PIX 6.2: Ejemplo del comando Configuration de la autenticación y autorización

Contenido

Introducción

En la versión 6.2, se introdujeron la autorización del comando PIX y la expansión de la autenticación local. Este documento ofrece un ejemplo de cómo establecer esto para que funcione en un PIX. Las funciones de autenticación previamente disponibles continúan estando disponibles pero no se explican en este documento (por ejemplo, Secure Shell (SSH), conexión del cliente IPSec desde un PC, etc.). Los comandos ejecutados pueden ser controlados de manera local en el PIX o de manera remota a través de TACACS+. La autorización del comando RADIUS no se admite; esta es una limitación del protocolo RADIUS.

La autorización de comandos locales se realiza a través de la asignación de comandos y usuarios a niveles de privilegios.

La autorización para el comando remoto se otorga a través de un servidor TACACS+ de Autenticación, autorización y contabilidad (AAA). Es posible definir múltiples servidores AAA en el evento en el que uno sea inalcanzable.

La autenticación también funciona con conexiones SSH y IPSec configuradas previamente. La autenticación SSH requiere que usted publique este comando:

```
aaa authentication ssh console <LOCAL | server_tag>
```

Nota: Si usted utiliza un TACACS+ o a un grupo de servidor de RADIUS para la autenticación, usted puede configurar el PIX para utilizar la base de datos local como método del **RETRASO** si el servidor de AAA es inasequible.

Por ejemplo

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

Usted puede alternativamente utilizar la base de datos local como su método principal de autenticación (sin el retraso) si usted ingresa solo LOCAL.

Por ejemplo, publique este comando para definir una cuenta de usuario en la base de datos local y realizar la autenticación local para una conexión SSH:

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

Refiérase a cómo realizar la autenticación y habilitación en el Firewall PIX (5.2 a través de 6.2) para más información sobre cómo crear el acceso autenticado AAA a un firewall PIX que funciona con la versión de software PIX 5.2 a 6.2 y para más información sobre la autenticación, el syslogging, y el acceso del permiso cuando el servidor de AAA está abajo.

Consulte 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 para más información sobre cómo crear AAA-autenticó (Corte-por el proxy) el acceso a un firewall PIX que funciona con las versiones de software PIX 6.3 y posterior.

Si la configuración se lleva a cabo correctamente, no debería prohibírsele el acceso a PIX. Si la configuración no se guarda, reiniciar el PIX debe volverlo a su estado de la PRE-configuración. Si no es posible acceder al PIX debido a un error de configuración, consulte el procedimiento de recuperación de contraseña y recuperación de configuración AAA para PIX.

Antes de comenzar

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

prerrequisitos

No hay requisitos previos específicos para este documento.

Componentes Utilizados

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

hardware.

- Versión 6.2 del software PIX
- 3.0 de la versión del Cisco Secure ACS for Windows (ACS)
- Cisco Secure ACS para la versión 2.3.6 de UNIX (CSUnix)

La información que se presenta en este documento se originó a partir de dispositivos dentro de 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 un comando antes de ejecutarlo.

Prueba previa al agregado de autenticación/autorización

Antes de implementar las nuevas 6.2 características de la autenticación/de la autorización, aseegurese que usted puede actualmente acceder al PIX usando estos comandos:

```
!--- IP range allowed to Telnet to the PIX (values depend on network). telnet 172.18.124.0
255.255.255.0
!--- Telnet password. passwd <password>
!--- Enable password. enable password <password>
```

Comprensión de configuración de privilegios

La mayoría de los comandos en el PIX están en el nivel 15, aunque algunos estén en el nivel 0. Para ver las configuraciones actuales para los comandos all, utilice este comando:

```
show privilege all
```

La mayoría de los comandos están en el nivel 15 por abandono, tal y como se muestra en de este ejemplo:

```
privilege configure level 15 command route
```

Algunos comandos están en el nivel 0, tal y como se muestra en de este ejemplo:

```
privilege show level 0 command curpriv
```

El PIX puede actuar en el permiso y configurar los modos. Algunos comandos, tales como **registro de la demostración**, están disponibles en los modos Both. Para fijar los privilegios en estos comandos, usted debe especificar el modo que existe el comando adentro, tal y como se muestra en del ejemplo. La otra opción de modo es **permiso**. Usted consigue el `registro es un comando disponible en el` mensaje de error de los `modos múltiples`. Si usted no configura el modo, utilice el **modo [permiso|**comando de la **configuración]**:

```
privilege show level 5 mode configure command logging
```

Estos ejemplos se dirigen al **comando clock**. Utilice este comando de determinar las configuraciones actuales para el **comando clock**:

```
show privilege command clock
```

La salida del **comando clock del comando show privilege** muestra que el **comando clock** existe en estos tres formatos:

```
!--- Users at level 15 can use the show clock command.

privilege show level 15 command clock
!--- Users at level 15 can use the clear clock command.

Privilege clear level 15 command clock
!--- Users at level 15 can configure the clock !--- (for example, clock set 12:00:00 Jan 01
2001).

privilege configure level 15 command clock
```

Autenticación/Autorización – Nombres de usuarios locales

Antes de cambiar el nivel de privilegio del **comando clock**, usted debe ir al puerto de la consola a configurar a un usuario administrador y a girar la autenticación de conexión local, tal y como se muestra en de este ejemplo:

```
GOSS(config)# username poweruser password poweruser privilege 15
GOSS(config)# aaa-server LOCAL protocol local
GOSS(config)# aaa authentication telnet console LOCAL
```

El PIX confirma la adición del usuario, tal y como se muestra en de este ejemplo:

```
GOSS(config)# 502101: New user added to local dbase:
      Uname: poweruser Priv: 15 Encpass: Nimjl8wRa7VAmpm5
```

El usuario “poweruser” debe poder a Telnet en el PIX y el permiso con la contraseña habilitada existente del PIX local (la que está del **comando <password> de la contraseña habilitada**).

Usted puede agregar más Seguridad agregando la autenticación para habilitar, tal y como se muestra en de este ejemplo:

```
GOSS(config)# aaa authentication enable console LOCAL
```

Esto requiere al usuario ingresar la contraseña amba para el login y habilitarla. En este ejemplo, la contraseña “poweruser” se utiliza para el login y el permiso. Un usuario “poweruser” debería poder realizar una conexión Telnet en el PIX y también debería poder lograr la habilitación con la contraseña PIX local.

Si usted quisiera que algunos usuarios pudieran utilizar solamente ciertos comandos, usted tiene que configurar a un usuario con privilegios más bajos, tal y como se muestra en de este ejemplo:

```
GOSS(config)# username ordinary password ordinary privilege 9
```

Puesto que prácticamente todos sus comandos están predeterminados en el nivel 15, debe bajar algunos comandos al nivel 9 para que los usuarios "comunes" puedan enviarlos. En este caso, usted quisiera que su usuario del nivel 9 pudiera utilizar el **comando show clock**, pero no configurar de nuevo el reloj, tal y como se muestra en de este ejemplo:

```
GOSS(config)# privilege show level 9 command clock
```

Usted también necesita a su usuario poder terminar la sesión del PIX (el usuario pudo estar en el nivel 1 o 9 al querer hacer esto), tal y como se muestra en de este ejemplo:

```
GOSS(config)# privilege configure level 1 command logout
```

Usted necesita al usuario poder utilizar el **comando enable** (el usuario está en el nivel 1 al intentar esto), tal y como se muestra en de este ejemplo:

```
GOSS(config)# privilege configure level 1 mode enable command enable
```

Moviendo el **comando disable al** nivel 1, cualquier usuario entre los niveles 2-15 puede salir del enable mode, tal y como se muestra en de este ejemplo:

```
GOSS(config)# privilege configure level 1 command disable
```

Si usted Telnet adentro como el usuario “ordinario” y permiso como el mismo usuario (la contraseña es también “ordinario”), usted utiliza la **neutralización del comando 1 del nivel de la configuración del privilegio**, tal y como se muestra en de este ejemplo:

```
GOSS# show curpriv
Username : ordinary
Current privilege level : 9
Current Mode/s : P_PRIV
```

Si aún tiene la sesión original abierta (la anterior a agregar cualquier autenticación), el PIX puede no saber quién es usted ya que no se registró inicialmente con un nombre de usuario. Si ése es el caso, utilice el **comando debug** de ver los mensajes sobre el usuario el "enable_15" o el "enable_1" si no hay nombre de usuario asociado. Por lo tanto, ingrese a Telnet en PIX como el usuario "poweruser" (el usuario de “nivel 15”) antes de configurar la autorización del comando, debido a que debe asegurarse de que PIX pueda asociar el nombre de usuario con los comandos con los que se está intentando. Usted está listo a la autorización del comando test usando este

comando:

```
GOSS(config)# aaa authorization command LOCAL
```

El usuario "súperusuario" debería ser capaz de establecer una sesión Telnet, y de activar y ejecutar todos los comandos. El usuario “ordinario” debe poder utilizar el **reloj de la demostración**, **habilita**, **inhabilita**, y los **comandos logout** pero no otros, tal y como se muestra en de este ejemplo:

```
GOSS# show xlate
Command authorization failed
```

Autenticación/autorización con un servidor AAA

También puede autenticar y autorizar usuarios mediante un servidor AAA. TACACS+ funciona mejor porque la autorización del comando es posible, pero también se puede usar RADIUS. Marque para ver si hay Telnet AAA anterior/comandos console en el PIX (en caso que utilizaron al **comando local aaa** previamente), tal y como se muestra en de este ejemplo:

```
GOSS(config)# show aaa
AAA authentication telnet console LOCAL
AAA authentication enable console LOCAL
AAA authorization command LOCAL
```

Si hay Telnet AAA anterior/comandos console, quítelos usando estos comandos:

```
GOSS(config)# no aaa authorization command LOCAL
GOSS(config)# no aaa authentication telnet console LOCAL
GOSS(config)# no aaa authentication enable console LOCAL
```

Como con configurar la autenticación local, la prueba para aseegurarse a los usuarios puede Telnet en el PIX usando estos comandos.

```
telnet 172.18.124.0 255.255.255.0
!--- IP range allowed to telnet to the PIX (values would depend on network). passwd <password>
!--- Telnet password. Enable password <password>
!--- Enable password.
```

Dependiendo de qué servidor usted está utilizando, configure el PIX para la autenticación/la autorización con un servidor de AAA.

ACS - TACACS+

La configuración ACS a comunicar con el PIX definiendo el PIX en la configuración de red con “autentica usando” el TACACS+ (para el software de Cisco IOS®). La configuración del usuario de ACS depende de la configuración del PIX. Al mínimo, el usuario de ACS debe ser configurado con un nombre de usuario y contraseña.

En el PIX, utilice estos comandos:

```
GOSS(config)# enable password cisco123
GOSS(config)# aaa-server TACSERVER protocol tacacs+
GOSS(config)# aaa-server TACSERVER (inside) host   timeout 10
GOSS(config)# aaa authentication telnet console TACSERVER
```

En este momento, el usuario de ACS debe poder a Telnet en el PIX, habilitarlo con la contraseña habilitada existente en el PIX, y realizar los comandos all. Complete estos pasos:

1. Si hay una necesidad de hacer la autenticación del permiso PIX con el ACS, elija **Interface Configuration > Advanced Tacacs+ Settings**.
2. Marque las **características del TACACS+ avanzado en el** cuadro de las **opciones de configuración avanzada**.
3. Haga clic en Submit (Enviar). Las configuraciones del TACACS+ avanzado son visibles ahora bajo configuración de usuario.
4. Fije el privilegio máximo para cualquier cliente AAA al nivel 15.
5. Elija el esquema de la contraseña habilitada para el usuario (que podría implicar el configurar de una contraseña habilitada separada).
6. Haga clic en Submit (Enviar).

Para girar la autenticación del permiso con el TACACS+ en el PIX, utilice este comando:

```
GOSS(config)# aaa authentication enable console TACSERVER
```

En este momento, el usuario de ACS debe poder a Telnet en el PIX y el permiso con la contraseña habilitada configurada en el ACS.

Antes de agregar la autorización del comando pix, el 3.0 ACS debe ser parcheado. Usted puede descargar la corrección del centro de software (clientes registrados solamente). Usted puede también ver la información adicional sobre esta corrección accediendo el Id. de bug Cisco CSCdw78255 (clientes registrados solamente).

La autenticación debe estar en funcionamiento antes de ejecutar la autorización de comandos. Si hay una necesidad de realizar el comando authorization con el ACS, elija **Interface Configuration > Tacacs+ (Cisco) > Shell (Exec) para el usuario y/o el grupo** y el tecleo **someten**. Las configuraciones de la autorización del comando shell son visibles ahora bajo configuración del usuario (o grupo).

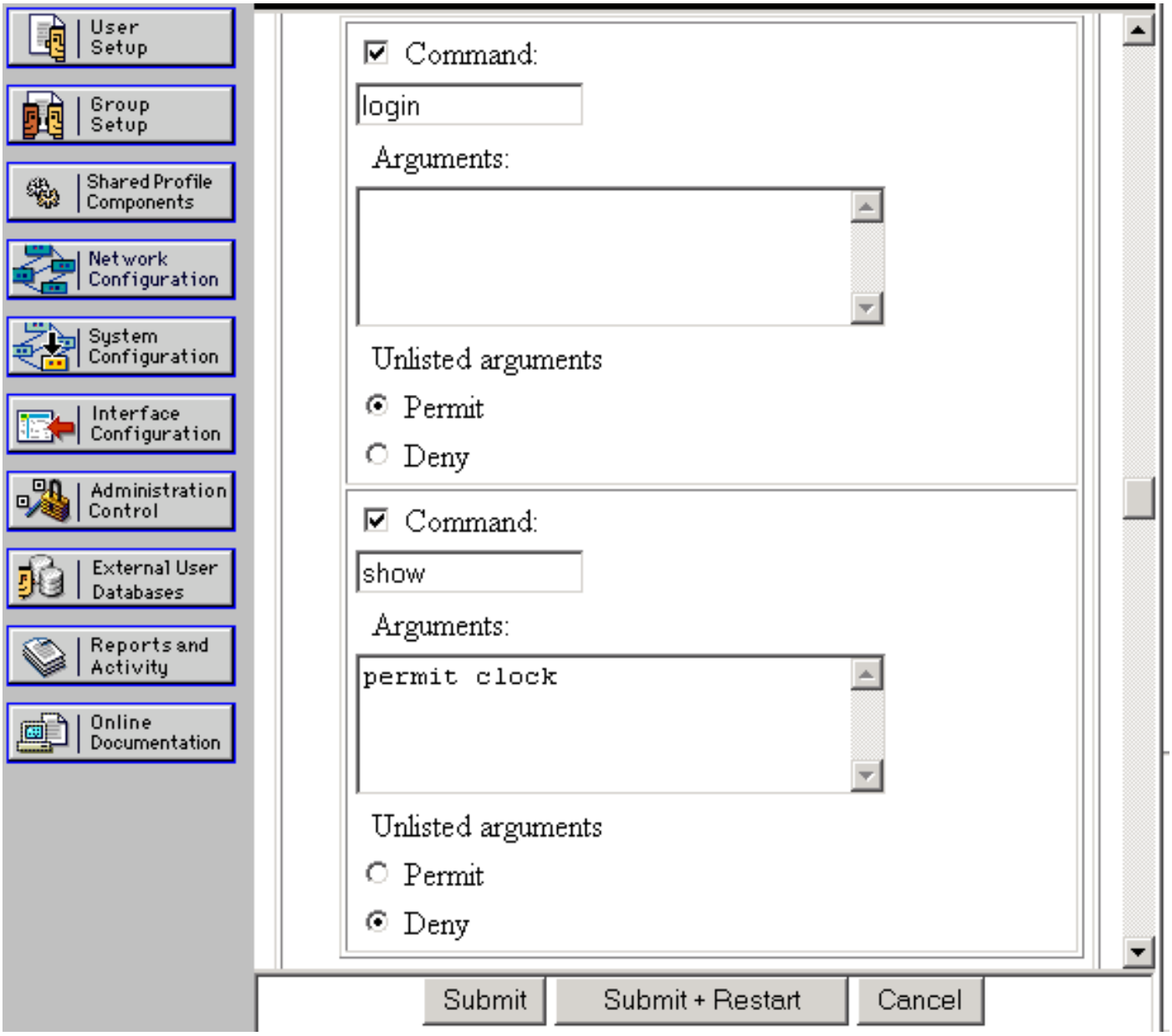
Es una buena idea configurar por lo menos a un usuario ACS poderoso para el comando authorization y permitir los comandos cisco ios incomparables.

Otros usuarios de ACS pueden ser configurados con el comando authorization permitiendo un subconjunto de comandos. Este ejemplo utiliza estos pasos:

1. Elija las configuraciones de grupo para encontrar al grupo deseado de la casilla desplegable.
2. El tecleo **edita las configuraciones**.
3. Elija el **conjunto de la autorización del comando shell**.
4. Haga clic el **botón comando**.
5. Ingrese el **login**.
6. Elija el permiso bajo argumentos no enumerados.
7. Relance este proceso para el **logout**, el **permiso**, y los **comandos disable**.

8. Elija el conjunto de la autorización del comando shell.
9. Haga clic el **botón comando**.
10. Entershow.
11. Bajo argumentos, ingrese el **reloj del permiso**.
12. Choose niega para los argumentos no enumerados.
13. Haga clic en Submit (Enviar).

Aquí está un ejemplo de estos pasos:



Si usted todavía tiene su sesión original abierta (la que está antes de agregar cualquier autenticación), el PIX puede no conocer quién usted es porque usted no inició sesión inicialmente con un nombre de usuario ACS. Si ése es el caso, utilice el **comando debug** de ver los mensajes sobre el usuario el "enable_15" o el "enable_1" si no hay nombre de usuario asociado. Usted necesita estar seguro que el PIX puede asociar un nombre de usuario a los comandos que son intentados. Usted puede hacer esto por el Telnetting en el PIX como el usuario de ACS del nivel 15 antes de configurar el comando authorization. Usted está listo a la autorización del comando test usando este comando:

```
aaa authorization command TACSERVER
```

En este momento, usted debe tener un usuario que deba poder a Telnet adentro, habilitar, y utilizar todos los comandos, y un segundo usuario que pueda hacer solamente cinco comandos.

CSUnix - TACACS+

Configuración CSUnix a comunicar con el PIX como usted con cualquier otro dispositivo de red. La configuración del usuario CSUnix depende de la configuración del PIX. Al mínimo, el usuario CSUnix debe ser configurado con un nombre de usuario y contraseña. En este ejemplo, han configurado a tres usuarios:

```
!--- This is our "poweruser" who can enable, use all commands, and log in. !--- The login
password is in the 'clear "*********"' statement. !--- The enable password is in the 'clear
"********" 15' statement. user = pixtest{ password = clear "********" privilege = clear
"********" 15 service=shell { default cmd=permit default attribute=permit } } !--- This user can
Telnet in, enable, and use four commands !--- (such as show clock, logout, exit, and enable). !-
-- The login password is in the 'clear "********"' statement. !--- The enable password is in the
'clear "********" 15' statement.

user = limitpix{
password = clear "********"
privilege = clear "********" 15
service=shell {
cmd=show {
permit "clock"
}
cmd=logout {
permit ".*"
}
cmd=enable {
permit ".*"
}
cmd=exit {
permit ".*"
}
}
}

 !--- This user can Telnet in, but not enable. This user can use any !--- show commands in non-
enable mode as well as logout, exit, and ?.

user = oneuser{
password = clear "********"
service=shell {
cmd=show {
permit ".*"
}
cmd=logout {
permit ".*"
}
cmd="?" {
permit ".*"
}
cmd=exit {
permit ".*"
}
}
}
```

En el PIX, utilice estos comandos:

```
GOSS(config)# enable password cisco123
GOSS(config)# aaa-server TACSERVER protocol tacacs+
GOSS(config)# aaa-server TACSERVER (inside) host <ip> <key> timeout 10
GOSS(config)# aaa authentication telnet console TACSERVER
```

En este momento, los usuarios CSUnixes uces de los deben poder a Telnet en el PIX, habilitar con la contraseña habilitada existente en el PIX, y utilizar todos los comandos.

Autenticación del permiso con el TACACS+ en el PIX:

```
GOSS(config)# aaa authentication enable console TACSERVER
```

En este momento, los usuarios CSUnix que poseen contraseñas "privilege15" deberían ser capaces de conectarse con Telnet a un PIX y realizar una activación con aquellas contraseñas "enable".

Si todavía continúa abierta su sesión original (la anterior a la incorporación de cualquier autenticación), es posible que PIX no conozca su identidad ya que usted inicialmente no inició sesión con un nombre de usuario. Si ese es el caso, ejecutar el comando de depuración puede mostrar mensajes acerca del usuario "enable_15" o "enable_1" si no existe un nombre de usuario asociado. Conéctese mediante Telnet a PIX como el usuario "pixtest" (el usuario de “nivel 15”) antes de configurar la autorización del comando, ya que debe asegurarse de que el PIX pueda asociar un nombre de usuario a los comandos que se están intentando. Enable authentication (Activar autenticación) debe estar activado antes de ejecutar el comando de autorización. Si hay una necesidad de realizar el comando authorization con CSUnix, agregue este comando:

```
GOSS(config)# aaa authorization command TACSERVER
```

De los tres usuarios, “el más pixtest” puede hacer todo, y los otros dos usuarios pueden hacer un subconjunto de comandos.

RADIUS ACS

La autorización del comando radius no se soporta. Telnet y la autenticación del permiso es posibles con el ACS. El ACS se puede configurar para comunicar con el PIX definiendo el PIX en configuración de red con “autentica usando” RADIUS (cualquier variedad). La configuración del usuario de ACS depende de la configuración del PIX. Al mínimo, el usuario de ACS debe ser configurado con un nombre de usuario y contraseña.

En el PIX, utilice estos comandos:

```
GOSS(config)# enable password cisco123
GOSS(config)# aaa-server RADSERVER protocol radius GOSS(config)
            # aaa-server RADSERVER (inside)
              host <ip> <key> timeout 10
GOSS(config)# aaa authentication telnet console RADSERVER
```

En este momento, el usuario de ACS debe poder a Telnet en el PIX, habilitar con la contraseña habilitada existente en el PIX, y los comandos all del uso (el PIX no hace los comandos send al servidor de RADIUS; La autorización del comando radius no se soporta).

Si usted quiere habilitar con el ACS y el RADIUS en el PIX, agregue este comando:

```
aaa authentication enable console RADSERVER
```

A diferencia con del TACACS+, la misma contraseña se utiliza para Habilitar Radius en cuanto al inicio de sesión en RADIUS.

CSUnix - RADIUS

Configure CSUnix para hablar con el PIX como usted con cualquier otro dispositivo de red. La configuración del usuario CSUnix depende de la configuración del PIX. Este perfil trabaja para la autenticación y habilitación:

```
user = pixradius{
profile_id = 26
profile_cycle = 1
!--- The login password is in the 'clear "********"' statement; !--- this is used for the login,
enable, and non-enable commands.

password = clear "********" < pixradius
}
```

En el PIX, utilice estos comandos:

```
GOSS(config)# enable password cisco123
GOSS(config)# aaa-server RADSERVER protocol radius
GOSS(config)# aaa-server RADSERVER (inside) host <ip> <key> timeout 10
```

Si usted quiere habilitar con el ACS y el RADIUS en el PIX, utilice este comando:

```
GOSS(config)# aaa authentication enable console RADSERVER
```

A diferencia con del TACACS+, la misma contraseña se utiliza para Habilitar Radius en cuanto al inicio de sesión en RADIUS.

Restricciones de acceso a la red

Las restricciones del acceso a la red se pueden utilizar en el ACS y CSUnix para limitar quién puede conectar con el PIX para fines administrativos.

- **ACS** — El PIX sería configurado en la Área de restricciones del acceso a la red de las configuraciones de grupo. La configuración PIX es “Denied Calling/Point of Access Locations” o “Permitted Calling/Point of Access Locations” (dependiendo del plan de la Seguridad).
- **CSUnix** — Éste es un ejemplo de un usuario que sea acceso permitido al PIX, pero no de los

otros dispositivos:

```
GOSS(config)# aaa authentication enable console RADSERVER
```

Depurar

Para girar el debug, utilice este comando:

```
logging on
logging <console|monitor> debug
```

Éstos son ejemplos de bueno y de los debug inadecuada:

- **Debug correcta** — El usuario puede utilizar el **login**, **habilitar**, y **realizar los** comandos.

  ```
  logging on
  logging <console|monitor> debug
  ```

- **Debug inadecuada** — La autorización falla para el usuario, tal y como se muestra en de este ejemplo:

  ```
  logging on
  logging <console|monitor> debug
  ```

- **El servidor AAA remoto es inalcanzable:**

  ```
  logging on
  logging <console|monitor> debug
  ```

Contabilidad

No hay el considerar real del comando disponible, pero teniendo Syslog activado en el PIX, usted puede ver qué acciones fueron realizadas, tal y como se muestra en de este ejemplo:

```
logging on
logging <console|monitor> debug
```

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 para resolver problemas su firewall PIX.
• 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

- Referencia de Comandos PIX
- Software Cisco PIX Firewall - Soporte técnico y documentación
- Cisco Secure Access Control Server para Windows - Soporte técnico y documentación
- Cisco Secure Access Control Server para Unix - Soporte técnico y documentación