Exemplo de Configuração de Conjuntos de Autorização de Comando Shell ACS no IOS e no ASA/PIX/FWSM

Contents

Introduction

Este documento descreve como configurar os conjuntos de autorização de shell no Cisco Secure Access Control Server (ACS) para clientes AAA, como roteadores ou switches Cisco IOS® e Cisco Security Appliances (ASA/PIX/FWSM) com TACACS+ como o protocolo de autorização.

Observação: o ACS Express não suporta autorização de comando.

Prerequisites

Requirements

Este documento pressupõe que as configurações básicas estejam definidas em clientes AAA e ACS.

No ACS, escolha **Interface Configuration > Advanced Options** e certifique-se de que a caixa de seleção **Per-user TACACS+/RADIUS Attributes** esteja marcada.

Componentes Utilizados

As informações neste documento são baseadas no Cisco Secure Access Control Server (ACS) que executa o software versão 3.3 e posterior.

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.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Conjuntos de autorização de comando

Os conjuntos de autorização de comandos fornecem um mecanismo central para controlar a autorização de cada comando emitido em qualquer dispositivo de rede. Esse recurso melhora muito a escalabilidade e a capacidade de gerenciamento necessárias para definir restrições de autorização.

No ACS, os conjuntos de autorização de comando padrão incluem Conjuntos de autorização de comando Shell e Conjuntos de autorização de comando PIX. Os aplicativos de gerenciamento de dispositivos da Cisco, como o CiscoWorks Management Center para Firewalls, podem instruir o ACS a suportar tipos adicionais de conjuntos de autorização de comandos.

Observação: os Conjuntos de Autorização de Comando PIX exigem que a solicitação de autorização de comando TACACS+ identifique o serviço como *pixshell*. Verifique se este serviço foi implementado na versão do PIX OS que seus firewalls usam; caso contrário, use Conjuntos de Autorização de Comando Shell para executar a autorização de comando para dispositivos PIX. Consulte Configuração de um Conjunto de Autorização de Comando Shell para um Grupo de Usuários para obter mais informações.

Observação: a partir do PIX OS versão 6.3, o serviço pixshell não foi implementado.

Observação: os Cisco Security Appliances (ASA/PIX) não permitem atualmente que o usuário seja colocado diretamente no modo de ativação durante o login. O usuário deve entrar manualmente no modo de ativação.

Para oferecer mais controle de sessões Telnet administrativas hospedadas em dispositivos, um dispositivo de rede que usa TACACS+ pode solicitar autorização para cada linha de comando antes de ser executado. Você pode definir um conjunto de comandos que são permitidos ou negados para execução por um usuário específico em um determinado dispositivo. O ACS aprimorou ainda mais esse recurso com estes recursos:

- **Conjuntos de autorizações de comandos nomeados reutilizáveis** — Sem citar diretamente qualquer usuário ou grupo de usuários, você pode criar um conjunto nomeado de autorizações de comandos. Você pode definir vários conjuntos de autorização de comandos que delineiam diferentes perfis de acesso. Por exemplo:Um conjunto de autorização de comandos do *Help desk* pode permitir acesso a comandos de navegação de alto nível, como **show run**, e negar qualquer comando de configuração.Um conjunto de autorizações de comandos *Todos os engenheiros de rede* pode conter uma lista limitada de comandos permitidos para qualquer engenheiro de rede na empresa.Um conjunto de autorização de comandos dos *engenheiros de rede locais* pode permitir todos os comandos (e incluir comandos de configuração de endereço IP).
- **Granularidade da configuração fina** — Você pode criar associações entre conjuntos de autorização de comandos nomeados e grupos de dispositivos de rede (NDGs). Assim, você pode definir diferentes perfis de acesso para usuários, dependendo de quais dispositivos de rede eles acessam. Você pode associar o mesmo conjunto de autorizações de comandos com nome a mais de um NDG e usá-lo para mais de um grupo de usuários. O ACS reforça a integridade dos dados. Os conjuntos de autorização de comandos nomeados são mantidos no banco de dados interno do ACS. Você pode usar os recursos de backup e restauração do ACS para fazer backup e restaurá-los. Você também pode replicar conjuntos de autorização de comandos para ACSs secundários juntamente com outros dados de configuração.

Para tipos de conjunto de autorização de comando que suportam aplicativos de gerenciamento de dispositivo Cisco, os benefícios são semelhantes quando você usa conjuntos de autorização de comando. Você pode aplicar conjuntos de autorização de comandos a grupos ACS que contenham usuários do aplicativo de gerenciamento de dispositivos para aplicar a autorização de vários privilégios em um aplicativo de gerenciamento de dispositivos. Os grupos ACS podem corresponder a diferentes funções no aplicativo de gerenciamento de dispositivos e você pode aplicar diferentes conjuntos de autorização de comandos a cada grupo, conforme aplicável.

O ACS tem três estágios sequenciais de filtragem de autorização de comando. Cada solicitação de autorização de comando é avaliada na ordem listada:

1. **Correspondência de comando** — O ACS determina se o comando processado corresponde a um comando listado no conjunto de autorização de comando. Se o comando não corresponder, a autorização do comando será determinada pela configuração Comandos sem correspondência: *permit or deny.* Caso contrário, se o comando for correspondido, a avaliação continuará.
2. **Correspondência de Argumento** — O ACS determina se os argumentos de comando apresentados correspondem aos argumentos de comando listados no conjunto de autorização de comando.Se algum argumento não corresponder, a autorização do comando é determinada pela ativação da opção Permitir Args Sem Correspondência. Se argumentos não correspondentes forem permitidos, o comando é autorizado e a avaliação termina; caso contrário, o comando não é autorizado e a avaliação termina.Se todos os argumentos corresponderem, a avaliação continuará.
3. **Política de Argumento** — Quando o ACS determina que os argumentos no comando correspondem aos argumentos no conjunto de autorização de comando, o ACS determina se cada argumento de comando é permitido explicitamente. Se todos os argumentos forem explicitamente permitidos, o ACS concederá autorização de comando. Se nenhum argumento for permitido, o ACS negará a autorização do comando.

Adicionar um conjunto de autorizações de comandos do shell

Esta seção inclui estes cenários que descrevem como adicionar um conjunto de autorização de comando:

- Cenário 1: Privilégio para acesso de leitura-gravação ou acesso total
- Cenário 2: Privilégio para acesso somente leitura
- Cenário 3: Privilégio para acesso restrito

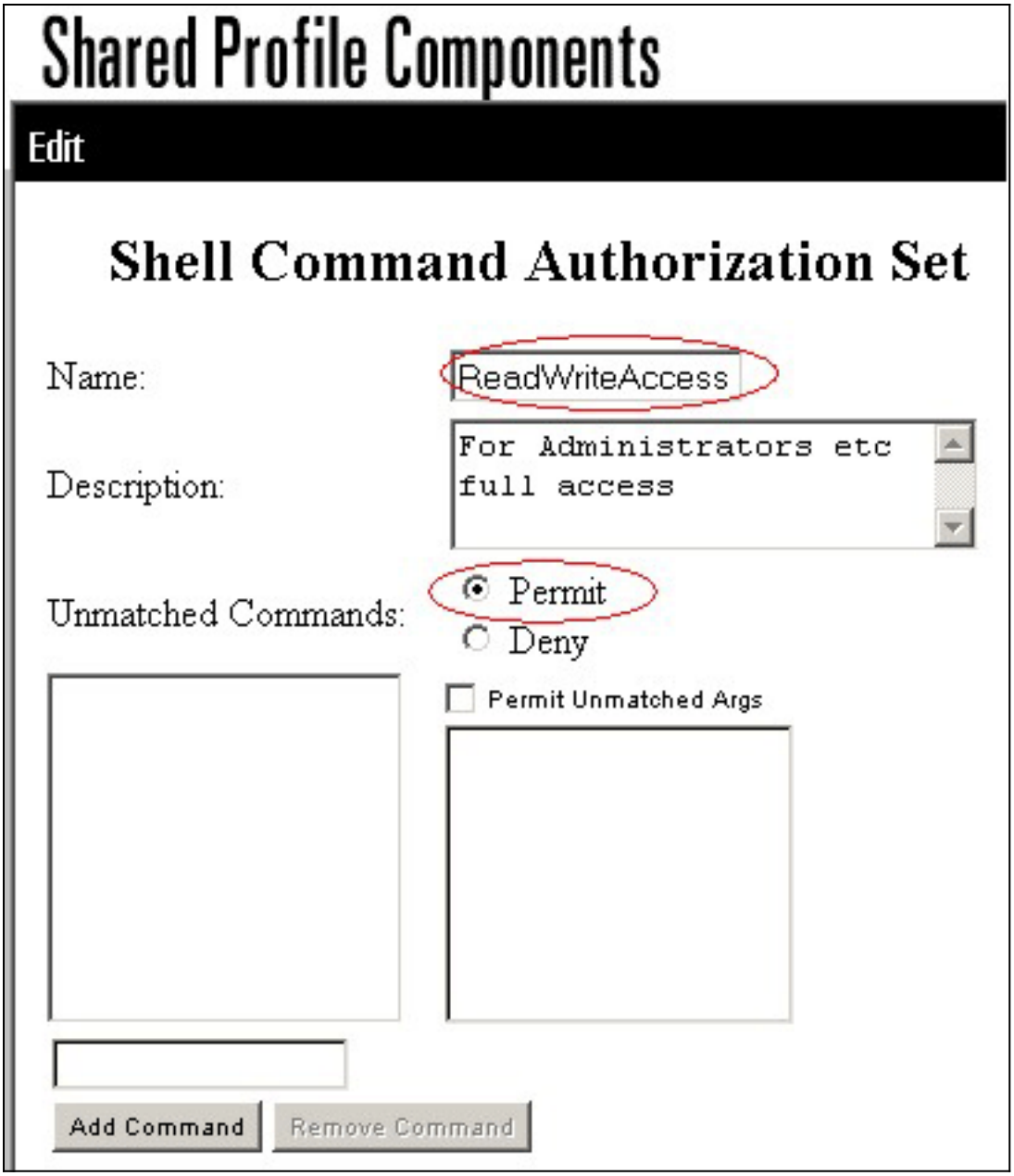
Observação: consulte a seção Adicionando um conjunto de autorização de comando do Guia do usuário do Cisco Secure Access Control Server 4.1 **para obter mais informações sobre como criar conjuntos de autorização de comando.** Consulte Edição de um conjunto de autorização de comando e Exclusão de um conjunto de autorização de comando para obter mais informações sobre como editar e excluir conjuntos de autorização de comando.

Cenário 1: Privilégio para acesso de leitura-gravação ou acesso total

Neste cenário, os usuários recebem acesso de leitura-gravação (ou total).

Na área Conjunto de autorizações de comandos do shell da janela Componentes de perfil compartilhado, defina estas configurações:

1. No campo Nome, insira **ReadWriteAccess** como o nome do conjunto de autorização do comando.
2. No campo Descrição, insira uma descrição para o conjunto de autorizações de comando.
3. Clique no botão de opção **Permit** e em **Submit**.

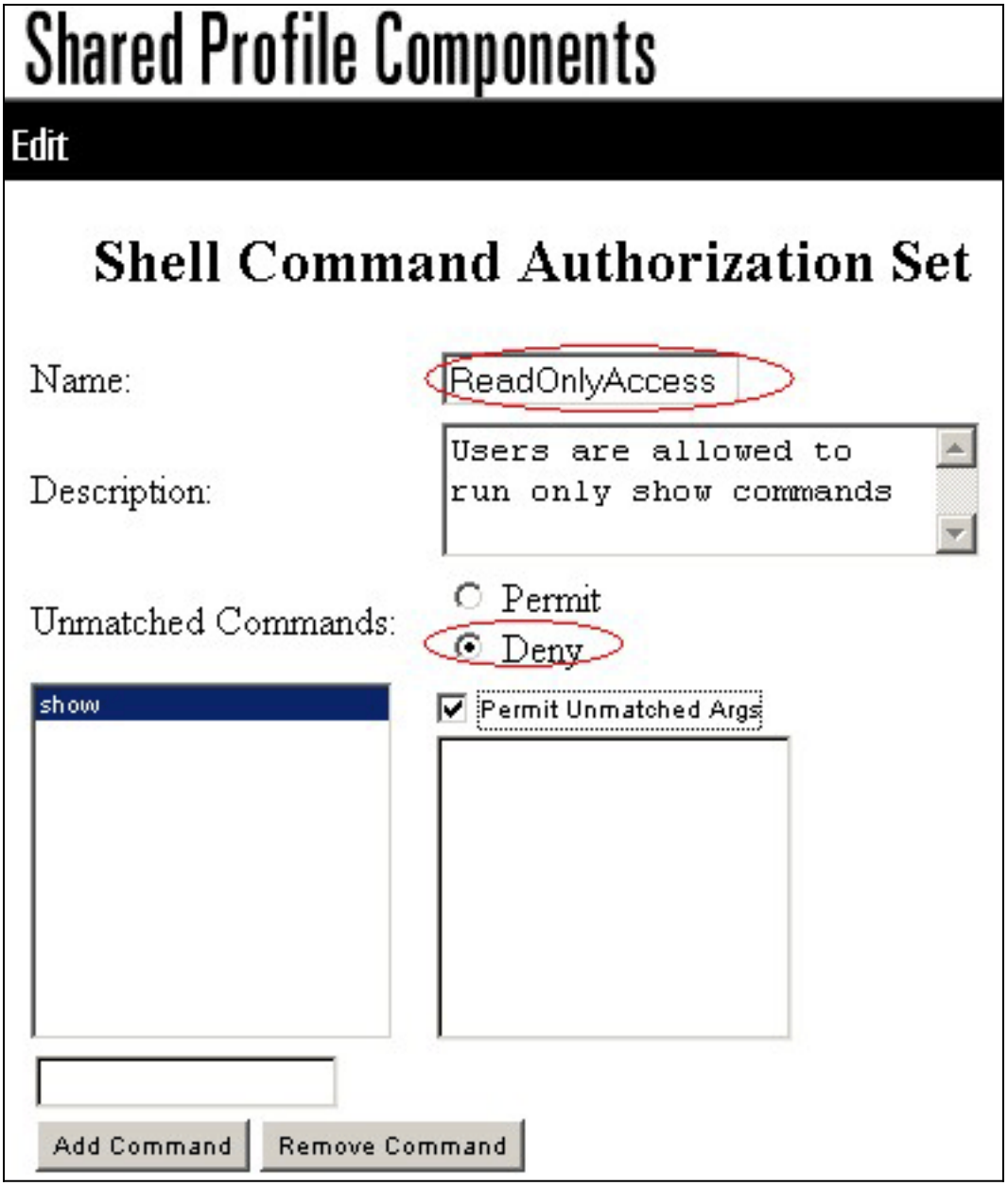


Cenário 2: Privilégio para acesso somente leitura

Neste cenário, os usuários podem usar apenas os comandos **show**.

Na área Conjunto de autorizações de comandos do shell da janela Componentes de perfil compartilhado, defina estas configurações:

1. No campo Nome, insira **ReadOnlyAccess** como o nome do conjunto de autorizações de comando.
2. No campo Descrição, insira uma descrição para o conjunto de autorizações de comando.
3. Clique no botão de opção **Deny**.
4. Insira o comando **show** no campo acima do botão Adicionar comando e clique em **Adicionar comando**.
5. Marque a caixa de seleção **Permitir argumentos sem correspondência** e clique em **Enviar**

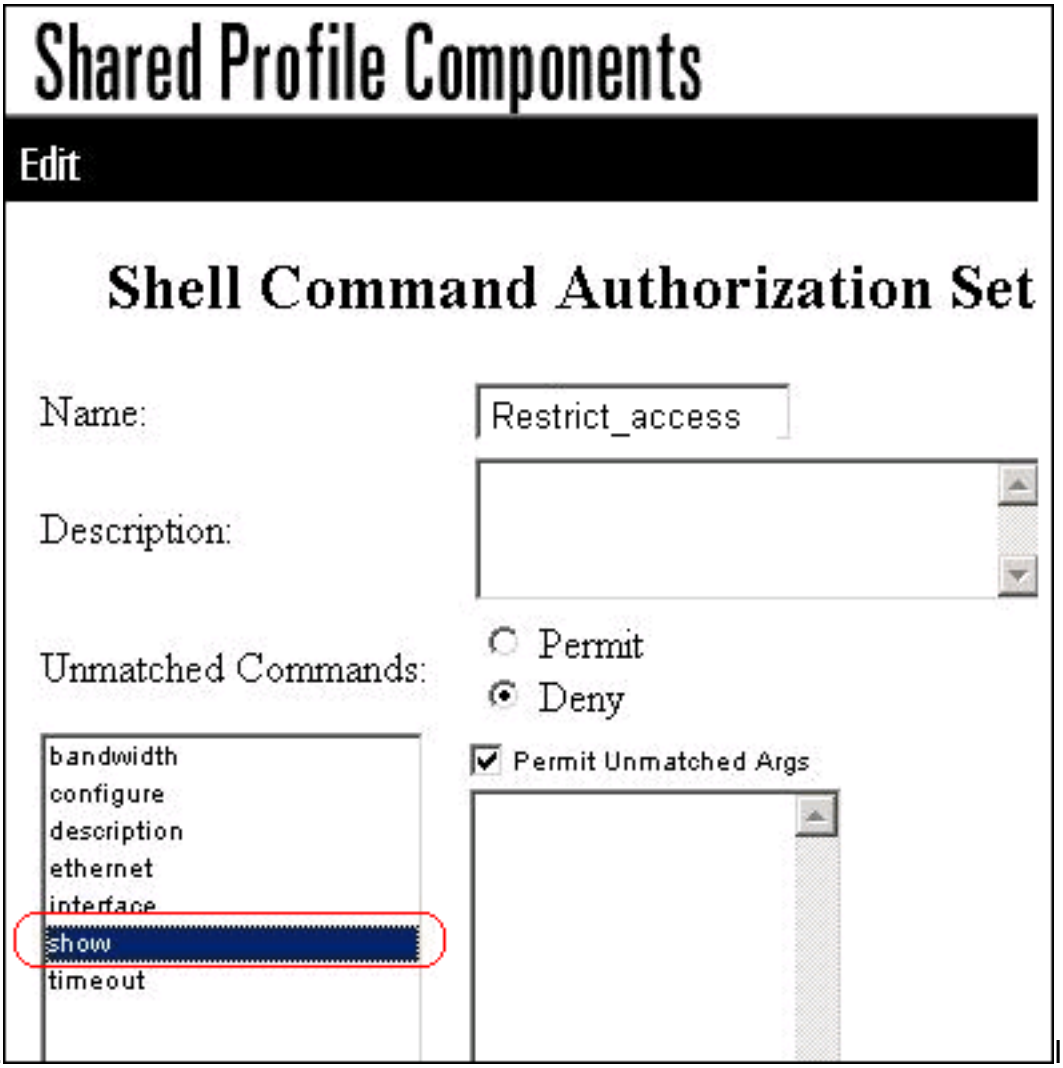


Cenário 3: Privilégio para acesso restrito

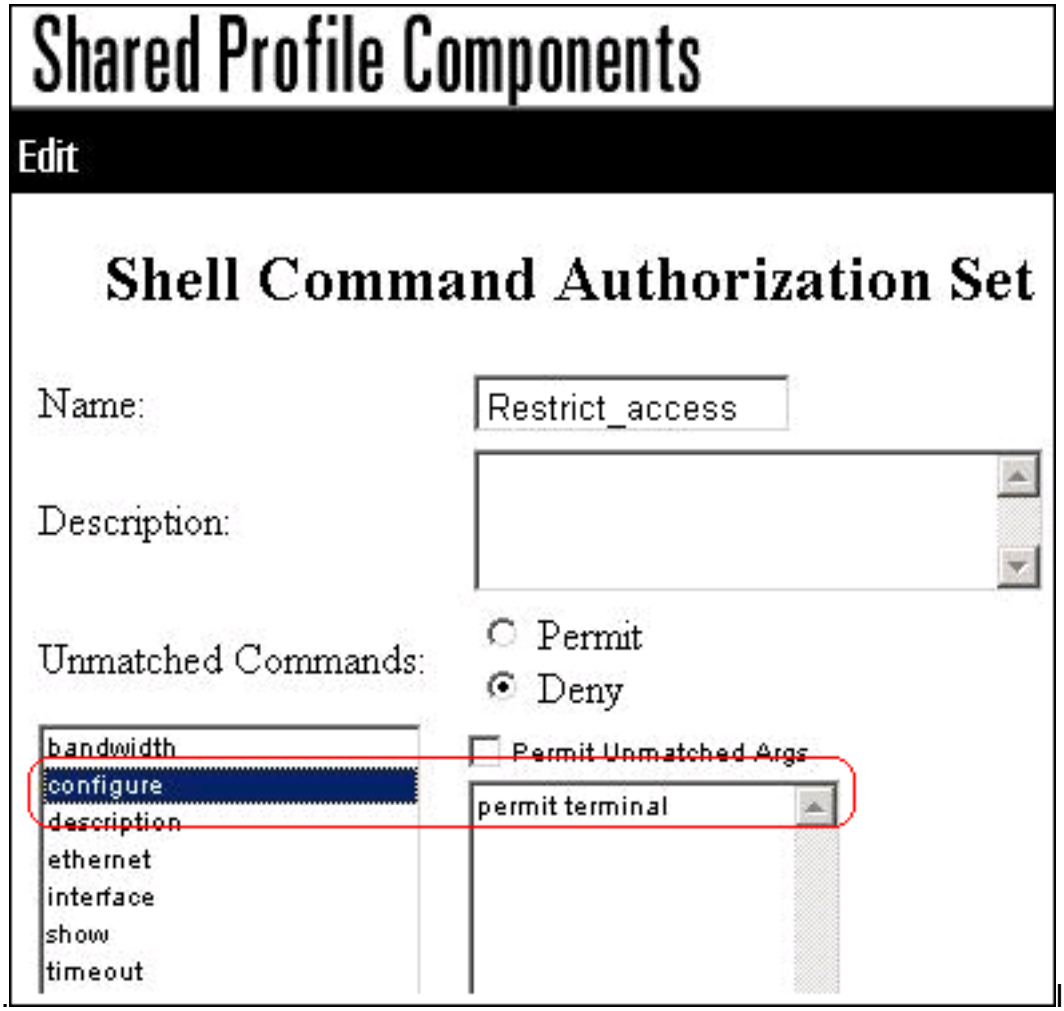
Neste cenário, os usuários podem usar comandos seletivos.

Na área Conjunto de autorizações de comandos do shell da janela Componentes de perfil compartilhado, defina estas configurações:

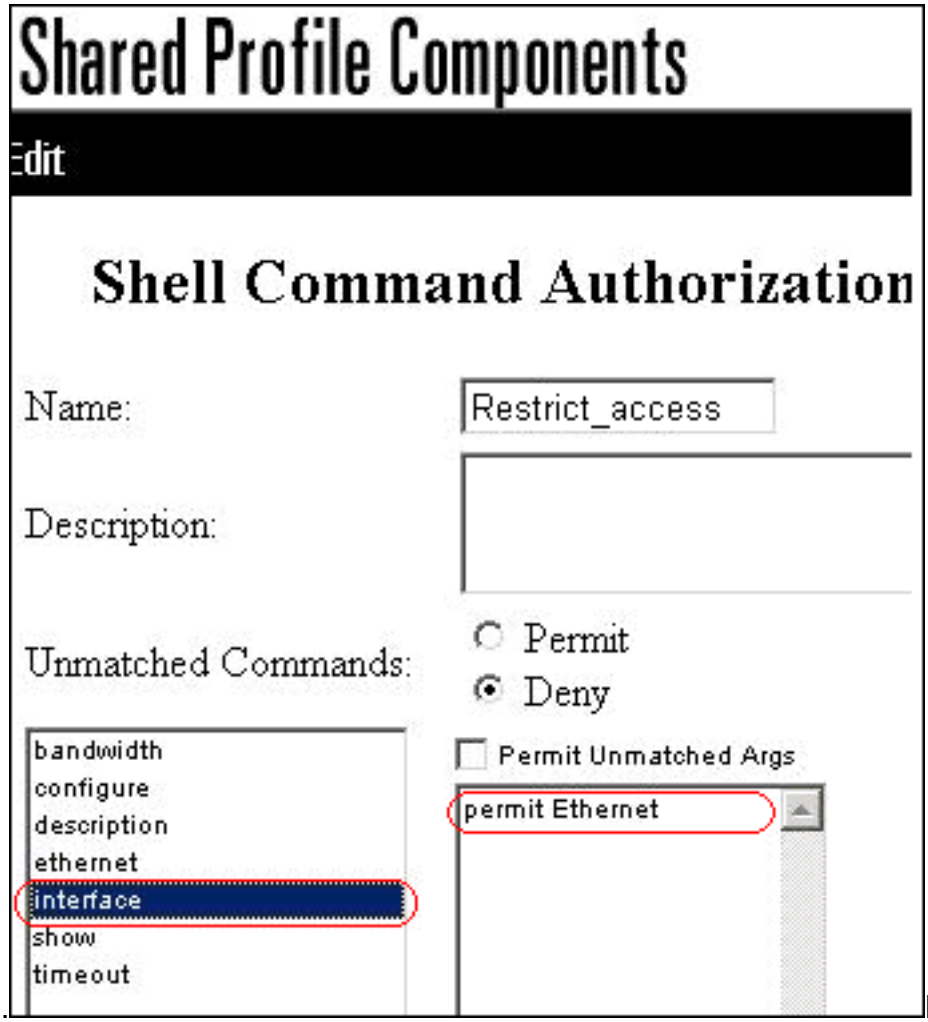
1. No campo de nome, insira **Restrict_access** como o nome do conjunto de autorização de comando.
2. Clique no botão de opção **Deny**.
3. Digite os comandos que deseja permitir nos clientes AAA.No campo localizado acima do botão Adicionar comando, insira o comando **show** e clique em **Adicionar**



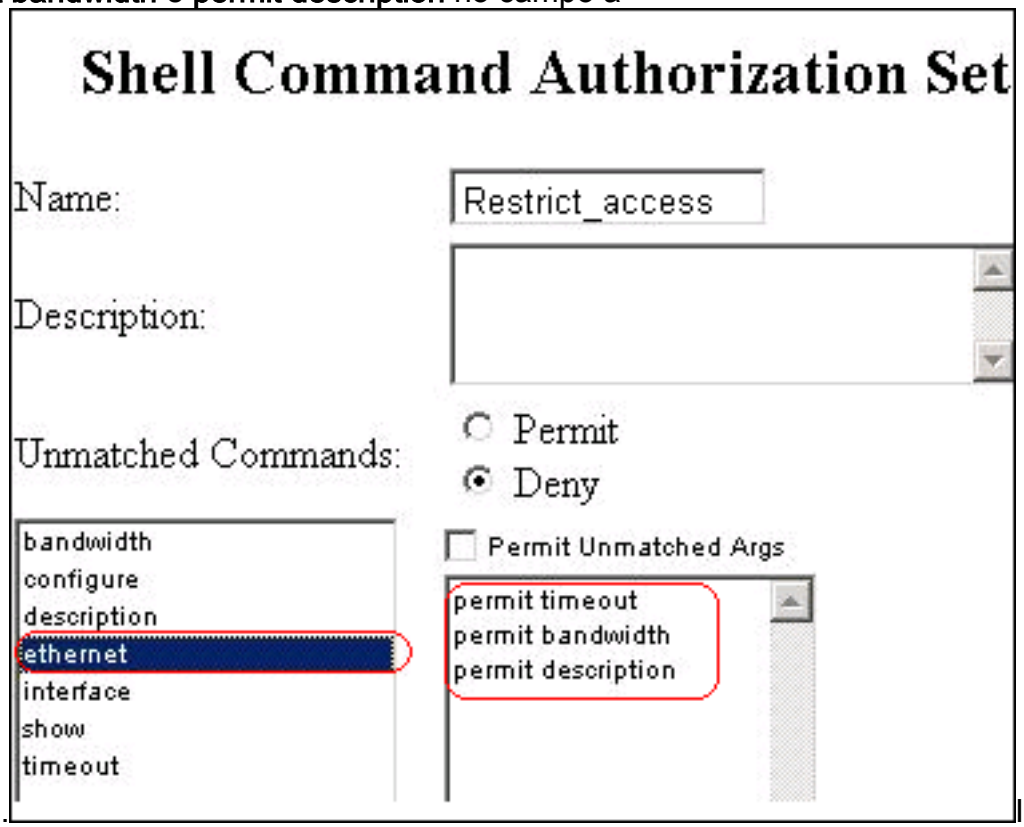
comando.Insira o comando **configure** e clique em **Add Command**.Selecione o comando **configure** e insira **permit terminal** no campo à



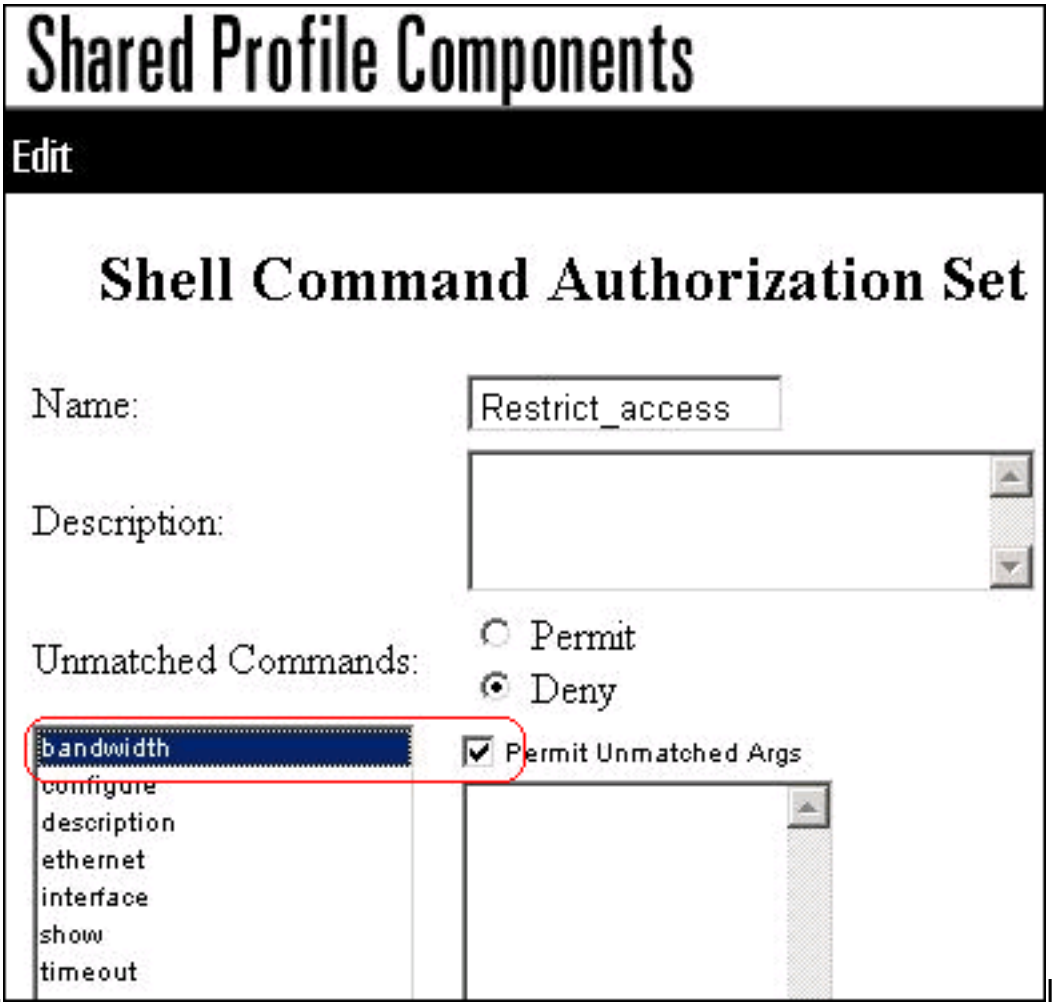
direita.Insira o comando **interface** e clique em **Add Command**.Selecione o comando **interface** e insira **permit Ethernet** no campo à



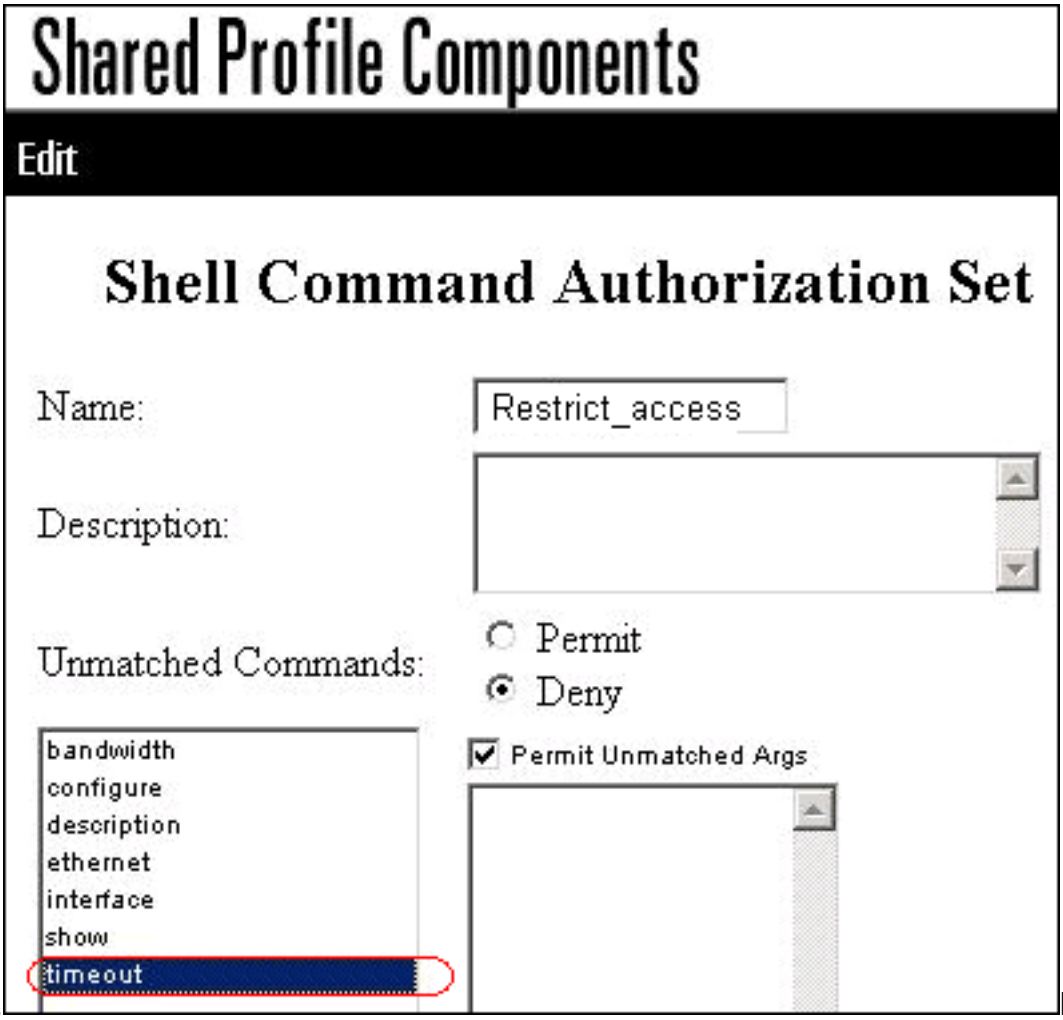
direita.Insira o comando **ethernet** e clique em **Add Command**.Selecione o comando **interface** e insira **permit timeout**, **permit bandwidth** e **permit description** no campo à



direita.Insira o comando **bandwidth** e clique em **Add**

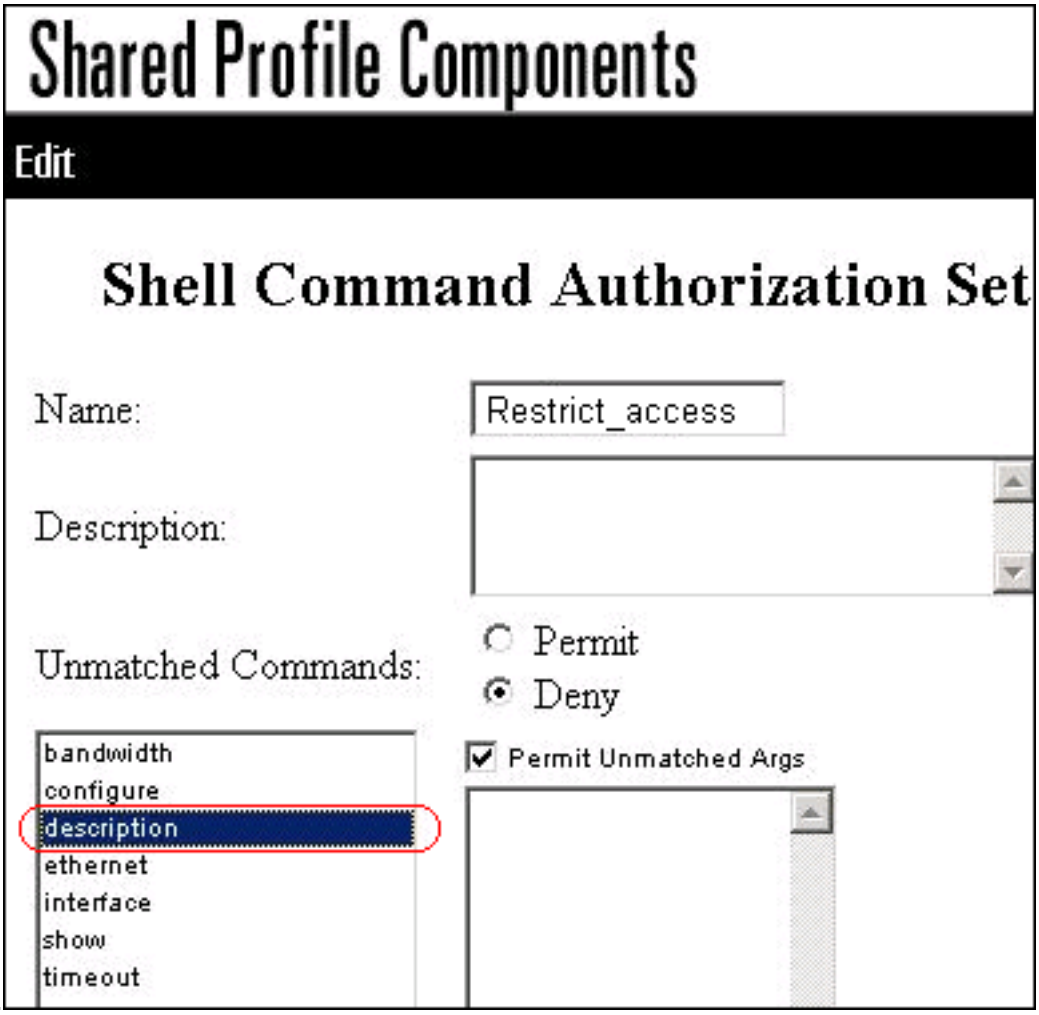


Command. Insira o comando **timeout** e clique em **Add**



Command. Insira o comando **description** e clique em **Add**

Command.



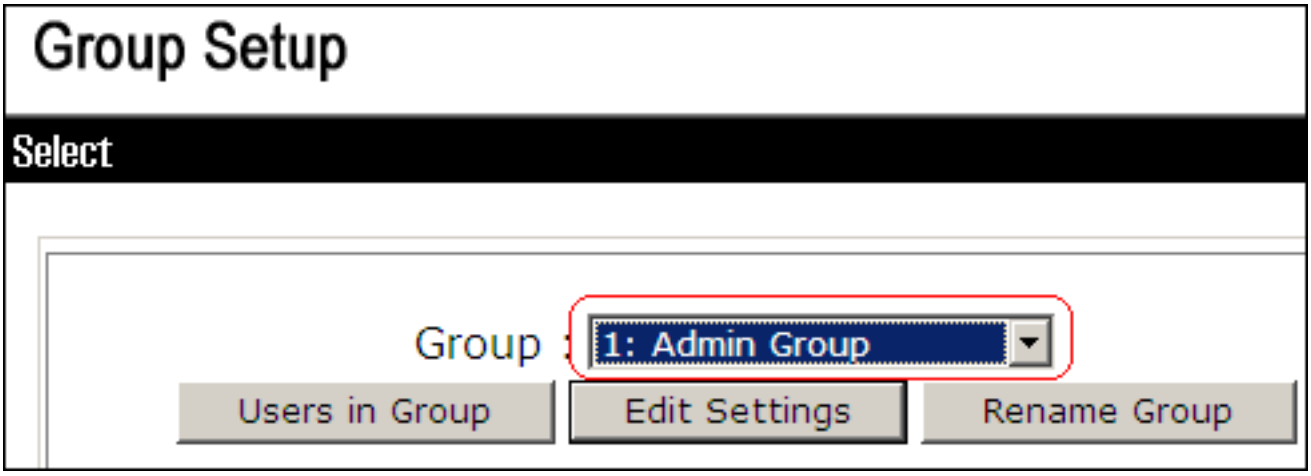
4. Clique em Submit.

Associar o conjunto de autorização do comando Shell ao grupo de usuários

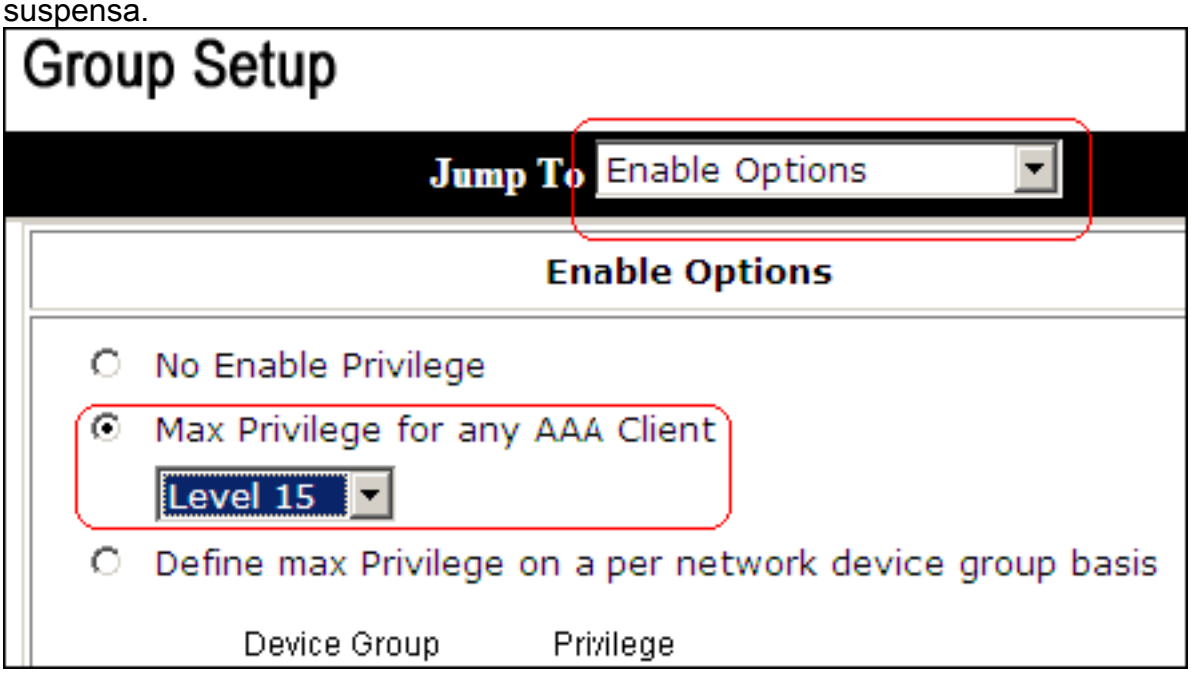
Consulte a seção Configuração de um Conjunto de Autorização de Comando Shell para um Grupo de Usuários do Guia do Usuário do Cisco Secure Access Control Server 4.1 para obter mais informações sobre como configurar o conjunto de autorização de comando shell para grupos de usuários.

Associar o conjunto de autorização de comandos do shell (acesso de leitura e gravação) ao grupo de usuários (grupo de administradores)

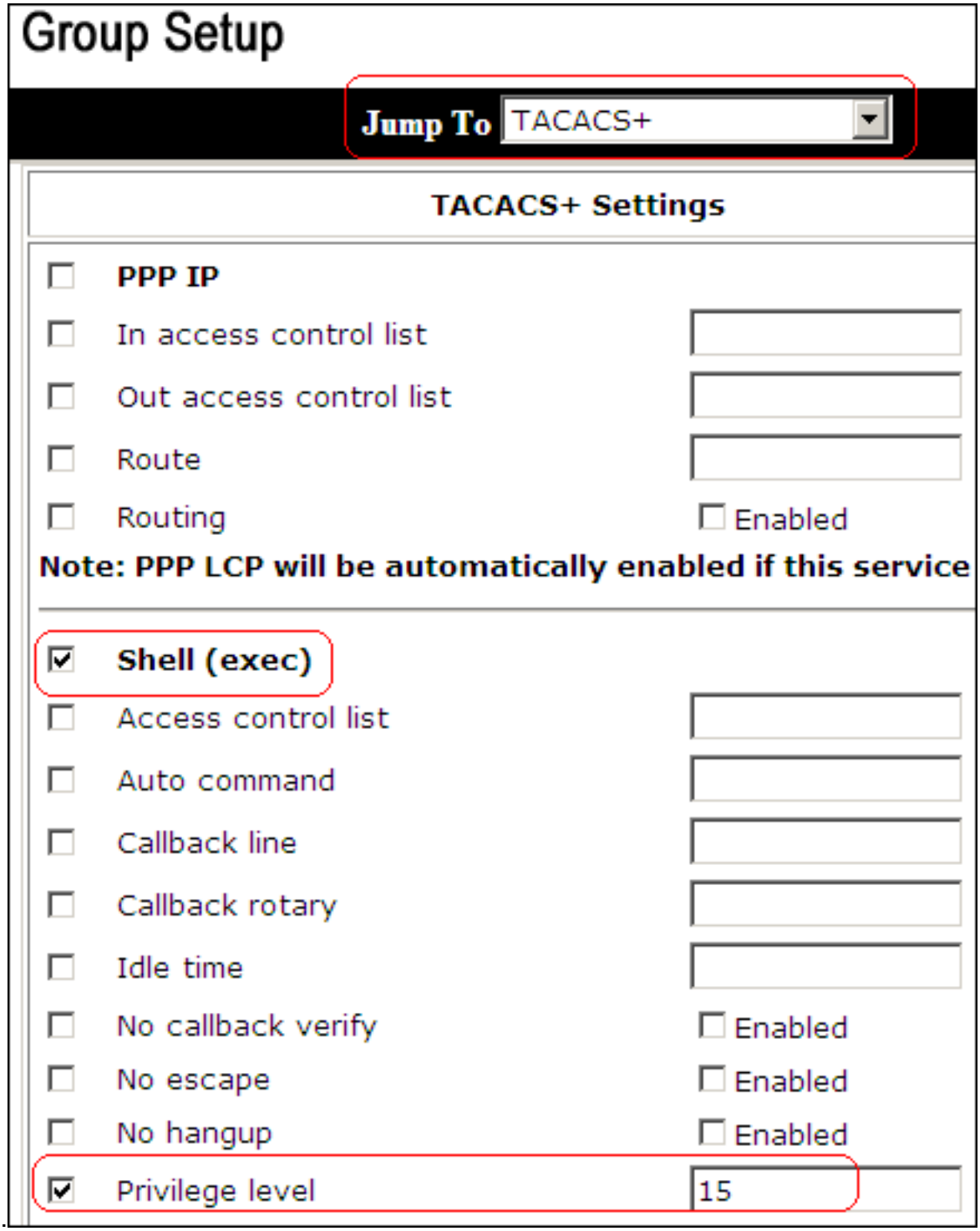
1. Na janela ACS, clique em **Group Setup** e escolha **Admin Group** na lista suspensa Group.



2. Clique em **Edit Settings**.
3. Na lista suspensa Ir para, escolha **Ativar opções**.
4. Na área Enable Options, clique no botão de opção **Max Privilege for any AAA client** e escolha **Level 15** na lista suspensa.

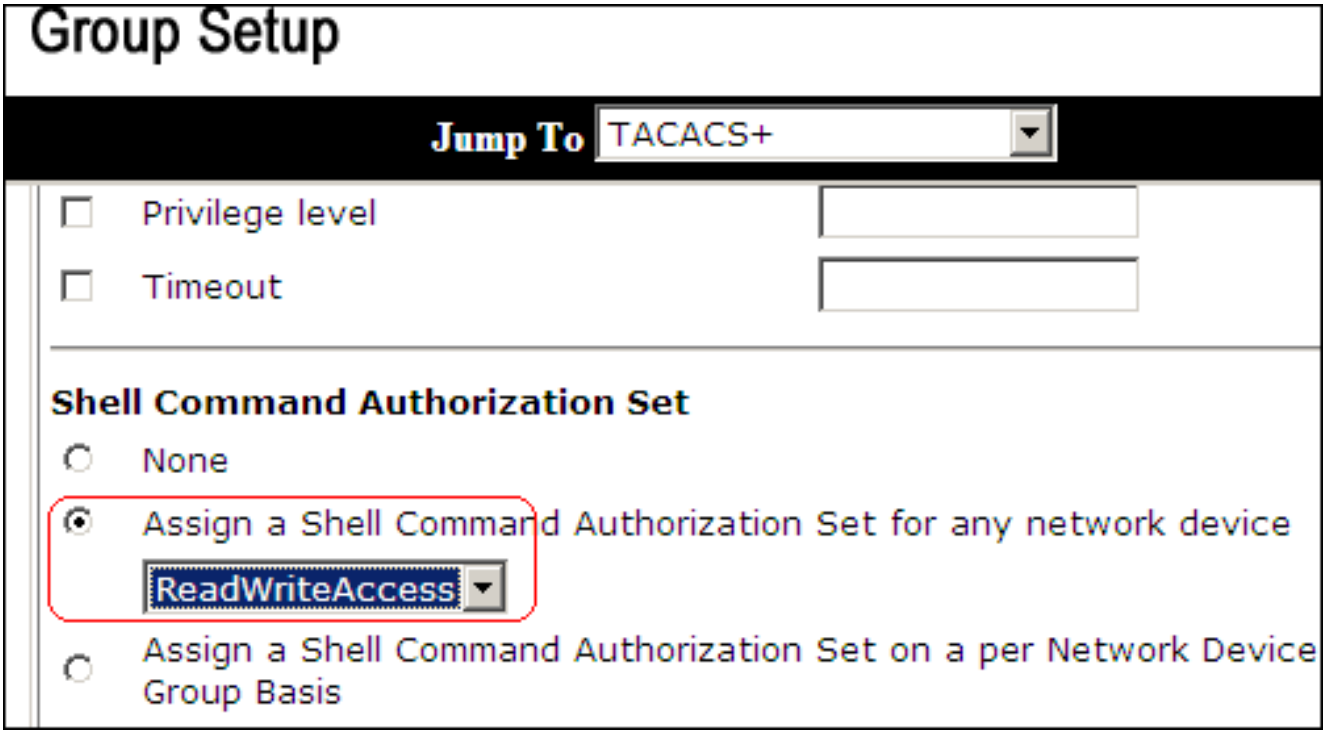


5. Na lista suspensa Ir para, escolha **TACACS+**.
6. Na área TACACS+ Settings, marque a caixa de seleção **Shell (exec)**, marque a caixa de seleção **Privilege level** e insira **15** no campo Privilege



level.

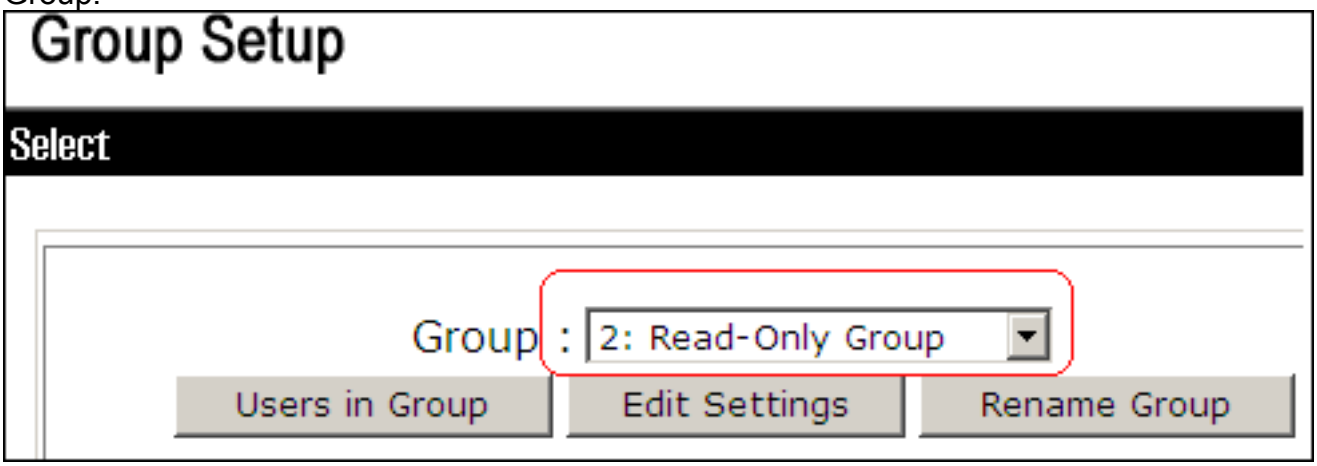
7. Na área Shell Command Authorization Set, clique no botão de opção **Assign a Shell Command Authorization Set for any network device** e escolha **ReadWriteAccess** na lista suspensa.



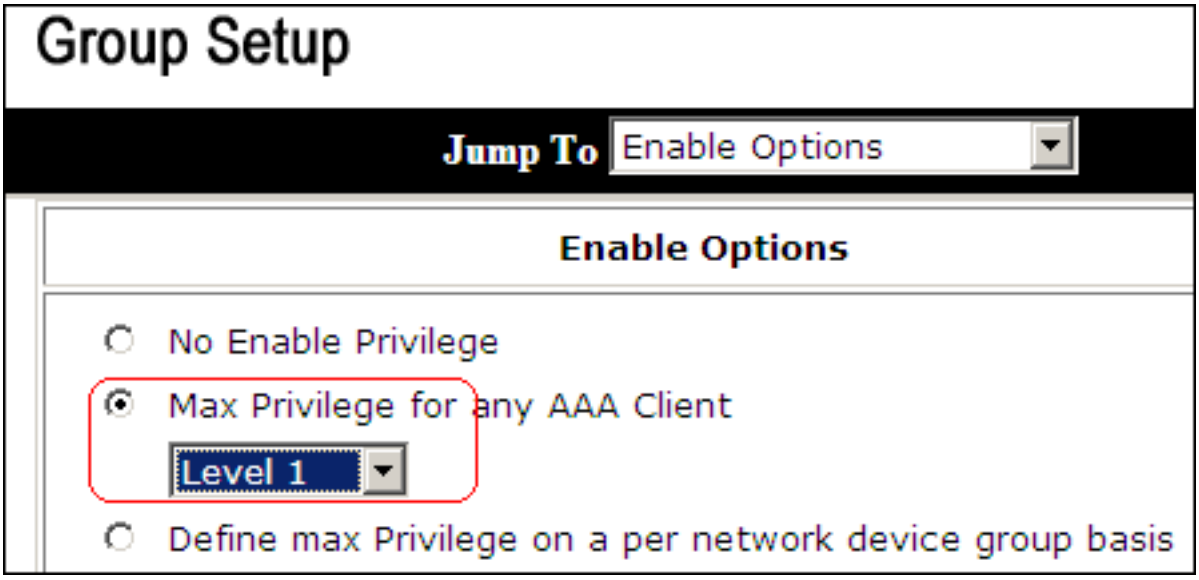
8. Clique em Submit

Associar o conjunto de autorização de comandos do shell (acesso somente leitura) ao grupo de usuários (grupo somente leitura)

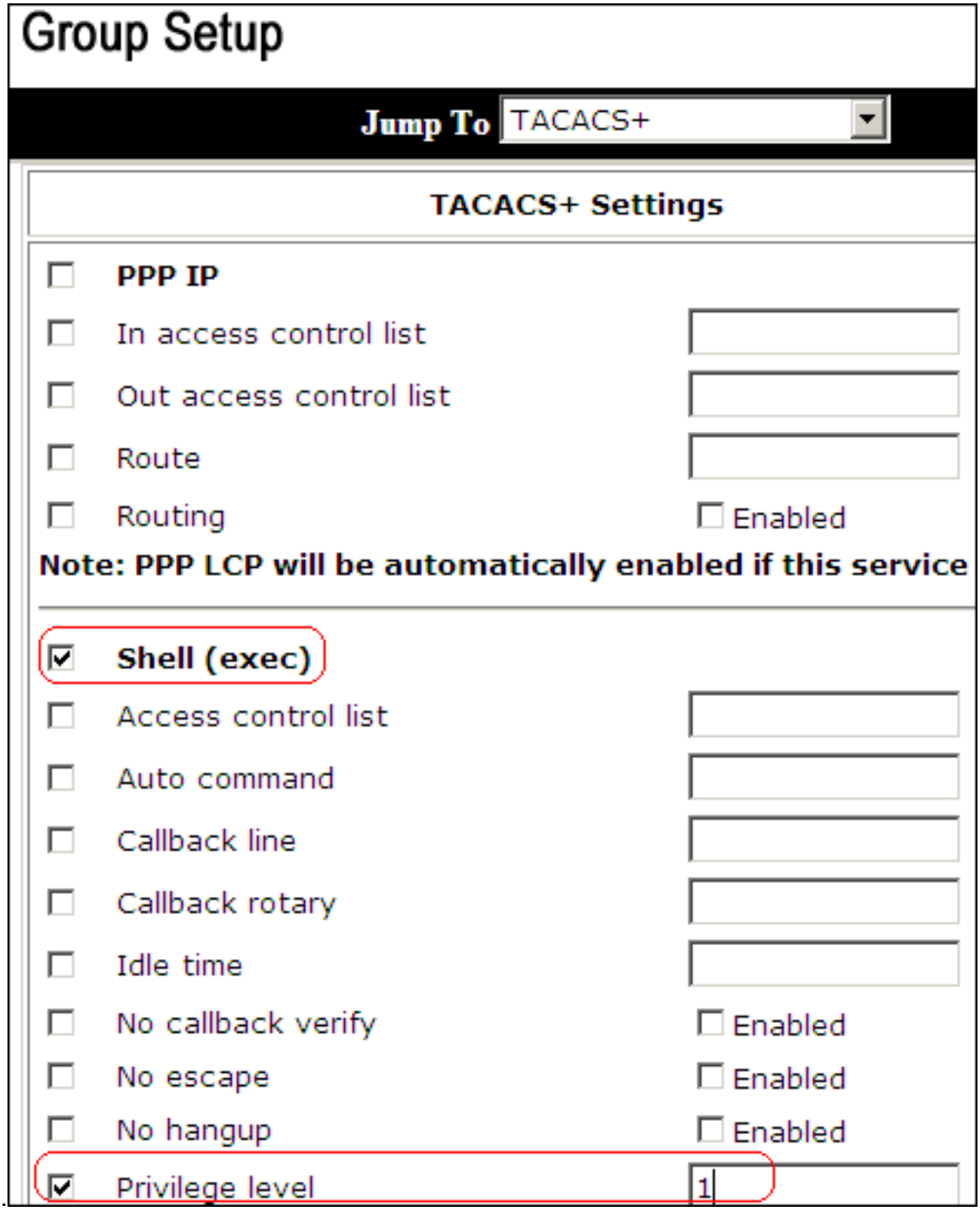
1. Na janela ACS, clique em **Group Setup** e escolha **Read-Only Group** na lista suspensa Group.



2. Clique em **Edit Settings**.
3. Na lista suspensa Ir para, escolha **Ativar opções**.
4. Na área Enable Options, clique no botão de opção **Max Privilege para qualquer cliente AAA** e escolha **Level 1** na lista suspensa.



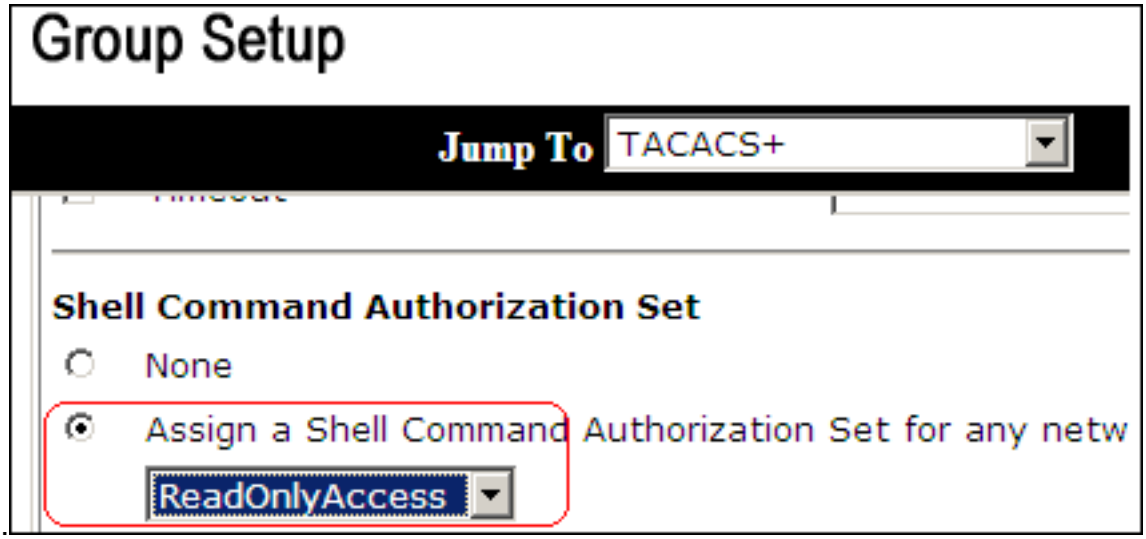
5. Na área TACACS+ Settings, marque a caixa de seleção **Shell (exec)**, marque a caixa de seleção **Privilege level** e insira **1** no campo Privilege



level.

6. Na área Shell Command Authorization Set, clique no botão de opção **Assign a Shell Command Authorization Set for any network device** e escolha **ReadOnlyAccess** na lista

suspensa.



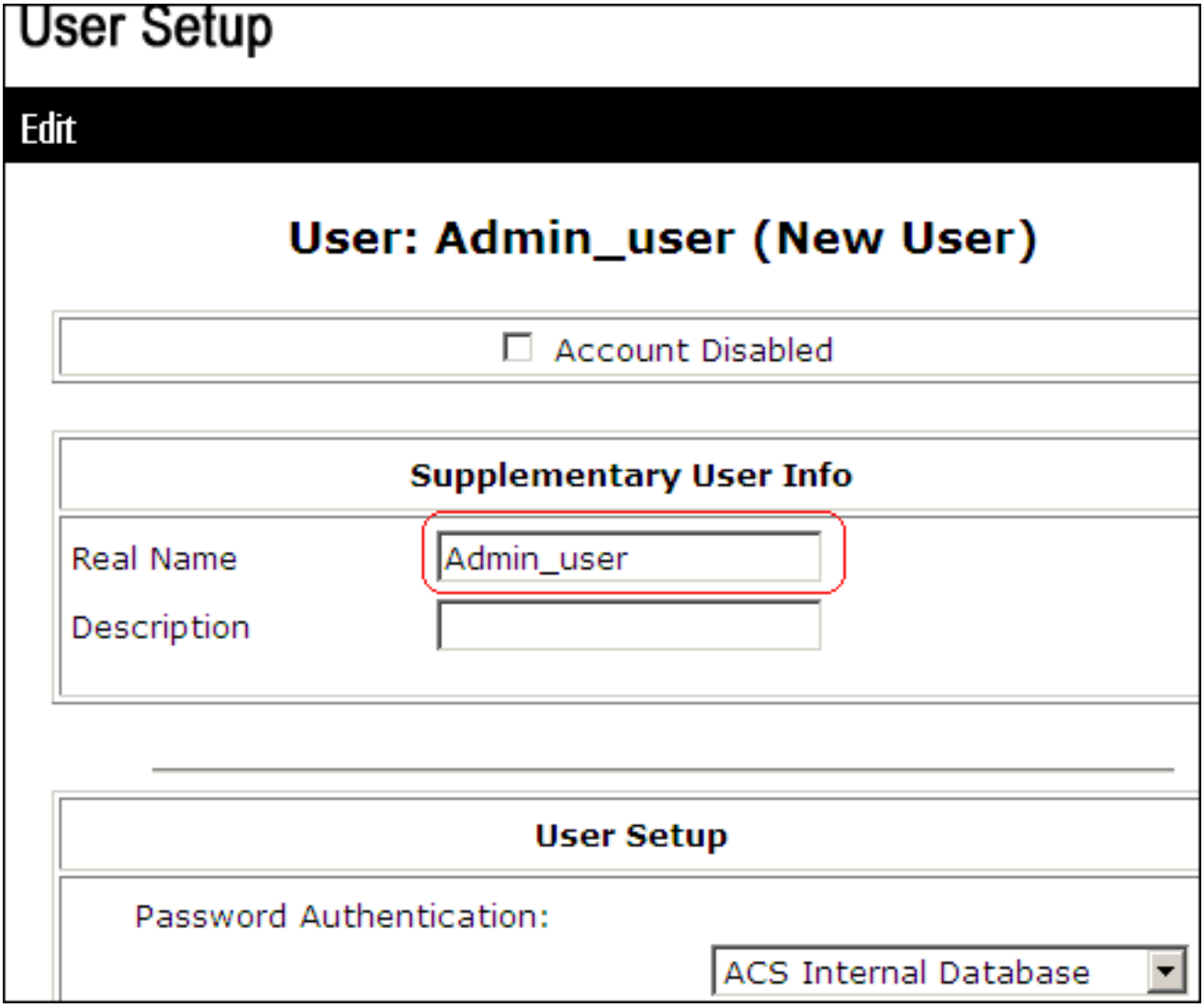
7. Clique em Submit

Associar o conjunto de autorização de comandos do shell (Restrict_access) ao usuário

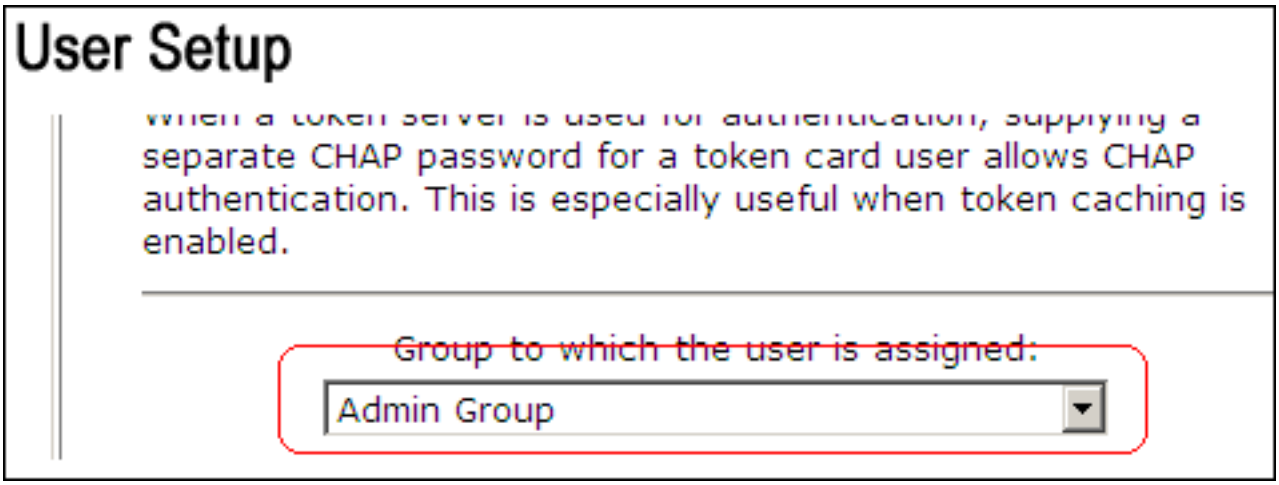
Consulte a seção Configuração de um Conjunto de Autorização de Comando Shell para um Usuário do Guia do Usuário do Cisco Secure Access Control Server 4.1 para obter mais informações sobre como configurar a configuração do conjunto de autorização de comando shell para usuários.

Observação: as configurações de nível de usuário substituem as configurações de nível de grupo no ACS, o que significa que se o usuário tiver uma autorização de comando de shell definida nas configurações de nível de usuário, ele substituirá as configurações de nível de grupo.

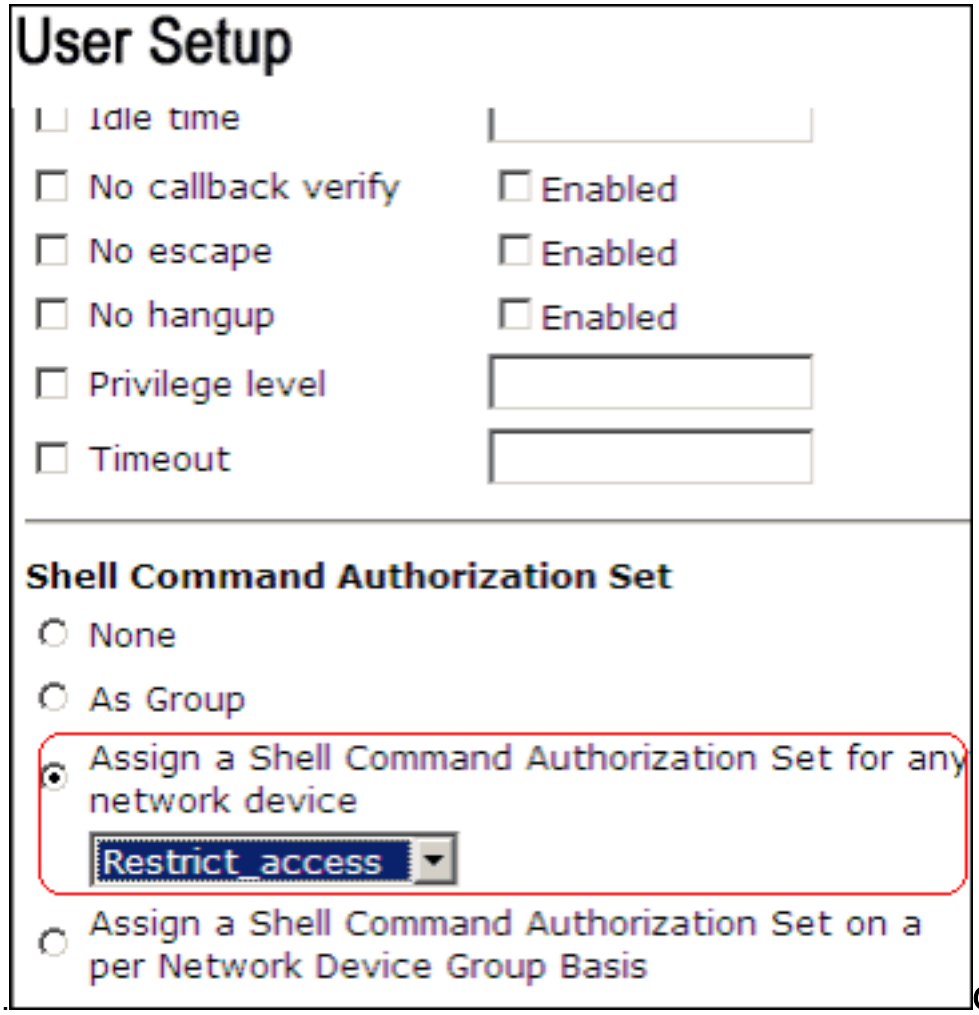
1. Clique em **User Setup > Add/Edit** para criar um novo usuário chamado *Admin_user* para fazer parte do grupo
   Admin.



2. Na lista suspensa do grupo ao qual o usuário está atribuído, escolha **Grupo Admin**.



3. Na área Shell Command Authorization Set, clique no botão de opção **Assign a Shell Command Authorization Set for any network device** e escolha **Restrict_access** na lista suspensa.**Observação:** neste cenário, este usuário faz parte do Grupo de administradores. O conjunto de autorização do shell *Restrict_access* é aplicável; o conjunto de autorizações do shell *ReadWrite Access* não é



aplicável. **Observação:** na seção TACACS+ (Cisco) da área Interface Configuration, certifique-se de que a opção **Shell (exec)** esteja selecionada na coluna User.

Configuração do IOS Router

Além da configuração predefinida, esses comandos são necessários em um roteador ou switch IOS para implementar a autorização de comandos através de um 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
```

Configuração de ASA/PIX/FWSM

Além da configuração predefinida, esses comandos são necessários no ASA/PIX/FWSM para implementar a autorização de comandos através de um servidor ACS:

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

Observação: Não é possível usar o protocolo RADIUS para restringir o acesso do usuário ao

ASDM para fins somente leitura. Como os pacotes RADIUS contêm autenticação e autorização ao mesmo tempo, todos os usuários autenticados no servidor RADIUS têm um nível de privilégio de 15. Você pode fazer isso por meio do TACACS com a implementação dos conjuntos de autorização de comandos.

Observação: o ASA/PIX/FWSM demora muito para executar cada comando digitado, mesmo que o ACS não esteja disponível para executar a autorização do comando. Se o ACS não estiver disponível e o ASA tiver a autorização de comando configurada, o ASA ainda solicitará a autorização de comando para cada comando.

Troubleshoot

Erro: falha na autorização do comando

Problema

Depois de fazer login no firewall através do registro TACACS, os comandos não funcionam. Quando você insere um comando, este erro é recebido: `falha na autorização do comando`.

Solução

Siga estes passos para resolver esse problema:

1. Verifique se o nome de usuário correto está sendo usado e se todos os privilégios necessários estão atribuídos ao usuário.
2. Se o nome de usuário e os privilégios estiverem corretos, verifique se o ASA tem conectividade com o ACS e se o ACS está ativo.

Observação: esse erro também pode ocorrer se o administrador configurou por engano a autorização de comandos para usuários locais, bem como TACACS. Nesse caso, execute uma recuperação de senha para resolver o problema.

Informações Relacionadas

- Cisco PIX Firewall Software
- Referências do comando Cisco Secure PIX Firewall
- Avisos de campo de produto de segurança (incluindo PIX)
- Solicitações de Comentários (RFCs)
- Página de Suporte do Cisco Secure Control Access Control Server
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.