PIX 6.2: Пример настройки команды проверки подлинности и авторизация

Содержание

Введение

Авторизация команд PIX и расширение локальной аутентификации были добавлены в версии 6.2. В этом документе приводится пример, как установить это на PIX. Доступные ранее функции аутентификации (например, защищенный интерпретатор команд (SSH), подключение с клиента IPSEC на ПК и т.п.) остаются доступными, но не рассматриваются в настоящем документе. Выполняемыми командами можно управлять локально на PIX или удаленно через TACACS+. Авторизация для выполнения команд RADIUS не поддерживается; это ограничение протокола RADIUS.

Локальная авторизация на исполнение команд осуществляется с помощью назначения команд и пользователей привилегированным уровням.

Удаленная авторизация команд выполняется при помощи сервера аутентификации, авторизации и учета (AAA) TACACS+. Если один недоступен, можно назначить несколько AAA-серверов.

Аутентификация также работает при использовании предварительно настроенных подключений IPSec и SSH. Аутентификация SSH требует, чтобы вы выполнили эту команду:

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

Примечание: Если AAA-сервер недоступен, при использовании TACACS + или группа сервера RADIUS для аутентификации можно настроить PIX для использования локальной базы данных в качестве Метода **НЕЙТРАЛИЗАЦИИ**.

Пример

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

Можно альтернативно использовать локальную базу данных в качестве основного способа аутентификации (без нейтрализации), если вы входите ЛОКАЛЬНЫЙ один.

Например, введите эту команду для обнаружения учетной записи пользователя в локальной базе данных и выполнения локальной проверки подлинности для соединения SSH:

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

См. то, Как Выполнить Проверку подлинности и включение на Cisco Secure PIX Firewall (от 5.2 до 6.2) для получения дополнительной информации о том, как создать Доступ с проверкой подлинности AAA к Межсетевому экрану PIX, который выполняет Версию ПО PIX 5.2 до 6.2, и для получения дополнительной информации о включают аутентификацию, запись в системный журнал и получающий доступ, когда AAA-сервер не работает.

См. PIX/ASA: Сквозной Прокси для Доступа к сети с помощью TACACS + и Пример Конфигурации сервера RADIUS для получения дополнительной информации о том, как создать АУТЕНТИФИЦИРУЕМЫЙ НА AAA (Сквозной Прокси) обращается к Межсетевому экрану PIX, который выполняет Версии ПО PIX 6.3 и позже.

Если настройка выполнена правильно, доступ к PIX не может быть заблокирован. Если конфигурация не сохранена, перезагружение PIX должно возвратить ее к своему состоянию предварительного конфигурирования. Если PIX недоступен из-за неправильной конфигурации, воспользуйтесь процедурами восстановления пароля и конфигурации AAA для PIX.

Перед началом работы

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Предварительные условия

Для данного документа отсутствуют предварительные условия.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Программное обеспечение PIX версии 6.2
- Cisco Secure ACS для Версии Windows 3.0 (ACS)

- Cisco Secure ACS для UNIX (CSUnix) версия 2.3.6

Сведения, содержащиеся в данном документе, были получены с устройств в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. При работе с реальной сетью необходимо полностью осознавать возможные результаты использования всех команд.

Тестирование перед добавлением аутентификации или авторизации

До реализования новых 6.2 опций аутентификации/авторизации удостоверьтесь, что вы в настоящее время в состоянии получить доступ к PIX с помощью этих команд:

```
!--- IP range allowed to Telnet to the PIX (values depend on network). telnet 172.18.124.0
255.255.255.0 !--- Telnet password. passwd <password> !--- Enable password. enable password
<password>
```

Общие сведения о настройке привилегий

Большинство команд в PIX на уровне 15, невзирая на то, что некоторые на уровне 0. Для просмотра текущих параметров для всех команд используйте эту команду:

```
show privilege all
```

Большинство команд на уровне 15 по умолчанию, как показано в данном примере:

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

Несколько команд на уровне 0, как показано в данном примере:

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

PIX может работать в, включают и настраивают режимы. Некоторые команды, такие как **show logging**, доступны в режимах Both. Для установки привилегий на этих командах необходимо задать режим, что команда существует в, как показано в примере. Другой параметр режима**, включают**. Вы получаете сообщение об ошибках `logging is a command available in multiple modes`. Если вы не настраиваете режим, используйте **команду mode [enable|configure]**:

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

Эти примеры обращаются к команде **часов**. Используйте эту команду для определения текущих параметров для команды **часов**:

```
show privilege command clock
```

Выходные данные **команды show privilege command clock** показывают, что команда **часов** существует в этих трех форматах:

```
!--- Users at level 15 can use the show clock command. privilege show level 15 command clock !--
- Users at level 15 can use the clear clock command. Privilege clear level 15 command clock !---
Users at level 15 can configure the clock !--- (for example, clock set 12:00:00 Jan 01 2001).
privilege configure level 15 command clock
```

Проверка подлинности/Авторизация – локальные имена пользователей

Прежде, чем изменить уровень привилегий команды **часов**, необходимо перейти к консольному порту, чтобы настроить административного пользователя и включить аутентификацию Локального входа в систему, как показано в данном примере:

```
GOSS(config)# username poweruser password poweruser privilege 15 GOSS(config)# aaa-server LOCAL protocol local GOSS(config)# aaa authentication telnet console LOCAL
```

PIX подтверждает добавление пользователя, как показано в данном примере:

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

Пользователь "poweruser" должен быть в состоянии к Telnet в PIX и включить с существующим enable password локального PIX (тот от команды *<password>* **enable password**).

Можно добавить больше безопасности путем добавления аутентификации для включения, как показано в данном примере:

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

Это требует, чтобы пользователь ввел пароль и для входа в систему и включил. В данном примере пароль "poweruser" используется и для входа в систему, и включить. Пользователь "poweruser" должен иметь возможность подключения с помощью Telnet к PIX и ввода пароля PIX.

Если вы хотите, чтобы некоторые пользователи были в состоянии только использовать определенные команды, необходимо установить пользователя с более низкими привилегиями, как показано в данном примере:

```
GOSS(config)# username ordinary password ordinary privilege 9
```

Поскольку практически все команды находятся на уровне 15 по умолчанию, необходимо переместить некоторые команды вниз до уровня 9 так, чтобы их могли выполнять "обычные" пользователи. В этом случае вы хотите, чтобы ваш пользователь уровня 9 был в состоянии использовать **команду show clock**, но не реконфигурировать часы, как показано в данном примере:

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

Вам также нужен ваш пользователь, чтобы быть в состоянии выйти из PIX (пользователь мог бы быть в уровне 1 или 9, желая сделать это), как показано в данном примере:

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

Вам нужен пользователь, чтобы быть в состоянии использовать **команду enable** (пользователь в в уровне 1 при попытке этого), как показано в данном примере:

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

Путем перемещения **запрещать** команды в уровень 1 любой пользователь между уровнями 2-15 может выйти из режима включения, как показано в данном примере:

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

Если вы, которых Telnet в как "обычный" пользователь и включает как тот же пользователь (пароль также "обычен"), необходимо использовать **привилегию, настраивают команду**

уровня 1, отключают, как показано в данном примере:

```
GOSS# show curpriv Username : ordinary Current privilege level : 9 Current Mode/s : P_PRIV
```

Если у вас открыт исходный сеанс (перед добавлением какой-либо аутентификации), PIX может не иметь информации о вас, поскольку вы не вошли в систему под своим именем пользователя. Если это так, используйте **команду отладки** для просмотра сообщений о пользователе "enable_15" или "enable_1", если нет никакого связанного имени пользователя. Поэтому до авторизации команды конфигурирования используйте сетевой теледоступ к PIX как пользователь “poweruser” (пользователь "уровня 15"), так как необходимо убедиться, что PIX может связать имя пользователя с применяемыми командами. Вы готовы протестировать авторизацию для выполнения команд при помощи этой команды:

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

Пользователь poweruser должен иметь сетевой теледоступ Telnet, включать и выполнять все команды. "Обычный" пользователь должен быть в состоянии использовать **show clock**, **включить**, **отключить**, и команды **выхода из системы**, но никакие другие, как показано в данном примере:

```
GOSS# show xlate Command authorization failed
```

Аутентификация и авторизация на сервере AAA

Вы можете так же аутентифицировать и авторизовать пользователей, используя сервер AAA. TACACS+ подходит лучше всего, поскольку на нем возможна командная авторизация, но можно использовать и RADIUS. Проверьте, чтобы видеть, существует ли предыдущий сеанс сетевого теледоступа AAA / команды консоли на PIX (если **команда LOCAL AAA** ранее использовалась), как показано в данном примере:

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

Если существует предыдущий сеанс сетевого теледоступа AAA / команды консоли, удаляет их при помощи этих команд:

```
GOSS(config)# no aaa authorization command LOCAL GOSS(config)# no aaa authentication telnet
console LOCAL GOSS(config)# no aaa authentication enable console LOCAL
```

Как с настройкой локальной проверки подлинности, тест для проверки пользователи могут Telnet в PIX при помощи этих команд.

```
telnet 172.18.124.0 255.255.255.0 !--- IP range allowed to telnet to the PIX (values would
depend on network). passwd <password> !--- Telnet password. Enable password <password> !---
Enable password.
```

В зависимости от какого сервера вы используете, настраиваете PIX для аутентификации/авторизации с AAA-сервером.

ACS - TACACS+

Настройте ACS для передачи с PIX путем определения PIX в Конфигурации сети с TACACS "Используемой аутентификации" + (для программного обеспечения Cisco IOS). Конфигурация пользователя ACS зависит от конфигурации PIX. Как минимум пользователь ACS должен быть установлен с именем пользователя и паролем.

На PIX используйте эти команды:

```
GOSS(config)# enable password cisco123 GOSS(config)# aaa-server TACSERVER protocol tacacs+
GOSS(config)# aaa-server TACSERVER (inside) host timeout 10 GOSS(config)# aaa authentication
telnet console TACSERVER
```

На этом этапе пользователь ACS должен быть в состоянии к Telnet в PIX, включить его с существующим enable password на PIX и выполнить все команды. Выполните следующие действия:

1. Если существует потребность сделать, PIX включает аутентификацию с ACS, выбирает **Interface Configuration> Advanced TACACS + Параметры настройки**.
2. Проверьте **Advanced TACACS + Функции в** коробке **Пунктов меню Advanced Configuration Option**.
3. **Нажмите кнопку Submit (Отправить).** Advanced TACACS + Параметры настройки теперь видимы под пользовательской конфигурацией.
4. Установите Привилегию Max для любого Клиента AAA к Уровню 15.
5. Выберите схему enable password пользователя (который мог включить настройку отдельного enable password).
6. **Нажмите кнопку Submit (Отправить).**

Для включения включают аутентификацию через TACACS + в PIX, используют эту команду:

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

На этом этапе пользователь ACS должен быть в состоянии к Telnet в PIX и включить с enable password, настроенным в ACS.

До добавляющей авторизации для выполнения команд PIX должен быть исправлен ACS 3.0. Можно загрузить исправление от Центра программного обеспечения (только зарегистрированные клиенты). Можно также просмотреть дополнительные сведения об этом исправлении путем доступа к идентификатору ошибки Cisco CSCdw78255 (только зарегистрированные клиенты).

Проверка подлинности должна быть включена до выполнения команды авторизации. Если существует потребность выполнить авторизацию для выполнения команд с ACS, выбрать **Interface Configuration> TACACS + (Cisco)> Shell (Exec) для пользователя и/или группы** и нажать **Submit**. Параметры настройки авторизации для выполнения команд оболочки теперь видимы при пользователе (или группа) конфигурация.

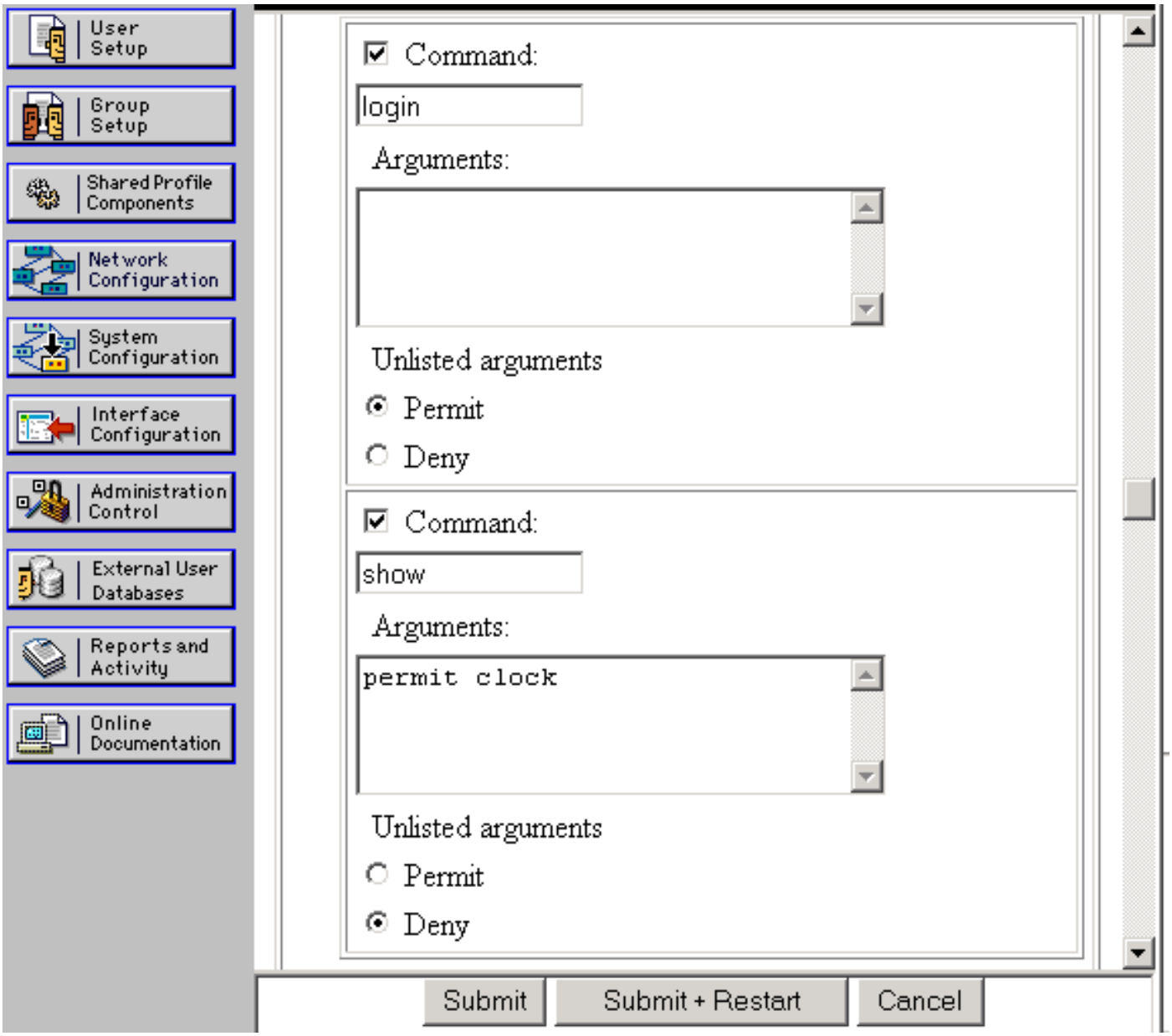
Это - хорошая идея установить по крайней мере одного пользователя высокопроизводительного сервера управления доступом (ACS) для авторизации для выполнения команд и разрешить несопоставленные Команды Cisco IOS.

Другие пользователи ACS могут быть установлены с авторизацией для выполнения команд путем разрешения подмножества команд. Данный пример использует эти шаги:

1. Выберите Group Settings для обнаружения желаемой группы от раскрывающегося окна.
2. **Нажмите кнопку Edit Settings (Изменить настройки).**
3. Выберите **Shell Command Authorization Set**.
4. Нажмите **Кнопку**.
5. Введите **вход в систему**.
6. Выберите Permit под не включенными в список аргумент.

7. Повторите этот процесс для **выхода из системы**, **включите** и **отключите** команды.
8. Выберите Shell Command Authorization Set.
9. Нажмите **Кнопку**.
10. **Entershow**.
11. Под Аргументами введите **часы разрешения**.
12. Выберите запрещают для Не включенных в список аргумент.
13. **Нажмите кнопку Submit (Отправить).**

Вот пример этих шагов:



Если у вас все еще есть свой открытый исходный сеанс (тот до добавления любой аутентификации), PIX может не знать, кто вы - то, потому что вы первоначально не входили с именем пользователя ACS. Если это так, используйте **команду отладки** для просмотра сообщений о пользователе "enable_15" или "enable_1", если нет никакого привязанного имени пользователя. Необходимо быть уверены, что PIX может привязать имя пользователя к предпринимаемым командам. Можно сделать это Telnet - сеансом в PIX как пользователь ACS уровня 15 до настройки авторизации для выполнения команд. Вы готовы протестировать авторизацию для выполнения команд при помощи этой команды:

```
aaa authorization command TACSERVER
```

На этом этапе у вас должен быть один пользователь, который должен быть в состоянии к Telnet в, включить и использовать все команды и второго пользователя, который может только сделать пять команд.

CSUnix - TACACS+

Настройте CSUnix для передачи с PIX, как вы были бы с любым другим сетевым устройством. Конфигурация пользователя CSUnix зависит от конфигурации PIX. Как минимум пользователь CSUnix должен быть установлен с именем пользователя и паролем. В данном примере были установлены три пользователя:

```
!--- This is our "poweruser" who can enable, use all commands, and log in. !--- The login
password is in the 'clear "********"' statement. !--- The enable password is in the 'clear
"********" 15' statement. user = pixtest{ password = clear "********" privilege = clear
"********" 15 service=shell { default cmd=permit default attribute=permit } } !--- This user can
Telnet in, enable, and use four commands !--- (such as show clock, logout, exit, and enable). !-
-- The login password is in the 'clear "********"' statement. !--- The enable password is in the
'clear "********" 15' statement. user = limitpix{ password = clear "********" privilege = clear
"********" 15 service=shell { cmd=show { permit "clock" } cmd=logout { permit ".*" } cmd=enable
{ permit ".*" } cmd=exit { permit ".*" } } } !--- This user can Telnet in, but not enable. This
user can use any !--- show commands in non-enable mode as well as logout, exit, and ?. user =
oneuser{ password = clear "********" service=shell { cmd=show { permit ".*" } cmd=logout {
permit ".*" } cmd="?" { permit ".*" } cmd=exit { permit ".*" } } }
```

На PIX используйте эти команды:

```
GOSS(config)# enable password cisco123 GOSS(config)# aaa-server TACSERVER protocol tacacs+
GOSS(config)# aaa-server TACSERVER (inside) host <ip> <key> timeout 10 GOSS(config)# aaa
authentication telnet console TACSERVER
```

На этом этапе любой из пользователей CSUnix должен быть в состоянии к Telnet в PIX, включить с существующим enable password на PIX и использовать все команды.

Включите аутентификацию через TACACS + в PIX:

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

На этом этапе пользователи CSUnix с паролями “privilege 15” могут иметь возможность установить сеанс с Telnet в PIX и включить пароли “enable”.

Если еще открыт первоначальный сеанс (сеанс, открытый перед прохождением аутентификации), межсетевой экран PIX может не распознать пользователя, поскольку изначально не был выполнен вход с указанием имени пользователя. **Если дело в этом, то выполнение команды debug может отобразить сообщения о пользователе "enable_15" или "enable_1", если нет сопоставленного имени пользователя.** Установите Telnet в PIX как пользователя с именем "pixtest" (исходное имя пользователя "level 15") перед настройкой авторизации команды и убедитесь, что PIX связывает имя пользователя с заданными командами. Проверка подлинности должна быть включена до выполнения команды авторизации. Если существует потребность выполнить авторизацию для выполнения команд с CSUnix, добавьте эту команду:

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

Из этих трех пользователей "pixtest" может сделать все, и другие два пользователя могут сделать подмножество команд.

ACS - RADIUS

Авторизация для выполнения команд RADIUS не поддерживается. Telnet и включает аутентификацию, возможно с ACS. ACS может быть настроен для передачи с PIX путем определения PIX в Конфигурации сети с RADIUS "Используемой аутентификации" (любое разнообразие). Конфигурация пользователя ACS зависит от конфигурации PIX. Как минимум пользователь ACS должен быть установлен с именем пользователя и паролем.

На PIX используйте эти команды:

```
GOSS(config)# enable password cisco123 GOSS(config)# aaa-server RADSERVER protocol radius
GOSS(config) # aaa-server RADSERVER (inside) host <ip> <key> timeout 10 GOSS(config)# aaa
authentication telnet console RADSERVER
```

На этом этапе пользователь ACS должен быть в состоянии к Telnet в PIX, включить с существующим enable password на PIX и использовать все команды (PIX не передает команды к серверу RADIUS; Авторизация для выполнения команд RADIUS не поддерживается.

Если вы хотите включить с ACS и RADIUS на PIX, добавьте эту команду:

```
aaa authentication enable console RADSERVER
```

В отличие от этого, с TACACS +, тот же пароль используется для Включения RADIUS что касается Входа RADIUS.

CSUnix - RADIUS

Настройте CSUnix, чтобы говорить с PIX, как вы были бы с любым другим сетевым устройством. Конфигурация пользователя CSUnix зависит от конфигурации PIX. Этот профиль работает для проверки подлинности и включение:

```
user = pixradius{
profile_id = 26
profile_cycle = 1
!--- The login password is in the 'clear "********"' statement; !--- this is used for the login,
enable, and non-enable commands. password = clear "********" < pixradius }
```

На PIX используйте эти команды:

```
GOSS(config)# enable password cisco123 GOSS(config)# aaa-server RADSERVER protocol radius
GOSS(config)# aaa-server RADSERVER (inside) host <ip> <key> timeout 10
```

Если вы хотите включить с ACS и RADIUS на PIX, используйте эту команду:

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

В отличие от этого, с TACACS +, тот же пароль используется для Включения RADIUS что касается Входа RADIUS.

Ограничения доступа к сети

Ограничения доступа к сети могут использоваться и в ACS и в CSUnix для ограничения, кто может соединиться с PIX для административных целей.

- ACS — PIX был бы настроен в области Network Access Restrictions Параметров группы. Конфигурация PIX является или "Denied Calling/Point of Access Locations" или "Permitted Calling/Point of Access Locations" (в зависимости от плана обеспечения безопасности).

- **CSUnix** — Это - пример пользователя, который является доступом разрешен к PIX, но не другими устройствами:
```
user = naruser{
profile_id = 119
profile_cycle = 1
password = clear "********"
privilege = clear "********" 15
service=shell {
allow "10.98.21.50" ".*" ".*"
refuse ".*" ".*" ".*"
default cmd=permit
default attribute=permit
}
}
```

.debug

Для включения отладки используйте эту команду:

```
logging on logging <console|monitor> debug
```

Это примеры пользы и неудачных отладок:

- **Хорошая отладка** — пользователь в состоянии использовать **журнал в**, **включить** и **выполнить** команды.
```
307002: Permitted Telnet login session from 172.18.124.111
111006: Console Login from pixpartial at console
502103: User priv level changed: Uname: pixpartial From: 1 To: 15
111009: User 'pixpartial' executed cmd: show clock
```
- **Неудачная отладка** — Авторизация отказывает для пользователя, как показано в данном примере:`610101: Authorization failed: Cmd: uauth Cmdtype: show`
- **Удаленный сервер AAA недоступен:**`AAA server host machine not responding`

Учет

Нет никакой фактической команды, считающей доступный, но путем активации системного журнала на PIX, вы видите, какие действия были выполнены, как показано в данном примере:

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

Информация, обязательная для сбора в случае обращения в Центр технической поддержки

Если после выполнения перечисленных выше

действий проблема остается, соберите указанные ниже сведения и обратитесь за помощью в Центр технической поддержки Cisco (TAC).
• Описание проблемы и соответствующие сведения о топологии • Меры по устранению неполадок, предпринятые до оформления запроса • **Выходные данные команды show tech-support** • **Выходные данные команды show log после выполнения команды logging buffered debugging или снимки консоли, демонстрирующие проблему (при их наличии)** Приложите собранные сведения по вашей ситуации в простом незаархивированном текстовом файле (.txt). Можно приложить эти сведения, загрузив их с помощью средства Case Query Tool (только для зарегистрированных клиентов). Если средство Case Query недоступно, необходимые данные можно отправить как вложение в электронное сообщение по адресу attach@cisco.com, указав в теме сообщения номер обращения.

Дополнительные сведения

- Справочник по командам PIX
- Программное обеспечение Cisco PIX Firewall - техническая поддержка и документация
- Сервер безопасного контроля доступа Cisco для Windows - техническая поддержка и документация
- Сервер управления безопасного доступа Cisco для Unix - техническая поддержка и документация
- Cisco Systems – техническая поддержка и документация