Cómo realizar la autenticación y la activación en Cisco Secure PIX Firewall (de 5.2 a 6.2)

Contenido

Introducción

Este documento describe cómo crear un acceso autenticado AAA a un Firewall PIX que ejecuta desde la versión 5.2 a la 6.2 del software PIX y también contiene información acerca de la habilitación de la autenticación, el registro del sistema y la obtención de acceso cuando el servidor AAA no está conectado. En PIX 5.3 y posteriores, el cambio en relación a la autenticación, autorización y contabilidad (AAA) respecto de las versiones de código anteriores es

que los puertos RADIUS son configurables.

En las versiones 5.2 y posteriores del software PIX se puede crear un acceso autenticado AAA al PIX de cinco maneras diferentes.

- Autenticación Telnet - Interna
- Autenticación del puerto de consola
- Authenticated Cisco Secure VPN Client 1.1 (Cliente de VPN seguro autenticado 1.1 de Cisco) – Fuera
- VPN 3000 2.5 autenticado - Fuera
- Shell seguro autenticado (SSH): interior o exterior

Nota: DES o 3DES deben estar habilitados en el PIX (ejecute un comando **show version** para verificar) para los últimos tres métodos. En la versión 6.0 y posterior del software PIX, el PIX Device Manager (PDM) también se puede cargar para habilitar la administración de la GUI. PDM está fuera del alcance de este documento.

Para obtener más información sobre el comando authentication and authorization para PIX 6.2, consulte PIX 6.2 : Ejemplo de Configuración de Comandos de Autenticación y Autorización.

Para crear acceso autenticado AAA (Proxy de Corte) a un Firewall PIX que ejecute las versiones 6.3 y posteriores del software PIX, consulte PIX/ASA : Ejemplo de Configuración de Proxy de Corte para Acceso a Red con TACACS+ y Servidor RADIUS.

Prerequisites

Requirements

Realice estas tareas antes de agregar autenticación AAA:

- Ejecute estos comandos para agregar una contraseña para el PIX:**passwd wwtelnet <local_ip> [<mask>] [<if_name>]**El PIX cifra automáticamente esta contraseña para formar una cadena cifrada con la palabra clave **encriptada**, como en este ejemplo:
  ```
  passwd OnTrBUG1Tp0edmkr encrypted
  ```
  No es necesario que agregue la palabra clave cifrada.
- Asegúrese de que puede Telnet desde la red interna a la interfaz interna del PIX *sin* autenticación AAA después de agregar estas sentencias.
- Tenga siempre una conexión abierta al PIX mientras agrega sentencias de autenticación en el caso de que sea necesario realizar una copia de seguridad de los comandos.

En la autenticación AAA (que no sea SSH donde la secuencia depende del cliente), el usuario ve una solicitud para la contraseña PIX (como en *passwd <any>*), luego una solicitud para el nombre de usuario y la contraseña RADIUS o TACACS.

Nota: No puede realizar Telnet a la interfaz exterior de PIX. SSH se puede utilizar en la interfaz exterior si se conecta desde un cliente SSH externo.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Software PIX versión 5.2, 5.3, 6.0, 6.1 ó 6.2
- Secure VPN Client 1.1 de Cisco
- Cliente Cisco VPN 3000 2.5
- Cisco VPN Client 3.0.x (se requiere código PIX 6.0)

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.

Puertos RADIUS configurables (5.3 y posteriores)

Algunos servidores RADIUS utilizan puertos RADIUS diferentes a 1645/1646 (generalmente 1812/1813). En PIX 5.3, los puertos de autenticación y contabilización RADIUS se pueden cambiar a un valor distinto del 1645/1646 predeterminado con estos comandos:

aaa-server radius-authport

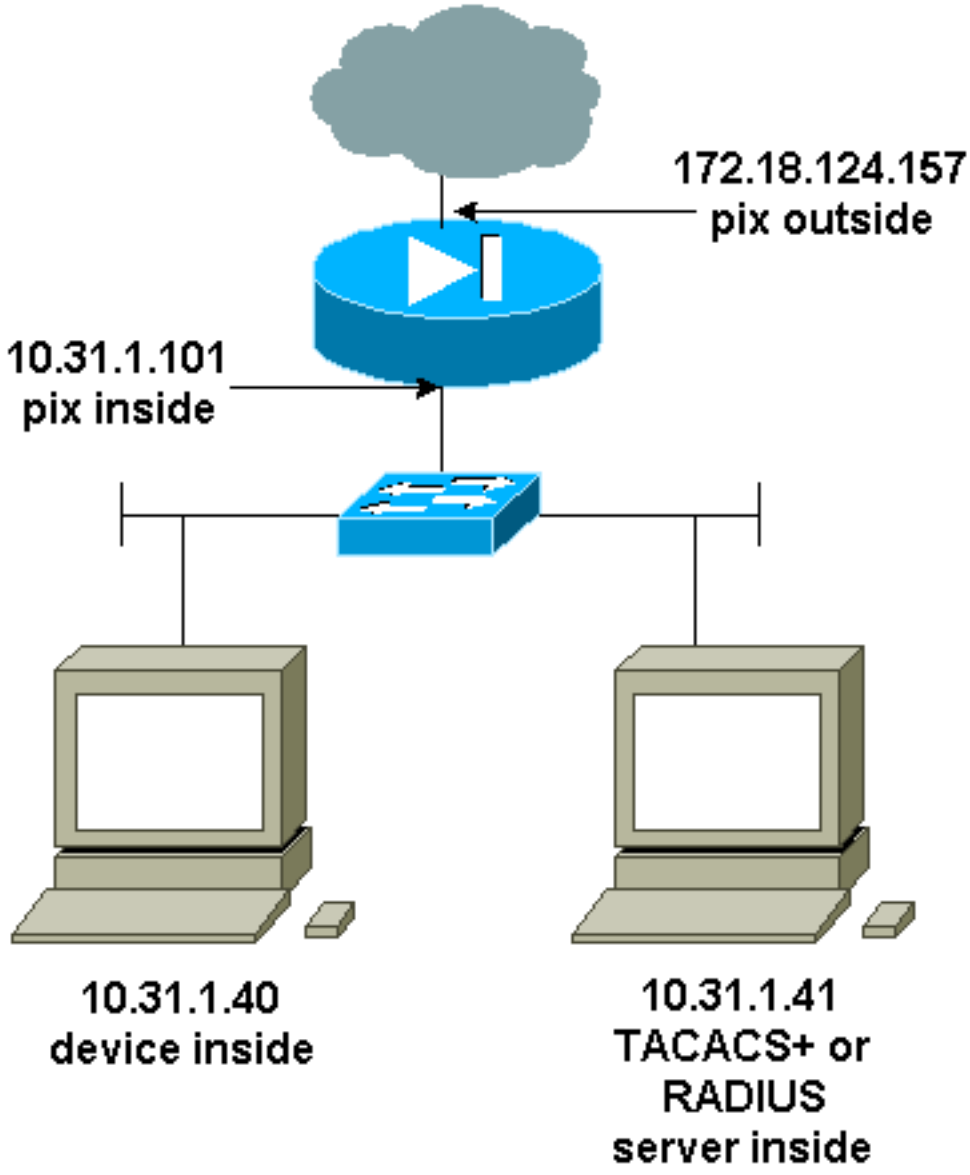
aaa-server radius-acctport #

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Autenticación Telnet - Interna

Diagrama de la red



Comandos agregados a la configuración de PIX

Agregue estos comandos a su configuración:

aaa-server topix protocol tacacs+

aaa-server topix host 10.31.1.41 tiempo de espera de cisco 5

aaa authentication telnet console topix

El usuario ve una solicitud para la contraseña de PIX (como en `passwd <any>`), y luego una solicitud para el nombre de usuario y la contraseña de RADIUS o TACACS (almacenados en el servidor TACACS 10.31.1.41 o RADIUS).

Autenticación del puerto de consola

Agregue estos comandos a su configuración:

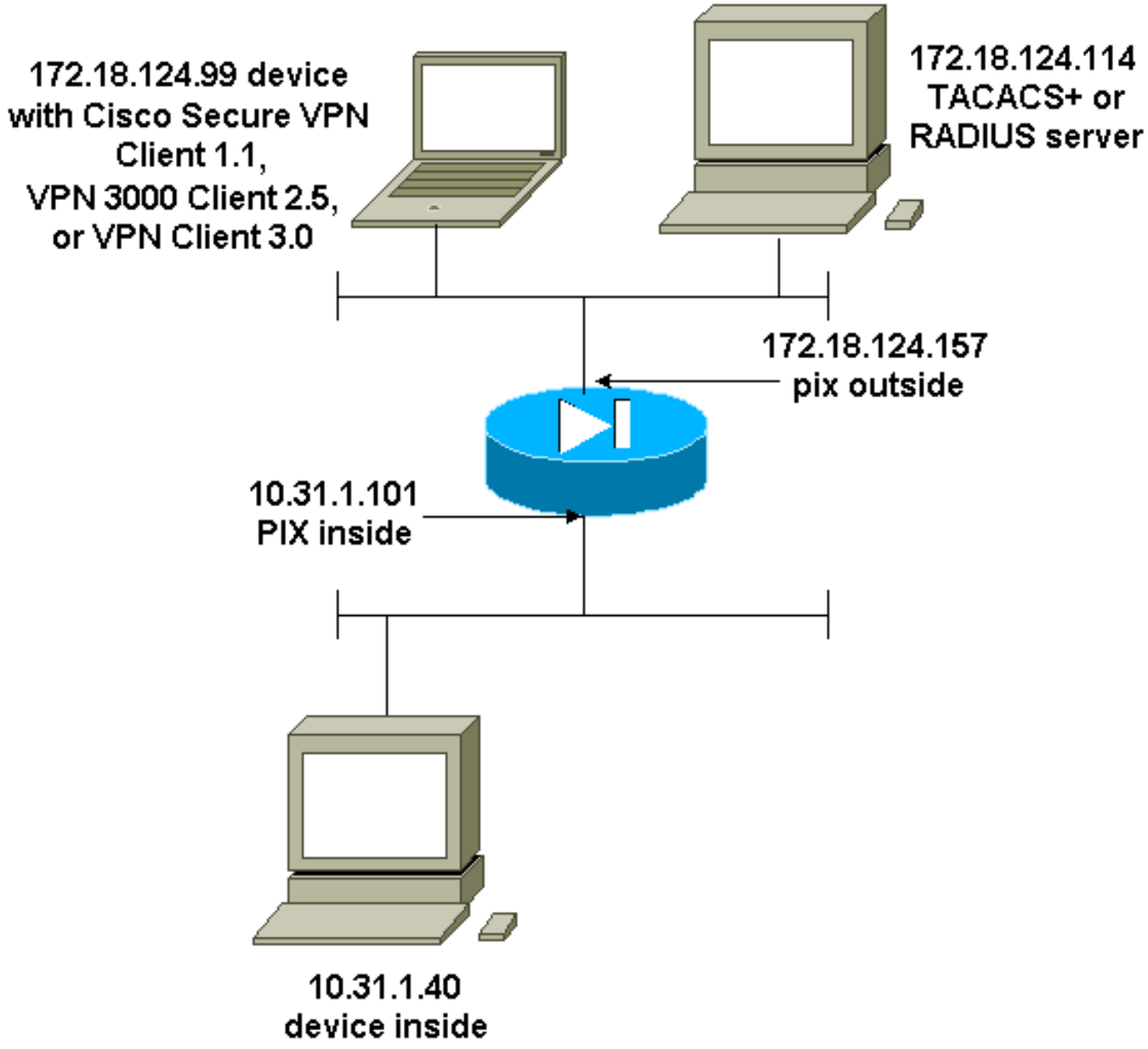
aaa-server topix protocol tacacs+

aaa-server topix host 10.31.1.41 tiempo de espera de cisco 5

aaa authentication serial console topix

El usuario ve una solicitud para la contraseña PIX (como en `passwd <any>`), luego una solicitud para el nombre de usuario/contraseña RADIUS/TACACS (almacenado en el servidor RADIUS o TACACS 10.31.1.41).

Diagrama - VPN Client 1.1, VPN 3000 2.5 o VPN Client 3.0 - Fuera



Authenticated Cisco Secure VPN Client 1.1 (Cliente de VPN seguro autenticado 1.1 de Cisco) – Fuera

Cisco Secure VPN Client 1.1 autenticado - Fuera - Configuración cliente
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 autenticado - Fuera - Configuración de PIX parcial

```
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
```

Authenticated VPN 3000 2.5 o VPN Client 3.0 - Fuera

VPN 3000 2.5 con autenticación o Cliente VPN 3.0 - Externo- Configuración del

cliente

1. Seleccione **VPN Dialer > Properties > Name the connection** from the VPN 3000.
2. Seleccione **Authentication > Group Access Information**. El nombre de grupo y la contraseña deben coincidir con lo que está en el PIX en la instrucción **vpngroup <*group_name*> password *******.

Cuando hace clic en Connect (Conectar), aparece el túnel de encripción y el PIX asigna una dirección IP desde la agrupación de prueba (con el cliente VPN 3000 sólo se admite la configuración del modo). Luego puede activar la ventana del terminal, y realizar una conexión Telnet a 172.18.124.157 y una autenticación AAA. El comando telnet 192.168.1.x en el PIX permite la conexión de usuarios en la agrupación hacia la interfaz exterior.

VPN 3000 2.5 autenticado - Exterior - Configuración parcial 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
```

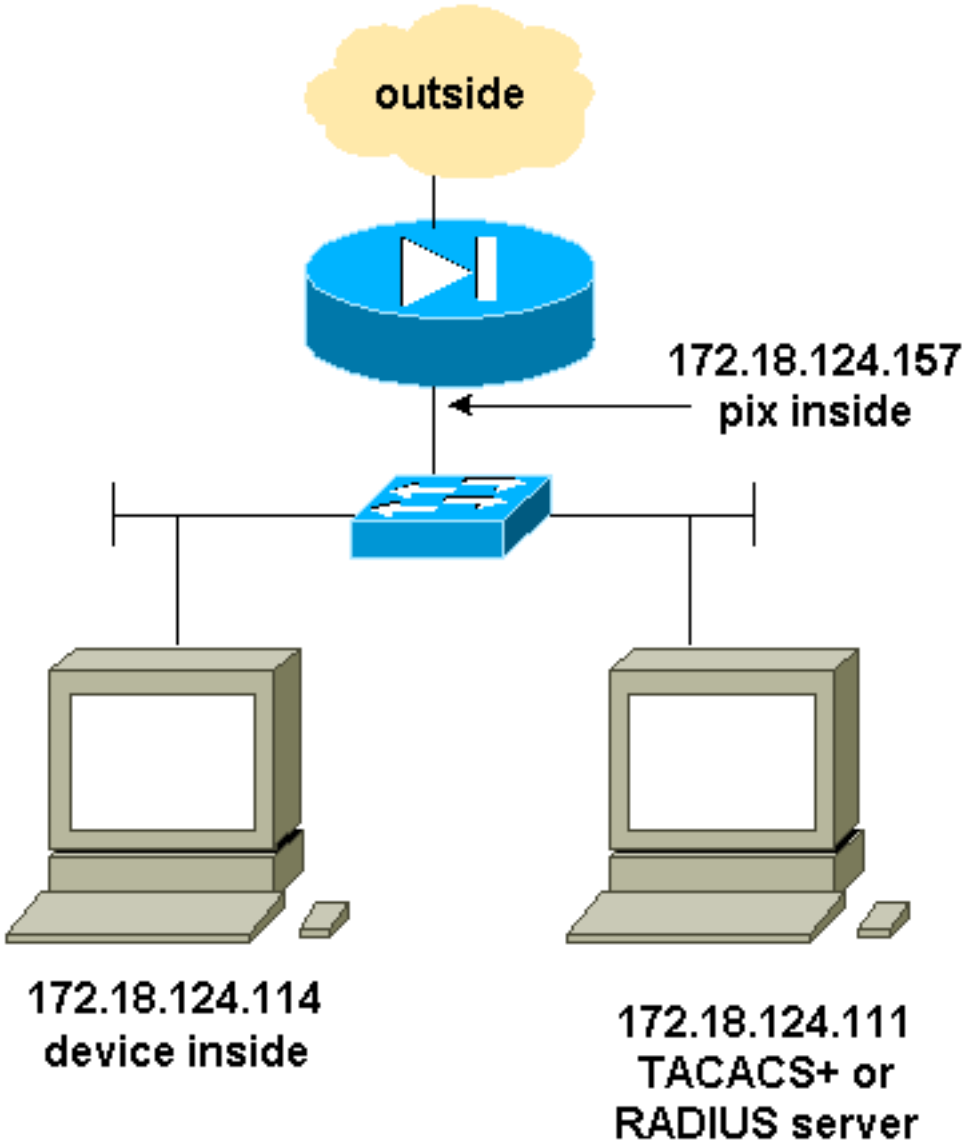
SSH - Dentro o Fuera

PIX 5.2 agregó soporte de Secure Shell (SSH) versión 1. SSH 1 se basa en un borrador IETF de noviembre de 1995. Las versiones 1 y 2 de SSH no son compatibles entre sí. Consulte Preguntas Frecuentes de Secure Shell (SSH) para obtener más información sobre SSH.

El PIX se considera el servidor SSH. El tráfico de los clientes SSH (es decir, las cajas que ejecutan SSH) al servidor SSH (el PIX) está cifrado. Algunos clientes de la versión 1 de SSH se enumeran en las notas de la versión del PIX 5.2. Las pruebas en nuestro laboratorio se realizaron con F-secure SSH 1.1 en NT y en la versión 1.2.26 de Solaris.

Nota: Para PIX 7.x, consulte la sección Cómo Permitir el Acceso SSH de Administración del Acceso al Sistema.

Diagrama de la red



Configuración de AAA Authenticated SSH

Complete estos pasos para configurar el SSH autenticado AAA:

1. Asegúrese de que puede Telnet a PIX con AAA en pero sin SSH:
   ```
   aaa-server AuthOutbound protocol radius (or tacacs+)
   aaa authentication telnet console AuthOutbound
   aaa-server AuthOutbound host 172.18.124.111 cisco
   ```
   Nota: Cuando se configura SSH, el **comando telnet 172.18.124.114 255.255.255.255** no es necesario porque el **ssh 172.18.124.114 255 255.255.255 interno** se ejecuta en el PIX. Ambos comandos se incluyen con fines de prueba.
2. Agregue SSH usando estos comandos:
   ```
   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. Ejecute el comando **show ca mypubkey rsa** en el modo 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. Pruebe una Telnet desde la estación Solaris:

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

Nota: "cisco" es el nombre de usuario en el servidor RADIUS/TACACS+ y 172.18.124.157 es el destino.

Configuración de SSH local (sin autenticación AAA)

También es posible configurar una conexión SSH al PIX con autenticación local y sin servidor AAA. Sin embargo, no hay un nombre de usuario por usuario discreto. El nombre de usuario siempre es "pix".

Utilice estos comandos para configurar el SSH local en el 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
```

Dado que el nombre de usuario predeterminado en esta disposición es siempre "pix," el comando para conectar a PIX (3DES en una caja Solaris) es:

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

Depuración SSH

Depurar sin el comando debug ssh - 3DES y 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
```

Depurar con el comando debug ssh - 3DES y 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"
```

Depuración: 3DES y 1024 cifras

```
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"
```

Depuración: DES y cifra 1024

Nota: Esta salida proviene de un PC con SSH, no 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"
```

Depuración: 3DES y cifra 2048

Nota: Esta salida proviene de un PC con SSH, no 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"
```

Qué Puede Salir Mal

Solaris debug - 2048-cipher y Solaris SSH

Nota: Solaris no pudo manejar el 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).
```

Contraseña o nombre de usuario incorrectos en el servidor 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
```

Usuario no permitido a través del comando:

ssh 172.18.124.114 255.255.255.255 dentro

Intentos de conexión:

315001: Sesión SSH denegada de 161.44.17.151 en interfaz interna

Con la clave eliminada del PIX (utilizando el comando ca zero rsa) o no guardada con el comando 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)
```

El servidor AAA no funciona:

```
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
```

El cliente está configurado para 3DES pero sólo hay una clave DES en PIX.

Nota: El cliente no era Solaris compatible con 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)
```

y en Solaris CLI:

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

Cómo quitar la clave RSA de PIX

ca zero rsa

Cómo guardar la clave RSA a PIX

ca save all

Cómo permitir SSH desde fuera del Cliente SSH

ssh outside_ip 255.255.255.255 outside

Habilitar autenticación

Con el comando:

aaa authentication enable console topix

(cuando topix está en nuestra lista de servidor) se le pide al usuario el nombre de usuario y la contraseña lo que se envía al servidor TACACS o RADIUS. Como el paquete de autenticación para la habilitación es el mismo que el paquete de autenticación para el inicio de sesión, si el usuario puede conectarse dentro del PIX con TACACS o RADIUS, pueden habilitarse a través de TACACS o RADIUS con el mismo nombre de usuario y contraseña.

Más información sobre estos problemas está disponible en el Id. de bug Cisco CSCdm47044 (sólo clientes registrados) .

Información de Syslogg

Si bien la contabilidad AAA sólo es válida para conexiones a través de PIX, y no al PIX, en caso de que syslogging se encuentre configurado, la información sobre lo que ha hecho el usuario autenticado es enviada al servidor syslog (y al servidor de administrador de red, si se encuentra configurado, a través del MIB del servidor de registro).

Si se configura syslogging, los mensajes como estos se muestran en el servidor syslog:

Nivel de notificación 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.
```

Nivel informativo de trampa de registro (que incluye el nivel de notificación):

307002: Sesión de inicio Telnet permitida desde 10.31.1.40

Obtener acceso cuando el servidor AAA está inactivo

Si el servidor AAA está inactivo, puede ingresar la contraseña Telnet acceder al PIX inicialmente, luego **pix** para el nombre de usuario y luego la contraseña de habilitación (**habilitar contraseña *lo que sea***) para la contraseña. Si enable password lo que sea no se encuentra en la configuración PIX, ingrese pix para el nombre de usuario y presione Enter (Aceptar). Si la contraseña de activación está establecida pero no se conoce, necesita un disco de recuperación de contraseña para restablecer la contraseña.

Información para recopilar si abre un caso del TAC

Si todavía necesita ayuda después de seguir los pasos de solución de problemas anteriores y desea abrir un caso con el TAC de Cisco, asegúrese de incluir la siguiente información.
• Descripción del problema y detalles relevantes de la topología • Trobleshooting realizado antes de abrir el caso • Resultado del comando show tech-support • Resultado del comando show log después de la ejecución con el comando logging buffered debugging o capturas de consola que muestran el problema (si están disponibles) Adjunte los datos recolectados a su caso en un texto sin formato (.txt), sin compactar. Puede vincular información a su caso transfiriéndola mediante la herramienta Case Query (sólo para clientes registrados) . Si no puede acceder a la herramienta Case Query Tool, puede enviar la información en un archivo adjunto de correo electrónico a attach@cisco.com con su número de caso en el asunto del mensaje.

Información Relacionada

- Referencias de Comandos de Cisco Secure PIX Firewall
- PIX RADIUS TACACS+