour SSH :

<#root>

```
pix(config)#
crypto key generate rsa modulus modulus_size
```

Remarque : le `module_size` (en bits) peut être 512, 768, 1024 ou 2048. Plus la taille de la clé modulus est grande, plus cela prend de temps pour produire la paire de clés RSA. La valeur de 1024 est recommandée.

Remarque : la commande utilisée pour générer une paire de clés RSA est différente pour les versions du logiciel PIX antérieures à 7.x. Dans les versions antérieures, un nom de domaine doit être défini avant que vous puissiez créer des clés.

Remarque : en mode de contexte multiple, vous devez générer les clés RSA pour chaque contexte. En outre, les commandes crypto ne sont pas supportées dans le mode contexte

système.

3. Spécifiez les hôtes permis pour se connecter à l'appliance de sécurité.

   Cette commande spécifie l'adresse source, le masque de réseau et l'interface du ou des hôtes autorisés à se connecter à SSH. Elle peut être entrée plusieurs fois pour plusieurs hôtes, réseaux ou interfaces. Dans cet exemple, on permet un hôte sur l'intérieur et un hôte sur l'extérieur.

   ```
   <#root>

   pix(config)#

   ssh 172.16.1.1 255.255.255.255 inside

   pix(config)#

   ssh 10.1.1.2 255.255.255.255 outside
   ```

4. Facultatif : par défaut, l'appliance de sécurité autorise les versions 1 et 2 de SSH. Entrez cette commande afin de restreindre les connexions à une version spécifique :

   ```
   <#root>

   pix(config)#

   ssh version
   ```

   Remarque : le `numéro de version` peut être 1 ou 2.

5. Facultatif : par défaut, les sessions SSH sont fermées après cinq minutes d'inactivité. Ce délai d'attente peut être configuré pour durer entre 1 et 60 minutes.

   ```
   <#root>

   pix(config)#

   ssh timeout minutes
   ```

Comment utiliser un client SSH

Fournissez le nom utilisateur et le mot de passe d'ouverture de connexion de l'Appliance de sécurité de la gamme PIX 500 tandis que vous ouvrez la session SSH. Quand vous lancez une

session SSH, un point (.) s'affiche sur la console de l'appliance de sécurité avant que la demande d'authentification des utilisateurs SSH n'apparaisse :

```
hostname(config)# .
```

L'affichage du point n'affecte pas la fonctionnalité de SSH. Le point apparaît à la console quand une clé de serveur est produite ou un message est déchiffré avec des clés privées pendant l'échange de clés SSH avant que l'authentification des utilisateurs ne se produise. Ces tâches peuvent prendre jusqu'à deux minutes ou plus. Le point est un indicateur de progrès qui vérifie que l'appliance de sécurité est occupée et ne s'est pas arrêtée.

Les versions 1.x et 2 de SSH sont des protocoles entièrement différents et ne sont pas compatibles. Téléchargez un client compatible. Référez-vous à la section Obtention d'un SSH client des configurations avancées pour plus d'informations.

Configuration PIX

Ce document utilise la configuration suivante :

Co
<#root> PIX Version 7.1(1) ! hostname pix enable password 8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0 nameif outside security-level 0 ip address 192.168.200.1 255.255.255.0 ! interface Ethernet1 nameif inside security-level 100 ip address 172.16.5.10 255.255.0.0 ! passwd 2KFQnbNIdI.2KYOU encrypted ftp mode passive pager lines 24 mtu outside 1500 mtu inside 1500 no failover icmp permit any outside no asdm history enable arp timeout 14400 route outside 10.1.1.0 255.255.255.0 192.168.200.1 1 timeout xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02

```
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute


!--- AAA for the SSH configuration


username ciscouser password 3USUcOPFUiMCO4Jk encrypted
aaa authentication ssh console LOCAL


http server enable
http 172.16.0.0 255.255.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstar
telnet timeout 5


!--- Enter this command for each address or subnet !--- to identify the IP addresses from which !--- t


ssh 10.1.1.2 255.255.255.255 outside


!--- Allows the users on the host 172.161.1.1 !--- to access the security appliance !--- on the inside


ssh 172.16.1.1 255.255.255.255 inside


!--- Sets the duration from 1 to 60 minutes !--- (default 5 minutes) that the SSH session can be idle,


ssh timeout 60


console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
```

```
  inspect xdmcp
!
service-policy global_policy global
Cryptochecksum:a6b05fd04f9fbd0a39f1ca7328de91f7
: end
```

Remarque : afin d'accéder à l'interface de gestion de l'ASA/PIX en utilisant SSH, émettez cette commande : `ssh 172.16.16.160 255.255.255.255 Management`

Configuration avec ASDM 5.x

Complétez ces étapes afin de configurer le périphérique pour SSH utilisant l'ASDM :

1. Choisissez Configuration > Properties > Device Administration > User Accounts afin d'ajouter un utilisateur avec l'ASDM.
2. Choisissez Configuration > Properties > Device Access > AAA Access > Authentication afin de définir l'authentification AAA pour SSH avec ASDM.
3. Choisissez Configuration > Properties > Device Administration > Password afin de changer le mot de passe Telnet avec ASDM.
4. Choisissez Configuration > Properties > Certificate > Key Pair, cliquez sur Add et utiliser les options par défaut présentées afin de produire les mêmes clés RSA avec ASDM.
5. Choisissez Configuration > Properties > Device Access > Secure Shell afin d'employer ASDM pour spécifier des hôtes permis pour se connecter avec SSH et pour spécifier la version et les options de délai d'attente.
6. Cliquez sur File > Save Running Configuration to Flash afin de sauvegarder la configuration.

Configuration avec ASDM 6.x

Procédez comme suit :

1. Choisissez Configuration > Device Management > Users/AAA > User Accounts afin d'ajouter un utilisateur avec ASDM.
2. Choisissez Configuration > Device Management > Users/AAA > AAA Access > Authentication afin de configurer l'authentification AAA pour SSH avec ASDM.
3. Choisissez Configuration > Device Setup > Device Name/Password afin de changer le mot de passe Telnet avec ASDM.
4. Choisissez Configuration > Device Management > Certificate Management > Identity Certificates, cliquez sur Add et utiliser les options par défaut présentées afin de produire les mêmes clés RSA avec ASDM.

5. Sous Add a new Identity certificate cliquez sur New afin d'ajouter une paire de clés par défaut si aucune n'existe. Puis cliquez sur Generate Now.
6. Choisissez Configuration > Device Management > Management Access > Command Line (CLI) > Secure Shell (SSH) afin d'employer ASDM pour spécifier les hôtes permis pour se connecter avec SSH et pour spécifier les options de version et de délai d'attente.
7. Cliquez sur Save en haut de la fenêtre pour sauvegarder la configuration.
8. Une fois invité à sauvegarder la configuration sur flash, choisissez Apply afin de sauvegarder la configuration.

Configuration Telnet

Afin d'ajouter l'accès Telnet à la console et définir le délai d'attente, émettez la commande telnet dans le mode de configuration globale. Par défaut, les sessions Telnet qui sont laissées en attente pendant cinq minutes sont fermées par l'appliance de sécurité. Afin de supprimer l'accès Telnet d'une adresse IP précédemment définie, employez la forme aucune de cette commande.

<#root>

telnet

{{hostname | IP_address mask interface_name} | {IPv6_address interface_name} | {timeout number}}

no telnet

{{hostname | IP_address mask interface_name} | {IPv6_address interface_name} | {timeout number}}

La commande telnet vous permet de spécifier quels hôtes peuvent accéder à la console de l'appliance de sécurité avec Telnet.

Remarque : vous pouvez activer Telnet sur l'appliance de sécurité sur toutes les interfaces. Cependant, l'appliance de sécurité impose que tout le trafic Telnet à l'interface externe soit protégé par IPsec. Afin d'activer une session Telnet à l'interface externe, configurez IPsec sur l'interface externe pour inclure le trafic IP qui est produit par l'appliance de sécurité et activer Telnet sur l'interface externe.

Remarque : en général, si une interface qui a un niveau de sécurité de 0 ou inférieur à toute autre interface, alors PIX/ASA n'autorise pas Telnet à cette interface.

Remarque : il n'est pas recommandé d'accéder au dispositif de sécurité via une session Telnet. Les informations de créance d'authentification, telles que le mot de passe, sont envoyées en texte clair. Les communications serveur et client Telnet ont lieu seulement en texte clair. Cisco recommande d'utiliser SSH pour une communication de données plus sécurisée.

Si vous entrez une adresse IP, vous devez également entrer un masque de réseau. Il n'y a aucun

masque de réseau par défaut. N'utilisez pas le masque de sous-réseau du réseau interne. Le masque de réseau est seulement un masque de bits pour l'adresse IP. Afin de limiter l'accès à une seule adresse IP, utilisez 255 dans chaque octet ; par exemple, 255.255.255.255.

Si IPsec fonctionne, vous pouvez spécifier un nom d'interface non sécurisé, qui est typiquement l'interface externe. Au minimum, vous pouvez configurer la commande crypto map afin de spécifier un nom d'interface avec la commande telnet.

Émettez la commande password afin de définir un mot de passe pour l'accès Telnet à la console. Le défaut est cisco. Émettez la commande who afin d'afficher quelles adresses IP accèdent actuellement à la console de l'appliance de sécurité. Émettez la commande kill afin de terminer une session de console Telnet active.

Afin d'activer une session Telnet à l'interface interne, passez en revue ces exemples :

Exemple 1

Cet exemple permet seulement à l'hôte 10.1.1.1 d'accéder à la console de l'appliance de sécurité par Telnet :

```
<#root>

pix(config)#

telnet

 10.1.1.1 255.255.255.255 inside
```

Exemple 2

Cet exemple permet seulement au réseau 10.0.0.0/8 d'accéder à la console de l'appliance de sécurité par Telnet :

```
<#root>

pix(config)#

telnet

 10.0.0.0 255.0.0.0 inside
```

Exemple 3

Cet exemple permet à tous les réseaux d'accéder à la console de l'appliance de sécurité par Telnet :

```
<#root>
```

```
pix(config)#
telnet
 0.0.0.0 0.0.0.0 inside
```

Si vous utilisez la commande AAA avec le mot clé console, l'accès à la console par Telnet doit être authentifié avec un serveur d'authentification.

Remarque : si vous avez configuré la commande aaa afin d'exiger l'authentification pour l'accès à la console Telnet de l'appliance de sécurité et que la demande de connexion à la console expire, vous pouvez accéder à l'appliance de sécurité à partir de la console série. Afin de faire ceci, entrez le nom utilisateur et le mot de passe de l'appliance de sécurité qui sont définis avec la commande activer le mot de passe.

Émettez la commande telnet timeout afin de définir la durée maximale du délai d'attente d'une session Telnet de la console avant qu'elle soit déconnectée par l'appliance de sécurité. Vous ne pouvez pas utiliser la commande no telnet avec la commande telnet timeout.

Cet exemple montre comment changer la durée d'attente maximale d'une session :

```
<#root>
hostname(config)#
telnet timeout
 10
hostname(config)#
show running-config
 telnet timeout

telnet timeout
10 minutes
```

Support SSH/Telnet dans l'ACS 4.x

Si vous regardez les fonctions RADIUS, vous pouvez utiliser RADIUS pour la fonctionnalité de SSH.

Quand une tentative est faite pour accéder à l'appliance de sécurité avec une connexion Telnet, SSH, HTTP ou console de série et le trafic correspond à une instruction d'authentification, l'appliance de sécurité demande un nom utilisateur et un mot de passe. Il envoie ensuite ces qualifications au serveur RADIUS (ACS), et accorde ou refuse l'accès CLI basé sur la réponse du serveur.

Référez-vous à la section Support du serveur AAA et de la base de données locale de Configuration des serveurs AAA et de la base de données locale pour plus d'informations.

Par exemple, votre appliance de sécurité ASA 7.0 a besoin d'une adresse IP avec laquelle l'appliance de sécurité accepte des connexions, telles que :

```
<#root>

hostname(config)#

ssh source_IP_address mask source_interface
```

Référez-vous à la section Permettre l'accès SSH de Configuration des serveurs AAA et de la base de données locale pour plus d'informations.

Référez-vous à Exemple de configuration de serveur PIX/ASA : Cut-through Proxy for Network Access using TACACS+ and RADIUS pour plus d'informations sur la façon de configurer l'accès SSH/Telnet à PIX avec l'authentification ACS.

Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Employez l'OIT afin d'afficher une analyse de la sortie de la commande show.

Débogage SSH

Émettez la commande debug ssh afin d'activer le débogage SSH.

```
<#root>

pix(config)#

debug ssh

   SSH debugging on
```

Cette sortie montre que la requête d'authentification de l'hôte 10.1.1.2 (externe à PIX) à « pix » est réussie :

```
<#root>

pix#
    Device ssh opened successfully.
   SSH0: SSH client: IP = '10.1.1.2' interface # = 1
   SSH: host key initialised
```

```
   SSH0: starting SSH control process
   SSH0: Exchanging versions - SSH-1.99-Cisco-1.25
    SSH0: send SSH message: outdata is NULL
            server version string:SSH-1.99-Cisco-1.25SSH0: receive SSH message: 83 (83)
   SSH0: client version is - SSH-1.99-3.2.0 SSH Secure Shell for Windows
            client version string:SSH-1.99-3.2.0 SSH Secure Shell for WindowsSSH0:
begin    ser ver key generation
   SSH0: complete server key generation, elapsed time = 1760 ms
    SSH2 0: SSH2_MSG_KEXINIT sent
   SSH2 0: SSH2_MSG_KEXINIT received
   SSH2: kex: client->server aes128-cbc hmac-md5 none
   SSH2: kex: server->client aes128-cbc hmac-md5 none
   SSH2 0: expecting SSH2_MSG_KEXDH_INIT
   SSH2 0: SSH2_MSG_KEXDH_INIT received
   SSH2 0: signature length 143
   SSH2: kex_derive_keys complete
   SSH2 0: newkeys: mode 1
   SSH2 0: SSH2_MSG_NEWKEYS sent
   SSH2 0: waiting for SSH2_MSG_NEWKEYS
   SSH2 0: newkeys: mode 0
   SSH2 0: SSH2_MSG_NEWKEYS receivedSSH(pix): user authen method is
'no AAA', aaa server group ID = 0
   SSH(pix): user authen method is 'no AAA', aaa server group ID = 0


SSH2 0: authentication successful for pix


!--- Authentication for the PIX was successful.

   SSH2 0: channel open request
   SSH2 0: pty-req request
   SSH2 0: requested tty: vt100, height 25, width 80
    SSH2 0: shell request
   SSH2 0: shell message received
```

Si un utilisateur donne un nom d'utilisateur erroné, par exemple, "pix1" au lieu de « pix », le pare-feu PIX rejette l'authentification. Cette sortie de débogage montre l'échec de l'authentification :

<#root>

```
pix#
Device ssh opened successfully.
SSH0: SSH client: IP = '10.1.1.2' interface # = 1
SSH: host key initialised
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-1.99-Cisco-1.25
SSH0: send SSH message: outdata is NULL
        server version string:SSH-1.99-Cisco-1.25SSH0: receive SSH message: 83 (83)
SSH0: client version is - SSH-1.99-3.2.0 SSH Secure Shell for Windows client version
        string:SSH-1.99-3.2.0 SSH Secure Shell for WindowsSSH0: begin server key generation
SSH0: complete server key generation, elapsed time = 1960 ms
SSH2 0: SSH2_MSG_KEXINIT sent
SSH2 0: SSH2_MSG_KEXINIT received
SSH2: kex: client->server aes128-cbc hmac-md5 none
SSH2: kex: server->client aes128-cbc hmac-md5 none
SSH2 0: expecting SSH2_MSG_KEXDH_INIT
SSH2 0: SSH2_MSG_KEXDH_INIT received
```

```
SSH2 0: signature length 143
SSH2: kex_derive_keys complete
SSH2 0: newkeys: mode 1
SSH2 0: SSH2_MSG_NEWKEYS sent
SSH2 0: waiting for SSH2_MSG_NEWKEYS
SSH2 0: newkeys: mode 0
SSH2 0: SSH2_MSG_NEWKEYS receivedSSH(pix1): user authen method is
'no AAA', aaa server group ID = 0
SSH(pix1): user authen method is 'no AAA', aaa server group ID = 0
```

SSH2 0: authentication failed for pix1

!--- Authentication for pix1 was not successful due to the wrong username.

De même, si l'utilisateur fournit un mot de passe erroné, cette sortie de débogage montre l'échec de l'authentification.

<#root>

```
pix#
Device ssh opened successfully.
SSH0: SSH client: IP = '10.1.1.2'  interface # = 1
SSH: host key initialised
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-1.99-Cisco-1.25
SSH0: send SSH message: outdata is NULL server version string:
SSH-1.99-Cisco-1.25SSH0: receive      SSH message: 83 (83)
SSH0: client version is - SSH-1.99-3.2.0 SSH Secure Shell for
Windows client version string:SSH-1.99-3.2.0
        SSH Secure Shell for WindowsSSH0: begin server key generation
SSH0: complete server key generation, elapsed time = 1920 ms
SSH2 0: SSH2_MSG_KEXINIT sent
SSH2 0: SSH2_MSG_KEXINIT received
SSH2: kex: client->server aes128-cbc hmac-md5 none
SSH2: kex: server->client aes128-cbc hmac-md5 none
SSH2 0: expecting SSH2_MSG_KEXDH_INIT
SSH2 0: SSH2_MSG_KEXDH_INIT received
SSH2 0: signature length 143
SSH2: kex_derive_keys complete
SSH2 0: newkeys: mode 1
SSH2 0: SSH2_MSG_NEWKEYS sent
SSH2 0: waiting for SSH2_MSG_NEWKEYS
SSH2 0: newkeys: mode 0
SSH2 0: SSH2_MSG_NEWKEYS receivedSSH(pix): user authen method
is 'no AAA', aaa server group ID = 0
     SSH(pix): user authen method is 'no AAA', aaa server group ID = 0
SSH2 0: authentication failed for pixSSH(pix): user authen method
is 'no AAA', aaa server group ID = 0
```

SSH2 0: authentication failed for pix

!--- Authentication for PIX was not successful due to the wrong password.

Affichage sessions actives SSH

Émettez cette commande afin de vérifier le nombre de sessions SSH qui sont connectées et l'état de connexion au PIX :

<#root>

```
pix#
```

show ssh session

```
SID Client IP       Version Mode Encryption Hmac     State            Username
0   10.1.1.2        1.99    IN   aes128-cbc md5      SessionStarted   pix
                            OUT  aes128-cbc md5      SessionStarted   pix
```

Choisissez Monitoring > Properties > Device Access > Secure Shell Sessions afin d'afficher les sessions avec ASDM.

Affichage clé publique RSA

Émettez cette commande afin d'afficher la partie publique des clés RSA sur l'appliance de sécurité :

<#root>

```
pix#
```

show crypto key mypubkey rsa

```
Key pair was generated at: 19:36:28 UTC May 19 2006
Key name: <Default-RSA-Key>
 Usage: General Purpose Key
 Modulus Size (bits): 1024
 Key Data:

  30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00c172f4
  95f66c34 2c2ced37 aa3442d8 12158c93 131480dd 967985ab 1d7b92d9 5290f695
  8e9b5b0d d88c0439 6169184c d8fb951c 19023347 d6b3f939 99ac2814 950f4422
  69b67328 f64916b1 82e15341 07590da2 390fbefd 38758888 7319196c de61aef1
  165c4bab 03d081d5 ddaf15cc c9ddb204 c2b451e0 f19ce0f3 485b1d69 8b020301 0001
```

Choisissez Configuration > Properties > Certificate > Key Pair, et cliquez sur Show Details afin d'afficher les clés RSA avec ASDM.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Comment supprimer les clés RSA du PIX

Certaines situations, comme quand vous mettez à niveau le logiciel PIX ou changez la version SSH dans PIX, peuvent vous exiger de supprimer et recréer les clés RSA. Émettez cette commande afin de supprimer la paire de clés RSA du PIX :

<#root>

```
pix(config)#
crypto key zeroize rsa
```

Choisissez Configuration > Properties > Certificate > Key Pair, et cliquez sur Delete afin de supprimer les clés RSA avec ASDM.

La connexion SSH a échoué ?

Message d'erreur sur PIX/ASA :

<#root>

```
%PIX|ASA-3-315004: Fail to establish SSH session because RSA host key retrieval failed.
```

Le message d'erreur correspondant sur l'ordinateur client de SSH :

<#root>

```
Selected cipher type
```

```
not supported by server.
```

Afin de résoudre ce problème, supprimer et recréer les clés RSA. Émettez cette commande afin de supprimer la paire de clés RSA du ASA :

<#root>

```
ASA(config)#
crypto key zeroize rsa
```

Émettez cette commande afin de produire la nouvelle clé :

```
<#root>
ASA(config)#
crypto key generate rsa modulus 1024
```

Incapable d'accéder à l'ASA avec SSH

Message d'erreur :

```
ssh_exchange_identification: read: Connection reset by peer
```

Pour résoudre ce problème, exécutez les étapes suivantes :

1. Rechargez l'ASA ou supprimez toutes les configuration associées SSH et les clés RSA.
2. Reconfigurer les commandes SSH et régénérer les clés RSA.

Impossible d'accéder à l'ASA secondaire en utilisant SSH

Lorsque l'ASA est en mode de basculement, il n'est pas possible d'établir une connexion SSH avec l'ASA de secours via le tunnel VPN. En effet, le trafic de réponse pour le SSH prend l'interface externe de l'ASA en veille.

Informations connexes

- Dispositifs de sécurité de la gamme Cisco PIX 500
- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Logiciels pare-feu Cisco PIX
- Références des commandes du pare-feu Cisco Secure PIX
- Configuration des connexions SSH - Routeurs Cisco et concentrateurs Cisco
- Demandes de commentaires (RFC)
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.