# PIX 6.2: Ejemplo de Configuración de Comandos de Autenticación y Autorización

## Contenido


Introducción
Antes de comenzar
Convenciones
Prerequisites
Componentes Utilizados
Prueba previa al agregado de autenticación/autorización
Comprensión de configuración de privilegios
Autenticación/Autorización – Nombres de usuarios locales
Autenticación/autorización con un servidor AAA
ACS - TACACS+
CSUnix - TACACS+
RADIUS ACS
CSUnix - RADIUS
Restricciones de acceso a la red
Depurar
Contabilidad
Información para recopilar si abre un caso del TAC
Información Relacionada


## 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 ejecute este comando:

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

**Nota:** Si utiliza un TACACS+ o un grupo de servidores RADIUS para la autenticación, puede configurar el PIX para utilizar la base de datos local como un método **FALLBACK** si el servidor AAA no está disponible.

Por ejemplo

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

Si introduce LOCAL solo, puede utilizar la base de datos local como método principal de autenticación (sin reserva).

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

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

Refiérase a Cómo Realizar la Autenticación y Habilitación en Cisco Secure PIX Firewall (5.2 a 6.2) para obtener más información sobre cómo crear acceso autenticado AAA a un PIX Firewall que ejecute la versión 5.2 a 6.2 del software PIX y para obtener más información sobre cómo habilitar la autenticación, syslogging y obtener acceso cuando el servidor AAA está inactivo.

Consulte PIX/ASA: Ejemplo de Configuración de Proxy de Corte para Acceso a la Red con TACACS+ y Servidor RADIUS para obtener más información sobre cómo crear acceso autenticado AAA (Proxy de Corte) a un Firewall PIX que ejecute las versiones 6.3 y posteriores del Software PIX.

Si la configuración se lleva a cabo correctamente, no debería prohibírsele el acceso a PIX. Si la configuración no se guarda, el reinicio del PIX debe devolverlo a su estado de configuración previa. 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.

## Prerequisites

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
- Cisco Secure ACS para Windows versión 3.0 (ACS)
- Cisco Secure ACS para UNIX (CSUnix) versión 2.3.6

La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. All of the devices used in this document started with a cleared (default) configuration. 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 funciones de autenticación/autorización 6.2, asegúrese de que actualmente pueda obtener acceso 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 están en el nivel 0. Para ver la configuración actual de todos los comandos, utilice este comando:

```
show privilege all
```

La mayoría de los comandos están en el nivel 15 de forma predeterminada, como se muestra en este ejemplo:

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

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

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

El PIX puede funcionar en los modos de habilitación y configuración. Algunos comandos, como **show logging**, están disponibles en ambos modos. Para establecer privilegios en estos comandos, debe especificar el modo en el que existe el comando, como se muestra en el ejemplo. La otra opción de modo es **enable**. Obtiene el `registro es un comando disponible en el` mensaje de error `de varios modos`. Si no configura el modo, utilice el comando **mode [enable|configure]**:

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

Estos ejemplos abordan el comando **clock**. Utilice este comando para determinar la configuración actual del comando **clock**:

```
show privilege command clock
```

La salida del comando **show privilege clock** 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**, debe ir al puerto de la consola para configurar un usuario administrativo y activar la autenticación de login LOCAL, como se muestra en 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, como se muestra en este ejemplo:

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

El usuario "poweruser" debe ser capaz de Telnet en el PIX y habilitar con la contraseña de habilitación PIX local existente (la del comando **enable password <*password*>**).

Puede agregar más seguridad agregando autenticación para habilitar, como se muestra en este ejemplo:

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

Esto requiere que el usuario introduzca la contraseña tanto para el inicio de sesión como para la activación. En este ejemplo, la contraseña "poweruser" se utiliza tanto para iniciar sesión como

para habilitar. 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 desea que algunos usuarios sólo puedan utilizar ciertos comandos, debe configurar un usuario con privilegios inferiores, como se muestra en 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, desea que su usuario de nivel 9 pueda utilizar el comando **show clock**, pero no reconfigurar el reloj, como se muestra en este ejemplo:

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

También necesita que su usuario pueda cerrar la sesión de PIX (el usuario puede estar en el nivel 1 o 9 cuando quiera hacer esto), como se muestra en este ejemplo:

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

Necesita que el usuario pueda utilizar el comando **enable** (el usuario se encuentra en el nivel 1 al intentar esto), como se muestra en este ejemplo:

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

Al mover el comando **disable** al nivel 1, cualquier usuario entre los niveles 2-15 puede salir del modo enable, como se muestra en este ejemplo:

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

Si utiliza Telnet como el usuario "ordinario" y habilita como el mismo usuario (la contraseña también es "común"), debe utilizar el **comando privilege configure level 1 disable**, como se muestra en 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 ese es el caso, utilice el comando **debug** para ver los mensajes sobre el usuario "enable_15" o "enable_1" si no hay un 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. Está listo para probar la autorización de comandos mediante 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 "común" debe poder utilizar los comandos **show clock**, **enable**, **disable** y **logout**, pero no otros, como se muestra en 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. Verifique para ver si hay comandos AAA Telnet/console anteriores en el PIX (en el caso de que el comando **LOCAL AAA** se utilizara previamente), como se muestra en este ejemplo:

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

Si hay comandos AAA Telnet/console anteriores, retírelos 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
```

Al igual que con la configuración de la autenticación local, pruebe para asegurarse de que los usuarios pueden 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 del servidor que esté utilizando, configure el PIX para la autenticación/autorización con un servidor AAA.

## ACS - TACACS+

Configure el ACS para comunicarse con el PIX mediante la definición del PIX en la Configuración de Red con "Autenticar mediante" TACACS+ (para Cisco IOS® Software). La configuración del usuario ACS depende de la configuración del PIX. Como mínimo, el usuario ACS debe configurarse con un nombre de usuario y una 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 punto, el usuario ACS debe ser capaz de Telnet en el PIX, habilitarlo con la contraseña de habilitación existente en el PIX y realizar todos los comandos. Complete estos pasos:

1. Si hay una necesidad de hacer PIX enable authentication con ACS, elija **Interface Configuration > Advanced TACACS+ Settings**.
2. Marque la casilla **Advanced TACACS+ Features in Advanced Configuration Options** .
3. Haga clic en Submit (Enviar). La configuración avanzada de TACACS+ ahora está visible en la configuración del usuario.
4. Establezca el privilegio máximo para cualquier cliente AAA en el nivel 15.
5. Elija el esquema de activación de contraseña para el usuario (que podría implicar la configuración de una contraseña de activación independiente).
6. Haga clic en Submit (Enviar).

Para activar habilitar la autenticación a través de TACACS+ en el PIX, utilice este comando:

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

En este punto, el usuario ACS debe ser capaz de Telnet en el PIX y habilitar con la contraseña de habilitación configurada en ACS.

Antes de agregar la autorización del comando PIX, se debe aplicar parches a ACS 3.0. Puede descargar el parche desde el Centro de Software (sólo clientes registrados) . También puede ver información adicional sobre este parche accediendo al ID de bug de Cisco CSCdw78255 (sólo clientes registrados) .

La autenticación debe estar en funcionamiento antes de ejecutar la autorización de comandos. Si es necesario realizar una autorización de comandos con ACS, elija **Interface Configuration > TACACS+ (Cisco) > Shell (exec) para el usuario y/o grupo** y haga clic en **Submit**. La configuración de autorización del comando shell ahora está visible en la configuración del usuario (o grupo).

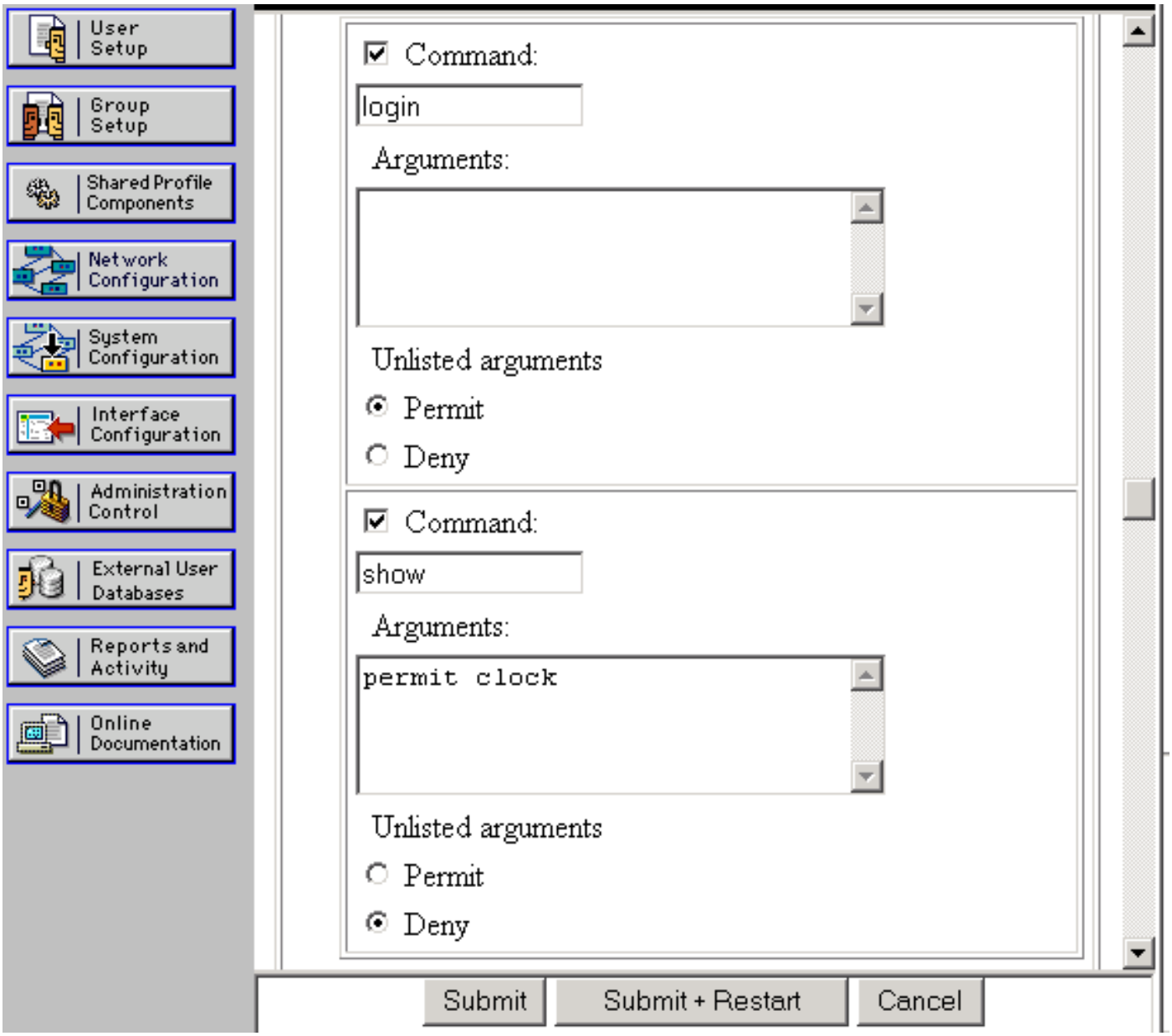
Es una buena idea configurar al menos un usuario ACS poderoso para la autorización de comandos y para permitir comandos Cisco IOS incomparables.

Otros usuarios ACS se pueden configurar con autorización de comandos permitiendo un subconjunto de comandos. Este ejemplo utiliza estos pasos:

1. Elija Group Settings (Configuración de grupo) para buscar el grupo deseado en el cuadro desplegable.
2. Haga clic en **Editar configuración**.
3. Elija **Shell Command Authorization Set**.
4. Haga clic en el botón **Comando**.
5. Ingrese **login**.
6. Elija Permit en Argumentos no enumerados.
7. Repita este proceso para los comandos **logout**, **enable** y **disable**.
8. Elija Shell Command Authorization Set.
9. Haga clic en el botón **Comando**.

10. **Entreshow**.
11. En Arguments , ingrese **permit clock**.
12. Elija deny para los argumentos no enumerados.
13. Haga clic en Submit (Enviar).

A continuación se muestra un ejemplo de estos pasos:




Si todavía tiene abierta su sesión original (la anterior a agregar cualquier autenticación), es posible que el PIX no sepa quién es porque inicialmente no se conectó con un nombre de usuario ACS. Si ese es el caso, utilice el comando **debug** para ver los mensajes sobre el usuario "enable_15" o "enable_1" si no hay ningún nombre de usuario asociado. Debe estar seguro de que el PIX puede asociar un nombre de usuario con los comandos que se intentan. Puede hacer esto mediante Telnet en el PIX como el usuario ACS de nivel 15 antes de configurar la autorización de comandos. Está listo para probar la autorización de comandos mediante este comando:

```
aaa authorization command TACSERVER
```

En este punto, debería tener un usuario que debería ser capaz de Telnet en, habilitar y utilizar

todos los comandos, y un segundo usuario que sólo puede hacer cinco comandos.

## CSUnix - TACACS+

Configure CSUnix para comunicarse con el PIX como lo haría con cualquier otro dispositivo de red. La configuración del usuario CSUnix depende de la configuración del PIX. Como mínimo, el usuario CSUnix debe configurarse con un nombre de usuario y una contraseña. En este ejemplo, se han configurado 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
```

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

En este punto, cualquiera de los usuarios de CSUnix debe ser capaz de Telnet en el PIX, habilitar con la contraseña de habilitación existente en el PIX y utilizar todos los comandos.

Habilite la autenticación a través de 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 es necesario realizar una autorización de comandos con CSUnix, agregue este comando:

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

De los tres usuarios, "pixtest" puede hacer todo y los otros dos pueden hacer un subconjunto de comandos.

## RADIUS ACS

La autorización del comando RADIUS no se admite. Telnet y enable authentication es posible con ACS. ACS se puede configurar para comunicarse con el PIX mediante la definición del PIX en Configuración de Red con RADIUS "Autenticar usando" (cualquier variedad). La configuración del usuario ACS depende de la configuración del PIX. Como mínimo, el usuario ACS debe configurarse con un nombre de usuario y una 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
```

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

En este punto, el usuario ACS debe ser capaz de Telnet en el PIX, habilitar con la contraseña de habilitación existente en el PIX y utilizar todos los comandos (el PIX no envía comandos al servidor RADIUS; No se admite la autorización de comandos RADIUS).

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

```
aaa authentication enable console RADSERVER
```

A diferencia de TACACS+, se utiliza la misma contraseña para RADIUS enable que para RADIUS login.

## CSUnix - RADIUS

Configure CSUnix para hablar con el PIX como lo haría con cualquier otro dispositivo de red. La configuración del usuario CSUnix depende de la configuración del PIX. Este perfil funciona para la autenticación y habilitar:

```
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
```

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

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

A diferencia de TACACS+, se utiliza la misma contraseña para RADIUS enable que para RADIUS login.

# Restricciones de acceso a la red

Las restricciones de acceso a la red se pueden utilizar tanto en ACS como en CSUnix para limitar quién puede conectarse al PIX con fines administrativos.

- **ACS**: el PIX se configuraría en el área Restricciones de Acceso a la Red de la Configuración de Grupo. La configuración de PIX es "Ubicaciones de punto de acceso/llamada denegada" o "Ubicaciones de punto de acceso/llamadas permitidas" (dependiendo del plan de seguridad).
- **CSUnix**: Este es un ejemplo de un usuario que tiene permiso para acceder al PIX, pero no a otros dispositivos:

```
user = naruser{
profile_id = 119
profile_cycle = 1
password = clear "********"
privilege = clear "********" 15
service=shell {
allow "10.98.21.50" ".*" ".*"
refuse ".*" ".*" ".*"
default cmd=permit
default attribute=permit
}
}
```

# Depurar

Para activar debug, utilice este comando:

```
logging on
logging
```

Estos son ejemplos de debugs buenos y malos:

- **Depuración correcta**: el usuario puede utilizar los comandos **log in**, **enable** y **performance**.
  ```
  307002: Permitted Telnet login session from 172.18.124.111
  111006: Console Login from pixpartial at console
  502103: User priv level changed: Uname: pixpartial From: 1 To: 15
  111009: User 'pixpartial' executed cmd: show clock
  ```
- **Depuración incorrecta**: la autorización falla para el usuario, como se muestra en este ejemplo:
  ```
  610101: Authorization failed: Cmd: uauth Cmdtype: show
  ```
- **El servidor AAA remoto es inalcanzable:**
  ```
  AAA server host machine not responding
  ```

# Contabilidad

No hay una contabilidad de comandos real disponible, pero al tener syslog activado en el PIX, puede ver qué acciones se realizaron, como se muestra en este ejemplo:

```
307002: Permitted Telnet login session from 172.18.124.111
111006: Console Login from pixtest at console
611103: User logged out: Uname: pixtest
307002: Permitted Telnet login session from 172.18.124.111
111006: Console Login from pixtest at console
502103: User priv level changed: Uname: pixtest From: 1 To: 15
111008: User 'pixtest' executed the 'enable' command.
111007: Begin configuration: 172.18.124.111 reading from terminal
111008: User 'pixtest' executed the 'configure t' command.
111008: User 'pixtest' executed the 'write t' command.
```

## 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 para solucionar el problema de su firewall PIX.** |
| --- |
| • Descripción del problema y detalles relevantes de la topología<br>• Trobleshooting realizado antes de abrir el caso<br>• Resultado del comando show tech-support<br>• 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)<br>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

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