Conjuntos de la autorización del comando shell ACS en el ejemplo de configuración IOS y ASA/PIX/FWSM

Contenido

Introducción

Este documento describe cómo configurar los conjuntos de la autorización del shell en el Cisco Secure Access Control Server (ACS) para los clientes AAA, tales como Routers del ® del Cisco IOS o Switches y dispositivos del Cisco Security (ASA/PIX/FWSM) con el TACACS+ como el protocolo de la autorización.

Nota: El ACS expreso no apoya el comando authorization.

prerrequisitos

Requisitos

Este documento asume que las configuraciones básicas están fijadas en los clientes AAA y el ACS.

En el ACS, elija **Interface Configuration > Advanced Options**, y asegúrese de que **por usuario la** casilla de verificación de los **atributos TACACS+/RADIUS** está marcada.

Componentes Utilizados

La información en este documento se basa en el Cisco Secure Access Control Server (ACS) esos funcionamientos la versión de software 3.3 y posterior.

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.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Conjuntos del comando authorization

Los conjuntos del comando authorization proporcionan un mecanismo central para controlar la autorización de cada comando que se publique en cualquier dispositivo de red dado. Esta característica aumenta grandemente el scalability y la manejabilidad requeridos para fijar las restricciones de la autorización.

En el ACS, los conjuntos de la autorización del comando default incluyen los conjuntos de la autorización del comando shell y la autorización del comando pix fija. Las aplicaciones de administración del dispositivo de Cisco, tales como CiscoWorks Management Center para firewalls, pueden dar instrucciones el ACS para apoyar los tipos del conjunto de la autorización del comando adicional.

Nota: Los conjuntos de la autorización del comando pix requieren que el pedido de autorización del comando tacacs+ identifique el servicio como *pixshell*. Verifique que este servicio se haya implementado en la versión de pix OS que sus Firewall utilizan; si no, utilice los conjuntos de la autorización del comando shell para realizar el comando authorization para los dispositivos PIX. Refiera a configurar una autorización del comando shell fijada para un grupo de usuarios para más información.

Nota: A partir del PIX OS de la versión 6.3, el servicio del pixshell no se ha implementado.

Nota: Los dispositivos del Cisco Security (ASA/PIX) no permiten actualmente que coloquen al usuario directamente en el enable mode durante el login. El usuario debe ingresar manualmente en el enable mode.

Para ofrecer más control de las sesiones de Telnet administrativa dispositivo-recibidas, un dispositivo de red que utiliza el TACACS+ puede solicitar el permiso para cada línea de comando antes de que ejecute. Usted puede definir un conjunto de comandos que se permite o se niega para la ejecución de un usuario determinado en un dispositivo dado. El ACS ha aumentado más

lejos esta capacidad con estas características:

- **Conjuntos Nombrados reutilizables del comando authorization** — Sin directamente la citación de cualquier usuario o grupo de usuarios, usted puede crear a un conjunto designado de autorizaciones de comando. Usted puede definir varios conjuntos del comando authorization que delineen diversos perfiles del acceso. Por ejemplo:Un conjunto del comando authorization del *escritorio de ayuda* podía permitir el acceso a los comandos de alto nivel de la ojeada, tales como **funcionamiento de la demostración**, y niega cualquier comando configuration.*Todo el* conjunto del comando authorization de los *ingenieros de red* podía contener una lista limitada de comandos permitidos para cualquier ingeniero de red en la empresa.*Una red local dirige el* comando authorization que el conjunto podría permitir los comandos all (e incluir los comandos de configuración de IP Address).
- **Granularity fino de la configuración** — Usted puede crear las asociaciones entre los conjuntos Nombrados y los grupos de dispositivos de red (NDGs) del comando authorization. Así, usted puede definir diversos perfiles del acceso para los usuarios dependiendo de qué dispositivos de red acceden. Usted puede asociar el mismo conjunto Nombrado del comando authorization a más de un NDG y utilizarlo para más de un grupo de usuarios. El ACS aplica la integridad de los datos. Los conjuntos Nombrados del comando authorization se mantienen la base de datos interna ACS. Usted puede utilizar las características de reserva ACS y del Restore a de reserva y al restore ellos. Usted puede también los conjuntos de la autorización del comando replicate a los ACS secundarios junto con otros datos de configuración.

Para los tipos del conjunto del comando authorization que soportan las aplicaciones de administración del dispositivo de Cisco, las ventajas son similares cuando usted utiliza los conjuntos del comando authorization. Usted puede los conjuntos de la autorización del comando apply a los grupos ACS que contienen a los usuarios de la aplicación de administración de dispositivos para aplicar la autorización de los diversos privilegios en una aplicación de administración de dispositivos. Los grupos ACS pueden corresponder a diversos papeles dentro de la aplicación de administración de dispositivos, y usted puede aplicar diversos conjuntos del comando authorization a cada grupo, como aplicable.

El ACS tiene tres etapas secuenciales de filtración del comando authorization. Cada petición del comando authorization se evalúa en la orden enumerada:

1. **Comando match** — El ACS determina si el comando se procesa que corresponde con un comando enumerado en el conjunto del comando authorization. Si el comando no se corresponde con, la determinación incomparable de los comandos determina al comando authorization: *permit or deny*. Si no, si se corresponde con el comando, la evaluación continúa.
2. **Emparejamiento del argumento** — El ACS determina si los argumentos del comando presentados corresponden con los argumentos del comando enumerados en el conjunto del comando authorization.Si ningún argumento no se corresponde con, determinan al comando authorization por si la opción incomparable del Args del permiso está habilitada. Si se permiten los argumentos incomparables, se autoriza el comando y los extremos de la evaluación; si no, el comando no se autoriza y los extremos de la evaluación.Si se corresponden con todos los argumentos, la evaluación continúa.
3. **Directiva del argumento** — Una vez que el ACS determina que los argumentos en los argumentos del comando match en el conjunto del comando authorization, ACS determinan si cada argumento del comando está permitido explícitamente. Si todos los argumentos se permiten explícitamente, el ACS concede el comando authorization. Si ninguna argumentos

no se permite, el ACS niega el comando authorization.

Agregue un conjunto de la autorización del comando shell

Esta sección incluye estos escenarios que describan cómo agregar un comando authorization fijado:

- Escenario 1: Privilegio para el acceso de lectura/escritura o el acceso total
- Escenario 2: Privilegio para acceso de sólo lectura
- Escenario 3: Privilegio para el acceso restringido

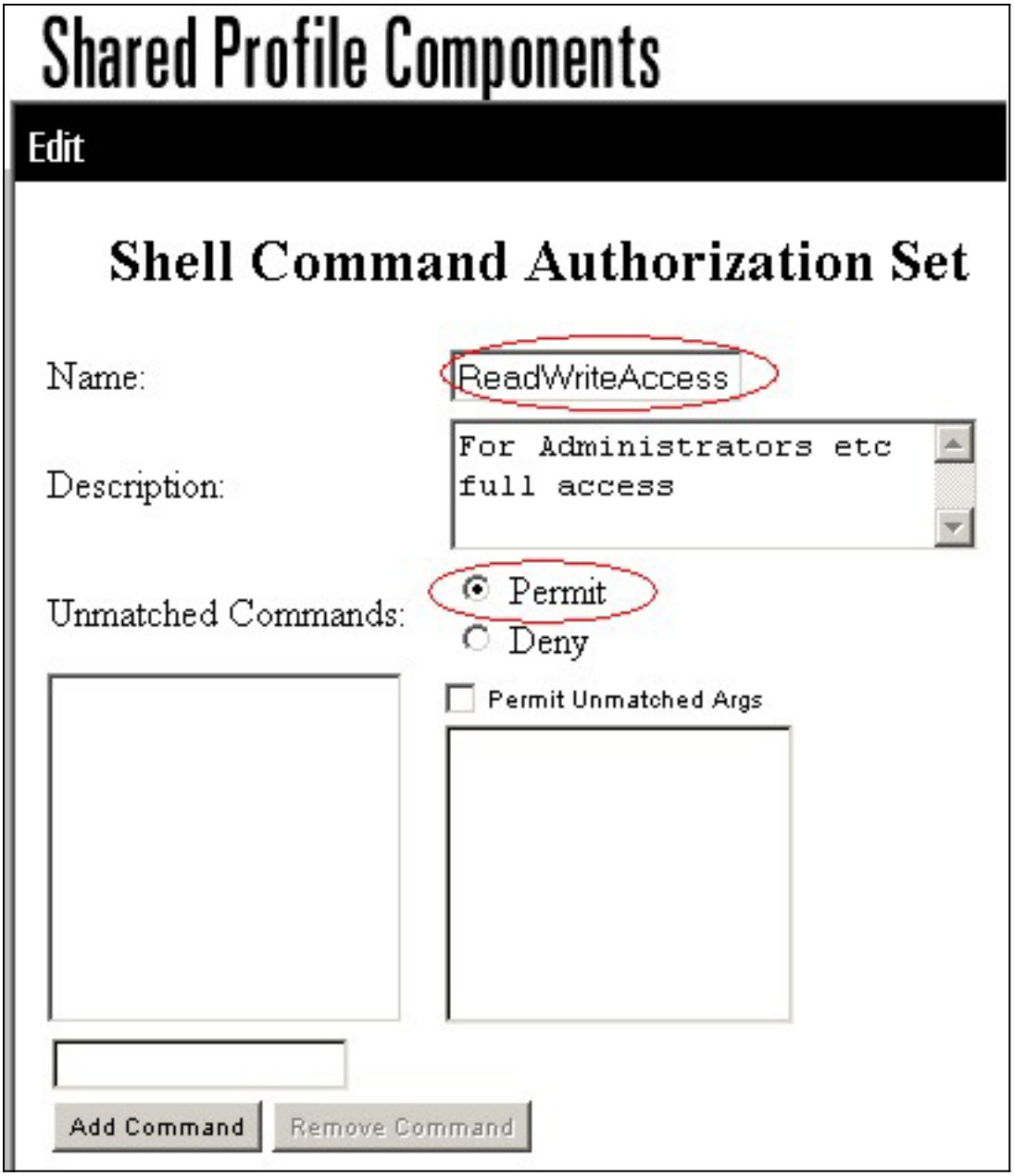
Nota: Refiera a agregar a una sección de configuración del comando authorization del guía del usuario para el Cisco Secure Access Control Server 4.1 para más información sobre cómo crear los conjuntos del comando authorization. Refiera a editar un comando authorization fijado y a borrar un comando authorization fijado para más información sobre cómo editar y los conjuntos de la autorización del comando delete.

Escenario 1: Privilegio para el acceso de lectura/escritura o el acceso total

En este los escenarios, los usuarios se conceden el acceso de lectura/grabación (o completo).

En el área determinada de la autorización del comando shell de la ventana de los componentes del perfil compartidos, configure estas configuraciones:

1. En el campo de nombre, ingrese **ReadWriteAccess** como el nombre del conjunto del comando authorization.
2. En el campo Description (Descripción), ingrese una descripción para el conjunto del comando authorization.
3. Haga clic el botón de radio del **permiso**, y después haga clic **someten**.

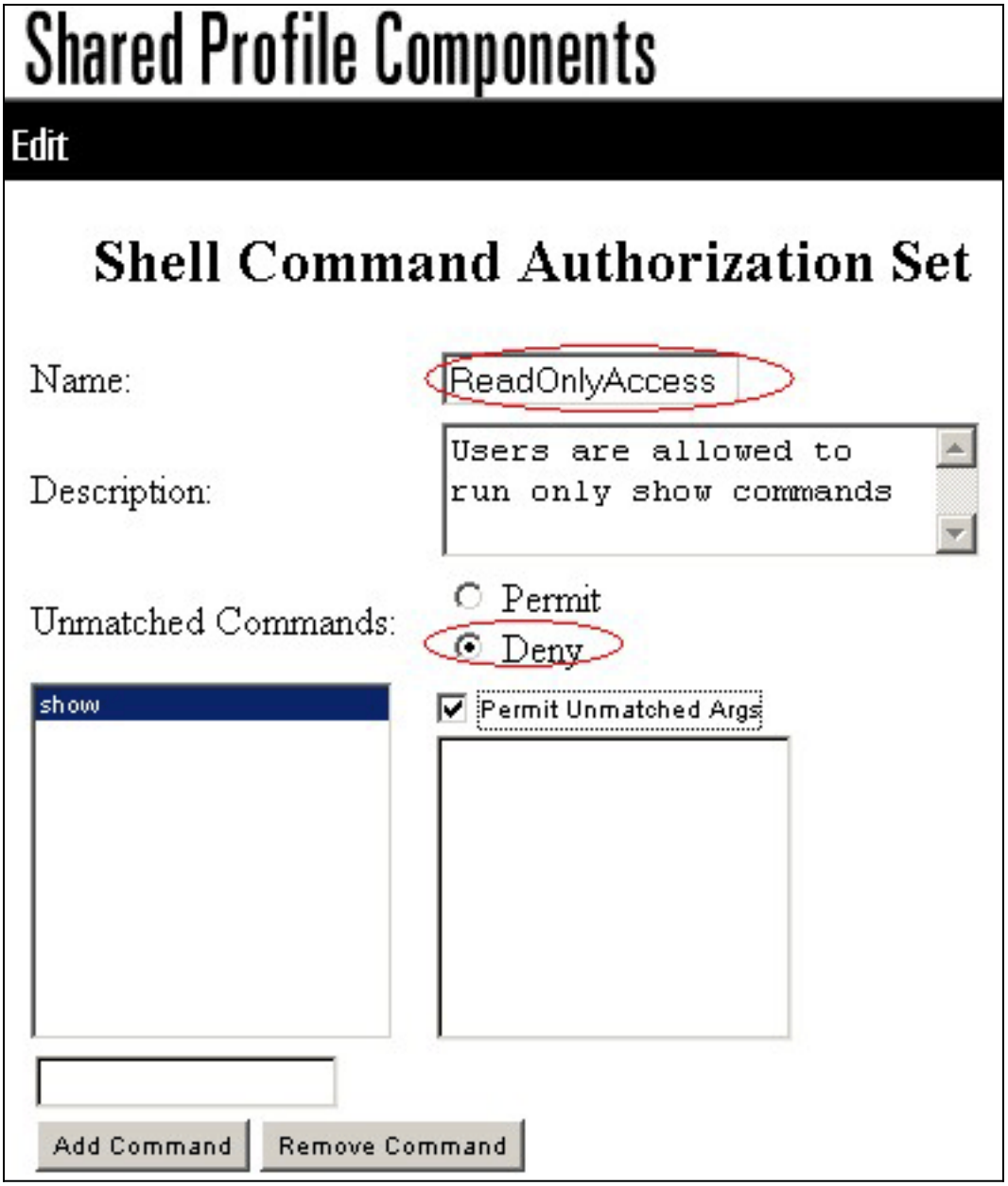


Escenario 2: Privilegio para acceso de sólo lectura

En este los escenarios, los usuarios pueden utilizar solamente los **comandos show**.

En el área determinada de la autorización del comando shell de la ventana de los componentes del perfil compartidos, configure estas configuraciones:

1. En el campo de nombre, ingrese **ReadOnlyAccess** como el nombre del conjunto del comando authorization.
2. En el campo Description (Descripción), ingrese una descripción para el conjunto del comando authorization.
3. Haga clic el botón de radio de la **negación**.
4. Ingrese el **comando show** en el campo sobre el botón de comando Add, y después haga clic el **comando Add**.
5. Marque la casilla de verificación **incomparable del Args del permiso**, y el tecleo **somete**

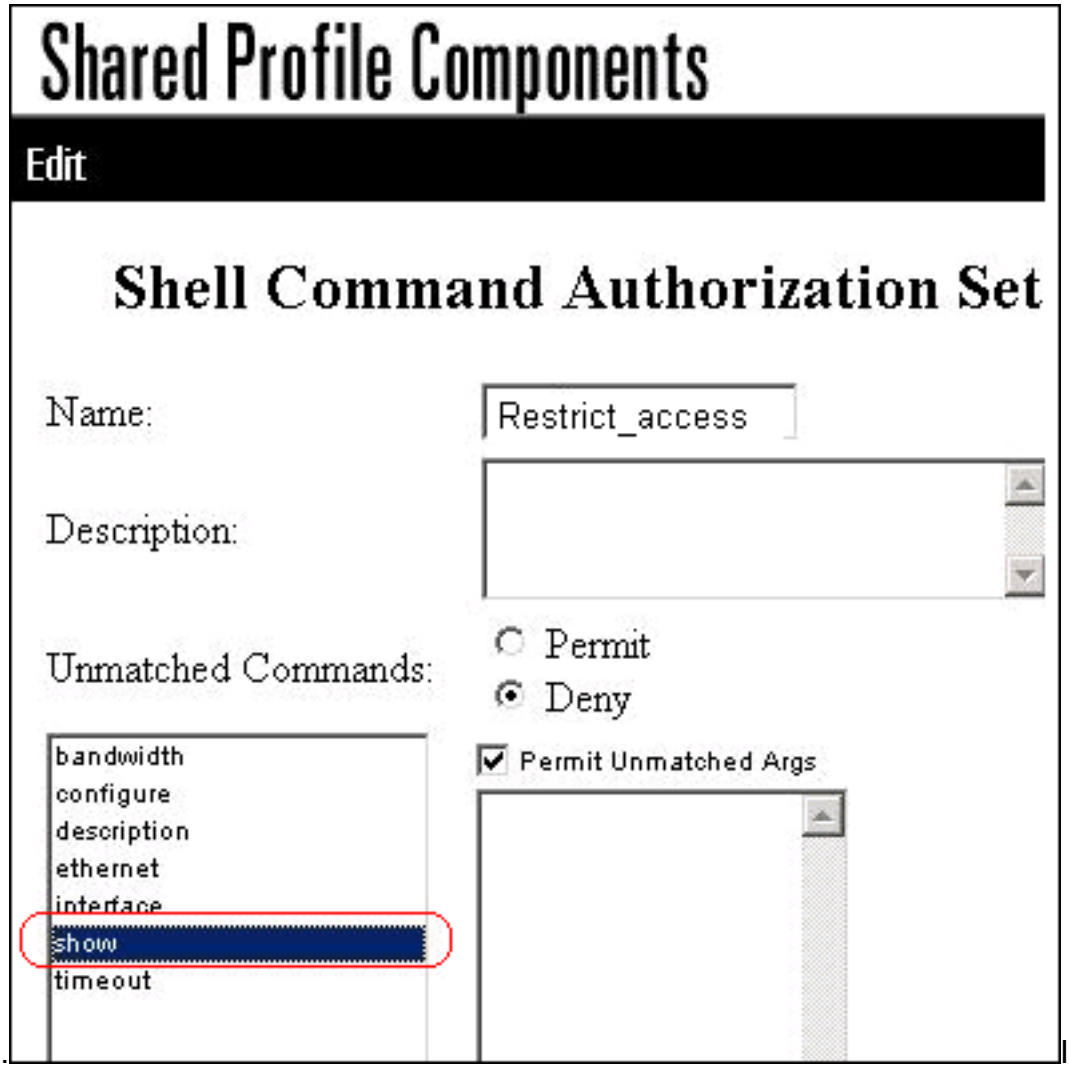


Escenario 3: Privilegio para el acceso restringido

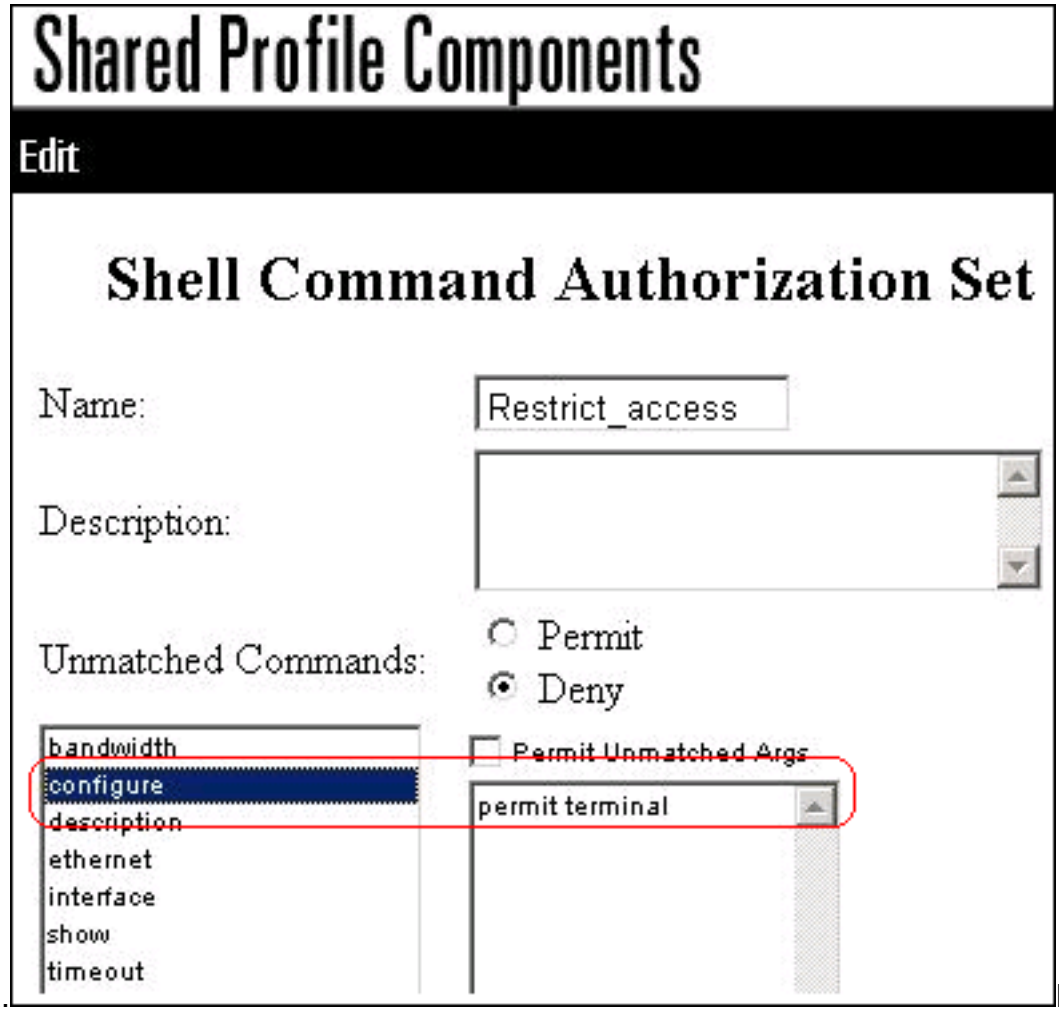
En este escenario, los usuarios pueden utilizar los comandos selectivos.

En el área determinada de la autorización del comando shell de la ventana de los componentes del perfil compartidos, configure estas configuraciones:

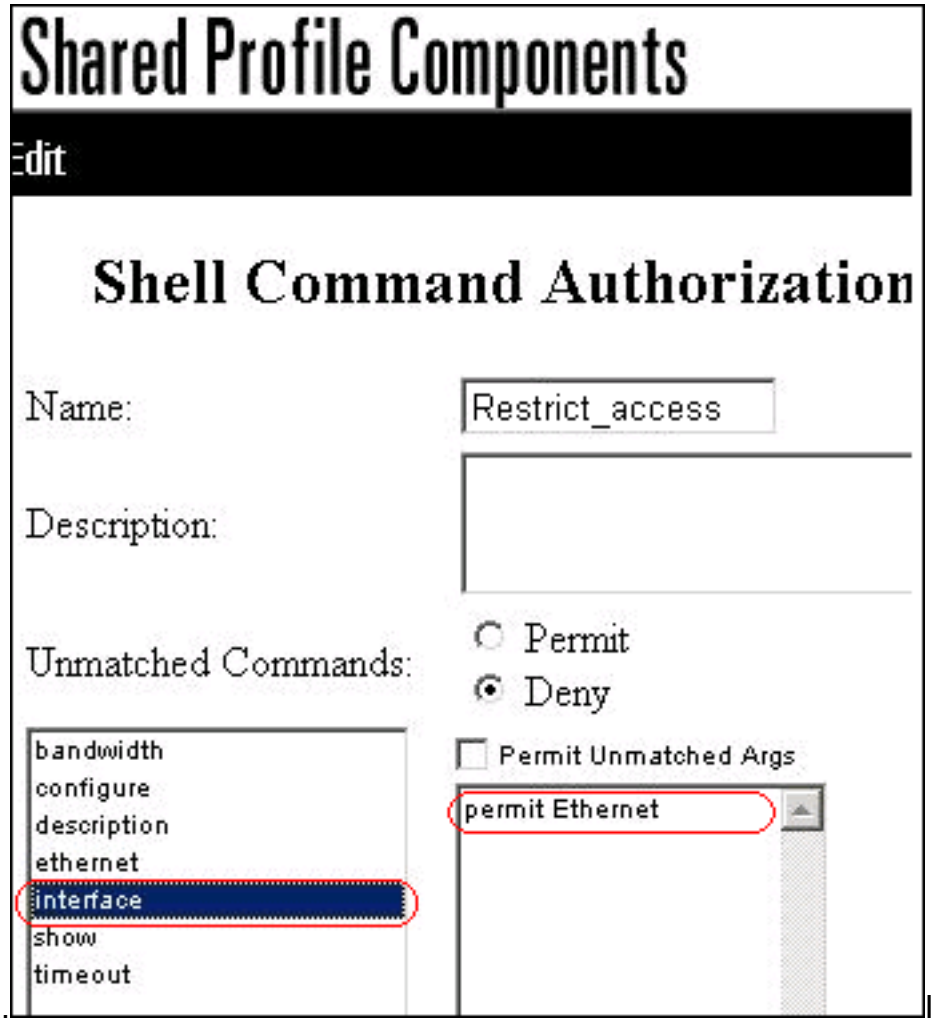
1. En el campo de nombre, ingrese **Restrict_access** como el nombre del conjunto del comando authorization.
2. Haga clic el botón de radio de la **negación**.
3. Ingrese los comandos que usted quiere permitir en los clientes AAA.En el campo situado sobre el botón de comando Add, ingrese el **comando show**, y haga clic el **comando**



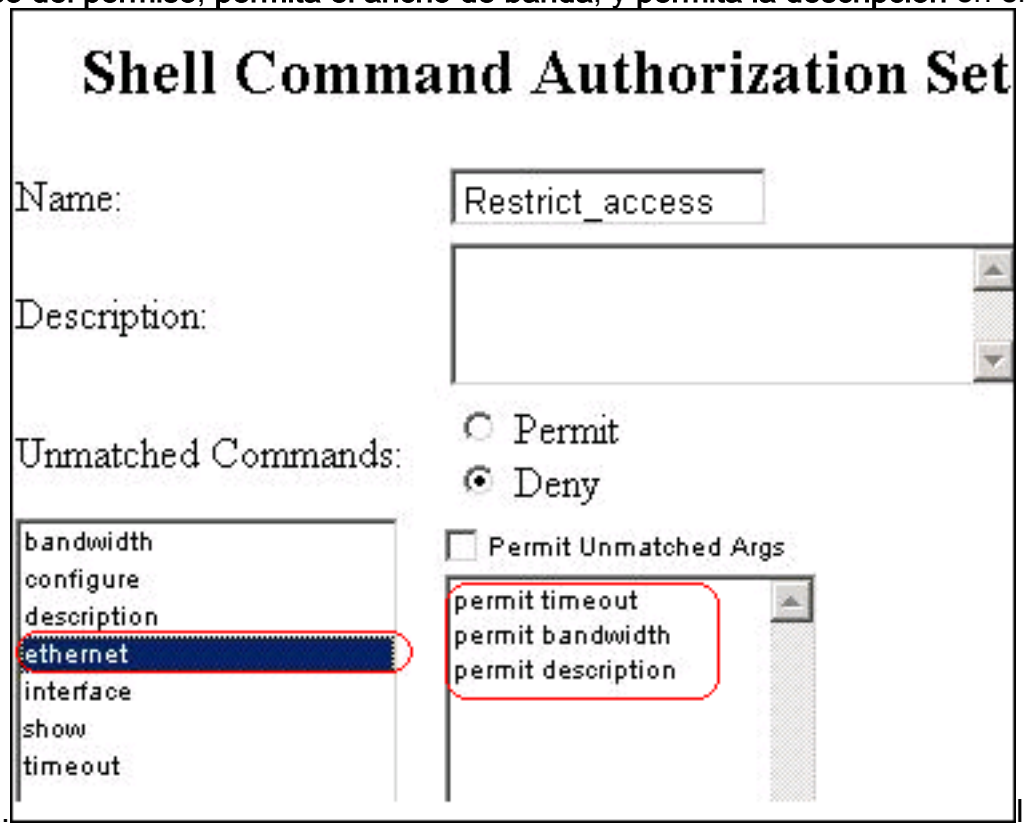
Add.Ingrese el **comando configure**, y haga clic el **comando Add**.Seleccione el **comando configure**, y ingrese la **terminal del permiso** en el campo a la



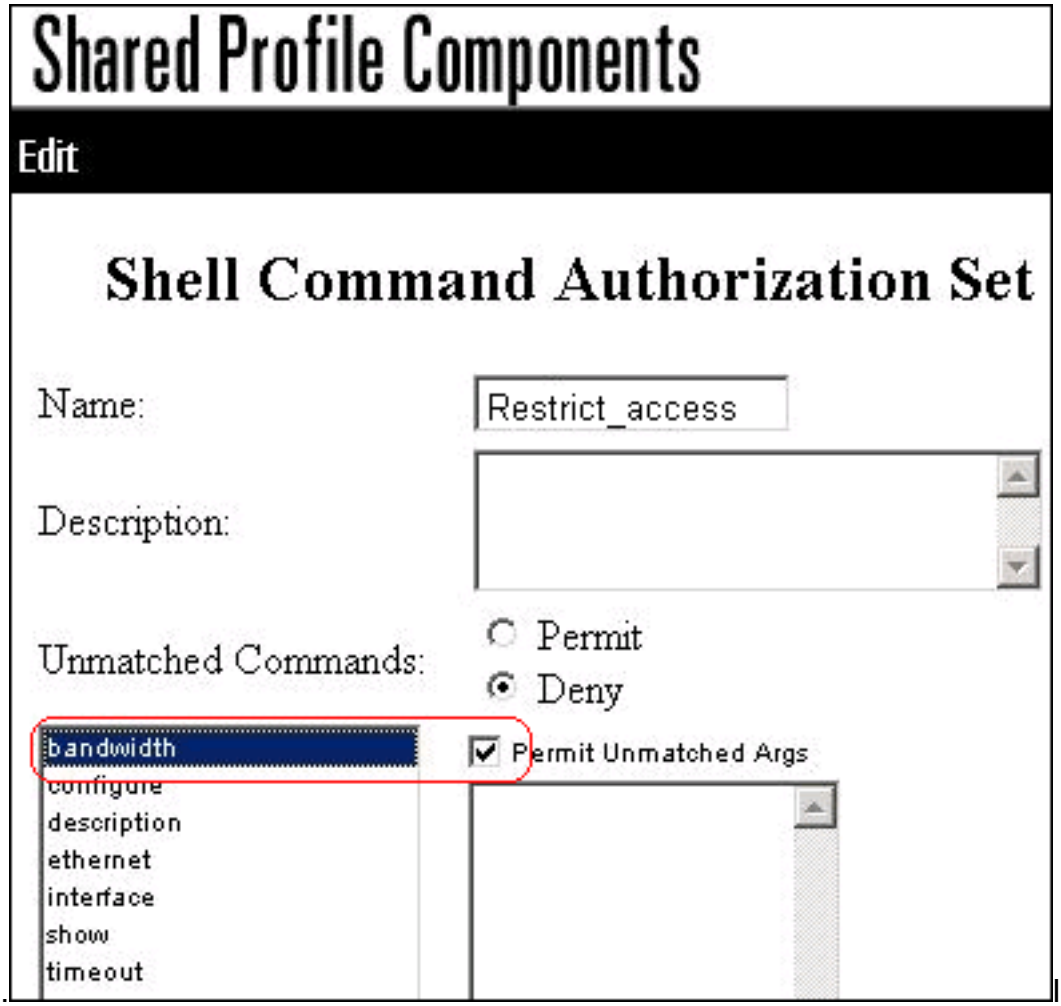
derecha. Ingrese el **comando interface**, y haga clic el **comando Add**.Seleccione el **comando interface**, y ingrese los **Ethernetes del permiso** en el campo a la



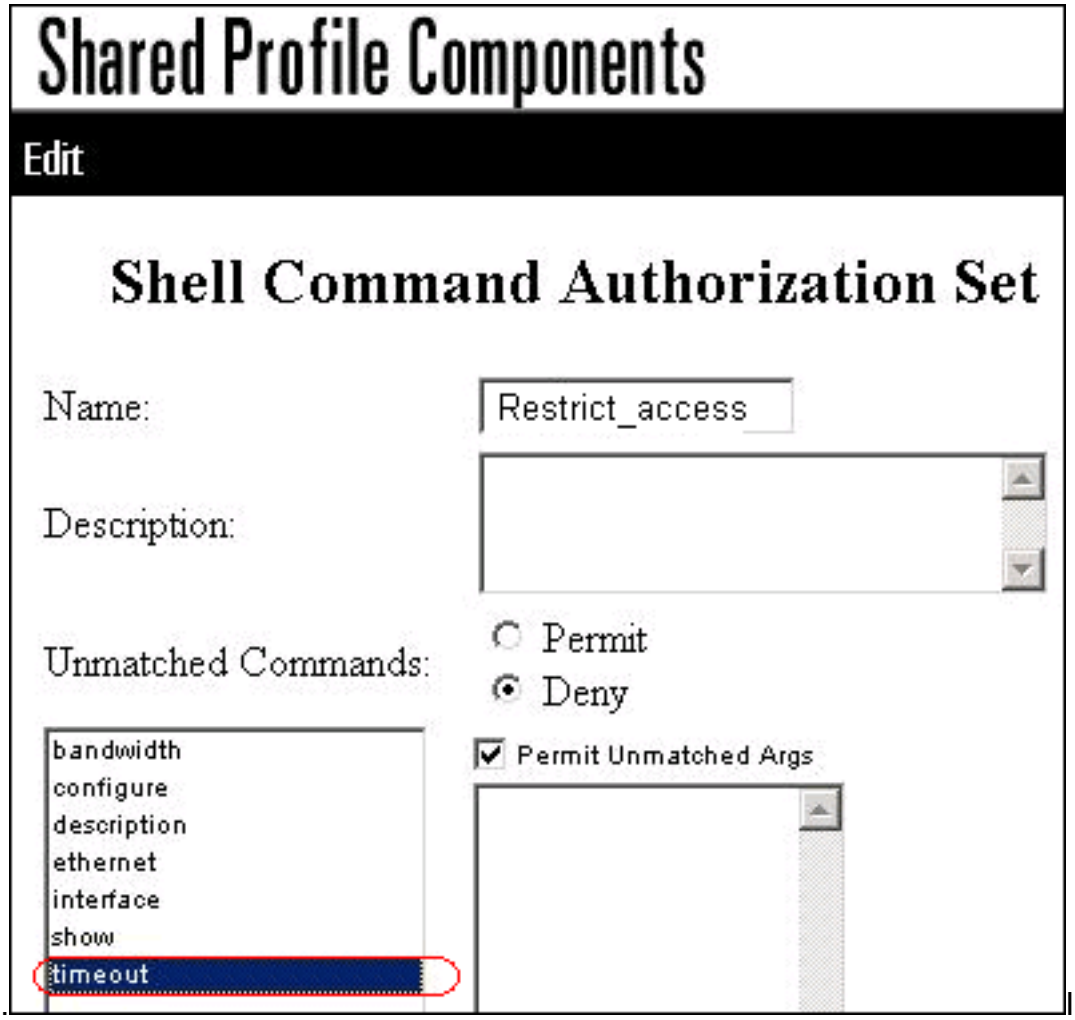
derecha. Ingrese el **comando ethernet**, y haga clic el **comando Add**.Seleccione el **comando interface**, y ingrese el **descanso del permiso**, **permita el ancho de banda**, y **permita la descripción** en el campo a la



derecha. Ingrese el **comando bandwidth**, y haga clic el **comando**

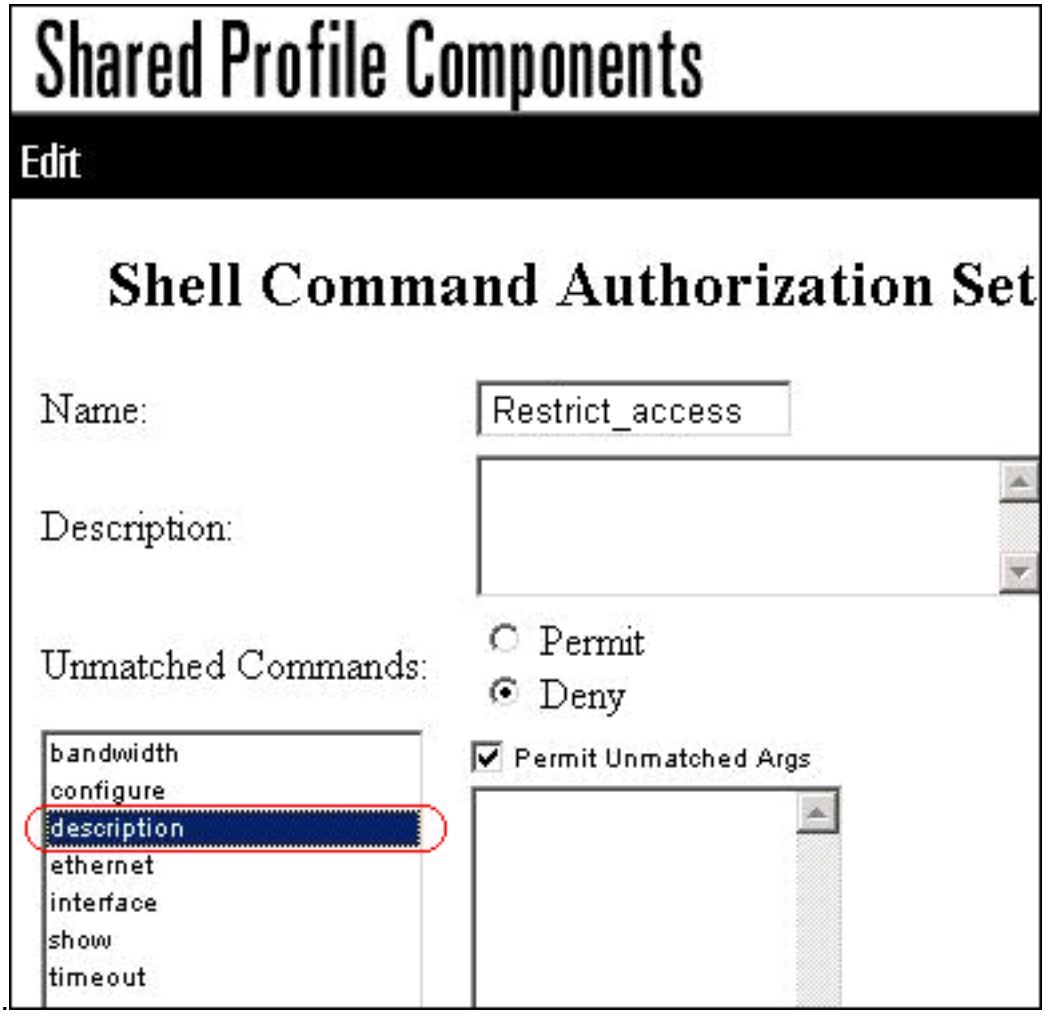


Add.Ingrese el **comando timeout**, y haga clic el **comando**



Add. Ingrese el **comando description**, y haga clic el **comando**

Add.



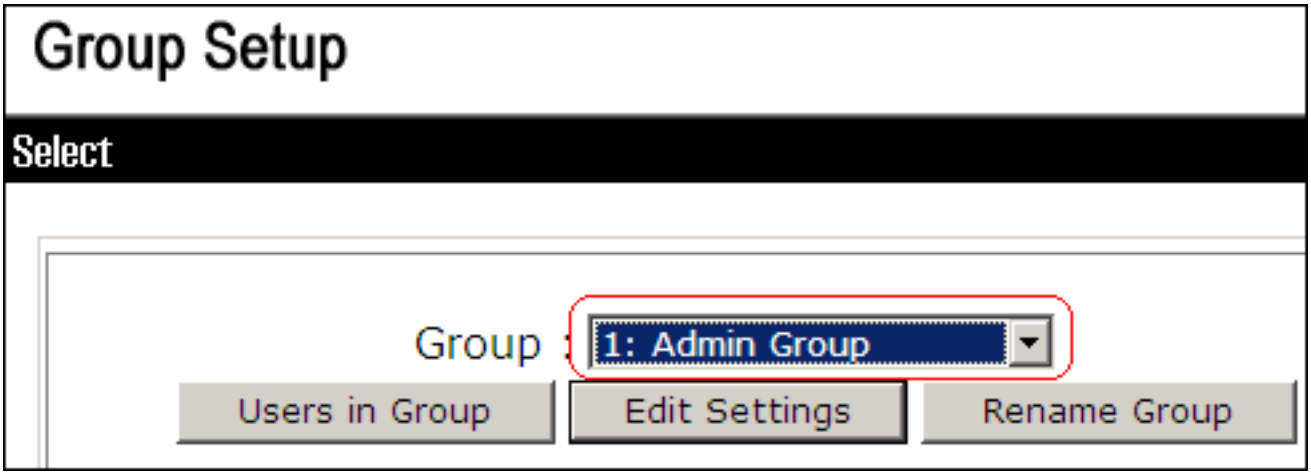
4. Haga clic en Submit (Enviar).

Asocie la autorización del comando shell fijada al grupo de usuarios

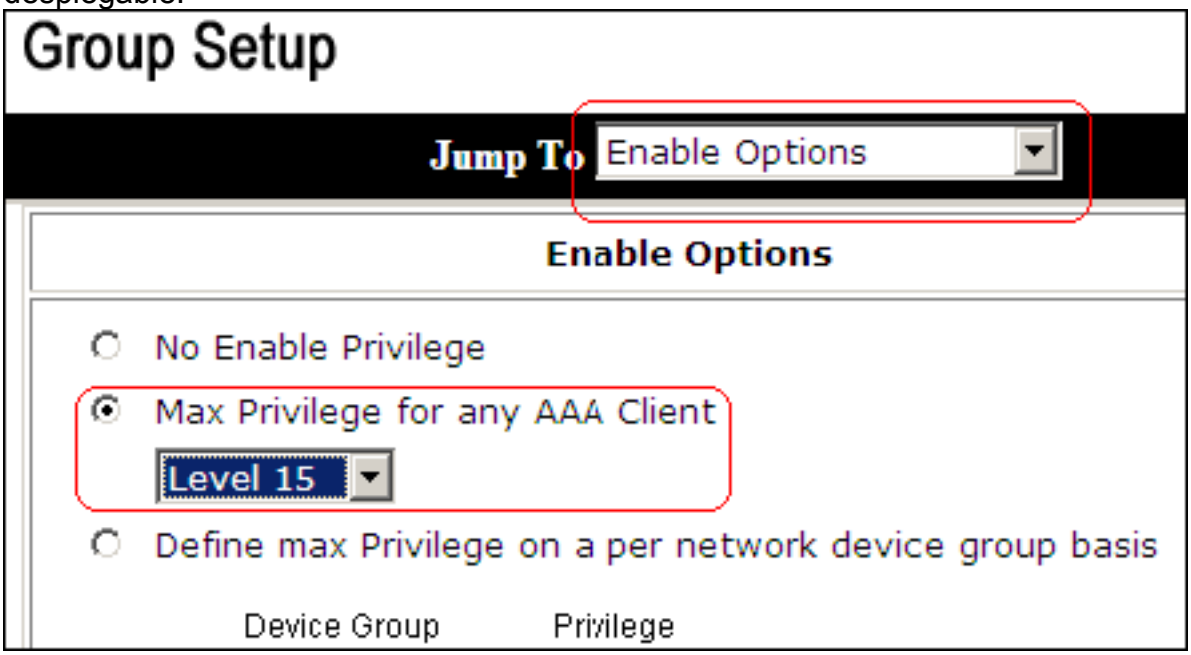
Refiera a configurar una autorización del comando shell fijada para una sección del grupo de usuarios del guía del usuario para el Cisco Secure Access Control Server 4.1 para más información sobre cómo configurar a los grupos determinados de la Configuración para el usuario de la autorización del comando shell.

Asocie la autorización del comando shell fijada (acceso de lectura/grabación) al grupo de usuarios (el admin group)

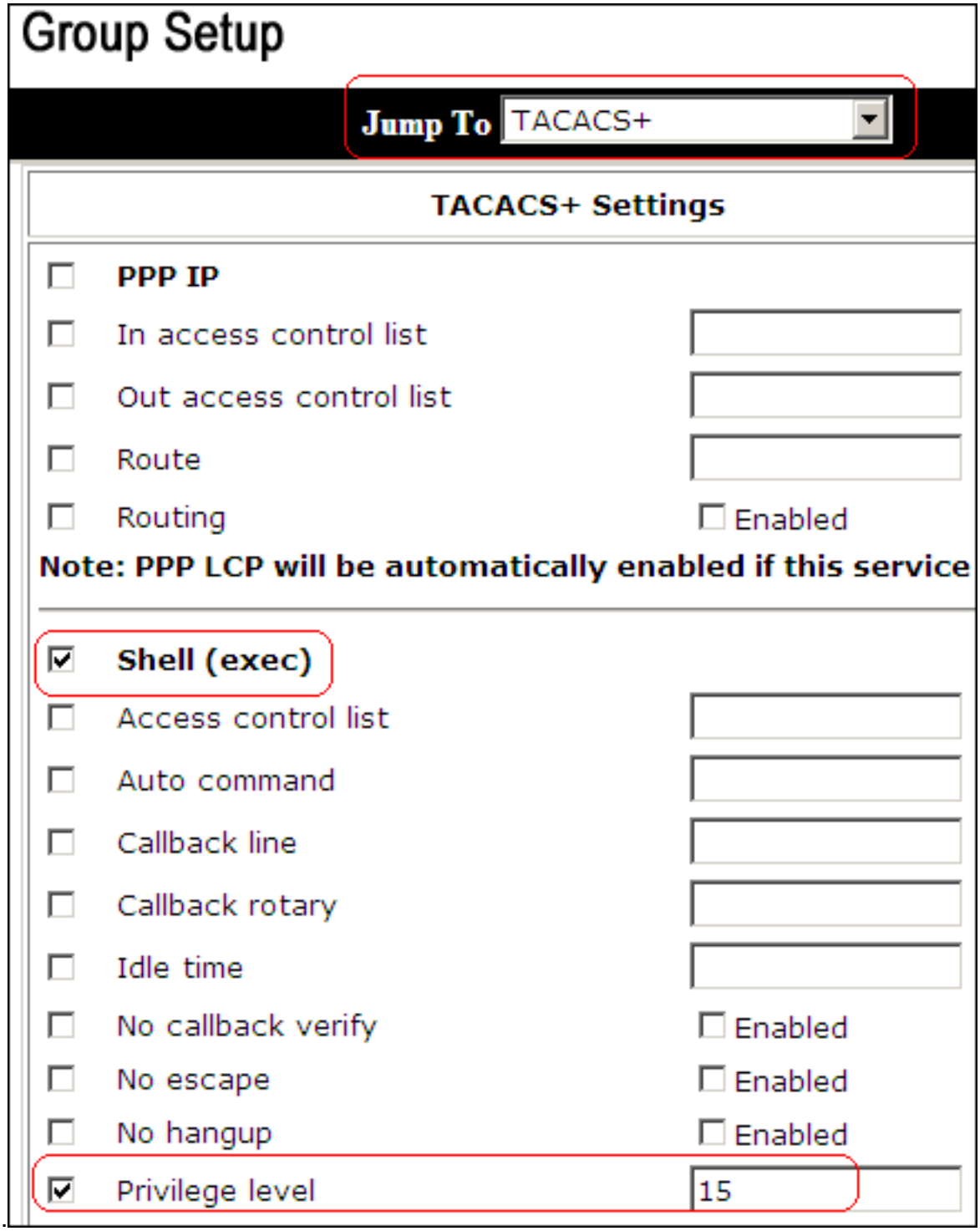
1. En la ventana ACS, haga clic la **configuración de grupo**, y elija el **admin group de la** lista desplegable del
grupo.



2. El tecleo **edita las configuraciones**.
3. Del salto a la lista desplegable, elija las **opciones del permiso**.
4. En el área de las opciones del permiso, haga clic el **privilegio máximo para cualquier** botón de radio del **cliente AAA**, y elija el **nivel 15 de la** lista desplegable.

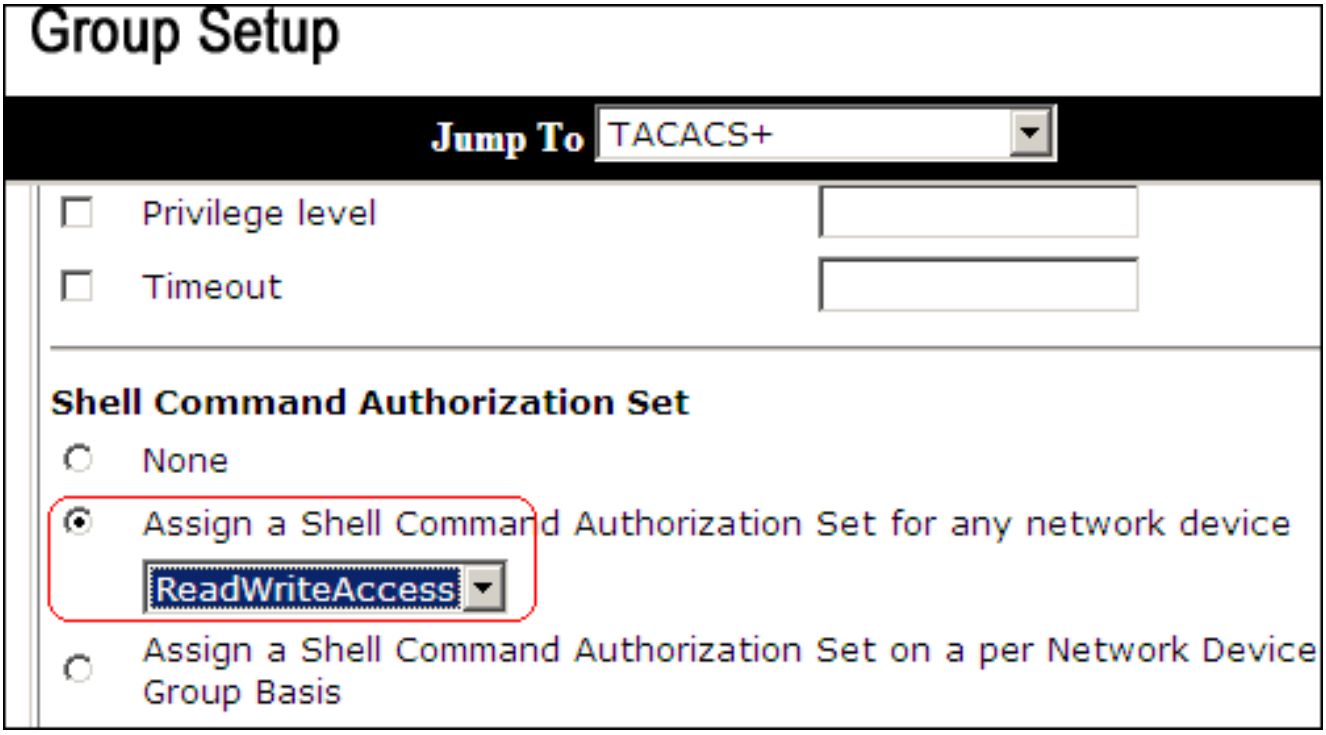


5. Del salto a la lista desplegable, elija el **TACACS+**.
6. En el área de las configuraciones TACACS+, marque la casilla de verificación del **shell (exec)**, marque la casilla de verificación del **nivel de privilegio**, y ingrese **15** en el campo del nivel de



privilegio.

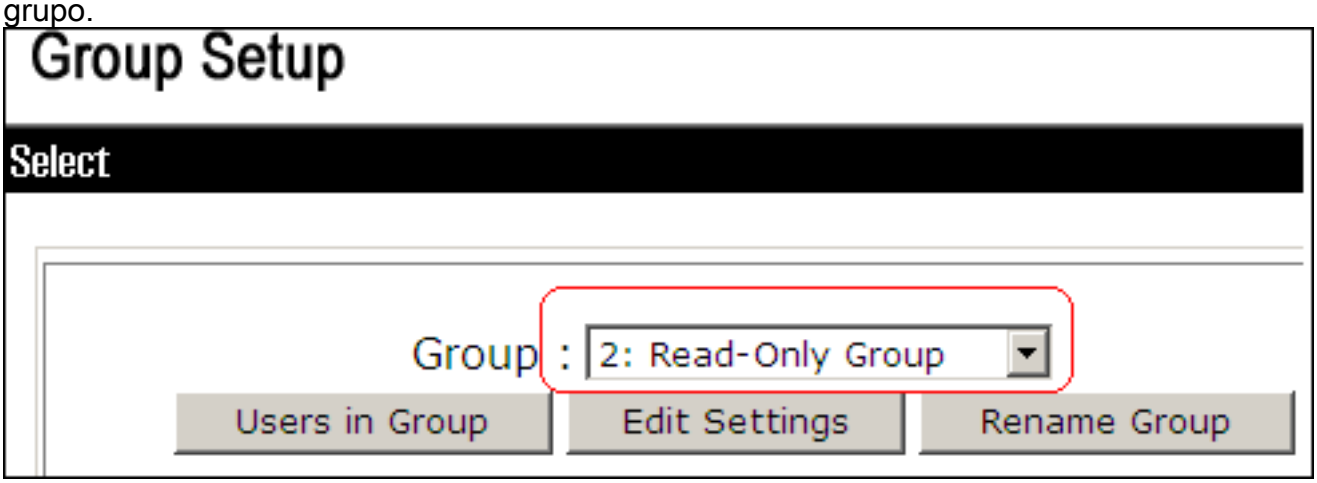
7. En el área determinada de la autorización del comando shell, haga clic la **asignación una autorización del comando shell fijada para cualquier** botón de radio del **dispositivo de red**, y elija **ReadWriteAccess de la** lista desplegable.



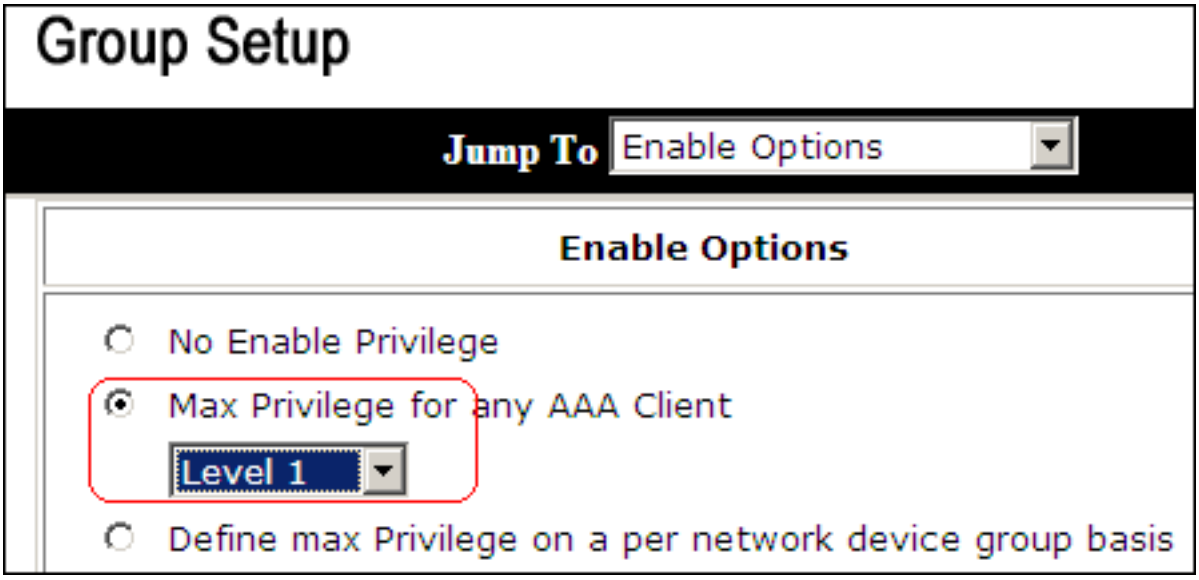
8. El tecleo **somete**

Asocie la autorización del comando shell fijada (acceso inalterable) al grupo de usuarios (el grupo solo lectura)

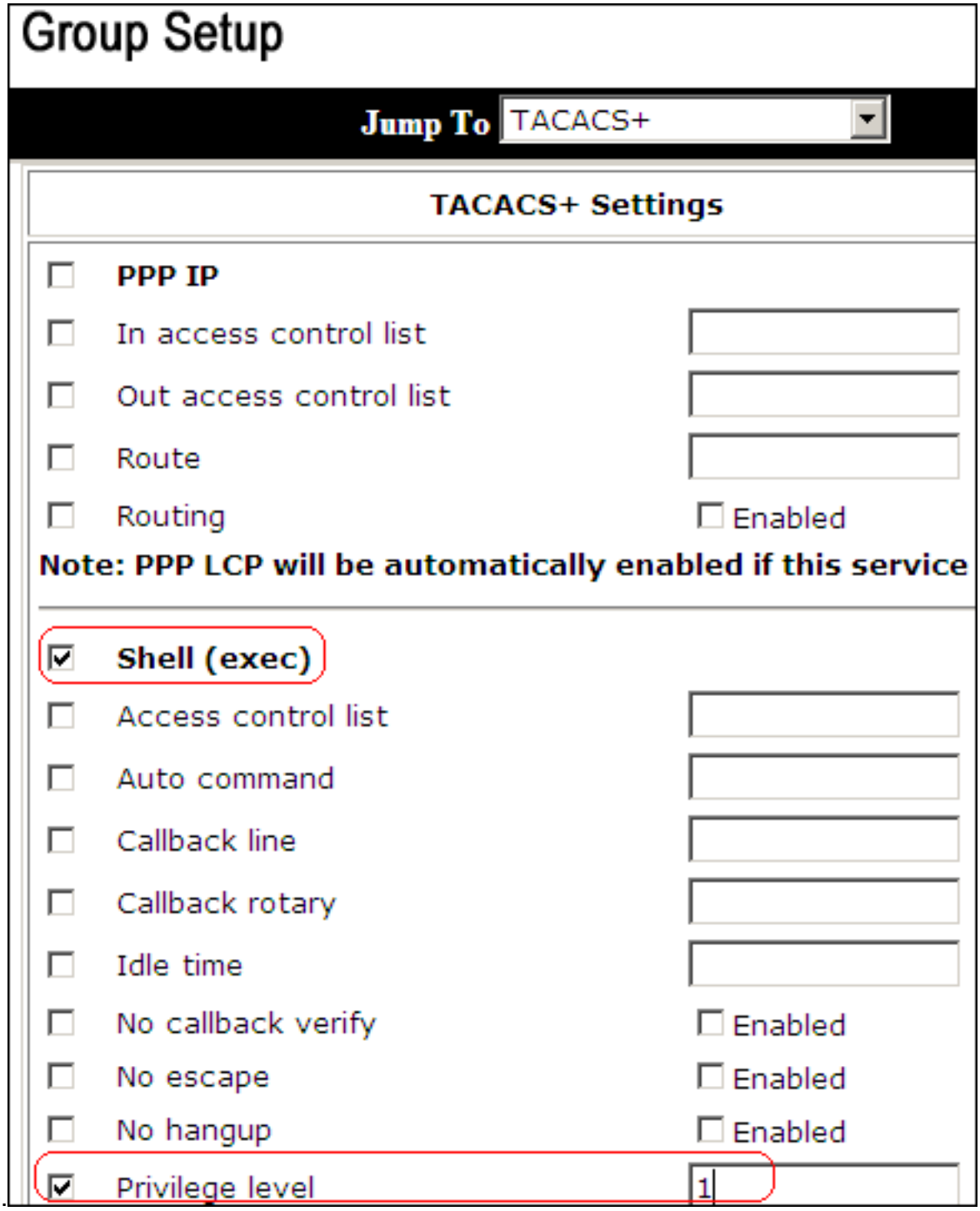
1. En la ventana ACS, haga clic la **configuración de grupo**, y elija al **grupo solo lectura de la** lista desplegable del grupo.



2. El tecleo **edita las configuraciones**.
3. Del salto a la lista desplegable, elija las **opciones del permiso**.
4. En el área de las opciones del permiso, haga clic el **privilegio máximo para cualquier** botón de radio del **cliente AAA**, y elija el **nivel 1 de la** lista desplegable.



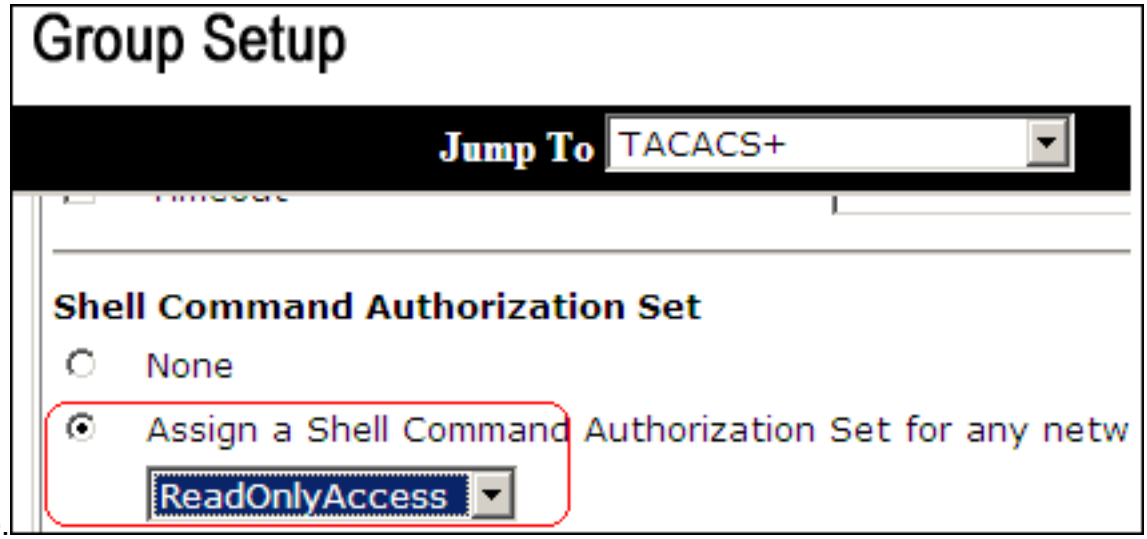
5. En el área de las configuraciones TACACS+, marque la casilla de verificación del **shell (exec)**, marque la casilla de verificación del **nivel de privilegio**, y ingrese **1** en el campo del nivel de



privilegio.

6. En el área determinada de la autorización del comando shell, haga clic la **asignación una autorización del comando shell fijada para cualquier** botón de radio del **dispositivo de red**, y elija **ReadOnlyAccess de la** lista

desplegable.



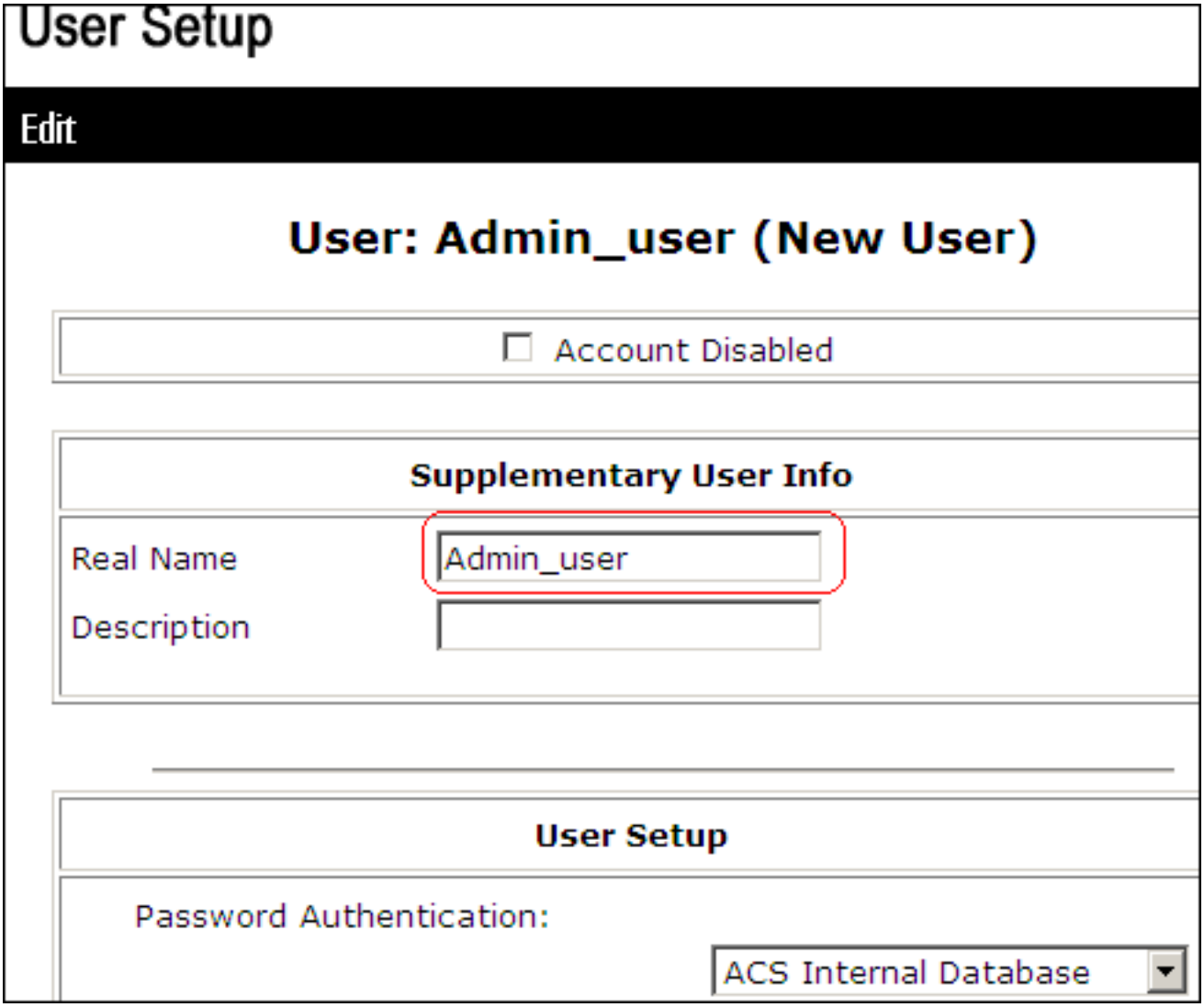
7. El tecleo **somete**

Asocie la autorización del comando shell fijada (Restrict_access) al usuario

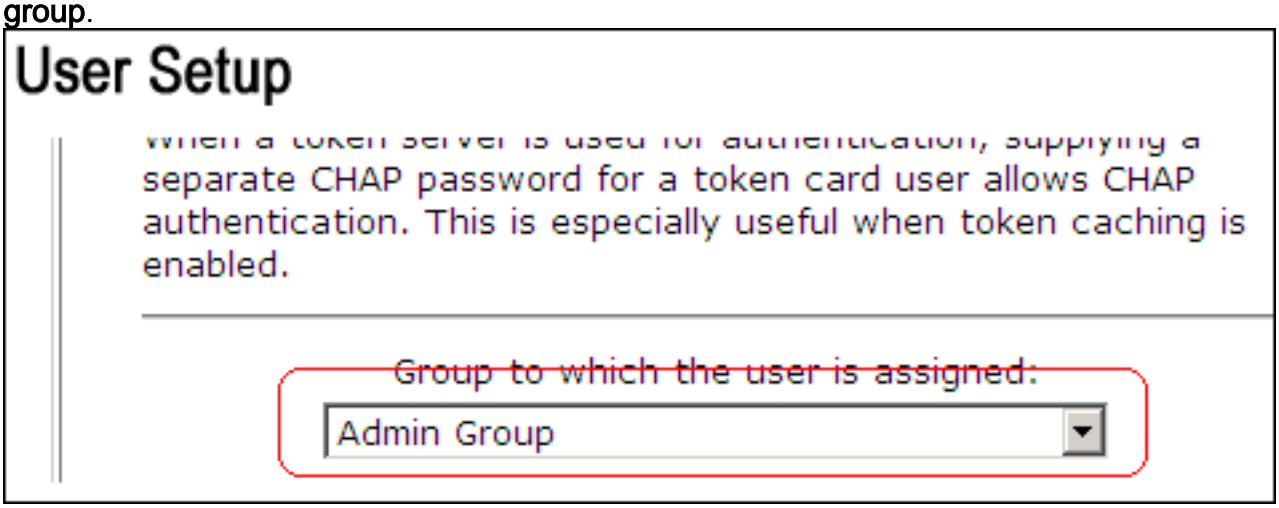
Refiera a configurar una autorización del comando shell fijada para una sección del usuario del guía del usuario para el Cisco Secure Access Control Server 4.1 para más información sobre cómo configurar la Configuración para el usuario determinada de la autorización del comando shell.

Nota: Las configuraciones del nivel de usuario reemplazan las configuraciones del grupo-nivel en el ACS, que significa si el usuario hace la autorización del comando shell fijar en las configuraciones del nivel de usuario, después reemplaza las configuraciones del grupo-nivel.

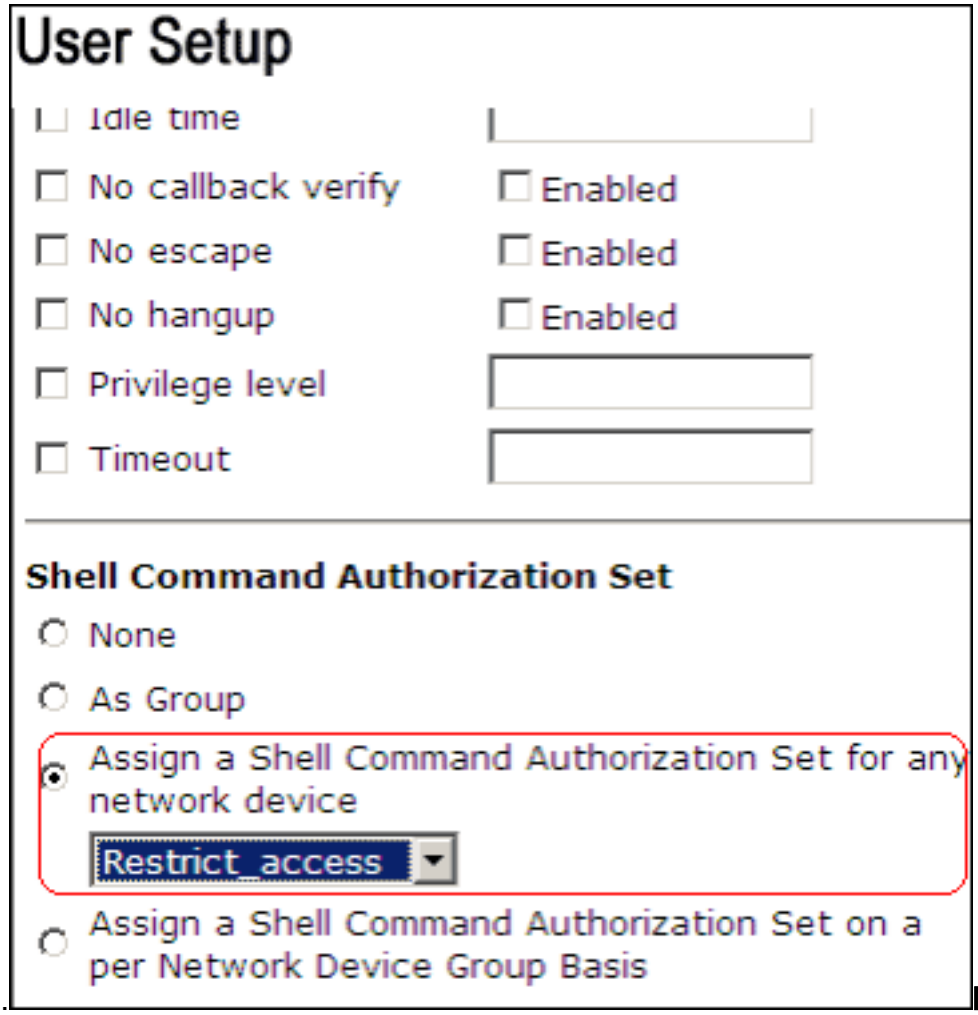
1. **La configuración de usuario del** tecleo **> Add/edita** para crear a un usuario nuevo nombrado *Admin_user* para ser admin group de la parte
de.



2. Del grupo a quien asignan el usuario la lista desplegable, elija el **admin group**.



3. En el área determinada de la autorización del comando shell, haga clic la **asignación una autorización del comando shell fijada para cualquier** botón de radio del **dispositivo de red**, y elija **Restrict_access de la** lista desplegable.**Nota:** En este escenario, este usuario es admin group de la parte de. El conjunto de la autorización del shell de *Restrict_access* es aplicable; el conjunto *de lectura/grabación de la* autorización del shell del *acceso* es no



corresponde.**Nota:** En la sección TACACS+ (Cisco) del área de la configuración de la interfaz, asegúrese de que la opción del **shell (exec)** esté seleccionada en la columna usuario.

Configuración del router IOS

Además de su configuración de la precolocación, estos comandos se requieren en un router IOS o un Switch para implementar el comando authorization a través de un servidor ACS:

```
aaa new-model
aaa authorization config-commands
aaa authorization commands 0 default  group tacacs+ local
aaa authorization commands 1 default  group tacacs+ local
aaa authorization commands 15 default group tacacs+ local
tacacs-server host 10.1.1.1
tacacs-server key cisco123
```

Configuración ASA/PIX/FWSM

Además de su configuración de la precolocación, estos comandos se requieren en ASA/PIX/FWSM para implementar el comando authorization a través de un servidor ACS:

```
aaa-server authserver protocol tacacs+
aaa-server authserver host 10.1.1.1
aaa authorization command authserver
```

Nota: No es posible utilizar el protocolo RADIUS para restringir el acceso del usuario al ASDM para los propósitos solo lecturas. Puesto que los paquetes RADIUS contienen la autenticación y autorización al mismo tiempo, todos los usuarios que se autentican en el servidor de RADIUS

tienen un nivel de privilegio de 15. Usted puede alcanzar esto con el TACACS con la implementación de los conjuntos del comando authorization.

Nota: ASA/PIX/FWSM tardan un tiempo prolongado para ejecutar cada comando tecleado incluso si el ACS es inasequible realizar el comando authorization. Si el ACS es inasequible y el ASA tiene el comando authorization configurado, el ASA todavía pedirá el comando authorization para cada comando.

Troubleshooting

Error: comando authorization fallado

Problema

Después de que usted inicie sesión al Firewall a través del registro TACACS, los comandos no trabajan. Cuando usted ingresa un comando, se recibe este error: `comando authorization fallado`.

Solución

Complete estos pasos para resolver este problema:

1. Asegúrese que el Nombre de usuario correcto esté utilizado y que todos los privilegios requeridos están asignados al usuario.
2. Si el Nombre de usuario y los privilegios están correctos, verifique que el ASA tenga Conectividad con el ACS y que el ACS es activo.

Nota: Este error puede también ocurrir si la autorización del comando configurado del administrador equivocadamente para el local, así como TACACS, los usuarios. En este caso, realice una recuperación de contraseña para resolver el problema.

Información Relacionada

- Cisco PIX Firewall Software
- Referencias de Comandos de Cisco Secure PIX Firewall
- Avisos de campos de productos de seguridad (incluido PIX)
- Solicitudes de Comentarios (RFC)
- Página de soporte segura del Access Control Server del control de Cisco
- Soporte Técnico y Documentación - Cisco Systems