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 autenticado 3000 2.5 - Afuera
- Secure Shell autenticado (SSH) - Interno o externo

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

Para más información sobre el comando de la autenticación y autorización para PIX 6.2, refiera a PIX 6.2: Ejemplo del comando Configuration de la autenticación y autorización.

Para crear (Corte-por el proxy) el acceso AAA-autenticado a un firewall PIX que funciona con las versiones de software PIX 6.3 y posterior, refiera al PIX/ASA: Corte-por el proxy para el acceso a la red usando el TACACS+ y el ejemplo de la configuración de servidor de RADIUS.

prerrequisitos

Requisitos

Realice estas tareas antes de que usted agregue la autenticación AAA:

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

En la autenticación AAA (con excepción de SSH donde la secuencia depende del cliente), el usuario ve una petición para la contraseña de PIX (como en el *<whatever> del passwd*), después una petición para nombre de usuario y contraseña de RADIUS o TACACS.

Nota: Usted no puede Telnet a la interfaz exterior del PIX. SSH se puede utilizar en la interfaz exterior si está conectado de un cliente SSH exterior.

Componentes Utilizados

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

- Versión de software PIX 5.2, 5.3, 6.0, 6.1, o 6.2
- Secure VPN Client 1.1 de Cisco
- Cliente Cisco VPN 3000 2.5
- Cliente Cisco VPN 3.0.x (código PIX 6.0 requerido)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Puertos RADIUS configurables (5.3 y posteriores)

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

aaa-server radius-authport

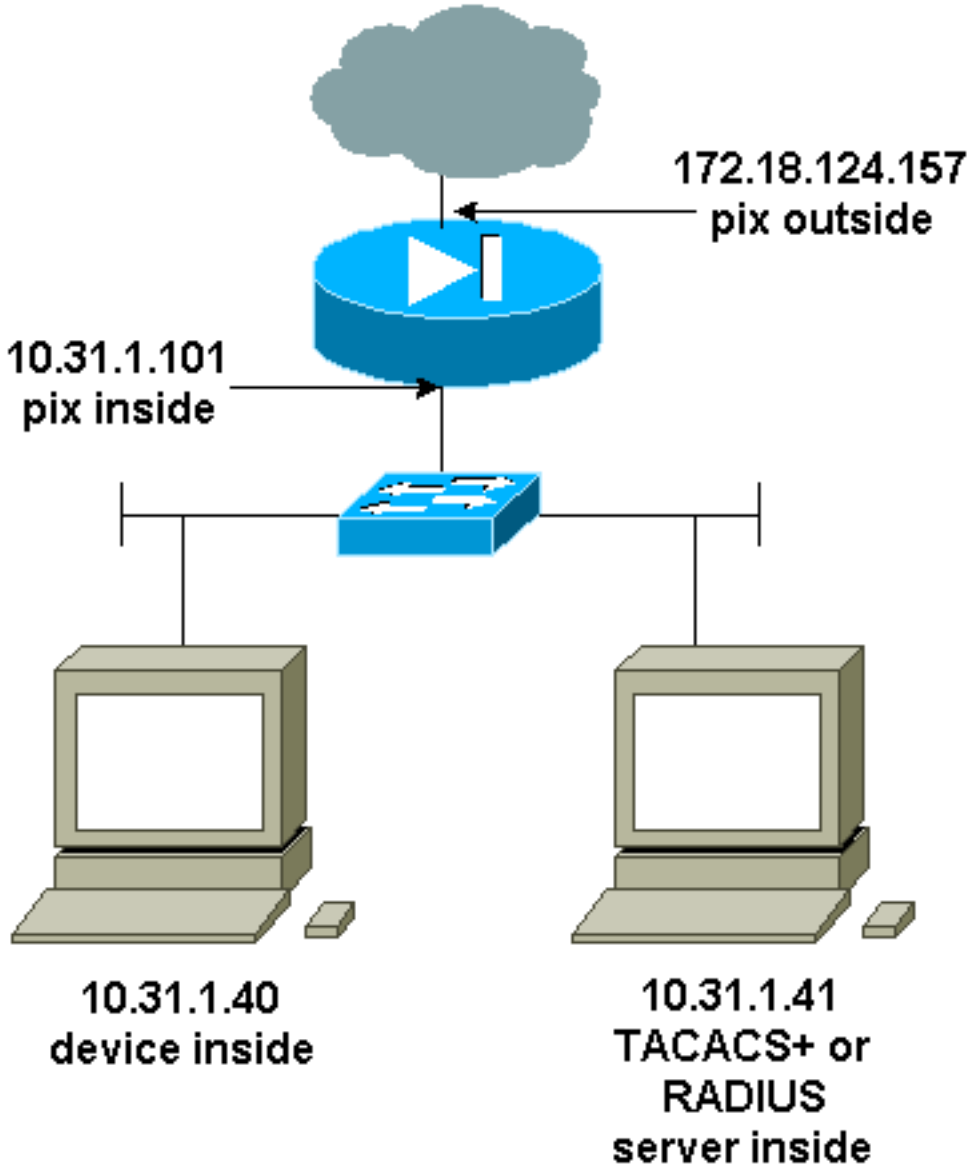
aaa-server radius-acctport #

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+

tiempo de espera agotado de Cisco 5 de 10.31.1.41 del host servidor AAA topix

consola Telnet de autenticación AAA topix

El usuario ve una petición para la contraseña de PIX (como en el `<whatever> del passwd`), y entonces una petición para nombre de usuario y contraseña de RADIUS o TACACS (salvado en 10.31.1.41 TACACS o servidor de RADIUS).

Autenticación del puerto de consola

Agregue estos comandos a su configuración:

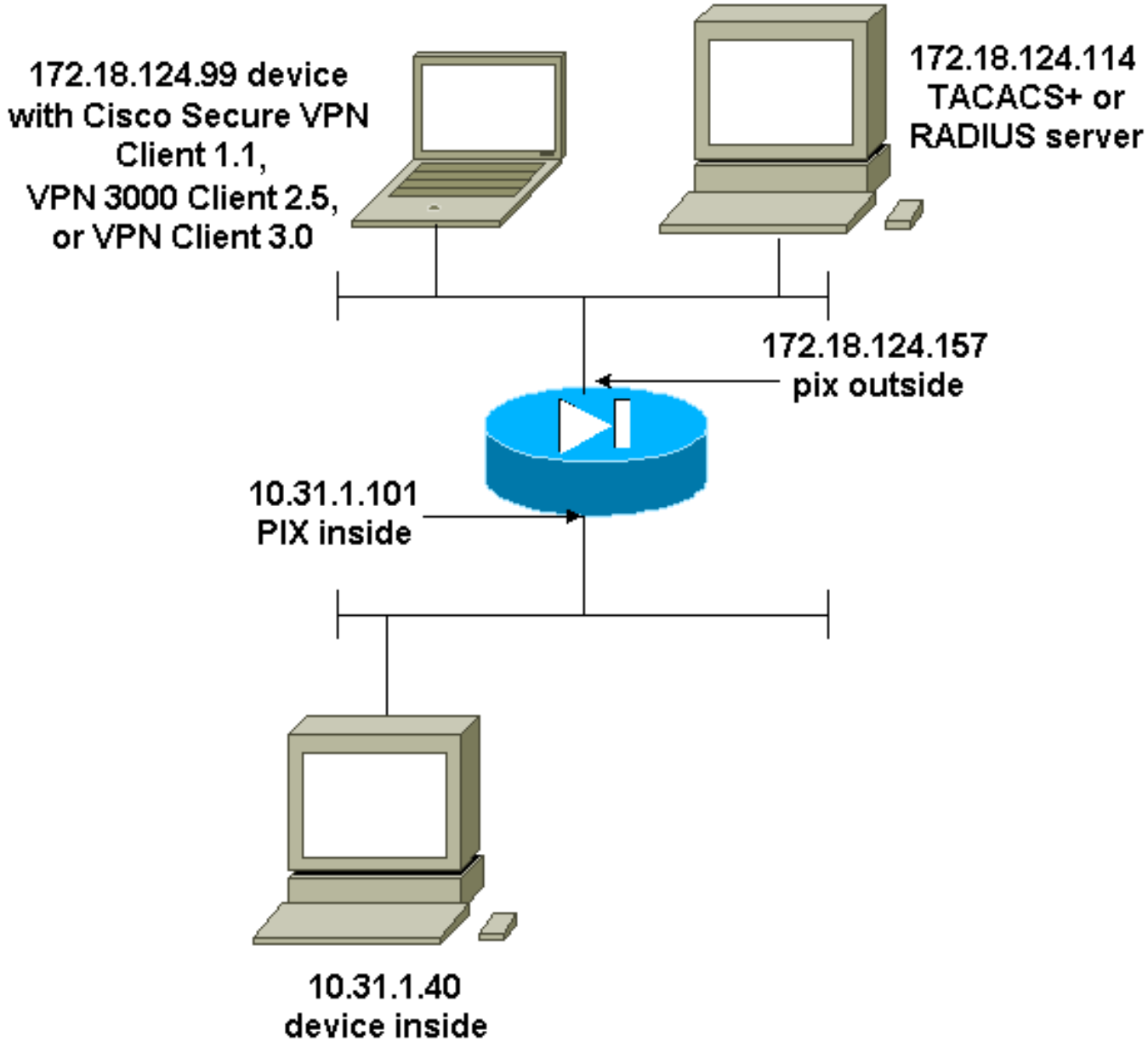
aaa-server topix protocol tacacs+

tiempo de espera agotado de Cisco 5 de 10.31.1.41 del host servidor AAA topix

topix de la consola Telnet en serie de autenticación AAA

El usuario ve una petición para la contraseña de PIX (como en el `<whatever> del passwd`), después un pedido el nombre de usuario/la contraseña RADIUS/TACACS (salvados en el servidor de 10.31.1.41 del radius or tacacs).

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 el **dialer VPN > las propiedades > el nombre la conexión del** VPN 3000.
2. Seleccione la **autenticación > la información de acceso a grupo**. El nombre del grupo y la contraseña deben hacer juego cuál está en el PIX en la declaración del ********** del <group_name > de la contraseña del vpngroup**.

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 autenticado 3000 2.5 - Fuera de - 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
```

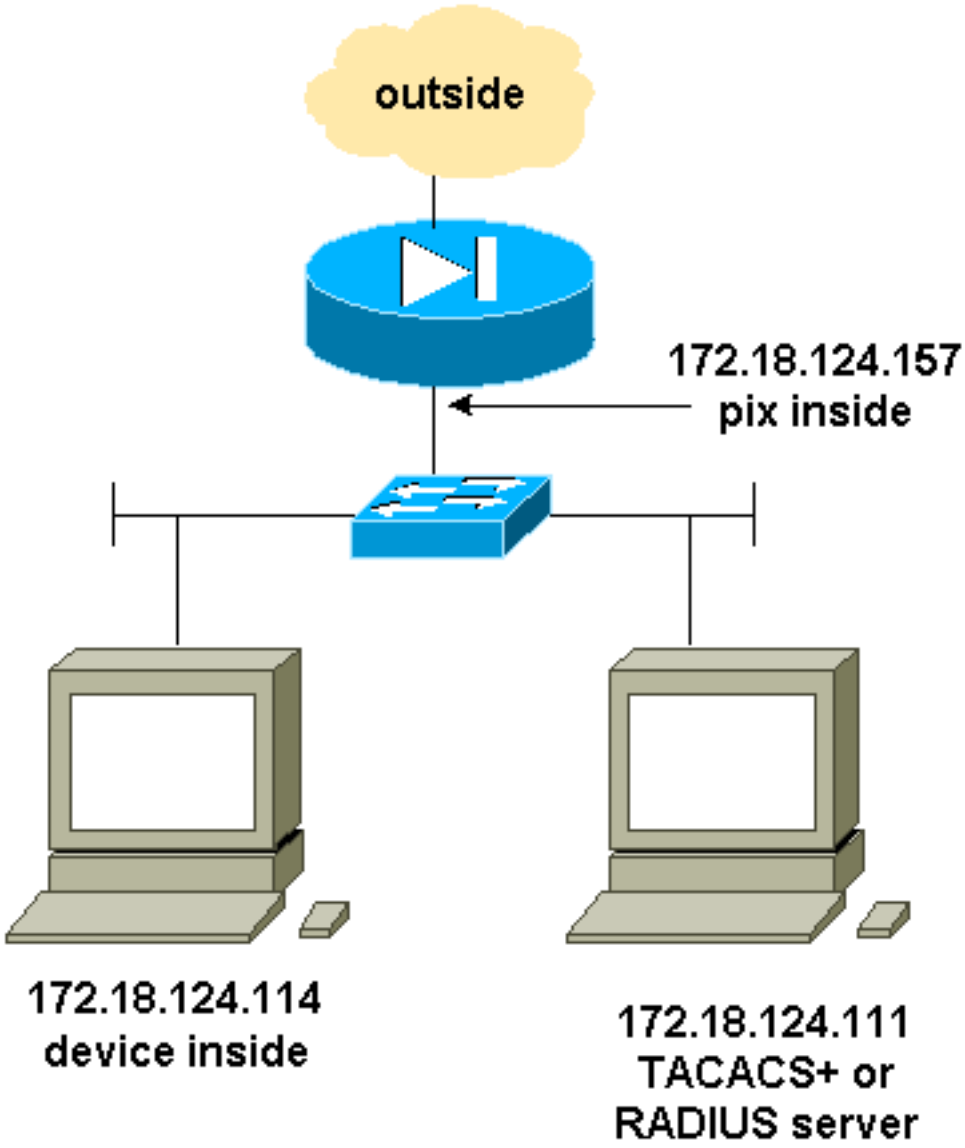
SSH - Interno o externo

Soporte agregado de la versión 1 del Secure Shell (SSH) PIX 5.2. El SSH1 se basa en un noviembre de 1995, borrador IETF. El SSH versión 1 y 2 no es compatible con uno a. Refiera a las preguntas frecuentes del Secure Shell (SSH) para más información sobre SSH.

El PIX se considera el servidor SSH. El tráfico de los clientes SSH (es decir, cuadros que ejecutan SSH) al servidor SSH (el PIX) se cifra. 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, refiera a la sección del acceso de SSH que permite manejo del acceso al sistema.

Diagrama de la red



Ssh con autenticación AAA de la configuración

Complete estos pasos para configurar el ssh con autenticación AAA:

1. Aseegurese le puede Telnet al PIX con el 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 **interior de 172.18.124.114 255.255.255.255 del ssh** se publica en el PIX. Incluyen a los comandos both para comprobar.
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. Publique el **comando show ca mypubkey rsa** en el modo de configuración.

```
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. Intente Telnet de la estación de 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 SSH local (ninguna autenticación AAA)

Es también posible configurar una conexión SSH al PIX con la autenticación local y ningún servidor de AAA. Sin embargo, no hay nombre de usuario discreto por usuario. El nombre de usuario es siempre “pix.”

Utilice estos comandos de configurar 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:

```
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
```

Depuración SSH

Debug sin el comando debug ssh - 3DES y 512-cipher

```
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
```

Debug 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"
```

Debug - 3DES y 1024-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 - DES y 1024-cipher

Nota: Este resultado proviene de una PC con SSH, no con Solaris.

```
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 y 2048-cipher

Nota: Este resultado proviene de una PC con SSH, no con Solaris.

```
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"
```

Qué Puede Salir Mal

Debug de Solaris - 2048-cipher y Solaris SSH

Nota: Solaris no pudo manejar el 2048-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"
```

Contraseña incorrecta o nombre de usuario en el servidor RADIUS/TACACS+

```
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"
```

Usuario no permitido a través del comando:

ssh 172.18.124.114 255.255.255.255 dentro

Tentativas de conectar:

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

```
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"
```

El servidor de AAA está abajo:

```
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"
```

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

Nota: El cliente era Solaris que no soportaba el DES.

```
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"
```

y en nuestro Solaris CLI:

```
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"
```

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:

topix de la consola del permiso de la autenticación aaa

(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 (clientes registrados solamente).

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 el syslogging, después los mensajes tales como éstos se visualizan en el servidor de Syslog:

Nivel de notificación de logging trap:

```
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"
```

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

307002: Sesión de inicio Telnet permitida desde 10.31.1.40

Acceda cuando el servidor de AAA está abajo

Si el servidor de AAA está abajo, usted puede inicialmente, después ingresar el acceso de la contraseña de Telnet el PIX **pix** para el nombre de usuario, y entonces la contraseña habilitada (**contraseña habilitada *sea cual 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 se fija pero no se sabe la contraseña habilitada, usted necesita un disco de recuperación de contraseña reajustar la contraseña.

Información para recopilar si abre un caso del TAC

Si usted todavía necesita la ayuda después de seguir los pasos de Troubleshooting arriba y quiere abrir un caso con el TAC de Cisco, esté seguro 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 usted no puede acceder la herramienta del Case Query, usted puede enviar la información en un elemento adjunto de correo electrónico a attach@cisco.com con su número de caso en el asunto de su mensaje.

Información Relacionada

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