Ejemplo de Configuración de Conjuntos de Autorización de Comandos de Shell ACS en IOS y ASA/PIX/FWSM

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Convenciones
Conjuntos de autorización de comandos
Agregar un conjunto de autorización de comandos de shell
Escenario 1: Privilegio para acceso de lectura/escritura o acceso completo
Escenario 2: Privilegio de acceso de sólo lectura
Escenario 3: Privilegio para acceso restringido
Asociar el conjunto de autorización de comandos de shell al grupo de usuarios
Asociar el conjunto de autorización de comandos de shell (acceso de lectura y escritura) al grupo de usuarios (grupo de administradores)
Asociar el conjunto de autorización de comandos de shell (acceso de sólo lectura) al grupo de usuarios (grupo de sólo lectura)
Asociar el conjunto de autorización de comandos de shell (Restrict_access) al usuario
Configuración del router IOS
Configuración de ASA/PIX/FWSM
Troubleshoot
Error: error de autorización de comando
Información Relacionada

Introducción

Este documento describe cómo configurar los conjuntos de autorización de shell en Cisco Secure Access Control Server (ACS) para clientes AAA, como routers o switches Cisco IOS® y Cisco Security Appliances (ASA/PIX/FWSM) con TACACS+ como protocolo de autorización.

Nota: ACS Express no admite la autorización de comandos.

Prerequisites

Requirements

Este documento asume que las configuraciones básicas se establecen en los clientes AAA y ACS.

En ACS, elija **Interface Configuration > Advanced Options**, y asegúrese de que la casilla de verificación **Per-user TACACS+/RADIUS Attributes** esté marcada.

Componentes Utilizados

La información de este documento se basa en Cisco Secure Access Control Server (ACS) que ejecuta la versión de software 3.3 y posteriores.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

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

Conjuntos de autorización de comandos

Los conjuntos de autorización de comandos proporcionan un mecanismo central para controlar la autorización de cada comando que se ejecuta en un dispositivo de red determinado. Esta característica mejora en gran medida la escalabilidad y la capacidad de administración necesarias para establecer restricciones de autorización.

En ACS, los conjuntos de autorización de comandos predeterminados incluyen Conjuntos de autorización de comandos de Shell y Conjuntos de autorización de comandos de PIX. Las aplicaciones de administración de dispositivos de Cisco, como CiscoWorks Management Center para firewalls, pueden indicar a ACS que admita tipos de conjuntos de autorización de comandos adicionales.

Nota: Los Conjuntos de Autorización de Comandos PIX requieren que la solicitud de autorización de comandos TACACS+ identifique el servicio como *pixshell*. Verifique que este servicio se haya implementado en la versión de PIX OS que utilizan sus firewalls; si no es así, utilice Conjuntos de autorización de comandos de shell para realizar la autorización de comandos para dispositivos PIX. Consulte Configuración de un Conjunto de Autorización de Comandos de Shell para un Grupo de Usuarios para obtener más información.

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

Nota: Los dispositivos de seguridad de Cisco (ASA/PIX) no permiten actualmente que el usuario se coloque directamente en el modo de activación durante el inicio de sesión. El usuario debe entrar manualmente en el modo de activación.

Para ofrecer un mayor control de las sesiones Telnet administrativas alojadas en dispositivos, un dispositivo de red que utiliza TACACS+ puede solicitar autorización para cada línea de comandos antes de que se ejecute. Puede definir un conjunto de comandos que se permiten o deniegan para su ejecución por un usuario determinado en un dispositivo determinado. ACS ha mejorado

aún más esta capacidad con estas funciones:

- **Conjuntos de autorización de comandos con nombre reutilizables**: sin citar directamente a ningún usuario o grupo de usuarios, puede crear un conjunto con nombre de autorizaciones de comandos. Puede definir varios conjuntos de autorización de comandos que delimitan diferentes perfiles de acceso. Por ejemplo:Un conjunto de autorización de comandos *Help desk* podría permitir el acceso a comandos de navegación de alto nivel, como **show run**, y denegar cualquier comando de configuración.Un conjunto de autorización de comandos *All network engineering* podría contener una lista limitada de comandos permitidos para cualquier ingeniero de redes de la empresa.Un conjunto de autorización de comandos *Ingenieros de red local* podría permitir todos los comandos (e incluir comandos de configuración de dirección IP).
- **Granularidad de configuración fina**: puede crear asociaciones entre conjuntos de autorización de comandos con nombre y grupos de dispositivos de red (NDG). De este modo, puede definir diferentes perfiles de acceso para los usuarios en función de los dispositivos de red a los que accedan. Puede asociar el mismo conjunto de autorización de comandos con nombre a más de un NDG y utilizarlo para más de un grupo de usuarios. ACS aplica la integridad de los datos. Los conjuntos de autorización de comandos con nombre se mantienen en la base de datos interna de ACS. Puede utilizar las funciones de copia de seguridad y restauración de ACS para realizar una copia de seguridad y restaurarlas. También puede replicar conjuntos de autorización de comandos en ACS secundarios junto con otros datos de configuración.

Para los tipos de conjuntos de autorización de comandos que admiten aplicaciones de administración de dispositivos de Cisco, las ventajas son similares cuando se utilizan conjuntos de autorización de comandos. Puede aplicar conjuntos de autorización de comandos a grupos ACS que contengan usuarios de la aplicación de administración de dispositivos para forzar la autorización de varios privilegios en una aplicación de administración de dispositivos. Los grupos ACS pueden corresponder a diferentes funciones dentro de la aplicación de administración de dispositivos, y puede aplicar diferentes conjuntos de autorización de comandos a cada grupo, según corresponda.

ACS tiene tres etapas secuenciales de filtrado de autorización de comandos. Cada solicitud de autorización de comandos se evalúa en el orden indicado:

1. **Coincidencia de comandos**: ACS determina si el comando que se procesa coincide con un comando enumerado en el conjunto de autorización de comandos. Si el comando no coincide, la autorización del comando viene determinada por la configuración Comandos no coincidentes: *permitir o rechazar.* De lo contrario, si el comando coincide, la evaluación continúa.
2. **Coincidencia de argumentos**: ACS determina si los argumentos de comando presentados coinciden con los argumentos de comando enumerados en el conjunto de autorización de comandos.Si algún argumento no coincide, la autorización del comando viene determinada por si está habilitada la opción Permitir argumentos no coincidentes. Si se permiten argumentos no coincidentes, se autoriza el comando y finaliza la evaluación; de lo contrario, el comando no se autoriza y finaliza la evaluación.Si todos los argumentos coinciden, la evaluación continúa.
3. **Directiva de argumentos**: una vez que ACS determina que los argumentos del comando coinciden con los argumentos del conjunto de autorización de comandos, ACS determina si cada argumento de comando está permitido explícitamente. Si se permiten explícitamente todos los argumentos, ACS otorga la autorización de comando. Si no se permite ningún

argumento, ACS deniega la autorización de comandos.

Agregar un conjunto de autorización de comandos de shell

Esta sección incluye estos escenarios que describen cómo agregar un conjunto de autorización de comandos:

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

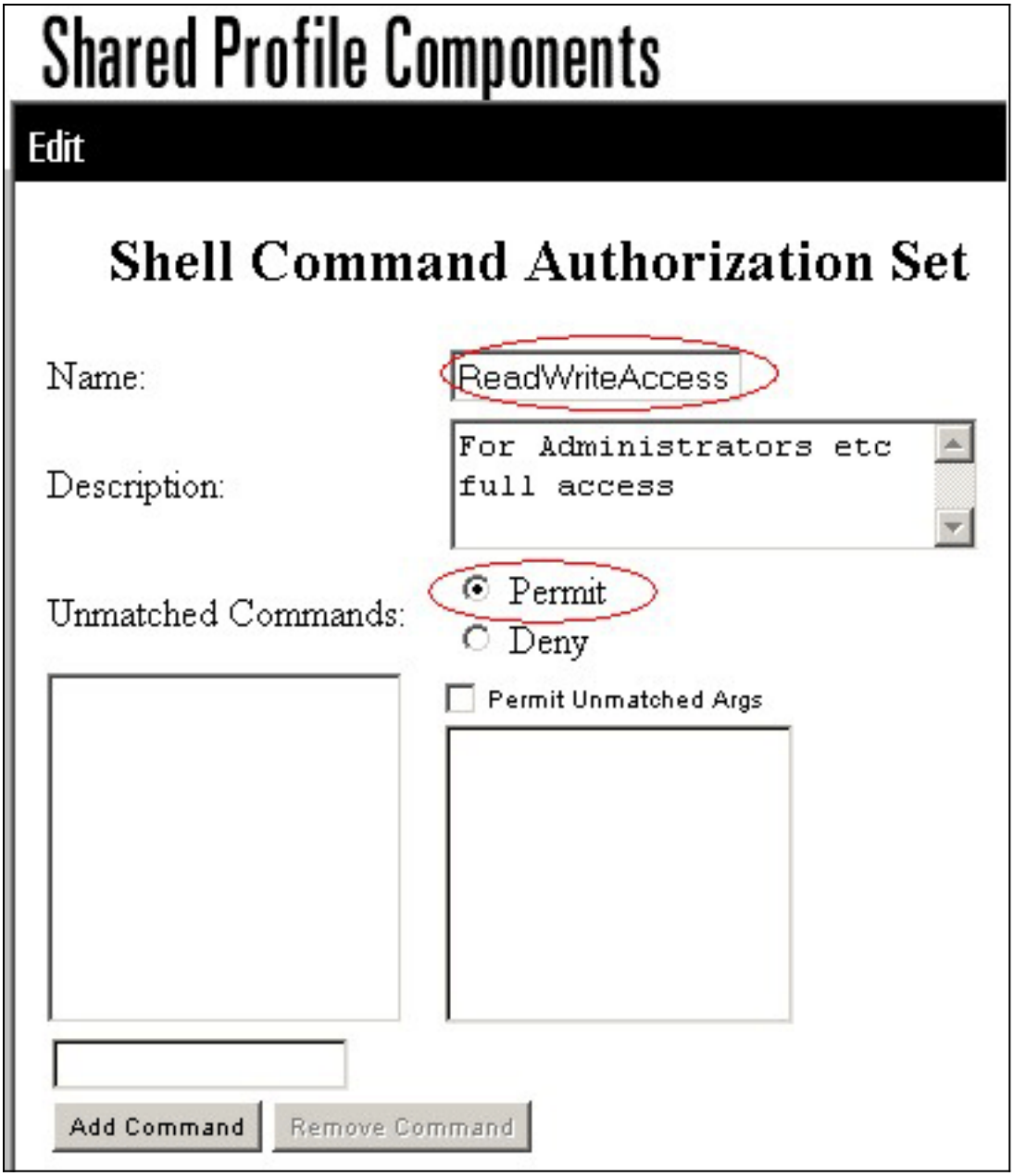
Nota: Refiérase a la sección Adición de un Conjunto de Autorización de Comandos de la Guía del Usuario para Cisco Secure Access Control Server 4.1 para obtener más información sobre cómo crear conjuntos de autorización de comandos. Consulte Edición de un conjunto de autorización de comandos y Eliminación de un conjunto de autorización de comandos para obtener más información sobre cómo editar y eliminar conjuntos de autorización de comandos.

Escenario 1: Privilegio para acceso de lectura/escritura o acceso completo

En estos escenarios, los usuarios tienen acceso de lectura y escritura (o total).

En el área Conjunto de autorización de comandos de shell de la ventana Componentes de perfil compartido, configure estos valores:

1. En el campo Nombre, escriba **ReadWriteAccess** como nombre del conjunto de autorización de comandos.
2. En el campo Descripción, escriba una descripción para el conjunto de autorización de comandos.
3. Haga clic en el botón de opción **Permitir** y, a continuación, haga clic en **Enviar**.

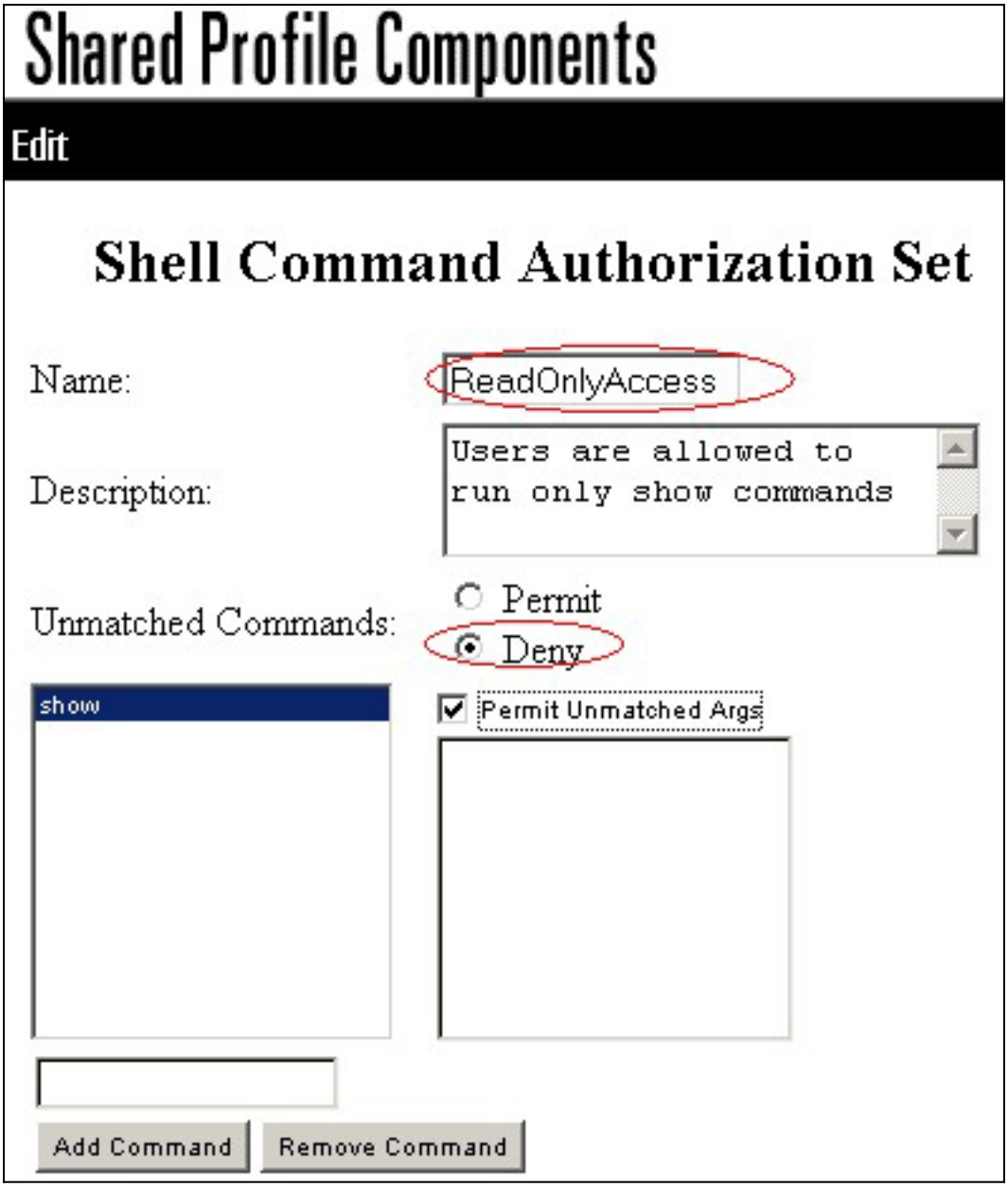


Escenario 2: Privilegio de acceso de sólo lectura

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

En el área Conjunto de autorización de comandos de shell de la ventana Componentes de perfil compartido, configure estos valores:

1. En el campo Nombre, escriba **ReadOnlyAccess** como nombre del conjunto de autorización de comandos.
2. En el campo Descripción, escriba una descripción para el conjunto de autorización de comandos.
3. Haga clic en el botón de opción **Denegar**.
4. Ingrese el comando **show** en el campo sobre el botón Add Command, y luego haga clic en **Add Command**.
5. Marque la casilla de verificación **Permitir argumentos no coincidentes** y haga clic en **Enviar**

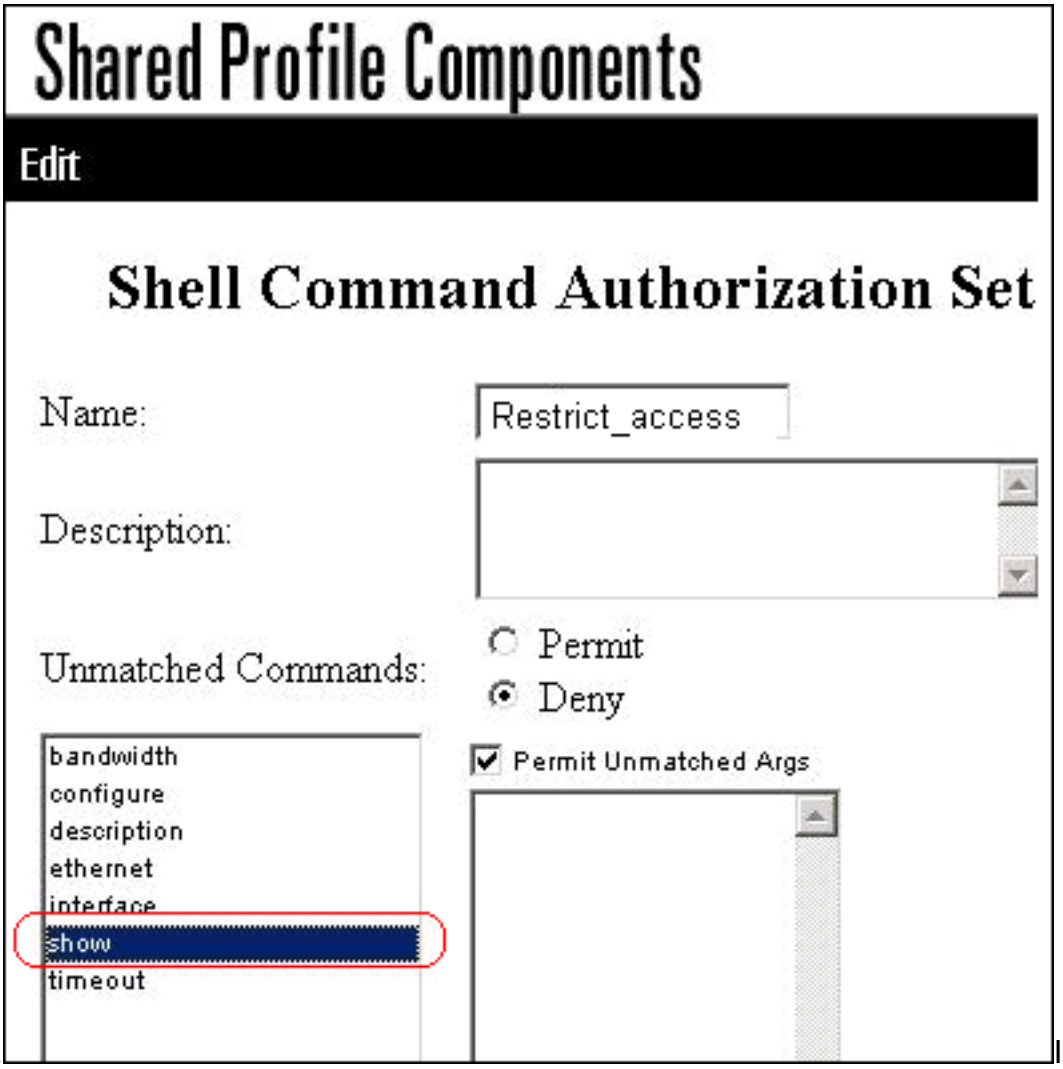


Escenario 3: Privilegio para acceso restringido

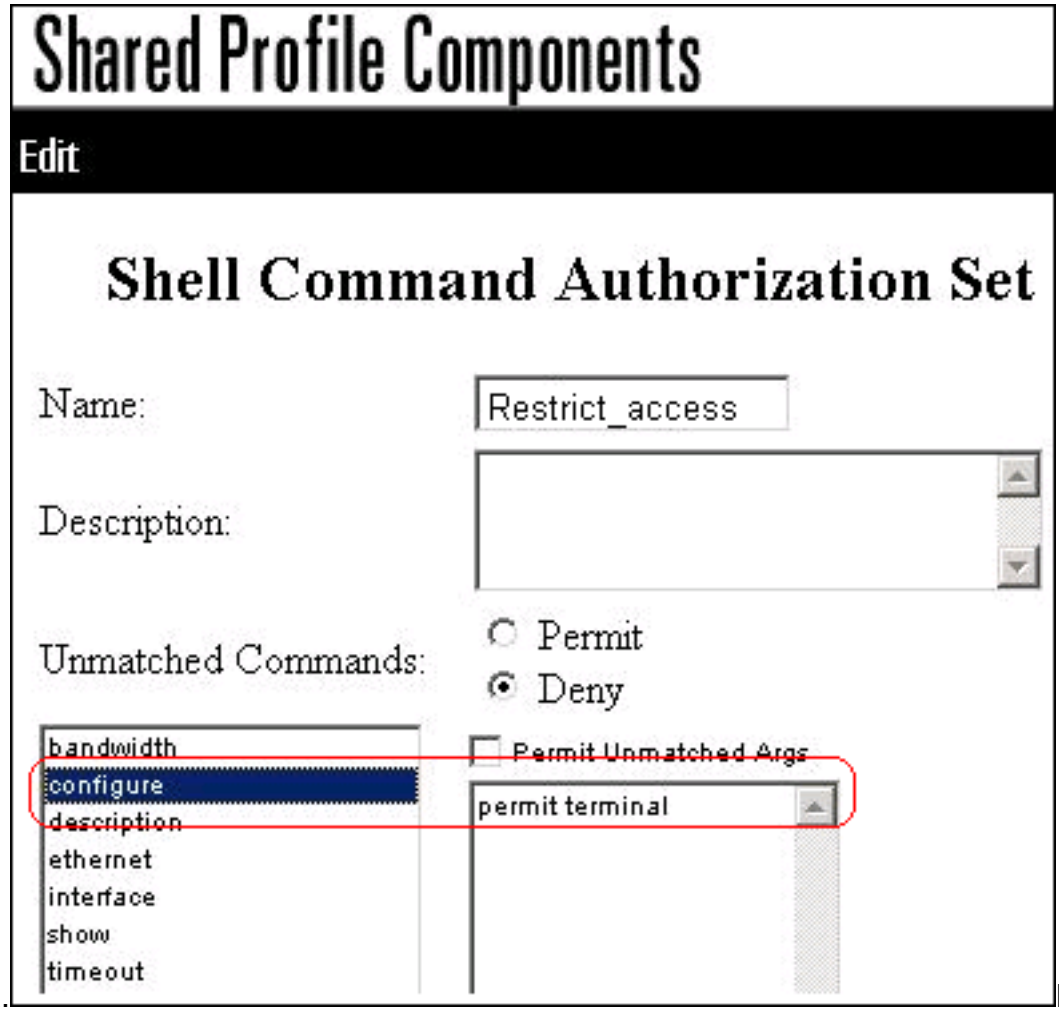
En esta situación, los usuarios pueden utilizar comandos selectivos.

En el área Conjunto de autorización de comandos de shell de la ventana Componentes de perfil compartido, configure estos valores:

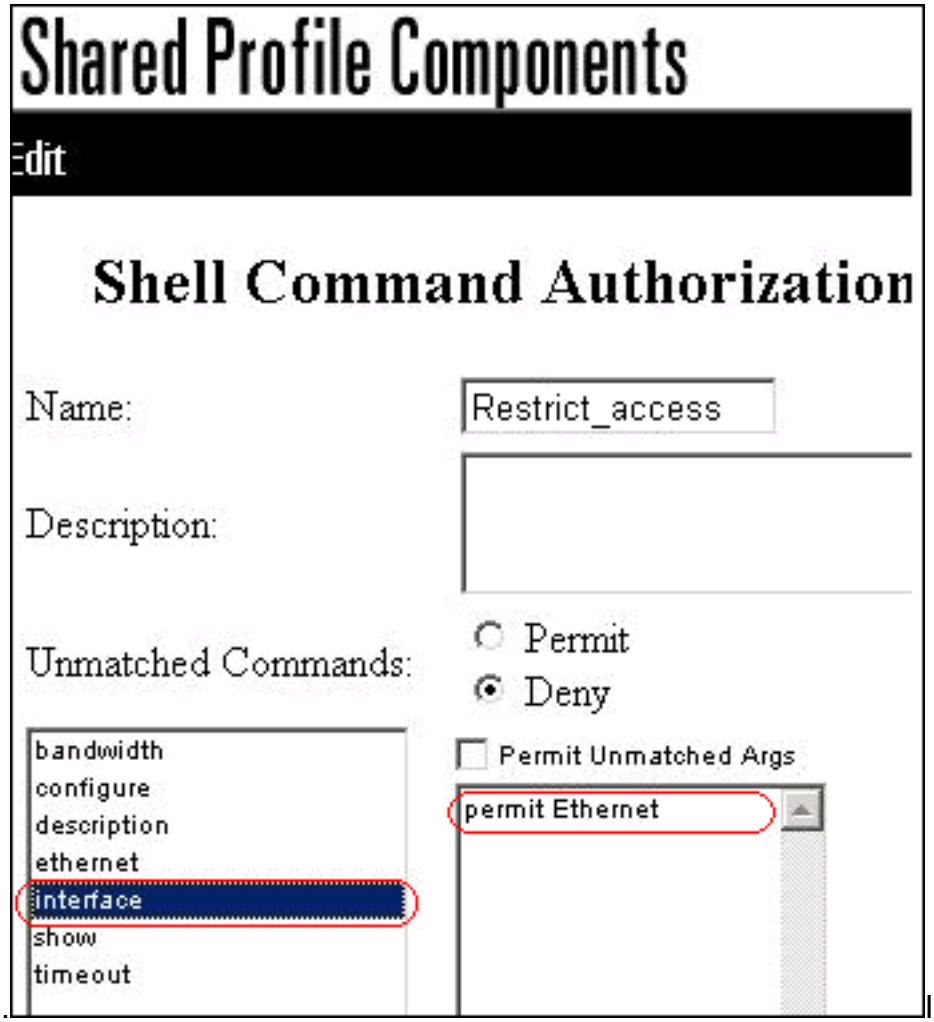
1. En el campo de nombre, ingrese **Restrict_access** como el nombre del conjunto de autorización de comandos.
2. Haga clic en el botón de opción **Denegar**.
3. Introduzca los comandos que desea permitir en los clientes AAA.En el campo situado encima del botón Agregar comando, ingrese el comando **show** y haga clic en **Agregar**



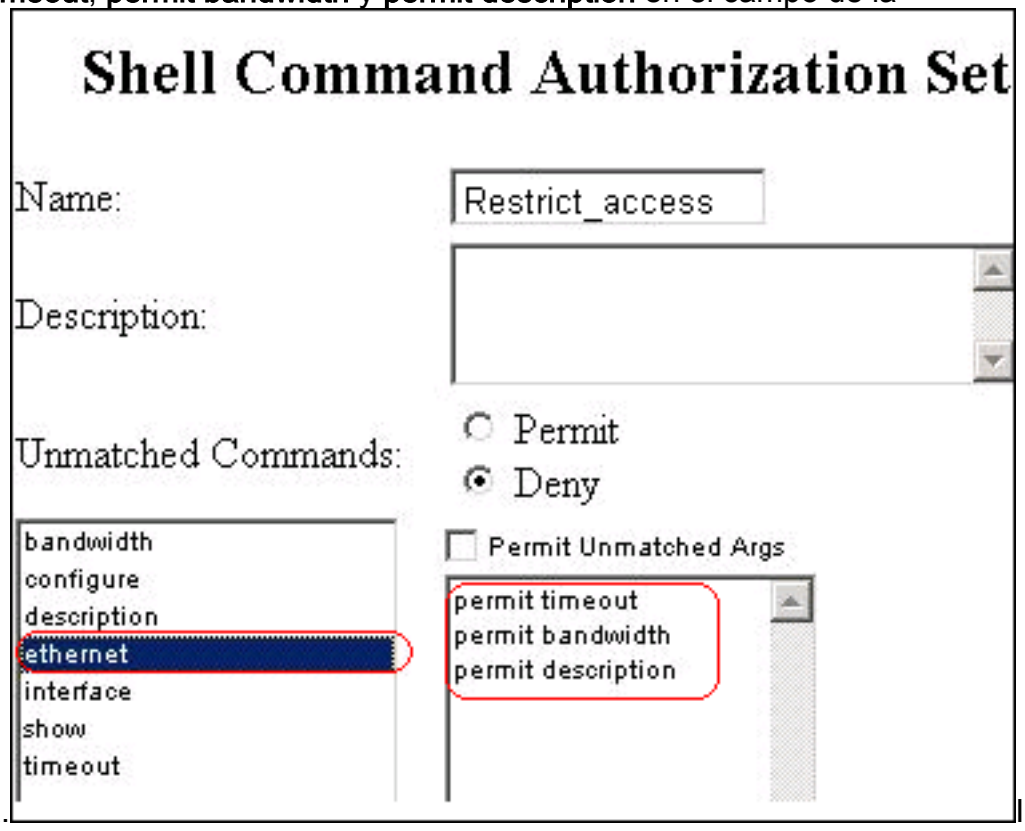
comando.Ingrese el comando **configure** y haga clic en **Add Command**.Seleccione el comando **configure** y escriba **permit terminal** en el campo de la



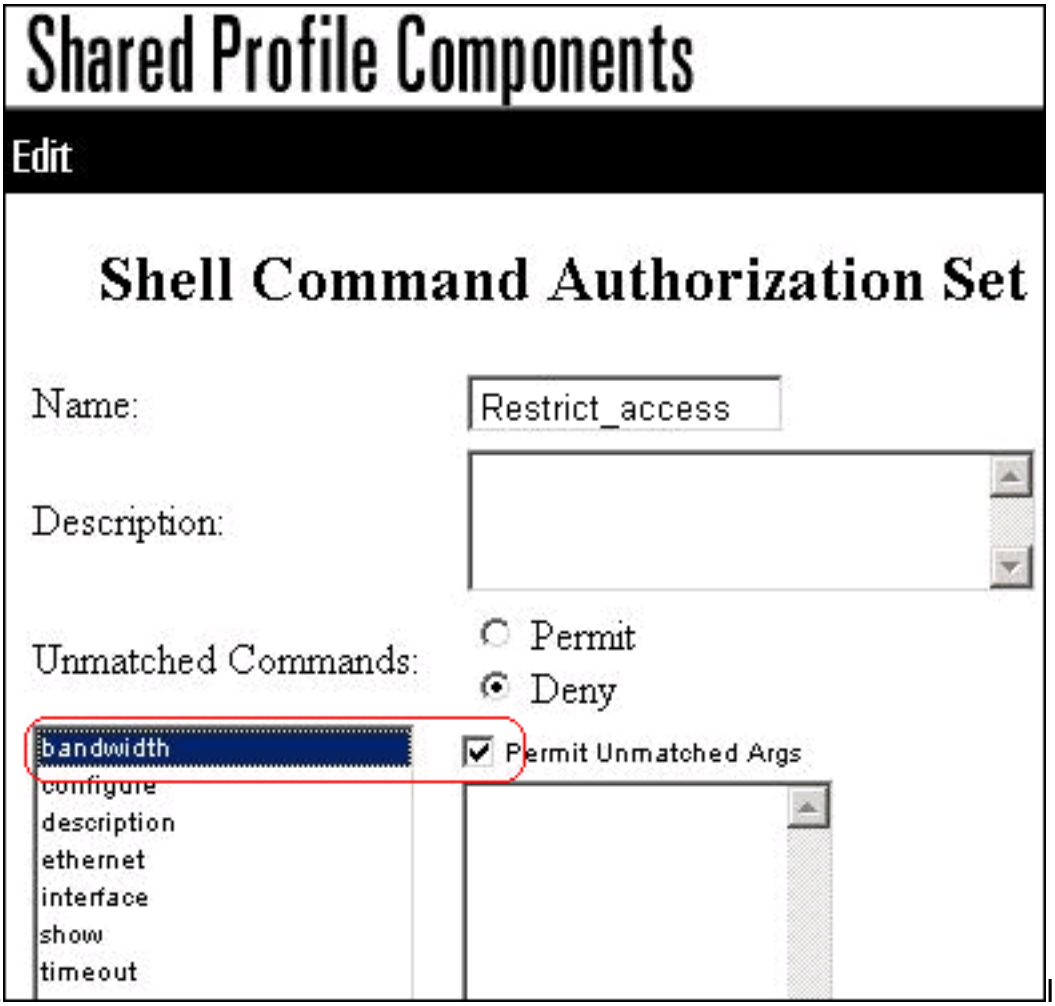
derecha. Ingrese el comando **interface** y haga clic en **Add Command**.Seleccione el comando **interface** y escriba **permit Ethernet** en el campo de la



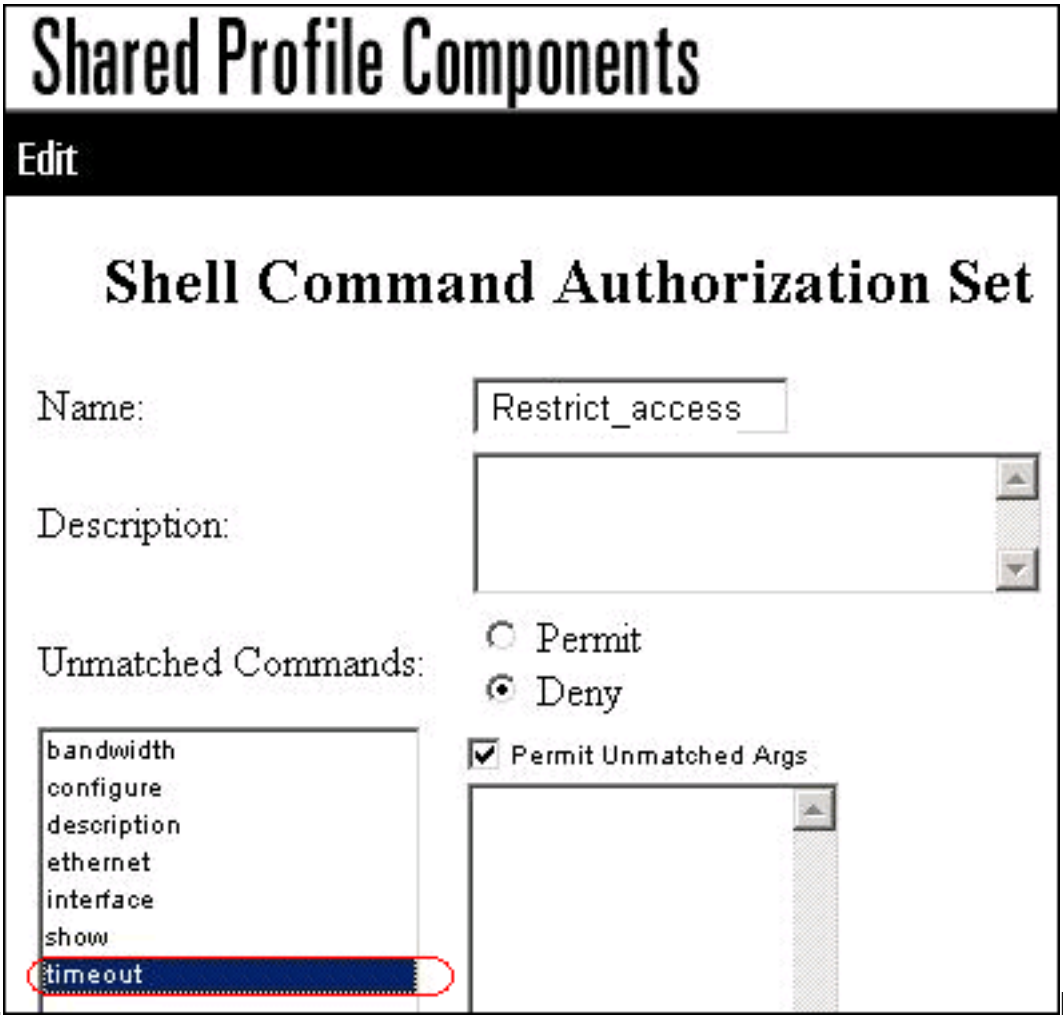
derecha. Ingrese el comando **ethernet** y haga clic en **Add Command**.Seleccione el comando **interface** e ingrese **permit timeout**, **permit bandwidth** y **permit description** en el campo de la



derecha. Ingrese el comando **bandwidth** y haga clic en **Add**

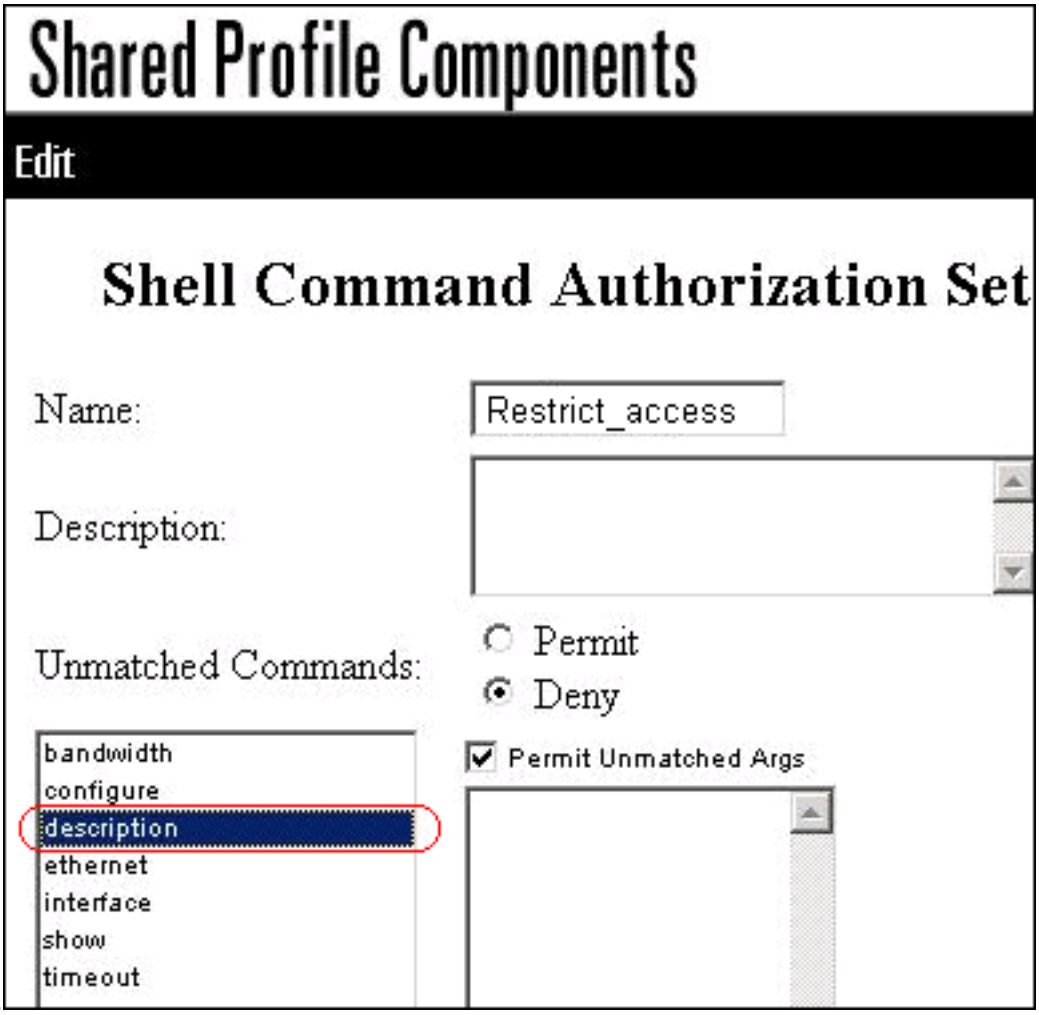


Command. Ingrese el comando **timeout** y haga clic en **Add**



Command. Ingrese el comando **description** y haga clic en **Add**

Command.



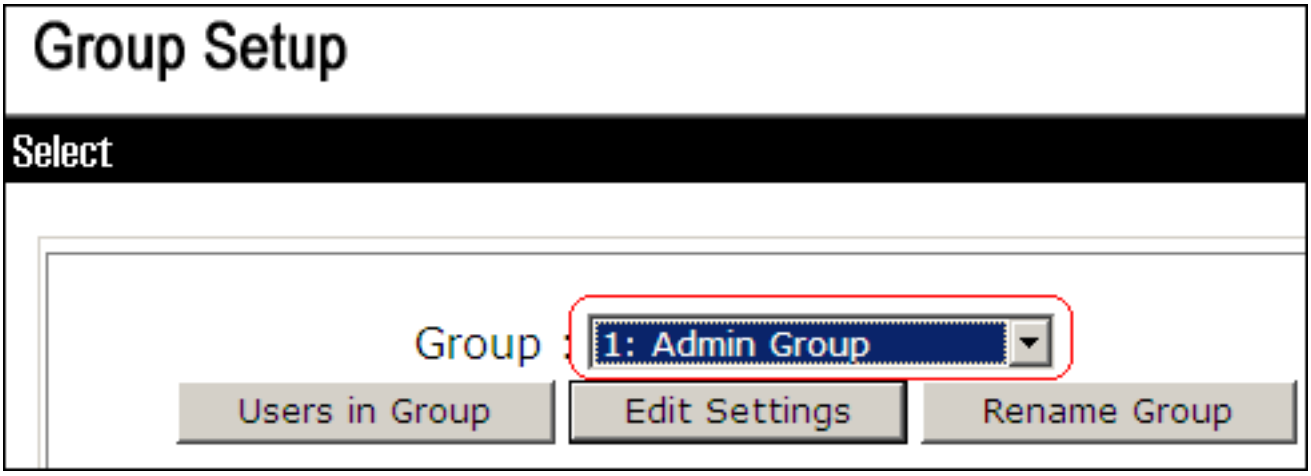
4. Haga clic en Submit (Enviar).

Asociar el conjunto de autorización de comandos de shell al grupo de usuarios

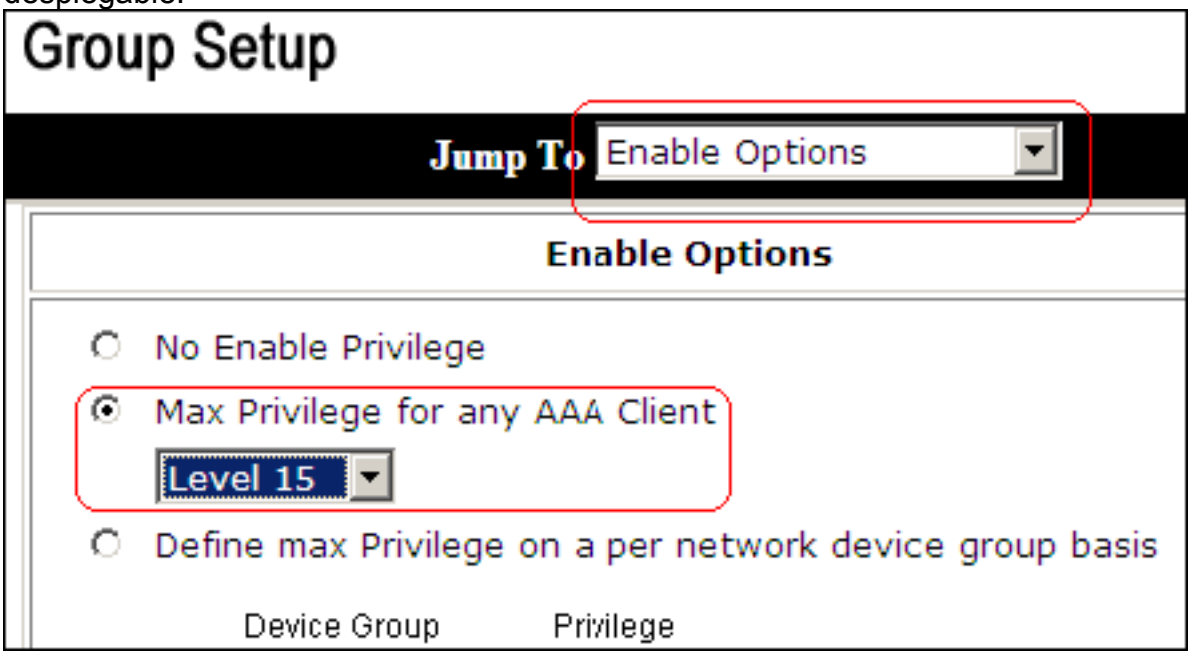
Consulte la sección Configuración de un Conjunto de Autorización de Comandos de Shell para un Grupo de Usuarios de la Guía del Usuario para Cisco Secure Access Control Server 4.1 para obtener más información sobre cómo configurar el conjunto de autorización de comandos de shell para los grupos de usuarios.

Asociar el conjunto de autorización de comandos de shell (acceso de lectura y escritura) al grupo de usuarios (grupo de administradores)

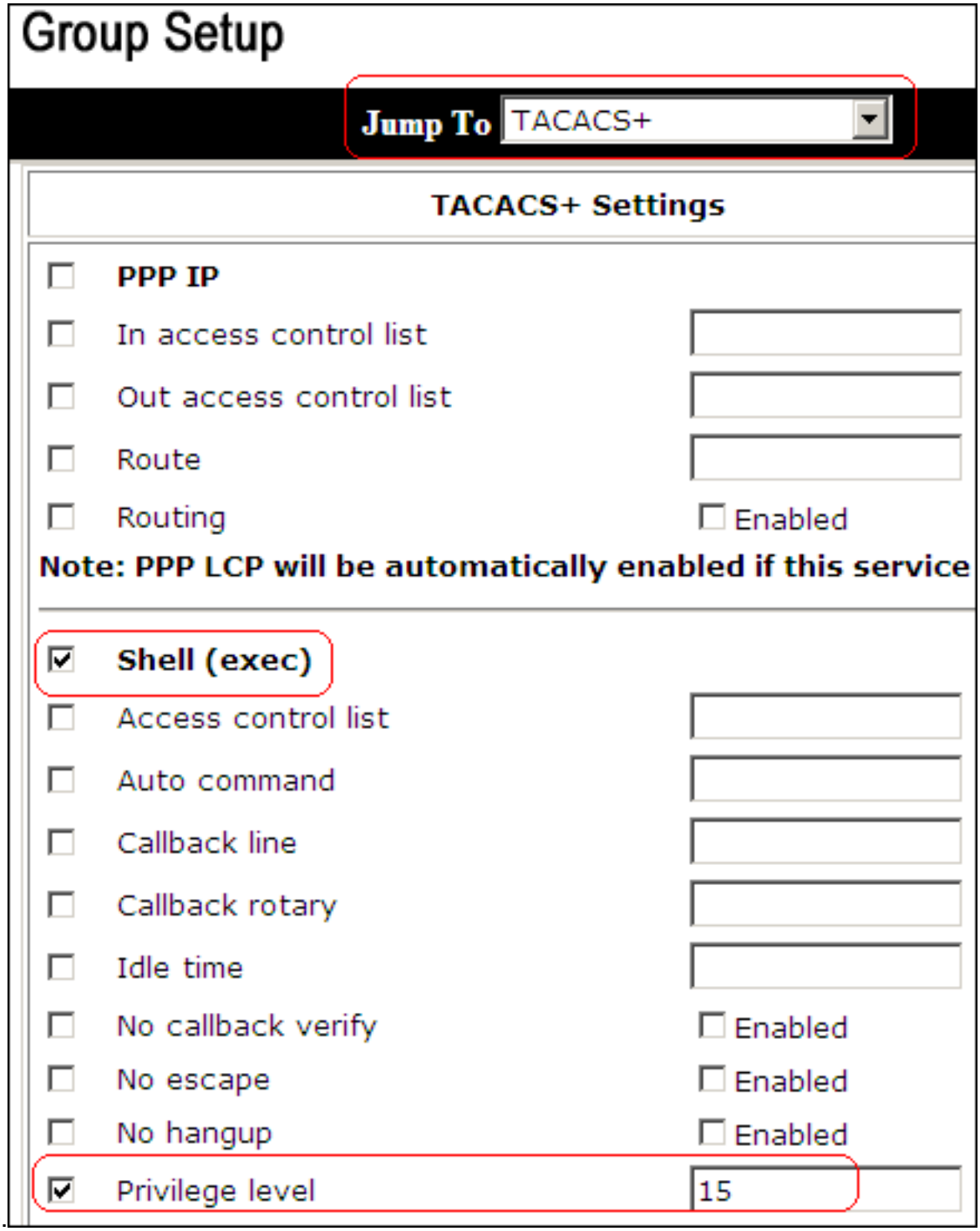
1. En la ventana ACS, haga clic en **Group Setup**, y elija **Admin Group** en la lista desplegable Group.



2. Haga clic en **Edit Settings**.
3. En la lista desplegable Jump To, elija **Enable Options**.
4. En el área Habilitar opciones, haga clic en el botón de opción **Max Privilege for any AAA client** y elija **Level 15** en la lista desplegable.

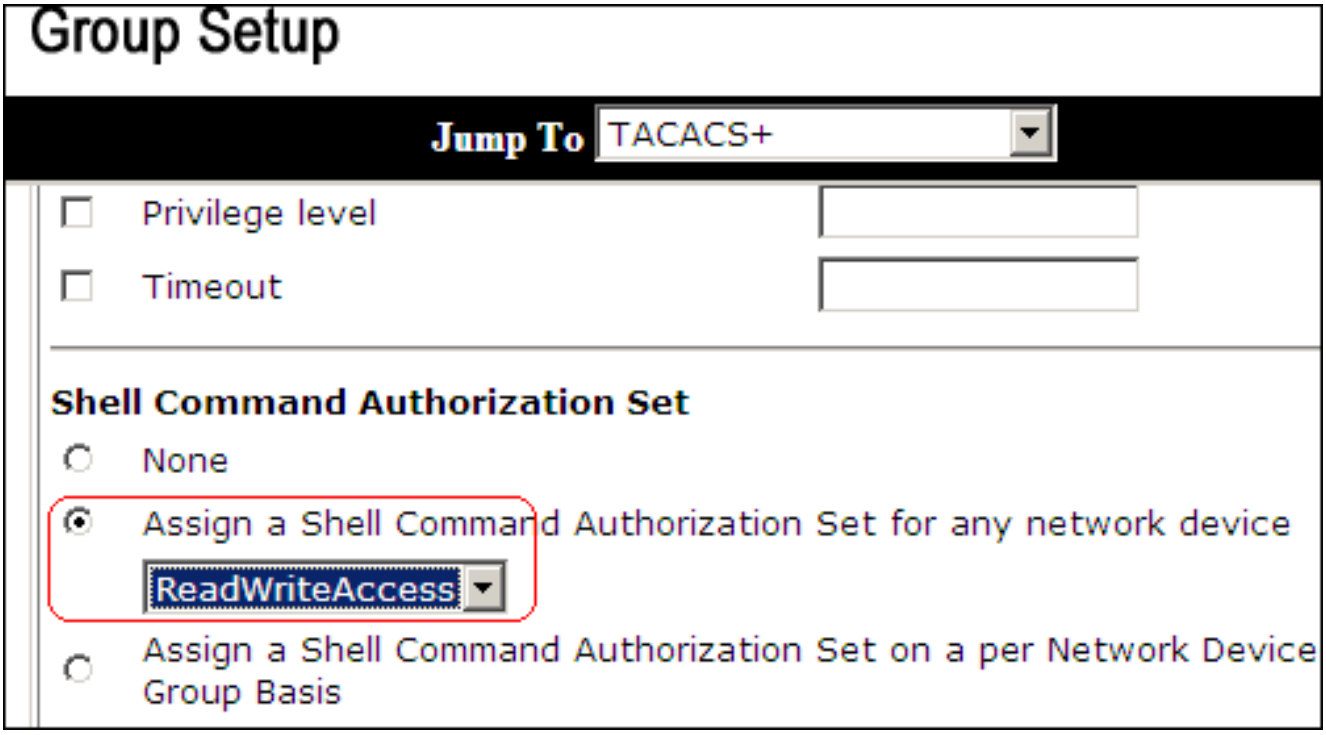


5. En la lista desplegable Jump To, elija **TACACS+**.
6. En el área Configuración de TACACS+, marque la casilla de verificación **Shell (exec)**, marque la casilla de verificación **Nivel de privilegio** y escriba **15** en el campo Nivel de



privilegio.

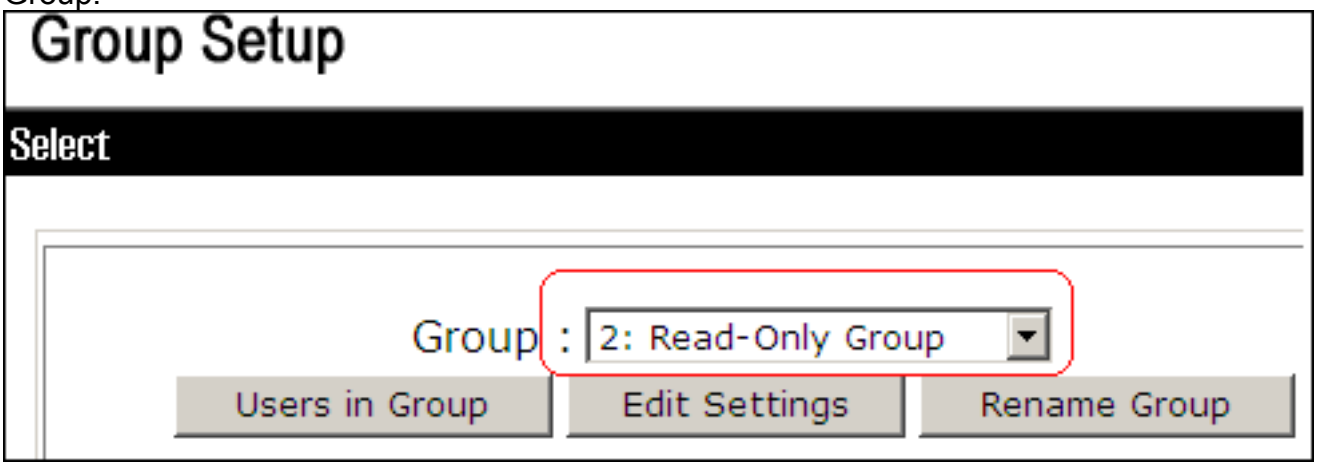
7. En el área Conjunto de autorización de comandos de shell, haga clic en el botón de opción **Asignar un conjunto de autorización de comandos de shell para cualquier dispositivo de red** y elija **ReadWriteAccess** en la lista desplegable.



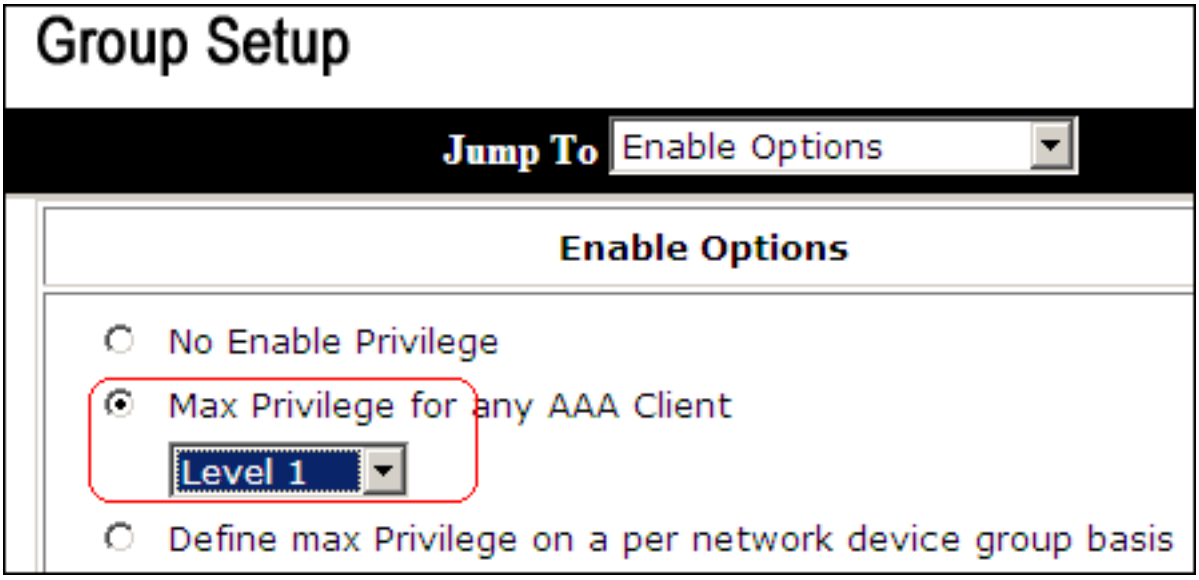
8. Haga clic en Submit (Enviar)

Asociar el conjunto de autorización de comandos de shell (acceso de sólo lectura) al grupo de usuarios (grupo de sólo lectura)

1. En la ventana ACS, haga clic en **Group Setup**, y elija **Read-Only Group** en la lista desplegable
Group.

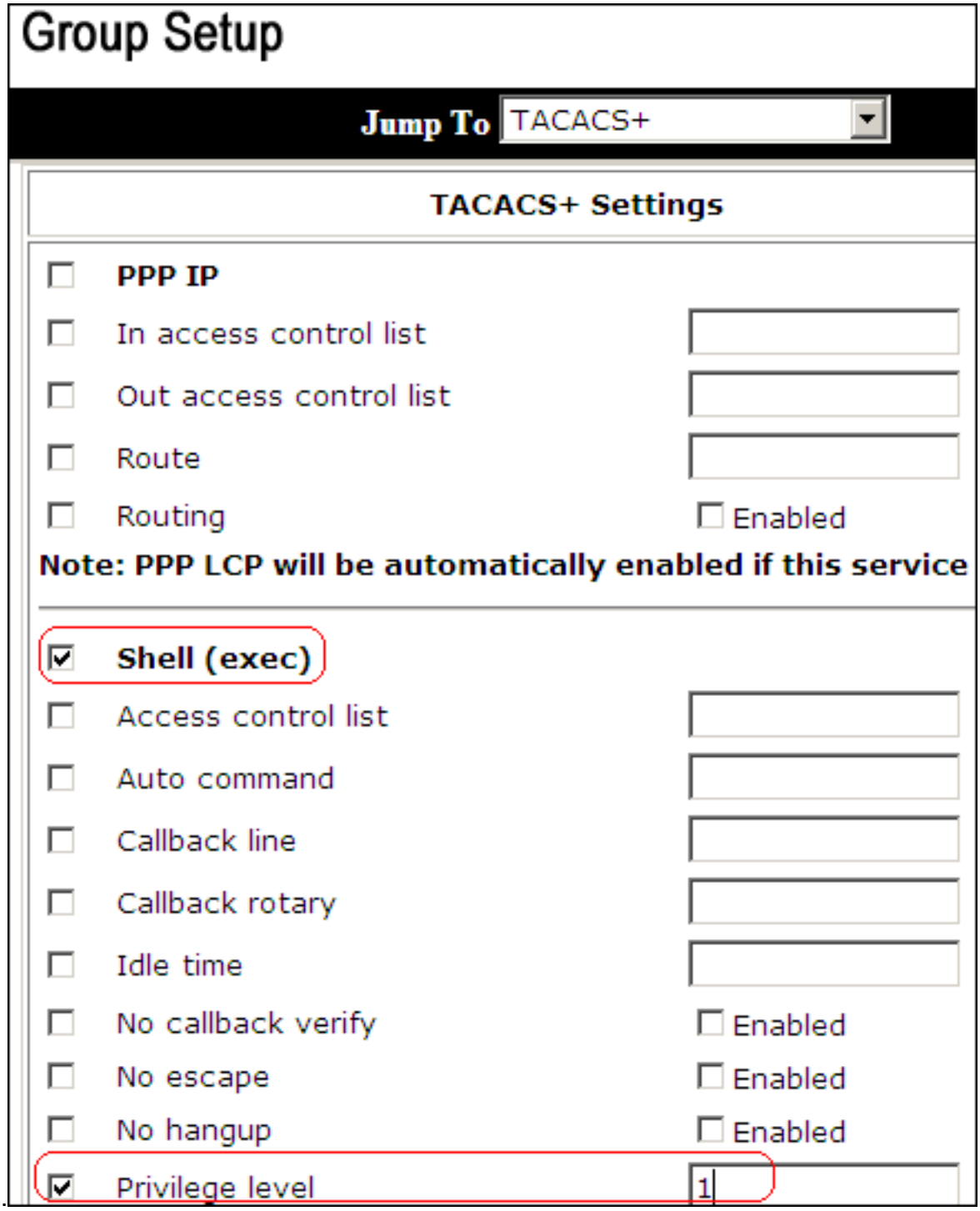


2. Haga clic en **Edit Settings**.
3. En la lista desplegable Jump To, elija **Enable Options**.
4. En el área Habilitar opciones, haga clic en el botón de opción **Max Privilege for any AAA client** y elija **Level 1** en la lista
desplegable.



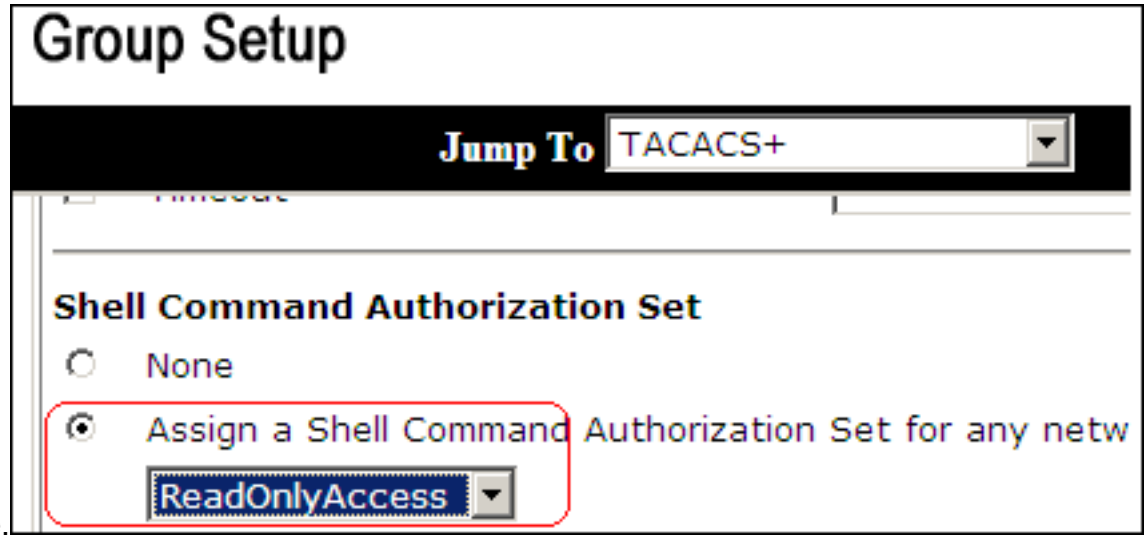
5. En el área Configuración de TACACS+, marque la casilla de verificación **Shell (exec)**, marque la casilla de verificación **Nivel de privilegio** y escriba **1** en el campo Nivel de

privilegio.



6. En el área Conjunto de autorización de comandos de shell, haga clic en el botón de opción **Asignar un conjunto de autorización de comandos de shell para cualquier dispositivo de red** y elija **ReadOnlyAccess** en la lista

desplegable.



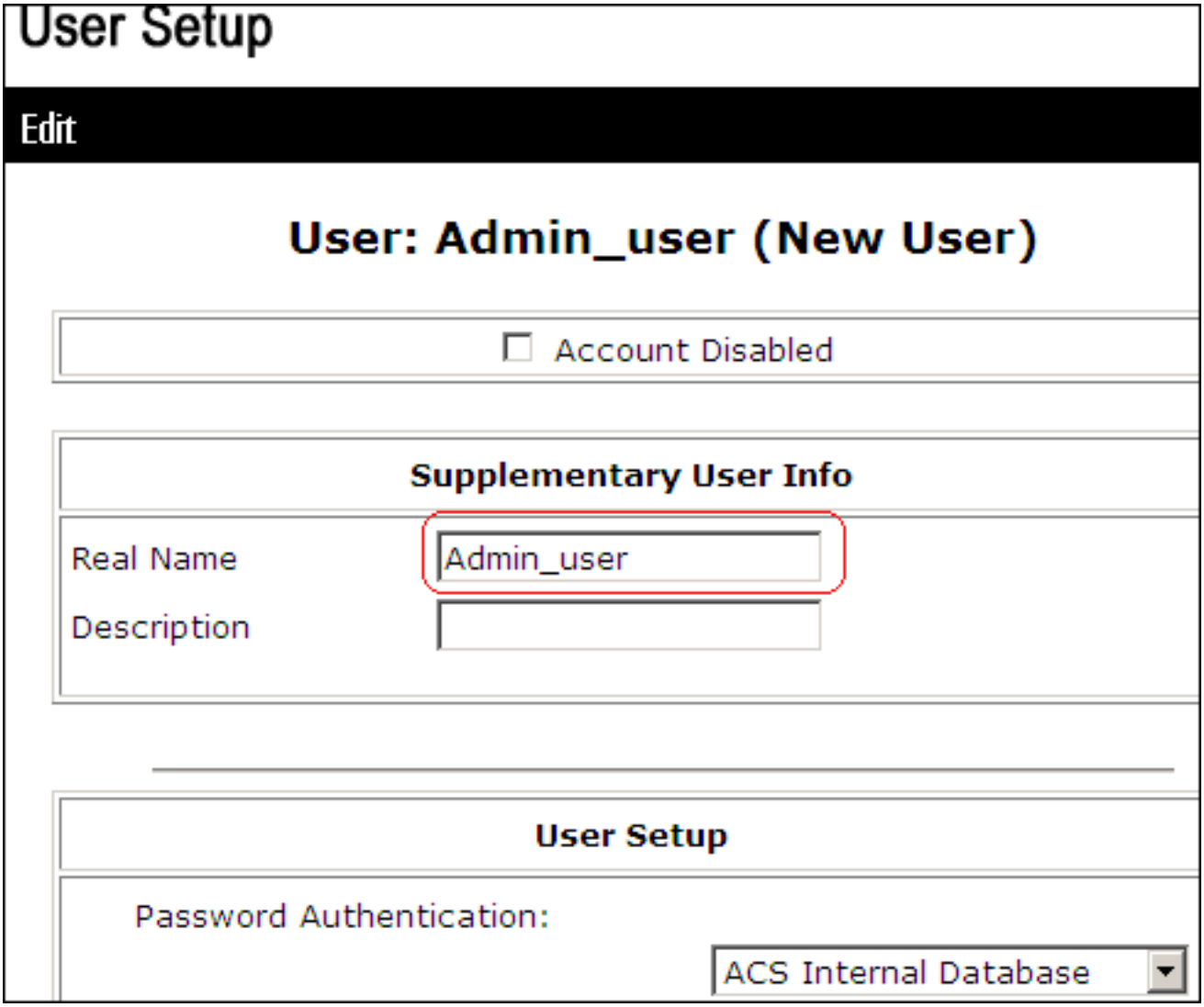
7. Haga clic en Submit (Enviar)

Asociar el conjunto de autorización de comandos de shell (Restrict_access) al usuario

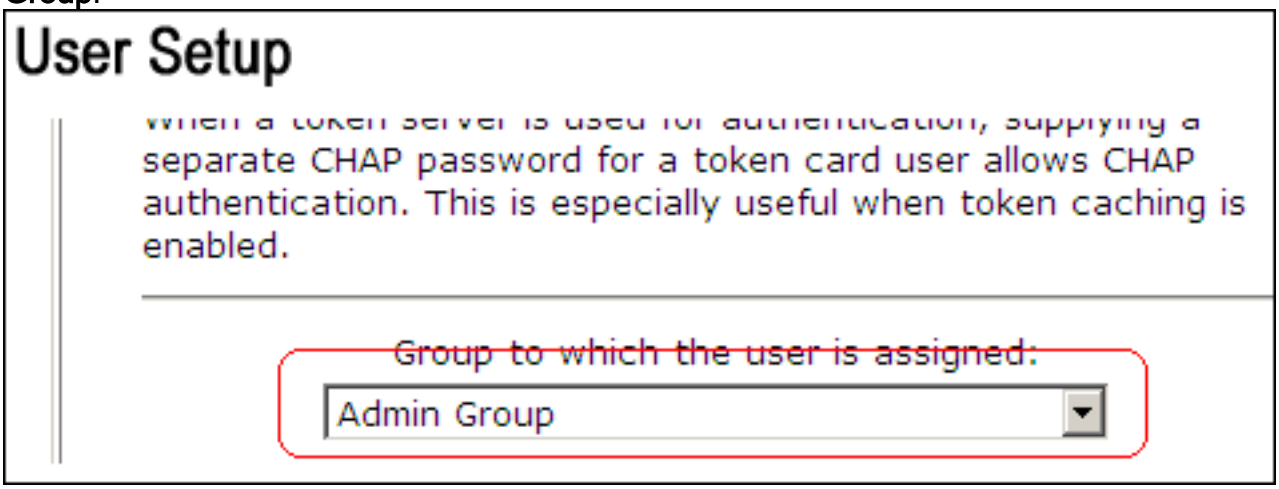
Consulte la sección Configuración de un Conjunto de Autorización de Comandos de Shell para un Usuario de la Guía del Usuario para Cisco Secure Access Control Server 4.1 para obtener más información sobre cómo configurar el conjunto de autorización de comandos de shell para los usuarios.

Nota: La configuración de nivel de usuario invalida la configuración de nivel de grupo en ACS, lo que significa que si el usuario tiene la autorización de comando shell establecida en la configuración de nivel de usuario, invalida la configuración de nivel de grupo.

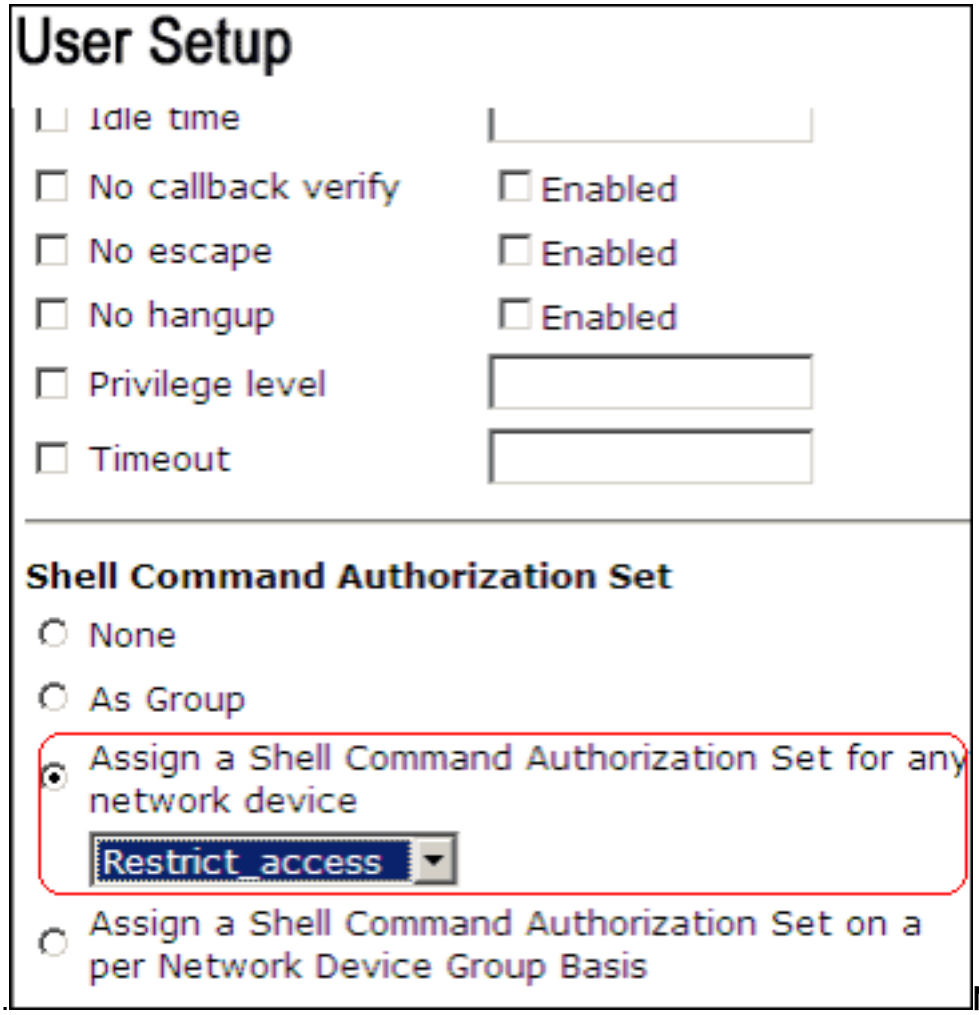
1. Haga clic en **User Setup > Add/Edit** para crear un nuevo usuario llamado *Admin_user* para ser parte del grupo
   Admin.



2. En la lista desplegable del grupo al que está asignado el usuario, seleccione **Admin Group**.



3. En el área Conjunto de autorización de comandos de shell, haga clic en el botón de opción **Asignar un conjunto de autorización de comandos de shell para cualquier dispositivo de red** y elija **Restrict_access** en la lista desplegable.**Nota:** En esta situación, este usuario forma parte del grupo de administradores. El conjunto de autorización de shell *Restrict_access* es aplicable; el conjunto de autorización del shell *ReadWrite Access* no es



aplicable.**Nota:** En la sección TACACS+ (Cisco) del área Configuración de la interfaz, asegúrese de que la opción **Shell (exec)** esté seleccionada en la columna Usuario.

Configuración del router IOS

Además de la configuración preestablecida, estos comandos son necesarios en un router o switch IOS para implementar la autorización de comandos 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 de ASA/PIX/FWSM

Además de la configuración preestablecida, estos comandos son necesarios en ASA/PIX/FWSM para implementar la autorización de comandos 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 a ASDM

para fines de sólo lectura. Dado que los paquetes RADIUS contienen autenticación y autorización al mismo tiempo, todos los usuarios que se autentican en el servidor RADIUS tienen un nivel de privilegio de 15. Puede lograr esto a través de TACACS con la implementación de conjuntos de autorización de comandos.

Nota: ASA/PIX/FWSM tardan mucho tiempo en ejecutar cada comando escrito, incluso si ACS no está disponible para realizar la autorización de comandos. Si ACS no está disponible y ASA tiene configurada la autorización de comandos, ASA seguirá solicitando la autorización de comandos para cada comando.

Troubleshoot

Error: error de autorización de comando

Problema

Después de iniciar sesión en el firewall a través del registro TACACS, los comandos no funcionan. Cuando ingresa un comando, se recibe este error: `error de autorización del comando.`

Solución

Complete estos pasos para resolver este problema:

1. Asegúrese de utilizar el nombre de usuario correcto y de que todos los privilegios necesarios están asignados al usuario.
2. Si el nombre de usuario y los privilegios son correctos, verifique que el ASA tenga conectividad con el ACS y que el ACS esté activo.

Nota: Este error también puede ocurrir si el administrador configuró erróneamente la autorización de comando para usuarios locales, así como TACACS. 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 de Cisco Secure Control Access Control Server
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).