Пример конфигурации "Авторизации команд Shell на IOS и ASA/PIX/FWSM"

Содержание

Введение

Этот документ описывает, как настроить наборы авторизации оболочки в сервере Cisco Secure Access Control Server (ACS) для клиентов AAA, таких как маршрутизаторы Cisco IOS® или коммутаторы и Устройства Cisco Security (ASA/PIX/FWSM) с TACACS + как протокол авторизации.

Примечание: ACS Express не поддерживает авторизацию для выполнения команд.

Предварительные условия

Требования

Этот документ предполагает, что в клиентах AAA и в ACS заданы базовые конфигурации.

В ACS выберите **Interface Configuration> Advanced Options** и гарантируйте, что проверен **TACACS Для каждого пользователя +/RADIUS** флажок **Attributes**.

Используемые компоненты

Информация в этом документе касается сервера Cisco ACS под управлением ПО версии 3.3 или более поздней версии.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Наборы авторизации для выполнения команд

Наборы авторизации для выполнения команд обеспечивают централизованное управление авторизацией каждой команды, выполняемой на любом отдельно взятом сетевом устройстве. Эта функция значительно улучшает масштабируемость и управляемость, необходимые для при установлении ограничений авторизации.

В сервере ACS наборы авторизации для выполнения команд по умолчанию включают в себя наборы авторизации команд интерпретатора и …наборы авторизации команд PIX. Приложения управления устройствами Cisco, такие как центр управления CiscoWorks для межсетевых экранов, могут дать серверу ACS инструкции для поддержки дополнительных типов наборов авторизации команд.

Примечание: Наборы Авторизации для выполнения команд PIX требуют, чтобы TACACS + запрос авторизации для выполнения команд определили сервис как *pixshell*. Убедитесь в том, что эта служба реализована в версии операционной системы PIX, используемой на межсетевых экранах; в противном случае для задания авторизации выполнения команд на устройствах PIX используйте наборы авторизации команд интерпретатора. Дополнительные сведения см. в документе Настройка набора авторизации команд интерпретатора для группы пользователей.

Примечание: С Версии PIX OS 6.3 не был внедрен pixshell сервис.

Примечание: Cisco Security Устройства (ASA/PIX) в настоящее время не позволяет пользователю быть размещенным непосредственно в режим включения во время входа в систему. Пользователь должен войти в разрешенный режим вручную.

Для более точного контроля за сеансами администрирования Telnet, размещаемыми на устройствах, сетевое устройство, использующее TACACS+, может запрашивать авторизацию для каждой команды, вводимой в командной строке, перед ее выполнением. Возможно задать набор команд, которые разрешены или запрещены к выполнению конкретным пользователем на данном устройстве. Сервер ACS развивает эту возможность, предлагая следующие функции:

- **Многоразовые именованные наборы авторизации для выполнения команд. Не указывая непосредственного пользователя или группу пользователей, можно создать именованный набор авторизаций для выполнения команд.** Возможно определить несколько наборов авторизации для выполнения команд, разграничивающих различные профили доступа. Пример:*Набор авторизации для выполнения команд Help desk (Служба сопровождения) может разрешать доступ к высокоуровневым командам обзора, например, show run, запрещая выполнение команд конфигурации.Набор авторизации для выполнения All network engineers (Все специалисты по сетям) может содержать ограниченный список разрешенных команд для любого специалиста по сетям на предприятии.Набор авторизации для выполнения команд Local network engineers (Специалисты локальной сети) может разрешить все команды (и включать в себя команды настройки IP-адреса).*
- **Высокая детализация конфигурации.——Можно создать ассоциации между именованными наборами авторизации для выполнения команд и группами сетевых устройств (NDG).** Это позволяет определить различные профили доступа для пользователей в зависимости от того, с каких сетевых устройств происходит доступ. Можно связать один именованный набор авторизации для выполнения команд сразу с несколькими группами NDG и использовать его для нескольких групп пользователей. Сервер ACS обеспечивает целостность информации. Именованные наборы авторизации для выполнения команд хранятся во внутренней базе данных ACS. Для их резервного копирования и восстановления можно использовать функции резервного копирования и восстановления сервера ACS. Также можно копировать наборы авторизации для выполнения команд на вторичные серверы ACS вместе с другими данными конфигурации.

Виды наборов авторизации для выполнения команд, поддерживающие приложения для управления устройствами Cisco, обладают аналогичными преимуществами с точки зрения их использования. Можно применять наборы авторизации для выполнения команд к группам ACS, содержащим пользователей приложения управления устройством для того, чтобы применять авторизацию различных полномочий в приложении управления устройством. Группы ACS могут соответствовать различным ролям в пределах приложения для управления устройством. Разные наборы авторизации для выполнения команд можно применять к отдельным группам.

Сервер ACS предусматривает три последовательных ступени фильтров авторизации выполнения команд. Каждый запрос авторизации выполнения команд анализируется в следующем порядке:

1. **Сопоставление команд.—Сервер ACS определяет, присутствует ли обрабатываемая команда в списке набора авторизации для выполнения команд.** Если команда в списке отсутствует, то авторизация для ее выполнения определяется настройкой Unmatched Commands (Не найденные команды): *permit (разрешать) или deny (запрещать).* В противном случае, если команда присутствует, анализ продолжается.
2. **Сопоставление аргументов.—Сервер ACS определяет, присутствуют ли аргументы команды в списке набора авторизации для выполнения команд.**Если имеется хотя бы один отсутствующий аргумент, то авторизация для выполнения команды зависит от того, включен ли параметр Permit Unmatched Args (Разрешать отсутствующие аргументы). Если отсутствующие аргументы разрешены, то команда получает авторизацию, и анализ завершается; в противном случае команда запрещается, и анализ заканчивается.При совпадении всех аргументов анализ продолжается.

3. **Политика аргументов. После того, как ACS найдет аргументы команды в наборе авторизации, ACS проверяет, разрешен ли каждый аргумент явным образом.** Если все аргументы разрешены явным образом, то сервер ACS предоставляет авторизацию для выполнения команды. Если же какие-либо аргументы не разрешены, ACS отказывает в авторизации.

Добавление набора авторизации для команд интерпретатора

Этот раздел содержит следующие сценарии, описывающие порядок добавления набора авторизации для выполнения команд:

- Сценарий 1: Полномочия для доступа на чтение и запись или полного доступа
- Сценарий 2: Полномочия для доступа только на чтение
- Ситуация 3: Полномочия для ограниченного доступа

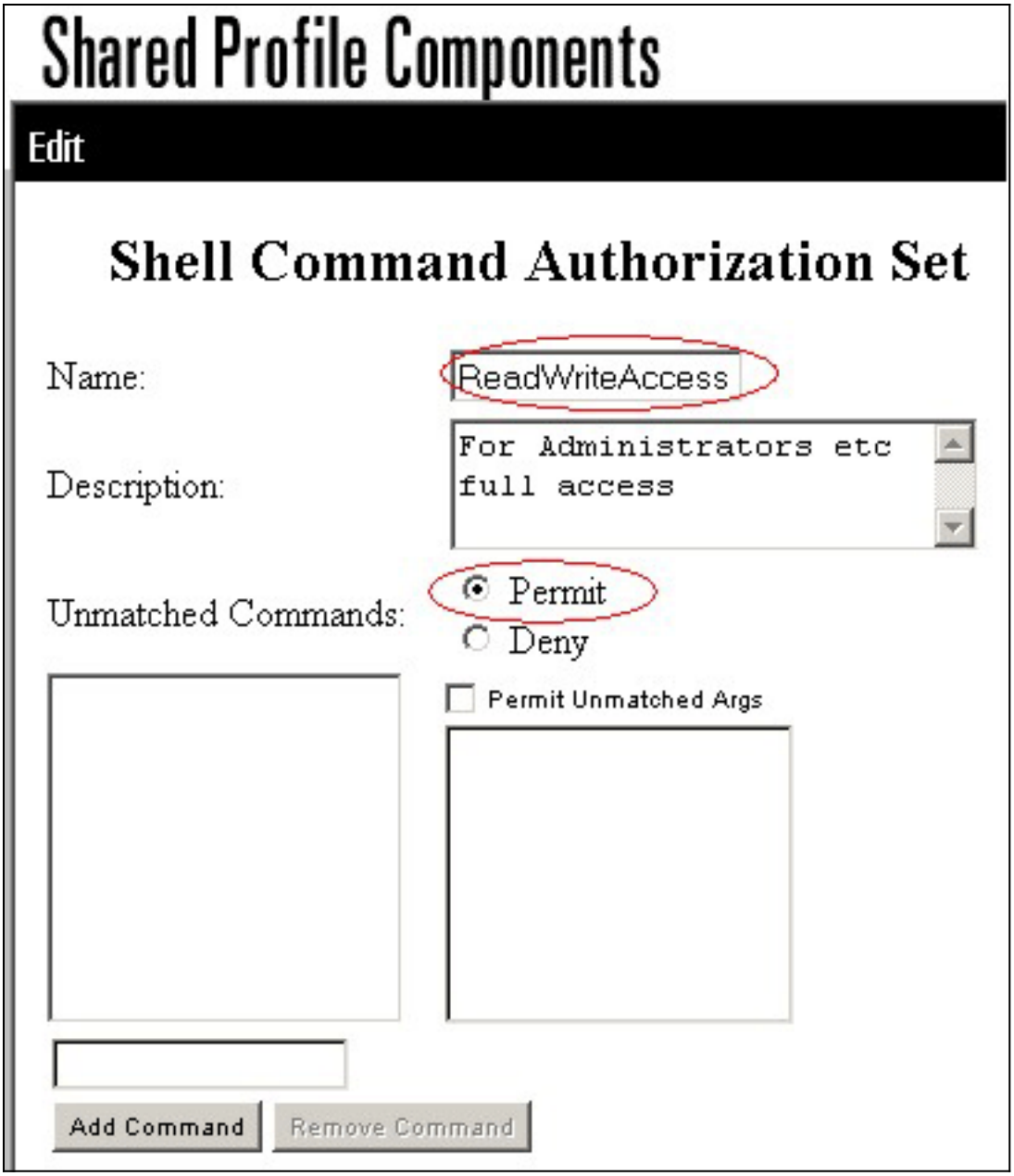
Примечание: См. Добавление раздела Набора Авторизации для выполнения команд Руководства пользователя для сервера Cisco Secure Access Control Server 4.1 для получения дополнительной информации о том, как создать наборы авторизации для выполнения команд. Дополнительные сведения об изменении и удалении наборов авторизации команд можно найти в документах Изменение набора авторизации для выполнения команд и Удаление набора авторизации для выполнения команд.

Сценарий 1: Полномочия для доступа на чтение и запись или полного доступа

В этом сценарии пользователям предоставлен доступ для чтения и запись (полный доступ).

В окне Shared Profile Components (Компоненты общего профиля) настройте следующие параметры в разделе Shell Command Authorization Set (Набор авторизации для выполнения команд интерпретатора):

1. **В поле Name (Имя) введите имя набора авторизации для выполнения команд: ReadWriteAccess.**
2. В поле Description (Описание) введите описание набора авторизации для выполнения команд.
3. **Выберите переключатель Permit (Разрешить) и нажмите кнопку Submit (Отправить).**

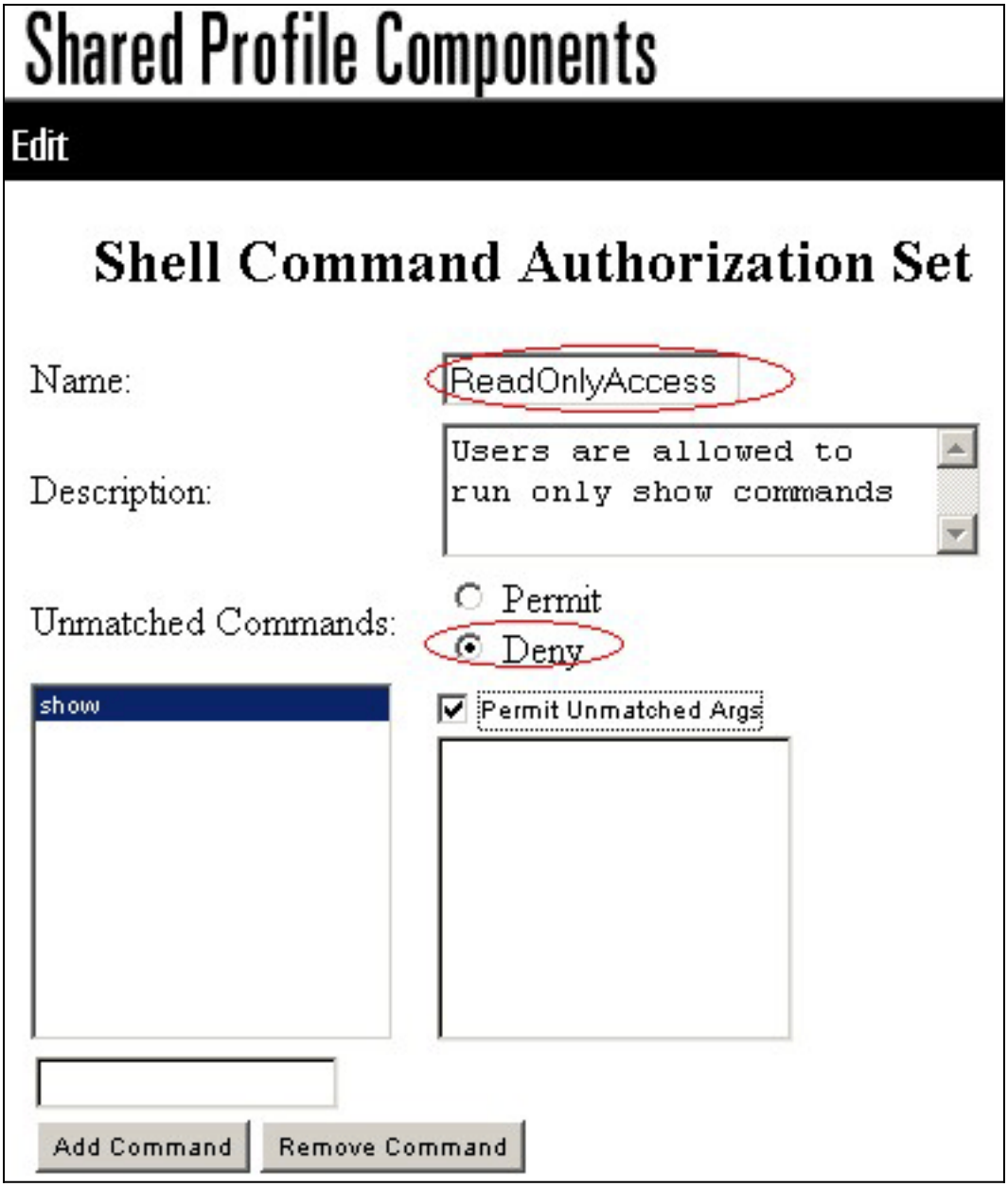


Сценарий 2: Полномочия для доступа только на чтение

В этом сценарии пользователи могут использовать только команды show.

В окне Shared Profile Components (Компоненты общего профиля) настройте следующие параметры в разделе Shell Command Authorization Set (Набор авторизации для выполнения команд интерпретатора):

1. **В поле Name (Имя) введите имя набора авторизации для выполнения команд: ReadOnlyAccess.**
2. В поле Description (Описание) введите описание набора авторизации для выполнения команд.
3. **Нажмите кнопку Deny (Запретить).**
4. **В поле над кнопкой Add Command (Добавить команду) введите команду show, затем нажмите кнопку Add Command.**
5. **Отметьте флажок Permit Unmatched Args (Разрешать отсутствующие аргументы) и нажмите кнопку Submit (Отправить)**

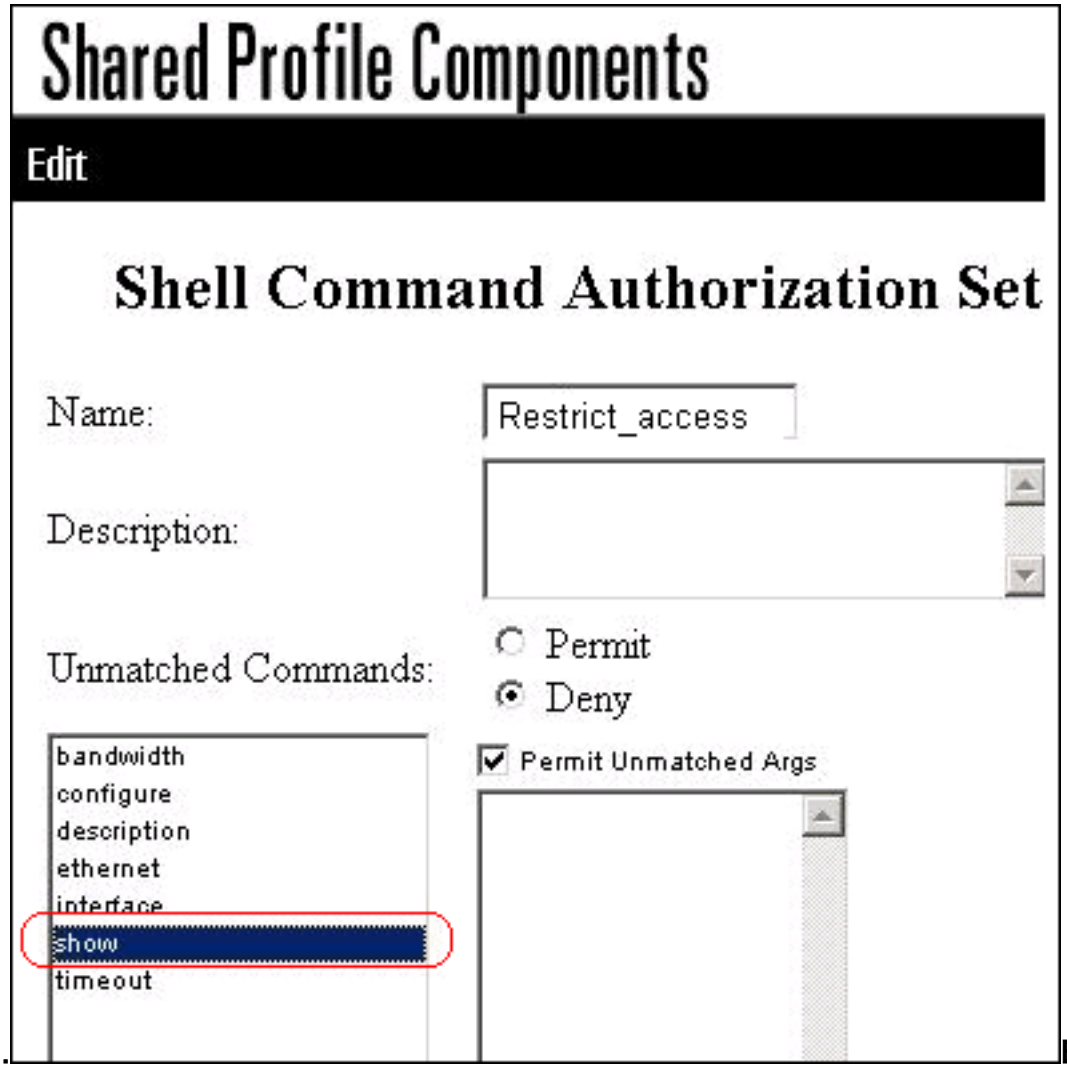


Ситуация 3: Полномочия для ограниченного доступа

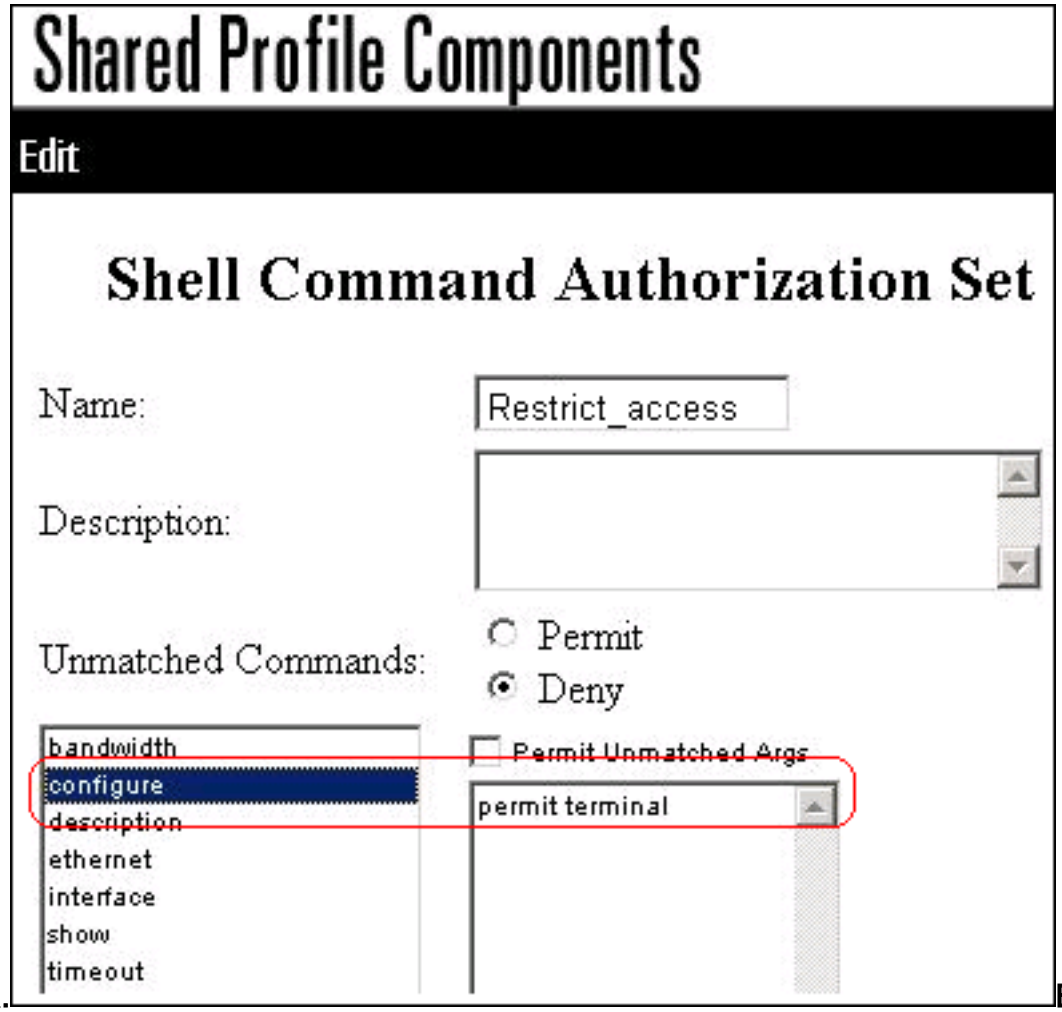
В этом сценарии пользователи могут использовать выбранные подмножества команд.

В окне Shared Profile Components (Компоненты общего профиля) настройте следующие параметры в разделе Shell Command Authorization Set (Набор авторизации для выполнения команд интерпретатора):

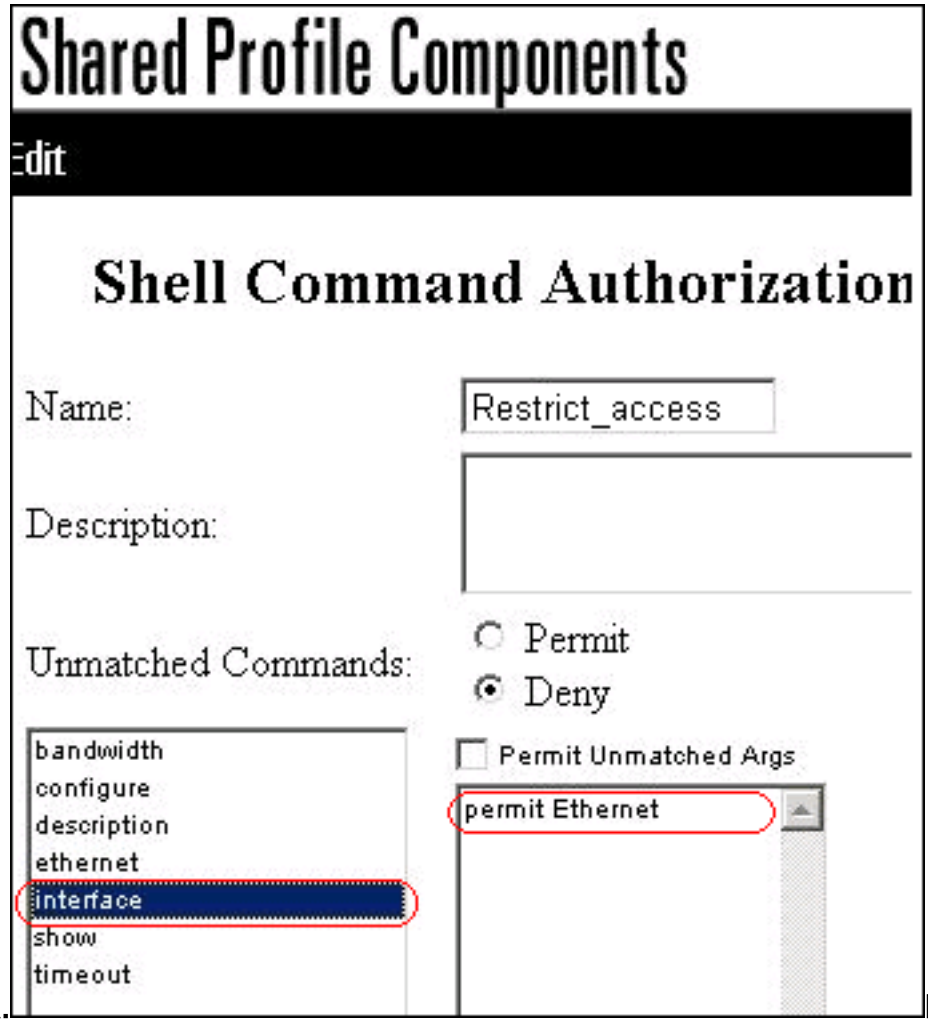
1. **В поле Name (Имя) введите имя набора авторизации для выполнения команд: Restrict_access.**
2. **Нажмите кнопку Deny (Запретить).**
3. Введите команды, которые требуется разрешить на клиентах AAA.**В поле над кнопкой Add Command (Добавить команду) введите команду show, затем нажмите кнопку Add**



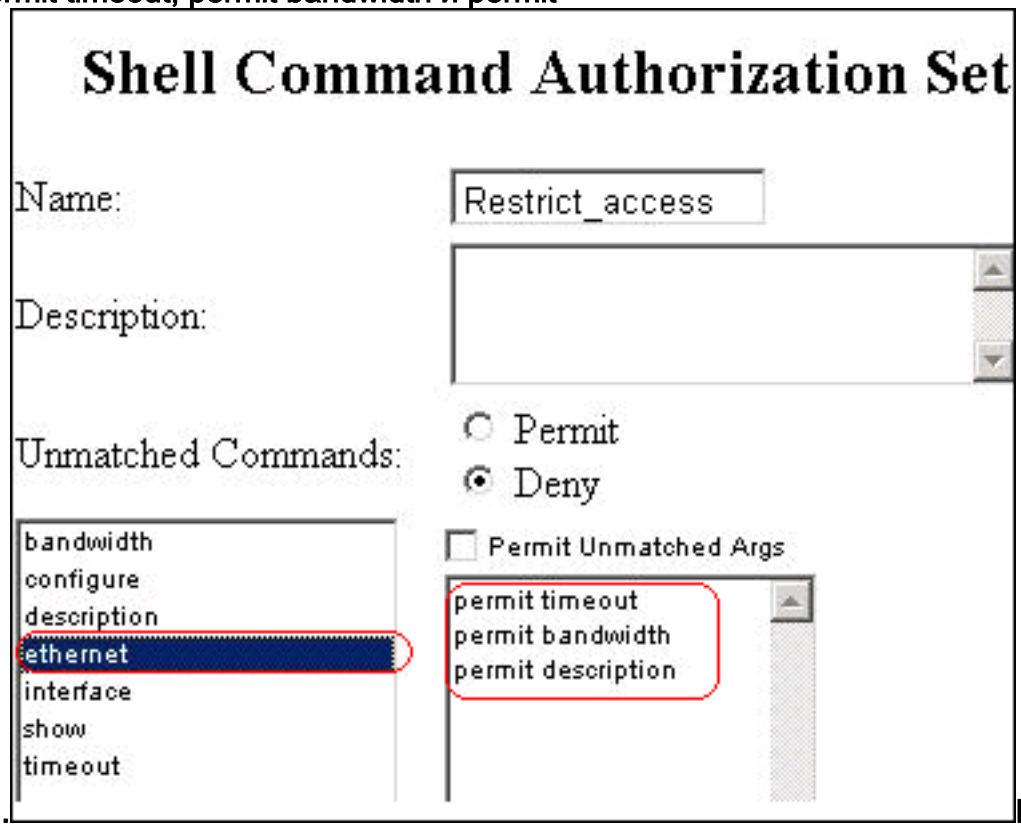
Command.Введите команду configure и нажмите кнопку Add Command.Выберите команду configure и введите permit terminal в поле



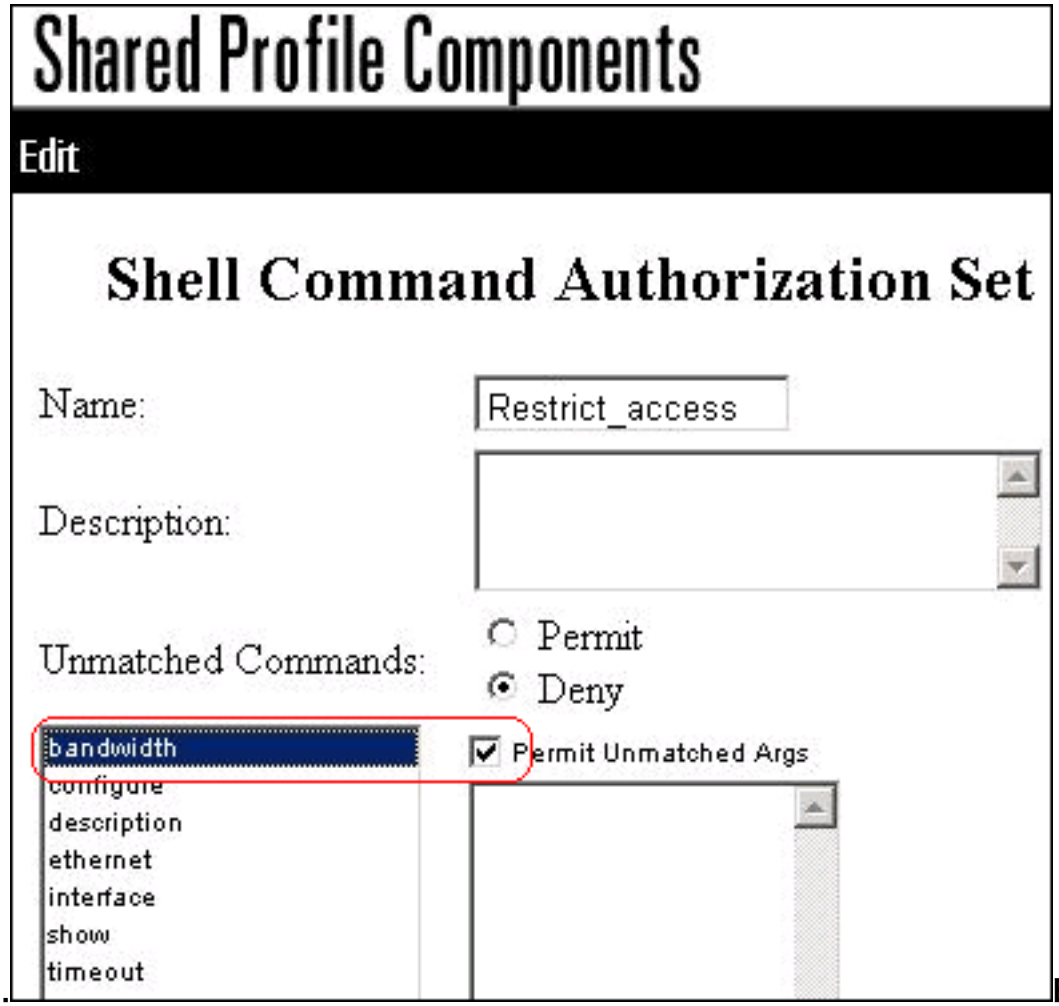
справа.Введите команду interface и нажмите кнопку Add Command.Выберите команду interface и введите permit Ethernet в поле



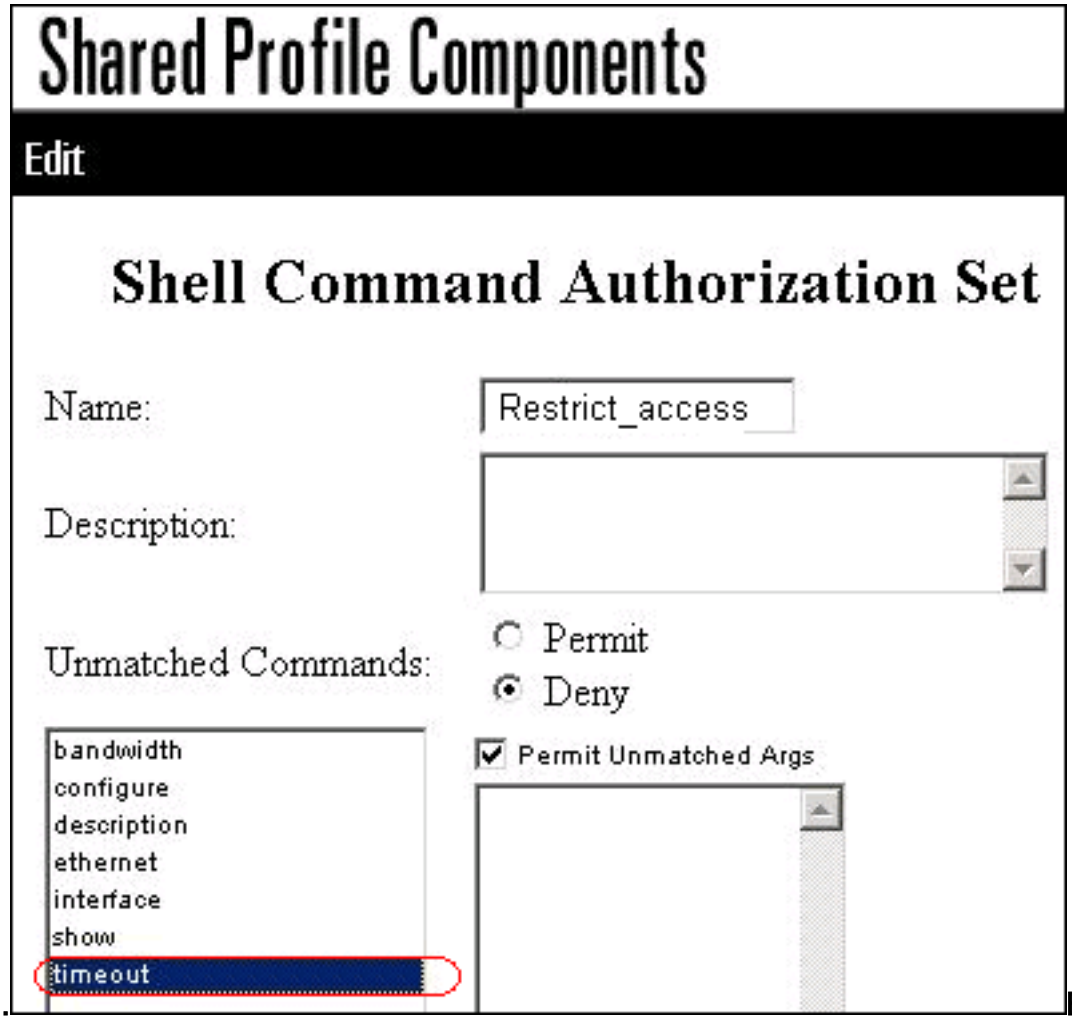
справа.Введите команду ethernet и нажмите кнопку Add Command.Выберите команду interface и введите в поле справа: permit timeout, permit bandwidth и permit



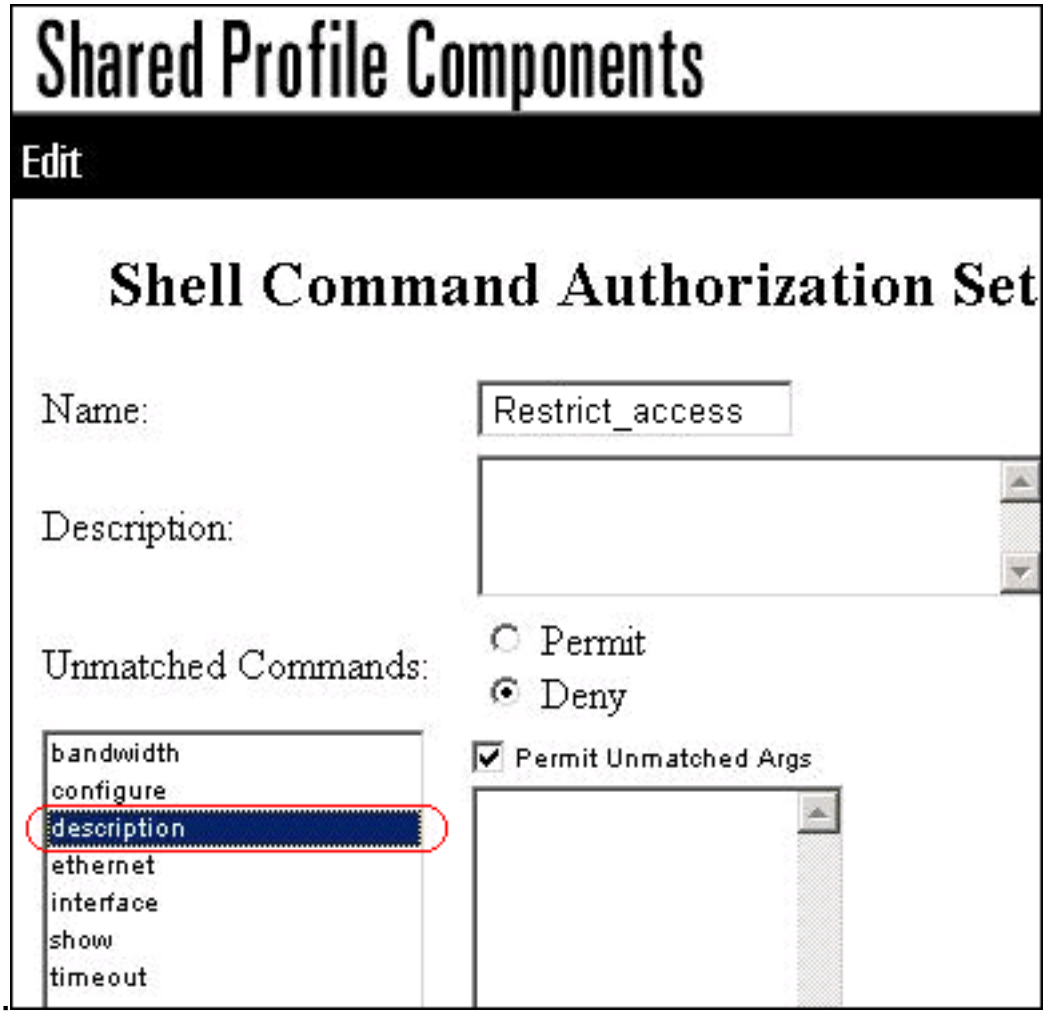
description.Введите команду bandwidth и нажмите кнопку Add



Command. Введите команду timeout и нажмите кнопку Add



Command. Введите команду description и нажмите кнопку Add



Command.

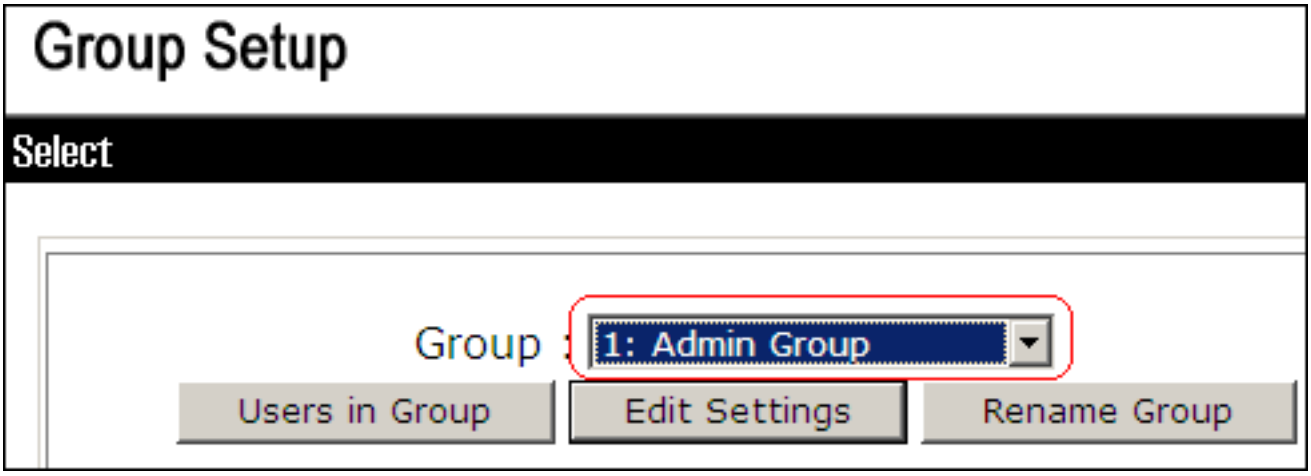
4. Нажмите кнопку Submit (Отправить).

Связывание набора авторизации команд интерпретатора с группой пользователей

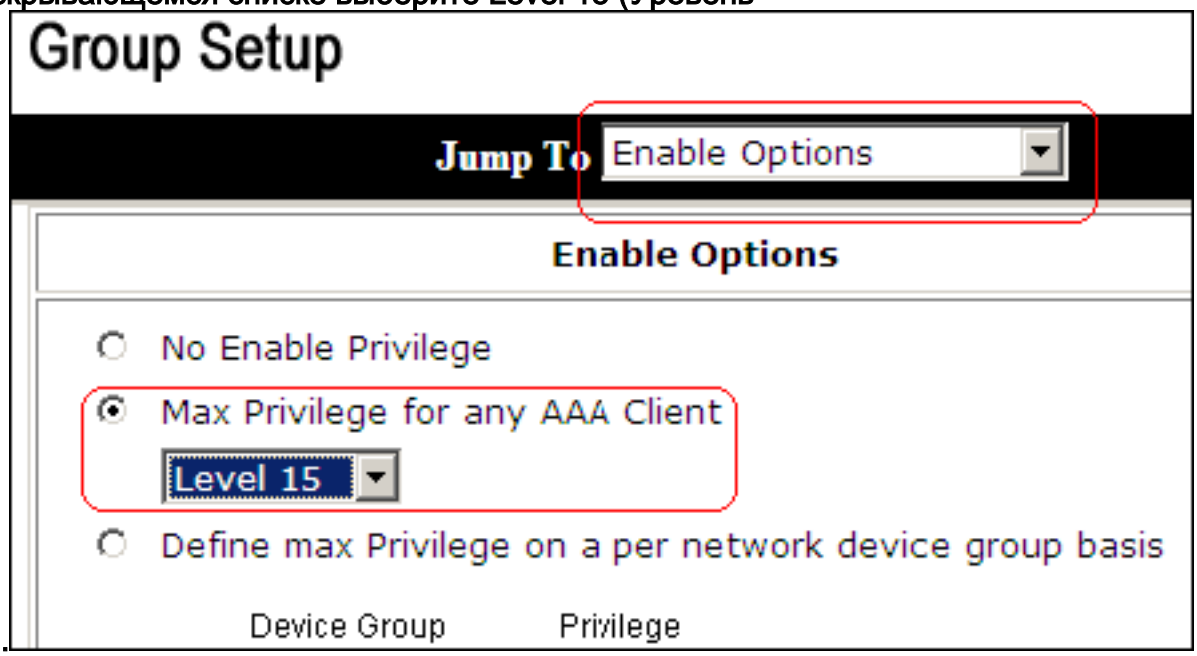
См. Настройку Набор авторизации команд Shell для раздела Группы пользователей Руководства пользователя для сервера Cisco Secure Access Control Server 4.1 для получения дополнительной информации о том, как настроить группы конфигурации для пользователя набора авторизации для выполнения команд оболочки.

Связывание набора авторизации команд интерпретатора (доступ на чтение и запись) с группой пользователей (группой администраторов)

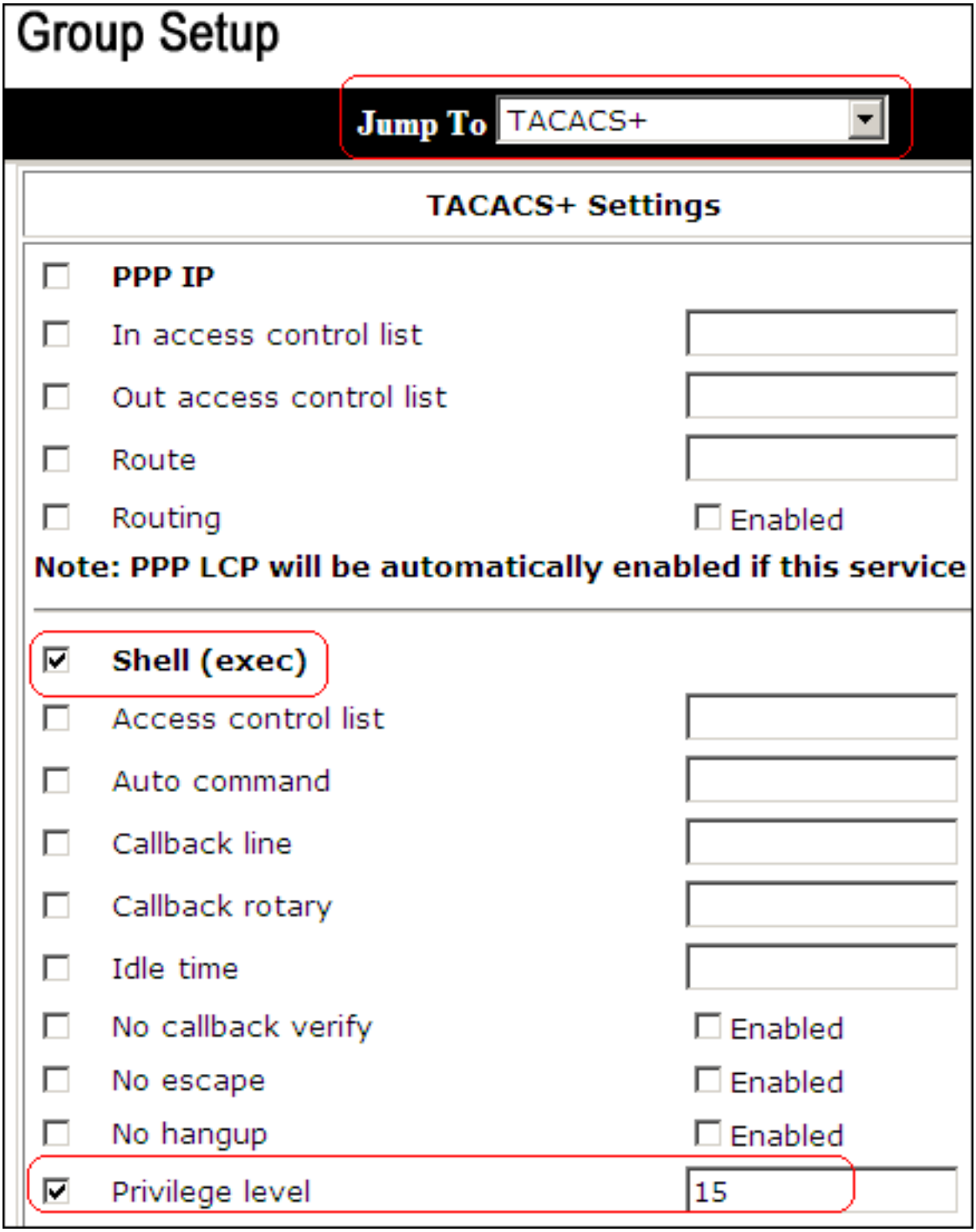
1. В окне ACS щелкните Group Setup (Настройка групп) и в раскрывающемся списке Group (Группа) выберите Admin Group (Группа администраторов).



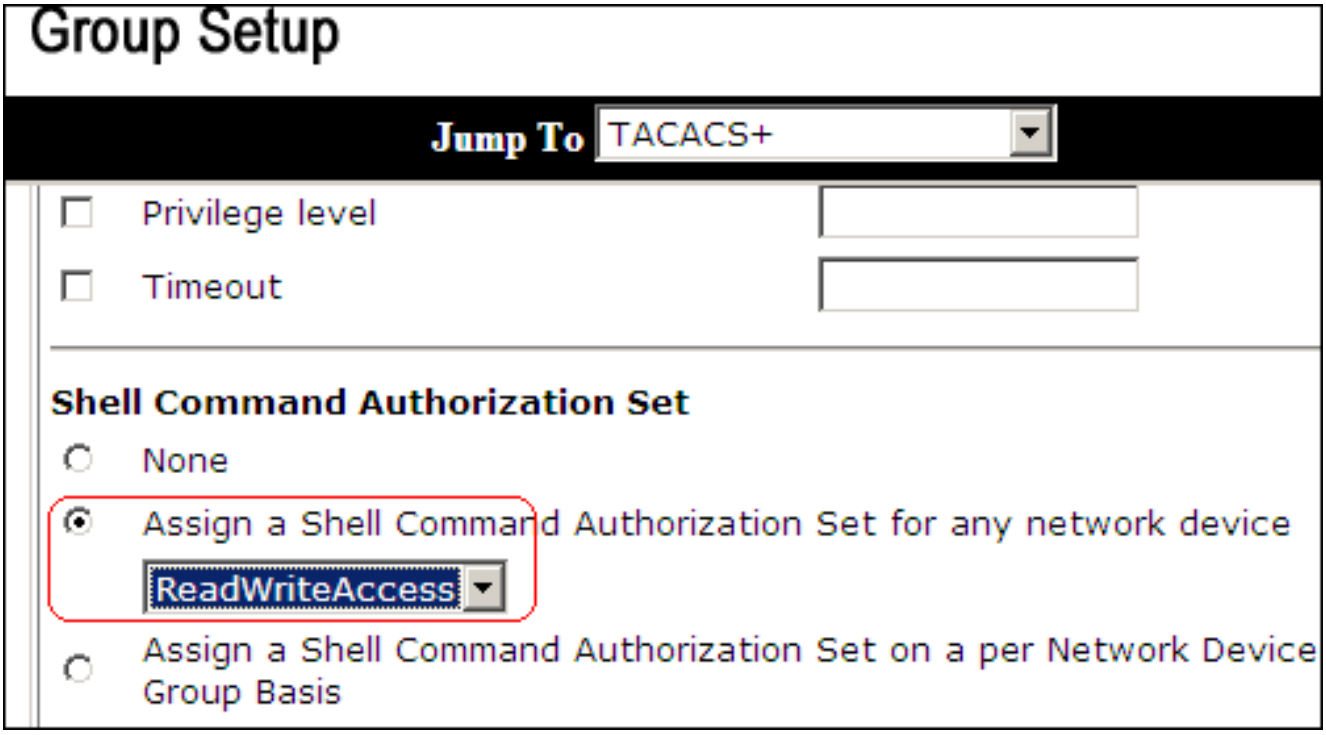
2. Нажмите кнопку Edit Settings (Изменить настройки).
3. В раскрывающемся списке Jump To (Перейти к) выберите Enable Options (Разрешение параметров).
4. В разделе Enable Options (Разрешение параметров) выберите переключатель Max Privilege for any AAA client (Максимальные полномочия для любого клиента AAA) и в раскрывающемся списке выберите Level 15 (Уровень



15).
5. В раскрывающемся списке Jump To (Перейти к) выберите TACACS+.
6. В разделе TACACS+ Settings (Настройки TACACS+) установите флажок Shell (exec), отметьте флажок Privilege level и введите 15 в поле Privilege level (Уровень полномочий).



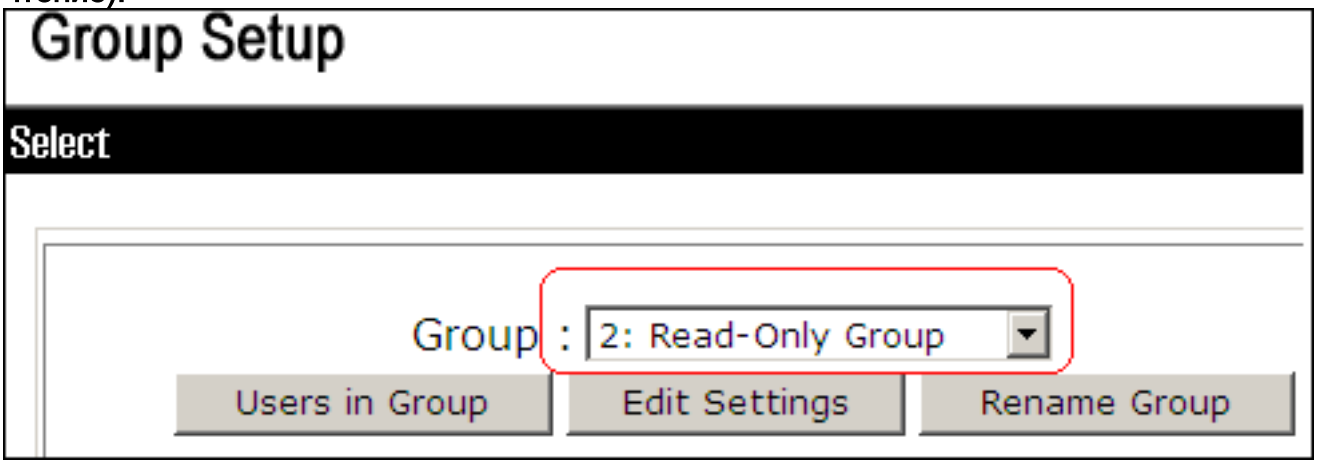
7. В разделе Shell Command Authorization Set (Набор авторизации для команд оператора) выберите переключатель Assign a Shell Command Authorization Set for any network device (Назначать набор авторизации команд интерпретатора любому сетевому устройству) и в раскрывающемся списке выберите ReadWriteAccess.



8. Нажмите кнопку Submit (Отправить)

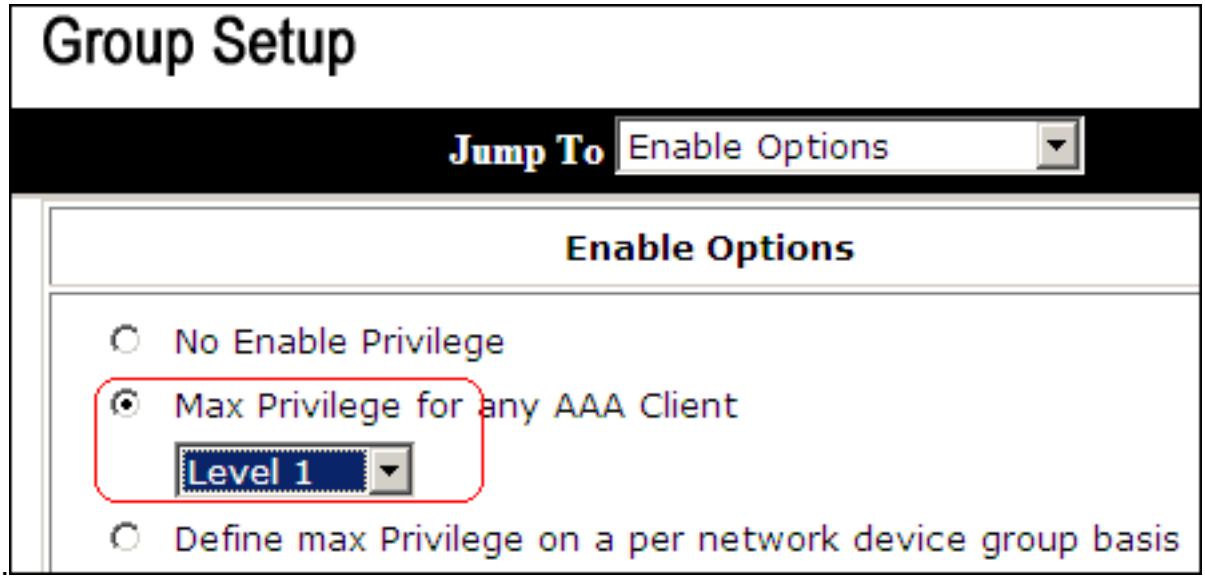
Связывание набора авторизации команд интерпретатора (доступ только на чтение) с группой пользователей (группой доступа только на чтение)

1. В окне ACS щелкните Group Setup (Настройка групп) и в раскрывающемся списке Group (Группа) выберите Read-Only Group (Группа доступа только на чтение).

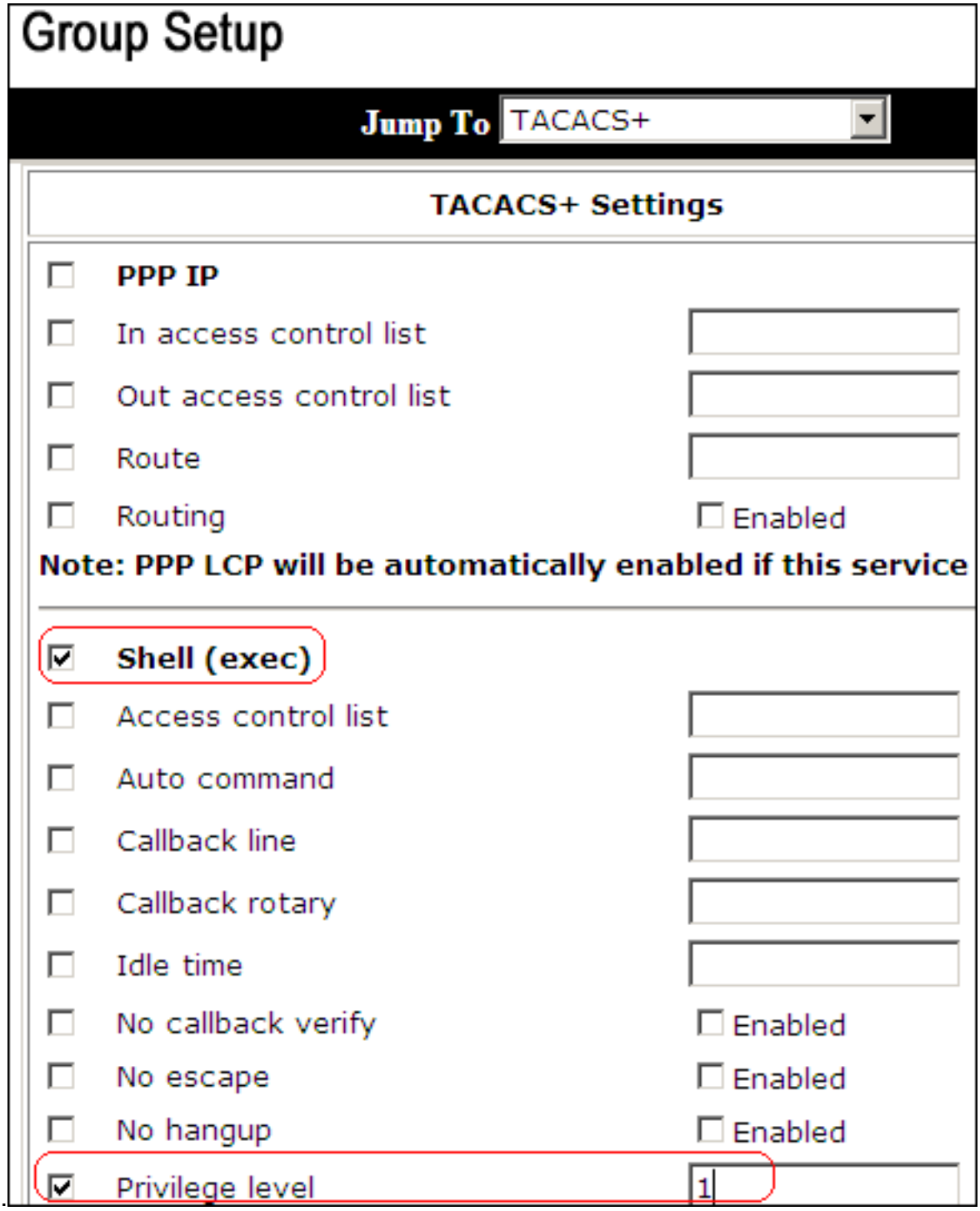


2. Нажмите кнопку Edit Settings (Изменить настройки).
3. В раскрывающемся списке Jump To (Перейти к) выберите Enable Options (Разрешение параметров).
4. В области Опций Enable нажмите **Max Privilege для любой** кнопки с зависимой фиксацией **клиента AAA** и выберите **Level 1** из выпадающего

списка.



5. В области TACACS + Settings проверьте флажок **Shell (exec)**, проверьте **флажок Privilege level** и войдите **1** в поле Privilege



level.

6. В разделе Shell Command Authorization Set (Набор авторизации для команд оператора) выберите переключатель Assign a Shell Command Authorization Set for any network device (Назначать набор авторизации команд интерпретатора любому сетевому устройству) и в раскрывающемся списке выберите ReadOnlyAccess.

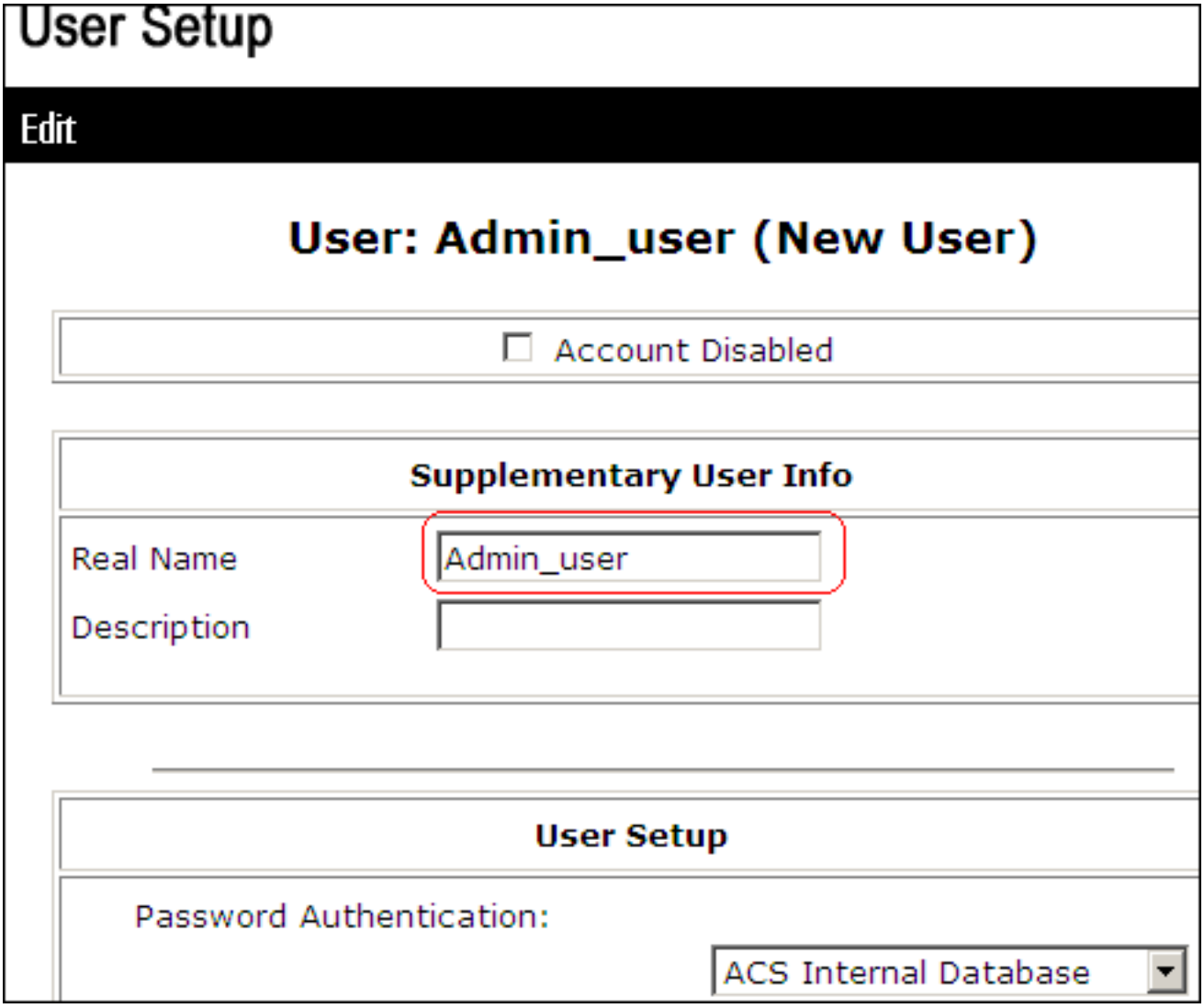
7. **Нажмите кнопку Submit (Отправить)**

Связывание набора авторизации команд интерпретатора (Restrict_access) с пользователем

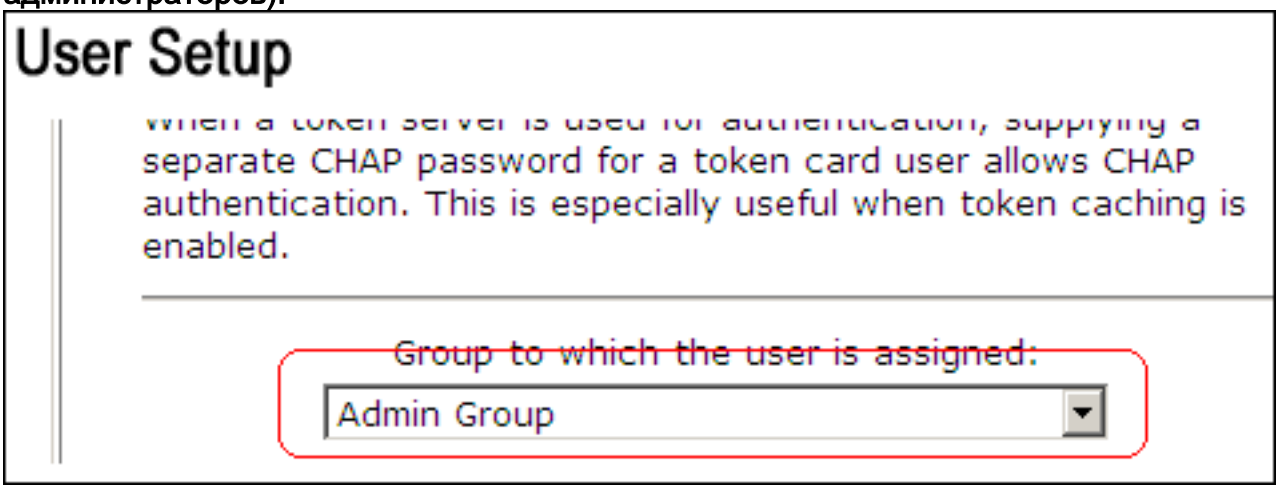
См. Настройку Набор авторизации команд Shell для Пользовательского раздела Руководства пользователя для сервера Cisco Secure Access Control Server 4.1 для получения дополнительной информации о том, как настроить конфигурацию набора авторизации для выполнения команд оболочки для пользователей.

Примечание: Параметры настройки пользовательского уровня отвергают параметры настройки уровня группы в ACS, что означает, есть ли у пользователя набор авторизации для выполнения команд оболочки в параметрах настройки пользовательского уровня, то это отвергает параметры настройки уровня группы.

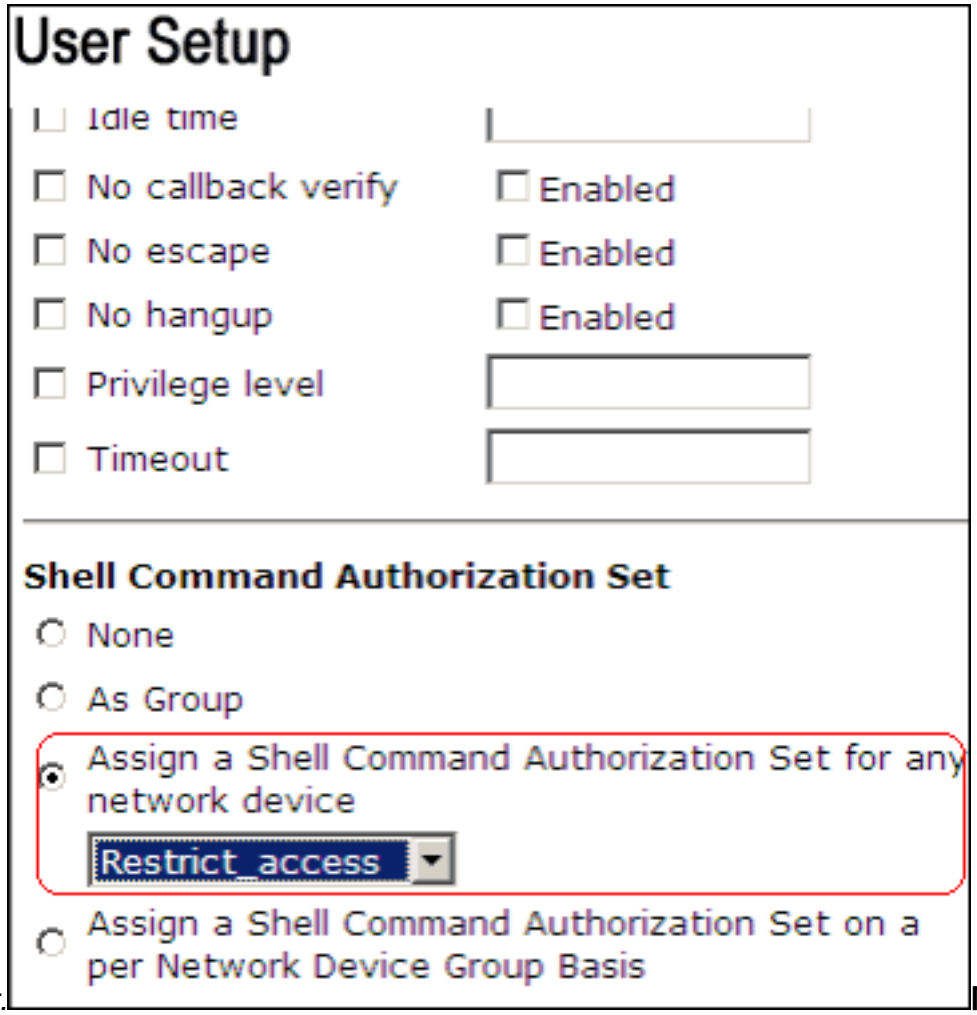
1. **Нажмите User Setup > Add/Edit (Настройка пользователей > Добавить/изменить) для создания нового пользователя Admin_user в составе группы администраторов.**



2. В раскрывающемся списке группы, к которой относится пользователь, выберите Admin Group (Группа администраторов).



3. В разделе Shell Command Authorization Set (Набор авторизации для команд оператора) выберите переключатель Assign a Shell Command Authorization Set for any network device (Назначать набор авторизации команд интерпретатора любому сетевому устройству) и в раскрывающемся списке выберите Restrict_access.**Примечание:** В этом сценарии этот пользователь является частью Admin Group. *Действует набор авторизации команд интерпретатора Restrict_access, а набор авторизации команд интерпретатора ReadWrite Access не*



действует. **Примечание:** В TACACS + (Cisco) раздел области Interface Configuration, гарантируйте, что опция **Shell (exec)** выбрана в Столбце пользователь.

Настройка маршрутизатора IOS

В дополнение к предустановленной конфигурации в маршрутизаторе или коммутаторе IOS необходимо выполнить следующие команды, чтобы реализовать авторизацию выполнения команд посредством сервера 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
```

Конфигурация ASA/PIX/FWSM

В дополнение к предустановленной конфигурации в устройствах ASA/PIX/FWSM необходимо выполнить следующие команды, чтобы реализовать авторизацию выполнения команд посредством сервера ACS:

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

Примечание: Не возможно использовать Протокол RADIUS для ограничения

пользовательского доступа к ASDM в целях только для чтения. Так как Пакеты RADIUS содержат проверку подлинности и авторизация в то же время, у всех пользователей, которые аутентифицируются в сервере RADIUS, есть уровень привилегий 15. Можно достигнуть этого через TACACS с реализацией наборов авторизации для выполнения команд.

Примечание: Даже если ACS недоступен для выполнения авторизации для выполнения команд, ASA/PIX/FWSM занимает много времени для выполнения каждой команды, введенной. Если ACS будет недоступен, и ASA настроили авторизацию для выполнения команд, то ASA все еще запросит авторизацию для выполнения команд на каждую команду.

Устранение неполадок

Ошибка: авторизация для выполнения команд отказала

Проблема

После регистрации к межсетевому экрану посредством регистрации TACACS команды не работают. При вводе команды эта ошибка получена: `command authorization failed`.

Решение

Для устранения указанной неполадки выполните следующие действия:

1. Гарантируйте, что корректное имя пользователя используется и что все требуемые полномочия назначены на пользователя.
2. Если имя пользователя и привилегии корректны, проверяют, что ASA имеет подключение с ACS и что ACS активен.

Примечание: Эта ошибка может также произойти если администратор по ошибке авторизация настроенной команды для локального, а также TACACS, пользователи. В этом случае выполните восстановление пароля для решения вопроса.

Дополнительные сведения

- Cisco PIX Firewall Software
- Справочники по командам для межсетевого экрана PIX Cisco Secure
- Уведомления о дефектах продуктов по безопасности (включая PIX)
- Запросы комментариев (RFC)
- Страница поддержки защищенного сервера управления доступом Cisco
- Cisco Systems – техническая поддержка и документация